CHAPTER 2

BACKGROUND AND PRELIMINARIES

Present networks are the basis of recent communication. The existence of networks is inspiring our society in innumerable different ways. Now days, wireless mesh network is measured as a promising technology for posturing the self-organizing, healing and configurable characteristics however one of the primary challenges in the venture of these networks is their vulnerability to security attacks. In order to conquer these threats, several security techniques are proposed, however, authentication is considered as a vital parameter to offer a secure communication. In this chapter, a review is conferred from beginning to the recent networking technology i.e. WMN. In addition, WMN security is explored with modern applications such as intelligent transportation system, smart grids and multimedia systems etc. Further an obvious outline of security with respect to each layer is explicated and finally the chapter is bankrupt by exactness of the future work which is the next step of this research.

2.1 INTRODUCTION

The revolt of devices in 1990, now enduring in the 21st century comprises “computer networks” that is a combination of devices/computers which allows a computer to converse the data or distribution of hardware and information [11]. Today, networks are the backbone aid for current correspondence whose presence is enriching our social order in endless separate approaches. Concerning illustration, the associations or organizations depend intensely on the capacity to allotment data in an effective and profitable manner. As the societies heavily depend on the ability to stake their information in a productive and efficient manner [12], Computer networks are now becoming the part of each and every organization firm in which computers can pursue a pathway anyhow. When it comes to locate up the classification of the network, an organization has two selections; wired network and wireless network (as depicted in Figure 2.1).

2.1.1 Types of Network

*Wired networking* is the widespread type of Local Area Network (LAN) technology [13] where the acquaintances among the technologies are made using a cable or physical wire. It is
simply a gathering of two or more devices connected through an Ethernet cables. To fix a computer or to the network, an Ethernet adapter is required, which attach the devices either externally or internally. The wired networks are further isolated under two parts; point to point and Multipoint.

**Figure 2.1 Network Classification**

Point-to-point networks utilizes a real length of link to interface two closures of devices and gives a devoted connection between these devices [14] where the whole limit of the connection is held just between the two devices as depicted in Figure 2.2 (a). Multipoint system is one in which more than two devices share a solitary connection as appeared in Figure 2.2 (b). There are essentially three system topologies in multipoint organizing. Star Network is the naive part of system which has at least two PCs associated with one focal center point [15] and this sort of system is to be utilized for private venture and home systems. Figure 2.2 (c) demonstrates the chart of star systems administration [16]. The benefits of a star system is that it is easy to handle but difficult to wire, introduce and keep up notwithstanding, from another side, it requires more link length and is more costly than transport topology. The star systems administration is valuable when some handling must be brought together. Bus networks (as appeared in Figure 2.2 (d)) are utilized for impermanent systems, simple expansion and execution. The disadvantages of these networks are that it is constrained to a link length and a simple blame in the link can bring about the decimation of the entire system. This kind of systems is basically utilized for modern applications. Ring Network is to some degree like bus network since it has no focal host PC. Every PC on this system has two neighboring hubs having their own particular applications freely. It is as a shut circle where every hub can transmit the information by devouring the token as presented in Figure 2.2 (e).
Figure 2.2 Point-to-point and Multipoint Network

Broadcasting of information is speedy in ring system, yet as the information parcels must go through each PC between each source and goal, information turns out to be moderate and disappointment of any hub can bring about the unsuccessful information transmission. As all these wired systems are settled and experience with specific downsides, for example, they are non-compact, static in nature, penetrate the openings into the dividers, handoff is least and requires the cost of fiber+ copper +co-hub link [17], the wireless systems administration innovation appeared. Further, the moving of wired systems causes the entire rewiring which consolidates the significant disadvantage in wired innovation. Peter Gold around 20 years back presented the idea of wired city i.e. the interconnection of phones in the workplaces and between the workplaces, faxes, and so forth. A wireless system is the one which utilizes high recurrence radio flags rather than wires to impart between hubs [18]. The single hop and multi-hop are the two noteworthy sorts of remote systems.

Single hop is a solitary association between the devices. Infrastructure less and framework based are further expansions of single hop systems administration. Infrastructure less has no settled structure between the hubs as in Bluetooth while Framework or infrastructure based has settled structure like in cell systems. Multi-hop is another sort where at least two jumps
exist between each source and goal. Multi-hop is additionally classified into framework based and less infrastructure. Cases of foundation based are remote sensor systems and remote work systems and at any rate the case of framework less is Vehicular Area Networks (VANETS). The cost of systems administration is proceeding to decrease and has turned into a fundamental part in finishing day by day business undertakings [19]. Progression in system innovation has considered associations to utilize the system to share assets, as well as to store extensive pool of information for investigation. In this manner, securing such information and assets of association on system is an incredible concern. As no PC system is totally secure.

2.2 SECURITY

Security is generally characterized as the condition of being free from risk or danger [20]. The biggest PC related crime in US history was conferred by Kevin Mitrick which cost of 80 million dollars in US licensed innovation [21]. The fundamental comprehension about the security methods is vital for the exploration being done today. A web is subjected to assault/attack from pernicious sources and these assaults can be separated into two classifications: passive assault and active assault [22].

Active assaults are additionally arranged into specific levels, for example, 1) masquerade where one element puts on a show to be an alternate substance. 2) A replay assault happens if the last catches the message from the sender and gets the inactive/replay message. 3) Modification of messages, the adjusting and reordering is finished by making an unapproved impact and 4) DOS assault where an aggressor may stifle all messages sent to the beneficiary [23]. Today, network services (i.e. Email, www and so on.) have turned into a fundamental need in everyday correspondence [24]. For giving the benefits to these systems more adequately, WMN has soured into a famous topology which assembles elite framework. To supply a last mile broadband access, WMN is a promising innovation. It is a most conspicuous development of system engendering. Let’s have a short portrayal on WMN, architecture, favorable position and its applications.

2.3 HISTORY OF WIRELESS MESH NETWORKS

2.3.1 Wireless Mesh Network

WMN is an augmentation of multi-hop Ad-hoc system and it is a mix of Ad-hoc and Mesh organizing. Ad-hoc system is one where every device can specifically speak with whatever
other device inside its radio reaches while in mesh networks; every hub goes about as a switch and has the ability to retransmit the parcel to goal hub [25, 26].

![Diagram of Wireless Mesh Network](image-url)

**Figure 2.3 WMN Technology**

Figure 2.3 demonstrates the extent of Wireless Mesh Network Technology. Like system classification, on the premise of availability, WMN is characterized into three gatherings i) Point to Point, ii) Point to Multipoint and iii) Multipoint-to-Multipoint. Point to Point systems are reliable; however their versatility and adaptability level is down. Multipoint-to-Multipoint networks have direct versatility; however have the low unwavering quality and flexibility. So as to surmount the above confinements, Multipoint-to-Multipoint systems are spearheaded which supply with high unwavering quality, versatility and flexibility [27]. The transmitting energy of every hub is downsized as the quantity of clients in the work increments.

<table>
<thead>
<tr>
<th>WMN</th>
<th>Reliability</th>
<th>Adaptability</th>
<th>Scalability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point to Point</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Point to Multipoint</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
</tr>
<tr>
<td>Multipoint to Multipoint</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

To expand the scope without need of transmitting force, Multipoint-to-Multipoint network utilizes the multi-hop characteristic. The IEEE 802.11 family principles are utilized by Multipoint-to-Multipoint systems [28]. The systems which use these guidelines are called mesh networks and WMN are a specific class of Multipoint-to-Multipoint organizes. Table 2.1 demonstrates the parametric contrast between Point to Point, Point to Multi-indicate and Multipoint systems.

**2.3.2 WMN Architecture**
The architecture of WMN is ordered into three fundamental gatherings i) Infrastructure/spine WMN ii) Client WMN and iii) Hybrid WMN.
**Infrastructure/backbone WMN** produced by mesh routers for clients to narrate them. Various cases of radio technologies are engaged to make the backbone WMN. IEEE 802.11 is the most extensively used technology, however in case of different radio technologies; clients must converse with base station.

*Figure 2.4 Infrastructure WMN*

Backbone WMN is the most frequently used wireless network as all the networks of neighborhood can be built using infrastructure meshing. In this, mesh networks are put on the upper side to serve as the access points for clients. The routers generally utilized two sorts of radios i.e. for backbone correspondence and for client correspondence. Figure 2.4 demonstrates the infrastructure WMN. Client WMN blesses with peer to peer systems among the devices. In this, client nodes encompass routing as well as giving an end user application to client’s from a individual type of getting set on devices [29]. Client WMN architecture is appeared in Figure 2.5. Hybrid WMN is a combination of two i.e., infrastructure and client WMN. The network can be retrieved by mesh client either through a router or direct meshing with mesh client only. In this, the infrastructure WMN provides association to other network and clients routing competence delivers improved connectivity and reporting [30]. Figure 2.6 indicates hybrid WMN. The discussed architecture of WMN comprises of different types of nodes, for example, WMN router, WMN client and WMN gateway. WMN client is the end client user that gets the system for utilizing the email, VoIP, gaming and area discovery applications. The end client devices can be tablets, PDA's, advanced cells, and so forth.

The WMN clients have confined power and steering capacity [31, 32]. It might possibly be associated with the system as its versatile nature. WMN Router is utilized to course the activity of systems. The WMN routers are dependable and have a negligible utilization of transmission power. To empower the versatility in multi-hop mesh condition, various channels and numerous interfaces are used at the MAC in the chain of mesh routers.
**WMN Gateways** have the direct access to the internet. These are expensive in nature as they have multiple interfaces to connect to wired/wireless networks.

![Figure 2.5 Client WMN](image)

### 2.3.3 Benefits of WMN

WMN are more affordable than customary systems and eradicates the establishment cost of cables and fibers. For a larger scope region, WMN is predominantly utilized [33]. WMN is expendable, adaptable and can be included or taken away based less or more coverage region. WMN is utilized where network setups are blocked and has the low line of sight [34]. WMN supports high requesting indoor and open air availability and perfect to convey high throughput and solid networks. A self-organized and configured characteristic of WMN reduces the maintenance cost and setup time by enhancing the network performance. [35].

### 2.3.4 Applications of WMN

![Figure 2.6 Hybrid WMN](image)
Peer to Peer mesh topology helps to overwhelm the various placement challenges such as installation of Ethernet cable, deployment models, etc. In case of network failure, the mesh topology results top quick reconfiguration. Mesh routers can be located anywhere as they are attached with freedom of mobility. These characteristics of WMN draw the community to practice it in a diversity of applications. Some of them are given as below.

**a) WMN in Smart Grids**

To improve the electrical infrastructure or to augment the power savings, smart power system is becoming a naive global commercial initiative. A smart power system is essentially a streamlined electric grid, which proposes effective and authentic distribution of energy by using communication techniques and digital information. The system was brought out to diminish the costly environmental influences and to confirm energy efficiency. Figure 2.7 depicts the key ideas of smart grids.

![Figure 2.7 Smart Grid Concepts](image)

**b) WMN in real time traffic information systems**

A probe method is a technique which gathers continuous movement information. To transmit the data information to the TMC (Traffic Management Center), a possible and cost effective remote correspondence is required. WMN is an architecture which is independent from some other wired/remote system and needs low correspondence cost. A WMN based activity framework comprises of two parts i) Probe vehicle during roving on roads consequently assembles the continuous traffic data and transmit to TMC over WMN. Probe vehicle is furnished with Data Collection Unit (DCU) and vehicular remote terminals. ii) WMN comprises of mesh routers and mesh clients. In this, mesh clients are our probe vehicles. WMN is framed powerfully by probe vehicle through remote associations. Data gathered on the vehicles compasses to the closest mesh routers that afterwards communicate with TMC.

**c) WMN in Motorola**

Mesh networking offers a consistent portability in changing remote information correspondence for subjects and gives financial and wellbeing benefits. Motorola has built up
a MEA (Mesh Enabled Architecture) that empowers practical and versatile network. The resonant out of mesh networking is basically performed in two modes i) framework based-it is honed to make wide or metro region systems and ii) Client networks that empowers the remote networks. The solitary element of work design in Motorola is that connections and courses are naturally framed between clients. Motorola has propelled different cross sections empowered arrangements that are Moto mesh (consolidates authorized and unlicensed radio in a solitary get to point) and mesh track that enables a faster and accurate user location.

**d) WMN in Streaming Multimedia**

Multipath existence between any pair of source and goal is one of the unparalleled characteristics of WMN. A video record may have different imitations, if reserving is incorporated at hubs in WMN, subsequently, if another customer ask for a video document, it might get that document from numerous sources. At whatever point different customers are keen in different video documents, then enlightening a numerous multicast tree may not be the best decision. Rather than organizing a different multicast tree, existing multipath normal for WMN is more productive. To build up a shared spilling framework and to discover the best video source area, let us assume that each WMN hub has pretty much memory space to spare nearby duplicates and disseminate these duplicates to peering WMN hubs. The association status is occasionally ordered by the media server. The server gathers the document area data and jellies them in a DMT.

**e) WMN in Cloud Computing**

Distributed computing is measured as an on-request fifth utility application. The design of portable distributed computing (MCC) is commonly erect upon intrigue driven mists, which enables the use of cloud administrations to versatile clients. Customarily MCC access experiences high cost and WAN execution issues. To rule over these issues, a scaled down cloud idea has developed, known as cloudlets. A cloudlet is a neighborhood server farm having the upside of self-overseeing; speedier access control, diminished cost in utilization and arrangement. By mixing a cloudlet with a remote availability i.e. WMN, nearby business can offer superior cloud administrations to bunch MCC clients. A WMN is a mix of two hubs, i.e. mesh client and mesh router which has the capacity to build up work availability among them. In light of self-mending, versatility and sorting out components, WMN can embrace to topology amid portability and blunder recuperation. Because of portability administration strategies, a mesh cloud design is being utilized which adequately underpins transmission between system switches and doors and possibly bolsters high data transfer capacity cloud
administrations, low reaction time, unwavering quality so along. The reconciliation of WMN and the mesh cloud system offers self-sorting out, self-administration and adaptable access to cloud administrations.

As WMN is a crisp worldview of remote systems administration, it offers a quick, modest and simple arrangement of systems. Today, every association is utilizing this innovation, in this way; it is the obligation of WMN to give administrations to clients in a secured and powerful way. One of the essential difficulties of conveying these systems is a security matter.

2.4 SECURITY ISSUES IN WIRELESS MESH NETWORK

2.4.1 Security Issues in Smart Grid
The most obligatory enabling mechanisms of the smart grid is the communication; merely in this there exist abundant scalability and defense matters. Security is one of the most acute concerns in smart grids that generally arise during the pre-serration of integrity and confidentiality of smart metering data in AMI.

2.4.2 Security issue in Intelligent Transportation System (ITS)
The primary objective of ITS is to provide a public safety by eliminating the accidents due to human mistakes. ITS innovation has been relentlessly presented in autos, yet security is one of the real worries in ITS. There exist two noteworthy security dangers i) ITS security risk, that is a string where hammers make rises around the vehicles to disturb the getting and transmission execution and ii) Wireless correspondence danger such as DOS, where system can be made inaccessible by flooding the false messages that take up all the usable data transmission. Therefore, digital security ought to be done on accessibility, confirmation and secrecy.

2.4.3 Security Issues in Multimedia
A similar security issues come up in mixed media i.e. integrity, confidentiality, non-repudiation, authentication, accountability, availability and encryption process are one of the real security dangers.

2.4.4 Security Issues in Cloud Computing
As cloud computing offers a cutting edge business for frameworks in light of strong, adaptable, effective and versatility exercises, overseeing bodies are still moderate in letting it
be known. A few issues and difficulties are aligned with it. Security is one of the significant
difficulties which harpers the development of cloud. Security issues in cloud computing are i) information misfortune where programmer may see your significant information or might erase the objective information.

Table 2.2: Security concerns in various applications

<table>
<thead>
<tr>
<th>Applications</th>
<th>Security issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Grids</td>
<td>Confidentiality, Authentication, Integrity.</td>
</tr>
<tr>
<td>ITS</td>
<td>Authentication, Availability, Confidentiality</td>
</tr>
<tr>
<td>Multi Media</td>
<td>Integrity, Confidentiality, Authentication, Encryption process, Availability, Non-repudiation,</td>
</tr>
<tr>
<td>Cloud Computing</td>
<td>DOS, Data loss, Confidentiality, Integrity, Accountability, Availability</td>
</tr>
</tbody>
</table>

An information misfortune may happen when proprietor of information misfortunes the key. ii) Account captured where if your record is seized by an assailant, then it might utilize the energy of your notoriety. An assailant having the control over record can listen in the exchange, control data, false harm reaction and soalong.iii) DOS-this assault is gotten in surge hour movement, where clients will be placarded by the aggressor's cloud benefit and there is no space to go to the goal with the exception of sit and anticipate. Thus, the integrity, confidentiality, accountability and accessibility are significant security assaults in distributed computing. Table 2.2 demonstrates the security issues in various utilizations of WMN. Open System Interconnection model (OSI Model) established by ISO describes a networking framework to device the protocols in seven layers. The OSI model assistances to breakdown the networking purpose into seven layers [36]. The OSI seven layer model trails in order when computer grasses data while it imitates to its reverse order when info enters into the data processor. The diagram of OSI model is shown in Figure 2.8. The detailed description of all seven layers is discussed below.

2.5 SECURITY ISSUES AND TRENDS IN OSI MODEL

2.5.1 Physical Layer

(a) Responsibility

It is accountable for carrier frequency generation, frequency selection, modulation, data encoding and signal detection. Existing wireless radios are capable to provision multiple
broadcast rates by combination of divers encoding and modulation rates. In society to surge the ability of wireless nets, numerous high speed physical skills have been designed i.e. Orthogonal frequency-division multiplexing (OFDM), Ultra Wide Band (UWB) [37]. To further surge the capacity, multiple antenna system has been castoff for wireless communication like smart antenna technology and antenna diversity, however due to high cost and complexity, fully adaptive smart antenna systems are castoff only in the base stations of cellular networks. In multiple antennas Multiple Input Multiple Output (MIMO) system are practical.

(b) Attacks possible at Physical Layer
The physical layer is in charge of flag identification, tweak and encryption of data. As WMN conveys through radio based medium, the most effective assault at this layer is jamming assault. Jamming assault blocks the radio frequencies that disjoin the whole system correspondence [38]. On the off chance that assaulting gadgets don't obey MAC layer convention and become difficult to recognize them. The point of jamming assault is to
interfere in radio frequencies which are utilized amid the correspondence in WMN. It might happen in three diverse ways i) jamming source: which disturbs the whole web. ii) Less capable jamming source: in this enemy conceivably upsets the system by going around the jamming source. iii) Intermittent jamming source: it demonstrates horrible as some correspondence in WMN might be time delicate.

(c) Mechanisms Against various Attacks on Physical Layer in WMN
The jamming attack can be encouraged by engaging different spread spectrum technologies: In Frequency hopping spread spectrum, a virtual random sequence is exploited which is known to both recipient and transmitter. By rapidly substituting a carrier signal, signals are troupe among many frequency networks. Thus, it is uncontrollable for an intruder to predict the, sequence and frequency selection and to jam it [39].

Direct sequence spread range exploiting a spreading code, each piece of sole flag is labeled by numerous bits. Spread code spread the flag finished a wide recurrence band, to slow the odds of intrusive from some other tuner.

(d) Physical layer open research issue
The research issue comprises improving the broadcast rate and public performance of physical layer technology over enhancement of the role of multiple antennas. MAC layer protocols essential to be deliberate carefully to top use the advance feature delivered by the physical layer.

2.5.2 Data link layer

(a) Responsibility
It secures the underlying association setup by isolating the data into information outlines. Data Link Layer (DLL) handles the acknowledgment from a beneficiary that the information made it effectively. DLL isolates the information parcels into casings. Data bundles are encoded and decoded into bits. It gives error handling, stream control and edge synchronization. The DLL is separated into two layers; i) MAC layer ii) Logical Link Control (LLC) layer. The MAC layer controls how a PC accesses the information while the undertaking of the LLC is to control the synchronization of edges.

(b) Attacks Possible at DLL
Jamming, MAC addressing, eavesdropping, spoofing and replays, are some probable attacks on link layer of WMN.
Jamming attack on link layer is additional hard to detect in contrast with the physical layer. In this, an intruder regularly conveys a MAC header on the channel so that, trusted nodes after the channel are demanding may lead to denial of service attack.

In Eavesdropping, due to the distribution nature, wireless systems may dispose to to passive eavesdropping attack within the range of message nodes. Passive eavesdropping does not instantly bear upon the functionality of the network; however conciliate confidentiality and data integrity.

Replay attack, is also known as man-in-middle attack. Replay attack can be hurled by external clients or internal clients. If an attack is ended by external nodes, then to influence the access over network resources, an intruder will convey the messages later, whereas an attack completed by internal nodes, the attacker may retain copies of all data to gain sanctioned contact of resources [40].

(c) Security Mechanisms at Link Layer
To protect against frame collision attacks, numerous error-congestion codes were castoff and to deliver the protection in contradiction of passive eavesdropping, message confidentiality service is used [41].

Depending on permutation vector generation, Omari et al. have proposed a Synchronous Dynamic Encryption System (SDES). The SDES is vigorous against key cooperation ii) biased bytes analysis and integrity violation. In this, the security is confirmed using two types i) secret session key (SSK) and ii) secret authentication key (SAK). Deng et al. have proposed a threshold identity based authentication scheme where key generation phase is answerable for allocating the Pu/PR or master key for each client and authentication is appreciated by identity based mechanism. Another author projected a wireless intrusion detection mechanism in which a system entails of a number of devices which are situated near an access spot.

(d) MAC layer research issues
As scalability of WMN can be talked by the MAC layer in 2 ways i) upgrading the current MAC conventions or proposes an another MAC convention to expand near end throughput and ii) allow transmission of numerous depressions in each client for instance Carrier Sense Multiple Access/impact shirking (CSMA/CA).

Hence, current open issues in the MAC are employed on most of the existing MAC protocols founded on CSMA/CA solve partial problems of general issue, however raise different problems, i.e. how to basically improve the scalability in multi-hop ad-hoc network.
2.5.3 Network Layer:

(a) Responsibility

Switching and routing information is delivered by the network layer. This layer varieties a virtual circuit to convey the data from one node to another node. The persistence this layer is internetworking, addressing, congestion control and error handling.

(b) Attacks at network layer

Information and control packets are two cases of threats on the network layer. These efforts are either passive or dynamic [42] in nature. Control packet attack goals the router functionality where the intruder’s objective is to access to the route available. Data packet attack goals the data forwarding functionality where attacker’s aim is to source the DOS by injecting malevolent data into the mesh. We initially deliberate the control packet attacks, and then spot data packet attacks.

**Control packet attack**, targets on claim routing is rushing attack. In rushing attack, a route is demanded from the root node to destination node by flooding the RREQ (Route REQuest) data with sequence numbers. A delay is ended between the receiving of the RREQ messages by a precise node and advancing the nodes to next node. Attacker promotes a malevolent node among source and destination [43]. The determined of malevolent node is to onward the RREQ message to target node earlier any intermediate node. Thus, route among source and destination comprises the malicious client that leaves out the packet flow subsequent DOS attack [44].

In Wormhole attack, the impartial is same as rushing attack, however, it can be proficient by applying diverse schemes. If more than one malevolent node launches a tunnel among source and destination, the RREQ messages are promoted between malevolent nodes [45]. As between each origin and destination malevolent nodes are comprised, it’s up to the malevolent node either to terminate the entire parcel or some discerning packets that are poignant among source and goal.

In Black hole attack, as malevolent node always retorts for positive RREQ, then approximately all the nodes dealings within a province of malevolent node is intended towards the malevolent node. The result origins a DOS attack. **The Gray hole attack** is a deviation of black hole approach. The sinking of whole packets may chief to easy revealing of malevolent nodes. So, attacker presented another attack, i.e. gray hole attack that may live hidden for longer duration of time by falling selected packets [46]. **Data Packet attacks** are chiefly launched by self-centered node. The most susceptible attack in this is inert
eavesdropping where the nodes are reliant on each other to onward the data. The selfish nodes may not achieve data promoting functionality. Selfish nodes either drop the discerning packets or entire packets. The malevolent node may familiarize trash packets to surge the packet or the bandwidth process time of the network.

In **Multicast Routing Attacks**, the intruder’s aim is to intrude network communication by scrutinizing the traffic or leading to packet dropping.

(e) **Security mechanisms at Network Layer**

Authenticated Routing for Ad-hoc networks (ARAN) is an on demand routing protocol that is engaged to offer an authenticated setup, route discovery and path maintenance. It provisions the security by cryptographic certificates [47].

Handle: The public key of the reliable certificate server is exploited where the key is recognized to all. Each node accepts a certificate supplied by the server whenever a node seams the network, the certificate conveys the IP address of node, creation timestamp of certificate, public key node and expire time of the certificate. During the route discovery process, signed route discovery packet (RDP) is directed by a node which grips the IP address of the destination node, time stamp, source node certificate and a nonce. The node in the route discovery authenticates signature of preceding node and eliminates the certificate of previous node after recognizing the IP address of it. The client ciphers the context of the data, adds its own certificate signed by its individual key and conveys it to the promoting node. A route reply packet (REP) is produced by destination node and unicast the packet beside the same route. The REP comprises the source IP address, nouns, certificate, identifier of packet character and timestamp. As REP spreads to the source node, it confirms the nuance and signature of the destination node. Whenever an attacker familiarizes a malicious, an error is created because certificate of that node miscarries to found the genuineness.

**Drawbacks**: If the intruder injects a large bit of spurious control packets, then a node may not be capable to confirm the force and signature a node to discard some control packets.

**Security-aware ad-hoc routing protocol (SAR)** is dissimilar the traditional routing protocol that feats location metrics and hop count for setting the routing path, SAR routines trust values and relationships metrics amongst the nodes. A client is talented to forward the RREQ to next node only if it accepts the obligatory authorization or trust level. A shared secret apparatus or a key distribution mechanism is realistic to regulate the trust levels amongst the guests. Trust levels will not work at different security levels [48].
**Drawbacks:** To offer the security at dissimilar floors, a protocol wants different keys. As the number of keys surges at each level, its conservation and stored computational overhead also rises.

**Secure Routing Protocol (SRP)** involves a security association (SA) survival between source and destination pair. SA launches a shared secret key amongst two nodes. Query sequence number (QSEQ) (castoff by destination to check legitimacy of RREQ) and a random key identifier (QID) (to recognize specific request) are conveyed by the basis node. The source node’s RREQ message is endangered by MAC which is calculated using shared key amongst source and destination. Each node onwards the received RREQ message, by accumulating the identifier. The ranking of a query is preserved by all nodes. The rate produced queries have the highest precedence. At the destination node, after checking the cogency of a query, destination node proves the authenticity and integrity of data and produces the RREP route responses using diverse paths. The authenticity and integrity of RREP are patterned by the same process as RREQ [49].

**Drawback:** The modification of unlicensed routes by malevolent clients cannot be prohibited by SRP.

Secure Link State Routing Protocol (SLSP) process is split into three parts; i) public key distribution and management (PKD) ii) Neighbor discovery and iii) link state updates. PKD is castoff to convey the public key certificates with zone while the NLP (Neighbor Lookup Protocol) is exploited to allocate the link state information [50]. The signed HELLO message (containing the sender MAC address and IP address) is castoff by NLP. The task of NLP is to generate a communication notification to SLP about wary observations. Wry explanations are those where a node privileges the MAC address of the existing node or the same MAC address is castoff by two diverse IP addresses. The introducing nodes’ IP addresses are illustrious by link state apprises (LSU).Whenever a client accepts an LSU, it validates its signature by a public key. The ranking priority of each neighborhood node is preserved by all node; nodes with lower rates of LSU have the uppermost precedence. Whenever a malevolent node deluges spurious control message in the mesh, due to cohort of high rate traffic, the node will be accredited to lower precedence and will never be comprised in the itinerary.

**Drawback:** it has higher computational overhead as there is a usage of asymmetric key cryptography.
(d) **Network Layer Open Issues**

Routing protocols for WMN are diverse from those in wired network and the cellular net. Despite the convenience of numerous routing protocols for ad-hoc networks, enterprise of routing protocols for WMN is still an active research area for numerous reasons: network performance metrics essential to be recognized and castoff to better the operation of routing protocols. Scalability is the most critical question in WMN.

### 2.5.4 Transport Layer

(a) **Responsibility**

As data packets portable in the form of segments, the transport layer is accountable for end to end connectivity amongst source and goal. Transport Control Protocol (TCP) and User Datagram Protocol (UDP) are the two chief protocols for transport layer. Reliable data transport and real time delivery are two suitcases of protocols. Reliable data transport is an ad-hoc transport protocols can be detached into two types: i) TCP variants ii) new transport protocols. An improved version of TCP supported networks is TCP variants. TCP acknowledge and TCP data revenue diverse paths in WMN which involvements latency, diverse packet loss and bandwidth while in ATP broadcast are rate founded which attains better recital. Real time delivery is usually to offer end to end delivery TCP are castoff instead of UDP. Additional protocols, i.e. Real Time Transport Protocol (RTCP) and Real time protocol (RTP) are castoff for congestion control.

(b) **Possible attacks in transport layer**

Synchronization (SYN) flooding attack, session hijacking attacks and de-synchronization attack are some probable attacks at the transfer layer. SYN flooding attacks are informal to launch at TCP, until resources essential by each connection are fatigued, an attacker may recurrently make new joining request. SYN Flooding Attack is a three way handshaking apparatus is practical to quality the session amongst two pairs of nodes as indicated in Figure 2.9.

![Figure 2.9 SYN Attack](image)

1. SYN, Sequence no. X
2. SYN/ACK, Sequence no. Y, ACK no. X+1
3. ACK, ACK no. Y+1
Let’s accept if node A desires to create a communiqué with node B then node A directs SYN packet beside with a sequence number another node B. Node B refers SYN sequence, ACK sequence number lastly node A finalizes the handshake procedure by distribution ACK with ACK bit. Straight off, the intruder by distribution too many SYN envelopes to node B may achievement and takeoff the return SYN protocol. In Security Hijacking, the security devices are accessible only at established time, however not at the on-going session. Thus, the intruder may accomplish the IP destination of a prey node and a form created sequence number and expected of victim node and then performs a DOS attack on victim node. Sequence number of victim node. In de-synchronization attack, the disturbance of an existing linking refers to a de-synchronization attack. De-synchronization attack indications to a TCP Acknowledgement (ACK) storm tricky. In this, the intruder inserts false messages by initiation a session hijacking in an enduring session amongst two clients. ACK of the interactive pair obtains this false message and refers an ACK to different client. Another end node is not proficient to discriminate the sequence number of this ACK so; it efforts to re-synchronize the session within its interactive peer. Thus, in this ACK containers go back and forth source an ACK storm.

(c) Security Mechanism at Transport Layer
The protocols hired for fortifying transport layers are Secure Socket Layer (SSL), private communication transport (PCT) and Transport Layer Security (TLS). To secure the session, SSL/TLS custom asymmetric key cryptography technique. EAP-TLS, an upper layer authentication protocol was planned by Ababa and Simon. EAP-TLS proposals mutual authentication amongst MR and MC. In this each terminal turns as an authenticator for its previous node.

(d) Transport layer Research Issues
It comprise several protocols occur for consistent real time delivery and data transport. Reliable data transport distresses with ACK, TCP data, ATP. In WMN, TCP acknowledgement and data surveys different path outcomes bandwidth, packet loss and reaction time. Even if same path usages face transmission in ATP and network asymmetry problems is rate based and for real time delivery, the protocols castoff are RTP, UDP and RCTP.

The current open research concerns are occupied on is to escape asymmetry amongst acknowledgement and data paths, it is expected for a routing protocol to choice an optimum route for both ACK and data packets but without increasing the budget items.
2.5.5 Application Layer

Application layer provisions the end user processes. It delivers electronic mail; network software’s and files transfer facilities. File Transfer Protocol (FTP) and Telnets are the claims that endure in this layer only.

(a) Responsibility

It confirms the user to contact the network and offers the user provision for services, i.e. email, file transfer and network virtual terminal.

(b) Attacks at Application Layer

Flooding and Snooping are the two major attacks in WMN. Flooding attack disturbs the accessibility of victim and huge serving of the network while snooping attack disturbs the unity of the message being connected.

(c) Mechanisms

IDS and firewalls are most normal conducts of securing application layer. Firewalls proposal the protection alongside spywares and malware etc.

2.6 CONCLUSION AND OPEN RESEARCH CHALLENGES

In the event that any association's system is hacked, programmers may get to all the individual databases of customers as effectively as its representatives. Thus, the main thing to keep your system secure is to give the get to just to approve clients. WMN designs comprising of two sorts of hubs, work switches (MRs) and work customers (MCs). Work switches go about as spine which give the system administrations to the customers and are in charge of sending the information parcels to their expected goal hubs though MCs are the end focuses that get to the system administrations through work switches.

Whenever a MC moves outside the boundary range of its current serving mesh router then the corresponding SNR of that serving MR will fall due to signal attenuation. A significant drop in SNR ratio makes the MC to search for a new mesh router having good signal strength for continuing its network services by triggering the handoff procedure. The SNR value is used to measure the signal strength between source and destination. It is important because by measuring this it is easy to predict at what distance a router can be placed between source and destination so that the signal will reach to its destination without any distortion. This concept of SNR is used in handoff authentication process where during the handoff procedure mesh client needs to search a new mesh router for resuming its
communication by measuring its SNR value. Since the nodes are dynamic, unstable and limited by security disputes with new performance issues, a significant delay in handoff procedure may cause copious performance concerns such as network attacks and delay in the network. Therefore, during the handoff procedure, it is prerequisite that roaming clients ample access authentication process not only with a short delay but also with the fortification of the roaming clients as well as the handoff networks. Further, if a node either inter-domain (communicating between two domains) or intra-domain (communicating within a domain) wants to send some messages to its intended destination node, the information is being passed among multiple MRs. However, to prevent the data exposure at each intermediate node, the messages must be encrypted by some security technique or an ornate encryption technique is required to guarantee that even if the message is forged by an intruder then it may not be able to decrypt it anyway. Due to the dynamic nature of WMN where information is being passed over multiple hops or MRs, data encryption process is taken to be an important parameter. Furthermore, the most significant factor that impacts the WMN performance is the nature of the fundamental routing protocols used for promoting the data packets. Presence of any malicious or misbehaving node within a routing path may interrupt the network activities either by spoofing or reducing the data packets or by degrading the overall performance of the network.

Although, a number of scientists/researchers have proposed various handoff authentication procedures and message encryption and secure routing techniques, however, the issues arise due to the intruders that encounter a number of malicious nodes or threats to disrupt the network performance. In addition to this, by increasing one parameter such as to ensure the security others parameters (such as end-to-end delay, network throughput, packet delivery ratio) get affected drastically, therefore, there is a need to propose an efficient security technique having reduced authentication delay, less encryption/decryption time and secure routing mechanism against routing layer attacks with the aim of increasing the other network parameters. Therefore, in order to provide an efficient and secure communication process, the security is ensured at three different aspects i.e. authentication of handoff clients, encrypted message transmission between source and destination and secure route discovery to route the transmitted data packets.