무선 센서 네트워크에서 퍼지 로직 기반의 허위 보고서 탐지 기법

김문수[1] · 이해영[1] · 조대호[1†]

A Fuzzy Logic-Based False Report Detection Method in Wireless Sensor Networks

Mun Su Kim · Hae Young Lee · Tae Ho Cho

ABSTRACT

Wireless sensor networks are comprised of sensor nodes with resource-constrained hardware. Nodes in the sensor network without adequate protection may be compromised by adversaries. Such compromised nodes are vulnerable to the attacks like false reports injection attacks and false data injection attacks on legitimate reports. In false report injection attacks, an adversary injects false report into the network with the goal of deceiving the sink or the depletion of the finite amount of energy in a battery powered network. In false data injection attacks on legitimate reports, the attacker may inject a false data for every legitimate report. To address such attacks, the probabilistic voting-based filtering scheme (PVFS) has been proposed by Li and Wu. However, each cluster head in PVFS needs additional transmission device. Therefore, this paper proposes a fuzzy logic-based false report detection method (FRD) to mitigate the threat of these attacks. FRD employs the statistical en-route filtering scheme as a basis and improves upon it. We demonstrate that FRD is efficient with respect to the security it provides, and allows a tradeoff between security and energy consumption, as shown in the simulation.

Key words : Wireless sensor networks, Compromised nodes, En-route filtering, Fuzzy logic

요 약

무선 센서 네트워크는 자원 제약을 가지는 센서 노드들로 이루어진다. 센서 네트워크에서 충분한 보호를 받지 못하는 노드들은 공격자들에 의해 훼손될 수 있다. 이러한 훼손된 노드들은 허위 보고서 주입 공격이나 정상 보고서에 대한 허위 데이터 주입 공격과 같은 공격들에 취약하다. 허위 보고서 주입 공격에서, 공격자는 싱크의 기만이나 배터리로 동작하는 네트워크의 제한된 에너지를 고갈을 목적으로 허위 보고서들을 네트워크에 주입한다. 정상 보고서에 대한 허위 데이터 주입 공격에서, 공격자는 모든 정상 보고서에 거짓 데이터를 주입할 수도 있다. 이러한 공격들을 다루기 위하여, Li와 Wu는 확률적 투표-기반 여과 기법(PVFS)을 제안하였다. 그러나 PVFS에서 각 클러스터 헤드는 추가적인 전송 장비를 필요로 한다. 그러므로 본 논문에서는 이러한 공격들의 위협을 완화시키기 위하여 퍼지 로직-기반 허위 보고서 탐지 기법(FRD)를 제안한다. FRD는 통계적 전달 중 여과 기법을 기반으로 채택하여 이를 개선한다. 시뮬레이션에서 FRD가 제공하는 보안 능력이 효율적이며, 보안과 에너지 소비 간의 트레이오프가 있음을 보인다.

주요어 : 무선 센서 네트워크, 훼손 노드, 전달 중 여과, 퍼지 로직

* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-C1090-0801-0028).

2008년 6월 12일 접수, 2008년 8월 17일 채택

[1] 성균관대학교 정보통신공학부
주 저 자 : 김문수
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

1. Introduction

Recent advances in nano-technology made it technologically feasible and economically viable to develop low-power, battery-operated devices that integrate special-purpose computing with low-power sensing and wireless communications capabilities (Olariu *et al*., 2005). Wireless sensor networks are comprised of a large number of these small devices, referred to as sensor nodes, with restricted processing power, small storage space, narrow bandwidth, and limited energy lifetime (Ferreira *et al*., 2005). These sensor networks have the potential to be widely deployed in a variety of applications, including military surveillance, forest fire monitoring, seismic monitoring of buildings, and habitat monitoring. In such a network, sensor nodes are deployed over vast territory to detect events of interest and transmit reports over multihop paths to the single collection point (called "sink") (Yang *et al*., 2005). A major benefit of sensor networks is that they perform in-networking processing to reduce large streams of raw data into useful aggregated information (Perrig *et al*., 2004). However, the security is an essential requirement for mission-critical applications that demand operation in adverse or hostile environments (Yang and Lu, 2004).

From a security perspective, symmetric cryptography is used by most applications since sensor nodes usually have severely constrained computation, memory, and energy resources. Sensor networks with symmetric cryptography contain a global key stored on each sensor node, prior to deployment. However, this system is particularly vulnerable to compromised nodes since the adversary only has to compromise any node in the networks. Once compromised, the node can launch false positive attacks or false negative attacks. A false positive attack indicates that an alarm is generated when no condition of attack is present to warrant one (Proctor, 2000). One such attack is a false reports injection attack, in which the adversary may generate non-existent events at arbitrary locations (Yang and Lu, 2004). To combat this problem, Ye *et al*. (2005) proposed the statistical en-route filtering scheme (SEF) to detect and drop injected false reports during the forwarding process. Another authentication-based scheme is called the interleaved hop-by-hop authentication scheme (IHA) (Zhu *et al*., 2004). This scheme focuses on false alarm and guarantees that the sink will detect any injected false data packets when no more than a certain threshold number of nodes are compromised (Xiao, 2006). Furthermore, Zhang *et al*. (2006) proposed the multipath-based filtering scheme to solve both problems such that secure and efficient authentication can be achieved. On the other hand, a false negative attack represents that an alarm is not generated when it should be due to the attacks (Yang and Lu, 2004). One such attack is the false data injection attack on a legitimate report, which means an adversary may inject false data into a legitimate report to filter out the report (Fig. 1). To address such an attack, Li and Wu (2006) proposed a probabilistic voting-based filtering scheme (PVFS). PVFS selects intermediate cluster-heads as verification nodes with a certain predefined probability. However, SEF and IHA do not address false negative attacks. Since PVFS is based on underlying cluster architecture each node in PVFS needs additional transmission device. Therefore, this paper proposes a fuzzy logic-based false report detection method (FRD). The proposed method deals with false reports injection attacks and false data injection attacks on legitimate reports without additional device.

As the same as SEF, FRD carefully loaded the limited amount of security information assigned to each node, and relies on the collective decisions of multiple sensors for detecting attack packet. When an event occurs, detecting nodes collectively generate a report and attach to the report their Message Authentication Codes (MACs). The source node sends the reports to the sink. Even

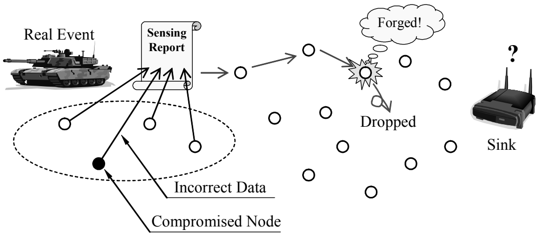


Fig. 1. False negative attacks

some intermediate nodes found some false MACs, the report can still be routed to the sink until threshold has been reached. The fuzzy rule-based system on the sink is exploited to determine a threshold value by considering the number of false reports, the average energy of the forwarding path, and the number of MACs in the report. We demonstrate that FRD is efficient with respect to the security provided and allows a tradeoff between security and energy consumption through simulation.

2. Background

In this section, we briefly describe SEF, and the system models and assumption of this work.

2.1 SEF Overview

SEF (Ye *et al.*, 2005) uses the random key predistribution approach (Chan *et al.*, 2003) as the key assignment method. In SEF, the sink maintains a global key pool of n keys, divided into p non-overlapping partitions. Each partition has q keys (i.e., $n=p\cdot q$), and each key has a unique key index. Each node selects t random keys from one of the p partitions (where t is the number of keys each node can carry in global key pool) and stores them into the node's key space, together with the associated key indices. After the sensor nodes are deployed, each node endorses any event it has observed by using its key to generate a MAC on the report (Yang *et al.*, 2005). The key assignment method of SEF is shown in Fig. 2.

When an event occurs, multiple surrounding sensors collectively generate a report that carries multiple MACs and the associated key indices (Li and Wu, 2006). When a forwarding node receives a report, it verifies the report as follows: it first checks whether the report has t distinct MACs and the associated key indices. Then, it checks whether the forwarding node has the key of the report. If it has the key, the node checks whether the carried MAC is the same as the MAC it computes via its stored key. If verification succeeds, the forwarding node transmits the report to the next hop. Otherwise the report is dropped. If it does not have any of the keys, it forwards the report to the next hop.

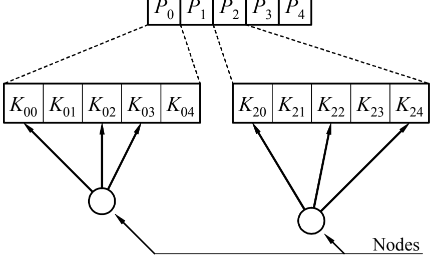


Fig. 2. Key assignments in SEF

When the sink receives a report, it checks whether the report carries t MACs and key indices. Then the sink verifies the correctness of every MAC and the associated key indices because it knows all the keys. If one mismatch happens the report is rejected. In this way, the sink serves as the final guard.

SEF design harnesses the advantage of large-scale by requiring endorsement of an event report from multiple detecting nodes and by detecting false reports through collaborative filtering of all forwarding nodes along the path (Ye *et al.*, 2005). However, SEF suffers from the major drawback that if a certain number of nodes, no matter where they locate, have been compromised, the adversary may claim false reports at an arbitrary location without the risk of being detected (Li and Wu, 2006). SEF also does not address false data injection attacks on legitimate reports. A compromised node can stall the proper reporting of a real event by injecting false data into the legitimate report that it to be filtered out.

2.2 System Models and Assumptions

This paper considers a large-scale sensor network composed of a large number of hardware-restricted sensor nodes in which the nodes are deployed in high density, so that a report can be cooperatively generated when an event is detected by multiple nodes. When this occurs, one node is elected to be the report generation node. This is a complex process, the task of choosing a node as the report generation node is out of the scope of this paper.

The attackers can be classified as either outsider or insider. The former is an attacker with no keying material beyond that generally available. The attacker may simply passively eavesdrop on radio transmissions. The latter is an attacker with access to information, obtained by keying material. We assume that attackers may be able to either compromise a node through the wireless channel, or even physically capture a node to obtain the security information installed in the node. However, we assume that the sink will not be compromised, because the protection at the sink is strong enough to defeat such compromise efforts. Once compromised, a node can be used for two types of attacks: the false report injection attacks and the false data injection attacks on legitimate reports. The compromised nodes also can launch several other attacks. For example, compromised nodes may drop every report received. However, this is out of the scope of this paper.

3. False Report Detection Method

In this section, we propose a fuzzy logic-based false report detection method (FRD), which offers a solution to problems of detection for the false report injection attacks and false data injection attacks on legitimate reports. FRD takes SEF framework as its base and improves it using four methods: report generation, en-route filtering, sink verification, and fuzzy rule-based system.

3.1 Report Generation

When an event occurs, multiple surrounding sensors collectively generate a report that carries predefined q MACs and the associated key indices (Fig. 3(a)). Then the report attaches check fields which are used to detect the false data injection attacks on legitimate reports. The check fields set corresponding bits to 0. After report generation, the center-of-stimulus (CoS) forward the report to the next hop. The report should be:

$$\text{Report: } \{event,\ index_1,\ MAC_1,\ index_2,\ MAC_2,\ \cdots,\ index_q,\ MAC_q,\ c_1,\ c_2\ \cdots\ c_q\}. \quad (1)$$

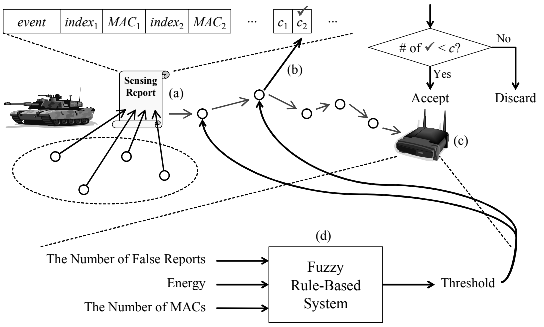


Fig. 3. FRD overview

The threshold value of c represents a trade off between the false report injection attacks, the false data injection attacks on legitimate reports, and energy consumption. The sink can set a system-wide value for the threshold value of c.

3.2 En-route Filtering

When a node receives a report, it will check whether there are q key indices and q MACs. It will then check whether the node has any of the keys of the report. If the node does not have any of the keys of the report, the node forwards the report to the next hop. Otherwise, the node computes MAC using its own key and then compares this with the report's MAC. The report is transmitted to the next hop if the attached one corresponds with the reproduced MAC. If an incorrect MAC is detected, the check fields set corresponding bits to 1 (Fig. 3(b)). The node will also check whether the number of incorrect MACs is less than the threshold value of c. If the number of incorrect MACs is greater than the threshold value of c, the report is discarded; otherwise the report is forwarded.

3.3 Sink Verification

When the sink receives a report, it checks whether the report carries t MACs and key indices. Then, the sink verifies the correctness of every MAC and the associated key indices because it knows all the keys. If one mismatch happens, the fields set corresponding bits to 1. The node will also check whether the number of incorrect MACs is less than the threshold value of c

(Fig. 3(c)). If the number of incorrect MAC has less than the threshold value of *c*, the report is accepted; otherwise the report is discarded. In this way, the sink serves as the final guard.

3.4 Fuzzy Rule-based System

After the sink verification, fuzzy rule-based system endows each node with the ability to make decisions against the two types of attack. In our approach, the system is implemented on the sink and the sink uses its fuzzy rule-based system to generate the optimal threshold value (Fig. 3(d)). One aspect of the appeal of fuzzy rule-based systems is that they can be used for approximate reasoning, which is particularly important when there is uncertainty in reasoning, in addition to imprecision in data (Serrano and Seraji, 2007). This threshold value will be sent to nodes in order to decide whether the report is legitimate.

FRD receives reports as inputs to the fuzzy logic and the fuzzification module converts inputs into fuzzy linguistic variable inputs. The number of false reports can be used to determine the attack type. A large number of false reports indicates that the attacker is launching false report injection attacks on the network. Under such situation, a small threshold value can save energy since it makes false reports to be dropped earlier. On the other hand, if no false report has been reported, a large threshold value would be recommended to mitigate the threat of false data injection attacks on legitimate reports. The energy is the most important resource that should be considered in sensor networks. Generally, sensor nodes are limited in power and irreplaceable since these nodes have limited capacity and are unattended (Chi and Cho, 2006). Therefore, we also have to choose a threshold value based on the energy of nodes. The threshold value should be determined based on the number of MACs since the number of incorrect MACs may be proportional to such number. If each report has a large number of MACs, we may well as choose a large threshold value. Conversely, a small threshold value should be chosen when each report carries a few MACs.

There are 5 types of linguistic variables as inputs to the fuzzy logic. The number of false reports per 5 reports can be represented as: Very Small (VS), Small (S), Medium (M), Large (L), and Very Large (VL). The nodes' energy to the average energy of the forwarding path includes 3 subsets: Large (L), Medium (M) and Small (S). The number of MACs for each report can be represented as: Very Small (VS), Small (S), Medium (M), Large (L), and Very Large (VL). The membership functions are shown in Fig. 4.

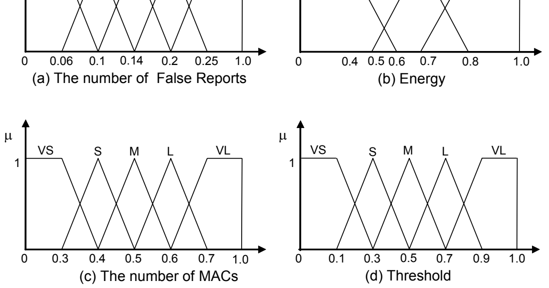
In this paper, the fuzzy inference engine converts the input data into the threshold value of false reports. In our simulation, we used the Free Fuzzy Logic Library (FFLL) to generate the Fuzzy logic. The fuzzy rules input in the FFLL are as follows:

If it is reported or estimated that no node has been compromised, a security threshold value can be very large (e.g., maximum value).

RULE 12:
IF (THE NUMBER OF FALSE REPORTS IS VS)
AND (AVERAGE ENERGY IS L)
AND (THE NUMBER OF MACS IS S)
THEN (THRESHOLD OF FALSE REPORT IS VL)

If a few nodes are compromised and reports have sufficient MACs, a security threshold value greater than the number of compromised nodes.

RULE 29:
IF (THE NUMBER OF FALSE REPORTS IS S)
AND (AVERAGE ENERGY IS L)



(a) The number of False Reports

(b) Energy

(c) The number of MACs

(d) Threshold

Fig. 4. Membership functions

AND (THE NUMBER OF MACS IS L)
THEN (THRESHOLD OF FALSE REPORT IS L)

If the number of compromised node exceeds the number of MACs, the proposed method may be inefficient and useless. Thus, a security threshold value set a very small (i.e., 0).

RULE 74:
IF (THE NUMBER OF FALSE REPORTS IS VL)
AND (AVERAGE ENERGY IS L)
AND (THE NUMBER OF MACS IS VL)
THEN (THRESHOLD OF FALSE REPORT IS VS)

The output is a threshold of check fields, and its membership function is shown in Fig. 3(d). In this paper, the Center of Area (COA) is used to obtain a crisp output to control threshold of incorrect MACs.

4. Simulation Results

We consider three existing scheme for comparison: SEF, PVFS, and FRD. As a result of the space limitation of this paper, we only present the results of false report filtering and energy consumption. All methods are simulated on simulator which generates random deployment and homogeneous nodes. We also generate random key assignment and random false reports. In case of PVFS, this method brings higher probability to filter out or accept a report with votes in the first few steps (Li and Wu, 2006). We use 10,000 sensor nodes in fields. The sink and the source, with about 100 hop in between. We use a whole key consisting of 1,000 keys, divided into 10 groups, with 100 keys in each group. Each node has 30 keys. Then we are assume that report transmission consumes the same amount of energy between any pair of nodes. Based on (Ye *et al*., 2005), transmit = 16.25 J/byte, receive = 12.5 J/byte, original packet size = 24 bytes, key index = 10 bits, and shorter MACs = 64 bits/MAC. In the simulation, we randomly generated 10,000 reports - 1,000 false reports and 1,000 false data injection on real reports. Then, the results are averaged over ten independent measures.

Fig. 5 compares the percentage of dropped false reports of SEF, PVFS ($T_f = 3$), and FRD. The longer a report travels, the more increase the filtering performance of FRD as shown in the figure. However, the FRD has a lower filtering ratio than SEF and a higher filtering ratio than PVFS, when the report travels from the source to the sink. When the application only cares about the false reports injection attacks, we would renegotiate fuzzy if-then rules.

Fig. 6 compares the dropped reports of false data injection attack on the legitimate report of SEF, PVFS, and FRD. When false data injection attack occurs, FRD always has a higher performance than the other methods. In case of false data injection attack, SEF always filter out legitimate reports in the sink. However, FRD and PVFS determined by the threshold value. Moreover, FRD change the threshold value by using statistical data on false reports.

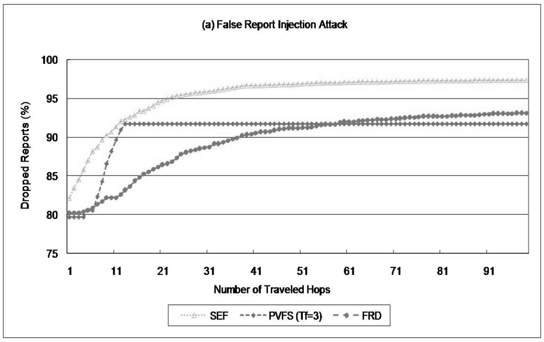


Fig. 5. Portion of dropped false reports

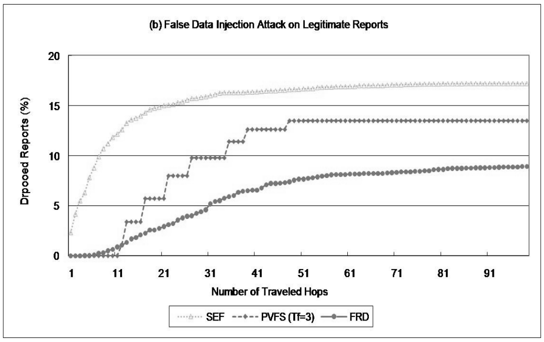


Fig. 6. Dropped reports of false data injection attack

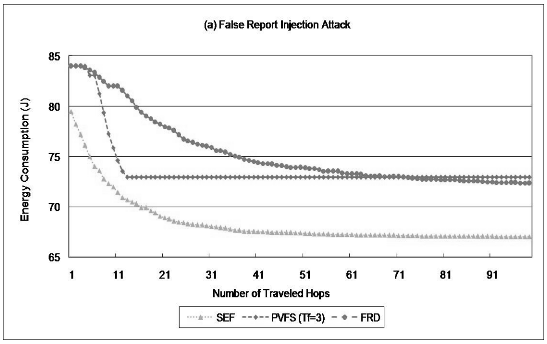


Fig. 7. Energy consumption of SEF, PVFS, and FRD

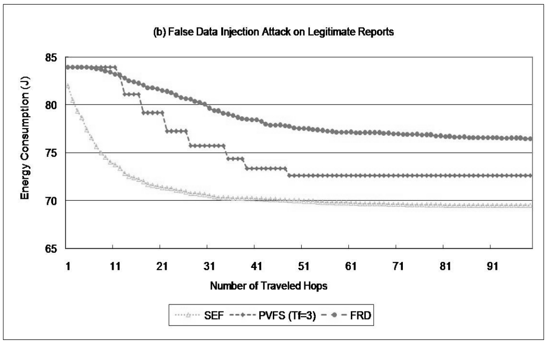


Fig. 8. Energy saving of FRD

Fig. 7 shows the energy consumption of SEF, PVFS (T_f = 3), and FRD on a false report injection attack. FRD always has more energy consumption than other methods in this figure. Sensor networks cannot classify into two types, false report injection attack and false data injection attack on legitimate reports. Since we more focus on the false data injection attack, FRD saves a low percentage of energy that may be consumed by a false report injection attack. However, there is little difference in energy consumption between them.

Fig. 8 shows the energy consumption caused by false data injection attack on legitimate reports. Because an attacker may inject a false data for every normal report, reports are delivered to the sink. Thus, FRD always has more energy consumption than other methods. Though some reports are not delivered due to the security threshold value, our method is more deliver reports than other methods.

5. Conclusion

This paper proposes FRD, to offer a solution to problems of detection for both the false report injection attack and false data injection attack on legitimate report. The method determines the threshold of check fields by considering the number of false reports, average energy of nodes, and the number of MACs. The simulation shows that this scheme is efficient with respect to the security it provides, and allows a tradeoff between security and performance.

As future work, other false negative attacks that can drop every report or modify the report it receives will be considered.

References

1. Andress, A. and Andress, M. (2001), *Surviving Security: How to Integrate the Process, and Technology*, SAMS.
2. Chan, H., Perrig, A. and Song, D. (2003), “Random Key Predistribution Schemes for Sensor Networks”, *Proc. of IEEE Symposium on Security and Privacy*, pp. 197-213.2.
3. Chi, S. H. and Cho, T. H. (2006), “Fuzzy Logic Based Propagation Limiting Method for Message Routing in Wireless Sensor Networks”, *Lecture Notes in Computer Science*, Vol. 3983, pp. 58-67.
4. Ferreira, A. C., Vilaca, M, A,, Oliveira, L. B., Habib, E., Wong, H. C. and Loureiro, A. A. (2005), “On the Security of Cluster-Based Communication Protocols for Wireless Sensor Networks”, *Lecture Notes in Computer Science*, Vol. 3420, pp. 449-458.
5. Li, F. and Wu, J. (2006), “A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks”, *Proc of International Conference on Communications and Mobile Computing*, pp. 27-32.1.
6. Olariu, S., Xu, Q., Eltoweissy, M., Wadaa, A. and Zomaya, A. Y. (2005), “Protecting the Communication Structure in Sensor Networks”, *International Journal of Distributed Sensor Networks*, Vol. 1, No.2, pp. 187-203.
7. Perrig, A., Stankovic, J. and Wagner, D. (2004), “Security in Wireless Sensor Networks”, *Communications of the ACM*, Vol. 47, No. 6, pp. 53-57.
8. Proctor, P. E. (2000), *The Practical Intrusion Detection Handbook*, Prentice Hall.

9. Serrano, N. and Seraji, H. (2007), "Landing Site Selection using Fuzzy Rule-Based Reasoning", *Proc. of IEEE International Conference on Robotics and Automation*, pp. 4899-4904.
10. Xiao, Y. (2006), *Security in Sensor Networks*, AUERBACH.
11. Yang, H. and Lu, S. (2004), "Commutative Cipher Based En-route Filtering in Wireless Sensor Networks", *Proc. of IEEE Vehicular Technology Conference*, Vol. 60, No. 2, pp. 1223-1227.
12. Yang, H., Ye, F., Yuan, Y., Lu, S. and Arbaugh, W. (2005), "Toward Resilient Security in Wireless Sensor Networks", *Proc. of International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 34-45.
13. Ye, F., Luo, H., Lu, S. and Zhang, L. (2005), "Statistical En-Route Filtering of Injected False Data in Sensor Networks", *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 4, pp. 839-850.
14. Zhu, S., Setia, S., Jajodia, S. and Ning, P. (2004), "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks", *Proc. of IEEE Symposium on Security and Privacy*, pp. 259-271.
15. Zhang, Y., Yang, J. and Vu, H. T. (2006), "The Interleaved Authentication for Filtering False Reports in Multipath Routing based Sensor Networks", *Parallel and Distributed Processing Symposium*, pp. 10-19.
16. Free Fuzzy Logic Library (FFLL), http://ffll.sourceforge.net/

김문수 (chiunostra@gmail.com)

2006 성균관대학교 정보통신공학부 학사
2008 성균관대학교 정보통신공학부 석사
2008 ~ 현재 LG전자

관심분야 : 무선 센서 네트워크, 모델링 및 시뮬레이션, 인공지능, 네트워크 보안

이해영 (sofware@ece.skku.ac.kr)

2003 성균관대학교 정보통신공학부 학사
2003 ~ 현재 성균관대학교 정보통신공학부 석박사통합과정

관심분야 : 무선 센서 네트워크, 지능 시스템, 컴퓨터 지원 설계, 인공지능, 모델링 및 시뮬레이션

조대호 (taecho@ece.skku.ac.kr)

1983 성균관대학교 전자공학과 학사
1987 Univ. of Alabama 전자공학과 석사
1993 Univ. of Arizona 전자 및 컴퓨터공학과 박사
1995 ~ 현재 성균관대학교 정보통신공학부 교수

관심분야 : 무선 센서 네트워크, 모델링 및 시뮬레이션, 지능 시스템, 모델링 방법론