International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

FBCFFS-Based Authentication Method for Node Privacy Message in WSN

Jung-sub Ahn, Tae-ho Cho

Abstract: ***In wireless sensor networks (WSNs), the design of the energy management of the nodes and report security are important. In particular, many studies have focused on maintaining report in applications where an Internet of Things (IoT) system is connected with a WSN, with the IoT actuator operated based on measured data of WSNs. A Fuzzy-based Cluster-based False Data Filtering Scheme (FBCFFS), which can dynamically adjust security in a vulnerable network situation, maintains security using the cluster state information of the network. This scheme uses fuzzy logic, a type of rule-based expert system. The fuzzy logic system of the FBCFFS determines security strength based on network monitoring information. However, previous work with the FBCFFS has not addressed the security of the cluster information. Thus, there exists risk of data transformation at the middle transmission step in the previous approach. In addition, the node periodically transmits state information to the base station, which is inefficient in terms of network lifetime management. In this paper, we provide a method to secure the state information message and to reduce the communication cost by controlling the number of messages.***

Keywords: fuzzy system, node energy efficiency management system, wireless sensor networks, node state data security, node privacy message, message authentication.

I. INTRODUCTION

Wireless sensor networks (WSNs) used in fields including healthcare, environment and agriculture, public safety and military systems, industry and transportation systems, and for field monitoring and industrial monitoring and control have densely deployed sensor nodes[1-6]. Each WSN is composed of many tiny nodes, such as the MICAz mote [7], which makes it difficult to supervise individual nodes. Also, most deployed sensor nodes in a wide range of application fields have finite energy. Research has been done for a long time to address the problem of limited energy. In particular, the Fuzzy-Based Cluster-Based False Data Filtering Scheme (FBCFFS) proposed by Ahn and Cho [8] verified that the lifetime of the nodes can be increased by dynamically setting cluster security strength based on fuzzy logic to increase the early filtering probability and adjust the report size. In this scheme, the node states are transmitted as the message format from each cluster region to cope with various situations. Since the base station (BS) periodically receives node status messages, periodic measurements are made, even in areas where there are no environmental changes. In other words, if periodic messages are sent to the base station even when there is no change in conditions, the lifetime of the intermediate forwarding cluster will be reduced. In addition, if the message is not secured and the wrong message is injected into the BS, the security is adjusted incorrectly. As a result, the network of manipulated secure strength cannot be secured against a false report injection attack.

In this paper, we introduce a method for minimizing the periodic state request messages from the FBCFFS. As a result, the number of messages sent and received can be reduced and the node lifetime can be extended. In this paper, we describe a data-centric approach to represent a new, energy-efficient method of node data processing for FBCFFS. There is an additional overhead of four messages to use the fuzzy system in FBCFFS.

1. State request message sent from BS to Cluster Head (CH) nodes at periodic intervals.
2. Node state messages sent from CH nodes to BS.
3. Attack detection message sent to BS when false report is detected at CH node.
4. Threshold setting message for setting new security threshold by deriving new threshold from BS.

This paper introduces a new, energy-efficient and message security method that manages the above messages. The main advantage of the proposed approach is that it reduces the intra-node processing cost by improving the efficiency of the message handling method to decrease the communication cost. The proposed method reduces network congestion by significantly reducing the amount of data transmitted to the BS. The main design of the proposed method is suitable for the case where the energy of the network is almost exhausted and the energy of the nodes needs to be saved while satisfying a minimum level of security. The system model of the proposed method is analyzed analytically using various mathematical expressions.

Revised Manuscript Received on February 05, 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

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

In addition, security algorithms such as DES (Data Encryption Standard) [9] and RC4 (Rivest's Cypher) [10] provide security for messages. As a result, the CH nodes trasmit securely privacy message of required to the expert system of BS. The rest of this paper is organized as follows. Section 2 briefly describes the general wireless sensor network background, countermeasures in threat of the application layer of the WSN with the FBCFFS and fuzzy system.

Section 3 presents our motivation and proposed method in detail, and Section 4 provides the security analysis. Finally, the conclusions are discussed at the end of this paper.

II. RELATED WORKS

This section provides background on WSNs and use of the fuzzy system for making security system decisions. It also describes FBCFFS used for WSN security.

A. Wireless Sensor Networks

A WSN is an independent set of sensors that can sense, compute, and communicate through a network of widely deployed sensor nodes. Sensor node devices have less memory, battery and computing power [11]. Sensor nodes send data to a central processing system called a BS through intercommunication between neighboring nodes. The BS collects node information and connects to various smart devices such as the Internet, smartphones and computers.

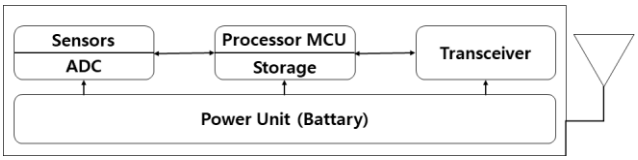

Fig. 1. Sensor node structure

The sensor node includes a transmitter and receiver module for transmitting and receiving a signal, either using an antenna or a connection to an external antenna, as shown in Fig. 1. The processor Micro Control Unit (MCU) is responsible for connecting the circuit to the power unit, creating an interface between the circuit and the power unit and communicating with other modules [12].

B. Fuzzy System

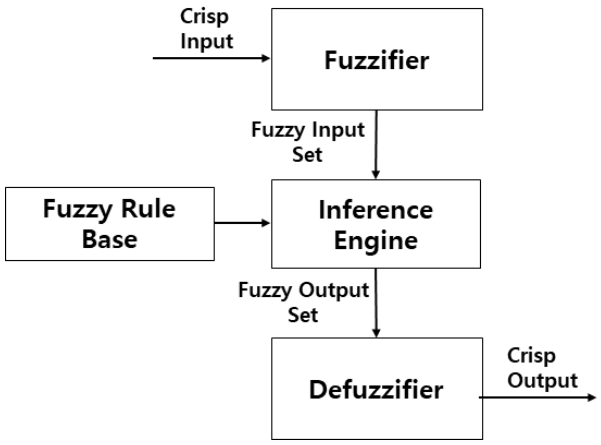

Fig. 2. Fuzzy inference system

A fuzzy system is a mathematical method that infers a result by expressing human thoughts and expert knowledge as a rule structure [13]. The output of a traditional reasoning system is clearly divided into true (1) or false (0), but the fuzzy system represents intermediate values between 1 and 0 based on inference rules defined by experts and a language variable set for various applications. This means that nonlinear systems can be described by rules, and nonlinear systems also can be modeled based on linguistic rules. The structure of the fuzzy logic system consists of three basic modules, namely the fuzzifier, inference engines and defuzzifier, as shown in Fig. 2. The fuzzifier takes crisp values as system inputs and returns the degree of the membership fuzzy function corresponding to each crisp value. Inference rules are required for fuzzy reasoning in a fuzzy system. Rules of a fuzzy rule base are expressed in If-Then format. Each rule is divided into first half and second half variables. The inference engine performs mapping between fuzzy system inputs and the corresponding fuzzy sets with the help of a rule base written in advance. The membership function assigns a membership percentage (or decimal value) to each fuzzy set characterized by linguistic terms such as 'far', 'medium', and 'near'. The input of the defuzzifier obtains the fuzzy set from the inference system. When a reasoning result is needed, such as process control, the intermediate value is converted into a crisp value through the defuzzification phase. Defuzzification methods include Zadeh's averaging method [14] and Mamdani's center of gravity method [15]. However, running fuzzy logic in a WSN requires minimizing system development costs, design time, and computational memory [16]. Therefore, most fuzzy-based WSNs use the Mamdani reasoning method, which is faster than other reasoning methods.

C. A Method of Improving Detection Ratio through Cluster Security Threshold Management in CFFS (FBCFFS)

Ahn and Cho [8] proposed a cluster dynamic throttling algorithm that determines security strength based on a fuzzy logic called CFFS [17] to secure WSN applications. The proper security strength is determined by applying the appropriate security level to the situation considering the energy state of the cluster and the attack level of the cluster. The fuzzy system evaluates multiple target output functions by aggregating individual targets through operators of fuzzy averaging (OFA) in a given order, independently defining fuzzy membership functions for each target. Simulation results show that FBCFFS is superior to CFFS in various attack situations in terms of minimizing energy consumption. Also, the FBCFFS maximizes the active duration of the sink node in the multi-connection sink scenario. However, there is increased overhead during the data transfer process. The next section shows to maximize network life by reducing the flow of data to solve this problem.The security threshold management method proposed by Ahn and Cho is a scheme to extend the network lifetime through the appropriate security threshold inferring to the field situation using fuzzy system. If a low threshold is set in a high-attack-rate environment, the BS is likely to receive a false report.

If a high threshold is set in a low-attack-rate environment, the size of the report increases, which increases the transmit/receive energy of the node. In other words, the threshold should be adjusted according to the network state to improve the energy efficiency of the node. In FBCFFS, the threshold is decided through four steps.

(1) A BS with the ability to execute a fuzzy system infer a new threshold using applied expert rules when the BS receives a security message requisition or specific time period correctly. The fuzzy system gathers cluster state factors from each CH node and uses them as fuzzifier inputs.

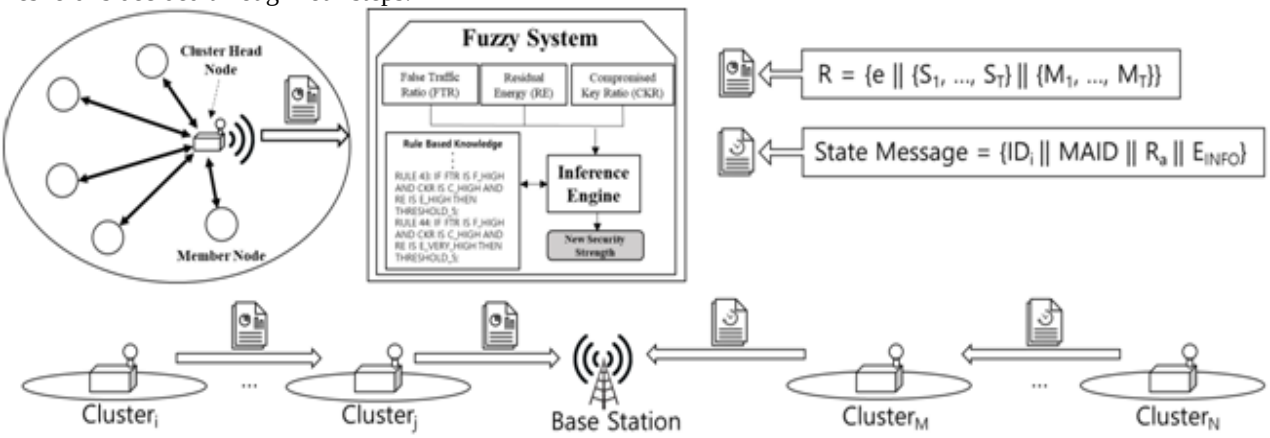

Fig. 3. Proposed scheme overview

(2) A new threshold is determined by the fuzzy system and this value is propagated to the specific cluster using geocast communication.
(3) If the CH node receives the new threshold message, it applies the new security setting to its cluster.
(4) When a bogus report is generated in a damaged area, the intermediate node can drop the bogus report more quickly, with an improved detection ratio. Also, the report size is reduced in areas with low attack rates. This means that less transmission energy is consumed. areas with low attack rates. It means to save transmission energy consumed.

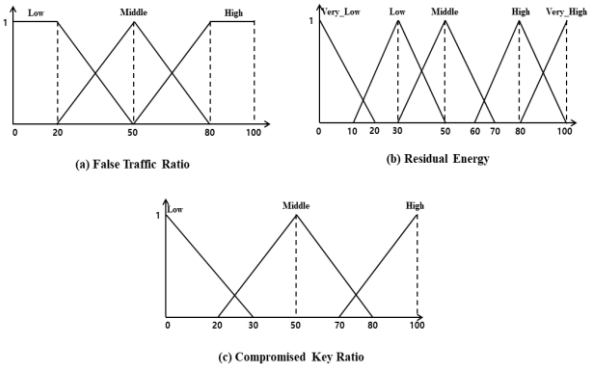

Figure 4 Fuzzy membership function

In the FBCFFS fuzzy system, there are three membership functions, as shown in Fig. 3 above. Each membership function description is as follows.

1) False Traffic Ratio (FTR): FTR represent a risk of clusters can be collected through the false report ratio of the BS. A higher FTR indicates a higher attack occurrence in a cluster.
2) Residual Energy (RE): Sensor nodes have limited power resources; the new security threshold should be decided based on the energy state of the node.
3) Compromised Key Ratio (CKR): If the ratio of the compromised key increases, the probability of verifying the false report becomes lower at the nodes. Therefore, the threshold value should be determined considering the compromised ratio of the key in a cluster. The fuzzy membership function's variables are as follows:

· False Traffic Ratio (FTR) : { Low (F_L), Middle (F_M), High (F_H) }
· Residual Energy (RE) : { Very_Low (R_V_L), Low (R_L), Middle (R_M), High (R_H), Very_High (R_V_H) }
· Compromised Key Ratio (CKR) : { Low (C_L), Middle (C_M), High (C_H) }
· Threshold (TH) : { THRESHOLD1, THRESHOLD2, THRESHOLD3, THRESHOLD4, THRESHOLD5 }

A periodic request message in the existing scheme is sent to a node to receive a node status message. However, the BS does not know how many events have occurred at each node because if a false report insertion attack occurs, intermediate nodes can filter the report through collaborative verification. In order to satisfy the input of the above fuzzy system, it is necessary for the BS to know the amount of energy remaining in the CH node.

III. PROPOSED SCHEME

A. Motivation

Existing schemes execute the fuzzy logic system periodically through a node information collection phase to determine a new security threshold. There is overhead to transmit and receive messages periodically to obtain node status information. However, frequent requests for node state information are disadvantageous in terms of the energy management of the nodes. WSNs often need the ability to maintain network secure with minimal energy costs. The node's state message is used as a fuzzy input for determining the new security strength, so the security of the message is important. If the security strength is set incorrectly, an attacker can change the value to easily derive a new security boundary outside the security range.

This result allows an attacker to launch a false report injection attack. Because of this type of attack, which causes false alarms and corrective actions from network administrators and wastes unnecessary energy at intermediate nodes, it is necessary to secure network node state messages.

B. Detailed proposed scheme

Fig. 4 shows an overview of the proposed scheme. Each cluster detects events, generates reports, and sends reports to the BS. In addition, reports are verified in en-route filtering through communication between CHs. When the report finally arrives at the BS, the BS verifies the report using its global key pool.

In addition, if the verification phase determines that a new security strength should be set, a status request message is sent to the target cluster node. Each CH node receives a state information request message from the BS or encrypts the privacy information message including residual energy at periodic intervals and sends the state information message to the BS. The BS verifies the state information message and uses the contents of the report as input to the fuzzy logic system when judging it as a legitimate report. In this proposed scheme, we introduce to control method the number of messages and event messages that occur periodically for energy saving.

Residual energy is an essential input element to the proposed fuzzy system, which is used to adjust the new security strength. However, existing methods do not include detailed security methods. The proposed scheme applies data encryption standard (DES) to the design to secure the required messages. This algorithm is designed to encrypt and decrypt data blocks. The key length is 64 bits and uses the previously distributed cluster key and node's private key. The base station receiving the message has a key pool that manages the keys of all the nodes so that it can decrypt the encrypted message. The notations used in this paper are defined in Table- I.

Table- I: Notation used in this paper

Notation	Description
e	Preset Field Event Content
S_n	Identity of a Sensor Node
MAC	Message Authentication Code
T	Cluster Security Threshold Value
RE_n	Residual Energy of S_N
E_{INFO}	Amplified Energy Info RE_N
CL_iK	Key of Cluster i
S_NK	Key of S_n
R_a	Random numbers generated by pseudo-random function
E()	Symmetric key cryptosystem using DES
H()	Cryptographic hash function using RC4
$\|\|$	Concatenation operation
$\oplus$	XOR operation

In the first step of the proposed scheme, when a sensor node detects an event such as pressure or context change, the sensor node collects and compares information about it to check whether it is a newly detected value. Also, the CH node compares the collected information to the average value. If the new value differs from the mean and the margin of error, the new measured value is ignored. The error range used may have various settings, depending on the application field. If the CH node receives a similar value, the node creates a report based on the received event and forwards it to the BS. In the second step, when receiving a state request message from the BS or at a specific condition, the state message is encrypted and transmitted as follows.

$$CID = ESNK(ID_i||CLK_i) \quad (1)$$

$$MAID = H(ID_i||SNK||R_a) \quad (2)$$

$$MAC = H(Ra||SNK) \quad (3)$$

$$E_{INFO}=E_{CLK}(CID_i \oplus RE_i \oplus MAC) \quad (4)$$

$$SM = (ID_i||MAID||R_a||E_{INFO}) \quad (5)$$

The node computes the cluster identification (CID) as shown in (1) using its own ID and the cluster key (CLK) distributed through the LEAP method. The node also selects a random number, R_A, using a pseudo-random function and computes the message authentication identification (MAID) using its secret key SNK and a stored RC4-based hash function H(). Using the random numbers R_A and H () selected in the previous step, the MAC is computed as shown in (3). The CID and MAC calculated in (1) and (3) and the remaining energy RE_i of the node are inserted, as shown in (4), and encrypted using the cluster key to compute E_{INFO}. Finally, the node constructs the privacy message state message (SM) as shown in (5) and sends it to the BS.

The above process can be used to verify a report's legitimacy. Thus, this method can prevent data tampering by a man-in-the-middle (MITM) attack. As a result, the BS can avoid the risk of inferring the wrong new security strength in the fuzzy system. In addition, the proposed method counts the number of reports forwarded and the number of events detected at each CH node at regular intervals in order to prevent meaningless reports from being sent. The CH node sums the count value and if a certain count is exceeded, an SM report is sent to the BS and the detection count is reset to 0. In this way, the proposed method saves energy by reducing the number of transmissions and receptions of meaningless reports in areas with low frequency of reports.

IV. SECURITY ANALYSIS AND RESULT

This section provides a security analysis for replay attacks, MITM attacks, offline password guessing attacks and denial-of-service (DoS) attack [20-23].

A. Replay Attack

A replay attack is an attack where a user acquires a MAC and reuses it. However, if a sufficiently large-scale random number is used for R_A, the attacker cannot obtain the node ID and node key value due to the discrete logarithm problem. Therefore, the RE_i information is secure against a replay attack.

B. Man-in-the-middle attack (MITM)

MITM attacks occur between sensor nodes and servers to intercept communications. However, the attacker cannot analyze the contents of the message because it transmits the information of the message that changes every time with the fresh random number of the MAC and the encrypted message using DES of the E_{INFO}.

C. Offline password guessing attack (OPGA)

An OPGA is an attack that guesses and transmits the key sent to the SM offline.

However, the SM does not include password-related information. Also, since the MAC uses the one-way hash function H (), the attacker could not compute the secret key.

D. Denial-of-Service attack (DoS)

DoS in WSNs is the disruption of services by sending numerous messages to the BS, restricting access to the service and causing the service to stop. The main aim of this attack is to render a network incapable of providing the general service by targeting the network's bandwidth. However, our proposed method can verify the ID of each message using MAID. Also, there is no way for the attacker to acquire the secret key and the cluster key from the message being transmitted.

Table- II: The security comparison between protocols

Type of threats	FBCFFS	Proposed Scheme
MAC usage	Yes	Yes
False report injection	Yes	Yes
Replay	No	Yes
MITM	No	Yes
OPGA	No	Yes
DoS	No	Yes
Security offered	Authentication	Authentication, integrity of messages

The Table II shows the advantages of our proposed scheme. Our proposed method is established to protect the confidential information like privacy information in healthcare and military application. So, our proposed method provides to denied access to an adversary using encryption data.

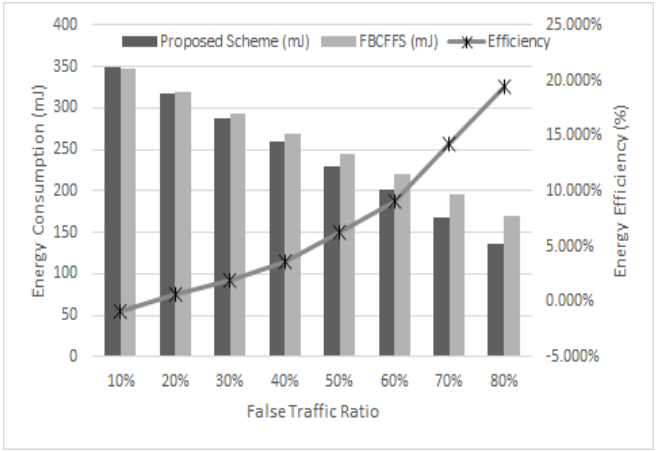

Figure 5 Comparison graph of FTR versus energy consumption between FBCFFS and proposed scheme

Figure 5 shows the energy consumption comparison graph. The graph assumes when 1000 events occur. In FBCFFS, a fixed security threshold was derived from the erroneous fuzzy input, and the proposed scheme balance an appropriate security threshold. When the attack rate was low, the energy efficiency was measured due to the additional message of the proposed scheme. The higher the attack rate, the higher the energy efficiency.

V. CONCLUSIONS

Attackers can compromise sensor nodes deployed in open environments for malicious purposes such as false report injection or network failures. The existing FBCFFS uses fuzzy logic to control the security strength of the network to defend against false reports. The BS receives a privacy message from a node selected as a cluster head node among nodes placed in a sensor field for a fuzzy inference system. However, because the node transmits the status information periodically even in areas where events do not occur frequently, the BS receives messages in which there is little status change. This fact leads to unnecessary energy consumption of the nodes. Also, the previous scheme uses vulnerable communication method about replay attacks etc. Therefore, there are many applications that require nodes to be used for long periods of time, where energy must be minimized while maintaining minimal security, so there is a need for a method of reducing unnecessary energy consumption.

In this paper, we proposed a method to reduce the number of periodic information request messages and maintain the minimum-security level in order to extend the cluster life of the FBCFFS. The proposed method restricts messages to areas where recent events occurred. Therefore, a new threshold value is not set in areas where events are less frequent, so the security may be weakened. However, the proposed scheme significantly improved cluster lifetime in terms of node energy management in areas with low occurrence of events. In addition, proposed scheme provides a variety of security schemes for privacy messages using low overhead encryption technique.

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. Zhang, Yuan, et al. "Ubiquitous WSN for healthcare: Recent advances and future prospects." IEEE Internet of Things Journal 1.4 (2014): 311-318.
2. Li, Xuemei, Yuyan Deng, and Lixing Ding. "Study on precision agriculture monitoring framework based on WSN." 2008 2nd International Conference on Anti-counterfeiting, Security and Identification. IEEE, 2008.
3. Đurišić, Milica Pejanović, et al. "A survey of military applications of wireless sensor networks." 2012 Mediterranean conference on embedded computing (MECO). IEEE, 2012.
4. Khanafer, Mounib, Mouhcine Guennoun, and Hussein T. Mouftah. "WSN architectures for intelligent transportation systems." 2009 3rd International Conference on New Technologies, Mobility and Security. IEEE, 2009.
5. 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.
6. Zhao, Gang. "Wireless Sensor Networks for Industrial Process Monitoring and Control: A Survey." Network Protocols & Algorithms 3.1 (2011): 46-63.
7. Ali, Nurul Amirah, Micheal Drieberg, and Patrick Sebastian. "Deployment of MICAz mote for wireless sensor network applications." 2011 IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE). IEEE, 2011.
8. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy Jung Sub Ahn and Tae Ho Cho , "A METHOD OF IMPROVING DETECTION RATIO THROUGH CLUSTER SECURITY THRESHOLD MANAGEMENT IN CFFS", International Journal of Advanced Research(IJAR), Vol. 5, No. 12, pp. 872-879, Jul. 2018.
9. Coppersmith, Don. "The Data Encryption Standard (DES) and its strength against attacks." IBM journal of research and development 38.3 (1994): 243-250.
10. Mironov, Ilya. "(Not so) random shuffles of RC4." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2002.
11. Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." Computer networks 38.4 (2002): 393-422.
12. Vieira, Marcos Augusto M., et al. "Survey on wireless sensor network devices." EFTA 2003. 2003 IEEE Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No. 03TH8696). Vol. 1. IEEE, 2003.
13. Yen, John, and Reza Langari. Fuzzy logic: intelligence, control, and information. Vol. 1. Upper Saddle River, NJ: Prentice hall, 1999.
14. Zadeh, Lotfi Asker. "Fuzzy sets as a basis for a theory of possibility." Fuzzy sets and systems 1.1 (1978): 3-28.
15. Mamdani, Ebrahim H., and Sedrak Assilian. "An experiment in linguistic synthesis with a fuzzy logic controller." International journal of man-machine studies 7.1 (1975): 1-13.
16. Lee, Chuen-Chien. "Fuzzy logic in control systems: fuzzy logic controller. II." IEEE Transactions on systems, man, and cybernetics 20.2 (1990): 419-435.
17. Liu, Zhixiong, et al. "A Cluster-Based False Data Filtering Scheme in Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 23 (2014).
18. Camp, Tracy, and Yu Liu. "An adaptive mesh-based protocol for geocast routing." Journal of Parallel and Distributed computing 63.2 (2003): 196-213.
19. O. Goldreich, S. Goldwasser, and S. Micali. How to Construct Random Functions. Journal of the ACM, Vol. 33, No. 4, 1986, pp 210-217.
20. Nyang, DaeHun, and Mun-Kyu Lee. "Improvement of Das's Two-Factor Authentication Protocol in Wireless Sensor Networks." IACR Cryptology ePrint Archive 2009 (2009): 631.
21. Mansouri, Djamel, et al. "Detecting DoS attacks in WSN based on clustering technique." 2013 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2013.
22. Pathan, Al-Sakib Khan, ed. Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press, 2016.
23. Udgata, Siba K., Alefiah Mubeen, and Samrat L. Sabat. "Wireless sensor network security model using zero knowledge protocol." 2011 IEEE International Conference on Communications (ICC). IEEE, 2011.

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.