Abstract: Ad-hoc networks have lots of challenges than traditional networks. It has challenges like infrastructureless and selforganizing networks. They don't have any fixed infrastructure. In Manets there will be no centralized authority to manage the network. Nodes have to rely on other nodes to keep the network connected. As the ad-hoc network is dynamic and every transmission in these networks become vulnerable to many number of attacks and security becomes a major issue. In this survey paper we study the different security attacks to ad-hoc networks and also discussed available solutions. We try to provide a brief introduction to the types of attacks and possible counter measures to prevent the attacks.

Keywords: Attacks, MANET, IDS, DOS

1. INTRODUCTION
A Mobile Ad hoc Network (MANET) is a collection of mobile node connected through wireless links. In MANET all nodes are connected with the nodes near in communication range. So if a node wants to communicate to another node it sends the data to the destination node through the neighbor node. Now the neighbor node will act as router like wired network. In wired network security protocols will be implemented in router node. But implementing security in MANET is a challenging task. Because here node itself will be acting as a router node. So identifying neighbor node as a legitimate node or malicious node is a difficult thing in MANET shown in Figure 1. Communication in the network depends upon the trust on each other also communication can work properly if each node co-operate for data transmission. As MANET has no fixed infrastructure, they have more security threats when compared to the infrastructure based wireless networks. Each communication layer has lots of attacks in MANET due to its dynamic

Fig 1. MANET

nature, lack of centralized monitoring, and limited resources like bandwidth and battery power. In this paper we have surveyed the security weakness in each layer and the current available security solutions. First section will describe security goals required for secure routing in MANET. Second Section gives detailed description of various attacks on MANET. Third section will provide various solutions proposed by the researchers against these attacks. Last section provides future directions for a secure MANET.

2. SECURITY GOALS
The following are five major security goals which require preventing from attacks [2]:

a) Authentication: Authentication ensures that the communication or transmission of data is done only by the authorized nodes. Without authentication any malicious node can pretend to be a trusted node in the network and can adversely affect the data transfer between the nodes.

b) Availability: Availability ensures the services should be available even in the presence of the attacks. Systems should be able to take care of various attacks such as denial of services, energy starvation attacks, and node misbehavior.

c) Confidentiality: Confidentiality ensures that data should be accessible only to the intended party. No other node except sender and receiver node can read the information. This is implemented through data encryption techniques.

d) Integrity: Integrity ensures transmitted data is not being altered by any other malicious node.

e) Non-Repudiation: Non-repudiation ensures that neither a sender nor a receiver should not deny a transmitted message.

3. MANET Security Challenges [1]

1) Dynamic topology: In Manets node may join or leave dynamically. As node moves frequently establishing trust among nodes is very difficult.

2) Battery Constraints: Mobile nodes will be running with battery. If node power utilized unnecessarily then node may come to idle state. [4]

3) Lack of Central Authority: In MANET there will be no centralized authority like infrastructure network. So implementing security without centralized authority is a challenging task.
4) **Insecure Environment**: Nodes may move randomly in MANET. So malicious node may attack and steal the data.

4. **Attacks on MANET**
   **Active Attacks**
   Performed by attackers for replicating, modifying and deletion of exchanged data. They try to change the behavior of the protocol [3]. These attacks are meant to degrade or prevent message flow among the nodes. Such attacks collectively can be called as DOS attacks that either degrade or completely block the communication between the nodes. Another type of attack involves insertion of extraneous packets in the network to cause congestion. Outdated routing information may be replayed back to the nodes in the network. Active attacks can be detected sometimes and this reason makes active attack less used by an attacker.

   **Passive Attacks**
   As discussed in [16] this type of attack involves unauthorized listening of the routing packets. Attacker may eavesdrop on all the routing updates. In this case an attacker does not disrupt the operation of a routing protocol rather it only listens to it to discover the valuable information about the routing. Such attacks are difficult to be detected. From the routing packets an attacker may understand about a node which is important in the network and route to that node is being requested very often by every other node. So an attacker tries to disable this node to bring the network down. Includes Covert channels, Traffic analysis, Shifting to compromised keys.

   **Physical Layer Attacks**
   1) **Eavesdropping**: In eavesdropping attack, attacker tries to get the secret information during communication.
   2) **Jamming**: Jamming attack will be implemented by knowing the frequency malicious nodes sends jam signal to disturb the communication.
   3) **Active Interference**: An active interference is a type of denial of service attack which distorts the communications

   **Link Layer Attacks**
   The data link layer can classified as to what effect it has on the state of the network as a whole .
   1) **Selfish Misbehaviour of Nodes**: In the selfish misbehaviour of nodes act as selfish and will not be willing to participate in forwarding process.
   2) **DOS Attack**: This attack prevents authorized access of resources to the legitimate node.
   3) **Resource Exhaustion**: Malicious nodes makes repeated collision to drain the battery power.
   4) **Malicious Behaviour of nodes**: The main task of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighboring nodes.

### Table 1. Layer Attacks in MANET

<table>
<thead>
<tr>
<th>Layers</th>
<th>Attacks</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Jamming</td>
<td>Using Spread spectrum mechanisms FHSS, DHSS</td>
</tr>
<tr>
<td></td>
<td>Eavesdropping</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active Interference</td>
<td></td>
</tr>
<tr>
<td>Data Link</td>
<td><strong>Selfish Misbehaviour of Nodes</strong></td>
<td>Secure link layer protocol like LLSP using</td>
</tr>
<tr>
<td></td>
<td><strong>Malicious Behaviour of nodes</strong></td>
<td>WPA</td>
</tr>
<tr>
<td></td>
<td><strong>DOS</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Misdirecting Traffic</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Attacking neighbour sensing protocols</strong></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td><strong>Worm Hole Attack</strong></td>
<td>Securing routing protocols like SAODV, SAR,</td>
</tr>
<tr>
<td></td>
<td><strong>Black Hole Attack</strong></td>
<td>ARAN to overcome blackhole, impersonation</td>
</tr>
<tr>
<td></td>
<td><strong>Byzantine Attack</strong></td>
<td>attacks, packet leashes, SECTOR</td>
</tr>
<tr>
<td></td>
<td><strong>Information Disclosure</strong></td>
<td>mechanism for wormhole attack</td>
</tr>
<tr>
<td></td>
<td><strong>Resource Consumption</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Routing Attack</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Routing Table Overflow</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Routing Table Poisoning</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Packet Replication</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Route Cache Poisoning</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Rushing Attack</strong></td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td><strong>Session Hijacking</strong></td>
<td>Securing End to End communication (SSL, TLS,</td>
</tr>
<tr>
<td></td>
<td><strong>SYN Flooding</strong></td>
<td>SET)</td>
</tr>
<tr>
<td>Application</td>
<td><strong>Virus, Worms</strong></td>
<td>Firewalls</td>
</tr>
<tr>
<td></td>
<td><strong>Dos, Man in the Middle Attack</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Impersonation</strong></td>
<td></td>
</tr>
</tbody>
</table>
4) Attacking neighbour sensing protocols: Malicious nodes advertise fake error messages so that important links interface are marked as broken.

Network Layer Attacks

Black Hole Attack:
In black hole attack the attacker node advertises other node that it has shortest route to reach destination. If this reply reaches before the actual reply a forged route will be established including the malicious node. Now the malicious node can drop packet or perform DOS attack or Man in the middle attack.

Wormhole Attack:
In wormhole attack involves the cooperation between two attacking nodes. One attacker captures the packet and tunnels it to the other attacker. The link between the attackers is high speed communication link. These two attackers makes the topology under their control.

Routing Table Poisoning Attack:
In routing table poisoning attack attacker poisons the routing table by changing the routes in the routing table. Other way is to inject RREQ packet with high sequence number. The packet with low sequence number will be deleted. This leads to selection of wrong routes.

Sleep Deprivation:
In this attack resources of a node is consumed unnecessarily by the attacker node by generating requesting for unexisting destinations. These leads to battery wastage and network bandwidth wastage.

Impersonation Attack:
In impersonation attack attacker nodes impersonates itself as legitimate node and sends false routing information and masks itself as sending from trusted node.

Node Isolation Attack:
In this attack attacker node prevents network information about a particular node or group of nodes from the rest of network. Hence other nodes will not know about the existence of this node.

Location Disclosure Attack:
In location disclosure attack attacker node by probing or by traffic analysis will locate the node and structure of the network.

Rushing Attack:
In rushing attack attacker node rushes to send route request to target nodes. These makes the target node to reject the legitimate node route request and makes attacker node to insert in any communication.

Blackmail:
The attack happens due to lack of authenticity and it grants provision for any node to corrupt other node’s legitimate information. Nodes usually keep information of perceived malicious nodes in a blacklist. This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and tell other nodes in the network to add that node to their blacklists and isolate legitimate nodes from the network.

The Invisible Node Attack (INA):
Andel et al.[19] have defined the invisible node attack and proved it to be different from the existing attacks (man in the middle, masquerading, and wormhole) and established its uniqueness. They have defined it as In any protocol that depends on identification for any functionality, any node that effectively participates in that protocol without revealing its identity is an invisible node and the action and protocol impact is termed an INA. Discussing the effects of INA on different routing protocols, they have shown it to be an unsolvable attack so far.

Byzantine Attack:
In Byzantine attack
A compromised intermediate node works alone or a set of compromised intermediate node works in collusion and carry out attacks. These attacks create routing loops, forwards packets through non optimal paths. It is difficult to detect this attack.

Transport Layer Attacks

Session Hijacking:
In session hijacking attacker hijacks the session after its set up. Here the attacker spoofs the IP address and launches the various attacks using the right sequence number.

Application Layer Attacks

Malicious code attacks:
Malicious code attacks include, viruses, Worms can attack both operating system and user application.

Multilayer Attacks
The DoS attacks, impersonation attacks, man-in-the-middle attacks, and many other attacks can target multiple layers.

Denial of service:
Denial of service (DoS) attacks could be launched from several layers. An attacker can employ signal jamming at the physical layer, which disrupts normal communications. At the link layer, malicious nodes can occupy channels through the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning[6]. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks.

Impersonation attacks: Impersonation attacks are just the first step for most attacks, and are used to launch further sophisticated attacks.

Man-in-the-middle attacks: An attacker sits between the sender and the receiver and sniffs any information being sent between two ends.
5. Security Solutions in MANET

**Physical Layer**
At this layer spread spectrum technology such as frequency hopping (FHSS) & direct sequence (DSSS) [5] can be used to prevent eavesdropping attack. It changes frequency in random fashion to make signal capture difficult. Also minimizes the potential for interference from other radio & electromagnetic devices.

**Link Layer**
Traffic analysis is prevented by encryption at data link layer. WEP has been widely criticized. A dynamic mix method is used to hide the source & destination information during message delivery via cryptography method & to “mix” nodes in the network [12]. WEP and WPA provides authentication mechanism for any node to join in network. LLSP is used to provide security at data link layer. But LLSP uses encryption algorithm to prevent from attacks. SLSP is used to prevent DOS attack. Man in the middle attack and its suitable for authenticating new nodes and not suitable for real time traffic.

**Network Layer**
SAODV routing protocol is used to prevent against blackhole attack but it requires heavy weight encryption algorithm[8]. (SAR) can be used to defend against black hole attacks. In SAR it needs excessive encryption and decryption at each hop. ARAN can be used to defend against impersonation & repudiation attacks. It may not defend against authenticated selfish nodes. Security protocol SEAD is used against modification attacks [13].

**Transport Layer**
In transport layer end-to-end encryption provides message confidentiality between two nodes. SSL protocol implements end to end security for a session. attacks are DoS attacks, impersonation attacks, man-in-the-middle attacks. The countermeasures for these attacks need to be implemented at different layers.

**Defense against multi-layer attacks**

**Denial of service**: Denial of service (DoS) attacks can be launched from several layers. In physical layer attacker employs signal jamming attack which disturbs communications. At the link layer, malicious nodes can occupy channels through the capture effect, which takes advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing table overflow attack fills the routing table with unnecessary or fake routes which leads to a DOS attack. At the transport and application layers. SYN flooding makes the other node to overload and it leads to DoS attacks.

**Application Layer**
In Application layer firewalls can effectively prevent many attack & application specific modules. An intrusion detection system (IDS) can be used as second line of defense.

**MultiLayer Attack**
Multiple layer attacks are difficult to detect. Because these attack may happen in data link layer or network layer or in transport layer. Such attacks are many IDS are currently available in MANET for detecting intrusions. In anomaly detection if there is a deviation from normal behavior then it will be identified as intrusion. But in anomaly based detection it may not detect if it deviates from normal activity. There is a chance for high false positive rate. Bella et al.

---

**Table 2. Security Solution and its limitations in Network Layer**

<table>
<thead>
<tr>
<th>Author</th>
<th>Attack</th>
<th>Solution</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cerri. D Politec di Milan, Ghioni A</td>
<td>Blackhole Attack</td>
<td>SAODV</td>
<td>Requires heavyweight asymmetric cryptographic algorithm</td>
</tr>
<tr>
<td>Seung Yi, Prasad Naldurg, Robin Kravets [20]</td>
<td>Replay Attacks</td>
<td>SAR</td>
<td>Require excessive encrypting and decrypting at each hop. Discovered route may not be shortest path</td>
</tr>
<tr>
<td>Davide Cerri and Alessandro Ghioni</td>
<td>DOS, Man in the Middle Attack</td>
<td>Adoptive SAODV</td>
<td>Routing Overhead and High Processing Power, Time delay</td>
</tr>
</tbody>
</table>
[22] propose a behavior based IDS that bases node reputation on the energy it uses for others in comparison with the energy it uses for itself. Buchegger and Le Boudec propose a distributed IDS called CONFIDANT which extends DSR by measuring reputation with “no forwarding” behavior. Michiardi and Molva propose an IDS called CORE. Neighbors of a suspect calculate its subjective reputation score from experience of some property f (for example, DSR routing or packet forwarding) weighting earlier and later observations differently, and nodes calculate a suspect’s functional reputation over multiple f weighting various f differently and aging (decreasing over time) the reputations of inactive nodes. Vigna et al. [23] propose a multitrust traffic based IDS. The authors focus on auditing AODV data. They found packet drop attacks had the best detection rate and spoofing attacks had the lowest false positive rate. Tseng et al. use an AODV based FSM to establish a specification for a traffic based IDS. Distributed network monitors maintain an FSM for each routing transaction.

6. Future Directions

There are lots of researches done in MANET for so many years. Many security solutions are provided by researchers. But still the security solutions in MANET are not sufficient due to its various challenges. DOS attack, Man in the middle attack is still open in MANET. More research is needed on secure routing protocol, key management, trust based systems, integrated approaches to routing security, data security in different level and cooperation enforcement. The security solutions of existing routing protocols are subject to a variety of attacks that can allow attackers to influence a victim’s selection of routes or enable denial-of-service attack. So, necessity of secure routing protocol is inevitable. Cryptography is one of the most common security mechanisms and its strength relies on the secure key management. The public cryptography scheme depends upon centralized CA (Certificate Authority) which is known as a security weak point in MANET. Symmetric cryptography is efficient but suffers from potential attack on key distribution. Hence, efficient key agreement and distribution in MANET is an ongoing research area. Finally, Building a trust-based system and integrating it to the intrusion detection system can be considered as a future research. Identifying new security threats as well as new countermeasures demands more research in MANET.

7. Conclusion

In this paper we have surveyed several attacks related to different layers in ad-hoc networks. As ad hoc networks are vulnerable to many types of attacks the security of this network is a major issue. Many researchers are trying to prevent the attacks done on ad-hoc networks at various levels. A variety of such attacks have been discussed. We have overviewed the challenges and solutions of the security threats in mobile ad hoc networks. In our study, we present a variety of attacks related to different layers. Here we focus on the currently used security countermeasures to defend against these attacks. A lot of research is still being carried out to identify new threats to ad-hoc networks & securing them.

References


