An Optical / Wireless Integrated Approach to provide Multiple Gateways in Wireless Mesh Networks

Muhammad Raheel[1] and M Salman Ashraf[2]

[1]Department of Computer Science
University Of Central Punjab,
Lahore, Pakistan

[2]Department of Computer Science
University Of Central Punjab,
Lahore, Pakistan

Abstract

Wireless Mesh Network is an application technology different from the traditional peer-to-peer wireless bridge; it provides the multi-hop and multi-path connection to form a wireless environment of MESH framework so that the occurrence of single point failure can be prevented.WMNs are to provide high bandwidth broadband service to a large community of users through the use Internet Gateways which acts as a central point of internet attachment for the mesh routers, it is likely to be a potential bottleneck because of its limited wireless link capacity and security considerations of the Internet Gateways .By integrating Optical fiber network technologies with wireless mesh network we can achieve the Security and increase the capacity of the network, in this paper we define integration models with multiple gateways in the access network, which increases the capacity of wireless networks, increase security in network gateways, and decreases access point complexity through centralized management.

Keywords*: WMN's, Multiple Gateways, Hybrid Networks, Access Networks*

1. Introduction

Wireless Mesh Networks (WMNs) represent a good solution to providing wireless Internet connectivity in a sizable geographic area; this new and promising paradigm allows network deployment at a much lower cost than with classic wireless networks.

WMNs are certainly one of the hot topics for research in both academia and industry. Recently, the increased demand for ubiquitous internet connectivity and broadband internet service has spurred the need for new innovative wireless technologies [10].

Although WMNs are based on the well known concept of a mobile ad hoc network (MANET), and thus adopt a self-configurable and self-healing approach[1]. Some key issues such as limited capacity and end-to-end fairness problem pose serious challenges to the wide spread deployment of this technology. In addition to the aforementioned challenges, load balancing of the traffic at the gateway nodes is also another important challenge to be addressed. As WMNs are envisioned to serve a large community of users, the average volume of traffic is significantly higher than in a typical MANET environment. Also, the existing mesh routing protocols do not focus on achieving fair load balancing at the Internet gateways.

The main drawback of WMNs is their complexity: it is relatively easy to design and build a line of products that will form a WMN and will forward packets to and from the destinations; however, it is very difficult to achieve optimum (or near-optimum) performance of this network while ensuring security and robustness. But if we integrate the optical fibers and wireless transmission, the technology is called "fiber-wireless" (Fi-Wi)[9].The advantage of bimodal Fi-Wi systems is that they can enjoy the strengths of both optical and wireless technologies - specifically, the inherently large bandwidth of optical fiber and the large, unused bandwidth in the wireless spectrum. For this reason, a hybrid system has the potential to provide very high data transmission rates with minimal time delay.

By combining the optical fiber and wireless technologies we can provide multiple gateways which will provide efficient load balancing based upon metrics to enhance the overall performance of the system.

2. Related Work

A vast amount of research has been done in FiWi (Optical and Wireless Integration) and designing load balanced routing algorithms for Wireless mesh networks. These existing approaches differ in the security and matric considered for evaluating the network. The proposed routing algorithm in [6] involves selection of a best route at the destination based on the number of queued packets at all the intermediate nodes. The route that has the least number of buffered packets is supposedly the less congested route and thus, such a route can be the best path. The approach followed by the authors in [7] is concerned with the involvement of gateways in the process of load balancing in the network. In one of their proposed schemes, the gateway node coordinates the load balancing in the top part of the network (part of the network comprising of nodes nearest to the gateway) using the number of flows as the load metric. Essentially, they consider a load to be defined as a flow and proceed to balance the number of loads in the network. However, these existing techniques are not directly applicable to WMNs. Due to a large number of nodes connected in a WMN, such algorithms are difficult to realize. Most of these schemes focus on load balancing over the links or intermediate nodes (MRs) connecting to the gateway and do not focus on alleviating the congestion at the gateway and the security of the gateways. Authors in [8] devise a scheme for load balancing over the links that uses path capacity and gateway link capacity as the cost metric. Recent work by Krishna et al [4] suggests that balancing load across gateways is probably more effective than load balancing along the paths. According to their scheme, a better gateway is selected than the current servicing gateway if the RTT for the new gateway is less than the registered one. In [5] authors proposed a system which uses hop count and focused on gateway discovery protocol by which if one gateway is overloaded it sends message to source about the discovery of new gateway which then respond to source and the source uses second gateway. Authors in [2] defined a system uses congestion in gateways which is broadcasted by the intermediate nodes, which receives by the source and then source uses second gateway. Thus, efficient load balancing techniques need to be designed that can be applicable to the WMNs for well-balanced network resource utilization and gateway security so we proposed a new mechanism of multiple gateways by integrating optical and wireless mesh network which provides security and enhances overall network performance.

3. Characteristics of WMNs

WMN is a wireless co-operative communication infrastructure between a numbers of individual wireless Routers. This type of infrastructure is decentralized, relatively inexpensive, and very reliable and resilient, as each node need only transmit as far as the next node. Nodes act as repeaters to transmit data from nearby nodes to peers that are too far away to reach, resulting in a network that can span large distances, especially over rough or difficult terrain.

WMNs are extremely reliable, as each node is connected to several other nodes. If one node drops out of the network, due to hardware failure or any other reason, its neighbors simply find another route. Extra capacity can be installed by simply adding more nodes. Mesh networks may involve either fixed or mobile devices as shown in Figure 1. The principle is simple: data will hop from one device to another until it reaches a given destination. One advantage is that, like a natural load balancing system, the more devices the more bandwidth becomes available. Since this wireless infrastructure has the potential to be much cheaper than the traditional networks, many wireless community network groups are already creating wireless mesh networks.

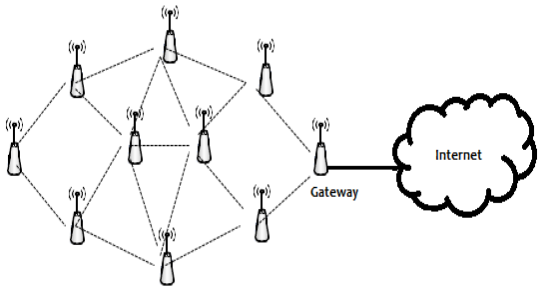


Figure 1

4. Security Issues and Attacks of WMN with single Gateway

WMNs pose challenges in achieving security goals for both mesh routers and mesh gateways. First of all, wireless links in WMN make it prone to active attacks, passive attacks and message distortion [3, 11]. In WMNs, passive attacks would compromise confidentiality and active attacks would result in violating availability, integrity, authentication, and non-repudiation [11].

Secondly, we have the probability of node being compromised due to the lack of physical protection. Hence, the system becomes unprotected to malicious attack from outside of the network as well as attacks launched from within the network.

Thirdly, a WMN may be dynamic because of frequent changes in both its topology and its membership. This ad hoc nature can cause the trust relationship among nodes to change also.

4.1 Vulnerabilities in security

- Physical threat
- Confidentiality and integrity
- Authentication in WMN
- Routing security

4.2 Attacks in WNM:

- Tempering
- Pretending
- Forging
- Analysis on topology and data flow
- Resource duplication attack
- Wormhole attack
- Blackhole attack
- Rushing attack

WMN with single gateway is expected to grow due to easier installation and excellent scalability but as the geographic area of WMN increases, the security related issues also increases.

4.3 Security Issues In WMN:

- Availability

  Availability ensures the survivability of network services despite attacks .As the Network grows the availability of gateway decreases because of network congestion and heavy loads of network traffic.

- Authenticity

  Authenticity enables a node to ensure the identity of the peer node it is communicating with. Without authenticity, an adversary could masquerade a node, thus gaining unauthorized access to resources and sensitive information and interfering with the operation of other nodes.so as network grows authenticity decreases.

- Integrity

  The concept of integrity ensures the transfer of data from sender to receiver. Integrity guarantee that a message sent is the message received, that is, it was not altered either intentionally or unintentionally during transmission. Attack on Integrity is usually done in two ways: by the intentional alteration of the or by the unintentional alteration of the data caused by operator input, computer system, or faulty application errors.

- Confidentiality

  The concept of confidentiality is the assurance that sensitive data is being accessed and viewed only by those who are authorized to see it. So the aim would be to protect data from breaches of unauthorized persons and to reduce the damage that would be done to the organization by such breaches.

4.4 Performance Issues in WMN

- Throughput
- Connectivity
- Scalability
- Radio Techniques
- Compatibility
- Security

5. Network Integration in WMN:

The security issues related to WMN can be removed by providing multiple gateways in the Architecture of WMN, which reduces the security risks and complexity of the whole network.

We proposed Four different Network Integration Techniques with multiple gateways to enhance network performance and reduce congestion in overall network. Our Architectures can be implemented in both small and large scale WMNs.

In our network architectures the WMN network is integrated with Optical fiber by using Optical/Wireless Integration Technique[9] FiWi, by which we can achieve the strengths of both optical and wireless technologies - specifically, the large bandwidth of optical fiber.

Fiber-wireless (Fi-Wi) to provide ultra-high-speed, short-range communication, By combining the capacity of Optical Fiber networks with the advantages of wireless networks, FiWi networks form a powerful platform for the support and creation of emerging future applications and services.

Characteristics of FiWi networks:

- Architecture
- Re-configurability
- Load balancing
- Cost-efficiency and Migration
- User-friendliness

There are two classifications of FiWi these are:

1. Radio-and-Fiber :

In Radio and Fiber classification Protocol translation might be done at the interface of optical and wireless segments by an appropriate optical-wireless device, such as Optical Network (ONU), or at the optical part, e.g., by an Optical Line Terminal (OLT).

2. Radio-over-Fiber :

In Radio Over Fiber classification the required protocol translation is done in the optical part by an appropriate optical element, e.g., OLT.

Optical/Wireless integration is use to provide two different types of WMNs. These are:

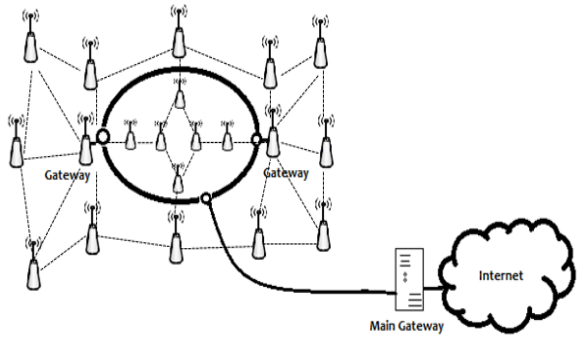
1. Small Scale WMN with Multiple gateways.
2. Large scale WMN with multiple gateways.

5.1 Small Scale WMN with Multiple gateways:

These small scale WMNs are implemented to provide high speed internet connections in small geographic areas.

1. Central Optical Ring with Multiple Gateways

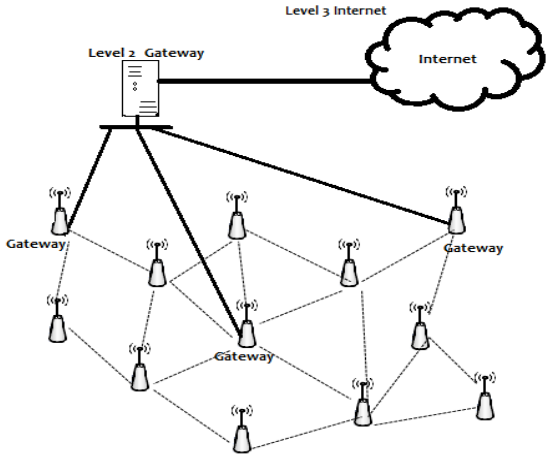
In our first Architecture we use the Optical ring technology to attach multiple gateways together and then to our main internet distribution center as in Figure 2.



As we know that in WMN all the Mesh Routers are connected to their adjacent Mesh Routers and because of such architecture there is a lot of congestion in the middle part of the WMN. So to reduce the network congestion in the middle of the network we provide a Ring Architecture using Optical Fiber. All the gateways are attached to a ring network , gateways are distributed in the middle part where there are heavy loads of network traffic and ring is created by the optical/wireless FiWi technology and all the nodes(gateways) using the ring are then connected to Main Gateway which is use to distribute internet to the WMN.

2. Hierarchical Architecture with Multiple gateways

In our Second Architecture we use the Hierarchical network model to attach multiple gateways together and then to our main internet gateway as in Figure 3.



All the Gateways are connected to each other in the hierarchical manner and are at level 2 of the network model. All the Mesh Routers are connected to the distributed gateways at level 1 and at the top level (Level 3) all the gateways (Level 2 Gateways) connected to central gateway which is then connected to Internet.

In this architecture at level 1 we can deploy the Gateways according to the analysis of data traffic load of the WMN. At level 2 we can provide multiple Level 2 gateways to manage the load of the overall network.

5.2 Large scale WMN with Multiple Gateways:

In large scale WMNs we need such architectures which are scalable and the gateways are distributed in such manner that they can provide high speed access all over the network.

1. Multi-Area Gateway Architecture:

Our first architecture in large scale WMN is scalable network model with multiple gateways in such a manner as depicted in Figure 4.

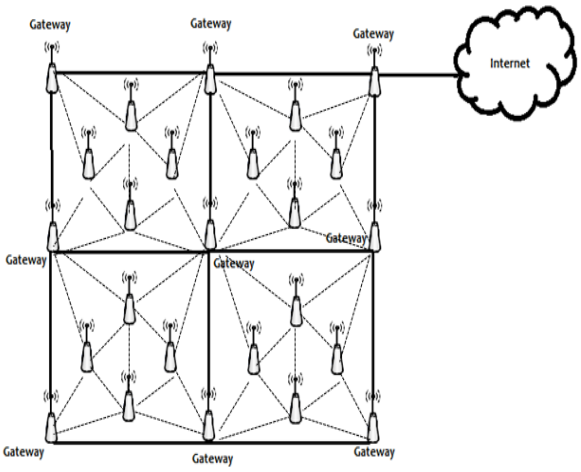


Figure 5

This is network model which is scalable and can be applied over large geographic area, the Mesh routers are connected to the gateways of there own area and then these gateways are connected to other gateways of different areas, creating a scalable architecture. We can grow this architecture according to our geographic need. All the gateways are connected to each other using optical fiber and there are redundant paths available to each gateway to send data out of the network.

2. Gateway to Gateway Architecture:

Our Second architecture in large scale WMN, we distribute multiple gateways as shown in Figure-5.

In this architecture there is a gateway to gateway communication, one gateway pass the data to next gateway and then to next gateway to put the data out of the network. All the Mesh routers are also connected to the gateways according to the hop count value to their adjacent Gateways. So because of that the load is balanced evenly to the Gateways. We can scale this network as depicted in Figure 5 we provide more

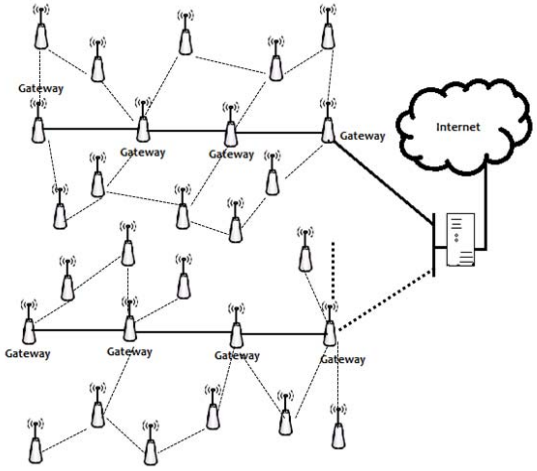


Figure 5

gateway to gateway links and connect them to the main internet provider gateway.

6. Proposed Gateway Switching Protocol for Network Integration Model:

The proposed scheme is divided into three phases.

1. Gateway Availability and Authentication
2. Creating Gateway List in Mesh Routers
3. Secured Transfer of Load from One Gateway to Another

In First Phase gateways are authenticated by the

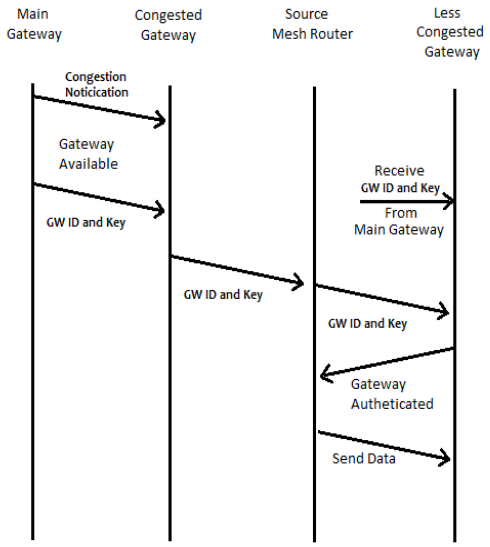


Figure 6

```
At Main Gateway
If Gateway Traffic Load > Max Threshold then
New  Gatewav=Check for Available Gateway
        If New_GATEWAY=TRUE  then
        Send GW_ID and Key to ( Gatewav AND New_GATEWAY )
        End If
End IF
At Congested Gateway
If GW_ID and Key then
Send GWID and Key to Source Mesh Router
End If
At New Gateway
If Receive GW_ID and Key From Main Gateway then
GWID and Key = REC_GW_ID and REC  Key (Received and Stored)
Authenticate (Accept Data from Source)
End If
At Source Mesh Router
If Receive GW_ID and Key From Connected Gateway then
New  GW=GW_ID
Send GW_ID and Key to New  GW
Authentication Accepted
UPDATE Gateway LIST
Transfer DATA
End If
```

Figure 7: Gateway Switching Algorithm

main gateway by using the gateway id and authentication key stored in main gateway and WMNs gateways. All the communication is done on optical Fiber Link. Main gateway is also responsible for maintaining the trust relationship between gateways by maintaining the gateway list. It also check the traffic load on each gateway periodically and creates a threshold limit table for each gateway.

After Authentication the gateways send small packets periodically into WMN for their presence in the WMN. And all the mesh routers create the list of gateways by using the hop count as the matric for creating gateway availability list. As the mesh router receive periodic packets from Gateways they Update their list periodically.

From that on all the Mesh Routers associate with its gateways and send data to them. If one gateway is down then the mesh router uses other gateway from the list.

The Main Gateway Server Also periodically checks the availability of the Gateways and also checks the Load on Each gateway. As the traffic Load reaches the threshold limit of the gateway then the main gateway sends the congested gateway the gateway id of the available lesser load gateway and also sends the authentication key to the congested gateway. This Key is also transferred to the lesser load gateway.

As the congested gateway receive the key and gateway id it sends them to the corresponding mesh router which works as the notification for the mesh router about the congested gateway. The mesh router then uses the same gateway id and the key to verify the lesser congested gateway and after verification uses the second gateway to send data out of the network. The transfer of load from one gateway to another is done by sending the unicast messages between congested gateway, WMR and the lesser congested gateway.

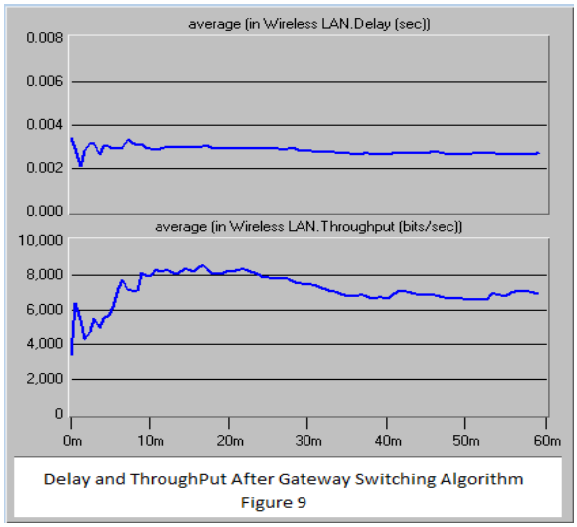
7. Performance Analysis:

We used OPNET [12] simulator to simulate our proposed Scheme. We run the simulations for duration of 60m. We have used the network model as in Figure 3.

Clients under multiple Mesh Routers generate traffic at different time 10, 20 and 30 minutes at the rate of 2048, 2048 and 2048 Kbps respectively. The packet size was set to 1024 bytes. We use IEEE 802.11 as the underlying MAC protocol.

In Figure 8 all the mesh routers connected to single gateway. After 20 minutes as the load increases the overall throughput decreases and the delay also increases.

After Gateway Switching Protocol as depicted in the Figure 9 after 20 minutes as the load increases the



Delay and ThroughPut After Gateway Switching Algorithm
Figure 9

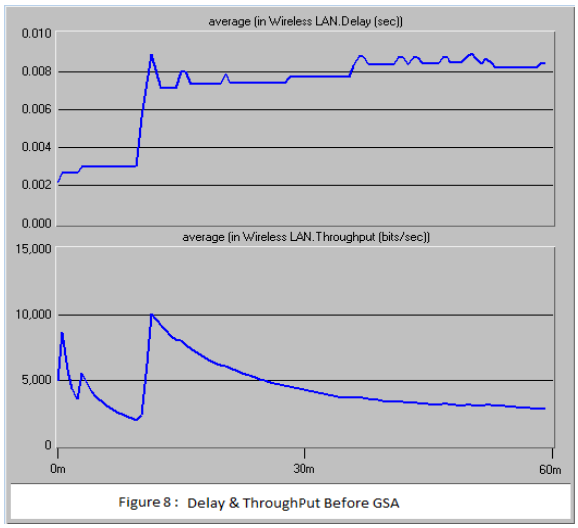


Figure 8 : Delay & ThroughPut Before GSA

GSP works and the load is shifted to other gateway and the overall delay remains constant and the through put also remains constant.

8. Conclusion and Future Work:

In this paper, we analyze the security concern of Wireless Mesh Network and their possible solutions by integrating WMNs with Optical Fiber technologies. Due to the ad hoc nature of WMNs and power and computational constraints, it is hard to implement the security attributes. But an optical/Wireless integrated solution may be implemented with a tradeoff between security and resource consumption.

In the Future work there are still scope for creating such gateway protocols by which multiple gateways communicate together securely and create trust relationship with each other to provide secure internet communication in WMNs. There is still scope for such protocols by which Mesh Routers can efficiently use the gateways and the network load is equally distributed to the gateways.

9. Acknowledgement:

In writing this Research Paper, I have been fortunate to be assisted by my teacher in many of the sub disciplines that make up the field of Wireless Networks. This Paper could not have been written without their help. I am deeply indebted to the following , who took the time to review my Paper Drafts and, in many cases, to tutor me and help organize My Research Paper in their individual areas of expertise.

Dr.Fareeha Zafar (Department of Computer Science, GC University Lahore, Pakistan)

I am also grateful to my Co-Author who helped me in various drafts of this Research Paper and who contributed his suggestions.

I would especially like to thank Dr.Fareeha Zafar, who throughout this project was a constant source of encouragement, technical expertise, and support of all kinds.

Reference:

[1] D. P. Agrawal, Q. A. Zeng, "Introductionto Wireless and Mobile Systems," textbook
published by Brooks/Cole, 438 pages, August2002, ISBN No. 0534-40851-6, second edition
April 2005, ISBN No. 0-534-49303-3.

[2].Keun-Woo Lim, Young-BaeKo, Sung-Hee Lee, Sangjoon Park,“Congestion-aware Multi-Gateway Routing for Wireless Mesh Video Surveillance Networks”, Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2011.

[3] S. Hansman and R. Hunt, “A Taxonomy of Network and Computer Attacks Computers and Security”, Elsevier, Vol 24, No 1, 2005, pp. 31-43.

[4] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer, and K. Almeroth, "On the Design and Implementation of Infrastructure Mesh Networks", IEEE Workshop on Wireless Mesh
Networks (WiMesh), Santa Clara, CA,September, 2005

[5]. DeeptiNandiraju, Lakshmi Santhanam, NageshNandiraju, Dharma P. Agrawal "Achieving Load Balancing in Wireless Mesh Networks Through Multiple Gateways",Oct. 2006 ,Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference

[6] S.J. Lee and M. Gerla; "Dynamic Load-Aware Routing in Ad hoc Networks"; Proc. of ICC 2001.

[7] P. Hsiao, A. Hwang, H. Kung, D. Vlah; "Load-Balancing Routing for Wireless Access Networks"; Proc. of IEEE INFOCOM 2001.

[8] A Raniwala, Prof Chiueh, "Architecture and Algorithms for an IEEE 802.11-based Multichannel Wireless Mesh Network", in proc of IEEE Infocom 2005.

[9] "Fi-Wi", http://www.zeitgeistlab.ca/doc/Fiber-Wireless-Broadband-Access-Networks.html

[10] "Wireless Technologies", http://www.radio-electronics.com/info/wireless/index.php

[11] William Stallings, "Network Security Essentials", Third Edition, Prentice Hall, July 2006;

[12] OPNET IT Guru Academic Addition , www.opnet.com/university_program/itguru_academic_edition/

Muhammad Raheel is M.Phil. / MS Computer Sciences with Specialization in Computer Networks in the Department of Information Technology at the University of Central Punjab, Lahore, Pakistan.
He has 4-5 Years of Research and Professional Practical experience. His Research interests include Designing and Configuration of Computer Networks, Network Security and Wireless Networks.

Muhammad Salman Ashraf is M.Phil. / MS Computer Sciences with Specialization in Computer Networks in the Department of Information Technology at the University of Central Punjab, Lahore, Pakistan. His Research interests include Network Security, Cryptography and Network Programing.