FUZZY-BASED ENERGY EFFICIENT METHOD FOR MULTIPLE ATTACKS IN SENSOR NETWORKS: AGAINST FALSE VOTE AND REPORT INJECTION ATTACKS

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

An adversary can easily compromise sensor nodes in wireless sensor networks, and generate multiple attacks through compromised nodes, such as false vote injection attacks and false report injection attacks. The false vote injection attack tries to drop legitimate reports in an intermediate node, and the false report injection attack tries to drain the energy consumption of each node. To prevent these attacks, a probabilistic voting-based filtering scheme (PVFS) has been proposed to select verification nodes, and to detect fabricated votes in the reports as they occur simultaneously. In this paper, we propose a method that improves the energy efficiency of each node and the security level of the false report injection attack, while maintaining the detection power of the false vote injection attack. Our proposed method effectively selects verification node with considering the conditions of each node, based on a fuzzy rule-based system. The verification node is decided through the energy remaining level, distance level, and number of detected false votes in the fuzzy system. We evaluated the effectiveness of the proposed method, as compared to PVFS, when two attacks occur simultaneously in the sensor network. The experimental results show that our method saves energy by up to 8%, by improving and maintaining the defence against these multiple attacks.

KEYWORDS

Wireless sensor network, Probabilistic voting-based filtering scheme, False report injection attacks, False vote injection attacks, Fuzzy system

1. INTRODUCTION

Wireless sensor networks (WSNs) are economically feasible technologies for a variety of applications [1]-[2]. These sensor networks enable the low-cost and low-power development of multi-functional use in open environments [2]. A WSN is composed of a base station, and a large number of sensors in a sensor field. The base station collects event data from the sensor nodes, and provides information to users [1], [3]. However, adversaries can easily compromise the nodes, because of their limited computation, communication, storage, and energy supply capacities [4]-[5]. The adversaries can simultaneously generate multiple attacks, such as false vote injection and false report injection attacks, to destroy the wireless network.

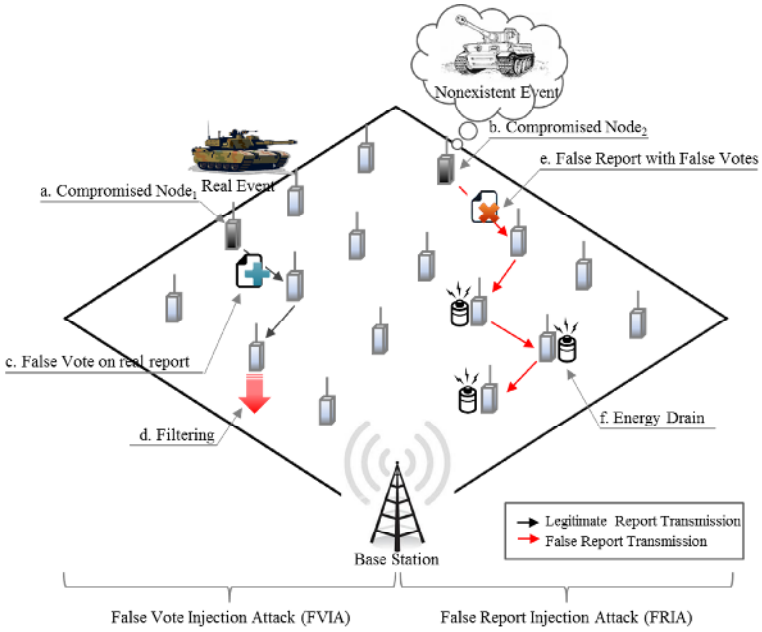

Figure 1. Multiple attacks.

Figure 1 show multiple attacks in the sensor network, such as a false vote injection attack (FRIA) [6]-[7], and a false report injection attack (FVIA) [7]. Two nodes (Figure 1-a and Figure 1-b) are compromised by forward false reports and false votes. In FVIV, a compromised node (Figure 1-a) injects a false vote in a legitimate report (Figure 1-c) to drop the report en route (Figure 1-d). The legitimate report is filtered out in an intermediate node, before arriving at the base station. In FRIA, a compromised node (Figure 1-b) injects a false report with false votes (Figure 1-e), to drain the energy resource of intermediate nodes (Figure 1-f), and cause false alarms in the base station. These attacks drop real event information, and consume needless energy.

Li et al. [7] proposed a probabilistic voting-based filtering scheme (PVFS) to detect multiple attacks in intermediate nodes, as FRIA and FVIA simultaneously occur in the sensor network. This method is suitable for filtering fabricated votes based on a cluster-based model. The scheme selects verification CHs with a probability to prevent the fabricated votes before forwarding a report. It is different from having verification CHs in a path, when reports are transmitted.

In this paper, we propose a method to effectively select verification CHs based on a fuzzy rule-based system [8]. Our proposed method decides the verification CHs through the energy remaining level, distance level, and number of detected false votes. Therefore, our method increases the security level and energy savings against FVIA and FRIA, as compared to PVFS.

The remainder of this paper is organized as follows. The background and motivation are described in Section 2. The proposed method is introduced in Section 3, and the experimental results are described in Section 4. Finally, conclusions and future work are discussed in Section5

2. BACKGROUND

In the sensor network, FRIA and FVIA are frequently generated in the application layer, and threaten the lifetime of the network. FRIA injects false reports to cause unnecessary energy of sensor nodes. FVIA injects false votes in a legitimate report to be filtered out. We will discuss an existing countermeasure against FRIA and FVIA in Section 2.1 and explains the motivation for our proposed method.

2.1. PVFS: Probabilistic Voting-based Filtering Scheme

Li et al. [1] proposed a probabilistic voting-based filtering scheme to simultaneously prevent multiple attacks in a sensor network, and to maintain the detection power at a sufficiently high level, such as FRIA and FVIA. PVFS uses a voting method with a cluster-based model and a probability key assignment. This scheme consists of four phases: 1) key assignment, 2) report generation, 3) verification node selection, and 4) en-route filtering. 1) As sensor nodes are deployed, a cluster head (CH) is elected in each cluster region, and each sensor selects one key from the partition of the CH in a global key pool. 2) When a real event occurs, the CH collects all votes (such as MAC [6]) from its neighboring nodes. The CH randomly selects the votes as a defined value, and attaches a report. 3) The CH chooses verification CHs with a probability to verify the attached votes in the report. 4) If the number of detected false votes in a report is lower than the threshold value, FVIA is considered in a verification CH, and transmits it to next hop. If the number of detected false votes is greater than the threshold value, FRIA is considered in a verification CH, and drops it. Therefore, PVFS detects fabricated votes generated from a compromised node and prevents FVIA and FRIA in the intermediate nodes.

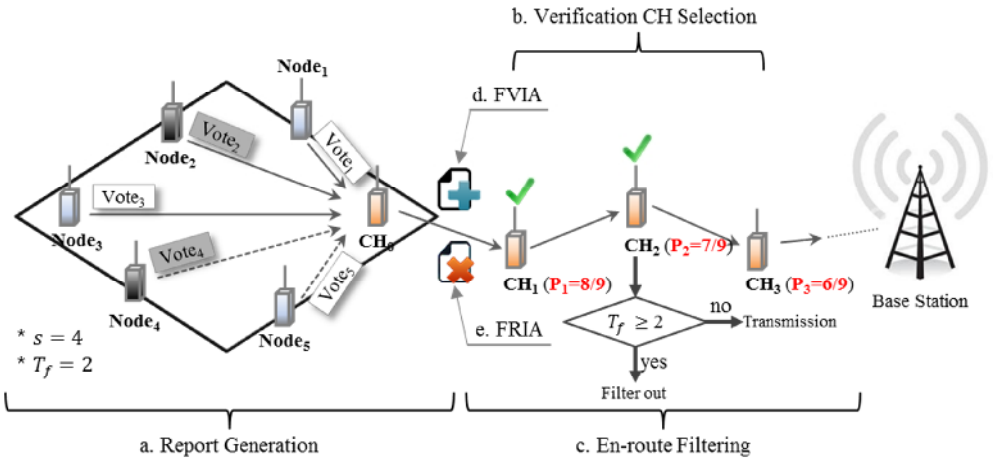

Figure 2. Filtering Processes in PVFS.

Figure 2 illustrates phases of the report generation in a cluster (Figure 2-a), the verification CH selection (Figure 2-b), and en-route filtering (Figure 2-c) in a path. The cluster is comprised of a CH and five nodes including two compromised node ($Node_2$ and $Node_4$). We consider that s is the required number of votes a legitimate report should carry, and T_f is the threshold of false votes required to drop a report. In phase of the report generation, when a real event occurs in the cluster, CH_0 broadcasts to its neighbors. The neighboring nodes forward their vote including event information to the CH. After collecting the votes, $Vote_1$, $Vote_2$, $Vote_3$, $Vote_5$ is randomly selected to produce a report. In phase of the verification CH selection, the CH1 and CH2 are chosen for verification of the votes by a probability $P = d_i / d_0$ (the hop count from a verification

CH_i/CH_0 to the base station). That is, there are $P_1 = 8/9$ of CH_1, $P_2 = 7/9$ of CH_2, and $P_3 = 6/9$ of CH_3, respectively (the hops of CH_0 is 9). Both CH_1 gets CH_2 get verification keys of CH_0. CH1 gets keys $K = \{1,3,4,5\}$, and CH2 get keys $K = \{1,2,3\}$. In phase of en-route filtering, when the report arrives in CH_1, $Vote_1$, $Vote_3$, and $Vote_5$ are true by using the keys of CH_1. The report is forwarded to CH_2 with $T_f = 0$. CH_2 finds a fabricated $Vote_2$ by key 2 and sets the corresponding bit to 1. The report is transmitted to next CH3 as $T_f = 2$ has not been reached yet. The legitimate report will be safely forwarded in the base station against FVIA (Figure 2-d). That is, PVFS detects FVIA through the number of the threshold value as $T_f = 2$ has not been reached yet. In contrast, when CH0 selects Vote1, Vote2, Vote3, and Vote 4, a false report is forwarded with fabricated Vote2 and Vote4. CH1 detects the false Vote4 by key 4, and sets the corresponding bit to 1. When the false report arrives in CH2, it drops the false report because the false Vote2 is detected by key 2 as $T_f = 2$ has been reached. The false report is en-route filtered out in intermediate nodes against FRIA. That is PVFS prevents FRIA through the number of threshold value in the false report as $T_f \geq 2$ has been reached. Therefore, PVFS selects verification CHs by using the probability, detects both of FRIA and FVIA through the threshold value as they simultaneously occurs in the sensor network.

2.2. Motivation

In order to simultaneously detect multiple attacks, such as FRIA and FVIA, PVFS should be operated in the sensor network. PVFS has the phases of the key assignment, the report generation, the verification CH selection, and en-route filtering. The phase of en-route filtering affects energy consumption of each node because of the detection of injected votes. In this paper, we effectively select verification CHs based a fuzzy rule-based system to early detect both of FRIA and FVIA.

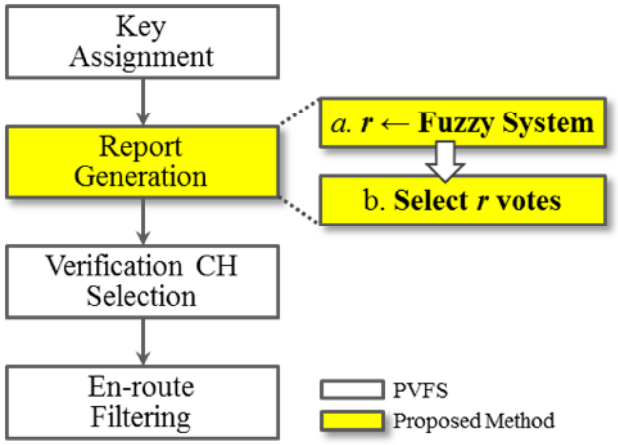

Figure 3. Motivation.

Figure 3 shows the verification CH selection in the proposed method based the fuzzy system instead of the probability selection of PVFS. Before forwarding a report, a CH effectively decide verification through a fuzzy rule-based system. Our method improves the detection power of FRIA while maintaining the security level of FVIA. Therefore, our proposed method saves energy resources of each node in the sensor network compared to PVFS. In addition, we expect that our method will prolong the lifetime as the whole network has a long-term operation.

3. PROPOSED METHOD

Our proposed method selects verification CHs based the fuzzy rule-based system to detect false votes before forwarding reports. The fuzzy system decides the verification CH through three input factors of energy remaining level, distance level, and the number of detected false votes. Therefore, our proposed method improves a security level and energy effectiveness compared to PVFS. In this section, the proposed method is described in detail.

3.1. Assumptions

We assume the sensor nodes are fixed after they are deployed. The sensor network composes a base station and a number of sensor nodes, e.g. the Berkeley MICAz motes [3], the initial paths is established through directed diffusion [4], and minimum cost forwarding algorithms [5]. We choose the cluster-based model [7] to organize the sensor nodes. In a cluster, one node is elected to be a CH.

It is further assumed that every node forwards reports into the base station along their path. A compromised node generates false reports in a path. The generated false reports are forwarded from a compromised node toward the base station before filtering it out.

3.2. Overview

Our proposed method selects verification CHs based the fuzzy rule-based system before forwarding a report to next intermediate CH. Our method decides the verification CHs by using three input factors of an intermediate CH: a) energy remaining level, b) distance level, and c) the number of detected false votes

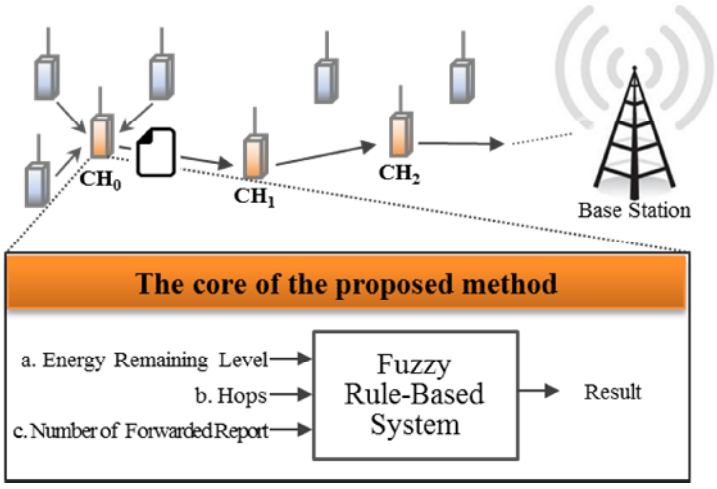

Figure 4. The proposed method based fuzzy logic.

Figure 4 shows the phases of the verification CH selection by applying the three input factors when they are selected in a path. The proposed method consider that the verification CH is effectively selected through energy remaining level, distance level, and the number of detected false votes. For example, CH_1 is a verification node, and CH_2 is a normal CH due to unsuited conditions. A report, which is forwarded from CH0, is verified in CH_1. CH2 then receives and directly transmit it to next hop. Thus, the proposed method effectively detects the multiple attacks

using the fuzzy rule-based system and saves needless energy of each sensor when FRIA and FVIA simultaneously occur.

3.3. Proposed Method based Fuzzy Logic

3.3.1. Further Subsections

This section discusses the factors that are used for fuzzy inference.

- ERL (Energy Remaining Level) This value indicates how much energy remains in CHs. It is important to present energy of each node in the sensor network. The value specifies energy level of each CH from 1 to 100. If this value is close to 1, energy reaming level is low.
- DTL (Distance Level) This value indicates the hop count from a CH to the base station. When a report is forwarded, it travels via the number of hops toward the base station. The value specifies the distance level of each CH from 1 to 100. Before forwarding the report, intermediate CHs calculate the level by $HC_i/HC_0 \times 100$ (HC_i is hops of an intermediate CH, HC_0 is hops of CH_0). If this value is high, the intermediate CH is close to CH_0.
- NDV (Number of Detected False Votes) This value indicates the condition of the sensor network security. If verification CHs detect many false votes occurred from compromised nodes, the verification CHs maintain high security level in a path. The value specifies the number of detected false votes from 1 to 50. If the value exceeds 50, the value keeps 50.

The three input factors ERL, DTL, and NDV decide a flag (FLG) for verification CHs through the fuzzy rule-based system.

3.3.2. Fuzzy Membership Functions and Rules

Figure 5, Figure 6, Figure 7 illustrate the membership functions of the fuzzy logic input parameters for selecting verification CHs. We tune membership functions as the best rule with lots of experiment. The input factors of the fuzzy variables are represented as:

- Energy Remaining Level = {Small (SM), Middle (MD), Large (LG)}
- Distance Level = {Very Near (VN), Near (NR), Middle (MD), Far (FR), Very Far (VF)}
- Number of Detected False Votes = {Low (LW), Middle (MD), High (HG)}

Figure 8 shows the membership function of the fuzzy logic output parameters for effectively deciding verification CHs. The output factors of the fuzzy variables are represented as:

- Flag = {Keep, Verification}

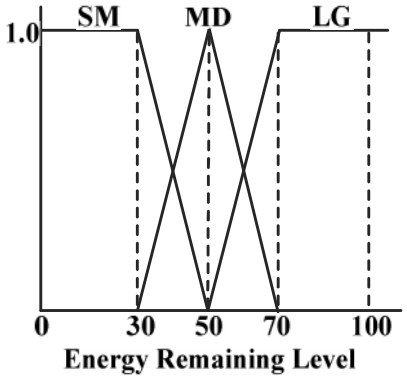

Figure 5. ERL of Fuzzy Membership Function.

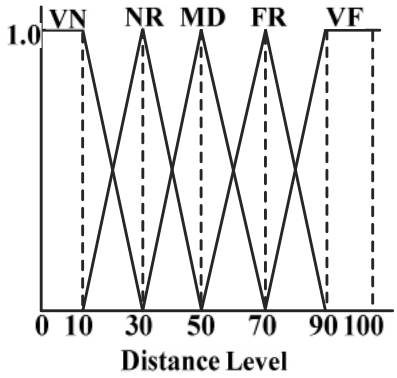

Figure 6. NDV of Fuzzy Membership Function.

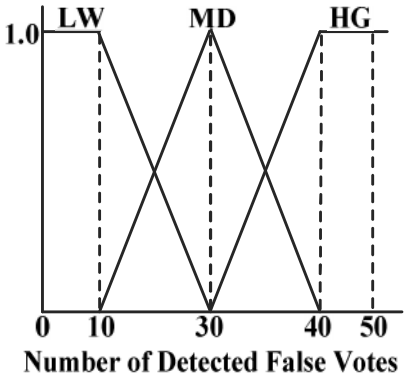

Figure 7. NDV of Fuzzy Membership Function.

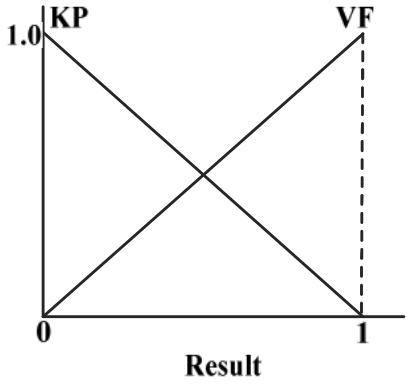

Figure 8. FLG of Fuzzy Membership Function.

We defined 45 (=3×5×3) fuzzy rules as shown in Table 1.

Table 1. Fuzzy if-then rules.

Rule No.	Input (if)			Output (then)
	ERL	**DTL**	**NDV**	**FLG**
0	SM	VN	LW	KP
14	SM	VF	HG	VF
23	MD	MD	HG	VF
30	LG	VN	LW	PS
44	LG	VF	HG	VF

Table 1 shows representative rules as frequently occurred in the fuzzy membership function. For instance, if ERL is SM, DTL is VN, and NDV is LW, then it keeps a normal CH to conserve energy resource (Rule 0). If ERL is SM, DTL VF, and NDV is HG, then it is recommended to have a verification node to maintain high detection power for detecting false votes in a report (Rule 14). If ERL is MD, DTL is MD, and NDV is HG, then it is also recommend detecting false votes in a verification CH (Rule 23). If ERL is LG, DTL is VN, and NDV is LW, then a normal CH transmits a report to next CH without verification (Rule 30). If ERL is LG, DTL is VF, and NDV is HG, then a normal CH is recommend for detecting false votes, maintains the high security level (Rule 44). Therefore, it is important to effectively select verification CHs appropriately before forwarding a report due to energy saving.

4. EXPERIMENTAL RESULTS

An experiment was performed for the proposed method and compared to PVFS. There are 500 total sensor nodes in the sensor network of the simulation environment. The simulation environment, which is 1,000×1,000 m2, is composed of 50 clusters and 10 nodes in a cluster. We compromised 20 nodes in 11 hops of the sensor network. The compromised nodes inject false reports to consume unnecessary energy and false votes to drop legitimate reports in intermediate nodes. The size of a report is 24 bytes, and the size of a vote is 1 byte. Each node uses 16.25 μJ to transmit per byte, 12.5 μJ to receive per byte, and 15 μJ to generate a vote per byte [2]. We randomly generate 300 events in clusters, and the ratio of false reports is 20% of the events.

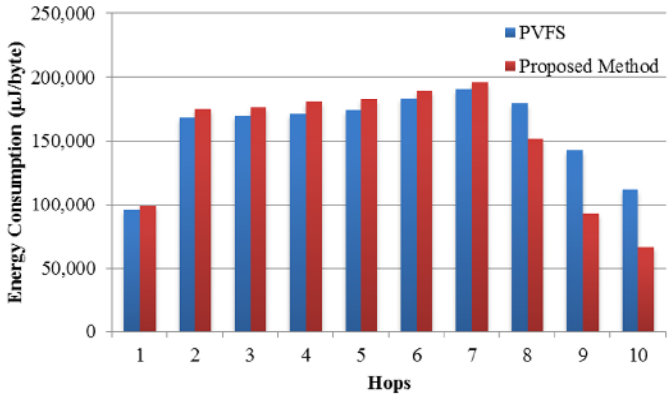

Figure 9. Energy consumptions per hop.

Figure 9 shows the energy consumptions of CHs as FRIA and FVIA simultaneously occur in the sensor network. These attacks are generated in hops 11 of compromised nodes. In the proposed method, the energy consumption between hops 8 and 10 is lower than PVFS. That is, our method improves energy savings because it selects verification CHs based the fuzzy rule-based system more than PVFS for selecting verification nodes by using the probability. Therefore, our proposal saves the energy resources of each node to effectively choose the verification CHs more than PVFS.

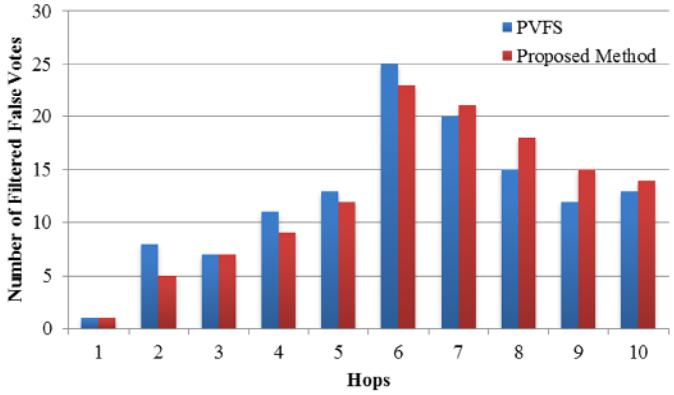

Figure 10. Number of filtered false votes per hop.

Figure 10 shows the number of detected false votes her hop for FVIA. Both of PVFS and the proposed method detects the false votes in verification CHs close to compromised nodes (hops 11). Our method prevents the most of the false votes in legitimate reports by up about 72% between hops 7 and 10. PVFS detects the false votes in verification CHs between hops 2 and 6 by using the probability selection. Thus, the proposed method maintains the security level of FVIA through the number of detected the false votes as compared to PVFS.

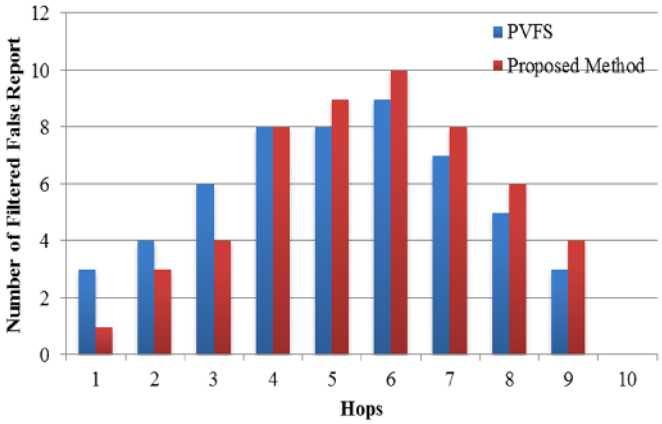

Figure 11. Number of filtered false reports per hop.

Figure 11 shows the number of detected false reports for FRIA. The proposed method improves the detection power of FRIA to effectively select the verification CHs through the fuzzy rule-based system. Our method improves the detection of the false report by up about 70% between hops 5 and 9 more than PVFS, influences the energy consumption of intermediate CHs as shown Figure 11. Therefore, the proposed method improves the security level of FRIA and decreased the energy consumption more than PVFS.

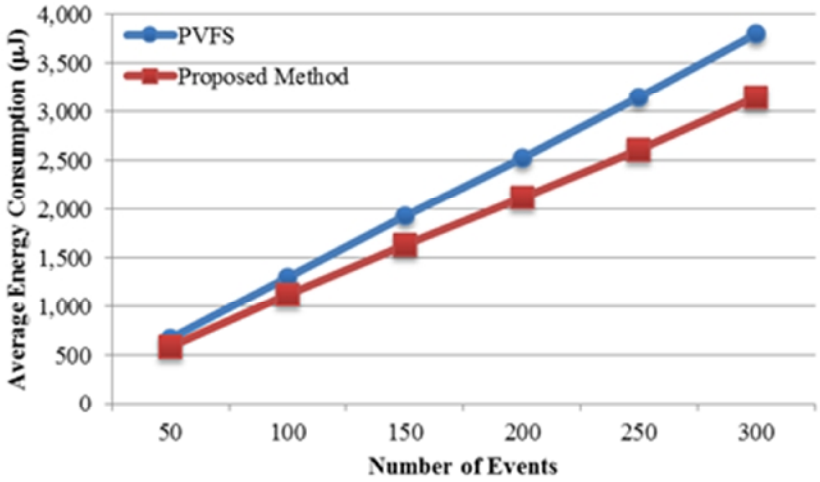

Figure 12. Average energy consumption per event.

Figure 12 shows the average energy consumption of intermediate CHs per events 50. The energy consumption in PVFS and the proposed method is approximated as 50 events occur in the sensor network. When 150 events are generated, the energy consumption of the proposed method saves about 292µm more than PVFS. That is, a gap for energy consumption is produced due to mutual security countermeasure against the multiple attacks, such as FVIA and FRIA. Therefore, our proposed method improves the energy consumption by up about 8% as compared to PVFS, we expect to prolong the lifetime of the whole sensor network.

5. CONCLUSIONS

In WSN, an adversary easily compromises sensor nodes and simultaneously generates the multiple attacks, such as FVIA and FRIA. These attacks block an inflow of legitimate reports and threaten the lifetime of the sensors. To detect these attacks, PVFS was proposed to select verification CH with a probability and to prevent false votes. In this paper, the proposed method decides effective verification CHs according to conditions of the CHs based a fuzzy rule-based system. Our proposed method improves the detection power of FRIA while maintaining the security level of FVIA as compared to PVFS, and saves the energy resources of each node by up about 8%. Therefore, our proposal effectively selects the verification CHs by using the fuzzy rule-based system as compared to PVFS, and improves energy consumption of each node and the security level of FRIA while maintaining the detection power of FVIA. In addition, we will apply various attacks of the sensor network to discuss further optimal solutions.

6. ACKNOWLEDGMENTS

This work was supported by National Research Foundation of Korea Grant funded by the Korean Government (No. 2012-0002475).

REFERENCES

[1] Akyildiz, I.F., Weilian Su, Sankarasubramaniam, Y. and Cayirci, E., "A survey on sensor networks," Communications Magazine IEEE, Vol. 40. 2002, pp. 102-114.

[2] Przydatek, D. Song and A. perrig, "SIA: Secure information aggregation in sensor networks," Proc. Of CCNC, Vol. 23. 2004, pp. 63-98.

[3] Kemal A. and Mohamed Y., "A survey on routing protocols for wireless sensor networks," Ad hoc Network. Vol. 3, May 2005, pp. 325–349.

[4] 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.

[5] Xiaojiang D., and Hsiao-Hwa C, "Security in Wireless Sensor Networks" IEEE Wireless Commununications, Vol. 15, Aug. 2008, pp. 60-66.

[6] Fan Ye; Luo,H., Songwu Lu and Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal on, Vol. 23, Apr. 2005, pp. 839-850.

[7] Li, Feng, Srinivasan, Avinash, Wu and Jie, "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks," International Journal of Security and Network, Vol. 3, No. 3, 2008, pp. 173-182.

[8] L. A. Zadeh, "Fuzzy Logic," 2011, http://en.wikipedia.org/wiki/Fuzzy_logic

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

[10] Chalermek I., Ramesh G. and Deborah E., "Directed diffusion: a scalable and robust communication paradigm for sensor networks," MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking, ACM, 2000, pp. 56-67.

[11] Fan Y., Chen A., Songwu L., and Lixia Z, "A scalable solution to minimum cost forwarding in large sensor networks," Computer Communications and Networks, 2001.

[12] Lee, S.hyun. & Kim Mi Na, (2008) "This is my paper", ABC Transactions on ECE, Vol. 10, No. 5, pp120-122.

[13] Gizem, Aksahya & Ayese, Ozcan (2009) Coomunications & Networks, Network Books, ABC Publishers.

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.