Research Article   **August 2017**

A Survey on Data Aggregation Attacks and Approaches in Wireless Sensor Network

Ajay Singh Sikarwar
(Research Scholar) Dept. of CSE,
ITM University, Gwalior, Madhya Pradesh, India

Kapil Sharma
(Asst.prof) Dept. of CSE,
ITM University, Gwalior, Madhya Pradesh, India

Abstract- With the development of internet technologies the application of Wireless Sensor Network (WSN) has become inescapable in our physical environment. Such technology depend on the WSN to capture environmental data and transmit it through the network to the specified location or storage. The transfer and capture of data by the WSN process, there is a challenge with research to continuous maintain the working of WSN device. To save energy in WSNs data aggregation (DA) technique is used. This could cause some security problems since false may be injected during data aggregation by data aggregator. In this paper, we present a survey that focus on data aggregation in WSN, problems in security and energy constrained in sensor networks.

Keywords- Data Aggregation, Wireless Sensor Network; Security; Clusterapproach.

I.   INTRODUCTION

Wireless Sensor Network has come out as one of the most rapidly emerging technology and it is a collection or group of specially designed transducers which is having communication infrastructure, which can be used for monitoring, measuring or recording conditions at remote or diverse locations [2]. Generally measured parameters are temperature, pressure, speed, humidity, sound intensity, direction of wind, intensity of illumination, voltage of power line, vibration intensity, concentrations of chemicals, pollutants presence level and body functions. WSNs have variety of applications like video surveillance, automation of industry, connected smart homes, controlling and monitoring of air traffic and medical equipment, robot control, monitoring atmospheric weather conditions and much more which may be critical to life safety and risk management [2]. A WSNs is made of different sensor nodes that are positioned in the network. Such nodes in the network are deployed either manually (deterministically) or randomly. A nodes in the network communicates either directly or indirectly with each other and then to the base station (i.e. the main storage location for the data) in order to perform any application oriented task.
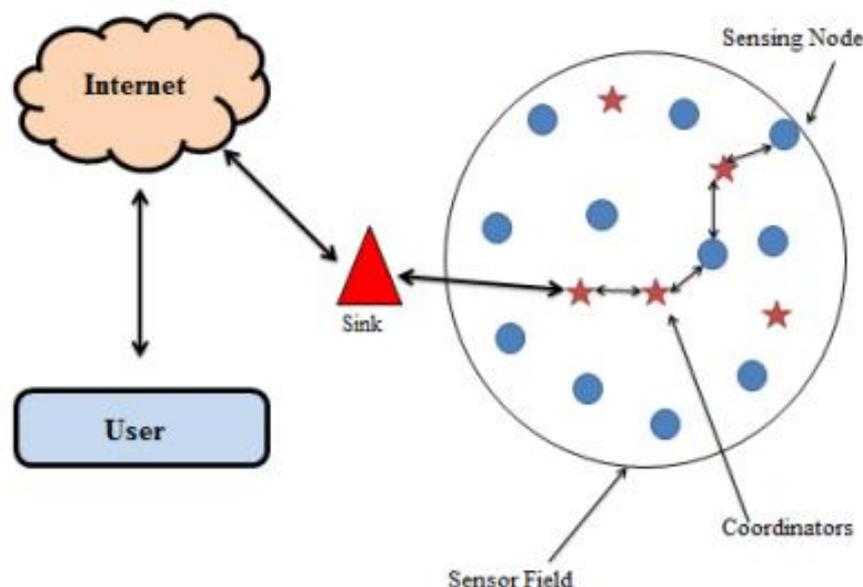

Fig.1. Wireless Sensor Network

In fig 1. Shows the scenario of WSN network, the deployment of sensor nodes in dense WSN environment, the neighboring sensor nodes often have overlapping sensing ranges. Therefore it produces some similar data resulting in large volume of raw network data. A large amount of redundant data transmission increase the amount of data transmission and also the usage of energy and bandwidth for transmission of data. So it is not efficient in an energy constrained wireless sensor network (WSN). One of the solutions to this is data aggregation [3].

Data aggregation (DA) is the method of combining data originating from different sources by utilizing aggregation function such as (min, max, average, sum etc.) and send the accumulated result to other high level aggregated node. Data aggregation (DA) method is to remove redundant transmitted data, reduce the amount of data transmission, saves energy and bandwidth also increase the network life time and data accuracy with robustness.

II. DATA AGGREGATION

In wireless sensor network, Data aggregation is the process of aggregation data from different sensor node by using aggregation techniques such as MAX, MIN, AVG, COUNT, SUM as in [4] etc. on aggregator nodes. Data Aggregation (DA) is a process of removing redundant data from multiple sensor nodes. In this technique of aggregation, how the data is to be routed on the network and processing method that are applied on the data packets. Data aggregation (DA) is a process that used to solve the implosion and overlap problems in data centric routing [5].
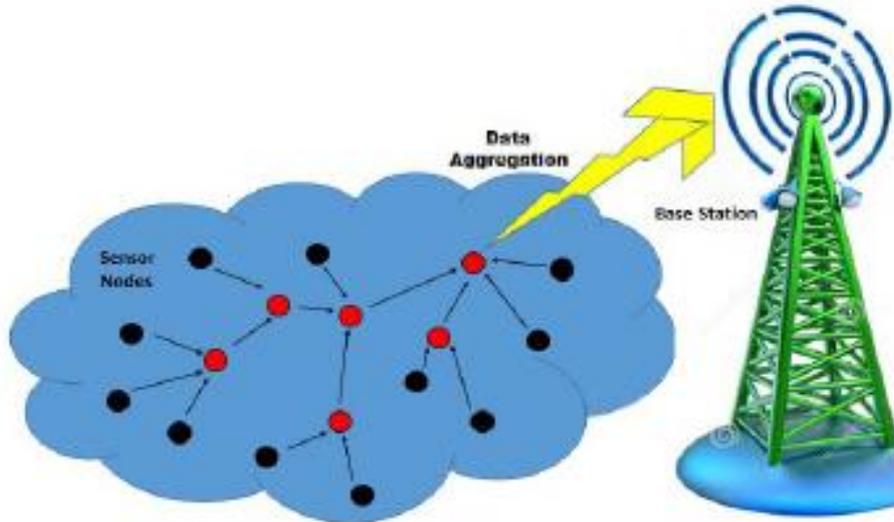

Fig.2. Data Aggregation [2]

Data coming from various sensor nodes are aggregate as they are about the same attribute of the phenomenon when they reach the same routing node on the way back to the sink. In data aggregation the security related issues are data confidentiality and integrity that becomes important when the sensor network is deployed in a hostile environment.

Data Confidentiality

Nodes in the network carry useful and confidential data, so it is necessary to assure that an unauthorized user could not access such information and prevent it from hacking attacks. The best way to secure transmit data is use of encryption method by encoding and decoding. In this manner, both routing and sensed data information should be maintained in secure way.

Data Integrity:

It assures that exact data sent by sensor on the network without any change. It means no modification or reordering in received data by any compromised nodes. The integrity of data is very important security issue because data send by one node should properly reached to destination without any change or inserting false data to the aggregated data.

Performance measure of Data Aggregation [6]
Energy Efficiency: If the functionality of the network is maximized, then data aggregation scheme is efficient in terms of energy.

Network Lifetime: The total number of data fusion rounds defines the network lifetime.

Latency: Latency is evaluation of time delay when data or message is send by sensor nodes and received by base station (sink) is experienced by the system.

Communication Overhead: It is the calculation of communication complexity of the network fusion algorithm.

Data Accuracy: Evaluation of ratio of total number of readings received at the base station (sink) to the total number of readings generated.

III. DATA AGGREGATION ATTACKS IN WSN

WSNs are vulnerable to different attacks due to the transmission medium nature, remote and hostile deployment of sensor nodes, and the lack of security mechanism. In this section, following are the attacks that affect the aggregation in the WSN [7].

A. *Replay Attack*

In this type of attack, the validated data is maliciously repeated by an adversary who misleads the aggregator, affecting the results.

B. *Denial of Service Attack*

DOS is an attack in which there is an attempt to make a network resource or machine inaccessible to its users, also called as jamming. From the aggregation point of view, an example of DoS can be an aggregator node that don't aggregate the data and prevents data from reaching querier [8].

C. *Sybil Attack*

The attacker in Sybil attack can create multiple identities within the network. It affects aggregation schemes by generating one or more identities and makes the base station accept the aggregated value.

D. *Sinkhole Attack*

Sink is a high capability resource node. So attacker places himself in a network with high capability resources in order to confuse other nodes. As a result all data passed to attackers [8].

IV. DATA AGGREGATION APPROACHES

Data aggregation is a process of gathering and aggregating the data using data aggregation approach. Several different Data aggregation are as follows:

A. *Tree-Based Approach*

In this approach perform aggregation by constructing an aggregation tree, which may be a minimum spanning tree, rooted at sink and source nodes are considered leaves. Each node has a parent node to send its data. The flow of data starts from leaves nodes up to the sink (BS) and therein the aggregation done by parent nodes [9]

Base Station

Cluster Head
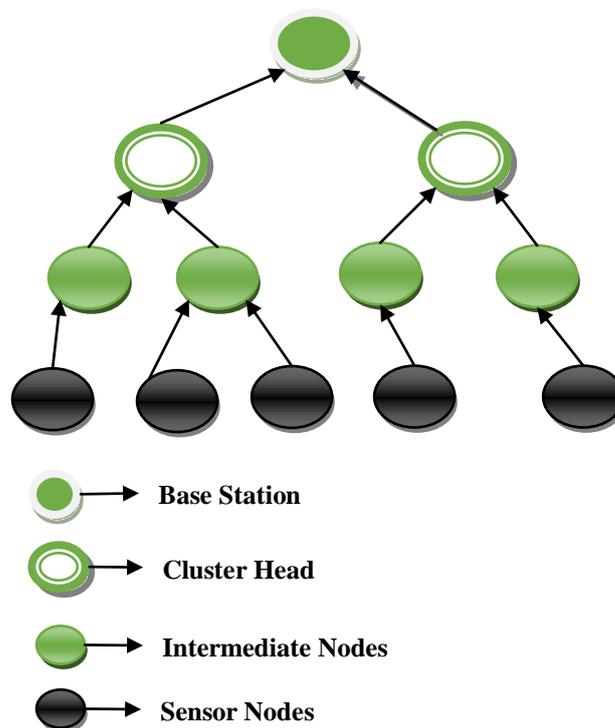
Intermediate Nodes

Sensor Nodes

Fig 3: Tree Based Approach

B. *Cluster-Based Approach*

In cluster based approach the whole network is divided into several clusters. The sensor nodes themselves form a cluster and elect a node as cluster head. The data sensed by the sensor nodes are passed to the cluster head and in the cluster head data aggregation is performed. Cluster head performs data aggregation and forward the data to the sink. In Cluster based approach, data aggregation is performed by cluster heads. Communication cost is reduced since only aggregated results reach the base station [10].

C. *Centralized Approach*

Centralized data aggregation approach is an address centric aggregation approach where each sensor nodes sends the sensed data to the central node or cluster head using the shortest path. The sensor nodes simply send the data packets to a leader, which is the powerful node. The leader aggregates the data which can be queried [11].
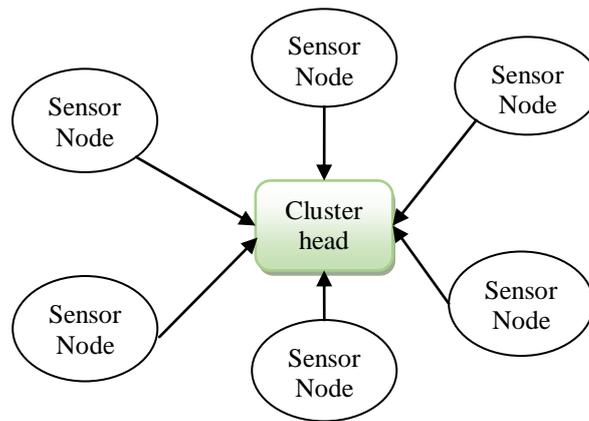
Fig 4: Centralized Aggregation Approach

D. Decentralized Approach

All sensor nodes play aggregator function to the sensed data. Here single centralized aggregator node is not available, but all nodes have the same priority to aggregate the sensed data. Also, all sensor nodes are connected to their neighbor node. This methodology has the benefit of more scalability, dynamic change node failure in the (WSNs).
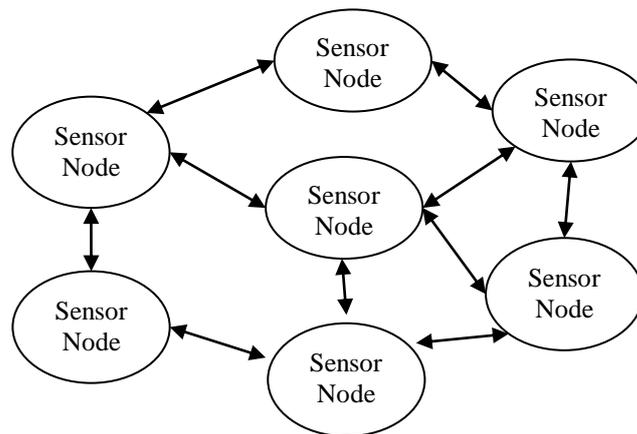
Fig 5: Decentralized Aggregation Approach

V. COMPARISON OF DATA AGGREGATION METHODS [9]

Parameters	Hop-by-Hop Data Encryption	End-to-End Data Encryption
End to End Privacy	No	Yes
Data Integrity	Maximum Data Integrity	Minimum Data Integrity
Delay	Delay with Aggregation	Delay without Aggregation
Aggregation Performed on	Plain Sensor Node	Encrypted Sensor Node
Computational Cost	Low	High
Energy Consumption	High	Low
Data Secrecy	Less Required	High Required
Vulnerable to attack	More to Passive attack	More to Active attack

VI. LITERATURE REVIEW

Miao et al. [12] proposed to utilize mobility for joint energy replenishment and data gathering. A multi-functional mobile entity, called SenCar was employed, not only as a mobile data collector roaming over the field to gather data via short-range communication but also as an energy transporter that charges static sensors on its migration tour via wireless energy transmissions.

Celestine, J., et al. [13], the proposed flooding protocol can enhance the security while conserving energy by adding complexity that makes it difficult for an adversary to identify the real packets. Despite the novelty, accuracy and efficiency of this protocol, its use in large and critical WSNs remains uncertain as it has been tested only in networks of limited size.

Shiliang Xiao et al. [14] have exploited the tradeoff between data quality and energy consumption in order to improve the data aggregation precision in case of heterogeneous per-node energy constraints.

Prabhudutta Mohanty et al [15] presents that an energy ESDAD protocol suggested, which aggregates redundant data in intermediate nodes. Waiting time for packets at all intermediate node is designed very reasonably so as to data may be aggregated proficiently in routing path. Using NS-2.30 simulation tool in this paper. The aim of imitation is to compare presentation of our proposed protocol, ESDAD, with the existing structure-free facts aggregation protocols for example SFEB and RAG that operates in a multi-hop network.

Ekta Choudhari et al. [16] proposed an advancement for IF method by providing approximation which will make them collusion robust and is converging fast. Advancement in the Iterative Filtering algorithm will enhance the performance of the system with good potential for implementation in WSN, IF algorithm is stretched with novel method for collusion detection & revocation based on an initial approximation of the aggregate values as well as distribution of differences of each sensor readings. The proposed system performance is checked through extensive simulation in C#. The RMS value in the graphs for series 2(0.1, 0.18, 0.22, 0.22, 0.22, 0.3, 0.36, 0.38) with standard deviation ranging from 0.5 to 4 shows that the proposed system performance is better as compare to existing system.

Manish V et al. [17] proposed an architecture using some parameters that affect energy consumption wireless sensor network, such as distance of nodes from sink, energy of each node. The formation of cluster is a very tedious task to form clusters, in this work presented an easy approach to form clusters and select cluster head using minimum energy. The simulation is done on energy parameter which work on an energy efficient and reliable location wise data in wireless sensor network called as EERLA and compare with two DRINA and LBERP from this result more energy will save and also it improve network lifetime.

Fei Yuan et al. [18] highlight the problem that the recent spatial correlation models of sensor nodes' data are not appropriate for measuring the correlation in a complex environment. In addition, the representative data are inaccurate when compared with real data. Thus, we propose the data density correlation degree, which is necessary to resolve this problem. The proposed correlation degree is a spatial correlation measurement that measures the correlation between a sensor node's data and its neighboring sensor nodes' data. Based on this correlation degree, a data density correlation degree (DDCD) clustering method is presented in detail so that the representative data have a low distortion on their correlated data in a WSN. In addition, simulation experiments with two real data sets are presented to evaluate the performance of the DDCD clustering method. The experimental results show that the resulting representative data achieved using the proposed method have a lower data distortion than those achieved using the Pearson correlation coefficient based clustering method or the α-local spatial clustering method. Moreover, the shape of clusters obtained by DDCD clustering method can be adapted to the environment.

VII. CONCLUSION

The main work of data aggregation schemes in WSN is to achieve energy efficiency and prolonging network lifetime. Since data aggregation has a trade-off relationship with delay, it is important to develop a data aggregation technique in such a way that aggregation gain could be maximized while keeping the energy consumption, delay and the computation overhead at the minimum possible. In this paper introduces a survey of wireless sensor network and data aggregation with its approaches to solve the security issues of energy.

REFERENCES

[1]   Iordanis Koutsopoulos and Maria Halkidi"Measurement Aggregation and Routing Techniques for Energy-Efficient Estimation in Wireless Sensor Networks," WiOpt 2010.

[2]   Ajay. K. Talele, Suraj G. Patil and Nilkanth. B. Chopade "A Survey on Data Routing and Aggregation Techniques for Wireless Sensor Networks" International Conference on Pervasive Computing (ICPC), IEEE, 2015.

[3]   Josna Jose, Joyce Jose and Fijo Jose "A Survey on Secure Data Aggregation Protocols in Wireless Sensor Networks" International Journal of Computer Applications Volume 55– No.18, October 2012

[4]   Vaibhav Pandey, AmarjeetKaur and Narottam Chand "A Review on Data Aggregation Techniques in Wireless Sensor Network", Journal of Electronic and Electrical Engineering Vol.1, Issue 2, 2010.

[5]   Dr. T.Ramaprabha, V.Premalatha "A Survey on Secure and Attacks of Data Aggregation in Wireless Sensor Networks" International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2016.

[6]   K.Maraiya, K. Kant, N.Gupta "Wireless Sensor Network: A Review on Data Aggregation", International Journal of Scientific & Engineering Research, April -2011,Volume 2, Issue 4.

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

[8]   Priyanka B.Gaikwad, Manisha R.Dhage "Survey on Secure Data Aggregation in Wireless Sensor Networks" International Conference on Computing Communication Control and Automation, IEEE, 2015.

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

[10]   P.N.Renjith and E. Baburaj "An Analysis on Data Aggregation in Wireless Sensor Networks" International Conference on Radar, Communication and Computing (ICRCC), 2012. pp.62-71.

[11]   NoritakaShigei, Hiromi Miyajima, Hiroki Morishita, Michiharu Maeda "Centralized and Distributed Clustering Methods for Energy Efficient Wireless Sensor Networks "Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 Vol I IMECS 2009, March 18 - 20, 2009, Hong Kong.

[12]   Miao Zhao, Ji Li, and Yuanyuan Yang, "A Framework of Joint Mobile Energy Replenishment and Data Gathering in Wireless Rechargeable Sensor Networks", IEEE Transactions On Mobile Computing,Pages 2689-2705, Vol. 13, No. 12, December 2014.

[13]   Celestine, J., et al. An energy efficient flooding protocol for enhanced security in Wireless Sensor Networks. in Systems, Applications and Technology Conference (LISAT), IEEE 2015.

[14]   Shiliang Xiao, Baoqing Li, Xiaobing Yuan, "Maximizing precision for energy-efficient data aggregation in wireless sensor networks with lossy links", Ad Hoc Networks,Elsevier, Vol 26,pages 103–113 ,March 2015.

[15]   Prabhudutta Mohanty and Manas Ranjan Kabat," Energy efficient structure-free data aggregation and delivery in WSN", Egyptian Informatics JournalElsevier ,2016.

[16]   Ekta Choudhari, Ketan D. Bodhe, Snehal M. Mundada "Secure Data Aggregation in WSN using Iterative Filtering algorithm" http://doi.org.ololo./10.1109/ICIMIA.2017.7975603

[17]   Manish V. Bhosle, Mininath K. Nighot, Somitra S. Das "An Energy Efficient and Reliable Location wise Data Aggregation In WSN" International Conference on Computing Communication Control and Automation, IEEE, 2015.

[18]   Fei Yuan, Yiju Zhan, and Yonghua Wang "Data Density Correlation Degree Clustering Method for Data Aggregation in WSN" IEEE Sensors Journal, Vol. 14, No. 4, April 2014.