Security in Wireless Mesh Networks

Master’s Thesis in Computer Network Engineering

Presented By: Shakeel Ahmad Ghumman

Supervisor: Per-Arne-Wiberg
In the name of the Lord, “ALLAH”, whom is my GOD
Preface

First and foremost I wish to thank my parents for their utmost moral support and freedom I needed to move on and to achieve this milestone. Thanks for eternally supporting me to pursue my wellbeing. I am sincerely grateful to my supervisor Per-Arne-Wiberg, for giving me the opportunity to carry out this interesting and challenging research and for his mentoring, supervision, encouragement, and close collaboration, since the days I begin working on this thesis.

I am enormously obliged for the harmonious environment of study and research in Halmstad University.

Shakeel Ahmad Ghumman
Halmstad University, May 2009
Security in Wireless Mesh Networks

Abstract

The Master’s thesis report describes the wireless mesh networks functions, characteristics, network management and finally different protocols with security issues and applications. Wireless Mesh Networks (WMNs) are replacing wireless Infrastructure networks in many areas because of their lower cost and higher flexibility. The wireless mesh networks (WMNs) provides network access for both mesh and conventional clients through mesh routers and mesh clients. Communication across the network is formed via the bridge functions. Mesh router also provides the minimal mobility and form the backbone of WMNs.

Wireless mesh network has resolved the limitation of ad hoc networks which is ultimately improves the performance of Ad hoc networks. Security is a very important issue which can be resolve through proper management of network. The improvement of 802.11i security has greatly improved the network performance and increase the encryption and integrity security capabilities. The key points which are being addressed in this report are security issues and threats and their counter measures. Attacks which can come on different layers are being discussed in this survey. Security of wireless mesh network is still under consideration. Wireless mesh network are attracting more attention due to its enhanced features.

Wireless mesh network topology and technology is being discussed in this report. Then network management of WMNs is explained and in the concluding chapters security issues are discussed. Threats, attacks and challenges of WMNs are discussed in this survey.

Keyword: Wireless mesh networks infrastructure, characteristics, network management, standards, security issues in WMNs and applications of WMNs.
List of Figures

Figure 2.1: a- PowerPC, b-Advanced Risc Machines (ARM) ........................... 14
Figure 2.2: a- Laptop, b- PDA, c- Wi-Fi IP Phone, d- Wi-Fi RFID Reader .......... 15
Figure 2.3: Infrastructure/backbone WMNs ................................................. 17
Figure 2.4: Client WMNs ............................................................................. 18
Figure 2.5: Hybrid WMNs ........................................................................... 19
Figure 6.1: 802.11s frame works ................................................................. 31
Figure 6.2: 802.11s topologies .................................................................... 32
Figure 8.1: Broadband Home Networking ...................................................... 44
Figure 8.2: Community and Neighborhood Networking .............................. 45
Figure 8.3: Enterprise Networking ................................................................. 46
Figure 8.4: Metropolitan Area Networks ....................................................... 47
Figure 8.5: Transportation Systems ............................................................... 48
Figure 8.6: Building Automation ................................................................. 49
# Table of Contents

1 Introduction ................................................................. 10
  1.1 Goal ........................................................................ 12
  1.2 Motivation .............................................................. 13

2 Wireless Mesh Networks .................................................... 14
  2.1-Mesh routers ............................................................ 14
  2.2-Mesh clients ............................................................ 15
  2.3 Wireless Mesh Networks Architecture ............................. 15
    2.3.1 Infrastructure/backbone WMNs ............................. 16
    2.3.2 Client WMNs .................................................... 18
    2.3.3 Hybrid WMNs .................................................... 18

3 Characteristics of WMNs .................................................... 20
  3.1 Difference between WMNs and Ad hoc Networks ............... 20
    3.1.1 Wireless infrastructure/backbone .......................... 20
    3.1.2 Integration ....................................................... 20
    3.1.3 Dedicated routing and configuration ....................... 20
    3.1.4 Multiple radios ................................................ 21
    3.1.5 Mobility ........................................................ 21
    3.1.6 Application Scenario ......................................... 21
  3.2 Technology of WMNs .................................................. 21
    3.2.1 Mesh Routing .................................................. 22
    3.2.2 Point to Point ................................................ 23
    3.2.3 Point to Multipoint .......................................... 23
    3.3.4 Multipoint to Multipoint ..................................... 23

4 Network Management in WMNs .......................................... 25
  4.1 Fault Management .................................................... 25
  4.2 Configuration Management .......................................... 26
  4.3 Administration management ......................................... 26
  4.4 Performance Management ........................................... 26
  4.5 Security Management ................................................ 26

5 Analysis of Standards ..................................................... 27
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>802.11a</td>
<td>27</td>
</tr>
<tr>
<td>5.1.1</td>
<td>802.11a Benefits</td>
<td>27</td>
</tr>
<tr>
<td>5.1.2</td>
<td>Security and Use of 802.11a</td>
<td>27</td>
</tr>
<tr>
<td>5.2</td>
<td>802.11b</td>
<td>28</td>
</tr>
<tr>
<td>5.2.1</td>
<td>802.11b Benefits</td>
<td>28</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Security and Use of 802.11b</td>
<td>29</td>
</tr>
<tr>
<td>5.3</td>
<td>802.11g</td>
<td>29</td>
</tr>
<tr>
<td>5.3.1</td>
<td>802.11g Benefits</td>
<td>29</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Security and Use of 802.11g</td>
<td>30</td>
</tr>
<tr>
<td>5.4</td>
<td>802.11n</td>
<td>30</td>
</tr>
<tr>
<td>6.</td>
<td>Analyses of Coming Standard</td>
<td>31</td>
</tr>
<tr>
<td>6.1</td>
<td>802.11s Scope, Topology, Discovery, and Extensible Framework</td>
<td>31</td>
</tr>
<tr>
<td>6.1.1</td>
<td>Mesh Portal</td>
<td>31</td>
</tr>
<tr>
<td>6.1.2</td>
<td>Mesh Point (MP)</td>
<td>32</td>
</tr>
<tr>
<td>6.1.3</td>
<td>Mesh AP (MAP)</td>
<td>32</td>
</tr>
<tr>
<td>6.1.4</td>
<td>Station (STA)</td>
<td>32</td>
</tr>
<tr>
<td>6.2</td>
<td>Security in 802.11s</td>
<td>33</td>
</tr>
<tr>
<td>7.</td>
<td>Security in Wireless Mesh Networks</td>
<td>34</td>
</tr>
<tr>
<td>7.1</td>
<td>Basic Prevention</td>
<td>34</td>
</tr>
<tr>
<td>7.1.1</td>
<td>Data Confidentiality</td>
<td>34</td>
</tr>
<tr>
<td>7.1.2</td>
<td>Traffic Confidentiality</td>
<td>34</td>
</tr>
<tr>
<td>7.2</td>
<td>Mesh Security and security goals</td>
<td>34</td>
</tr>
<tr>
<td>7.2.1</td>
<td>Confidentiality</td>
<td>35</td>
</tr>
<tr>
<td>7.2.2</td>
<td>Availability</td>
<td>35</td>
</tr>
<tr>
<td>7.2.3</td>
<td>Authentication</td>
<td>35</td>
</tr>
<tr>
<td>7.2.4</td>
<td>Authorization</td>
<td>36</td>
</tr>
<tr>
<td>7.2.5</td>
<td>Accounting</td>
<td>36</td>
</tr>
<tr>
<td>7.2.6</td>
<td>Integrity</td>
<td>36</td>
</tr>
<tr>
<td>7.2.7</td>
<td>Access Control</td>
<td>36</td>
</tr>
<tr>
<td>7.3</td>
<td>Security Challenges</td>
<td>36</td>
</tr>
<tr>
<td>7.4</td>
<td>Overview of Potential Attacks to WMNs</td>
<td>37</td>
</tr>
</tbody>
</table>
7.4.1 External Attacks ...............................................................................................37
7.4.2 Internal Attacks ............................................................................................37
7.4.3 Flooding Attack ............................................................................................38
7.4.4 Jamming Attacks ..........................................................................................38
7.4.5 Sleep Deprivation and Packet Dropping Attacks ...........................................38
7.5 Routing Attacks ...............................................................................................38
7.5.1 Black-hole Attacks .......................................................................................38
7.5.2 Grey-hole Attacks .........................................................................................39
7.5.3 Worm-hole Attacks ......................................................................................39
7.5.4 Route error injection .....................................................................................39
7.6 Solution against the threats and attacks ............................................................39
7.6.1 Cryptography ................................................................................................39
7.6.1.1 Conventional Key ......................................................................................40
7.6.1.2 Public Key Management ..........................................................................40
7.6.1.3 Pretty Good Privacy (PGP) ......................................................................41
7.7 Wired Equivalent Privacy (WEP) .....................................................................41
7.8 Temporal Key Integrity Protocol (TKIP) ..............................................................42
7.9 802.11i ............................................................................................................43
7.10 Information Exchange Polices ..........................................................................43
7.11 Physical threats and their counter measures ....................................................43
8 Use Cases of Wireless Mesh Networks .................................................................44
8.1 Broadband Home Networking ........................................................................44
8.2 Community and Neighborhood Networking ....................................................45
8.3 Enterprise Networking ......................................................................................46
8.4 Metropolitan Area Networks ............................................................................47
8.5 Transportation Systems .....................................................................................48
8.6 Building Automation ........................................................................................48
8.7 Health and Medical Systems ...........................................................................49
9 Conclusions ..........................................................................................................50
9.1 Recommendations ............................................................................................51
References ..............................................................................................................52
1 Introduction

Wireless mesh networking is an attractive, emerging and new way of communication due to its low cost and its scalable wireless internetworking solutions for near future, which is the reason that it is becoming little popular communication sector.

In all kind of networks security is one of the major factor for reliable and trusted communication. [1] WMNs have many advantages other wireless networks. For example it provides very simple settings, broadband capability and the inherent fault tolerance in case of network failures. Deployment of WMNs is very easy. It is dynamically self-configured and self organized with the existing nodes in the network by automatically establishing and maintaining mesh connectivity among the nodes so it brings reliable service coverage in the network. [2]

Due to its cost effective solution it has been proposed in different networks. Mesh networks can be seen as one type of mobile ad hoc network (MANET). Data can be transmit to destination nodes by using multiple hops, and provides the backbone nodes that are generally not mobile. The IEEE 802.11 working group has provided many standards for communication and now they are more focusing on 802.11s standard due to its dynamic path configuration and topology learning. Wireless mesh networking is a way of routing the data, voice and instructions between the nodes. Sometimes WMNs provides local 802.11g access to clients and connects neighbors using 802.11a “backhaul” but not always because requirements varies like peak data rate and coverage range etc. [2]

Nodes automatically establish an ad hoc network and maintain the connectivity due to that network provide dynamically self-organization and self-healing and self-configuration and selects the optimal path back to the “wired” network. WMNs consist of mesh routers and mesh clients. Mesh routers provide network access for both mesh and conventional clients. Mesh routers form the mesh backbone and provides the minimum mobility. It provides the same coverage as conventional routers do but with the lower transmission power. Usually it has multiple wireless interfaces but has similar hardware. [3]. It provides the additional routing functions for mesh networking. On the other hand mesh clients must have necessary mesh functions for behaving like mesh routers and for
transmission of data in the network. They have only one wireless interface for connectivity. Gateway or bridge functions do not exist in these nodes. Clients are being interconnected via a wired backbone network with wireless access points in WLAN deployments so due to that wireless networks can have only a single hop of the end to end path. For connectivity clients must need to be within a single hop range of wireless access point. For achieving the more coverage they must have more number of fixed access points. In large scale the deployment of WLAN is very costly and time consuming as well. In contrast WMNs one can achieve wireless network coverage of large area without dedicated access points and without relying on wired backbone infrastructure. Mesh routers provide network access to wireless clients in WMNs and by involving multiple wireless hops communication between these mesh routers is achieved. Multiple mesh routers can serve as gateway for internet connectivity in mesh network or nodes.

The key difference between these two is that the wired backbone network is replaced by a wireless mesh network. In this thesis security of wireless mesh networks will be investigated. Furthermore, I present the features IEEE 802.11s which is the proposed solution for WMNs.

Chapter 1 describes the introduction with goal and motivation. In chapter 2 WMNs is discussed in detail then in chapter 4 important characteristics are written. In chapter 4 network management is briefly described and in chapter 5 and 6 analysis of existing and coming standard is discussed. In the chapter 7 and chapter 8 the most focus is on security with their counter measures. At the last conclusion with recommendation and reference is described in detail.
1.1 Goal

Security in all kind of networks is a big challenge. Various types of threats and attacks can be caused for network failure and they can disturb and change the routing updates, data and decrease the network performance. This project should survey possible attacks against wireless mesh networks and present counter measures against such attacks in a wireless mesh network.
1.2 Motivation

The main motivation of choosing wireless mesh networks is that now a days around the globe IEEE 802.11 wireless mesh networks are being deployed for the purpose of allowing internet access and offering many other services to the users in the cities. Currently, there are already many applications for wireless networks. IEEE 802.11 wireless mesh technologies are a critical part in the infrastructure of wireless networks, and even more in the performance of wireless applications. WMNs are providing high coverage to all users. For these reasons, vendors and the research community are actively investigating new ways of improving the performance of IEEE 802.11 wireless mesh networks. In that regard different standard like IEEE 802.11s would be studied in this thesis.
2 Wireless Mesh Networks

The term WMNs describes wireless networks in which nodes can communicate directly or indirectly with one or more peer nodes. The word mesh describes that all nodes were connected to all other nodes directly but in most modern meshes it connects only a subset of nodes to each other. In WMNs we have two types of nodes

2.1-Mesh routers
2.2-Mesh clients

Both type of nodes can operates as a host and router as well. Packets are being forward on behalf of other nodes that may not be within direct wireless transmission range of their destinations. [4]

2.1 Mesh Routers

Mesh routers are mainly stationary devices. Through multi-hop technology they can achieve the same coverage as a conventional router do but with much less power. They have additional routing functions that support mesh networking. [2] Its greatly helps the users by connecting them with wireless mesh routers through Ethernet even though they do not have wireless NICs, so user can be always online, anywhere and any time. Through gateway or bridge functions they integrate with different existing wireless networks such as cellular, wireless-fidelity (Wi-Fi) 802.11 a,b,g and 802.11n. [4]

Figure 2.1: Examples of mesh routers based on different embedded systems: (a) PowerPC and (b) Advanced Risc Machines (ARM).
2.2 Mesh Clients

Mesh clients can be mobile or stationary as well. Mesh clients have necessary mesh functions and they can acts as a router but they do not have gateway or bridge functionality. They only have one wireless interface. We have large variety of devices that can acts as mesh clients. [3]

![Figure 2.2: Examples of mesh clients: (a) Laptop, (b) PDA, (c) Wi-Fi IP Phone and (d) Wi-Fi RFID Reader.](image)

2.3 Wireless Mesh Networks Architecture

AWMN can be categories in three different network architectures based on the network topology and functionality of the nodes. These categories are briefly discussed below.
2.3.1 Infrastructure/backbone WMNs

In this type of architecture the network is formed by connecting different type of nodes that are both routers and clients. Each node is at the same level as that of its peers. [5] They include mesh routers that form an infrastructure for clients that connect to them. The infrastructure can be built by using different types of radio technologies and that technology varies significantly. We have typically two types of radios which are used in routers, one for backbone communication and other for user communication. The directional antennas are used for long range communication in backbone communication. Backbone networks are being formed by applying self-configuring, self-healing links among themselves [6]. Mesh network have ability to build and configure itself. As any end node is powered on it listens and finds the neighbor nodes and sent them a request to join the networks and then nodes get admitted after fulfilling the network security requirements. Automatically path or routes will be established by the end node as the information that it transmits gets relayed by neighboring nodes until it reaches the central node [10]. If one or more than one end nodes are moved from one location to another location then self healing function provide the reorganization for those nodes in mesh networks and keep those nodes functioning in the network. Self healing function provide the redundancy in the mesh network because if a node is removed or fails in the network then message can be transmit around the network via other nodes. Self-configuration capability provides no human intervention for re-routing of messages to the destination nodes [10].

Through gateway functionality, mesh routers can be connected to the Internet and provides backbone for conventional clients in the mesh network [4]. Users which have Ethernet interface can be connected to mesh routers via Ethernet links. The routers form a mesh by connecting to one another and are responsible for routing client data. The data may travel via multiple router hops before reaching its final destination. [7]. The primary advantage of this architecture is its simplicity, and its disadvantages include lack of network scalability and high resource constraints. If the conventional clients have the same radio technology as the mesh routers has then they can directly communicate with
mesh routers, but if they have different radio technologies then clients must communicate with the base stations that have Ethernet connections to mesh routers.

**For example:** Community and neighborhood networks can be built by using this, the mesh routers can be placed on roof which serve as access point for user whether they are home users or they are using it on the road.

Figure 2.3: Infrastructure/backbone WMNs.
2.3.2 Client WMNs

They provides the peer to peer networks among clients, the client nodes perform the routing and other configuration functionalities as well as providing end-user applications to customers. The clients themselves perform these responsibilities and uphold the network connectivity. In this we have end devices more strained than infrastructure meshing. We do not have central infrastructure for performing regular networking functions client mesh resembles a MANET. We do not need mesh router for performing these types of functions. [4]

Multiple nodes are being used for packet delivery from source to destination. Client WMNs are formed by using one type of radios on nodes. As end users have to perform additional functions such as self configuration and routing so their requirements on end-user devices are increased as compare to infrastructure meshing. [6]

Figure 2.4: Client WMNs.

2.3.3 Hybrid WMNs

This is the combination of both meshing architectures (infrastructure and client). In Hybrid mesh through mesh routers or by directly meshing clients with other mesh clients
can access the network. As I discussed earlier that infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks; the routing capabilities of clients provide improved connectivity and coverage inside the WMN. Since the growth of WMNs depend heavily on how it works with other existing wireless networking solutions, this architecture becomes very important and most applicable in WMNs. [6]

Figure 2.5: Hybrid WMNs
3 Characteristics of WMNs

Wireless mesh networks are multi hop networks and provides much coverage range. Like if one node is failed or turns off then through other nodes message can be transmitted to destination nodes that function provides the redundancy in the mesh network. They have capability of self healing and self forming and self organization and provide support for Ad Hoc Networking. As we have multi-hoping so it achieves higher throughput, and more efficient frequency re-use. They provide low cost for installation because the reduction of the number of access points to internet so the main advantages of WMNs is that easiness of deployment. Multiple type of network access like support for internet and p2p communication as well. Provide compatibility with existing wireless networks like WiMax, Wi-Fi, cellular networks. It has flexible network architecture.

3.1 Difference between WMNs and Ad hoc Networks

The comparison of WMNs and Ad hoc networks is discussed and summarized as below:-

3.1.1 Wireless infrastructure/backbone
The WMNs consist of wireless backbone with mesh routers, WMNs provides large coverage, connectivity, and robustness. On the other hand the coverage of ad hoc networks depends on contributions of end users, which may not be reliable.

3.1.2 Integration

Through gateway or bridge functions WMNs enables the integration of various existing networks such as Wi-Fi (802.11a, b, g, n), the Internet, cellular and sensor networks.

3.1.3 Dedicated routing and configuration
For these functionalities the WMNs contain mesh routers and in ad-hoc networks, end-user devices perform routing and configuration functionalities for all other nodes or users. In WMNs we do not have much load on end-user devices. [4]
3.1.4 Multiple radios

In WMNs mesh routers may have multiple radios for performing and access functionalities. Routing and configuration are performed between mesh routers which improve the capacity of network and in Ad hoc we have one radio for all functions which works on the same channel. [6]

3.1.5 Mobility

The network topology changed dynamically in Ad hoc networks because we have high mobile networks and it depends on the movement of uses. On the other hand, WMNs have fixed nodes and they provide relatively static mobility, and their network mobility is relatively low as compare to ad-hoc networks. [6]

3.1.6 Application Scenario

WMNs are being used in military and civilian applications as well due to their permanent and semi permanent devices but in the other hand in ad hoc mostly ad-hoc networks are temporary so they can not be used for both purposes. WMNs are used in many other applications as well like broadband home networking, community and neighborhood networking, enterprise networking, metropolitan area networking, transportation systems, health and medical systems and in security and surveillance systems. [5]

3.2 Technology of WMNs

It is a communications network model that works in the same way as the wired internet works. We have more than one possible pathway between each node for communication. In mesh network architecture we have multiple possible connections for every other node which improves on point-to-point and point to- multi-point like centralized hub and spoke topologies.
3.2.1 Mesh Routing

For Wireless mesh routing multiple technologies are being used that proactively and reactively determine traffic paths within the radio network. On demand a route is being established to a destination by using reactive routing protocol but the proactive routing protocol are often based on link state for finding the routing paths irrespective of the path usage or demand. Combination of reactive or proactive mechanisms is used in vast numbers of different routing protocols. Mostly the implementation of ad-hoc networks is based on hybrid on-demand and link-state routing protocols. [24]

On-demand basic operation

The most popular example of an on-demand ad-hoc routing protocol is Ad-Hoc On-Demand Distance Vector (AODV) routing. In this route is being discovered be sending request messages called (RREQ) through a sub-portion of the network. In response path to destination is being announced by route replies called (RREP). List of all neighbor nodes and routes to other nodes are maintained on nodes. If we have link breakage in the network that can be reported through using route error messages (RERR). [24]

Link state basic operation

The example of a proactive routing protocol is Optimized Link State Routing Protocol (OLSR). In this neighbor routes are discovered by using the periodic broadcasts. For communicating with the neighbor nodes RREQ message is broadcasted in case of not finding the destination and after receiving the RREQ on neighbor nodes a uni-cast RREP is being replied if the neighbor knows the route otherwise the request is rebroadcasted and at then RREP with sequence number is received for optimal route. [24]
Network Topologies

For self healing and optimization of ongoing process between the nodes mesh topologies are used, which are discussed as below:-

3.2.2 Point to Point

Point to point provides high performance, high speed interconnections and dedicated connection between the nodes. It is very simplest form of wireless communications that enables two nodes for communication with each other. It is not highly scalable and relatively it can be deployed quickly.

3.2.3 Point to Multipoint

In this type of topology we have more than one connection for a single node. By using multiple nodes a connection is being established between base station and other nodes. When a new user wants to enter in the existing network it can easily do that but user must be in the range of base station and subscriber requires only equipment for deployment at the user end, so this solution is best suited for backhaul operations like connection to main central site. [8]

Backhaul Operation

Data traffic and voice is transmitted from a remote site to a central site/backbone. The connection is being established from the main radio towers or transmitters to the rest of the network. We must have wireless architectures at every site in the network. This is mainly done with land lines.

3.3.4 Multipoint to Multipoint

Data is routed between different nodes for the destination so for that a routed mesh topology is created for that purpose. Multiple access routers are deployed for maximum
coverage and for high density, so all routers perform the functions for data through the
network over multiple hops. [8] User can join network any time, any where in the entire
mesh does not matter that the user is going to be connect through wireless or wired.
4 Network Management in WMNs

Network monitoring and management is very difficult in all type of networks. If we talk about the network management lot of queries comes in our mind like how we can protect of network from different type of faults. If we want to make our network more operational in performance and quality of service then we have to consider network management at the time of network deployment. We have different areas for network management like fault management, Configuration management, accounting/administration management, Performance management, and Security management. [11]

4.1 Fault Management

The typically goal of fault management is to detect fault and respond to fault conditions of the network to the administrator. Fault is corrected either by manually administration or by automatic fault recovery process. Manually fault management is relatively more time consuming as compare to automatic fault recovery. For manually recovery human expert should be available who has thorough knowledge of the network. In large scale usually automatic fault management is desirable for providing more efficiency in the network. [12] In automatic fault recovery network is continuously monitored as any fault is occurred in the network it is detected and self recovery process is applied on that fault. It can reduce the latency and human error as well and can respond faster and effectively in the network.

In WMNs variety of faults may be occurred. Transmission link fault may occur due to prolonged delays on a wireless link by misbehaving the clients in the network. Fault can be occurred in network elements, like mesh devices may fail due power supply or software or hardware crashes/failure. Congestion in traffic may collapse the network performance. If more load is offered on link and it exceeds the link or network capacity then congestion may occurred in the network is it is not handled properly. Usually those nodes which are near the gateway can be affected by more congestion due to aggregated packet relay. Fault management is handled in more efficient way by implementing
automatic fault management process. Automatic fault recovery brings the WMNs to a desirable state effectively.

4.2 Configuration Management

The main aim of configuration management is to allow network managers that they can track the whole network. Network manager must have rights that he or she can modify the software or hardware configurations of the devices being used or managed in the network. Configuration management in the network can be performed by performing configuration in different ways like by configuring the wireless gateway or by configuring the wireless access points managers can handle the situation. [13]

4.3 Administration management

Administration of authorized users is being done by establishing passwords and permissions. Administration of the equipments is sensitive issue and can be solved easily by implementing different policies.

4.4 Performance Management

The main goal of performance management in the network is to measure, analyze, report and control the network components performance over extended periods of time. During this process network performance is being monitored by analyzing the imposed QoS and other factors such as mesh security and scalability. [11]

4.5 Security Management

The main aim of security management is that to control the access of users in the network. Many factors are involved in security management which will be discussed later in this report. [11]
5 Analysis of Standards

5.1- 802.11a

802.11a works on 5 GHz frequency. In market products of this standard are rapidly launching. The standard delivers typically 23Mbit/sec and maximum data rate of delivery is 54Mbit/sec. It covers 115 feet range which is somewhat less than 802.11b systems. In some cases cost can be increases due to excess number of AP’s (access points). The modulation technique which is used for 802.11a applications is known as (OFDM). It has 8 non-overlapping channels and 64 users per AP which works on 5 GHz. In USA it operates in the 5-GHz frequency band. However in some European countries it is not more favorable due to some legal regulations. Now it is a chance that it will be accepted soon globally which would greatly enhance its and 802.11’s worldwide demand. [12, 13]

5.1.1- 802.11a Benefits

It has several benefits over other standards like 802.11b which are as follows:-

- It has high speed which is up to 54Mbit/sec. In turbo mode it can be 108 Mbit/sec which is currently not available in Europe.
- 802.11a has higher density as compare to 802.11b due to its more access points. 802.11a can supports more users due to more access point.

5.1.2- Security and Use of 802.11a

Security is a major concern in all type of applications so 802.11a used the wired equivalent privacy (WEP) algorithms. It protects the 802.11a networks and its applications. Stronger encryption key is needed for that purpose. If an administrator wants more networks security then it should be properly configured. 802.11a is mostly used in bandwidth intensive applications like convention halls, offices, computer labs, and large conference rooms. It is not directly compatible with other standards like
802.11b or 802.11g. If they want to access each others networks then they must uses routers for that purpose. It has shorter range as it is discussed above and is less capable of working through walls and floors. It consumes more power which ultimately reduces the battery life. [13]

5.2- 802.11b

It is vastly used in the market. It works on 2.4 GHz frequency and typically covers 4.5 Mbit/sec throughputs. Used mostly in the application where fast actions are needed like if user wants to share a file in the network then they can use this for file transfers. In 802.11b fewer access points are typically needed for deployment. It drains less battery because it uses lower frequencies. It is widely used in many applications like at the airports, coffee shops, and hotels. The modulation technique which is used for 802.11b protocols is known as direct sequence spread spectrum (DSSS). There are 14 frequency channels which are being defined for 802.11b standard. The channel range in USA is 1 through 11, in Europe it is from 1 through 13 and in Japan channel 14 is only a one choice. 802.11b has 3 non overlapping channels which has 32 users per AP’s. [13]

5.2.1- 802.11b Benefits

It has many befits over other protocols which are as follows:-

- It is most affordable as compare to other standards due to its lowest price points for routers and AP’s (access points)
- Can operate with dual-band such as 802.11g. It is compatible with different vendor’s equipments.
- It covers from 115 feet to 500 meters range in an open environment. As it is written above in the report it consumes less battery power so due to that clients devices can operate Longley.
5.2.2- Security and Use of 802.11b

The 802.11b networks also use the Wired Equivalent Privacy (WEP) algorithm. By using this algorithm one can protect the data from unauthorized users and eavesdropping. Proper configuration is needed for security and it can be achieved with 48, 64 and 128 bit encryptions. Mostly used in those networks where changing are often occurred. It provides more reliability in these types of networks. It provides more range in open space and through walls networks which one can not be achieved through 802.11a protocols. Ideally used in office environments like when user wants a file transfer or print sharing, database queries and e-mails. It has higher density deployments. When multiple Ap’s are needed to be configured the it can be more costly in high density or high usage situations. It should not be used where privacy is most important factor. If user wants to use 802.11b then its products must be supportive with 802.1x authentications. [13]

5.3- 802.11g

It is an extension of 802.11b standard. It works on 2.4GHz frequency and typically data rate is 19Mbit/sec and maximum data rate is 54Mbit/sec. The modulation technique which is typically used for this is OFDM. 802.11g devices can be connected with 802.11b devices due to its backward compatibility feature. It has non overlapping channels. [12]

5.3.1- 802.11g Benefits

802.11g has several benefits which are as follows:-

- It provides peak throughput which is up to 54Mbit/sec
- As it is discussed earlier that it is backward compatible with 802.11b devices
- It consumes less battery power which ultimately increases the battery use
- It is more effective than 5GHz signals and covers more range
- It can work through walls and floors
5.3.2- Security and Use of 802.11g

It uses the same Wired Equivalent Privacy security mechanism/algorithms as 802.11b. As it is compatible with 802.11b device so it can provide smooth for higher performance. It is faster than 802.11b and it is widely used in that application where more range and connection speed is important. It is less costly as compared to 802.11a. It can be used in many small businesses where use of large files such as graphic and video operate. It is not compatible with 802.11a devices. Both standards can exist in the network and access each other through the routers. [13]

5.4- 802.11n

The main aim of new IEEE 802.11n amendment is to provide more quality of service. 802.11n is a first standard which supports 5GHz and 2.4 GHz. The typical data rate which is being achieved by this standard is 74Mbit/sec and the maximum data rate is 600Mbit/sec. The basic range which this standard can be achieved is 230 feet. It uses the MIMO radio technology as a basis. Multiple streams are being used in this standard. As it has been viewed that the throughput is very important in all type of networks. 802.11n dramatically improves the throughput which is the main goal of this standard. For communication with each other 802.11n changes the basic format of communication. 802.11n increased the effective throughput by increasing the modulation rate, reducing the overheads and by increasing the channel size which are the most important changes in the network. It also extends the power management capability of the 802.11 MAC. 802.11n provides the backward compatibility with existing devices like 802.11a,b and 802.11g. It has many mechanisms through which they provide the backward compatibility with the existing devices (a, b, g). [20]
6 Analyses of Coming Standard

6.1- 802.11s Scope, Topology, Discovery, and Extensible Framework

It’s an amendment being developed to the IEEE 802.11 WLAN (Wireless Local Area Networks) standard to create a wireless distribution system with automatic topology learning and path configuration. 802.11s defines how wireless devices can interconnect to create an ad-hoc network. Under 802.11s one can build small, medium and large mesh networks. 802.11s have dynamic radio-aware path selection in the mesh that enables data delivery on single-hop and multi-hop paths, means data can be unicast/broadcast and multicast. 802.11s is easily extensible to allow support for diverse applications and future innovation. For traffic sending and receiving it uses the 802.11i security.

![Diagram showing the 802.11s network framework]

Figure 6.1: 802.11s frame works

6.1.1- Mesh Portal

The point at which MSDUs (MAC service data unit) exits. Mesh portal interconnect the MPA with External network that can be a WLAN Mesh.
6.1.2- Mesh Point (MP)

It establishes peer links with MP neighbors, full participant in WLAN Mesh services. Light Weight MP participates only in 1-hop communication with immediate neighbors.

6.1.3- Mesh AP (MAP)

Functionality of MP’s is being performed through (MAP). It is collocated with AP which provides BSS services to support communication with STAs.

6.1.4- Station (STA):  

STA are Points outside the WLAN Mesh which are being connected via Mesh AP.

Figure 6.2: 802.11s topologies  

In wireless mesh networks Mesh Points (MPs) discover the neighbor’s candidate which are based on new IEs in send (beacons) and receive (probe) response frames. For Support of Single & Multi-Channel Meshes each Mesh Point may have one or more logical radio interface. Mesh networks have extensible framework support for mandatory and alternative path selection protocols. Any vendor may implement any protocol and/or metric within the framework. A particular mesh will have only one active protocol at a time and only one protocol/metric will be active on a particular link at a time. Mesh Points use the WLAN Mesh Capability IE to indicate which protocol is in use. A mesh
that is using other than mandatory protocol is not required to change its protocol when a new MP joins.

6.2 Security in 802.11s

The MPs are no longer wired to one another so that there is no intrinsic node hierarchy between the nodes. For a secure communication MPs need to maintain secure links with many other MPs.
7 Security in Wireless Mesh Networks

Security issues and the potential of WMNs are cannot be ignored. In WMNs the understanding and properly addressing of these problems and challenges is very necessary. Due to dynamic change of network topology, distributed network architecture and shared wireless mediums WMNs lacks in security solutions. Attacks can occur on different protocol layers which can harm the network traffic and data. In wireless mesh there are different types of architecture which may uses different approaches for wireless mesh security purpose. [17]

7.1 Basic Prevention
The primary issues which are very necessary for privacy preventions are as follows:-

7.1.1 Data Confidentiality

Its main purpose to prevent from eavesdropping and protect the data against the attacks. It is controlled by intermediate mesh routers. The algorithm by which one can protect the data from misbehaviors is message encryption.

7.1.2 Traffic Confidentiality

Traffic confidentiality is quite difficult to prevent against the attacks. For traffic confidentiality users must know that to whom they are communicating and their traffic patterns must be followed by the communicators. It is usually occurred by the attackers at mesh routers while traffic transfer. By following the key distribution mechanism WMNs can overcome on this type of attacks. [18]

7.2 Mesh Security

802.11s is a standard which will be followed in future for all kind of commercial mesh products. Right now mesh products are using different approaches for security and many
of them may be derived from existing ad-hoc security mechanisms. 802.11s is a standard which will be based primarily on 802.11i security mechanisms.

**Security Goals**

In any application these are the general goals and need to be considered to overcome on the security. These goals are not application specific. In WMN application there are same basic threats which are also common for other application. e.g:- Wired and wireless networks. An attacker can intercept, modify, delayed, replayed, the message. Attacker can insert the new message in the network.

**7.2.1 Confidentiality**

In this the whole path should be protected and message should not be altered during the communication. Users must know each other for secure communication. The message and data information should not be disclosed. The data is only revealed to the intentional users.

**7.2.2 Availability**

Insurance of authorized user actions can be done for secure communication. Provide the reliable delivery of data to the destination node. Protect the message and data against DoS (Denial of Service)

**7.2.3 Authentication**

In WMNs authentication is very important because of change of shared medium. A proper mechanism should be followed for data sending and receiving. Users must know each other because it very necessary for reliable transmission of data. If user will not follow the any process then data may be infected or fabricated by any body else which cause the problem in the network transmission.
7.2.4 Authorization

Users have the right to amend the data. If anybody wants to perform any task then there should be a proper process which ensures that the person have right to perform that task.

7.2.5 Accounting

If a user is using any service then their should be a process or method through which measurement of used resources can be done for billing information of specific user.

7.2.6 Integrity

Users cannot modify the data without having proper right to perform that task. If a user do not have right to perform any task then he/she cannot modify or change the message.

7.2.7 Access Control

User should ensure that only authorized actions can be performed, like if one cannot have authorization of changing the message then that user must be communicate with administrator for performing that task which he/she wants to perform.

7.3 Security Challenges

Many challenges can be seen in WMNs due to its dynamic change in the network. Physical security of nodes is also a big considerable issue which can also be caused of network failure. New challenges are mostly seen because of multi-hop wireless communication. If administrator wants to apply statically security configuration it will not be sufficient for the network because of users frequently joining and leaving the mesh network. For mesh router and mesh clients same security solutions will not work because they have a lot of different characteristics such as mobility and power constraints.[23]
7.4 Overview of Potential Attacks to WMNs

There are two types of attacks in WMNs which are as follows:-

1) Internal Attacks
2) External Attacks

7.4.1 External Attacks

Attacker can jam the communication in the network. Attacker which is not belonging to mesh network can inject any information in the network. Active attacks can occur at this stage means attacker may can modify and inject the messages into the mesh networks.

7.4.2 Internal Attacks

These are the most severe attack which can come from compromised nodes inside the mesh networks. Its prevention is not that much easy as compare to external attacks prevention. Passive attacks can be occurred in this type of attacks. Attacker can steal the traffic and inject the messages within the network.

On different layer there are different types of attacks. An attacker may harm the hardware at physical layer. Attacker can jam the transmission and can exploit the nodes. These are the attacks which can easily locate and detected. Protocols can be destroyed by the attackers at Mac layer. An attacker can attack on the legal nodes and may misuse the medium access by sending data packets. An attacker may change the routing table at routing layer which can harm the network traffic. An attacker can sneak into the network and may not follow the required specifications of a routing protocol. An attacker may inject the fake information at application layer. [23]
These are the some major attacks which can come on Mac layer:-

7.4.3 Flooding Attack

As it is discussed above that an attacker can send a MAC control messages to its neighbor users so due to that neighbor can suffer with the DoS problem. It can also affect the victim node’s battery and channel bandwidth.

7.4.4 Jamming Attacks

This type of attack may affect the performance of wireless networks. To over come on this type of attack one can use RTS signal jamming. This is also know as DoS on the victim nodes.

7.4.5 Sleep Deprivation and Packet Dropping Attacks:-

An attacker may drain the battery of victim notes which will ultimately destroy the computational power of the victim node. If a node is not relaying the packets then packet dropping attack can also be occurred.

7.5 Routing Attacks

There are many attacks which can harm the routing tables and disturb the route traffic. Followings are the unique attacks which can come in wireless mesh networks:-

7.5.1 Black-hole Attacks

Fake packets can be created by an attacker which can exploit the network traffic. Fake routes are being advertised with low cost. Due to advertisement of false routing updates any node can be trapped by attackers.
7.5.2 Grey-hole Attacks

In this type of attack any attacker can creates a fake packet and specifically drops them on the particular nodes. An attacker can also destroy the traffic and existing routes.

7.5.3 Worm-hole Attacks

An attacker may replayed the routing control messages from one location to another which can ultimately disturb the routing of the network. Network can be jam due to its replaying behavior.

7.5.4 Route error injection

Mesh links can be breaked by injecting fake routes in the network. It’s a severe attack which can easily exploit the network traffic.

7.6 Solution against the threats and attacks

7.6.1- Cryptography
7.6.2- WEP (Wired Equivalent privacy)
7.6.3- TKIP (Temporal key integrity Protocol)

7.6.1 Cryptography

The process or system of data encryption and decryption is known as cryptosystem or cryptography. By using cryptography any sender can send their data to intended recipient in a secure way by using encryption and decryption algorithms. In method of encryption data can be transfer in to its original form which is know as plaintext or clear-text. It is unreadable until it is decrypted by the particular receivers. By following these steps one can send data in secure way. [16]
Plaintext $\rightarrow$ Encryption $\rightarrow$ Cipher-text $\rightarrow$ decryption $\rightarrow$ plaintext

Cryptography can be divided into weak and strong cryptography. The strong cryptography is cipher-text of data which is not easy to decipher without any permission or by the appropriate decoding tool. The best available implementation of strong cryptography is employed by PGP.

### 7.6.1.1 Conventional Key

In conventional cryptography, sender and receiver used the one key for encryption and decryption. It is very fast and useful for that data which is not going anywhere. For implementing the conventional key algorithm, sender and receiver must agree on the same key. If the sender and receiver are not in the same network or they are physically located away from each other, then they must use a reliable medium for confidentiality of data transmission. If they do not have a reliable medium between the sending and receiving end then any one may attack on their data. Then an attacker can read, modify the information easily. \[15, 16\]

### 7.6.1.2 Public Key Management

It is an asymmetric way through which user can secure their data. Pair of keys is being used in this process. For encryption of data a public key can be used and for decryption that encrypted information intended user must have the private or secret key. Public key can be globally published but the secret or private key is kept secreted. By copying and using the public key anybody can encrypt the data but without having secret or private key no body can decrypt the data. The basic benefit of using this key is that it allows the users to send their data in a secure way if they do not have any security system. If an intender wants to decrypt the data then sender and receiver must have the same secret or private key which can be shared via some secure way. Publically only public key is transmitted but the secret or private key is never shared or transmitted. It is most affordable as compare to conventional cryptography. \[15, 16\]
7.6.1.3 Pretty Good Privacy (PGP)

It is a hybrid cryptosystem that uses the best features of public and conventional keys. Features are combined in the pretty good privacy. By using that a user can first compress the plaintext. By compression of plaintext a user can save the disk space. If data is not so big then it can not be compressed so for securing that data a session key is being created. It can be used only one time after that new key must be created. By using the session key data can be transmitted very fast. In session key random numbers are being created that uses the conventional encryption algorithm for encrypting the data. When data is being encrypted the resultant cipher-text can see easily. When data is being encrypted the session key then encrypt the public key of receiver. Session key is the being encrypted by the public key and it is being transferred to the intender along with the cipher-text. [16]

7.7 Wired Equivalent Privacy (WEP)

It is a protocol which is being used for secure communication between access points (AP’s) and Stations (STAs). By using WEP users can secure their data it does not matter that whether u r applying this in wireless environment or in the wired infrastructure. The encryption algorithm which is used in this is known as "RC4". It is used for data confidentiality. In a network if sender and user want to communicate with each other then they must have a correct secret key. By using the secret key user can secure their information. WEP used a 40-bit key by default so due to that it does not provide as much security. That is also a main drawback of this key. WEP may support 104-bit key but it causes problem in those environments where devices used 40-bit key encryption. It does not provide much security even though they use the 104-bit key encryption. An attacker may disclose the key within 20 minutes. Encryption key is being repeated after a specific period of time so due to that cipher-text can be break. [19]

Wired equivalent privacy protects the communication from eavesdropping. It protects the wireless networks from unauthorized users. The main goal of this protocol is to ensure that the wireless infrastructure is not used means access control. It provides the data integrity. Means it ensures that the packets are not modified in the transmission. As it
relies on the secret key that is being shared between two users. Sender and receiver can be any. For example a sender may be using laptop which is being connected through wireless ethernet card and receiver is a base station (access point). By using secret key packets are being encrypted before transmission then integrity check is used for checking that packets are not changed during the transmission. [19]

7.8 Temporal Key Integrity Protocol (TKIP)

It is adopted as a part of WPA certification. The main purpose of TKIP is to allow WEP system to be upgraded in a secure way. It provides the backward compatibility. TKIP addresses the all known attacks and deficiencies in WEP. Its design has restriction in hardware. It is also known as an enhancement over WEP protocol. TKIP works on same hardware where WEP work but with software enhancement for more security. If users want to have a better secure system then they must use a better cipher technique by using that one can overcome on WEP problem permanently. For better technique new security protocol can be designed from scratch and it needs new hardware in access points and wireless cards. This technique may increase the cost to wireless equipments. In current situation it is only economical where no extra hardware is needed that provides more feasibility solution to WEP problems. TKIP uses long encryption keys and based on RC4 cipher stream. For more security it uses long keys like 48 bit IV with 64 authentication key and 128 encryption key. In TKIP keys are not reused every time different key per packet is used. For transmission between access points and stations different encryptions keys are used. A sequence number is being created by keys generation from different combination. In sequence number sender’s MAC address and packet sequence number is combined together. A tool which is defined for reply attacks of WEP protocol is known as TSC and it requires synchronization between sender and receiver. By using TKIP one can overcome on data integrity by including cryptographic protocol (Message integrity code). In MIC message is being accepted as a input and a special tag is produced as a output which uses one-way hash. One-way- hash accepts 64-bit authentication key for this process. The main enhancement in TKIP is that it increases the length to 48-bit. It uses the IV as sequence counter against the reply attacks. [19]
7.9- **802.11i**

802.11i provides enhanced security and support the inherent protocols for backward compatibility. It is a new standard which solve the security problems of TKIP and WEP. It is based on IEEE802.11 and provides security enhancement at MAC layer. By using this standard one can overcome on most important security goals like authentication, integrity and confidentiality. 802.11i introduced strong encryption algorithm and advanced encryption standard and introduced also new key management schemes. By overcoming on the attacks and secure authentication and integrity 802.11i can be implemented. [19]

7.10- **Information Exchange Policies**

If any body wants to join a network then he/she must follow the basic authentication rules which are discussed above in the report. After joining the mesh network a user must have to follow the terms and condition which are being made by an administrator. For example if a user wants to sends information to another user then he/she must follow the basic transmission rules. For secure communication it is necessary that they must know each other. For more security administrators must developed security monitoring and response system. By developing these systems network can work in a secure way.

7.11- **Physical threats and their counter measures**

Their should be a operator who monitor the outdoor deployment. All access point must be in control of and operator. Physically security of device is very difficult but it can be done through security and monitoring systems. Typically access point are deployed on light poles are on the buildings so for their security there should be system. Administrators can protect them by putting them in the racks or any sensor can be attached with the access points. In some case wired mesh connectivity is needed which can expose sensitive network connections.
8 Use Cases of Wireless Mesh Networks

The applications of wireless mesh networks are as follows:-

8.1 Broadband Home Networking

Broadband home networking is realized through IEEE802.11 Wireless LANs. Deployment of AP’s is quite difficult in home networking. For connecting to the small house with AP’s is very easy through WMNs. Installing multiple access points is expensive and inconvenient in wireless networks because each access point needs to be wired and also not convenient because of Ethernet wiring from access points to backhaul network access modem or hub. Homes may have many dead zones without service coverage. The overall solution is too expensive for site surveys and not practical for home networking. If there are two AP’s then communications between end nodes under two different access points have to go all the way back to the access hub and it is not an efficient solution, especially for broadband networking. Mesh networking can resolve all these issues in home networking. As the number of hops increase, throughput degrades. [21]
8.2 Community and Neighborhood Networking

For connecting and managing the neighbors in community is little difficult because in the community and neighborhood networking a common architecture for network access is based on cable or DSL (Digital subscribers line). The last-hop is wireless router which connects the wireless with a cable or DSL modem. Several drawbacks can be seen in this type of networks. More network resources are used for information sharing within a community or neighborhood. All information must pass through the internet for communication between communities. Cost is also a issues between these type of networks. Multiple homes or neighborhoods may not be shared the information and wireless services must be set up individually. For communicating with the neighbors only a single path may be available for one home to access the Internet. WMNs can mitigate these disadvantages and provide many applications such as distributed file storage, distributed file access, and video streaming. [21, 22]
8.3 Enterprise Networking

Currently IEEE802.11 WLANs are widely used on many places like in offices and in the buildings. They are still isolated islands. In offices connections between the devices are achieved through wired ethernet which is very costly. For increasing the throughput locally more backhaul access modems can be added. It does not provide strong connection in case of link failure. Network congestion can be seen in enterprise networks. Wireless mesh networks provides the multiple backhaul access modems which can be shared by all nodes in the entire network [22]. Scalability is also a advantage of using WMNs in enterprises. Wireless mesh networks can grow easily as the size of enterprise expands.

Figure 8.3: Enterprise Networking
8.4 Metropolitan Area Networks

It provides the higher transmission rate at the physical-layer as compare to other networks such as cellular networks. Like the transmission rate of IEEE 802.11g nodes is 54 Mbps. The communication between nodes in WMNs does not rely on a wired backbone. Economically it is a best alternative for underdeveloped regions and broadband networking. Large range can be covered through wireless mesh MAN (Metropolitan area networks). For scalability purpose wireless mesh MAN needed have more requirements. [21]

Figure 8.4: Metropolitan Area Networks
8.5 Transportation Systems

For communication between transports mesh networking needed two key techniques. The one is that they needed high-speed mobile backhaul for communication from a vehicle (car, bus, or train) to the internet and the second one is mobile mesh networks within the vehicles. Mesh networks can extend access into different transports by using mesh networking technology. Mesh networking technology provides the facility to drivers that they can communicate with the remote monitoring administrators easily. Driver can pass convenient information to the monitoring person. [21]

8.6 Building Automation

Monitoring and controlling is a quite critical issue in all type of applications. Like if administrators wants to monitor and control the building devices like elevator, air conditioners they may need a better control system. Wireless mesh networks provides the facility which is much cheaper solution as compare to wired an WIFI systems. In many building they are still using the wired network which is quite expensive as compare to wireless mesh networks. Wi-Fi reduces the cost by replacing the wired networks but still performance is not much satisfactory because they are also expensive as compare to mesh routers. Deployment of wireless mesh networks is quite simpler due to having mesh connectivity between wireless devices like routers [22].
8.7 Health and Medical Systems

Wireless mesh networks provides a good solution for controlling and monitoring the activities in the medical centers and hospitals. Transmission of information from one room to another must be diagnosed and monitored by the controller. In mostly health centers they are using wired networks which provide the limited network access and increase the cost of the system. [21]
Conclusions

The ability of self healing and self organization is key factor in WMNs which reduces the network complexity and maintenance. Provides the backbone ability through which a user can connect to internet any where any time. WMNs are a promising technology for next generation wireless networking. WMNs have enhanced the capability and reliability of ad hoc net works.

There are still many problems in WMNs which needs to be improved. The existing approaches are effective at specific layers but there is still need to have a comprehensive mechanism which can prevent from the attacks at protocol layers. For self healing and self organization WMNs still requires a inclusive protocol.

The main focus of this thesis survey is to provide right recommendation and direction towards security enhancement. The security solutions used in Wireless LANs are not getting ready for WMNs. Cryptography, key management; WEP and TKIP are considerable solutions which are available right now for WMNs devices. IEEE task group defines 802.11s which is a pre draft for wireless mesh networks. In near future it can be deployed with its full functionality. Right now 802.11s is using the techniques of 802.11i. There are still many research problems in WMNs but it is most promising technologies for next-generation wireless networking.
Recommendations

As Wireless mesh network security is still in its infancy so it is quite difficult to overcome on these threats and attacks. Security is a tough challenge which influences the deployments of wireless mesh networks however there should be strong efficient solution for WMNs. The security requirement varies in different scenarios. There trusted relationship should be developed between the users. As authentication, authorization, and accounting are important parameters so there will be trusted handshakes between the users. By following these recommendations one can overcome on many problems, issues, threats and attacks.

- Proper implementation and management of security controls is needed
- Network management tools need to be developed for mesh design, maintenance, monitoring and management
- Still need better and secure routing protocols to handle multi-hop networks and other issues unique to WMNs
- Performance management is very important from administrative prospective because through proper management an administrator can overcome on many threats.
- Neighbor monitoring to avoid from malicious attacks
- Protect the privacy of Users as the position of user can easily be determined
References


Security in Wireless Mesh Networks


[14] Puttipong Mahasukhon, Michael Hempel, Song Ci, Hamid Sharif “’Comparison of Throughput Performance for the IEEE 802.11a and 802.11g Networks’”.


