Abstract: - Wireless Mesh Networks (WMNs) are the next step in the evaluation of wireless architecture, delivering services for a large variety of applications in personal, enterprise, campus and metropolitan areas. They can be considered as hybrid between wireless infrastructure (WLAN) and ad-hoc networks (MANET), with mesh points providing flexibility in building & expanding the network, allowing automatic discovery of neighboring nodes, increased reliability and redundancy. In this paper we discuss as to how WMNs can be practically deployed to support wireless multihop communications in a campus-wide area. To this aim, we have deployed a real WMN at PEC University of Technology campus utilizing state-of-the-art technology and analyzed the performance of this architecture when supporting multihop heterogeneous traffic. Currently the network is being used to provide services to the residential areas of the campus.

Keywords: - Wireless Mesh Network; testbed; IEEE 802.11s draft; performance evaluation

I. INTRODUCTION

Unlike WLAN, mesh networks are self-configuring systems where each Mesh Point (MP) can relay messages on behalf of others, thus increasing the communication range and available bandwidth. In WLAN, the wireless AP has to be wired to the infrastructure, whereas in WMNs MPs can be connected to the rest of the network by wireless radio links only. WMNs are easy to install, require no cable cost, connections amongst nodes are automatic, offer network flexibility, discovery of newly added nodes, redundancy, and self healing reliability. WMNs are important for distributed applications that cannot rely on a fixed infrastructure, but require instant deployment, dynamism, self-configuration and self-organization [3, 6].

However to explore the full potential and limitations of this new technology, we have deployed a realtime testbed for multi-hop WMNs using the Orinoco mesh creation protocol (OMCP) which is the part of Orinoco 4000MR-LR mesh device. The main contribution of this paper is reporting our experiences of deploying a real Wireless Mesh Network which is used as a testbed for validation of experimental results and is also used to offer services to campus residents.

II. INFRASTRUCTURE OF WIRELESS MESH NETWORKS

Wireless mesh network are able to extend the network without any infrastructure by using the multihop wireless connections between AP’s. Various types of nodes used in WMN are described as follows:

A. Mesh Point (MP):- MP which provides mesh services, can be a dedicated infrastructure device enabled to fully participate in the network. It can relay messages in ad-hoc fashion on behalf of other MPs to create a self-configuring system that extends the coverage range and increase the available bandwidth.

B. Mesh Access point (MAP):- A special type of MP which provides the AP services in addition to mesh services provided by MPs.

C. Mesh Portal Point (MPP):- A special MP that serves as a gateway to a wired network, it supports transparent bridging, address learning and bridge-to-bridge communication.
D. Station (STA):- STA is totally mobile user device and does not participate in mesh services; it communicates with other stations via an AP, a MAP, or an MPP.

WMNs may connect to the internet via MPP and MPs work as wireless bridges within WMN. They facilitate the connectivity and intercommunication of wireless clients through multihop wireless paths. MPs in WMNs are often stationary and not power-constrained, thus freeing routing protocols from the burden of dealing with mobility and power constraints [2].

A peculiar feature of WMNs is that, if the source and the destination are not in the same Basis Service Set (BSS) domain, the source MAP does not forward packets to all the MAPs in the Extended Service Set (ESS), instead the packets are sent via MPs to reach the destination.

III. RELATED WORK

1. University of California, Santa Barbara Mesh Testbed [1] is an experimental wireless mesh network consisting of nodes equipped with multiple IEEE802.11a/b/g wireless radios and distributed on various floors of a campus building. The aim of this testbed is to test new protocols supporting robustness in multihop wireless networks.

2. The Broadband and Wireless network (BWN) lab at Georgia institute of Technology [7, 8] has recently built a WMN testbed. The testbed includes 15 IEEE802.11b/g based mesh routers, some of which are connected to the internet. The testbed is distributed among various rooms on a single floor and laptops are used as mobile stations. The aim of this WMN testbed is to investigate the effects of inter-router distance, backhaul placement, and clustering. Recent research has been devoted to study adaptive protocols for transport layer, routing and MAC layers, and their cross-layer design.

3. MAP at Purdue is an experimental WMN testbed[7] composed of several nodes capable of running in both 802.11a and 802.11b/g mode. Purpose of this testbed is to study routing problems and solutions to create high throughput routes.

4. A general purpose WMN testbed using Intel IXP425 series Xscale network processors as routers and iPAQ as clients has been built at Carleton University [4]. Two WLAN network interfaces are installed on the two Mini-PCI slots, one is a Prism 2/2.5 card, which supports IEEE 802.11b, and the other is an Atheros card, which supports IEEE 802.11a/b/g.

IV. NEED AND ANALYSIS OF DEPLOYING WMN IN THE CAMPUS

Prior to the above mentioned testbed, the university had marginal network connectivity to the faculty residential areas. The academic area is fully connected using gigabit wired network. Looking at the architecture of low lying residences and scattered locations around the campus, the only choice available was ADSL connectivity. Wireless connectivity was desirable as most of the faculty members have laptops at homes. Traditional wireless connectivity through Access Points required a wired backbone and placement of switches and laying down of structured cables. It was a challenging task to provide wireless connectivity which did not require lying of cables. The above problem was solved by creating a state of the art wireless mesh network offering a robust, secure and easy connectivity to the above users as the mesh APs can be plugged onto the electrical poles without having any need to stretch Ethernet cables unlike wifi Access Points. The locations of the wireless mesh points were decided after conducting an exhaustive site survey. The Mesh Networking was done using the Orinoco Mesh APs which supports structured Mesh networking. In a Mesh network, mesh access points use their wireless interface as a backhaul to the rest of the network.

Portals are connected directly to the wired infrastructure are while Mesh Points relay packets to other Mesh Points to reach the Portal, dynamically determining the best route over multiple hops to follow their characteristic of being self-configuring and self-healing. The Mesh APs use the ORiNOCO Mesh Creation Protocol (OMCP) for creating wireless mesh network. The formation of a Proxim ORiNOCO mesh network begins as soon as the Wi-Fi cell is turned on. Wi-Fi cells cannot sense that they have a direct network
connection and hence begin an automatic discovery process.

Secure links to the other mesh APs are created using secure AES encryption and authentication which was enabled as a part of deployment. OMCP then determines the most efficient path through the mesh, taking into account the traffic load, link speed, signal strength, number of hops and other parameters. Based on this calculation, specific routes from each mesh AP to mesh portal APs are set up. In addition to serving as an experimental testbed, the university’s wireless mesh network is also being used for providing wireless connectivity to the residential areas of faculty of the campus. Such a mesh can also be replicated for other solutions such as wireless video surveillance in nearby cities, WISPs, and city-wide wireless networks. Another objective of the deployment was to be able to deploy a secure wireless testbed which offers mutual authentication at the level of user as well as mesh points with 128 bit AES encryption of data so that the services offered through the WMN are secure and reliable. This deployment helped us in building a prototype for designing and deploying secure wireless mesh networks which can span over entire city and can be utilized for making it application oriented suitably.

V. ARCHITECTURAL DESIGN OF WIRELESS MESH NETWORK

In this section, we describe the main devices used for setting up our testbed and motivate our choice. We have used the ORiNOCO 4000MR-LR mesh AP’s for the deployment of the wireless mesh network, and also used the centralized authentication system i.e. RADIUS which is integrated with the Active directory. While active directory is not themselves an authentication system, it is used as centralized account storage mechanism.

The ORiNOCO 4000MR-LR mesh AP’s uses the ORiNOCO Mesh Creation Protocol (OMCP) that allows creation of self-forming and self-healing nonline of sight mesh networks.

Figure 1: WMN Network Architecture

Figure 1 shows the view of our network setup. A total of six mesh capable devices including MPs and MPP are part of our wireless mesh network. Amongst them there one mesh portal has been configured and the rest five are configured as mesh AP’s. The mesh portal is connected to the internet through radius server. In our case Mesh portal is capable to act as both a portal as well as a mesh point. A large number of clients get connected to the mesh portal as well as mesh AP’s for accessing internet services.

Salient characteristics of Proxim’s mesh products include: a dual-radio configuration, increasing system capacity by allowing one radio to focus on Wi-Fi access and the other radio to perform mesh backhaul duties; Quality of Service (QoS) enabling voice and video capability; and enterprise-class security features. If a mesh link becomes obstructed, client traffic is dynamically re-routed, ensuring uninterrupted video streams and voice calls. Other interesting features of the Proxim Orinoco mesh points which were considered are simultaneous 802.11b, 802.11g & 802.11a support, IEEE 802.1x and 128-bit AES support for authentication and encryption methods including mutual authentication, message integrity check, per packet keys initialization vector hashing and broadcast key rotation, detection of alerts and unauthorized rogue access points and clients in both the 2.4 GHz and 5 GHz bands, automatically receiving correct configuration by new AP’s and preventing security vulnerabilities with deliberate
resets, extensive RADIUS accounting support, intra cell blocking to prevent client to client snooping, multiple VLAN support with different security modes and SNMPv3 and SSL support to protect against unauthorized AP changes by the management interface.

In the next section we report the process of getting authenticated and hence connected to the WMN. As per the WMN topology represented in the Figure 1 the working of wireless mesh network given below:-

1. Wireless Client PC sends Access-request to the Mesh AP
2. The Mesh AP which is configured to use RADIUS as the authentication, authorization, and accounting protocol and receive Access-request of client.
3. The Mesh AP creates an Access-Request message and sends it to the Mesh Portal.
5. The Radius server evaluates the Access-Request message.
6. If required, the Radius server sends an Access-Challenge message to the Mesh Portal. The Mesh Portal processes the challenge and sends an updated Access-Request to the Radius server.
7. The user credentials are checked and the dial-in properties of the user account are obtained by using a secure connection to a domain controller.
8. If the Credentials are verified by the Domain Controller, then Radius server allows the user to connect.
9. After the successful connection the clients able to access the Internet.

VI. WMN TESTBED DEVELOPMENT

In this section we describe the real time deployment which also acts as a secure testbed; both for offering services and also for conduct of experiments. We have build WMN testbed at PEC University of Technology campus, under the Cyber Security Research Center, Chandigarh. The google map of residential area of the campus in Figure 2 shows the actual positioning of mesh devices.

![Figure 2: Positioning of Mesh Devices in testbed map](image)

The areas marked with red line in Figure 2 indicate the areas of interest where there was no connectivity existing. The total area covered by the current WMN spans over 1000x700 sq mts. Shaded triangles in the figure above depict the position of the mesh points. The white rectangle depicts the position of the mesh portal. The location of the mesh portal was chosen based upon the last mile wired connectivity that was available in the campus. Beyond this point wired connectivity did not exist in any form.

The mesh points on the mesh backbone are operating on 5 GHz, 8dBi, while the clients are communicating with the mesh AP’s on 2.4GHz, 8 dBi. The mesh backbone is implemented using 5GHz radio’s that is mounted on ORINOCO Mesh AP’s, where as clients may be any wireless device such as laptop etc. The rationale behind this choice is that of keeping these two frequencies far from each other so as to prevent the interference that could affect the performance of the network. Distance between the mesh AP’s have been chosen such that the neighboring mesh AP’s can get better connectivity with each other so as to maintain mesh backbone. Figure 3 shows the pictures of the actual mesh points and the mesh portal being deployed in the network. All the MPs and MPP have been weather protected to provide protection against the climatic changes. Since the power supply already existed in the
form of street light poles and hence the existing light poles were being used for ease of installation.

VII. THE WMN TESTBED IN ACTION

In this section we report on preliminary experimental outcomes achieved through our WMN testbed. The purpose of these experiments is to assess the functioning of our test bed and to evaluate the performance. We used the Netstumbler[9] tool running on a Linux laptop equipped with a wireless IEEE 802.11g based PCI card to take signal strength measurements at various locations around the campus. The measured SNR values (in dB) are shown in the figure 4. The SNR values show satisfactory results and hence justify the location of mesh points in WMN and hence the overall architecture. This also results in overall user satisfaction while accessing Internet through the Wireless Mesh Network.

We conducted another experiment to measure the time taken to download a file when a client was accessing the network through different hops. In our experiment, we run a single download session over wireless mesh network, varying the number of hops that a packet has to transverse from the source to the desired destination; the client has to download the 4.91 MB file. The Mesh devices were positioned as depicted in the figure 1 whereas the position of the client were made to vary on the basis of different hops.

When the client was directly connecting to a Mesh portal, it was considered to be operating through a single hop network. The client was then moved in such a way that it would connect to different mesh points to enable us to measure the performance at each hop.
The time taken from each hop was measured and the results of the experiment are shown in Figure 5 which depicts that the time taken to download the file increases linearly with the number of hops of flow transversal. This is not surprising and indicates that our test bed is performing correctly; it is well known in the scientific literature that the available data rate for the TCP-based flows decreases for each wireless hop until it reaches a point where it is no more in a position to support any application.

VIII. CONCLUSION

In this paper, we have reported our experiences while deploying real wireless multihop testbed utilizing WMN technology based on the ORINOCO AP’s. Based upon the results presented in this paper, we claim that today’s WMN technology is promising even if the performance quickly deteriorates when increasing the number of wireless hops between the source and the destination. A wise design of the network architecture that limits the number if consecutive wireless hops may generate a WMN which can satisfy the user’s needs. Such a deployment clearly shows that the WMN has a huge potential in being able to rapidly deploy the network services without incurring high costs and laying down of cables.

Moreover, besides serving as means to test and refine the practical applicability of wireless mesh network, the testbed also allows us to study many practical issues that inspired us to take future directions for this work.

IX. ACKNOWLEDGMENTS

This work is done in Cyber Security Research Center (CSRC) located at PEC University of Technology. The authors would like to thank Government of India, Ministry of Communications and Information Technology, Department of Information Technology, New Delhi, for funding the Project “Design and Development of Dependable, Secure and Efficient Protocol for Wireless Mesh Network (WMN)”, under which this research work has been done.

X. REFERENCES