ENSP: ENERGY EFFICIENT NEXT HOP SELECTION IN A PROBABILISTIC VOTING-BASED FILTERING SCHEME USING FUZZY LOGIC

Jae Kwan Lee[1], Su Man Nam[2] and Tae Ho Cho[3]

[1,2,3]College of Information Communication Engineering, Sungkyunkwan University
Suwon 400-746, Republic of Korea

ABSTRACT

In wireless sensor networks, sensor nodes are easily compromised due to their restricted hardware resources. These compromised nodes inject fabricated votes into legitimate reports, and generate false report and false vote injection attacks. These attacks deplete energy resources and block report transmission. A probabilistic voting-based filtering scheme was proposed to detect the bogus votes in reports en-route to protect against attacks. Although this method detects false votes in intermediate nodes, the sensor network needs to be effectively operated in consideration of a node's conditions. In this paper, the proposed method selects effective verification nodes by considering the condition of nodes based on a fuzzy logic system. In the proposed method, the intermediate node selects between two next hop nodes in its range through a fuzzy logic system before forwarding the report. Experimental results suggest that, compared to the original method, the proposed method improves energy savings up to 11% while maintaining a high security level.

KEYWORDS

Wireless sensor networks, Probabilistic Voting-based Filtering Scheme, Fuzzy logic system

1. INTRODUCTION

Wireless sensor networks (WSNs) have a large number of sensor nodes to detect events, and base stations (BSs) to collect the sensing data in sensor fields [1-4]. A sensor node operates sensing, computing, and wireless communication modules. When a real event occurs, the node detects it and produces a report to cause its BS to notice it. The BS collects the forwarded report via multiple hops, and provides event information to users through the Internet or communication infrastructure. Although the nodes are suitable for a random distribution in an open environment, they are compromised due to their hardware resource restrictions. In addition, they are exposed to various malicious attacks due to environmental constraints. False report injection [5-7] and false vote injection attacks consume needless energy and block report transmissions in the sensor network. Thus, the network's lifetime is reduced and it is impossible to collect sensing information.

DOI : 10.5121/ieij.2014.2401

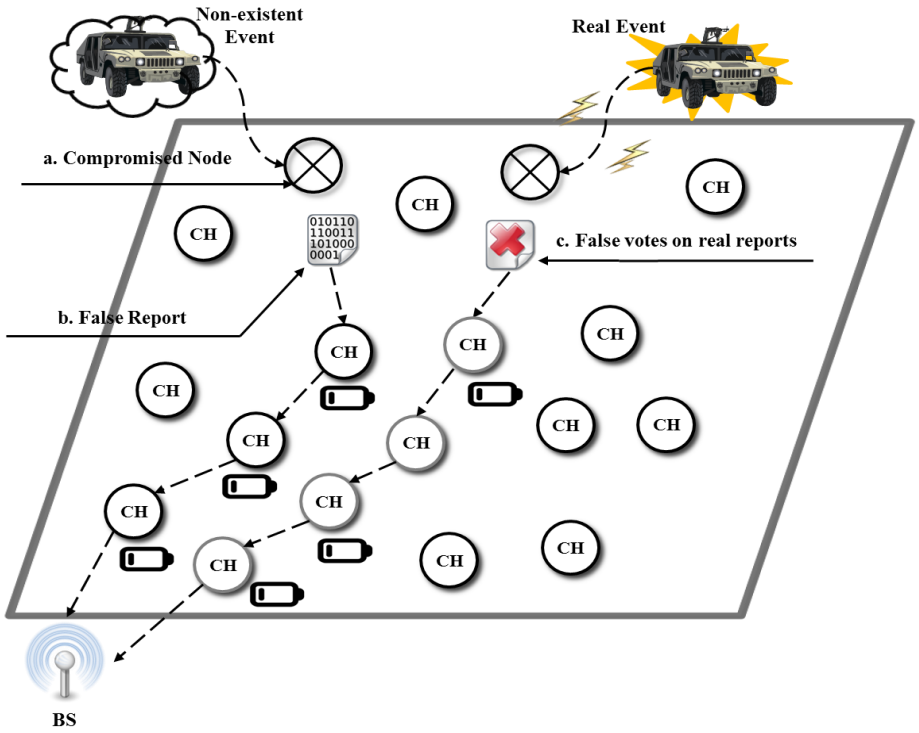

Figure 1.False report and false vote attacks

Figure. 1 shows the false report injection attack and the false vote injection attack in the sensor network. These attacks compromise sensor nodes, and false votes are produced by the compromised nodes. In the false report injection attack, the compromised node injects a false report without detecting an event. If the false report with false votes arrives at the BS, intermediate nodes consume unnecessary energy resources for the transmission of the false report. In the false vote injection attack, the compromised node injects a false vote into a legitimate report to be dropped in an intermediate node. If the legitimate report is dropped due to the false vote, the BS does not receive the report information. Thus, energy consumption and report transmission are damaged by the two attacks in the sensor network.

In order to deal with these two attacks, Li et al. proposed a probabilistic voting-based filtering scheme (PVFS) [8, 9]. While forwarding the report, this method determines one of the attacks based on the number of false votes detected in the report. If the number of detected false votes exceeds a threshold, the report with the false votes is filtered out in an intermediate node against the false report injection attack. In the method, if the number of detected false votes is less than the threshold, the report is forwarded to the BS against the false vote injection attack. Therefore, the PVFS detects the false votes in intermediate nodes against the false report and false vote injection attacks.

In this paper, we propose a method to select the next hop node in order to improve energy savings based on a fuzzy logic system. In the proposed method, before a node forwards a report to its next hop node, the node considers the next hop node's factors (energy, distance, and time) and selects a relevant next hop node. Therefore, the proposed method improves energy efficiency through the selection of effective next hop nodes as compared to the PVFS.

The rest of this paper is organized as follows: Section 2 introduces the PVFS and the motivation behind it. The proposed method is described in detail in Section 3. In Section 4, the

experimental results of the proposed method are analyzed and discussed. The conclusions are given in Section 5.

2. BACKGROUND

In this section, we introduce the PVFS in Section 2.1, and the motivation for the proposed method in Section 2.2.

2.1. PVFS

Li et al. proposed a PVFS to detect false report injection attacks and false vote injection attacks. The PVFS consists of three phases: key assignment, report generation, and en-route filtering. In the key assignment phase, the BS distributes keys to every cluster. In the report generation phase, a node produces a report with the votes as an event occurs. In the en-route filtering phase, selected verification nodes detect false votes generated by compromised nodes.

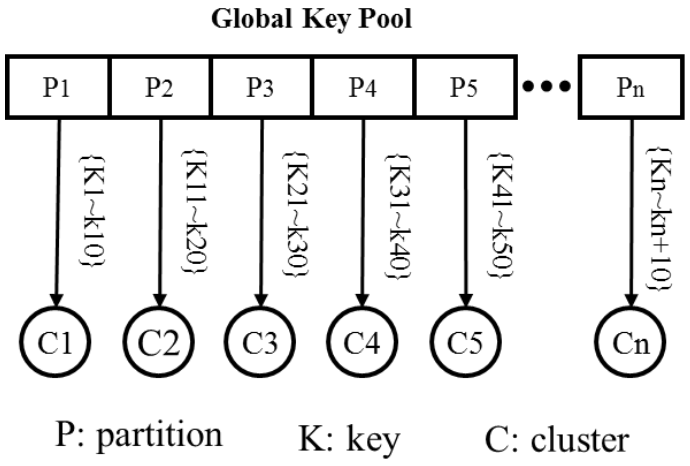

Figure 2.Key assignment phase

Figure. 2 shows the key assignment phase after the cluster-head (CH) and normal nodes are deployed in the sensor field. The clusters receive the keys of a partition from the BS, and the CH and normal nodes select a key from the cluster.

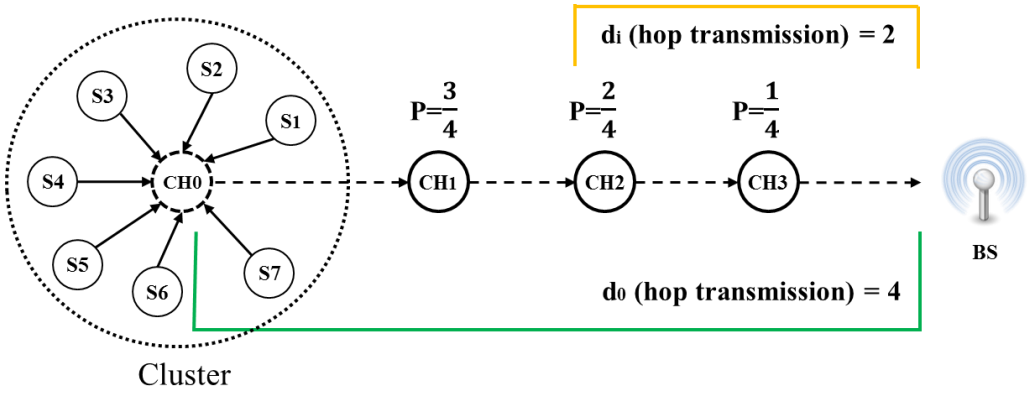

Figure 3.Report generation

Figure. 3 shows the report generation phase which sends event information to the BS. When an event occurs in a cluster, the normal nodes in the cluster forward their vote to the CH. The CH randomly selects a defined number of votes to produce a report. Before forwarding the report, the CH determines the verification nodes through a probabilistic calculation based on their distance. For example, as the hop of CH2 is 2, the probability is 2/4. The verification node verifies the votes of the report.

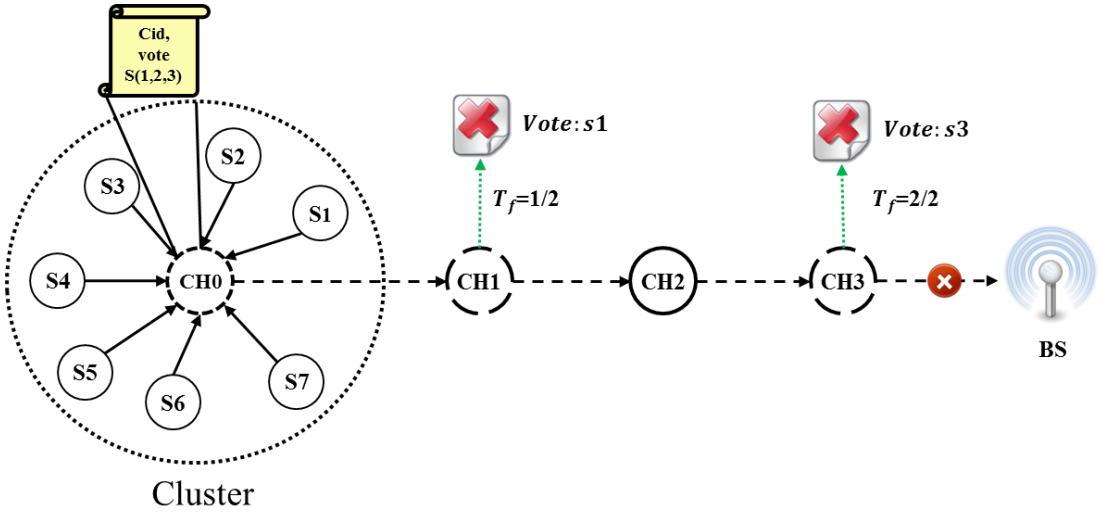

Figure 4.En-route filtering phase

Fig. 4 shows the en-route filter phase while forwarding the report from a source CH to the BS. After determining the verification nodes, the report is forwarded along a path toward the BS. CH0 randomly selects five votes when the votes are collected from the normal nodes (we assume the number of votes is 2). CH0 then transmits the report to CH1. CH1 detects false Vote:s1. CH1 transmits a report to CH2. CH2 doesn't have a verification node to transmit a report to CH3. CH3 filters out the report after false Vote:s3 was detected. The reason for this is that report T_f=2 has been reached.

2.2. Motivation

A PVFS was proposed to detect false report and vote injection attacks in the sensor network. In the PVFS, before forwarding a report, a source CH determines the verification nodes through a probabilistic calculation based on their distance. The report is authenticated in the verification nodes along a constructed path. However, the PVFS does not consider the energy resource of a next hop node while transmitting the report. In addition, the report is transmitted along the constructed path in the initial phase. In this paper, the proposed method effectively selects verification nodes for improving energy efficiency based on a fuzzy logic system. In the proposed method, intermediate nodes select one of two next hop nodes through the fuzzy logic system. Thus, compared to the PVFS, the proposed method enhances energy savings while maintaining security power.

3. PROPOSED METHOD

In this section, we describe the assumptions, the operational process, and the fuzzy logic system of the proposed method for effectively selecting next hop nodes.

3.1. Assumptions

In this paper, we assume that sensor nodes (e.g., MICA2 mote) [4] are deployed by using a cluster-based model in the sensor field [10-12]. The sensor nodes are uniformly spread and fixed. Each node has unique ID and location information through the GPS module. A CH is elected in a cluster, and it is more powerful than a normal node. When a report is generated, a source CH transmits the report downstream to the BS. In addition, an adversary compromises nodes in order to launch false report and false vote injection attacks after distributing the sensor node in the sensor field.

3.2. Overview

We propose a method to select the next hop node based on a fuzzy logic system. In the fuzzy logic system, the input factors are the remaining energy, hop count and operating time. The output value represents the quality condition of the sensor node. A CH selects its next hop node according to the next input factors. Fig. 5 shows that intermediate CHs use the fuzzy rule-based system to select the next hop node. When an event occurs in a cluster of CH0, CH0 produces a report with the votes to send it to the BS. CH0 then determines the next hop node according to the conditions of the next node. Thus, our proposed method selects next hop nodes by using the fuzzy rule-based system while forwarding the report.

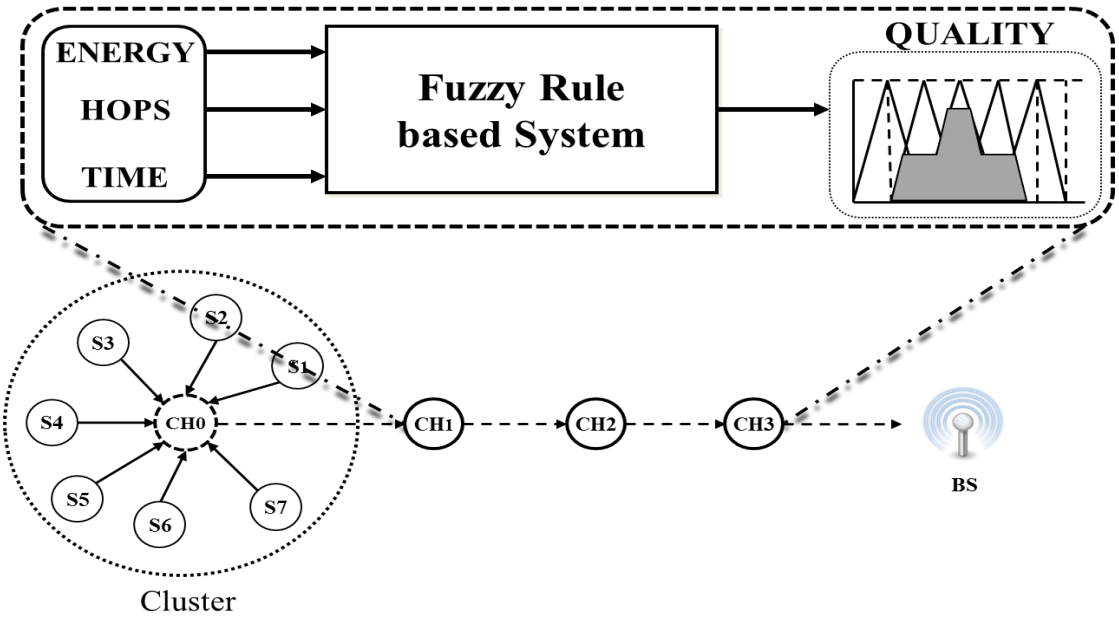

Figure 5.Operating process of the proposed method

3.3. Fuzzy Logic System

We apply the fuzzy logic system [13, 14] to effectively determine the next hop node for a verification node. The input factors for the fuzzy logic are the remaining energy, hop count, and operating time of the node in the sensor network. The next section will describe these factors in detail.

1)Input factors

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

1-1) Remaining energy is a very important part of the sensor network. If a sensor node has many computations for transmission, reception, and verification, the sensor node quickly destroys its energy resource. Therefore, the remaining energy of the sensor node is important for the network lifetime extension of WSNs.

1-2) The hop count is the distance from a node to the BS. If a CH has many hop counts, a large amount of energy will be consumed in intermediate CHs. Thus, this factor needs to decrease for the energy savings of the sensor node considering the vote verification.

1-3) The operating time is the history of when a sensor node is used. When the sensor node selects the next hop node, the history of the sensor node is important.

2)Fuzzy Membership Functions and Rules

This section presents the membership function of the fuzzy logic input factors. The labels for the fuzzy variables are as follows:

2-1) Remaining Energy (E) = {LOW, HALF, UPPER}

2-2) Hop Count (H) = {SHORT, MIDDLE, LONG}

2-3) Operating Time (T) = {LESS, HALF, OODLES}

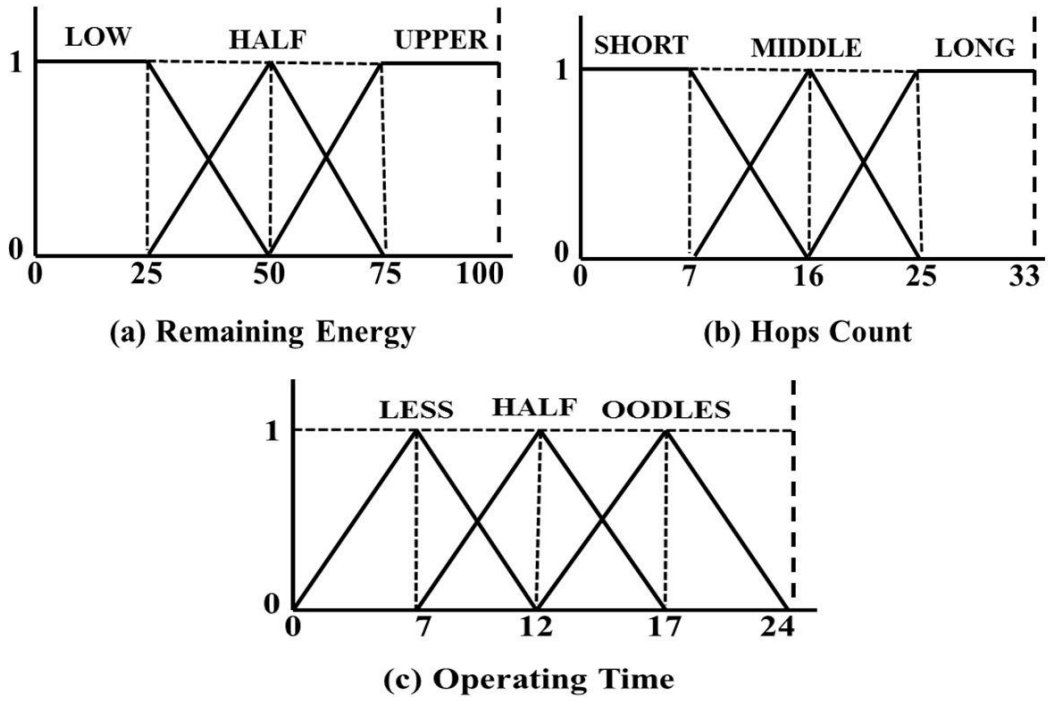

Figure 6.Fuzzy membership input function

The fuzzy logic output parameters are represented by a label. The label value represents the condition of the next hop node as follows:

2-4) Quality (Q) = {VERY_LOW, LOW, MEDIUM, HIGH, VERY_HIGH}

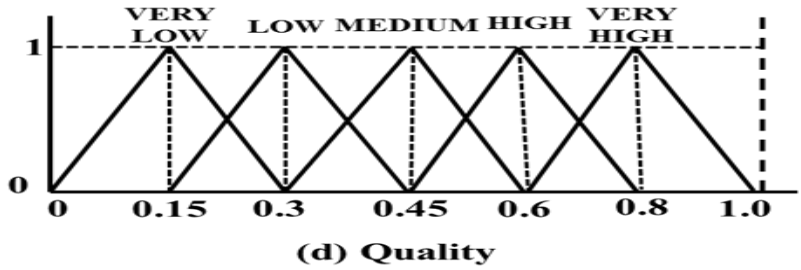

Figure 7.Fuzzy membership output function

Table 1.Fuzzy Rules.

R	Input			Output
	E	H	T	Q
0	LOW	SHORT	LESS	VERY_LOW
5	LOW	MIDDLE	OODLES	HIGH
10	HALF	SHORT	HALF	LOW
15	HALF	LONG	LESS	LOW
20	UPPER	SHORT	OODLES	MEDIUM
…	…	…	…	…
26	UPPER	LONG	OODLES	VERY_HIGH

In R0 (Rule 1), E is LOW, H is SHORT, T is LESS and Q is VERY_LOW. This means that the case values for the condition of the sensor node are very low. In other words, the quality of the sensor node is 0 to 0.3. In case R26 (Rule 26), E is UPPER, H is LONG, T is OODLES and Q is VERY_HIGH. In other words, the quality of the sensor node is 0.6 to 1.0.

3.4. Example of the next hop node selection

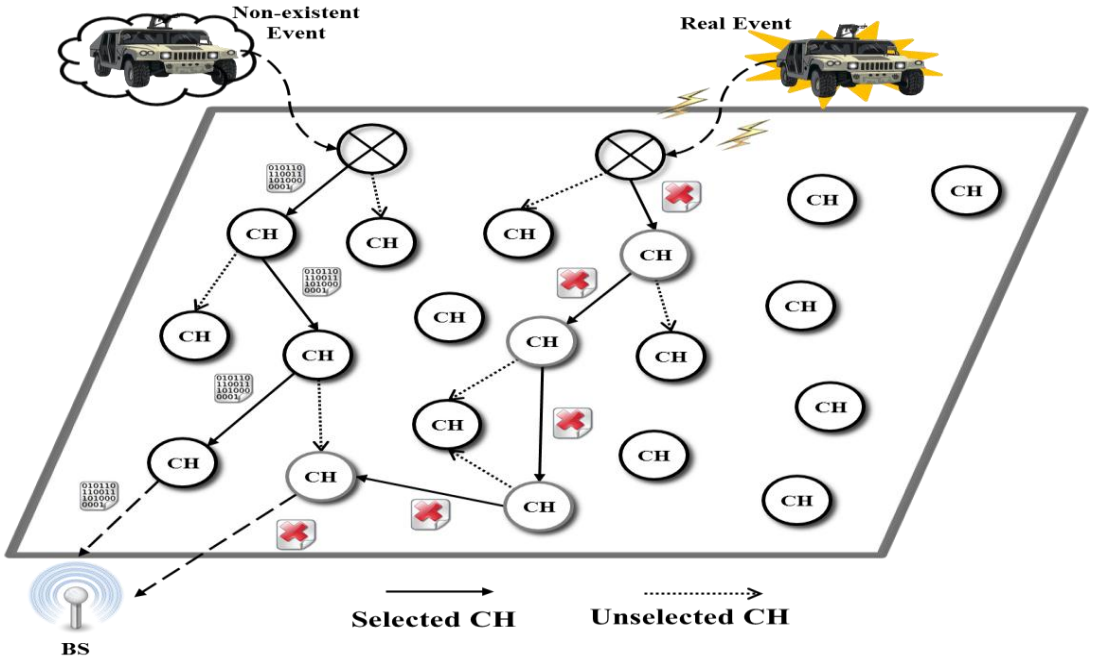

Figure 8.Example of proposed method

Figure. 8 shows an example of the proposed method. In the sensor field, when an event occurs, the source CH selects the next hop node from the two next hop nodes. The next hop nodes transmit the condition to the CH based on a fuzzy logic system. The CH selects the next hop node with a high condition, and transmits a report to the next hop node. The next hop node verifies the votes in the report after the report is received by the CH. The existing proposed method inefficiently uses the energy resources of the sensor nodes due to the selection of a fixed verification node. Therefore, we propose a method to select the next hop node based on a fuzzy logic system for conserving the energy resources of the sensor node.

4. EXPERIMENTAL RESULTS

In this study, a simulation was performed to compare the proposed method with the existing PVFS. In the simulation, the sensor field size is 1500×1000 m^2, where 6,000 sensor nodes are randomly distributed. Each sensor node randomly selects a key partition from a cluster. The sensor node consumes 16.25 μJ to transmit and 12.5 μJ to receive, per byte [15]. In addition, it consumes 15 μJ to generate a vote. The size of an original report is 36 bytes [16], and the vote size is 1 byte. Fig. 9 shows the energy consumption when false votes occur at a rate of 10% to 100 %.

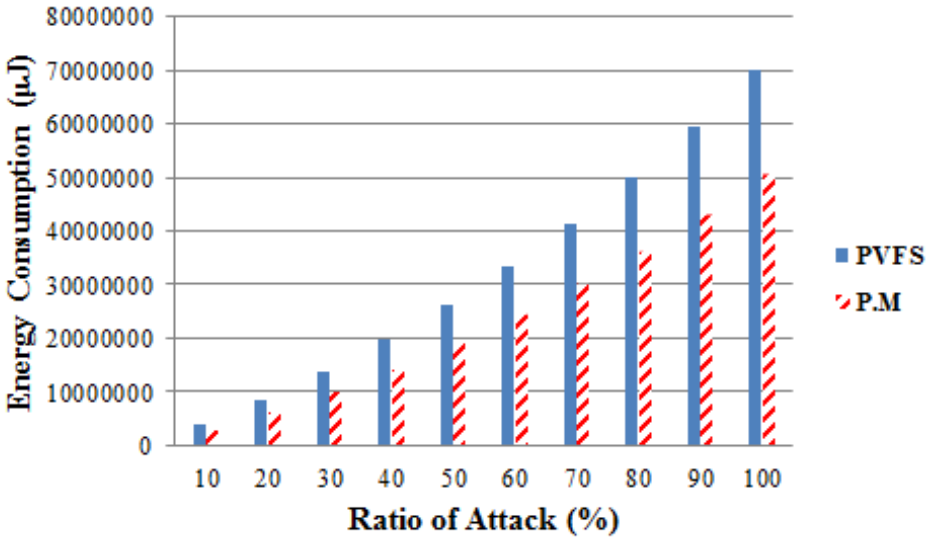

Figure 9. Energy consumption

Figure 9 shows the energy consumption of the PVFS and the proposed method. The proposed method has to minimize wire traffic when the next hop node is selected. In the simulation results, the proposed method improves the energy by about 11% more than the PVFS.

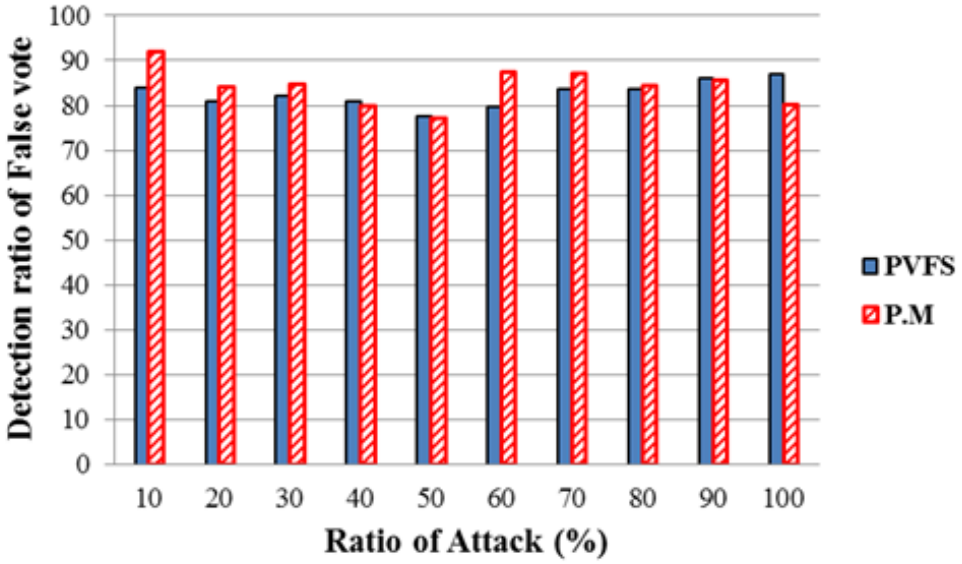

Figure 10. Ratio of detected false votes

Figure. 10 shows the ratio of detected false votes. We compare the PVFS with the proposed method according to the ratio of attacks. In the simulation results, the proposed method detected an average of 2.3% less false votes than the PVFS.

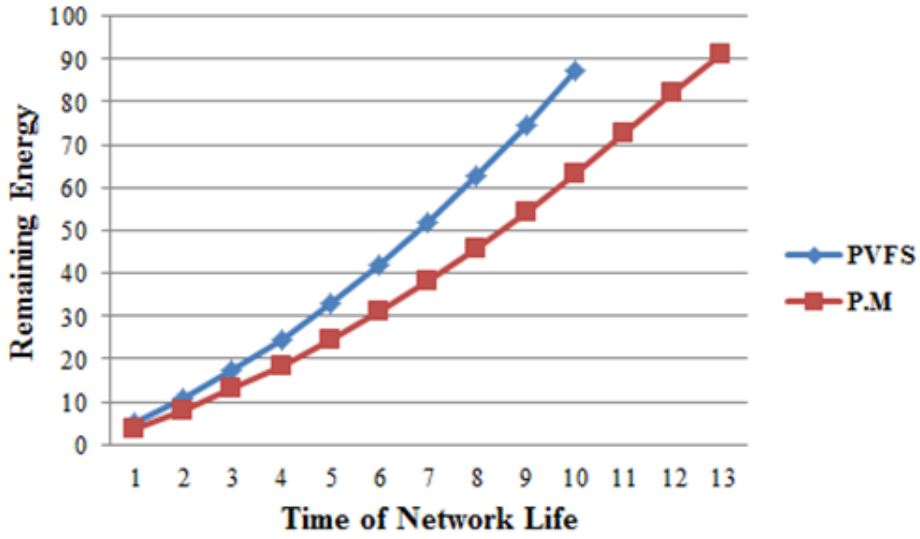

Figure 11. Time of network life

Figure. 11 shows the network lifetime. We measure the amount of sensor node energy. In the simulation results, the proposed method had a better network life efficiency than the PVFS. The proposed method is extended about 3 rounds in the network life.

5. CONCLUSION

A WSN is vulnerable to attacks such as false report and vote injection attacks. In order to detect these, a PVFS was proposed to detect false reports or false votes as events occur in the sensor

networks. The original method filters out the fabricated votes through keys in the verification nodes selected based on their distance. Although this method simultaneously detects the two attacks in the sensor network, it does not consider the energy resources of the sensor nodes as reports are transmitted to the next hop nodes. In this paper, the proposed method selects the next hop node for improving the energy savings of the node based on a fuzzy logic system. In the proposed method, the three input factors in the fuzzy logic system are the remaining energy, distance, and time. These factors evaluate the conditions of the next hop node to effectively transmit the report. The report is forwarded along a changing path to the BS based on the conditions of the next hop node. Thus, the proposed method saves energy resources because effective next hop nodes reduce the amount of wireless communication. As shown in the experimental results, the proposed method enhances the energy efficiency by an average of 11% as compared to the original method. In the future, we will study the security threat of WSNs by applying various routing protocols and security countermeasures in the sensor network.

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. 2013R1A2A2A01013971).

REFERENCES

[1] J. N. Al-Karaki Kamal, "Routing techniques in wireless sensor networks: a survey," Wireless Communications11, 2004.

[2] X. N, "A Survey of Sensor Network Applications,"Tech. Rep., University of Southern California, 2002.

[3] S. N. Pakzad, G. L.Fenves, S. Kim and D. E. Culler, "Design and Implementation of Scalable Wireless Sensor Network for Structural Monitoring,"JOURNAL OF INFRASTRUCTURE SYSTEMS, pp. 89-101, Mar, 2008.

[4] M. H, M. J.Lyons, D. B and G. Wei, "Survey of Hardware Systems for Wireless Sensor Networks,"American Scientific Publishers, vol. 4, pp. 1-10, 2008.

[5] Z. Yu and Y. Guan, "A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks," IEEE/ACM TRANSACTIONS ON NETWORKING, vol. 18, pp. 150-163, Feb, 2010.

[6] G. Wittenburg, N. Dziengel, C. Wartenburger and J. Schiller, "A System for Distributed Event Detection in Wireless Sensor Networks,"9th ACM/IEEE International Conference on Information Processing in Sensor Networks, pp. 94-104,2010.

[7] J. Sen, "A Survey on Wireless Sensor Network Security,"IJCNIS, vol. 1, pp.55-78,Aug,2009.

[8] F. Li and J. Wu, "A Probabilistic voting-based Filtering scheme in wireless sensor networks,"Proc. IWCMC, pp. 27-32, July, 2006.

[9] F. Li and J. Wu, "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks,"International Journal of Security and Networks, pp. 173-182, August, 27, 2008.

[10] M. Jiang, J. Li and Y. c. Tay, "Cluster based routing protocol (CBRP),"Functional Specification Internet Draft, 1998.

[11] C. Jong-Shin, H. Zeng-Wei, H. Neng-Chung and J. San-Heui, "Efficient Cluster Head Selection Methods for Wireless Sensor Networks,"Journal of Networks, vol. 5, pp. 964-970, Aug, 2010.

[12] O. Younis, M. Krunz and S. Ramasubramanian, "Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges," IEEE, pp. 20-25, 2006.

[13] R. Babuska,"Fuzzy Systems, Modeling and Identification,"CiteSeerX, Delft University of Technology, 2001.

[14] S. H. Chi and T. H. Cho, "Fuzzy Logic Based Propagation Limiting Method for Message Routing in Wireless Sensor Networks,"ICCSA (LNCS), vol. 3983,pp. 58-67, 2006.

[15] F. Ye, H. Luo, S. Lu and L. Z, "Statistical En-Route Filtering of Injected False Data in Sensor Networks,"IEEE, vol. 4, pp. 2446-2457, Mar, 2004.

[16] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sesnsor Networks,"IEEE, J. Sel. Area Comm, vol. 23, pp. 839-850, 2005, April, 2005.

Authors

Jae Kwan Lee received his B.S. degrees in computer information from BaekSeok University, Korea, in February 2013 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, intelligent system and modelling & simulation.

Su Man Nam re ceived 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 researchinterests 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, modelling & simulation, and enterprise resource planning.