FUZZY LOGIC-BASED EFFICIENT MESSAGE ROUTE SELECTION METHOD TO PROLONG THE NETWORK LIFETIME IN WSNS

Jungsub Ahn[1] and Sanghyeok Lim[2] and Taeho Cho[3*]

[1]Department of Electrical and Computer Engineering,
Sungkyunkwan University, Republic of Korea
[2]Amorepacific Republic of Korea
[3*]Department of Computer Science and Engineering,
Sungkyunkwan University, Republic of Korea

ABSTRACT

Recently, sensor networks have been used in a wide range of applications, and interest in sensor node performance has increased. A sensor network is composed of tiny nodes with limited resources. The sensor network communicates between nodes in a configured network through self-organization. An energy-efficient security protocol with a hierarchy structure with various advantages has been proposed to prolong the network lifetime of sensor networks. But due to structural problems in traditional protocols, nodes located upstream tend to consume relatively high energy compared to other nodes. A network protocol should be considered to provide minimal security and efficient allocation of energy consumption by nodes to increase the network lifetime. In this paper, we introduce a solution to solve the bottleneck problem through an efficient message route selection method. The proposed method selects an efficient messaging path using GA and fuzzy logic composed of multiple rules. Message route selection plays an important role in controlling the load balancing of nodes. A principal benefit of the proposed scheme is the potential portability of the clustering-based protocol. In addition, the proposed method is updated to find the optimal path through the genetic algorithm to respond to various environments. We demonstrated the effectiveness of the proposed method through an experiment in which the proposed method is applied to a probabilistic voting-based filtering scheme that is one of the cluster-based security schemes.

KEYWORDS

Wireless sensor network, Fuzzy logic, Load balancing, Genetic algorithm.

1. INTRODUCTION

Wireless sensor networks (WSNs) are used for environmental monitoring through data collection in various fields, such as industrial Inter of Things (IIoT), military, and healthcare systems. They are consist of many sensor nodes as MicaZ and a fully-featured base station (BS) [1-3, 31]. If an event occurs, detected sensor nodes generate a report of the corresponding event and send it over multiple sensor node hops to the BS. However, sensor nodes are vulnerable to attack because of various disadvantages such as limited resources, a random distribution in an open environment, independent operations, and difficulties in individual node management.

As shown in Fig. 1, the attacker exploits this weakness to compromise nodes using various kinds of attacks. These attacks cause unnecessary processing in the node, shortening the lifespan of the node and interfering with the transmission control. Several protocols have been proposed to increase network security and lifetime by defending against such attacks [4-9], [35-38]. Most of these methods involve cluster-based routing. Cluster-based routing benefits from the local

management of nodes and makes systemic report generation possible. However, there are some disadvantages. A routing path consisting only of a Cluster Head (CH) node can be easily burdened with energy consumption loads to a certain CH when that CH is no longer usable due to battery discharge. In particular, in a protocol in which a CH is not re-elected, if the corresponding node is out of service, the region detected by that CH becomes a shadow region and further detection and report generation become impossible [10].

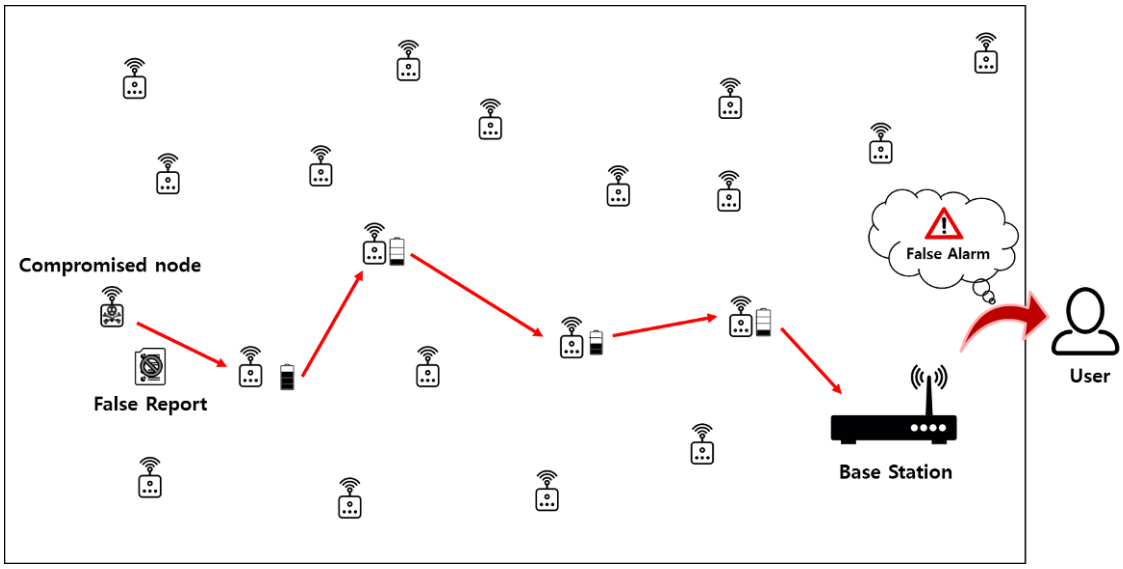

Figure 1. An attack on a WSN

To prevent such problems, a low-energy adaptive clustering hierarchy with deterministic cluster-head selection (LEACH) has been proposed as an algorithm for the re-election of report generation nodes [11]. However, this algorithm does not consider the state of the node, but simply re-elects it with a binary probability. Thus a better method is needed to improve the efficiency of the whole network. The proposed scheme performs load balancing using fuzzy logic considering the energy states of the nodes, event occurrence rate, and the geographical importance of the nodes. The nodes that are tagged through the proposed system are classified as nodes with a high risk of energy exhaustion. The existing routing path is reconfigured to include only untagged nodes; the tagged node performs only event detection and reports generation to save energy. In this way, the range of nodes that are incapable of receiving events is minimized and the success rate of report transmission for normal events is increased.

The proposed scheme can be applied to various security protocols through the evaluation function related to the selection of verification nodes. Experiments on the proposed method are applied to a probabilistic voting-based filtering scheme (PVFS), specifically one from a cluster-based security protocol. In this scheme, the security, energy efficiency, node survival rate, and report transmission success rate are all measured. The composition of this paper is as follows. In Section 2, the PVFS and fuzzy theory are explained. In Section 3, the problems of the existing routing and the proposed scheme are explained. In Section 4, the experimental results and the results of the proposed scheme are analyzed. Finally, in Section 5, conclusions are given.

2. BACKGROUNDS

2.1. Probabilistic Voting-Based Filtering Scheme (PVFS)

A PVFS [6] is a typical cluster-based security protocol. It simultaneously defends against false report injection attacks and false message authentication code (MAC) injection attacks. Nodes randomly arranged in the target field form clusters between neighbouring nodes within the communication range to generate reports through cooperative communication between nodes. Fig. 2 shows the en-route filtering process of the PVFS. In the PVFS, the node with the smallest ID in each cluster is selected as the CH, and CH re-election does not occur. The en-route filtering consists of four steps.

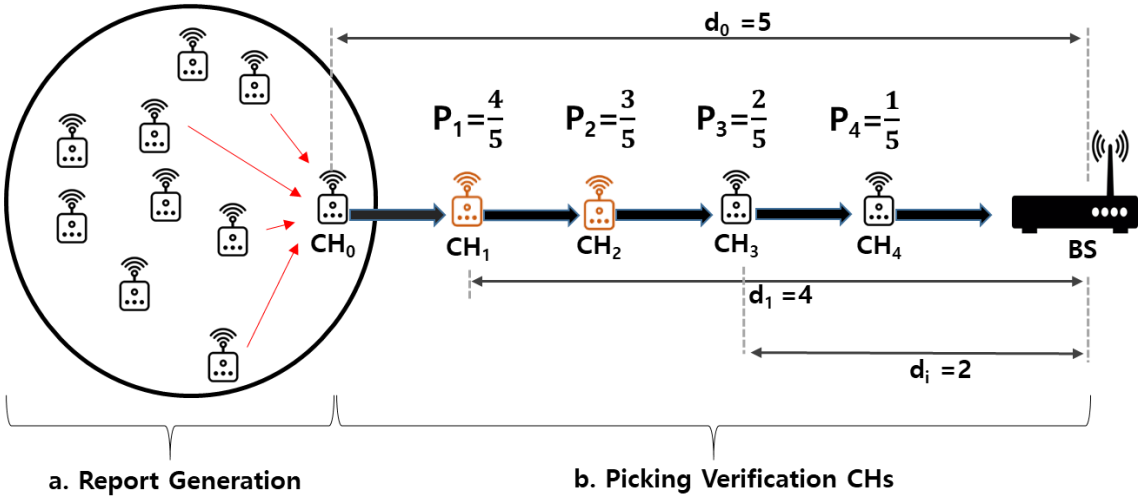

Figure 2. En route filtering of the PVFS

(1) Key distribution and report generation phase: The BS loads to each CH node a set of keys separated by cluster unit. The CH distributes one key to each member node. Every node has a single key.
(2) Selection step of the verification node: An intermediate CH to be a verification node probabilistically selects a verification node based on the distance configured by routing based on the shortest path algorithm. The CH node selected as the verification node receives one of the keys of member nodes randomly after exchanging the session key with the member nodes of the event detection cluster.
(3) If nodes detect an event, they generate MAC based on the detected event and forward it to the CH node. The CH node collects MACs and then attaches them to the report to generate a report to be transmitted.
(4) Verification step: Upon receiving the report, the verification node first verifies that its key index is within the range of the MAC's key index attached to the report. If the key indices overlap, a MAC check is performed. otherwise, the report is forwarded to the node on the following path. If the MAC verification result through one's own key is determined as a normal report, a normal vote is cast. When an incorrect MAC is detected, the false MACs count increases. When another verification node detects false MAC again and the number of votes reaches a pre-set threshold, the report is immediately identified as false and deleted. If the threshold has not been reached, it is considered a normal report and transmitted to the base station.

2.2. Fuzzy Logic System

Fuzzy logic is based on the fuzzy set concept introduced by Professor L. A. Zadeh of the University of California at Berkeley in 1965 to quantitatively express the ambiguity of natural language [14].

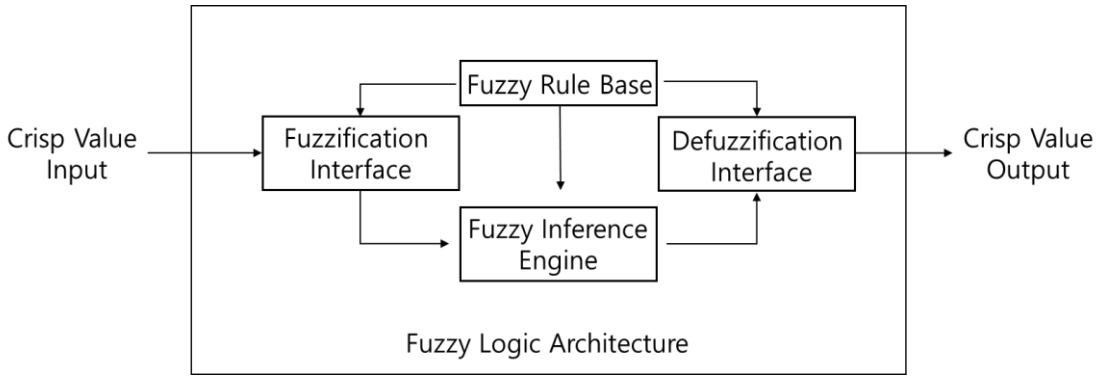

Figure 3. Fuzzy controller

In well-known propositions or sets, only objects that are objectively meaningful, such as true or false, are dealt with. However, in real-life situations, things are rarely true or false. The mathematical tool for dealing with such ambiguous criteria is the fuzzy set theory. Thus, in fuzzy theory, unclear or subjective criteria can be explained using propositions, aggregation, etc. The process of fuzzy control can be largely divided into three parts [13-16]:

- Fuzzification Interface
- Fuzzy Inference Engine
- Defuzzification Interface

The fuzzification interface handles the process of replacing crisp input values measured by the fuzzy feedback control system with the respective language values and membership functions associated with the fuzzy rules. The fuzzification of correct values is shown in Fig. 4.

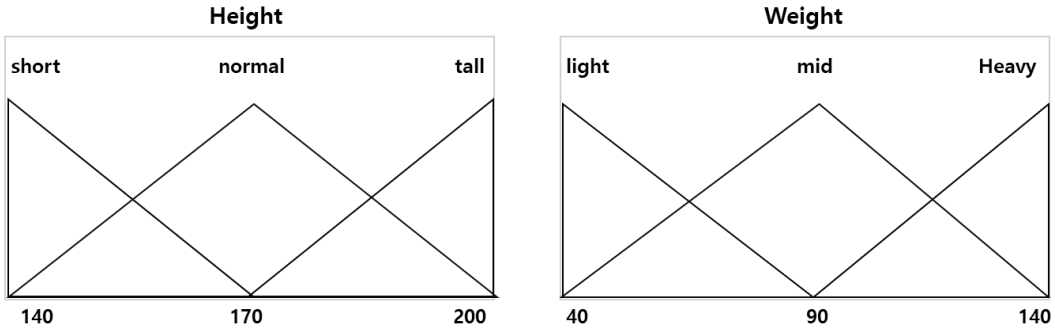

Figure 4. Fuzzy membership functions

Fuzzy inference is a process of deducing a result with membership values obtained through fuzzy logic and by inferring a fuzzy input using a fuzzy rule. Said differently, the fuzzy inference is the process of deducing an appropriate setting with respect to a fuzzy membership function. The fuzzy inference rule base corresponds to the controller of the system. The rule base is based on a

truth table logic, which is a set of rules associated with fuzzy sets, input variables, and output variables that determine what occurs in each case.

The inverse fuzzy function is used to transform the fuzzy output value into an equivalent crisp value that is easily interpretable by humans. There are various methods for the reverse fuzzy process, including center-of-gravity methods and the Mamdani inference method. Today, fuzzy functions are applied to various items, including washing machines, cameras, fermented food, automobile brakes and engines, color film phenomena, manufacturing processes, weather analysis, and artificial intelligence. Fuzzy functions are also used to classify information that mimics certain social phenomena [17-21].

3. PROPOSED METHOD

3.1. Problem Statement

The main purposes of WSNs are to gather information about events that occur in vast areas that are difficult for a user to reach directly and mount an appropriate response. If the report of the detected event is not successfully transmitted to the BS, this defeats the main purpose of a WSN, which is to receive information about events occurring in distant locations. Similarly, if the energy of the node is depleted, then event detection in the corresponding region is not possible. Further, if the residual energy of the sensor nodes is high but the events to be delivered are not properly transmitted, the sensor nodes distributed in those areas become useless. In an environment where WSNs are installed, there are many areas where the user cannot distribute nodes directly and the nodes are scattered randomly, thus rearrangement of nodes is difficult. In the case of a cluster-based security protocol without re-election of the CH, a zone appears where the energy of the CH is exhausted and detection of events in the area becomes impossible.

Each node has a different number of downstream nodes depending on its location. The tail refers to the number of CHs that use the node to forward detected events to the BS, as shown in Fig. 5. For CHs positioned at the edges of the field, the tail value of the corresponding node is zero. A node that has many tails consumes a large amount of energy while sending, receiving, and verifying the reports, and plays an important role in transferring event reports occurring in other regions. When these nodes are deactivated, the event detection node must elect a new path excluding the deactivated node to transmit the report. In most cluster-based protocols, the CH is chosen only once during the initial node dispatch phase. Therefore, events detected in the downstream area of the inactive node cannot be detected anymore. The risk of energy exhaustion is higher within these CHs that are located closer to the BS. Therefore, even if the total consumption of nodes deployed in the network increases, it is important to increase the number of event detection reported to BS by modifying routing with an approach based on geographic elements and residual energy of nodes.

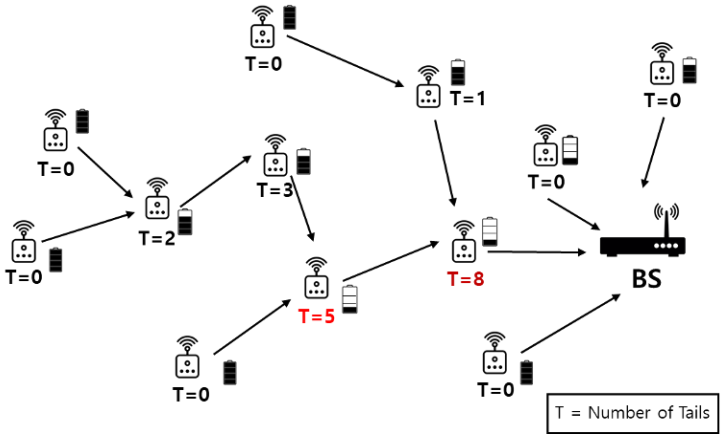

Figure 5. Importance of node geography on energy consumption

3.2. System Overview

This section presents an overview of the proposed system. All CHs are equipped with a node tag decision system. This system is software running on the top of the CHs. The node tag system determines whether or not to tag a node depending on the proposed fuzzy system. A node tag decision system runs periodically on CH nodes and reconfigures the routing throughout the system. Every CH has a list of the IDs of the nodes that are closer to the BS within its communication range. IDs list is used to select a new routing path, except the tagged node among the list members.

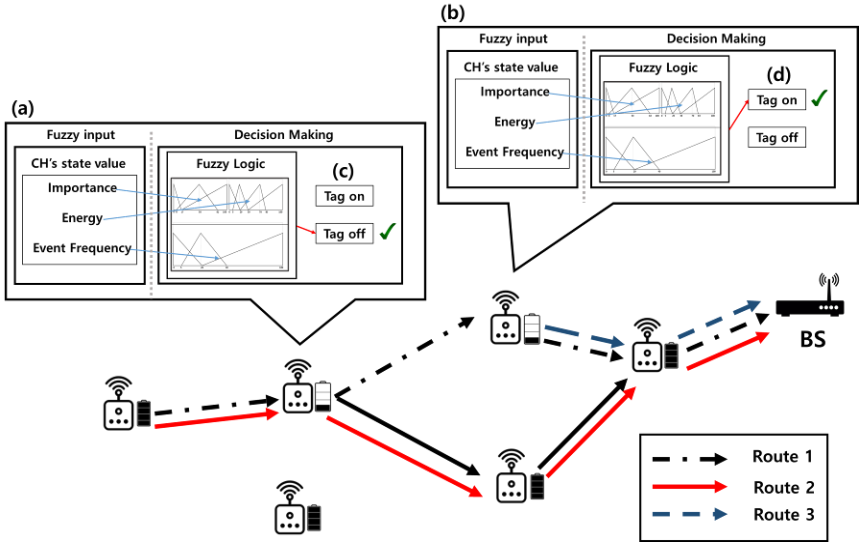

Figure 6. Fuzzy logic-based routing management

Fig. 6 shows a resetting of the routing in the proposed scheme. Each CH checks whether its energy reaches a predetermined energy threshold during each cycle. A node that reaches the threshold value initiates the fuzzy logic system, which inputs its geographical importance, available energy, and event occurrence frequency, and checks whether the node is at risk of energy exhaustion. Nodes that are determined to be at risk of exhaustion are tagged. A tagged node breaks all routing to itself for the remaining lifetime of the battery and performs only event detection and report generation, as shown in Route 3 of Fig. 6. Each CH also has a routing list, as shown in Fig. 7. Nodes with depleted energy are dropped from the list, whereas the tagged nodes

remain on the list but are excluded from routing priority. As shown in Fig 7-(b), if all nodes in the Routing node list are tagged, the next forwarding node is selected according to DST to BS (Destination to Base Station). By managing the routing list in this way, nodes can avoid the confusion that can occur in energy-starved or tagged situations and prevent routing bottlenecks, which can cause the number of hops to the BS to increase.

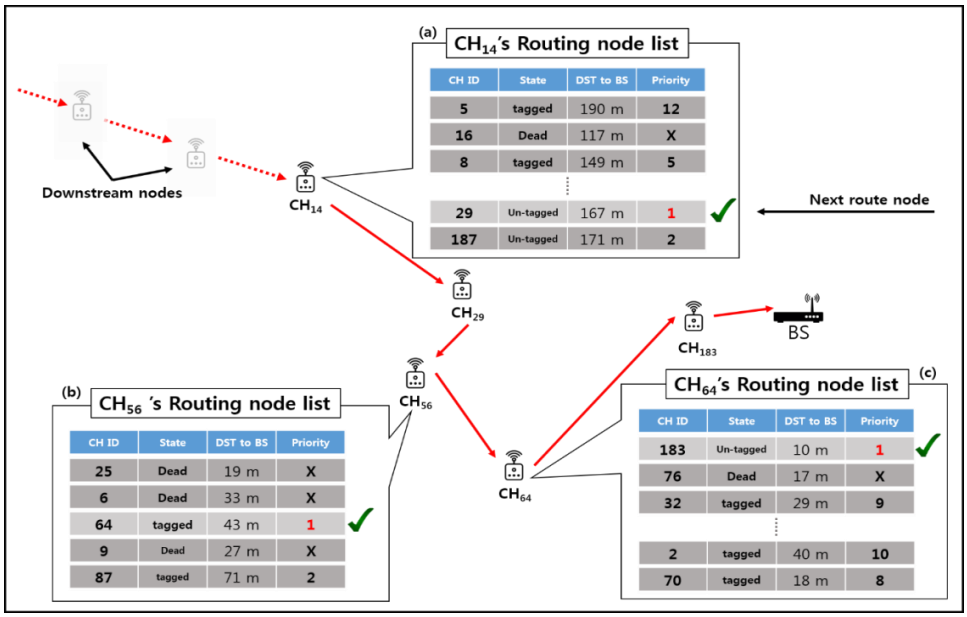

Figure 7. Routing node list and routing priority

Fig. 7 shows the routing of a proposed scheme for the WSN field using CHs using cluster-based security protocols [4], [6], [8], [9], [35], [36]. Node (c) in Fig. 8 is tagged and blocks all incoming routes to itself. It performs only event detection and report generation until the battery runs out. In the case of node (a) in Fig. 8, the routing to node (c) is blocked and the routing is re-selected based on its routing node list. However, the routing to node (c) in Fig. 8 is forcibly rerouted because it has no other options. In the case of node (b) in Fig. 8, the routing to node (c) in Fig. 8 is cut off, and the routing is changed by selecting the next priority node in the routing list.

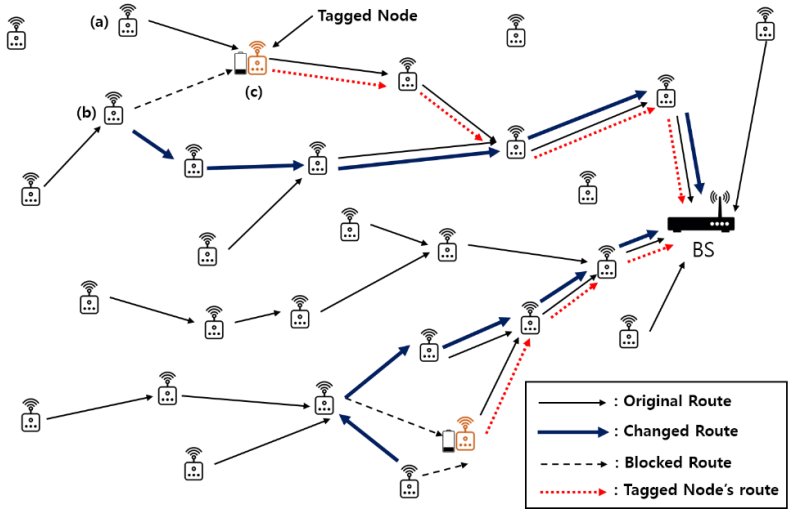

Figure 8. Dynamic routing with the proposed scheme

3.3. Fuzzy Inputs

The proposed scheme exploits a fuzzy rule-based system for CH load balancing. Part of the advantages of fuzzy rule-based systems is that they output efficient inference results in a short time. This is particularly important when there is logical uncertainty in addition to imprecision in the data. The fuzzy input includes the Potential importance, the energy level of the node, and the event occurrence frequency (EOF). The frequency of local events considers both normal events and attacks. Next, we discuss the characteristics of the following input values and the reasons for selecting them as fuzzy inputs.

- Potential Importance
- Energy Level
- Event Occurrence Frequency (Eof)

Potential Importance is one of the fuzzy function inputs that is a measure of whether a given CH plays an important role in the network. This approach considers the probability that a CH node will be selected as a validation node from a downstream node and the tail number of that CHs. A node with a high probability of becoming a verification node is expected to have high energy consumption and its value of potential importance is increased. In general, the closer the position of the CH to the BS, the less likely it is to become a validation node. Thus, the probability distribution has a linear shape. However, this is not accurate because it does not reflect the probability of the node becoming a verification node for each protocol. Therefore, in the proposed scheme, the filtering effectiveness evaluation function for the probability that the CH of each protocol becomes a verification node is applied. The potential importance of a node is derived from the importance function. The important function of the *i*-th node $E_{tag}{}^{i}$ is the amount of energy consumed from the event generation to the process of arriving at the BS as Equations (1), (2), and (3). α is energy consumption about the number of reports to be generated on average at CH node, and is given as follows:

$$\alpha = e_t * \frac{N_{evt}}{N_n}, \quad (1)$$

where e_t is the transmitting cost, N_n is the number of CHs in the field, and N_{evt} is the number of events which is a value measured at regular intervals. β is the expected cost of sending and receiving the report and is given as follows:

$$\beta = T * (e_t + e_r) * \left(\frac{N_{evt}}{N_n}\right), \quad (2)$$

where e_r denotes the receiving cost and T is the *i*-th CH's tail node mentioned in Fig. 5. The γ has a slightly higher complexity than other equations. In the tail node, the probability that the *i*-th node is selected as a verification node may be calculated. Then, multiply the probability of having the same key when the verification node is present. The γ that is sum of probabilities is given as follows:

$$\gamma = e_{cal} * \sum_{j=1}^{n} P_i^j, \quad (3)$$

where $P_i{}^j$ is the probability that the *i*-th CH becomes a verification node of the *j*-th node, and e_{cal} denotes the calculated cost. The probability $P_i{}^j$ differs from protocol to protocol. The $P_i{}^j$ for each protocol filtering effectiveness for representative cluster-based protocols as the below Table 1.

Table 1. Filtering effectiveness of cluster-based protocols

Protocol	Filtering Effectiveness Evaluation Function
CCEF[35]	$\mathrm{p} = \frac{1}{\alpha \mathrm{h}}$
DEF[8]	$p = 1 - \frac{\binom{v-l}{l}}{\binom{v}{l}} + \frac{1}{w} - \left(1 - \frac{\binom{v-l}{l}}{\binom{v}{l}}\right)\frac{1}{w} \cong 1 - \frac{\binom{v-l}{l}}{\binom{v}{l}}$
PVFS[6]	$P_i^j = \frac{HopCountToEVT_{N_j}}{HopCountToBS_{N_i}} * \frac{S}{L}$
IHA[4]	$P_i^j = \frac{vf}{HopCountToEVT_{N_i}}$
CFFS[36]	$p = 1 - (1 - \frac{t - N_d}{L_0})^{D_{CH\,0}^{CH\,i}}$

Therefore, the importance function for measuring importance is as follows:

$$E_{tag}^{i} = \alpha + \beta + \gamma. \tag{4}$$

Equation (4) represents the geographical importance of the *i*-th node and is considered a fuzzy input. In particular, it represents the expectation of energy consumption according to the position where the node is placed, with a value that differs according to each protocol. This value also varies for the scope of the fuzzy membership function. The residual energy of the node is an important core as fuzzy inputs. If nodes with sufficient energy are tagged on the IDs list, there is an adverse effect of increasing communication costs when resetting routing paths. Furthermore, the probability of encountering a hijacked node during the hop movement increases. In contrast, if a node with little energy is tagged in the list, there is a risk of energy depletion to perform the event detection function. If a node is depleted, the additional overhead will be required to find that node. In other words, the network lifetime and report passing rate are also lowered because the node is deactivated while generating a report or waiting for a report.

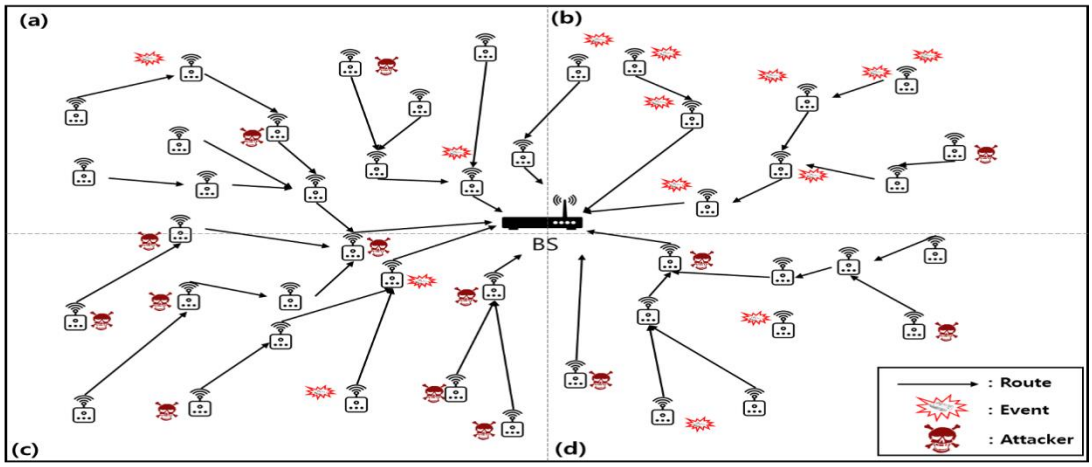

Figure 9. The frequency of event occurrence

The occurrence frequency of events represents the ratio of events occurring in the area where the corresponding node is located among all the fields. If the event frequency is high, the probability of event detection and report generation increases, and the probability of being tagged increases accordingly. On the other hand, The higher the frequency of event detection in an area, the higher the probability of generating reports and the higher the probability of being tagged. If the frequency of event detection is low, it is preferable to delay the tagging time. This is because it is advantageous for nodes to act as verification and transmission nodes for a long time to increase the overall network working time. The BS can determine the number of events and frequency of occurrences in each region based on the number of reports reaching the BS and the IDs of the nodes included in the report. If at least one false MAC is found in a report arriving at the BS, the report is considered to be a false MAC injected attack and counts the false reports dropped in the intermediate verification node. A report containing only the normal MAC is considered a normal report. Based on this information, the BS calculates the event rate and the attack rate. Providing information on the event occurrence rate in real time to the BS increases the network energy consumption. Thus, the BS provides each CH with a certain periodicity for polling to dynamically and efficiently allocate energy. The amount of data transmitted to each node in the BS does not exceed 1 byte. Additionally, since the size of the data to be transmitted is smaller than the size of the event report, the network is not significantly burdened. In real-world WSN applications, events and attacks are very unlikely to occur uniformly and regularly in different locations. In particular, it is difficult for an attacker to attempt simultaneously in all areas of the WSN field, and there is a high probability that an attack will occur through a few compromised nodes. Therefore, load balancing is needed in consideration of the probability of regional attack occurrence. This is also why the frequency of occurrence of fuzzy input values in the proposed method is important. Fig. 9 shows the frequency of event occurrence in the field. The proposed scheme extends the lifetime of the network through the load balancing of nodes considering these characteristics and improves the report transmission success rate and the event detection rate.

3.4. Fuzzy Rules and Membership Functions

This section describes the fuzzy membership functions and rules for the input values used in the proposed system.

Table 2. Fuzzy IF-THEN rules

No.	INPUT			OUTPUT
	Importance	Energy	Event Occurrence	ON/OFF
1	LOW	VERY_LOW	LOW	ON
5	HIGH	VERY_LOW	LOW	ON
14	MID	LOW	HIGH	OFF
18	LOW	MID	LOW	ON
31	MID	HIGH	LOW	OFF
…	….	….	….	….

The proposed system uses three membership functions: importance, energy, and event occurrence. The fuzzy inference engine also has two outputs: tags on and tags off (holding tagging). Based on the number of membership functions, there are 36 total rules; some of the rules are shown in Table 2. The optimization of the membership functions based on the rules was implemented using a genetic algorithm (GA) [22-24]. Optimization algorithms using GAs have been studied extensively [25-27]. A GA is a global optimization technique developed by John Holland in 1975 as a computational model based on the evolutionary process of the natural

world. Models involve a representative technique of evolutionary computation that mimics the evolution of living things. Such techniques represent a normal course of evolution, including mutations and mating operations [28].

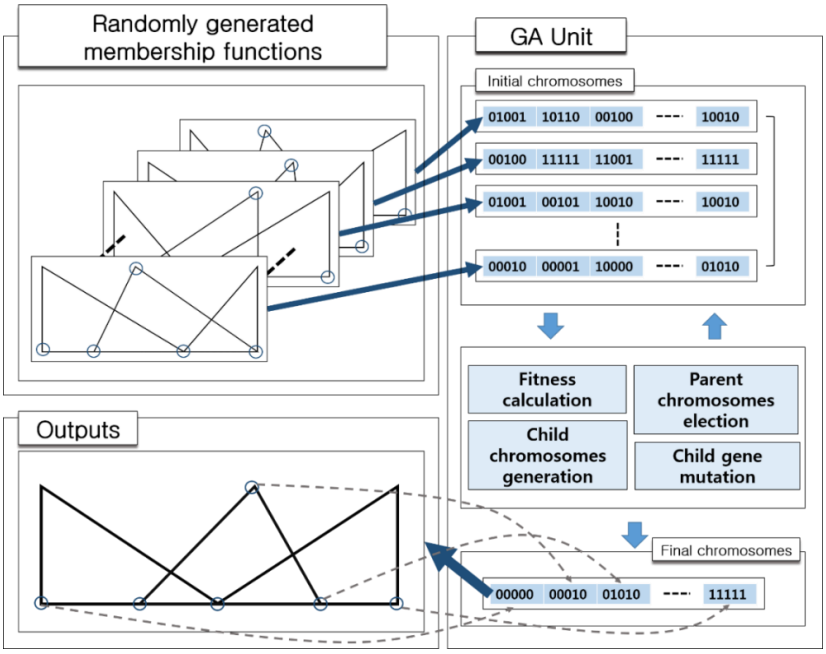

Figure 10. Membership optimization using a GA

In the proposed scheme, 20 membership functions were randomly generated, and each point value was converted into genetic information for the chromosome used in the GA unit. In the GA unit, the fitness of each chromosome is evaluated based on the error rate between the output values of the chromosomes and the output values set based on the rules of the fuzzy system. In the GA unit, the chromosomes are ranked in order of best fit, and the parent chromosomes are randomly selected based on the ranking. In the proposed method, the diversity of the chromosomes was increased by applying a mutation technique, with a mutation rate of 0.3% [29-30]. Only results with a zero-error rate were used, and the desired result can be obtained in less than one minute within approximately 50 generations on a desktop computer base station with a single modern CPU. The optimization of membership functions using a GA ensures high accuracy and allows developers to optimize the problem much faster than they could manually. Fuzzy membership function optimization using a GA also benefits from fast updates in dynamic situations in which the size of a field or the number of nodes changes. This is because the GA takes much less time to execute than a manual optimization technique. The membership function for the input values finally obtained in the proposed scheme is given in Fig. 11.

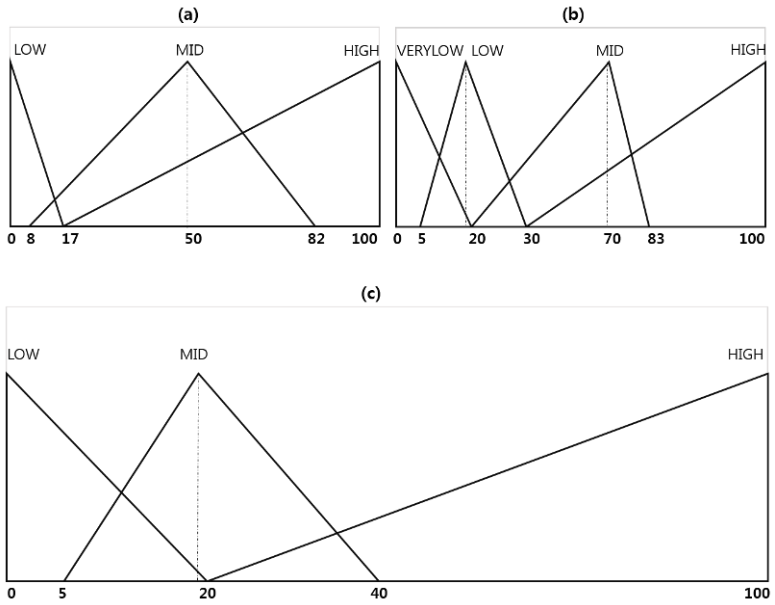

Figure 11. Fuzzy membership functions

4. EXPERIMENTAL RESULTS AND ANALYSIS

4.1. Experimental Environment

Table 3. Experiment Parameters

Item	Value
Sensor field size (m^2)	1,000 × 1,000
Number of sensor nodes	2,000
Number of cluster head nodes	200
S (Number of MAC)	5
L (Cluster size)	10
Report size (byte)	24
Transmission range (m)	150

The performance simulation of the proposed scheme is based on the specifications of the MICAz mote model used in most WSNs [31]. Experiments were conducted assuming that the attack rates ranged from 0 to 90 In our experiment, 100% FTR is not shown in the experimental results to evaluate the failure rate of the normal report. The communication cost consumes 16.25 μJ /byte for a transmission, 12.5 μJ /byte for a reception, and 15 μJ /byte for the calculated cost of voting [7]. For routing, the shortest path routing scheme is used [32]. The experimental environment implemented true threshold (Tt) and false threshold (Tf) parameters to derive reliable results to struct the same environment as the existing security protocol method PVFS [6]. The computation time of the fuzzy logic with 36 rules is about 3 μs and each node consumes approximately 90 μJ of energy per cycle [33-34]. We do not consider the cost of transmitting information about an attack dropped on each CH provided at regular intervals because it is negligible.

4.2. Assumptions

The field was divided into four parts, as shown in Fig. 9, and the experiment was conducted by varying the event occurrence rate in each region with an attack ratio of 100% to increase the

reliability of the experiment. The bias values of -1, 2, 3, and 4 represent cases where the occurrence ratios of events occurring in four regions are 1: 1: 1: 1, 2.5: 2.5: 5: 1, 1: 2: 3: 4 and 1: 1: 0: 0, respectively. The nodes are arranged randomly. The CH's location is not changed during the experiment. The nodes used in our experiment set limited energy as initial energy by implementing the original node without considering energy recharge techniques. If energy is assumed to be infinite, it is difficult to calculate the event detection failure and report transmission failure accurately. The routing list size used in the proposed scheme is 50, which is large enough to accommodate a typical WSN in the field. The BS has all keys of all nodes as the global key pool and has the computing power to verify reports. Additionally, the events and attacks occurred randomly, as shown in Fig. 4, so we experimented with different local incidence rates.

4.3. Experimental Results

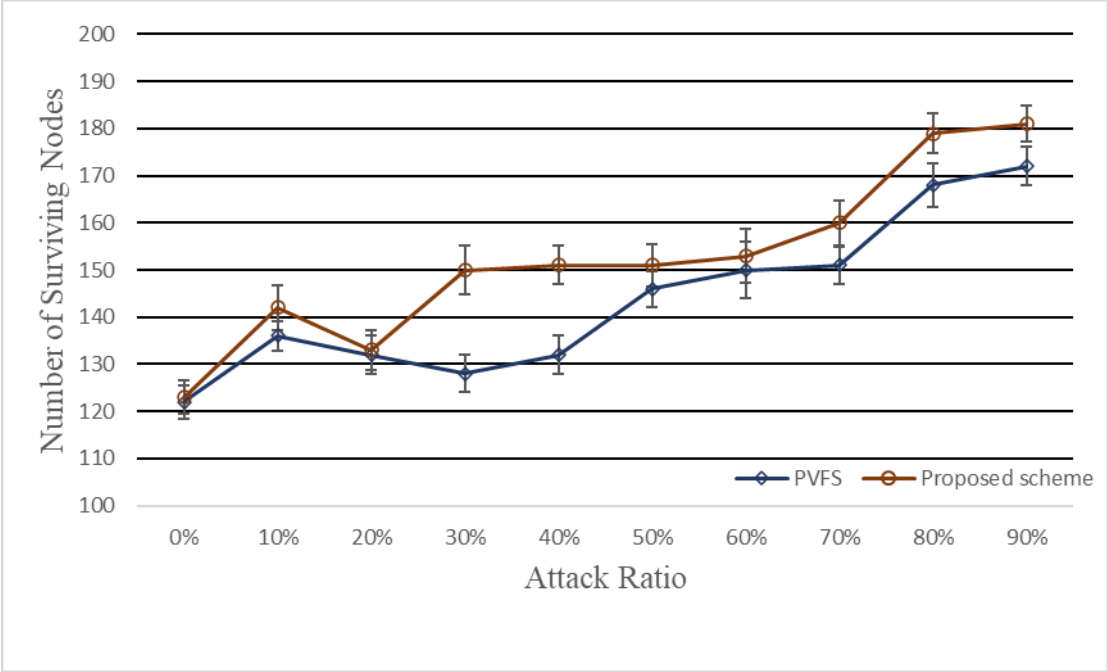

Figure 12. Number of surviving nodes

Fig. 12 shows the number of surviving nodes in field situations with various attack rates. In a WSN with the reflected security protocols, most false reports are detected and dropped in a few hops. Therefore, as the attack rate increases, the energy consumed by the entire network decreases. The graph also shows that under the proposed scheme, the number of surviving nodes increases. In a protocol such as the PVFS where CH re-selection does not occur, it is impossible to detect events in the energy-depleted regions of the CH. The proposed technique can alleviate the problem of such shadow areas. Overall, we confirmed an improvement of the node survival rate, and the shadow area problem was improved by about 9.55%.

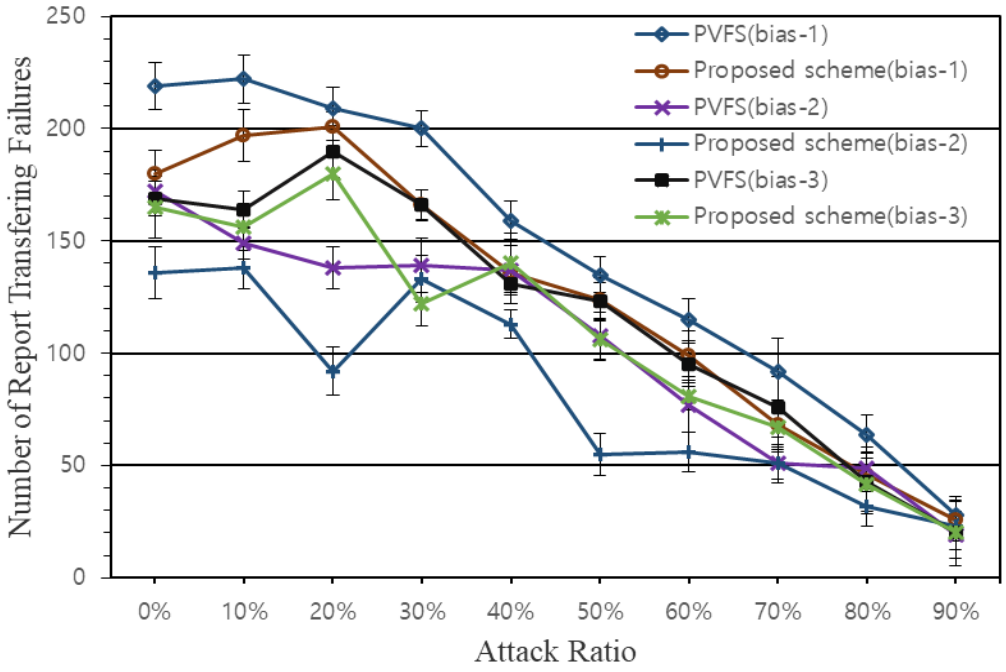

Figure 13. Number of transfer failures

Fig. 13 shows the number of report failures in field situations with various attack rates. As can be seen in Fig. 13, as the attack rate increases, the number of report transferring failures decreases in all schemes. This is because when the attack ratio increases, the number of normal event reports decreases. As the attack rate increases, the difference between the number of report transmission failures of the proposed scheme and PVFS is also reduced. Experiments confirmed that the security protocol using the proposed load-balancing method shows a better report delivery success rate than the existing protocol in fields under almost all attack rates. This experiment shows the main goal of the proposed method and shows that the load balancing of the proposed method is well done considering the field conditions, including the attack ratio, location of nodes, and each node's energy, which network users are not likely to be aware of.

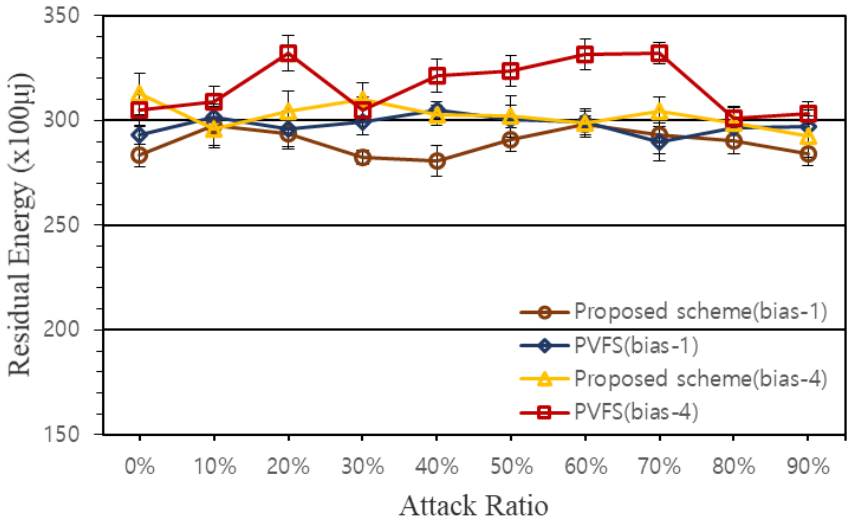

Figure 14. Residual energy of nodes

Fig. 14 shows a comparison of the residual energy averages of the surviving nodes in the proposed scheme and the PVFS in the region where there is no difference in the occurrence frequency of the events (bias-1) and the region with the greatest gap (bias-4). Regardless of the frequency of occurrence, we can see that the residual energy of the node in the field applying the proposed scheme is lower than that in the field using the original PVFS. There are two reasons for this. One is that the absolute energy usage in the proposed scheme is larger than that of PVFS. The other is that the proposed scheme saves nodes and performs energy management until the node reaches the end of its life. This means that our proposed scheme consumes more energy, so it is not suitable in a clean area where the attack rate is 0%. As shown in Fig. 12 and Fig. 13, the node survival rate and the report transmission success rate of the proposed scheme are higher than those of the original PVFS. Therefore, it is incorrect to assume the energy consumption in the proposed method is larger than that of the original PVFS.

This can be interpreted as a result of extending the lifetime of the node via the load distribution of the node through the proposed scheme. In the proposed scheme, it is desirable to consider that the average residual energy of surviving nodes is relatively low because it estimates and tags the expected lifetime of the node considering the energy of the nodes and various environmental variables. While it may be desirable to have low energy consumption, energy efficiency improvements with low report delivery rates are not meaningful for network efficiency. Nodes placed in a field will eventually run out of energy, and if a large number of nodes die so that event detection is no longer possible, the network user will have to unconditionally relocate nodes in the field. In a situation where a node is relocated, the remaining energy of the node is high and it is no longer necessary to consider low energy situations. Therefore, it is important to increase network availability by extending the maximum lifetime.

Residual energy differences between the two schemes in areas with a high frequency of events are greater than in areas with a low frequency. Therefore, it can be concluded that the proposed technique is more effective when the bias is large. In the case of the original PVFS, the routing is not flexible and routing using the relatively low energy consumption region is not executed. On the other hand, this result is obtained because the proposed scheme can consider the entire network situation.

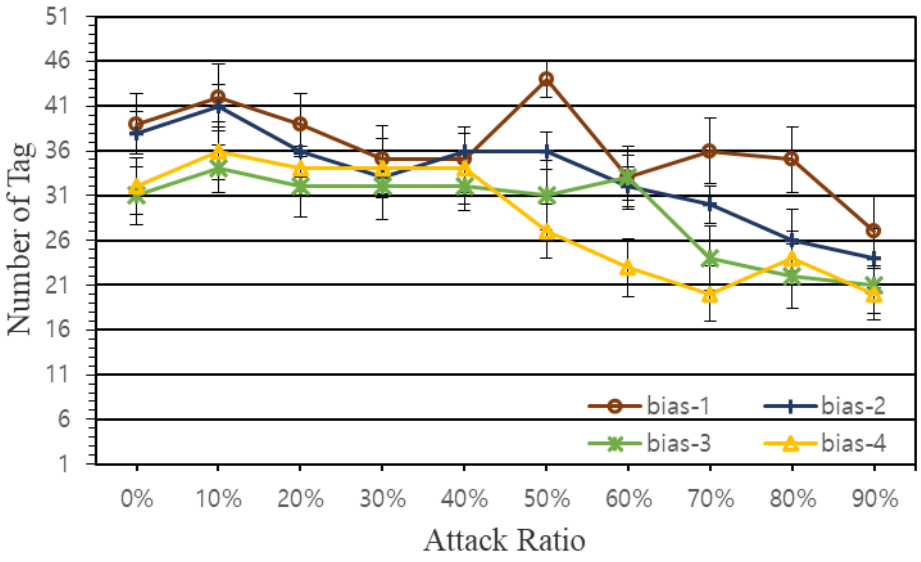

Figure 15. Number of tagged nodes

Fig. 15 shows the number of tagged nodes according to the attack rate when the total number of events is 1,000. In real situations, events may not occur evenly throughout the field, so the experiment using the proposed scheme considers a situation with a locally-biased event occurrence. The reason that the gap in the number of node tags according to these four deflected situations is not huge is because the proposed method considers the frequency of events as a fuzzy input and the node itself manages the routing list, as shown in Fig. 7. As the attack rate increases, the overall number of tagged nodes decreases. In a network environment where a security protocol is applied, when a false report attack occurs, most false reports are filtered within several hop movements. Therefore, when the total number of events is constant, the energy consumption of the whole network field decreases as the attack rate increases. Fig. 15 shows that the larger the regional deviation, the fewer the number of nodes that are tagged. Thus, the larger the attack rate, the larger the difference in the number of tagged nodes. Hence, the larger the regional variance, the more likely it is that there will be reduced energy consumption compared to earlier models. It is possible to improve the efficiency in the whole network by forming the routing through the nodes located in these high-attack locations. The reason why the peak point is shown when it is 50% of bias-1 in Fig. 15 is that bias-1 represents an ambiguous probability to separate an attack. Even when suspected as an attack, a node tag is selected to increase a node lifetime in the proposed scheme. We implemented this using fuzzy logic by considering the regional importance in the proposed method. We see that the proposed scheme has more effective load balancing in situations with a relatively low attack rate.

5. CONCLUSIONS

In this paper, we experimentally proved that the lifetime of the network increases by changing the role through TAG management based on fuzzy logic-based decision-making in CH nodes that generate and verify reports. Users want successful reporting of normal events from the WSN. Therefore, the experimental analysis of the proposed technique excluded the consideration of the unimportant successful transmission of false reports. WSN users periodically replace the node batteries throughout the entire field or pick up the nodes placed in the field when the local network is not needed. Therefore, the total sum of the residual energy for all nodes in the field does not influence the performance of the network when replacing the nodes. Even though the total amount of energy used increases, it is desirable to transmit the information to be provided by extending the life of the nodes. The proposed scheme is a method of simultaneously increasing the report success rate and the number of surviving nodes. For further study, we plan to study energy consumption and load distribution efficiency according to the GA optimization execution cycle of the proposed system.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGEMENTS

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2021R1A2C2005480)

REFERENCES

[1] J.S. Ahn and T.H. Cho "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).

[2] Pantazis, Nikolaos A., Stefanos A. Nikolidakis, and Dimitrios D. Vergados. "Energy-efficient routing protocols in wireless sensor networks: A survey." IEEE Communications surveys & tutorials 15.2 (2012): 551-591.

[3] Nam, Su Man, and Tae Ho Cho. "Discrete event simulation–based energy efficient path determination scheme for probabilistic voting–based filtering scheme in sensor networks." International Journal of Distributed Sensor Networks 16.8 (2020): 1550147720949134.

[4] Zhu, Sencun, et al. "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks." Security and privacy, 2004. Proceedings. 2004 IEEE symposium on. IEEE, 2004.

[5] Yang, Hao, and Songwu Lu. "Commutative cipher based en-route filtering in wireless sensor networks." Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. Vol. 2. IEEE, 2004.

[6] 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.

[7] 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

[8] Yu, Zhen, and Yong Guan. "A dynamic en-route filtering scheme for data reporting in wireless sensor networks." IEEE/ACM Transactions on Networking (ToN) 18.1 (2010)

[9] Nam, Su Man, et al. "A Method of Improving Energy Efficiency Through Geofencing and False Data Blocking In Context-Aware Architecture for Probabilistic Voting-Based Filtering Scheme of WSNs International Journal of Computer Networks & Communications (IJCNC) Vol 13 (2021)

[10] Malik, Meena, Dr Yudhvir Singh, and Anshu Arora. "Analysis of LEACH protocol in wireless sensor networks." International Journal of Advanced Research in Computer Science and Software Engineering 3.2 (2013).

[11] Handy, M. J., Marc Haase, and Dirk Timmermann. "Low energy adaptive clustering hierarchy with deterministic cluster-head selection." Mobile and Wireless Communications Network, 2002. 4th International Workshop on. IEEE, 2002.

[12] Zadeh, Lotfi A. "Outline of a new approach to the analysis of complex systems and decision processes." IEEE Transactions on systems, Man, and Cybernetics 1 (1973): 28-44.

[13] J. Yen and R. Langari, Fuzzy Logic: Intelligence, Control, and Information. Prentice-Hall, Inc., 1998.

[14] Zadeh, Lotfi A. "Fuzzy sets." Information and control 8.3 (1965): 338-353.

[15] G. Klir and B. Yuan, Fuzzy Sets and Fuzzy Logic. Prentice hall New Jersey, 1995.

[16] Castillo, Oscar, et al. "Type-2 fuzzy logic: theory and applications." 2007 IEEE international conference on granular computing (GRC 2007). IEEE, 2007.

[17] Ashraf, Muhammad, and Tae Ho Cho. "Energy Efficiency Enhancement of TICK-based Fuzzy Logic for Selecting Forwarding Nodes in WSNs." KSII Transactions on Internet and Information Systems (TIIS) 12.9 (2018): 4271-4294.

[18] Patcharaprakiti, Nopporn, Suttichai Premrudeepreechacharn, and Yosanai Sriuthaisiriwong. "Maximum power point tracking using adaptive fuzzy logic control for grid-connected photovoltaic system." Renewable Energy 30.11 (2005): 1771-1788.

[19] Larsen, P. Martin. "Industrial applications of fuzzy logic control." International Journal of Man-Machine Studies 12.1 (1980): 3-10.

[20] Simoes, M. Godoy, Bimal K. Bose, and Ronald J. Spiegel. "Fuzzy logic based intelligent control of a variable speed cage machine wind generation system." IEEE transactions on power electronics 12.1 (1997): 87-95.

[21] Alajmi, Bader N., et al. "Fuzzy-logic-control approach of a modified hill-climbing method for maximum power point in microgrid standalone photovoltaic system." IEEE Transactions on Power Electronics 26.4 (2011): 1022-1030.

[22] Gen, Mitsuo, and Runwei Cheng. Genetic algorithms and engineering optimization. Vol. 7. John Wiley & Sons, 1999.

[23] C. L. Karr, "Design of an adaptive fuzzy logic controller using a genetic algorithm." in Icga, 1991, pp. 450-457.
[24] A. Geyer-Schulz, Fuzzy Rule-Based Expert Systems and Genetic Machine Learning. Physica Verlag, 1997.
[25] Jung Sub Ahn & Tae Ho Cho. "Fuzzy Logic Optimization Method for Energy Efficiency Improvement of CFFS using GA in WSN" International Journal of Engineering and Advanced Technology (IJEAT), Vol. 9, No. 6, pp. 474 - 480, Aug. 2020.
[26] Lee, Hae Young, and Tae Ho Cho. "Fuzzy adaptive selection of filtering schemes for energy saving in sensor networks." IEICE Transactions on Communications 90.12 (2007): 3346-3353.
[27] Lim, Sang-Hyeok, and Tae-Ho Cho. "WSN Lifetime Extension using GA Optimized Fuzzy Logic." International Journal of Computer Science & Information Technology 9.5 (2017):1-14
[28] Deb, Kalyanmoy, et al. "A fast and elitist multiobjective genetic algorithm: NSGA-II." IEEE transactions on evolutionary computation 6.2 (2002): 182-197.
[29] Fogarty, Terence C. "Varying the probability of mutation in the genetic algorithm." Proceedings of the 3rd international conference on genetic algorithms. Morgan Kaufmann Publishers Inc., 1989.
[30] Srinivas, Mandavilli, and Lalit M. Patnaik. "Adaptive probabilities of crossover and mutation in genetic algorithms." IEEE Transactions on Systems, Man, and Cybernetics 24.4 (1994): 656-667.
[31] https://www.scribd.com/document/91069327/Micaz-Datasheet-t
[32] Akkaya, Kemal, and Mohamed Younis. "A survey on routing protocols for wireless sensor networks." Ad hoc networks 3.3 (2005): 325-349.
[33] Karlof, Chris, Naveen Sastry, and David Wagner. "TinySec: a link layer security architecture for wireless sensor networks." Proceedings of the 2nd international conference on Embedded networked sensor systems. ACM, 2004.
[34] 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.
[35] Yang, Hao, and Songwu Lu. "Commutative cipher based en-route filtering in wireless sensor networks." Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. Vol. 2. IEEE, 2004.
[36] Liu, Zhixiong, et al. "A Cluster-Based False Data Filtering Scheme in Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 23 (2014).
[37] Hai, Tran Hoang, and Eui nam Huh. "Network Anomaly Detection Based On Late Fusion Of Several Machine Learning Algorithms." International Journal of Computer Networks and Communications (IJCNC) 12.6 (2020): 117-131.
[38] Farahani, Gholamreza. "Energy Consumption Reduction in Wireless Sensor Network Based on Clustering." International Journal of Computer Networks & Communications (IJCNC) Vol 11 (2019).

AUTHORS

Jung Sub Ahn received the B.S. degree in computer engineering from Kyunil University in 2016 and now doing Ph.D. degree in Department of Electrical and Computer Engineering from Sungkyunkwan University, Republic of Korea. His research interests include wireless sensor network security, modelling & simulation, IoT security

Sang Hyeok Lim received his B.S. degree in digital information engineering from Hankuk University of Foreign Studies, in February 2017 and M.S degree in Electrical and Computer Engineering from Sungkyunkwan University in 2019, respectively. He is currently working as a machine learning engineer at amorepacific. His research interests include wireless sensor network, deep learning, and modelling & simulation.

Tea Ho Cho received a Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical and Computer Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Software at Sungkyunkwan University, Korea.