Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 11, pp.42249-42252, November, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

DETECTION AND REMOVAL OF SECURITY ATTACKS USING ALARM PROTOCOL IN WSN ENVIRONMENT

***Bhawna Dhruv and Vibhor Dhruv**

JIMS, Greater Noida, VIPS IP University, India

ARTICLE INFO

Article History:
Received 15th August, 2016
Received in revised form
14th September, 2016
Accepted 21st October, 2016
Published online 30th November, 2016

Key words:

MANET, ALARM, Security Attacks, Wireless Sensor Network.

ABSTRACT

A mobile ad hoc network comprises of many mobile wireless nodes. MANET is a self configuring network and such network can be organized easily without any base station. MANET can be very efficiently used in salvage related area, military and law enforcement. But it faces the issues of security and confidentiality, especially when used in susceptible areas. Safe routing protocols have been refined to provide protection and confidentiality at various levels for e.g. ALARM protocol (Anonymous Location Aided Routing) provides both privacy features and security which includes data virtue, node verification and obscurity. This network focuses on achieving the major security objectives which are Confidentiality, Authentication, Authorization and Integrity. In this paper, we have proposed ALARM protocol in WSN environment which uses network time protocol synchronization and removes the malicious node from the network, hence preventing the network from attacks.

Citation: Bhawna Dhruv and Vibhor Dhruv, 2016. "Detection and removal of security attacks using alarm protocol in wsn environment", *International Journal of Current Research*, 8, (11), 42249-42252.

INTRODUCTION

Wireless Networking is an automation field in which two or more systems interact with each other using typical network protocol without using any cable. Such networks are of two type: Infrastructure or Infrastructure less. In Infrastructure network, the interaction takes place among the wireless nodes and few access points. Ad hoc network is a type of infrastructure less and decentralized type wireless network which basically means, there is no actual infrastructure such as router devices or access points in wireless networks. In routing process each node involves itself by forwarding data to and for all the nodes (Israel Levya Mayorga, 2014). In ad hoc network, the regulation of which node to forward data is made dynamically on the basis of network design and connection. Essentially, it is a network which is generally used in emergency situations. A fixed infrastructure is not required in such types of networks. Nodes which are in close radio range, interact directly which each other using the wireless links where as the nodes which are far from each other take the help of intermediate nodes so that relay message can be passed. Wireless networks are the networks which make use of radio waves or microwaves in order to establish interact between the devices. In such network, all the nodes acts as router. MANET is mobile ad-hoc network. It is self-establishing network which is infrastructure less in nature. In MANET different mobiles are associated through different wireless link. Every mobile node can freely move, which further means that there is no central control available. In MANET, mobile nodes can join or leave the network at any instance (Shen and Zhoa, 2013). MANET is used in some crucial applications such as: emergency salvage, vehicular network, military and law prosecution etc. There are various problems in MANET like security concerns, transfer issue etc. Due to same reason there are different types of attack which are provoked in MANET. These attacks can be of different type, such as:

- Eavesdropping is a type of attack which takes place in the mobile ad hoc networks. Eavesdropping is executed to obtain any information which is secret in nature and is kept classified during entire communication.
- Gray-hole attack's other name is routing misbehavior attack. It leads to message dropping.
- Replay Attack is a type of attack in which the attacker executes a replay attack that are repeatedly re-transmitted. The actual data that has been captured by the network is repeatedly transferred. This attack spots the route novelty and brings out the poor security design.

To isolate these attacks from interaction path in the network, there are different techniques which we will be discussed further. In this proposed mechanism, we tried to prevent these attacks (Replay Attack) by using mutual authentication among the nodes in the entire network. For this, we used

****Corresponding author: Bhawna Dhruv,***
JIMS, Greater Noida, VIPS IP University, India.

authentication based protocol called ALARM using cryptographic mechanism of digital signature in the wireless sensor network.

Manet

MANET is a type of mobile ad hoc network. This is a self configuring and infrastructure less network. In this network, many mobile nodes are connected through wireless link. There is no central controller available in this network. Type of MANET are:

1) Wireless sensor network: A wireless sensor network is a group of devices which are sensing in nature and are used for monitoring and recording the physical condition while passing the information to central location.
2) Wireless Mesh network: This network works upon mesh topology. This network comprises of gateway, routers and clients. The traffic in this network is forwarded by routers from gateways. This is not connected to the internet.

The absence of infrastructure in the ad hoc network proves to be a huge challenge in these networks. All the mobile nodes share the power to accept as well as route the traffic to further nodes. MANET work upon limited bandwidth and mobility of the nodes, therefore there is a need to have energy efficiency hence making the whole communication very unreliable. The protocols of ad hoc routing are:

- Zone Routing Protocol (ZRP)
- Ad Hoc On Demand Distance Vector (AODV)
- Wireless Routing Protocol (WRP)

In MANET, the topology changes very dynamically. This type of network does not have fixed infrastructure. This network have typical following characteristics : Changing topology, Limited bandwidth and energy inefficient.

A. Types of MANET

The different type of MANETs are discussed below:

- Vehicular Ad hoc network: This type of network is used for communication in the mobile vehicles. The communication does not come to halt even if the vehicles are moving in different or opposite direction.
- Intelligent vehicular ad hoc network: This is used in emergency situations. This senses the data intelligently and allows further data communication.
- Internet based mobile ad hoc network: In such type of network, the routing algorithms cannot be directly deployed. This network uses fixed nodes for data interaction.

Alarm Protocol

ALARM- It is defined as Anonymous Location Aided Routing in MANET. The nodes which are used in this protocol indicate the current location and are used to forward the data to other nodes for communication. ALARM is highly recommended because this serves the purpose of both authentication and security. It is also to prevent the network from the active and passive attacks. This basically follows 2 schemes i.e. Initialization and Operation.

Initialization

- The group manager is the head of the entire network. He is the one who adds all the nodes in the network as the group members. During this phase, every group member is assigned a private key that is unknown to anyone. This key is required to implement the valid group signatures for security purpose (Piyush Agarwal and Ghosh, 2008). Every group member has a public key as well which is only known to the group manager. The group manager is only responsible for every group signature and verifies all the signers.
- The group manager is responsible for adding or deleting the group member. The GM must check whether joining or joining is feasible for the network or not.

Operation

- The time duration is divided into equal parts. While beginning process, every node member generated a temporary public private key combination.
- Every stop will let us know about the location of the node through GPRS.
- The GPRS would contain its location, time stamp as well as the temporary public key.
- When a new 'Location Announcement Message' is received, every node member will check that the same LAM has not been received by them before (Cheng and Agarwal, 2005). When this is verified, the time stamp with group signature is checked. If all the entities are verified, the node forwards the LAM to its neighboring node.
- Whenever a node wishes to interact with the other location, it asks if the other node already exists there or not and generates a session key if there is no node at that particular location.
- Then, the message is forwarded to the nodes. The path is chosen based upon shortest path or other path computing algorithms.

Proposed Work

The protocol ALARM is used majorly for mutual authentication among the nodes. Having read the assumptions like location and time, we get to know that clocks of the mobile nodes are weakly synchronized. When the clocks are weakly synchronized in any network, then the possibility of replay attack becomes more, making the data transmission among the nodes very unreliable. In this work, we will isolate the replay attack in the mutual authentication using ALARM protocol in wireless sensor network. Using NTP, we can ensure strong clock synchronization among the nodes. The term "strongly synchronized" refers to that if the data is transferred from one node to other, the processing speed is very fast. If there exists trust relationship among the nodes, no replay attack is possible in the network because there is no waiting time in the data transfer during communication. Due to weak synchronization, the confidential information from the network may be lost. But while using NTP, mutual authentication among the nodes takes place and malicious node is removed from the network.

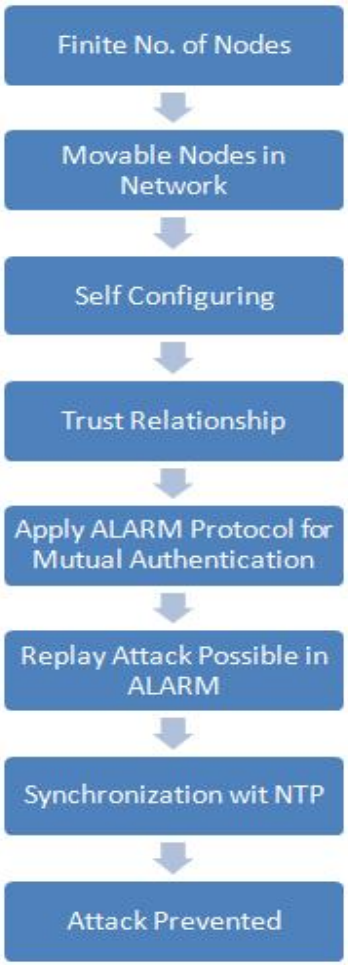

Fig.1. Flowchart of proposed methodology

RESULTS

In this figure shown below it can be seen that the flood messages moves to the monitor node which then identifies the malicious node and finds the best suitable path for further data transmission.

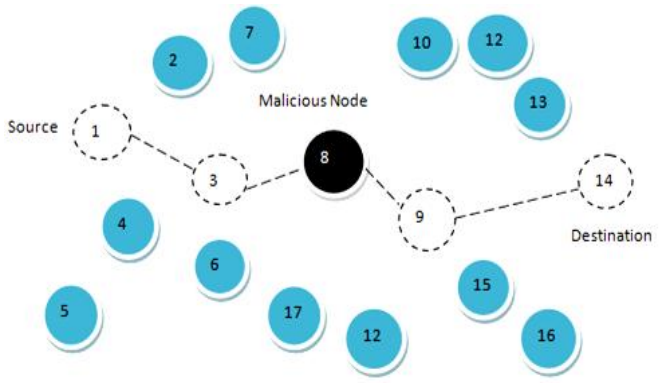

Fig.2. Malicious Node Detection

In the figure shown below, it is seen that the source node gets reply message from each node for carrying forward the data communication. In this way, the interaction among the nodes is stopped and new path is established. In the figure shown above it is clear that, due to new proposed algorithm, whenever a malicious node is detected in the network, we find the best suitable path hence removing the malicious node from the entire network.

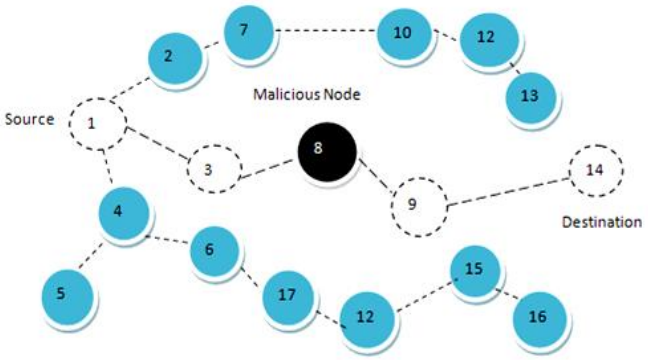

Fig. 3. New Path identified

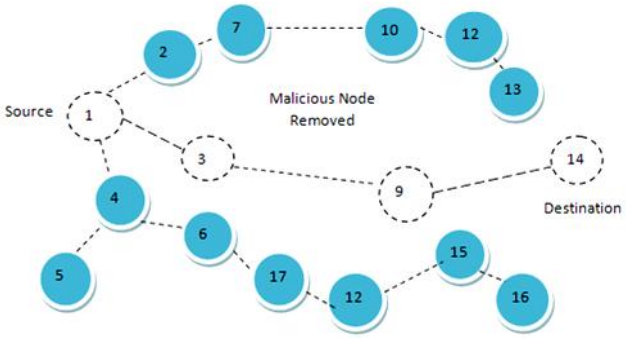

Fig. 4. Removal of Malicious Node

Packet loss

The two axis of the graph represents different entities; X being the time and Y being the packet loss. As in this network, the replay attack takes place resulting in higher packet loss due to delayed transmission of the data packets. The graph basically represents that earlier there was huge packet loss which is in green color and now it has been majorly reduced by which is depicted by red line. This is only possible due to isolation of the malicious node.

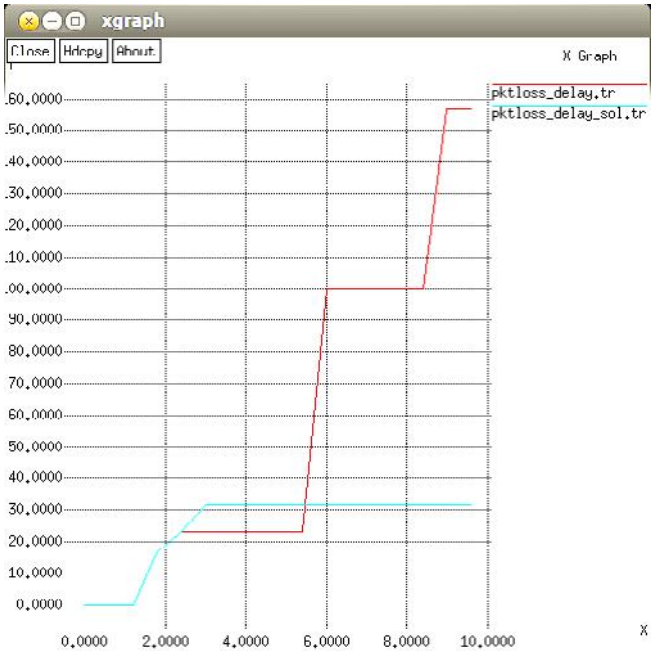

Fig. 5. Packet Loss

Network Throughput

Throughput can be defined as the average rate per unit time. In this case, it can be defined as the average rate of packets delivered successfully in per unit time. The throughput of any network should always be high. But in this case, due to replay attacks, it is very low. On the contrary, we see that the network throughput increases rapidly after isolation of the malicious node. In this graph shown below, red line represents the throughput of the network while replay attack is being taking place. Whereas the green line depicts the new throughput which is very high after the isolation of the malicious node.

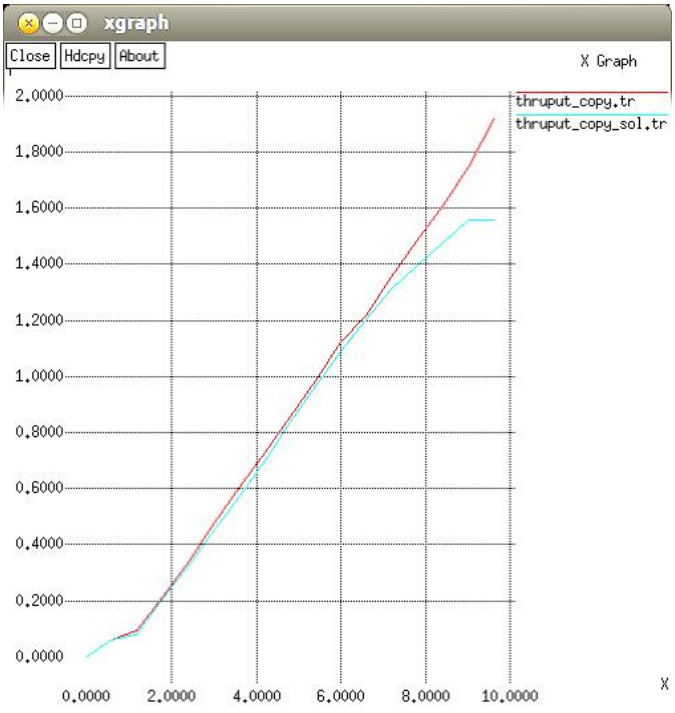

Fig. 6. Network Throughput

Conclusion

In this work, we can conclude that due to major properties of the mobile ad hoc network, various attacks are possible. These properties are open channel, infrastructure less network and variably changing topologies. These attacks can be prevented by different authentication protocols. In our work, different types of attack, their detection, isolation and impacts on the network are well analyzed. The main aim of security is that the packet transmission in the entire network from one location to another should be reliable and verified. In the network, all the nodes should follow strong trust relationship because any type of malicious node can attack the network, modifying or fabricating the information which is very important. We have reviewed the ALARM protocol in the WSN environment which has increased security as well as privacy in the networks. In our proposed algorithm, we detect and isolate any malicious using network time protocol which supports strong synchronization of the nodes in the network, reducing the packet loss and increasing the network throughput.

REFERENCES

Atif Sharif, Vidyasagar Potdar, "Prioritising Information for Achieving QOS Control in WSN", 24th International Conference on Advanced Information Networking and Applications, IEEE, April 2010.

Cheng, Y. and D Agarwal, "Distributed Anonymous Secure Routing Protocol in Wireless MANET", OPNETWORK, 2005.

Chun Ming Rong, Skjalg Eggen," A Novel Intrusion Detection Algorithm for Wireless Sensor Network", Pg 1-7, 2nd International Conference on Wireless Communication Vehicular Technology Information Theory and Aerospace and Electronic System Technology, IEEE, March 2011.

Dong, Y., T Wing, Chim," ARMR: Anonymous Routing Protocol with Multiple Routes for Communication in Mobile Ad hoc Network", Ad hoc Network, Vol 17, 2009.

Israel Levya Mayorga, "Performance Analysis of a Non Preemptive Hybrid WSN Protocol in Mobile Environment," Pg: 486-491, 28th International Conference on Advanced Information Networking and Applications Workshop, IEEE, May, 2014.

Ji Won Kim, Soo Young Moon," Improved Message Communication Scheme in Selective Forwarding Attack Detection Method", Pg 169-172,7th International Conference on Digital Content Media Technology and its Applications, IEEE, Aug 2014.

Karim El Defrway, Gene Tsudik, "ALARM : Anonymous Location Aided Routing in Suspicious MANET,"IEEE Transacions on Mobile Computing, Vol-10, Sep, 2011.

Koulali, M A., A Kobbane," Optimal Distributed Relay Selection for Duty Cycling Wireless Sensor Network", Pg 145-150, Global Communication Conference, IEEE, Dec 2012.

Liu, F., X Ching, "Insider Attacker Detection in Wireless Sensor Network", 26th International Conference on Computer Communications, IEEE, May 2007.

Pandiyan Durairajan, T Sasikala," Enhancing the Pervasive Trust Management Model in MANET by Analyzing the Factor Affecting Performance of Various Attack", International Conference on Emerging Trends in Robotics and Communication Technology, IEEE, Dec 2010.

Piyush Agarwal, RK Ghosh," Cooperative Black and Gray Hole Attacks in Mobile Ad hoc Network", 2nd International Conference on Ubiquitous IMC, Korea, 2008.

Shen H. and Zhoa L, "ALERT: Anonymous Location Based Efficient Routing Protocol in MANET,"IEEE Transaction on Mobile Computing, Vol 12 No.6, June 2013.

Srikanth B, Harish M, "An Energy Efficient Hybrid MAC Protocol for WSN Containing Mobile Nodes", Pg 1-5, 8th International Conference on Information Communication and Signal Processing, IEEE, Dec 2011.

****