

Fuzzy-based Determination Method for Redistributing Keys in Sensor Networks

Chung Il Sun*, Man Ho Han*, and Tae Ho Cho*

* School of Information and Computer Engineering, Sungkyunkwan University, Korea
cisun@ece.skku.ac.kr, mhhan@ece.skku.ac.kr, taecho@ece.skku.ac.kr

Abstract— Wireless Sensor Networks (WSNs) are ad-hoc mobile networks that contain sensor nodes with limited energy resource and wireless communication facilities. WSNs are typically deployed in wide, unattended, and hostile areas. Therefore, sensor nodes are subject to compromise physically and surreptitious use by an adversary. An adversary can capture them to inject an incorrect data into the sensor field, which causes unnecessary energy consumption of nodes. A dynamic en-route filtering scheme is proposed to detect and drop the fabricated data as soon as possible. In this scheme, the authentication keys used to verify event reports are redistributed to neighbour nodes to enhance the detection power during the post-deployment phase. In this paper, we present a fuzzy based key redistribution determining method in which when keys are redistributed to neighbour nodes to determine by a fuzzy system with the network situation. The proposed method can provide more efficient energy consumption and sufficient detection power.

Keywords— Wireless sensor networks, key redistribution, en-route filtering, fuzzy system, fabricated data

I. INTRODUCTION

Wireless sensor networks with hundreds or thousands of low-cost, limited power, and tiny sensors have enable effectively monitor different types of environments by sensing and collecting information. Sensor nodes can be densely deployed in unattended environments such as hostile area, battle field, and civil environment [1]. Sensor networks include tiny sensor nodes with sensing, restricted resource, wireless communication, and computing facilities [2]. Due to the characteristics of operation in the unattended environment, sensor networks are subjected several threats and vulnerable to physical attacks. Therefore, an adversary can capture some nodes to steal the information that includes the authentication keys, routing tables, and sensing data. Using information of nodes adversary can make fabricated reports and then injects them into the sensor field. Transmitting of fabricated reports can not only cause the false alarm but also reduce the lifetime of sensor networks (Fig. 1).

To minimize damage, fabricated reports should be filtered out as soon as possible, and few elude ones should be further rejected at the base station [3]. Researchers have proposed

several symmetric cryptography key based security schemes [4-8] to drop fabricated reports during transmitting process. Yu and Guan [4] proposed the dynamic en-route filtering scheme (DEF) to filter out such fabricated reports. DEF differs from existing solutions in that it can better deal with the dynamic topology of sensor field and outperform them in term of energy efficiency in large-scale networks. In this scheme, sensing reports that include sensing data, event location, and event information are endorsed and verified by forwarding nodes using authentication keys, which are distributed after deployment phase. DEF can provide sufficient detection power even in heavy changes of the network topology [9]. However, If authentication keys are disseminated to increase the detection power frequently, the restrict energy resource of nodes can be drained in key redistribution phase. Because of this phase demands a lot of energy consumption of nodes for transmitting key data. The execution of redistribution phase of authentication is determined prudently by considering the network situation. In this paper, we propose a key redistribution determining method using fuzzy system that focuses on the dynamic topology. Two fuzzy systems are used to determine the execution of redistribution phase. The proposed method can provide enough detection power, while it does not consume the energy resource.

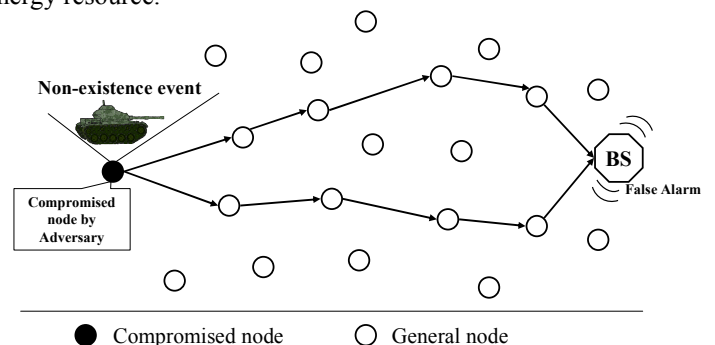


Figure 1. False data injection attack

The remainder of the paper is organized as follows: Section 2 briefly describes DEF and our motivation. Section 3 introduces the proposed method in detail. Section 4 reviews the simulation result. Finally, the conclusion and future work is discussed in Section 5.

II. BACKGROUND

A. Dynamic en-route filtering scheme

Yu and Guan proposed DEF [4] to detect and drop fabricated reports in sensor networks. Topology of sensor network can easily be changed. DEF can better deal with dynamic topology of sensor networks and outperform them in terms of energy efficiency [10]. DEF comprise of three phase: *pre-deployment*, *filtering phase*, and *post-deployment*.

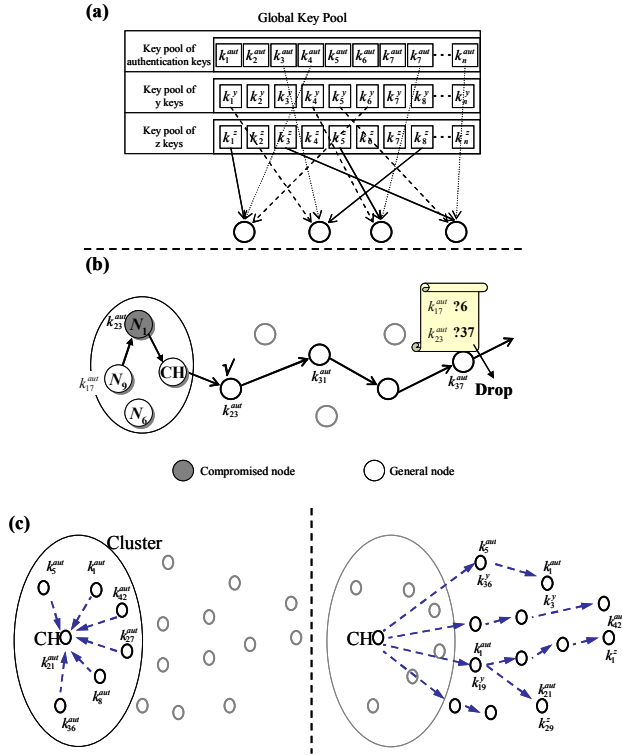


Figure 2. Three phase in DEF

Pre-deployment phase is executed before initial deployment. In this phase, entire sensor nodes preload a seed authentication key with $l + 1$ security y-keys and one z-key randomly picked from a global key pool (Fig. 2(a)). Sensor nodes use the authentication key to make and verify event reports. Moreover, y-key and z-key are used to disseminate the authentication keys generated by a cluster head to neighbour nodes. In the post-deployment phase, every cluster node encrypts its authentication key by using $l+1$ y-keys and sends the $l+1$ encrypted authentication keys to its cluster head (CH). Then CH disseminates the authentication keys of all nodes in the cluster to q (>0) neighbor nodes (Fig. 2(c)). When the nodes receive the authentication keys, if its secret key happens to be the same one as the secret key used to encrypt the authentication key, it decrypts the authentication keys using its secret keys. In the filtering phase, every event reports are verified by forwarding nodes using the disseminated authentication keys. When an interesting event occurs in a certain area, event sensing nodes send event data with message authentication codes (MACs) generated by

using its authentication key to its CH. CH generates the event report using the collected MACs and sends it toward the base station(BS) through the forwarding nodes. Each forwarding nodes verifies the correctness of the MACs attached at the event report using its authentication key (Fig. 2(b)).

B. Motivation

In DEF, it is important that when the authentication keys are redistributed to the neighbor nodes, since this process can enhance the detection power of the network. However, key redistribution process consumes a lot of energy of sensor nodes. Sensor nodes have to conserve its energy resource, since it is limited and not easy recharged. We should carefully determine the time to redistribute the authentication keys and execution of this process with the consideration of the network conditions using two fuzzy systems.

III. FUZZY KEY REDISTRIBUTION METHOD

A. Assumption

We consider a sensor networks composed of a large number of tiny sensor nodes. We assume that sensor nodes form a number of clusters after initial deployment. Each sensor node has a clustering mechanism that organizes a cluster automatically. One of cluster nodes is elected to be a cluster head, which aggregates a sensing data from the other nodes in that cluster and produce an event report. We further assume all nodes of the same cluster may take turns playing the role of cluster head to balance of energy consumption of nodes. We assume that the base station and cluster head cannot be compromised. The base station can know the information of the keys assigned to whole nodes, the estimated mobility of the sensor filed, and the energy level of the network. We further assume the base station has a mechanism to authenticate a broadcast message.

B. Overview

Two fuzzy systems in our method are used to determine the time to execute the key redistribution phase e . One fuzzy system determines the fuzzy security value (FSSV) considering the energy level of the network (ELN), the ratio of the false traffic (RFT). The fuzzy security value represents the general state of network. Another fuzzy system determines whether execution of the key redistribution or not considering network conditions (FSER). Three factors – the fuzzy security value (FSV), the energy level of CH (ELC), and distance from base station to the cluster head (DIS). The fuzzy security value that is output value of FSSV is used as input value of the FSER. The proposed fuzzy systems consider the condition of the sensor network and decide the best time to redistribute authentication keys.

C. Input Factors of two Fuzzy Systems

Two fuzzy systems FSSV and FSER determine e by considering the situation of the networks. FSSV uses two input factors: ELN and RFT.

1) ELN: The energy is the critical important resource that should be considered in the networks. In general, sensor nodes have a limited and irreplaceable battery, since these nodes have restrictive capacity and are unattended. When sensor nodes diffuse authentication keys, they should consider their energy since its phase consumes a lot of energy. If sensor nodes in a cluster region have low energy, they should restrict that phase. However, they should disseminate authentication keys when their energy is sufficient to enhance the detection power. Thus, we have to determine the state that represents the security value of network based on the energy level of the network.

2) RFT: The ratio of the false traffic is also considered carefully. If amount of fabricated reports of the entire network is large, the security level of network is low, so each cluster head should execute the key redistribution to enhance the detection power frequently. However, if the ratio of the false traffic is low, the key redistribution should be executed to conserve the energy of network loosely. Therefore, we further have to determine the state of the network based on the ratio of the false traffic.

Using the fuzzy security value (FSV) which is output of the FSSV, FSER determine the execution of the key redistribution with two factors: ELC and DIS

3) ELC: The energy level of cluster head is considered to determine FSER. We already assume the network has a cluster-mechanism that organizes a cluster automatically. All nodes in the same cluster will take turns playing the role of cluster head. CH may consume much energy than cluster nodes since it have to distribute the authentication keys to q nodes. Therefore, if current CH has not much energy to diffuse the authentication keys, it cannot redistribute the authentication keys to neighbor nodes. Thus, we have to determine e based on the energy level of the cluster head.

4) DIS: The distance from a cluster head to the base station is considered to determine FSER. If the cluster region is located far from the base station, the cluster head in that region should diffuse the authentication keys frequently because of the false report generated in that region can be detected and dropped by forwarding node with high probability. However, the cluster head in a region located closed by the base station should seldom redistribute the authentication keys, since it has the low probability for filtering out fabricated reports. Moreover, nodes located in that region may be consumed more energy than other nodes, since they have to transmit the event report forwarded toward the base station. Therefore, we further have to determine the e based on the distance from a cluster head to the base station.

D. Fuzzy Rule-based Systems

FSER exploits a fuzzy rule based system to determine the time to execution phase. The membership functions of the three input factors that determine FSER are shown in Fig. 3(a), (b), and (c). The membership function of the output parameter, FSER, is illustrated in Fig. 3(d). The labels in the fuzzy variables are presented as follows.

- FSV = {W (Weak), N (Normal), S (Strong)}
- ELC = {VL (Very Low), L (Low), E (Enough)}
- DIS = {N (Near), M (Middle), F (Far)}
- e = { UC (Unchanged), CON (Consider), C (Change)}

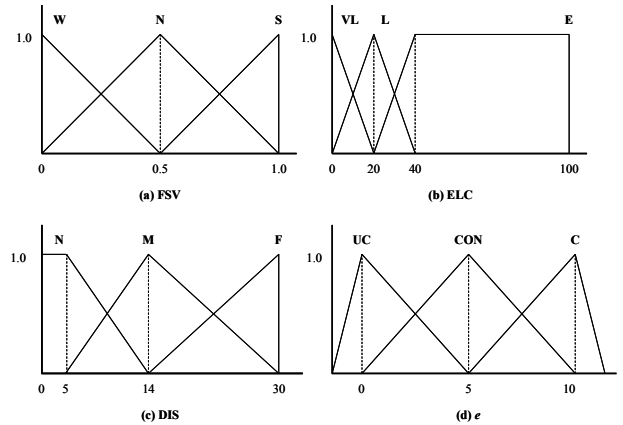


Figure 3. Fuzzy membership functions for determining e

Fig. 4(a), (b), and (c) show the membership functions to determine the FSV. The membership function of the output parameter, FSSV, is illustrated in Fig. 5(c). The labels are presented as follows.

- ELN = {VL (Very Low), L (Low), E (Enough), Very Enough (VE)}
- RFT = {VS (Very Small), S (Small), M (Medium), L (Large), VL (Very Large)}
- FSV = {W (Weak), N (Normal), S (Strong)}

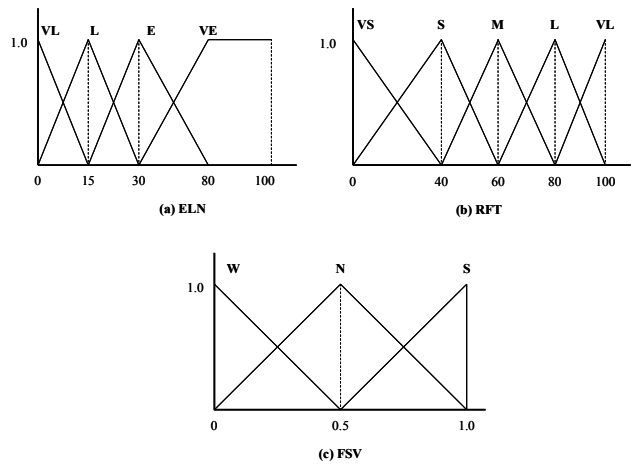


Figure 4. Fuzzy membership functions for determining FSV

We define fuzzy rules to use the fuzzy membership functions of defined parameters. Some of the rules are show in table 1 and 2.

Table 1. Fuzzy if-then rules of FSSV

Rule No.	IF		THEN
	ELN	RFT	FSV
1	VL	VS	W
2	L	M	N
3	E	S	S
4	E	L	N
5	VE	VL	W

Table 1 shows some rules of the fuzzy system to determine FSV.

Table 2. Fuzzy if-then rules of FSER

Rule No.	IF			THEN
	FSV	ELC	DIS	e
3	W	VL	F	UC
8	W	E	M	C
9	W	E	F	C
10	N	VL	N	UC
17	N	E	M	CON
18	N	E	F	C
20	S	VL	M	UC
23	S	L	M	CON
27	S	E	F	C

Table 2 shows some rules of the fuzzy system to determine e .

The execution of redistributing the authentication keys is determined at a states period, p , which is fixed by user before node deployment using fuzzy system. If the period is 10, CH determines the execution phase using fuzzy system after forwarding the tenth reports. CH receives the state data of network that includes the ratio of false traffic and the energy level of network, and then executes the fuzzy system to determine the execution phase. If e is consider, CH executes the fuzzy system next new period which is half of initial period fixed by the user.

IV. SIMULATION RESULTS

To show the effectiveness of FSER, we have compared FSER with DEF through simulation. We use a virtual sensor network of $500 \times 500m^2$, where 1000 CH are randomly distributed and 9000 sensor nodes are uniformly distributed. Each sensor nodes randomly picks five y-keys from the y-key pool whose size is 100. It also randomly picks one z-key from the z-key pool. Each CH in the cluster regions forwards the diffusion message of the authentication keys to forwarding nodes via ten hops. Each CH uses Hill Climbing [11] to select the forwarding node to conserve forwarding energy. Different five MACs from event-sensing nodes in the same cluster are needed to make an event report. Each node consumes $16.25 \mu J$ to transmit and $12.5 \mu J$ to receive a byte. The size of an original report is 24bytes and each MAC size is 1byte. The fixed period to execute the fuzzy system sets up to five.

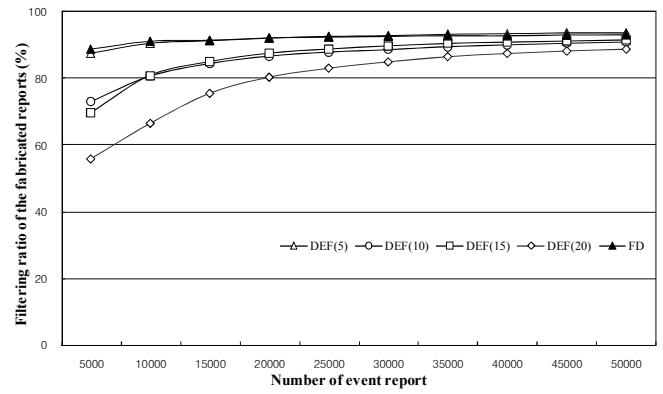


Figure 5. Filtering Efficiency

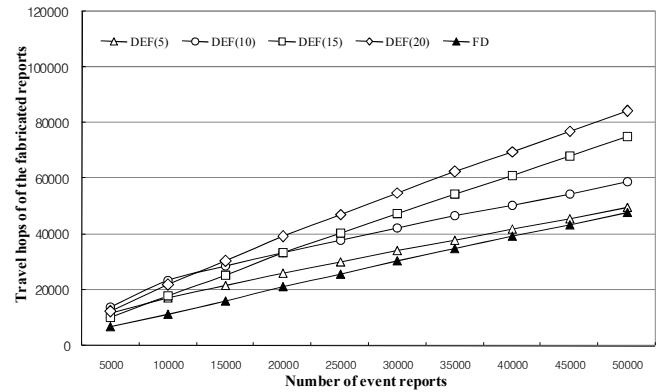


Figure 6. Travels of Fabricated reports

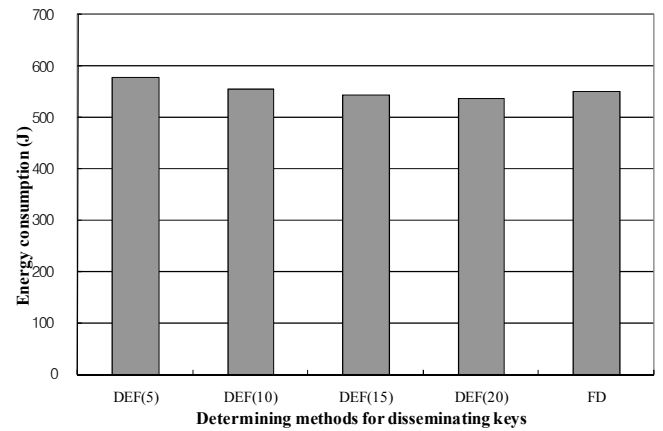


Figure 7. Energy Consumption

Figure 5 shows the ratio of filtered reports according to the fixed period, when p is 5, 10, 15, and 20. As shown in the figure, FD (Fuzzy with DEF) and DEF with $p = 5$ can detect most fabricated reports. On the other hand, as p increases, DEF cannot provide sufficient resilience against false data injection attack. That is, the execution of key redistribution is executed loosely, which cannot provide powerful detection power.

Figure 6 shows the hops that fabricated reports travelled before it is detected when p is 5, 10, 15, and 20. As shown in the figure, the proposed method can detect fabricated reports earlier than the DEF with $p = 5, 10, 15$ and 20 approach.

Figure 7 shows the average energy consumption, caused by a false report, when p is 5, 10, 15, and 20. As shown in the figure, FD is less efficient than the DEF with $p = 5$ and 10. However, the difference between them is very small. DEF consumes less energy as p decreases because of it does not execute the redistribution of keys frequently. That is, FD can provide the energy efficiency and the detection power sufficiently.

V. CONCLUSION AND FUTURE WORK

In this paper, we proposed the determination method for the key redistribution using two fuzzy rule based system with the consideration of network situation. Three parameters – the ration of the false traffic, the energy level of cluster head, and the distance from a cluster head to the base station – are used to determine e . The simulation results show that the proposed method can provide more sufficient detection power, while it dose not consume much energy.

In our future research, we will run additional simulations with other input factors which are not considered in the present work. We will apply our method to other filtering schemes requiring key redistribution phase.

ACKNOWLEDGEMENT

This work was supported by National Research Foundation of Korea Grant funded by the Korean Government (No. 2009-0076504).

REFERENCES

- [1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks", *IEEE Commun. Mag.*, vol.40, no.8, pp.102-114, Aug. 2002.
- [2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", *Ad Hoc Netw.*, vol. 1, no2-3, pp293-315. Sep. 2003.
- [3] H. Yang and S. Lu, "Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks", *Proc. of VTC*, pp.1223-1227, Oct. 2003.
- [4] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks", In *Proc. Of SenSys*, 2005.
- [5] 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.
- [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, Apr. 2005.
- [7] 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", *Proc. of S&P*, pp.259-271, May 2004.
- [8] F. Li and J. Wu, "A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks", *Proc. of IWCMC*, pp.27-32, Jul. 2006.
- [9] B.H. Kim, H.Y. Lee and T.H. Cho, "Fuzzy Key Dissemination Limiting Method for the Dynamic Filtering-Based Sensor Networks", *Lect. Notes Comput. Sc.*, vol.4681, pp.261-272, Aug. 2007.
- [10] 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.
- [11] D.B. Skalak, "Prototype and Feature Selection by Sampling and Random Mutation Hill Climbing Algorithms", In *Proc. of Eleventh International Machine Learning*, pp. 293-301, 1994.