Secured File Sharing using Trust Mechanism in Wireless Sensor Network

Vaishali Gupta
Assitant Lecturer
Computer Science and Engineering
Chitkara University
Rajpura, India

Manik Gupta
Assistant Professor
Computer Science and Engineering
Chitkara University
Himachal Pradesh, India

ABSTRACT

Wireless sensor network is an emerging technology. WSN's are deployed in an open and unattended environment. Therefore they are prone to security threats. The traditional approach of cryptography alone was not sufficient for security. Cryptography was not able to prevent internal adversaries from inserting the forged data. As a result Trust factor scheme was introduced in wireless sensor networks to prevent internal security threats in a network. In a distributed deployment of wireless sensor network, nodes communicate with each other on the basis of their trustworthiness. But in a huge network it becomes challenge for sensor nodes to recognize all the sensor nodes present in a network and retain their trust values with it, as the changes are very frequent in wireless sensor networks. So nodes are more vulnerable to attacks. In a proposed work, the main base station keeps the trust value of all the sensor nodes. The trust values are defined by belief of an individual node in a network. Belief is the subjective trust which can be justified by the past judgments in a network. If the value of belief is more, the sensor node will be more trustworthy. Different algorithms have been applied to authenticate the new sensor node and to provide secured file sharing in a wireless sensor network.

Keywords

Belief, Reputation, Sensor, Trust

1. INTRODUCTION

Wireless Sensor Network is a combination of sensor nodes which works in an open and real time environment. Wireless sensor network works on low cost, low power capacity. The sensor nodes communicate at small distances and are multifunctional. Sensor nodes are deployed at large number in the environment. Sensor nodes monitor homes, cities and environments where users are not capable to reach easily. High peaks, forests, defense areas etc. Wireless sensor network is used to monitor the environment in which the sensor nodes sense the data from the environment and send this information to the sink node or main base station where this information is further processed. When the access to the location is prohibited or remote areas where it is not easy to reach, the sensors nodes can be deployed there. The data that is collected from the sensors nodes can be sent to the central node for processing [1]. There are different applications of wireless sensor network which is used in day to day life. Some of the applications are discussed.

Habitat Monitoring: Sensor nodes acquire data without any interruption in habitats where human presence can affect the breeding rate in animals and plants.

Serve Multiple Purposes: Sensor nodes serve different purposes in different environments. They are scalable so can do different tasks in different environments. They can use in sensing seismic data, acoustic data and high resolution images. They provide multi-dimensional view of the environment.

Agricultural uses: Heat, humidity, soil moisture, temperature and nitrogen content in soil can be monitored using sensor nodes. Measuring these factors can lead to the good growth of crops.

Motion tracking: Sensor nodes sense movements in a room. These nodes can install in the rooms which serves the purpose lights get automatically switched off when no one present in the room. Nodes installed in the vehicles which sense the automobiles disturbances [2].

Seismic sensing: Sensor nodes can provide more precise study on seismic activities than other studies. It provides aftermath of earthquakes on buildings very precisely. Sensor nodes deployed in different parts of a building which provides the effects of earthquake strength to the building [3].

Security: Sensor nodes can deploy for security purposes. Military can deploy sensor nodes on borders which can detect armed men while crossing the border and alarmed border patrolling team [4].

Wireless sensor network often deployed in an open environment, therefore they are prone to security attacks. The security attacks are of two type: external and internal. Security attacks can degrade data confidentiality, source authentication and integrity. A single attack can make whole network unusable. So to avoid these there are different methods introduced to secure the integrity of the confidential data. The security primitives like trust management provide robustness and reliability to the network. It provides trust on the behavior of the network elements which increases the security in the network. Trust is the security mechanism which is used to maintain the integrity of the network. Trust management techniques are used to detect the malicious node in a network. It protects from internal attacks. [5]Trust is an abstract entity with the influence of which people interact with each other. Same happens in a sensor network. Trust can be calculated on the basis of degree of belief. More belief, more trust. Degree of belief tells about the future behavior of nodes present in a network which is based on the past behavior of the nodes [6]. The trust management systems also take the concept of reputation into consideration. Trust management can be done in two ways: In the first way the trust is computed by obtaining values from individual peer to peer behavior. Second way is the certificate based. In certificate based method trust is established from a valid certificate that proves the target node is trustworthy. The certificate is issued by either trusted base station or the other nodes which issue trust in the network. [7]

This paper is organized as follows- Section 2 describe Related Work, section 3 describes proposed methodology, section 4 describes the experimental results and section 5 describes the conclusion and future work.

2. LITERATURE SURVEY

Different trust models have been proposed by researchers. Trust models can be classified into two categories Centralized and Distributed. In centralized trust models main base station is used to calculate the trust values for sensor nodes but in distributed trust models, sensor nodes calculates trust by themselves. In this context researchers proposed many trust models. The Trust Computation method using Fuzzy Logic has been developed by Tae Kyung Kim and Hee Suk Seo. In this method the trustworthiness of the path has been calculated by nodes' trust values. In a network more the value of trust for nodes more is the trustworthy path. This model uses fuzzy logic deduction to quantize the imprecise or uncertain data [8].

Another proposed model is Reputation based Framework for sensor network. In RFSN the trust is updated according to aging mechanism. Every time node interacts in the network its reputation score increases or decreases according to its behavior in the network. This model improves the security for each node but is unable to increase the robustness [9] of the system.

In Parameterized and Localized trust management Scheme each sensor node maintains abstracted parameters which are useful to calculate the trustworthiness of the neighbor nodes and helps in detecting the malicious nodes in the network. In this model all important control packets generated by base station contain a hashed sequence number. But the hashed sequence number increases the size of a packet which may lead to the more energy consumption for the transmission and [10] receiving of the packet. Therefore the PLUS scheme is not successful in high traffic networks because its trust convergence rate is high.

The Agent based trust model uses agent nodes to monitor the sensor nodes. Agent nodes calculate the trust values for the sensor nodes. The computational complexity of ordinary sensor nodes increases due to agent nodes in a network. Only agent nodes are responsible for calculating trust in a network, So in heavy traffic neighbor nodes behavior may not be fully recorded. The performance of agent based trust highly relies on agent nodes. If an agent node becomes malicious then the integrity of whole network will be compromised [11].

In real time scenarios wireless sensor networks are organized in this way that it will lower the energy consumption of communication overhead and increase the security and connectivity of a network. Researchers proposed trust models for cluster based WSN's in which the trust is calculated on the basis of whole cluster in the network not for the individual node present in the network. Group based Trust Management Scheme (GTMS) gives single trust value to the whole group. In this scheme all sensor nodes within a group calculate trust values individually for all group members, after that cluster head aggregate those values and send it to the base station. Then the base station will assign the possible state to the group on the basis of cumulative trust value of the whole group calculated by it. The states are: trusted, untrusted and uncertain. Therefore, the state of the whole group is calculated and stored by the base station [12].

Researchers Bo Zhang et.al proposed ML-Trust, a multiple-level trust management framework for trust management in wireless sensor networks. They use three levels to establish trust between sensor nodes of a network. Subjective trust is known as a belief. Objective trust is termed as reputation. Third one the recommended trust method which is used to get trustable impressions from strangers [13].

Uyen Trang Nguyen et.al proposed authentication protocols to support fast handover. In these protocols the handover authentication does not require authentication server to be involved. The mobile clients directly authenticate via mesh points using tickets [14].

3. PROPOSED ALGORITHM

The aim of the proposed framework is to increase the trustworthiness of a network. Trustworthiness of a network is achieved by belief factor. The framework is designed which consists of main base station, cluster heads, sensor nodes and database. The belief resides at base station for every sensor node present in a network which gets updated with every transaction. The authentication of sensor nodes has done by main base station. The trustworthiness of sensor node is calculated by belief of a node. The belief of sensor nodes present in a network is saved by main base station and updated after every file sharing. The file sharing has been carried out between two sink nodes of different clusters. The trustworthy secured file sharing in a network consists of different steps which are discussed below:

3.1 Base Station

Base station is the main authenticating entity of a network which issues authentication certificate for sensor nodes and users in a network. The cluster heads communicate with base station for the authentication of sensor nodes. Sensor nodes do not keep a routing table with them in which belief of neighbor sensor nodes resides. As the size of network increases due to demand of a network then it becomes very difficult for sensor nodes to keep routing table for every neighbor node present in a network. Base station is directly connected with a database which contains routing table of sensor nodes with its belief in a network. So the main base station decreases the complexity of a network. The belief of a network is a subjective trust which depends on the past judgments or experiences in a network for a node. If the transaction is successful with respect to the sensor node with less number of faults and increased confidentiality of data then the belief of a sensor node is updated at database. It increases the accuracy of a network. The trust is high of a network if the belief of each and every node is high. The belief of a node with every transaction increases if and only if the network does not allow any adversary to come in a network. The communication of confidential data takes place with those sensor nodes in a network which are having high belief. In the proposed work the main base station communicates only with the cluster heads of a network.

3.2 Cluster Head

Cluster head is a head for all the sensor nodes present in a network. Any sensor node which wants to communicate in a network, want to send a file or any new sensor node which wants to get connected in a network seeks authentication from the cluster head in a network. Cluster head communicates with the base station as well as with the sensor nodes in a network. It is the intermediate between sensor nodes and the base station. Sensor nodes send request to the cluster head, cluster head forward that requests to the main base station for the authentication of sensor nodes and trustworthy path in a network. After getting authentication from base station it forwards confirmation to the sensor nodes.

3.3 Authentication of Sensor Nodes

The authentication of sensor nodes is done by main base station. When a sensor node wants to enter in a network it sends request to the sink node present with which it wants to get connected. It sends its credentials to the sink node eg. ip address. The sink node encrypts sensor node's details via AES (Advanced Encryption Standard) algorithm. Then these details will send to the cluster head via multiple hops present in a network. Cluster head forwards these details to the main base station. Base station decrypts the details and checks the details of the sensor nodes in its database, its ip address, belief. If belief of a node is high then base station issues a certificate to the cluster node that the sensor node is authenticated and can be added in a network. Every time node sends file in a network its belief get updated at the base station for its successful and secured transmission in a network. More the belief of the node more is its trustworthiness. In the proposed framework AES algorithm has been used to send credentials of sensor node to the base station. As base station stores the routing table for sensor nodes in a network AES algorithm takes less time for the communication in a network. The overhead will be less for communication. AES algorithm provides low latency and high throughput in a network. Therefore, it provides faster encryption. So it will save the energy of the nodes in a network. It is more secure algorithm. The belief of a node on the basis of past judgments concerning the target node can be calculated by the base station by using the formula. Initially there are two nodes d_i and d_j. d_j interacted with d_i n times in the past. Every interaction calculates the judgment value. $Jud_t(d_j)$ (jud t(dj)ε[0, 1]) Assume that malicious judgments are denoted by m. The belief from di to each similar type of node dj is signified by belief (di, type(dj)). The belief of past judgments can be calculated as:

$$belief_{j(d_i,d_j)} = \begin{cases} \frac{\sum_{t=1}^{n} jud\ _t(d_j)}{n} \times \left(\frac{n-m}{n}\right)^{\frac{1}{n-m}} & n \neq 0 \\ \alpha \times \frac{\sum belief\ (d_i,type\ (d_j))}{p} & n = 0 \end{cases} \qquad (1)\ [13]$$

3.4 File Sharing

After authentication of sensor nodes in a network the sharing of files between two clusters will take place. When a node in one cluster wants to send a file to a node of different cluster, the file will be sending in an encrypted form. The file will be encrypted via fully homomorphic algorithm. The fully homomorphic algorithm increases the security of cipher text as in fully homomorphic algorithm computation can be done when the file is still in the encrypted form. One person could add two encrypted numbers and then another person could decrypt the result without even knowing about the individual numbers. Fully homomorphic encryption algorithm provides ability to compute on cipher text instead of the plain text. The fully homomorphic algorithm revolutionized the file sharing system in wireless sensor networks.

4. EXPERIMENTAL RESULTS

This section shows the results computed by the proposed framework. The result is calculated on the basis of accuracy, client mobility speed and computation cost.

Accuracy: The accuracy of the proposed belief computation framework is compared with paper [13] against 4000 number of transaction. As authentication of sensor nodes present in a network is given by the main base station which is based on the past interactions in a network. The average accuracy with 4000 transactions is 97.

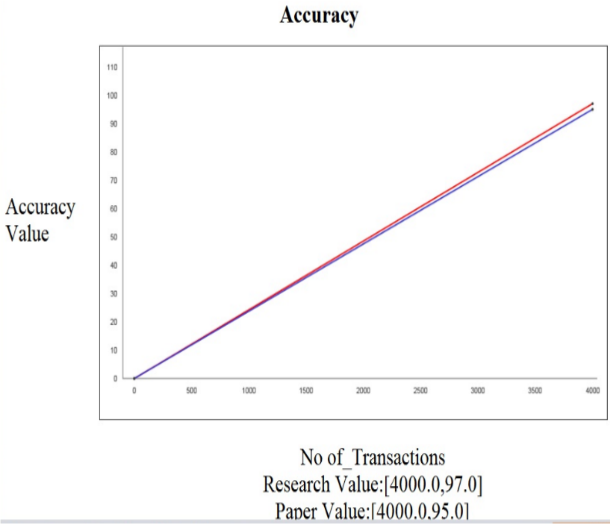

Fig 1: Graph showing the accuracy of proposed method as compared to paper [13]

Client Mobility Speed: The fast handover allows a user to send file from different cluster with which it was not associated earlier. The user will get authenticated from the main base station and can send file. The mobility of user from one cluster to another cluster is the client mobility speed. The client mobility speed is compared with paper [14].

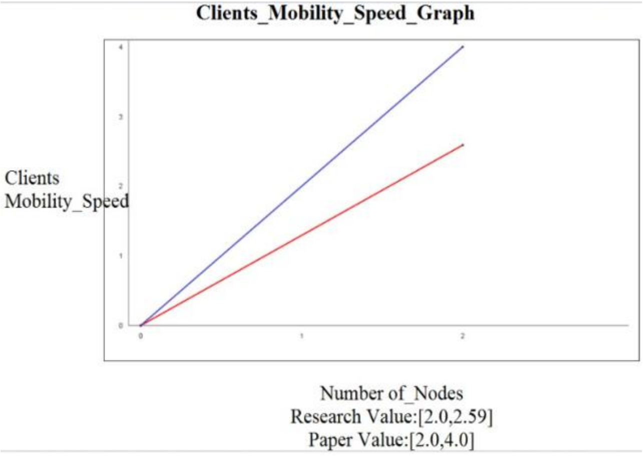

Fig 2: Graph showing the Client Mobility Speed using the proposed method as compared to paper [14]

Computation cost: Computation cost is the latency time which it take to encrypt and decrypt the file when it is send from one cluster to another cluster. Computation cost is decreasing in comparison with paper [14]

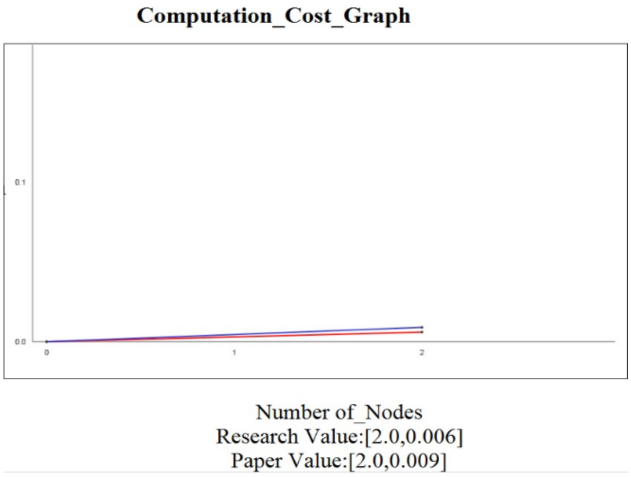

Fig 3: Graph showing the Computation Cost using the proposed method as compared to paper [14]

5. CONCLUSION

The security threats are rising for wireless sensor networks as they work in an unattended and open environment. Traditional cryptography techniques alone were not efficient to provide security in wireless sensor network completely because they provide only external security but WSN's lacks in internal security. So, different trust mechanisms were introduced to provide security to the internal wireless sensor network. The proposed framework has main base station which authenticates the sensor nodes present in a network. The trustworthiness of sensor nodes is checked by the belief of a node. Belief of an individual node increases with each transaction in a network. After the node authentication by main base station the sharing of files between two clusters can be done. Various algorithms are used for the authentication and sharing of file in a network. The proposed work increases the security of network by reducing the entry of malicious nodes in a network. The computation cost during file sharing has been decreased. The client mobility speed increases when it switches from one cluster to another cluster to share the file. In the future work, different algorithms can be applied to get good results in terms of accuracy. This can be applied on the distributed system to enhance the capability of sensor nodes.

6. REFERENCES

[1] Agrawal, Dharma, and Qing-An Zeng. Introduction to wireless and mobile systems, Cengage Learning, 2015.

[2] Al-Turjman, Fadi M., Hossam S. Hassanein, and Mohamed A. Ibnkahla. Efficient deployment of wireless sensor networks targeting environment monitoring applications. Computer Communications 36. no. 2 . pp. 135-148. 2013

[3] Liu, Guojin, Rui Tan, Ruogu Zhou, Guoliang Xing, Wen-Zhan Song, and Jonathan M. Lees. Volcanic earthquake timing using wireless sensor networks. In Proceedings of the 12th international conference on Information processing in sensor networks. pp. 91-102. ACM. 2013.

[4] Pannetier, Benjamin, Jean Dezert, and Genevieve Sella. Multiple target tracking with wireless sensor network for ground battlefield surveillance. In Information Fusion (FUSION). 2014 17th International Conference on. pp. 1-8. IEEE. 2014.

[5] Lu, Huang, Jie Li, and Mohsen Guizani. Secure and efficient data transmission for cluster-based wireless sensor networks. Parallel and Distributed Systems. IEEE Transactions on 25 no. 3 750-761.2014

[6] Dhulipala, V. S., Karthik, N., & Chandrasekaran, R. M.. A novel heuristic approach based trust worthy architecture for wireless sensor networks. Wireless personal communications, 70(1) pp: 189-205 2013.

[7] Gago, M., Rodrigo Román, and Javier Lopez. A survey on the applicability of trust management systems for wireless sensor networks. Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. SECPerU 2007. Third International Workshop on. IEEE 2007.

[8] Rana, Sohel, Ali Newaz Bahar, Nazrul Islam, and Johirul Islam. Fuzzy based Energy efficient multiple cluster head selection routing protocol for wireless sensor networks. International Journal of Computer Network and Information Security (IJCNIS) 7 no. 4 : 54-61 2015.

[9] Alzaid, Hani, Manal Alfaraj, Sebastian Ries, Audun Jøsang, Muneera Albabtain, and Alhanof Abuhaimed. Reputation-based trust systems for wireless sensor networks: A comprehensive review. In Trust Management VII,. Springer Berlin Heidelberg, pp. 66-82. 2013.

[10] Yao, Zhiying, Daeyoung Kim, and Yoonmee Doh. PLUS: Parameterized and localized trust management scheme for sensor networks security. In Mobile Adhoc and Sensor Systems (MASS) 2006 IEEE International Conference on pp. 437-446. IEEE, 2006.

[11] Govindan, Kannan, and Prasant Mohapatra. Trust computations and trust dynamics in mobile adhoc networks: a survey. Communications Surveys & Tutorials IEEE 14.2 pp: 279-298,2012.

[12] Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems (Volume:20 , Issue: 11) page 1698 – 1712, IEEE Computer Society, Nov. 2009

[13] Zhang, Bo, Zhenhua Huang, and Yang Xiang. A novel multiple-level trust management framework for wireless sensor networks. Computer Networks 72 pp: 45-61,2014.

[14] Li, Celia, Uyen Trang Nguyen, Hoang Lan Nguyen, and Nurul Huda. Efficient authentication for fast handover in wireless mesh networks. computers & security 37 pp: 124-142,2013.