

Fuzzy Efficient MAC length Determination Method for Commutative Cipher Based Filtering

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

**school of Information and Communication Engineering, Sungkyunkwan University*

mhhan@ece.skku.ac.kr, cisun@ece.skku.ac.kr, taecho@ece.skku.ac.kr

Abstract—Wireless Sensor Networks are vulnerable to false data injection attack, because they are often deployed in a hostile environment. Adversaries may attempt various security attacks on sensor networks through a compromised node, with the goal of deceiving the sink node or depleting the limited energy resources of nodes. The commutative cipher based en-route filtering scheme (CCEF) was proposed to detect and drop such false reports during the forwarding process. In this scheme, the number of message authentication codes (MAC) is important to detect false reports and save energy in the sensor network. In this paper, we propose a fuzzy efficient MAC length determination method for CCEF, in which the MAC length is adaptively determined by a fuzzy rule based system. The distance from the sink node to the cluster head (CH), the false traffic rate, and energy level are used to determine the MAC length through a fuzzy rule based system. We show the proposed method can save energy and provide sufficient resilience against false data injection attack.

Keywords— wireless sensor network, MAC, false data injection attack, fuzzy rule based system, filtering scheme

I. INTRODUCTION

Wireless communications and electronics have enabled development of small, low-cost, low-power and multi-functional sensor nodes. Sensor nodes consist of sensing, data processing, and communicating components. They leverage the idea of a sensor network [1]. Wireless sensor networks consist of a large number of sensor nodes that have limited processing power, small storages space, narrow bandwidth and limited energy and a few sink nodes that collect the sensor reading [2]. Sensor networks are expected to interact with the physical world at an unprecedented level of universality, enable various new applications [5]. Sensor nodes are usually scattered in unattended areas and communicate either with other nodes or directly with an external sink node [2].

Nodes are vulnerable to physical attacks, potentially compromising the nodes' cryptographic key. They are scattered in a hostile environment for various applications [4]. Forged sensing reports can be injected through compromised nodes. This can lead to false alarms and the depletion of limited energy resources in battery powered networks (Fig.1) [3]. False data ought to be dropped en-route as early as

possible to minimize grave damage; the few elusive reports should be rejected at the sink node [3].

Various security solutions [5-8] and adaptive methods [9-11] have been proposed to detect and drop false reports before the data consumes a significant amount of energy. Their basic idea is that every node is preloaded with some symmetric key. When a real event occurs, multiple sensing nodes collaboratively originate a report that includes multiple message authentication codes (MAC). Each MAC is generated by a node using one of its symmetric keys and represents its accords on the report [12]. As a report is forwarded to the sink node over multiple hops, each forwarding node inspects the correctness of the MACs carried in the report. If the verification of a report fails, the report is dropped. Yang and Lu proposed the commutative cipher based en-route filtering scheme (CCEF) [6] as a means to detect and drop injected false reports during the forwarding process to sink nodes.

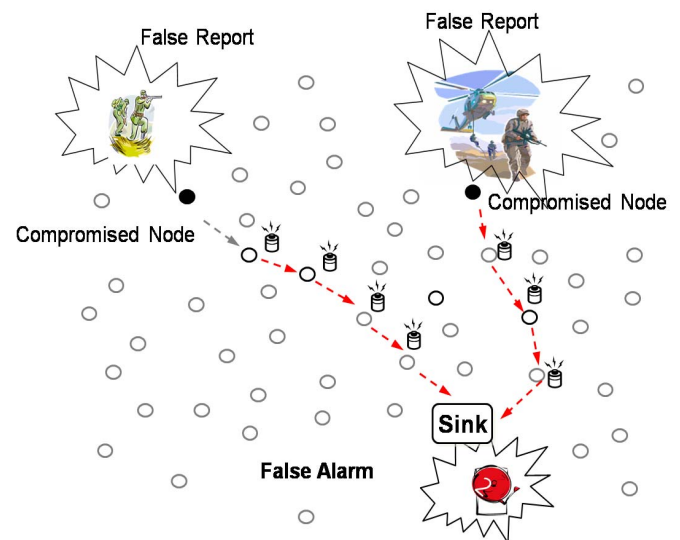


Figure 1. False data inject attack

CCEF carefully limits the amount of security information assigned to each node, to prevent any single compromised node from disrupting the entire system. When an event occurs in the field, multiple surrounding sensors collectively generate a legitimate report and endorse it by attaching to it their MACs. Thus, in the case of a report with an inadequate number of MACs, the MAC length is dropped during the forwarding

process to the sink node by intermediate nodes. As a report is forwarded through multiple hops toward the sink node, each intermediate node verifies the correctness of the MACs carried in the report with a certain probability and drops the report if an incorrect MAC is detected. So the MAC length is important in CCEF and other schemes, since it includes a trade-off of security communication overhead.

In this paper, we proposed a fuzzy based adaptive MAC length determining method for the commutative cipher based en-route filtering scheme in a sensor network. The distance from the sink node to the cluster head, false traffic rate and energy level are used to determine the MAC length. Since there is uncertainty in estimating the input parameters, the proposed method exploits a fuzzy rule based system. Fuzzy systems have shown a good degree of robustness in the face of large variability and uncertainty in parameters

The remainder of the paper is organized as follows: Section 2 briefly describes CCEF. Section 3 details the proposed method. Finally, the conclusion is discussed in Section 4.

II. BACKGROUND

In this section, we briefly describe the commutative cipher based en-route filtering scheme (CCEF) and its operation at each stage.

A. Commutative Cipher Based En-route Filtering Overview (CCEF)

In [6], Yang and Lu proposed the commutative cipher based en-route filtering scheme (CCEF) to defend against false data injection attacks without symmetric key sharing among sensor nodes. A commutative cipher has certain features that satisfy the following equation for any message M and any two keys K_1 and K_2 . CE represents a commutative cipher encryption function [6].

$$CE(CE(M, K_1), K_2) = (CE(CE(M, K_2), K_1) \quad (1)$$

The monitoring capability in CCEF is protected by secrets shared between the sensor nodes and sink node, while the en-route filtering capability is achieved via partial evidence of the secret association [6]. Thus, CCEF is able to provide much stronger security protection against compromised nodes than does a symmetric cryptography based security solution.

In CCEF, each node has a unique ID and is preloaded with unique key it shares only with the sink node. The sensor nodes are tasked by the sink node through queries in the operational phase. For each session, the sink prepares two keys K_s and K_w .

$$CE(M, K_w) = CE^{-1}(M, K_s) \quad (2)$$

CE and CE^{-1} are the encryption and decryption algorithm of the cipher, respectively. The sink node randomly selects

one sensor node at the location of interest as a cluster head and sends a query to the cluster head. A unique query ID is QID, the cluster head's unique ID is CID, K_s encrypted by the cluster head's key, and K_w as plaintext are included in query. Each forwarding node stores the QID and K_w for future verification. When the cluster head accepts the query, it decrypts the K_s and then forwards the query to its local neighbours (Fig 2(a)). After query propagation, each forwarding node has QID and K_w , and the cluster head has QID and K_s (Fig. 2(b)). So the cluster head generates a sensing report. Each sensing report is endorsed by two MACs. One MAC is generated by the cluster head using K_s . The other is generated by its neighbour nodes. The report is forwarded to the sink along the reverse path the query traverses. Every forwarding node is able to verify the report using K_w .

$$CE(CE(R, K_s), K_w) = R \quad (3)$$

The forwarding nodes validate a report from the cluster head based on a probability P , that is determined by the security parameter a and hop count h from the cluster head to the sink node, as shown in the following equation.

$$P = \frac{1}{ah} \quad (4)$$

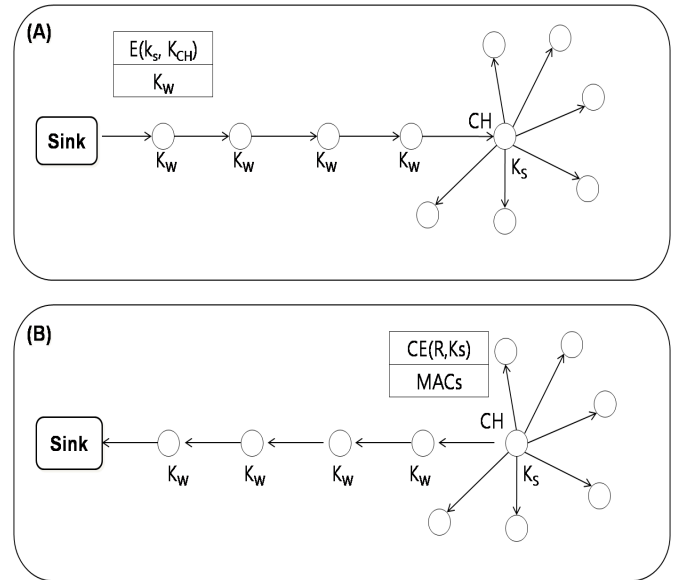


Figure 2. Commutative Cipher based En-route Filtering Scheme

III. PROPOSED METHOD

In this section, we detail our proposed method.

A. Assumption

We consider a sensor network composed of a large number of small sensor nodes. Our proposed method includes the assumption of the CCEF scheme described in section II. Similar

to the CCEF scheme, the sensor nodes in our proposed method move after initial deployment, possess limited memory and energy resources, and cover a small sensing range. Sensor nodes may be compromised or physically captured. Due to cost constraints, we assume that each sensor node is not equipped with tamper-resistant hardware. The sink node initiates the session and sends a query message to the selected cluster head to obtain the report. The sink node cannot be compromised, and cluster head cannot be destroyed. CCEF assumes that the sink node is able to know their locations [6]. Thus, the sink node knows the number of hops from each node to itself. We also assume that the sink node is able to know or estimate the rate of false traffic, and the distance and energy level in the sensor network. We further assume that the sink node has a mechanism to authenticate a broadcast message, and every sensor node can verify broadcast messages.

B. Motivation

In the CCEF scheme, when events occur in the sensing field, they are detected by all surrounding sensor nodes. Each node generates MAC through one of its keys, and sends the set of MAC and Key index that are used to generate MAC to the cluster head. Each sensing report is endorsed by two MACs. One MAC is generated by the cluster head; the other is generated by its neighbourhood nodes. It generates a legitimate report consisting of event information and sets of key indexes and MAC. The MAC length, that is number of attached sets of key indexes and MAC in a legitimate report, is important, because it includes a trade-off of the probability of detecting false reports and communication overhead. We carefully determine the MAC length based on the false traffic rate, distance, and energy level of the node in the sensor network.

C. Overview

The proposed method is based on CCEF. For each session, the sink node randomly selects a node at the location of interest as a cluster head. It determines the MAC length with a fuzzy rule based system. The false traffic rate, distance from sink node to cluster head and the energy level of cluster head and its neighbour nodes are used to determine the MAC length. The sink node broadcasts to the cluster head and its neighbour nodes. Every cluster head create the session MAC length and its neighbour nodes also create the node MAC length. We apply the fuzzy rule based system to the node MAC length. The sink node determines the MAC length every time network status changes, based on the fuzzy factors. Thus the proposed method is more flexible than the CCEF.

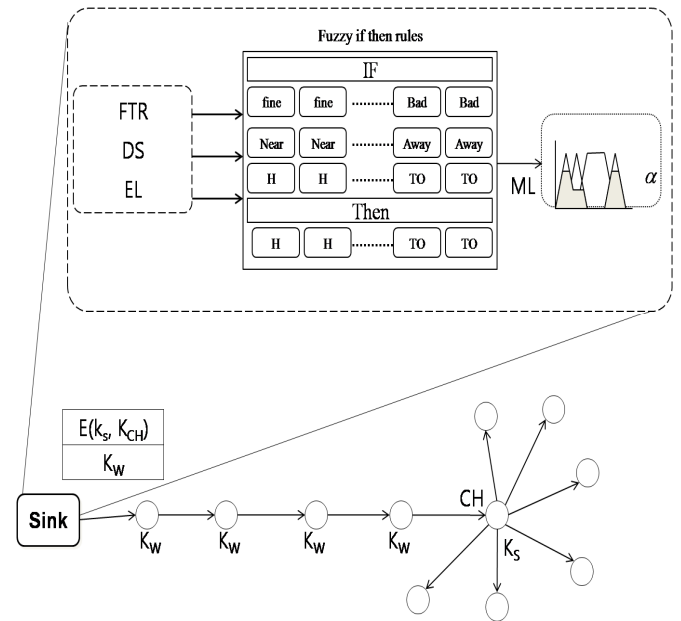


Figure 3. Proposed Method

D. Input parameters

In this section, we discuss the factors that are used for fuzzy inference. The factors are the false traffic rate (FTR), distance from sink node to cluster head (BS), and energy level of nodes (EL) in the network. 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 false reports. Conversely, if this value is small, the fitness value of the node ought to be small to reduce unnecessary energy consumption. The DS should be considered to conserve network energy and enable efficient key diffusion. Usually, nodes are distributed with high density, and used as a path that leads to the sink nodes, so these nodes consume more energy than other nodes. So we should reduce the overhead of diffusion messages, and conserve energy. EL is also considered to be important. Generally, sensor nodes have limited power and are irreplaceable, since they have limited capacity and are left unattended. Thus, we have to determine the MAC length based on the energy level of the node.

E. Fuzzy Logic function

The membership functions of three input parameters – False traffic rate (FTR), distance from sink node to cluster head (DS) and energy level of nodes (EL) – of the fuzzy logic are shown in Fig. 4(a), (b) and (c). The labels in the variables are presented as follows.

- FTR = {F (fine), N (normal), B (poor)}
- DS = {S (small), M (medium), L (large)}
- EL = {VS (very small), S (small), E (enough)}

The output parameter of the fuzzy logic is ML = {VS (very small), S (small), M (medium), L (large), VL (very large)}. It is represented by the membership function, as shown in 4(d).

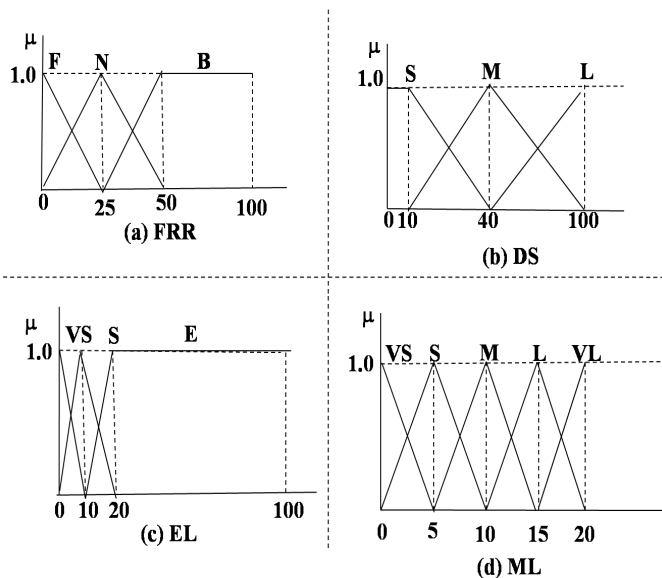


Figure 4. Fuzzy membership functions

Table 1. Fuzzy if-then rules

#RULE	IF			THEN
	FRR	DS	EL	
01	F	S	E	VS
02	F	M	E	VS
04	F	L	S	VS
05	N	L	E	L
07	N	M	E	VL
08	N	S	E	VL
09	B	S	E	L
10	B	S	S	S
12	B	M	S	M
13	B	M	S	M
15	N	M	S	S
16	F	L	E	S
18	F	M	M	M
19	B	L	VS	VS

TABLE 1 SHOWS SOME OF THE FUZZY RULE-BASED SYSTEM.

Rule 1: If FRR is F (fine), DS is S (small) and EL is E (enough), ML is VS (very small), because sink nodes do not accept a number of false data reports, energy is enough and distance is small.

Rule 9: If FRR is B (bad), DS is S (small) and EL is E (enough), ML is L (large), because sink nodes accept a

number of false data reports, each node's energy is enough and distance is small. Therefore, ML is L (large).

Rule 10: If FRR is B (bad), DS is S (small) and EL is S (small), ML is S (small), because sink nodes accept a number of false data reports, each node energy is enough and distance is small. Therefore, ML is S (small).

IV. SIMULATION RESULT

In order to validate the efficiency of proposed method, we simulated the method against the false report injection attacks and compared it to the CCEF scheme. We used $150 \times 100 \text{m}^2$ field and 3,600 sensor nodes uniformly deployed in the field. There are 600 $5 \times 5 \text{m}^2$ -size clusters and each clusters and each cluster has exactly six nodes. The hop count from the BS to the CH nodes is defined as the number of clusters from the BS to the CH node. Routing of each query or report is performed on the square. The energy consumption for transmitting and accepting a report is 1.15 mJ and the energy consumption for performing commutative cipher computation is 9 mJ [6].

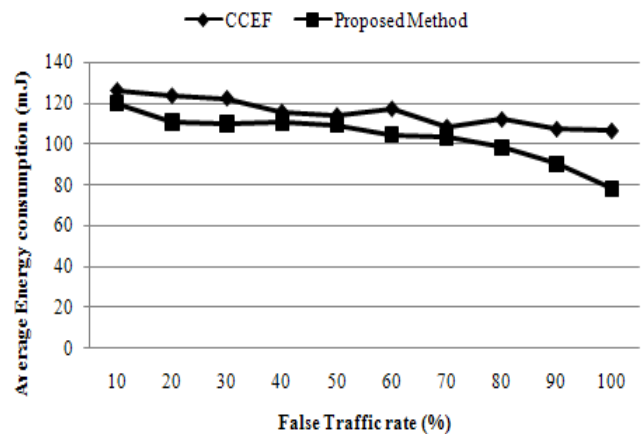


Figure 5. Average energy consumption

Fig. 5 shows the average energy consumption per report when the false traffic rate (FRR) varies from 0% to 100% (MAC=1). It can be shown that the CCEF and Proposed method is similar to energy consumption when false traffic rate is less than 70%, however Proposed method is efficient than CCEF when false traffic rate is greater than 70%.

Fig. 6 show the filtering count per report when the false traffic rate (FRR) varies from 0% to 100% (MAC=1). It can be shown that the CCEF and Proposed method is similar to filtering count when false traffic rate is less than 60%. But Proposed method is efficient than CCEF when false traffic rate is greater than 60%.

The proposed method is much more efficient than CCEF against legitimate traffic in conserving energy, since only a small number of forwarding nodes verify data in the proposed method.

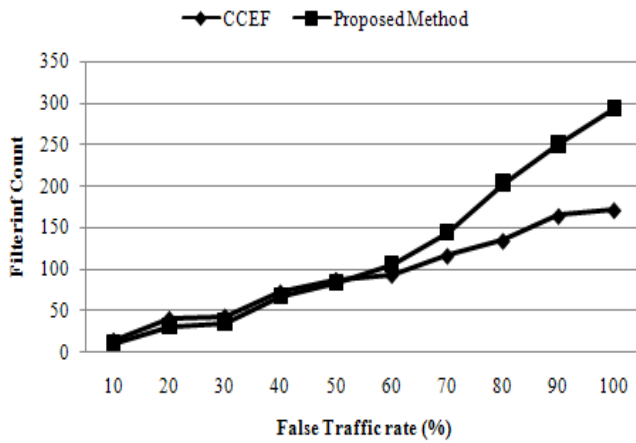


Figure 6. Filtering Count

V. CONCLUSIONS AND FUTURE WORKS

This paper proposes an efficient MAC length determination method for CCEF using a fuzzy rule based system. The false traffic rate (FRR), distance from sink node to cluster head (DS) and energy level of nodes (EL) are used to determine the input parameters. The effectiveness of the proposed method is shown via simulation at the end of the paper.

We will also run additional simulations with other input factors not covered in this work.

ACKNOWLEDGMENT

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 Communications Magazine," vol. 40, no. 8, pp. 102-116, 2002.
- [2] Al-Karaki, J. N., Kamal, A. E.: Routing techniques in wireless sensor networks: a survey. IEE Wirel. Commun. 11(6) (2004) 6-28
- [3] Zhang, W., Cao, G.: Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach. In Proc. of INFOCOM (2005) 503-514
- [4] Przydatek, B., Song, D., Perring, A.: SIA: Secure Information Aggregation in Sensor Networks. In Proc. of SenSys (2003) 255-265.
- [5] Ye, F., Luo, H., Lu, S.: Statistical En-Route Filtering of Injected False Data in Sensor Networks, IEEE J. Sel. Area Comm. 23(4) (2005) 839-850.
- [6] Yang, H, Lu, S. Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks. In Proc. of VTC(2003) 1223-1227
- [7] Yu, Z., Guan, Y. A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks. In Proc. Of SenSys (2005) 294-295
- [8] 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.
- [9] 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.
- [10] M.H Han, H. Y. Lee and T.H. Cho, "Fuzzy-Based Verification-Probability Determination Method for Dynamic Filtering in Sensor Networks," International Journal of computer Science and Network Security, vol. 8, no. 8, pp 132-136, Aug.2008.
- [11] Li, F., Wu, J: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks. In Proc. of IWCMC (2006) 27-32
- [12] Turcan, A., Ocelikova, E.: Fuzzy Clustering Applied on Mobile Agent Behaviour Selection. In Proc. of SAMI (2005)