WIRELESS MESH NETWORK: AN ENABLING TECHNOLOGY

Abhishek Kumar Gupta*

Princi Chauhan*

Amit Kumar Chauhan*

Abstract:

Wireless Mesh Network is the enabling technology and is the right solution for metropolitan area networks; the network has number of attractive qualities like the network has low cost deployment, robustness and has comparatively stable form. The number of research being conducted in the field of wireless mesh design, security, QoS. In this paper we describe the possible architecture for Wireless Mesh Network with its challenges and applications to present day communication. Further we present you with routing methods and security issues related to wireless mesh network. In the later section QoS challenges and pitfalls in WMN is presented.

Keywords: Wireless Mesh Networks, Routing, Security, QoS.

* Department of Computer Science, Deparment of Electronics, Phonics School of Engineering, Roorkee

I. INTRODUCTION

Wireless communication is a desirable service in the present day scenario and is showing tremendous growth in both cellular as well as wireless local area network (based on IEEE 802.11 standards marketed under Wi-Fi brand name).These two technologies have a narrow range of connectivity but are showing number of applications in the wireless field. Cellular Networks [1] offers a wide coverage area, since the service is very expensive and offers low data rates, So attention is now focused on higher data-rate packet services for cellular systems. Although many packet multiple access schemes have been studied over the years, researchers have often studied single cell performance and ignored reuse. Moreover, direct sequence spread spectrum (DSSS) has been considered unsuitable for high data-rate packet multiple accesses since spreading limits the permitted data rates, DSSS requires large overhead (preambles) for acquisition and requires closed-loop power control.

As far as the Wireless LAN is concerned they provide better data rates than cellular networks (>80 Mbps according for 802.11ac in 2011), in spite of better data rates this service is suffering from limited coverage area.

The solution to Wireless LAN is Wireless Metropolitan Area Network (based on 802.16 marketed under Wi-Max services)[2] that offers high data rates with larger coverage area. But this service is also suffering from large number of drawbacks. One of the major problems is the Line of Sight (LOS) problem which occurs due to high density of obstruction (high buildings and trees), Also this service is complex and expensive.

Wireless mesh architecture is a first step towards providing cost effective and dynamic high-bandwidth networks over a specific coverage area, Wireless mesh network is the door step towards the next generation services, for both fixed and

mobile users. We will discuss wireless mesh network as a

whole, in the next section i.e. section II we discuss the architecture of WMN, thereafter we will discuss the protocols related to WMN, this section security related information will be explained, Later on we will also present the problems that need to be solved to produce a high performance, secure and reliable WMN.

II.OVERVIEW TO WIRELESS MESH NETWORKING ARCHITECTURE

Wireless mesh network is showing rapid progress and inspiring numerous applications. The driving force in the development of wireless mesh network comes from advantages like coverage, robustness, self configuration, easy maintenance and low cost. In this section we will discuss the architecture of WMN. The architecture of WMNs can be classified into three main groups based on the functionality of the nodes: Client Mesh, Infrastructure, and hybrid mesh [3]. This classification is shown in fig.1 the lower-tier in the architecture diagram corresponds to the client mesh architecture which provides peer-to-peer ad-hoc connections among the mesh clients. This is also referred to as pure mesh, where most of the traffic is classified as intra-mesh traffic. In contrast, the infrastructure mesh architecture is portrayed at the middle-tier where mesh routers form a backbone infrastructure of self-healing, self-configuring links among themselves, for clients that connect to them. Finally, the architecture as a whole represents the hybrid mesh architecture, where mesh clients can connect to the service platform through mesh routers as well as directly meshing with other mesh clients (assuming that the mesh clients can be directly connected to the service platform). The traffic flows and hence the appropriate architecture depends on whether the content to be accessed is inside or outside the mesh. Thus, the type of mesh architecture required in a given situation is driven by the user and application needs for content.

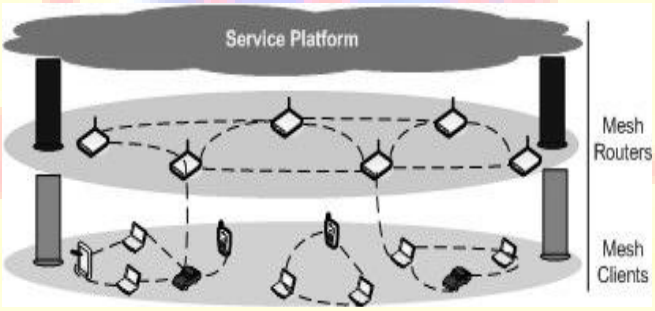

Fig 1: Architecture of Wireless Mesh Network

As already discussed WMN consists of mesh clients and mesh routers. . Compared with a conventional wireless router, a wireless mesh router can achieve the same coverage with much lower transmission power through multi-hop communications. In addition, mesh clients have only one wireless interface. Various examples of mesh clients are laptop/desktop PC, pocket PC,

PDA, IP phone, RFID reader, BACnet (building automation and control networks) controller, and many other devices.

III. CHARACTERISTICS AND APPLICATIONS OF WMN

The characteristics of wireless mesh network are as follows:

1. In order to provide the non line-of-sight connectivity to the users the mesh-style multi-hopping is used, which achieves higher throughput without sacrificing with the radio range via shorter link distances, also provides less interference between the nodes, and more efficient in frequency re-use.
2. Multi-radio and multi channel capabilities of WMN provide an opportunity to achieve high throughput.
3. Mesh routers usually do not have strict constraints on power consumption. But mesh clients put constraints on power consumption and for this reason mesh clients require power efficient protocols.
4. WMN is compatible and interoperable with the existing wireless network.
5. As WMN is a flexible network so we can say that it supports ad-hoc networking. The network have low upfront investment requirement, and the network can grow gradually as needed.

Applications of WMN:

1. It constructs a wireless backhaul rapidly by using the mesh network in the areas that are not easy to wire.
2. To satisfy non-interrupted operation environment, use of mesh network is suggested to build a backup network.
3. Compared to Peer-to-Peer Bridge, the application of wireless mesh network provides more flexibility especially when used for multi hop networks.
4. Instead of limiting IEEE 802.11 or 802.16 accesses to station and stops, mesh networking technology has extended its access to buses, ferries and trains.
5. In addition to above applications, WMN can also be applied to Security surveillance systems, Health and Medical systems, building automation.

IV. RESOURCE MANAGEMENT CHALLENGES: AN OVERVIEW

This management in WMN basically covers three main areas:

1. Network Configuration and Deployment: As the network involves wireless hubs, access points (APs) and these APs are in turn connected to backhaul, so this is the main challenge in initial infrastructure which involves the appropriate placement of nodes like APs and routers.

2. Routing: Routing in WMN involves network connectivity to the end users through various ways. Routing can be classified based on two types: topology based routing and position based routing. This ultimately should be done with proper optimization and utilization of network resources.

3. Mobility Management: For this management there should be efficient hand-off management and location management mechanisms. Routing is tightly coupled with mobility in ad-hoc networks; So WMN has to consider both the aspects.

V. ROUTING

Routing [4] is the process of determining the end-to-end path between a source node and destination node.WMN exhibit unique characteristics that differentiate it from existing wireless networks, and for this reason the existing protocols must be revised to make them adaptive to WMN. There are many fields that need to be taken care of while designing a WMN network: Network Topology, Traffic Pattern, Inter path interference, Link capacity and Channel diversity. Routing Protocols can be broadly classified based on four criteria: Routing Philosophy, Network Organization, Location Awareness and Mobility Management.

There are number of protocols designed for existing wireless networks but very few protocols have been designed for WMN. MIT (SrcRR [5]) and Mesh Networks (Mesh Network scalable Routing [6]) designed new protocols for WMN.

VI. CLASSIFICATION OF ROUTING PROTOCOL

Routing Protocol [10] for WMN are mostly based on protocols designed for ad-hoc networks. These are classified into three categories: Proactive Routing Protocols, Reactive Routing Protocols and Hybrid Routing Protocol.

Proactive Routing Protocol: These protocols maintain the table for each node representing the entire network topology which is regularly updated in order to maintain the freshness of routing information. In this technique each node knows how to reach the other node of the network. The main advantage of these protocols is that they minimizes the delay at the cost of exchanging data periodically but also at the same time the approach consumes network bandwidth, these protocols are suitable for small networks. Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing Protocol (OSLR), Open Shortest path first- MANET (OSPF-MANET) are some of the examples of Proactive Routing Protocols.

Reactive Routing Protocol: In this technique the nodes are not aware of the network topology; the routing table is constructed on demand. These protocols are better suited for the networks with low node density and static traffic patterns. These protocols leads to high latency due to the fact that route has to be discovered. Dynamic Source Networks (DSR), Ad-hoc On-demand Vector (AODV) are some of the reactive routing protocols.

Hybrid Routing Protocols: These protocols are the mixed design of the two protocols. If WMN is segmented into clusters .Within each cluster a proactive algorithm is used whereas between clusters a reactive algorithm is used.

Various other protocols are HWMP, BABEL, BATMAN, and SHWMP.

AODV work very well in Wireless Mesh Networks with small traffic load. As the traffic load increases AODV protocol is not scalable. In multi-hop ad hoc networks the overhead of routing protocol has the largest impact on throughput. Babel provides higher throughput in smaller networks, however it has to be tested in large networks. SHWMP is proposed Hybrid Wireless mesh network protocol.

VII. WMN DESIGN PROBLEMS

The nature and impact of interference is highly in predictable which challenges the design of all upper layer protocols. Various ways have been proposed to model [9] the impact of interference out of which some is discussed here:

1. Protocol Interference Model: Communication between nodes u and v results in collision free data reception at node v if no other node within a certain interference range from v is transmitting simultaneously.

2. Physical Interference Model: Communication between nodes u and v results in collision free data reception at node v if SINR (Signal to Interference and Noise Ratio) at node v is above certain threshold.

3. K-hpo Interference Model: No two links within K hops distance from each other can successfully transmit at the same time.

Modeling link quality, capacity and the effect of interference can be extremely difficult task as the wireless environment is a complex combination of so many parameters. Researchers have proposed to rely on actual measurements to capture the effects of interference.

VIIII. SECURITY

Many approaches have derived from ad-hoc security research [8] but the future mesh products will standardize security through the 802.11s. Ad-hoc networks (often called Mobile Ad-Hoc Networks or MANETs) are the evolutionary basis of mesh networking technology that forms the basis of fixed wireless mesh networks. Threat models for ad-hoc networks raised concerns about hackers being able to directly attack the network, inject erroneous messages, or impersonate a mesh node. The most prevalent on-demand and link-state routing algorithms do not specify a scheme to protect data or sensitive routing information. This is mainly because any centralized entity could lead to significant vulnerability, where the security solution envisioned for ad-hoc must be based on the principle of distributed trust. There are many different methods within the ad-hoc security research community to address authentication and communication protection in ad-hoc networks. Adhoc security research strives to resolve security issues related to trust in a

dynamic and arbitrary assembly of nodes, where nodes many originate from different trust realms.

Lack of security is a serious issue, and lays waste to all efforts expended in providing QoS. The IEEE 802.16 standard specifies a security sub layer which is responsible for enabling per-link encryption and security mechanism.

However, some of the concepts from ad-hoc network security provide insights into key technologies for mesh network security, where some of them are summarized below:

1. Message integrity protection using public/private key security, including transitive trust architectures, between routing peers.
2. Message authentication using hash chains to ensure detect tampering of routing information within the network;
3. Authentication of routing messages using digital certificates;
4. Protection by symmetric cryptography, using shared secrets or digital signatures.

By concentrating on protection against external attackers the authentication and key management overhead could be significantly reduced. This allows WMNSec to be deployed in scenarios where interruption-free connectivity and mobility are required, e.g. tele-operation of mobile robots. Still WMNSec relies on the secure mechanisms introduced by 802.11i the 4-Way-Handshake and the periodic update of the used cryptographic keys. The main restriction compared to 802.11i is that there is no protection against attackers with insider knowledge (i.e. participants of the WMN). While this has some relevance in roof-net WMNs, it is not an issue in centrally organized industrial networks. In future work WMNSec will be evaluated using a larger scale WMN test bed with 30-40 stations. Additionally it can be evaluated using client certificates issued for every station to verify the upper layer authentication support. WMNSec is however only one of the aspects covered in the ongoing work on reliable and dependable Wireless Mesh Networks. Other elements will ensure wireless network coverage, prevent overloads of the network and use more than one wireless channel to increase the redundancy.

IX. QOS CHALLENGES AND PITFALLS IN WMN

The vision to support self-organizing mechanism for network configuration, control and optimization. Supporting a Quality of Service (QoS)[11] to enable a rich portfolio of applications and scenarios is foreseen to be vital for the success of next generation WMN. So the care needs to taken while designing algorithms for supporting QoS on the top of standard's mechanisms.

The current operation towards QoS provisioning in the internet, namely that of over provisioning of bandwidth and other resources is not applicable to WMN. Due to the broadcast nature of wireless medium, wireless network needs to deal with the fundamental issue of interference and noise. So, the bandwidth is the precise resource in wireless networks.

QoS in WMN is supported on packet by packet basis using parts of mesh connection identifier present in each MAC Protocol Data Unit. Here without the loss of generality, we are going to outline the challenges, pitfalls of WMN.

Differentiation of Service, Interworking: To enable various applications, the differentiation of service is crucial. IEEE 802.16 identifies Point to Multipoint mode of operation for the following scheduling services .And also the interworking of the QoS mechanisms with higher layer such as IP needs to be addressed.

End to End QoS Provisioning: A Cross layer approach is needed to make effective use of MAC layer mechanisms when provisioning end to end Qos, so the further work needs to be carried out to analyze the dependencies across layers.

Efficient and Effective Bandwidth Management: When different traffic classes are supported the bandwidth reservation has to adapt to the needs of the applications. In addition concepts such as network coding may be applied to WMN to increase the traffic that can be supported by WMN.

Security Issues: This one is the most challenging issue especially in the open and unplanned WMN and also the issues of dependability need to be addressed.

Mobility and Physical Layer Issues: These issues lead to the complexity of the problem and also emphasize the need for the solution that enables internetworking and compatibility between standards.

X. CONCLUSION

Wireless mesh network has emerged has new promising technology. In this paper we have reviewed the architecture, its characteristics and applications, with this we have also discussed routing and security issues and we came to know that security is a strong challenges to a great extent the commercial deployments of WMN.

There has been a tremendous amount of work is going on the design of wireless mesh networks. Later we proposed the roadmap for the realization of QoS in WMN. The selection of an optimal combination of application and tool is the next step to reach the set goal. The standard's mechanisms need to harness as well. Such an approach is vital for QoS to successfully accomplish the transition from theory to practice in WMN.

Some of more open research issues include efficient MAC design, scalability of the network. Also WMN has the potential to be integrated with other networks like sensor networks, delay tolerance networks; Wi-Max based infrastructure based networks. Further there is great need of research in the fields like link layer and physical layer techniques.

REFERENCES

[1] Kumar, S. High data-rate packet communications for cellular networks using CDMA: algorithms and performance,IEEE Journal & magazine ,MAR1999.

[2] Mihail L.Sichitiu,",Wireless Mesh Networks: Opportunities and challenges".

[3] Hassana Mustaffa ,Usman javaid,Tinku Mohd Rasheed,Sidi Mohd Senouci,Djamal Eddine,"A Panorama on wireless Mesh Network:Architecture,Application, and Technical challenges",

[4] Sonia Waharte, Rouf Bautaba , Youssef Iraqi Brent IshiBeshi, "Routing Protocol in Wireless Mesh Network: Challenges and Design consideration",Precedings published by Springer, 6, July 2006

[5] MITRoofnet. http://www.pdos.lcs.mit.edu/roofnet/

[6] Mesh Networks. http://www.meshnetworks.com

[7] Mijahed Nasser Alijober, R.C.Thool, Atul Negi,"A Sufficient and Scalable Multicast Routing Protocol in Wireless Mesh Network, MeshSPT (shortest Path Tree algorithm for wireless mesh network)",Precedings published by IJCA,7-8,April 2012

[8] A Gerkis, J Purcell,A Survey of Wireless Mesh Networking Security Technology and Threats: Technologies and challenges related to wireless mesh networks, September 2006.

[9] Parth H. Pathak and Rudra Dutta," A survey on Network Design Problems and Joint Design Approaches in WMN", U.S Army Research Office management by NCSU.

[10] Venkat Mohan S, Dr. Kaiwiswanath .N," Routing Protocols for wireless Mesh Networks",Precedinds published by International Journal of Scientific & Research Volume 2, August 2008.

[11] Parag S. Mogre, Mathias Hollik Raif Steinmetz," QoS in wireless Mesh Network: Challenges , Pitfalls, and roadmap to its Realization.