

# ENSF: ENERGY-EFFICIENT NEXT-HOP SELECTION METHOD USING FUZZY LOGIC IN PROBABILISTIC VOTING-BASED FILTERING SCHEME

Jae Kwan Lee<sup>1</sup> and Tae Ho Cho<sup>2</sup>

<sup>1,2</sup> College of Information and Communication Engineering, Sungkyunkwan University, Suwon 440-746, Republic of Korea

## ABSTRACT

*Wireless sensor networks (WSNs) are regularly deployed in harsh and unattended environments, and sensor nodes are easily exposed to attacks due to the random arrangement of the sensor field. An attacker can inject fabricated reports from a compromised node with false votes and false vote-based reports. The false report attacks can waste the energy of the intermediate nodes, shortening the network lifetime. Furthermore, false votes cause the filtering out of legitimate reports. A probabilistic voting-based filtering scheme (PVFS) was proposed as a countermeasure against this type of attacks by Li and Wu. PVFS uses a vote threshold, a security threshold, and a verification node. The scheme does not make additional use energy or communications resources because the verification node and threshold values are fixed. There needs to be a verification node selection method that considers the energy resources of the node. In this paper, we propose a verification path election scheme based on a fuzzy logic system. In the proposed scheme, one node transmits reports in the node with a strong state through a fuzzy logic system after which a neighbor is selected out of two from the surroundings. Experimental results show that the proposed scheme improves energy savings up to maximum 13% relative to the PVFS.*

## KEYWORDS

*Wireless Sensor Networks, Fabricated Report, False Votes, Fuzzy Logic System*

## 1. INTRODUCTION

Wireless sensor networks (WSNs) operate in open environments. WSNs have applications in the fields of home networking, forest management, logistics management, fire monitoring and healthcare [1]. The sensor nodes of the WSNs collect contextual information of the surroundings, and the collected data are transmitted to the users [2-4]. The limitations of the sensor nodes are the limited memory, and energy. Also the sensor nodes can be easily compromised and destroyed as a result of their distribution in open environment [5-6]. An attacker can inject fabricated reports and false votes to a network through a compromised node [7-10], and these attacks deplete the energy and reduce lifetime of the sensor nodes [11].

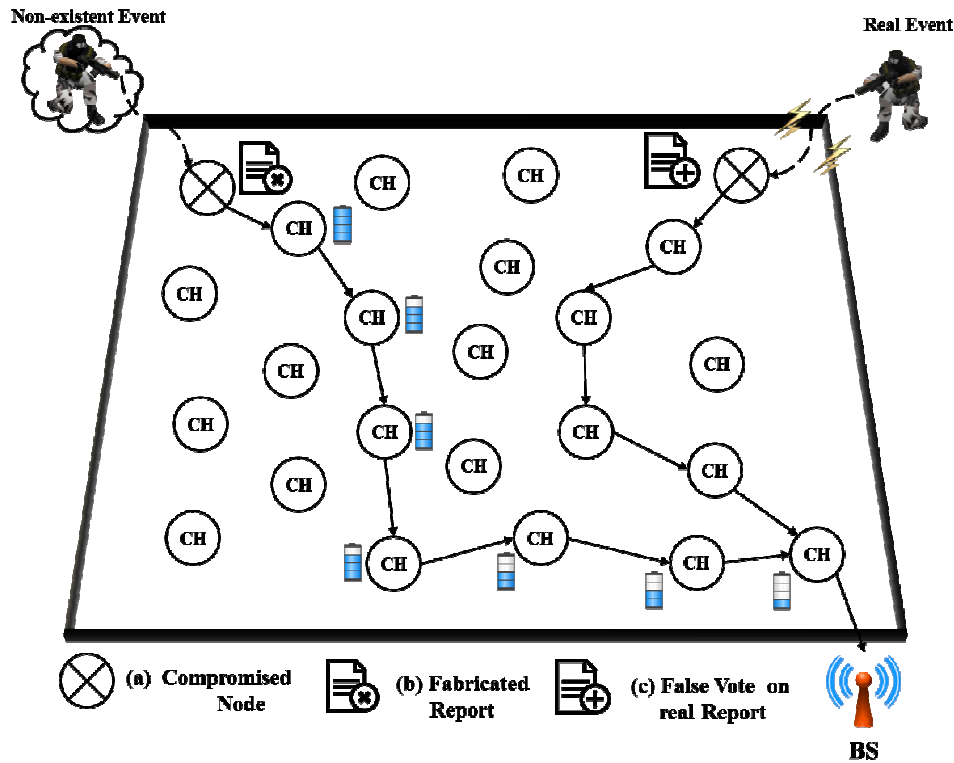


Figure 1. Fabricated report and false votes attacks

Figure 1 shows an attack consisting of a fabricated report and the false votes. Figure 1(a) shows a compromised node, Figure 1(b) shows false votes attached to a fabricated report and Figure 1(c) shows a false vote attached to a legitimate report. The fabricated report is injected through a compromised node, and the attack unnecessarily consumes the energy of the sensor node on transmission paths. A false vote attack can inject false votes attached to a legitimate report, filtering out legitimate reports from the intermediate node. Therefore it is desirable to filter out these attacks as early as possible to avoid wasting energy in processing and forwarding illegitimate information.

A probabilistic voting-based filtering scheme (PVFS) was proposed as a countermeasure for attacks by Li and Wu [12-13]. The scheme distinguishes among two types of attacks with the help of the threshold ( $T_f = 2$ ). The threshold  $T_f = 1$  indicates false vote attack, and  $T_f = 2$  indicates a false report attack. In the case of  $T_f = 1$ , the cluster head (CH) forwards the report to the base station (BS) and does not drop it. In the case of 2, CH drops the report by countering it as a false report attack. The original scheme uses the voting threshold ('1') and security threshold ('2') in a fixed manner, where the decision verification nodes are based on pre-set path. However, the selection verification nodes are fixed, which does not comply with the requirements for a dynamic network.

In this paper, we propose a new Energy-efficient Next-hop Selection using Fuzzy-logic (ENSF). The proposed scheme randomly selected two neighbor nodes before a report is transmitted. The selected neighbor nodes transmit their current state [State\_Ni (R\_ENERGY, HOPS, FTR)] using a fuzzy logic system. The CH evaluates the fitness value of the two received states and transmits the report to the neighboring node with a state higher value between the two neighbors.

The rest of the paper is organized as follows: Section 2, describe several en-route filtering schemes, specifically PVFS. The design and operation of the proposed scheme is described in detail in Section 3. In Section 4, the experimental results the analysis of PVFS and ENSF are presented. The conclusions and future work are given at the end of the paper.

## **2. BACKGROUND**

We review the schemes closely related to our work in Section 2.1, Section 2.2 describes the background, and the motivation of this paper is presented in Section 2.3.

### **2.1. Related Works**

A statistical en-route filtering scheme (SEF) was proposed to filter out fabricated report injection attacks [7-8]. SEF verifies a report using a symmetric key and probability in an intermediate node. If a report fails verification, it is dropped between the intermediate nodes. The interleaved hop-by-hop authentication scheme (IHA) is a verification or disuse scheme using a pair wise key during report transmission in the node [6]. Commutative cipher based en-route filtering (CCEF) uses a commutative cipher to verify the reports with a signature a countermeasure against fabricated report injection attack [14]. A bandwidth-efficient cooperative authentication scheme (BECAN) validates report through a private key before they are shared when the source CH generate the report [15].

These schemes [6-8, 14, 15] have been proposed to reduce unnecessary energy consumption that results from fabricated report injection attacks. When implemented in WSNs these schemes may not detect false votes and false report attacks. Therefore, we need an en-route filtering scheme which can detect both types of attacks at the same time. PVFS was proposed to detect both of these attacks. However, it is not an energy efficient solution. Our work is closely related to this last scheme in which we improve detection of the above attacks conserving energy using a fuzzy logic based system.

## 2.2. PVFS

PVFS was proposed by Li and Wu as a countermeasure against false votes and fabricated report attacks [12]. This scheme uses fixed verification nodes and thresholds which do not cater to the network dynamics (e.g., the residual energy of a node). There are three phase of PVFS: 1) the key assignment phase, 2) the report generation phase, and 3) the filtering phase. Figure 2 shows the key assignment phase.

### 1) Key Assignment Phase

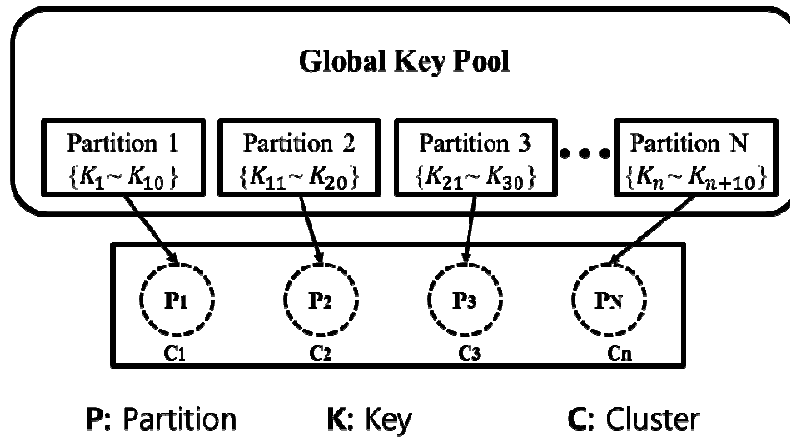


Figure 2. Key assignment phase

After the sensor nodes are deployed in the sensor field, the global key pool (GKP) of the base station (BS) generates symmetric keys and stores them in the (GKP). The keys in the GKP are grouped into partitions and keys from each partition are sent to the CHs. Each node randomly selects a symmetric key from the respective GKP partition in the cluster.

### 2) Report Generation Phase

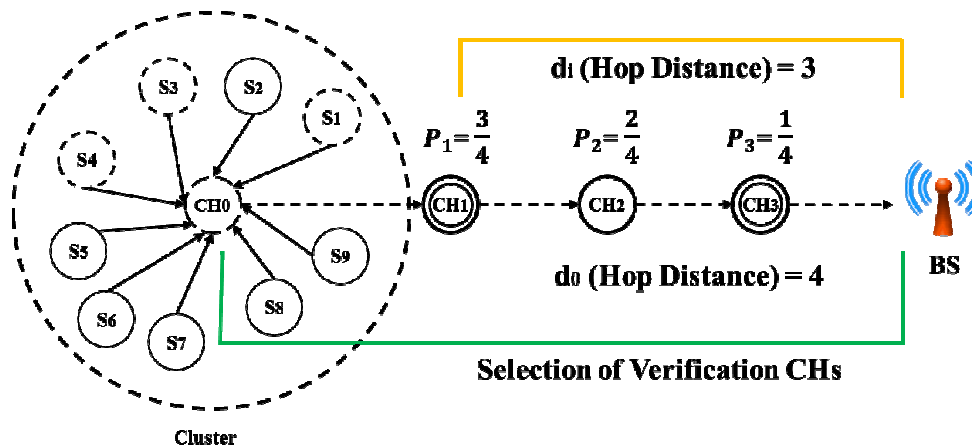


Figure 3. Report generation phase

Figure 3 describes the report generation phase. If an event occur in the cluster, CH0 receive votes of the event from each of the normal nodes. CH0 randomly select five votes and attach them to generate a report. Furthermore, CH0 selects the verification nodes, based on an already preset path. CH0 decide verification node based on the equation  $d_i, d_0$ . Where  $d_0$  represents the distance between CH0 and the base station, and  $d_i$  represents the distance between an intermediate CH0 and the base station. In the Fig. 3,  $d_0 = 4$  and  $d_i = 3$  based on CH1, and the probability of CH1 to be a verification node is  $P_{1=3/4}$ .

3) En-route Filtering Phase

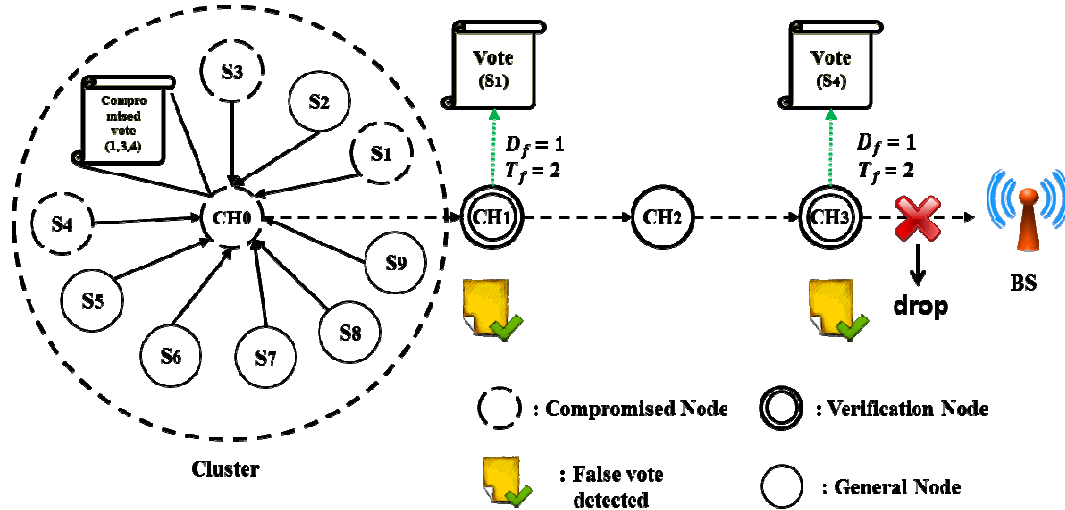


Figure 4. En-route filtering phase

Figure 4 shows the en-route filtering phase. After a report is generated in phase 2, CH0 transmits the report to CH1. CH1 verifies the votes in the report by using the symmetric key. If CH1 identifies a false vote, CH1 attach the information on the false vote to the report and CH1 check if  $T_f = 2$  has been reached. If the security threshold has not been reached, CH1 transmits the report to CH2. Since CH2 is not a verification node, it transmits the report to CH3. If CH3 detects another false vote after the report verification by using the symmetric key, CH3 filters out the report. The reason for this is that the threshold  $T_f = 2$  has been reached.

2.3. Motivation

WSNs are deployed in an open environment without any physical protection, and an attacker can inject false votes and fabricated report through a compromised node. PVFS has been proposed as a countermeasure against false votes and fabricated report injection attacks. When CH or normal nodes are compromised, the original scheme cannot reset the path. In the case where symmetric keys and the path are reset, then the BS has to redistribute symmetric keys on all CHs and nodes (in those clusters) through the old path. Moreover, a new path has to be created. Such overhead causes a waste in energy and shortens the lifetime of the network. In this paper, we propose a verification path election scheme based on a fuzzy logic system in order to improve energy consumption and improve network lifetime.

### 3. PROPOSED SCHEME

In this section, we describe the assumptions of the proposed scheme, the working procedure, the fuzzy logic system, and the proposed verification path election scheme in Subsections 3.1 to 3.4. The scheme and fuzzy logic system are presented in 3.4.

#### 3.1. Assumptions

The sensor nodes of the sensor field are grouped into clusters [3]. The sensor nodes are distributed uniformly in the sensor field grid, and it is further assumed that, sensor nodes are static. Each node is assumed to be a Mica2 mote [16], with memory of  $512_{kb}$  and energy of  $3_J$ . Each sensor node is aware of its unique ID, location, energy level and the number of hops to the BS. Each CH manages the routing table of the neighbor nodes within its transmission range. The BS is assumed to have unlimited resources and the CH also has enough energy to receive and manage the GKP. Finally, we assume that the sensor nodes are prone to false votes and fabricated report attacks.

#### 3.2. Operation Procedure

The sensor nodes receive a unique ID from the user before deployment in the sensor field. A user can connect to the CH unit through the BS using the internet. Each cluster receives the symmetric key partition from the BS. When an event occurs in one of the clusters, the CH generates a report, and the generated report is sent to the next neighbor node based on the verification path election scheme for verification. The verification path election scheme randomly select one of two of the neighbor nodes as a source CH. Neighbor nodes transmit the state of their fitness values based on a fuzzy logic system to the source CH, and the CH transmits the report to the neighbor node with high fitness. This neighbor node is used as a verification node to verify the votes on the report through a symmetric key in the report.

#### 3.3. Fuzzy Logic System

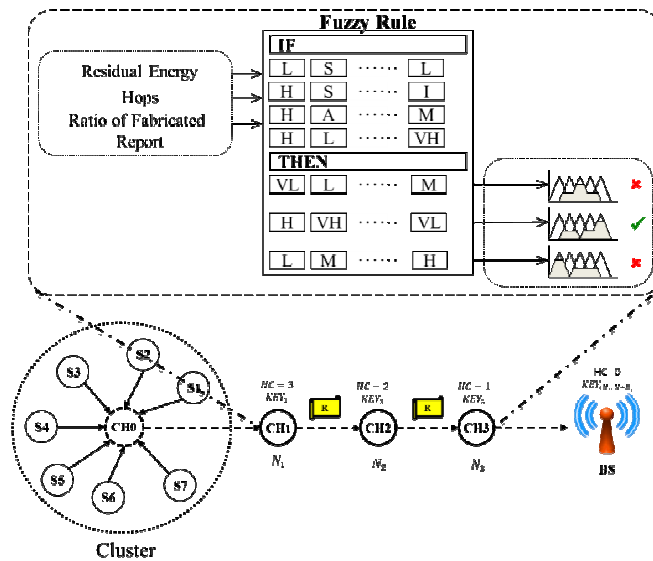


Figure 5. Fuzzy logic system process

Figure 5 shows the operating process of the fuzzy logic system. In the figure, when CH0 selects the verification path to report the transmission, which is selected as the nodes with high fitness in the neighboring area, the inference of the fuzzy logic system is the min-max centroid of the mamdani, and defuzzification uses the centroid technique. Input factors are the residual energy, hops, and ratio of fabricated reports.

- Input factors

- 1) Residual Energy = {LOW, HALF, HIGH}

- 2) Hops = {SHORT, AVERAGE, LONG}

- 3) Ratio of Fabricated Report = {VERY\_LOW, LOW, MEDIUM, HIGH, VERY\_HIGH}

- 1) Residual Energy

The sensor node needs to have efficiency when using the scheme due to the limited energy available. WSN protocols consider the energy of the sensor nodes. The original scheme could shorten the network lifetime as well as the unnecessarily high energy consumption of the nodes because of the fixed threshold verification node. Therefore, the residual energy of the node is very important information for the fuzzy logic system when verifying node selection.

- 2) Hops

The number of hops is count of the number of connections of the path from the position of sensor node until the BS. This path causes energy consumption at the nodes depending on the ratio of fabricated reports. For example, if there is a case of a legitimate report, intermediate nodes use resources efficiently, shortening the distance to the BS. Otherwise, sensor nodes use energy unnecessarily due to the long intermediate distance to the BS.

- 3) Ratio of Fabricated Report

The ratio of the fabricated reports represents the strength of the attack in the WSN. In a WSN environment, if there is a high ratio of fabricated reports, sensor nodes are able to save energy of the sensor nodes as a result of the probabilistic verification of the intermediate node. Otherwise, if the ratio of the fabricated report is low, the sensor nodes consume energy unnecessarily because of probabilistic verification of the intermediate node to low since the intermediate node verifies for duplication in the report. Finally, a probabilistic verification of the intermediate node is different according to ratio of the fabricated reports.

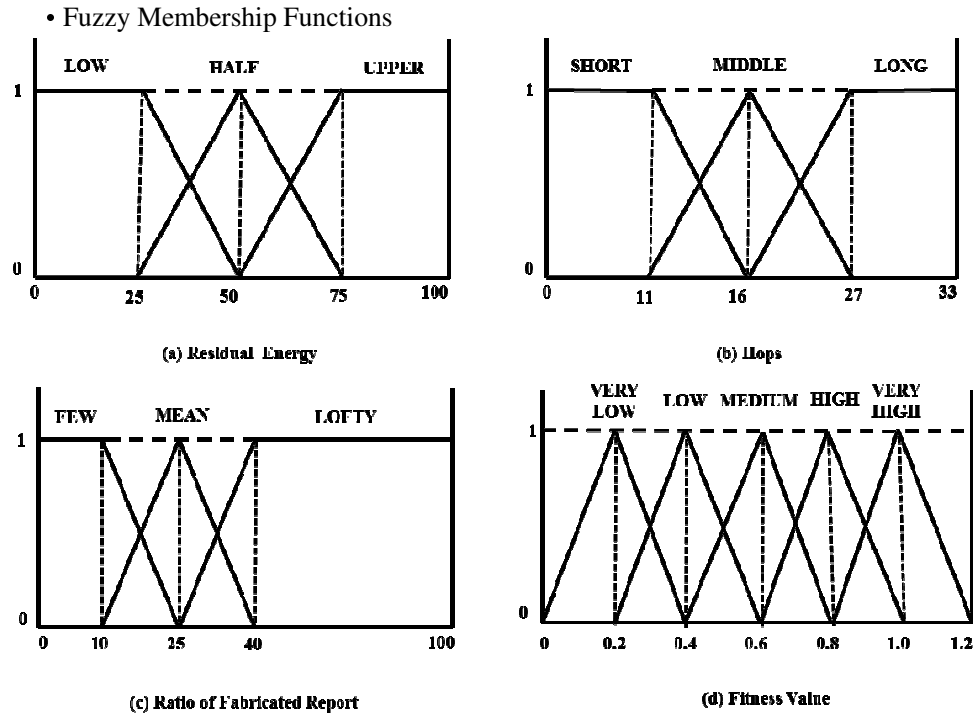


Figure 6. Membership functions of the input and out parameters.

Table 1. Fuzzy if-then rules.

Rule No.	Input			Output
	ENG	HOP	FTR	FV
0	L	S	F	VL
1	L	S	M	L
2	L	S	M	L
3	H	M	F	M
4	H	L	L	H
...	...	...	...	...
26	U	S	F	L

### 3.4. Proposed Verification Path Election Scheme

After the report generation phase,  $CH_0$  receives votes from the normal nodes that are connected on their own.  $CH_0$  attaches votes to the report and  $CH_0$  transmits the message to the neighboring nodes ( $N_{r1}$ ,  $N_{r2}$ ) to verify the votes of the report.  $N_{r1}$  and  $N_{r2}$  transmits their own fitness values to  $CH_0$  transmits the reports to the node with high fitness in the neighboring nodes ( $N_{r1}$ ,  $N_{r2}$ ). The verification path election algorithm is as follows:



```

Cluster Head  $CH_0$ 
Neighbor Node  $N_{r1}, N_{r2}$ ;
 $CH_0$  receives votes of normal nodes; // normal nodes transmit the vote.
 $CH_0$  finds neighbor normal nodes; // The neighbor node are CHs.
IF neighbor nodes are NOT NULL AND
fitness ( $N_{r1}$ ) > fitness ( $N_{r2}$ ) THEN
Send R to  $N_{r1}$ ;
 $N_{r1}$  migrates to new  $N_{ri}$ ;
IF fitness ( $N_{r2}$ ) > fitness ( $N_{r1}$ ) THEN
Send R to  $N_{r2}$ ;
 $N_{r2}$  migrates to new  $N_{ri}$ ;
    
```

In the Table 2,  $N_{r1}$  and  $N_{r2}$  are selected randomly by  $CH_0$ , R is the generated report generated by  $CH_0$ . Finally,  $N_{ri}$  selects the next neighbor nodes when  $T_f = 2$  has been not reached.

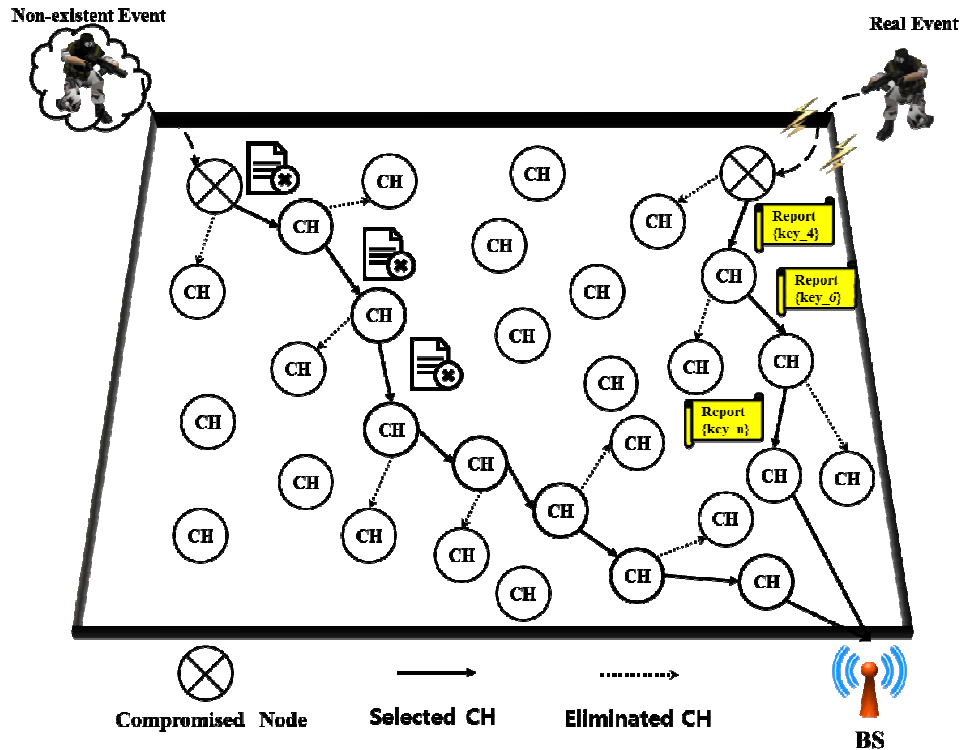


Figure 7. Process of verification path election.

Figure 7 shows the process of verification of the path election. The original scheme attempts verification node selection based on a pre-set path, which uses energy unnecessarily because they are fixed. Therefore, this scheme needs a solution due the effects on the network lifetime of WSNs. In this paper, the proposed scheme fluidly selects the next verification path to use energy efficiently. In the figure, the source CH randomly selects a neighbor node out of two for report verification. They transmit their own fitness based on a fuzzy logic system to the source CH. CH transmits the report to the node with high fitness. The node verifies the votes through a symmetric key on the report after the report is received. The proposed scheme decreases energy use and operation overhead through the fuzzy logic system. However, in a WSN environment, if there are

many legitimate reports, the sensor nodes will have operational overhead. In the experiment, the ENSF scheme efficiently used the energy of the sensor nodes.

#### 4. EXPERIMENTAL RESULTS

In order to validate the effectiveness of the proposed scheme, we compared it against PVFS via a simulation. We assume that the sensor field size is of  $1500 \times 2000 m^2$ , where 6,000 nodes are uniformly distributed. The base station is located at the end of the field, and each sensor node consumes 16.25/12.5  $\mu J$  to transmit/receive a data byte, and each MAC generation consumes 15  $\mu J$  [8]. The size of a legitimate report is 40 bytes and, the size of a MAC is 1byte. Each cluster consists of ten nodes, and each node can store a symmetric key. We have prepared five graphs that show a comparison between the proposed scheme and PVFS when implemented in WSNs. Figure 8 shows the energy consumption with respect to the ratio of attacks. Figure 9 shows the energy distinction, and Figure 10 shows the ratio of false votes with respect to the ratio of attacks, Figure 11 is the ratio of filtering, and Figure 12 shows the network life time.

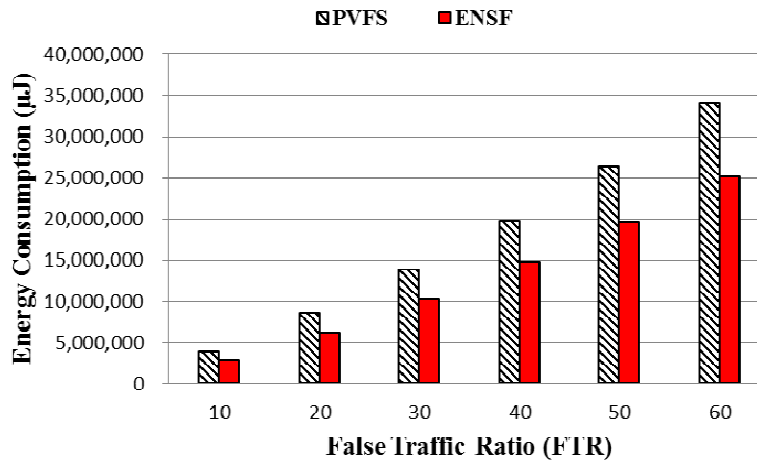


Figure 8. Energy consumption.

Figure 8 compares the energy efficiency of ENSF to that of PVFS. The proposed scheme shows a steady and significant energy savings for different FTRs. The reason is that proposed scheme uses a new verification path election scheme which considers the residual energy of a node before selecting it as the verification node. On the other hand, in the original scheme, unnecessary energy is wasted with fixed paths and verification nodes. The proposed scheme can save energy when subjected to false traffic. Therefore, ENSF scheme consume about 7 percent less energy than original scheme.

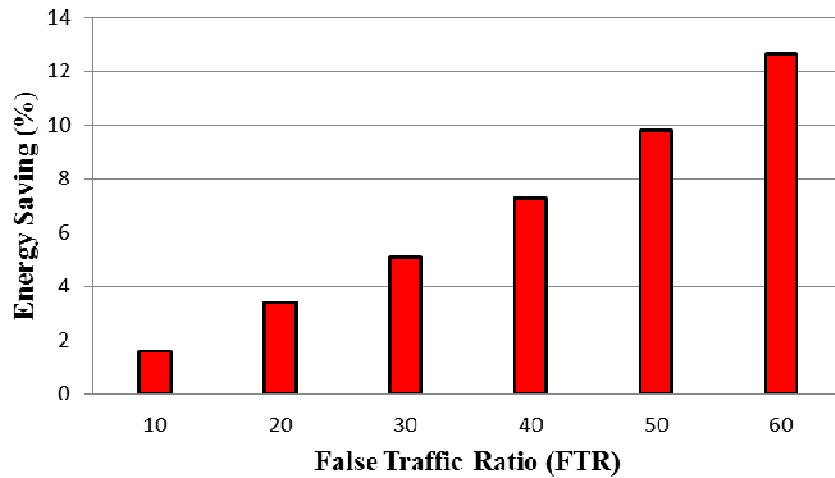


Figure 9. Percentage of energy saving by ENSF over PVFS.

Figure 9 shows the ratio of energy according to the ratio of attacks. In the figure, the proposed scheme improves energy savings up to 13% when we have an experiment between 10 and 60 percent false traffic. The reason is that the proposed scheme minimized traffic (operation, transmission, path distance).

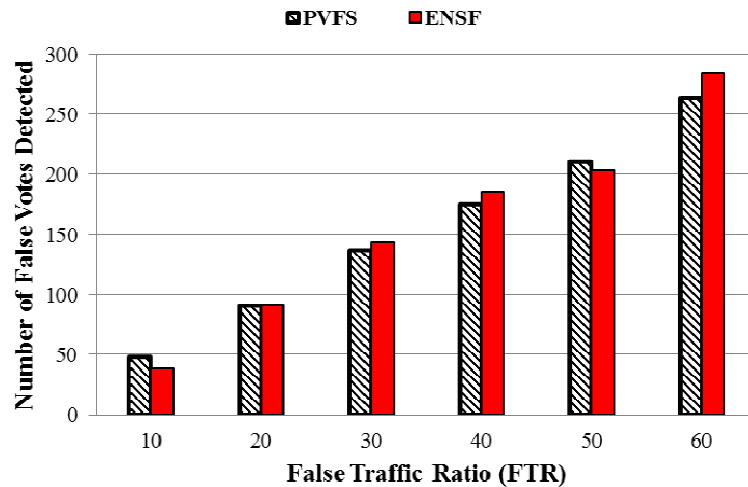


Figure 10. Numbers of false vote.

Figure 10 shows the ratio of the false vote detection of the proposed scheme and the original scheme. In the figure, the proposed scheme has a high ratio of false vote detection relative to the original scheme when the ratio of attacks is 30, 40, and 60 percent.

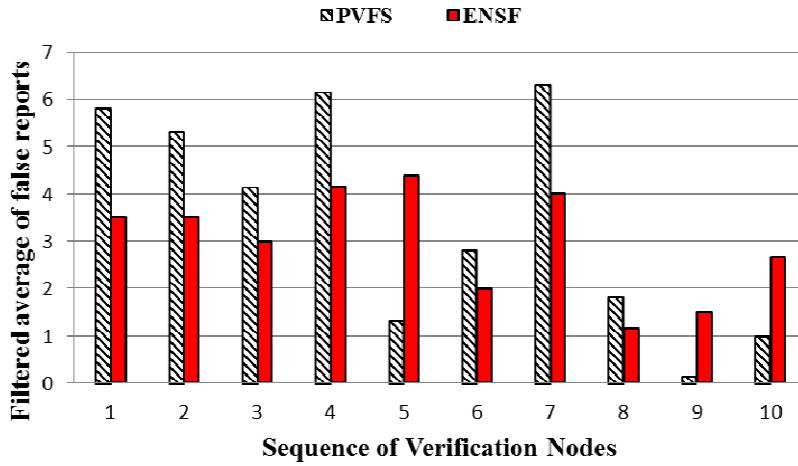


Figure 11. Average of false reports.

Figure 11 shows the filtering number with respect to each hop. In the figure, the proposed scheme has many filter numbers relative to the original scheme in 5, 9, and 10 of the hops. On average, the proposed scheme had a low ratio of filtering of the fabricated reports than did the original scheme, and the energy consumption of the sensors was improved.

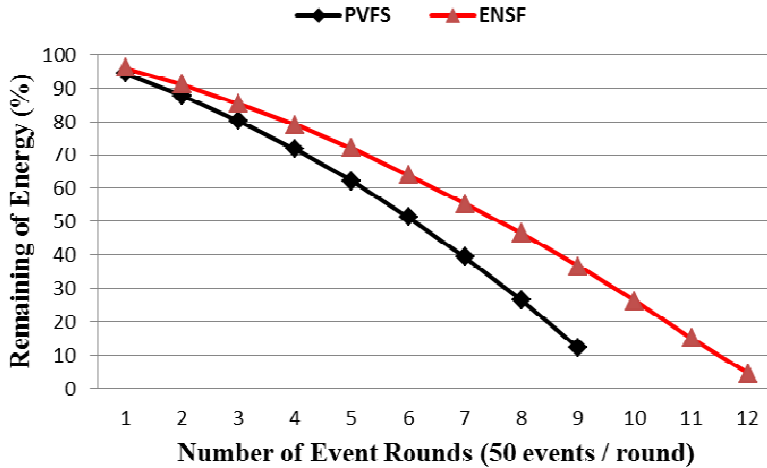


Figure 12. Network lifetime.

Fig. 12 shows the network lifetime of the ENSF and the PVFS. In the experiments, when the network lifetime is measurement according to the ratio of the attack. The numbers of events for each is 50. The lifetime of PVFS is 9 rounds and the lifetime of the ENSF is 12 rounds. In the figure 12, network is disconnected in the PVFS more quickly compare to the ENSF. Therefore, the ENSF extends to network lifetime compared to the PVFS.

## 5. CONCLUSION AND FUTURE WORK

PVFS was proposed by Li and Wu as a countermeasure against fabricated reports and false vote attacks in WSNs. This scheme uses a security threshold to detect attacks about false report and false vote. The scheme consumes the energy of the sensor nodes because it has a fixed threshold and verification node. In this paper, we propose a verification path election scheme based on a fuzzy logic system to efficiently use the energy of the nodes. The scheme compares the state of neighboring nodes for the report transmission. The input for the neighbor node selection is the energy, the number of hops, and the ratio of the fabricated report. The proposed scheme considers the state of the next node when the intermediate node transmits the report to the next node. Therefore, the proposed scheme can decrease the ratio of the sensor node and the overhead of the communications because of the selection of the next node is more efficient than that in the original scheme. In the experiment, the proposed scheme improves energy consumption on average by 7 percent and a maximum of 13 percent. For future work, some AI algorithms will be applied in order to find future optimal solutions and security.

## 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] K. C and W. D, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, vol. 1, pp. 293-315, 2003.
- [2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Mag, vol. 40, pp. 102-114, Aug, 2002.
- [3] J. N. Al-Karaki Kamal, "Routing techniques in wireless sensor networks: a survey," Wireless Communications11, 2004.
- [4] B. P, D. S and A. P, "SIA: Secure Information Aggregation in Sensor Network\*," ACM, pp. 255-265, 2003.
- [5] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Network: A predistribution and Local Collaboration-based Approach," Proc. of INFOCOM, pp. 503-514, 2005.
- [6] S. S, J. S and P. N, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," IEEE, pp. 259-271, May, 2004.
- [7] 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.
- [8] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," IEEE J. Sel. Area Comm, vol. 23, pp. 839-850, 2005, April, 2005.
- [9] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," Journal of Network and Computer Applications, vol. 33, pp. 63-75, 3, 2010.
- [10] C. Karlof, N. Sastry and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," ACM, pp. 162-175, 2004.
- [11] J. H. Chang, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE, vol. 12, pp. 609-619, Aug, 2004.
- [12] F. Li and J. Wu, "A Probabilistic voting-based Filtering scheme in wireless sensor networks," Proc. IWCMC, pp. 27-32, July, 2006.
- [13] F. Li and J. Wu, "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks," Inderscience Enterprises Ltd, pp. 173-182, Aug, 2008.
- [14] H. Y and S. Lu, "Commutative Cipher Based En-route Filtering in Wireless Sensor Networks," IEEE, pp. 1223-1227, Sept, 2004.

- [15] R. Lu, X. Lin, H. Zhu and X. Li, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol. 23, pp. 32-43, Jan, 2012.
- [16] 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.

### 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.



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.

