ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

A Survey on Secure and Attacks of Data Aggregation in Wireless Sensor Networks

Dr. T.Ramaprabha[1], V.Premalatha[2]

Professor, Department of Computer Science and Applications, Vivekanandha College of Arts and Science for Women, Elayampalayam, Tiruchengode, Namakkal, India[1]

Full Time M.Phil Scholar, Department of Computer Science, Vivekanandha College of Arts and Science for Women, Elayampalayam, Tiruchengode, Namakkal, India[2]

ABSTRACT: Wireless sensor networks (WSNs) consist of sensor nodes. These networks have huge application in habitat monitoring, disaster management, security and military, etc. Wireless sensor nodes are very small in size and have limited processing capability very low battery power. This restriction of low battery power makes the sensor network prone to failure. Data aggregation is very crucial technique in wireless sensor networks. With the help of data aggregation to reduce the energy consumption by eliminating redundancy. In this paper we discuss about data aggregation and its various energy-efficient technique used for data aggregation in WSN.

KEYWORDS: Data Aggregation, Wireless Sensor Network, Security, Attacks.

I.INTRODUCTION

The wireless sensor network is formed by large number of sensor nodes. Sensor nodes may be homogeneous or heterogeneous. These networks are highly distributed and consist of many number of less cost, less power, less memory and self-organizing sensor nodes. The sensor nodes have the ability of sensing the temperature, pressure, vibration, motion, humidity, sound as in [1] etc. These sensor nodes consists four main units: sensing unit, processing unit, transmission unit, and power unit. For listening event, sensor nodes ere programmed. When an event occurs, by generating wireless traffic sensors inform the end point or sink node. In wireless sensor networks as the number of sensor nodes increases the chances of congestion increases near the event. There are various applications of WSN like forest monitoring, manufacturing, forecast systems, military surveillance, health, home, office monitoring and many intelligent and smart systems. WSN communication architecture shown in figure 1.

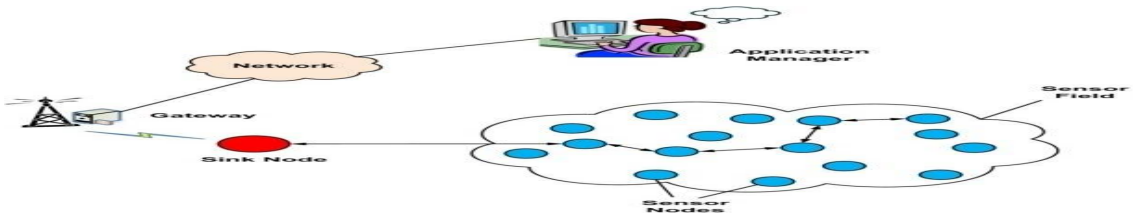

Figure 1: Communication Architecture for WSN

Data aggregation in wireless sensor networks is an important technique because it helps in minimization of energy consumption, communication overheads and tries to reduce the problem of localized congestion. It allows collecting useful data from the sensor nodes and then transmitting useful data to the end nodes or sink node. *Data aggregation* is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and provide fused information to the base station. Data aggregation usually involves the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

fusion of data from multiple sensors at intermediate nodes and transmission of the aggregated data to the base station (sink).

II. DATA AGGREGATION IN WSN

Data Aggregation is a process of combining and summarizing the data from sensor nodes in wireless sensor networks by using aggregation function such as MAX, MIN, AVG, COUNT, SUM as in [2] etc. on aggregator nodes. Data Aggregation is a process of eliminating redundant data from various sensor nodes. Data aggregation techniques as in [20] defined that how the data is to be routed on the network and processing method that are applied on the data packets. The data aggregation is a technique used to solve the implosion and overlap problems in data centric routing. Data Aggregation Techniques in WSN shown in figure 2. Data coming from multiple sensor nodes are aggregated as if they are about the same attribute of the phenomenon when they reach the same routing node on the way back to the sink.

Figure 2: Data Aggregation Techniques in WSN

Data aggregation is a widely used technique in wireless sensor networks. The security issues, data confidentiality and integrity, in data aggregation become vital when the sensor network is deployed in a hostile environment. Figure 3 illustrates that data aggregation is the process of aggregating the sensor data using aggregation approaches.

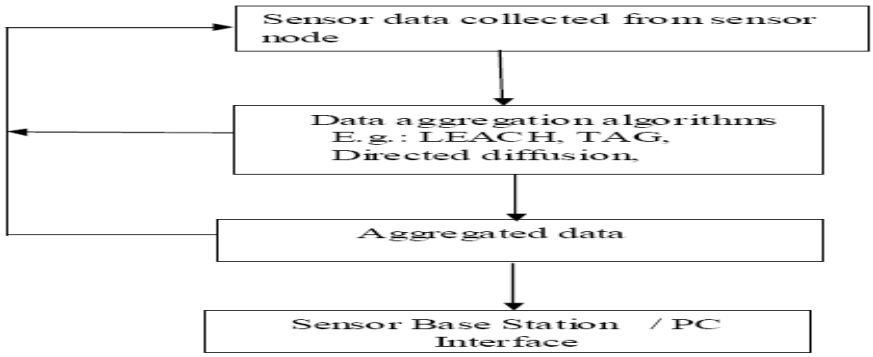

Figure 3: Architecture of Data Aggregation Process

Then the algorithm uses the sensor data from the sensor nodes and then aggregates the data by using some aggregation algorithms such as centralized approach, LEACH(Low Energy Adaptive Clustering Hierarchy), TAG(Tiny Aggregation) etc. This aggregated data is transfer to the sink node by selecting the efficient path.

III. DATA AGGREGATION BASED NETWORKS

A.Flat Networks:

In flat networks, each sensor node plays the same role and is equipped with approximately the same battery power. In such networks, data aggregation is accomplished by data centric routing where the sink usually transmits a query message to the sensors, for example, via flooding and sensors which have data matching the query send response

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

messages back to the sink. The choice of a particular communication protocol depends on the specific application at hand.

a.Diffusion:

Directed diffusion (DD) [2] may be a popular information aggregation paradigm for wireless device networks. it's a data-centric and application aware paradigm, within the sense that every one information generated by sensor nodes is called by attribute-value pairs. Such a scheme combines the information coming back from totally different sources en-route to the sink by eliminating redundancy and minimizing the amount of transmissions. during this means, it saves the energy consumption and will increase the network lifespan of WSNs. during this theme usually base station broadcast the message to the interested supply node. subsequently every node receives interest.

b.SPIN:

The sensor protocol for data via negotiation[3] The staring node that has new data advertises the data to the close nodes within the network using the meta data. A close node that is interested in this type of information sends asking to the leader node for data. The leader node responds and send data to the sinks every node has a resource managing capability to keeps track of its energy usage within the sensing element network. every node polls its resources like battery power before data transmission.

B.Hierarchical Networks:

In the hierarchical network, In which data aggregation data has to be done at special nodes, with the help of these special node we can reduce the number of number of data packet transmitted to the sink. So with this network improves the energy efficiency of the whole network. Various type hierarchical data-aggregation protocols as follows:

a.Cluster-Based Networks for data aggregation
b.Chain –Based Networks for Data Aggregation
c.Tree Based Networks for Data Aggregation

a.Cluster-Based Networks for data aggregation

These Wireless sensor network is resource constraint that's why sensor cannot directly transmit data to the base station. In which all regular sensors can send data packet to a cluster head (local aggregator) which aggregates data packet from all the regular sensors in its cluster and sends the concise digest to the base station. With the help of the scheme we save the energy of the sensors. LEACH [4]: Low energy adaptive clustering has been proposed to organise a sensor network into a set of clusters so that the energy consumption can be event distributed among all the sensor nodes.

b.Chain –Based Networks for Data Aggregation

In which each sensor sends data to the closer neighbour. Power- Efficient Data - Gathering Protocol for Sensor Information Systems (PEGASIS) is type of chain based data aggregation. In PEGASIS [5], all sensors are structured into a linear chain for data aggregation. The nodes can form a chain by employing a greedy algorithm or the sink can decide the chain in a centralized manner. In the Greedy chain formation assumes that all sensors have inclusive knowledge of the network. The farthest node from the sink initiates chain formation and, at each step, the closest neighbour of a node is selected as its successor in the chain. In each data-gathering round, a node receives data packet from one of its neighbours, aggregates the data with its own, and sends the aggregates data packet to its other neighbour along the chain.

c.Tree Based Networks for Data Aggregation

In which all node are organized in form of tree means hierarchical, with then help of intermediate node we can perform data aggregation process and data transmit leaf node root node. Tree based data aggregation is suitable for applications which involve innetwork data aggregation. An example application is radiation-level monitoring in a nuclear plant where the maximum value provides the most useful information for the safety of the plant. One of the main aspects of tree-based networks is the construction of an energy efficient data-aggregation tree.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

IV. SURVEY OF WIRELESS SENSOR NETWORKS

Several attempts were made by the researchers to study the major challenges in WSNs, security requirements of WSNs, Constraints of WSNs. That survey mentions in below Table 1.

WSNs Major Challenges	**WSNs Constraints**	**ecurity Requirements**
Mobility and topology changes Due to mobility of Sensor nodes network topology would be changed dynamically.	**Limited Physical Resources** like memory, computational power, energy (Battery).	**Availability** Networks services are available even in the presence of denial-of service attacks.
Energy constraints Limited battery power of small tiny sensor nodes.	**Scalability-** The protocols must be scalable enough to respond and operate with such large number of sensor nodes.	**Authentication** a malicious node cannot masquerade as a trusted network node.
Security Issues All the traditional networks security approaches are cannot directly apply on WSNs.	**Quality of Service** the data should be delivered within a certain period of time from the moment it is sensed otherwise the data will be careless.	**Confidentiality** a given message cannot be understood by anyone other than the desired recipients.
		Integrity a message sent from one node to another is not modified by malicious intermediate nodes.
		Authorization Only authorized sensors can be involved in providing information to network services.

Table 1: A Survey for Wireless Sensor networks

V. SECURITY NEEDS IN DATA AGGREGATION

Data Aggregation in wireless sensor network is an important technique as well as security to aggregated data is an important issue. In some important application such as military surveillance and various life critical application data transmission, data aggregation, and data reception should be in a secured and energy efficient way. So to achieve this many facts should be considered such as: Confidentiality of Data, Integrity of Data, Freshness of data, Source Authentication, and Secure Node localization [5].

A. **Secure on WSN Aggregation:**

a. Confidentiality of Data: It assures that an unauthorized user could not access the private or confidential information and data should be prevented from passive attack. By using secret key data can be encrypted and sent to the receiver node. Both routing information and sensed data should be maintained in secure way.

b. Integrity of Data: Integrity of data assures that the data on the network are changed only by authorized user not any compromised nodes. It means that, there is no modification, reordering in the received

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

data. It ensures that data which have to send should not be corrupted before reaching the destination. This is very important issue because compromised node can change the data by inserting false data to the aggregated data.

c. Freshness of Data: Data freshness is necessary to prevent the reply of old messages at aggregator node. Performance of network and energy can be effectively used by achieving data freshness.

d. Secure Node localization: Node localization is very important issue in WSN so it should be kept secure and should not be accessed by malicious node. If location of sensor node is revealed to malicious node then all routing information also revealed so node location should be secure.

e. Source Authentication: Data Authentication ensures that received data should be the same as original data. Source authentication allows that the data is sent only by the actual sender. Source authentication can prevent the data from Sybil attack in which an attacker gain access to any node and capture the stored information.

B. Attacks on WSN Aggregation:

On wireless sensor network various kind of attacks are possible because it deployed in the environment which is not secure and have less physical security to the sensor nodes. On different schemes different type of attacks are performed by the adversary to break the security [19]. There is brief discussion of these attacks given below:

a.Node Compromise attack: In this type of attack the attacker gain control over the deployed sensor node and takes information stored on the sensor nodes. Compromised node can insert the false data bit in the already stored true data. If an adversary gain access to the aggregator node then data is not secured in the network.

b.Sybil Attack: In this attack attacker can make multiple identities and affects various data aggregation techniques in many ways. After creating multiple fake ids, it participates in election of aggregator nodes and tries to elect the malicious node as aggregator node. After that it affects the data at the aggregator node.

c.Denial of Service attack: In this type of attack, attacker jams the signal through interfere the radio frequencies by transmitting radio signals on the network. In this attack the aggregator node refuses to aggregate the data gathered from various sensor nodes and helps data from routing in upper levels.

d. Selective Forwarding Attack: Normally sensor nodes forward the data which it receives from other sensor nodes. But in this attack the compromise node does not do that and affect the data at aggregator node. Any compromised node can launch the selective forwarding attack.

e. Replay Attack: In this from the network attacker takes control on the traffic and record the traffic. After that mislead the aggregator node by replays the recorded traffic and affects the result which is aggregated from the aggregator node.

f. Injection Attack: In this the attacker injects the wrong data into the network. In the process of aggregation this wrong data will result in false aggregated data. Some types of attacks and that causes areshown in below Table 2.

Attack	**Cause**	**Solution**
Denial of service attack	By making interference with radio frequency	By using MAC and spread spectrum techniques
False packet, Malleability attack	Due to injection of malicious nodes	By using HMAC
Replay Attack	Without data freshness transmitting same data	By using time stamp to all data packet

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Physical Attack	Due to lack security of symmetric key approach	Use of Asymmetric public key approach
Energy Drain attack	Due to energy depletion	By making use of several energy harvesting techniques as: solar power.
Sybil attack	By making multiple false identities	By using authentication technique
Sinkhole Attack	By attracting traffic to the specific compromised node	By using proper routing and localization information
Sniffing Attack	Because of capturing data by using malicious nodes	By using protocols with confidentiality of data
Data Integrity Attack	Bye inserting false data	Use of digital signature scheme

Table 2: Overview of attacks and security mechanism

VI. SECURITY ISSUES IN DATA AGGREGATION

Data aggregation in Wireless sensor Network refers to exploit the sensed data from the sensors to the gateway node. data aggregation plays a significant role in Wireless Sensor Networks since the aggregation schemes followed here involve in reducing the amount of power consumed throughout data transmission between the sensor nodes within the data aggregation of WSN, 2 security requirements, confidentiality and integrity, ought to be consummated. Specifically, the fundamental security issue is data confidentiality, that protects the sensitive transmitted data from passive attacks, such as eavesdropping. data confidentiality is especially very important in a hostile environment, where the wireless channel is at risk of eavesdropping. though there are many methods provided by cryptography, the difficult encryption and decryption operations, like modular multiplications of large numbers in public key primarily based cryptosystems, will assign the sensor's power quickly [8]. the other security issue is data integrity, that prevents the compromised source nodes or aggregator nodes from considerably altering the final aggregation value [9]. sensor nodes are easy to be compromised because they lack expensive tampering-resistant hardware, and even that tampering-resistant hardware may not continually be reliable. A compromised node will modify, forge or discard messages.

VII. CONCLUSION

Wireless Sensor Networks is very useful in various applications such as military surveillance, health, home, office monitoring and in many intelligent and smart systems. In Wireless Sensor Networks there are several issues to the security of the network and secure data aggregation is also a big issue. This paper introduces a brief discussion of wireless sensor network, data aggregation, various attacks of data aggregation in WSN, Security needs to data aggregation, overview of WSN and some networks based data aggregation in WSN.

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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

2. 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.
3. P. D. Patel, P.B. Lapsiwala, R.V. Kshirsagar "Data Aggregation in Wireless Sensor Network", International Journal of Management, IT and Engineering, vol. 2, Issue 7 July-2012.
4. Kiran Maraiya, Kamal Kant, Nitin Gupta "Architectural Based Data Aggregation Techniques in Wireless Sensor Network: A Comparative Study", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 3 Mar 2011.
5. Vaibhav Pandey, Amarjeet Kaur and Narottam Chand "A review on data aggregation techniques in wireless sensor network", Journal of Electronic and Electrical Engineering, ISSN: 0976–8106 & E-ISSN: 0976–8114, Vol. 1,Issue 2, 2010.
6. Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", Proceedings of the 33rd Hawaii International Conference on System Sciences IEEE, 2000.
7. Stephanie Lmdsey and Cauligi S. Raghavendra "PEGASIS: Power-Efficient Gathering in Sensor Information Systems", IEEE 2002.
8. 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.
9. H.Alzaid, E. Foo, J. G. Nieto, "Secure Data Aggregation in Wireless Sensor Network: a survey", Australasian Information Society Conference, vol. 81, Jan-2008.
10. Guorui Li, Ying Wang "efficient Data aggregation scheme leveraging time series prediction in WSN" International Journal of Machine learning and Computing Vol.1. No.4. October 2011.
11. Shen Xueli , Wu Wenjum ,"The Research Of Data Aggregation In Wireless Sensor Networks", International Forum Of Information And Technology, IEEE Computer Society, 2010.