A METHOD FOR DETECTING MULTIPLE ATTACKS AGAINST FALSE REPORT INJECTION ATTACKS AND WORMHOLE ATTACKS IN SENSOR NETWORKS

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

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

ABSTRACT

In wireless sensor networks, adversaries can easily launch multiple attacks on the application layer and the network layer, such as false report injection attacks and wormhole attacks. These attacks drain finite energy resources through false reports of compromised nodes, and devastate the constructed routing paths through the illegal messages of adversary nodes. Statistical en-route filtering (SEF) is proposed in order to drop the false reports against the false report injection attack, and a localized encryption and authentication protocol (LEAP) is proposed to detect the illegal messages to protect against wormhole attacks. When these attacks occur at the same time, SEF and LEAP should be operated simultaneously to confront the false reports and the illegal message in the sensor network. In this paper, we propose a method to improve the energy efficiency and the security level as compared to the simultaneous application of SEF and LEAP. In the proposed method, three types of new keys are designed to effectively detect these attacks, identifying and eliminating the redundancies. The effectiveness of the proposed method is verified through experimentation, and the results are compared to the simultaneous application of SEF and LEAP when the two attacks occur. The experiment results show that our proposed method saves up to 8% more energy, improves the security level of the compromised nodes up to 10%, and maintains the same detection power of the adversary nodes.

KEYWORDS

Wireless Sensor Network, Multiple Attacks, Statistical En-route Filtering (SEF), Localized Encryption and Authentication Protocol (LEAP)

1. INTRODUCTION

Recent advances in wireless communications and electronics have enabled the development of small sensor nodes that are low-cost, low-power, and provide multiple functions [1]. A wireless sensor network (WSN) is composed of a large number of sensor nodes and a base station in the sensor field [2]. A sensor node is used for sensing, computing, and wireless communication without users [3]. The base station collects information from the sensor node via a wireless channel. The nodes have a disadvantage in that they can be captured and compromised due to their limited functions such as computation, communication, storage, and energy supply resource [4]-[5]. In addition, adversary nodes are easily inserted to dispute data transmission in the sensor field [6-7]. Therefore, malicious attackers use various types of attacks to fabricate or eliminate sensing data in the sensor network.

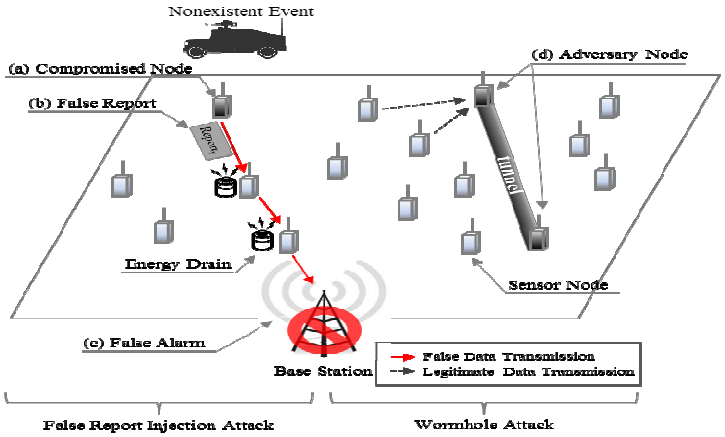


Figure 1. Multiple attacks.

Figure 1 shows a false report injection attack on the application layer and a wormhole attack on the network layer in the sensor network at the same time. In the false report injection attack, a compromised node (Figure 1-(a)) generates a false report (Figure 1-(b)) about a non-existent event. The compromised node injects the false report in the sensor network to make a false alarm (Figure 1-(c)) in the base station. While forwarding the false report in a path, intermediate sensor nodes drain the finite energy resources due to needless transmissions. In the wormhole attack, two adversary nodes (Figure 1-(d)) forward a false routing control message to their neighbors to change routing paths. When the adversary node receives a report to a neighboring node, it instantly communicates the report with another adversary node through a tunnel to fabricate or steal data. Thus, the multiple attacks occur at the same time, and the sensor network suffers serious damage in terms of the energy resources of the sensor nodes.

Ye et al. [5] proposed a statistical en-route filtering scheme (SEF) to drop false reports in intermediate nodes to protect against the false report injection attack. When a real event occurs, one of the detecting nodes prepares to generate an event report by attaching multiple message authentication codes (MACs) of the other detecting nodes. The intermediate nodes verify some of the MACs in the report through their keys as the event report is forwarded toward the base station. If a false MAC is detected, an intermediate node filters out the false report before it reaches the base station. That is, the SEF detects the false report through collective decision-making by using multiple detecting nodes and collective false detection by using multiple forwarding nodes. In addition, Zhu et al. [6] proposed a localized encryption and authentication protocol (LEAP) with a key management protocol in the sensor network. LEAP establishes four types of keys for confidentiality and authentication in each node. The method prevents various attacks of the network layer such as a wormhole attack by using those keys.

When multiple attacks occur at the same time, SEF and LEAP should be run simultaneously to maintain a high security level in the sensor network. The simultaneous application of SEF and LEAP consumes significant energy resources due to the overlapped functions and the communications of the methods. In this paper, we propose a method that enhances the energy efficiency and the security level against the false report injection attack and the wormhole attack. Our proposed method uses four types of keys for each node: a new individual key, a new pairwise key, a new cluster key, and a group key. Our method detects forged MACs, reports, routing control messages generated from a compromised node, and an adversary node through the four types of keys. Therefore, we decrease the energy consumption of each node through the effectiveness of the four keys in the sensor network as compared to the simultaneous application of SEF and LEAP.

The rest of this paper is organized as follows: Section 2 briefly describes SEF, LEAP, and the motivation. Section 3 introduces the proposed method, and Section 4 presents the optimization results. Finally, the conclusions and future work are discussed in Section 5.

2. BACKGROUND AND MOTIVATION

This section briefly describes useful information about SEF and LEAP and the motivation for proposing the new method.

2.1. Statistical En-Route Filtering (SEF)

Ye et al. [5] statistically authenticates all of the reports in intermediate nodes by using symmetric keys to improve the early detection of a false report, low computation, and communication overhead against false report injection attacks. SEF is comprised of four phases: 1) key assignment, 2) report generation, 3) en-route filtering, and 4) base station verification. The base station maintains a global key pool, which is divided into *n* nonoverlapping partitions with m keys for each partition. In phase 1), the key assignment, the base station randomly distributes a partition and numerous keys to all of the sensor nodes from the global key pool before they are deployed. In phase 2), the report generation, one of the detecting nodes is elected as the center-of-stimulus (CoS) node to generate a sensing report using the message authentication codes (MACs) of the surrounding nodes after a real event occurs. A MAC includes the key of a partition and the event information. In phase 3), the en-route filtering, after the CoS forwards the report toward the base station over multi hops, the intermediate nodes prove the correctness of the multiple MACs in the report by using their keys. If a forged MAC is detected, the report is dropped in an intermediate node. In phase 4), the base station verification, when the base station receives the report, it authenticates all of the MACs in the report through the keys of the global key pool. Therefore, SEF detects and drops false reports through collective decision-making by multiple detecting nodes and collective false detection by multiple forwarding nodes.

2.2. Localized Encryption and Authentication Protocol (LEAP)

Zhu et al. [6] proposed multiple keying mechanisms to detect false routing control messages in order to protect against attacks on the network layer, such as the wormhole attack. It observes the different types of messages that are exchanged between the security requirements for providing confidentiality and authentication. It is necessary to require authentication and confidentiality for all routing control messages. LEAP provides four types of keys for each sensor node: 1) individual key, 2) pairwise key, 3) cluster key, and 4) group key. In 1), the individual key, every node has a unique key to share secure information between a node and the base station. When an event occurs, this key encrypts the information of the event. In addition, the key encrypts an alert message to notify any abnormal or unexpected behaviour of its neighbors in the base station. That is, the individual key maintains the secure information from a node to the base station. In 2), the pairwise key, a node shares a key with the next hop node to maintain secure routing paths. When a report or message is transmitted, a node uses the key to verify the condition of the neighboring nodes. If the authentication of the neighboring node fails, a node decides on an adversary node and finds a detour to a secure path for the report and message transmission. That is, the pairwise key holds the correctness in a path between a node and another node. In 3), the cluster key, a node shares this key for securing local routing control messages within a cluster region between a node and all of its neighbors. This key prevents passive participation within the cluster as an adversary node generates

false routing control messages. It is important to detect the false routing control message that ruins the routing paths of the sensor network [7-8]. If an adversary node forwards a routing control message to a node without a cluster key, the destination node immediately verifies that and drops the routing control message using its cluster key. In 4), the group key, every node has a key to encrypt and decrypt the messages in a sensor field. For example, after the sensor nodes are deployed, a newly added node encrypts a broadcast message to update the routing paths by using a group key. The neighboring nodes then modify their routing paths after verifying the message. That is, the group key is shared in the whole network, and every sensor node uses the key to encrypt the message. Therefore, LEAP detects attack types of the network layer for fabricating the routing path of sensor nodes, such as the wormhole attack.

2.3. Motivation

An adversary launches various attack types such as the false report injection attack or the wormhole attack to spread damage in the sensor network. In addition, when the adversary tries to implement these attacks at the same time, every sensor node is quickly diverted from its usual operation. In order to cope with these attacks, SEF and LEAP should be applied in the sensor network. Unfortunately, when SEF and LEAP operate simultaneously, the sensor node energy consumption increases rapidly due to the duplication of functions and communication.

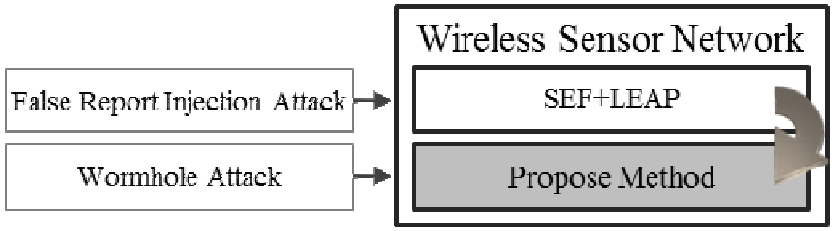


Figure 1. Motivation.

We propose a method to detect the false report injection attack and wormhole attack more effectively than the simultaneous application of SEF and LEAP as shown in Figure 2. There are four types of keys in each node: a new individual key, a new pairwise key, a new cluster key, and a group key. The three new keys are designed for identifying and eliminating the redundancies of the simultaneous application of the two methods. Our method uses the new pairwise key and the new cluster key to protect against the false report injection attack, and provides the new cluster key and group key to protect against the wormhole attack. In addition, the individual key encrypts a MAC and an alert message. Therefore, our proposed method improves the energy savings and security level of each node more than the simultaneous application of SEF and LEAP in the sensor network.

3. PROPOSED METHOD

We propose early detection of the false report injection attack and the wormhole attack with the maximum reduction of the energy consumption as they simultaneously occur in the sensor network. Our proposed method effectively prevents the multiple attacks by using four types of keys. Every sensor has four types of keys: a new individual key, a new pairwise key, a new cluster key, and a group key. The design of the four keys is described in Section 3.2, and the detection of the multiple attacks is described in Section 3.3.

3.1. Assumptions

We assume a static sensor network in which the sensor nodes are fixed after they are deployed. The sensor network is comprised of a base station and a large number of sensor nodes in a sensor field, e.g., the Berkeley MICA2 motes [9]. The initial paths of the topology are established through directed diffusion [10] and minimum cost forwarding algorithms [11] after the distribution of the sensor nodes. In addition, the sensor nodes complete the establishment of the keys after they are deployed. It is further assumed that every node forwards all reports into the base station along a path. We consider that all of the compromised nodes and adversary nodes capture keys in another region. The compromised nodes try to inject reports including a false MAC to forward them into the base station, and the two adversary nodes try to send their neighbors a false routing control message to destroy the routing paths and to construct a tunnel for the manipulation of data.

3.2. Key Design

The four types of keys are as follows:

- New Individual key (NI): Every node has a unique key between a node and the base station to secure information against compromised nodes or adversary nodes. When a real event occurs, a node encrypts a MAC using its NI. In addition, the key encrypts an alert message in order to notify any abnormal or unexpected behaviour of its neighbors in the base station. The MAC and the alert message are decrypted in the base station. Therefore, the NI encrypts the MAC and the alert message to fabricate data in the intermediate nodes, and an NI of the base station decrypts them for verification.
- New pairwise Key (NP): A node shares this key with its immediate neighbor (i.e. one-hop neighbors). When a CoS node forwards a report, a next-hop node of the CoS node (verification node) receives the report, verifies the report by using its NP, and transmits the report to the next node. For example, if a CoS node is compromised to try a false report injection, the false report is dropped in a verification node by its NP. In addition, an intermediate node makes a detour path through its NP when it detects a compromised node or an adversary node within the next hop. That is, the NP prevents the injection of the false report and makes a secure path during communication between a node and another node.
- New Cluster Key (NC): All nodes share a key within a cluster region. When a CoS node receives MACs from its neighbors, the CoS node filters out the MACs generated in a different cluster to produce an accurate report of an event. Besides, when a node receives a false routing control message from an adversary node, the message is authenticated in the node by its NC. Thus, a node verifies all MACs and routing control messages in the sensor network to protect against multiple attacks.
- Group Key (GK): Every node in a sensor field shares a key for encrypting and decrypting primary messages such as the routing control message.

3.3. Designs against Multiple Attacks

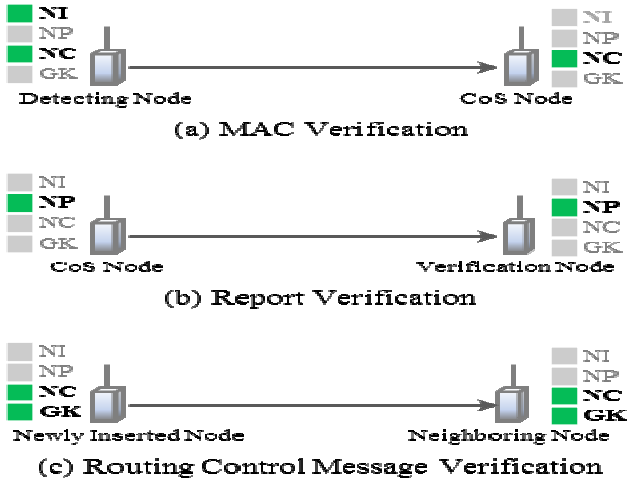


Figure 2. The verification of a MAC, report, and routing control message.

Our proposed method simultaneously detects the false report injection attack and wormhole attack through four types of keys in a sensor network. Our scheme verifies all of the MACs and reports by using an NP and NC against the false report injection attack and all of the routing control messages by using an NC and GK against the wormhole attack.

Figure 3 shows the keys use of the proposed method as a MAC, report, and routing control message occur between two nodes. In Figure 3-a, each node that detects a real event transmits its MAC to a CoS node. A MAC of the detecting node includes its NI, NC, and event information, which includes the location of the event (LE), the time of detection (t), and type of event (E). After collecting the MACs, the CoS node verifies all of the MACs of its neighbors by using the NI and NC. If a false MAC is detected, the CoS node drops it because a compromised node forwards the false MAC, including the forged keys. That is, the CoS node detects false MACs by verifying the NC, and the BS verifies all MACs as the report arrives at the BS. In Figure 3-b, the CoS node forwards a report to a verification node (next-hop node). The report is comprised $R = \{NP, L_E, t, E, M_{i1}, M_{i2}, ..., M_{iT}\}$. If the report is fabricated, the verification node drops the report by the NP. That is, the verification node prevents false reports by verifying the NC. In Figure 4-c, a newly inserted node sends a routing control message to a neighboring node. Before applying the routing control message, the neighboring node verifies it through NC and GK. If an adversary node indiscriminately forwards a false routing control message to its neighbors, the neighboring nodes detect and immediately drop the message by using the NC and GK. Thus, our proposed method detects the multiple attacks by combining four types of keys in the sensor network more effectively than the simultaneous application of SEF and LEAP.

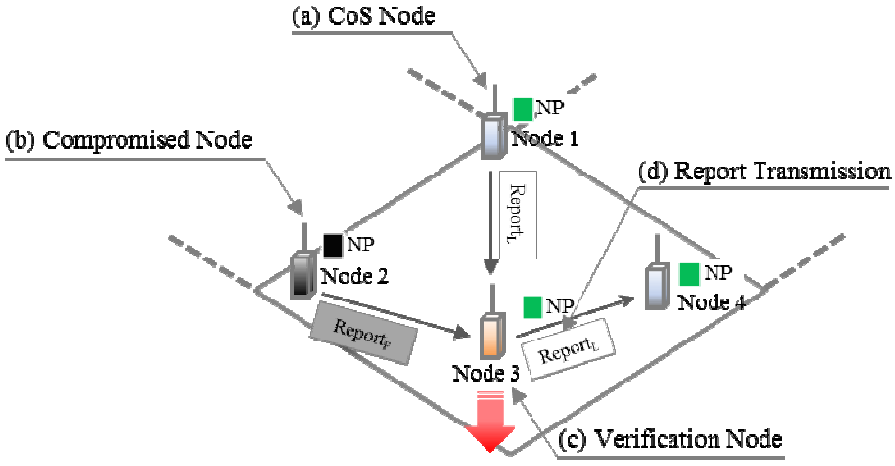


Figure 3. Detection against a false report injection attacks.

Figure 4 illustrates the detection of compromised nodes using an NP within a region against the false report injection attack. Node 1 (Figure 4-a) is a CoS node to transmit a legitimate report ($Report_L$), Node 2 (Figure 4-b) is a compromised node to inject a false report ($Report_F$), and Node 3 (Figure 4-c) is a verification node to drop the false report. Node 1 collects the MACs of its neighbors and verifies the MACs by using the NI after an event occurs. Node 1 then forwards the legitimate report, including the NP, event information, and MACs of its neighbors to Node 3. After receiving the report, Node 3 verifies the report by using NP and forwards it to Node 4 toward the base station (Figure 4-d). On the other hand, Node 2 injects a false MAC in a report about a non-existing event and transmits a false report including its false NP, which is captured in another region from a node, to Node 3. Node 3 authenticates the false report through its NP and filters out the false report against the false report injection attack because the false MAC is detected. Therefore, our proposed method effectively drops the false MACs and false reports to protect against the false report injection attack.

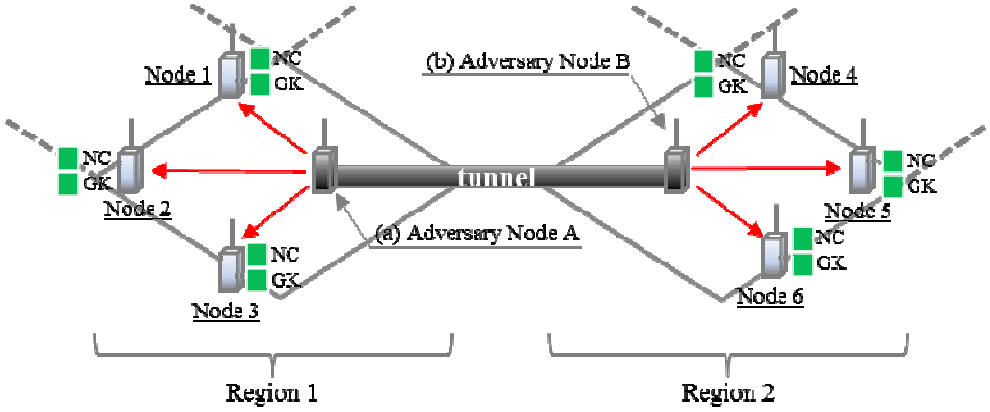


Figure 4. Detection against a wormhole attack.

Figure 5 presents the detection of two adversary nodes in two regions against the wormhole attack. Nodes A and B (Figures 5-(a) and (b)) are inserted by an adversary. The two adversary nodes send a false routing control message in order to change the routing paths to their neighbors without NC and GK. The adversary nodes communicate with each other for a fabrication or

elimination through a tunnel. In Region 1, the adversary node A (Figure 5-(a)) forwards false routing control messages without an NC and GK to Nodes 1, 2, and 3. In Region 2, Nodes 4, 5, and 6 are affected by adversary node B (Figure 5-(b)). After receiving the false routing control message, all of the affected nodes detect and drop the false routing control messages through their NC and GK against the adversaries. Therefore, our proposed method effectively prevents the false routing control message generated by the adversary nodes through an NC and GK against the wormhole attack.

4. EXPERIMENT RESULTS

Table 1. Parameters.

Parameter		Value
Number of nodes		500
Field Size		500×500 m^2
Number of compromised nodes		10
Percentage of false reports		10%
Number of adversary nodes		2
Size of transmission	Report	24 bytes
	MAC	1 byte
	Routing Control Message	12 bytes
Energy consumption	Transmit	16.56μJ/byte
	Reception	12.5μJ/byte
	MAC generation	15μJ/byte

The parameters used in the simulations are shown in Table 1. We generated false report injection attacks and wormhole attacks from 10 compromised nodes and two adversary nodes in the sensor network. The compromised nodes generated 10% false reports to try the false report injection attack, and the adversary nodes forwarded twice to their neighbors to try the wormhole attack. In addition, we generated 500 events with legitimate and false reports and the routing control message. In this case, the false reports and routing control message were done separately by the compromised nodes and the adversary nodes in the sensor network.

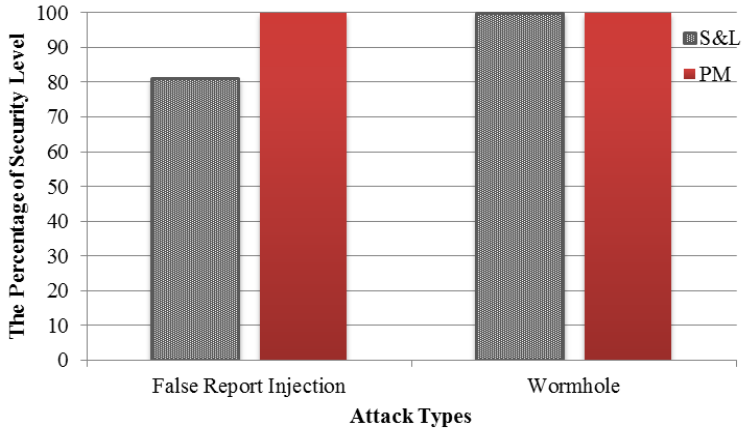
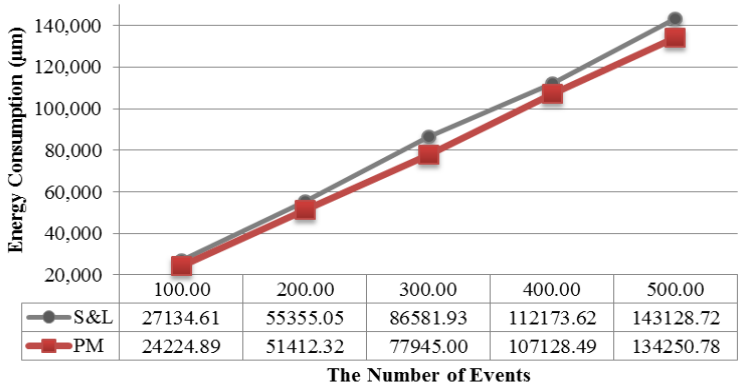


Figure 5. Security level of the sensor network.

Figure 6 shows the percentage of the security level for the simultaneous application of SEF and LEAP (S&L) and for our proposed method (PM) as the false report injection and wormhole attacks occur at the same time. In the false report injection attack, the proposed method improved the detection power of the false reports up to about 20% more than the simultaneous application of the two methods, because the false reports are filtered out early in the CoS nodes or verification nodes by using NKs and NPs. In the wormhole attack, the security levels of S&L and the proposed method are the same because they immediately detect the false routing control messages in all affected nodes. Therefore, the proposed method enhances the detection of the false report injection attack by about 20%, and maintains the security level against the wormhole attack as compared to the simultaneous application of SEF and LEAP.



	100.00	200.00	300.00	400.00	500.00
S&L	27134.61	55355.05	86581.93	112173.62	143128.72
PM	24224.89	51412.32	77945.00	107128.49	134250.78

Figure 6. Energy consumption of the sensor network

Figure 7 illustrates the energy consumption of S&L and the PM in the sensor network against the false report injection and wormhole attacks. When 100 events occur, the proposed method decreases the energy consumption of each node more than S&L. In addition, when 500 events occur, the proposed method saves energy resources about 8% more than the simultaneous application of SEF and LEAP. Thus, the proposed method improves the energy savings while maintaining the security level for multiple attacks in the sensor network. We expect that our method will prolong the lifetime of the entire sensor network against multiple attacks.

5. CONCLUSION AND FUTURE WORK

In the sensor network, in order to detect the false report injection attacks and wormhole attacks at the same time, we propose four types of keys in each node: a new individual key (NI), a new pairwise key (NP), a new cluster key (NC), and a group key (GK). The NI encrypts a MAC and an alert message when an event occurs and abnormal behavior is detected. The NP maintains a secure path and drops the false report. The NC detects false MACs and a false routing control message within a region. The GK encrypts and decrypts routing control messages to change the routing paths when a new node is inserted. In our proposed method, the NP and NC detect the false MAC or false report generated from a compromised node against the false report injection attack, and NC and GK prevent the false routing control message from an adversary node. In the experiment results, the security levels of our scheme improved about 20% for the false report injection attack as compared to the simultaneous application of SEF and LEAP, and maintained the same detection power against the wormhole attack as the simultaneous application of SEF and LEAP. In addition, the proposed method saves about 8% more energy when the multiple attacks occur at the same time than the simultaneous operation of the two methods. Therefore, our proposed method effectively detects the false report injection attack and the wormhole attack by

using four types of keys in the sensor network. In future work, we will apply additional simulation environments and perform experiments to test the robustness of our method against various attacks.

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. 2012-0002475).

REFERENCES

[1] Akyildiz, I.F., Weilian Su, Sankarasubramaniam, Y. & Cayirci, E., (2008) "A survey on sensor networks," Communications Magazine IEEE, Vol. 40. pp 102-114.
[2] Al-Karaki, J.N. & Kamal, A.E., (2004) "Routing techniques in wireless sensor networks: a survey," Wireless Communications, IEEE, Vol.11, No.6, pp 6-28.
[3] H.Y. Lee & T.H. Cho, (2010) "A Scheme for Adaptively Countering Application Layer Security Attacks in Wireless Sensor Networks," IEICE Transactions on Communications, Vol. E93-B, No. 7, pp 1881-1889.
[4] Culler, D., Estrin, D. & Srivastava, M., (2004) "Guest Editors' Introduction: Overview of Sensor Networks," Computer, Vol.37, No.8, pp 41-49.
[5] Fan Y., Luo, H., Songwu L., & Lixia Z, (2005) "Statistical En-route Filtering of Injected False Data in Sensor Networks," IEEE Journal Selected Area Communications, Vol. 23, No. 4, pp 839-850.
[6] Sencun Z., Sanjeev S., & Sushil J., (2003) "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," ACM Conference on Computer and Communications Security, pp 62-72.
[7] S.Y. Moon & T.H. Cho, (2012) "Key Index-Based Routing for Filtering False Event Reports in Wireless Sensor Networks," IEICE Transactions on Communications, Vol.E95-B, No.09, pp 2807-2814.
[8] P.T. Nghiem and T.H. Cho, (2010) "A Multi-path Interleaved Hop by Hop En-route Filtering Scheme in Wireless Sensor Networks," Computer Communications, Elsevier, Vol. 33, No. 10, pp 1202-1209.
[9] C. Karlof & Wagner, D., (2003) "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, Vol. 1, No. 2-3, pp 293-315.
[10] Crossbow technology Inc. http://www.xbow.com.
[11] Fan Y., Chen A., Songwu L., & Lixia Z, (2001) "A scalable solution to minimum cost forwarding in large sensor networks," Computer Communications and Networks, pp 304-309.

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 Cho received 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.