Appl. Math. Inf. Sci. 6 No. 1S pp. 285S-291S (2012)

Applied Mathematics & Information Sciences
An International Journal

Fuzzy Based Filtering Nodes Assigning Method for Sensor Networks

Soo Young Moon[1] and Hee Suk Seo[2]

[1]Sungkyunkwan University, 300 Cheoncheon-dong, Jangan-gu, Suwon 440-746, South Korea
Email Address: moonmous@ece.skku.ac.kr
[2]Korea University of Technology and Education, 307 Byungcheon, Cheonan, 330-708, South Korea
Email Address: histone@kut.ac.kr

In most sensor networks, sensor nodes are vulnerable to many security attacks because of open and harsh environment. In false report attacks, an attacker can capture some sensor nodes and inject false reports into the network through the compromised nodes. The false reports injected may confuse the user and more importantly deplete the limited energy of the network. Several filtering schemes are employed to detect and drop false reports at an early stage, for example, the commutative cipher-based en-route filtering scheme (CCEF). In the CCEF, each forwarding node performs verification of received event reports based on a probability without consideration of false traffic ratio. Hence, it is difficult to adapt to the change of false traffic ratio. That is, it is possible that the network performs too many or too few filtering operations, which results in energy inefficiency. In this paper, we propose a fuzzy-based filtering nodes assigning method for wireless sensor networks to cope with these problems. Our simulation results on the proposed method show the effectiveness of energy consumption against false report injection attacks.

Keywords: Wireless sensor networks, false report injection attacks, filtering scheme, fuzzy logic.

1 Introduction

Sensor networks comprise small, cheap sensor nodes with sensing, processing, transmission modules, and possibly mobilizers and position-finding systems [1, 2]. The application areas include military, habitat monitoring, forecasting, and health monitoring. In such applications, the sensor nodes are generally deployed in open, hostile environments, and hence they are vulnerable to many security attacks [3]. In false report injection attacks, the attacker captures some sensor nodes and injects false reports into the network through the compromised sensor nodes. The false report injection attacks give rise to false alarms or the depletion of energy resources in the networks.

Several filtering schemes [4-10] can be applied in sensor networks to detect and drop false reports at an early stage. Commutative cipher-based filtering (CCEF) [4] was proposed by Yang, et al. and detects and removes false reports based on a secure session between base station (BS) and a cluster header (CH) node in an interesting region. Unlike symmetric key sharing based en-route filtering schemes, in CCEF sensor nodes do not need to know a secret session key to verify and detect false reports. As an event report is forwarded to the BS, each forwarding node verifies the received report by using a commutative cipher based on a probability previously set as a system parameter. In CCEF, every false report is detected and dropped en-route unless the selected node and exact number of neighbor nodes in the interesting region are compromised.

In CCEF, sensor nodes verify event reports probabilistically without consideration of the current false traffic ratio. Because the verification probability at each node for a given session does not change, it is hard to adapt to the change of false traffic ratio and energy inefficiency occurs. For this reason, we propose a fuzzy-based filtering node assigning method for sensor networks. In the proposed method, each forwarding node has a fitness value that ranges from zero to one, and the BS determines the sensor nodes that perform filtering operations based on the fitness value of every sensor node and the threshold value. Hence, the network performs at least one and not too many filtering operations.

The remaining sections are organized as follows. Section 2 describes the CCEF scheme and its operation briefly. Section 3 explains our proposed method in detail.

Section 4 shows the simulation results of the performance of the proposed method and the CCEF in terms of energy. Finally, section 5 concludes the paper.

2 Commutative Cipher-based En-route Filtering scheme

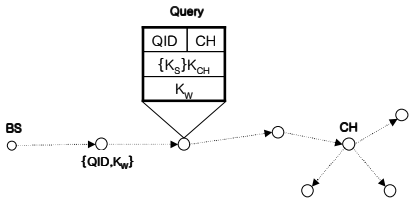
In CCEF, the report-generating nodes and forwarding nodes use a commutative cipher to endorse and authenticate reports. A commutative cipher has certain features that if we apply two encryption operations for a message using a commutative cipher CE, it leads to the same result regardless of the order of operations.

The following assumptions are associated with the CCEF scheme. The sensor nodes are stationary, equipped with limited memory and energy resources, and cover a small sensing range. Unique IDs and keys are provided to the sensor nodes and information regarding their locations can be obtained from the localization components in the network. The network operates in the query-response mode and is sufficiently dense to sense events and make reports [4].

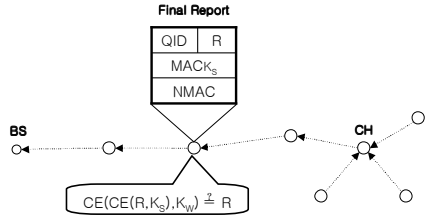
The overall operation of a network that employs the CCEF scheme is as follow. On the initialization phase of the network, the sensor nodes obtain their location information from the localization component in the network and report it to the BS. In each session the BS selects one node in the region of interest as the CH node and prepares two keys K_s and K_w for endorsing and authenticating a report. The BS sends a query message to the CH node through the intermediate nodes. The intermediate nodes verify received reports from the CH node based on a probability P, which is determined by the security parameter α and hop count h from the CH node to the BS, as shown in the following equation.

$$P = \frac{1}{\alpha h} \quad (1)$$

Fig. 2.1 shows overview of CCEF operation.



(a) Forwarding of query message



(b) Report generation & en-route filtering

Figure 2.1 Overview of CCEF

In eq. (1), the security parameter α is the main factor that determines the probability with which the intermediate nodes authenticate the received reports. The detection capability and overhead of a network are inversely related and depend on the security parameter of the network. If the value of α is small, the detection capability of the network increases along with the overhead of the network. Otherwise, if the value of α is large, the network overhead decreases along with the detection capability of the network. Hence, the parameter α is a very important factor that indicates the overall performance of the network. A static value of α may be inefficient in terms of energy consumption and detection capability [4].

3 Proposed method

3.1 Assumptions

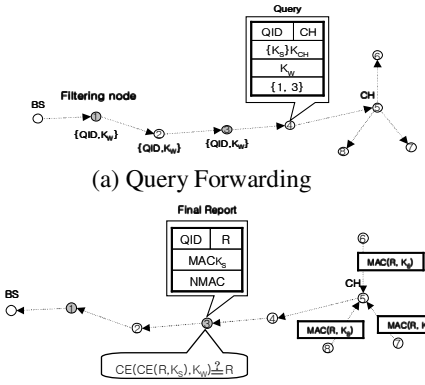
In addition to the assumptions of the CCEF scheme, we assume that the BS can estimate the energy resource level of each sensor node and the state of the network change dynamically. For example, the false traffic ratio of the network varies with time. When sending valid event reports to BS, sensor nodes can use 'piggybacking' to inform the BS of the statistical information about false reports detection.

3.2 Motivation

In the CCEF scheme, each intermediate node independently performs verification probabilistically. Hence, it is possible that the network performs either a considerably large number of filtering operations or no filtering operation. In the case of a legitimate report, the report does not need to be authenticated en-route, whereas a false report should be validated at least once. In order to filter out false reports in advance and prevent unnecessary filtering operations, a few filtering nodes should be assigned as the filtering nodes in each path. In a probability-based en-route filtering scheme, it is difficult to control the number of en-route filtering operations in the network. Hence, it is more suitable to assign filtering nodes based on fuzzy logic [11] than based on probabilistic method for limiting the number of en-route filtering operations to consume energy resource efficiently and lengthen the network life.

3.3 Overview

The proposed method differs with the CCEF in only two phases, the session setup and the en-route filtering phase. In the session setup phase, BS randomly selects one node as the CH node in interesting region and computes a fitness value as a filtering node for every node in the path between CH and BS by using fuzzy logic. BS can access all the parameters required to derive the fitness value of every node in the path, such as (1) the energy resource level of a node, (2) number of node MACs for a final report, and (3) false traffic ratio in the network. Then, BS assigns a maximum of two nodes as the filtering nodes depending on the threshold value. If the fitness value of a node is larger than the threshold value, it can be a filtering node. Subsequently, BS generates and sends a query message, which contains the (1) query ID (QID), (2) CH node ID, (3) session key K_s encrypted by the CH node key ($\{K_s\} K_{CH}$), (4) witness key K_w, and (5) sequence of filtering node IDs, to the CH. As the query is forwarded to the CH, each intermediate node stores the {QID, K_w} pair and checks if its node ID matches to any filtering node IDs in the query message. If the ID matches, the intermediate node prepares for future filtering operations for the session. Then, it sends the query message to the next forwarding node in the path. Fig. 3.1 shows an overview of the proposed method.



(a) Query Forwarding

(b) Report Creation & En-Route Filtering

Figure 3.1: Overview of the proposed method

After the CH node creates the final report and sends it to the BS through the intermediate nodes, each intermediate node checks for the {QID, K_w} pair that corresponds to the QID in the final report. If this pair does not exist, the node removes the received report. If the pair exists and the node is a filtering node, the node performs message authentication by using a commutative cipher and the witness key K_w. Then, the node forwards the received report only when the report is valid.

3.4 Factors

Three factors are involved in the derivation of the fitness value of a node as a filtering node: (1) the energy level of a node (NODE_ENERGY), (2) the number of MACs making a node MAC (NUM_MAC), and (3) the false traffic rate (FTR) in the network. If NODE_ENERGY is significantly low, the fitness value of the node should be small so that the node does not perform en-route filtering operations. However, if NODE_ENERGY is high, the fitness value of the node can be large so that the node filters out false reports. The parameter NUM_MAC denotes the number of neighbor nodes that collaborate with the CH node when making a report. If this parameter is large, a large amount of energy is consumed for communication among the neighbor nodes. Hence, the fitness value for the node should be small to reduce the energy consumption for verification operation and conserve the total energy of the network. If the parameter is small, the fitness value can be large. The FTR is the last and most important factor. If the FTR value is high, the fitness value of the node must be large so that the node filters out false reports. On the other hand, if this value is small, the fitness value of the node should be small in order to reduce unnecessary energy consumption.

3.5 Fuzzy logic design

The membership functions for the fuzzy inputs and output variables have been designed as follows. First, we normalized the ranges of the variables except NODE_ENERGY (of which range is 1 ~ 5) as 0 ~ 100. Since the FTR is the most important input factor to derive the fitness value, we have defined five fuzzy sets for it – Very Low (VL), Low (L), Medium (M), Large (L), and Very Large (VL) – with almost same widths. Each of the other variables is related to three fuzzy sets. For NODE_ENERGY, we have defined the values lower than 10% as VL and values about 20% as L. If it is larger than 30%, we consider it as Enough (E). The classification can change based on applications. NUM_MAC has its range of 1 ~ 5. We have simply chosen the minimum, median and maximum value of the range as the peaks of the three fuzzy sets – Small (S), M and L. Fitness Value has three fuzzy sets. Normal (N) has its peak value which is the median of the range. Unfit (U) and Fit (F) have their peak values when the value is lower than 30% or larger than 70%, respectively.

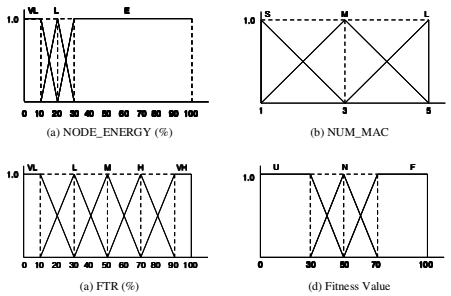


Figure 3.2: Fuzzy inputs and output variables

Table 1 shows examples of the if-then rules of the fuzzy logic.

Table 1. Fuzzy if-then rules

Rule #	NODE_ENERGY	NUM_MAC	FTR	Fitness Value
1	VL	S	VL	U
15	VL	L	VH	U
25	L	M	VH	F
36	E	M	VL	U
42	E	L	L	N
45	E	L	VH	F

For example, in rule #1, because NODE_ENERGY is VL and NUM_MAC is S, but FTR is VL, Fitness Value becomes U. In rule 45, because NODE_ENERGY is E and NUM_MAC is L, and most importantly FTR is VH, Fitness Value becomes F.

4. Simulation Results

In order to validate the efficiency of the proposed method, we simulated the method against the false report injection attacks and compared it to the CCEF scheme. In our simulation, the field size is 125 × 125 m^2 with 3750 sensor nodes. There are 625 clusters with a size of 5 × 5 m^2 and each cluster contains six sensor nodes. The energy consumed to transmit or receive a report of 40 Bytes is 1.15 mJ and that consumed to perform one commutative cipher operation (that is, one filtering operation) for a node is 9 mJ [5, 12]. We assumed that the CH node is not compromised in the simulation. Hence, every false report can be filtered out by the intermediate nodes if it is authenticated en-route at least once. The fitness value of each forwarding node ranges from zero to one and the threshold value is 0.5. We used the free fuzzy logic library (FFLL) [13] on the web to perform the simulation. Fig. 4.1 shows the average energy consumption per report as the FTR in the network increases from 0% to 100%.

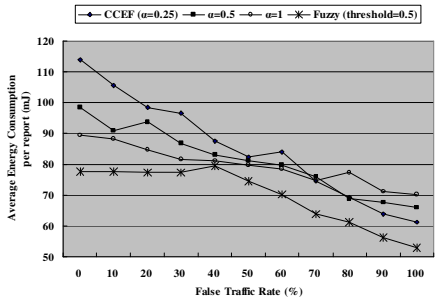


Figure 4.1: Average Energy Consumption per Report

The average energy consumption of the filtering schemes tends to decrease as the FTR in the network increases because many false reports in the network are dropped en-route. The CCEF scheme with small α achieves high probability for filtering operations, so it is energy-efficient when the FTR is high, and vice versa. The CCEF with α = 1 (checks) is relatively energy-efficient when the FTR is lower than 70%; however, it is inefficient when the FTR is higher than 70%. The CCEF with α = 0.25 (diamonds).

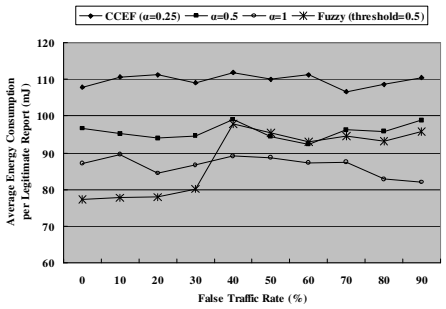


Figure 4.2: Average Energy Consumption per Legitimate Report

The CCEFs with α = 0.25, 0.5, and 1 consume a relatively constant energy for processing a legitimate report because their filtering probability at each node is static. On the other hand, the proposed method based on fuzzy logic adjusts the detection power to the network state. The method consumes the least energy to process a legitimate report when the FTR is less than 40% and an average amount of energy when the FTR is larger than 40%. Fig. 4.3 represents the average energy consumption per false report of the filtering schemes.

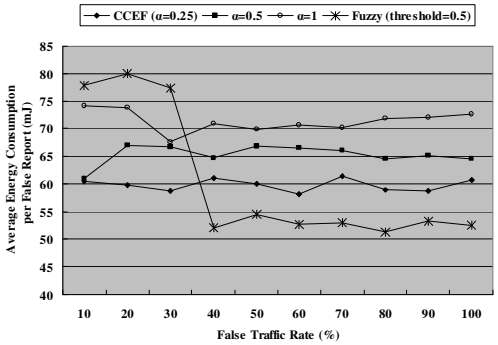


Figure 4.3: Average Energy Consumption per False Report

The CCEFs expend a relatively static energy to manage a false report. When the FTR is less than 40%, the proposed method consumes the most energy. However, when the FTR is greater than 40%, it consumes the minimum energy. Hence, the average energy consumption of the proposed method is the minimum.

5. Conclusion

In this paper, we investigated the operation of the CCEF scheme and indicated the shortcomings of the probability based en-route filtering schemes. In order to enhance the energy efficiency of the CCEF scheme we proposed the fuzzy–based filtering node assigning method for wireless sensor networks; the method can improve the energy efficiency of filtering schemes for wireless sensor networks. The proposed method assigns some of the nodes in a routing path as the filtering nodes based on the fuzzy logic output. The input factors are the energy resource level of a node, the number of MACs for generating a node MAC, and the false traffic rate in the network. We validated the energy efficiency of the proposed method by simulating the method against false report injection attacks and comparing it with the CCEF scheme. We plan to conduct further research on the optimal selection of the filtering nodes in a path in order to conserve more energy.

References

[1] Akyldiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E.. A Survey on Sensor Networks, IEEE Wireless Communication Magazine, 40(8) (2002) 102--116.

[2] Al-Karaki, J.N., and Kamal, A.E.. Routing techniques in wireless sensor networks: a survey. IEEE Wireless Communication Magazine. 11(6) (2004) 6--28.

[3] Karlof, C., and Wagner, D.. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Elsevier, Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, 1(2-3) (2003) 293--315.

[4] Yang, H. and Lu. S., Commutative Cipher Based En-route Filtering in Wireless Sensor Networks. IEEE in Proc. of VTC (2004) 1223--1227.

[5] Lee, H.Y. and Cho, T.H.. Fuzzy Adaptive Selection of Filtering Schemes for Energy Saving in Sensor Networks. IEICE Transactions on Communications E90-B(12) (2007) 3346--3353.

[6] Lee, H.Y. and Cho, T.H.. Fuzzy-Based Path Selection Method for Improving the Detection of False Reports in Sensor Networks. IEICE Transactions on Information and Systems E92-D(8) (2009) 1574--1576.

[7] Nghiem, P.T. and Cho, T.H.. A Multi-path Interleaved Hop by Hop En-route Filtering Scheme in Wireless Sensor Networks. Computer Communications, Elsevier 33(10) (2010) 1202--1209.

[8] Seo, H.S., Lee, H.Y., Lee, S.J., Lee, D.G.. FUZZY-BASED FILTERING SOLUTION SELECTION METHOD FOR DYNAMIC SENSOR NETWORKS. Intelligent Automation and Soft Computing 16(4) (2010) 577--590.

[9] Kim, J.M., Han, Y.S., Lee, H.Y. and Cho, T.H.. Path Renewal Method in Filtering Based Wireless Sensor Networks. Sensors 11 (2011) 1396--1404.

[10] Kim, J.M., Seo, H.S., Kwak, J.. Routing Protocol for Heterogeneous Hierarchical Wireless Multimedia Sensor Networks. Wireless Personal Communications 57(3) (2011) 577--590.

[11] Yen, John and Langari, Reza. 1999. Fuzzy Logic - Prentice Hall.

[12] Xbow sensor networks, http://www.xbow.com/

[13] FFLL, http://ffll.sourceforge.net

Soo Young Moon received the B.S. and M.S. degrees in Electrical and Computer Engineering from Sungkyunkwan University in 2007 and 2009, respectively. He is now a doctoral student in the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include modeling and simulation, wireless sensor networks, network security, and artificial intelligence.

Hee Suk Seo (Corresponding Author) is now a Full Professor of Korea University of Technology and Education, Republic of Korea. He received his Ph.D. degree from Sungkyunkwan University, Republic of Korea, in 2005. USN, network security, and simulation are his interesting topic.