Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET)

Rakesh Kumar Singh
Scientist-C,
G.B. Pant Institute of Himalayan Environment & Development, Almora-263 643, Uttarakhand, India and
Research Scholar,
Monad University, Hapur,
Uttar Pradesh, India.

Rajesh Joshi
Scientist-C,
G.B. Pant Institute of Himalayan Environment & Development,
Almora – 263 643,
Uttarakhand, India.

Mayank Singhal
Assistant Professor,
Monad University, Hapur,
Uttar Pradesh, India.

ABSTRACT
A Mobile Ad-Hoc Network (MANET) is a collection of mobile nodes communicating in a multi hop way without any fixed infrastructure such as access points or base stations. Mobile ad hoc networks have several advantages over the traditional wired networks, on the other sides they have a unique set of challenges like MANETs face challenges in secure communication, mobile nodes without adequate protection are easy to compromise, static configuration may not be adequate for the dynamically changing topology in terms of security solution and finally, lack of cooperation and constrained capability is common in MANET. MANET has not well specified defense mechanism, so malicious attacker can easily access this kind of network. Although security issues in Mobile Ad-hoc Networks (MANETs) have been a major focus in the recent years, the development of most secure schemes for these networks has not been entirely achieved till now. This research paper will provide an overview about the security issues and available detection techniques in Mobile ad hoc networks. In this research paper, we will identify the existent security threats an ad hoc network faces, the security services required to be achieved and the countermeasures for attacks.

Keywords
MANET, Security Threats, Denial of Service (DoS), Passive & Active Attack, etc

1. INTRODUCTION
Mobile Ad Hoc Network (MANET) is the category of wireless networks which do not require any fixed infrastructure or base stations or in other words Mobile Ad Hoc Network is a collection of wireless mobile communication devices or nodes that communicate with each other without any fixed infrastructure or centralized administration. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. In MANET, it may be necessary for one wireless mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each wireless mobile node operates not only as a host but also as a router forwarding packets for other wireless mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multi-hop paths through the network to any other node. This type of wireless networking of Mobile ad hoc network is also called infrastructureless networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly.

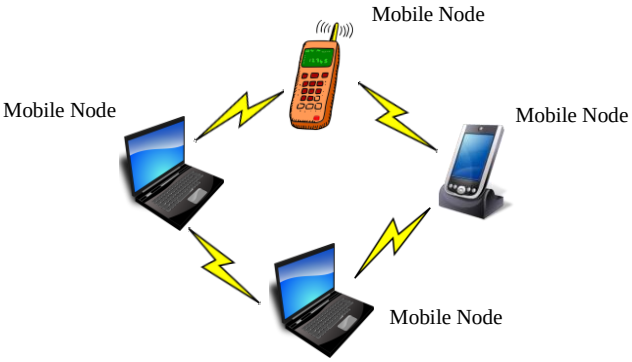

Fig 1: Structure of Mobile Ad Hoc Network (MANET)

2. COMMUNICATION IN MOBILE AD HOC NETWORK
Conventional networks use dedicated nodes to carry out basic functions like packet forwarding, routing, and network management. In mobile ad hoc networks these are carried out collaboratively by all available nodes. Nodes on MANETs use multi-hop communication: nodes that are within each other's radio range can communicate directly via wireless links, while those that are far apart must rely on intermediate nodes to act as routers to relay messages. For example, node X can communicate with node Y by using the shortest path X-P-Q-Y as shown in Fig 2 (the dashed lines show the direct links between the nodes). If node P moves out then alternative route to node Y will be X-R-S-Q-Y.

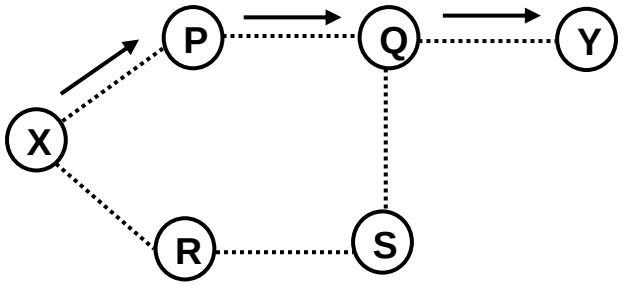

Fig 2: Communication between nodes in Mobile Ad Hoc Networks (MANETs)

3. ADVANTAGES AND APPLICATIONS AREAS OF MOBILE AD HOC NETWORK

The following are the main advantages of the MANET:

(a) ***Low Cost of Deployment*:** As the name suggests, ad hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.
(b) ***Fast Deployment*:** When compared to WLANs, ad hoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.
(c) ***Dynamic Configuration:*** Ad hoc network configuration can change dynamically with time. For the many scenarios such as data sharing in classrooms, etc., this is a useful feature. When compared to configurability of LANs, it is very easy to change the network topology.

Mobile Ad Hoc Network has several interesting applications and some of them are Battlefield, Rescue Operation, Event Coverage, Classroom, Inter-group Communication and Cooperative Work, Personal Area Networks (PAN), Working at Sites with no Infrastructure or where the Infrastructure has been Destroyed, Sensor Networks and Moving Networks.

4. GENERAL ISSUES & VULNERABILITIES ASSOCIATED WITH MOBILE AD HOC NETWORK

The general issues which are associated with mobile ad hoc network are given as follows:

(a) ***Wireless Links:*** The use of wireless links makes the network susceptible to attacks such as eavesdropping and active interference. Wireless networks typically have lower bandwidths than wired networks. Attackers can exploit this feature, consuming network bandwidth with ease to prevent normal communication among nodes.
(b) ***Distributed Network:*** A MANET can be considered as a distributed wireless network without any fixed infrastructure. By distributed, it is meant that there is no centralized server to maintain the state of the clients, similar to peer-to-peer (P2P) networks.
(c) ***Dynamic Topology:*** MANET nodes can leave and join the network, and move independently. As a result the network topology can change frequently. The nodes are mobile and hence the network is self-organizing. It is hard to differentiate normal behaviour of the network from anomaly/malicious behaviour in this dynamic environment.
(d) ***Power Awareness:*** Since the nodes in a mobile ad hoc network typically run on batteries and deployed in hostile terrains, they have stringent power requirements.
(e) ***Addressing Scheme:*** Mobile IP is currently being used in cellular networks where a base station handles all the node addressing. However, such a scheme doesn't apply to mobile ad hoc networks due to their decentralized nature.
(f) ***Network Size:*** Commercial applications of mobile ad hoc networks are an attractive feature of mobile ad hoc networks. However, the delay involved in the underlying protocols places a strict upper bound on the size of the network.
(g) ***Security:*** The three goals of security - confidentiality, integrity and authenticity are very difficult to achieve since every node in the network participates equally in the network.
(h) ***Cooperativeness:*** Routing algorithms for MANETs usually assume that nodes are cooperative and non malicious. As a result, a malicious attacker can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications.
(i) ***Lack of a Clear Line of Defense:*** MANETs do not have a clear line of defense; attacks can come from all directions.
(j) ***Limited Resources:*** Resource constraints are a further vulnerability. There can be a variety of devices on MANETs, ranging from laptops to handheld devices such as PDAs and mobile phones. These will generally have different computing and storage capacities that can be the focus of new attacks. This has led to emergence of innovative attacks targeting this aspect.

5. SECURITY ASPECTS OF MOBILE AD HOC NETWORK

Operating in open and shared media, wireless communication is inherently less secure than wired communication. In addition, since mobile wireless devices usually have limited resources, such as bandwidth, storage space, processing capability and energy – enforcement of security is difficult. The following requirements need to be considered for secure real-time communications:

Confidentiality: Confidentiality ensures that classified information in the network is never disclosed to unauthorized entities.

Integrity: Integrity guarantees that a message being transferred between nodes is never altered or corrupted.

Availability: Availability implies that the requested services (e.g. bandwidth and connectivity) are available in a timely manner even though there is a potential problem in the system.

Authenticity: Authenticity is a network service to determine a user's identity.

Non-repudiation: Non-repudiation ensures that the information originator cannot deny having sent the message.

6. RELATED WORK

The literature survey provides a framework for establishing the importance of the study. It provides direction for the research questions and hypotheses. To understand the current security issues regarding MANET, the literature survey is the essential starting step, which helped to gain in-depth knowledge about different security threats related to MANET.

Kamaljit Lakhtaria (2012) from Sir Padampat Singhania University, Udaipur, India in his book "Technological Advancements and Applications in Mobile Ad-Hoc Networks: Research Trends" has worked on the recent technological advancements and applications in Mobile Ad-Hoc Networks and he has also describe physical level security aspects in MANET. Kamanshis Biswas and Md. Liakat Ali (2007) from Blekinge Institute of Technology, Sweden in his research "Security Threats in Mobile Ad Hoc Network" has provided the comprehensive study on the layer based security issues in MANET. Zhou and Haas (1999) from Cornell University, Ithaca, New York in their research "Securing Ad Hoc Networks" have proposed using threshold cryptography for providing security to the ad hoc network. Sanzgiri, et al. (2002) from University of California, Santa Barbara, CA in his research "A Secure Routing Protocol for Ad Hoc Networks" has proposed a secure routing protocol ARAN which is based on certificates and successfully defeats all identified attacks. Hongmei Deng, Wei Li, and Dharma P. Agrawal (2002) form University of Cincinnati, United States in their research "Routing Security in Wireless Ad Hoc Networks" have focused on the routing security issues in MANETs and have described a solution of 'black hole' problem. Bin Xie and Anup Kumar (2004) in their research "A Framework for Internet and Ad hoc Network Security" has proposed the security issues in different protocol stack of MANET with routing protocol discovery.

7. RESEARCH GAP

- ***Research in Other Countries on MANET:*** Number of research have been carry out in past in many countries on the subjects "Routing Protocols, Internet Connectivity in MANET, Routing Algorithms, MANET Challenges, Security Aspects of MANET, Distributed Data Caching in MANET, Multi-Path Algorithms, Energy Conservation in MANET, TCP over MANET, Cryptography Techniques, etc. But no research has been done on "Layer based security threats and countermeasures in MANET".

- ***Research in INDIA on MANET:*** Less research work has been carried out in India on MANET (mostly research work has been done on routing protocols based algorithms and security, etc.).

8. NEED OF STUDY

Mobile ad hoc network has been a challenging research area for the last few years because of its dynamic topology, power constraints, limited range of each mobile host's wireless transmissions and security issues etc. If consideration is given only a stand-alone MANET then it has limited applications, because the connectivity is limited to itself. MANET user can have better utilization of network resources only when it is connected to the Internet. But, global connectivity adds new security threats to the existing active and passive attacks on MANET. A connection could be disrupted either by attacks on any of the layer of MANET and due to this reason, almost all possible attacks on the traditional ad hoc networks also exist in mobile ad hoc networks. Whatever the attacks are, the attackers will exhibit their actions in the form of refusal to participate fully and correctly in communication between the mobile nodes according to the principles of integrity, authentication, confidentiality and cooperation.

9. PROBLEM STATEMENT

This research is focused on the overall security threats and challenges in Mobile ad hoc networks *(MANET)*. Studies on MANET have focused more on single attacks. In the meanwhile some attacks involving multiple nodes have received little attention since they are unanticipated and combined attacks. There have been no proper definition and categorization of these kinds of attacks (multiple node attacks) in MANET. Some mitigation plans have been proposed to counteract against some form of multiple node attacks; thus, there is need to figure out the consequences of the category of collaborative attacks and their possible mitigation plans. Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network.

10. OBJECTIVES

In this research, different security aspects will be discussed and how these security issues can be resolved? The security issues will be analyzed from individual layers namely application layer, transport layer, network layer, data link layer and physical layer. This research will provide a good understanding of the current security threads and optimum solutions of the MANETs. The broad objectives of the research are:

- To study and analysis of security threats and vulnerabilities in Mobile Ad Hoc Network (MANET).
- To achieve optimum solutions and countermeasures for the security threats in MANET.
- To study and enlisting the challenges of MANET.

11. SCOPE OF RESEARCH

Wireless mobile ad hoc nature of MANET brings new security challenges to network design. Mobile ad hoc networks, due to their unique characteristics, are generally more vulnerable to information and physical security threats than wired networks or infrastructure-based wireless networks. In this research, various security requirements for mobile ad hoc network will be explored and the different types of threats an ad hoc network faces. This research

identifies the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In this research, there is lots of scope to focus on the fundamental security problems of the Mobile ad hoc network.

12. RESEARCH METHODOLOGY

Research methodology defines the research activity, development of research activity and measurements used to advance the research work by implementing these measures which assist to achieve the objectives of the research. During the starting phase, extensive literature survey will be carried out; the information gained in this phase will play important inputs for the research and further following studies and analysis will be undergone to find out the research objectives:

- Complete study and analysis of each layer of MANET.
- Identification of security threats and vulnerabilities in each layer.
- Discover best solutions and countermeasures for security threats.
- Analysis of challenges in MANET.
- Research output and thesis.

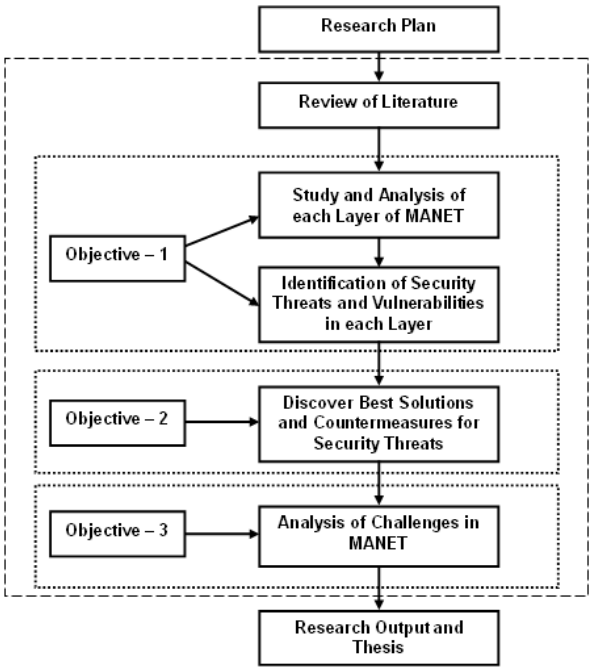

Fig 3: Graphical representation of Research Methodology

In this research, consideration are not only given to define and categorize collaborative security attacks in MANET, but also to identify the performance impact in MANET under a collaborative attack as well as which mitigation plans can be used to alleviate this kind of attack. The Fig 3 represents the proposed research methodology for this research in a pictorial view.

13. ATTACKS IN MOBILE AD HOC NETWORK

At the highest level, the security goals of MANETs are not that different from other networks: most typically authentication, confidentiality, integrity, availability, and non-repudiation. Authentication is the verification of claims about the identity of a source of information. Confidentiality means that only authorized people or systems can read or execute protected data or programs. It should be noted that the sensitivity of information in MANETs may decay much more rapidly than in other information. In MANETs security goals of a system can change in different modes. The characteristics of MANETs make them susceptible to many new attacks. At the top level attacks can be classified according to network protocol stacks.

Table 1. Some attacks in MANET

Layer	Attack	Security Issues
Application	Data corruption, viruses and worms	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport	TCP/UDP SYN flood	Authentication and securing end-to-end or point-to-point communication through data encryption
Network	Wormhole, Hello flood, Black hole	Protecting the ad hoc routing and forwarding protocols
Data Link	Monitoring, traffic analysis	Protecting the wireless MAC protocol and providing link layer security support
Physical	Jamming, Eavesdropping, active interface	Preventing signal jamming denial-of-service attacks

The attacks can be classified as passive or active attack:

(A). Passive Attacks: In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis. Some of passive attacks are:

- Eavesdropping Attacks
- Traffic Analysis

(B) Active Attacks: These attacks cause unauthorized state changes in the network such as denial of service, modification of packets, and the like. These attacks are generally launched by users or nodes with authorization to operate within the network. We classify active attacks into four groups: dropping, modification, fabrication, and timing attacks. It should be noted that an attack can be classified into more than one group. Some of active attacks are:

- Dropping Attacks
- Modification Attacks
- Fabrication Attacks
- Timing Attacks

14. CONCLUSION

In this research, it has been tried to deal with security issues in Mobile ad hoc networks. A Mobile ad hoc network has open media nature and free mobility that's why it needs much more prone with respect to security risks e.g. intrusions, information disclosure and denial of service etc. A Mobile ad hoc network needs high level of security as compare to the traditional wired networks. The aim of this research is to discuss different aspects of security threats and to achieve optimum solution for these types of security threats with challenges of MANET

15. ACKNOWLEDGEMENT

We would like to thank Dr. L.M.S. Palni, Director, G.B. Pant Institute of Himalayan Environment & Development, Kosi-Katarmal, Almora, Uttarakhand, India and Dr. Mianjan, Vice-Chancellor, MONAD University, Hapur, Uttar Pradesh, India for their continuous support and encouragement for writing this paper.

16. REFERENCES

[1] Kamanshis Biswas and Md. Liakat Ali (2006), "*Security threats in Mobile Ad Hoc Network"*. School of Engineering, Blekinge Institute of Technology, Sweden.

[2] H. Deng, W. Li, Agrawal, D.P. (2002), "*Routing security in wireless ad hoc networks,"* Cincinnati Univ., OH, USA; IEEE Communications Magazine, Volume: 40, page(s): 70- 75, ISSN: 0163-6804.

[3] B. Wu, J. Chen, J. Wu, M. Cardei (2006), "*A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,"* Department of Computer Science and Engineering, Florida Atlantic University.

[4] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang (2004), "*Security in mobile ad hoc networks: challenges and solutions,"* In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s): 38- 47, ISSN: 1536-128439.

[5] L. Zhou, Z.J. Haas (1999), Cornell University, New York, USA. "*Securing ad hoc networks,"* IEEE Network, Volume: 13, Page(s): 24-30, ISSN: 0890-8044.

[6] Ching -Chuan Chiang, Hsiao-Kunag Wu, Winston Liu and Mario Gerla (1997), "*Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel*," IEEE Singapore International Conference on Networks, SICON'97, pp. 197-211.

[7] C.E. Perkins, E. Royer, and S.R. Das (2000), "*Ad hoc on demand distance vector (AODV) routing*," Internet Draft.

[8] Hongmei Deng, Wei Li, and Dharma P. Agrawal (2002), "*Routing Security in Wireless Ad Hoc Network*," IEEE Communications Magzine, vol. 40, no. 10.

[9] P. Papadimitratos and Z. Haas (2002). *"Secure routing for mobile ad hoc networks" (SRP)* SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, pp. 27-31.

[10] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang (2001). "Providing robust and Ubiquitous Security support for Mobile Ad Hoc Networks ", Proceedings of the 9th International conference on Network Protocols (ICNP), Riverside, California, USA.

[11] F. Stajano and R. J. Anderson (1999). "*The resurrecting duckling: Security issues for ad-hoc wireless networks*" In 7th Security Protocols Workshop, volume 1796 of Lecture Notes in Computer Science, Cambridge, United Kingdom. Springer-Verlag, Berlin Germany.

[12] T. Camp, J. Boleng, and V. Davies (2002). "*A Survey of Mobility Models for Ad Hoc Network Research*", in Wireless Communication & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, vol. 2, no. 5.

[13] Manel Guerrero Zapata (2002), "*Secure Ad hoc On-Demand Distance Vector Routing",* ACM Mobile Computing and Communications Review (MC2R), 6(3):106-107.

[14] Technological Advancements and Applications in Mobile Ad-Hoc Networks: Research Trends (2012) by Kamaljit Lakhtaria, Sir Padampat Singhania University, Udaipur, India.

[15] Mobile Ad Hoc Networks: From Wireless LANS to 4G Networks (2009) by George Aggelou, Tata McGraw Hill Education Private Limited, Noida, India.

[16] Security Threats in Mobile Ad Hoc Network (2007) by Kamanshis Biswas and Md. Liakat Ali, Blekinge Institute of Technology, Sweden.

[17] Secure Tracking of Node Encounters in Multi-Hop Wireless Networks (2003) by Srdjan Capkun , Levente Buttyán , Jean-Pierre Hubaux, Swiss Federal Institute of Technology Lausanne (EPFL), Lausanne, Switzerland.

[18] Securing Vehicular Ad Hoc Networks (2007) by Maxim Raya and Jean-Pierre Hubaux, School of Computer and Communication Sciences, EPFL, Switzerland.

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

[20] Routing Security in Wireless Ad Hoc Networks (2002) by Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati, Clifton Avenue Cincinnati, OH, United States.

[21] M. Jakobsson, S. Wetzel, and B. Yener (2004). *"Stealth Attacks on Ad Hoc Wireless Networks"*. *Proc. of IEEE Vehicular Technology Conference* (VTC). IEEE 60th, Volume: 2.