Security Attacks and Countermeasures in Manets: A Survey

Sunitha R[1], Spoorthi Y[2]
[1,2] *Assistant Professor , dept. E&CE , GSSSIETW,Mysuru,India*

***Abstract*- Security is a fundamental and important service for wired and wireless network communications. The effective operation of mobile ad hoc networks (MANET) strongly relies on wireless node's confidence in its security and cooperation among themselves. In any case, the characteristic attributes of MANET, such as, open and shared communication medium, absence of fixed central infrastructure etc, offers more noteworthy difficulties and openings in accomplishing security objectives. In MANET, the security goals comprises of confidentiality, authentication, integrity, availability, access control, and non-repudiation. MANET should guarantee each of the security goals in order to provide a higher degree of performance. A brief survey on security attacks and countermeasures for individual layers on a protocol stack in a MANET is presented this paper. The countermeasures are approaches or functions that are intended to reduce or eliminate security vulnerabilities and attacks. Initially, a brief prologue to MANETs, and security needs and mechanisms are presented. Then a brief survey on different attacks and the preventive approaches as per the protocol stack is presented.**

I. INTRODUCTION

MANET is a collection of autonomous wireless mobile nodes forming a temporary network without the help of any fixed infrastructure or centralized administration. A MANET operates as a decentralized infrastructure-less architecture since, the mobile nodes dynamically set up paths among themselves in cooperative environment to transmit packets in the network temporarily. In a MANET, nodes which are in the radio transmission ranges of each other's can communicate directly, however, nodes lying outside the range depends upon other nodes in the network to transmit the messages. Thus, a hop by hop communication scenario occurs, where in several intermediate hosts relay the packets to destination host form the source node. Every individual node functions both as a router and a host. The success of communication highly depends on other nodes' cooperation. A Typical MANET scenario is as shown in figure 1 which consists of number of wireless mobile nodes communicating with each other without aid of any fixed network infrastructure.

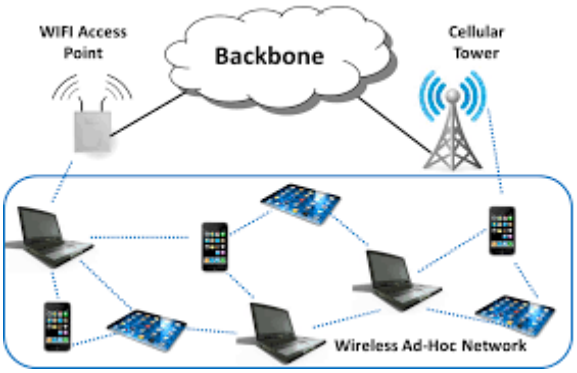

Figure 1: MANET example.

The nodes in network are equipped with wireless transmitters and receivers with either a omni directional (broadcast), highly-directional (point-to-point) antennas, or some combination of both. Since nodes in the system are dynamic in nature, the system topology may change with time as the nodes move. At any point of time, the network structure is random because of the frequent topology changes, their transmitter/receiver coverage patterns, the transmission power levels, and the channel interference levels.

Thus, a MANET has several distinct characteristics:

- Dynamic topologies
- Resource limitations
- Limited physical security
- Absence of centralized infrastructure

The MANET has wide variety of applications which includes: Soldiers exchanging information in the battlefield, sharing of information between associates during a business meeting, in interactive conferences

and emergency disaster relief operations during natural calamities such as hurricane, or earthquake, information sharing in personal area and home networks, location-based services and the sensor networks. There are a wide variety of attacks that targets the weakness of MANET.

There is range of attacks which targets functioning of individual layers of TCP/IP model, i.e application layer, transport layer, network layer, data link layer, physical layer.

II.SECURITY CHALLENGES IN MANETS

The notable attributes of MANETs make it more defenseless against range of security attacks and threats which degrades the network performance in overall. Such attributes which posture difficulties to security of MANET are listed as follows:

- Dynamic nature
- Shared broadcast radio communication channel
- Absence of central authority
- Lack of cooperation among nodes
- Insecure operating environment
- Limited resource availability

III.SECURITY REQUIREMENTS AND ATTCKS

Security in MANET is key element which directly influences the network operation. Security in wired and wireless networks has similar necessities that should be addressed. It can be stated that security is the blend of procedures, processes and system frameworks used to guarantee following necessities:

- Confidentiality
- Authentication
- Integrity
- Non-repudiation
- Availability
- Access control

The security attacks in MANET can generally be grouped into two major classes as, active attacks and passive attacks, on the basis of means of attacks. A passive attack does not disturb the network operation but, rather gathers information exchanged in the network communications. An active attack is aimed at altering or destroying the information in the network by data interruption, alteration, or creation, in this way disturbing the normal operation of a MANET.

Table 1 summarizes the general classification of security attacks against MANET. Examples of passive attacks are traffic analysis, eavesdropping and traffic monitoring. The active attacks include denial of service (DoS), message replay, jamming, impersonating and modification.

Table 1. General classification of attacks

Passive attacks	Eavesdropping, traffic analysis, monitoring.
Active attacks	Jamming, spoofing, modification, replaying, DoS.

The attacks can also be classified into two categories according to domain of the attacks, namely external attacks and internal attacks, also referred as outsider and insider attacks. Attacks performed by nodes that do not belong to the network are referred as external attacks. Internal attacks are from compromised nodes within the network. Internal attacks are more serious in contrast with the external attacks since the insider knows secret and sensitive data, and has privileged access rights.

The mobile hosts share a common wireless medium for communication channel which makes MANETs prone to many attacks at each layer. Attackers challenge normal operation of MANET by targeting its key characteristics discussed in section II. Attacks can also be classified according to network protocol stacks. Table 2 gives the overview on classification of security attacks in relation with protocol stack.

Table 2: Survey of security threats as per protocol stack

Layer	Attacks	Countermeasures
1.Physical Layer	1. Jamming 2. Interception	• Frequency Hopping Spread Spectrum (FHSS) • Direct Sequence Spread Spectrum (DSSS)
2. Link Layer	1. Traffic Analysis & Monitoring 2. Disruption on MAC DCF and back off mechanisms	• ERA-802.11 • Encryption
3. Network Layer	1. Route Discovery Phase: • Flooding • Routing table overflow • Route cache poisoning • Routing loops 2. Route Maintenance phase • RERR flooding 3. Data forwarding phase • Modification / Altering • Deletion, Delaying 4. Other attacks • Wormhole attack • Blackhole attack • Byzantine attack • Rushing attack • Location disclosure attack • Resource Consumption attack • Denial of Service attacks • Impersonation & non-repudiation attacks • Modification attacks	• Authentication & Integrity • Hash function, Digital Signatures • Message Authentication Codes (MAC), HMAC • Packet Leashes • SECTOR • Using Directional antenna's • Secure Adhoc Routing (SAR) protocol • ARAN • SEAD
4.Transport layer	• Session hijacking • SYN flooding	• Secure Socket Layer(SSL) • Transport Layer Security(TLS) • Private Communication Transport (PCT)
5. Application Layer	• Repudiation • Data Corruption	• Firewall • Application specific modules, e.g. spyware detection software • Intrusion Detection System (IDS)
6. Multilayer Attacks	• Denial of Service (Dos) • Impersonation • Man in Middle attacks • Key management attacks	• End-to-End authentication • Key Encryption Key Approach

A. Physical layer attacks

Physical layer is in charge of transmission and gathering of information bits and it manages electrical and mechanical properties and specifications of network hardware and physical communication medium utilized for transmission. Attacks at the physical layer targets vulnerabilities of network hardware and physical communication medium i.e normal shared wireless broadcast communication medium utilized. Attacks at physical layer are Jamming, Interception and Eavesdropping

The process of capturing and perusing of messages and data by unintended receivers is Eavesdropping. The mobile nodes in MANET share common shared wireless communication medium. The greater parts of wireless communication utilize the radio frequency (RF) spectrum and are broadcast in nature. Signals communicate can be effectively captured with receivers tuned to the particular frequency. In this manner, messages transmitted can be spied, and fake messages can be infused into network by unauthorized nodes.

Likewise, a radio signal can be interfered or jammed, which may brings about corrupted or lost message. If the attacker possesses a powerful transmitter, a signal can be created which is sufficiently strong enough to overwhelm the targeted signal and disrupt the communications. The most widely recognized sorts of this type of signal jamming are random pulse and noise. Jamming equipment is readily available. Moreover, jamming attacks can be mounted from an remote location to the targeted network.

COUNTERMEASURES FOR PHYSICAL LAYER ATTACKS:

Wireless communication is broadcast by nature. A broadcasted radio signal is easy to jam or intercept. Spread spectrum technologies, such as frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS), can make it difficult to detect or jam signals. In both the techniques frequency changes in a random fashion, which makes it difficult to capture the signal or it spreads the energy to a wider spectrum so the transmission power is hidden behind the noise level.

In an alternative approach Directional antennas can also be deployed since the communication techniques can be intended to spread the signal energy in space.

Both FHSS and DSSS posture troubles for outsider nodes trying to capture the radio signals. The eavesdropper must have the knowledge on frequency band, spreading code, and techniques used for modulation to precisely read the transmitted signs.

B. LINK LAYER ATTACKS

The MANET is open multipoint shared network architecture. In particular, single hop connectivity among neighbors is kept up by the link layer protocols, and the network layer protocols extend the network to other nodes in the network. Attacks may target the link layer by upsetting the cooperation of the layer's protocols. Link layer protocols help to find single hop neighbors, handle reasonable channel access, casing blunder control, frame error control, and maintain neighbor connections.

Wireless medium access control (MAC) protocols are proposed to coordinate the transmissions of the nodes on the common transmission medium. IEEE 802.11 protocol is specifically devoted to wireless LANs. The IEEE 802.11 MAC protocol utilizes contention mechanisms for sharing the common wireless channel. The IEEE 802.11 work group proposed two algorithms for contention resolution. One is a completely distributed protocol called the distributed coordination function (DCF). The other is centralized access scheme called point coordination function (PCF). The attacks at link layer are traffic monitoring and analysis, disruption MAC DCF and back-off system.

Traffic monitoring and analysis can be considered as passive form of attack wherein the attacker just identify the communicating nodes and their functionalities, which could be used as a information to launch further attacks.

The present wireless MAC protocols assume agreeable cooperation among every node in the network. The selfish or malicious nodes are purposefully doesn't take after the normal functions of the protocols. In the link layer, a malicious or selfish node could hinder either contention based or reservation-based MAC protocols. A malicious neighbor of either the sender or the recipient could deliberately not take after the specifications of the protocol. For instance, the aggressor may disrupt the frames effectively by inducing a few bits or overlooking the progressing transmission.

It can likewise abuse double exponential back-off plan to dispatch DoS attacks in IEEE 802.11 MAC. Since the binary exponential scheme favors the last winner amongst the contending nodes which leads to

the capture effect. The heavily loaded nodes tend to capture the channel by continually transmitting data, which causes lightly loaded neighbors to back-off endlessly.

Malicious node takes advantage of the capture effect vulnerability.

In addition, a back-off at the link layer can bring about a chain response in any upper layer protocols that utilizes a back-off scheme, similar to TCP window transmission.

The network allocation vector (NAV) field conveyed in RTS/CTS frames represents defenselessness to DoS attacks in the link layer. The NAV field was proposed to relieve the hidden terminal issue in the carrier sense mechanism. Amid the RTS/CTS handshake the sender first sends a RTS frame containing the time expected to finish the CTS, information, and ACK frames. Each neighbor of the sender and recipient will refresh the NAV field and defer their transmission for the term without bounds exchange as per the time that they overheard. An attacker may likewise overhear the NAV data and afterward deliberately degenerate the link layer frame through wireless interference to the progressing transmission.

COUNTER MEASURES FOR LINK LAYER ATTACKS

The malicious attacks target the link layer by disrupting the cooperative nature of link layer protocols. In order to maximize their own throughput selfish nodes could disobey the channel access rule, manipulate the NAV field and cheat backoff values, and so on. Neighbors should monitor these misbehaviors. Several schemes are proposed to prevent selfishness, such as ERA- 802.11, where detection algorithms are proposed. Traffic analysis is prevented by encryption at data link layer. The wired equivalent privacy (WEP) encryption technique characterized in the IEEE 802.11 wireless LAN standard uses link encryption to conceal the end-to-end traffic streaming data.

In MANET, some schemes are proposed to create a security cloud, construct a traffic cover mode or dynamic mix method, or use traditional traffic padding and traffic rerouting techniques to prevent traffic analysis. A security cloud implies that every node under the security cloud is indistinguishable regarding traffic generation. A traffic cover mode conceals the progressions of a end to end traffic flow pattern, on the grounds that specific strategic data may be deduced from the unusual changes in the traffic pattern.

C. NETWORK LAYER ATTACKS

Network layer protocols extend connectivity from neighboring single hops nodes to all other nodes in MANET. The connectivity among mobile nodes over a multi-hop wireless connection emphatically relies on cooperative interactions among each of the nodes in network. A variety of attacks targeting the network layer have been identified. By attacking the routing protocols, attackers can assimilate network traffic, infuse themselves into the way between the source and destination, and in this way control the traffic flow. The significant delay could be introduced by forwarding traffic packets to a non-optimal path, or packets could be forwarded to nonexistent path and get lost.

The attackers upset the layer operation by creating routing loops, presenting serious network congestions, and channel conflict. Multiple colluding attackers may even prevent a source node from finding any route to the destination, causing the network to partition, which triggers excessive network control traffic, and further intensifies network congestion and performance degradation.

Attacks on network layer are possible during route discovery phase, route maintenance phase or data forwarding phase. Attackers could also launch attacks targeted towards specific routing protocols and there are few sophisticated attacks such as blackhole, wormhole, byzantine and rushing attacks which severely degrades the layers normal functioning.

C.1 ATTACKS AT THE ROUTING DISCOVERY PHASE:

Attacks are network layer during route discovery and maintenance phase are mainly due to the fact that compromised nodes violating the protocol specifications. Routing message flooding attacks, such as hello flooding, RREQ flooding, acknowledgement flooding, routing table overflow, routing cache poisoning, and routing loop are simple examples of routing attacks targeting the route discovery phase.

Routing in MANETs can be broadly categorized as proactive and reactive. Proactive protocols maintain a routing table comprising routing information of all nodes in the network which are updated periodically. Reactive protocols on the other hand initiates route

discovery only when it is needed. Proactive routing protocols, for example, DSDV and OLSR endeavor to find routing data before it is needed, while reactive protocols, for example, DSR and AODV create routes just when they are required. Thus, proactive algorithms are more vulnerable to routing table overflow attacks. Some of these attacks are listed below.

Routing table overflow attack: Since proactive algorithms periodically update the routing information, a malicious node exploits this feature by advertising the authorized nodes, routes that lead to non-existent nodes. The attacker tries to create enough routes to keep new routes from being made. An attacker can simply send excessive route advertisements to overflow the victim's routing table thereby inhibiting the normal protocol operation. Proactive algorithms are more prone routing table overflow attacks.

Routing cache poisoning attack: Here attackers take advantage of the promiscuous mode of routing table updating, where a node overhearing any packet may add the routing information contained in that packet header to its own route cache, even if that node is not on the path. Assume malicious node M needs to spoil routes to node X. M could broadcast spoofed packets with source route to X by means of M itself; in this way, neighboring nodes that overhear the packet may add the route to their route caches.

C.2 ATTACKS AT THE ROUTING MAINTENANCE PHASE

Attackers target the route maintenance phase by broadcasting false control messages, such as link-broken error messages, which cause the invocation of the costly route maintenance or repairing operation. For instance, AODV and DSR implement path maintenance procedures to recuperate broken paths when nodes move. In the event that the destination node or a intermediate node along a active path moves, the upstream node of the broken connection broadcasts a route error message to all active upstream neighbors. The node likewise invalidates the route for this destination in its routing table. Attackers could exploit this scheme to launch attacks by sending false route error messages.

C.3. ATTACKS AT DATA FORWARDING PHASE

The attacker targets data packet forwarding functionality in the network layer. In this situation the malicious nodes agreeably take an interest in the routing discovery and maintenance stages; however they don't forward the information packets as indicated by routing table in the data forwarding stage.

Malicious node quietly drops data packets, modifies the data content, replay, or floods the data packets or they can also delay forwarding time-sensitive data packets selectively or inject junk packets.

C.4 ATTACKS ON PARTICULAR ROUTING PROTOCOLS

Few attacks particularly targets functioning of some specific routing protocols. In Dynamic Source Routing protocol, the attacker may change the source route recorded in the RREQ or RREP packets. It can erase a node from the route stored in cache, switch the request, or add another node into the route. In Adhoc On demand Distance Vector protocol, the attacker may promote a route with a smaller distance metric than the actual distance, or publicize a routing update with a large sequence number and invalidate all routing updates from other nodes.

C.5 OTHER ADVANCED ATTACKS

There some routing attacks identified which targets the routing protocol in a more sophisticated and subtle manner. The blackhole (or sinkhole), Byzantine, and wormhole attacks are examples such advanced attacks, which are described in brief in following sections

C.5.1. WORMHOLE ATTACK

In the wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point .In this attack an attacker records packets at one location in the network and tunnels them to another location. If the routing control messages are tunneled then the routing operation is disrupted. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

C.5.2. BLACKHOLE ATTACK

The blackhole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, by advertising itself has as a valid route to a destination node, even though the route is

fake, with an intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding.

However, the attacker keeps running at the danger of being observed and exposed by the neighboring nodes on the ongoing attacks. The more complex form of these attacks is when an attacker decides to selectively forwards packets. If an attacker selectively suppresses or modifies packets from targeted nodes while leaving information other nodes unaffected limits the suspicion of being caught.

C.5.3. 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.

C.5.4. RUSHING ATTACK

Two colluded attackers use the tunnel like structure to form a wormhole in case of rushing attack. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack poses a greater challenge to on demand routing protocols by causing an effective denial-of-service attack.

C.5.5. SOURCE CONSUMPTION ATTACK

Source Consumption attack is also referred as the sleep deprivation attack. A compromised node or an attacker attempts to consume battery life of a victim node by requesting excessive route discovery, or by forwarding unnecessary packets.

C.5.6. LOCATION DISCLOSURE ATTACK

An attacker or a compromised node reveals location information of the nodes or the structure of the network or the route map. Such acquired location information then used plan and implement further attacks. Traffic analysis, one of the difficult security attacks against MANET, since it is tough to find. Compromised nodes try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security sensitive scenarios.

NETWORK LAYER DEFENSE

The routing information can be protected with the same method as that of being used to protect data traffic from the passive attack. Active attacks like illegal modification of routing messages can be prevented by source authentication and message integrity mechanisms. DoS attacks on a routing protocol could take many forms. DoS attacks can be countered by not allowing the attacker from creating routing loops, enforcing the packet to travel maximum route length or using other active approaches.

By using an unalterable and independent physical metric, such as time delay or geographical location the wormhole can be detected. For example, packet leashes are used to combat wormhole attacks.

By using authentication and integrity mechanism, either the hop-by-hop or the end-to-end approach, the correctness of routing data can be ensured. For example, digital signature, one-way hash function, hash chain, message authentication code (MAC), and hashed message authentication code (HMAC) are widely used. IPsec and ESP are standards of security protocols on the network layer used in the Internet that could also be used in MANET, in certain circumstances, to provide network layer data packet authentication, and a certain level of confidentiality; in addition, some protocols are designed to defend against selfish nodes, which intend to save resources and avoid network cooperation.

DEFENSE AGAINST WORMHOLE ATTACKS

A packet leash protocol has been proposed as a countermeasure to the wormhole attack, a leash is the information added into a packet to restrict its transmission distance. A temporal packet leash adds an additional constraint of bound on lifetime of a packet along with the travel distance.

Wormholes are detected using the SECTOR mechanism without the need of clock synchronization. The mechanism depends basically on distance-bounding techniques, one-way hash chains, and the Merkle hash tree. Thus Wormholes in MANET can be prevented without the requirement of any clock synchronization or location information by implementing SECTOR mechanism. SECTOR can also be used to help to detect cheating by means of topology tracking

Directional antennas are also proposed to prevent wormhole attacks, which does not require either

location information or clock synchronization, and is more efficient with energy.

Even the hardware design or signal processing techniques can be used to counter Wormhole attacks in MANETs. Also if the data bits are transferred in some modulating method with only to the neighbor nodes having its knowledge, they can resist closed wormholes. Alternative solution is of integrating the prevention scheme into intrusion detection systems. Since the packets sent by the wormhole are identical to the packets sent by legitimate nodes it is difficult to isolate the attacker with a software-only approach,.

DEFENSE AGAINST BLACKHOLE ATTACKS

Some secure routing protocols, for example, the security-mindful impromptu directing convention (SAR) , in light of on demand conventions, for example, AODV, DSR can be utilized to guard against black hole attacks. In SAR, a security metric is included into the RREQ packet, and an alternative route discovery method is used. Intermediate nodes can handle the RREQ just if the security metric or some trust level is met and it will propagate to its neighbors utilizing controlled flooding. Something else, the RREQ is dropped. The destination reacts back just if end to end way with the required security characteristics can be found.

In SAR, a malicious node that intrudes on the flow of packets by modifying the security metric to a higher or lower level can't bring about serious harm because of the fact that the legitimate intermediate node should drop the packet, and the attacker is not able to decrypt the packet. SAR gives a suite of cryptographic schemes, such as, digital signature and encryption, which can be incorporated on a need-to-utilize premise to counter modification.

DEFENSE AGAINST IMPERSONATION AND REPUDIATION ATTACK

ARAN can be utilized to counter impersonation and repudiation attacks. ARAN scheme facilitates authentication and non-repudiation services utilizing defined cryptographic certificates for end-to-end authentication. In ARAN, every node asks for a certificate from a trusted certificate server. Source node initiates route discovery by broadcasting route discovery packet (RDP). Then destination unicasts the replay (REP) message back to the source. At every intermediate hop routing messages are authenticated.

ARAN utilizes hop by hop authentication, which acquires a huge computation overhead which is the major setback for the algorithm. In the mean time, every node needs to keep up one table entry for each source-destination pair that is active currently.

The SEAD protocol is proposed to shield against alteration or modification attacks. Like a packet leash, the SEAD protocol uses a one-way hash chain to keep malicious nodes from incrementing the sequence number or decreasing the hop count in route advertisement packets. In SEAD, nodes need to verify neighbors by utilizing TESLA broadcast authentication or a symmetric cryptographic scheme.

The attacker can never forge metric value, or higher sequence number. Since, subsequent to getting a routing update in DSDV scheme, a node updates its advertized routing table when the sequence number is more prominent or when sequence number is same however the metric is lower, SEAD keeps malicious nodes from diminishing the hop count value or increasing sequence number in light of the plan of DSDV.

D.TRANSPORT LAYER ATTACKS

The principle targets of TCP-like Transport layer protocols in MANET includes setting up of end-to-end connections, reliable end-to-end to packet delivery , flow control, congestion control, termination of end-to-end connections. The TCP protocols are powerless against the SYN flooding or session hijacking attacks.

In contrast with wired networks a MANET has a higher channel error rate. Since TCP does not have any scheme to recognize between loss caused because of congestion, random error, or malicious attacks, TCP multiplicatively diminishes its congestion window after encountering losses, which debases network performance altogether.

SYN FLOODING ATTACK

The SYN flooding attack is kind of a denial of service attack. The attacker initiates a large number of half-opened TCP connections with a victim node, however never finishes the handshake to complete the connection. For two nodes to communicate utilizing the TCP, they should first build up a TCP connection using a three-way handshake. The three messages exchanged amid the handshake, SYN, SYNACK, ACK which permits nodes to understand that the other is prepared for the connection. Amid the attack, a malicious node sends a lot of SYN

packets to a victim node, spoofing the arrival addresses of the SYN packets. The SYNACK packets are conveyed from the victim right after it gets the SYN packets from the attacker and after that the victim waits for the reaction of ACK packet from the attacker to complete the connection.

With no response of ACK packets, the half-open information structure stays in the victim node. If the victim node stores these half-opened connections in a fixed size table while it anticipates the connections of the three-way handshake, these pending connections could overflow the buffer, and the victim node would not have the capacity to acknowledge requests of legitimate nodes to open an connection. Regularly there is a time out related with a pending connection, so the half-open connections will expire and the victim node will recover. In any case, malicious nodes can attempt to keep sending packets that demand new connections quicker than the expiration of pending connections.

SESSION HIJACKING

Large portion of the communications are secured at session setup, however not thereafter, Session hijacking exploits the above certainty to launch the attacks. In the TCP session attack, the attacker spoofs the victim's IP address to decide the right sequence number anticipated by the target to launch a DoS attack on the victim. Along these lines the attacker mimics the victim node and proceeds the session with the target. The TCP ACK storm issue could be made when an attacker launches a TCP session hijacking attack.

Hijacking a session over UDP is the same as over TCP, with the exception of UDP attackers don't need to stress over the overhead of management of sequence numbers and other TCP schemes. Since UDP is connectionless, edging into a session without being identified is substantially easier than the TCP session attacks.

TRANSPORT LAYER DEFENSE

In MANET, similar to TCP protocols in the Internet, nodes are helpless against the SYN flooding attack, or session hijacking attack. End to end encryption gives message privacy at or over the transport layer. TCP is a connection oriented transport layer protocol. Since TCP does not perform 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 proposed, however none of these protocols are planned in light of security.

Secure Socket Layer (SSL), Transport Layer Security (TLS), and Private Communications Transport (PCT) protocols were intended for secure communications and depend on public key cryptography. TLS/SSL can help secure information transmission. It can likewise secure against masquerade attacks, man-in-the-middle attacks, rollback attacks, and replay attacks. TLS/SSL depends on public key cryptography, which is CPU-concentrated and requires comprehensive administrative design. Consequently, the use of these mechanisms in MANET is confined. TLS/SSL must be altered so as to address the special needs of MANET. Some firewall at a higher can be designed to safeguard against SYN flooding attacks.

E. APPLICATION LAYER ATTACKS

Application layer goes about as interface to application processes which require communication support. It gives schemes to information transmission, access to distributed database, running application on a remote machine. Application layer attacks can be mobile viruses, worm attacks, and repudiation attacks.

E.1. MOBILE VIRUS AND WORM ATTACKS

The application layer contains user information, and it supports numerous protocols, for example, HTTP, SMTP, FTP. Malicious programs are broadly spread in a system, such codes incorporates viruses and worms, which is material applicable over operating systems and applications. There are diverse courses by which a worm can find new machines to attack. One of such strategy is IP address checking utilized by Internet worms. This scheme includes generation of probe packets to a vulnerable UDP/TCP port at a wide range of IP addresses. Hosts that are hit by the scan react, get a duplicate of the worm, and consequently get infected. The Code Red worm is one of the scanning worms.

A few worms exploits the loophole of the framework. For instance, Worm.Blaster and Worm.Sasser are the worm codes which misuse diverse set of loopholes. Worm.Blaster utilizes a framework RPC DCOM loophole, and Worm.Sasser utilizes the framework LSASS (Local Security Authentication Subsystem Service). In MANET, an attacker can likewise create a worm attack utilizing any loophole of the system of the MANET.

E.2. REPUDIATION ATTACK

Repudiation alludes to a refusal of participation in all or some portion of the communications. For instance, a selfish individual could deny leading an operation on a credit card buy, or deny any on-line bank exchange, which is one of the sorts of a repudiation attack on a business framework. In the network layer, firewalls can be introduced to keep packets in or keep packets out. In the transport layer, whole connections can be encrypted, end-to-end. Be that as it may, these arrangements do not solve the authentication or non-repudiation issues in general.

E.3. APPLICATION LAYER DEFENSE

The application layer additionally should be secured as the other protocol layers. The firewall can facilitate access control, user validation, packet filtering, and a logging and accounting administration. Application layer firewalls can viably avert many attacks, and application-particular modules, for instance, spyware detection software, have likewise been produced to monitor mission-critical services. Be that as it may, a firewall is mostly limited to essential access control and is not able to take care of all security issues. For instance, it is not compelling against attacks from insiders. As a result of MANET's absence of framework, a firewall is not especially helpful.

Intrusion Detection System (IDS) can be utilized as other line of protection in MANET. Intrusion detection can be introduced at the network layer, however in the application layer it is feasible and also fundamental. For example, the application layer can identify a DoS attack more rapidly than the lower layers when an extensive number of incoming connections have no genuine operations, since low layers require more time to identify it.

F. MULTI-LAYER ATTACKS

There are a few attacks which are propelled from various layers rather from a specific layer. Cases of multi-layer attacks are denial of service (DoS), man-in-the middle, and impersonation attacks.

F.1 DENIAL OF SERVICE ATTACK

Denial of Service (DoS) attacks could be propelled from a several layers. Under DoS attack, compromised node can focus on a particular layer and can keep it from conveying its service. An attacker can utilize jamming signals at the physical layer, which disturbs normal communications. At the link layer, malicious nodes can possess channels through the capture effect, which exploits the binary exponential mechanism in MAC protocols and keeps different nodes from channel access. At the network layer, the routing procedure can be hindered through routing control packet adjustment, specific dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can bring about DoS attacks.

F.2 IMPERSONATION ATTACKS

Impersonation attacks are the initial step for most attacks, and are utilized to launch further advanced attacks. For instance, a malicious node can go before an attack by adjusting its MAC or IP address.

F.3 MAN-IN-THE-MIDDLE ATTACKS

In Man in the Middle attack as the name itself indicates an attacker places himself in the middle of the sender and the recipient and gathers the data exchanged between the two closures. Now and again the attacker may imitate by pretending the sender to communicate with the recipient, or mimic the receiver to reply to the sender.

F.4 DEFENSE AGAINST MULTI-LAYER ATTACKS

Since the multilayer attacks focuses on various layers, the countermeasures should be executed at various layers. For instance, directional antennas are utilized at the media access layer to safeguard against wormhole attacks, and packet leashes are utilized as a network layer barrier against wormhole attacks. The countermeasures for multi-layer attacks can likewise be executed in an integrated scheme. For instance, if a node distinguishes a nearby interruption at a higher layer, lower layers are informed to do further examination.

DoS attacks in MANET can be of two sorts, one at the network layer, and another at the MAC layer. Attacks at the routing layer could comprise of following mischievous activities:

1. The malicious node takes part in a route however essentially drops a portion of the information packets.
2. The malicious node transmits false updates.
3. The malicious node could conceivably replay stale updates. 4. The malicious node lessens the TTL (time-to-live) field in the IP header so that the packet never reaches destination.

End-to-End authentication implementation might counter the attacks by independent malicious node of sorts (2) and (3). An attack of sort (1) might be taken care of by confidence level metric assignment to each

nodes and utilizing routes that facilitate highest confidence level. An attack of sort (4) might be countered by making it compulsory; a intermediate node must guarantee that the TTL field is set to a value more noteworthy than the hop count to the expected destinations. In the case of colluded nodes, the authentication schemes may fail and it is an open issue to provide protection against such routing attacks.

At the MAC layer DoS attacks could incorporate, among others, the following mischievous activities:

1. Channel is kept occupied in the neighborhood region of a node prompts a DoS attack at that node.
2. The battery life of a node might be depleted, by utilizing a specific node to consistently relay spurious information.

End-to-end authentication may keep the over two cases from succeeding. In the event that the node does not have an authentication certificate, it might be kept out from the channel access. Generally the nodes collude, if nodes conspire, and the colluded nodes include the sending node and the destination, MAC layer attacks are very much achievable.

MANET INTRUSION DETECTION SYSTEMS (IDS)

MANETs key features incorporating an open medium, dynamic topology, and the absence of a central authority makes a significant number of the intrusion detection methods designed for a wired system not feasible for MANET. IDS intended for MANET goes for intrusion detection and reactive schemes for MANET. Two systems to be specific are guard dog and pathrater, goes for enhancing the throughput in MANET within the sight of nodes that consent to forward packets however fail to do as such. In MANET, cooperative participation is essential to support the fundamental elements of the system so the token-based, the credit-based, and the receipt based schemes were proposed to enforce the cooperation.

In an IDS actualized MANET, every portable node independently runs as an IDS agent. Its obligation is to watch the conduct of neighboring nodes, identify nearby interruption, cooperate with neighboring nodes, and, if necessary take actions. An IDS agent has information gathering, local detection, nearby reaction, a cooperative identification engine, and secure correspondence with neighboring IDS agents.

G. CONCLUSION & FUTURE SCOPE

Security is a vital perspective that decides the achievement and wide deployment of MANETs. A concise study on various attacks and proposed Security countermeasures intended for MANETs, for wireless systems are presented in this paper. Security must be guaranteed in the whole framework including the security primitives, since general security level is controlled by the framework's weakest point.

The exploration on MANET is still in an early stage. Existing proposals are aimed at countering one particular attack. Since the attacks could function admirably within the sight of planned particular attacks, however there are many joined and conspired attacks that stance test to MANET operation. A ton of research is still while in transit to recognize new threats and create a secure scheme to counter such threats. A greater amount of research should be possible on critical areas, such as, the key management framework, trust-based protocols, incorporated approaches to deal with enhancing routing security, and information security at various layers, Cross layer approach to counter multilayer attacks.

The vast majority of the present work is on preventive strategies with intrusion detection as the second line of defense. One fascinating research issue is to propose a trust-based framework so that the level of security requirement is reliant on the trust level. Cryptography-based techniques offer a subset of arrangements. Different arrangements will be in future research.

REFERENCES

[1] Amit Kumar, Vijay K. Katiyar and Kamal Kumar, "SECURE ROUTING PROPOSALS IN MANETS:A Review, International Journal in Foundations of Computer Science & Technology (IJFCST) Vol.6, No.1, January 2016.
[2] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", WIRELESS/MOBILE NETWORK SECURITY, 2006 Springer
[3] Supriya Tayal 1, Vinti Gupta , "A Survey of Attacks on Manet Routing Protocols" , International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 6, June 2013.

[4] W. Lou and Y. Fang, A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions. Ad Hoc Wireless Networks, edited by X. Chen, X. Huang and D. Du. Kluwer Academic Publishers, pp. 319-364, 2003.
[5] Rajni Sharma1, Alisha saini, "A Study of Various Security Attacks and their Countermeasures in MANET", Vol.1, Issue 1, International Journal of Advance reasearch in computer science and Software Engineering. December .
[6] Nishu Garg and R.P.Mahapatra, "MANET Security Issues ," IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.
[7] P. Yi, Y.P. Zhong, S.Y. Zhang, and Z.L.Dai, "Flodding Attack and Defence in Ad hoc NEtwork", J Syst Engineer Electro, Vol. 17 , no. 2, pp. 410-6, 2006.
[8] 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
[9] 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.
[10] S. Yi, P. Naldurg, and R. Kravets, Security-Aware Ad-hoc Routing for Wireless Networks. Report No.UIUCDCS-R-2002-2290, UIUC, 2002.
[11] Khan, S., Loo, K. K., & Din, Z. U. (2010). Framework for intrusion detection in IEEE 802.11 wireless mesh networks. Int. Arab J. Inf. Technol., 7(4), 435-440.
[12] Rafsanjani, M. K., Movaghar, A., & Koroupi, F. (2008). Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes. World Academy of Science, Engineering and Technology, 20, 351-355.
[13] Ramanujan, R., Ahamad, A., Bonney, J., Hagelstrom, R., & Thurber, K. (2000). Techniques for intrusion-resistant ad hoc routing algorithms (TIARA). In MILCOM 2000. 21st Century Military Communications Conference Proceedings (Vol. 2, pp. 660-664). IEEE.
[14] Papadimitratos, P., & Haas, Z. J. (2003). Secure message transmission in mobile ad hoc networks.Ad Hoc Networks, 1(1), 193-209. International Journal in Foundations of Computer Science & Technology (IJFCST) Vol.6, No.1, January 2016