Security Attacks and Defensive Measures For Routing Mechanisms in MANETs – A Survey

Devi. P
Department of Computer Applications
Anna University of Technology, Coimbatore
Coimbatore, India

A. Kannammal
Department of Computer Applications
Coimbatore Institute of Technology
Coimbatore, India

ABSTRACT
Indispensable feature of MANETs is security. MANET is a sort of wireless network communications that can construct itself on the run. One of the significant properties of MANET is dynamic organization. To lodge the varying topology and to provide security, well defined routing algorithms are needed. No protocols detain all the security attacks and provide strategies to prevent them. A network layer protocol is necessary to incorporate all security solution to protect both route and data forwarding operations. The aim of this paper is to analyze security issues and their countermeasures in the ad hoc network layer environment. We discuss the hazards on the network layer and various security protocols.

General Terms
Wireless ad hoc network, MANETs, Security attacks, Survey

Keywords
Network-layer attacks, Threats, Secure routing, Defense metrics

1. INTRODUCTION
A MANET is an infrastructureless network because mobile nodes in the network subject to change and create paths dynamically among themselves to broadcast packets. Each node functions as a router to forward packets if it is not an end node. MANET can be viewed as a random graph because the nodes in the wireless network keep on moving. The nodes can move anywhere and organize themselves into the network. Since MANET has dynamic topology, it possesses several salient features like resource constraints, limited physical security, and no infrastructure [1].

MANET needs special routing algorithms because of its dynamic topology. No protocols can satisfy all the network constraints perfectly. Protocol is selected based on the network characteristics, like volume, density and the mobility of the nodes. Routing protocols should launch most possible and reliable communication path between nodes. Routing phase is very crucial and any attack in this phase may upset the entire network. The most susceptible layer in MANET environment is Network layer. Thus, Security in network layer determines the security of the whole network. Routing protocol must comprise security solutions to prevent, detect, and respond to security attacks. These solutions used to stop malicious nodes in the network; they promptly act as routers to collapse the whole network. This malicious node may disturb the network, like slow delivery of packets, dropping of packets, and stale routing information. Network layer can be protected by efficient protocols. These protocols should identify and prevent malicious nodes.

MANETs exhibit some of the characteristics to accomplish consistent and secure wireless communication. They may include Confidentiality, Availability, Authentication, Integrity and Non-repudiation [2].

- Confidentiality: Protection of data packets from malicious nodes. Normally intermediate nodes may eavesdrop the information which is passing through those nodes. It's a challenging job to prevent data packets being disclosed by compromised nodes.
- Availability: The feature of present at any time. Denying a service when it is required is one kind attack happens in MANET environment. Security protocols should offer minimum survivability even though there is a Denial of Service (DOS) attack.
- Authentication: A security measure intended to protect communication system from fraudulent transmission. An attacker may imitate a node and achieve unauthorized access to resource and sensitive information if there is no authentication.
- Integrity: Giving assurance that information being whole and unchanged.
- Non-repudiation: Ensures that source and destination nodes can never deny about their sending and receiving of information.

Since MANET is a kind of wireless communication environment, the nodes have to compete with the effects of wireless communication, such as interference, noise, fading and less bandwidth. In addition, the control of the network is disseminated among the nodes. Each node performs as a host as well as a router. If a node moves, this will make changes in the whole network topology. Thus, protocols exercise efficient handover and auto configuration of traveling nodes.

MANETs need some efficient protocols to challenge the troubles are lack of infrastructure, motility of nodes, limited resources, inadequate of battery power, and memory. Security of MANETS totally depends upon the routing protocol which adopt. A secure routing protocol should be able to detect malicious nodes, should follow precise route discovery method, route maintenance process, regular updating of routing table information and to be immune against attacks.

This paper is structured as follows. In Section 2, common network security attacks include advanced attacks in network layer. In Section 3, defense Metrics against Routing Attacks in ad hoc environment. In Section 4, a discussion on open challenges and future directions.

2. COMMON NETWORK SECURITY ATTACKS IN MANETS

Wireless networks are more vulnerable than a wired network. There is a range of attacks aim at the weakness of MANETs. All data packets should pass through many intermediate nodes before reaching destination. Each node maintains route entry to other nodes in two ways either node itself initiates the route discovery or other nodes push to discover routes. Hence it maintains proper routing table entry and it becomes an essential job of mobile network communications. Route discovery and maintenance phase are always monitored by malicious node, make other nodes to follow fake route entry and disrupt the directions of the routing protocols. Some widespread network layer exposures and some of their controls are listed in Table 1.

TABLE 1. Network Layer exposures and Some Controls

Network Layer exposures	Controls
i. Route spoofing - transmission of false network topology	i. Exercise firm anti-spoofing and route filters at periphery network
ii. IP Address Spoofing- fake source address on malicious data packets	ii. Firewalls should exercise well-built filter and anti-spoofing as well
iii. Identify resource ID vulnerability - depend on addressing of resources and peers can be broken and vulnerable	iii. Implementation of broadcast monitoring system that minimizes the exploitation of protocol features.

Generally the attacks in MANETS can be grouped into two categories namely passive attacks and active attacks [3] [4].

2.1 Passive Attacks

The data exchanged in the network is monitored by Passive attacks are initiated by the adversaries. The operations of the network will not be disrupted by these adversaries. It is very hard to recognition these attacks because these attacks will not disturb network operations. Though passive attacks try to snoop sensitive data by listening to traffic. Protecting the network against such attacks is really a very tough and complicated job. Passive attacks may include eavesdropping, monitoring, and traffic analysis.

Some sensitive information kept secret will be eavesdropped by an intruder during the communication. It also said to be disclosure attacks. An attacker eavesdrops on the network communication to reveal which node tries to create route to which node, location, private key, and password of the nodes. And this attack smells the essential or key nodes for whole network operations. This information will be passed to an accomplice who will use it to initiate attacks.

2.2 Active Attacks

Active attack attempts to modify or destroy the data packets being exchanged between source and destination. Hence normal functionality of the communication will be disrupted. Operation of the protocol will be collapsed in order to limit availability or gain authentication. The aim of this attack is to attract all packets to the malicious node as means to drop or change packets to bring down the network. These attacks can be easily sensed and malicious nodes can be easily recognized. The compromised nodes may from internal or external. If it is from internal part of the network, it may be very tedious job to detect the node than external. Active attacks may be dropping of packets, modification of packets, replaying of packets, impersonation as some other nodes, fabrication of messages, and rushing of packets over high-speed private network like wormhole attack [5] [6] and black hole attack [7].

2.2.1 Attacks based on modification

Routing protocol packets bring control messages which rule data transmission among nodes. Malicious node announces fake routes to reach destination and cause redirection of network traffic. This is uncomplicated way for a malicious node to upset the operations of an ad-hoc network. This attack may consist of the adaptation of the metric value for a route or by modification of control message fields. This attack can be classified as redirection attacks and DOS attacks.

i. *Redirection by modified route sequence number*: To choose a reliable path each node relies on the information like hop count, sequence number etc. The smaller in value shows the most favorable route. So easy way of attacking is to change the original values with the smaller values to attract nodes, whose packets to be intercepted. ii. *Redirection by modified hop count*: The protocol like AODV, the optimal path is selected based on the path length where as path length is denoted as hop count metric. A malicious node can advertise smallest hop count to a particular destination through itself to attract all data packet to that destination. iii. *Denial of Service by modifying source route*: A malicious node insert itself between communicating parties and dominates over data packets passing through them. This can modify the source route so that can create loops or drops packet to launch denial of service attack.

2.2.2 Impersonation Attacks

Attacker node pretends its identity by changing its' own IP or MAC address and adopt some other node identity. This is also called 'spoofing'. The attacker node masquerading as another node and can launch many attacks like route looping, isolating nodes etc. This type of an attack could easily be improved by the use of a well built authentication procedures.

2.2.3 Attacks by Fabrication of Information

Generation of fake route messages is said to be fabrication of information. In [8], Fabrication attacks include "active forge" sends forged message without receiving any messages and "forge reply" sends forged reply to original route request. There are 3 sub categories for fabrication attacks.

2.2.3.1. *Falsification of Route Error Messages*

This is very common in AODV and DSR, because these two protocols use maintenance measures if the destination node or intermediate node in an optimal path moves or fails. The node which precedes the failed link sends a Route error message to all other neighboring nodes that it follows a broken link. Then all nodes invalidate that particular route as inaccessible path and removes routing table entry. A malicious node can spoof any node and send fake route error message to all other nodes. Thus a Denial of Service attack can quiet easily be launched. The node S has route to D passing through X, Y, and Z as in Figure1 malicious node M tries to insert itself in to the network, and launch a Denial of Service attack against the destination node D. It sends forged route error messages to other nodes that route between Z and D is no longer accessible. So that X and Y deletes its' routing table entry to the node D through Z.

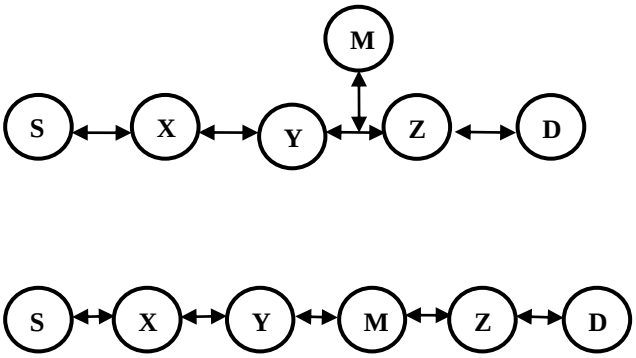

Figure 1. Malicious node tries to intrude a network

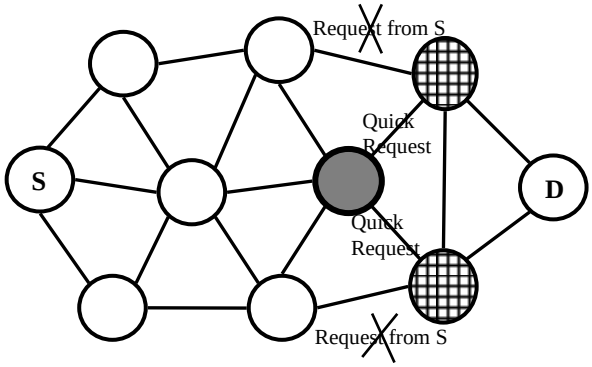

Figure 2: A Network illustrates rushing attack

2.2.3.2 Route Cache Poisoning

This is very common attack in DSR protocol. A node overhears any packets which may pose routing information in their header will be updated in the routing cache of that node. This method of learning routes will be exploited by malicious nodes. They send spoofed packets to other nodes via themselves, such that other nodes may alter their routing cache and start communicating with attacker node. This result in congestion of network, network inaccessible or least advantageous path selection.

2.2.3.3 *Routing table overflow attack*

Proactive algorithms are more vulnerable to this attack. Proactive protocols try to find routes even before they need and a malicious node misleads the protocol to find routes to non-existent nodes. Thus no more routes can be stored in the routing table because they already stuffed with fake routes. In any of the 3 cases, recognition of attack is very difficult.

2.2.4 Routing Attacks

A malicious node can absorb network traffic, add itself into the routing path between communicating parties and be in command of network traffic. As shown in the figure 1, a malicious node **M** can insert itself between sender **S** and receiver D [9].

2.2.4.1 Packet Replication attack

An attacker replicates the stale packets. Thus network resources like bandwidth and battery power will be consumed.

2.2.4.2 Rushing attack

As shown in the Figure 2, an attacker obtains the RouteRequest packet from source node floods that packet rapidly to all the other nodes in the network. Thus all nodes will receive forged route request before the original request reaches them. Later while reaching nodes, original RouteReque*st* packet will be treated as a duplicate one and rejected. Rushing attack is an effective denial-of-service attack against all on-demand network routing protocols [10].

2.3 Other Advanced Network Attacks

More sophisticated and subtle routing attacks have been identified in recent research papers. The black hole, Byzantine and wormhole attacks are the typical examples, which are described in detail below.

2.3.1 Wormhole attack

Wormhole attack connects one part of the network to another via exclusive path; packets are passed over this path in a rapid speed. An adversary tunnels packets from one point to another and control over the packets from that point [11]. This attack can be easily launched in reactive protocols like DSR and AODV. The RouteRequest from source will be directly tunneled from one compromised node to another, from that Route Requests are replayed to other nodes, and reaches destination. If the same requests travel through normal path will be discarded. Thus wormhole attack redirects all packets via compromised nodes. The attacker does not need to know about any cryptographic methods or keys, hence wormhole attack is launched against all exchange of information that offers authenticity and privacy. In figure 3, source S sends RouteRequest to Destination D through all neighboring nodes. Node X and Y tunnels the request, reaches node D, makes it to accept the route, and makes node D to reject the requests from other nodes as duplicate requests.

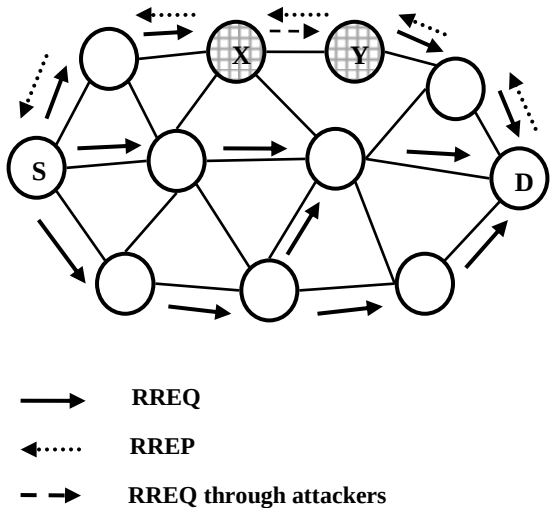

Figure 3. Illustration of wormhole attack in a network

2.3.2 Black hole attack

A node in the selected path is an attacker can deny the communication to take place. As shown in the Figure 4, if an adversary is selected as an intermediate node then it stops the packet forwarding to next node. This is a common attack in AODV protocol. Once a malicious node receives a RREQ, it sends RREP packet with higher sequence number without delay. Hence source node starts communicating with malicious node and discard RREP comes from other nodes. It consumes all data packets and not passing to anywhere.

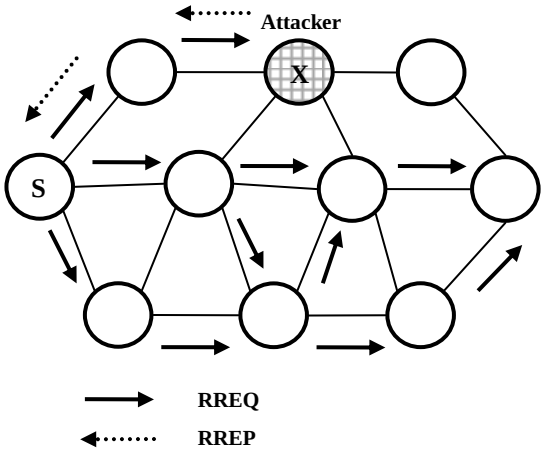

Figure 4. Illustration of Black hole attack in a Network

2.3.3 Gray hole attack

A smaller variation of black hole attack is gray hole attack. This partially drops the data packets. This may happen selectively or statistically. In both the cases detection of attack is very complicated.

2.3.4 Byzantine attack

An adversary node or a group of malicious nodes working together to do attacks such as create routing loops, dropping of packets or stop forwarding packets, selective dropping of packets, forwarding packets through least favorable paths. This attack is simple to recognize, thus it gradually degrades the performance of the network [12].

2.3.5 Resource consumption attack

In ad hoc environment power of nodes is very crucial factor to keep alive. An adversary node can try to consume battery power by forwarding unwanted data packets, creating loop routes, thus node will lose power without reaching destination, or demanding unnecessary route discovery to the target node. So that victim node slowly depreciate its' battery power.

2.3.6 Location disclosure attack

An attacker discloses information about the construction of nodes in a network. It smells the location of nodes, the way nodes are arranged. It figures out the important nodes and their communicating parties, analysis network traffic pattern. Based on that it draws the routing plan and generate attack scenarios. This attack overwhelms security at times.

3. DEFENSE METRICS AGAINST ROUTING ATTACKS IN MANET

Network layer faces a prominent range of security threats than other layers in MANET. Efficient routing protocols may protect the network in a fair way such that even in the presence of malicious node. Protocol detects any malicious node; rest of network should be altered about the existence of this poisoning node. Thus other nodes can change their route entry, which includes that adversary node as one of the intermediate nodes. Well-organized protocol should preserve network topology to protect information like nodes play important roles, analysis of traffic flow etc. Some SRPs have been discussed about many solutions for attack imposed in MANETs such as IPsec, SAODV, SEAD, SRP, ARAN, SSL, and so on. But none of them gives total protection against all attacks. All preventive mechanisms rely on cryptography to ensure security to provide authentication, confidentiality, integrity and non repudiation of routing information. The goals and methods of some protection schemes have been discussed below.

3.1 Secure Ad-hoc On-demand Distance Vector Routing Protocol (SAODV) [13]

SAODV is an effort to add security to SODV. The key attribute of SAODV is using digital signature to authenticate the fields of routing messages and using hash chains to authenticate hop count. It uses node-to-node verification so that establishes end-to-end authentication. RREQs are digitally signed and propagated, in each node the signature is verified before updating the routing table. RREQs include single signature extension. This same process is followed for RREPs also. The intermediate nodes should sign the RREP as it comes from destination node, it uses double signature extension. All fields are immutable except hop count. The hop count is authenticated by hop count authenticator, is a hash chain element.

3.2 Authenticated Routing for Ad-hoc Networks (ARAN) [14]

ARAN is a security protocol based on public-key cryptography against all malicious nodes which may cause impersonation or repudiation attack. It introduces authentication, message integrity and non-repudiation concepts, hence it operates on cryptographic certificates. Each node holds a certificate signed by trusted authority which connects IP address and public key. The functionality of this on-demand routing protocol is divided as route discovery and route maintenance. RREQ packet of ARAN contains address of destination, certificate of source, nonce, and a timestamp. The first intermediate node checks the signature of source and appends its' own certificate with original. All later intermediate nodes removes the certificate of pervious node and appends its' certificate. Thus each node makes an entry in their routing table. The same process is again replicated for RREP packet also. If any path breaks, that particular node sends ROUTE ERROR message to previous node. Then ROUTE ERROR message will be passed to other nodes in that route and route entry in each node will be removed from route table. Though ARAN is pretty well against attacks, little vulnerable to DoS attack by flooding the network with fake data packets. Hence all packets need verification which slows the network, force the node to drop some packets.

3.3 Security - Aware ad hoc Routing (SAR) [15]

S. Yi et al., recommended a protocol based on on-demand protocols like AODV or DSR, uses symmetric key encryption. This can be easily deployed on the top of any existing protocols, without any major issues. This protocol makes use of word Trust Hierarchy, each node is assigned with different trust levels. And this trust levels are immutable. Source node defines the minimum trust level to nodes to participate in the route discovery; hence a node of particular trust level will possess a key for that level. This key value to set each security level among nodes, thus this process produces trouble that a fresh key has to be set for each node which is subject to come in or go out of the network. In route discovery stage, additional fields are given to RREQ and RREP packets. Source node indicates minimum trust level in RREQ packet; an intermediate node should possess this trust level to be a part of the network. When an intermediate node receives this RREQ packet, it checks for the security rating in RREQ packet and compares with the value it has. If it is greater than the request packet value, then it forwards it else it drops the packet. Another field gives maximum security level can be given by the discovered path. An optimal route is discovered by SAR need not to be a shortest path but it ensures the path found is the most protected in terms of trust level. There is a possibility that an attacker may give higher trust level key to a node though it owns lower trust level.

3.4 Secure Routing Protocol (SRP) [16]

Secure Routing Protocol can be applied on any top of the existing protocols. This protocol guarantees that the source node which initiates route discovery will be able to differentiate genuine replies and fabricated replies to give fake topological information and discard it. This can be achieved through the basic idea Security Association (SA) between the source and the destination to authenticate Route Request and Route Response packets using Message Authentication Codes. SA can be attained by a shared key based on the other party's public key, is used for both encryption and decryption. SRP is an extension header, attached to RREQ and RREP, when an intermediate node receives RREQ, it checks whether SRP header is present or not. If not present, packet will be rejected. Else the IP address of source and destination will be extracted and it creates an entry in its routing table. An intermediate node with cached route shares a group key with source node can use that group key to authenticate the RREPs. The destination node has to counter to source with different types of topology in order to reply to the one or more route request packets.

3.5 SEAD [17]

SEAD protocol is designed on the DSDV protocol. The goal of this protocol is defend modification attacks, routing attacks, and Dos attacks. It implements on-way hash function instead of asymmetric cryptographic operations to prevent adversary nodes from changing of sequence number and hop count. SEAD authenticates those values of each update routing information. This protocol needs broadcast authentication like TESLA [12] or a symmetric key cryptography. SEAD evades routing loops, but the downside is an adversary node uses the information of sequence number and hop count which were the recent updates of routing information and updates a new routing message.

3.6 ARIADNE [18]

Ariadne is a design and performance evaluation of reactive protocols. It uses symmetric cryptographic primitives. Ariadne authenticates its' routing messages through TESLA a authentication broadcast uses Message Authentication Code (MAC) and this needs low synchronization time than using pair-wise shared keys. Hence it establishes secure end-to-end communication. The features of this protocol hold three stages.

i. *Target authenticates ROUTE REQUESTs*: To assure the authority of each field of RREQ at the end node, the source includes MAC with key over a unique data like timestamp. The target verifies its' freshness using that key.

ii. *Techniques for authentication routing information*: Ariadne permits the target to authenticate each individual node in the RREQ. Now the initiator authenticates all node list in the RREP, possibly RREP contains only legitimate nodes. There are three methods for node list authentication. They are TESLA protocol, digital signatures and standard MACs.

iii. *Per-hop hashing method*: An adversary may remove a node from the node list in RREQ packet. Ariadne uses one way hash functions to check the no. of hop counts. So it avoids removing of nodes from the node list and prevents adversary nodes in advertising shorter path. Ariadne defends flooding of route request and cache poisoning attack. Since Ariadne adopts the method of periodic updates of routing protocol and clock synchronization between communicating parties, is said to be complicated one.

4. DISCUSSION ON OPEN CHALLENGES AND FUTURE DIRECTIONS:

We have discussed various routing attacks in ad hoc environment and many defense metrics against those attacks in this survey. Defense will be achieved successfully if prevention metrics should work as a base line. Detection and reaction against attacks should be done as soon as possible if any malicious nodes have been sketched. Protocols plays key role in terms of security. They should offer error-free and well-organized networks. If any path break or partition of network happens there in the position that they could reorganize the network. Presently working protocols are against one or more routing attacks not for all the attacks that a network layer may anticipate. Dynamic infrastructure of ad hoc environment forces it to be more vulnerable to attack and makes it hard to detect malicious node entrant. Cryptography is one of the key techniques to provide security and prevent attacks as well. There are many efficient key exchange or distribution protocols have been launched for security. But they are confined because of limited resources and dynamic topology. A lot of research efforts should be carried out to find an efficient and effective routing protocol that should bind the characteristics minimum complexity and less cost.

5. REFERENCE

H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, pp. 38-47, 2004.

[2] Y. Xiao, X. Shen, and D.-Z. Du (Eds.), "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", WIRELESS/MOBILE NETWORK SECURITY, Springer, 2006

[3] S. Yi and R. Kravets, "Composite Key Management for Ad Hoc Networks", Proc. of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), pp. 52-61, 2004.

[4] R. Oppliger, "Internet and Intranet Security", Artech House, 1998.

[5] Y. Hu, A Perrig, and D. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks", Proc. of IEEE INFORCOM, 2002.

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

[7] Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security & Privacy, pp. 28-39, 2004.

[8] Ning P., Sun K., "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-hoc Routing Protocols", In Proc. of the IEEE Workshop on Information Assurance, pp. 60-67, 2003

[9] Y. Xiao, X. Shen, and D.-Z. Du (Eds.), "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", WIRELESS/MOBILE NETWORK SECURITY, Springer, 2006

[10]Yih-Chun Hu, Adrian Perrig, and David Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", ACM Workshop on Wireless Security (WiSe 2003) September 19, 2003, California, U.S.A.

[11] M. Ilyas, "The Handbook of Ad Hoc Wireless Networks", CRC Press, 2003.

[12] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures", Proc. of the ACM Workshop on Wireless Security, pp. 21-30, 2002.

[13] Manel Guerrero Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing" INTERNET-DRAFT draft-guerrero-manet-saodv-00.txt, August 2002. First published in the IETF MANET Mailing List (October 8th 2001).

[14] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, "A secure routing protocol for ad hoc networks", Proc. of 2002 IEEE International Conference on Network Protocols (ICNP), November 2002, IEEE Press, pp. 78–87

[15] S. Yi, P. Naldurg, R. Kravets, "A security-aware ad hoc routing protocol for wireless networks", The 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2002), 2002.

[16] P. Papadimitratos, Z.J. Haas, "Secure Routing for Mobile Ad hoc Networks SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)", San Antonio, TX, January27–31, 2002.

[17] Y.-C. Hu, D.B. Johnson, A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", Proc. of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), IEEE, Calicoon, NY, June 2002, pp. 3–13.

[18] Y.-C. Hu, A. Perrig, D.B. Johnson, "ARIADNE: A Secure On-Demand Routing Protocol for Ad hoc Networks", MobiCom 2002, Atlanta, Georgia, USA, September 23–28, 2002.