Advanced Path Control Method for Filtering Secure Method in Sensor Networks

Byung Hee Kim and Tae Ho Cho

Sungkyunkwan University, Suwon 440-746, Republic of Korea

Summary
In many wireless sensor network applications, sensor nodes that have a limited battery power are deployed in open and unattended environments. Owing to these features, an adversary can compromise the deployed sensor nodes and easily inject fabricated reports into the sensor network through the compromised nodes. This attack not only depletes a limited energy resource but also gives a false alarm for deceiving base station. Recently, filtering-based secure methods have been proposed to protect sensor networks from this type of attack. In these schemes, forwarding nodes verify all event reports to detect and drop a fabricated report. To verify received event reports, sensor nodes consume a significant amount of energy. In this paper, we propose an advance path control method by using a fuzzy system. The proposed method can conserves consumption energy and reduce latency. The sufficient resilience and energy efficiency of the proposed method are shown by the simulation results.

Key words:
Sensor networks, fabric report, event report, secure method, fuzzy system.

1. Introduction

Recent advances in micro-electro-mechanical systems and low-power highly integrated digital electronics have enabled the development of low-cost sensor networks and paved the way to use sensor networks in real fields [1, 2]. Wireless sensor networks typically comprised of a few base stations that collect the sensor reading and forward sensing information to managers and a large number of sensor nodes that have limited processing power, small storage space, narrow bandwidth and limited energy. Sensor networks are expected to interact with the physical world at an unprecedented level of universality and enable various new applications [3]. In many sensor network applications, sensor nodes are deployed in an open and unattended environment. Owing to these features, sensor nodes are vulnerable to physical attacks potentially compromising cryptographic keys of them [4]. Through the compromised nodes, an adversary can inject fabricated reports into the sensor network with a goal of spreading false alarms that waste real world response efforts and depleting a limited energy resource of sensor nodes [3]. Figure 1 shows a false data injection attack.

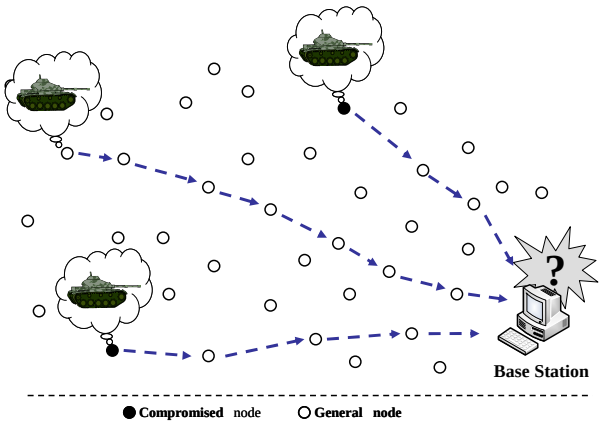


Fig. 1. A false data injection attack.

Several security solutions [5-9] have proposed to overcome this attack. The proposed methods filter out injected fabricated reports during a forwarding process before the fabricated reports consume significant amount of energy. Their key idea is that every sensor node verifies the validity of event reports using symmetric keys. When an interesting event occurs, multiple surrounding sensor nodes collectively generate an event report with multiple message authentication codes (MACs). The MAC is generated by each event-sensing node using one of its symmetric keys and represents its agreement on the event report. When the event report is forwarded toward the base station over multiple hops, each forwarding node verifies the correctness of the MACs carried in the event report. An event report with an inadequate number of the MACs will not be delivered [5]. When an incorrect MAC is detected by a sensor node, the event report is dropped at the sensor node before that reports consume amount of energy. In this scheme, forwarding nodes consume a large amount of energy to verify received event reports. The energy resource of the sensor node is very critical since the battery power of sensor nodes is limited, irreplaceable, and cannot be recharged.

In this paper, we propose an advanced path control method for filtering secure method with using fuzzy rule-based system to conserve consumption energy. A fuzzy rule-based system is used to determine a secure time by

Manuscript received March 5, 2008
Manuscript revised March 20, 2008

considering energy level of the sensor network, a distance from the base station to the cluster head, and a number of the fabricated report. The proposed method can conserve consumption energy when a sensor node sends and receives an event report and provide sufficient resilience. The effectiveness of the proposed method is shown in the simulation result.

The rest of this paper is organized as follows: Section 2 briefly reviews filtering-based secure schemes, namely, the statistical en-route filtering scheme (SEF) [5] and the interleaved hop-by-hop authentication scheme (IHA) [6]. Section 3 describes the proposed method in detail. Section 4 reviews the simulation results. Finally, section 5 concludes the paper.

2. Background

Filtering-based secure method is proposed to overcome the false data injection attack. If a sensor node detects a fabricated report, that node drops it to conserve energy of sensor networks and to avoid confusion on the base station. In this section, we briefly describe a filtering scheme and two proposed secure methods: SEF and IHA.

2.1 Filtering Scheme

The filtering scheme is a secure method to overcome a false data injection attack for sensor networks. Fig. 2 shows the filtering process when a sensor node receives an event report.

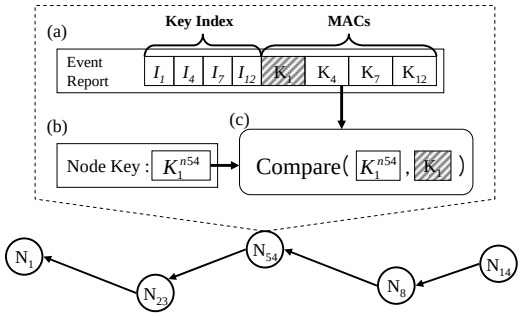


Fig. 2. A process of a filtering-based secure scheme.

If sensor node received an event report (e.g., Figure 2(a)), that node checks the key index of the report. After receiving event report, sensor node checks that it has certain number of a key index and MAC. Sensor node drops a received event report when it has uncertain number of a key index and MAC. If the information of the same key is in the index (Fig. 2(b)), a sensor node creates an MAC using a private key of that node and event information of the received report through the hash function. And that node compares the created MAC with the MAC of the event report (Fig. 2(c)). If the compared MACs are the same, that node forwards the event report to the next forwarding node. If the result shows that the two MACs are different, that node disposes of the received report to conserve the energy.

2.2 Statistical En-Route Filtering scheme (SEF)

SEF [5] is the first paper that addresses the filtering-based secure method to detect false data in the presence of compromised node. SEF can detect the probability of fabricated reports. In SEF, the base station maintains a global key pool that is divided into multiple partitions and can verify whether or not the received reports are false. Every sensor node loads a small number of keys from a randomly selected partition in the global key pool before the sensor node is deployed in interesting region. SEF assumes that the same event can be detected by multiple nodes. When an event occurs, one of the detecting nodes collects event information with an MAC from the other event-sensing nodes. Then that node produces an event report and forwards it toward the base station.

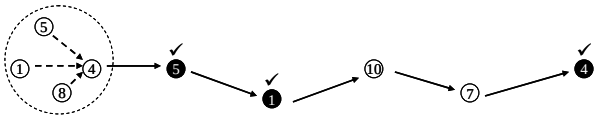


Fig. 3. En-route filtering scheme in SEF.

Figure 3 shows the en-route filtering scheme of SEF. In Figure 3, the sensor nodes (e.g., N_1, N_4, N_5, and N_8) have a key (e.g., k_1, k_4, k_5, and k_8). When an event occurs in the dot circle, one of the sensing nodes (N_4) collects sensing information with an MAC that is made of the key (k_1, k_5, and k_8) of each sensing node (N_1, N_5, and N_8) and sensing information through the hash function. Forwarding nodes verify an event report by using a private key and event information when a key index of the received event report has the same key of a forwarding node. If forwarding node finds a false MAC, that node considers the received event report as a fabricated report and drops it.

2.3 Interleaved Hop-by-hop Authentication scheme (IHA)

In IHA [6], sensor nodes are associated and MACs are verified within association pairs. IHA uses a cluster-based organization. It assumes that all sensor nodes in a cluster can detect a single event simultaneously. Basically, an intermediate node has an upper and a lower associated node, a certain number of hops away from it. Each associate pair shares the same symmetric key. To establish

such associations, either the Bloom scheme [10] or the Blundo scheme [11] can be used. When an event occurs, the cluster head collects MACs over the event from the other event-sensing nodes in that cluster. Then it produces an event report and forwards it towards the base station. Every sensor node verifies the event report based on the pair-wised key shared with the associated node.

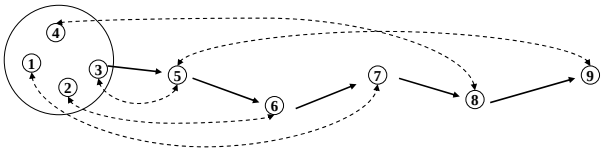


Fig. 4. En-route filtering scheme in IHA.

In Figure 4, sensor nodes (e.g., N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8, and N_9) have keys (e.g., k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, and k_9). The pair nodes (N_1 and N_7), (N_2 and N_6), (N_3 and N_5), (N_4 and N_8), and (N_5 and N_9) share a key (k_{17}, k_{26}, k_{35}, k_{48}, *and* k_{59}) to verify whether the report is false. If a sensor node detects a different key index and false MAC, that node drops the received report.

3. Advanced Path Control Method

3.1 Assumptions

We assume a sensor network is composed of a large number of small sensor nodes. We further assume that all sensor nodes have a mechanism to organize a cluster automatically after a deployment phase. Each cluster has a unique identifier to distinguish from the other clusters. In each cluster, one of the sensor nodes is elected to be cluster head. The cluster head aggregates sensing data from the other sensor nodes in the cluster and produces an event report on behalf of those sensor nodes. To balance energy consumption, all sensor nodes of the same cluster take turns playing the role of cluster head. All sensor nodes can also set up a time to synchronize. We assume that the base station cannot be compromised. We also assume that the base station can acquire or estimate average network energy level and have a mechanism to authenticate a broadcast message (e.g., based on TESLA [12]), and every sensor node can verify the broadcast message.

3.2 Overview

In many sensor network applications, an occurred event is maintained for a long time in the same region after an interesting event occurs (e.g., a forest fire, battlefield, or detecting an emergency). In this situation, a manager needs correct and promptitude information to control that state. Sensor nodes should send many event reports to provide information promptly and they may consume much energy to send the reports. If the sensor nodes verify every event report to detect a fabricated report, the sensor nodes might consume a lot of energy and have latency times. To conserve the consumption energy for verifying process, we propose an advance path control method using the fuzzy system. In proposed method, we set a fuzzy rule-based verified path (FVP).

3.3 Verified path

In our proposed method, we use the verified path to conserve consumption energy for verifying event reports. If a base station received a correct event report from a cluster head, it assumes that the received report comes through a safe path and anticipates that the next event report is also a true event report. The base station uses that forwarding path to the verified path to receive an event report safely. To distinguish the sensor nodes in the verified path from the other sensor nodes, the base station assigns a unique event number to the forwarding nodes and the cluster head. After receiving an event number from the base station, sensor nodes do not verify and just forwards the event report that has a correct event number to the next forwarding node. If a sensor nodes assigned as verified path receives an event report that does not have an event number, that node verifies a correctness of a received event report.

3.4 Secure time determining method

After establishing a verified path, we should determine a secure time that is a maintenance time of the verified path. The verified path has an enhanced secure strength to maintain a secure time. To determine the secure time, we use the fuzzy rule-based system. The fuzzy system determines the secure time by considering an energy level of the sensor network, distance from the base station to the cluster head, and number of the fabricated report.

3.4.1 Fuzzy input parameters

Sensor nodes in a verified path maintain an event number during a secure time to avoid that an adversary uses the event number. To determine the secure time, the fuzzy system uses three input parameters: 1) Networks energy level, 2) distance, and 3) a number of the fabricated report.

1) Network energy level: When determining the secure time, the energy level of sensor networks must be considered since each sensor node has a small battery with a limited capacity. And it is infeasible to recharge all the batteries because the sensor network comprises a large number of sensor nodes and sensor nodes are deployed in

an open environment. Therefore, the energy of the sensor nodes should be conserved to maintain sensing regions for a long time. If the energy level is high, a short secure time is better than the long secure time to maintain a high detection power. But the energy level is low, secure time should be long to conserve the energy.

2) Distance (Hops from the cluster head to the base station): The distance is also considered to determine the secure time. If a cluster head is away from the base station, the FVP can conserve a lot of energy. When the cluster head is close to the base station, the verified path is not useful to conserve the consumption energy since the base station sends a message to set up a verified path. Therefore, the secure time is short. But the secure time is to be long when a distance is long.

3) The number of fabricated reports: When the base station receives an event report form a cluster head, the base station can know whether the received report is fabricated report or not since it has the global key pool. The base station also knows where that report comes from because the report contains information of a location. When the base station decides a secure time of a forwarding path, the number of fabricated reports has to be considered. A fabricated report means that a compromised node in that cluster. Therefore, the base station assigns a shorter time to a cluster region that sends many fabricated reports than a reliable cluster region that sends a few fabric report. By maintaining a safe forwarding path for a long time, the FVP can conserve much energy of the sensor network.

3.4.2 Fuzzy Logic

Figures 5(a), (b), and (c) illustrate membership functions of three fuzzy logic input parameters. The labels of the fuzzy variables are represented as follows:

· ENERGY_LEVEL = {VL, L, E}
· DISTANCE = {N, AD, AW}
· FABRICATED_REPORT = {VS, S, ME, M, VM}

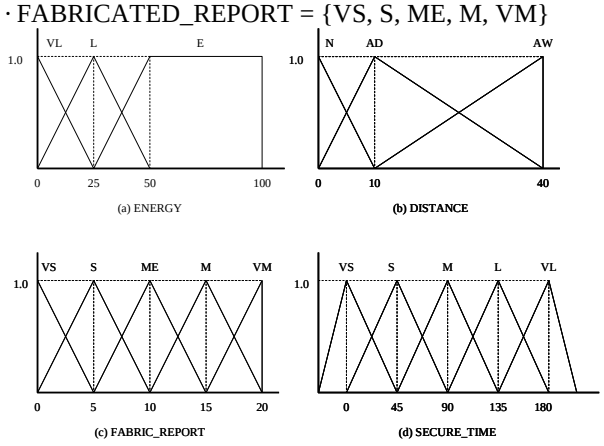


Fig. 5. Fuzzy membership functions for determining secure time.

The output parameter of fuzzy logic is SECURE_TIME = {VS, S, M, L, VL}, which is represented by the membership function as show in Figures 5 (d).

3.4.3 Fuzzy If-Then Rules

To use the fuzzy membership functions, the fuzzy rule should be defined. Table 1 shows some rule of the fuzzy rule-based system. If ENERGY_LEVLE is VL (VERY_LOW) and DISTANCE is N (NEAR), the value of the SECURE_TIME can take on a value of either VS (VERE_SMALL) or S (SMALL) depending on the value of FABRICATED_REPORT. Some of the rules are shown in Table 1.

Table 1: Margin specifications

Rule	IF			THEN
No.	ENERGY LEVLE	DISTANCE	FABRIC REPORT	
0	VL	N	VS	VS
10	VL	AW	S	L
20	L	AD	ME	M
30	E	AW	AW	VL
40	E	N	VM	VS

3.5 Fuzzy rule-based control method for the verified path (FVP)

In FVP, each sensor node has a security key shared with the base station before a deployment phase. Our proposed method consists of three phases: 1) *Pre-verified phase* (Fig. 6(a)), 2) *secure time determining phase* (Fig. 6(b)), and 3) *post-verified phase* (Fig. 6(c)).

1) Pre-verified phase (Fig. 6(a)): When an interesting event occurs, a cluster head aggregates sensing information from event-sensing nodes in the same cluster region. After collecting of event information with an MAC, the cluster head sends an event report to the base station. Forwarding nodes verify a received event report whether the event report is a fabricated report or not.

2) Secure time determining phase (Fig. 6(b)): When the base station receives a correctness report from the cluster head, the base station determines the secure time by using the fuzzy system. The fuzzy system considers the energy level of sensor networks, distance from the base station to the cluster head, and the number of the fabricated report. The base station also determines an event number. To consider the number of the fabricated report, the base station records a number of fabricated reports of every cluster region.

3) Post-verified phase (Fig. 6(c)): After determining the secure time and event number, the base station sends determined information with an encrypted random number made of security keys of the cluster head to the cluster

head and forwarding node. After receiving the event number, the cluster head sends an event report that has the received event number. Forwarding nodes, that received the event number, do not verify the event report if it has a certain event number.

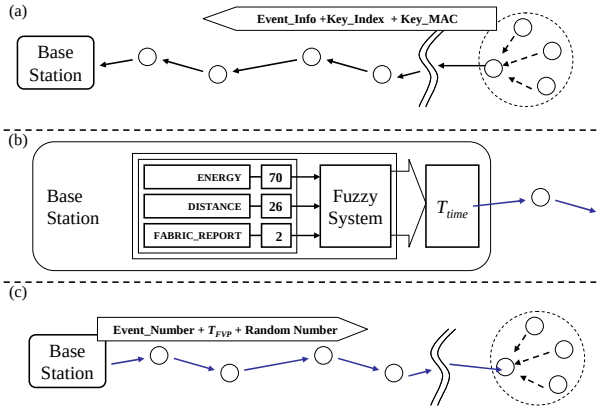


Fig. 6. The set-up phases of the FVP.

In FVP, not every forwarding node needs to verify the event report. Therefore, we reduce the size of the MAC to conserve energy. In the proposed filtering-based secure scheme [5], it uses the Bloom filter [9] to reduce the packet size of MACs. If a size of MAC is long, a sensor node consumes much energy to send and receive an event report. In SEF [5], MACs take 320 bits (about 40 bytes) for each report when each MAC is 64 bit and five MAC are needed for creating an event report. Using the Bloom filter, the MACs reduce to 114bits. To reduce a size of MACs in FVP, in proposed method, we use exclusive OR scheme and hash algorism (H). After a cluster head receive an event number from the base station, the cluster head make verified MACs using received random number (R) from the base station. If an event report needs five MACs to make certain MACs, a cluster head should receive five MACs (e.g., M_1, M_2, M_3, M_4, and M_5) from event-sensing nodes. After the cluster head receives event information with MACs, the cluster head compresses them into a node MAC using standard XOR scheme as follows:

1. $M_T = (M_1 \oplus M_2 \oplus M_3 \oplus M_4 \oplus M_5)$
2. $M_h = (H(M_T \oplus R))$
3. Divides M_h to two partitions: M_{h1} and M_{h2}; M_{h1} and M_{h2} have the same bit size
4. $M_{FVP} = (M_{h1} \oplus M_{h2})$
5. $R = R + 1$; to create next event report.

In our proposed method, the M_{FVP} just has 32bit. Sensor nodes can conserve a lot of energy to send and receive an event report than the other proposed secure methods.

4. Simulation Result

We have compared SEF with FVP-based SEF (FVP_SEF) and IHA with FVP-based IHA (FVP_IHA) to show the effectiveness of the proposed method. The FVP_SEF and FVP_IHA are schemes using our proposed method.

We randomly deployed 400 cluster head. And each cluster head contains five or six sensor nodes. Each sensor node takes 16.56μJ to transmit a byte and 12.5μJ to receive a byte. We use an RC5 [13] block cipher for a hash function that consumes 15μJ. There are 1,000 secret keys in a global key pool. An event is occurred as 10000 times and a false event is occurred as 1000 times. Fig. 8 shows architecture of proposed method for the simulation.

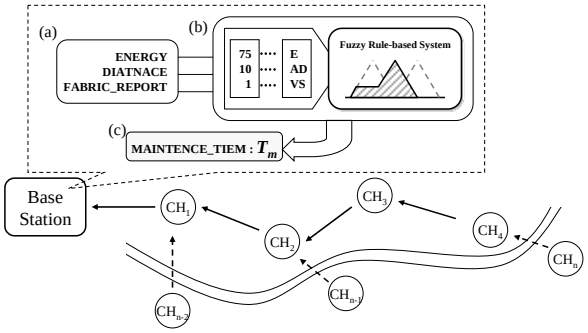
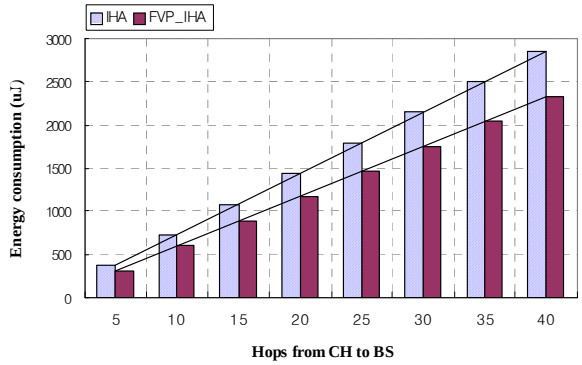


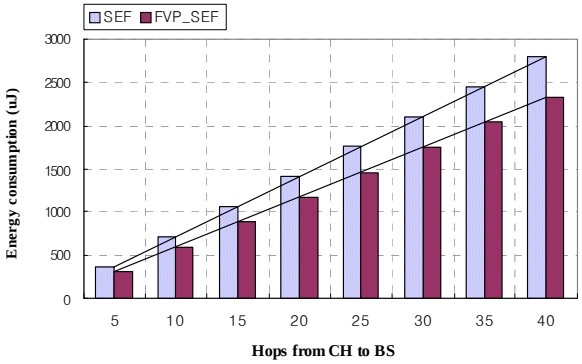
Fig. 7. Architecture of FVP.

In the proposed method, the base station determines secure time and an event number when it receives a correctness event report from a cluster head in an event occurred region. And the base station sends decided information to the cluster head and each forwarding node.

Figures 8(a) and (b) show an average energy consumptions of SEF, FVP_SEF, IHA, and FVP_IHA by hops when the number of hops is from 5 to 40 and the event report occurred as 100 times. Our proposed methods, FVP_SEF and FVP_IHA, can conserve the consumption energy compared with the SEF and IHA. However, the FVP is not useful when the distance from the base station to a cluster head is short. If the duration of the event is short and a distance is short, the proposed method consumes more energy then SEF and IHA.



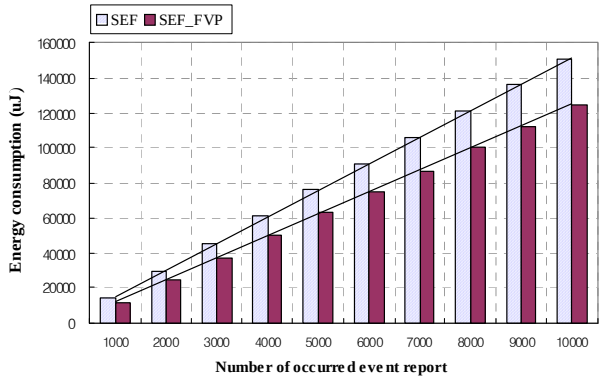
(a) Energy consumption of SEF and FVP_SEF



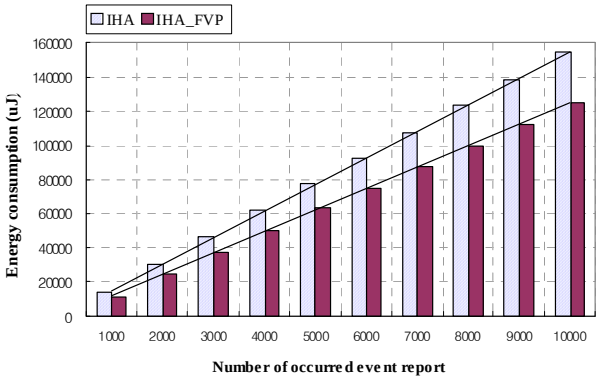
(b) Energy consumption of IHA and FVP_IHA

Fig. 8. Average energy consumption of SEF, FVP_SEF, IHA, and FVP_IHA by hops.

Figures 9(a), (b), and (c) shows average energy consumptions caused by the number of event reports and fabricated event reports in the simulation. Our proposed methods, FVP_SEF and FVP_IHA, are more efficient than SEF and IHA. Our proposed method can conserve the consumption energy to send and received event reports compared with original proposed method.



(a) Energy consumption of SEF and FVP_SEF



(b) Energy consumption of IHA and FVP_IHA

Fig. 9. Average energy consumptions caused by the number of event report.

The simulation results show that the filtering-based secure methods using the FVP is more efficient than original filtering-based secure method.

5. Conclusion and Future work

In filtering-based secure schemes, sensor nodes consume a large amount of energy when verifying an event report. To conserve the consumption energy, we proposed the advanced path control method using the fuzzy rule-based system for sensor networks. Our proposed method uses a verified path to reduce the consumption energy and a secure time to control the verified path. We use a fuzzy rule-based system to determine the secure time by considering the energy level of the sensor network, the distance from the base station to the cluster head, and the number of the fabricated report since the secure time provides the enhanced security to the verified path. The effectiveness of the proposed method is demonstrated by the simulation results.

Our future research will apply our proposed method to the other filtering-based secure schemes and simulate them with other input factors that have not been considered in this work.

Acknowledgments

This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement). (IITA-2008-C1090-0801-0028)

References

[1] I. F. Akyildiz, Su Weilian, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, pp. 102-114, 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] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," IEEE Wireless Communications, vol 11, pp. 6-28, 2005.

[4] B. Przydatek, D. Song, and A. Perrig, "SIA: secure information aggregation in sensor networks," in Proceedings of the 1st international conference on Embedded networked sensor systems, pp. 255-265, 2003.

[5] Y. Fan, H. Luo, L. Songwu, and Z. Lixiz, "Statistical en-route filtering of injected false data in sensor networks," IEEE Journal on Selected Areas in Communications, vol 23, pp. 839-850, 2005.

[6] 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 Proceeding of IEEE Symposium on Security and Privacy, pp. 259-271, 2004.

[7] H. Y. Lee and T. H. Cho, "Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks," Lecture Notes in Computer Science, vol 4317, pp. 1611-3349, 2006.

[8] H. Y. Lee and S. Lu, "Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks," In Proceeding of VTC, pp. 1223-1227, 2003.

[9] W. Zhang and G. Cao, “Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach,” In Proceeding of INFO-COM, pp. 503-514, 2005.

[10] A. Perrig, R. Szewczyk, and J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol 8, pp. 512-534, 2002.

[11] A. Blom, “An Optimal Class of Symmetric Key Generation Systems,” Lecture Notes in Computer Science, vol. 209, pp. 335-228, 1984.

[12] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, “Perfectly-Secure Key Distribution for Dynamic Conferences,” Information and Computation, vol. 146, pp. 1-23, 1998.

[13] R. Rivest, “The RC5 Encryption Algorithm,” In Workshop on Fast Software Encryption, pp. 146-148, 1995.

Byung Hee Kim received his B.S. degree in Information and Communication engineering from Dongseo University, Korea, in 2003. He is currently a graduate student in the School of Information and Communication Engineering, Sungkyunkwan University, Korea. His research interests include wireless sensor network, Ad-hoc network, Mobile Computing.

Tae Ho Cho earned a Ph.D. degree in Computer Engineering from University of Arizona, M.S. degree in Electronics Engineering from University of Alabama, and B.S. degree in Electronics Engineering from Sungkyunkwan University, Korea. He is a Professor of the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include ubiquitous sensor network, modeling and simulation, intelligent system, and enterprise resource planning.