A Review on Data Aggregation in WSN

[1]Anushree J, [2]Chinnaswamy C.N.

[1]PG Student, NIE, Mysuru, India, [2]Associate Professor, NIE, Mysuru, India
[1]Dept of ISE,
[1]The National Institute of Engineering, Mysuru, India

Abstract: **In WSN data aggregation is an important technique which reduces the communication overhead and aims at achieving the power efficiency in the sensor network,sensor nodes have limited battery power so data aggregation is an important technique in WSN which reduces the consumption of energy by the sensor nodes.In this paper data aggregation and its approches namely Centralized,Cluster based,Tree based and In network approches along with the security requirements for data aggregation process has been discussed.The last part of the paper is focused on the several secure data aggregation schemes which are essential in the data aggregation process.**

Keywords- Data Aggregation, Centralized, Cluster, Tree based, In Network, Data Aggregation schemes

I. INTRODUCTION

A wireless sensor network is a collection of small light weighted wireless nodes called sensor nodes deployed in an environment.WSN is an adhoc network and consists of several sensor nodes, one or more base stations.These sensor nodes are deployed in a large field and collaborate with each other to from a network and has the capacity to report the collection of data to the sink(base station).Sensor nodes communicate with each other or they communicate with the help of intermediate sensor nodes,the Architecture of the Sensor network is shown in the below figure 1. Sensor nodes senses the data and farwards the sensed data to the the sink or base station.The sensor nodes have the ability of sensing the temperature, pressure, vibration, motion, humidity, sound as in [1] etc.

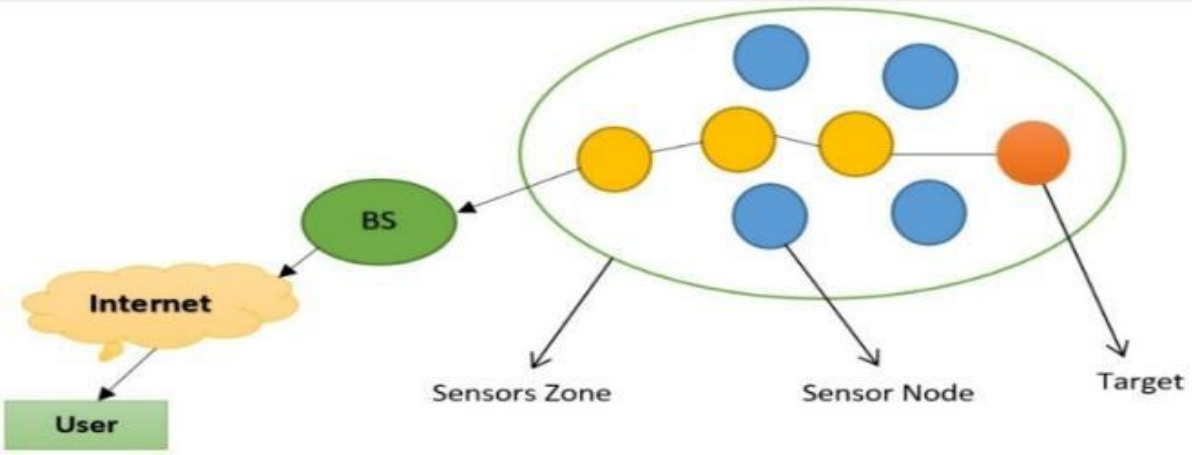

Figure 1: Architecture of the Sensor network

II. DATA AGGREGATION IN WSN

Data aggregation is the process of accumulation of data and presenting the data in a summing up form,it is a technique which reduces the size of the data and the amount of energy that is required for farwarding the data and reception of the data.Data aggregation decreases the overhead that occurs due to the communication and consumption of energy by the sensor nodes[2].The main goal of data aggregation is to eradicate redundant transmission of data and increase the energy life time of a network

As shown in the below figure 2 and 3, four packets flows through the network,with data aggregation only one data packet is transmitted from aggregator node to the base station,without data aggregation four data packets are transmitted from aggregator node to the base station,this indicates that the data aggregation technique reduces the number of data packets that is to be transmitted to the base station[3].

At begining the data from the sensor node is collected,then aggregation of data occurs by using algorithms like LEACH(low energy adjustive bunch hierarchy),TAG(Tiny Aggregation) etc. and then the aggregation information is transmitted to the sink by chosing most efficient path the figure 4 illustrates the fundamental design of data architecture technique[4]

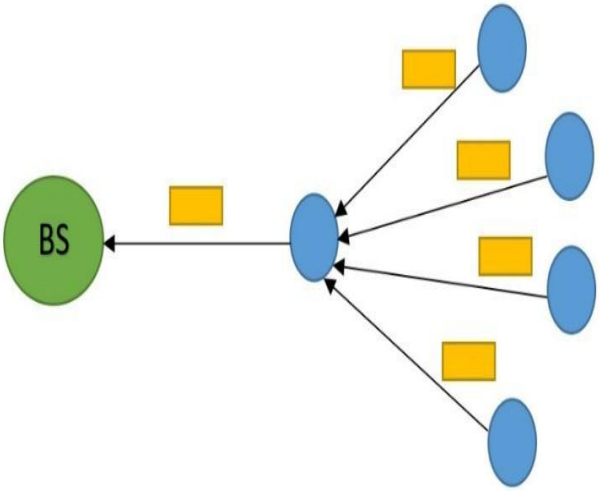

Figure 2: With Data Aggregation model

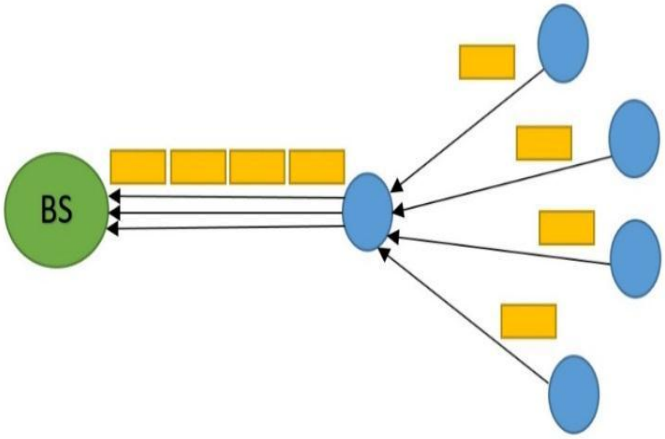

Figure 3: Without Data Aggregtion model

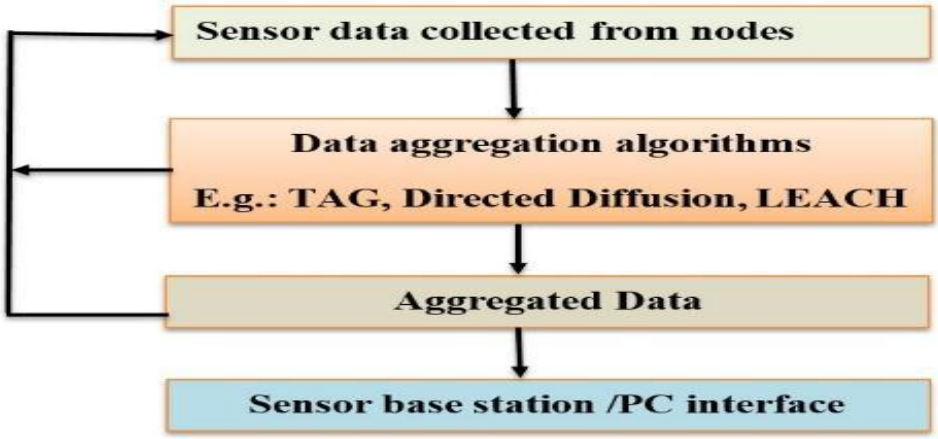

Figure 4: Architecture of Data Aggregation technique

III. SECURITY REQUIREMENTS IN DATA AGGREGATION

Data Aggregation is an important technique in WSN hence aggregation of data must be energy efficient and must be done in a secure manner,in order to achieve this technique many security needs should be considered such as: Confidentiality of Data, Integrity of Data, Freshness of data, Source Authentication[5],they are described briefly below

- **Confidentiality of Data:** It ensures that the private and the confidential data cannot be accessed by the unauthorized users.The data is encrypted using a secret key and transmitted to the intended receiver who has this key can perform decryption and read the data.
- **Integrity of Data:** It ensures that the authorized users have the authority to make changes to the data.The data should not be altered,rearranged or corrupted before reaching the destination.Integrity is an important issue because malicious nodes can perform attacks and make changes to the data by inserting false information
- **Freshness of Data:** It ensures that the data is recent and prevents replaying to the old messages by an adversary.Data frehness protects the data from the replay attack
- **Source Authentication:** It ensures that the data has been sent by the actual sender who claims be the sender of the data.Sourcs authentication prevents from Sybil attack where in which the attacker traps a node and gain access to the secret information present in the node.

IV. TYPES OF ATTACKS ON DATA AGGREGATION

Different types of attacks [6] will be performed by the attacker some of them are breifly explained below,due to the lack of security which will affect the data aggregation process in WSN

➢ **Node Compromization Attack:** In this attack the attacker gains the control of the nodes and starts collecting the confindential information stored in that node,once the attacker takes the control of any node in the network then data on the network will not be secure.

➢ **Sybil Attack:** The attacker creates several fake identities which causes serious effects on data aggregation technique.After creation of multiple fake identities the attacker participates in the selection process of aggregator node and choses malicious nodes as the aggregator node.

➢ **Denial of Service Attack:** It is an attack in which the resources of the network are inaccessible to the authorized users.In this case the aggregator node does not perform the aggregation process and prevents the data reaching to the base station.

➢ **Selective Farwarding Attack:** Nodes usually farwards the received packets to the neighbhouring node but the compromised nodes does not do this, it simply drops the packets received and this may result in the packet drop.

➢ **Replay Attack:** The compromised node repeatedly sends the same data without any freshness which may misguide the aggregator node and finally affecting the results of aggregation process

➢ **Injection Attack:** The attacker inserts false data into the network which results in false output of the aggregation process

V. DATA AGGREGATION TECHNIQUES IN WSN

There are many data aggregation techniques namely which are described below

➢ **Centralized Approch:** In this approach a central node acts as a aggregator node and all the other nodes will be connected to the central node which can also be called as aggregator node.Nodes apart from the central node senses the data and transmits the data to the central or aggregator node.All the data exists on the central node and the load on it will be more hence it requires more enegy and security[7].

➢ **Cluster Based Approch:** In this approch the network will be split into many cluster where each cluster has a cluster head,the cluster head will be chosen by the cluster members.The cluster head acts as the aggregator node which assembles the data received from its members and transmits the outcome to the base station[8].

➢ **Tree Based Approch:** Data Aggregation Tree (DAT) is formed at first,minimal spanning tree will be created for each of the transmission.Data flow occurs from leaf to the sink node,the parent node does the data aggregation process[9].

➢ **In Network Approch:** In this approach we have two types[9]- **with size reduction:** Data packets received from the neighbour node is combined and compressed,this is done to reduce the length of the packet which is to be farwareded to the sink.- **without size reduction:** Data packets received from the neighbours are combined to form a single packet of data but the value of data without being processed.

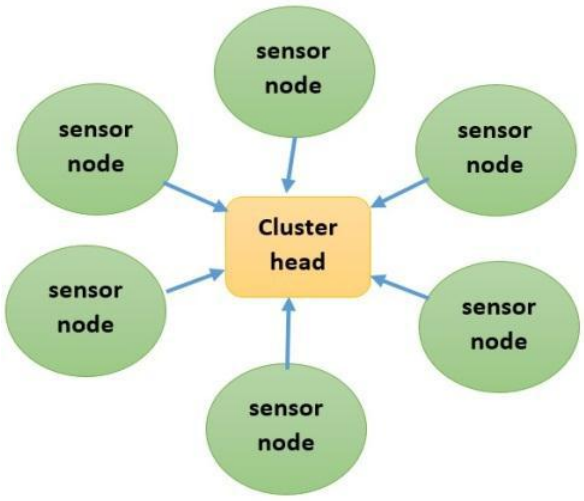

Figure 5: Centralized approch

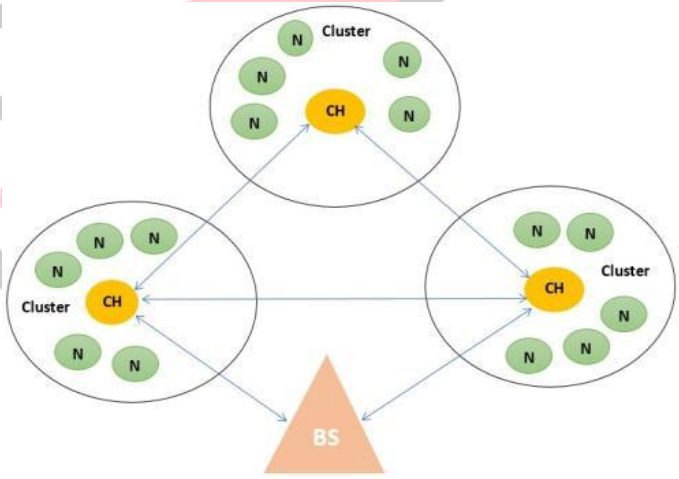

Figure 6: Cluster based approach

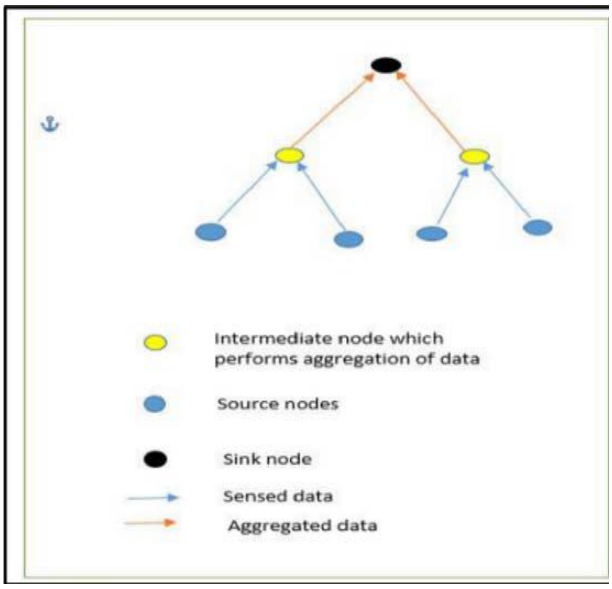

Figure 7: Tree Based Approch

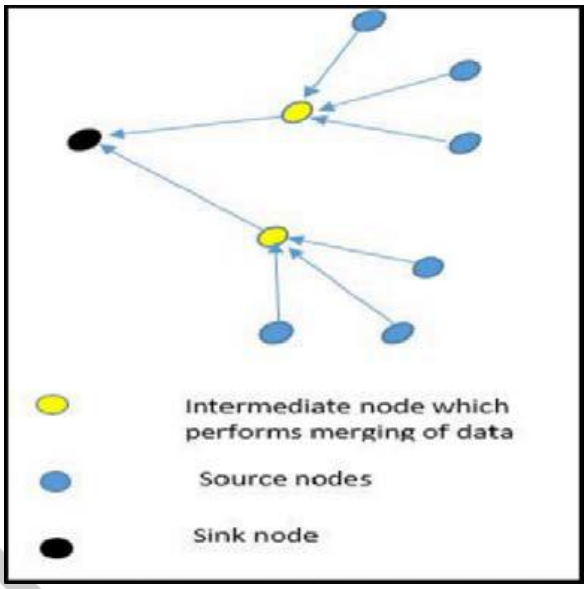

Figure 8: In Network Approch

VI. SEVERAL SECURE DATA AGGREAGTION SCHEMES

There are many secure data aggregation schemes which are discussed briefly in this section.

CPDA(Conflict Periodic Data Aggregation)[10] scheme which supports regular data aggregation with data rate being high,it is a technique which also supports conflict free data aggregation by using a timing called delta between two successive packets of data.CDPA aims at achieving data aggregation process with conflict free and it works with sensor nodes with battery power being low.

ESDAD(Energy Efficient Structure Free Data Aggregation and Delivary)[11] is a scheme in which the data is transmitted to the node which is in the next hop based on the reliability which is required for data aggregation.The ESDAD allows favoured number of senders to farward the data that is sensed depending upon the required reliability,it not only reduces the consumption of energy of the nodes but also reduces the traffic load in the network.

SAC-TA(A Secure Area Based Clustering for Data Aggregation Using Traffic Analysis)[12] is a scheme in which the network is partitioned into cluster with each cluster having the cluster head to adminster and collect the information from the cluster members.The cluster head is elected based on 3 requirements namely time slot,cluster center,highest residual energy.The data which is collected is checked based on the analysis of the traffic and one time key generation is used to check whether any malicious node is present in the network or not.This scheme provides secure data aggregation with enhanced energy efficiency.

ERDL(Efficient and Real Time algorithm based on Dynamic message List)[13] in this scheme the cluster head acts as a filter node,dynamic list will be created in every filtereing node which is used to store information regarding the history of the packets that are transmitted by a node.When a data packet arrives at the filtering node comparission is done with the existing items in the list,if the content of the packet already exists in the list,it will be unused if not available it will be farwarded at once and the list updation takes place.Using ERDL filtering efficiency will be improved and has the advantage in real time transmission.

VELCT(Velocity Energy Efficient and Link aware Cluster Tree)[14] is used for aggregation of data that has been collected,which is used to reduce the overhead of the sink.VELCT notices the information that is being collected at the collection node,and checks whether the information collected is genuine or not,when any information that is not valid is noticed,it detects the attacker in each cluster and control the attacker malicious information and ensures that information which is authenticated is farwarded to the sink.

SDAMQ(Secure Data Aggregation for Multiple Queries)[15] is a authenticated query distribution which assures that no false query is introduces into the network.SDMAQ discovers replay attack and drops all the malicious information from the aggregation process.

RCDA(Recoverable Concealed Data Agrregation)[16]Aggregate signature scheme is combined with RCDA to assure data integrity and authenticity.Individual sensor data can be retrieved by the base station even if the cluster head has aggregated the data.

Sen-SDA[17] is a secured data aggregation scheme which ensures end to end confidentiality and hop by hop authentication but this scheme suffers from computational overhead and adds cost on the communication.

Secure Data Aggregation with MAC Authentication[18] scheme presents a way to achieve data aggregation with confidentiality and integrity in WSN,it uses MAC(Message Authentication Code) and homomorphic encryption(elliptic curve elgamal) to ensure integrity,authenticity and confidentiality of the data.

RSDA(Reputation based Secure Data Aggregation)[19] scheme aims on availability and data accuracy by combining the functionalities of data aggregation,it increases the life time of the network and aggregation accuracy.In RSDA scheme the area is split into cells which are equal in size,each sensor nodes investigates the behaviour of its cell by supervising the neighbour nodes in order to remove the unstable data.

SDAP(Secure Hop by Hop Data Aggregation Protocol)[20]scheme uses two principles divide and conquer,commit and attest.First step is construction of tree,where aggregation tree is constructed.Nodes discover their parents after the base station spreading the aggregation query message through out the tree.Second step is divide and conquer principle in which the entire tree is split into subtrees based the technique which is called as probabilistic grouping.

WDA(Witness based Data Aggregation) [21] is a scheme in which data aggragtion is performed by the witness node,it doesnot transmit the result rather a MAC(Message Authentication Code) of the result will be calculated by every witness noded,after that the witness node sends this to the aggregator node,the aggregator node transmits the proof to the base station.The aggregator node should provide proofs in order to prove the validation.

DA Schemes	Data confidentiality	Integrity	Authentication
SDMAQ	no	yes	yes
RCDA	no	yes	yes
Sen SDA	yes	no	yes
Secure DA with MAC	yes	yes	yes
RSDA	no	yes	yes
SDAP	yes	yes	yes
WDA	no	yes	yes

Table 1: Comparison table

VII. CONCLUSION AND FUTURE WORK

This paper introduces discussion about data aggregation and its approaches,security requirements in data aggregation and some secure data aggregation schemes. Data aggregation is an important technique in WSN which presents the data in summary form and reduces the size of the data which results in the reduction of energy consumption by the nodes while sending and receiving the data. Data aggregation approaches which are discussed here are Centralized,Cluster based,Tree based and In network approaches. In centralized approach central node acts as a aggregator node,in cluster approach entire network will be divided into cluster with each cluster having cluster head,minimal spanning tree creation takes place for each transmission in the tree based approch,in network approch has two types they are with size reduction and without size reduction.Data aggregation process must be carried out securely and should be energy efficient,to achieve this security requirements are necessary they are confidentiality of data, integrity of data, freshness of data, source authentication.Several secure data aggregation schemes has been discussed which makes the data aggregation process an efficient one.In the future work data aggregation using iterating filtering technique and privacy preservation data aggregation schemes can be done.

REFERENCES

[1] Aashima Singla, Ratika Sachdeva "Review on Security Issues and Attacks in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 4, 2013

[2] Wael Y. Alghamdi, Hui Wu, Salil S. Kanhere "Reliable and Secure End-to-End Data Aggregation Using Secret Sharing in WSNs"Wireless Communication on Networking Conference(WCNC), 2017IEEE

[3] Kiran Maraiya, Kamal Kant, Nitin Gupta" Wireless Sensor Network: A Review on Data Aggregation" International Journal of Scientific & Engineering Research Volume 2, Issue 4, April -2011 1

[4] Ameya S. Bhatlavande, Amol A. Phatak. (2015), Data Aggregation Techniques in Wireless Sensor Networks: Literature Survey , *International Journal of Computer Applications*, Vol.115 – No. 10, pp. 21–25.

[5] Mukesh Kumar Jha, T.P Sharma "Secure Data aggregation in Wireless Sensor Network: A Survey", International Journal of Engineering Science and Technology, ISSN: 0975-5462, Vol. 3 No.3, March-2011

[6] Priyanka B. Gaikwad, Manisha R. Dhage.(2015), Survey on Secure Data Aggregation in Wireless Sensor Networks, *Computing ommunication Control and Automation (ICCUBEA), 2015 International Conference* , pp. 242-246.

[7] Jyoti Rajput Naveen Garg," A Survey on Secure Data Aggregation in Wireless Sensor Network",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014

[8] Youssef Emhemmad Mohammad Youssef* and Raghav Yadav,"Survey on Several Secure Data Aggregation Schemes in WSN",International Journal of Current Engineering and Technology, 11 July 2016, Vol.6, No.4 (Aug 2016)

[9] Sumedha Sirsikar,Samarth Anavatti,"Issues of Data Aggregation Methods in Wireless Sensor Network :A Survey" 4th International Conference on Advances in Computing,Communication and Control(ICAC3'15)

[10] Chhabi Rani Panigrahi,Bibudhendu Pati,Joy Lal Sarkar," CPDA: A conflict-free periodic data aggregation technique in wireless sensor networks", Egyptian Informatics Journal,19 June 2016

[11] Prabhudutta Mohanty,Manas Ranjan Kabat," Energy efficient structure-free data aggregation and delivery in WSN", Egyptian Informatics Journal, 4 March 2016
[12] Mohanbabu Gopalakrishnan, Gopi Saminathan Arumugam, Karthigai Lakshmi
Shanmuga Vel," SAC-TA: A Secure Area Based Clustering for Data Aggregation Using Traffic Analysis in WSN", Scientific Research Publishing,9 June 2016
[13] Tao Du, Shouning Qu, Kaiqiang Liu,,Jinwen Xu, Yinghua Cao," An efficient data aggregation algorithm for WSNs based on dynamic message list", The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016), ScienceDirect,2016
[14] Sneha Kamble,Tanuja Dhope," Reliable Routing Data Aggregation using Efficient Clustering in WSN",International Conference on Advanced Communication Control and Computing Technologies (ICACCCT),2016
[15] E. G Prathima,T. Shiv Prakash,K. R. Venugopal,S. S. Iyengar and L. M. Patnaik,*"* SDAMQ: Secure Data Aggregation for Multiple Queries in Wireless Sensor Networks", Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016), ScienceDirect,2016
[16] Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin and Hung-Min Sun, RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks, *IEEE Transactions on Parallel and Distributed Systems*, vol. 23(4), pp. 727–734, (2012).
[17] Kyung-Ah Shim and Cheol-Min Park, A Secure Data Aggregation Scheme based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks, *IEEE Transactions on Parallel and Distributed Systems*, vol. 26(6), pp. 2128–2139, (2014).
[18] S.B.Othman, A.Trad, and H.Youssef "Secure Data Aggregation with Mac Authentication in Wireless Sensor Networks", 12th Int. Conf. on Trust, Security and Privacy in Computing and Communications, 2013
[19] H.Alzaid, E.Foo, and J.G.Nieto "Reputation-based Secure Data Aggregation in Wireless sensor Networks" in Proc. 1st int. Workshop on sensor Networks and Ambient Intelligence
[20] Y.Yang, X.Wang, S.Zhu and G. Cao "A Secure Hop-by Hop Data Aggregation Protocol for Sensor Networks" in Proc. 7th ACM Int. Symp. Mobile Ad-hoc, 2006
[21] W. Du, J. Deng, Y.S. Han and P.K. Varshney., A witness based approach for data fusion assurance in wireless sensor networks, *'IEEE Global Communications Conference (GLOBECOM)',* Vol.3, pp1435-1439