Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/6000
DOI URL: http://dx.doi.org/10.21474/IJAR01/6000

RESEARCH ARTICLE

LOAD BALANCING MANAGEMENT USING EVALUATION FUNCTION TO IMPROVE THE REPORT TRANSFER SUCCESS RATE.

Sang Hyeok Lim[1] and *Tae Ho 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: 08 October 2017
Final Accepted: 10 November 2017
Published: December 2017

Key words:-
Wireless sensor networks
Network security
PVFS
False Report Attack
False Vote injection Attack.

Abstract

A wireless sensor network (WSN) consists of multiple sensor nodes and base stations that collect information from sensors deployed over a wide range. The existence of nodes that are randomly distributed in an open environment (which are difficult to manage individually) is a disadvantage because the nodes can be easily found and compromised by an attacker. An attacker can execute a false report insert attack or an invalid vote insert attack through a compromised node. The Probabilistic Voting Filtering Scheme (PVFS) is a scheme that prevents these two types of attacks. The proposed method probabilistically selects a validation node, determines the validity of the report, and filters the report based on the thresholds that have been set. Because of the characteristics of PVFS, which show weaknesses in both the individual management of sensor nodes responsible for event reception and probabilistic security and the management of random routing in the WSN, it is necessary to manage the lifetimes of individual nodes. The proposed scheme increases the network lifetime and event detection and transmission rates of the overall WSN by varying the role of the node via an evaluation function, which evaluates the energy state of the node. Experimental results showed that the event transmission success rate was improved up to 13.45% from threshold value 2, the threshold value is variable used in the evaluation function.

Introduction:-

WSNs are composed of many sensor nodes and a base station (BS). When an event occurs, the sensor node detects the event and reports this event over multiple hops of the sensor nodes to the BS [1]. These WSNs are used for data collection and event detection in various fields such as home networks, military systems, and forest fire monitoring [2].

Corresponding Author:- Sang Hyeok Lim.
Address:- College of Information and Communication Engineering, Sungkyunkwan University, Republic of Korea.

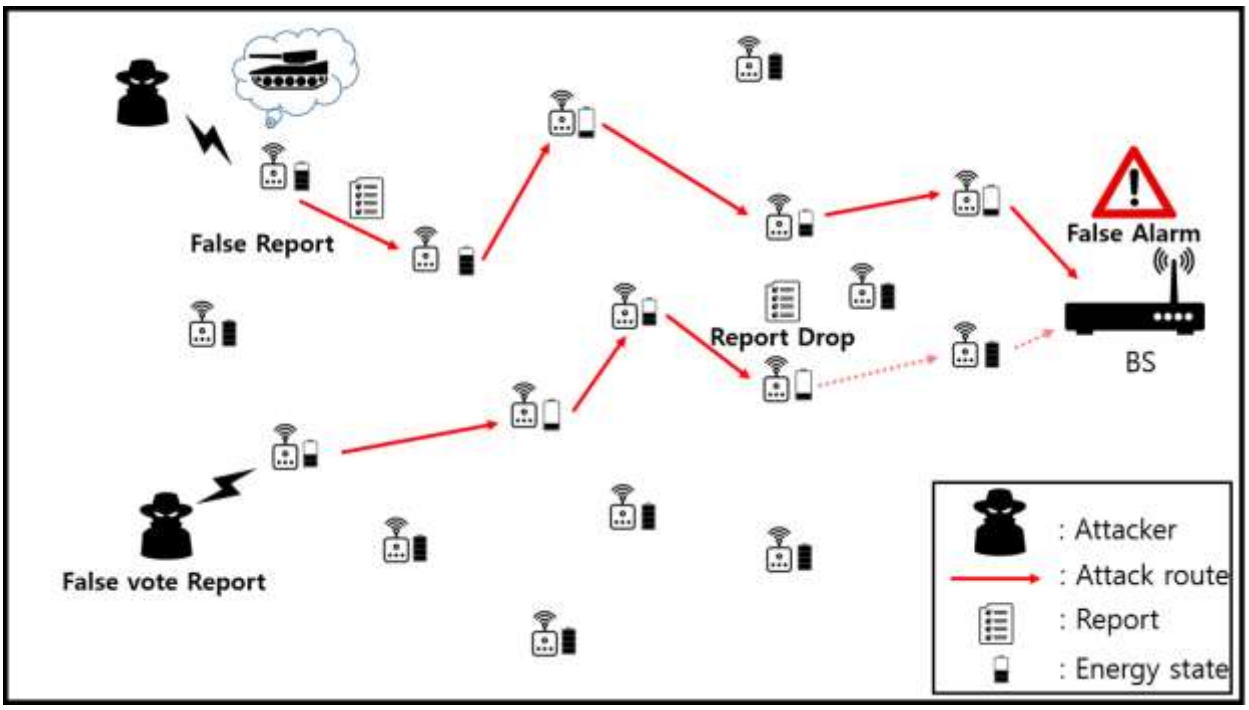

Fig. 1:- False report and false vote injection attacks.

However, sensor nodes are vulnerable to attack because of the disadvantages of limited computation, limited energy, random distribution in an open environment that operates independently, and difficulties in individual management [3],[4]. Attackers exploit these vulnerabilities to attack WSNs by injecting reports containing false information or injecting false Message Authentication Codes (MACs). Figures 1 shows a schematic of these attacks. Li and Wu proposed a probabilistic voting-based filtering scheme (PVFS) [5] to prevent such attacks.

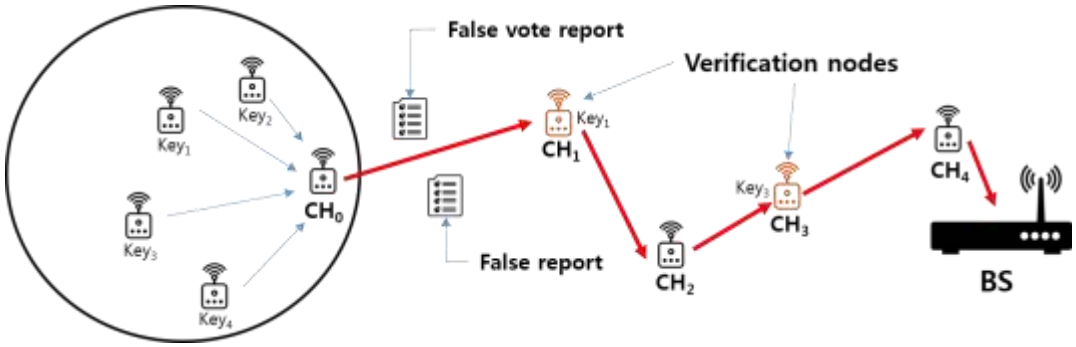

Fig. 2:- Report send & verification process.

In PVFS, all nodes constitute a network that exploits cluster-based organization. When a cluster head (CH) recognizes an event, it generates a report of that event. It then sends this report to the member nodes. Next, the member nodes judge the authenticity of the report and generate their own MACs, alternatively referred to as votes in PVFS. The CH randomly selects votes and inserts them into the report. Validation nodes on the path use MAC and threshold values to defend against these attacks.

Related Works:-

False report injection attack:-

A false report injection attack is one that sends a report about a non-existent event through the compromised sensor node [6], [7]. Such an attack occurs mainly in the CH but can also occur in member nodes. The goal of this attack is to exhaust the energy resources of the nodes on the propagation path and generate a false alarm at the BS. Dynamin En-routing Filtering Scheme (DEF), Statistical En-route Filtering Scheme (SEF), Commutative Cipher Based En-

route Filtering (CCEF), Interleaved Hop-by-Hop Authentication Scheme for Filtering (IHA), and Bandwidth-Efficient Cooperative Authentication Scheme (BECAN) are examples of defense schemes against false report attacks [8], [9], [10], [11], [12]. An attacker can attempt a false report injection attack and false vote injection attack through the compromised member node. A PVFS based defense protocol against that kind of attack is proposed [13].

False vote injection attack:-

The false vote injection attack refers to injecting false votes into legitimate reports that are generated from an event-detecting CH. This is an attack in which the validation node judges the report as a false report and intends to prevent it from reaching the BS. The report is mainly generated from captured member nodes. PVFS is the only protocol that has been applied in the application layer to deal with both of these attacks.

PVFS:-

To cope with false report injection and false vote injection attacks in WSNs, the proposed PVFS uses a true threshold value (Tt) and a false threshold value (Tf) to detect and filter false reports and false vote injection reports with validation nodes. PVFS has three phases: a key distribution phase, a report generation phase, and a verification phase.

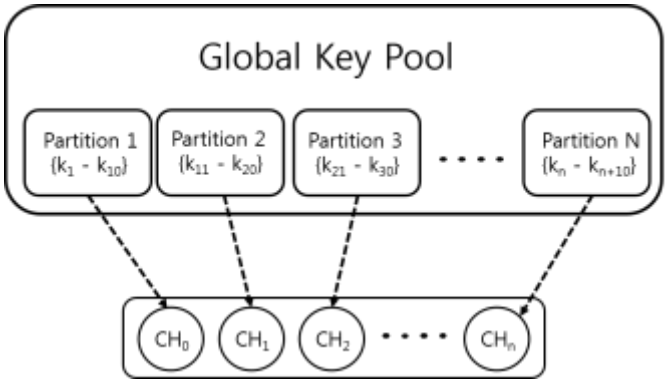

Fig. 3:- Key distribution process.

Figure 3 shows the key allocation step in which the BS divides the key pool into N partitions and delivers them to each CH. Each partition contains L keys. The CH uses one of the keys in the partition as its own key and distributes the remaining L-1 keys to the member nodes. A key is allocated to the member nodes according to the partition of the key pool. With this process, every node gets a single key from a global key pool.

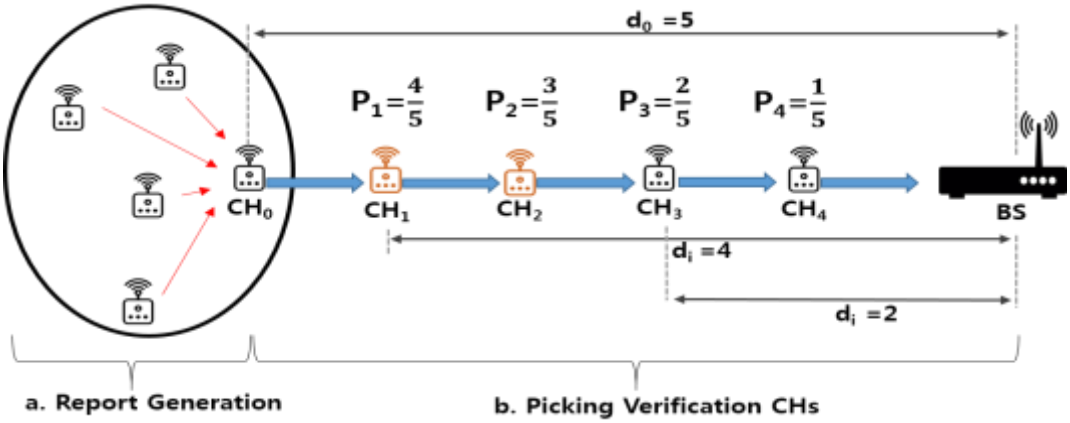

Fig. 4:- Report generation and verification node selection processes.

Figure 4 shows the report generation and validation node selection process. In the initial network configuration, nodes are divided into cluster units and the CHs responsible for report generation are selected for each cluster. When an event occurs, the cluster closest to the event area wins the chance to generate a report of that event. CH generates a report and broadcasts it to member nodes of its cluster. The member nodes confirm this, and if the report is judged

to be a normal report, the MAC created by its own key is transmitted to the CH. CH extracts a predetermined number of MACs received from the member nodes and adds them to the report. The node selected as the verification node stores the keys of the member nodes of the event occurrence cluster one by one. In the report verification process, the verifying nodes compare their own keys with the keys in the report. If they have the same key, they determine the MAC of the report. If the MAC value generated by the same key is different, the vote is regarded as false, and Tf is increased. In the filtering process, if the false count reaches the threshold value, the report is judged to be false and is immediately dropped. If the true count value reaches the threshold value, the report is considered legitimate and is sent to the BS without further validation. The verification node selection process is shown in Fig. 4-b. The verification nodes among the CHs are probabilistically selected to verify the report. The probability 'p' uses the distance d_0 which is the hopcount from the BS to the event cluster and the distance d_i between the BS and CH_i. The closer the CHs are to the event cluster, the higher the probability of verification. The probability of the report being authenticated in a small number of hops is high.

Proposed Scheme:-

Motivation:-

In an environment where a WSN is installed, there are many areas where the user cannot distribute nodes directly and the nodes are scattered randomly. Therefore, there is a high possibility that a good routing path based on energy efficiency and characteristics of PVFS is not generated every time. One of the main purposes of the WSN is to gather information about events that occur in vast areas where it is difficult for a user to directly reach and respond appropriately. The main purpose of the WSN could not be achieved if event reception at the deployed node failed to reach the BS, or if the energy of the node is depleted so that event detection in the corresponding region is not possible. Also, if the residual energy of the sensor nodes is high but the events to be delivered are not properly transmitted, the sensor nodes distributed in those areas become useless. Therefore, it is important to improve the event detection rate and report delivery success rate even if the total energy consumption of the WSN increases by modifying the node to be available for multiple purposes. Since PVFS has probabilistic security, there is a tendency to show extremely high and low performance in random routing environments. Therefore, it is important to use nodes efficiently in the WSN by adjusting the role of nodes appropriately and raising the event detection rate.

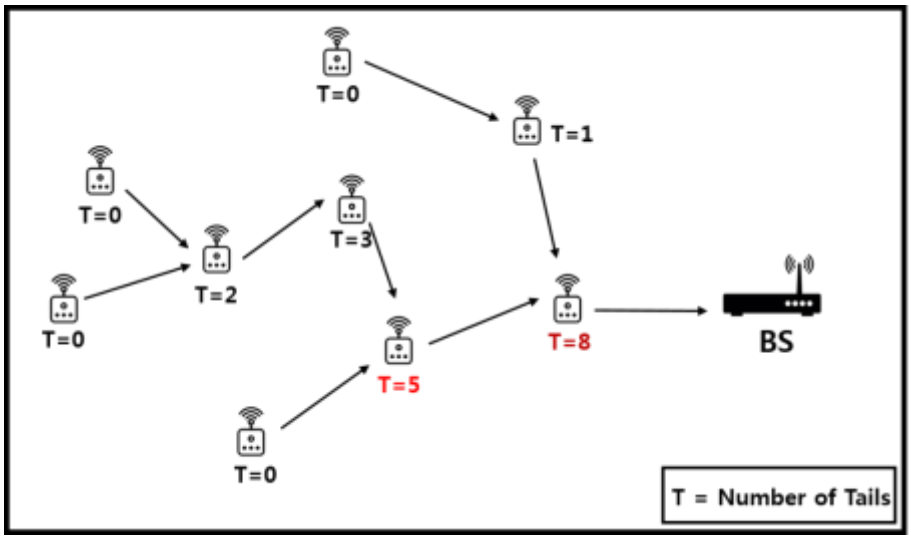

Fig. 5:- Calculating tail number.

Figure 5 shows the part of the field where the WSN is configured. As shown in the figure, CHs that detect the event have limited communication distances, so they need to cooperate with other nodes to deliver the report to the BS through hop movement. Therefore, the number of downstream nodes is large since it is close to the BS. Tail refers to the number of CH nodes that use the node to forward detected events. If the CH is positioned at the end of the field, the tail value of the corresponding node is zero. A node with many tails can consume a large amount of energy for sending, receiving, and verifying the report, which plays an important role in transferring events occurring in other regions. If such a node dies, the event detection node must forward the report through the new path except for that node, and the event detected in the area where the dead node was receiving is no longer detectable. Therefore, by applying every CHs an evaluation function that takes into account the total number of nodes, the number of events,

the number of tails, and the probability 'p' that the corresponding node's probability of being selected as a verification node. The node whose output of it exceeds the threshold value is selected as a 'warning node'. This warning node is tagged on to only acts as event detection and report generation instead of acting as a forwarding node or verification node.

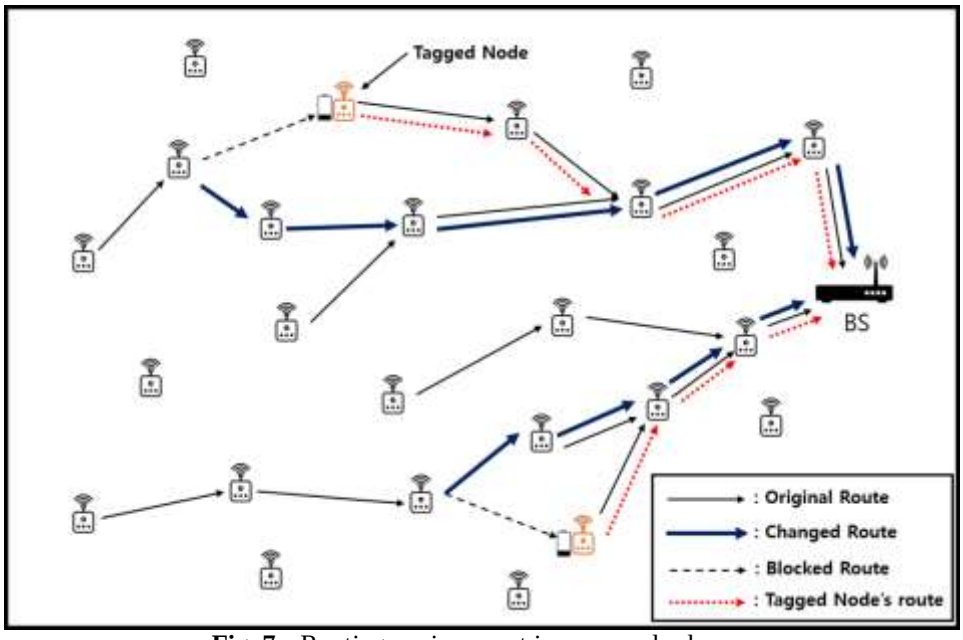

Fig. 7:- Routing environment in proposed scheme.

Figure7 shows an example of the network on a field using the proposed method. Every CH has a list of the IDs of the nodes that are closer to the BS within its communication range. This list is used for the formation of new routing except for the nodes selected by the tagging node among the list members. Nodes with depleted energy are dropped from the list and the tagged nodes remain in the list but are excluded from the routing priority. If all the nodes in the list are tagged, the node closest to the BS is forcibly routed again. The proposed method selects nodes to perform a tag operation through an evaluation function. The node tagged by the evaluation function on the original route requests the previous route node to set up new routing, and the tagged node performs only event detection and report generation during the remaining period. The upstream node selects the 0-ranked node in the routing list and sends the event detected by itself and the events detected by the tail nodes to the BS through the corresponding routing. If the output value of the function is less than the user defined threshold value, the tagging is immediately performed. The threshold value is selected according to the characteristics of the user. The number of surviving nodes and the amount of event generation are updated in each cycle, and the output value of the evaluation function is determined in this way.

Evaluation functions:-

The evaluation function of i-th node E_{tag}^{i} is expressed as the sum of α, β and γ, which are the amount of energy used during the role of the forwarding node, the amount of energy consumed during the role of the event detection node and the energy used by the verification node to report transmission after event detection, respectively. α is given by $\alpha = e_t * \frac{N_{evt}}{N_n}$, where e_t is the transmitting cost, N_n is the number of nodes in the field and N_{evt} is the number of events. β is given by $\beta = T * (e_t + e_r) * \left(\frac{N_{evt}}{N_n}\right)$, where e_r denotes the receiving cost and T is the i-th CH's tail node. γ is more complicated, and can be expressed as the sum of probabilities that the i-th node is a verification node of each tail node, all times the probability of having the same key when it is a verification node. The sum of probabilities that a node is a verification node of the tail nodes is given by $e_{cal} * \sum_{j=1}^{n} P_i^j$, where $P_i^j = \frac{HopCount_{N_j}}{HopCount_{N_i}}$ and e_{cal} denotes calculating cost. Then, the sum of probabilities of each node is $P_i^1 + p_i^2 + \cdots + P_i^T = \frac{1}{HopCount_{N_i}} * \sum_{j=1}^{T} HopCount_{N_j}$. When the node performs verifying, the probability that the key of the corresponding node

overlaps with the key of the report is $\frac{S}{L}$, where s is the number of votes in the report and L denotes the number of member nodes from each tail nodes. Therefore, the evaluation function is as follows:

$$E_{tag}^{i} = e_t * \frac{N_{evt}}{N_n} + T * (e_t + e_r) * \left(\frac{N_{evt}}{N_n}\right) + \frac{S}{L} e_{cal} * \frac{1}{HopCount_{N_i}} * \sum_{j=1}^{T} HopCount_{N_j}. \quad (1)$$

During the event in the WSN, the node selected as the warning node through the evaluation function selects whether to switch to the event detection node through the secondary evaluation function when its energy falls below the threshold value. The secondary evaluation function is as follows:

$E_{LowEnergy}^{i}$ = α ∗ (100 − Event progress) + α ∗ C. (2)

Event progress (2) refers to the ratio of the current event progress in the whole cycle. When C is the expected number of event reception times, C can be configured to suit the user's preference. If the value of C is set too high, tagging is performed even if the energy is sufficient, resulting in an adverse effect of long routing in the entire network. This increases the number of hops that is delivered, dramatically reducing the network lifetime. Therefore, it is necessary to set an appropriate evaluation function (1).

Experimental results:-

Assumptions:-

Events occur randomly throughout the region. Due to the nature of random routing, there may be nodes that do not form routing in the initial node placement stage. The cycle uses the unit time, not the number of events. The BS counts all the events and attacks that have occurred and selects new evaluation functions based on these numbers.

Experimental environment:

Table 1:- Experiment parameters

Item	Value
Sensor field size	1500 × 1500
Number of sensor nodes	5000
Number of cluster head nodes	500
S L Packet size	5 10 24
Transmission range	150

Experiments were conducted assuming that the attack rates were 0, 30, 50, and 70%. The reason a 100% attack rate is excluded from experiments is that this experiment is an experiment that evaluates the failure rate of a normal report. The transmission and reception costs are set to 16.25μj and 12.5μj, respectively, and the calculated cost of voting was set to 15μj [14].

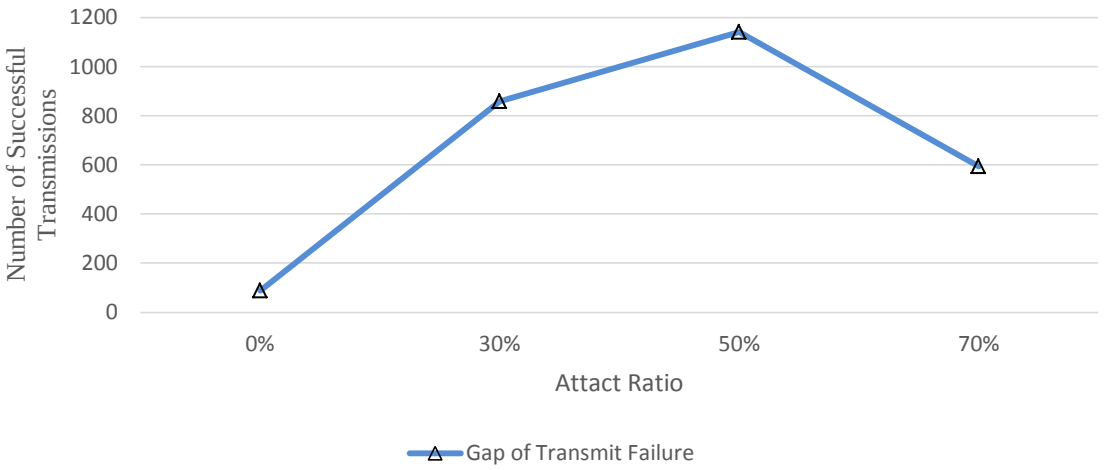

Fig. 8:- Difference in number of successful transmission according to attack rate

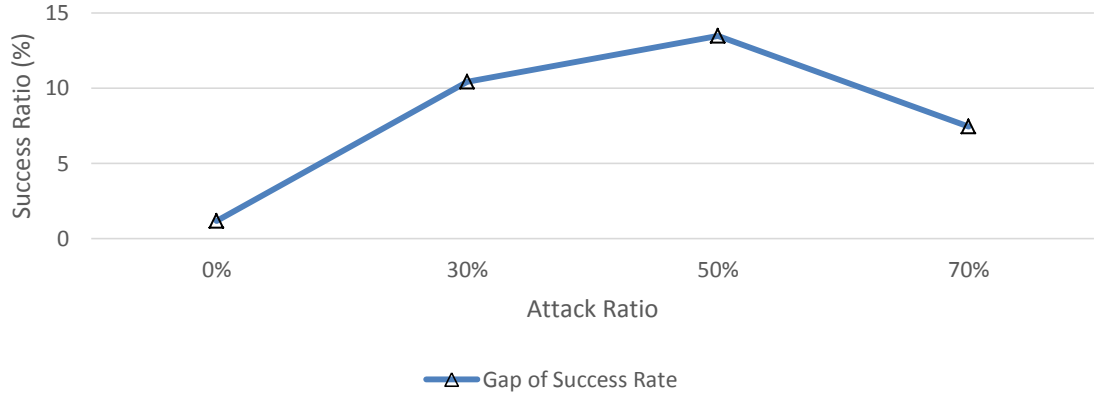

Fig. 9:- Difference in transmission success rate according to attack rate

Figures 8 and 9 show the difference between the number of successful reports and the success rate in the PVFS and the proposed scheme when the event occurrence number is 500 to 4000. These results show that the proposed method has the greatest effect when the attack rate is between 30% and 50%. At the 70% attack rate, most of the reports are false reports and normal reports being sent rarely occurs, so the performance difference between the proposed scheme and PVFS is not significant. When the attack rate is 0%, all the reports are normal reports. Therefore, it is interpreted that the routing change through the proposed scheme does not play a big role because it is an environment in which the routing does not need to be changed. Similarly, the role of the node in situations where attacks do not occur is also not significant.

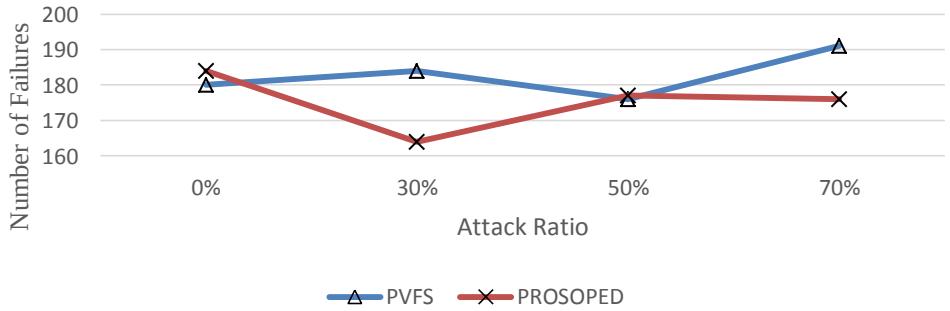

Fig. 10:- Number of transmission failures when C = 1

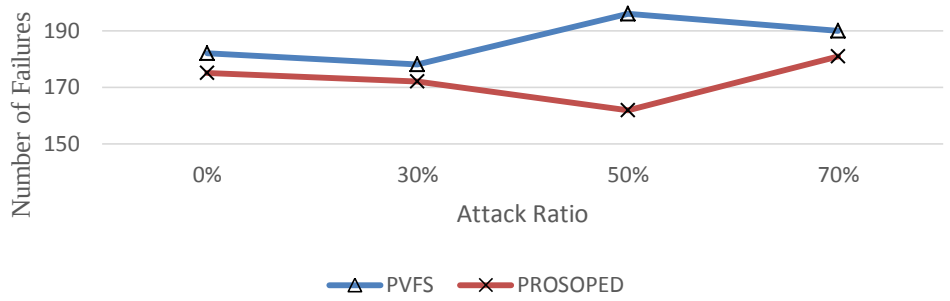

Fig. 11:- Number of transmission failures when C = 2

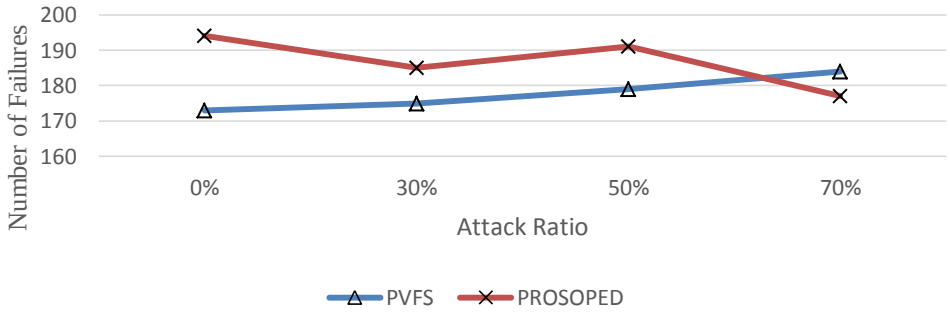

Fig. 12:- Number of transmission failures when C = 3

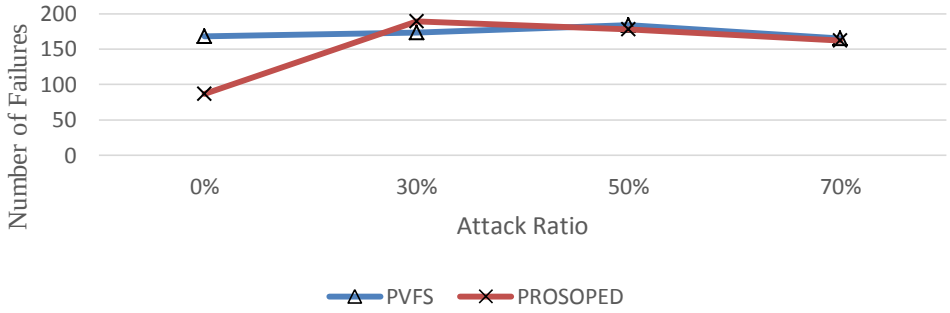

Fig. 13:- Number of transmission failures when C = 4

Figures 10 – 13 shows the number of event transmission failures of PVFS and the proposed method according to C when 1000 events occur. As C increases from the proper value, the difference in the report failure rate between the proposed scheme and the original PVFS may be decreased or increased (on average). If the C value is small and the attack rate is 0%, the performance differences were poor. It can be seen that if an evaluation function sets a threshold C that is too large, this increases the failure rate of the report transmission.

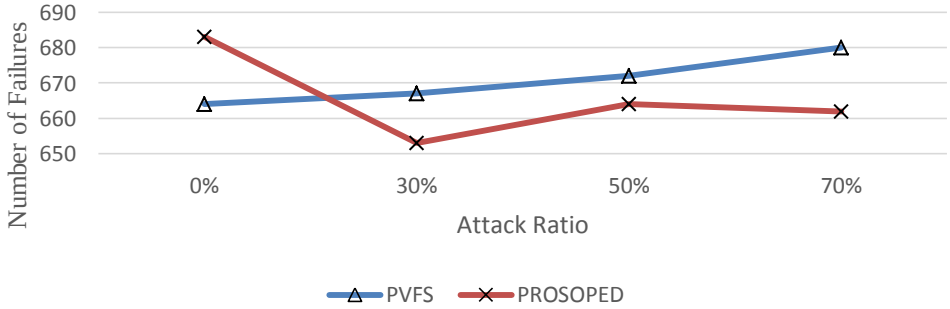

Fig. 14:- Number of transmission failures when C = 1

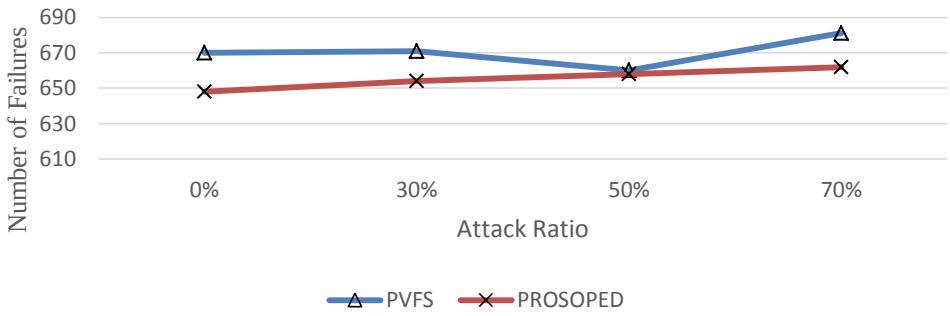

Fig. 15:- Number of transmission failures when C = 2

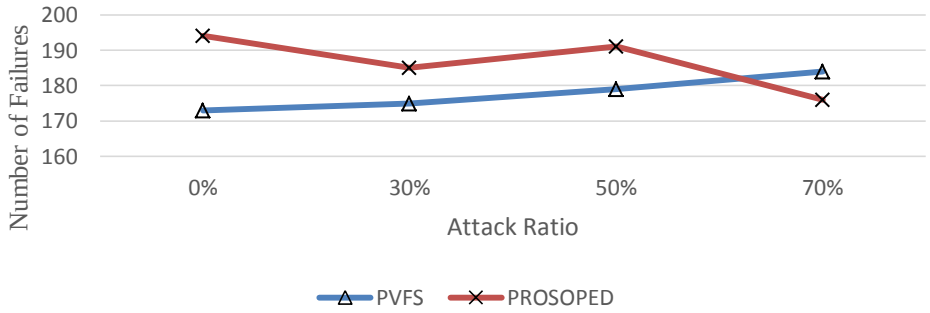

Fig. 16:- Number of transmission failures when C = 3

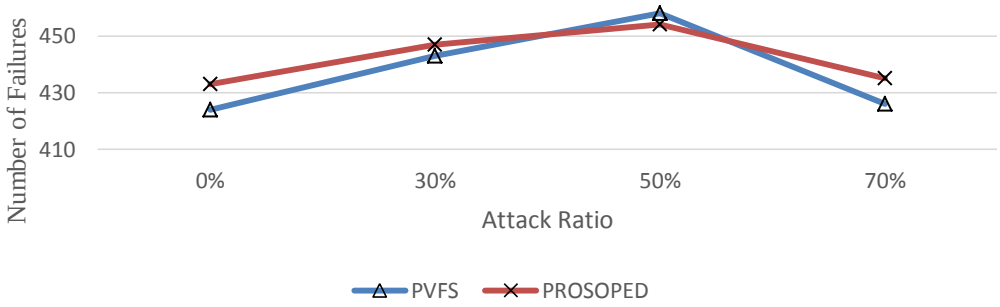

Fig. 17:- Number of transmission failures when C = 4

Figures 14 – 17 show the number of event transmission failures of PVFS and the proposed method according to the C value when 1500 events occur. Although the number of events is a bit different, the resulting graphs and the performance difference between 1000 and 1500 events are found to be similar. In addition, the gap between the proposed method and the failure rate of report deliveries in PVFS does not differ greatly depending on the number of events. This is because the evaluation function reflects the number of events and the number of nodes on the field, thus appropriately corresponding to the number of events in all cases.

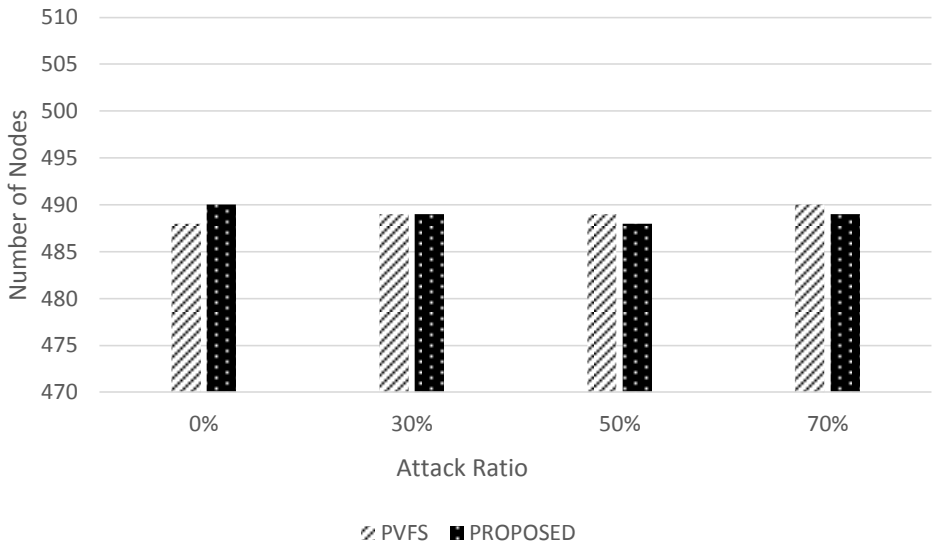

Fig. 18:- The number of surviving nodes.

At the end of the cycle, the gap between the number of surviving nodes is not huge. The reason for this can be explained in relation to graph 1. In the proposed technique, the node that changed the role of the node during the event process actually has a small amount of residual energy. Therefore, after one or two events are detected, energy is depleted and the node dies. This is the main purpose of the WSN, i.e., to improve the report transfer success rate regardless of the number of surviving nodes. The remaining energy or high survival rate of the node no longer affects network performance when the network usage is high or when the node has to be replaced.

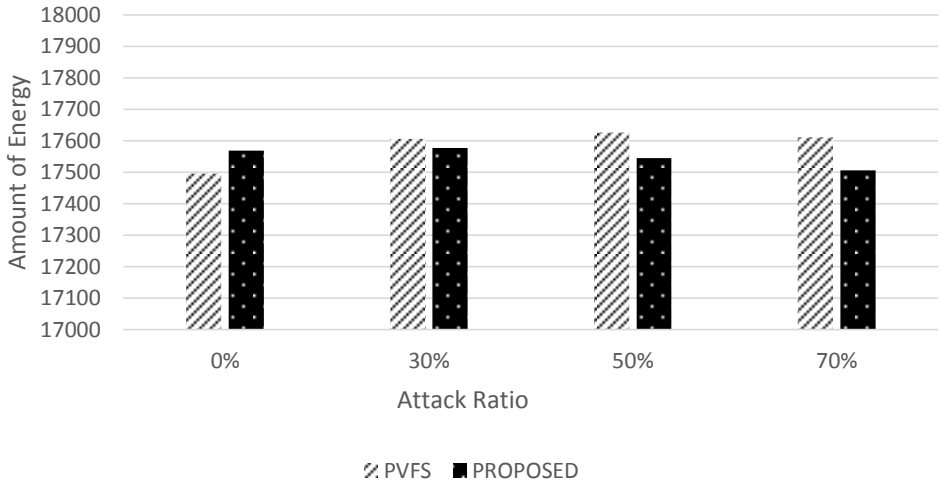

Fig. 19:- Average Residual Energy Size

The average residual energy magnitude on the graph is measured only for surviving nodes, not all sensor nodes in the field. The number of surviving nodes for a proposed scheme is similar to the original PVFS in the previous experiment. This graph shows that the residual energy is also about the same or slightly lower when the proposed scheme is adopted. This means an efficient distribution of energy is achieved. In PVFS, the energy consumed by the surviving node is relatively low because the event occurring in the area to be detected by the dead node was not transmitted through the other node. However, in the proposed scheme, the event detection and transmission success rates are higher than that of PVFS, which shows that the efficient energy distribution has enabled the network to operate on a line where all nodes have reached the end of their life.

Conclusions and Future Works:-

In the proposed method, we experimentally confirmed that a WSN's event detection success rate, report transmission success rate, and overall network lifetime are increased by organically changing the roles of the nodes through evaluation functions that evaluate the node status. Through experimentation, it was found that an inappropriate evaluation function increases the routing cost of the WSN, increasing the hop count of the nodes towards the BS. These cause bottlenecks in the forwarding node. Experimentation also shows that an inappropriate evaluation function shortens the lifetime of the network and also reduces the event delivery rate. In the future, we will develop a more intelligent system that reflects local event generation variances by experimenting with changing the node roles using more accurate evaluation functions by considering the attack rate and event frequency in the evaluation function or by loading fuzzy logic to modify the node itself to do voluntary role replacement.

Acknowledgements:-

This research was supported by the MISP(Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW)(2015-0-00914) supervised by the IITP(Institute for Information & communications Technology Promotion)"(2015-0-00914)

References:-

1. Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47.6 (2004): 53-57.
2. Zhang, Wensheng, and Guohong Cao. "Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach." INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. Vol. 1. IEEE, 2005.
3. Al-Karaki, Jamal N., and Ahmed E. Kamal. "Routing techniques in wireless sensor networks: a survey." IEEE wireless communications 11.6 (2004): 6-28.
4. Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47.6.
5. 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.
6. Jeba, S. A., and B. Paramasivan. "False data injection attack and its countermeasures in wireless sensor networks." European Journal of Scientific Research 82.2 (2012): 248-257.
7. Jeba, S. A., and B. Paramasivan. "An evaluation of en-route filtering schemes on wireless sensor networks." International Journal of Computer Engineering & Technology (IJCET) 3 (2012): 62-73
8. Yu, Zhen, and Yong Guan. "A dynamic en-route scheme for filtering false data injection in wireless sensor networks." SenSys. Vol. 5. 2005.
9. 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.
10. 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.
11. Yang, Hao, and Songwu Lu. "Commutative cipher based en-route filtering in wireless sensor networks." Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. Vol. 2. IEEE, 2004.
12. 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.
13. Sang-hyeok Lim and Tae-ho Cho. Report Verification Technique for Improvement of the Energy Efficiency in a Probabilistic Voting-based Filtering Scheme of WSNs. *International Journal of Computer Applications* 171(3):21-25, August 2017.
14. Sastry, C. K. N., & Wagner, D. (2003). TinySec: Security for TinyOS.