International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:2, No:2, 2008

Fuzzy based Security Threshold Determining for the Statistical En-Route Filtering in Sensor Networks

Hae Young Lee, and Tae Ho Cho

***Abstract*—**In many sensor network applications, sensor nodes are deployed in open environments, and hence are vulnerable to physical attacks, potentially compromising the node's cryptographic keys. False sensing report can be injected through compromised nodes, which can lead to not only false alarms but also the depletion of limited energy resource in battery powered networks. Ye *et al*. proposed a statistical en-route filtering scheme (SEF) to detect such false reports during the forwarding process. In this scheme, the choice of a security threshold value is important since it trades off detection power and overhead. In this paper, we propose a fuzzy logic for determining a security threshold value in the SEF based sensor networks. The fuzzy logic determines a security threshold by considering the number of partitions in a global key pool, the number of compromised partitions, and the energy level of nodes. The fuzzy based threshold value can conserve energy, while it provides sufficient detection power.

***Keywords*—**Fuzzy logic, security, sensor network.

I. Introduction

RECENT advances in MEMS (micro-electro-mechanical systems) and low power highly integrated digital electronics have enabled the development of low-cost sensor net-works [1], [2]. Wireless sensor networks consist of small nodes with sensing, computation, and wireless communications capabilities. Sensor nodes are usually scattered in a sensor field, which is an area where the sensor nodes are deployed [3]. These sensor nodes have the ability to communicate either among each other or directly to the base station [4]. As a result, sensor networks have emerged as an important new tool for tracking contamination in hazardous environments, habitat monitoring in the nature preserves, enemy tracking in battlefield environments, etc [5].

In many applications sensor nodes are deployed in open environments, and hence are vulnerable to physical attacks, potentially compromising the node's cryptographic keys [6]. False sensing reports can be injected through compromised nodes, which can lead to not only false alarms but also the depletion of limited energy resource in battery powered networks (Fig. 1) [7].

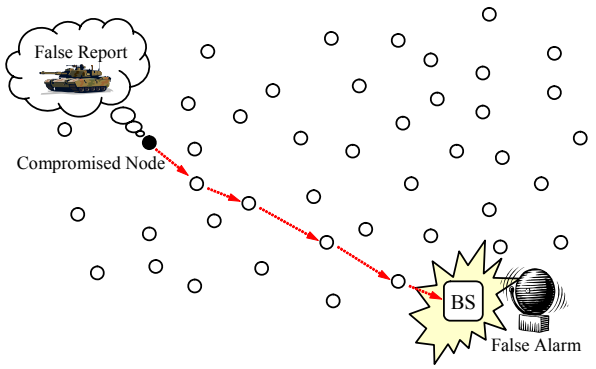

Fig. 1 False data injection

To minimize the grave damage, false reports should be dropped en-route as early as possible, and the few eluded ones should be further rejected at the base station [8]. Several security solutions have recently been proposed for this purpose. Zhu *et al* [9] proposed the interleaved hop-by-hop authentication scheme that detects false reports through interleaved authentication. Zhang *et al*. [10] proposed the interleaved authentication scheme for the braided multipath routing [11]. Ye *et al*. [7] proposed a statistical en-route filtering scheme (SEF) in which a report is forwarded only if it contains the message authentication codes (MACs) generated by multiple nodes, by using keys from different partitions in a global key pool. In these schemes, the choice of a security threshold value is important since it trades off between detection power and overhead [7], [9]. A large threshold value makes forging reports more difficult, but it consumes more energy in forwarding [7]. A small threshold value may make these schemes inefficient or even useless if the adversary has compromised a large number of nodes [12]. Therefore, we should choose a threshold value such that it provides sufficient detection power, while still small enough to conserve energy [7].

In this paper, we propose a fuzzy logic for determining a security threshold value in the SEF based sensor networks. The

Manuscript received June 30, 2006. The first author was supported by the second phase of BK21 (Brain Korea 21).

Hae Young Lee is with the School of Information and Communication Engineering, Sungkyunkwan University, Suwon, Gyeonggi-do 440-746 Korea (e-mail: sofware@ece.skku.ac.kr).

Tae Ho Cho is with the School of Information and Communication Engineering, Sungkyunkwan University, Suwon, Gyeonggi-do 440-746, Korea (corresponding author to provide phone: +82-31-290-7221; fax: +82-31-290-7230; e-mail: taecho@ece.skku.ac.kr).

fuzzy logic determines the security threshold value by considering the number of partitions in a global key pool, the number of compromised partitions, and the energy level of nodes. The fuzzy based threshold value can conserve energy, while it provides sufficient detection power. The effectiveness of the proposed fuzzy logic is shown with the simulation result at the end of the paper.

The remainder of the paper is organized as follows: Section II gives a brief description of SEF and motivation of this work. Section III describes the fuzzy logic for determining security threshold value in detail. Section IV reviews the simulation result. Finally, conclusion is discussed in Section 5.

II. Background and Motivation

A. The Statistical En-Route Filtering (SEF) Overview

In SEF [7], the base station maintains a global key pool that 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. Fig. 2 shows an example of global key pool. SEF assumes that the same event can be detected by multiple nodes. One of the detecting nodes is elected as the center-of-stimulus (CoS) node. The CoS collects MACs from the other nodes and produces a sensing report with T MACs generated by the detecting nodes, by using keys from different partitions in the global key pool, where T is a security threshold value. Fig. 3 shows an example of the report generation (a) and en-route filtering (b) in SEF when $T = 3$.

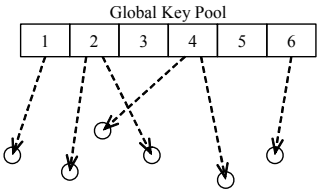

Fig. 2 Global key pool

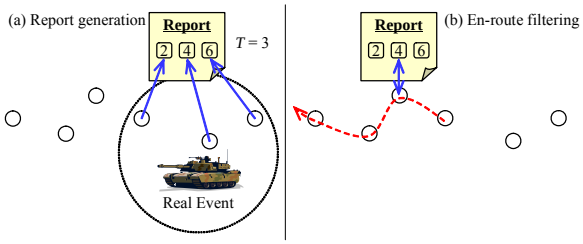

Fig. 3 Report generation and en-route filtering

An adversary can inject a forged report with incorrect MACs through a compromised node as shown in Fig. 4(a). However, the forged report may be dropped since each forwarding node verifies the correctness of the MACs carried in the report with certain probability (Fig. 4(b)). The probability of detecting incorrect MACs increases with the number of hops the report travels. SEF can detect false reports forged by an adversary with compromised keys in up to $T - 1$ partitions.

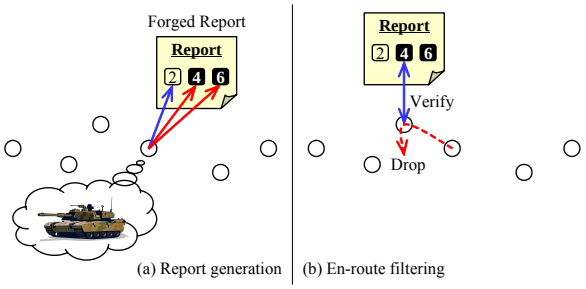

Fig. 4 Forged report filtering

B. Motivation

The choice of T is important since it trades off between detection power and overhead [7], [9]. A large T makes forging reports more difficult, but it consumes more energy in forwarding [7]. A small T may make SEF inefficient or even useless if all the partitions in a global key pool are compromised [9]. Therefore, we should adaptively choose T such that it achieves sufficient detection power, while still small enough to conserve energy [7].

III. Fuzzy Based Threshold Determining

A. Assumptions

We assume that the density of sensor field is dense enough, so that, for an event, CoS can collect p MACs generated by the detecting nodes, by using keys from different partitions in a global key pool, where p is the number of partitions in the global key pool. We also assume that the base station can know or estimate the number of compromised partitions and the energy level of nodes. We further assumes that the base station has a mechanism to authenticate broadcast messages (e.g., based on μTESLA [13]), and every node can verify the broadcast messages.

B. Factors that Determine the Security Threshold Value

In SEF, T should be equal to or smaller than the number of partitions in a global key pool because a report with less than T MACs will not be forwarded. For example, if a global key pool is divided into four partitions, T can be 0 (disable filtering), 1, 2, 3, or 4. Thus, we have to determine T based on the number of partitions in a global key pool.

SEF can detect false reports forged by an adversary with compromised keys in up to $T - 1$ partitions. Thus, if a certain number c partitions are compromised, we should set T larger than c. If all the partitions in the global key pool are compromised, SEF may be inefficient or even useless [12]. Under this situation, we may as well disable the en-route filtering, i.e., set T zero. So, we have to determine T based on the number of compromised partitions.

The energy is the most important resource that should be considered in sensor networks [3]. Generally, sensor nodes are limited in power and irreplaceable since these nodes have limited capacity and are unattended. The choice of T trades off

between detection power and overhead. Therefore, we also have to determine T based on the energy level of nodes.

C. Fuzzy Logic for Determining the Threshold Value

Fig. 5 illustrates the membership functions of three input parameters – the number of PARTITIONS in a global key pool (a), the number of COMPROMISED partitions (b), and the ENERGY level of nodes (c) – and the output parameter (the security THRESHOLD value (d)) of the fuzzy logic.

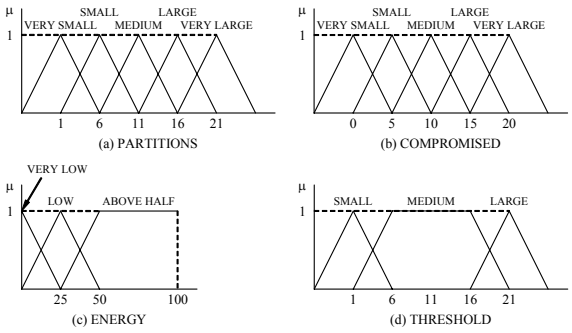

Fig. 5 Membership function of fuzzy logic

If it is reported or estimated that no node has been compromised, the fuzzy logic minimizes T (e.g., 0). If a few partitions are compromised and nodes have enough energy resource, the fuzzy logic sets T greater than the number of compromised partitions. If all the partitions are compromised, the fuzzy logic disables the en-route filtering, i.e., set T zero. If non-compromised nodes have not enough energy, although the number of compromised partitions is smaller than the number of partitions, T can be either greater than the number of compromised or 0 (if the overhead for the en-route filtering consumes too much energy). Some of the rules are shown below.

```
R1: IF PARTITIONS IS VERY LARGE
    AND COMPROMISED IS VERY LARGE
    AND ENERGY IS ABOVE HALF
    THEN THRESHOLD IS LARGE
R2: IF PARTITIONS IS VERY LARGE
    AND COMPROMISED IS VERY LARGE
    AND ENERGY IS LOW
    THEN THRESHOLD IS LARGE
R3: IF PARTITIONS IS VERY LARGE
    AND COMPROMISED IS VERY LARGE
    AND ENERGY IS VERY LOW
    THEN THRESHOLD IS SMALL
R4: IF PARTITIONS IS VERY LARGE
    AND COMPROMISED IS LARGE
    AND ENERGY IS ABOVE HALF
    THEN THRESHOLD IS LARGE
R5: IF PARTITIONS IS VERY LARGE
    AND COMPROMISED IS LARGE
    AND ENERGY IS LOW
    THEN THRESHOLD IS LARGE
R6: IF PARTITIONS IS VERY LARGE
    AND COMPROMISED IS LARGE
    AND ENERGY IS VERY LOW
    THEN THRESHOLD IS SMALL
```

D. Applying the New Security Threshold Value

The base station periodically determines T with the fuzzy logic. If the new T_n differs from the current T_c, the base station broadcasts T_n to all the nodes in the network as shown in Fig. 6. Broadcasting T_n can be achieved using by authenticated broadcast protocols such as μTESLA [13]. After applying T_n, each authenticated report should contain T_n MACs generated by using keys from different partitions.

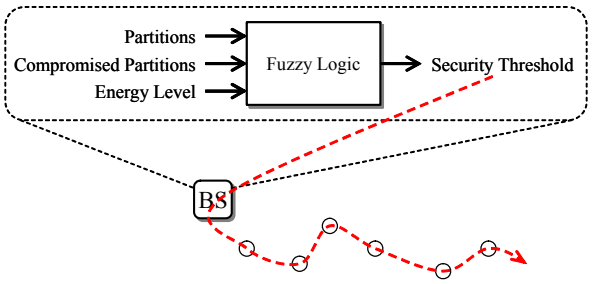

Fig. 6 Applying the new security threshold value

IV. Simulation Result

To show the effectiveness of the proposed fuzzy logic, we have compared the fuzzy based threshold value with the fixed threshold values through the simulation. Each node takes 16.25, 12.5 μJ to transmit/receive a byte and each MAC generation consumes 15 μJ [7]. The size of an original report is 24 bytes. The size of a MAC is 1 byte.

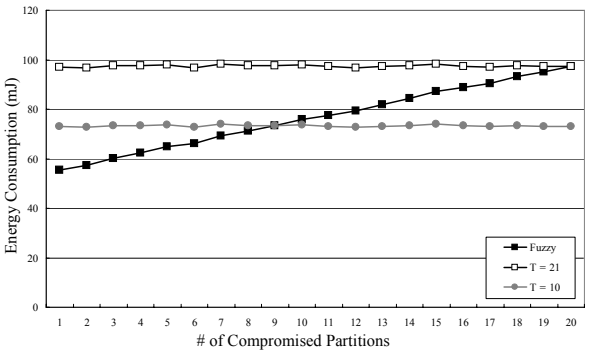

Fig. 7 Average energy consumption per authenticated report (p = 21)

Fig. 7 shows the average energy consumption caused by an authenticated report when the number of partitions p is 21 and the number of compromised partitions is between 1 and 20. As shown in the figure, the fuzzy based threshold value (filled rectangles) consumes no more energy than the fixed threshold values (T = 10 and 21) up to nine compromised partitions since the fuzzy logic determines T adaptively according to the number of compromised partitions. SEF with T = 10 (filled

circle) consumes less energy than the fuzzy based threshold if the number of compromised partitions exceeds 10. However, it cannot detect false reports because the number of compromised partitions exceeds *T*. On the other hand, the fuzzy based threshold value provides sufficient detection power, while still small enough to conserve energy.

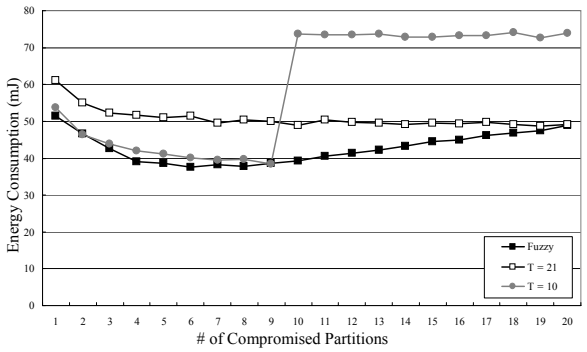

Fig. 8 Average energy consumption per report (p = 21)

Fig. 8 shows the average energy consumption caused by a report (authenticated or forged) when p = 21. As shown in the figure, the fuzzy based threshold value (filled rectangles) consumes no more energy than the fixed threshold values.

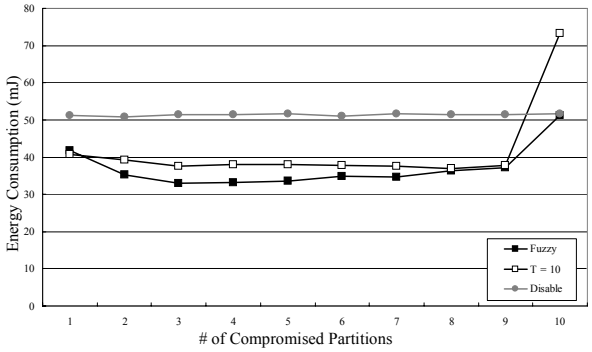

Fig. 9 Average energy consumption per report (p = 10)

Fig. 9 shows the average energy consumption caused by a report when p = 10. As shown in the figure, the fuzzy logic can save energy even if all the partitions are compromised (the number of compromised partitions = 10).

V. Conclusion

In this paper, we proposed a fuzzy logic for determining a security threshold value in the SEF based sensor networks. The fuzzy logic determines the threshold value by considering the number of partitions in a global key pool, the number of compromised partitions, and the energy level of nodes. The fuzzy based threshold value can conserve energy, while it provides sufficient detection power. The effectiveness of the proposed fuzzy logic was shown with the simulation result.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," *IEEE Commun. Mag.*, vol. 40, no. 8, Aug. 2002, pp. 102-114.

[2] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks," *Ad hoc Networks*, vol. 3, no. 3, May 2005, pp. 325-349.

[3] S. Chi and T. Cho, "Fuzzy Logic based Propagation Limiting Method for Message Routing in Wireless Sensor Networks," *Lect. Notes Comput. Sc.*, vol. 3983, May 2006, pp. 58-67.

[4] J. Al-Karaki and A. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wirel. Commun.*, vol. 11, no. 6, Dec. 2004, pp. 6-28.

[5] Q. Jiang and D. Manivannan, "Routing Protocols for Sensor Networks," in *Proc. of CCNC*, pp. 63-98, Jan. 2004.

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

[7] 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.

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

[9] 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. of S&P*, pp. 259-271, May 2004.

[10] Y. Zhang, J. Yang, and H. Vu, "The Interleaved Authentication for Filtering False Reports in Multipath Routing based Sensor Networks," in *Proc. of IPDPS*, pp. 1-10, Apr. 2006..

[11] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, Energy-efficient Multipath Routing in Wireless Sensor Networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 4, pp. 11-25, Oct. 2001.

[12] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach," in *Proc. of INFOCOM*, pp. 503-514, Mar. 2005.

[13] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "SPINS: Security Protocols for Sensor Networks," *Wirel. Netw.*, vol. 8, no. 5, pp. 521-534, Sep. 2002.