Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/6294
DOI URL: http://dx.doi.org/10.21474/IJAR01/6294

***RESEARCH ARTICLE***

# ENERGY CONSUMPTION ANALYSIS OF WSN’S VARIOUS ENVIRONMENT FOR ADEQUATE KEY-REDISTRIBUTION IN DEF.

**Jungsub Ahn[1] and *Taeho Cho[2].**
1. College of information and communication engineering, sungkyunkwan university, republic of korea.
2. College of software, sungkyunkwan university, republic of korea.

## Manuscript Info

*Manuscript History*

Received: 12 November 2017
Final Accepted: 14 December 2017
Published: January 2018

***Key words:-***
WSN Security Network Communication Dynamic En-route Filtering False Report Injection Attack Energy Management.

## Abstract

Increasing energy efficiency in wireless sensor networks is important because it is related to network lifetime. The sensor nodes are deployed in open environment, it causes threat like captured the sensor node. An attacker is possible to generate a false report using a compromised node and inject an attack on the network. False report injection attack causes fatal damage like false alarms, energy depletion, and other loss to users at the wireless sensor networks. To solve this problem Yu and Guan proposed dynamic en-route filtering scheme. It method detects and filters false reports early. Also, research has been conducted to increase energy efficiency through key-redistribution based on Dynamic en-route Filtering. In this paper, we analyze the average energy consumption of wireless sensor networks various environment for adequate key redistribution. The Experimental results show up to 32.75% energy efficiency improvement.

## Introduction:-

The Wireless Sensor Network(WSN) consists of hundreds to thousands of low-cost sensor nodes and several Base Station node(BS), Which are used for industrial, medical, and military purpose to monitoring of the target field in real time [1]. The BS is interface for managing sensor nodes. Each sensor node has event detection capability, and the BS node collects report of detected event. A BS node verifies reports and transmit to user event alarm. A sensor node composed of a processor, a memory, a power supply, and a wireless transmitter [2]. Wireless sensor nodes have limited processing capability, memory, and battery Due to their limited production cost [3]. Nodes can form a cluster topology for efficient energy management [4]. In WSN, nodes are vulnerable to network security attacks because its are deployed open environments [5]. As shown in Figure 1, an attacker can manipulate a report by compromising and exposed node or generate a false report directly. In addition, the attacker can obtain the control capability of the node and inject the false report generated by the attacker into the network as shown in the following figure 1.

**Corresponding Author:- Jungsub ahn.**
Address:- College of information and communication engineering, sungkyunkwan university, republic of korea.

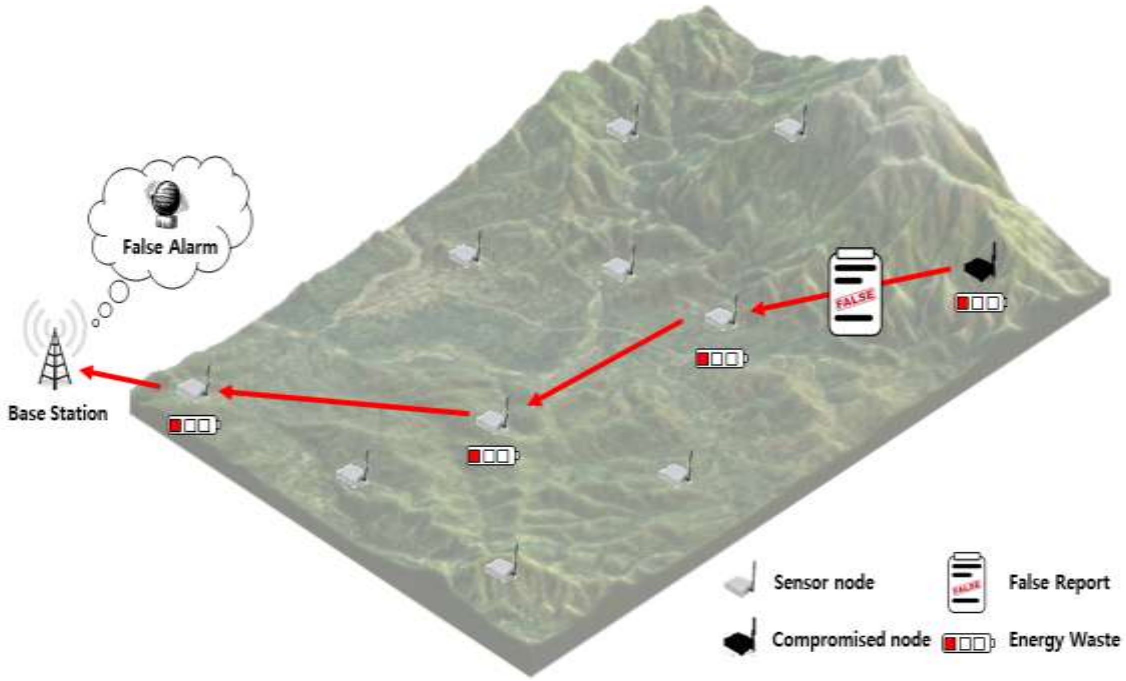

**Figure 1:-** False report injection attack

When a false report reaches the BS, it informs the user of a false alarm and exhausts the limited energy of the node. If This attack is repeated, it confuses the user. Furthermore, it causes energy depletion of node energy that means a fatal network corruption like disable the cluster or event collection. Therefore, false report should be detected and filtered early and intermediate nodes need to reject the corrupted node. Network protocols to validate reports have been studied [6-9]. One of the schemes is Dynamic En-route Filtering(DEF) proposed by Yu and Guan [10]. DEF can detect false reports using authentication key and secret key. Also, a key redistribution method using DEF has been proposed [11]. But it is not efficiency. In order to increase the energy efficiency, it is necessary to change parameters appropriately according to the environment. In this paper, we analyze the power consumption according to the environment to find the appropriate key redistribution cycle for each situation. Through this paper, it is expected that untrained network administrators can select proper key redistribution cycle in each situation and it will help to develop intelligent key redistribution algorithm in the future. In particular, it will be helpful to optimize the fuzzy function in order to determine efficient key redistribution cycle using fuzzy in the future research topic.

The rest of this paper is as follows. We introduce DEF scheme including key redistribution in Section 2 and then describes the simulation environment Section 3. Section 4 analyzes the simulation results. Finally, We discusses conclusions and future research in Section 5.

## Related Works:-

### Dynamic En-route Filtering:-

Yu and Guan proposed the DEF scheme to protect false report injection attack using authentication keys and secret keys in sensor networks. This scheme can be applied to a network for a dynamically changing topology. In addition, It has an energy efficiency advantage over other WSN security protocols in changing the environment. As seen in Figure 2, the DEF consists of three phases: key pre-deployment, key post-deployment, and report filtering.

In the first phase of key Pre-deployment, the BS distributes a distinct seed key to nodes, and nodes can generate a sequence of authentication keys consist hash-chain. This phase is executed only once at the BS. The auth-key is calculated as follows:

$$k^{v_{i_{m-1}}} = h(k^{v_{i_m}})$$

$$k^{v_{i_{m-2}}} = h(k^{v_{i_{m-1}}}) = h^2(k^{v_{i_m}})$$

$$\dots$$

$$k^{v_{i_1}} = h^{m-1}(k^{v_{i_m}})$$

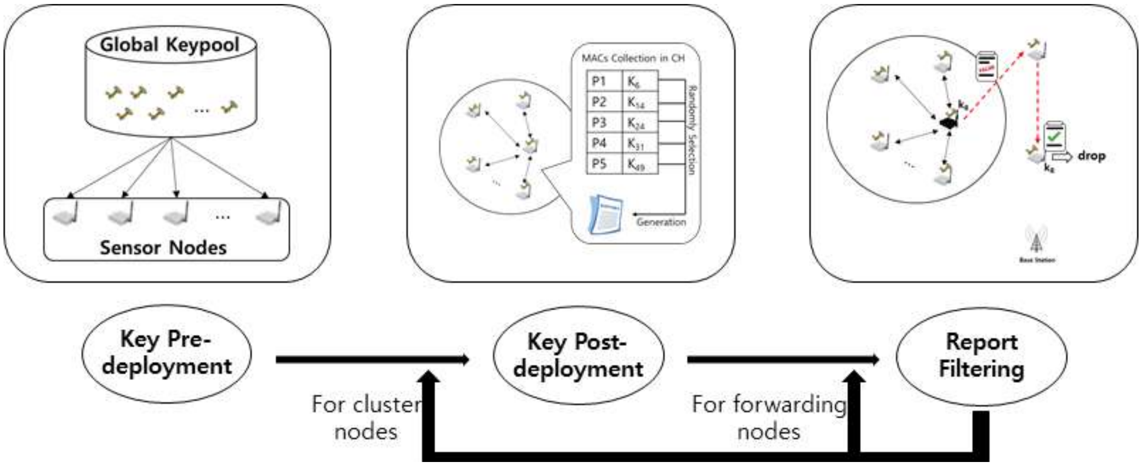

**Figure 2:-** 3-phases for DEF scheme

$v_i$ means the index of the node, and the $k^{vi}{}_1$ mean the first key used. Also, it loads $l$+1 secret keys randomly selected in the y-key pool of v size. In the second phase of post-deployment, the nodes that are divided into member nodes in the cluster encrypt the auth-message using one of its secret keys. It then sends auth-message to the CH node. Thus, compromised nodes make it difficult to disguised as a CH node. The auth-message is as follows:

$$Auth(v_i)=\{v_i,j_i,id(y_1{}^{vi}),\{id(y_1{}^{vi}),k_j{}^{vi}\},\\ ..., id(y_l{}^{vi}),\{id(y_l{}^{vi}),k_{ji}{}^{v1}\}y_l{}^{vi},\\ id(z^{vi}),(id(z^{vi}),k_{ji}{}^{vi})z^{vi}\}$$

where $j_i$ is the index of the authentication. If $j_i$ = 1 means the first dissemination. $id(y_1{}^{vi})$ means the index of $y_1{}^{vi}$ in the y-key pool. $\{.\}y_l{}^{vi}$ means to the encryption operation using $y_l{}^{vi}$. The CH nodes spread the encrypted authentication key that received from the member node to the forwarding nodes. This process is repeated by the number of hops determined by the user. When the forwarding node receives the authentication key, it checks whether it has the same secret key. If the node has the same key, decrypt and store the authentication key. In the third phase of report filtering, the forwarding nodes validate the reports and detect and filtered false reports. When an event occurs, the CH collects the MAC containing the event information from the member node and merge the MACs into the report through a pre-established security threshold value. A high security threshold has the advantage of increasing detection rates, but it has the disadvantage of consuming higher power because it has a higher report size [12]. The generated report is transmitted to the BS through the forwarding nodes. This process is repeated until the report arrives at the BS or is discarded.

**Motivation:-**

Park proposed a key re-distribution scheme to reduce unnecessary energy consumption when an attacker continuously attacks a false report injection attack in DEF. In the proposed scheme, the key redistribution step improves the energy problem by reducing the number of hops where false reports are detected [11]. The network administrator must know the network condition well for applying that scheme. If untrained network administrators set up an improper key redistribution cycle, energy management problems may arise. As described above, the energy management of nodes in WSNs is an important issue.

**Simulation Environments:-**

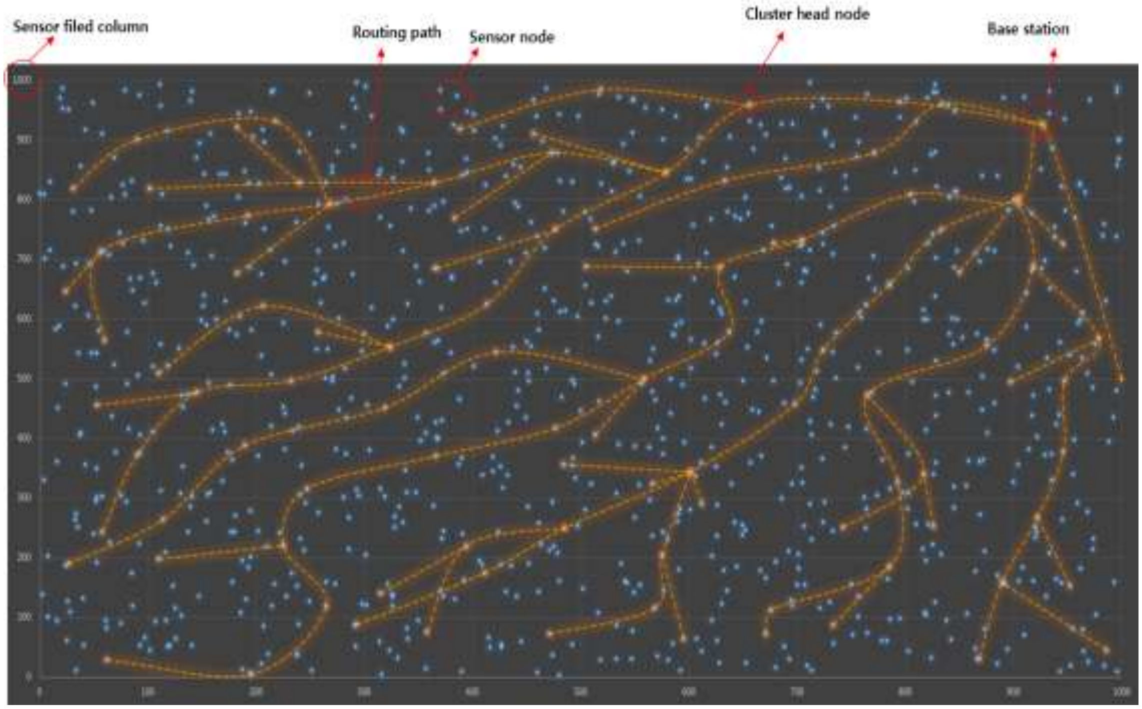

**Figure 3:-** Virtual sensor field

We randomly placed 100 CHs in a field of size 1000m✕1000m for simulation. A sensing node is arbitrarily arrange d within one cluster range. It is assumed that each node consumes 16.25 μJ per byte as transmission energy and 12.5 μJ per byte as receiving energy [13]. The size of one MAC to be added for report verification is 1 byte and the transmission message size is 24 bytes. Each node is randomly loaded with one z-key and four y-keys from 100 full key sets before deployment. Events occurred randomly within the field and generated a total of 1000 events.

## Experimental results:-

We have analyzed the power consumption according to the environment through various possible situations. The threshold value refers to the key redistribution period.

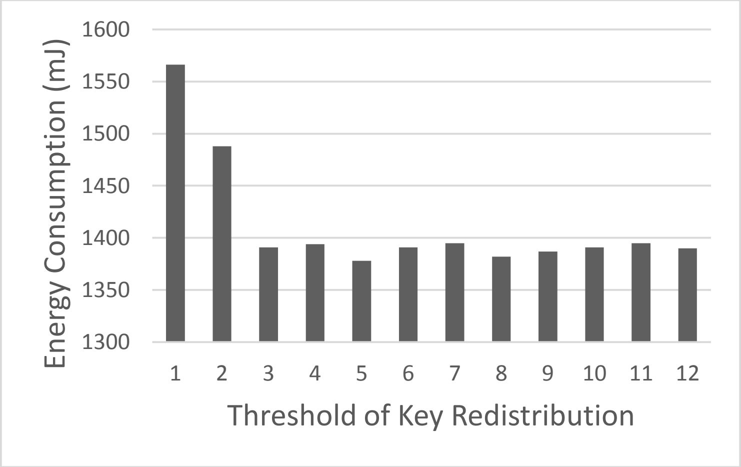

**Figure 4:-** Energy Consumption for 10% Attack Ratio

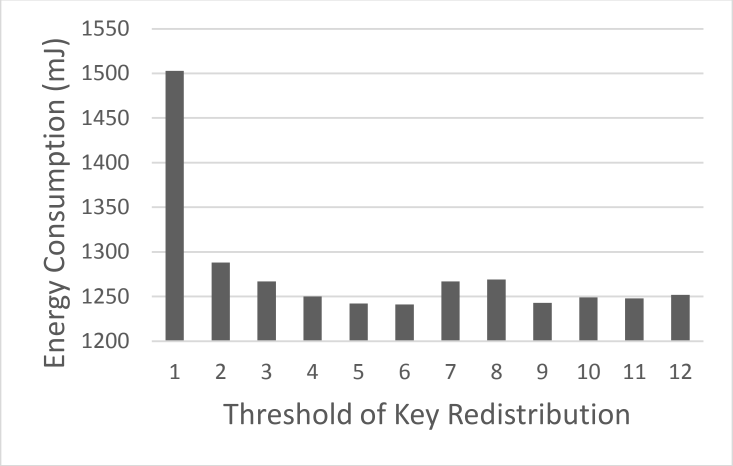

**Figure 5:-** Energy Consumption for 30% Attack Ratio

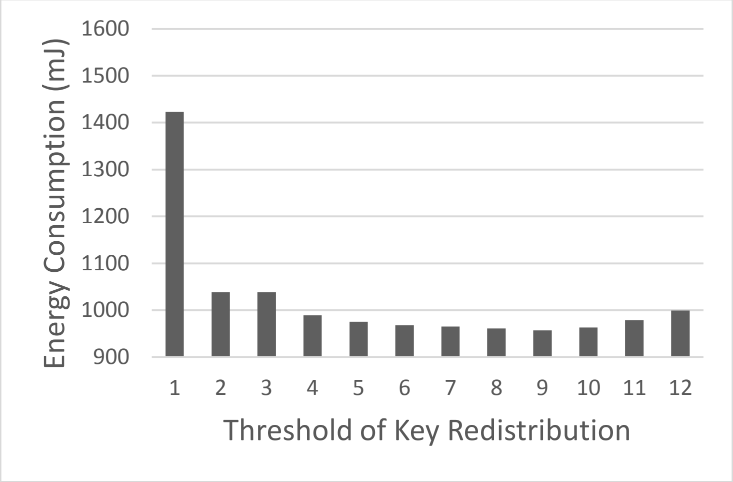

**Figure 6:-** Energy Consumption for 50% Attack Ratio

Figure 4–6 shows the Energy consumption of the networks when the attack ratio is 10%, 30% and 50%. Experimental results show that energy consumption is high when the threshold is set to one in the overall experiment. Because the redistribution of the key to the node occurs immediately after the detection of the attack, which increases the cost of maintaining the network. As seem the above figures, by selecting appropriate thresholds for the situation, we can see better results in terms of energy efficiency and security strength than existing method. Especially, it is possible to evaluate and modify the decision value of the whole cycle through the analyzed result. Therefore, even if a specific threshold value is initially set, an appropriate threshold value is selected through the network environment, we can expect better results.

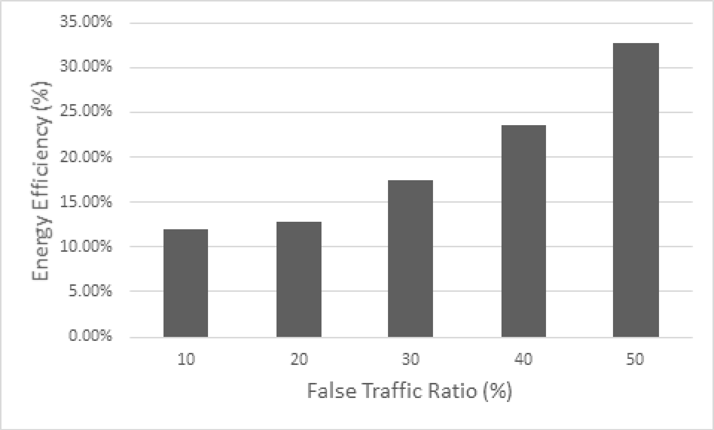

**Figure 7:-** Energy Efficiency versus FTR

Figure 7 shows energy efficiency based on False Traffic Ratio(FTR) when an optimal key redistribution threshold is set. As can be seen from the figure, the higher the FTR have the better the energy efficiency. The reason is the higher the FTR, the higher the key redistribution count. If the key redistribution threshold is small, the key energy replacement cost is high during the same experiment time. Conversely, if the key redistribution threshold is large, the key redistribution does not occur and adversely affects the filtering. Therefore, it is important to set an effective threshold value for the environment because it can save energy.

## Conclusion:-

In WSN, sensor nodes are exposed and vulnerable to false report injection attack. In order to detect false reports early, Yu and Guan proposed DEF. Also, a key redistribution method in DEF has been studied. However, an appropriate threshold value should be selected for the environment for efficiently operate that method. In this paper, we analyze power consumption according to various environment for efficient key redistribution. This result shows that energy savings up to 32.75% depending on the attack rate. This conclusion expects that future research will help develop intelligent adaptive fuzzy techniques.

## 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. Yassen, Muneer Bani, Shadi Aljawaerneh, and Reema Abdulraziq. "Secure low energy adaptive clustering hierarchal based on internet of things for wireless sensor network (WSN): Survey." Engineering & MIS (ICEMIS), International Conference on. IEEE, 2016.
2. Haas, Christian, and Joachim Wilke. "Energy evaluations in wireless sensor networks: a reality check." Proceedings of the 14th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems. ACM, 2011.
3. Karray, Fatma, et al. "A review on wireless sensor node architectures." Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC), 2014 9th International Symposium on. IEEE, 2014.
4. Vlajic, Natalija, and David Xia. "Wireless sensor networks: to cluster or not to cluster?." Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks. IEEE Computer Society, 2006.
5. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).
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. Lu, Rongxing, et al. "BECAN: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks." IEEE transactions on parallel and distributed systems 23.1 (2012): 32-43.
10. Yu, Zhen, and Yong Guan. "A dynamic en-route scheme for filtering false data injection in wireless sensor networks." Proceedings of the 3rd international conference on Embedded networked sensor systems. ACM, 2005.
11. Park and Cho. “Key Re-distribution Scheme of Dynamic Filtering Utilizing Attack Information for Improving Energy Efficiency in WSNs.” Korean Institute of Intelligent Systems 26.2 (2016): 113-119
12. Jung-Sub Ahn and Tae-Ho Cho. "PREVENTION METHOD OF FALSE REPORT GENERATION IN CLUSTER HEADS FOR DYNAMIC EN-ROUTE FILTERING OF WIRELESS SENSOR NETWORKS."
13. Kramer, Marc, and Alexander Geraldy. "Energy measurements for micaz node." University of Kaiserslautern, Kaiserslautern, Germany, Technical Report KrGe06 (2006).