AN ENERGY EFFICIENT COUNTERMEASURE AGAINST MULTIPLE ATTACKS OF THE FALSE DATA INJECTION ATTACK AND FALSE HELLO FLOOD ATTACK IN THE 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
smnam@ece.skku.ac.kr
[2]College of Information and Communication Engineering, Sungkyunkwan University,
Suwon 440-746, Republic of Korea
taecho@ece.skku.ac.kr

ABSTRACT

Nodes are easily exposed from generated attacks on various layers because they compose simple functions in sensor networks. The false data injection attack drains finite energy resource in a compromised node, and the false HELLO flood attack threatens constructed routing paths in an adversary node. A localized encryption and authentication protocol (LEAP) was developed to prevent the aforementioned attacks through the use of four keys. However, when these attacks occur simultaneously, LEAP may not prevent damage from spreading rapidly throughout the network. In this paper, we propose a method that addresses these attacks through the use of four types of keys, including two new keys. We also improve energy consumption while maintaining a suitable security level. The effectiveness of the proposed method was evaluated relative to that of LEAP when multiple attacks occur. The experimental results reveal that the proposed method enhances energy saving by up to 12% while maintaining sufficient detection power.

KEYWORDS

wireless sensor networks, security attack detection, false data injection attacks, hello flood attacks.

1. INTRODUCTION

Wireless sensor networks (WSNs) supply economically feasible technologies for various applications based on wireless communication [1-2]. A WSN is composed of a large number of sensor nodes and a base station (BS) in a sensor field. The sensor nodes are used for sensing, computing, and wireless communication. The BS collects information from the sensor node throughout the network infrastructure. The nodes have a disadvantage in that they are captured and compromised due to their limited computation, communication, storage, and energy supply resources [1]. Thus, malicious attackers use various attacks to destroy the lifetime of the sensor network.

DOI : 10.5121/ijcsity.2013.1303

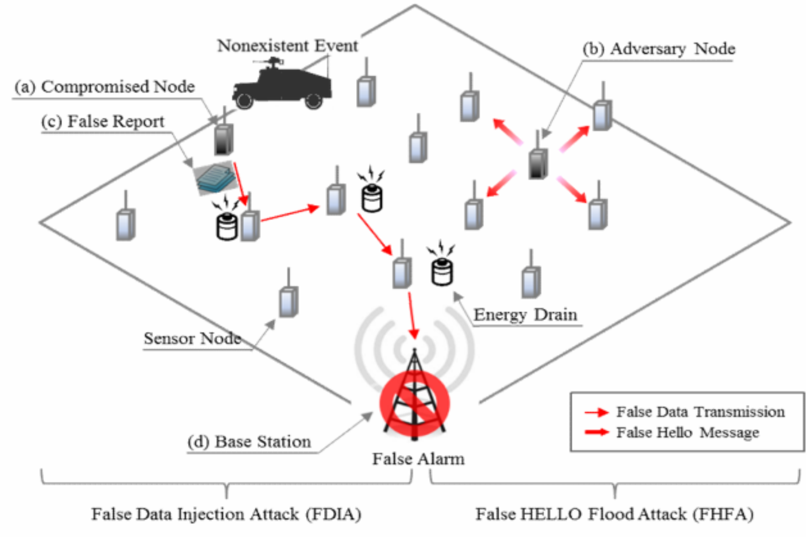


Figure 1. Multiple attacks: the false data injection attack and the false HELLO flood attack.

The generation of multiple attacks, such as the false data injection attack (FDIA) and false HELLO flood attack (FHFA), as they occur simultaneously in a sensor network is shown in Fig. 1. The FDIA generates false reports from the compromised node (Figure 1(a)) on the application layer, while the FHFA forwards false HELLO massages from an adversary node (Figure 1(b)) with its only ID on the network layer. As a consequence of the FDIA, the compromised node transmits a false report (Figure 1(c)) to the base station (Figure 1(d)), which drains energy resources from the intermediate nodes. Thus, the FDIA causes energy consumption in the sensor network due to the generation of the false report from the compromised node. Because of the FHFA, the adversary node forwards a false HELLO message to its neighbors, which ruins constructed routing paths. Thus, the FHFA induces the establishment of a false path due to the false HELLO messages from the adversary node.

To detect these attacks, Zhu et al. [5] proposed a localized encryption and authentication protocol (LEAP) that uses multiple keying mechanisms. LEAP establishes four types of keys for each node with confidentiality and authentication – an individual key for encrypting information, a pairwise key for maintaining secure paths, a cluster key for verifying a specific region, and a group key for encrypting a HELLO message. However, LEAP cannot effectively detect multiple attacks that occur on both the application layer and network layer at the same time because it verifies all data that are generated from the sender in the only base station.

In this paper, we propose a security method to effectively detect aforementioned attacks when they occur simultaneously in a sensor network. Our proposed scheme uses four types of keys: a new individual key set, a pairwise key, a new cluster key, and a group key. Thus, it enhances energy consumption in the sensor network while maintaining detection power when an FDIA and FHFA occur at the same time.

The remainder of this paper is organized as follows. Relevant research on the above attacks and the motivation for this work are described in Section 2. The proposed method is introduced in Section 3, and the optimization results are presented in Section 4. Finally, conclusions and future work are discussed in Section 5.

2. RELATED RESEARCH AND MOTIVATION

When the FDIA of an inside attack [2] is generated on an application layer, false data, including a false report of non-existent events, are injected into sensor network by the compromised node. The false data cause false alarms via multiple hops to the BS, and they drain the limited energy resources of forwarding nodes [4]. Ye et al. [5] proposed a statistical en-route filtering (SEF) scheme to detect and drop false reports during the forwarding process via multiple hops toward the BS. In the SEF, each of the detecting nodes generates a message authentication code (MAC). Multiple MACs are then attached to an event report in a center-of-stimulus (CoS) node that collects MACs from its neighboring nodes. As the report is forwarded, each node along a path probabilistically verifies the correctness of the MACs, and it drops the report if a forged MAC is detected. Yu et al. [6] presented a dynamic en-route filtering (DEF) method for the early detection and removal of both false reports and DoS attacks in a sensor network. In the DEF, event reports that include MACs allow for discernment between legitimate and fake reports, and intermediate nodes are guaranteed a legitimate report with their own authentication keys that are generated from one-way hash chains. Thus, DEF reduces unnecessary energy consumption by preventing the duplication of data based on the use of a cluster-based organization. Zhu et al. [7] proposed an interleaved hop-by-hop authentication (IHA) scheme using cluster-based organization. The method guarantees that false data are detected in the BS. The scheme proposed in this work will achieve early detection power through a new cluster key established between a sensing node and a CoS node. We will discuss how to detect false reports with early detection power in Section 3.

The FHFA of an outside attack [2] is generated on the network layer. An adversary node indiscriminately broadcasts HELLO packets to announce itself to its neighbors within its radio range so that the neighbors believe the adversary node belongs to them. Zhu et al. [3] proposed multiple keying mechanisms to detect false HELLO messages through confidentiality and authentication in the sensor network. The scheme supports the establishment of four types of keys for each node – an individual key for encrypting information, a pairwise key for maintaining secure paths, a cluster key for a specific cluster, and a group key for encrypting messages. A cluster key and a group key are detected as HELLO messages and forwarded for joining a node in a specific region of the network. Hamid et al. [9] presented a probabilistic secret sharing protocol where secrets shared between two sensor nodes not exposed to any other nodes. The protocol builds these secrets to establish a new pairwise key for authentication, and it designs multi-path routing. The scheme proposed in this work uses four types of keys to efficiently detect false HELLO messages in the entire network.

2.2. Motivation

To ensure security in a WSN, various countermeasures are used to detect both an FDIA that drains the energy of each node and an FHFA that ruins the routing path within a specific region. Conventional countermeasure methods are usually aware of only an attack, so the operation of various countermeasures causes the life of each node in the sensor network to be shortened. In addition, an adversary injects multiple attacks through compromised nodes or a powerful laptop-level node (adversary node) [2]. A diversity of countermeasures and multiple attacks constantly consume the limited energy resources of each node in the sensor network. Therefore, we propose a method of countermeasures to prevent both an FDIA and FHFA from being simultaneously generated in the sensor network.

3. PROPOSED METHOD

3.1. Assumption

We assume a static sensor network, where the sensor nodes are fixed in a sensor field. The sensor network consists of a BS and a large number of small nodes, such as Berkeley MICA2 motes [10]. The initial paths of the topology are established through directed diffusion [11] and minimum cost forwarding algorithms [12]. It is further assumed that every node forwards data packets toward the BS. An attacker simultaneously implements a FDIA and a FHFA through compromised nodes and an adversary node in the sensor network.

3.2. Overview

FDIA and FHFA attacks consume energy and destroy the routing paths of each node. In the proposed method, four types of keys in the sensor network are used to detect such attacks as they are simultaneously generated. Each node establishes a new individual key set for shared with the BS, a pairwise key for shared with another node, a new cluster key for shared with its neighboring node, and a group key for shared by all the nodes in the network. The devised scheme employs the new individual key set and the new cluster key based on previous work [5] to detect an FDIA in a CoS node as a forged MAC occurs from a compromised node. The new cluster key and a group key based on previous research [3] are used to detect an FHFA in affected nodes as a false HELLO message occurs from an adversary node. After detecting these attacks, the proposed method filters out both false data, including the false report, and false HELLO messages. Therefore, we effectively prevent FHFAs and FDIAs using four types of keys as false MACs or false HELLO messages are simultaneously generated. We now discuss each of the four keys and describe the reasons for including them in the proposed method.

3.3. Detection of FDIA and FHFA

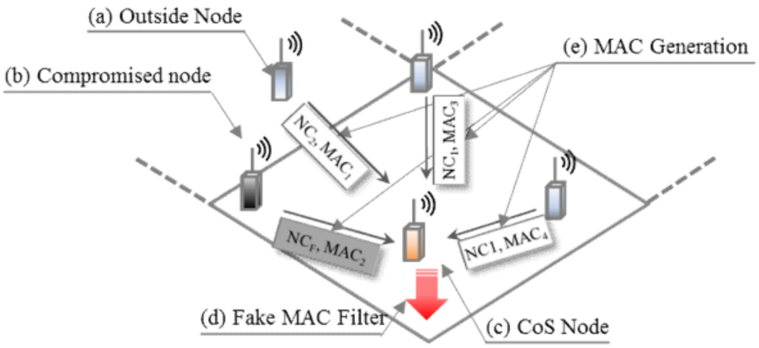


Figure 2. Forged MAC filtering through the NC.

The process of filtering a forged MAC through the NC of the CoS node as an event occurs within a cluster region is shown in Figure 2. There are two nodes – including NC_1 – within the cluster, a node including NC_2 (Figure 2(a)) out of the cluster, and a compromised node (Figure 2(b)) including NC_F within the cluster region. When an event occurs in the region, sensing nodes that detected the event transmit their NC and MAC to the CoS node (Figure 2(c)). The CoS node then verifies the MAC so as to filter out a forged MAC and the MAC of NC_2. As shown in Figure 2, NC_F is produced from the compromised node via an adversary, while NC_2 is generated from an outside node (Figure 2(a)) in out of the region. The CoS node drops NC_F and NC_2 to generate a legitimate report. That is, our proposed method improves the detection power against an FDIA through the use of the NC.

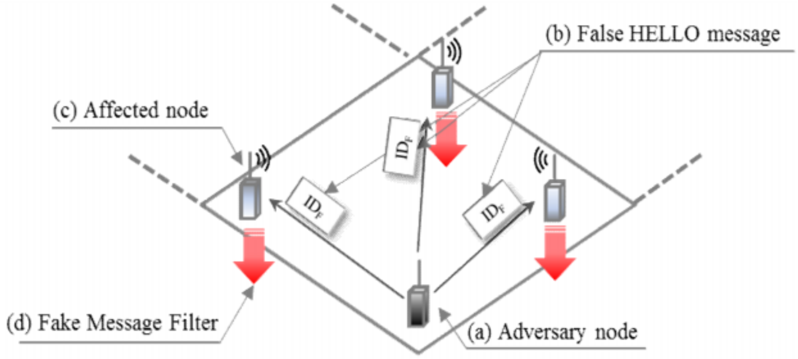
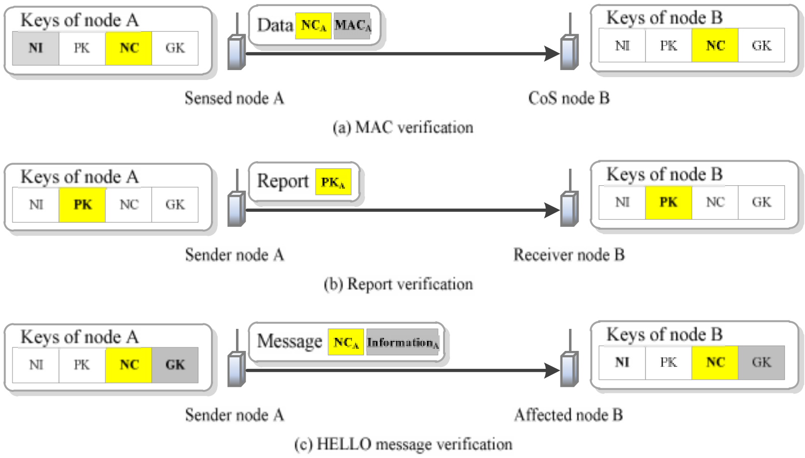


Figure 3. False HELLO message detection through the NK and GK.

False HELLO message detection using the NC and GK of each node within a region is shown in Figure 3. In the region, a malicious attacker inserts an adversary node (Figure 3(a)), which forwards a false HELLO message (Figure 3(b)) to the neighboring nodes (Figure 3(c)). These neighboring nodes are affected by the false message. The affected nodes verify the false message using their NC and GK. The nodes drop the false HELLO message of the adversary node after the authentication process is complete (Figure 3(d)). If the message succeeds in being authenticated, the nodes decrypt the message to renew their routing path. That is, our proposed method using the NC and GK of affected nodes to detect a false HELLO message as it is generated from an adversary node.



(a) MAC verification

(b) Report verification

(c) HELLO message verification

Figure 4. Key authentication between two nodes.

Three cases for MAC verification, report verification, and HELLO message verification are shown in Figure 4. In Figure 4(a), the sensed node encrypts the information of an event using NI_A, and then it transmits MAC_A with the information, as well as NC_A to the CoS node B. After receiving MAC_A, the CoS node B verifies NC_A using NC_B to avoid a forged MAC in a report. If a forged MAC is detected through NC_B, NC_B drops the forged MAC_A. Thus, an FDIA is detected using an NC as the sensed node generates a MAC. In Figure 4(b), a sender node uses its PK to check the condition of a receiver node before transmitting data. Before sender node A transmits data, the PK_A identifies the normal node of the receiver node B through the authentication of PKs. If an adversary node is inserted without keys, a report is not sent out from sender node A, and the sender makes a detour to another path. If the verification of PK is complete between two nodes, sender node A forwards the report to receiver node B. Thus, we maintain the secure path of each node using PKs while transmitting a report. In Figure 4(c), a receiver node verifies a HELLO message using its NC and GK between a node and its neighbors. Sender node A encrypts the HELLO message using its GK, and the sender node A transmits it with NCA to receiver node B. Receiver node B verifies the HELLO message using its NK_B and GK_B. If the message is fake, receiver node B drops the messages and notices it to the BS. Thus, we prevent false HELLO messages using NC and GK. As illustrated in Figure 4, we propose the use of four types of keys between two nodes for MAC authentication, report authentication, and HELLO message authentication. Therefore, our devised scheme effectively detects multiple attacks of the FDIAs and FHFAs that occur simultaneously.

4. PERFORMANCE ANALYSIS

The simulation parameters used to compare the proposed method to LEAP. The sensor network in the simulation environment consists 500 nodes over a field size is 500 × 500m2. Each node owns an NK with 10 keys, a PK, a CK, and a GK. We assumed that 10 nodes are compromised for generating the FDIA, and one node is used as an adversary node produces the FHFA with 5. Thus, 900 events were generated, including normal reports, false reports, and false HELLO messages. The events were generated separately by the compromised nodes and the adversary node in the sensor network. Each node consumes 16.56μJ/12.5μJ to transmit/receive a byte, and each MAC generation consumes 15μJ [5]. The size of a report 24 bytes, HELLO message is 12 bytes, and MAC is 1 byte [3]-[5].

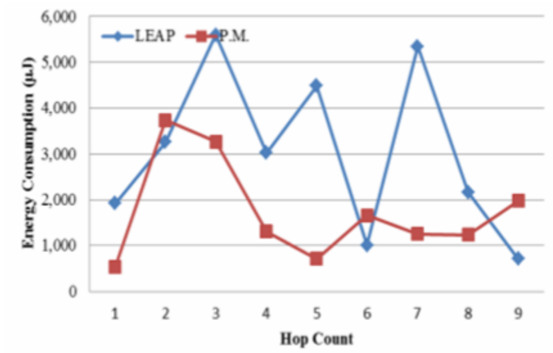


Figure 5. Energy performance as only false report occurs.

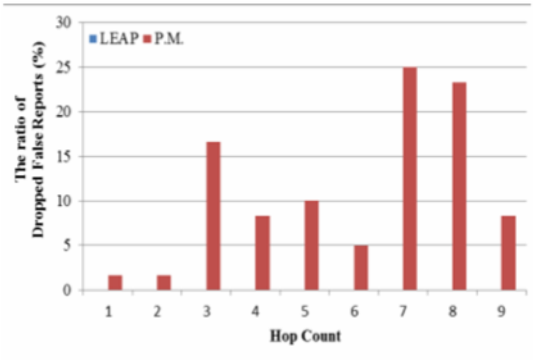


Figure 6. Filtering performance as only false report occurs.

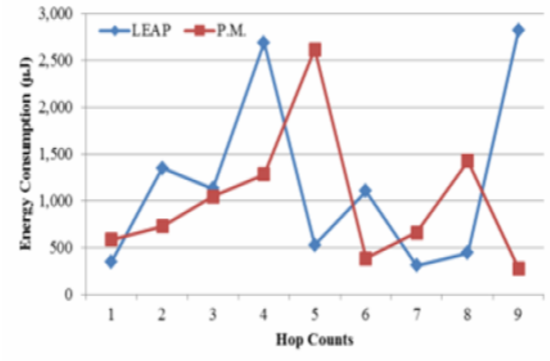


Figure 7. Energy performance as only false HELLO message occurs.

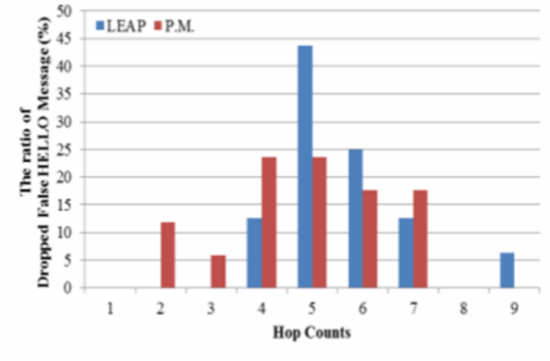
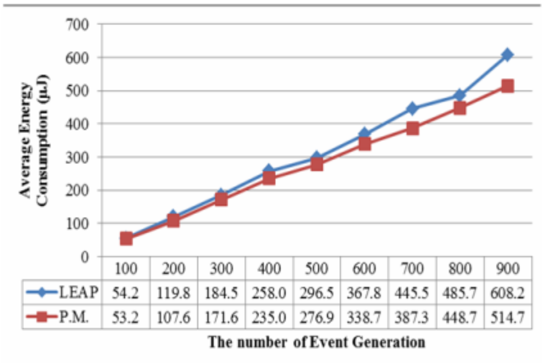


Figure 8. Filtering performance as only false HELLO message occurs.

Comparisons of the energy consumption and dropped false report ratio obtained with the proposed method and LEAP when only false reports are forwarded in the sensor network are shown in Figure 5 and Figure 6, respectively. In Figure 5, the proposed method saves more energy than LEAP because the NC of each node drops a false MAC before attaching a MAC in the report. On the other hand, LEAP transmits a false report to the BS as a forged MAC occurs. In Figure 6, the proposed method uses the NC to detect false MACs better than LEAP. With LEAP, false reports are not detected while forwarding progresses to the BS because the individual key of LEAP verifies false reports in the BS.

Comparisons of the energy consumption and dropped false HELLO message ratio obtained with the proposed method and LEAP when only false HELLO messages are forwarded in the sensor network are shown in Figure 7 and Figure 8, respectively. The simulation results acquired with the proposed method and LEAP are almost the same. Thus, the proposed method improves the detection of an FDIA when compared to LEAP, and offers a similar level of detection with respect to an FHFA.



	100	200	300	400	500	600	700	800	900
LEAP	54.2	119.8	184.5	258.0	296.5	367.8	445.5	485.7	608.2
P.M.	53.2	107.6	171.6	235.0	276.9	338.7	387.3	448.7	514.7

Figure 9. Comparison of the average energy consumption against FDIA and FHFA.

A comparison of the average energy consumption of the two methods as multiple FDIA and FHFA attacks occur at the same time in a sensor network is shown in Figure 9. As the number of events increases above 200, the average energy consumption of LEAP is about 10% higher than that of the proposed method (P.M) due to mutual security countermeasures. When 900 events have occurred, the proposed method saves an average of 93.5µJ of energy when compared to LEAP. That is, energy consumption with the proposed method is lower than that of LEAP as attacks are simultaneously generated. Specifically, the proposed method improves energy consumption by up to 12% when compared to LEAP, while maintaining the detection power.

5. CONCLUSION AND FUTURE WORK

In this work, we proposed a security method with four types of keys, including two new keys, for effectively detecting attacks as FDIA and FHFA are simultaneously occurs in a sensor network. A NI for each node is used to encrypt a MAC and information, and a NC is used to detect a false MAC and verify a specific cluster within a region. Our method selectively loads the four types of keys on a report or message as a real event occurs. Simulation results showed that the proposed method leads to an increase in energy savings as compared to LEAP. Specifically, our proposed method enhances energy savings by an average of about 12% for each node in the sensor network more than LEAP. Therefore, we expect that the devised scheme will effectively detect FDIAs and FHFAs generated at the same time, while enhancing energy in each node. In the future work, we will run additional simulation scenarios and perform various experiments for robustness with AI algorithms against other 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. 2013R1A2A2A01013971)

REFERENCES

[1] Akyildiz, I.F., Weilian Su, Sankarasubramaniam, Y., and Cayirci, E., "A survey on sensor networks," Communications Magazine, IEEE, vol.40, no.8, pp. 102- 114, Aug 2002.

[2] Zhu, S., Setia, S., and Jajodia, S., “LEAP: efficient security mechanisms for large-scale distributed sensor networks,” Proceedings of the 10th ACM conference on Computer and communications security, ACM, 62-72, 2003.

[3] Xiaojiang Du; Hsiao-Hwa Chen, "Security in wireless sensor networks," Wireless Communications, IEEE, vol.15, no.4, pp.60-66, Aug. 2008.

[4] H.Y. Lee and T.H. Cho, "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, Jul. 2010.

[5] Zhen Yu and Yong Guan, "A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks," Networking, IEEE/ACM Transactions on, vol.18, no.1, pp.150-163, Feb. 2010.

[6] Sencun Zhu; Setia, S., Jajodia, S., and Peng 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, pp. 259- 271, 9-12 May 2004.

[7] Sencun Zhu, Setia, S., Jajodia, S., and Peng 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, vol., no., pp. 259- 271, 9-12 May 2004.

[8] Karlof, C. and Wagner, D., "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, pp. 113- 127, 11 May 2003.

[9] Hamid, A., Mamun-Or-Rashid, and Choong Seon Hong, "Defense against lap-top class attacker in wireless sensor network," Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, vol.1, pp.5 pp.-318, 20-22 Feb. 2006.

[10] Crossbow technology Inc., “http://www.xbow.com”

[11] Intanagonwiwat, C., Govindan, R., and Estrin, D., “Directed Diffusion: A scalable and robust communication paradigm for sensor networks,” MOBICOM, ACM, pp. 56-67, 2000.

[12] Fan Ye, Chen, A., Songwu Lu, and Lixia Zhang, "A scalable solution to minimum cost forwarding in large sensor networks," Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on, pp.304-309, 2001.

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.