International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

# Node Burden-based Load-balancing Management Method for Extended Network Lifetimes of WSNs

**Jung-sub Ahn, Tae-ho Cho**

***Abstract*: The sensor nodes of a wireless sensor networks (WSNs) are difficult to replace when they fails after deployment. Sensor nodes are small and low-cost due to limited resources and are vulnerable to several types of application attacks. To solve this problem, many security protocols have been meticulously researched considering the energy efficiency and network attacks. The statistical en-route filtering (SEF) scheme has been proposed to detect bogus data and false report injection attacks that reduce network life. SEF performs early filtering of modulated data using the en-route technique. Deployed nodes transmit a report to the sink node through hop-by-hop communication, and as a result nodes close to the sink node have a relatively high burden. Although many studies have been proposed to improve the energy efficiency of each node based on the SEF scheme, these studies are not considered the Burden of the cluster. A cluster with a high burden exhausts the node energy faster than another cluster with low burden. If a cluster in the upper stream is depleted, it will not be able to receive reports from many regions in the lower stream. Therefore, the SEF should be used to determine proper routing while considering the node density to increase the lifetime of the network. In this paper, we propose a method to control the load balancing of nodes considering the burden ratio and density of nodes. The cluster head node controls the route path using additional cluster information in the proposed scheme. The experimental results show that the proposed scheme prolongs the network lifetime efficiency by 35.645% compared to the existing scheme.***

***Keywords* : Cluster lifetime extension, Load balancing management, Routing bottleneck, Statistical en-route filtering, Wireless sensor networks***

## I. INTRODUCTION

Wireless sensor networks (WSNs), which are used for industrial, medical, and military wide-field monitoring, are composed of a large number of sensor nodes and several base stations (BS) [1][2][3]. Sensor nodes consist of a power unit, processor, sensor, memory and transceiver. Sensor nodes have limited memory and battery life because they are produced at a low cost [4]. Additionally, sensor nodes are vulnerable to false report injection attacks because they are deployed in an open environment for data collection over a wide field. An attacker can generate false reports utilizing the vulnerability of the compromised sensor node in various ways and then inject a false report with false data into the sensor network [5][6][7]. False report injection attacks notify a false event to the user and reduce the network lifetime. Fan et al. proposed a statistical en-route filtering (SEF) scheme based on a symmetric cryptography technique for detecting a false report injection attack [8]. SEF uses cooperative certification between nodes to check the report's legitimacy.

When nodes are deployed in hazardous areas such as a battlefield, it is difficult for nodes to be evenly distributed due to various environmental factors. Consequently, the density of nodes is determined based on many factors. More reports are received for nodes close to the base station if the nearby node density is low. SEF can apply various routing protocols such as Directed Diffusion, TTDD, and Low-Energy Adaptive Clustering Hierarchy (LEACH) [9][10][11]. SEF cannot know the residual energy of each cluster. If a cluster selects a new node with low energy, it will reselect new nodes in the near future, resetting the routing path many times. If the energy of the upstream node is depleted and no replacement node exists, the base station cannot collect events from downstream nodes. The base station cannot perform necessary tasks such as detecting intrusions when the node is disabled because it is impossible to collect reports from the region. In this paper, we propose a load-balancing method considering the node density and node burden for SEF to prevent this problem. In the proposed scheme, the node determines whether to re-nominate using periodically measured cluster energy information. The base station collects the load ratio information of clusters through the additional burden measure phase that transmits the burden value to upstream the leaf node at the routing initialization phase to calculate the cluster load. In this process, nodes can replace the node tables. The proposed method adjusts routing according to the node density of the cluster so that the load ratio of cluster nodes can be uniformly distributed. Therefore, the WSN can prolong the lifetime of the cluster by adjusting the burden of the region according to the expected life of the node. This paper is organized as follows. Section 2 introduces the related researches, the SEF security scheme and LEACH routing technique. Section 3 describes the proposed method in detail considering density. In Section 4, the validity of the proposed scheme is verified through the experimental results. Finally, Section 5 is the conclusion.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
**Jung-sub Ahn**, Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea. Email: sc4217@skku.edu
**Tae-ho Cho**, Department of Software Platform, Sungkyunkwan University, Suwon, Republic of Korea. Email: thcho@skku.edu

## II. BACKGROUNDS

### A. Statistical En-route Filtering (SEF)

Fan et al. proposed the SEF scheme to detect the false data injection of application layer attacks. Each node has a determined detection capability depending on the size of the assigned key. A base station and intermediate nodes verify the report for integrity. The SEF scheme has four phases: Key Deployment, Event Report Generation, En-route Filtering, and Sink Filtering, as shown in Fig. 1.

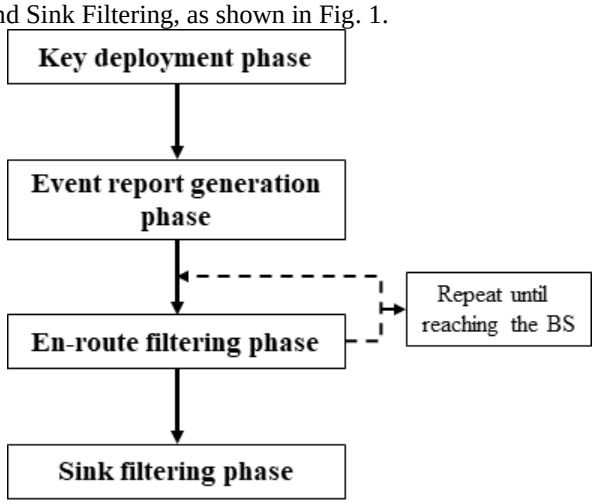


**Fig. 1. 4-phase SEF operation**

The base station distributes keys to the nodes for the report verification key during the deployment phase. First, the network manager sets the key partition size. After the base station creates the key pool by dividing the key into partitions, the nodes are then randomly assigned a key from the key pool.

The event report generation phase performs report generation and transmission. If a member node of a cluster detects an event, the member node generates a Message Authentication Code (MAC) and forwards it to the center of the stimulus node. The MAC structure is given as follows:

$$M_i = MAC(K_i, L_E || t || E)$$

$K_i$ is the key index, $L_E$ the event location, $t$ is the detection time and $E$ represents the event type. $M_i$ encryption uses the key K of the node and one-way functions. The center of the stimulus node generates a report using the MAC that includes the event information and key index [12]. The report includes a MAC selected randomly by a preset threshold. The generated MAC is used later to check the integrity of the report.

The En-route Filtering phase verifies the MACs of the reports. If an intermediate node receives the reports, the number of MACs is compared. The intermediate node receiving the report checks whether it has the key index in the report. If a node has the same key index, the node creates a new MAC using the node's key and the event information in the report. If the generated MAC and report's MAC match, the report is transmitted to the parent node. If the MAC does not match, the report is dropped. It also forwards the report to the parent node if it does not have the same key index. The En-route Filtering process is repeated until the report reaches the base station.

The Sink Filtering phase verifies all MACs in the report. The sink node can generate all MACs using the event information in the report because the sink node has a global key pool. In addition, the generated MAC can be used to fully verify the report. If all MACs are intact, the sink node sends the report contents to the network manager, and if the reports have modulated data, the sink node deletes the report.

### B. Low energy adaptive clustering hierarchy with deterministic cluster-head selection (LEACH)

Various routing schemes have been proposed to prolong the lifetime of WSNs. Handy proposed a LEACH routing method to a cluster between nodes with small complexity. Fig. 2 shows the LEACH protocol.

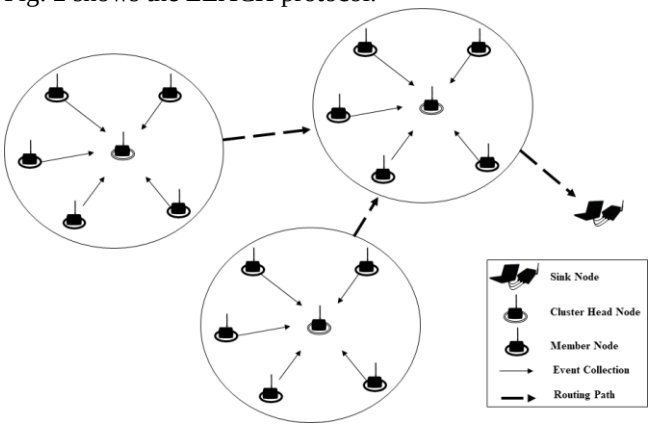


**Fig. 2. LEACH protocol**

The LEACH scheme consists of multiple clusters in a WSN with one representative node in a cluster [11]. When member nodes that are not a cluster head node in the cluster detect the event, the nodes transmit the event information to the cluster head node. The cluster head node generates a report using a received event from the member nodes. The report is forwarded to the BS through cooperative communication between the CH nodes selected in the WSN. LEACH rotates the cluster head nodes randomly according to a fixed probability, consuming energy evenly between the sensor nodes. This process distributes the load on the nodes so that the node energy in the cluster can be consumed evenly. However, LEACH does not consider other variables such as the residual energy, geographic location of the node, or cluster burden. Additionally, LEACH cannot check whether nodes maintain residual energy uniformly to use security schemes. The proposed scheme provides an efficient routing method by solving this problem.

## III. PROPOSED SCHEME

There are many replacement nodes that can function as a cluster head in a relatively high-density node region. However, when the node density is low, there are far fewer nodes available for the cluster head role as well. If the node located upstream is disabled due to an energy depletion problem and there are no alternative nodes, the BS cannot collect reports of all nodes downstream the disabled cluster region [13]. The proposed scheme prolongs the lifetime of the network via routing load adjustments of the cluster considering the density of the nodes. The node stores additional information such as replacement routing tables and the node burden value in the proposed scheme. When the cluster head node reaches a replacement threshold, the cluster head node

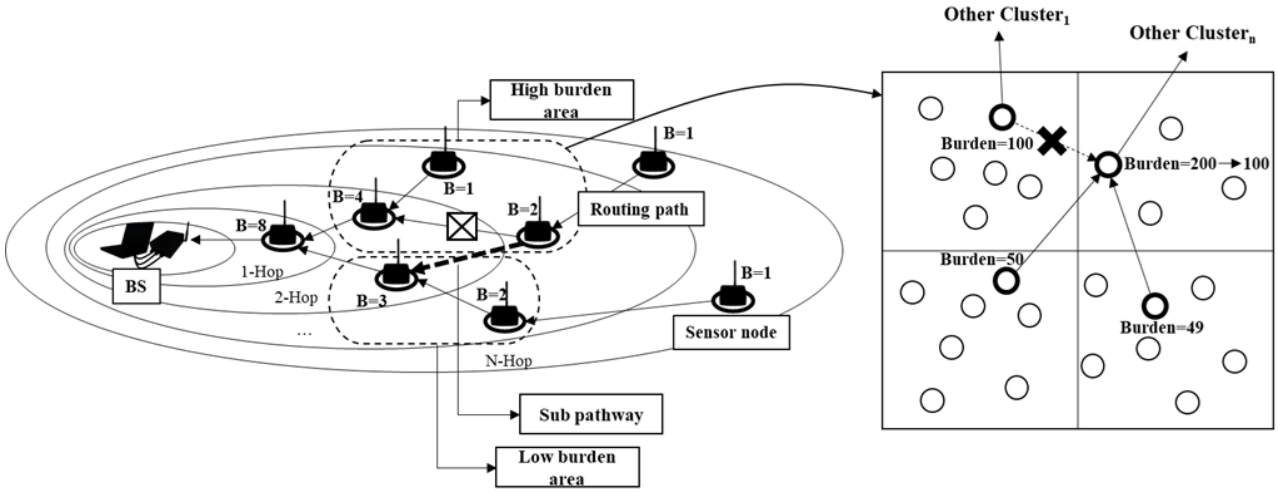


**Figure 3 Proposed scheme overview**

uses the additional information stored in the memory to find an efficient routing path. The proposed scheme controls a load of cluster head nodes to extend the life of the network. The proposed scheme is described in overview in Section 3.1. Section 3.2 details the proposed scheme process.

### A. Proposed Scheme Overview

This chapter briefly introduces the overall flow of the proposed scheme.

The burden is the amount of the cluster head node loads, i.e., the number of downstream cluster regions. The burden is set differently depending on many environmental factors. Therefore, the existing routing scheme is not efficient at extending the cluster lifetime because it is a static routing technique. A cluster with a high node density allows more reports. In particular, if the node located near the BS disabled, it is not possible to receive all of the reports of the child nodes. Therefore, it is necessary to control the load ratio. Network routing should be routed according to the load to extend network life. Fig. 3 shows an overview of the proposed scheme. The cluster head node calculates the burden value of the cluster using forwarded burden values from child nodes. Additionally, the sub-route of the selected node for the proposed scheme is determined by the replacement routing table. The cluster can extend the network lifetime by child routing replacement processes, which transfer child loads to other clusters.

### B. Detailed Proposed Scheme

This chapter describes the routing procedure in detail through the node density and burden distribution process for proposed method routing. The operation process of the proposed scheme consists of three steps.

In the first step, deployed nodes in a field organize the cluster as LEACH scheme and the cluster creates a routing table with the BS of the root node. Afterwards, the leaf nodes of a cluster transmit their own burden value upstream until the BS for burden organization. The detailed process is as follows.

(1) The sink broadcasts a Hello message, including its ID to its neighboring cluster heads.

(2) Upon receiving a Hello message, the sink checks whether its ID has been included in the message. If the message does not contain its ID, it records a path to the sink following the reversed order of the IDs in the message. It then appends its ID to the end of the message and broadcasts the message to all its neighbors. Node that completed the above process (CH) sets the flag to true.

(3) CH checks whether a node is a leaf node by overhearing Hello messages sent by its neighbors. If its path to the sink node is a sub-path of one of its neighbors' paths to the sink node, it is not a leaf node. Otherwise, it is a leaf node.

When the Hello message reaches the leaf node, the leaf node begins to transmit the burden value. The process of creating the burden table of the CH nodes is as follows.

1) All CH nodes have a burden value of 1 as the initialization value.

2) When each CH node receives all of the burden values from the nodes registered in its child table, it sums the received values and sends the calculated burden value to the upstream node.

Parent nodes know the child cluster burden ratio through the above process. The cluster head nodes know the load factor to cover the received burden. The CH nodes calculate the energy level for each round. A CH node requires the BS to change the routing according to its own energy level [14]. The CH selecting process has an additional phase for the node selection efficiency. In this process, the CH node checks the number of replaceable nodes in its cluster and the number of hops via the BS. If the CH node replacement condition is met, the path of the child node is changed. If the condition is not met, the node re-election process via the LEACH scheme is performed. The CH nodes are recognized by monitoring the energy status of the member nodes through periodic communication with the member nodes. Fig. 4 illustrates the path update process of the proposed scheme.

The elected child node can select the replacement node, except an existing parent node in the replacement table, as shown in Fig. 4. The child node knows the parent ID, the distance from the parent node to the sink, the parent burden value, and the number of replacement nodes of the parent node through the replacement table. The parent selection condition of the child node is as follows.

1. Exclude a node that has previously been selected as a parent node.

2. The smaller the distance between the node and BS in the replacement node list, the higher the selection priority.

3. There must not exist a parent node for the upstream node of the selected node.

4. The node with the lowest burden value of the parent node has the highest priority.

5. If the same score nodes have existed, a node is selected according to the number of replacement nodes of the parent node.

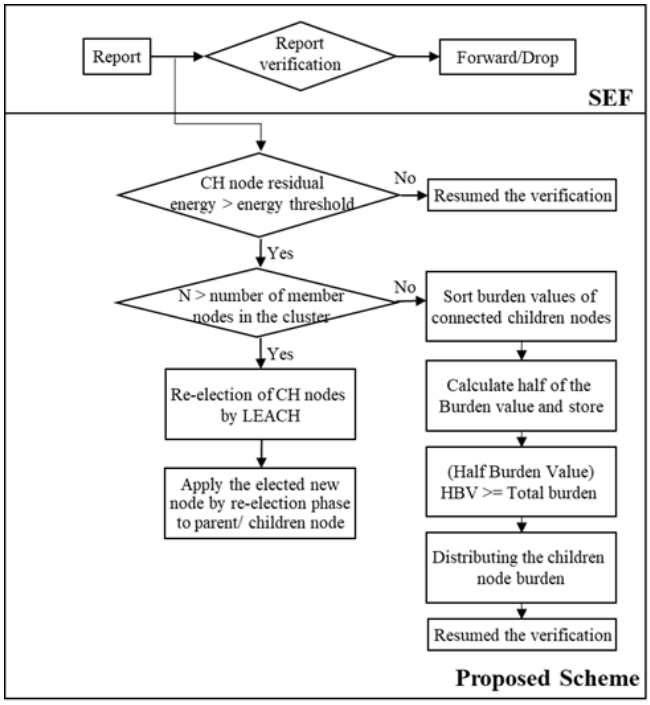


**Fig. 4. Path re-election process in the proposed scheme**

The node selects an efficient node as the parent node in the replacement table according to the above process. The number of replacement nodes of the parent node is analyzed first, and the parent node with the most replacement nodes has the highest priority.

Additionally, the proposed scheme calculates the life expectancy of the cluster. As a result, our scheme improves the network activation time and transmits more event reports to the BS through the cluster burden control.

## IV. EXPERIMENT

This chapter shows the results of various experiments on the proposed scheme.

### A. Assumption

Multiple sensor nodes are randomly and densely deployed in the destination field using various deployment methods [15]. It is assumed that each sensor node is not compromised during the deployment phase. The nodes are given unique identification numbers. The BS stores the global key pool with the nodes' full keys. The WSN experimental environment is composed of 1600 clusters and static nodes. A cluster in the field consists of one cluster head node and several member nodes. If the sensor node detects an event, the CH node collects the MAC from event detection nodes. The CH generates a report and transmits the report to the BS after collecting enough MACs to generate a report. It is assumed that the report is not compromised during transmission. Nodes of experiment environments applied the specifications of MICAZ [16].

### B. Experimental environment parameters

**Table- I: Experiment parameters**

| parameters | | value |
|---|---|---|
| ***Field Environment*** | Sensor Field Size | 1400m x 1400m |
| | Number of Nodes | 16000 |
| | Number of Clusters | 1600 |
| | Number of Compromised Nodes | 100 |
| | Number of Occurred Event | Depend on node life |
| | Base Station Location | (x,y) = (700m,700m) |
| | Node Transmit Range | up to 150m (Mica2) [16] |
| ***Transmission Information*** | Report Size | 30bytes |
| | Key Index | 14bit [19] |
| | A MAC Size | 1byte |
| ***Energy Consumption*** **[8]** | Transmit | 16.25μJ (per 1byte) |
| | Receive | 12.5μJ (per 1byte) |
| | MAC Generation | 15μJ |
| | Verification | 75μJ |
| | Cipher | 9μJ |
| ***Security Value*** | SEF Threshold Value | 3 |
| | Key Number per a Node | 1 |
| | Global Key Pool Size | 5 |

### C. Experiment Results

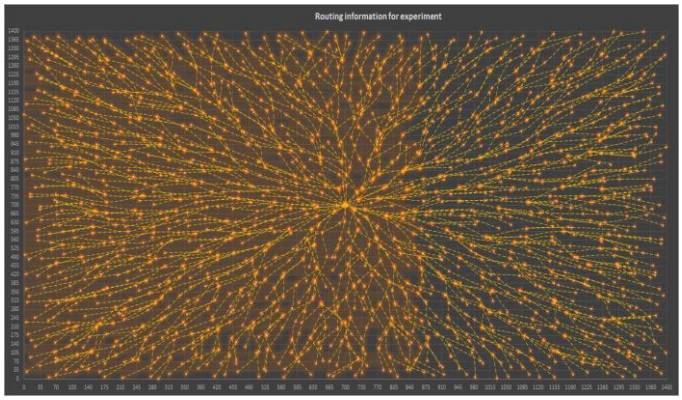


**Fig. 5. Routing information of the proposed scheme**

Fig. 5 shows the routing path in this experiment environment. The nodes configure the routing path using the Directed Diffusion algorithm. The two-dimensional field is 1400m x 1400m and a cluster size is 35m x 35m. The BS position is located at (700m, 700m), which is the center of the field. Clusters close to the BS have a relatively large number of child clusters to cover, as shown in Fig. 5.

Fig. 6 shows the burden of each cluster measured at the end of the cluster life in the experimental environment of the SEF and proposed scheme.

The x-axis and y-axis represent the cluster area, and the z-axis represents the burden value. As shown in Fig. 6, the closer the cluster is to the BS center, the higher the cluster burden. The proposed scheme has a mitigated load rate because the cluster performs load balancing through the routing path reset. The proposed method shows that the load ratio of one cluster is reduced by up to 29.3% compared to the existing method.

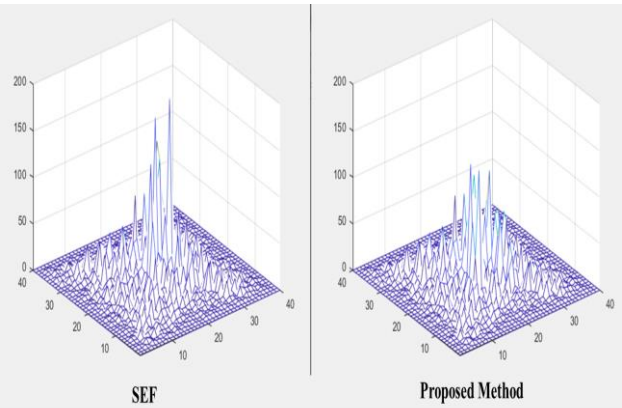


**Fig. 6. Comparison of the burden of clusters between SEF and the Proposed Method**

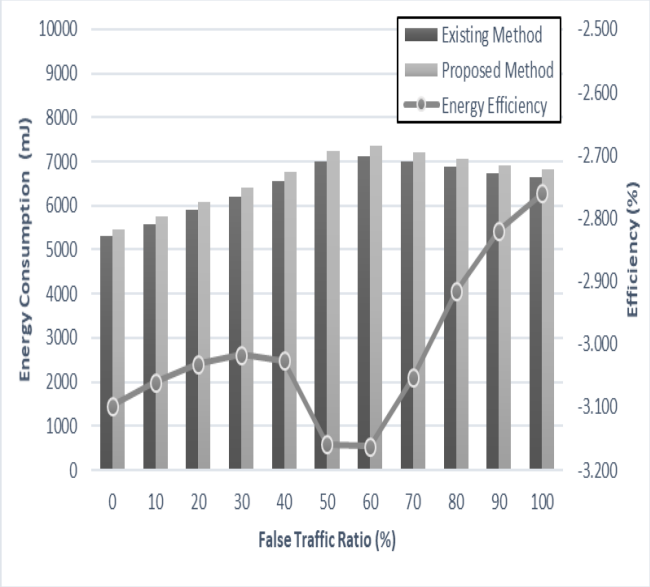


**Fig. 7. Energy consumption versus FTR**

The report hops increased because the CH node chooses the efficient route rather than the shortest route to prolong the cluster lifetime. Therefore, the proposed scheme consumes more total network energy than the existing scheme, as shown in Fig. 7. The experimental results show that the proposed method consumes 3.009% more energy than the traditional method. The attack rate and energy consumption rate are proportional to some extent according to Fig. 7; this is because of the higher attack ratio leads to more false reports being dropped, which increases the overall network lifetime.

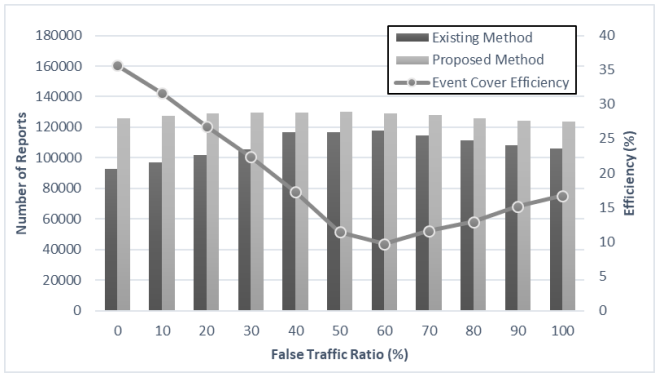


**Fig. 8. Received BS reports versus FTR**

Fig. 8 shows the received BS reports versus false traffic ratio (FTR) until a cluster is deactivated. At a 0% attack rate, the proposed method allows 35.645% more reception than the traditional method. In a safe environment without attacks, the proposed method shows the best efficiency because it distributes the load of the cluster to the surrounding clusters. The proposed scheme received 19.202% more reports on average than the existing method through the cluster load distribution. In other words, this result can be analyzed as an increase in the cluster lifetime of the proposed scheme.

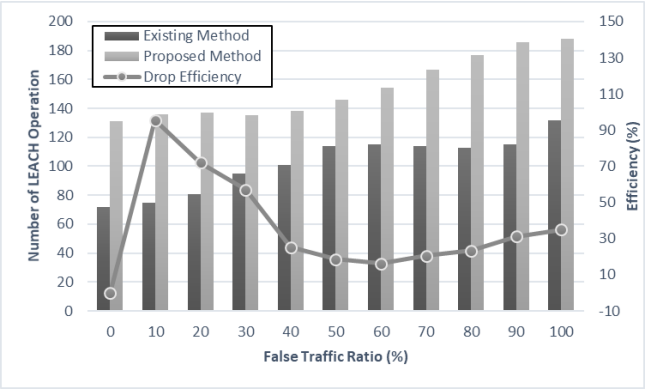


**Fig. 9. Number of LEACH operation**

Fig. 9 shows the number of CH node re-elections for the LEACH scheme in a cluster.

The proposed scheme adjusts the load balancing of the cluster using the burden value set in the post-deployment phase. Therefore, the proposed scheme has more CH node re-election than SEF. For this reason, the proposed scheme increases the filtering efficiency of false reports more than the existing scheme.

## V. CONCLUSIONS

Nodes in a large WSN have limited energy and processing capability and collect monitoring data in the destination field through self-organization. In general, since sensor nodes are irregularly deployed, a routing method considering the density of nodes is required. In this paper, we improved the lifetime of the cluster by managing the load ratio of nodes. Our method requires an extra phase for the nodes to know additional information about the child or parent, but the extra phase has little overhead.

Our scheme allows administrators to apply thresholds flexibly to various network environments [17][18][19][20]. If the set threshold is high, the overall lifetime of the network is reduced. However, this also increases the lifetime of the cluster.

It is important to balance the energy consumption and cluster lifetime to efficiently operate the WSN, but this is beyond the scope of this paper. We experimentally demonstrated that the overall network energy consumption rate of the proposed scheme is high, but the cluster survival time increased. Our proposed method has been demonstrated with SEF, but can be applied to various security protocols.

## ACKNOWLEDGMENT

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-2018R1D1A1B07048961)

## REFERENCES

1. Đurišić, Milica Pejanović, et al. "A survey of military applications of wireless sensor networks." 2012 Mediterranean conference on embedded computing (MECO). IEEE, 2012.
2. Chi, Qingping, et al. "A reconfigurable smart sensor interface for industrial WSN in IoT environment." IEEE transactions on industrial informatics 10.2 (2014): 1417-1425.
3. Zhang, Yuan, et al. "Ubiquitous WSN for healthcare: Recent advances and future prospects." IEEE Internet of Things Journal 1.4 (2014): 311-318.
4. Jangra, Ajay. "Wireless sensor network (WSN): Architectural design issues and challenges." (2010).
5. Pathan, Al-Sakib Khan, Hyung-Woo Lee, and Choong Seon Hong. "Security in wireless sensor networks: issues and challenges." 2006 8th International Conference Advanced Communication Technology. Vol. 2. IEEE, 2006.
6. Anwar, Raja Waseem, et al. "Security issues and attacks in wireless sensor network." World Applied Sciences Journal 30.10 (2014): 1224-1227.
7. Singla, Aashima, and Ratika Sachdeva. "Review on security issues and attacks in wireless sensor networks." International Journal of Advanced Research in Computer Science and Software Engineering 3.4 (2013).
8. Ye, Fan, et al. "Statistical en-route filtering of injected false data in sensor networks." IEEE Journal on Selected Areas in Communications 23.4 (2005): 839-850.
9. Luo, Haiyun, et al. "TTDD: Two-tier data dissemination in large-scale wireless sensor networks." Wireless networks 11.1-2 (2005): 161-175.
10. Intanagonwiwat, Chalermek, Ramesh Govindan, and Deborah Estrin. "Directed diffusion: A scalable and robust communication paradigm for sensor networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.
11. Handy, M. J., Marc Haase, and Dirk Timmermann. "Low energy adaptive clustering hierarchy with deterministic cluster-head selection." 4th international workshop on mobile and wireless communications network. IEEE, 2002.
12. Ye, Fan, et al. "Gradient broadcast: A robust data delivery protocol for large scale sensor networks." Wireless Networks 11.3 (2005): 285-298.
13. Gou, Haosong, and Younghwan Yoo. "Distributed bottleneck node detection in wireless sensor network." 2010 10th IEEE International Conference on Computer and Information Technology. IEEE, 2010.
14. Jo, O., and Tae-Wook Kwon. "Data Direction Aware Clustering Method in Sensor Networks." The Journal of Korean Institute of Communications and Information Sciences 34.7B (2009): 721-727.
15. Gajbhiye, Pradnya, and Anjali Mahajan. "A survey of architecture and node deployment in wireless sensor network." 2008 First International Conference on the Applications of Digital Information and Web Technologies (ICADIWT). Ieee, 2008.
16. Kramer, Marc, and Alexander Geraldy. "Energy measurements for micaz node." University of Kaiserslautern, Kaiserslautern, Germany, Technical Report KrGe06 (2006).
17. Yu, Zhen, and Yong Guan. "A dynamic en-route scheme for filtering false data injection in wireless sensor networks." Proceedings of the 3rd international conference on Embedded networked sensor systems. ACM, 2005.
18. Nam, Su Man, and Tae Ho Cho. "Context-aware architecture for probabilistic voting-based filtering scheme in sensor networks." IEEE Transactions on Mobile Computing 16.10 (2016): 2751-2763.
19. JungSub, Ahn, and Cho TaeHo. "An Enhancement of Cluster-Based False Data Filtering Scheme Through Dynamic Security Selection in Wireless Sensor Networks." International Journal of Computer Networks & Communications (IJCNC) Vol 11 (2019).
20. Li, Feng, and Jie Wu. "A probabilistic voting-based filtering scheme in wireless sensor networks." Proceedings of the 2006 international conference on Wireless communications and mobile computing. ACM, 2006.

## AUTHORS PROFILE

**Jung Sub Ahn** received his B.S. degree in computer information from Kyungil University, Korea, in February 2016. 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, network security, context aware architecture, and modelling & simulation.

**Tae Ho Cho** received his Ph.D. in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Computing at Sungkyunkwan University, Korea. His research interests include wireless sensor networks, intelligent systems, modeling and simulation, and enterprise resource planning.