An En-route Filtering Scheme Based on Priority as determined by the Fuzzy rule-based system

Sang Jin Lee[†] **and Tae Ho Cho**[††],

Sungkyunkwan University, Suwon 440-746, Republic of Korea

Summary
Wireless sensor networks (WSNs) can be generally easily compromised by attackers since the networks are deployed in hostile environments. The attackers can inject a false report into the networks or fabricate MACs (message authentication codes) on real reports through compromised nodes. The attacks break down the networks as a result of the dissipation of energy or the interception of the message. Li and Wu proposed the PVFS (probabilistic voting-based filtering scheme) in order to protect against this type of attack. In the PVFS, determining the number of votes is very important since it determines the trade-off between the security level and the energy consumption.

In this paper, we propose an EFSP (En-route Filtering Scheme based on Priority) to control the number of votes. The EFSP determines priorities through the fuzzy rule-based system. Each cluster head receives priority from the base station and then the cluster head attaches a specified number of votes to the report according to the priority. We demonstrate the efficiency of our EFSP through the simulation results.

Key words:
Wireless sensor networks, false injection attack, PVFS (probabilistic voting-based filtering scheme), fuzzy rule-based system.

1. Introduction

Recent advances in wireless communications and electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and they communicate unfettered over short distances [1].

Wireless sensor networks (WSNs) consist of small nodes with sensing, computation and wireless communications capabilities. WSNs can be applied to numerous applications such as target field imaging, intrusion detection, weather monitoring, security and tactical surveillance, distributing computing and detecting ambient conditions [2].

WSNs have a limited capability in terms of the available energy, the memory capacity and the processing speed, and they are exposed to a hostile environment [3]. Thus, sensor nodes may be captured or compromised by adversaries, and secret information such as the symmetric key may be revealed to the adversaries. Adversaries can easily inject false data reports of non-existent events or fake readings (Fig. 1(a)) and false votes on real reports (Fig. 1(b)) [8].

Such attacks may cause false alarms, and they exhaust the limited energy of the nodes that are forwarding these reports, and so the attacks reduce the lifetime of sensor networks [4].

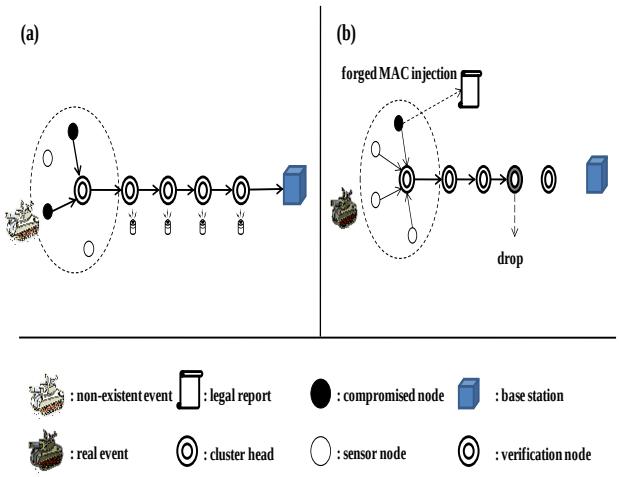

Fig. 1 False date injection and forged MAC attacks.

To minimize damage, the fabricated reports should be dropped en-route as early as possible, and the few elusive ones should be rejected at the base station [6]. Various security solutions [4-8] and adaptive methods [10-11] have been proposed to detect and drop false reports. A probability voting-based filtering scheme is one of these solutions.

In PVFS, the choice of the security threshold value is very important since it trades off between the security level and the amount of energy consumption. A large threshold value allows false reports to be more easily detected, but it consumes more energy during forwarding. In contrast, a small threshold value may consume less energy, but it will cause inefficient filtering or it may even be useless if a large number of nodes have been compromised. We

Manuscript received July 5, 2009
Manuscript revised July 20, 2009

should choose the threshold value such that it provides sufficient resilience, whilst still conserving energy [7].

In this paper, we propose an En-route Filtering Scheme based on Priority as determined by the Fuzzy rule-based system to select an appropriate threshold value. A fuzzy rule-based system is exploited to determine priority, which implies the required number of votes per report.

2. Related Work

2.1 PVFS (A probability voting-based filtering scheme)

To protect wireless sensor networks (WSNs) from two types of attacks, Li and Wu proposed PVFS [8]. In PVFS, the vote is used to authenticate the real reports. In this paper, we refer to the vote as a security threshold value. PVFS consists of three phases: key assignment, report generation and en-route filtering.

In the key assignment phase, each cluster organizes L keys from the global key pool of n keys. After each cluster organizes the L keys, the cluster head selects a verification node in the upstream CHs.

The verification node will be selected with a probability *P* given as the formula (1) [8]:

$$p = \frac{d_i}{d_o} \quad (1)$$

d_0 represents the distance between the original cluster head (CH) and the base station, and d_i represents the distance between the upstream CH and the base station.

In the report generation phase, if the sensor node senses an event, then each node generates a vote using its pre-loaded key from the global key pool. The event reports have to contain distinct s votes. If the event reports do not have a sufficient number of votes, then they cannot be generated.

In the en-route filtering phase, each verification node will check on the vote that is generated by nodes in the same cluster. If it is true, then the event report will be passed, otherwise it will be dropped. It will then verify a vote using the corresponding verification key. The node will check that the number of the false reports or the number of the true votes among the verified votes has reached the threshold.

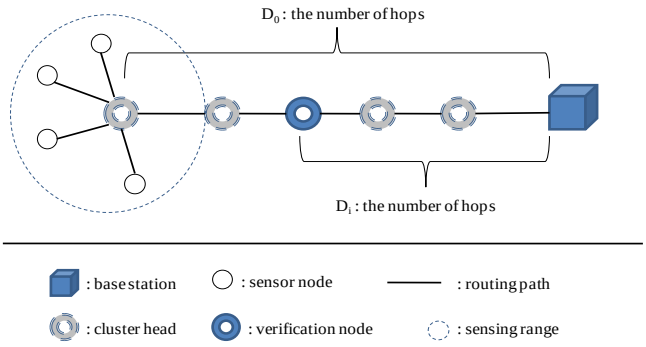

Fig. 2 Selection of the verification nodes.

However, PVFS always has a static security threshold value after being selected. This is unfair on dynamic environments in WSNs since each cluster has a different status such as the number of cluster nodes and the key assignment.

3. Proposed method

3.1 Assumption

We assume that a sensor network consists of a large number of small sensor nodes. Nodes within the cluster can elect one cluster head from amongst them. To balance the energy consumption, all the nodes of the same cluster may take turns playing the role of the cluster head. As nodes are not equipped with tamper-resistant hardware, they can be compromised by adversaries and they can be used to inject false reports. However, the base station (BS) cannot be compromised. We also assume the BS can determine the estimated distance from the BS to each cluster and it can determine the rate of reports that are rejected by the BS. We further assume that the BS has a mechanism to authenticate the broadcast messages (e.g., based on μTESLA [9]), and every node can verify the broadcast messages.

3.2 Our En-route Filtering Scheme based on Priority (EFSP)

Our proposed method, an En-route Filtering Scheme based on Priority (EFSP), is based on PVFS.

The BS periodically determines the priority of the security (SP) for each CH through a fuzzy rule-based system to determine an adaptive security threshold that can be achieved with sufficient detection ability while conserving energy consumption. The rate of the false reports rejected by the BS (RRB), the frequency of the event report (FE) and the estimated distance from the BS to each cluster (DBS) are all used to determine the SP.

The SP changes from the priority of the security to the number of votes attached to reports through a simple formula (2).

$$SP = f(\text{priority}) \times L \quad (2)$$

L is the number of nodes in one cluster and the function *f* means the fuzzy rule-based system.

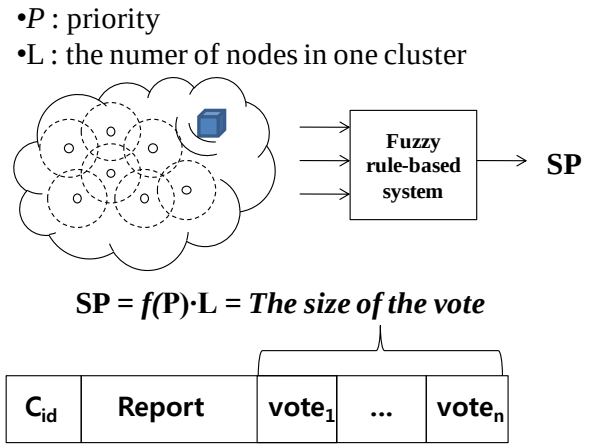

Fig. 3 The overview of EFSP.

We used the Fuzzy rule-based system for determining the priority of each CH. The following figures are the membership function of this fuzzy rule-based system input parameters (Fig. 4).

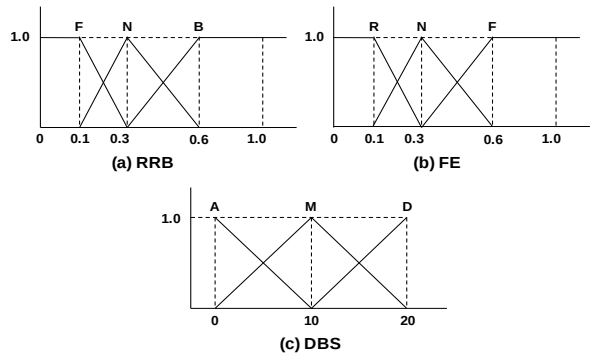

Fig. 4 Input parameters.

Input parameters

The RRB (The rate of false reports rejected by the BS) needs to anticipate the ratio of the generated false reports. If the RRB is high, then the probability of generating a false report may become higher than the RRB, which is not high. Thus, we used this parameter as the input value.

When event reports frequently occur, the probability of a false report may be more increased than when an event report is not frequent. Thus, we need to adjust the security threshold value according to the FE (Frequency of the event report).

The sensor nodes near the BS consume less energy than other nodes while forwarding reports to the BS. When a false report occurs, the unfiltered reports near the BS have less travel hops than those generated by a compromised node that is further away from the BS. Therefore, we have to consider the DBS to provide the efficient energy uage and sufficient security ability.

The labels of the fuzzy variables are represented as follows:

- RRB = {F (Fine), N (Normal), B (Bad)} (Fig. 4(a))
- FE = {R (Rare), N (Normal), F (Frequency)} (Fig. 4(b))
- DBS = {A (Around), M (Medium), D (Distant)} (Fig. 4(c))

Output parameter

The output parameter of the fuzzy rule-based system is SP = {VS (Very Small), S (Small), M (Medium), L (Large), VL (Very Large)}, which is represented by the membership functions, as shown in Fig. 5.

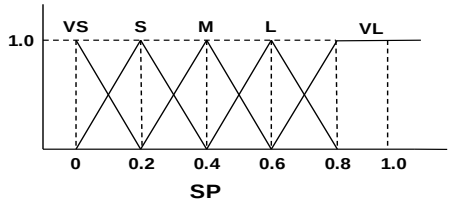

Fig. 5 output parameter.

Table 1 shows a portion of the entire fuzzy if-then rules. The fuzzy if-then rules determine the SP based on the RRB and the MAR.

Table 1: The portion of the fuzzy if-then rules.

RULE #	IF			THEN
	RRB	FE	DBS	SP
0	F	F	D	M
1	F	N	D	L
2	F	R	D	S
3	B	F	D	VL
4	B	N	D	VL
5	B	R	D	L

Rule 0: If RRB is F (fine) and FE is F (frequency), then it means the network is well protected from attackers while event reports are being frequently generated. Thus, SP is determined as M (medium).

Rule 3: If RRB is B (bad) and FE is F (frequency), then it means the filtering scheme cannot provide sufficient security power with the current security threshold vale. Therefore, the SP will be increased in the VL (very large).

Rule 2, 5: If event reports are not frequently generated, then SP prefers to be decreased since the verification process also wastes energy. The eluded reports can be detected and dropped as the BS.

4. Simulation Results

We compare the original PVFS and the EFSP. In the simulation background; we use a virtual sensor network that has 400 randomly distributed clusters; each cluster consists of 10 nodes and the false report rate is from thirty percent to eighty percent.

Fig. 6 shows the number of dead nodes when false reports occurred at a rate of 30%. The EFSP preserves energy more efficiently than the original PVFS while providing efficient security power (as shown by Fig. 7).

In the PVFS, the security threshold value is always static. It means it cannot have it both ways for security and energy. The PVFS with a large security threshold (Fig. 6: PVFS(7)) can provide sufficient security power that also conserves energy by quickly dropping false reports.

However, this only happened when false reports frequently occurred. Legitimate reports may consume more energy than a small security threshold (Fig. 6: PVFS(3)) because the verification processing is implemented for both false reports and legitimate reports. That is, if the rate of false traffic reports is not high in the networks, then the total energy consumption with larger security is greater than the energy consumed with a smaller security.

The EFSP can control the security threshold value by using the fuzzy rule-based system, and so the EFSP can conserve energy as compared with the original PVFS as you can see from the simulation result (Fig. 6).

Fig. 7 shows the rate of filtered false reports when false reports occurred at a rate of 80%. The EFSP with an adaptive security threshold, which is determined by the fuzzy rule-based system, can provide sufficient security power.

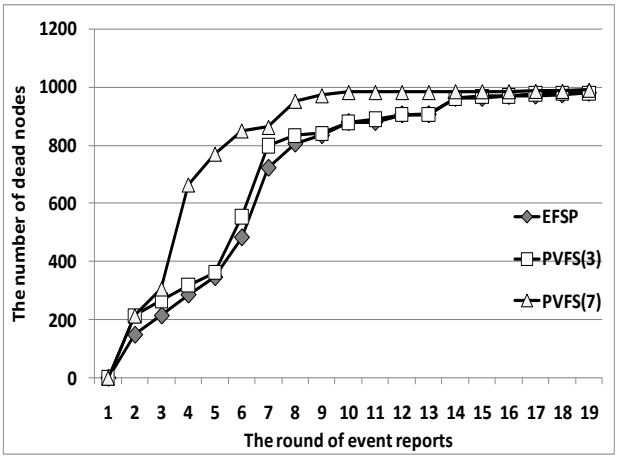

Fig. 6 The number of dead nodes.

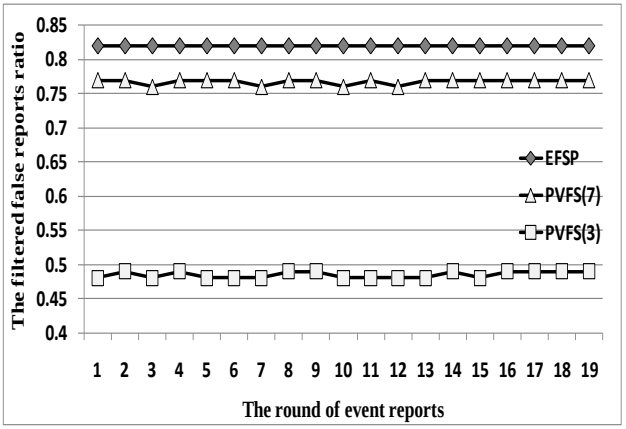

Fig. 7 The filtered reports ratio.

We have demonstrated that the EFSP can determine the adaptive security threshold value such that it provides sufficient resilience between the security level and energy usage through the two simulation results.

5. Conclusion

The adaptive security threshold value, which is the output of the fuzzy rule-based system, plays a vital role in enhancing the capability of the PVFS. It determines the trade-off between the security level and the amount of energy consumed.

The proposed EFSP uses the rate of false reports rejected by the base station, the frequency of event reports and the estimated distance from the base station to each cluster as inputs to the fuzzy rule-based system to determine the security threshold value. As shown by our simulation, our proposed method exhibits effective performance in terms

of balancing between the energy consumption and the security through the fuzzy rule-based system.

Acknowledgment

This work was supported by a Korean Research Foundation Grant funded by the Korean Government (KRF-2008-313-D00827)

References

[1] Akyildiz, I.F.; Weilian Su; Sankarasubramaniam, Y.; Cayirci, E., "*A survey on sensor networks*," *Communications Magazine, IEEE* , vol.40, no.8, pp. 102-114, Aug 2002.

[2] J.N. Al-K Karaki , and A.E. Kamal, "*Routing techniques in wireless sensor networks: a survey*", IEEE Wireless Communication Mag., vol. 11, no. 6, pp. 6-28, 2004.

[3] D. Djenouri and L. Khelladi, "*A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks*", IEEE Communication Surveys and Tutorials, vol. 7, no. 4, pp. 2-28, December 2005.

[4] Z. Yu and Y. Guan, "*A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks*", in Proc. IEEE INFOCOM'06, Apr. 2006.

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

[6] Yang H, Lu S. Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks. In Proc. VTC, 2003, pp.1223-1227.

[7] Ye F, Luo H, Lu S., "*Statistical En-Route Filtering of Injected False Data in Sensor Networks*", IEEE J. Sel. Area Comm., 2005, 23(4): 839-850.

[8] F. Li and J. Wu, "*A probabilistic voting-based filtering scheme in wireless sensor networks*", Proc. IWCMC, pp.27–32, July 2006.

[9] Perrig A, Szewczyk R, Tygar J D, Wen V, Culler D E., "*SPINS: Security Protocols for Sensor Networks*", Wirel. Netw., 2002, 8(5): 521-534

[10] H.Y. Lee and T.H. Cho, "*Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks*", Lect. Notes Comput. Sc., vol.4317, pp.116-127, Dec. 2006

[11] H.Y. Lee and T.H. Cho, "*Fuzzy Adaptive Selection of Filtering Schemes for Energy Saving in Sensor Networks*", IEICE Transactions on Communications, vol. E90-B, no.12, pp.3346-3353, Dec. 2007.

Sang Jin Lee received his B.S. degree in Software Engineering from Baekseok University, South Korea, in August 2007. 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 and security.

Tae Ho Cho received his Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and his 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.