Sixth International Conference on Emerging trends in Engineering and Technology (ICETET'16)
www.ijera.com
ISSN: 2248-9622, pp.28-34

RESEARCH ARTICLE OPEN ACCESS

An Constructive For Secure Data Aggregation Protocol in Wireless Sensor Network

[1]Sasikumar.S, M.E Student., [2]Sugin.S.V, Assistant Professor,
Department Of Computer Science And Engineering, Annai Vailankanni College Of Engineering.

ABSTRACT
Wireless sensor networks are randomly deployed and responsible for monitoring wide geographical area. In WSN, the aggregation of data is very complex because of its limited power and computing capabilities. Issue in data aggregation is that the data may be passed on malicious node. All existing data aggregation technique suffers the security issues because of the transfer of large amount of data. In this paper we propose a protocol named as Secure Data Aggregation Protocol(SDAP) which identifies the malicious node by providing a logical group in the form of tree topology. In the tree topology the aggregate nodes are formed as aggregators, which is a non-leaf node and high level of trust is required to provide a better approximation and accuracy against the security threats. Thus the data is securely aggregated and the efficiency is achieved.

Keywords: Wireless Sensor Network (WSN), aggregation, Secure Data Aggregation Protocol (SDAP).

I. INTRODUCTION

The wireless sensor network is defined as the highly distributed networks of small, lightweight wireless node, deployed in large numbers to trust the environment or system by the measurement of physical parameters such as temperature, pressure or relative humidity. In the WSN, the data from the sensor nodes are collected by means of data aggregation. Sensory information is collected by the nodes. WSN consists of a base station and the number of nodes. The aggregator node is used to aggregate the data from multiple sensor nodes and then the data is forwarded to the base station.

There is several security challenges can be faced during the aggregation of data. Due to this wireless aggregation, eavesdropping and packet injection are occurred. Providing security in the sensor network is more difficult than the mobile adhoc network.

To achieve the security in WSN, they perform various cryptographic operations like encryption, decryption and authentication and so on. For any cryptographic operationthey must use any of the key like symmetric key or asymmetric key. If symmetric key is used then it is very difficult to design for security purpose. If asymmetric key is used then it is too expensive. For applying any of the encryption scheme then it has extra bits, memory required, delay occurred and so on.

In the existing system, various algorithms are used to achieve the security during data aggregation. Many algorithms focus only on the specific attacks or problems. The iterative filtering algorithm is only concentrate on collusion attack.

The secure data aggregation protocol is widely used to overcome the faults that mainly occurred on the existing system. In the existing system, the raw data is transferred to the base station. Therefore more amount of energy is utilized. To provide the energy constrained mechanism, then the transfer of the unwanted data must be prevented. This is achieved by Secure Data Aggregation Protocol(SDAP). Here the hierarchical structure is formed as a tree. The root is the base station. The nodes other than the root areaggregators. The aggregators are not the child nodes. The group is formed with the aggregators. All the necessary processing is done within the group. Now, all the groups transfer the processed data to the base station. From the received data, the groups with malicious nodes are identified.

The security to the data is provided using the cryptographic keys. The aggregation is performed through hop-by-hop. This performs efficiency at each node to detect the malicious node. The difficulty arises by using per-hop aggregation, since it does not verify the correctness of the data.

The major challenge in SDAP under the tree topology is that, a high level trust is needed for the aggregator's node. Therefore, to provide a better approximation and accuracy, divide and conquer method is adopted. A logical group are formed to reduce the threat to the number of nodes. To provide the security to the groups, a commit and attest technique is used. In this technique, when a group is committed to aggregate, it cannot be denied.

To validate the groups, the bivariate-multiple outlier detection algorithm is used. The validation is processed based on the attestation from the group.

II. RELATED WORKS

In wireless sensor network, the nodes are placed randomlyand the data's are collected and aggregated from the sensor nodes and transferred to the base station. Base station has an unlimited amount of energy. During aggregation it reduces the occurrence of the traffic in the network which in turn helps to reduce the energy consumption done on the sensor nodes.

The two main security issues in secure data aggregation are confidentiality and integrity of data. To achieve the confidentiality of data introduce a protocol named as secure data aggregation using privacy homomorphism. It offers high degree of confidentiality because of using the encrypted data processing. It also provides the computation overhead much lesser and symmetric key is used for encryption.

To achieve the integrity of data they use three data aggregation techniques which provide that the message is more secure, computation cost is low and communication is easy. The first one is a homomorphic MAC which defines that all the data collecting nodes to share one global key with the base stationand is used in a symmetric key approach. It provides better computation and communication is efficient. The other two techniques use a public key based homomorphic hashing. One is combined aggregation MAC and the other is identity based aggregate signature. The aggregate MAC technique defines that to all the base station to share the distinct key with every node. The identity based aggregate signature enables all the intermediate nodes beside the base station to verify the authenticity of aggregate messages.

Another secure data aggregation technique is a combinatorial key distribution. Here the performance of hashing the data is improved because of sending the data across the network. This minimizes the power consumption and increases the security of aggregated data.

Secure hierarchical data algorithm is a new technique to provide the security of aggregate data. Here use an effective public key cryptography (Elliptic curve cryptography) to achieve an end to end security. There is no intermediate node to aggregate data. There is a direct aggregation between source and the sink nodes. Thus the energy efficiency is improved and more secure by using the end to end communication and also there is no intermediate node failure.

Iterative filtering algorithm is also a new technique which is concentrate only on collusion attacks. One of the fundamental usages is to determine trust-worthiness. It is calculated through the distance from the sensors and is compared for the correctness of the previous iteration. Through this estimation the level of trust is determined.

III. OVERVIEW

An overview shows the aggregation process through various models. The model shows how the data is being aggregated. The models are as follows:

3.1 Network model:

The network model shows the environment in WSN. In this model, the nodes are clustered depending on the network. The node head is determined as an aggregator. The security algorithms are provided to determine the trustworthiness. The disturbance in the iterative filtering algorithm is overcomes through the efficient SDAP.

In SDAP, large number of resources constrained sensor nodes is used. It helps to connect the sensor network and the outside network. Here, the aggregation is provided by means of the tree topology. It can be used for real time application for a dynamic environment.

3.2 Privacy determination over attack model:

It is primarily used for the authentication phenomenon. It easily defeats the outside contender. The attacks are many over the cluster based aggregation protocol. Depending on the behaviour of the node, many types of attacks are formed. In this privacy determining model, the defence is provided against the attacks.

3.3 Contender model:

The contender model is mainly used for adversary. It is used to produce the false data. For instance, consider the remote environment were the sensors are placed.The contender sends the false data to the aggregator the security algorithms are enhanced for this purpose.

3.4 Goals to be achieved:

The goals are achieved through the proposed protocol, in which the groups are formed by means of the Cluster Formation. The groups are efficiently used to determine the attackers. The certification / attestation are provided for this purpose. It ensures the privacy for this purpose. It ensures the privacy for the transmission of data.

IV. PROPOSED SCHEME

4.1 Finding the trusted node:

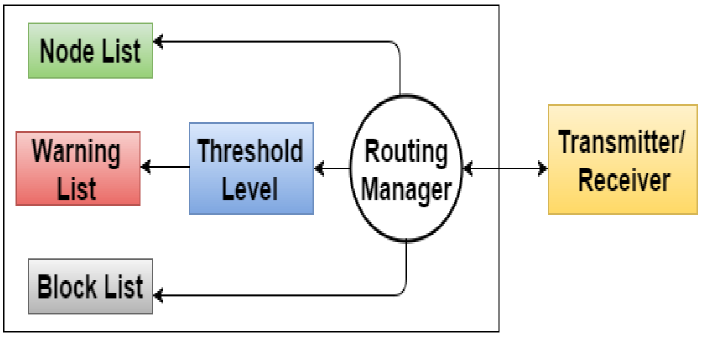

Fig 1 Identify the Trusted node

In the above figure, the routing manager decides the status of the node to transmit the data. Based on the requests of data made, the routing manager is used to process the requests. The client connections are managed and they are performed across the set of servers provided by the client manager. The routing manager helps to establish the connection between the client and the server. Depending on the status of the node, the node is either added to the node list or added to the block list. If it is difficult to determine the status of the node, then the threshold level is estimated. The threshold value of the corresponding node is compared with the associated threshold value. Through this comparison we can determine the status of that node. If it is equal or exceeds the estimated threshold value, the node is added to the node list else it is added to the block list.

4.2 Certificate Authority:

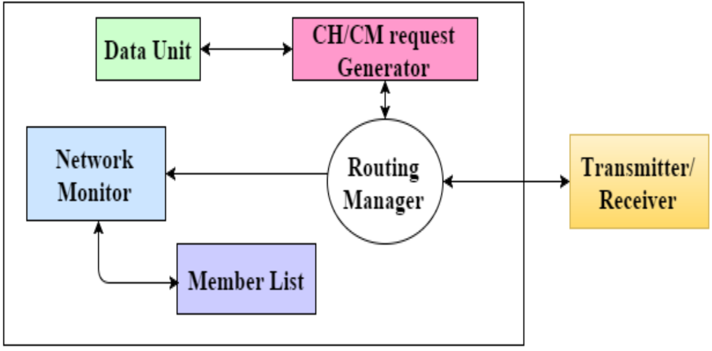

Fig 2. Certificate Authority

When the node in the network is determined, the clustering is done. The cluster head is used to provide the request to the routing manager. The data is stored in the data unit. The routing manager provides the acknowledgement in response to the request. Then the verification is done for the malicious node by the network monitor. The network monitor identifies that the node is vulnerable or not. If the node is not vulnerable then the node is stored in the member list. If the node determined as thread then the node is blocked for the transmission of data. The network monitor determines the authorized users to transmit the data. The certificate authority helps to issue the certificates to determine the efficiency in the transmission of the data to prevent the failure of the nodes.

4.3 Algorithm:

In the following algorithm describes that how the data’s are securely aggregated and transmitted by using the protocol.

Algorithm 1: Secure Aggregation Algorithm

Input: A set N of x tuples (L, C_L, A_L) where L is a cluster leader id, C_L is the cluster count value, A_L is the cluster aggregation result and C is the total number of clusters.

Output: Secure aggregated data D to the base station in secure manner.
Procedure:

```
loop
    To compute the $\mu_c$ and $s_c$ for all the counts in the set Nwhere $\mu_c$is the mean and $s_c$ is the standard deviation;
    To compute the mean $\mu_v$ and standard deviation $s_v$ for all the values use in the given set N;
    Find the maximum count value $C_L$ in the set N;
    Compute the statistic $S_c$ for count $C_L = (C_L - \mu_c) / S_c$
    To compute p-value $P_c$ based on the statistic $S_c$;
    Compute the statistic $S_v$ for the corresponding value $A_L$
        $( | A_L - \mu_v | ) / s_v$;
    Compute p-value $P_v$ based on the statistic $S_v$;
    If $(P_c * P_v) < \alpha$ then
        $N = N - \{(L, C_L, A_L)\}$
        $D = D \cup \{ L \}$
    else
        break;
    end if
end loop
return D;
```

The above algorithm describes that it checks three stages

4.3.1 Check the aggregated message:

The base station receives the aggregated data from cluster heads. Each cluster head has a separate cluster head id which is denoted by L. After the base station receives the aggregated data it checks whether the data is an authenticated or not. Each node has a separate key denoted by K_L. By using this key count value C_L and aggregated value A_L are determined. If all the values are in certain range then the data is an authenticated data.

4.3.2 Provide the Certificate:

In the given network, each node must find the separate mean and standard deviation values. After finding the value it also finds the maximum value in the network. If any node count value exceeds the maximum value the node is declared as the malicious node. The certificate is not issued in the node. After finding this, there is no communication through this node.

V. PERFORMANCE EVALUATION

In this section, it shows the screenshots as well as it provides the detailed description about the performance graph.

5.1 Simulation:

The simulation section provides the detailed description about the screen shots and clearly verifies the generated output.

In Fig 3, the nodes are placed in the network randomly. Totally there are 25 nodes placed in the network. Node 24 denotes the base station of the network. The network containsfour clusters. Each clusterhas a separate Cluster Head.The Node number 6, 8, 16 and 18 are the cluster heads. Each node is placed in the specific point. The base station, cluster heads and cluster members are differentiating by separate colours.

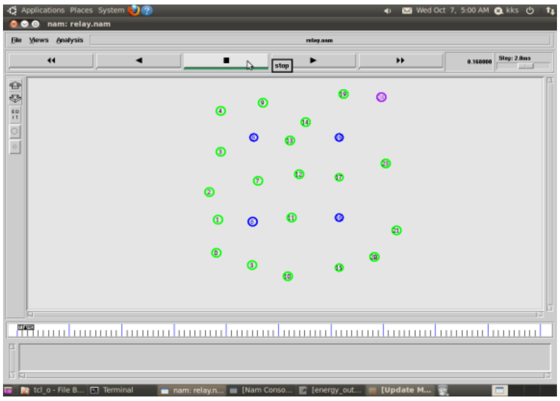

Fig 3. Placing nodes in the network

In Fig 4, the data aggregation between the client and the server is explained. Each cluster member sends the data to their own cluster head. All the aggregator collects the data and transferred to the base station. If the base station is in the farthest distance the transmission is done between two cluster heads. The farthest cluster head can transfer the data to its coverage neighbour cluster head and again this is transferred to the base station. All these transmission is done only the particular coverage area. In the below figure, the ring shape denotes the coverage area of the network.

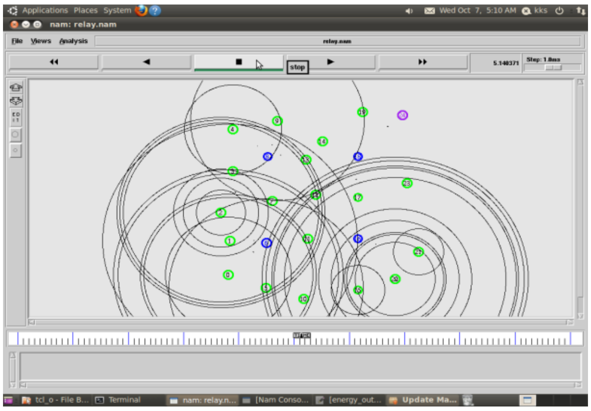

Fig 4 Data Aggregation

During the aggregation technique security is one of the main challenging issues. To aggregate the secure data using the new protocol named as secure data aggregation protocol. At each level it checks whether the data is secure or not. If it identifies the malicious node then the data transmission is not present through this node. Thus the security is achieved during data aggregation.

5.2 Performance Graph:

The performance evaluation compares the previously used protocol and determines that which is more efficient and securely aggregated.

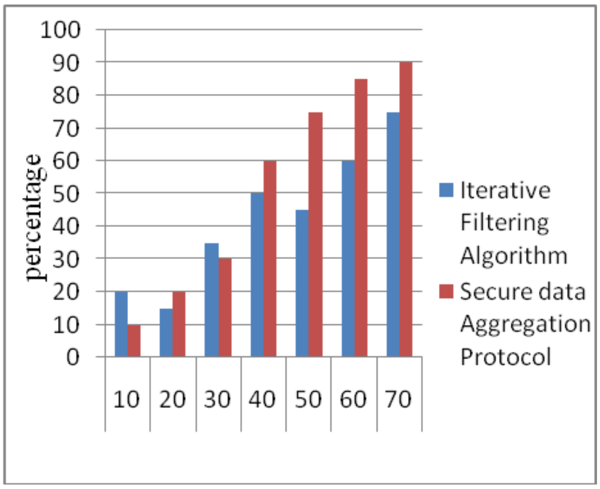

Fig 5 Comparison between IFA and SDAP

In the fig 5 shows that comparison between two secure aggregation methods. If the nodes present in the network is less in number, then the Iterative Filtering Algorithm (IFA) is efficient. If the nodes presentin the network increases in number then the SDAP protocol is efficient.

VI. CONCLUSION

In this paper, we introduced a protocol named as secure data aggregation protocol. By using this data aggregation is more secure and the certificate authority is provided by each trusted node. In this protocol checks each node and check whether the node is trust or not. Thus the security is achieved during aggregation. In future work, we will enhance the same protocol with detailed explanation.

REFERENCES

[1]. H.-S. Lim, Y.-S. Moon, and E. Bertino, “Provenance-based trustworthiness assessment in sensor networks,” in Proc. 7th Int. Workshop Data Manage. Sensor Netw., 2010, pp. 2–7.

[2]. H.-L. Shi, K. M. Hou, H. ying Zhou, and X. Liu, “Energy efficient and fault tolerant multicore wireless sensor network: E2MWSN,” in Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput., 2011, pp. 1–4.

[3]. C. de Kerchove and P. Van Dooren, “Iterative filtering in reputation systems,” SIAM J. Matrix Anal. Appl., vol. 31, no. 4, pp. 1812– 1834, Mar. 2010.

[4]. Y. Zhou, T. Lei, and T. Zhou, “A robust ranking algorithm to spamming,” Europhys. Lett., vol. 94, p. 48002, 2011.

[5]. R.-H. Li, J. X. Yu, X. Huang, and H. Cheng, “Robust reputation based ranking on bipartite rating networks,” in Proc. SIAM Int. Conf. Data Mining, 2012, pp. 612–623.’

[6]. H. Liao, G. Cimini, and M. Medo, “Measuring quality, reputation and trust in online communities,” in Proc. 20th Int. Conf. Found. Intell. Syst., Aug. 2012, pp. 405–414.

[7]. B.-C. Chen, J. Guo, B. Tseng, and J. Yang, “User reputation in a comment rating environment,” in Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2011, pp. 159–167.

[8]. C. T. Chou, A. Ignatovic, and W. Hu, “Efficient computation of robust average of compressive sensing data in wireless sensor networks in the presence of sensor faults,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 8, pp. 1525–1534, Aug. 2013.

[9]. Y. Yu, K. Li, W. Zhou, and P. Li, “Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures,” J. Netw. Comput. Appl., vol. 35, no. 3, pp. 867–880, 2012.

[10]. H.-S. Lim, G. Ghinita, E. Bertino, and M. Kantarcioglu, “A gametheoreticapproach for high-assurance of data trustworthiness insensor networks,” in Proc. IEEE 28th Int. Conf. Data Eng., Apr.2012, pp. 1192–1203.

[11]. M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, “Secure dataaggregation technique for wireless sensor networks in the presenceof collusion attacks,” School Comput. Sci. and Eng., Univ.New South Wales, Kensington, NSW, Australia, Tech. Rep.UNSW-CSE-TR-201319, Jul. 2013.

[12]. Y. Sun, H. Luo, and S. K. Das, “A trust-based framework for faulttolerantdata aggregation in wireless multimedia sensornetworks,” IEEE Trans. Dependable Secure Comput., vol. 9, no. 6,pp. 785–797, Nov. 2012.

[13]. S. Ozdemir and H. C¸ am, “Integration of false data detection withdata aggregation and confidential transmission in wireless sensornetworks,” IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 736–749, Jun. 2010.

[14]. H. Chan, A. Perrig, and D. Song, “Secure hierarchical in-networkaggregation in sensor networks,” in Proc. 13th ACM Conf. Comput.Commun. Security, 2006, pp. 278–287.