International Journal Of Engineering Research & Management Technology ISSN: 2348-4039

May- 2014 Volume 1, Issue 3

Email: editor@ijermt.org Website: ijermt.org

Attacks and Prevention Mechanism In Mobile Adhoc Network

Mandeep Singh, Ajay Kumar
Department of Computer Science & Engineering
Shree Siddhivinayak Group Of Institutions,
Bilaspur, Yamuna Nagar, Haryana, India

Abstract:
The collection of different types of nodes that are connected through each other via wireless link is called Mobile Ad-hoc Network (MANET). These nodes communicate with each other through wireless link. In order to protect the communication between these mobile nodes we need security. In this paper, we have attempted to present an overview of the known routing attacks and existing proposed countermeasures with a brief comparison among them for secured routing in MANET.

Keywords: Security, MANET, Prevention, Attacks

I. Introduction

Mobile Ad hoc Network (MANET) is a self-created and self organized network of mobile nodes interconnected using multi-hop wireless links in a strictly peer to peer fashion. The characteristics of mobile ad hoc networks pose numerous challenges in achieving conventional security goals. Since the nodes are responsible for basic MANET functions like packet forwarding and routing, network operations can be easily jeopardized if countermeasures are not integrated into these network functions at the early stages of design [1]. MANET features make it vulnerable to different types of attacks.

Non Secure Boundaries: In MANET, Node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. Due to no secure boundaries, MANET is more susceptible to attacks [2]. The links are compromised and are open to link spoofing attack [3][4].

Compromised Node: Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANET are autonomous and due to this autonomy during communication, ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity [4].

No Central Management: MANET is a self-configurable network, which consists of mobile nodes where the communication among these nodes is done without a central control. Each and every node act as router and can forward and receive packets [5]. MANET works without any preexisting infrastructure. The node connect with each other on the basis of blind mutual trust, a central entity can manage this by applying a filter on the nodes to find out the suspicious one, and let the other nodes know which node is suspicious [6] [7]

Shared Broadcast Radio Channel: This is in opposition to wired networks, where a separate dedicated transmission line can be provided between two end users. The radio channel used for communication in a MANET is broadcast in nature, and is shared by all nodes in the network, allowing a malicious node to easily obtain data being transmitted [8].

Lack of Association: Because of dynamic topology of MANET, there is no proper authentication mechanism that associates nodes with a network. Thus, an intruder would be able to join the network easily and carry out attacks [7].

Limited Resource Availability: The resources in MANET such as bandwidth, battery power, and computational power are limited, making it difficult to implement complex cryptography-based security mechanism in such networks [8].

Problem of Scalability: In traditional networks, where the network is build and each machine is connected to the other machine with help of wire. The network and the scale of the network, while designing it is defined and that do not change much during the use. In other words we can say that the scalability of the network is defined in the beginning phase of the designing of the network [9]. The case is quite opposite in MANET because the nodes are mobile and due to their mobility in MANET, the scale of the MANET is changing. [8].

None of existing routing protocols incorporate mechanisms to prevent, tolerate or defend against attacks from malicious adversaries. Due to the close relationship between security and the characteristics of ad hoc networks these protocols will have to be fundamentally altered or re-designed to effectively incorporate security mechanisms. The rest of the paper is organized as follows: In Section II, we discuss the various routing attacks in MANET. Survey of the current security solutions for the mobile ad hoc networks is describe in section III In Section IV, we draw the conclusion for the paper and point out some potential works in the future.

II. Security Attacks On MANET

A passive adversary or intruder is only able to listen to (eavesdrop on) network traffic without disrupting protocol operation and uses the information gained to breach network security. An active adversary, in addition, has full control over the communication channel, making it possible for the adversary to record and inject modified or selected data into the channel. Both passive and active attacks can be made on any layer of the network protocol stack [10]. This section however, focuses on network layer attacks only (routing attacks). Depending upon the various attacking behavior, routing attacks can be classified into five categories:

1. Information Disclosure Attack

In this, a compromised node may leak confidential information to unauthorized nodes in the network. Such information may include information's regarding the network topology, geographic location of nodes or optimal routes to unauthorized nodes in the network [11]. Attacks such as location disclosure and traffic analysis come under this category.

2. Attacks Using Impersonation

In impersonation attacks, the attacker assumes the identity and privileges of an authorized node, either to make use of the network resources that may not be available to it under normal circumstances or to disrupt the normal functioning of the network by injecting false routing information into the network. Some of the impersonation attacks include:

Man-in-the-Middle Attack: In this attack, a malicious node impersonates the receiver with respect to the sender, and the sender with respect to the receiver, without having either of them realize that they have been attacked with an intention to read or modify the messages between two parties [12].

Sybil Attack: In the Sybil attack [13], an attacker pretends to have multiple identities. A malicious node can behaves as if it were a larger number of nodes either by impersonating other nodes or simply by claiming false identities. Sybil attacks are classified into three categories: direct/indirect communication, fabricated/stolen identity, and simultaneity. In the direct communication, Sybil nodes communicate directly with legitimate nodes, whereas in the indirect communication messages sent to sybil nodes are routed through malicious nodes. An attacker can fabricate a new identity or it can simply steal it after destroying or temporarily disabling the impersonated node.

3. Attacks Using Modification

This attack disrupts the routing function by having the attacker illegally modifying the content of the messages. Some of the attacks involving packet modification are given below:

Misrouting Attack: In the misrouting attack, a non-legitimate node redirects the routing message and sends data packet to the wrong destination [14]. This type of attack is carried out by modifying the final destination address of the data packet or by forwarding a data packet to the wrong next hop in the route to the destination.

Byzantine Attack: Here a compromised intermediate node or a set of compromised intermediate nodes collectively carries out attacks such as creating routing loops, routing packets on non-optimal paths and selectively dropping packets [15]. Since in such attacks the network would seem to operate normally Byzantine failure are hard to detect.

Denial of Service (DoS) Attack: In this type of attack, an attacker attempts to prevent legitimate and authorized users of services offered by the network from accessing those services. A DoS attack can be carried out in many ways and against any layer in the network protocol stack. The classic way is to flood packets to any centralized resource used in the network by modifying the routes information in the packets so that the resource is no longer available to nodes in the network, resulting the network no longer operating in the manner it was designed to operate. This may lead to failure in the delivery of guaranteed services to the end users.

4. Attacks Using Fabrication

In fabrication attacks, an intruder generates false routing messages such as routing updates and route error messages, in order to disturb network operation or to consume other node resources. A number of fabrication based attacks are presented below:

Resource Consumption Attack: In this attack, a malicious node deliberately tries to consume the resources (e.g. battery power, bandwidth, etc.) of other nodes in the network [16]. The attacks could be in the form of unnecessary route request control messages, very frequent generation of beacon packets, or forwarding of stale information to nodes.

Routing Table or Route Cache Poisoning: In this attack, a malicious node sends false routing updates to other uncompromised nodes [10]. Such an attack may result in suboptimal routing, network congestion or even make some part of the network inaccessible.

Routing Table Overflow: The attacker advertises routes to non-existing nodes, to the authorized nodes present in the network. The main objective of such an attack is to cause an overflow of the routing table, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes [10].

Rushing Attack: On demand routing protocols that use route discovery process are vulnerable to this type of attack [17]. An attacker node which receives a “route request” packet from the source node floods the packet quickly through out the network before other nodes which also receive the same “route request” packet can react. Nodes that receive the legitimate “route request” packet assume those packets to be the duplicates of the packet already received through the attacker node and hence discard those packets. Any route discovered by the source node would contain the attacker node as one of the intermediate nodes. Hence the source node would not be able to find secure routes.

Black Hole Attack: A malicious node falsely advertises good path (e.g., shortest path or most stable path) to the destination node during the path finding process [10]. The intension of the malicious nodes could be to hinder the path finding process or to interrupt all the data packets being sent to the concerned destination node.

Gray Hole Attack: Under this attack, an attacker drops all data packets but it lets control messages to route through it [18]. This selective dropping makes gray hole attacks much more difficult to detect then blackhole attack.

5. Replay Attacks

In replay attack, an attacker retransmits data to produce an unauthorized effect. Examples of replay attacks are wormhole attack and tunneling attack.

Wormhole Attack: In this attack [17], two compromised nodes can communicate with each other by a private network connection. The attacker can create a vertex cut of nodes in the network by recording a packet at one location in network, tunneling the packet to another location, and replaying it there. The attacker does not require key material as it only needs two transceivers and one high quality out-of-band channel. The wormhole can drop packets or it can selectively forward packets to avoid detection. It is particularly dangerous against different network routing protocols in which the nodes consider themselves neighbor after hearing a packet transmission directly from some node.

Tunneling Attack: In a tunneling attack [17], two or more nodes collaborate and exchange encapsulated messages along existing data routes. For example, if a Route Request packet is encapsulated and sent between two attackers, the packet will not contain the path travelled between the two attackers. This would falsely make the receiver conclude that the path containing the attackers is the shortest path available.

Secure Routing In MANETs

To meet the recent and rapidly increasing demand in decentralized environments like mobile ad hoc networks [19] the need for a secure routing protocol becomes inevitable so that the various routing attacks such as malicious routing misdirection, black hole, gray hole, denial of service etc. can be averted [20]. Security protocols for MANET's can be mainly categorized in two major categories:

Prevention: This mechanism involves protocols which prohibit the attacking node to initiate any action. This approach requires encryption technique to authenticate the confidentiality, integrity, non-repudiation of routing packet information.

Detection and Reaction: Detection and Reaction mechanism as the name suggest will identify any malicious node or activity in the network and take proper action to maintain the proper routing in the network.

On the basis of our survey, various security protocols of MANET can be classified as Figure 1. In this paper, our focus is on prevention based security protocol of MANET that we discuss next briefly.

1. Authenticated Routing for Ad hoc Networks (ARAN)

Authenticated Routing for Ad hoc Networks (ARAN) [21] is a secure routing protocol based on the AODV protocol. The assumption in ARAN is that every node has a certificate that is signed by a trusted authority. The route discovery and route maintenance mechanisms are based on AODV and elaborated as follows –

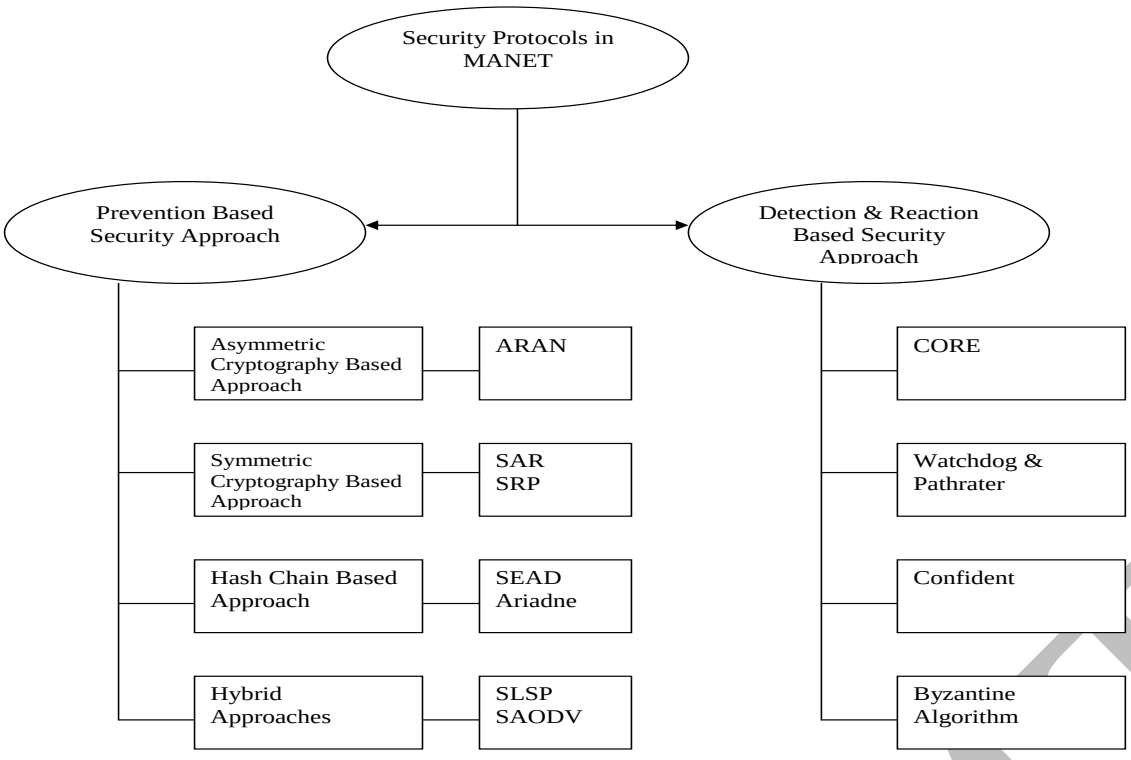

Figure 1: Security Approaches in MANET

Let us assume that a source node S wants to discover a route to destination node D. Also assume that A, B and C are three intermediate nodes on the path from S to D, having certificates as $cert_A$, $cert_B$, $cert_C$ and their private keys as K_a, K_b, K_c respectively. During the route discovery phase, a source node broadcasts a RREQ packet signed with its public key. The packet contains the destination node's address D, source node's certificate $cert_S$, a nonce N and a timestamp t. The nonce and timestamp ensure that the route is fresh. A sequence of route discovery messages is shown below:

$$S \rightarrow * : (RREQ, D, cert_S, N, t)\ K_s$$

$$A \rightarrow * : ((RREQ, D, cert_S, N, t)\ K_s)\ K_a, cert_A$$

$$B \rightarrow * : ((RREQ, D, cert_S, N, t)\ K_s)\ K_b, cert_B$$

$$C \rightarrow * : ((RREQ, D, cert_S, N, t)\ K_s)\ K_c, cert_C$$

(NOTE: * denotes that it is broadcast message)

Each intermediate node (such as A, B or C) that forwards the RREQ packet checks the signature(s) of the previous node on the packet by extracting the public key from the certificate. Further, it removes the previous node's signature, signs the RREQ packet with its own private key, adds the certificate to the header and broadcasts the packet to its neighboring nodes.

$$D \rightarrow C : (RREP, S, cert_D, N, t)\ K_d$$

$$C \rightarrow B : ((RREP, S, cert_D, N, t)\ K_d)\ K_c, cert_C$$

$$B \rightarrow A : ((RREP, S, cert_D, N, t)\ K_d)\ K_b, cert_B$$

$$A \rightarrow S : ((RREP, S, cert_D, N, t)\ K_d)\ K_a, cert_A$$

This process continues until the packet reaches the destination D. On receiving the RREQ, D will create a route reply (RREP) packet, add the source address S, its own certificate $cert_D$, a nonce and a timestamp and sign it with its private key. An intermediate route C on receiving the RREP packet will in turn verify the signature(s) of the previous node. For example, when node B receives the RREP packet from node C, it will verify the signature of node C. It will then remove C's certificate, sign the packet with its own private key K_b, add its certificate $cert_B$ and unicast it to the next node A on the reverse path as shown above. Nodes B and A will also add a routing table entry to node D indicating that the next hop is C and B respectively.
When node B discovers a broken link to C, it initiates route maintenance in the following manners:

$$B \rightarrow A : ((RERR, S, D, cert_{B,} N, t) K_b)$$
$$A \rightarrow S : ((RERR, S, D, cert_{B,} N, t) K_b)$$

Thus it sends a RERR packet, the source node's address, the destination address, its own certificate $cert_B$, a nonce and a timestamp signed with its private key to its previous node A. Node A will forward this unchanged to the source node S. ARAN prevents against attacks which modify the routing information since it uses public key authentication. However, it is vulnerable to DoS attacks which flood the network with fake packets due to the use of certificates which require high bandwidth and processing power of nodes.

2. ARIADNE

The ARIADNE routing protocol [22] proposed by Yi-Chun Hu et al. prevents against several types of active and passive attacks. Active attacks are those where a malicious node eavesdrops on a network and injects fake packets. On the other hand, passive attacks are threats against the confidentiality of the communication rather than the network's function. Active attacks can be of several types such as Active-0-1 (in which the attacker owns one node), Active-1-x (in which the attacker owns one compromised node and distributes the cryptographic keys to its x-1 other nodes), and Active-y-x. The wormhole attack is an example of this type of attack.
The ARIADNE protocol is a secure routing protocol based on DSR, which withstands node compromise and uses efficient symmetric key cryptography. The assumption made in ARIADNE is that the nodes can authenticate routing messages using three schemes – shared secrets between each pair of nodes, shared secret between the communicating nodes combined with broadcast authentication or by using digital signatures. ARIADNE works in two phases, route discovery and route maintenance similar to DSR. They are in turn described below –
Route Discovery: In order to authenticate the RREQ packets, every source node adds a Message Authentication Code (MAC) [23] computed with the shared key between the source and the destination (K_{SD}). In order to verify the intermediate nodes in a RREQ packet, every node along the path from source to destination authenticates the new information in RREQ packet using a TESLA key [APE2000]. The destination node will buffer the RREP packet until the intermediate nodes can release their corresponding TESLA keys, after which a security condition is met. Now, the target adds a MAC to the RREP packet hashed with K_{SD} and forwards it on the reverse path to the source node. Further, in order to prevent any malicious node from removing any previous hop from the route, a technique called per-hop hashing is used [22].
Route maintenance: Route maintenance in ARIADNE is similar to DSR, where a node forwarding a packet to the next hop along the source route sends a RERR packet back to the originating node if it is unable to deliver the packet to next hop. The sender node authenticates an RERR packet by checking the time delay in receiving the packet. By using a mechanism such as TESLA, each node that will be able to authenticate the RERR packet buffers it until it can be authenticated.
ARIDANE prevents against both active and passive attacks, specifically it prevent attacks using fabrication such as forming routing loops by spoofing. It also prevent against the black hole attack by using per hop hashing mechanism and many kinds of Denial of Service (DoS) attacks due to flooding of route request

packets in the network. Furthermore, it is also efficient since it is based on a reactive protocol which has a better performance than table-driven protocols and symmetric key cryptography.

3. Secure and Efficient Ad hoc Distance Vector (SEAD) Routing Protocol

The Secure and Efficient Ad hoc Distance vector routing protocol (SEAD) [24] is based upon the DSDV-SQ routing protocol (which is a modified version of DSDV routing protocol). It uses efficient one-way hash function to authenticate the lower bound of the distance metric and sequence number in the routing table. More specifically, for authenticating a particular sequence number and metric, the node generates a random initial value $x \in (0,1)^{\rho}$ where ρ is the length in bits of the output of the hash function, and computes the list of values $h_0, h_1, h_2, h_3, \ldots, h_n$, where $h_0 = x$, and $h_i = H(h_i - 1)$ for $0 < i \leq n$. As an example, given an authenticated *hi* value, a node can authenticate h_{i-3} by computing H (H (H (h_i-3))) and verifying that the resulting value equals h_i.

Each node uses one authentic element of the hash chain in each routing update it sends about itself with metric 0. This enables the authentication for the lower bound of the metric in other routing updates for that node. The use of a hash value corresponding to sequence number and metric in a routing update entry prevents any node from advertising a route greater than the destination's own current sequence number. The receiving node authenticates the route update by applying the hash function according to the prior authentic hash value obtained and compares it with the hash value in the routing update message. The update message is authentic if both value matches. The source must be authenticated using some kind of broadcast authentication mechanism such as TESLA [23]. Apart from the hash functions used, SEAD does not use average settling time for sending triggered updates as in DSDV in order to prevent eavesdropping from neighboring nodes. SEAD prevents against several types of Denial of Service attacks. It also prevents formation of routing loops. However, it does not prevent the wormhole attack.

4. Secure Ad hoc On-Demand Distance Vector (SAODV)

SAODV is an extension of the AODV routing protocol, and it can be used to protect the route discovery mechanism by providing security features like integrity, authentication and non-repudiation [25]. SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each node is capable of securely verifying the association between the address of other node and the public key of that node. A key management scheme is needed for SAODV. Two mechanisms are used to secure the AODV messages that are Digital signatures to authenticate the non-mutable fields of the messages, and Hash chains to secure the mutable hop count field of the message. For the non-mutable fields, authentication can be performed in a point-to-point manner, but the techniques cannot be applied to the mutable information. Route error messages are protected in a different manner because of a big amount of mutable information. According to the author et al. [25] highlight the fact that it is not important which node started the route error and which nodes are just forwarding it. The important information is that a neighbor node is informing other nodes about its inability to route messages to certain destinations anymore. Therefore, every node (generating or forwarding a route error message) uses digital signatures to sign the whole RERR message and any neighbor that receives RERR verifies the signature.

5. Secure Routing Protocol (SRP)

SRP is an on demand source routing protocol based on symmetric key cryptography [26]. In SRP, only the source and the destination node share a key resulting to a strict end-to-end exchange of routing information between them, and end-to-end authentication of routing control packets. The design of SRP is influenced by the observation that due to the mobility of the nodes, it would be impractical that the source or destination shares keys with all intermediate nodes on a route. Therefore sharing the key only between source and destination simplifies the key management considerably. In SRP intermediate nodes do not send replies to route discovery messages and they do not cache route information from overheard routing control packets. SRP is a very efficient protocol as the route request and route reply messages contain only a single MAC value. Moreover, the MAC value is not processed by the intermediate nodes. SRP is resistant to attacks

aiming at route disruption and route diversion from a single adversarial node but not against attacks mounted by colluding adversaries. SRP assumes that a shared secret is established between the source and destination but do not solve the problem of key agreement.

6. Secure Link State Protocol (SLSP)

The Secure Link State Protocol (SLSP) [27] for mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. The scope of SLSP may range from a secure neighborhood discovery to a network-wide secure link state protocol. SLSP nodes disseminate their link state updates and maintain topological information for the subset of network nodes within *R* hops, which is termed as their *zone*. Nevertheless, SLSP is a self-contained link state discovery protocol, even though it draws from, and naturally fits within, the concept of hybrid routing. To counter adversaries, SLSP protects link state update (*LSU*) packets from malicious alteration, as they propagate across the network. It disallows advertisements of non-existent, fabricated links, stops nodes from masquerading their peers, strengthens the robustness of neighbor discovery, and thwarts deliberate floods of control traffic that exhausts network and node resources. To operate efficiently in the absence of a central key management, SLSP provides for each node to distribute its public key to nodes within its zone. Nodes periodically broadcast their certified key, so that the receiving nodes validate their subsequent link state updates. As the network topology changes, nodes learn the keys of nodes that move into their zone, thus keeping track of a relatively limited number of keys at every instance. SLSP defines a secure neighbor discovery that binds each node *V* to its Medium Access Control (*MAC*) address and its *IP* address, and allows all other nodes within transmission range to identify *V* unambiguously, given that they already have *EV*. Nodes advertise the state of their incident links by broadcasting periodically signed link state updates (*LSU*).

SLSP restricts the propagation of the *LSU* packets within the zone of their origin node. Receiving nodes validate the updates, suppress duplicates, and relay previously unseen updates that have not already propagated *R* hops. Link state information acquired from validated *LSU* packets is accepted only if both nodes incident on each link advertise the same state of the link.

III. Conclusion

In this paper, we have presented an overview of the current state of the art routing attacks and various prevention based countermeasures in MANETs. It has been observed that although active research is being carried out in this area, the proposed solutions are not complete in terms of effective and efficient routing security. There are limitations on all solutions. They may be of high computational or communication overhead, i.e. in case of cryptography which is detrimental in case of resource constrained MANETS, or of the ability to cope with only single malicious node and ineffectiveness in case of multiple colluding attackers. Some solutions may require special hardware such as a GPS or a modification to the existing protocol. Furthermore, most of the proposed solutions can work only with one or two specific attacks and are still vulnerable to unexpected attacks. Future research efforts should be focused not only on improving the effectiveness of the security schemes but also on minimizing the cost to make them suitable for a MANET environment.

References

1. L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks,” IEEE Network: special issue on network security, vol. 13(6), pp. 24–30, 1999.
2. S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.,” International Conference on Computational Intelligence and Security, pp. 421-425, 2009.
3. Amitabh Mishra and Ketan M. Nadkarni, “Security in Wireless Ad Hoc Networks”, The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.
4. D.B.Roy, R.Chaki and N.Chaki, “A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad Hoc Neworks,” International Journal of Network Security and Its Application (IJNSA), Vol. 1(1), pp. 44-52, April, 2009.

5. Carlos T. Calafate, Juan-Carlos Cano, Pietro Manzoni, Manuel P. Malumbres, "A QoS architecture for MANETs supporting real-time peer-to-peer multimedia applications", ISM.2005.18, pp.193-200, Dec. 2005
6. Yongguang Zhang and Wenke Lee, "Security in Mobile Ad-Hoc Networks", the Book AdHoc Networks Technologies and Protocols", Springer, 2005.
7. C. K. Toh, "Adhoc Mobile Wireless networks: Protocols and Systems", Prentice-Hall, New-Jersey, pp. 34-37, 2002.
8. Jameels Al-Jaroodi, "Security Issues in Wireless Mobile Adhoc Networks (MANET)", technical Report TR02-10-07, University of Nebraska-Lincoln, 2002
9. Panagiotis Papadimitraos and Zygmunt J. Hass, "Securing Mobile Ad Hoc Networks", The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC, 2003
10. C. Siva Ram Murthy and B. S Manoj, "Ad Hoc Wireless Networks, Architecture and Protocols", Prentice Hall PTR, 2004.
11. Stefano Basagni, Macro Conti, Silvia Giordano and Ivan Stojmenovic, "Mobile Ad Hoc Networks" , IEEE press, john Wily & Sons, INC. publication, 2003
12. M. O. Pervaiz, M. Cardei, and J. Wu, "Routing Security in Ad Hoc Wireless Networks," Network Security, S. Huang, D. MacCallum, and D. -Z. Du (Eds.), Springer, 2008.
13. J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks: Analysis & Defenses, Proceeding of the 3rd International Symposium on Information Processing in Sensor Networks, pp. 259-268, 2004
14. K.Sanzgir, and B.Dahill, "A secure routing protocol for ad hoc networks", Proceeding of the 10th IEEE International Conference on Network Protocols, pp.1-10, 2000
15. B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure routing protocol Resilient to Byzantine failures", Proceedings of ACM workshop on Wireless Security, pp. 21-30, September 2003
16. Imrich Chlamtac, Marco Conti, Jenifer J.-N. Liu, "Mobile Ad Hoc Networking: Imperatives and Challanges", Elsevier Network Magazine, vol. 13, pp. 13-64, 2003
17. Y. Hu, A. Perrig and D. B Johnson, "Rushing attacks and defense in Wireless Ad Hoc Network Routing Protocol", Proceedings of ACM workshop on wireless security, pp. 30-40, September 2003
18. Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy and P. Balamuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", Proceedings of 6th International Conference on Information, Communications and Signal Processing, December 2007
19. Vincent D. Park and M.Scott Corson, " Temporally –Ordered Routing Algorithm(TORA) version1:Functionalspecification. Internet-Draft,draft-ietf-manettora- spec-00.txt,Novenber 1997.Work in Progress
20. David Lundberg Ad hoc Protocol Evaluation and Experiences of Real World Ad Hoc Networking, Department of Information Technology, Uppsala University, Sweden
21. B. Dahill, B. N. Levine, E. Royer, and C. Shields, "ARAN: A Secure Routing Protocol for Ad Hoc Networks," UMass Tech Report 02-32, 2002.
22. Y.-C. Hu, A. Perrig , and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proceeding of 8th ACM International Conference on Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, pages 12-23, 2002.
23. A. Perrig, R. Canetti, "The TESLA Broadcast Authentication Protocol", RSA Labratories, Vol. 5(2), 2002.
24. Yih-Chun Hu, David B. Johnson, Adrian Perrig. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", Proceeding of 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), pp: 3-13, Jun 2002.
25. Zapata, M. G., "Secure ad-hoc on-demand distance vector (SAODV) routing," IETF MANET, internet draft, draft-guerreromanet- saodv 00.txt, 2001.- accessed 10/10/2006.
26. Asad Amir Prizada and Chris McDonald, "Secure Routing Protocols for Mobile Ad hoc Wireless Networks," Proceeding of 2nd Workshop on Internet, Telecommunication and Signal Processing, pp. 57-80, 2003.
27. P. Papadimitratos and Z.J. Haas, "*Secure Link State Routing for Mobile Ad Hoc Networks*" Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks, IEEE Press, 2003, pp. 27–31.
28. Srdjan Capkun and Jean-Pierre Hubaux, "*Building Secure Routing out of an Incomplete Set of Security Associations" WiSE'03,* September 19, 2003, San Diego, California, USA.