International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

# Appraisal of Secure Data Aggregation protocol for Wireless Sensor Network (WSN)

**Sunil kumar[1], Priyanka jangra[2]**

[1,2]*Dept. of Electronics and Communication Engineering, U.I.ET (KUK), Kurukshetra, Haryana (India)*

---

**Abstract:-** *Wireless sensor networks (WSNs) have widely used for many applications such as military, hospital, agriculture, and in other commercial applications [7]. WSN is the group of homogenous sensor nodes. Each node has provides a few amount of energy. The largest part of the energy of sensor nodes are expends for data aggregation. Energy expended by the cluster head be additional than the sensor node. For WSN it is necessary to check the truth worthiness of data & reputation of sensor nodes. Consider the security is the very most important issue in WSN. Initially we demonstrated the data before the data aggregation by the cluster head. The most important goal of this paper to be present a state of the survey on secure data aggregation algorithms reported in the literature of WSNs.*

**Key words: WSN, data aggregation, security, sensor node etc.**

## 1. INTRODUCTION

In WSNs repeatedly consider many sensor nodes. Which have lower cost, limited energy resources and fixed memory and communication capabilities [8]. Sensor nodes are deployed at random and huge scale [10]. These networks mainly used for observes bodily or natural conditions i.e. temp, pressure, echo, vibration at critical locations. Since WSNs are generally dissemination in distant as well as aggressive environments and used to broadcast perceptive information [8].

Power executive is extremely essential issue in allowing for wireless sensor network and it has been to facilitate that the communication cost of the nodes is larger than the computation. Because nodes are spends larger energy in communication. Thus we will deploy the sensor nodes must closely to each other [13]. If we reduce the no. of transmitted bits then the network lifetime will increase [1]. Figure illustrates the architecture diagram of WSN.

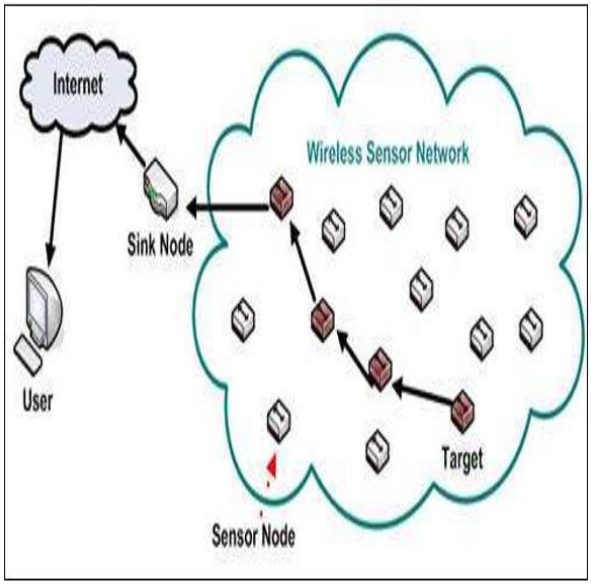


Figure 1.1 Architecture diagram of WSN [12]

### 1.1 Features of WSN

- Less costly
- Less power consumption
- End-to-end quality of service
- connectionless procedure
- context changes

### 1.2 Challenges of WSN

- Security
- Coverage area of nodes
- Mobility of nodes

## 2. DATA AGGREGATION

In WSN data transfer directly to the sink node is able to increase various problems. In WSN, the data aggregation is vital role for saving the energy of sensor nodes [2]. In Data aggregation method consists of larger no. of sensor nodes and an Aggregation Node. Each nodes have own energy and power. The averaging method is the simplest method used for data aggregation, in this method we collects the

data from numerous sensor nodes and calculate its averages (MIN/MAX, VARIANCE, MEAN etc.) then send to the base station [9]. Thus the data aggregation drastically reduces the total quantity of Data which transmitted to the base station, and total amount of energy will decreases so the network lifetime will increased [5]. When compromise attacks are there in the network then the averaging technique is highly vulnerable [9].

Data aggregation (DA) procedure consists of two tasks data gathering and routing. Information gathering technique is the mainly essential for the Wireless Sensor Network. In WSN data is gathered via sensor nodes furthermore these gathered data is transfer to the base station (BS) [10].

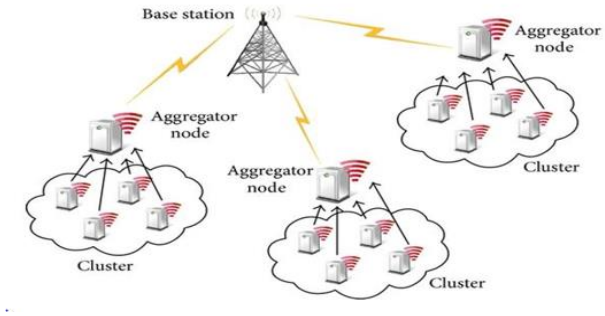


Figure 1.2 Data aggregation of WSN

There are the two types of approaches are used for data aggregation in WSN. (a) Cluster based approach. (b) Tree based approach. Both approaches are very high vulnerable due to communication link failure. To overcome this problem we divide the information into multiple shares. These shares are transmitted through multiple disjoint paths [16].

If we secured such a network, it is significant to reducing the amount of computationally costly security operations with no compromise lying on the security [2].

## 2.1 Types of attacks in WSN

### 2.1.1 Denial o/Service Attack

The sensor nodes sense the data and broadcast it to the top level node. Several compromise nodes may reject the sensing data to the top level node. But it didn't found any data through a time constraint; it will continuously broadcast all the previous data. Inside this type of attack various information are lost.

### 2.1.2 False data injection Attack

The main objective of this type attack is to add fake data and totally change the last data of the BS. Two schemes are generally used to avoid such type of attacks. One is passive, which provide the safety of every sensor data as well as safely data confidentiality. Another is active, which dynamically senses all the data from sensor nodes with makes confidentiality all the sensor data reduce into certain limit.

### 2.1 3 Syb/i Attack

The attacker disguises it because an applicable sensor are used in WSN, with usually the only one unacceptable node can participate in data aggregation procedure, hence to facilitate it can attack the network from a huge enlarge exclusive of detect.

### 2.1.4 Replay Attack

Attackers are continuously known about the last information of sensor node in the network. Which effect the freshness of the data and base station cannot obtain the original data from the sensor node? To overcome this problem a mechanism is design in which the information is transmitted by each sensor node.

## 2.2 Security Issues in WSN

***Data confidentiality:*** It requires every sensor nodes might be transmit data confidentially without being eavesdrop or tamper. Generally confidentiality of the data preserve reliable during key-based system. Only sender and receiver know the data. There are many attacks related to confidentiality such as stealthy attack, eavesdropping attack, and false data injection attack.

***Data integrity:*** In the integrity problem the received data will not tamped between the sender and receiver path. The stealthy attack in the network is due to data integrity problem.

***Data freshness:*** Data freshness make convinced that the entire information which sends to the BS or higher level sensor node will fresh by reflect the current condition. Replay attack will destroy networks data freshness.

***Data availability:*** In this condition the sensor nodes may possibly broadcast all data to the base station in a suitable mode. Denial of service attack will be avoiding the transmitted data.

***Authentication:*** Two types of authentication in WSN. (a) Data authentication. (b) Sensor node authentication. Authentications are requiring getting the trustworthiness of data from sensor nodes and reflect trustworthy information. Sybli attack avoids the authentication of data in the network.

## 3. SECURE DATA AGGREGATION

In WSNs the sensor nodes could be deployed in distant as well as aggressive environments. So many attacks are there on the data and attacker can insert the false data into the original information. The fake values not detected in aggregation process [8]. Where the security with data integrity are more preferred.

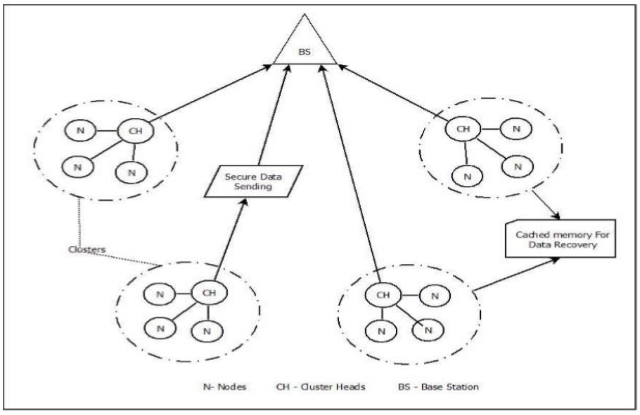


Figure 1.3 Secure data aggregation in WSN [15]

Also, nodes that perform the aggregation function are most attractive to attackers. In given system cache memory is provided by the cluster head for recovery of data loss. Therefore, secure data aggregation in sensor networks, based on several encryption techniques as show in literature survey.

The inadequate resources of sensor nodes construct the choice of an encryption algorithm extremely essential for providing security for data aggregation. Asymmetric cryptography involves huge cipher texts and important computations although solves, on the other hand, the difficulty of key distribution of symmetric one [6].

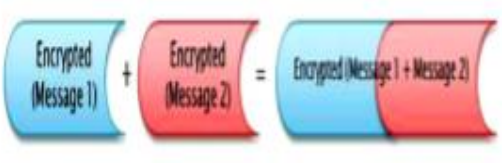


Figure1.4 Encryption of two messages

For secure message communication cryptography is used in sensor network. Inside this approach we disjointedly the information into various shares and transmit the dissimilar shares during many disjoint paths between senor nodes to sink node (base station). The original message is reconstructed at the receiver end by adding together these shares during multiple paths.

## 4. LITERATURE SURVEY

A.S.Poornima et.al [1] proposed SEEDA protocol for secure data aggregation in WSN. This protocol provides the confidentiality of data. The protocol uses best quality of hop-by-hop that is amount of bits transmitted.

Vimal Kumar et.al [2] estimates the performance of such an end to end security algorithm. Presents our results from the performance of the algorithm on mica2 motes and conclude how it is enhanced than traditional hop by hop security. In further decreasing the number of transmissions in the network and therefore will rise the network lifetime.

Mingxin Yang et.al [3] which consider of three parts. First, the typical K-average clustering algorithm to the phase of cluster distribution which is the first step of the aggregate tree. Second, the cluster head node and the cluster set nodes are constructed such that depend on the entropy formula H (Sg|x)<Fg(c) and pseudo-random function. To conclude, we study the secure data fusion method with the nodes.

Jailin.S et.al [4] proposed hybrid cryptography named DSAA used to verify an individual in an indoor situation. Normally the authentication method is done on sink level. However the proposed technique will lead to perform relationship of Message Digest on the node level itself, which reduces the communication overheads.

Jia Guo et.al [5] the secure data aggregation scheme is divided into two ways. One is hop by hop and another end to end data aggregation. Consequently the secure data aggregation procedure be review through analyze based on four phases: bootstrapping, data aggregation, confirmation as well as remedy.

Merad Boudia Omar Rafik et.al [6] proposed (SA-SPKC) scheme is a unique security procedure which regularly provides the security for WSNs additional where the base station be able to confirm the individual data as well as discover the malicious node. Our method is based on stateful public key encryption (StPKE).

Bharath K. Samanthula et.al [7] by using probabilistic encryption method proposed two solution used for strongly calculating MIN/MAX function into WSN. The duplicate sensor reading is rejecting through first solution in WSN. But second solution acts as a standard method. Since a future work, we will enhance the efficiency of the standard method by decreasing the size of the encoding matrix by heuristics and dimensionality decreasing techniques.

Soufiene Ben Othman et.al [8] the new approach uses homomorphic encryption EC-OU algorithm to accomplish data confidentiality for network aggregation and contain an ESDSA based algorithm called additively digital signature algorithm used to attain integrity of the data. The performance estimation shows that the proposed scheme is capable as well as scalable intended for huge WSNs.

Mohsen Rezvani et.al [9] proposed an improved iterative filtering technique whereas considerably more robust than the simple averaging methods. Which makes them not only collusion robust, but have more accuracy and faster converging? This technique can be used for deployed sensor network.

M.Thangaraj et.al [10] Proposed scheme Secured Hybrid (GA-ABC) Data Aggregation Tree (SHDT) used for increasing the energy efficiency of sensor network. Proposed results show that this scheme practically will enhance the network lifetime than the other method.

Sankardas Roy et.al [11] the attack possibly will reason when huge no. of errors calculates on the base station. Proposed an algorithm to facilitate the base station to securely calculate predicate count with sum still in the presence of such attack. In the resilient algorithm calculate the accurate aggregate through filtering out the aid of compromised node.

S.Archana et.al [12] proposed two routing protocols that is Ad hoc On-demand Distance Vector (AODV) as well as Secure-aware Ad hoc Routing Protocol (SAR). Through these protocols the network performances are evaluated during the attacks in WSNs. The future work is to be optimized the output obtained with using SAR protocol in the occurrence of attacks in the network.

Mohamed Ben Haj Frej et.al [13] the proposed method is Secure Data Aggregation Model (SDAM). This method is used for secure aggregate communication on lower cost (in terms of resources). The proposed results also showed an around 40% upgrading in the cross-layering.

H.S Annapurna et.al [14] proposed a system called fault tolerance for WSN which provides both end to end confidentiality as well as fault tolerance through data aggregation in WSN. It used a cryptography technique to secure data transmission in WSN. So proposed system suitable work in communication link failure.

Renuka Suryawanshi [15] proposed a scheme used for getting the data which has lost due to the buffer excess. In given scheme cache memory is provided with the cluster head for getting data. By using proposed scheme can increase the network lifetime.

G Prathima E et.al [16] the author proposes Secure Approximate Data Aggregation (SADA). By using primitive polynomial will generated the synopsis in this scheme and Message Authentication Codes (MACs) are broadcast along with the synopsis to guarantee integrity. SADA consume less energy and thus improved lifetime of the WSNs.

Mohan B A et.al [17] proposed an energy capable clustering scheme with aggregate of data to save the bandwidth constraint. Which enhance the network lifetime. The proposed algorithm has better than LECH because it has superior throughput, more packet release ratio and smaller power utilization. The proposed scheme provides security also.

Kai Zhang et.al [18] proposed two efficient IBMS schemes based on the cubic residue assumption, which is equal to the integer factorization assumption. We utilize two dissimilar methods to determine a cubic root for a cubic residue number through the signer's private key removal. Our schemes have been verified for secure data aggregation during attack.

## 5. CONCLUSION

In WSN larger no. of sensor nodes are deployed in dangerous environment. Each sensor node has some amount of energy. Most of the energy is utilized by sensor node for data aggregation. Wireless sensor networks are less secured due to many attacks. Several secure DA scheme have been used in the literature survey. The Security is big problem in data aggregation. Security provides the confidentiality as well as integrity. Integrating security as an important part of data aggregation protocols is an interesting problem for future research. Public keys and symmetric key have been used for attain end to end or hop-by hop encryptions.

## REFERENCES

[1]. A.S.Poornima et.al, "SEEDA: Secure End-to-End Data Aggregation in Wireless Sensor Networks", in IEEE 2010.

[2]. Vimal Kumar et.al, "Performance Analysis of Secure Hierarchical Data Aggregation in Wireless Sensor Networks", in IEEE 2010.

[3]. Mingxin Yang et.al, "Research on Secure Data Aggregation in Wireless Sensor Networks based on Clustering Method", in IEEE 2011.

[4]. Jailin.S et.al, "Performance Analysis of Hybrid Cryptography for Secured Data Aggregation in Wireless Sensor Networks", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.

[5]. Jia Guo et.al, "Survey on Secure Data Aggregation for Wireless Sensor Networks", in IEEE 2011.

[6]. Merad Boudia Omar Rafik et.al, "SA-SPKC: Secure and efficient Aggregation scheme for wireless sensor networks using Stateful Public", in IEEE 2013.

[7].Bharath K. Samanthula, "A Probabilistic Encryption based MIN/MAX Computation in Wireless Sensor Networks", 2013 IEEE 14th International Conference on Mobile Data Management.

[8]. Soufiene Ben Othman, "An Efficient Secure Data Aggregation Scheme for Wireless Sensor Networks", in IEEE 2013.

[9].Mohsen Rezvani, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING (TDSC) 2013.

[10]. M.Thangaraj, "Swarm Intelligence based Secured Data Aggregation in Wireless Sensor Networks", in IEEE 2014.

[11]. Sankardas Roy et.al, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014.

[12]. S.ARCHANA et.al, "SAR Protocol Based Secure Data Aggregation in Wireless Sensor Network", IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO) 2015.

[13]. Mohamed Ben Haj Frej et.al, "Secure Data Aggregation Model (SDAM) in Wireless Sensor Networks", 2015 IEEE 14th International Conference on Machine Learning and Applications.

[14]. H.S.Annapurna, "Secure Data Aggregation with Fault Tolerance for Wireless Sensor Networks", in IEEE 2015.

[15].Renuka Suryawanshi, "H-WSN with Maximized QoS using Secure Data Aggregation", in IEEE 2016.

[16]. G Prathima E et.al, "SADA: Secure Approximate Data Aggregation in Wireless Sensor Networks", in IEEE 2016.

[17]. Mohan B A et.al, "Energy Efficient Clustering Scheme with secure dataaggregation for mobile wireless sensor networks (EECSSDA)", Online International Conference on Green Engineering and Technologies (IC-GET), in IEEE 2016.

[18]. Kai Zhang et.al, "Efficient and Provably Secure Identity-Based Multi-Signature Schemes for Data Aggregation in Marine Wireless Sensor Networks", in IEEE 2017.