International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-6, August 2020

Fuzzy Logic Optimization Method for Energy Efficiency Improvement of CFFS using GA in WSN

Jung-sub Ahn, Tae-ho Cho

Abstract: ***Recently, the range of applications for wireless sensor networks has grown. In industrial applications using data-driven approaches, data reliability is particularly important. However, deployed sensor nodes can be easily damaged due to physical damage or node acquisition factors caused by attackers, and false report injection attacks may occur. CFFS with collaborative verification has been proposed to filter out false reports. The proposed CFFS reduces the probability of a successful attack by separating sensor nodes into clusters. The false report filtering performance in the existing scheme is determined according to the pre-security strength setting. Unfortunately, with CFFS, it is impossible to secure each cluster because multiple attacks in a region are not considered. DCFFS uses fuzzy logic to enable security management for each cluster in consideration of the network environment and the geographical arrangement of the nodes. It is necessary for a network administrator to adjust the scope of the membership function parameter to fit the network environment to ensure that the output has an appropriate security strength value for the environment; however, this is difficult to know because it has dissimilar optimum ranges for each application. This paper introduces a fuzzy optimization method that can be adapted to various environments using a genetic algorithm in CFFS. The energy efficiency of nodes is increased by correcting the scope of the membership function in the proposed method. We used experiments to verify that the energy efficiency of the proposed scheme is increased, as compared to the existing scheme.***

Keywords: Genetic Algorithm, Fuzzy Optimization, Network Lifetime Extension, Fuzzy Logic, WSN Security Protocol.

I. INTRODUCTION

Recently, wireless sensor networks, which are a core technology of the fourth industrial revolution, have undergone rapid development. Wireless sensor networks refer to groups of sensor nodes with complex system applications; these can be used in various fields, including military, healthcare, and agriculture [1-3]. The data reliability of report content for military and healthcare applications provided by wireless sensor networks is particularly important. In addition, since data-based control applications, such as smart factories, are controlled based on the collected data, reliability verification of the collected data is necessary [4]. Sensor nodes of wireless sensor networks can be easily damaged because they are deployed in an open environment. Therefore, an adversary can collect and destroy nodes to generate false events or inject false reports into the network [5]. If a created false event is delivered to a base station (BS), various threats can occur, such as causing unnecessary energy consumption of nodes located in the middle and causing false alarms. In the case of pipeline monitoring of the SCADA system or the utilization of a production line control or management system where data information is sensitive, if the wrong data is inserted and the actuator operates abnormally, a serious accident can occur [6]. A cluster-based false data filtering scheme (CFFS) [7] that efficiently manages energy by classifying nodes into clusters to prevent false report insertion attacks was proposed by Z. Liu et al. CFFS improves the filtering probability of false reports by solving the local problem of node verification. CFFS has a security strength value, which is the maximum compromised node count allowance threshold for nodes; if an attacker has a compromised node that exceeds this value, CFFS can't detect false reports. In CFFS, a higher threshold value increases the filtering probability, but the report size also increases. Alternatively, a lower threshold value decreases the filtering probability and the report size decreases. All clusters have the same security strength, which is not efficient when CFFS is applied to real-world applications because it is very difficult to attack a wide range of sensor nodes. Therefore, the fuzzy-based cluster false data filtering scheme (FBCFFS) [8] was proposed to determine the appropriate security strength value for each cluster by considering the partial attack area in CFFS. The security strength value of FBCFFS is determined based on fuzzy logic. However, this method has the disadvantage of having a static membership function, which prevents proper control in the attack environment. In other words, if the situation changes frequently, the scope of the fuzzy rules should also be changed accordingly. We propose a method to efficiently rebuild the fuzzy rule using a genetic algorithm (GA) [9], which is an optimization algorithm. In the proposed method, a fuzzy rule base is used as one chromosome.

Revised Manuscript Received on August 15, 2020.
* Correspondence Author
Jung-sub Ahn, Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea. E-mail: sc4217@skku.edu
Tae-ho Cho*, Department of Computer Science and Engineering, Sungkyunkwan, University, Suwon, Republic of Korea. E-mail: thcho@skku.edu

GA allows good chromosomes to be passed on to the next generation, so the fuzzy rules are adjusted to suit the changing situation. In this paper, the energy efficiency of the newly proposed method is verified through experiments using realistic numerical models of wireless sensor networks.

The composition of this paper is as follows.

Chapter 2 describes the related research, genetic algorithm, and CFFS. Chapter 3 describes the proposed scheme. In Chapter 4, the performance of the proposed scheme is evaluated through experiments. Finally, our conclusions are provided in Chapter 5.

II. BACKGROUNDS

A. Genetic Algorithm (GA)

John Holland proposed the genetic algorithm (GA) in 1975. It is an optimization algorithm based on the principle of natural selection. GA is still used today to search for good solutions in a short amount of time. GA is advantageous because it can approach problems that are not clearly defined mathematically and it does not require a large amount of training data, unlike neural networks (NNs). The GA process consists of seven phases [10-11]: 1) Initialization, 2) Evaluation, 3) Selection, 4) Crossover, 5) Mutation, 6) Replace, and 7) Loop, as shown in Fig. 1.

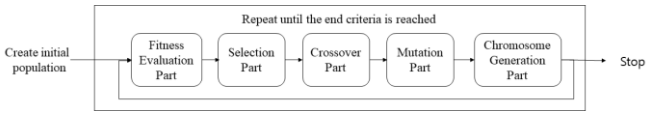

Fig. 1 Genetic Algorithm Process

First, the system creates various initial populations with random values in the initializing phase. The resulting chromosomes become the first parent generation. Effective chromosomes are selected and evolved to form the next generation in the selection phase. The selection phase selects good chromosomes that align with the goal. Selection methods include the proportionality strategy (similar to a roulette wheel), in which the probability of selection varies according to the fitness of a chromosome. Also, the ranking selection method which is one of the selection methods is selected in proportion to the radio of fitness. And the elite selection strategy method selects a chromosome with high fitness value. In the selection step, a chromosome is selected according to the fitness value. The chromosome crossing phase changes the position of the gene by specifying a cross position to generate the new chromosome. There is a simple cross method that specifies a single point; a multiple cross method, in which a plurality of cross positions exist; and a mask cross method, in which crossing is performed through a mask gene. The mutation phase generates mutant chromosomes that have all of their genes inverted. There are two types of variations: static variation with fixed probability and dynamic variation with dynamic probability.

An advantage of GA is that it is easy to find a good solution in a short time because this method searches for an efficient solution among multiple chromosomes. The back-propagation algorithm and neural networks that use as an optimization method require a complex differential operation because the differential value of the evaluation function is required, but GA has a simple algorithm. To improve the system performance, the GA part of the proposed scheme introduced in this paper is applied to the security system of a WSN, which requires fast processing to obtain an efficient value in a short time.

B. Fuzzy Logic

The fuzzy theory, which is based on fuzzy logic, was first introduced by Lofti A. Zadeh at the University of Berkeley. Fuzzy logic can recognize the degree of belonging to various situations to see which group it belongs to, unlike a system based on Boolean logic [12]. Therefore, fuzzy logic is a very effective theory for describing unclear or ambiguous propositions or sets in the real world. New facts are obtained by using given rules and inputting facts into the rules-based expert system based on fuzzy theory, as shown in Fig. 2.

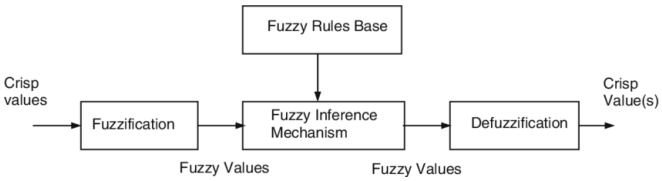

Fig. 2 Fuzzy Logic Process

Fuzzy logic consists of a fuzzification interface, fuzzy inference, and a defuzzification interface. The fuzzification interface uses a transformed fuzzy value from the actual value to calculate the overall fit for each rule. Fuzzy inference refers to the process of obtaining a result from something input into a nonlinear system. The fuzzy inference system requires a fuzzy rule base that has expressed if-then format rules. The fuzzy reasoning method includes various reasoning methods, such as a direct reasoning method (Mamdani reasoning method), an indirect reasoning method (Tzukamoto reasoning method), and a mixed reasoning method (Sugeno reasoning method). The defuzzification interface process de-fuzzes the value calculated as a result of the fuzzy inference mechanism [13]. The final phase outputs crisp values from the obtained fuzzy values through a fuzzy inference engine in the defuzzification phase. We apply the Mamdani reasoning method to our proposed method after considering the application limitations because this reasoning method has a faster computation rate than other inference reasoning methods. Additionally, defuzzification computes real values using the center of gravity (CoG) method.

Fuzzy logic is applied to various industrial applications, including time-series input/output data and sewage treatment data of gas furnaces, as well as to intelligent-control-related applications, such as elevator control.

C. Cluster based False Data Filtering Scheme

CFFS groups nodes into clusters and organizes them as tree structures. A cluster consists of a number of member nodes, which has the advantage of balancing the key overhead of tree nodes through a distributed key allocation method. Nodes of a cluster elect the cluster head nodes. If the sensor nodes detect an event, nodes transmit event reports to the base stations through the cluster head nodes.

In addition, the MAC (message authentication code) in the report is verified through the en-route verification process to filter false reports. In this way, it is possible to detect an erroneous data report created through compromised nodes existing in different geographical locations. Its mechanism also provides a cooperative and balanced key exchange between nodes. This allows the cluster head node to detect and filter false reports injected within a few hops by holding various keys. Fig. 3 shows the intermediate filtering procedure of the CFFS protocol.

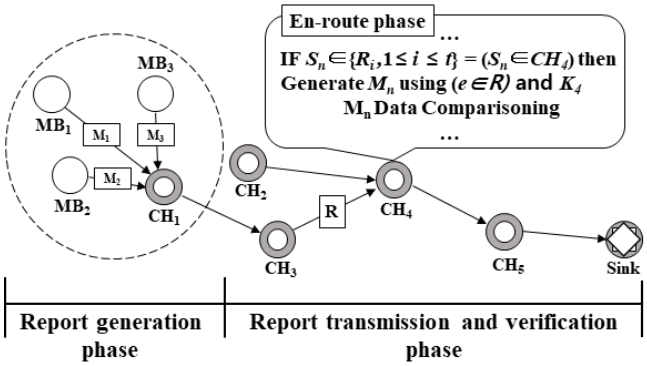

Fig. 3 En-route Procedure of CFFS

The traditional CFFS consists of the following phases.

1) Pre-deployment and bootstrapping phase

Each node randomly distributes and stores a key by using a global key pool, which is divided into partitions by the BS. Nodes that have distributed keys are placed in the field in various ways. The deployed static nodes are self-organized, and this self-organization forms a cluster-type tree structure through the hello message that is broadcast from the BS. If tree-structured routing is conFig.d, the leaf node of the tree broadcasts its burden value to neighboring nodes. Each node has a first burden value of 1. If a node received a burden value, their own burden value is added and transferred to the BS. The burden value collected from the BS is used for a subsequent key distribution step. Depending on the burden value, the cluster head nodes select the number of keys to be sent to the upstream node. Nodes that receive this value store the keys probabilistically.

2) En-route filtering phase

When a node detects an event, the detecting node communicates with other nodes in the same cluster to create a MAC. Communicating nodes encrypt the contents of the detected event by using the granted individual key in step 1 for MAC generation. The generated MAC is transmitted to the CH node, and the CH creates a report that is transmitted to the BS using the received MAC. The created report is transmitted to the CH node according to a set routing path, and if intermediate nodes have the same encryption key as the report, the report is verified. Otherwise, it is passed to an upstream node until it reaches the BS. During verification, if the content of the report is determined to be false, the report is filtered.

3) Base station verification phase

The intermediate filtering phase performs statistical filtering. Therefore, if the forwarding nodes on the routing path do not have the same stored key, it may not be possible to filter the report. However, since the BS has a global key pool, all keys can be stored. The report contains a collected MAC according to the predefined threshold. When the BS receives the report, it verifies all MACs using the event contents included in the report and the BS key values. By verifying the MACs at the BS, it is possible to determine whether the report is bogus. If the content is different, or if the event content does not exist, the detecting node drops the report. Therefore, even if the nodes are less damaged than the security threshold, CFFS conducts verification through the distributed key and determines whether the nodes are false.

III. PROPOSED SCHEME

A. Problem Statement

In the recently proposed enhanced CFFS, it is possible to dynamically control the security strength value using a fuzzy system [8]. The fuzzy rules used in the fuzzy system are made based on the knowledge of managers or experts. In addition, the fuzzy membership function used in the presupposition phase is also defined by the administrator. The FBCFFS output value, according to the crisp input value, is determined based on the stored rule and the membership function. FBCFFS has various membership functions. However, these membership functions have fixed parameter values, which are not suitable for environments where the environment changes. The creation of false reports is dependent on the region. Therefore, in the case of an area with a high attack rate (as shown in the Fig. below), there is a high probability that another attack will occur. If the security strength is set with the initial membership function, an improper security strength may be applied to the environment. As a countermeasure, a method of physically relocating nodes exists. However, it is hard to replace nodes deployed in difficult-to-access areas, such as those used in military applications. Furthermore, the energy management of nodes located upstream is more important because upstream nodes must be covered with a large number of nodes. When an upstream node's energy is exhausted, multiple local events in a lower node cannot be detected. Therefore, flexible security strength control is needed for each region.

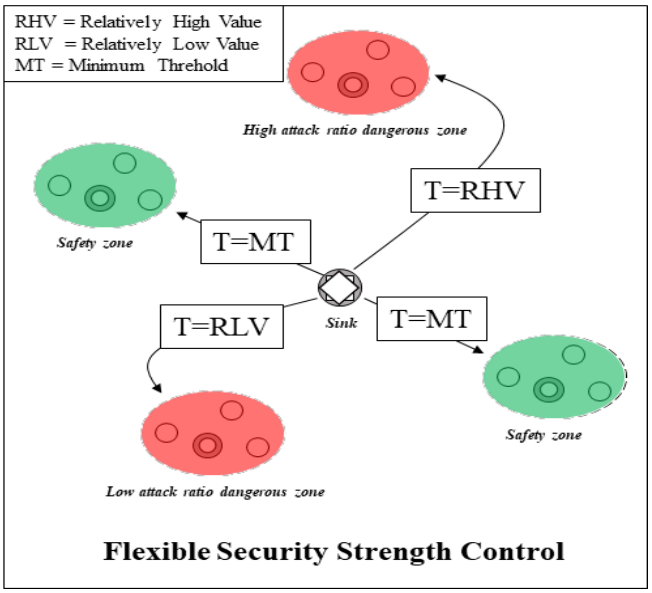

Fig. 4 Flexible Security Strength Control

B. Membership Function Fuzzy-Based CFFS Membership Parameter Optimization Scheme Using GA

Optimization problems in many areas use analytical and numerical optimization methods. However, traditional methods are limited because they require an auxiliary method, such as a differential calculation, and there are very few applicable systems [14]. If all areas are searched, the processing amount becomes very large, resulting in poor processing efficiency. We use the genetic algorithm search approach method to solve the problem of the two methods mentioned above. A GA search uses a random search method to overcome limitations.

Additionally, the proposed method uses a binary serial method to optimize the fuzzy model. Additionally, the selection operation uses the roulette wheel method and the crossover operation uses the one-point crossover operation. The mutation operation uses an invert method to reverse the selected bit.

This section introduces the optimization method of the fuzzy membership structure in greater detail, as well as parameters using genetic algorithms to design the optimal fuzzy model for the network situation. The proposed method is performed in the following steps.

- Initial chromosome set and population generation
- Calculation of chromosome fitness
- Generation of offspring from current chromosomes
- Calculation of the error rate according to the fitness function of the generated descendants
- Termination condition determination

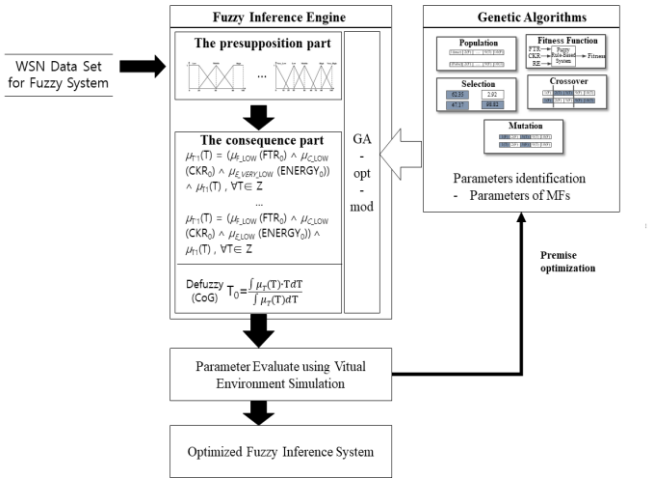

Fig. 5 Fuzzy Membership Function Optimization Core Idea for CFFS

Fig. 5 shows the process of optimizing the membership function of FBCFFS through GA. The secure method of passing data from the source node to the BS [8] offers security within the data transmission method in relationship to event reports. When the BS system receives the input of the WSN data set, it creates various mutant genes with the corresponding data. Fuzzy inference is performed by the membership function, as defined in advance by the fuzzy inference engine. The security strength value is derived through the rules and the defuzzification method by using the center of gravity method.

The expression for each rule is as follows.

$$\mu_{T'1}(T) = (\mu_{F\_LOW}(FTR_0) \wedge \mu_{C\_LOW}(CKR_0) \wedge \mu_{E\_VERY\_LOW}(ENERGY_0)) \wedge \mu_{T1}(T), \forall T \in Z$$

…

$$\mu_{T'1}(T) = (\mu_{F\_LOW}(FTR_0) \wedge \mu_{C\_LOW}(CKR_0) \wedge \mu_{E\_LOW}(ENERGY_0)) \wedge \mu_{T1}(T), \forall T \in Z$$

The set threshold depends on the saved rule base file.

$$T_0 = \int \mu_T(T) \cdot T dT \Big/ \int \mu_T(T) dT$$

The above equation represents the center of gravity method. The security threshold value determined in this way is applied to the virtual environment for simulation. Therefore, each virtual environment simulation establishes membership functions composed of different genes. Each simulation calculates the total energy consumption of the network according to a membership function. The fitness of a chromosome is determined by the energy consumption calculated in the simulation. The proposed scheme adjusts the main parameters of the first half of the fuzzy model, like the input variable, the number of membership functions, and the type of the polynomial function, in accordance with the GA process. The first-half membership parameter is optimally adjusted using GA. For example, the environment of the attack rate will be set to the high F_LOW value in the rule because the fitness of FTR is evaluated as a good match. If the algorithm satisfies the termination condition, the BS sets the optimally calculated security strength. Otherwise, it repeats the previous phase and adjusts the parameters of the membership functions. By repeating the above process, the proposed scheme outputs the appropriate security strength for the attack environment.

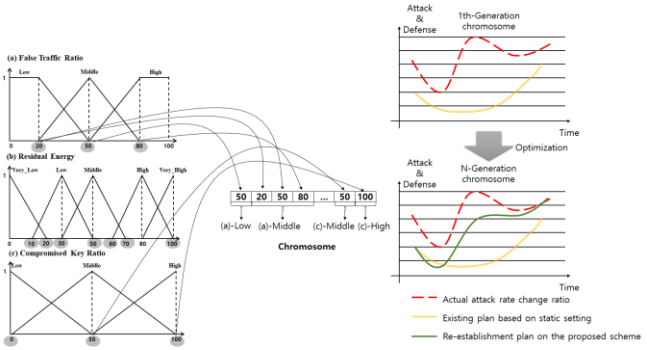

Fig. 6 Transformation process from the fuzzy rule to a chromosome

Fig. 6 represents the process of chromosome mutation of the parameters stored in the fuzzy rule base. One chromosome includes the parameter values of the membership function. On the right side of Fig. 6, the expected effect of GA is adapted to the environment. In the traditional method, it is designed to depend only on a static parameter and does not consider the rate of environmental change. However, the proposed scheme is designed to adapt to the environment; it is determined that there is a high probability that an attack will occur again in an attack-prone area, and the parameter value is tuned. As a result, this provides security by expanding or contracting the minimum security range suitable for the environment.

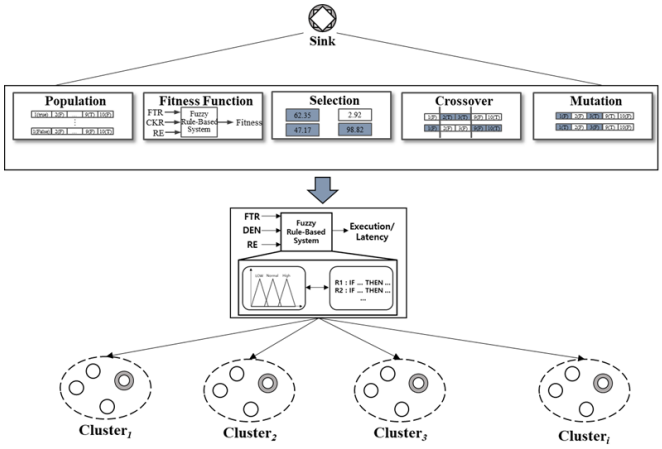

Fig. 7 Detailed GA Process in Proposed Scheme

Fig. 7 shows the GA post-process of the proposed scheme. The BS optimizes the fuzzy rule using a GA process consisting of five steps. Each cluster of the fuzzy system can use the optimal rule base file through the proposed scheme. In the proposed scheme, the old fuzzy membership functions are dynamically adjusted and optimized according to the cluster using GA. The proposed method consists of the initial population set generation phase, fitness function evaluation phase, roulette wheel selection phase, one-point crossover phase, and reverse mutation process phase. Each phase performs the following tasks.

-Initial population set generation phase

The initial chromosome is a Directed Initialization technique that uses a method based on prior knowledge or experience. The initial chromosome population is calculated as 126 bits and consists of a total of 10 populations. This can be adjusted by the user according to the environment.

-Fitness function evaluation phase

The generated chromosomes are saved as fuzzy rule files according to their format. The saved rule files are used for fitness evaluation and for generating the offspring of the next generation. One rule file is 6 KB. If the system create a 50th-generation chromosome, a total rule file size of 3,000 KB is required. However, in a general environment that is not being used for analysis purposes, the proposed scheme only requires rule files of the previous generation. Therefore, the fuzzy result files use a small capacity of 60KB.

-Roulette wheel selection phase

$$f_i = \frac{(C_w - C_i) + (C_w - C_b)}{(k-1)}, k > 1$$

The above equation is expressed by formulating a roulette wheel. C_w is the cost of the worst solution in the solution group, C_b is the cost of the best solution in the solution group, and C_i is the cost of solution I. Additionally, k is the selection pressure so that C_b can be selected with a high probability that is k times that of C_w.

-One-point cross over phase

Two randomly selected old chromosomes combine to generate new chromosomes. There are many methods for chromosome selection. We use the most commonly used method: the one-point crossover method. This method selects one random position and two genes are intersected at the selected position. Genes are expressed as binary numbers in the proposed scheme, and newly generated chromosome values may go out of range differently than planned. We check the output range every time to prevent this problem. If a number out of range is output, the system repeats the crossover phase until the conditions are satisfied.

-Reverse mutation process phase

Random chromosome mutations occur in this phase, and this phase escapes the local optimization problem. We applied a probability of mutation of 1%. The reverse mutation phase reverses all of the values of genes.

IV. EXPERIMENT

This section provides a comparative analysis of the proposed approach method and the traditional approach method through experiments. The error rate for each gene for the first population chromosome was calculated and applied. This was done because one gene is determined to be one result element.

A. Experiment Parameters

Table- I: Experiment parameters

Parameters		Value
Field Environment	Sensor Field Size	1,000m x 1,000m
	Number of Nodes	3000
	Number of Clusters	100
	Number of Compromised Nodes	10
	Number of Occurring Events	Depends on the node life
	Base Station Location	(x,y) = (1000m,1000m)
	Node Transmit Range	up to 150m (Mica2)
Transmission Information	Report Size	24 bytes
	Key Index	14 bits
	MAC Size	1 byte
Energy Consumption [15]	Transmit	16.25μJ (per 1byte)
	Receive	12.5μJ (per 1byte)
	MAC Generation	15μJ
	Verification	75μJ
	Cipher	9μJ
Security Value	Security Threshold	5

	Key Number Per Node	1
	Global Key Pool Size	5
	Hop Threshold	2
GA Settings	Crossover Rate	0.7
	Mutation Rate	0.01
	Population Size	10
	Chromosome Length	126
	Gene Length	7
	Max Generation	50

B. Experiment Results

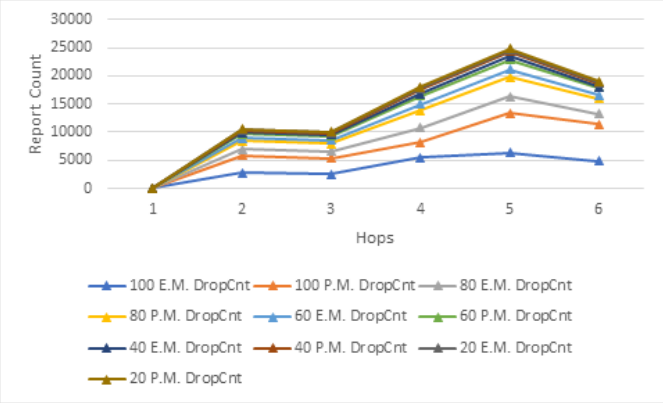

Fig. 8 Number of False Report Drops per Hop Count

Fig. 8 shows the number of false reports filtered by hop count. Overall, the proposed method shows a higher false report filter count than the traditional method. This is because the proposed scheme adjusts the number of MACs included in the report to suit the attack situation. So, it quickly filters out false reports generated in the attacked area.

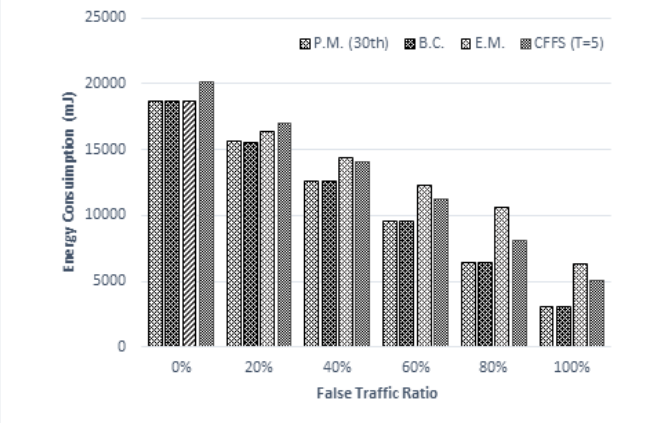

Fig. 9 Overall Network Energy Consumption versus FTR

Fig. 9 shows the total energy consumption of the network. The proposed method (P.M.) refers to a final fuzzy rule that was created by running 50 generations of the proposed scheme. The best case (B.C.) refers to the most efficient chromosome among the 50 generations of chromosomes. When the attack rate is 0%, the energy consumption rate is equal. The reason for this is that the GA fuzzy logic adjusts the security value when the sensor node is attacked, so it outputs the same value. The efficiency of the P.M. increased by 4.451% and the efficiency of the B.C. increased by 4.599% in the 20% attack ratio environment. When the attack rate is 100%, the energy efficiency is improved by up to 51.935%.

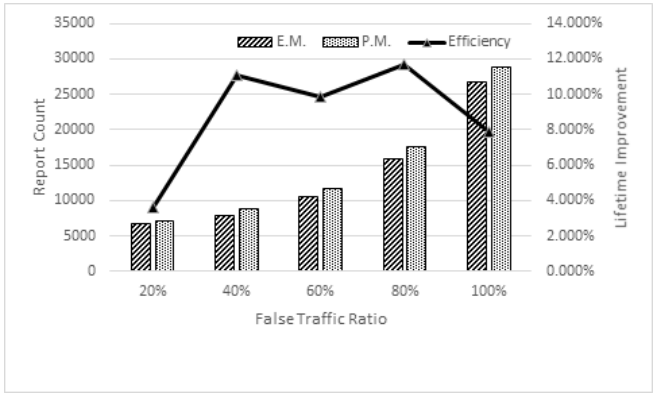

Fig. 10 Network Lifetime versus FTR

Fig. 10 shows the number of events that occurred until any CH node's energy was exhausted. We measured until the energy of a certain node was depleted and a shaded area appeared. The total amount of energy of the node is 2J, according to the specification of the MICAz mote. Based on the results of the experiment, the network lifetime was increased by 8.811% on average. When the false traffic ratio was 80%, the lifetime was increased by up to 11.669%.

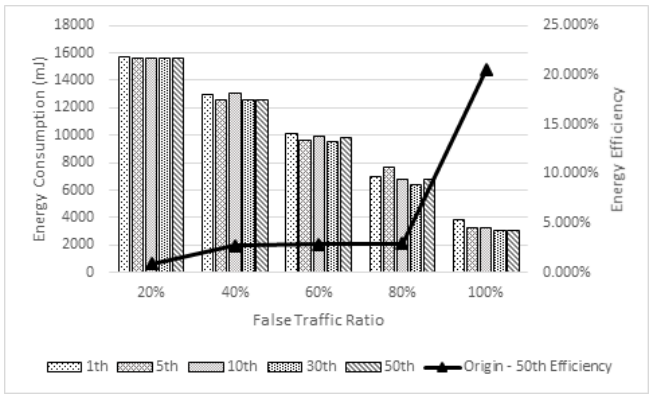

Fig. 11 Total Energy Consumption according to Generation

Fig. 11 shows the energy consumption by generation at the same attack rate in the proposed scheme. The experiment was carried out for 50 generations. As a result, the proposed scheme improves the node energy efficiency by less than 2% in the low attack ratio area. However, when the attack rate was 100%, the energy efficiency increased by up to 20.475%. Based on this analysis of the energy consumption rate by generation, it was determined that most genes after 30 generations consumed a similar amount of energy.

This experimental result indicates that this scheme is adaptively converted to suit the environment after the 30th generation.

Fig. 12 represents the fuzzy membership function transformed by the proposed GA. The membership function parameter adaptively changed according to the environment, as shown in the above Fig.. When the network situation is unstable, the false traffic ratio (FTR) is changed to a lower value for security enhancement. Additionally, the residual energy (RE) and compromised key ratio (CKR) are evolved to suit special environments. As a result, the membership functions have changed so that the security threshold can be set sensitively to detect false reports.

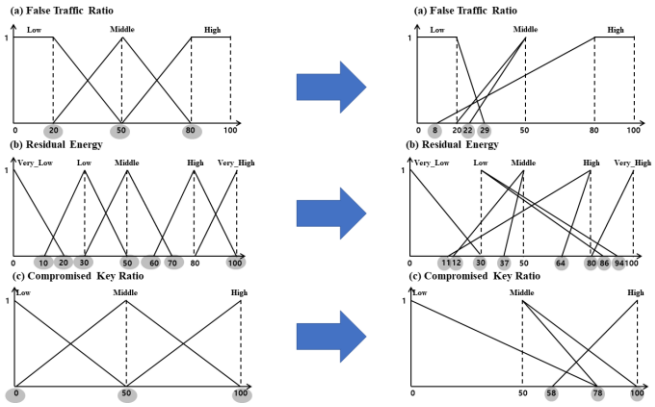

Fig. 12 Improved Fuzzy Membership Function

V. CONCLUSION

In this paper, we introduced a method to extend the overall network life performance by adjusting the parameters of the fuzzy rule to suit the environment; this was done by using GA (a natural evolution theory) to increase the process through fuzzy optimization in fuzzy-based CFFS. According to the results of the experiment, it shows that sufficient energy efficiency was effectively improved with 30 generations of evolution on average. Especially, A cluster node of high attacked area save energy efficiency gradually. We expect that an adaptive system for various fields can be constructed by applying an optimization method to various protocols [15-17] by using the proposed scheme.

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. Xu, Lina, Rem Collier, and Gregory MP O'Hare. "A survey of clustering techniques in WSNs and consideration of the challenges of applying such to 5G IoT scenarios." IEEE Internet of Things Journal 4.5 (2017): 1229-1249.
2. Đurišić, Milica Pejanović, et al. "A survey of military applications of wireless sensor networks." 2012 Mediterranean conference on embedded computing (MECO). IEEE, 2012.
3. Kuorilehto, Mauri, Marko Hännikäinen, and Timo D. Hämäläinen. "A survey of application distribution in wireless sensor networks." EURASIP Journal on Wireless Communications and Networking 2005.5 (2005): 859712.
4. Metke, Anthony R., and Randy L. Ekl. "Security technology for smart grid networks." IEEE Transactions on Smart Grid 1.1 (2010): 99-107.
5. Lin, Jie, et al. "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications." IEEE Internet of Things Journal 4.5 (2017): 1125-1142.
6. Igure, Vinay M., Sean A. Laughter, and Ronald D. Williams. "Security issues in SCADA networks." computers & security 25.7 (2006): 498-506.
7. Liu, Zhixiong, et al. "A Cluster-Based False Data Filtering Scheme in Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 23 (2014).
8. Jung Sub Ahn, & Tae Ho Cho. "FBCFFS-Based Authentication Method for Node Privacy Message in WSN" International Journal of Engineering and Advanced Technology (IJEAT), (2020): Vol. 9, No. 3, pp. 313 – 318.
9. Tanese, Reiko. "Distributed genetic algorithms for function optimization." (1989).
10. Whitley, Darrell. "A genetic algorithm tutorial." Statistics and computing 4.2 (1994): 65-85.
11. Maulik, Ujjwal, and Sanghamitra Bandyopadhyay. "Genetic algorithm-based clustering technique." Pattern recognition 33.9 (2000): 1455-1465.
12. Klir, George, and Bo Yuan. Fuzzy sets and fuzzy logic. Vol. 4. New Jersey: Prentice hall, 1995.
13. Yen, John, and Reza Langari. Fuzzy logic: intelligence, control, and information. Vol. 1. Upper Saddle River, NJ: Prentice Hall, 1999.
14. Oh, S. K. "Advanced Hybrid Fuzzy Inference Systems by Programming." (2005).
15. 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.
16. Jung Sub Ahn, & Tae Ho Cho. "Node Density Based Security Level Determining to Prolong the Lifetime of WSN through Network Conditions" International Journal of Innovative Technology and Exploring Engineering (IJITEE), Jul. (2020): Vol. 9, No. 9, pp. 340 – 344.
17. 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. 2006.G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

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.