International Journal of Multidisciplinary and Current Research

General Article

ISSN: 2321-3124
Available at: http://ijmcr.com

Security in MANET: Vulnerabilities, Attacks & Solutions

Sachin Lalar

Department of Computer Science & Engg., TERI, Kurukshetra

Accepted 30 December 2013, Available online 10 January 2014, **Vol.2 (Jan/Feb 2014 issue)**

Abstract

A MANET is an infrastructure-less type network, which consists of number of mobile nodes with wireless network interfaces. In MANET nodes can directly communicate to all other nodes within the radio communication range. If a node could not have direct communication then they can use intermediate nodes to communicate with other nodes. Though each node in MANET will act as host as well as router, the security is a major issue and the chances of having the vulnerabilities are also more In this paper we discuss various types of vulnerabilities in MANET. Different types of attacker attempts different approaches to decrease the network performance, throughput. In this paper the principal focus is on routing and security issues associated with mobile ad hoc networks which are required in order to provide secure communication.

Keywords: *MANET, Security, vulnerabilities, Attacks, Solutions*

1. Introduction

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. Mobile ad hoc networks are collection of wireless networks, which consists of large number of mobile nodes. Nodes in MANETs can join and leave the network dynamically. There is no fixed set of infrastructure and centralized administration in this type of networks. Nodes are interconnected through wireless interface. The dynamic nature of such type networks makes it highly susceptible to various link attacks. The basic requirements for a secured networking are secure protocols which ensure the confidentiality, availability, authenticity, integrity of network. Many existing security solutions for wired networks are ineffective and inefficient for MANET environment. As the transmission takes place in open medium makes the MANETs more vulnerable to security attacks. In the presence of security protocol affect of various attacks can be reduced. The mobile hosts dynamically establish paths among one another in order to communicate. Therefore, the success of MANET communication highly relies on the collaboration of the involved mobile nodes [1].

Such dynamism of MANET-based architectures leads to some inherent weaknesses and a wide variety of attacks target these weaknesses. In this paper, we discuss some of the existing malicious attacks against MANETs and also the solutions to defend against them.

2. Security Goals

Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

2.1 Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

2.2 Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.

2.3 Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.

2.4 Authentication: Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators.

Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.

2.5 Non repudiation: Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

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

2.7 Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

3. MANET Vulnerabilities

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

3.1 Lack of centralized management: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

3.2 Resource availability: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

3.3 Scalability: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

3.4 Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

3.5 Dynamic topology: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

3.6 Limited power supply: The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

3.7Bandwidth constraint: Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

3.8 Adversary inside the Network: The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

3.9 No predefined Boundary: In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node. The attacks include Eavesdropping impersonation; tempering, replay and Denial of Service (DoS) attack [Mishra].

4. Attacks in MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information[Hass et al].Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

1. External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

2. Internal Attack: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious that is part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

4.1 Denial of Service attack: This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

4.2 Impersonation: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

4.3 Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

4.4 Routing Attacks: The malicious node make routing services a target because it's an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

4.5 Black hole Attack:: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it[Broch et al]. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

4.6 Wormhole Attack: In a wormhole 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. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

4.7. Replay Attack: An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

4.8 Jamming: In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

4.9 Man- in- the- middle attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

4.10 Gray-hole attack: This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

5. Routing Protocols

Routing is the most fundamental research issue in MANET and must deal with limitations such as high power consumption, low bandwidth, high error rates and unpredictable movements of nodes. Generally, current routing protocols for MANET can be categorized as:

5.1 Proactive (Table-Driven): The pro-active routing protocols [Royer et al] are the same as current Internet routing protocols such as the RIP(Routing Information Protocol), DV(distance-vector), OSPF (Open Shortest Path First) and link-state . They attempt to maintain consistent, up-to-date routing information of the whole network. Each node has to maintain one or more tables to store routing information, and response to changes in network topology by broadcasting and propagating. Some of the existing pro-active ad hoc routing protocols are: DSDV (Destination Sequenced Distance-Vector, 1994), WRP (Wireless Routing Protocol, 1996), CGSR (Cluster head Gateway Switch Routing, 1997), GSR (Global State Routing, 1998), FSR (Fisheye State Routing, 1999), HSR (Hierarchical State Routing, 1999), ZHLS (Zone based Hierarchical Link State,1999),STAR (Source Tree Adaptive Routing, 2000).

5.2 Reactive (Source-Initiated On-Demand Driven): These protocols try to eliminate the conventional routing tables and consequently reduce the need for updating these tables to track changes in the network topology. When a source requires to a destination, it has to establish a route by route discovery procedure, maintain it by some form of route maintenance procedure until either the route is no longer desired or it becomes inaccessible, and finally tear down it by route deletion procedure. Some of the existing re-active routing protocols are [Frodigh et al][Royer et al].DSR (Dynamic Source Routing, 1996), ABR (Associativity Based Routing, 1996), TORA (Temporally-Ordered Routing Algorithm, 1997), SSR (Signal Stability Routing, 1997), PAR (Power-Aware Routing,1998), LAR (Location Aided Routing, 1998), CBR (Cluster Based Routing, 1999), AODV (ad hoc On-Demand Distance Vector Routing, 1999). In pro-active routing protocols, routes are always available (regardless of need), with the consumption of signaling traffic and power. On the other hand, being more efficient at signaling and power consumption, re-active protocols suffer longer delay while route discovery. Both categories of routing protocols have been improving g to be more scalable, secure, and to support higher quality of service**.**

5.3 Hybrid Protocols: Hybrid routing protocols [Frodigh et al] aggregates a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used. Consequently, in hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones. The zone routing protocol (ZRP) and zone-based hierarchical link state (ZHLS) routing protocol provide a compromise on scalability issue in relation to the frequency of end-to-end

connection, the total number of nodes, and the frequency of topology change. Furthermore, these protocols can provide a better trade-off between communication overhead and delay, but this trade-off is subjected to the size of a zone and the dynamics of a zone. Thus, the hybrid approach is an appropriate candidate for routing in a large network. At network layer, routing protocols are used to find route for transmission of packets. The merit of a routing protocol can be analyzed through metrics-both qualitative and quantitative with which to measure its suitability and performance. These metrics should be independent of any given routing protocol. Desirable qualitative properties of MANET are Distributed operation, Loop-freedom, Demand-based operation, Proactive operation, Security, Sleep period operation and unidirectional link support. Some quantitative metrics that can be used to assess the performance of any routing protocol are End-to-end delay, throughput, Route Acquisition Time, Percentage Out-of-Order Delivery and Efficiency. Essential parameters that should be varied include: Network size, Network connectivity, Topological rate of change, Link capacity, Fraction of unidirectional links, Traffic patterns, Mobility, Fraction and frequency of sleeping nodes [Broch et al][Perkins et al].

6. Routing Attacks

Generally, there are four different types of MANET routing protocol attacks which is divided in to two main types which are given below [Kimaya et al][Huang et al]:

1. Routing disruption attacks
2. Resource consumption attacks

In case of routing disruption attacks, the main task of attacker is to disrupt routing process by routing packets in order to introduce wrong paths. In case of resource consumption attacks are concerned the main task of the attacker is to introduce some non-cooperative or selfish nodes that can be used to inject false packets due to this way load on the network increases and it will become a cause of consuming network bandwidth.

Mainly both of these attacks in MANET routing protocols are the best examples of Denial of Service (DoS) attacks. In Figure 1, there is a broader classification attacks in MANET routing protocols which are given below.

6.1 Attacks using Modification: In case of modification type of attacks some of the messages in the protocol fields are modified and then these messages passed among the nodes, due to this way it becomes the cause of traffic subversion, as well as traffic redirection and also act as a Denial of Service (DoS) attacks. There are some of these types of attacks are given below:

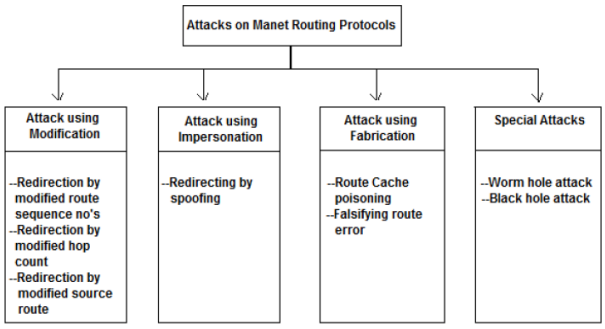

Figure 1: Classification of attacks on MANET routing protocols

6.1.1 Route sequence numbers modification :In this type of attack which is mainly possible against the AODV protocol. In this case an attacker (i.e. malicious node) used to modify the sequence number in the route request packets.

6.1.2 Hop count modification attack:In this type of attacks where it is also mainly possible against the routing protocol AODV, here attacker mostly change hope count value and due to this way it will become the cause of attract traffic. They are mainly used to include new routes in order to reset the value of hop count field to a lower value of a RREQ packet or sometime even it is used to set to zero.

6.1.3 Source route modification attack :In this type of attack which is possible against DSR routing protocol where attacker (malicious node) modify source address and move traffic towards its own destination. In Figure 2 the mechanism is defined, where the shortest path between source S and destination X is defined (S-A-B-C-D-X). Which shows that node S and the node X cannot communicate each other directly, and in the scenario (Fig. 2) where the node M which act as a malicious node which are going to attempt a denial-of-service attack. Let suppose that the node S which act as a source try to send a data packet towards the node X but if the node M intercept the packet and remove the node D from the list and the packet forward towards node C, where the node C will try to send the picket towards the distention X which is not possible because the node C can't communicate with X directly, Due to this way the M node has successfully established a DoS attack on X.

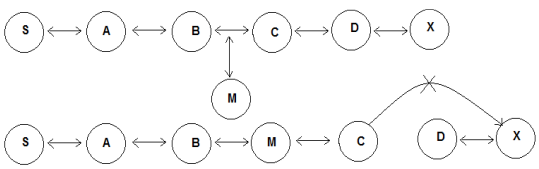

Figure 2: An example of route modification attack

6.1.4 Attacks using Impersonation: In this type of attacks where attacker is used to violates authenticity and confidentiality of a network. In this attack an attacker (i.e. malicious node) uses to impersonate the address of other

user node in order to change the network topology. This type of attack can be described in the Figure 3 given below:

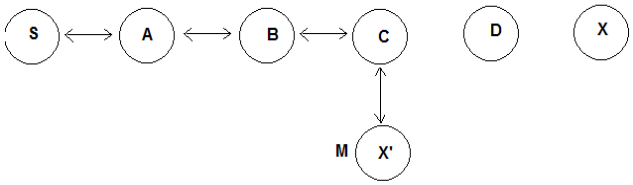

Figure 3: Type of impersonation attack

In the above figure where the S node wants to send data towards the node X and before sending data to node X it starts a Route Discovery process. During route discovery process there is a malicious node M, when it receive route discovery packet regarding the node X then it modify its address and change to node X, like impersonates node X as X'. After that it send packet back to source node S that I am the destination node by RREP packet request. When the source node receives RREP packet information it doesn't authenticate node and accept the route and send data to the malicious node. This type of attacks also called routing loop attack which will become the cause of loops within the network.

6.3 Attacks using Fabrication: In this type of attacks, where an attacker as a malicious node try to inject wrong messages or fake routing packets in order to disrupt the routing process. The fabrication attacks are very much difficult to detect in the mobile ad hoc network. Attacks using fabrication process are discussed very well in [Karygiannis et al] and [Sadawarti et al]. In Figure 4, where fabrication attacks is explained by an example. In the example where the source node S wants to send data towards the destination node X, so therefore at start it sends broadcast message and request for route towards the destination node X. An attacker as a malicious node M try to pretends and modify route and returns route reply to the node (S). Furthermore, an attacker's nodes use to fabricate RERR requests and advertise a link break nodes in a mobile ad hoc network by using AODV or DSR routing protocols.

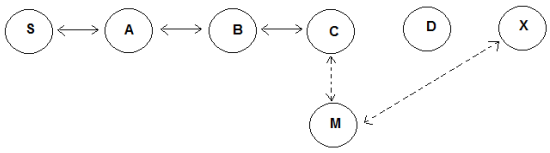

Figure 4: Fabrication attack example

6.4 Special Attacks: There are also some other severe attacks in MANET network which are possible against routing protocols such as AODV and DSR.

6.4.1 Wormhole Attack: The wormhole attack [HU et al] is one of the severe types of attack in which an attacker introduces two malicious nodes in the network where an attacker used to forward packets through a private "tunnel". This complete scenario described in Figure 5 which is given below:

6.4.2 Black hole attack :This kind of attack is described very well in detail in [Sadawarti et al]. In this type of attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to shares their routing tables among each other.

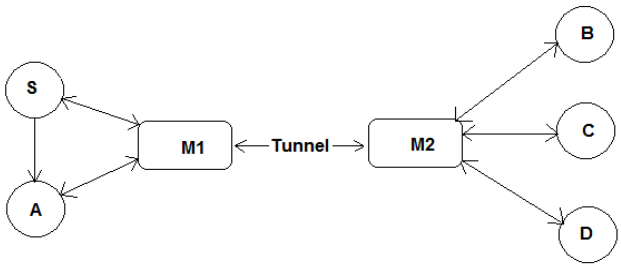

Figure 5: Wormhole attack example

In the above example where there are two malicious nodes M1 and M2 which link through a private connection. In this type of attack every packet which an attacker receive from network 1 forward to other network where another malicious node exist, simple speaking these two nodes use to exchange network information and fabricate traffic among each other. The traffic between the two nodes passes through "wormhole" among each other. Due to this way it will become the cause of disrupts routing protocols and violating normal flow of routing packets. These types of attacks are very difficult to detect in a network, and become the cause of severe damages to the nodes. These types of attacks can be prevented by using mechanism packet leashes, which are used to authenticate nodes among each other by timing information process.

7. Security solutions to avoid Attacks in MANET

7.1 Secure Multicasting :Multicast is a mechanism where any user become the part of multicast group and even send traffic to the multicast users as well as receive traffic, but due to this procedure it can easily fall into denial of service attacks (DoS). There is an architecture usually used to secure multicast traffic that is DIPLOMA. DIPLOMA stands for Distributed Policy enforcement Architecture which is use to protect or secure end user services as well as network bandwidth. Audio and video traffic usually fall into the category of multicast traffic which is usually use by militaries as well as disaster backup plans (teams). There are some of the major responsibilities of DIPLOMA architecture which are given below [Alicherry and Keromytis].

- It gives solution for both sender and receiver whenever they access to the multicast group.
- It also used to limit the bandwidth.
- DIPLOMA integrates with common multicasting routing protocols like PIM-SM and ODMRP.
- It also uses to provide (allocate) network resources in a fair manner during attacks.

7.2 Secure routing: MANET is a self-organized wireless network, due to the fact it has vulnerable attacks that can easily damage the whole network; that's why there should be some solutions which works even some of the mobile nodes compromised in the network. One of the primary challenges of secure routing is to provide authentication (trustworthiness) of users in the network. In case of distributed communication environment in MANET, authentication is open and any un-authentic node may be use to compromise routing traffic in order to disrupt the communication. There are some of the major responsibilities of secure routing which are given below.

- It provides assurance that modified and replayed route replies should be rejected in order to avoid fabrication of attacks.
- Routing protocol responsiveness itself provide safety among different routing attacks.

7.3 Privacy-aware and Position based Routing :MANET is a kind of wireless network in which mobile nodes move from one station to another. In this type of network environment routing process among different nodes is important that's why privacy-aware and position based routing is used to avoid route overhead. In case of position based routing mechanism, a mobile node within the MANET network broadcast its position co-ordinates as well as its one-hop neighbors. This information can easily be attacked, so therefore privacy-aware mechanism is together with position based routing in order to provide secure communication. PPBR stands for privacy aware and position based routing in which a mobile node mainly takes pseudo identifiers that are usually dynamic and it is also use to provide end-to-end inconspicuousness to other nodes.

7.4 Key management: Certified Authority (CA) is one of the mechanisms which provide key management; if it is compromised then entire network can easily be damaged. One of the major functionality of key management and distribution for MANET, it provide solutions for mobility related issues. In section [Biswas et al] writers discuss different aspect of key management and distribution for MANET. In the paper, the approach for key management use to solve high mobility issue as well as it provide an efficient method to reduce control overhead also gives an idea how to increase reliability in key management with respect to conventional key management process.

7.5 Intrusion detection System: Intrusion detection system is a complete security solution which provides information about malicious activities in the network, it also uses to detect and report about malicious activities. MANET is also design for route traffic mechanism when there is congestion in the network, faulty nodes as well as topology changes due to its dynamic behavior. IDS use to detect critical nodes and then analyze its data traffic, critical node also degrade network performance. There are different IDS systems which has some specific features, some of them are given blow

- Cluster based voting
- Neighbor-monitoring
- Trust building For detail description of these IDS system see section [Kimaya et al].

7.6 Multi-layer Intrusion detection technique: Multi-layer intrusion detection technique is a technique in which an attacker attacks at multiple layers in order to stay below the detection threshold so that they will escape easily whenever a single layer impropriety detects. These type of attacks mainly attack at cross layer which are more alarming and frightening as compare to single layer attack and they can easily be escaped. Although these type of attacks can be detected by a multiple layer insubordination detector, where with respect to all network layer's input are use to combine and examine by the cross-layer detector in a detailed fashion. There is also another way to detect these kinds of attacks by working together with RTS/CTS and network layer detection with respect to dropped packets.

Conclusion

The future of ad- hoc networks is really appealing, giving the vision of—anytime, anywhere and cheap communications.

In this survey paper, we try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind 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 wired networks.

References

[1] Ilyas, M., 2003. The hand book of ad -hoc wireless networks. CRC press LLC.

[2] A Mishra and K.M Nadkarni, security in wireless Ad -hoc network, in Book. The Hand book of Ad Hoc Wireless Networks (chapter 30), CRC press LLC, 2003.

[3] Jie Wu , Fei Dai (2003),—Broadcasting in Ad Hoc Networks: Based on Self-Pruning, Twenty Second Annual Joint Conferences of IEEE Computer and Communication Societies, IEEE INFOCOM 2003

[4] P. Papadimitrates and Z.J. Hass(Jan 2002), secure Routing for mobile Ad Hoc Networks in proceeding of SCS Communication Networks and Distributed system modelling and simulation Conference (CNDS), San Antonio, TX.

[5] Y.Hu, A Perrig and D. Johnson, Ariadne(2002): A secure On-demand Routing Protocol for Ad Hoc Networks, in Proceeding of ACM MOBICOM'02.

[6] K. Sanzgiri, B. Dahill, B.N. Levine, C. shield and E.M Belding(2002)- Royar, A secure routing protocol for Ad Hoc Networks, in Proceedings of ICNP'02.

[7] Y. Hu, D. Johnson and A Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wire.

[8] D. Johnson and D. Maltz(1996) —Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer.

[9] Broch,J., A.M David and B. David(1998), A Performance comparison of multi-hop wireless ad hoc network routing protocols. Proc.IEEE/ACM MOBICOM'98, pp: 85-97.
[10] C.E.Perkins and P. Bhagwat(Oct 1994) —Highly dynamic destination-sequenced distance vector routing for mobile computers‖, Comp, Comm. Rev., pp 234-44
[11] Belding-Royer,E.M. and C.K. Toh, (1999). A review of current routing protocols for ad-hoc mobile wireless networks.IEEE Personal Communication magazine pp:46-55.
[12] M. Frodigh, P. Johansson, and P. Larsson(2000)—Wireless ad hoc networking: the art of networking without a network,Ericsson Review,No.4, pp. 248-263.
[13] Magnus Frodigh, Per Johansson and Peter Larsson. Wireless ad hoc networking— The art of networking without a network.
[14] E. M. Royer and C-K Toh , —A review of Current routing protocols for Ad Hoc Mobile Wireless.
[15] Chlamtac, I., Conti, M., and Liu, J. J.-N.(2003), Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), pp. 13–6.
[16] HaoYang, Haiyun & Fan Ye (Feb 2004)— Security in mobile ad-hoc networks : Challenges and solutions,Pg. 38-47, Vol 11, issue 1.
[17].Karygiannis, A.; Antonakakis, E.; Apostolopoulos, A.(2006),Detecting critical nodes for MANET intrusion detection systems, Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. Second International Workshop, vol., no., pp.9 pp.-15, doi: 10.1109/SECPERU.2006.8
[18] Anuj K. Gupta, Member, IACSIT, Dr. Harsh Sadawarti, Dr. Anil K. Verma (April 2002), Performance analysis of AODV, DSR & TORA Routing Protocols ,IACSIT International Journal of Engineering and Technology, Vol.2, No.2,ISSN: 1793-8236 .
[19] Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer(Nov 2002),*A Secure Routing Protocol for Ad Hoc Networks*. Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, pp. 78-90.
[20] Yi-an Huang and Wenke Lee(September 2004) ,*Attack analysis and Detection for Ad-hoc Routing protocol*. Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera, France.
[21] Y. Hu, A. Perrig, D. Johnson (March 2003),*Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks*. Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003).
[22] M. Alicherry and A.D. Keromytis,(2010),Securing MANET Multicast Using DIPLOMA, in Proc. IWSEC, pp.232-250.
[23] Biswas, J.; Nandy, S.K.(2006),Efficient Key Management and Distribution for MANET, Communications. ICC '06. IEEE International Conference on , vol.5, no., pp.2256-2261,doi: 10.1109/ICC.2006.255106.