ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: https://doi.org/10.29121/granthaalayah.v5.i11.2017.2340

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

METHOD FOR THE PERIOD DETERMINATION OF SECURITY LEVEL UPDATE IN STATISTICAL EN-ROUTE FILTERING

Tae-Ho Cho [*1], Jung-Sub Ahn [2]

[*1] College of software, Sungkyunkwan University, Republic of Korea

[2] College of Information and Communication Engineering, Sungkyunkwan University, Republic of Korea

Abstract

Energy management of WSN is one of the major issues. Many kind of attacks in WSN paralyze the network by exhausting node energy. Especially false report insertion attack, which is one of the several WSN attacks, is to inform users of false alarms as well as unnecessary energy consumption. F. Ye et al. proposed statistical en-route filtering to prevent false report injection attacks. In order to effectively use their scheme, techniques for determining thresholds using fuzzy logic have been studied. To effectively apply these techniques to the network, an appropriate security level period update should be set according to the network environments. In this paper, we propose a security period update method using fuzzy logic in order to improve the lifetime of the network in the statistical en-route filtering approach based on a wireless sensor network of the cluster environment. Normally SEF thresholds should be changed by a user according to the network environment. Our proposed method allows automatically setting the effective threshold for the environment by fuzzy logic. The experimental results show that the energy efficiency increased by 26.5%.

Keywords: Network Simulation; Wireless Sensor Network; Statistical En-route Filtering; False Report Injection Attack; Energy Efficiency.

Cite This Article: Tae-Ho Cho, and Jung-Sub Ahn. (2017). "METHOD FOR THE PERIOD DETERMINATION OF SECURITY LEVEL UPDATE IN STATISTICAL EN-ROUTE FILTERING." *International Journal of Research - Granthaalayah*, 5(11), 158-167. https://doi.org/10.29121/granthaalayah.v5.i11.2017.2340.

1. Introduction

A wireless sensor network (WSN) consists of hundreds to thousands of sensor nodes and a base station (BS), providing real-time monitoring of sensor fields in industrial, medical, and military applications. A sensor node consists of a processor, memory, a battery, and a wireless transmitter [1-2]. Due to battery limitations, research involving increasing the network lifetime considering limit factors is currently actively studied [3]. If an event occurs, the sensor node generates a report with detected information and sends it to the BS using a hop-by-hop technique to notify

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1069419

the user. Sensor nodes are vulnerable to physical attacks because they have limited memory and batteries, and are deployed in open environments [4]. The attacker can compromise the sensor node and generate a false report using the secret information contained in the node. In addition, the attacker can inject a false report with the wrong event data type into the networks, as shown in Figure 1.

Figure 1: False report injection attack

If a WSN consists of a cluster, false report insertion attacks are divided into two cases when the cluster head (CH) node that generates the report is compromised and when the member (MB) node that creates the authentication key is compromised. If the CH node is compromised, the attacker generates an arbitrary report and transmits it to the next node, causing false notification and energy exhaustion problems of intermediate nodes in the routing path [5-6]. If the MB node is compromised, it can generate a false event notification to the CH node, depleting the node energy of the cluster region and deploy incapacitating nodes. To minimize this problem, it is necessary to detect and remove the false report early and to filter out incorrect alarms to users. To prevent false report injection attack, F. Ye et al. proposed statistical en-route filtering (SEF) [7]. In SEF, it is important to set an appropriate security threshold because the security threshold has a trade-off relationship between power consumption and filtering probability. Security threshold determining methods using fuzzy logic was proposed to obtain an appropriate security threshold value [8]. However, this method does not consider the security update cycle of the node. If the update period is not taken into consideration, the worst case consumes more power.

In this paper, we propose a security period update method using the fuzzy logic to improve the energy efficiency of SEF-based WSNs. The proposed method automatically determines the update cycle considering network environment factors. Nodes that are updated on a periodic basis do not have to send the information messages needed for the update and can save energy by adjusting the security strength in a timely manner. We demonstrated the performance of the proposed method through performance analysis by the applied various environment. The experimental results show that the proposed method saves up to 26.5% of energy.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1069419

The remainder of the paper is organized as follows. In Section 2, we explain the statistical en-route filtering scheme and motivation. Section 3 introduces the proposed scheme using fuzzy logic. Section 4 details the experiment results and, finally, the conclusions of this study are discussed in Section 5.

2. Related Works

This section describes the background and motivation of this paper.

2.1. Statistical En-route Filtering (SEF)

F. Ye et al. proposed SEF to prevent false report injection attacks. SEF statistically filters false reports by adding threshold values for authentication to the report generated by the representative node. The intermediate node verifies the report when a false report is transmitted. In addition, the intermediate nodes block false reports, thereby reducing unnecessary energy consumption to the BS. The SEF method consists of four phase: the key distribution phase, report generation phase, intermediate filtering phase, and BS node verification phase. In the key distribution phase, the user sets various setting values including the threshold value before the sensor nodes are deployed in the target area. The higher the threshold, the greater the false report detection rate, which makes it difficult for an attacker to generate false reports. However, high thresholds require high power consumption to transmit reports. Each node is randomly distributed among the key sets divided by the partition in the global key pool created at the BS. Figure 2 shows the key distribution process, where p_1 to p_l denote the partition containing the key.

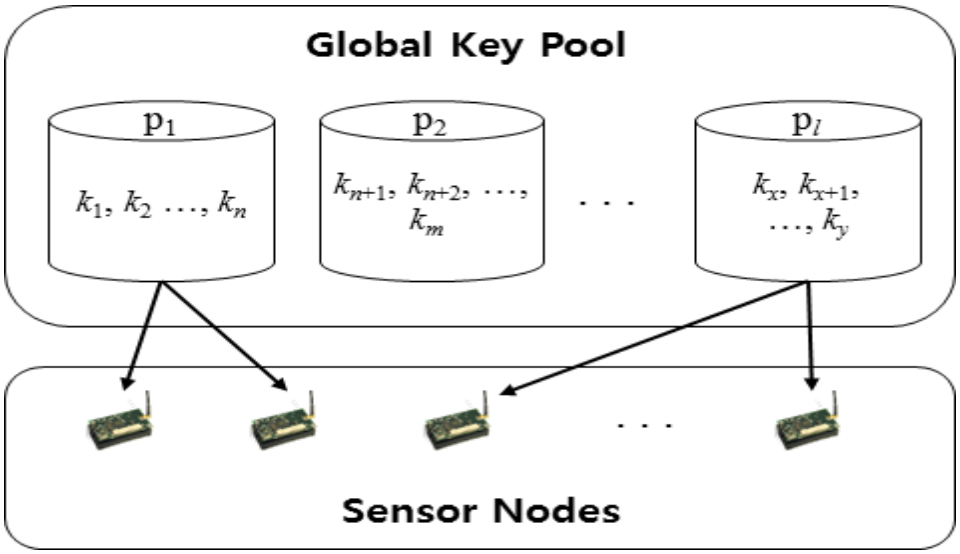

Figure 2: Key distribution phase in SEF

After the key distribution process is over, the nodes are deployed in the target area where they want to collect information. When the deployed sensor nodes detect the event, the node with the highest detection rate is selected as the representative node. The representative node broadcasts event information to find neighboring nodes that have detected the same event signal value. Neighboring nodes that have received the event information compare whether occurrence same event information. If the generated events are the same, the message authentication code (MAC)

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1069419

is generated and transmitted to the representative node using the pre-distributed key and hash function. The generated MACs are used to verify the report. The threshold value signifies the number of MACs included in the report when the representative node generates the report. If a MAC is collected that is smaller than the threshold for collecting MACs, no reports are generated. The representative node generates the report by including event contents and MACs that vary from one another as the threshold value. Since each node has a certain probability of a common key, it can probabilistically detect false reports. Event reports are transmitted to the BS node through multi-hop routing. If the forwarding node receives the report, it goes through the verification process shown in Figure 3.

1) Check that T { i_j, M_{ij} } tuples exist in the packet; drop the packet otherwise.

2) Check that the T key indices { i_j, 1 = j = T } belong to T instinct partitions; drop the packet otherwise.

3) If it has one key K ∈ { K_{ij}, 1 = j = T }, it computes M= MAC(K,L_e||t||E) using Equation 1. Determine if the corresponding M_{ij} is the same as M. If so, it sends the packet to the next hop; otherwise, the packet is dropped.

4) If it does not have any of the keys in { K_{ij}, 1 = j = T }, send the packet to the next hop.

Figure 3: Four operation phases of en-route filtering

M_{ij} refers to the MACs included in the report. The MAC consists of K, which is the key value of the node, Le is the event information, t is the event occurrence time, and E is the contents of the event. Finally, when the BS node receives the report, it verifies all MACs included in the report using the global key pool. If the BS node determines that it is a normal report after verification, it sends the event contents to the user.

Figure 4 shows the false report filtering process. In Figure 4, MAC_n refers to the MAC belonging to *n* partitions. The attacker must compromise the same number of nodes as the threshold value to generate a complete false report using the compromised node. In Figure 4, assuming that the partition compromised two different nodes in a situation where the threshold value is three, MAC_1 and MAC_4 are known, but MAC_2 is unknown. In the forwarding node, the node having MAC_2 compares it to the verification report to verify the compromised MAC and drops the report. This mechanism can reduce unnecessary energy consumption by performing intermediate filtering of false reports.

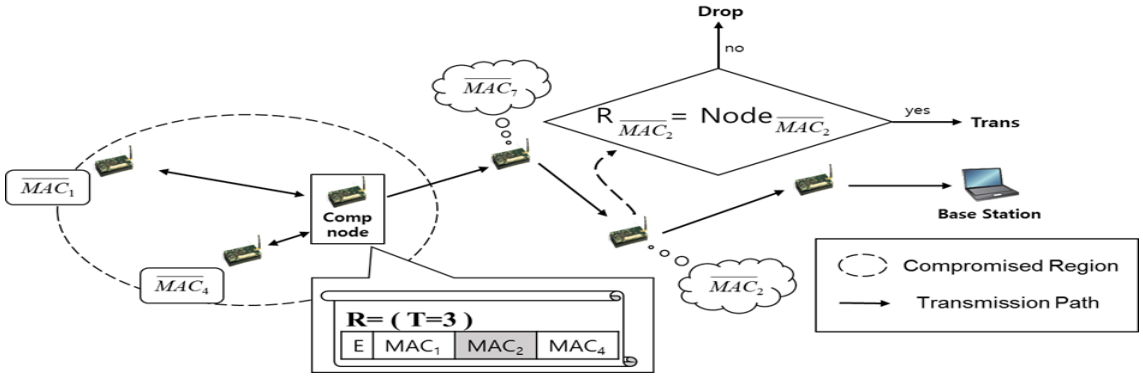

Figure 4: False report filtering process

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1069419

2.2. Motivation

Setting an erroneous threshold according to the environment in the SEF has an adverse effect on the energy consumption efficiency [9]. To perform this task, research was conducted to determine the threshold value using fuzzy logic [8]. However, we did not consider the cycle of updating the threshold value for efficient use of this scheme. If the update period is wide, the node information value must be requested to the node every time, which is inefficient in an environment where the attack rate does not change. Conversely, if the period is narrow, it is inefficient in environments where the attack rate changes frequently. Therefore, in order to manage energy efficiently, it is important to determine the threshold update period. In particular, a method of determining the threshold update period is needed to establish an adaptive fuzzy system that can reduce energy consumption while maintaining security.

3. Proposed Scheme

3.1. Assumptions

It is assumed that the plurality of sensor nodes is randomly placed in the destination field and arranged closely to each other. The route path is set during the pre-deployment phase and is assumed to use single-path routing. Each sensor node has a unique identification number. Each time the CH nodes transmit node information to the BS, the BS knows the specific information of the CH node. The WSN uses a cluster approach, which is advantageous because it considers performance and limited resources [10]. One cluster consists of a cluster head node and nine member nodes. Each member node collects the event and notifies the cluster head node, and the cluster head sends the report to the BS.

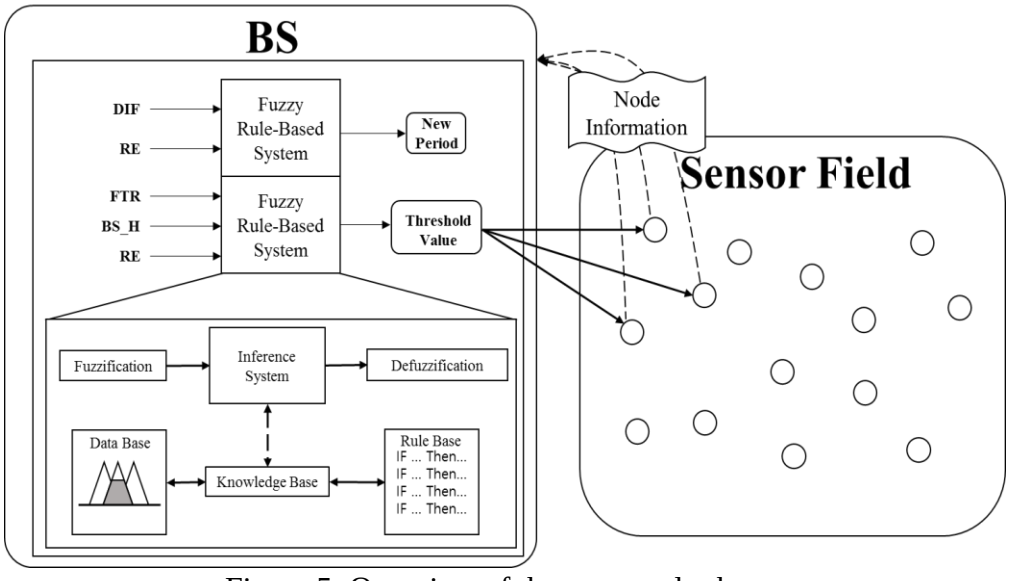

Figure 5: Overview of the proposed scheme

We analyzed the power consumption depending on the update period to the experimental environment based on SEF. Threshold determination fuzzy logic uses the information transmitted at a particular node to determine the threshold. Fuzzy inference uses the min-max

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1069419

composition [11] of the mandani model, which is one of the inference models, and the center of area (COA) method is used for the defuzzification method. Figure 5 shows that the CH node receives specific data and determines a new threshold value and new update period for the environment according to the update cycle. The FTR (False Traffic Ratio), BS_H (Base Station Hop), and RE (Residual Energy) were used fuzzy logic inputs for the new threshold value determination. And the DIF (Differential), RE (Residual Energy) were used Fuzzy logic inputs for new period determination.

3.2. Security Level Period Update Method

In the initial period in the CH, the CH transmits specific information such as the current set period value, the power consumption value of the node, and the attack rate to the BS. The BS transmits a new threshold value and period to the CH node after determining whether to update the update period through the received information and new period decision fuzzy logic. Figure 6 (a), (b) show the membership function to find the efficient update cycle. The input values are defined as follows.

- **Differential(DIF) = {L(Low), M(Middle), H(High)}**
- **Residual Energy(RE) = {VL(Very_Low), L(Low), H(High), VH(Very_High)}**

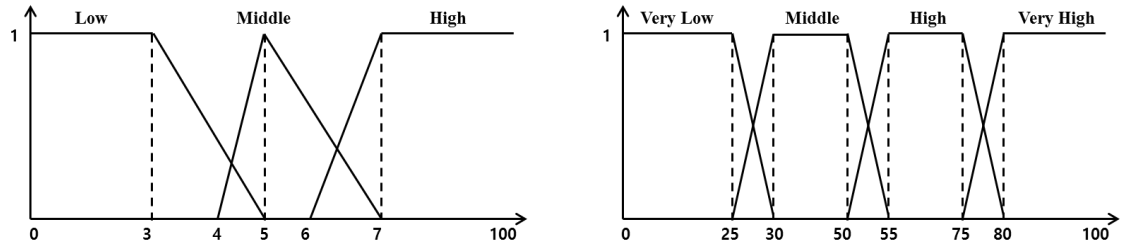

Figure 6: Fuzzy membership functions for new period

(a) DIF: The rate of change of the network environment is used to measure the network situation.
(b) RE: This value is calculated as a percentage of the energy remaining in the node. It is used to save energy consumption and increase the node life time.

DIF means the change rate of the environment of the network. If there is no change to the attack on the network, this value will be small. The BS evaluates the security rate for determining the new period. When the cycle is determined, the new threshold value is output using the fuzzy algorithm as shown below.

- **False Traffic Ratio(FTR) = {L(Low), M(Middle), H(High)}**
- **Base Station Hop(BS_H) = {VN(Very_Near), N(Near), M(Middle), F(Far), VF(Very_Far)}**
- **Residual Energy(RE) = {VL(Very_Low), L(Low), H(High), VH(Very_High)}**

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1069419

Figure 7 (a), (b), and (c) show the membership function to find the efficient threshold. The input values are defined as follows.

The proposed scheme adjusts the security strength and the energy consumption of the node by setting the attack rate, the energy state measured by the period, and the distance to the BS as the input value of the fuzzy system to set the new threshold value suitable for the current network situation. The new threshold and the new period are broadcast to the sensor network, as shown in Figure 5.

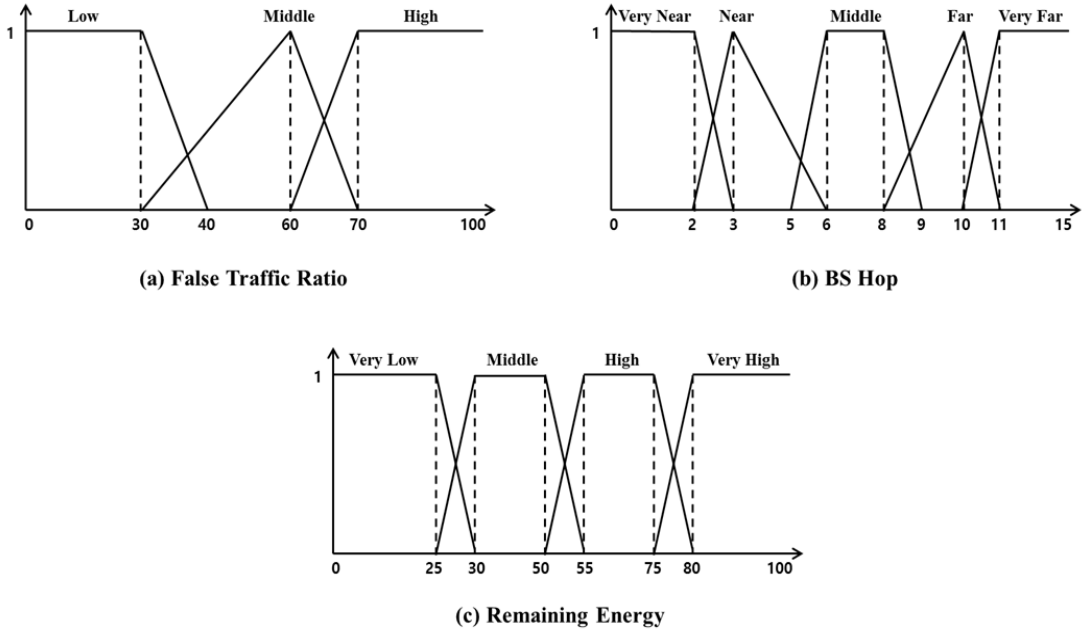

Figure 7: Fuzzy membership functions for threshold value

(a) FTR: The attack rate measured per cycle, which is used to improve the filtering performance.
(b) BS_H: The number of hops from the cluster head node to the BS. This can reduce energy consumption by considering the number of hops.
(c) RE: This value is calculated as a percentage of the energy remaining in the node. It is used to save energy consumption and increase the node life time.

Table 1: Fuzzy if-then rules for Period

Rule No.	Input		output
	DIF	RE	Period
2	L	L	P5
4	L	VH	P3
5	M	VL	P4
9	H	VL	P2
12	H	VH	P1

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1069419

Table 2: Fuzzy if-then rules for threshold

Rule No.	Input			output
	FTR	BS_H	RE	Threshold
7	L	N	H	T3
17	L	VF	VL	T2
24	M	VN	VH	T2
41	M	VF	VH	T4
56	H	F	VH	T5

4. Experimental Results

Table 3: Simulation parameters

Parameters		**Value**
Network Environment	Field Size	1,000 m x 1,000 m
	Number of Nodes	1,000
	Cluster Head Nodes	100
	Number of Event (Discrete Occur)	1,000
	Node Transmit Range	100–150 m
Transmit Size	Report Size	25 + MAC Size
	MAC Size	1 byte
	CH Node Info Size	2 byte
Energy Consumption	Transmit	16.25 μJ (per 1byte)
	Receive	12.5 μJ (per 1byte)
	Report Generation	70 μJ
	MAC Generation	15 μJ
	Verification	75 μJ
Security Value	SEF Threshold Value	2-10
	Key Number Per Node	1
	Global Key Pool Size	50

In this section, we compared the performance of the SEF with the fuzzy update period through experiments. Table 3 shows the parameter values for the experiment. The node information was created based on the Mica2 model [12]. The report size depends on the threshold value. The reason why the threshold value starts from two is that if the threshold value is one, even if only one node is damaged, a complete false report can be made. If the false report threshold is one, the BS cannot filter the false report. The threshold is updated every cycle and is determined by the fuzzy rule. The global key pool size is fifty and five partitions are used. Events occur one thousand times at random locations.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1069419

Figure 8: Energy consumption as a function of the FTR

Figure 8 shows the energy consumption of the FTR and fuzzy logic according to the threshold update period. SEF (T = 2) means the initial threshold set by the existing SEF scheme. As shown in Figure 8, the proposed scheme consumes less energy than the existing SEF scheme because it considers the environment and maintains the appropriate threshold.

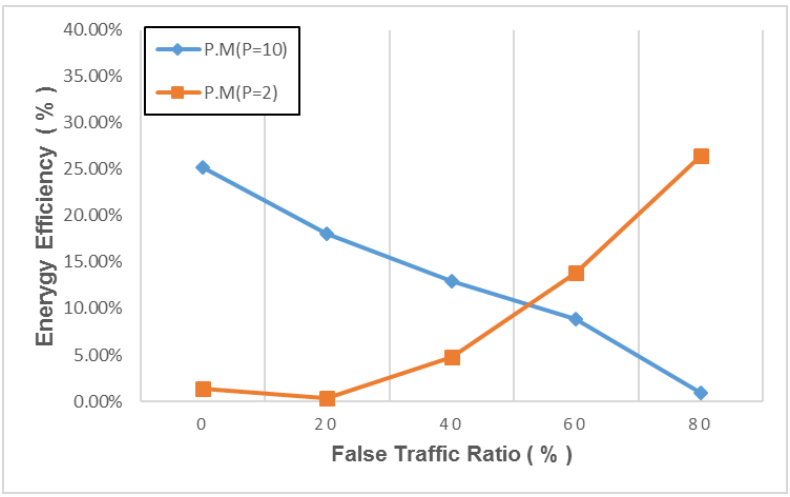

Figure 9: Increased energy efficiency with new update cycles

Figure 9 shows the graph of the energy efficiency comparison with the optimum cycles. When the thresholds are two and ten, the energy efficiency improved by up to 25.16% and 26.5%, respectively. If the user applies the proposed scheme in an area where the attack occurs frequently, it helps to save energy.

5. Conclusions

WSN is vulnerable to false report injection attacks because nodes are exposed to the open environment. To solve this problem, Fan Ye et al. proposed a SEF scheme that performs en-route filtering using a key. In statistical filtering techniques, thresholds affect energy management.

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.1069419

Although research has been conducted to establish thresholds appropriate to the environment, energy management is adversely affected if the cycle is set incorrectly because the threshold update period is not taken into consideration. In this paper, we proposed a method of updating the threshold value through the fuzzy logic to update the appropriate period of the threshold value suitable for the network environment. The experimental results show that the energy efficiency increased by 26.5% with the optimum cycles.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2015R1D1A1A01059484).

References

[1] Reejamol, K. J., and P. Dhanya Raj. "Hole handling techniques in wireless sensor networks: A survey." Computational Intelligence and Computing Research (ICCIC), 2016 IEEE International Conference on. IEEE, (2016)
[2] Nam, Su Man, and Tae Ho Cho. "A fuzzy rule-based path configuration method for LEAP in sensor networks." Ad Hoc Networks 31 (2015)
[3] Sen, Soumita, Chandreyee Chowdhury, and Sarmistha Neogy. "Design of cluster-chain based WSN for energy efficiency." Applied and Theoretical Computing and Communication Technology (iCATccT), 2016 2nd International Conference on. IEEE, (2016)
[4] Winkler, Thomas, and Bernhard Rinner. "Security and privacy protection in visual sensor networks: A survey." ACM Computing Surveys (CSUR) 47.1 (2014)
[5] Gupta, Pallavi, Vinay Prakash, and Preetam Suman. "Noticeable key points and issues of sensor deployment for large area Wireless Sensor Network: A survey." System Modeling & Advancement in Research Trends (SMART), International Conference. IEEE, (2016)
[6] Alanwar, Amr, et al. "PrOLoc: resilient localization with private observers using partial homomorphic encryption: demo abstract." Proceedings of the 16th ACM/IEEE International Conference on Information Processing in Sensor Networks. ACM, (2017)
[7] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal on, vol. 23, pp. 839-850, (2005)
[8] Kim, Cho. "Determination Method of Security Threshold using Fuzzy Logic for Statistical Filtering based Sensor Networks." Journal of the Korea Society for Simulation 16.2 27-35 (2007)
[9] Ahn, Cho. "A Correlation Analysis of the MAC Length in Statistical En-route Filtering based WSNS." International Journal of Advanced Research (IJAR) 4.8 (2016).
[10] Sahul, Ashwani, Bindiya, and Gursewak "Location Based-Balanced Clustering Algorithm for Wireless Sensor Network." International conference on Signal Processing, Communication, Power and Embedded System (SCOPES) (2016)
[11] Babuška, Robert. "Fuzzy systems, modeling and identification." Delft University of Technology, Department of Electrical Engineering Control Laboratory, Mekelweg 4 (1996).
[12] Quwaider, Muhannad. "Real-time intruder surveillance using low-cost remote wireless sensors." Information and Communication Systems (ICICS), 2017 8th International Conference on. IEEE, (2017)

*Corresponding author.
E-mail address: thcho@ skku.edu