ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Secure Data Aggregation Types in Wireless Sensor Networks: A Review

Sheetal
M.Tech Student (CSE)
UIET, MDU, Rohtak, India

Dr. Chhavi Rana
Assistant Professor (CSE)
UIET, MDU, Rohtak, India

Abstract: With pace of time there is huge development in the field of advances of WSN (Wireless Sensor Networks) that leads to many emerging applications like target tracking application. Sensor nodes spend most of their energy during data transmission. With data aggregation, one can eliminate the redundant data transmission and so reduce the energy consumption. Sensor nodes are set up in a varied adverse environment which often compromise. So the maintenance of parameters of security such as confidentiality, integrity, authentication and availability become crucial. Nowadays there are many fields where wireless sensor network can be used like health care monitoring, earth/environmental sensing, climate observation, air pollution monitoring, forest fire detection as well in wearable devices, target-tracking. Prior transform it into valuable information that is essential to decide the degree of data aggregation due to scarcity of network management and controlling systems. Because of restricted transmission area of sensors, they couldn't be used in huge geo graphical areas. There is some network management tools required in huge area networks for the development of the huge scale sensor network such as routing and data aggregation etc.

Keywords: Aggregation, base station (BS), confidentiality, cluster head (CH), security, Sensor Nodes (SN's).

1. INTRODUCTION

With the amelioration in time and technology, WSN become more important now a day in security techniques as they may connect with conscious data or control in adverse unattended environment**.** Sensor networks build up of tiny and worthwhile sensing devices assembled with wireless radio transceiver for the purpose of climate observation come to be attainable. The main benefit of using the tiny devices is that they don't need any framework for example electric mains for power supply and wired lines for Internet connections to collect data. They don't require individual cooperation during deploying WSN because of containing many sensor nodes. They collect data from deployed environment. The sensor nodes (SN's) collect information from surrounding to monitor the environment [1]. Now a day, there are huge number of rich applications proposed for WSNs, such as climate observation, accident reporting, and military investigation etc. SN's are customized to read various types of data (e.g. temperature, light, or smoke), based on the purpose of each application. Basically, SN's are bounded by the resources because of the restricted computing power and less power supply. Clustering is the important method for enhancing the lifetime of network in WSN [1].

In WSN the procedure of combining the sensor nodes into clusters and choose the cluster head for all the clusters is known as clustering [1]. In cluster based environment, the way of blend and constrict the data into a single cluster is known as data aggregation. During procedure of clustering various issues can occur. These are [2]:

- How many clusters should be used to enhance the performance?
- How many nodes we can add in a individual cluster?
- The process of selecting the CH (Cluster-Head) in cluster.

Some powerful nodes can be used in terms of energy which acts as a CH (cluster-head) and other node act as cluster-member only [3]. The most important factor in considering WSN is power management because WSN has limited battery power. Therefore transmission cost is higher than the computing cost because nodes absorb most of the energy during intercommunication. So it's important for the nodes to be energy efficient. To resolve these issues the concept of data aggregation was introduced. Data aggregation was added to enhance the performance and for cost reduction [4].

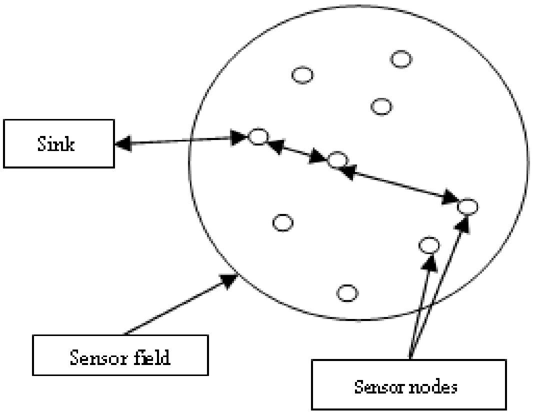


Figure 1 Sensor Network

A. Energy-Efficient Secure Pattern-based Data Aggregation Protocol (ESPDA)*:* This protocol is used for energy efficient data aggregation and secure intercommunication in WSN [5]. ESPDA is also called as data aggregation protocol based on cluster. To perform data aggregation it uses pattern codes instead of sensed data. Cluster-head (CH) first broadcasts the route or we can say pattern seed to the sensor nodes and requests them to transfer the related pattern code for sensed data. Pattern Seed is a random number which is used to enhance the privacy. Using secret patterns (using encryption) by cluster head, the pattern codes are created which prevent the unauthorized users to retrieve the actual data.

Various pattern codes and pattern generation (PG) algorithms are used in ESPDA. If more than one SN (sensor nodes) wants to send the same pattern code to the CH (cluster head), then only one out of them will be allowed to send the pattern code to the CH. Before original data transmission from the sensor nodes (SN), data aggregation is executed. ESPDA also provides security because it gathers the data using pattern codes, so CH do not required knowing the essence of the transposed data. Thus the sensor data is transposed to base station in encoded form without any decoding in the communication path. ESPDA employs a code hopping technique as Non-blocking Orthogonal Variable Spreading Factor (NOVSF). Sensor nodes compute a Node-Specific-Secret-Key (NSSK) using their unique secret built-in key and a session key broadcasted by the base station. This node-specific-secret-key is used to encode and decode whole data (information) transmissions throughout a process.

Thus, ESPDA is an energy-efficient, bandwidth efficient, and secure protocol which provides data confidentiality, authenticity, and data freshness.

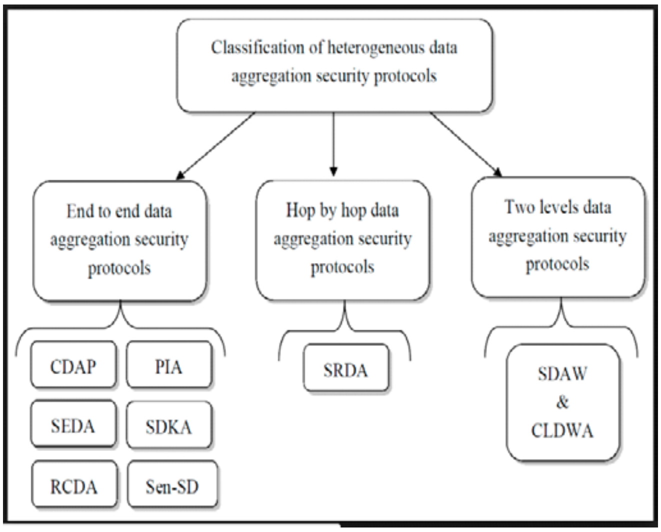

Classification of heterogeneous data aggregation security protocols
End to end data aggregation security protocols
Hop by hop data aggregation security protocols
Two levels data aggregation security protocols
CDAP
PIA
SEDA
SDKA
RCDA
Sen-SD
SRDA
SDAW & CLDWA

Figure 2 Classification of Heterogeneous aggregations Security Protocol

B. Energy-Efficient and High-Accuracy Secure Data Aggregation: *Cao, X. M., W. I. Li, and Geng Yang* proposed a protocol EEHA [6], in which distinct aggregation of data is acquired without discharge any interpretation of discreet sensor as well as without any expressive significant over burden on the battery-limited sensors. The main objective of EEHA protocol is on the exculpation of eavesdropping attack in which an intruder makes effort to spy the transmission over wireless connections to acquire obscured information. The main motive of this scheme is to accomplish the correct aggregation of data with balanced communication overhead for the purpose of maintaining the data privacy. EEHA protocol basically consists of three types of nodes. These are:

a) Base Station.

b) Intermediate Nodes.

c) Termination Nodes.

The first step towards the process is to construct the aggregation directed tree. This directed tree is assembled by combining all paths from the SN (sensor nodes) to the BS (base station). After that the termination node makes the use of “slicing and mixing” technique. In this technique they slice the private data into pieces and send these pieces of data to the neighbours while one piece is kept by itself. All the leaf nodes wait for a certain time and then mix (sum) each of accepted slices (data into portions) and the slice (piece of data) left out itself to achieve a latest result then to the intermediate node. The intermediate node aggregates the accepted data or information & then sends it to its parent.

2. LITERATURE REVIEW

“Secure Data Aggregation Types in Wireless Sensor Network”, the present paper reviewed the various data aggregation types and their security aspects. Many researchers already have done work on aggregation methods in secure wireless sensor network. They implement the WSN using the best data aggregation techniques to reduce the main drawbacks of the network i.e. limited power supply. The study of existing work already done by various researchers is discussed hereby.

Fasolo, Elena et-al [7] described in-network aggregation technique and protocols. The main purpose of this paper was to support appropriate taxonomy of in-network aggregation. At one side it provides the existing solutions and on other side, it provides the solution for future use. The main motive was to motivate the researchers to use in-network aggregation.

Suman Nathy, Phillip B. Gibbons et al [8] was described the synopsis diffusion basic framework in an in-network aggregation. Synopsis diffusion used Ordered and Duplicate-Insensitive (ODI) which avoided duplicate data. ODI synopses used to conclude the intermediate resultant during in-network aggregation.

Sushruta Mishra and Hiren Thakkar [9] have discussed the features of WSN along with data aggregation. In this paper different architecture for data aggregation techniques is explained and simulation software discussed.

Nanthini.D and R.A.Roseline [10] had focused on different kinds of data aggregation in WSN as well as illustrated the general techniques and protocols used for it. A protocol had been proposed to route packets for providing the data aggregation.

Sirsikar, Sumedha, and Samarth Anavatti [11] have focused on different issues in spite of data aggregation process like delay, redundant data elimination and reliability. Various existing data aggregation approaches used some different issues like redundancy, delay, accuracy, and traffic load that affect the performance of data aggregation.

This paper used different approaches and technique to solve these issues and they proposed one model which performed data aggregation at two levels at cluster head and at a storage node that maintained between energy efficiency and accuracy as well as it also balance traffic load.

3. DATA AGGREGATION

Data aggregation is very important method in which each node transmits the data to a central node but that data will follow the shortest destination path with the help of multi hop wireless protocol. Simply, the SN's transmit the data to the leader node (powerful node). Every intermediate node has to transmit the data packets that forwarded to powerful node from the child node. Therefore, vast number of messages has to be sent for any doubt which is equal to the addition of external path length for all nodes in the best alternative case [12].

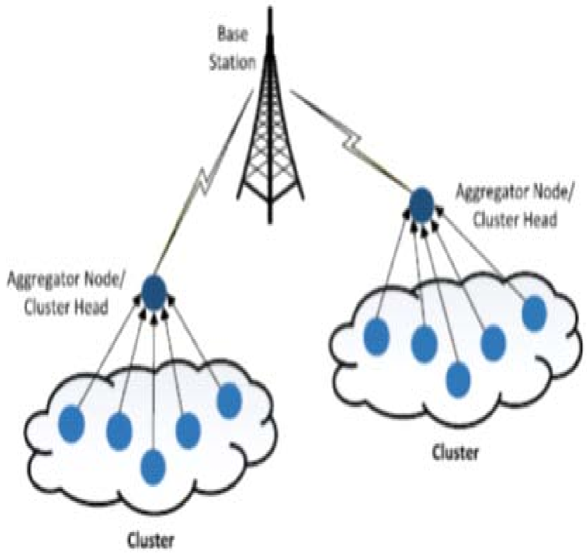


Figure 3 Secure Data Aggregation Model

A. *Data Aggregation Approaches in WSN:* The process of Data Aggregation is performed by specific routing protocol. The main purpose is to reduce the energy consumption by grouping the data. So, the SN's must route packets that is based on the data packet content after that select the next hop for improvement in network aggregation [13]. Routing protocols is based upon the considered approaches because it is basically differentiated by the network structure.

a) In-Network Aggregation: It is the universal procedure of grouping and routing data by Multi-Hop Network, processing information at intermediate node with the purpose of optimal utilization of resources to enhance the lifetime of network. Basically two techniques are there in In-Network Aggregation which includes size [14].

(i) Size Reduction Method
(ii) Without Size Reduction Method

(i) **Size Reduction:** It refers to the procedure of blend and constricts the data packets where information is stored and accepted by a node from its neighbors to minimize the size of data to be sent towards sink.

(ii) **Without Reduction Method:** It refers to the process of bringing out the data packets together into a single data packet without altering the actual value of data.

b) *Tree Based Approach:* The tree based approach carried out the aggregation of data by designing an aggregation tree. This aggregation tree rooted as base station (sink) and source nodes are analyzed as leaf nodes that could be as minimum spanning tree (MST). Each and every node consist a parent node to transmit its information. The data follows the bottom up approach because it starts from leaves nodes up to the sink and data aggregation is done by their parent nodes [15].

As we know that wireless sensor networks are not free from failure. The data would be lost for single level as well as for whole related sub trees in the situation when data packet lost at any level of tree. This approach is well suited for constructing optimal aggregation techniques.

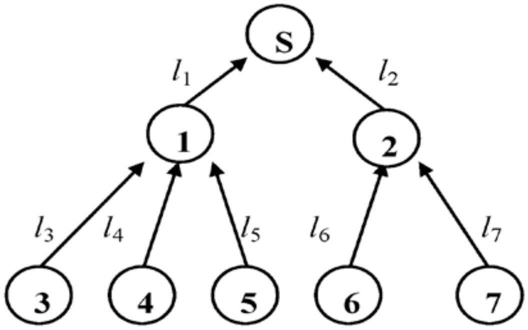


Figure 4 Tree base Aggregation model

c) *Cluster-based approach:* In energy-constrained SN's of huge size, it's improvident for sensors to transfer the information directly to the base station that considered Cluster based approach as hierarchical approach. In this approach a complete network is distributed into various clusters [16]. Each cluster has a CH which performs as aggregator which combines the information retrieved from cluster members and then sends the result to sink. In recent past various cluster-based network organization and data-aggregation protocols have been proposed for the WSN.

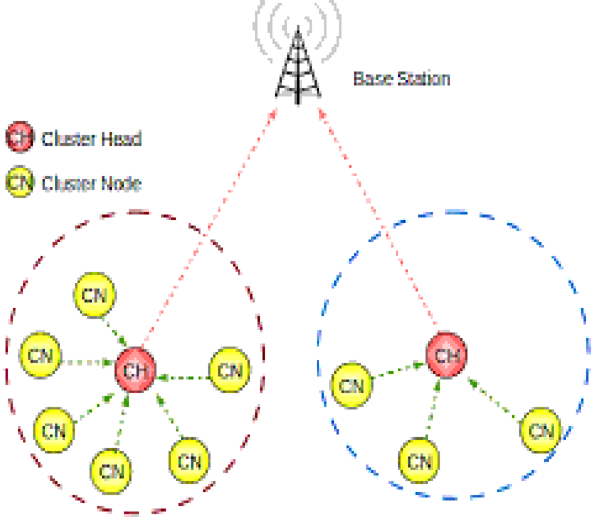


Figure 5 Aggregation model based on Cluster-Head

d) *Multi-path Approach:* This approach is used to minimize the limitation of tree-based approach i.e. the limited strength of the system. To minimize the limitation, a newly concept was projected with the help of various researchers [17]. They combines the data transparently transmitted to one parent node in aggregation tree, a node can transmit the information beyond multiple paths, in which each node is able to transmit the data packets to its multiple neighbor nodes based on possibilities. Thus, aggregation is done at each intermediate node because the flow of data packets is from source node to destination node which has optional multiple path and lots of intermediate nodes between source node to sink node (special node). This approach helps to make the system robust but along with few extra overhead.

e) ***Hybrid Approach:*** Hybrid approach is used for implementation of tree like cluster based and multipath scheme based which consists of the structure of data aggregation that may be adapted due to specified network position and performance statistics.

The wireless sensor networks are susceptible to security attacks because of broadcasting nature of the communication system. Additionally, wireless networks also have an extraneous susceptibility as the nodes are placed in adverse environment.

B) Cryptography:

Cryptography is a mechanism used for security purposes. It is the science used to keep the data secure and confidential. It basically converts the plain text into cipher text. Now a day's cryptography is more than encoding and decoding the data [18]. In cryptography a key is used for both encryption and decryption. Cryptography basically resolves two kinds of security issues: Privacy and Authenticity. In encryption data is encrypted by any encryption algorithms at sender side and decrypted at receiver side with the help of key.

a) ***Public Key Cryptography****:*

In this technique, both sender and receiver uses the different kinds of keys. They have a pair of keys: Private Key, Public Key. Public key is known to all or other devices for communication. But private key is a secret key only known by the sender and receiver that is used to encipher and decipher the information during communication. Example of public key cryptography is RSA Algorithm.

b) ***Private Key Cryptography****:*

In this technique, only a single key is used for both encipher and decipher the secrete information that should be known to both sender and receiver. Only the authenticated users have the access to the same 'key' can decode the encoded information. Examples are AES (Advanced Encryption system), DES (Data Encryption system) etc.

4. PLANNING OF WORK AND METHODOLOGY

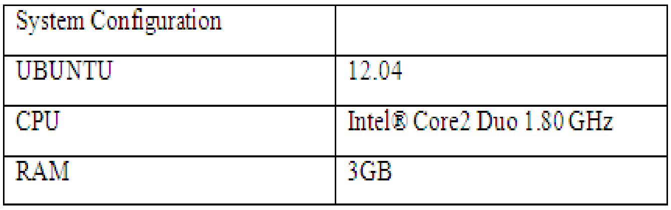
In our proposed work, the cluster consists of various access points that have energy (unlimited) at large scale comparatively cluster head. Thus, instead the use of cluster head, we will use the Access points. The Access points work similar to the mini base stations. All clusters have an access point and every time needs not to form new cluster head even if cluster heads does not exist. With the transformation of nodes, the access point i.e. head remains same. We will implement this protocol with the help of Ns2 Simulator. Network Simulator, commonly known as NS2 that is simply a simulation tool to drive the events that has proved beneficial during the study of active behavior of intercommunication network. Using NS2, imitation of both wired and wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done. In general, NS2 software provides a way of specifying such network protocols and imitating their respective nature to the users. Beyond its birth in 1989, it has achieved much attention in the field of networking research because of its adjustable and modular behavior.

Software Used and Simulation Result

Software NS-2:

NS stands for- Network Simulator (NS). NS is used for a series of discrete event network simulators, mainly NS-1, NS-2 and NS-3. We use NS-2 (v-2.35), an open source network simulation tool to imitate wireless communication network. NS2 is discrete event simulator developed. It provides a good platform for WSN imitation. The random way point model is selected as a mobility model in a rectangular field (2000 x 2000 m^2). AODV is used for simulation at network layer and the nodes transmit constant bit rate (CBR) traffic at distinct varying rates of transmission. The performance of Energy Efficient based Cluster protocol in WSN is being calculated with the simulation on network simulator-2. We can calculate the following results with the help of .awk script. We can also plot the bar graphs of following parameters by using output. The final result is carried out by NS-2 simulator by using below parameters:

1. Throughput
2. Packet Delivery Ratio
3. Energy Consumption
4. Average End to End Delay
5. Normalized Routing Load



System Configuration	
UBUNTU	12.04
CPU	Intel® Core2 Duo 1.80 GHz
RAM	3GB

5. CONCLUSION

In our study it is reviewed that based upon the resu1ts of simu1ation a comparative ana1ysis is done between se1ected aggregation approaches. The performance has been eva1uated based on parameters that aim to figure out the effects of routing protoco1s. We know that WSN consists of an ample number of SN's. The lifetime of the network is insufficient because the nodes are resource constraint. So, to enhance the lifetime of WSN diverse proposals and protocols has been proposed. After studying various research papers we discussed and analyzed that the data aggregation techniques are important and crucial techniques for increasing the lifetime of network. The main security concerns are data integrity. We can diminish the sensor source nodes with the help of data integrity. We will try to enhance more security in our future proposed work using new algorithm or can say protocols.

REFERENCES

[1] Yang, Mingxin, Jingsha He, and Xuguang Sun. "Research on secure data aggregation in wireless sensor networks based on clustering method."Internet Technology and Applications (iTAP), International Conference on. IEEE, 2011.

[2] Karthikeyan, B., et al. "Analysis of data aggregation in wireless sensor network." Electronics and Communication Systems (ICECS), 2nd International Conference on. IEEE, 2015.

[3] Rezvani, Mohsen, et al. "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks." IEEE Transactions on Dependable and Secure Computing, 2015.

[4] Jiang, Jinfang, et al. "An efficient distributed trust model for wireless sensor networks." IEEE transactions on parallel and distributed systems, 2015.

[5] Jose, Josna, S. Manoj Kumar, and Joyce Jose. "Energy efficient recoverable concealed data aggregation in wireless sensor networks." Emerging Trends in Computing, Communication and Nanotechnology (ICE-CCN), International Conference on. IEEE, 2013.

[6] Cao, X. M., W. I. Li, and Geng Yang. "Research on Secure Data Aggregation in Wireless Sensor Network." Computer Technology and Development, 2012.

[7] Fasolo, Elena, et al. "In-network aggregation techniques for wireless sensor networks: a survey." IEEE Wireless Communications , 2007.

[8] Nath, Suman, et al. "Synopsis diffusion for robust aggregation in sensor networks." Proceedings of the 2nd international conference on Embedded networked sensor systems. ACM, 2004.

[9] Mishra, Sushruta, and Hiren Thakkar. "Features of WSN and Data Aggregation techniques in WSN: A Survey." International. Journal of Engineering Innovation and Technologies (IJEIT), 2012.

[10] Nanthini.D and R.A.Roseline, “Aggregation Protocols in Wireless Sensor Network- A Survey“ by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 7, July 2014.

[11] Sirsikar, Sumedha, and Samarth Anavatti. "Issues of data aggregation methods in wireless sensor network: a survey." Procedia Computer Science, 2015.

[12] Patil, Nandini S., and P. R. Patil. "Data aggregation in wireless sensor network." IEEE international conference on computational intelligence and computing research. Volume 6, 2010.

[13] Rezvani, Mohsen, et al. "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks." IEEE Transactions on Dependable and Secure Computing, 2015.

[14] Chan, Haowen, Adrian Perrig, and Dawn Song. "Secure hierarchical in-network aggregation in sensor networks." Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006.

[15] Roy, Sankardas, et al. "Secure data aggregation in wireless sensor networks." IEEE Transactions on Information Forensics and Security, 2012.

[16] Yang, Yi, et al. "SDAP: A secure hop-by-hop data aggregation protocol for sensor networks." ACM Transactions on Information and System Security (TISSEC), 2008.

[17] Patil, Nandini S., and P. R. Patil. "Data aggregation in wireless sensor network." IEEE international conference on computational intelligence and computing research, Volume 6, 2010.

[18] Rezvani, Mohsen, et al. "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks." IEEE Transactions on Dependable and Secure Computing, 2015.