A Report Generation Method for Defending False Negative Attacks in Ubiquitous Sensor Networks

Hae Young Lee and Tae Ho Cho,

Sungkyunkwan University, Suwon 440-740, South Korea

Summary

Ye *et al*. proposed the statistical en-route filtering scheme to address false data injection attacks in which an adversary uses compromised nodes to inject forged reports into the network with the goal of deceiving the base station or depleting the resources of the relaying nodes. This scheme can detect such forged reports but is vulnerable to false negative attacks during the report generation process. Thus, a legitimate event may not be reported properly. In this paper, we propose a report generation method to achieve resilience in terms of false negative attacks against the report generation process of the statistical en-route filtering scheme in ubiquitous sensor networks. In the proposed method, one of the detecting nodes randomly selects several nodes to generate sensing reports and key indices to generate message authentication codes (MACs). Each of the nodes selected to produce reports generates a sensing report which contains only the matched MACs, collected from different nodes, using the keys indicated by the key indices. We analyze the security level of the proposed method under various false negative attacks against the report generation process at the end of this paper.

Key words:

Ubiquitous sensor network, false negative attacks, false data filtering, security.

1. Introduction

Ubiquitous sensor networks consist of a large number of sensor nodes that monitor the environment, and a few base stations that collect the sensor readings [1]. Sensor networks have attracted a lot of attention recently due to their broad applications in both military and civilian operations [2]. Sensor nodes are vulnerable to physical attacks, potentially compromising the node's cryptographic keys since they are deployed in open environments in many applications [3]. An adversary can use compromised nodes inject false reports into the network with the goal of deceiving the base station or depleting the resources of the relaying nodes (Fig. 1) [4]. The energy is most important resource that should be considered in sensor networks. Since sensor nodes generally have limited capacity and are unattended, they are limited in power and irreplaceable. Thus, to minimize the grave damage, false reports should be detected and dropped en-route as early as possible, and the few eluded ones should be further rejected at the base station [5]. Ye *et al*. proposed the statistical en-route filtering scheme (SEF) [6] to detect and drop such false reports during the forwarding process. However, compromised detecting nodes can launch false negative attacks against the report generation process. In false negative attacks, an adversary does not generate any sensing reports for legitimate events or inserts incorrect MACs into sensing reports. Thus, a legitimate event may not be reported properly. In many applications, prompt detection and prompt reporting of each relevant event in the field are important [7].

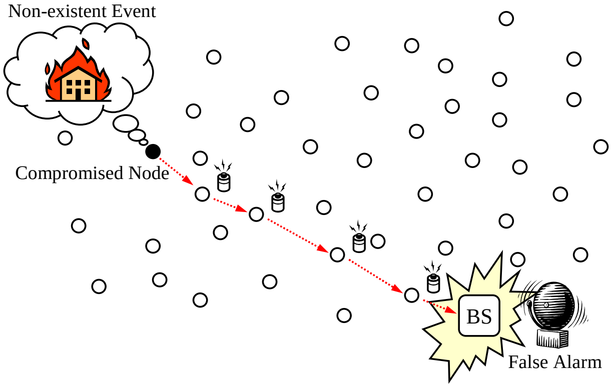

Fig. 1 False data injection attacks.

In this paper, we propose a report generation method to achieve the resilience against false negative attacks in the SEF based sensor networks. In the proposed method, one of the detecting nodes randomly selects several nodes to generate sensing reports and key indices to generate MACs. The nodes selected to produce reports collect the MACs generated by other detecting nodes, using the keys indicated by the key indices. Each of them then produces a sensing report which contains only the matched MACs collected from different nodes for each of the key indices. We analyze the security level of the proposed method under various false negative attacks against the report generation process at the end of this paper.

The remainder of the paper is organized as follows: Section 2 gives a brief description of SEF and false negative attacks in SEF. Section 3 describes the proposed method in detail. Section 4 analyzes the security level of

Manuscript received October 30, 2007
Manuscript revised November 20, 2007

the proposed method. Section 5 reviews the simulation result. Finally, conclusion is discussed in Sect. 6.

2. Background

2.1 Statistical En-Route Filtering (SEF)

SEF [6] is the first paper that addresses false data injection attacks in the presence of compromised nodes [8]. SEF can detect false reports probabilistically. The overhead of SEF is relatively small. But, SEF does not guarantee that a false report can be always detected and dropped in the forwarding process. The base station maintains a global key pool which is divided into multiple partitions. Every node loads a small number of keys from a randomly selected partition in the global key pool before the node is deployed. SEF assumes that the same event can be detected by multiple nodes. When an event occurs, each detecting node sets a random timer (Fig. 2(a)). Upon the timer expiration, it broadcasts its sensor readings (Fig. 2(b)). If another node finds the difference between the broadcast readings and its own readings is within some predefined error range, it accepts the broadcast readings and cancels its own timer. The node whose broadcast readings are accepted by others is elected as the Center-of-Stimulus (henceforth CoS) node (filled circles in Fig. 2). After the CoS election, each detecting node randomly selects one of its keys and generates a MAC over the broadcast readings by using the key. The node then sends the key index and the MAC to the CoS (Fig. 2(c)). The CoS collects them from detecting nodes and produces a sensing report which contains the MACs generated using keys from different partitions in the global key pool. Finally, it forwards the sensing report towards the base station (Fig. 2(d)). A report is forwarded if and only if it has multiple MACs generated by multiple nodes, using keys from different partitions in the global key pool.

2.2 False Negative Attacks in SEF

A compromised detecting node can launch false negative attacks against the collaborative report generation process to intercept the reporting of legitimate events [6]. For example, after the CoS election, a compromised detecting node can send any key index and an incorrect MAC to the CoS (Fig. 3(a)). Since the CoS cannot verify the correctness of the MAC, it may produce a sensing report that contains the incorrect MAC. Thus, the sensing report may be dropped during the forwarding process. Besides, a compromised detecting node may be elected as the CoS by immediate broadcasting of its sensor reading. Other detecting nodes may accept the broadcast reading and cancel its own timer. They then may generate and send MACs to the CoS (Fig. 3(b)). However, the compromised CoS may not produce any sensing report. Thus, a legitimate event may not be reported properly [6]. In many applications, prompt detection and prompt reporting of each relevant event in the field are important [7].

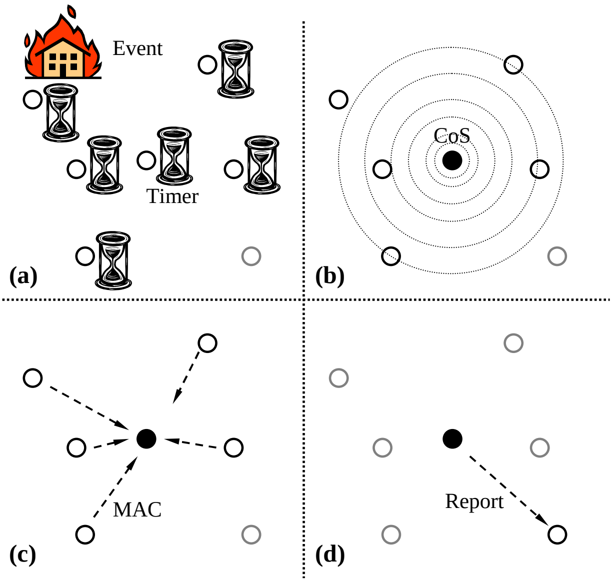

Fig. 2 Report generation process of SEF.

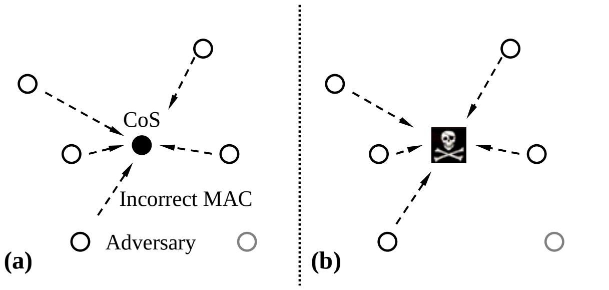

Fig. 3 False negative attacks in SEF.

3. False Negative-Resilient Report Generation

3.1 Assumptions

We consider a sensor network composed of a large number of small sensor nodes. We assume that the network is very dense, so that a sensing target can be detected by at least $2 \cdot n$ sensor nodes, where n is the number of partitions in the global key pool. Sensor nodes are similar to the current generation of sensor nodes in their computational and communication capability and power resources. Due to cost constraints, we assume that each sensor node is not equipped with tamper-resistant hardware. Once compromised, a node can be used to inject false reports into the sensor network. We also assume that each node has a unique identifier and can know the identifiers of its neighbor nodes (nodes within its transmission range). We further assume that the base station cannot be compromised.

3.2 Overview

When an event occurs, each detecting node sets a random timer (Fig. 4(a)). One of the detecting nodes is elected as an *announcer* in the SEF fashion. In contrast with SEF, an announcer randomly selects several nodes, *reporters* (Fig. 4(b)). After the election, every detecting node generates a MAC for the event and sends it to the reporters (Fig. 4(c)). Each reporter collects them and produces a sensing report by adding only the matched MACs. It then forwards the report toward the base station (Fig. 4(d)).

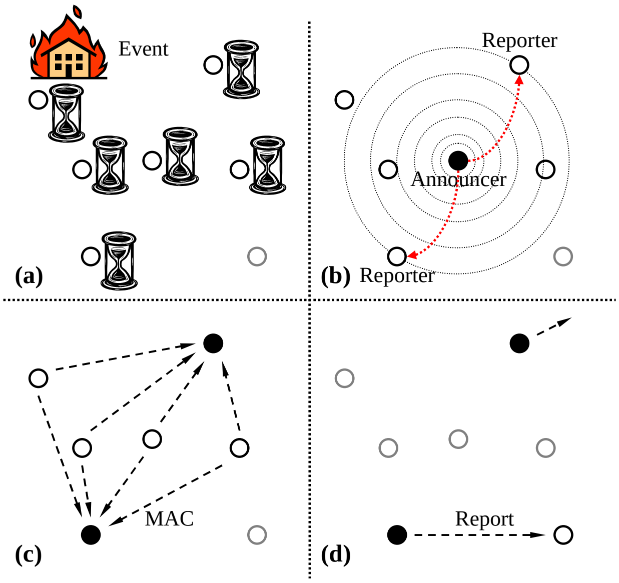

Fig. 4 False negative-resilient report generation.

3.3 Event Announcement Phase

When a sensing target appears, all the detecting nodes prepare a message in the form of:

$$\{L_E, t, E, r_1, r_2, i_1, i_2, \cdots, i_n\}, \quad (1)$$

where L_E is the location of the event, t is the time of detection, E is the type of event, n is the number of partitions in the global key pool, r_1 and r_2 are IDs of randomly selected neighbor nodes (excluding itself), and i_1, i_2, ···, i_n are the key indices randomly selected from every partition. Similar to SEF [6], each detecting node sets a random timer (Fig. 4(a)), upon the timer expiration it broadcasts its message of $\{L_E, t, E, r_1, r_2, i_1, i_2, \cdots, i_n\}$ (Fig. 4(b)).

When another node receives a broadcast message, it first examines where there are the IDs of two different nodes, $\{r_1, r_2\}$, and n key indices, $\{i_1, i_2, \cdots, i_n\}$, selected from every partition. Messages with less than two node IDs or less than n key indices are ignored. Then if the difference between the broadcast readings, $\{L_E, t, E\}$, and its own readings is within some predefined error range, the node accepts the message and cancels its own timer. Otherwise, it broadcasts its own message on expiration of its timer. The node whose broadcast message is accepted by others is elected as an announcer.

3.4 MAC Generation Phase

If a detecting node has one of the keys indicated by the broadcast key indices, $\{i_1, i_2, \cdots, i_n\}$, it generates a MAC over the broadcast readings, $\{L_E, t, E\}$, using the key. The node then sends the key index and the MAC to the nodes indicated by the broadcast node IDs, $\{r_1, r_2\}$ (Fig. 4(c)). If a detection node does not have nay of the keys indicated by the broadcast key indices, it simply ignores the broadcast message.

3.5 Report Generation Phase

The nodes indicated by r_1 and r_2 of the broadcast message are elected as reporters. Each reporter collects the MACs from other detecting nodes and produces a sensing report. Since we assume that the network is very dense, a reporter may collect at least two MACs for each broadcast key index. For each broadcast index, only the matched MACs collected from different nodes are attached into the report. If different MACs for the same index are collected, they are ignored. That is, they are not attached into the report. If just one MAC for one index or any MAC not indicated by the broadcast key indices is collected, it is also ignored (and not attached). The report produced by the reporter is then forwarded toward the base station (Fig. 4(d)). In SEF, every legitimate report should contain a certain number T MACs generated by using keys from different partitions [6]. If a reporter collected less than the T matched MACs, it broadcasts its message of $\{L_E, t, E, r_1, r_2, i_1, i_2, \cdots, i_n\}$ to be an announcer.

3.5 Report Generation Example

Figure 5 shows a very simple example of report generation. There are only three keys in the global key pool and each node loads one key from the pool (Fig. 5(a)). When an event occurs, each detecting node prepares its broadcast message and sets a random timer. Upon the timer expiration it broadcasts its message. Suppose that node 2 broadcasts its message of {L_E, t, E, 4, 8, 1, 2, 3} first. If all the detecting nodes accept the message, node 2 is elected as an announcer, and node 4 and 8 are chosen as reporters (Fig. 5(b)). Each detecting node generates a MAC using one of the keys indicated by the broadcast indices, {1, 2, 3} if it possesses. If it has any of the keys, it ignores the broadcast message. Each of the two reporters produces a sensing report and attaches the MACs collected from the detecting nodes into the report. If any mismatched MAC for one of the broadcast indices is found, all the MACs generated using the corresponding key are ignored. That is, they are not attached into the report. Suppose that the MAC collected from node 6 differs from the MACs generated using key 3, by other nodes (node 3 and 7). Then, the reporters may not attach these MACs into the reports. Finally, they forward the reports toward the base station.

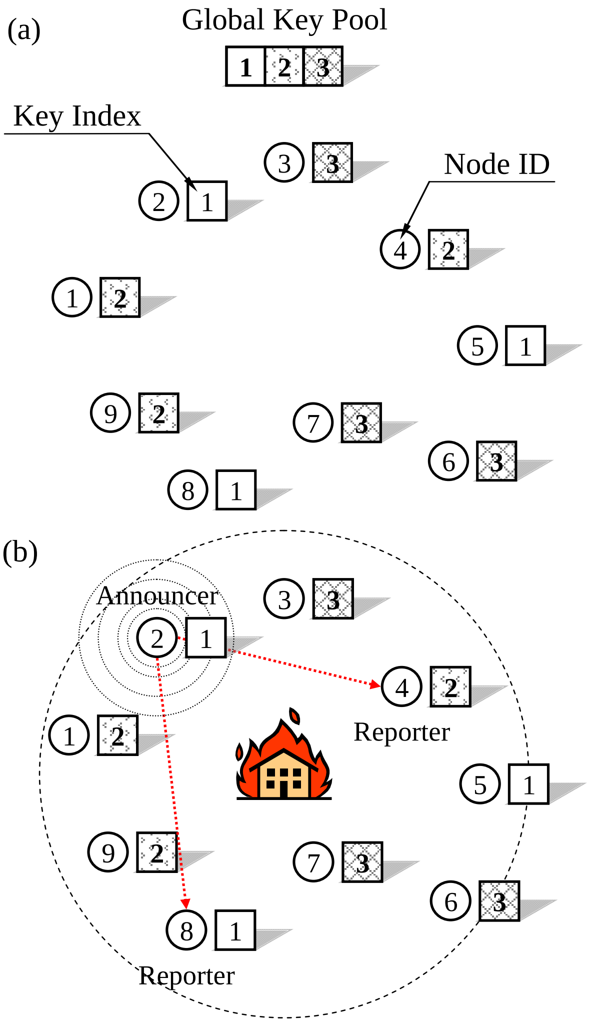

Fig. 5 Report generation example.

4. Security Analysis

4.1 Being a Announcer

When an event occurs, a compromised detecting node can broadcast immediately its message to be an announcer (Fig. 6(a)). However, sensing reports are generated by reporters (Fig. 6(b)). For example, node 4 and 8 may produce reports in Fig. 5(b) if node 2 is compromised. Thus, the event may be reported properly. Note that an announcer cannot be a reporter for the same event.

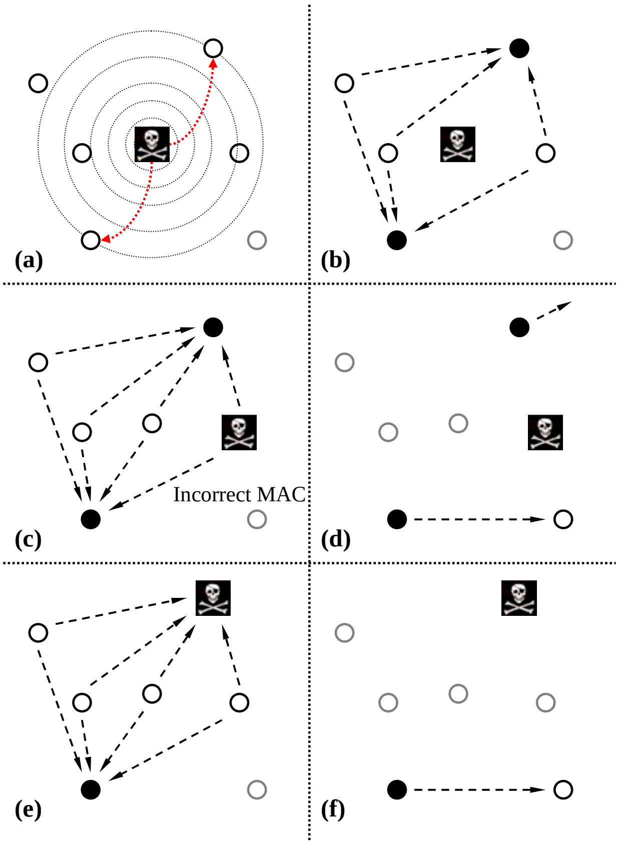

Fig. 6 False negative attacks in the proposed method.

4.2 Inserting Incorrect MACs

After an announcer's broadcast, a compromised detecting node can send an incorrect MAC for one of the broadcast key indices to reporters (Fig. 6(c)). However, other detecting nodes which have the key indicated by that index may send the correct MACs to reporters. Thus, a reporter may not attach any MAC for that index into a sensing report (since they differ each other), and the event may be reported properly (Fig. 6(d)). For example, node 4 and 8 in Fig. 5(b) may not add the MACs generated using key 3 if the MAC generated by node 3 differs from the MAC generated by node 7.

4.3 Being a Reporter

A compromised detecting node can be a reporter (Fig. 6(e)). The compromised reporter may not produce any sensing report. However, there are at least two reporters for one event (e.g., node 4 and 8 in Fig. 5(b)). The other reporters selected by the announcer may produce and forward a sensing report (Fig. 6(f)). Thus, the event may be reported properly.

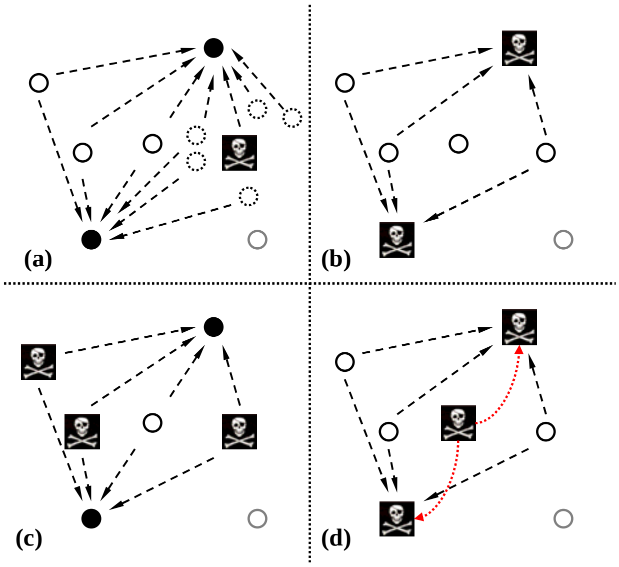

Fig. 7 Other attacks in the proposed method.

4.4 Other Attacks

After an announcer's broadcast, a compromised detecting node can launch Sybil attacks [9], in which a single node presents multiple identities other nodes in the network [10], to send incorrect MACs for multiple key indices (Fig. 7(a)). The proposed method is not designed to address false negative attacks using Sybil attacks. However, several techniques can be applied to achieve resilience against such attacks. For example, Newsome *et al.* proposed several techniques [11] to defend against Sybil attack using random key pre-distribution schemes [12], which SEF exploits to detect false reports.

An adversary can use a large number of compromised nodes to launch false negative attacks during the report generation process. Although there is very little probability, two compromised detecting nodes can be chosen as reporters (Fig. 7(b)). A large number of compromised nodes can be used to inject a large number of incorrect MACs (Fig. 7(c)). Three colluding compromised nodes can intercept the reporting of legitimate events perfectly (Fig. 7(d)). However, by increasing the number of reporters, we may strengthen the resilience against such attacks.

5. Simulation Result

To show the effectiveness of the proposed method, we have compared the proposed method with the report generation method in SEF through the simulation. Figure 8 shows the ratio of delivered reports when the number of compromised nodes for the incorrect MAC insertion is from one two ten. The base station maintains a global key pool of one thousand keys, divided into ten partitions. Each node has fifty keys from one partition. Every report should contain at least six MACs generated using keys from different partitions (i.e., T = 6). As shown in the figure, most legitimate reports can be delivered to the base station in the proposed method (filled rectangles) since reports have a chance to detect incorrect MACs during the report generation phase. On the other hand, most legitimate reports cannot be reported properly in SEF (empty rectangles).

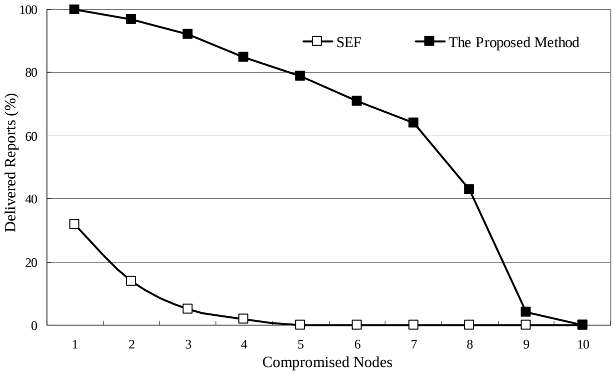

Fig. 8 The ratio of delivered reports (inserting incorrect MACs).

Figure 9 shows the ratio of delivered reports when the number of compromised nodes for the incorrect MAC insertion is from one two ten and a CoS/an announcer is compromised. The other parameters are equal to those of Fig. 8. As shown in the figure, any legitimate report cannot be delivered to the base station in SEF. On the other hand, they can be reported properly in the proposed method.

The proposed method consumes more energy than SEF in report generation. According the result, the proposed method and SEF consume 77.16mJ and 52.38mJ for each report generation, respectively. However, the proposed method can provide reliable data delivery against the false negative attacks which are launched during the report generation phases. In many applications, prompt detection and prompt reporting of each relevant event in the field are important [7]. Thus, the proposed method can be applied to such applications.

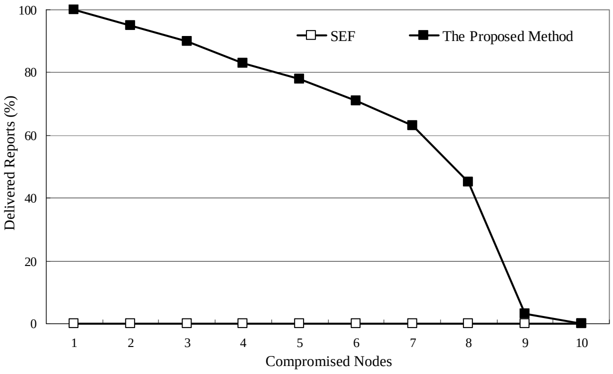

Fig. 9 The ratio of delivered reports (being a CoS/announcer).

6. Conclusion

In this paper, we proposed a report generation method to achieve the resilience against false negative attacks in the SEF based sensor networks. One of the detecting nodes, an announcer, randomly selects several reporters to generate sensing reports and key indices to generate MACs. Reporters collect the MACs, generated by other detecting nodes, using the keys indicated by the key indices. Each reporter then produces a sensing report which contains only the matched MACs collected from different nodes for each of the key indices. We analyzed the security level of the proposed method under various false negative attacks against the report generation process.

Acknowledgments

This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement). (IITA-2007-C1090-0701-0028)

References

[1] L. Buttyan, L. Dora, and I. Vajda, “Statistical Wormhole Detection in Sensor Networks,” *Lect. Notes Comput. Sc.*, vol. 3813, pp. 128-141, 2005.

[2] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-Based Compromise-Tolerant Security Mechanism for Wireless Sensor Networks," *IEEE J. Sel. Area Comm.*, vol. 24, no. 2, pp. 247-260, 2006.

[3] I. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," in *Proc. SenSys*, 2003, pp. 255-265.

[4] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," in *Proc. S&P*, 2004, pp. 259-271.

[5] H. Yang and S. Lu, "Commutative Cipher Based En-route Filtering in Wireless Sensor Networks," in *Proc. VTC*, 2004, pp. 1223-1227.

[6] F. Ye, H. Luo, and S. Lu, "Statistical En-route Filtering of Injected False Data in Sensor Networks," *IEEE J. Sel. Area Comm.*, vol. 23, no. 4, pp. 839-850, 2005.

[7] B. Yu and B. Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," in *Proc. IPDPS*, 2006.

[8] F. Li and J. Wu, "A Probabilistic Voting-Based Filtering Scheme in Wireless Sensor Networks," in *Proc. MobiHoc*, 2005, pp. 34-45.

[9] J. Douceur, "The Sybil Attack," *Lect. Notes Comput. Sc.*, vol. 2429, pp. 251-260, 2002.

[10] C. Karlof and D. Wagner, "Secure Routing in Wirless Sensor Networks: Attacks and Countermeasures," *Ad Hoc Netw.*, vol. 1, no. 2-3, pp. 293-315, 2003.

[11] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," in *Proc. IPSN*, 2004, pp. 259-268.

[12] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," in *Proc. S&P*, 2003, pp. 197-213.

Hae Young Lee received his B.S. degree in Electrical and Computer Engineering from Sungkyunkwan University, South Korea, in February 2003. He is currently a graduate student in the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include wireless sensor networks, intelligent systems, computer-aided design, artificial intelligence, and modeling & 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, South Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the School of Information and Communication Engineering, Sungkyunkwan University, Korea. His research interests are in the areas of wireless sensor network, intelligent system, modeling & simulation, enterprise resource planning.