

Control Method of Checkpoint Node Selection Using a Fuzzy Rule System and Feedback in CHEMAS

Ji Won Kim*, Soo Young Moon*, Tae Ho Cho*, Jin Myoung Kim**, Won Tae Kim**, Seung Min Park**

*School of Information and Communication Engineering, Sungkyunkwan University, Suwon 440-746, Republic of Korea

**Electronics and Telecommunications Research Institute (ETRI), Daejeon 305-700, Republic of Korea

{jwonkim, moonmous, taecho}@ece.skku.ac.kr

{jm.kim, wtkim, minpark}@etri.re.kr

Abstract— Wireless sensor networks (WSNs) have security vulnerabilities. Thus, they are exposed to diverse attacks. A selective forwarding attack is service denial attack. In this attack, an adversary stains nodes and uses compromised nodes to selectively drop important messages. The checkpoint based multi-hop acknowledgement scheme (CHEMAS) is proposed to detect selective forwarding attack. The checkpoint node is selected due to a previously fixed probability. The selection of checkpoint nodes affects security intensity and energy efficiency. We propose a control method of checkpoint node selection using a fuzzy rule system and feedback concept in CHEMAS. Simulation shows the proposed method obtains a high detection ratio and achieves efficient energy conservation.

Keywords— Wireless Sensor Network, Selective Forwarding Attack, CHEMAS, Fuzzy Rule System, Feedback

I. INTRODUCTION

Wireless sensor networks (WSNs) are actively used in various fields, such as military applications, environment sensing, home networks, due to technology advances [1]. WSNs are vulnerable to an adversary's attack, since sensor nodes have low energy, and limited computational capacity. Early WSNs designs did not consider security. Adversaries attempt various attack schemes for WSNs. For example, selective forwarding attack damages intermediate nodes in the path between the source node and sink node. A damaged node is used to selectively drop important information [2].

Bin Xiao et al. proposed a checkpoint based multi-hop acknowledgement scheme (CHEMAS) to detect selective forwarding attacks [3]. In this scheme, when checkpoint nodes receive an event packet, the acknowledgement (ACK) packet is used to confirm normal packet transmission. If abnormal transmission occurs in the path, then an alert packet is generated to report the suspicious node. A checkpoint node is randomly selected based upon static probability. The number of Checkpoints is an important factor that affects security intensity and energy efficiency. We propose a checkpoint node selection control method using a fuzzy rule system and feedback concept. The proposed scheme's fuzzy rule system has three inputs and one output parameter. The Input parameters are the average remaining energy, variation of alert

packet, and previous round checkpoint node selection probability control value. The output parameter is the next round checkpoint node selection probability control value. In this system, the previous round output value is the next round input value. We expect feedback about the current WSN status using this process. Thus, delicate control of checkpoint node selection probability is enabled.

The remainder of this paper is organized as follows. In section 2, we review the selective forwarding attack and CHEMAS. Section 3 explains the proposed method. Section 4 shows other selective forwarding attack detection schemes and existing security intensity control methods in CHEMAS. Section 5 discusses simulation. We conclude this paper in section 6.

II. BACKGROUND

A. Selective forwarding attack

Sensor nodes are usually easily damaged by an adversary's attack, as they have limited capacity and are located in a dangerous environment. Thus, many attacks exist; among these attacks, in selective forwarding, an adversary uses compromised nodes to selectively drop important event packets. Fig 1 shows a selective forwarding attack example.

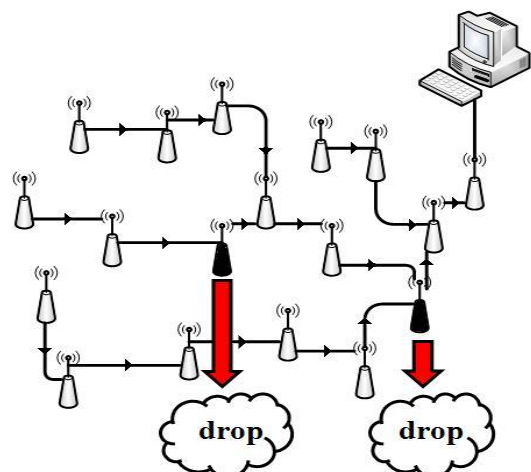


Figure 1. Selective forwarding attack in WSN

Compromised nodes normally look like other common nodes. However, when important sensing data are forwarded, compromised nodes between the sources and sink node drop the packet. Thus, it is difficult to detect selective forwarding attack. This attack arouses confusion in the user, because information that should certainly be delivered to the user cannot be forwarded.

B. CHEMAS

The checkpoint based multi-hop acknowledgement scheme (CHEMAS) was proposed by Bin Xiao et al. to detect selective forwarding attack. When an event packet is generated by a source node and delivered to a sink node in CHEMAS, checkpoints are selected according to a probability fixed in advance. The sink node and each checkpoint node generate acknowledgement (ACK) packets to confirm normal packet delivery. Each ACK packet is forwarded in the direction from the start node (sink or checkpoint node) to the source node based on the Time to Live (TTL) value in this packet. If a node has not received sufficient ACK packets, then the nodes generates an alert packet to report the suspect node. We can detect compromised nodes by analysing the alert information reported. Fig 2 overviews CHEMAS.

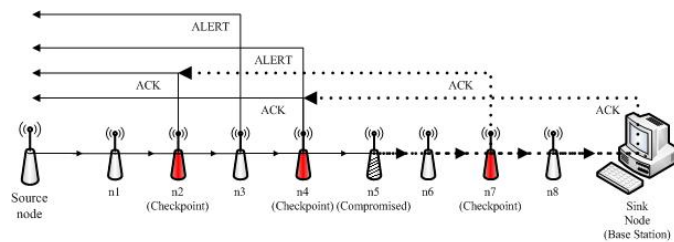


Figure 2. Overview of CHEMAS

III. CONTROL METHOD OF CHECKPOINT SELECTION

A. Motivation

Checkpoint node selection probability (P) and acknowledgement packet delivery hop count (ACK_TTL) are the main factors affecting security intensity and energy efficiency. A high value for P and ACK_TTL provides strong security intensity but yields low energy efficiency. Conversely, low values for these factors provide weak security intensity but achieve high energy efficiency. These factors are a trade-off. Thus, making decisions on these factors is an important issue, as WSNs have limited energy.

B. Assumptions

The proposed method makes the following assumptions. The compromised nodes can only drop packets. These nodes cannot generate fake alert packets. Fake alert means that the compromised node prosecutes an innocent node as a suspect node. Nodes are not compromised in a deployed state. The adversary does not drop all packets but drops them selectively. We designed the attack model and the sensor network model based on discrete event system specification (DEVS) formalism [4].

C. Overview

We propose a fuzzy rule system and feedback concept to control checkpoint node selection probability. The fuzzy rule system has three inputs and one output parameter. The input parameters are the previous round's checkpoint node selection probability control value, average remaining energy and variation of alert packet numbers. The output parameter is the next round's checkpoint node selection probability control value. The fuzzy rule system is on the sink node. Each round has a fixed number of event packet deliveries. After one round, the fuzzy rule system infers the next round control value from information of the previous round. Fig 3 overviews the proposed method.

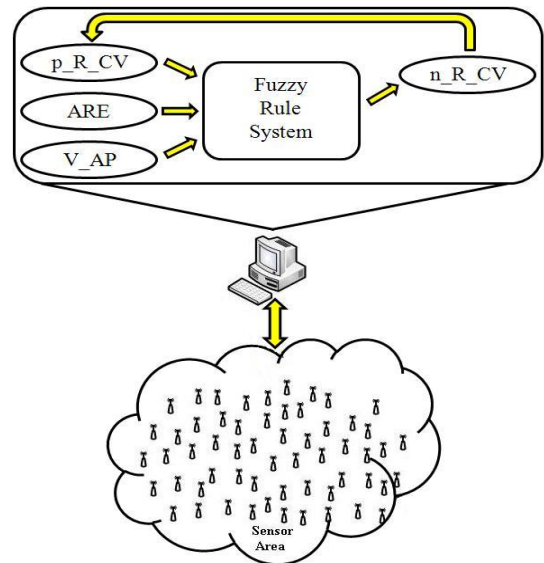


Figure 3. Proposed system overview

D. Input & output parameters

The first input parameter is the average remaining energy (ARE). ARE denotes the average remaining energy of nodes in each path. If nodes have sufficient remaining energy then the system has strong security intensity. However, if they have insufficient energy, then the system must decrease the number of checkpoint nodes to increase the lifetime of the WSN. We can know the remaining energy of each path through an event packet. The remaining energy is inserted inside the event packet by the node when it forwards an event packet.

The second input parameter is the variation of the generated alert packet number (V_AP). An increase in alert packets implies an active attack by an adversary. In contrast, a decrease of alert packets means that attacks are decreasing. Consequently, we can immediately implement a control based on the change state of WSNs.

The third input parameter and output parameter are the checkpoint node selection probability control values. These values are used as input and output parameters. The system decides the next round control value (n_R_CV) based on other input parameters and previous round control value (p_R_CV). This value is the interaction with other values. As a result, the

system generates feedback about the next round control value. The labels in the parameters are presented as follows.

$ARE = \{S \text{ (small)}, M \text{ (medium)}, L \text{ (large)}\}$

$V_AP = \{D \text{ (decrease)}, K \text{ (keep)}, I \text{ (increase)}\}$

$p_R_CV, n_R_CV = \{D \text{ (decrease)}, K \text{ (keep)}, I \text{ (increase)}\}$

Fig 4 shows the membership function of each parameter.

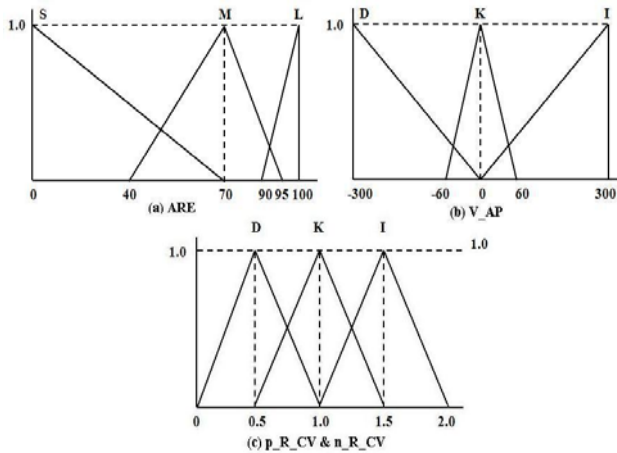


Figure 4. Membership function

E. Design fuzzy rule

Table 1 shows some of the designed fuzzy rules.

Table 1. Fuzzy if-then rules

RULE	IF			THEN
	ARE	V_AE	p_R_CV	n_R_CV
01	L	I	I	I
03	L	D	I	K
06	M	D	I	D
10	L	I	K	I
16	S	K	K	D
20	L	K	D	K
26	S	K	D	D

In rule 1, if p_R_CV is I (increase), V_AE is I (increase), and ARE is L (large); then, n_R_CV is I (increase). The system increases security intensity, since it is not concerned about energy exhaustion when the path is attacked actively by an adversary, because the average remaining energy is large. In contrast, in rule 16, as ARE is S (small), although V_AE shows K (keep) state, n_R_CV must be changed D (Decrease).

In rule 3, if p_R_CV is I (increase) and V_AE is D (decrease) then n_R_CV is K (keep). That is, the system decreases security intensity based on the change of the damaged state of the path.

In rule 6, if ARE is M (medium) and V_AE is D (decrease) then the system decreases n_R_CV . That is, security intensity is decreased based on the declining remaining energy.

IV. RELATED WORK

Many detection schemes have been proposed for selective forwarding attack. Sophia Kaplantzis et al. proposed a scheme

using a support vector machine (SVM) to detect selective forwarding attack and black hole attack [5]. In [5], the proposed system is a centralized IDS that detects selective forwarding attack and black hole attack. This was the first study to use SVMs for intrusion detection in WSNs. However, it is inaccurate when there is low participation for selective forwarding. In the Game theory model proposed by Yenumula B Reddy et al [6], a framework is proposed to detect malicious nodes using a zero-sum game approach and selective node acknowledgements in the forwarding data path [6]. In a sequential mesh test based detection scheme proposed by Guorui Li et al [7], the cluster head node detects the packet drop nodes based on the sequential mesh test method after receiving the packet drop reports.

Several methods were proposed to improve CHEMAS using a fuzzy rule system. The ACK_TTL control method used a fuzzy rule system proposed by Sang Jin Lee et al [8]. In [7], the energy level, the number of compromised nodes, and distance to each node from the sink node are used to determine ACK_TTL in CHEMAS. Lee also proposed a control method for the number of checkpoint nodes [9]. In [9], the remaining energy in the path and the number of suspect nodes are used as input parameters. The fuzzy rule system uses these variables to control the number of checkpoint nodes.

V. SIMULATION RESULT

We simulate the detection ratio and energy consumption of CHEMAS and the proposed method to evaluate the efficiency. In this simulation, the detection ratio is defined as the reported number of alert packets for real compromised nodes against the entire reported alert number.

300 sensor nodes are randomly deployed. We operate simulation for 10 rounds, during which 200 event packets are delivered from the source node to sink node at each round. The ratio of compromised nodes is 20%, 40%, 60% and 80% of the entire nodes. Compromised nodes drop 30% of all event packets. The energy consumption for packet transmission, receiving and generation is 15μJ, 10μJ, and 15μJ respectively for each node. The path range is 10 ~ 15 hops. The initial value of P (checkpoint selection probability) is 0.7 and 0.45.

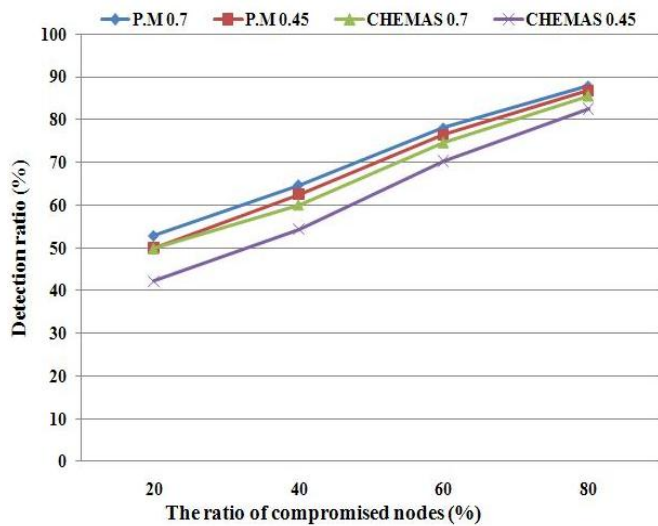


Figure 5. Comparison detection ratio

Fig 5 shows the detection ratio in proportion to the degree of damage in the entire network. The proposed method achieves higher detection ratio than original CHEMAS. Thus, the proposed method can control checkpoint selection probability based on the change of attack degree.

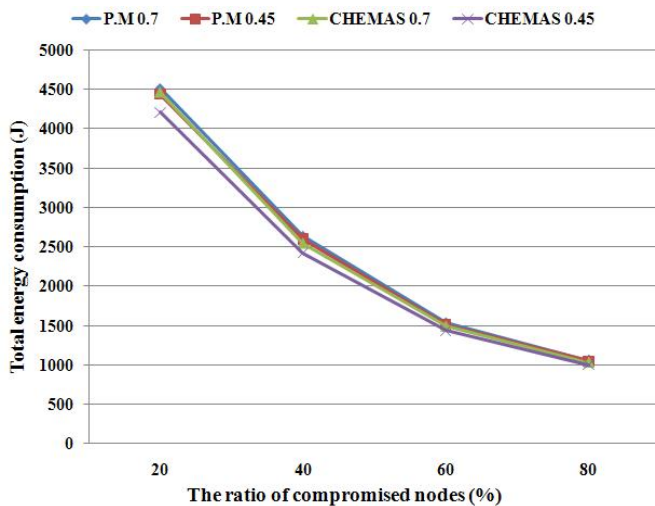


Figure 6. Comparison of total energy consumption

Fig 6 shows total energy consumption of the proposed method and CHEMAS. The energy consumption degree of each method is similar. Since all detection ratios of the proposed method are higher than the original CHEMAS 0.7,

with similar energy consumption, it is more efficient than the original method.

VI. CONCLUSIONS

In this paper, we proposed a control method of checkpoint selection probability using a fuzzy rule system and feedback concept in CHEMAS. In original CHEMAS, the selection probability of checkpoint is an important factor to determine the security intensity and energy efficiency. We can consider the state of affected networks using the fuzzy rule system and feedback. The proposed method enhances detection ratio with similar energy consumption to the original CHEMAS scheme.

In future work, we will perform additional simulations in various situations not covered in this study.

ACKNOWLEDGMENT

This work was supported by the IT R&D Program of MKE/KEIT [10035708, "The Development of CPS(Cyber-Physical Systems) Core Technologies for High Confidential Autonomic Control Software"]

REFERENCES

- [1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, Volume 38, Issue 4, pp. 393-422, 2002,
- [2] Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks, Volume 1, Issues 2-3, pp. 293-315, 2003.
- [3] Bin Xiao, Bo Yu and Chunanshan Gao, "CHEMAS: Identify suspect nodes in selective forwarding attacks", Journal of Parallel and Distributed Computing, Volume 67, Issue 11, pp. 1218-1230, 2007.
- [4] B. P. Zeigler, H. Praehofer and T. G. Kim, Theory of modeling and simulation, 2nd edition, Academic Press, New York, 2000.
- [5] Sophia Kaplantzis, Alistair Shilton, Nallasamy Mani and Y. Ahmet Sekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines", Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference, pp. 335-340, 3-6 Dec. 2007
- [6] Yenumula B Reddy and S. Srivathsan, "Game theory model for selective forward attacks in wireless sensor networks", Control and Automation, 2009. MED '09. 17th Mediterranean Conference, pp. 458-463, 24-26 June 2009
- [7] Guorui Li, Xiangdong Liu and Cuirong Wang, "A sequential mesh test based selective forwarding attack detection scheme in wireless sensor networks", Networking, Sensing and Control (ICNSC), 2010 International Conference, pp. 554 - 558, 10-12 April 2010
- [8] Sang Jin Lee, Jong Hyun Kim, Tae Ho Cho, "Control Method for the Number of Travel Hops for the ACK Packets in Selective Forwarding Detection Scheme", Journal of the Korea Society for Simulation, vol. 19- 2, pp. 73-80, The Korea Society For Simulation, Jun 2010.
- [9] Sang Jin Lee, Tae-Ho Cho, "Control Method for the number of checkpoint nodes in detection scheme for selective forwarding attacks", proceedings of the ITFE Summer Conference, pp. 387-390, Aug 27-30 2009.