Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Secure Data Aggregation in Wireless Sensor Network

Jyoti Rajput
M.Tech, Dep. of CSE
Graphic Era Hill University
Dehradun, India

Naveen Garg
H.O.D, Dep. of CSE
Graphic Era Hill University
Dehradun, India

Abstract—In Wireless Sensor Network Data Aggregation is an important technique to achieve power efficiency in the sensor network. In some application such as: wireless sensor network, data mining, cloud computing data aggregation is widely used. Because sensor node has limited battery power so data aggregation techniques have been proposed for wireless sensor networks. A challenge to data aggregation is how to secure aggregated data from disclosing during aggregating process as well as obtain accurate aggregated results. In this survey paper we described various protocols for securing aggregated data in wireless sensor networks.

Keywords— Wireless Sensor Network, Data Aggregation, Security needs, Attacks, Security protocols

1. 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. 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.

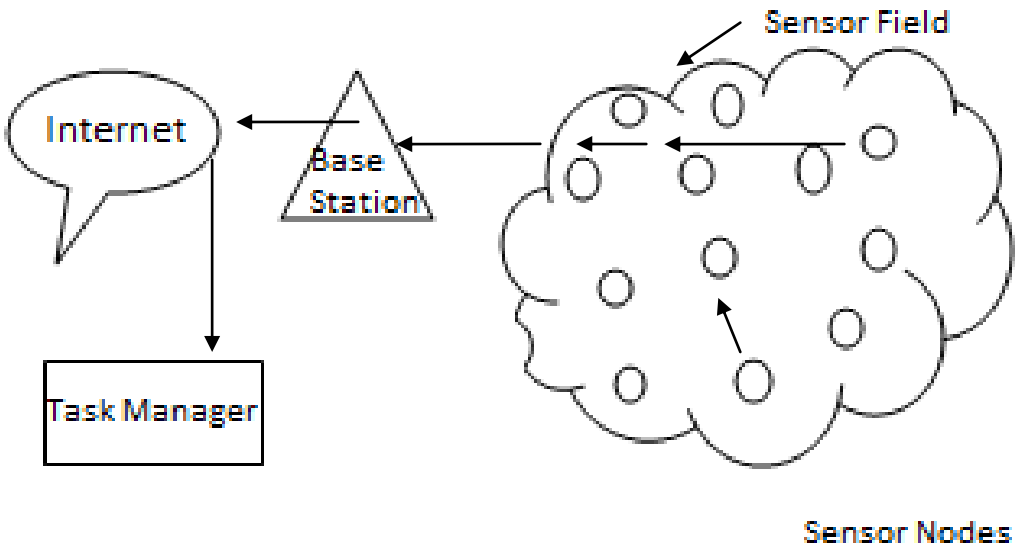

Fig1.Communication Architecture for WSN

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.

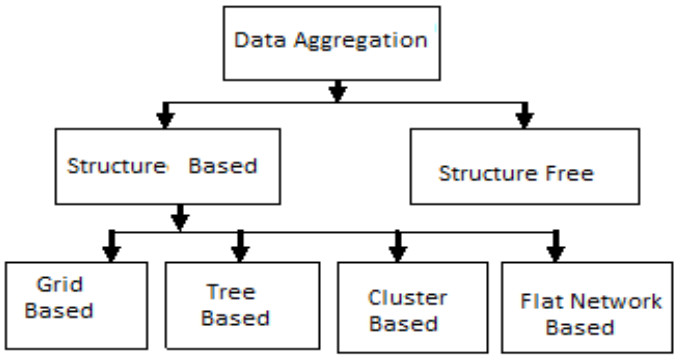

Fig2.Data Aggregation Techniques in WSN

A. Data Aggregation Approaches:

There are various approaches of data aggregation [3] some are as follows:

1) Centralized Approach: In this approach only one sensor node play a role of aggregator node and all other sensor nodes are connected to that aggregator node. All other sensor nodes sense the data and transmit to the aggregator node which is called centralized node. There are so many loads on that aggregator node, so there is need of more energy and security on that aggregator node because all data is on the centralized aggregator node.

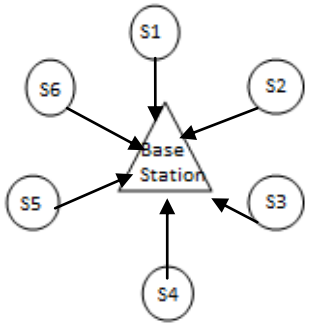

Fig3. Centralized approach for data aggregation in WSN

2) Decentralized Approach: In this approach all sensor nodes performs aggregator function to the sensed data .In this approach there is no single centralized aggregator node but all nodes have same priority to aggregate the sensed data. In this approach all sensor nodes are connected to their neighbor node. This approach has the advantage of more scalability, dynamic changes node failure in the wireless sensor network.

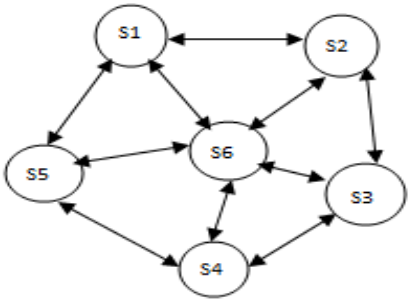

Fig4. Decentralize approach for data aggregation in WSN

*3) In network Aggregation Approach***:** In this approach one or more node can be aggregator node means sub-aggregator node. This approach aggregates multiple data into single data. It is important for improving the network lifetime and reduces the size of transmitted data on the network.

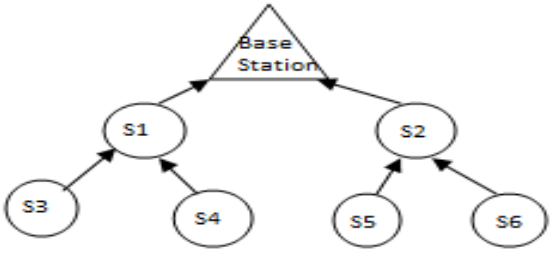

Fig5. In network aggregation approach in WSN

B. Data Aggregation Function in WSN:

For aggregation of sensed data various aggregation function is needed and related to sensor network application such as: Max (Maximum), Min (Minimum), Avg (Average), Count, Sum, Median [4] etc.

TABLE 1: DATA AGGREGATION FUNCTION

Duplicate Sensitive	Duplicate Insensitive	Lossy	Lossless
Avg	Min, Max	Median	Sum, Count

C. Performance Metrics of Data aggregation:

There are several performance measures [4] given below:

TABLE 2: PEFORMANCE MEASURES OF DATA AGGREGATION

Energy Efficiency	**Network lifetime**	**Data Accuracy**	**Latency**	**Communication Overhead**
Energy is effectively used. Increased efficiency of the network.	Increased lifetime of network.	It means correctness of data. Good data accuracy.	It means delay between data sending reception. Less Delay	It means complexity of the network and depends on the aggregation method.

III. 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].

1) 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.

2) 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 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.

3) 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.

4) 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.

5) 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.

A. 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:

1) *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.

2) *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.

3) *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.

4) *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.

5) *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.

6) *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.

TABLE3. OVERVIEW OF ATTACKS AND SECURITY MECHANISM

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
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

IV. **OVERVIEW OF SECURITY PROTOCOLS**

In wireless sensor network security is a big challenge because sensor nodes are deployed in hostile environment, vulnerable to physical attacks and can be compromised by an attacker. Data aggregation in WSN is also an important issue for security to maintain the data confidentiality, data integrity, data freshness, data authentication. Various approaches for secure data aggregation are described as:

In Secure Information Aggregation (SIA) [6], various approaches are used such as "aggregate-commit-prove" in this approach aggregator's help for computing aggregated data of various sensor nodes reading and to base station with aggregated result to gather with a commitment to collection of data and home server (BS) can verify the correctness of data. This paper provided technique for securely computing the median, minimum and maximum values, average of measurements. This protocol need only sub-linear communication between aggregator and user, proposed a scheme for forwarding secure authentication to confirm that there is no change in sensor previous reading the sensor has recorded, even if an attacker corrupts sensor nodes at a point. In a Tiny Aggregation Service (TAG) [7], this is data aggregation service without any provision for security. This paper proposed aggregation in low-power, distributed, wireless environment. This approach provided two attribute: first, it provided a basic, declarative, medium for data gathering and aggregation which is inspired by selection and aggregation facilities in data base query language. Second, it distributes executes aggregation queries in the sensor network. It is sensitive to lossy communication and resource constrained properties of WSN. This service discards irrelevant data and combines relevant data into more compact records.

In Synopsis Diffusion for Robust Aggregation in Sensor Networks [8], this paper designed an aggregation framework called synopsis diffusion. This is in network aggregation scheme and it avoids double counting by using "order-and duplicate-insensitive (ODI) synopses" that summarize intermediate result. Both ODI synopsis and synopsis diffusion has the property of creating elusive acknowledgement of packet delivery.

In A Secure Hop-by Hop Data Aggregation Protocol (SDAP) [9], this protocol is based on "divide and conquer and commit and attest" principles. First to divide the sensor nodes in a tree topology of similar sizes it used a novel probabilistic grouping technique. For security reason base station identifies the dishonest groups which are based on the set of group aggregates. This protocol is applicable to multiple aggregation function.

In A Secure Data Aggregation and verification Protocol (SDAV) [10], this paper designed two sub-protocols. First protocol used verifiable secret sharing of cluster keys in sensor network by using Elliptic Curve Cryptography (ECC). Second, designed Secure Data Aggregation and Verification Protocol. In this protocol base station never accepts false aggregate data and by using Merkle Hash Trees, it checks integrity of data.

In Secure and Efficient protocol for Data Aggregation (SEDAN) [11], this paper developed two hops verification mechanism for data integrity. This scheme does not require base station to verify and detect mistakes in aggregated results, and each node can verify integrity of data of two hops away neighbors and aggregation of immediate neighbors. This scheme is beneficial to avoid useless transmission of bogus data and saves energy of sensor nodes.

In Reputation-based Secure Data Aggregation (RSDA) [12], this paper focused on data availability and data accuracy. By integrating aggregation functionalities it enhance the network lifetime and accuracy of aggregated data. The area is divided into smaller cells of equal size where RSDA is implemented. In order to filter out the inconsistent data in presence of multiple compromised nodes, each sensor nodes evaluates the behavior of its cell member by monitoring neighborhood's activities. This approach is required to detect compromised nodes and black list them and helps to extend network life time and protect the accuracy of aggregated data.

In Secure Hop-by-Hop Aggregation of End-to-End Concealed Data [13], this paper presented an efficient heuristic approach for checking data integrity and cost effective heuristic based divide and conquer (declared to be true) process, which has complexity O (ln n) in average, and O(n) in the worst case. In this approach base station used O (1) heuristic to verify final aggregation data.

Secure Data Aggregation with MAC Authentication in Wireless Sensor Networks [14] this paper represents a novel way to provide confidentiality and integrity preserving aggregation in wireless sensor network. This scheme uses homomorphic encryption Elliptic Curve Elgamal) algorithm to achieve data confidentiality and an homomorphic MAC algorithm based on message authentication code to achieve integrity of the data.

Secure End-to-End Data Aggregation in Wireless Sensor Networks [15] this paper represents a protocol for secure data aggregation, called secure end-to-end data aggregation, it provides end-to end data privacy of the aggregated data, the data is encrypted at sensor nodes and decrypted by the base station .This protocol uses additive homomorphic encryption technique for encryption of the data.

Secure Data Aggregation in Wireless Sensor Networks [16] this paper presents synopsis diffusion approach, this approach secure against the false data injection attacks in which malicious nodes inject wrong sub-aggregate values and a rare featherweight verification algorithm by which the base station can determine any wrong contribution in computed aggregate data.

Secure and Efficient Data Aggregation for Wireless Sensor Networks [17] presented the Leaf Node Representation Scheme (LNR) to solve ID problem in key stream-based encryption for WSN with static tree architecture, in this scheme leaf's node id can represent other node's id in its route to the base station. The Delayed Hop-by-hop Authentication Scheme (DHA*)* guarantee the data integrity for WSN with dynamic cluster based architecture and it uses individual key for data encryption.

A New Approach to Secure Data Aggregation protocol for Wireless Sensor Networks [18] represented the approach which is based on revelation and clarification duplicitous sensor nodes with their sensed data. It uses outlier detection algorithm to find and clarify out the outlier sensor nodes. It provides high outlier revelation rate because to the use of distributed approach. It uses MAC for authentication of data and integrity of data. For providing confidentiality to data, symmetric encryption approach is used in this paper.

TABLE4.COMPARISION OF SECURITY PROTOCOLS OF DATA AGGREGATIONIN WSN

Protocol	Architecture	Data confidentiality	Data Integrity	Data Authentication
TAG[7]	T	-	-	-
SIA[6]	T	+	+	+
SDRA[8]	G	+	-	-
SDAP[9]	T	+	+	+
SDAV[10]	T	+	+	+
SEDAN[11]	T	-	+	+
RSDA[12]	G	-	+	+
[13]	T	+	+	+
[14]	C	+	+	+

Explanation of Symbols: T (Tree), C (Cluster), G (Grid), - (No), + (Yes)

VI. 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 approaches of data aggregation in WSN, Security needs to data aggregation, overview of various security protocols and their comparison.

ACKNOWLEDGEMENT

During the time of writing of this paper I received support and help from many people. In particular, I am thankful to my supervisor, Mr. Naveen Garg at Computer Science department of *GRAPHIC ERA HILL UNIVERSITY***,** who was very generous with his time and knowledge and assisted me in each step to complete the paper. I am grateful to all my friends for their encouragement.

REFERENCE

[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] 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] N.Sugandhi, D.Manivannan "Analysis of Various Deterioration Factors of Data Aggregation in Wireless Sensor Networks", International Journal of Engineering and Technology, ISSN: 0975-4024 Vol. 5 No 1 Feb-Mar 2013

[4] 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

[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] B.Przydatek, D.Song, and A.Perrig"SIA: Secure Information Aggregation in Sensor Networks" in Proc. ACM conf. Embedded Network Sensor Systems, 2003

[7] S.Madden, M.J Franklin, and W.Hong "TAG: A Tinny Aggregation Service for Ad-Hoc Sensor Networks" in Proc. 5th Annual Symposium on Operating Systems Design and Implementation, Dec-2002

[8] S.Nath, P.B.Gibbons, S.Seshan, and Z.R.Anderson "Synopsis Diffusion for Robust Aggregation in Sensor Networks" in Proc. ACM conf. Embedded Network Sensor System Nov-2004

[9] 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

[10] A.Mahimkar, T.S.Rappaport "A Secure Data Aggregation and verification Protocol for Sensor networks", IEEE Communications Society Globecom 2004

[11] M.Bagaa, N.Lasla, A. Ouadjaout, Y.Challal, "Secure and efficient protocol for Data Aggregation in wireless sensor networks", 32nd IEEE Conference on Local Computer Networks, 2007

[12] 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, 2008

[13] E.Mlaih, S.A.Aly "Secure Hop-by-Hop Aggregation of End-to-End Concealed Data in Wireless Sensor Networks"in IEEE international Conference, 2008

[14] 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

[15] A.S.Poornima, B.B.Amberker "Secure End-to-End Data Aggregation in Wireless Sensor Networks", in IEEE international Conference, 2010

[16] S.Roy, M.Conti, S.Setia, and S.Jajodia, "Secure Data Aggregation in Wireless Sensor Networks", in IEEE International Conference, 2012

[17] X.Wang, J.Li, X.Peng, and B.Zou "Secure and Efficient Data Aggregation for Wireless sensor Networks", in IEEE International Conference, 2010

[18] M.K.Jha, T.P Shrama, "A New Approach to Secure Data Aggregation protocol for Wireless Sensor Networks", International Journal on Computer Science and Engineering, vol. 2, No. 5, 2010

[19] H.Alzaid, E. Foo, J. G. Nieto, "Secure Data Aggregation in Wireless Sensor Network: a survey", Australasian Information Society Conference, vol. 81, Jan-2008

[20] 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

