International Journal of Research in Science And Technology http://www.ijrst.com

(IJRST) 2013, Vol. No. 3, Issue No. IV, Oct-Dec **ISSN: 2249-0604**

SECURITY THREATS IN MOBILE AD HOC NETWORK

***Ujjal Agarwal, #Prof. K. P. Yadav, $Upendra Tiwari**

**Asstt. Lecturer, AL-MERGIB UNIVERSITY, AL-KHUMS, LIBYA*
#Director, SIET, Ghaziabad (UP), India
$Asstt. Prof., SIET, Ghaziabad (UP), India

ABSTRACT

Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. In this thesis, we identify the existent security threats an ad hoc network faces, the security services required to be achieved and the countermeasures for attacks in each layer. To accomplish our goal, we have done literature survey in gathering information related to various types of attacks and solutions, as well as we have made comparative study to address the threats in different layers. Finally, we have identified the challenges and proposed solutions to overcome them. In our study, we have found that necessity of secure routing protocol is still a burning question. There is no general algorithm that suits well against the most commonly known attacks such as wormhole, rushing attack etc. In conclusion, we focus on the findings and future works which may be interesting for the researchers like robust key management, trust based systems, data security in different layer etc. However, in short, we can say that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET.

Keywords: *Mobile Ad hoc Network, Security Threats, Link Layer, Application Layer, Countermeasure for Security Threats, Traffic, Distributed Coordination Function.*

INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one mobile node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multihop paths through the network to any other node. Idea of Mobile ad hoc network is also called infrastructureless networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly [2].

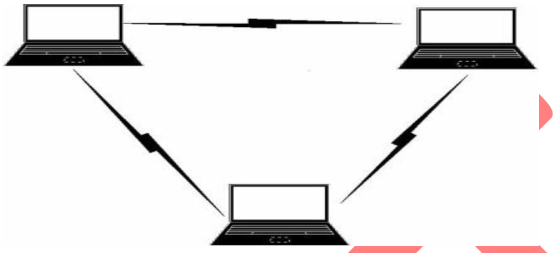


Figure 1: AD HOC NETWORK

Mobile ad hoc network (MANET) is one of the recent active fields and has received marvelous attention because of their self-configuration and self-maintenance capabilities [16]. A number of researches are done on security challenges and solutions in Mobile ad hoc network. Zhou and Haas have proposed using threshold cryptography for providing security to the network [18]. Hubaux et al. have defined a method that is designed to ensure equal participation among members of the ad hoc group, and that gives each node the authority to issue certificates [3]. Kong, et al. [8] have proposed a secure ad hoc routing protocol based on secret sharing;unfortunately, this protocol is based on erroneous assumptions While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Recent wireless research indicates that the wireless *MANET* presents a larger security problem than conventional wired and wireless networks. Mobile ad hoc networks have several unique set of challenges. Firstly, MANETs face challenges in secure communication. For example the resource constraintson nodes in ad hoc networks limit the cryptographic measures that are used for secure messages. Thus it is susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Secondly, mobile nodes without adequate protection are easy to compromise. An attacker can listen, modify and attempt to masquerade all the traffic on the wireless communication channel as one of the legitimate node in the network. Thirdly, static configuration may not be adequate for the dynamically changing topology in terms of security solution. Various attacks like *DoS* (Denial of Service) can easily be launched and flood the network with spurious routing messages through a malicious node that gives incorrect updating information by pretending to be a legitimate change of routing information. Finally, lack of cooperation and constrained capability is common in wireless *MANET* which makes anomalies hard to distinguish from normalcy. In general, the wireless *MANET* is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, and absence of central authorities, distribution cooperation and constrained capability [2].

Table 1: Security Attacks on each layer in MANET

Layer	**Attacks**
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP Weakness
Physical layer	Jamming, interceptions, eavesdropping

SECURITY THREATS

The security of the ad hoc networks greatly depends on the secure routing protocol, transmission technology and communication mechanisms used by the participating nodes. In this research, we have focused on the common attacks in *MANET and* the threats in each layer in the protocol stack and prescribe solution of those attacks.

a) Security Threats in Physical Layer

Physical layer security is important for securing *MANET* as many attacks can take place in this layer. The physical layer must adapt to rapid changes in link characteristics. The most common physical layer attacks in *MANET* are eavesdropping, interference, denialof- service and jamming. The common radio signal in *MANET* is easy to jam or intercept. Moreover an attacker can verhear or disrupt the service of wireless network physically. An attacker with sufficient transmission power and knowledge of the physical and medium access control layer mechanismscan gain access to the wireless medium. Here we will describe eavesdropping, interference and jamming attacks in brief.

b) Eavesdropping

Eavesdropping is the reading of messages and conversations by unintended receivers. The nodes in *MANET* share a wireless medium and the wireless communication use the RF spectrum and broadcast by nature which can be easily intercepted with receivers tuned to the proper frequency. As a result transmitted message can be overheard as well as fake message can be injected into the network.

c) Interference and Jamming

Jamming and interference of radio signals causes message to be lost or corrupt. A powerful transmitter can generate signal that will be strong enough to overwhelm the target signal and can disrupt communications. Pulse and random noise are the most common type of signal jamming [15].

d) Security Threats in Link Layer

The MANET is an open multipoint peer-to-peer network architecture in which the link layer protocols maintain one-hop connectivity among the neighbors. Many attacks can be launched in link layer by disrupting the cooperation of the protocols of this layer. Wireless medium access control (MAC) protocols have to coordinate the transmission of the nodes on the common communication or transmission medium. The IEEE 802.11 MAC protocol uses distributed contention resolution mechanisms which are based on two different coordination functions. One is Distributed Coordination Function (DCF) which is fully distributed access protocol and the other is a centralized access protocol called Point Coordination Function (PCF). For resolving channel contention among the multiple wireless hosts, DCF uses a carrier sense multiple access with collision avoidance or CSMA/CA mechanism.

e) Threats in IEEE 802.11 MAC

The IEEE 802.11 MAC is vulnerable to DoS attacks. To launch the DoS attack, the attacker may exploit the binary exponential back off scheme. For example, the attacker may corrupt frames easily by adding some bits or ignoring the ongoing transmission. Among the contending nodes, the binary exponential scheme favors the last winner which leads to capture effect. Capture effect means that nodes which are heavily loaded tend to capture the channel by sending data continuously, thereby resulting lightly loaded neighbors to backoff endlessly. Malicious nodes may take the advantage of this capture effect vulnerability. Moreover, it can cause a chain reaction in the upper level protocols using backoff scheme, like TCP window management [15].

f) Threats in IEEE 802.11 WEP

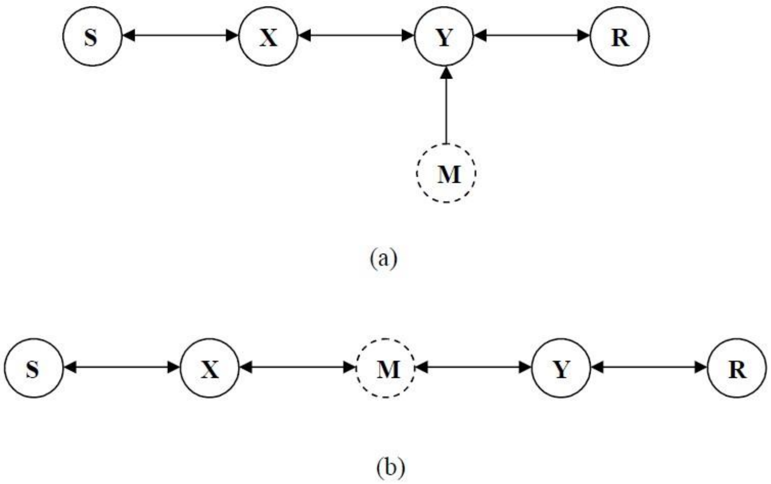
The first security scheme provided by IEEE 802.11 standards is Wired Equivalent Privacy (WEP). Basically, it was designed to provide security for WLAN. But it suffers from many design flaws and some weakness in the way RC4 cipher used in WEP. It is well known that WEPis vulnerable to message privacy and message integrity attacks and probabilistic cipher key recovery attacks.

g) Security Threats in Network Layer

In MANET, the nodes also function as routers that discover and maintain routes to other nodes in the network. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security in network layer plays an important role in the security of the whole network.

h) Network Layer Attacks

A number of attacks in network layer have been identified and studied in security research. An attacker can absorb network traffic, inject themselves into the path between the source and destination and thus control the network traffic flow. For example, as shown in the *figure (a) and (b),* a malicious node ***M*** can inject itself into the routing path between sender ***S*** and receiver ***R***.



(a)

(b)

Figure 2: ROUTING ATTACK

Network layer vulnerabilities fall into two categories: routing attacks and packet forwarding attacks [16]. The family of routing attacks refers to any action of advertising routing updates that does not follow the specifications of the routing protocols. The specific attack behaviors are related to the routing protocol used by the MANET.

i) Rushing Attack

In wormhole attack, two colluded attackers form a tunnel to falsify the original route. If luckily the transmission path is fast enough (e.g. a dedicated channel) then the tunneled packets can propagate faster than those through a normal multi-hop route, and result in the rushing attack. Basically, it is another form of denial of service (DoS) attack that can be launched against all currently proposed on-demand MANET routing protocols such as ARAN and Ariadne [5].

j) Blackhole Attack

The backhole attack is performed in two steps. At first step, the malicious node exploits the mobile ad hoc routing protocol such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting the packets.In second step, the attacker consumes the packets and never forwards. In an advanced form, the

attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected. In this way, the attacker falsified the neighboring nodes that monitor the ongoing packets. In *figure*, node 1 wants to send data packets to node 4 and initiates the route discovery process. We assume that node 3 is a malicious node and it claims that it has route to the destination whenever it receives RREQ packets, and immediately sends the response to node 1. If the response from the node 3 reaches first to node 1 then node 1 thinks that the routeDiscovery is complete, ignores all other reply messages and begins to send data packets to node
3. As a result, all packets through the malicious node is consumed or lost [2].

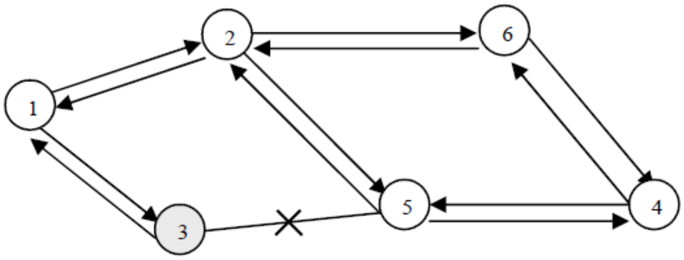


Figure 3. THE BLACK-HOLE PROBLEM

k) Rushing Attack

In wormhole attack, two colluded attackers form a tunnel to falsify the original route. If luckily the transmission path is fast enough (e.g. a dedicated channel) then the tunneled packets can propagate faster than those through a normal multi-hop route, and result in the rushing attack. Basically, it is another form of denial of service (DoS) attack that can be launched against all currently proposed on-demand MANET routing protocols such as ARAN and Ariadne [5].

l) Security Threats in Transport Layer

The security issues related to transport layer are authentication, securing end-to-end communications through data encryption, handling delays, packet loss and so on. The transport layer protocols in MANET provides end-to-end connection, reliable packet delivery, flow control, congestion control and clearing of end-to-end connection. Like TCP protocol in the Internet model, the nodes in a MANET are also vulnerable to the SYN flooding and session hijacking attacks. In the next sections, threats in transport layer are discussed in detail.

m) SYN Flooding Attack

The SYN flooding attack is also DoS attack which is performed by creating a large number of half-opened TCP connections with a target node. TCP connection between two communicating parties is established through completing three way handshakes which is described in the *figure*.

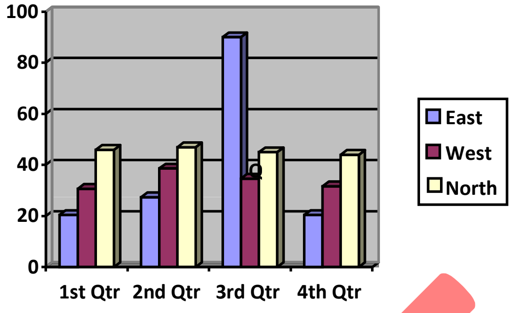


Figure 4. TCP THREE WAY HANDSHAKE

The sender sends a SYN message to the receiver with a randomly generated ISN (Initial Sequence Number). The receiver also generates another ISN and sends a SYN message includingthe ISN as an acknowledgement of the received SYN message. The sender sends acknowledgement to the receiver. In this way the connection is established between two communicating parties using TCP three way handshakes.

During SYN flooding attack, a malicious node sends a large amount of SYN packets to the target node, spoofing the return address of the SYN packets. When the target machine receives the SYN packets, it sends out SYN-ACK packets to the sender and waits for response i.e. ACK packet. The victim node stores all the SYN packets in a fixed-size table as it waits for the acknowledgement of the three-way handshake. These pending connection requests could overflow the buffer and may make the system unavailable for long time.

n) Security Threats in Application Layer

Applications need to be designed to handle frequent disconnection and reconnection with peer applications as well as widely varying delay and packet loss characteristics [13]. Like other layers application layer also vulnerable and attractive layer for the attacker to attack. Because this layer contains user data that supports many protocols such as SMTP, HTTP, TELNET and FTP which have many vulnerabilities and access points for attackers. The main attacks in application layer are malicious code attacks and repudiation attacks.

o) Malicious Code Attacks

Various malicious codes such as virus, worm, spy-wares and Trojan horse attack both operating systems and user applications that cause the computer system and network to slow down or even damaged. An attacker can produce this type of attacks in MANET and can seek their desire information [15].

p) Repudiation Attacks

The solution that taken to solve authentication or non-repudiation attacks in network layer or in transport layer is not enough. Because, repudiation refers to a denial of participation in the communication. Example of repudiation attack on a commercial system: a selfish person could deny conducting an operation on a credit card purchase or deny any on-line transaction [15].

COUNTERMEASURES FOR SECURITY THREAT

Security is a primary concern in MANET in order to provide protected communication between the communicating parties. It is essential for basic network functions like routing and packet forwarding. Network operation can easily be jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design [11]. Hence, a variety of security mechanisms have been developed to counter malicious attacks. There are some attacks such as man-in-middle attack which is known as a multi-layer attack. The countermeasures for this type of attack need to be implemented at different layers. For example, directional antennas [1] are used at the media access layer to defend against wormhole attacks while packet leashes [6] are used for network layer defense.

a) Countermeasures on Physical Layer Attacks

The physical layer of MANET is immune to signal jamming, DoS attack and also some passive attacks. Two spread spectrum technologies can be used to make it difficult to detect or jam signals. Spread spectrum technology changes frequency in a random fashion or spreads it to a wider spectrum which makes the capture of signal difficult. The FHSS (Frequency Hopping Spread Spectrum) makes the signal unintelligible duration impulse noise to the eavesdroppers. On the other hand, DSSS (Direct Sequence Spread Spectrum) represents each data bit in the original signal by multiple bits in the transmitted signal through 11-bit Barker code. However, both FHSS and DSSS pose difficulties for the malicious user while trying to intercept the radio signals. To capture and release the content of transmitted signal, the attacker must know frequency band, spreading code and modulation techniques. Still, there is a problem. These mechanisms are secure only when the hopping pattern or spreading code is unknown to the eavesdropper [15].

b) Countermeasures on Link Layer Attacks

The security issues that are closely related to link layer are protecting the wireless MAC protocol and providing link-layer security support. One of the vulnerabilities in link layer is its binary exponential backoff scheme which we described in fifth chapter 5.4 section. But recently a security extension to 802.11 proposed in [10]. The original 802.11 backoff scheme is slightly modified in that the backoff timer at the sender is provided by the receiver in stead of setting an arbitrary timer value on its own. As mentioned earlier, the threats of resource consumption(using NAV field) is still an open challenge though some schemes have been proposed such as

ERA-802.11[12]. Finally, the common known security fault in link layer is the weakness of WEP. Fortunately, the 802.11i/WPA [7] has mended all obvious loopholes in WEP and future countermeasures such as RSN/AESCCMP are also being developed to improve the strength of wireless security.

c) Countermeasures on Network Layer Attacks

Network layer is more vulnerable to attacks than all other layers in MANET. A variety of security threats is imposed in this layer. Use of secure routing protocols provides the first line of defense. The active attack like modification of routing messages can be prevented through source authentication and message integrity mechanism. For example, digital signature, message authentication code (MAC), hashed MAC (HMAC), one-way HMAC key chain is used for this purpose. By an unalterable and independent physical metric such as time delay or geographical location can be used to detect wormhole attack. For example, packet leashes are used to combat this attack [6]. IPSec is most commonly used on the network layer in internet that could be used in MANET to provide certain level of confidentiality. The secure routing protocol named ARAN protects from various attacks like modification of sequence number, modification of hop counts, modification of source routes, spoofing, fabrication of source route etc [14]. The research by Deng [2], et al presents a solution to overcome blackhole attack. The solution is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node.

d) Countermeasures on Transport Layer Attacks

One way to provide message confidentiality in transport layer is point-to-point or end-to end communication through data encryption. Though TCP is the main connection oriented reliable protocol in Internet, it does not fit well in MANET. TCP feedback (TCP-F) [4], TCP explicit failure notification (TCP-ELFN) [4], ad-hoc transmission control protocol (ATCP) [4], and ad hoc transport protocol (ATP) have been developed but none of them covers security issues involved in MANET. Secure Socket Layer (SSL) [9], Transport Layer Security (TLS) [9] and Private Communications Transport (PCT) [9] protocols were designed on the basis of public key cryptography to provide secure communications. TLS/SSL provides protection against masquerade attacks, man-in middle attacks, rollback attacks, and replay attacks.

e) Countermeasures on Application Layer Attacks

Viruses, worms, spywares, Trojan horses are the common and challenging application layer attacks in any network. Firewall provides protection against some of these attacks. For example, it can provide access control, user authentication, incoming and outgoing packet filtering, network filtering, accounting service etc. Anti-spyware software can detect spyware and malicious programs running on the system. Still using firewall is not enough because in certain situation the attacker even can penetrate firewall and make an attack. Another mechanism, Intrusion Detection System (IDS) is effective to prevent certain attacks such as trying to gain unauthorized access to a service, pretending like a legitimate user etc. The application layer also detects a DoS attack more quickly than the lower layers.

CONCLUSION

Mobile Ad Hoc Networks have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Whether ad hoc networks have vast potential, still there are many challenges left to overcome. Security is an important feature for deployment of MANET. In this research, we have overviewed the challenges and solutions of the security threats in mobile ad hoc networks. The first research question is „what are the vulnerabilities and security threats in MANET? Which level is most vulnerable to attack?‟ In our research, we present a variety of attacks related to different layers and find that network layer is most vulnerable than all other layers in MANET. This isolation of attacks on the basis of different layers makes easy to understand about the security attacks in ad hoc networks. The second question is „what are the countermeasures? How the security of the entire system is ensured?‟ We focus on the potential countermeasures either currently used in wired or wireless networking or newly designed specifically for MANET in our research. Wecan say that security must be ensured for the entire system since a single weak point may givethe attacker the opportunity to gain the access of the system and perform malicious tasks. The final research question is „what are the potential dangers that may be crucial in future?‟ Everyday, the attackers are trying to find out the new vulnerability in MANET. But it is sure that the multi-layer or combined attacks will be vital for secure communication in MANET.

REFERENCES

[1] S. Capkun, L. Buttyan, and J. Hubaux, "*Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks,"* 2003.

[2] H. Deng, W. Li, Agrawal, D.P., "*Routing security in wireless ad hoc networks,"* Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804

[3] J.-P. HuBaux, L. Buttyan, and S. Capkun., "*The quest for security immobile ad hoc network,"* In Proc. ACM MOBICOM, Oct. 2001.

[4] H. Hsieh and R. Sivakumar, "*Transport OverWireless Networks,"* Handbook of Wireless Networks and Mobile Computing, Edited by Ivan Stojmenovic. John Wiley and Sons, Inc., 2002.

[5] Y. Hu, A. Perrig, and D. Johnson, "*Ariadne: A Secure On-Demand Routing for Ad Hoc Networks,"* Proc. of MobiCom 2002, Atlanta, 2002.

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

[7] IEEE Std. 802.11i/D30, *"Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security,"* 2002.

[8] J. Kong et al., "*Providing robust and ubiquitous security support for mobile ad-hoc networks,"* In Proc. IEEE ICNP, pages 251–260, 2001.

[9] C. Kaufman, R. Perlman, and M. Speciner, "*Network Security Private Communication in a Public World,"* Prentice Hall PTR, A division of Pearson Education, Inc., 2002

[10] P. Kyasanur, and N. Vaidya, *"Detection and Handling of MAC Layer Misbehavior in Wireless Networks,"* DCC, 2003.

[11] P. Michiardi, R. Molva, "*Ad hoc networks security,"* IEEE Press Wiley, New York, 2003.

[12] A. Perrig, R. Canetti, J. Tygar, and D. Song, "*The TESLA Broadcast Authentication Protocol*," Internet Draft, 2000.

[13] R. Ramanathan, J. Redi and BBN Technologies, "*A brief overview of ad hoc networks: challenges and directions,"* IEEE Communication Magazine, May 2002, Volume: 40, page(s): 20-22, ISSN: 0163-6804

[14]K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, "*Secure routing protocol for ad hoc networks,"* In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. 12-15 Nov. 2002,
Page(s): 78- 87, ISSN: 1092-1648

[15] B. Wu, J. Chen, J. Wu, M. Cardei, "*A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,"* Department of Computer Science and Engineering, Florida Atlantic University,http://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf

[16] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "*Security in mobile ad hoc networks: challenges and solutions,"* In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume-11, Page(s): 38- 47, ISSN: 1536-128439

[17] S. Yi, P. Naldurg, and R. Kravets, "*Security-aware ad hoc routing for wireless networks,*" In Proc. ACM Mobihoc, 2001.