Layerwise Security Framework with SNAuth-SPMAODV to defend Denial of Service attack for Mobile adhoc Networks in Hostile Environment

MANETs are subject to layerwise attacks and almost all the existing solutions do not take this aspect into consideration. Security issues are analyzed for individual layers namely application layer, transport layer, network layer, link layer and physical layer. The ultimate goal of the security solution for MANETs is to provide security services, such as confidentiality, integrity, authentication, non-repudiation, anonymity and availability. In order to achieve these goals, the security solution should provide complete protection spanning the entire protocol stack. There is no solution that provides layer wise security which is a major challenge for Mobile Adhoc networks. As the MANET is basically an infrastructure less network, the security attacks reduce the performance of the network. As the attacks affect the different layers of the network, the solutions to be provided should also take this aspect into consideration. How to design MANET security layers that can work well in hostile environments will be one major challenge in Mobile ad hoc networks, and none of the existing works have fully addressed it.

2.1 Famous Layerwise Security Approaches for MANET

Some of the famous layerwise security approaches for MANET are chosen from the literature and analyzed.

2.1.1 Session Initiation Protocol

Session Initiation Protocol (SIP) is an application layer control protocol used for establishing, modifying and tearing down multimedia sessions, both unicast and multicast (Rosenberg, 2002). It has been standardized within the IETF for the invitation to multicast conferences and Internet telephone calls. The most important SIP operation is that of inviting new participants to a call. To achieve this functionality to distinguish different SIP entities are:

**Proxy server:** A proxy server receives a request and then forwards it towards the current location of the callee either directly to the callee or to another server that might be better informed about the actual location of the callee.

**Redirect server:** A redirect server receives a request and informs the caller about the next hop server. The caller then contacts the next hop server directly.

**User Agent (UA):** A logical entity in the terminal equipment that can act as both User Agent Client (UAC) and User Agent Server (UAS).

**Register:** The register server is mainly thought to be a database containing locations as well as user preferences as indicated by the user agents. In detail, a SIP call setup is essentially a
3-way handshake between a caller (UAC) and a callee (UAS). For instance, the main legs are an INVITE (to initiate a call) message, a 200 OK (to communicate a definitive successful response) message and an ACK (to acknowledge the response) message. However, implementations can make use of provisional responses, such as 180 RINGING message. 180 RINGING message indicates that the callee (UAS) receiving the INVITE message is trying to alert the user. The call setup is followed by the actual media transfer (speech and video) using the Real-time Transport Protocol (RTP). The release of the call is made by means of the BYE message and the successful call release can be communicated through a 200 OK message.

2.1.2 Wireless Transport Layer Security (WTLS)

The transport layer protocols in MANET provide end-to-end connection, reliable packet delivery, flow control, congestion control and clearing of end-to-end connection. Like TCP protocol in the Internet model, the nodes in a MANET also are vulnerable to the Denial of Service (DoS) attacks. The extensive use of mobile communication has created an important demand for value-added services. WAP (Wireless Application Protocol) is a framework for developing applications to run over wireless networks. WAP is developed by an international industry-wide organization called the WAP Forum. WTLS (Wireless Transport Layer Security) is the security protocol of the WAP protocol suite (Saarinen, 1999).

WTLS operates over the transport layer and provides end-to-end security, where one end is the mobile client, and the other end is the WAP gateway. WAP gateway acts as a proxy of the mobile client to access an application server hosted somewhere on the Internet. The communication beyond the WAP gateway is conducted using the regular Internet (TCP/IP) protocol suite. A set of handshake messages is exchanged in order to set up a secure environment between the mobile client and the server (WAP gateway). Cryptographic algorithms, keys and related parameters are negotiated during the handshake. Once the handshake messages are exchanged and session key is generated, all WTLS and upper layer protocol messages can be exchanged in encrypted form. In this way, confidentiality and integrity are provided. Authentication is an optional service in WTLS. Authentication is provided if the parties provide digital certificates during the handshake. Certificates are digital identities that contain public-keys to be used during the key exchange. Certificates are issued by trusted Certification Authorities (CA) with a digital signature on the certificate content. Validation of a certificate means the legitimacy of the enclosed public-key. A party, who does not have a certificate, should use an unapproved public-key. Therefore, the communication party cannot be authenticated. Certificate validation, authentication and session key exchange use asymmetric public-key cryptosystems that require computation-intensive processes, and are therefore slow. Speed is inversely proportional to the key size used in public-key cryptosystems. Since the
processing power of mobile clients is limited, relatively smaller keys are selected for WTLS. Moreover, data transfer rate is also limited in mobile communication environment and using smaller keys would help to save bandwidth (Kahraman and Gokhan, 2002).

**Public-key cryptosystems in WTLS**

Public-key cryptosystem operations use two different, but related keys: public-key and private-key. Public-key operations are for encryption and signature verification. Private-key operations are for decryption and certificate revocation. Key exchange operations are also public-key cryptosystem operations, but their nature depends on the cryptosystem used.

Public-key cryptosystems are used in the WTLS handshake for key exchange and certificate verification purposes. Authentication is automatically provided when key exchange is performed using certified keys. WTLS supports two public-key cryptosystems: RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) (Miller, 1996).

**2.1.3 IP Security (IPSec)**

IPSec developed by Internet Engineering Task Force (IETF) is a suite of protocols used to secure traffic at the IP layer. The main protocol components of IPSec are Authentication Header (AH) and Encapsulating Security Payload (ESP), which describe the IP header extensions for carrying cryptographically protected data, and Internet Key Exchange (IKE) (Islam.S, 2006). IPSec is based on Security Associations (SAs). A security association is a simplex connection whose traffic is protected by security service designated by parameters such as the encryption algorithm, keys, and lifetime. SA is uniquely identified by a tuple of Security Parameter Index (SPI), destination IP address, and IPSec protocol (AH or ESP). IPSec protocol is based on the establishment of Security Association between packet sender and receiver. SA is set up in the IKE phase by Diffie-Hellman (DH) algorithm. Although DH algorithm is subject to man-in-the-middle attack, this problem could be alleviated in most of the Mobile Ad Hoc Network application scenarios due to the following reasons: The nodes can always be pre-assigned with certain initial shared secret by their manufacturer; these secrets can be used at the initial IKE phase to authenticate the validity of the DH connections.

This pre-configured shared secret can then be available in most MANET systems, and is essential for adopting IPSec secure communications and membership verification. Upon the establishment of membership management mechanism and the corresponding trust model in MANET, IPSec can be an appropriate choice for MANET network layer to protect both routing information and data message. For IPsec to work, communication entities must share a public key. This key exchange process is accomplished through key management mechanisms that refer to the creation, distribution, installation, authentication, and access control of the keying
material. A number of cryptographic algorithms are also specified in IPsec for authentication and encryption (Ghosh et al., 2005).

**Key Management Protocols in IPsec**

The main goal of key management is to share a secret among a group of participants. Figure 2.1 shows IP security document roadmap. The common approaches to key management are:

- **Key redistributions**: Keys are distributed to all participants before the communication.
- **Key transport**: Keys are generated in one communication entity and transport to all participants.
- **Key arbitration**: Keys are created and distributed by a central arbitrator to all participants.
- **Key agreement**: Participants agree on a secret key for further communications.

![Figure 2.1: IP Security document roadmap](image)

**2.1.4 CCMP-AES Model**

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol (Junaid et al., 2006). The CCMP algorithm is based on the U.S. federal government's Advanced Encryption Standards (AES). CCMP offers enhanced security compared with similar technologies such as Temporal Key Integrity Protocol (TKIP). CCMP employs 128-bit keys and a 48-bit initialization vector that minimizes the vulnerability of black hole attack. CCMP is a robust security network association (RSNA) data confidentiality and integrity protocol. CCMP is based on the Counter Mode with CBC-MAC (CCM) of the
AES encryption algorithm. CCM is a generic authenticate-and-encrypt block cipher mode. A unique temporal key (for each session) and a unique nonce value (a value that’s used only once for each frame) are required for protecting the Medium Access Control Protocol Data Unit (MPDU). CCMP uses a 48-bit Packet Number (PN) to protect the MPDUs (Whiting et al., 2002). CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting cipher text using the following algorithm. Figure 2.2 shows CCMP encapsulation algorithm.

**Figure 2.2 : CCMP Encapsulation algorithm**

CCMP decrypts the payload of a cipher text MPDU and decapsulates plaintext MPDU using the following algorithm. Figure 2.3 shows CCMP decapsulation algorithm. The decapsulation process succeeds when the calculated Message Integrity Code (MIC) matches the MIC value obtained from decrypting the received encrypted MPDU. The original MPDU header is concatenated with the plaintext data resulting from the successful CCM recipient processing to create the plaintext MPDU.
2.1.5 Direct-sequence spread spectrum

Direct sequence spread spectrum, also known as direct sequence code division multiple access (DS-CDMA) is one of two approaches to spread spectrum modulation for digital signal transmission over the airwaves. In direct sequence spread spectrum, the stream of information to be transmitted is divided into small pieces, each of which is allocated across to a frequency channel across the spectrum. A data signal at the point of transmission is combined with a higher data-rate bit sequence (also known as a chipping code) that divides the data according to a spreading ratio. The redundant chipping code helps the signal resist interference and also enables the original data to be recovered if data bits are damaged during transmission (http://searchnetworking.techtarget.com/definition/direct-sequence-spreadspectrum).
Hopping spread spectrum, or frequency hopping code division multiple access (FH-CDMA), in which a broad slice of the bandwidth spectrum is divided into many possible broadcast frequencies. In general, frequency-hopping devices use less power and are cheaper, but the performance of DS-CDMA systems is usually better and more reliable.

Spread spectrum first was developed for use by the military because it uses wideband signals that are difficult to detect and that resist attempts at jamming.

**Feature’s of DSSS**

DSSS phase-modulates a sine wave pseudo randomly with a continuous string of pseudo noise (PN) code symbols called "chips", each of which has a much shorter duration than an information bit. That is, each information bit is modulated by a sequence of much faster chips. Therefore, the chip rate is much higher than the information signal bit rate. DSSS uses a signal structure in which the sequence of chips produced by the transmitter is already known by the receiver. The receiver can then use the same PN sequence to counteract the effect of the PN sequence on the received signal in order to reconstruct the information signal (http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum).

**Transmission method**

Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal. This noise signal is a pseudorandom sequence of 1 and −1 values, at a frequency much higher than that of the original signal.

The resulting signal resembles white noise, like an audio recording of "static". However, this noise-like signal can be used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence (because $1 \times 1 = 1$, and $-1 \times -1 = 1$). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted PN sequence with the PN sequence that the receiver believes the transmitter is using.

The resulting effect of enhancing signal to noise ratio on the channel is called *process gain*. This effect can be made larger by employing a longer PN sequence and more chips per bit, but physical devices used to generate the PN sequence impose practical limits on attainable processing gain.

If an undesired transmitter transmits on the same channel but with a different PN sequence (or no sequence at all), the de-spreading process results in no processing gain for that signal. This effect is the basis for the code division multiple access (CDMA) property of
DSSS, which allows multiple transmitters to share the same channel within the limits of the cross-correlation properties of their PN sequences.

As this description suggests, a plot of the transmitted waveform has a roughly bell-shaped envelope centered on the carrier frequency, just like a normal AM transmission, except that the added noise causes the distribution to be much wider than that of an AM transmission.

In contrast, frequency-hopping spread spectrum pseudo-randomly re-tunes the carrier, instead of adding pseudo-random noise to the data, the latter process resulting in a uniform frequency distribution whose width is determined by the output range of the pseudorandom number generator.

Benefits of DSSS

- Resistance to intended or unintended jamming.
- Sharing of a single channel among multiple users.
- Reduced signal/background-noise level hampers interception.
- Determination of relative timing between transmitter and receive.

Discussions

Mobile ad hoc networks are basically open networks for different types of attacks. The ultimate goals of the security like authentication, confidentiality, integrity, authentication, non-repudiation, anonymity and availability must be available to mobile users. To achieve these goals, the security solution protects the entire protocol stack. The fundamental idea is that each layer uses the services of the layer below, adds functionality, and provides a service to the layer alone. Famous layerwise security approaches are used in the proposed method to defend against denial of service attacks in MANET layers.

2.2 Routing Protocols for MANET

The design of routing protocols for use in mobile ad hoc networks is challenging and is still an open research area (http://en.wikipedia.org/wiki/Ad_Hoc_Routing_Protocol). The protocols that have served the wired Internet well do not translate to the MANET environment. In particular, the existing IP protocols were not designed to cope with the rapid changes in network topology that are possible with node mobility. Other factors, such as power management, should also be taken into account in a successful MANET routing protocol design. The protocols that are being considered for use in MANETs are varied in their approaches. Although other ways of categorizing them are certainly possible, one way to group these techniques is by their approach to route creation and maintenance. Some protocols take a
proactive approach, attempting to identify the best routes at any time between every pair of nodes in the network (Hsu et al., 2003). That way, the routes will be available if and when they are needed. Other protocols take the point of view that maintaining a route that is unused is wasteful. These methods discover and maintain routes only as needed. Of course, no categorization is perfect, so included a third, catch-all group. The protocols in this group may have proactive or on demand features or both, but they also have characteristics that set them apart from the first two categories (Chaba and Medishetti, 2005). Table 2.1 shows Classification of MANET routing protocols.

### Table 2.1: Classification of MANET routing protocols

<table>
<thead>
<tr>
<th>Algorithm Type</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive Routing</td>
<td>Destination Sequenced Distance Vector (DSDV)</td>
</tr>
<tr>
<td></td>
<td>Optimized Link State Routing (OLSR)</td>
</tr>
<tr>
<td>Reactive Routing</td>
<td>Dynamic Source Routing (DSR)</td>
</tr>
<tr>
<td></td>
<td>Ad hoc On-demand Distance Vector (AODV)</td>
</tr>
<tr>
<td></td>
<td>Temporally Ordered Routing Algorithm (TORA)</td>
</tr>
<tr>
<td>Other</td>
<td>Zone Routing Protocol (ZRP)</td>
</tr>
</tbody>
</table>

#### 2.2.1 Proactive protocols

The aim of a proactive routing protocol is to maintain up-to-date routes from every node to every other node in the network (Boukerche, 2004). For each destination, a node knows which of its neighbors is the next step, or hop, along the shortest path to that destination. Routing a packet requires only a simple table lookup, hence these protocols are also called table-driven. Changes in network topology are propagated throughout the network in updates in order to maintain a consistent view of the network.

Table-driven protocols can be categorized as either distance vector or link state. In distance vector algorithms each node maintains, for each destination, the distance to that destination from each of the node’s neighbors. The neighbor with the shortest entry in this vector of distances is chosen to be the next hop to the destination. Choosing next hops in this fashion results in the shortest path to any destination. A node derives the information in its distance vector via periodically broadcast updates from its neighbors. This method, the Distributed Bellman-Ford (DBF) algorithm, is computationally efficient and straightforward to
implement. However, the DBF algorithm is subject to both short-lived and long-lived routing loops because nodes choose their next hops in a distributed manner using information that may be out-of-date. Nevertheless, the simplicity of DBF has made it an attractive choice for implementation, the Routing Information Protocol (RIP) being a well-known example. In a link state algorithm, each node monitors the status of its link with each of its neighbors. This information is shared periodically with the other nodes in the network. Thus each node acquires a complete description of the network topology, and can apply a shortest-path algorithm to choose its next hop for each destination. Due to propagation delays, the link state information at a particular node may be temporarily out-of-date, possibly resulting in loop formation. Such loops are short-lived, however, disappearing as routing updates traverse the network. Link state algorithms are more complex computationally and require more memory than distance vector algorithms, but they are not subject to the formation of long-lived loops. The Open Shortest Path First (OSPF) routing protocol in the wired Internet is an example of a link state protocol.

**Destination Sequenced Distance Vector – DSDV**

The Destination Sequenced Distance Vector (DSDV) protocol is based on the distance vector algorithm. DSDV avoids the looping problem of a traditional distance vector method by associating a sequence number with each routing table entry. This sequence number, originally assigned and advertised by the destination node, is used to determine the relative freshness of routing information. Updates are broadcast periodically to maintain routing table consistency. For each routing table entry included in an update, a node increments the hop count (metric) by one since a node receiving the update will be one hop further from the destination. When a node receives an update, it will update the entries in its routing table for which the corresponding update entry has either a higher sequence number or the same sequence number but a lower metric. If a node does not receive three consecutive periodic updates from a neighbor, the link to this neighbor is considered to be broken.

Alternatively, the MAC layer may detect link breakage and report this to the routing agent. A node increments its own sequence number by two each time it broadcasts a routing update. By convention, these sequence numbers are even. If a node determines that the link to one of its neighbors is broken, it searches its routing table for routes that use the neighbor as the next hop. In any such entries, the metric is set to infinity and one is added to the sequence number. Odd sequence numbers, therefore, denote broken or invalid routes. The use of an odd number ensures that any newer update entry with a valid (not infinite) metric will have a greater sequence number. To reduce the potentially large volume of network traffic produced by routing updates, DSDV uses two different types of updates. Full updates are broadcast periodically and include every entry in the routing table. Smaller, incremental updates include only those routing
entries that have changed since the last full update. Incremental updates are triggered when significant changes are made to the routing table. For instance, a route invalidation is considered sufficiently important to trigger an update. Nodes keep track of the weighted average time that routes to a destination fluctuate before an update with the best metric is received. The broadcast of a routing update is delayed by the length of this settling time, which further reduces network traffic by eliminating the broadcast of sub-optimal routes. Still, DSDV has been shown to have very high routing overhead compared to on-demand routing protocols. While the number of routing packets transmitted per second will be smaller for DSDV, the large number of routing entries in each update packet accounts for the higher overhead (Etorbanpeter and Trinder, 2007)

**Optimized Link State Routing Protocol – OLSR**

The Optimized Link State Routing (OLSR) protocol is an extension of the pure link state algorithm, optimized for use in MANETs. In OLSR, routing overhead is reduced in two ways. First, the flooding of control traffic is minimized by restricting the set of nodes, called multipoint relays (MPR), which relay control packets through the network. Every node in the network selects a MPR set from among its neighbors in such a way that control packets retransmitted by these relay nodes reach all nodes in its 2-hop neighborhood. Second, the size of control packets is reduced because a node only includes link state information for the members of its MPR Selector set. This is the set of neighbors which have selected the node to be one of their multipoint relays. Generally speaking, the smaller the MPR sets are, the more optimal the protocol will be. The frequency of the periodic updates can be increased to optimize OSLR’s adaptability to changes in topology. Since only periodic updates are used, OLSR can accommodate high node mobility. The use of MPRs makes OLSR particularly well-suited for use in large, dense networks (Plesse et al., 2004).

**2.2.2 Reactive Routing Protocol**

In contrast to the methods in the previous section, on-demand protocols are not concerned with identifying and maintaining routes that are not currently in use (Chaudhry et al., 2005). In an effort to reduce routing overheads, these techniques have a reactive nature – “we will create no route before it’s time.” Although discovering routes only when needed results in higher packet latencies on average, many researchers believe that on-demand protocols inherently have lower overhead and higher throughput than proactive methods, and are hence superior (Pirzada et al., 2006).

**Dynamic Source Routing – DSR**

The Dynamic Source Routing (DSR) protocol uses source routing to deliver data packets (Johnson and Maltz, 1996). Routes are stored in a route cache, and each cache entry
contains the entire path to be traversed to the destination. When a data packet is originated, the source places the entire path in the packet header. The intermediate nodes along this path simply forward the packet to the next hop specified in the header. Avoiding routing loops is clearly trivial with the use of source routing. If a source does not have a route to the destination in its cache, it begins a route discovery process by broadcasting a route request (RREQ) packet. Each node receiving the RREQ searches its own route cache for a route to the requested destination. If no route is found, it adds its own address to the hop sequence contained in the RREQ header and broadcasts the RREQ again. A RREQ is tagged with an identification number that each node records so that it will not broadcast the request more than once. The RREQ propagates through the network until it reaches either the destination or an intermediate node which has a route to the destination in its route cache. The RREQ header contains a record of the hops taken from the source, so this route can be reversed and used to unicast a route reply (RREP) packet back to the source. In the case that bi-directional links cannot be assumed, the RREP is piggybacked on a new request for a route to the source.

If an intermediate node is unable to forward a data packet to the next hop in its source route, it unicasts a route error (RERR) packet back to the source informing it of the broken link. The source removes the broken link from its route cache and all routes containing this hop are truncated at the point of the broken link. Any intermediate node that forwards the RERR will learn of the broken link and remove it from its route cache as well. The source can then attempt to use another route to the destination if one exists in the route cache, or it can initiate a new route discovery. DSR uses source routing and route caching very aggressively. An intermediate node, upon finding the next hop link to be broken, can use an alternate route to the destination from its own route cache. A source receiving a RERR packet piggybacks the RERR on the following RREQ to help clean up the caches of other nodes which may have the failed link in a cached source route. Nodes are allowed to operate in promiscuous mode, examining the source route in the header of packets not addressed to it. If an intermediate node determines that a shorter route exists through itself, it sends this information back to the source in a RREP. In any case, the intermediate node can use snooping to learn of new source routes and add them to its cache. There is no mechanism in DSR by which a stale route can be expired, nor is DSR able to choose the freshest route when multiple choices are available in the cache. If stale routes are used, they may cause other caches to become polluted. The use of promiscuous listening coupled with node mobility can result in stale routes polluting caches faster than they can be deleted by route error packets (Chenna and Dr. Chandrasekhar, 2007).

**Ad hoc On-demand Distance Vector – AODV**

The Ad hoc On-demand Distance Vector (AODV) protocol is based upon the distance vector algorithm, and like DSDV, it uses sequence numbers to avoid the formation of long-lived
routing loops (Boomaranimalany et al., 2009). Unlike DSDV however, AODV only maintains routes that are in active use. If a source does not have a route to a packet’s intended destination, it buffers the data packet and broadcasts a RREQ in a manner similar to DSR. The source includes the most recent sequence number it has for the destination in the RREQ header. The RREQ is propagated through the network until it reaches the destination or a node with a fresh enough route to the destination, i.e. a route with a higher sequence number than the one in the RREQ. As the RREQ makes its way through the network, the intermediate nodes which forward the RREQ set up a reverse route to the source. This is the path along which the RREP from the destination (or other node with a fresh route) will be unicast back to the source. As the RREP is propagated, the intermediate nodes construct the forward path from the source to the destination. An important feature of AODV is its use of timers to expire routes which have not been used for some period of time.

This policy is intended to minimize the stale route problem to which DSR, for example, is subject. Each node maintains a list of predecessor nodes for each of its routing table entries. This is the set of neighbors which use the node as a next hop to the destination. When a next hop link breakage is detected by the MAC layer, the intermediate node which is unable to forward the data packet drops the packet and sends a RERR to each of its predecessor nodes. Each of these nodes in turn forward it to their predecessors, effectively erasing all routes which use the broken link. To reduce the number of RREQ broadcasts required for route discovery, AODV uses an expanding ring search in the hope that the destination may be nearby. The time-to-live (TTL) field in the IP packet header is used to limit the number of times the RREQ is re-broadcast. At first only the 1-hop neighbors will receive the RREQ. If the source does not receive a RREP from one of these neighbors within a certain amount of time, it broadcasts another RREQ. This time the RREQ will reach all the nodes that are two hops away. If a reply is still not received, the process continues until the TTL reaches some threshold. At that point the RREQ is simply flooded throughout the network. Another AODV optimization is local route repair. If an intermediate node which detects a route failure is more than half way from the source to the destination, it initiates a route discovery of its own rather than sending a RERR back to the source. Data packets are buffered during local route repair rather than being dropped (Du et al., 2003).

**Temporally Ordered Routing Algorithm – TORA**

The Temporally Ordered Routing Algorithm (TORA) is a link reversal protocol designed to operate in a highly dynamic mobile networking environment (http://wiki.uni.lu/secan-lab/Temporally-Ordered+Routing+Algorithm.html). Route discovery is source-initiated and multiple paths are provided to any destination. With the exception of short-lived loops, routes are guaranteed to be loop free. Control messages are localized to a very small number of nodes.
in the vicinity of a change in network topology. When a route is created, nodes use a “height” metric to establish a directed acyclic graph (DAG) rooted at the destination. Each link in the route is in either an upstream or a downstream direction depending on the relative height of its endpoints. If node mobility causes the DAG route to break, the height metric will change for some nodes and the direction of some links may be reversed. The height metric depends on the logical time of a link failure, so TORA assumes all nodes have synchronized clocks, perhaps by means of a Global Positioning System. TORA runs on top of the Internet MANET Encapsulation Protocol (IMEP), which is required to provide reliable, in-order to deliver control messages. TORA is susceptible to routing packet losses and has been shown to perform poorly when compared to DSR and AODV (Ohta et al., 2002).

2.2.3 Hybrid Routing Protocol

The ad hoc network can use the hybrid routing protocol that have the advantage of both proactive and reactive routing protocols to balance the delay and control overhead.

Zone Routing Protocol – ZRP

The Zone Routing Protocol (ZRP) is designed to be used in an ad hoc wireless network consisting of many fast-moving nodes dispersed over a large geographical area. Due to the high degree of node mobility and the potentially large number of destinations, neither a pure proactive or a pure on-demand method would be adequate (Giannoulis et al., 2005). The long delay and excessive control traffic during route discovery means an on-demand approach may not be applicable to real-time communication. On the other hand, proactive schemes are not appropriate because they use a lot of network capacity keeping routing information up-to-date. So, ZRP takes a hybrid approach, combining both types of routing. Each node belongs to a routing zone, which is the set of nodes whose minimum distance (in hops) from the node in question is no greater than a specified number, called the zone radius. Within the routing zone, routes are maintained proactively. Packets destined for a node outside the zone are first propagated to a node on the periphery of the zone, and from there to a peripheral node of the destination’s routing zone. Interzone routing is accomplished using an on-demand algorithm. The zone radius is a parameter that is used to adjust ZRP operation to network conditions. However, the zone radius must be chosen at the time the network is set up and cannot be changed. Hence, this decision may have a considerable impact on protocol performance.

Reactive protocols acquire routing information only when it is actually needed. They are considered to be the most suited one for ad hoc networks. AODV is the routing protocol mostly used in MANET and the same is taken for the research work.
AODV routing protocol fulfills the requirements of routing protocol in MANETs and it is efficient in terms of network performance. However, security aspects have not been considered in the protocol; attackers, therefore, can use many kinds of attacks via route discovery or path maintenance process such as advertising falsified route information, redirecting routes, launching denial-of-service attacks, sending falsified error reports (Kuosmanen, 2002).

2.2.4 Multipath Based AODV Routing protocols

Multi-path routing protocols with the following fundamental properties: (i) The routing protocol provides multiple, loop-free, and preferably node-disjoint paths to destinations, (ii) the multiple paths are used simultaneously for data transport and (iii) multiple routes need to be known at the source (Lee and Gerla, 2001). Multi-path routing protocols that have been proposed for Mobile Adhoc Networks and satisfy the above-mentioned requirements are:

SMR (Split Multi-path Routing)

SMR is based on DSR. This protocol attempts to discover maximally disjoint paths. The routes are discovered on demand in the same way as it is done with DSR. That is, the sender floods a Route REQuest (RREQ) message in the entire network. However, the main difference is that intermediate nodes do not reply even if they know a route to the destination. From the received RREQs, the destination then identifies multiple disjoint paths and sends a Route REPlay9 (RREP) packet back to the source for each individual route.

AOMDV (Ad hoc On demand Multi-path Distance Vector routing)

AOMDV extends AODV to provide multiple paths. In AOMDV each RREQ and respectively RREP defines an alternative path to the source or destination. Multiple paths are maintained in routing entries in each node. The routing entries contain a list of next-hops along with corresponding hop counts for each destination. To ensure loop-free paths AOMDV introduces the advertised hop count value at node $i$ for destination $d$. This value represents the maximum hop-count for destination $d$ available at node $i$. Consequently, alternate paths at node $i$ for destination $d$ are accepted only with lower hop count than the advertised hop count value. Node-disjointness is achieved by suppressing duplicate RREQ at intermediate nodes.

AODV Multipath (Ad hoc On-demand Distance Vector Multi-path)

AODV Multipath is an extension of the AODV protocol designed to discover multiple node-disjoint paths. Intermediate nodes forward RREQ packets towards the destination. Duplicate RREQ for the same source-destination pair are not discarded and recorded in the RREQ table. The destination accordingly replies to all route requests targeting at maximizing the number of calculated multiple paths. RREP packets are forwarded to the source via the
inverse route traversed by the RREQ. To ensure node-disjointness, when intermediate nodes overhear broadcasting of a RREP message from neighbor nodes, they delete the corresponding entry of the transmitting node from their RREQ table. In AODV Multipath, node-disjoint paths are established during the forwarding of the route reply messages towards the source, while in AOMDV node-disjointness is achieved at the route request procedure (Motegi and Horiuchi 2004).

Each of these multipath routing protocols broadcast data over all paths simultaneously. This technique has all the advantages previously mentioned, but it also introduces more packets into the MANET.

2.2.5 Scheduling algorithm for MANET

Scheduling algorithms decide which packet is served next among the packets in the queues (Kanodia et al., 2001). Scheduling algorithms are dependable for distributing resources among all users in the network, and provide them with a higher QoS. Users request different classes of service that may have different requirements (such as bandwidth and delay), so the main goal of any scheduling algorithm is to maximize the network utilization and achieve fairness among all users.

Strict Priority (SP)

In this algorithm, packets are represented by the scheduler depending on the QoS class and then they are assigned into different priority queues. These queues are served according to their priority from the highest to the lowest as shown in Figure 2.4, in which this mechanism may cause some priority QoS classes to be starved.

Figure 2.4. Strict Priority Scheduler
Round Robin (RR)

Figure 2.5 shows that the procedure of RR scheduler works in rounds by serving the first packet in each priority queue in sequence according to their precedence till all queues are served and then it restarts over to the second packet in each queue.

![Figure 2.5. Round Robin Scheduler](image)

Weighted Round Robin (WRR)

In WRR procedure, packets are categorized into different service classes and then assigned to a queue that can be assigned different percentage of bandwidth and served based on Round Robin order as shown in Figure 2.6. This algorithm addresses the problem of starvation by guarantees that all service classes have the ability to access at least some configured amount of network bandwidth.

![Figure 2.6. Weighted Round Robin Scheduler](image)
Diff-Serv (DS) Enabled

Diff-Serv uses the 6-bit Differentiated Services Code Point (DSCP) field in the header of IP packets that is used to classify packets, by replacing the outdated IP precedence with a 3-bit field in the Type of Service byte of the IP header originally used to classify and prioritize types of traffic.

2.3 Some of the well-published existing frameworks for securing MANETs

The following sections briefly describe some of the well-published frameworks for securing MANETs. These frameworks use encryption/authentication to secure the network.

Security Aware Ad-hoc Routing (SAR)

The Security Aware ad-hoc Routing protocol (SAR) is based on on-demand protocols, such as AODV and DSR (Yi et al., 2001). In SAR, a security metric is added into the route request packet and a different route discovery procedure is used. Relay nodes receive a route request packet with a particular security metric or trust level. At the relay node, if the security metric or trust level is satisfied, the node will process the route request packet and propagate it to its neighbors using controlled flooding. Otherwise, the route request is dropped. If an end-to-end path with the required security attributes can be found, the receiver will generate a route reply packet with the specific security metric. If the receiver node fails to find a route with the required security metric or trust level, it sends a notification to the sender and allows the sender to adjust the security level in order to find a route. SAR uses encryption to protect data but does not protect individual nodes from attack. It does not use multipath routing and defend against denial of service attacks.

Self-Organized Network-Layer Security (SCAN)

Self-Organized Network-Layer Security (SCAN) is a unified network layer prevention scheme that uses AODV routing (Yang et al., 2002). It takes a self-organized approach by exploiting a full localized design without assuming any a priori trust or secret association between nodes. Each node has a token in order to participate in the network operations and its local neighbors collaboratively monitor it to detect any misbehavior in routing or packet forwarding services. Upon expiration of the token, each node renews its token via its multiple neighbors. The period of the validity of a node’s token is dependent on how long it has behaved well in the network. A well-behaving node accumulates its credit and renews its token less frequently over time. SCAN protects the network by detecting and reacting to malicious nodes. It does not employ encryption to protect the data or the nodes. It also does not address node selfishness and security threats in the network’s physical and link layers. It does not use multipath routing and defend against denial of service attacks.
On-demand Secure Routing Protocol (OSRP)

The On-demand Secure Routing Protocol (OSRP) defines a reliability metric based on ast records and uses it to select a secure path in the MANET (Papadimitratos and Haas 2002). The reliability metric is represented by a list of link weights where high weights correspond to low reliability. Each node in the network maintains its own list, referred to as a weight list, and dynamically updates it when faults are detected. Faulty links are identified using a secure adaptive probing technique that is embedded in the normal packet stream. OSRP is designed to protect the MANET from byzantine failures by detecting a malicious link after log n faults have occurred, where n is the length of the path. It uses both encryption and behavior grading, but is not effective against many behavior based attacks nor against DoS attacks. It does not use multipath routing and defend against denial of service attacks.

MOBILE Certification Authority (MOCA)

The framework MOBILE Certification Authority (MOCA) employs threshold cryptography (distributing information among a cluster of cooperating computers) to distribute the Certificate Authority (CA) functionality over specially selected nodes based on the security and the physical characteristics of nodes (Yi and Kravet, 2003). The selected nodes that collectively provide PKI functionality is called MOCAs. MOCA is a key distribution framework and does not incorporate multipath routing and layerwise security. The encryption scheme employed is designed to protect data and authenticate users, but not to protect the nodes themselves. It does not defend against denial of service attacks.

Secure Efficient Ad-hoc Distance Vector. Secure Efficient Ad-hoc Distance Vector (SEAD)

The framework SEAD uses efficient one-way hash functions to encrypt data and does not use symmetric cryptographic operations in the protocol in order to support the nodes of limited processing capabilities. The authors believe nodes in an ad-hoc network are unable to verify asymmetric signatures quick enough for routing protocols to decide on the routing path. Therefore, it is subject to numerous attacks common in MANETs. It does not use multipath routing (Hu et al., 2003).

Alliance of Remote Instructional Authoring and Distributed Networks for Europe (ARIADNE)

Alliance of Remote Instructional Authoring and Distributed Networks for Europe (ARIADNE) (Hu et al., 2005) prevent attackers from tampering uncompromised routes consisting of uncompromised nodes. It is based on the DSR protocol and relies on symmetric cryptography only. It operates in three stages. The first stage shows a method that enables the target to verify the authenticity of the route request. The second stage presents a key
management protocol that relies on digital signatures, and standard message authentication
code for authenticating data in route requests and route replies. The third stage presents an
efficient per-hop hashing technique to verify that no node is missing from the node list in the
route request. ARIADNE uses encryption to authenticate nodes and protect data, but it is not
used to protect nodes from direct attacks. It does not use multipath routing and defend against
denial of service attacks.
Table 2.2. Comparison of some of the well-published frameworks with proposed framework for securing MANETs

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>Encryption</td>
<td>Multipath</td>
<td>Based on Reactive protocol</td>
<td>Neighbor Authentication</td>
<td>Certification Service</td>
<td>Attack Defense</td>
<td>Denial of Service attacks</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
2.4 Conclusion

Layerwise Security is a significant requirement in emerging applications of Mobile Ad-hoc environments like military or public emergency network applications. Security approaches play a vital role in secure communication. The summary of different Layerwise security approaches are presented briefly. As the nodes are dynamic in nature, ensuring effective routing is one of the major challenges for MANET. Some of the well known routing protocols are discussed. The previous enhancement of multipath routing protocol is also discussed. The need for scheduling algorithm for MANET responsible for distributing resources among all users in the network for MANET is presented. These directions paved the way to propose a novel methodology for efficient secure communication in MANET.