Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/7436
DOI URL: http://dx.doi.org/10.21474/IJAR01/7436

RESEARCH ARTICLE

A METHOD OF IMPROVING DETECTION RATIO THROUGH CLUSTER SECURITY THRESHOLD MANAGEMENT IN CFFS.

Jungsub Ahn and Taeho Cho.
Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea.

Manuscript Info

Manuscript History

Received: 18 May 2018
Final Accepted: 20 June 2018
Published: July 2018

Keywords:-
WSN Security Network Communication Cluster-based False Data Filtering Scheme False Report Injection Attack Energy Management.

Abstract

Today, security is becoming more important as more WSN applications are developed. In a sensor network, an attacker can easily physically acquire and compromise the node, and such threats can be used to inject false reports into the network. The Cluster-based False Data Filtering Scheme (CFFS), a recently proposed security protocol, divides the nodes into cluster units, and the nodes verify the report. This scheme exhibits a high false report filtering performance, but does not consider the regional environment. Further, this scheme consumes a lot of energy in areas where no attacks occur. Energy management is important because nodes are difficult to charge or replace after deployment. This paper proposes an independent security threshold setting method considering regional characteristics using a fuzzy system to select appropriate security boundaries. In the fuzzy system, the appropriate security threshold value is output considering the false report ratio, ratio of the damaged key, and residual energy of the node. Experimental results show that the proposed method improves the energy efficiency by an average of 11.717% over CFFS.

Introduction:-

Internet of Thing (IoT) applications using Wireless Sensor Networks (WSNs) have grown in number over the past decade. IoT has various application domains such as transportation and logistics, healthcare, smart environments, personal and social, and futuristic domains [1]. IoT can be configured based on a WSN, which consists of many nodes and performs peer-to-peer communication between the nodes to transmit the event data to the sink node [2]. Military applications, one type of WSN applications, need a reliable multi-hop networking path from the source node to the sink node because it collects important information [3]. As a result, filtering false data in this area is also a very important issue. In particular, nodes have limited resources and may be subject to repetitive application layer attacks or may malfunction due to energy exhaustion [4]. Generally, sensor nodes have limited capability and it is difficult to supply or replace their power after deployment [5].

Corresponding Author:- :- TaeHo Cho
Address:- College of information and communication engineering, sungkyunkwan university, republic of korea.

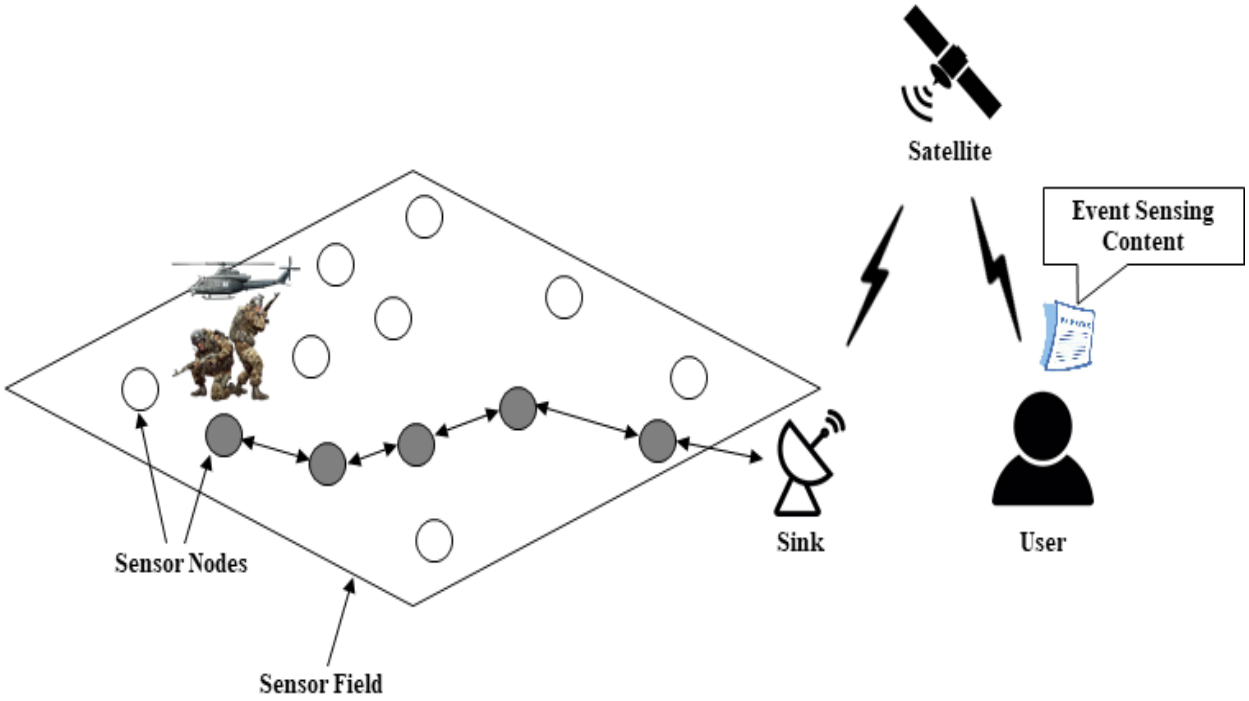

Figure 1:-Wireless Sensor Network Overview

Figure 1 shows a schematic of the adversary detection situation in WSNs. When a sensor node detects an event, it generates a report based on the corresponding information. Then, the sensor nodes transmit the report to the sink node according to the determined routing path, and the sink node transmits the corresponding contents to the user or network administrator via the Internet or satellites. However, sensor nodes are vulnerable to attacks because they are deployed in open environments. False report injection attacks can be performed using keys from compromised nodes. Research has been performed to prevent such threats [6-10]. The proposed Cluster-based False Data Filtering Scheme (CFFS) verifies the report that is generated randomly, specifically using the contents of the report and the key of the node [11]. The verification process is described in Section 2. The false report validation probability is proportional to the number of Message Authentication Codes (MACs) included in the report. The number of MACs included in the report is propagated before the nodes are deployed. Thus, a high number of MACs guarantees high security for the network. However, as the number of MACs increases, the report size will also increase, which will require a large amount of energy to transfer and receive the report. Therefore, since the number of MACs suitable for each cluster is different, an independent threshold value should be set that considers environmental factors. This paper proposes a method to determine the appropriate number of MACs according to the environmental factors of the cluster and the network environment using fuzzy logic. The proposed method reduced the number of MACs in areas with a low attack ratio and reduced the report capacity to lower the costs of sending and receiving data. Alternatively, in regions where the attack rate is high, the number of MACs is increased in order to increase the probability of en-route filtering. Therefore, the proposed scheme provides efficient network energy management considering the security and node energy. Section 2 describes a false report injection attack process and CFFS. In Section 3, the proposed scheme is introduced. Section 4 demonstrates the effectiveness of the proposed scheme through experiments. Section 5 concludes the paper.

Related Works:-

This section introduces the false report injection attacks, the proposed scheme motivation and the operation of CFFS.

False Report Injection Attack:-

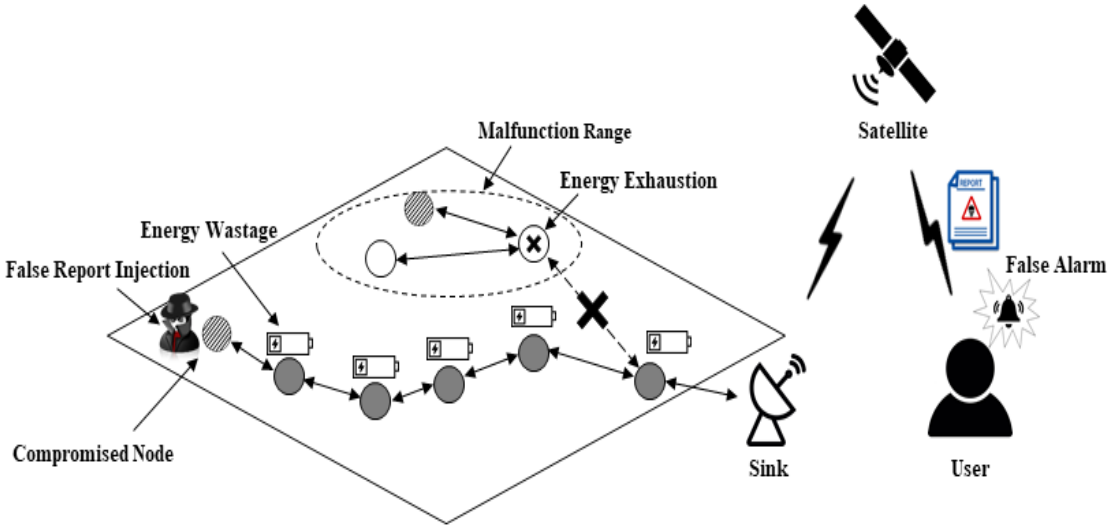

Figure 2:-False Report Injection attack Problems

Figure 2 shows an example of a false report insert attack. It is possible for attackers to physically compromise few nodes and capture the node information. In addition, false reports can be created and injected into the network based on the confidential information obtained by the compromised node. False report injection attacks have three critical adverse effects on networks:

1. A node can consume unnecessary energy and deplete its energy.
2. Energy depletion of nodes hinders node routing, which prevents transmission of normal reports.
3. False alarms are generated that can require unnecessary actions of the user.

Cluster-based False Data Filtering Scheme:-

CFFS consists of five phases: the Pre-deployment and bootstrapping phase, Distributed key assignment phase, Report generation phase, En-route filtering phase, and Sink verification phase [11]. In the Pre-distribution phase, the CH nodes calculate the burden value and send it to the upstream node. This phase is determined by two factors: distance to the sink node and number of paths. When a node detects an event, it generates a report as follows:

$$R : \{e; S_1, S_2, ..., S_i; M_1, M_2, ..., M_i \} / \text{MAC } M_i : K_i(e),$$

where e denotes event content, S_i is the id of node$_i$, and M_i denotes the MAC. When an event occurs, the node that detects the strongest signal is selected as the Cluster Head (CH) node. The CH node broadcasts the event content e and informs its member nodes. The member node compares the content of e with its own content. If the contents of the event are detected as the same, the member node generates a MAC with its own key. The CH node collects the MAC generated from the member node and generates a report by attaching the MAC corresponding to the security threshold value T. Finally, the report is sent to the sink node. During transmission, if the intermediate nodes have the same key as included in the report, they generate and verify the MAC of the report. Later on, the sink node verifies the integrity of the report by verifying all MACs using the global key pool.

Motivation:-

In CFFS, a report is generated by a CH node selected by a cluster-based filtering scheme. The probability of verification of this report at the intermediate node is determined in proportion to the number of MACs included in the report. Therefore, if the node has a high security threshold, it has a high false report validation probability. However, there is a trade-off between security and energy consumption of report delivery. If a false report is detected through the verification node's filtering or BS verification, the network risk increases, and if the security threshold of all nodes is increased, the network maintenance time may be adversely affected. This is because, even in pure areas, a lot of energy is required to send and receive reports. Therefore, the security threshold needs to be adjusted based on the compromised key ratio per cluster.

Proposed Scheme:-

Overview:-

If CFFS detects false reports through an intermediate verification node or BS validation, the source cluster of the report is considered as corrupt. In the en-route phase of CFFS, it is checked whether the node belongs to the same cluster. Therefore, a false report injection attack cannot be performed in the other cluster using the damaged node. The proposed scheme uses these characteristics of CFFS to set the damage rate for each cluster and to increase the probability of intermediate filtering of the false reports by assigning independent thresholds. As a result, the proposed scheme will provide sufficient security power for the cluster environment and increases network lifetime.

Detailed Procedure:-

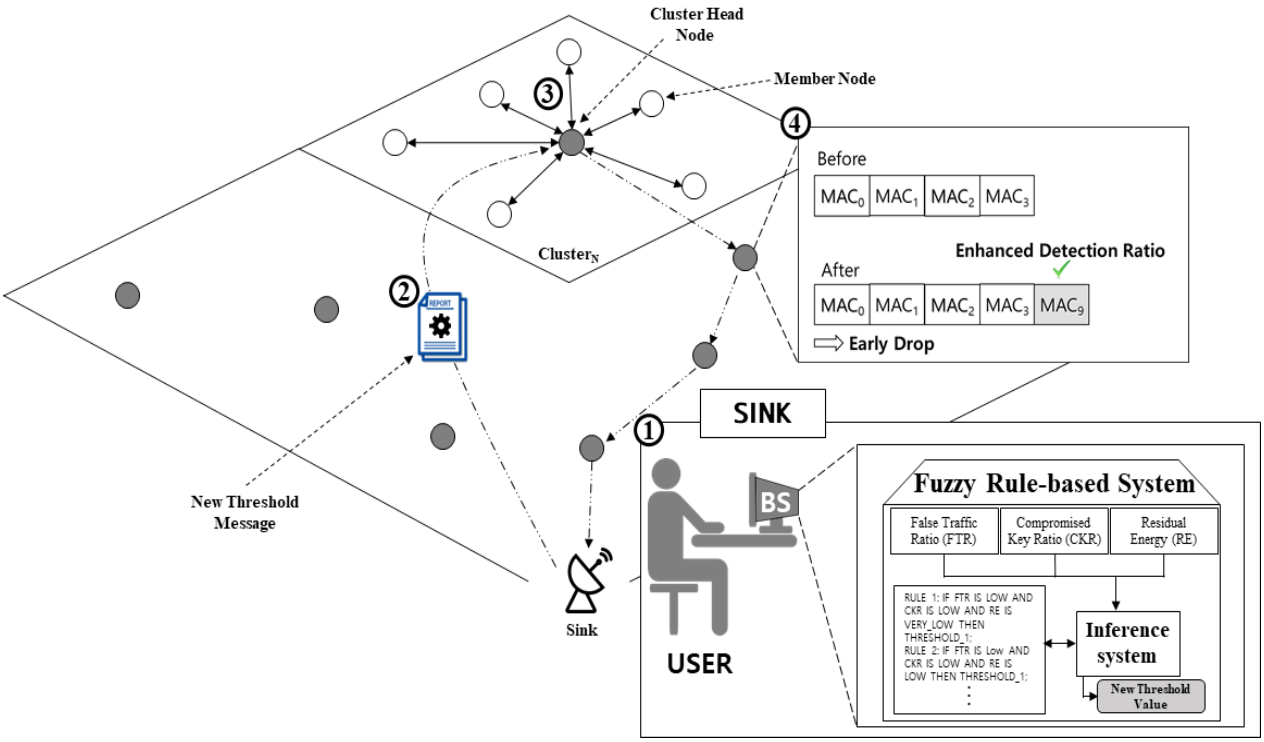

Figure 3:-Proposed Scheme Overview

Sink nodes are more likely to receive false reports if they are configured with low thresholds in an environment with high attack rates. If the intermediate verification node detects a false report, it notifies the sink node.

1. The sink node executes the fuzzy system when receiving the message about false report detection or the set period. The fuzzy system collects environmental factors from nodes and uses them as inputs.
2. In the fuzzy system, a new threshold value is derived, and this value is propagated to the damaged cluster.
3. The cluster head node that receives the message sets a new threshold value.
4. If a false report is generated in the compromised area, the false report can be dropped early with an enhanced detection power. In areas with low attack rates, it also reduces the size of the report, saving energy between transmissions. The threshold updating frequency is also an important issue, but it is beyond the scope of this paper.

Fuzzy System:-
Fuzzy Membership Function:-

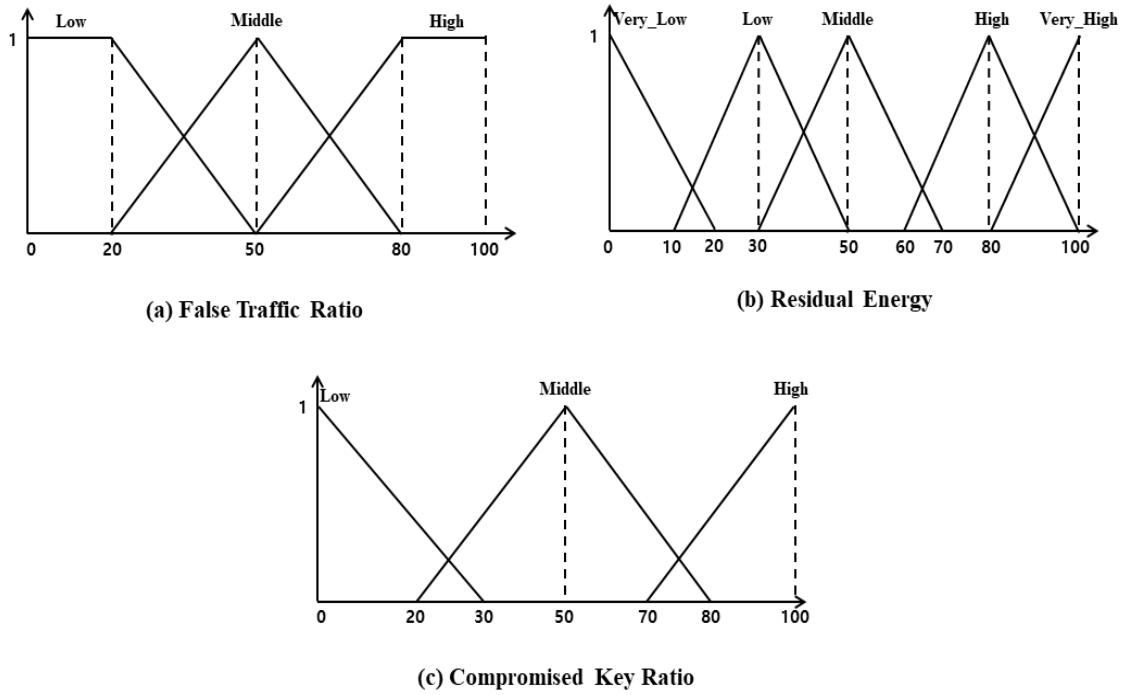

Figure 4:-Fuzzy Membership Function

The proposed fuzzy system has three membership functions.

1. False Traffic Ratio (FTR): The risk of clusters can be measured through the percentage of false reports. A higher cluster risk indicates a higher attack frequency in the cluster.
2. Residual Energy (RE): Since the sensor nodes have limited energy resources, an increase of the security threshold should be decided on by considering the energy level of the node.
3. Compromised Key Ratio (CKR): If the ratio of the compromised key increases, the probability of verifying the forged report decreases. Therefore, the threshold value should be determined considering the compromising ratio of the key. The variables of the fuzzy membership function are as follows:
4. False Traffic Ratio (FTR) : { Low (F_L), Middle (F_M), High (F_H) }
5. Residual Energy (RE) : { Very_Low (R_V_L), Low (R_L), Middle (R_M), High (R_H), Very_High (R_V_H) }
6. Compromised Key Ratio (CKR) : { Low (C_L), Middle (C_M), High (C_H) }
7. Threshold (TH) : { THRESHOLD1, THRESHOLD2, THRESHOLD3, THRESHOLD4, THRESHOLD5 }

Fuzzy Rules:-

Rule No.	IF			THEN
	FTR	CKR	RE	TH
01	F_L	C_L	E_V_L	TH1
02	F_L	C_L	E_L	TH1
03	F_L	C_L	E_M	TH1
...				
15	F_L	C_H	E_V_H	TH3
16	F_M	C_L	E_V_L	TH2
17	F_M	C_L	E_L	TH3
...				
35	F_H	C_L	E_V_H	TH4
36	F_H	C_M	E_V_L	TH3
37	F_H	C_M	E_L	TH3

...				
43	F_H	C_H	E_M	TH4
44	F_H	C_H	E_H	TH5
45	F_H	C_H	E_V_H	TH5

Table 1:-Fuzzy Rules for Proposed Scheme

Table 1 shows some of the fuzzy rules for the proposed scheme. A total of 45 rules are used in the proposed fuzzy system. In addition, there are 3 inputs for fuzzification, and the Mamdani model and center of gravity are used for defuzzification [12-13]. The Inference Engine outputs a new security threshold value considering the 45 rules in Table 1, False Traffic Ratio, Compromised Key Ratio, and Residual Energy. When the attack rate, i.e., the ratio of the damaged key, is low and the amount of residual energy is small, a small security threshold value is selected that can reduce the report delivery cost while providing minimum-security power.

Experimental results:-

In this section, the CFFS and proposed scheme are experimentally analyzed in terms of the energy management and detection rate. The Network Area for the Experiment is set to 1,000 x 1,000 m^2 and 3000 nodes are randomly deployed. 100 nodes among these are randomly chosen for CH nodes and 10 nodes are chosen as compromised nodes. The Mica2 node is considered for the proposed experiment [14]. 16.25μJ and 12.5μJ of energy are consumed while transmitting and receiving a byte, respectively. Every member nodes consume 15μJ and 75μJ for MAC generation and report validation, respectively. The node's routing path is established with directed diffusion and GPSR during the node distribution phase [15-16]. The sizes of the report and MAC are 24 and 1 bytes, respectively.

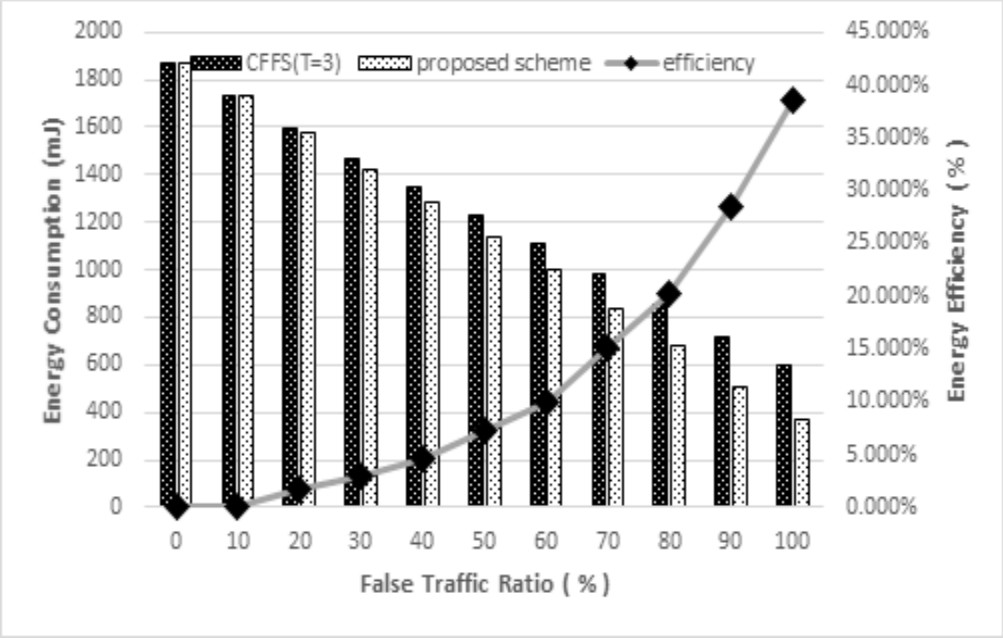

Figure 5:-Energy Consumption and Efficiency versus FTR

The performance comparison between the existing scheme and the proposed scheme is shown in Figure 5. We generated 5000 events at random locations and analyzed the energy consumption of the nodes. When the false report rate is 0%, the fuzzy system does not operate and therefore shows the same energy consumption as the existing CFFS. However, starting from when the false report injection attack occurs, the detection rate is improved by adjusting the security threshold value to the cluster range in the proposed method. The following is the experimental results of the energy consumption according to the attack rate. The proposed method improves the energy efficiency by 11.717% on average compared to the original CFFS.

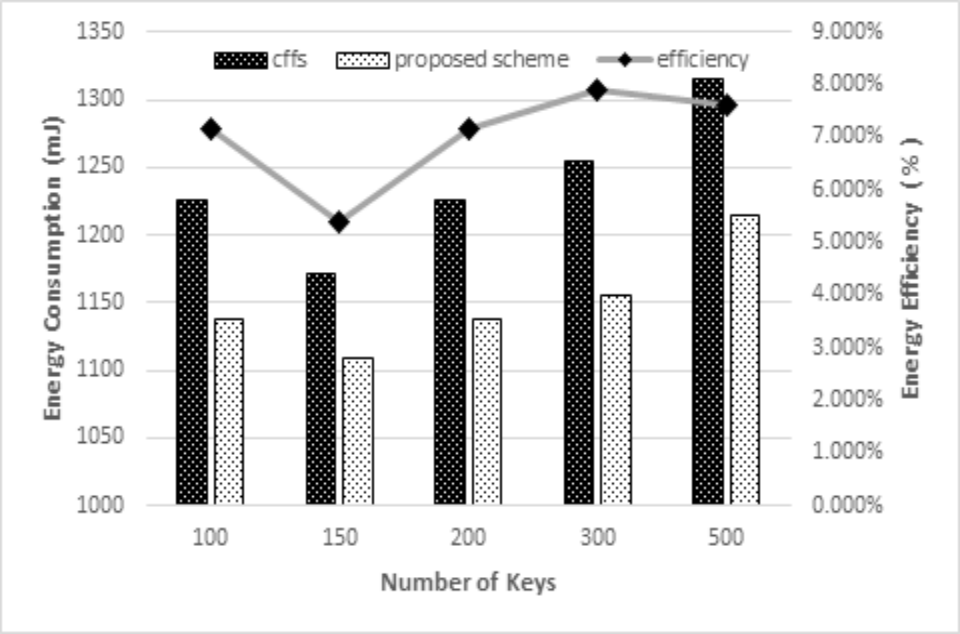

Figure 6:-Energy Consumption and Efficiency versus Number of Keys

Figure 6 shows the energy consumption and its efficiency according to the number of distributed keys at a 50% attack ratio. The amount of energy consumption increases while the number of distributed keys increases. However, the proposed scheme shows better performance than the existing scheme. Experiments on energy consumption according to the number of keys showed that the average energy efficiency increased by 7.045%.

Conclusion:-

Zhixiong et al. proposed CFFS to prevent false report injection attacks. In CFFS, nodes are configured on a cluster basis to verify reports. The attack ratio may be different from each cluster. Therefore, for efficient-energy management, a method of constructing a dynamic threshold value for each cluster is needed. This paper proposes an adaptive security threshold setting method by applying fuzzy logic according to the cluster environment for CFFS. In the proposed method, different security boundaries are set for each cluster to maintain proper security and show efficient energy management.

Acknowledgement:-

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

References:-

1. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.
2. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).
3. Akkaya, Kemal, and Mohamed Younis. "A survey on routing protocols for wireless sensor networks." Ad hoc networks 3.3 (2005): 325-349.
4. Nayak, Padmalaya, R. Sri Uma Suseela, and Veena Trivedi. "A review on DoS attack for WSN: Defense and detection mechanisms." *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*. IEEE, 2017.
5. Akyildiz, Ian F., et al. "Wireless sensor networks: a survey." Computer networks 38.4 (2002): 393-422
6. 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.
7. 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.

8. 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.
9. Nam, Su Man, and Tae Ho Cho. "Context-aware architecture for probabilistic voting-based filtering scheme in sensor networks." *IEEE Transactions on Mobile Computing* 16.10 (2017): 2751-2763.
10. Yashavanth, T. R., Ravi S. Malashetty, and C. R. Rashmi. "A Bandwidth-Efficient Cooperative Authentication and an En-route Filtering Scheme for Filtering Injected False Data in Wireless Sensor Networks." *International Journal of Advanced Computer Research (IJACR)*: 2277-7970.
11. Liu, Zhixiong, et al. "A Cluster-Based False Data Filtering Scheme in Wireless Sensor Networks." *Adhoc & Sensor Wireless Networks* 23 (2014).
12. Babuška, Robert. Fuzzy systems, modeling and identification. Technical Report, 1997.
13. Mamdani, Ebrahim H. "Application of fuzzy algorithms for control of simple dynamic plant." Proceedings of the institution of electrical engineers. Vol. 121. No. 12. IET, 1974.
14. https://www.eol.ucar.edu/isf/facilities/isa/internal/CrossBow/DataSheets/mica2.pdf
15. Intanagonwiwat, Chalermek, Ramesh Govindan, and Deborah Estrin. "Directed diffusion: A scalable and robust communication paradigm for sensor networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.
16. Karp, Brad, and Hsiang-Tsung Kung. "GPSR: Greedy perimeter stateless routing for wireless networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.