An Improved Method for Probabilistic Voting-based Filtering using Blacklists in Sensor Networks

Jong Kun Lee, Su Man Nam and Tae Ho Cho

Sungkyunkwan University
College of Information and Communication Engineering, Sungkyunkwan University
Suwon 440-746, Republic of Korea
soulmatek87@gmail.com, smnam@ece.skku.ac.kr, taecho@ece.skku.ac.kr

Abstract

False report injection attacks and false vote injection attacks can be perpetrated easily by malicious attackers on the application layer in a wireless sensor network. These attacks drain the lifetime of the sensor nodes and prevent the forwarding of legitimate reports in the sensor network. A probabilistic voting-based filtering scheme (PVFS) was proposed in order to drop these two types of attacks simultaneously in intermediate cluster heads. Before transmitting a report, the scheme selects verification nodes within the intermediate cluster nodes to detect false votes attached from compromised nodes. In this paper, we propose a method to improve the detection power and energy savings by using a blacklist in every cluster head. The blacklist stores each compromised node ID and false key. The performance of the proposed method against these attacks was evaluated and compared to that of PVFS. The simulation results reveal that the proposed method enhances the average energy consumption and security level of each cluster head as compared with PVFS.

Keywords: *Wireless Sensor Network (WSN), Probabilistic Voting-based Filtering Scheme (PVFS)*

1. Introduction

The newest technology provides economically and technologically efficient wireless sensor networks (WSNs) for the development of low-power, battery-operated devices which combine special-purpose computing with low-power sensing and wireless communications capabilities [1]. A WSN consists of a very large number of sensor nodes with limited processing power, little storage space, restricted energy lifetime, and narrow bandwidth [2]. These sensors have a significant disadvantage due to the possibility of being captured or compromised due to their limited capabilities [3]. With a variety of applications, such as forest fire monitoring or military surveillance, these sensor nodes are deployed over vast areas to detect events of interest and to transmit reports over multi-hop paths to a single collection point called the “sink” (Figure 1-e).

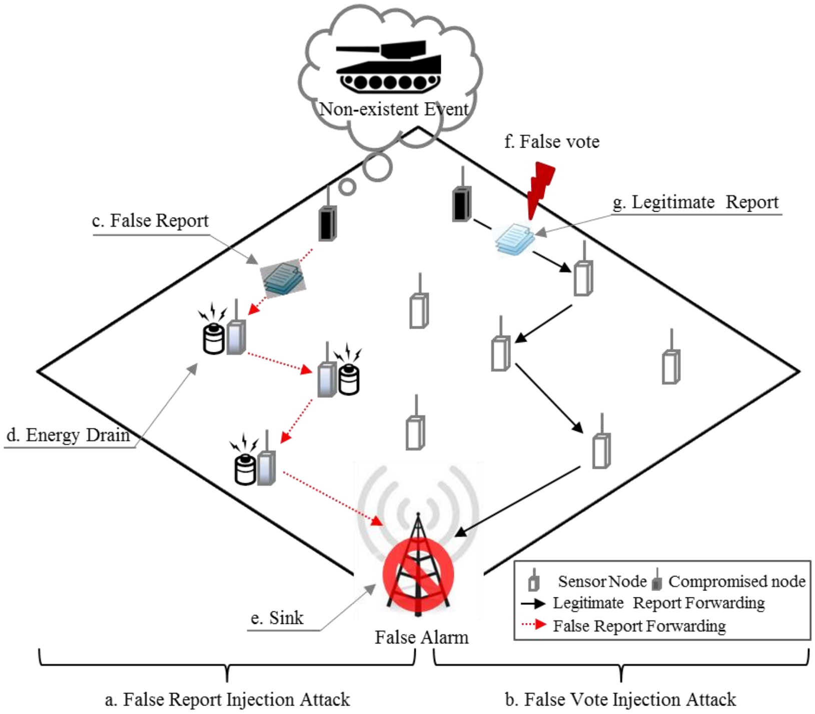


Figure 1. False Report and Vote Injection Attacks

Figure 1 shows an example of a false vote injection attack (called a “false votes on real reports attack” in [5]) and a false report injection attack (called a “fabricated report with false votes attack” in [5]) in a sensor network. As shown in Figure 1-a, a compromised node generates a false report (Figure 1-c) without detecting an event to drain the energy resource of the intermediate nodes (Figure 1-d). In addition, a false alarm occurs as the false report arrives at the sink (Figure 1-e). In Figure 1-b, the other compromised node injects a false vote (Figure 1-f) in a legitimate report (Figure 1-g) to drop it within intermediate nodes. Thus, users get unnecessary information from the sensor network through these attacks. The detection of an en-route discarding of fabricated reports injected by compromised nodes is a significant challenge, since the attacker will know all of the security information regarding the compromised nodes.

To detect the false report injection attack and the false vote injection attack, *Li et al.* [5] propose a probabilistic voting-based filtering scheme (PVFS) to effectively eliminate false reports and votes by using selected intermediate cluster-heads (CHs) as verification nodes. We propose to improve the power of detection of multiple attacks by using a blacklist in every intermediate CH, more than used by PVFS. Our proposed method reduces the energy consumption of each node and improves the security level in the sensor network against the false report injection attack and the false vote injection attack.

The remainder of this paper is organized as follows. The background and purpose are described in Section 2. The proposed scheme is introduced in Section 3, and the simulation results are described in Section 4. Finally, the conclusion and future work are discussed in Section 5.

2. Background and Motivation

In this section, we briefly describe PVFS and the motivation for this work.

2.1. PVFS (Probabilistic Voting-based Filtering Scheme)

PVFS is proposed here in order to improve security within intermediate CHs against false report injection attacks and false vote injection attacks during the forwarding process. On the basis of the en-route filtering scheme, PVFS combines cluster-based organization, probabilistic key assignment, and voting methods, as shown in Figure 1. In cluster-based organization, the WSNs are broken into clusters in order to organize sensor nodes within one hop distance, a set of keys is bound to each cluster, and a designed probability is used in order to select intermediate cluster-heads as verification nodes. In the probabilistic key assignment, the sink assigns L (the number of keys for one cluster) keys to every CH from a global key pool. A node will use this key as the generation key to generate a vote for an event report. The CH then randomly distributes the other keys to the other nodes.

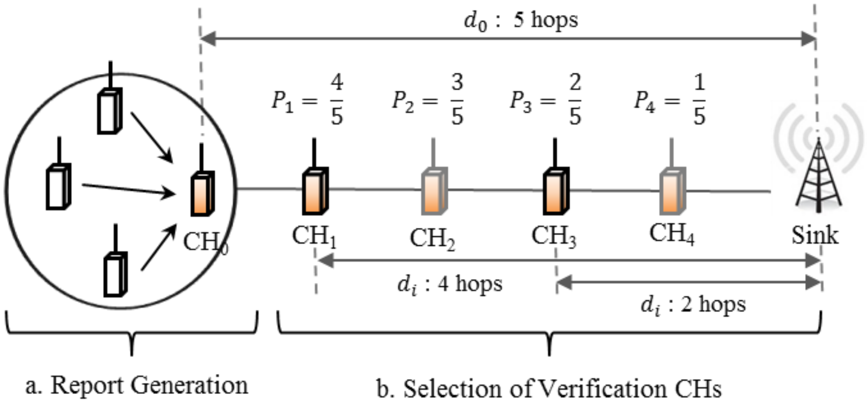


Figure 2. Report Generation and Selection of Verification CHs

Figure 2 illustrates the report generation phase and the selection of the verification CHs in a path. During report generation (Figure 2-a), CH_0 generates a report describing the event and broadcasts it in that cluster. The other nodes in that cluster cast votes using their own generation keys. When CH_0has received all of the votes, it randomly chooses a pre-determined number of votes within a cluster and appends them to the report. CH_0 then forwards the report to its upstream neighbors. In the selection of the verification CHs (Figure 2-b), before forwarding the report CH_0 selects an intermediate CH_i to be a verification node with a probability $\mathrm{P} = d_i/d_0$. CH_1 has a probability $P_1 = 4/5$ to be a verification node of CH_0, and CH_3 has a probability $P_3 = 2/5$ to be a verification node of CH_0. Both CH_1 and CH_3 get verification keys from CH_0.

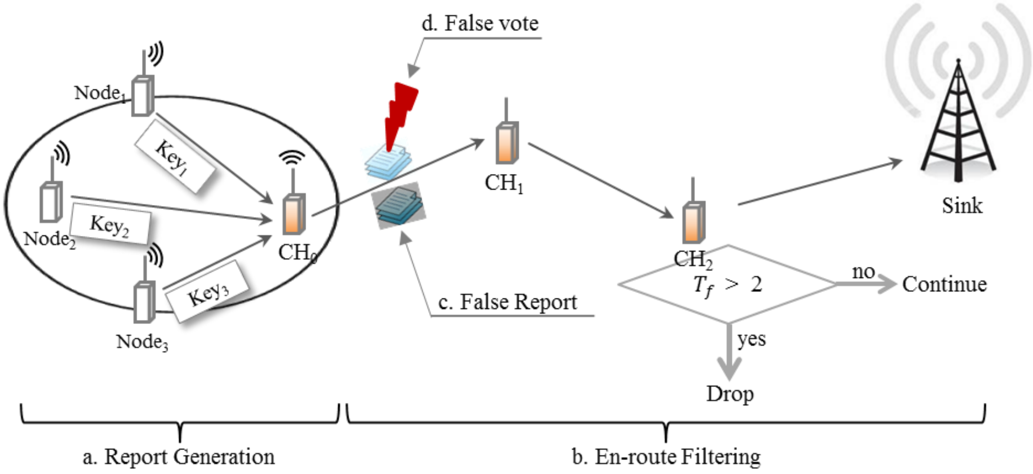


Figure 3. The Detection and Elimination of the False Report and Vote

Figure 3 shows the phases of report generation and en-route filtering from CH_0 and the sink. During report generation (Figure 3-a), CH_0 randomly selects votes from its nodes as an event occurs. If nodes 1 and 2 are compromised, the report is fabricated by two false votes in CH_0. In en-route filtering (Figure 3-b), the selected verification CHs verifies the votes by counting the T_f of the report against the false report injection attack and the false vote injection attack. The forwarded false report is dropped in either CH_1 or CH_2 as $T_f = 2$ is reached, as shown in Figure 3-c. If there are no pairwise keys at the verification node, the report is forwarded over the routing paths. When $T_f = 1$, the verification node does not drop a report, and the report is also forwarded to the routing paths until the condition $T_f = 2$ is satisfied. On the other hand, if a legitimate report (Figure 3-d) includes a vote from a compromised node$_1$ in CH_0, it is also transmitted via CH_1 and CH_2 toward the sink after it is generated. The chosen verification cluster heads CH_1 and CH_2 safely forward the legitimate reports into the sink even though $T_f = 1$ has been reached. Therefore, PVFS can detect the false votes of a source CH in selected intermediate CH_s against multiple attacks.

2.2. Motivation

False report injection attacks and false vote injection attacks can quickly drain the lifetime of the entire sensor network. PVFS is proposed to detect these attacks in the verification CHs before they arrive at the sink. The energy consumption of each node must be decreased through early detection of multiple attacks. Our proposed method detects fabricated votes by using a blacklist in an intermediate CHs, which is more effective compared with the original PVFS. This method drops the fabricated vote by using the blacklist as the forged votes are detected, even when the intermediate CHs are unselected. Thus, the proposed method saves energy by detecting and preventing the forged votes that are generated from the compromised node. As a result, our proposed method prolongs the lifetime of the network and maintains a strong detection power of the sensor network.

3. Proposed Method

3.1. Assumptions

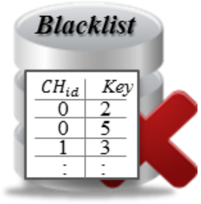
We consider a large-scale sensor network in which none of the nodes in the sensor network moves after the initial deployment. We assume that the attacker cannot generate enough true votes for a fabricated report, and that, for a very short period of time, no node is compromised at the start of sensor deployment. We complete the cluster formulation, the key distribution from the key pool, and the route discovery without being attacked. The sink cannot be compromised and knows the estimated distance to each cluster, as well as the energy consumption.

3.2. Overview

In this paper, the proposed method improves the lifetime of the entire network using black lists based on PVFS. Every cluster head operates a black list to detect false votes against the false report injection attack and the false vote injection attacks. When every report arrives in an intermediate CH, its black list uses to verify every vote in the report. If an event occurs within a cluster including compromised nodes, they inject votes as a CH generates a report. The votes in the report are then verified in an intermediate node using its black list, even though the intermediate CH is unselected. In addition, selected intermediate CHs verify the false report through their keys of a source CH. If $T_f = 2$ is reached in an intermediate CH, the CH drops the false report that the false report injection attack is tried. On the other hand, if $T_f = 1$ is reached in an intermediate CH using its black list and keys of the source CH, the CH distinguishes a legitimate report that the false vote injection attack is tried. Therefore, our proposed method enhances security level of the intermediate CH s and saves energy consumption of each node.

3.3. Proposed Method

Our proposed method uses a blacklist of each intermediate CH for early detection of the votes in a report generated during the forwarding processes. The blacklist stores information regarding CH_{ID} and Key_{ID} after detecting false votes in an intermediate CH. The CH selects votes within the same cluster to generate a report sent to the sink, and the report is then forwarded. When the report arrives at a selected verification CH, the CH counts the number of false votes if false votes were detected in the report. The verification CH then stores the false vote information in its blacklist. A report including the false votes is passed to the CH that owns the false vote information in the blacklist, and the CH verifies the report using the blacklist, even if it is not a selected verification CH. In this way, the proposed method increases security against multiple attacks over PVFS, since every intermediate CH improves the security level through the blacklist.



CH_{id}	Key
0	2
0	5
1	3
:	:

Figure 4. Blacklist Structure

Figure 4 shows the blacklist structure. The blacklist has two types of data, namely CH_{ID}(CH_{ID}: Unique cluster ID) and Key. When false votes or a fabricated report are detected, the CH_{ID} and Key_{ID} information are stored on the blacklist. In the detection phase, the blacklist is checked to determine whether the blacklist has a pair-wise key with a report that has votes. When the same key exists in the blacklist, a compromised node has been detected. The threshold value, T_f, is then checked. If there is no pair-wise key in the blacklist, this scheme verifies the vote or report using the individual verification key.

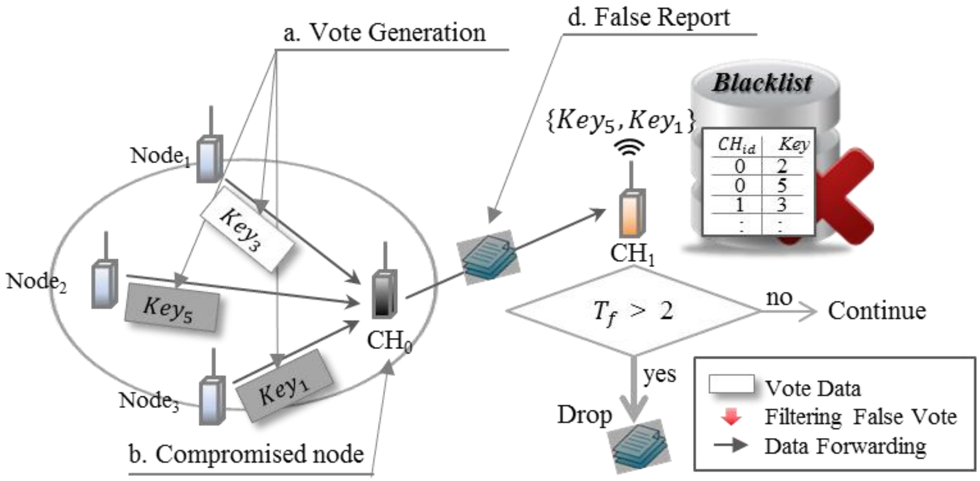


Figure 5. Detection of the False Report Injection Attack

Figure 5 shows the case in which a verification node detects a false report injection attack and updates CH_{ID} and Key_{ID} in its blacklist. Within the cluster region, there are two type nodes: three normal nodes, a CH of a compromised node (Figure 5-b). If the compromised node fabricates a report about a non-existing event, it has to inject two false votes (a value of 3 is used in this paper). The compromised CH forwards a false report (Figure 5-d) to drain energy resources of intermediate CHs. After CH_1 receives a report during the verification sequence, it checks its blacklist to see if the blacklist has the same key as a report that has votes. A compromised node is detected if the same key is in the blacklist. If the key in the blacklist is not the same as that in a report, the scheme verifies the vote using the verification key. Node$_3$ is thus detected as having been compromised. CH_1 updates its blacklist and the number of recorded false votes, and also checks to see if the number of false votes has reached the threshold, and decides whether or not to drop the report. If the predefined threshold, T_f, has not been reached, CH_1 continues forwarding the report. During the forwarding phases, the report is dropped when T_f has been reached. The sink performs the final verification on the received reports. The sink knows all of the keys, so is capable of verifying every vote in the report and can make a final decision. In this way, the sink serves as the final guard.

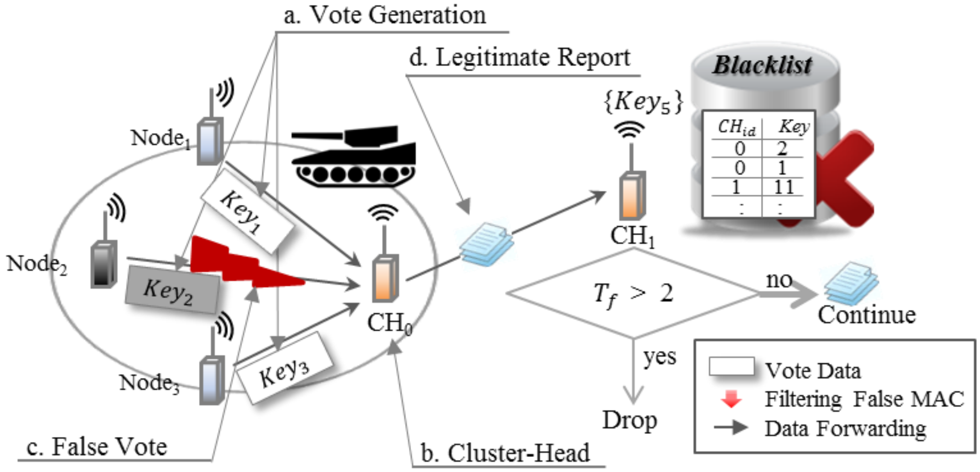


Figure 6. Detection of the False Vote Injection Attack

Figure 6 shows the detection of a false vote injection attack. False vote injection attacks prevent the reporting of important information in the field. Figure 6 shows the case in which a verification node detects a false vote injection attack. As an example, consider the situation in which a node that owns Key_5 has been compromised and launches false votes on a real reports attack. The node gives a false vote for the real report (Figure 6-d) of CH_0. If CH_0 still selects votes with *i* = 1, 2, 3, CH_1 will find that the vote with *i* = 2 is a false vote (Figure 6-c). However, the report will not be dropped because $T_f = 2$ has not yet been reached. In this method, this scheme checks its blacklist during the verification sequence to see if the blacklist has a key that is the same as the key for a node that made the false vote. A compromised node is detected if the same key exists in the blacklist. If the key does not match a key in the blacklist, it verifies the vote using the verification key. In this case, the real report could still reach the sink. If a compromised node tries to send a false vote, then the message can still reach the sink since only one vote is wrong and the threshold has not yet been reached. The verification node is set up so that it will not drop a report immediately when it finds a false vote; instead, it will simply record the result. Only when the number of verified false votes reaches a designated threshold will a report be dropped. Therefore, our proposed method improves the energy consumption of each node by using the early detection power of the blacklist. When event reports frequently occur, the probability of a false report may be increased, and each blacklist will have more data regarding compromised nodes. Thus, our proposed method detects the false report early on and conserves the energy consumption of each node.

4. Performance Analysis

In this section, we explain the simulation results of the proposed method. This simulation was performed to show the energy efficiency of the proposed method compared with that of PVFS. The simulation included several virtual environments. The first is a sensor field that is 100 m wide and 100 m tall. Within this sensor field, 10 cluster heads and 90 general sensor nodes are randomly deployed. A sink node in this sensor field has 100 keys in the global key pool. The global key pool was divided into 10, 8, 6, or 4 partitions, and each partition uniformly includes 10 keys. The sensor node consumes 16.25/12.5 μJ to transmit/receive a byte, and each vote consumes 15 μJ for verification. The event report packet is 24 bytes, and a vote is 1 byte. The number of event occurrences is 1,000.

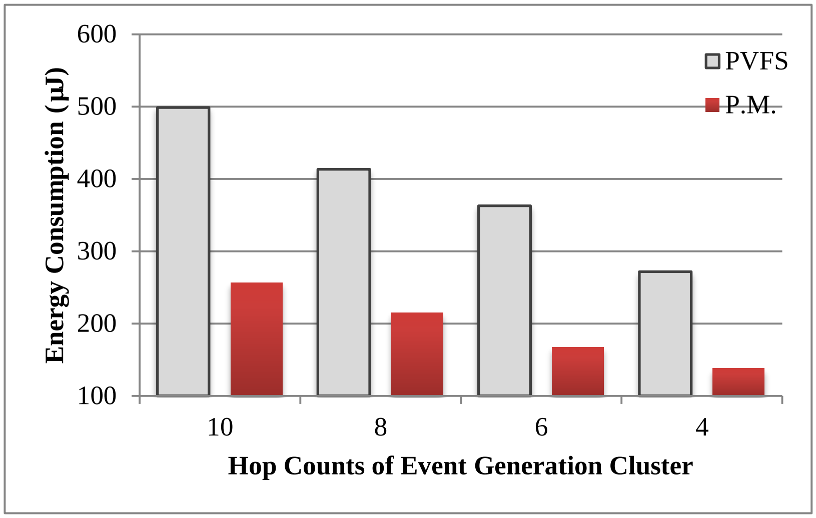


Figure 7. Comparisons of Energy Consumption in PVFS and the Proposed Method

Figure 7 shows the energy consumption per hop count of the event generation cluster in comparison with the original PVFS. The proposed method shows less energy consumption than the original PVFS. That is, the proposed method detects false reports earlier than the original PVFS as the forged votes consistently occur from compromised nodes. As a result, the security level of the proposed method is improved more than PVFS. Our method reduces energy consumption by reducing unnecessary energy waste, such as repetitive non-existent event reports. Thus, the proposed method saves the energy up to average 192.5㎛ as compared with PVFS.

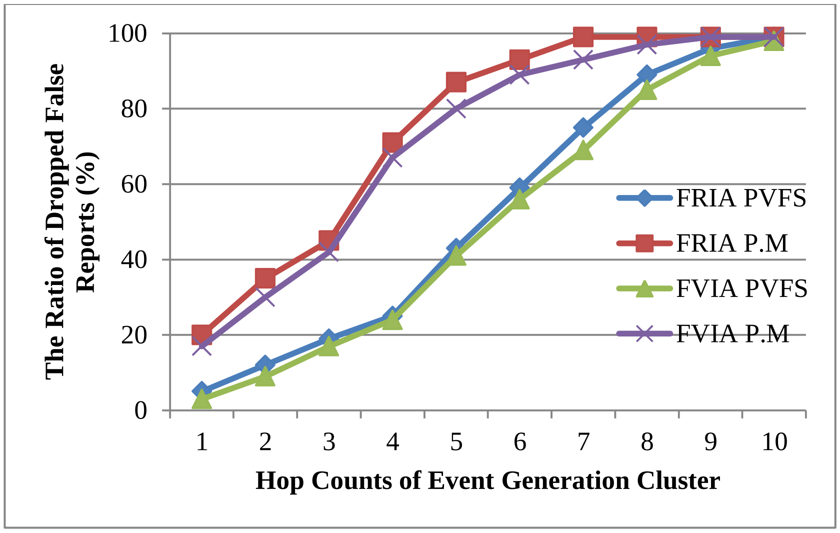


Figure 8. The Ratio of Dropped False Votes in PVFS and the Proposed Method

Figure 8 shows the ratio of dropped false reports per hop count of the event generation cluster in comparison with the original PVFS. The proposed method shows a higher ratio of dropped false reports than the original PVFS. That is, the proposed method detects false reports earlier as the forged votes consistently occur from compromised nodes than the original PVFS. As a result, the proposed method enhances the security level of each node more than PVFS. Therefore, simulation results of our proposed method shows improved the energy saving and security level of each node through the blacklist in the sensor network.

5. Conclusion and Future Work

WSN are often deployed in unattended environments, thus leaving these WSNs vulnerable to false data injection attacks. In these attacks, the attacker injects fabricated reports into the network through compromised nodes, with the aim of deceiving the sink or draining the resources of the sensor nodes. In this paper, we propose a method which uses a blacklist system with the PVFS to increase energy efficiency with improving security performance. This method stores the information from the compromised node during the verification sequence, and later decides whether or not the node is compromised without verification. The simulation result demonstrates the ability of this method to detect and verify a fabricated report, and guarantees greater energy efficiency. Future research will be focused on optimizing the proposed method and applying it to various en-route filtering schemes.

Acknowledgements

This research was supported by the 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] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A Survey on Sensor Networks”, IEEE Communication Magazine, **(2002)** August, pp. 102-114

[2] J. N. Al-Karaki and A. E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey”, IEEE Wireless Communications, vol. 11, Issue 6, (2004) December, pp. 6-28.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, no. 2-3, **(2003)**, pp. 293-315. [Online]. Available: http://www.cs.berkeley.edu/-daw/papers/.

[4] B. Przydatek, D. Song and A. perrig, “SIA: Secure information aggregation in sensor networks”, Proc. Of CCNC, vol. 23, **(2004)** January, pp. 63-98.

[5] F. Li and J. Wu, “A probabilistic voting-based filtering scheme in wireless sensor networks”, In Proceedings of International Conference on Wireless Communications and Mobile Computing, Vancouver, BC, Canada, **(2006)** July 3-6, pp. 27-32.

[6] C. I. Sun, H. Y. Lee and T. H. Cho, “A path selection method for improving the detection power of statistical filtering in sensor networks”, J. Inf. Sci. Eng., vol. 25, **(2009)**, pp. 1163-1175.

[7] F. Ye, H. Luo and S. Lu, “Statistical en-route filtering of injected false data in sensor networks”, IEEE J. Sel. Area. Commun., vol. 23, **(2005)**, pp. 839-850.

[8] H. Y. Lee and T. H. Cho, “Fuzzy-based path selection method for improving the detection of false reports in sensor networks”, IEICE Trans. Inf. Syst., vol. E92-D, **(2009)**, pp. 1574-1576.

[9] T. Arampatzis, J. Lygeros and S. Manesis, “A survey of applications of wireless sensor and wireless sensor networks”, In Proceedings of IEEE International Symposium on, Mediterranean Conference on Control and Automation, Limassol, Cyprus, **(2005)** June 27-29, pp. 719-724.

[10] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A survey on sensor networks”, IEEE Commun.

Mag., vol. 40, **(2002)**, pp. 102-114.

[11] Z. Yu and Y. Guan, “A dynamic en-route scheme for filtering false data in wireless sensor networks”, in Proc. IEEE INFOCOM, Barcelona, Spain, **(2006)** April 23-27, pp. 1–12.

[12] T. K. Kim and H. S. Seo, World Academy of Science, Engineering and Technology, Simulation using the Recursive, vol. 42, **(2008)**.

[13] H. Y. Lee and T. H. Cho, "Fuzzy Logic Based Key Disseminating in Ubiquitous Sensor Networks", Advanced Communication Technology, 2008. ICACT 2008. 10th International Conference on, vol. 2, **(2008)** February 20, pp. 958-962.

Authors

Jong Kun Lee

He is currently an underground student in the College of Information and Communication Engineering at Sungkyunkwan University, Korea. His research interests include sensor network security.

Su Man Nam

He received his B.S. degrees in computer information from Hanseo university, Korea, in February 2009. He is currently a graduate 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 modeling & simulation.

Tae Ho Cho

He 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.