A SECURITY METHOD FOR MULTIPLE ATTACKS IN SENSOR NETWORKS: AGAINST FALSE-REPORT INJECTION, FALSE-VOTE INJECTION, AND WORMHOLE ATTACKS

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

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

ABSTRACT

In a large-scale wireless sensor network, damage spreads rapidly in the network when under false report injection, false votes injection, or wormhole attacks. These attacks cause finite energy resources to be drained, legitimate reports to be dropped, and data to be intercepted by adversary nodes. A probabilistic voting-based filtering scheme (PVFS) and localized encryption and authentication protocol (LEAP) can be used to cope with these attacks. When multiple attacks occur simultaneously, PVFS and LEAP should be operated together. But the concurrent application of PVFS and LEAP provides inefficient duplications of operations in the sensor network. In this paper, we propose a security method which improves the energy efficiency while maintaining the security level of applying PVFS and LEAP simultaneously. The proposed method was designed by identifying and eliminating the redundancies of employing both methods together and providing more efficient functionalities. Four types of new keys were also designed for simultaneous detection of multiple attacks. We evaluated the effectiveness of the proposed method compared to simply applying PVFS and LEAP simultaneously when under multiple attacks. The experimental results demonstrate that our proposed method saves energy by up to 11% while maintaining detection power.

KEYWORDS

wireless sensor networks, multiple attacks detection, false report injection attacks, false vote injection attacks, wormhole attacks

1. INTRODUCTION

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

X. Du et al. [7,8] presented that attacks on sensor networks may supervene on application, transportation, link (medium access control), or physical layers. The attacks are also categorized based on the capability of the attackers, such as laptop-level or sensor-level. A powerful laptop-level adversary causes more harm to the power supply than does a sensor-level attack. In addition, the attacks are classified into outside or inside attacks. An outside attacker has no access to most of the cryptographic materials; these include sinkhole [8,9], sybil [10], selective

forwarding , wormhole [12], and HELLO flood [13] attacks, which usually occur on the network layer. Inside attacks, such as false report injection [14] and false vote injection [15] attacks, have imperfect key materials and usually occur on the application layer.

We chose a scenario of multiple attacks consisting of the wormhole attack by an outside attacker and the false report injection attack and false vote injection attack of an inside attacker; this is a situation that frequently occurs in sensor networks under multiple attacks. As shown in Figure 1, an adversary simultaneously uses attack nodes (compromised nodes (Figure 1-a) and two adversary nodes (Figure 1-b)) to launch a false report injection attack (FRIA; Figure 1-c), a false vote injection attack (FVIA; Figure 1-d), and a wormhole attack (WA; Figure 1-e). The compromised nodes try to attack a false report with false votes and false votes on a real report with the goal of deceiving the base station or depleting the limited energy resources [14]–[18]. This devastates constructed routing paths through the adversary node with a gain of report information in the network [8]–[13]. To minimize the damage of energy consumption, detection of false reports, votes, and routing message in the sensor network should occur as early as possible.

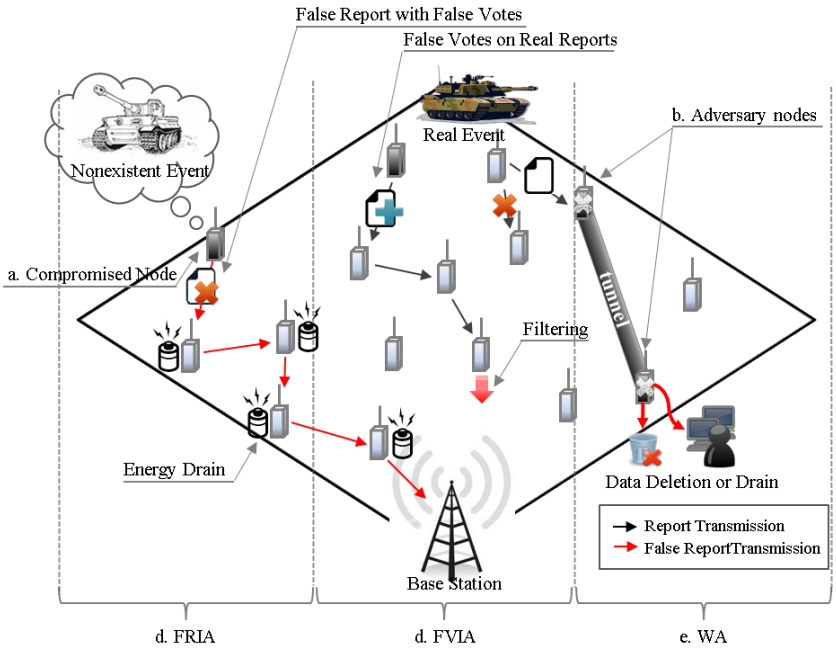

Figure 1. Multiple attacks generation in the sensor networks

Li et al. [17] proposed a probabilistic voting-based filtering scheme (PVFS) to filter out forged reports and votes during the forwarding process into the base station in order to detect attacks, such as FRIA and FVIA, at the application layer. In this scheme, multiple sensing nodes collaboratively generate a sensing report that consists of multiple votes (such as message authentication codes (MACs)) from neighboring nodes using their symmetric keys [14], [19], [20]. As a report passes through multiple hops into the base station, each forwarding cluster heads (CHs) along the way probabilistically authenticates the correctness of the votes and counts any false votes in the report. If the number of false votes is greater than a threshold value, the report is dropped due to its being identified as a false report with false votes; if the number of false votes is less than the threshold value, the report is forwarded due to its being identified as a legitimate report with a false vote. With this strategy, PVFS prevents false reports and votes through collective decision making by using multiple detecting CHs and through collective false detection by using multiple forwarding CHs.

Zhu et al. [12] proposed a localized encryption and authentication protocol (LEAP), a key management protocol for sensor networks to detect attacks of the network layer, such as WA. In this protocol, different types of messages exchanged between the sensor nodes have different security demands, and a single-key method is inappropriate to communicate these different security requirements. Therefore, 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 neighboring nodes, and a group key shared by all nodes in the network [12], [21].

When three attacks occur at the same time, PVFS and LEAP should be operated simultaneously in the sensor network. As shown in Figure 1, such multiple attacks can cause serious damage to the network. In this case, the network should be effectively managed, because a node has limited energy and computation capacity. In this paper, we present a security method that improves energy efficiency while maintaining the detection power of using the simultaneous application of PVFS and LEAP. Our method detects false reports, votes, and routing message by using the four keys, without the function duplication of using the simultaneous application of two methods at the same time. Thus, we decrease the communication and energy consumption of each node in the network.

The rest of this paper is organized as follows. Section 2 briefly describes countermeasures in the application and network layers as general background information. Section 3 introduces our proposed method, and Section 4 presents the optimizations results. Finally, conclusions and future work are discussed in Section 5.

2. BACKGROUND AND MOTIVATION

In the sensor network, an adversary can execute diverse attacks that drain the limited resources of sensor nodes in every layer of the network. The attacks in the application and network layers inject false data and destroy routing paths from the adversary node. Through these attacks, the adversary accelerates damage of the network through multiple attacks in multiple layers. Three representative attacks in the application and network layers are FRIAs, FVIAs, and WAs. In an FRIA, a fabricated report causes false alarms as it arrives at the base station, and it also drains the limited energy of sensor nodes as it passes through multiple hops [4], [6], [14], [22]. In an FVIA, a legitimate report is filtered out at an intermediate node before it can arrive at the base station, because a fabricated vote is deliberately injected. In a WA, a wormhole is built to demolish the network between two adversary nodes; the effects can include data tap, destruction, invention, and damage. We will discuss existing countermeasures for FRIAs and FVIAs in Section 2.1 and existing countermeasures for WAs in Section 2.2. Section 2.3 explains the motivation for our proposed method.

2.1. Countermeasures in Application Layer

FRIAs and FVIAs frequently occur from compromised nodes in the sensor network. In an FRIA, a compromised node injects false reports with false MACs without detecting an event, with the goal of deceiving the base station or depleting the limited energy resources [22]. As countermeasures against an FRIA, several security solutions have been proposed, such as the statistical en-route filtering scheme (SEF) [14], the dynamic en-route filtering scheme (DEF) [23], the interleaved hop-by-hop authentication scheme (IHA) [6], and the key inheritance-based filtering scheme (KIF) [24]. In SEF, when a real event occurs, a center-of-stimulus (CoS) node, generate an event report after electing one of neighbors, and it collects MACs from its neighbors. As the report is forwarded toward a base station, intermediate nodes along the way verify the correctness of the MAC. In DEF, each node has a hash chain of authentication keys used to endorse all reports, and a legitimate report should be authenticated by a certain number of nodes. In IHA, a base station detects a false report when no more than t nodes are

compromised, where t is a security threshold. In KIF, the keys of each node used in the message authentication consist of the node's own key and the keys inherited from nodes upstream. Every authenticated report contains the combination of the MACs generated by using the keys of the consecutive nodes in the path from the base station to the terminal node. That is, these solutions such as SEF, DEF, and KIF filter the false report at an intermediate node using verification keys. However, if the false report is dropped after traveling many hops, intermediate nodes along the way consume their energy needlessly. In an FVIA, a compromised node injects false votes on the legitimate report to cause it to be dropped at an intermediate node. As countermeasures against an FVIA, several security solutions have been proposed, such as MEF [25]. In MEF, a report is delivered to the BS through a multipath routing technique and a random key pre-distribution. However, this scheme consumes extraneous energy in employing the multipath routing technique.

In order to detect the presence of both an FRIA and an FVIA in the application layer, PVFS was proposed, which drops a report as false only when the number of votes that it is false reaches a threshold value: the number of verified false votes required to drop a report. This scheme combines cluster-based organization, probabilistic key assignment, and voting methods. For example, when a real event occurs in a cluster, sensor nodes in the cluster transmit their votes to a cluster header node. After the CH randomly chooses the number of required votes, the selected votes are attached to a report. Before forwarding the report, the CH selects verification CHs to be a verification node with a probability $P = d_i/d_0$ (d_i is the distance from ith verification CH node to the base station, and d_0 is the distance from the report generation CH to the base station).. After selecting a verification node, selected verification CHs get a verification key of the CH. As the report arrives in a verification CH, it verifies the votes in the report through the obtained keys. If the number of false votes exceeds a threshold value, the report is dropped, such as under an FRIA. On the other hand, if the number of false votes is less than the threshold value, the legitimate report including a few false votes is securely delivered to the BS, after considering an FVIA. Therefore, PVFS detects false votes in a report at selected verification nodes through their keys and decides whether there is an FRIA or FVIA through the threshold value, as they simultaneously occur in the sensor network.

2.2. General Format, Page Layout and Margins

WAs frequently occur from two adversary nodes in the sensor network. A fast tunnel (e.g., a wire-line link) can be built to intercept or remove data between two adversary nodes that are physically very far from each other. As countermeasures against a WA, several solutions have been proposed, such as the INtrusion-tolerant routing protocol for wireless Sensor NetworkS (INSENS) [26], the SECure Tracking Of node encounteRs (SECTOR) [27], the WOrmhole attack DEfense mechanism (Wodem) [28]. INSENS constructs forwarding tables at each node to make communication easier between nodes and the base station. This scheme uses one-way hashes while constructing routing paths of the whole network. Each node deals with a WA through main and alternative paths. While constructing the topology of the sensor network, a route request and feedback messages are used for implementing secure paths using information from neighboring nodes. SECTOR is based primarily on distance-bounding techniques on a one-way hash. This scheme detects a WA when the roundtrip time of a packet exceeds a max distance after computing the distance between two nodes. Wodem detects a WA by forwarding authentication packets in advance as two nodes set up routing paths for communication after an event occurs. If the attack is detected, the adversary nodes are found by comparing the minimum hops over a distance with real hop counts. The adversary nodes are then dropped after the information from their neighbors is deleted.

In order to prevent a WA in the network layer, LEAP was proposed to observe the different types of messages that are exchanged between the security requirements to provide

confidentiality and authentication. Every sensor node has an individual key (IK), pairwise key (PK), cluster key (CK), and group key (GK). The types of keys verify a message while forwarding it. This scheme is important to maintain confidentiality for the transmission of event reports and routing messages by using the keys between a node and the base station, or a node and another node. When a newly inserted node forwards a routing message after every node is deployed, its neighboring nodes verify the message through their keys and change routing paths. On the other hand, if two adversary nodes try to construct a tunnel through a false message without keys in each cluster, such as under a WA, their neighboring nodes check and drop the false message. Thus, LEAP effectively detects false message through four types of keys, as adversary nodes try to destroy the topology of the sensor network, such as in a WA.

2.3. Motivation

The sensor network has the high disadvantage, due to its limited capabilities, of being compromised and destroyed from various attacks, such as FRIAs, FVIAs, and WAs. These attacks waste the resources and obstruct the operation of the sensors through the fabrication of false data and routing paths. In addition, when these attacks occur simultaneously, a scheme would be to apply both PVFS and LEAP; however, the simultaneous application of PVFS and LEAP consumes energy resource needlessly due to resulting duplication of operations. For example, when a CH transmits a report after detecting an event, authentication CHs should be selected through a probability in PVFS, and the authentication CHs gain keys to verify the report. While forwarding the report, intermediate nodes along the way forward and verify it through both PVFS and LEAP keys, consuming unnecessary energy due to duplication of communication overhead. Therefore, we propose our method to maintain the security level and reduce energy consumption by employing four types of keys to avoid duplication of operations.

3. PROPOSED METHOD

In the sensor network, an adversary frequently tries to coincide with various other attacks in the application and network layers, such as FRIAs, FVIAs, and WAs. Our proposed method uses four types of keys: a new individual key (NI), a new pairwise key (NP), a new cluster key (NC), and a new group key (NG). Our proposal effectively protects against multiple simultaneous attacks in the network by using these four types of keys. Therefore, the proposed method maintains the security level and improves energy effectiveness compared to the simultaneous application of PVFS and LEAP. In this section, the proposed method is described in detail.

3.1. Assumptions

We assume a static sensor network (i.e. the topology of the network is fixed) and that the sensor nodes are immobile. The sensor network comprises a base station and a large number of small sensor nodes; e.g., for the Berkeley MICAz motes [29], the topology establishes the initial paths through directed diffusion [30] and minimum cost forwarding algorithms [31]. We choose the cluster-based model to organize the sensor nodes. In a cluster, one node is elected to be the cluster-head, denoted as CH. Each CH uses a larger transmission range than the normal nodes and discovers a routing path toward the base station. In addition, a CH chooses a routing path based on the cost, which is the distance from the base station to itself. Every node forwards packets upstream (toward the base station) along this path. Four types of keys are then created in each sensor node, as in the processes of LEAP [12].

As mentioned, we focus on three attacks: FRIA, FVIA, and WA. An adversary launches the multiple attacks using compromised nodes and two adversary nodes at the same time. False reports with false votes and legitimate reports with false votes flow into the base station, and two adversary nodes are inserted into a two-cluster area to be damaged through a tunnel for intercepting reports. We set the threshold value for detecting false votes as two. If the number of

false votes in a false report is greater than the threshold, FRIA is detected; if the number of false votes in a legitimate report is fewer than the threshold, FVIA is detected. The issues of other security attacks are out of the scope of this paper.

3.2. Overview

In our proposed method, we use four types of keys in each sensor node to effectively detect the multiple attacks: 1) a new individual key (NI), 2) a new pairwise key (NP), 3) a new cluster key (NC), and 4) a new group key (NG). 1) An NI is used for encrypting information of events from a CH's neighbors and notifying abnormal behaviors to the base station. 2) An NP is used for detecting false reports in authentication nodes and maintaining secure paths in intermediate nodes. 3) An NC is used for detecting false votes in CHs and verifying routing messages. 4) An NG is used for detecting false reports at the base station and confirming routing messages. These four types of keys are provided to enable simultaneous detection of the three attacks. For example, when an FRIA tries to inject a false report through a compromised node, the NP and NG cause dropping of the false report at an authentication node and the base station. When an FVIA tries to transmit a false vote from a compromised node of a CH, the NC filters out the false vote in the CH. When a WA tries to forward false routing messages from two adversary nodes, the NC and NG cause the false message to be dropped at neighbors of the adversary nodes. Therefore, our proposed method uses the four types of keys to effectively protect the sensor network against multiple simultaneous attacks, such as FRIAs, FVIAs, and WAs.

3.3. General Format, Page Layout and Margins

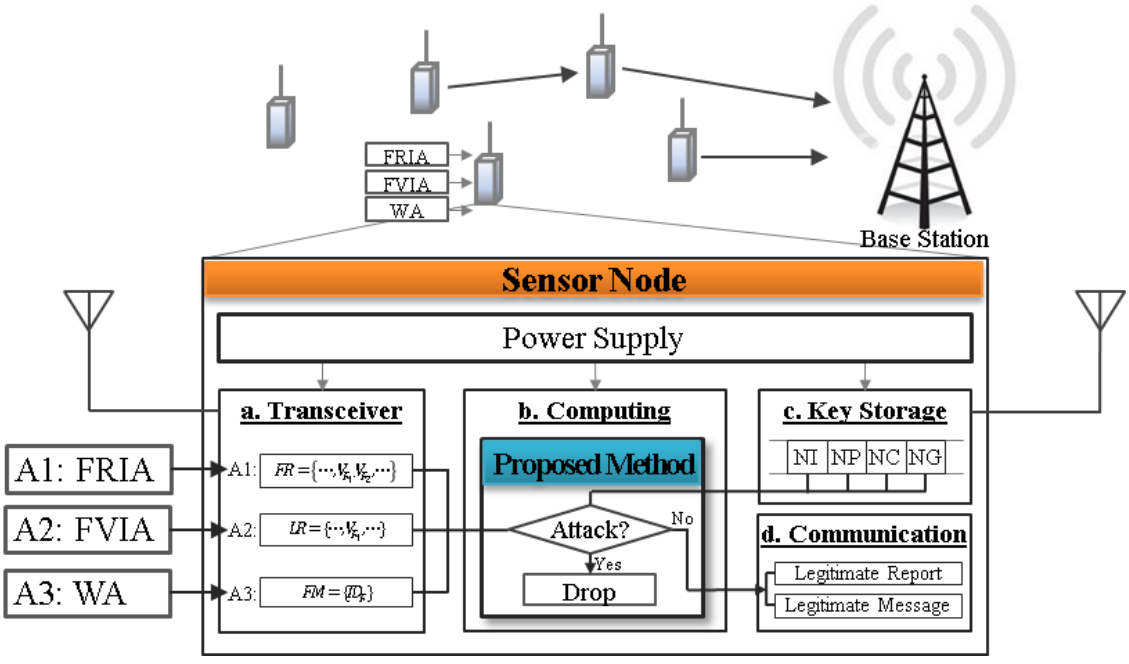

Figure 2. Proposed method's structure

Figure 2 shows a detection process in a sensor node when 1) FRIA, 2) FVIA, and 3) WA are simultaneously generated in the sensor network. Our proposed method detects the multiple attacks using four common components: a. Transceiver, b. Computing, c. Key Storage, and d. Communication as shown in Figure 2. a. Transceiver component receives a report and message from a neighbor, b. Computing component verifies a false vote and message through proposed keys in c. Key Storage. If the node detects the false vote or message, they are dropped through four types of keys. On the other hand, if the vote or message is legitimate, they are transmitted

to next node. We denote that 1) a false report (FR) is $\{\cdots, V_{F_1}, V_{F_2}, \cdots\}$, 2) a legitimate report (LR) is $\{\cdots, M_{F_1}, \cdots\}$, and 3) a false message (FM) is $\{ID_F\}$. In addition, a threshold value is two in the proposed method. When the FRIA is tried with a false report as shown in Figure 2-1), the sensor node receives the false report (FR) through Transceiver (Figure 2-a) and send Computing (Figure 2-b). A NP of the proposed method in Key Storage (Figure 2-c) then confirms false votes in false report. After detecting the false votes V_{F_1}, V_{F_2}, the FR is filtered out due to approaching the threshold value. When the FVIA is tried with a legitimate report (LR) as shown in Figure 2-2), the LR passes through Transceiver component and arrives in Computing component, and the false vote V_{F_1} is detected through the NP of the proposal in the LR. The sensor node transmits the LR through Communication component to a neighboring node. Finally, when the WA is tried with false message (FM) as shown in Figure 2-3), the FM is detected and dropped through its NC and NG after passing through Transceiver component. Thus, the proposed method effectively detects the multiple attacks using four types of keys when FRIA, FVIA, and WA occur in the sensor network at the same time.

3.4. Multi-Attacks Detection

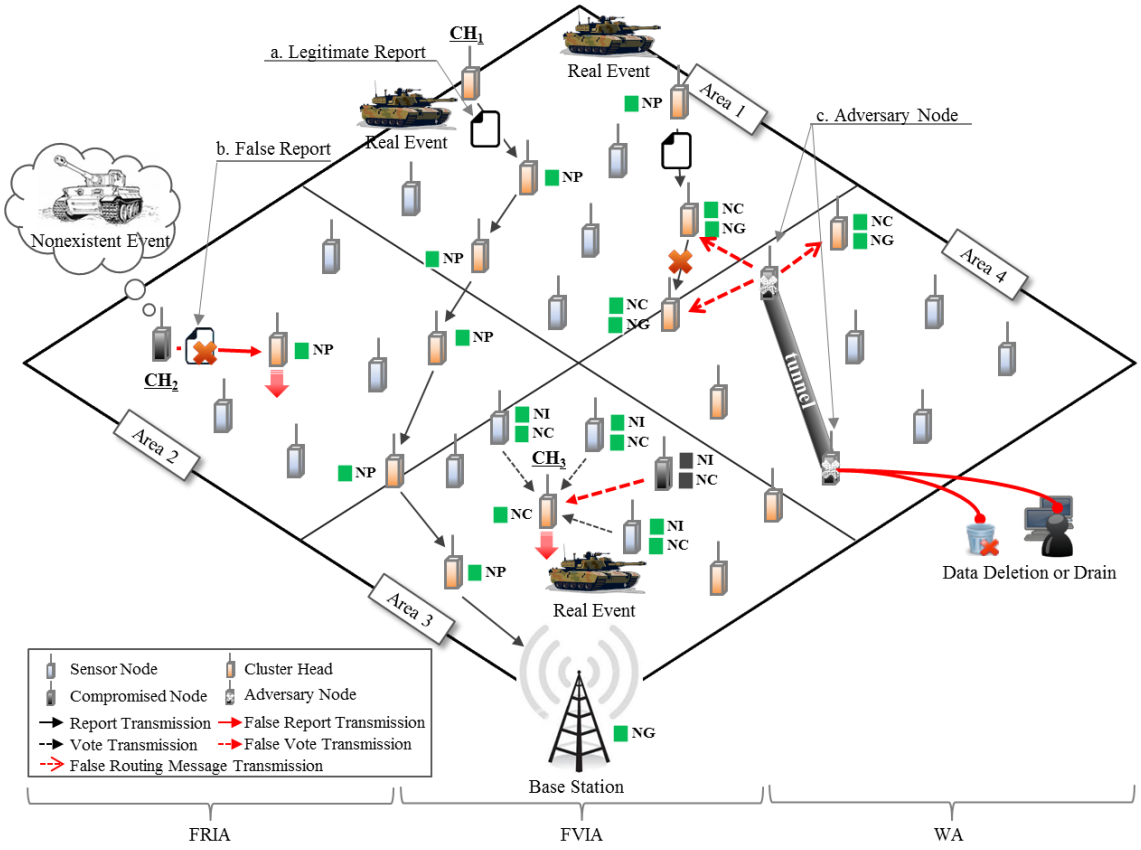

Figure 3. Target system model

Figure 3 shows a target system model in the sensor network to protect against FRIAs, FVIAs, and WAs. The sensor network is composed of a sensor field with four areas and a base station. There are multiple CHs and normal nodes,withseveral compromised nodes in each area. The CHs and the nodes have four types of keys and can detect FRIAs, FVIAs, and WAs in the sensor network. In Area 1, a legitimate report without false votes is forwarded via multiple hops to the base station. When CH_1 detects a real event, it attaches the legitimate report (Figure 3-a) after randomly selecting its neighboring nodes' votes. An authentication CH verifies the report through its NP. While forwarding the report via multiple hops, intermediate CHs maintain a

secure path through their NPs. When the report arrives at the base station, the base stationconfirms it through its NG. That is, a legitimate report verifies an authentication CH and the base station through their NP and NG. In Area 2, a compromised node (CH_2) transmits a false report about a nonexistent event such as an FRIA. After calculatedly injecting false votes at the compromised node, the false report with the false votes is forwarded to the next CH. The false report with the false votes is detected and droppedat an authentication CH through its NP. That is, the authentication node provides early filtering power using its NPagainst forged reports from a compromised node. If the false report arrives at the base station, the base station checks the false report through its NG. In Area 3, a compromised node injects a false vote to be dropped at an authentication CH when an event occurs, such as an FRIA. The compromised node transmits a false vote to its CH as an event occurs. Before producing a report, CH_3 collects and verifies all of the neighboring nodes' votes. When a false vote is detected, CH_3 drops the false vote and transmits a legitimate report via multiple hops to the base station. That is, a CH provides early detection power using its NC against forged votes from a compromised node. In Area 4, two adversary nodes try to forward a false routing message including their IDs to threaten its neighbors, such as in a WA. The WA causes serious damage to the neighboring nodes without keys within the region of the adversary nodes. An adversary inserts two nodes (Figure 3-c and Figure 3-d) to construct a tunnel for intercepting all data. The newly inserted nodes forward false message to their neighboring nodes without any keys. After receiving the false routing message, the neighbors detect and filter out the false routing message through their NC and NG. The neighbors transmit no ACK message to the adversary nodes. That is, all of the neighboring nodes check to verify the routing message through their NC and NG. Therefore, our proposed method provides simultaneous detection of multiple attacks using four types of keys in the sensor network. We further describe and verify the proposed method in Figure 5, Figure 6, and Figure 7.

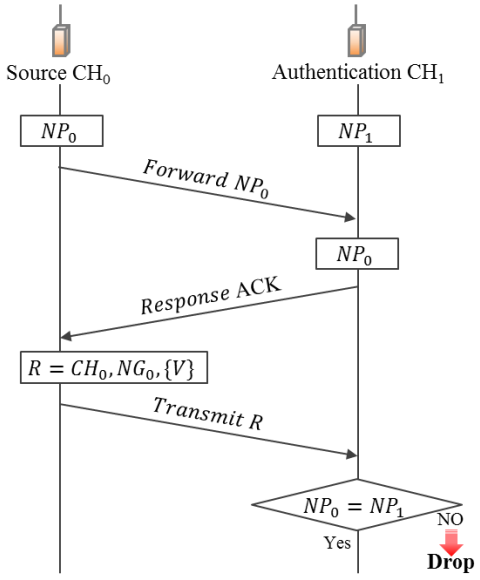

Figure 4. Detection against FRIA

Figure 4 shows an authentication process between a CH and an authentication CH against an FRIA, as shown in Area 2 of Figure 3. When a real event occurs in a region, a source CH_0 collects votes from its neighboring nodes. The source CH attaches the votes and prepares a report (R) for forwarding. Before transmitting the report to the authentication CH_1, CH_0 sends its NP_0 to CH_1. CH_1 then verifies the key with its NP_1. After verifying, CH_1 transmits ACK to CH_0. Next, CH_0 forwards the legitimate report and its NG to CH_1. When the report arrives at the base station, it verifies the NG_0in the report through its NG_1. On the other hand, if CH_0 is

compromised, CH_0 may have a false NP_0 and try to allowan FRIA into the sensor network. CH_0 injects a false report of detecting no event and sends the false NP_0 to CH_1 to forward the false report. CH_1, which receives the false key, verifies it with its NP and responds with an ACK to receive and drop the false report. The compromised node then forwards the false report to CH_1. The authentication CH_1 directly drops the false report. CH_1 transmits an abnormal condition to the base station. If the false report arrives at the base station after passing through the authentication CH, the base station verifies the NG_0 of the report through its NG_{BS}. Therefore, our proposed method filters out a false report more quickly than using the simultaneous application of PVFS and LEAP against an FRIA.

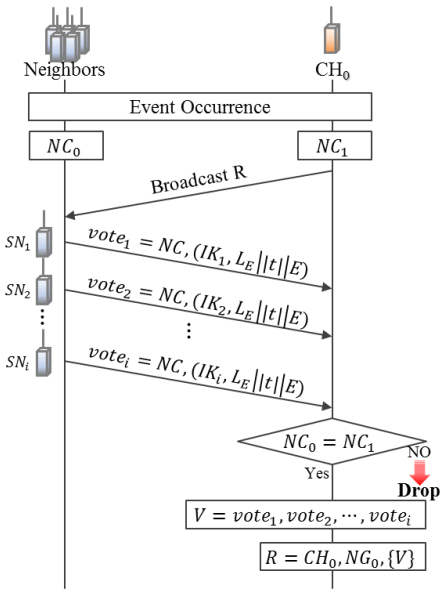

Figure 5. Detection against FRIA

Figure 5 shows an authentication process between a CH and its neighboring nodes against an FVIA, as shown in Area 3 of Figure 3. When a real event occurs in a cluster region, CH_0 broadcasts to collect votes from its neighbors. The neighbors send their votes, including their NC and event information (L_E is the location of the event, t is the time of detection, E is the type of eventFigure 5) to CH_0. After collecting the votes, CH_0 verifies the votes by using its NC_1. The votes are randomly selected and attached in a report. On the other hand, if a node is compromised among the neighbors of CH_0 in a cluster region, the compromised node transmits a false vote to CH_0 with its false NC to cause other nodes to drop a legitimate report while forwarding it. However, the false vote is filtered out through the NC_1 of CH_0. Therefore, our proposed method detects a false vote earlier than using the simultaneous application of PVFS and LEAP, and itallows the legitimate report to be securely forwarded.

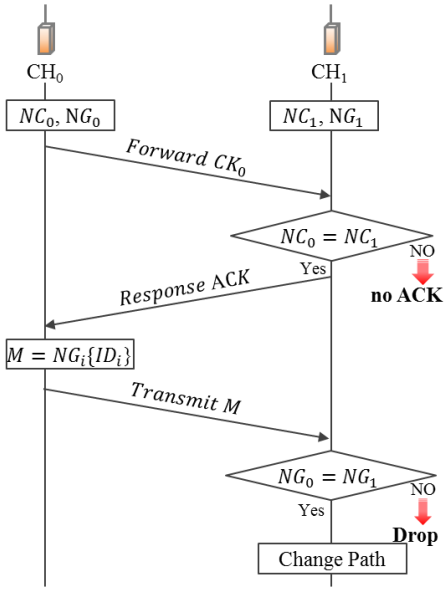

Figure 6. Detection against FVIA

Figure 6 shows an authentication process between a CH_0 and a CH_1 against a WA, as shown in Area 4 of Figure 3. When a new node is inserted into the sensor network, the newly inserted node usually forwards a routing message (M) including its ID to neighboring nodesFigure 6. In our proposal, a newly inserted CH_0 should send its CK to CH_1 before forwarding the routing message. CH_1 verifies the NC_0 through the NC_1 and transmits an ACK. CH_0 transmits the routing message with its NG to CH_1. Before applying the routing message, CH_1 verifies NG_0 through NG_1 and applies a routing path. If CH_0 is an adversary node, it produces a false routing message with a false key. When CH_1 receives the false message with a false key, CH_1 transmits no ACK to the adversary node. Therefore, our proposed method maintains the same security level as using the simultaneous application of PVFS and LEAP.

4. SIMULATION RESULTS

Table 1. Simulation parameters

Parameter		Value
Number of a cluster		100
Number of nodes in a cluster		10
Field size		1,000×1,000 m^2
Number of compromised nodes		2 or 10
Number of adversary nodes		2
Size of transmission	Report	24 bytes
	Vote	1 byte
	Routing Message	12 bytes
Energy consumption	Transmit	16.56μJ/byte
	Reception	12.5μJ/byte
	Vote generation	15μJ/byte

A simulation was performed to test the proposed method, compared to using the simultaneous application of PVFS and LEAP. The sensor network used in the simulation comprises 100

clustersin the simulation environment, which is 1,000×1,000m^2. That is, the total sensor nodes are 1,000 (100×10). The simulation is based on Ye et al.'s method of energy consumption [12]. We set the simulation to have2 or 10 compromised nodes and 2 adversary nodes in the sensor network. Each node takes 16.25 and 12.5 µJ to transmit and receive a byte, respectively, and each vote generation consumes 15 µJ per byte. The size of a report is 24 bytes, and the size of a vote is 1 byte.In addition, the size of a routing message is 2 bytes (if it only includes a node ID), and the size of an ACK message is 12 bytes (id size is 4 bytes, and vote size is 8 bytes) [9, 24]. The simultaneous application of the two methodsresults in 100 keys in the global key pool, which is divided into 10 partitions. We assumed that the compromised nodes are 2 or 10 nodes for the false report injection attack, and an adversary node is one node for the sinkhole attack. In addition, we generated 1,000 events of FRIAs, FVIAs, and WAs. The false reports,false votes, and routing messageswere createdseparately by the compromised nodes and theadversary node.

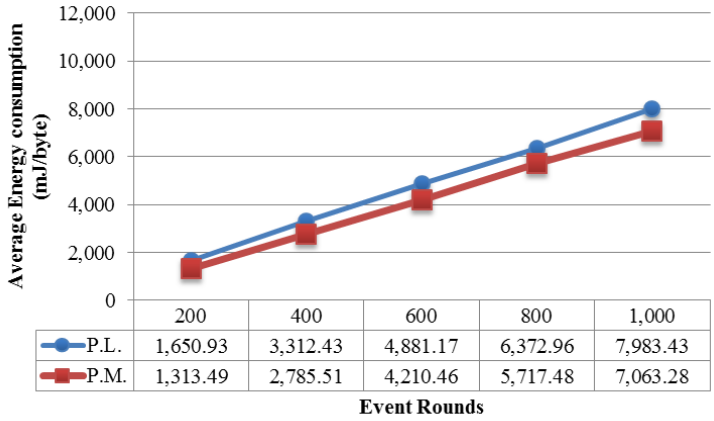

Figure 7. Average energy consumption per event generation (attack occurrence: FRIA, FVIA, and WA)

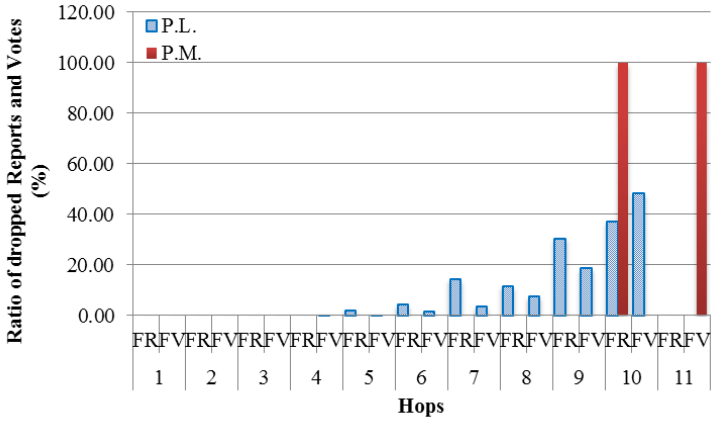

Figure 8. Number of filtered votes and reports (attack occurrence: FRIA, FVIA, and WA)

Figure 7 and Figure 8show theaverage energy consumption and the probability of filtered false reports and votes through two compromised nodes, as the FRIA, FVIA, and WA occur simultaneously in the sensor network. The compromised nodes are randomly located at hop 11. In Figure 7, we show the measurements, using the simultaneous application of PVFS and LEAP (P.L.) and the proposed method (P.M.), of the energy consumption for every 200 events. After 200 events occurred, the simultaneous application of the two methods consumed about 340µm

more energy, and after 1,000events, the proposed method savedup to 11%of the energy consumed when using the simultaneous application of PVFS and LEAP. Figure 8shows the probability of a filtered false report and votes through two compromised nodes (This figure is untanned because the probability of P.L. and P.M. is the same for false routing messages, as shown in Figure 14.). In P.L., the false reports and votes are almost dropped at hops 9 and 10, and needless energy is consumed, more than with the proposed method. In P.M., the false reports and votes are detected in CHs through their PKs and CKs, and less energy is consumed than with the simultaneous application of PVFS and LEAP,when FRIA, FVIA, and WA occur at the same time.

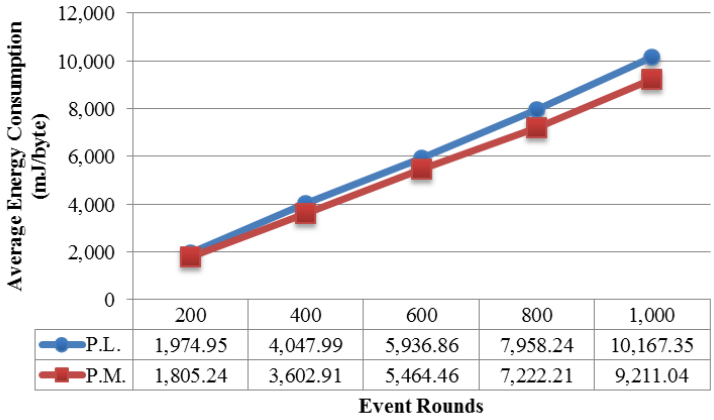

Figure 9. Average energy consumption per event generation (attack occurrence: FRIA, FVIA, and WA)

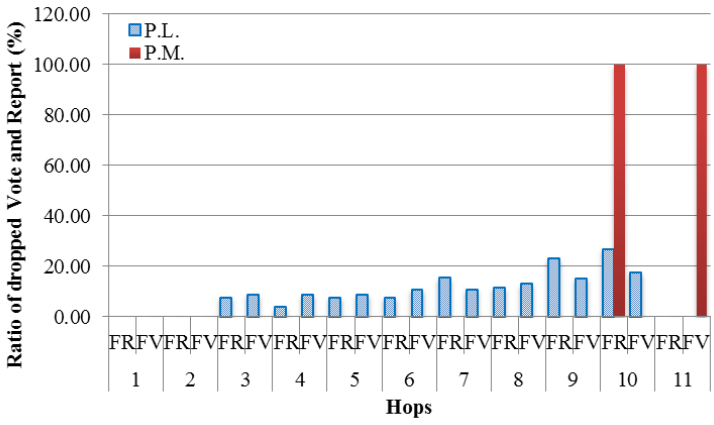

Figure 10. Ratio of filtered votes and reports per hop (attack occurrence: FRIA, FVIA, and WA)

Figure 9 and Figure 10shows the average energy consumption and the probability of filtered false reports and votes with 10 compromised nodes, as FRIA, FVIA, and WA occur at the same time in the sensor network. After 200 events occurred, more energy was consumed withboth P.L. and P.M. than with the simulation of two compromised node, as shown in Figure 8. That is, energy consumption is increased by about 500µm and 325µm in P.L. and P.M., respectively. In Figure 9, after 1,000 events, the proposed method reduces energy consumption up to 10% more than with the simultaneous application of two methods. As shown in Figure 10, P.L. detected the false reports and votes between hops 3 and 10. In P.L., the filtering probability was 50% within 2 hops and 3 hops against FRIA and FVIA, respectively. With P.M, all of the reports and

votes weredropped within 1 hop against both FRIA and FVIA. Therefore, the proposed method improves the energy consumption and filtering rate compared to the simultaneous application of two methods, when FRIAs, FVIAs, and WAs occursimultaneously in the sensor network.

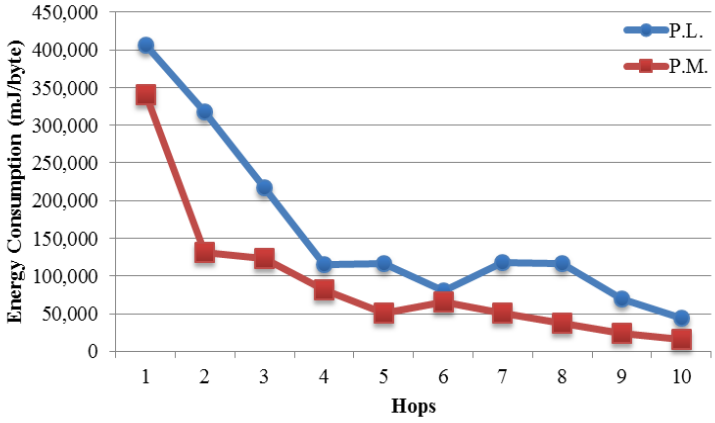

Figure 11. Energy consumption per hop (attack occurrence: FRIA and FVIA)

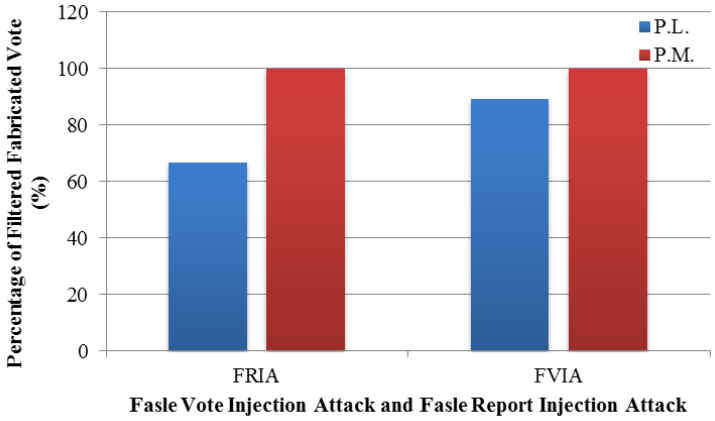

Figure 12. Percentage of filtered false reports and votes (attack occurrence: FRIA and FVIA)

Figure 11 and Figure 12show the energy consumption and the filtering percentage as FRIA and FVIA attacks occur in the application layer over 1,000 events. The number of compromised nodes is 2, and they are randomly located in hop 11. A shown in Figure 11, P.M. reduces energy consumption because the false report and votes are filtered out earlier than with P.L. That is, they are detected within hops 10 or 11, and P.M. improves the effectiveness of energy consumption because legitimate reports are forwarded more often than with the simultaneous application of PVFS and LEAP. In P.L., the energy consumption is influenced by the false report and votes. Figure 12 shows that the proposed scheme improves filtering probabilitiesby about 25% and 15% against FRIA and FVIA, respectively. Therefore, the proposed method improves detection power and energy consumption compared to the simultaneous application of the PVFS and LEAP when FRIA and FVIA occur in the application layer of the sensor network at the same time.

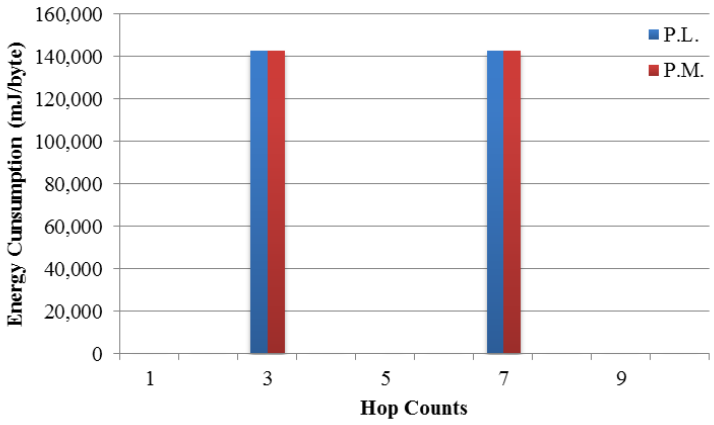

Figure 13. Energy consumption per hop (attack occurrence: WA)

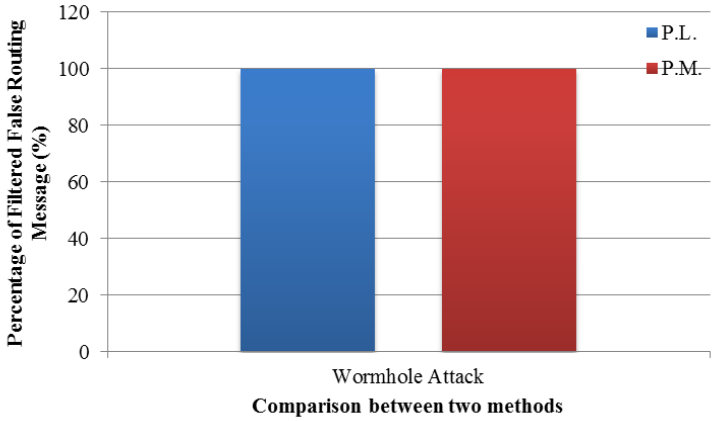

Figure 14. Percentage of filtered false routing messages (attack occurrence: WA)

Figure 13 and Figure 14 show the energy consumption and filtering percentage of false routing messages as WAs occur in the network layer. Two adversary nodes are located to construct a tunnel and five attacks are attempted among 1,000 events in the sensor network. The adversary nodes are inserted to intercept and drop legitimate reports at hops 3 and 7. As shown in Figure 13 and Figure 14, the energy consumption and the filtering probability of P.L. and P.M. are the same. Therefore, the proposed method maintains the same security level as the simultaneous application of PVFS and LEAP when WAs occur in the sensor network.

5. CONCLUSIONS

In WSNs, attacks such as FRIA, FVIA, and WA produce serious harm to the sensor network. FRIA consumesunnecessary energy and causes false alarms in the base station; FVIA drops legitimate reports by inserting a false vote at an intermediate node; and WA constructs a tunnel to intercept and drop reports. PVFS and LEAP have been separately proposed to detect these attacks in the sensor network. When multiple types of attacks occur at the same time in the network, PVFS and LEAP should be operated simultaneously, but this introduces some inefficiency. In this paper, we propose a security method that improves energy efficiency while maintaining the detection power provided by the simultaneous application of PVFS and LEAP against these attacks. We use four types of new keys—NI, NP, NP, and NG—to efficiently detect the multiple attacks. NI is used forthe vote and alert information encryption, NP is used

for the detection of false reports and maintenance of secure paths, NC is used for the detection of false votes and the verification of routing messages, and NG is used for the verification of legitimate reports and routing messages. The simulation results show that,with our method, each node has significantly increased energy savings compared with using the simultaneous application of PVFS and LEAP. Our method improves energy by about 11% while maintaining the detection power against multiple attacks, compared to the simultaneous application of the two methods. As future work, the performance of our method will be compared to the simultaneous application of PVFS and LEAP against diverse inside and outside attacks. We also intend to simulate various scenarios for investigation. In addition, we will 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. NRF-2013R1A2A2A01013971)

REFERENCES

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

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

[3] K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Ad Hoc Networks, ACM 3(3) (2005) 325-349.

[4] H.Y. Lee, T.H. Cho, Optimized fuzzy adaptive filtering for ubiquitous sensor networks, IEICE Transactions on Communications E94.B(6) (2011) 1648-1656.

[5] H. Chan, A. Perrig, B. Przydatek, D. Song, SIA: Secure information aggregation in sensor networks, J. of Computer Security 15(1) (2007) 69-102.

[6] S. Setia, S. Jajodia, P. Ning, An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks, Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on (2004) 259-271.

[7] X. Du, H.-H. Chen, Security in wireless sensor networks, Wireless Communications, IEEE 15(4) (2008) 60-66.

[8] E.C.H. Ngai, J. Liu, M.R. Lyu, On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks, Wireless Sensor Networks. Commun., 2006. ICC '06 (2006) 8164-9547.

[9] C.H. Ngai, J. Liu, M. R. Lyu, An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks, J. Computer Communications 30(11-12) (2007) 2353-2364.

[10] S. Chen, G. Yang, S. Chen, A Security Routing Mechanism Against Sybil Attack for Wireless Sensor Networks, Communications and Mobile Computing (CMC), 2010 International Conference on 1 (2010) 142-146.

[11] M. Tiwari, K.V. Arya, R. Choudhari, K.S. Choudhary, Designing Intrusion Detection to Detect Black Hole and Selective Forwarding Attack in WSN Based on Local Information, Computer Sciences and Convergence Information Technology, 2009 (ICCIT '09) (2009) 824-828.

[12] S. Zhu, S. Setia, S. Jajodia, LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks, ACM Conference on Comput. and Commun. Security (2004) 62-72.

[13] R. Mavropodi, P. Kotzanikolaou, C. Douligeris, Secmr- a secure multipath routing protocol for ad hoc networks, Elsevier Journal of Ad Hoc Networks 5(1) (2007) 87-99.

[14] F. Ye, H. Luo, S. Lu, Statistical En-route Filtering of Injected False Data in Sensor Networks, IEEE J. Selected Area Commun. 23(4) (2005) 839-850.

[15] Y.-S. Chen, C.-L. Lei, Filtering False Messages En-Route in Wireless Multi-Hop Networks, Wireless Communications and Networking Conference (WCNC), 2010 IEEE, (2010), 1-6.

[16] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on (2003) 113-127.

[17] F. Li, J. WU, A probabilistic voting-based filtering scheme in wireless sensor networks, Proceedings of the 2006 international conference on Wireless communications and mobile computing (IWCMC '06) (2006) 27-32.

[18] S.Y. Moon, T.H. Cho, Key Index-Based Routing for Filtering False Event Reports in Wireless Sensor Networks, IEICE Transactions on Communications, E95-B(9) (2012) 2807-2814.

[19] H Chan, A. Perrig D. Song, Random key predistribution schemes for sensor networks, SP '03 Proceedings of the 2003 IEEE Symposium on Security and Privacy, (2003) 197-214.

[20] W. Ye, J. Heidemann, D. Estrin, Medium access control with coordinated adaptive sleeping for wireless sensor networks, Networking, IEEE/ACM Transactions on 12(3) (2004) 493-506.

[21] A. Achtzehn, C. Rohner, I. Rodhe, ARPD: Asynchronous random key predistribution in the LEAP framework for Wireless Sensor Networks, Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE International Conference on (2007) 1-6.

[22] H.Y. Lee, T.H. Cho, A scheme for Adaptively Countering Application Layer Security Attacks in Wireless Sensor Networks, IEICE Transactions on Communications, E93-B(7) (2010) 1881-1889.

[23] Z. Yu, Y. Guan, A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks, Networking, IEEE 18(1) (2010) 150-163.

[24] H.Y. Lee, T.H. Cho, Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks, Lecture Notes in Computer Science Volume 4317 (2006) 116-127

[25] M.S. Kim; T.H. Cho, A multipath en-route filtering method for dropping in sensor networks, IEICE Trans. Inf. & Syst. (E90-D) (2008) 2108-2109.

[26] J. Deng, R. Han, S. Mishra, INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks, Computer Communications 29(2) (2006) 216-230.

[27] S. Čapkun, L. Buttyán, J.-P. Hubaux, SECTOR: secure tracking of node encounters in multi-hop wireless networks, SASN '03 Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (2003) 21-32.

[28] J.H. Yun, I.H Kim, J.H. Lim, S.W. Seo, Wodem: Wormhole attack defense mechanism in wireless sensor networks, ICUCT'06 Proceedings of the 1st international conference on Ubiquitous convergence technology (2006) 200-209.

[29] Crossbox Wireless Sensor Networks, http://www.xbox.com/

[30] C. Intanagonwiwat, R. Govindan, D. Estrin, Directed diffusion: A scalable and robust communication paradigm for sensor networks. In Proc. of MobiCOM ‘00 (2000) 56-67

[31] F. Ye, A. Chen, S. Lu, L. Zhang, A scalable solution to minimum cost forwarding in large sensor networks. Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on (2001) 304-309.

Authors

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

Tae Ho Cho received a Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and 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 networks, intelligent systems, modeling & simulation, and enterprise resource planning.