SELECTING NUMBER OF FORWARDING REPORTS TO IMPROVE ENERGY SAVINGS IN BANDWIDTH EFFICIENT COOPERATIVE AUTHENTICATIONS FOR SENSOR NETWORKS

Su Man Nam[1]and Tae Ho Cho[2]

[1,2]College of Information Communication Engineering, Sungkyunkwan University, Suwon, 400-746, Republic of Korea

ABSTRACT

Wireless sensor networks provide ubiquitous computing systems in various open environments. In the environment, sensor nodes can easily be compromised by adversaries to generate injecting false data attacks. The injecting false data attack not only consumes unnecessary energy in en-route nodes, but also causes false alarms at the base station. To detect this type of attack, a bandwidth-efficient cooperative authentication (BECAN) scheme was proposed to achieve high filtering probability and high reliability based on random graph characteristics and cooperative bit-compressed authentication techniques. This scheme may waste energy resources in en-route nodes due to the fixed number of forwarding reports. In this paper, our proposed method effectively selects a dynamic number of forwarding reports in the source nodes based on an evaluation function. The experimental results indicate that our proposed method enhances the energy savings while maintaining security levels as compared to BECAN.

KEYWORDS

wireless sensor network, network security, false data injection attack, bandwidth efficient cooperative authentication

1. INTRODUCTION

Recent wireless sensor networks (WSNs) have a large number of sensors and a base station in various applications such as health care monitoring, forest fire detection, natural disaster prevention, etc. [1]. The sensors enable the development of low-cost, low-power, and multi-functional sensors [1, 2]. The functions of a sensor node include sensing, computing, and wireless communication. When a real event occurs, the sensor node senses the event, computes it for a report, and transmits the report through wireless communication to a base station. The base station collects the report, analyses the event data of the report, and provides the event information to users. The technology of the sensor network easily and conveniently provides diverse information to users. However, the sensor network has the greatest probability of being captured and compromised because it operates in an open environment [3, 4]. In addition, the sensor node is readily exposed to diverse attack patterns from malicious attackers. In order to effectively operate the network, a confident countermeasure is needed against these attacks.

The sensor network is vulnerable to the various attacks because it is easily captured and compromised. Among those attacks, injecting false data attacks can result in one of two cases that

DOI:10.5121/ijasa.2014.2401

consume unnecessary energy in the en-route nodes and generate a false alarm at the base station as shown in Figure 1.

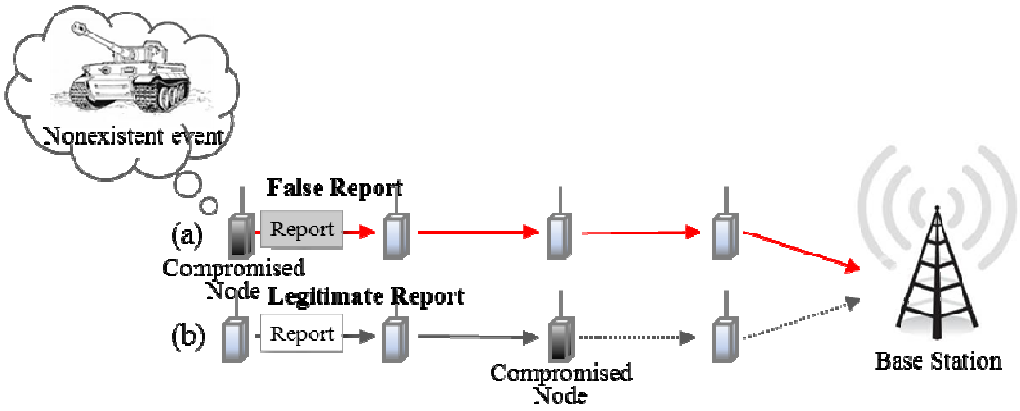

Figure 1. Injecting false data attack

Figure 1 shows two cases (Figures 1-(a) and (b)) of injecting false data attacks [5-7] in the sensor network. We assume that a source node is compromised and an en-route node is compromised. In Figure 1-(a), a source node is compromised, and the compromised node injects a false report into the network. The injected false report passes through the en-route nodes until it reaches the base station. The en-route nodes consume unnecessary energy due to the reception and transmission of the false report. If the false report arrives at the base station, the base station may generate false alarms. In Figure 1-(b), a legitimate report is transmitted for a source node. If the report arrives at a compromised node while forwarding it, the compromised node intentionally drops the report. An alarm cannot be generated at the base station. Thus, if false reports are flooding into the network, not only will a large amount of energy be wasted in the en-route nodes, but heavy verification burdens will also undoubtedly fall on the base station [5].

Bandwidth-efficient cooperative authentication (BECAN) was proposed in order to prevent false data injection attacks. BECAN achieves high filtering probability by using a cooperative neighbors × router-based (CNR) filtering mechanism and high reliability by using a multireport solution (i.e., multiple paths). When a real event occurs within a cluster, a source node collects message authentication codes (macs) by using the CNR filtering mechanism from its neighbors. Then the source node produces a MAC by using macs to include in a report. When the node forwards the report, it uses the multireport solution, which is transmitted along multiple routing paths. Although BECAN simultaneously provides high filtering probability and reliability, the en-route nodes can consume unnecessary energy resources due to the multireport solution.

In this paper, we propose a method to effectively select a dynamic number of forwarding reports for the multireport solution based on an evaluation function in the source node. Before forwarding a report, the source node dynamically selects the number of forwarding reports by using the evaluation function. Effectively selecting the number of forwarding reports influences the high reliability and energy savings in the sensor network. Thus, our proposed method more effectively chooses the dynamic number of forwarding reports in order to enhance the energy efficiency against the injecting false data attacks.

The rest of this paper is organized as follows: the background and motivation of this proposal are described in Section 2. Section 3 introduces our proposed method in detail, and Section 4

provides the analysis and experimental results. Finally, the conclusions and future works are discussed in Section 5.

2. BACKGROUND

In this section, we first discuss BECAN among the countermeasures [8, 9] of the sensor network in Section 2.1, and the motivation of this paper is presented in Section 2.2.

2.1. BECAN

BECAN consists of four phases: (1) sensor nodes initialization and deployment, (2) sensed results reporting protocol, (3) en-routing filtering, and (4) base station (sink) verification.

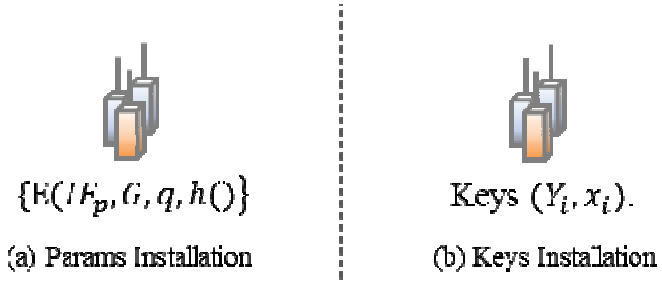

Figure 2. Sensor nodes initialization

Figure 2 shows phase (1), which is the initialization of the sensor nodes with the (a) parameters (*params*) and (b) keys installation. Before distributing the *params*, the base station selects an elliptic curve $E\left((IF_p), G, q\right)$ and a hash function h(). All of the sensor nodes set the params with TinyECC [10] before they are deployed in the sensor field. Each node receives a private key x_i (where the private key x_i is randomly chosen from z_p^*) from the base station. It then collectively generates the public key Y_i ($Y_i = x_i G$, where i is a node's identifier.) Thus, each node has a public key and a private key (Y_i, x_i).

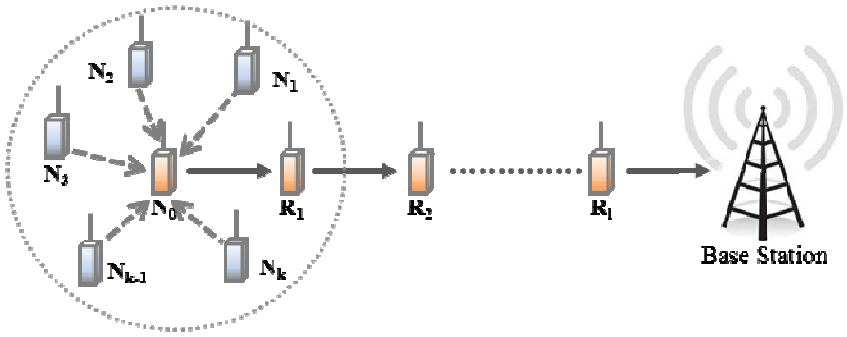

Figure 3. Sensed results routing

Figure 3 illustrates phase (2), which is the sensed results routing phase. A source node N_0 consists of k neighboring nodes N_{N_0}:$\{N_1, N_2, N_3, N_{k-1}, N_k\}$, and establishes a routing path R_{N_0}:$\{R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_l \rightarrow Base\ Station\}$. When an event occurs in a cluster, the source node senses the

event data (m). The source obtains the current timestamp T, selects the neighboring nodes, and transmits the event (m, T) to the neighboring nodes. Each neighbor transmits a mac (m, T) to the sources after each neighbor verifies the event data. The source node aggregates all of the macs (m, T) and produces a report (m, T, MAC) to send to the base station. For transmitting a report, the multireport solution is used. Once a real event occurs, a source node selects k different neighbors, produces the reports, and sends them to the base station via different paths.

In phase (3), the en-routing filtering, the en-route nodes ($R_1, R_2, \cdots, R_l$) verify the integrity of the message m and the timestamp T. If T is out of date, the report will be discarded. The en-route nodes then authenticate the MAC in the report using their public key and the CNR-based MAC verification algorithm. Once it is verified that the report is legitimate, the report is transmitted to the next hop node.

In phase (4), the base station verification, when the report reaches the base station, the report is verified by its keys. When a legitimate report arrives, it is successfully reported.

2.2. Motivation

In a WSN, sensor nodes are easily compromised by attackers due to limited resource hardware. These attackers can fabricate a bad report through the compromised node and can inject the false report into the sensor network. BECAN was proposed to detect this attack. This method achieves not only high filtering probability but also high reliability. Although the existing method performs well in the sensor network, the sensor nodes may waste energy resources in the en-route nodes due to the fixed number of forwarding reports by using the multireport solution. In this paper, our proposed method effectively selects a dynamic number of forwarding reports considering three input factors before transmitting the reports. Therefore, the proposed method improves the energy efficiency while maintaining the same security level against the attack compared to BECAN.

3. PROPOSED METHOD

This section describes our proposed method in detail.

3.1. BECAN

The sensor nodes are deployed with fixed positions in a sensor field. The sensor network is comprised of a base station and a large number of sensor nodes including H-sensors and L-sensors, e.g., Berkeley MICAz motes [11]. The H-sensor hardware (processors, memory, battery, storage, etc.) is more powerful than the L-Sensor [12]. An H-sensor consists of some L-sensors in a cluster. The topology is established by directed diffusion and a minimum cost forwarding algorithm. Each H-sensor discovers the routing paths toward the base station. Compromised nodes can inject false reports and interrupt the transmission of legitimate reports in the sensor network.

3.2. Overview

Our proposed method selects a dynamic number of forwarding reports for the multireport solution by using an evaluation function.

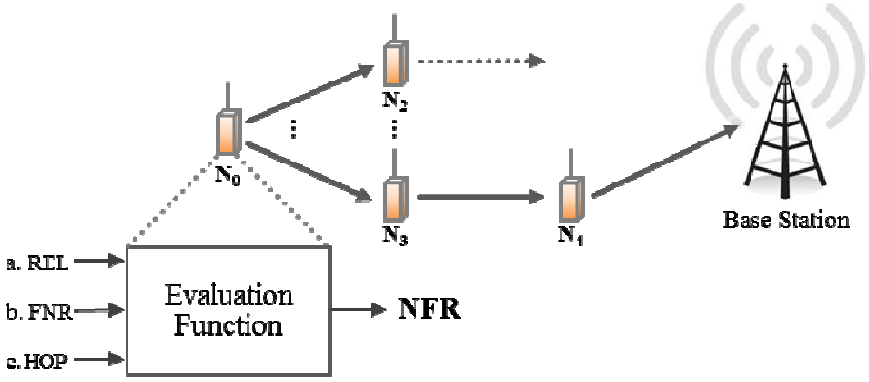

Figure 4. Overview of proposal

Figure 4 shows the processes of the proposed method when a source node transmits a report to the base station. As shown in Figure 4, the source node forwards the report, and it evaluates its current status in order to select the dynamic number of forwarding reports by using an evaluation function. In the evaluation function, there are three input factors (REL, FNR, and HOP) and one output factor (NFR). The resulting value is compared to a defined value. If the result value is greater than the defined value, the number of forwarding reports (NFR) is increased, while if the result value is less than the defined value, NFR is decreased. Thus, our proposed method effectively determines the dynamic number of forwarding reports through the condition of the sensor network based on the evaluation.

3.3. Operation process of the proposed method

In the sensor network, the sensor nodes' energy resources can be wasted by injecting false data attacks. In order to effectively detect this attack, our proposed method decides a dynamic number of forwarding reports in a source node through an evaluation function. The source node executes Algorithm 1 before forwarding a report.

Algorithm 1 SetNumberForwardingReports(REL, FNR, HOP)	
1:	*state*←*REL*/*HOP*+*FNR*;
2:	
3:	**if***state* ≥ *threshold***then**
4:	*NFR*++;
5:	**else**
6:	*NFR*−−;
7:	**end if**
8:	**return***NFR*;

Algorithm 1 shows the operation process of the proposed method for effectively selecting the number of forwarding reports in the source node. The source node executes Algorithm 1 and selects the dynamic number of forwarding reports before forwarding the report to the base station. In the algorithm, the input factors are REL, FNR, and HOP, and the output factor is NFR. The status of the source node is evaluated with these input factors, and a result value *state* is stored (line 1). If the value *state* is greater than *threshold*, NFR is increased, while if the value is less than *threshold*, NFR is decreased (lines 3-7). The NFR is then returned in line 9. The source node applies the NFR and transmits the report after selecting NFR different neighbors.

3.4. Evaluation Function

In order to select the dynamic number of forwarding reports, the evaluation function in the proposed method uses three input factors: REL, FNR, and HOP. The input factors of the evaluation function are as follows.

- Remaining energy level: This value is an important factor for saving energy in the sensor network. If the energy level of the source node is small, the number of forwarding reports should be decreased to save the network energy. The enhancement of the energy efficiency is influenced by the number of communications.
- Number of Hops: This factor describes the hop count, which is the number of hops from the base station to a source node. If the source node is far from the base station, reports transmitted from the base station consume a great deal of the energy of the en-route nodes.
- False negative rate: This factor represents the security of the network. This factor is calculated as the number of true reports that cannot reach the base station over the total number of true reports. If FNR is small, the sensor network demonstrates high reliability. The security level is influenced by FNR.

To effectively decide the dynamic number of forwarding reports, we define an evaluation function by considering these factors. The evaluation function is defined as follows:

$$\mathrm{F(i)} = \frac{ENG}{HOP} + FNR \qquad (1)$$

In Equation (1), i is an identifier of the source node. The source node calculates the ratio of energy consumption through energy over the number of hops and evaluates its current status of the node through FNR. That is, the number of forwarding reports is selected by the evaluation function. If the resulting value is greater than a defined threshold, NRF is increased, and if the result is less than the threshold, NRF is decreased.

3.5. Example

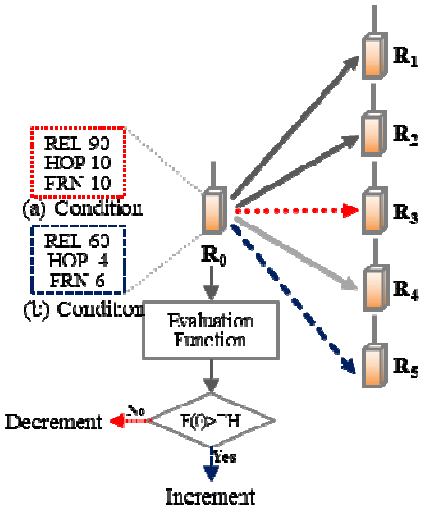

Figure 5. Selection of the number of forwarding reports, including a comparison with a threshold

Figure 5 shows an example of the process for selecting the number of forwarding reports in the proposed method. The source node outputs its current status by using the evaluation function before forwarding a report to its neighbors. The result of the function is compared to the defined threshold (TH). We consider that the source node's condition has two cases (Figures 5-(a) and 5-(b)) and the defined TH is 20. If REL is 90, HOP is 10, and FRN is 10, such as the current state Figure 5-(a), the result of the evaluation function is 19. The result 19 is compared to the TH of 20. The NFR is decreased because the result is less than the TH. Otherwise, if REL is 60, HOP is 4, and FRN is 6, such as in the current state in Figure 5-(b), the function has a result of 21. The NFR is then increased. Therefore, our proposed method can improve the effective performance of the sensor network because it selects the dynamic number of forwarding reports.

4. EXPERIMENTAL RESULTS

Experimental results were obtained to demonstrate the effectiveness of the proposed method as compared to BECAN. In the sensor network, the sensor field's size is 500×500 m^2 including a total of 500 nodes (100 H-sensors and 400 L-sensor). They are uniformly distributed in the field, and an H-sensor consists of nine L-sensors in a cluster. When a sensor receives and transmits a report, it consumes 16.25 µJ and 12.5 µJ per byte, respectively. It also consumes 15 µJ and 75 µ when a MAC is generated and verified, respectively. The report size is 24 bytes. We randomly generated 2,000 events in the sensor field. To randomly generate injecting false data attacks, we compromised five sensor nodes after deployment. The compromised nodes inject false reports with 5% probability into the network.

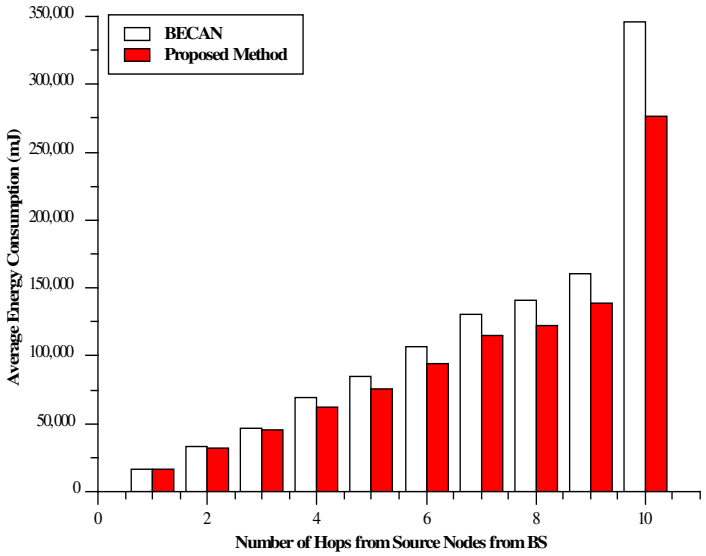

Figure 6. Average Energy consumption vs. number of hops from source nodes to base station (BS)

Figure 6 shows the average energy consumption as a function of the number of hops in the sensor network. In the proposed method, the energy used when the en-route nodes are close to the source nodes is almost the same as for BECAN. Having the en-route nodes between 4 and 10 hops improves the energy efficiency. That is, the proposed method saves energy resources close to the base station. The reason for the energy savings in the proposed method is shown in Figure 7 in detail.

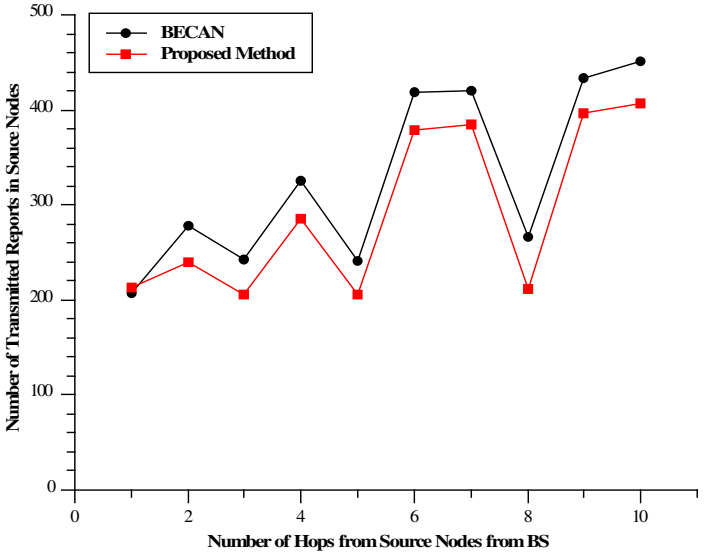

Figure 7. Number of transmitted reports in source nodes vs. number of hops from source node to BS (Base Station)

Figure 7 shows the number of transmitted reports according to the number of hops. The proposed method reduces the number of transmitted reports as compared to BECAN. The reason is that the source nodes in the proposed method select the effective number of forwarding reports through the evaluation function by considering three input factors. Thus, the proposed method enhances the energy savings by decreasing the number of forwarding reports as compared to BECAN.

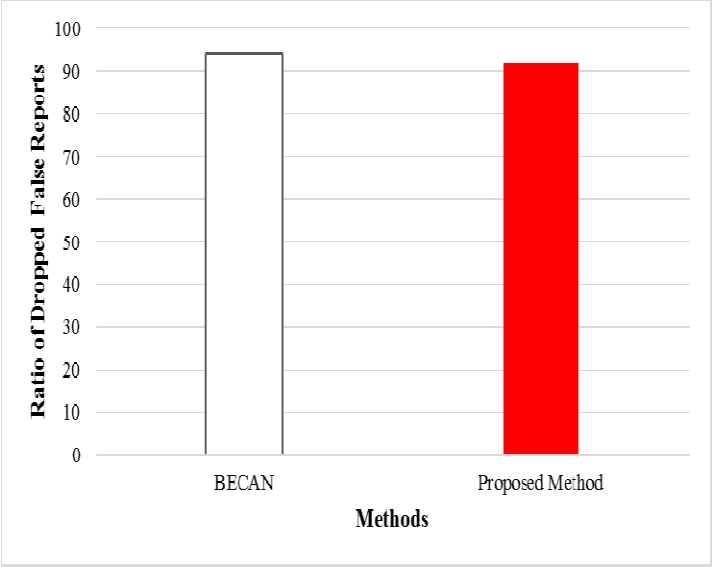

Figure 8. Ratio of dropped false reports vs. methods

Figure 8 shows the ratio of dropped false reports between the two methods. As shown in Figure 8, the two methods are approximately equal in terms of the ratio of dropped false reports. Therefore, our proposed method maintains the same security levels as BECAN.

5. CONCLUSIONS AND FUTURE WORKS

In WSNs, injecting false data attacks are easily generated in compromised nodes because sensor nodes are vulnerable to diverse attacks. These attacks not only cause unnecessary energy consumption in the en-route nodes, but they also generate false alarms at the base station. To detect the attack, BECAN was proposed to achieve both high filtering probability and high reliability. In BECAN, the sensors may consume needless energy resources in the en-route nodes because of the fixed number of forwarding reports. In this paper, our proposed method effectively selects a dynamic number of forwarding reports in the source nodes through an evaluation function. The experimental results demonstrated improved energy savings while maintaining the same security levels as compared to BECAN. Therefore, the proposed method improves the energy efficiency up to 10% with the same security level against attacks. In the future, we propose to optimize the evaluation function in the proposed method to increase the lifetime of the sensor network.

ACKNOWLEDGEMENTS

This research 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 (No. 2013R1A2A2A01013971).

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, pp. 102-114, Aug., 2002.
[2] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," Ad Hoc Networks, vol. 3, pp. 325-349, 2005.
[3] H. Y. Lee and T. H. Cho, "A Scheme for Adaptively Countering Application Layer Security Attacks in Wireless Sensor Networks," IEICE Transactions on Communications, vol. E93.B, pp. 1881-1889, 2010.
[4] A. Ferreira, M. VilaÃ§a, L. Oliveira, E. Habib, H. Wong and A. Loureiro, "On the Security of Cluster-Based Communication Protocols for Wireless Sensor Networks," vol. 3420, pp. 449-458, 2005.
[5] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang and Xuemin Shen, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," Parallel and Distributed Systems, IEEE Transactions On, vol. 23, pp. 32-43, 2012.
[6] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal On, vol. 23, pp. 839-850, 2005.
[7] F. Li, A. Srinivasan and J. Wu, "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks," International Journal of Security and Network, vol. 3, pp. 173-182, 2008.
[8] H. Chan and A. Perrig, "Security and privacy in sensor networks," Computer, vol. 36, pp. 103-105, 2003.
[9] A. Perrig, J. Stankovic and D. Wagner, "Security in wireless sensor network,"Communication of the ACM, vol. 47, pp. 53-57, 2004, 2004.
[10] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in Proceedings of the 7th International Conference on Information Processing in Sensor Networks, 2008, pp. 245-256.

[11] Crossbow, MICAz. http://bullseye.xbow.com:81/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf.
[12] J. Yu, Y. Qi, G. Wang and X. Gu, "A cluster-based routing protocol for wireless sensor networks with nonuniform node distribution," AEU - International Journal of Electronics and Communications, vol. 66, pp. 54-61, 1, 2012.

Authors

Su Man Nam received his B.S. degrees in computer information from Hanseo University, Korea, in February 2009 and M.S degrees in in Electrical and Computer Engineering from Sungkyunkwan University in 2013, respectively. He is currently a doctoral student in the College of Information and Communication Engineering at Sungkyunkwan University, Korea. His research interests include wireless sensor network, security in wireless sensor networks, and modelling & simulation.

Tae Ho Cho received the Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and the B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Information and Communication Engineering, Sungkyunkwan University, Korea. His research interests are in the areas of wireless sensor network, intelligent systems, modeling & simulation, and enterprise resource planning.