Indonesian Journal of Electrical Engineering and Computer Science
Vol. 11, No. 1, July 2018, pp. 284~293
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v11.i1.pp284-293

A Secure Data Aggregation Technique for Wireless Sensor Networks Using Iterative Filtering

Jyothi R[1], Nagaraj G Cholli[2]
[1]Research Scholar, Assistant Professor, Dept of CSE, GAT, Bengaluru, India
[2]Associate Professor, Department of ISE, R.V.College of Engineering, Bengaluru, India

Article Info

Article history:

Received Jul 2, 2017
Revised Jan 12, 2018
Accepted Apr 18, 2018

Keywords:

Cryptographic algorithm
Data aggregation
Iterative filtering
Security
Wireless sensor network

ABSTRACT

Wireless sensor systems are accumulation of sensor hubs which send the detected information to sink hub. As sensor hubs are constrained to computational power and vitality asset, a vitality proficient usage of assets are basic keeping in mind the end goal to utilize organize for longer length. Hence data traffic inside network and large amount of data sending to base station need to be reduced. The main goal of data aggregation is to enhance the network life time by gathering an aggregate data in an energy efficient manner. Iterative Filtering algorithm are more reliable and efficient compared to existing method and it provides the way for aggregating the data at secure level and data trustworthiness. In order to strengthen security levels at cluster head cryptographic algorithm such as RSA algorithm is used to encrypt the aggregated data by using public key and decrypt data at base station by using its own private key. Where this method is responsible for securing the information that is aggregated at cluster head and also secures the information passed through the networks. The simulation results shows that proposed method consumes less computation time, data transmitting, high security and has a good storage capacity than compared to existing algorithm.

Corresponding Author:

Jyothi R,
Research Scholar, Assistant Professor, Dept of CSE, GAT, Bengaluru, India
Email: jyothir.gat @gmail

1. INTRODUCTION

1.1. Background

Wireless sensor network is a distributed network and it is comprised of a large number of distributed, self-directed, tiny and low powered devices called sensor nodes. Sensor nodes are limited to computational power and energy resources. Lifetime of sensor nodes are short because of low battery powered and lower communication range. Examples of WSN are flood detection, environmental monitoring and army surveillance, accident report, health care. WSN continuously collects data and send it to sink i.e. Base station. Due to limited lifetime of sensor developing WSN faces a number of challenges. WSN have many issues that consumption, security, calibration, localization, Development, synchronization etc. out of which security and energy consumption are major issues of sensors.The process of gathering and aggregating the data is known as data aggregation and its main goal is to enhance the lifetime of nodes in a network. Data aggregation is a process of aggregating data sensed by sensor nodes using function such as max, min, and average and then transmits the aggregated data to base station. By these algorithm sensor nodes consumes less power to transmit data.

Data aggregation reduces the energy consumption by eliminating redundancy[1]. Sensor nodes are battery limited hence to save energy and resources are the most potential element.Some of the significant performance measures of data aggregation algorithm are network lifetime, data accuracy and latency[2,3].

1.2. Problem

As wireless sensor networks are used in remote and hostile environment in order to transfer sensitive information. Therefore security becomes major issues in WSN. Hence a suitable security mechanism need to be designed to prevent the compromised node from altering aggregated.

In WSN communication takes up most of the sensors energy because sensor nodes are limited to battery powered and energy resources. In WSN sensor nodes are going to be deployed in most critical environment in order to transfer sensitive information to destination node. Simple data aggregation is more vulnerable to node compromising attacks, where compromised nodes inject false data to nodes and alters the final original data. And this simple method degrades the performance of nodes and lack in accuracy.

1.3. Proposed Solution

Hence an Iterative filtering algorithms are attractive option in WNS because it eliminates both the problems such as data aggregation and data trustworthiness using single iterative method but simple traditional security approach are not suitable to achieve end to end confidentiality and privacy[4,5]. To address all this security issues we propose an improvement to iterativefiltering method by applying a suitable security mechanism.

In the Figure 1 data aggregation happens at cluster head where cluster head is chosen one among the sensor nodes in network. Cluster head transmit the aggregated data to base station which in turn reduce redundancy and consumes less energy[6,7].

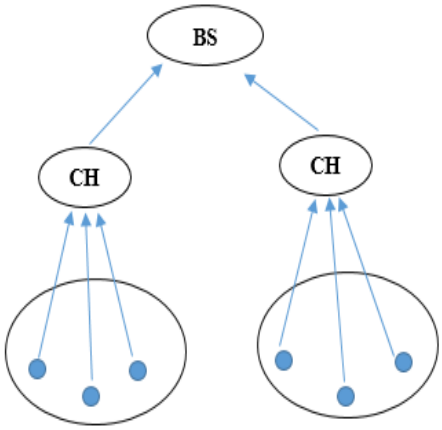

Figure 1. Cluster Based Data Aggregation.

Traditionally sensor nodes send data to base station whenever base station requests for network. But through this type of method energy consumption will be high. In order to increase node lifetime cluster based data aggregation is used.

2. TECHNIQUES USED

2.1. Data Aggregation

2.1.1. Importanceof Aggregation

Aggregator function figure out the readings from sensor nodes. Following requirements need to be applicable for computing the aggregate functions. (1) Individual sensor nodes data has to be protected with the privacy. (2) Minimum number of messages has to be transmitted within the network because data aggregation process needs to minimal. (3) Maintain the exact accuracy of the data aggregation result[8]. It's an effective approach to aggregate the data at cluster head for optimal making use of the resources like bandwidth and energy in WSN.Data aggregation framework shown in the below Figure 2.

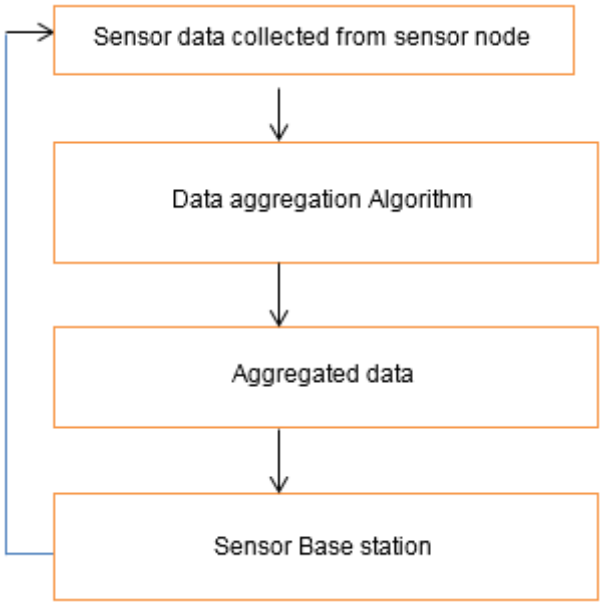

Figure 2. Data Aggregation Algorithm Framework

2.1.2. Cluster Approach

In wireless sensor networks sensor nodes are not capable for sending the data directly to the base station in such cases, make use of a cluster approach is acceptable. In this elegant type of method divides the whole network into number of grouped clusters. Each cluster group is having the own Cluster Head. Aggregation of all the data has to be taken care by the head of the cluster and it will transmit the result of the aggregation to base station. The cluster head can directly communicate with the base station through other cluster head.

3. PROJECT DESCRIPTION

Secure data aggregation is the process of securing the aggregated content at the cluster head level. Basically the data which is sensed from the sensor nodes are transferred between the nodes and then we are applying the iterative filtering algorithm to find out the malicious nodes among the cluster nodes. After finding out the malicious nodes data which we have received from that particular node will be blocked and then processed with the secure data. Till now it's the first phase of our project, in this paper we are going to provide the one more level of security to the aggregated data at the cluster head.Initially sensors nodes having the error, sensors can be modeled by using Gaussian variable to estimate the bias. Bias estimation is the first step of the finding out the malicious node. Based on the estimated bias value define and compute the matrices to estimate the variance value. Estimated bias value is subtracted from the sensor readings, using MLE method reputation vector estimated. The sensor nodes having the non-zero MLE value will be the malicious node in our approach.

4. RESEARCH METHOD

4.1. Iterative Filtering

Iterative Filtering algorithm is an attractive solution for WSN because it solves both problems aggregation of data and data trustworthiness using a single procedure.This kind of trustworthiness estimation is based on the distance of the readings from the sensor. Aggregation is usually a weighted average; sensors whose readings most differ from such estimation are assigned to be a less trustworthiness.

4.1.1. Bias Sstimation

In this approach Bias estimation will be the first step of finding out the malicious nodes. Initially sensors read the data around that is taken as $S_{i.}$ Gaussian distribution variable value will be considered as $E_{i.}$ By Adding the actual value of the sensor S_i with the Gaussian distribution variable $E_{i,}$ we will get a value to

be considered as $X_{i.}$ If an attacker include the invalid data that will be considered as a value $A_{i.}$ Consider the below explanation

$$X_i = S_i + E_i \quad (1)$$

If an attacker include the invalid data that will be considered as A_i

$$F_i = X_i + A_i \quad (2)$$

F_i is the bias value we have calculated from the sensor data.
We have implemented this simple approach to find out the malicious nodes.

Bias value = F_i

4.1.2. Variance Estimation

We can now obtain an estimation based on the bias value which we have calculated. For finding out the variance value we have a simple approach, subtracting the bias value F_i with Gaussian distribution random variable E_i will get a variance value.

$$FF_i = F_i - E_i \quad (3)$$

Variance = FF_i

4.1.3. MLE Estimation

In the previous sections, we proposed an approach for estimating the bias and variance value for based on their readings. Maximum likelihood estimation is based on the variance value and the actual reading of the sensor which is denoted as S_i in the previous section.

MLE = FF_i - S_i

Here $FF_i$is the variance value we obtain in the previous section and S_i is the initial reading of the sensor node, as this is the simple approach we have implemented in this paper. After subtraction we will get the MLE value correspondence to the variance.

Non-zero MLE value indicates that there's an injection of invalid data in the network;we mark that node as a Malicious node in the network. MLE value zero indicates that there's no malicious activity in the network. Aggregator node takes the data from all these secure nodes then itsaggregate and passed to the sink node.

4.2. System Architecture

The important necessary reason for data aggregation is to acquire and aggregate the data in effective manner to utilize the resources. Iterating Filtering plays the major role in the aggregation of data in WSN.IF, simultaneously aggregate data from different cluster members and evaluation of these data is based on the weight factor assigned to each sensor in the network.

The architecture diagram for the proposed system is shown in Figure 3. After the node deployment sensor nodes reads data around the network. Data which comes through the sensor nodes need to be aggregated at the cluster head. As we implemented the Iterative filtering at the next level to find out the malicious nodes across the cluster members. Once we eliminate the invalid data through Iterative filtering secure data has to be transferred to Base station. If any error occurs while filtering operation, first estimate the errors and calculate the variance of data with MLE and then transmit the aggregated data to Base station[9,10].

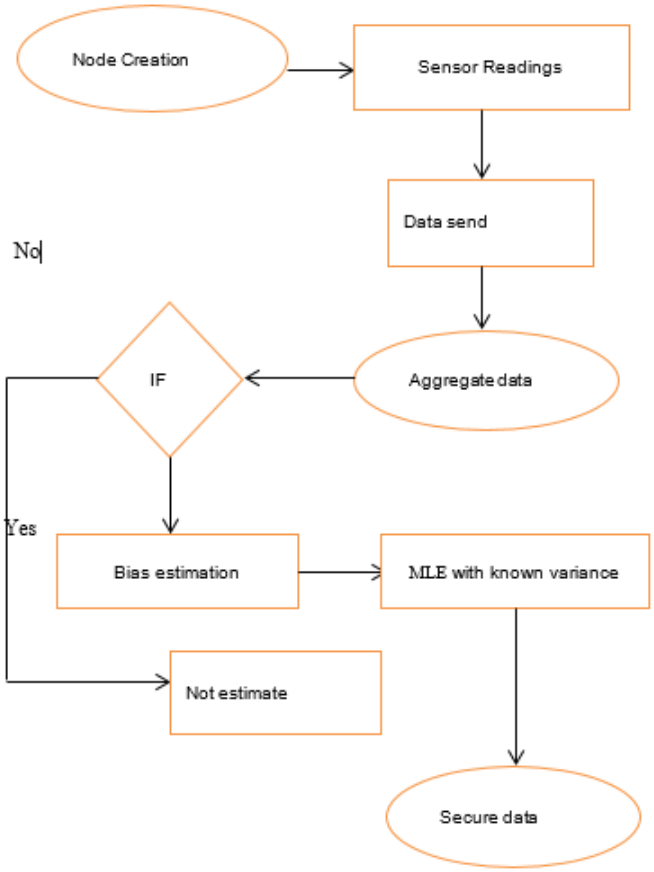

Figure 3. System Architecture.

5. IMPLEMENTATION

We have make use of the Network simulator-2 platform for implementing this Project. Nodes get deployed in the environment based on the approximation given by the authors. Cluster formation takes vital role in the WSN; cluster is the combination of the different nodes. Where each cluster is having the cluster head that has to be chosen based on the residual energy of the node. Basically cluster head is always having the highest energy among all other cluster members because it has to be taken care of aggregation of the data.

Figure 4 shows the implementation framework of secure data aggregation. Initially nodes are scattered and then it's deployed in the environment. These sensor nodes are formed to create the cluster, each cluster will have the cluster head. Crucial part of the project is started over after the cluster formation, calculation of Bias and variance with MLE will be happen based on the equation that we have derived in the previous section. Detection of malicious nodes and aggregating the data at the cluster head has to be undergone after the values reveled by those equations.

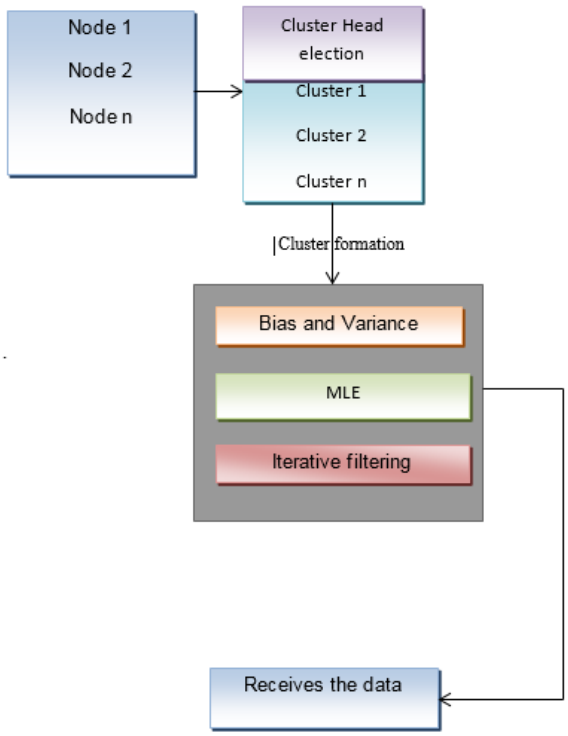

Figure 4. Implementation Framework

6. RESULTS AND DISCUSSIONS

The nodes are grouped together to form the cluster. Each Cluster group is having the Cluster head. 40 is the node denoted as a base station. Figure 5 represents the initial nodes creation in the network.

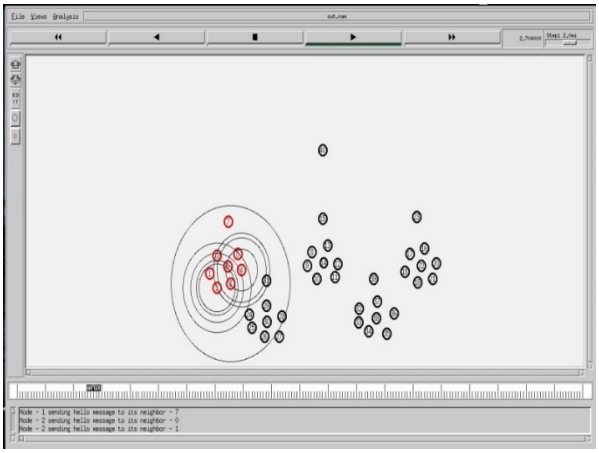

Figure 5. Initial Node Creation in the network

Figure 6 shows the data aggregation process in wireless sensor networks. Data gathered from the cluster members are aggregated at the cluster head and then transferred between the other clusters to transfer directly to the base station. Data which is transferred to the base station is the secure data, iterative filtering is executed before aggregating the data.

Figure 6. Data Aggregation

Figure 7 shows the malicious node detection in the network. Node 2, 0, 5 are malicious nodes detected through our iterative filtering operation. Once we find out the misbehavior node data from those nodes will not be considered for aggregation. Cluster head aggregates the data which taken only by the secure no.

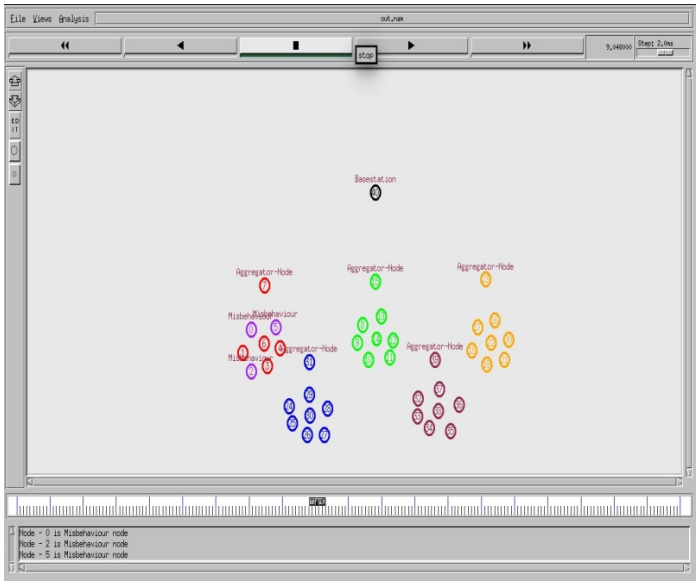

Figure 7. Malicious Node Detection

Figure 8 shows the secure transmission of the aggregated data to the base station 40. After filtering out the invalid data at the cluster head aggregated data has to be transferred between the cluster heads to send the data directly to the base station.

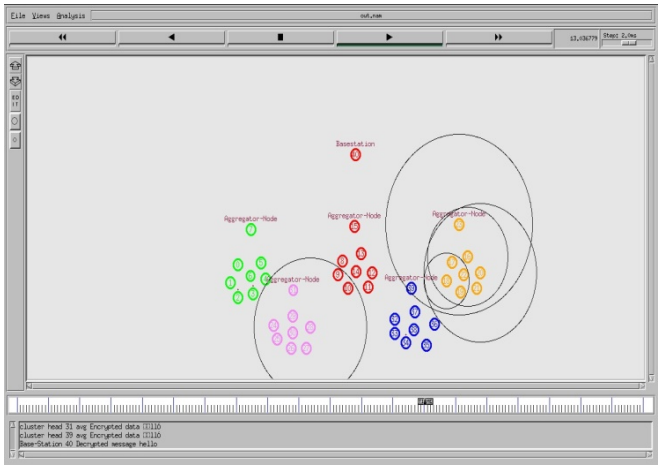

Figure 8. Secure Transmission to Base Station

Figure 9 represents the comparison of delay with the existing system. This graph is obtained by executing our system. Compare to the existing system delay gets reduced. Data is completely secured and transmitted even if delay gets reduced.

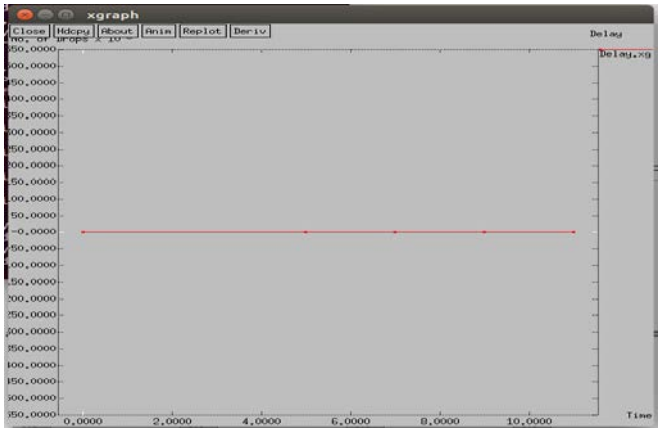

Figure 9. Delay Comparison

Figure 10 shows the robust aggregate affine and Figure 11 shows the RMS error. These graphs are obtained by executing this experiment. This result shows that proposed iterative filtering technique improves the efficiency of the algorithm by reducing the error data transmission to the base station and through number of iterations.

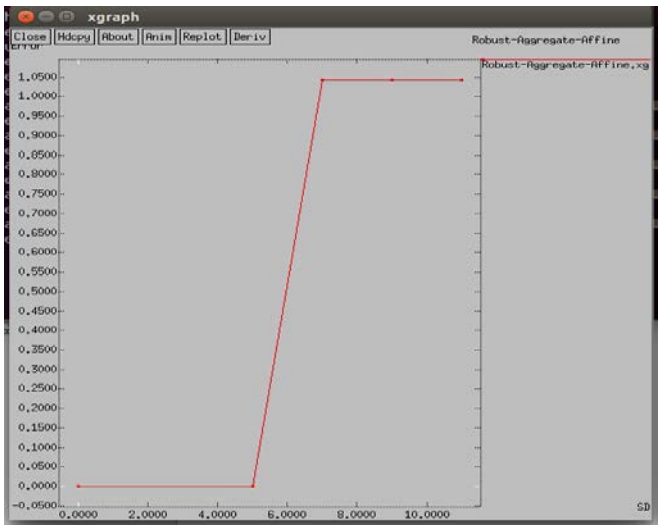

Figure 10. Robust-Aggregate-Affine

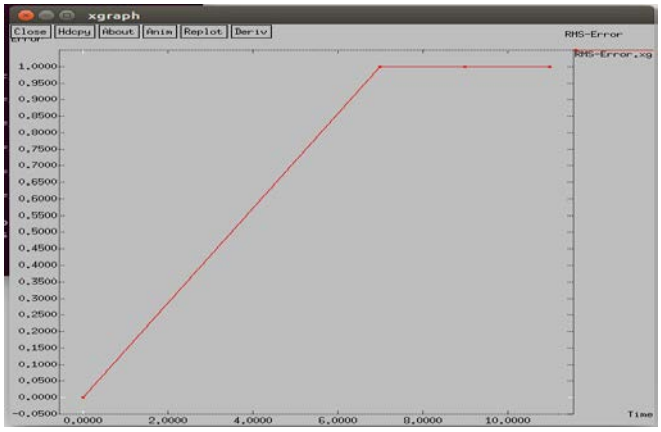

Figure 11. RMS-Error

7. CONCLUSION

Compromised node gives the invalid aggregated data to the aggregator node so that entire data will be false. This will be avoided by implementing the Iterative filtering algorithm at the head level for security purpose. Trust and data aggregation is the main thing to be happeningin the wireless sensor networks.Our system is designed to solve these problems. In the future enchantment we will design the network for reduce no of overheads in the network.

REFERENCES

[1] Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, and Sanjay Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks", *IEEE Transactions on Dependa-ble and Secure Computing (TDSC)*, 2014.

[2] Y. Sun, H. Luo, and S. K. Das, "A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks", *IEEE Transaction on Dependable & Secure Computing*, Nov. 2012.

[3] D. Wagner, "Resilient aggregation in sensor networks", in *Proc. 2nd ACM Workshop Security Ad Hoc Sens. Netw.*, 2004, pp.78–87.

[4] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: a secure hopby-hop data aggregation protocol for sensor networks", in *MobiHoc*, 2006, pp. 356–367.

[5] Chan H., Perrig A., and Song D, "Secure hierarchical in-network aggregation in sensor networks", in *Proc. 13th ACM Conf. Comput. Commun. Security*, 2006, pp. 278–287.

[6] Chou C. T., Ignatovic A., and Hu W, "Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults", *IEEE Trans. Parallel Distrib. Syst.*, 2013, vol. 24, no. 8, pp. 1525–1534.
[7] H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, "Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN," in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*, 2011, pp. 1-4.
[8] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-rotaru, and H. Rubens, "Mitigating byzantine attacks in ad hoc wireless networks," Department of Computer Science, Johns Hopkins University, Tech, Tech. Rep., 2004.
[9] X.-Y. Xiao, W.-C. Peng, C.-C. Hung, and W.-C. Lee, "Using SensorRanks for in-network detection of faulty readings in wireless sensor networks," in *Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access, ser. MobiDE '*07, 2007.
[10] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensornetworks", *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 3, pp. 1040–1052.
[11] Azeem Mohammed Abdul, Syed Umar, "Attacks of Denial-of-Service on Networks Layer of OSI Model and Maintaining of Security", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 5, No. 1, January 2017, pp. 181 -186.
[12] Rahul Desai, B P Patil2 Dual, "Reinforcement Q Routing for Ad Hoc Networks", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 7, No. 3, September 2017, pp. 786 – 794.