

Research Article

Aggregation Scheme with Secure Hierarchical Clustering for Wireless Sensor Networks

Tung-Shih Su,¹ Mei-Wen Huang,² Wei-Shou Li,³ and Wen-Shyong Hsieh^{2,3}

¹ Department of Information Management, Fortune Institute of Technology, No. 1-10, Nongchang Rd., Neighborhood 28, Lyouchiyou Village, Daliao Township, Kaohsiung County 831, Taiwan

² Department of Computer Science and Engineering, National Sun-Yat-Sen University, No. 70, Lienhai Rd., Kaohsiung 80424, Taiwan

³ Department of Computer Science and Information Engineering, SHU-TE University, No. 59, Hengshan Rd., Yanchao Dist., Kaohsiung City 82445, Taiwan

Correspondence should be addressed to Tung-Shih Su, tomjunk@ms37.hinet.net

Received 9 December 2011; Revised 16 April 2012; Accepted 12 May 2012

Academic Editor: Hasan Cam

Copyright © 2012 Tung-Shih Su et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In a large-scale wireless sensor network, a topology is needed to gather state-based data from sensor network and efficiently aggregate the data given the requirements of balanced load, minimal energy consumption, and prolonged network lifetime. In this study, we proposed a ring-based hierarchical clustering scheme (RHC) consisting of four phases: predeployment, parent-child relationship building, deployment, and member join phases. Two node types are distributed throughout the network: cluster head nodes (type 1 node) and general sensor nodes (type 2 node). The type 1 node has better battery life, software capability, and hardware features than the type 2 node; therefore, the type 1 node is a better cluster head than type 2 node. Due to our IP naming rules and type 1 nodes as cluster heads, public key cryptography, such as RSA (Rivest, Shamir, Adleman), or ECC (Elliptic Curve Cryptosystem), is easily implanted to our system to strengthen our security. The sink node is the only certification authority in our system, but n level cluster heads can be extended to n level certification authorities if needed, where n is maximum number of level.

1. Introduction

In recent years, wireless sensor networks have been studied in many different applications, including environmental monitoring, battlefield surveillance, and other domains. In each of these applications, global state-based data are collected by all sensors and periodically transmitted to a sink. Given their compactness and extremely low cost, wireless sensor nodes are often drained by the limited source.

Fortunately, most nearby sensors report very similar ambient parameters to base station; hence, these data can be aggregated and/or compressed before being relayed to base station. In addition to improving accuracy, data aggregation also substantially reduces energy requirements due to reduced network communication overhead.

Two optimization metrics are often used to prolong network lifetime. One minimizes total energy consumption, and the other maximizes the lifetime of the network node with

the shortest lifetime because a node failure can cause network partitioning and inaccuracies in sensing data.

To minimize energy consumption, nodes are partitioned into “clusters,” each with a cluster head belonging to a type 1 node and several member nodes belonging to type 2 nodes. The type 1 node has better battery life, software capability, and hardware features than the type 2 node. The network structure is also organized heterogeneously and hierarchically such that cluster head nodes are further classified into different levels, which achieves substantial energy savings, and employing the ring-based way of predeployment.

The cluster head nodes in the proposed scheme are deployed according to a predeployment process before deploying general sensor nodes. The predeployment is followed by a parent-child relationship building process in which each cluster head node follows a specific naming rule as described in later subsection. The deployment of type 2 nodes is also followed by a member join process.

The remainder of this paper is organized as follows. Section 2 presents related work. The proposed scheme is proposed in Section 3. Section 4 evaluates the performance of the proposed scheme. Section 5 concludes the study.

2. Related Work

Due to the technical difficulty and energy constraints on recharging sensor nodes, several approaches have been proposed to save energy and prolong network lifetime. Data aggregation makes use of the property that different local regions may report the same aggregated values to the information center.

Tiny aggregation (TAG) [1] processes perform aggregation by discarding irrelevant data and combining and compacting relevant data. Directed diffusion [2] proposes a new data-centric dissemination paradigm which organizes data according to attribute-value pairs. When a user requests data, it sends the interest for the data. Data matching the interest is then transmitted back to the requestor. Hence, energy savings can be achieved by selecting good paths and by implementing data aggregation.

Also, in order to prolong network lifetime, LEACH [3] uses a clustering technique by rotating the role of cluster heads for each time period; therefore, the total number of nodes remaining active exceeds that when using static clustering. Furthermore, Bhardwaj et al. [4] provided an upper bound on the lifetime of sensor networks to minimize energy dissipation by using an optimum number of relay nodes. The minimum energy consumed by transmitting from one sensor to next is characteristic distance, denoted by D_{char} , where $D_{\text{char}} = \sqrt[p]{\alpha_1/\alpha_2(p-1)}$, p is path attenuation exponent (usually ranging from 2 to 4), α_1 is electronic energy consumption coefficient, and α_2 is amplifier energy consumption coefficient.

Mhatre and Rosenberg [5] proposed two node types, one with more power for cluster head and the other for cluster member. Two communication modes were proposed (single hop mode and multiple hop mode both from sensors to cluster head), and the optimum numbers of cluster heads under single and multiple hop modes were determined supposed that from all clusters to base station need only one hop. Bandyopadhyay and Coyle [6] proposed a distributed algorithm for organizing sensors into a cluster of hierarchies to minimize the system energy consumed from general sensors to cluster heads and finally to sink node. Chen et al. [7] proposed EPAS and later hEPAS, which conserve energy by organizing cluster heads into a hierarchy in which each sensor node follows a two-phase pickup rule to be a cluster head in order to maintain the expected optimal cluster number at each level. In [8–11], the clustering technique is also used as an efficient method of improving network lifetime and is a primary metric for evaluating network performance.

There are several papers related to heterogeneous sensor networks except [5]. In [12], Matrouk and Landfeldt propose a routing protocol, based on temperature to which energy is transformed, by using heat conduction formulas. The protocol transforms the expected lifetime of each node into an

equivalent temperature, and then finds the hottest path from source node to sink in order to equalize the residual energy throughout the heterogeneous wireless sensor networks.

In hostile environment, solid and efficient synchronization scheme needs to be designed to defend against different kind of attacks. In [13], Du et al. present a secure and efficient time synchronization scheme for heterogeneous sensor networks (HSNs). The authors also propose a secure and efficient routing protocol for HSNs—Two Tier Secure Routing (TTSR) [14]. In [15] Du et al. present an efficient routing protocol based on the chessboard clustering scheme, which balances node energy consumption and significantly increases network lifetime.

In [16] Yang and Cardei propose a delay-constrained energy-efficient routing in heterogeneous wireless sensor networks in which the scheme consists of static sensor nodes, mobile and static super-nodes. Each source sensor, with data to be transmitted, selects the best relay supernode in its routing table so as to satisfy the delay requirements. Message is transmitted from source sensor to relay supernode by sensor-to-sensor way, and from relay node to sink by supernode-to-supernode way.

Since data aggregation is one key approach to extending lifetime of sensor networks, a number of paper are published. Adaptive aggregate tree [17] is proposed to dynamically transform the structure of the routing tree to improve the efficiency of data aggregation. The author of [18] introduces multiple-input turbo code to implement jointly source coding channel coding and data aggregation. Due to the character of multiple input sequences and implementation of partial interleaving, both memory size and access requirements are reduced.

The proposed data aggregation scheme in [19] employs an elliptic curve cryptography-based homomorphic encryption algorithm to offer data integrity and confidentiality along with hierarchical aggregation. In [20] Wu et al. present a Delay-Constrained Optimal Data Aggregation framework that considers the unique feature of traffic patterns and information processing at application nodes for energy saving. In [21] Ozdemir and Xiao investigate the relationship between security and data integrity process in wireless sensor networks. A taxonomy data aggregation protocol is given by surveying the current “state-of-the-art” work in this area.

A scheduling called Distributed Power Scheduling [22], a medium access control protocol which supports data aggregation, is proposed. It integrates data aggregation into power-mode scheduling in the MAC layer and effectively reduced packet delay. In [23] Solis and Obraczka explores in-network aggregation as a power-efficient mechanism for collecting data in wireless sensor networks. The authors evaluate the performance of different in-network aggregation algorithms in terms of tradeoffs between energy efficiency, data accuracy and freshness.

In [24] Wu et al. propose a secure aggregation tree (SAT) to detect and prevent cheating. Through the method which is without persistent cryptographic operations when all sensor nodes are working honestly, the energy and CPU source can be saved. In [25] Li et al. propose an efficient algorithm to solve the maximum lifetime many-to-one data gathering

with aggregation (MLMTODA) problem. In [26] Cheng and Yin propose a new balanced aggregation tree (BAT) for tree construction that can be used for aggregate data and nonaggregate data.

In [27] Kafetzoglou and Papavassiliou propose a framework which combines two different energy-saving methods from two different layers, application layer and Medium Access Control (MAC), by appropriately adopting sleeping mechanisms. In [28] Zou et al. introduce the concept of flow loss multiplier, which is dependent on the spatial relationship among sensed areas, to express the impact of data aggregation on the conveyed traffic. The approach based on in-network data aggregation at the First Hop away from each sensor data source, followed by flow-based routing of the resulting traffic, is proposed to extend the lifetime of wireless sensor networks (WSNs). In [29] the authors propose a routing protocol called the Clustering-Base Expanding Ring Routing Protocol (CBERRP) which mainly focuses on the network layer while integrating factors from other layers to gain the preferred performance. In [30] Stanford and Tongngam propose the approximation algorithm for the problem of maximizing sensor networks lifetime with data aggregation by applying Garg-Könemann algorithm.

In [31] the authors propose an idea of energy management by employing relay nodes in a wireless sensor network. The locations and data generation rates of sensor are predetermined by the application's sensor placement algorithm whose problem is a nonlinear programming. The algorithm determines the optimal locations of relay nodes which dissipate optimal energy so as to satisfy desired lifetime with minimum total energy of the entire network.

In [32] the authors superpose two types of clustered architectures of wireless sensor networks to yield ultra hierarchical structures. A secure aggregation protocol for sensor networks is derived from this architecture. The authors significantly improve the SAPC [33]. The clustered WSN of Sun et al. [34] is used as the cluster of level 1. A variant of the method for defining virtual architectures in [35] is developed to produce clusters of level 2 and higher. Base station is the only one which can be trusted, and it does not need to fulfill any aggregation process.

Ultra hierarchical cluster formation consists of three phases. In phase 1, the BS first generates a chain of key $K\{n/bs\}$ needed to perform broadcasts to all authenticated sensors. The BS then loads each sensor u with a unique identifier ID_u , a secret key $K_{bs,u}$ shared with itself for future communications in unicast, and the first key $K\{0/bs\}$ of its key chain for future broadcasts throughout the network by protocol μ TESLA [36]. In phase 2, the clusters of level 1 are formed by the protocol in [34]. This protocol uses the key $K_{u,v}$ established between two neighboring nodes u and v . Each node u also generates a string of keys $K\{n/u\}$ using its hardware cryptographic key and distributing the first key of the chain $K\{0/u\}$ to its neighbors by protocol μ TESLA. Finally, whenever a CH is determined, it sends a message to BS containing the list of members of this cluster. In phase 3, a virtual architecture [35] partition clusters of level 1 into clusters of level 2 or higher depend on two parameters C_a for angular coefficient (between 1° and 360°) and C_p for range

coefficient (between 0.1 and 1). The parameter C_a is used by BS to create angular sectors, and C_p is used by BS to create coronas.

Data aggregation also comprises three phases. The cluster heads do not achieve the aggregation but all the other members of their clusters do so as to promote the probability of overall honesty. In phase 1, BS generates two private key K1 for all non-CH nodes and K2 for all CH nodes. In phase 2, data aggregation is formed and passed from low level to higher level following eight steps recursively until phase 3: reception of data by the BS. During phase 2, each member except CH¹ (cluster head of level 1) sends to other members of its cluster with data encrypted by $K_{u,v}$ shared by node u and v . All the non-CH nodes carry out the aggregation of data received, and they encrypt the result with the private key K1. Then the encrypted data is sent to its CH¹ by authenticating the message by the key K_{u,CH^1} . Once this message is selected, the CH¹ will encrypt it with its key K2 and send the chain K2(K1(data)) to CH² by multiple-hop fashion unless CH¹ is equal to CH². The CH² distributes the decrypted message to all member of its cluster of level 1. These members are able to decrypt the message with their key K1, and those non-CH members carry out data aggregation process, encrypt the result with K1, and send to CH². CH² encrypts it with K2 and sends the chain K2(K1(data)) to CH³ by multiple-hop fashion unless CH² is equal to CH³. The procedure above will repeat until BS receives the final aggregation data.

Compared to scheme in [32], our proposed scheme RHC has two node types which are distributed throughout the network. The type 1 node has better battery life, software capability, and hardware features than the type 2 node does; therefore, the type 1 node is a better cluster head than type 2 node. Predeploying type 1 nodes at roughly certain positions can save many type 1 nodes to be distributed over the whole area. Due to their better battery life and aggregator roles, the whole system lifetime of network can also be extended. Besides, members of clusters which do not need to carry our aggregation can save a large amount of energy consumption of type 2 nodes. In [32] two types nodes with same battery life but different roles: CHs through election, members of clusters.

Once deployment process completes, the self-organization process is initiated by parent-child relationship building process and then member join process. Due to our hierarchical structure which is well suitable for public key cryptography, the use of public key cryptography can ease many problems during the data delivery processes, for example, authentication, integrity, and nonrepudiation. Public key infrastructure can also easily be applied to future new public key cryptography. Any node in our system only needs two keys (a public key and a private key); therefore, the total keys of our system are less than those in [32].

In our proposed scheme, it has the following characteristics:

- (1) Heterogeneity,
- (2) multilayer hierarchical structure,

- (3) IP naming way,
- (4) public key infrastructure.

3. Proposed Scheme

As noted above, the proposed network employs two types of nodes: cluster head nodes and general sensor nodes. In the one-level data aggregator mechanism (only one hop is required from the farthest cluster head to sink), the sink is located at the center of the region (red circle), as Figure 1 shows. For being simple and easy to recognize, all sensor nodes in this structure are partitioned into seven clusters represented by black circles (actually each cluster range is larger than black circle), and each cluster has a cluster head.

The cluster range (radius), which is indicated by the region between the black circle and its concentric blue circle, is large enough to cover all type 2 nodes for all clusters. Each cluster head radius can be approximated as radius of the region divided by square root of cluster number as proposed in [37], which is larger than the radius of the black circle and less than the radius of blue concentric circle, and can enough cover all its own type 2 nodes. Like many other simulation modes, transmission power is assumedly adjusted to satisfy all transmission distances between nodes. The blue circle represents the communication range between two neighboring cluster heads. The cluster head collects data from their member sensors then aggregates, compresses, and sends the aggregated data to the sink. Therefore, the sink and each cluster head have a parent-child relationship which is determined by the parent-child relationship building process. The sink and each cluster head have several general sensors. The general sensors are randomly and uniformly distributed such that each cluster has approximately the same cluster members. Therefore, the energy consumption of the type 2 node is evenly consumed and thus minimized. This approach requires the six cluster heads to be deployed to respective around positions. The radius of the region is assumed to be R ; therefore, the six cluster heads are located around $2 * R/3$ away from the sink, and the arc of two adjacent cluster heads is approximately $2 * \pi * (2 * R/3)/6$. Cluster heads gather, aggregate, compress, and send data to the sink whereas general sensors send and transfer data to their own cluster heads. Next, a two-level data aggregator mechanism (the farthest cluster head and the sink are two hops apart) is described.

In Figure 2, for being simple and easy to recognize, each cluster is also represented by a black circle. In fact, the range of a cluster is larger than the black circle, and all the clusters cover the area of whole deployment region. In the two-level hierarchical structure, the first level has six clusters, and the second level has twelve (because the distance from level 2 cluster head to sink is twice that from level 1 cluster head to sink); that is, the sensor nodes are partitioned into nineteen clusters (including the sink). The six first-level cluster heads are located around $2 * R/5$ away from the sink, and the arc of two adjacent cluster heads is approximately $2 * \pi * (2 * R/5)/6$. The twelve second-level cluster heads are located around $4 * R/5$ away from the sink,

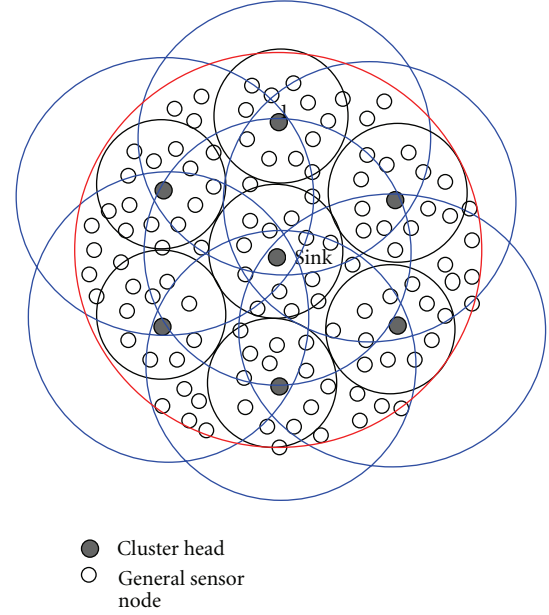


FIGURE 1: One-level hierarchy.

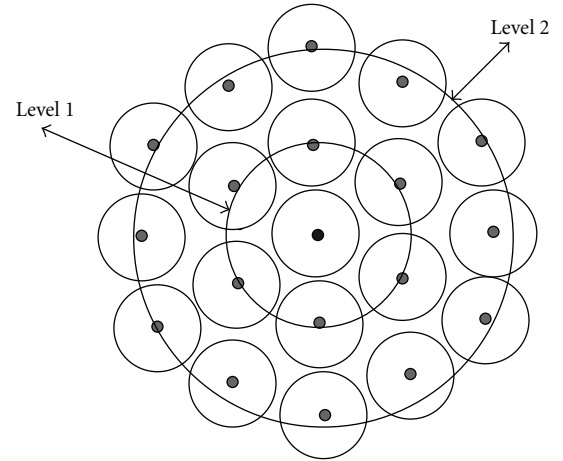


FIGURE 2: Two-level hierarchy.

and the arc of two adjacent cluster heads is approximately $2 * \pi * (4 * R/5)/12$. Notably, in the one-level structure, the distance from the level one cluster head to sink is around $2 * R/3$ whereas, in the two-level structure, the distance from level one cluster head to sink is around $2 * R/5$. This configuration provides a concentric distribution of cluster heads throughout the region. By doing so, the system life time is long when considering one failure node metric. Since the proposed scheme is also following a special naming rule, therefore the scheme also satisfied the total consumption metric [38].

Generally, in L -level hierarchical structure (L hops are required from the farthest cluster head to sink), the level i cluster head number is $6 * i$. Level i cluster heads are located around $(2 * i) * R/(2 * L + 1)$ away from the sink. The arc of

two adjacent cluster heads is approximately $2 * \pi * [(2 * i) * R / (2 * L + 1)] / 6 * i$. Organizing network as a ring-based wireless sensor network has advantage of energy savings because the clusters at outer ring always forward data to clusters at inner ring.

After the predeployment and deployment process, the parent-child relationship building process and the member join process are performed, respectively. Those processes employ an IP naming rule, which is described in the later subsection.

3.1. Predeployment Process. This study assumes that the network has only one sink located at the center of the circle region although the scheme can also be applied to other region shapes with many sinks. During this period, the cluster head nodes (type 1 nodes) are roughly deployed at certain positions ring by ring surrounding the sink, depending on how many levels are distributed. Figures 1 and 2 are examples of a one-level and a two-level hierarchy, respectively.

3.2. Deployment Process. During this period, all type 2 sensor nodes are randomly and uniformly distributed over the region. The nodes join their cluster head nodes after receiving cluster head signals based on the member join mechanism described in the next subsection.

3.3. Parent-Child Relationship Building and Member Join Process. In the parent-child building process, the sink node initiates the process by issuing a signal and then asking other nearby nodes (type 1 nodes) to become its subroot child nodes. If the value of received signal strength (RSS) received by nearby type 1 node is within the acceptable threshold range depending on distance between the two neighboring level, then the node becomes a subroot child node of the sink. After becoming a subroot child node or the descendants of the sink, each node has been assigned by the sink or the descendants of the sink can ask nearby unassigned nodes to become their subroot child nodes. If a type 1 node receives two or more signals requesting it to become a subroot child node, then the lowest level cluster head (the one nearest the sink) within RSS signal range is selected as its parent node; otherwise, the cluster head with the strongest and within RSS signal range becomes its parent node.

In the member join process, if a general node receives only one signal from a nearby cluster head, it joins this cluster as a member. If a general node receives two or more than two signals from nearby cluster heads simultaneously, it then becomes a member of cluster head with the strongest signal. After this process, the topology structure is complete.

3.4. IP Naming (Assignment) Rule. There are three reserved ranges in IP4 version:

10.0.0.0–10.255.255.255/8 (16,777,216 hosts)

172.16.0.0–172.31.255.255/12 (1,048,576 hosts)

192.168.0.0–192.168.255.255/16 (65,536 hosts).

We use first range as our addresses which are from 10.0.0.0 to 10.255.255.255. The first 8 bits of IP are always 00001010. Hence, the last 24 bits can be used for IP naming.

A simple but powerful naming rule is used to establish relations among all nodes in the parent-child relationship building and member join phases. Each node IP is named as follows. The last 24 bits of 32-bit IP are divided into eleven fields, My_IP(1)~My_IP(11). My_IP(1) is 1 bit long with value 0 or 1, and My_IP(2) is 3 bit long with values ranging from 0 to 7; My_IP(3)~My_IP(10) are 2 bits long with values ranging from 0 to 3; My_IP(11) is 4 bits long with values ranging from 0 to 15. If My_IP(11) is not 0, then the node must be a leaf node. Each node in the network is named by its parent (except the sink, which names by itself), and according to the named IP, each node can identify its level and its parent and child if any. The three different network roles, assuming only one sink, are as follows:

- (1) root node (sink): type 1 node,
- (2) subroot node (cluster head): type 1 node: all cluster heads except sink are subroot nodes, which are type 1 nodes,
- (3) leaf node (sensor node): type 2 node.

Root Node (Sink). The root node initiates the parent-child relationship building process. We assume that a type 1 node is adopted as a root node and placed at the center of the region. A value 1 is selected and assigned to My_IP(1), and the remaining fields are set to zero. Hence, every field except My_IP(1) is zero. In the proposed scheme the root node (sink) has six subroot child nodes (from My_IP(2), which has a maximum of seven and reserves 0 for root-node), which can be controlled and recorded by the root node. This feature is precious because, in a stationary multihop network, signal strength of a node is optimal when it has six neighboring nodes [39]. An example of a root node is the following. A node with an IP address 00001010(reserved) 1 000 00 00 00 00 00 00 00 0000 is a root node (sink) because My_IP(1) is 1 and the remaining fields from My_IP(2)~My_IP(11) are all 0. From My_IP(3) to My_IP(11) together are 20 bits which can be assigned to be a leaf node of root node except My_IP(2) that must be zero.

Subroot Node (Type 1 Node). A subroot node can become a child of another subroot node or a child of the sink. Further details can be found in [40]. For simplicity, only the condition in which a subroot node joins the sink and becomes its child node is described here. When a sink (e.g., node S) sends a signal to ask an unsigned type 1 node (e.g., node B) to become a child of the sink, S first assigns the IP of node B to that of node S and then adds an unused value (1 to 6) to the first zero field from left side of the IP of B. Once a node becomes a subroot node, it then signals other unsigned type 1 nodes to join and become its subroot child nodes. The sink can have a maximum of six subroot child nodes. For instance, the node with the IP address 00001010 1 001 00 00 00 00 00 000000 0000 is a subroot node of the sink and is a level 1 subroot node

because My_IP(1) and My_IP(2) are not 0, and the rest of the fields are all 0. In this example, from My_IP(4) to My_IP(11) together are 18 bits which can be assigned to be a leaf node of this subroot node except My_IP(3) that must be zero.

Leaf Node (Type 2 Node). When a subroot node requests a type 2 node to become a member of the subroot node, the subroot node first assigns the IP of the type 2 node to its own IP and adds an unused value to second zero My_IP field (first zero My_IP field must be zero) from left side to My_IP(11) to obtain the final IP of this leaf child node. For instance, the node with the IP address 00001010 1 001 00 00 00 00 00 00 00 0010 is a leaf node of level one because the My_IP(11) is not 0, My_IP(1) and My_IP(2) are not 0, and the remaining fields are all 0.

Having built all the relationships among all nodes, each leaf node knows who its parent is and should send sensed data to its parent (cluster head), and each subroot node aggregates and compresses received data and then sends to its parent. Finally all sensed data will be received by the sink. Wireless sensor network with IP naming rule has several advantages such as free role switching, fault tolerance, load balancing, and secure data transmission which are described in Section 3.6.

3.5. Energy Consumption of an L-Level Hierarchy. This subsection describes how total energy consumption of an L-level hierarchy structure in the proposed scenario is calculated according to transmission, aggregation, and compression. Table 1 lists the system notations used for measurement. The sink is assumed to be located at the center of the circular region A with radius R.

One-Level Hierarchy. An example of a one-level ($L = 1$) hierarchy is considered first. In a one-level hierarchy, the number of cluster heads, N_{ch} , is 7 as Figure 1 shows. The D_{char} is distance of the minimum energy consumed when sending signals from one sensor to the next. The D_c is the total distance traveled by all members to their common cluster head. Sensor data rate is b bits/cycle. Variable α_1 is the energy consumption coefficient for receiving and transmitting. Variable α_2 is the antenna energy consumption coefficient. Variable α is the energy consumed by sending one unit of data at distance of one unit. The cluster head radius can be approximated by $R / \sqrt{N_{ch}}$ in [37]. Let E_{ct1} denote total energy consumed by all sensor nodes transmitting data to their common cluster head at level 1. The E_{ct1} can be expressed as follows:

$$E_{ct1} = b * D_c * \alpha, \quad (1)$$

where $\alpha = (\alpha_1 + \alpha_2 * D_{char}^p) / D_{char}^p$,

$$\begin{aligned} D_c &= \left(\iint_{CH} r \, dx \, dy \right) * \frac{N_s}{\pi R^2} \\ &= \left(\iint_{CH} r r \, dr \, d\theta \right) * \frac{N_s}{\pi R^2} \end{aligned}$$

TABLE 1: System notation.

Symbol	Meaning
L	Level of the constructed tree
N_{ch-fl}	Number of cluster heads at first level
N_{leaf-c}	Number of leaf node per cluster
N_{ch}	Number of type 1 nodes which is dependent on value L
N_s	Number of type 2 nodes
A	Area of the deployment area
R	Radius of the deployment area
b	Sensor data rate
b_i	Data rate of a node at level i
D_c	Total distance from all cluster members to cluster head
D_{char}	Characteristic distance
E_{cti}	Single cluster energy consumption of data transmission at level i
E_{cai}	Single cluster energy consumption of data aggregation at level i
E_{cuai}	Single cluster energy consumption of data transmission from level i to $i - 1$
E_i	Total energy consumption at level i
E	Total energy consumption
$f_a(\cdot)$	Function of energy consumption of data aggregation
$f_c(\cdot)$	Function of data compression
α_1	Electronic energy consumption coefficient
α_2	Amplifier energy consumption coefficient
β	Coefficient of energy consumption of data aggregation
γ	Data compression rate
c	Data compression overhead
p	Path attenuation exponent

$$= \left(\frac{r^3}{3} * 2\pi \right) * \frac{N_s}{\pi R^2}, \quad r = \frac{R}{\sqrt{N_{ch}}},$$

$$N_{ch} = 7, \quad N_{leaf-c} = \frac{N_s}{N_{ch}}. \quad (2)$$

If E_{ca1} denotes the single cluster energy consumption of data aggregation at level 1,

$$E_{ca1} = f_a(b * N_{leaf-c}). \quad (3)$$

The data rate b_1 from level 1 cluster head to sink is

$$b_1 = f_c(b * N_{leaf-c}) + c. \quad (4)$$

The energy consumption E_{cua1} from level 1 cluster head to sink is

$$E_{cua1} = b_1 * 2 * \frac{R}{(2i + 1)} * \alpha = b_1 * \alpha * 2 * \frac{R}{3}, \quad (5)$$

where $i = 1$ because of level 1.

Since the first level cluster number is N_{ch-fl} , the total energy consumption E is

$$\begin{aligned} E &= (E_{ct1} * (N_{ch-fl} + 1)) + E_{ca1} * N_{ch-fl} \\ &\quad + E_{cua1} * N_{ch-fl}. \end{aligned} \quad (6)$$

Two-Level Hierarchy. For a two-level ($L = 2$) hierarchy, let E_{ct2} denote total energy consumed by all sensor nodes sending data to their cluster heads at level 2. The hierarchy can be derived as

$$E_{ct2} = b * D_c * \alpha, \quad (7)$$

where $\alpha = (\alpha_1 + \alpha_2 * D_{char}^p) / D_{char}^p$,

$$r = \frac{R}{\sqrt{N_{ch}}}, \quad N_{ch} = 19, \quad N_{leaf-c} = \frac{N_s}{N_{ch}}. \quad (8)$$

Also, let E_{ca2} denote the single cluster energy consumption of data aggregation at level 2, which is given as

$$E_{ca2} = f_a(b * N_{leaf-c}) \quad (9)$$

The data rate from level 2 cluster head to level 1 cluster head is $b_2 = f_c(b * N_{leaf-c}) + c$, and energy consumption from level 2 cluster head to level 1 cluster head is

$$E_{cua2} = b_2 * (2) * \frac{R}{(2i+1)} * \alpha = b_2 * \alpha * \frac{(2 * R)}{5}, \quad (10)$$

where $i = 2$ because of level 2.

The total energy consumption at level 2 is

$$E_2 = (E_{ct2} * (N_{ch-fl} * 2)) + E_{ca2} * N_{ch-fl} * 2 + E_{cua2} * N_{ch-fl} * 2 \quad (11)$$

because level 2 has $N_{ch-fl} * 2$ cluster heads.

Let E_{ct1} denote total energy consumed by all sensor nodes sending data to their cluster heads at level 1, which is given as

$$E_{ct1} = b * D_c * \alpha. \quad (12)$$

Because each cluster head has an average of two children other than the sink, E_{ca1} can be expressed as

$$E_{ca1} = f_a(b_2 * 2 + b * N_{leaf-c}). \quad (13)$$

Also, b_1 can be expressed as

$$b_1 = f_c(b_2 * 2 + b * N_{leaf-c}) + c$$

$$E_{cua1} = b_1 * (2) * \frac{R}{(2i+1)} * \alpha = b_1 * \alpha * \frac{(2 * R)}{5}, \quad (14)$$

where $i = 1$ because of level 1 and

$$E_1 = (E_{ct1} * (N_{ch-fl} + 1)) + E_{ca1} * N_{ch-fl} + E_{cua1} * N_{ch-fl}$$

$$E = E_1 + E_2. \quad (15)$$

L-Level Hierarchy. Let E_{ctL} denote total energy consumed by all sensor nodes sending data to their cluster heads at level L ($L > 2$), which is given as

$$E_{ctL} = b * D_c * \alpha. \quad (16)$$

The remaining energy consumption formulas are as follows:

$$E_{caL} = f_a(b * N_{leaf-c})$$

$$b_L = f_c(b * N_{leaf-c}) + c$$

$$E_{cuaL} = b_L * (2) * \frac{R}{(2L+1)} * \alpha$$

$$E_{ca(L-1)} = f_a(b_L * 2 + b * N_{leaf-c}) \quad (17)$$

$$E_{cua(L-1)} = b_{(L-1)} * (2) * \frac{R}{(2(L-1)+1)} * \alpha$$

$$E_{cai} = f_a(b_{i+1} * 2 + b * N_{leaf-c})$$

$$E_{cuai} = b_i * (2) * \frac{R}{(2i+1)} * \alpha.$$

For level L down to level 2, E_i is derived as

$$E_i = (E_{cti} * (N_{ch-fl} * i)) + E_{cai} * N_{ch-fl} * i + E_{cuai} * N_{ch-fl} * i. \quad (18)$$

For level 1, E_1 is expressed as

$$E_1 = (E_{ct1} * (N_{ch-fl} + 1)) + E_{ca1} * N_{ch-fl} + E_{cua1} * N_{ch-fl}. \quad (19)$$

In summary, total energy consumption is

$$E = \sum_{i=1}^L E_i. \quad (20)$$

3.6. Discussion. The proposed scheme has several advantages as follows.

(1) *No Switch for Role.* Type 1 nodes are cluster heads responsible for data aggregation, compression, and transmission to their upper layer (parent node); type 2 nodes are solely responsible for collecting and transferring sensed data to the cluster head. By avoiding cluster pickup and role switching, these node roles substantially reduce computation time.

(2) *Fault Tolerance.* In accordance with the naming rule, a subroot node can have at most three subroot child nodes. Generally, a subroot node allows only two subroot child nodes to become its child nodes. If a sibling subroot node malfunctions and then breaks the links with the sibling subroot child nodes, the subroot node can still assign one free IP address to one of the subroot child nodes of the sibling. As a result, fault tolerance is promoted. Additionally, by performing the parent-child building relationship and member join process, each general sensor node may receive two or three cluster head signals. Once its cluster head is out of function, a sensor node can try to join another nearby type 1 node.

(3) *Load Balancing.* By predeploying type 1 nodes and deploying type 2 nodes over the region, the burden of energy dissipation is evenly distributed amongst all sensor nodes. The upper layer cluster head nodes gradually become heavier than the lower layer cluster head. The lack of abrupt changes enables excellent load balancing.

(4) *Secure Data Transmission.* We use public key cryptography to strengthen our security. Our hierarchical structure is well suitable for public key cryptography. The use of public key cryptography can ease many problems during the data delivery processes, for instance, authentication, integrity, and nonrepudiation. After member join process, each node has an IP and knows its children if any, and also father IPs. Sink acts as trusted third party certificate authority T , whose public key (PK_T) is known to all valid nodes. A node L receives a certificate from T as follows:

$$T \rightarrow L : \text{cert}_L = [\text{IP}_L, \text{PK}_L, t, \text{exp}] \text{RK}_T. \quad (21)$$

The certificate contains the IP address of node L (IP_L), public key of node L (PK_L), created certificate time (t), and expire time of the certificate (exp). These variables are concatenated and signed by T 's private key (RK_T). Before a leaf node L sends its data to its father node, the data packet (DP) and a nonce N_L signed with L 's private key along with cert_L will be sent by node L to its father as follows:

$$L \rightarrow \text{broadcasting} : [\text{DP}, N_L] \text{RK}_L, \text{cert}_L. \quad (22)$$

The purpose of the nonce is to uniquely identify a data packet coming from a transmitter. For a cluster head node, it needs to decrypt all packets received from its children with their public keys, respectively, to aggregate its own packet and its children's nonduplicate packets, and to encrypt and send them to its father node. It should be noted that the father node IP of sender cannot be included due to that father and son have already known the addresses of each other. The data packets then will be safely sent to sink eventually.

4. Simulation Result

Table 2 shows the defined system parameters, which are referenced from [3, 5, 7]. The simulation is performed using java language. Ten thousand type 2 sensor nodes are uniformly distributed over a circular region with a 1000-meter radius. The aggregation function is $f_a(x) = \beta x$, where coefficient of energy consumption of data aggregation β is 5nj/bit, compression function is $f_c(x) = \gamma x + c$, compression ratio γ is 0.5, the path attenuation exponent is 2, and the overhead of data compression c is 50 bits. The simulated sending rate b is 4000 bits per cycle. In one type node hierarchical clustering protocol, sensors become cluster heads at each level according to the two-phase pickup rule; therefore, half of the members of a cluster head should be located between sink and their cluster head. Accordingly, these half members must send their aggregation data to their cluster head in a direction opposite to the sink. In our proposed protocol, the aggregation data are always sent to the sink, which significantly reduces energy requirements.

TABLE 2: System parameters.

Number of type 2 node	10000
Radius of the region A	1000 m
$\alpha 1$	$5 * 10^{-8}$ J/bit
$\alpha 2$	$1 * 10^{-10}$ J/bit/m ²
β	5 nj/bit
γ	0.5
c	50 bits
Sensor data rate b	4000 bits/cycle
$N_{\text{ch-fl}}$	6
$f_a(x)$	βx
$f_c(x)$	$\gamma x + c$

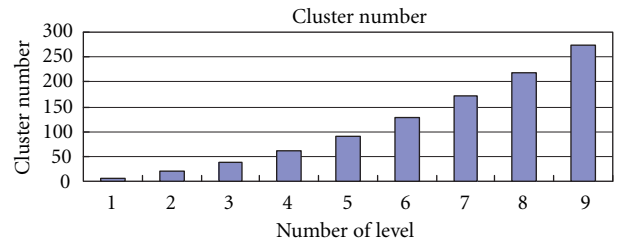


FIGURE 3: Relationship between number of level and cluster number.

Our proposed scheme has considered using two types of sensor node and also building multiple level hierarchies of cluster heads to reduce energy consumption. In order to compare with the other schemes, we also propose a uniform deployment single level scheme (USL) which also has two types of sensor node but from each cluster head to sink needs only one hop.

Figure 3 shows the number of cluster heads for different levels in the proposed scheme. Clearly, more type 1 nodes in the system enable more type 1 levels. In Figures 4 and 5, for RHC (proposed scheme) scheme the values of x-axis represent number of level while for USL scheme each value L_i , $i = 1, 2, \dots$, of x-axis represents the scenario which has the same number of type 1 nodes as that of RHC scheme at L_i level. Figure 4 shows the total energy consumption of the two schemes. Figure 5 also shows the maximum energy consumption of type 1 node in two different schemes. The number of type 1 and type 2 nodes is assumedly the same in the two schemes. However, the number of layers in these two schemes differs. Figure 4 reveals that the more levels or the more cluster heads the system uses, the lower the energy requirements for two different schemes. Although deploying more level needs more type 1 nodes and the predeployment process is more complicated and is more expensive, the system lifetime is much longer than one with fewer levels. As the total energy consumption metric in Figure 4 shows, shifting from a one-level to two-level hierarchy with twelve type 1 nodes can save 23.5 J. Shifting from two-level to three-level with twenty-four type 1 nodes can save 21.2 J. Shifting from three-level to four-level with forty-eight type 1 nodes can save 16.7 J. If a two-level or larger hierarchy

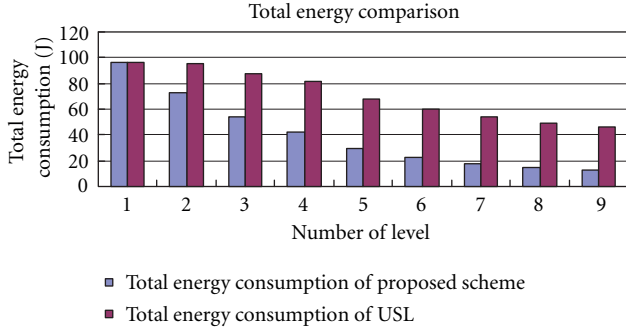


FIGURE 4: Total energy consumption for two different schemes.

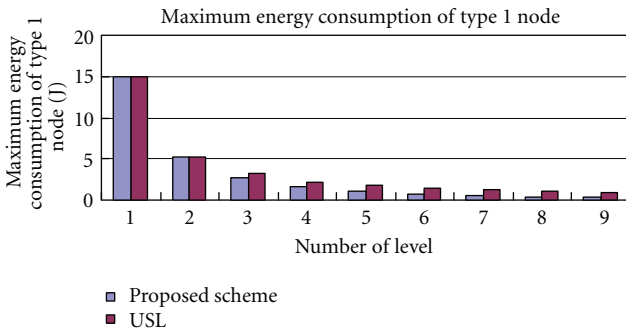


FIGURE 5: Maximum energy consumption of type 1 node for two different schemes.

is selected, then the lifetime is longer than that of the USL scheme with correspondingly similar cluster heads, as Figure 4 shows. However, for the first node failure metric, shifting from lower level to higher level has same tendency as the total energy consumption metric, if a three-level or larger hierarchy is selected, then the lifetime is longer than that of the USL scheme with correspondingly similar cluster heads, as Figure 5 shows.

Now we would like to investigate the ratio of lifetime and cost under different level for first type 1 node failure metric. Let N_{1i} denote the total number of type 1 nodes for i -level RHC, N_2 the number of type 2 nodes, P_1 price of type 1 node, P_2 price of type 2 node, C_{1i} maximum energy consumption of type 1 node for i -level RHC, LT_1 as maximum energy available for a type 1 node obtained among all level, LC_{1i} ratio of lifetime for type 1 node and cost for i -level RHC, then the LC_{1i} is as follows:

$$LC_{1i} = \frac{LT_1/C_{1i}}{(N_{1i} * P_1 + N_2 * P_2)}. \quad (23)$$

We assume that the price P_1 is 50 times the price P_2 which is 5 units, and LT_1 is 1000 J, and for each cluster, type 1 node will die before all type 2 nodes do. Figure 6 shows the experiment results of LC_{1i} for $i = 1$ to 9. Figure 7 shows the lifetime cycle gain by increasing one unit cost of type 1 node. From the figure we know from 2-level to 3-level can get the best lifetime cycle per unit cost of type 1 node.

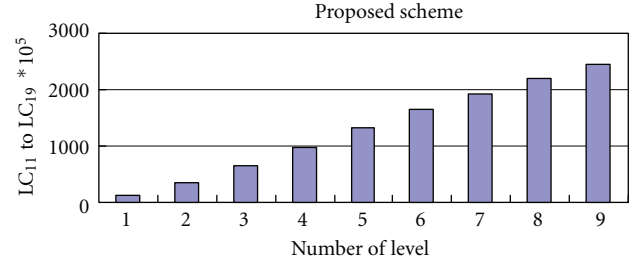
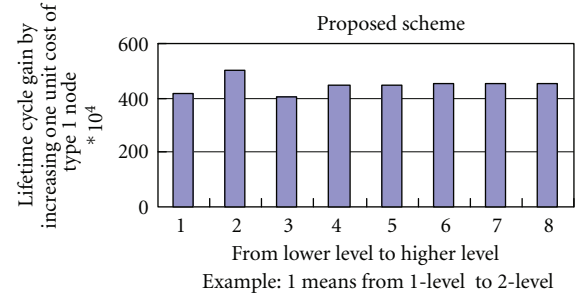
FIGURE 6: LC_{1i} from level 1 to level 9 using proposed scheme.

FIGURE 7: Lifetime cycle gain by increasing one unit cost of type 1 node.

5. Conclusion

This study proposed a ring-based scheme using two node types to organize a ring-based efficient hierarchical topology with many levels to optimize energy utilization. Type 1 nodes were first predeployed in approximate positions calculated by our formula. Type 2 nodes were then randomly and uniformly deployed over the circular region with the sink located at center of the area. The relationships between the sensor nodes were determined by the parent-child building and member join process. The three network roles are root-node, subroot node, and leaf node. Several simulations using the same system parameters but different levels demonstrate that the proposed scheme can achieve substantial energy savings. Due to our IP naming rules, public key cryptography is easily implanted to our system to strengthen our security. The sink node is the only certification authority in our system, and data can be sent to any node safely by the public key cryptosystem.

References

- [1] S. Madden, M. J. Frankin, J. Hellerstein, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," in *Proceedings of the 5th Symposium on Operating Systems Design and Implementation (OSDI '02)*, pp. 131–146, Boston, Mass, USA, December 2002.
- [2] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, pp. 2–16, 2003.
- [3] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless

- microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.
- [4] M. Bhardwaj, T. Garnett, and A. P. Chandrakasan, "Upper bounds on the lifetime of sensor networks," in *International Conference on Communications (ICC '01)*, pp. 785–790, June 2000.
 - [5] V. Mhatre and C. Rosenberg, "Design guidelines for wireless sensor networks: communication, clustering and aggregation," *Ad Hoc Networks*, vol. 2, no. 1, pp. 45–63, 2004.
 - [6] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies*, pp. 1713–1723, San Francisco, Calif, USA, April 2003.
 - [7] Y. P. Chen, A. L. Liestman, and J. Liu, "A hierarchical energy-efficient framework for data aggregation in wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 3, pp. 789–796, 2006.
 - [8] F. Kuhn, T. Moscibroda, and R. Wattenhofer, "Initializing newly deployed ad hoc and sensor networks," in *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom '04)*, pp. 260–274, September 2004.
 - [9] A. D. Amis, R. Prakash, T. H. P. Vuong, and D. T. Huynh, "Max-min d-cluster formation in wireless ad hoc networks," in *Proceedings of the 19th Annual Conference of the IEEE Computer and Communications Societies (INFOCOM '00)*, pp. 32–41, March 2000.
 - [10] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *Wireless Networks*, vol. 8, no. 5, pp. 481–494, 2002.
 - [11] S. Banerjee and S. Khuller, "A clustering scheme for hierarchical control in multi-hop wireless networks," in *Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies*, pp. 1028–1037, April 2001.
 - [12] K. Matrouk and B. Landfeldt, "Prolonging the system lifetime and equalising the energy for heterogeneous sensor networks using RETT protocol," *International Journal of Sensor Networks*, vol. 6, no. 2, pp. 65–77, 2009.
 - [13] X. Du, M. Guizani, Y. Xiao, and H. H. Chen, "Secure and efficient time synchronization in heterogeneous sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2387–2394, 2008.
 - [14] X. Du, M. Guizani, Y. Xiao, and H. H. Chen, "Two tier secure routing protocol for heterogeneous sensor networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 9, pp. 3395–3401, 2007.
 - [15] X. Du, Y. Xiao, and F. Dai, "Increasing network lifetime by balancing node energy consumption in heterogeneous sensor networks," *Wireless Communications and Mobile Computing*, vol. 8, no. 1, pp. 125–136, 2008.
 - [16] Y. Yang and M. Cardei, "Delay-constrained energy-efficient routing in heterogeneous wireless sensor networks," *International Journal of Sensor Networks*, vol. 7, no. 4, pp. 236–247, 2010.
 - [17] M. Chiang and G. T. Byrd, "Adaptive aggregation tree transformation for energy-efficient query processing in sensor networks," *International Journal of Sensor Networks*, vol. 6, no. 1, pp. 51–64, 2009.
 - [18] H. Cam, "Multiple-input turbo code for secure data aggregation and source-channel coding in wireless sensor networks," *International Journal of Sensor Networks*, vol. 2, no. 5-6, pp. 375–385, 2007.
 - [19] S. Ozdemir and Y. Xiao, "Integrity protecting hierarchical concealed data aggregation for wireless sensor networks," *Computer Networks*, vol. 55, no. 8, pp. 1735–1746, 2011.
 - [20] K. Wu, C. Liu, Y. Xiao, and J. Liu, "Delay-constrained optimal data aggregation in hierarchical wireless sensor networks," *Mobile Networks and Applications*, vol. 14, no. 5, pp. 571–589, 2009.
 - [21] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: a comprehensive overview," *Computer Networks*, vol. 53, no. 12, pp. 2022–2037, 2009.
 - [22] M. Moh, E. J. Kim, and T. Moh, "Design and analysis of distributed power scheduling for data aggregation in wireless sensor networks," *International Journal of Sensor Networks*, vol. 1, no. 3-4, pp. 143–155, 2006.
 - [23] I. Solis and K. Obraczka, "In-network aggregation trade-offs for data collection in wireless sensor networks," *International Journal of Sensor Networks*, vol. 1, no. 3-4, pp. 200–212, 2006.
 - [24] K. Wu, D. Dreif, B. Sun, and Y. Xiao, "Secure data aggregation without persistent cryptographic operations in wireless sensor networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 100–111, 2007.
 - [25] D. Li, Q. Zhu, and W. Chen, "Efficient algorithm for maximum lifetime many-to-one data aggregation in wireless sensor networks," *International Journal of Sensor Networks*, vol. 9, no. 2, pp. 61–68, 2011.
 - [26] M. X. Cheng and L. Yin, "Energy-efficient data gathering algorithm in sensor networks with partial aggregation," *International Journal of Sensor Networks*, vol. 4, no. 1-2, pp. 48–54, 2008.
 - [27] S. Kafetzoglou and S. Papavassiliou, "Energy-efficient framework for data gathering in wireless sensor networks via the combination of sleeping MAC and data aggregation strategies," *International Journal of Sensor Networks*, vol. 10, no. 1-2, pp. 3–13, 2011.
 - [28] S. Zou, I. Nikolaidis, and J. Harms, "Efficient aggregation using first hop selection in WSNs," *International Journal of Sensor Networks*, vol. 4, no. 1-2, pp. 55–67, 2008.
 - [29] Y. Jia, L. Zhao, and B. Ma, "A hierarchical clustering-based routing protocol for wireless sensor networks supporting multiple data aggregation qualities," *International Journal of Sensor Networks*, vol. 4, no. 1-2, pp. 79–91, 2008.
 - [30] J. Stanford and S. Tongngam, "Approximation algorithm for maximum lifetime in wireless sensor networks with data aggregation," *International Journal of Sensor Networks*, vol. 6, no. 1, pp. 44–50, 2009.
 - [31] S. C. Ergen and P. Varaiya, "Optimal placement of relay nodes for energy efficiency in sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '06)*, pp. 3473–3479, July 2006.
 - [32] S. Faye and J. F. Myoupo, "An ultra hierarchical clustering-based secure aggregation protocol for wireless sensor networks," *Advances in Information Sciences and Service Sciences*, vol. 3, no. 9, pp. 309–319, 2011.
 - [33] C. Bekara, M. Laurent-Maknawicius, and K. Bekara, "SAPC: a secure aggregation protocol for cluster-based wireless sensor networks," in *Proceedings of the Mobile Ad-Hoc and Sensor Networks (MSN '07)*, no. Lecture Notes in Computer Science, pp. 784–798, 2007.
 - [34] K. Sun, P. Peng, P. Ning, and C. Wang, "Secure distributed cluster formation in wireless sensor networks," in *Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC '06)*, pp. 131–140, December 2006.
 - [35] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, and K. Jones, "Training a wireless sensor network," *Mobile Networks and Applications*, vol. 10, no. 1, pp. 151–168, 2005.

- [36] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, pp. 189–199, July 2001.
- [37] R. Kershner, "The number of circles covering a set," *American Journal of Mathematics*, vol. 61, no. 3, pp. 665–671, 1939.
- [38] W. Liang and Y. Liu, "Online data gathering for maximizing network lifetime in sensor networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 1, pp. 2–11, 2007.
- [39] L. Kleinrock and J. Silvester, "Optimum transmission radii for packet radio networks or why six is a magic number," in *Proceedings of the IEEE National Telecommunications Conference*, pp. 1–5, Birmingham, Ala, USA, December 1978.
- [40] T.-S. Su, W.-L. Jeng, J.-Y. Huang, and W.-S. Hsieh, "A novel hierarchical ad hoc networks," in *International Conference on Networking and Services (ICNS '06)*, July 2006.

