International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(3), pp.188-191
DOI: http://dx.doi.org/10.21172/1.83.027
e-ISSN:2278-621X

ATTACKS AND COUNTERMEASURE, TRUST MODEL IN WIRELESS SENSOR NETWORK: RESEARCH CHALLENGES

Shaileshkumar Mahendralal Gheewala[1]

Abstract- A wireless Sensor network (WSN) consists of battery operated sensing and computing devices deploying for monitoring application. With the advent of new technologies WSNs are providing a new class of information to human beings, In most cases the network are stationary but as a revolutionary step the WSNs have to consider mobility. Recent research has provided means by which WSN has more secure communication or data aggregation. The unreliable network and deployment of nodes in open environments leads to several kind of attack. In this research paper analyzed existing attacks, counter measure model and methods are proposed.

Keywords – Wireless Sensor Network, Security issue, Trust based Model.

I. INTRODUCTION

The Wireless Sensor Network (WSN) consists of large number of deployed sensor nodes and base nodes. In the near future, due to immense development of MEMS technology the wireless sensor networks are anticipated to consist of thousand of inexpensive nodes, each having sensing capability with limited computational and communication power.

The node consists of one processing unit like microcontroller or microprocessor (generally 8 or 16 bit), memory unit and power unit. Base node or sink node received data from the deployed node which measure any physical quantity.

The sensor node can be used in variety of application such as military, environment, wildlife, home automation and health monitoring etc. As, node are deployed in environment, the network is more susceptible for attacks. The cryptographic solution is used for other network are not fusible due to resource constraints. This leads WSN in need of a new approach for providing security. It must be light weighted in terms of processing and communication cost in order to increase lifespan of the network.

The research paper was proposed after study and analysis of existing attacks and counter measure for that attack's algorithm in terms of memory and power consumption.

However, the following issues are reaming:

- By using various counter measure algorithm process become delayed
- Overall system performance becomes very slow as number of nodes is increase.
- Multiple message transmission affected.

The section II describes various kind of attacks in wireless Sensor Network, Section III provides Trust and Trust based Management System, and Section IV discuss about Trust based model and Limitations followed by conclusion and references.

[1] *Department of Electrical Engineering Government Polytechnic, Valsad, Gujarat, India*

II. ATTACKS IN WIRELESS SENSOR NETWORK

The wireless sensor networks are more prone to attacks as they are deployed in the environment. This section provides the list of existing attacks.

A. Sniffing attack–

Sniffing attack is generally found in following kind of topology in which data can reach to the sink by hop to hop basis. A node can listen to all the packets sent by its all neighbors. However, if two nodes are exchanging information regarding routing, data or signaling information and the malicious node overhead it, then in future the malicious node can go for new types of attacks in the network.

Countermeasure

Cryptography of messages which needs point to point communication reduces the sniffing attack. But key management and heavy cryptography algorithm like RSA, DES, and AES make process slow and consume more power in processing rather in communication.

B. Hello Flood Attack –

Hello packets are used to exchange routing information. Each node broadcast the information, if it comes to know that there is an update for shortest path to sink node. This creates flooding in entire network. An intruder will always try to broadcast the packet subsequently advertising low-cost routes. The sensor node is generally deployed for application in the environment and nodes configured themselves and preparing the routing table for reaching sink via neighbour nodes with minimum hop count. In case of dynamic network every new node in the network broadcast the advertising of minimum hop count message and that will cross verify by other nodes. It causes the delay in entire process. The energy consume by the node for routing information is more rather data aggregation.

Countermeasure

The static and pre planned location of node avoid the flooding attacks in the network. If dynamic topology required then Hash key authentication algorithm is good solution with lowest bit authenticate key.

C. *Energy Drain Attack*

The attacker initiates the large no of traffic through which the energy of the network gets drained. Eg. Denial-of-services attacks.

Countermeasure

As, WSN is energy constrained network and this kind of attack drain the network lifespan. The data aggregation and cluster head based approach overcome the energy drain attacks.

D. *Droop Packet Attacks*

In this type of attack node try to catch the packet and drop them. In multihop kind of network and data aggregation algorithm affect lot with this kind of attack.

Countermeasure

Authentication key, secure

routing algorithm with proper weight channel and monitor the behavior of the sleep and wake time of node with reduce amount of acknowledge and handshaking frame can overcome Droop packet attacks.

E. *Sink, black, grey and worm hole attack*

In sink hole attack, false node misguide the other node of network by advertising shortest path to base station or sink node. The advertisement packet consist of black hole attack signifies the low latency channel for sink node. The attacker forward this packet to other node and try to find out other information by proper study of packet like node Id, packet size and authentication key and MAC address of the node. Where worm hole attack drop certain type of packet like routing and handshaking information packet. The combination of Sink, Black and worm hole packet Detroit the network performance.

Countermeasure

Secure routing algorithm with proper end to end communication. Static and fixed topology overcomes this problem. [1-4]

F. *Stealthy attack*

In this type of attack, attacker tries to send the high or low value of data rather than aggregate data value. The stealthy attack is targeted for dynamic and distributed type of network where cluster head send the aggregate data to the sink node. Cluster head algorithm works on selection of minimum or aggregate data collected from the neighbour node. So, poor data aggregation algorithm easily broke by sending false value of aggregation function.

Countermeasure

To overcome stealthy attack the cluster head threshold design such a way that it can sense the drastic change of neighbour data. Cluster head has to compare the current data with the previous aggregate data and threshold data.

The attacks which discussed above are applicable for hop to hop architecture and every node depends on the neighbor node for data, routing and control information. For proper management of node functionality still it require more research work in synchronization, sleep and wake time MAC algorithm. To overcome intruder attacks trust based mode between the neighboring node proposed by many researchers and few popular model discuss in the section III but still more research work require for tiny device have low processing, power and memory capability.

III. TRUST AND TRUST MANAGEMENT SYSTEM IN WIRELESS SENSOR NETWORK

It has been used in field like e-bay, e-commerce application, and MANET etc. All trust model applied in specific application are not same would not apply to WSN. As, WSN is more resource constrain in terms of processing, space and communication.

Trust is normally interpreted as belief, subjective probability or reputation. Trust is subjective opinion in the reliability of other entities or functions, including veracity of data, connectivity path, processing capability of node and availability of services etc.

The trust is subjective, dynamic, asymmetric, non transitive and reflexive in characteristics. In the network, each node collects information about services provided by its neighbors. When a node needs the service of its neighbor nodes, it uses the collected information to calculate the trust, based on which it decides whether to get services with its neighbor or not. [5]

Trust Management System

The trust is generally for node trust, communication trust and path trust in the network. The following methods are for trust management system.

A. *Threshold of Trust value*

The threshold value for particular value can be high or low depending on the application and trust based model and threshold value could be continuous or discrete.

B. Data Gathering

Data gathering can be implicit or explicit. It can be collecting the data implicitly based on observation of other entity or by explicitly sending request to other entity to send required information. [6]

C. *Decision making and updates*

Based on trust value, the node performs necessary action with other entity. After action gets completed, based on result of action, the node updates the trust value. If entity behaves in the same manner as predicted, then update the value positively else negatively. [5]

IV. THE TRUST MODEL IN WIRELESS SENSOR NETWORK

A. *Agent based Trust Model*

Chen et al., [6] proposed an agent based trust model. ATSN (Agent based trust on sensor network) runs at middle-ware of every agent node. As, agent based approach is applied for multi hop WSN communication topology. In that every node monitor the behavior of the neighbor node like forwarding data time and control frame time and processing time for algorithms. The ATSN and RFSN are almost similar with one another and differ with several uncertainties.

Limitation of Trust based Model

ATSN uses agent nodes with more power, long radio range and large storage space then normal sensor node to perform operations. ATSN work with fixed window and aging is specified by considering the positive outcome from current window. The agent node propagates the trust value to sensor node with encryption technique.

B. Weight based Trust Model

Hur et al. [7] proposed a weight based trust model. The trust is used to eliminate data from malicious node, during data aggregation. The every node is capable enough to compare the receive data with sensed data duration and develop a weight trust model on it.

Limitation of Weight based trust model

The model highly based on synchronism phenomenon.

C. BEACON BASED TRUST MODEL

Srinivasan et al. [8] propose a reputation based beacon system. The system was developed on the location information of the node. When node advertise beacon that time it also advertise its location to neighbor node. The node with location information consider as a malicious node and reputation develop with location information is quite slow process for huge node network.

A sensor node uses a neighbor reputation table to determine whether or not to use a given beacon's location information based on a simple majority scheme. This will help to find out malicious node.

Limitation of Beacon Trust Model

Beacon Trust model is depend on the neighbor reputation table that highly vulnerable for attacks.

ATTACK RELATED TO TRUST BASE MODEL IN WSN

The good node sends the negative feedback for reputation. There is little method by which malicious node try to establish trust in WSN.

- The node just spoofs their identity with different MAC address or with different authentication key id.
- The malicious node sends different trust or threshold value for all neighboring node to develop the trust.

V.CONCLUSION

Importance of Wireless Sensor Network cannot be denied as the world of computing is getting portable and compact. Unlike wired networks, WSN pose a number of challenges to security solution due to their unpredictable topology, wireless shared medium, heterogeneous resources and stringent resources etc. Security is not a single layer issue but multilayered issue. It requires multi fence security solutions that provide complete security spanning over the entire protocol stack. The existing protocols are typically attack- oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol. Therefore, more ambitious goal for WSN, MANET and ad hoc network security is to develop a multifence security solution that is embedded into possibly every component in network, resulting in depth protection that offers multiple lines of defense against many both known and unknown security threats.

REFERENCES

[1] C. Karlof, D. Wagnor, "Secure routing in wireless sensor networks: attacks and countermeasures", University of California at Berkley, USA.

[2] J.P. Walters, Z.Liang, W. Shi, and V.Chaudhary, "Wireless Sensor Network Security: A Survey", Department of Computer Science Wayne State University.

[3] F.Stajano, R.J.Anderson, The resurrecting duckling: Security issue for ad-hoc wireless networks, in seventh international security protocol workshop, 1999, pp. 172-194.

[4] L.Zhou, Z.Hass, Securing ad hoc networks, IEEE network magazine 13 (6) (1999) 24-30.

[5] V.Geetha, K.Chandrasekaran, " Trust Model in Wireless Sensor Nework:Research Challenges" in International Conference on Emerging Trends in Engineering (ICETE'10), Karnataka, India

[6] Chen, H.Wu, X.Zhou and C.Gao, "Reputation-based Trust in Wireless Sensor Networks", in International Conference on Multimedia and Ubiquitous Engineering (MUE'07), Seoul Korea, 2007.

[7] J.Hur, Y.Lee, H.Yoon, D.Choi and S.Jin, "Trust Evaluation Model for Wireless Sensor Networks", in the 7th International Conference on Advance Communication Technology (ICACT'05), Gangwondo, Korea 2005.

[8] D.Liu, P.Ning and W.Du, " Detecting Malicious Beacon node for Secure Location Recovery in Wireless Sensor Networks" in the 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05), 2005.