Security issues and vulnerabilities in Mobile Ad hoc Networks (MANET)-A Survey

P.Visalakshi, [1] S.Anjugam[2]
[1, 2] Asst.Professor (Selection Grade)
Department of Computer Applications
SRM University, Kattankulathur, Chennai.
Tamil Nadu, South India

Abstract
The MANET is a collection of mobile nodes such as laptop, palmtop, cellphones, walkie-talkie etc., form a network. It does not have definite topology. The nodes which comprise MANET will always having moving nature. That is why it could not maintain a permanent topology such as ring, star, bus, and mesh in wired network. In MANET nodes can directly communicate to all other nodes within the radio communication range. If a node could not have direct communication then they can use intermediate nodes to communicate with other nodes. Though each node in MANET will act as host as well as router, the security is a major issue and the chances of having the vulnerabilities are also more. This survey paper includes various issues, prevention techniques and vulnerabilities of MANET nodes during data communication.

Index Terms: Mobile Ad hoc Network (MANET), Authentication, topology.

I Introduction

Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The important characteristics of MANET nodes are:

- Operating without a central coordinator
- Multi-hop radio relaying
- Frequent link breakage due to mobile nodes
- Constraint resources (bandwidth, computing power, battery lifetime)
- Instant deployment
- Communication channel is highly insecure in wireless communication. Overhearing and concealing can be done easily.
- The mobile nodes can go out of control, node security is mainly concerned. MANET nodes are not much safer as the nodes could be compromised and act as unreceptive node.
- Node tampering can be caused because of theft and it might disrupt network operations or release critical information.
- Denial of service is caused due to limited power in the mobile nodes. In this case, additional transmissions or expensive computations are created by the attacker.
- The usage of classical solutions based upon the certification authorities and on-line servers, is stopped due to the absence of infrastructure.
- The usage of PKI(Public Key Infrastructure) has become highly infeasible due to the computational powers of the nodes.
- Routing protocols are highly sophisticated due to non-fixed topology. It is quite challenging to secure such protocols in the presence of hostile nodes.

Figure 1. Nodes in the MANET

The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antenna. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area.

II Related Work

S.Madhaviet al [13] have examined the vulnerabilities of wireless networks and included intrusion detection in the security architecture for mobile computing environment. They have propose an mIDS (Mobile Intrusion Detection System) suitable for multi-hop ad-hoc wireless networks, which detects nodes misbehavior, anomalies in packet forwarding, such as intermediate nodes dropping or delaying packets. mIDS does rely on overhearing packet transmissions of neighboring nodes.

Vladimir Berman et al have proposed directional antennas and intelligent multipath routing toenhance end-to-end data confidentiality and data availability with respect to outsider attacks. The goal is to impede rogue attempts to gain unauthorized access to classified information or disrupt the information flow. The interplay between the physical, link, and network layers is considered.

HaiyunLuo et al havedesigned a self-securing approach, in which multiple nodes collaboratively provide authentication services for other nodes in the network. They have first formalized a localized trust model that lays the foundation for the design. They have further proposed refined localized certification services based on their previous work, and develop a new scalable share update to resist more powerful adversaries.

Reijo M. Savola et al [22] have proposed integrated security measurement architecture and framework for a dynamic self-organizing monitoring system based on mobile ad hoc networks (MANETs), structured according to currently known security challenges. The aim is to predict, as well as to monitor, the security performance, concentrating on the principal effects contributing to it.

Iii Security Concepts

The main security criteria are

- **Availability**
- **Integrity**
- **Confidentiality**
- **Authenticity**
- **Non repudiation**
- **Authorization**
- **Anonymity**

AVAILABILITY → A node should maintain its ability in order to provide all the designed services.
INTEGRITY → It guarantees the identity of messages sent when they are sent. Integrity may be altered by activity of malicious node or accidental altering by node
CONFIDENTIALITY → Information access is possible only for authorized node.(ie) Confidentiality will be maintained in accessing messages by the way of providing privileges to authorized nodes
AUTHENTICITY → Providing assurance for the nodes which are participating in the communication and not the impersonators.
NON-REPUDIATION → It ensures that the sender cannot deny or repudiate that he has not send the message and receiver cannot deny or repudiate that he has not receive the message.
AUTHORIZATION → Authorization is a process in which an entity is issued a credential which privileges and permissions it has and cannot falsified y the certificate authority. It is also used to assign different access rights to different level of users.
ANONYMITY → It provides the all possible information that can be used to identify the owner or the current user of the node should be kept private and not be distributed by the node itself.

IV Behaviour of Malicious Node

A node in MANET which underwent some attack exhibits an anomalous behavior called malicious behavior. An ad hoc is said to be a malicious node if and only if it undergoes with one or more of following characteristics.

- Packet drop
- Battery drained
- Buffer over Flow
- Bandwidth consumption
- Stale packets
- Delay of packets
- Link break
- Message tampering
- Fake or wrong routing
- Stealing information
- Session capturing

Node Information

Each node in MANET has unique id. Every node can communicate directly with other node within communication range. The maximum range of communication distance of a node is used to identify neighbor nodes which are very close to a particular node.

- Each node maintains Traffic Flow Table (TFT)
- Traffic Information Table (TIT)

V VULNERABILITIES IN MANET

(1) Unsecured boundaries
(2) Compromised nodal threat
(3) Non availability of centralized management facility
(4) Limited power supply
(5) Scalability

Unsecured boundaries
Possible MANET attacks

VI Security Monitoring System In Manet

An essential part in the MANETs is security monitoring: the security levels are monitored by each node in the ad hoc networks and decisions are made with respect to the measurements. Security monitoring or measurement of the security should be carried out by a node which is responsible for its own security, so that the desired security level is maintained in a self-organized mobile ad hoc network.

We cannot restrict the nodes movement and same physical area cannot be monitored by a node for an extended period of time. In order to diagnose other nodes accurately, a single node may not be able to obtain a large enough sample size of data.

Some of the drawbacks in the existing malicious node detection Systems for MANETs are listed below:

- ***Lack of Central Points:*** Entry points such as routers, gateways, etc are not present in MANETs. All the network traffic which passes through the entry points is monitored by them. The sending and receiving of the packets with other packets can be viewed by a node in the mobile ad hoc network only if it's within the radio range. The intrusion detection and response systems in MANETs need to be distributed and cooperative since the wireless ad hoc networks are distributed and cooperative.

- **Mobility**: The network topology can be changed easily, as the nodes can independently leave and join the network. The traditional techniques of IDS can be defective due to the highly dynamic operation of a MANET.

- ***Limited Resources:*** Battery power with different capacities is used by the mobile nodes.

- ***Lack of a Clear Line of Defense and Secure Communication****:* MANETs are attacked from all the directions since they do not have a clear line of defense. Access controlled mechanisms cannot be placed on MANETs as there are no central points.

- ***Passive eavesdropping and active interference*** which require radio contact can be exploited without the need of physical access to the network contrasting to the wired networks.

- ***Cooperativeness:***MANETs have highly cooperative routing protocolswhich lead to new attacks. For instance, the significant parts of the network are affected when a node pose as a neighbor and contribute in the decision mechanisms.

- ***Diverse MANET*** environments don't support a two tier IDS framework.
- For a battery conscious and reduced communication environment, computing the anomaly model for traffic payload or other rich feature sets should be avoided as they consume much time and it is a processor-heavy task.

- Characterization of normal behavior estimates the anomaly detection which is quite difficult in ad hoc networks.

Vii Security Schemes In Mobile Ad Hoc Network

6.1. Intrusion Detection Systems (IDS)

Method for detection and isolation of malicious node

1) Traffic Flow monitoring Phase
2) Attack Isolation Phase

Traffic Flow monitoring

In this phase, traffic flow features of neighbor nodes are collected and traffic flow table is created with the following parameters

- Packet type or packet size (CBR,VBR)
- Flow direction (send, forward, receive, drop)
- Sampling Periods (No. of packets transacted within a stipulated time)
- Statistical measures (Standard deviation of no of packets transacted)

By using TFT, the neighbor node's behavior is monitored. If a node has one or more number of malicious node's character, it will be reflected in Traffic Flow table. It leads to deviation in the traffic pattern and hence profile will also be changed.

Attack Isolation

Trust

In isolating the node, the trust is considered as a major issue. It is a belief in attributes such as reliability and competence of trusted agent. Each node maintains Trust information table of its neighboring node in the network.

6.2 Cluster based IDS

I n this cluster based IDS a MANET nodes can be arranged into a number of clusters in such a way that every node is a member of at least one cluster and there will be only one node per cluster that will take care of the monitoring the issues in a certain period of time. The cluster nodes will be residing within the same radio range with each other**.** The probability of every node in the cluster to be selected as the cluster head should be equal and each node should act as the cluster head for a certain period of time.

6.3 Cross layer detection mechanism

Thevulnerabilities at the multiple layers but keep the attack to each of the vulnerabilities stay below the detection threshold so as to escape from capture by the single-layer misbehavior detector.

Viii Conclusion

Firstly, chapter is an introduction part in which we have briefly classified the basic characteristics of mobile ad hoc nodes.

Secondly, a few research works have been explained and the method they used for IDS also explained well.

Thirdly, we have listed out all the security concepts of nodes in MANET.

Fourthly, malicious node behavior and nodal information and techniques which are adapted to remove malicious nodes from MANET.

Fifthly, vulnerabilities and possible attacks in the MANET.

Sixthly, securing monitoring system to maintain security by using monitoring system.

Seventhly, various security schemes such as IDS, Cluster based IDS, Cross layer detection etc.,

This survey paper can be an exhaustively used and it may be used for further research areas such as routing algorithms, QOS etc.,

REFERENCES

1. ReijoSavola and IlkkaUusitalo, "Towards Node-Level Security Management in Self-Organizing Mobile Ad Hoc Networks", Proceedings of the Advanced International Conference on Telecommunications International Conference on Internet and Web Applications and Services (AICT/ICIW 2006) IEEE 2006.

2. Gabriela F. Cretu, Janak J. Parekh, Ke Wang and Salvatore J. Stolfo, "Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks", 3rd IEEE Conference on Consumer Communications and Networking, 2006.

3. S.Madhavi and Tai Hoon Kim, "An Intrusion Detection System in Mobile Adhoc Networks", International Journal of Security and Its Applications Vol. 2, No.3, July, 2008.

4. Angelo Rossi and Samuel Pierre, "Collusion-resistant reputation-based intrusion detection system for MANETs", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11, November 2009.

5. Animesh Kr Trivedi, Rishi Kapoor, RajanArora, SudipSanya and SugataSanya, "RISM - Reputation Based Intrusion Detection System for Mobile Adhoc Networks", 3rd International Conference on Computers and Devices for Communication – 2006.

6. Bo Sun, Kui Wu and Udo W. Pooch, "Zone-Based Intrusion Detection for Mobile Ad Hoc Networks", http://webhome.cs.uvic.ca/~wkui/research/IDS.pdf

7. Vladimir Berman and Biswanath Mukherjee "Data Security in MANETs using Multipath Routing and Directional Transmission" in Proc. IEEE ICC 2006, 2006.

8. N.Jaisankar ,R.Saravanan and K.Duraiswamy "An agent based security framework for protecting routing layer operations in MANET",2009 First International Conference on Networks & Communications. Year 2009.

9. S.Dhanalakshmi and Dr.M.Rajaram "A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET"IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008.

10. Reijo M. Savola and HabtamuAbie "On-Line and Off-Line Security Measurement Framework for Mobile Ad Hoc Networks" JOURNAL OF NETWORKS, VOL. 4, NO. 7, SEPTEMBER 2009.