A Survey of Layer Specific and Cryptographic primitive attacks and their countermeasures in MANETS

Sapna Boora[1], Sonia Ohri[2]

[1,2] *Department of Computer science , Maharishi Markandeshwar university Mullana -Ambala ,India*

***Abstract*—** Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. In MANET nodes which are within the range of each other can connect directly where as nodes which are not in the vicinity of each other rely on the intermediate node for communication. Each node in MANET can work as a sender, receiver as well as router. Communication in the network depends upon the trust on each other. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANETs).These attacks actually need some counter measures so that these attacks can be avoided. The hackers attacks are reduce the capacity and efficiency of network in MANET. In this paper we have studied how various layer specific attacks and cryptographic primitive attacks affects the performance of the network then we have also presented their countermeasures that can be taken to avoid them .

Keywords— MANET ,WEP ,DSSS,FHSS

I INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies [1]. Mobile ad hoc networks are collection of wireless networks, which consists of large number of mobile nodes. Nodes in MANETs can join and leave the network dynamically. There is no fixed set of infrastructure and centralized administration in this type of networks. Nodes are interconnected through wireless interface. The dynamic nature of such type networks makes it highly susceptible to various link attacks. The basic requirements for a secured networking are secure protocols which ensure the confidentiality, availability, authenticity, integrity of new attacks can be reduced. The mobile hosts dynamically establish paths among one another in order to communicate. Therefore, the success of MANET communication highly relies on the collaboration of the involved mobile nodes. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

Confidentiality: Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediates nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

Availability: Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services.

Authentication: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes

.**Integrity:** Message being transmitted is never altered

.**Non-repudiation:** Ensures that sending and receiving parties can never deny ever sending or receiving the message.

A. Vulnerabilities of MANETs

- Dynamic Topology: In MANETs, nodes can join and leave the network dynamically and can move independently [2]. Due to such type nature there is no fixed set of topology works in MANETs. The nodes with inadequate physical protection may become malicious node and reduce the network performance

- Wireless Links: As the nodes in such networks are interconnected through wireless interface that makes it highly susceptible to link attacks. The bandwidths of wireless networks are less as compared to wired networks, which attracts many attackers to prevent normal communication among nodes.
- Cooperativeness: In MANETs, all routing protocols assume that nodes provide secure communication. But some nodes may become malicious nodes which disrupt the network operation by changing routing information etc [1].
- Lack of clear line of defence: There is no clear line of defence mechanism available in the MANETs; attacks can come from any directions. Attackers can attack the network either internally or externally.

• Limited resources: The MANETs consists of different set of devices such as laptops, computers, mobile phones etc. All of such devices having different storage capacity, processing speed, computational power etc. This may attracts the attackers to focus on new attacks.

B. Merits of MANET

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.
- These networks work without any pre-existing infrastructure.

C. Demerits of MANET

- Limited resources: Limited resource invokes the problem of limited security
- Lack of authorization facilities: Intrinsic mutual trust is vulnerable to attacks
- Time varying topology: Volatile, changing network topology makes it hard to detect malicious nodes.
- Security protocols for wired network can not work for ad- hoc networks

II CLASSIFICATION OF ATTACKS

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks.

1. Attacks on the basic mechanisms of ad-hoc network such as Routing and these attacks can be prevented using cryptographic algorithms.
2. Attack on security mechanisms and key management mechanisms.

A. On the basis of nature

1.)Passive attacks: In passive attack there is not any alteration in the message which is transmitted. There is an attacker (intermediated node) between sender & receiver which reads the message. This intermediate attacker node is also doing the task of network monitoring to analyse which type of communication is going on.

2.)Active attacks : The information which is routing through the nodes in MANET is altered by an attacker node. Attacker node also streams some false information in the network. Attacker node also do the task of RREQ (re request) though it is not an authenticated node so the other node rejecting its request due these RREQs the bandwidth is consumed and network is jammed.

B. On the basis of domain

1.)External attacks: In external attack the attacker wants to cause congestion in the network this can be done by the propagation of fake routing information. The attacker disturbs the nodes to avail services.

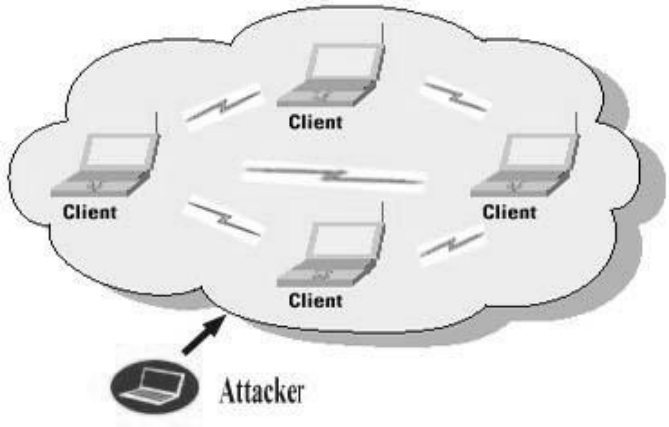

Fig 1 External Attack

2.) Internal attacks: In internal attacks the attacker wants to gain the access to network & wants to participate in network activities. Attacker does this by some malicious impersonation to get the access to the network as a new node or by directly through a current node and using it as a basis to conduct the attack.

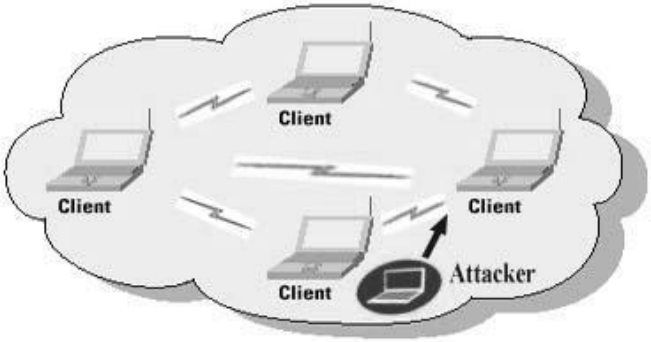

Fig 2 Internal Attack

III LAYER SPECIFIC ATTACKS

The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack.

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding, jellyfish attack
Network layer	Wormhole, blackhole, Byzantine, Sinkhole, Link spoofing, Rushing Attack, Replay attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping

Table 1 Description Of Layer Specific Attacks

A. Attacks on physical layer

The attacks on physical layer are hardware oriented and they need help from hardware sources to come into effect [4]. These attacks are simple to execute as compared to other attacks. They do not require the complete knowledge of technology. Some of the attacks identified at physical layer include eavesdropping, interference, and jamming etc.

1.)Eavesdropping : Eavesdropping can also be defined as interception and reading of messages and conversations by unintended receivers [4]. As the communication takes place on wireless medium can easily be intercepted with receiver tuned to the proper frequency. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication. The information may include private key, public key, location or passwords of the nodes. Classified data can be eavesdropped by tapping communication lines, and wireless links are easier to tap.

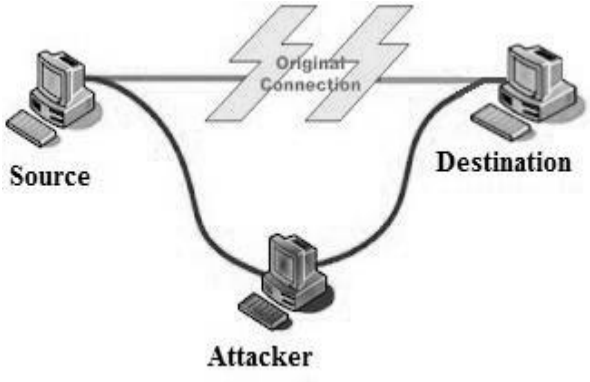

Fig 3 Eavesdropping

2.) Jamming : Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.

3.)Active Interference : An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications. The effects of such attacks depend on their duration, and the routing protocol in use [1]. Attacker can change the order of messages or attempt to replay old messages. Old messages may be replayed to reintroduce out of date information.

Countermeasures for 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.

B. Attacks on Mac layer

The algorithms used in data link layer/MAC layer are susceptible to many DoS attacks. MAC layer attacks can be classified as to what effect it has on the state of the network as a whole. The effects can be measured in terms of route discovery failure, energy consumption, link breakage initiating route discovery and so on. The misbehavior of a node can be purely in selfish interest or with malicious intents.

1.)Selfish Misbehavior of Nodes: Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of the network [1]. It may include two important factors.

- Conservation of battery power
- Gaining unfair share of bandwidth

The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources. These attacks exploit the routing protocol to their own advantage. Packet dropping is one of the main attacks by selfish node which leads to congestion in network. However most of routing protocols have no mechanism to detect whether the packets being forwarded or not except DSR (dynamic source routing).

2.)Traffic analysis and monitoring: Traffic analysis is a passive type of attack in nature this kind of analysis is done by attacker to find out which type of communication is going on. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self organization in the network, and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information.

- Location of nodes
- Network topology used for communication
- Roles played by nodes
- Available source an destination nodes

3.) WEP targeted attacks: The wired equivalent privacy (WEP) is designed to enhance the security in wireless communication that is privacy and

authorization. However it is well known that WEP has number of weaknesses and is subject to attacks. Some of them are:-

1. WEP protocol does not specify key management.
2. The initialization vector (IV) is a 24 bit field which is the part of the RC4 encryption key. The reuse of IV and weakness of RC4 help to produce analytic attacks.
3. The combined cure of non cryptographic integrity algorithm, CRC32, with the stream cipher has a security risk .

Countermeasures for Mac 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 back off scheme . The original 802.11 back off scheme is slightly modified in that the back off 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.The common known security fault in link layer is the weakness of WEP.The 802.11i/WPA 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. Attacks on network layer

The network layer protocols enable the MANET nodes to be connected with another through hop-by-hop. In MANETs every individual node takes route decision to forward the packet, so it's very easy for malicious node to attack on such network. The basic idea behind network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic. In such attacks, the attackers can create routing loops to form severe congestion. Different type of attacks are identified which are initiated by malicious node. The malicious node "X" can absorb important data by placing itself between source "A" and destination "D" as shown in fig 4. "X" can also divert the data packets exchanged between "A" and "D", which results in significant end to end delay between "A" and "D". In this type of attacks attackers attacks against Routing and Path.

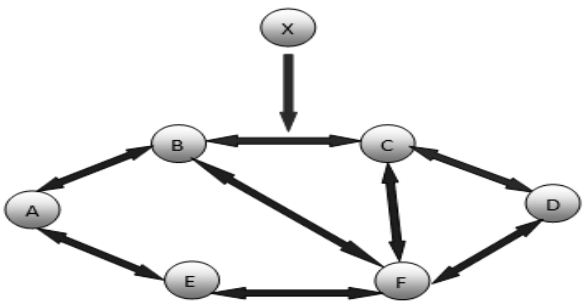

Fig 4 Detection of Malacious Node

1) Blackhole Attack: In a blackhole attack a attacker node sends fake routing information in the network to claims that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example in an Ad-Hoc on demand distance vector routing (AODV), attacker can send fake RREQs including a fake destination sequence number that is fabricated to be equal or higher than the one contain in the RREQ to source node, claiming that it has a sufficient fresh route to the destination node. This causes the source node to select the route that passes through the attacker node. Therefore all the traffic will be routed through the attacker and therefore, the attacker can misuse the information or sometime discard the traffic [4].

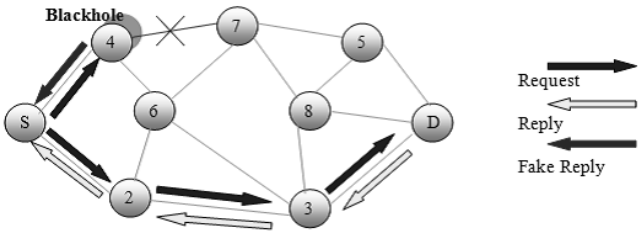

Fig 5 Blackhole Attack

2) Wormhole Attack : It is the dangerous one among the all attacks. In this attack, a pair of colluding attackers recodes packets at one location and replays them at another location using a private high speed network [2]. The seriousness of this attack is that it can be launched in all communication that provides authenticity & confidentiality.

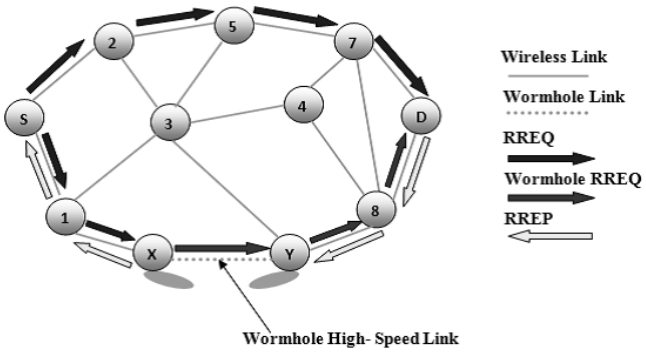

Fig 6 **:** Wormhole Attack

3) Sinkhole Attack **:** Sinkhole attack is one of the severe attacks in wireless Ad hoc network. In sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving whole network traffic it modifies the secret information, such as changes made to data packet or drops them to make the network complicated. A malicious node tries to attract the secure data from all neighboring nodes. Sinkhole attacks affects the performance of Ad hoc networks protocols such as AODV by using flaws as

maximizing the sequence number or minimizing the hop count [2]. In this way the path presented through the malicious node appears to be the best available route for the nodes to communicate. In DSR protocol, sinkhole attack modifies sequence no in RREQ.

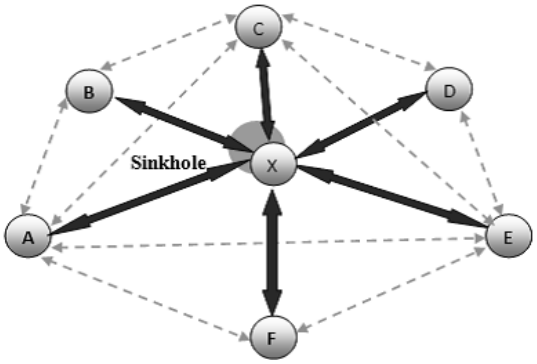

Fig 7 Sinkhole Attack

4) Link Withholding & Link Spoofing Attacks: In link withholding attack, the malicious node does not broadcast any information about the links to specific nodes. It results in losing the links between nodes. In Link spoofing attacks, a malicious node broadcasts or advertises the fake route information to disrupt the routing operation [7]. It results in, malicious node manipulate the data or routing traffic.

5) Sybil Attack : In Sybil attack, Sybil attacker may generate fake identities of number of additional nodes. In this, a malicious node produces itself as a large number of instead of single node. The additional identities that the node acquires are called Sybil nodes. A Sybil node may fabricate a new identity for itself or it steals an identity of the legitimate node. Various effects due to presence of Sybil attacks are:

- In the presence of Sybil nodes in network, it may make difficult to identify a misbehaving node.
- Sybil attacks prevent fair resource allocation among the nodes in network.
- In certain application, sensors can be used to perform voting for decision making. Due to presence of duplicate identities the outcome of voting process may vary.
- Sybil nodes affect the normal operation of routing protocols by appearing itself at various locations in network.

Countermeasures for 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. 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. The research by Deng , 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. *Attacks on transport layer*

1) Session Hijacking : Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DoS attacks. In Session hijacking, the malicious node tries to collect secure data (passwords, secret keys, logon names etc) and other information from nodes. Session hijacking attacks are also known as address attack which make affect on OLSR protocol.

2) SYN Flooding Attack : The SYN flooding attacks are the type of Denial of Service (DoS) attacks, in which attacker creates a large number of half opened TCP connection with victim node. These half opened connection are never completes the handshake to fully open the connection.

3) Jelly Fish attack :The attacker disrupts the TCP connection which was established for communication. A jelly fish attacker needs to intrude into forwarding group and then it delays data packets unnecessarily for some amount of time before forward them. Due to this attack a high end to end delay & delay jitter is happened. So the performance of real time applications becomes worst.

Countermeasures for 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), TCP explicit failure notification (TCP-ELFN), ad-hoc transmission control protocol (ATCP), and ad hoc transport protocol (ATP) have been developed but none of them covers security issues involved in MANET.
Secure Socket Layer (SSL), Transport Layer Security (TLS) and Private Communications Transport (PCT) 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. Attacks on application layer

1) Malicious code attacks : Malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application.

2) Repudiation attacks : Repudiation refers to a denial of participation in all or part of the communications. Many of encryption mechanism and firewalls used at different layer are not sufficient for packet security. Application layer firewalls may take into account in order to provide security to packets against many attacks. For example, spyware detection software has been developed in order to monitor mission critical services.

Countermeasures for application layer attacks

Viruses, worms, spywares, trozan 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.

IV CRYPTOGRAPHIC PRIMITIVE ATTACKS

Cryptography is an important and powerful security tool. It provides security services ,such as authentication, confidentiality, integrity, and non-repudiation. In all likelihood, there exist attacks on many cryptographic primitives that have not yet been discovered. There could be new attacks designed and developed for hash functions, digital signatures, both block and stream ciphers. Most security holes are due to poor implementation, i.e. weakness in security protocols. For example, authentication protocols and key exchange protocols are often the target of malicious attacks. Cryptographic primitives are considered to be secure, however, recently some problems were discovered, such as collision attacks on hash function, e.g. SHA-1 [1]. Pseudorandom number attacks [1], digital signature attacks and hash collision attacks.

1.) Pseudorandom number attacks: To make packets fresh, a timestamp or random number (nonce) is used to prevent a replay attack . The session key is often generated from a random number. In the public key infrastructure the shared secret key can be generated from a random number too. The conventional random number generators in most programming languages are designed for statistical randomness, not to resist prediction by cryptanalysts. In the optimal case, random numbers are generated based on physical sources of randomness that cannot be predicted. The noise froman electronic device or the position of a pointer device is a source of such randomness. However, true random numbers are difficult to generate. When true physical randomness is not available, pseudorandom numbers must be used. Cryptographic pseudorandom generators typically have a large pool (seed value) containing randomness. New environmental noise should be mixed into the pool to prevent others from determining previous or future values. The design and implementation of cryptographic pseudorandom generators could easily become the weakest point of the system.

2.) Digital signature attacks: The RSA public key algorithm can be used to generate a digital signature. The signature scheme has one problem: it could suffer the blind signature attack. The user can get the signature of a message and use the signature and the message to fake another message's signature. The El Gamal signature is based on the difficulty in breaking the discrete log problem. Digital Signature Algorithm (DSA) is an updated version of the El Gamal digital signature scheme published in 1994 by FIPS, and was chosen as the digital signature standard (DSS) [4]. The attack models for digital signature can be classified into known-message, chosen-message, and key-only attacks. In the known-message attack, the attacker knows a list of messages previously signed by the victim. In the chosen-message attack, the attacker can choose a specific message that it wants the victim to sign. But in the key-only attack, the adversary only knows the verification algorithm, which is public. Very often the digital signature algorithm is used in combination with a hash function. The hash function needs to be collision resistant.

3.) Hash collision attacks: The goal of a collision attack is to find two messages with the same hash, but the attacker cannot pick what the hash will be. Collision attacks were announced in SHA-0, MD4, MD5, HAVAL-128, and RIPEMD. The collisions against MD4, MD5,HAVAL-128,andRIPEMDwere found recently. A successful attack against SHA-1 [4] was found, and the collisions in SHA-1 can be found with an estimated effort of 269 hash computations. Normally all major digital signature techniques (including DSA and RSA) involve first hashing the data and then signing the hash value. The original message data is not signed directly by the digital signature algorithm for both performance and security reasons. Collision attacks could be used to tamper with existing certificates. An adversary might be able to construct a valid certificate corresponding to the hash collision.

V. CONCLUSION

Due to dynamic infrastructure of MANETs and having no centralized administration makes such network more vulnerable to many attacks. In this paper, we discuss about how different attacks layer specific and cryptographic primitive attacks become vulnerable. These attacks can classified as a active or passive attacks. Different security mechanisms are introduced in order to prevent such network. Here we have provided some counter measures for layer specific attacks. In future study we will try to invent such security algorithm, which will be installed along with routing protocols that helps to reduce the impact of different attacks and also develop some techniques to avoid the cryptographic primitive attacks.

REFERENCES

1. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei., " A Survey of attacks and countermeasuresin mobie adhoc networks", WIRELESS/MOBILE NETWORK SECURITYY. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. – - –,°c 2006 Springer.
2. Gagandeep, Aashima, Pawan Kumar, **"**Analysis of different security attacks in MANET on protocol stack-A Review", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.
3. P.J Sweetlin Subha1, Jeban Chandir Moses2 **,"**A survey of various risks mitigating techniques in MANET environment," Internationa Journal of scientific and research publications,volume 3 issue 2 feburary 2013.
4. Ms. Preetee K. Karmore, Ms. Sonali T. Bodkh. "A survey on intrusionin adhoc networksand its detection measures", International Journal on Computer Science and Engineering (IJCSE),
5. Mohammad Wazid ,Rajesh kumar singh, R.H Goudar " A survey of attacks happened at different layers of mobile adhoc networks and some available detection techniques" ; International Journal of computer applications.
6. Pradip M Jawandhiya,Manghesh M Ghonghe,dr. MS ali "A Survey of Mobile Ad hoc Network Attacks "International journal of Engineering ,Science and Technology
7. Djamel DJENOURIx, Nadjib BADACHEz," A survey on Security Issues in Mobile Ad hoc Networks", Computer Systems Laboratory, Computer Science Department, University of Science and technology, Algiers, Algeria
8. G.S. Mamatha, Dr. S.C. Sharma, "Network Layer Attacks and Their Defence Mechanisms In MANETS – A survey"
9. Pallavi Khatri1 , Sarita Bhadoria2, and Mamta Narwariya3,"A Survey on Security Issues in Mobile Ad hoc Networks"
10. P.Visalakshi, 1 S.Anjugam2 ,"Security Issues and Vulnerability in Mobile Ad hoc Networks"