An Energy-Efficient Routing Method with Intrusion Detection and Prevention for Wireless Sensor Networks

Soo Young Moon*, Ji Won Kim**, Tae Ho Cho*

*College of Information and Communication Engineering, Sungkyunkwan University, Korea
**CAE Division Solution Develop Team, CEDIC, Korea
moonmouse@skku.edu, jwkim@cedic.biz, thcho@skku.edu

***Abstract*— Because of the features such as limited resources, wireless communication and harsh environments, wireless sensor networks (WSNs) are prone to various security attacks. Therefore, we need intrusion detection and prevention methods in WSNs. When the two types of schemes are applied, heavy communication overhead and resulting excessive energy consumption of nodes occur. For this reason, we propose an energy efficient routing method in an environment where both intrusion detection and prevention schemes are used in WSNs. We confirmed through experiments that the proposed scheme reduces the communication overhead and energy consumption compared to existing schemes.**

***Keywords*— wireless sensor networks, network layer attacks, intrusion detection, intrusion prevention**

I. INTRODUCTION

The wireless sensor network (WSN) is an infrastructure that senses environmental information such as temperature, humidity, sound and image, collects and provides the information to users [1]. A WSN is composed of many sensor nodes and one or more sink nodes. The main features of WSNs are limited resources such as CPU, memory, and battery and exploitation of wireless communication between nodes.

Because of the above features, the WSNs are vulnerable to security attacks. Selective forwarding, wormhole, and Sybil attacks among them are representative attacks in the network layer. In selective forwarding attacks, compromised nodes in the network maliciously drop all or portion of event reports that are forwarded through the routing paths that contain them. In wormhole and Sybil attacks, attackers manipulate routing paths so that compromised nodes are included in many routing paths. The two attacks make the selective forwarding attacks easy for the attacker.

There have been many studies on intrusion detection and intrusion prevention schemes depending on attack types in WSNs. However, it is infeasible to predict which attack will occur in real WSN. In addition to that, multiple attacks may occur alternatively or simultaneously. Therefore, we need to employ both intrusion detection and intrusion preventions schemes in WSNs.

When the two types of schemes are applied, heavy communication overhead and resulting excessive energy consumption of nodes occur. For this reason, we propose an energy efficient routing method in an environment where both intrusion detection and prevention schemes are used in WSNs.

We confirmed through experiments that the proposed scheme reduces the communication overhead and energy consumption compared to existing schemes.

II. BACKGROUND

A. Network layer attacks

The purpose of wormhole attack is to construct a routing path that contains an invisible tunnel composed of laptop-class attack nodes. In wormhole attacks, the attacker exploits powerful devices to create a wormhole. The attacker node at each end of the wormhole eavesdrops and forwards control messages or event reports through the wormhole. Then the other attacker node replays them. The wormhole attack enables that routing paths in the network include the wormhole. Therefore, it makes selective forwarding attacks easy for the attacker [2-4].

The goal of the Sybil attack is to lure data traffic by advertising multiple IDs through few attack nodes. In Sybil attacks, an attacker compromises many IDs in the network. An insider or outsider attack node broadcasts a forged hello messages with the compromised IDs. Then normal nodes include the compromised IDs into their neighbour nodes lists. As a result, there is a high probability that attacker node is included in routing paths [5].

The selective forwarding attacks aim to prevent important event reports from being forwarded to BS. In selective forwarding attacks, a compromised node selectively drops all or some of event reports that would be forwarded through the node. The selective forwarding attacks seriously harm the availability of the entire WSN by preventing the user from being informed of important events that had occurred in the field [6].

B. *Existing countermeasures against network layer attacks*

Intrusion-tolerant routing protocol for wireless Sensor NetworkS (INSENS)[7] is a secure routing protocol that aims to reduce damage caused by intruders who compromises nodes and tries false report injection, modification and blocking attacks. The advantage of INSENS is that even though some attacks by compromised nodes occur, it can limit the area affected by the attacks.

INSENS operates based on symmetric key based encryption. In addition to that, INSENS keep the energy consumption of sensor nodes low by exploiting BS for complex task such as computation of a routing table. Figure 1 shows the process of INSENS.

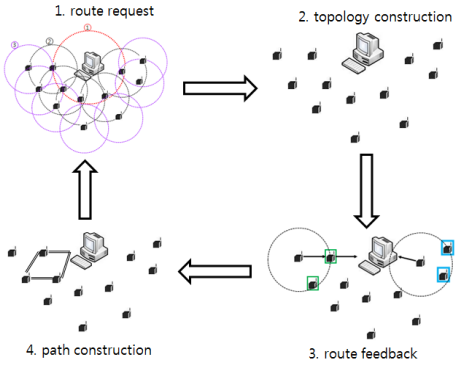

Figure 1 Process of INSENS

The process of INSENS consists of route request & topology construction, route feedback and path construction phases. In route request & topology construction phase, BS disseminates route request messages by flooding. Each sensor node records the sender of the first route request message received in the current round as its parent node. Then it updates the ID and MAC in the message and broadcasts to its neighbour nodes. Whenever a node receives a route request message, it adds the sender to its neighbour nodes list.

In the route feedback phase, every sensor node reports back local topology information to the BS. Each message authentication code (MAC) is generated by using the MACs of upstream nodes and the one way hash chain number (OHC). Therefore, an attacker cannot reuse an eavesdropped route feedback message in other region, or in later rounds.

In the path construction phase, BS verifies the topology of the network and computes a multipath forwarding table. BS sends the multipath forwarding table based on unicast routing.

In INSENS, all the nodes in the network send the route feedback messages to BS. Therefore, for every round excessive energy consumption occurs due to the route request and feedback messages exchanged.

CHEckpoint-based Multi-hop Acknowledgement Scheme (CHEMAS) [6] is a security scheme to detect selective forwarding attacks. In CHEMAS, randomly selected nodes on forwarding paths of event reports are assigned as checkpoint nodes. The checkpoint nodes send multi-hop ACK messages in source node direction. Sensor nodes are able to detect selective forwarding attacks based on the multi-hop ACK messages. Figure 2 shows the event report and ACK forwarding process in CHEMAS.

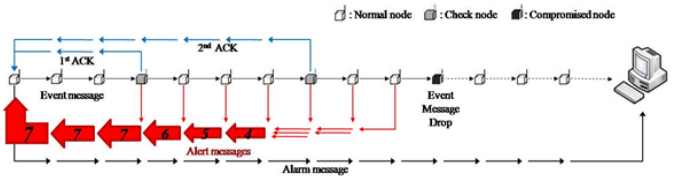

Figure 2 Process of CHEMAS

In figure 2, two checkpoint nodes send back ACK messages in the source node direction. If a compromised node selectively drops event reports, intermediate nodes detect the attack since they cannot receive enough number of ACK messages for forwarded event reports. Then the detecting nodes send ALERT messages to the source node. When the source node receives the ALERT messages, it sends the ALARM message to the BS. The ALERT and ALARM messages in CHMAS cause excessive energy consumption.

III. PROPOSED METHOD

A. *Assumptions*

The assumptions in the proposed method are as follows. Each node x shares a symmetric key K_X with the BS, and it can derive the encryption key K_{XE} and the MAC generation key K_{XM}.

B. *Operation*

The proposed method is composed of three phases: an initial construction phase, a sensing data transmission phase, and a re-construction phase. The initial construction phase is executed only once. The initial construction phase and sensing data transmission phase are designed based on [7] and [6], respectively.

1) Initial construction phase

In the initial construction phase, the topology and routing path of the entire network are constructed. BS and every node in the network communicate with each other using the topology and route construction message (TRC message) and the neighbor information response message (NIR message). The TRC message has the following form:

$$TRC||ID_x||OHC_{TRC}||MAC(Key_{Xm},TRC||ID_x||OHC||MAC_{parent}) \quad (1)$$

TRC is a message type and ID_x is the sending node's ID. OHC is a one-way hash chain number generated by BS. This is used to prevent malicious reuse of the TRC message by an intruder. MAC_{parent} is the MAC generated by the parent of sender. BS broadcasts the first TRC message within the transmission range. Each receiving node records the sender in its neighbour list. If the sender is the first node from which it receives a TRC message in the current round, it records the sender as its parent node.

After that, these nodes modify the ID_x and MAC of the TRC message and re-broadcast this TRC message. Figure 3 describes this phase.

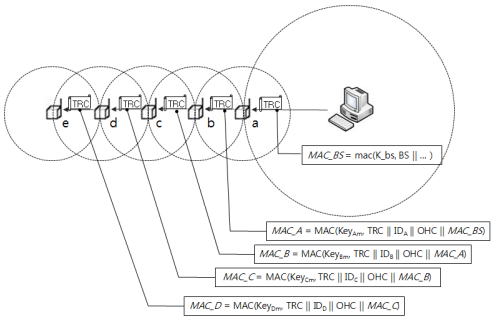

Figure 3 Broadcast of TRC message and nested MAC

After all the nodes receive a TRC message, each of them generates a neighbor information respond (NIR) message and sends it to the BS. The NIR message has the following form:

$$NIR \parallel ID_X \mid \mid E\ (K_{Xe}, NInfo) \parallel MAC\ (Key_{Xm}, OHC \| NIR \| ID_X \| E\ (Key_{Xe}, NInfo)) \quad (2)$$

NInfo indicates the neighbor node information of the sender, E (K_{Xe}, NInfo) is the encrypted NInfo by using the encryption key K_{Xe}. The NIR messages are forwarded to BS. BS obtains neighbour node information from the NIR messages, and constructs the network information table as shown in figure 4.

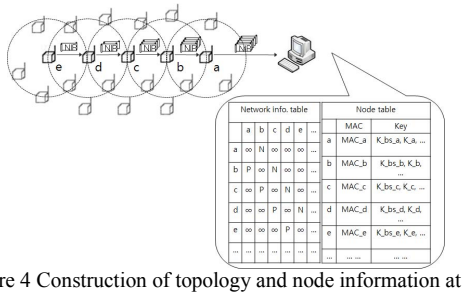

Figure 4 Construction of topology and node information at BS

After the network topology is complete, the BS computes the routing path and makes a routing table for each node. The routing path is composed of the main path and report/fallback path. The main path is used to transmit the sensing data, while the report/fallback path is used when control messages are transmitted, such as an alert message that implicates the malicious node. The report/fallback path may also be used when the main path is damaged. Computed paths are reorganized by the routing table of each node. The BS sends a routing table to each node using the routing table update message (RTU message) by unicast in a breadth-first manner [24]. The RTU message has the following form:

$$RTU \parallel OHC_{RTU} \parallel RT<dest, src, immediate\_sender> \quad (3)$$

The routing table of each node is composed of RT<dest, src, immediate_sender> in the RTU message. The three elements in RT are the destination node, source node, and immediate sending node.

2) *Sensing data transmission phase*

In the sensing data transmission phase, a sensing node generates and forwards an event report to the BS. During the forwarding process, some nodes on the path are randomly selected as check nodes. The event message (EV message) has the following form:

$$RInfo \parallel msg\_ID \parallel CHK\_seed \parallel payload \quad (4)$$

RInfo of EV messages is the routing information. CHK_seed is a seed value for probability function Fprob() that was previously loaded into the memory of the receiving node. The output of Fprob() becomes one with certain probability and if the output is one, the receiving node becomes a check node. A check node sends back an ACK message in direction to the source node. The ACK message has the following form:

$$RInfo \parallel ACK \parallel ack\_m\_ID \parallel MAC(K_{Xm}, ACK \| ack\_m\_ID) \| TTL \quad (5)$$

The ACK message is forwarded limited number of hops, the time to live (TTL) value. If TTL is one, an ACK message is forwarded to the next check node in direction to the source node. Sensor nodes that forwarded an event report but not received sufficient number of ACK messages transmit an ALERT message to the first check node in direction to the source node. The ALERT message has the following form:

$$RInfo \parallel ALERT \parallel P\_ID \parallel L\_M\_ID \parallel MAC\ (K_{Xm}, ALERT \| P\_ID \parallel L\_M\_ID) \quad (6)$$

Alert message sending node selects one of its parent nodes and adds this information to the ALERT message. P_ID indicates the ID of the prosecuting node that creates the ALERT message. L_M_ID indicates the ID of a lost message. The first check node that receives ALERT messages transmits the ALARM message using the fallback path to report the damage that occurred in the main path. The ALARM message has the following form:

$$RInfo \parallel ALARM \parallel P\_ID\_list \parallel lost\_payload \parallel MAC\ (K_{Xm}, ALARM \| P\_ID\_list \| lost\_payload) \quad (7)$$

Figure 5 illustrates the abnormal data transmission process.

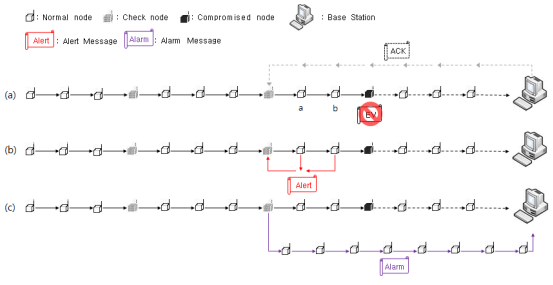

Figure 5 Abnormal data transmission process

3) Re-construction phase

In this phase, the network topology and routing path is re-constructed. However, initial construction phase do not have to be repeated, since BS obtains the path and node information in the sensing data transmission phase. More specifically, ALERT and ALARM messages offer the information necessary to update the path and network topology information. BS selects a path and modifies the topology and routing tables. Figure 6 shows the routing information update in BS.

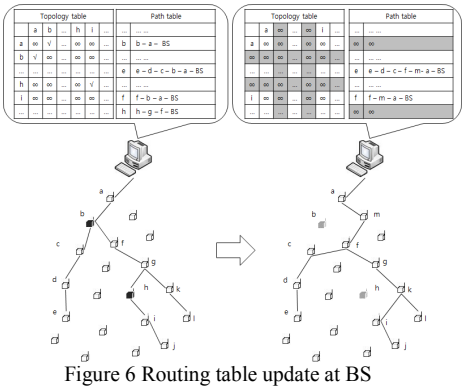

Figure 6 Routing table update at BS

IV. EXPERIMENTAL RESULTS

We compare the energy efficiency of the original method, that is a combination of INSENS and CHEMAS, and the proposed method. The environment assumed is as follows. Total 504 sensor nodes are distributed in a 1,000 m × 1,000 m network. Each node consumes 16.25/12.5μJ for transmitting/receiving a byte, and consumes 75μJ for generating a MAC [8]. Figure 7 shows the number of messages that are communicated during the initial construction and reconstruction phase.

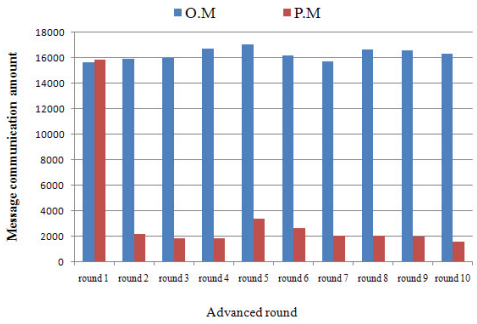

Figure 7 Communication overhead in initial construction and reconstruction phase

In the initial construction phase, the two methods show similar energy consumption. However, from the 2nd round, proposed method (PM) consumes far less energy than the original method (OM) since the proposed method perform re-construction of topology and routing path based on the information obtained in the sensing data transmission phase, whereas the original method repeat the initial construction phase to re-construct the topology and routing paths at each round.

V. CONCLUSIONS

In this paper, we proposed an energy efficient routing method in an environment where both intrusion detection and prevention schemes are used in WSNs. In WSNs, multiple attacks may occur alternatively or simultaneously, and we cannot predict which attack will occur next. Therefore, we need both intrusion detection and prevention schemes. We proposed an energy efficient routing method for the environment where both intrusion detection and prevention schemes are used. We also confirmed through experiments that the proposed method reduces the communication overhead and energy consumption compared to combination of existing methods.

ACKNOWLEDGMENT

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. 2013R1A2A2A01013971)

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," Communications magazine, IEEE, vol.40, no.8, pp.102-114.
[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad hoc networks, vol.1, no.2, pp.293-315.
[3] Y. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks,"INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, pp.1976-1986.
[4] I. Khalil, S. Bagchi, and N. B. Shroff, "LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks,"Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, pp.612-621.
[5] J. R. Douceur, "The sybil attack," in Peer-to-peer SystemsAnonymous , pp.251-260, Springer, 2002.
[6] B. Xiao, B. Yu, and C. Gao, "CHEMAS: Identify suspect nodes in selective forwarding attacks," Journal of Parallel and Distributed Computing, vol.67, no.11, pp.1218-1230, 2007.
[7] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," Comput.Commun., vol.29, no.2, pp.216-230, 2006.
[8] Fan Ye, Haiyun Luo, Songwu Lu, and Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," IEEE Journal on Selected Areas in Communications, vol.23, no.4, pp.839-850, 2005.