Mobile Ad Hoc Networks- A Holistic Overview

Ritika Sharma
Pursuing M.Tech, Dept. of ECE
AITR, Mangaliya Square
Indore, MP, India

Minakshi Halder
Pursuing M.E. Dept. of ECE
SGSITS, 23 Park Road
Indore, MP, India

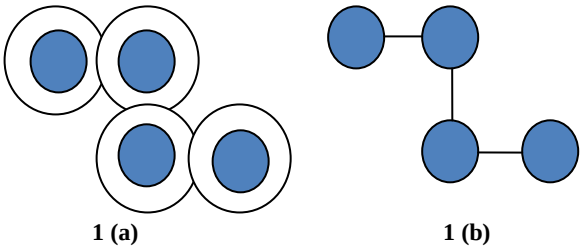
Kamlesh Gupta
Associate Prof., Dept. of ECE
AITR, Mangaliya Square
Indore, MP, India

ABSTRACT
Mobile ad hoc networks (MANET) comprise mobile devices to form an ad hoc network for some ad hoc purpose. So, this special feature of a MANET allows it to be the most demanding technology amongst the users, and the most concerned topic of research in the field of wireless networks. Following the latest trends of research in the field of wireless communication, this paper attempts to focus on some growing issues in MANETs. Security, one of the most important aspects of communication, which faces severe challenges due to various constraints imposed by MANET, is discussed in this paper including vulnerabilities, attacks, various security goals and the applications of MANET. Along with the security, it also describes the routing protocols and the related work that has already been done in this field.

General Terms
Mobile ad hoc network (MANET), topology, protocol, routing, router, security.

Keywords
MANET, Wireless Networks, Ad hoc Networking, Routing Protocol.

1. INTRODUCTION
The name, Mobile ad hoc network (MANET), itself implies three considerations about the technology, namely, "Mobile", which entails moving nature of the network, "Ad hoc", which means temporary in nature, and "Network", which illustrates an arrangement of mobile devices for sharing information with one another. Other than these three main considerations, appending some more features gives us a clear and a complete definition of MANET. The simplest example of a MANET is shown in Figure 1 (a), (b):



1 (a) 1 (b)

Fig 1 (a): Mobile devices in each other's wireless range.
1 (b): Mobile devices forming wireless links.

So, mobile devices forming an autonomous, provisional, infrastructureless, dynamic (in topology), self-configuring, self-organizing, and self-administrating wireless network for information sharing is known to be a 'mobile ad hoc network', [1, 2, 3, 4, 5]. It has become the most prominent and challenging area of research in recent years due to abundance of inexpensive, widely available, more user affable and more powerful wireless mobile devices [6, 7,]. Moreover, such devices offered the users to exploit their features up to the greatest flexibility provided by the MANET. In addition to the abundant existence of such devices, another important fact that sparks the need of MANET than other traditional wireless networks is their availability in emergency and rescue operations [2]. In such events, the users cannot afford (in terms of time, cost, and resources) to set up an infrastructure for communication. Since there is no fixed range or size of MANET, the devices can abruptly leave or join the network, whenever it is required. All what the devices need to do for establishing communication with one another is to be within the wireless range of their neighboring mobile nodes. The biggest drawback faced by the MANETs is their vulnerability to malicious attacks, which are comfortably introduced by the attackers due to the various features such as dynamic topology, mobile nodes, limited physical security, scalability and decentralized management offered by them.

2. RELATED WORK
Many authors working in this field have suggested that security is one of the most important issues that have to be considered while having communication in MANET [1, 3, 4, 8, 9]. The authors of many research papers have considered routing security a serious issue [5, 8, 10, 11]. The major research areas in the field of MANET attempt to propose secure routing solutions to prevent the network from various attacks [12, 13]. The current trends as mentioned by some authors in this field suggests the researchers to study the role of MANET in the evolution of future wireless technologies for bringing ad hoc networks at the center of evolution towards the 4^{th} generation wireless technology [14, 15]. Various researchers stress their work on the attacks that impose threat to a MANET [16, 17, 18]. Most of the related works available in the literature of MANET include its challenges and applications as it directs the future of the technology [14, 19]. The major research areas of MANET also lie in, working on various vulnerabilities and threats that a wireless ad hoc environment is exposed to, than from traditional wired or wireless network environments [1, 3, 4, 6]. Some other weaknesses of MANET such as energy constraints, frequent node mobility, limited bandwidth, routing disruption, lack of centralized management etc., that can easily expose a MANET to severe attacks and threats, draws the attention of many researchers to work on them. The growing market of wireless devices, such as PDAs, laptops, palmtops, tablet computers etc. that sparks the MANET technology to be used aggressively is also studied and stressed by some authors to focus on the increasing applications of MANET [1, 2, 3]. This paper attempts to comfort the beginners in this field by emphasizing on such challenges, routing schemes, applications and vulnerabilities of MANET and the efforts it needs to protect its vulnerabilities from being

exploited, so that they may be able to produce a clear picture of MANET to work ahead.

3. VULNERABILITIES AND CHALLANGES IN MANET

Vulnerability is a weakness, which allows an attacker to reduce a system's information assurance. It is the intersection of three elements: system susceptibility or flaw, attacker access to the flaw and attacker's capability to exploit the flaw [9, 6, 12, 19]. The various challenges that are exploited and so appear as vulnerabilities in MANET are discussed below:

3.1 Stingy Resources

As the resources available to the mobile nodes in a mobile ad hoc environment are not sufficient, the users become stingy while communicating. Due to limited bandwidth, higher cost, slower links and power constraints, the users, i.e., the mobile nodes may be lured for these constraints by the attackers and therefore such stingy resources may make the network vulnerable to attacks.

3.2 Decentralized Management System

The two important features of MANET, namely, ad hoc nature, and the dynamic topology make the network unpredictable. So in the absence of centralized monitoring systems, such unpredictable networks may easily be exposed to various attacks at anytime and anywhere.

3.3 Packet Dropping

If the network is suffering from packet drop, it may not be able to identify the reason for it. As the packet dropping can be due to attack as well as due to some physical characteristic of the node and the network, there will not be a clear difference between a malicious node and a legitimate network node. So, packet dropping can make the network easily vulnerable to attack, as it cannot be easily detected.

3.4 Routing Table Entries

As many of the routing schemes, protocols and algorithms rely on routing table entries for maintaining the routes established before communication, the attacker node may easily attack the routing table of the nodes and then easily attack and harm the network.

3.5 Assumption Taken by Routing Protocols

Almost all the routing protocols available for the MANET, work with an assumption that all the nodes of the network are legitimate; as a result an attacker can easily befool the routing scheme to be a part of the prey network. Many authors who have worked in this stream have not included this aspect, which can be harmful for a network.

3.6 Dynamic Topology

The MANET is prone to attacks mainly due to three dynamic features; firstly, the nodes do not have any fixed location in the network, they are flexible enough to move around the network without any limitation at any time. Secondly, the nodes do not have any fixed links with each other for communication; they can establish the routes at any time with any of the nodes of the network. Thirdly, the nodes can randomly and abruptly leave or join the network. These three dynamic features make the MANET vulnerable to the attacks. Figure 2 shows topology at different instants of time.

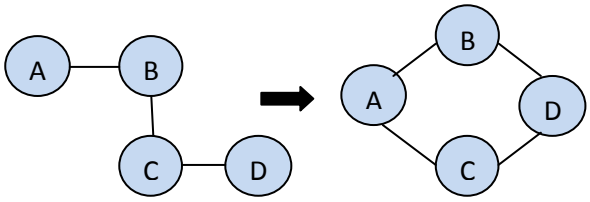


Fig 2: Topology changes dynamically to connect node A and node B, as the nodes move.

3.7 Limited Power Supply

The mobile nodes used in MANETs are the devices, which are battery dependent. As the batteries have limited power the nodes may suffer frequent power failures. Also, due to less power, the lifetime of the node may reduce and it may not be able to run complex security algorithms to secure itself from attack.

3.8 Bandwidth Constraint

The wireless networks have limited capacity links, and therefore, they are more vulnerable to environmental disturbances, which can degrade the quality of service of the network. They are more prone to external interferences, external noise, signal attenuation etc.

3.9 Compromised Nodes

The internal nodes of the MANET that behave maliciously are the inside attackers and are known as compromised nodes. These inside malicious nodes are compromised by some unauthorized users known as attackers or hackers through remote penetration.

3.10 Unclear Boundary of Defense

The physical boundary of the network would define the area where the attack would happen only from within the network, and no outside intrusion would be allowed. However, as the MANETs do not have any physical boundaries, the attacker node just has to be within the radio range of the prey node.

4. SECURITY ASPECTS

Communication security plays a vital role while dealing with MANETs. The self-organizing and self-configuring natures of the nodes make them more prone to attacks. The information that is to be communicated can be easily harmed by the adversary, so there is a great deal of efforts required to secure the data. Before securing the information, one must be aware of the features that information should bear so as to understand the effects of attack. The aspects of communication required to be fulfilled to keep the data secure are discussed below [9, 6, 17]:

4.1 Availability

This aspect demands the authorized parties to access the resources at suitable times i.e. whenever required for communication. This means, all the authorized or legitimate nodes must be available to each other at any time they need to communicate, whether for data, services or some resources.

4.2 Confidentiality

The license or authorization of the information content only to the legitimate nodes offers the confidentiality of the information as well as the network. Privacy, secrecy, discretion are some synonyms of confidentiality, which are used in literature. For this to be maintained, we must mount

some security mechanisms such as cryptography, to make our information confidential.

4.3 Integrity

Integrity defines the capability of the information not to be manipulated, and, if needed, then only by legitimate nodes in a legitimate manner. Manipulation of the data can be done in many ways, for instance, appending some information, deleting, overwriting, changing the content, changing the sense or meaning, creating new data, and changing status of the data. It is the responsibility of the network for transmitting the data without corrupting the content.

4.4 Authentication

It is possible in a network that an adversary attempts to change its identity to destination's identity, so the peer nodes must be able to recognize and ensure each other's identity to provide authentication of data. Only the required nodes must be able to receive the data. Even if the data is received by an adversary, it must not be able to decrypt it.

4.5 Non Repudiation

In some situations of compromised nodes it is possible that the compromised sender or receiver denies that they have ever transmitted or received the data. So, for such scenarios non repudiation ensures the activity of sender and receiver, i.e., that sender and receiver of a message cannot renounce that they have ever sent or received such a message.

4.6 Anonymity

Anonymity means all information that can be used to identify owner or current user of node should be kept private and not be distributed by node itself or the system software.

4.7 Authorization

This specifies the different users to have authority to work for different functions. For example a network management can be performed by network administrator only.

5. ATTACKS IN MANET

Wireless ad hoc networks are severely and frequently exposed to the attackers. The reasons behind this vulnerability are very clear, i.e., the shared physical media, decentralized management, limited resources, and highly dynamic topology. All these reasons motivate the attackers to easily disrupt the network performance [1, 3, 4, 13, 16, 18]. There are three major levels of classification of attacks a MANET suffers and are not yet discussed by many authors, they are as follows:

5.1 On the Basis of the Location of Node

The location or the placement of the node whether it is within the network boundaries or outside it decides the type of attacks that can be implemented on a network.

5.1.1 Outside or External Attacks

The location of the malicious nodes in such networks is outside the boundaries of a network. In this, the malicious nodes are not the part of the network but try to disrupt the network operation.

5.1.2 Inside or Internal Attacks

Here the location of the malicious nodes or a node lies within the geographic boundaries of the network under attack. In this type of attack, the nodes of the actual network are compromised by unauthorized access by attacker node through remote penetration. Such attacked nodes are also known as compromised nodes

5.2 On the Basis of Attacker's Intension

The attackers in MANETs usually target the network, to fulfill two main intensions. The first is to disrupt the normal network operation to degrade the network performance, and second is just to listen to the messages being transmitted through the network without altering its normal operation. The above two intensions aim to information disclosure. These two intensions specify two types of attacks, discussed as follows [4, 3]:

5.2.1 Active Attacks

These are the attacks where the attacker node alters the normal network operation to disrupt the network performance. They can physically damage a node to terminate its operation from the network, can capture the messages to modify and replay the messages back in the network; they can also disrupt the normal routing scheme, and can consume the network resources such as bandwidth, memory, computational power, and energy. An example of such an attack is shown in the following Figure 3.

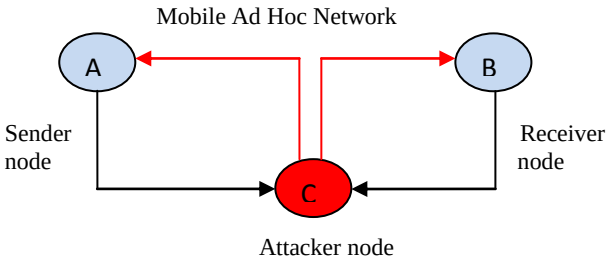


Fig 3: An active attack where the attacker alters the network operation.

5.2.2 Passive Attacks

In such attacks, the attacker does not disturb the network operation; it just aims to hear the information, and monitors the traffic to understand the routing so that it may hinder the privacy of communication, and cause eavesdropping of the messages from the network. An example is in Figure 4.

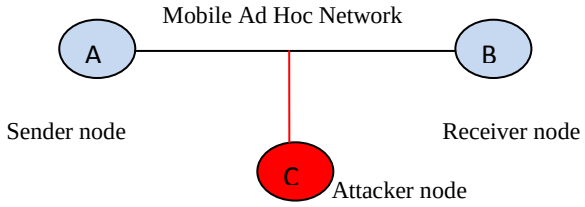


Fig 4: A passive attack where the attacker hears the messages on the links in usage.

5.3 On the Basis of the Layer Attacked

The different layers at which communication is done can also be attacked. Such types of attacks can be classified as follows [3, 4, 9]:

5.3.1 Network Layer Attack

On the network layer, following attacks may occur:

5.3.1.1 Wormhole Attack

In this attack, two malicious nodes tunnel the data from one point to other through a wireless or a wired link. These two malicious nodes are the wormhole nodes pretending the prey nodes that they will provide them with shortest and the fastest link than the normal multi hop links. They achieve this by

attacking the routing table of the prey nodes and by making their route entries in their routing table.

5.3.1.2 Black Hole Attack

In this type of attack, the malicious node provides source with false path to the destination, and then it forwards all the messages to itself. The messages that are forwarded to itself will not be forwarded to any node in the network again. We can say it engulfs the entire data of the attacked nodes from the network.

5.3.1.3 Routing Attack

The prime objective of this attack is to disrupt the normal routing scheme of the normal network. It can cause severe damages in the network by overflowing the routing table entries, by sending false route updates, and modifying the routing table to jam the networks. The various examples of routing attack are: routing table poisoning attack, packet replication attack, rushing attack and routing table overflow attack.

5.3.2 Transport Layer Attacks

The adverse type of activity that an attacker does at the transport layer is session hijacking. Generally a session is executed between the two parties and is done for the purpose of authentication; an attacker can act as one party in the whole session and so hijack it.

5.3.3 Application Layer Attack

The attacker takes care of all the vulnerabilities of the attack and then tries to corrupt the data in all the possible ways it can.

5.3.4 Multi Layer Attacks

The attacks that can occur at any layer fall under this category of attacks. Some of these attacks are discussed below:

5.3.4.1 Spoofing Attack

In this, the attacker replicates its identity as the node to which the messages are directed in the network.

5.3.4.2 Denial of Service Attack

This attack affects the network in two ways; Firstly, by routing disruption, which makes the routing scheme disfunctioning so that it may not provide the networking services. Secondly, it affects the network by consuming the network resources like bandwidth, memory, computational power, and energy. Some other attacks which fall under this category are; replay attacks, man in the middle attacks etc.

6. MANET APPLICATIONS

With the advent of various digital devices and wireless communication, MANET is becoming one of the most demanding technologies in the field of communication with an infrastructureless scenario. As infrastructure cannot be set up in some situations, it becomes impossible to communicate with the recent wireless and wired technology. So, it is necessary to find a way out of this constraint. Following this current trend of wireless technology, MANET finds various applications in various areas of communication. As these networks are autonomous in nature, they do not depend on any supervising authority to regulate communication amongst the devices. There is a wide range of flexibility offered by MANETs. Devices in the network do not have to be bounded with specific services. They can be utilized for variety of applications at any time. The optimal utilization of the links is possible in MANETs. The applications offered by MANETs are unique in nature from the traditional wired and wireless networks. These applications with their possible scenarios and services offered by them are listed below [7, 14, 19]:

6.1 Military and Battlefield Networks

The real origin of ad hoc networks are the military and battlefield networks, which allows the soldiers to establish their communication whenever required and wherever it is needed. The autonomous arrangement of the vehicles and communication among them becomes possible by such networks only. The rescue operations could be made possible easily through such networks by sharing the information with the headquarters.

6.2 Emergency Services

Emergency can arrive in various situations like during disasters, rescue & search operations, policing & fire fighting, medical aids. So, whenever such emergencies come around us, we need to have a fast and temporary network, which does not depend on any infrastructure to be laid. As emergencies cannot bear or afford to wait for such infrastructures to be installed, communication and information reach out are provided through such mobile ad hoc networks. Moreover, if infrastructure networks are laid for emergency services they will not be needed after the emergency goes off, so such attempts can prove to be a waste of investment.

6.3 Commercial and Civilian Environment

Nowadays, commercial environments also require systems which could provide them with the fastest way of sharing information anywhere and anytime the need. The commonest example of such category of communication is E-Commerce; where electronic payments are possible anywhere and anytime. Also, the users from business environments also take advantage of these networks by accessing the dynamic and versatile data base system.

Civilians or the common people need such networks in vehicle systems to guide them with the traffic scenarios, which could in turn reduce the frequency of accidents, weather information, inter vehicle networks, such ad hoc networks are now known to be Vehicular ad hoc networks (VANETs).

Other than above, areas of public gatherings like stadiums, shopping malls, fairs, airports etc. also require having communication and information sharing through such networks.

6.4 Home and Enterprise Networking

For creating wireless networks for communication within the range of a home or an enterprise like a conference or a meeting, MANETs are best suited.

Public Area Networks (PANs) are the best application of MANETs where digital devices like PDAs, mobile phones, laptops etc. are in housed with wireless connectivity features with short range so that all the neighboring devices could be connected to each other for communication and can also have access to the internet by WLANs, and GPRS systems.

6.5 Education and Entertainment

Universities and campuses are bow moving towards virtual classrooms for the students, so that they can be benefitted with every piece of knowledge without being any constraint of connectivity, from anywhere it is possible. Ad hoc communications could be held during lectures.

6.6 Sensor Networks

Smart sensor systems and actuators can be embedded in mobile devices so that they can be able to sense and detect

various environmental conditions, chemical or biological detections, temperature information, humidity, animal movements etc. Then these sensed data can be communicated for further required action.

7. ROUTING PROTOCOLS

'Routing', as the name implies, is the mechanism which provides the routes for connecting the nodes with each other in a network. There are different routing protocols which employ different mechanisms depending upon the different scenarios of network. As the wireless networks are entirely different from wired networks, there is also great difference in the routing protocols employed for them, moreover in wireless networks also, the infrastructure less and infrastructure networks have slightly different protocols to support the autonomous nature of the nodes. In MANETs the wireless nodes serve as routers for communication. Many authors up till now have covered various protocols individually but the general tasks are not discussed [4, 5, 8, 11, 12, 13]. The main tasks or responsibilities of a routing protocol: to send route request messages (RREQ) for investigating the routes, to receive route reply messages (RREP) from the neighboring nodes for route confirmation, and to maintain the established routes, by updating the route entries in the routing tables. Routing protocols in MANETs are broadly classified into three categories, described as follows [5, 8, 10, 13, 15]:

7.1 Proactive or Table Driven Routing Protocols

These protocols work aggressively for establishing and maintaining the routes in the network. In this, the whole network is known to all the nodes comprising the network. The routing tables of all the nodes are updated in advance for other nodes and therefore run in pace with the dynamic topology.

Examples: Destination-Sequenced Distance Vector Routing Protocol (DSDV), Wireless Routing Protocol (WRP), Global State Routing (GSR), Fisheye State Routing (FSR), Hierarchical State Routing (HSR), Zone-Based Hierarchical Link State Routing Protocol (ZHLS), and Cluster head Gateway Switch Routing Protocol (CGSR).

Problems: Periodically updating the network topology and route entries exhaust the batteries of the nodes as they always have to be active, increases the bandwidth overhead, unwanted redundant route entries.

7.2 Reactive or On Demand Routing Protocols

These protocols are known to have a little lazy approach. They do not update their routing tables periodically unless it is demanded by any node. They aren't suitable for the networks that are highly dynamic and prone to frequent changes. The lives of the route entries in routing tables of the nodes are until the routes are no longer needed. The routes are decided on the basis of the shortest path.

Examples: Cluster Based Routing Protocols (CBRP), Ad Hoc On Demand Distance Vector Routing Protocol (AODV), Dynamic Source Routing Protocol (DSRP), Temporarily Ordered Routing Algorithm (TORA), Associativity Based Routing (ABR), Signal Stability Routing (SSR).

Problems: They do not find the routes unless demanded hence do not update themselves to the route changes. Due to lack of awareness of the changing topology, the routes may expire after certain duration of time.

7.3 Hybrid or Exploited Reactive and Proactive Routing Protocols

It exploits the characteristics of both the reactive and proactive routing protocols to get the better results. It combines the two different protocols in a way unique way. It arranges the network into zones, it uses proactive protocol with in a zone and reactive to route the packets in the nodes of different zones.

Example: Zone Routing Protocol (ZRP).

Problem: Hybrid Routing Protocol is not an appropriate choice for small networks.

The afore mentioned routing protocols are tactical and smart enough to deal with constraints like power consumption, low bandwidth, high error rate, and unpredictable node movements. The effectiveness of these protocols is evaluated on the basis of some quantitative performance metrics like, average end to end delay, throughput, packet delivery ratio, route acquisition time etc.

8. CONCLUSION AND FUTURE SCOPE

The future of any technology depends on variety of applications it follows and vigorous research work going in that particular field. As MANET is not a new technology in the field of wireless communication, a lot of work has been done and more than this is still required to be done. The increasing number of users of MANET encourages the researchers to continuously work in this field to produce better and satisfactory results. The various areas of researches that are possible in this direction are deeply analyzed in our paper. Security which is importantly required for a successful communication attracts various researchers to implement their work in this field. The current researches [1, 2, 3, 4, 6, 15], have tried to emphasize on the threats, vulnerabilities and attacks, a MANET is prone to. The efforts are still going to produce much energy efficient, cheaper, and more capable mobile nodes, performance. The future of the ad hoc networks can be foreseen as a much cheaper, easily deployable, anytime, anywhere so that it may turn out to provide us with much improved network, large scale wireless network which will be able to serve a variety of applications to a variety of users.

9. REFERENCES

[1] Pradip M, Jawandhiya, Mangesh M Ghonge, Dr. M S Ali, "A Survey of Mobile A d Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 02, 2010, 4063-4071. .

[2] Imrich Chlamtac, Marco Conti, Jennifer J-N Liu, "Mobile Ad Hoc Networking-Imperatives and Challenges", Elsevier, 2003, 13-64.

[3] Vikas Solomon Abel. "Survey of Attacks on Mobile Ad Hoc Networks", International Journal on Computer Science and Engineering, Vol. 03, No. 02, February 2011, 826-829.

[4] Shalini Jain, Dr. Satbir Jain, "Detection and Prevention of Wormhole Attack in Mobile Ad Hoc Network", International Journal of Computer Theory and Engineering, Vol. 2, No.1, Feb 2010, 78-86.

[5] Panagiotis Papadimitratos and Zugmunt J. Haas, "Secure routing for Mobile Ad Hoc Networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS-2002), San Antonio, TX, January 27-31, 2002.

[6] Priyanka Goyal, Vinti Parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Applications", International Journal of Computational Engineering & Management, Vol. 11, January 2011, 32-37.

[7] A Rahim, I Ahmed, Z S Khan, M Sher, M Shoaib, A Javed, R Mahmood, "A Comparative Study of Mobile and Vehicular Ad Hoc Networks", International Journal of Recent Trends in Engineering, Vol. 02, No. 04, November 2009. 195-197.

[8] Hongmei Deng Weiji, and Dharma P Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Magazine, October 2002, 70-75.

[9] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks-A Survey", Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 1-23.

[10] Po- Wah Yau and Chris J. Mitchell, "Security of Attacks on Mobile Ad Hoc Wireless Networks", Information Security Group, University of London.

[11] Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 01, No. 03, August 2010, 279-285.

[12] GS. Mamatha and Dr. S.C. Sharma, "Analyzing MANET Variations, Challenges, Capacity and Protocol Issues", International Journal of Computer Science and Engineering Survey (IJCSES), Vol. 1, No.1, August 2010, 14-21.

[13] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A Survey of Blackhole Attacks in Wireless Mobile Ad hoc Networks", Human-Centric Computing and Information Sciences (a Springer journal), 2011, 1-16.

[14] Jiazi YI, "A Survey on the Applications of MANET", Polytech' Nantes, February 2008.

[15] G. Vijaya Kumar, Y Vasudev Reddyr, Dr. M. Nagendra, "Current Research Work on Routing Protocols for MANET: A Literature Survey", International Journal on Computer Science and Engineering, Vol. 02, No. 03, 2010, 706-713.

[16] Priyanka Goyal, Sahil Batra, Ajit Singh, "A Literature Review of Security Attacks in Mobile Ad-Hoc Networks", International Journal of Computer Applications, Vol. 09-No. 12, November 2010, 11-15.

[17] Nishu Garg, R.P. Mahapatra, "MANET Security Issues", International Journal of Computer Science and Network Security", Vol. 09, No.08, August 2009, 241-246.

[18] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshika Nemoto, and Nei Kato, "A Survey of Routing Attacks in Mobile Ad hoc Networka", IEEE wireless communications, October 2007, 85-91.

[19] Jun-Zhao Sun, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing", Info-Tech and Info-net, 2001. Proceedings. ICII 2001-Beijing.2001 International conference, 2001, Vol. No. 03, 316-321.