



International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Issues in MANET

Manjeet Singh, Apurva Sharma

Computer Science Department,
Shaheed Udham Singh College of Engineering and Technology,
Tangori, Punjab, India

Abstract - Mobile ad-hoc network (MANET) is a self-constructing mobile network in which each device is free to move independently in any direction & change its links to other devices frequently. So the Mobile ad-hoc networks might be more prone to security issues as compared to wired networks. There might number of passive and active attacks affecting the network. In this paper we discuss the various security issues or vulnerabilities, threats and different measures to handle them.

Index Terms – Mobile Ad hoc Networks, CBDS, BFTR, Intrusion detection.

I. INTRODUCTION

With the emerge of mobile technology, the wireless communication is becoming more popular than ever before. This is due to technological advances in laptops & wireless data communication devices such as wireless modems & wireless LANs. It has lead to lower prices & higher the data rates which has resulted in rapid growth of mobile computing.

There are two main approaches for enabling wireless communication between hosts. First is enabling existing cellular infrastructure to carry data as well as voice which includes the major problem of handoffs. Another main problem is that they are only limited to places where exists such a cellular data network.

Second approach is ad-hoc networking between users wanting to communicate with each other. Packets are delivered from source to destination. The ad-hoc network is limited in range as compared to cellular network but it has several advantages over cellular network.

Mobile ad-hoc network (MANET) is a self-constructing mobile network in which each device is free to move independently in any direction & change its links to other devices frequently. Ad-hoc networks do not rely on any pre-established infrastructure, so therefore they can be even deployed on places with no infrastructure. So it's useful in disaster recovery situations. Ad-hoc networks are helpful in conferences where people participating in conference can form a temporary network without engaging in services of any pre-existing network [2]. So the Mobile ad-hoc networks might be more prone to security issues as compared to wired networks.

Security is an important issue in the integrated MANET-Internet environment because in this environment the attacks on Internet connectivity and also on the ad hoc routing protocols are of main concern.

II. SECURITY ISSUES IN MANET

A vulnerability is a weakness in security system [3]. A particular system may be vulnerable to unauthorized data access because the system does not verify a user's identity before allowing data ease to access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

A. Lack of centralized management

MANET doesn't have a centralized monitor server. The absence of such management makes the detection of attacks difficult as it is not easy to monitor the traffic in a large scale ad-hoc network. Lack of centralized management will easily break the trust management for nodes.

B. Resource availability

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security architectures which provide safety to the user. Collaborative ad-hoc environments also allow us to develop such security mechanism.

C. Scalability

Due to mobile nature of nodes, scale of ad-hoc network keeps on changing frequently. So scalability is a major issue concerning security and authentication. Security mechanism should be capable of handling various range and size of network.

D. Cooperativeness

Routing algorithm for MANETs usually assume that nodes are cooperative and non-malicious. As a result a malicious attacker can easily attack, disroute the mechanism and disrupt network operation by breaking the protocol specifications.

E. Dynamic configuration

Dynamic configuration and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as faulty. This dynamic behavior could be better protected with widely distributed and adaptive security mechanisms in terms of area.

F. Limited Power Supply

The nodes in mobile ad-hoc network need to consider restricted power supply.. A node in mobile ad-hoc network may behave in a selfish manner when it is find that there is only limited power supply, it make use of it for itself.

There are different types of attacker present in MANETs, which tries to decrease the performance of network by consuming more battery.

G. No predefined boundary

In the mobile ad-hoc networks the nodes work in the wireless environment where they are free to join and leave the wireless network. So the malicious nodes might come and communicate with the nodes in their radio range.

III. ATTACKS CLASSIFICATION

Attacks in MANET could be classified under certain categories according to the severity of the attack.

A. The behavior of the attacks (passive vs. active)

Passive attacks are launched to steal in the targeted networks. In Passive attack, the attacker listen to network in order to get information, what is going in the network [3]. In active attack the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network. Active attacks can be an internal or an external attack. Passive attacks include information disclosure and eavesdropping whereas active attacks include Denial of service and Data modification by Trojans & viruses.[1]

B. The source of the attacks (external vs. internal)

External attacks are attacks launched by users who are not an authorized to participate in the network manipulation and operations. These attacks usually aim to congest the network, denying access to specific network function or to disrupt the whole network operations. Bogus packets injection, denial of service, and impersonation are some of the attacks that are usually initiated by the external source.

Internal attacks are initiated by the authorized nodes in the networks, and might come from both compromised and misbehaving nodes. Internal nodes are identified as compromised nodes if the external attackers hijacked the authorized internal nodes and are then using them to launch attacks against the ad hoc networks[5].

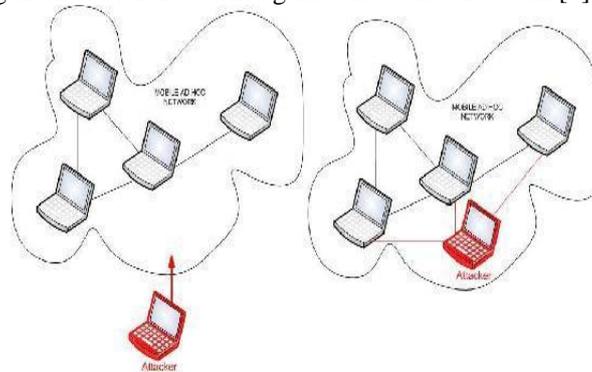


Fig 1.1: Internal and External Attack

C. The processing capability of the attackers (mobile vs. wired)

Mobile attackers are attackers that have the same capabilities as the other nodes in the ad hoc networks. Since they have the same resources limitations, their capabilities to harm the networks operations are also limited. For instance, with the limited transmitting capabilities and battery powers, mobile attackers could only jam the wireless links within its vicinity. On the other hand, wired attackers are attackers that are capable of gaining access to the external resources such as the Since they have more resources, they could launch more severe attacks in the networks, such as jamming the whole networks or breaking expensive cryptography algorithms.

D. The number of the attackers (single vs. multiple).

Attackers might choose to launch attacks against the ad hoc networks independently or by colluding with the other attackers. One man action or single attackers usually generate a moderate traffic load as long as they are not capable to reach any wired facilities. Since they also have similar abilities to the other nodes in the networks, their limited resources become the weak points to them [2].

However, if several attackers are colluding to launch attacks, defending the ad hoc networks against them will be much harder. Colluding attackers could easily shut down any single node in the network and be capable to degrading the effectiveness of network's distributed operations including the security mechanisms.

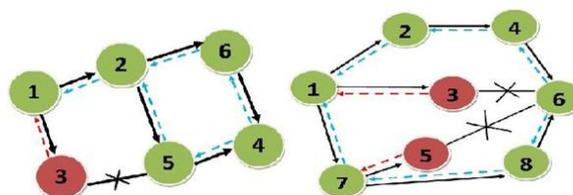


Fig 1.2: shows Single and multiple attacks

MAJOR APPROACHES TO DETECT THE MALICIOUS NODES IN THE NETWORK.

- A. **2 ACK** – In this scheme 2 hop acknowledgement packets are sent in opposite directions of routing path to indicate that data packets have been successfully received. Scheme belongs to class of proactive schemes & hence produces additional routing overhead to malicious nodes.
- B. **BFTR (Best Fault Tolerant Routing)** – BFTR uses end to end acknowledgement to monitor quality of routing path to be chosen by destination node. Main drawback of BFTR is that malicious nodes may still exist in newly chosen route.
- C. **CBDS** – This technique works on DSR mechanism to detect the malicious nodes in the network. It combines the advantages of both proactive and reactive detection schemes to detect malicious nodes.
- D. **Intrusion detection** - Y Zhang & W Lee proposed intrusion the approach in which they proposed distributed and cooperative framework to detect the attack. Each node in the MANET participates in the process & detects the sign of intrusion locally and independently and also sends the information to other nodes in the network[4].
- E. **Cluster based intrusion detection** - In this approach the whole network is organized as a set of clusters such that each node is member of one or more clusters. Only one node in the cluster will monitor intrusion detection. Nodes are in the same radio range[4].
- F. **Defending wormhole attack using leash** - Wormhole attacks are defended using packet leashes. It is the maximum information added to the packet to restrict its maximum allowable transmission distance. Receiver examines its time & distance[4].

IV. CONCLUSION

In this paper we try to inspect the various security issues of the Mobile Ad hoc networks which might be the main reason to the disturbance of its operation. As in Mobile Ad hoc networks nodes are free to move, so the threat risk factor is increases. So the security in these networks needs to be much higher as compared to the wired networks.

Firstly in this paper we introduced the various security issues related to the MANETs. Then we classified the various types of attacks under certain categories. Then finally we introduced the various approaches to detect the malicious nodes in the MANETs.

During the survey we found some points that further needed to be explored such as BFTR technique is not much satisfactory as the malicious nodes may still exist in the newly chosen route. CBDS technique is very costly. Intrusion detection technique also needed to be improved further.

REFERENCES

- [1] Chang Li Shi, Lan Yang Hao, Sheng Zhu Qing (College of Computer Science Chongqing University Chongqing, China). *Research on MANET Security Architecture design*.
- [2] Joshi Nikhil R, D.N Chandrappa, "MANET Security Based On Hybrid Routing Protocol and Unique Cryptographic Identity"
- [3] Khala Babak Hossein, Bagheri Hamidreza, Katz Marcos, Salehi Mohammad Javad, mohammadpour Mohammad Noor, and AsghariPari Seyed Mohammad. *A Self-Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks*.
- [4] Mishra Durgesh Kumar (Acropolis Institute of Technology and Research, Indore, India). Chandel Mahakal Singh (Arjun Institute of Advaced Studies and Research Centre, Indore, India), Sheikh Rashid. *Security Issues in MANET: A Review*.
- [5] Villalba Luis Javier García , Matesanz Julián García , Orozco Ana Lucila Sandoval 1,3 and Díaz José Duván Márquez, "Auto-Configuration Protocols in Mobile Ad Hoc Networks", *The 11th International Workshop on Knowledge Management and Acquisition for Smart Systems and Services (PKAW 2010)*