Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review

Monika
M.Tech Student
Department of CSE
The Technological Institute of Textile & Science
Bhiwani, Haryana

Mukesh Kumar
Assisstant Professor
Department of CSE
The Technological Institute of Textile & Science
Bhiwani, Haryana

Rahul Rishi
Assossiate Professor
Department of CSE
The Technological Institute of Textile & Science
Bhiwani, Haryana

ABSTRACT

Mobile Ad hoc networks (MANETs) are a new paradigm of wireless network, offering unrestricted mobility without any underlying infrastructure such as base station or mobile switching centers. Basically ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network. In a mobile ad hoc network, it is much more vulnerable to attacks than a wired network due to its limited physical security, dynamically changing network topology, energy constrained operations and lack of centralized administration. Since all the nodes in the network collaborate to forward the data, the wireless channel is prone to active and passive attacks by malicious nodes, such as Denial of Service (DoS), eavesdropping, spoofing, etc. The intent of this paper is to investigate the security goal, security challenges and different types of active and passive attacks on MANETs.

General Terms

MANETs

Keywords

MANETs, Security, Mobility, Attack, Vulnerable.

1. INTRODUCTION

With the proliferation of cheaper, small, and more powerful mobile devices, mobile ad hoc networks (MANETs) have become one of the fastest growing areas of research .A Mobile ad hoc network is a system of wireless mobile nodes with routing capabilities, any group of them capable of forming an autonomous network that require no infrastructure and is capable of organizing itself into arbitrary changeable topologies. Such a network may operate in a stand-alone fashion, or may be connected to the larger Internet [1, 2] .The definition, which is given by the Internet Engineering Task Force (IETF)[3] . Unlike traditional mobile wireless networks, Ad hoc networks don't rely on any fixed infrastructure(base stations, access points).This flexibility makes them attractive technology for many applications such as rescue and tactical operations, disaster recovery operations and educational applications where we can setup virtual class or conferences. The following are the advantages of MANETs:-

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.
- These networks work without any pre-existing infrastructure.

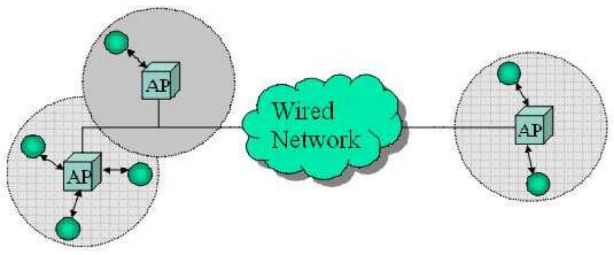


Figure1: Infrastructure based

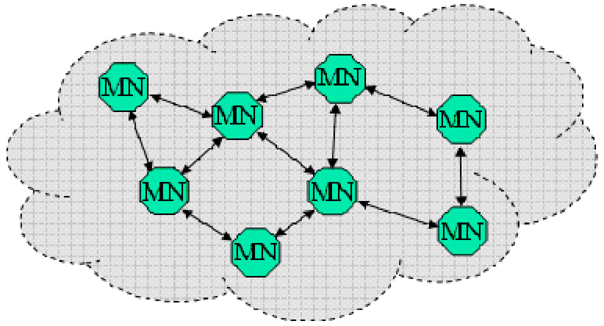


Figure2: Infrastructure less

Security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. In a mobile ad hoc network, it is much more vulnerable to attacks than a wired network due to its limited physical security, volatile network topologies, power-constrained operations, and lack of centralized monitoring and management point.

1.1 APPLICATIONS OF MANETs

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance with the increasing number of widespread application.

TABLE1: Application of MANETs

Application	Possible Scenarios Services
Tactical networks	• Military communication and operation • Automated battlefields
Emergency Services	• Search and rescue operations • Disaster Recovery • Policing and fire fighting • Supporting doctors and nurses in hospitals
Commercial and Civilian environments	• Networks of visitors at airports. • Vehicular services: road or accident guidance, transmission of road and weather conditions, inter-vehicle network.
Sensor Network	• Body Area network (BAN) • Home application: Smart sensors and actuators embedded in consumer electronics.
Education	• Universities and campus settings. • Virtual classrooms. • Adhoc communications during meetings or lectures.
Entertainment	• Multiuser games. • Wireless P2P networking • outdoor Internet access • Theme parks
Location Aware Services	• Automatic call forwarding • advertise location specific services • location-dependent travel guide

2. FEATURES OF MANETs

MANETs are new paradigm of networks, offering unrestricted mobility without any underlying infrastructure such as base station or access point. Basically, ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network. Following are the characteristics of a MANET [4, 5]:

- Autonomous Terminal
- Infrastructure- less and Self Operated
- Distributed operation
- Dynamic network topologies
- Multi-hop routing
- Energy constrained Operation
- Light –weight Terminal
- Ease of deployment
- Speed of deployment

3. SECURITY PROBLEMS IN MANETs

MANETs are much more vulnerable to attack than wired network. This is because of following reasons:

3.1 Absence of Infrastructure

Ad hoc networks operate independently of any infrastructure, which makes inapplicable any classical solutions based on certification authorities and on line servers.

3.2 Limited physical security

Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threat.

3.3 Cooperative Algorithms

The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of network security.

3.4 Restricted power Supply

Due to mobility of nodes in the ad hoc network, nodes will reply on battery as their power supply method, the problem that may be caused by restricted power supply is denial-of-service attacks and selfish manner

.

3.5 Dynamically changing network topology

Nodes are free to move arbitrarily. The network topology may change randomly and have no restriction on their distance from other nodes. As a result of this random movement, the whole topology is changing in an unpredictable manner, which in turn gives rise to both directional as well as unidirectional links between the nodes.

3.6 Lack of Centralized monitoring

Absence of any centralized monitoring makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly and large scale ad hoc network [6]. It is rather common in the ad hoc network that benign failures such as transmission impairments and packet dropping.

4. SECURITY GOALS IN ADHOC NETWORKS

The goals of security mechanism of MANETs are similar to that of other networks. Security is a great issue in network especially in MANETs where security attacks can affect the nodes limited resources and consume them or waste the time before rote chain broke. Security is a vectored term of multi systems, procedures and functions that works together to reach certain level of security attributes[7]. Table 2 below shows those attributes

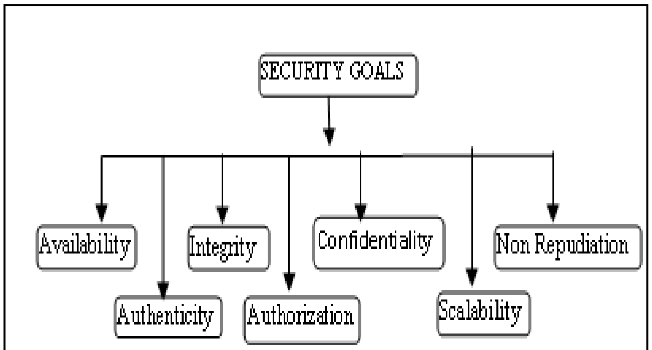


Figure3: Types of Security Goals

4.1 Availability

The main goal of availability is to node will be available to its users when expected, i.e. survivability of network services despite denial of service attack. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network. Again, in higher levels, an adversary could bring down high-level services such as key management service, authentication service [8].

4.2 Confidentiality

The goal of confidentiality is to keeping information secret from unauthorized user or nodes. In other words, ensures payload data and header information is never disclosed to unauthorized nodes. The standard approach for keeping information confidential is to encrypt the data with a secret key that only intended receiver's posses, hence achieving confidentiality.

4.3 Integrity

The goal of integrity is to message being transmitted is never corrupted. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [9].

- Malicious altering: - A message can be removed, replayed or revised by an adversary with malicious goal.
- Accidental altering:- , if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure.

4.4 Authentication

The goal of authentication is too able to identify a user and to able to prevent impersonation. In infrastructure-based wireless network, it is possible to implement a central authority at a point such as base station or access point. But in MANETs, no central administration so it is difficult to authenticate an entity.

4.5 Non repudiation

The main goal of non repudiation is to the origin of a message cannot deny having sent the message. This is useful when for detection and isolation of compromised nodes. When node P receives an erroneous message from Q, non repudiation allows P to access Q using this message and to convince other nodes that Q is compromised.

4.6 Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users.

Table 2:Classification of Security Attacks

Active Attacks	Worm hole, Denial of Service, Byzantine, Location disclosure, Resource Consumption, Interference and Jamming, Malicious code, Session hijacking, Impersonation, Routing attacks.
Passive Attacks	Eavesdropping, monitoring, Snooping, Selfishness, traffic analysis.

Table3: Security Attributes.

Attribute	**Goal**	**Goal matching through remarks**
Authentication	Able to identify the node, Prevent Impersonation	Message Authentication code(MAC), Public key Infrastructure(PKI), Digital signatures, Digital Certificates
Integrity	Prevent illegal deletion, modification, replay of a messages	Digital signature using one-way hash function.
Confidentiality	Keep information sent unreadable to unauthorized nodes.	Data Encryption
Availability	Keep network resources available to users within the same network.	Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS).
Access Control	Prevent unauthorized use of network resources.	Very tide to authentication
Non-repudiation	Prevent message denial from the sender node	Attaching signature to each message
Authorization	Prevent Impersonation.	Credentials, Passwords, Access Control List(ACL), Firewall.

5. ATTACKS ON MANET

Malicious and selfish nodes are the ones that fabricate attacks [10] against physical, data link, network, and application-layer functionality. Current routing protocols are exposed to two types of attacks

5.1Active attacks

Through which the misbehaving node has to bear some energy costs in order to perform some harmful operation, and Nodes that perform **active attacks** with the aim of damaging other nodes by causing network outage are considered to be **malicious.**

5.2 Passive attacks

That mainly consists of lack of cooperation with the purpose of energy saving Nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be **selfish. Selfish** nodes can severely degrade network performances and eventually partition the network

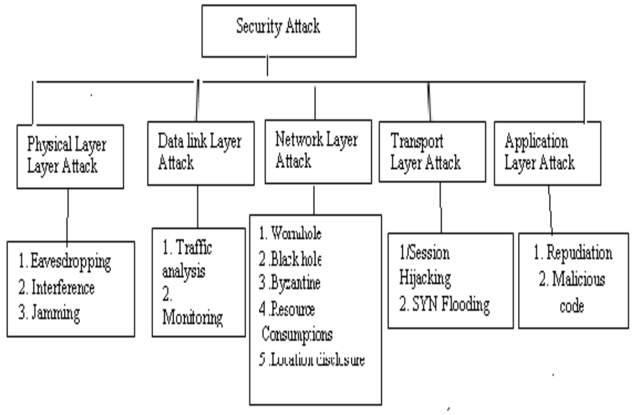


Figure4: Classification of Attacks

Eavesdropping (Physical layer attack) :- Eavesdropping is special kind of attack that usually happen in the mobile ad hoc networks. The goal of eavesdropping is to obtain some confidential information(location, public key, private key or even passwords of the node) that should be kept secret during the communication .Solutions protecting the radio interface from attacks such as eavesdropping (and jamming) attacks have been proposed in the literature, e.g. spread spectrum communication and frequency hopping[11].

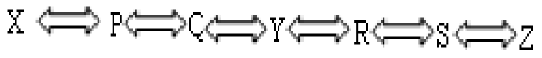
Interference and Jamming (Physical layer Attack):- An adversary sends signals with the same frequently in that a sender and receiver communicates what cause a lot of errors in the transmission. Pulse and random noise are the most common type of signal jamming [12]

Traffic analysis (Data link layer attack):- this is not necessarily an entire passive activity. It is perfectly to engage in protocols, or seek to to provoke communication between nodes. Attackers may employ techniques such as RF direction finding, traffic rate analysis, and time-correlation monitoring. For example, by timing analysis it can be revealed that two packets in and out of an explicit forwarding node at time t and $t+€$ are likely to be from the same packet flow. Traffic analysis in ad hoc networks may reveal: the communications network topology;

- the existence and location of nodes;
- the communications network topology;
- the roles played by nodes;
- the current sources and destination of communications
- The current location of specific individuals or functions (e.g. if the commander issues a daily briefing at 10am, traffic analysis may reveal a source geographic location).

Denial of service (Data link Layer Attach):-In this attack malicious node floods irrelevant data to consume network bandwidth or to consume the resources (e.g. power, storage capacity or computation resource) of a particular node. With fixed infrastructure networks, we can control denial of service attack by using "Round Robin Scheduling", but with mobile ad hoc networks, this approach has to be extended to adapt to the lack of infrastructure, which requires the identification of neighbor nodes by using cryptographic tools, and cost is very high.

For example, consider the following Fig. 3. Assume a shortest path exists from **X** to **Z** and **R** and **Z** cannot hear each other, that nodes **Q** and **R** cannot hear each other, and that **Y** is a malicious node attempting a denial of service attack. Suppose **X** wishes to communicate with **Z** and that **X** has an unexpired route to **Z** in its route cache. **T**ransmits a data packet toward **Z** with the source route **X** --> **P** --> **Q** --> **Y** --> **R** --> **S** --> **Z** contained in the packet's header. When **Y** receives the packet, it can alter the source route in the packet's header, such as deleting **S** from the source route. Consequently, when **R** receives the altered packet, it attempts to forward the packet to **Z**. Since **Z** cannot hear **R**, the transmission is unsuccessful.



Figer 5: Denial of service attack

Spoofing Attack:-

Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its *MAC* or *IP address* in outgoing packets) and alters the target of the network topology that a benign node can gather. As for example, a spoofing attack allows forming loops in routing packets which may also result in partitioning network. Here we have described the scenario in details.

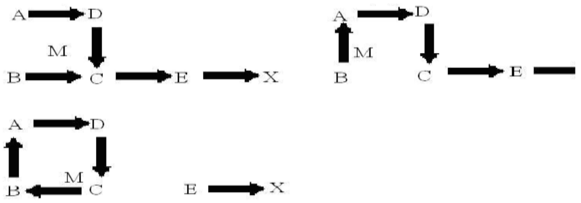


Figure6: A sequence of events forming loops by spoofing packets

Blackhole/Sinkhole (Network Layer Attack):-In a black hole attack a malicious node advertising itself as having a valid route to the destination. With this intension the attacker consume or intercept the packet without any forwarding [13]. An attacker can completely modify the packet and generate fake information, this cause the network traffic diverted or dropped.

Byzantine(Network Layer Attack): A compromised with set of intermediate, or intermediate nodes that working alone within the network carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services within the network [14].

Rushing (Network Layer Attack);- Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack [15]. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Adriane [16]

Partition (Network Layer Attack) An attacker may try to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another.

Tunneling /Wormhole(Network layer attack):

Tunneling attack is also called wormhole attack. In a tunneling attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. It is called tunneling attack because the colluding malicious nodes are linked through a private network connection which is invisible at higher layers [17,18,19]

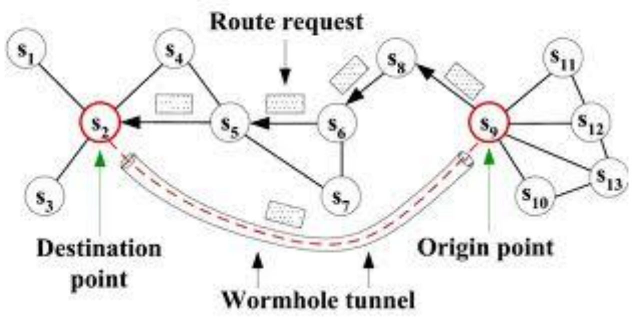


Figure 7: Wormhole Attack

Sybil attack Malicious nodes in a network may not only impersonate one node, they could assume the identity of several nodes, by doing so undermining the redundancy of many routing protocols. In [20], this attack is called the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for storage, routing mechanism, air resource allocation and misbehavior detection. Basically, any peer-to-peer network (especially wireless adhoc networks) is vulnerable to Sybil attack.

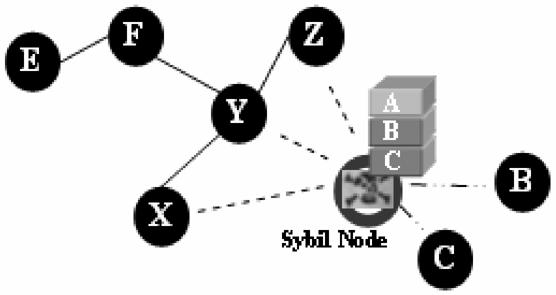


Figure8: Sybil Attack

Session Hijacking (Transport Layer Attach): One weak point is that most authentications processes are only carried out once when a session starts. An adversary could try to appear as an authentic node and hijack the session.

Malicious Code (Application layer Attack) various malicious codes such as virus, worm, spy-wares and Trojan horse attack both operating systems and user applications that cause the computer system and network to slow down or even damaged. An attacker can produce this type of attacks in MANET and can seek their desire information.

Security should be taken into account at the early stage of design of basic networking mechanisms. Have identities security attacks in each layer and corresponding countermeasures. The following table summarizes the potential security attacks and the actions that can be taken to prevent the attack

Table 3: Security Solutions for MANETs.

Layer	Attacks	Solution
Application Layer	Repudiation, data corruption	Detecting and preventing virus, worms, malicious codes and application abuses by use of Firewalls, IDS.
Transport Layer	Session hijacking, SYN Flooding	Authentication and securing end-to-end or point-to-point communication use of public cryptography(SSL, TLS, PCT) etc.
Network Layer	Routing protocol attacks (e.g. DSR, AODV etc.),Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks	Protecting the ad hoc routing and forwarding protocols
Data Link Layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness etc.	Protecting the wireless MAC protocol and providing link layer security support.
Physical Layer	Eavesdropping, Jamming, interceptions,	Preventing signal jamming denial-of-service attacks by using Spread Spectrum Mechanism.

6. CONCLUSION

Mobile ad hoc Network have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Due to mobility and open media nature, the mobile ad hoc networks are much more prone to all kinds 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 wires networks. In this paper we have highlighted the some typical vulnerability which are caused by characteristics of mobile ad hoc networks such as dynamic topology, limited resources (e.g. bandwidth, power), lack of central management's points. And finally we discussed the active and passive security attacks on each layer and their solutions.

7. ACKNOWLEDGMENTS

The authors would like to thank the The Technological Institute of Textile & Science authorities for providing infrastructure to carry out the experiment. And my Research Guide without their help that work is not completed.

8. REFERENCES

[1] B.G.KIN, "The Quality of Service in The Internet" ,IEEE,0-7803-7093-7/0.

[2] T. Bheemarjuna Reddy, I. Karthigeyan, B.S. Manoj, C. SivaRam Murthy."Quality Of Service Provisioning In Ad Hoc Wireless Networks: A Survey of Issues And Solutions. AdHoc Networks" , Ad Hoc NetworksVol.4, pp. 83–124,

[3] Shakeel Ahmed A K Ramani, "Exploring the Requirementsfor QoS in Mobile Ad hoc Networks" Journal of Information & Communication Technology, Vol. 1 No. 2,01-09 , (Fall 2007).

[4] IETF MANET Working Group. Mobile Ad Hoc Networks (MANET). Working Group, Charter available at http://www.ietf.org/html.charters/manet-charter.html

[5] Sannella, M. Ilyas, "The Handbook of Ad Hoc Wireless Networks," CRC Press, 2003.

[6] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 31)*, CRC Press LLC, 2003.

[7] Kostas Papadopoulos, Theodore Zahariadis, Nelly Leligou, Stamatis Voliotis," Sensor Networks Security Issues In Augmented Home Environment", IEEE. ISBN: 978-1-4244-2422-1.

[8] L. Zhou, Z.J. Haas, Cornell Univ., "*Securing ad hoc networks,"* IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044..

[9] Data Integrity, from *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Data_integrity.

[10] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L. Security in mobile ad hoc networks Challenge and solution. IEEE wireless communication, 11, 1, (2004), 38-47.

[11] Hubaux J.-P., Buttyan L., Capkun S., "The Quest for Security in Mobile Ad Hoc Networks", In Proc. of the 2nd

[12] B. Wu, J. Chen, J. Wu, M. Cardei, "*A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,"* Department of Computer Science and Engineering, Florida Atlantic niversityhttp://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf .

[13] Sonja Buchegger and Jean-Yves Le Buddec, "Increasing Routing Security in Mobile ad hoc Network," IBM Research Report: RR 3354, 2001 ACM Int. Symp. on Mobile Ad hoc Networking & Computing, pp. 146-155, 2001

[14] H Deng, W. Li, and D. Agrawal, Routing Security in Wireless Ad Hoc Networks.IEEE Communications Magazine. Vol. 40, No. 10, 2002

[15] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002