Wireless Sensor Network, **2011, 3, 357-361**
doi:10.4236/wsn.2011.311041 Published Online November 2011 (http://www.SciRP.org/journal/wsn)

Secure Path Cycle Selection Method Using Fuzzy Logic System for Improving Energy Efficiency in Statistical En-Route Filtering Based WSNs*

Su Man Nam, Chung Il Sun, Tae Ho Cho
School of Information and Communication Engineering, Sungkyunkwan University, Suwon,
Republic of Korea
E-mail: *smnam@ece.skku.ac.kr*, *cisun@ece.skku.ac.kr*, *taecho@ece.skku.ac.kr*
Received September 23, 2011; *revised October* 21, 2011; *accepted October* 31, 2011

Abstract

Sensor nodes are easily compromised to malicious attackers due to an open environment. A false injected attack which takes place on application layer is elected by the compromised node. If the false report arrives in a base station, a false alarm is occurred, and the energy of the nodes is consumed. To detect the false report, statistical en-route filtering method is proposed. In this paper, we proposed the secure path cycle selection method using fuzzy rule-based system to consume effective energy. The method makes balanced energy consumption of each node. Moreover, the lifetime of the whole network will be increased. The base station determines the path cycle using the fuzzy rule-based system. The performance of the proposed method is demonstrated using simulation studies with the three methods.

Keywords: Wireless Sensor Network, Secure Path Cycle Selection, Statistical En-route Filtering, Path Selection Method, Fuzzy System

1. Introduction

Wireless Sensor Networks (WSNs) have rapidly become widely used based on development of wireless communication with low-cost, low-power, multifunction sensors which enable a wide variety of new applications [1,2]. A WSN is composed of a sensor field which includes a large number of sensor nodes and a base station. A sensor node is made up of sensing, computing, and wireless communication modules. If an event occurs in a sensor field, the sensor nodes sense the event, and create a report. A base station provides information to users through the Internet or a communications infrastructure. Because the sensor network can communicate without the infrastructure, it is well suited for random distribution in an open environment [3]. WSNs are vulnerable to malicious attackers using various attack patters. The sensor nodes are therefore at high risk of being captured and compromised [4,5].

False report injection attacks [6] occurring in the application layer are initiated by a compromised node, such as node A, in **Figure 1**. For example, if a malicious attacker injects false reports through node A into a network, a base station may transmit the false report via nodes B, C and D. The base station which owns the false report issues a false alarm to notify users. Moreover, nodes B, C and D, which are located on the same path as node A, expend unnecessary energy. Because of these injected false reports, the lifetime of the whole network is lost.

Ye *et al.* [6] proposed the statistical en-route filtering scheme (SEF) to filter out false reports during the forwarding process. The scheme is intended to drop false reports as soon as possible before they reach a base station. The path selection method (PSM) [7] was proposed to improve the detection power of the SEF using a control message. In PSM, each node determines a secure path using the partition ID information for its own node in the control message. To increase network lifetime and to distribute communication traffic more effectively, the path renewal method (PR-M) [8] was proposed. The method checks the remaining energy in the network and ensures balanced energy consumption in each node.

In this paper, a fuzzy logic-based secure path cycle

*This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No. 2011-0004955).

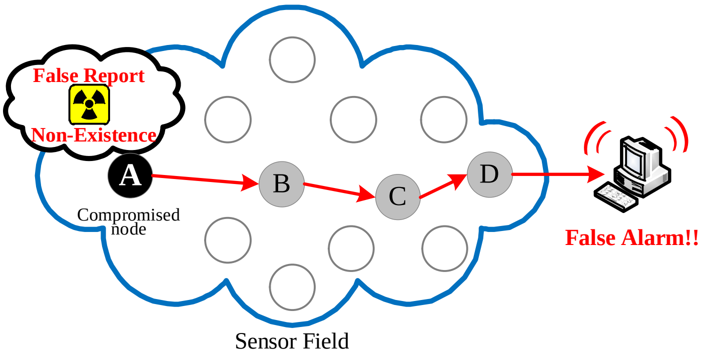


Figure 1. False report injection attack.

selection method is proposed to ensure balanced energy consumption in the PRM. The paper is organized as follows: Section 2 outlines the related research and the motivation of this work. Section 3 presents the proposed method using a fuzzy-rule based system [13], and Section 4 presents simulation results. Finally, conclusions and directions for future research are covered in Section 5.

2. Related Work and Motivation

This section reviews the three existing methods (SEF, PSM and PRM) and then explains the motivation for this research.

2.1. Statistical En-Route Filtering (SEF)

SEF [6] statistically identifies false report injection attacks using keys before filtering them out. In SEF, a base station manages a global key, including keys for divided multiple partitions, and every node, before it is deployed receives a small number of keys, from a randomly selected partition in the global key pool. **Figure 2** represents an example of the global key pool.

When real events occur, a center-of-stimulus (CoS) node, which is one of the detecting nodes, decides to generate a report.Surrounding nodes, upon sensing the same event, create message authentication codes (MACs) and send them to the CoS node, which generates a sensing report using the collected MACs. The report is transmitted toward the base station via multiple hops; the base station can prove that the report is legitimate using its keys [6]. When the base station receives the report, the keys of all the MACs in the report are verified against the keys in the global key pool. **Figure 2** shows examples of the report generation and en-route filtering in the SEF scheme.

2.2. Path Selection Method (PSM)

In SEF, the power to detect false reports is influenced by the choice of routing paths. In the worst case, if the partition IDs in the report differs from the partition IDs in forwarding nodes, the report cannot be verified as real or false while passing nodes toward the base station. In PSM [7], a control message establishes routing paths in the initial phase to improve detection power for false reports. Each node receiving a control message can choose its desired the security level and the transmission distance using an evaluation function. The control message consists of the partition IDs of the visited nodes and the hop count.

2.3. Path Renewal Method (PRM)

In PRM [8], the balanced energy consumption is maintained in each node to increase network lifetimebecause nodes have secure paths, which are set by PSM, has many communications. Each super-node checks its remaining energy after establishing the routing paths. If its remaining energy is less than defined threshold value, one of the super-node’s child nodes takes over communication traffic to and from the child nodes. Then, a child node which has lowest communication traffic among the super-node’s child nodes selects a new super-node. Through path renews, PRM makes it possible to distribute the communication traffic evenly and to increase the lifetime of the network.

2.4. Motivation

PRM maintains the detection ability of SEF, and consumes a balanced amount of energy from every node. To determine effectiveness of path renewal, it is important to consider information about the whole network state because this network state changes dynamically.

In this research, the secure path cycle selection method is determined using the hop count, the number of normal reports, and the number of false reports to select the secure path using a fuzzy rule-based system [9-13]. The next section presents a detailed description of the fuzzy rule-based system.

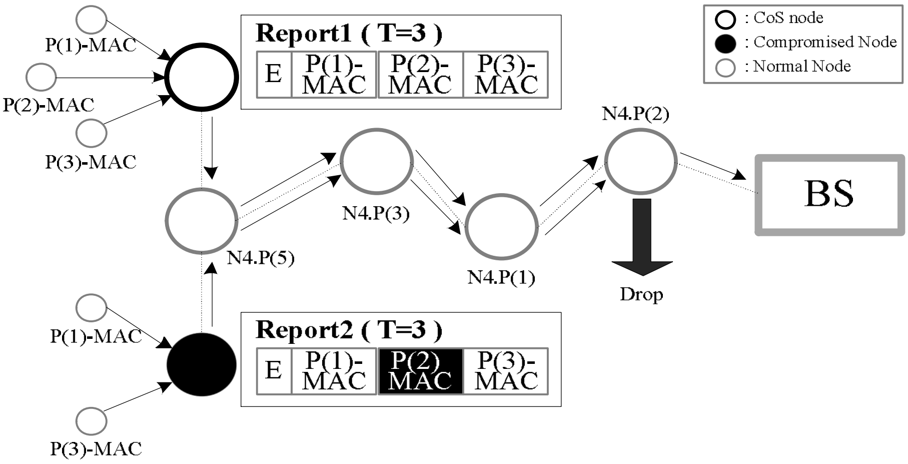


Figure 2. Generating a report and filtering a false report.

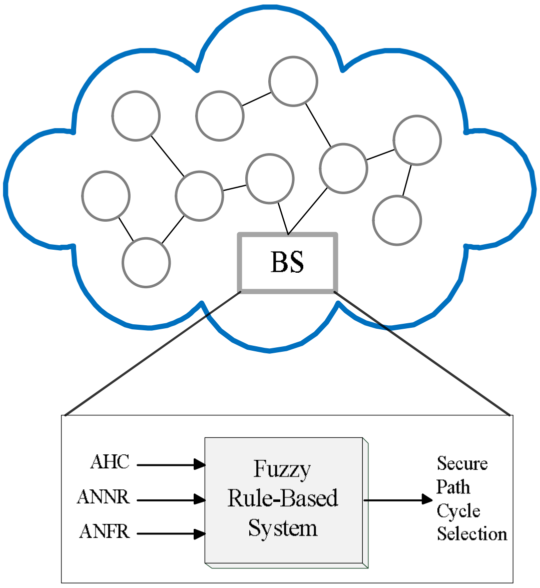


Figure 3. Overview of the fuzzy secure path cycle selection method.

3. Fuzzy-Based Secure Path Cycle SelectionMethod

3.1. Assumptions

A sensor network is assumed to be composed of a large number of small sensor nodes and a base station. It is assumed that the routing paths are established by the PSM in the initial phase, and the network uses a single-path routing protocol. To preform the secure path cycle selection effectively, the base station knows certain information about each node, including hop count, the number of normal reports, and the number of false reports.

3.2. Overview

The proposed method is based on SEF to improve energy efficiency after the nodes have been deployed. It is important to maintain the energy conservation in many secure protocols. In the proposed method, the base station determines the secure path cycle selection for the whole network using the average hop count, the average number of normal reports transmitted, and the average number of false reports. Fuzzy logic is then used to represent the fitness of each secure path cycle selection based on its different values of these three variables.

3.3. Input Factors

This section discusses the factors that are used for fuzzy inference.

- AHC (Average Hop Count): When a report is transmitted by a CoS node, the report travels via multiple hops toward a base station. If a WSN has high hop counts much energy will be consumed in each node. Therefore, the lifetime of the sensor network is influenced by high hop counts in each node.
- ANNR (Average Number of Normal Reports): This value indicates how many normal reports, on average, arrive at the base station from CoS nodes. If each node transmits many reports, the lifetime of the sensor network will rapidly decrease. Therefore, a number of normal reports is assumed over the network lifetime.
- ANFR (Average Number of False Reports): This value represents the condition of network security. If the base station receives many false reports from compromised nodes, the sensor network needs to change its secure paths to improve its detection power for false reports. Accordingly, this value is an indicator of network security.

3.4. Fuzzy Membership Functions and Rules

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

- AHC = {S (Small), M (Medium), L (Large)}
- ANNR = {L (Low), M (Medium), L (Large)}
- ANFR = {F (Few), M (Many)}

The fuzzy logic output parameters are represented by a label, S or C. The label values represent a cycle selection (CS) as follows:

CS = {S (Stay), C (Change)}

The rule base of the fuzzy system consists of 18(=3 × 3 × 2) rules. Some of these rules are shown in **Table 1**. If AHC is High, ANNR is Medium, and AQFR is Many, then it is recommended to change the secure path cycle to conserve energy and to maintain detection power (Rule 11). This case indicates that there are problems in the network, and that therefore the secure path cycle must quickly be altered. If AHC is Low, ANNR is Large, and AQFR is Low, then the cycle selection does not change because the network is normal (Rule 12). The network will wait in this condition until required to move from 0 (Stay) to 1 (Change). Therefore, it is important to select the secure path cycle appropriately.

Table 1. Fuzzy if-then rules.

Rule No.	Input			Output
	AHC	ANNR	ANFR	CS
04	Medium	Small	Low	Stay
11	High	Medium	Many	Change
12	Low	Large	Low	Stay
16	Medium	Large	Low	Change

4. Simulation Results

To show the effectiveness of the proposed method, it is compared with the SEF, PSM, and PRM approaches through simulation studies. The simulation environment consists of a sensor network with 200 nodes in the simulation environment. Each node consumes 16.56 μJ to transmit a report, 12.5 μJ to receive a report, and 15 μJ to generate a MAC [6]. There is a global key pool of 100 keys, the number of partitions is 10 and each node owns four keys.

Figure5 shows the energy consumption for each method for 300 iterations of the network. This figure indicates that SEF consumed higher than the other methods because reports on SEF pass via many hops. PRM is better than PSM because routing paths is changed through energy check of each node. The energy consumption of the proposed method is low because changes in the secure path using the fuzzy logic system improved the condition of the network. It is expected that with a larger number of iterations, the gap between the

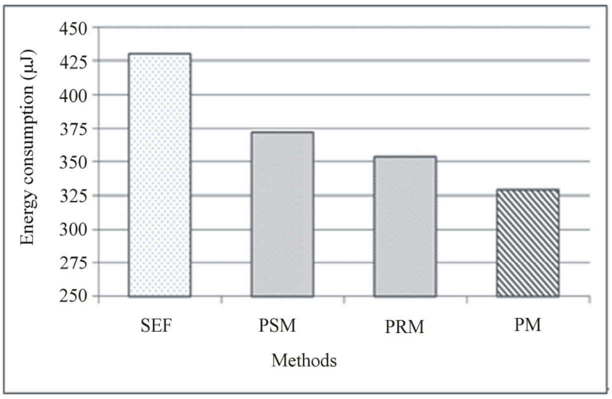
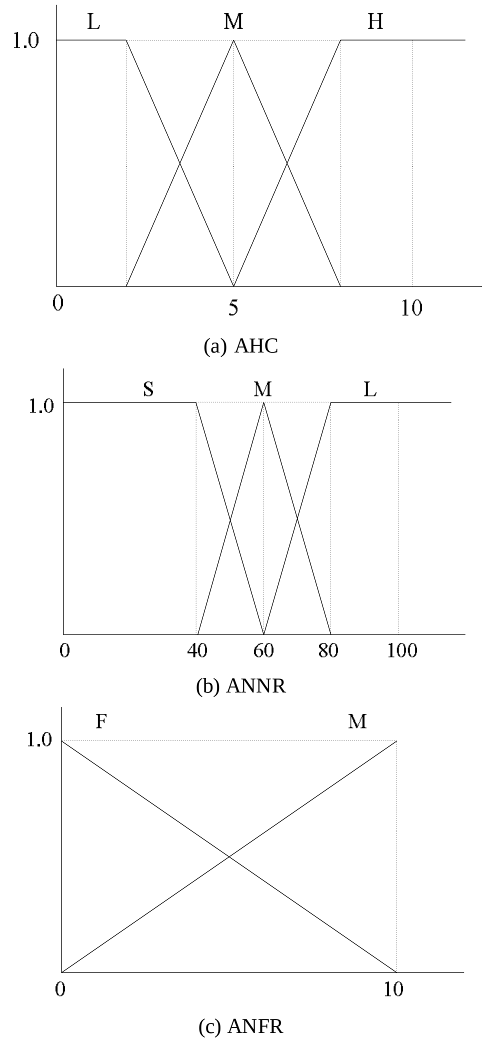


Figure 4. Energy consumption for each method.



(a) AHC

(b) ANNR

(c) ANFR

Figure 5. Fuzzy Input Membership Functions.

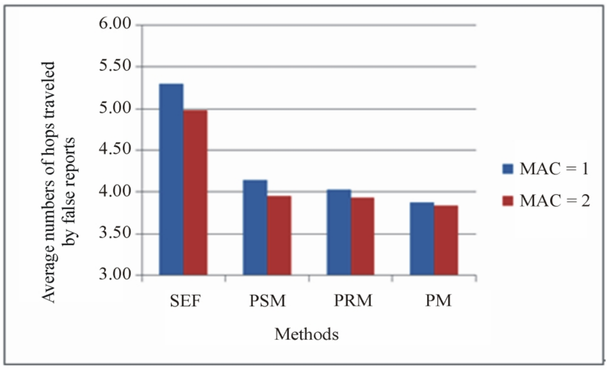


Figure 6. Average numbers of hops traveled by false reports for each method

proposed network and the other networks would increase. Therefore, it can be said that the proposed method consumes less energy than SEF, PSM, or PRM.

Figure 6 shows the average simulated performance for each method in filtering out false reports. Because PSM, PRM, and PM apply secure paths, SEF requires a higher number of nodes for transmission than the other three methods. The method proposed here offers almost the same detection power as the PSM and PRM. The proposed method can therefore maintain a security level similar to that of PSM or PRM.

5. Conclusions and Future Work

This paper has proposed a fuzzy-based secure path cycle selection method to conserve energy and maintain detection power in networks. It has been demonstrated that the proposed method improves the balance in energy consumption among nodes to increase network lifetime, considering the average hop count, the average number of normal reports transmitted, and the average number of false reports. The simulation results show that the proposed method is able to provide higher energy efficiency and appropriate security level in the network. In the future, the authors propose to apply optimization to the fuzzy logic system in the proposed method to increase the lifetime of the whole network.

6. References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine*, Vol. 40, No. 8, 2002, pp. 102-114. doi:10.1109/MCOM.2002.1024422

[2] K. Akkaya and M. Younis., "A Survey on Routing protocols for Wireless Sensor Networks," *Ad Hoc Network*, Vol.3, No.3, 2005, pp. 325-349. doi:10.1016/j.adhoc.2003.09.010

[3] J. N. Al-Karaki and A. E. Kanmal, "Routing techniques in wireless sensor networks: a survey," IEEE Wireless Communication Society, Vol. 11, No. 6, 2004, pp. 6-28. doi:10.1109/MWC.2004.1368893

[4] D. Culler, D. Estrin and M. Srivastava, "Guest Editors' Introduction: Overview of sensor networks," *IEEE Computer Society*, Vol.37, No. 8, 2004, pp. 41-49. doi:10.1109/MC.2004.93

[5] C. Karlof *et al.*, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications*, Vol. 1, No. 2-3, 2003, pp. 293-315. doi:10.1109/SNPA.2003.1203362

[6] F. Ye, H. Luo and S. Lu, "Statistical En-route Filtering of Injected False Data in Sensor Networks," *IEEE Journal Selected Area Communications*, Vol. 23, No. 4, 2005, pp. 839-850. doi:10.1109/JSAC.2005.843561

[7] C. I. Sun, H. Y. Lee and T. H. Cho, "A Path Selection Method for Improving the Detection Power of Statistical Filtering in Sensor Networks," *Journal of Information Science and Engineering*, Vol. 25, No. 4, 2009, pp. 1163-1175.

[8] J. M. Kim, Y. S. Han, H. Y. Lee and T. H. Cho, "Path Renewal Method in Filtering Based Wireless Sensor Networks," Vol. 11, No. 2, 2011, pp. 1396-1404. doi:10.3390/s110201396

[9] S. J. Lee, H. Y. Lee and T. H. Cho, "Environment-Based Selection Method for En-route Filtering Scheme Using Fuzzy Logic," *Journal of Networks*, Vol. 5, No 3, 2010, pp. 292-299. doi:10.4304/jnw.5.3.292-299

[10] S. H. Lee and T. H. Cho, "Fuzzy Based Key Re-Distribution Period Determination Method in Wireless Sensor Networks," *Lecture Notes in Computer Science*, Vol. 6216, 2010, pp. 495-502. doi:10.1007/978-3-642-14932-0_62

[11] H. Y. Lee and T. H. Cho, "Fuzzy-Based Adaptive Threshold Determining Method for the Interleaved Authentication in Sensor Networks," ICDCIT 2006, *Lecture Notes in Computer Science*, Vol. 4319, 2006, pp. 116-127. doi:10.1007/11925231_11

[12] Louder than a Bomb Software, "Free Fuzzy Logic Library," 2001, http://ffll.sourceforge.net

[13] L. A. Zadeh, "Fuzzy Logic," 2011, http://en.wikipedia.org/wiki/Fuzzy_logic