Wireless Personal Communications (2020) 113:1775–1790
https://doi.org/10.1007/s11277-020-07291-5

# Malicious Node Detection in Wireless Sensor Networks Using an Efficient Secure Data Aggregation Protocol

**S. Gomathi**[1] · **C. Gopala Krishnan**[1]

Published online: 9 April 2020


**Abstract**
Wireless sensor networks are randomly deployed and responsible for monitoring geographical area wide. 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 the existing data aggregation techniques undergo security issues because of the transfer of large amount of data. In this paper we propose a protocol named 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 aggregation is formed by aggregating the nodes, which are 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 in data aggregation.

**Keywords** Wireless sensor networks (WSN) · Secure data aggregation protocol (SDAP) · Certificate authority (CA) · Malicious node detection

## 1 Introduction

A Wireless Sensor Network (WSN) is defined as a highly distributed network formed by large number of small, lightweight sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. WSN consists of a base station, a sink and sensor nodes. The sensor nodes are mostly deployed in harsh environments and they have the facility to sense, process data and communicate with each other via a wireless connection. Sensory information collected by the sensor nodes is communicated to the base station which is the centralized point of control within the network through hop by hop transmissions. The data collected is aggregated at the aggregator node and only the aggregate values are forwarded to the base station. Using aggregation, the overall energy requirements of the network can be reduced by decreasing the amount of network traffic.

✉ C. Gopala Krishnan
skywarekrish@gmail.com

S. Gomathi
gomathyrajah@gmail.com

[1] CSE Department, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India

Data aggregation makes the already existing security challenges more complicated. Secure data aggregation in wireless sensor networks refers to providing security to aggregate data. The two main security issues in secure data aggregation are confidentiality and integrity of data. Highly sensitive data may be communicated by the sensor nodes such as key distribution. So it is important to build a secure channel in a wireless sensor network. Data confidentiality is the ability to hide messages from a passive attacker. Encryption is the technique used to provide confidentiality in wireless sensor network. While performing aggregation, the aggregator has to decrypt the encrypted data which makes the data unprotected. In a similar way, false data can be injected into the aggregate by the aggregator, and sent to the base station. Data integrity refers to the ability to confirm that the data being sent is not altered.

A certificate can be used for secure encrypted information as well as to uniquely identify the holder. An appropriate cryptography method for sensor nodes should be selected to provide secured services in WSNs. In the existing systems, different algorithms are used to achieve the security during data aggregation. In general, existing symmetric cryptographic solutions for WSNs focus particularly on the efficiency of key establishment after the deployment of the network. Many works focus on the lightweight adoption of asymmetric cryptographic algorithms.

Iterative filtering technique which is more robust against collusion attacks aggregate data from multiple sources simultaneously usually in a form of corresponding weight factors. The sensor nodes are divided into disjoint clusters, and every cluster has a cluster head which acts as an aggregator.

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

The security to the data packet is provided using the cryptographic keys. The aggregation is performed through hop-by-hop. This executes efficiency at each sensor node to detect the malicious node. The difficulty arises when 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 accuracy, divide and conquer method is adopted. A logical group is formed to reduce the threat to the sensor nodes. To provide the security to the groups, a commit and attest technique is used. In this technique, when a present group is committed to aggregate, it cannot be denied. To validate the present groups, the bivariate-multiple outlier detection algorithm is used. The validation process is done based on the attestation from the group.

## 2 Related Works

In wireless sensor networks, the sensor nodes are placed randomly and information is collected from the sensor nodes, it is aggregated and then transferred to the base station. Base station has sufficient amount of energy. The base station is assumed to be secured

with unlimited available energy while the other are assumed to be unsecured with limited available energy. During aggregation it reduces the occurrence of the traffic in the network which in turn helps to reduce the energy consumption on the sensor nodes. The two main security issues in secure data aggregation are confidentiality and integrity of data.

Hu and Evans [1] designed the first Secure Data Aggregation (SDA) scheme which works under the assumption that at most a single node is malicious. This protocol secures in-network aggregation by providing a light weight security mechanism to effectively detect node misbehaviour. In another secure data aggregation study Przydatek et al. [2], proposed Secure Information Aggregation (SIA), which works under the assumption of a single-aggregator model. The authors use "Aggregate-Commit-Prove" approach where the base stations check the correctness of the aggregated data by requesting sample small data pieces from sensors.

ESPDA protocol presented by Cam et al. [3] provides energy—efficient data aggregation together with secure data communication in wireless sensor networks. It is a cluster—based data aggregation protocol and aggregates data by pattern codes. So the cluster-heads are not required to know the contents of the transmitted data. Ozdemir et al. [4] developed the Secure Reference-Based Data Aggregation (SRDA) protocol which incorporated both data aggregation and security concepts together in cluster-based wireless sensor networks. The raw data sensed by sensor nodes are compared with a reference data and then only the difference between the sensed data and the reference value are transmitted.

A secure hop-by-hop data aggregation protocol using a tree-based topology to compute the aggregation in the presence of a few compromised nodes was proposed by Yang et al. [5] Divide-and-Conquer and commit-and-attest are the two principles on which this scheme has been designed. Recently, several data aggregation schemes based on privacy homomorphism encryption have been proposed and investigated on wireless sensor networks. These data aggregation schemes provide better security compared with traditional aggregation since cluster heads can directly aggregate the ciphertexts without decryption; consequently, transmission overhead is reduced. An approach that uses homomorphic encryption and Message Authentication Code (MAC) to achieve confidentiality, authentication and integrity for secure data aggregation in wireless sensor networks has been proposed by Othman et al. [6]. Privacy Homomorphism (PH) proposed by Rivest et al. [7] allows aggregating encrypted data.

To achieve the integrity of data the researchers use three data aggregation techniques which provide more security to the message, lessens the computation cost and makes the communication easy. The first one is a homomorphic MAC which defines that all the data collecting sensor nodes share one global key with the base station and uses a symmetric key approach. It provides better computation and efficient communication. The other two techniques use a public key based homomorphic hashing.

Girao et al. [8] proposed a protocol called CDA which uses an additive and multiplicative homomorphic encryption scheme that allows the aggregator to aggregate encrypted data. The developers of this protocol had applied the Privacy Homomorphism (PH). Since PH is unsecure against chosen plain text attacks, CDA ensures only data confidentiality. Wagner [9] addressed the issue of measuring and bounding malicious nodes' contribution to the final aggregation result for the single-aggregator case.

Secure hierarchical data algorithm is a new technique that provides security to the aggregated data. Effective public key cryptography (Elliptic curve cryptography) is used 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 protected by using the end to end communication and also there is no intermediate node failure.

Perrig et al. [10] had proposed security protocols for sensor networks which address the key establishment problem. In the approach which is based on authentication between sensors with a shared secret key, all nodes trust the base station at the network creation time and each node is given a master key which is shared with the base station. To achieve authentication between a sensor and base station, a Message Authentication Code (MAC) is used.

Junior et al. [11] suggested detecting malicious node through detection of malicious message transmissions in a network. A message transmission is considered suspicious if its signal strength is incompatible with its originator's geographical position. The work reported by Curiac et al. [12] proposed to detect malicious node by comparing its output with an aggregation value. A neighbor-based malicious node detection scheme for wireless sensor networks was proposed by Yim and Choi [13]

Iterative filtering algorithm is also a new technique which only concentrates on collision 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. An improvement for the IF algorithms has been put forward by Gomathi et al. [14] by providing an initial approximation of the trustworthiness of sensor nodes which makes the algorithms not only collusion robust, but also more precise and faster converging.

Ayday et al. [15] introduces an Iterative method for Trust and Reputation Management referred as ITRM. The proposed algorithm can be applied to centralized schemes, in which a central authority collects the reports and forms the reputations of the service providers as well as report/rating trustworthiness of the consumers. Jinfang et al. [16] proposed an Efficient Distributed Trust Model (EDTM) for WSNs. The authors selectively calculated direct trust and recommendation trust according to the number of packets received by sensor nodes. Then, they considered communication trust, energy trust and data trust during the calculation of direct trust. Furthermore, they defined trust reliability and familiarity to improve the accuracy of recommendation trust. Their proposed EDTM can evaluate trustworthiness of sensor nodes more precisely and prevent the security breaches effectively.

Chang et al. [17] devised a methodology to classify the nodes behaviour based on their cooperative bait approaches which predicted the attacks in the network. The problems of the conventional malicious node detection system were tolerated by implementing Cooperative Bait Detection Scheme (CBDS).The anomaly nodes were detected based on fuzzy theory and revised evidence theory. The malicious nodes in a network can be identified by monitoring the behaviours of the evaluated nodes with multidimensional features and integrating this information, thus, the normal operation of the whole network can be verified.

Kresimir et al. [18] dealt with the security aspects of these IPv6-based WSNs. The authors proposed the solution to an adaptive distributed system for malicious node detection in the IPv6-based WSN. Their intrusion detection system is based on distributed algorithms and a collective decision-making process. It introduces an innovative concept of probability estimation for malicious behaviour of sensor nodes.

Nirmal Raja and Maraline Beno [19] carried out to prevent the Sybil attack and increase the performance of the network. The authors presented the novel security mechanism and Fujisaki Okamoto algorithm and also application of the work. The Fujisaki-Okamoto (FO) algorithm is ID based cryptographic scheme and gives strong authentication against Sybil attack. In this scheme the authors analyzed broadcasting key, time taken for different key sizes, energy consumption, Packet delivery ratio and Throughput. Xie Jinhui et al. [21]

aimed at the hybrid DoS attack in wireless sensor network. The authors proposed a new intrusion detection method based on energy trust (IDSET)on the existing detection mechanism, which improved the detection rate of hybrid DoS attacks.

## 3 Overview

This section shows the aggregation process through various models. The following models show the data aggregation. 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 head node is determined as an aggregator. The security algorithms are provided to determine the trustworthiness. The disturbance in the iterative filtering algorithm has been overcome by efficient SDAP. In SDAP, large number of resources constrained sensor nodes are 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.

### 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 over attack 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 where the sensors are placed. The security algorithms are enhanced because the contender sends the false data to the aggregator.

### 3.4 Goals to be Achieved

The main goal is to transmit the data in secure manner through the secured path. By the usage of the proposed protocol, the goals are achieved in which the groups are formed by means of the cluster formation. The created groups are efficiently used to determine the attackers. The certification / attestation is provided by Certificate Authority. It ensures the privacy for the transmission of data.

## 4 Proposed Scheme

To overcome the disadvantage that arises when using the iterative filtering algorithm, a new technique called Certificate Authority (CA) has been introduced in each cluster. Iterative filtering algorithm works better for solving the issues of collision attacks. Data

Aggregation is used to aggregate data by the cluster head and transmit it to the static station or base station. The base station collects all the data from the cluster head and aggregates for a secured data transmission. To perform the aggregation more secure, the CA is used to check each node's condition whether it is a is trust node or malicious node. By using the CA the node's processes are monitored. The data must be transmitted from a member node to the cluster head and from cluster head there to either the cluster head or base station with in a given time.

The data should be transmitted through the secure path and for this secure data transmission Path Verification Packet (PVP) is used. The Path Verification Packet contains a return back message. The path is analyzed using PVP. The packet is transmitted to the base station through the secure path and if the acknowledgement is received then the path is considered to be secure path. Otherwise different path is selected for data transmission. After the path analyzation gets over, the data is transmitted from the cluster head to the base station.

If a cluster head data transmission time exceeds or any modifications made in the data then the certificate authority checks the threshold value of that node. If the threshold value is in range, then the node is a trusted node and data aggregation is done through this node. If the threshold value is out of range then the node is marked as malicious node. After marking the malicious node, the data is not transferred to that particular node. By using PVP, the path security is checked and the data is transmitted through the selected secure path. Thus the data is transmitted only through the trusted node and it can be aggregated more securely and efficiently.

### 4.1 Data Aggregation

The data is gathered from the Cluster Member and transmitted to the Cluster Head. The collected data is transmitted from the Cluster Member to the Base Station. If the Base Station is present far away, then the data is transmitted between the Cluster Heads and finally transmitted to the Base Station. The Certificate Authority is present in the midst of the network and the Certificate Authority is used to select the trust node among the Cluster and then offer the certificate for every trust node present in the network. The nodes which are not trust nodes will not be allowed to transmit the data to the Cluster Head. For finding the trust node, the threshold value is considered.

Figure 1 represents data aggregation. The data are transmitted from the Cluster Member to the Cluster Head. The Cluster Head aggregates the transmitted data and forward it to the Base Station.

### 4.2 Finding 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, the routing manager process the requests. The client connections are managed 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 the status of the nodes are determined. 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. The threshold

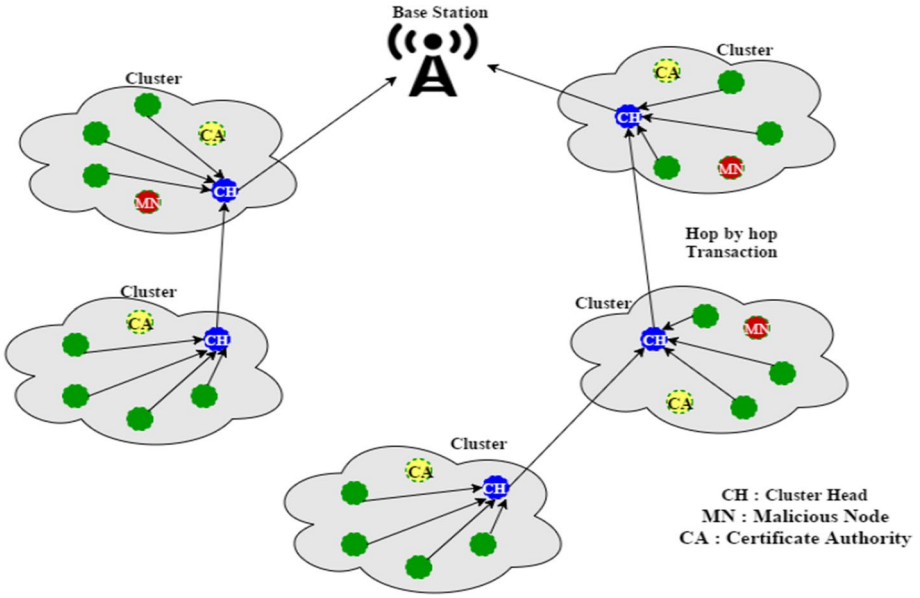



**Fig. 1** Data aggregation

value is calculated depending upon the number of data packets transmitted and the number of data packets successfully obtained (Figs. 2, 3 and 4).

### 4.3 Certificate Authority

When the node in the network is determined, (i.e. present) the clustering is done. The cluster head is used to provide the request to the routing manager. The data are 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 whether the node is vulnerable or not. If the node is not vulnerable then the node is stored in the member list. The node is blocked for the transmission of data if the node is determined as thread. 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, a node can transmit while it has CA permission, throughput differs from efficiency because it deals with time.

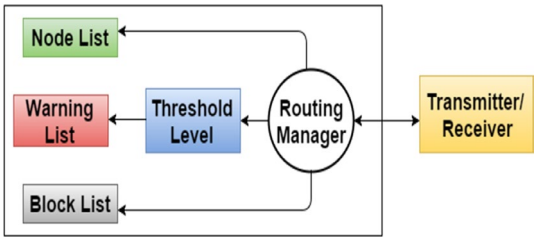



**Fig. 2** Trusted node identification

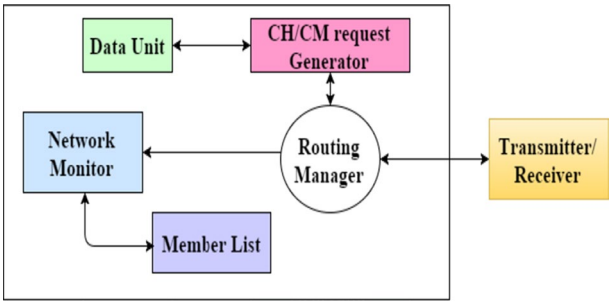



**Fig. 3** Certificate authority

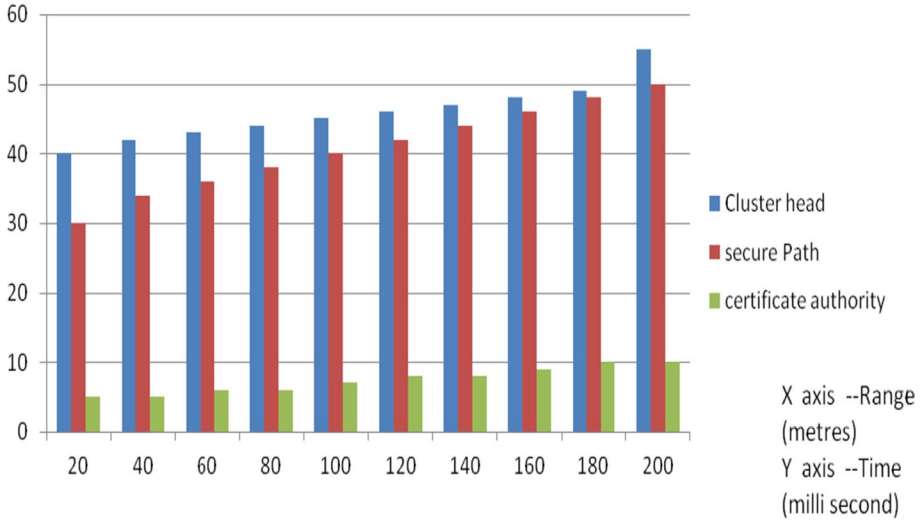



**Fig. 4** Performance graph between CA, CH and secure path

### 4.4 Algorithm

The algorithm describes that how the data are securely aggregated and transmitted by using the secure aggregation protocol.

## 5 Algorithm 1: Secure Aggregation Algorithm

Input: A set N of x tuples (L, C, $C_L$, $A_L$) 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.

### 5.1 Procedure:

1. loop
2. Compute the $\mu_c$ and $s_c$ for all the counts in the set N where $\mu_c$ is the mean and $s_c$ is the standard deviation;
3. Compute the mean $\mu_v$ and standard deviation $s_v$ for all the values use in the given set N;
4. Find the maximum count value $C_L$ in the set N;
5. Compute the statistic $S_c$ for count $C_L = (C_L — \mu_c) / S_c$ (where Sc –statistical data of cluster node)
6. Compute p-value $P_c$ based on the statistic $S_c$; $p = 1\text{-}Sc$
7. Compute the statistic $S_v$ for the corresponding value $A_L$
8. $(\left| A_L - \mu_v \right|)/ s_v$; $A_L$ cluster agg node count
9. Compute p-value $P_v$ based on the statistic $S_v$;
10. If $(P_c * P_v) < \alpha$ then ( $\alpha$ is threshold for node)
11. $N = N - \{(L, C_L, A_L)\}$ (N is over all set count, which has × tuples)
12. $D = D \cup \{L\}$
13. else
14. break;
15. end if
16. end loop
17. return D;

The above algorithm checks three stages

#### 5.1.1 Checking the Aggregated Message

The static base station receives the aggregated data packet 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 authenticated or not. Each node has a separate key denoted by $K_L$. By using this key count value $C_L$ [cluster count & key count are same] and aggregated value $A_L$ are determined. If all the values are in certain range then the data is an authenticated data. Range is fixed by WSN capability (maximum cluster node value).

#### 5.1.2 Providing the Certificate

WSN has mathematical function which helps to set the formulae needed and set the threshold value. 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. Certificate is provided based on Pc* Pv.

### 5.2 Path Verification Packet

The data which are involved in the transmission should be passed through secured path. For the secure transmission the Path Verification Packet (PVP) is considered. The Path Verification Packet (PVP) consists of return back message. The paths present in the

networks are analyzed using Path Verification Packet. The PVP packet is transmitted through the from Cluster Head to the Base Station. The path is considered as secured when the acknowledgement is received from the Base Station. If the PVP packet is not transmitted then they select a different path for the data transmission. After the path analyzation gets over, the data is transmitted from the cluster head to the Base Station.

#### 5.2.1 Path Verification Request

The Cluster Head sends the request to the Base Station and the request is considered as verification request. The verification request contains the details such as "return back message" and the sent time. After viewing the return back message by the Base Station, if the path is secured then they are returned to the required Cluster Head through the same path.

#### 5.2.2 Path Verification Reply

The Base Station sends the reply message to the Cluster Head and the reply is considered as verification reply. The verification reply has the information details like return back message and the receive time. After the Cluster Head viewing the return back message, the data transmission involves through the secured path. Thus the path is secured and the network is also secure.

## 6 Performance Evaluation

The proposed work deals with the identification of trust node and secure path. For the identification of trust node, Certificate Authority is used. For path security, Path verification packet is used. The Path verification Packet is transmitted between the cluster head and the base station. If the acknowledgement is received from the base station then the path involved in verification is to be secured. In this section, the screenshots as well as the detailed description about the performance graph is described.

If acknowledgement is not received from the base station then different path for communication is selected in order to perform secure transmission. The Certificate Authority does not provide certificate to the node whose threshold value is above the range and confirmed that particular node as a malicious node. If the cluster head changes into malicious node then different cluster head is selected from same cluster. Thus for secure data transmission the certificate authority and path verification packet is considered and security gets increased.

### 6.1 Simulation

The simulation section provides the detailed description about the screen shots and clearly verifies the generated output. The Network Simulator NS2 software has been used for the simulation section.

In Fig. 5 the nodes are placed in the network randomly. Totally there are 50 nodes placed in the network. Node 26 denotes the base station of the present network. The network contains five clusters. Each cluster has a separate Cluster Head. The Node number 24, 25, 30, 31, and 35 are the cluster heads. The cluster heads are selected based on initial energy of the nodes. On the basis of energy and stable feature, these nodes are selected as

cluster heads. Each node is placed in a specific point. Each cluster has a specific Certificate Authority. The base station, cluster heads cluster members and certificate authority are simulated by separate colours.

In Fig. 6, Path Verification Packet is sent through the aggregated path. It travels through the shortest path to the base station. When it reaches the base station it will be returned back to the exact node. If the packet is received then it is a secure path. Otherwise a new path is selected for aggregating the data.

Figure 7 represents the Verification Request of the Path Verification Packet. The request packet is transmitted from the Cluster Head to the Base Station. The Base Station verifies the path and the Cluster Head condition. The path is analyzed and if the path is secured then the Base Station transmits the message back to the Base Station. The verification packet contains the sent time of the Cluster Head.

Next represents the Verification Reply of the Path Verification Packet. The reply packet is transmitted from the Base Station to the Cluster Head. The Base Station verifies the path and the Cluster Head condition. Using the secure path, the reply packet is transmitted and the transmitted packet reaches the Clusters. The Reply Packet contains the received time of the packet. After the process is ended, the data transmission starts through the secured path.

The data aggregation between the client and the server is explained. Each cluster member sends the data to their own cluster head. The data is collected by the aggregator and transmitted to the base station. If the base station is in the farthest distance, then 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

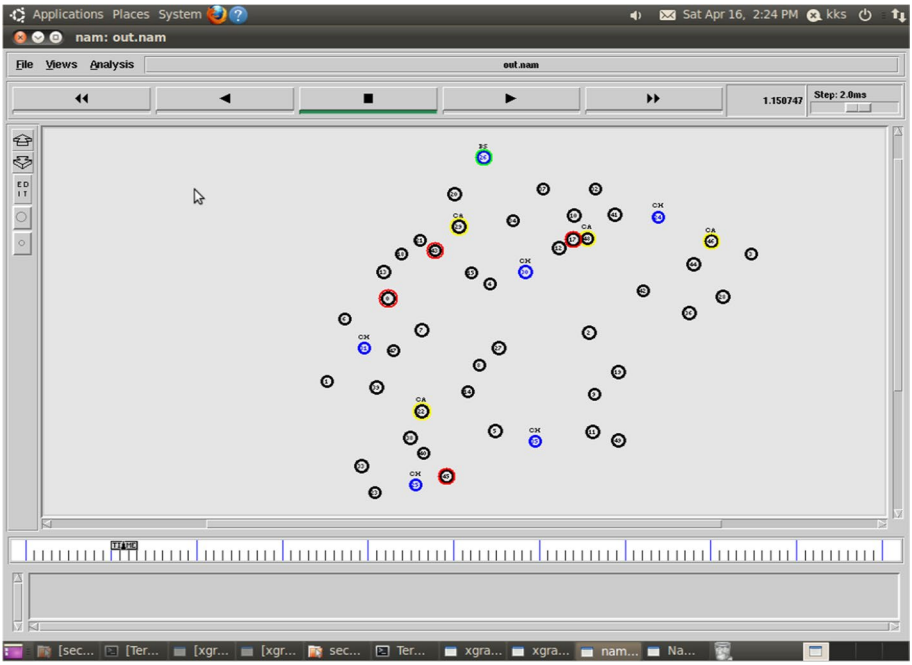



**Fig. 5** Placing nodes in the network

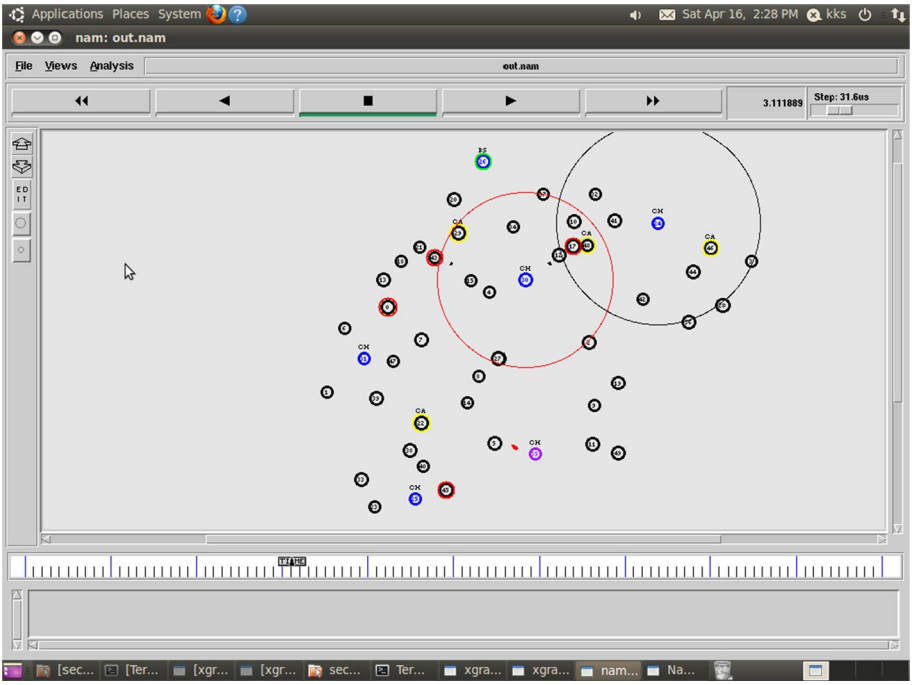



**Fig. 6** Path verification packet

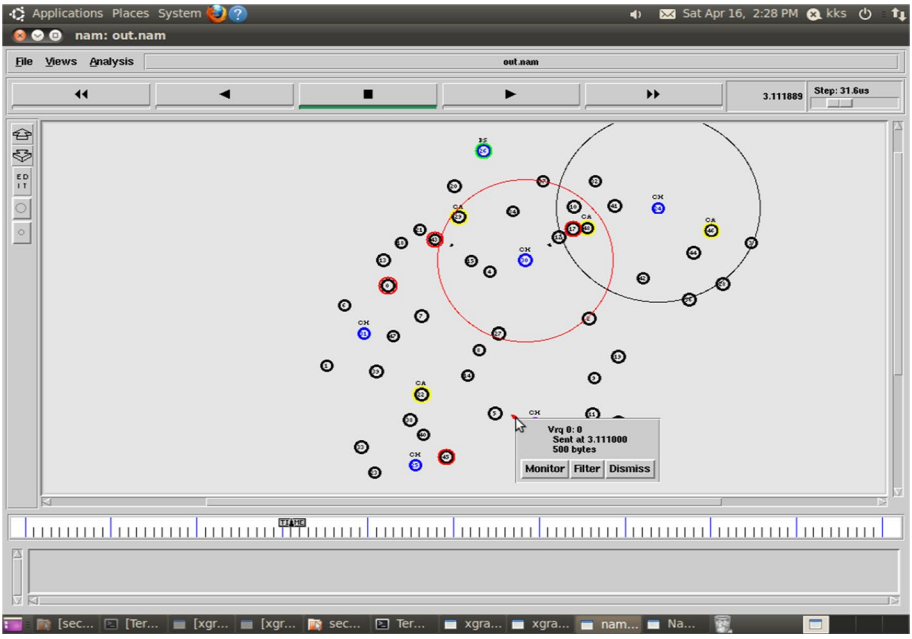



**Fig. 7** Verification request

station. The transmission is done only in the WSN coverage area. In the below figure, the ring shape denotes the coverage area of the network.

In Fig. 8, the cluster heads 24 and 31 have changed into malicious nodes. During aggregation, the cluster head has changed to malicious node so the aggregation process has stopped suddenly. The node is marked as malicious node and the data are not transmitted through the malicious node as per the rule.

In Fig. 9, a new cluster head is selected for data transmission since the previous cluster head turns into malicious node. When the malicious node is found, a new cluster head is selected for data transmission. After selecting new cluster head, the path is verified by using path verification packet. If the path is a secure one then the aggregation process starts.

During the aggregation technique security is one of the main issues. To aggregate the secure data a new protocol named as secure data aggregation protocol is used. 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.

## 6.2 Performance Graph

Figure 10 shows the comparison between two secure aggregation methods. If the nodes present in the network are less in number, then the Iterative Filtering Algorithm (IFA) is efficient. If the nodes present in the network increases in number then the SDAP protocol is efficient.

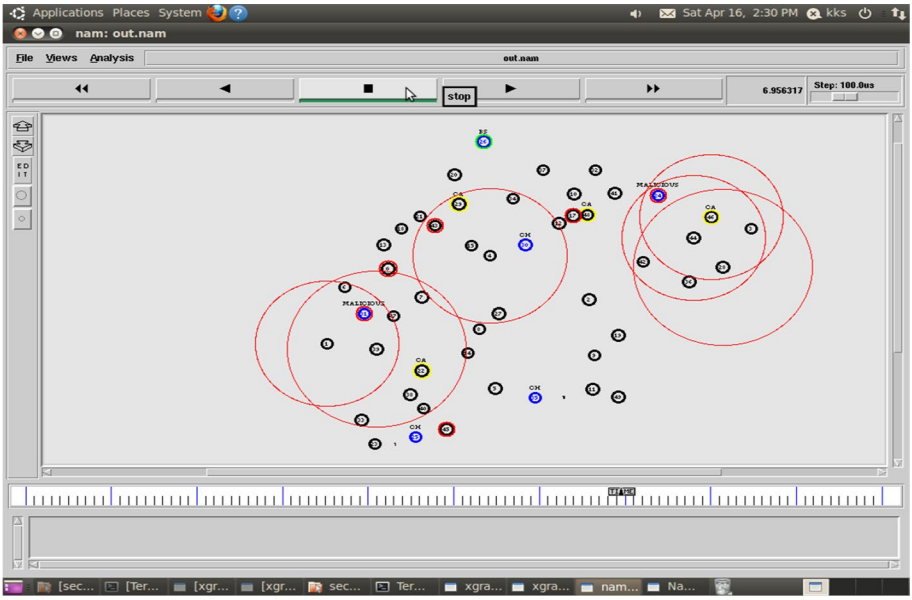



**Fig. 8** Malicious node detection

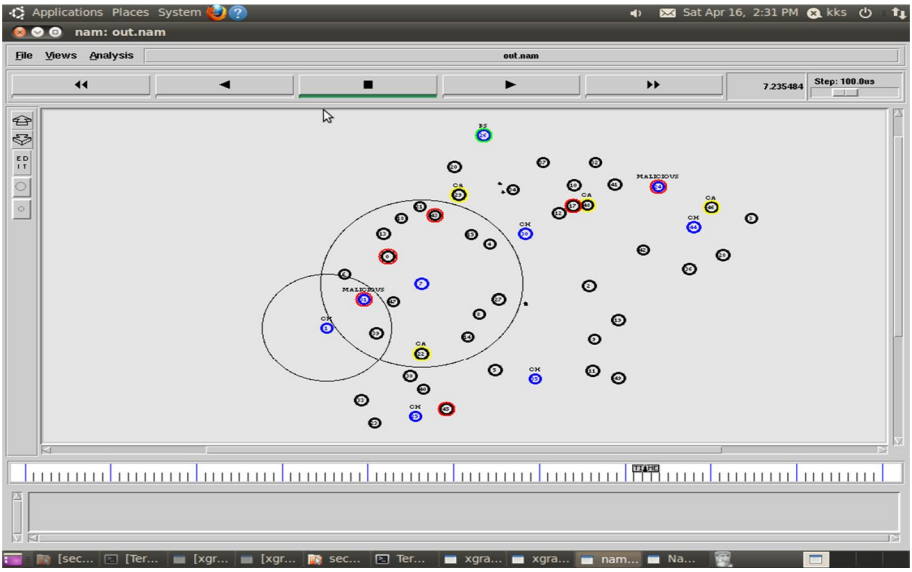
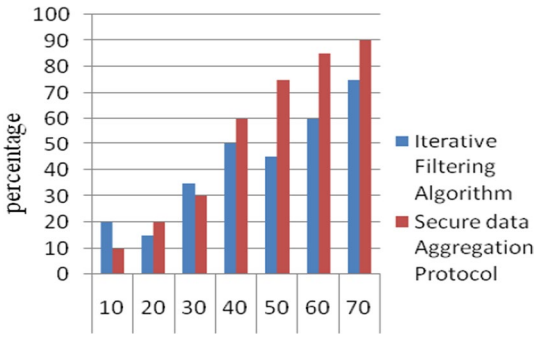



**Fig. 9** Selection of new Cluster Head for data transmission

**Fig. 10** Comparison between IFA and SDAP (*x* axis, *No* of nodes, *y* axis Percentage of throughput achieved)




## 7 Conclusion

In this manuscript, secure data aggregation protocol for wireless sensor networks is proposed. By using this technique data aggregation is more secure and the certificate authority is provided by each trusted node. In this protocol, each node is checked whether it is trustworthy. Thus the security is achieved during aggregation. In future work, we will enhance the same protocol with additional routing protocols.

## References

1. Hu, L., & Evans, D. (2003 Jan 23). Secure aggregation for wireless networks. Proceedings of Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL.

2. Przydatek, B., Song, D. & Perrig, A. (2003). SIA: Secure information aggregation in sensor networks. Proceedings of SenSys' 03, Nov 5–7, Los Angeles, CA.
3. Cam, H., Ozdemir, S., Nair, P., & Muthuavinashiappan, D. (2003). ESPDA: Energy-efficient and secure pattern based data aggregation for wireless sensor networks. *Proceedings of IEEE sensors, 2*, 732–736.
4. Ozdemir, S., Ozgur Sanli, H., & Cam, H. (2004 Sep). SRDA: Secure reference-based data aggregation protocol for wireless sensor networks. In IEEE 60th conference on vehicular technology, VTC2004-Fall, Vol. 7, pp. 26–29, pp. 4650–4654.
5. Yang, Y., Wang, X., Zhu, S., & Cao, G. (2006). SDAP: A secure hop-by-hop data aggregation protocol for sensor networks. In Proceedings of the 7th ACM international symposium on mobile ad hoc networking and computing (MobiHoc '06), pp. 356–367.
6. Othman, S. B., Trad, A., Youssef, H. & Alzaid, H. (2013). Secure data aggregation with MAC authentication in wireless sensor networks. 12th IEEE international conference on trust, security and privacy in computing and communications, ISSN: 2324–898X, pp 188–195.
7. Rivest, R., Adleman, L., & Dertouzos, M. (1978). On data banks and privacy homomorphisms. *Foundations of Secure Computation, 4*, 169–179.
8. Girao, J., Schneider, M., & Westhoff, D. (2005). CDA: Concealed data aggregation in wireless sensor networks. *IEEE International Conference on Communications, 5*, 3044–3049.
9. Wagner, D. (2004). Resilient aggregation in sensor networks. In Proceedings of the 2nd ACM Workshop on Security of Ad-hoc and Sensor Networks.
10. Perrig, R. S., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks, 8*(5), 521–534.
11. Junior, W., Figueriredo, T., Wong, H.-C. & Loureiro, A. Malicious node detection in wireless sensor networks. The 18th International parallel and distributed processing symposium (IPDPS'04), April 26–30, 2004, Santa Fe, Nex Mexico, USA
12. Curiac, D.-I., Banias, O., Dragan, F., Volosencu, C. & Dranga, O. (2007). Malicious node detection in wireless sensor networks using an autoregression technique. The 3rd International conference on networking and services (ICNS'07), June 19–25, 2007, Athens, Greece.
13. Yim, S.-J., & Choi, Y.-H. (2012). Neighbor-based malicious node detection in wireless sensor networks. *Wireless Sensor Network, 4*, 219–225. https://doi.org/10.4236/wsn.2012.49032.
14. Gomathi, G., Yalini, C., & Revathi, T. K. (2014). Secure data aggregation technique for wireless sensor networks in the presence of security threats. *International Journal of Emerging Technologies and Engineering (IJETE)*, *1*(9), 229–234.
15. Ayday, E., Lee, H., & Fekri, F. (2009). An iterative algorithm for trust and reputation management. In Proceedings of the IEEE international conference on symposium on information, pp. 2051–2055.
16. Jiang, J., Han, G., Wang, F., Member, S. L. (2015). An efficient distributed trust model for wireless sensor networks. IEEE, and Mohsen Guizani, Fellow, IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 5, May 2015.
17. Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2015). Defending against collaborative attacks by malicious nodes in MANETs: Cooperative bait detection approach. *IEEE Systems Journal, 9*(1), 65–75.
18. Grgic, K., Zagar, D., & Cik, V. K. (2016). System for malicious node detection in IPv6-based wireless sensor networks. *Journal of Sensors*. https://doi.org/10.1155/2016/6206353.
19. Nirmal Raja, K., & Maraline Beno, M. (2017). Secure data aggregation in wireless sensor Network-Fujisaki Okamoto (FO) authentication scheme against Sybil attack. *Journal of Medwell Systems*. https://doi.org/10.1007/s10916-017-0743-2.
20. Shim, K. A., & Park, C. M. (2015). A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. *IEEE Trans. Parallel and Distributed Systems (TPDS), 26*(8), 2128–2139.
21. X. Jinhui, T. Yang, Y. Feiyue, P. Leina, X. Juan., H. Yao. (2018). Intrusion detection system for hybrid DoS attacks using energy trust in wireless sensor networks. Scicedirect, Procedia, Computer Science 131, 8th International Congress of Information and Communication Technology (ICICT-2018), pp. 1188–1195.

**Dr. S. Gomathi** received her B.E from M.S. University and M.E. (CSE) degree from Anna University, Tamil Nadu. She received her Ph.D from Anna University, Chennai. She has teaching experience of more than 12 years. Her research interests include wireless sensor networks, cloud computing and big data. She has published many papers in International Conferences and reputed journals in networks.

**Dr. C. Gopala Krishnan** received his PhD in Computer science and Engineering in 2018 from St. Peter's University, Chennai, India. He received his M.E. degree in Computer science and Engg in 2010 from Anna University Tirunelveli, India and B.E. degree in Computer Science and Engineering in 2002 from Madurai KamaRaj University, India. His areas of interest are Mobile computing, Operating systems and Computer Networks and Multi Core Architecture. He has published many papers in International Conferences and journals in various fields.