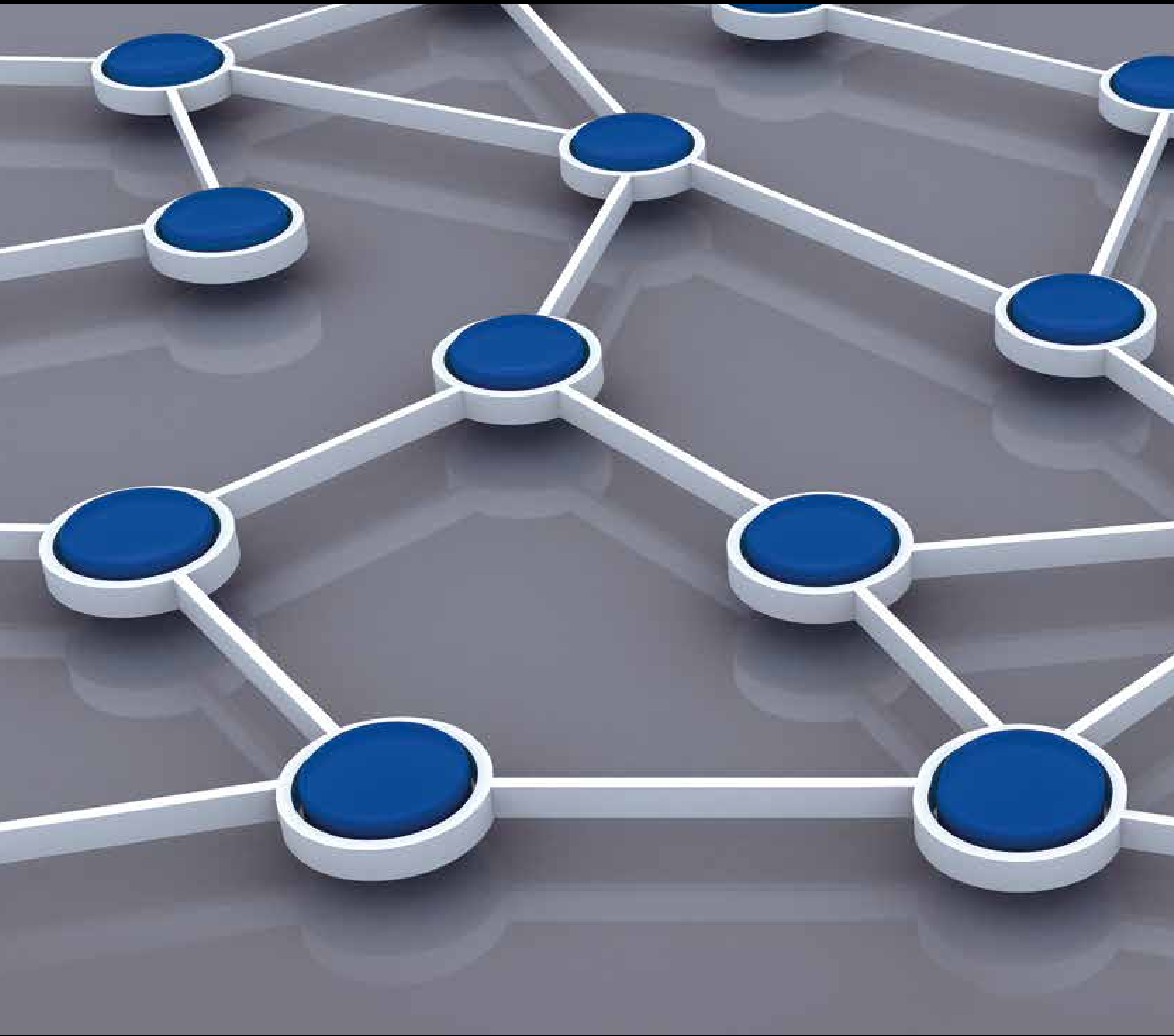
International Journal of Distributed Sensor Networks

Pervasive Sensing Technologies and Emerging Trends

Guest Editors: Jong Hyuk Park, Han-Chieh Chao, Sajid Hussain, and Neil Y. Yen



Pervasive Sensing Technologies and Emerging Trends

International Journal of Distributed Sensor Networks

Pervasive Sensing Technologies and Emerging Trends

Guest Editors: Jong Hyuk Park, Han-Chieh Chao, Sajid Hussain, and Neil Y. Yen

Editorial Board

Tan-Hsu Tan, Taiwan
Guozhen Tan, China
Shaojie Tang, USA
Bulent Tavli, Turkey
Anthony Tzes, Greece
Agustinus B. Waluyo, Australia
Yu Wang, USA
Ran Wolff, Israel
Jianshe Wu, China
Wen-Jong Wu, Taiwan
Chase Qishi Wu, USA
Bin Xiao, Hong Kong
Qin Xin, Faroe Islands
Jianliang Xu, Hong Kong
Yuan Xue, USA
Ting Yang, China
Hong-Hsu Yen, Taiwan
Li-Hsing Yen, Taiwan
Seong-eun Yoo, Korea
Ning Yu, China
Changyuan Yu, Singapore
Tianle Zhang, China
Yanmin Zhu, China
T. L. Zhu, USA
Yi-hua Zhu, China
Qingxin Zhu, China
Li Zhuo, China
Shihong Zou, China

Contents

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 303805, 3 pages
http://dx.doi.org/10.1155/2014/303805

Editorial

Pervasive Sensing Technologies and Emerging Trends

Jong Hyuk Park,[1] Han-Chieh Chao,[2] Sajid Hussain,[3] and Neil Y. Yen[4]

[1] *Seoul National University of Science and Technology, Seoul 139-743, Republic of Korea*
[2] *National Ilan University, Yilan 260-47, Taiwan*
[3] *Fisk University, Nashville, TN 37208, USA*
[4] *University of Aizu, Aizuwakamatsu, Fukushima 965-8580, Japan*

Correspondence should be addressed to Jong Hyuk Park; parkjonghyuk1@hotmail.com

Received 23 March 2014; Accepted 23 March 2014; Published 5 May 2014

Goal of pervasive computing is to prompt a thorough integration on information processing into everyday objects and activities of human beings. With recent advances and mature techniques in both software and hardware of sensor development, making a plethora of embedded platforms that equip well computation, communication, and sensing capabilities available has brought rich experiences to end users. The phenomenon indeed reveals dramatic changes on the way we live, we act, we think, and so forth which all directly are linked to our daily lives. That is, we have been, or thought to be, tightly integrated (and linked as well) with these amazing and small things around us. Taking the growing usage of smartphone, for instance, you may easily find that modern smartphones are equipped with a variety of sensors that can be applied to continuously monitor activities (e.g., behaviors), associated geographical information, services, and so on. In addition to those frequently-accessed devices, a rapidly-growing number of sensors (e.g., sensors on/in public facilities services or similar devices) around us also makes it possible to gain understanding of users in the real living world of human beings. As a summary of above-mentioned concerns in this promising area of study, the term "pervasive sensing" identifies, in essence, a promising momentum that incorporates different techniques, approaches, and thoughts in a hybrid realm of pervasive computing and ubiquitous sensing so as to overcome individual limitations and achieve synergistic effects.

This special issue received around many submissions from nine countries where the corresponding authors were majorly counted by the deadline for paper submission. All these submissions were considered significant in the area of pervasive sensing; but, however, only two-thirds of them passed the first-round examination which is based on a strict and rigorous review policy. After a two-round review process, sixteen papers were accepted for being included in this issue. These accepted papers mainly look at our issue from the perspectives of smart sensors, wireless sensor networking, sensor data management, data stream processing, RFID, embedded systems, distributed processing, artificial intelligence, agent theory, speech recognition, image and video analysis, signal processing, computational intelligence, machine learning, data and text mining, information retrieval, gesture recognition, biometrics, text-to-speech processing, software engineering, and their union, which lively brought discussions to the public.

"Intelligent supply chain integration and management based on cloud of things" by J. Yan et al. addresses the importance of the integration of intelligence for supply chain management and further provision of seamless services to end users in open and federated warehouses. Authors propose a new idea in the realm of cloud of things so as to develop flexible and agile approaches for facilitating the resource sharing and participant collaboration in lifecycles of supply chains. Convergence of intelligent supply chain condition perception, heterogeneous network access convergence, and resource servicisation are also demonstrated in a real-world system.

"Service-oriented node scheduling schemes with energy efficiency in wireless sensor networks" by H. Cheng et al. focuses on the essence of wireless sensor network, which looks at the issue of energy-efficient service provision via advantages of data sensing. The node scheduling problem is particularly

discussed for the construction of the service-oriented wireless sensor network. A new framework, named energy-aware centralized heuristic scheme (ECHS), where an energy-aware benefit algorithm is applied for the determination of active sensor nodes and rotate sensor nodes by periodically reconstructing the scheduling scheme, was first introduced. Following the similar consideration, an energy-aware distributed heuristic scheme (EDHS) which serves as the distributed version of ECHS was presented to provide preliminary solutions to the real-world problems.

"Investigating how user's activities in both virtual and physical world impact each other leveraging LBSN data" by Z. Yu et al. discusses the impact of user activities, such as their online behavior (e.g., social relationship) and offline activities, on other correlated users by leveraging the data widely collected from location-based social networks. The graph theory is applied to represent the nodes (e.g., participants) and attributes of nodes such as popularity entropy and correlated impacts. A series of algorithms are defined to formulize the applied graph and further discover this implicit information among the graphs. With the results, link prediction is conducted for the comparison with other similar works and brings about the experiences to the real-world social-based applications and services.

"Intrusion-tolerant Jini service architecture for integrating security and survivability support in DSN" by S.-K. Kim et al. discusses a challenging issue on reliability of connections applied in distributed sensor works for the provision of ubiquitous services. An intrusion-tolerant Jini service architecture was proposed to integrate security and survivability support and provide end users with associated services. This architecture is expected to protect developed services not only from ordinary faults on network partitioning or server crash but also from unexpected attached exploiting flaws. The performance reaches a significant growth compared with other similar works in the area and is considered better to support seamless service usage in the ubiquitous environment.

"A signature-based data security technique for energy-efficient data aggregation in wireless sensor networks" by M. Yoon et al. discusses the issue of data aggregation in wireless sensor network. A signature-based data security technique is proposed for protecting sensitive data aggregation. This technique adopts additive property of complex numbers, between targeted node and its neighborhood nodes, to support privacy-preserving data aggregation and integrity checking. A real-world performance evaluation of proposed technique outperforms the existing techniques up to 50% in terms of communication and computation overheads and significantly reduces the integrity checking and data propagation delay.

"Community vitality in dynamic temporal networks" by F. Cai et al. discusses an emerging issue on construction of temporal networks over existing community structure. Authors propose the concept of community vitality that shows a community's life intensity on a time slice. The lifecycle, from its birth, maturing, and death, of the community vitality is defined as a self-regular computational process. The expected use scenarios of the community vitality are also addressed to help users understand or model the community evolution.

"Developing a mobile learning system in augmented reality context" by D.-R. Chen et al. focuses on the sensing techniques towards well assistance of ubiquitous learning environment. Authors point out the use of augmented reality technology to create virtual objects for use in mobile devices to create a context-aware and AR-enabled guided tour application for ubiquitous learning with a fundamental goal on providing users with a friendly, highly-interactive interface and rich, engaging media to stimulate intrinsic motivation and performance.

"A study of smart power control algorithm using RF communication in smart home environment" by S.-H. Shin et al. gives a comprehensive glance on the existing power control algorithms for the development of smart home environment using sensor techniques, the performance comparison, use scenarios, and advantages of them. In addition, essential solutions that foster the improvement of these existing algorithms are provided. This study implements the smart power control system using standby power and RF communication, among smart home technologies through the use of a current booster, an AC/DC converter, and a DC/DC converter to operate electric lights.

"A smart service model based on ubiquitous sensor networks using vertical farm ontology" by S. Sivamani et al. then considers a promising application of agriculture using sensing techniques. This study initializes a conceptual framework named vertical farm ontology, and an OWL-based ontology model that supports the topology understanding is defined. This model can recompose the information widely collected from the Internet or sensors and share essential information with other connected (or federated) systems. The result, for the sake of agriculture, is expected to pave great path for the development of smart and intelligent agricultural services.

"A novel mechanism for fire detection in subway transportation systems based on wireless sensor networks" by Z.-J. Zhang et al. raises an interesting research issue in regard to fire, which is considered a common and disastrous phenomenon in transportation system, especially in a closed environment (e.g., subway system) with large passenger flow. This paper proposes a new algorithm that concentrates on the alternative of data fusion via existing wireless sensor networks. It utilizes the quantity information and distribution of collected data so as to make prediction of fire incidents.

"*Performance evaluation of page migration scheme for NVRAM-based wireless sensor nodes*" by Y. Ryu comes back to the energy issue and tends to solve the low-powered and multifunctional sensor node(s) in an open wireless sensor network. A buffer management scheme for hybrid main memory, which combines low-power nonvolatile RAM (NVRAM) and DRAM to reduce the energy consumption in a sensor node, is discussed. The proposed scheme employs the page migration technique in order to reduce the write operations on NVRAM part of hybrid main memory. The real-world experiment results outperform the legacy buffer management schemes in terms of the number of write operations on NVRAM.

"Human-robot interaction learning using demonstration-based learning and Q-learning in a pervasive sensing environment" by Y. Sung et al. then considers the machine learning-based human-computer interaction in a pervasive sensing environment. In essence, a novel interaction learning approach based on a virtual environment is defined in which the motor primitives are defined by manipulating a robot directly using demonstration-based learning. Through the proposed approach, a robot is expected to apply Q-learning to learn interactions with humans, and an enhanced performance is obtained compared with other similar works.

"Privacy protection based secure data transaction protocol for smart sensor meter in smart grid" by W. Go et al. goes into the issue of security and privacy for smart sensor meter in smart grid. Authors propose a privacy-enhanced secure data transaction protocol that can protect private data through real-time encryption that applies the user identity, home appliance serial number, and electricity consumption, so as to prevent attackers to obtain important data from the encrypted data. And also, unauthorized power companies cannot access this information either.

"An efficient cluster authentication scheme based on VANET environment in M2M application" by Y.-B. Jeon et al. discusses the authentication issue from the viewpoint of M2M application in VANET (vehicular ad hoc network) environment. Authors propose a cluster authentication scheme that mutually authenticates vehicles by composing vehicle movement as cluster configuration architecture. This scheme has successfully included the establishment of secure channels, the detection of replay attacks, mutual cluster authentication, and prevention of vehicle identity fabrication and secured distribution of provisional session key.

"Integrated validation system for the simulation of diverse sensors in WSNs" by H.-W. Kim and Y.-S. Jeong investigates the validation problem to a growing number of diverse sensors in wireless sensor networks. Authors propose diverse sensor definable simulators for the performance of experiments on diverse sensors with different communication distances in open wireless sensor network environments where geography markup language based coordinates are utilized. The primary goal is to provide flexibility to those existing simulators which are tailored to certain sensor characteristics.

"A sensor positioning scheme with high accuracy in nonuniform wireless sensor networks" by J. Park et al. then goes deeply to discuss the performance on accuracy in a nonuniform wireless sensor network environment. A novel sensor positioning scheme in nonuniform wireless sensor networks is first introduced and defined as a solution. As a result, it is applied to ensure the high accuracy of sensor positioning, and its superiority is demonstrated through a comprehensive comparison with the existing scheme such as DV-based position scheme.

The era of pervasive sensor network has begun, which promises to enhance the awareness of the cyber, physical, and social contexts and thus provide essential supports, in forms of services, applications, and so forth, to our daily lives. With the success in the organization of this special issue, it becomes possible for researchers (and interesting readers as well) who have been engaged in this emerging direction or related areas to receive state-of-the-art information, gain experiences, and further bring about the benefits in this promising area of study. We, the guest editors, also envision that the advanced stimulation of development of innovative services and solutions in pervasive sensing technology can be achieved in the coming future.

Jong Hyuk Park
Han-Chieh Chao
Sajid Hussain
Neil Y. Yen

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 754898, 14 pages
http://dx.doi.org/10.1155/2014/754898

Research Article

Design of an Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN) Using Cooperative Overlay Network

V. Akilandeswari and S. Mercy Shalinie

Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, Tamil Nadu 625010, India

Correspondence should be addressed to V. Akilandeswari; akilasenthil07@gmail.com

Received 8 October 2013; Revised 4 February 2014; Accepted 5 February 2014; Published 30 March 2014

Academic Editor: Neil Y. Yen

The main objective of this paper is to propose Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN) which includes self-management and self-defense in the network. The proposed network has the following considerations. (1) Dynamic coevolution is elucidated with interaction between independent rational strategies and structure of overlay network. (2) Evolutionary Game Theory (EGT) specific to overlay network is adopted with the combination of network reciprocity and group selection mechanism. (3) The cooperative efficient network structure is put forth by the multinode link-formation game. In this network, each node will be trained independently based on Naïve Bayes classification algorithm to react against any critical services in the network. The proposed network's significant characteristics are self-learning, independent training, collaborative detection, reaction to critical services, protecting the target machine before being collapsed, and maintaining the network performance without any hindrances. It controls the flow of high rate critical services such as Distributed Denial of Services (DDoS) flooding attacks and blocks the unwarranted services without any interruption to legitimate users. Hence, there is no doubt that this self-managed and self-defensive system will move from realm of fiction to real-time network engineering with high detection accuracy (98.3%), classification rate up to 99%, and improved clustering coefficient.

1. Introduction

A network is nothing but billions of tightly connected and distributed heterogeneous systems. The network systems are vulnerable to getting affected by some source of abnormalities, which results due to attacks launched by set of compromised computer systems, otherwise known as "zombies." A compromised computer system operates through a simultaneous interaction among large number of hosts which are distributed through the Internet [1]. Zombies normally throw an extremely high volume stream of packets towards the target machine. Various kinds of abnormalities will create some critical situations which will end up in a network node failure. Most of the critical network services consume the bandwidth resources of the network or the computing resources at the target system.

Providing security to all the internet communication machines against the network critical services is unrealistic and also remains as an unsolved problem. It is true to say that popular websites handle these critical network attacks by protection system with abundant resources. Even the protection systems will sometime fail when the attacks become highly intensified.

Dynamic defense mechanism helps to detect the network attacks and respond by dropping the excess traffic. The ideal defense mechanism detects the abnormality before reaction mechanisms realize that an attack must be detected before a response can be mounted [2]. This may be achieved even though when there are no common characteristics on attack traffic to detect the nature of attacks near the source [3]. At this juncture, the dynamic defense mechanism should make unsupervised changes in the compromised computing environment. Hence this type of defense mechanism will possibly stop the attack closest to the source. Moreover, this will not disturb the network resources and network

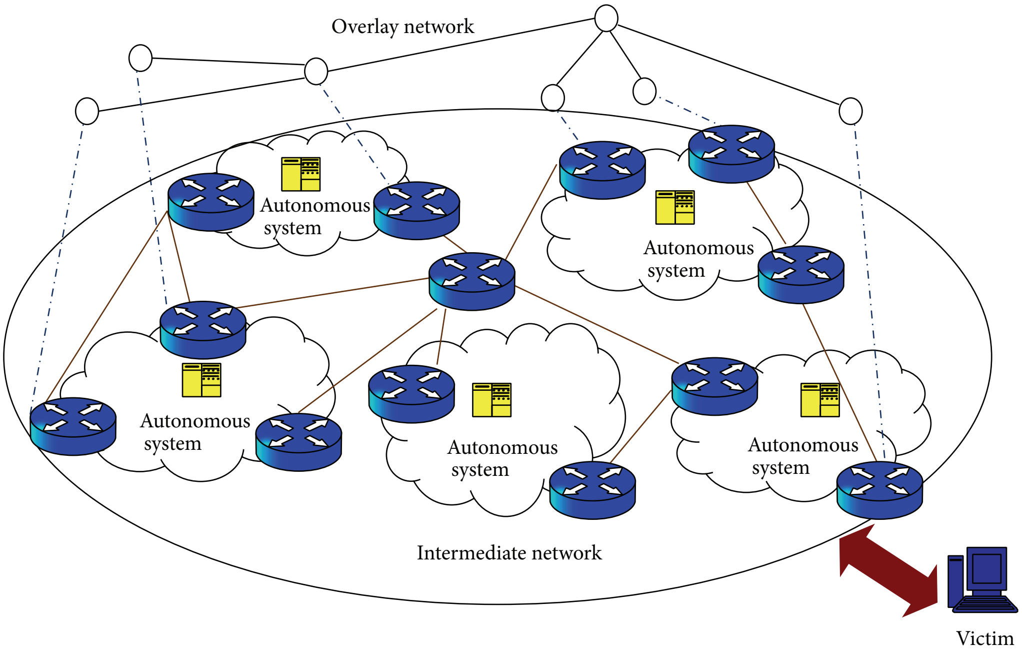


Figure 1: Basic structure of overlay network-virtual topology superstructure.

congestion in any way. A defense system is designed with the above-mentioned approach and with an objective to detect DDoS attacks at the intermediate level.

An overlay network is a virtual topology found (Figure 1) on the top of the current underlying infrastructure, which consists of autonomous systems and independent nodes [3]. The overlay network nodes are locally interactive and need the collaboration of its autonomous level system and numerous constituent parts of independent nodes for effective functioning. Most of the participating nodes contribute some of their resources; while some of the nodes show unwillingness to contribute their resources, the implications of the selfish behavior can be found in the overlay networks. In reality, many nodes show selfish behavior to maximize their own utility by exploiting the system without contributing among them [4].

The concept of having overlay network is an effective technique to support new application as well as protocols without any changes in the underlying network layer. This concept is helpful in finding Quality of Service (QoS) and multicast services in the light weight traffic differentiation schemes without any significant complexity. It also helps in providing virtual network infrastructure for each user and application.

The Internet is organized as an independent operating Autonomous System (AS). In this architecture, the detailed routing information is maintained only within a single AS and across its constituent networks [5, 6]. The AS can be independently administered and configured and that is why it is operated by some network service providers in other networks. However, using Border Gateway Protocol 4 (BGP-4), the information shared with other service providers and the AS can be heavily filtered and summarized by having border router connected to AS. This BGP hides many topological details due to its heavy cost [7].

The overlay topology can significantly impact the overlay routing in terms of routing performance and routing overhead. Mainly, physical topology information can benefit by constructing an efficient topology. The improved routing performance can be obtained within the overlay network by using the better topology construction. Several different overlay network services are available such as Resilient Overlay Network (RON) [8], Service Overlay Network (SON) [9], QoS-aware Routing for Overlay Networks (QROS) [10], and OverQoS [11]. Unfortunately, these overlay network nodes are selfish and strive to maximize their own utility by exploiting the system without contributing much for it [4]. The selfish behavior in overlay networks has important implications, that is, the nodes' unwillingness to contribute bandwidth or memory. Most of the aforementioned existing approaches are based on the growth rules that depend on the instantaneous and full topological properties of the network and devoid of the coevolution between the network structure and individual rational behaviors.

For this purpose, we design an Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN) using evolutionary algorithm. It tries to detect and react to the DDoS attacks at the intermediate level. This network focuses on effective information sharing by providing current incoming traffic attack messages, which is generated by detection algorithm through the overlay network. The algorithm helps in deriving the accuracy of classification and clustering coefficient. The Evolutionary Game Theory- (EGT-) based overlay topology provides high-level global network efficiency and widespread cooperation among the independent nodes. Further, it improves the accuracy of DDoS detection in the intermediate networks using the machine learning approach. In AD-CERN system, the resilient and scalable communication mechanism can be obtained to exchange the attack information within the large scale networks and by designing sharing gossip and warning messages the overhead information sharing can also be reduced.

The main objective of this paper is to design an overlay network with an Evolutionary Game Theory- (EGT-) based overlay topology evolution scheme and include this infrastructure into our proposed AD-CERN system with the following features:

(i) EGT-based overlay network brings the cooperation between individual nodes and prevents the nodes from indulging in selfish behavior;

(ii) using entire cooperative overlay network with increased network efficiency;

(iii) higher detection rate and improved classification accura-cy;

(iv) with the power of adaptivity, the network reacts to the attack at an early stage;

(v) protecting the network with machine learning-based training and learning;

(vi) finally, with improved performance potential, AD-CERN system should be deployed for self-management and self-defense.

The rest of this paper is organized as follows. Section 2 briefly reviews some essential notations, including evolution of cooperation, network reciprocity, group selection, and multinode link-formation game theory; Section 3 discusses design of EGT-based overlay topology and their evolutionary operation of individual nodes. Section 4 proposes Adaptive Distributed Critical-Care Extensive Response network (AD-CERN) with machine learning-based Naïve Bayes classification algorithm. Section 5 theoretically analyzes the EGT-based overlay network performances. Section 6 discusses the design of AD-CERN system, operation, and efficiency evaluation. Section 7 compares the evaluation results in the existing overlay network. Section 8 concludes this paper with self-defense and self-management nature of AD-CERN system and possible future extensions.

2. Preliminaries

The cooperation means selfish replicators which should forgo some of their reproductive potential to help one another [12]. Unfortunately, in reality, many existing overlay network nodes are selfish and maximizing their own utility. Generally, natural selection implies competition between nodes and therefore nodes oppose cooperation unless a specific mechanism is at work. Figure 2 shows the declining process of average fitness without involving the evolution of cooperation C and natural selection of defectors D.

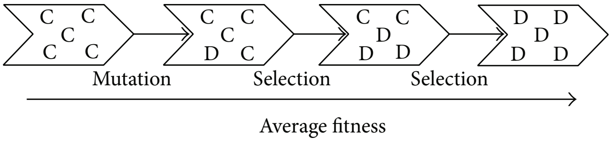


Figure 2: Declining process of average fitness.

A cooperator C is someone who pays cost $\hat{c}$ for another individual to receive a benefit b. A defector D has no cost and does not deal out the benefits. Cost $\hat{c}$ and benefits b are measured in terms of fitness as

$$\text{fitness} = \frac{(\text{Own contribution} + \text{Contribution of relatives})}{\text{Average contribution of the population}}. \tag{1}$$

In any mixed population, defectors d have a higher average fitness than the cooperators c. The natural selection process acts to increase the relative abundance of defectors which helps in establishing cooperation [12].

2.1. Evolution of Cooperation. Evolution is based on the brutal competition between the individuals and should therefore reward only selfish behavior [12]. In reality, every organism is designed to promote its own evolutionary success at the expense of its competitors. Biological and social science model behaviors are expressed in the form of evolutionary algorithms [13]. These entities are represented as interacting, mutable, and reproducing. These entities are also represented as a computational model. Such models are coevolutionary in nature, which means individual entities expose some kind of interaction with other evolving entities in the population [4]. Generally it includes three phases: interaction phase, reproduction phase, and mutation phase.

Interaction Phase. It specifies the rule of entities which interacts and gains some rewards.

Reproduction Phase. Each agent differently reproduces offspring based on its utility. It can be genetic or cultural reproduction.

Mutation Phase. In the reproduction stage, with a very small probability, the agents change their structure to incorporate innovation.

Cultural reproduction entities are seen as behaviors that can horizontally replicate between nodes within a generation. This interpretation is accommodated within the overlay network structure evolution. In [12], the author discusses the five mechanisms for the evolution of cooperation such as kin selection, direct reciprocity, indirect reciprocity, network reciprocity, and group selection. A simple rule is derived from each aforementioned mechanism which specifies whether natural selection can lead to cooperation or not. The network reciprocity and group selection mechanisms are found to be perfect for constructed EGT-based overlay topology with an adaptive distributive nature.

In network reciprocity, the natural selection of defection is based on a well-mixed population, where everybody interacts equally with each other. Figure 3 includes the

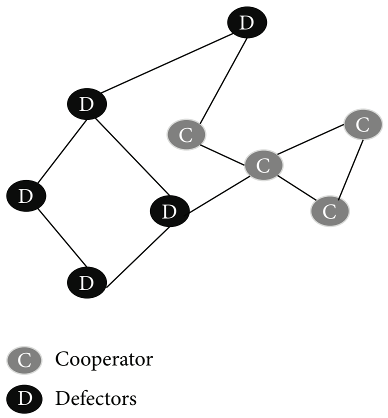


Figure 3: Process of network reciprocity.

mechanisms of network reciprocity which means the cluster of cooperators outcompete defectors [4, 12].

The real world interactions are often restricted to small local groups, because real populations are not mixed. Spatial structures or social networks imply that some individuals interact more often than others. Evolutionary Graph Theory allows us to study how a spatial structure affects evolutionary and ecological dynamics [14].

The network reciprocity equally interacts with every node in the overlay network. Individuals occupy the vertices of the graph and the edges denote who interact with whom. The graph is fixed for the duration of evolutionary dynamics [15, 16]. This evolutionary dynamics on graphs can favor operation over defection if the benefit-to-cost ratio b/c of the altruistic act that exceeds the average number of neighbors, K, per individual is

$$\frac{b}{c} > K. \tag{2}$$

This result is given as the generalization of "spatial reciprocity."

In the overlay network construction, nodes' interaction is constrained to its neighbors instead of fixed network of some duration. In coevolutionary model, links are removed based on the members of the population with respect to time [17].

The main objective of group selection is to form a close relationship with the individual group nodes and to find out more suitable groups of nodes. Group selection refers to the process of natural selection which favors the characteristics in individuals and increases the fitness of the group individuals [12]. Figure 4 shows the idea of group selection competitions, which is not only between individuals but also between the groups.

Group selection splits up the population into groups, which determines the interaction scope of the agents. Individually reproduced proportional payoff and its offspring are added to the same group. If the group reaches certain size, it can split up into two with a certain probability.

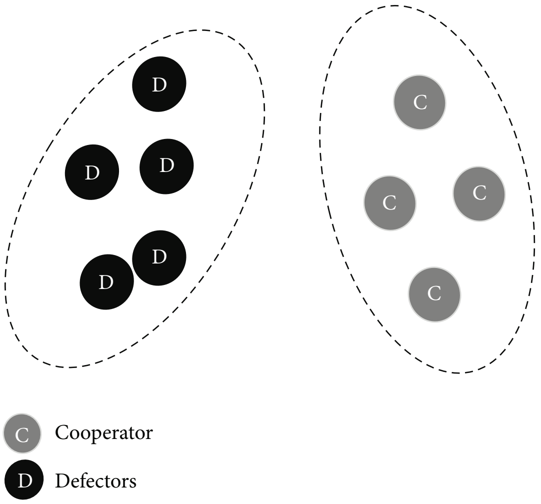


Figure 4: Process of group selection between cooperator and defectors.

The perfect cooperator groups grow faster than pure defector groups, whereas, in any mixed group, defectors reproduce faster than the cooperators. Therefore, the selection on the lower level (within group) favors defectors, as the selection on higher level (between groups) favors cooperators. Hence, under some conditions, well-performing groups can survive and the agents of groups providing poor conditions will be eliminated automatically [18].

The authors consider that if n is the maximum number of group sizes and m is the number of groups, then group selection allows for the evolution of cooperation, provided that

$$\left(\frac{b}{c}\right) > 1 + \frac{n}{m}. \tag{3}$$

Group selection is a fully decentralized mechanism that focuses on the dynamic view of groups and iteratively guides its evolution towards more optimal configurations.

The node's neighbor views the group and the reproduction phase. It is imitated to join the filter group attacks. Furthermore, explicit investigation on evolution of the adaptive distributed overlay network structure based on the node's local interaction is carried out.

2.2. Multinode Link-Formation Game. Multinode link-formation game [4] is an overlay network which characterizes self-interested nodes to form links in the overlay network. Each node keeps one link to a cooperative neighbor node in its neighborhood node which can slightly speed up the convergence cooperation and increases the network efficiency. Individual nodes are capable of making rational choices to establish new links or to give up existing links. Social dilemma of forming links in an overlay network says the aggregation of payoffs by mutual cooperation nodes and the aggregated payoff is always better than higher payoffs given by deflection node [12]. Cooperative overlay network evolution is analyzed by coupling the network formation rules with dynamic states of the elements in the system. Dynamic evolution of the network can be evolved similar to biological method, using the design of multinode link-formation game with their neighbor nodes, and each node preferentially links to the more suitable node with higher utility and joins the group selection to form the similar neighborhood.

Here, we combine the network reciprocity, group selection, and multinode link-formation game to evolve the arbitrary EGT-based overlay topology for achievement of "Adaptive Distributed Critical-Care Extensive Response Network" (AD-CERN).

3. Construction of EGT-Based Overlay Network

In this section, the effect of cooperation and rational behaviors on the overlay network nodes is theoretically analyzed. For the evolution process, the evolutionary mechanisms [4] are adopted for the construction of EGT-based overlay network topology such as network reciprocity [12], group selection [12], and multinode link-formation game [4]; these are described in Section 2.

3.1. Cooperation among Overlay Network. Cooperation is needed to obtain the dynamic coevolution between independent nodes on the overlay networks. The overlay network operates based on the principle of cooperation and it has an ability to run an application in particular node. A cooperator C is someone who pays a cost $\widehat{c}$ for another individual to receive a benefit b. The cooperator behavior brings cooperator cost $\widehat{c}$ and brings its partner the benefit, that is, 1. The defect node D faces no cost because it will not use a resource to provide any service for its partner. In general, most of the aforementioned existing overlay network nodes are based on growth properties and it neglects the coevolution between the network structure and individual rational behaviors [3, 19, 20].

3.2. Rational Behavior of Overlay Network Nodes. According to the general concept of EGT, individual nodes will imitate the behavior of other nodes that has the higher utility. Including the same, the node can randomly discover the other nodes from the entire overlay network and compare the utility with them.

Moreover, nodes can change its strategy and drop/make links to other nodes based on the comparison of utility. Mainly, we consider this rational behavior to deal with the selfish behavior in overlay network topology formation using the fact "Tragedy of Commons" [21]. It aims to produce a simple generalized topology evolution scheme that is scaled well and functions under a reasonable selfish assumption.

3.3. Evolutionary Mechanism. The evolutionary mechanism decorates the overlay network as convergence of autonomous and rational nodes into a cooperative network structure. Network reciprocity forces an overlay network as cooperative by means of simple interaction among autonomous and rational nodes.

First, the overlay network is constructed with the following structure. Let us consider the population of N nodes consisting of cooperative C and defect D nodes; initially all nodes randomly form connections as in Figure 5, and all nodes adopt the "defect" D strategy except the nodes having the "cooperative" C strategy. A cooperative node helps all neighbors to bring cooperator to some cost, which is forwarding packets or answering queries for its neighbors or sharing information to all neighbors [4, 22]. Any two nodes can make a connection without loss of generality; the cooperative C node brings cooperator cost $\widehat{c}$ and gives its partner the benefit b, that is, 1. The defect node D faces no cost, because it will not use any resource to provide any service for its partner.

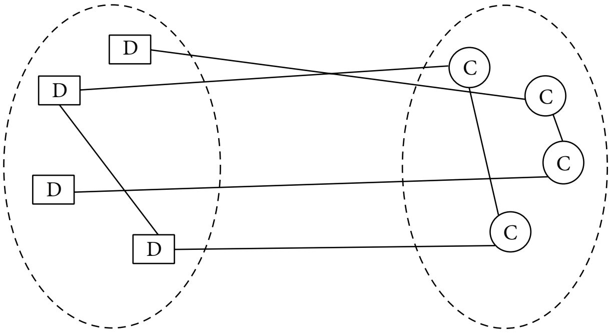


Figure 5: Overlay network nodes with random connection.

Table 1: Payoff matrix.

	Payoff matrix Cooperator C	Defector D
Network reciprocity		
C	$(b - c)$	$(H - c)$
D	$(b - H)$	0
Group selection		
C	$(b - c)(m + n)$	$(b - c)(m - cn)$
D	$(b - n)$	0

Table 2: Node i and j's payoff in link-formation game.

	Pay off Cooperator C	Defector D
Link formation		
C	$(1 - \widehat{c})(1 - \widehat{c})$	$(-\widehat{c}, 1)$
D	$(1 - \widehat{c})$	$(0, 0)$

$\widehat{c}$ is decided by specific scenarios and varied according to different nodes. Here the maximum cost nodes are assigned to $\widehat{c}$ as $\widehat{C}$ = maximum cost of nodes.

Thus, at each step, neighboring node calculates payoffs from Table 1 according to their strategies, that is, cooperative C and defect D, where $H = [(b - c)k - 2c]/[(k + 1)(k - 2)]$ and K is the number of neighbors.

Each matrix is helped to derive the necessary conditions for evolution of cooperation. It simply specifies the interaction between cooperators C and defectors D. The payoffs elements are summarized in Table 2, which are derived between neighbor node i and node j ($\widehat{c}$ is constant).

In Figure 5, the connection between network nodes is fixed. Here the main issue is how to construct an overlay network with minimized average neighbor distance. Initial stages of randomly selecting neighbors may result in more links between far away host and fewer links between nearby hosts. The resulting average neighbor distance would be relatively long. It degrades the network efficiency [7, 23]. The simple multinode link-formation game is used to capture the intrinsic problem of link creation among the overlay network nodes. It is very much different from Bilateral Connection Game (BCG) [24, 25]. The multinode link-formation game is proposed to characterize the topology formed by selfish nodes, in which each node attempts to minimize nodes and minimize costs by minimizing the number of connections. In addition, each node establishes a sum of the costs of reaching all other nodes. Multinode link-formation game shows that is very difficult for each node to utilize local information based on global network topology. The partial view of overlay structure and the local interaction with the neighbors are combined to obtain its utility.

This link-formation game concept is more feasible for large scale and dynamic p2p network nodes to obtain overlay approach.

Here, nodes locally interact with a small subset of partners defined by current network topology. Every step of interaction, individual node, and its neighbors invoke their strategies to get the utility using Tables 1 and 2. This iterative interaction calculates an individual's payoff which is sum of the payoffs obtained across the bilateral game [4]. Thus, it is named as multinode link-formation game. An individual node's utility is determined by the following factors:

(1) degree of the node;

(2) strategies of the neighbor nodes.

The multinode link-formation game implies the following factors.

If node i is cooperative, then node i's utility $u_i(G)$ in the formed overlay network graph G can be denoted as follows:

$$U_i(G) = (1-\delta)\, n_i^c(G) - \delta n_i^{nc} = n_i^c(G) - \delta n_i(G). \quad (4)$$

If node i is noncooperative, then its utility is

$$U_i(G) = n_i^c(G), \quad (5)$$

where $n_i(G)$, $n_i^c(G)$, and $n_i^{nc}(G)$ represent the number of node i's total neighbors, node i's cooperative neighbors, and node i's noncooperative neighbors in the formed overlay network structure G, respectively.

In the evolutionary phase, the multinode link-formation game designated defect node's utility is 1, and this node is compared with the cooperative node. It is illustrated in Figure 6. If the cooperative node's C utility $(2-2\delta)$ exceeds 1, then the designated defect node D will copy the designated cooperative node's C strategy and the resulting link structure will add an extra link to the right side node [4].

Figure 7 shows the formation of the nodes connectivity in the overlay network which evolves from the above multinode link-formation game. The dotted lines represent the added links in the evolutionary phase. Thus, the structure characterizes the social dilemma of forming links in an overlay network, and it incorporates individual rational decisions. In addition, individual node preferentially links to the more suitable nodes with higher utility and forms the group.

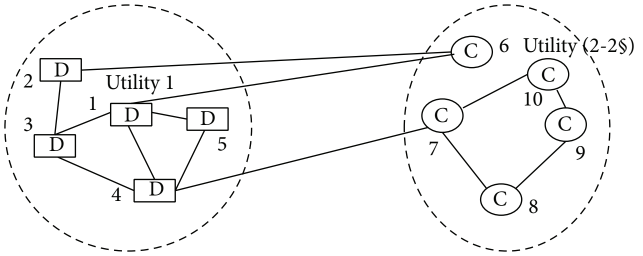
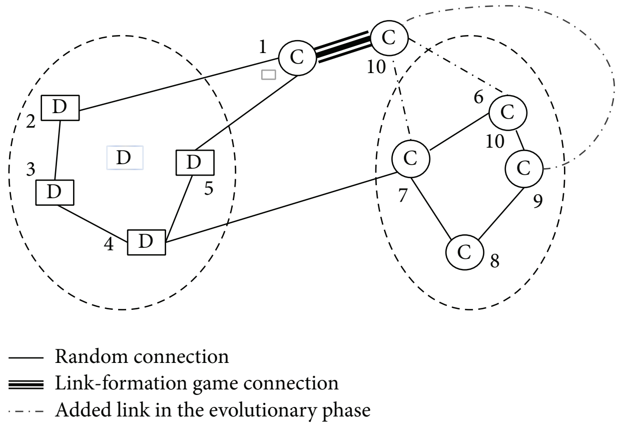


Figure 6: Overlay network node's evolution phase: defector and cooperator strategies.



1
C
C
10
6
C
D
2
10
D
D
C
C
3
5
D
7
9
4
D
C
8
Random connection
Link-formation game connection
Added link in the evolutionary phase

Figure 7: Illustration of evolution phase in the multinode-link formation game.

Normally, a group consists of a set of nodes that are close to each other. For any positions, P, in the physical network, if the distance between P and node i and the distance between P and node j are the same, then they are likely to form a group. Assume that nodes i and j are in the same group. Here, the distance between two nodes can be network latency, or round trip time, or minimum bandwidth on the links along a path between the two nodes, or some user-defined cost functions between the two nodes. A group can exchange messages with several other groups, which are referred to as neighbor groups. The neighbor groups in this overlay are the groups that are nearby the underlying physical network.

3.4. Operation of Evolutionary Game Theory- (EGT-) Based Overlay Topology. Figure 8 shows the operation of individual EGT-based overlay network node. In this scheme, nodes are randomly bootstrapped into an arbitrary network structure. In the beginning, 10% of the nodes are cooperative in nature; then the three phases of evolutionary algorithm such as interaction phase, evolution phase, and mutation phase are included for entire cooperative overlay network.

In the interaction phase, initially, each node and its neighbors are connected by the current network structure with their strategies and get payoffs as per Tables 1 and 2.

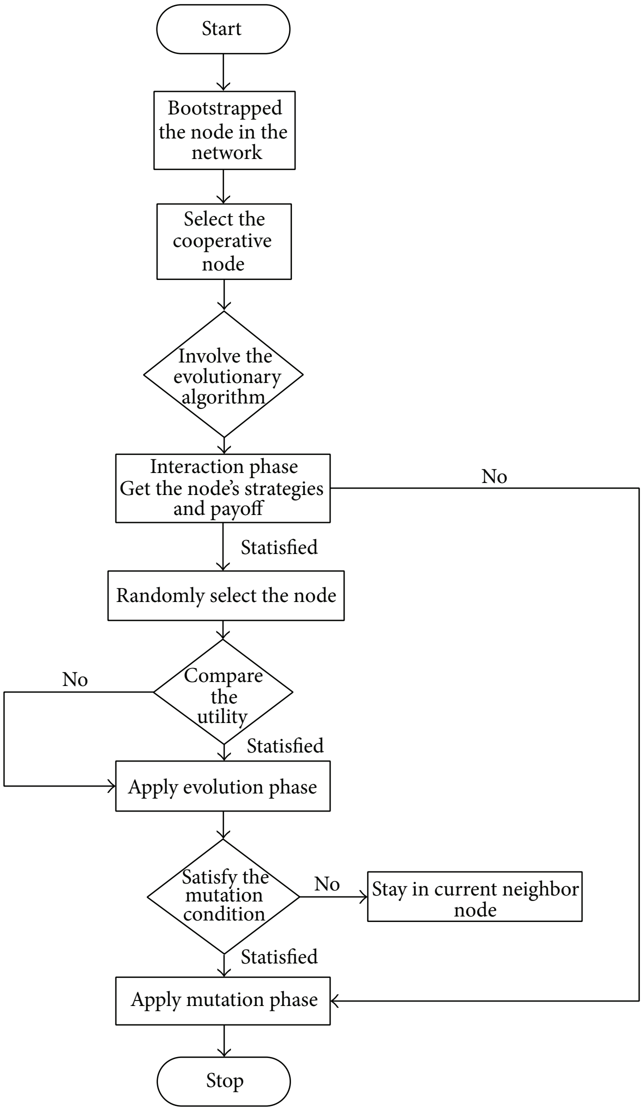

Start
Bootstrapped the node in the network
Select the cooperative node
Involve the evolutionary algorithm
Interaction phase Get the node's strategies and payoff
No
Statisfied
Randomly select the node
No
Compare the utility
Statisfied
Apply evolution phase
Satisfy the mutation condition
No
Stay in current neighbor node
Statisfied
Apply mutation phase
Stop

Figure 8: Operation of individual Evolutionary Game Theory-(EGT-) based overlay network node.

Secondly, by applying the evolution phase according to their satisfactory condition, the node is reallocated to a new neighborhood view. It happens when the node i is failed to find a suitable node in the overlay network and then the node i skips the operation in this round and directly goes to the mutation phase as in step 9 of Figure 8. In addition, each node drops its neighborhood view and randomly selects nodes to form a group. In mutation phase, the creation of a brand new group, that is, node i which discards its current group and randomly selects a node to form a link. As a result, the other nodes migrate to the seed group in the future and increase the group size. Hence, the introduction of mutation in cooperative and defect strategies is unnecessary for the emergence of cooperative/coordination.

The interpretation of cultural reproduction is accommodated in the overlay network structure. In our proposed technique, reproduction phase will help to produce a counterpart of the existing overlay network by either rewiring the nodes or changing the topology of the network. It is a simple logical process in which nodes drop, copy, or exchange symbolic links [4, 12].

Here multinode link-formation game can be done as pairwise, which means two nodes should provide mutual consent in the formation of a link connection [4]. Hence intuitively, each node will form a link with another node. The former node should persuade the latter to accept this connection. Therefore, based on the simple economic strategy in the node's evolutionary phase, the node will keep the link to one cooperative node in its original neighborhood view as shown in Figure 7. On the whole, this process will facilitate the evolution of an overlay network structure.

4. Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN)

Machine learning and data mining theories provide the relevance of self-management and self-defense to the networks and its distributed systems. For the proposed AD-CERN, EGT based on efficient overlay network has been used and the details of which are mentioned in the Section 3. Nodes in this EGT-based overlay network will be inducted with detection and classification capabilities. They cooperatively detect and react to critical behaviors before specific response mounts in the target machine or network performance degradation. The machine learning induction provides the power of adaptivity in particular application techniques [26].

This AD-CERN node includes detection, classification, information sharing, network learning, and training phase as in Figure 9.

4.1. Detection Algorithm. In this phase, each node is equipped to detect whether current incoming network traffic represents the normal or critical situation in the system. Here, the "IP address-based high rate flooding attack detection" algorithm [1] is included to detect the traffic behavior changes in the specific traffic measures and send gossip to the classification phase. Inclusion of multiple detection algorithms in every node helps to achieve higher detection rate.

4.2. Classification Algorithm. This phase has high sensitivity than all other ones and also called as detection-and-reaction phase. When the gossip message arrives, the accumulated mean for its destination is renewed and a gossip is added for that destination. Then each node gathers self-gossip and neighbor-gossip as shown in Figure 9. After this, classifier node will evaluate message attributes like <source, warning, destination, gossip>.

It uses the statistical or machine learning classifiers to produce predictions about the incoming traffic. It distinguishes the critical traffic patterns from normal traffic patterns. The well-known Naïve Bayes method [27] is used to integrate and share local traffic information with neighbors. Here network reciprocity is adopted for equal interaction among the nodes.

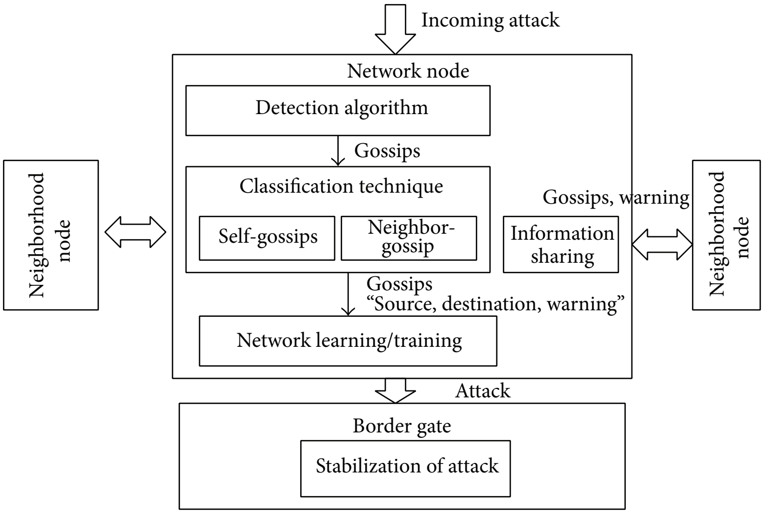


Figure 9: Block diagram of individual proposed network nodes operation.

4.3. Information Sharing. The information sharing improves the classification with the two kinds of messages. These messages are shared between nodes to update the maximum global knowledge about traffic. In the first step, gossips help to indicate suspicion of flooding attack. It is sent and received to/from the neighbors in any direction of the overlay network. In the second step, warning, it is another message which helps to indicate high certainty of an ongoing attack. It is sent only in the direction of attackers, in order to strangle attacks as close as possible to the source.

4.4. Network Learning and Training. Generally, overlay network nodes have different characteristics depending on the context and the network situation. Here the classifier accuracy itself seems to be a problem; hence it can be resolved by adjusting the classifiers according to their detection algorithm, maintenance level of trust to a concrete gossip, and checking the amount or type of usual traffic which passes through the node.

Thus, the network nodes are equipped with a learner/classifier. With the machine learning technique each node's ability should be trained to adapt their thresholds of gossips trusting and detection mechanisms for each target node. Now a perfect training is given to the node which is similar to its situations denoting it as critical.

In the Naïve Bayes method, different message attributes are supposed to be statistically independent. The description of this method uses the two numbers a and b, and they are denoted as a destination warning, gossip, respectively,

$$\begin{aligned} a < b &= \{1 \text{ if } a > b\}, \\ a < b &= \{0 \text{ if } a < b\}. \end{aligned} \tag{6}$$

Given a traffic T, regarded a tuple <source, warning, destination, gossip>, the Naïve Bayes method estimates of $P(\text{Attack} \mid T)$ and $P(\text{Non\_Attack} \mid T)$ and simply predicts "Critical" status when $P(\text{Attack} \mid T) \lesseqgtr P(\text{Non\_Attack} \mid T)$ and, otherwise, it says "Normal" status [27]. These two probabilities are computed using Bayes theorem; that is,

$$P(\text{Attack} \mid T) = \frac{P(T \mid \text{Attack}) \cdot P(\text{Attack})}{P(T)}. \tag{7}$$

The observed $P(T)$ can be disregarded because it only cares with the ratio of $P(\text{Attack} \mid T)$ and $P(\text{Non\_Attack} \mid T) \cdot P(\text{Non\_Attack} \mid T)$ and $P(\text{Non\_Attack} \mid T)$ can be estimated from training data, locally to each node.

To estimate $P(T \mid \text{Attack})$, use the independence assumption, as follows: $= P(\text{source, warnng} \mid \text{Attack}) \cdot P(\text{destination, gossip} \mid \text{Attack})$. Again, these two probabilities can be estimated from the empirical distribution of messages in the training data as follows:

$$\begin{aligned} P(\text{source, warning} \mid \text{Attack}) &= \frac{P(\text{source, warning, attack})}{P(\text{Attack})}, \\ P(\text{Destination, Gossip} \mid \text{Attack}) & \\ &= \frac{P(\text{Destinaon, Gossip, Attack})}{P(\text{Attack})}, \end{aligned} \tag{8}$$

where $P(\text{Attack})$ is the attack ratio at this node.

We train the network node by enabling the gossips and at the same time warnings must be disabled. In total, the Naive Bayes machine was found to be learned the following things which (1) increases the "Critical" status warning probability and decreases the "Normal" status warning probability; (2) the probabilities remain stable until a relative high number of gossips get decrease, where the "Critical" status probability increases, and "Normal" status warning probability becomes zero. It means that the False Positive Rate (FPR) and True Positive Rate (TPR) rate are rich and False Negative Rate (FNR) is zero in every node of AD-CERN system.

If the critical services appearance is suspected, this status will help to determine whether a message to a particular node should be forwarded or blocked. The entire cooperative

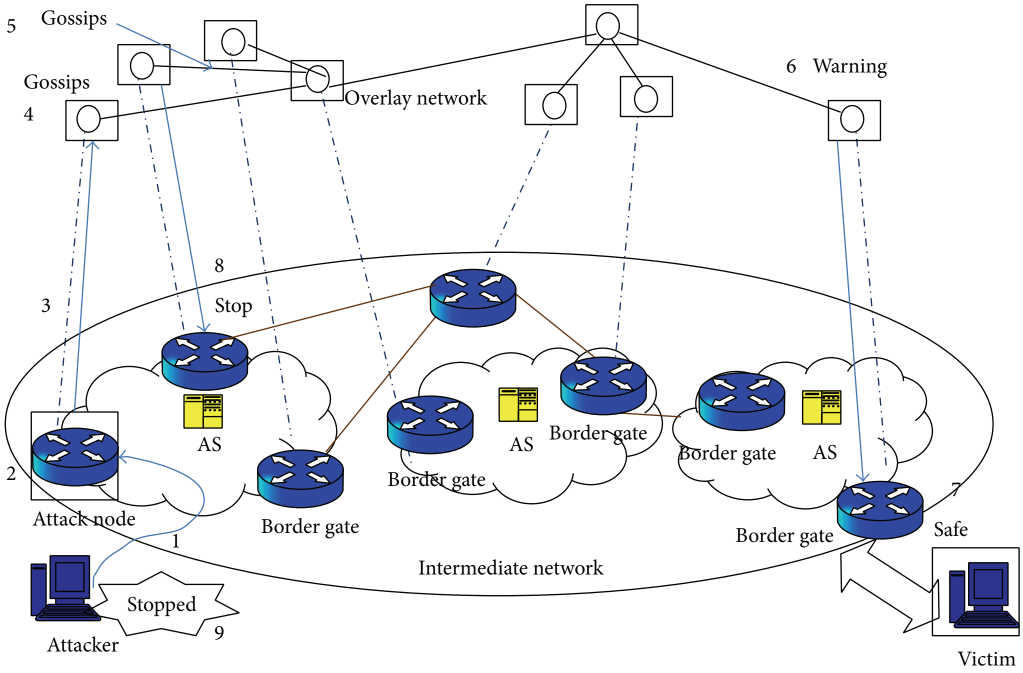


Figure 10: Overall operation of Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN) during critical services.

network drives overlay network nodes to learn about the behavior of its portion of network by adjusting its classifier to its own location in the network traffic. As in Figure 10, overlay network nodes can exchange gossiping and warnings about the declared critical attack service. When the warning arrives to the border-gate nodes, it curtails the attacks whichever is very close to the source, while the gossips keep all the border-gate nodes. Every node in an overlay network is nothing but a key node and the nodes which receive the more request than the other are only facing enormous attacks. Hence, in the overlay network, the node should maintain the detection mechanism even during the abnormal situation and further it should exchange and aggregate the information about traffic condition in all different parts of the network system. In order to restrict the attack strike to the network borders, a backward warning system is included to the source which is as close as possible. By implementing this method, our network elements will learn to determine whether the situation is normal or critical. Even though the attacks are found very close to the border gate of the network; it can be curtailed before reaching the victim.

After this operation, EGT-based overlay network is able to stop and avoid distributed critical services, like high rate flooding, abuse, or failures. Each node shares with its neighbor's node the status of the network and aggregates its local information using the nature of evolution of cooperation. It includes every node into the convergence of cooperation and increases network efficiency. As a result of the above discussed facts, the present AD-CERN system comes into existence. Now the AD-CERN will work in self-optimizing, self-organizing, self-healing, and self-defending methodology, in order to protect networks against critical network service attacks and network node failures. Here, each node is allowed to make unsupervised changes in the computing environment. This permission will definitely increase the ability of AD-CERN system, particularly, while independent learning during any critical situation. Hence, this network is named as an "Adaptive Distributed Critical-Care Extensive Response Network" (AD-CERN).

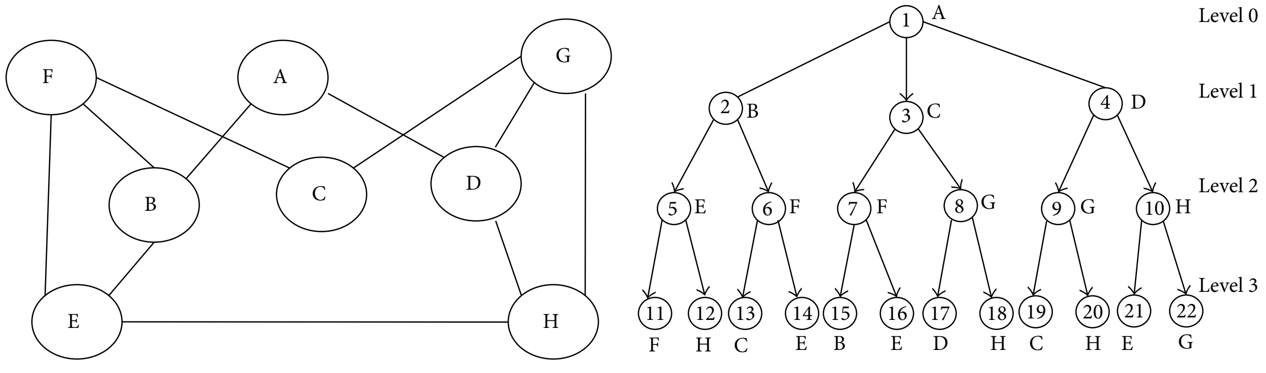
4.5. Performance Analysis of Evolutionary Game Theory-(EGT-) Based Overlay Network. In this section, the proposed EGT-based overlay network is considered as a connected graph as in Figure 11(a), where each node in the graph represents a group in the overlay network and neighbor relationship between two groups is represented by edges between two nodes in the overlay. In Figure 11(b), the overlay network nodes are arranged in the tree structure [7]. The root of the tree is node A as in level 0.

Node A's direct neighbors, $B, C,$ and D, are one hop away and are placed below node A (at level 1). Here, the node A is the parent of nodes B, C, D and nodes C and D, are children of node A. Then, each node adds its neighbor into the tree. This process is repeated until all nodes are included in the tree structure.

The proposed overlay network's performance is analyzed with average neighbor distance $N(E)$, network efficiency $E(G)$, and average clustering coefficient $C(G)$.

4.5.1. Average Neighbor Distance (AND). The AND [7] of our proposed EGT-based overlay network is theoretically calculated using the formula:

$$\overline{D} = \frac{D_i\left(\left(N \cdot n \cdot m\right)/2\right) + D_b\left(\left(N \cdot M\right)/2\right)}{\left(\left(N \cdot n \cdot m\right)/2\right) + \left(\left(N \cdot M\right)/2\right)} = \frac{D_i \cdot n \cdot m + D_b \cdot M}{n \cdot m + M}. \tag{9}$$



(a)

(b)

Figure 11: (a) Neighbor relationship of Evolutionary Game Theory- (EGT-) based overlay network. (b) The tree structure of Evolutionary Game Theory- (EGT-) based overlay network.

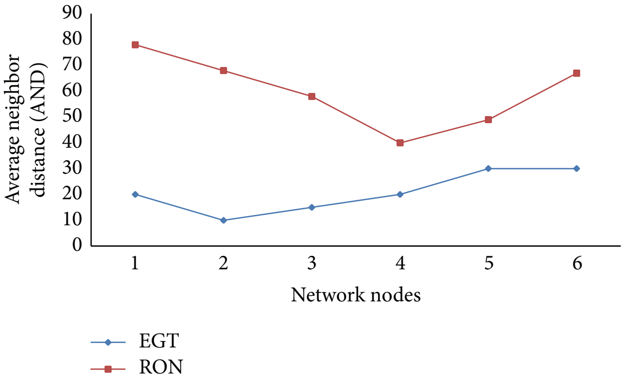


Figure 12: Average neighbor distance between Evolutionary Game Theory- (EGT-) based overlay network and Randomly Connected Overlay Network (RON).

The EGT-based overlay network contains the N groups and each group consists of n hosts. Every group has M neighbor, in which each host has m neighbor hosts. The average distance between neighbor groups is denoted as D_b and the average distance between two hosts in the same group is denoted as D_i. The total number of intragroup neighborhood links is $n \cdot (m/2)$. The total number of intergroup neighborhood links is $N \cdot (M/2)$.

The proposed EGT-based overlay network will prove the shorter average neighbor distance as in Figure 12 and this will be comparable with Randomly Connected Overlay (RCO) Network.

This could be attained with the concept of group selection mechanism as discussed in Section 2 which allows for the evolution of cooperation. It focuses on the dynamic view of group selection and iteratively guides its evolution towards more optical configuration. Moreover, it decreases the D_b with the shortened neighbor links between different groups. It increases them with more neighbors in the same group. Finally, it helps to place the hosts to their proper group and further increases the D_i so that $(D_i \approx D_i')$.

4.5.2. Network Efficiency E(G). The measurement of network efficiency [7] E shows how efficiently the network exchanges the information between the nodes. The efficiency $\varepsilon(G, j, K)$ in the communication between the two points j and K is defined as the inverse of the shortest path length $d(G, j, K)$, and the efficiency of G is the average of $\varepsilon(G, j, K)$; that is,

$$\begin{aligned} E(G) &= \frac{1}{N(N-1)} \sum_{j \neq k \in G} \varepsilon(G, j, k) \\ &= \frac{1}{N(N-1)} \sum j. \end{aligned} \tag{10}$$

In the Randomly Connected Overlay Network, that is, the nonconnected graphs, there is no path between the two points j and K, $\varepsilon(G, j, K) = 0$, and $d(G, j, K) = +\infty$. For that reason, EGT adopts the network reciprocity for equal interaction with every node N in the overlay network.

4.5.3. Average Clustering Coefficient C(G). The calculation of clustering coefficient [4] $C(G)$ of node i is defined as

$$\begin{aligned} C_i &= \frac{\text{Number of edges in } G_i}{\text{Maximum possible number of edges in } G_i} \\ &= \frac{\text{Number of edges in } G_i}{K_i(K_{i-1})/2}, \end{aligned} \tag{11}$$

where G_i is the subgraph of neighbors of i and K_i is the number of neighbors of node i.

5. Simulations

5.1. Network Topology. In this work, two topology models are used in the simulation. The first overlay network is constructed randomly, and nearby hosts in the overlay network may actually be far away in the underlying network (Figure 1).

In another network topology, network is equipped with the intermediate network nodes and border-gate nodes with the detection mechanisms and classification technique. The nodes can exchange gossiping and warnings about the

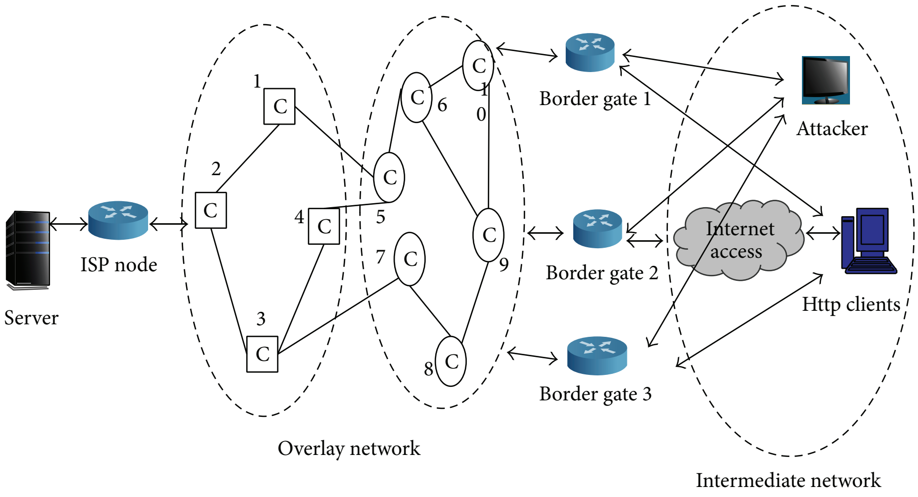


Figure 13: Adaptive Distributed Critical-Care Extensive Response Network (AD-CERN).

Table 3: TCP SYN and UDP flooding attacks at border-gate nodes.

Attack profile	SYN flooding	UDP flooding
Period 1	95%	78%
Period 2	87%	76%
Period 3	85%	78%

declared critical attacks. The main aspect is that all routing nodes from the network should be passed only through the overlay networks. But this may be unfeasible in practice. Hence, considering this difficultly the cooperative overlay network is constructed as in Figure 13.

5.2. DataSet. Using our proposed network topology as in Figure 13, HTTP server collects the normal and attack traffic. Normal traffic is generated between the victim and nodes in the intermediate network. For the attack traffic, Stacheldraht [28] is used to generate distributed denial-of-service attack traffic. During this attack period all nodes receive the generated attack traffic.

The Stacheldraht is selected because it is a more matured attacking tool compared to other attacking tools, such as TFN, TFN2k, or Trinoo. The Stacheldraht is composed of handler (master) and agent (daemon) programs [29]. The handler system scans vulnerabilities of the victim before ending an attack command to the corresponding multiple agent systems. Agent systems produce a large flood of packets targeting the victim. It interrupts the system resources and network resources. For the evaluation of network, two types of flooding attacks are collected for some periods: TCP-SYN flooding and UDP flooding. Attack traffic profiles are gathered during attack period. The parameters are depicted in Table 3. Figure 14 shows a typical traffic behavior in border-gate nodes.

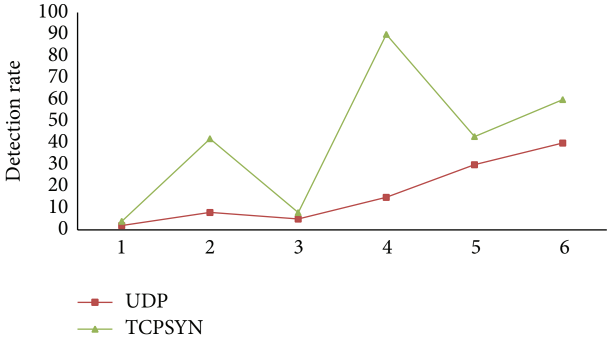


Figure 14: TCP SYN, UDP attack traffic behavior at the border-gate network nodes.

6. Network Evaluation

6.1. Randomly Connected Overlay Network (RON). The individual nodes are equipped with detection algorithm and placed in the egress routers of an autonomous system, which collect meaningful information and locally detect Distributed Denial of Service (DDoS) attacks. The system shares the attack information using gossip protocol within the next-step-node only. Detection algorithm will detect any local attacks and the local decision will be sent to the cooperative detection engine [3, 19]. It combines these local decisions from the neighboring nodes. Finally the detection decision will take appropriate action to defend the attack. In Figure 15, the TCP SYN attacks and UDP attack have moderate detection rate as 65% and 45%, respectively, and also depend on the local detection algorithm.

6.2. Evolutionary Game Theory- (EGT-) Based Overlay Network. This network will run in the normal status until a critical service appears, like DDoS flooding attacks. It attacks the path to the service and also interferes with normal

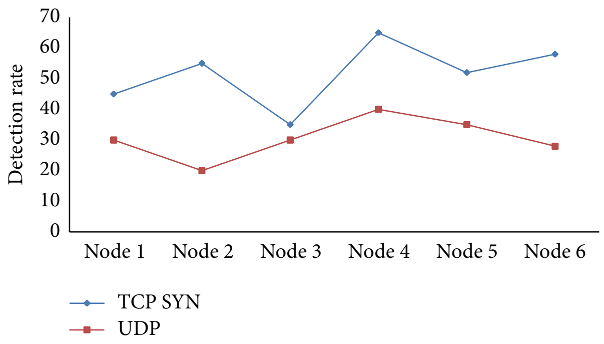


Figure 15: Attack detection rate in Randomly Connected Overlay Network (RON).

Table 4: Classification accuracy of Naïve Bayes algorithm.

Attack profile	SYN flooding	UDP flooding	Classification accuracy
Period 1	99%	98%	98.3%
Period 2	98%	98%	98.0%
Period 3	99%	100%	99.3%

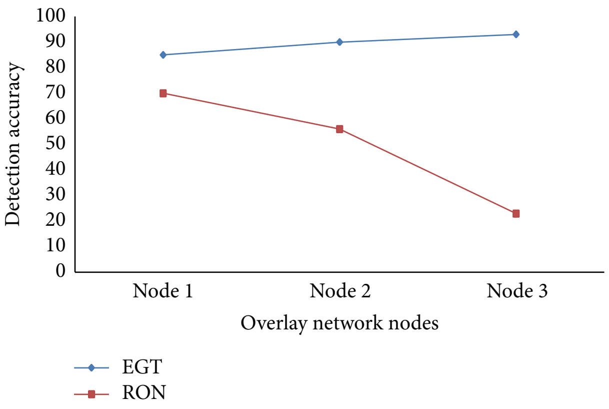


Figure 16: Performance analysis of attack detection between Evolutionary Game Theory- (EGT-) based overlay network nodes and Randomly Connected Overlay Network (RON) nodes.

connections. The detector ingests every incoming traffic T to the victim in an abnormal way. A gossip will spread among the neighbors to indicate the victim which is in attack. The network reciprocity mechanism helps the overlay nodes to interact equally with every node in the overlay network. In connection to this, all the neighbors will receive the gossip. The gossip message contains the possible victim ID and the confirmation. At this time, classifier determines that the victim is under attack, and immediately a warning is sent to the node from where the message is received and sent to every node. Each node uses the aggregated gossips and warnings to provide high confidence of classification accuracy. For the performance evaluation, the classification accuracy [19] is calculated using

$$\text{Classification Accuracy} = \frac{\sum_{i=1}^{n} T_i}{\sum_{i=1}^{n} I_i}, \tag{12}$$

where I is an individual attack traffic record in the corresponding attack class and T is the correctly classified attack traffic record. As shown in Table 4, the Naïve Bayes overall classification accuracy is above 99.3%. The result indicates that the proposed Naïve Bayes mechanism classifies attacks into detailed attack types with acceptable accuracy. It identifies the TCP-SYN attacks and UDP attacks with less false positives. At the same time, it shows mistake in false negative and absolutely there are no issues in false positives.

The EGT-based overlay network operated in the following scheme is with the warning-victim-closest nodes will indicate to the border-gate nodes to stop the attack flow and with the gossips the nodes closest to the source will indicate to the intermediate network nodes [30]. It means that the aggregated traffic is still attempting to enter the network. The result should improve the accuracy in classification and also in attack detection to stop undesired traffic as close to the sources as possible.

7. Performance Evaluation of Randomly Connected Overlay Network (RON) and Evolutionary Game Theory- (EGT-) Based Overlay Network

The Randomly Connected Overlay Network provides decentralized certificate authority to the nodes. The EGT-based overlay network nodes share digitally signed messages to the other nodes. By this way, it allows other nodes to validate the authenticity of sending nodes. EGT-based overlay network nodes spread their gossip among all the neighbors with network reciprocity, whereas the randomly connected nodes spread only the next-step node. Hence local anomaly can only be detected.

In EGT-based overlay network, the accuracy of the classification is very high due to the global level sharing of gossips and detection accuracy is very fast with the multinode link-formation game connectivity among network nodes. Figure 16 shows EGT-based overlay network nodes functions with 85%, 90%, and 95% detection accuracy. Table 5 lists values of True Positive Rate (TPR), False Positive Rate (FPR), and False Negative Rate (FNR). Both are rich in EGT-based overlay network.

This connectivity increases the interaction among the nodes to define the strategies of the node and to select the path to send the warning message to the node from where the message was received. In the random connection overlay network nodes, the links are completely saturated during a DDoS attack [3]. Unfortunately, standard packet flooding attacks effectively remove some sets of nodes from the infrastructure. This cooperation brings the detection and defense process before a response can be mounted to particular victim.

Table 5: Attack detection rate at border-gate nodes.

Detection accuracy	Evolutionary Game Theory- (EGT-) based overlay network			Randomly Connected Overlay Network (RON)		
	TPR* (%)	FPR* (%)	FNR* (%)	TPR* (%)	FPR* (%)	FNR* (%)
Node 1	85	.6	0	70	2	1
Node 2	95	.4	0	68	2.5	3
Node 3	98	.1	.1	29	3	.8

*True Positive Rate (TPR), False Positive Rate (FPR), and False Negative Rate (FNR).

8. Conclusion

In order to include the self-management and self-defense in network engineering, "Adaptive Distributed Critical-Care Extensive Response Network" (ADCERN) is designed using evolution of cooperation mechanism. The AD-CERN is invented from two innovative techniques. At first level, the free-form and flexible structure of overlay network is included. This structure recovers the rigid nature of existing overlay network. Here, the EGT-based overlay network is adopted for the achievement of entire cooperation among the autonomous nodes. The multinode link-formation game keeps one link to the cooperative node in the nodes' original group, which leads to the formation of efficient cooperative network structure. The combination of network reciprocity and group selection mechanisms is considered for the evolution of cooperation in the overlay network.

In the second level, every node is fed with the ability to adapt. Each node gets a learning component with a mechanism for information sharing and classification techniques. The machine learning and data mining techniques use Naïve Bayes classification algorithm. Here, the evolutionary mechanism leads to the global optimization procedure.

In the network evaluation, the proposed AD-CERN system detects the distributed critical attack points which are found to be closer to the service. This system achieves 99% average detection rate and 98.3% classification accuracy with very high global level sharing of gossips and warning. Moreover, it provides the highest detection accuracy in both TCP SYN and UDP flooding attacks. The FPR and TPR rate is rich in every node of AD-CERN system.

Our work is a significant step towards the exploration of rigid to malleability characteristics of unstructured overlay network. The AD-CERN greatly increases the network efficiency and convergence of cooperation. In addition, we utilize the property of physical network with shorter average neighbor distance. The robustness of network is also maintained even in the high flooding rate attacks. Thus, self-management and self-defense method is moved from realm of fiction to real-time network engineering.

In future, we are trying to utilize the more intelligent gossip and warning, which will reduce the information sharing overheard. In addition, we are planning to deploy our network structure in a real-time large scale environment with real attack. We are also planning to explore exciting usages of AD-CERN, in applications such as media streaming, application-level multicasting, and media distribution.

The link-formation game connectivity maintains all the components in all critical services, so that the EGT-based overlay networks obtain the cooperative nature of infrastructure. Further, it maintains its robustness in the removal of nodes by failures or attacks. Thus the EGT-based overlay network relatively gives high level of tolerance in the network critical services. The EGT-based overlay network nodes are protected from the large amounts of data to and from the compromised overlay node.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to thank their institutional authorities for extending unmatched cooperation in making available all educational materials and infrastructure required to undertake this study. Not to mention, their encouragement and moral support in helping them conducting this study successfully. Further, they would like to place on record their sincere thanks and gratitude to Tata Consultancy Services, Chennai, for their generous financial assistance to their study.

References

[1] E. Ahmed, G. Mohay, A. Tickle, and S. Bhatia, "Use of IP addresses for high rate flooding attack detection," in *Security and Privacy-Silver Linings in the Cloud*, vol. 330, pp. 124–135, Springer, Berlin, Germany, 2010.

[2] M. E. Locasto, "Self-healing: science, engineering, and fiction," in *Proceedings of the Workshop on New Security Paradigms (NSPW '07)*, pp. 43–48, New York, NY, USA, September 2007.

[3] G. Zhang and M. Parashar, "Cooperative defence against DDoS attacks," *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, pp. 69–83, 2006.

[4] Y. Wang and A. Nakao, "On cooperative and efficient overlay network evolution based on a group selection pattern," *IEEE Transactions on Systems, Man, and Cybernetics B: Cybernetics*, vol. 40, no. 2, pp. 493–504, 2010.

[5] A. Castelucio, A. Ziviani, and R. Salles, "An AS-level overlay network for IP traceback," *IEEE Network*, vol. 23, no. 1, pp. 36–41, 2009.

[6] E. S. Pilli, R. C. Joshi, and R. Niyogi, "An IP traceback model for network forensics," in *Digital Forensics and Cyber Crime*, vol.

53 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 129–136, Springer, Berlin, Germany, 2011.

[7] X. Y. Zhang, Q. Zhang, Z. Zhang, G. Song, and W. Zhu, "A construction of locality-aware overlay network: mOverlay and its performance," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 1, pp. 18–28, 2004.

[8] D. Andersen, H. Balakrishnan, F. Kaashoek, and R. Morris, "Resilient overlay networks," *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 1, p. 66, 2002.

[9] Z. Duan, Z. Zhang, and Y. T. Hou, "Bandwidth provisioning for service overlay networks," in *Scalability and Traffic Control in IP Networks II*, vol. 4868 of *proceedings of SPIE*, Boston, Mass, USA, 2002.

[10] Z. Li and P. Mohapatra, "QRON: QoS-aware routing in overlay networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 1, pp. 29–40, 2004.

[11] L. Subramanian, I. Stoica, H. Balakrishnan, and R. H. Katz, "OverQoS: offering internet hierarchy from multiple vantage points," in *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '02)*, New York, NY, USA, October 2002.

[12] M. A. Nowak, "Five rules for the evolution of cooperation," *Science*, vol. 314, no. 5805, pp. 1560–1563, 2006.

[13] Z. Wang, A. Szolnoki, and M. Perc, "Optimal interdependence between networks for the evolution of cooperation," *Scientific Reports*, vol. 3, article 2470, 2013.

[14] E. lieberman, C. Hauert, and M. A. Nowak, "Five rules for the evolution of cooperation," *Nature*, vol. 433, no. 5805, p. 312, 2005.

[15] H. Ohtsuki, C. Hauert, E. Lieberman, and M. A. Nowak, "A simple rule for the evolution of cooperation on graphs and social networks," *Nature*, vol. 441, no. 7092, pp. 502–505, 2006.

[16] D. Hales, "From selfish nodes to cooperative networks—emergent link-based incentives in peer-to-peer networks," in *Proceedings ot the 4th International Conference on Peer-to-Peer Computing (P2P '04)*, pp. 151–158, Zurich, Switzerland, August 2004.

[17] A. Szolnoki and M. Perc, "Emergence of multilevel selection in the prisoner's dilemma game on coevolving random networks," *New Journal of Physics*, vol. 11, Article ID 093033, 2009.

[18] A. Traulsen and M. A. Nowak, "Evolution of cooperation by multilevel selection," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 103, no. 29, pp. 10952–10955, 2006.

[19] T. Velauthapillai, A. Harwood, and S. Karunasekera, "Global detection of flooding-based DDoS attacks using a cooperative overlay network," in *Proceedings of the 4th International Conference on Network and System Security (NSS '10)*, pp. 357–364, Australia, September 2010.

[20] C. Xie, G. Chen, A. Vandenberg, and Y. Pan, "Analysis of hybrid P2P overlay network topology," *Computer Communications*, vol. 31, no. 2, pp. 190–200, 2008.

[21] G. Hardin, "The tragedy of the commons," *Science*, vol. 162, no. 3859, pp. 1243–1248, 1968.

[22] M. Perc and P. Grigolini, "Collective behavior and evolutionary games—an introduction," *Chaos, Solitons & Fractals*, vol. 56, pp. 1–5, 2013.

[23] B. F. Cooper, "An optimal overlay topology for routing peer-to-peer searches," in *Middleware 2005*, pp. 82–101, Springer, Berlin, Germany, 2005.

[24] J. Corbo and D. Parkes, "The price of selfish behavior in bilateral network formation," in *Proceedings of the 24th Annual ACM Symposium on Principles of Distributed Computing (PODC '05)*, pp. 99–107, July 2005.

[25] T. Moscibroda, S. Schmid, and R. Wattenhofer, "On the topologies formed by selfish peers," in *Proceedings of the 25th Annual ACM Symposium on Principles of Distributed Computing*, pp. 133–142, July 2006.

[26] N. Poggi, T. Moreno, J. Berral, R. Gavalda, and J. Torres, "Web customer modeling for automated session prioritization on high traffic sites," in *User Modeling 2007*, vol. 4511 of *Lecture Notes in Computer Science*, pp. 450–454, Springer, 2007.

[27] J. L. Berral, N. Poggi, J. Alonso, R. Gavaldà, J. Torres, and M. Parashar, "Adaptive distributed mechanism against flooding network attacks based on machine learning," in *Proceedings of the 1st ACM workshop on Workshop on AISec (AISec '08)*, pp. 1–11, New York, NY, USA, October 2008.

[28] D. Dittrich, "Distributed Denial-of-Service (DDoS) Attacks/tools," http://staff.washington.edu/dittrich/misc/ddos/.

[29] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," *Computer Communications*, vol. 31, no. 17, pp. 4212–4219, 2008.

[30] V. Akilandeswari, D. Namachivayam, S. Prasanna, and S. M. Shalinie, "Design of an early response system using EGT-based overlay network," in *Proceedings of the IEEE International Conference on Recent Trends In Information Technology (ICRTIT '12)*, pp. 445–451, 2012.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 624839, 15 pages
http://dx.doi.org/10.1155/2014/624839

Research Article

Intelligent Supply Chain Integration and Management Based on Cloud of Things

Junwei Yan,[1,2] Sijin Xin,[1] Quan Liu,[1] Wenjun Xu,[1,2] Liwen Yang,[3] Li Fan,[3] Bo Chen,[3] and Qiang Wang[3]

[1] *School of Information Engineering, Wuhan University of Technology, Wuhan 430070, China*
[2] *Joint Mobile Communication Lab., Wuhan University of Technology and China Mobile Group, Hubei Co., Ltd., Wuhan 430070, China*
[3] *China Mobile Group Hubei Co., Ltd., Wuhan 430023, China*

Correspondence should be addressed to Wenjun Xu; xuwenjun@whut.edu.cn

Received 4 October 2013; Revised 5 January 2014; Accepted 1 February 2014; Published 16 March 2014

Academic Editor: Neil Y. Yen

The fierce global competition and market turbulence has been forcing the enterprises towards to the integration and intelligence for supply chain management, and the seamless information sharing and collaboration as well as operation agility are the challenges which need to be conquered, in terms of the highly distributed and heterogeneous resources located in separated warehouses. Although a number of works have been done to achieve the aforementioned targets, few of them are able to provide an overall integration and intelligence support for such system management. In this context, a novel intelligent supply chain integration and management system based on Cloud of Things is presented, in order to provide flexible and agile approaches to facilitate the resource sharing and participant collaboration in the whole supply chain life cycle. Furthermore, the enabling technologies, such as intelligent supply chain condition perception, heterogeneous network access convergence, and resource servicisation, are also studied. Finally, a case study together with the prototype system is implemented and demonstrates that the developed system can efficiently realise the integration of supply chain processes in the form of services, and also provide the effective intelligence support for physical resource management, so as to achieve an overall performance assurance for the system operation.

1. Introduction

As a vital and important process of industrial production, supply chain affects the operation efficiency and beneficial value of enterprises with the cost of transportation, land, and labor. Supply chain integration, which is widely considered as a vital factor determining the supply chain performance, for instance, reducing cost, improving responsiveness, increasing service level, and facilitating decision making, has attracted more and more attention [1–4]. Information sharing and collaboration [1, 5] as well as the agility [6] are the key characteristics of the supply chain integration. On one hand, information sharing and collaboration is able to enhance the supply chain visibility and avoid the information delay and distortion, which would result in tremendous variations and inefficiencies, and even a phenomenon called the bullwhip effect [7, 8]. On the other hand, agility aims at providing the required abilities for an enterprise to respond properly and being actively adapted to rapid and unexpected changes in global market [9]. Over the past decades, the two aspects of supply chain integration are technically challenging due to the high fragmentation of industry, which is induced by economic globalization and distributed manufacturing [10]. With the highly distributed and heterogeneous resources located in separated warehouses, the warehouse integration, which is an indispensable part of supply chain management, will face more challenges. In this context, supply chain integration has higher requirements for real-time information sharing, response speed, and flexibility in agile management. However, few of the existing frameworks and technologies are able to satisfy all of these diverse needs and the adoption of several different technologies and systems may lead to higher cost, lower system flexibility and extensibility, and more complex integration, such as Electronic Data Interchange

(EDI) and Enterprise Resource Planning (ERP). Therefore, there is a need for novel frameworks and tools to enhance the performance of agility, real-time sharing, and flexible collaboration in supply chain management.

With the rapid development of ICT technologies, for example, Cloud Computing and Internet of Things (IoT) [11], new opportunities were created to build applications, which better integrate the real-time conditions of physical resources and fill the gap between the virtual and real world [12]. Cloud of Things (CoT) [13], launched initiatively by the MIT Auto-ID Labs, builds on the two concepts of IoT and Cloud Computing and constructs a model of an object in the cloud with a defined set of Application Programming Interfaces (APIs), facilitating the integration of data from heterogeneous sources more readily than trying to establish a common registry or protocol across multiple organizations. In the architecture of CoT [12, 13], the heterogeneous resources (sensing, actuation, computing, and storage) can be virtualised as a service, be aggregated in terms of a given thing-like semantics, and then be provided to the end users. The CoT has emerged as a promising framework and technology solution to integrate the distributed physical resources and manage the things in terms of cloud services in a scalable, flexible, and reusable manner, which can be seen as interfaces independent from location and accessed with simple and pervasive methods [14]. Due to the features of modern supply chain management, such as high distribution of items, more requirements of integration, and agility, the basic ideas and framework of CoT suit the design of supply chain system well.

In order to facilitate the modern supply chain integration and conquer the aforementioned challenges, such as lacking of real-time information and agility, this paper presents an intelligent supply chain integration and management system based on the conception of CoT. In traditional supply chain management system, the efficient supply chain and response supply chain are two main branches [15]. The primary goal of the previous one is to supply demands at the lowest level cost [16], while the other one's aim is to respond quickly to various demands [17]. In this system, more attention is paid to supply chain integration, real-time monitoring requirements, and cloud service for agility, to meet various demands at lowest cost in agile way. It uses the intelligent perception techniques to collect the condition information of resources during the whole life cycle of supply chain for real-time monitoring and enable the resources to be seamlessly adapted to the service management platform using a set of networking approaches for supply chain integration. Moreover, the supply chain resources are virtualised as cloud services to be provided to the users on demand, so as to facilitate the agility for various demands.

The remainder of this paper is structured as follows. Section 2 describes the related works on operation models and technologies for supply chain integration and management. Section 3 develops a system framework for supply chain integration and management based on CoT. Section 4 presents the enabling technologies for the developed system. Then, a case study together with the system implementation and evaluation are presented in Section 5. Finally, Section 6 concludes the paper.

2. Related Works

With the rapid changes in the logistics industry, the following problems [1, 6, 18–22] in supply chain management are identified: (i) high fragments in supply chain, (ii) information sharing and collaboration between participants, and (iii) agile supply chain management for rapid, effective, and efficient response to the changes in market. Some previous researches have been done on the supply chain management, including theoretical research and practical system development. Nevertheless, none of the single existing technologies can solve the problems and provide an overall performance assurance for information sharing and collaboration as well as the agility of supply chain management.

With the emergency of new ICT technologies, the supply chain management system has made a certain development in the last decades. Sense of the operation condition is usually the first step for information sharing and collaboration in the supply chain management. In [11], current development trend of IoT was discussed and the applications in the transportation and logistics domain are analyzed. Real-time information collection technologies based on RFID and other sensors can monitor almost all the supply chain links. Miorandi et al. [23] presented the digital and physical entities that can be linked by various appropriate information and communication technologies using IoT. It not only provided localization and tracking capabilities, but also enabled the things communication with low power. In general, the barcode [24, 25] and RFID technology [26–29] are frequently used to store and acquire product information in logistics, which is considered as an important part of supply chain management. Moreover, the collected information will be transmitted using various communication networks, such as Zigbee, wireless sensor network (WSN), 2G/3G, and Ethernet, located in different part of the supply chain, and this is the realisation foundation of information sharing and collaboration. In [30], the WSN technology was widely adopted in diverse environments, such as remote environmental monitoring and target tracking. In [30–32], the Zigbee technology provided solutions for communication among distributed sensor nodes deployed in the logistics links. After all, the degree of information sharing and collaboration can be improved by the usage of IoT and relevant key technologies. However, the agility which is another target of modern supply chain system cannot be achieved with these.

For the purpose of pursuing the agile and flexible system, more attention has been paid on system architecture, virtualisation, and servicisation technologies. The two technologies are critical for supporting the resource sharing and collaboration. In early stage of cloud computing [33, 34], everything was treated as service and three distinct layers from computing resources were defined to end-user applications in cloud computing architecture, for example, Software as a Service (Saas), Platform as a Service (PaaS), and Infrastructure as

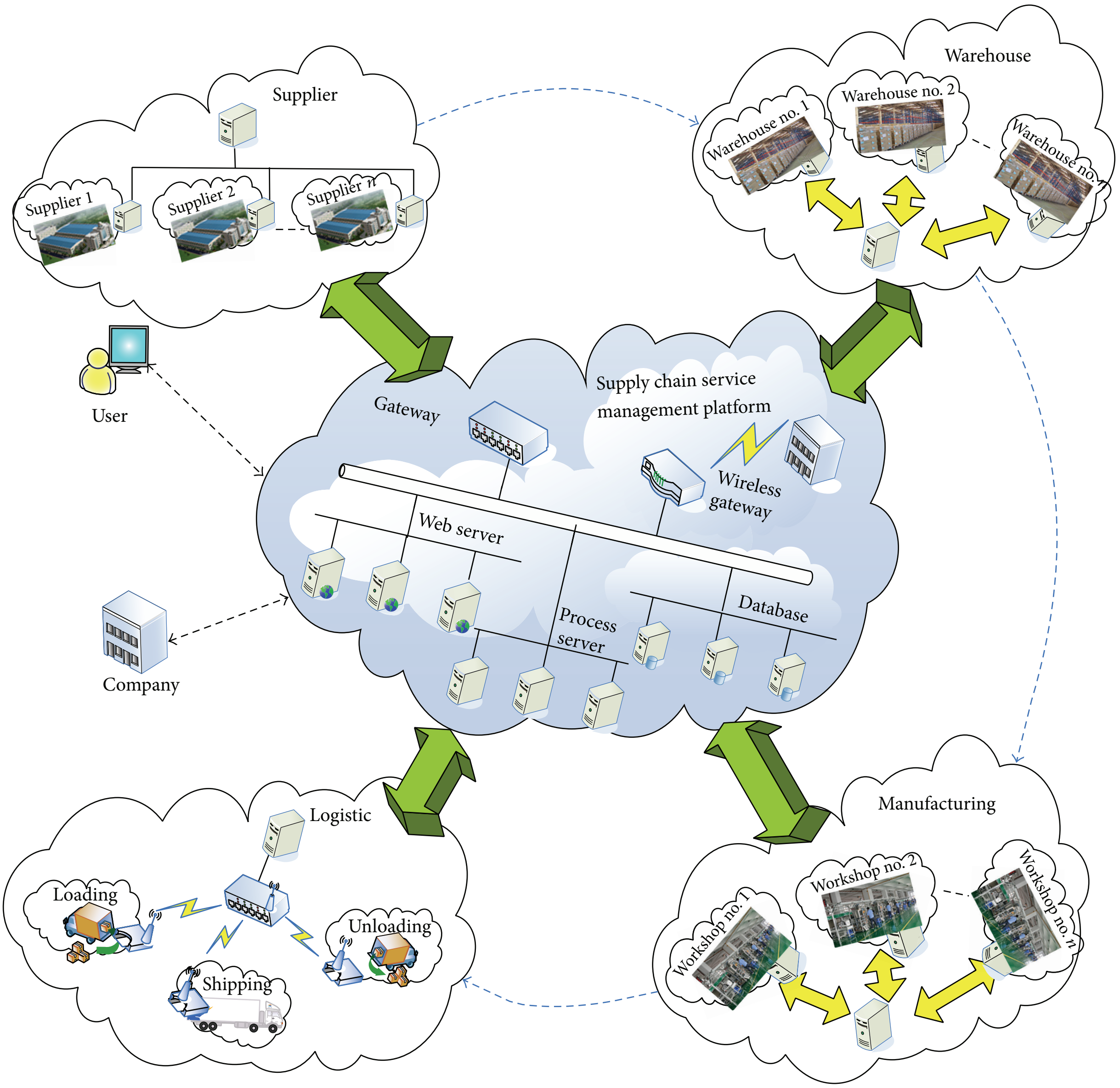


FIGURE 1: The CoT model for supply chain integration and management.

a Service (IaaS). Virtualisation and servicisation mean the abstraction of computing and storage resource [35]. In recent years, the applications of resource virtualisation and servicisation have extended to other areas with the development of cloud computing and its enabling technologies, such as manufacturing industry and logistics. In manufacturing domain [36–38], a new computing- and service-oriented manufacturing model, named cloud manufacturing, was proposed, and the manufacturing resources and capabilities can be virtualised and encapsulated for on demand using the virtualisation and servicisation technologies. Xu [39] compared cloud computing and cloud manufacturing and also indicated that cloud manufacturing performs agile and flexible way, in which distributed manufacturing resources are encapsulated into cloud services and the clients use them according to their requirements. In logistics area, as vital link of supply chain, Li et al. [40] proposed the logistics equipment and computing resources can be used flexibly by resource virtualisation, and the methods of selecting the best logistics services to raise the feasibility and effectiveness of logistics system were presented. As the data collected by various sensors becomes more and more large-scale and complex in supply chain management, traditional database software tools for data capturing, storing, managing, and analyzing cannot meet the requirements for the big data processing [41]. Big data strategies, seen as ways and tools for big data processing, are used to deal with the big data. Reference [42] introduces distributed computing as a strategy for big data, including distributing store and analysis.

In summary, most researchers have focused on virtualisation and servicisation technologies as well as the related applications in computing, manufacturing, logistics, and so

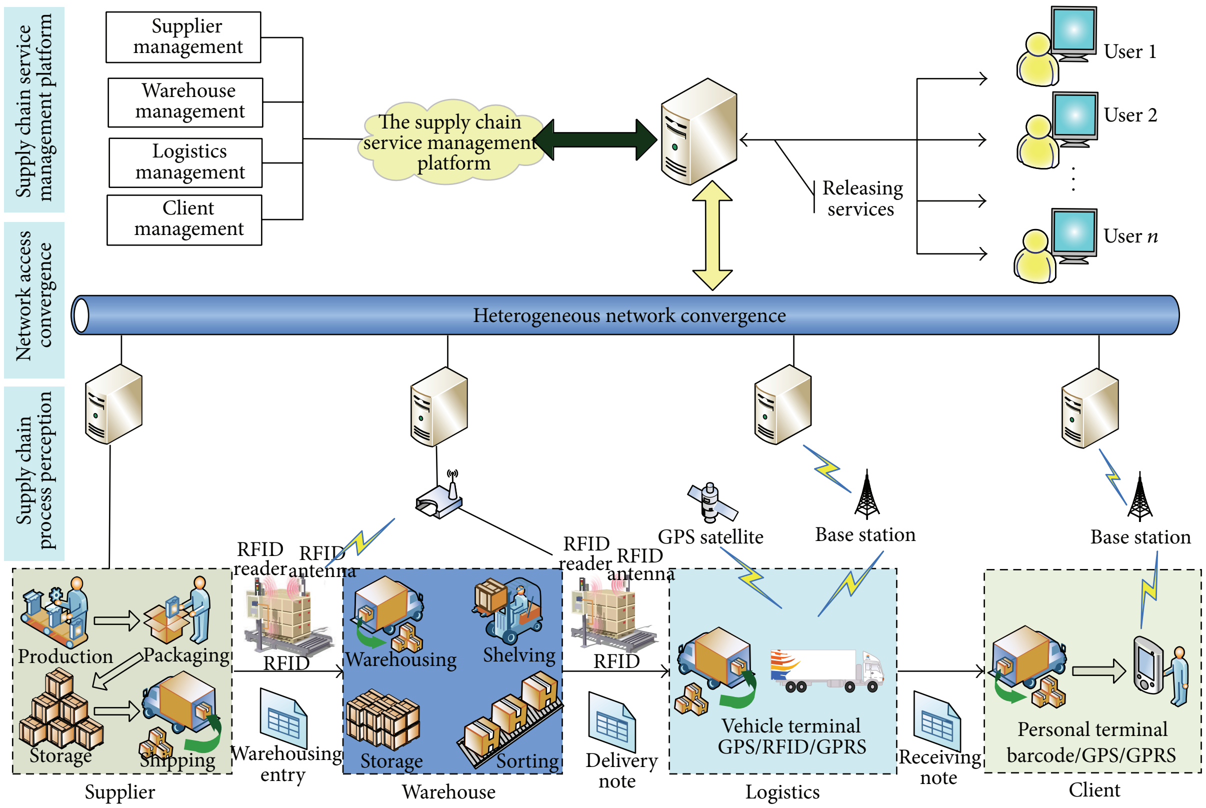


Figure 2: Architecture of an intelligent supply chain integration and management system based on CoT.

forth. Few researches investigate the architecture of supply chain integration and management with the integration of IoT and cloud technology, in which distributed resources, for example, suppliers, warehouses, transportations, and so forth, can be treated as services and coordinated dynamically. The CoT aims to integrate the two concepts of IoT and cloud computing and provides the relevant services which can interact with the surrounding environment by collecting data and applying the management using the big data strategies. In a CoT system, things are treated as a service, which means heterogeneous resources can be aggregated and abstracted according to tailored thing-like semantics. As the new characteristics, the CoT is able to provide an advisable solution for improving the performance of agility, information sharing, and collaboration in supply chain system integration and management.

3. Framework

In this section, an overview of the developed system is presented. We firstly introduce a CoT model for supply chain integration and management,and then the architecture of the developed system is described in detail. The research assumes the supply chain management consists of supplier management, warehouse management, manufacturing management, and logistics management. The model of the supply chain integration and management system is developed based on CoT, which can provide diverse services to both the users and resource providers. In the CoT model, as shown in Figure 1, the supply chain management integration and platform are fulfilled with the services provided by individual clouds, supplier cloud, manufacturing cloud, warehouse cloud, and logistics cloud.

Various suppliers, providing respective services, gather together to realise the supplier cloud for supply chain management. The warehouse cloud servers the management platform with services provided by distributed warehouses. The resource services and capabilities are provided in the form of service cloud. In logistics cloud, each link of logistics is defined as a service provider, who collects logistics information and provides logistics services to the management platform.

As aforementioned discussion, the developed system focuses on the CoT and relevant enabling technologies for developing the functional system. As illustrated in Figure 2, the architecture of CoT-oriented supply chain integration and management system can be divided into three layers.

(i) Supply chain process perception lies in the bottom of the system architecture and is developed to acquire link condition information of supply chain for material tracking as well as resource integration and management. The whole supply chain management consists of four parts which involve the supplier management, warehouse management, logistics management, and client management.

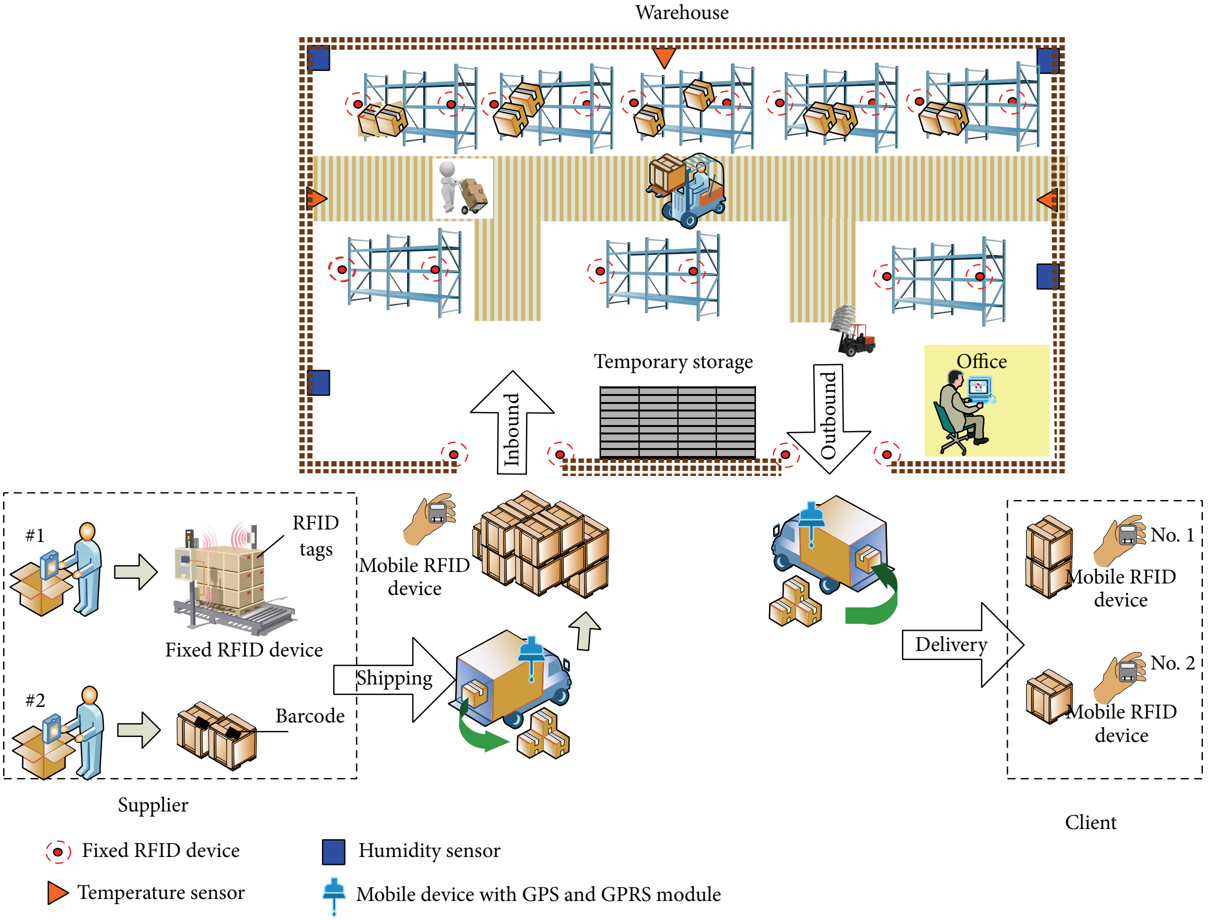


Figure 3: Deployment of process condition perception modules.

(ii) Network access convergence is to connect heterogeneous networks, which are used for transmitting perception information. The process condition perception information is transmitted using a set of different communication approaches according to the requirements of application types and working environment. For instance, the Ethernet used for huge amount and wide area information transmission, Zigbee network used for local monitoring information transmission, GPRS used for logistics location information transmission, and so forth. Diverse subsystems of networking can connect the management platform by heterogeneous network access convergence technology.

(iii) Supply chain service management platform is developed to manage the whole life cycle of supply chain activities, including the suppliers, warehouses, logistics, and clients, based on the process condition information collected by the intelligent perception modules. The service management platform can be divided into the supplier management, logistics management, client management, and warehouse management, which consists of the warehouse-entry management, shelves management, warehouse-out management, and storage management. In each management module of the platform, the resources in the supply chain are virtualised and encapsulated into services based on the perception information, and the users can inquire the services and invoke them with diverse demands.

4. Enabling Technologies

4.1. Intelligent Process Condition Perception. In order to collect various condition information required by supply chain integration and management, various intelligent condition perception technologies, such as RFID, embedded technology, barcode, and other sensor technologies, are adopted in the developed system.

RFID is an automatic identification technology which depends on remotely storing and retrieving data using RFID tags. Compared with the traditional tracking manual tracking system, the RFID is widely used in the supply chain management with the characteristics of automatic identification, retrieving, tracking, and storing. A whole RFID system consists of two parts, RFID readers connected to one or more antennas and RFID tags, which store produced information in the form of electronic product code. On the other hand,

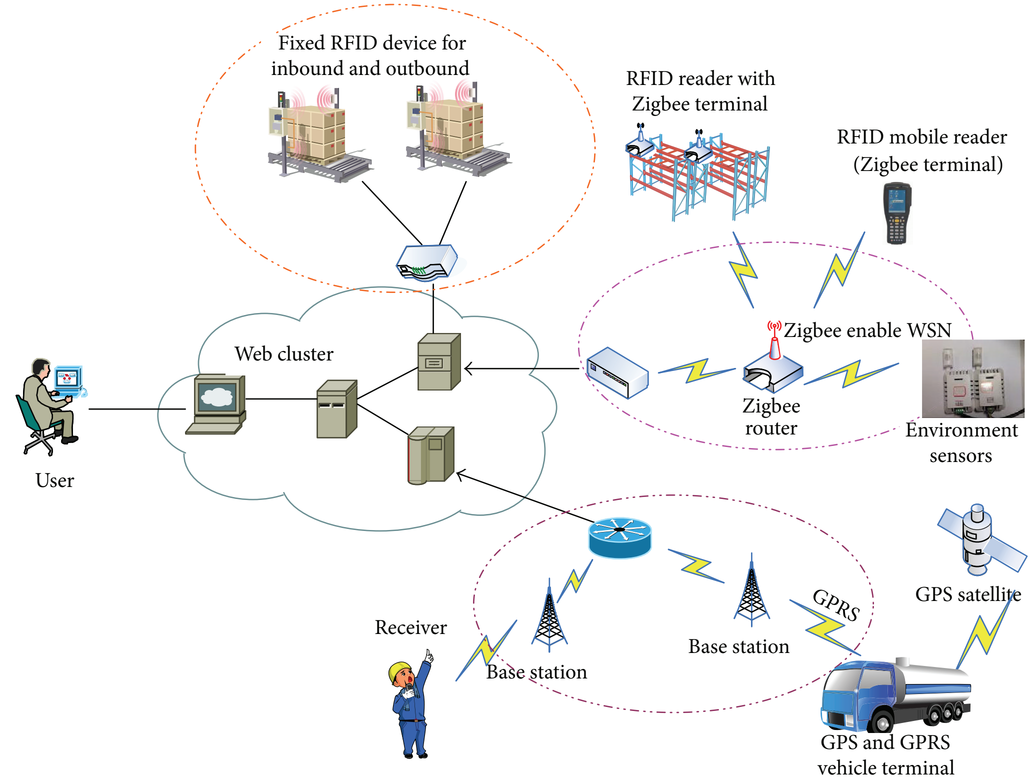


Figure 4: Heterogeneous networking solution.

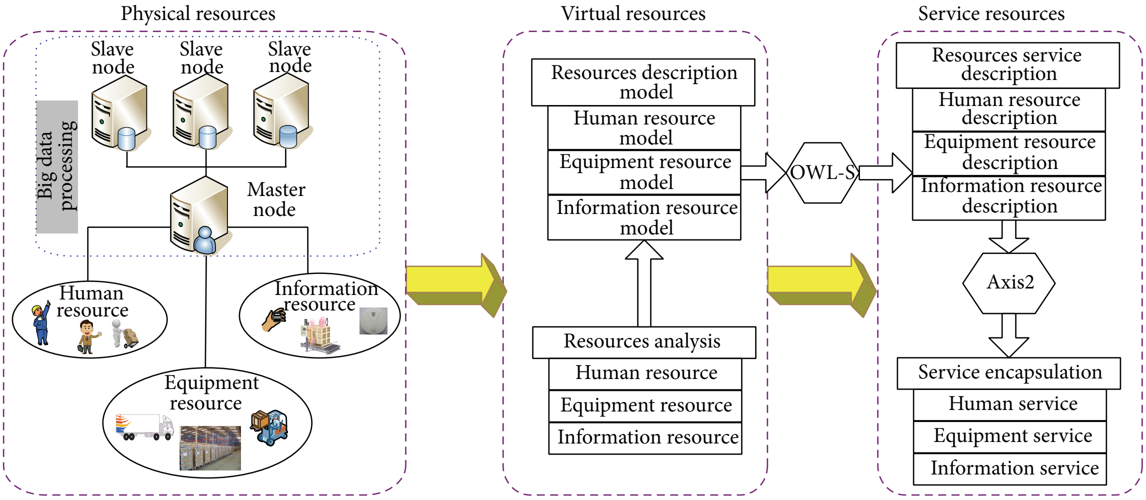


Figure 5: Big data processing and service packing.

the barcode system is the most popular management approach that has obtained much attention in the field of logistics. There are two kinds of barcode, one is one-dimensional barcode and the other is two-dimensional barcode. With the development of mobile intelligent terminal technology, the barcode data is more and more easily got by smart phones through mobile applications. Although the RFID technology has great unique advantages with wireless operations, it still cannot completely replace barcodes due to the cost and work environmental constraints.

As shown in Figure 3, the suppliers provide the goods with RFID tags or barcodes, which contain their basic information, such as name, model, quantity, producer, and supplier. As RFID tags are not selected by all suppliers, so the RFID tags, which have the same information with barcodes pasted on the surface of goods, should be added before entering warehouse for warehouse management. A fixed RFID device is deployed in the front of entrance to check the inbound goods according to the receipt. In the warehouses, the RFID readers are fixed on the shelves for goods location

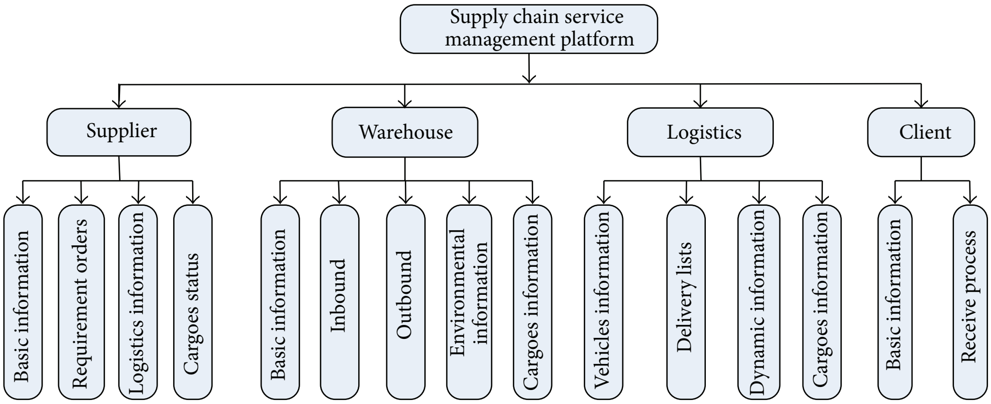


Figure 6: Functional modules of the supply chain service management platform.

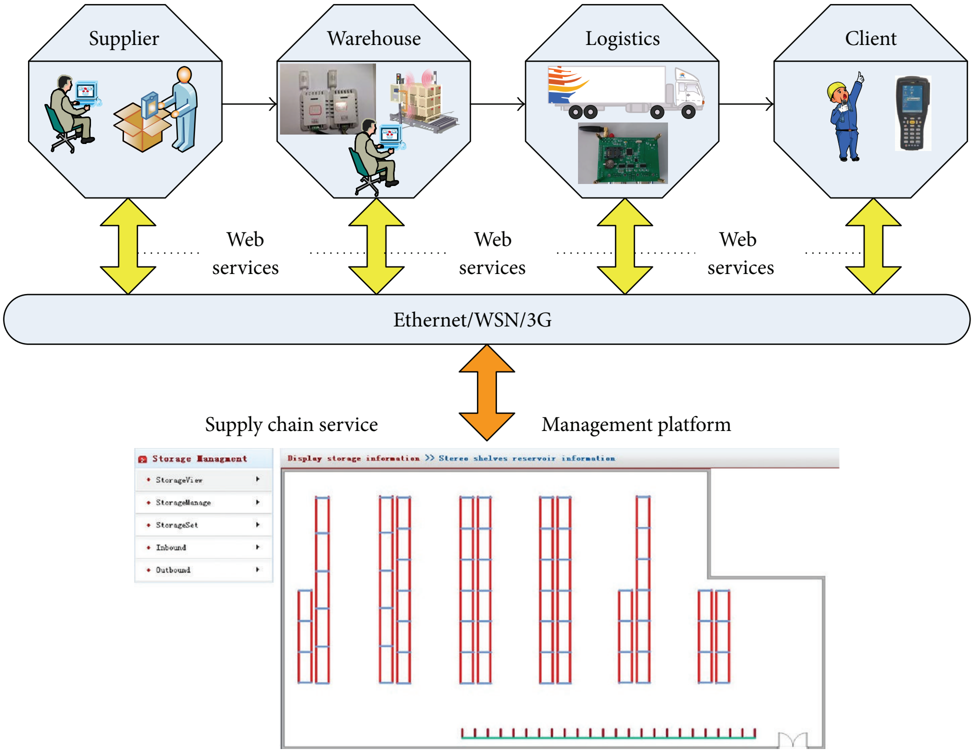


Figure 7: Demonstration system for supply chain integration and management.

and inventory through scanning the RFID tags pasted on the goods. Individual environment sensors are deployed to collect the temperature and humidity information as well. As the inbound process, the fixed RFID device is also used to check the outbound goods according to the delivery list. In the process of logistics, the trucks are positioned with a mobile device consisting of GPS and GPRS module for good tracking. When the cargoes arrive at the destination, the receiver will check and sign automatically using a mobile RFID device, which compared the good information of RFID tags with the receive order information shown in the device.

4.2. Heterogeneous Network Access Convergence. The resource access adaptation and its data transmission are the premise and guarantee of perception information analysis in the supply chain integration and management. It aims at interconnecting sensor nodes and communicates in real-time and accuracy. During the supply chain process, the perception information is multi-source, massive, and heterogeneous, such as cargo condition information, vehicle position information, and warehouse basic information. The traditional single transmission mode cannot satisfy the diverse needs of distributed information transmission in such complex working environment. Therefore, the heterogeneous network accessing and convergence are used to achieve reliable and real-time transmission of the dynamic condition perception information.

In particular, various means of communication techniques, such as Internet, WiFi, Zigbee, and GPRS are selected according to the types of information perception and the

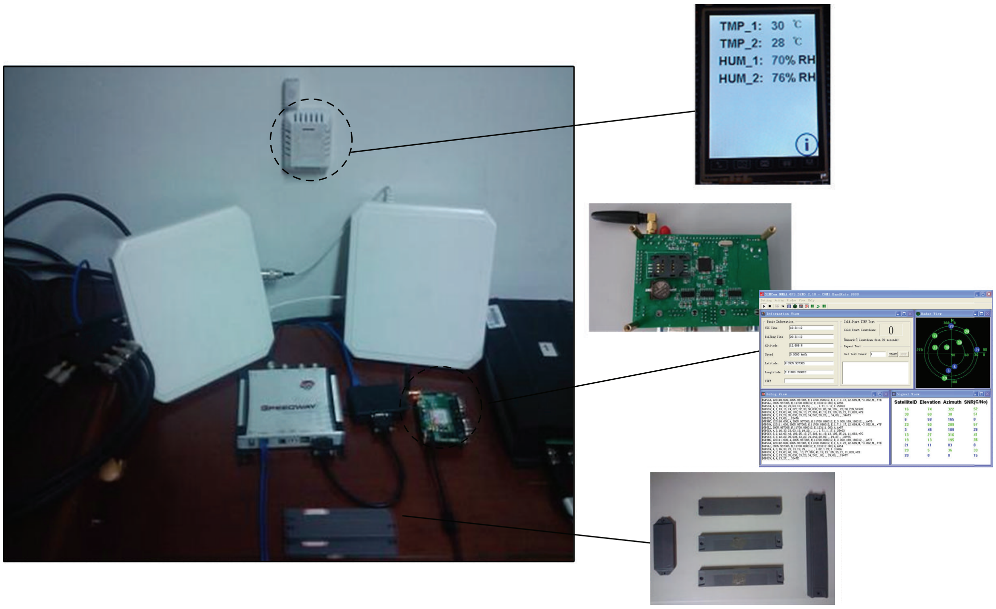


FIGURE 8: Process condition perception tools.

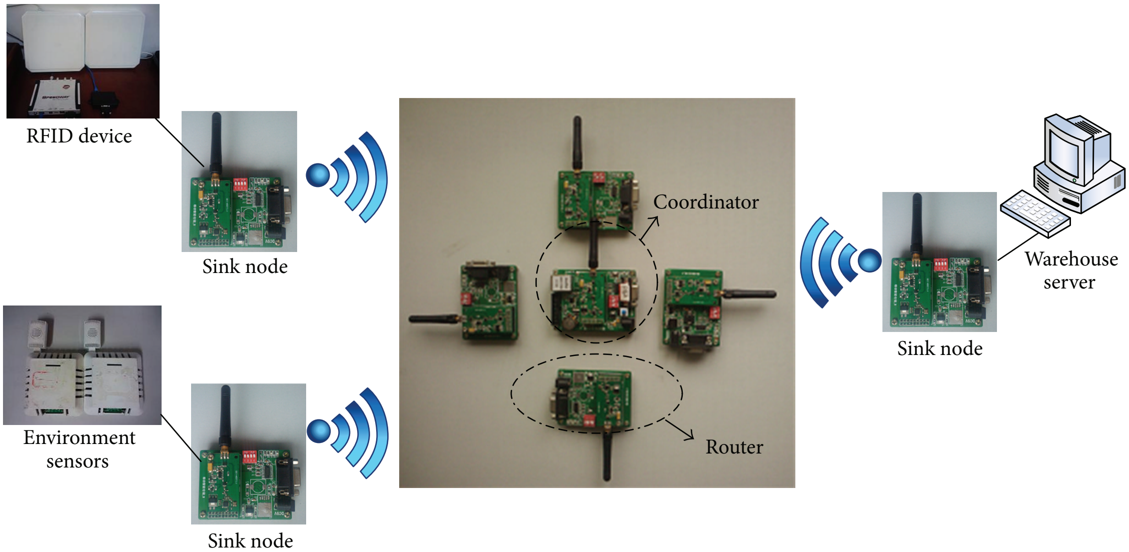
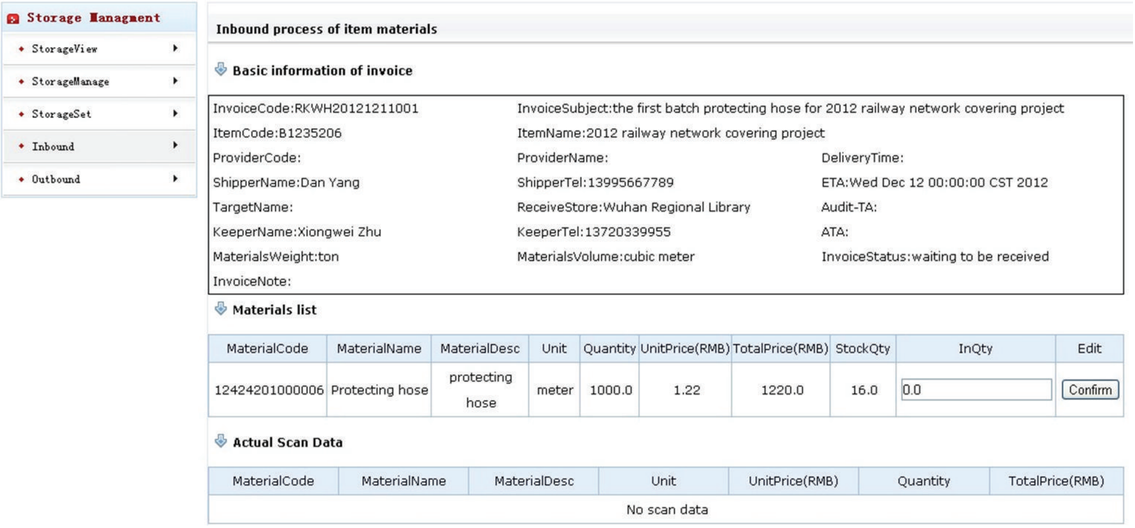


FIGURE 9: Network access for warehouse resources using Zigbee.

TABLE 1: Facilities description.

Facilities	Description
RFID devices number 1 (for inbound and outbound)	Invengo XC-RF807 Reader. Output power: 11 dBm~36 dBm. Ports: RS-232, GPIO, Ethernet interface. Extensions performance: one reader is only for 4 antennas
RFID devices number 2 (for shelves management)	Impinj Speedway Revolution R420. Output power: 10.0 dBm~30.0 dBm. Ports: RS-232, GPIO, Ethernet interface, USB. Extensions performance: one reader can be expanded for 32 antennas with a hub
5 E-tags	Invengo XCTF-8405. Work frequency: 902 MHz~928 MHz. TID: 64bit. Anticollision mechanism (suitable for multitag read)
Zigbee module	RFC-1100A, 433 MHz, 1 W
Mobile phone	Android 4.1, CPU 1638 MHz, RAM 2 G
Server	Windows Server Standard, CPU 2.13 GHz, RAM 16 G
Test PC	Windows XP, CPU 2.09 GHz, RAM 2.96 G



Inbound process of item materials

Basic information of invoice

InvoiceCode:RKWH20121211001
InvoiceSubject:the first batch protecting hose for 2012 railway network covering project
ItemCode:B1235206
ItemName:2012 railway network covering project
ProviderCode:
ProviderName:
DeliveryTime:
ShipperName:Dan Yang
ShipperTel:13995667789
ETA:Wed Dec 12 00:00:00 CST 2012
TargetName:
ReceiveStore:Wuhan Regional Library
Audit-TA:
KeeperName:Xiongwei Zhu
KeeperTel:13720339955
ATA:
MaterialsWeight:ton
MaterialsVolume:cubic meter
InvoiceStatus:waiting to be received
InvoiceNote:

Materials list

MaterialCode	MaterialName	MaterialDesc	Unit	Quantity	UnitPrice(RMB)	TotalPrice(RMB)	StockQty	InQty	Edit
12424201000006	Protecting hose	protecting hose	meter	1000.0	1.22	1220.0	16.0	0.0	Confirm

Actual Scan Data

MaterialCode	MaterialName	MaterialDesc	Unit	UnitPrice(RMB)	Quantity	TotalPrice(RMB)
No scan data						

Figure 10: Inbound management.

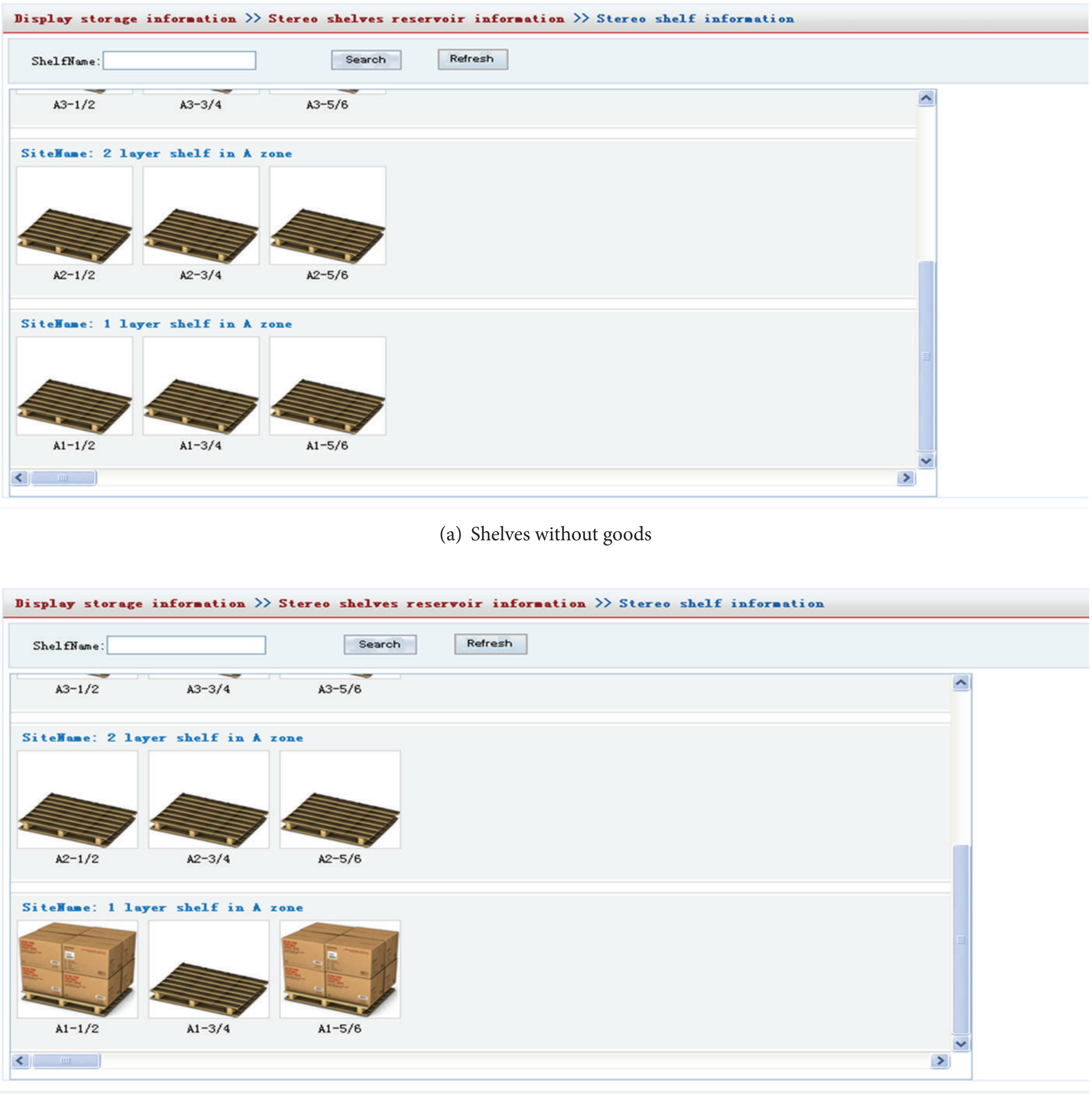
Table 2: Comparison between CoT-based and original system.

Stage	CoT-based system operations	Original system operations	CoT-based system operation time (s)	Original system operation time (s)
(1) Inbound	Scanning RFID tags	Scanning barcodes	2.47	15
	Record automatically and show on the platform	Record data in platform manually	5.18	10
(2) Shelves management	Scanning RFID tags on shelves	Manual count	2.72	60
	Record automatically and show on the platform	Record data in platform manually	4.16	10
	Send environment information by ZigBee (temperature, humidity)	None	16.96	None
(3) Outbound	Scanning RFID tags	Scanning barcodes	3.51	15
	Record automatically and show on the platform	Record data in platform manually	5.23	10
(4) Logistics	Fix position by smart phone	None	2.5	None
	Record and show the position on the platform	None	5	None
	Accept goods by smart phone	None	1.5	None

application scenarios. Figure 4 illustrates the realisation of the network accessing and convergence for connecting the resources in the supply chain process. For instance, in the management of warehouse, the goods information, acquired by the RFID readers which are located in the door, is transmitted using the Ethernet, the warehouse environment information is collected by the distributed sensors, and the shelves information will be sent by the Zigbee networks. In the process of transportation, we utilise the GPRS to transmit shipping information, such as location, name, and count. After arriving at the destination, the goods will be checked by customers, who use a mobile device to scan the RFID tags and send the checked information with GPRS to the server.

4.3. Big Data Processing and Cloud Service Management. For the development of the intelligent supply chain management system, services packaging is a key work and the big data processing is the foundation. Figure 5 shows the processes from physical resources to resource service.

Since the massive and heterogeneous data is collected by the process condition perception modules, the traditional data analysis tools cannot satisfy the requirements of such data processing. However, big data technology, as a new data processing technology, is playing an increasingly important role in data storage, exchange, and processing. According to the features of perception information, nonrelational database is utilised to store data instead of


Display storage information >> Stereo shelves reservoir information >> Stereo shelf information
ShelfName:
Search
Refresh
A3-1/2
A3-3/4
A3-5/6
SiteName: 2 layer shelf in A zone
A2-1/2
A2-3/4
A2-5/6
SiteName: 1 layer shelf in A zone
A1-1/2
A1-3/4
A1-5/6

(a) Shelves without goods

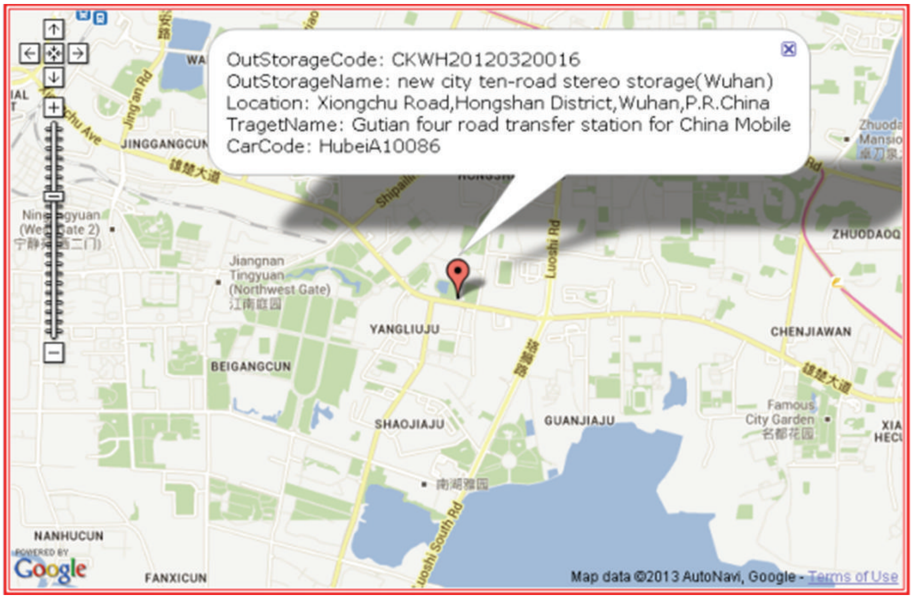
(b) Shelves with goods

Figure 11: Shelves management in warehouse.

traditional relational databases. In order to improve data processing capability, the Hadoop framework is used to achieve the distribution storage and analysis work of the collected big data. The goal of big data technology is to improve data processing capability and improve the data value.

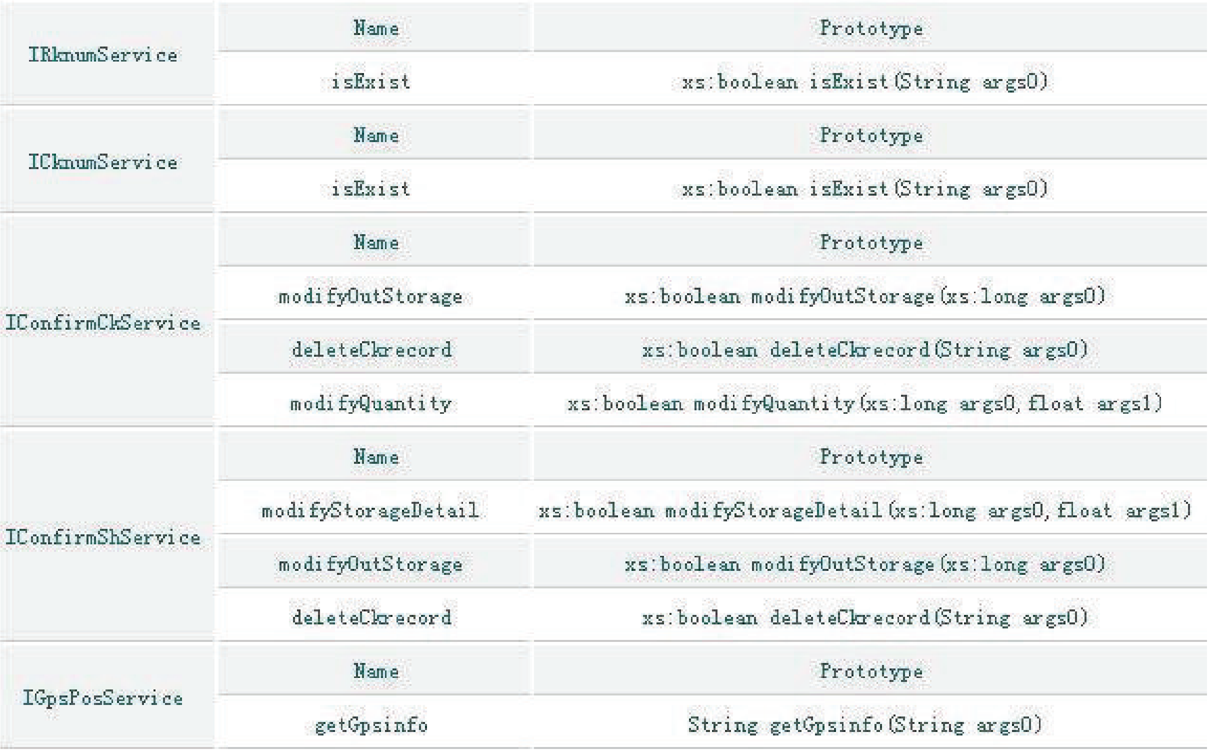
The services packaging aims to provide users with the appropriate supply chain services and it can be divided into four steps: (i) the resources analysis is used for the physical resources classification in terms of their characteristics in the supply chain process, (ii) the resource description model should be built to represent the resource information such as basic attributes and functional attributes, (iii) the OWL-S, which is an ontology web language for services, is used to describe the resource services, and (iv) the appropriate containers, such as Axis2, CXF, are utilised for web services releasing.

The conception of CoT guides the development of the whole supply chain integration and management, in particular for the service management platform. The platform is developed to manage the whole supply chain using the supply chain information collected by the process condition perception modules. As shown in Figure 6, the functional modules of the platform can be divided into four parts roughly, supplier management, warehouse management, logistics management, and client management. Each part is realised with SOA architecture. For example, the warehouse management module is designed with the services provided by the distributed warehouse management system. Meanwhile, the supply chain management platform also



OutStorageCode: CKWH20120320016
OutStorageName: new city ten-road stereo storage(Wuhan)
Location: Xiongchu Road,Hongshan District,Wuhan,P.R.China
TragetName: Gutian four road transfer station for China Mobile
CarCode: HubeiA10086

Figure 12: Logistics tracking management.



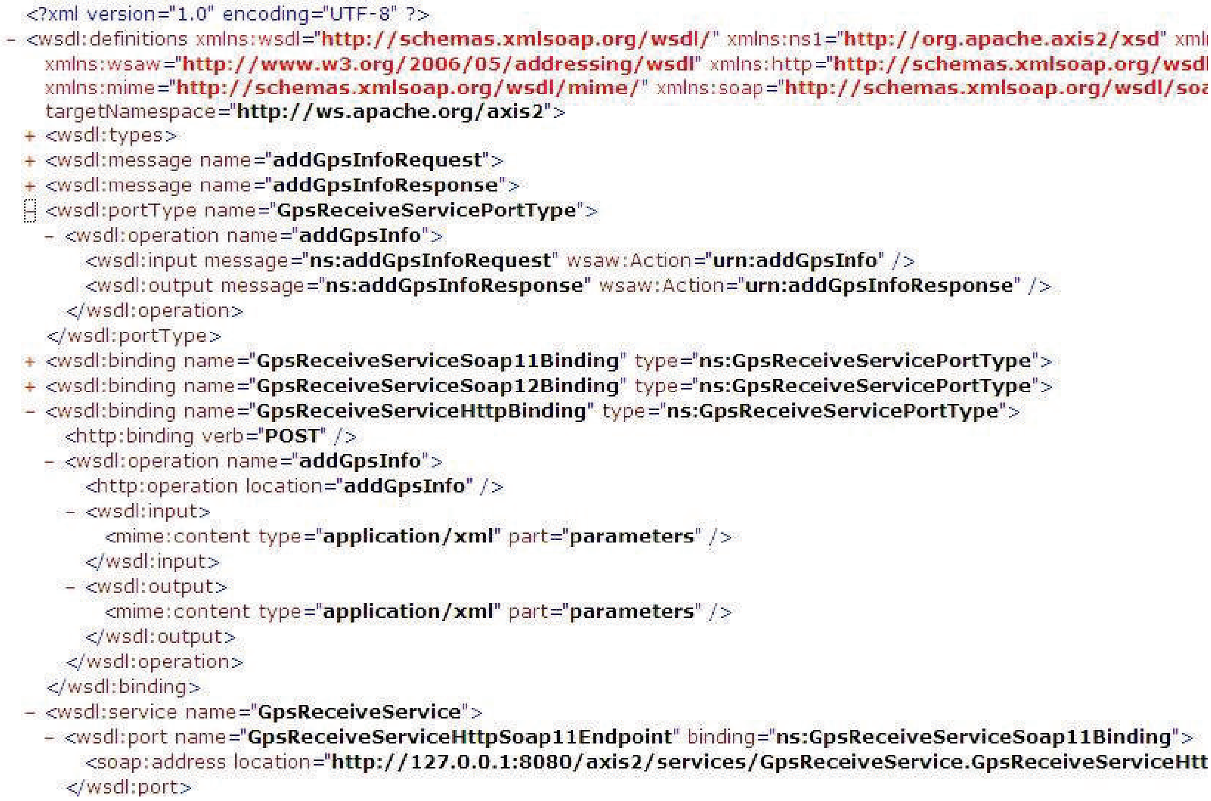
	Name	Prototype
IRknumService	Name	Prototype
	isExist	xs:boolean isExist(String args0)
ICknumService	Name	Prototype
	isExist	xs:boolean isExist(String args0)
IConfirmCkService	Name	Prototype
	modifyOutStorage	xs:boolean modifyOutStorage(xs:long args0)
	deleteCkrecord	xs:boolean deleteCkrecord(String args0)
	modifyQuantity	xs:boolean modifyQuantity(xs:long args0, float args1)
IConfirmShService	Name	Prototype
	modifyStorageDetail	xs:boolean modifyStorageDetail(xs:long args0, float args1)
	modifyOutStorage	xs:boolean modifyOutStorage(xs:long args0)
	deleteCkrecord	xs:boolean deleteCkrecord(String args0)
IGpsPosService	Name	Prototype
	getGpsinfo	String getGpsinfo(String args0)

Figure 13: Service list of the developed system.

can provide cloud service for other users by gathering the distributed resource services.

5. Case Study and Prototype System Implementation

5.1. Case Study. As shown in Figure 7, a demonstration prototype system in laboratory environment has been built to a case study, and it simulates the supply chain integration and management process of the enterprises based on the developed system and the enabling technologies. The whole supply chain process can be divided into four parts, including the supplier, warehouse, logistics, and customer. Compared to the traditional systems, the demonstration system focuses on the supply chain integration with web services released by each useful independently functional subsystem, in which



```
  <?xml version="1.0" encoding="UTF-8" ?>
- <wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:ns1="http://org.apache.axis2/xsd" xml
    xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl" xmlns:http="http://schemas.xmlsoap.org/wsdl
    xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soa
    targetNamespace="http://ws.apache.org/axis2">
  + <wsdl:types>
  + <wsdl:message name="addGpsInfoRequest">
  + <wsdl:message name="addGpsInfoResponse">
  - <wsdl:portType name="GpsReceiveServicePortType">
    - <wsdl:operation name="addGpsInfo">
        <wsdl:input message="ns:addGpsInfoRequest" wsaw:Action="urn:addGpsInfo" />
        <wsdl:output message="ns:addGpsInfoResponse" wsaw:Action="urn:addGpsInfoResponse" />
      </wsdl:operation>
    </wsdl:portType>
  + <wsdl:binding name="GpsReceiveServiceSoap11Binding" type="ns:GpsReceiveServicePortType">
  + <wsdl:binding name="GpsReceiveServiceSoap12Binding" type="ns:GpsReceiveServicePortType">
  - <wsdl:binding name="GpsReceiveServiceHttpBinding" type="ns:GpsReceiveServicePortType">
      <http:binding verb="POST" />
    - <wsdl:operation name="addGpsInfo">
        <http:operation location="addGpsInfo" />
      - <wsdl:input>
          <mime:content type="application/xml" part="parameters" />
        </wsdl:input>
      - <wsdl:output>
          <mime:content type="application/xml" part="parameters" />
        </wsdl:output>
      </wsdl:operation>
    </wsdl:binding>
  - <wsdl:service name="GpsReceiveService">
    - <wsdl:port name="GpsReceiveServiceHttpSoap11Endpoint" binding="ns:GpsReceiveServiceSoap11Binding">
        <soap:address location="http://127.0.0.1:8080/axis2/services/GpsReceiveService.GpsReceiveServiceHtt
      </wsdl:port>
```

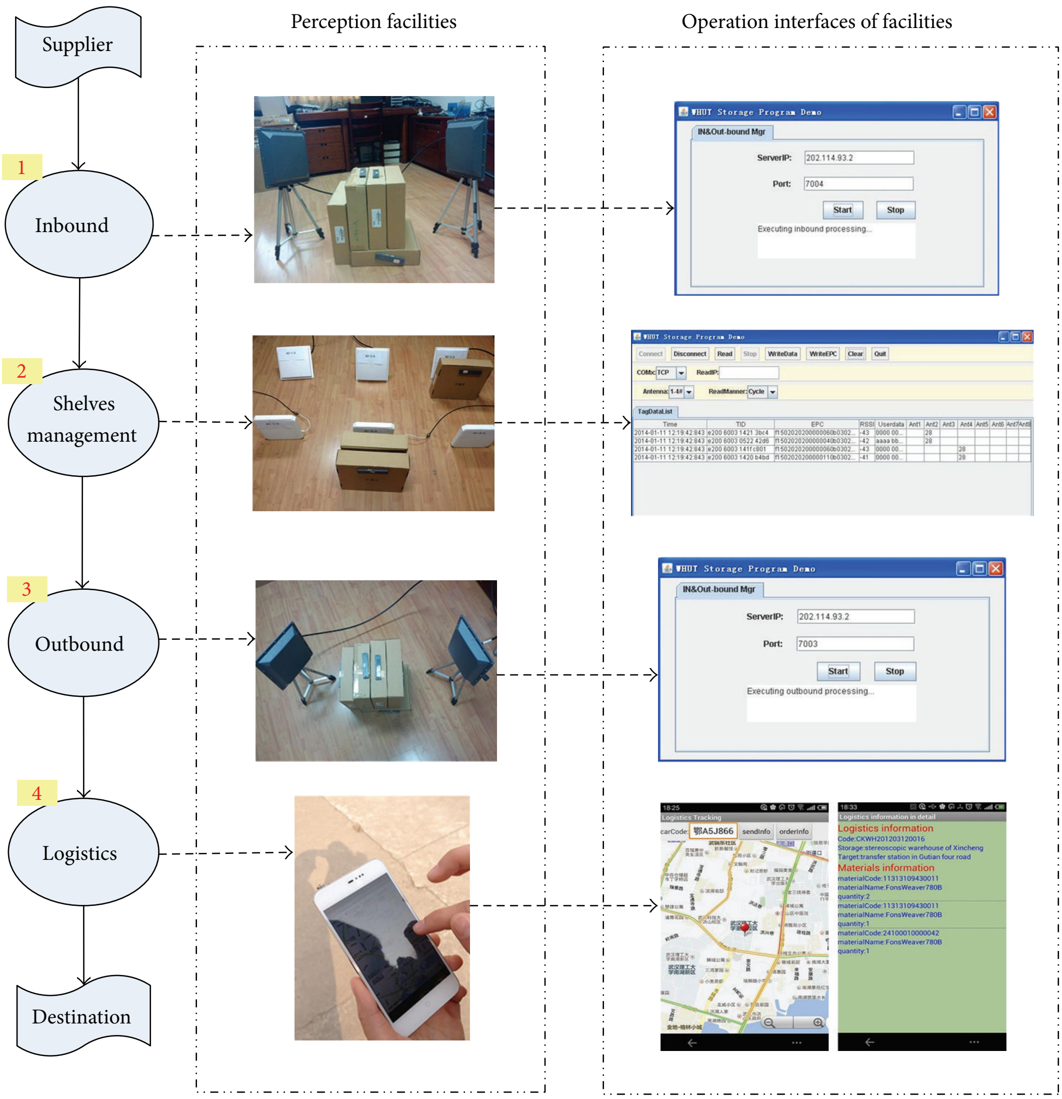
Figure 14: Service description with WSDL.

sensing and actuation resources are not only discovered, but also provided and aggregated as a service. According to the services provided by the warehouse management module, the warehouse keeper can adjust the warehouses for cargoes from suppliers. In the warehouse, distributed sensors and intelligent devices can be encapsulated into services for warehouse management. In order to select the best way for logistics, the manager will use the best logistics services provided by the devices located in the vehicles. When the cargoes arrive at the destination, the clients accept the cargoes with smart device which can provide accepting state service.

5.2. Prototype System Implementation

5.2.1. Process Condition Perception. The process condition perception subsystem in the supply chain integration and management is presented in Figure 8. In the subsystem, there are three condition perception modules, including the RFID tags and readers, the GPS module, and the temperature and humidity sensors. Before entering the warehouse, the packing boxes with two-dimension codes provided by the suppliers, which contain the information of supplier, name, count, and so forth, will be labeled with RFID tags. The RFID readers, fixed on the shelves, scan the RFID tags periodically to acquire the goods information automatically. The tags pasted on the boxes are the typical EPC GEN2 UHF passive RFID tags and the RFID reader is Speedway R420, and the reader can connect 32 antennas through an antenna hub. In the process of transportation, the GPS device, which consists of a GPS chip and the GPRS module, is used to locate the goods and transmit the position information in time. As the popularity of mobile phones, which integrates GPS and GPRS modules, we developed a software program based on android system for goods tracking. This subsystem shows the feasibility of our architecture and its hardware realization.

5.2.2. Network Access Convergence. The network access convergence subsystem is deployed in the warehouse to gather and transmit the information collected by the condition perception subsystem. As shown in Figure 9, the Zigbee network used in the warehouse environment can be divided into three parts, including the Zigbee coordinator, Zigbee routers, and sink nodes. Firstly, a Zigbee coordinator establishes the core network, and then four routers join the Zigbee network. Several sink nodes with RFID devices or other sensors can join the network with a plug-and-play way. The sink node with RFID device is deployed on the shelves to monitor quantity and position of goods. Environment information collected by the sensors will be transmitted from sink node to the routers. The warehouse server acts as a gateway, which cannot only access the Zigbee network by a sink node, but also retrieve and transfer the collected information using Internet.



ServerIP: 202.114.93.2

Port: 7004

Executing inbound processing...

COMx: TCP ReadIP:

Antenna: 1-4# ReadManner: Cycle

Time	TID	EPC	RSSI	Userdata	Ant1	Ant2	Ant3	Ant4	Ant5	Ant6	Ant7	Ant8
2014-01-11 12:19:42:843	e200 6003 1421 3bc4	f150202020000000060b0302...	-43	0000 00...		28						
2014-01-11 12:19:42:843	e200 6003 0522 42d6	f150202020000000040b0302...	-42	aaaa bb...		28						
2014-01-11 12:19:42:843	e200 6003 141f c801	f150202020000000060b0302...	-43	0000 00...				28				
2014-01-11 12:19:42:843	e200 6003 1420 b4bd	f150202020000000110b0302...	-41	0000 00...				28				

ServerIP: 202.114.93.2

Port: 7003

Executing outbound processing...

carCode: 鄂A5J866

Logistics information

Code:CKWH201203120016

Storage:stereoscopic warehouse of Xincheng

Target:transfer station in Gutian four road

Materials information

materialCode:11313109430011
materialName:FonsWeaver780B
quantity:2

materialCode:11313109430011
materialName:FonsWeaver780B
quantity:1

materialCode:24100010000042
materialName:FonsWeaver780B
quantity:1

Figure 15: CoT-based system test process.

5.2.3. Supply Chain Service Management Platform. The supply chain service management platform, which uses the B/S structure, is the user-oriented interface of the system. The manager is able to acquire each link real-time status of supply chain process, so as to adjust the management strategies in time. Then the functionality of the supply chain service management platform, which includes supplier management, inbound management, shelves management, outbound management, storage management, and logistics tracking, will be presented individually. Figure 10 illustrates the process of inbound management, which contains three parts including the basic information of invoice, materials list, and actual materials data collected by the RFID devices. The inbound result will be displayed automatically in the web instead of making the comparison manually. After being inbound, the storekeeper sorts the goods into the shelves, selected by the shelves management interface, as shown in Figure 11, which not only help choose shelves, but also display the basic information of goods on shelves in real-time. For the logistics management, as shown in Figure 12, the invoices can be traced and the detailed information of invoices, such as the location, destination, and vehicle number, can be displayed on the web.

In the CoT environment, the supply chain resources are virtualised and encapsulated into cloud services. We focus on the warehouse resources and logistics resources in the supply chain integration and management. The service list of the developed system is depicted in Figure 13. Moreover, as shown in Figure 14, each web service is described with web service description language (WSDL), which contains name, operation, types of parameters, and so forth. After encapsulating the services and generating WSDL files, the tomcat container is used to release the services online.

5.3. Field Trail and Evaluation of System. The prototype system based on the CoT architecture is implemented and tested in the laboratory environment. In order to test the performance of the proposed system, such as real-time, integration of subsystems, and information sharing, the system is deployed in an evaluation environment. Firstly, we deploy the RFID devices in the front of entrance and exit and fix the environment sensors with the Zigbee modules on the board and then install the goods tracking program on the mobile phone. Secondly, the management platform is deployed in the server. Finally, the system is initiated by setting up the server and connecting the distributed RFID devices by wire mode and environment sensors using Zigbee coordinator. The facilities used in the testing are listed in Table 1. Following the test process shown in Figure 15, the CoT-based prototype system, from the warehouse management to the delivery of materials to destination, is evaluated. For a comparison, the original system using barcodes to manage goods is measured in terms of the evaluation time. The test results are summarized in Table 2 by comparing the operation time between the CoT-based system and the original one. From the test results, an obvious improvement has been done in each stage of supply chain management in terms of execution time. Furthermore, the system provides a set of other benefits, such as the availability of goods status in each stage of supply chain and the flexibility of the system with services.

6. Conclusion

Highly distributed warehouses and heterogeneous resources located in each link of supply chains may increase the complexity of supply chain integration and management, especially in information sharing and collaboration as well as operation agility. The paper developed an intelligent integrated supply chain integration and management system based on CoT. The developed system is able to facilitate the users managing each link of the supply chain through the real-time collected and analyzed condition information from the subsystems of intelligent perception and network access convergence. The supply chain service management platform can list the services for users inquiring and invoking, and it provides the relevant services by virtualising the resources in warehouse and logistics, such as environment monitoring service and cargoes tracking service. Moreover, a case study with the implementation of the developed system demonstrates that it is an effective approach for supply chain integration and also provides the intelligence support for the physical resource management in the form of services. In the future, further research should be done for improving the performance of real-time, robustness, and security of such system.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research is supported by National Natural Science Foundation of China (Grant no. 51305319), the Keygrant Project of Chinese Ministry of Education (Grant no. 313042), the Wuhan International Scientific and Technological Cooperation Project (Grant no. 2013030409020112), and the Project of Joint Mobile Communication Lab of Wuhan University of Technology and China Mobile Group Hubei Co. Ltd. We are grateful to the postgraduate students Xiaojie Liu, Duzhong Zhang, Xiaolin Sun, Yingying Hu, Sisi Tian, and Shilong Zhang in the lab for their kind help in this work.

References

[1] J. C. P. Cheng, K. H. Law, H. Bjornsson, A. Jones, and R. Sriram, "A service oriented framework for construction supply chain integration," *Automation in Construction*, vol. 19, no. 2, pp. 245–260, 2010.

[2] K. C. Tan, "A framework of supply chain management literature," *European Journal of Purchasing & Supply Management*, vol. 7, no. 1, pp. 39–48, 2001.

[3] D. P. van Donk and T. van der Vaart, "A case of shared resources, uncertainty and supply chain integration in the process industry," *International Journal of Production Economics*, vol. 96, no. 1, pp. 97–108, 2005.

[4] D. Power, "Supply chain management integration and implementation: a literature review," *Supply Chain Management*, vol. 10, no. 4, pp. 252–263, 2005.

[5] H. L. Lee and S. Whang, "Information sharing in a supply chain," *International Journal of Technology Management*, vol. 1, no. 1, pp. 79–93, 2000.

[6] C. F. Cheung, C. M. Cheung, and S. K. Kwok, "A knowledge-based customization system for supply chain integration," *Expert Systems with Applications*, vol. 39, no. 4, pp. 3906–3924, 2012.

[7] H. L. Lee, V. Padmanabhan, and S. Whang, "Information distortion in a supply chain: the bullwhip effect," *Management Science*, vol. 43, no. 4, pp. 546–558, 1997.

[8] H. L. Lee, V. Padmanabhan, and S. Whang, "The bullwhip effect in supply chains1," *Sloan Management Review*, vol. 38, no. 3, pp. 93–102, 1997.

[9] H. Sharifi and Z. Zhang, "Agile manufacturing in practice application of a methodology," *International Journal of Operations & Production Management*, vol. 21, no. 5-6, pp. 772–779, 2001.

[10] L.-G. Mattsson, "Reorganization of distribution in globalization of markets: the dynamic context of supply chain management," *Supply Chain Management*, vol. 8, no. 5, pp. 416–426, 2003.

[11] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[12] S. Distefano, G. Merlino, and A. Puliafito, "Enabling the cloud of things," in *Proceedings of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS '12)*, pp. 858–863, 2012.

[13] P. Parwekar, "From internet of things towards cloud of things," in *Proceedings of the 2nd International Conference on Computer and Communication Technology (ICCCT '11)*, pp. 329–333, 2011.

[14] L. Wang, G. von Laszewski, A. Younge et al., "Cloud computing: a perspective study," *New Generation Computing*, vol. 28, no. 2, pp. 137–146, 2010.

[15] M. Lindner, F. Galán, C. Chapman, S. Clayman, D. Henriksson, and E. Elmroth, "The cloud supply chain: a framework for information, monitoring, accounting and billing," in *Proceedings of the 2nd International ICST Conference on Cloud Computing (CloudComp '10)*, 2010.

[16] D. M. Lambert and M. C. Cooper, "Issues in supply chain management," *Industrial Marketing Management*, vol. 29, no. 1, pp. 65–83, 2000.

[17] A. Hunter, R. King, and B. Lowson, *Quick Response: Managing the Supply Chain to Meet Consumer Demand*, Wiley, 1999.

[18] A. Gunasekaran and E. W. T. Ngai, "Information systems in supply chain integration and management," *European Journal of Operational Research*, vol. 159, no. 2, pp. 269–295, 2004.

[19] M. Rudberg and J. Olhager, "Manufacturing networks and supply chains: an operations strategy perspective," *Omega*, vol. 31, no. 1, pp. 29–39, 2003.

[20] T.-H. Shin, S. Chin, S.-W. Yoon, and S.-W. Kwon, "A service-oriented integrated information framework for RFID/WSN-based intelligent construction supply chain management," *Automation in Construction*, vol. 20, no. 6, pp. 706–715, 2011.

[21] P. M. Swafford, S. Ghosh, and N. Murthy, "Achieving supply chain agility through IT integration and flexibility," *International Journal of Production Economics*, vol. 116, no. 2, pp. 288–297, 2008.

[22] M. Themistocleous, Z. Irani, and P. E. D. Love, "Evaluating the integration of supply chain information systems: a case study," *European Journal of Operational Research*, vol. 159, no. 2, pp. 393–405, 2004.

[23] D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[24] S. M. Youssef and R. M. Salem, "Automated barcode recognition for smart identification and inspection automation," *Expert Systems with Applications*, vol. 33, no. 4, pp. 968–977, 2007.

[25] T. Sriram, V. K. Rao, S. Biswas, and B. Ahmed, "Applications of barcode technology in automated storage and retrieval systems," in *Proceedings of the IEEE IECON 22nd International Conference on Industrial Electronics, Control, and Instrumentation*, pp. 641–646, 1996.

[26] R. Angeles, "RFID technologies: supply-chain applications and implementation issues," *Information Systems Management*, vol. 22, no. 1, pp. 51–65, 2005.

[27] M. Attaran, "RFID: an enabler of supply chain operations," *Supply Chain Management*, vol. 12, no. 4, pp. 249–257, 2007.

[28] T. Kelepouris, K. Pramatari, and G. Doukidis, "RFID-enabled traceability in the food supply chain," *Industrial Management & Data Systems*, vol. 107, no. 2, pp. 183–200, 2007.

[29] M. K. Lim, W. Bahr, and S. Leung, "RFID in the warehouse: a literature analysis (1995–2010) of its applications, benefits, challenges and future trends," *International Journal of Production Economics*, vol. 145, no. 1, pp. 409–430, 2013.

[30] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[31] L. Ruiz-Garcia, P. Barreiro, and J. I. Robla, "Performance of Zigbee-based wireless sensor nodes for real-time monitoring of fruit logistics," *Journal of Food Engineering*, vol. 87, no. 3, pp. 405–415, 2008.

[32] H. Yang, L. Yang, and S.-H. Yang, "Hybrid Zigbee RFID sensor network for humanitarian logistics centre management," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 938–948, 2011.

[33] M. Armbrust, A. Fox, R. Griffith et al., "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[34] G. Pallis, "Cloud computing: the new frontier of internet computing," *IEEE Internet Computing*, vol. 14, no. 5, pp. 70–73, 2010.

[35] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," in *Proceedings of the 5th International Joint Conference on International Conference on Networked Computing, International Conference on Advanced Information Management and Service, and International Conference on Digital Content, Multimedia Technology and Its Applications (NCM '09)*, pp. 44–51, 2009.

[36] B.-H. Li, L. Zhang, S.-L. Wang et al., "Cloud manufacturing: a new service-oriented networked manufacturing model," *Computer Integrated Manufacturing Systems*, vol. 16, no. 1, pp. 1–7, 2010.

[37] B.-H. Li, L. Zhang, L. Ren et al., "Further discussion on cloud manufacturing," *Computer Integrated Manufacturing Systems*, vol. 17, no. 3, pp. 449–457, 2011.

[38] F. Tao, L. Zhang, V. C. Venkatesh, Y. Luo, and Y. Cheng, "Cloud manufacturing: a computing and service-oriented manufacturing model," *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, vol. 225, no. 10, pp. 1969–1976, 2011.

[39] X. Xu, "From cloud computing to cloud manufacturing," *Robotics and Computer-Integrated Manufacturing*, vol. 28, no. 1, pp. 75–86, 2012.

[40] W. Li, Ye Zhong, X. Wang, and Y. Cao, "Resource virtualization and service selection in cloud logistics," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1696–1704, 2013.

[41] J. Manyika, M. Chui, B. Brown et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, 2011.

[42] A. Jacobs, "The pathologies of big data," *Communications of the ACM*, vol. 52, no. 8, pp. 36–44, 2009.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 247173, 12 pages
http://dx.doi.org/10.1155/2014/247173

Research Article

Service-Oriented Node Scheduling Schemes with Energy Efficiency in Wireless Sensor Networks

Hongju Cheng,[1] Ronglie Guo,[1] Zhihuang Su,[1] Naixue Xiong,[2] and Wenzhong Guo[1]

[1] *College of Mathematics and Computer Science, Fuzhou University, Fuzhou, Fujian 350108, China*
[2] *Department of Computer Science, Georgia State University, Atlanta, GA 30303, USA*

Correspondence should be addressed to Hongju Cheng; cscheng@fzu.edu.cn

Received 29 October 2013; Revised 1 January 2014; Accepted 1 January 2014; Published 20 February 2014

Academic Editor: Jong Hyuk Park

The wireless sensor network is expected to provide various data sensing services by employing the advantage of dense deployment. Energy efficiency is an important criterion for many applications since the sensor nodes are generally budgeted by limited battery. In this paper, we are concerned with the node scheduling problem to provide the required services for the service-oriented wireless sensor network. We firstly propose an Energy-aware Centralized Heuristic Scheme (ECHS) for the problem in which an energy-aware benefit function is used to determine active sensor nodes and rotate sensor nodes by periodically reconstructing the scheduling scheme. We also present an Energy-aware Distributed Heuristic Scheme (EDHS) as the distributed version. Extensive simulation is performed to evaluate the proposed schemes, and the results show that the two schemes have better performance compared with related works.

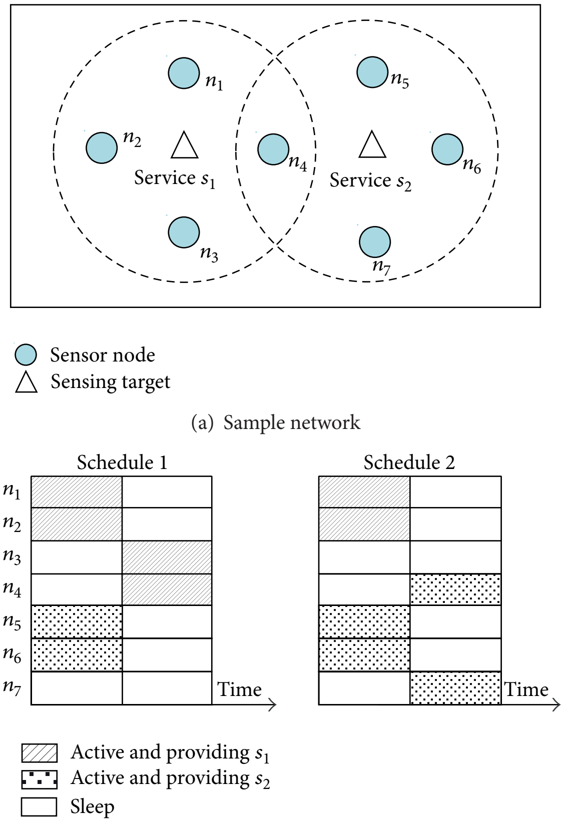
1. Introduction

Wireless sensor network (WSN) [1] is emerging as an important technology, which includes hundreds or thousands of self-organized sensor nodes connected by wireless communications. These sensor nodes are generally designed with lower-energy units and their cheapness and self-organization characteristics make it possible to deploy the network in various applications, such as environment data collection, industrial process monitoring and control, and machine health monitoring. The rapid development and deployment of sensor technology involve many new type sensors that are equipped with different sensing components. One important trend for the sensor networks is to provide various services to users, and *service-oriented wireless sensor network* has been proposed as an important solution for the future of sensor networks [2–7]. It can be seen that the current wireless sensor networks are generally data centric or application centric which leads to many obvious disadvantages, such as lacking both uniform operations and a standard representation for sensor data that can be used by diverse sensor applications [4]. The service-oriented wireless sensor networks can support different applications in more general and flexible way, which helps to improve the network performance and also leads to some other advantages, for example, the resource sharing among applications and efficient collection of the information generated by heterogeneous sensor nodes. However, *service* is not a pure new term and it may be a task of data sensing [8, 9] or a software component provided by sensors [10]. In case the task of data sensing is considered as service, different services provided by the network are helpful to gather different types of sensed data in the monitored area, such as temperature, humidity, sound, or motion. To provide all these different services is one challenge issue for the future service-oriented wireless sensor networks.

In general, a lot of redundancy and correlation occur among the sensed data especially in wireless sensor networks due to the following observations. Firstly, the network is intended to deploy in dense way so that the node failure and other faults can be tolerant to support the network to work in proper way. Secondly, the sensed data depends on the location of nodes as well as the event source. The data of adjacent nodes is generally correlated since they observe the same physical phenomena in the same geographic region [11–13]. Obviously, it is not efficient to wake up all nodes in the network to collect data and provide services since it leads to unnecessary energy consumption due to the data redundancy among neighbor nodes. It means that the sensor nodes should be organized in one more efficient way to enlarge the network lifetime while the required services are guaranteed. It leads to the problem of scheduling large numbers of sensor nodes in an energy-efficient way to support various services in the service-oriented wireless sensor networks.

In order to conserve energy resources and extend network lifetime, one important idea is to schedule the nodes in the network. The scheduling techniques generally select a group of nodes in each epoch, and the selected nodes work in active mode to provide the required services, while other nodes are kept in sleep mode in order to reduce energy consumption since that the sleep mode consumes only a small fraction of energy compared to the active mode [14, 15]. The scheduling problems in wireless sensor network are widely investigated in the literature recently [16–19], but most of them focus on fully different research issues, such as target tracking, coverage, topology control.

However, the node scheduling problem in the service-oriented sensor networks is not only to select a set of nodes to provide the required services during each epoch but also to choose the service each active node should provide. Furthermore, different services in the sensor network have different metrics in the applications, such as different importance (profit) of the applications and different amount of resources (requirement) required in providing the service [20–22]. How to measure the importance of these different services is one challenge issue in the network. Since the sensor is generally budgeted by limited battery, and the network lifetime is the most important criterion for the wireless sensor networks, we introduce the *profit* to describe the benefit received from one service when it is provided by the network. Generally, the service is more preferred in case that its profit is larger than others in the network since it is helpful to improve the network performance.



(a) Sample network

(b) Two scheduling schemes

Figure 1: An example to demonstrate the node scheduling problem in service-oriented wireless sensor networks.

Figure 1 shows an example including seven sensor nodes supporting two different services. In Figure 1(a), the circle represents sensor node, the triangle denotes sensing target (we assume that each sensing target is combined with one different service), and the dotted line indicates that nodes within the event area are available to support corresponding service. In this example, service s_1 is supported by nodes n_1, n_2, n_3, and n_4, and s_2 is supported by nodes n_4, n_5, n_6, and n_7. Assume that the selected number of nodes is at least two for each service. Obviously, there are several ways to schedule nodes to provide the required services, and Figure 1(b) shows two of them. The major difference between them is the second epoch in which the first scheduling selects $\{n_3, n_4\}$ to provide s_1, while the second scheduling selects $\{n_4, n_7\}$ to provide s_2. As shown in Figure 1(a), the network can only support one service in the next epoch due to the lack of resources if we use the above two scheduling schemes. However, in case that service s_1 is more crucial than service s_2 (i.e., service profit of s_1 is larger than s_2), scheduling 1 is preferred compared with scheduling 2 because it can obtain more profit for the network.

In this paper, we study the energy-efficient node scheduling problem in service-oriented wireless sensor networks by adopting profit to measure the network performance, and aim at maximizing the total profit during the network lifetime. Since this problem is proven to be NP-hard [20, 21], we propose two heuristic schemes with energy efficiency. The main contributions of this paper are summarized as follows. (1) We have proposed an Energy-aware Centralized Heuristic Scheme (ECHS) in which an energy-aware benefit function is used to determine the state of nodes as well as the corresponding services provided by each active node. The function takes into account both the capabilities of providing services and the residual energy of nodes, which is helpful to improve the network performance as demonstrated in the simulation results. (2) We have designed a distributed solution for this problem, namely, Energy-aware Distributed Heuristic Scheme (EDHS), in which one header is assigned to each service and the scheduling scheme is carried out in a distributed way that only local information is necessary for the active node selection process.

The rest of this paper is organized as follows. In Section 2, we present the related works. Section 3 introduces the network model and the problem formulation. In Sections 4 and 5, we introduce the centralized and distributed node scheduling schemes, respectively. Section 6 provides performance comparison by detailed simulation. And Section 7 is the conclusion.

2. Related Works

Recently, the service-oriented wireless sensor networks appear as a new emerging trend for the future of wireless sensor networks, which are generally considered as a service provider. It leads to the idea of service-oriented wireless sensor networks [2, 3]. Gračanin et al. [2] proposed a service-centric model, which provides a general and flexible framework for wireless sensor networks. This model consists of mission, network, region, sensor, and capability layers. Within each layer, there are four planes or functionality sets: communication, management, application, and generational learning. Rezgui and Eltoweissy [3] introduced service-oriented sensor-actuator networks as an approach for building a new generation of open, efficient, interoperable, scalable, and application-aware sensor-actuator networks. In this approach, sensor-actuator networks would providing sensing and actuation services to any application, rather than provide sensing and actuation capabilities to a specific application.

Some researchers focused on building the platform/middleware to provide various services in the wireless sensor networks. Mohamed and Al-Jaroodi [5] surveyed the challenges and requirements of service-oriented middleware for wireless sensor network and reviewed some representative approaches. Familiar et al. [6] presented a service-oriented middleware that implements an agent-based virtual sensor service abstraction in ubiquitous smart environments. This middleware offers a lightweight service-oriented framework for sensor networks, with compact service exposure and dynamic virtual service composition through the use of semantic tags. In [7], a service-oriented architecture called TinySOA is proposed, which provides a high-level abstraction for the development of applications in wireless sensor networks. In addition, TinySOA allows application developers to access sensor networks from their applications using a simple service-oriented API via the programming language of their choice, which helps to relive application developers from dealing with the low-level technical details of the sensor networks. Zhang et al. [8] considered the sensor data as the service and designed an open community-oriented platform. The proposed platform allowed users to discover reusable data and data analysis tools and to integrate them into value-added workflows.

To provide various services satisfying the requirement of client applications is an important design goal in the service-oriented sensor networks, and several works have been done to achieve the efficiency of supporting services. Cheng et al. [9] investigated the node selection problem with data accuracy guarantee in service-oriented wireless sensor networks by exploiting the spatial correlation between the service data. However, the proposed algorithms select active sensor nodes without considering energy efficiency that may lead to shorter network lifetime. Geyik et al. [23] proposed a graph-based model for describing sensor services and formulated the process of dynamic sensor service composition as a cost-optimization problem that is shown to be NP-complete. The objective of this problem is to minimize the total cost of the component services that are selected for the composition. Besides, they designed two heuristic algorithms for service composition problem that differ in the direction of traversing the service graph during the composition process. Wang et al. [10] introduced the service-availability-aware sleep scheduling, which aimed to minimize the energy consumption, and guaranteed that there are enough active sensors providing each required service in the system at any time. They considered the wake-up energy consumption and developed approximation algorithms based on LP relaxation. However, they assumed that each service needs fixed number of nodes in order to process the service in the system. In fact, sensor nodes might have different capacities in providing services due to the fact that they have different distances to the monitored target.

Node scheduling is an efficient way to prolong the network lifetime with respect to a network with nodes always on [14]. Under different application backgrounds and assumptions, researchers have proposed many schemes to determine how many and which nodes should be put into sleep mode. Zhao et al. [16] presented a sleep-scheduling technique called Virtual Backbone Scheduling (VBS), which forms multiple overlapped backbones that work alternatively. The rotation of multiple backbones helps to balance the energy consumption of all sensor nodes, which fully utilizes the energy and prolongs the network lifetime. Lin et al. [17] explored the node scheduling scheme for target tracking. Their scheme selects multiple sensors to track target collaboratively such that it achieves better tracking accuracy and reliability with respect to single-sensor-based schemes. Zorbas et al. [18] proposed a cover sets-based node scheduling technique for solving coverage problem, which adopts the strategy that produces both disjoint cover sets, that is, cover sets with no common sensor nodes, and nondisjoint cover sets. In [19], the minimum energy broadcast problem was formulated as the problem of finding the minimum Connected Dominating Set (CDS), and a Minimum Energy-consumption Broadcast scheme (MEBS) was proposed that aimed at providing an efficient scheduling scheme with maximized network lifetime.

Node scheduling in service-oriented wireless sensor network should determine the states of sensor nodes, that is, sleep or active, and the service should provide when a sensor node is in active state. In [20], sensor-mission (service) assignment problem was investigated with the objective of maximizing the achieved profit, which was shown to be NP-hard. In this problem, the profit is a property of services indicating their importance as well as the reward for their execution. They modeled this problem as a weighted bipartite graph whose vertex sets consist of sensors and services and discussed some of its variants. Furthermore, they proposed a centralized Greedy algorithm and a distributed Energy-aware Dynamic Proposal Algorithm (EDPA). The Greedy algorithm repeatedly attempted the highest-potential-profit untried service that can be satisfied with the greatest profit using the currently available sensors. The EDPA algorithm uses information about the current energy level of sensors to make better decisions, which helps to improve the network lifetime. Furthermore, the EDPA algorithm adopts the strategy that sensor nodes are allowed to be stolen by other services, while it may lead to a large amount of messages exchange. Johnson et al. [21] extended the work of [20], and proposed a multiround proposal algorithm called MRGAP, which treats the services as knapsacks that together form an instance of the Generalized Assignment Problem (GAP). Moreover, Porta et al. [22] extended the work of [20, 21] into the environment that sensor nodes equipped with energy harvesting components. The proposed scheduling algorithm exploits not only the nodal residual energy, but also takes into account the energy that is expected to be harvested in the future, which can ensure that the required energy of sensor nodes is always available regardless of the fact that its source is battery or harvesting. However, their solution assumed that the distribution of services' profit and requirement is known a priori, which may not be the case in practice. Recently, Cho et al. [24] proposed a multiple dynamic mission (service) assignment problem for tactical mobile ad hoc networks. The proposed solution is based on combinatorial auction theory, which can minimize communication overhead while maximizing node utilization and mission completion ratio. In this paper, we aim at the node scheduling problem with energy efficiency in the service-oriented wireless sensor networks. We present two heuristic node scheduling schemes that exploit redundancy among sensed data to conserve energy while preserving the availability of required services.

3. System Model and Problem Formulation

In this section, we first introduce the system model as well as the definition of network lifetime and then formulate the node scheduling problem in the service-oriented wireless sensor networks. To be convenient, the symbols used in this work are summarized in Abbreviations Section.

3.1. System Model. We consider a wireless sensor network in the plane consisting of a set of nodes $N = \{n_1, n_2, \ldots, n_n\}$. Suppose that every node has limited sensing range R_s and communication range R_c. The initial energy of each node is denoted as E. Then, the senor network can be described as an undirected graph $G = (N, L)$, where N denotes the set of nodes and L denotes the set of links. There is a link (n_i, n_j) in case that nodes n_i and n_j are within the transmission range of each other. We also assume that all nodes are stationary and each node knows its geographic location [25, 26].

The service in the wireless sensor network is considered as a sensing task for a specific target located as a stationary position, and all the services provided in the network is notated as $S = \{s_1, s_2, \ldots, s_m\}$. In this paper, we use a triple (l_j, d_j, p_j) to describe the property for a given service s_j, where l_j is the geographic location of the sensing target in the field, d_j is the service requirement which indicates the amount of sensing resources it needs, and p_j is the profit of the service which indicates both its importance and the reward achieved by the network for its execution. Generally, these services are fully separate and we assume there is no correlation relationship among them in this paper.

For a given sensing task located at a given position, the corresponding service is generally provided by several nodes. Each node whose sensing range covers the task position has contribution to the service, and here we denote the effect of node n_i to provide service s_j as $e_{i,j}$. Generally, we have $e_{i,j} = 0$ in case that node n_i cannot provide service s_j or service s_j is located outside of the sensing range of n_i. We also assume that the value $e_{i,j}$ for service s_j is additive [21]. It shall be mentioned that the value of $e_{i,j}$ depends on the practical scenario and the sensing object and is generally considered as one preknown parameter for the node scheduling problem. However, there are several models that can be used to formulate this parameter. For example, the distance-based model is proposed in [20–22], which can be described as

$$e_{i,j} = \begin{cases} \dfrac{1}{1 + D_{i,j}^2 / c}, & \text{if } D_{i,j} \leq R_s, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

where $D_{i,j}$ is the Euclidean distance between node n_i and the sensing target of service s_j and c is the decay factor. This model follows typical signal attenuation models in which signal strength decays inversely with distance squared.

In the practical application, some nodes might be deployed in an area far away from the sensing task and they cannot provide the required services due to the limited sensing range. In this case, the effect for this given service is zero. However, such nodes can be used to forward the collected data to the sink since the sensor networks always run in ad hoc model. On the other hand, one node is feasible to provide a given service only in case that the service is located in the sensing range.

3.2. Network Lifetime. The network lifetime is one of the most important metrics for the wireless sensor networks, and there are various measurements for network lifetime, such as the first node to die, the number of alive nodes, and the fraction of alive nodes [27, 28]. In this paper, we focus on the problem of how to schedule nodes in an efficient way to provide required services. Due to the fact that the sensor network is generally densely deployed, the network can still keep on providing required services although the first node is already dead since there is data redundancy among the adjacent nodes. Let $\mathrm{AN}(t)$ be the number of nodes that are alive and also available to provide services at time slot t, and the network lifetime TL is defined as follows in this paper:

$$\mathrm{TL} = \max \{t : \mathrm{AN}(t) \geq \tau \mathrm{AN}(0)\}, \tag{2}$$

where τ denotes a given alive nodes threshold. It is obvious that the network lifetime indicates the time-period during which the wireless sensor network can keep on providing the required services.

3.3. Problem Formulation. The problem studied in this paper is to find a schedule for each node so that the required services in the sensor network can be guaranteed. In some special case, it might be impossible to satisfy all the constraints required by all services in the network due to the lack of resources. Then the network intends to provide the service with higher importance, which is generally described as the profit of the service. Meanwhile, the network has better performance when it supports more services during its lifetime. In this way, we aim at maximizing the total profit during the network lifetime for the node scheduling problem.

The total network profit is calculated as the sum of the profits achieved over all time slots during the network lifetime. Let $x_{i,j,t}$ be a binary variables (0 or 1), where $x_{i,j,t}$ is 1 if and only if node n_i is active and assigned to provide s_j at time slot t, and $\{x_{i,j,t}\}$ indicates one scheduling scheme for the given wireless sensor network at time slot t. In some cases, the services are still tolerant with acceptable quality even though the required resources are partly satisfied. Based on the above observation, we adopt a simple model to describe the profit obtained during the service providing process. Let $y_{j,t}$ denote the stratification level of service requirement at time slot t, the profit $p_j(y_{j,t})$ which is obtained by providing service s_j at time slot t can be formulated as follows [20, 21]:

$$p_j\left(y_{j,t}\right) = \begin{cases} p_j, & \text{if } y_{j,t} \geq 1, \\ p_j \cdot y_{j,t}, & \text{if } T_{\text{sat}} \leq y_{j,t} < 1, \\ 0, & \text{if } y_{j,t} < T_{\text{sat}}, \end{cases} \tag{3}$$

where $y_{j,t} = \sum_{i=1}^{n} x_{i,j,t} e_{i,j} / d_j$.

Given a set of nodes $N = \{n_1, n_2, \ldots, n_n\}$, a set of services $S = \{s_1, s_2, \ldots, s_m\}$, the requirement d_j and profit p_j for each service $s_j \in S$, and the service effect $e_{i,j}$ for each node $n_i \in N$ and each service $s_j \in S$, the node scheduling problem for the service-oriented wireless sensor network is to find a set of scheduling schemes $\{x_{i,j,1}\}, \{x_{i,j,2}\}, \ldots, \{x_{i,j,\text{TL}}\}$, so that the total achieved profit of the network, that is, $\sum_{t=1}^{\text{TL}} \sum_{j=1}^{m} p_j(y_{j,t})$ is maximized.

The node scheduling problem studied in this paper has been proven to be NP-hard [20, 21], which means that it is impossible to find optimal solution in polynomial time. In this work, we develop two heuristic schemes to obtain suboptimal solution, namely, energy-aware centralized heuristic scheme (ECHS) and energy-aware distributed heuristic scheme (EDHS).

4. Centralized Scheme

The basic idea for the proposed Energy-aware Centralized Heuristic Scheme (ECHS) can be described as follows. (1) Use a novel heuristic approach to construct a scheduling scheme based on the concept of energy-aware benefit function and a greedy strategy aiming at minimizing the number of selected nodes. (2) Secondarily, reconstruct the scheduling scheme after the time expires by replacing the selected nodes that have low level of residual energy with the unselected nodes that have high level of residual energy. The second process continues until the fraction of alive nodes is below a given threshold τ, and finally the network ends.

In this section, we first introduce the novel energy-aware benefit function and then describe the procedure of initial scheduling construction and the swapping procedure, respectively; finally, we describe the detailed process of the proposed ECHS.

4.1. Energy-Aware Benefit Function. Here we introduce a novel energy-aware benefit function that is used as metric to sort nodes during the node selection process. We consider three important factors for the benefit function, that is, the node's service effect for a service, the remaining requirement of a service, and the node's residual energy. Let u_j be the sum of the selected nodes' service effect for service s_j. Then, the remaining requirement of service s_j can be described as $(d_j - u_j)$. The nodes with larger service effect and higher level of residual energy are preferred to be selected so that the number of required nodes can be minimized. Meanwhile, the part of service effect that exceeds the requirement is generally neglected since the solution only needs to satisfy the requirement. In this way, the benefit function is formulated as follows:

$$f\left(e_{i,j}, \text{RE}_i\right) = \frac{\min\left(e_{i,j}, d_j - u_j\right)}{d_j} \cdot \left(\frac{\text{RE}_i}{E}\right)^{\beta}, \tag{4}$$

where RE_i denotes the current residual energy of node n_i and β ($\beta \geq 0$) is a given parameter. Note that β represents the trade-off between the service effect and the residual energy, and the scheme intends to select nodes with larger residual energy rather than better service effect in case that the value of β is larger.

4.2. Initial Scheduling Construction. The basic idea of the initial scheduling construction is that we select a minimum number of nodes for each required service in a separate way, and the union of selected nodes for all services is considered as a scheduling scheme. Note that all the selected nodes will switch into active state to provide corresponding service when scheduling process has been finished. We prefer to select nodes for services that have more profit but fewer requirements for resources so that the network can achieve larger profit with less number of active nodes. Thus, we firstly sort services and then select nodes for services with the above energy-aware benefit function in the sequence. The selection process for each service terminates if the service requirement is satisfied or no more nodes can be found.

There are two different states for the nodes during the scheduling construction process, *UNSELECTED* and *SELECTED*. Nodes in the *SELECTED* state are scheduled to provide the required service, and nodes in *UNSLECTED* are candidates, which are possible to change to *SELECTED* in the next time slot. Here, we introduce a new notation, $B_{i,j}$, to denote the profit contribution of node n_i for providing service s_j, where $B_{i,j} = e_{i,j} \cdot p_j / d_j$. It is obvious that node n_i contributes more profit to the network if the assigned service s_j has larger $B_{i,j}$. Consequently, we determine node $n_i \in N$ as a candidate node for service s_j in case that n_i is *UNSELECTED*

```
Input: $N$, $S$, $d_j$ and $p_j$ for each $s_j \in S$, $e_{i,j}$ for each $n_i \in N$ and $s_j \in S$, and $T_{\text{sat}}$.
Output: A scheduling scheme.
Initialize all nodes as UNSELECTED;
$S' \leftarrow S$;
while $S' \neq \emptyset$
    Search candidate nodes for each service $s_j \in S'$, and calculate the maximum achieved
    profit $p_{\max}(j)$ that $s_j$ is provided by all candidate nodes;
    Select the one $s_j$ from $S'$ with maximum $p_{\max}(j)/d_j$;
    Select nodes for $s_j$ from candidate nodes in decreasing order of $f(e_{i,j}, \text{RE}_i)$
    until the requirement of $s_j$ is satisfied, and neglect the node which is SELECTED
    and the reassignment  will cause previously assigned service failed;
    set these selected nodes as SELECTED;
    Search redundant nodes, and set them as UNSELECTED;
    If the satisfaction level of $s_j$ is less than threshold $T_{\text{sat}}$, change the selected
    nodes for $s_j$ to UNSELECTED;
    $S' \leftarrow S - \{s_j\}$;
end while
```

Procedure 1: Initial scheduling construction.

and $e_{i,j} > 0$, or if n_i is selected by another service, for example, service s_k, and $B_{i,j} > B_{i,k}$. It means that the network profit might be increased by changing n_i to provide service s_j.

Redundancy might occur when the selected nodes have fully satisfied services' requirement because the node selection process considers both the service effect and the residual energy. For example, consider service s_1 with requirement $d_1 = 0.5$ and candidate nodes are assumed to be n_1, n_2, and n_3. Suppose that these nodes' service effect and fraction of residual energy are (0.3, 0.8), (0.1, 1.0) and (0.2, 0.4), respectively. We also assume that $\beta = 1$ in (4). It is seen that n_1, n_2, and n_3 will be selected simultaneously. However, the requirement of service s_1 can be guaranteed by n_1 and n_3, which means n_2 is a redundant node. The basic idea to eliminate these redundant nodes is described as follows. In case that a service, for example, s_j, is fully satisfied with its requirement for resources, we will firstly sort the selected nodes for service s_j in increasing order of service effect $e_{i,j}$, and then remove nodes from the selected nodes in sequence until the requirement d_j cannot be guaranteed by the rest nodes. The pseudocode for the initial scheduling construction is listed in Procedure 1.

4.3. Swapping Procedure. The objective of swapping is to balance the energy consumption of nodes selected in the previous initial scheduling construction procedure, which aims at finding enough nodes to provide services and match the requirements. In case those nodes with lower energy are selected to provide the services, these nodes will run to death, which finally results in other serious issues such as network partition and failure to provide the services. In this way, to balance the residual energy is one important way to extend the network lifetime.

In this section, we introduce a novel swapping procedure used to replace some low-energy *SELECTED* nodes with high-energy *UNSELECTED* nodes. A decrement of the network profit is helpful to find candidates for the selected nodes whose contribution to the network is rather small it is possible to provide more benefit services (i.e., services with larger value of $B_{i,j}$) in the subsequent times. In this paper, we adopt $(1-\text{RE}_i/E)\,(\max B_{i,j} - B_{i,k})$ as the maximum acceptable profit decrement when we perform swapping for selected node n_i that assigned to service s_k.

The pseudo-code for the swapping procedure is listed in Procedure 2. Firstly, calculate the average residual energy of all the selected nodes and denote it as E_{avg} (in Line 1). Secondarily, initialize node list *RList* with the selected nodes whose residual energy is less than E_{avg} and then sort *RList* in increasing order (in Lines 2-3); Finally, perform swapping operation for node in *RList* in sequence (in Lines 4–9). The swapping operation is done as follows. Given a node n_i that assigned to provide s_k, we firstly calculate the minimum acceptable level of achieved profit for s_k that indicates that the achieved profit is not less than it after swapping (in Line 6). Secondarily, searchs candidate nodes with residual energy larger than E_{avg} from these unselected nodes (in Line 7). Finally, check candidate nodes and select one to replace n_i, if no candidate node can be found and the network profit is still within acceptable level, n_i will be released (in Line 8).

4.4. Scheme Description. With the above description, the detailed ECHS is introduced as follows. The basic idea behind ECHS is that we reconstruct the scheduling scheme periodically or when it is necessary. Consider two special conditions that the scheduling scheme is rebuilt: (1) the scheduling scheme runs for $T_{\max}$ time slots; (2) some selected nodes are unable to provide services due to the fact that they run out of energy. The process of node scheduling will continue until the network ends; that is, $\text{AN}(t) < \tau\text{AN}(0)$. Algorithm 1 provides details of pseudo-code for ECHS.

```
Input: $N$, $S$, $d_j$ and $p_j$ for each $s_j \in S$, $e_{i,j}$ for each $n_i \in N$, and $s_j \in S$, $\tau$, $T_{\text{sat}}$, and $T_{\max}$.
Output: A scheduling scheme.
(1) Run Procedures 1 and 2 in sequence and get a scheduling scheme;
(2) Provide services under the scheduling scheme;
(3) Calculate the residual energy of nodes as well as $\text{AN}(t)$, if $\text{AN}(t) \geq \tau\ \text{AN}(0)$ is not satisfied, go to step 5;
(4) If the scheduling scheme has been used for $T_{\max}$ time slots or there exists active nodes
    with residual energy cannot support service in the scheduling scheme, go to step 1, otherwise go to step 2;
(5) The network ends.
```

Algorithm 1: Energy aware centralized heuristic scheme (ECHS).

```
Input: $N$, $S$, $d_j$ and $p_j$ for each $s_j \in S$, $e_{i,j}$ for each $n_i \in N$, and $s_j \in S$, $T_{\text{sat}}$, and a scheduling scheme.
Output: An improved scheduling scheme.
$E_{\text{avg}} \leftarrow$ average residual energy of all nodes in SELECTED state;
Initial node list RList with the nodes in SELECTED state and their residual energy is less than $E_{\text{avg}}$;
Sort RList in increasing order of residual energy;
for each node $n_i$ in RList
    $s_k \leftarrow$ the assigned service of $n_i$;
    Calculate acceptable level of profit for $s_k$;
    Search candidate nodes for $n_i$ from nodes in UNSELECTED state with residual energy
        larger than $E_{\text{avg}}$ and $e_{i,k} > 0$;
    Select one node as the replacement of $n_i$ from candidate nodes with the constraints that
        achieved profit of $s_k$ is within acceptable level and the satisfaction level of $s_k$
        is not less than threshold $T_{\text{sat}}$; if no such a replacement node is found, change $n_i$
        to UNSELECTED state in case that above constraints can be satisfied, otherwise swap
        the state of $n_i$ and its replacement node;
end for
```

Procedure 2: Swapping procedure.

5. Distributed Scheme

The centralized heuristic schemes are generally efficient to find a suboptimal solution and it can be carried out on one powerful node, that is, the sink, which supports a large amount of computation and heavy communication tasks. This centralized nature requires that the sink knows the global information of the network and results in better scheduling scheme. However, in the practical applications, it is usually difficult and costly to gather a large amount of information to the sink and disseminate schedules from the sink to all other nodes especially in networks deployed in large scale. Distributed scheduling is often performed by each node in the network that only local information necessary to determine whether one node is active or not. Thus, it is more practical to deploy distributed scheduling schemes in the wireless sensor networks.

The proposed EDHS assigns a specific node as the header for each service, and the header performs a local node scheduling to select node resources for the given service. The other nodes in the network are called normal node. The EDHS consists of three phases: the data collection phase, the node selection phase, and maintenance phase. In the data collection phase, nodes collect information of required services, and then the EDHS chooses initial header node for each service. In the node selection phase, the headers select active nodes to provide services. After schedules are constructed on nodes, the nodes begin to execute their schedules and provide required services. To rotate active nodes and balance the energy consumption among nodes, the nodes will reenter the node selection phase when necessary. The details of each phase are described in the following sections.

5.1. Data Collection Phase. In this phase, each node detects sensing targets within its sensing range and the node closest to a specific sensing target will be elected as an initial header node. Then, the sink node transmits service information including profit and requirement to the corresponding header node. After receiving the information, the header node also broadcasts the service information to its neighbors. In case that a normal node receives the service information, it checks whether it is available to provide this service and drops this message if not or this message is received already; otherwise the node sends the message to neighbors and stores the information of corresponding header node for this service. Then, each normal node transmits its service effect and residual energy to the corresponding header node. The header node maintains one node table, and each entry has the following fields: *node ID*, *service effect* and *residual energy*. The residual energy of each node defines the reluctance or willingness of that node to provide the service. Because current energy levels of nodes are accordingly changed with the running of the network, nodes periodically update the residual energy to the header nodes so that the header nodes can select suitable nodes to provide services. This message also can be delivered in a piggyback fashion during the service data gathering process.

5.2. Node Selection Phase. In this phase, the header node runs the local node selection scheme and selects a set of active nodes to provide services. The idea of local node selection scheme is similar to the proposed centralized scheme. The difference is that selection process is done with only local information.

The basic selection process for service s_j is described as follows. (1) Firstly, the header node orders the candidates to decrease of $f(e_{i,j}, \mathrm{RE}_i)$ and choose the nodes one by one until the requirement of s_j is satisfied or there is no available node. (2) Secondarily, remove the redundant nodes by using the idea described in Section 4.2. After the active nodes are selected, the header node sends *NOTIFICATION* messages including the information of service s_j and $\mathrm{dec}(i, j)$ to these selected nodes. Let N_j be the set of selected nodes for s_j, and let $p_j(N_j)$ be the achieved network profit when s_j is provided by N_j. For each $n_i \in N_j$, $\mathrm{dec}(i, j) = p_j(N_j) - p_j(N_j - \{n_i\})$ is the network profit decrement when n_i is removed from N_j. Clearly, $\mathrm{dec}(i, j)$ indicates that the level s_j benefits from n_i.

After the *NOTIFICATION* is sent out, the header node waits for *ACCEPTANCE* messages from the selected nodes. When the timer expires, the header node checks *ACCEPTANCE* messages and determines whether the number of nodes that agree to provide s_j is enough or not. If it is not, the header node selects more nodes from candidates and modifies the selected nodes set N_j accordingly. This process continues until the service requirement is satisfied. However, the process terminates if the header node cannot select enough nodes to meet with the service satisfaction threshold T_{sat}, and then the service is not provided in the current time slot.

The initial state for a normal node, that is, n_i, is either *UNSELECTED* or *SELECTED* for a given service s_k. During the node selection phase, n_i just waits for *NOTIFICATION*, and selects the s_j with maximum $\mathrm{dec}(i, j)$ from all the received *NOTIFICATION* messages when the timer expires. In case that the initial state is *UNSELECCTED*, n_i changes to *SELECTED* and sends an *ACCEPTANCE* message to the header node. Otherwise, it is obvious that n_i has already been selected to provide another service, that is, s_k. In case that $\mathrm{dec}(i, j) > \mathrm{dec}(i, k)$, n_i sends a *MODIFICATION* message to the header node of service s_k to rearrange the schedule and an *ACCEPTANCE* message to the header node of service s_j. In case that the header node of service s_k receives *MODIFICATION* message, it will remove the corresponding node from N_j and continue the node selection process for s_k.

5.3. Maintenance Phase. In order to balance the residual energy among all nodes, the proposed EDHS adopts the similar strategy to reconstruct the scheduling scheme: reconstruct the selected nodes set when the scheduling scheme runs for a predefined time slots denoted as $T_{\max}$ or some selected nodes are unable to provide the required services due to lack of energy. Once the reconstruction is triggered, the header nodes just reset the selected nodes into *UNSELECTED*, and then the selection phase starts again.

As we can see, the header node plays an important role in the proposed EDHS and shall be replaced in case that its energy is below a given threshold. The new header node can be elected by the old header node since it has collected all information of neighbor nodes that are available to provide the corresponding service. Note that the header node provides the required service too, and so the new header node shall be selected by means of the energy-aware benefit function described in Section 4.1 with $u_j = 0$. However, if several header nodes intend to select the same node as their new headers, the selected node generally chooses the service with maximum service effect. Once the new header is chosen, the elder one delivers *CHANGE* messages to all normal nodes of the service to notify the new header node so that the normal nodes can record the new header.

6. Simulation Results and Analysis

In this section, we present our simulation results demonstrate the performance and effectiveness of proposed schemes. We first introduce the building process of our simulation, then analyze the impact of parameter β of the energy-aware benefit function, and compare these schemes with related works.

6.1. Simulation Setup. We use MATLAB as the simulation platform that is used popularly as the simulation tools of wireless networks. All the experiments are implemented on a PC with Intel Pentium 3.0 GHz and 4 GB RAM. In our simulations, sensor nodes and sensing targets are randomly and uniformly distributed in a square sensing field. The service profit and requirement are also randomly generated. Note that we focus on the problem of scheduling nodes to provide services and thus only energy consumption during the service providing process is considered in this paper. Assume that one node spends a certain amount of energy E_c in one time slot if it is active and spends zero energy otherwise. The service satisfaction threshold T_{sat} is assumed to be 50%, which means that at least half of the service requirement shall be received. The simulation setting is summarized in Table 1. The final results are the average values of 100 different scenarios.

6.2. Impact of Parameter β. The parameter β is an important factor used in the energy-aware benefit function as described in Section 4.1, and it is helpful to ensure trade-off between the residual energy and service effect of nodes during

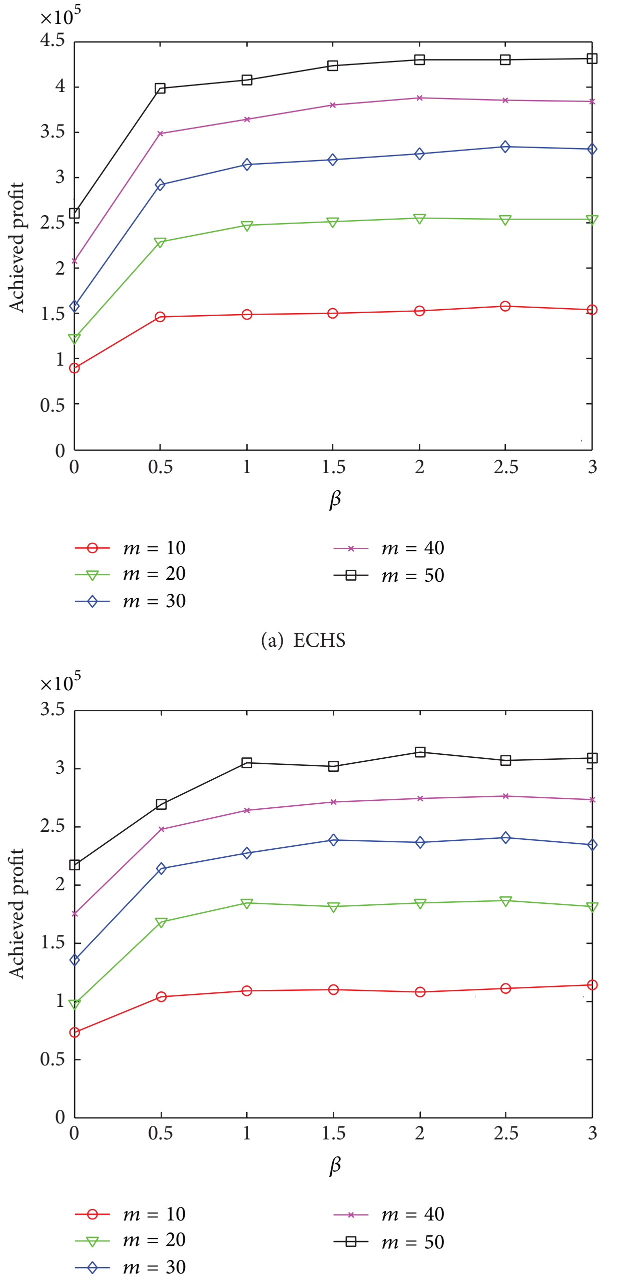
Table 1: Simulation setting.

Sensing field	200 m × 200 m
Number of nodes	200, . . ., 500
Number of services	10, . . ., 50
Requirements for services	[0.2, 1.2]
Profits for services	[1, 10]
Service satisfaction threshold T_{sat}	50%
Initial energy of nodes E	100 unit
Energy consumption E_c	0.1 unit
Sensing range R_s	30 m
Communication range R_c	40 m
Decay factor c	60
Maximum time period for reconstructing scheduling $T_{\max}$	50
Alive nodes threshold τ	0.5, . . ., 1.0

the node selection process. Figure 2 shows the results of network profit achieved by ECHS and EDHS with different value of β, respectively. The simulation is done with 300 nodes and the fraction of alive nodes threshold, τ, is set as 0.8. We compare the performance with different numbers of services when the parameter βvaries from 0 to 3 in steps of 0.5. As we can see from Figure 2, the achieved network profit increases together with β, and then it begins to stabilize when β is larger than 0.5, which demonstrates that the residual energy has more impact on the energy-aware benefit function when β is larger. However, the achieved network profit cannot be further improved when β is larger enough due to the fact that the schemes have distributed energy load evenly among the nodes.

Figure 3 shows the impact of parameter β on the achieved network profit when network size is different. The number of services provided by the network is set as 30, and other settings are identical to those in Figure 2. As we can see from Figure 3, the simulation results are similar to the cases in Figure 2, especially when β is larger. Especially, the network performance is comparatively better when β is 3. Therefore, we choose 3 as the value of β in the following simulations process.

6.3. Performance Comparison. The related works [20, 21] are most closed to the node scheduling problem in service-oriented wireless sensor networks. In order to evaluate the performance of proposed ECHS and EDHS, we compare them with Greedy and EDPA algorithms proposed in [20], and MRGAP algorithm proposed in [21], in which Greedy and MRGAP are centralized algorithms and EDPA is one distributed algorithm. We employ the following modifications to make above algorithms suitable for solving the node scheduling problem addressed in this paper. (1) Use the proposed energy-aware benefit function during the node selection process for Greedy and MRGAP algorithms since energy of nodes is not considered in these algorithms. (2) Use the same strategy as our schemes to reconstruct the node scheduling scheme.

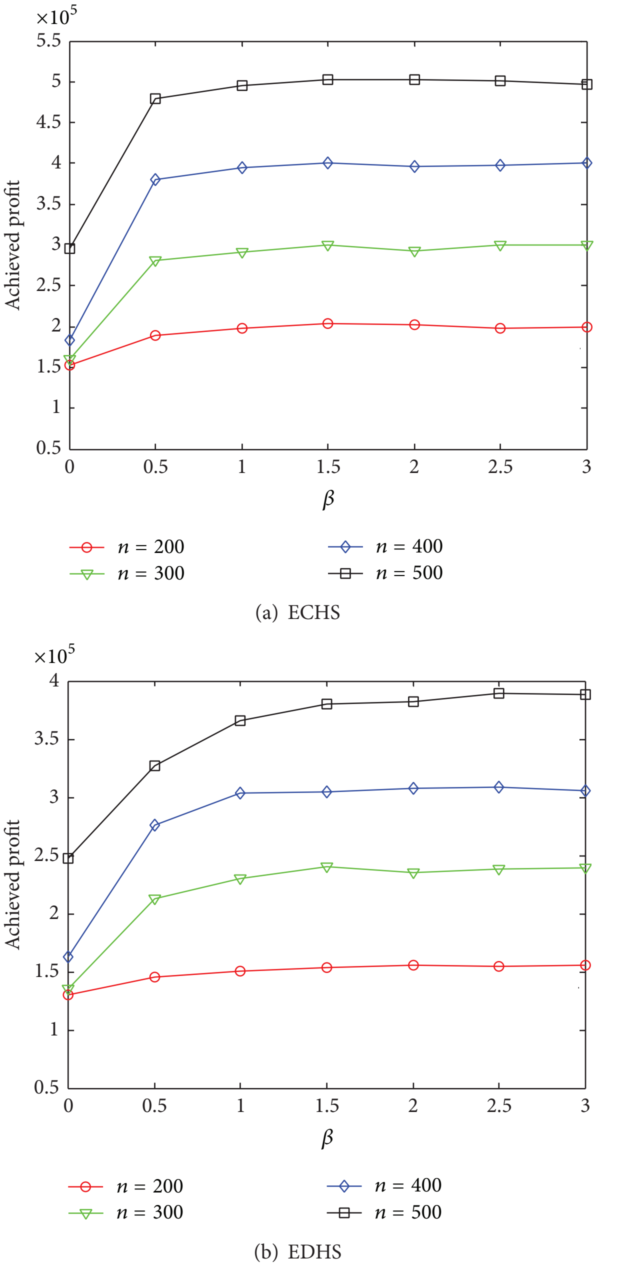


(a) ECHS

(b) EDHS

Figure 2: Impact of parameter β on achieved profit, $m \in \{10, 20, 30, 40, 50\}$.

The first set of experiment is done with 300 nodes and the threshold τ is set as 0.8, and the number of services varies from 10 to 50 in steps of 5. As shown in Figure 4, we have the following two conclusions. (1) The achieved network profit increases together with the number of services, but the trend is not obvious when the number of services is larger enough. Note that the required resource increases with the increasing number of services and thus more profit can be obtained in case that the network provides more services, and the network resources is consumed rapidly so



(a) ECHS

(b) EDHS

Figure 3: Impact of parameter β on achieved profit, $n \in \{200, 300, 400, 500\}$.

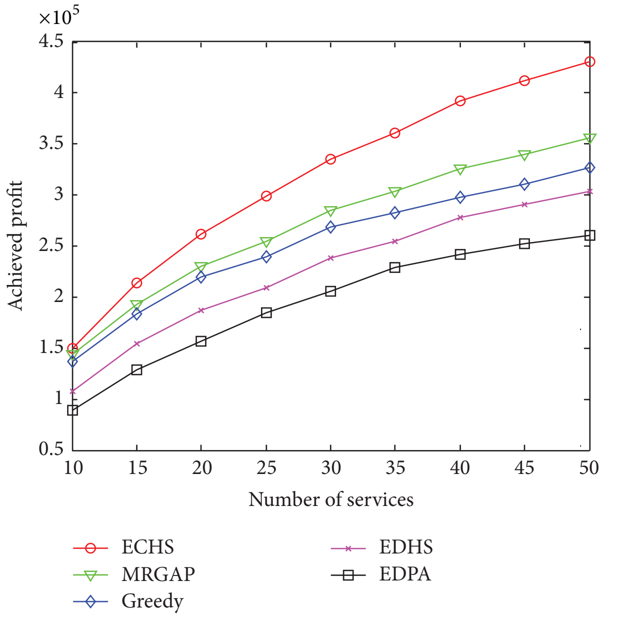


Figure 4: Achieved profit versus number of services.

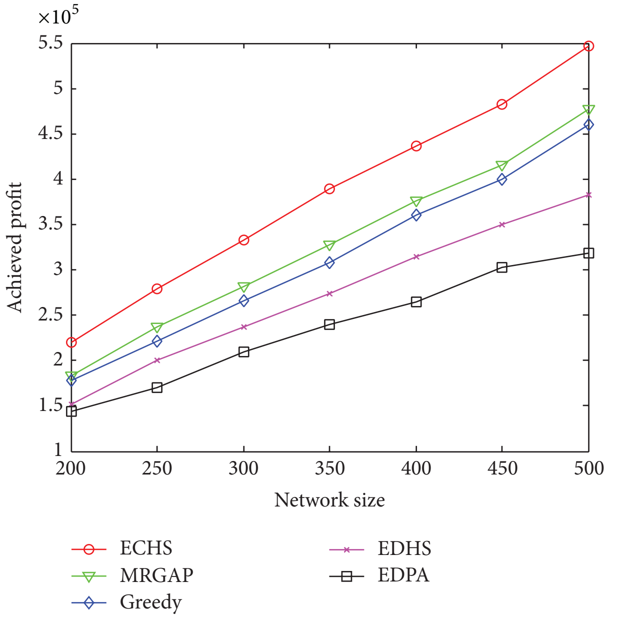


Figure 5: Achieved profit versus network size.

that the network cannot support services in a longer time. Therefore, the achieved network profit increases slowly when the network provides a larger number of services. (2) The ECHS has better performance than MRGAP and Greedy in all cases, and EDHS also has better performance than EDPA.

The second set of experiment is done with 30 services and the threshold τ is set as 0.8, and the network size varies from 200 to 500 in steps of 50. It can be seen from Figure 5 that the larger network size helps to achieve more profit. This is due to the fact that sensor nodes are the carrier of network resources in the wireless sensor network, and the network much better capabilities has when more nodes are deployed. Furthermore, both ECHS and EDHS run better in this set of experiment. Especially, in case that the network size is 300, ECHS performs 18.0% and 25.0% better than MRGAP and Greedy, respectively, EDHS performs 13.5% better than EDPA. In case that the network size is 500, the performance improvements are 14.6%, 18.8%, and 20.3%, respectively.

The third set of experiment is to evaluate the performance of different algorithms with respect to achieved profit under different threshold τ. The simulation is done with 300 nodes and 30 services, and we vary the threshold τ from 0.5 to 1.0. Figure 6 depicts that the achieved profit of network

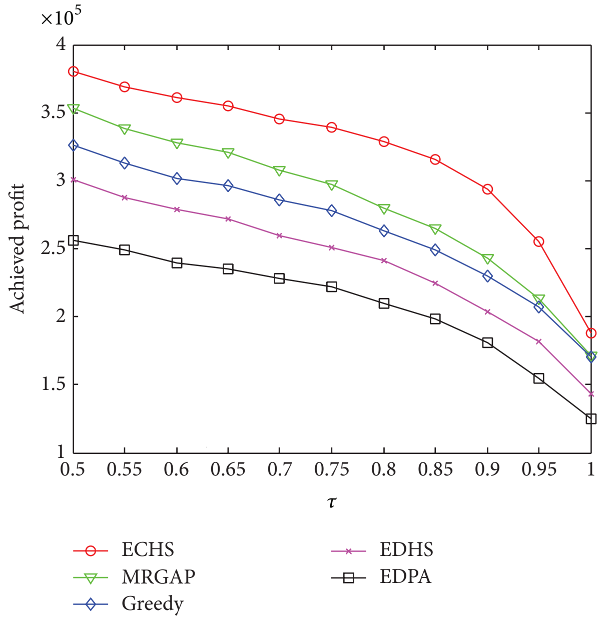


Figure 6: Achieved profit versus threshold τ.

increases with the decreasing of τ and shows that the network can still provide services when a fraction of nodes run out of energy. However, the network provides worse quality of services when the number of such nodes increases. Therefore, the achieved profit increases slightly in case that τ is small enough. Moreover, it is seen that ECHS outperforms the other algorithms, and EDHS also shows better performance than EDPA. In case that τ is 1.0, the ECHS performs 9.8% and 10.1% better than MRGAP and Greedy. While the value of τ is 0.8, the performance improvements are 17.4 and 24.9%, respectively. In addition, the performance improvement of EDHS to EDPA is 14.7% in case that τ is 1.0 or 0.8.

The simulations that we performed showed that the proposed approaches efficiently construct scheduling schemes and are effective in improving the network performance. The strategy of Greedy algorithm is to repeatedly satisfy the most currently profitable service, which is easy to implement. The MRGAP algorithm treats the problem instance as a Generalized Assignment Problem (GAP) that improves the results of Greedy algorithm. However, the proposed ECHS conserves energy by energy-aware benefit function to select active nodes for the required services and performs swapping operation for nodes with low residual energy. The EDHS can dynamically adjust nodes to provide a service that is more beneficial during the node selection phase. Although the EDPA adopts similar strategies, EDHS selects initial nodes in an efficient way with the help of header nodes and so obtains better performance in the subsequent nodes selection process, as we can see from the simulation results. In the distributed scheduling scheme EDHS, is more difficult to obtain better results than centralized approaches. The localized computation and communication make it more suitable in the practical environment.

7. Conclusion

To develop the service-oriented architecture is an important trend for the future wireless sensor network. In this paper, we are concerned with the node scheduling problem to provide various services with energy efficiency, and we propose two heuristic schemes, namely, Energy-aware Centralized Heuristic Scheme (ECHS) and Energy-aware Distributed Heuristic Scheme (EDHS). The proposed schemes select active nodes based on their contribution to services as well as residual energy, which helps to balance the load of energy consumption in the network. Extensive simulations show that both of the two schemes can significantly improve the performance of the network. In this paper, we use a simplifying energy model that neglects the energy consumed in message exchange. In addition, the temporal/spatial correlations between sensed data are important potential to improve the efficiency of scheduling schemes. In the future, we plan to investigate the node scheduling problem with a practical energy model as well as considering the correlation between sensed data and develop a fully solution in the service-oriented wireless sensor network.

Abbreviations

n:	The number of nodes
m:	The number of services
N:	The set of nodes
S:	The set of services
d_j:	The requirement of service s_j
p_j:	The profit of service s_j
$e_{i,j}$:	The effect of node n_i when providing service s_j
T_{sat}:	Threshold that each service shall satisfy
E:	Initial energy of nodes
RE_i:	Current residual energy of node n_i
TL:	Network lifetime.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is partially supported by the National Science Foundation of China under Grant no. 61370210 and 61103175, the Fujian Provincial Natural Science Foundation of China under Grant no. 2011J01345 and 2013J01229, and the Development Foundation of Educational Committee of Fujian Province under Grant no. 2012JA12027.

References

[1] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[2] D. Gračanin, M. Eltoweissy, A. Wadaa, and L. A. DaSilva, “A service-centric model for wireless sensor networks,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 6, pp. 1159–1165, 2005.

[3] A. Rezgui and M. Eltoweissy, "Service-oriented sensor-actuator networks: promises, challenges, and the road ahead," *Computer Communications*, vol. 30, no. 13, pp. 2627–2648, 2007.

[4] X. Chu and R. Buyya, "Service oriented sensor web," in *Sensor Network and Configuration: Fundamentals, Techniques, Platforms, and Experiments*, N. P. Mahalik, Ed., pp. 51–74, Springer, Berlin, Germany, 2007.

[5] N. Mohamed and J. Al-Jaroodi, "A survey on service-oriented middleware for wireless sensor networks," *Service Oriented Computing and Applications*, vol. 5, no. 2, pp. 71–85, 2011.

[6] M. S. Familiar, J. F. Martínez, and L. López, "Pervasive smart spaces and environments: a service-oriented middleware architecture for wireless ad hoc and sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 725190, 11 pages, 2012.

[7] E. Avilés-López and J. A. García-Macías, "TinySOA: a service-oriented architecture for wireless sensor networks," *Service Oriented Computing and Applications*, vol. 3, no. 2, pp. 99–108, 2009.

[8] J. Zhang, B. Iannucci, M. Hennessy et al., "Sensor data as a service—a federated platform for mobile data-centric service development and sharing," in *Proceedings of the IEEE International Conference on Services Computing (SCC '13)*, pp. 446–453, Santa Clara, Calif, USA, July 2013.

[9] H. Cheng, R. Guo, and Y. Chen, "Node selection algorithms with data accuracy guarantee in service-oriented wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 527965, 14 pages, 2013.

[10] J. Wang, D. Li, G. Xing, and H. Du, "Cross-layer sleep scheduling design in service-oriented wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 11, pp. 1622–1633, 2010.

[11] C. Wang, H. Ma, Y. He, and S. Xiong, "Adaptive approximate data collection for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1004–1016, 2012.

[12] H.-C. Weng, Y.-H. Chen, E. H.-K. Wu, and G.-H. Chen, "Correlated data gathering with double trees in wireless sensor networks," *IEEE Sensors Journal*, vol. 12, no. 5, pp. 1147–1156, 2012.

[13] C. Hung, W. Peng, and W. Lee, "Energy-aware set-covering approaches for approximate data collection in wireless sensor networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 24, no. 11, pp. 1993–2007, 2012.

[14] G. Anastasi, M. Conti, M. di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: a survey," *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, 2009.

[15] S. Kumar, T. H. Lai, and J. Balogh, "On k-coverage in a mostly sleeping sensor network," in *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom '04)*, pp. 144–158, Philadelphia, Pa, USA, September 2004.

[16] Y. Zhao, J. Wu, F. Li, and S. Lu, "On maximizing the lifetime of wireless sensor networks using virtual backbone scheduling," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1528–1535, 2012.

[17] J. Lin, W. Xiao, F. L. Lewis, and L. Xie, "Energy-efficient distributed adaptive multisensor scheduling for target tracking in wireless sensor networks," *IEEE Transactions on Instrumentation and Measurement*, vol. 58, no. 6, pp. 1886–1896, 2009.

[18] D. Zorbas, D. Glynos, P. Kotzanikolaou, and C. Douligeris, "Solving coverage problems in wireless sensor networks using cover sets," *Ad Hoc Networks*, vol. 8, no. 4, pp. 400–415, 2010.

[19] N. Xiong, X. Huang, H. Cheng, and Z. Wan, "Energy-efficient algorithm for broadcasting in ad hoc wireless sensor networks," *Sensors*, vol. 13, no. 4, pp. 4922–4946, 2013.

[20] H. Rowaihy, M. P. Johnson, O. Liu, A. Bar-Noy, T. Brown, and T. La Porta, "Sensor-mission assignment in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 6, no. 4, pp. 1–33, 2010.

[21] M. P. Johnson, H. Rowaihy, D. Pizzocaro et al., "Sensor-mission assignment in constrained environments," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 11, pp. 1692–1705, 2010.

[22] T. L. Porta, C. Petrioli, and D. Spenza, "Sensor-mission assignment in wireless sensor networks with energy harvesting," in *Proceedings of the 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '11)*, pp. 413–421, Salt Lake City, Utah, USA, June 2011.

[23] S. C. Geyik, B. K. Szymanski, P. Zerfos, and D. Verma, "Dynamic composition of services in sensor networks," in *Proceedings of the 7th IEEE International Conference on Services Computing (SCC '10)*, pp. 242–249, Miami, Fla, USA, July 2010.

[24] J.-H. Cho, A. Swami, and T. Cook, "Combinatorial auction-based multiple dynamic mission assignment," in *Proceedings of the IEEE Military Communications Conference (MILCOM '11)*, pp. 1327–1332, Baltimore, Md, USA, November 2011.

[25] Y. Wang, X. Wang, D. Wang, and D. P. Agrawal, "Range-free localization using expected hop progress in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 10, pp. 1540–1552, 2009.

[26] J.-P. Sheu, P.-C. Chen, and C.-S. Hsu, "A distributed localization scheme for wireless sensor networks with improved grid-scan and vector-based refinement," *IEEE Transactions on Mobile Computing*, vol. 7, no. 9, pp. 1110–1123, 2008.

[27] A. A. Aziz, Y. A. Sekercioglu, P. Fitzpatrick, and M. Ivanovich, "A survey on distributed topology control techniques for extending the lifetime of battery powered wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 121–144, 2013.

[28] R. Soua and P. Minet, "A survey on energy efficient techniques in wireless sensor networks," in *Proceedings of the 4th Joint IFIP Wireless and Mobile Networking Conference (WMNC '11)*, pp. 1–9, Toulouse, France, October 2011.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 461780, 9 pages
http://dx.doi.org/10.1155/2014/461780

Research Article

Investigating How User's Activities in Both Virtual and Physical World Impact Each Other Leveraging LBSN Data

Zhiwen Yu,[1] Yue Yang,[1] Xingshe Zhou,[1] Yu Zheng,[2] and Xing Xie[2]

[1] *School of Computer Science, Northwestern Polytechnical University, Xi'an 710072, China*
[2] *Microsoft Research Asia, Beijing 100080, China*

Correspondence should be addressed to Zhiwen Yu; zhiweny@gmail.com

Received 5 October 2013; Accepted 15 December 2013; Published 19 February 2014

Academic Editor: Jong Hyuk Park

In this paper, we investigate how user's online behavior (e.g., making friendships) and their offline activity (e.g., check-ins) affected each other by leveraging the data collected from LBSN. First, we use vectors to represent nodes and define popularity entropy for each node to weigh their popularities and the impact on forming a new edge. Then, we propose an algorithm to calculate the weight of each edge based on our findings that the more overlap of linked nodes they have, the heavier weight the edge has and the more popular the nodes in their overlap are, the lighter the weight of the edge is. Finally, we conduct link prediction by using the random walk with restart method considering the effect of every node and every edge. Experimental results show that user's activity in virtual world and physical world do really have great impact on each other.

1. Introduction

The advent of GPS-enabled smart phones has had a significant impact on the development of location-based services. Combined with user's growing interests in on-line social networks, it leads to the emergence of many location-based social network (LBSN) services, such as Foursquare (http://foursquare.com/), Brightkite (http://brightkite.com/), and Loopt (http://www.loopt.com/). Millions of users have already been attracted to such kind of services, with which they can leave digital footprints [1], known as check-ins, at the places where they have been to. This service also makes it possible for users to share their locations, photos, and tips with friends anytime and anywhere. Many users prefer to share their trajectories on LBSNs rather than to directly tell people where they are on traditional microblogs. The possible reason is that LBSNs provide much stronger social security, that is, user's check-ins can only be seen by a small group of people specified by the user themselves, while user's microblogs are public to anyone who has followed them on microblogging websites. When a user publishes where they are, they may worry about revealing too much personal information.

As a classical problem in complex network [2], link prediction became a hot topic again when all the nodes are replaced by humans instead of physical network nodes. A considerable amount of attention has been devoted to this problem in social networks and a lot of consensuses have been reached. The most widely accepted one is that, for any two users, the more friends they have in common, the more likely that they would become friends in the coming future. This naive idea really works and has been used in link recommendation by different on-line social networks. However, based on a sociology theory called homophily [3] which emphasizes the importance of similarity in the process of forming a new link between any two strangers, it is intuitive to infer that similar people usually go to similar places, which is to say if any two users often visit the same or similar places, they are likely to be friends. However, it has not been well explored yet because large-scale user's movements in physical world are difficult to monitor.

In this paper, we use the data crawled from Foursquare to explore how users' activities in virtual world and physical world impact each other, particularly how users' movements affect users' online friendships and vice versa. As a location-based social network, Foursquare contains two kinds of information: one is user's social graph in visual world and the other is user's check-ins in the physical world. However, it is difficult to get check-ins directly for security reasons; thus we use tips instead, which contain not only time and location as check-ins but also some comments or messages created by users.

We use vectors with different amount of elements to represent different users and places. Each element in a vector represents an entity, which can be another user or a location linked to the user. If any two users are friends or a user has been to a place, we can say that the two users are linked to each other or the user and the place are linked to each other, which means that there is an edge between them in graph made up by users and locations. In this way, we store all the information and edges in the graph consisting of users and locations that are regarded as nodes.

All the vectors representing users and locations make up a graph, which is called global graph, while a certain user's friends and his/her visited locations make up the user's local graph. It is known to all that many ordinary users may follow many famous movie stars or famous writers in the on-line social network, but for any two of this kind of ordinary users, they are not much less possible to be friends in the future. The reason is obvious that famous users usually have very large local graphs linking them to many users, and these users do not have much in common with each other. This phenomenon also exists among the users who visited a very popular place. For example, there are numerous visitors visiting the Imperial Palace every day, but only very few users may be friends. On the contrary, users who are linked to unpopular locations and unpopular users are highly likely to be friends in the future. In order to portray this characteristic to be used in link prediction, we define a weighing entropy to weigh every node so that we can take all the information that each node contains when predicting users' relationships and movements. Finally, we conduct link prediction by using the random walk with restart method considering the effect of every node and every edge.

In the remainder of this paper, we first discuss related works in Section 2 and give several basic definitions and our motivation in Section 3. In Section 4, we analyse the statistic features of the data. The link prediction and experimental results are presented in Sections 5 and 6, respectively. Finally, we conclude the paper in Section 7.

2. Related Work

The link prediction problem in social networks has attracted a considerable attention since it was introduced by Liben-Nowell and Kleinberg [4]. Link prediction was first explored in the complex networks and when more and more users' started joining on-line social networks, researchers started to analyse users' activities in on-line social networks with different backgrounds and different purposes. In fact, we can view social networks as special complex networks whose nodes are entities (users or locations) and edges represent interaction, collaboration, or influence between entities. Before introducing the studies in link prediction, firstly we try to define this problem as follows.

Given a snapshot of a graph representing social network at time T_0, we seek to accurately predict the new edges that will be added to the graph during a certain time interval from time T_0 to a given future time T_1.

Pondering over this problem deeply, we can easily find that it contains two questions. The first one is that by what features intrinsic to the network itself the social network evolves. The second one is how the social network evolves. The key to get the answer is to find the factors that have the greatest impact on the network's evolution. We try to summarize the related work according to the factors that were used in link prediction.

2.1. Factors with User's Movements in Physical World. To predict the occurrence of new edge between any two users in a social network, the first step is to find the similarities between them. Many researchers tried to mine user similarity from users' movements. Users' movements in the physical world usually show their travelling trajectories in daily life and represent users' activities in the physical world directly. When users are at a certain place, they can only do certain things; for example, users can only watch movies in a movie theatre while have dinner at restaurants. Furthermore, similar people go to similar places with similar visiting sequences at similar time. Based on these ideas, issues focusing on mining users' similarities from users' movements have largely been explored. Li et al. [5] hire several volunteers from different countries and different cities equipped with GPS loggers to collect their trajectories for several months to mine similarities among these volunteers. They firstly detect stay points from trajectories considering the length of user's staying time and the distance among different GPS points and transferred user's raw GPS trajectories into the sequences of stay points. They build a hierarchical graph with three levels, which have different ranges of areas, to model user's location history. They argue that except for colocations, which refer to the locations that are visited by related users, among the users, visiting sequences make more sense and carry more meaningful information in mining users' similarities. Then, they tried to find similar sequences with different lengths among users and compute the similarity across multilevels. This work has made a great process in mining user similarity from physical world resources. However, it is difficult to get a large-scale nonvolunteer user's trajectories, partly because it is impossible to let everyone equip with a GPS logger and partly due to privacy issues. Therefore it is hard to apply this idea to find similarities among a large scale of users.

As more and more users use cell phones, researchers try to infer social ties from cellular network data. Cho et al. [6] use data from Brightkite (http://brightkite.com/) and Gowalla (http://gowalla.com/) along with a dataset of cell phone location trace data to understand the basic laws that govern users' motion and dynamics. They find that there basically exist two features in users' travel style. One is that users' short-ranged travel is geographically and temporally periodic and has nothing to do with social network structure; the other is that users' long-distance travel is largely affected by social network ties. More than 50% of user's movements can be explained by periodic behaviour while less than 30% of user's movements can be explained by social ties. Thus, they build a periodic and social mobility model to predict individuals' mobility combining periodic short-ranged movements with social-ties related travels. Their model has three different components capturing the feature of user's regularly visiting spatial locations, the temporal movement between these locations, and user's movements influenced by social ties, respectively. The model has acceptable performance in predicting user's mobility. However, it only explores how user's mobility is influenced by features like social ties and periodic activities but pays no attention to how user's mobility can impact other aspects of user's life.

There are also many research works making use of users' trajectories in physical world for other interesting purposes. For instance, Lian and Xie [7] proposed a novel location naming approach to automatically provide concrete and meaningful location names to users based on their current location, time, and check-in histories.

2.2. Factors with User's Relation in the Virtual World. Nowadays, many people spent more and more time on on-line social networks such as Facebook and Twitter, keeping in touch with existing friends, getting to know new friends, and sharing ideas and resources. Many factors might have impact on the evolution of the user's social network. Xiang et al. [8] try to model relationship strength using users' profiles and interactions among users using the data from Facebook and LinkedIn. Before building a model, they first assume that people tend to form ties with people having similar characteristics and relationship strength has impact on online interactions, both on nature and frequency. They develop an unsupervised latent variable model to estimate relationship strength from interaction activities, which can be communication, tagging or something else, and user similarity extracted from users' profiles. The estimated relationship strengths result in a weighted graph of which the spurious links have been downweighted while the important ones have been highlighted. Finally, these weighted links can be used to increase the accuracy of social network mining tasks, including link prediction. Tang et al. [9] try to do link prediction using data across heterogeneous networks. The main question is how to bridge the available knowledge from different networks to help infer different types of social relationships. Their main ideas come from several social psychological theories such as social balance, structural hole, and social status. They proposed a transfer-based factor graph model incorporating social theories into a semisupervised learning framework used to transfer supervised information from the source network to help infer social ties in the target network. As we all know almost every user has accounts on different online social networks and different networks contain different aspects of information of a user. This work represents a new and interesting research direction in making full use of user's online activities.

Besides the data from online social network, emails can be regarded as users' activities in the virtual world. Researchers from Google [10] made use of users' implicit social graph, which is formed by users' interactions with contact and groups of contacts in Gmail, to do friendship recommendation. They also proposed an interaction-based metric for estimating a user's affinity to their contacts and groups. Their experiments showed that both implicit social graph and interaction based affinity were important in suggesting friends.

2.3. Factors with Mixed Resources. As online social networks and user's movements contain user's activities and relationships in virtual and physical world, respectively, if we try to understand user's activities from only one point of view, we can only get biased results. To get better and unbiased understanding of user's activities in both circumstances, several researchers turn to combine information from these two aspects to do link prediction. Cranshaw et al. [11] first analyze the social context of a geographic region from a set of location-based features including location entropy. Then, they compose a model to predict the friendship between any two users by analyzing their location trails. Finally, they show a positive relationship between the colocation histories and the social ties that the user has in the network. Their work proves that offline mobility has impact on user's online activities. Wang et al. [12] try to find the relation between human mobility, social ties, and link prediction. Mobile communication records are regarded as the representation of social ties while user's moving trajectories are extracted from cellular network. The authors try to predict the social ties with different datasets, each of which contains different proportion of user's mobility.

Scellato et al. [13] described a supervised learning framework which exploits prediction features which they extracted from data of Gowalla to predict new links among friends-of-friends and place-friends and showed that the inclusion of information about places and related user activity offers high link prediction performance.

User's friendship usually can be crawled from online social networks, but user's mobility is very hard to get. Previous works usually tend to use cellular network data or hire volunteers to collect trajectories. However, cellular network data is often of low accuracy, while hiring volunteers to collect data is only suitable for a small scale of study. No matter which one of these two resources was used, researchers have to spend much time in extracting locations with semantic or geographic context from the raw data. In fact, we care much more about where the user has been to instead of how he/she got there. Location-based online social networks offer such kind of information as users often tag the places they have visited. In this way, we can do link prediction and study the impact that user's mobility and social ties have on each other from a new point of view.

3. Preliminary

In this section, we first give several definitions and then introduce our main motivations. To simplify the explanation, we view locations and users as the same which is determined by our motivations.

3.1. Definitions

Definition 1 (node). A node v refers to a user or a location that the network contains. Users and locations have the same status in this paper. Each node v is associated with a unique ID, $v \cdot id$, which starts from 1 and ends at the number of total nodes.

Definition 2 (edge). If two users, represented by node j and node k in the network, are friends, there will be an edge $e_{j,k}$ between them, showing that they are connected to each other. Similarly, if a user has visited a place, there will also be an edge between them. Each edge $e_{j,k}$ is undirected and associated with two terminal points, $e_{j,k} \cdot v_j$ and $e_{j,k} \cdot v_k$, referring to the two nodes (node j and node k) it connects. $e_{j,k} \cdot w$ is the weight of the edge determined by the popularity entropy of two nodes. Furthermore, a user can visit a place for several times but only can be friends with another user for only once, which means that part of edges may occur more than once. To record this feature, the last attribute of each edge $e_{j,k}$ is $e_{j,k} \cdot t$ recording the times the edge occurred. For edges connecting users, the value is 1, but for those connecting users and locations, the value may be large than 1.

Definition 3 (global social graph). A global social graph $G(V, E)$ contains all the information and represents the structure of a whole location-based social network containing two types of elements, node v and edge e. It is an undirected graph.

Definition 4 (local social graph). Node l's local social graph $G_l(V_l, E_l)$ may contain the complete friendship and all the visited places of a user, or all the users who have been to a particular place. All nodes in the local social graph G_l are connected to the node l directly; that is, only one-hop connections exist in local graph. The graph is also an undirected graph.

Definition 5 (cofriend). For any two friends, A and B, of a user, the user is a cofriend cf of them.

Definition 6 (colocation). If two users have been to the same place, the place is their colocation cl. We do not require that the two users must visit the place at the same time.

Definition 7 (popularity entropy). Popularity entropy pe is used to weigh a node's popularity among all the nodes and has impact on the strength of links connected to the nodes.

3.2. Motivations. Our motivation is quite simple and direct. Most existing research works focus on predicting the link among friends' friends or between friends and friends' visited locations, all of which are nodes that are no more than 2 hops away from each other. However, we argue that new links within 2 hops away are just a small part of all the newly added edges and there are a large amount of newly added edges occurring between the nodes whose distance is more than 2 hops. Figure 1 shows the proportion of the two kinds of new added links occurring during the period from September 2011 to February 2012 in our dataset collected from Foursquare.

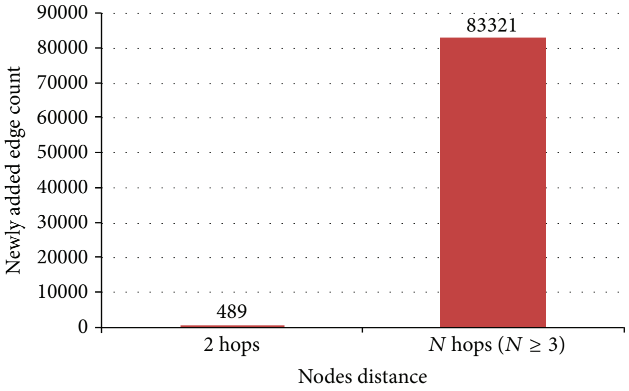


FIGURE 1: Distance of nodes that newly added edges link.

We can see from Figure 1 that very few new links are added among the nodes within 2-hop distance while most new links are added among the nodes which are farther away from each other. The result shows that if we only pay attention to the new links within 2 hops, much information will be lost and high precision of link prediction cannot be achieved.

It is well accepted that for any two unconnected users, the more friends they share, the more likely that they would be friends in the near future. But we may have a common sense that famous users, such as movie stars like Justin Bieber, or some dignitaries, for example, Obama, usually have a very large social network in those online social networks. If any two users whose most friends are the famous users on the network, do they have large probability to be friends in the future? It is probably not. We argue that except the amount of common friends any two users have, the scale of common friends' social network also has impact on forming a new link between two strangers.

The last motivation is that since online social network has become a part of life, we want to analyse the interaction between our daily life and the online social network. To explain it in detail, we divide user's activities into two parts: the first part is user's activities in the offline world, for example, moving to a new city or meeting with new friends and so forth, while the other part is user's online activities, such as adding new friends or commenting on friends' photos. What kind of influence these two kinds of activities have on each other is largely unexplored.

Before further introducing our work, we introduce two basic hypotheses in this paper as follows:

Hypothesis 1. The larger the scale of overlap that any two users' relationship has in virtual world is, the more likely that they will have larger scale of overlap in check-ins in physical world.

Hypothesis 2. The larger the scale of overlap that any two users' check-ins in physical world have is, the more likely that they will have large scale of overlap of relationship in virtual world.

Table 1: Amount of newly added edges in different groups.

Group	Amount of shared friends	Amount of shared friends' friends	Amount of new added edges
1	10.33	25.74	1.41
2	11.56	14.79	3.75

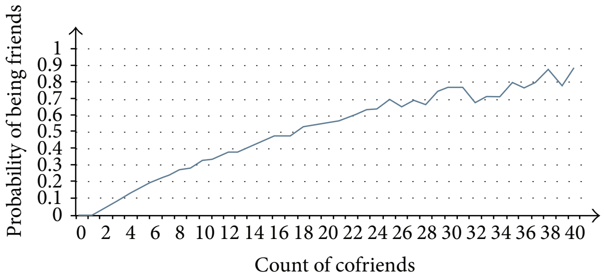


Figure 2: The relationship between probability of being friends and the amount of cofriends.

These two hypotheses come from the goal of exploring the impact of user's activities in physical and virtual world on each other. Our further experimental results will show that these two hypotheses are reasonable and meet the phenomenon in reality.

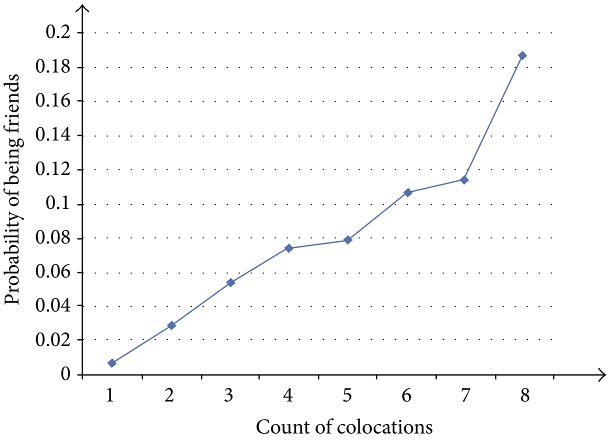


Figure 3: The relationship between probability of being friends and the amount of colocations.

4. Observations

We use the dataset crawled from Foursquare. The dataset contains 31524 users, 51265 venues (locations), and users' tips about these venues from July 2011 to May 2012. In this paper, we take user's check-ins extracted from tips (time and geographic information) as user's activity in the physical world and the evolution of user's friendship as user's activity in the virtual world. We here present the statistic characteristic of the data collected from July 2011 to February 2012.

Firstly, we analyze how the amount of shared friends has influence on users' social ties. Figure 2 shows the relationship between the amount of shared friends that any two users have and their probability of being friends.

In Figure 2, we only show the records of samples with a relatively larger scale. It is easy to find that the probability of being friends almost rises as the amount of shared friends grows. However, it is also obvious that the curve shakes with the increment and the probability does not grow purely. How does it happen? Dose the probability not grow as the amount of common friends rises? Just as our motivation, it is not always true. To verify the idea, we choose two groups of users. In Group 1, the shared friends of any two users are almost the users who own a relatively larger social network, while in Group 2, shared friends are with a relatively smaller social network. We analyse the average amount of new links added among these users from September 2011 to February 2012 in different groups and the results are definitely different, as shown in Table 1.

It is not surprising to find that there are only very few new links added in the first group but much more in the second group. Just as mentioned in our motivation, users with a large amount of friends are usually some kind of famous people in the social network and anyone who is interested in them can add them as friends. As a result, the links between the famous user and their friends are quite weak and cannot be used as the support to predict new links. But for the less popular users, since their social networks are relatively smaller, their friends are closely connected with them and the links are the strong supports for predicting new links.

Since we take user's check-ins as users' activities in physical world and evolution of their friendships as activities in virtual world, and our goal is to find whether user's activities in virtual and physical world have impact on each other, we have to investigate two topics. The first one is that if two users have N colocations, we want to know what the probability of the two users being friends is.

From Figure 3, we can observe that as the number of colocations of two users rises, the probability of being friends increases obviously. However, we can observe some shakes clearly again. The reason why the shakes occur is similar to that in Figure 2. There are always some places attracting numerous people while some others are visited by a very small group of people. The popularity of a place has great impact on the strength of the links between the place and the attracted users. The more the people visit a place, the more popular the place is, the weaker the links between the place and user are and vice versa. As the number of colocations rises, the proportion of popular colocations changes and the amount of pairs of users who have colocations changes, which is the reason why the shakes occur.

The second topic we want to investigate is that, as the number of cofriends increases, whether the probability of having colocations will rise. The result is shown in Figure 4.

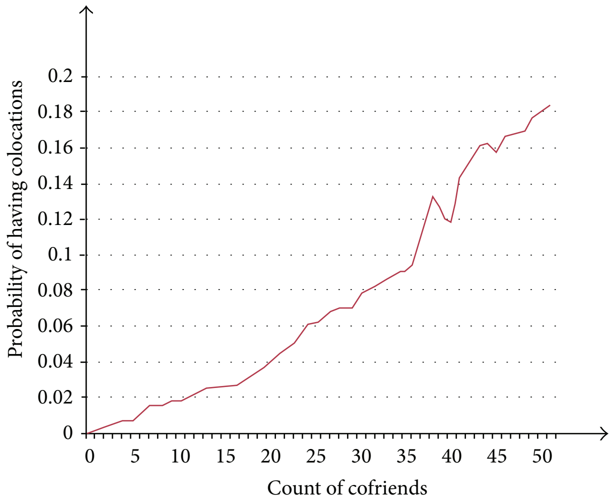


Figure 4: The relationship between probability of having colocations and the count of cofriends.

We can observe that when the number of cofriends increases, the probability of having colocations also increases, but there are also some shakes. The explanation is similar to the above one.

All the static analysis results show that it is not proper to consider the amount of colocations or cofriends only when predicting new links. Each member of colocations and cofriends contains much information about the links and helps us to understand the existing links better. But how to translate the information into a form that can be used in link prediction remains a problem. In the next section, we will try to solve it.

5. Impact Detection

We try to study how user's friendship and their check-ins impact each other. Our main task is to predict the new edges (links) in the graph with nodes representing users and locations. It is well accepted that the more information we obtain and use when we try to predict new links, the higher precision we can get. However, due to the limits of the space of storage and time, it is not practical to store all information. It is not a good way to simply count the number of colocations and cofriends, since each element of them also contains some factors that have impact on the addition of new links. In this paper, we propose an effective way to handle the issue.

Every node in the global graph is connected with many nodes and these nodes may be connected with many other nodes. Each node's popularity is determined by its connection with the rest of nodes. We use a vector to represent each node. There are a very large number of nodes including users and locations in the global graph but only a few nodes are connected with each other, which means that the global graph is very sparse. If we store all the edges in the graph without considering whether they really exist, the most elements in every vector will be 0 meaning that the nodes are not connected and most information in the vectors is meaningless. In fact, only the connected nodes and their edges make sense in link prediction. Since each edge stores the information about its weight, its occurrence times, and the two nodes it connects, a node's vector which contains all the edges connected to the node can store all the information that the node has. By doing so, the topology of the social networks is stored with high coefficient of storage space utilization and it also ensures that all the nodes in the social network have the same status.

If the social network contains N nodes in total, for node i connected with n edges, its vector, v_i, is defined as follows:

$$v_i = v\left(e_{i,j_1}, e_{i,j_2}, \ldots, e_{i,j_n}\right), \quad i \in [1, N], \; j_m \neq i, \; m \in [1, n], \tag{1}$$

where $e_{i,j}$ $(i \neq j)$ represents the edge existing between node i and node j and $e_{i,j}$ is the same with $e_{j,i}$ $(i \neq j)$, because we treat the graph of social network as on undirected graph in this paper. All the elements' initial values of weight are set to be 1 and the final value will be larger than 0 in every vector. Since all the weights are associated with the nodes' popularity entropy, we introduce a method to calculate entropy as shown in Algorithm 1. $e_j \cdot t$ means that the number of the edges of e_j appears in the dataset.

For a node i, we first get the sum count n of its vector's elements, then we calculate the sum value of occurrence times of the edges linked to node i. According to our hypothesis, for any node, its popularity is proportional to the amount n of other nodes it is connected with and the occurrence times of edges that are linked to the node. In order to get normalized weight for each node, the popularity entropy pe_i for node i is computed as follows:

$$\mathrm{pe}_i = n * \frac{\mathrm{value}}{\mathrm{Sum}_E}, \tag{2}$$

where the sum Sum_E of edges is used to complete the normalization. To explain the algorithm in detail, the basic idea of calculating the weight of each edge is summarized as follows.

For two nodes that have been connected to each other in the location-based social network,

(1) the more shared nodes they have, the stronger the tie between them is; that is why we use the sum of the values got from each element as edge's weight between the two nodes;

(2) the more less-popular nodes they share, the stronger the tie between them is; that is why we use the reciprocal of the nodes' popularity entropy as a factor that has impact on the strength of tie between the two nodes;

(3) the more times an edge occurs, the more important the linking nodes are for each other; so we use the sum of the occurrence times they connected with their shared nodes to weigh the importance of the shared nodes for the two nodes.

As the values of $e_{j,i} \cdot w$ and $e_{i,j} \cdot w$ are the same, we can compute them at the same time. To keep the computation in

```
Input: a collection of nodes' initial vectors $V$, the sum of edges $\mathrm{Sum}_E$
Output: a collection of nodes' popularity entropy $\mathrm{PE} = \{\mathrm{pe}\}$
$i \leftarrow 1, N \leftarrow |V|$
While ($i < N + 1$)
    $\mathrm{pe}_i \leftarrow 0, n \leftarrow \|v_i\|$, $value \leftarrow 0$
    foreach $e_j$ in $v_i$
        $value = value + e_j.t$
        $j \leftarrow j + 1$
    $\mathrm{pe}_i = n * value/\mathrm{Sum}_E$
    $i \leftarrow i + 1$
    return $\mathrm{pe}_{i-1}$
```

Algorithm 1: Popularity entropy calculation.

```
Input: a collection of nodes' vectors $V$, a collection of nodes'
popularity PE, the sum of edges $\mathrm{Sum}_E$
Output: a collection of nodes' vectors $V = \{v\}$,
$i \leftarrow 1, N \leftarrow |V_{\mathrm{ini}}|, Initial(V)$
While ($i < N + 1$)
    foreach $e_{i,j}$ in $v_i$
        if $e_{i,j}.vj > i$
            $j \leftarrow e_{i,j}.vj, P \leftarrow CommonNodes(v_t, v_j), e_{i,j}.w = e_{j,i}.w = 0$
            foreach $p$ in $P$
                $m \leftarrow \|v_p\|, n \leftarrow \mathrm{sum}(e_{i,p}.t, e_{j,p}.t)$
                $e_{j,i}.w = e_{i,j}.w = e_{i,j}.w + reverse(\mathrm{pe}_p) * n/m$
    $i \leftarrow i + 1$
    return $v_{i-1}$
```

Algorithm 2: Edge final weight calculation.

a controllable style and save both the time and space, we let each node only compute the strengths of ties with the other nodes having larger node ID than it does. For any node i, we check the elements in its vector one by one. For an element $e_{j,i}$ in node i's vector, we first check the id $v_j \cdot id$ of the other node that node i connects; if $v_j \cdot id$ is larger than $v_i \cdot id$, then we store the node's id as j and try to get the shared nodes of node i and node j. Then, for every shared node p, we calculate its vector's count m and the sum of $e_{j,p} \cdot t$. According to our hypothesis the occurrence times of edges linking to shared nodes are proportional to the weight of edge $e_{i,j}$, while the popularity entropy of shared nodes is inversely proportional to the weight of that edge. So each shared node's contribution to the edge $e_{i,j}$ is computed by the following formula:

$$C_{p-ij} = \mathrm{reverse}\left(\mathrm{pe}_p\right) * \frac{n}{m}. \tag{3}$$

C_{p-ij} represents the shared node p's contribution to the edge $e_{i,j}$, and reverse (pe_p) represents the reverse value of pe_p. By computing the sum of all shared nodes' contribution, we get the value of edge $e_{i,j}$. All these processes are shown in Algorithm 2. The algorithm is different from TF-IDF [14]. Using TF-IDF algorithm, we should firstly specify one kind of nodes as a document containing many words and the others are chosen to be words. However users and locations have the same status in the social network; choosing any one of them as document will destroy the balanced status.

Using Algorithm 2, we can get the weights of all the edges existing in the social network. After getting the popularity of each node and weight of each edge, we use random walk with restart [15] as the model to do link prediction.

6. Experimental Results

We divide the crawled dataset into two parts: the first part starts from July 2011 to February 2012 and the second part start from February 2012 to May 2012. We use the first part data as training set and the second part as test data. We would like to use the test set to verify the effectiveness of our method in improving the accuracy of link prediction. To go one step further, we also want to show that user's activities in virtual world and physical world have impact on each other, which can be shown in the result of link prediction.

First, we would like to experimentally evaluate the capability of our method to compute the strength of ties between real entities, for example, between user and user or between user and location. We use Algorithm 2 to calculate the weights of existing edges and the possible weights of edges between nodes that are not really connected to each other. In other words, we suppose that any two nodes in the social network were connected to each other and we

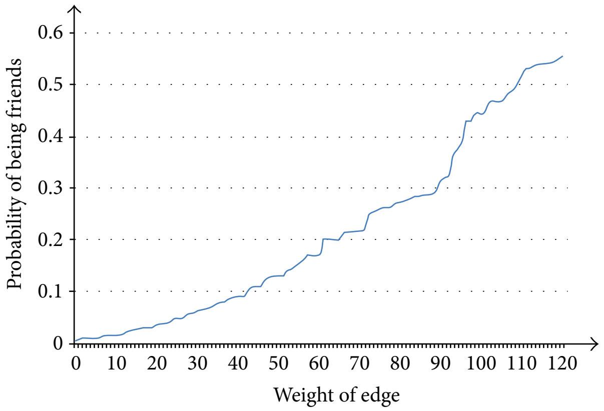


Figure 5: The relationship between probability of being friend-nodes and the weight of edges.

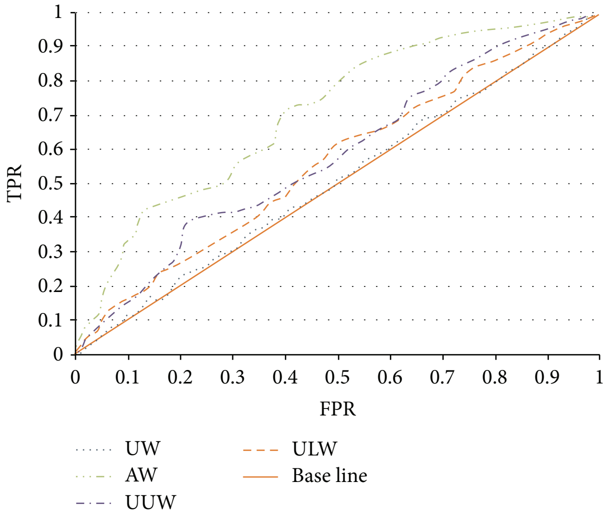


Figure 6: Link prediction results using different information (the graph with all weighted edges (AW), the graph with all edges' weights to be 1 (UW), graph with only user-user edges (UUW), and graph with only user-location edges (ULW)).

Table 2: Contents of different graphs.

Graph Feature	AW	UW	UUW	ULW
User' relation	*	*	*	—
User's tips	*	*	—	*
Weighted or not	*	—	*	*

calculate the weights of all edges even though some of them may not exist. Then, we view the pair of nodes that are really connected as friend-nodes and finally get the relationship between probability of being friend-nodes and the weight of edges. The results are shown in Figure 5 where the whole dataset is used (i.e., July 2011 to May 2012).

From Figure 5, we can observe that for any two nodes, the probability that they are connected with each other varies directly with the weight of the edge linking them. Furthermore, there is almost no shake before the ending part of the curve. Comparing to Figure 2, this result verifies our idea that nodes' relations are not only impacted by the amounts of shared nodes but also the amounts of connected nodes each shared node owns. Since the probability varies along with the weight of edge, the curve also shows that it is really necessary to take the existing edges' weights into account when performing link prediction instead of counting the amount of shared nodes only.

To analyze the impact that the physical world and virtual world have on each other, we conduct the experiments on different graphs, for example, the graph with all weighted edges (AW), the graph with all edges' weights to be 1 (UW), graph with only user-user edges (UUW), and graph with only user-location edges (ULW). Details are as shown in Table 2, where "*" means that the corresponding vertical line contains the information in the related horizontal line while "—" means that is does not. For instance, UW contains the information of user relation and tips (i.e., check-ins).

We use the four graphs to show how different types of information have impact on the result of link prediction. Comparing the results of AW and UW, we intend to see how the weighted information can be used to improve the performance of link prediction. The purpose of comparing the results of AW and UUW is to find out how a user's activities in the physical world can influence his/her activities in the virtual world, while comparing the results of AW and ULW is just for the inverse purpose. We use the graph in MAY 2012 as ground truth. The new links are predicted based on the previous observations and the graph in February 2012. Finally, we use ROC curve to demonstrate each graph's result as shown in Figure 6.

From Figure 6 we can observe that the performance of the unweight graph (UW) is the worst while the weighted graph with all kinds of nodes and edges (AW) performs the best, which means that our method of calculating each edge's weight is basically effective. Furthermore, UUW containing the weighted user-user edge only performs better than UW but much worse than AW, which shows that using both the information in physical world and virtual world in link prediction can provide much better results. This also proves that user's activities in physical world have impact on his/her virtual world activities. On the other hand, we can draw a conclusion that user's activities in the virtual world can influence user's activities in the physical world by comparing the performance of AW and ULW (the graph with only weighted user-location edges).

7. Conclusion

In this paper, we present a study investigating how user's activities in virtual world and physical world impact each other. We use information vector to represent nodes and to store all the edges that are linked to every node. We define popularity entropy to weigh each node's popularity according to the amount of nodes it connects and the occurrence times of edges linked to it. Then, we calculate each edge's weight considering its linking nodes' popularity entropy and their shared nodes' features. In this way, we get a weighted graph and use it for link prediction. The results show that user's activities in virtual world and physical world do have impact on each other and using both virtual world and physical world information can improve the accuracy of link prediction.

In the future, we plan to detect and analyze communities formed by the nodes of online social network to see whether user's activities in virtual and physical world have impact on community dynamics. Real applications that employ the results will also be a future work of this study.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was partially supported by the National Basic Research Program of China (no. 2012CB316400), the National Natural Science Foundation of China (nos. 61103063, 61222209, 61373119, and 61332005), the Specialized Research Fund for the Doctoral Program of Higher Education (no. 20126102110043), and Microsoft Corporation.

References

[1] D. Zhang, B. Guo, and Z. Yu, "The emergence of social and community intelligence," *IEEE Computer*, vol. 44, no. 7, pp. 21–28, 2011.

[2] M. E. J. Newman, "The structure and function of complex networks," *SIAM Review*, vol. 45, no. 2, pp. 167–256, 2003.

[3] M. McPherson, L. Smith-Lovin, and J. M. Cook, "Birds of a feather: homophily in social networks," *Annual Review of Sociology*, vol. 27, pp. 415–444, 2001.

[4] D. Liben-Nowell and J. Kleinberg, "The link-prediction problem for social networks," *Journal of the American Society for Information Science and Technology*, vol. 58, no. 7, pp. 1019–1031, 2007.

[5] Q. Li, Y. Zheng, X. Xie, Y. Chen, W. Liu, and W.-Y. Ma, "Mining user similarity based on location history," in *Proceedings of the 16th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS '08)*, pp. 298–307, ACM Press, November 2008.

[6] E. Cho, S. A. Myers, and J. Leskovec, "Friendship and mobility: user movement in location-based social networks," in *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '11)*, pp. 1082–1090, ACM Press, August 2011.

[7] D. Lian and X. Xie, "Learning location naming from user check-in histories," in *Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS '11)*, pp. 112–121, ACM Press, November 2011.

[8] R. Xiang, J. Neville, and M. Rogati, "Modeling relationship strength in online social networks," in *Proceedings of the 19th International World Wide Web Conference (WWW '10)*, pp. 981–990, ACM Press, April 2010.

[9] J. Tang, T. Lou, and J. Kleinberg, "Inferring social ties across heterogeneous networks," in *Proceedings of the 5th ACM International Conference on Web Search and Data Mining (WSDM '12)*, pp. 743–752, ACM Press, February 2012.

[10] M. Roth, D. Deutscher, G. Flysher, I. Horn, and A. Leichtberg, "Friends using the implicit social graph," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '10)*, pp. 233–242, ACM Press, July 2011.

[11] J. Cranshaw, E. Toch, J. Hong, A. Kittur, and N. Sadeh, "Bridging the gap between physical location and online social networks," in *Proceedings of the 12th International Conference on Ubiquitous Computing (UbiComp '10)*, pp. 119–128, ACM Press, October 2010.

[12] D. Wang, D. Pedreschi, C. Song, F. Giannotti, and A.-L. Barabási, "Human mobility, social ties, and link prediction," in *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '11)*, pp. 1100–1108, ACM Press, August 2011.

[13] S. Scellato, A. Noulas, and C. Mascolo, "Exploiting place features in link prediction on location-based social networks," in *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '11)*, pp. 1046–1054, ACM Press, August 2011.

[14] G. Salton and C. Buckley, "Term-weighting approaches in automatic text retrieval," *Information Processing and Management*, vol. 24, no. 5, pp. 513–523, 1988.

[15] H. Tong, C. Faloutsos, and J.-Y. Pan, "Fast random walk with restart and its applications," in *Proceedings of the 6th International Conference on Data Mining (ICDM '06)*, pp. 613–622, IEEE Press, December 2006.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 695240, 11 pages
http://dx.doi.org/10.1155/2014/695240

Research Article

Intrusion-Tolerant Jini Service Architecture for Integrating Security and Survivability Support in DSN

Sung-Ki Kim,[1] Byung-Gyu Kim,[2] and Byoung-Joon Min[3]

[1] *Division of IT Education, Sun Moon University, 100 Kalsan-ri, Tangjeong-myeon, Asan-si 336-708, Republic of Korea*
[2] *Department of Computer Science and Engineering, Sun Moon University, 100 Kalsan-ri, Tangjeong-myeon, Asan-si 336-708, Republic of Korea*
[3] *Department of Computer Science and Engineering, Incheon National University, 119 Academy-ro, Yeonsu-gu, 406-772 Incheon, Republic of Korea*

Correspondence should be addressed to Byoung-Joon Min; bjmin@incheon.ac.kr

Received 30 August 2013; Accepted 3 December 2013; Published 22 January 2014

Academic Editor: James J. Park

Ubiquitous service environment based on DSN (distributed sensor networks) is poor in reliability of connection and has a high probability that the intrusion and the system failure may occur. In this paper, we propose an intrusion-tolerant Jini service architecture for integrating security and survivability support in order to provide end users with Jini services having a persistent state in ubiquitous environments. The proposed architecture is able to protect Jini service delivery not only from faults such as network partitioning or server crash but also from attacks exploiting flaws. It is designed to provide performance enough to show a low response latency so as to support seamless service usage. Through the experiment on a testbed, we have confirmed that the architecture is able to provide high security and availability at the level that the degradation of services quality is ignorable.

1. Introduction

Jini [1], also called Apache River [2], is a java-based middleware supporting share of resources such as ubiquitous devices and software on networks while it copes with the heterogeneity of the lower levels such as the various types of devices or communication protocols. A service that can cause us to use these pervasive resources is called the ubiquitous service. Jini provides a mechanism that discovers available services through the lookup services and make a connection to the services that clients requested.

It is important to enhance the survivability of the ubiquitous service because we live depending on the ubiquitous service environment providing valuable services through pervasive use of computation in everyday experiences.

However, the networked systems in the environment are apt to be partitioned due to a poor reliability of connection and have a high probability that the intrusion against a system providing services and the failure of the services may happen [3]. Therefore, it is very important to guarantee that the legitimate users make use of trustable services without discontinuance or obstacle of the services they are enjoying.

The standard Jini has two main problems in regard to these requirements. First, the Jini does not support building of fault tolerance services to mask the failure of services leased for resource use [4]. Second, the Jini has an insufficient security mechanism that cannot support dynamic trust establishment within a Jini system [5].

The former problem means that clients cannot keep using their service they are enjoying persistently when a Jini system is partitioned due to both communication link failures and server (service provider) crash failures. To solve this problem, the Jini system should have a mechanism that makes all service components in the system aware of failure events such as both network partition and server crash in a timely manner, and which replicated servers in the Jini system can maintain the user service states on behalf of failed servers persistently. The standard Jini architecture has not a real-time fault detection mechanism and does not support the replication of services for developing fault tolerant service.

The later problem is a security problem caused by the characteristics of Jini technology that sets free developing of a Jini system from the addition, modification of services, and the federation among all existing other services on networks. To respond to the security threats, the Jini system must have a security mechanism that is not only able to establish the trust among entities comprising a Jini system so that malicious services and their proxies are not introduced into the system, but also to respond to the intrusion exploiting flaws in the system.

The Jgroup/ARM framework [6] presented a middleware technology supporting the building of a dependable service in a distributed environment by introducing a concept that is called Java-based object group platform. A set of distributed objects making a group takes the responsibility for a service. It provides a good framework to solve the first problem of the standard Jini system as mentioned above. However, there are some shortcomings to apply this framework in the real environment directly. The first shortcoming is in which the omission of the design that the security provision responding to the intrusion has not been considered in the framework design. The Jgroup/ARM framework focuses on how to reach agreement among the service states of each of the Jini service entities, while the system that is built by this framework tolerates the events such as network partition or server crash, so it does not consider the problems of security. The system that is made through this framework is of greater danger more than the standard Jini system because it is defenseless against intrusion due to no security mechanism and it can be easily compromised caused by group communication protocols performing share of service state data among replicated service objects as well. Once an attacker has succeeded in the intrusion just in a part of the system, the entire Jini distributed systems may be seriously compromised. The second shortcoming is in which the overhead causes both the unnecessary computation and communication costs to delay the reply to the clients. The third shortcoming is in which both the computation and communication costs are needed to merge the user service states among replicas are very high, when the partitioned replicas are merged into one group after a network is recovered, and in the case of having a lot of clients keeping connections to the replicas.

In this paper, we present the solutions to improve the shortcomings that the Jgroup/ARM framework has and then propose a secure Jini service architecture providing ubiquitous services having a persistent state, while it establishes the dynamic trust in a Jini system and tolerates the failures and intrusions. In addition, we discuss the experimental results in terms of the proposed intrusion-tolerant Jini service architecture. Section 2 briefly describes the standard Jini service environment and points out its problems and then discusses the related work. Section 3 introduces the Jgroup/ARM framework and briefly describes what it overcomes when the standard Jini system meets the failure conditions such as network partition or server crash, and then it analyzes their shortcomings. In Section 4, we introduce our secure Jini service architecture. Section 5 discusses the experimental results in terms of our architecture that has been introduced in Section 4. Section 6 concludes the paper.

2. The Problems and Related Work

2.1. The Standard Jini Service Environment. A Jini system consists of the lookup servers, clients, and servers in which service codes are implemented. The servers and clients discover the presence of lookup servers in the ubiquitous network environment by performing the discovery protocol. After discovery of any lookup server anywhere, the servers and clients download a lookup service proxy that the lookup server provides. Afterward, the servers register their own service proxies with the lookup server and the clients discover a set of available service implementations through the lookup service proxy. At this time, if a client selects a specific service of available services, the client gets a service proxy that the corresponding server had registered from the lookup server. Subsequently, the clients call the remote service implementation through the downloaded service proxy. All request/response messages are transferred to be transparent to the lower layer protocols by using Java RMI (remote method invocation) protocols.

A scope that a server or a client can discover a lookup server depends on how far a multicast discovery message can be transferred. In generally, a range of these messages depends on the TTL parameter of multicast discovery packets. However, the lookup servers, servers, and clients comprising a Jini system have to be included in a same multicast group and the routers have to support the delivery of the multicast discovery packets. Thus, the distributed lookup servers on networks can discover the presence of each other and federate the services they introduce through the discovery protocol execution, but even so the scope of the Jini service environment cannot help, but it is limited to the edge of a manageable network.

If the limitations of the lookup server discovery and the service federation as mentioned above are solved through the interdomain cooperation, the scope of a Jini service environment can be more expanded because the range of multicast discovery messages is limited, but the range of RMI messages is not limited.

2.2. The Problems in the Jini Service Environment. Problems in the Jini service environment can be divided into four categories, namely, how to enhance the availability, quality, and security of Jini services and how to ensure the consistency of Jini service states.

The main causes of decreasing the availability of Jini services include the case of which the Jini distributed systems are broken due to both network partition and server crash failures. In general, a solution for enhancing the availability of services by overcoming these problems is to build the system based on the replication of the service [7]. However, the replication of the service carries how to ensure the consistency of replicated service states.

The Jini service environments overcome the heterogeneity of devices by using the JVM (Java Virtual Machine). System development in java in order to overcome the heterogeneity of devices reduces the burden of system development, but it may provide attackers with security holes that will help to exploit flaws in different types of devices comprising the system. For example, a method to hide attacker's intents in native code in which a Java runtime code calls through JNI (Java Native Interface) is an untouchable security flaw in java-based systems [8]. The reason is that no technologies based on java language can guarantee the security of native code below JVM layer, but they can guarantee the security of code above it. The Jini service environment sets free the discovery, addition, and modification of services on ubiquitous networks on the basis of mobile codes such as service proxies while they bear these risks. Therefore, the Jini systems must have a mechanism not only to provide security services such as enforcement of authentication and authorization among the Jini entities, ensuring of confidentiality and integrity for exchanged messages, but also to respond to intrusion.

The building of a Jini service environment considering the four problems as mentioned above generates the trade-off problems. In other words, applying the replication to the Jini services to enhance the availability makes it more difficult to ensure the consistency of their states and increases the targets that will have to protect from the viewpoint of security. In addition, increasing the degree of replication and enhancing the security incur reducing the quality of services due to considerable delays that is required to reply to the clients.

2.3. Related Work. We have not found works resolving all four problems as mentioned in Section 2.2 yet. Meling et al. [6] proposed Java-based middleware architecture and a programming model, which ensure consistency among the replicated service states in spite of applying replication to service objects in order to enhance their availability. We discuss in detail this work in Section 3.

Kolltveit and Hvasshovd [9] discussed the experimental results on the response time that was measured at the client from transaction initiation to transaction completion on condition that the two different servers can have up to two replicas each and a transaction manager (TM) can have up to four replicas on the middleware architecture that [6] proposed. This work also has investigated whether the response times are allowable latency that can satisfy a seamless service use under failover operations with recovery activities.

Meling and Helvik [10] presented the techniques to maintain consistency between the dynamic server-side group membership and its representations both at the client-side and in the registry as equivalent to the lookup server in the event of server failures and recoveries.

In order to solve the single point of failure problem of servers, Tichy and Giese [11] introduced an approach to which a client has multiple connections to replicated servers as applying the client to smart-proxy providing that function. The ensuring of consistency among the replicated servers relies on the communication protocols that are performed between the servers and the smart-proxy.

Several works [12–14] were carried out on how to enhance the security in the standard Jini system. The security requirements for the Jini system that had been suggested in these works commonly are as follows:

(1) trust establishment among the client, the service proxy and the server;

(2) access control to services;

(3) protecting the client from mobile code;

(4) ensuring the confidentiality and integrity of communication.

The security requirement (1) means that the Jini system needs to have the authentication mechanism that establishes the trust among the Jini entities. The security requirement (2) means that the Jini system needs to have the authorization mechanism forcing authenticated users to make use of services within their own right. The security requirement (3) means that a mechanism is necessary for preventing the client from the execution of download proxy codes that may impair them but are authenticated. The security requirement (4) means that all exchanged messages in Jini system have to be protected from tempering by attacker through cryptography technology.

Hasselmeyer et al. [12] presented a Jini service architecture that meets the security requirement associated with access control and trust establishment among server, service proxy, and lookup server through centralized security server providing authentication and authorization services in the Jini system.

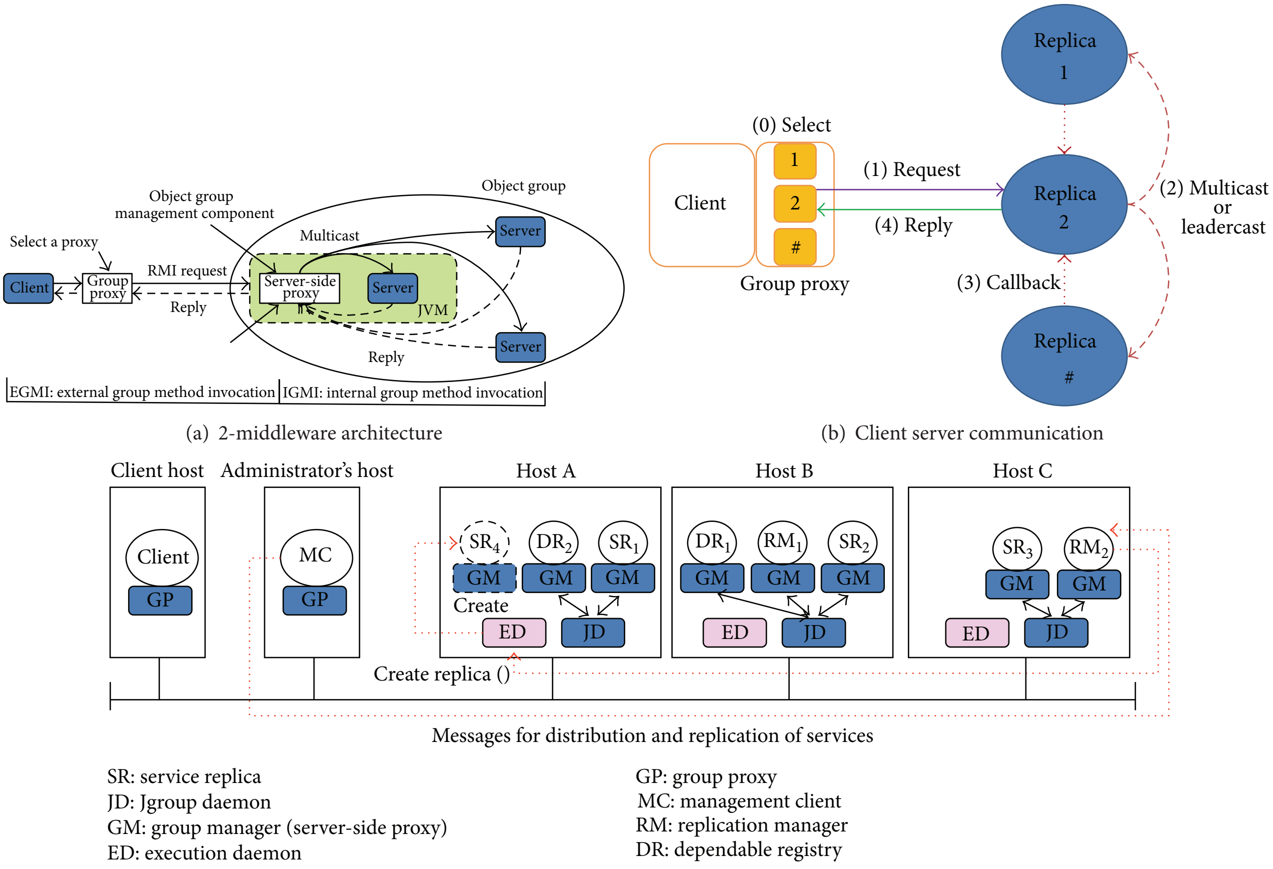
Eronen and Nikander [13] proposed a method that establishes an authentication-authorization chain among users, service proxies, and servers by using the SPKI (Simple Public key infrastructure) certificate in Jini system.

Schoch et al. [14] presented a Jini service architecture similar to that of [12]. However, in this architecture, both the mechanism ensuring the confidentiality and integrity of communication and the client-side proxy supporting considerable security features so as not to break client transparency differ from those of the other works [12, 13].

As regards the safety of download proxy code, [12–14] are based on an assumption that all the authenticated proxy codes are trustable from the view point of safety in the client side. To support the security of communication, the communication implementation in [12] is based on the SSL-based Java RMI implementation using Java-based open source API. In [13], the communication implementation is based on the TLS-based Java RMI implementation using the standard JSSE (Java socket security extension) API. The implementation in [14] uses the DH (Diffie-Hallman)-based algorithm and HMAC-MD5 algorithm to ensure the confidentiality and integrity of all exchanged messages, respectively.

The Jini technology has reinforced the supports to meet four security requirements as mentioned above. Especially, a constraint-based remote invocation mechanism for protecting clients from mobile codes has been added.

There are two works on intrusion tolerance systems based on diverse server replication. One example is HACQIT (hierarchical adaptive control of quality of service for intrusion tolerance) project [15], and another example is SITAR (scalable intrusion tolerance architecture) [16]. The method to commit secure result with replicated servers is found in [17]. A coordination model for improving software



(a) 2-middleware architecture

(b) Client server communication

(c) Architectural features for fault tolerance

FIGURE 1: The Overview of the Jgroup/ARM system.

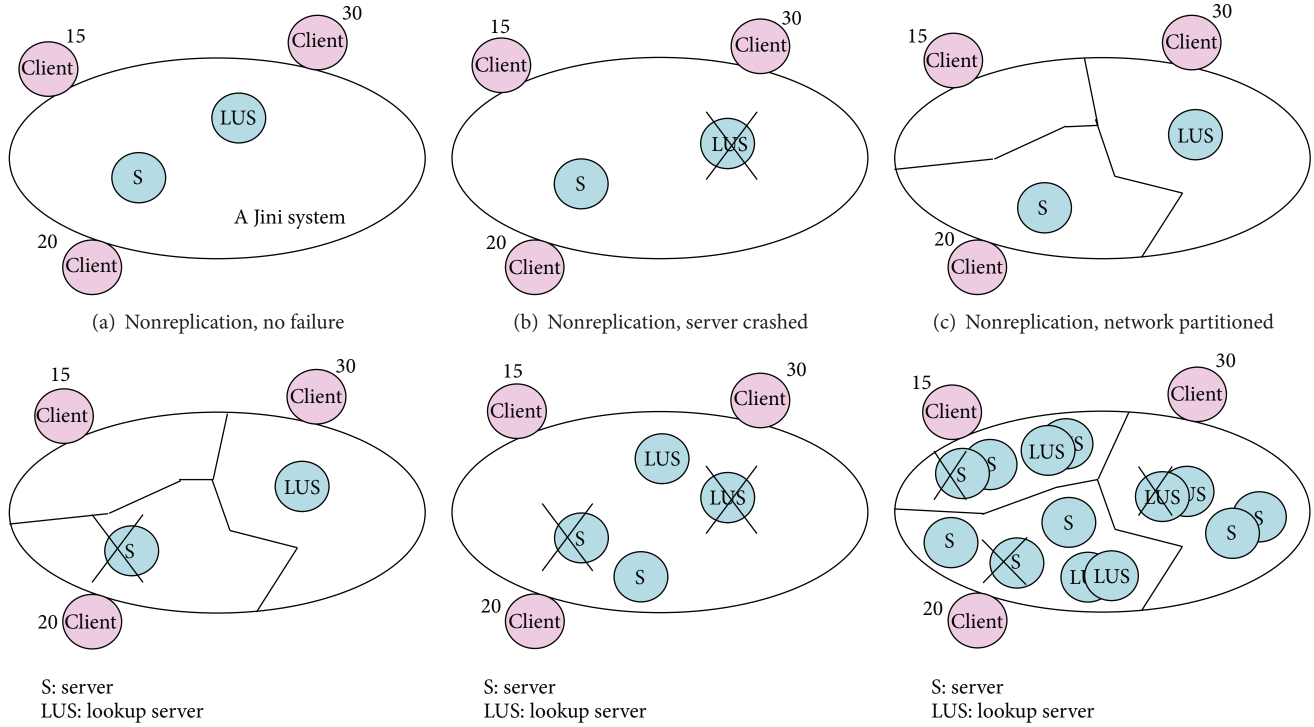
system attack-tolerance and survivability is also found in [18]. An analysis of replication enhancement for a cluster-based high availability service is found in [19]. The method for cost-saving key agreement via secret sharing in two-party communication systems is found in [20].

3. The Jgroup/ARM System

3.1. The Jgroup/ARM System Architecture. The architectural features of the Jgroup/ARM system are summarized in Figure 1. As shown in Figure 1(a), the Jgroup/ARM system supports 2 middlewares: one is for client-server communication; the other is for communication among replicated service objects. If a proxy is selected from the group-proxy in the client-side, the selected proxy sends an RMI request corresponding to their service replica. The server-side proxy (GM in Figure 1(a)) in the corresponding replica dispatches the request message to their group members by using multicast or leadercast delivery. The use of multicast delivery means that the replica that is selected from client-side proxy has responsibility of dispatching a request message to other members of replica group in the server-side (SR in Figure 1(c)) and merging the results from them. The use of leadercast delivery means that the replica that is selected from client-side proxy performs their service and then shares the result of their service with other group members. Figures 1(a) and 1(b) illustrate this concept. In order to overcome failure situation that cannot deliver the implemented service, Jgroup/ARM system supports a fault tolerance mechanism such as failure detection, reliable group membership communication, and dynamic resource reallocation. Figure 1(c) illustrates these features.

3.2. The Contribution of Jgroup/ARM System. In this section, we do not describe how Jgroup/ARM system overcomes the failure events such as both network partition and server crash in detail. We just discuss what the Jgroup/ARM framework contributes to the standard Jini system and then point out the shortcoming this framework.

Figures 2(a)–2(d) illustrate service failure situations that may happen in the standard Jini service environment. In Figure 2(a), all 65 users can make use of a Jini service without any problems. However, when a lookup server is crashed as shown in Figure 2(b), all existing users keeping connections to the server can make use of the service within a given lease time. In the case of Figure 2(c), 15 users lose their connection and the opportunities that they can discover other services again. 30 users lose their connection to the server and only can rediscover unreachable service, and the presence of the service disappears from the lookup server. Only 20



(a) Nonreplication, no failure

(b) Nonreplication, server crashed

(c) Nonreplication, network partitioned

(d) Nonreplication, server crashed and network partitioned

(e) Partially replication, server failover

(f) Full replication, failure tolerance

Figure 2: Service failure and tolerance in a Jgroup/ARM Environment.

users can make use of the service within a given lease time. In the case of Figure 2(d), all users lose their connection to the server and only 30 users can rediscover unreachable service. In the case of Figure 2(e), some users are subject to restriction on making use of services according to how a Jini network is partitioned, but the situation that servers are crashed can be overcome. In the case of Figure 2(f), the Jini system overcomes failure events such as a specific server's crash and network partition by replicating the tasks providing the services on distributed computing nodes. The Jgroup/ARM system supports the case of Figure 2(f). In Figure 2(f), though considerable service resources are replicated, the Jgroup/ARM system can support the autonomous management of available resources so as to overcome all failure events through a dynamic service deployment and reconfiguration.

The service replication for supporting the case of Figure 2(f) in the standard Jini service environment without use of the Jgroup/ARM framework is possible. However, this approach generates the following two problems. First, in the standard Jini service environment, the lookup server introduces users to the failed servers repeatedly until the lease time of their proxies given by the lookup server is expired. Second, the users become aware of the failure of services after their proxies disappear in the lookup server because no components comprising the system can detect the failure event such as both network partition and server crash in timely manner. After all, it is hard for users to look forward to the quality of services.

3.3. A Definition and Examples for Discussion

Definition. In this section, we define the notion of a group of the distributed service objects for the further discussions as follows:

$$G_s \longrightarrow \{R_1, R_2, R_3, \ldots, R_n\}^e, \tag{1}$$

where G_s is a server group that consists of a group of n replicated service objects, R_n: the nth replica which is a member of G_s, e is the number of endpoints (i.e., service instances) that is created in each R_n in order to establish connection from clients under the no failure condition that the system is not partitioned.

Example 1. The expression, $G_s \rightarrow \{R_1, R_2, R_3, \ldots, R_7\}^{20}$ means that all of 7 replicas takes the responsibility for a service and each replica has equally 20 connections from clients. This expression describes normal scenarios under no failure condition.

Example 2. The expression, $G_s \rightarrow \{\{R_1, R_2\}_a^3, \{R_3, R_4, R_5\}_b^7, \{R_6, R_7\}_c^{10}\}$, means that one server group is partitioned into 3 partitioned subgroups that take the responsibility for a service. This expression describes failure scenarios that the system is partitioned due to the intrusions and the system failures. In this scenario, replicas in each partitioned subgroup have endpoints enough to connect to their clients according to how a Jini network is partitioned. In this example, each replica in the subgroups*a*, *b*, and *c* has 3, 7, and 10 endpoints to connect to their client side proxy, respectively.

3.4. The Shortcomings of Jgroup/ARM System

The Computational Overhead for Merging Distributed Service States of End User. When the partitioned subgroups are merged into one group after the network failure is recovered, the Jgroup/ARM system faces a significant problem in bearing a heavy computation overhead for merging distributed service states of end user. For recovery, the Jgroup/ARM system has a 2-phase merging operation as follows:

(i) merging operation between leader replicas (e.g., R_1-R_3-R_6);

(ii) merging operation between a leader and members (e.g., R_1-R_2, R_3-R_4-R_5, and R_6-R_7).

The time-cost for these 2-phase merging operations in the Jgroup/ARM system can be estimated as follows:

$$\text{Time} - \text{Cost}_{(\text{Jgroup System})} = \sum_{i=1}^{p} \left\{ e_i^p * \left(e - e_i^p \right) * (mdt + c) \right\}, \quad (2)$$

where p is the number of partitioned groups, e_i^p is the number of endpoints in each R_n of the *i*th partitioned subgroups after network is partitioned, and c is a required time to make the service instances in each endpoint, and also *mts* means multicast delay time for message delivery in group communication.

Latency in Callback Handler. In the Jgroup/ARM system, a group proxy [10] for the use of a service is offered, and a selected proxy in the group of proxies sends the requests to server-side replica corresponding to it. The selected replica replies their service result on behalf of all of members after the callback handler in the selected replica receives the service results from all members. This latency in callback handler operation is a cost to pay for fault detection and failover provision.

The Lack of the Security Mechanism. The group communication among replicas relies on the Jgroup Daemon (JD) in every node hosting services [6]. However, the JD supporting group multicast communication does not ensure the confidentiality and integrity of messages. In addition, there is no authentication mechanism providing the trust among replicas. Thus, attackers can easily intrude into the system by tempering all communication messages and configuration files.

4. Our Proposed Architecture

4.1. Architectural Features. The goal of our proposed architecture is to support the integrated services that can provide security and service survivability in order to respond against intrusion and failure scenario. To achieve this goal, we have developed the extension of Jgroup/ARM framework. Figures 3 and 4 show a high-level system overview and architectural extension for security.

As shown in Figure 3, the service replicas can be distributed on necessary computing nodes and the service object repository (SOR) as a service manages the reposition of these distributed service replicas. According to the configuration supporting domain administration policy, these service replicas can be activated or inactivated by control from replication manager (RM). Unlike the Jgroup/ARM architecture, our system supports secure group membership communication in the underlying communication mechanism. Figure 4 illustrates our architectural extension for security and service state management. To support key management for secure group communication, we have adopted the use of the contributory group key agreement protocol [21] in the secure reliable group membership multicast layer.

The service provider provides their service state data to group manager (GM) through setServiceState (SID, KEY, STATE) method. SID is a service ID and KEY is a shared group key used while being on communication. STATE is a reference to a context container that caches service state data including session ID. These service state data is stored in GM's service state repository (SSR) which has interaction with the smart proxy in the client-side. GM gets the data associated with user service state from smart proxy when the absentee data are needed in merging operation.

4.2. An Extension to Session-Based Allocation of Replica Instances. In comparison with the Jgroup/ARM architecture, one of extended features in our proposed architecture is to support the identification and management of endpoints in each replica on the basis of the session while maintaining group membership among replicas regardless of merging subgroups. In our system, a smart group proxy in the client-side manages the user service states whenever it receives reply messages in order to solve the problem above. The smart group proxy is a group of smart proxies. Each smart proxy as a wrapper around a stub performs the predefined functions associated with remote service implementation (i.e., service provider) after the reception of reply message. The predefined function manages a cache for saving the user service states associated with remote service implementation. This cache can be used as a backup to help in the recovery of the user service state when the partitioned subgroups are merged into a single group. That is, just like the use of cookie in the web application, the user service state data cached in each smart proxy can be offered to leadercast contributor which has responsibility of the distribution of the absentee data as shown in Table 1.

Figures 5 and 6 show our architecture and contribution in comparison with Jgroup/ARM system through Example 2 in Section 3.3 and expression (2) in Section 3.4, respectively.

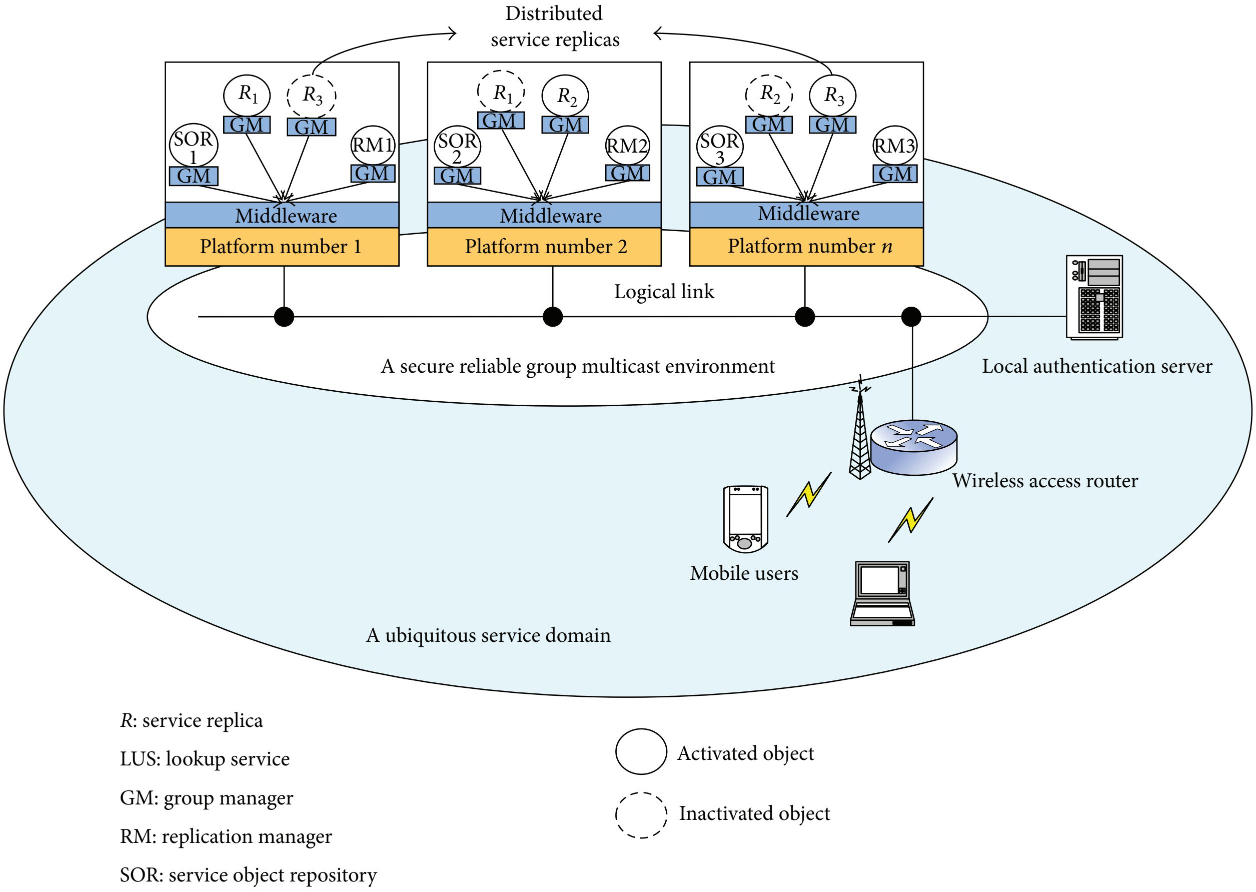


Figure 3: Our system overview.

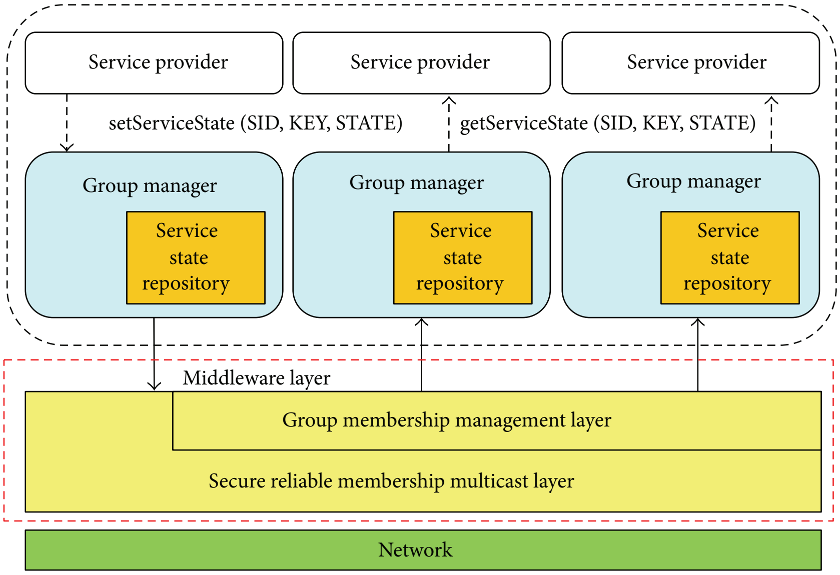


Figure 4: Architectural extension for secure group membership communication.

TABLE 1: A Simple simulation that is to be illustratedin Figure 6.

Replica	No failure condition	Before recovery	After recovery	Absentee data	Leadercast contributor
R_1	U_1	U_1, U_2	$U_1, U_2, U_5,$	U_3, U_4	R_3, R_6
R_2	U_1	U_1, U_2	$U_1, U_2, U_5,$		
R_3	U_1	U_1, U_3	$U_1, U_3, U_5,$	U_2, U_4	R_1, R_6
R_4	U_1	U_1, U_3	$U_1, U_3, U_5,$		
R_5	U_1	U_1, U_3	$U_1, U_3, U_5,$		
R_6	U_1	U_1, U_4	$U_1, U_4, U_5,$	U_2, U_3	R_1, R_3
R_7	U_1	U_1, U_4	$U_1, U_4, U_5,$		

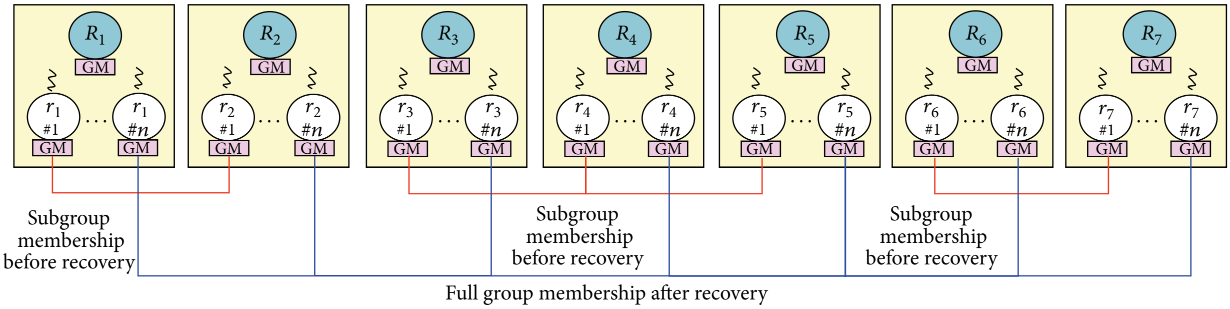


FIGURE 5: Session-based allocation of replica instances and their membership management.

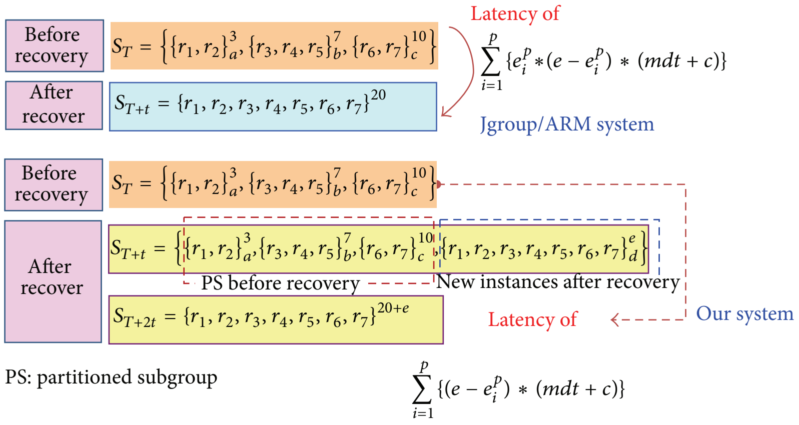

Before recovery
$S_T = \left\{\{r_1, r_2\}_a^3, \{r_3, r_4, r_5\}_b^7, \{r_6, r_7\}_c^{10}\right\}$
After recover
$S_{T+t} = \{r_1, r_2, r_3, r_4, r_5, r_6, r_7\}^{20}$
Latency of
$\sum_{i=1}^{p} \{e_i^p * (e - e_i^p) * (mdt + c)\}$
Jgroup/ARM system
Before recovery
$S_T = \left\{\{r_1, r_2\}_a^3, \{r_3, r_4, r_5\}_b^7, \{r_6, r_7\}_c^{10}\right\}$
After recover
$S_{T+t} = \left\{\{r_1, r_2\}_a^3, \{r_3, r_4, r_5\}_b^7, \{r_6, r_7\}_c^{10}, \{r_1, r_2, r_3, r_4, r_5, r_6, r_7\}_d^e\right\}$
PS before recovery
New instances after recovery
$S_{T+2t} = \{r_1, r_2, r_3, r_4, r_5, r_6, r_7\}^{20+e}$
Latency of
Our system
PS: partitioned subgroup
$\sum_{i=1}^{p} \{(e - e_i^p) * (mdt + c)\}$

FIGURE 6: Reduction of time-cost for merging the user service states.

Table 1 illustrates Figure 6 above. In Table 1, U means users who send requests through client for use of a service, and the prefix i indicates a number to identify individuals. The time-cost for merging the user service states in our system can be estimated as follows:

$$\text{Time} - \text{Cost}_{(\text{our system})} = \sum_{i=1}^{p} \left\{\left(e - e_i^p\right) * (mdt + c)\right\}. \quad (3)$$

4.3. Callback Handler for Intrusion Tolerance. Our proposed architecture applies the byzantine agreement algorithm [17, 22] and design diversity to service implementation in order to mask results introduced from compromised server due to intrusions. To accomplish this goal, we have added an additional function to callback handler in order to act as a voter masking the compromised results. When the number of total replica is N and the number of compromised replica is T of N, if there are replicas of more than 2/3 N to satisfy a condition that $N > 3T$, callback handler replies the service results to client.

4.4. Security Architecture for Secure Communication. Our proposed architecture supports security provisions to satisfy the goals for providing secure Jini services such as authentication, access control and confidentiality as shown in (see Figure 7).

Unlike server-side group communication feature as mentioned in Section 4.1, in our system, the communication between client and server uses a protocol as shown in Figure 7.

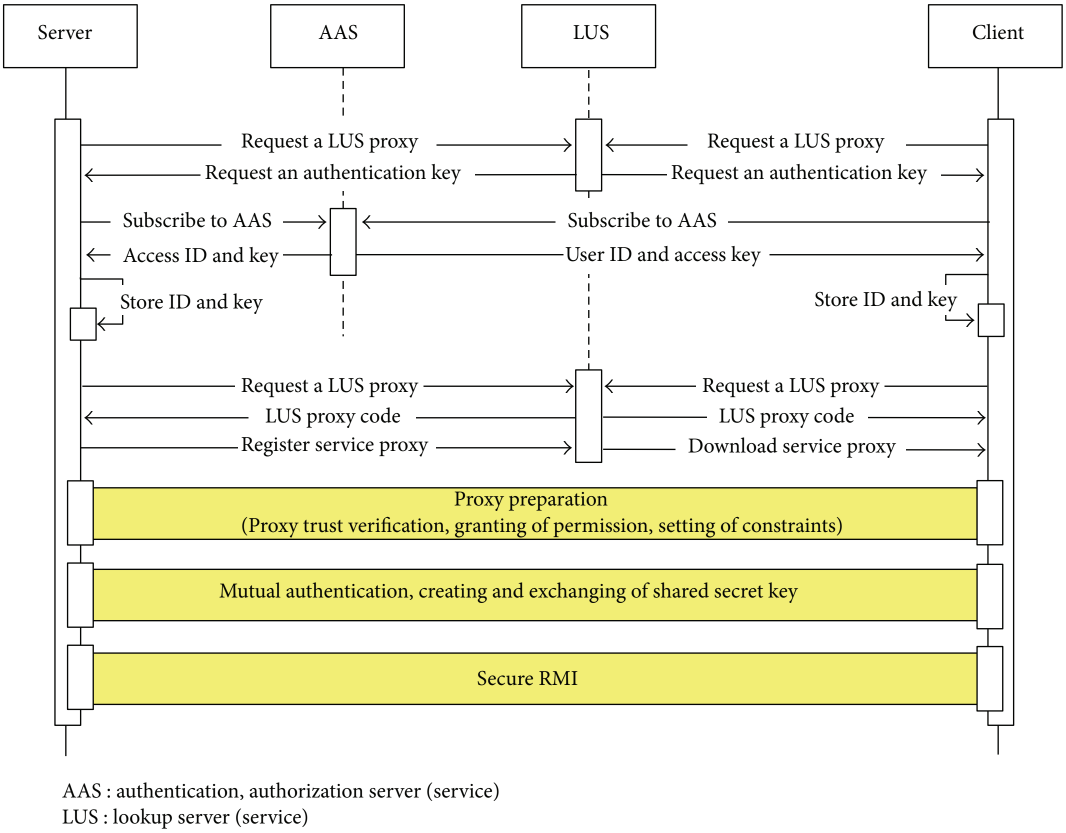


Figure 7: Architecture for Secure Communication between Client and Server.

5. The Discussion on Experimental Results

5.1. Performance Analysis. We have experimented with measures of user state merging times and turnaround times. When a recovery operation to merge the user service states has been performed under system-partitioned condition as shown in Figure 8, it has been shown that the time-cost for recovery operation in our system is 2 times lower than one in Jgroup/ARM system in proportional to e (i.e., the number of users in condition that a user has one connection to the service) of expression (1). In Figure 8, "our systems 2PG, 3P/PG" are meant for the condition that our system has been partitioned into 2 partitioned subgroups and each partitioned subgroup has 3 service replicas.

Figure 9 shows measurement results of turnaround time in concern with leadercast, multicast, and voting application in condition that the security protocol of Figure 7 has not been applied. In Figure 9, if the number of replica increases, the leadercast application shows that the turnaround time is reduced because the resource allocation for serving client's requests is distributed among replicas. In contrast, the multicast application shows that the turnaround time is increased because the client's requests are allocated in all replicas. In particular, the voting application shows that the turnaround time is not impacted by the number of replica because of callback handler for intrusion tolerance as mentioned in Section 4.3.

Table 2: Time cost for seamless service use.

Measurements	Latency
Failover	180 ms
Failure detection	160 ms
Reception of stateful service from other replica	340 ms

5.2. The Implementation Results. Table 2 shows results measured while a file transfer service is keeping up its mission in spite of a server-crashed failure. In this experiment, when a system consists of one client and two replicated services in 100 Mbps Ethernet environment, it has been shown that the failover latency is 340 ms (160 ms for failure detection + 180 ms for receiving stateful service from other replica) for seamless service usage.

6. Conclusion

Ubiquitous service environment based on DSN is poor in reliability of connection and has a high probability that the intrusion and the system failure may occur. In this paper, we propose an intrusion-tolerant Jini service architecture for integrating security and survivability mechanisms in order to provide end users with trustable Jini services having a persistent state in DSN. The proposed architecture is able to protect a Jini system not only from faults such as network partitioning or server crash, but also from attacks exploiting

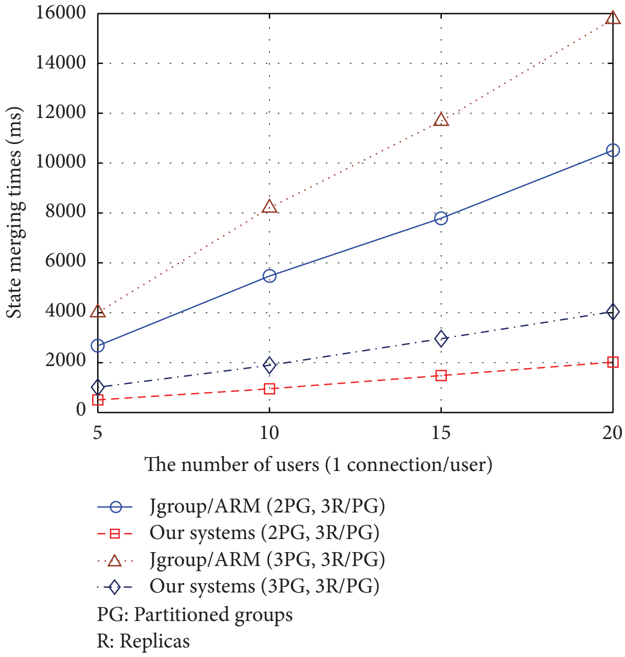


Figure 8: Time cost merging user service states.

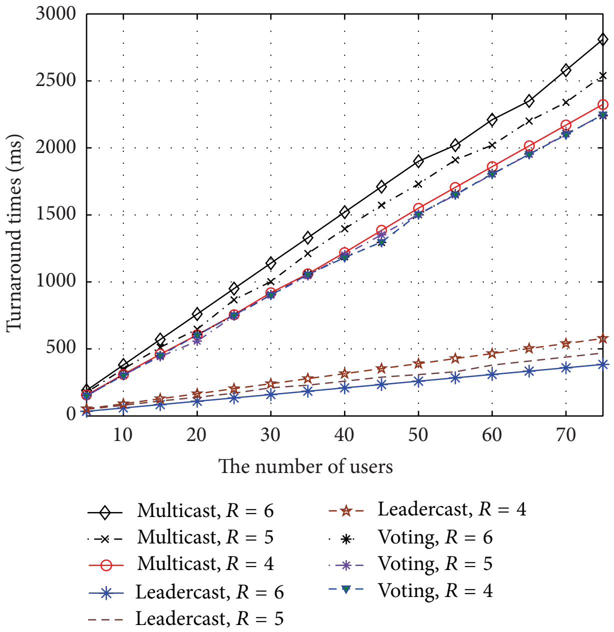


Figure 9: Turnaround time cost.

flaws. It is designed to provide performance enough to show a low response latency so as to support seamless service usage. We believe that our proposed architecture is a good reference model for building a better secure ubiquitous service infrastructure.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the Incheon National University Research Grant.

References

[1] Apache Software Foundation, "Apache Jini Specifications v2.1.2," http://river.apache.org/doc/spec-index.html.

[2] Apache Software Foundation, "Apache River User Guide," http://river.apache.org/user-guide-basic-river-services.html.

[3] K. Peng, "A secure network for mobile wireless service," *Journal of Information Processing Systems*, vol. 9, no. 2, pp. 247–258, 2013.

[4] D. Szentivanyi and S. Nadjm-Tehrani, "Middleware support for fault tolerance," in *Middleware for Communications*, Q. Mahmoud, Ed., chapter 28, John Wiley & Sons, 2004.

[5] F. Sommers, *Jini Starter Kit 2.0 Tightens Jini's Security Framework*, IEEE Computer Society Press, Los Alamitos, Calif, USA, 2003.

[6] H. Meling, A. Montresor, B. E. Helvik, and O. Babaoglu, "Jgroup/ARM: a distributed object group platform with autonomous replication managements," in *Software Practice and Experience*, John Wiley & Sons, 2007.

[7] J. Osrael, L. Froihofer, G. Stoifl et al., "Using replication to build highly available .net applications," in *Proceedings of the 17th International Conference on Database and Expert Systems Applications*, pp. 385–398, 2006.

[8] M. Schönefeld, "Hunting flaws in JDK," in *Proceedings of the Blackhat Europe*, May 2003.

[9] H. Kolltveit and S.-O. Hvasshovd, "Preventing orphan requests by integrating replication and transactions," in *Advances in Databases and Information Systems*, vol. 4690 of *Lecture Notes in Computer Science*, pp. 41–54, Springer, Berlin, Germany, 2007.

[10] H. Meling and B. E. Helvik, "Performance consequences of inconsistent client-side membership information in the open group model," in *Proceedings of the 23rd IEEE International Performance, Computing, and Communications Conference (IPCCC '04)*, pp. 777–782, April 2004.

[11] M. Tichy and H. Giese, "An architecture for configurable dependability of application services," in *Proceedings of the ICSE Workshop on Software Architectures for Dependable Systems*, pp. 65–70, Portland, Ore, USA, April 2003.

[12] P. Hasselmeyer, R. Kehr, and M. Voß, "Trade-offs in a secure jini service architecture," in *Trends in Distributed Systems: Towards a Universal Service Market*, vol. 1890 of *Lecture Notes in Computer Science*, pp. 190–201, Springer, Berlin, Germany, 2000.

[13] P. Eronen and P. Nikander, "Decentralized Jini security," in *Proceedings of the Network and Distributed System Security Symposium (NDSS '01)*, pp. 161–172, San Diego, Calif, USA, February 2001.

[14] T. Schoch, O. Krone, and H. Federrath, "Making jini secure," in *Proceedings of the 4th International Conference on Electronic Commerce Research*, pp. 276–286, November 2001.

[15] J. Reynolds, J. Just, E. Lawson, L. Clough, R. Maglich, and K. Levitt, "The design and implementation of an intrusion

tolerant system," in *Proceedings of the International Conference on Dependable Systems and Networks (DNS '02)*, pp. 285–290, June 2002.

[16] F. Wang and R. Upppalli, "SITAR: a scalable intrusion-tolerant architecture for distributed services," in *Proceedings of the DARPA Information Survivability Conference and Exposition*, 2003.

[17] B. J. Min, S. K. Kim, and C. Im, *Committing Secure Results with Replicated Servers*, vol. 3043 of *Lecture Notes in Computer Science*, Springer, Berlin, Germany, 2004.

[18] S. Ren, Y. Yu, K. A. Kwiat, and J. Tsai, "A coordination model for improving software system attack-tolerance and survivability in open hostile environments," *International Journal of Distributed Sensor Networks*, vol. 3, no. 2, pp. 175–199, 2007.

[19] S. Park, I. Y. Jung, H. Eom, and H. Y. Yeom, "An analysis of replication enhancement for a high availability cluster," *Journal of Information Processing Systems*, vol. 9, no. 2, pp. 205–216, 2013.

[20] Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, "Secure group communication using robust contributory key agreement," *IEEE Transactions on Parallel and Distributed Systems*, vol. 15, no. 5, pp. 468–480, 2004.

[21] Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, "Secure group communication using robust contributory key agreement," *IEEE Transactions on Parallel and Distributed Systems*, vol. 15, no. 5, pp. 468–480, 2004.

[22] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *Journal of the ACM*, vol. 27, no. 2, pp. 228–234, 1980.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 272537, 10 pages
http://dx.doi.org/10.1155/2014/272537

Research Article

A Signature-Based Data Security Technique for Energy-Efficient Data Aggregation in Wireless Sensor Networks

Min Yoon, Miyoung Jang, Hyeong-Il Kim, and Jae-Woo Chang

Department of Computer Engineering, Chonbuk National University, Chonju, Chonbuk 561-756, Republic of Korea

Correspondence should be addressed to Jae-Woo Chang; jwchang@jbnu.ac.kr

Received 26 July 2013; Revised 13 December 2013; Accepted 15 December 2013; Published 16 January 2014

Academic Editor: Jong Hyuk Park

Data aggregation techniques have been widely used in wireless sensor networks (WSNs) to solve the energy constraint problems of sensor nodes. They can conserve the significant amount of energy by reducing data packet transmission costs. However, many data aggregation applications require privacy and integrity protection of the real data while transmitting data from the sensing nodes to a sink node. The existing schemes for supporting both privacy and integrity, that is, iCDPA, and iPDA, suffer from high communication cost, high computation cost, and data propagation delay. To resolve the problems, we propose a signature-based data security technique for protecting sensitive data aggregation in WSNs. To support privacy-preserving data aggregation and integrity checking, our technique makes use of the additive property of complex numbers. Out of two parts of a complex number, the real part is used to hide the sampled data of a sensor node from its neighboring nodes and adversaries, whereas the imaginary part is used for data integrity checking at both data aggregators and the sink node. Through a performance analysis, we prove that our privacy-preserving data aggregation scheme outperforms the existing schemes up to 50% in terms of communication and computation overheads as well as up to 3 times in terms of integrity checking and data propagation delay.

1. Introduction

Wireless sensor networks (WSNs) have been widely studied in ubiquitous computing environment. The WSNs can be applied to various types of applications, such as environment management and military monitoring [1–4]. However, the sensor nodes that form WSNs have resource constraints such as limited power, slow processor, and less memory. For these reasons, it is essential to improve the energy efficiency of sensor nodes (or WSN) in order to enhance the quality of application service [5–10]. The first issue of WSNs is to reduce energy consumption in WSNs. Because the amount of energy consumption for communication is the greatest, it is important to reduce communication overhead. For reducing communication cost, transmitting the required and partially processed data is more meaningful than sending a large amount of raw data. In general, sending raw data causes the energy consumption of sensor nodes because duplicated messages are sent to the same node, called implosion, as well as neighboring nodes receive the duplicated messages if two nodes share the same observing region, called overlapping. In recent years, data aggregation has been actively used to combine data coming from many sensor nodes. An extension of this approach is in-network aggregation which aggregates data progressively as data are passed through the network [11–14]. In-network data aggregation can reduce the number of data transmissions and the number of nodes involved in gathering data from a WSN.

The second issue of WSNs is how to preserve sensitive measurements where data privacy becomes an important aspect from an adversary [15]. In many scenarios, the confidentiality of transported data can be considered critical. For instance, data from sensors might measure patients' health information such as heartbeat and blood pressure details. In addition, a future application might measure household details such as power and water usage, thus computing average trends and making local recommendations. Since sensitive data is transported wirelessly among sensor nodes, it is typically prone to interception and eavesdropping. It is mandatory to maintain the data privacy of sensor nodes even from other trusted participating sensor nodes of the WSNs. As a result, even though private data are overheard and

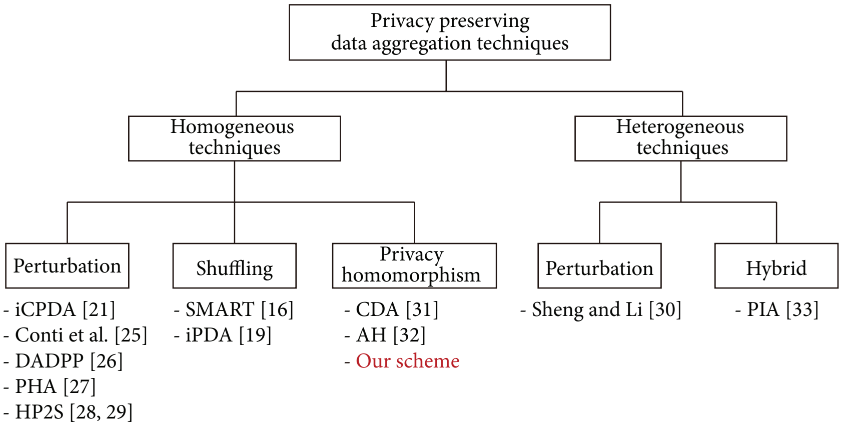


Figure 1: Classification of the privacy preserving-data aggregation techniques for WSNs.

decrypted by adversaries, it is necessary to prevent recovering the sensitive information of a sensor node [16–18].

The last issue of WSNs is data integrity [19–21]. In communication, data integrity is simply defined as maintaining consistency and correctness of messages (message without modification by adversaries). In other words, it is ensured that the received data is not altered in transit either by an adversary or by noise in the data collecting node, that is, sink node. Data pollution due to the noise is an unintentional process and it can be handled by using some existing mechanisms like cyclic redundancy checking (CRC). Hence, the integrity checking due to the unintentional data pollution is out of the scope of this research. On the other hand, the mechanisms like CRC are unable to cope with the intentional data pollution by an adversary because the adversary can generate the same CRC of the source node after modifying the data. As data aggregation result is used for making critical decisions, the aggregation result must be verified before accepting it. For this reason, it is required to design a data protocol for WSNs which can ensure that the aggregated result has not been polluted (manipulation of data by an adversary) on the way to the sink node.

Since data privacy and integrity protection processes consume a significant amount of precious resource (i.e., limited power) of sensor nodes, they shorten the lifetime of the WSNs. Therefore, it is necessary to devise a light-weight technique, which can achieve data privacy and integrity protection efficiently. However, the existing work needs much resource consumption of sensor nodes due to generating unnecessary messages in the network. For this reason, in this paper, we propose a resource-efficient data security technique that can aggregate sensitive data while protecting data integrity in WSNs. Our technique protects from the leak of the sensed data by using the algebraic properties of the complex numbers. Our technique not only ensures that no trend about the sensitive data of a sensor node is released to any other nodes and adversaries, but also can aggregate and hide data for data privacy during transmissions to the data sink. Out of two parts of a complex number, the real part is used to hide the sampled data of a sensor node from its neighboring nodes and adversaries, whereas the imaginary part is used for data integrity. Before transmitting data to a parent node, every sensor node transforms its sampled data into a complex number form. The real part is generated by combining the sampled data with a unique private seed and the imaginary part is generated by appending an imaginary unit to the modified sampled data. Thus, our technique prevents from recovering sensitive information even though private data are overheard and decrypted by adversaries or other trusted participants. For strong data security, our technique can be built on the top of the existing secure communication protocols like [22]. Moreover, our technique can be applied to any type of WSNs regardless of network topology since it is a general approach.

The rest of the paper is organized as follows. In Section 2, we present some related work. Section 3 describes our integrity-protecting sensitive data aggregation technique. Simulation results are shown in Section 4. Along with some future research directions, we finally conclude our work in Section 5.

2. Related Work

In this section, we present related work for privacy-preserving data aggregation schemes. Figure 1 illustrates the classification of the privacy-preserving data aggregation techniques for WSNs. These techniques are broadly categorized into two categories: homogeneous techniques and heterogeneous ones. They are categorized based on the type of nodes in the WSNs, particularly the type of data aggregating nodes (aggregators). The aggregators can either be special (more powerful) nodes or regular sensor nodes. Moreover, the techniques are further divided into five groups: perturbation in homogeneous technique, shuffling, privacy homomorphism, perturbation in heterogeneous, and hybrid. First, the perturbation technique is also known as data customization. In this technique, every sensor node uses encryption key and/or seeds (private or public) generated by randomization techniques [23, 24] in order to hide the sampled data before transmitting them to a parent node. The perturbation in homogeneous technique include iCPDA [21], Conti et al.'s scheme [25], DADPP [26], PHA [27], and HP2S [28, 29], while the perturbation technique in heterogeneous includes Sheng and Li's scheme [30]. Second, in the shuffling technique, every sensor node slices its data into the fixed number (J) of data pieces and sends a data piece to the selected $J - 1$ number of neighboring sensor nodes. The remaining one piece of data is kept with it. After that, every sensor node assembles the received data pieces including its own piece of data and sends the assembled data to a parent node. SMART [16] and iPDA [19] belong to the shuffling techniques. Third, the privacy homomorphism technique has a special feature that allows arithmetic operations to be performed on ciphertext without decryption. This technique is fast and resource-efficient for privacy-preserving data aggregation, but it has a limitation that it performs only addition and multiplication operations. Before the sensed data are sent to the aggregators, they are encrypted by using the respective keys of sensor nodes and they are added or multiplied without decryption. The CDA [31], AH scheme [32], and our scheme belong to the privacy homomorphism techniques. Finally, the hybrid technique achieves privacy-preserving data aggregation for WSNs by combining the previous techniques. PIA [33] is only the hybrid technique in this literature.

In the previous section, we addressed three important considerations for WSNs, which are energy consumption, data privacy, and data integrity. However, iPDA and iCPDA are the only works to support both privacy preservation and data integrity for WSNs; we provide the detailed explanation of iPDA and iCPDA in Section 2.1.

2.1. Privacy Preserving Data Aggregation Scheme with Data Integrity. He et al. proposed iPDA [19] and iCPDA [21] schemes for WSNs to support privacy-preserving data aggregation as well as data integrity. In the iPDA scheme, they protect data integrity by designing two node-disjoint aggregation trees rooted at the query server where each node belongs to a single aggregation tree. In this technique, first, every sensor node slices its private data randomly into L pieces and $L - 1$ pieces are encrypted and sent to the randomly selected sensor nodes of the aggregation tree keeping one piece at the same sensor node. The same process is independently done for each sensor node using another aggregation tree. Then, all the sensor nodes which received data slices from multiple sensor nodes decrypt the slices using their shared keys and sum the received data slices including their own. After that, each sensor node sends the sum value to its parent from the respective aggregation tree. In the same way, the sum data from another set of sensor nodes are transmitted to the query server through another aggregation tree. In the end, the aggregated data from two node-disjoint aggregation trees reach to the base station where the aggregated data from both aggregation trees are compared. If the difference of the aggregated data from the two aggregation trees does not deviate from the predefined threshold value the query server accepts the aggregation result; otherwise, it rejects the aggregated result by considering it as polluted data. However, there are some shortcomings in the iPDA. First of all, during protecting data privacy it generates high traffics in the WSN. As a result, communication cost is significantly increased in the iPDA. Secondly, all sensor nodes use secret keys to encrypt all of their data slices before sending to their respective $2(L - 1)$ number of sensor nodes. So, every sensor node has computation overhead of decrypting all the slices they received before aggregating them.

In the iCPDA, three rounds of interactions are required. Firstly, each node sends a seed to other cluster members. Next, each node hides its sensory data via the received seeds and sends the hidden sensory data to each cluster member. Then, each node adds its own hidden data to the received hidden data and sends the calculated results to its cluster head which calculates the aggregation results via inverse and multiplication of matrix. To enforce data integrity, cluster members check the transmitted aggregated data of the cluster head. There are some disadvantages of iCPDA. Firstly, the communication overhead of iCPDA increases quadratically with the cluster size. Secondly, the computational overhead of CPDA increases quickly with the increase of the cluster size which introduces large matrix, whereas lower cluster size introduces lower privacy-preserving efficacy.

Both iPDA and iCPDA support very weak data integrity checking because if any node modifies its sampled value 30 to 300 and uses the value 300 for aggregation process none of both methods can detect such misbehavior in the network. Hence, in this paper, we propose a new, efficient (in terms of communication overhead and data propagation delay), and general (in terms of supporting network topology) scheme in order to support data privacy and achieve integrity assurance in data aggregation for WSNs. Our scheme is based on the algebraic properties of the complex numbers and it not only ensures that no trend about sensitive data of a sensor node is released to any other nodes and adversaries but also provides data integrity checking of the aggregated value of sensor data.

3. Integrity-Protecting Sensitive Data Aggregation Technique

To overcome the previously mentioned shortcomings of the iPDA and iCPDA, in this section, we propose a new energy-efficient data aggregation scheme for preserving data privacy in WSNs. Our scheme exploits an additive property of complex number to aggregate the sensed data in WSNs. Our assumption is that we only focus on additive aggregation function (SUM), like the iCPDA and iPDA. This is because other aggregation functions, such as average, count, variance, and standard deviation, can be obtained by using the additive aggregation function [34]. In our scheme, out of two parts of a complex number ($a + bi$), the real part (a) is used to hide the sampled data of a sensor node from its neighboring nodes and adversaries, whereas the imaginary part (bi) is used for data integrity checking at both data aggregators and the sink node. Before transmitting data to a parent node, every sensor node transforms its sampled data into a complex number form. The real part is generated by combining the sampled data with a unique private seed and the imaginary part is generated by appending an imaginary unit to the modified sampled data. For this, the sampled value is first mingled with a private seed and then the result (a) is combined with another real number

Table 1: Real ID of 8 sensor nodes with signature.

SN	Node-ID	2-Byte signature
1	$2^0 = 1$	0000000000000001
2	$2^1 = 2$	0000000000000010
3	$2^2 = 4$	0000000000000100
4	$2^3 = 8$	0000000000001000
5	$2^4 = 16$	0000000000010000
6	$2^5 = 32$	0000000000100000
7	$2^6 = 64$	0000000001000000
8	$2^7 = 128$	0000000010000000

having i (bi) to generate a complex number form ($c = a + bi$). The real number with i (bi) is the absolute difference between the previous sample data and the current sample data of a node. Note that during network deployment, a Master Device (MD) [35] securely provides a unique real number as a seed to every sensor node of the WSNs after establishing a pairwise secret key with them. Since the MD is an offline server, it shares this information only with the query server for future reference. Thus, the seed of each sensor node is private in the network. Data can be aggregated in upper levels during their transmissions to the query server by using the algebraic properties of complex numbers. Our scheme can check the integrity of the aggregated data at both data aggregators and the sink node at the same time.

The proposed privacy and integrity preserving technique is performed through five steps. In the first step, we assign a special type of positive integer 2^n (where $n = 0$ to $Bn \times 8 - 1$, such that Bn is the number of free bytes available in the payload) to every sensor node as node ID. This is because the binary value of every integer of 2^n type has only one high bit (1). In addition, the position of the high bit for all integers of this type is unique. The sink node knows a data contributing sensor node through the signature of Node-ID as shown in Table 1. The Node-ID of a sensor node is used to generate a signature of a fixed length. A signature is a fixed size bit stream of binary numbers for a given integer. Signature of a senor node ID can be generated by using the technique presented in the work [36]. We can determine the length of the signature based on the size of a given WSN. When the size of the WSN increases we can increase the length of the signature up to the Bn bytes. In other words, different size WSNs can have signatures of different lengths. The detail of using signatures has been presented in our previous work [37].

When the network receives an SQL-like query for SUM aggregation function, in the second step, the sampled sensitive data ds of each sensor node is, first, concealed in a by combining with a unique seed (sr) which is a private real number. The seeds can be selected from an integer range (i.e., space between lower bound and upper bound). By increasing the size of the range, we can further increase the level of the data privacy. Hence, our approach can support data privacy feature strongly. To support data integrity, an integer value b—*the difference of the previous sensed value and the current sensed value* of the sensor node—with i is appended to the a by using *genCpxNum*() function to form a complex number $C = a + bi$, where a and b are real numbers called the real part and the imaginary part of the complex number, respectively, as shown in Table 2. Complex numbers can be added, subtracted, multiplied, and divided by formally applying associative, commutative, and distributed laws of algebra. For the first round, the complex number (value of b) is zero. In Table 2, for instance, the reading 17 of node 5 is encrypted into $46 + 3i$. The reading 17 is added to 29, which is a private seed of node 5 and the mask value 46 is calculated. Then, assuming that $3i$ is the difference value of previous reading and current reading of node 5, the $3i$ is appended to the result 46 to get $46 + 3i$ which is a complex number form of the 17 after data customization process. Node 5 includes its signature, that is, 00000101, when it transmits the data as $\langle 00000101, 46 + 3i \rangle$. We assumed that any sensor node cannot be compromised before sending first round data to the sink node. Every source sensor node keeps the original sensed value d of the current round to deduce b in the next round which is updated in each round of data transmission. Next, the source node encrypts the customized data R_1', that is, $R_1 = a + bi$, and the signature of the node by using a secret key Kx, y [22] and transmits the cipher text C_j to its parent. The term Kx, y denotes a pairwise symmetric key shared by nodes x and y, where the node x encrypts data by using a key Kx, y and the node y decrypts the data by using the key Kx, y. In this way, our algorithm converts the sampled data into an encrypted complex number form. Hence, it not only protects the transmitting trend of private data but also does not let neighboring sensor nodes and adversaries to recover sensitive data even though they overheard and decrypted the sensitive data.

In the third step, the parent sensor node (i.e., data aggregator) decrypts the received data by using respective pairwise symmetric keys of its child sensor nodes. For each child node, the parent node computes the difference value (b') of the two real units by using the stored previous data and the received current data of the child node. For the first round, the value of b' is also zero. For this, the parent node always keeps the record of the previously received data from each of the child nodes and it updates the previous data by current one in every round. To support local integrity checking, the parent node first compares just computed difference value with the currently received difference value (imaginary unit) from the child node and then compares the difference value with local threshold δ. If the imaginary unit of the child's current data is equal to the computed difference value and the imaginary unit is not greater than δ, then the parent node accepts the data of the child node. Otherwise, the parent node rejects the data of the child sensor node considering it as polluted data. For example, we assume that the value for δ is set to 2 for local integrity checking. Because a parent node checks the integrity of its' child nodes, node 4 checks the local integrity of the node 8. In Figure 1, since the imaginary part of node 8 is 2, which is less than or equal to δ, node 4 accepts the data of node 8. On the other hand, node 5 will be rejected by its parent node 2 because imaginary part of node 5 is greater than δ. In the same way, the parent node assures the data integrity of child nodes. After that the parent node adds the data of child nodes including its own by using additive property

Table 2: Customized data creation for each node.

SN	Reading (ds)	Real seed (sr)	Mask value (a = ds + sr)	Difference value (bi)	Complex number ($a + bi$)
1	16	40	56	$2i$	$56 + 2i$
2	14	51	65	$0i$	$65 + 0i$
3	19	32	51	i	$51 + i$
4	21	23	44	i	$44 + i$
5	17	29	46	$3i$	$46 + 3i$
6	18	33	51	i	$51 + i$
7	13	39	52	$2i$	$52 + 2i$
8	15	67	82	$2i$	$82 + 2i$

of complex number to produce an intermediate result R'. At the same time, it superimposes signatures (SSig) of the contributed nodes by performing bitwise OR operation on the bit-streams of the node IDs and forwards the encrypted intermediate result "C_r" towards the sink node. Since this approach needs just one bit to carry an ID of a sensor node it is 16 times scalable than the existing work CMT [34] where plaintexts (2-byte each) are used for carrying IDs of sensor nodes by simply concatenating them. Note that different types of application can have different value for the threshold δ. Thus, our algorithm supports local integrity checking which enforces to provide consistent data from child nodes. The above process continues at all nodes of the upper levels of the network until the whole partially aggregated data of the network reach to the sink node.

In the fourth step, when the sink node receives all intermediate result sets C_{rs} (partially aggregated encrypted customized data with superimposed signature) from the 1-hop child nodes, it decrypts them by using respective pairwise symmetric keys and computes the final aggregation SUM_2 from C_{rs}. Since SUM_2 is of complex number form and the sensed data has been concealed in the real unit by using private seeds, identifying the information of the contributed sensor nodes is necessary to deduce actual SUM value. In the last step, the sink node first knows data contributing nodes by checking the high bits (1 s) of the received superimposed signature by performing bitwise AND operation with the prestored signature files or superimposed signature of the Node-IDs of the all nodes of the network. For this, it separates SUM_2 into real unit $\text{SUM}_{2\text{R}}$ and imaginary unit $\text{SUM}_{2\text{IM}}$. Because the sampled data of sensor nodes has been concealed within the real unit, the sink node computes the actual aggregated result SUM by subtracting (an inverse operation of masking, step 2) $\text{SUM}_{1\text{R}}$ (a freshly computed sum value of the private seeds of the contributed source nodes) from $\text{SUM}_{2\text{R}}$. The final result SUM is always accurate and reliable because of the following two reasons. First, a complex number is an algebraic expression and hence the underlying algebra gives the accurate result of the aggregated sensor data. Second, since the private seeds are fixed integer values (i.e., seeds are not random numbers) after collecting data by the sink node a complex number subtracts exactly the same values that have been added to the sensor data during data hiding process by every source node. At the same time, before accepting the SUM, the sink node performs global integrity checking of SUM to assure whether the SUM_2 has been polluted by an adversary in transit or not. For this, like parent nodes, the sink node also computes the difference value (B') of the two real units by using the stored previous data and the received current data from the network. The sink node first compares just computed difference value $B'i$ with the currently received difference value, that is, $\text{SUM}_{2\text{IM}}$, from the network and then compares the difference value ($\text{SUM}_{2\text{IM}}$) with global threshold Δ (for every application, the maximum value for $\Delta = \delta \times N$, where N is the total number of nodes in a network). If the imaginary unit $\text{SUM}_{2\text{IM}}$ of the current data from the network is equal to the just computed difference value $B'i$ and the $\text{SUM}_{2\text{IM}}$ is not larger than Δ, then the sink node accepts the data of the network and returned the actual SUM to the query issuer. Otherwise, the sink node rejects the SUM considering it as forged/polluted data by adversary or other nodes. For example, as shown in Figure 2, we assume that a local integrity threshold per node δ equals to $2i$ and the maximum value for a global threshold (Δ) is calculated as $\Delta = \delta \times N = 2i \times 8 = 16i$. Since a sensor node 5 does not participate in data collection, the global integrity checking value Δ can be computed as $\delta \times N = 2i \times 7 = 14i$. In this scenario, the received data is considered as a consistent one and is accepted by the sink node, (1) because the value computed at the sink node, that is, $9i$, is the same as the one received from the network and (2) the value is less than the global integrity checking value, that is, $9i < 14i$. The overall algorithm that performs sensitive data aggregation and integrity checking is illustrated in Algorithm 1.

4. Performance Evaluation

In this section, we present simulation results of our scheme by comparing it with iPDA and iCPDA schemes in terms of communication overhead and integrity checking. For this, we use TOSSIM [38] simulator running over TinyOS [39] operating system and GCC compiler. We consider 100 sensor nodes distributed randomly in 100 m × 100 m area. As presented in directed diffusion [40], we use such parameters as receiving power dissipation of 395 mW and transmitting power dissipation of 660 mW. Moreover, MATLAB 7.6.0.324 (R2008a) is used to get execution time required for data customization and data aggregation.

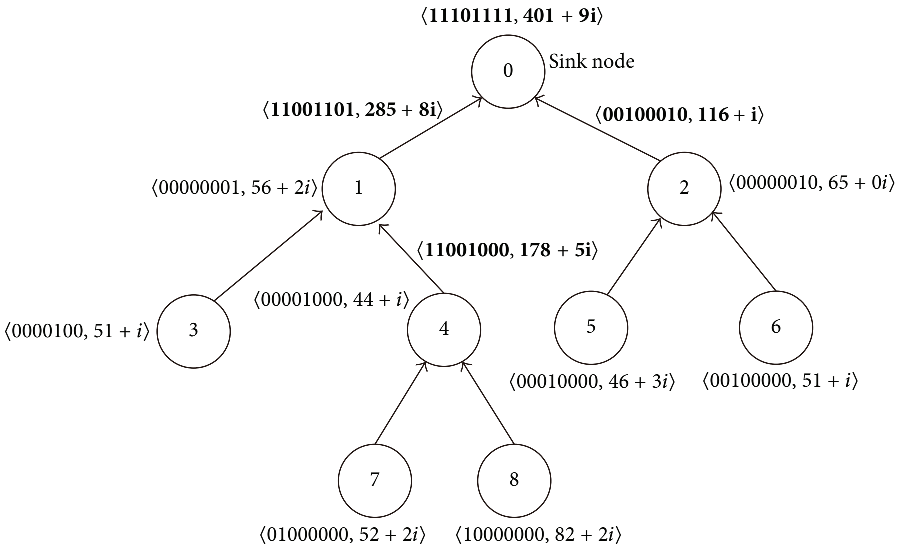


Figure 2: Superimposing signatures and addition of customized sensor readings in a multihop WSN ($\delta = 2$).

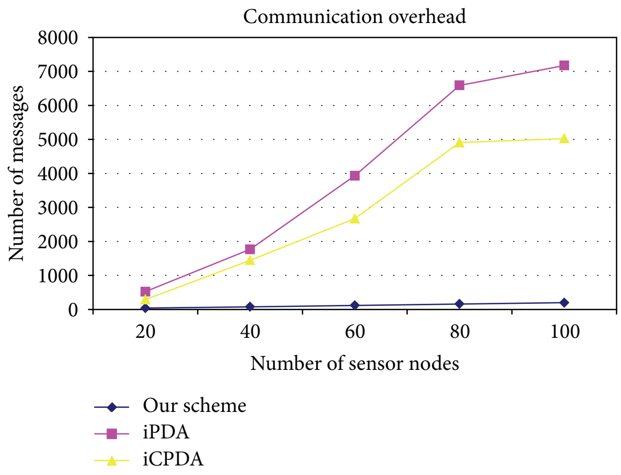


Figure 3: Energy consumption.

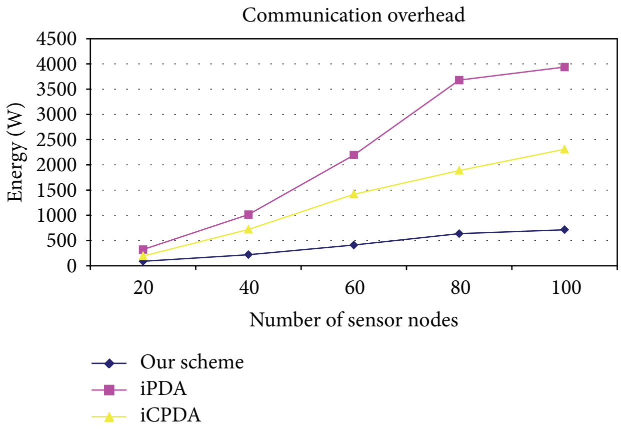


Figure 4: Energy consumption by the iPDA, iCPDA, and our schemes.

4.1. Data Aggregation. Figure 3 shows communication overhead in terms of the number of messages generated in a WSN with respect to varying number of sensor nodes. As expected, the number of messages in the iPDA, iCPDA, and our schemes increases when the number of sensor nodes increases. This is because every sensor node in the WSN is capable of sensing data and when the number of source nodes increases, the number of messages also naturally increases in all of the three schemes. However, our scheme outperforms the iPDA and iCPDA schemes because the existing schemes generate unnecessary messages in the network. The reason is that in our scheme each sensor node can customize its data by itself and it does not need to generate extra messages in the network for data privacy and integrity checking. On the other hand, the iPDA and iCPDA schemes generate six messages and four messages, respectively, for privacy preservation and integrity checking. Due to many messages exchanged among the nodes, the existing schemes cause high data collisions. That is to say, the number of messages generated in the network increases drastically as the number of sensor nodes becomes larger. iPDA and iCPDA schemes consume much energy for successful data transmission, compared with our scheme.

The messages generated in the WSN are finally consumed by the sink node. For this, message transmission and message reception processes are involved. Both processes require significant amount of energy. Figure 4 shows communication overhead in terms of energy dissipation by the iPDA, iCPDA, and our schemes with respect to varying number of sensor nodes in the WSN. As expected, the dissipated energy by all three schemes increases when the number of sensor nodes increases. This is because every message generated in the network requires some amount of energy to reach the sink node. However, the power consumption by our scheme is always lower than that of iPDA and iCPDA schemes. The reason is that the iPDA and iCPDA schemes generate too many unnecessary messages in the WSN while

```
Input: An aggregated WSN and SUM aggregation query
Output: SUM aggregation result
Step 1. Assign node ID and generate signature of the ID
    for all sensor nodes {
        ID = $2^n$;  // where $n = 0, 1, 2, \ldots$
        ID = Signature($2^n$);    $n = n + 1$;}
Step 2. Create customized data from the data of the source nodes
    for all sensor nodes {
        sense ds;
        $a$ = mask(ds, sr); // sr is a unique private seed
        $R'_1$ = genCmpxNum($a$, $bi$);
        $C_j$ = Enc($K_{x,y}$, (ID, $R'_1$));
        transmit($C_j$);}
Step 3. Local integrity checking and applying additive property of complex numbers to get intermediate result of the
customized data
    for every intermediate aggregators {
        for all received customized data {
            Drc($K_{y,x}$, ($C_j$));
            If ($bi$ ! = $b'i$ AND $bi > \delta$) //local integrity checking
             {reject $C_j$; inform_Sink();}
            Else {
                SSig = Superimpose($\mathrm{ID}_1, \ldots, \mathrm{ID}_k$);
                $R'$ = SUM($R'_1, \ldots, R'_k$);
                $C_r$ = Enc($K_{y,x}$, (SSig, $R'$));
                transmit($C_r$);} } }
Step 4. Compute aggregation result at the sink node
    for all receive($C_{\mathrm{rs}}$){Drc($K$, ($C_1$));
        $\mathrm{SUM}_2$ = add ($IR'_1, \ldots, IR'_k$);}
Step 5. Identify contributed sensor nodes, extract actual SUM of the sensors data and check global data integrity at the
sink
    fetch_Nodes_IDs();
    Node_IDs = SuperSig && SSig;
    $\mathrm{SUM}_2$ = disjoin ($\mathrm{SUM}_{2\mathrm{R}}$, $\mathrm{SUM}_{2\mathrm{IM}}$);
    $\mathrm{SUM}_{1\mathrm{R}}$ = Compute (sum of real seeds of contributed nodes);
    SUM = $\mathrm{SUM}_{2\mathrm{R}} - \mathrm{SUM}_{1\mathrm{R}}$;
    If ($\mathrm{SUM}_{2\mathrm{IM}} = B'i$ AND $\mathrm{SUM}_{2\mathrm{IM}} \le \Delta$)/* global integrity
                                                        checking */
        {return SUM;}
    Else {reject SUM;}
```

Algorithm 1: Algorithm for SUM aggregation with privacy-preservation and integrity checking.

achieving integrity protection and privacy preservation in data aggregation. And also every sensor node becomes active for longer time to communicate all the messages. However, in our scheme, every sensor node can achieve both integrity protection and privacy preservation by comparing the current complex number with the previous one. Hence, the energy consumption of our scheme is reduced by 80% and 60% over the iPDA and iCPDA, respectively.

Table 3 shows the computation overhead of data aggregation. The result shows that iCPDA has the worst performance on the computation overhead for privacy-preserving data aggregation. The reason is that the iCPDA uses a time-consuming encryption method with two seeds to achieve data privacy. On the other hand, the computation cost of our scheme is about two times and 83 times faster than those of the iPDA and iCDPA, respectively. It is shown that our scheme reduces a significant amount of resource (CPU time) usage for achieving private data aggregation. This is because our scheme reduces the number of communication messages by using the additive property of a complex number.

4.2. Data Integrity. Figure 5 shows data propagation delay in terms of average time required by sampled data of sensor nodes to reach to the sink node considering data privacy and integrity checking. During this process, a sensor node in iPDA and iCPDA has to communicate (i.e., transmit and receive) at least six and four messages, respectively. Hence, sensor nodes in both iPDA and iCPDA need more active time to perform all communications than our scheme resulting in very high data propagation delay in the existing work. In this way, dutycycling, which is the percent of time that an entity spends in an active state as a fraction of the total time [41], is also increased in the existing schemes. The iCPDA generates less number of messages than the iPDA but has complex

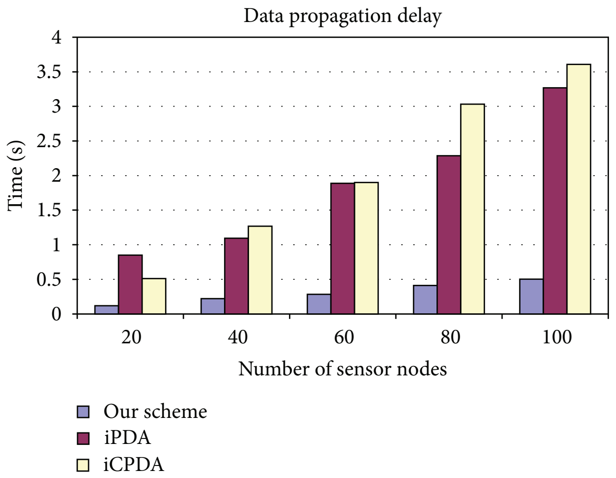


Figure 5: Average data transmissions time for iPDA, iCPDA, and our schemes.

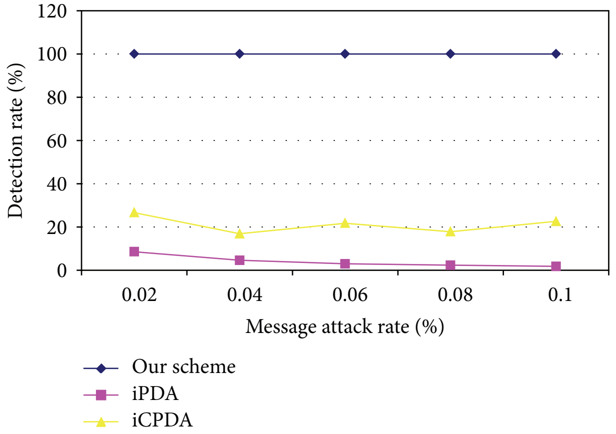


Figure 6: Integrity checking.

Table 3: Computational overhead for data customization and aggregation.

Protocols	Execution time (in sec)
iPDA	0.005924
iCPDA	0.219325
Our scheme	0.002632

computation for privacy preservation and longer size message than that of the iPDA. Moreover, in iCPDA, the sampled data of sensor nodes is sent to the opposite direction (data is transmitted from the cluster head to the cluster members) of the sink node for privacy preservation process. Therefore, the iCPDA has the worst performance among the three schemes. On the other hand, every sensor node in our scheme sends only one message (the aggregated data) to its parent node because it checks the integrity of the sensed data without the communication of other sensor nodes.

Figure 6 provides the performance of three schemes in terms of the detection ratio of polluted messages for integrity checking. It is shown that our scheme can detect all polluted messages, whereas iPDA and iCPDA can detect less than 30% of polluted messages. The reason is that every node in our scheme checks the integrity of its incoming data received from the lower-level nodes. On the other hand, only the sink node can check the integrity of the aggregated data in iPDA, whereas only the sink node and the cluster heads can perform the integrity checking in iCPDA.

5. Conclusion

In this paper, we proposed an efficient and general scheme in order to aggregate sensitive data protecting data integrity for private data generating environments such as patients' health monitoring application. For maintaining data privacy, our scheme applies the additive property of complex numbers where sampled data are customized and given the form of complex number before transmitting towards the sink node. As a result, it protects the trend of private data of a sensor node from being known by its neighboring nodes including data aggregators in WSNs. Moreover, it is still difficult for an adversary to recover sensitive information even though data are overheard and decrypted. Meanwhile, data integrity is protected by using the imaginary unit of complex-number-form customized data at the cost of just two extra bytes. Through simulation results, we have shown that our scheme is much more efficient in terms of communication and computation overheads, data propagation delay, and integrity checking than the iPDA and iCPDA schemes.

As future work, we will provide more simulation results by designing data integrity and sensitive data-preserving scheme under collusive attacks. Moreover, we will improve our privacy-preserving data aggregation scheme to support MAX and MIN aggregations.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Grant no. 2013010099). And this research was supported by the Brain Korea 21 PLUS Project, NRF.

References

[1] S. K. Dhurandher, M. S. Obaidat, and M. Gupta, "An acoustic communication based AQUA-GLOMO simulator for underwater networks," *Human-Centric Computing and Information Sciences*, vol. 2, article 3, 2012.

[2] H. Karl and A. Willig, "A short survey of wireless sensor networks," Tech. Rep. TKN-03-018, 2003.

[3] K. Romer, "Programming paradigms and middleware for sensor networks," in *Proceedings of the GI/ITG Workshop on Sensor Networks*, pp. 49–54, Karlsruhe, Germany, 2004.

[4] Q. Liu and D. Oh, "Performance evaluation of multi-hop communication based on a mobile multi-robot system in a subterranean laneway," *Journal of Information Processing Systems*, vol. 8, no. 3, pp. 471–482, 2012.

[5] G. Carvalho, I. Woungang, A. Anpalagan, and S. Dhurandher, "Energy-efficient radio resource management scheme for heterogeneous wireless networks: a queueing theory perspective," *Journal of Convergence*, vol. 3, no. 4, pp. 15–22, 2012.

[6] X. Li, N. Mitton, A. Nayak, and I. Stojmenovic, "Achieving load awareness in position-based wireless Ad Hoc routing," *Journal of Convergence*, vol. 3, no. 3, pp. 17–22, 2012.

[7] M. Yoon, Y. K. Kim, and J. W. Chang, "An energy-efficient routing protocol using message success rate in wireless sensor networks," *Journal of Convergence*, vol. 4, no. 1, pp. 15–22, 2013.

[8] B. Singh and D. Lobiyal, "A novel energy-aware cluster head selection based on particle swarm optimization for wireless sensor networks," *Human-Centric Computing and Information Sciences*, vol. 2, article 13, 2012.

[9] R. Sumathi and M. G. Srinivas, "A survey of QoS based routing protocols for wireless sensor networks," *Journal of Information Processing Systems*, vol. 8, no. 4, pp. 589–602, 2012.

[10] M. S. Obaidat, S. K. Dhurandher, and K. Diwakar, "CASPER: congestion aware selection of path with efficient routing in multimedia networks," *Journal of Information Processing Systems*, vol. 7, no. 2, pp. 241–260, 2011.

[11] J. Considine, F. Li, G. Kollios, and J. Byers, "Approximate aggregation techniques for sensor databases," in *Proceedings of the 20th International Conference on Data Engineering (ICDE '04)*, pp. 449–460, April 2004.

[12] M. Samuel, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TAG: a tiny aggregation service for ad hoc sensor networks," in *Proceedings of the Symposium on Operating Systems Design and Implementation (OSDI '02)*, 2002.

[13] S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TinyDB: an acquisitional query processing system for sensor networks," *ACM Transactions on Database Systems*, vol. 30, no. 1, pp. 122–173, 2005.

[14] R. Bista, Y.-K. Kim, and J.-W. Chang, "A new approach for energy-balanced data aggregation in wireless sensor networks," in *Proceedings of the 9th IEEE International Conference on Computer and Information Technology (CIT '09)*, vol. 2, pp. 9–15, October 2009.

[15] F. Tseng, L. Chou, and H. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Human-Centric Computing and Information Sciences*, vol. 1, article 4, 2011.

[16] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: privacy-preserving data aggregation in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 2045–2053, May 2007.

[17] T. Feng, C. Wang, W. Zhang, and L. Ruan, "Confidentiality protection for distributed sensor data aggregation," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 475–483, April 2008.

[18] M. Conti, L. Zhang, S. Roy, R. Di Pietro, S. Jajodia, and L. V. Mancini, "Privacy-preserving robust data aggregation in wireless sensor networks," *Security and Communication Networks*, vol. 2, no. 2, pp. 195–213, 2009.

[19] W. He, H. Nguyen, X. Liu, K. Nahrstedt, and T. Abdelzaher, "iPDA: an integrity-protecting private data aggregation scheme for wireless sensor networks," in *Proceedings of the IEEE Military Communications Conference (MILCOM '08)*, pp. 1–7, November 2008.

[20] E. Mlaih and S. A. Aly, "Secure hop-by-hop aggregation of end-to-end concealed data in wireless sensor networks," in *Proceedings of the IEEE INFOCOM Workshops*, pp. 1–6, April 2008.

[21] W. He, X. Liu, H. Nguyen, and K. Nahrstedt, "A cluster-based protocol to enforce integrity and preserve privacy in data aggregation," in *Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops*, pp. 14–19, 2009.

[22] E.-O. Blaß and M. Zitterbart, "An efficient key establishment scheme for secure aggregating sensor networks," in *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS '06)*, pp. 303–310, March 2006.

[23] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *Proceedings of the ACM SIGMOD International Conference on Management of Data*, pp. 439–450, Dallas, Tex, USA, May 2000.

[24] H. Kargupta, S. Datta, Q. Wang, and K. Sivakumar, "On the privacy preserving properties of random data perturbation techniques," in *Proceedings of the 3rd IEEE International Conference on Data Mining (ICDM '03)*, pp. 99–106, Melbourne, Australia, November 2003.

[25] M. Conti, L. Zhang, S. Roy, R. Di Pietro, S. Jajodia, and L. V. Mancini, "Privacy-preserving robust data aggregation in wireless sensor networks," *Security and Communication Networks*, vol. 2, no. 2, pp. 195–213, 2009.

[26] J. Yao and G. Wen, "Protecting classification privacy data aggregation in wireless sensor networks," in *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '08)*, pp. 1–5, Dalian, China, October 2008.

[27] W. Zhang, C. Wang, and T. Feng, "GP^{2}S: generic privacy-preservation solutions for approximate aggregation of sensor data," in *Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom '08)*, pp. 179–184, Hong Kong, China, March 2008.

[28] M. Yoon, K. Yong-Ki, and J. Chang, "A new data aggregation scheme to support energy efficiency and privacy preservation for wireless sensor networks," *International Journal of Security & Its Applications*, vol. 7, no. 1, pp. 129–142, 2013.

[29] Y. K. Kim, H. Lee, M. Yoon, and J. W. Chang, "Hilbert-curve based data aggregation scheme to enforce data privacy and data integrity for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 217876, 14 pages, 2013.

[30] B. Sheng and Q. Li, "Verifiable privacy-preserving range query in two-tiered sensor networks," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 457–465, Phoenix, AZ, USA, April 2008.

[31] J. Girao, D. Westhoff, and M. Schneider, "CDA: concealed data aggregation for reverse multicast traffic in wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '05)*, vol. 5, pp. 3044–3049, Seoul, Korea, May 2005.

[32] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in *Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems -Networking and Services (MobiQuitous '05)*, pp. 109–117, San Diego, Calif, USA, July 2005.

[33] G. Taban and D. Gligor, "Privacy-preserving integrity-assured data aggregation in sensor networks," in *Proceedings of the IEEE International Conference on Privacy, Security, Risk, and Trust (PASSAT '09)*, pp. 168–175, Vancouver, Canada, August 2009.

[34] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in *Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems -Networking and Services (MobiQuitous '05)*, pp. 109–117, July 2005.

[35] E.-O. Blaß and M. Zitterbart, "An efficient key establishment scheme for secure aggregating sensor networks," in *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS '06)*, pp. 303–310, March 2007.

[36] J. Zobel, A. Moffat, and K. Ramamohanarao, "Inverted files versus signature files for text indexing," *ACM Transactions on Database Systems*, vol. 23, no. 4, pp. 453–490, 1998.

[37] R. Bista and J. W. Chang, "Energy efficient data aggregation for wireless sensor networks," in *Sustainable Wireless Sensor Networks*, 2010.

[38] P. Levis, N. Lee, M. Welsh, and D. Cullar, "TOSSIM: accurate and scalable simulation of entire TinyOS applications," in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, pp. 126–137, 2003.

[39] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," in *Proceedings of the 9th Internatinal Conference Architectural Support for Programming Languages and Operating Systems (ASPLOS '00)*, pp. 93–104, November 2000.

[40] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 56–67, August 2000.

[41] http://en.wikipedia.org/wiki/Duty_cycle.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 281565, 10 pages
http://dx.doi.org/10.1155/2013/281565

Research Article

Community Vitality in Dynamic Temporal Networks

Fu Cai,[1] Li Min,[1] Zou Deqing,[1] Qu Shuyan,[1] Han Lansheng,[1] and James J. Park[2]

[1] *School of Computer Sci & Tech, Huazhong University of Science and Technology, Wuhan 430074, China*
[2] *Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 139-742, Republic of Korea*

Correspondence should be addressed to Zou Deqing; deqingzou@hust.edu.cn

Received 3 October 2013; Accepted 26 November 2013

Academic Editor: Neil Y. Yen

Current researches on temporal networks mainly tend to detect community structure. A number of community detection algorithms can obtain community structure on each time slice or each period of time but rarely present the evolution of community structure. Some papers discussed the process of community structure evolution but lacked quantifying the evolution. In this paper, we put forward the concept of *Community Vitality* (CV), which shows a community's life intensity on a time slice. In the process of computing CV, the "dead communities" can also be distinguished. Moreover, CV cannot only be used to quantify the life intensity of a community but also be used to describe the process of community evolution over time. More specifically, the change of community's structure will be found if CVs for different time slices of a community were compared, while the community with big value of CV can be selected if CVs for different communities were compared. Furthermore, *community vitality* change rate (CVCR) is proposed for revealing communities' structure change. The results of our experiments show that community vitality is a novel and effective way to understand or model the community evolution.

1. Introduction

As we all know, many systems, such as traffic system or information system, can be modeled as networks.

By studying structure and features of networks we can realise and predict networks' behavior and then discover the laws of corresponding real system. For instance, with the help of evolution research, *adhoc* networks' structure can be optimized in order to improve their transmit efficiency. Virus immunization strategies aimed to avoid virus outbreak in a large scale can also be optimized through the study on virus propagation networks. In addition, by researching production sales networks we can discover the consumers who prefer specific productions and then achieve the goal of maximizing the benefits of goods promotion.

The above-mentioned networks can be considered as temporal networks, in which active time of network connections is limited and sequenced, and events are propagated along temporal paths [1]. Up to now, the research on temporal networks are mainly focused on three aspects [2]: detecting temporal community structure; analyzing characteristics of community structure, such as temporal node centrality, temporal distances, and temporal clustering coefficient; and modelling temporal networks, such as TVG framework proposed by Arnaud and Paola and TRG framework proposed by John Whitbeck.

Detecting community structure in temporal networks is the foundation of studying networks' structure, which includes static community detection [3] and dynamic community detection [4]. As networks' structure changes over time, it is hard for static community detection algorithm to deal with noises in networks and insignificant communities might be detected. Therefore, the dynamic methods have been put forward currently. However, they cannot find *"dead communities"* and present the process of evolution. From Figure 1 we can find that the four communities have almost the same complexity and activeness (Figure 1(a)) when the final accumulating data is considered. But when the data is shown on time slices, we can find that the four communities are completely different: some are in the state of *"growing"* and others in the state of *"dying"* (Figure 1(b)). Although there are a few researches on the evolution of temporal

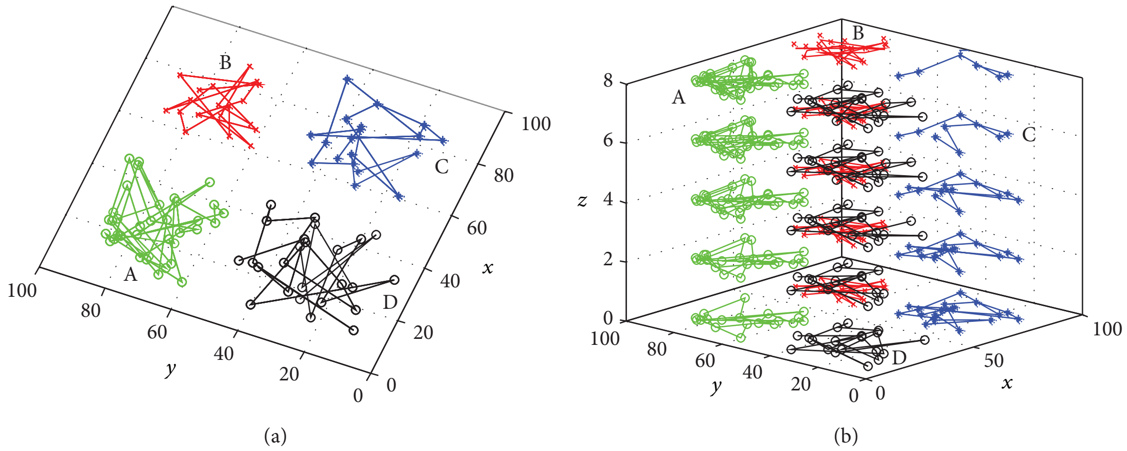


Figure 1: Temporal communities.

networks [5, 6], they did not quantify the process of evolution. These researches cannot quantify the process of community structure changed over time and also cannot recognize the process of a community's structure changing from *"birth"* to *"death."*.

In this paper, we put forward the conception of *Community Vitality* (CV) designed for describing the life intensity of communities, on the basis of static community detection. What's more, CV can reflect communities' structure change quantitatively. We can analyze a community's status, structure changes, and life intensity between different communities also. And in the process of computing CV, we cannot only detect community structure changes, but also distinguish between the shrinking and increasing communities. By analyzing a time slice, we can get a community's life intensity, the complexity between different communities and then find out the *"dead"* communities.

The rest of the paper is organized as follows. In Section 2, different community detection methods are compared, and the definition of *Community Inheritability* (CI), the decision rules, and algorithm of *Community Inheritability* are given. In Section 3, the core conception of CV and CVCR which describes the change process of a community's CV are defined. In Section 4, experiments on two real datasets are given. In the experiments the values of CV are calculated, and inner structure and some laws of the real system which represented by the datasets are discovered. Applications in *adhoc* networks were also analyzed in this section. A conclusion and some future works are given in Section 5.

2. Community Detection and Inheritability

Before computing CI and CV, the initial communities of temporal networks must be detected first. Recently, lots of static community detection algorithms have been put forward. The algorithms are mainly divided into two categories: one is graphs segmentation algorithm, such as the most representative algorithms Kernighan-Lin algorithm [7] and spectral bisection method [8] and the other one is hierarchical clustering algorithm, such as GN algorithm [9], Fast algorithm [10], and CNM algorithm [11]. Considering CNM algorithm has low time complexity which almost equal to $O(n)$ and high algorithm efficiency, we choose CNM algorithm as temporal networks' static community detection algorithm.

After detecting communities on the given time slice, *Community Similarity* (CSS) is defined to judge the state of a community on the next time slice. CI can show us when a community is *"born"* or *"die"*, that is, the start or end of a community's lifecycle, and serve for computing community vitality. Below we analyze three types of community changes (Keep, Separation, and Mergence) to judge inheritability between communities on consecutive time slices, by computing CSS between different communities.

Definition 1 (critical events). Critical events are those events who can cause community structures changes. A community's nodes or edges must have been changed if its structure changed. Thus, the four critical events *N*_Join, *N*_Leave, *E*_Appear, and *E*_Disappear are defined as follows.

*(N_Join). N*_Join is an event that a node joins into a community, which includes two situations: a new created node come into the community and a node from another community that moves to the community. Node v joins into community C on the time slice t represented as follows:

$$N_{\text{Join}(v,t)} = 1 \quad \text{iff } v \notin V_{t-1},\ v \in V_t. \tag{1}$$

*(N_Leave). N*_Leave is an event that a node leaves from a community, which includes two situations: a node disappears and a node from one community that moves to another community. Node v leaves from community C on the time slice t represented as follows:

$$N_{\text{Leave}(v,t)} = 1 \quad \text{iff } v \in V_{t-1},\ v \notin V_t. \tag{2}$$

*(E_Appear). E*_Appear is an event that an edge appears in a community, which includes two situations: a new edge that appears in the community and an edge that comes from

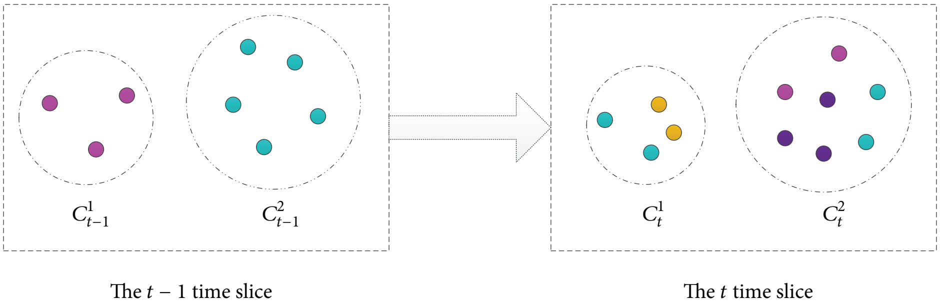


Figure 2: Community structure on adjoining time slices.

another community. Edge e appears in community C on the time slice t is represented as follows:

$$E_{\text{Appear}(e,t)} = 1 \quad \text{iff } e \notin E_{t-1},\ e \in E_t. \tag{3}$$

(E_Disappear). E_Disappear is an event that an edge disappears from a community, which includes two situations: an edge that disappears from the community and an edge that moves to another community. Edge e disappears from community C on the time slice t represented as follows:

$$E_{\text{Disappear}(e,t)} = 1 \quad \text{iff } e \in E_{t-1},\ e \notin E_t. \tag{4}$$

In the definitions above, V_{t-1} and V_t are the set of C's nodes on time slice $t-1$ and t; E_{t-1} and E_t are the set of C's edges on time slice $t-1$ and t.

Definition 2 (community structure change events). *Community structure change events* (CSCE) are used to reflect communities' relationship between adjacent time slices. Three types of CSCEs, which are Keep, Separation, and Mergence are defined as follows.

(Keep). A community C_{t-1}^{p} on time slice $t-1$ and another community C_t^q on time slice t has a relationship called Keep, when and only when C_{t-1}^{p} only has the same nodes with C_t^q on time slice t and C_t^q only has the same nodes with C_{t-1}^{p} on time slice $t-1$. In Figure 2, C_{t-1}^{1} and C_t^2 have the relationship called Keep. The event can be formalized as follows:

$$\begin{gathered}\text{Keep}\left(C_{t-1}^{p}, C_t^q\right) = 1, \quad \text{iff } V_{t-1}^{p} \cap V_t^q \neq \Phi, \\ V_{t-1}^{p} \cap V_t^i = \Phi, \qquad V_{t-1}^{j} \cap V_t^q = \Phi, \\ \text{here } i = 1, \ldots, q-1, q+1, \ldots, n, \\ j = 1, \ldots, p-1, p+1, \ldots, m;\end{gathered} \tag{5}$$

(Separation). A community C_{t-1}^{p} on time slice $t-1$ and k ($k \geq 2$) communities $C_t^{k_1}, C_t^{k_2}, \ldots, C_t^{k_k}$ on time slice t has a relationship called Separation when C_{t-1}^{p} have the same nodes with all of the k communities on time slice t. In Figure 2, C_{t-1}^{2} and C_t^1, C_t^2 has the relationship called Separation. The event can be formalized as follows:

$$\begin{gathered}\text{Separation}\left(C_{t-1}^{p}, C_t^{k_1}, C_t^{k_2}, \ldots, C_t^{k_k}\right) = 1, \\ \text{iff } V_{t-1}^{p} \cap V_t^i \neq \Phi, \quad V_{t-1}^{p} \cap V_t^j = \Phi, \\ \text{here } i = k_1, k_2, \ldots, k_k,\ \ j \in [1, n],\ \ j \neq k_1, k_2, \ldots, k_k;\end{gathered} \tag{6}$$

(Mergence). k ($k \geq 2$) communities $C_{t-1}^{k_1}, C_{t-1}^{k_2}, \ldots, C_{t-1}^{k_k}$ on time slice $t-1$ and a community C_t^q on time slice t has a relationship called Mergence when all of the k communities on time slice $t-1$ have the same nodes with C_t^q. In Figure 2, C_t^2 and C_{t-1}^{1}, C_{t-1}^{2} have the relationship called Mergence. The event can be formalized as follows:

$$\begin{gathered}\text{Mergence}\left(C_{t-1}^{k_1}, C_{t-1}^{k_2}, \ldots, C_{t-1}^{k_k}, C_t^q\right) = 1, \\ \text{iff } V_{t-1}^{i} \cap V_t^q \neq \Phi, \quad V_{t-1}^{j} \cap V_t^q = \Phi, \\ \text{here } i = k_1, k_2, \ldots, k_k,\ \ j \in [1, m],\ \ j \neq k_1, k_2, \ldots, k_k.\end{gathered} \tag{7}$$

In the definitions above, m and n, respectively, represent the number of community on time slice $t-1$ and t.

Definition 3 (influence of a node). Influence of a node indicates the importance of the node in its community. A node with big influence can attract a new connection with larger probability.

Let a community on time slice t be C_t^p, whose node ID is denoted by $1, 2, \ldots, n$ and degree of nodes is denoted by $d_1, d_2, \ldots, d_n$; then the influence of node i can be calculated as

$$\text{Inf}\left(i, C_t^p\right) = \frac{d_i}{\sum_{j=1}^{n} d_j}. \tag{8}$$

Definition 4 (community structure similarity). CSS can quantify the similarity of two communities on consecutive time slices. And it is the criterion of CI: bigger similarity have higher probability inheritability.

Let a community on time slice $t-1$ be C_{t-1}^{p}, whose number of node is n_1 and number of edge is e_1. Another community

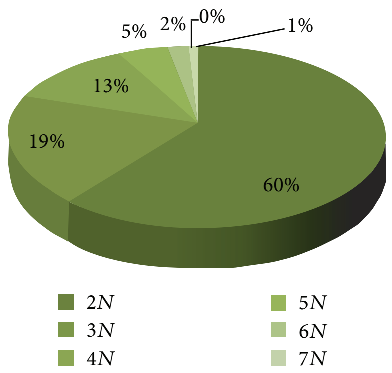


Figure 3: Community lifecycle distribution in CDBLP.

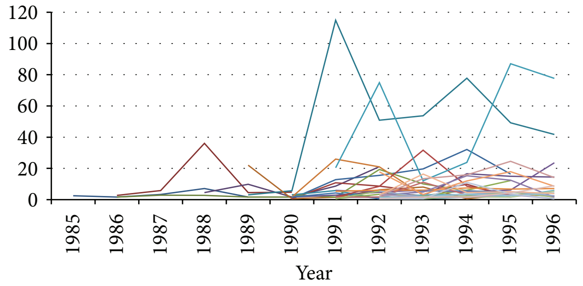


Figure 4: CV change in CDBLP.

C_t^q on time slice t whose number of node is n_2 and number of edge is e_2. The number of the same nodes between C_{t-1}^p and C_t^q is denoted by n, and the n nodes' ID is denoted by $1, 2, \ldots, n$. Also, the number of the same edges between C_{t-1}^p and C_t^q is denoted by e. The weight of node and edge of networks' community structure are denoted by w_1 and w_2, respectively. Then we have the following conclusions.

(a) If two communities have the relationship Keep, CSS can be calculated as follows:

$$\begin{aligned}\operatorname{Sim}\left(C_{t-1}^p, C_t^q\right) &= w_1 \times \frac{n}{n_1} \times \frac{\sum_{i=1}^n \operatorname{Inf}\left(i, C_{t-1}^p\right)}{n} \\ &\quad + w_2 \times \frac{e}{e_1} \\ &= w_1 \times \frac{\sum_{i=1}^n \operatorname{Inf}\left(i, C_{t-1}^p\right)}{n_1} + w_2 \times \frac{e}{e_1}.\end{aligned} \tag{9}$$

(b) If two communities have the relationship Separation, CSS can be calculated as follows:

$$\begin{aligned}\operatorname{Sim}\left(C_{t-1}^p, C_t^q\right) &= w_1 \times \frac{n}{n_1} \times \frac{\sum_{i=1}^n \operatorname{Inf}\left(i, C_{t-1}^p\right)}{n} \\ &\quad + w_2 \times \frac{e}{e_1} \\ &= w_1 \times \frac{\sum_{i=1}^n \operatorname{Inf}\left(i, C_{t-1}^p\right)}{n_1} + w_2 \times \frac{e}{e_1}.\end{aligned} \tag{10}$$

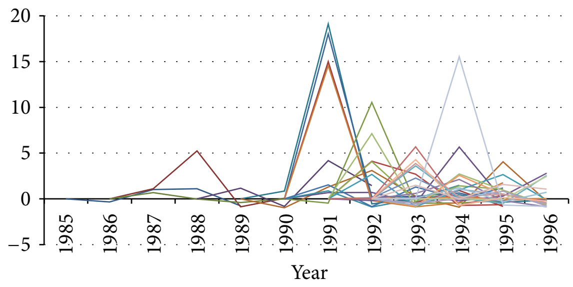


Figure 5: CVCR change over time in CDBLP.

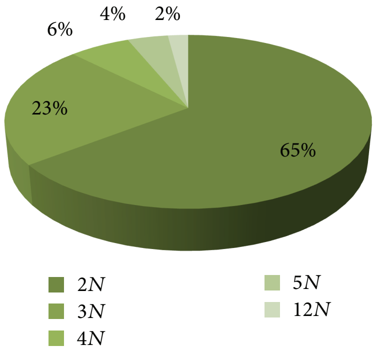


Figure 6: Community lifecycle distribution in EED.

(c) If two communities have the relationship Mergence, CSS can be calculated as follows:

$$\begin{aligned}\operatorname{Sim}\left(C_{t-1}^p, C_t^q\right) &= w_1 \times \frac{n}{n_2} \times \frac{\sum_{i=1}^n \operatorname{Inf}\left(i, C_t^q\right)}{n} \\ &\quad + w_2 \times \frac{e}{e_2} \\ &= w_1 \times \frac{\sum_{i=1}^n \operatorname{Inf}\left(i, C_t^q\right)}{n_2} + w_2 \times \frac{e}{e_2}.\end{aligned} \tag{11}$$

(d) Two communities has any of these relationships above, CSS is equal to 0; that is, Sim = 0.

All parameters appeared in the paper (including w_1, w_2 and w_3, w_4, w_5 appeared in chapter III) are decided by entropy method, which can be used to determine evaluation indicators of arbitrary evaluation problem and remove the indicators having slight effect on evaluation result, then reflect the importance of every indicator objectively.

Definition 5 (community inheritability). CI represents that a community on last time slice whose state and position on current time slice. Next we will analyze all cases of communities' CI between consecutive time slices.

(a) If a community C_{t-1}^p on time slice $t-1$ and another community C_t^q on time slice t has a relationship called Keep; then C_t^q inherits from C_{t-1}^p.

(b) If a community C_{t-1}^p on time slice $t-1$ and another k $(k \geq 2)$ communities $C_t^{k_1}, C_t^{k_2}, \ldots, C_t^{k_k}$ on time

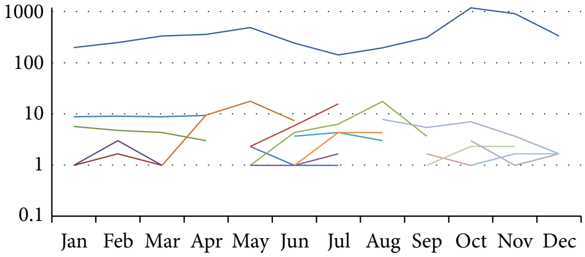


Figure 7: CV change in EED.

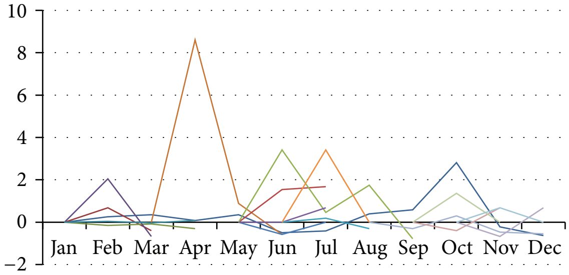


Figure 8: CVCR change over time in EED.

slice t have a relationship called Separation; then community structure similarity $\mathrm{Sim}_1, \mathrm{Sim}_2, \ldots, \mathrm{Sim}_k$ between community C_{t-1}^p and k communities on time slice t should be computed. After that, the maximum and the second largest value Sim_i and Sim_j $(i, j \in [k_1, k_k])$ should be selected from these values. If $\mathrm{Sim}_i \neq \mathrm{Sim}_j$; then C_t^i inherits from C_{t-1}^p and other communities C_t^x $(x = k_1, k_2, \ldots, i-1, i+1, \ldots, k_k)$ are all treated as new communities or else, C_{t-1}^p is *"dead"* and communities $C_t^{k_1}, C_t^{k_2}, \ldots, C_t^{k_k}$ are all treated as new community.

(c) If k $(k \geq 2)$ communities $C_{t-1}^{k_1}, C_{t-1}^{k_2}, \ldots, C_{t-1}^{k_k}$ on time slice $t-1$ and a community C_t^q on time slice t has a relationship called Mergence; then community structure similarity $\mathrm{Sim}_1, \mathrm{Sim}_2, \ldots, \mathrm{Sim}_k$ between k communities and community C_t^q should be computed. And next, the maximum and the second largest value Sim_i and Sim_j $(i, j \in [k_1, k_k])$ should be selected from these values. If $\mathrm{Sim}_i \neq \mathrm{Sim}_j$, then C_t^q inherits from C_{t-1}^i and other communities C_{t-1}^x $(x = k_1, k_2, \ldots, i-1, i+1, \ldots, k_k)$ are all *"dead"* or else, communities $C_{t-1}^{k_1}, C_{t-1}^{k_2}, \ldots, C_{t-1}^{k_k}$ are all *"dead"* and C_t^q are treated as a new community.

(d) If a community C_{t-1}^p on time slice $t-1$ and another community C_t^q on time slice t has none of these relationships above; then C_t^q does not inherit from C_{t-1}^p.

After defining the method that CSS under three cases of CSCE, judgement method of CI in each case are defined. Furthermore, we design Algorithm 1 called CI decision algorithm to decide communities' CI between consecutive time slices. Time complexity of the algorithm is $O(n * m)$. Here n is the number of communities on time slice $t-1$ and m is the number of communities on time slice t.

3. Community Vitality

We define the concept of CI in order to determine when a community is *"born or dies"*, so we can obtain a community's lifecycle. Also the concept is the precondition of computing CV. Furthermore, the concept of CV is used to quantify the life intensity of communities on every time slice, and if a community's different CVs in its lifecycle are compared, the evolution of community structure can be described quantificationally. CV can be used to forecast community structure changes to optimize *adhoc* networks and to analyze virus propagation and so on.

Definition 6 (community vitality). CV reflects the life intensity of a community on a time slice. Considering a community's CV change over time, the evolution process of community structure can be obtained quantificationally. Besides, a community with bigger CV than others has more complex structure. As we all know, a community's structure change is equal to some of critical events that happened, which leads to the community's CV change. Thus, it can be concluded that a community's CV change is decided by the change of critical events and finally puts down to the change of number of nodes, edges, and compactness of structure in the community. In fact, clustering coefficient [3] describes the aggregation of nodes in the network, namely, compactness of the network, so it's a influence factor of CV.

Let a community on time slice t be C_t^q, whose number of nodes is n, number of edges is e, and clustering coefficient is C. Then C_t^p's CV is defined as

$$\mathrm{VI}(t, q) = w_3 \times n + w_4 \times e + w_5 \times C. \tag{12}$$

Here parameters w_3, w_4, and w_5 respectively, present the degree of importance that nodes, edges, and community structure to CV.

Definition 7 (community vitality change rate). In oder to see a community's state and change degree directly, CVCR is put forward. CVCR shows a community's community structure change degree between consecutive time slices.

If the community C_t^q on time slice t inherits from the community C_{t-1}^p on time slice $t-1$, then CVCR can be calculated as follows:

$$\Delta \mathrm{VI}\left(C_{t-1}^p, C_t^q\right) = \frac{\mathrm{VI}(t, q) - \mathrm{VI}(t-1, p)}{\mathrm{VI}(t-1, p)}. \tag{13}$$

If the community C_t^q on time slice t is a newly created community, then CVCR can be calculated as

$$\Delta \mathrm{VI}\left(\Phi, C_t^q\right) = 0. \tag{14}$$

```
Input:
        Communities on time slice $t-1$: $C_{t-1}^{1}, C_{t-1}^{2}, \ldots, C_{t-1}^{m}$
        Communities on time slice $t$: $C_{t}^{1}, C_{t}^{2}, \ldots, C_{t}^{n}$
Output: continuity_matrix [$n$] [$m$]
% $n$ is the number of communities on time slice $t$
% $m$ is the number of communities on time slice $t-1$
% node_num_matrix [$n$] [$m$] saves the number of same
nodes between communities on adjacent time slices
% continuity_matrix [$n$] [$m$] saves the result of CI
between communities on adjacent time slices
% merger_matrix [$n$] [$m$] saves the Mergence
relationships and results of CI in the case
for $i \in [0, n)$ do //keep
    if (only one element in the $i$th row of
    node_num_matrix is not equal to 0) then
        continuity_matrix [$i$] [$j$] = 1;
    end if
end for
for $i \in [0, n)$ do //mergence
    if (more than one element in the $i$th row of
    node_num_matrix are not equal to 0) then
        Modifying continuity_matrix as
        Definition 3(d) and relevant elements of
        merger_matrix;
    end if
end for
for $i \in [0, m)$ do //separation
    if (more than one element in the $i$th column
    of node_num_matrix are not equal to 0) then
        Modifying continuity_matrix based on
        merger_matrix and results of CI computed as
        Definition 3(c);
    end if
end for
```

Algorithm 1: CI decision algorithm.

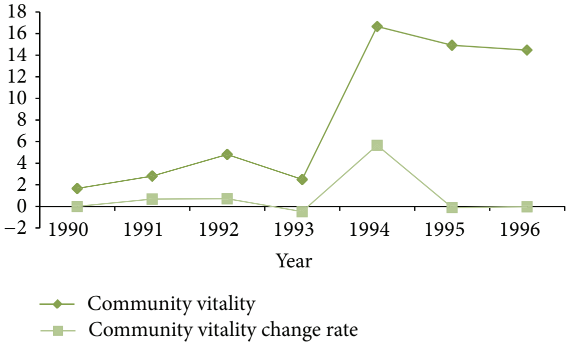


Figure 9: The 10th series of CDBLP CV and CVCR.

The value of CVCR $\Delta\,\mathrm{VI}(C_{t-1}^{p}, C_{t}^{q})$ has the following meanings.

If $\Delta\,\mathrm{VI}(C_{t-1}^{p}, C_{t}^{q}) > 0$, then C_{t}^{q} in the state of growing and the multiple of growth is $\Delta\,\mathrm{VI}(C_{t-1}^{p}, C_{t}^{q})$;

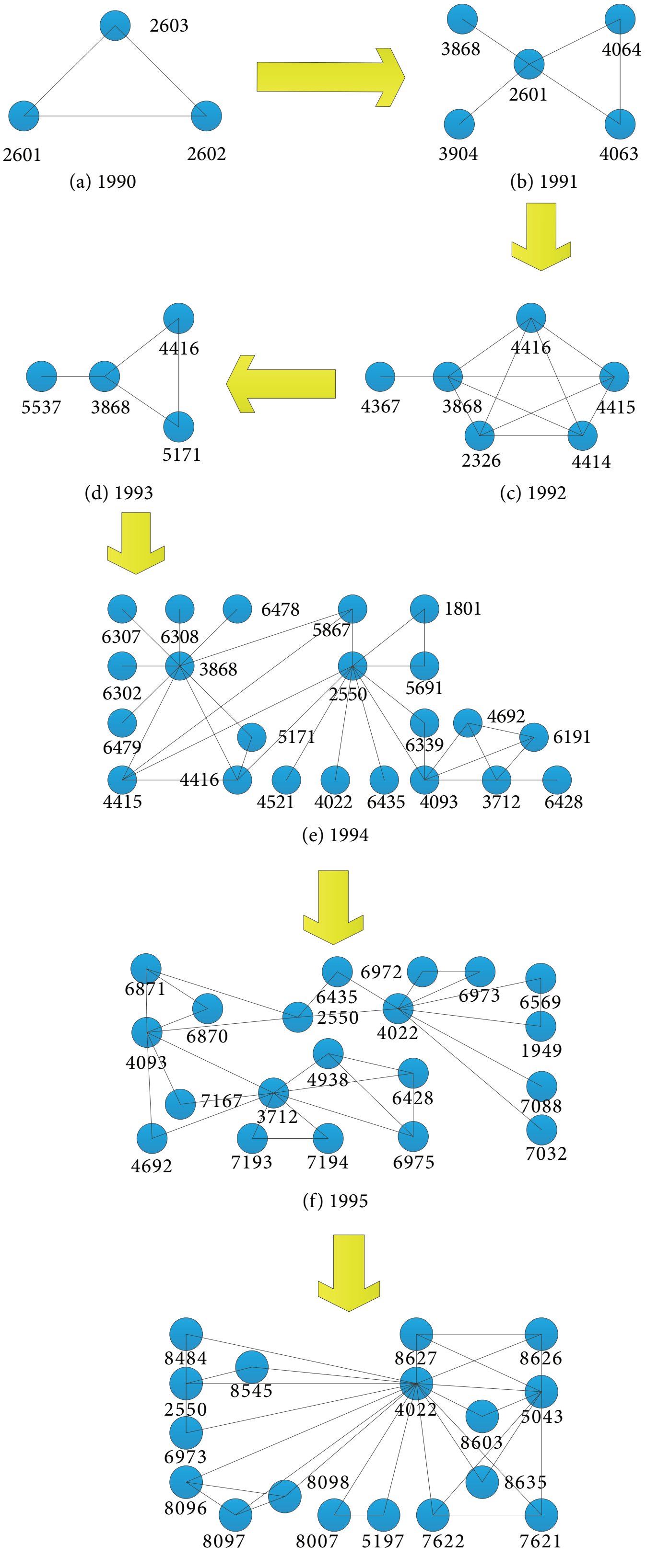
If $\Delta\,\mathrm{VI}(C_{t-1}^{p}, C_{t}^{q}) = 0$, then C_{t}^{q} has steady community structure;

If $\Delta\,\mathrm{VI}(C_{t-1}^{p}, C_{t}^{q}) < 0$, then C_{t}^{q} in the state of shrink and the shrink multiple is $|\Delta\,\mathrm{VI}(C_{t-1}^{p}, C_{t}^{q})|$.

4. Experiments and Analysis

In this section, experiments are carried out on two real datasets, Chinese DBLP Dataset (CDBLP) and Enron Email Dataset (EED). And then our method is analyzed and compared with some existing algorithms and methods.

4.1. Experiments. CDBLP was published by "Automation Discipline Innovation Method" research group of Chinese Academy of Sciences Institute of automation and it derived from the network of Computer Chinese Journal. The part of the data from 1985 to 1996 is used in our experiment. We set a year as the time interval and integrate annual data as a time slice data.



(a) 1990

(b) 1991

(c) 1992

(d) 1993

(e) 1994

(f) 1995

(g) 1996

Figure 10: Change of 10th series of community structure.

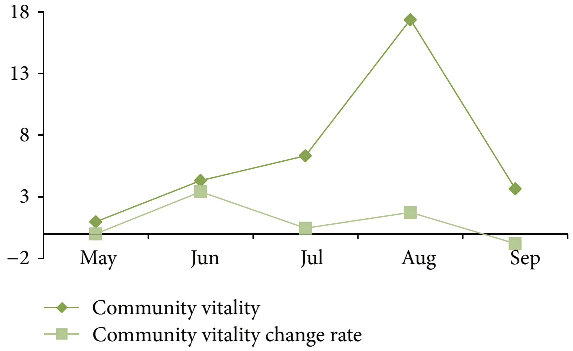


Figure 11: The 9th series of EED CV and CVCR.

EED was collected by CALO Project (a cognitive assistant that learns and organizes). The dataset represents the connections between employees. The part of the data in 2001 is used in our experiment. We set a month as the time interval and integrate each month data as a time slice data.

In Figures 3 and 6, N is the number of time slices in a community's lifecycle.

From the results (Figures 3, 4, 5, 6, 7, and 8), we can find the distribution of community's lifecycle. In fact, from the lifecycle distribution and CV change process of all communities in the network, structure features or rules of real system corresponded by the dataset are mined.

Figures 4 and 5 shows the change process of all communities' CV and CVCR during their lifecycle. Those communities in Figures 4 and 5 are formed from 12 years data of CDBLP and the communities whose lifecycle less than five time slices are ignored. Figures 7 and 8 show the change process of all communities' CV and CVCR during their lifecycle. Those communities in Figures 7 and 8 are formed from one year data of EED and the communities whose lifecycle are less than three time slices are ignored. By analyzing Figure 3 to Figure 8, we can get the following conclusions.

(1) The communities' lifecycles are generally short, which show that the relationships between users of the real systems are sustained for a short period of time.

(2) It can show the structure features or rules of the real system. Analyzing CDBLP, the number of papers published in the Computer Chinese Journal network is increasing over time. In other words, theoretical research is more and more popular, it actually has achieved outstanding progress. Analyzing EED, the communication between employees of Enron Corporation is in a stable state without obvious change over time in general.

(3) A community with big CV tends to have long lifecycle, which means that core leaders or core structure may be included in the community. And more attention need to be paid on this kind of community.

(4) In Figures 4–8, each line presents the evolution process of a community structure, in which the line's start point and terminal point represent the beginning and end of community lifecycle, respectively. In Figures 4 and 7, a point means a community's CV on a time slice. And in Figures 5 and 8, a point beside the first point represents the extent of communities' structure enlargement or decrease comparing with the community on the last time slice. Furthermore, we can find *"dead"* communities if a community's lifecycle ends; for instance, dead communities are the communities represented by the 3rd series and the 5th series on the time slice of April in Figure 7. Therefore, compared with other community detection algorithms, our algorithm cannot only find communities' structure and analyze its evolution process, but also quantify communities' life intensity on each time slice by analyzing CV.

In order to verify whether CV can correctly describe the change of growing or shrinking community structure, we randomly select two communities in the two real datasets (communities represent by the 10th series of Chinese DBLP Dataset and the 9th series of Enron Email Dataset), and then we compare the change of the community structure with the change process of CV and CVCR. Finally, we find the change process of community structure is consistent with the change process of CV. Now we use a series of the following diagrams (Figures 9, 10, 11, and 12) to give a specific verification.

Figure 10 shows structures of the community represented by the 10th series of Chinese DBLP Dataset on each time slice. By comparing arbitrary adjacent two pictures, we can obviously find that changes in the community's community structure can be described as increase, increase, decrease, increase sharply, decrease, decrease a little, and almost constant. On the last three time slices, the community's structure shows a steady state. On the whole, the change process of the community's structure is completely consistent with the change rules described in Figure 9 which shows the change process of CV.

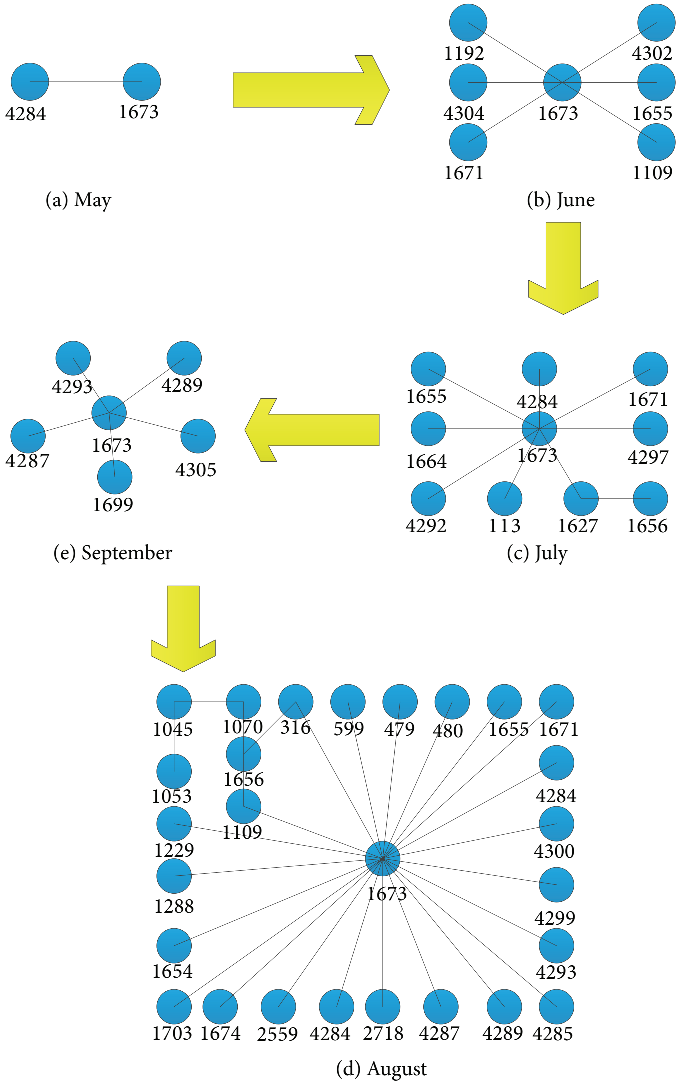
Figure 11 shows structures of the community represented by the 9th series of EED on each time slice. By comparing arbitrary adjacent two pictures, we can obviously find that changes in the community's community structure can be described as increase, increase slightly, increase sharply, and decrease. Because a community in EED whose community structure always centers on a node, the community's structure relies on the central node to survive; the aggregation of the community is poor. In fact, the change process of the community's structure is completely consistent with the change rules described in Figure 12 which shows the change process of CV.

4.2. Analysis. Our method is devote to study community structure's evolution based on CV quantificationally. Then a comparison of some proposed algorithms and methods is given as Table 1.

Furthermore, CV can quantify the change process of dynamic networks. On the one hand, it can be applied to mining change pattern of dynamic networks. On the other hand, we can use these laws to optimize applications, such as

Table 1: A comparison of some proposed algorithms and methods.

Algorithm	Static community detection	Dynamic community detection		Community evolution	
		CQA [4]	Incremental algorithm [12]	An event-based framework [5]	Our method
Obtaining community structure	√	√	√	√	√
Obtaining insignificance community	√	✗	✗	✗	✗
Detecting death community	✗	✗	✗	√	√
A community structure's change	✗	✗	✗	✗	√
Change process of communities on consecutive time slices	✗	✗	✗	√	√
Quantifying community state	✗	✗	✗	✗	√
Analysis community evolution quantificationally	✗	✗	✗	✗	√



(a) May

(b) June

(c) July

(e) September

(d) August

Figure 12: Change of 9th series of community structure.

optimizing communication of *adhoc* networks. Most practicable *adhoc* networks adopt the cluster-based routing protocols and a cluster can be treated as a relatively concentrated communication community. As the sample data showed in Figure 1, we assume that community B communicates with community D through community A or community C, and we acquire the change in communication condition of each cluster, shown as Figure 1(b) by setting appropriate monitoring points and collecting the communication between nodes at regular time interval. Via CV, community B can perceive that community A is a communication cluster in the state of steady and active gradually and community C is a communication cluster in the state of *"dying"*. Thus, community B can adjust the communication routing from community B to community D all through community A and communication efficiency of the communication routing will be better than that through community C.

5. Conclusion

In this paper, we put forward the concept of CV and design CI decision algorithm based on existing static community detection algorithm CNM, to calculate CVs. CV is defined for studying communities' life intensity and describing the process of community evolution quantitatively. Furthermore, the concept CV has many practical applications. The main contributions are as follows.

(1) Four critical events are proposed to describe community structure changes. And they are the basic of the research on the evolution of community structure.

(2) Three types of CSCEs (Keep, Separation, and Mergence) are defined, and then the computing method of CSS is designed under the three circumstances. By computing the value of CSS, inheritability between communities on consecutive time slices can be found out.

(3) Decision rules of CI are put forward in each type of CSCE and CI decision algorithm is designed. CI is designed to determine when a community is *"born"* or *"die"*; namely, a community's lifecycle can be presented. Also *"dead"* community can be mined.

(4) The core concept of CV is defined. CV can quantify a community's life intensity and describe the evolution process of community structure dynamically. Then CVCR is defined to find a community's state and change degree directly.

(5) We utilize two real datasets which are Chinese DBLP Dataset and Enron Email Dataset to perform experiments. And we use the figures to express the evolution process of community structure and randomly select two communities to verify the correctness of CV. In the end, simulated data is used to show that CV can be applied to communication of *adhoc* networks.

In future researches, we will focus on studying the applications of CV.

Acknowledgments

The paper is supported by China 973 Program (2014CB340600), NSF (60903175, 61272405, 61272033, and 61272451), and University Innovation Foundation (2013TS102 and 2013TS106).

References

[1] P. Holme and J. Saramäki, "Temporal networks," *Physics Reports*, vol. 519, no. 3, pp. 97–125, 2012.

[2] H. Kim and R. Anderson, "Temporal node centrality in complex networks," *Physical Review E*, vol. 85, no. 2, Article ID 026107, 8 pages, 2012.

[3] A. Clauset, M. E. J. Newman, and C. Moore, "Finding community structure in very large networks," *Physical Review E*, vol. 70, no. 6, Article ID 066111, 6 pages, 2004.

[4] N. P. Nguyen, T. N. Dinh, Y. Xuan, and M. T. Thai, "Adaptive algorithms for detecting community structure in dynamic social networks," in *Proceedings of the IEEE International Conference on Computer Communication (INFOCOM '11)*, pp. 2282–2290, Shanghai, China, April 2011.

[5] S. Asur, S. Parthasarathy, and D. Ucar, "An event-based framework for characterizing the evolutionary behavior of interaction graphs," *ACM Transactions on Knowledge Discovery from Data*, vol. 3, no. 4, article 16, 2009.

[6] Y.-R. Lin, H. Sundaram, Y. Chi, S. Zhu, and B. L. Tseng, "Facetnet: a framework for analyzing communities and their evolutions in dynamic networks," in *Proceedings of the 17th International Conference on World Wide Web (WWW '08)*, pp. 685–694, Beijing, China, April 2008.

[7] B. W. Kernighan and S. Lin, "An efficient heuristic procedure for portioning graph," *Bell System Technical Journal*, vol. 49, no. 2, pp. 291–307, 1970.

[8] A. Pothen, H. D. Simon, and K. Liou, "Partitioning sparse matrices with eigenvectors of graphs," *SIAM Journal on Metrix Analysis and Applications*, vol. 11, no. 3, pp. 430–452, 1990.

[9] M. Girvan and N. E. J. Newman, "Community structure in social and biological networks," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 99, no. 12, pp. 7821–7826, 2001.

[10] M. E. J. Newman, "Fast algorithm for detecting community structure in networks," *Physical Review E*, vol. 69, no. 6, Article ID 066133, 5 pages, 2004.

[11] U. N. Raghavan, R. Albert, and S. Kumara, "Near linear time algorithm to detect community structures in large-scale networks," *Physical Review E*, vol. 76, no. 3, Article ID 036106, 11 pages, 2007.

[12] H.-F. Wang, L.-P. Huang, and S. Yu, "An incremental community discovering approach," *Computer Simulation*, vol. 25, no. 1, 2008.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 594627, 7 pages
http://dx.doi.org/10.1155/2013/594627

Research Article

Developing a Mobile Learning System in Augmented Reality Context

Da-Ren Chen, Mu-Yen Chen, Tien-Chi Huang, and Wen-Pao Hsu

Department of Information Management, National Taichung University of Science and Technology, 129 Section 3, San-Min Road, Taichung 40444, Taiwan

Correspondence should be addressed to Mu-Yen Chen; mychen@nutc.edu.tw

Received 4 October 2013; Accepted 2 December 2013

Academic Editor: Neil Y. Yen

In recent years, many emerging information technologies have been applied to learning environments in an attempt to overcome drawbacks associated with traditional teaching environments. Some of these technologies have been shown to improve learning outcomes and learning motivation. Advances in wireless communications have raised research interest in the development of ubiquitous learning (u-learning) environments and their impact on learner attitudes and behavior. This study reports the use of augmented reality (AR) technology to create virtual objects for use in mobile devices to create a context-aware, AR-enabled guided tour application for outdoor learning. The goal is to provide learners with a friendly, interactive interface and rich, engaging media to stimulate intrinsic motivation and learning performance. The main advantages of the proposed system include the following: (1) it helps stimulate learning intention through pursuing outdoor learning objectives, (2) AR technology provides learners with contextual information related to the outdoor learning environment, and (3) it enhances learner retention of teaching contents easily with the situated learning strategy.

1. Introduction

Rapid advances in information technology have created venues for organized learning beyond the traditional classroom, especially through the use of mobile devices to create opportunities for context-aware ubiquitous learning [1, 2]. In traditional classroom learning environments, instruction is conducted through lectures and activities provided by the teacher along with course books and audio-visual materials. Learners listen to their teachers' instruction while receiving visual cues through PowerPoint presentations, handouts, or whiteboard content before participating in learning activities or group discussions. However, traditional classroom learning is normally quite structured and is limited to preexisting teaching materials or preplanned learning activities.

M-learning has recently emerged as a trend in instruction, offering learners with networked mobile devices unprecedented convenience and allowing them to learn anywhere, anytime [3–5]. In contrast to traditional classroom instruction, m-learning allows learners to use Internet resources, multimedia technologies, and virtual team skills in online discussions, exams, video conferencing, and other activities. Ubiquitous learning overcomes time and place limitations to allow engagement in reality-based learning applications through which they experience, explore, and develop problem solving skills, thus improving learner motivation [6].

Hwang et al. claimed that the formation of individual knowledge is structured by practice and past experience [7]. Hence, the traditional classroom environment cannot help improve learners' concentration nor can the teacher immediately determine whether knowledge acquisition has occurred [8]. Through ubiquitous learning, learners can form their own concepts and knowledge and take responsibility for their own behavior through learning methods based on constructionism [9, 10]. In a traditional classroom teaching environment, teachers unilaterally provide supplementary material through text and/or images, leading to learner disengagement. U-learning methods can replace classroom learning in a way that allows learners to obtain situated knowledge in the real-world environment [11].

This research integrates radio frequency identification (RFID) and augmented reality (AR) technologies on mobile

Table 1: Learning methods comparison.

	Traditional digital learning network	Mobile and ubiquitous learning
Learning features	(1) No distance limitations (2) Comprehensive learning (3) The information received synchronously or asynchronously	(1) No distance limitations (2) Comprehensive learning (3) Synchronous or asynchronous way (4) Placed in a real environment (5) Learning to accept real-time information
Learning technology tools	(1) PC (2) Notebook (3) Wireless support equipment	(1) Mobile devices (2) Wireless support equipment (3) Radio-frequency identification
The main source of information	Connected servers	Wireless servers and physical connection
Learning contexts	Passive online learning environment	Real-world and passive online learning environment
Related teaching theories or strategies	Almost all teaching theory or teaching strategies	Almost all teaching theories or teaching strategies, especially on program-based learning, authentic learning environment, and scaffolding learning

devices. The learner uses the device while exploring a geopark, looking up supplementary information and acquiring knowledge through situational purpose-driven learning. In this way, learners can take the initiative to explore learning, actively constructing new knowledge [12]. This research adapts innovative information technologies to create learning activities, enabling learners to explore geology in depth and stimulate learner motivations to study and understand geological concepts and knowledge.

2. Literature Review

2.1. RFID Technology. Reduced costs and improved performance of RFID hardware hold promise for the development of new smart living applications [13]. RFID allows for automatic identification of objects and the wireless transmission of various kinds of data from an RFID tag attached to the target object to RFID readers [14].

Hwang et al. integrated the use of concept maps and ubiquitous learning applications using mobile devices and RFID technology to help learners assess their knowledge acquisition following learning actives [15]. Their approach allows learners to learn anytime, anywhere, using their handheld mobile devices to engage in learning on demand. Hwang et al. created a u-learning environment in the Southern Taiwan Science Park, using RFID systems to teach astronomical concepts [7].

2.2. Ubiquitous Learning RFID/Wireless. Ubiquitous learning is broadly defined as "anytime, anywhere learning" [7]. Over the past 10 years, advances in wireless networks, sensor technology, and mobile devices have contributed to the development of this innovative teaching model [16]. Innovations in technology now allow students to learn in real world environments with the digital devices providing personalized instruction [17]. Such a learning mode has several advantages as follows [11] and listed in Table 1.

(i) Easy access to new knowledge and sharing information: using mobile devices, students access the desired information or knowledge anytime and anyplace [15].

(ii) Unlimited learning venues: with their mobile devices, students can learn at any location or on the go, both indoors and outdoors [18].

(iii) Real-world, situated learning: mobile learning allows learners to access information in highly contextualized situations, drawing on resources which enrich their understanding of their immediate surroundings and context. Knowledge is presented in authentic contexts, thus enhancing learner autonomy, and the use of the proposed system in group activities can promote peer interaction [19].

(iv) Students can record their learning process in real-life situations: the outdoor learning course allows students to engage supplementary course material in the context of their authentic surroundings and provides a complete record of the learning process, providing a basis for recommendations from instructors or expert systems [20].

2.3. Augmented Reality Integrated into Learning. Augmented reality uses a calculated field position and camera angle to impose a layer of virtual objects over the "real-world" background [21]. Users can not only immerse themselves in the combined virtual and real-world scenes but also interact with the virtual objects and access relevant and useful information [22].

Until recently, augmented reality applications were limited to "hot-spots" providing limited supplementary information at specific points on guided tours. However, the technology has advanced significantly in recent years to the point where it can now be used to effectively increase learning motivation and engagement without the need for purpose-built hardware. AR systems can be designed to provide students with personalized scaffolding and support and help them construct personal knowledge as they observe and experience real-world contexts [23, 24].

Augmented reality technology is developing rapidly. Both the Android and iPhone operating systems support AR in navigation features, providing users with location-specific

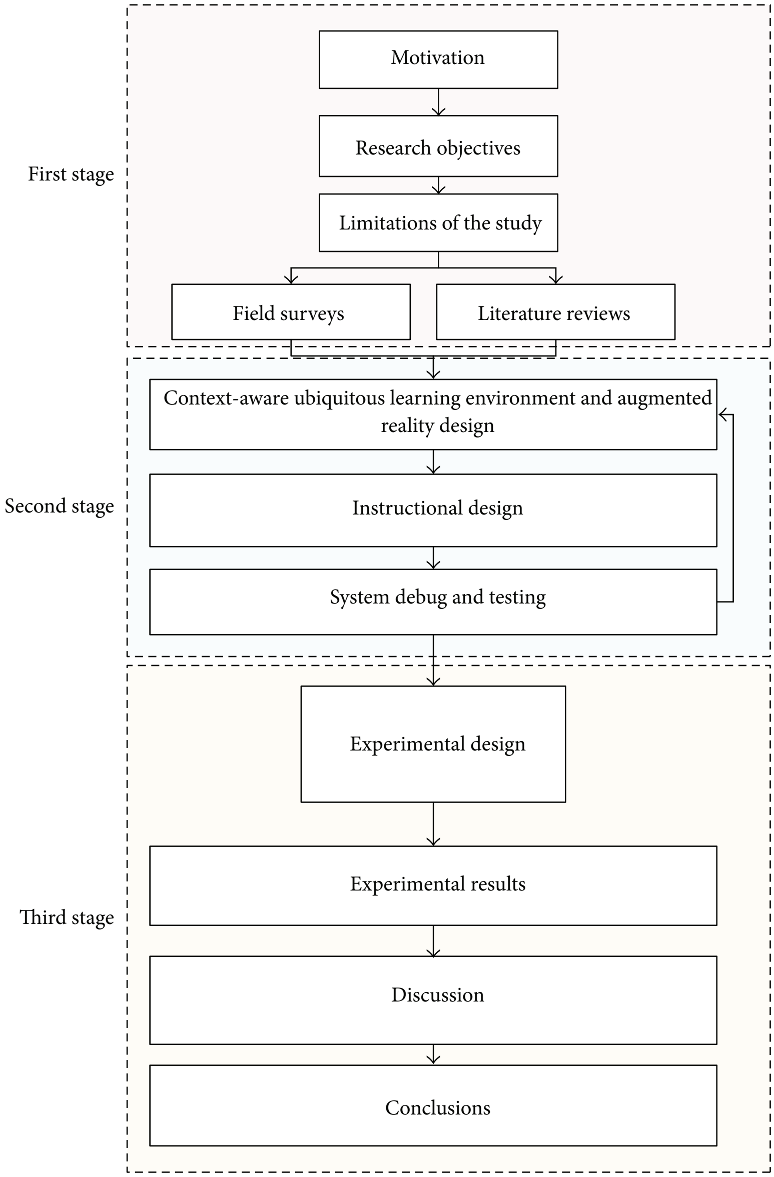


Figure 1: Research flowchart.

information. Images have a stronger impact on memory than text, thus layering supplementary images and information over the real world environment in the AR environment can promote knowledge retention [25].

Liarokapis et al. proposed an interactive Multimedia Augmented Reality Interface for E-learning (MARIE) system and developed a user-friendly interface to explore the potential for AR in instruction by superimposing virtual multimedia content (VMC) information in an AR tabletop environment [26]. Matcha and Awang Rambli investigated the potential of AR spaces to supply communication cues and promote collaboration in learning environments. Their empirical results indicated that AR techniques have significant potential to serve as a shared medium in collaborative learning [27].

3. Methodology

3.1. Research Process. This research integrates a context-aware ubiquitous learning environment and AR techniques, using content based on the Yehliu Geological National Park. The application design and testing process were conducted in three stages detailed as follows and also showed in Figure 1.

(1) First stage: catalog the required learning material regarding the Yehliu Geological State Park, and create appropriate teaching materials for integration into the AR application. This stage contains two steps as follows.

(a) Field surveys: interviews with park's staff and surveys of legacy systems, to gather material for use in the construction of the content for the context-aware ubiquitous learning system.

(b) Literature review: review studies of relevant technologies and learning theories to determine the technical feasibility of the proposed approach, combining ubiquitous learning, augmented reality, and RFID along with research on the design principles for acquired learning systems.

(2) Second stage: develop the ubiquitous learning system and integrate the developed content for testing.

(a) System implementation: the D'Fusion software platform is used for Android-based development, creating presentations based on plan views and 3D graphs perspective views.

(b) Instructional design: layer the teaching materials in the AR environment to increase richness and engagement. The AR content is layered on top of real images of the geological formations, thus improving learner recall. Student knowledge acquisition and learning outcomes are measured experimentally through questionnaires, and interviews are used to solicit user feedback.

(c) System testing and debugging: check to ensure the system works reliably, and use learner feedback to determine how to improve system performance and usability.

(3) Third stage: assess learner response to the system.

(a) Experimental design assessment: observe learners in the process of using the proposed u-learning system to achieve predetermined tasks in Yehliu Geological Park. System effectiveness and learning outcomes are assessed using a questionnaire after the usage session.

(b) Conclusion and recommendations: questionnaire responses are analyzed to assess user perceptions of and reactions to the proposed system and to obtain ideas for potential improvements to the system and content.

3.2. Experimental Design Environment. The proposed u-learning system incorporates radio frequency identification (RFID) and augmented reality (AR) technologies on mobile devices, allowing the learner to immediately access supplementary information on geological objects observed in the geopark. This section describes the hardware and software requirements of the proposed system.

Hardware requirements include a mobile device providing Internet access and an RFID-enabled environment. RFID tags and readers are used to identify individual students/users and to record learner progress and scores. An HTC Sensation XL mobile phone and an ASUS Eee Pad Transformer Prime TF201 Tablet PC were used as the mobile devices in system development and testing. The RFID-enabled environment was built using active RFID readers and tags, wherein the tag draws on an internal power supply to detect signals transmitted by the RFID reader and to reply back to the reader [28, 29].

Software requirements include platform-specific software development kits and an augmented reality development environment. Eclipse was used as development for Android 4.0.1 because it offered many relevant development tools and good compatibility [30]. AR development was done using D'Fusion on an Android platform, with the ubiquitous learning system developed from plan views and 3D graphs. D'Fusion offers better performance by using additional graphs in place of real-time computing effects for light/shadow and material textures.

4. Experimental Design and Results

4.1. System Architecture and Module Description. Situational awareness was used to allow users to follow learning activities along a predetermined route, using the augmented reality features to engage in image memory-based learning to increase comprehension and retention. Figure 2 shows the system architecture, and each module and function is described in detail below.

4.1.1. Teachers. Teachers can use a classroom version of the AR system to introduce system usage and content in the classroom. In traditional classrooms, learners can only learn about nature through text and pictures, making it difficult for them to truly understand the essence of the natural sciences. However, using the proposed system, the teacher in the classroom can lead students through the supplemental teaching material at various difficulty levels.

The system offers two modules through which teachers can customize the content and activities. The first is the teaching plan management module, which allows teachers to select an appropriate level of difficulty for the learning objectives. The other module is the content management module, allowing teachers to easily swap different activities in or out of the course. In the module, all teaching materials are classified according to level of difficulty, allowing teachers to, for example, adjust the difficulty of the reading program to continuously challenge learners. Learners can also use ancillary and supplemental teaching materials in the AR environment, using geographical location information to elevate their learning efficiency.

4.1.2. Learners. The system logs all learner activity, automatically adjusts the scope of learning objectives, selects an appropriate learning difficulty level, and updates parameters according to learner search results. While navigating the learning path, learners can engage with one topic after another. In the traditional classroom, learners often have difficulty keeping pace with a teacher's presentation because of a lack of understanding. Using the proposed u-learning system, students can repeatedly engage with the instructional material at his or her own pace, thus developing a sound understanding of the topic.

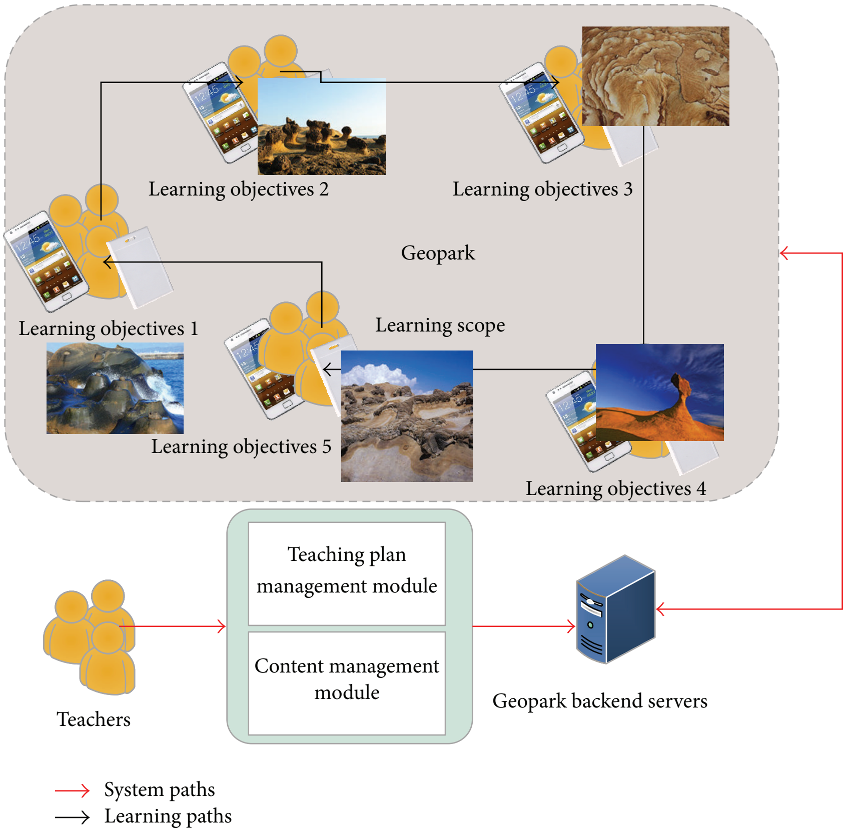
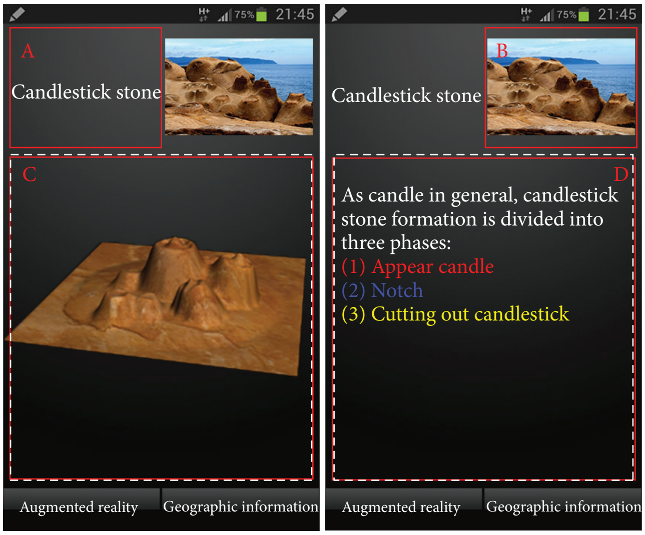


Figure 2: Ubiquitous learning system architecture diagram.

4.2. Augmented Reality Interface and Operations. The AR interface allows users to follow a series of learning activities and targets along a predetermined context-aware route. When observing a particular object, the learner clicks the Augmented Reality button to access supplementary information about the object. The action of actively seeking out supplementary knowledge promotes knowledge acquisition and retention. In addition, learners can access contextualized geographic information by clicking the Geographic Information button. Figure 3 illustrates the AR interface. Area "A" provides the name of the learning objectives, while "B" provides an image. Area "C" provides an augmented reality view of the learning objectives, while area "D" provides relevant geological information.



As candle in general, candlestick stone formation is divided into three phases:
(1) Appear candle
(2) Notch
(3) Cutting out candlestick

Figure 3: AR interface.

5. Conclusions

Augmented reality and RFID technologies were integrated to create contextually-aware instructional system for use in outdoor environments. Content specific to the Yehliu Geological Park in northern Taiwan was adapted to the platform, allowing students to engage in self-paced learning activities and exploration along a predetermined trail in the park. The system was designed to increase learner engagement and autonomy, while improving knowledge acquisition and retention.

The system helps learners easily develop an understanding of local geological and cultural conditions. The immediacy of the environment increases learner engagement, with the potential of sparking learner motivation for further exploration and learning.

This research has some limitations and they need to be addressed in future work. Some learners indicated that software and hardware limitations resulted in unacceptably long latency to load relevant content. Since the platform was developed to improve learner engagement and learning outcomes, latency and other ease of use issues must be improved.

Acknowledgment

The authors would like to thank the National Science Council of the Republic of China, Taiwan, for financially supporting this research under NSC 102-2221-E-025-003, NSC102-2622-E-025-001-CC3, and NSC-101-2622-E-025-002-CC3.

References

[1] T. C. Huang and C. C. Chen, "Animating cvic education: developing a knowledge navigation system using blogging and topic map technology," *Journal of Educational Technology & Society*, vol. 16, no. 1, pp. 79–92, 2013.

[2] M. Y. Chen, M. T. F. Chang, C. C. Chen, M. J. Huang, and J. W. Chen, "Why do individuals use e-portfolios?" *Journal of Educational Technology & Society*, vol. 15, no. 4, pp. 114–125, 2012.

[3] K. S. Chung and J. E. Lee, "Design and development of m-learning service based on 3G cellular phones," *Journal of Information Processing System*, vol. 8, no. 3, pp. 521–538, 2012.

[4] C.-M. Chen and Y.-L. Li, "Personalised context-aware ubiquitous learning system for supporting effective english vocabulary learning," *Interactive Learning Environments*, vol. 18, no. 4, pp. 341–364, 2010.

[5] S. Oh, "Using an adaptive search tree to predict user location," *Journal of Information Processing System*, vol. 8, no. 3, pp. 437–444, 2012.

[6] C. C. Chen and T. C. Huang, "Learning in a u-museum: developing a context-aware ubiquitous learning environment," *Computers & Education*, vol. 59, no. 3, pp. 873–883, 2012.

[7] G. J. Hwang, C. C. Tsai, H. C. Chu, Kinshuk, and C. Y. Chen, "A context-aware ubiquitous learning approach to conducting scientific inquiry activities in a science park," *Australasian Journal of Educational Technology*, vol. 28, no. 5, pp. 931–947, 2012.

[8] G.-J. Hwang, H.-C. Chu, Y.-S. Lin, and C.-C. Tsai, "A knowledge acquisition approach to developing mindtools for organizing and sharing differentiating knowledge in a ubiquitous learning environment," *Computers & Education*, vol. 57, no. 1, pp. 1368–1377, 2011.

[9] D. Gallego and G. Huecas, "An empirical case of a context-aware mobile recommender system in a banking environment," *Journal of Convergence*, vol. 3, no. 4, pp. 41–48, 2012.

[10] Y. Zhu and Q. Jin, "An adaptively emerging mechanism for context-aware service selections regulated by feedback distributions," *Human-Centric Computing and Information Sciences*, vol. 2, article 15, 2012.

[11] C.-S. Chang, T.-S. Chen, and W.-H. Hsu, "The study on integrating WebQuest with mobile learning for environmental education," *Computers & Education*, vol. 57, no. 1, pp. 1228–1239, 2011.

[12] R. T. Azuma, "A survey of augmented reality," *Presence*, vol. 6, no. 4, pp. 355–385, 1997.

[13] C. C. Chen and Y. F. Chang, "Developing a smart shopping automation system: ambient intelligence in practice," *Ad Hoc & Sensor Wireless Networks*, vol. 20, no. 1-2, pp. 95–105, 2014.

[14] C. C. Chen and Y. F. Chang, "Smart healthcare environment: design with RFID technology and performance evaluation," *Journal of Medical and Biological Engineering*, vol. 33, no. 4, pp. 427–432, 2013.

[15] G.-J. Hwang, P.-H. Wu, and H.-R. Ke, "An interactive concept map approach to supporting mobile learning activities for natural science courses," *Computers & Education*, vol. 57, no. 4, pp. 2272–2280, 2011.

[16] J. K. Y. Ng, "Ubiquitous healthcare: healthcare systems and applications enabled by mobile and wireless technologies," *Journal of Convergence*, vol. 3, no. 2, pp. 15–20, 2012.

[17] B. J. Oommen, A. Yazidi, and O. C. Granmo, "An adaptive approach to learning the preferences of users in a social network using weak estimators," *Journal of Information Processing System*, vol. 8, no. 2, pp. 191–212, 2012.

[18] E. Klopfer, K. Squire, and H. Jenkins, "Environmental detectives: PDAs as a window into a virtual simulated world," in *Proceedings of IEEE International Workshop on Wireless and Mobile Technologies in Education*, pp. 95–98, 2002.

[19] T.-Y. Liu, T.-H. Tan, and Y.-L. Chu, "Outdoor natural science learning with an RFID-supported immersive ubiquitous learning environment," *Educational Technology & Society*, vol. 12, no. 4, pp. 161–175, 2009.

[20] E. von Glasersfeld, "An introduction to radical constructivism," in *The Invented Reality*, P. Watzlawick, Ed., pp. 16–38, Norton, New York, NY, USA, 1984.

[21] C.-M. Chen and Y.-N. Tsai, "Interactive augmented reality system for enhancing library instruction in elementary schools," *Computers & Education*, vol. 59, no. 2, pp. 638–652, 2012.

[22] Á. di Serio, M. B. Ibáñez, and C. D. Kloos, "Impact of an augmented reality system on students' motivation for a visual art course," *Computers & Education*, vol. 68, pp. 586–596, 2013.

[23] A. M. Kamarainen, S. Metcalf, T. Grotzer et al., "EcoMOBILE: integrating augmented reality and probeware with environmental education field trips," *Computers & Education*, vol. 68, pp. 545–556, 2013.

[24] P.-S. Tsai, C.-C. Tsai, and G.-H. Hwang, "College students' conceptions of context-aware ubiquitous learning: a phenomenographic analysis," *Internet and Higher Education*, vol. 14, no. 3, pp. 137–141, 2011.

[25] P. Milgram, H. Takemura, A. Utsumi, and F. Kishino, "Augmented reality: a class of displays on the reality-virtuality continuum," in *Telemanipulator and Telepresence Technologies*, vol. 2351 of *Proceedings of SPIE*, pp. 282–292, November 1994.

[26] F. Liarokapis, P. Petridis, P. F. Lister, and M. White, "Multimedia Augmented Reality Interface for E-learning (MARIE)," *World Transactions on Engineering and Technology Education*, vol. 1, no. 2, pp. 173–176, 2002.

[27] W. Matcha and D. R. Awang Rambli, "Preliminary investigation on the use of augmented reality in collaborative learning," *Communications in Computer and Information Science*, vol. 254, no. 4, pp. 189–198, 2011.

[28] T.-H. Tan, T.-Y. Liu, and C.-C. Chang, "Development and evaluation of an RFID-based ubiquitous learning environment for outdoor learning," *Interactive Learning Environments*, vol. 15, no. 3, pp. 253–269, 2007.

[29] E. W. T. Ngai, K. K. L. Moon, F. J. Riggins, and C. Y. Yi, "RFID research: an academic literature review (1995–2005) and future research directions," *International Journal of Production Economics*, vol. 112, no. 2, pp. 510–520, 2008.

[30] D.-H. Shin, Y.-J. Shin, H. Choo, and K. Beom, "Smartphones as smart pedagogical tools: implications for smartphones as u-learning devices," *Computers in Human Behavior*, vol. 27, no. 6, pp. 2207–2214, 2011.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 690902, 8 pages
http://dx.doi.org/10.1155/2013/690902

Research Article

A Study of Smart Power Control Algorithm Using RF Communication in Smart Home Environment

Su-hong Shin,[1] Kyoung-hwa Do,[2] and Byoung-soo Koh[1]

[1] *Digicap Co., Ltd., Republic of Korea*
[2] *Ministry of Security and Public Administration, Republic of Korea*

Correspondence should be addressed to Kyoung-hwa Do; doda0905@gmail.com

Received 9 September 2013; Accepted 24 October 2013

Academic Editor: James J. Park

Today's technologies in the IT area face the era of combination and convergence of technologies in many different areas. Through the natural interaction between people and devices in the environment where various kinds of devices are connected over a single network, they have been developing from human-oriented service technologies to smart and futuristic home technologies. Smart home technology is one of them. It is a technology of establishing a digital home in which various kinds of home appliances are connected over a home network and diverse services are provided for users regardless of time and place. Technologies in the IT area are combined with technologies in many different areas, creating and producing numerous technologies. Also, much research on smart home, the theme of this work, has actively been conducted. In this work, the use of a current booster, an AC/DC converter, and a DC/DC converter to operate electric lights; this work implements the smart power control system using standby power and RF communication, among smart home technologies.

1. Introduction

1.1. Overview of the Study. Smart home refers to a home to which various digital convergence technologies are applied in the course of changing from the analogy era to the digital era. Today, regardless of place and type, digital technologies are used in every part of our life. People who lived in the past analog era now experience fast changes in their life of the present digital era. For instance, cassette tapes used in the past changed to MP3, analog TVs to digital TVs, and film cameras to digital cameras. In other words, our life is gradually changing from analogy life to digital one. The fast spreading of various digital devices, in fact, is not because of the development of the time, but because of the support of technologies helping to share a variety of information on the high speed internet. Through the internet and network, we are able to control or manage various digital devices. By connecting each one of different digital devices, we can control and manage all things that have something to do with us. As a result, smart home provides us with diverse services. Figure 1 presents a consumer service environment in a smart home [1].

As shown in Figure 1, smart home includes convergence of various services, including security, health, work, energy, environment, and communication, which are connected together on a single network.

One of these technologies is u-Health. u-Health has changed by various consumer service environments and is now different from past methods. Contrary to the previous method in which a wired instrument was attached to the user's body and the user's body data was taken, the current method involves collecting the user's body data using various wireless instruments. In other words, the traditional wired network environment is not used as much as the wireless network environment. The wireless network environment enables the use of systems that include but are not limited to personal computers and smartphones. In addition to collecting the user's body data, the wireless environment helps users to manage their diet and health [2].

Technologies for collecting user data in diverse environments and providing information that is necessary to users based on the collected data are also studied [3].

Through smart home, it is possible to provide ecoenergy system service. The value of smart home is basically in the

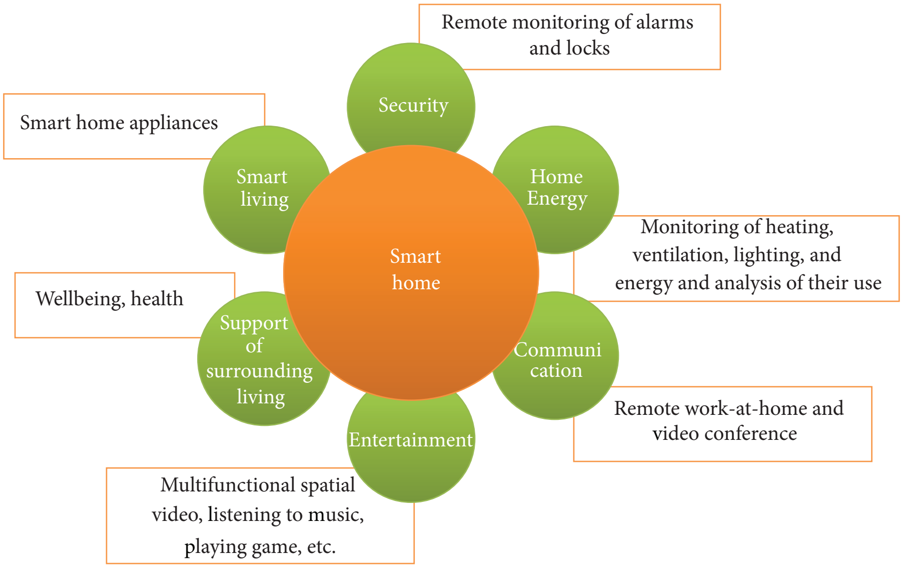

Remote monitoring of alarms and locks
Security
Smart home appliances
Smart living
Home Energy
Smart home
Monitoring of heating, ventilation, lighting, and energy and analysis of their use
Wellbeing, health
Support of surrounding living
Communi cation
Remote work-at-home and video conference
Entertainment
Multifunctional spatial video, listening to music, playing game, etc.

Figure 1: A consumer service environment in a smart home.

extension line of home automation, referring to a further advanced concept of it. The main features of smart home are presented as follows.

The First One Is Smart Control. It is one of important features of smart home. Smart control includes improved control ways like motion control and serves the function of remotely monitoring each state of home appliances through smartphones or tablet PCs.

The Second One Is Smart Power-Saving. Consumers pay great attention to energy-saving. Smart home appliances can help to minimize energy cost according to consumers' patterns.

The Third One Is Smart Application. Smart home provides applications suitable for the features of smart home appliances, so that it is possible to increase the usability of smart devices. In particular, home appliances with a screen like TV can expand their functions with the help of applications [4].

Smart home is in the initial stage in terms of technological development, and therefore it has yet to provide perfect implementation. For this reason, the purpose of this work is to implement a system to monitor and control a smart home at any time and place, as smart home will be popularized and interoperate with various devices.

Smart home allows various kinds of equipment and devices to get connected on a network, helps users to receive and monitor proper information at any time and place, and makes possible better quality of life through a wide range of services in everyday life.

1.2. The Necessity and Importance of the Study. With the emergence of ubiquitous and digital convergence environments, smart home contributes to an improvement in individuals' quality of life and to providing of services regardless of time and place. Thanks to the development of network technology, all information devices and home appliances are connected and controlled on a single network. The environment is called smart home.

Smart home serves the function of connecting a variety of conventional digital devices and the function of using them as if they are a single digital system by using wired and/or wireless networking technologies, such as radio frequency (RF), ZigBee, Bluetooth, and Ethernet [5].

Thanks to the fusion of IT technologies, machine to machine (M2M) communication, which has a number of meanings, has significantly changed our lives. As information collection and utilization are extended from men to machines, new services and technology have become necessary. Thus, M2M communication services have encouraged the development of a new business model for mobile communication enterprises and the smartphone industry.

M2M communication can refer to machine to machine, mobile to machine, and machine to mobile communication. M2M, also called machine intelligence communication, may mean the communication between a machine and a person, or between a device and another device. In a broad sense, M2M is the concept of networking the machines and the devices that are widespread throughout our daily lives. M2M enables us to check and control an object, system, vehicle, state of a person, and positional information from a remote place by combining communication and information technologies. M2M communication enables us to use various devices, from a computer mainframe to the daily electronic products, by connecting them with each other. For example, M2M can be applied to home electric appliances, transportation, such as a car, or a residential building. This concept enables machines or devices to transmit the desired data from a remote place through a mobile communication network or transmission media. The current concept of M2M communication is being extended to utilize various wired and wireless networks beyond the global standard for mobile communication (GSM) network. The concept is for machines or devices to transmit their own data from a remote place through a communication network, such as a mobile communication network. Various data, such as position, health status, and temperature, may be acquired through the interaction between a person and a machine. M2M is the next-generation network and will create added value by integrating the current assets of all the companies, such as an IT system, through the combination of information communication and information technology for an automated processer [6].

Although much research on the ways of connecting a variety of equipment in a smart home has been conducted, research on consumption power of each digital device just began. Implementation of a smart home brings about advantages yet causes some disadvantages, one of which is a great deal of consumption power caused by the connection of home appliances.

One of the major problems is the security problem. Security may be an issue when exchanging data among devices in an environment where various devices are combined without a standard protocol. In receiving information from a variety of devices, the data protocol and the vulnerable security areas will be attacked by hackers. In solving the security problem, the unsecured protocol and the vulnerable parts may be safely protected through message integrity, use of cipher, and personal information protection policy [7].

The degree to which data losses are minimized in wireless network environments is important in sensor networks, as the smaller the data losses, the higher the reliability [8].

Another drawback is the inefficient management of energy. This article suggests a method to solve the inefficient energy management problem.

Korea's energy consumption is dependent on overseas accounts for 97%. Along with an increase in Korea's income level, Korea as an energy dependent country sees annual rises in living energy consumption (household, commercial, etc.) and transportation energy consumption [9]. In particular, because the use of home appliances and office device leads to an increase in electric energy consumption in a home, more attention has been paid not only to the electricity amount consumed at the time of using devices, but also to the standby power consumed at the time when devices are plugged in. Annually, power consumption caused by the standby power is on the rise, accounting for about 10% of the entire energy consumption in a home [10]. Therefore, it is necessary to recognize the circumstance and develop a system to reduce the standby power. Accordingly, in designing smart home service, this work tries to use the standby power for other purposes and thereby provides various services in a smart home. This work tries to make an RF-based light switch controller power supply device by using quiescent current which flows in electric lights installed in each room of a house. We can block the standby power of general home appliances we use by plugging them out. But, electric lights are exceptional. A current always flows in electric lights, and as a result, the standby power consumption of electric lights used in a large factory or a public institute is very high, though that used in a house is low. This work tries to use the standby power of electric lights and implement a system that can control and turn on/off multiple electric lights at any time and place through smartphones [11].

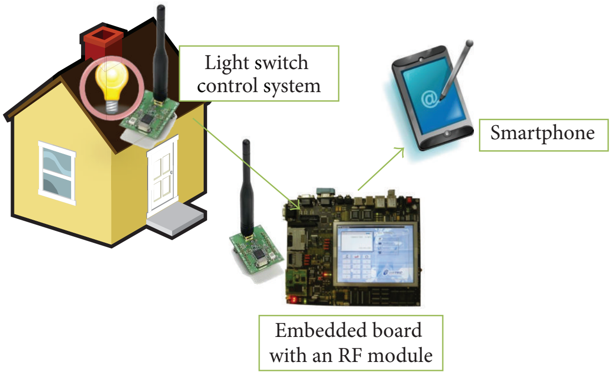


Figure 2: A scenario of the smart power control system proposed in this work.

2. Design of a Smart Power Control System

2.1. A Scenario of a Power Control System. It is assumed that the smart power control system proposed in this work is able to help users to turn on/off electric lights in a home at any time and place. For making a light switch on or off, a module to control the switch and a board with an RF module are installed. The relevant system is operated by the use of standby power. In fact, the standby power is not powerful enough to operate the system. So, this research designed the system that has multiple-trans connected in series and extracts a current from each trans. As a result, the system is operated by the currents accumulated from the trans connected in series and helps a user to control a light switch at any place of a house through RF communication. Figure 2 illustrates the scenario suggested in this work.

In this work, data between the RF switch and the embedded board are transmitted through a CC1020 RF module, and data between the embedded board and a smartphone are transmitted over TCP/IP. Since data are gathered in real time, they can be monitored in real time, the embedded board can control an electric light in real time, and a user can control an electric light through a smartphone. The differences between the system and other conventional systems are that the system efficiently uses standby power and that the system controls a device through an embedded board, rather than a PC. Because of the use of an embedded board, the system has advantages of low price, mobility, low consumption power, and replace ability of an embedded board. Given the aspects, the system provides the environment most suitable for a smart home.

2.2. A Data Transmission Device. In this work, the data transmission device uses an RF module with CC1020 chipset. The RF module is a low power RF TX/RX module with 400 MHz. The module supports 402~470 MHz in terms of frequency bandwidth, supports 153.6 Kbps at the maximum speed, and consumes 16.2 mA at Tx, 19.9 mA at Rx, and 1.8 uA at standby mode. It is attached to a switch and an

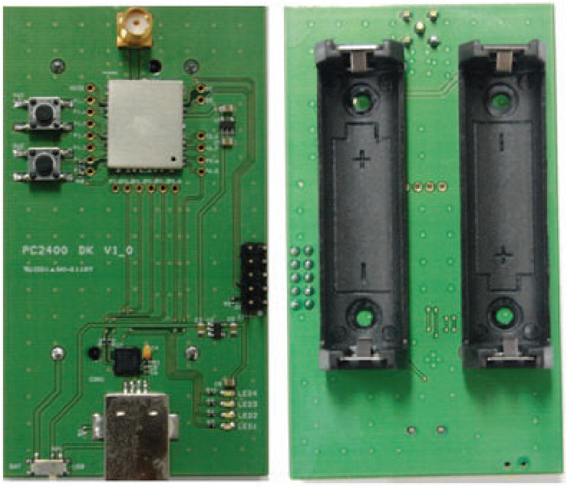


Figure 3: The RF module on which CC1020 is mounted.

embedded board, helping to send and receive data between both devices. The reason why this work uses the CC1020 module is that the Zigbee module of CC2420 or CC2500 mostly used these days arises as an issue in terms of radio wave certification and data reliability. However, CC1020 does not require a radio wave certificate and shows the highest data reliability at 400 MHz. For this reason, it is used in this work. A microprocessor of the communication module in this work is ATmega16L. ATMega16L uses CC1020 chipset, has a communication program built in, transmits communication packets through the serial communication with MCU, and supports MAC function. It serves the function of controlling CC1020 through the communication with SPI and DIO. The CC1020 used in this work have advantages of a small size, low battery consumption, and a wide range of RF signal strength.

2.3. The Equipment for the Control of the Smart Power Control System. For the control of the smart power control system, an imbedded board, instead of a conventional personal computer, was employed. An imbedded board is cheaper than a personal computer and easy to move and install, and it is possible to replace a module when there is a problem. Additionally, an imbedded board consumes significantly less electrical power than a personal computer. Thus, it is suitable for this research project.

2.3.1. RF Data Transmission and Reception Instrument. The system employs a low power RF TX/RX module using 400 MHz band frequency. Both the frequency band of 402–470 MHz and the maximum rate of 153.6 Kbps are supported. The low-power TX/RX module consumes 16.2 mA during Tx, 19.9 mA during Tx, and 1.8 uA in the waiting mode. The module is attached to the switch and the imbedded board, respectively, transmitting and receiving data between the two devices. Figure 3 shows the picture of the RF module on which the CC1020 is mounted.

In this study, the CC1020 module was used because the frequently used Zigbee modules, such as the CC2420 and the CC2500, have problems with electromagnetic wave certification and data reliability. However, the CC1020 does not require an electromagnetic wave certification, and the data reliability is the highest in the 400 MHz band. Hence, the CC1020 module was employed in this study. The microprocessor of the communication module is ATMega16. ATMega16L mounts communication software by using CC1020's chip set, transmits communication packets through the serial communication with MCU, and supports the MAC function. ATMega16L controls CC1020 by using the SPI and DIO communication. The advantages of the CC1020 are the small size, low battery consumption, and the broad RF signal strength width. Figure 4 shows block diagram of the RF communication module.

2.3.2. RF Data Message Information. The data sheet of the RF module used in this study is shown below. Different from the serial communication using the conventional Zigbee, the data sheet allows for a convenient checkup of the results. Thus, the messages do not need to be integrated and presented as a new message. The resulting values can be derived on the basis of the command values and the data values of the command.

(A) Communication Method

(1) Communication PORT: composed of DCLK [Input] and DIO [OutPut] (General-purpose IO, Serial input and output data bus clock).

(2) DATA composition: one time preamble data composed of 8 bytes as shown in Figure 10:

(a) preamble: one time,

(b) CMD: COMMAND,

(c) DATA: SUB DATA for the COMMAND,

(d) serial number: to distinguish the equipment,

(e) CHECK SUM: (serial number ∧ layer ∧ DATA1 ∧ ID),

(f) transmitted by the imbedded board and responded by the switch. (retransmission is tried if there is no response within 200 ms),

(g) considers the maximum 30 lamp switches.

The transmission timing is synchronized among the RF modules by using the preamble signal. Thereby, the system information transmission is started at a predetermined timing. After receiving the preamble signal, the RF module transmits the CMD, serial number, Data 1, and Data 2 information. The maximum number of the provided lamp switches is 30.

(B) Command. The communication information between the imbedded board and the switch controller mounted on a lamp is summarized below. Table 1 shows communication information from the imbedded board to the switch. Table 2 shows communication information from the switch to the imbedded board.

ID Assignment. There are about 10 to 20 lamps in a household. Therefore, the maximum number of lamp switches provided

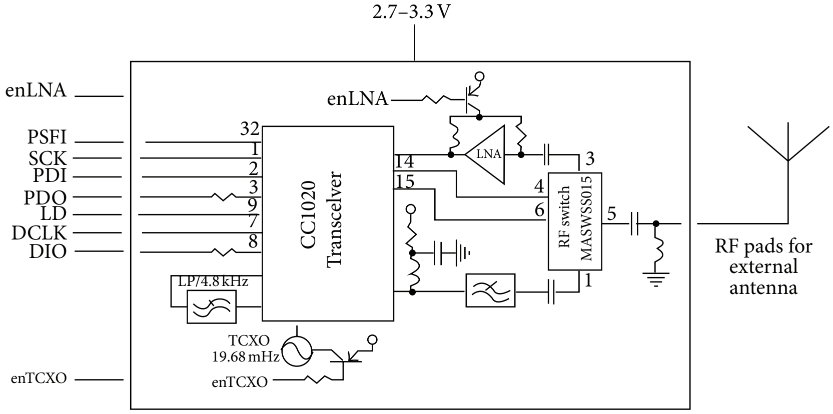


Figure 4: Block diagram of the RF communication module.

Table 1: Communication information from the imbedded board to the switch.

CMD	ID	DATA 1	DATA 2	Content
0x00				
0x01	ID	1 [on], 0 [off]		POWER
0x02	New ID	1 [on], 0 [off]		Serial + ID
0x03	ID	0: ALL 1: Switch 2: Time		Switch Setting
0x04	ID	1 [on], 0 [off]		Switch save
0x05	ID	T_HOUR	T_MIN	Time setting
0x06	ID	A_HOUR	A_MIN	Alarm setting

Table 2: Communication information from the switch to the imbedded board.

CMD	ID	DATA 1	DATA 2	Content
0x00				
0x01				POWER
0x02	New ID	1 [on], 0 [off]		Serial + ID
0x03				Switch setting
0x04	ID	1 [on], 0 [off]		Switch save
0x05	ID	T_HOUR	T_MIN	Time setting
0x06	ID	A_HOUR	A_MIN	Alarm Setting

Table 3: ID value assignment to lamp switches.

0	ALL
1~30	ID

in this study was set to 30. Table 3 shows IDs were assigned to the lamp switches.

2.4. Design of the Main Program. The main program was written using C# development language provided by MS (Microsoft). The C# language was used to realize the main program because the scenario of this study does not have a separate server. Thus, the imbedded board simultaneously plays the role of a client and a server. The original purpose is to manage, share, and save data by means of a server, but no separate server is needed because the purpose is to actuate the lamp switches. Therefore, the main program was designed using the C# programming language, which has excellent memory management and provides various functions in an internet environment. The platform of the imbedded board platform is based on WinCE 6.0. The RF sensor in the lamp switch controller is always turned on, waiting for the data request from the imbedded board. When a data request comes in, the RF sensor sends the current status information (CMD, serial number, and data information) to the imbedded board, which then receives the information and processes the received information so that it can be monitored on a screen. The information can be monitored with a smartphone; a smartphone is also able to turn the lamps on and off. (Figure 5 shows inner action of the main program.)

3. Implementation

3.1. Implementation of a Light Switch by the Use of RF Communication. It is a device to supply power to an electric light through radio frequency (RF). More specifically, it is an RF switch drive system to control the power of electric lights in and out of a house through RF. Before power supply, the system converts an alternating current into a direct current. The RF switch controller turns on/off an electric light through RF communication with the RF module built in an embedded board and receives power by the use of standby power. The current booster of the switch controller, which serves as a role to boot a microcurrent to a high current and rectify into a direct current, saves a microcurrent when a switch is off and communicates through RF by the use of the saved microcurrent or standby power when a switch is on. The current booster, a set of more than 20 trans, gathers and saves standby power. Figure 6 shows a diagram of the standby power RF light switch system [12].

3.2. Implementation of a Monitoring System. The main program installed into the embedded board (Mango 310) provides a communication environment to monitor the current

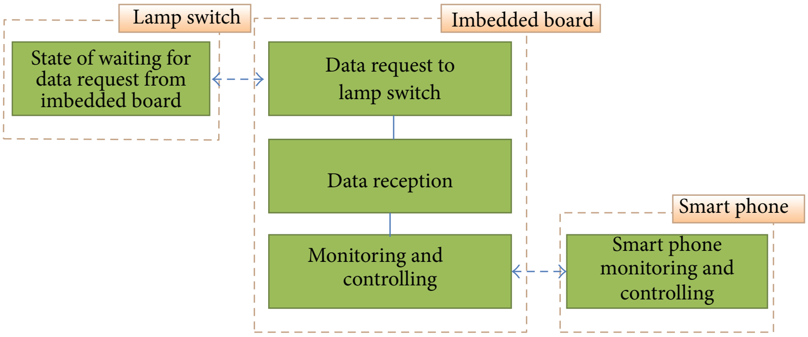

Lamp switch
Imbedded board
State of waiting for data request from imbedded board
Data request to lamp switch
Data reception
Smart phone
Monitoring and controlling
Smart phone monitoring and controlling

Figure 5: Inner action of the main program.

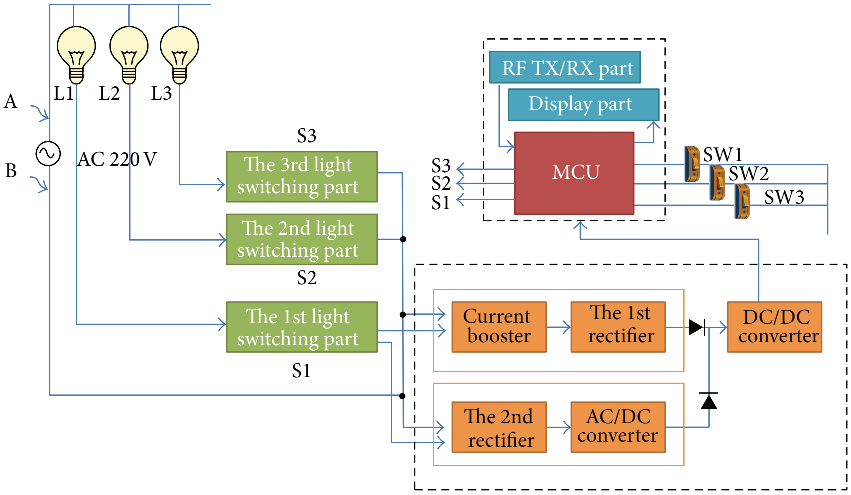
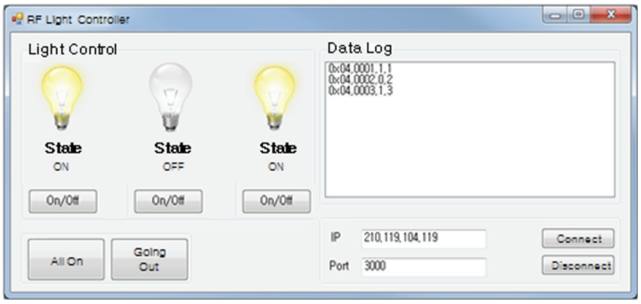


Figure 6: A diagram of the RF light switch system.

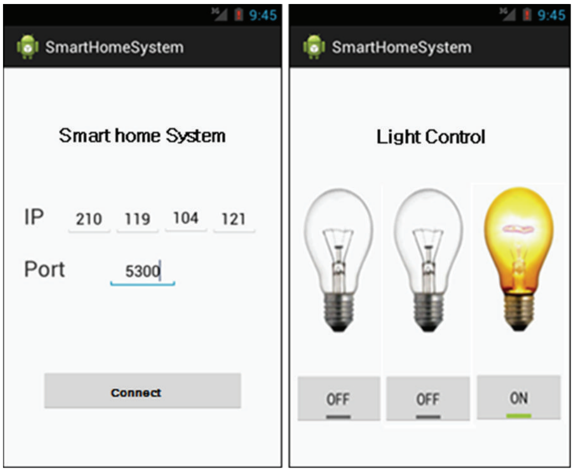


0x04,0001,1,1
0x04,0002,0,2
0x04,0003,1,3

IP 210,119,104,119

Port 3000

Figure 7: A window of the main program.



IP 210 119 104 121

Port 5300

Figure 8: Screens of the smart power control application.

light state and make access through a smartphone. Figure 7 shows illustrates a window of the main program. When a user enters an IP address and a port number and clicks Access button, the user can have access at any time through a smartphone. By looking at the data log, a user can check a current ID value, a command value, and the state of lights.

In addition, a user can check the state of lights in the type of images in real time and turn on/off lights by using the on/off option.

If an electric light is turned on, the main program shows the state of the light as a turn-on image and displays each value of CMD, ID, and DATA1 on the data log section. Also, on the option section of the main program, there are two buttons: All On and Going out. When All On button is clicked, all lights are turned on, and when Going out button is clicked, all lights are turned off. When a user enters an IP

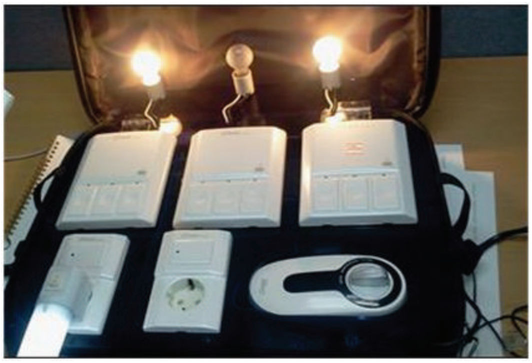
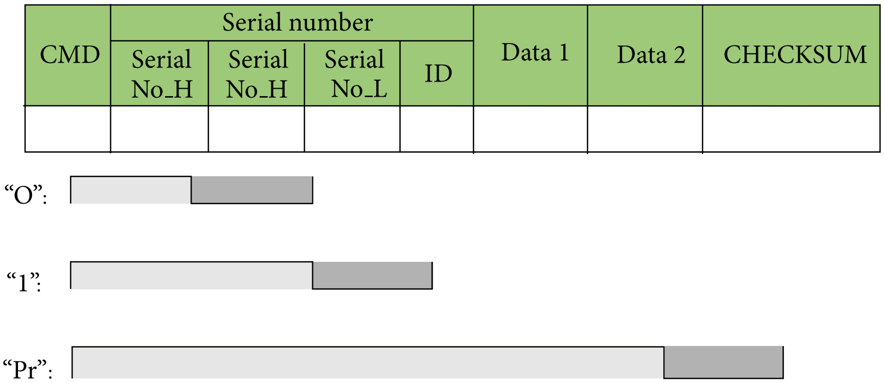


Figure 9: Smart power control system architecture.



CMD	Serial number				Data 1	Data 2	CHECKSUM
	Serial No_H	Serial No_H	Serial No_L	ID			

Figure 10

address and a port number necessary to make access from outside on the Set-up section and clicks Access button, the user can access the embedded board to control electric lights at any time through a smartphone.

3.3. Implementation of a Smartphone Application. The smartphone application is used for a user to control electric lights at any time and place through a smartphone.

When an embedded board opens a communication port and sets up an IP address, a user can have access to the embedded board through the IP address and communication port by using the application program. Figure 8 shows the main screen popping up first when the smart power control application runs.

When a user enters an IP address and a port number on the main screen and clicks Access button, the user can access an embedded board. As shown in the next screen, the state of electric lights in a house is displayed. On the screen, a user can turn on/off the lights.

4. Examination and Evaluation

To evaluate and analyze the smart power control system implemented in this work, this research made some preparation as shown in Figure 9 and began to evaluate the system.

The system was tested on the basis of the whole scenario. The control of electric lights was tested in each embedded board and smartphone environment. To make access through a smartphone, an IP address and a port number were assigned to an embedded board. After that, the given IP address and port number were entered in a smartphone for access. Turning on/off electric lights was tested in each embedded board and smartphone environment. And it was found that the embedded board and smartphone worked well. In the case of smartphone control, one problem was that it took different time to turn on/off electric lights depending on the wireless interest speed. It is a technical issue, so that it seems to be solved through the change of an IP address sharing router or through the change of the internet line. To investigate how much the RF controller of an electric light switch uses standby power with the naked eye, this research attached a watt meter to the controller and measured standby power. The electric lights did not consume electricity apparently. When an electric light was off, a microcurrent flowed in the light. The test of the system revealed that the microcurrent was supplied to RF devices. The supply of a microcurrent is the core technology of this work.

As seen earlier, electric lights were controlled through the use of an embedded board and a smartphone and therefore were successfully turned on/off. In addition, since the system supplied power to each RF device by using the standby power flowing in electric lights, any additional power consumption didn't occur. As a result, it was found that invisible standby power was remarkably used, and thus this work suggested that the system is able to control electric lights in a house at any time and place.

5. Conclusion and Future Research

This work developed the smart power control system to turn on/off electric lights through the use of RF communication, an embedded board, and a smartphone and showed the results of the system. In the past, a user controlled various home appliances including electric lights through wired communication rather than wireless communication. However, today, with the development of wireless communication, a user is able to control home appliances at any time and place.

By suggesting the service to control electric lights regardless of a user's location, this work provided an example of the service to monitor various kinds of indoor lights used in a home network, a factory, a commercial building, and others. Also, it proposed the service to induce users to save energy, which helps them to control electric lights.

Additionally, this work designed the system called current booster with multiple-trans to use invisible standby power. It used the current booster to operate an RF module for wireless communication.

Since the proposed functions work well, it would be possible to have an RF module built in home appliances in the future, and therefore a user could control the home appliances at any time and place through a smartphone or an embedded board by registering each ID value of home appliances.

The smart power control system developed and implemented is a prototype. Therefore, it is required to check whether the system would be applicable to actual home appliances. Also, it is needed to test safety when the system is applied to gas valves, door locks, and devices other than electric lights. In the future, this research plans to apply an RF module to home devices basically installed in a house, such as gas valves or door locks, and to control the devices. In addition, by adding more smart services, checking whether a user is at home through various sensors, accumulating information on the basis of a user's pattern, applying such information to an algorithm, this work will continue to be performed in order to improve users' quality of life.

Acknowledgment

This study was conducted as part of research for the 2013 Copyright Technology Development Project by the Ministry of Culture, Sports, and Tourism and Korea Commission.

References

[1] H. J. Chung, K. M. Jeon, and C. W. Park, "Analysis of smart home service scenario," *Korea Electronics Technology Institute*, vol. 2005, no. 11, pp. 1157–1160, 2005.

[2] J. K. Ng, "Ubiquitous healthcare: healthcare systems and applications enabled by mobile and wireless technologies," *The KITCS/FTRA Journal of Convergence*, vol. 3, no. 2, pp. 31–36, 2012.

[3] T. Teraoka, "Organization and exploration of heterogeneous personal data collected in daily life," *Human-Centric Computing and Information Sciences*, vol. 2, article 1, 2012.

[4] H. Ryu, "The value provided by Smart home appliances and Smart home".

[5] D. M. Konidala, D. Kim, C. Y. Yeun, and B. Lee, "Security framework for RFID-based applications in smart home environment," *Journal of Infor-Mation Processing Systems*, vol. 7, no. 1, pp. 111–120, 2011.

[6] T. Shon, H. H. Choi, and E. Kim, "Joint routing and scheduling in multi-cannel capillary machine-to-machine networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, article 126, 2013.

[7] D. H. Seo and I. Y. Lee, "A study on RFID system with secure service availability for ubiquitous computing," *Journal of Information Processing Systems*, vol. 1, no. 1, pp. 96–101, 2005.

[8] M. Yoon, Y.-K. Kim, and J.-W. Chang, "An energy-efficient routing protocol using message success rate in wireless sensor networks," *Journal of Convergence*, vol. 4, no. 1, pp. 16–22, 2013.

[9] S.-K. Lee, J.-W. Kim, and Y.-J. Yoon, "A study on world energy outlook and the optimal alternatives for energy technology development: focusing on coal utilization technology," *Journal of Energy Engineering*, vol. 15, no. 3, pp. 174–180, 2006.

[10] K.-M. Im and J.-H. Lim, "Design of standby power control system based on user's location for smart home," *Review of Korean Society for Internet Information*, vol. 12, no. 1, 2011.

[11] "KT Advanced Institute of Technology: smart home service of the connected home appliance era," Technology Insights, 2010.

[12] T. Lim, "Power supply apparatus for RF switch controller of lamp," 2010.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 161495, 8 pages
http://dx.doi.org/10.1155/2013/161495

Research Article

A Smart Service Model Based on Ubiquitous Sensor Networks Using Vertical Farm Ontology

Saraswathi Sivamani, Namjin Bae, and Yongyun Cho

Information and Communication Engineering, Sunchon National University, 413 Jungangno, Suncheon, Jeonnam 540-742, Republic of Korea

Correspondence should be addressed to Yongyun Cho; yycho@sunchon.ac.kr

Received 21 August 2013; Accepted 21 October 2013

Academic Editor: James J. Park

Application of the technology systems is growing in various fields and the agriculture is not an exception. Agriculture is also reaping the benefits of technological innovation which helps in quantitative and qualitative food production. Vertical farm, one of the agricultural practices, is considered to be the future of agriculture with the rate of population migrating into urban areas. Ubiquitous computing in agriculture is emerging remarkably in this fast processing pervasive environment, owing to wireless sensor network (WSN). Building a context aware system for the vertical farm is complex without the semantic interoperability between the Internet of things (IOT). In this paper, we propose a vertical farm ontology (VFO), an OWL based ontology model which helps in more understanding of the relationship between the domain factors. With the proposed model, the information from the Internet of things is recomposed as context information and made understandable for the other systems. For the sake of agriculture, we hope that our proposed model will pave great path for the development of smart and intelligent agricultural services.

1. Introduction

Recently, ubiquitous computing technology has been flourishing widely in agricultural field [1]. Some of the progresses in this area include automation process on the u-agriculture and smart services to control the activities. Such advancement in the ubiquitous computing encourages the agricultural researchers and even farmers to apply automation in the process.

Agriculture is a fundamental human activity and also inseparable from human life. As per the history, human started cultivating crop around 10,000 years ago, also referred as the Neolithic Age [2]. Starting from using simple tools such as stick and stones to advanced wireless computing technology, the development agricultural technology has major contribution [3]. Agriculture technique takes different form of advancement through centuries according to the lifestyle of the people. It is also estimated that 80% of the world population is expected to live in the urban areas by 2050. Also the rapid increase in population may be a threat to farmland [4]. For the future agriculture, existing indoor cultivation method is improved with the expert engineering and termed as vertical farming. Vertical farming is already in practice in many countries. Currently, vertical farms are rapidly evolving in the large-scale production of variety of crops in the urban centres [5].

Vertical farming is a fully automated system without any human intervention, which is also considered as the new agricultural evolution. To serve as ubiquitous computing infrastructure, it needs to be aware of the context and provide appropriate data and services. Considering the situation of the large-scale farming system like vertical farming in real time, the system is independent of each other. Context-aware service is being realized between the system by using the set of common ontology that supports the communication and the relationship.

In this paper, we propose an OWL based ontology model for the vertical farming environment. The suggested model concentrates more on the controlling and monitoring services of the environment. An upper-class ontology model is designed by identifying the important concepts in the vertical farm environment that focuses majorly on the services. The model is designed in a way that can be improvised further according to the needs and requirements without starting from scratch.

2. Background Study

This section represents the background work of the proposed ontology. First, we have discussed about the vertical farming which has both technological and expert engineering that makes a perfect combination for the ubiquitous computing environment. Next, OWL based ontology model is briefly discussed which is considered to be well suited for the development of semantic interoperability and finally the related works that helped in the development of context model.

2.1. Ubiquitous in Vertical Farming Overview. Vertical farming is considered as one of the modern agricultural technique in the future urban area, in where most of the people are expected to live [5]. Agricultural farming took different forms over the millennium since the invention of agriculture in stone ages to which it finally reached the vertical farming. And it may take different dimensions in the future, as the technologies are evolving nonstop. Computer technology during the last decade has numerous changes in the many fields. Looking back the evolution of the computer, in the early ages, the mainframe era was made a big evolution in which only expert accessed the computer. But today, the popular devices as laptops, tablets and Smartphone are owned and accessed by all ages. The third wave of computing (ubiquitous computing) is already upon us, leading to the departure of mainframe and personal computer [6].

As per the recent study [7], the paradigm shift is evidently occurring from personal to ubiquitous computing in which the evolution of the data-centric application encapsulates the data environment to ontology based application with automated reasoning capabilities [8]. Weiser [9] articulated the term “ubiquitous” which meant “everywhere” and defined many of its attributes. One of the goals of ubiquitous computing is to enable devices to sense changes in their environment and to automatically adapt and act based on these changes and preferences.

2.2. OWL. OWL is the ontology representation language which helps in the process of context information instead of presenting the information. Basic OWL ontology concept include classes representing domain concepts, properties of classes, and individual instances specified from classes. Ontology is referred to as the shared understanding of some domains, which is often conceived as a set of entities, relations, functions, axioms, and instances.

The reason for choosing OWL is to realize our context model and define our context model as follows. It is much expressive compared to other ontology languages. It has the capability of supporting semantic interoperability to exchange and share context knowledge between different systems. The context can be exchanged and understood between the systems in various domains.

2.3. Related Work. The gust of third wave computing has made a great evolution of computer in the past few years. Since the introduction of first context aware application “Active Badge Location System” by Want et al., [10] that used an infrared based system to determine a user’s current location that helped to forward phone call to the close user. Many such research focused on finding the user’s location and identifying the current situation [11–13]. Although many definitions were proposed for the term “context,” the most appropriate definition was given by Dey and Abowd [14].

Prekop and Burnett [15] proposed two dimensions of contexts such as external and internal context. The external context is the context that is measured by hardware sensors that is, location, temperature, or light. The internal context refers to the user’s goal, task, or work. In this modern world, the sensors have become a part of human life. To add value to the day today life, the sensors along wireless sensor network have made human life easier. The interest in wireless sensor network has increased considerably. Although the wireless sensor network was used in the military purpose, recently it is used in various fields such as health monitoring, transportation, smart home, habitat monitoring and agriculture [16].

Extensive usage of WSN has developed the interest in routing protocols. WSN is available everywhere, but it is impossible that there is a common routing protocol for all the application. Many survey has been undergone in the routing technique of wireless sensor network and classified according to Location-based, Data-centric based, Hierarchical based, Multipath based and QoS-based protocols [17]. With many kinds of routing protocol in practice, the recent researches [18, 19] have been focused on the major concern, which is the energy awareness.

The u-agriculture or intelligent agriculture is one of the applications of Internet of things (WSN). Zigbee standards in the wireless sensor network are recognised as the authoritative standards of agricultural environment [20]. Zigbee uses wireless mesh protocol for wireless control and monitoring, and is well known for long-lived battery and high reliability with a low cost and low power. Many studies have been undergone in the u-agriculture focusing mainly on the monitoring and automatic process controlling. Cho et al. [21] explain the service based system workflow model of agriculture with a situation context information. Hwang et al. [22] depict the monitoring service of the greenhouse through the wireless sensor network. Similarly, a real-time “field area” monitoring service in agricultural field was successfully created by Mizoguchi et al. [23]. In [24], Hwang and Yoe focuse one the importance of wireless sensor network in the context aware middleware of the greenhouse environment. Many real-time and prototypic implementations have been performed on ubiquitous agriculture [25–27].

Most of the researches in ubiquitous agriculture are service based automation. In the large-scale environment like vertical farming, the common understanding of the structure of information among the system is more important for a flawless automation. The context model which helps to fulfill such need is ontology which is termed as “formal, explicit specification of a shared conceptualisation” [28]. Ontology is a widely accepted tool for the modelling of context

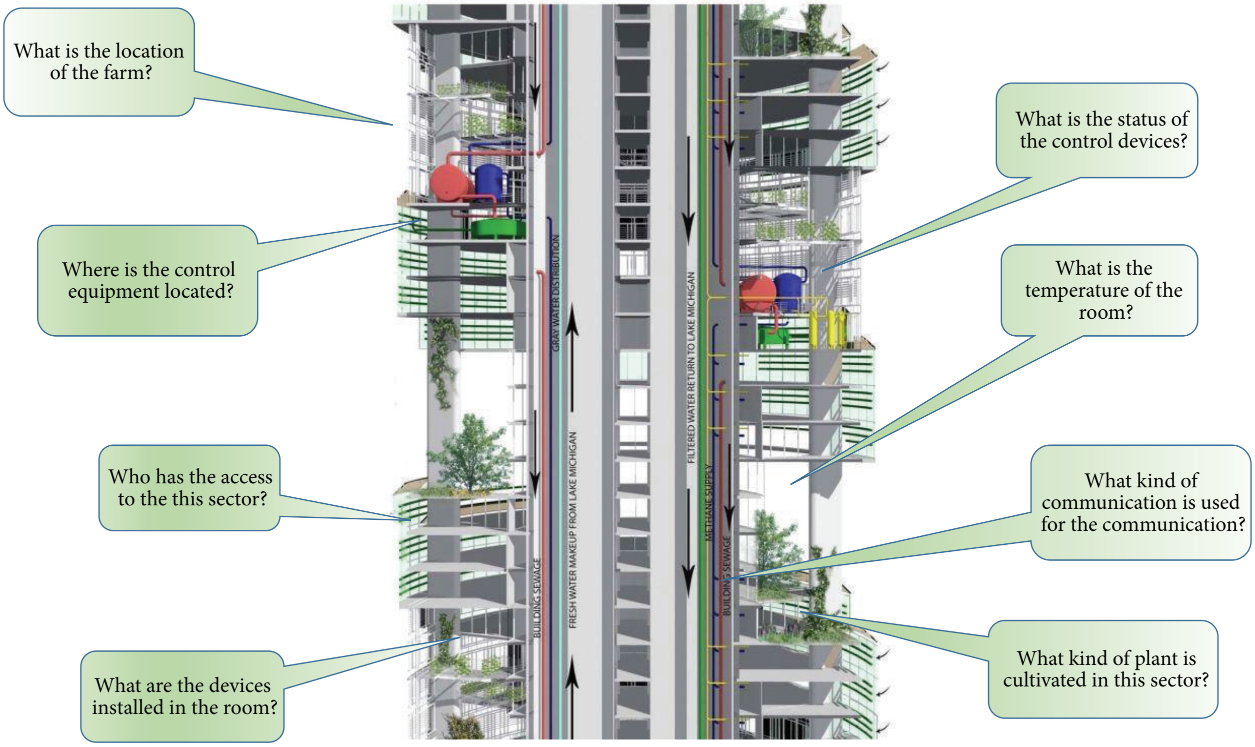

What is the location of the farm?
Where is the control equipment located?
Who has the access to the this sector?
What are the devices installed in the room?
What is the status of the control devices?
What is the temperature of the room?
What kind of communication is used for the communication?
What kind of plant is cultivated in this sector?
GRAY WATER DISTRIBUTION
FRESH WATER MAKEUP FROM LAKE MICHIGAN
BUILDING SEWAGE
FILTERED WATER RETURN TO LAKE MICHIGAN
METHANE SUPPLY
BUILDING SEWAGE

Figure 1: Vertical farm environment.

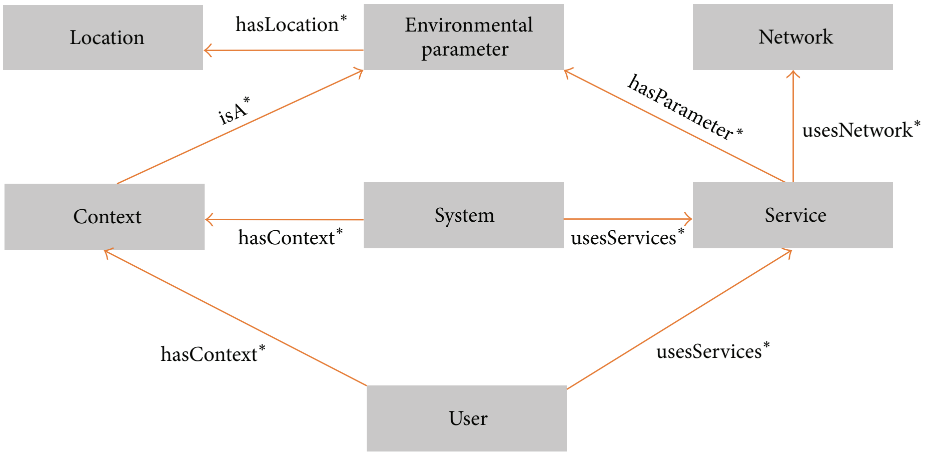


Figure 2: Upper-level model of VFO.

information in pervasive computing and also considered to be advantages over the other modelling techniques [29]. The OWL is part of the growing stack of W3C recommendation related to the semantic web. As semantic web is considered to be the future of web, OWL based ontology is widely used in the applications.

Many researches have been undergone in the vertical farm context modelling based on the OWL Ontology, in which Kim et al. [30] explains the situation categorization and its services relationship through OWL based on RDF. As it is in the beginning stage, many such research and development are expected.

3. Vertical Farm Ontology

Vertical farm ontology (VFO) is designed focusing on the service based vertical farm without any human intervention. The ontology model is designed using OWL based on RDF and implemented in Protégé 4.2.

In this fast evolving world of technologies, the model needs to be developed considering the future evolution. In our paper, we built a domain-specific model which is extensible. The first step handled in designing the model is by identifying the concepts of the environment. The concepts are physical or conceptual objects in the domain. For example, let

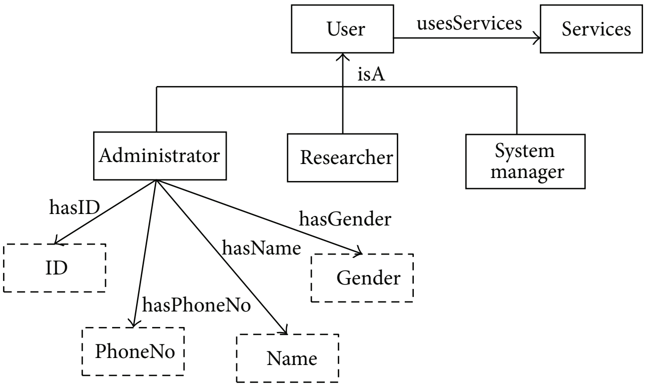


Figure 3: User concept.

us consider the vertical farm environment. As vertical farm is a large-scale production environment with optimal growth condition regardless of time and season. Although there are many designs available in vertical famring, we have used one of Bluke Kurasek design [31] for better understanding. As shown in Figure 1, we are left with many question.

By answering each question and analyzing the common dependency among the domain, the major classes are identified and structured as set of concepts. The concepts are context, devices, service, environment, network, location, and user. Figure 2 shows the upper ontology of the VFO which can be extended according to the domain of interest.

In the next subsections, each of the concepts is distinctly presented and explained.

3.1. Context Concept. Context is an often noted notion in the ubiquitous environment. Although context has various definitions, Dey and Abowd [14] definition was considered to be more accurate. Context awareness adds much to the dynamicity of the systems as their behavior varies depending on circumstances. Context aware systems are well known for their adaptability to the current context without any human intervention. The context information is mostly derived from sensors through a proper channel wireless sensor network. In VFO model, the context holds the set environmental parameter of a single location with a scheduled interval time. Also, an instance of the context class can be associated with a user in a time. The environmental parameter such as temperature, humidity, CO_2, and light as a context element, associated with appropriate control equipment, can range from specific sector, floor, or building. Thus, the location is interrelated with the context related concepts.

3.2. User Concept. Vertical farm environment is entirely automated environment with intelligent services such as monitoring and controlling services. The user concept makes use of such smart services. The context information obtained from time to time are monitored by the User. Although the control services are automatic, in case of emergency or necessity, the user can manually access the control services. Figure 3 depicts the user concept on VFO. In the vertical farm environment, the user can also be represented as person who has access to the services such as administrator, researcher, and system manager.

3.3. Environmental Parameter Concept. For a healthy crop growth, an optimal environmental condition is needed. The environmental condition information is very important to control the most appropriate devices. The parameters are useful to express the functionality of both devices and services. Internet of things acts as the bridge between the physical objects such as place, person, or device which is known as “things”. IOT consist of set of heterogeneous set of devices which are uniformly discoverable, closely integrated with the Internet infrastructure and service, regardless of the devices (RFID, sensor, or embedded devices). Presently, IOT is considered as the ideal emerging technology to influence the domain by providing new evolving data and the required computational resources for creating revolutionary apps [32]. In VFO, the autonomous services are achieved through the sensors and actuators. Sensors are directly related to the environmental parameter, from which the values are sent to the server via Wireless communication protocol (Zigbee). The actuators are indirectly linked to the parameter. Actuator controls the control equipment such as air conditioner, heater, window, humidifier, and light. The result in the variation of environmental parameter affects the actuator to maintain the optimal condition through controlling the equipment.

As we mention environmental parameter, it includes both the indoor and outdoor environmental conditions. Although the indoor factor plays major role, the outdoor factors are not to be omitted. According to the daily weather condition, the environment parameter needs to be manipulated and processed. Factors such as season, daily weather, and day-night atmospheric differences are also taken into account for the more appropriate growth condition. As for the indoor parameter, the atmospheric condition and the soil condition (can also referred as soil nutrient) are given major concern. Figure 4 represents the overview of the environmental parameter concept.

3.4. Service Concept. VFO model is designed focusing on the service based environment. The two main services that revolve around the vertical farm automation monitoring and controlling services. The controlling service helps the control equipment to be controlled through the actuator node. Figure 5 shows the service concept and its relation with the other concepts.

3.5. Network Concept. In this pervasive environment, the communication is most important factor that cannot be ignored. Not to mention, the WSN is overwhelming all over the world. The sensor uses the wireless communication protocol to deliver the parameter to the server. The wireless technology used in the vertical farm environment is Zigbee technique, which uses the frequency of 2.4 GHz. The programmable logic controller (PLC) which is the wired communication protocol helps in controlling the control equipment. Figure 6 depicts the network concept used in the VFO model.

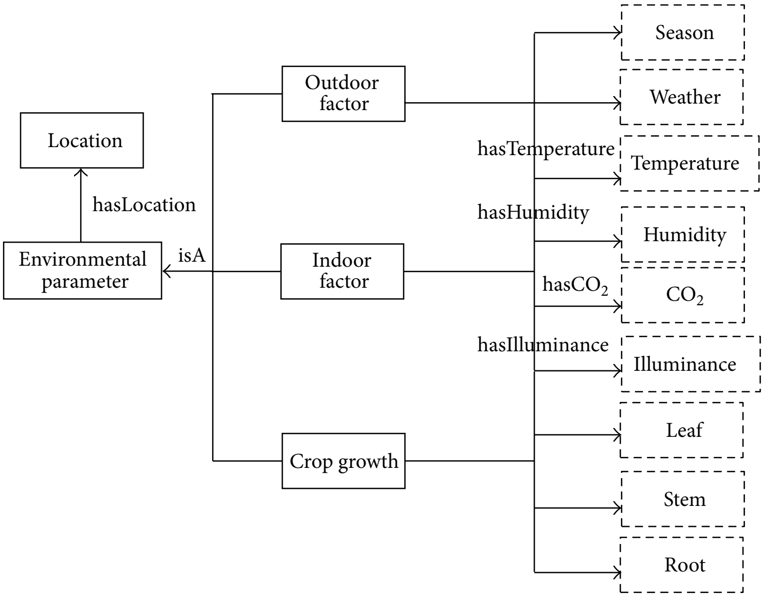


Figure 4: Environmental Parameter Concept.

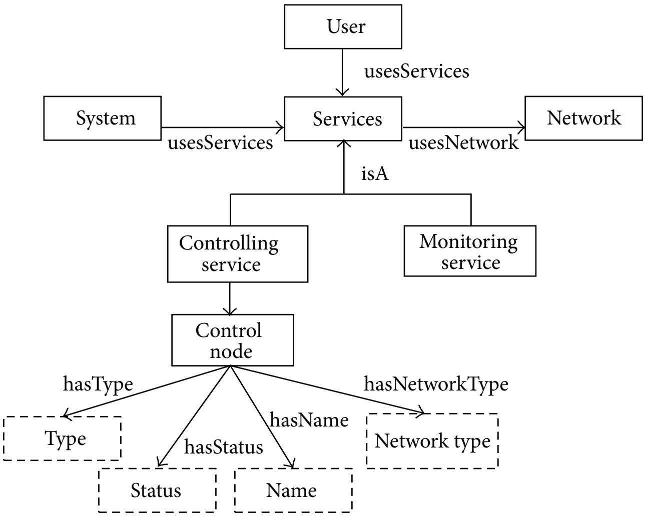


Figure 5: Service concept.

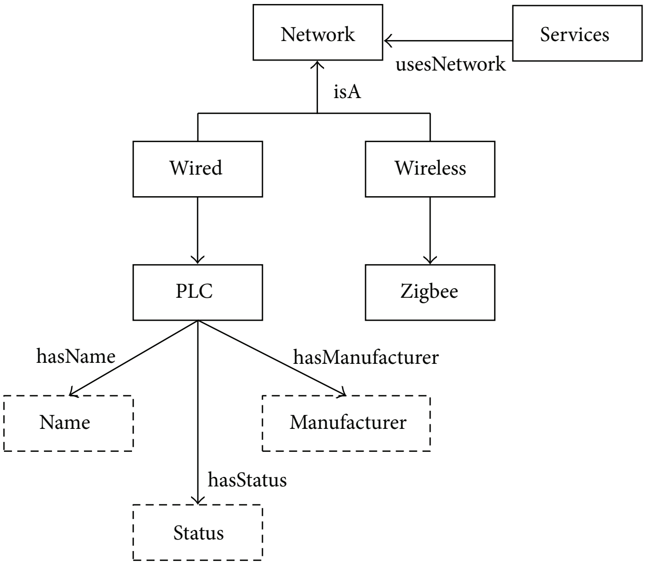


Figure 6: Network Concept.

3.6. Location Concept. The main concept of vertical farm is to produce maximum amount of crop production with optimal condition, even in the middle of the urban area. Hence the skyscrapers have much number of floors with variety of crops in it. As each crop is distinct, each needs a different environmental condition. Therefore, keeping a track of the crop and its location is much more important. The environmental parameter of the corresponding sector should be maintained properly so as to control the equipment of the above required sector. Figure 7 shows the overlook of location concept.

3.7. System Concept. The system concept is commonly divided into devices and control Equipment. The concept is classified on the basis of their services. The devices that are categorized in the VFO model are computer and the so called smart devices which are sensors and actuators. As discussed in the environmental parameter concept, the sensor returns certain parameters and actuator performs the control actions. The sensed data from the each sensor are transferred to the sink node through the wireless sensor network. The control equipment are air conditioner, humidifier, CO_2 generator, light, irrigator, and window. Figure 8 shows the underlying relationship of the system concept.

4. Experiment and Results

In this section, we present the implemented part of our VFO model. According to Hendrickson and Indulska, efficient use

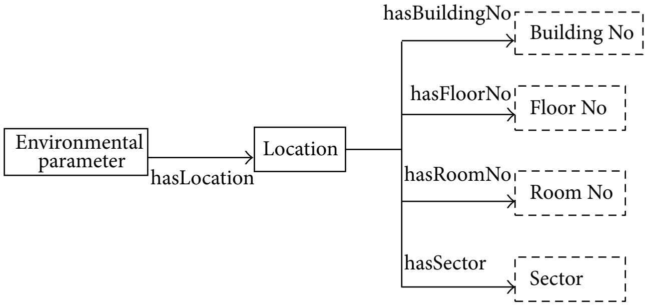


FIGURE 7: Location concept.

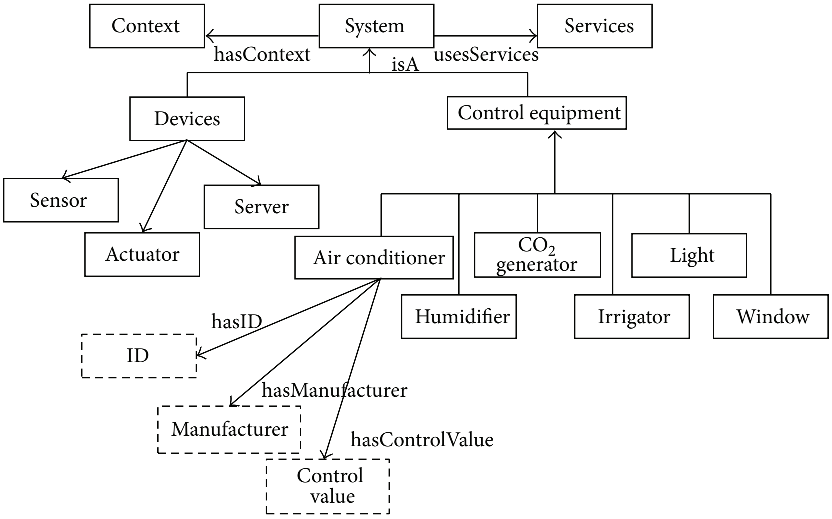


FIGURE 8: System Concept.

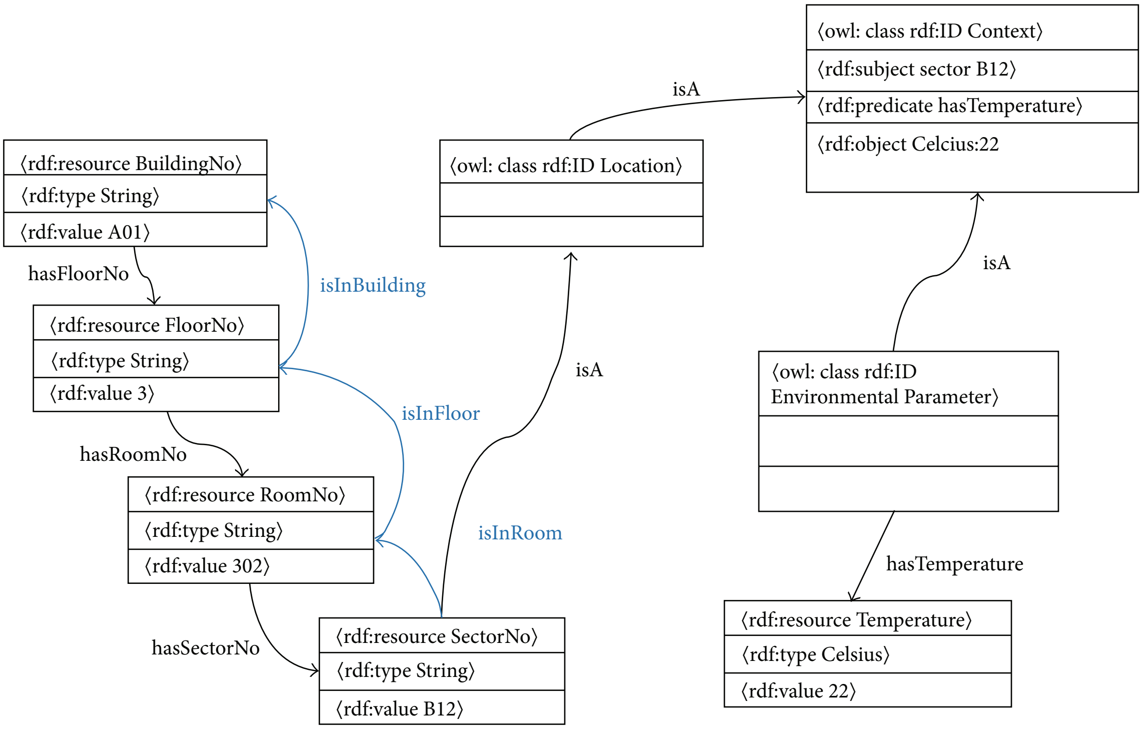
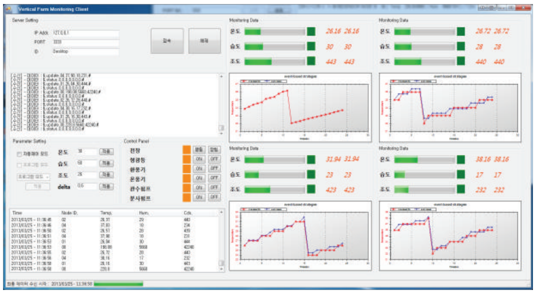
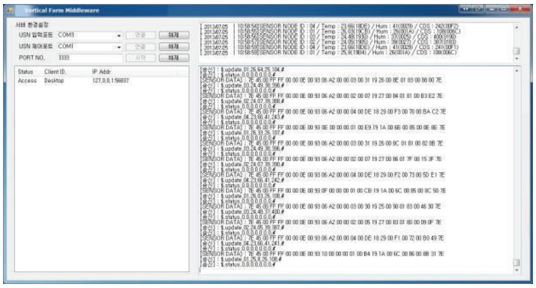


FIGURE 9: High level context information.



Time	Node ID.	Temp.	Hum.	Cds.
2013/03/25 - 11:36:45	02	26.37	29	440
2013/03/25 - 11:36:46	04	37.83	18	234
2013/03/25 - 11:36:50	02	26.57	28	439
2013/03/25 - 11:36:51	04	37.98	18	231
2013/03/25 - 11:36:53	01	26.94	30	444
2013/03/25 - 11:36:53	08	198.08	5668	42240
2013/03/25 - 11:36:55	02	26.72	28	440
2013/03/25 - 11:36:56	04	38.16	17	232
2013/03/25 - 11:36:58	01	28.16	30	443
2013/03/25 - 11:36:58	08	226.8	5668	42240

Figure 10: Vertical farm monitoring client.



```
[ 2013/07/05 | 10:58:54]SENSOR NODE ID : 04 / Temp : 23.66(18DE) / Hum : 41(0029) / CDS : 242(00F2)
[ 2013/07/05 | 10:58:55]SENSOR NODE ID : 01 / Temp : 26.03(19CB) / Hum : 26(001A) / CDS : 108(006C)
[ 2013/07/05 | 10:58:56]SENSOR NODE ID : 03 / Temp : 24.48(1930) / Hum : 37(0025) / CDS : 400(0190)
[ 2013/07/05 | 10:58:57]SENSOR NODE ID : 02 / Temp : 24.05(1905) / Hum : 39(0027) / CDS : 387(0183)
[ 2013/07/05 | 10:58:59]SENSOR NODE ID : 04 / Temp : 23.66(18DE) / Hum : 41(0029) / CDS : 241(00F1)
[ 2013/07/05 | 10:58:59]SENSOR NODE ID : 01 / Temp : 25.8(1984) / Hum : 26(001A) / CDS : 108(006C)
```

```
[송신] : $,update,01,26.64,25,104,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 06 A2 00 00 03 00 31 19 26 00 8E 01 83 00 88 00 7E
[송신] : $,update,03,24.49,38,396,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 06 A2 00 00 02 00 07 19 27 00 84 01 81 00 B3 E2 7E
[송신] : $,update,02,24.07,39,388,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 06 A2 00 00 04 00 DE 18 29 00 F3 00 70 00 BA C2 7E
[송신] : $,update,04,23.66,41,243,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 0E 00 00 00 01 00 E9 19 1A 00 6B 00 85 00 0E 8E 7E
[송신] : $,update,01,26.33,25,107,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 06 A2 00 00 03 00 31 19 26 00 8C 01 81 00 82 6B 7E
[송신] : $,update,03,24.49,38,396,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 06 A2 00 00 02 00 07 19 27 00 86 01 7F 00 15 3F 7E
[송신] : $,update,02,24.07,39,390,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 06 A2 00 00 04 00 DE 18 29 00 F2 00 73 00 5D E1 7E
[송신] : $,update,04,23.66,41,242,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 0F 00 00 00 01 00 CB 19 1A 00 6C 00 85 00 8C 50 7E
[송신] : $,update,01,26.03,26,108,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 06 A2 00 00 03 00 30 19 25 00 90 01 83 00 46 30 7E
[송신] : $,update,03,24.48,37,400,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 06 A2 00 00 02 00 05 19 27 00 83 01 80 00 09 0F 7E
[송신] : $,update,02,24.05,39,387,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 06 A2 00 00 04 00 DE 18 29 00 F1 00 72 00 B0 49 7E
[송신] : $,update,04,23.66,41,241,#
[송신] : $,status,0,0,0,0,0,0,0,#
[SENSOR DATA] : 7E 45 00 FF FF 00 00 0E 00 93 10 00 00 00 01 00 B4 19 1A 00 6C 00 86 00 8B 31 7E
[송신] : $,update,01,25.8,26,108,#
[송신] : $,status,0,0,0,0,0,0,0,#
```

Figure 11: Vertical farm middleware.

of context model needs careful planning; therefore, careful planning was done before the implementation. In our model, we have domain named class context where all the context information is gathered. In vertical farm environment, the set of environmental parameter and the location of the particular factor is considered to be more important. Figure 9 shows the high level context information and the relationship of the particular scenario. It indicates that the temperature in the sector B12 is 22 degree Celsius. As we know the OWL based ontology is interrelated. The location of the sector B12 is in Building no. A01, Floor no. 3, and Room no. 302. The relationships between the type of crop, location of the crop, and the temperature of the environment are all well defined to form an appropriate context.

Various devices such as sensor, actuator, and control equipment were installed in the vertical farming prototype to examine the monitoring and control services. Figure 10 shows GUI application of the monitoring service where the context information is gathered and displayed.

The sensed data are updated in the monitoring client on a regular time interval. Both the time-based and event-based readings are graphed for the comparison. The readings are taken from a single port ID, in other words, from a particular sector of the vertical farm. Each sector has different crop, which is mapped well to compare and monitor the crop's optimal growth environment.

A detailed middleware response of sensed data is presented in Figure 11. As the wireless sensor network has number of sensors, each node of sensor with a unique node value sends the sensed value to the sink, where the mapped devices are found.

The entire controlling service is performed automatically without any human intervention. The process is based on the following step.

(1) The sensed data from the sensor such as temperature sensor, humidity sensor or light sensor are sent to the sink (wireless sensor node) through the wireless communication protocol.

(2) The sensed values are stored in the server database.

(3) The values are then sent to the actuator through the wired communication protocol.

(4) PLC decides on the action after analyzing the values for the corresponding crop.

(5) The control action is performed on the corresponding control equipment to maintain the optimal condition in the environment.

5. Conclusion and Future Works

Recently, researchers are willing to make computing services smarter [33–35]. In this paper, we presented vertical farm ontology (VFO) for the future agriculture evolutionary environment. The suggested context model uses OWL based ontology to define common understanding and relationship between the system and services. The upper level ontology is analyzed and derived with the set of concepts such as location, user, system, context, environmental parameter, user, and Network. The basic concepts proposed can be reused and extended for the agricultural based smart environments.

With the gained experience from the prototype implementation, our VFO model and the concept will be more refined according to the domain-specific environment. By doing this, it may serve as a very helpful to develop agricultural service automation and smart service application in the agricultural environment.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported by the Ministry of Science, ICT and Future Planning (MSIP), Korea, under the Convergence Information Technology Research Center (CITRC) support program (NIPA-2013-H0401-13-2008) supervised by the National IT Industry Promotion Agency (NIPA).

References

[1] A. Rehman, "A review of wireless sensors and networks applications in agriculture," *Computer Standards & Interfaces*, 2011.

[2] Wikipedia, http://en.wikipedia.org/wiki/Neolithic_Revolution.

[3] A. Suprem, N. Mahalik, and K. Kim, "A review on application of technology systems, standards and interfaces for agriculture and food sector," *Computer Standards & Interfaces*, vol. 35, pp. 355–364, 2013.

[4] D. Despommier, “Vertical farming,” http://www.eoearth.org/view/article/156849.

[5] D. Despommier, “Farming up the city: the rise of urban vertical farms,” *Trends in Biotechnology*, vol. 31, no. 7, pp. 388–389, 2013.

[6] B. Rao and H. Zimmermann, “Preface to the focus theme selection ‘Pervasive Computing/ Ambient Intelligence’,” *Electronic Markets*, vol. 15, no. 1, p. 3.

[7] J. C. Augusto, V. Callaghan, A. Kameas, and I. Satoh, “Intelligent environments: a manifesto,” *Human-Centric Computing and Information Sciences*, vol. 3, p. 12, 2013.

[8] J. G. Pohl, “The evolution of intelligent computer software and the semantic web,” in *Proceedings of the 16th International Conference on System Research, Informatics and Cybernetics*, 2004.

[9] M. Weiser, *The Computer for the 21st Century*, Scientific American, 1991.

[10] R. Want, A. Hopper, V. Falcao, and J. Gibbons, “Active badge location system,” *ACM Transactions on Information Systems*, vol. 10, no. 1, pp. 91–102, 1992.

[11] G. D. Abowd, C. G. Atkeson, J. Hong, S. Long, R. Kooper, and M. Pinkerton, “Cyberguide: a mobile context-aware tour guide,” *Wireless Networks*, vol. 3, no. 5, pp. 421–433, 1997.

[12] Y. Sumi, T. Etani, S. Fels, N. Simonet, K. Kobayashi, and K. Mase, “C-map: building a context-aware mobile assistant for exhibition tours,” in *Community Computing and Support Systems, Social Interaction in Networked Communities*, pp. 137–154, Springer, London, UK, 1998, the book is based on the Kyoto Meeting on Social Interaction and Community aware, held in Kyoto, Japan, in June 1998.

[13] K. Cheverst, N. Davies, K. Mitchell, A. Friday, and C. Efstratiou, “Developing a context-aware electronic tourist guide: some issues and experiences,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 17–24, ACM Press, New York, NY, USA, April 2000.

[14] A. K. Dey and G. D. Abowd, “Towards a better understanding of context and context-awareness,” in *Proceedings of the Workshop on the What, Who, Where, When and How of Context-Awareness*, ACM Press, New York, NY, USA.

[15] P. Prekop and M. Burnett, “Activities, context and ubiquitous computing,” *Computer Communications*, vol. 26, no. 11, pp. 1168–1176, 2003.

[16] K. Maraiya, K. Kant, and N. Gupta, “Application based study on wireless sensor networks,” *International Journal of Computer Application*, vol. 21, no. 8, 2011.

[17] D. Goyal and M. R. Tripathy, “Routing protocols in wireless sensor networks: a survey,” in *Proceedings of the 2nd International Conference on Advanced Computing and Communication Technologies (ACCT ’12)*, pp. 474–480, January 2012.

[18] M. M. A. Azim, “MAP: a balances energy consumption routing protocol for wireless sensor networks,” *Journal of Information Processing Systems*, vol. 6, no. 3, pp. 295–306, 2010.

[19] M. Yoon, Y. K. Kim, and J. W. Chang, “An energy efficient routing protocol using message success rate in wireless sensor networks,” *Journal of Convergence*, vol. 4, no. 1, 2013.

[20] X. Zhu and Y. Lin, “Zigbee implementation in intelligent agriculture based on internet of things,” Proceedings of the 2nd International Conference on Electronic & Mechanical Engineering and Information Technology (EMEIT ’12), 2012.

[21] Y. Cho, S. Park, J. Lee, and J. Moon, “An OWL-based context model for U-agricultural environments,” *Lecture Notes in Computer Science*, vol. 6785, no. 4, pp. 452–461, 2011.

[22] J. Hwang, C. Shin, and H. Yoe, “Study on an agricultural environment monitoring server system using wireless sensor networks,” *Sensors*, vol. 10, no. 12, pp. 11189–11211, 2010.

[23] M. Mizoguchi, T. Ito, and S. Mitsuishi, “Ubiquitous monitoring of agricultural fields in Asia using wireless sensor network,” in *Proceedings of the 19th World Congress of Soil Science*, August 2010.

[24] J. Hwang and H. Yoe, “Study on the context-aware middleware for ubiquitous greenhouses using wireless sensor networks,” *Sensors*, vol. 11, no. 5, pp. 4539–4561, 2011.

[25] J. Lee, H. Lee, J. Hwang, Y. Cho, C. Shin, and H. Yoe, “Design and implementation of wireless sensor networks based paprika green house system,” *Communications in Computer and Information Science*, vol. 78, pp. 638–646, 2010.

[26] M. Baek, M. Lee, H. Kim et al., “A novel model for greenhouse control architecture,” *Grid and Pervasive Computing*, vol. 7861, pp. 262–269, 2013.

[27] Y. Cho, K. Cho, C. Shin, J. Park, and E. Lee, “An agricultural expert cloud for a smart farm,” *Future Information Technology, Application, and Service*, vol. 164, pp. 657–662, 2012.

[28] T. R. Gruber, “A translation approach to portable ontology specifications,” *Knowledge Acquisition*, vol. 5, no. 2, pp. 199–220, 1993.

[29] M. Baldauf, S. Dustdar, and F. Rosenberg, “A survey on context-aware systems,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 2, no. 4, pp. 263–277, 2007.

[30] T. Kim, N. Bae, M. Lee, C. Shin, J. Park, and Y. Cho, “A study of an agricultural ontology model for an intelligent service in a vertical farm,” *International Journal of Smart Homes*, vol. 7, no. 4, 2013.

[31] http://www.verticalfarm.com/FrontEnd/Common/FileStreamer.aspx?guid=2e801b29-2f25-44c5-98d9-4eb0f2b6e271&w=700.

[32] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internat of things (IoT): a vision, architectural elements and future directions,” *Future Generation Computer Science*, vol. 29, no. 7, pp. 1645–1660, 2013.

[33] N. Howard and E. Cambria, “Intention awareness: improving upon situation awareness in human-centric environments,” *Human-Centric Computing and Information Sciences*, vol. 3, no. 9, pp. 1–17, 2013.

[34] D. Gallego and G. Huecas, “An empirical case of a context-aware mobile recommender system in a banking environment,” *Journal of Convergence*, vol. 3, no. 4, pp. 49–56, 2012.

[35] E. Cho and S. Helal, “Expressive exceptions for safe pervasive spaces,” *Journal of Information Processing Systems*, vol. 4, no. 3, pp. 279–300, 2012.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 185327, 10 pages
http://dx.doi.org/10.1155/2013/185327

Research Article

A Novel Mechanism for Fire Detection in Subway Transportation Systems Based on Wireless Sensor Networks

Zhen-Jiang Zhang,[1] Jun-Song Fu,[1] Hua-Pei Chiang,[2] and Yueh-Min Huang[2]

[1] *Department of Electronic and Information Engineering, Key Laboratory of Communication and Information Systems, Beijing Municipal Commission of Education, Beijing Jiaotong University, Beijing 100044, China*
[2] *Department of Engineering Science, National Cheng Kung University, Tainan 701, Taiwan*

Correspondence should be addressed to Zhen-Jiang Zhang; zhjzhang1@bjtu.edu.cn

Received 16 September 2013; Accepted 27 October 2013

Academic Editor: Han-Chieh Chao

Fire is a common and disastrous phenomenon in subway transportation systems because of closed environment and large passenger flow. Traditional methods detect and forecast fire incidents by fusing the data collected by wireless sensor networks and compare the fusion result with a threshold. However, this approach has a significant shortcoming. Fusion of data decreases the amount of useful information since the distribution of data is not considered. In this paper, a novel mechanism based on wireless sensor networks is proposed and we can use the mechanism to detect fire in subway transportation systems. The core algorithm in this mechanism is an alternative of data fusion in wireless sensor networks. The mechanism uses the quantity information acquired from the data and also considers the distribution information of the data in order to predict the occurrence of fire incidents. The simulation results show that fire incidents can be detected fast and efficiently.

1. Introduction

Wireless sensor networks (WSNs) have extensively been used due to their excellent capability of monitoring real physical environments and collecting data [1]. For example, WSNs have been used in military, medical, and environmental monitoring applications, among others. Surely, the fields in which they are applied will continue to expand.

With the rapid process of urbanization, more and more people live and work in big cities. As a result, public transportation systems are under great pressure, and subway transportation systems are good choices to help relieve this pressure. However, fire is a common and disastrous phenomenon in subway transportation systems, and great attention must be paid to guarantee the safety of the public in such systems. Thus, the research on fire detection in subway transportation systems is very important.

In this paper, WSNs are used in subway transportation systems to monitor fire. The sensors deployed can collect data about temperature, and then we store the data in the database. Fire incidents can be predicted by comparing the distribution of the data collected and the normal distribution of the data on the condition when there is no fire. There are two rules that will be followed when comparing the distributions—the rule of the best consistency comparison and the rule of the best squared comparison. In this paper, these two rules are the core of the mechanism for fire detection. The best consistency comparison is a good method for fire locating, but it cannot provide any indication of the situation of the fire. Conversely, the best squared comparison cannot locate a fire, but it is a perfect method for estimating the severity of the situation, because this method has accumulated all the differences of these two functions rather than just the large differences. Therefore, the two methods have their own advantages and shortcomings and fire can be detected more accurately and efficiently by making use of the strengths of these two methods.

The mechanism proposed in this paper is an alternative of the mechanisms based on data fusion. Compared with other mechanisms, our mechanism can detect fire incidents all around and the result is more accurate. Fire incidents can be sensed, located, and monitored and the situation of the

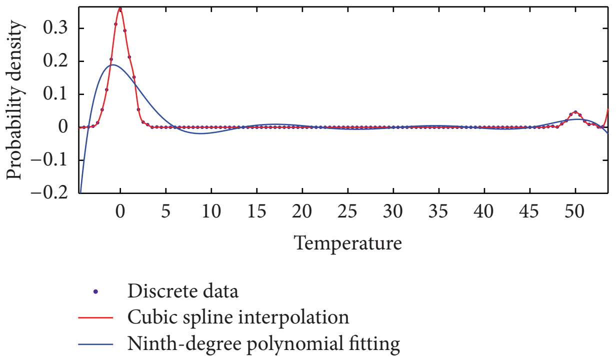


Figure 1: Cubic spline interpolation and a ninth-degree polynomial fitting.

fire incidents can be estimated. Therefore, the mechanism proposed in this paper is more valuable.

The rest of the paper is organized as follows. Section 2 introduces the related work of this paper, and Section 3 introduces the preliminary techniques. The fire detection system is discussed in detail in Section 4, and its performance is evaluated in Section 5. The conclusions are presented in Section 6.

2. Related Work

Studies on smart home [3–6] such as fire monitoring and detection have been researched for many years. Most monitoring and detection approaches make use of temperature and humidity sensors, smoke detectors, cameras and so on. In [7], a fire-detection system is proposed based on multisensory technology and neural networks. However, this method requires a large number of training samples due to the multivariate classification that applies to a neutral network. Moreover, it is assumed that possible events of fire detection have to be well studied for its priori information by the neural network. Hence, for an unseen event to be learned, the entire neural structure must be reformed. In [8, 9], the authors presented a system that was based on various types of sensors and that used probabilistic neural networks. However, such systems require the use of a training set, and most of them are evaluated in indoor environments, where the environmental conditions are absolutely controllable and, of course, completely different from the outdoor environment. A method for fire detection based on multisensory data fusion was presented in [10]. There are three types of sensors, that is, temperature sensors, humidity sensors, and cameras, and the authors combined the three types of data by D-S evidence theory (Dempster-Shafer evidence theory) to detect a fire [2, 11]. In [12], the authors proposed adaptive fusion algorithms, which are improvements over data fusion algorithms. Neubauer [13] applies genetic algorithms to an automatic fire detection system. The online identification of stochastic signal models for measured fire signals was presented. A system for monitoring fires using a WSN that collects temperature, humidity, and barometric pressure is described in [14].

Our approach is a novel mechanism for monitoring fires, and it is based mainly on statistical data and the process is different from the approaches used in previous methods. In order to illustrate the mechanism easily, we assume that there are only temperature sensors present. The occurrence of fire is judged by combining the distribution of the data collected and the normal distribution of the ordinary data when there is no fire. If the data show significant differences, it is very likely that there is a fire.

3. Preliminary Techniques

The proposed novel mechanism for fire detection mainly has three preliminary techniques

(1) Interpolation is an alternative method of data fitting, and, in some conditions, it is an easier and more accurate method especially for the complicated functions; for some extreme cases, the performance of data fitting cannot be accepted. Because of the reasons we proposed before, in this paper, cubic spline interpolation is used rather than Gaussian data fitting or some other data fitting techniques to get the continuous function of the discrete data collected by the sensors.

(2) The second preliminary technique is the best consistency comparison. It is a method that can identify the points at which the two distributions have obvious differences. The differences will be used to locate fire.

(3) The third preliminary technique is the best squared comparison, which can be used to obtain the whole difference between two distributions that can be compared. It can accumulate all of the differences rather than just the main differences. Therefore, it is a good way to estimate the situation of the fire.

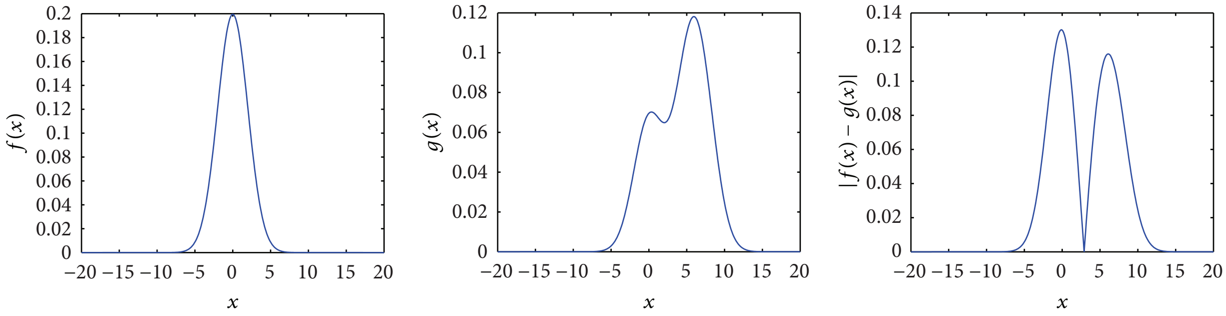
We will introduce the techniques in detail below.

3.1. Cubic Spline Interpolation. Interpolation is an alternative method of data fitting whose characteristic is the continuous function across all the discrete data points. Cubic spline interpolation is a classic method because of its gliding property. The performance of interpolation is better than the performance of fitting when the function is not a simple function, for example, when the discrete data have two peaks.

As shown in Figure 1, the continuous function obtained using the method of cubic spline interpolation crosses all the discrete points and is smooth. However, the continuous function obtained by polynomial fitting is not close to the actual data, even though the order of the polynomial is nine. Therefore, in this paper, cubic spline interpolation is used to process the discrete data.

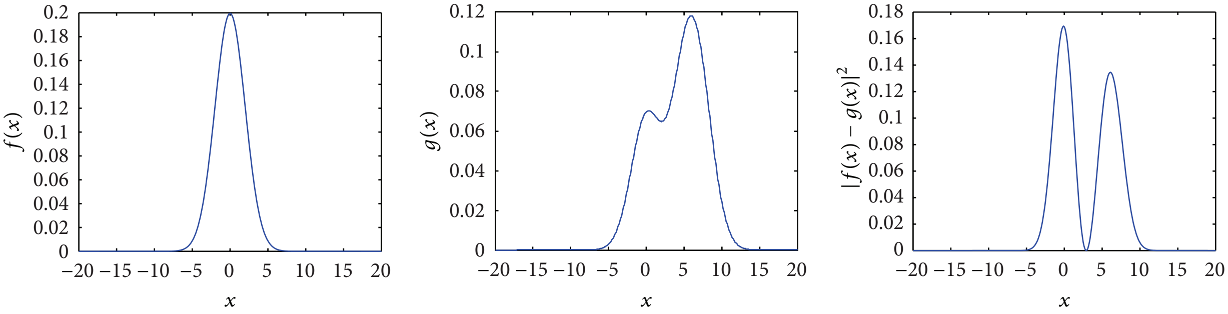
3.2. The Best Consistency Comparison. Assuming there are two continuous functions, for example, $f(x)$ and $g(x)$, with the domain of definition of $[a,b]$, we define the best consistency comparison as follows:

$$\Delta(f(x), g(x)) = |f(x) - g(x)|, \quad a \le x \le b. \tag{1}$$



(a) (b) (c)

Figure 2: (a) $f(x)$ (b) $g(x)$ (c) $\Delta(f(x), g(x))$.



(a) (b) (c)

Figure 3: (a)$f(x)$ (b)$g(x)$ (c) $|f(x) - g(x)|^2$.

The peaks of $\Delta(f, g)$ are recorded as (T_i, P_i), where T is short for temperature and P is short for probability. The differences between $f(x)$ and $g(x)$ can be determined through the records. Obviously, one piece of record is ignored if $P_i \le \mu$, where μ is a predefined set of thresholds, for example, $\mu = 0.005$. If $T_i \gg T_{\text{normal}}$ and $P_i \ge \alpha$, it is concluded that there is fire with temperature T_i; otherwise, there is no fire. α is a probability threshold for judging if there is fire and often α is set to be equal to 0.02. There is an example for the best consistency comparison shown in Figure 2.

As shown in Figure 2, the peaks of $\Delta(f(x), g(x))$ are recorded as (−0.2, 0.128) and (6.1, 0.116). We assume that the normal temperature is inferred around 0°C. Therefore, the peak (−0.2, 0.128) is normal and the peak (6.1, 0.116) attracts our attention. The sensors that detect a temperature around 6.1°C will be selected in the database and the sensor positions can be located by location system in WSNs.

The best consistency comparison is very sensitive to the big differences in a point and it is quite good for locating the fire. But the shortcoming is that this method cannot provide any information about the fire situation. To offset the shorting of the best consistency comparison, we propose another rule for comparison in Section 3.3.

3.3. The Best Squared Comparison. When there are two continuous functions, for example, $f(x)$ and $g(x)$, with the domain of definition of $[a, b]$, we define the best squared comparison γ as follows:

$$\gamma = 0.5 * \frac{\int_a^b |f(x) - g(x)|^2 dx}{\int_a^b f(x)^2 dx}, \qquad (2)$$

where γ is a number between 0 and 1. In fact, the maximum of $\int_a^b |f(x) - g(x)|^2 dx$ is equal to $2 * \int_a^b f(x)^2 dx$ on the condition that there is a large fire that influenced all of the deployed sensors, and the continuous bar graph and the normal distribution staggered completely; the minimum of $\int_a^b |f(x) - g(x)|^2 dx$ equals 0 on the condition that the situation is as usual, and $f(x)$ and $g(x)$ are almost all the same everywhere. Figure 3 is an example of the best squared comparison rather than being an example of the condition that $f(x)$ and $g(x)$ are almost all the same everywhere.

We can define the severity of a fire by γ:

$$\begin{array}{cc} \text{no fire,} & 0 \le \gamma \le 0.05 \\ \text{not that severe,} & 0.05 < \gamma \le 0.3 \\ \text{the fire is severe,} & 0.3 < \gamma \le 0.6 \\ \text{the fire is very severe,} & 0.6 < \gamma \le 0.8 \\ \text{a large fire,} & 0.8 < \gamma \le 1 \end{array} \qquad (3)$$

and it is obvious that there is a large fire if $\gamma \ge 0.8$.

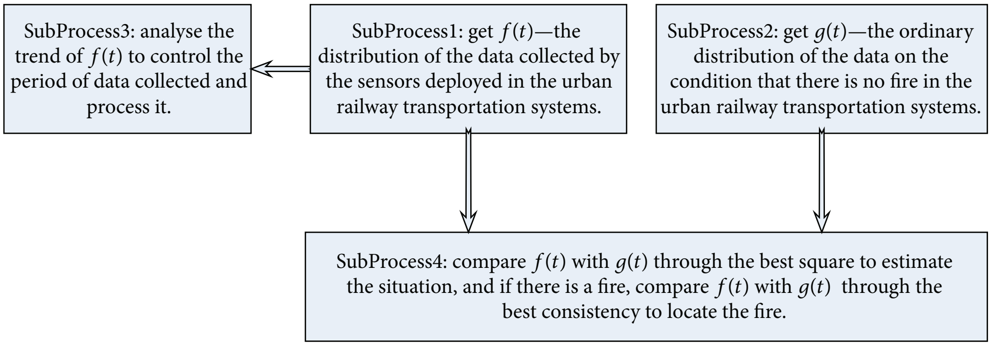

SubProcess3: analyse the trend of $f(t)$ to control the period of data collected and process it.
SubProcess1: get $f(t)$—the distribution of the data collected by the sensors deployed in the urban railway transportation systems.
SubProcess2: get $g(t)$—the ordinary distribution of the data on the condition that there is no fire in the urban railway transportation systems.
SubProcess4: compare $f(t)$ with $g(t)$ through the best square to estimate the situation, and if there is a fire, compare $f(t)$ with $g(t)$ through the best consistency to locate the fire.

Figure 4: Flow of the fire detection mechanism.

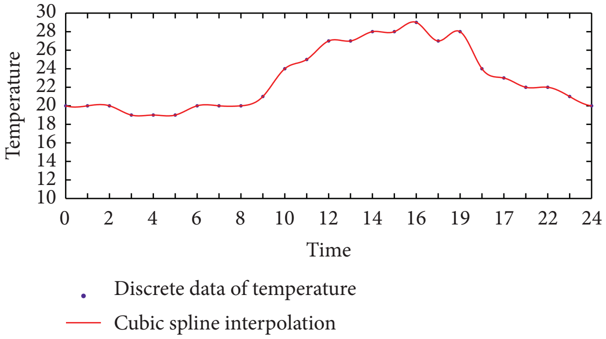


Figure 5: Continuous temperature for a day obtained by cubic spline interpolation.

The best squared comparison is a good measure for estimating the situation because this method accumulates all the differences between the two functions. On the contrary with the best consistency comparison, the shortcoming of the best squared comparison is that it cannot locate a fire, so these two comparisons will become complementary.

4. Fire Detection System

Applying the technologies introduced in Section 3, this paper proposes a new fire detection mechanism as shown in Figure 4 briefly to predict the fire perfectly. To be specific, the implementation details of each subprocess are expounded in Sections 4.1–4.5.

As shown in Figure 4, SubProcess4 is the core of our mechanism by which we can judge whether there is a fire. SubProcess1 and SubProcess2 are the basement of SubProcess4 through which we can get $f(t)$ and $g(t)$. The period we collect data in is important for real-time of our mechanism; the smaller the period is, the more real-time the data is. In the normal situation, we need not to collect the data very frequent, but if there are some indications of fire incident, we should collect the data more real-timely which means we should shorten the period. In SubProcess3, we described the method to control the period.

4.1. Predict the Normal Temperature in the Subway Transportation Systems. To predict the normal temperature in the subway transportation system, the association rules between the climate of the city and the normal temperature in the system are to be determined. A weather report provides the climate of city in a discrete way, for example, every 30 minutes or 60 minutes, and through the association rule, we can predict the normal temperature in the subway transportation system.

To our knowledge, the association rule between the climate and temperature in the subway transportation system can be mined by the technique of data mining, and then we can get the normal temperature, but it is not the core algorithm in this paper. Therefore, normal temperature in Beijing subway transportation system is given and is a set of discrete data at different times on a day as shown in Figure 5.

To get the temperature at any time, continuous function to represent the discrete data based on cubic spline interpolation is developed, and the result is presented in Figure 5. We can find that the continuous function crossed all the discrete points and it is very smooth and it satisfied our feeling better than data fitting.

This is the continuous function of temperature for a day obtained by cubic spline interpolation, and the actual temperature at any time of the day can be obtained using this function. Getting the accurate temperature is the basement of fire detection.

4.2. Reason the Normal Distribution $g(t)$ of the Data We Collected by WSNs. Because of the inherent features of sensors, accurate measurements of the temperature in the subway transportation system cannot be obtained. The observed value often follows a Gaussian distribution with a variance δ^2 of the real value, and has a relationship with the property of the sensors deployed. Obviously, δ^2 is an important parameter of the sensors, since smaller δ^2 means better quality and accuracy of the sensors.

In Section 4.1, we obtain the normal temperature T and the distribution of the temperature obtained from the sensors should be a Gaussian distribution with a mean of T and a variance of δ^2, namely, $N(T, \delta^2)$.

For example, the sensors deployed in the subway transportation systems with a variance $\delta^2 = 2$ and the temperature

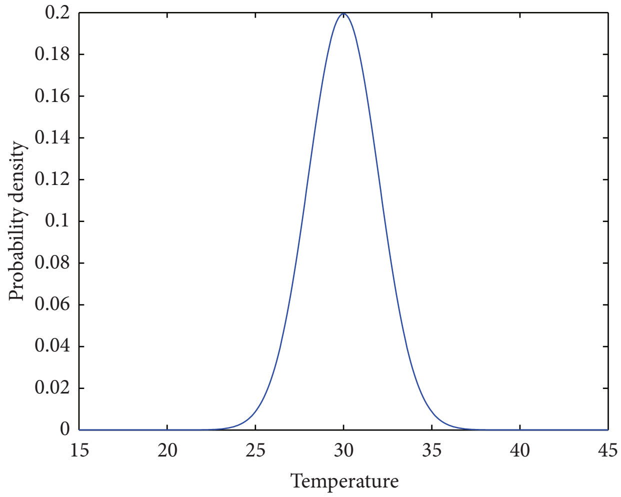


Figure 6: Normal distribution of temperature for 30°C.

is $T_0 = 30^\circ\mathrm{C}$. Then, the temperature provided by a sensor follows a Gaussian distribution, as shown in Figure 6.

Figure 6 shows that, although the temperature is 30°C accurately, because of the property of sensors, we cannot obtain the temperature accurately using the sensors; often, the measuring result follows a Gaussian distribution. Therefore, if the distribution of the data obtained from the sensors is very similar to the distribution shown in Figure 6, we believe that the actual temperature is 30°C.

4.3. Get the Distribution $f(t)$ of the Data Collected by WSNs. After collecting the temperature data from the sensors deployed in the subway transportation system, we process the data to get their approximate distribution function, as described below.

First, the smallest and the largest number of data is found, recorded as x_s and x_b, respectively.

Second, the range $[x_s, x_b]$ is divided into n segments. Usually, n is a number in 30–50. However, n can be set somewhat larger to get a more accurate result at the expense of increasing the amount of calculations required.

Third, for each segment, the number of the data that fall into this segment is added up, and a bar graph of data is obtained that comprises of discrete points.

Fourth, we use cubic spline interpolation to get a continuous function, which is an approximation of the discrete data. The pseudocode of this algorithm is described as in Algorithm 1.

Figure 7(a) is a bar graph of 2000 temperature readings generated by the 2000 sensors deployed, and Figure 7(b) is the continuous function obtained by cubic spline interpolation.

4.4. Control the Period T_p of Data Collected and Process by Analyzing $f(t)$. At the beginning of fire, the distribution of $f(t)$ tends to have two peaks because the temperature increases in the local area, and the discrete data of the temperature tends to be greater there. Therefore, if the function has two peaks that are not obvious, the period of data processing should be decreased to get more information about the fire.

To find the peaks, the algorithm proposed is described as follows.

First, the derivative of $f(t)$ is acquired and find zero points, that is, $t_0 \le t_1 \le \cdots \le t_n$ in order.

Second, get the normal temperature T through Section 4.1.

Third, if there is a zero point t_j that satisfies $f(t_j) \ge \beta_1$ and $t_j - T \ge \gamma_1$, T_p is decreased to $0.5T_p$; if $f(t_j) \ge \beta_2$ and $t_j - T \ge \gamma_2$, T_p is decreased to the limit value T_{limite} that is proposed. β_1, β_2 are the thresholds for probability and γ_1, γ_2 are the thresholds for temperature difference. Often we set $\beta_1 = 0.02$, $\gamma_1 = 10$ and $\beta_2 = 0.05$, $\gamma_2 = 10$.

In Figure 7(b), there are six zero points, that is, 23.4, 23.7, 29.8, 35.5, 36, and 36.7. However, there is no zero point that satisfies the conditions described in the third step; therefore, T_p remains the same. In Figure 10, there is a zero point that satisfies the condition $f(t_j) \ge 0.05$ and $t_j - T \ge 10$; T_p is decreased to observe the situation more carefully. In fact, there are some occasional cases in which data collected implies that there is fire and that would lead to erroneous T_p. However, it may have less impact as data will be collected more often, and the influence of occasional cases will be smaller.

Conversely, if the fire alarm is removed, T_p would be reset to normal value manually.

The pseudocode of this algorithm is described in Algorithm 2.

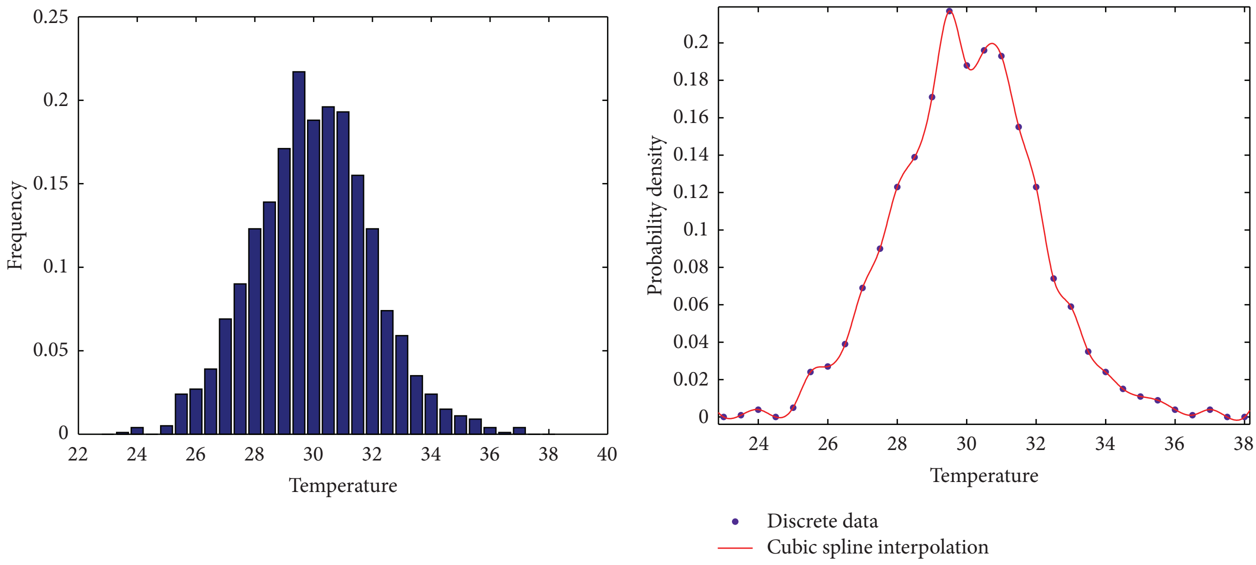
4.5. Compare $f(t)$ and $g(t)$ to Find Whether There Is Fire. We have got $f(t)$, $g(t)$ and we will compare them through the two comparisons to predict whether there is a fire. If there is no fire in the subway transportation system,$f(t)$ and $g(t)$ are almost all the same; if there is a local fire, $f(t)$ will be a little different from $g(t)$, for example, $f(t)$ has two peaks and $g(t)$ has one peak and in this situation, the best consistency comparision is a good method; if the fire is occurring almost everywhere of the system, $f(t)$ will be very different from $g(t)$ and in this situation, we cannot only focus our attention on the places where the fire is the most severe but also on the overall conditions.

The flow to judge whether there is a fire is shown in Figure 8.

Just as we described in the Introduction, the best consistency comparison and the best squared comparison have their own advantages and disadvantage. So, we will use both of them to get an all-sided result and for different results we should take different methods to process the fire appropriately.

5. Performance Evaluation

To examine the mechanism for fire detection in subway transportation systems, we set two different situations of fire incidents and they can check the mechanism in different aspects. The local fire incident is used mainly to examine



(a)

(b)

Figure 7: (a) Discrete bar graph of the data (b) Continuous function of the discrete data (°C).

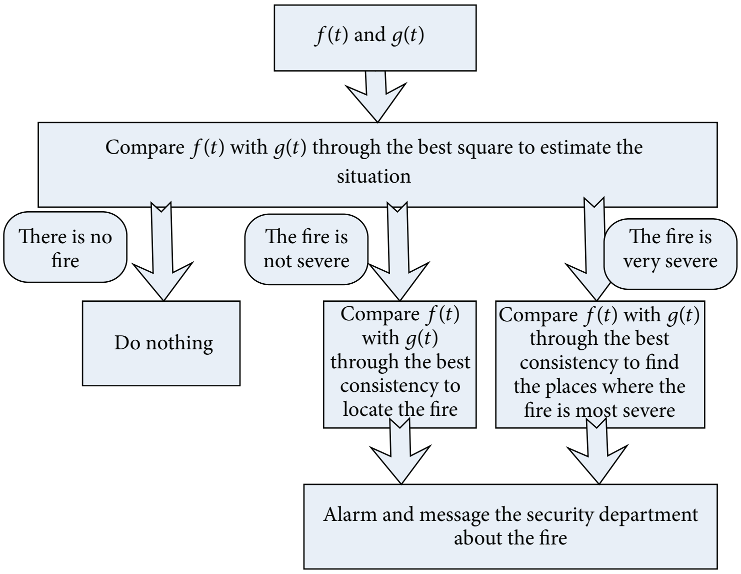

$f(t)$ and $g(t)$
Compare $f(t)$ with $g(t)$ through the best square to estimate the situation
There is no fire
The fire is not severe
The fire is very severe
Do nothing
Compare $f(t)$ with $g(t)$ through the best consistency to locate the fire
Compare $f(t)$ with $g(t)$ through the best consistency to find the places where the fire is most severe
Alarm and message the security department about the fire

Figure 8: Flow of the fire judgement.

the best consistency comparison and the large fire incident is used mainly to check the best squared comparison. For different fire, our experimental parameters are set as in Table 1.

Through our mechanism, the fire incidents will be predicted. If there are local fires in various places, we will locate them quickly and inform the security officers; if there is a large fire that is almost everywhere in the system, we will locate the places where the fire is very severe, and then we will inform the security officers.

5.1. Hypotheses of Simulation. To simplify the simulation, there are some hypotheses.

(1) Difference of properties in sensor measurement between the sensors is not considered. We assume that all the sensors have the same properties, such as the same measuring range and the same measuring error. In this paper, we assume that each sensor used can measure temperature up to 1000°C and the errors in the measurements are presented in the distribution of the data measured by the sensors.

(2) The temperature around a fire is all the same. In fact, the temperature decreases with the increase of the distance between the fire and the sensors. In this case, it is very difficult to simulate. Therefore, in this paper, we ignore the influence of this phenomenon.

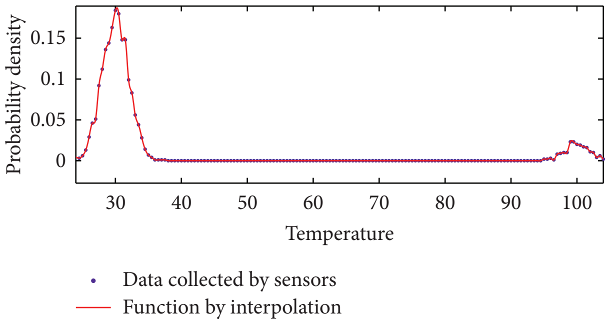


Figure 9: Continuous function of the discrete data obtained by cubic spline interpolation.

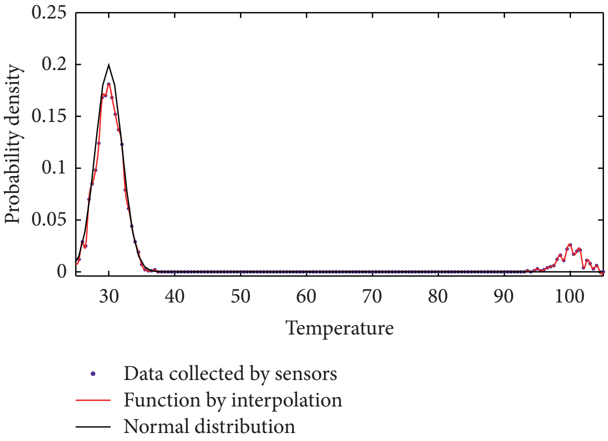


Figure 10: Normal distribution and the continuous bar graph.

Table 1: Experimental parameters.

Name of the parameters	Value of the parameters
Number of sensors	2000
Normal temperature	30°C
σ^2 of the sensors	2
Temperature of the environment around a fire	100°C (for local fire) 200°C (for large fire)
Number of the sensors that detect a fire	200 (for local fire) 1500 (for large fire)
Initial value of T_p	20 minutes
Smallest value of T_p	5 minutes
Interval of the bar graph	0.5°C
Threshold α	0.02
Threshold γ	as defined in (3)

(3) The temperature of the subway transportation system is all the same. This hypothesis is reasonable because for a subway transportation system, the environment of a subway is almost all the same. If the subway transportation system is too big that the temperature is different between different parts, we can divide the subway transportation system into several parts and it is feasible that the environment of each part is almost all the same. We can use our mechanism in each part.

(4) To guarantee a good result, we assume that the number of sensors is large enough and the sensors are deployed uniformly in the subway transportation system. In our experiment, we assume that for a local fire, there are 200 sensors that can defect the fire, and for a large fire, there are about 1500 sensors that can defect the fire.

Based on the three hypotheses, our experiment results are presented as follows.

5.2. Detect Local Fires. In this part, local fire at about 100°C is simulated and the system consists of 200 sensors for temperature measurement.

The simulation results are shown in Figure 9.

As shown in Table 1, 2000 temperature measurements are obtained, and the interval is 0.5°C. Figure 9 shows that there are two peaks: one peak is at 30°C and the other peak at 100°C indicates a local fire.

A continuous function of the discrete bar graph is obtained by cubic spline interpolation, and this function could be easily compared with the normal distribution.

Figure 10 shows the normal distribution and the continuous function obtained by cubic spline interpolation. It is evident that there are mainly two large differences between them. The first difference occurs at 30°C, and the second occurs at a temperature of 100°C. However, they are not equally important, because the first difference means that some sensors may have moved to a higher temperature, and our more important concern is the new location of the sensors. The second peak shows that the temperature of some places in the subway transportation systems has increased to 100°C. Because $(T = 100) \gg (T_{\text{normal}} = 30)$ and $P \geq \alpha$, it is reasonable to conclude that there is a fire. Figure 11 shows the consistency difference and the square difference between the normal distribution and the continuous bar graph.

After determining the unusual points through the best consistency comparison and locating the fire, the situation can be estimated using the best squared comparison. By (2), we get $\gamma = 0.11$, and by (3), we can conclude that the fire is not very severe and it is most likely a local fire.

5.3. Detect Large Fires. In this part, a large fire is simulated with a temperature of 200°C, and the fire is measured using 1500 sensors.

It is evident that there are two peaks of the data collected by the sensors in the subway transportation system. The first peak is at 30°C and the second one is at about 200°C. Obviously, it is unusual for the second peak which is much higher than the first peak, and this indicates that the fire is large.

In order to compare the distribution of the discrete data with the normal distribution through our two comparison rules, the discrete data are interpolated by cubic spline interpolation, and the results are shown in Figure 12.

Figure 13 shows that there are two big differences between them: one is at 30°C and the other is at 200°C. Figure 14 shows

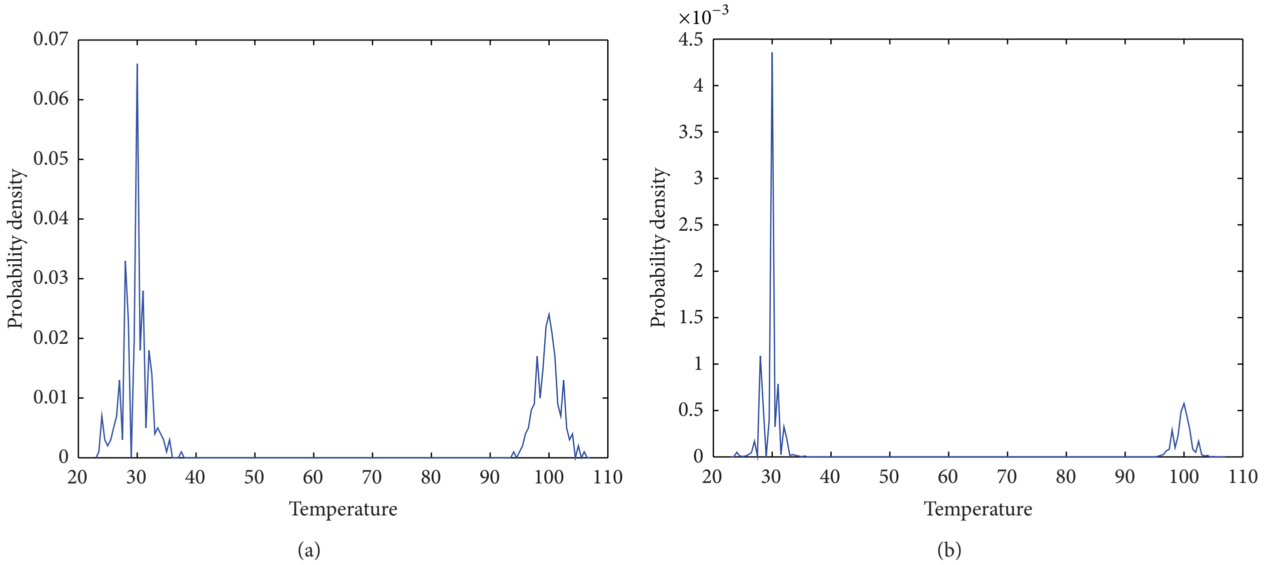


FIGURE 11: (a) Consistency difference between the normal distribution and the continuous bar graph. (b) Square difference between the normal distribution and the continuous bar graph.

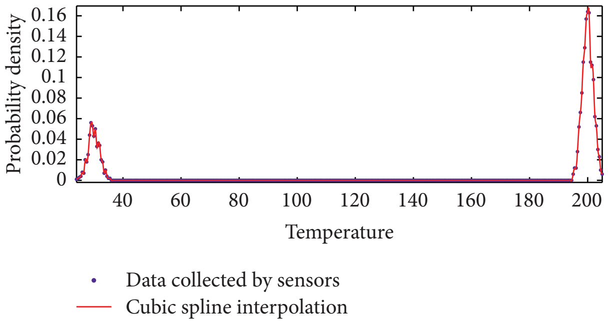


FIGURE 12: Continuous function of the discrete data obtained by cubic spline interpolation.

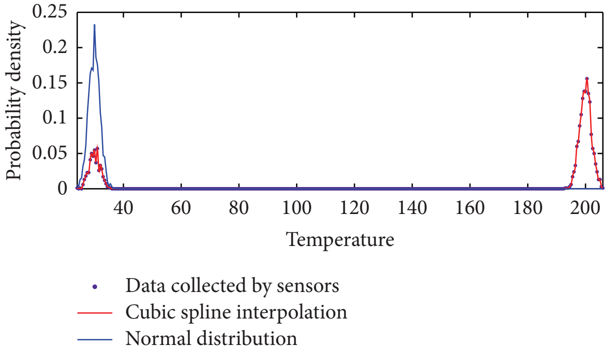


FIGURE 13: Normal distribution and the continuous bar graph.

the consistency difference and the square difference between the normal distribution and the continuous bar graph.

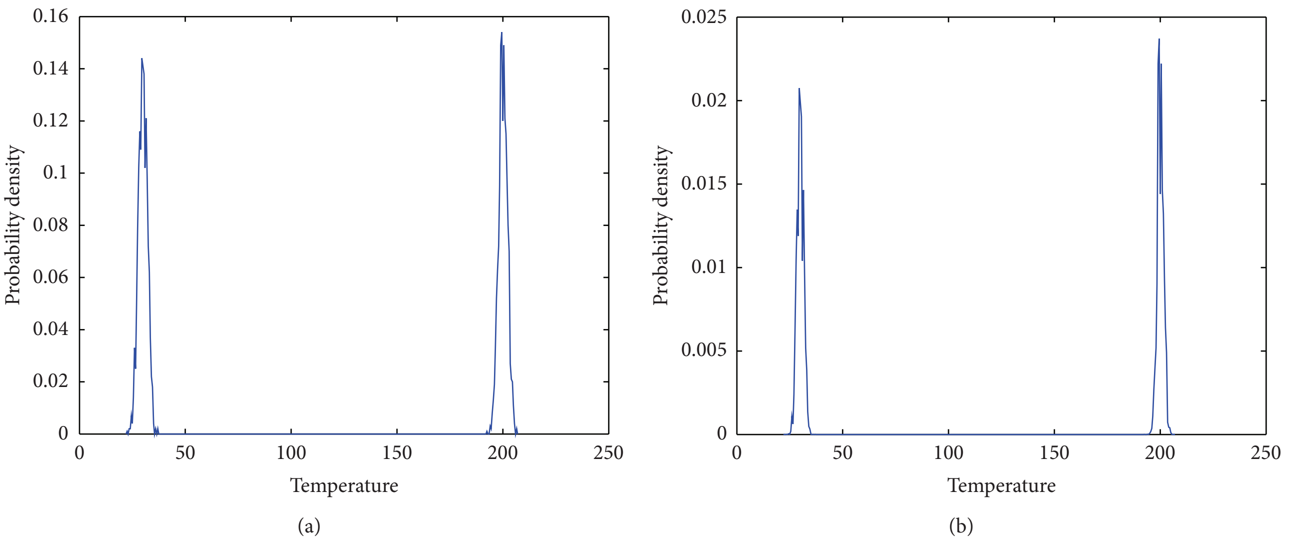
Because $(T = 200) \gg (T_{\text{normal}} = 30)$ and $P \geq \alpha$, as described in Section 3.2, it is reasonable to conclude that there is a fire. After finding the unusual points through the best consistency comparison and locating the fire, the best squared comparison is used to estimate the situation. By (2), we get $\gamma = 0.82$; and by (3), we can conclude that the fire is very severe and it is most likely a large fire.

6. Conclusion and Future Work

In this paper, we have proposed a novel mechanism based on WSNs for fire detection in subway transportation systems. For different types of fire incidents, it is obvious that we focus our attention on different aspects of them. For a local fire, it is important to locate the places where the fire happens quickly and efficiently because it is the best result to put out the fire when it is small, and for a large fire incident, it is important to estimate the situation as accurate as possible because it is impossible to extinguish a big fire immediately. For different order of severity we should take different measures. Through the two comparisons we proposed in our paper, we can get a satisfied result. The simulation shows that the performance of the mechanism described in this paper is satisfactory, and we can detect almost all the situations associated with a fire efficiently and quickly.

As our future work, to improve the reliability and safety of the mechanism, we will introduce some other important measures for a fire, such as the humidity of the environment and the concentration of smoke in the subway transportation system. In this way, there will be several results for the prediction of fire. However, it is not competent for our mechanism to fuse these several results. Therefore, we will use the technique of fuzzy set theory or D-S evidence theory to fuse the results on decision level.

On the other hand, we will design a better simulation which is closer to the actual situation. In this paper, we have several hypotheses to simplify our simulation which may have some influence on the simulation results.



(a)

(b)

FIGURE 14: (a) Consistency difference between the normal distribution and the continuous bar graph. (b) Square difference between the normal distribution and the continuous bar graph.

```
Input: the data set $D := \{x_1, x_2, \ldots, x_m\}$ collected by the sensors deployed in subway system
Output: the distribution $f(t)$ of the data set
Sort the data in $D$ and get new sequence $x_{11} \le x_{21}, \ldots, \le x_{m1}$
$T_p = (x_{m1} - x_{11})/n$
$\text{num}_i = 0,\ (i = 1, 2, \ldots, n)$
for each $x_i \in D$
    if $(x_{11} + T_p * j \le x_i \le x_{11} + T_p * (j + 1))$
        $\text{num}_i + +$;
    end if
end for
Get the two dimension data set DS:= $\{(x_{11} + (T_p/2), \text{num}_1),\ (x_{11} + ((3 * T_p)/2), \text{num}_2), \ldots,$
    $(x_{11} + (((2 * i - 1) * T_p)/2), \text{num}_i), \ldots,\ (x_{11} + (((2 * m - 1) * T_p)/2), \text{num}_m)\}$;
Interpolate the discrete data set DS by cubic spline interpolation as shown in [2].
Return $f(t)$ // the approximate continuous distribution of the data by cubic spline interpolation.
```

ALGORITHM 1: getDistribution (D).

```
Input: $f\ (t)$ is the distribution,$T$ is the normal temperature, $\beta_1$ and $\beta_2$ are probability
        thresholds, $\gamma_1$ and $\gamma_2$ are the temperature thresholds, $T_{\text{limite}}$ is the limit value of $T_p$
Output: the new period $T_p$
Take the derivation of $f\ (t)$ and get $f'(t)$.
Find the zero points of $f'(t)$ who is also the extreme values of $f\ (t)$ and record
them in the data set $E := \{t_1, t_2, \ldots, t_k\}$
for each $t_i \in E$
    if $(f\ (t_i) \ge \beta_2\ \&\&\ t_i - T \ge \gamma_2)\{$
        $T_p = T_{\text{limite}}$
          break;}
     else if $(f\ (t_i) \ge \beta_1\ \&\&\ t_i - T \ge \gamma_1)\{$
        $T_p = T_p/2$;
          break;}
     end if;
end for
return $T_p$
```

ALGORITHM 2: ControlPeriod ($f(t), T, \beta_1, \gamma_1, \beta_2, \gamma_2, T_{\text{limite}}$).

Acknowledgments

This research is supported by Beijing Science and Technology Program under Grant Z121100007612003, Beijing Natural Science Foundation under Grant 4132057, and National Natural Science Foundation under Grant 61371071.

References

[1] Y. Kim and H. Chang, "An exploratory study for designing business services based on sensor networks," *Journal of Internet Technology*, vol. 14, no. 3, pp. 477–484, 2013.

[2] K. L. Su, "Automatic fire detection system using adaptive fusion algorithm for fire fighting robot," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, pp. 966–971, Taipei City, Taiwan, October 2006.

[3] C.-F. Lai, H.-C. Huang, Y.-M. Huang, and H.-C. Chao, "Design and implementation of the DLNA family intercom system for smart homes," *Computer Journal*, vol. 52, no. 8, pp. 960–968, 2009.

[4] C.-F. Lai, Y.-M. Huang, J. H. Park, and H.-C. Chao, "Adaptive body posture analysis for elderly-falling detection with multisensors," *IEEE Intelligent Systems*, vol. 25, no. 2, pp. 20–30, 2010.

[5] C.-F. Lai, Y.-M. Huang, and H.-C. Chao, "A context-aware multi-model remote controller for electronic home devices," *Journal of Supercomputing*, vol. 54, no. 1, pp. 43–60, 2010.

[6] C.-F. Lai, S.-Y. Chang, H.-C. Chao, and Y.-M. Huang, "Detection of cognitive injured body region using multiple triaxial accelerometers for elderly falling," *IEEE Sensors Journal*, vol. 11, no. 3, pp. 763–770, 2011.

[7] S. Chen, H. Bao, X. Zeng, and Y. Yang, "A fire detecting method based on multi-sensor data fusion," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, pp. 3775–3780, October 2003.

[8] S. L. Rose-Pehrsson, R. E. Shaffer, S. J. Hart et al., "Multi-criteria fire detection systems using a probabilistic neural network," *Sensors and Actuators B*, vol. 69, no. 3, pp. 325–335, 2000.

[9] S. L. Rose-Pehrsson, S. J. Hart, T. T. Street et al., "Early warning fire detection system using a probabilistic neural network," *Fire Technology*, vol. 39, no. 2, pp. 147–171, 2003.

[10] E. Zervas, A. Mpimpoudis, C. Anagnostopoulos, O. Sekkas, and S. Hadjiefthymiades, "Multisensor data fusion for fire detection," *Information Fusion*, vol. 12, no. 3, pp. 150–159, 2011.

[11] K. -S. Lee and C. -G. Lee, "A component-based reconfigurable sensor network monitor for adapting time-critical requirements," *Journal of Internet Technology*, vol. 14, no. 3, pp. 443–452, 2013.

[12] R. C. Luo and K. L. Su, "Autonomous fire-detection system using adaptive sensory fusion for intelligent security robot," *IEEE/ASME Transactions on Mechatronics*, vol. 12, no. 3, pp. 274–281, 2007.

[13] A. Neubauer, "Genetic algorithms in automatic fire detection technology," in *Proceedings of the 2nd International Conference on Genetic Algorithms in Engineering Systems: Innovations and Applications*, pp. 180–185, 1997.

[14] D. M. Doolin and N. Sitar, "Wireless sensors for wildfire monitoring," in *Smart Structures and Materials 2005: Sensors and Smart Structures Technologies for Civil, Mechanical, and Aerospace Systems*, vol. 5765 of *Proceedings of SPIE*, San Diego, Calif, USA, March 2005.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 278132, 7 pages
http://dx.doi.org/10.1155/2013/278132

Research Article

Performance Evaluation of Page Migration Scheme for NVRAM-Based Wireless Sensor Nodes

Yeonseung Ryu

Department of Computer Engineering, Myongji University, Nam-dong, Yongin, Gyeonggi-do 449-728, Republic of Korea

Correspondence should be addressed to Yeonseung Ryu; ysryu@mju.ac.kr

Received 2 October 2013; Accepted 4 November 2013

Academic Editor: James J. Park

A wireless sensor network consists of low-powered and multifunctional sensor nodes. Since each sensor node is operated by a battery, the energy management has become one of the critical design challenges in wireless sensor networks. Some recent studies have shown that DRAM-based main memory spends a significant portion of the total system power. In this paper, we studied a buffer management scheme for hybrid main memory that combines low-power nonvolatile RAM (NVRAM) and DRAM in order to reduce the energy consumption in a sensor node. Though NVRAMs consume less power than volatile memories, they have common problems in write performance. The proposed scheme employs the page migration technique in order to reduce the write operations on NVRAM part of hybrid main memory. We have performed simulation studies and showed that the proposed page migration scheme outperforms the legacy buffer management schemes in terms of the number of write operations on NVRAM.

1. Introduction

Wireless sensor networks (WSNs) are composed of a number of sensor nodes and are able to perform complex tasks such as monitoring a region to obtain data about the environment and sending data to a central repository station. Today's sensor nodes are full-fledged computer systems, with a processor, main memory, storage, operating system, and a suite of sensors [1–4]. Sensor nodes collect not only sensed data from the environment, but also a stream of mass media data like videos and images. In order to process massive data volumes, sensor nodes are expected to require much more memory than legacy sensor nodes. Each sensor node is operated by a battery, and usually it is not feasible to replace or recharge this battery after deployment. The lifetime of a sensor network is considered over as soon as the battery power of the nodes is completely depleted. Therefore, the energy management of sensor nodes has become one of the key challenges in designing WSNs.

There have been a lot of studies to minimize the energy consumption for WSNs [5, 6]. While most previous studies have dealt with low power communication [7–10], this work focuses on reducing the energy consumption in the main memory in sensor nodes. Sensor nodes use DRAM for main memory as legacy computer systems do. However, recent studies have shown that DRAM-based main memory spends a significant portion of the total system power [11]. Since the capacitors used in DRAM lose their charge over time, DRAM must refresh all the cells approximately 20 times a second, reading each one and rewriting its contents. Such endless refresh operations consume nontrivial amount of power and become a contributing factor for power depletion of sensor node.

The recent advance of memory technology has ushered in new nonvolatile RAM (NVRAM) designs such as PRAM (phase change RAM), STT-MRAM (spin-torque transfer magnetic RAM), and FeRAM (ferroelectric RAM) that overcome the drawbacks of existing volatile memories such as SRAM or DRAM [12–15]. Among the NVRAMs, PRAM and STT-MRAM are becoming promising candidates for main memory because of their high density, comparable read access speed, and low power consumption. Unfortunately, cost per byte of new NVRAMs is extremely higher than that of DRAM until now. As a result, hybrid main memory using DRAM and NVRAM seems to be practicable instead of pure NVRAM-based main memory in the near future. Some recent studies have introduced NVRAM-based main memory organization as follows: PRAM-based main memory organization [16, 17], DRAM/PRAM hybrid main memory organization [18–22], and STT-MRAM-based memory organization [23, 24]. Also, there have been some buffer management schemes for PRAM-based main memory and DRAM/PRAM hybrid main memory [20, 25, 26]. From this research trend, it is highly expected that NVRAM-based hybrid main memory will be used in the next generation sensor nodes soon.

In this paper, we study an NVRAM-aware buffer management scheme for wireless sensor nodes which use DRAM/NVRAM hybrid main memory. Figure 1 illustrates the system configuration considered in this paper. Though NVRAM has attractive features, the write performance (access latency and energy consumption) of NVRAM is not comparable to that of DRAM. The goal of proposed buffer management scheme is to reduce the number of write operations on NVRAM. To do so, the proposed buffer management scheme performs *page migration* which moves the data from NVRAM to DRAM when the data needs to be written on NVRAM. Furthermore, proposed scheme deallocates clean DRAM buffers eagerly (*greedy deallocation*) in order to secure free DRAM buffers and thus minimize the number of write operations on NVRAM. We show, through trace-driven simulation, that the proposed scheme outperforms other legacy buffer management schemes in terms of the buffer hit ratio and the number of writes on NVRAM.

The rest of this paper is organized as follows. In Section 2, we describe the characteristics of nonvolatile memories such as PRAM, STT-MRAM, and NAND flash memory. Also, we introduce major buffer management schemes which are based on nonvolatile memory. In Section 3, we propose a buffer management scheme called NVRAM-aware buffer (NAB) scheme. It is followed by the description of page migration and greedy deallocation techniques in detail. Section 4 presents the performance evaluation results. Finally, Section 5 concludes the paper.

2. Related Works

2.1. Nonvolatile Memories. Among the NVRAMs, PRAM and STT-MRAM are becoming promising candidates for main memory because of their high density, comparable read access speed, and low power consumption. Table 1 shows the comparison of PRAM, STT-MRAM, and DRAM.

A PRAM cell uses a special material, called phase change material, to represent a bit [12, 27]. The phase change material can exist in two different but stable structural states: amorphous and crystalline, each of which has drastically different resistivity which can be used to represent logic 0 or 1. PRAM density is expected to be much greater than that of DRAM (about four times). Further, PRAM has negligible leakage energy regardless of the size of the memory. While its read performance (latency and energy) is comparable to that of DRAM, its write performance is worse than that of DRAM. Also, PRAM has a worn-out problem caused by limited write endurance (i.e., 10^8). Since the write operations on PRAM significantly affect the performance of system, it should be carefully handled.

STT-MRAM is a next generation memory technology that takes advantage of magnetoresistance for storing data [13–15]. It uses a magnetic tunnel junction (MTJ), the fundamental building block, as a binary storage. An MTJ comprises a three-layered stack: two ferromagnetic layers and an MgO tunnel barrier in the middle (see Figure 2). Among them, the fixed layer located at the bottom has a static magnetic spin, the spin of the electrons in the free layer at the top is influenced by applying adequate current through the fixed layer to polarize the current, and the current is passed to the free layer. Depending on the current, the spin polarity of the free layer changes either parallel or antiparallel to that of the fixed layer. The parallel indicates a zero state, and the antiparallel a one state.

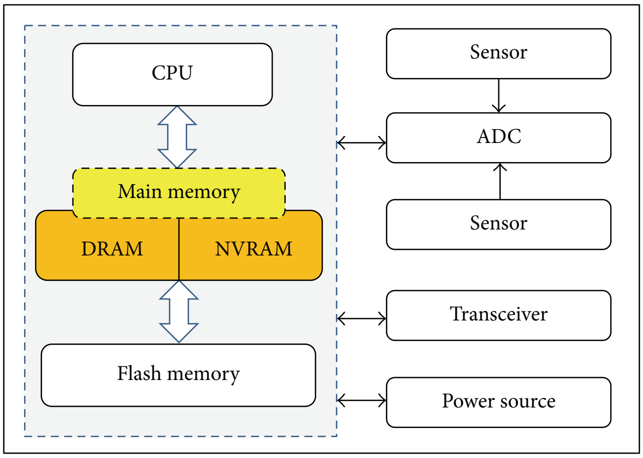


Figure 1: Internal organization of the proposed sensor node.

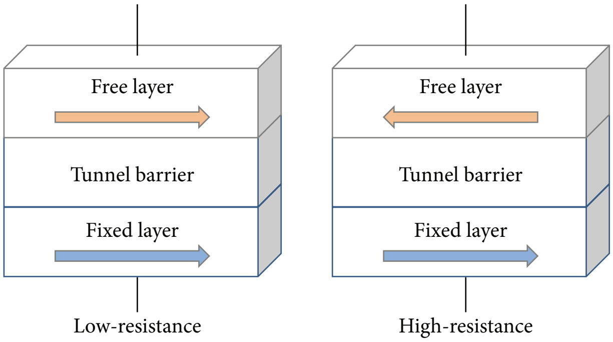


Figure 2: MTJ block [13–15].

One of the biggest weaknesses of STT-MRAM is long write latency compared to DRAM. Since the fast access time of memories on a chip must be guaranteed and cannot be negotiable, the slow write operations of STT-MRAM limit its popularity, even though it shows competitive read performance. Another serious drawback of STT-MRAM is high power consumption in write operations.

Flash memory is a sort of nonvolatile memory which has been widely used in storage devices [28, 29]. Unlike PRAM and STT-MRAM, flash memory is a kind of electrically erasable programmable ROM (EEPROM). A flash memory consists of multiple blocks, and each block is composed of multiple pages. A block is the smallest unit of an erase operation, whereas the smallest unit for the read and write operation is a page. Erase operations are

Table 1: Comparison of memories.

	PRAM	STT-MRAM	DRAM
Volatility	No	No	Yes
Cost/TB	High	High	Low
Read latency	50~100 ns	30 ns	15~50 ns
Write latency	150 ns	30~100 ns	15~50 ns
Endurance	10^8 for write	—	—
Idle power	~0.05 W	~0.05 W	~1.3 W/GB
Read energy	~0.1 nJ/b	~0.1 nJ/b	~0.1 nJ/b
Write energy	~0.5 nJ/b	~0.5 nJ/b	~0.1 nJ/b

significantly slower than the read/write operations. Further, write operations are slower than read operations. Existing data in flash memory cannot be written over; the memory has to be erased in advance in order to write new data. Erase operation degrades the system performance and consumes a considerable amount of power.

2.2. Buffer Management Schemes. There have been a lot of studies on buffer management schemes considering nonvolatile memories [25, 26, 28–33]. In particular, a number of flash memory aware buffer management schemes have been studied over the past decade [28–33]. The goal of these schemes is to minimize the number of erase operations on flash memory. A page-level scheme called clean-first least recently used (CFLRU) was proposed by [32]. CFLRU maintains a page list by LRU order and divides the page list into two regions, namely, the working region and clean-first region. In order to reduce the write cost on flash memory, CFLRU first evicts clean pages in the clean-first region by the LRU order, and if there are no clean pages in the clean-first region, it evicts dirty pages by their LRU order. CFLRU can reduce the number of write and erase operations by delaying the flush of dirty pages in the page cache.

Also, a block-level buffer cache scheme called block padding LRU (BPLRU) was proposed, which considers the erase operations on flash memory [33]. BPLRU maintains an LRU list based on the flash memory block. Whenever a page in the buffer cache is referenced, all pages in the same block are moved to the MRU position. When buffer cache is full, BPLRU scheme evicts all the pages of a victim block but it simply selects the victim block at the LRU position. In addition, it writes a whole block into a log block by the in-place scheme using the page padding technique. In page padding procedure, BPLRU reads some pages that are not in the victim block and writes all pages in the block sequentially. The page padding may perform unnecessary reads and writes, but it is effective because it can change an expensive full merge to an efficient switch merge. In BPLRU, all log blocks can be merged by the switch merge, which results in decreasing the number of erase operations.

For the DRAM/PRAM hybrid main memory, a multiple queue scheme (we call it 4Q scheme) was proposed [25]. 4Q maintains a page list by LRU order and evicts a page from LRU position. In order to reduce the writes on PRAM, 4Q predicts the page access pattern and migrates pages to DRAM or PRAM according to the access pattern. 4Q dynamically moves the write-bound pages from PRAM to DRAM and moves the read-bound pages from DRAM to PRAM. For prediction of the access pattern, 4Q calculates the weighting values of each page at every request and maintains 4 types of monitoring queues (see Figure 3). 4Q shows good performance when the access pattern is highly skewed like financial workload. Though 4Q tries to reduce the number of write operations on PRAM, it does incur high run-time overhead.

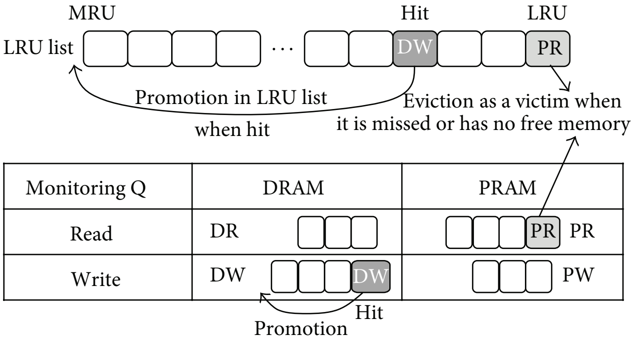


Figure 3: Monitoring queues of 4Q scheme [25].

3. NVRAM-Aware Buffer Management

We propose a buffer management scheme called NVRAM-aware buffer (NAB) for wireless sensor nodes which use DRAM/NVRAM hybrid main memory. Figure 1 illustrates the system configuration considered in this paper. The goal of the proposed scheme is to reduce the number of write operations on NVRAM.

3.1. Buffer Page Management. We assume that the main memory is divided into DRAM and NVRAM by a memory address. A portion of main memory is reserved for use as buffer. The buffer space is divided into a set of pages, each of which is a unit of buffer allocation/deallocation. The size of a page is fixed (i.e., 1 Kbytes).

The proposed NAB scheme maintains allocated pages as a page list by least recently used (LRU) order shown in Figure 4. The NAB defines a search region as a set of pages from the LRU position of the page list. When a new page needs to be allocated for storing data, the NAB allocates it from the free buffer pool and stores the data in it. And then, the NAB places it at the most recently used (MRU) position of the page list.

Whenever a page in the page list is accessed, it is moved to the MRU position. When a page is deallocated, it is removed from the page list and returned to the free buffer pool.

In Figure 4, there are 6 pages in the page list. The gray pages are allocated from NVRAM and the white pages are allocated from DRAM. The search region size is 3 pages.

3.2. Page Migration. In order to reduce the number of write operations on NVRAM, when a clean (i.e., not modified) page in the NVRAM is referenced by a write operation, the NAB performs the *page migration* procedure as shown in Algorithm 1.

First, the NAB tries to allocate a free DRAM page and writes requested data to the allocated DRAM page. Then it deallocates the original NVRAM page. In Figure 5, for example, data D0 in a NVRAM page is accessed by write request. Then the NAB allocates a free DRAM page and migrates the new data D0 to the newly allocated DRAM page. And then the NAB places it at MRU position of the page list.

If there is no free DRAM page in the free buffer pool, the NAB tries to find a clean DRAM page from the search region and uses it for storing the requested write data. If there is no clean DRAM page in the search region, the NAB writes requested data to the original NVRAM page.

3.3. Page Deallocation. The NAB proposes a greedy deallocation technique which frees clean DRAM pages even though free buffers are still available in the system. Because there could be a lot of used buffers that will not be accessed soon, we can free them early with little influence on the cache performance. To do so, the NAB searches clean DRAM pages from the search region periodically or whenever the number of free DRAM pages falls down below a threshold. Then, it makes them free. This scheme results in decreasing the number of writes on NVRAM because the NAB can secure free DRAM pages for new page allocations.

If all free pages are used up, the NAB selects a victim page from the search region in order to make free pages. In order to reduce the number of write operations on flash memory, the NAB tries to find a clean page. If there is no clean page in the search region, the NAB just selects a page at the LRU position of the page list. If necessary, the data in the victim page is stored in the storage (flash memory).

4. Performance Evaluation

4.1. Experiment Setup. In order to evaluate the proposed scheme, we have developed a trace-driven simulator. For the workload, we obtained the virtual memory traces of an application which is similar to database applications.

For example, TinyDB is a distributed query processor that runs on each of the nodes in a sensor network [4]. TinyDB runs on the Berkeley mote platform, on top of the TinyOS operating system [3]. Using sensor data management functionalities, users connect to the sensor network using a workstation or base station directly connected to a sensor designated as the sink. Aggregate queries over the sensor data are formulated using a simple SQL-like language and then distributed across the network. Aggregate results are sent back to the workstation over a spanning tree, with each sensor combining its own data with results received from its children.

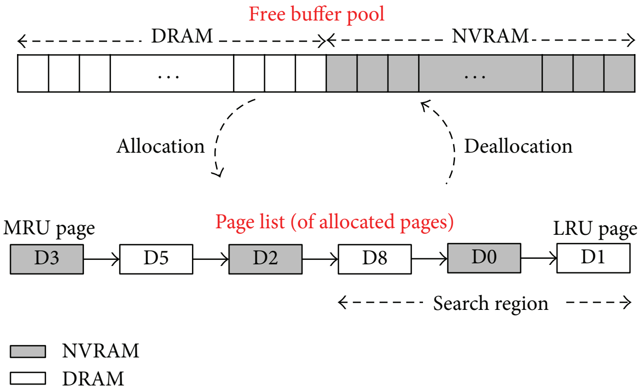


Figure 4: List-based buffer page management.

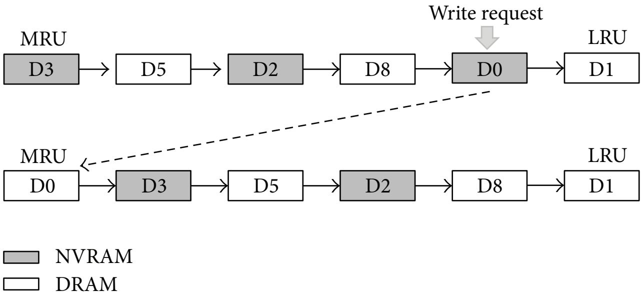


Figure 5: Page migration when write occurs.

We set the DRAM-to-NVRAM ratio as 1 : 1 and the search region size as 1/3 of the page list. We evaluate the buffer hit ratio and the write counts on NVRAM with varying the buffer size until the buffer hit ratio becomes 100%.

4.2. Buffer Hit Ratio. Figure 6 shows the comparison of buffer hit ratio with varying the buffer size. All schemes except Q4 are similar. When the buffer size is small (i.e., 10), the buffer hit ratio of Q4 is nearly 5% smaller than those of other schemes.

However, as the buffer size increases, the buffer hit ratios of all schemes increase rapidly and reach almost 100%.

4.3. Write Counts on NVRAM. Figure 7 shows the comparison of write counts on NVRAM. As the buffer size increases, the write counts on NVRAM decreases. Also, we can see that NVRAM-aware schemes such as Q4 and the NAB outperform other schemes. But, the write counts of NAB decreases faster than that of Q4 as the buffer size increases. Therefore, proposed NAB scheme outperforms all other legacy schemes in terms of the write counts on NVRAM.

4.4. Effect of DRAM-to-NVRAM Ratio. Figure 8 shows the write counts on NVRAM when the ratio of the size of DRAM to the size of NVRAM varies. We set the total buffer size as 500 pages. It is normal that the write counts on NVRAM increase as the ratio of NVRAM size increases. However, the

```
Page Migration
if (free DRAM page exists)
        allocate a DRAM page;
        perform write to the DRAM page;
        free original NVRAM page;
else if (clean DRAM page exists in search region)
        free it and allocate a DRAM page;
        perform write to the DRAM page;
        free original NVRAM page;
else
        perform write to the original NVRAM page;
place the page at MRU position of the page list;
```

Algorithm 1: Page migration procedure.

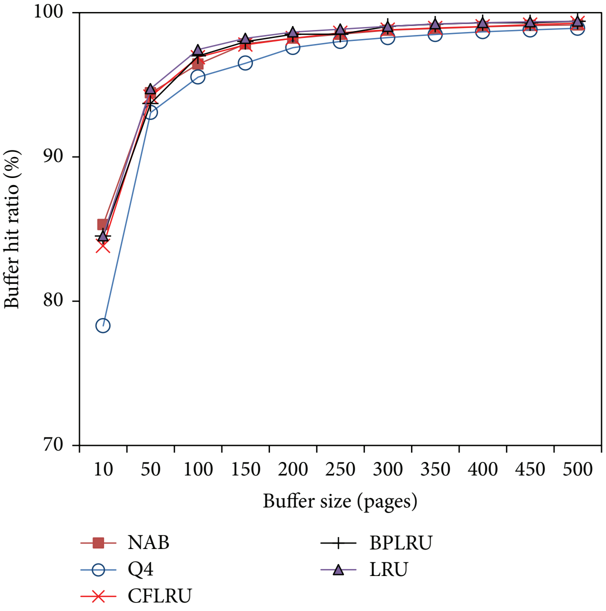


Figure 6: Buffer hit ratio.

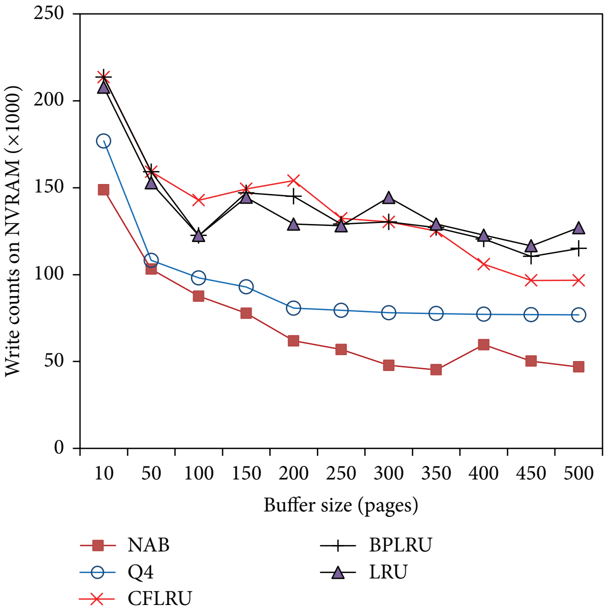


Figure 7: Write counts on NVRAM.

write counts of NAB are smaller than those of other schemes for all cases. Hence, the proposed NAB scheme outperforms legacy buffer schemes regardless of the DRAM-to-NVRAM ratio. The evaluation results of buffer hit ratios are not shown because they are similar to Figure 6.

5. Conclusion

The power of wireless sensor networks lies in the ability to deploy large number of sensor nodes that assemble and configure themselves. A sensor node is a battery-powered computer. If power is used naively, individual nodes will deplete their energy supplies in only a few days. In contrast, if sensor nodes are very spartan about power consumption, months or years of lifetime are possible. Hence, the energy management of sensor nodes has become one of the key design challenges in WSNs. While there are many studies about energy management for low power communication, there have been few researches on low power main memory using NVRAMs in sensor nodes.

In this paper, we study a buffer management scheme for sensor nodes which use NVRAM-based hybrid main memory. Though NVRAM is attractive in terms of power consumption and read performance, the write performance (access latency and energy consumption) of NVRAM is worse than that of DRAM. The proposed buffer management scheme employs a simple page migration technique which migrates the data from NVRAM to DRAM when the data needs to be written on NVRAM. Further, in order to secure free DRAM buffer, the proposed scheme employs a greedy deallocation technique that deallocates clean DRAM buffers even though free buffers are still available in the system. The proposed page migration scheme exhibits better performance than legacy buffer management schemes in terms of the buffer hit ratio and the number of writes on NVRAM. The

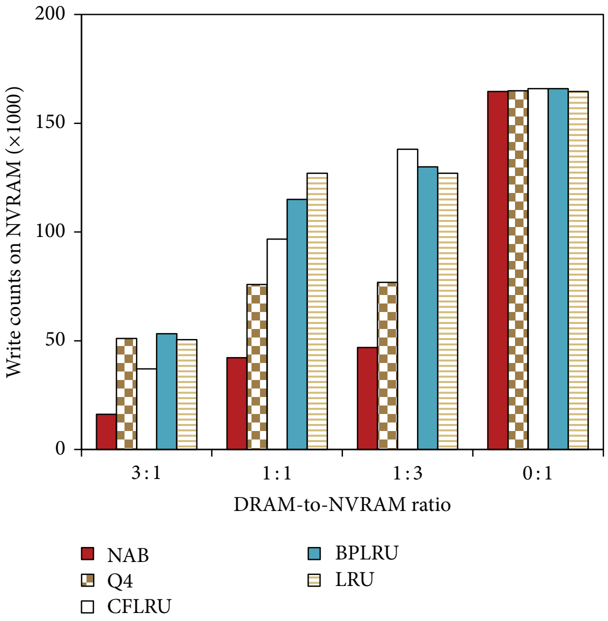


Figure 8: Write counts on NVRAM.

proposed scheme can be used when DRAM/NVRAM hybrid main memory is adopted in sensor nodes in the near future.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0021897). The author would like to thank Soohyun Yang who helped in the simulation experiment.

References

[1] N. Lin, Y. Dong, and D. Lu, "Providing virtual memory support for sensor networks with mass data processing," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 324641, 20 pages, 2013.

[2] A. Lachenmann, P. J. Marrón, M. Gauger, D. Minder, O. Saukh, and K. Rothermel, "Removing the memory limitations of sensor networks with flash-based virtual memory," in *Proceedings of the Eurosys Conference*, pp. 131–144, March 2007.

[3] M. O. Farooq and T. Kunz, "Operating systems for wireless sensor networks: a survey," *Sensors*, vol. 11, no. 6, pp. 5900–5930, 2011.

[4] S. R. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TinyDB: an acquisitional query processing system for sensor networks," *ACM Transactions on Database Systems*, vol. 30, no. 1, pp. 122–173, 2005.

[5] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," *ACM Transactions on Sensor Networks*, vol. 5, no. 1, article 6, 2009.

[6] Y. Gu and T. He, "Bounding communication delay in energy harvesting sensor networks," in *Proceedings of the 30th IEEE International Conference on Distributed Computing Systems (ICDCS '10)*, pp. 837–847, Genoa, Italy, June 2010.

[7] M. Yoon, Y. Kim, and J. Chang, "An energy-efficient routing protocol using message success rate in wireless sensor networks," *Journal of Convergence*, vol. 4, no. 2, pp. 15–22, 2013.

[8] G. Carvalho, I. Woungang, A. Anpalagan, and S. Dhurandher, "Energy-efficient radio resource management scheme for heterogeneous wireless networks: a queueing theory perspective," *Journal of Convergence*, vol. 3, no. 4, pp. 15–22, 2012.

[9] B. Singh and D. Lobiyal, "A novel energy-aware cluster head selection based on particle swarm optimization for wireless sensor networks," *Human-Centric Computing and Information Science*, vol. 2, no. 13, 2012.

[10] R. Sumathi and M. Srinivas, "A survey of QoS based routing protocols for wireless sensor networks," *Journal of Information Processing Systems*, vol. 8, no. 4, pp. 589–602, 2012.

[11] L. A. Barroso and U. Hölzle, "The case for energy-proportional computing," *Computer*, vol. 40, no. 12, pp. 33–37, 2007.

[12] Y. Xie, "Modeling, architecture, and applications for emerging memory technologies," *IEEE Design and Test of Computers*, vol. 28, no. 1, pp. 44–50, 2011.

[13] C. Augustine, N. N. Mojumder, X. Fong, S. H. Choday, S. P. Park, and K. Roy, "Spin-transfer torque MRAMs for low power memories: perspective and prospective," *IEEE Sensors Journal*, vol. 12, no. 4, pp. 756–766, 2012.

[14] D. Lee and S. Gupta K Roy, "High-performance low-energy STT-MRAM based on balanced write scheme," in *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED '12)*, pp. 9–14, 2012.

[15] X. Guo, E. Ipek, and T. Soyata, "Resistive computation: avoiding the power wall with low-leakage, STT-MRAM based computing," in *Proceedings of the 37th International Symposium on Computer Architecture (ISCA '10)*, pp. 371–382, June 2010.

[16] M. K. Qureshi, V. Srinivasan, and J. A. Rivers, "Scalable high performance main memory system using phase-change memory technology," in *Proceedings of the 36th Annual International Symposium on Computer Architecture (ISCA '09)*, pp. 24–33, June 2009.

[17] P. Zhou, B. Zhao, J. Yang, and Y. Zhang, "A durable and energy efficient main memory using phase change memory technology," in *Proceedings of the 36th Annual International Symposium on Computer Architecture (ISCA '09)*, pp. 14–23, June 2009.

[18] H. Park, S. Yoo, and S. Lee, "Power management of hybrid DRAM/PRAM-based main memory," in *Proceedings of the 48th ACM/EDAC/IEEE Design Automation Conference (DAC '11)*, pp. 59–64, June 2011.

[19] J. Hu, Q. Zhuge, C. Xue, W. Tseng, and E. Sha, "Software enabled wear-leveling for hybrid PCM main memory on embedded systems," in *Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE '13)*, pp. 599–602, March 2013.

[20] D. Lee and H. Oh, "A lifetime aware buffer assignment method for streaming applications on DRAM/PRAM hybrid memory," *ACM Transactions on Embedded Computing Systems*, vol. 12, no. 1, 2013.

[21] D. Kim, S. Lee, J. Chung et al., "Hybrid DRAM/PRAM-based main memory for single-chip CPU/GPU," in *Proceedings of the 49th Annual Design Automation Conference (DAC '12)*, pp. 888–896, 2012.

[22] J. Choi, S. Kim, C. Kim, and K. Park, "OPAMP: evaluation framework for optimal page allocation of hybrid main memory architecture," in *Proceedings of the International Conference on Parallel and Distributed Systems (ICPADS '12)*, pp. 620–627, 2012.

[23] H. Jang, B. An, N. Kulkarni, K. Yum, and E. Kim, "A hybrid buffer design with STT-MRAM for on-chip interconnects," in *Proceedings of the ACM/IEEE International Symposium on Networks-on-Chip (NOCS '12)*, pp. 193–200, 2012.

[24] E. Kultursay, M. Kandemir, A. Sivasubramaniam, and O. Mutlu, "Evaluating STT-RAM as an energy-efficient main memory alternative," in *Proceedings of the IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS '13)*, 2013.

[25] H. Seok, Y. Park, and K. Park, "Efficient page caching algorithm with prediction and migration for a hybrid main memory," *Applied Computing Review*, vol. 11, no. 4, 2012.

[26] L. E. Ramos, E. Gorbatov, and R. Bianchini, "Page placement in hybrid memory systems," in *Proceedings of the 25th ACM International Conference on Supercomputing (ICS '11)*, pp. 85–95, June 2011.

[27] O. Zilberberg, S. Weiss, and S. Toledo, "Phase-change memory: an architectural perspective," *ACM Computing Surveys*, vol. 45, no. 3, 2013.

[28] E. Gal and S. Toledo, "Algorithms and data structures for flash memories," *ACM Computing Surveys*, vol. 37, no. 2, pp. 138–163, 2005.

[29] Y. Ryu, "SAT: switchable address translation for flash memory storages," in *Proceedings of the 34th Annual IEEE International Computer Software and Applications Conference (COMPSAC '10)*, pp. 453–461, Seoul, South Korea, July 2010.

[30] Y. Yoo, H. Lee, Y. Ryu, and H. Bahn, "Page replacement algorithms for NAND flash memory storages," in *Proceedings of the International Conference on Computational Science and its Applications*, pp. 201–212, 2007.

[31] X. Tang and X. Meng, "ACR: an adaptive cost-aware buffer replacement algorithm for flash storage devices," in *Proceedings of the 11th IEEE International Conference on Mobile Data Management (MDM '10)*, pp. 33–42, Kansas City, Mo, USA, May 2010.

[32] S.-Y. Park, D. Jung, J.-U. Kang, J.-S. Kim, and J. Lee, "CFLRU: a replacement algorithm for flash memory," in *Proceedings of the International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES '06)*, pp. 234–241, October 2006.

[33] H. Kim and S. Ahn, "BPLRU: a buffer management scheme for improving random writes in flash storage," in *Proceedings of the 6th USENIX Conference on File and Storage Technologies*, 2008.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 782043, 8 pages
http://dx.doi.org/10.1155/2013/782043

Research Article

Human-Robot Interaction Learning Using Demonstration-Based Learning and *Q*-Learning in a Pervasive Sensing Environment

Yunsick Sung,[1] Seoungjae Cho,[2] Kyhyun Um,[3] Young-Sik Jeong,[3] Simon Fong,[4] and Kyungeun Cho[3]

[1] *The Department of Game Mobile Contents, Keimyung University, Daegu 704-701, Republic of Korea*
[2] *Department of Multimedia Engineering, Graduate School of Dongguk University, Seoul 100-715, Republic of Korea*
[3] *Department of Multimedia Engineering, Dongguk University, Seoul 100-715, Republic of Korea*
[4] *Department of Computer and Information Science, University of Macau, Macau 3000, China*

Correspondence should be addressed to Kyungeun Cho; cke@dongguk.edu

Received 28 August 2013; Accepted 16 October 2013

Academic Editor: James J. Park

Given that robots provide services in any locations after they move toward humans, the pervasive sensing environment can provide diverse kinds of services through the robots not depending on the locations of humans. For various services, robots need to learn accurate motor primitives such as walking and grabbing objects. However, learning motor primitives in a pervasive sensing environment are very time consuming. Several previous studies have considered robots learning motor primitives and interacting with humans in virtual environments. Given that a robot learns motor primitives based on observations, a disadvantage is that there is no way of defining motor primitives that cannot be observed by a robot. In this paper, we develop a novel interaction learning approach based on a virtual environment. The motor primitives are defined by manipulating a robot directly using demonstration-based learning. In addition, a robot can apply *Q*-learning to learn interactions with humans. In an experiment, using the proposed method, the motor primitives were generated intuitively and the amount of movement required by a virtual human in one of the experiments was reduced by about 25% after applying the generated motor primitives.

1. Introduction

In pervasive sensing environments, robots can provide various services in an active manner. Irrespective of the locations of humans, robots can provide services after they move toward humans based on the information of the humans' daily life [1]. However, the following problems may occur after a robot learns interactions with a human. First, a robot cannot learn interactions with humans rapidly, which leads to learning time problems during interaction learning. Therefore, it is necessary to learn interactions with humans without the participation of humans. Second, an interaction between a robot and a human could injure the latter, because of the incomplete perception of robots. Therefore, protective equipment is required by humans.

Previous studies have considered interaction learning with a human in virtual environments, which can solve the problems described above [2–4]. A virtual robot can generate its motor primitives by observing a virtual human in virtual environments and utilizing demonstration-based learning. However, unobservable motor primitives cannot be generated. In addition, because of the differences in the appearance of a robot and a human, the motor primitives of robots may differ from the movements of humans and it might not be possible to perform the motor primitives generated for a robot. Thus, the methods used to generate different motor primitives need to be improved. Further research is required to determine how to teach motor primitives to a robot while learning interactions with humans in a virtual environment.

In this paper, we propose a virtual pervasive sensing environment-based interaction learning method that utilizes demonstration-based learning to learn motor primitives and Q-learning to execute motor primitives. The motor primitives are defined during manipulations based on demonstration learning, so the motor primitives can be generated intuitively by users who are not programmers. The application of Q-learning allows the newly generated motor primitives to be performed without modifying any of the algorithms after their production.

The remainder of this paper is organized as follows. Section 2 introduces demonstration-based learning approaches and virtual environment-based learning. Section 3 proposes an interaction learning method for a virtual pervasive sensing environment. Section 4 presents the results of interaction learning experiments in virtual pervasive sensing environments. Finally, we provide our conclusions in Section 5.

2. Related Work

Various types of learning algorithms are required to allow robots to interact with humans. In this section, we summarize related research into the learning of motor primitives and the learning of interactions with humans in virtual environment.

The motor primitives learned by robots are very important for achieving their goals. The repulsion of robots can be reduced by different motor primitives. Different types of research are ongoing to produce motor primitives for robots that appear more natural, like those of humans. For example, a related study defined natural motor primitives for following the shortest path [5, 6]. A genetic algorithm was used to generate these movements. Following mutation, the motor primitives that failed to follow the shortest path were eliminated and new motor primitives were generated. Another approach is to use demonstration-based learning [7–9]. Demonstration-based learning algorithms learn each motor primitive separately based on repetition, before analyzing the same learned motor primitives [7, 10]. Another approach involves learning motor primitives by dividing a series of movements [8], where each motor primitive is defined as a part of the series of movements. Furthermore, an approach was proposed that generates motor primitives as a hierarchical tree [9, 11]. Within the same hierarchical tree, a robot executes the same motor primitive initially but executes different motor primitives in different states. The motor primitives are usually generated by planning algorithms [12]. However, some problems may occur if planning algorithms are applied. For example, planning algorithms are defined based on the generated motor primitives. If the motor primitives change, the planning algorithms must also be changed to execute the motor primitives. An advantage of demonstration-based learning is that humans can define motor primitives without any requirement for programming. However, this advantage does not apply to planning algorithms. Therefore, algorithms are required that are not affected by changes to the motor primitives.

There is a method that learns the interaction with humans by utilizing motor primitives after generating the motor primitives using demonstration-based learning [13]. A previous study defined a virtual human and a virtual robot, where the former is a virtual agent that behaves in virtual environments in the same way as a human in a virtual environment, while the latter behaves like a real robot. Therefore, a virtual robot interacts with a virtual human to learn an interaction with a real human. If a virtual human executes a motor primitive, the virtual robot also executes the motor primitive at the same time. However, virtual-based interaction learning has problems. For example, the motor primitives used by a virtual robot cannot be generated if a virtual human does not execute the motor primitives, because they are generated by observing the virtual human. Therefore, another approach is required for generating motor primitives.

Thus, we propose a new approach for defining the motor primitives for a virtual robot. We also apply Q-learning to solve the problem of executing motor primitives, which does not require any changes after the modification of motor primitives.

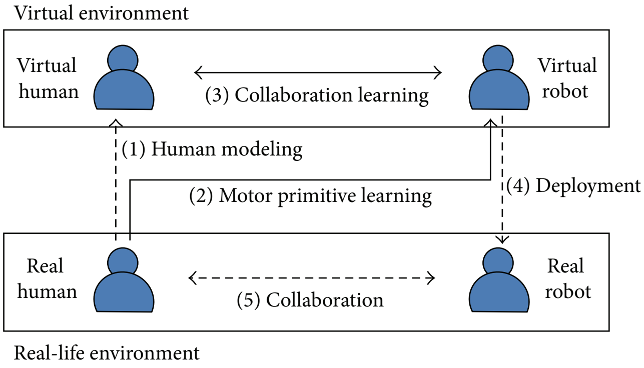


Figure 1: Process used for learning interactions.

3. Virtual Learning Framework for Human-Robot Interaction

3.1. Concept. In a pervasive sensing environment, it takes a long time to learn interactions with humans and the number of interactions with robots is limited. Therefore, the number of interactions should be reduced to increase the amount of the learning to facilitate the high quality execution of motor primitives. In our approach, the interactions are learned via a virtual pervasive sensing environment, so no interactions are required in real pervasive sensing environments, as shown in Figure 1.

We define two types of virtual agents for learning in a virtual pervasive sensing environment: a virtual human and a virtual robot. The virtual human acts like a human while the virtual robot executes motor primitives to collaborate with the virtual human. The virtual robot learns interactions with real humans by interacting with virtual humans. The learning result is then embedded in the real robot. The real robot executes motor primitives based on the results of virtual learning to interact with a real human.

Table 1: Approaches used in different stages of interaction learning by robots.

Stage	Type of agent	Learning approach
Motor primitive learning	Virtual robot	Direct manipulation of a robot
Collaboration learning	Virtual robot	Interaction with a virtual human by Q-learning [13]

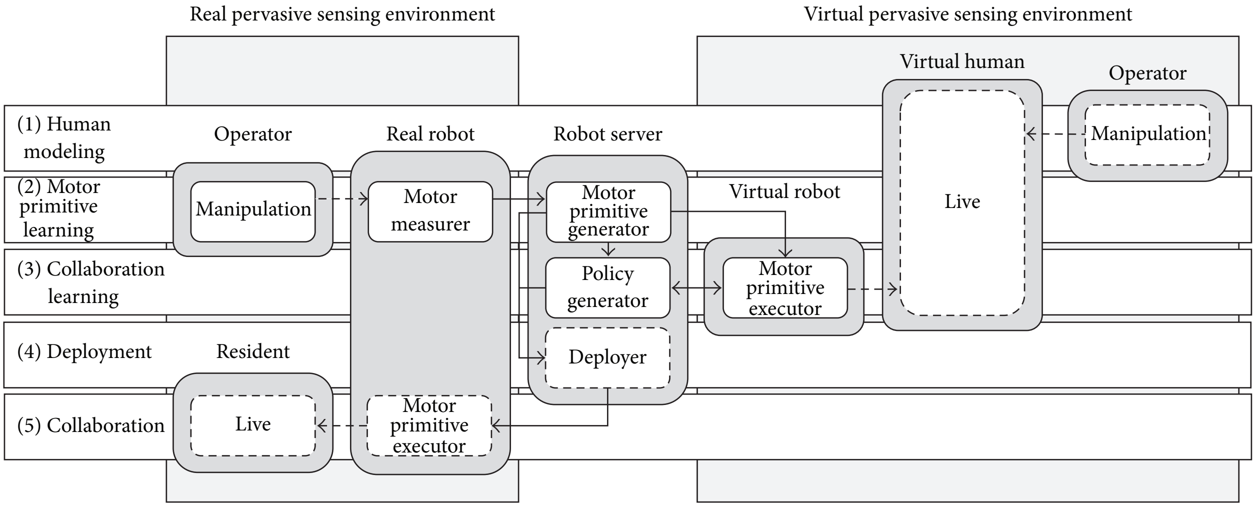


Figure 2: Framework for interaction learning.

There is no requirement for interactions with real humans. The learning time problem is always invoked if a human is involved during learning processes, which makes it very hard to reduce the learning time. However, the learning time can be reduced more by increasing the speed of interactions between a virtual human and a virtual robot. This is because a virtual human and a virtual robot do not need to execute motor primitives at the same speed as a real human and a real robot.

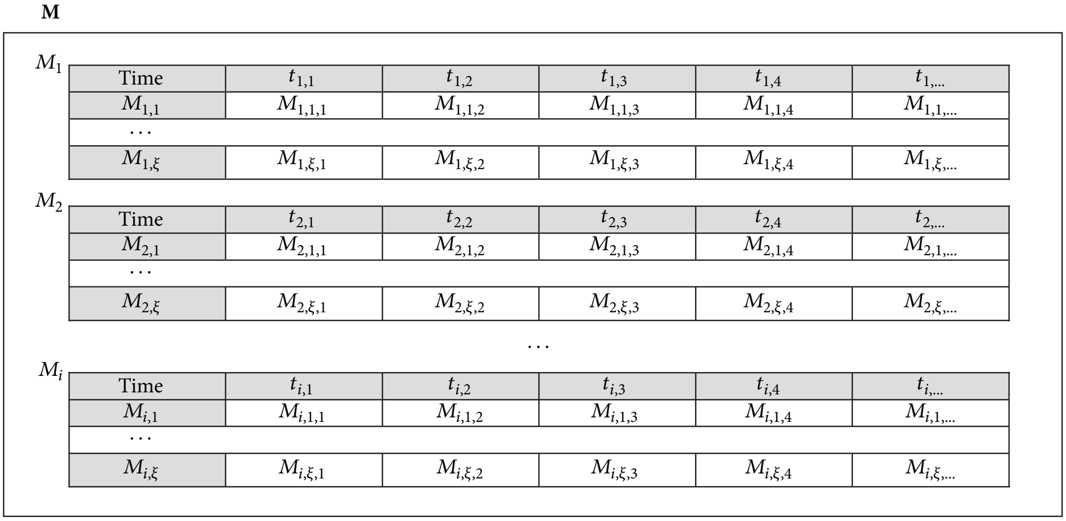
In our approach, interaction learning includes human modeling, motor primitive learning, collaboration learning, deployment, and collaboration stages. In this paper, we only propose the processes used during the motor primitive learning stage and the collaboration learning stage as shown in Table 1. During the human modeling stage, humans control a virtual human to make them act like humans by executing predefined motor primitives. The virtual humans learn how to execute motor primitives by analyzing the human control process. During the motor primitive learning stage, humans control the virtual robots directly to teach them how to move, and the virtual robots then generate their own motor primitives. Next, the virtual robot interacts with a virtual human by executing the learnt motor primitives. During this interaction, the virtual robot learns how to provide services to humans. The results obtained from motor primitive generation and from interactions are then applied in a real robot, which can interact with real humans.

3.2. Human-Robot Interaction Framework and Processes. The roles of real humans are divided into two groups during whole learning processes: one for residents and the other for operators. Operators teach real robots while residents live in pervasive sensing environments. All of the virtual humans in the virtual pervasive sensing environment are virtual residents. We also define a robot server as a server that generates motor primitives and policies, which transfers data between a real robot and a virtual robot. Our proposed framework is shown in Figure 2.

First, an operator controls a virtual human via a user interface. During the motor primitive learning stage, there are two modules in a real robot: a motor measurer and a motor primitive generator. The motor measurer is deployed in a real robot. When the operator manipulates a real robot directly, the motor measurer determines the degrees of the joints in the real robot. The motor primitive generator is embedded in the robot server rather than the real robot, which separates the dependency of the motor primitive generator from the robot platform. The generated motor primitives are deployed in the virtual robot and the real robot.

During the collaboration learning stage, a policy generator and a motor primitive executor are utilized to learn the interactions between a resident and a real robot based on the interactions that occur between a virtual human and a virtual robot. The motor primitive executor executes the generated motor primitives and the policy generator then generates the results of the interaction. The interaction results are then deployed in the real robot. Finally, the real robot can provide various services by executing the motor primitives based on the interaction learning results.

In our approach, a robot executes multiple motor primitives. M_i is the ith motor primitive. A motor primitive is de fined as a part of a series of movements, which is described by multiple joints of the robot. Therefore, M_i comprises multiple joints. The kth joint of the ith motor primitive is defined



M

M_1

Time	$t_{1,1}$	$t_{1,2}$	$t_{1,3}$	$t_{1,4}$	$t_{1,...}$
$M_{1,1}$	$M_{1,1,1}$	$M_{1,1,2}$	$M_{1,1,3}$	$M_{1,1,4}$	$M_{1,1,...}$
⋯					
$M_{1,\xi}$	$M_{1,\xi,1}$	$M_{1,\xi,2}$	$M_{1,\xi,3}$	$M_{1,\xi,4}$	$M_{1,\xi,...}$

M_2

Time	$t_{2,1}$	$t_{2,2}$	$t_{2,3}$	$t_{2,4}$	$t_{2,...}$
$M_{2,1}$	$M_{2,1,1}$	$M_{2,1,2}$	$M_{2,1,3}$	$M_{2,1,4}$	$M_{2,1,...}$
⋯					
$M_{2,\xi}$	$M_{2,\xi,1}$	$M_{2,\xi,2}$	$M_{2,\xi,3}$	$M_{2,\xi,4}$	$M_{2,\xi,...}$

⋯

M_i

Time	$t_{i,1}$	$t_{i,2}$	$t_{i,3}$	$t_{i,4}$	$t_{i,...}$
$M_{i,1}$	$M_{i,1,1}$	$M_{i,1,2}$	$M_{i,1,3}$	$M_{i,1,4}$	$M_{i,1,...}$
⋯					
$M_{i,\xi}$	$M_{i,\xi,1}$	$M_{i,\xi,2}$	$M_{i,\xi,3}$	$M_{i,\xi,4}$	$M_{i,\xi,...}$

Figure 3: Configuration of the motor primitive set.

by $M_{i,k}$. $M_{i,k,h}$ is the hth measured $M_{i,k}$. If ξ is the number of joints, M_i is $\langle M_{i,1}, \ldots, M_{i,k}, \ldots, M_{i,\xi}\rangle$. Each joint moves irregularly. $t_{i,h}$ denotes the time when $M_{i,k,h}$ is executed. Finally, the set **M** is a motor primitive set. Figure 3 shows the example of the configuration of the motor primitive set.

To eliminate any differences between motor primitives of a virtual robot and a real robot, the motor primitive generator generates the same motor primitives for both. To reduce the number of movements measured, any movements are eliminated that do not change as much as the difference calculated using (1). After similar movements are eliminated, the motor primitives are generated using the remaining measured movements. Consider

$$\left(M_{i,k,1} - M_{i,k-1,1}\right)^2 + \left(M_{i,k,2} - M_{i,k-1,2}\right)^2 + \cdots < \delta^2. \quad (1)$$

Given that pervasive sensing environment is usually complex, the policy generator used by our approach utilizes Q-learning [14] to execute the generated motor primitives, because Q-learning has the advantage that a model of the environment does not need to be defined. In addition, Q-learning algorithm does not need to be modified after the motor primitives are generated. The policy generator selects motor primitives depending on the current state s and sends the selected motor primitive to the motor primitive executor for execution. After executing each motor primitive, the corresponding reward of the executed motor primitives is calculated and transferred back to the policy generator. The policy generator updates the Q-values with the reward using

$$\begin{aligned} Q(s, M) \longleftarrow\, & Q(s, M) + \alpha \\ & \times \left\{r + \gamma \times \max Q\left(s', M'\right) - Q(s, M)\right\}, \end{aligned} \quad (2)$$

where M is an executed motor primitive, s is a state, r is a reward after executing M, s' and M' are the next state and the next motor primitive, respectively, α denotes the learning rate, and γ is a discount factor.

The motor primitive executor receives motor primitives from the motor primitive generator and executes the motor primitives according to the decisions made by the policy generator. After executing the motor primitives, the corresponding reward of the executed motor primitives is transferred to the policy generator.

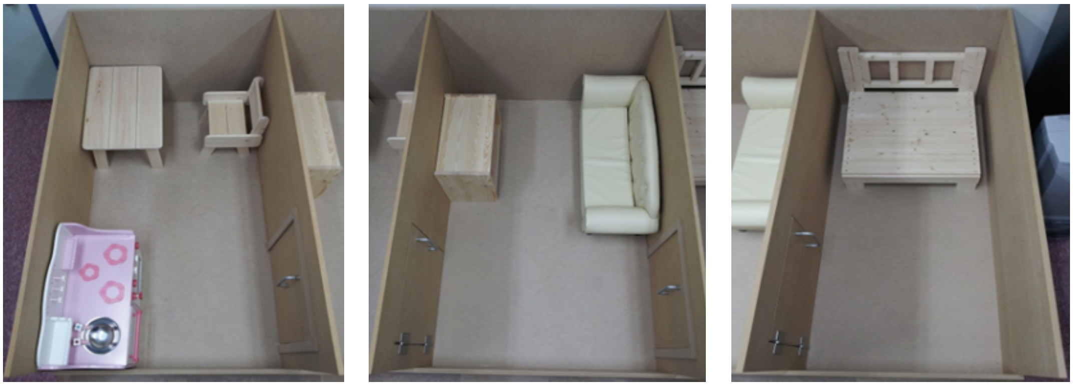
4. Experiment

4.1. Configurations of the Real and Virtual Pervasive Sensing Environments. In our experiment, we used a Nao as a real robot. We also built a model house, which was a suitable size for the Nao, as shown in Figure 4. The model house contained a kitchen, living room, and bedroom. The Nao learned during interactions with a real human.

The objective of the Nao was to transfer the objects required by a real human. After recognizing the object, the Nao moved toward the object initially. Next, it grabbed the object, moved toward the real human, and gave the object to the real human. In the experiments, we used the objects shown in Table 2. There were two types of objects: static objects that could not be moved and movable objects, which a Nao and a human could grab, carry, and put down.

The state space must be defined in advance to use Q-learning. In this experiment, we denoted the positions of the human and the robot based on their grid coordinates, after taking a picture using an omnicamera placed on the ceiling and dividing the picture into the grid shown in Figure 5. The size of each cell was set to the width of the Nao. Thus, 50 cells were defined. We defined each state based on the coordinates of the human, the robot, and the object located nearest to the human.

To learn interactions between a real human and a real robot, the virtual pervasive sensing environment used in this experiment was modeled in exactly the same way as the real pervasive sensing environment, as shown in Figure 6. Therefore, the structure and size of the virtual pervasive sensing environment were the same as the real pervasive



(a) (b) (c)

Figure 4: Model house as a pervasive sensing environment.

Table 2: Objects used in the experiments.

Location	Object	Object type
Kitchen	Cup	Movable object
	Kettle	Movable object
	Chair	Movable object
	Kitchen table	Static object
	Stove	Static object
Living room	TV table	Static object
	TV (assumed)	Static object
	Couch	Static object
	Remote controller	Movable object
	Newspaper	Movable object
Room	Bed	Static object

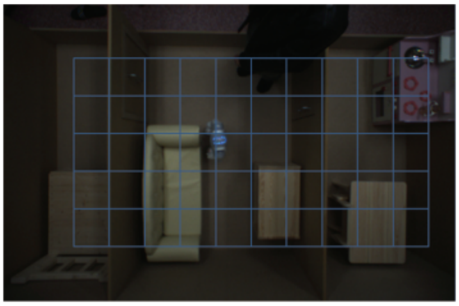


Figure 5: Grid environment of the real pervasive sensing environment used for interaction learning.

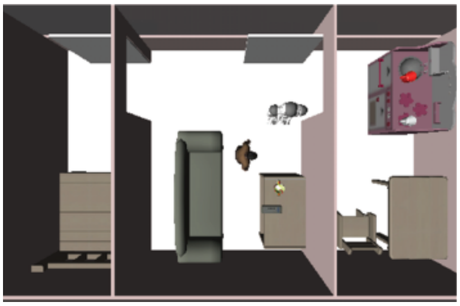


Figure 6: Virtual pervasive sensing environment used for interaction learning.

Table 3: Predefined motor primitives for a virtual robot and a real robot.

Notation	Name	Description
M_0	Standing before grabbing	If a real robot has not grabbed an object, it stands and waits to execute the next motor primitive
M_1	Standing after grabbing	If a real robot has grabbed an object, it stands and waits to execute the next motor primitive
M_{10}	Walking	A real robot follows a ball while remaining at a fixed distance from the ball

sensing environment. Objects were also deployed in the same way as the real pervasive sensing environment. We utilized two virtual agents as a virtual human and a virtual robot.

4.2. Configuration of the Motor Primitives. A real operator controlled a virtual robot, while a virtual human and a robot server were also used, depending on the stage. The robot followed a different process during each stage and the real operator also controlled the state of the real robot by touching a touch sensor on the head of the real robot.

The motor primitives of the robot were defined as follows. The real operator manipulated the robot directly to make the robot learn the motor primitives. There were two types of motor primitives. First, a type of motor primitive was predefined by programming, as shown in Table 3. For example, given that an initial motor primitive was required and that it was very hard to define a walking motor primitive by

Table 4: Virtual human animations.

Name	Description
Standing	Standing with arms down
One-hand grabbing	Stretching arms, grabbing objects, and carrying objects while standing
One-hand placing	Stretching arms and placing one of the grabbed objects while standing
Touching	Turning the switch of a light or stove on or off
Receiving	Receiving an object with the right hand
Giving	Giving an object with the right hand
Walking	Walking toward a specific object
Sitting	Sitting on a chair or couch
Laying	Laying down on a bed

manipulation, the real robot executed two preprogrammed standing motor primitives and one walking motor primitive. The other type of motor primitive was defined by the manipulations performed by the operator.

For the walking motor primitive, the algorithm determined a path from the current coordinates to specific coordinates. We used the A^* search algorithm because the grids of the virtual and real pervasive sensing environments were not complex and they only comprised 50 cells. For example, if a real operator was in the specific position where a virtual human needed to move, the virtual human moved to the position while avoiding objects and walls.

While the real robot was learning the motor primitives, the real robot measured its joints every 500 ms and transferred the values of the joints to the robot server. If the interval is set under 500 ms, the joints are not measured accurately, which delays the performance of the real robot.

We predefined the animation of the virtual human, as shown in Table 4. The objective of the Nao was to transfer objects for a virtual human, so the animation of the virtual human also focused on transferring objects.

4.3. Motor Primitive Generation Experiment. The first experiment aimed to generate motor primitives for the Nao. An operator defined the motor primitives from M_2 to M_7 by manipulating the arms and touching the touch sensors on the arms, as shown in Table 5. In this experiment, the operator only controlled the arms because the legs only moved when the robot walked.

The real robot executed a series of motor primitives. The end of a motor primitive was connected to the end of the next motor primitive in a natural manner. Thus, the standing motor primitives were executed after each motor primitive and the next motor primitive started after the end of the standing motor primitive. Therefore, we defined the sequence of motor primitives as shown in Figure 7.

Some of motor primitives could not be connected with the standing motor primitive because of the grabbed objects. Therefore, standing after grabbing was added. Standing after grabbing was performed after executing, receiving, or one-hand grabbing, followed by one-hand placing or giving.

Table 5: Motor primitives learned during the manipulations.

Notation	Name	Description
M_2	One-hand grabbing	Stretching arms, grabbing objects, and carrying objects while standing
M_3	One-hand placing	Stretching arms and placing one of the grabbed objects while standing
M_4	Touching	Turning the switch of a light or stove on or off
M_5	(Reserved)	
M_6	Receiving	Receiving an object with the right hand
M_7	Giving	Giving an object with the right hand

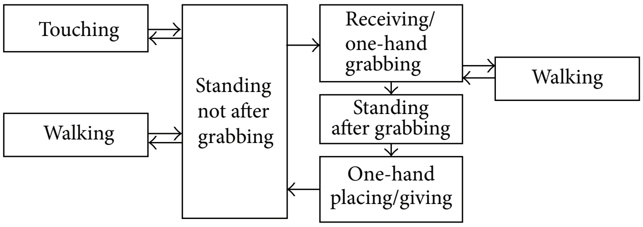


Figure 7: Sequential relationships among the motor primitives.

Each motor primitive was generated based on separate manipulation performed by a real human. Figure 8 shows four of the generated motor primitives. Only five joints were measured, which were all related to the right hand. The generated motor primitive was then performed by the virtual robot.

4.4. Interaction Learning Experiment. We specified a scenario for learning the interactions. First, we applied our approach to the scenario where a human stood up, sat on a couch, and then read a newspaper after picking it up, as shown in the following list (a).

Interaction Learning Results

(a) Scenario where a virtual human lives alone is as follows:

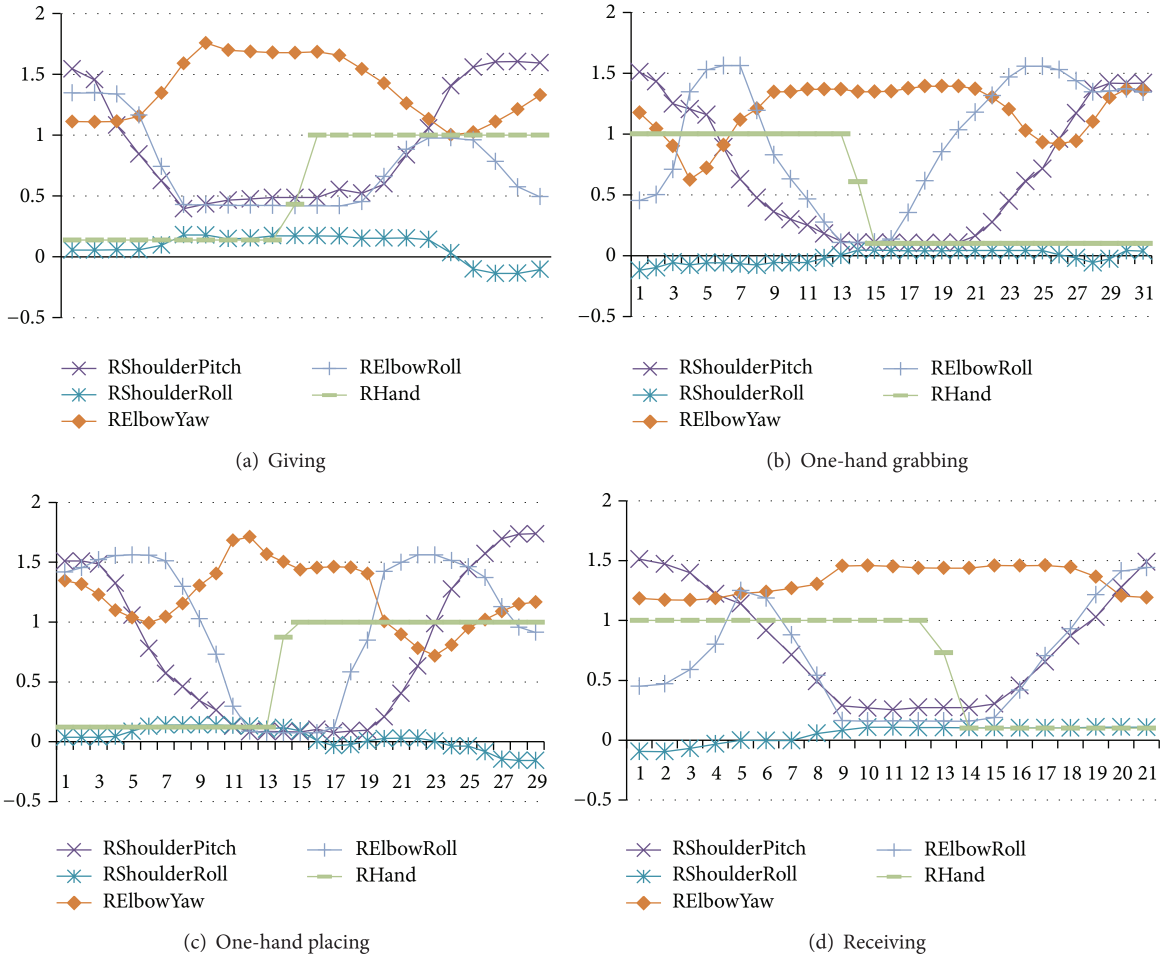
(i) a virtual human sleeps,

(ii) the human wakes up on a bed,

(iii) the human walks to a couch,

(iv) the human sits on the couch for a while,

(v) the human stands up on the couch,



(a) Giving

(b) One-hand grabbing

(c) One-hand placing

(d) Receiving

Figure 8: Four motor primitives produced for a robot.

(vi) the human walks to a newspaper,

(vii) the human picks up the newspaper, and

(viii) the human reads the newspaper.

(b) Scenario where a virtual robot provides services is as follows:

(i) a virtual human sleeps,

(ii) the human wakes up on a bed,

(iii) the human walks to a couch,

(iv) while the human sits on the couch:

(1) a virtual robot walks to a newspaper, and

(2) picks up the newspaper.

(v) when the human stands up on the couch:

(1) the robot walks to a virtual human, and

(2) gives the newspaper.

(vi) the human receives the newspaper, and

(vii) the human reads the newspaper.

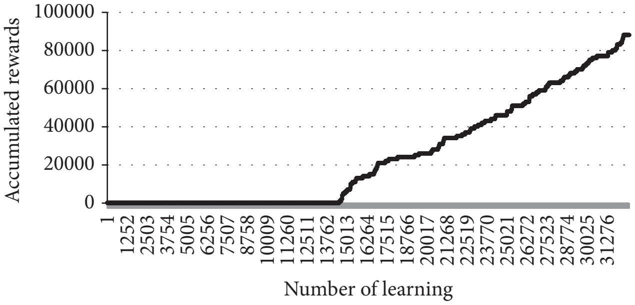


Figure 9: A virtual robot delivers a newspaper to a virtual human.

Figure 9 shows the accumulated rewards according to the increase in the amount of interaction learning. After 14,000, the robot started to learn the interaction. The previous list (b) shows the changed scenario by the virtual robot based on the result of the interaction after the interaction learning. If a virtual human lived alone, the virtual human walked to the newspaper and picked it up for itself. However, if a virtual robot was present, the virtual robot walked to the newspaper and picked it up, then walked to the virtual human, and gave it the newspaper.

5. Conclusion

In this paper, we developed an approach to virtual pervasive sensing environment-based interaction learning where the operators taught motor primitives to a real robot by manipulating its arms directly. The learned motor primitives were utilized by a virtual robot and executed to learn interactions with a human. The operators defined the motor primitives using manipulations, so various different types of motor primitives could be defined intuitively, which overcame the problems of previous approaches.

The virtual human and the virtual robot used in our proposed method and Q-learning are suitable for single agent-based learning algorithms, so it is necessary to improve our proposed method by applying multi-agent-based Q-learning. A method is also required to allow a virtual robot to provide services to multiple virtual humans. Finally, an approach will be developed to facilitate the application of the learned interaction results to a real robot.

Acknowledgments

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0011266). And this work was also supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012R1A1A2009148).

References

[1] T. Teraoka, “Organization and exploration of heterogeneous personal data collected in daily life,” *Human-Centric Computing and Information Sciences*, vol. 2, no. 1, pp. 1–15, 2012.

[2] M. Lim and Y. Lee, “A simulation model of object movement for evaluating the communication load in networked virtual environments,” *Journal of Information Processing Systems*, vol. 9, no. 3, pp. 489–498, 2013.

[3] H. T. Panduranga, S. K. Naveen Kumar, and H. S. Sharath Kumar, “Hardware software co-simulation of the multiple image encryption technique using the xilinx system generator,” *Journal of Information Processing Systems*, vol. 9, no. 3, p. 499, 2013.

[4] Y. Sung and K. Cho, “Collaborative programming by demonstration in a virtual environment,” *IEEE Intelligent Systems*, vol. 27, no. 2, pp. 14–17, 2012.

[5] S. Ra, G. Park, C. H. Kim, and B.-J. You, “PCA-based genetic operator for evolving movements of humanoid robot,” in *Proceedings of the IEEE Congress on Evolutionary Computation (CEC ’08)*, pp. 1219–1225, Hong Kong, China, June 2008.

[6] G. Park, S. Ra, C. Kim, and J.-B. Song, “Imitation learning of robot movement using evolutionary algorithm,” in *Proceedings of the 17th World Congress, International Federation of Automatic Control (IFAC ’08)*, pp. 730–735, Seoul, Republic of Korea, July 2008.

[7] S. Calinon, F. Guenter, and A. Billard, “On learning, representing, and generalizing a task in a humanoid robot,” *IEEE Transactions on Systems, Man, and Cybernetics B*, vol. 37, no. 2, pp. 286–298, 2007.

[8] N. Koenig and M. J. Matarić, “Behavior-based segmentation of demonstrated task,” in *Proceedings of International Conference on Development and Learning (ICDL ’06)*, 2006.

[9] M. N. Nicolescu and M. J. Matarić, “Natural methods for robot task learning: instructive demonstrations, generalization and practice,” in *Proceedings of the 2nd International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS ’03)*, pp. 241–248, Melbourne, Australia, July 2003.

[10] S. Calinon and A. Billard, “A probabilistic programming by demonstration framework handling constraints in joint space and task space,” in *Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS ’08)*, pp. 367–372, Nice, France, September 2008.

[11] M. N. Nicolescu and M. J. Matarić, “Extending behavior-based systems capabilities using an abstract behavior representation,” in *Proceedings of the AAAI Fall Symposium on Parallel Congnition*, pp. 27–34, 2000.

[12] M. J. Matarić, “Sensory-motor primitives as a basis for imitation: linking perception to action and biology to robotics,” in *Imitation in Animals and Artifacts*, pp. 391–422, MIT Press, 2000.

[13] Y. Sung and K. Cho, “A method for learning macro-actions for virtual characters using programming by demonstration and reinforcement learning,” *Journal of Information Processing Systems*, vol. 8, no. 3, pp. 409–420, 2012.

[14] C. J. C. H. Watkins and P. Dayan, “Q-learning,” *Machine Learning*, vol. 8, no. 3-4, pp. 279–292, 1992.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 829721, 9 pages
http://dx.doi.org/10.1155/2013/829721

Research Article

Privacy Protection Based Secure Data Transaction Protocol for Smart Sensor Meter in Smart Grid

Woong Go,[1] SeulKi Choi,[1] and Jin Kwak[2]

[1] *ISAA Lab, Department of Information Security Engineering, Soonchunhyang University, Asan, Chungchungnam-do 336-745, Republic of Korea*
[2] *Department of Information Security Engineering, Soonchunhyang University, Asan, Chungchungnam-do 336-745, Republic of Korea*

Correspondence should be addressed to Jin Kwak; jkwak@sch.ac.kr

Received 16 August 2013; Accepted 1 October 2013

Academic Editor: James J. Park

A smart grid is a data communications network integrated with an electrical grid that collects and analyzes near-real-time data on power transmission, distribution, and consumption. Currently, smart grid systems are considered to be necessary for improving the monitoring and control of a power distribution infrastructure. Using distributed measurement architecture, it is possible to gather information about the smart grid status for monitoring and controlling the overall infrastructure, including remote units. This architecture can control the use of electricity. In particular, users can monitor and regulate the electricity consumption of each home appliance in real time. Likewise, power companies can monitor and control electricity consumption for stabilizing electricity supply. However, serious problems can arise in case of data leakage. For example, if malicious attackers can sniff and analyze data, they can obtain the usage pattern of a house and ascertain when it is empty. They could then burgle the house. We propose a privacy-enhanced secure data transaction protocol that can protect private data by encrypting them. The encrypted data include the user's ID, home appliance serial number, and electricity consumption. Thus, attackers cannot obtain important data from the encrypted data. In addition, unauthorized power companies cannot access this information too.

1. Introduction

Recently, environmental issues such as global warming have become more serious because of industrial emissions. Many studies on low-carbon green growth are being carried out around the world to address them. The objective of aiming for low-carbon green growth is the abatement of carbon dioxide emissions and the efficient use of environmentally friendly resources. Thus, many researchers are studying application methods for these problems in various industries. In particular, interest in the use of smart grids for the effective use of electricity is increasing [1, 2].

A smart grid is a digitally enabled electrical grid that gathers, distributes, and acts on information about the behavior of all participants (suppliers and consumers) in order to improve the efficiency, reliability, economics, and sustainability of electricity services [3].

A key feature of smart grids is their ability to transmit information between the user and the electricity company in real time. In other words, users can check the electricity consumption of home appliances in real time, and electricity companies can generate only the electricity they need by analyzing usage patterns. The control of electricity production can help reduce carbon dioxide emissions. Interaction between users and power companies requires many types of sensitive information, such as user and home appliance information and smart sensor meter information. This information should be transmitted securely [4, 5]. Otherwise, a malicious attacker could gather data on the electricity consumption of home appliances in order to determine a user's routine and could plan a burglary when no one is at home.

We propose a privacy protection-based data transaction protocol for smart sensor meter in a smart grid. This protocol has two phases: a transmission phase and a check phase.

The remainder of this paper is organized as follows. In Section 2, we briefly provide basic information about smart grids. In Section 3, we discuss problems regarding

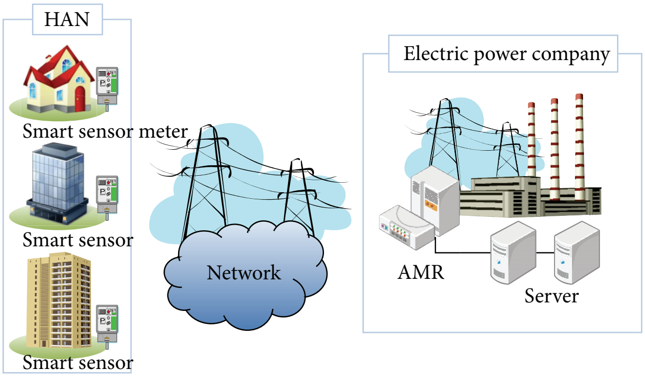


Figure 1: Smart grid system.

the security of private information in smart grids, while in Section 4, we describe our proposed protocol. We present an analysis of the proposed protocol in Section 5, and finally, we summarize our research in Section 6.

2. Related Work

2.1. Smart Grid. A smart grid is a digitally enabled electrical grid that gathers, distributes, and acts on information about the behavior of all participants (suppliers and consumers) in order to improve the efficiency, reliability, economics, and sustainability of electricity services (see Figure 1) [1].

A smart grid communication network will comprise several different subsystems—it is truly a network of networks. These networks include a supervisory control and data acquisition (SCADA) system; a land mobile radio (LMR) system; cellular, microwave, fiber optic, dedicated, or switched wirelines; RS-232/RS-485 serial links; wired and wireless local area networks (LAN), and so on [6, 7].

2.1.1. SCADA. An important component required for the monitoring and control of a substation is the SCADA system. It is utilized for distribution automation (DA) and computerized remote control of medium voltage (MV) substations and power grids, and it helps electricity utilities increase the reliability of power supply and reduce operating and maintenance costs. In the past, sectionalizer switchgear, ring main units, reclosers, and capacitor banks were designed for local operation with limited remote control capability. Today, using a SCADA system over reliable wireless communication links, remote terminal units (RTUs) provide powerful integrated solutions for upgrading remotely installed electrical equipment. In a Distribution Management System (DMS), RTUs seamlessly interface via a SCADA system with a wide range of high-performance control centers supplied by leading vendors worldwide. Connection to these Enterprise Management Systems (EMS) and DA/DMS control centers is typically provided via a high-performance IP Gateway or similar nodes [2, 8].

2.1.2. Wireless Networks. Different areas of the smart grid network require different wireless networking solutions. Advanced metering infrastructure (AMI) solutions can be meshed or point-to-point, with local coverage or long-range communication. Options for backhaul solutions are fiber, wireless broadband, or broadband over powerline, to name a few. Workforce mobility solutions include WiMax, WLAN, Cellular, and LMR, depending on the reliability, throughput, and coverage desired by the utility. Wireless communication solutions can be either licensed or unlicensed, again depending on the needs of the utility. For achieving the highest reliability, a licensed solution should be chosen. Each of the above options has advantages and disadvantages, but what is consistently true of all of them is the necessity of a scalable security solution [2, 9].

Table 1: Notation of Ren et al.'s scheme.

Notation	Description
UN	User name
SM	Smart meter
SGCC	Smart grid control center
$\mathrm{TTP}_{\mathrm{PubK}}$	Public key of TTP
V	Value of automatic meter readings
MK	Preloaded master key
SIK	Session integrity key
AID	Anonymous ID
TTP	Trusted third party
USR	User
$\mathrm{TTP}_{\mathrm{PriK}}$	Private key of TTP
LocID	Location ID
SEK	Session encryption key
$\|$	Concatenation

2.1.3. Security. Smart grid deployments must meet stringent security requirements. Strong authentication is necessary for all users and devices that may affect the operation of the grid. With the large number of users and devices affected, scalable key and trust management systems, customized to the specific needs of the energy service provider, are essential.

The deployment and operation of large, secure network communication systems over many years has taught us that the effort required to provision symmetric keys into thousands of devices can be too expensive or insecure. The development of key and trust management systems for large network deployments is required; these systems can be adopted from other industries, for example, LMR systems and Association of Public-Safety Communications Officials (APCO) radio systems. Several APCO-deployed systems provide statewide wireless coverage, with tens of thousands of secure devices. Trust management systems based on public key infrastructure (PKI) technology could be specifically customized for smart grid operators, easing the burden of providing security that adheres to accepted and guidelines that are known to be secure [10, 11].

2.2. Review of Ren et al.'s Scheme. In this section, we present an analysis of Ren et al.'s scheme [12] (see Table 1). These

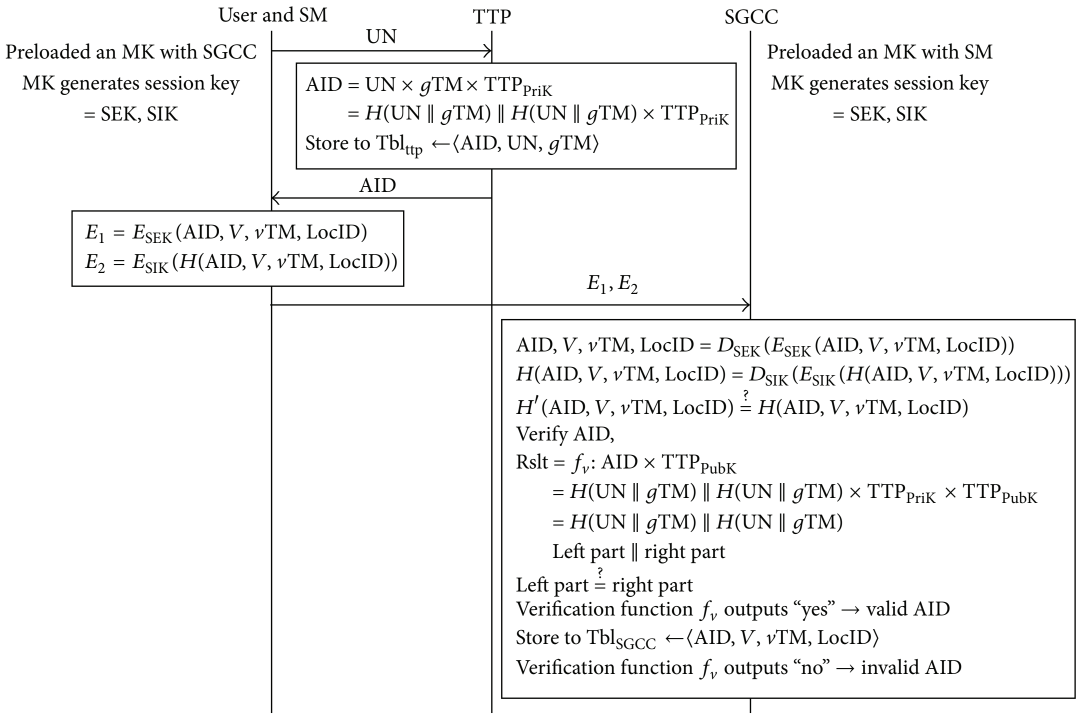

User and SM
TTP
SGCC
UN
Preloaded an MK with SGCC
MK generates session key
= SEK, SIK
AID = UN × gTM × TTP_PriK
= H(UN ‖ gTM) ‖ H(UN ‖ gTM) × TTP_PriK
Store to Tbl_ttp ←⟨AID, UN, gTM⟩
Preloaded an MK with SM
MK generates session key
= SEK, SIK
AID
E_1 = E_SEK(AID, V, vTM, LocID)
E_2 = E_SIK(H(AID, V, vTM, LocID))
E_1, E_2
AID, V, vTM, LocID = D_SEK(E_SEK(AID, V, vTM, LocID))
H(AID, V, vTM, LocID) = D_SIK(E_SIK(H(AID, V, vTM, LocID)))
H'(AID, V, vTM, LocID) ≟ H(AID, V, vTM, LocID)
Verify AID,
Rslt = f_v: AID × TTP_PubK
= H(UN ‖ gTM) ‖ H(UN ‖ gTM) × TTP_PriK × TTP_PubK
= H(UN ‖ gTM) ‖ H(UN ‖ gTM)
Left part ‖ right part
Left part ≟ right part
Verification function f_v outputs "yes" → valid AID
Store to Tbl_SGCC ←⟨AID, V, vTM, LocID⟩
Verification function f_v outputs "no" → invalid AID

Figure 2: Protocol of Ren et al.'s scheme.

researchers proposed lightweight privacy-aware yet accountable secure communication scheme (PASS) between SM sensors and a Smart Grid Control Center (SGCC). PASS has five components: AID generation, attaching AID, uploading data, AID verification, and AID traceability.

(1) AID generation: the customer presents a UN to a TTP. The TTP generates the corresponding AID by using the generation function:

$$\left(f_g : \mathrm{UN} \times g\mathrm{TM} \times \mathrm{TTP}_{\mathrm{PriK}} \longrightarrow \mathrm{AID}\right), \quad (1)$$

where gTM is the time-stamp used for the AID generation. After the AID generation, the TTP returns the AID to the customer and stores an item in a table called $\mathrm{Tbl}_{\mathrm{ttp}}$, which stores tuples $\langle \mathrm{AID}, \mathrm{UN}, \text{ and } g\mathrm{TM}\rangle$.

(2) Attaching AID: the customer inputs the obtained AID into a SM at his/her residence.

(3) Data uploading: the customer uploads data messages E_1 and E_2 (defined below). The SGCC creates a table called $\mathrm{Tbl}_{\mathrm{sgcc}}$, in which tuples $\langle \mathrm{AID}, V, v\mathrm{TM}$, and LocID⟩ are stored. vTM is the time-stamp for uploading the data.

Consider

$$E_1 = E_{\mathrm{SEK}}(\mathrm{AID}, V, v\mathrm{TM}, \mathrm{LocID}),$$
$$E_2 = E_{\mathrm{SIK}}(H(\mathrm{AID}, V, v\mathrm{TM}, \mathrm{LocID})). \quad (2)$$

(4) AID verification: the SGCC decrypts the uploaded data and examines whether the AID is valid and whether it has been forged by a malicious user. The verification function is $f_g : \mathrm{AID} \times \mathrm{TTP}_{\mathrm{PubK}} \rightarrow$ Rslt. If Rslt has a "given" *a priori* pattern; that is, its left half and right half are identical, the verification function outputs "Yes," which means the AID is valid. Otherwise, the output is "No," which means the AID is invalid.

(5) AID traceability: the SGCC can trace back to AID's LocID. However, it cannot recover the UN of the AID by itself. Only the TTP can recover the AID. Given the AID, TTP fetches $\langle \mathrm{UN}, g\mathrm{TM}\rangle$ from $\mathrm{Tbl}_{\mathrm{ttp}} = \langle \mathrm{AID}, \mathrm{UN}, g\mathrm{TM}\rangle$ and checks whether the following equation is satisfied:

$$\mathrm{AID} \times \mathrm{TTP}_{\mathrm{PubK}} = H(\mathrm{UN} \parallel g\mathrm{TM}) \parallel H(\mathrm{UN} \parallel g\mathrm{TM}). \quad (3)$$

If it is satisfied, the TTP can confirm that the "opened" TTP is the UN, and such a UN is not repudiated.

3. Security Problems in Smart Grid Systems

3.1. Privacy Problem. The security issues in smart grid have been widely discussed in recent years. The primary security issue is privacy because information transmitted over a smart grid contains electricity usage patterns of home appliances. This information could indicate not only the amount of energy consumed by each user, but also when they are at home, at work, or traveling [13]. Furthermore, it might be

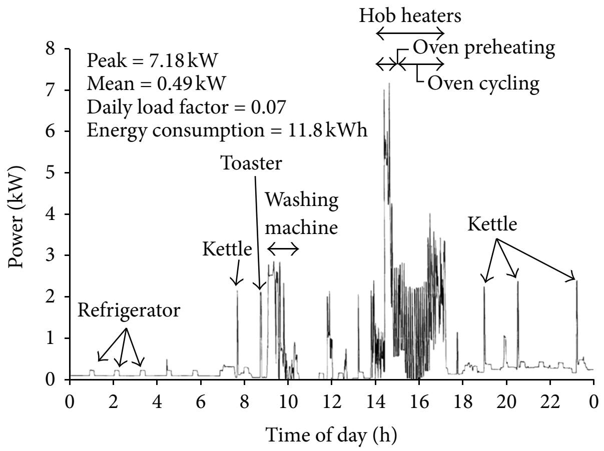


Figure 3: Household electricity demand profile recorded on a one minute time base.

possible to infer what types of home appliances are present by compromising users' home area networks. The present smart grid system gathers user information in order to check and calculate the amount of electricity consumption.

Thus, if a criminal or malicious attacker can determine when a user is not at home, they may break into his/her house at such a time. Thus, energy-related information could support burglars or provide business intelligence to competitors [14].

3.2. Electricity Consumption Loss. According to the report Smart Metering & Privacy: Existing Law and Competing Policies, researchers at MIT have developed a nonintrusive appliance load monitor (NALM) [15, 16].

If NALMs could be incorporated in the existing metering infrastructure to allow for real-time logging of electricity consumption, information concerning appliance use may be reconstructed from the overall load data; thereby removing the need to intrude residential space and install new equipment in the house. NALMs were designed as research tools, and they were set up to monitor only a small number of customers in order to facilitate load forecasting and management (see Figure 3). However, smart grids allow the collection and communication of highly detailed electricity usage information, in much the same way as the NALM [16]. Thus, the problem of privacy within a smart grid is the main concern.

3.3. Modification of Electricity Consumption. Existing power companies require only power lines to connect a house to a power source. Thus, individual customers cannot access the electrical grid through the Internet. This feature provides security from the risks associated with the Internet. However, smart grid architecture connects a house (smart sensor network) to not only an electrical grid but also the Internet. This means that a smart grid is exposed to additional risks, one of which is illegal modification of electricity consumption [17].

Table 2: Notation used for the proposed.

Notation	Description
PC	Power company
HA	Home appliance
$\mathrm{SN}_{\mathrm{HA}}$	Home appliance serial number
$\mathrm{SN}_{\mathrm{list}}$	List of smart sensor meter serial number
Kus	User's password as an encryption/decryption key (between user and smart sensor meter)
r	Random nonce
$H(\cdot)$	Hash function
E_n	Encrypted data
SM	Smart sensor meter
ID_U	User ID
$\mathrm{SN}_{\mathrm{SM}}$	Smart sensor meter serial number
EC	Electricity consumption
Ksp	Encryption/decryption key (between smart sensor meter and power company)
PRNG$(\cdot)$	Pseudorandom number generator
H_n	Hashed data

In a smart grid, users and electricity companies communicate with each other through a wired or wireless network. Information about electricity consumption and the user is transmitted via this network. Thus, if a malicious attacker modifies a user's electricity consumption, the user might have to pay a lot of money for electricity that has not actually been used. In addition, unscrupulous users could modify their electricity consumption in order to profit by paying less. There is a high likelihood of such instances [18].

4. Proposed Protocol

4.1. Basic Structure. In this section, we propose a data transaction protocol for privacy protection (see Figure 2). To solve the problems faced in existing smart grid systems, our scheme creates hash data from the information on home appliances. Thus, electricity companies or attackers cannot obtain any valuable information.

This scheme has two steps: a transmission phase and a check phase. In the former, the user sends encrypted information, such as electricity consumption and serial numbers of home appliances, to the power company and the power company stores this information. In the check phase, the user requests his/her electricity consumption from the power company and can check the power consumption of each home appliance. Figure 4 shows an overview of the proposed scheme.

4.2. Overview of Entire Scheme. Table 2 describes the notation used for discussing the proposed scheme. The notation is used throughout this paper.

4.3. Registration Phase. In the registration phase, the user inputs his/her ID (ID_U) and password (Kus) by using a smart

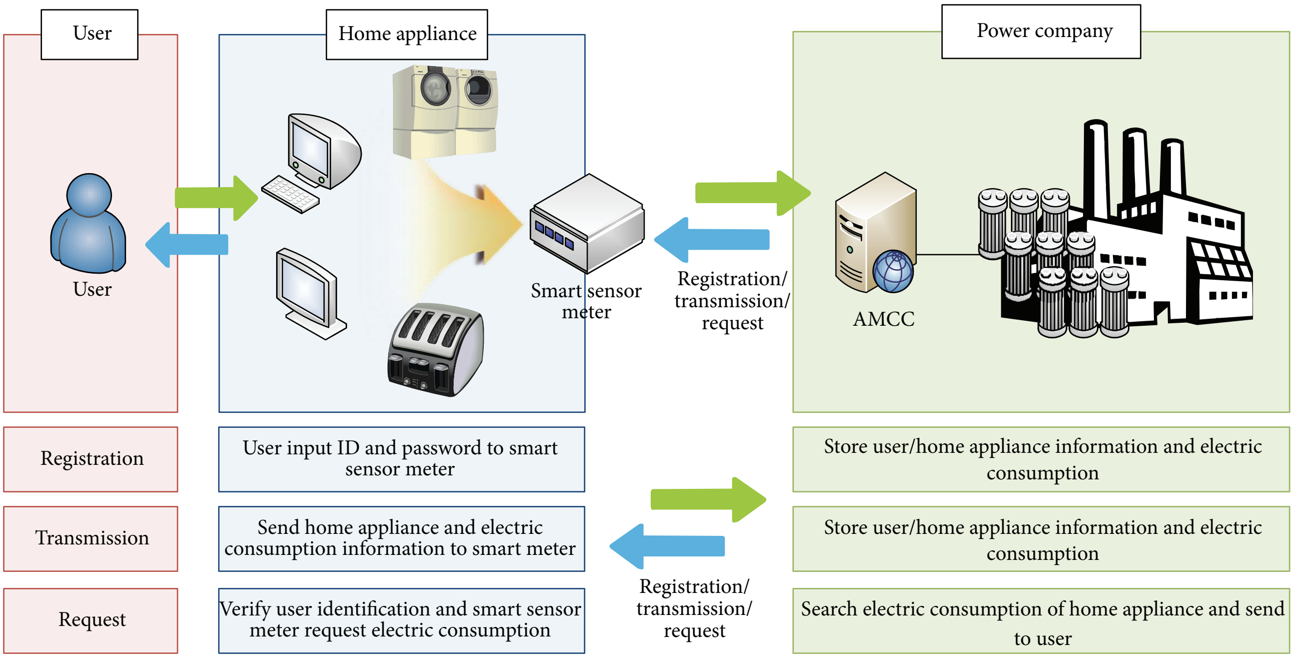

User
Home appliance
Power company
User
Smart sensor meter
Registration/ transmission/ request
AMCC
Registration
User input ID and password to smart sensor meter
Store user/home appliance information and electric consumption
Transmission
Send home appliance and electric consumption information to smart meter
Store user/home appliance information and electric consumption
Request
Verify user identification and smart sensor meter request electric consumption
Search electric consumption of home appliance and send to user
Registration/ transmission/ request

FIGURE 4: Overview of the proposed scheme.

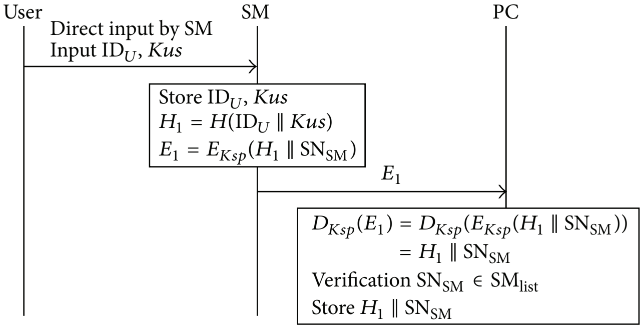

User
SM
PC
Direct input by SM
Input ID_U, Kus
Store ID_U, Kus
$H_1 = H(\mathrm{ID}_U \parallel Kus)$
$E_1 = E_{Ksp}(H_1 \parallel \mathrm{SN}_{\mathrm{SM}})$
E_1
$D_{Ksp}(E_1) = D_{Ksp}(E_{Ksp}(H_1 \parallel \mathrm{SN}_{\mathrm{SM}}))$
$= H_1 \parallel \mathrm{SN}_{\mathrm{SM}}$
Verification $\mathrm{SN}_{\mathrm{SM}} \in \mathrm{SM}_{\mathrm{list}}$
Store $H_1 \parallel \mathrm{SN}_{\mathrm{SM}}$

FIGURE 5: Registration phase.

sensor meter (SM) display. The SM display is the interface between the user and the SM (see Figure 5).

The SM sends these information to the power company (PC), and the PC stores the information. The information is used as the user's identity and encryption/decryption key between the user and SM. Moreover, the PC does not have knowledge of these information because the ID_U and Kus are hashed before communication.

When the user moves into a new house, he/she should register his/her ID_U and Kus with the SM

$$\begin{gathered}\text{User} \longrightarrow \text{Smart Meter} \\ \text{Input } \mathrm{ID}_U, Kus.\end{gathered} \tag{4}$$

The SM stores the ID_U and Kus and creates hash data (H_1) from these information. This hash data are used as the user identification and for extracting electricity consumption (EC) from other data ($H_1 \oplus \mathrm{EC}$). Then, the hash data (H_1) and SM serial number ($\mathrm{SN}_{\mathrm{SM}}$) are encrypted ($E_1$) with an encryption/decryption key (Ksp). The SM sends the encrypted data the PC

$$\begin{aligned}&\text{Smart Meter} \\ &\quad \text{Store } \mathrm{ID}_U, Kus, \\ &\quad H_1 = H(\mathrm{ID}_U \parallel Kus), \\ &\quad E_1 = E_{Ksp}(H_1 \parallel \mathrm{SN}_{\mathrm{SM}}), \\ &\text{Smart Meter} \longrightarrow \text{Power Company} \\ &\quad E_1 = E_{Ksp}(H_1 \parallel \mathrm{SN}_{\mathrm{SM}}).\end{aligned} \tag{5}$$

The PC decrypts the hash data (H_1) and SM serial number ($\mathrm{SN}_{\mathrm{SM}}$) obtained from E_1. Then, the SM verifies the SM serial number ($\mathrm{SN}_{\mathrm{SM}}$) by checking if it exists in the list of SMs ($\mathrm{SN}_{\mathrm{list}}$). If the SM serial number is valid, the PC stores these information ($H_1 \parallel \mathrm{SN}_{\mathrm{SM}}$)

$$\begin{aligned}&\text{Power Company} \\ &\quad D_{Ksp}(E_1) = D_{Ksp}(E_{Ksp}(H_1 \parallel \mathrm{SN}_{\mathrm{SM}})) \\ &\qquad\qquad = H_1 \parallel \mathrm{SN}_{\mathrm{SM}}, \\ &\quad \text{Verification } \mathrm{SN}_{\mathrm{SM}} \in \mathrm{SM}_{\mathrm{list}}, \\ &\quad \text{Store } H_1 \parallel \mathrm{SN}_{\mathrm{SM}}.\end{aligned} \tag{6}$$

4.4. Transmission Phase. In the transmission phase, information on home appliances (HA) and electricity consumption (EC) is transmitted securely (see Figure 6). Thus, third parties and the PC do not have any knowledge of this information. In addition, the PC only knows the electricity consumption.

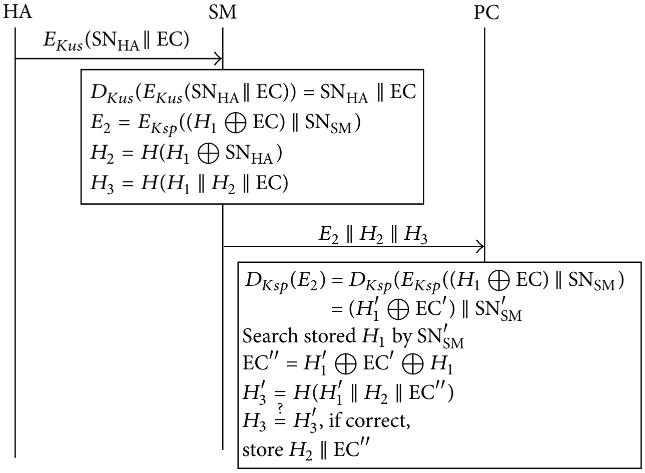

HA
SM
PC
$E_{Kus}(\mathrm{SN_{HA}} \| \mathrm{EC})$
$D_{Kus}(E_{Kus}(\mathrm{SN_{HA}} \| \mathrm{EC})) = \mathrm{SN_{HA}} \| \mathrm{EC}$
$E_2 = E_{Ksp}((H_1 \oplus \mathrm{EC}) \| \mathrm{SN_{SM}})$
$H_2 = H(H_1 \oplus \mathrm{SN_{HA}})$
$H_3 = H(H_1 \| H_2 \| \mathrm{EC})$
$E_2 \| H_2 \| H_3$
$D_{Ksp}(E_2) = D_{Ksp}(E_{Ksp}((H_1 \oplus \mathrm{EC}) \| \mathrm{SN_{SM}})$
$= (H_1' \oplus \mathrm{EC}') \| \mathrm{SN}_{\mathrm{SM}}'$
Search stored H_1 by $\mathrm{SN}_{\mathrm{SM}}'$
$\mathrm{EC}'' = H_1' \oplus \mathrm{EC}' \oplus H_1$
$H_3' = H(H_1' \| H_2 \| \mathrm{EC}'')$
$H_3 \overset{?}{=} H_3'$, if correct,
store $H_2 \| \mathrm{EC}''$

FIGURE 6: Transmission phase.

Thus, the user's private information, such as daily routine or the home appliances possessed by him/her, is protected.

Each home appliance sends the home appliance serial number ($\mathrm{SN_{HA}}$) and electricity consumption (EC), encrypted with *Kus*, to the SM

$$\text{Home Appliance} \longrightarrow \text{Smart Meter}$$
$$E_{Kus}(\mathrm{SN_{HA}} \| \mathrm{EC}). \tag{7}$$

The SM decrypts the home appliance serial number ($\mathrm{SN_{HA}}$) and electricity consumption (EC) before encrypting the hash data (H_1), electricity consumption (EC), and SM serial number ($\mathrm{SN_{SM}}$) with *Ksp* and creating hash data (H_2) from H_1 and the HA serial number ($\mathrm{SN_{HA}}$). Then, the two sets of hash data (H_1, H_2) and electricity consumption (EC) are hashed (H_3). H_3 is used for performing an integrity check. The SM then sends encrypted data (E_2) with the two sets of hash data (H_2, H_3) to the PC

$$\begin{aligned}
&\text{Smart Meter}\\
&\quad D_{Kus}(E_{Kus}(\mathrm{SN_{HA}} \| \mathrm{EC})) = \mathrm{SN_{HA}} \| \mathrm{EC},\\
&\quad E_2 = E_{Ksp}((H_1 \oplus \mathrm{EC}) \| \mathrm{SN_{SM}}),\\
&\quad H_2 = H(H_1 \oplus \mathrm{SN_{HA}}),\\
&\quad H_3 = H(H_1 \| H_2 \| \mathrm{EC}),\\
&\text{Smart Meter} \longrightarrow \text{Power Company}\\
&\quad E_2 \| H_2 \| H_3.
\end{aligned} \tag{8}$$

The PC obtains $H_1' \oplus \mathrm{EC}'$ and the SM serial number ($\mathrm{SN}_{\mathrm{SM}}'$) via the encrypted information (E_2). Next, the PC searches the stored H_1 by using $\mathrm{SN}_{\mathrm{SM}}'$ and extracts the electricity consumption (EC'') from $H_1' \oplus \mathrm{EC}'$ by using the stored H_1. After the extraction is complete, the PC creates hash data (H_3') from H_1', H_2, and EC'' and makes a comparison between the received H_3 and H_3'. If the comparison shows that the hash data are identical, the EC is stored with the hashed information H_2

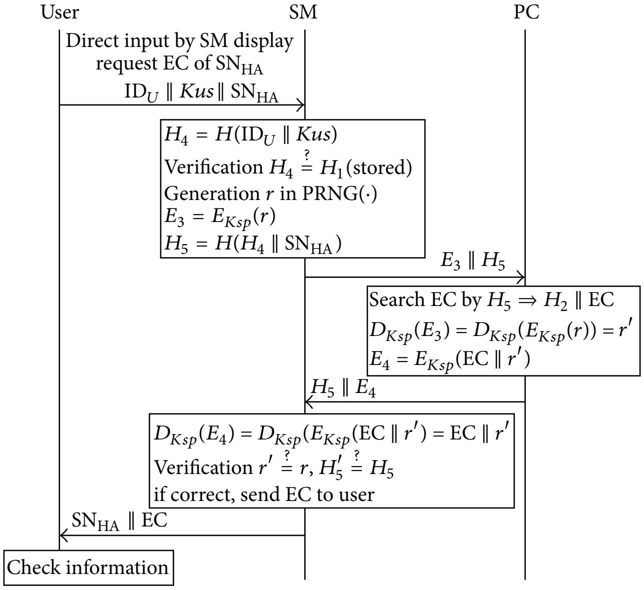

User
SM
PC
Direct input by SM display
request EC of $\mathrm{SN_{HA}}$
$\mathrm{ID}_U \| Kus \| \mathrm{SN_{HA}}$
$H_4 = H(\mathrm{ID}_U \| Kus)$
Verification $H_4 \overset{?}{=} H_1$(stored)
Generation r in PRNG(·)
$E_3 = E_{Ksp}(r)$
$H_5 = H(H_4 \| \mathrm{SN_{HA}})$
$E_3 \| H_5$
Search EC by $H_5 \Rightarrow H_2 \| \mathrm{EC}$
$D_{Ksp}(E_3) = D_{Ksp}(E_{Ksp}(r)) = r'$
$E_4 = E_{Ksp}(\mathrm{EC} \| r')$
$H_5 \| E_4$
$D_{Ksp}(E_4) = D_{Ksp}(E_{Ksp}(\mathrm{EC} \| r') = \mathrm{EC} \| r'$
Verification $r' \overset{?}{=} r$, $H_5' \overset{?}{=} H_5$
if correct, send EC to user
$\mathrm{SN_{HA}} \| \mathrm{EC}$
Check information

FIGURE 7: Check phase.

$$\begin{aligned}
&\text{Power Company}\\
&\quad D_{Ksp}(E_2) = D_{Ksp}\left(E_{Ksp}((H_1 \oplus \mathrm{EC}) \| \mathrm{SN_{SM}})\right)\\
&\qquad\qquad = \left(H_1' \oplus \mathrm{EC}'\right) \| \mathrm{SN}_{\mathrm{SM}}',\\
&\quad \text{Search sorted } H_1 \text{ using } \mathrm{SN}_{\mathrm{SM}}'\\
&\quad \mathrm{EC}'' = H_1' \oplus \mathrm{EC}' \oplus H_1,\\
&\quad \text{Comparison } H_3 \overset{?}{=} H_3',\\
&\quad \text{If correct, store } H_2 \| \mathrm{EC}''.
\end{aligned} \tag{9}$$

H_2 is used as an index of the home appliance. In addition, when a user requests the electricity consumption of any home appliance, the PC can search for it using H_2 obtained from the user.

4.5. Check Phase. In this phase, the user requests the electricity consumption of one or more home appliances from the PC (see Figure 7).

First, the user inputs the ID_U and *Kus* along with the serial number ($\mathrm{SN_{HA}}$) of the home appliance whose electricity consumption is required

$$\text{User} \longrightarrow \text{Smart Meter}$$
$$U_{\mathrm{ID}} \| Kus \| \mathrm{SN_{HA}}. \tag{10}$$

To verify that the request has come from an authorized user, the SM creates hash data (H_4) by using the data input by the user ($U_{\mathrm{ID}} \parallel Kus$). It then verifies the user from the information stored in the registration phase. After user verification, the SM generates random nonce (r) by using the PRNG(·) function and encrypts it with Ksp. The purpose of generating r is for facilitating the verification of the electricity consumption by the user when he/she receives information from the PC. Hash data (H_5) are generated in order to search stored electricity consumption values. Lastly, the SM sends encryption data and hash data ($E_3 \parallel H_5$) to the PC

$$\begin{aligned} &\text{Smart Meter} \\ &\quad H_4 = H\left(\mathrm{ID}_U \parallel Kus\right), \\ &\quad \text{Verification } H_4 \overset{?}{=} H_1 \text{ (stored)}, \\ &\quad \text{Generation of } r \text{ in PRNG}(\cdot), \\ &\quad E_3 = E_{Ksp}(r), \\ &\quad H_5 = H\left(H_4 \parallel \mathrm{SH}_{\mathrm{HA}}\right), \\ &\text{Smart Meter} \longrightarrow \text{Power Company} \\ &E_3 \parallel H_5. \end{aligned} \tag{11}$$

H_5 allows the PC to retrieve the EC of the home appliance from its database. Further, random nonce (r') is decrypted from the received information (E_3). Subsequently, the PC encrypts the EC and r' with Ksp. All computed data ($H_5 \parallel E_4$) are sent to the SM

$$\begin{aligned} &\text{Power Company} \\ &\quad \text{Search EC by } H_5 \Longrightarrow H_2 \parallel \mathrm{EC}, \\ &\quad D_{Ksp}\left(E_3\right) = D_{Ksp}\left(E_{Ksp}(r)\right) = r', \\ &\quad E_4 = E_{Ksp}\left(\mathrm{EC} \parallel r'\right), \\ &\text{Power Company} \longrightarrow \text{Smart Meter} \\ &\quad H_5 \parallel E_4. \end{aligned} \tag{12}$$

When $H_5 \parallel E_4$ are received, the SM decrypts the EC and r' and makes a comparison between the initial random nonce r and the decrypted random nonce (r'). If the random nonce comparison result is not correct, it means that E_4 has been modified. Thus, the SM discards the data. Similarly, H_5' should be compared with the initial hash data H_5. If these two comparisons indicate that the sent data are correct, the SM sends the requested electricity consumption (EC) with the home appliance serial number ($\mathrm{SN}_{\mathrm{HA}}$) to the user

$$\begin{aligned} &\text{Smart Meter} \\ &D_{Ksp}\left(E_4\right) = D_{Ksp}\left(E_{Ksp}\left(\mathrm{EC} \parallel r'\right)\right) = \mathrm{EC} \parallel r', \\ &\text{Verification } r \overset{?}{=} r',\ H_5 \overset{?}{=} H_5', \\ &\text{If correct, send EC to User.} \end{aligned} \tag{13}$$

Finally, the user can check the electricity consumption of his/her home appliances.

5. Analysis

5.1. Protection against Privacy Invasion. The proposed protocol protects against privacy invasion by using a user password (Kus) and an encryption/decryption key (Ksp). The user password is entered as a key between the home appliance and SM when the SM is first installed, and the encryption/decryption key is entered when the SM is manufactured. The target information necessary for privacy invasion is the user ID, home appliance serial number, and electricity consumption. To determine when the user is at home, at work, or traveling, a malicious attacker would need this information.

However, the protocol proposed in this paper uses encrypted data. This contains the home appliance serial number and electricity consumption ($E_{Kus}(\mathrm{SN}_{\mathrm{HA}} \parallel \mathrm{EC})$). If a malicious attacker eavesdrops on the encrypted information, they would need the user password (Kus) to decrypt it. Therefore, malicious attackers cannot decrypt this information as long as the user password is known only to the user.

5.2. Protection against Electricity Consumption Loss. The proposed protocol protects against data leakage by using a user password (Kus), an encryption/decryption key (Ksp), and random nonce (r). The target information is the home appliance serial number ($\mathrm{SN}_{\mathrm{HA}}$) and electricity consumption (EC). To determine when the user is at home, at work, or traveling, a malicious attacker would need this information.

In the transmission phase, we encrypt the home appliance serial number ($\mathrm{SN}_{\mathrm{HA}}$) and electricity consumption (EC) by using the user password (Kus). In addition, this electricity consumption and hash data (H_1) are computed using the exclusive-OR operation. Additionally, the PC encrypts the electricity consumption with a random nonce (r) using an encryption/decryption key (Ksp) in the check phase. The use of the exclusive-OR operation and random nonce makes it difficult to extract the electricity consumption. Therefore, any intercepted home appliance electricity consumption information is different from the real data.

5.3. Protection against Modification of Electricity Consumption. If a malicious attacker modifies the electricity consumption data of a home appliance, the user may have to pay more money because of the modification. On the other hand, if unscrupulous users modify their electricity consumption in order to profit, the PC may suffer significant losses. Thus, the proposed protocol uses two keys (Kus and Ksp) and a hash function ($H(\cdot)$) to protect against illegal modification. For example, if an attacker knows the encryption/decryption key (Ksp) and attempts to modify the electricity consumption in the transmission phase, the PC can detect this modified information.

Table 3: Analysis of computational cost.

	Computation	Proposed scheme	Ren et al. [12]
Registration	Asymmetric encryption	—	—
	Symmetric encryption	2Sym	—
	Hash function	1T (h)	—
Transmission (PASS)	Asymmetric encryption	—	2Asym
	Symmetric encryption	4Sym	4Sym
	Hash function	3T (h)	4T (h)
Request	Asymmetric encryption	—	—
	Symmetric encryption	3Sym	—
	Hash function	3T (h)	—

Consider

(i)

$$\begin{aligned} &E_2 = E_{Ksp}\left(\left(H_1 \oplus \mathrm{EC}\right) \parallel \mathrm{SN_{SM}}\right), \\ \mathrm{SM} \Longrightarrow\ &H_2 = H\left(H_1 \oplus \mathrm{SN_{HA}}\right), \quad H_3 = H\left(H_1 \parallel H_2 \parallel \mathrm{EC}\right), \\ &\text{Send } E_2 \parallel H_2 \parallel H_3 \text{ to PC.} \end{aligned} \tag{14}$$

(ii)

Attacker

$$\Longrightarrow \begin{aligned} &\text{Computation, } E_{2A} = E_{Ksp}\left(\left(H_{1A} \oplus \mathrm{EC}_A\right) \parallel \mathrm{SN_{SMA}}\right) \\ &\text{Send } \ E_{2A} \parallel H_2 \parallel H_3 \text{ to PC.} \end{aligned} \tag{15}$$

(iii) Attacker cannot create H_2 and H_3 because he/she does not know H_1.

(iv) The PC extracts electricity consumption using exclusive-OR operation.

(v) The PC computes new hashed data (H_3') and compares them with received hashed data (H_3)

$$\begin{aligned} &\mathrm{EC}_A = \left(H_{1A} \oplus \mathrm{EC}_A\right) \oplus H_1, \\ &H_{3A} = H\left(H_1 \parallel H_2 \parallel \mathrm{EC}_A\right), \qquad H_3 \overset{?}{=} H_{3A} \ \text{(incorrect)}. \end{aligned} \tag{16}$$

(vi) The comparison result shows that the received data is incorrect.

(vii) Therefore, the PC discards the information transmitted by the attacker.

5.4. Performance Analysis. In this section, we compare the performance of our proposed scheme with that of Ren et al.'s scheme. The proposed scheme has three phases: registration, transmission, and request. In contrast, Ren et al.'s scheme has only one phase, called PASS. PASS is similar to the transmission phase of the proposed scheme. Therefore, we compare PASS and the transmission phase.

Table 4: Analysis of communication cost.

	Proposed scheme	Ren et al. [12]
Registration	2	—
Transmission (PASS)	2	3
Request	4	—

Table 3 shows an analysis of the computational cost. The proposed scheme is computationally more efficient compared to Ren et al.'s scheme. Besides, in the former, asymmetric encryption is not used and the hash function is used less.

Table 4 shows an analysis of the communication cost. As can be seen, our proposed scheme needs two handshakes in the transmission phase. On the other hand, Ren et al.'s scheme needs three handshakes in PASS. Thus, our proposed scheme is more efficient with regard to the communication cost.

In order to compare the proposed scheme and Ren et al.'s scheme, we simplify the computational cost for carrying out a quantitative analysis. We assume that the computational cost of asymmetric encryption, symmetric encryption, and the hash function are 3, 2, and 1, respectively. Actually, asymmetric encryption involves higher computational cost compared to symmetric encryption and the hash function. Further, symmetric encryption involves higher computational cost compared to the hash function. Thus, the computational cost of the proposed scheme is 11 (4Sym + 3T (h) = 4 × 2 + 3 × 1 = 11), while that of Ren et al.'s scheme is 18 (2Asym + 4Sym + 4T (h) = 2 × 3 + 4 × 2 + 4 × 1 = 18).

Figure 8 shows the changes in the computational cost and communication cost with time. We calculate the costs for the case where data are transmitted at regular intervals. For example, if data are transmitted at 10 min intervals (144 = 1 day/10 min), the cost of the proposed scheme is 1584 (= 144 × 11), while that of Ren et al.'s scheme is 2592 (= 144 × 18).

6. Conclusion

In this paper, we have proposed a secure data transaction protocol for smart grids to protect private information. The proposed protocol has two phases: a transmission phase and a check phase. In the former, we encrypt the user ID, home appliance serial number, and electricity consumption to protect against attacks such as eavesdropping and modification. For the encryption, the user password, encryption/decryption key, and hash function are used. In the check phase, the user can request information about the electricity consumption of a home appliance. For this, he/she sends an encrypted user ID and home appliance serial number to the PC. And the SM generates a random nonce. The purpose of generating the random nonce is to protect electricity consumption data from illegal modification. Thus, the PC sends the desired electricity consumption and random nonce in an encrypted state. The above features provide security to the data transaction.

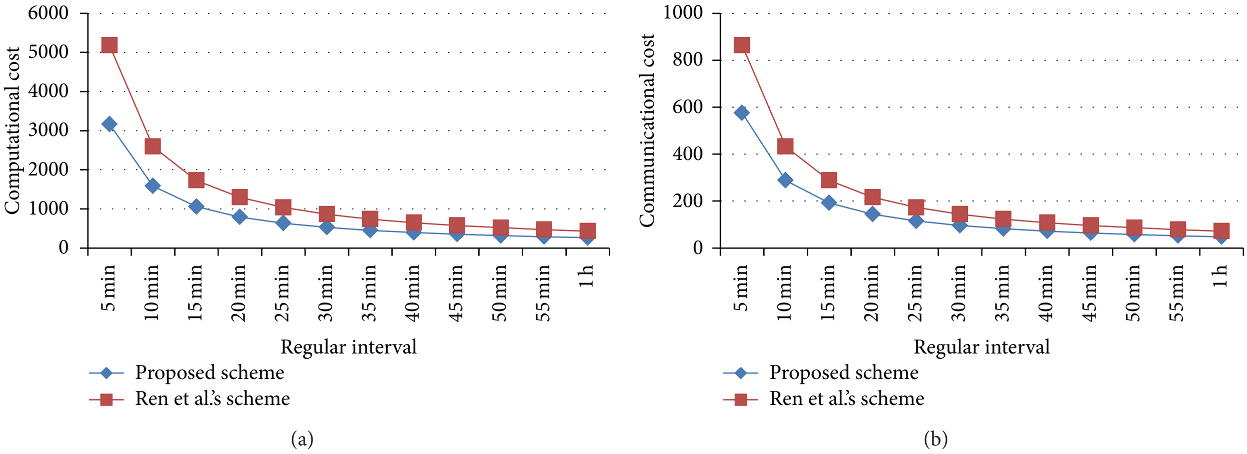


Figure 8: Changes in computational and communication cost for data transmission at regular intervals.

Conflict of Interests

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This research was supported by the Ministry of Knowledge Economy (MKE), Republic of Korea, under the Information Technology Research Center (ITRC) support program (NIPA-2012-H0301-12-3007) supervised by the National IT Industry Promotion Agency (NIPA). This work was supported by the Soonchunhyang University Research Fund.

References

[1] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, no. 15, pp. 3604–3629, 2011.

[2] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Proceedings of the Innovative Smart Grid Technologies*, January 2010.

[3] S. Adwitiya and K. L. Daya, "Performance evaluation of data aggregation for cluster-based wireless sensor network," *Human-Centric Computing and Information Sciences*, vol. 3, pp. 1–17, 2013.

[4] Y. Min, K. Yong-Ki, and C. Jae-Woo, "An energy-efficient routing protocol using message success rate in wireless sensor networks," *Journal of Covenvergence*, vol. 4, pp. 15–22, 2013.

[5] R. Sumathi and M. G. Srinivas, "A survey of QoS based routing protocols for wireless sensor networks," *Journal of Information Processing Systems*, no. 8, pp. 589–602, 2012.

[6] R. S. Tolentino and T.H. Kim, "Review: distributed system network architecture for securing SCADA system," *International Journal of Smart Home*, vol. 4, no. 1, pp. 13–22, 2010.

[7] U. Ahmad and H. S. Sajjad, "Evolution of communication technologies for smart grid applications," *Revewable and Sustainable Energy Revies*, vol. 19, pp. 191–199, 2013.

[8] K. Dong-Joo and P. Sunju, "A conceptual approach to data visualization for user interface design of smart grid operation tools," *International Journal of Energy, Information and Communications*, no. 1, pp. 64–76, 2010.

[9] A. Emilio, B. Raffaele, and C. Marco, "The role of communication systems in smart grids: architectures, technical solutions and research challenges," *Computer Communications*, 2013.

[10] K. Wu, T. Zhang, and W. Li, "Research and design of security defense model in power grid enterprise information system," in *Proceedings of the International Conference on Multimedia Technology (ICMT '10)*, October 2010.

[11] J. R. Rosslin and C. Min-kyu, "Assessment of the vulnerabilities of SCADA, control systems and critical infrastructure systems," *International Journal of Grid and Distributed Computing*, vol. 2, pp. 27–34, 2009.

[12] W. Ren, J. Song, Y. Yang, and Y. Ren, "Lightweight privacy-aware yet accountable secure scheme for SM-SGCC communications in smart grid," *Tsinghua Science and Technology*, vol. 16, no. 6, pp. 640–647, 2011.

[13] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[14] R. Cristina, V. Giacomo, and C. Antonio, "Privacy-preserving smart metering with multiple data consumers," *Computer Netowkrs*, vol. 57, pp. 1699–1713, 2013.

[15] S. Drenker and A. Kader, "Nonintrusive monitoring of electric loads," *IEEE Computer Applications in Power*, vol. 12, no. 4, pp. 47–51, 1999.

[16] E. L. Quinn, "Smart metering and privacy: existing laws and competing policies," Tech. Rep., 2009, http://ssrn.com/abstract=1462285, http://dx.doi.org/ 10.2139/ssrn.1462285.

[17] S. D'Antonio,, L. Coppolino, I. A. Elia, and V. Fromicola, "Security issues of a phasor data concentrator for smart grid infrastructure," in *Proceedings of the 13th European Workshop on Dependable Computing (EWDC '11)*, pp. 3–8, May 2011.

[18] W. Wenye and L. Zhuo, "Cyber security in the smart grid: survey and challenges," *Computer Networks*, no. 57, pp. 1344–1371, 2013.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 219396, 9 pages
http://dx.doi.org/10.1155/2013/219396

Research Article

An Efficient Cluster Authentication Scheme Based on VANET Environment in M2M Application

You-Boo Jeon,[1] Keun-Ho Lee,[2] Doo-Soon Park,[3] and Chang-Sung Jeong[4]

[1] *Visual Information Processing, Korea University, Seoul 136-713, Republic of Korea*
[2] *Information and Communication, Baekseok University, Chungcheongnam-do 330-704, Republic of Korea*
[3] *Computer Software Engineering, SoonChunHyang University, Chungcheongnam-do 336-745, Republic of Korea*
[4] *Electronic and Computer Engineering, Korea University, Seoul 136-713, Republic of Korea*

Correspondence should be addressed to Chang-Sung Jeong; csjeong@korea.ac.kr

Received 17 June 2013; Accepted 14 September 2013

Academic Editor: James J. Park

Wireless and mobile sensor network technologies in M2M (machine to machine) are rapidly applied to our real life. Thus, in near future, advanced wireless and mobile sensor network in M2M application will be major key factor of the future generation convergence network which is based on the state of the application. It is expected that smart machines will appear as new business service model with other machines. Most numerous researches within M2M sectors are carried out in intelligent vehicle sector integrated with IT technology. Intelligent vehicle section shows severe changes in position between vehicles and has numerous large scales of networks in its components; therefore, it is required to provide safety by exchanging information between vehicles equipped with wireless communication function via VANET (vehicular ad hoc network) and fixed apparatus at roadside regarding the status of road. In this paper, we proposed cluster authentication scheme that mutually authenticates between vehicles by composing vehicle movement as cluster configuration architecture. We have successfully included the establishment of secure channels, the detection of replay attacks, mutual cluster authentication, prevention of vehicle identity fabrication, and secure distribution of provisional session key.

1. Introduction

Rapid development of IT has brought changes in development from personal PC to smart phone, and new service environment is constructed by converging with other peripheral devices based on smart phone. Now IT is leading rapid changes in society. The new field of "pervasive computing" has brought computing capabilities to the physical context and has expanded the intelligence of objects around us. Internet of things is the combination of the variety of information sensing machines and devices, such as radio frequency identification (RFID) devices, infrared sensors, global positioning system, and Internet, forming a huge network, so that all items are connected to the network to facilitate the identification and management, which ultimately provides the full range of services to people everywhere based on the integration of applications. The most important part in the network of things is the interconnection and interoperability between the machines, which is often called M2M. It is a general term of all that can enhance the communication of machinery equipment and capability of network technology, which organically combined in communication between machines, machine control communications, interactive communication, mobile internet communications, and other types of communication technologies, to share information with machine, equipment, application process, background information system, and operator [1].

Whenever and wherever information is obtained with no difficultly, and M2M, which is for communication between machines and surrounding devices, became a major research topic in technology among researchers and wireless communication entities. It creates new and various service environments by applying with new technologies. Research direction of M2M is to transmit a number of pieces of information via various communication environments between devices and machines. One of these researches is to integrate IT and

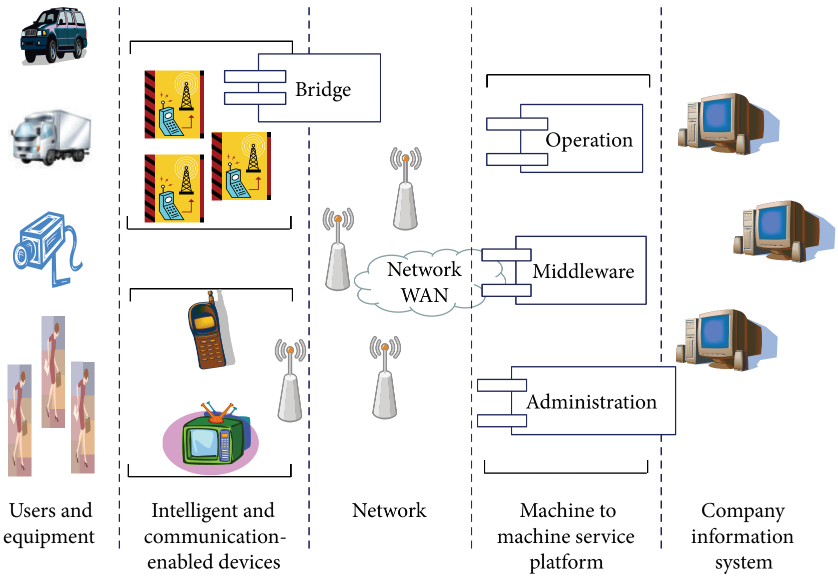

Bridge
Operation
Network
WAN
Middleware
Administration
Users and equipment
Intelligent and communication-enabled devices
Network
Machine to machine service platform
Company information system

Figure 1: M2M communication network architecture.

intelligent vehicles to enable various types of information to be transmitted, which means various devices are connected and linked to vehicles. Recent convergence technologies have impacted our life in various ways, and its technology is important to the extent that the country which initiates convergence technology is leading the world. IT technology is placed at the core of convergence, and the latter requires basis of IT. However, development of IT-based convergence technology bears a number of issues in itself, and the most critical factor is to ensure safety and security in communication between machines.

This research aims to examine what security factors exist in M2M and intelligent vehicles, then compose intelligent vehicles as cluster configuration architecture, and then propose authentication protocol of cluster unit. Finally, we show the performance evaluation of the proposed cluster authentication protocol.

2. Related Works

2.1. M2M Application Service and Security. M2M service is defined as machine to machine, machine to man, and man to machine. As depicted in Figure 1, various devices are installed to communicate and collect information from surrounding equipment and devices. Its concept is to provide information service to people and surrounding machines. M2M is utilized in the sectors of sensor network, tracking, c, and emerging device. Core technologies in M2M are identification, information collection, communication, intelligence, and minimization, and every device and system should be maintained autonomously and securely through control and information exchange between machines [2].

Threatening factors in devices in M2M architecture are bugging between equipment, hijacking, and alteration of privacy in relation with denial. There are possible threatening factors in gateway such as authorization violation by illegal usage and access, physical intrusion, replay attack, and man-in-the-middle attack. Other types of threatening factors are paralysis through illegal intrusion, service denial, virus, worm, troy wooden horse, and depletion of resources [2].

2.2. Intelligent Vehicle Security Requirements. Wireless ad hoc networks are currently a very active area of academic and industrial research for their foreseeable broad applications. These networks do not have any fixed infrastructure. The vehicles in ad hoc networks are usually limited devices with respect to their energy sources, computational capabilities, and communication range. However, it is vulnerable to a wide range of attacks due to the open medium, dynamically changing topology, possible vehicle compromise, difficulty in physical protection, absence of infrastructure, and lack of trust among vehicles [3]. Policing traffic management (PTM) is applied to improve the quality of service (QoS) over an intervehicular communications system (IVCS) [4]. The security threats have been extensively discussed and investigated in the wired and wireless networks; the correspondingly perplexing situation has also happened in MANET due to the inherent design defects. There are many security issues which have been studied in recent years. For instance, snooping attacks, wormhole attacks, black hole attacks, routing table overflow and poisoning attacks, packet replication, denial of service (DoS) attacks, and distributed DoS (DDoS) attacks. Specially, the misbehavior routing problem is one of the popularized security threats such as black hole attacks. Some researchers propose their secure routing idea to solve this issue, but the security problem is still unable to prevent completely [5].

Intelligent vehicle is evolving with various types of services to provide convenience of life by integrating with home network, telematics, and intelligent robot, thanks to development of convergence technology. Service models of intelligent vehicle are car to enterprise (C2E), car to car

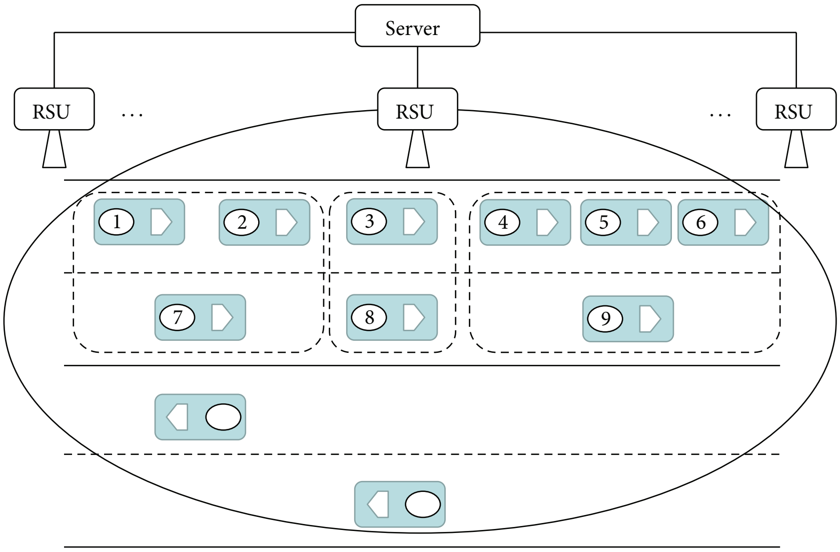


Figure 2: Intelligent vehicle communication architecture.

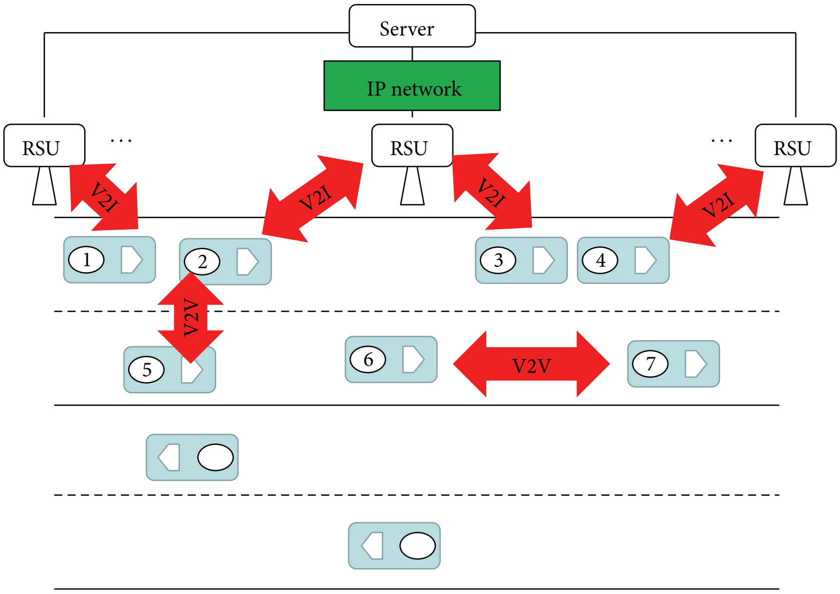


Figure 3: V2V and V2I communication network system architecture.

(C2C), and car to home (C2H). As seen in Figure 2, intelligent vehicle communication network technology is classified with internal network and external network of vehicle from the reference point of vehicle as illustrated in Figure 3. Internal network of vehicle is in general called IVN, whereas external network of vehicle is divided into V2V (vehicle to vehicle) and V2I (vehicle to infrastructure). IVN is composed of CAN, which connects and controls body or frame of car, MOST, which is for access to multimedia devices such as audio, amp, and CDP of vehicle, and X-by-Wire which connects and controls break or steering. V2V establishes vehicle communication network which constructs communication network based on vehicle-to-vehicle communication without having infrastructure of transmitting information, whereas V2I lets the vehicle access infranetwork via wire and wireless communication and provides communication network that supports communication between terminals and servers. V2V provides vehicle collision warning services and group communication based on communication between vehicles, whereas V2I provides IP based traffic information and safety support and downloads service to vehicles [6–8].

Intelligent transmission system (ITS) is an intelligent traffic system applied with state-of-the-art scientific technologies such as computer, communication, and electronics for improving existing traffic system more efficiently and economically in terms of solving traffic delay, accident, and air pollution. ITS is composed of various types of information transmission systems such as ATMS (Advanced Traffic Management System), ATIS (Advanced Traveler Information System), APTS (Advanced Public Transportation System), CVO (Commercial Vehicle Operation), and AVHS (Advanced Vehicle and Highway System).

However, there are some dysfunctions of intelligent vehicle services: violation of personal information and privacy, vehicle information, communication messages between vehicles, and communication traffic information. It requires safe and secure message transmission against these threats and forgery. There are some security framework of intelligent vehicle for the safe and secure vehicle services and communications: secure positioning, vehicle-to-infrastructure secure communication, vehicle-to-vehicle secure communication and user access control, and VPKI (Vehicles PKI).

Security treat factors in intelligent vehicle lie in network aspects. One type of security treat is forgery in which one vehicle generates false information and transmits to other vehicles located in a certain network zone. The other treat is jamming attack which generates interfering signal to other vehicles located in a certain network zone. Information forgery is executed with drop, corrupt, or modified messages or information in the process of transmission in the running of vehicle. Impersonation attack is executed in a way of in-transit traffic tampering and modifying of vehicle status information for misleading other cars. Privacy violation is executed in a way of infringement of personal privacy related information such as time, location, vehicle ID, and movement information of vehicle. On-board tampering is executed in a way of modifying speed, position, vehicle interior status information, and various sensing information of on-board vehicle [6, 9].

We present the security requirements for our VANET security system and will show the fulfillment of these requirements after presenting the design details. The privacy requirements state that private information such as vehicle owner's identity and location privacy is preserved against unlawful tracing and user profiling. A secure VANET system should satisfy several fundamental requirements, namely, authentication, nonrepudiation, message integrity, and confidentiality, where sensitive information is being exchanged, to protect the system against unauthorized-message injection, denial of message disseminations, message alteration, and eavesdropping, respectively. Nonrepudiation also requires that violators or misbehaving users cannot deny the fact that they have violated the law or misbehaved [10].

3. Cluster Configuration Scheme

This scheme uses the same two types of messages used in the CH(v) and Join(v, u). This CH (ClusterHead) selection scheme uses Cluster(v) and ClusterHead to indicate the set of vehicles in the cluster whose CH is v and the CH of a vehicle's cluster, respectively. CH(v), the Boolean variable of v, is set to true if v has sent a CH message. Its variables ClusterHead, CH(−), and Cluster(−) are initialized to nil, false, and zero, respectively.

The cluster topology is initialized and maintained through the periodic transmission of messages by each vehicle. When a vehicle is initialized, it has an undefined status cluster. To set its status cluster, it must determine whether it is within the bounds of any currently defined clusters. The vehicle broadcasts a message to its neighbors to announce its presence and to search for a neighboring CH. In the event that all vehicles initialize simultaneously, the vehicles broadcast messages looking for neighboring CHs at approximately the same time.

The following describes the two procedures that are executed at each vehicle v. On receiving a CH message from neighbor u, vehicle v checks to see whether it has received messages from all its neighbors z and that $w_v > w_z$, as indicated by a Join(z, v) message. In this case, v will not receive a CH message from these neighboring vehicles. Therefore, by default, u is the vehicle with the greatest weight in v's neighborhood that has sent a CH message. At the initial clustering setup or when vehicle v is added to the network, vehicle v executes the CH-selection procedure in order to determine its own role. If its neighbors include at least one CH with a greater weight, then v will join it. Otherwise, it will be a CH [11].

Note that a neighbor with a greater weight that has not yet decided its role will eventually send a message. If this message is a CH message, then vehicle v will try to affiliate with the new CH. When vehicle v receives the corresponding CH message, it checks to see if $w_n > w_v$. If this is the case, then v joins n's cluster independent of its current role [11]. When a neighbor u becomes a CH, on receiving the corresponding CH message, vehicle v checks whether it has to affiliate with u; that is, it checks whether w_u is greater than the weight of v's CH. In this case, independent of its current role, v joins u's cluster.

Every vehicle must either be a member of a cluster or else be a CH. Hence, if a vehicle is not within the transmission range of any CH, it should be a CH itself. When a vehicle moves to the periphery of a network, it is possible that it will move out of direct transmission range of all other CHs. When a vehicle loses contact with all CHs, it transmits a message to look for another CH, to verify that it is not within the transmission range of any CH. It then sets a timer to wait for the reception of a message from a CH. As vehicle s wander to the periphery of a network, it is likely that they will become CHs because they will be out of transmission range of all other CHs. To prevent continued growth in the number of CHs, there must be a mechanism for CHs to revoke their CH status and become non-CHs. A number of clustering protocols have the requirement that when two CHs come within direct transmission range of one another, one CH must give up its CH status. The protocol for deciding which CH should revoke its CH status can be based on a weighted algorithm. This results in a ripple effect, whereby one CH change results in additional changes within the network. CH changes are expensive due to the change in routing paths that occur as a result. Therefore, the ripple effect can have a detrimental impact on the performance of a network and should be avoided. Hence, CH changes should be minimized. This algorithm minimizes CH changes during

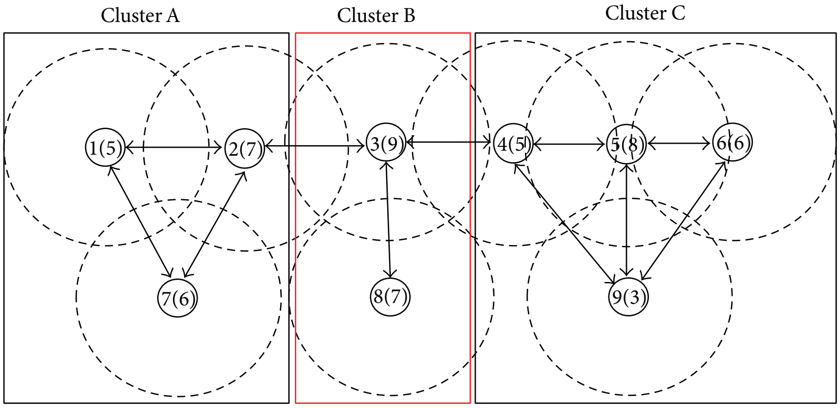


Figure 4: Cluster configuration.

```
Procedure Initialize:
begin
   if $\{z \in (v) : w_z > w_v \wedge \mathrm{Ch}(z)\} \neq \emptyset$
   then begin
         $x := \max_{w_z > w_v} \{z : \mathrm{Ch}(z)\}$;
         send Join $(v, x)$;
         ClusterHead:= $x$
      end
   else begin
         send Ch($v$)
         Ch($v$):= true;
         ClusterHead:= $v$;
         Cluster $(v)$ := $\{v\}$
      end
   end;
Repeat—On receiving ClusterHead (u)
begin
  if $(w_u > w_{\mathrm{ClusterHead}})$ then
       begin
         send Join $(v, u)$;
         ClusterHead := $u$;
         if Ch($v$) then Ch($v$) := false
       end
end;
```

Algorithm 1

weighting the network and prevents the ripple effect [11]; see Algorithm 1.

4. Cluster Based Authentication Protocol

4.1. Assumption. Protocol environment is proposed based on the following hypotheses: all vehicles are running in the same environment. Each vehicle is represented as a vehicle in Figure 4 with weighted reference on the basis of structure of Figure 2. First, vehicle in running is authorized from server via RSU. DoS (denial of service) attack is possible in physical layers of real network. But this DoS attack is not considered. Second, in the cluster configuration, each vehicle is supposed to know vehicle information received from RSU or surrounding vehicles. RSU ensures safe connection in communication between authorizing server and CH (ClusterHead). CH maintains $\mathrm{ID_s}$ of vehicles within cluster, and each CH should be always reliable. CH is assumed to play a role as a server within cluster. Each vehicle is randomly composed with weighted value for each vehicle as seen in Figure 4 according to selection criteria of CH.

It is assumed that references of weighted value are determined on the basis of characteristics of vehicle (speed, distance of vehicles, and calculation function of vehicle). When authorization of vehicles is expired, it will be disposed immediately and receives a new one. Authorization via CH is reissued by using key of each vehicle from authentication server.

Each cluster is composed as Cluster A, B, and C on the basis of Figure 4. Relationship with neighbor vehicles and weighted value are the criteria in cluster composition. CH in Cluster A, vehicle 2 shows highest weighted value 7, so it plays as a ClusterHead. It is assumed that vehicle 3 in Cluster B and vehicle 5 in Cluster C play a CH role, respectively. The vehicle approaching in cluster plays gateway for connecting each cluster.

4.2. Symbols. The following symbols are used in this research.

$\mathrm{CH_A}$:	ClusterHead A
$\mathrm{ID_X}$:	Identification X
$\mathrm{K_{S,CH}}$:	Confidential key shared between session key S and CH or S and CH
Time:	Current time
S:	$\mathrm{CH_A}$ member vehicle
X:	$\mathrm{CH_B}$ member vehicle
$\mathrm{K_{A+}}$:	Public key of vehicle A
$\mathrm{K_{A-}}$:	Private key of vehicle A
$\mathrm{cert_A}$:	Certification of vehicle A
e:	Effective date of authentication
$\mathrm{Nonce_A}$:	Vehicle A nonce generation.

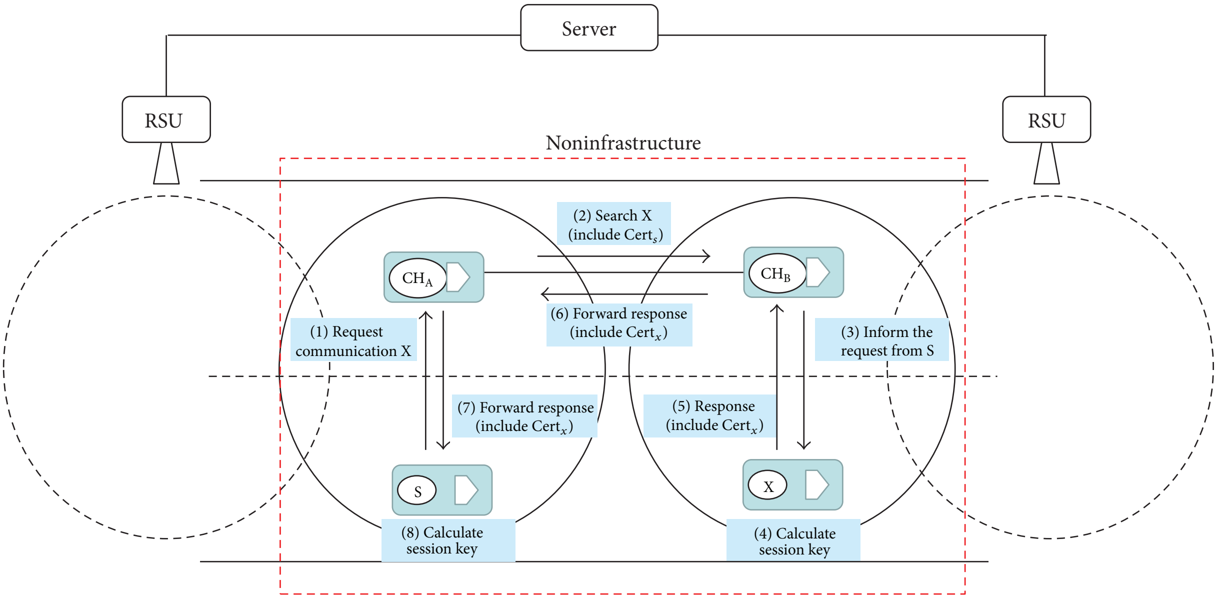

Server
RSU
RSU
Noninfrastructure
CH_A
CH_B
S
X
(1) Request communication X
(2) Search X (include $Cert_s$)
(3) Inform the request from S
(4) Calculate session key
(5) Response (include $Cert_x$)
(6) Forward response (include $Cert_x$)
(7) Forward response (include $Cert_x$)
(8) Calculate session key

Figure 5: Noninfrastructure authentication scheme.

4.3. Authentication Scheme and Protocol. Cluster authentication protocol is composed of authentication protocol with cluster units without existing infrastructure and one with existing infrastructure.

4.3.1. Noninfrastructure Authentication Scheme. Noninfrastructure authentication method is to authorize with signature between ClusterHeads as depicted in Figure 5. It provides security between clusters by using session key as a key value.

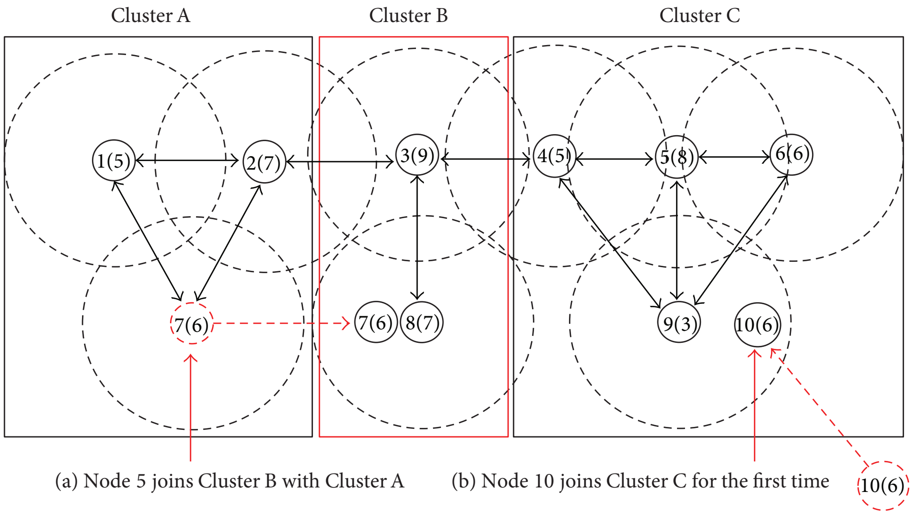
After authenticating a CH using the server, there are nine steps in our end-to-end key exchange procedure and authentication process for Noninfrastructure networks, as shown in Figure 5. First, using a previously shared secret key K_{S,CH_A}, S sends a message to CH_A requesting communication with X. Since ID_s is encrypted using K_{S,CH_A}, only vehicles S and CH_A know the vehicle with which S wishes to communicate. As $Cert_S$ and $Nonce_S$ are also encrypted, they can be transferred securely.

On receiving the request, CH_A checks to see whether S is a member. If this is the case, steps 2 and 6 shown in Figure 6 are not required. Otherwise, in step 2, CH_A asks the other ClusterHeads where X is using their public keys. Let us assume that X is located in cluster B. By using the CH_B public key that was previously established for communication between CHs, the search reveals that X is located in cluster B.

In step 3, X is informed of the request from S to communicate with it. CH_B sends S's certificate along with $Nonce_{CH_B}$. On deriving the public key for S from the certificate, X calculates the session key $K_{X,S} = (PK_S)^{K_X} \bmod P$, which will be shared between S and X. X uses $K_{S,X}$ in step 4 to let CH_B know in step 5 that it accepts S's request for communication. In step 6, CH_B and CH_A pass to S the part of the message in step 4 that contains X's confirmation using $K_{S,X}$. CH_B and CH_A also forward X's certificate to S. In step 7, S receives a message from CH_A that includes X's certificate. In step 8, S calculates the session key $K_{S,X} = (PK_X)^{K_S} \bmod P$ using PK_X derived from $Cert_X$. Finally, in step 9, S communicates with X by sending back X's nonce encrypted using their shared key $K_{S,X}$.

4.3.2. Changing Vehicle into Cluster. A vehicle joining a cluster for the first time needs strong authentication. We use the system key pair because it allows mutual authentication between the joining vehicle and an existing member vehicle of the cluster. When a vehicle joins a cluster, it is given a system public key and a system private key. All the vehicles of the cluster share this key pair. When a new vehicle moves into the network and is detected by the CH, it is given the cluster key and the table containing the cluster IDs, shadow key (SK), and CH public keys. The CH acts as the certification authority for all of its members. This information is exchanged after mutual authentication in which the corresponding CHs of the vehicles act as servers. The CH keys are used to exchange session keys secretly. The CH then decrypts and transmits the session key to other members involved in the session. If a vehicle wants to establish a session with other vehicles, it also sends this request to the CH. The CH generates a set of random prime numbers. First, the numbers are encrypted with the CH's private key and then with the cluster key. Along with each number, a time stamp is encrypted so that the keys can be used for only a limited amount of time. All the other cluster members also receive this information and buffer the values, since these number values can serve as authentication.

As the composition of a CH network changes dynamically when CHs are added, deleted, or merged in the network, the secret shares must also be renewed regularly because the number of shares needs to adapt to the number of CHs. In addition, it is necessary to ensure that the key shares are renewed after a certain period of time to make it difficult for a moving attacker to compromise several SK CHs over time.



(a) Node 5 joins Cluster B with Cluster A

(b) Node 10 joins Cluster C for the first time

FIGURE 6: A vehicle joins a cluster for the first time.

In our approach, we always combine the addition, deletion, and merging of CHs with key share renewal and only schedule additional renewals if the CH network remains unchanged for some time. The public key of the CH network must be known to all vehicles in the VANET. It is propagated via the CH beacons, which are broadcast periodically in every cluster. Besides the public network key, a CH beacon also contains the CH's own public key, a list of vehicles in the current cluster, including their status, and a list of gateways connected to adjacent clusters. This beacon message contains information regarding the neighbors, including the clusters that they belong to, adjacent clusters, and certificates. On receiving a message, a vehicle updates its local related tables with the message information and can detect vehicles that are joining or leaving. This method provides a useful means of maintaining cluster membership synchronization.

Figure 6 shows the join situation. When a vehicle joins a cluster area for the first time, the CH detects that a new vehicle has joined based on the messages in Figure 6(b). When a vehicle leaves a cluster or joins a new cluster area, the system begins the CH selection algorithm for remaining vehicles that have not yet been chosen as CHs or assigned to a cluster area (Figure 6(a)). The CH at the old location receives newer messages from its one- and two-hop neighbors that do not contain the member entities of the leaving vehicle for a predefined time interval, at which point the old CH purges the leaving vehicle.

When a new vehicle joins the network and is detected by a CH, it receives the cluster key and the table containing the cluster IDs, lifetime, mobility, weight, and CH public keys. When a vehicle leaves a cluster and joins another cluster with the movement of vehicles, the new CH treats it as a new vehicle joining its cluster. Mutual authentication is performed between the moved vehicle and its new CH using the system key pair (K/k). The CH then gives the vehicle the cluster key for the new cluster. The old cluster purges the entry for this vehicle when it does not receive a message within a predefined time interval.

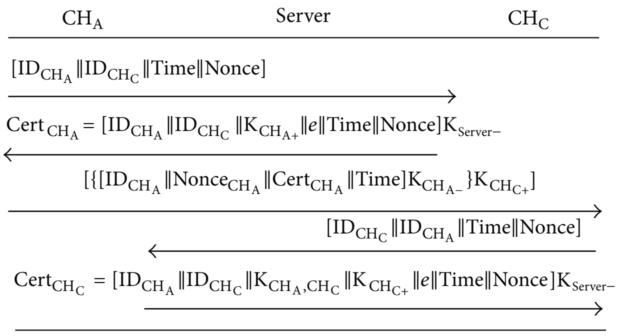

$\mathrm{CH_A}$
Server
$\mathrm{CH_C}$
$[\mathrm{ID_{CH_A}} \| \mathrm{ID_{CH_C}} \| \mathrm{Time} \| \mathrm{Nonce}]$
$\mathrm{Cert}_{\mathrm{CH_A}} = [\mathrm{ID_{CH_A}} \| \mathrm{ID_{CH_C}} \| \mathrm{K_{CH_{A+}}} \| e \| \mathrm{Time} \| \mathrm{Nonce}]\mathrm{K_{Server-}}$
$[\{[\mathrm{ID_{CH_A}} \| \mathrm{Nonce_{CH_A}} \| \mathrm{Cert_{CH_A}} \| \mathrm{Time}]\mathrm{K_{CH_{A-}}}\}\mathrm{K_{CH_{C+}}}]$
$[\mathrm{ID_{CH_C}} \| \mathrm{ID_{CH_A}} \| \mathrm{Time} \| \mathrm{Nonce}]$
$\mathrm{Cert}_{\mathrm{CH_C}} = [\mathrm{ID_{CH_A}} \| \mathrm{ID_{CH_C}} \| \mathrm{K_{CH_A,CH_C}} \| \mathrm{K_{CH_{C+}}} \| e \| \mathrm{Time} \| \mathrm{Nonce}]\mathrm{K_{Server-}}$

FIGURE 7: Authentication protocol between terminals.

The merging of two clusters into a single cluster is one of the most difficult and expensive operations. As two cluster SKs cannot be mixed, one must be dropped and the other distributed over the entire network. All of the certificates that were signed with the dropped key eventually have to be reissued, although it is possible to keep the dropped key for a period of time to facilitate this process. It may become necessary to adapt a (K, SK) threshold for the changed number of vehicles and CHs in the networks. If merging two bigger networks is difficult, any decision about the remaining network depends on parameters such as the number of CHs and the number of vehicles that would like to apply for a new configuration cluster using the CH selection algorithm and obtain new certificates.

4.3.3. Infrastructure Authentication. Figure 7 shows authentication protocol between CHs by using other RSU on the basis of Figure 4 cluster composition. In order to authorize via other RSU, it needs to receive authentication by using server key from authentication server and confirm whether CH is registered in authentication server.

In the fast moving environment of intelligence vehicle where its status keeps changing, the changes of each vehicle can be checked by cluster unit. This brings efficiency of management. In the event that vehicle 1 in Figure 4 moves quickly to Cluster B zone at other RSU zone, $\mathrm{CH_B}$, for proceeding of authentication work for this vehicle, can check whether this is the right vehicle by communication with $\mathrm{CH_B}$ which used to maintain vehicle 1 from authentication server.

Where, the server is reliable and officially certified server and maintains CH through each RSU. This is able to react to malicious attack against each vehicle by transmitting to server information about newly approaching vehicle to RSU and leaving vehicle on a real time basis. Every CH can initiate authentication work by receiving authentication from reliable server. As seen in Figure 4, in the event that CH misses message of vehicle, it can transmit correct message by threshold. Security is ensured by that CH knows public key of server and private key of each CH.

Upon request for communication between each CH, ID of CH, current time, and Nonce are generated and sent, and server transmits authentication including effective date. This is how mutual authentication is made between CHs.

5. Attack Analysis

In this section, we compare the efficiency of existing clustering protocols and our proposed protocol. We also discuss how authentication scheme and protocol is able to deny possible attacks in VANET. As scheme and protocol establishes authentication based on a trusted layer, it guarantees end-to-end security.

We evaluated the performance of our protocol and identified the advantages and limitations of our proposed approach. In our protocol, a CH establishes a member vehicle that is worthy of trust by the other members of the CH. Falsehood detection in the certification process is achieved. Authentication scheme and protocol is more reliable during the certification of a CH because it uses a server and it has fewer processing operations. The scheme and protocol enforces stronger security as it uses a server to obtain a higher level of security than can be realized by other clustering routing protocols.

An analysis of its performance verified its authentication, efficiency, safety, and scalability. Authentication and nonrepudiation use a cryptographic certificate. Each vehicle receives a certificate from its trusted CH. We evaluated four performance metrics.

5.1. Modification Attacks. Attacks using modification are generally targeted against the integrity of routing computations. By modifying routing information, an attacker can cause network traffic to be dropped, redirected to a different destination, or take a longer route to its destination, resulting in increased communication delays.

Proposed scheme and protocol can use the session keys to encrypt the traffic flow of both data and control packets. Therefore, since the Diffie-Hellman key exchange $\mathrm{K_{X,S}} = (PK_{\mathrm{S}})^{\mathrm{K_X}} \bmod P$ of the message contents is included in every packet transmitted, the integrity of the contents is guaranteed, along with confidentiality.

5.2. Fabrication Attack. Fabrication attacks involve generating false routing messages. These attacks are difficult to recognize as they are received as genuine routing packets. An attacker can nullify a working route to a destination by fabricating a routing error message claiming that a neighbor can no longer be contacted.

The authenticity of the received control and data packets can be verified using the session keys and the server. As the session keys are unique, fabricated packets can easily be detected and hence discarded.

5.3. Spoofed Route Attack and Unauthorized Participation. A malicious vehicle can launch several attacks in a network by masquerading as another vehicle (spoofing). Spoofing occurs when a malicious vehicle misrepresents its identity by altering its MAC or IP address in order to fool a benign vehicle into arriving at an inaccurate picture of the network topology.

Proposed scheme and protocol participation accepts only packets that have been signed with a certified key issued by a trusted authority using a server. There are many mechanisms for authenticating users to a trusted certificate authority. Since only the source vehicle can sign using its own private key, vehicles cannot spoof other vehicles in route instantiation. The encryption of all end-to-end traffic indirectly ensures the verification of packets, as the session keys are held only by the previously authenticated end points. Consequently, the legitimacy of all packets is verified automatically during the decryption phase, ensuring that any packets that were spoofed are discarded. Similarly, replay packets include the destination vehicle's certificate and signature, ensuring that only the destination can respond to route discovery.

5.4. Replay Attacks. When the attacker receives a request for a route to the target vehicle, the attacker creates a replay in which an extremely short route is advertised. If the malicious replay reaches the requesting vehicle before the replay from the actual vehicle, a forged route has been created.

Replay attacks are prevented by including a nonce and a time stamp with the routing message. Proposed scheme and protocol minimizes changes in the certificate process of cluster networks. Our analysis of scalability has verified the authentication, efficiency, safety, and scalability of our method.

6. Conclusion

It is expected that various security issues are raised in the development of intelligent vehicle and its convergence technology. Future security issues in vehicle industry have inherently critical treat factors; therefore, it is important to research on security. Among all other security threatening factors, this research has proposed authentication protocol on a cluster basis to counteract various changes in vehicle. Proposed protocol can improve safety and security by effective authentication in a scalable wide area such as express road environment. For the future further research subjects in cluster configuration, it may require to research about an algorithm which can configure more efficiently with various changes and increase security level while reducing resources in the middle of various changes.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (no. 2011-0010457). This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2012-C1090-1201-0008).

References

[1] J. Du and S. Chao, "A study of information security for M2M of IOT," in *Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10)*, pp. V3576–V3579, August 2010.

[2] G.-S. Ryu and K.-H. Lee, "Authentication based on cluster in machine to machine," *Journal of the Korea Knowledge Information Technology Society*, vol. 5, no. 6, pp. 103–110, 2010.

[3] M. Imani, M. Taheri, and M. Naderi, "Security enhanced routing protocol for Ad hoc networks," *Journal of Convergence*, vol. 1, no. 1, pp. 43–48, 2010.

[4] S. Prahmkaew, "Performance evaluation of convergence Ad hoc networks," *Journal of Convergence*, vol. 1, no. 1, pp. 101–106, 2010.

[5] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, "A survey of black hole attacks in wireless mobile Ad hoc networks," *Human-Centric Computing and Information Sciences*, vol. 1, article 4, 2011.

[6] G.-W. Kim, S.-K. Kim, and K.-H. Lee, "The security requirement based on intelligent vehicular network in M2M environment," *Journal of the Korea Knowledge Information Technology Society*, vol. 5, no. 6, pp. 124–129, 2010.

[7] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8–15, 2006.

[8] I. Cha, Y. Shah, A. U. . Schmidt, A. Leicher, M. Victor, and Trust in M2M communication, *IEEE Vehicular Technology Magazine*, vol. 4, no. 3, pp. 69–75, 2009.

[9] D.-R. Kim, J.-Y. Song, and S.-K. Cha, "Introduction of case study for M2M intelligent machine tools," in *Proceedings of the IEEE International Symposium on Assembly and Manufacturing (ISAM '09)*, pp. 408–411, November 2009.

[10] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular Ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[11] S. Basagni, "Distributed clustering for Ad hoc networks," in *Proceedings of the 1999 International Symposium on Parallel Architectures, Algorithms, and Networks (ISPAN '99)*, pp. 310–315, June 1999.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 694829, 13 pages
http://dx.doi.org/10.1155/2013/694829

Research Article

Integrated Validation System for the Simulation of Diverse Sensors in WSNs

Hyun-Woo Kim and Young-Sik Jeong

Department of Multimedia Engineering, Dongguk University, 30 Pildongro 1 Gil, Jung-Gu, Seoul 100-715, Republic of Korea

Correspondence should be addressed to Young-Sik Jeong; ysjeong@dongguk.edu

Received 8 June 2013; Accepted 8 July 2013

Academic Editor: Jong Hyuk Park

In wireless sensor networks (WSNs), sensors use different types of information, such as temperatures, humidity, magnetic fields, and sound; their communication distances and battery sizes and capacities may be different. Differences in communication distances and battery capacities when the same communication method is used affect the life of the entire sensor network topology. Tests for the maximum life of the sensor network topology require many sensor nodes and huge proportional costs. In addition, experiments to verify new ideas for WSNs as alternatives to existing methods also require large expenditures. Since experiments with the arrangement of actual sensors are expensive, such experiments are conducted using simulators so that solutions for protocol design and verification can be compared through software. Existing simulators are tailored to certain sensor characteristics, so that only quite limited results can be obtained through the implementation of simulated operations, simulations of sensor arrangements, and the comparison of limited information transmission routing functions provided by simulators. This paper proposes diverse sensor definable simulators (DSDs) for the performance of experiments on diverse sensors with different communication distances in WSN environments where Geography Markup Language (GML) based coordinates are utilized.

1. Introduction

Wireless sensor networks (WSNs) have been actively studied by many researchers thus far and are grafted on actual life areas (e.g., surveillance area, living room with sensors etc.). In WSN environments, diverse sensors are generally used depending on the types of data to be collected from sensing target regions, including temperature, humidity, magnetic fields, and sound. Events are sensed using these sensors and the data are transmitted to sink nodes through sensor networks. The transmitted information is applied to engines that have different roles in many application services. These include national safety, medical devices, senior citizens who live alone, traffic control and safety, process control, energy savings, weapon systems, distributed robots, manufacturing, and communication systems. To build up these WSN environments, many sensors and appropriate protocols for communication between them are necessary. Since protocols for communication between sensors are used differently according to their diverse types, it is not easy to set up optimum environments. Arranging sensors in target regions to test them for verification of theoretical contents is expensive. Sensor node arrangements require the use of many sensor nodes, along with arrangement algorithms. Finding and correcting errors in these sensor nodes require huge amounts of time and effort, and inspecting individual sensor nodes is practically impossible [1–4].

Therefore, to build up WSN environments, software simulators that enable prior testing, verification, and supplementation of theoretically designed contents are necessary. Thus far many simulator tools for the design and verification of WSNs have been developed, including GloMoSim [5], SNetSim [6], ATEMU [7], QualNet [8], NS2 [9], EmStar [10], TOSSIM [11], J-Sim [12], AVRORA [13], SWANS [14], SENSE [15], MSPsim [16], WSim [17], Atarraya [18], WSNet [19], AlgoSenSim [20], NetTopo [21], and SIDnet-SWANS [22]. However, although such simulators have been developed, tests are conducted using limited sensor information, so that only very restricted results are obtained, or large- or small-scale networks are insufficiently treated. In addition, since simulations are basically conducted with those types of sensors that are built in simulators, these simulations are not suitable of experiments on other sensors, new sensors, or combinations of sensors [1, 2, 23, 24].

Therefore, this paper proposes a diverse sensor definable simulators (DSDs) for performance experiments on diverse sensors with different communication distances not only in experimental environments but also in WSN environments where geography-markup-language- (GML-) based coordinates are utilized. The DSDs use GMLs that can be mapped with actual topography so that the simulations of target topography can be provided in more detail. This can create dynamic and diverse static arrangements of mobile sensor nodes (MSNs) and fixed sensor nodes (FSNs). In addition, this paper also proposes a simulator that provides not only basic sensor-setting methods but also functions for users to define sensor types so that more concrete experiments can be conducted. It provides functions for users to define additional sensor node types other than MSNs and FSNs, so that not only new sensor types but also existing diverse sensors can be universally simulated.

The remainder of the paper is composed as follows. In Section 2, simulators that have been developed as tools for the design and verification of existing WSNs are introduced in detail. In Section 3, the specification of the definition of sensor types in the DSDs proposed in the present paper is explained. In Sections 4 and 5, contents regarding the design and implementation of the DSDs are described.

2. Related Works

In this section, the characteristics and functions of simulators already developed for simulations of protocols, packet losses, coverage, and connectivity ratios in WSN are given (Table 1) [1].

As shown in Table 1, the tools operate simulations of certain sensors or provide limited results due to restrictions in their functions. Therefore, in the present paper, a framework will be provided in which diverse types of sensors, such as temperature, humidity, magnetic field, and sound sensors, can be used to simulate various performances, including the sensor arrangements necessary for WSNs.

3. Definition of Sensor Type

The DSDs proposed in the present paper provide a function to define basic sensor types necessary for the simulations of the functions and performance of WSNs using diverse sensor nodes. This definition of sensor types enables users to select the basic sensor node information necessary for simulator operation and colors for visualization.

First, information on sensors necessary for the definition of sensor types is given as follows.

(1) Each sensor's identifier should be unique.

(2) The definition of the types of sensor functions refers to temperature sensing, illumination sensing, magnetic field sensing, sound sensing capabilities, and so on, and the sensing ranges of sensors by type can be inputted in detail.

(3) As sensors' operation periods, the periods of basic sensors' active states are entered.

(4) As sensors' operating time, the time for which the active mode of sensors should be maintained for operation should be entered.

(5) The sensor sleeping time refers to the sleeping time when sensors are in the resting state.

(6) The range of sensor communication is the range of communication for information transmission between sensors, and the values of the maximum range of communication and the basic range of communication are required.

(7) Sensors' battery sizes refer to the basic battery sizes of sensors, which indicate their capacities.

(8) The definitions of the amounts of battery consumption by sensor function should be entered. In the case of mobile sensors, the rate of battery consumption during movements should be given (for instance, if 50 mA is consumed per 1 m, the migration length (1 m) and the amount of consumption (50 mA) should be entered). When sensors are in operation in the active mode, the operation time and the amount of consumption are required. When sensors are in operation in the sleep mode, the operation time and the amount of consumption are required.

(9) The details of the residual battery capacity should be entered. As methods for obtaining the residual battery capacity, two methods, one for the user to prepare the formula and another to obtain the residual battery capacity relying on the DSDs, are provided. The formula is to be entered by the user with the sensor information entered earlier (the formula can be generated for the four fundamental arithmetic operations and parentheses can be used based on the priorities of operations). In the case of the method relying on DSDs, the residual battery capacity after deducting the amounts of battery consumption applying the rates of battery consumption for the operations of individual functions of independently operating sensors is calculated.

(10) The information necessary for the prediction of battery life should be entered. When the user has entered a formula into the details for the residual battery capacity, information is provided so that the user can predict the life based on the entered formula considering the residual battery capacity. In the case of the method relying on DSDs, the expected life time is calculated for the residual battery capacity after deducting the amounts of battery consumption, applying the rates of battery consumption for the operations of independently operating sensors. In this case, the rates of battery consumption are rates accumulated in proportion to operating time in accordance with operations by function.

The three pieces of information to be added on the definition of sensor types for the visualization functions of

Table 1: Characteristics and functions of the existed simulators.

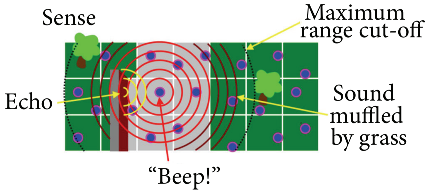
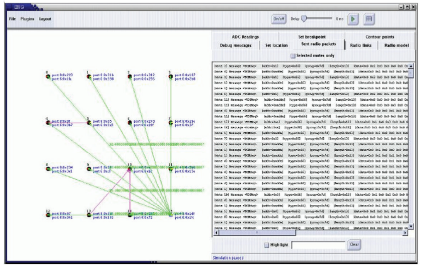
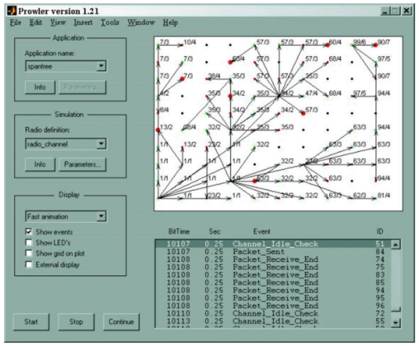
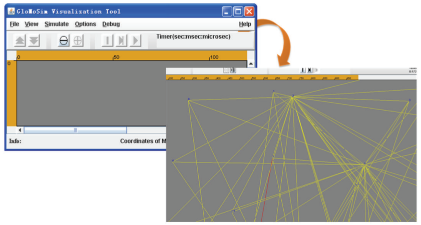
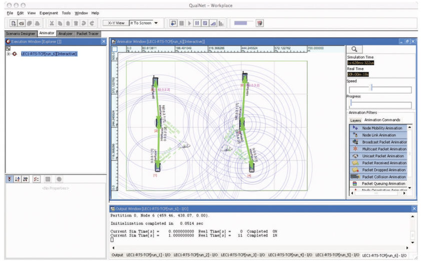
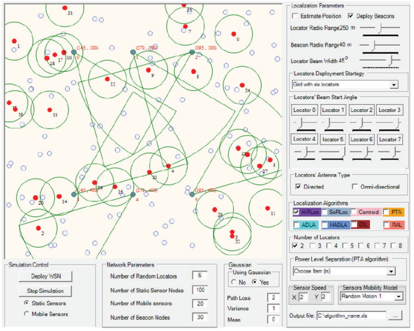
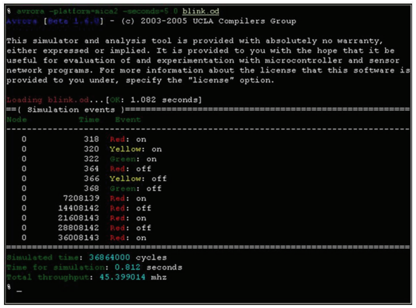
Tools	Explanations
 Sense Maximum range cut-off Echo Sound muffled by grass "Beep!"	A sensor, environment, and network simulator. Errors are common; wireless communication, noisy measurements, and node failures are to be expected. Network interacts heavily with environment. Highly constrained nodes (e.g., 4 k RAM, 2 AA batteries, and 20 msg/s radio) must operate for months; little supervision and experiments are time and space intensive.
TOSSIM (tinyOS simulator) 	An open source TinyOS-based simulator from UC Berkeley. TOSSIM can simulate Mica2 series simulation from CrossBow. Main features are packet loss calculation and CRC sensing. However, it can only work with Mica2 series.
Prowler  Prowler version 1.21 File Edit View Insert Tools Window Help Application Application name: spantree Info Parameters Simulation Radio definition: radio_channel Info Parameters... Display Fast animation ☑ Show events □ Show LED's □ Show grid on plot □ External display Start Stop Continue BitTime Sec Event ID 10107 0.25 Channel_Idle_Check 51 10107 0.25 Packet_Sent 84 10108 0.25 Packet_Receive_End 74 10108 0.25 Packet_Receive_End 75 10108 0.25 Packet_Receive_End 83 10108 0.25 Packet_Receive_End 85 10108 0.25 Packet_Receive_End 94 10108 0.25 Packet_Receive_End 95 10108 0.25 Packet_Receive_End 96 10110 0.25 Channel_Idle_Check 72 10113 0.25 Channel_Idle_Check 55	A probabilistic WSN simulator running under the MATLAB environment. The tool supports the Gaussian and Rayleigh radio propagation models, complemented with two collision detection schemes and the following MICA2 MAC-layer communication protocol.
GloMoSim  GloMoSim Visualization Tool File View Simulate Options Debug Help Timer(sec:msec:microsec) Info: Coordinates of M	A PARSEC- (C-based parallel simulation language) based discrete event simulator. GloMosim is a simulation environment for wireless mobile network. Like OSI 7-hierarchical model, GloMoSim is composed of number of layers. It monitors packet transmission status and verifies network model or transmission scenario; however, it cannot work as sensor network.

TABLE 1: Continued.

Tools	Explanations
QualNet 	GloMoSim's next version. QualNet is a massive wireless network simulator. It uses IEEE 802.11 MAC and Physical layer standard, and like GloMoSim it has several layers. When modules for layer are developed by different designers, the scenarios and models are being tested. Packet flow statistics can be checked through automatically collected data from each layer. Features for sensor network are designed as well, nevertheless, visualization of sensed objects.
Wireless sensor network localization simulator 	A determination of the location of sensor nodes is a simulation task that wireless sensor network localization simulator is designed for. The program comes with eight localization algorithms, while other required procedures may be implemented. Numerous parameters that define network topology include network size, locators deployment strategy, and antenna type, as well as the path loss and node mobility
AVRORA 	A command-line framework capable of simulating and analyzing programs developed for MEMSIC Mica2 and MicaZ sensor platforms. In the simulation each node has its own separated thread. It supports applications written using the Atmel and GNU assembler syntaxes.

QualNet - Workplace
Output LEC1-RTS-TCP[run_1] - I/O LEC1-RTS-TCP[run_2] - I/O LEC1-RTS-TCP[run_3] - I/O LEC1-RTS-TCP[run_4] - I/O LEC1-RTS-TCP[run_5] - I/O LEC1-RTS-TCP[run_6] - I/O

Localization Parameters
□ Estimate Position ☑ Deploy Beacons
Locator Radio Range250 m
Beacon Radio Range40 m
Locator Beam Width 45°
Locators Deployment Startegy: Grid with six locators
Locators' Beam Start Angle: Locator 0, Locator 1, Locator 2, Locator 3, Locator 4, locator 5, Locator 6, Locator 7
Locators' Antenna Type: ☑ Directed □ Omni-directional
Localization Algorithms: ☑ HiRLoc □ SeRLoc □ Centroid □ PTA □ ADLA □ HADLA □ DIL □ RAL
Number of Locators: ☑ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8
Power Level Separation (PTA algorithm): Choose Item (m)
Sensor Speed: X 2 Y 2
Sensors Mobility Model: Random Motion 1
Output file: C:\algorithm_name.xls

Simulation Control
Deploy WSN
Stop Simulation
● Static Sensors
○ Mobile Sensors

Network Parameters
Number of Random Locators 6
Number of Static Sensor Nodes 100
Number of Mobile sensors 20
Number of Beacon Nodes 30

Gaussian
Using Gaussian ○ No ● Yes
Path Loss 2
Variance 1
Mean 0

```
$ avrora -platform=mica2 -seconds=5.0 blink.od
Avrora [Beta 1.6.0] - (c) 2003-2005 UCLA Compilers Group

This simulator and analysis tool is provided with absolutely no warranty,
either expressed or implied. It is provided to you with the hope that it be
useful for evaluation of and experimentation with microcontroller and sensor
network programs. For more information about the license that this software is
provided to you under, specify the "license" option.

Loading blink.od...[OK: 1.082 seconds]
=={ Simulation events }=========================================================
Node          Time   Event
--------------------------------------------------------------------------------
   0           318   Red: on
   0           320   Yellow: on
   0           322   Green: on
   0           364   Red: off
   0           366   Yellow: off
   0           368   Green: off
   0       7208139   Red: on
   0      14408142   Red: off
   0      21608143   Red: on
   0      28808142   Red: off
   0      36008143   Red: on
================================================================================
Simulated time: 36864000 cycles
Time for simulation: 0.812 seconds
Total throughput: 45.399014 mhz
$ _
```

Table 1: Continued.

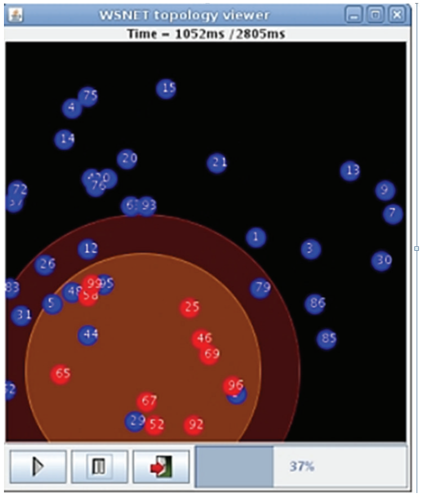
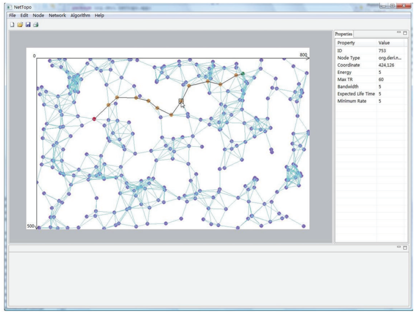
Tools	Explanations
WSNet  	It allows researchers to simulate environment focusing on physical measures and phenomena. It also offers means to analyze energy consumption and provides mobility. Radio communication models involve a simple ideal physical layer, as well as more complex representations of fading, interference, delays, transmission errors, modulations, and channel access methods.
NetTopo  NetTopo File Edit Node Network Algorithm Help Properties 0 800 Property Value ID 753 Node Type org.deri.n... Coordinate 424,126 Energy 5 Max TR 60 Bandwidth 5 Expected Life Time 5 Minimum Rate 5	It comprises simulation and visualization frameworks that share common elements for high level operations. The GUI, left figure, allows the user to view the network topology and control the properties of selected nodes. The simulator is designed to simplify studies of various WSNs algorithms. Consequently, modules are used to represent built-in and user-defined controlling, scheduling, routing, or clustering algorithms.

Table 1: Continued.

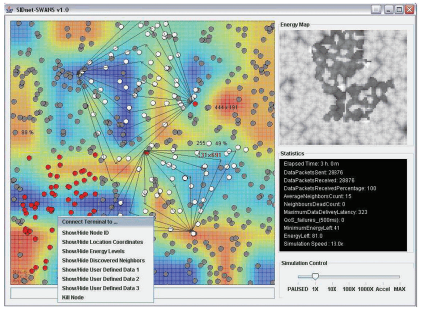
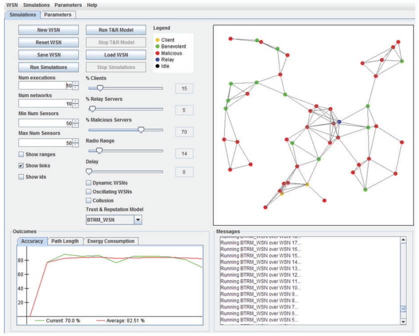
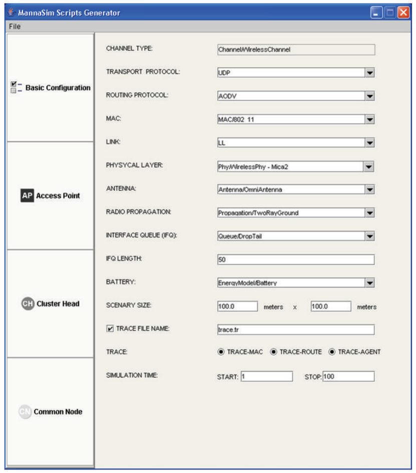
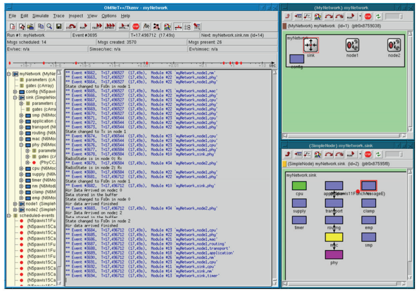
Tools	Explanations
SWANS  SIDnet-SWANS v1.0 Energy Map Statistics Simulation Control PAUSED 1X 10X 100X 1000X Accel MAX Connect Terminal to ... Show/Hide Node ID Show/Hide Location Coordinates Show/Hide Energy Levels Show/Hide Discovered Neighbors Show/Hide User Defined Data 1 Show/Hide User Defined Data 2 Show/Hide User Defined Data 3 Kill Node 88 % 444 x 191 255 49 % 331x691 Elapsed Time: 3 h. 0 m DataPacketsSent: 28876 DataPacketsReceived: 28876 DataPacketsReceivedPercentage: 100 AverageNeighborsCount: 15 NeighboursDeadCount: 0 MaximumDataDeliveryLatency: 323 QoS_failures_(500ms): 0 MinimumEnergyLeft: 41 EnergyLeft: 81.0 Simulation Speed : 13.0x	It is an expansion of JiST, a PARSEC-based scattered event simulator. It is open source simulator, and compared to NS2 or GloMoSim, it can carry out massive network simulation; nevertheless, like other simulators it can only carry out protocol verification.
TRMSim-WSN  WSN Simulations Parameters Help Simulations Parameters New WSN Reset WSN Save WSN Run Simulations Run T&R Model Stop T&R Model Load WSN Stop Simulations Legend Client Benevolent Malicious Relay Idle Outcomes Accuracy Path Length Energy Consumption 80 60 40 20 Current: 70.0 % Average: 82.51 % Messages Num executions: 10 Num networks: 10 Min Num Sensors: 50 Max Num Sensors: 50 ☐ Show ranges ☑ Show links ☐ Show ids % Clients: 15 % Relay Servers: 5 % Malicious Servers: 70 Radio Range: 14 Delay: 0 ☐ Dynamic WSNs ☐ Oscillating WSNs ☐ Collusion Trust & Reputation Model: BTRM_WSN Running BTRM_WSN over WSN 17... Running BTRM_WSN over WSN 16... Running BTRM_WSN over WSN 15... Running BTRM_WSN over WSN 14... Running BTRM_WSN over WSN 13... Running BTRM_WSN over WSN 12... Running BTRM_WSN over WSN 11... Running BTRM_WSN over WSN 10... Running BTRM_WSN over WSN 9... Running BTRM_WSN over WSN 8... Running BTRM_WSN over WSN 7... Running BTRM_WSN over WSN 6... Running BTRM_WSN over WSN 5...	TRMSim-WSN (trust and reputation models simulator for wireless sensor networks) is a software designed to help researchers study and compare trust and reputation models. The simulation can be run over a single randomly generated WSN or over a set of networks. The user is able to define parameters of the network, such as the percentage of clients and that of malicious nodes
NS-2 based simulators  MannaSim Scripts Generator File Basic Configuration AP Access Point CH Cluster Head CN Common Node CHANNEL TYPE: Channel/WirelessChannel TRANSPORT PROTOCOL: UDP ROUTING PROTOCOL: AODV MAC: MAC/802_11 LINK: LL PHYSYCAL LAYER: Phy/WirelessPhy - Mica2 ANTENNA: Antenna/OmniAntenna RADIO PROPAGATION: Propagation/TwoRayGround INTERFACE QUEUE (IFQ): Queue/DropTail IFQ LENGTH: 50 BATTERY: EnergyModel/Battery SCENARY SIZE: 100.0 meters x 100.0 meters ☑ TRACE FILE NAME: trace.tr TRACE: ● TRACE-MAC ● TRACE-ROUTE ● TRACE-AGENT SIMULATION TIME: START: 1 STOP: 100	A Discrete event simulator and a popular general purpose network simulator mainly used in the studies of TCP, routing and multicast protocols. Although many ad hoc protocols are implemented, the framework lacks support for WSNs and only the module for directed diffusion is included.

Table 1: Continued.

Tools	Explanations
PAWiS 	PAWiS (power aware wireless sensors) framework is capable of simulating different types of nodes and networks due to the modular design. Generated simulation log files can be analyzed by a special application that visualizes timings, interactions, and power requirements for each node. There is a module responsible for defining processor characteristics such as interrupt handling or power management.

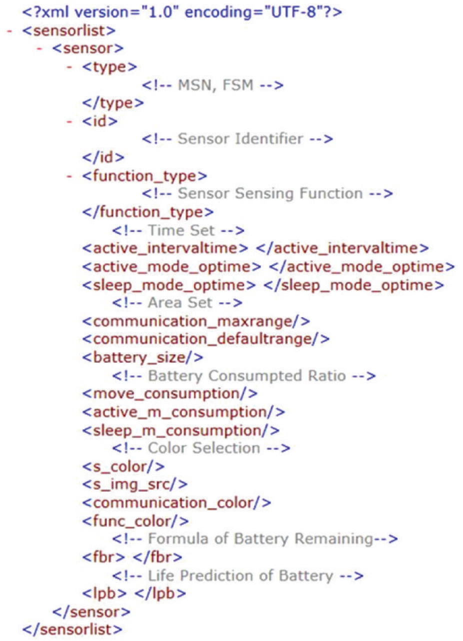
```
Run #1: myNetwork    Event #3695    T=17.496712  (17.49s)    Next: myNetwork.sink.nm (id=14)
Msgs scheduled: 14    Msgs created: 3570    Msgs present: 26
Ev/sec: n/a    Simsec/sec: n/a    Ev/simsec: n/a

** Event #3662.  T=17.496527  (17.49s).  Module #26 `myNetwork.node1.nm'
** Event #3663.  T=17.496527  (17.49s).  Module #22 `myNetwork.node1.phy'
** Event #3664.  T=17.496527  (17.49s).  Module #22 `myNetwork.node1.phy'
State changed to FsOn in node 1
** Event #3665.  T=17.496527  (17.49s).  Module #21 `myNetwork.node1.mac'
** Event #3666.  T=17.496527  (17.49s).  Module #22 `myNetwork.node1.phy'
** Event #3667.  T=17.496527  (17.49s).  Module #23 `myNetwork.node1.cpu'
** Event #3668.  T=17.496527  (17.49s).  Module #22 `myNetwork.node1.phy'
** Event #3669.  T=17.496527  (17.49s).  Module #22 `myNetwork.node1.phy'
** Event #3670.  T=17.496527  (17.49s).  Module #22 `myNetwork.node1.phy'
** Event #3671.  T=17.496544  (17.49s).  Module #23 `myNetwork.node1.cpu'
** Event #3672.  T=17.496544  (17.49s).  Module #22 `myNetwork.node1.phy'
** Event #3673.  T=17.496544  (17.49s).  Module #22 `myNetwork.node1.phy'
State changed to Tx in node 1
** Event #3674.  T=17.496544  (17.49s).  Module #23 `myNetwork.node1.cpu'
** Event #3675.  T=17.496544  (17.49s).  Module #23 `myNetwork.node1.cpu'
** Event #3676.  T=17.496544  (17.49s).  Module #23 `myNetwork.node1.cpu'
** Event #3677.  T=17.496584  (17.49s).  Module #22 `myNetwork.node1.phy'
** Event #3678.  T=17.496584  (17.49s).  Module #10 `myNetwork.sink.phy'
RadioState is in node 0: Rx
** Event #3679.  T=17.496584  (17.49s).  Module #34 `myNetwork.node2.phy'
RadioState is in node 2: Rx
** Event #3680.  T=17.496584  (17.49s).  Module #22 `myNetwork.node1.phy'
** Event #3681.  T=17.496712  (17.49s).  Module #22 `myNetwork.node1.phy'
State changed to FsOn in node 1
** Event #3682.  T=17.496712  (17.49s).  Module #10 `myNetwork.sink.phy'
Air Data Arrived on node: 0
Data stored in the buffer
State changed to FsOn in node 0
Air data arrived finished
** Event #3683.  T=17.496712  (17.49s).  Module #34 `myNetwork.node2.phy'
Air Data Arrived on node: 2
Data stored in the buffer
State changed to FsOn in node 2
Air data arrived finished
** Event #3684.  T=17.496712  (17.49s).  Module #23 `myNetwork.node1.cpu'
** Event #3685.  T=17.496712  (17.49s).  Module #22 `myNetwork.node1.phy'
** Event #3686.  T=17.496712  (17.49s).  Module #21 `myNetwork.node1.mac'
** Event #3687.  T=17.496712  (17.49s).  Module #20 `myNetwork.node1.routing'
** Event #3688.  T=17.496712  (17.49s).  Module #19 `myNetwork.node1.transport'
** Event #3689.  T=17.496712  (17.49s).  Module #18 `myNetwork.node1.application'
** Event #3690.  T=17.496712  (17.49s).  Module #26 `myNetwork.node1.nm'
** Event #3691.  T=17.496712  (17.49s).  Module #23 `myNetwork.node1.cpu'
** Event #3692.  T=17.496712  (17.49s).  Module #11 `myNetwork.sink.cpu'
** Event #3693.  T=17.496712  (17.49s).  Module #14 `myNetwork.sink.nm'
** Event #3694.  T=17.496712  (17.49s).  Module #13 `myNetwork.sink.timer'
```

```
(MyNetwork) myNetwork  (id=1)  (ptr0x8759038)
(SimpleNode) myNetwork.sink  (id=2)  (ptr0x87595f8)
```

DSDs simulators are as follows. (1) Information for sensor type division should be entered. If sensor division by type has not been set, unique colors will be randomly selected and applied. If the user wishes to select the colors, a list of colors not overlapping with each other will be shown so that the user can choose. When images are selected, it must be ensured that the same image is not used. (2) Values for color setting for sensor communication should be entered. Some colors are provided in addition to the colors basically applied so that the user can revise the colors. The colors can be easily observed using the visual part. (3) Values for sensors' sensing color setting should be set. The colors applied to the range of sensing should be selected so that they do not overlap with the colors for previous sensors using the color table.

Basic information on sensors necessary for conducting simulations is also essential. Through this function, information on existing sensors can be entered and experimented and changes can be made to existing sensors to verify the efficiency of topology in relation to sensor functions. Trial simulations can be conducted by entering new sensor information, and added functions for visualized expression can be selectively provided so that the user can quickly understand diverse experiments and their results. In addition, the defined types can be stored as XML documents so that the information can be reused and applied in many fields, by not only the user but also by other users in DSDs-based systems. Figure 1 shows an XML schema configured for sensor type definition.



```
  <?xml version="1.0" encoding="UTF-8"?>
- <sensorlist>
  - <sensor>
    - <type>
            <!-- MSN, FSM -->
      </type>
    - <id>
            <!-- Sensor Identifier -->
      </id>
    - <function_type>
            <!-- Sensor Sensing Function -->
      </function_type>
         <!-- Time Set -->
      <active_intervaltime> </active_intervaltime>
      <active_mode_optime> </active_mode_optime>
      <sleep_mode_optime> </sleep_mode_optime>
         <!-- Area Set -->
      <communication_maxrange/>
      <communication_defaultrange/>
      <battery_size/>
         <!-- Battery Consumpted Ratio -->
      <move_consumption/>
      <active_m_consumption/>
      <sleep_m_consumption/>
         <!-- Color Selection -->
      <s_color/>
      <s_img_src/>
      <communication_color/>
      <func_color/>
         <!-- Formula of Battery Remaining-->
      <fbr> </fbr>
         <!-- Life Prediction of Battery -->
      <lpb> </lpb>
    </sensor>
  </sensorlist>
```

Figure 1: User-defined sensor type with XML schema.

4. Design of DSDs

The DSDs proposed in the present study are largely divided by function into a User Interface, a Target Area Manager, an Interaction Broker, a Map Manager, a Map Controller, a Node Manager, a Coordinate Converter, and a Viewer. The *User Interface* sets the user's definition of sensor node types, revisions and deletions of the defined types, and screen configuration information. The *Target Area Manager* manages sensing target regions set by the user and the *Interaction Broker* connects the node- and map-setting values set by the user to the system. The *Map Controller* applies the map-setting values entered by the user and the *Node Manager* manages the sensor types defined by the user in addition to the sensor types basically provided for independent operations. The *Coordinate Converter* processes data in order to provide the simulated states of operation to the Viewer. The *Viewer* finally provides simulations visually. Figure 2 gives a structural diagram of all of the functions of the DSDs.

The *User Interface Component* is subdivided into a Map Interface, a Node Type Manager, and a View Mode. The Map Interface receives the entries of actual topography and mappable GML. The Node Type Manager consists of a Node Importer for adding node types defined by other DSDs in advance, a Node Exporter for storing the nodes types defined by the simulator currently in operation as XML documents, a Node Parser for adding read documents to the Node Manager, and Mobile Information and Fixed Information for receiving the entries of type addition, revision, and deletion for MSNs and FSNs. The View Mode is an interface for providing the screens operated by the DSDs so that they can be selected by the user; it is composed of Integration to operate MSN, FSN, or MSN and FSN simultaneously.

The *Target Area Manager Component* sets areas in target regions for which the GML documents read and analyze through the GML Importer should be observed for more detailed experiments. The *Interaction Broker Component* plays the role of a broker to send the set values entered by the user in the User Interface to the Map Controller and the Node Manager. The *Map Manager Component* plays the role of applying GML documents mappable with actual topography to the DSDs and managing the documents. It is composed of a GML Importer that adds the GML documents selected through the Map Interface of the User Interface to the simulator, a GML Parser that analyzes the added GML documents for application to the DSDs, a Map Layer that creates Map Objects for obstacles in the analyzed GML topography data and sends them to the Layer Manager, and a Layer Manager that manages the topographical information received from the Map Layer.

The *Controller Component* serves functions such as enlarging, reducing, area enlarging, and moving for the maps of the set values received through the Interaction Broker and managed by the Layer Manager. These functions are implemented when values have been entered through the Map Interface of the User Interface and the results are outputted on the Viewer through the Coordinate Converter. The *Node Manager Component* manages the sensor nodes types entered and defined by the user. It is subdivided into MSNs, which are mobile sensors, and FSNs, which are sensors at fixed locations. MSNs and FSNs are composed of Sensor Identifiers (S_IDs) that show the unique identifications of sensor nodes, Function Types (F_TYPEs) that define sensors'

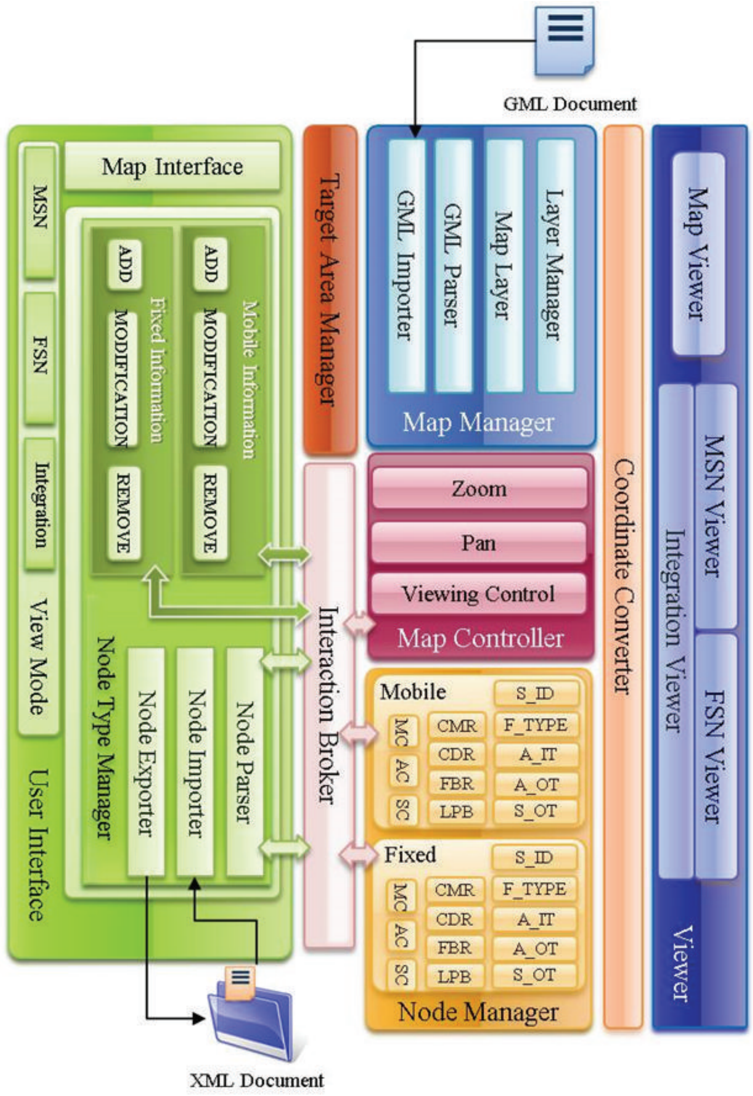
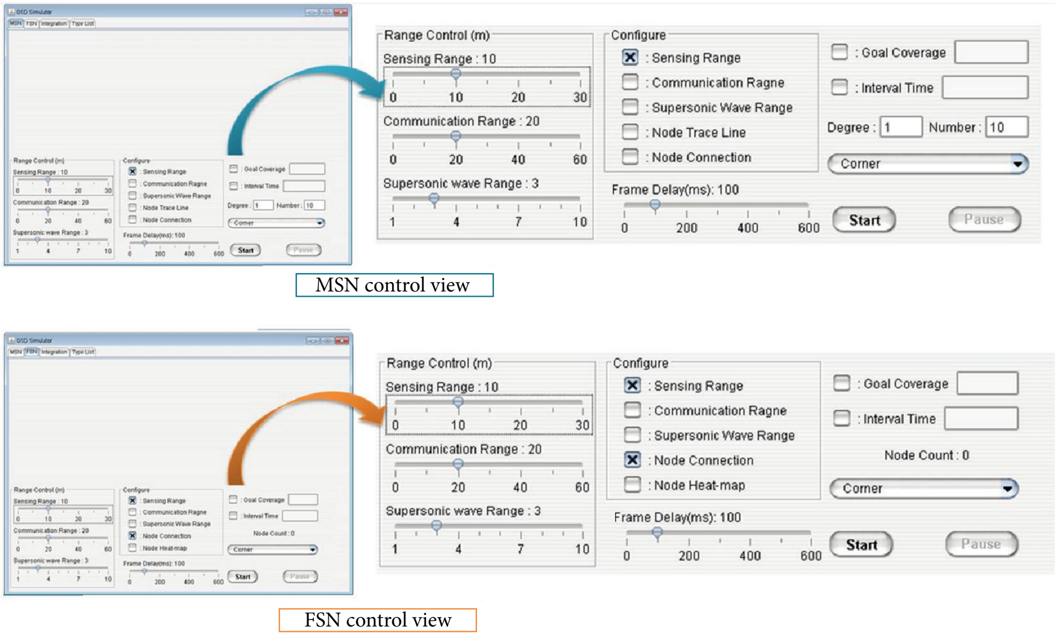


Figure 2: Module Components of DSDs.

sensing ranges and sensing types, Active Interval Time (A_IT) that shows the operating periods of sensors, Active Operator Time (A_OT) that shows operating times when sensors are in the active mode, Sleep Operator Time (S_OT) that shows operating times when sensors are in the sleep mode, Communication Max Ranges (CMRs) that show maximum communication ranges between sensors, and Communication Default Range (CDR) that shows the ranges of basic communication between sensors. MSNs are composed of Move Consumption (MC) that shows the amount of battery consumption during movements; Active Consumption (AC) that shows the amount of battery consumption when sensors are in the active mode; Sleep Consumption (SC) that shows the amount of battery consumption when sensors are in the sleep mode; the Formula of Battery Remaining (FBR) that shows a formula for obtaining the residual battery capacity of diverse sensors such as temperature, humidity, magnetic field, and sound sensors; and the Life Prediction of Battery (LPB) that predicts and shows lifecycles from the viewpoint of batteries in proportion to the residual battery capacity and operating time, which is calculated through the FBR when sensor nodes operate independently in cases where simulations are conducted.

The *Coordinate Converter Component* plays the role of processing and transmitting basic information on topography and nodes and data on their operating situations so that the information data can be displayed on the Viewer. The *Viewer Component* provides the data received through the Coordinate Converter to the user as visual information. The *Viewer Component* is composed of a Map Viewer for showing topography, an MSN Viewer that shows the situation of operation of MSNs and Mobile Sensor information, an FSN Viewer that shows the situation of operation of FSNs and Fixed Sensor information, and an Integration Viewer that shows MSNs and FSNs together so that they can be compared and analyzed.



Range Control (m)
Sensing Range : 10
0 10 20 30
Communication Range : 20
0 20 40 60
Supersonic wave Range : 3
1 4 7 10

Configure
☒ : Sensing Range
□ : Communication Ragne
□ : Supersonic Wave Range
□ : Node Trace Line
□ : Node Connection

Frame Delay(ms): 100
0 200 400 600

□ : Goal Coverage
□ : Interval Time
Degree : 1 Number : 10
Corner
Start Pause

MSN control view

Range Control (m)
Sensing Range : 10
0 10 20 30
Communication Range : 20
0 20 40 60
Supersonic wave Range : 3
1 4 7 10

Configure
☒ : Sensing Range
□ : Communication Ragne
□ : Supersonic Wave Range
☒ : Node Connection
□ : Node Heat-map

Frame Delay(ms): 100
0 200 400 600

□ : Goal Coverage
□ : Interval Time
Node Count : 0
Corner
Start Pause

FSN control view

Figure 3: Control view of MSN and FSN.

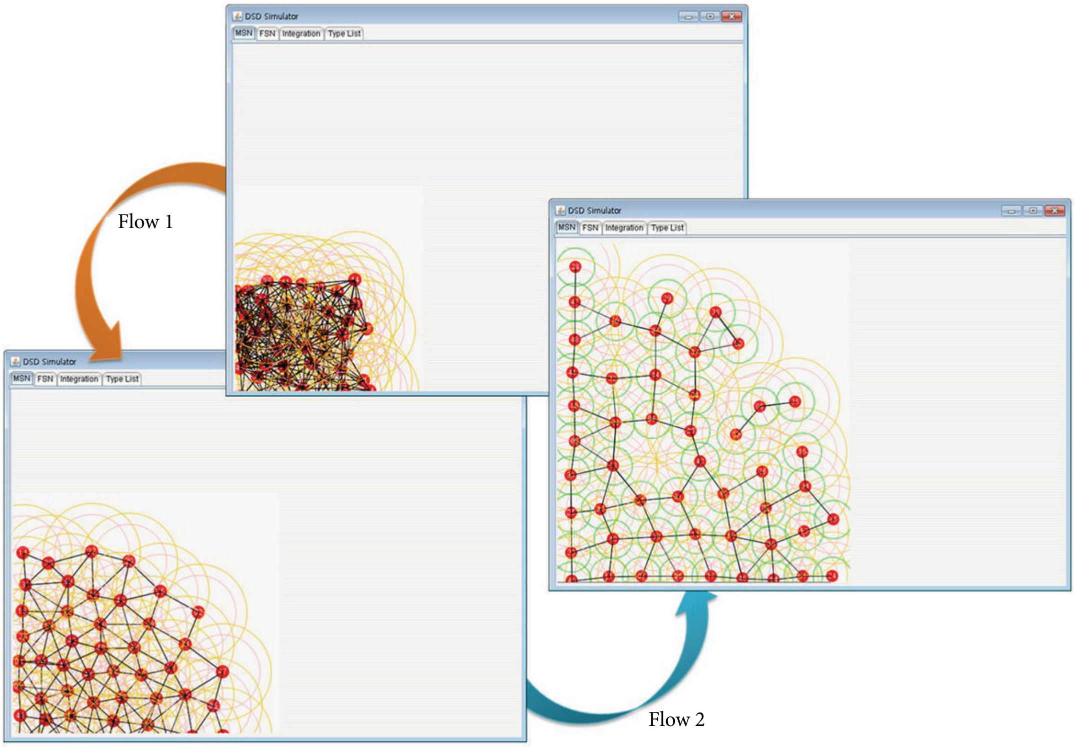


Figure 4: Moving sensors in MSN execution.

5. Implementation of DSDs

The DSDs are composed of MSN Views, FSN Views, Integration Views, and Type List Views. Figure 3 shows a screen of MSN and FSN controlled by the DSDs. The control screen is set to hidden as a default option. The hidden state can be released through a right mouse click on the View to control sensor nodes for MSNs and FSNs. MSN Control enables the selection of sensing ranges, communication ranges, the number of sensor nodes to be operated, the range to be displayed on the screen, and the state of connection. Whereas the number of sensor nodes should be entered in the case of MSN Control, sensor node locations can be directly set on the screen in the case of FSN Control. FSN Control basically

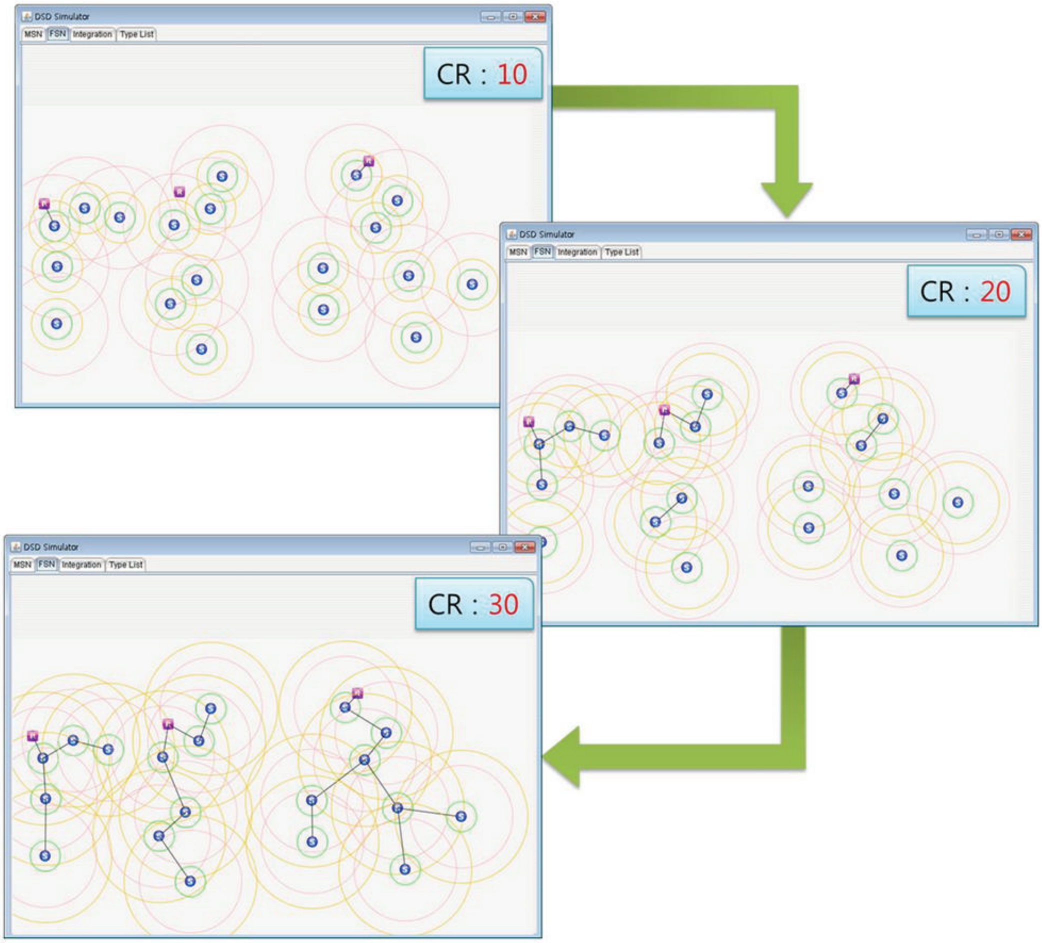


Figure 5: Operation of sensors in FSN execution.

provides the same functions as those provided by the MSN Control.

Figure 4 shows a screen of MSN operation that illustrates MSN movements.

Figure 5 shows a screen after selecting the FSN on the tab at the top to operate FSNs. For FSNs, the user sets the locations of sensor nodes individually. The CR in Figure 5 refers to the Communication Range between sensors and the number indicates the set range value. It can be seen that the view of communication between sensors varies with the value of the CR and that communication is possible only when the value of the CR is at least 30.

Figure 6 shows the results of implementation of the Integration function in order to compare MSNs and FSNs simultaneously. The left side of Figure 6 shows an MSN operation screen and the right side shows FSNs for which the user sets sensor locations. The screen shows that the MSN has set the number of sensor nodes to 100 and gradually covers the target topography. When the MSN has finally completed its coverage, the number of sensor nodes falling short in terms of covering the entire target topography can be inferred.

Figure 7 shows an execution screen where the user sets the definition of sensor types. The TYPE to select between MSN and FSN as sensor information, unique numbers of sensors, sensors' sensing functions, the Active Interval Time to enter the period of switching between the active and sleep modes, the Active Mode Operation Time and Sleep Mode Operation Time indicating the active and sleep mode operating times, the Communication Max Range indicating the maximum communication range between sensors, the Communication Default Range indicating the default communication range between sensors, basic sensor battery sizes, the rate of battery consumption during movements in the case of Mobile Sensors, the rate of battery consumption during the active state, and the rate of battery consumption during sleep states should be essentially entered while the residual battery capacity formula can be selectively entered by the user.

Figure 8 shows a list of the sensor types defined by the user as shown in Figure 7. The sensor types defined previously can be selected from the table for revision or deletion.

6. Conclusion and Future Research

The diverse sensor definable simulators (DSDs) proposed in the present paper are intended to provide frameworks in which various performances, including sensor arrangements

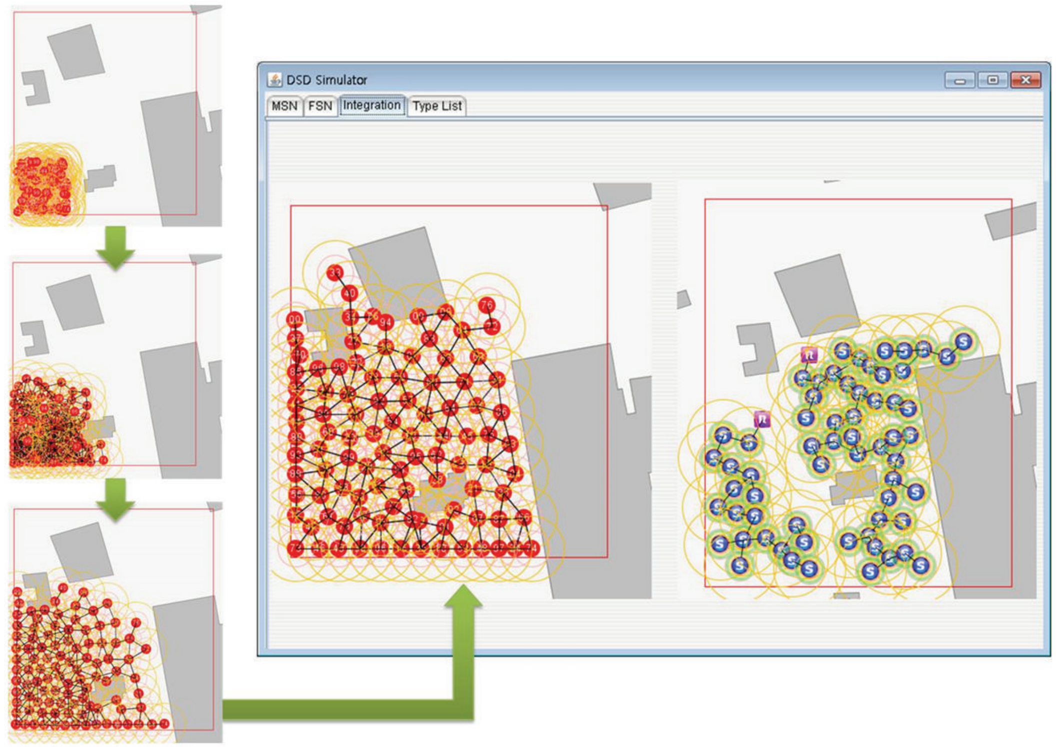
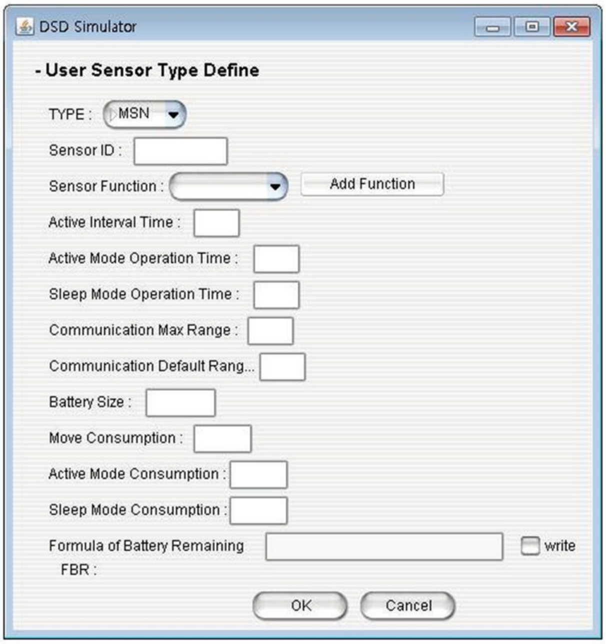


Figure 6: Integration of MSN and FSN execution.



- User Sensor Type Define

TYPE : MSN

Sensor ID :

Sensor Function : Add Function

Active Interval Time :

Active Mode Operation Time :

Sleep Mode Operation Time :

Communication Max Range :

Communication Default Rang...

Battery Size :

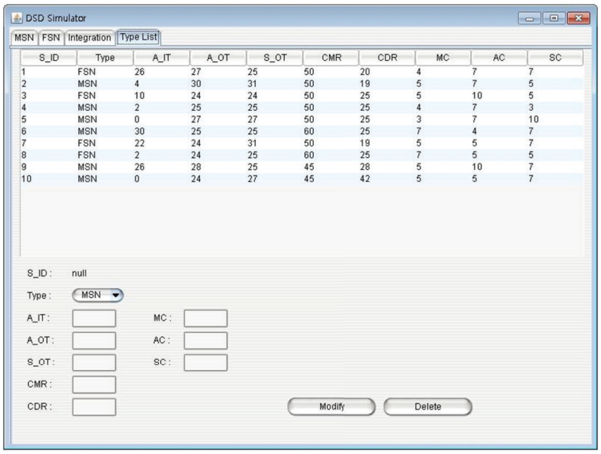
Move Consumption :

Active Mode Consumption :

Sleep Mode Consumption :

Formula of Battery Remaining FBR : □ write

Figure 7: User-defined sensor type.



S_ID	Type	A_IT	A_OT	S_OT	CMR	CDR	MC	AC	SC
1	FSN	26	27	25	50	20	4	7	7
2	MSN	4	30	31	50	19	5	7	5
3	FSN	10	24	24	50	25	5	10	5
4	MSN	2	25	25	50	25	4	7	3
5	MSN	0	27	27	50	25	3	7	10
6	MSN	30	25	25	60	25	7	4	7
7	FSN	22	24	31	50	19	5	5	7
8	FSN	2	24	25	60	25	7	5	5
9	MSN	26	28	25	45	28	5	10	7
10	MSN	0	24	27	45	42	5	5	7

S_ID : null

Type : MSN

A_IT :

A_OT :

S_OT :

CMR :

CDR :

MC :

AC :

SC :

Figure 8: Result of user-defined sensor types.

necessary for WSNs, can be simulated using diverse types of sensors such as temperature, humidity, magnetic field, and sound sensors. Basically, functions to define the sensor types were provided so that the functions could be implemented. Since existing simulators operate simulations for the same types of sensor nodes or conduct simulations using only the limited types and functions of sensors defined in the simulator, restricted results are necessarily obtained. The DSDs were able simulate the target topography consisting of various types of sensors through experiments of diverse sensors. Furthermore, they could conduct additional experiments of new sensors to be made later. In addition, defined sensors were stored as XML documents so that they can be used in various application programs and the sensor types defined by the user can be reused.

In future work, precise logs will be set in the DSDs and log visualization will be provided. By setting precise logs, users will be able to select the activity types of individual sensors, and log visualization functions for the selected activities will be provided so that users can make the best selection during different simulation implementation processes.

Acknowledgment

This research supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2013-H0301-13-4007) supervised by the NIPA (National IT Industry Promotion Agency).

References

[1] B. Musznicki and P. Zwierzykowski, "Survey of simulators for wireless sensor networks," *International Journal of Grid and Distributed Computing*, vol. 5, no. 3, pp. 23–50, 2012.

[2] J. Chen, M. B. Salim, and M. Matsumoto, "A single mobile target tracking in Voronoi-based clustered wireless sensor network," *Journal of Information Processing Systems*, vol. 6, no. 4, pp. 17–28, 2010.

[3] A. U. Bandaranayake, V. Pandit, and D. P. Agrawal, "Indoor link quality comparison of IEEE 802. 11a channels in a multiradio mesh network testbed," *Journal of Information Processing Systems*, vol. 8, no. 1, pp. 1–20, 2012.

[4] Y. Jeong, Y. Han, J. J. Park, and S. Lee, "MSNS: mobile sensor network simulator for area coverage and obstacle avoidance based on GML," *EURASIP Journal on Wireless Communications and Networking*, vol. 95, no. 1, pp. 1–15, 2012.

[5] GloMoSim, http://pcl.cs.ucla.edu/projects/glomosim.

[6] SNetSim, http://www.softpedia.com/get/Science-CAD/SNetSim.shtml.

[7] J. Polley, D. Blazakis, J. McGee, D. Rusk, J. S. Baras, and M. Karir, "ATEMU: a fine-grained sensor network simulator," in *Proceedings of the 2004 1st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, pp. 145–152, October 2004.

[8] Qualnet, http://web.scalable-networks.com/content/qualnet.

[9] The Network Simulator—ns-2, http://www.isi.edu/nsnam/ns/.

[10] L. Girod, J. Elson, A. Cerpa, T. Stathopoulos, N. R. Ramanathan, and D. Estrin, "Emstar: a software environment for developing and deploying wireless sensor networks," in *Proceedings of the 2004 USENIX Annual Technical Conference*, Boston, Mass, USA, August 2004.

[11] P. Levis, N. Lee, M. Welsh, and D. Culler, "TOSSIM: accurate and scalable simulation of entire TinyOS applications," in *Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems (SenSys '03)*, pp. 126–137, November 2003.

[12] "J-Sim: a simulation and emulation environment for wireless sensor networks," http://icserv.kjist.ac.kr/mis/publications/data/2006/01678171.pdf.

[13] B. L. Titzer, D. K. Lee, and J. Palsberg, "Avrora: scalable sensor networksimulation with precise timing," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*, pp. 477–482, Los Angeles, Calif, USA, April 2005.

[14] Java in Simulation Time/Scalable Wireless Ad hoc Network Simulator, http://jist.ece.cornell.edu/.

[15] G. Chen, J. Branch, M. J. Pflug, L. Zhu, and B. K. Szymanski, "SENSE: a wireless sensor network simulator," http://www.ita.cs.rpi.edu/publications/sense-book-chapter.pdf.

[16] J. Eriksson, A. Dunkels, N. Finne, F. Österlind, and T. Voigt, "Mspsim—an extensible simulator for msp430-equipped sensor boards," in *Proceedings of the European Conference on Wireless Sensor Networks, Poster/Demo session (EWSN '07)*, pp. 29–31, Delft, The Netherlands, January 2007.

[17] WSim, http://wsim.gforge.inria.fr/tutorials/wasp/distributed.html.

[18] P. Wightman and M. A. Labrador, "Atarraya: a simulation tool to teach and research topology control algorithms for wireless sensor networks," in *Proceedings of the 2nd International Conference on Simulation Tools and Techniques (SIMUTools '09)*, pp. 2–6, Rome, Italy, March 2009.

[19] WSNet Overview, http://wsnet.gforge.inria.fr/overview.html.

[20] J. Fontignie and A. Marculescu, "AlgoSenSim: developer's guide," 2006.

[21] L. Shu, C. Wu, and M. Hauswirth, "NetTopo: beyond simulator and visualizor for wireless sensor networks," Tech. Rep., Digital Enterprise Research Institute (DERI), Galway, Ireland, 2008.

[22] O. C. Ghica, "SIDnet-SWANS manual," March 2010, http://users.eecs.northwestern.edu/~ocg474/SIDnet/SIDnet-SWANS%20manual.pdf.

[23] S. Silas, K. Ezra, and E. B. Rajsingh, "A novel fault tolerant service selection framework for pervasive computing," *Human-Centric Computing and Information Sciences*, vol. 2, no. 5, pp. 1–14, 2012.

[24] X. Zhou, Y. Ge, X. Chen, Y. Jing, and W. Sun, "A distributed cache based reliable service execution and recovery approach in MANETs," *Journal of Convergence*, vol. 3, no. 1, pp. 5–12, 2012.

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 507605, 7 pages
http://dx.doi.org/10.1155/2013/507605

Research Article

A Sensor Positioning Scheme with High Accuracy in Nonuniform Wireless Sensor Networks

Junho Park,[1] Hyuk Park,[1] Dong-ook Seong,[2] and Jaesoo Yoo[1]

[1] *School of Information and Communication Engineering, Chungbuk National University, Cheongju, Chungbuk 361-763, Republic of Korea*
[2] *BOAS Electronics Inc., Industrial Technology Research Park, Cheongju, Chungbuk 361-763, Republic of Korea*

Correspondence should be addressed to Jaesoo Yoo; yjs@chungbuk.ac.kr

Received 8 April 2013; Accepted 21 May 2013

Academic Editor: James J. Park

In wireless sensor networks, a geographical positioning scheme is one of core technologies for sensor applications such as disaster monitoring, environment monitoring, and military services. For this reason, the research for range-free positioning schemes had progressing actively. And a density probability scheme based on the central limit theorem and normal distribution theory has been proposed to improve the location accuracy in nonuniform sensor network environments. The density probability scheme estimates 1-hop distance by using communication between nodes. After that, it estimates the final position of an unknown node. But the density probability scheme has a problem thatit has equivalent 1-hop distance for all of nodes in the same area. To overcome this problem, we propose a novel sensor positioning scheme in non-uniform wireless sensor networks. As a result, the proposed scheme ensures the high accuracy of sensor positioning in non-uniform networks. To show the superiority of our proposed scheme, we compare it with the existing scheme such as DV-based position scheme. Our experimental results show that the proposed scheme improves by about 36% sensor positioning accuracy over the existing scheme on average even in non-uniform wireless sensor networks.

1. Introduction

By the remarkable development of computing technologies, the ubiquitous environment has been served to provide human beings with more convenient life. This ubiquitous environment provides us with diverse and convenient services through the organic interaction among human beings, computers, and things. The wireless sensor network, one of basic technologies to detect the event and to control the external human environment in the ubiquitous environment, has been vigorously studied. The ad hoc wireless sensor network is constructed autonomously and collects diverse environment information through the communication among sensor nodes. A sink node receives sensing values from sensor nodes in sensing area and transmits them to a user. The collected information is used for diverse purposes such as observation of wildlife's habitat, military affair, fire detection, environmental monitoring, medical service, and U-City for application environment [1, 2].

In the sensor network, the positioning technology is one of the most required and basic technologies. In the positioning scheme using the wireless devices, every equipment is generally carrying the Global Positioning System (GPS) in order to collect positioning information. But it causes problems such as excessive energy consumption due to GPS modules and high costs for their construction in the large-scale sensor network environments [3, 4]. Therefore, the positioning schemes to reduce the energy consumption in the sensor network with limited energy have been actively studied.

Typical positioning schemes are classified into the range-based schemes and range-free schemes. The range-based schemes measure the position of sensor nodes by using signal strength or time difference between nodes and the range-free schemes measure the distance and estimate the position through the connection information between nodes and the position information of an anchor node without any subsidiary hardware equipments [5]. Recently range-free schemes have been proposed [6–9]. Unlikely range-based schemes, range-free schemes measure the distance and estimate the position through the connection information between nodes and the position information of an anchor node. In addition, it is efficient in the energy consumption and the cost to construct the network because only an anchor node is equipped with GPS module. Therefore, the positioning schemes through the anchor nodes have been actively studied. The existing schemes estimated the distance between nodes and decided the position in the uniform sensor network environments without considering density. However, in real applications, since sensors are distributed on the sensing fields randomly through aircrafts, missile, and so on, the nonuniform sensor network environments are constructed in specific areas [10]. Therefore, the positioning schemes for the uniform sensor network environments are not suitable for the actual situations since their error rates of density probability are very high in the non-uniform sensor network environments.

To solve the problem of the existing range-free schemes, we propose a novel positioning scheme by using the density probability model in the non-uniform network environment. In the proposed scheme, the minimum anchor nodes are used and the distance is estimated according to the density in the non-uniform sensor network environments. By doing so, the cost to construct the sensor network can be minimized and the positioning precision can be improved.

The remainder of this paper is organized as follows. Section 2 overviews the existing positioning schemes in the wireless sensor networks and analyzes their problems. In Section 3, we present our sensor positioning scheme using density probability models in non-uniform wireless sensor networks. Section 4 shows the simulated experiments and compares the existing scheme with the proposed scheme. Finally, we present concluding remarks in Section 5.

2. Related Work

2.1. Range-Based Positioning Schemes. Range-based schemes use absolute point-to-point distance or angle information to calculate positions between neighboring sensors using extra communication modules. After this, the node estimates position of unknown nodes by trilateration algorithm [11]. Common approaches for range-based schemes include Time of Arrival (ToA), Time Difference of Arrival (TDoA), and Angle of Arrival (AoA) for this algorithm [3]. ToA and TDoA measure signal arrival time or the difference of arrival times to calculate distance based on transmission time and speed. They can be applied to many different kinds of signals such as RF, acoustic, and ultrasound signals.

Range-based positioning schemes, such as ToA, TDoA, and AoA, suffer from the positioning errors since wireless channels are very sensitive to the surrounding environment when they use the strength and arrival time of each signal for positioning. ToA, TDoA, and AoA also have problems such as the usage of additional equipments, additional costs, and large energy consumption due to extra modules for a synchronization system among sensor nodes. Therefore, the range-based schemes in the wireless sensor network have a difficulty to positioning.

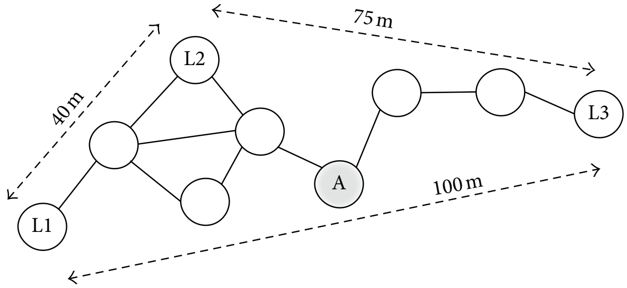


Figure 1: Example of DV-HOP estimated distance.

2.2. Range-Free Positioning Schemes. DV-HOP algorithm [7] and improved DV-HOP scheme [8, 9] are range-free and multi-hop routing positioning scheme in wireless sensor networks. They measure the positions of the unknown nodes by using the average distance of 1-hop between anchor nodes. DV-HOP algorithm is composed of steps as follows.

Firstly, each anchor node broadcasts a beacon frame containing its position with a hop-count value initialized to 0 to be flooded throughout the network. Then, the nodes that receive the information of anchor nodes store the cumulated hop counts from the anchor nodes to themselves and the positions of the anchor nodes. After that, all of the nodes calculate average 1-hop distance through the hop count from each anchor node to themselves. The average 1-hop distance of anchor node i is estimated using (1). Here h_{ij} is the minimum hop count of anchor nodes i and j, and (x_i, y_i) and (x_j, y_j) are their coordinates. As a result, C_{ij} is the calculated average 1-hop distance. In the example in Figure 1, nodes L1, L2, and L3 are anchor nodes. Consider

$$C_{ij} = \frac{\sum \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2}}{\sum h_{ij}}, \quad i \neq j. \tag{1}$$

In a similar manner, the estimated average distances of 1-hop of L2 and L3 are 16.42 m and 15.90 m, respectively. Unknown node A selects 1-hop distance of anchor node L2 as the average 1-hop distance since node L2 has the shortest path for the node A compared with nodes L1 and L3. And then, node A calculates the estimated distance from three anchor nodes, anchor nodes i, j, and k as (2). Finally, node A is assuming its position from three anchor nodes using trilateration. Consider

$$D_i = h_{ai} \times C_{ij}, \quad (i = 1, 2, 3 \ldots, n). \tag{2}$$

DV-HOP causes lower positioning error and uses fewer anchor nodes than the existing schemes However, in non-uniform environments where each area has a different density, DV-HOP causes higher positioning errors. DV-HOP should also distribute many anchor nodes to increase positioning accuracy. Therefore, we propose the node density probability model and the positioning scheme to overcome the problems of DV-HOP.

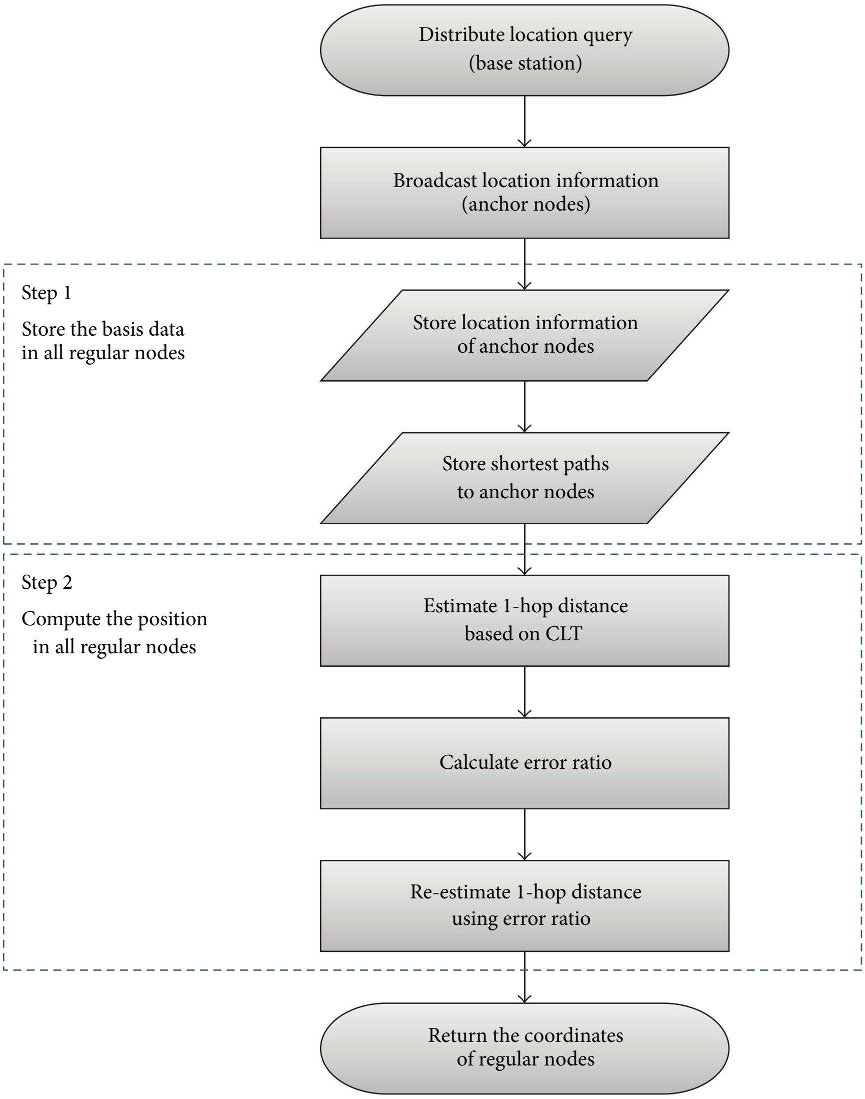


Figure 2: Flow chart of the proposed scheme.

3. The Proposed Sensor Positioning Scheme Based on Neighbor Density

In this paper, we propose a novel positioning scheme to reduce the positioning error and to decrease the construction costs in the non-uniform distributed sensor networks. The existing schemes cause very large positioning errors in each area with a different density. To reduce the positioning errors, it needs to distribute more anchor nodes in the network. However, it significantly increases the construction cost due to many anchor nodes. To solve this problem, the proposed scheme uses at least 4 anchor nodes placed at the boundary of the sensing fields. Thereby, the proposed scheme minimizes the cost of construction of the sensor network. Figure 2 shows the process of the proposed positioning scheme. First, when a position query is issued in the sensor network, the unknown nodes assume their distances through the information of the anchor nodes. Second, the distances of the unknown nodes are refined with distances between the anchor nodes and them. We explain steps 1 and 2 of Figure 2 in detail in Sections 3.2 and 3.3.

The proposed scheme is composed of the following four steps.

Step 1. The anchor nodes that exist in the boundary of the network broadcast their positions.

Step 2. The unknown nodes estimate the 1-hop distances of their neighbor nodes according to the densities of themselves and their neighboring nodes.

Step 3. Each node refines the estimated 1-hop distance by calculating distance error ratio between the real distances of anchor nodes and the relative distances through the shortest paths between anchor nodes.

Step 4. The unknown nodes estimate their positions by using the refined distance.

Table 1: Shortest path and neighbor node list.

Shortest path ID	Shortest path hop	Neighbor list
n_i	Cumulated hop	$n_i, n_{i+1}, \ldots, n_{i+n}$

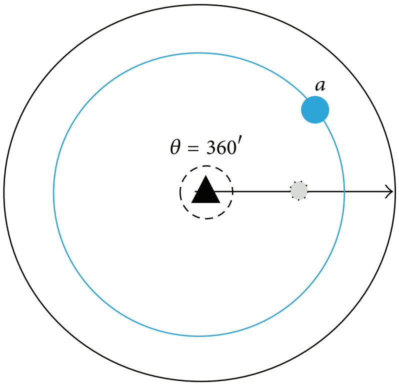


Figure 3: The estimated position of a sensor node.

3.1. Network Model and Characteristics. The anchor nodes A1, A2, A3, and A4 are deployed in each corner of the sensing area. In the initial step, anchor nodes broadcast their positioning information messages (node ID, hop, coordinates) to all the nodes. The normal sensor nodes save the information of the anchor nodes and neighbor nodes like Table 1.

3.2. Distance Estimation Considering Neighbor Density Probability. Each node estimates 1-hop distance by using Central Limit Theorem [12, 13] based on a normal probability distribution. The normal distribution or Gaussian distribution is a continuous probability distribution that has a bell-shaped probability density function. If the number of trials or samples objects increase, it shows the normal distribution curve. The theory that sensor network environment is consistent with the normal distribution model is the central limit theorem. The average of normal distribution model approximates to μ as the number of samples increases. In the sensor network environment where thousands of sensors are deployed, samples are located in the center of the normal distribution curve. Therefore, on the basis of the central limit theorem and the normal distribution model, each sensor node estimates the distances to the neighboring nodes. For 1-dimension, there is a point of the specific node that is an average of zero point. In other words, the point of 1/2 of the communication radius is the probability that node exists.

As shown in Figure 3, if the node draws a circle for the communication range and angle ($\theta = 360^\circ$), it is farther away than the estimated position of 1-dimension. Therefore, the estimated position for 2-dimension unlike the position of 1-dimension is a point in the circle that the area of its inner circle is equal to the area of its outer circle. As a result, it is possible to estimate the distance between nodes through the values of the normal distribution table.

Equation (3) is the distance calculation equation between neighbor nodes based on the values of the normal distribution table. R is a communication range of a sensor node and n is the number of its neighbor nodes. And then, the entire sensor nodes estimate the distance between them and their neighbor nodes through (3). It makes it possible to estimate more real distance in the non-uniform sensor network where the areas have different densities. Consider

$$d_{\text{Est}(k)} = \sqrt{\frac{\pi r^2/3}{\pi}} = \sqrt{\frac{r^2}{3}}, \quad n = 2,$$
$$d_{\text{Est}(k)} = \sqrt{\frac{r^2}{n+1}}, \quad n \geq 3. \tag{3}$$

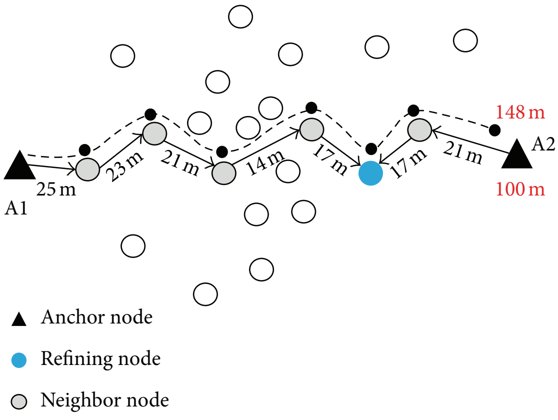


Figure 4: Correction of error rate for an estimated distance.

3.3. Error Correction of an Estimated Distance. If the position of a node is localized using the estimated distance, it has an error for shorter or longer than the real distance since the size of the whole network is not considered. As a result, the proposed scheme needs the correction to reduce the error rate of the estimated distance. Figure 4 shows the error rate of an estimated distance. A real distance between anchor node A2 and anchor node A3 is 100 m. However, the estimated distance through (3) is 148 m. Therefore, in order to correct the error between the real distance and the estimated distance, each node through (4) calculates an error rate for the accumulated distance of the two anchor nodes through their shortest path and their real linear distance.

And then, each unknown node refines the estimated distance through the error rate. Finally, the unknown nodes through 4 anchor nodes measure their positions with traditional trilateration. Consider

$$d_{\text{est}-\text{All}(k)} = \sum_{\text{Node ID}(k)=0}^{i} d_{\text{Est}(k)} + \sum_{\text{Node ID}(k)=0}^{j} d_{\text{Est}(k)}, \quad i \neq j,$$
$$d_{\text{Real}(i,j)} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2},$$
$$\text{error}\,(k) = \frac{d_{\text{Real}}}{d_{\text{Est}-\text{All}(k)}},$$
$$d_{\text{ref}(k)} = d_{\text{Est}(k)} \times \text{error}. \tag{4}$$

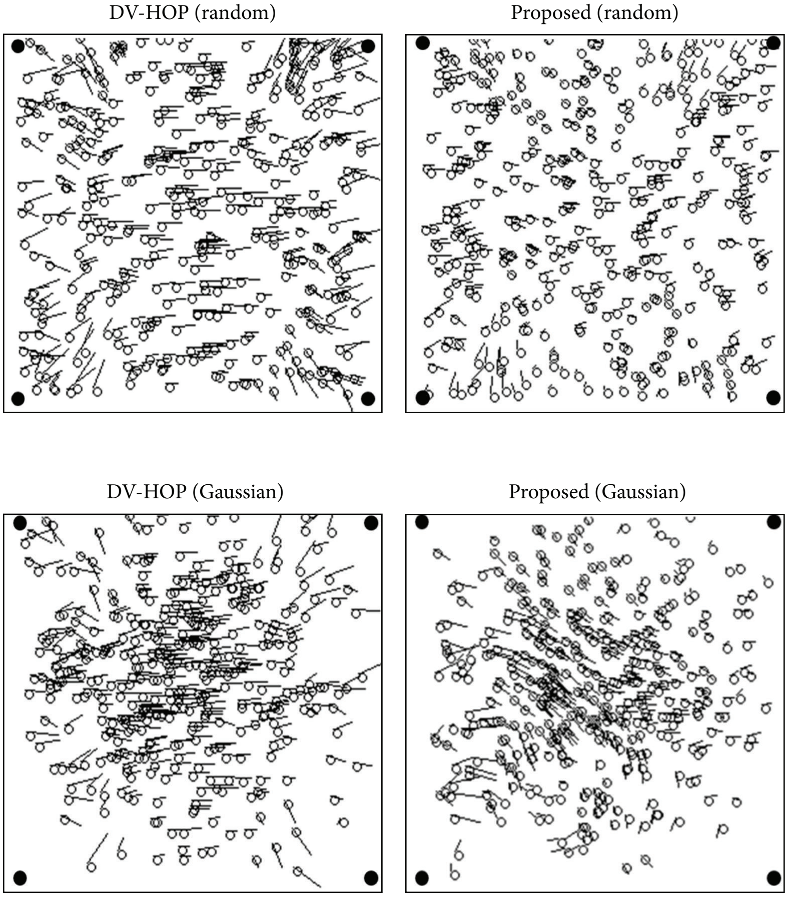


Figure 5: Comparison of localization results.

Table 2: Evaluation environment.

Parameter	Value
Size of sensor networks (m × m)	200 × 200
Number of distributed normal nodes	100~500
Number of distributed anchor nodes	4
Radius of communication (m)	10~30

4. Performance Evaluation

4.1. Network Environment. We have developed a simulator based on JAVA to evaluate our proposed scheme and the existing scheme, DV-Hop. The sensor network is based on random and non-uniform (Gaussian) models by considering the real distribution characteristics of sensors. Table 2 shows the evaluation environments. The size of the sensor network is a square area of 200 m × 200 m. Four anchor nodes are deployed at each corner of the sensing field and the number of sensor nodes is varied from 100 to 500. The communication ranges for sensor nodes and anchor nodes are 10 m, 15 m, 20 m, 25 m, and 30 m. The performance evaluation is performed based on J-Sim v.0.6.0 [14].

A positioning error rate is difference between a real coordinate and an estimated coordinate. Therefore, we evaluate the accuracy as the distance error rate between the real coordinate of a node and the coordinate of its estimated position. Equation (5) for a real distance and a positioning coordinate is used:

$$\text{Position Error } (\%R) = \frac{\sqrt{(x' - x)^2 + (y' - y)^2}}{r_{\max}} \times 100. \tag{5}$$

4.2. Performance Evaluation Results. Figure 5 shows the localization results of DV-HOP and the proposed scheme. As shown in Figure 5, our proposed scheme achieves better performance than the DV-HOP. In Figure 5, black points are anchor nodes and white points are unknown nodes. And, a black line is the distance between a real position and an estimated position. Simulation calculated the average error rates every ten times for the proposed and DV-HOP algorithms when the communication range is varied from 10 m to 30 m.

Figure 6 shows the average positioning error rate according to the communication range. With the same communication range, the position error rate of our proposed scheme is smaller than that of DV-HOP. In the case of DV-HOP, since the hop distance is proportional to the communication range, the accuracy of its positioning is low. In the random mode, the proposed scheme achieves about 30% performance improvements over DV-HOP in terms of the positioning

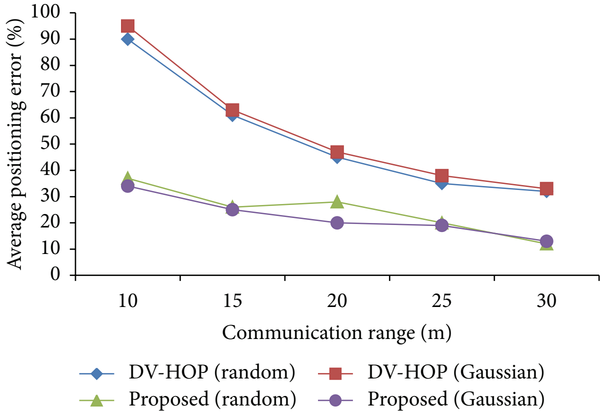


Figure 6: Average positioning error according to the communication range.

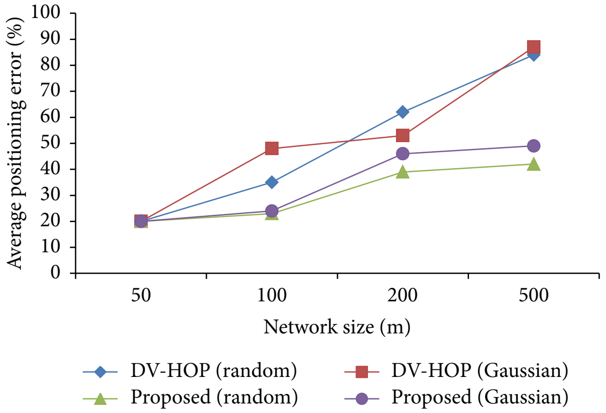


Figure 7: Average position error according to the network size.

accuracy. In the non-uniform model that has very large deviation of density, the proposed scheme achieves about 36% higher accuracy than DV-HOP. The reason is that the proposed scheme measures the positions of the nodes by considering their densities. As a result, our scheme improves the accuracy of positioning over the existing scheme.

Figures 7 and 8 show the average positioning error rate according to the network size and the number of sensor nodes. Figure 7 shows similar positioning error ratio for our scheme and DV-Hop in the small 50 × 50 scale network. However, the proposed scheme in the large 500 × 500 scale network improves the accuracy of positioning over DV-Hop. Figure 8 shows the average positioning error according to the number of total nodes. Our scheme improves the accuracy of positioning by about 49% over DV-Hop on average. Unlike DV-Hop, the proposed scheme shows the high position accuracy as each node has a different 1-hop distance. As a result, our scheme has an advantage that it can be applied to various environments because it has high accuracy in the large scale network as well as the small scale network.

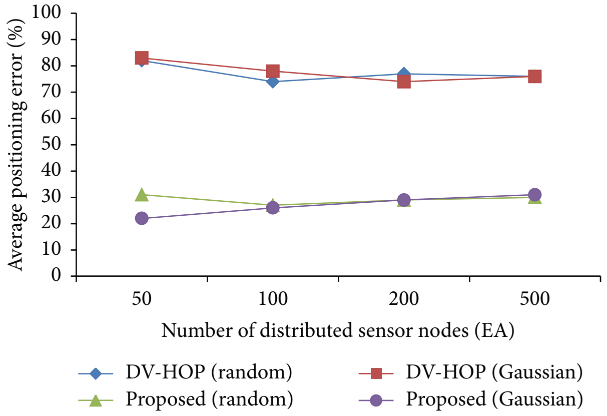


Figure 8: Average positioning error according to the sensor nodes.

5. Conclusion

In this paper, we have proposed the sensor positioning scheme using density probability models in non-uniform wireless sensor networks that considered characteristics of the sensor node deployment. The proposed scheme estimates the distance between nodes using the characteristics of density in non-uniform sensor network environments. The proposed scheme performs error correction between the estimated distance and the real distance. Therefore, it is possible to reduce the positioning error. As the results of performance evaluation, the proposed scheme showed that the positioning accuracy was significantly improved over the existing scheme. In the future work, we plan to extend our work to estimate the positions of sensor nodes in the case of network-hole occurrence.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012R1A1A2A10042015) and Technology Development Program for "Agriculture and Forestry" or "Food" or "Fisheries", and Ministry for Food, Agriculture, Forestry and Fisheries, Republic of Korea.

References

[1] G. Chatzimilioudis, D. Zeinalipour-Yazti, and D. Gunopulos, "Minimum-hot-spot query trees for wireless sensor networks," in *Proceedings of the 9th ACM International Workshop on Data Engineering for Wireless and Mobile Access (MobiDE '10)*, pp. 33–40, June 2010.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[3] G. Mao, B. Fidan, and B. D. O. Anderson, "Wireless sensor network localization techniques," *Computer Networks*, vol. 51, no. 10, pp. 2529–2553, 2007.

[4] E. Schlecht, C. Hülsebusch, F. Mahler, and K. Becker, "The use of differentially corrected global positioning system to monitor

activities of cattle at pasture," *Applied Animal Behaviour Science*, vol. 85, no. 3-4, pp. 185–202, 2004.

[5] J. J. Caffery Jr., "New approach to the geometry of TOA location," in *Proceedings of the 52nd Vehicular Technology Conference (VTC '00)*, vol. 4, pp. 1943–1949, September 2000.

[6] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom '03)*, pp. 81–95, September 2003.

[7] D. Niculescu and B. Nath, "DV based positioning in Ad Hoc networks," *Telecommunication Systems*, vol. 22, no. 1–4, pp. 267–280, 2003.

[8] W.-W. Ji and Z. Liu, "An improvement of DV-Hop algorithm in wireless sensor networks," in *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '06)*, pp. 1–4, September 2006.

[9] H. Chen, K. Sezaki, P. Deng, and H. C. So, "An improved DV-Hop localization algorithm with reduced node location error for wireless sensor networks," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E91-A, no. 8, pp. 2232–2236, 2008.

[10] P.-H. Huang, J.-L. Chen, Y. T. Larosa, and T.-L. Chiang, "Estimation of distributed fermat-point location for wireless sensor networking," *Sensors*, vol. 11, pp. 4358–4371, 2011.

[11] F. Thomas and L. Ros, "Revisiting trilateration for robot localization," *IEEE Transactions on Robotics*, vol. 21, no. 1, pp. 93–101, 2005.

[12] O. Johnson, *Information Theory and the Central Limit Theorem*, World Scientific, 2004.

[13] A. William, *Central Limit Theorem*, International Encyclopedia of the Social Sciences, 2008.

[14] J-Sim, http://www.j-sim.zcu.cz/.