IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ANALYSIS AND REVIEW ON VARIOUS SECURITY ISSUES AND THEIR PREVENTION TECHNIQUES IN THE AD-HOC SENSOR NETWORKS

Dr. Srinivas Ambala*, Dr. Ravi Kumar Yeatha
[*] Associate Professor VMTW, Hyderabad
Professor KMIT, Hyderabad

DOI: 10.5281/zenodo.290263

ABSTRACT

Ad-hoc Sensor Networks (ASN) is the most demanded and happening research area now a day. Here mainly the security is important issue in ASN. The following paper describes process of communication in MANET, Security issues, Black hole attack, and Intrusion detection. In the mobile ad-hoc network the nodes keep travelling in its surrounded environment. In the process of data communication from source to destination the intermediate nodes plays important role. We know that MANET is most demanded and useful because of its decentralized and wireless infrastructre.Due to this nature it also faces so many security issues such as black hole attack, Denial of Service, Grey hole attck,Sink Hole Attack, Intrusion detection system. In the following discussion we have described DS architectures and different intrusion detection mechanisms.

INTRODUCTION

In the standard mobile network it consists a fixed network of servers and clients. In the wired mobile network, servers have unlimited power and communicate with mobile hosts over a wireless connection. The Mobile clients establishes the communication through a server. Here the issues in this type of network are client power consumption, efficient connectivity of the network, and reach ability of mobile clients from a server. The MANET is group of mobile servers and clients. All nodes are wireless, mobile and battery powered [1]. The networks have dynamic topologies for its routing. The nodes can form a specific route to transmit the data based on the available node frequency radius[2]. All nodes can freely communicate with remaining other node. In addition to the issues associated with a mobile network, the power consumption and mobility of the server(s) must also be considered in a MANET. Originally called Mobile Packet Radio, Mobile Ad-hoc Network (MANET) technology has been an important military research area [4]. This technology has practical use whenever a temporary network with no fixed infrastructure is needed. Other uses include rescue operations and sensor networks [3]. The support of these military and civilian uses often requires the presence of a database to store and transmit critical mission information such as inventories and tactical information. There is one other crucial characteristic of a MANET. Traditional mobile networks involve the server in all data communication.

CHALLENGES IN MANET

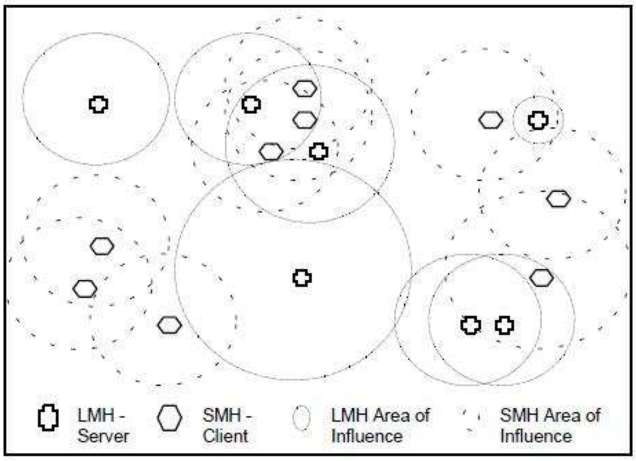
MANETS are more vulnerable to attacks than wired networks due to the following reasons i) open medium, ii)dynamically changing network topology, iii) cooperative algorithms, iv) lack of centralized monitoring. Security is a process that is as secure as its weakest link. So, in order to make MANETs secure, all its weak points are to be identified and solutions to make all those weak points safe, are to be considered. Node mobility on MANET cannot be restricted. As results, many IDS solutions have been proposed for wired network, which they are defined on strategic points such as switches, gateways, and routers, can not be implemented on the MANET. Thus, the wired network IDS characteristics must be modified prior to be implemented in the MANET.

MANET ARCHITECTURE

The nodes in a MANET can be classified by their capabilities. A Client or *Small Mobile Host (SMH)* is a node with reduced processing, storage, communication, and power resources. A Server or *Large Mobile Host (LMH)* is a node having a larger share of resources [1]. Servers, due to their larger capacity contain the complete DBMS and bear primary responsibility for data broadcast and satisfying client queries. Clients typically have sufficient resources to cache portions of the database as well as storing some DBMS query and processing modules [1].

MANET characteristics include a preference for reactive (on-demand) routing, unpredictable and frequent topology changes and distributed control [7]. The primary MANET limitations remain limited bandwidth and battery power [7].Nodes may not remain connected to the network throughout their life. To be connected to the network, a node must be within the area of influence of at least one other node on the network and have sufficient power to function.

In the following Figure 1, a few nodes of a MANET are shown graphically. It is important to note that each node has an area of influence. This is the area over which its transmissions can be heard. A LMH will initially have a larger area of influence as it generally has a more powerful battery. As the power level decreases, the area of influence of any node will shrink. This is due to the fact that the power available to broadcast is reduced.



It is clear from the description and Figure 1 that a node may not be reachable by another node (LMH or SMH). In other words, nodes may become disconnected from the entire network. When moving back in range of other nodes, they will become reconnected. Conversely, a node may be reachable by several LMHs or SMHs. The potentially rapid and regular reconfiguration of the network topology is routine with the MANET.

ALGORITHMS

Two algorithms to handle data push and data pull within the MANET were proposed in [1]. i) Adaptive broadcast scheduling algorithm and ii) Utilizing the popularity factor (PF) Algorithm. The first is the adaptive broadcast scheduling algorithm. Within this algorithm there are two potential ways to construct a broadcast. New items may be either added to the algorithm or may replace less important data items [1].

A global network where all servers in a region know the location and power of all other servers in the region and full replication of the database is assumed. Periodically, each server broadcasts its location and power level. This begins the broadcast cycle [1]. This is a soft real-time system. There are deadlines for data delivery. The deadlines were used to determine which data request to service although no penalty for missing a deadline was mentioned. There is a leader protocol that selects the server in a region with the greatest remaining power. The leader coordinates the broadcast responsibilities of other servers in its area of influence [1]. The lead server determines which portion of a broadcast each

This initial algorithm has a potentially large communication overhead, servers with no clients still broadcast, and less popular items may starve or be broadcast too late [1].

The second algorithm utilizes a popularity factor (PF), as suggested by Datta et. al. [7]. The PF is a measure of the importance of a data item. The PF increases each time a request is made for a data item [1]. The amount of time since the request was made also affects the PF. If it has been too long, the need to broadcast the item may be gone. This factor is called the Resident Latency (RL) and is system and scenario specific [1]. The PF decreases whenever a request exceeds the RL value [1]. The PF is used to assist in the building of relevant broadcasts and includes RL in order to make allowances for the movement of nodes. When the PF of broadcast items is high, the probability of a broadcast that serves maximum needs increases. If a server has not received any requests for a certain number of broadcasts, it will sleep rather than broadcast to an empty audience [1]. Finally, to localize data delivery, the lead server assigns each server the amount of data to broadcast but not the items to broadcast [9]. To deal with insufficient power levels, the servers rebroadcast the previous index and broadcast if they have insufficient power to build a new broadcast [1].

Attacks in MANET:

Passive attack: Malicious nodes cannot find the sender, receiver and other intermediate node just by eavesdropping on path discovery messages.

Active attack: Any modi_cation of the path discovery messages will be detected by receiver because of signatures ppended, which preserves integrity of message.

Denial of Service Attack: The protocol is incapable of resisting DOS attack involing flooding the network with meaningless path discovery messages.

It is because verification of these messages involves complex computations which is resource consuming. Also it consumes network bandwidth. In fact DOS attack is very difficult to resist in any protocol.

NTRUSION DETECTION IN MANETs

Intrusion Detection systems (IDS) serves as second line of defense, after first line of defense by prevention techniques. The two major analytical techniques in intrusion detection are Misuse detection: It uses signature of known attacks, to identify those attacks

Anomaly detection: It uses established normal profiles only to identify any unreasonable deviation from them.

Architecture of an IDS agent

Figure 2 shows the architecture of an IDS agent that can be deployed on each mobile node. The various components are: Data Collection Module: It collects various security related data from various audit data sources and preprocess them to the input format of detection engines.

Detection Engine: It determines whether a particular state of system is anomalous, based on predetermined normal profile of network created during training process.

Local Aggregation and Correlation Engine (LACE): It aggregates and correlates various detection results and transfer them to GACE.

Global Aggregation and Correlation Engine (GACE): Its function to aggregate detection results from a number of nodes and globally make decision about any malicious event.

This subsection will describe how Routing anomalies can be detected in MANETs. One important assumption of intrusion detection is that normal and intrusive behaviors are distinguishable.

The following are the challenges in routing anomaly detection Due to arbitrary mobility, it is very difficult to establish a mathematical model to characterize routing disruption attack. Difficulty in distinguishing Routing control packets generated by attacker, and that by mobility induced error.

In this sub-section, a Markov Chain Based Anomaly detection scheme is briey described. The following steps are required

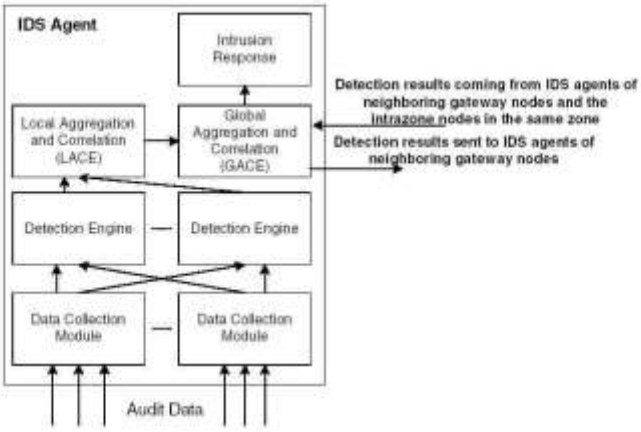

IDS Agent
Intrusion Response
Local Aggregation and Correlation (LACE)
Global Aggregation and Correlation (GACE)
Detection Engine
Detection Engine
Data Collection Module
Data Collection Module
Audit Data
Detection results coming from IDS agents of neighboring gateway nodes and the intrazone nodes in the same zone
Detection results sent to IDS agents of neighboring gateway nodes

Figure 2: IDS Agent.

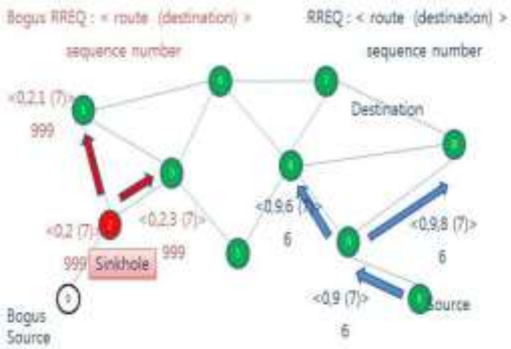
Feature Selection
Features are the attributes of data that needs to be considered. Features associated with routing caches of mobile nodes are determined in order to characterize their normal changes. Two main features are used.

PCR: % Change in number of routing entries in certain time periods.

PCH: % Changes in sum of hops of all routing entries in a certain time periods

Sinkhole attack
The Sinkhole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets [11]. Second, the attacker consumes the intercepted packets without any forwarding.

Sinkhole attack, a sinkhole node tries to attract the data to itself from all neighboring nodes. It generates fake routing information that let the nodes in local network know itself on the way to specific nodes. Through this procedure, sinkhole node attempts to draw all network traffic to itself. Thereafter it alters the data packet or drops the packet silently [11]. Sinkhole attack increases network overhead, decreases network's life time by boosting energy consumption, finally destroy the network. It observes the source node's sequence number carefully, and generates bogus RREQ with selected source, destination and higher sequence number than observed source sequence number. It adds itself on the source route and broadcasts the bogus RREQ.



Intermediate nodes on route learn that node 2 is on one hop distance to node 0 and to send packet to node 0, the data packet may go through the node 2. Sinkhole node 2 can easily repeat this procedure, draw all local network traffic to itself. Thereafter node 2 can do malicious acts including dropping, modifying the traffic.

Sinkhole Indicators

Sinkhole Indicators are network features of occurrence of sinkhole attack on DSR protocol. Tseng et al proposed two sinkhole indicators, sequence number discontinuity, route add ratio.

Sequence number discontinuity

'Sequence number discontinuity (SeqN_D)' is a difference between source sequence number of current and last received RREQ. When a source node initiates route discovery, it publish sequence number, and increase its sequence number by 1. Because sinkhole node advertises fake route information by generating high sequence number, sequence number difference between normal and sinkhole node can be an clue of sinkhole's existence.

Route add ratio

Because of sinkhole node's advertising, nodes affected by fake route information include the sinkhole node in almost all of its route. So the proportion of route including sinkhole node to entire route in route cache become pretty high. This is what is called 'route add ratio (Ra_r)'. Through observing Ra_r it could be checked whether sinkhole node exist or not.

BLACK HOLE ATTACK

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks [25]. An example is shown as Figure 1, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical influence is that the PDR diminished severely.

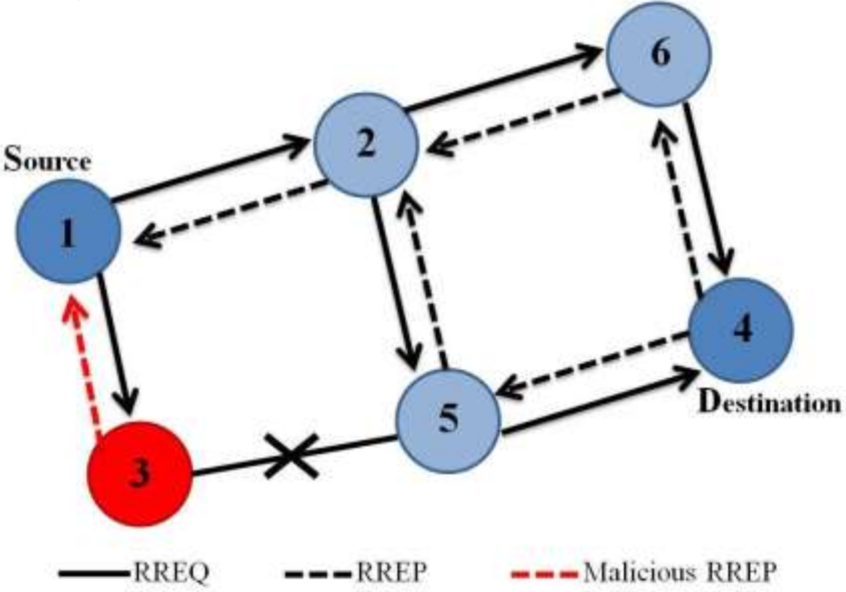


Figure 1

The single black hole problem. Figure 1 is an example of single black hole attack in the mobile ad hoc networks [25]. Node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. In the mobile ad hoc networks, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem.

CONCLUSION AND FUTURE SCOPE OF RESEARCH

The following conclusions are made based on the study communication and security and Intrusion detection in MANET's. The data communication research issues in MANET databases center around two areas. The first area concerns the limitations of the environment (wireless, limited bandwidth, battery powered). The second area concerns the many ways in which data communication may take place. Data communication is an important topic that needs to be addressed when designing database systems in MANET environments. This topic involves far more than network routing. In addition, existing mobile protocols are insufficient. They are not geared towards the specialized needs of a MANET. The areas of concern within MANET data communication are raised. Future research will need to begin to address these issues. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. Because of the emergence of the concept pervasive computing, there is an increasing need for the network users to get connection with the world anytime at anywhere, which inspires the emergence of the mobile ad hoc network. However, with the convenience that the mobile ad hoc networks have brought to us, there are also increasing security threats for the mobile ad hoc network, which need to gain enough attention

REFERENCES

[1] Gruenwald, L., Javed, M., and Gu, M. Energy- Efficient Data roadcasting in Mobile Ad-Hoc Networks. In Proc. International Database Engineering and Applications Symposium (IDEAS '02), July, 2002.

[2] Section 2.5.3. In Proc. 54th Internet Engineering Task Force July, 2002.

[3] Kahn, J., Katz, R., and Pister, K. Next Century Challenges: Mobile Networking for "Smart Dust". In Proc. 5th International Conf. on Mobile Computing and Networking (MOBICOM '99), pp. 271-276, August, 1999.

[4] Corson, M., Freebergyser, J., and Sastry, A., "Mobile Ad Hoc Networking: Editorial," Mobile Networks and Applications, 4(3): pp. 137-138, 1999.

[5] Aksoy, D. and Franklin, M. Scheduling for Large- Scale On-Demand Data Broadcasting. In Proc. 12th International Conf. on Information Networking pp. 651-659, January, 1998.

[6] Wieselthier, J., Nguyen, G., and Ephremides, A., "Algorithms for Energy-Efficient Multicasting in Static Ad Hoc Wireless Networks," Mobile Networks and Applications, 6(4): pp. 251-263, 2001.

[7] Liu, J., Zhang, Q., Li, B., Zhu, W., and Zhang, J., "A Unified Framework for Resource Discovery and QoS-Aware Provider Selection in Ad Hoc Networks," ACM Mobile Computing and Communications Review, 6(1): pp. 13-21, 2002.

[8] Lee, S., Su, W., and Gerla, M., "Wireless Ad Hoc Multicast Routing with Mobility Prediction," Mobile Networks and Applications, 6(4): pp. 351-360, 2001.

[9] Singh, S., Woo, M., and Raghavendra, C. Power Aware Routing in Mobile Ad Hoc Networks. In Proc. 4th International Conf. on Mobile Computing and Networking (MOBICOM '98), pp. 181-190, October, 1998.

[10] Satria Mandala, Md. Asri Ngadi, A.Hanan AbdullahA Survey on MANET Intrusion Detection., International Journal of Computer Science and Security, Volume (2) : Issue (1)-2005.

[11] J. Parker, A. Patwardhan and A. Joshi, "Cross-layer Analysis for Detecting Wireless Misbehavior", in Proceedings of the IEEE Consumer ommunications and NetworkingConference(CCNC 2006), Las Vegas, Nevada, USA, Jan. 2006

[12] Sonal R. Jathe, ananjay M. Dakhane Assistant Professor, Jawaharlal Darda Institute of Engg.,Yavatmal Associate Professor, Sipnas College Of Engg. Amravati " Indicators for Detecting Sinkhole Attack in MANET".