MANETs is a collection of wireless mobile nodes forming flexible networks, thus they do not require any existing infrastructure and centralized access points. With increase in the use of Mobile Ad hoc Networks security became an fundamental requirement due to its dynamic topology, limited processing capability, bandwidth constraints, lack of central control and high bit error rate. To provide protected communication between mobile nodes, there is need to build multi-faceted security and routing solution to overcome from these challenges. In this paper we attempts to give a review on various secure routing protocols, security analysis of available secure protocols by identifying their advantages and disadvantages as well as comparing their relative metrics and requirements. This paper structured into three sections: Section first includes a brief introduction of MANETs with their routing protocols. Section second explains the security attacks and challenges in MANETs. Third, discusses the security analysis of each secure routing protocols with comparison.

**KEYWORDS:** MANETs, Security Attacks, Secure routing protocols, Ad hoc security.

### 1. INTRODUCTION

#### 1.1 MANETs:
Mobile Ad Hoc Networks (MANETs) are formed by mobile nodes having no infrastructure. In MANETs mobile nodes act as router. These nodes connect themselves on wireless medium and thus form dynamic network with wireless link. Intermediate nodes are used for communication because of limited bandwidth. Mobile ad-hoc networks are new paradigm of wireless communication for mobile nodes. There is no fixed Infrastructure for mobile switching. Nodes within a network range communicate directly via wireless links while those which are far apart rely on other nodes to relay messages. Node mobility causes frequent Changes in topology. The wireless nature of communication and lack of any security infrastructure raises several security problems discussed in further sections. As Figure 1 shows a mobile ad- hoc network with 5 nodes in which first node can communicate with last node via second, third and fourth intermediate nodes, and vice versa.

![Figure 1 Mobile Ad Hoc network](image)

### 1.2 ROUTING PROTOCOLS IN MANETs:
Mobile Ad-hoc routing protocols can broadly be classified into three categories as:

- **Proactive Routing Protocols.**
- **Reactive Routing Protocols**
- **Hybrid Routing Protocols.**

The approaches involve a trade-off between the amount of overhead required to maintain routes between node pairs (possibly those pairs that will never communicate), and the latency involved in discovering new routes as required.

**Proactive or Table-Driven Protocols** involve attempting to maintain routes between nodes in the network at all times, plus when the routes are not currently being used. Updates to the individual links within the networks are propagated to all nodes or a relevant subset of nodes, in the network such that all nodes in the network eventually share a consistent view of the state of the network. The advantage of this approach is that there is little or no latency involved when a node wishes to begin communicating with an arbitrary node that it has not yet been in communication with. The disadvantage is that the control message overhead of maintaining all routes within the network can rapidly overwhelm the capacity of the network in very large networks, or situations of high mobility. Examples of pro-active protocols include the Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR) and etc.

**Reactive or On-Demand Protocols** involve searching for routes to other nodes only as they are needed. A route discovery process is invoked when a node wishes to communicate with another node for which it has no route table entry. When a route is discovered, it is maintained only for as long as it is needed by a route maintenance process. Inactive routes are purged at regular intervals. Reactive protocols have the advantage of being more scalable than table-driven protocols. They require less control traffic to maintain routes that are not in use than in table-driven methods. The disadvantage of these methods is that an additional latency is incurred in order to discover a route to a node for which there is no entry in the route table. Dynamic Source Routing (DSR), Ad-hoc On-demand Distance Vector Routing (AODV) and etc.

**Hybrid Routing Protocols** such as the Zone Routing Protocol (ZRP), which employs a combination of proactive and reactive methods. The Zone Routing Protocols maintains groups of nodes in which routing between members within a zone is via proactive methods, and routing between different groups of nodes is via reactive methods.

### 2. SECURITY ATTACKS IN MANETs:
MANETs are unsecure from various attacks. ATTACKs can cause reduction of network traffic and alteration of control message fields or forwarding routing messages.
Main goal of Attacks:

a) Increase latency of particular packets.
b) Decrease overall network throughput.
c) Break down a particular node or link.
d) Divert packets to affect bandwidth.

The attacks in mobile ad-hoc network are done in order to interrupt the communication or to steal the information. The attacks in mobile ad hoc networks can be broadly classified into two distinct categories viz. Active attacks and Passive attacks. An active attack is that attack in which any data or information is inserted into the network so that information and operation may harm. It involves modification, fabrication and disruption and affects the operation of the network. Example of active attacks is impersonation, spoofing. A passive attack obtains data exchanged in the network without disturbing the communications operation. The passive attacks are difficult to detection. In its, operations are not affected, but tries to discover valuable information by listening to traffic and sniffing about the network. Some of the most common attacks on mobile ad-hoc networks include:

2.1. Wormhole Attacks
In wormhole attack is one of the most complicated attacks in MANETs mainly for reactive type of routing protocols. In this type of attack a pair of malicious nodes creates tunnel between two groups of nodes. One malicious node receives the packet from the one end and tunnels them to another location in the network. The tunnel between two malicious nodes is called wormhole. It could be reputable through a single long range wireless link. The attacker nodes may create a wormhole even for the packets which are not addressed to itself because of the broadcast nature of MANETs.

2.2. Packet Replication:
In packet replication attack an attacker replicate stale packet. This consumes battery power resources available to the nodes and their additional bandwidth.

2.3 Denial-of Service Attack:
A Denial-of Service Attack is one of the attacks in MANETs that affects proactive Type routing protocols. The main goals of this type of attack are:

1) Modifying the packet header.
2) Inducing Junk packets into the network.
3) Routing table overflow.

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include

- Attempts to "flood" a network, thereby preventing legitimate network traffic.
- Attempts to disrupt connections between two machines, thereby preventing access to a service.
- Attempts to prevent a particular individual from accessing a service.
- Attempts to disrupt service to a specific system or person.

Denial-of-service attacks can essentially disable your computer or your network. Denial-of-service attacks come in a variety of forms and aim at a variety of services. There are three basic types of attack:

- consumption of scarce, limited, or non-renewable resources
- destruction or alteration of configuration information
- physical destruction or alteration of network components

2.4. Byzantine Attack
In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behaviour.

2.5. Blackhole Attack:
Blackhole Attack is one of the major attacks in MANETs mainly for proactive & reactive type of routing protocols. A malicious node provides fake routing information by advertising itself having shortest path to the source node. When malicious node receives the route request to the destination node, it sends a reply consisting of a definite shortest route. If the reply request send by the malicious node reaches the source node before the reply from the genuine node. As the malicious node able to insert itself between the genuine communicating nodes, it will be able to drop or can change the destination address of the packets passing through them.
2.6. Gray-hole attack
This attack is also known as routing misbehavior attack. It leads to messages dropping. It has two phases. In the first phase a valid route to destination is advertise by nodes itself. In second phase, with a certain probability nodes drops intercepted packets.

3. Various Challenges in MANET Security are discussed as follows:
- **Confidentiality**: Protection of any information from being exposed to unauthorised entities. Because intermediate mobile nodes receive the packets for other recipients, the information being routed in MANETS can be easily eavesdropped.
- **Availability**: Services should be available whenever required and should endure survivability regardless of DOS attacks. As on MAC and Physical layer attacker can use jamming techniques to hinder with communication on physical channel. Attacker can interrupt the routing protocol on network layer and on higher layers the attacker could bring down high level services such as key management service.
- **Authentication**: Enables a node to defend the characteristics of the peer node it is communicating, without which an attacker would impersonate a node, thus gaining unauthorised access to resource, sensitive information and interfering with operation of other nodes.
- **Non-repudiation**: Ensures that sending and receiving nodes can never deny ever sending and receiving the message. Non-repudiation is useful for detection and isolation of compromised nodes.
- **Integrity**: Guarantees that a message being transmitted is never altered.

3. EXISTING SECURE ROUTING PROTOCOLS:
Operation of secure routing plays a very important role in MANETs security. Due to rapidly increasing demand in mobile ad hoc networks the need for secure routing protocols becomes unavoidable so that the different security attacks can be prevent. In this section we will discuss different existing secure routing protocols with their advantages and disadvantages along with a comparison table.

3.1 SEAD
It stands for Secure Efficient Ad hoc Distance Vector Routing Protocol. SEAD is a proactive secure routing protocol based on DSDV routing protocol. It relies on one way hash chain of security to guard against Denial of Service. The idea behind SEAD is to authenticate the sequence no. and metric of a routing table update message using hash chain functions. Long lived routing loops can be reduced by using destination sequence numbers which provide replay protection of routing update messages in SEAD.
- **Advantages**: It is robust against multiple uncoordinated attackers, compromised nodes or active attackers. It plays important role in computation and bandwidth-constrained nodes by using efficient, inexpensive cryptographic primitives.
- **Disadvantages**: It cannot authenticate smaller sequence numbers and it doesn’t provide a way to prevent an attacker from tampering with “next hop” or “destination” columns.

3.2 SAODV
This protocol is designed to secure AODV. To utilizes security feature like authentication and integrity SAODV is an enhancement over AODV. To authenticate non mutable fields messages such as route request (RREQ) and route reply (RREP) it uses digital signatures and to secure hop count information it uses hash chains. IPSec provides secure data messages in transmission in MANETs. Digital Signature is used when RREQ is sent from the source node to the destination node, sender signs the message. Intermediate nodes check the signature before creating or updating a reverse route. And only if the signature is verified they store the reverse route at last the destination node signs the RREP with its private key.
- **Advantages**: Replay, delay attacks can be prevented by sequence number system. Reducing the hop count to increase the chance of being in the route path this can be prevented by using one way hash chain for hop authentication.
- **Disadvantages**: Malicious node can pass the received authenticator and hop count without changing them. Public key cryptography imposes high processing overhead.

3.3 ARAN
ARAN is a on demand secure routing protocol and it relies on digital certificates. It provides authentication, message integrity and non repudiation. ARAN ensure that each node knows the correct next hop on a route to the destination by public key cryptography. During message delivery between source and destination it provides end to end guarantee.
- **Advantages**: ARAN is capable of protecting itself against spoofing, modification, fabrication, Denial of service attacks. It is secure as long as CA is not compromised, network structure is not exposed.
- **Disadvantages**: It leads to wastage of bandwidth. It requires extra memory, has high processing overhead for encryption. Because it doesn’t use hop count, so the discovered path may not be optimal.

3.4 ARIADNE:
A secure extension of DSR is Ariadne. It uses one way Message Authentication Code key chain TESLA. TESLA is an efficient authentication scheme that requires loose time synchronization. Ariadne assume
that the network links are bidirectional and network may drop, reorder and duplicate packets. In it each node must be able to estimate the end to end estimation time to any other node in the network. Firstly it verifies route authenticity and secondly it checks that no node is missing on RREQ message. It uses one of the three schemes for authenticate routing messages: (a) Shared secrets between each pair of nodes. (b) Shared secrets between communicating nodes combined with digital signatures, or broadcast authentication.

- **Advantages:** It prevents many types of DOS attacks. In it any alteration of node list can be detected and it prevents attackers with uncompromised routes.
- **Disadvantages:** It cannot defend against active attacks. Second the key exchange is very complicated.

### 3.5 SLSP

It stands for Secure Link State Protocol. It known as standalone and self contained link state discovery protocol. SLSP is responsible for securing the route discovery and distribution of link state information. It provides secure proactive topology discovery which is beneficial for network operation. In this protocol every node is assumed to be equipped with public/private key pairs and single network interface per node within the Mobile Ad hoc Networks domain. Each node update its neighbourhood by neighbour lookup protocol and periodically floods link state update packets to proliferate link state information.

- **Advantages:** SLSP is robust against DOS and Byzantine attacks. Nodes can make a decision if they want to authenticate the public key or not.
- **Disadvantages:** It is still vulnerable to colluding attacks.

### 3.6 SRP

It stands for Secure Routing protocol and it is on demand routing protocol. Basic idea behind this secure protocol is to build a security association between the source and destination with sole assumption that at the beginning all nodes share a group key K and can be trusted. After that the key can be used to encrypt and decrypt the messages. This algorithm is suitable for various applications like military and emergency situations.

- **Advantages:** It guarantees the discovery of right connectivity information over an unknown network. Confidentiality is protected in presence of malicious node. Alteration of messages cannot be possible. Routing loops cannot be formed through malicious actions. Route signalling cannot be spoofed. Fabricated routing messages cannot be injected into network.
- **Disadvantages:** It exposes network configuration with unencrypted routing path. Vulnerable to invisible node attack.

### 3.7 SAR

SAR uses AODV or DSR as a base protocol. To take secure and efficient routing decision this protocol considers trust level mechanism. It embeds the security metric into RREQ packet itself and changes the forwarding behaviour of the protocol. As intermediate nodes receive RREQ packet with a security metric or trust level the node can only process the packet or forward it if it can provide the required security or trust level.

- **Advantages:** To improve the relevance of routes discovered by ad hoc routing protocols it enables the use of security as a negotiable metric. SAR increase overhead due to calculations of encryption and decryption at each node.
- **Disadvantages:** It doesn’t describe anything about how to implement the security level as a metric. Route discovery can be fail due to not having proper security clearance.

### Comparison of Secure Routing Protocols:

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Secrets Key</th>
<th>MAC</th>
<th>Digital Signature</th>
<th>Hash Chain</th>
<th>Cryptography Mechanism</th>
<th>Assumption</th>
<th>Verification Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEAD</td>
<td>Initial secret Key K for hash functions</td>
<td>-----</td>
<td>-----</td>
<td>One way hash function to authenticate the sequence number</td>
<td>-----</td>
<td>Secure way of delivering initial secret key K</td>
<td>Hash chain verification</td>
</tr>
<tr>
<td>SAODV</td>
<td>Public/Private Key per node for each node</td>
<td>-----</td>
<td>Used by Sender</td>
<td>One Way Hash function to authenticate hop counts</td>
<td>-----</td>
<td>Key Distribution Network</td>
<td>Digital Signature Verification Mechanism</td>
</tr>
<tr>
<td>ARAN</td>
<td>Public/Private Key per node for each node</td>
<td>-----</td>
<td>Public Key Cryptography</td>
<td>Trusted Certificate Server</td>
<td>-----</td>
<td>Public Key Cryptography Verification mechanism</td>
<td></td>
</tr>
<tr>
<td>ARIADE</td>
<td>MAC keys</td>
<td>MACasf</td>
<td>TESLA</td>
<td>Nodes have loosely Synchronized Clocks</td>
<td>-----</td>
<td>MAC verification mechanism</td>
<td></td>
</tr>
<tr>
<td>SLP</td>
<td>Public/Private Key per node for each node</td>
<td>MAC</td>
<td>Threshold Cryptography</td>
<td>Single network Interface per node</td>
<td>Threshold cryptography for key authentication, MAC verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRP</td>
<td>SA between Source and Destination</td>
<td>MAC Calculation</td>
<td>-----</td>
<td>Secure way of delivering the SA</td>
<td>-----</td>
<td>MAC verification mechanism</td>
<td></td>
</tr>
<tr>
<td>SAR</td>
<td>Symmetric encryption key</td>
<td>-----</td>
<td>-----</td>
<td>Simple encryption and decryption on each node</td>
<td>Shared key distribution network</td>
<td>Trust level mechanism</td>
<td></td>
</tr>
</tbody>
</table>
4. CONCLUSION:
This paper mainly focused with a review on various security attacks and secure routing algorithms in MANETs along with their comparison on various parameters have given. We have examined that different authentication mechanisms and secure routing protocols till yet defend against these attacks to a certain level, no one is perfect since most of the solutions are having drawbacks such as more time delay, much network routing overhead because of newly introduced packets, exposes network configuration, wastage of bandwidth etc. To provide more security and immovability in MANETs there is need to develop efficient security mechanism and secure routing protocols.

REFERENCES
19. K.P. Manikandan, Dr. R. Satyaprasad, Dr. Rajasekhararao, “Analysis and Diminution of Security Attacks on Mobile Ad hoc Network”.IJCA Special Issue on “Mobile Ad-hoc Networks “MANETs, 2010