Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 369502, 7 pages
http://dx.doi.org/10.1155/2013/369502

Research Article

Privacy Care Architecture in Wireless Sensor Networks

Kyong-Jin Kim[1] and Seng-Phil Hong[2]

[1] *Department of Computer Science, Sungshin Women's University, Seongbuk-gu, Seoul 136-742, Republic of Korea*
[2] *School of Information Technology, Sungshin Women's University, Seongbuk-gu, Seoul 136-742, Republic of Korea*

Correspondence should be addressed to Seng-Phil Hong; philhong@sungshin.ac.kr

Received 22 February 2013; Accepted 21 April 2013

Academic Editor: Tai-hoon Kim

With regard to the spread of innovative technologies, wireless sensor networks (WSNs) have great research interest in recent years. Although the WSN service is being facilitated, security related accidents are continuously incurring. In particular, many activities between mobile devices and sensor nodes take place without too much of protection of privacy information. To avoid these risks in WSN, we do need to devise the privacy care architecture to prevent the private data loss or breach especially in WSN. In this paper, we focus on WSN privacy issues with respect to mobile environments. We also suggest architecture to securely manage private data collected by WSN. It helps to protect the collected private data more efficiently and prevent the private data loss and breach.

1. Introduction

Wireless sensor networks (WSNs) or, in Korea, ubiquitous sensor networks, are mesh networks [1, 2] by which any tag node can signal to any other node provided it is in range. Another node automatically joins the network without human intervention [3]. It is important that a ubiquitous paradigm from anywhere, at anytime, access to a computing environment that can be expanded globally and oriented, and human-centered research and technology is one of the active. (See Figure 1 [4]).

WSNs are being used in a wide range of application areas [5]. The major application domains are environmental, medical, military, transportation, and smart spaces. According to the latest finding from the IDTechEx report "Wireless Sensor Networks 2012–2021" [6], WSN will grow rapidly to well over two billion US dollars for the systems in 2022. Figure 2 described that WSN market is expected to increase the revenues. They also note that the US dollar would reach over 1 billion in 2014.

The emergence of new technologies is more interested in WSN services. In particulars with regard to the spread of innovative technologies such as location-based services (LBS), smart phones, and smart pads, the applied sensor technology has great research interest in recent years. The growth of worldwide LBS market that use services including SNS and personal navigation began growing rapidly in 2008 and will reach US $8.2 billion in size by 2014, according to Gartner [7]. In this way, more significant is the continuing growth of sensor network services.

WSNs bring privacy challenges to a fundamental matter about a security vulnerability of wireless services during data collection and data transmission. Security and privacy issues in WSNs have been always part of research interest. Some works [8, 9] have focused on providing the core security services such as confidentiality, integrity, and availability. While these are security requirements, they are not sufficient to ensure the legal protection. In the case of Korea [10, 11], the protection of the private data to prevent the collective personal information has to be closely related to the government's regulatory efforts. Therefore, it is very important to understand the associated privacy regulations including location information on WSN. To achieve this, we can suggest controlling architecture for private data between the data protection technology and the related law and regulations.

The rest of this paper is organized as follows. In Section 2, we briefly describe principles based on the Korean privacy law and regulations for WSN and outline some related research. Section 3 discusses privacy concerns related to WSN services. Section 4 introduces our architecture, which

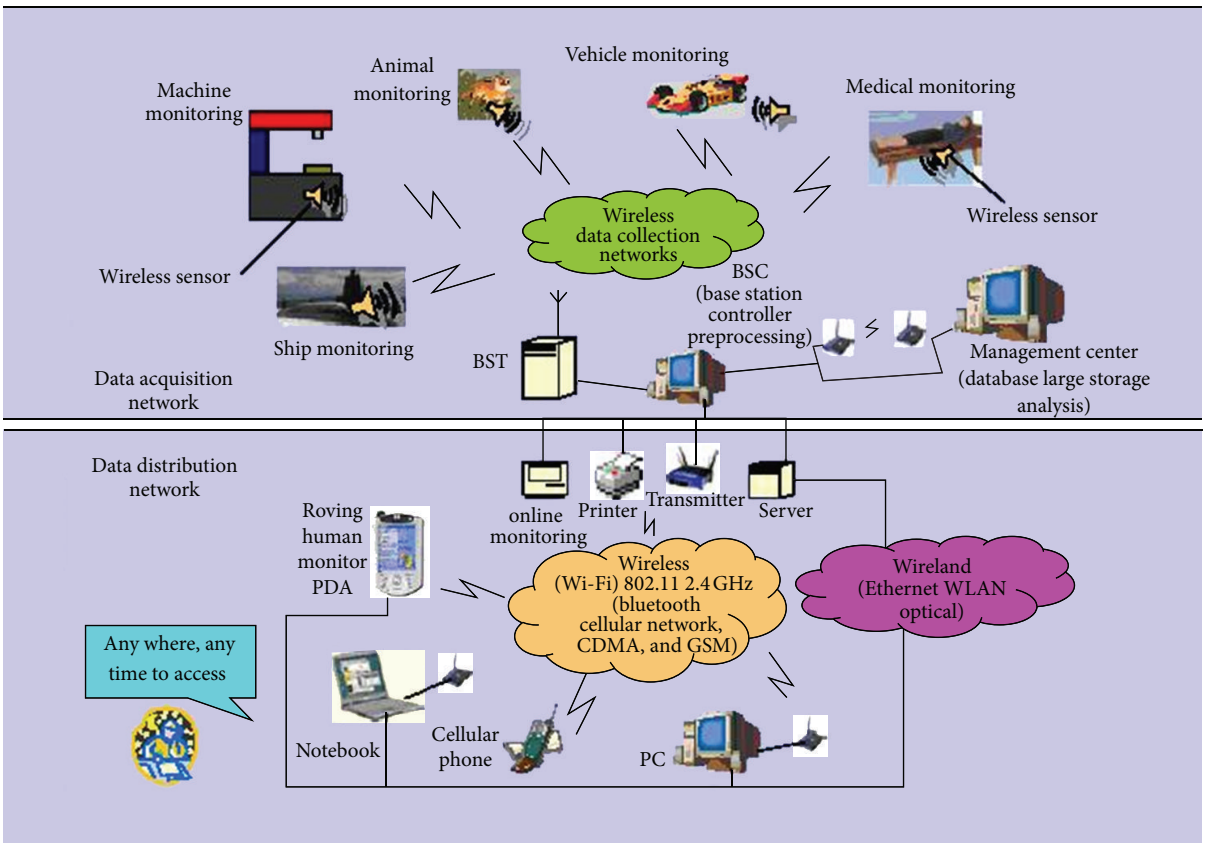

Figure 1: Wireless sensor networks architecture.

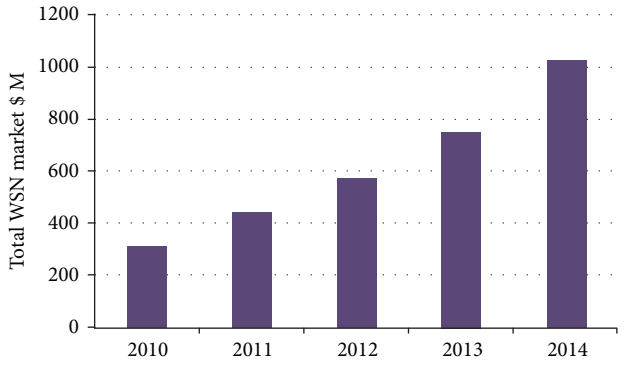

Figure 2: Total WSN market 2010–2014 ($ millions).

incorporates 3 key compositions for privacy protection in WSN, and we present an overall flowchart by leveraging the usability of our architecture. Section 5 presents the system performance through simulation. Finally, in Section 6, we conclude and discuss some ideas for future research work.

2. Background and Related Works

2.1. Korea Related Privacy Law for WSN. Privacy issues surrounding WSNs are becoming increasingly important aspects of society and are therefore important to the Korean government. The Korean government has established privacy related laws [10, 12] in order to protect the users' private data and location information.

There should be some rules in accessing the personal information on WSN.

2.1.1. Collect Personal Information Only What Is Necessary for Attaining the Purpose. In case the acquirer (or the service provider, the handler for data, etc.) wishes to collect private information by many sensors in WSN, it must obtain the consent of subjects. In particular, the unique identifying or sensitive information, such as a social security number, is not stored or is only used for encryption.

2.1.2. Use or Provision Only If Necessary. Except for cases where there was a consent of subjects, the acquirer may not use or provision private data collected by sensors beyond the scope specified or notified in the purpose or provide it for a third party. The reason is that accessing private data beyond necessity may burden the acquirer with compliance issue.

2.1.3. Data Collection and Transmission among WSN Nodes Are Critical. The private data often get accessed during the data collection and delivery. The acquirer must take security measures, such as designating those with access authority or using encryption. When the use purpose is accomplished, the acquirer must immediately destroy any private data collected by WSN.

2.1.4. Information on Owner's Rights Is Important. The information owner must be notified in case of a private data breach. Also, he or she may request the acquirer at any time to suspend or withdraw their personal information. In this case, he may not refuse this request.

These principles can be used by secure information management in WSN. In this paper, we are to focus on the private data collected by WSN and the individuals' sensitive information transferred from the relevant node to the acquirer, the service provider, and so forth.

2.2. Related Research Works. With the extensive application of WSN services, security and privacy issues have been always part of interest research.

Recently, in research works for WSN [8, 13, 14], more emphasis was given to WSN privacy issues. They discussed the method of various attacks and threats. They are also addressed that securing the WSN in general opinion needs to consider the classical security properties such as confidentiality, integrity, authenticity, and availability. Then, we can realize that privacy is the important part of WSN by these research works. Al Ameen et al. [15] discuss privacy issues and analyze their possible measures for healthcare applications. They also have specifically addressed security and privacy issues with respect to various environments. Practically, Dimitriou and Ioannis [16] discuss some security concerns and issues in biomedical sensor networks that need further consideration such as run-time composition of security services for practical sensor system. In order to build a reliable WSN for smart grid, Liu [17] presented an application of relevant cyber security and privacy issue and developed unified frameworks for identification of applications in smart grid.

Thus, the concern that many people have is how to remedy the problem of private data breach and protecting privacy information in WSN. Existing research in wireless sensor networks focused on the basic security features, but it does not meet to provide appropriate security features in wireless services when laws related to privacy were enacted.

Our work can be achieved mainly by focusing on the basic security features and the safety for compliance with the specific requirements. Also, we focus on WSN privacy issues with respect to mobile environments. We illustrate architecture to securely manage private data collected by WSN and also design the integrated system where we could link the protection method closely with the private data protection law and regulation in Korea. This architecture is to first verify that the user through authenticated connections, and it is to gather information regarding the way that the user is accessing the system in wireless networks, and it is to share data among validated WSN sensors.

3. Privacy Issues in WSN

Security for data integrity and accuracy, in particular privacy, is a critical issue in WSN. Many activities between mobile devices and sensor nodes take place without too much of protection of privacy information [4, 18, 19]. For example, the individual who uses services such as a location-based service and a geographic information system can access remote applications via wireless networks. In order to use services, the device may provide personal data to the acquirer.

However, use of services among WSN sensors has led to the danger of personal details including personal data and its location. In particular, road services can be linked to an individual according to current location of driver, and it has no difficulty to collect personal data on WSN. The danger of personal identity breach and the magnitude of its damage are more serious when malicious hackers are trying to steal collected data. Thus, it is clear that WSNs have privacy issues [1, 8, 9].

(i) *Data Collection*. The extensive application of WSN services, and in particular LBSs, provides a great convenience for people's lives. It is possible to access mobile users' location information anytime and anywhere, so most people who use LBS are due to convenience, but they cannot realize that the sensor was collecting their data during the service. The acquirer can gather unprecedented amounts of personal information. They may also collect more personal data than the minimum required for the purpose for which it is collected.

(ii) *Data Transmission*. In case WSNs allow for transmission of collected data to third party, although there are regulations that require consents by the information owner to such transfers, they are rarely enforced. Private data collected by a sensor can also be in other people's hands so easily when some people with malicious intentions are trying to steal data.

(iii) *Data Sharing*. The challenge in data privacy is to share data while protecting personally identifiable information [20]. In WSN, sensor nodes can also sense the physical movement and status related to an individual, and they are used for sharing sensed data. Then, because unknown people can access public sensor nodes, sharing on WSN can have a serious impact on an individual's activity.

To avoid private data disclosing risks in WSN, mobile devices need to consider whether any sensitive personal information is being collected or transferred. They also should review whether it is still necessary for the purpose for which it was collected.

4. Proposed Privacy Care Architecture (PCA) in WSN

In WSN, there are many data to be collected to use any given service. There are personal data to be collected and transferred during the service for a mobile device. The service provider sometimes requires sensitive or private information which includes mobile device data that are used for personal, and the mobile device may provide personal information to the acquirer in order to use services. In these processes for mobile services, there is concern over the potential dangers of wireless networking. Personal data can be collected and may

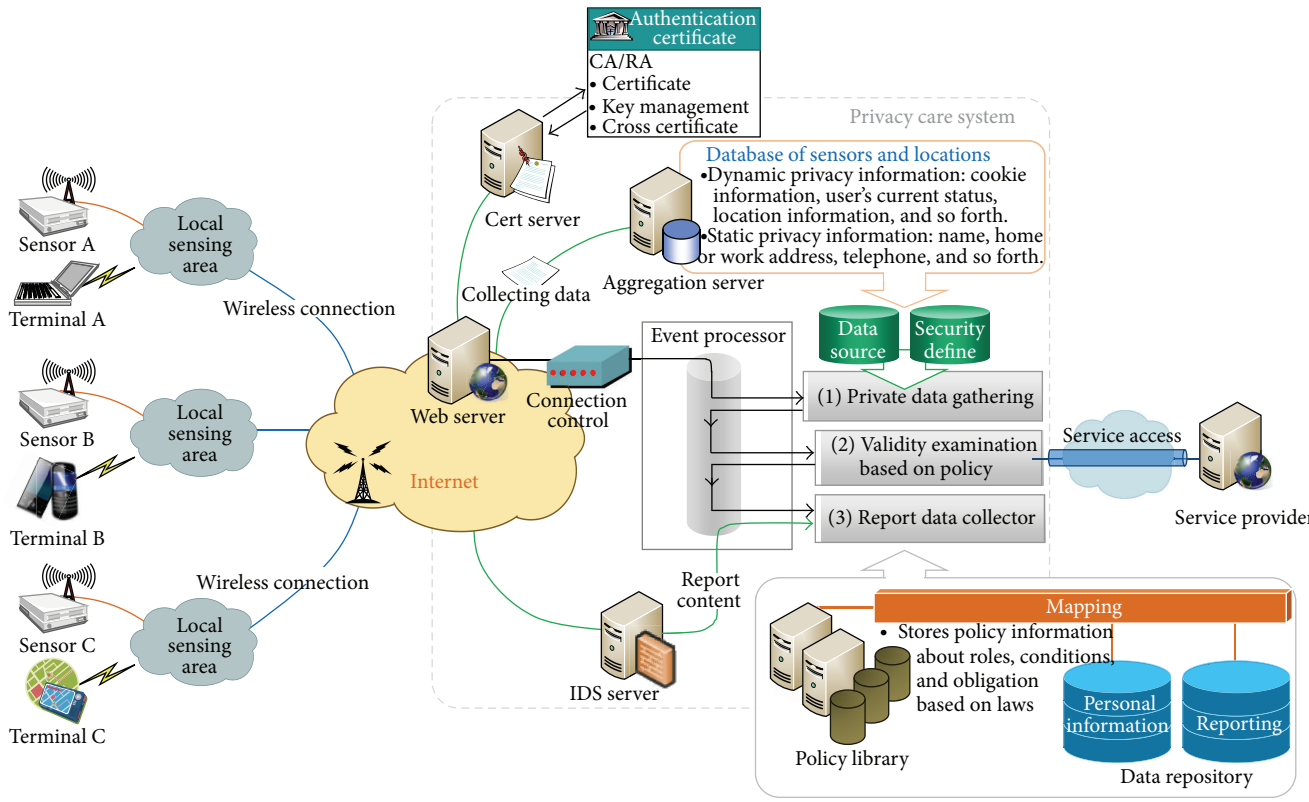

Figure 3: Framework of the privacy care architecture (PCA).

be transferred even without the knowledge of the information owners who use the service. In addition, the magnitude of its damage is more serious when malicious hackers are trying to steal collected personal information. For this reason, we do need to devise the privacy care architecture (PCA) to prevent the private data loss or breach especially in WSN.

We are proposing the PCA which is provided to data for secure transaction. To illustrate the concept, we provide the overview of process for protecting the private data as shown in Figure 3. The figure depicts how architecture works between users and service providers. The PCA for private data can be classified into major keys of (1) a private data gathering, (2) a validity examination based on policy, and (3) a report data collector.

WSN can overcome physical network infrastructure limitations, so it can link many people who have a mobile device. Sensor nodes can be collected for continuous location sensing, event detection, and personal data. These privacy information collected from the users should be stored without unique identifying or sensitive information and used for encryption. This means that, it must collect, use, or provide the least amount of data necessary for attaining the purpose for which it is collected. The privacy data gathering classifies collected personal data on WSN users in order to manage effectively. Collected data of a person or mobile is classified into static privacy information and dynamic privacy information. Static privacy information continuously maintaines personal data such as name, home or work address, or telephone number until an individual withdraws from the requesting service. Dynamic privacy information, called context information, means the cookie information that informs the user's current status and location information, and so forth.

All personal data collected from the users can be transferred from the acquired point on the local node to the aggregation server. In this architecture, security functions such as authentication and IDS can be applied at the privacy care system (PCS) to monitor the event detection. This is an authentication method that combines user information relating to an identified or identifiable person with device information. In general, the information owners or the acquirer can use a signed certificate. The device information based on dynamic privacy information and identifiers such as the unique serial number issued by the manufacturer must be considered as exact contexts, and it may be aggregated by wireless sensor nodes. In this case, the basic service may be provided if the location information includes public places such as on road reserve. There may also be refused a request if necessary.

The PCS shown in Figure 4 is given authority according to that of the authentication information relating to an authenticated or trustable person. A label entity can be created based on their authentication factors and values. This is an encrypted data, and it contains information that help the system know about the request. A label entity is to provide an authenticated user, so it can verify an accessed user. These are designed to help users protect their personal information.

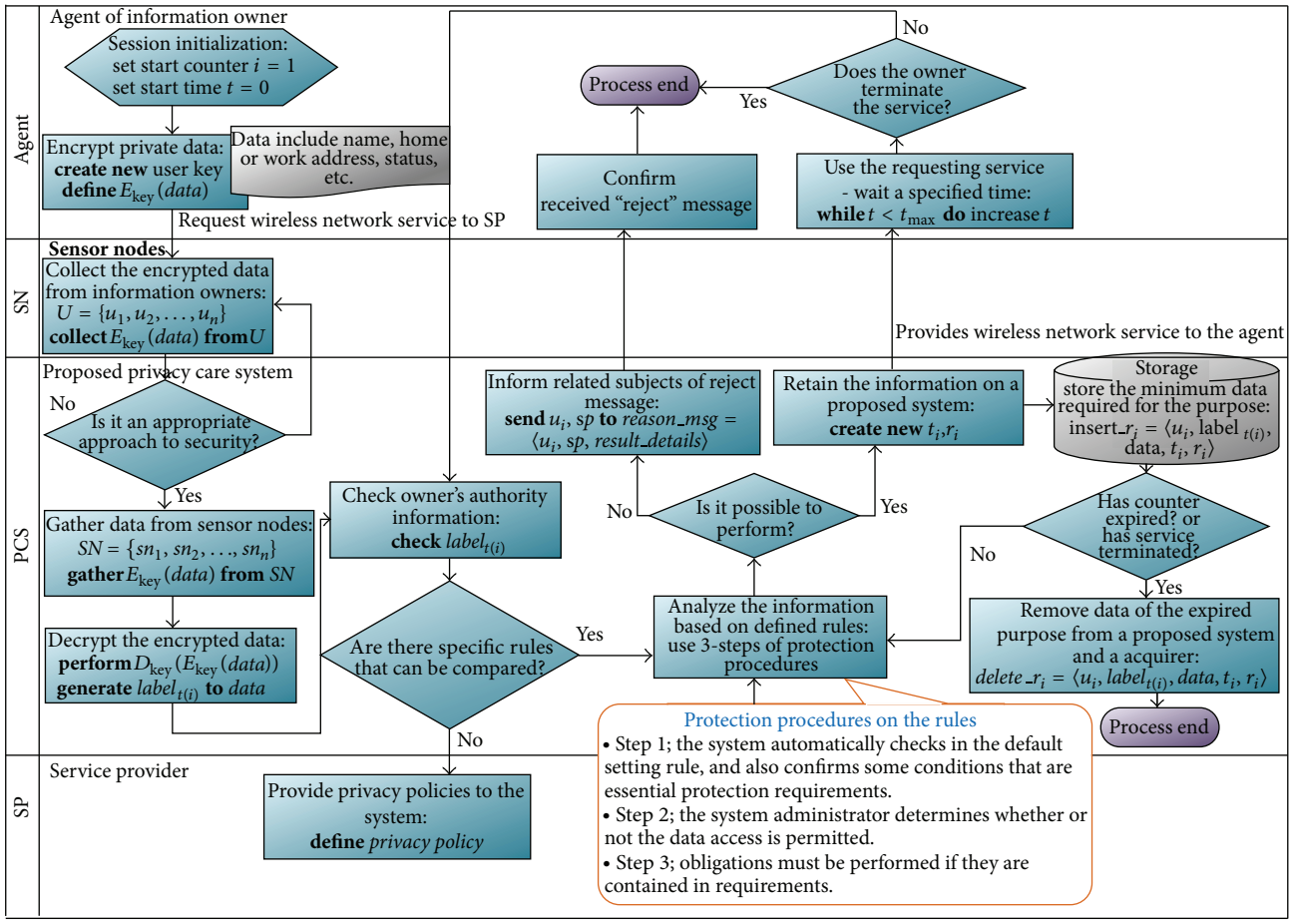

Figure 4: Process of the PCA.

The authenticated person enables access to data based on the label entity. In order to provide the requested service, we suggest the validity examination based on policy for systematic verification. The key composition plan involves defining the laws about protecting and managing user information and based on these providing the rule about privacy information management. Verification on information based on defining rules is enabled in order to efficiently and systematically manage the data, which is trusted by the PCS in WSN. Data should be used to determine whether or not the data access is permitted. Data is reviewed for whether it is still necessary for the purpose for which it was collected. It also examines the purpose whether this information is suitable for WSN by rules. For example, if the data is acquired at sensor node, it can immediately examine the suitability between the request and the rule for collecting. But in fact, the process of data collection in WSN has some more vulnerability because many sensor nodes can collect and manage private data remotely. The requirement for which it is collected may be changed if the user changes the service in a mobile device and moves to another area and also may have privacy implications. Thus, there should be an examination in accessing the information by periods.

In the report data collector, all process data collected from sensor nodes are recorded. This means that the acquirer must make sure that data confirming the collection, use, and provision of privacy information will be automatically recorded and preserved by the system. The process data is a record, which reports the function to monitor a user from making a request of private data by leaving a log to track which user of the system requested whose information for what purpose and when. The handler or the administrator, who coordinates the personal information protection system, can allow services to examine the details of the technical and managerial measures. It is also possible to set and later change automated retention period or data deletion. Because individuals are being made aware of their personal data being processed, we should be informed about data use to the information owners and also must be notified in case of a data loss or breach.

Figure 5 represents the example of prototype for setting the privacy rule in the privacy care system (PCS).

5. Evaluation

As we mentioned earlier, security in WSN is a major issue as it deals with private data or operative in exposed environments. So, WSN with various security functions should be considered as the important factors that affect the performance. In a security process for WSN, these processes

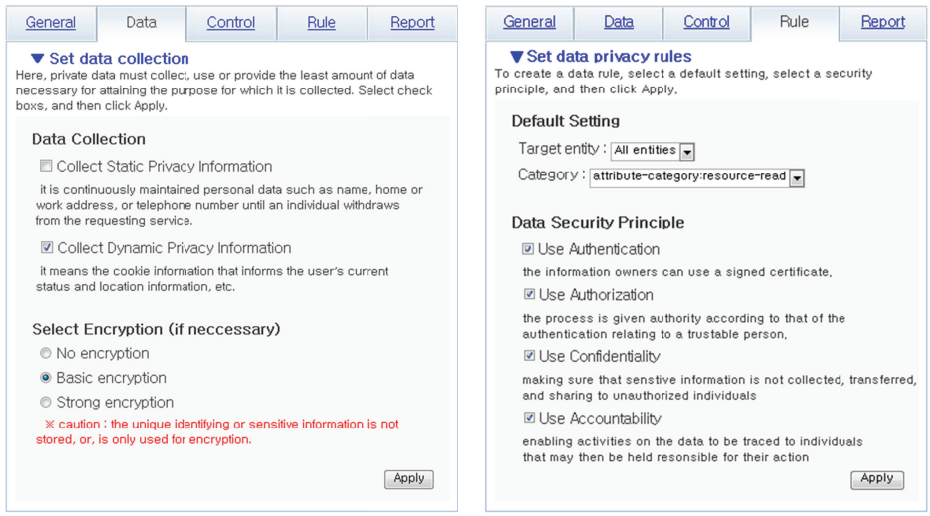

Figure 5: Prototype for the PCS.

are particularly difficult to ensure the good performance that because resources are limited in a tiny sensor network and that because these environments are low power devices.

Here, we have proposed a method for security features, and it achieves better performance and results by using a tiny security label. In order to simplify the testing environment and the algorithms, this research can have the same transaction size by the same information owner and also can compare the performance from before and after the test by applying the security methods. For operating in a simulated environment, the PCA is composed of two components. One is the server, which protects the private data, is implemented in the Windows 7 operating system, and the development language of server is jsp and java. The second is the client, which is the mobile device, which is used to implement Android 2.2. The performance method can be useful for calculating the response time for message through a process. This process involves requesting access to wireless network data, based on security rules, processing the request about privacy management, and completing the access request for a user. We can see that the time taken performance is an insignificant difference between the PCS and the general system without privacy care (see Figure 6).

The figure represents the time taken depending on the number of users connected to the transaction. Two systems (the privacy care system and the nonprivacy care system) use the same simulation environment and compare the average time it took for transactions in each system. In the table in Figure 6, as the number of users increases, its time taken also increase. Instead, there is only a very slight difference in time performance in view of the concept that performance is inversely proportional to the security of system. The graph on the right is based on the results of the time taken. The solid line represents the time taken from privacy care system by applying the security methods. The dotted line represents the average time taken for transactions of the existing system such as nonprivacy care. As shown in the graph, the performance result that applies for security function is really not much different from the change in network environments. Based on these experimental results, our approach can offer better reliability than the previously studied general systems. Data can be protected through preventing the theft of private data that can incur on mobile environments by defining the policy for privacy care. Thus, the PCA is a very effective way to prevent the illegal use and the information leakage in WSN.

6. Conclusion and Future Work

The development of information technology and network has significantly changed people's lives and also contributed a growing impact on social and business environment in Korea. It is no exception for a wireless sensor network area that it has innovated the ways we communicate wirelessly and form ad hoc networks in order to perform some specific operation. WSNs have very broad application domains, and it means providing related network services including medical, military, transportation, and smart spaces. Although the WSN service is being facilitated, security related accidents and in particular privacy are continuously incurring because group or some people with malicious intentions make large volumes of information easily available through remote access.

In this paper, we focus on WSN privacy issues with respect to mobile environments. This research suggested architecture to securely manage private data collected by WSN. We also designed the integrated system where we could link the protection methods closely with the private data protection law and regulation in Korea. We argue that the integrated system will provide the reliability of the sensor service in the exposed wireless environment as a policy-based solution, which helps to protect the collected private data more efficiently. It also helps to prevent the private data loss and breach through the authentication information related to places or the environment. As a leveraging system, the PCA will play a role in protecting the private data on WSN. As part of this work, the privacy care system provides technical support to policies based on specific requirement of the security. Testing in local environment is not difficult, but we require a huge infrastructure that protects all the

Users	Privacy care system (PCS)	Nonprivacy care system
10000	0.8618	0.8406
20000	1.7235	1.6812
30000	2.4991	2.2696
40000	3.2747	3.1102
50000	4.3088	3.9507
60000	5.1706	4.8754
70000	6.1186	5.5479
80000	6.9803	6.4725
90000	7.7559	7.0609

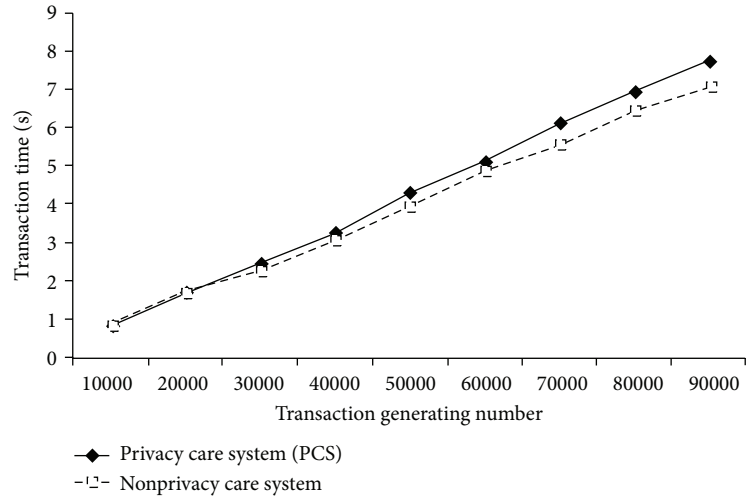

Figure 6: Performance graph and data table.

nodes in order to the actual implementation and use in a real environment. So, it takes time and effort to apply this security method in WSN.

We plan to pursue the related research on establishment of trustful service environment on WSN by conducting the studies on processing speed, power, and storage capacity.

Acknowledgment

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the support program for producing bi-direction TV programs supervised by the KISA (Korea Internet & Security Agency).

References

[1] P. Harrop and R. Das, *Wireless Sensor Networks 2012–2022*, IDTechEx, 2012.

[2] A. Ukil, "Security and privacy in wireless sensor networks," in *Smart Wireless Sensor Neworks*, pp. 395–418, Intech, 2010.

[3] J. P. Barbin and M. Masdari, "Enhancing name resolution security in mobile ad hoc networks," *International Journal of Advanced Science and Technology*, vol. 50, pp. 41–50, 2013.

[4] S. U. Khan and L. Lavagno, "Security in wireless sensor networks," http://polimage.polito.it/wsn/security-in-wireless-sensor-networks/.

[5] S. K. Singh, M. P. Singh, and D. K. Singh, "Intrusion detection based security solution for cluster-based wireless sensor networks," *International Journal of Advanced Science and Technology*, vol. 30, pp. 83–95, 2011.

[6] P. Harrop, "Wireless sensor networks and the new internet of things," *Energy Harvesting Journal*, http://www.energyharvestingjournal.com/, 2012.

[7] Gartner, "Forecast: Consumer LBS, Worldwide," 2010.

[8] B. Park, "Techniques and practices for securing wireless networks," *International Journal of Advanced Science and Technology*, vol. 48, pp. 133–138, 2012.

[9] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, 2009.

[10] J. Yoon, "The overview of personal information protection legislation," *Informedia Law*, vol. 13, no. 1, 2011.

[11] G. Cha, H. han, and Y. Shin, "An effective personal information management system to ensure self-imposed control on personal information protection act," *Journal of KISS*, vol. 39, no. 3, pp. 276–281, 2012.

[12] Korea Communications Commission, "Personal Information Protection Act," Act no. 10465, 2011.

[13] A. Araujo, J. Blesa, E. Romero, and D. Villanueva, "Security in cognitive wireless sensor networks Challenges and open problems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, article 48, 2012.

[14] I. R. A. Hamid, J. Abawajy, and T.-H. Kim, "Using feature selection and classification scheme for automating phishing email detection," *Studies in Informatics and Control*, vol. 22, no. 1, pp. 61–70, 2013.

[15] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, pp. 93–101, 2012.

[16] T. Dimitriou and K. Ioannis, "Security issues in biomedical wireless sensor networks," in *Proceedings of the 1st International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL '08)*, October 2008.

[17] Y. Liu, "Wireless sensor network applications in smart grid: recent trends and challenges," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 492819, 8 pages, 2012.

[18] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: a state-of-the-art survey," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1501–1514, 2009.

[19] J. R. Ribon, L. J. G. Villalba, and T.-H. Kim, "Application of mobile technology in virtual communities with information of conflict-affected areas," *Studies in Informatics and Control*, vol. 22, no. 1, pp. 33–42, 2013.

[20] J. F. Ransome and J. W. Rittinghouse, *Cloud Computing: Implementation, Management, and Security*, Auerbach, 2010.