A Security Method for Multiple Attacks in Sensor Networks: Against the False Report Injection Attack and the Sinkhole Attack

Su Man Nam[1]and Tae Ho Cho[2]

[1,2]College of Information and Communication Engineering, Sungkyunkwan University
Suwon, 440-746, Republic of Korea

ABSTRACT

In a large scale wireless sensor network, various attacks rapidly spread damages in the network from inside and outside attacks such as the false report injection attack and the sinkhole attack, respectively. These attacks drain finite energy resources and devastate constructed routing paths via compromised nodes. The security methods like SEF (statistical en-route filtering scheme) and LEAP (localized encryption and authentication protocol) try to cope with these attacks. When these attacks occur at the same time, SEF and LEAP should be operated simultaneously in the sensor network thus, it introduces some inefficiency. In this paper, we propose a security method which improves the energy efficiency while maintaining the security level compared to the simultaneous application of SEF and LEAP. The proposed method is designed by identifying and eliminating the redundancies within the simultaneous application of the two methods and providing more efficient functionalities. In the proposed method, two types of new keys are designed and provided for simultaneous detection of the attacks. Four types of keys are used in each sensor node – a P1 for encrypting information, a PK (pairwise key) for keeping secure paths, a P2 for verifying a specific cluster, and a GK (group key) for encrypting message. Among these keys, P1 and P2 are newly provided keys. We have evaluated the effectiveness of the proposed method compared to the simultaneous application of SEF and LEAP when the multiple attacks occur. The experiment results show that our proposed method saves energy up to 10% while maintaining the detection power.

KEYWORDS

Wireless sensor network, a statistical en-route filtering scheme, a localized encryption and authentication protocol, multiple attacks countermeasure

1. INTRODUCTION

Wireless sensor networks (WSNs) provide economically viable technologies for a variety of applications [1]. The sensor network enables the development of low-cost, low-power, and multi-functional sensor [2-3]. WSN is composed of a large number of sensor nodes and a base station. The nodes densely spread in open environments without an infrastructure and it observes a given physical event. The base station collects their sensor readings [4]. The sensors have a high disadvantage of being captured and compromised due to the limited capabilities of the sensor nodes in terms of computation, communication, storage, and energy supply [5-6]. In addition, they are defenseless to various offense patterns from malicious attackers. For a large-scale sensor network, it is impractical to observe and detect each individual node from physical or logical attack.

X. Du et al. [7-8] presented that the attacks on sensor networks supervenes on application, transportation, link (medium access control), or physical layers. The attacks are also categorized

DOI : 10.5121/ijit.2014.2402

based on the capability of the attackers, such as laptop-level and sensor-level. A powerful laptop-level adversary influences more harm of power supply than the sensor level. In addition, the attacks are separately classified into outside and inside attacks. An outside attacker has no access to most of the cryptographic materials such as sinkhole, sybil, selective forwarding, wormhole, HELLO flood attacks occurred usually on the network layer, whereas an inside attack has imperfect key materials such as false report inject, false MAC injection attacks that occurred usually on the application layer[9-16].

We choose both the sinkhole attack of the outside attack and the false report injection attack of the inside attack which frequently occur in the sensor network among multiple attacks. As shown in Fig. 1, an adversary uses two attack nodes (a compromised node (Fig. 1-(a)) and an adversary node (Fig. 1-(b)) to launch a false report injection and false routing control message (RCM; RCM is HELLO message). The adversary injects false report into the network through the compromised node with the goal of deceiving the base station or depleting the limited energy resource [6]. It devastates constructed routing paths through the adversary node with a gain of report information in the network. To minimize the damage of energy consumption, false reports and false RCMs should be detected as early as possible in the sensor network.

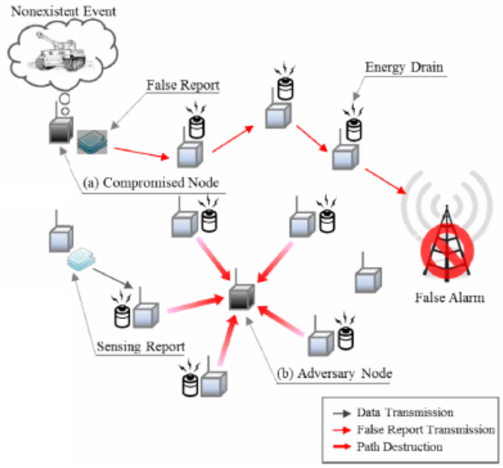


Figure 1.Multiple attacks: the false report injection attack and the sinkhole attacks

Ye et al.[9] proposed a statistical en-route filtering scheme (SEF) to filter out forged reports during the forwarding process into the base station. In the scheme, multiple sensing nodes collaboratively generate a sensing report which consists of multiple message authentication codes (MACs) of its neighboring nodes using its symmetric keys. As a report passes through multiple hops into the base station, each forwarding node along a way probabilistically authenticates the correctness of the MACs and drops those with bogus MACs in the report. Consequently, SEF uses to drop false reports through collective decision-making by using multiple detecting nodes and collective false detection by using multiple forwarding nodes.

Zhu et al. [11] proposed a localized encryption and authentication protocol (LEAP), a key management protocol for sensor networks. In the protocol, different types of messages exchanged between the sensor nodes have different security demands, and the use of a single-key method is inappropriate to communicate these different security requirements. Hence, LEAP establishes four types of keys for each sensor: an individual key shared with the base station, a pairwise key shared with another node, a cluster key shared with its neighboring nodes, and a group key that is shared by all nodes in the network [17-18].

When two attacks occur at the same time, SEF and LEAP should be operated simultaneously in the sensor network. As shown in Fig. 1, the attacks cause serious damage to the network at same time. In fact, instead of a variety of security schemes the network should be effectively managed as a node has limited energy and computation. In this paper, we will present a security method which improves the energy efficiency while maintaining the detection power. Our method detects false MAC and false RCM through the four keys while keeping the security level instead of the various keys of SEF and LEAP. Thus, we decrease the amount of communications and the energy consumptions of each node in the network.

The rest of this paper is organized as follows. Section 2 briefly describes the statistical en-route filtering and localized encryption and authentication protocol as general background knowledge. Section 3 explains assumptions and design goals of our scheme. Section 4 introduces our proposed method, and Section 5 presents the optimizations results. We discuss the related work in Section 6. Finally, conclusions and future work are discussed in Section 7.

2. BACKGROUND

2.1. A. Statistical En-route Filtering (SEF)

Ye et al.[9] proposed a detection scheme called SEF, which statistically distinguishes false report using the stored keys of each node. In SEF, there is a pregenerated global key pool, divided into n non-overlapping partitions, and each partition has m keys (Ks). The base station manages the global pool. Before a node is deployed, the node randomly stores an n partition (PID) and numerous Ks from the global key.

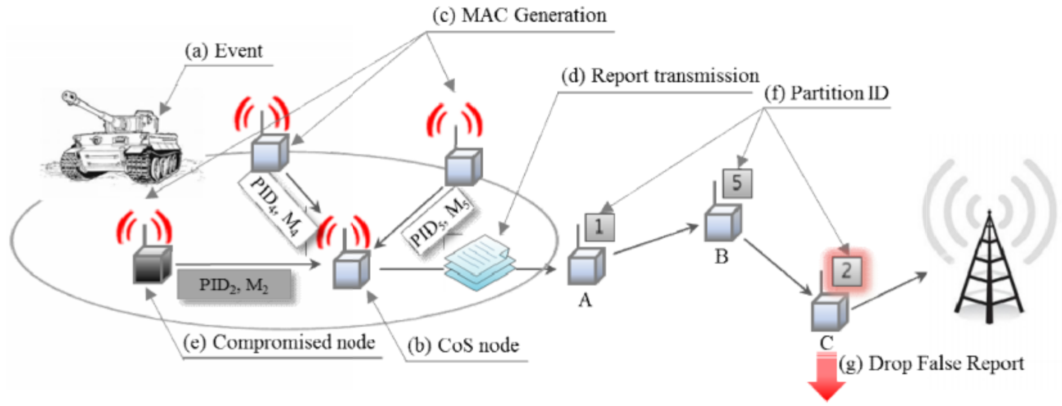


Figure 2.Filtering out a false report

Fig. 2 shows an example of a generated report and dropped report. When a real event throughout an area (Fig. 2-(a)), a center-of-stimulus (CoS) node (Fig. 2-(b)) is detected to generate the event report. After the election process finishes, neighbors of the CoS node detect the event randomly by selecting Ki, one of its Ks, and then the node sends its PID and message authentication codes (MACs) to the CoS node (Fig. 2-(c)). A MAC is as follows (// denotes stream concatenation):

$$M_i = \overline{MAC}(K_i, L_E \,\square\, \mathrm{t} \,\square\, \mathrm{E})$$

The MAC includes that L_E is the location of the event, t is the time of detection, and E is the type of event. After collecting MACs, the CoS node chooses MACs of *T* categories except the duplication of PIDs (*T* is predefined), and attaches them to the report (Fig. 2-(d)). The final report format is in the following form:

$$\{L_E, \mathrm{t}, \mathrm{E}, PID_1, M_{i1}, PID_2, M_{i2}, \ldots, PID_T, M_{iT}\}$$

As shown in Fig. 2, Fig. 2-(e) is a compromised node. The compromised node has no keys but generates a bogus MAC using a fake PID and fake Ks. The CoS node collects MACs from its neighbors and makes a report. The report is sent out toward the base station via multiple hops of Nodes A, B and C (Fig. 2-(f)). The report passes Node A as PID of the node is different from PIDs of the report. While passing on Node B, M5 of the report is verified with PID5 of the node, and the report passes the node as PID5 of the report is from a regular MAC. On the other hand, Node C drops the report because PID2 of the node compares it with a bogus M2 of the report (Fig. 2-(g)). If the report is regular, the report will continually transmit via intermediate nodes into the base station. Therefore, SEF statistically decides the detection of a false report and it is important for en-route filtering out the false report within intermediate nodes.

2.2. Localized Encryption and Authentication Protocol (LEAP)

Zhu et al.[11]proposed a key management protocol in the sensor network called LEAP. This observes the different types of messages that are exchanged between the security requirements for providing confidentiality and authentication. It is necessary to require authentication for all types of packets: control, data, broadcast, unicast, and so on. It is also important to maintain confidentiality for the transmission of event reports and RCMs between a node and the base station or a node and another node. LEAP supports four types of keys for the establishment:

- Individual Key (IK) Every node has a unique key for secure communication between the node and the base station. The key functions two cases for providing confidentiality. First, a node makes encryption of MACs using its IK. Second, a node transmits an alert message using its IK to the base station if it detects any abnormal or unexpected behavior of its neighbors.

- Pairwise Key (PK) Every node shares the key between a node and its immediate neighbor (i.e. one-hop neighbors). Before leaving a report or message in a node, the node always verifies the condition of its neighbor using the PK. The node then sends the event report or message to the neighbor. If a malicious attacker inserts a node in the sensor network without a PK, the adversary node captures a report or message while passing the node. That is, a node and one of its neighbors confirm their PK while sending data, for use of PKs precludes passive participation.

- Cluster Key (CK) Nodes within a cluster region shares a CK, and the CK is used for verifying locally broadcast message such as RCM or securing sensor message to prevent passive participation. Detecting a false RCM is important for saving energy consumption in the sensor network as the false RCM ruins the routing paths of the network [21-23]. The key usually has two functions for verifying the neighbors of a cluster. First, when an event occurred in an area of the network, the surrounding sensor nodes transmit information of the same event to a CoS node. Then, the CoS node removes the information of different CK which a node overhears from an event in another area. Second, a node decrypts or verifies some classes of message such as the RCM or securing sensor message. For example, if an adversary node, which is inserted by an attacker in the sensor network, forwards RCM to its neighbors without a CK, destination nodes authenticate the message through their CK.

- Group Key (GK) Every node and the base station own a group key for encrypting and decrypting messages that are broadcast to the entire group. For example, if a new node sends RCM using its GK to its neighbors, the neighbors authenticate the RCM through their GK, and the nodes reply using ACK message. If a false RCM is detected then, no ACK message will be transmitted.

3.ASSUMPTIONS AND DESIGN GOAL

3.1. Assumptions

We assume a static sensor network (i.e. the topology of the network is fixed), and the sensor nodes are immobile. The sensor network composes a base station and a large number of small sensor nodes, e.g. the Berkeley MICA2 motes [19], the topology establishes the initial paths through directed diffusion [20] and minimum cost forwarding algorithms [21].

We used sensor medium access control (S-MAC) to reduce contention latency for applications of the sensor network. The S-MAC applies message passing according to RTS and CTS between a sender node and a receiver node in motes.

It is further assumed that each node chooses a routing path based on the cost which is a distance from the base station to itself. In addition, every node forwards packets by upstream (toward the base station) along their path. An adversary launches a false report inject attack using compromised nodes and a sinkhole attack using an adversary node at the same time. The false report flows into the base station, and the adversary node is inserted into a central cluster area to be damaged through false RCMs. The issues of other security attacks are out of scope of this paper.

3.2. Design Goal

We implement RC5 block cipher[9]in Mica2 and use them for MAC generation. Based on the battery voltage (3V) and data rate (19.2kb/s), each sensor node takes $\boldsymbol{e_t} = \mathbf{16.25}\mu\boldsymbol{J}$ per byte when receiving, $\boldsymbol{e_r} = \mathbf{12.5}\mu\boldsymbol{J}$ per byte while transmitting, and$\boldsymbol{e_m} = \mathbf{15}\mu\boldsymbol{J}$ per byte while generating MAC [22-23]. Energy consumption of a node is defined as follows:

$$E_C(n_i) = e_t + e_r + e_m$$

Where E_C is the total energy consumption of a node, n_i is the node identifier, e_t is the quantity of the transmitted energy, e_r is the quantity of the received energy, and e_m is the quantity of energy generated by MAC.

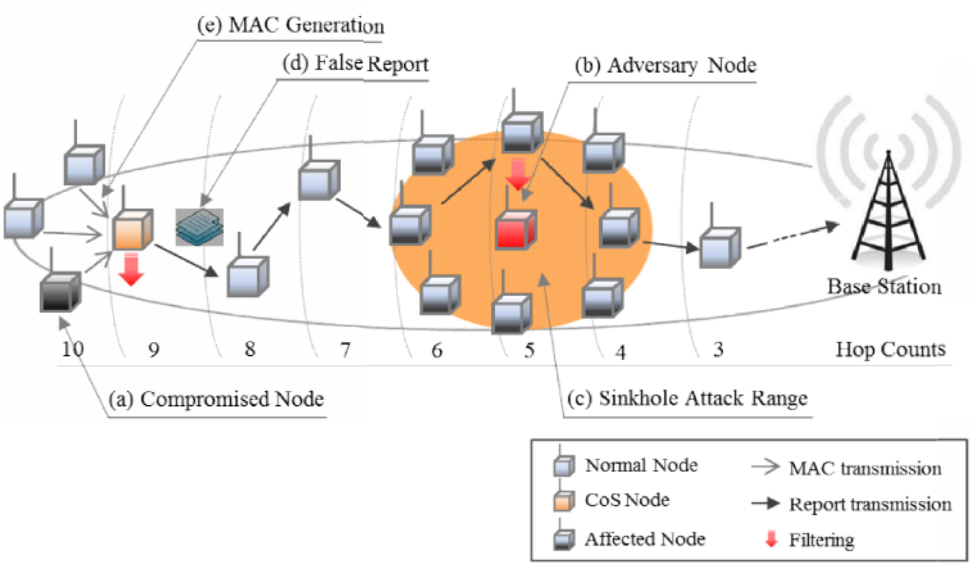


Figure 3.The design of a path including two attacks

We designed two cases of a path for calculating energy consumption as in Fig. 3. One case possesses the simultaneous application of SEF and LEAP, and the other case is our proposed method. Both of them composed of 10 hop counts including the false report injection attack and the sinkhole attack. That is, two cases of the path exist separately from these attacks. A compromised node (Fig. 3-(a)) on 10 hops generates a forged MAC such as the false report injection attack, and an adversary node on 5 hops (Fig. 3-(b)) transmits false RCM to eight affected nodes (Fig. 3-(c)) such as the sinkhole attack. We assume that the size of the report is 12 bytes (original report size is 24 bytes), the size of MAC and RCM is one byte. We simply generated 100 rounds with these attacks on the path: a false report (Fig. 3-(d)) including generated MACs (Fig. 3-(e)) that were sent out sequentially, whereas the false RCM is transmitted two times among the 100 rounds because the sinkhole attack is a discontinuity task. In the simultaneous application of the two methods, the false reports are filtered by PID and Ks of SEF on the node of 5 hops, and the false RCM are dropped by their CK and GK on the affected nodes. On the other hand, in our proposed method, the false reports are filtered out by a P2 on a node of 9 hops more than the simultaneous application of SEF and LEAP, and false dropped RCM of our method is almost the same quantity as the simultaneous application of the two methods.

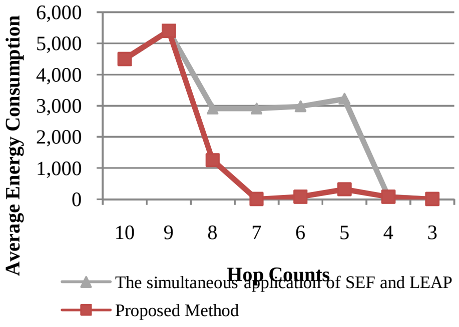


Figure 4Energy condition of a path.

Fig. 4 shows the average energy consumption for two methods which are the simultaneous application of two methods and the proposed method. Nodes on 10 and 9 hops have the same energy consumption because the MAC and report are equally generated, whereas a gap between 5 and 8 hops is large. In other words, energy consumption of the proposed method is better than the simultaneous application of the two methods. In the proposed method, a CoS node on 9 hops drops all of the forged MACs that occurred by the compromised node of 10 hops because of using a fake key; On the other hand, the false reports affect the energy consumption of all nodes of 6, 7, and 8 hops in the simultaneous application of SEF and LEAP as PIDs of the report and the nodes are mutually different. Therefore, our proposed method saves energy resource of each node more than the simultaneous application of two methods as the travel of the false reports decreases. In the next section, we will further discuss our proposed method with four types of keys and how to conserve energy consumed by each node against the multiple attacks at the same time.

4. PROPOSED METHOD

4.1. Overview

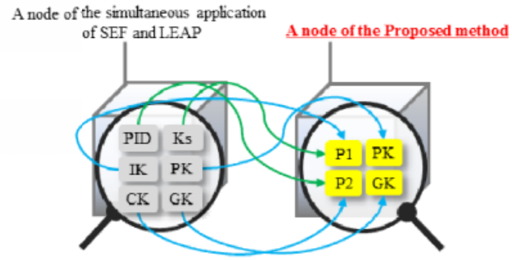

A node of the simultaneous application of SEF and LEAP
A node of the Proposed method
PID
Ks
IK
PK
CK
GK
P1
PK
P2
GK

Figure 5.Keys Type of the proposed method

Various attacks rapidly spread damages to the network with the false report injection attack and the sinkhole attack. When these attacks occur at the same time, SEF and LEAP should be operated simultaneously to cope with these attacks in the sensor network. To effectively detect these attacks in the sensor network, we propose a security method which conserves the energy consumption while maintaining the detection power as it is impossible to work on a diversity of countermeasures with limited resources at each node. We provide reduction in the energy consumption of each node by keeping the security level through our method against these attacks at the same time. In this paper, our method aims at achieving the following goals.

- Detection of the false report injection attack: We use P1 and P2 to filter out false reports that occur on the application layer for detecting this attack. P1 combines Ks with IK to encrypt event information, and P2 combines PID of SEF with CK of LEAP to en-route drop the false report. Thus, the proposed method reduces a quantity of false reports that occur from the compromised node by P1 and P2 on the CoS node.

- Detection of the sinkhole attack: The proposed method verifies RCM that occur on the network layer by P2 and GK instead of CK and GK of LEAP. Our method maintains the same security level of the simultaneous application of two methods for detecting false RCM.

- Conservation of energy consumption: Our method uses four types of keys less than the simultaneous application of SEF and LEAP – P1 for encrypting data, PK for securing communications, P2 for identifying a cluster, GK for verifying RCM. The proposed method reduces the energy consumptions of each node because it uses a few communications between nodes more than multiple keys of the simultaneous application of two methods in the sensor network.

Fig. 5 shows four keys of our proposed method from six keys of the simultaneous application of two methods in a node. P1 is designed from Ks and IK as two keys are alike in functions for MACs encryption. P2 is designed for achieving the detection of false report and false RCM instead of PID and CK. We expect legal multiple countermeasures through our proposed method against the multiple attacks to reduce energy consumption of each node in the sensor network.

4.2. Functions of Proposed Keys

Our proposed method supports the establishment of four types of keys for each sensor node – a proposed key 1 (P1) shared with the base station, a pairwise key shared with another node, proposed key 2 (P2) shared with multiple neighbouring nodes, and a GK with whole sensor nodes in the network. Before a sensor node is deployed, the node stores a P1 and GK received from the base station, and then the node generates PK and P2 by its neighbours that are similar the establishment of four keys in LEAP as soon as the nodes are deployed in the sensor field. We now discuss the P1 and P2 without PK and GK that are the keys of LEAP as we stated in Section 2.B.

P1 provides three functions:

- Each node owns a P1, and the base station manages all P1s of each sensor nodes.
- An event sensing node uses its P1 to encrypt MACs and decrypt the MACs in the base station as the base station has all the P1s of each node.
- A node sends alert information with encryption to the base station when it observes abnormal or unexpected behaviour of a neighbouring node.

P2 provides three functions:

- All sensor nodes within a cluster share the same P2 for decrypting or verifying messages.
- A CoS node suppresses MACs of another cluster area when a real event occurs in the sensor field.
- Every node prevents false RCM occurred by passive participation.

We propose the detection of multiple attacks through our method by keeping the security level in the network. The P1 is useful for secure communication between the node and the base station. The P2 is effective for detecting a fake MAC and false RCM instead of the functions of SEF and LEAP as this key is shared between a node and all its neighbors. Furthermore, P2 generally filters out the false MAC occurring from a compromised node within one or two hops and false RCM that occur from an adversary node through our proposed method. P1 and P2 give the effect of defending the two attacks to the network, and we will discuss more on the capability of P1 and P2 in the next subsection.

4.3.Filtering out a false report by Keys P1 and P2

Similar to [9][10], a sensed node (N_s), which is a neighbor of a CoS node, generate a MAC (M_{NS}) after real events occur. A sensed node prepares its $P2_{NS}$ and a MAC including $P1_{NS}$ and event information Then, the sensed node transmits them to the CoS node (N_C). The CoS node collects MACs from its neighbors, it verifies their $P2_{NS}$ and makes a report to notify the event to the base station. A process of the MAC is,

N_S □ Event Sensing.
$N_S \rightarrow N_C : P2_{N_S}, M_{N_S}$
$= \overline{MAC}(P1_{N_S}, L_E$ □ t □ E$)$
N_C □ $P2_{N_S}\, Verification$

Fig. 6 shows an example of MACs transmission between a CoS node and its neighbors with forged MACs. Three nodes including a compromised node are in the same cluster region with the CoS node, and the other is in a different cluster. It means that the two normal nodes own same $P2_1$, while the other node has $P2_2$ (Fig. 6-(e)). When an event occurs in an area of $P2_1$ in the sensor network, neighbors of the CoS node transmit each $P2_i$ and MAC M_i to the CoS node. After receiving the all the MACs, the CoS filters out fake $P2_F$ and $P2_2$ (Fig. 6-(d)) as $P2_F$ is a forged key and $P2_2$ overhears the event in the other area. Through authentication of the P2, the all the bogus MACs are filtered out in the CoS node earlier than the SEF scheme. That is, our proposed method improves detection power of the false report injection attack through the P2. We expect newly provided P1 and P2 to detect the false report injection attack for conserving the energy consumption of each node.

4.4.Inside and Outside Attacks Detection

In this paper, we focus on the energy efficiency against multiple attacks (the false report injection attack and the sinkhole attack). These attacks can easily arise through an attacker in the network at the same time. To usually transmit the false report and the false RCM, a malicious adversary should make the fabrication of keys for communication between the nodes. If these attacks occurred without any security protocol then, the compromised nodes ruin the lifetime and routing path of each node in the network. We will describe the capability of our scheme for defending against these malicious attacks.

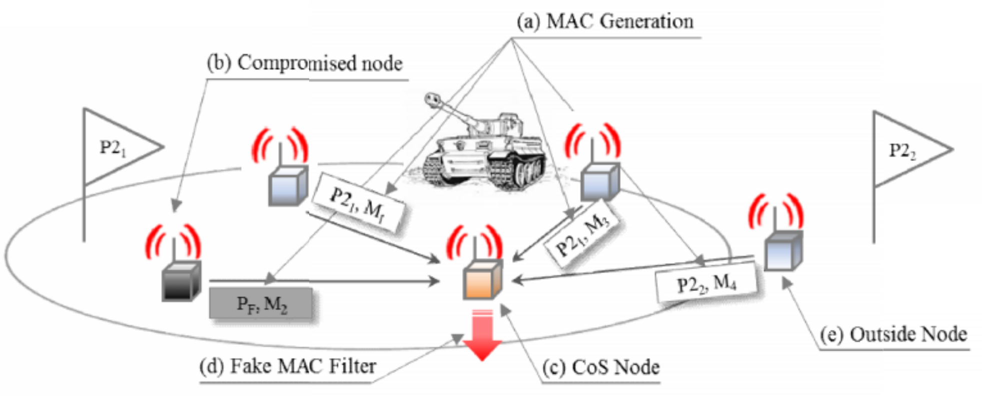


Figure 6.Forged MAC detection by P2

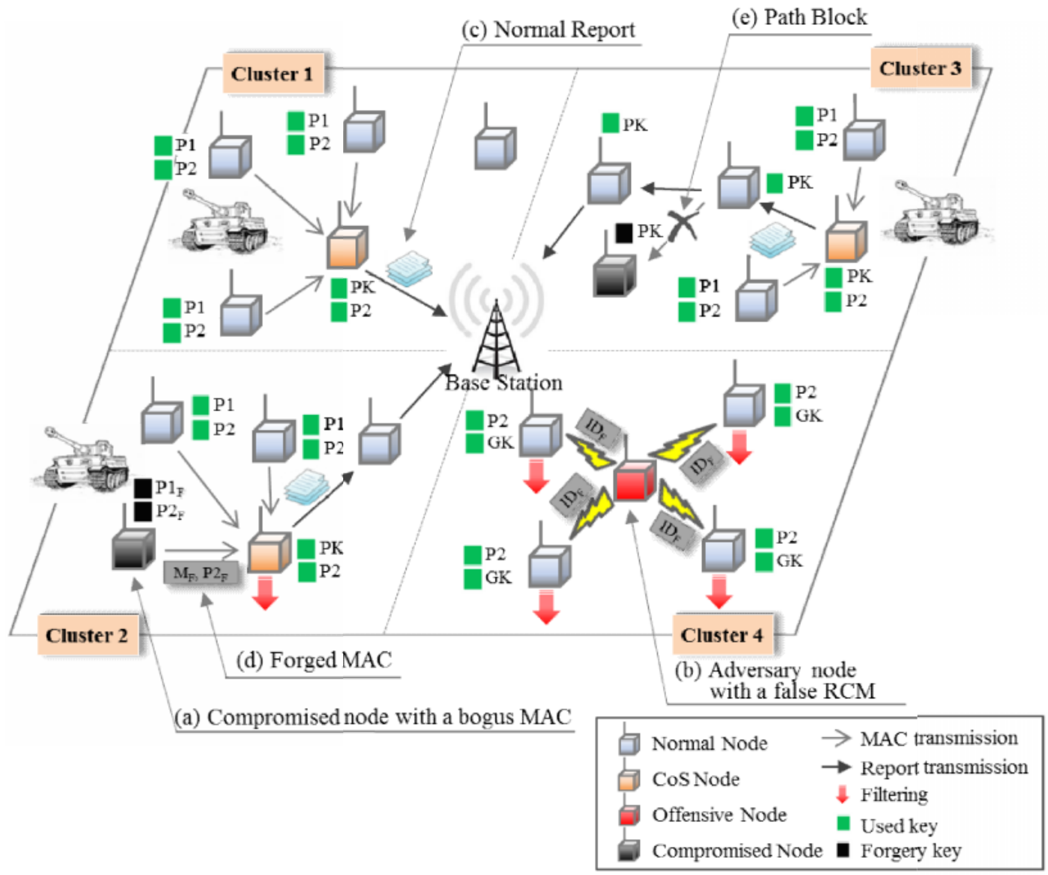
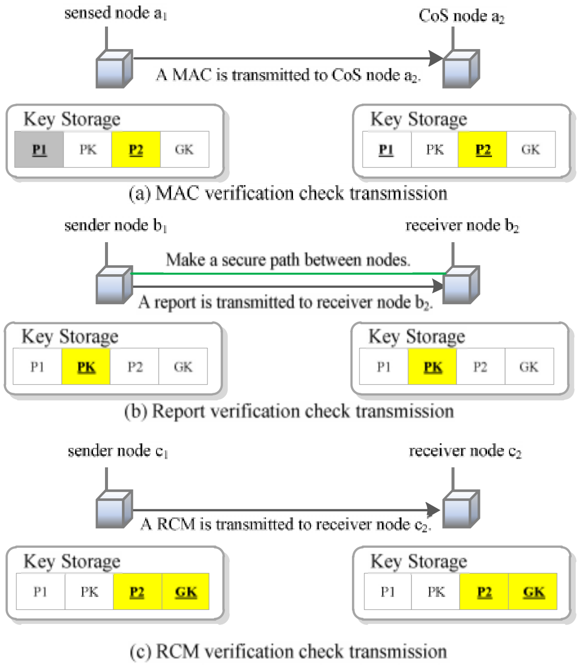


Figure 7.Target system model

Figure 7 illustrates a target system of our proposed method to detect multiple attacks in a sensor network. The sensor network is composed of a sensor field and a middle base station. In addition, there are four region, nodes including four keys on each region, and the two generated attacks which the false report injection attack (Figure 7-(a)) and the sinkhole attack (Figure 7-(b)). The sensor field includes four divided clusters and each node has each P1, PK, P2, and GK. In Cluster 1, a report occurs from a CoS node through legitimate MACs with each fair P1, P2, and PK. On the other hand, Clusters 2, 3, and 4 generate these attacks from the compromised nodes in the network (Figure 7-(c)). In Cluster 2, a compromised node (Figure 7-(a)) makes a forged MAC (Figure 7-(d)) including a P2F to inject a false report in the network after sensing an event such as a false report injection attack. While collecting MACs from its neighbors, a CoS node on Cluster 2 drops the forged MAC through its legitimate P2. A report then, goes toward the base station after the CoS node generate the report. The CoS node provides early detection power through P2 against forged MACs that occurred due to the compromised node. In Cluster 3, an adversary node is inserted by an adversary with no keys to intercept and it removes event information such as the sinkhole attack. After generating a report from a CoS node, nodes verify their PK to detect the fake node while travelling via multiple hops. If an intermediate node detects the compromised node before transmitting data by its PK (Figure 7-(e)), the node makes a detour to another path. While transmitting the legitimate report into the base station, each node communicates with only authorized nodes including the PK for the discovery of the adversary node. In Cluster 4, an adversary node (Figure 7-(b)) tries to forward false RCM including its node ID for threat of its neighbors such as a sinkhole attack. The sinkhole attack seriously damages and affects the neighboring nodes through false RCM without keys. After receiving the false RCM, the neighbors detect and drop the false RCM through their P2 and GK, and then the nodes transmit no ACK message. The nodes detect the false RCM through P2 and GK. Our proposed method provides simultaneous detection of these attacks using these keys. We will further describe and verify each key between a node and another node in the next section.

4.5.Secure Communications



(a) MAC verification check transmission

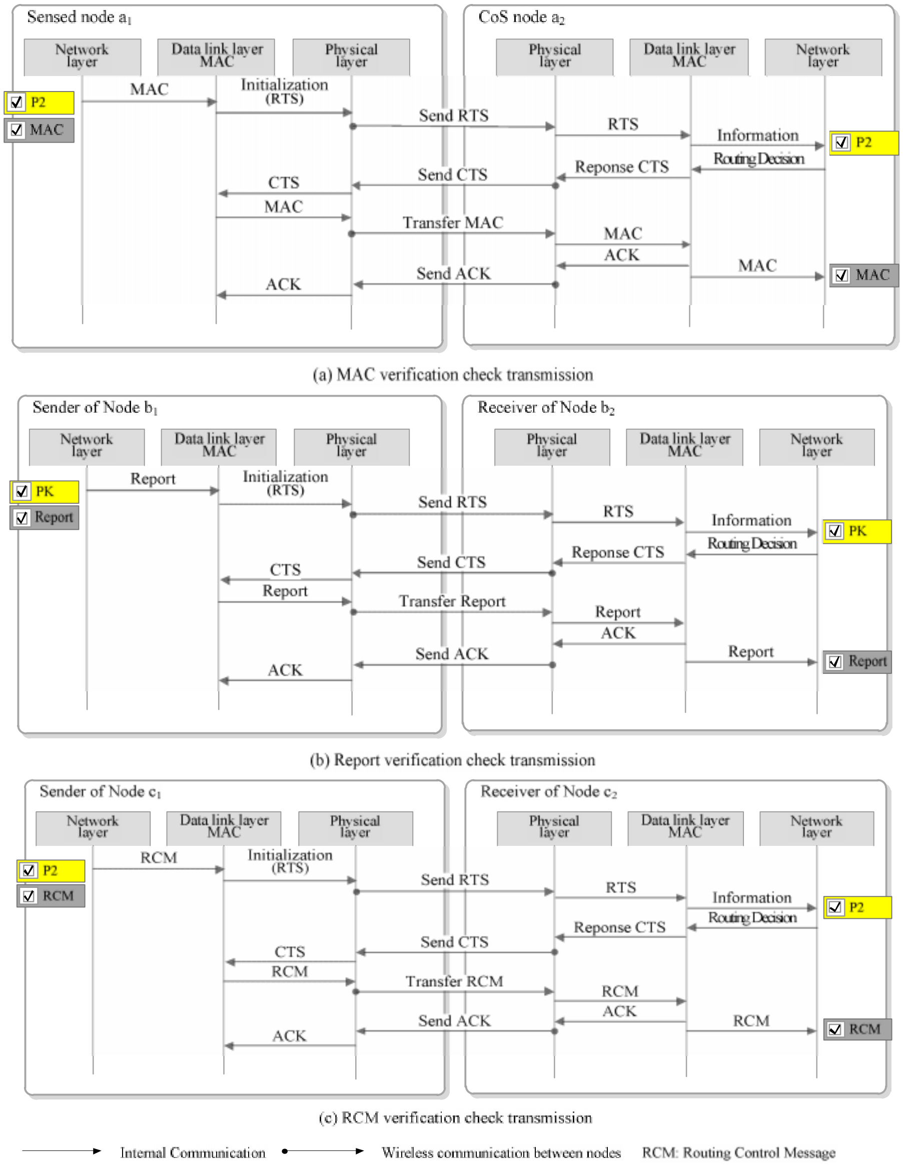
(b) Report verification check transmission

(c) RCM verification check transmission

Figure 8.Key verification between two nodes

There are three cases of verification to detect the false report injection attacks and the sinkhole attack in Figure 8. As we stated in Section 2.B, each key functions as a central role for decrypting, verifying, or securing communication. In Figure 8-(a), a sensed node a1 submits its P2 and MAC including its P1 to a CoS node a2 as sensing an event in an area of a sensor field. The sensed node a1 uses its P1 for decryption of the MAC and its P2 for verification of a cluster before transmitting such as Cluster 2 shown in Figure 7. The CoS node authenticates the P2 of the sensed node a1 through the P2 of the CoS node b2 for a normal or forged MAC, and the node generates a report. The CoS node detects a forged MAC through its P2 as received from the sensed node a1. In Figure 8-(b), PKs are used for maintaining a secure path between a node and its neighboring node. Before transmitting a report, the sender node b1 identifies condition of its receiver node b2 as an adversary node inserted by the attacker which has no keys such as the Cluster 3 shown in Figure 7. This operation achieves secure paths until arriving in the base station. The sender node b1 submits a report to the permitted receiver node b2 after verifying mutual P2. In Figure 8-(c), the RCM uses P2 and GK for changing routing path. When a receiver node c2 receives the RCM, the receiver node c2 verifies P2 of the sender node c1 for same region and decrypts the message through its GK such as Cluster 4 shown in Figure 7. These keys detect false RCM occurred from the adversary node such as the sinkhole attack. Four keys of the proposed method authenticate all report including MACs and RCMs against the multiple attacks, such as the false injection report attack and the sinkhole attack. As a result, our proposed method detects multiple attacks at the same time and maintains secure paths of the network. Furthermore, a network using the method saves energy consumption of each node. Next, we will express more communications ofthe internal nodes using S-MAC and on how to verify the keys and transmit data including reports between a sensed node and a CoS node, or a sender node and a receiver node.

4.6.Key Use inside Node



(a) MAC verification check transmission

(b) Report verification check transmission

(c) RCM verification check transmission

Figure 9.Key verification between two nodes

We mainly defined three cases when a sender node broadcasts a MAC, a report, and a RCM to a receiver node in Figure 9. In Figure 9-(a), before sending a MAC to the sensed node a_2, two nodes preferentially communicate through RTS and CTS in order to authenticate P2 of the two nodes. Next, the sensed node a_1 transmits an encrypted MAC using its P1 to the CoS node a_2.The CoS node then collects MACs from its neighbors, and it generates a report for transmission toward the base station.On the other hand, if a fake P2 fails in authentication between the sender node and receiver node, the receiver node a_2 transmits no CTS, and the sender node a_1 is also unable to transmit a MAC. The P2 of the CoS node a_2 authenticates the P2 of the sensed node a_1 through RTS to detect forged MACs such as shown in Figure 8-(a). In Figure 9-(b), the PK is used for maintaining secure communications such as shown in Figure 8-(b). For example, if an attacker inserts a malicious node with the purpose of the sinkhole attack without keys in the sensor network, a sender node b_2 measures the attack node through its PK, and then the sender node blocks an inflow of the report. That is, while transmitting RTS with the PK, the PKs of the sender node and the receiver node are confirmed in the receiver node b_2. After verifying the PKs through RTS, the receiver node b_2 sends CTS to the sender node b_1. The sender node b_1 then transmits a report including MACs into the base station. If two PKs are different then, the sinkhole attack of the adversary node is recognized and a detour of the routing path is found. The PK usually maintains secure paths between two nodes while transmitting the report. In Figure 9-(c), the sender node c_1 forwards a RCM to the receiver node c_2 such as Figure 8-(c). In this case the receiver verifies RTS of the sender node c_1 including a P2. After verifying P2, the sender node c_1 transmit an encrypted RCM using GK. If the keys fail for the authentication then, the receiver node c_2 is aware of false RCM. The receiver node c_2 notices the behavior of its neighbor using P1 of the receiver node c_2 to the base station [23]. P2 verifies the sender node c_1, and GK authenticates the encrypted RCM that occurred from the receiver node c_1. Figure 9-(a) shows how to detect the bogus MAC against the false report injection attack, Figure 9-(b) shows how to keep a secure path against the sinkhole attack, and Figure 9-(c) shows how to detect the false RCM against the sinkhole attack. Overall, we provide simultaneous detection of multiple attacks through four types of keys in each sensor node.

5. SIMULATION RESULT

A simulation was performed for the proposed method as compared to the simultaneous application of SEF and LEAP. A sensor network of the simulation comprises 500 nodes in the simulation environment, and field size is 500 x 500 m2. The simulation basically uses Ye et al.'s method of energy consumption [9]. Each node takes 16.25 and 12.5 µJ to transmit and receive a byte, each MAC generation consumes 15 µJ a byte. The size of a report is 24 bytes, and the size of a MAC is 1 byte. In addition, the size of a RCM (HELLO message) is 2 bytes (only include a node ID), and the size of an ACK message is 12 bytes (size of an id is 4 bytes and the MAC size is 8 bytes) [9, 22-23]. The simultaneous application of two methods is 100 keys in the global key pool, which is divided into 10 partitions. We assumed that the compromised nodes are 10 nodes for the false report injection attack and an adversary node is a node for sinkhole attack in the sensor network. In addition, we generated 1,000 events among legitimate reports, RCMs, false reports, and false RCM. In this case, the false report and RCMs occurred separately by the compromised nodes and the adversary node in the sensor network.

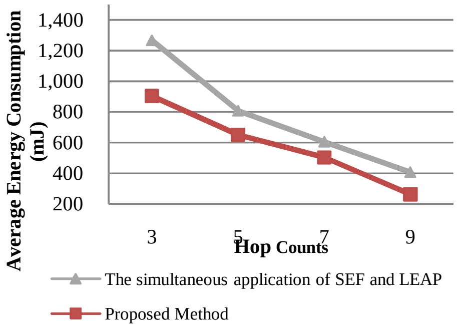


Figure 10. Average energy consumption when generating only false reports

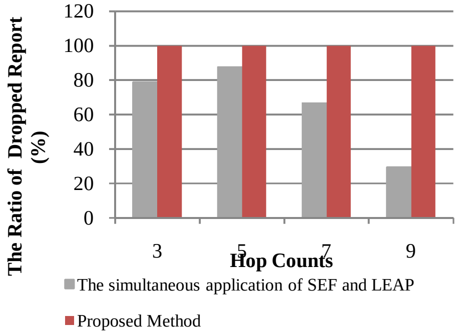


Figure 11.Probability of filtered reports

Figures 10 and 11 illustrate the average energy consumption as generating only a false report and the probability of a filtered report. We are randomly composed of 2% compromised nodes (the compromised nodes are 10 nodes in the network) for generating the false MAC in these figures. As shown in Figure 10, the proposed method detects false MACs through P2s of each CoS node earlier than the simultaneous application of SEF and LEAP. Consequently, a simultaneous application of the two methods consumes greater than about 10% energy of each node as the false reports travel in multi hops in the simultaneous application of the two methods. In addition, Figure 11 shows the probability of the dropped report on 3, 5, 7, and 9 hops. The proposed method is 100% for the filtered false report as the method detects the false MAC through P2. On the other hand, the simultaneous application of SEF and LEAP increasingly filters out the false reports in close hops of the nodes from the base station because PIDs of the report are checked in the nodes. Therefore, the proposed method is more efficient than the simultaneous application of SEF and LEAP against the false report injection attack while maintaining the security level.

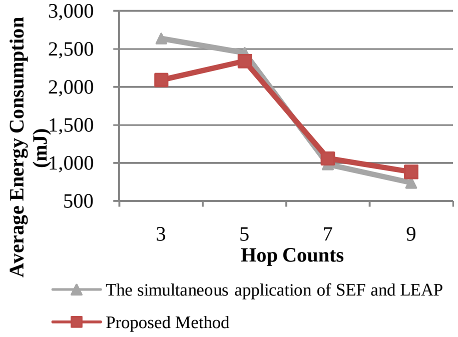


Figure 12.Average energy consumption when generating only a false RCM

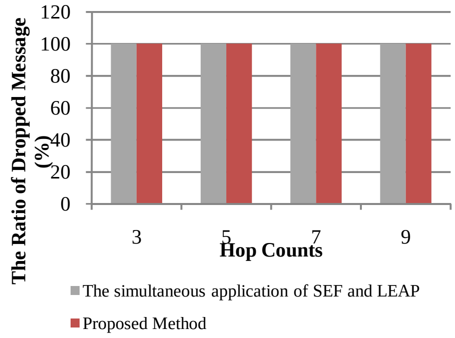


Figure 13.Probability of dropped messages

Figures 12 and 13 illustrate the average energy consumption when generating only a false RCM and the probability of a dropped message. It comprises of a new node for the sinkhole attack on 3, 5, 7, and 9 hops, respectively, and forwarded false RCMs into its neighbors without P2 and GK. The simulation results of the two methods are almost same as the simultaneous application of SEF and LEAP is influenced by CK and GK of LEAP. The proposed method is influenced by P2 and GK while forwarding a RCM. As shows in these figures, the result, we have achieved that the simultaneous application of two methods and the proposed method have the same detection power against the sinkhole attack.

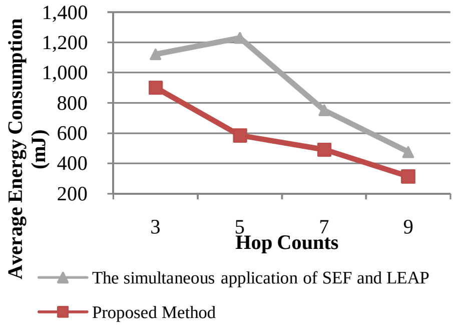


Figure 14.Average energy consumption when generating two attacks at the same time

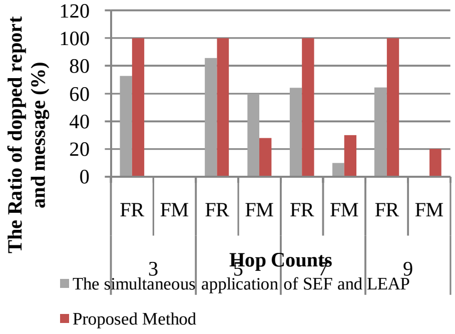


Figure 15.Probability of filtered reports and dropped message at the same time

Figures 14 and 15 illustrate the average energy consumption while generating an inside and outside attack and the probability of a filtered report and dropped message at the same time. It is composed of 2% compromised nodes for generating the false report at random and it forwarded the false RCM on a node of 5 hops. In Figure 14, the combined method occurs about an average 10% of the energy consumption more than the proposed method. FR and FM are false report and false RCM, respectively in Figure 15. The filtered report of the proposed method is higher than about 30%, but the two methods are difference gaps of FM between 5 and 9 hops as the density of the sensor nodes is dissimilar. We will show energy consumption of the two attacks at one time on next figure.

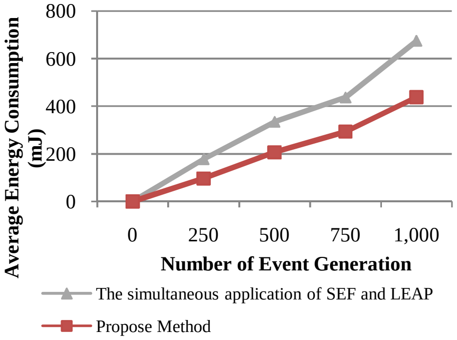


Figure 16.Average energy consumption per event generation

Figure 16 shows the average energy consumption per particular round on the simultaneous application of SEF and LEAP and the proposed method. We simultaneously generated multiple attacks, such as the false report injection attack and the sinkhole attack in the sensor network. A gap between the methods is made by mutual security countermeasures from 250 rounds in the sensor network. When 1,000 rounds occurred, the simultaneous application of two methods consumes more energy about 200 µJ than the proposed method. That is, energy consumption of the proposed method is better than the simultaneous application of SEF and LEAP which is used to detect these in the sensor network at the same time. Therefore, the proposed method saves the energy up to 10% while maintaining the security power as compared to the simultaneous application of two methods.

6. Related Work

The sensor network security has been studied in the recent years with a number of proposals. Yu et al.[24] presented a dynamic en-route filtering scheme based on the SEF scheme for detecting and filtering false data injection by endorsing a legitimate report from multiple sensing nodes using their own authentication keys of one-way hash chains. Zhu et al.[25] proposed an interleaved hop-by-hop authentication (IHA) scheme to guarantee that the base station detects a false report generated from a compromised node. This scheme verifies the report with a pairwise symmetric keys in deterministic and hop-by-hop fashion using a cluster-based organization. Li et al.[10] presented a probabilistic voting-based filtering scheme (PVFS) to detect a false negative attack such the false injection data attack. The scheme combines cluster-based organization, probabilistic key assignment, and voting methods to accomplish protection power against the attack while maintaining a sufficiently high filtering ability. In contrast, our scheme achieves early detection power through P2 between a sensing node and a CoS node as shown in Section 4.A.

Ngaiet al.[16] present a novel algorithm for detecting the intruder in a sinkhole attack. It investigates suspected nodes by checking data consistency and it identifies the intruder by analyzing information of the network. However, as Section 4, our scheme uses multiple keys to efficiently exchange different types of messages between the sensor nodes.

Perriget al.[26] presented security protocols for sensor networks: authenticated and confidential communication, and authenticated broadcast, called SNEP which has SNEP and μTESLA. SNEP provides data confidentiality, two-party data, authentication, and evidence of data freshness. μTESLA includes authenticated broadcast for severely resource-constrained environments. SNEP implements an authenticated routing scheme and a secure node-to-node key agreement protocol. In contrast, our scheme establishes PKs without the involvement of the base station between the sensor nodes such as LEAP.

Polastreet al.[27] showed a Berkeley media access control (B-MAC). This is a reconfigurable carrier sense multiple access (CSMA) protocol that supports a flexible interface to obtain ultra-low power operation, effective collision avoidance, and high channel utilization. Akyildiz et al. [28] presented a spatial correlation-based collaborative medium access control (CC-MAC) which has Event MAC (E-MAC) and Network MAC (N-MAC) components to provide a localized control based on the spatial correlation. Event MAC (E-MAC) filters out the correlation in source records, and Network MAC (N-MAC) prioritizes the transmission of the route-thru packets. CC-MAC accomplishes high performance of energy consumption, packet filtering rate, and waiting time. We used S-MAC to communicate with other nodes and send some control packets as shown in Figure 9. In addition, it reduces energy consumption and supports self-configuration.

7. CONCLUSION AND FUTURE WORK

In WSNs, various inside and outside attacks create serious harms to the sensor network. The inside attack of the sensor level causes false alarms through the injection of forged MACs or forged reports with a partial key on the application layer such as the false report injection attack. The outside attack of the laptop level changes the routing paths of each node to capture and eliminate the event information such as the sinkhole attack. SEF and LEAP are separately proposed to detect these attacks in the sensor network. When these attacks occur at the same time in the network, SEF and LEAP should be operated simultaneously thus, it introduces some inefficiency. In this paper, we propose a security method which improves energy efficiency while keeping the detection power compared to the simultaneous application of SEF and LEAP against these attacks. We use new P1 and P2 with PK and GK of LEAP to efficiently detect multiple attacks. The functions of P1 is to use the MAC and alert information encryption, and the functions of P2 uses RTS verification in a specific cluster, a MAC suppression of another cluster, and the block of false RCM occurred from an adversary node. In addition, our method exchanges RTS, CTS and ACK using four keys through S-MAC between a receiver node and a sender node. As a result, simulation results show that each node of our method significantly increases for energy savings more than the simultaneous application of the two methods. Our method improves energy to about 10% while maintaining the detection power against multiple attacks compared to the simultaneous application of the two methods in the sensor network. As future work, the performance of our method will be compared to the simultaneous application of SEF and LEAP against diversity in inside and outside attacks. We also intend to build in our simulator various scenarios to investigate them. In addition, we apply AI algorithms to obtain further optimal solutions.

ACKNOWLEDGEMENTS

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] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., &Cayirci, E. (2002). A survey on sensor networks.*Communications Magazine, IEEE, 40*(8), 102-114.

[2] Weilian Su, Sankarasubramaniam, Y., &Cayirci, E. (2002). A survey on sensor networks., *40*(8), 102.

[3] Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: a survey.*Wireless Communications, IEEE, 11*(6), 6-28.

[4] Lee, H. Y., & Cho, T. H. (2011). Optimized Fuzzy Adaptive Filtering for Ubiquitous Sensor Networks., *E94.B*, 1648-1656.

[5] Lee, H. Y., & Cho, T. H. (2010). A Scheme for Adaptively Countering Application Layer Security Attacks in Wireless Sensor Networks., *E93.B*(7), 1881-1889.

[6] Lee, H. Y., & Cho, T. H. (2005). Fuzzy Adaptive Selection of Filtering Schemes for Energy Saving in Sensor Networks., *E90-B*(12), 3346-3353.

[7] Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor network., *47*, 53-57.

[8] Chan, H., &Perrig, A. (2003). Security and privacy in sensor networks.*Computer, 36*(10), 103-105.

[9] Ye, F., Luo, H., Lu, S., & Zhang, L. (2004) Statistical en-route filtering of injected false data in sensor networks. *Selected Areas in Communications, IEEE Journal on, 23*(4), 839-850.

[10] Li, F., Srinivasan, A., & Wu, J. (2006). PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks. , *3*(3), 173-182.

[11] S. Zhu, S. Setia, & S. Jajodia.(2004) LEAP: efficient security mechanisms for large-scale distributed sensor networks. , 62-72.

[12] Zhu, S., Setia, S., &Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans.Sen.Netw., 2*(4), 500-528.

[13] B. Xiao, B. Yu, & C. Gao. (2007). CHEMAS: Identify suspect nodes in selective forwarding attacks. , *67*(11), 1218-1230.

[14] Jing Deng, Richard Han, &Shivakant Mishra. (2006). INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks. , *29*(2), 216-230.

[15] Ngai, E. C. H., Liu, J., &Lyu, M. R. (2007). An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. , *30*, 2353-2364.

[16] Ngai, E. C. H., Jiangchuan Liu, &Lyu, M. R. (2006). On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks., *8*, 3383-3389.

[17] Wenliang Du, Jing Deng, Han, Y. S., Shigang Chen, &Varshney, P. K. (2004). A key management scheme for wireless sensor networks using deployment knowledge. , *1*, 597.

[18] Eschenauer, L., &Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. , 41-47.

[19] Crossbow technology Inc. MICAz. http://www.xbow.com.

[20] Intanagonwiwat, C., Govindan, R., &Estrin, D. (200) Directed Diffusion: A scalable and robust communication paradigm for sensor networks. , 56-67.

[21] Ye, F., Chen, A., Lu, S., & Zhang, L. (2001). A scalable solution to minimum cost forwarding in large sensor networks. , 304-309.

[22] Soo Young, M., & Tae Ho, C. (Sep. 2012). Key Index-Based Routing for Filtering False Event Reports in Wireless Sensor Networks., *E95-B*(9), 2807-2814.

[23] Jin Myoung Kim, Soo Young Moon, & Tae Ho Cho.(2010). Key re-dissemination for maintaining detection power in sensor networks., *1*, 147-150.

[24] Zhen Yu. (2010). A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks., *18*(1), 150-163.

[25] Zhu, S., Setia, S., Jajodia, S., &Ning, P. (2004). An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. , 259-271.

[26] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: security protocols for sensor networks. *Wirel.Netw., 8*(5), 521-534.

[27] Polastre, J., Hill, J., & Culler, D. (2004). Versatile low power media access for wireless sensor networks. , 95-107.

[28] Vuran, M. C., &Akyildiz, I. F. (2006). Spatial correlation-based collaborative medium access control in wireless sensor networks.*IEEE/ACM Trans.Netw.*, *14*(2), 316-329.

Authors

Su Man Nam received his B.S. degrees in computer information from Hanseo university, Korea, in February 2009 and M.S degrees in in Electrical and Computer Engineering from Sungkyunkwan University in 2013, respectively. He is currently a doctoral student in the College of Information and Communication Engineering at Sungkyunkwan University, Korea. His research interests include wireless sensor network, security in wireless sensor networks, and modelling & simulation.

Tae Ho Choreceived the Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and the B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Information and Communication Engineering, Sungkyunkwan University, Korea. His research interests are in the areas of wireless sensor network, intelligent systems, modeling & simulation, and enterprise resource planning.