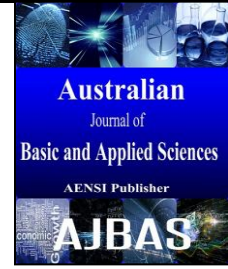




ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com



A Survey on Attacks in Wireless Networks

¹J.Martin Leo Manickam and ²D.Muruganandam

¹Department of Electronics and Communication Engineering St.Joseph's College of Engineering Chennai, India

²Department of Computer Science and Engineering University College of Engineering Panruti Cuddalore, India

ARTICLE INFO

Article history:

Article Received 12 January 2015

Revised 1 May 2015

Accepted 8 May 2015

Keywords:

Ad-Hoc network, Security threat, Routing protocol, Active and passive attack.

ABSTRACT

Wireless networks are gaining popularity to its peak today, as the users want connectivity in terms of wireless medium irrespective of their geographic position. The wireless networks can be categorized into two types: Infrastructure and Ad-hoc mode. An ad-hoc network is a formed group of nodes which can communicate with each other without any infrastructure. So, the attacker can easy be possible to attacks. There is an increasing threat and various attacks on the Wireless Network. The attacks ad-hoc networks are divided into two parts: passive and active attacks. The main aim of this paper is to provide a survey of wireless attacks in MANET and we will also be discussing the presently methods of those attacks.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: J.Martin Leo Manickam and D.Muruganandam., A Survey on Attacks in Wireless Networks. *Aust. J. Basic & Appl. Sci.*, 9(21): 72-78, 2015

INTRODUCTION

Communications being a mode of sending and receiving information is gaining more popularity in today's world. There are various modes of communication one of them is wireless mode; in which communication takes place through an open medium. There are various types of wireless networks. These are cellular networks, satellite networks and ad hoc mobile networks. Amongst the wireless networks 802.11 networks are the most popular. Wireless 802.11 networks can be categorized into two types: Infrastructure and Ad-hoc mode. Infrastructure based networks have a fix backbone. An ad-hoc network is a group of mobile nodes which can communicate with each other without any infrastructure. Wireless medium is a medium which can be accessed by both legitimate users and attackers. End users and corporations are heavily interested in taking the advantage of this wireless medium (Ankur Bawiskar, Dr. B.B. Meshram, 2013).

Adhoc Network:

Wireless LANs can be classified based on their mode of operation such as either infrastructure or ad-hoc. Infrastructure mode has a fixed wired backbone for communicating with each other; whereas the ad-hoc mode doesn't rely on a backbone.

Security is an indispensable need for both wired and wireless network communications. Unlike wired

networks, wireless networks pose a number of challenges to security solutions due to their unpredictable topology; wireless shared medium, heterogeneous resources and stringent resource constraints etc. There are a wide variety of attacks that target the weakness of this kind of network. In this type of network, security is not a single layer issue but a multilayered one. We have focused on network layer where the possible attacks are most vulnerable. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

Confidentiality:

Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediates nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

Availability:

Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can

Corresponding Author: J.Martin Leo Manickam, Department of Electronics and Communication Engineering St.Joseph's College of Engineering Chennai, India
E-mail: josephmartin_74@yahoo.co.in

disrupt the routing protocol. On higher layers, the attacker could bring down high level services.

Authentication:

Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

Integrity:

Message being transmitted is never altered.

Non-repudiation:

Ensures that sending and receiving parties can never deny ever sending or receiving the message.

A. Ad-hoc Network Characteristics:

An ad hoc network can be formed when a group of mobile devices communicate with each other without depending on any fixed infrastructure (Ahed M. Alshanyour, Uthman Baroudi, 2008). In such cases, neighboring nodes communicate with each other while communication between non-neighbor nodes is performed via the intermediate nodes that can act as routers. The network topology also frequently changes in ad-hoc network. Ad-hoc wireless networks are prone to route breaks that can result due to various sources such as node mobility, signal interference, high error rate and packet collision (Ahed M. Alshanyour, Uthman Baroudi, 2008).

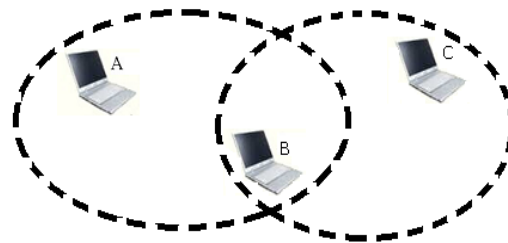


Fig. 1: Ad-hoc network

The above figure 1 explains the ad-hoc network wherein there are three nodes A,B and C. Node A and Node B are in the range of each other. Similarly node B and C are in range of each other. If node A wants to send some data to node C it has to pass through the intermediate node b so node B acts as a router. Here comes the main operation of routing in ad-hoc network.

B. Routing in Ad-hoc network:

Routing in an ad-hoc network is the most important task that needs to be handled with care. Since nodes in ad-hoc network depend on intermediate nodes in carrying of the data so there are various routing protocols used in this process. The main aim of routing protocols in an ad-hoc network is to find minimum hop distance between source and destination with minimum overhead and bandwidth (Amol, A., *et al.*, 2012). Depending on the routing topology being used they are classified as : proactive, reactive and hybrid.

Proactive Protocols:

In proactive protocol each node present in the network has information of complete topology (Amol, A., *et al.*, 2012). The tables are updated constantly so that they contain fresh enough information for routing.

Reactive Protocols:

In reactive protocol nodes create path on an on-demand basis. Information about the network topology is collected only when it is required. This avoids the overhead associated with frequent updating of routing table in each node in the network (Amol, A., *et al.*, 2012).

Hybrid Protocols:

In hybrid protocols group of nodes are formed and then the nodes are assigned different functionalities inside and outside of the group. Grouping is done based on position of nodes (Amol, A., *et al.*, 2012).

I. Attacks in Wireless Manet:

The attacks on the MANETs are divided into two parts. The Fig 2 explains about passive and active attacks. Both passive and active attacks can be present in layers of the network protocol stack (Siva Ram Murthy, C. and B.S. Manoj, 2006).

II. Passive Attacks:

A passive attack doesn't affect in the normal operation of the network; the attacks in terms of the number of messages the attacker must insert into the network and the time he must spend. Detection of passive attack is very complexity since the operation of the network itself doesn't get affected. There are some attacks are; Eves dropping, Traffic analysis, monitoring.

A.Eavesdropping:

Eavesdropping is a passive attack, which occurred in the mobile ad-hoc network. The aim of eavesdropping is to find some secret or confidential information that should be kept secret during the communication. This confidential information may be private or public key of sender or receiver or any password.

B.Traffic Analysis:

In this type of attack, an attacker tries to sense the communication path between the sender and receiver. This way attacker found the amount of data which is travel between the route of sender and receiver. There is no alteration in data by the traffic analysis.

C.Monitoring:

Monitoring is a passive attack in which attacker can see the confidential data, but he cannot change the data or cannot modify the data.

III. Active Attacks:

An Active attack always tries to modify the normal operation of MANET, which means the interruptions have been made in the network, such as doing data interruption, modification, deletion and fabrication. Active attacks can be internal or external. The information which is routing through the nodes in MANET is altered by an attacker node. Attacker node also streams some false information in the network. Attacker node also do the task of route request though it is not authenticated node so the other node rejecting its request due to these route requests the bandwidth is consumed and network is jammed (Solomon Abel, V., 2011). Some of the security threats in the networks are Interruption, Interception and Modification. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks (Sahadevaiah, K., P.V.G.D. Prasad Reddy, 2011).

The names of some active attacks are,

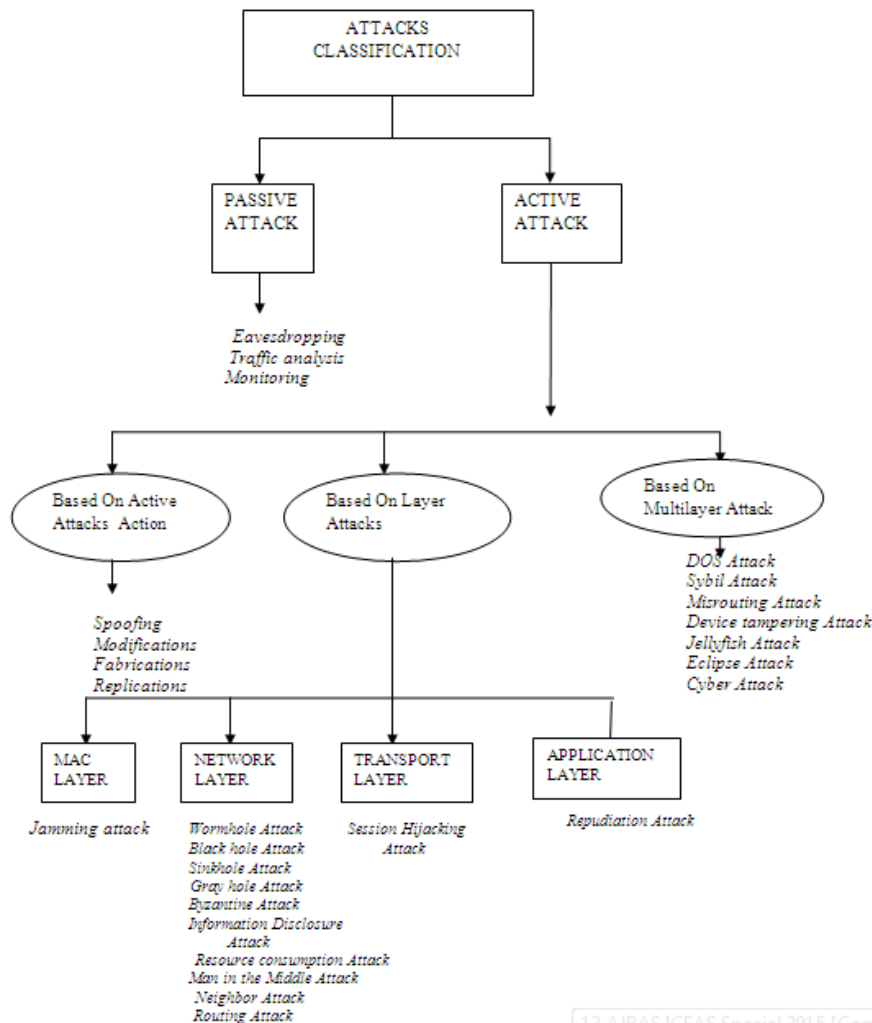


Fig. 2: Classification of Attacks

A. Based On Active Attacks Action:

Active attacks involve actions are present in the some attacks, there are: Spoofing, Modification, Fabrications and Replications attacks

a) *Spoofing* - When a malicious node misrepresent his identity, so this way it can alter the vision of sender and sender change the topology (Kuldeep Sharma, Neha Khandelwal, M. Prabhakar).

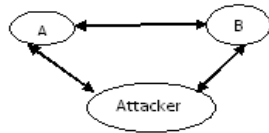


Fig. 3: Spoofing Attack

b) *Modification* - Malicious node performs some modification in the routing, so that sender sends the message through the long route which causes time delay and communication delay. This is occurred between sender and receiver.

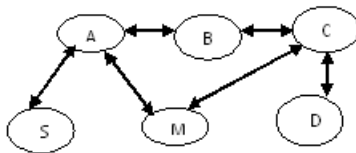


Fig. 4: Modification Attack

c) *Fabrication* - When a malicious node generates the false routing message. This means malicious node generate the incorrect information about the route between devices (Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, 2006).

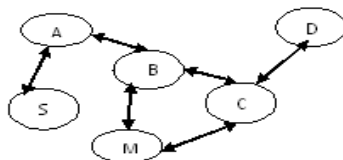


Fig. 5: Fabrication Attack

d) *Replication attack* - It is a network attack in which a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and retransmit it. Suppose node S want to send some data to D. For this S has to prove his identity to R. This way S sends his password to R. This way S sends his password to R for identification. At that time, an attacker intercept the password of S and a presenting itself as S, when asked for the proof of identity. A sends S password read from the last session, which D accepts (Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay).

B. Based On Layer Attacks:

The active attacks are present the layers are: MAC layer, Network layer, transport layer, application layer.

a) *Jamming Attack* - It is MAC layer attacks Jamming is the particular class of DoS attacks. Jamming attacks can severely interface with the normal operation of the wireless communications. A jammer can attack a packet before a real traffic source from sending out, or before receiving a packet (Siva Ram Murthy, C. and B.S. Manoj, 2006).

b) *Wormhole Attack* - Wormhole attack is also called the tunneling attack. An attacker receives a packet at one point and tunnels it to another innocent malicious node in the network. This way longer assumes that he found the shortest path in the network. This wrong path between two colluding attackers is called the wormhole (Ali Ghaffari, 2006).

c) *Black Hole Attack* - Black hole attack is an active attack type, which leads to dropping of messages. In this type of attack, malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives a RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself. This black hole node assigns a high sequence number to settle in the routing table of the victim node and sends before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over the malicious node. In the same manner the malicious node attacks all RREQ messages and takes over all routes. Therefore all packets are sent to black hole node. The black hole node without forwarding the packets to the destination discards them. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network. In this way a black hole node can affects the whole network (Yi-Chun Hu and Adrian Perrig, 2004).

d) *Sinkhole Attack* - In this attack, the adversary's goal is to attract all the virtual traffic from a specific area through a compromised node, creating a symbolic sinkhole with the opponent at the center as nodes on or near the path those packets follow have many opportunities to interfere with data (Solomon Abel, V., 2011).

e) *Gray Hole Attack* - It is an active attack type, which leads to dropping of messages. Attacking node first agrees to forward the packets and then fails to do so. Initially the attacker node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets. If neighboring nodes (that try to send packets over attacking nodes) lose the connection to destination then they may want to discover a route again,

broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption) (Jaydip Sen, M *et al.*, 2007).

f) *Byzantine Attack* - A compromised intermediate node work alone or a set of compromised intermediate node works between the sender and receiver and perform some changes such as creating routing loops, forwarding packet through non-optimal path or selectively dropping packet, which result in disruption or degradation of routing services (Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, 2006; Awerbuch, B., *et al.*, 2002).

g) *Information Disclosure Attack* - In this type of attack, Malicious nodes are collects the information about the nodes and about the routing path by computing and monitoring the traffic. This way malicious node may perform more attack on the network (Manikandan, K.P., *et al.*, 2011).

h) *Resource Consumption Attack* - In this attack, a malicious node intentionally tries to consume or misuse of the resources (battery power, bandwidth, and computational power) of other nodes' exist in the networks by requesting unnecessary route messages or forwarding unnecessary packets to that node (Siva Ram Murthy, C. and B.S. Manoj, 2006).

i) *Man-In-The-Middle Attack* - In Man in Middle attack, the attacker node creeps into a valid route and tries to sniff packets flowing through it. To perform man in middle attack, the attacker first needs to be part of that route. It can do that by either temporarily disrupting the route by deregistering a node by sending malicious disassociation beacon captured previously or registering itself in next route timeout event (Gandhi, C. and M. Dave, 2006).

j) *Neighbor Attack* - In this attack to disrupt multicast routes by making two nodes that are in fact out of communication range believe that they can communicate directly with each other. Neighbors are usually defined a nodes that lie within radio range of each other's. (Yi-Chun Hu and Adrian Perrig, 2004).

k) *Routing Attacks* - In this attack, an attacker comes between the route of sender and receiver. When sender send packet to the receiver, then attacker intercept the packet and forward to receiver. Attacker performs duplicate suppression mechanism and then sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so that receiver will be busy continuously. This way, it reduces the efficiency of receiver (Siva Ram Murthy, C. and B.S. Manoj, 2006).

l) *Stealth Attacks* - Stealth attacks with a high cost for the attacker, and with a high visibility. Therefore, only powerful and dedicated attackers would have any hope of succeeding with such attacks for any extended period of time. However, as we will show, there are other attacks with lower cost and

visibility, but which are at least as harmful as brute force attacks. These allow a skilled but not very powerful attacker to target communication networks in a way that makes it unlikely that he gets traced and caught. Some stealthy attacks are misrouting, power control, colluding and collision, identity delegation (Jakobsson, M., S. Wetzel and B. Yener, 2003).

m) *Session Hijacking Attack* - This type of attacks at present in the transport layer here, an adversary between two nodes takes control over a session. Once the session gets known between two nodes, the misbehaving node covers up at end node of the session and takes control over the session (Siva Ram Murthy, C. and B.S. Manoj, 2006).

n) *Repudiation Attack* - In this attack, this is by passed by attacker from transport layer and network layer. Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks. For example, spyware detection software has been developed in order to monitor mission critical services ((Siva Ram Murthy, C. and B.S. Manoj, 2006)).

C. Based On Multi Layer Attacks:

The multilayer attacks are involves all the layers there are,

a) *Denial of Service Attack* - In this type of attack, malicious node sending the message to the node and consume the bandwidth of the network. The aim of malicious node is to be busy to the network node. This way, if a message from the authorized node will come, then receiver will not receive the message because he is busy and beginner has to wait for the receiver response. (Aad, I., *et al.*, 2004).

b) *Sybil Attack* - Sybil attack refers to the multiple copies of malicious nodes. It can be happen, if the malicious node shares its secret key with other malicious nodes. This way the number of malicious node is increased in the network and the probability of the attack is also increased. If we use the multipath routing, then the possibility of choosing a path in the network, those contain the malicious node will be increased (Douceur, J., 2002).

c) *Misrouting Attack* - This attack is also known as manipulation of network traffic attack. This is a very simple one compromised node in the wrong route between the sender and receiver. In the misrouting attack, the packet is received in wrong next hop (Sanzgiri, K., *et al*, 2002).

d) *Device Tampering Attack* - In this attack is a physical layer attack. A node in ad-hoc wireless network is small, dense and hand-held dissimilar wired device so can be easily stolen or damaged by an opponent (Siva Ram Murthy, C. and B.S. Manoj, 2006).

e) *Jellyfish Attack* - A jellyfish attacks as more than malicious nodes intrude into forward to group of network and then it unwanted delays data packets for the some amount of time before forwarding them. This results high end-to-end delays and, thus, degrades the real-time applications performance (Aad, I., *et al.*, 2004).

f) *Eclipse Attack* - In this attack, some pattern of misbehavior called an *eclipse* attack, which consists of the geographic positioning of the good uncompromised nodes' routing tables with links to compromised nodes [5].

g) *Cyber Attack*-The complexity has also been increasing threats are called cyber attacks. These attacks are used to spread misinformation, cripple tactical services, access sensitive information, espionage, data theft and financial losses. The cyber attacks are classified: Cyber Crime, Cyber Espionage, Cyber Terrorism, and Cyber war (Shimeall, T., 2002).

Conclusion:

Wireless networks are gaining more and more popularity in today's world because of their many benefits and applications. Because wireless communication use open medium for sending and receiving data they are more susceptible to attack. Wireless ad-hoc networks have more security threats as they solely rely on the nodes present in the network. Routing is an important issue that needs to be handled with care in ad-hoc network. In this paper we have discussed A survey on attacks in wireless and ad-hoc network. We can understand of wireless ad-hoc network and also attacks occurring on them.

ACKNOWLEDGMENT

The authors would like to acknowledge and thank their parents, god and all the human being with great heart for their support and encouragement as well.

REFERENCES

Ankur Bawiskar, Dr. B.B. Meshram, 2013. "Survey of Attacks on Wireless Network" International Journal of Innovative Research in Computer and Communication Engineering, 1: 1.

Ahed M. Alshanyour, Uthman Baroudi, 2008. "Bypass AODV: Improving Performance of Ad Hoc On- Demand Distance Vector (AODV) Routing Protocol in Wireless Ad Hoc Networks", Paper Published in ICST and Ambi-sys.

Amol, A., Bhosle, Tushar P. Thosar and Snehal Mehatre, 2012." Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA, 2(1): 45-54.

Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay, "Different Types of Attacks

on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) (4): 3.

Yi-Chun Hu and Adrian Perrig, 2004."A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, 2(3): 28-39.

Solomon Abel, V., 2011. "Survey of Attacks on Mobile Ad- Hoc Network" IJCSE, 3: 2.

Manikandan, K.P., Dr.R. Satyaprasad, Dr.K. Rajasekhararao, 2011."A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks", International Journal of Advanced Computer Science and Applications, 2: 3.

Gandhi, C. and M. Dave, 2006."A Review of Security in Mobile Ad Hoc Networks", IETE Technical Review, ISSN: 02564602, 23(6): 35-344.

Sahadevaiah, K., P.V.G.D. Prasad Reddy, 2011. "Network Protocols and Algorithms" ISSN 1943-3581, 3: 4.

Ali Ghaffari, 2006. "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, 22-24.

Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy and P. Balamuralidhar, 2007."A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", Proceedings of IEEE 6th International Conference on Information, Communications and Signal Processing, pp: 1-5.

Jakobsson, M., S. Wetzel and B. Yener, 2003. "Stealth Attacks on Ad Hoc Wireless Networks", Proceedings of IEEE 58th Vehicular Technology Conference, 3: 2103-2111.

Douceur, J., 2002. "The Sybil Attack", Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), pp: 251-260.

Sanzgiri, K., B. Dahill, B.N. Levine, C. Shields and E.M. Belding-Royer, 2002. "A Secure Routing Protocol for Ad hoc Networks", Proceedings of 10th IEEE International Conference on Network Protocols(ICNP2002), pp.78-87.

Aad, I., J.P. Hubaux and E.W. Knightly, 2004. "Denial of Service Resilience in Ad Hoc Networks", Proceedings of the ACM 10th Annual International Conference (MobiCom- 2004), Philadelphia, PA.

Shimeall, T., 2002. *Cyberterrorism*, Software Engineering Institution Carnegie Mellon University Pittsburg, pp: 1-18.

Siva Ram Murthy, C. and B.S. Manoj, 2006."Ad Hoc Wireless Networks: Architectures and Protocols", Pearson Education, ISBN: 978-81-317-0688-6.

Kuldeep Sharma, Neha Khandelwal, M. Prabhakar, "An Overview Of security Problems in MANET".

Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, 2006. "A survey on attacks and countermeasures in mobile ad hoc networks.

Awerbuch, B., D. Holmer, C. Nita-Rotaru and H. Rubens, 2002. "An On-Demand Secure Routing Protocol Resilient to Byzantine failures", Proceedings of 1st ACM Workshop on Wireless

Security (WiSe'02), ISBN: 1-58113-585-8, pp: 10, NY, USA.

Stallings, W., 2010. "Cryptography and Network Security: Principles and Practice", Fifth Edition, Prentice Hall.