Detecting Adversary Location in Mobile Sensor Networks

[1] Pushadapu Venkata Pradeep , [2] Ch.Harika

[1]M.Tech Research Scholar, Department of CSE,
[2] Assistant Professor, Department of CSE
Priyadarshini Institute of Technology & Science, Chintalapudi, India

Abstract—*Mobile Ad-hoc networks (MANET) with wireless devices supporting multitude of mobile access technologies are witnessing increasing interest from network providers and consumers alike. Energy efficiency in such networks has become an important design consideration due to the limited battery life of mobile terminals on one side, and the ever increasing operational expenses pertaining to energy spending on the other. In this paper, we present a routing protocol for multi–mobile multi–hop wireless networks, which aims to achieve a trade–off between energy consumption in the network and routing delay, considering both the energy consumption at the devices and the link energy costs. We also present optimum route-path selection strategies by defining a utility function to minimize the energy consumption in the network while maximizing the network lifetime. Using simulations, we verify the utility of the route-path selection approaches and the efficiency of the energy aware routing algorithm. It turns out that the proposed protocol is energy efficient in terms of path selection, with a slight compromise in the end–to–end delay.*

Index Terms—Sybil attacks, mobile ad-hoc networks, Wireless security, location disclosure.

1. INTRODUCTION

Mobile ad hoc networking (MANET) is gradually emerging to be one of the more innovative and challenging area of wireless networking. MANETS consists of mobile nodes (MNs) with autonomously self-organizing capabilities in arbitrary and temporary network topologies, communicating over wireless links. MANETs have self-configuration and self-maintenance capabilities in which network topology may change rapidly and unpredictably over time due to the mobility of nodes. All the network activity including discovering the topology and messages delivery is executed by the nodes in Self/themselves. Routing functionality incorporated into the mobile nodes in MANETs. Peer-to-peer communication over multihop channels will be provided in MANETs through ensuring on-hop connectivity through link layer protocols and extending connectivity to multiple hops through network layer routing and data forwarding protocols. As the communication carried out over wireless links, contend with effects of radio communication, such as noise, fading and interference. In addition the links have less bandwidth than wired network. The wireless network is accessible to both legitimate users and malicious attackers making the network vulnerable, as there is no place to define traffic monitoring or access control. Hence security issues in MANETs rely on implicit trust relationship to route packets among participating nodes. The general security objectives like authentication, confidentiality, integrity, availability and non repudiation are to be addressed along with location confidentiality, cooperation fairness and absence of

traffic diversion. The provision of security services in MANET is dependent on the characteristics of the

supported application and the networked environment which may vary significantly. The unique characteristics

of mobile ad hoc networks pose a number of nontrivial challenges to the security design.

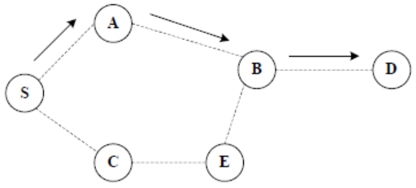


Figure 1. *Communication Between Nodes on MANETs*

Much research has been done to counter and detect attacks against existing MANET routing protocols, including work on secure routing protocols and intrusion detection systems. However, for practical Reasons the proposed solutions typically focus on a few particular security vulnerabilities since providing a comprehensive solution is non-trivial. If we are to develop more general solutions we must first have a comprehensive understanding of possible vulnerabilities' and security risks against MANETs. This is the main goal of this chapter. Section 2 presents the specific vulnerabilities of MANETs and the fundamentals of an exemplar routing protocol (AODV) to help understanding of the attacks given in Section 3. An overview of security solutions proposed to prevent and detect attacks on MANETs is presented in Section 4. Finally, ideas for future research are given.

2. MANET VULNERABILITIES

Mobile Ad-hoc network are more vulnerable in comparison to the traditional wired network due to their characteristics, which are to be discussed next.

A. Unreliability of wireless Link

Wireless links have a poor protection to noise, fading and signal interferences so routing related control message can be tampered. Also the wireless links have less bandwidth in comparisons to the wired networks. This makes the wireless links between mobile nodes in the ad hoc network inconsistent and unreliable for the communication participants [1].

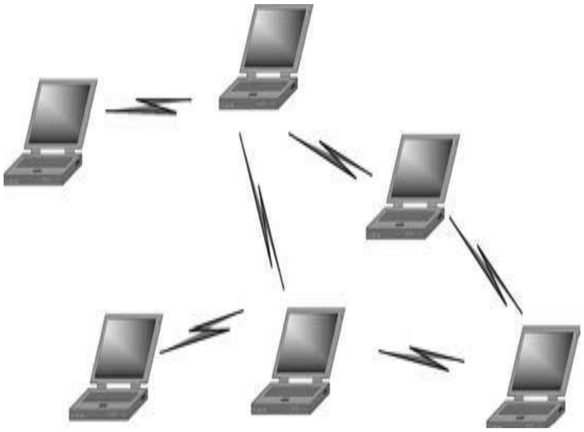


Figure 1.1: Structure of MANET

B. Dynamic topologies

In MANET nodes are free to move arbitrarily; and the network topology is typically multihop in nature. It may change randomly and rapidly at unpredictable time. As the MANET topology is changing frequently, it is necessary for each pair of adjacent nodes to incorporate in the routing issue to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol [1]. Here due to the mixing of several ad hoc networks there can be duplication of IP addresses making the impersonation attack to occur.

C. **Implicit trust relationship between neighbours**

Actual ad-hoc routing protocols suppose that all the participating nodes in the network are honest. This feature directly allows malicious a node to operate and try to paralyse the whole network, just by providing wrong information and spreading over the network [2].

D. Lack of Secure Boundaries As compared to traditional wired network, the mobile ad hoc network is more vulnerable which means self-evident. No such clear secure boundary in the MANET compared with the clear line of defence in the traditional wired network. In mobile ad hoc network nodes have freedom to join, leave and move inside the network? Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. Due to this mobile ad hoc network suffers from all attacks coming from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, making it even harder for the nodes in the network to resist. The attacks mainly include passive eavesdropping, active interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service [3].

E. Threats from Compromised nodes

Inside the Network in MANET mobile nodes are autonomous units that are free to join or leave the network, it becomes so difficult for the nodes themselves to make some effective policies which can prevent the possible malicious behaviours from all the nodes it communicate with because of the behavioral diversity of different nodes.

Furthermore, it is very difficult to track the malicious behavior performed by a compromised node especially in a large scale ad hoc network due to change in their attack target frequently because of their mobility aspect. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from

Outside the network and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised.

F. Unavailable Centralized Management Facility

Ad hoc networks do not have a centralized piece of management machinery such as a name server. Due to absence of centralized management facility each node is allowed to take its own decision and hence problems like detection of attacks, path breakages, transmission impairments and packet dropping, breakage of the cooperative algorithm take place.

G. Restricted Power Supply

MANET nodes are battery powered and for which energy must be conserved. For these nodes, the most important system design criteria for optimization may be energy conservation. The problem that may be caused by the restricted power supply is denial-of-service attacks [3]. Since the adversary knows that the target node is battery restricted, either it can continuously send additional packets to the target and ask it routing those additional packets, or it can induce the target to be trapped in some kind of time consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests since it has run out of power.

H. Scalability

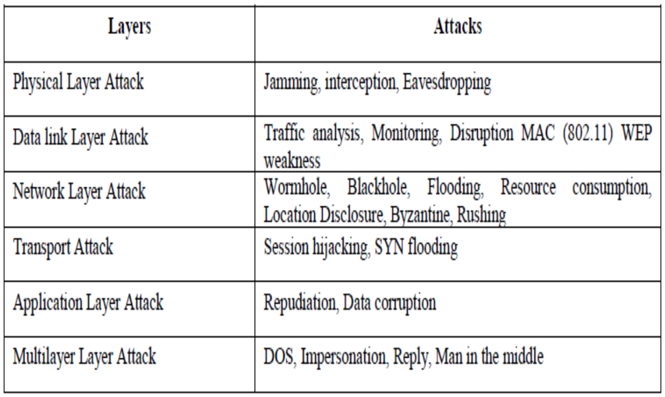
Scalability is the problem in the mobile ad hoc network [3]. Unlike the traditional wired network in that its scale is generally predefined and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, we cannot predict the number of nodes there will be in the future. As a result, the protocols and services applied to the ad hoc network such as routing protocol and key management services should be compatible to the continuously changing scaleof the ad hoc network.

3. TYPES OF ATTACKS IN MANET

Ad-hoc networks are more easily attacked than wired network. We can distinguish two kinds of attack: the passive attacks and the active attacks. In a passive attack, the operation of the protocol does not disrupted, but tries to discover valuable information by listening to traffic. Whereas, an active attack injects arbitrary packets and tries to disrupt the operation of the protocol in order to limiting availability, gaining authentication, or attracting packets destined to other nodes. In an attacker point of view attacks can be classified into three types Attacks Using Modification, Attacks using impersonation and Attacks using fabrication. Different types of attacks on different layers of protocol stack are shown in Table 3.1.

A. Physical Layer Attacks

1) Eavesdropping: Eavesdropping is a passive attack carried out by unintended receivers to intercept and read the messages and conversations during communication. The main idea is to obtain the confidential Information during the communication. In mobile ad hoc networks, mobile nodes share a wireless medium,



Layers	Attacks
Physical Layer Attack	Jamming, interception, Eavesdropping
Data link Layer Attack	Traffic analysis, Monitoring, Disruption MAC (802.11) WEP weakness
Network Layer Attack	Wormhole, Blackhole, Flooding, Resource consumption, Location Disclosure, Byzantine, Rushing
Transport Attack	Session hijacking, SYN flooding
Application Layer Attack	Repudiation, Data corruption
Multilayer Layer Attack	DOS, Impersonation, Reply, Man in the middle

Table 3.1: Classification of different types of attacks on different layers of protocol stack.

Table 3.1: Classification of different types of attacks on different layers of protocol stack.

which basically uses the RF spectrum and broadcast by nature of communication. Signals which broadcast over wireless can be easily analysed and intercepted to reveal some information about the network, with receivers tuned to the proper frequency [4] [5] in comparison to wired medium.

2) Jamming: Jamming is a active attack in which radio signals can be jammed or interfered causing the message to be corrupted or lost [4] [5]. If the attacker has a powerful transmitter or a jammer device, a strong enough signal can be generated to overwhelm the targeted signals disrupting communication between two interacting nodes. Random noise and pulse are the most common type of signal jamming.

3) Interception: Signals broadcast over the wireless can be easily monitored and intercepted with intruders tuned to that communication frequency [4] [5]. In active interception the messages transmitted can be overheard by the intruder, and afterwards may inject fake messages into network on the user's behalf where as in passive interception the network traffic is routinely monitored to collect qualitative information, such as communication

volume, or other information not explicitly communicated via a data stream.

B. Link Layer Attacks

1) Traffic Monitoring and Analysis: Traffic monitoring and analysis is not an actual attack, but further it may lead to various vulnerable attacks. Via traffic monitoring and analysis an attacker may receive information about the communicating users present within the network like their identity, geographical locations, network topology, and their communication functionalities like communicating bandwidth, time of communication etc. Such information allows a malicious node to attack a victim node easily with high efficiency. Hence the traffic monitoring and analysis may not be an attack itself but to be considered as a massive threat in MANET.

2) Disruption in MAC: Current wireless MAC protocol is based upon the implicit trust relationship between the nodes. The selfish nodes may deny in the participation of packet forwarding or drop packets to

consume battery power or unfair sharing of bandwidth. Similarly the malicious nodes disrupt the normal operations of contention-based or reservation-based MAC protocol.

3) Weakness of 802.11 WEP: IEEE 802.11 WEP incorporates wired equivalent privacy (WEP) for providing modest level of privacy to WLAN systems a by encryption of radio signals. 802.11 WEP standards support WEP 40 bit cryptographic keys, where as 104bit and 128 bits are already implemented. As WEP is having a number of weaknesses [6] [7] [8] it is broken and is replaced by AES in 802.11.

C. Network Layer Attacks

1) Wormhole Attack: Wormhole attacks are also known as tunneling attack in which the attacker receives packets at one region in the network and tunnels them to another location within or outside of the network, and replays the packets there. This tunnel between two colluding attackers is called a wormhole [9] [10] [11 and made of a wired or long range wireless link. Wormhole attacks can be easily implemented but very hard to detect. Wormhole attack can be classified as hidden attacks and exposed attacks. In hidden attacks attacker nodes don't realize their identity to the communicating nodes by hiding their MAC address during updating of packet header. In exposed attack, packet includes the attacker nodes identity and they communicate as legitimate nodes without any modification to the content of the packet. Wormhole attacks are launched in MANET using several modes like; using encapsulation, using out-

of-bound channel, using packet relay, with high power transmission, using protocol deviation techniques.

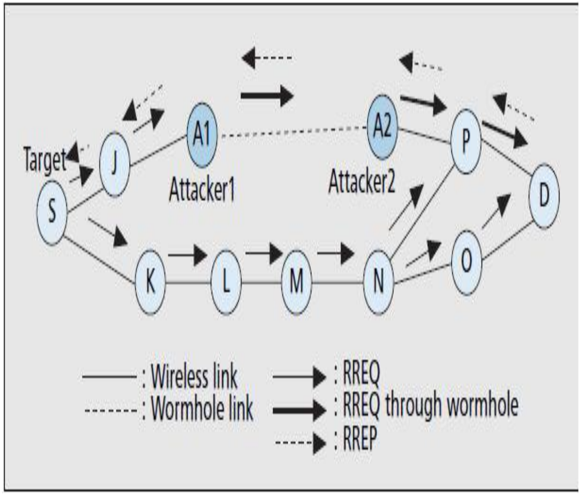
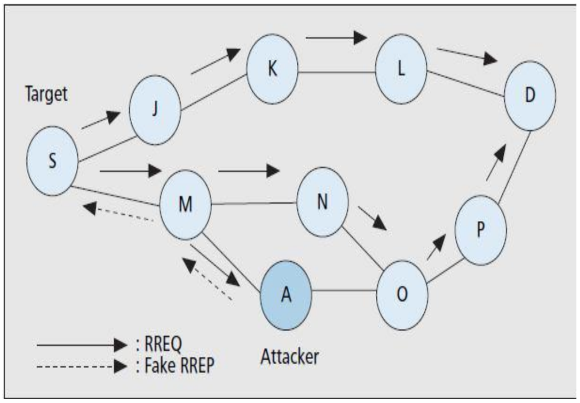


Figure 3.1: Wormhole Attack

2) Black hole Attack: The black hole attack has two properties. First, the 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 packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks [12].



3.2: Black hole Attack

3) Rushing Attack: Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunnelled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack [13].

4) Byzantine Attack: A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services [14].

5) Routing Messages Flooding Attack: Flooding attacks are basically classified into two types as control packet flooding (hello flooding, RREQ flooding and RREP flooding) and data packet flooding, which have the goal to disrupt the routing discovery or the maintenance phase within MANET. In flooding attack a malicious node/an attacker's main goal is to exhaust the network resources like network bandwidth and consume the resources of an authentic network user like computational and battery power. Furthermore influencing the network performance, by hindering the proper execution of routing algorithm during route discovery [15][16]. Using RREQ or RREP flooding a malicious node causes the routing table overflow and prevents the creation of actual routes by sending multiple RREQ or RREP packets to nonexistent recipients on a very short interval of time. Hello flooding is a active attack [17] in which a malicious node floods Hello packets unnecessarily to result in congestion and preventing its neighbor to receive other packets.

6) Resource Consumption Attack: This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node [18].

7) Location Disclosure Attack: An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios. Traffic analysis, one of the subtlest security attacks against MANET, is unsolved. Adversaries try to figure out the identities of communication parties and analyse traffic to learn the network traffic pattern and track changes in the traffic pattern.

D. Transport Layer Attacks

1) SYN Flooding Attack: In SYN flooding attack main goal of attacker is to create a multiple number of half opened TCP connections as a legitimate user, but never completes the synchronization process by completing the handshake to fully open the connection [19]. In this attack adversary node using flooding via synchronization of packets, exhausts the resources of an authentic node. This attack makes an authentic node fail to initialize any new connection.

2) Session Hijacking: In session hijacking attack an attacker tries to get the identity (IP address) of the victim node [19]. Initially attacker determines the particular sequence which is expected by the target node by spoofing the IP address of the victim. Then attacker tries to perform a DoS attack on the victim node and thinks to continue the session with the target node.

E. Application Layer Attacks

1) Repudiation Attack: Repudiation attack happens when application/system doesn't control or tracks log users' actions, permitting vulnerable manipulations and forging the identifications of new actions. Encryption mechanisms and firewalls used in various layers are insufficient for providing security to packets. This attack leads to manipulation of data stored on log files making it invalid or misleading. Basically repudiation attack refers to a user denying about his participation in an action or a transaction.

2) Data Corruption: The application layer supports many protocols such as HTTP, SMTP, and FTP which includes malicious codes. Malicious codes are spread over the network widely and can affect both operating system and user data or programs. Malicious codes are nothing but a part of software system or script that causes undesired effects, security breaches or damage to computer system. These include viruses, worms, Trojan Horses, backdoors malicious active contents.

F. Multi-Layer Attacks

1) Denial-of-Service (DOS): Another type of packet forwarding attack is the denial-of-service (DOS) attack via network-layer packet blasting, in which the attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks.

2) Impersonation Attack: A malicious node can precede an attack by altering its MAC or IP address in the control message or persuade nodes to change their routing tables pretending to be a friendly node. It is treated as the initial case in most of the attacks and further goes for more sophisticated attacks.

3) Man-in-the-middle Attack: An attacker sits between the sender and the receiver and sniffs any information being sent between two ends.

4. SECURITY ATTRIBUTES

MANET Security can be described by the analysis of certain attributes. These attributes are described thoroughly in this section.

A. Availability

The term Availability means the ability to provide services at any situation without considering its security state [3]. DoS attack mostly affects this attribute.

B. Integrity

Integrity of a message guarantees its identity during transmission. Integrity can be compromised mainly in two ways; malicious altering and Accidental altering. In malicious altering, a message can be removed, replayed or revised by an adversary with malicious goal; on the other hand, a message is lost or its content is changed due to some benign failures, which may be transmission errors during communication or hardware errors such as hard disk failure occurs in accidental altering.

C. Non-repudiation

Non-repudiation is related to a fact that if a node sends a message, later that node cannot deny that the message was sent by it. By producing a signature for the message, we can maintain non-repudiation. In public key cryptography, a node A signs the message using its private key. All other nodes can verify the signed message by using A's public key, and A cannot deny about the message.

D. Confidentiality

Confidentiality indicates that certain information's are only accessible to their authorized entities and never disclosed to unauthorized entities.

E. Authenticity

Authenticity assuring participation of genuine participants in communication and not impersonators [3]. The communication participants must prove their identities to avoid authorized access to resources and sensitive information.

F. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority.

G. Access control

The goal of access control is to prevent unauthorized use of network services and system resources. It governs the way the users can have accesses to data. Access control mechanism tied to authentication attributes. Access control involves the mechanism for forming a group of nodes, communicating a new logged node with other nodes present before in the network etc.

H. Anonymity

Anonymity means that all the information that can be used to identify the owner of the node should be kept private and not be distributed by the node itself or the system software for protecting the privacy of the node from arbitrary disclosure to any other entities.

5. Future Directions for Research

Given their flexibility MANETs are very attractive for military and disaster recovery applications.

Moreover mobile devices are getting smaller, cheaper, more powerful and more mobile every day. In the future MANETs will likely be a part of our lives. There has been much research on this promising new networking. Security is one of the hot topics in the area due to new security threats MANETs have introduced. The threats to MANETs have been examined in many research papers. However more research needs to be done on identifying new security threats. We believe that with the increase in the use of MANETs, new intrusions are going to emerge continuously. Since conventional security solutions are not easily applicable to MANETs, new solutions have been proposed for the last decade, which is far fewer than proposed approaches for conventional networks. 16 None of the proposed systems are necessarily the best solution taking into account different applications which they can have their own requirements and characteristics. They also usually consider few specific attacks and target a specific routing protocol. Furthermore they emphasize just a few specific MANET features. For instance the consequences of having limited resources is generally little explored.. Some solutions might not be suitable for some nodes which can have limited computational capabilities and resources. Researchers can develop solutions considering different characteristics of these nodes. Cooperation and communication between nodes is another area need to be explored. Proposed network architectures should not introduce new weakness/overheads to the system. To conclude, researcher should focus on developing solutions suitable to MANETs' specific features.

A. Secure Message Transmission (SMT)

SMT (secure Message Transmission) protocol combines end-to-end secure and robust mechanism, dispersion of transmitted data, simultaneous usage of multiple paths and adapting the dynamic changes in the network. SMT mainly supports quality of service (QoS) for real time traffic. In SMT source and destination nodes employ a secure communication in between them by authenticating each other. Then a set of diverse paths are found in between the source and destination node from the current network topology. Sources disperse a message into N number of pieces [36] and transmit them across the paths, so that destination can reconstruct the original dispersed message by combining successfully received pieces. Each dispersed piece assigned with a MAC [37] or verifying its integrity, reply protection and authenticity of origin. Destination acknowledges each successfully received message piece by a feedback to the source. If sufficient number of pieces are received successfully at the destination then the message is reconstructed, otherwise I awaits for the missing packet that are retransmitted by the source. Source re-encodes and re-allocates the undelivered messages over the path set for the transmission. The end nodes need to be successfully associated to each other, where as none of them needs to be securely associated with any of the remaining nodes in the network. As a result no cryptographic operations are needed at the intermediate nodes. Using feedback mechanism, a successfully received piece implies route to be operational while a failure indicates the route to be broken or compromised.

B. Intrusion Detection Techniques

An Intrusion Detection System [38] (or IDS) generally detects unwanted manipulations to systems [39]. In IDS basically two types of models are implemented; anomaly detection and misuse detection [40]. It works in three basic steps; to control the collection of data (monitor), decides the data collected indicates an intrusion or not (analyze), and manages the response action to the intrusion (response). Intrusion Detection may work in a distributive or cooperative environment for MANET. Each mobile node in a MANET has an individual IDS agent running independently to monitor local activities and identify possible intrusions. Various solutions are proposed to address intrusion detection in MANET[41].

C. Message Authentication Primitives

1) MAC (message authentication codes): MAC algorithms referred as keyed hash functions [42] as they use one way hash function and take a secret key as argument to produce a fixed length output from an arbitrary length input message. For two nodes with a shared secret key K, a authentication tag T=MACk(P) is generated

for message P using key K by the sender and(P,T) pair is sent to the receiver. Using the same key K and the authentication tag the message pair is verified on the receiver side, assuring authentication to the legitimate

users only.

2) CMAC: CMAC[43] is a derived version of CBC-MAC[44] (Cipher-Block-Chaining) in which the plaintext or the input message is broken into N block encrypted iteratively and XORed with next block until the last block. The last block is XORed with two key dependent constants to yield a authentication tag. Here the message size must be known before the computation of the tag and for each message of different length additional encryption needed.

3) PMAC1 (parallelizable MAC version 1):

PMAC1[45] is a refined version of PMAC [46], in which offsets re generated though finite field multiplications of an ffset seed R. further variants of this are propose to be iPMAC[47] which is supporting faster ad word oriented generation of offset. 4) GMAC (galois MAC): GMAC [48] is a variant of the GCM[48] authenticated encryption which follows Carte-Wegman design [49] to reduce the amount of processing for its operation. GMAC are difficult to implement a main focused for powerful platforms. I. Digital Signature in RSA like symmetric cryptographic schemes much more computations are needed for the signing and Verifying operations of a signature. An attacker node floods victim node with a large number of bogus signatures, exhausting victims computational resources used for verification purpose. Along with that a certificate of revocation (CRL) must have to be kept with each node. Whereas digital signature scheme uses symmetric key cryptography and can be verified by any node that knows the public key of signing node. Same number of public/private key pairs needed as the size of the network, which makes digital signature scalable to a large number of receivers. It provides more resilience against DOS attacks and the digital signature approach used by SAODV [50] protocol.

6. CONCLUSIONS

In this chapter we have examined the main security issues in MANETs. They have most of the problems of wired networks and many more besides due to their specific features: dynamic topology, limited resources (*e.g.* bandwidth, power), lack of central management points. Firstly we have presented specific vulnerabilities of this new environment. Then we have surveyed the attacks exploit these vulnerabilities and, possible proactive and reactive solutions proposed in the literature. Attacks are classified into passive and active attacks at the top level. Since proposed routing protocols on MANETs are insecure, we have mainly focused on active routing attacks which are classified into dropping, modification, fabrication, and timing attacks. Attackers have also been discussed and examined under insider and outsider attackers. Insider attacks are examined on our exemplar routing protocol AODV. Conventional security techniques are not directly applicable to MANETs due to their very nature. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs. In this chapter we summarize secure routing approaches proposed for MANETs. The difficulty of key management on this distributed and cooperative environment is also discussed. Furthermore we have surveyed intrusion detection systems with different detection techniques proposed in the literature. Each approach and technique is presented with attacks they can and cannot detect. To conclude, MANET security is a complex and challenging topic. To propose security solutions well-suited to this new environment, we recommend researchers investigate possible security risks to MANETs most thoroughly.

REFERENCES

1] Zaiba Ishrat, "Security issues, challenges & solution in MANET", IJCST Vol. 2, Issue 4, Oct . - Dec. 2011.

[2] Praveen Joshi," Security issues in routing protocols in MANETs at network layer", Elsevier, Procedia Computer Science 3 (2011) 954–960.

[3] Amitabh Mishra, Ketan M. Nadkarni, "Security in Wireless Ad Hoc Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[4] T. Karygiannis and L. Owens, Wireless Network Security-802.11, Bluetooth and Handheld Devices.National Institute of Standards and Technology. Technology Administration, U.S Department of Commerce, Special Publication 800-848, 2002.

[5] R. Nichols and P. Lekkas, Wireless Security-Models, Threats, and Solutions, McGraw-Hill, Chapter 7,2002.

[6] W. Stallings, Wireless Communication and Networks, Pearson Education, 2002.

[7] N. Borisov, I. Goldberg and D.Wagner, "Interception Mobile Communications: The Insecurity of 802.11.",Conference of Mobile Computing and Networking, 2001.

[8] T. Karygiannis and L. Owens, "Wireless Network Security-802.11, Bluetooth and Handheld Devices"National Institute of Standards and Technology. Technology Administration, U.S Department of Commerce, Special Publication, pp. 800-848, 2002.

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

[10] Rashid Hafeez Khokhar; Md Asri Ngadi; Satria Mandala. "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, 2:12, 2008. In Proceedings of IEEE INFOCOM'03, 2003.

[11] Preeti Nagrath, Bhawna Gupta, "Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A Survey", Vol. 6, pp. 245 – 250, International Conference on Electronics Computer Technology (ICECT), IEEE, 2011.

[12] H.Yang, X. Meng, S. Lu,"Self-Organized Network Layer Security in Mobile Ad Hoc Networks," ACM Workshop on Wireless Security (WiSe), 2002.

[13] Y. Hu, A. Perrig, and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", Proc. of the ACM Workshop on Wireless Security (WiSe), pp. 30-40, 2003.

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

[15] 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.

[16] Mihaela Cardei; BingWu; Jianmin Chen; JieWu. "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, page 38, 2006.

[17] Hamid, A., M.O. Rashid and C.S. Hong, "Routing security in sensor network: HELLO flood attack and defense", IEEE ICNEWS, pp. 2-4, 2006.

[18] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, “Security in mobile ad hoc networks: Challenges and solutions”, IEEE Wireless Communications, pp. 38-47, 2004.

[19] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks”, Wireless Network Security, Part II, pp. 103-135, 2007.

[20] Y. Hu, A. Perrig, D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks", ACM Wireless Security 2006.

[21] Perrig, R. Canetti, J. Tygar, and D. Song, “The TESLA Broadcast Authentication Protocol”, Internet Draft, 2000.

[22] Y. C. Hu, A. Perrig, and D.B. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in Proceedings of the 22nd INFOCOM, pp. 1976-1986, 2003.

[23] T. V. Phuong, N. T. Canh, Y.-K. Lee, S. Lee, and H. Lee, “Transmission time-based mechanism to detect wormhole attack,” In the proceedings of the IEEE Asia-Pacific service computing conference, pp. 172-178,2007,.