IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

Mobile Ad-Hoc Network -Issues and Challenges

Falguni Sawai
Dr. Ambedkar Institute of Management Studies & Research, Nagpur, Maharashtra, India

Abstract: *Due to its self-upkeep and self-configuration characteristics or behavior, mobile ad hoc networks (MANET) have achieved great success and attention. Routing attacks are used to quickly alter the network topology of MANETs based on wired and wireless networks. Therefore, securing this network without infrastructure is a big problem. The routing protocols for ad-hoc networks can adapt to the topology's dynamic changes well, but they are not built to support defense against malicious attackers. Malicious nodes have the ability to alter, reject, or promote fictitious routes to draw user data to pass through themselves. In this post, we go through a hybrid strategy for reducing MANET assaults that combines anonymity, one-way trapdoor protocol, hash functions, and elliptic curve cryptography.*

Keywords: Asymmetric Authentication, Attacks, Key Exchange, Routing, Security, Wireless Network

I. INTRODUCTION

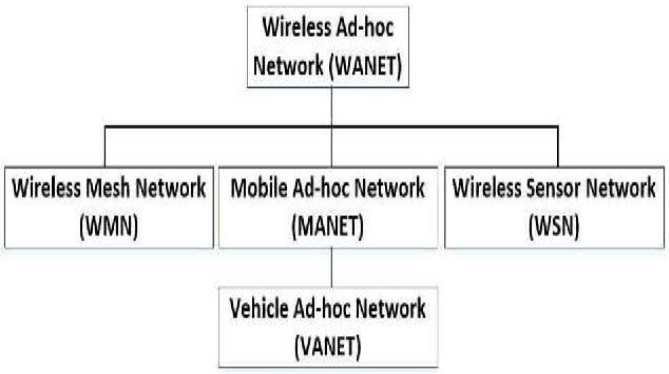
Wireless networks have become increasingly popular in the computing industry, since their emergence in the 1970s. This is particularly true within the past decade which has seen wireless networks being adapted to enable mobility. There are currently two variations of mobile wireless networks. The first is known as infrastructure networks, i.e., those networks with fixed and wired gateways. The bridges for these networks are known as base stations. A mobile unit within these networks connects to, and communicates with, the nearest base station that is within its communication radius. As the mobile travels out of range of one base station and goes into the range of another, a “handoff" occurs from the old base station to the new, and the mobile is able to continue communication seamlessly throughout the network. Typical applications of this type of network include wireless local area networks (WLANs). The second type of mobile wireless network is the infrastructure less mobile network, commonly known as a Mobile ad-hoc network (MANET). Infrastructure less networks have no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network. Example applications of ad-hoc networks are emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrains.

II. CLASSIFICATION

Mobile ad-hoc networks (MANET’s) are of following types:

- Vehicular Ad hoc Networks (VANETs): These are used for communication among Vehicles and between vehicles and roadside equipments.
- Internet based mobile ad hoc networks (iMANET): These are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal Adhoc routing algorithms don't apply directly.
- Intelligent vehicular ad hoc networks (InVANETs): These are a kind of artificial Intelligence that helps vehicles to behave in intelligent manners during vehicle-to- Vehicle collisions, accidents, drunken driving etc.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023



III. CHARACTERISTICS

Mobile ad-hoc networks (MANET's) have following characteristics:

- No infrastructure – flat network
- Radio communication – shared medium
- Every computer or device (node) is a router as well as end host
- Nodes are in general autonomous
- Mobility – dynamic topology
- Limited energy and computing resources.
- Unreliability of wireless links between nodes.
- Lack of incorporation of security features in statically configured wireless Routing-Protocol not meant for ad hoc environments.

IV. ISSUES IN MOBILE AD-HOC NETWORKS

There are several issues within ad hoc networks that make them very complicated to integrate with the existing global internet. The problems are addressed below:

- **Routing:** Routing is one of the most complicated problems to solve as ad hoc networks have a seamless connectivity to other devices in its neighborhood. Because of multi hop routing no default route is available. Every node acts as a router and forwards each other's packets to enable information sharing between mobile nodes.
- **Security**: Clearly a wireless link is much more vulnerable than a wired link. The science of cracking the encryption and Eaves dropping on radio links has gone on since the first encryption of radio links was established. The user can insert spurious information into routing packets and cause routing loops, long time-outs and advertisements of false or old routing table updates. Security has several unsolved issues that are important to solve to make the ad hoc network into a good solution.
- **Quality of Service (QoS):** QoS is a difficult task for the developers, because the topology of an ad hoc network will constantly change. Reserving resources and sustaining a certain quality of service, while the network condition constantly changes, is very challenging.

V. CHALLENGES IN MOBILE AD-HOC NETWORKS:

Host is no longer an end system - can also be an acting intermediate system changing the network topology over time
Potentially frequent network partitions

- Every node can be mobile
- Limited power capacity
- Limited wireless bandwidth
- Presence of varying channel quality
- No centralized entity – distributed

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

- How to support routing?
- How to support channel access?
- How to deal with mobility?
- How to conserve power?
- How to use bandwidth efficiently?

VI. PROBLEMS WITH AD-HOC ROUTING PROTOCOLS

In ad-hoc routing protocols, nodes exchange information with each other about the network topology, because the nodes are also routers. This fact is also an important weakness because a compromised node could give bad information to redirect traffic or simply stop it. Moreover, we can say that routing protocols are very brittle in term of security. This part aims to provide a description of the causes of the problems with ad-hoc routing protocols. Infrastructure of ad-hoc networks Ad-hoc networks have no predetermined fixed infrastructure, that's why the nodes themselves have to deal with the routing of packets. Each node relies on the other neighboring nodes to route packets for them.

6.1 Dynamic topology of ad-hoc networks

The organization of the nodes may change because of the mobility-aspect of ad-hoc networks: they contain nodes that may frequently change their locations. Because of this fact, we talk about the dynamic topology of these networks, which is a main characteristic that causes problems: when several ad-hoc networks mix together, there can be duplications of IP addresses, and resolving it is not so simple. Then, attacks can easily occur by using this duplication of IP address.

6.2 Problems associated with wireless communication

Wireless channels have a poor protection to noise and signal interferences, therefore routing related control messages can be tampered. A malicious intruder can just spy on the line, jam, interrupt or distort the information circulating within this network.

6.3 Implicit trust relationship between neighbors

Actual ad-hoc routing protocols suppose that all participants are honest. Then, this directly allows malicious nodes to operate and try to paralyze the whole network, just by providing wrong information.

6.4 Types of Attacks in MANET

Due to their particular architecture, ad-hoc networks are more easily attacked than wired network. We can distinguish two kinds of attack: the passive attacks and the active attacks. A passive attack does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic. Instead, an active attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or attract packets destined to other nodes. The routing protocols in MANET are quite insecure because attackers can easily obtain information about network topology.

6.5 Attacks Using Modification

One of the simplest ways for a malicious node to disturb the good operation of an ad-hoc network is to announce better routes (to reach other nodes or just a specific one) than the other nodes. This kind of attack is based on the modification of the metric value for a route or by altering control message fields.

6.6 Attacks using impersonation

These attacks are called spoofing since the malicious node hides its real IP address or MAC addresses and uses another one. As current ad-hoc routing protocols like AODV and DSR do not authenticate source IP address, a malicious node can launch many attacks by using spoofing. For example, a hacker can create loops in the network to isolate a node from the remainder of the network. To do this, the hacker just has to take IP address of other node in the network and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

then usethem to announce new route (with smallest metric) to the others nodes. By doing this, he can easily modify the network topology as he wants.

6.7 Security Threats in Network Layer

In MANET, the nodes also function as routers that discover and maintain routes to other nodes in the network. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security in network layer plays an important role in the security of the whole network.

6.8 Network Layer Attacks

A number of attacks in network layer have been identified and studied in security research. An attacker can absorb network traffic, inject themselves into the path between the source and destination and thus control the network traffic flow.

Attacks at different stages are as:

1. Attacks at the routing discovery phase
2. Attacks at the routing maintenance phase.
3. Attacks at data forwarding phase.
4. Attacks on particular routing protocols.

Attacks by Names are as:

1. Wormhole attack.
2. Black hole attack.
3. Byzantine attack.
4. Rushing attack.
5. Resource consumption attack.
6. Location disclosure attack.

Counter Measures

Security is a primary concern in MANET in order to provide protected communication between the communicating parties. It is essential for basic network functions like routing and packet forwarding. Network operation can easily be jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. Hence, a variety of security mechanisms have been developed to counter malicious attacks. There are two mechanisms which are widely used to protect the MANET from the attackers.

Security mechanisms

A variety of security mechanisms have been invented to counter malicious attacks. The conventional approaches such as authentication, access control, encryption, and digital signature provide a first line of defense. As a second line of defense, intrusion detection systems and cooperation enforcement mechanisms implemented in MANET can also help to defend against attacks or enforce cooperation, reducing selfish node behavior.

Preventive mechanism

The conventional authentication and encryption schemes are based on cryptography, which includes asymmetric and symmetric cryptography. Cryptographic primitives such as hash functions (message digests) can be used to enhance data integrity in transmission as well. Threshold cryptography can be used to hide data by dividing it into a number of shares. Digital signatures can be used to achieve data integrity and authentication services as well. It is also necessary to consider the physical safety of mobile devices, since the hosts are normally small devices, which are physically vulnerable. For example, a device could easily be stolen, lost, or damaged. In the battlefield they are at risk of being hijacked. The protection of the sensitive data on a physical device can be enforced by some security modules, such as

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

tokens or a smart card that is accessible through PIN, pass phrases, or biometrics. Although all of these cryptographic primitives combined can prevent most attacks in theory, in reality, due to the design, implementation, or selection of protocols and physical device restrictions, there are still a number of malicious attacks bypassing prevention mechanisms.

Reactive mechanism

An intrusion detection system is a second line of defense. There are widely used to detect misuse and anomalies. A misuse detection system attempts to define improper behavior based on the patterns of well-known attacks, but it lacks the ability to detect any attacks that were not considered during the creation of the patterns; Anomaly detection attempts to define normal or expected behavior statistically. It collects data from legitimate user behavior over a period of time, and then statistical tests are applied to determine anomalous behavior with a high level of confidence. In practice, both approaches can be combined to be more effective against attacks. Some intrusion detection systems for MANET have been proposed in recent research papers.

VII. CONCLUSION AND FUTURE SCOPE

This paper discussed about Mobile Ad-hoc networks, their classification, their characteristics, and the issues and challenges that are posed by Mobile ad-hoc networks. This paper also gave a detailed review of literature about Mobile ad-hoc networks and the issues and challenges posed by them. The future scope of this research paper is to improve the standard of Mobile adhoc networks so as to overcome the issues and challenges posed by them.

REFERENCES

[1] ImrichChlamtac a, Marco Conti b, Jennifer J.-N. Liu c, “Mobile ad hoc networking: Imperatives and Challenges”, ELSEVIER, 2003, 13-64.
[2] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.
[3] M. Weiser, “The Computer for the Twenty-First Century”, Scientific American, September 1991.
[4] Wenjia Li and Anupam Joshi, Security Issues in Mobile Ad Hoc Networks - A Survey.
[5] M.S. Corson, J.P. Maker, and J.H. Cernicione, “Internet-based Mobile Ad Hoc Networking”, IEEE Internet Computing, pages 63– 70, July-August 1999