Mobile Ad Hoc Networks (MANET): Security Threats, Vulnerabilities and Routing Mechanism

Dr. Pradosh Chandra Patnaik

Associate Professor and Head, Dept. of CSE,
Aurora's Scientific, Technological and Research Academy, Hyderabad.

***Abstract*: A mobile ad-hoc network is a self-organizing, infrastructure-free network in which nodes communicate over wireless networks. In comparison to infrastructure networks, security becomes a critical concern because to its dynamic topology. Due to the lack of a trusted centralised authority, MANETs are more vulnerable to numerous sorts of security threats. For these networks, several routing protocols have been proposed to construct an end-to-end link for communication between nodes. These protocols are vulnerable to attacks from malicious nodes, and it is always necessary to identify and mitigate attacks before the network collapses. The focus of this study is on current routing attacks, ad-hoc network security challenges, and strategies to minimise attacks against routing protocols based on network node cooperation. Because there is no centralised authority to control the individual nodes functioning in the network, security in the mobile ADHOC network is a significant concern. The attacks might occur from both inside and outside the network. We're attempting to categorise the current attacks into two groups: DATA traffic attacks and CONTROL traffic attacks. We'll also talk about the current mitigation options for these types of assaults.**

***Keywords*: Mobile Ad Hoc Networks (MANETs), Security, Threats, Solutions, Routing Protocols**

Introduction

A mobile ad hoc network (MANET) is a network of mobile nodes that self-configures. It is devoid of any permanent infrastructure, like as access points or base stations. It has no centralised administration and is connected to the rest of the world via wireless networks and cables. Where wireless connection is not available or a wired backbone is not viable, a wireless ad hoc network can be set up. All ad hoc network services are configured and created on the fly. As a result, security in ad hoc networks becomes an inherent weakness due to a lack of infrastructural support and vulnerability to wireless connection attacks. Nodes in a nomadic environment with a shared radio link can readily participate in the creation of ad hoc infrastructure. However, secure communication between nodes necessitates the use of a secure communication channel. Link the node should be capable of identifying itself before starting secure communication. **"**In present-day society mobile devices (e.g. laptops and cell phones) are increasingly being integrated to daily activities. This makes them an integral, inseparable and critical part of life in contemporary society. Literally, mobile devices are found virtually anywhere there is human life. For this reason, ever more, these mobile devices are required to interconnect to pass messages along between individuals and groups, thus enabling effective communication"[1].

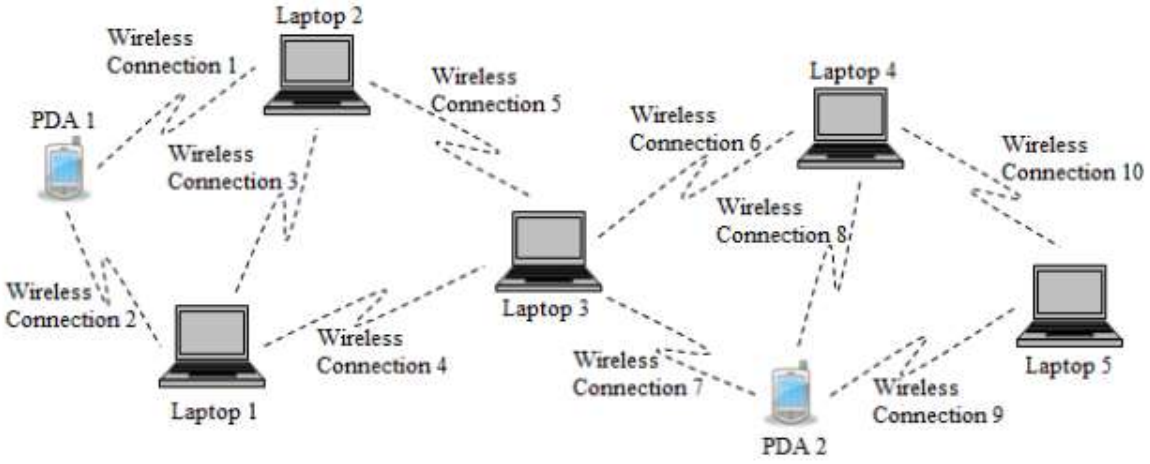

Fig. 1: MANET Architecture

The establishment of survivable, efficient, and dynamic communication in emergency and rescue operations, disasters, war battlefields, personal area networks, and the commercial sector are all major applications of MANETs. These kind of networks can't rely on centralised, wired connectivity.

When compared to wire networks, MANETs are more vulnerable to security attacks due to a lack of trusted centralised authority, simple eavesdropping due to shared wireless medium, unpredictable network architecture, poor bandwidth, and mobile device battery and memory limits. Due to the presence of numerous senders and receivers, security of MANETs is a more difficult issue in group communication.

Earlier Work

A number of studies have been carried out on security challenges and solutions in mobile ad hoc networks MANETs. "Manet's attacks may take place in two major ways. That is, either passively or actively. In passive attack, the data under transmission is not affected. Rather, passive attack pretends to be part of the data, but with the sole motive of collecting important information" [2]. "A passive attack may be seen as planting an evil spy within a group of good guys with intention of stealing information. There is no disruption of routing while passive attack occurs. In an active attack, nonetheless, the transmission of data is interrupted. Compared to the passive attack, an active attack is more severe because the normal transmission of data between nodes is negatively affected"[2]. Either of the types of attacks can emanate internally or externally.

Because MANETs depend on nodes for self-reorganization, their network systems are more vulnerable to attacks than the wired networks. "For this reason, securing MANETs can be a daunting task. But there are security objectives that must be pursued in MANETs to guarantee some safety for the users. Confidentiality should be always considered. Only the authorized devices and users are allowed to access the network to protect privacy and secrecy" [3]. Every node requires the capability to validate the ingenuity of the peer node and user. Valid network users and nodes need validation credentials to access the network. Authentication prevents imitators from accessing the network illegitimately.

"Due to their vulnerability, researchers have developed numerous ways of fighting insecurity in MANETs. For instance, Intrusion Detection is a response scheme for detecting threats beforehand. Intrusion Detection put forth both distributed and cooperative model, designed for sensing and identifying attacks"[4]. Sheikhl et al. [4] observe "that in the Intrusion Detection all nodes in a network are called to action. Once a node identifies a threat independently, it broadcasts a warning to the rest of the nodes. But at times, as a result of power limitation of the nodes, the dissemination of the warning may not be successful. Such incidents require cluster-driven Instruction Detection. Cluster-driven Intrusion Detection is designed in such a way that the network is divided into subgroups (clusters)."

Vulnerabilities of MANET

Vulnerability is a weakness in security system. Wireless ad-hoc networks are more vulnerable than wired networks. Few of the vulnerabilities of MANETs are:

Absence of Centralized Management

"The absence of centralized management makes identifying the attacks over the network is very difficult; it is not easy to observe the traffic in dynamic environments."[5]

Resource Availability

"The availability of resources is a major issue in MANET. In dynamic environments secure communication leads to the elaboration of various security schemes" [5].

Scalability

"A major concern regarding security, due to mobility networking of nodes varies all the time. Security mechanisms need to provide security for large and small networks as well"[5]

Cooperativeness

"Routing algorithms proposed for routing in MANETs assumes all the nodes over the network are cooperative and non-malicious. As a result of this attackers can become a crucial routing agent and disturb entire functionalities of the network."[5]

Dynamic Topology

"High mobility and dynamic topology disturbs the trust relation among the nodes. Sometimes trust may be disturbed because of some compromised nodes. The security mechanisms like adaptive and distributed protects the dynamic behaviour."[5]

Limited Power Supply

"Considering their limited power capability by the MANETs stations, which will be the cause of several threats? A station exhibit selfishness and does not cooperate in packet forwarding" [5].

Bandwidth Constraint

"The links with low capacity are susceptible of interference effects, noise and signal reduction" [5].

No Predefined Boundary

"Physical boundaries are cannot be defined precisely in MANETs. So an attacker can intrude into the network in the medium range of a node, and can exchange information with the node."[5]

Security Threats in MANETs

The need for a central administration is avoided because MANET connections and data packet transfer rely on clusters of nodes or mobile devices that form, in most circumstances, short-lived, hence transitory networks. Because of the lack of centralised administration, mobile node interconnection must be built on complete trust. Furthermore, because of the dynamic nature of MANETs and the resulting quick change of topological information, they are vulnerable to internal attacks.

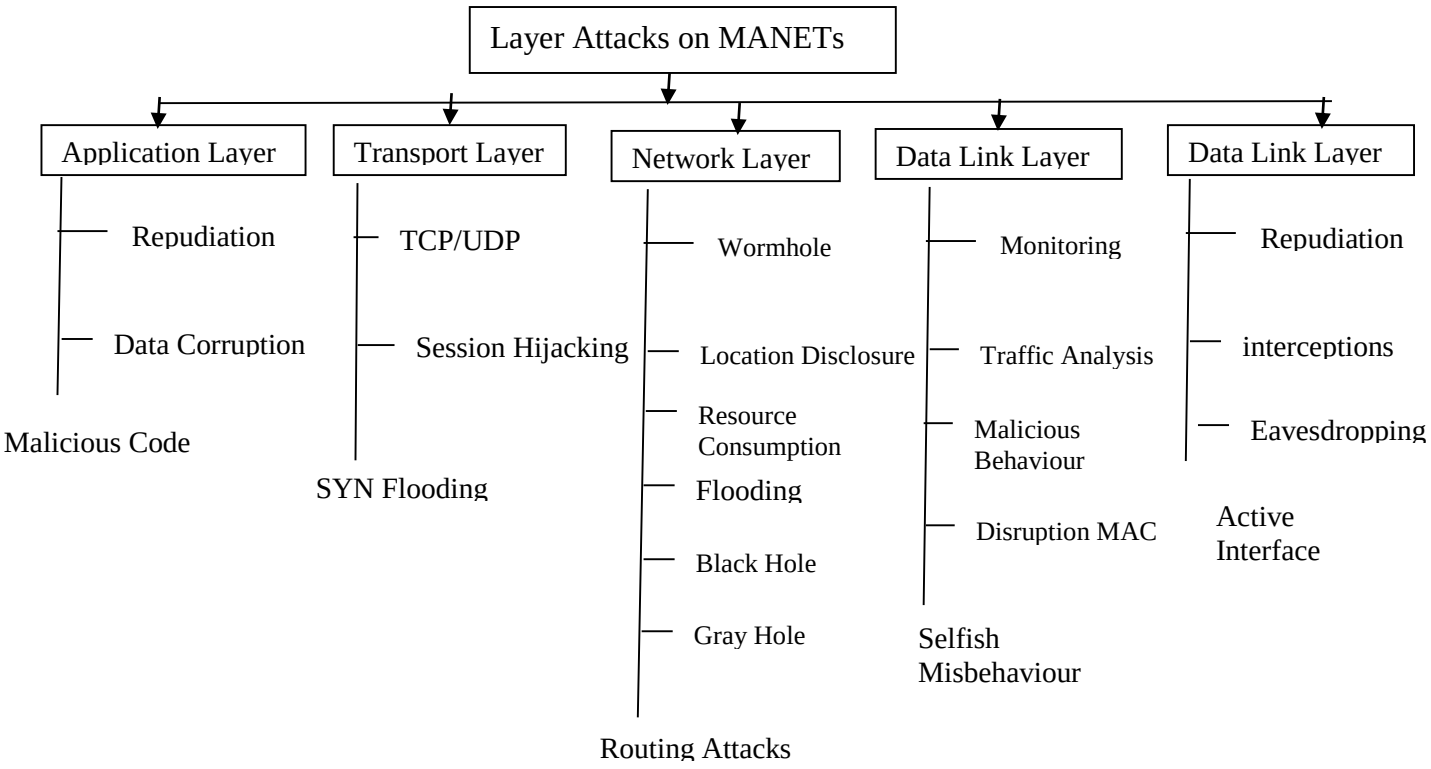

Fig.2: Attacks in Various Layers of MANET

Layers	Attacks	Solutions
Application Layer	Lack of cooperation attacks, Malicious Code attacks(virus, worms, Trojan horses etc.)	Cooperation enforcement mechanism, Firewalls, IDs etc
Transport Layer	Session Hijacking attack, SYN Flooding, TCP ACK storm attack etc.	Authentication and securing end to end or point to point communication, use of public cryptography
Network Layer	Routing Protocol attacks, cache poisoning, table overflow attacks, worm hole, black hole, gray hole	Source authentication and message integrity mechanisms to prevent routing message modification, securing routing protocols
Data Link Layer	Traffic analysis, monitoring disruption MAC(802.11)	No effective mechanism to prevent traffic analysis and monitoring, secure link layer protocol like LLSP
Physical Layer	Jamming, interceptions, Eavesdropping	Using spread spectrum mechanism

Table 1: Security Threats and possible responses in MANETs

Protocols for Routing in MANETs

Routing protocols in MANETs are classified into three types they are:

- ❖ Proactive (or) Table-Driven Routing Protocols
- ❖ Reactive (or) On-Demand Routing Protocols
- ❖ Hybrid Routing Protocols

Proactive Approach

Attempts to thwart an attacker's attempts using a variety of cryptographic techniques: By frequently distributing routing tables throughout the network, this sort of protocol keeps a fresh list of destinations and their paths. The mechanism in pro-active routing protocols differs from that in re-active routing systems. Basically, routes in this family of protocols are dependent on constant traffic control.

Reactive Approach

Attempts to detect and respond to security threats. By frequently distributing routing tables throughout the network, this sort of protocol keeps a fresh list of destinations and their paths. Reactive routing protocols have two key characteristics: first, they never take the initiative to establish routes for the network, and second, they develop routes on demand via a flooding mechanism.

Hybrid Routing Protocols

These protocols combine the qualities of proactive and reactive protocols, in which proximate (maximum two hops) routes are kept up-to-date proactively, while further routes are built up reactively. Both preventive and reactive methods are

rendered ineffective in these conditions. Zone Routing Protocol (ZRP) and Zone based Hierarchical Link State (ZHLS) routing protocols are examples of hybrid protocols.

Conclusion

The rise of mobile ad-hoc networks is a result of users' increased desire to connect with the rest of the world at any time and from any location. Mobile ad-hoc networks' mobility and open media nature exposes them to a variety of security vulnerabilities (such as DOS, intrusion, and so on), underlining the importance of addressing security concerns. When compared to typical wired networks, this study focuses on the importance of security requirements in mobile ad-hoc networks. First, we'll go over some of the basic characteristics of mobile ad-hoc networks, as well as the benefits that these networks have provided. Then, because of the characteristics of mobile ad-hoc networks, such as mobility, changing topology, open media, limited battery power, and so on, we focus on some dangerous vulnerabilities in these networks, emphasising the need to find effective solutions to protect mobile ad-hoc networks from external and internal security threats. Finally, some features of intrusion detection techniques that can be improved in the future are discussed.

References

[1] R. Derveloy, "Security Issues of Ad Hoc Networks", CPSC-5620 SPRING 2012, 2012.
[2] P. Kaur and Sukhman, "An Overview on MANET- Advantages, Characteristics and Security Attacks", International Journal of Computer Applications (0975 – 8887), 2016. Available:https://research.ijcaonline.org/icaet2016/number1/icaet018.pdf.
[3] M. Yadav and N. Uparosiya, "Survey on MANET: Routing Protocols, Advantages, Problems and Security", International Journal of Innovative Computer Science & Engineering, vol. 1, no. 2, pp. 12-17, 2014. Available: http://ijicse.in/wp-content/uploads/2014/12/12-17.pdf.
[4] R. Sheikhl, M. Chandee and D. Mishra, "Security Issues in MANET: A Review", 978-1-4244-7202-4/10/$26.00 ©2010 IEEE, 2018.
[5] Mohamed Elboukhari1, Mostafa Azizi1 and Abdelmalek Azizi, Impact Analysis of Black Hole Attacks on Mobile Ad-hoc Networks Performance, International Journal of Grid Computing & Applications (IJGCA), Vol.6, No.1/2, pp:1-11, June 2015, DOI:10.5121/ijgca.2015.620.