INSTITUTO SUPERIOR TÉCNICO
Universidade Técnica de Lisboa

Performance Evaluation of a Wireless Mesh Network in a Campus Scenario

Salvatore Messina

Dissertation submitted for obtaining the degree of
Master in Electrical and Computer Engineering

Jury

Supervisor:	Prof. Luís Manuel Correia
President:	Prof. António Topa
Members:	Prof. António Rodrigues
	Prof. Luís Manuel Correia

March 2008

To Titidda & Giacomino

Acknowledgements

I would like to thank Prof. Luís Correia for having supervised this work, driving me from the start to the end of the development of this thesis.

To Lúcio Ferreira, with his advises and his patience, this is also his work.

To GROW people, because without their help OPNET would have been a half labyrinth (and probably without the right path loss propagation model!).

To Prof. Fabio Graziosi that has given the possibility to do this experience and to all my friends in Italy, especially the fantastic “TLC group”, crazy people and one mathematician (crazy by definition).

A special thanks to Rua I de Dezembro people, my local family, to Sanjay, and to my “brother-son-grandson” Andrea. At the end, “tudo correu bem”.

To who has generated me, educated, and believed in me, to them a particular “thanks”.

Abstract

This work was done to analyse the capacity and the performance of a Wireless Mesh Network in a Campus Scenario. The effects of multihop were studied and analysed in two cases. The first one considers a Basic Scenario, to understand the behaviour of a wireless multihop network, when there are only FTP and VoIP services; the second case considers a Campus Scenario with a mix of services of HTTP, FTP, E-mail, and VoIP, to provide a high capacity to each user. The problem is that in this scenario there are a lot of users, and so the network is very loaded. OPNET Modeler was used, which includes a collection of libraries with several devices. The results show that, using a wireless multihop network to cover an area, users with a large hop distance are penalised relatively to users closer to the gateway, in terms of performance. This is a consequence of the fact that the 802.11a and 802.11g standards do not provide a fairness management to network nodes. A conclusion of this work is that, using a Wireless Mesh Network, the throughput can increases 4 times comparatively to WLAN. Unfortunately, in a wireless hop network, fairness problem appears.

Keywords

Wireless Mesh Network; Backhaul; Capacity; Mesh Access Point; Simulation.

Riassunto

Questo lavoro è stato svolto al fine di analizzare le prestazioni di una Wireless Mesh Network in un Campus. Gli effetti del multihop sono stati studiati ed analizzati in due casi. Il primo considera uno scenario Base per capire il comportamento di una rete wireless multihop quando sono presenti FTP e VoIP; il secondo caso considera lo scenario di un Campus con un mix i servizi del tipo HTTP, FTP, E-mail e VoIP dovendo fornire, al contempo, un'alta capacità agli utenti. Il problema di questo scenario è che la presenza di molti utenti carica molto la rete. Come simulatore è stato usato OPNET Modeler, il quale include una collezione di librerie contenenti diversi dispositivi. I risultati mostrano che, usando una rete multihop per coprire una certa area, gli utenti con una grande distanza in termini di hop fruiscono di prestazioni peggiori rispetto agli utenti vicini al gateway. Questa è una conseguenza del fatto che gli standard 802.11 e 802.11b non garantiscono eque prestazioni a tutti i nodi della rete. Tra le conclusioni di questo lavoro si nota che, utilizzando una Wireless Mesh Network, il throughput può aumentare di ben 4 volte rispetto a quello che si otterrebbe usando una WLAN.

Parole-chiave

Wireless Mesh Network; Backhaul; Capacity; Mesh Access Point; Simulazione.

Table of Contents

List of Figures

List of Tables

List of Acronyms

ACK	Acknowledgement
ACs	Access Categories
AIFS	Arbitration Interframe Space
AIFSN	AIFS Number
APs	Access Points
AWPP	Adaptive Wireless Path Protocol
BE	Best Effort
BK	Background
BSS	Basic Service Set
CA	Collision Avoidance
CFP	Contention Free Period
CF-Poll	Contention Free-Poll
CL	Controlled Load
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CW	Contention Window
DCF	Distributed Coordination Function
DCFS	Distributed Coordination Function interframe Space
DNS	Domain Name Server
DSSS	Direct Sequence Spread Spectrum
EDCA	Enhanced DCF Channel Access
EE	Excellent Effort
EIFS	Extended Interframe Space
ESS	Extended Service Set
FCS	Frame Check Sequence
FHSS	Frequency Hopping Spread Spectrum
FTP	File Transfer Protocol
GSM	Global System for Mobile Communications
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
HTTP	HyperText Transfer Protocol
IFS	Interframe Space
IPTV	Internet Protocol Television
IR	Infrared

LoS	Line-of-Sight
MAC	Medium Access Control
MAP	Mesh AP
MP	Mesh Point
MPP	Mesh Portal
MSS	Maximum Segment Size
NC	Network Control
NLoS	Non-Line-of-Sight
OPNET	Optimum Performance Network
PCF	Point Coordination Function
PHY	Physical layer
PIFS	Point Coordination Function interframe Space
QoS	Quality of Service
RTS/CTS	Request-to-Send/Clear-to-Send
RTT	Round-Trip Time
SIFS	Short Interframe Spaces
STD	State Transitions Diagrams
TC	Traffic Classes
TCP	Transmission Control Protocol
TDMA	Time Division Multiplexing Access
TFTP	Trivial File Transfer Protocol
TG	Task Group
TMT	Theoretical Maximum Throughput
TO	Transmit Opportunity
UDP	User Datagram Protocol
UP	User Priority
VI	Video
VO	Voice
VoIP	Voice over IP
WDS	Wireless Distribution System
WiMA	Wi-Mesh Alliance
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WMN	Wireless Mesh Network

List of Symbols

ε	Zero-mean Gaussian distributed random variable
A	Total amount of traffic offered
A_{user}	User Traffic
B	Probability of blocking
CW_{max}	Maximum Contention Window
CW_{min}	Minimum Contention Window
d	Distance
d_0	Reference distance
D_{COtx}	Compression Delay
D_{DATA}	Data dropped
D_{DCrx}	Decompression Delay
D_{DErx}	Decoding Delay
D_{ENtx}	Encoding Delay
D_{MAD}	WLAN Media Access Delay
D_{NET}	Network delay
D_{WLAN}	WLAN Delay
E_{VPD}	Voice Packet End-to-End Delay
f	Frequency
L	Average path loss
L_0	Free space path loss
L_{WLAN}	WLAN Load
n	Path loss exponent
N	Number of resources in the network
N_{calls}	Number of calls per hour
N_{SV}	Number of simultaneous VoIP users
N_u	Average number of user per BSS

N_V	Maximum number of VoIP users
R^2	Correlation coefficient
R_A	Average FTP user throughput
R_{BSS}	BSS data rate
RT	Response Time
RT_{Email}	E-mail Response Time
RT_{FTP}	FTP Response Time
RT_{HTTP}	HTTP Response Time
R_U	FTP user throughput
R_{WDS}	WDS data rate
R_{WLAN}	WLAN Throughput
T_{ACK}	Acknowledge packet period
T_{AIFS}	AIFS period
T_{BO}	Backoff period
T_{call}	Average holding time
T_{MAChdr}	Time taken to transmit a MAC header
TMT	Theoretical Maximum Throughput
T_{PAYpkt}	Time taken to transmit a packet with a particular payload
T_{PHYhdr}	Time taken to transmit a PLPC header
T_{SIFS}	SIFS period
T_t	Time for a successfully transmission between MAPs
x	Payload

List of Programmes

Microsoft Excel 2002	It is an electronic spreadsheet program. It is useful to record, to analyse, and to show information. It is also helpful in computing formulas.
Microsoft Office Visio 2007	Visio is a tool for creating all kind of business diagrams, network layouts, storyboards and site flows, software entity relationship diagram, etc..
Microsoft Visual C++ 6.0	Microsoft Visual C++ is a programming environment used to create computer applications for the Microsoft Windows family of operating systems.
Microsoft Word 2002	Microsoft Word provides powerful tools for creating and sharing professional word processing documents.
OPNET Modeler 14.0	It is a Discrete Event Simulator, which allows the implementation of models using the library of object already done. Several technologies, protocols, and devices, are available to analyse various kind of networks. Several output are available to analyse the results.

Chapter 1

Introduction

In this chapter, a brief overview of this thesis is given. Motivation, state of the art, and the goals of this work are presented. Moreover, the thesis structure is provided at the end of the chapter.

In recent years, there has been an explosive increase in technology. Computers, Internet, and cell phones have become common household words. With this increase in technology, wireless networks have also appeared, which have drastically changed our world. We now have freedom to connect to the Internet almost anywhere and anytime, without the use of a wired link. Wireless networks, as the word implies, do not contain a physical medium to connect, such as wired ones do. Many of the protocols in wireless networks have been taken straight from the ones used in wired networks, with some modifications to make them work with wireless networks.

Short for “wireless fidelity”, Wi-Fi is one of the most popular wireless communications standard in the market. The official name of the standard is IEEE 802.11, provided by the 802.11 Working Group, which was formed in September of 1990. Their goal was to create a Wireless Local Area Network (WLAN) specification that would operate in one of the Industrial, Scientific and Medical (ISM) frequency ranges, the first standard being released in 1997. IEEE expanded the original 802.11 standard in July 1999, creating the 802.11b specification [IEEE03], which supports data rates up to 11 Mbps, comparable to traditional Ethernet. Moreover, this standard uses the same unregulated radio frequency (2.4 GHz) as the original 802.11 one. While 802.11b was in development, IEEE created a second extension to the original 802.11 standard, called 802.11a [IEEE03], which supports data rates up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. In 2002 and 2003, WLAN products supporting a new standard called 802.11g [IEEE03] came to the market, which attempts to combine the best of both 802.11a and 802.11b, supporting data rates up to 54 Mbps, and using the 2.4 GHz frequency for greater range.

Wireless Mesh Networks (WMNs) have received a lot of attention, since they are able to provide reliable and robust wireless broadband service accessibility [HoLe08]. WMNs are predicted to solve some of the limitations, and to improve performance, of others wireless networking methods, such as ad-hoc networks, WLANs, and wireless Personal Area Network. In building a WMN, there is not a huge need of means, and they can be easily expanded, which adds to their popularity. Some applications may include medical systems, military operations, surveillance, emergency disaster, and wireless broadband services access.

A mesh network is a Local Area Network (LAN) that allows for continuous connections and dynamic reconfiguration if a path breaks [AkWW04]. WMNs are part of distributed wireless networks, which are wireless nodes communicating with each other, without any pre-existing infrastructure in place. There is no central administration, so the network does not crash when one node goes down, rather, other nodes just take over for that one. Mesh networking is a subcategory of ad hoc networking, and the main difference between the two is the traffic pattern. In WMNs, almost all traffic flows to and from a gateway connected to Internet, whereas in an ad-hoc network, traffic flows randomly between different pairs of nodes. The nodes in a WMN maintain and establish their own routes. Packets reach their destination by “hopping” from node to node, meaning that each node is not only a host, but also acts as a router. Even though all the protocols that are in place for WMNs use the existing protocols from ad-hoc networks, more work needs to be done on protocols to enable them to work more efficiently on

a WMN, and to allow throughput not to be degraded by multi-hop forwarding and hidden terminals.

An IEEE technical group is working to develop the 802.11s standard for WLAN mesh networking [HoLe08]. At the plenary session, held in feb. 2008, the group announced the baseline document for the standard. The group is defining capabilities in several areas, including topology discovery, path selection and forwarding, channel allocation, traffic management, and network management. The existing 802.11 Media Access Control (MAC) layer is being enhanced to support mesh services. Mesh networking will work with existing 802.11 radio technologies, and mesh services will be compatible with existing WLAN clients. The 802.11s group intends to take advantage of security mechanisms specified in 802.11i, but extensions will be necessary, because 802.11i provides only one-hop link security, and mesh networks require multihop or end-to-end one. Additional work will define how mesh nodes can mutually authenticate themselves and create secure associations. Each node will act as a supplicant and authenticator for adjacent nodes.

Engineering traffic to avoid congestion within a multihop wireless mesh network is a challenge. Local congestion on a mesh node can affect neighbouring nodes using the same channel. Extensions to the Quality of Services (QoS) mechanisms defined in 802.11e are being considered to support hop-by-hop congestion control [IEEE03]. The standards body is also looking at ways to implement rate control to alleviate congestion.

Deploying a mesh network with thousands of nodes requires a scalable and comprehensive centralised network management system, and it must manage bandwidth, security and QoS policies across a network. Planning and designing a network are essential prerequisites for a successful deployment. A mesh network is dynamic in nature, with topology changes happening in real time, hence, monitoring of a network with rapid corrective action becomes critical to deliver performance and reliability.

During network design, it is important to know the capacity and performance that it must ensure. So, it is fundamental to understand how the delay and capacity of the WMN scale with the number of clients and mesh routers. The design of a WMN depends on various factors, such as client density, available budget, required bit rate, and expected traffic pattern. So, it is important to be able to answer questions, like what bit rate will be available to a certain number of clients, if the budget allows an established number of mesh routers with some available channels, or how many clients can be served with a given bit rate, if the budget allows deployment of an established number of mesh routers with a fixed number of available channels over a given area. The goal of this thesis is to characterise the average delay, the maximum achievable throughput, and loss rates in terms of various network parameters. Latency is very important for VoIP, multicast applications, video streaming, and also small HyperText Transfer Protocol (HTTP) transfers, over mesh networks. On the other hand, loss rate affects web access and Transmission Control Protocol (TCP) performance, and can also be used by routing protocols to construct high-quality paths.

To study the capacity and the performance of a WMN, OPNET Modeler 14.0 [OPNE07] was used,

which includes a collection of libraries with several devices. Models of various kinds of networks are provided, as WLANs, which allow to build the WMNs. The devices used in this work are Access Points (APs) with double radio interface, servers, and stations, all provided by libraries.

Two groups of simulations were done, the first dedicated to a Basic Scenario and the second is dedicated to study a Campus Scenario. The first one is useful to understand the behaviour of the network, consisting of a circular area with a radius of more or less 900 m. To cover this area, which contains only one internet gateway situated in its centre, several topologies are used, with various rings. Only two kinds of applications, File Transfer Protocol (FTP) and Voice over IP (VoIP), are chosen. In the Campus Scenario there are four types of available applications: HTTP, FTP, E-mail, and VoIP. In this case, only three topologies were implemented: 2, 3, and 4 rings.

The thesis is structured as follows. Chapter 2 provides an overview of WLANs about general concepts, MAC, and the 802.11e standard. Then, basic concepts of WMNs are described, including the services and scenarios that are possible to implement. Subsequently, Chapter 3 is dedicated to the modelling of WMNs: the state of the art is shown, then, the mains performance parameters are provided, and there is also a description of OPNET. Next, in Chapter 4, the scenarios description is given in detail, together with the results for each scenario and their analysis. Chapter 5 provides some conclusions, and gives some ideas on possible future works.

Chapter 2

Wireless Mesh Networks

This chapter provides an overview of a Wireless Mesh Network, and in particular Mesh WLAN. Initially, it is shown an overview of the IEEE 802.11 WLAN standard, and then it focus on Mesh WLAN, discussing the network architecture, the characteristics and the challenges. At the end of the chapter, the possible scenarios are provided.

2.1 Basic concepts of WLANs

2.1.1 General concepts

Short for “wireless fidelity”, Wi-Fi is one of the most popular wireless communications standard in the market. The 802 standard defines the two lower layers of the OSI model. The 802.11 protocol defines the MAC and the Physical layer (PHY) [IEEE03], the former providing data transfer between the Logical Link Control (LLC) and the physical medium. The protocol division is show in Figure 2.1.

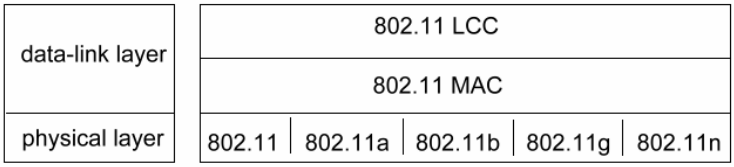


Figure 2.1. OSI layers and the corresponding 802 structure (extracted from [Bagh03]).

There are many different PHY standards in use nowadays. The original 802.11 specification defined three different mechanisms: Infrared (IR), 2.4 GHz Frequency Hopping Spread Spectrum (FHSS), and 2.4 GHz Direct Sequence Spread Spectrum (DSSS). All these mechanisms provide a data rate of 1 or 2 Mbps, depending on the signal quality.

802.11b [IEEE03] supports data rates up to 11 Mbps, comparable to traditional Ethernet. Moreover, this standard uses the same unregulated radio frequency (2.4 GHz) as the original 802.11b one. Vendors often prefer using these frequencies to lower their production costs. Being in unregulated spectrum, it can interfere with other systems, but, by installing 802.11b devices a reasonable distance from other appliances, interference can easily avoided. The advantages of using the 802.11b standard are the low cost and the fact that the signal range is good and not to much obstructed. Disadvantages are the low maximum speed, and, moreover, that home appliances may interfere on the unregulated frequency band.

802.11a [IEEE03] supports data rates up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. This higher frequency, compared to 802.11b, shortens the range of 802.11a networks. The higher frequency also means that 802.1a signals have more difficulty in penetrating walls and other obstructions. 802.11a is usually found in business networks, whereas 802.11b serves better the home market. The pros of 802.11a are a fast maximum speed and the regulated frequencies preventing signal interference from other devices; the cons are a higher cost and the shorter range signal that is more easily obstructed.

802.11g [IEEE03] attempts to combine the best of both 802.11a and 802.11b, supporting data rates up to 54 Mbps, and using the 2.4 GHz frequency for greater range. 802.11g is backwards compatible with 802.11b, meaning that 802.11g Access Points work with 802.11b wireless network adapters and *vice versa*. The fast maximum speed and the fact that the signal range is good, and not easily obstructed, are the mainly advantages; the cons are that this technology costs more than 802.11b and that appliances may interfere on the unregulated signal frequency. Table 2.1. summarises some 802.11 PHY specifications.

Table 2.1. PHY specifications [IEEE03].

	802.11a	**802.11b**	**802.11g**	**802.11n**
Standard approved by IEEE	January 2000	December 1999	June 2003	Initiate in 2007
Maximal Bit Rate [Mbps]	54	11	54	248
Typical Bit Rate [Mbps]	23	4.3	19	74
Modulation technology	OFDM	DSSS, CCK	DSSS, CCK, OFDM	DSSS, CCK, OFDM
RF band [GHz]	5	2.4	2.4	2.4 and 5
Channel Bandwidth [MHz]	20	20	20	20 or 40
N°of non-overlapping channels	24	3	3	3
Max EIRP Level [mW]	1000	100	100	100
Range indoor [m]	35	38	38	70
Range outdoor [m]	120	140	140	250

The new IEEE standard in the Wi-Fi category is 802.11n [WaMa06]. It was designed to improve 802.11g in the amount of bandwidth supported by using multiple wireless signals and antennas (called MIMO) instead of one. When this standard is finalised, 802.11n connections should support data rates over 100 Mbps. 802.11n also offers somewhat better range over earlier Wi-Fi standards, due to its increased signal magnitude. 802.11n equipment will be backward compatible with 802.11.

Within the IEEE 802.11 Working Group, more amendments exist. For example, 802.11r is the unapproved standard that specifies fast BSS (Basic Service Set) transitions [WaMa06]. This will allows connectivity aboard vehicles in motion, with fast handover from one AP to another, managed in a seamless manner. Handover is supported under the “a”, “b” and “g” implementations, but only for data, *i.e.*, the handover delay is too long to support applications like voice and video. The primary

application currently envisioned for the 802.11r standard is VoIP via mobile phones designed to work with wireless Internet networks, instead of (or in addition to) standard cellular ones.

Another unapproved extension is IEEE 802.11s [AkWW04], which is the standard for Extended Service Set (ESS) Mesh Networking. It specifies an extension to the IEEE 802.11 MAC to solve the interoperability problem by defining an architecture and protocol that support both broadcast/multicast and unicast delivery, using radio-aware metrics over self configuring multi-hop topologies. This amendment is not ready, and has not been used in this work on WMNs, since with the current standard a WMN can still be built, although less performing.

The IEEE 802.11k [IEEE03] is a proposed standard for radio resource management. It defines and exposes radio and network information to facilitate the management and maintenance of a mobile WLAN. This standard provides information to discover the best available AP. 802.11k is intended to improve the way traffic is distributed within a network. In a WLAN, each device normally connects to the AP that provides the strongest signal. Depending on the number and geographic locations of subscribers, this arrangement can sometimes lead to excessive demand on one AP and under usage of an other, resulting in degradation of overall network performance. In a network conforming to 802.11k, if the AP having the strongest signal is loaded to its full capacity, a wireless device is connected to one of the under used APs. Even though the signal may be weaker, the overall throughput is greater, because a more efficient use is made of the network resources.

The IEEE 802.11 working group chartered the 802.11e Task Group (TG) [IEEE03] with the responsibility of enhancing the 802.11 MAC to include bidirectional QoS to support to latency-sensitive applications, such as voice and video. The new applications for 802.11 require an effective QoS mechanism to ensure that their latency-sensitive audio/visual data has priority over other data, such as e-mail and web browsing. Section 2.1.3 addresses how the IEEE 802.11 working group is addressing the requirement for QoS, by reviewing the challenges for effective QoS in 802.11 networks.

2.1.2 Medium Access Control

The MAC sub-layer, as illustrated in Figure 2.1. regulates the access to the shared wireless medium, so that transmission stations do not interfere with each other. The MAC layer can work using two possible techniques: the Distributed Coordination Function (DCF), which uses an algorithm that provides access to all traffic, and the Point Coordination Function (PCF), which is a centralised algorithm that provides contention-free service by polling stations in turn. Moreover, there is the Logical Link Control sub-layer, which provides an interface to higher layers and performs basic functions, such as error control.

The basic 802.11 MAC layer uses the DCF to share the medium among multiple stations relying on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). DCF, however, has several

limitations. In fact, if several stations try to communicate at the same time, collisions occur, which will lower the available bandwidth (just like in Ethernet, which uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD)), the notion of high or low priority traffic not existing in the basic 802.11 standard. With DCF, once a station “wins” access to the medium, it may keep the medium for as long as it chooses. If a station has a low bit rate (1 Mbps, for example), then, it will take a long time to send its packet, and all other stations will suffer from that. So, more generally, there are no QoS guarantees.

The original 802.11 MAC defines another coordination function called PCF: this is available only in “infrastructure” mode, where stations are connected to the network through an AP. This mode is optional, and only very few APs or Wi-Fi adapters actually implement it. APs send “beacon” frames at regular intervals (usually every 0.1 s). Between these beacon frames, PCF defines two periods: the Contention Free Period (CFP) and the Contention Period (CP). In CP, the DCF is simply used; in CFP, the AP sends Contention Free-Poll (CF-Poll) packets to each station, one at a time, to give them the right to send a packet. The AP is the coordinator. This allows for a better management of the QoS.

Concurrent transmissions by multiple nodes results in frame collisions. The multiple transmissions interfere with each other, so that receivers are unable to distinguish the overlapping received signals from each other. It is impossible to entirely prevent collision in CSMA, but several ways exist to reduce them.

In pure CSMA, only the carrier sense is used to avoid collisions. If two nodes try to send a frame at nearly the same time, neither detects a carrier so that both begin transmitting, The transmitters do not detect collisions, so that they transmit the entire frame (thus, wasting the bandwidth used). Receivers cannot distinguish between collisions and other sources of frames errors, so collision recovery relies on the ability of the communicating nodes to detect frame errors and invoke an error recovery procedure.

The use of Time Division Multiplexing Access (TDMA) for the wireless medium access is unsuitable. In fact, the separation of the wireless medium into time slots may lead again to inefficient channel usage if the data packets do not completely fill in a time slot. TDMA requires a system wide synchronisation, in order to guarantee a time transmission of burst in slots, and thereby introduces more complexity. Guard times as part of slots help to avoid interference between time slots/channels, but reduce the user data capacity.

In wireless communication system that use carrier sensing, the so-called hidden station problem can occur. This problem arises when a station is able to successfully receive frames from two different stations but the two stations cannot detect each other. When stations cannot detect each other, a station, may sense the channel as idle, even when other hidden stations are transmitting, and it may initiate a transmission while the other station is already transmitting. To decrease throughput reduction owing to hidden stations, 802.11 specifies the exchange of Request-to-Send/Clear-to-Send (RTS/CTS) frames as an option. Before transmitting a data frame, a station may transmit a short RTS

frame, which must be followed by a CTS frame transmitted by a receiving station.

In CSMA/CA, each node must inform others nodes of the intention to transmit. When the other nodes have been notified, data is transmitted. This arrangement prevents collision, because all nodes are aware of a transmission before it occurs. However, collisions are still possible, and not detected, which has the same consequences as in pure CSMA.

Concerning timing, the time between two MAC frames is called the Interframe Space (IFS) [WaMa06], 802.11 defining four different IFSs: the Short Interframe Spaces (SIFS), the Point Coordination Function interframe Space (PIFS), the Distributed Coordination Function interframe Space (DCFS) and the Extended Interframe Space (EIFS). These interframes do not depend on the channel data rate, but only on the used transmission scheme. A slot duration (aSlotTime) is used to calculate the IFSs, and aSlotTime is used during the Collision Avoidance (CA).

SIFS is used to prioritise the immediate Acknowledgement (ACK) frame of a data frame, the response CTS frame to a RTS frame. PIFS is used by stations operating under PCF to obtain channel access with the highest priority; in particular, PIFS = SIFS + aSlotTime. DIFS is used by stations operating under the DCF to obtain channel access for frame exchanges, with DIFS = SIFS + 2. EIFS is used instead of DIFS whenever the PHY indicates that a frame transmission does not result in a correct Frame Check Sequence (FCS). The EIFS is therefore used when multiple stations initiated frame exchanges at different starting times.

In general, when more stations detect the channel as being idle simultaneously, inevitably a collision occurs if these stations initiate a frame exchange at the same time. To reduce the probability of collision, the Collision Avoidance mechanism is used: each station performs the backoff procedure before starting the transmission. A station, which has a frame to deliver, has to keep sensing the channel for an additional random time duration after detecting the channel as being idle for the minimum duration DIFS. Only if the channel remains idle for this additional random time duration, then, the station can initiate its transmission. The duration of this random time is a multiple of aSlotTime. Each station maintains a Contention Window (CW), which is used to determine the number of slot times that a station has to wait before transmission; therefore, the backoff time is a random number between 0 and CW. The CW size increases when a transmission fails; CW varies from a minimum value, CW_{min}, being doubled after each unsuccessful transmission, until it reaches its maximum, CW_{max}, which is called binary exponential backoff. This reduces the collision probability, if multiple stations attempt to access the channel.

Figure 2.2 shows an example of communication between two nodes: before each transmission, a backoff is applied for a number of slot durations within the limits of CW.

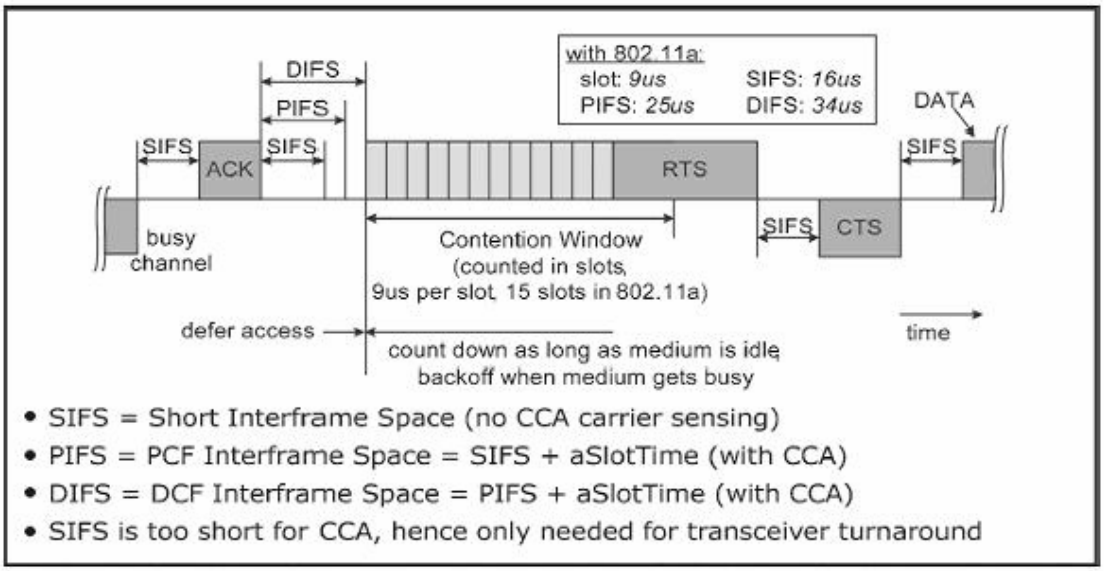


Figure 2.2. Contention for Collision Avoidance (extracted from [WaMa06]).

When a packet is sent using the 802.11 standard, an overhead is created by headers of various stack layers during the encapsulation phases [FCFN07]. For example, in a voice session in which VoIP is used there is, in addition to the vocal payload, headers due to encapsulation relatively to the Real-Time Protocol (RTP), User Datagram Protocol (UDP) and Internet Protocol (IP) protocols, but also to the MAC and the PLPC physical headers. Therefore, 802.11 introduces a large overhead to transmit a single voice data packet, and in compliance with this overhead and the contention access mechanism it is logic to think that the main drawbacks of 802.11 standard are in the support of real time services.

2.1.3 802.11e

IEEE 802.11e [IEEE03] is the standard that defines a series of QoS enhancements for LAN applications, in particular the 802.11 Wi-Fi standard. The standard is considered of critical importance for delay-sensitive applications, such VoIP and Streaming Multimedia. The protocol enhances the IEEE 802.11 MAC layer, and, in particular, it enhances DCF and PCF, through a new coordination function: the Hybrid Coordination Function (HCF). In HCF, there are two methods of channel access, similar to those defined in the legacy 802.11 MAC: HCF Controlled Channel Access (HCCA) and Enhanced DCF Channel Access (EDCA). Both EDCA and HCCA define Traffic Classes (TC). For example, e-mails could be assigned to a low priority class, and VoIP could be assigned to a high priority class. When the APs or the stations support QoS, their names become QoS Access Points (QAPs) and QoS Stations (QSTAs).

With EDCA, high priority traffic has a higher chance of being sent than low priority one, because in 802.11e the CW size is variable depending on traffic priority. In addition, each priority level is assigned a Transmit Opportunity (TXOP). A TXOP is a bounded time interval during which a station can send as many frames as possible (as long as the duration of the transmissions does not extend beyond the maximum duration of the TXOP). If a frame is too large to be transmitted in a single TXOP, it should

be fragmented into smaller frames. The use of TXOPs reduces the problem of low rate stations gaining an inordinate amount of channel time in the legacy 802.11 DCF MAC.

The first attempt to deal with LAN QoS in a standardised fashion appears in the original version of IEEE 802.1D [Stall01]. User Priority (UP) relates to the problem of how to handle priorities. UP is determined from the priority field of the incoming frame, and placed in the priority field of the outbound frame. Priorities are not used to transmit 802.11 MAC frames, therefore, if the outbound frame requires a priority field, then the priority field in the outbound frame is set to a default UP value.

IEEE 802.1D defines seven Traffic Classes:

- **Network Control (NC)**: simultaneously time and safety critical, consisting of traffic needed to maintain and support the network infrastructure, such as routing protocol frames.
- **Voice (VO)**: Time critical, characterised by less than 10 ms delay, such as interactive voice.
- **Video (VI)**: Time critical, characterised by less than 100 ms delay, such as interactive video.
- **Controlled Load (CL)**: Non-time-critical, but loss sensitive, such as streaming multimedia and business-critical traffic.
- **Excellent Effort (EE)**: Also non-time-critical, but loss sensitive, of lower priority than controlled load.
- **Best Effort (BE)**: Non-time-critical and loss insensitive. It is the normal LAN traffic.
- **Background (BK)**: Non-time-critical and loss insensitive, but of lower priority than best effort.

The 802.11e standard defines four Access Categories (ACs) being labelled according to their target application, i.e., AC_VO for voice, AC_VI for video, AC_BE for the best effort, and AC_BK for background. Table 2.2 shows the 802.1D User Priorities into 802.11e Access Categories.

Table 2.2 The 802.1D User Priorities into 802.11e Access Categories (extracted from [Liaw05]).

User Priority (same as 802.1D user priority)	802.1D Designation	Access category (AC)	Designation (Informative)
1	BK	AC_BK	Background
2	-	AC_BK	Background
0	BE	AC_BE	Best effort
3	EE	AC_BE	Video
4	CL	AC_VI	Video
5	VI	AC_VI	Video
6	VO	AC_VO	Voice
7	NC	AC_VO	Voice

Another IFS, called Arbitration Interframe Space (AIFS), is calculated based on SIFS, being used for each AC. Different values for AIFS allow further differentiation among different ACs. The AIFS Number (AIFSN) is the number of timeslots that are added to SIFS to obtain the AIFS. Table 2.3 shows values of CW and AIFSN for the different ACs.

Table 2.3. QSTAs Access Category medium access default parameters (extracted from [IEEE03]).

AC	CW_{min}	CW_{max}	AIFSN
BK	CW_{min}	CW_{max}	7
BE	CW_{min}	CW_{max}	3
VI	((CW_{min} + 1) / 2) - 1	CW_{min}	2
VO	((CW_{min} + 1) / 4) - 1	((CW_{min} + 1) / 2) - 1	2

2.2 Basic concepts of WMNs

A possibility to expand a WLAN in a large area is to use Wireless Mesh Networks. A WMN consists of mesh routers and mesh clients, where the former have minimal mobility, forming the backhaul of WMNs [AkWW04]. Mesh Point (MP) is the general term for a device participating in a mesh WLAN, able to forward traffic. The mesh WLAN is formed among APs; an AP that forwards frames is called Mesh AP (MAP), and only a sub-set of MAPs is connected to the fixed network (Internet). Figure 2.3 shows how mesh routers form an infrastructure for clients, where dashed and solid lines indicate wireless and wired links. It shows also the hierarchical structure of the WMN, where MAPs form the so-called Wireless Mesh backhaul. Others architectures of WMNs are available in [AkWW04].

The WMN backhaul can be built by using various types of radio technologies, in addition to the mostly used IEEE 802.11 technologies. The mesh routers form a mesh of self-configuring, self-healing links among themselves. With a gateway functionality, mesh routers can be connected to the Internet. This approach provides a backbone for conventional clients and enables integration of WMNs with existing wireless networks, through gateway/bridge functionalities in mesh routers. The mesh backhaul communication can be established using long-range communication techniques, including directional antennas.

Relatively to the characteristics of WMNs, the most important are the support for ad hoc networking and the capability of self-forming, self-healing and self-organisation. In this way, WMN improves network performance via flexible network architecture, easy deployment and configuration, fault tolerance, and mesh connectivity. Moreover, WMNs are multi-hop wireless networks, extending the coverage range of the current wireless networks, without sacrificing channel capacity, and providing

Non-Line-of-Sight (NLoS) connectivity among users without direct Line-of-Sight (LoS) links.

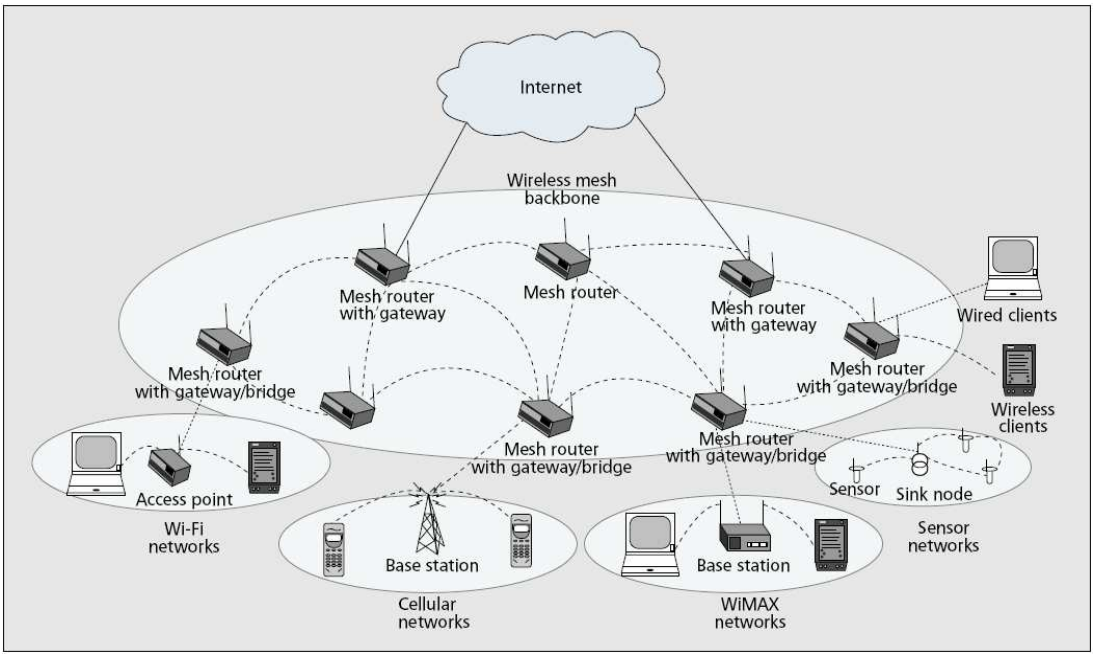


Figure 2.3. Infrastructure/backhaul WMNs (extracted from [AkWW04]).

Therefore, a WMN can provide a lot of services, but, on the other hand, critical factors can influence it, *e.g.*, WMN must assure scalability: if the network size increases, network performance should not decreased significantly. To solve this problem, it is necessary that protocols are scalable. Moreover, algorithms of topology control and network self-organisation are necessary to provide mesh connectivity, especially MAC and routing protocols.

As for the applications provided by WMNs, they can have various QoS requirements, therefore, it is important to consider end-to-end transmission delay and others performance metrics, like delay jitter and packet loss ratio. Another important problem is security, because the WMN architecture is decentralised and there is no centralised authority to distribute a public key security, schemes proposed for WLANs not being applicable for WMN.

It is possible to do a classification of WMNs considering the frequency channel used; indeed mesh networks may operate on single or multiple frequency channels [WaMa06]. In a single channel, frames travel in the same channel while multiple channels may work using a single or multiple radios. Figure 2.4 shows how mesh function may operate in band or out of band.

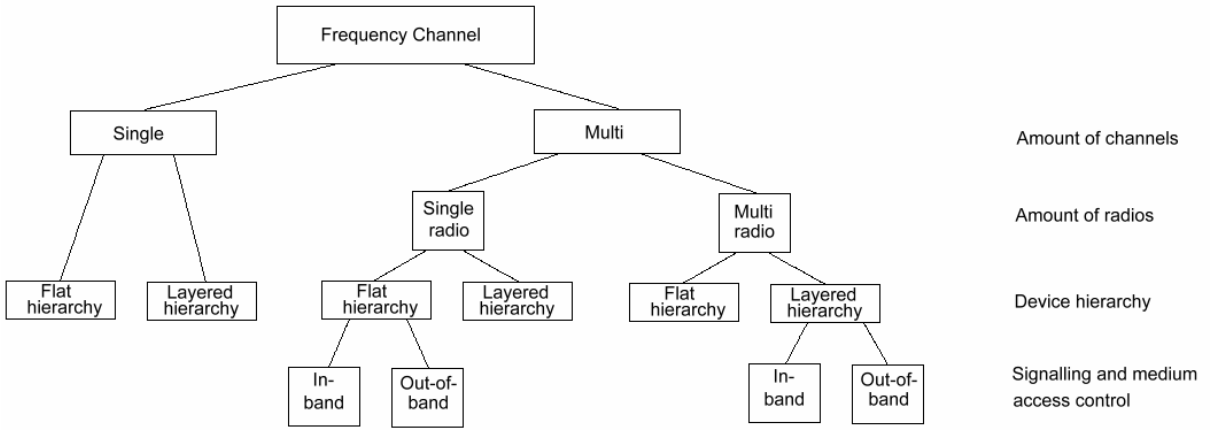


Figure 2.4. Classification of Wireless Mesh Network (extracted from [WaMa06]).

Some of the first products have done a good marketing and built relationships with first generation single radio architectures. Yet, these architectures are proven to be less superior and degrade performance in bandwidth, increased interference and higher latency. This makes it difficult to deploy and scale a larger number of nodes, and support more bandwidth intensive applications, such multimedia services.

Second generation mesh architectures employ dual radios, one for backhaul and one for access. Although there is a slight improvement in performance, it remains similar to first generation ones with a single backhaul radio.

The third generation architecture uses a multi-radio technology with dedicated radios for different functions, like backhaul ingress, and egress, and client ingress. The multi-radio approach is designed for a low latency and high performance for real time packet transmissions, versus the store and forward method and architectures from first and second generation mesh solutions.

Table 2.4. Differences between single, double and multiple radio.

	SINGLE RADIO	DOUBLE RADIO	MULTIRADIO
Density	1 radio	2 radio	3 or more radios
Scalability	Very Limited	Limited	High
Latency over hops	High	Medium High	Low
Throughput over hops	Very low	Low	High
Real Time Applications Support	Limited	Limited	High

Comparing WMNs with ad hoc networks, the first difference is that the network topology in WMNs is relatively static with respect to ad hoc networks, which is highly dynamic. Moreover, WMNs have most relay nodes fixed, whereas in Ad hoc network the mobility of relay nodes is high. WMNs can have a

partial or fully fixed infrastructure, and usually have better energy storage, and so are not energy constraint; this is not true for ad hoc networks, which are infrastructureless and have high energy constraints. The main difference between WMNs and classical WLANs is that in the former the APs have also a routing functionality to forward wirelessly data to other APs, whereas WLANs rely on APs that must be individually wired, resulting in a complex (APs must also be within 100 m of a network switch) and costly to deploy architecture.

Currently several solution for WMNs exist. For example, Cisco [Cisc07] use wireless mesh technology, wireless bridging and mobile networks to allow government, public safety, and transportation organisations to build cost effective outdoor wireless networks for private or public use. Cisco provides Patent-pending Adaptive Wireless Path Protocol (AWPP), which forms a WMN among nodes. Dual-radio option provides separate channels for the mesh infrastructure and client access, enabling pico-cellular design, minimising system interference, and delivering high system capacity. Single-radio option is available for environments that require a single band solution. Moreover, this solution complies with 802.11a and b/g standards for interoperability with any Wi-Fi-compliant client, and supports wireless backhaul over the 4.9 GHz band for reduced interference for public safety licenses. Support for 802.11e Wi-Fi Multimedia (WMM) provides QoS and seamless roaming for high-priority traffic, such as voice or video. The access protocol is the CSMA/CA and the data rate is up to 54 Mbps.

Others solutions are provided by Tropos [Trop07] and BelAir [BelA07]. BelAir, for example, supports unlicensed 2.4 GHz and 5.25 to 5.85 GHz frequencies, as well as licensed 2.3, 2.5, and 4.9 GHz frequencies. The access and backhaul radio modules support a broad range of frequencies, including Wi-Fi, WiMax and 4.9 Public Safety. BelAir has proposed also a solution able to support Global System for Mobile communications (GSM). Each of these solutions extends the range of WLANs securely and cost effectively for enterprises and end-users, and offer service providers new opportunities to drive increased revenue generation. The Tropos routers, *e.g.*, offers wireless access to both 2.4 and 4.9 GHz client devices in their proximity, and extend the mesh by providing wireless uplinks to other Tropos routers. The Tropos solution is optimised for vehicle mounting, provides in-vehicle access via Ethernet and can be easily fitted with an optional Global Position System (GPS) receiver.

An example of wireless technology is Worldwide Interoperability for Microwave Access (WiMax), which is the industry term for a long-range wireless networking standard. WiMax technology has the potential to deliver high-speed Internet access to rural areas and other locations not served by cable or DSL technology. WiMax also offers an alternative to satellite Internet services. This technology is based on the IEEE 802.16 WAN (Wide Area Networks) communications standard. WiMax signals can function over a distance of several kilometres. Data rates for WiMax can reach up to 75 Mbps; a number of wireless signalling options exist, ranging anywhere from 2 up to 66 GHz. In order to improve network coverage and scalability, the mesh mode is supported in 802.16. In the mesh mode, all nodes are organised in an ad hoc way, and use a pseudo-random function to compete for their transmission

opportunities, based on the scheduling information in the two-hop neighbourhood.

The IEEE 802.11s [HoLe08] standard for ESS Mesh Networking is being defined by IEEE TGs. The purpose of the project is to provide a protocol for auto-configuring paths between APs over-configuring multi-hop topologies in a Wireless Distribution System (WDS) to support both broadcast, multicast and unicast traffic in an ESS Mesh. The Wi-Mesh Alliance (WiMA) [WiMA07] has presented a proposal that will enable seamless communications for wireless users regardless of equipment vendor. The WiMA proposal is designed to work with all three major applications of mesh technology: consumer and small business, metropolitan, and military. The standard is expected to be approved by 2008.

2.3 Services and scenarios

Several services are possible to implement in WMSs [WaMa06]:

- **VoIP**: it is the transmission of voice traffic over IP-based networks.
- **E-mail**: it is a store and forward method of composing, sending, storing, and receiving messages over electronic communication system.
- **Videoconference**: it allows two or more locations to interact via two-way video and audio transmissions simultaneously.
- **Video streaming**: it is multimedia that is continuously received by the end user, while it is being delivered by the provider.
- **Web browsing**: a user can interact with text, images, videos and other information typically located on a web page at a website.
- **FTP**: it is used to transfer data from one computer to another.

For all of these services, users prefer also a minimal delay, mainly in real-time applications with vocal and video services. On the transport level, it is possible to implement various protocols, namely TCP and UDP. TCP allows the transport of a flux of traffic between two applications on different hosts in connection oriented mode; before transmitting data, TCP must establish a communication, negotiating a connection between sender and addressee; after this, the transmission of data can occur; then it finishes closing the connection. TCP guarantees that the transmitted data arrives at destination by means of acknowledgement and retransmission mechanisms. To enable this, a TCP segment must to have a long header. To decrease the overhead it is possible to use UDP, which does not give any guarantee about the datagram arrival, neither their order of arrival. UDP is connection less, and so this protocol does not need to send other packet to establish and close connections. In general, the TCP is preferred to UDP when it is necessary to have guarantees about the data delivery or about the order of arrival of various segments (like, for example, the case of FTP). On the other hand, UDP is used manly when there is a demand about the velocity and the network resources economy. Common network applications that use UDP include the Domain Name System (DNS), streaming media

applications such as VoIP and Internet Protocol Television (IPTV), Trivial File Transfer Protocol (TFTP) and online games.

With WMNs, cities can connect citizens and public services over a widespread high-speed wireless connection. A growing number of downtown areas are installing public Wi-Fi hotspots. Mesh networks allow cities to inexpensively and easily link all those hotspots together to cover the entire municipality. WMNs are useful in countries without a widespread wired infrastructure, such as telephone service or even electricity. Solar-powered nodes can be connected to one cellular or satellite Internet connection, which could keep a whole village online. Even in developed countries, there are rugged locations too far off the grid for traditional high-speed Internet service providers. WMNs are being considered for these areas. A series of nodes would be mounted from the nearest available wired AP out to the hard to reach area.

Many colleges, universities and high schools are converting their entire campuses to WMNs. This solution eliminates the need to bury cables in old building and across campuses. With some of well-placed indoor and outdoor nodes, everyone will be connected all the time. Mesh networks also have the capacity to handle the high-bandwidth needs required by students who need to download large files. Schools can also rig their entire public safety system up to the network, monitoring security cameras and keeping all personnel in constant communication in emergency solutions.

Many hospitals are spread out through clusters of densely constructed buildings that were not built with computer networks in mind. The ability to connect to the network is crucial as more doctors and caregivers maintain and update patient information (test results, medical history, even insurance information) on portable electronic devices carried from room to room.

Already several cities use mesh networks. Cisco Systems [Cisc07] has deployed in Dayton (Ohio, USA) and Lebanon (Oregon, USA) his WMN. With a population of nearly 13.000, Lebanon mirrors hundreds of other small-town environments where offering affordable high-speed Internet access has been a challenge. In Lebanon, the Wi-Fi mesh solution covers 60 percent of the town, but the focus is on rolling out new city services on top of the mesh network. The city plans to test the mesh network with police cars and public works vehicles equipped with mobile terminals. This way, officers and city workers can wirelessly connect to their existing infrastructure and take advantage applications, IP communications, and streaming video. City of Dayton officials have big ideas about the types of services their metro wireless network can support in the future. They envision a day when a citywide wireless network will support remote reading of water meters, real-time video streaming to police cruiser, wireless links between emergency vehicles and hospitals for processing blood tests remotely, and even parking meter enforcement. Chittagong, a port city of 3.5 million people that is the commercial capital of Bangladesh, is the site of a new wireless mesh network that provides both phone and Internet service to residential and business customers.

2.4 State of the Art

During network design it is important to know the capacity and performance that the network must ensure. While designing a WMN, it is important to understand how the delay and capacity of the WMN scale with the number of clients and mesh routers. The design of a WMN would depends on various factors such as mesh client density, the available budget, required bit rate and the expected traffic pattern. So, it is important to be able to answer questions as what bit rate is available to a certain number of clients if the budget allows an established number of mesh routers with some available channels, or how many mesh clients can be served with a given bit rate if the budget allows deployment of an established number of mesh routers with a fixed number of available channels over given area. The goal of this thesis is to characterise the average delay, the maximum achievable throughput in WMNs, and the loss rates in terms of various network parameters. Latency is very important for VoIP, multicast applications, video streaming, and also small HTTP, over mesh networks. On the other hand, loss rate affects web access and TCP performance, and can also be used by routing protocols to construct high-quality paths.

The asymptotic capacity of multi-hop wireless networks is studied in [GrTs02], [GuKu00], [LCLM01], [NeTu01]. In [GuKu00], it is shown that for a network with m stationary nodes, each capable of transmitting at *W* bps, then, the per-node capacity scales as $W/\sqrt{m\log m}$. Extensive simulations are used in order to study the effects of variation of various network parameters, like number of nodes and path length, on network throughput [NeTu01], and the simulation results agree closely with [GuKu00]. [LCLM01] considers the capacity of regular ad hoc networks. An interesting probabilistic model is used in [Haen02] to compute the capacity of a chain of wireless nodes.

In [KiVa05] the authors study the effect of the number of channels and interfaces on the capacity of multi-hop wireless networks. They found that in general if the number of available channels is greater than the number of interfaces, then, the capacity of the wireless network degrades by a factor that depends on the radio of the number of interfaces to the number of available channels. However in some cases, where the number of available channels is $\log m$, there is no degradation in the capacity. Some recent papers have focussed on measurement based performance evaluation of WMNs [BABM05], [RaCh05].

[JuSi03] shows that the existence of gateways in WMNs introduces “hot spots” in the network that act as bottlenecks. Due to the presence of these bottlenecks, the available capacity for each node is reduce to $1/m$. Most importantly, in our analysis, one not only treats the asymptotic case, but also computes exactly the minimum and the maximum data rates available for each node in a WMN for a given network topology and link layer protocol. The key concept enabling this computation is the bottleneck collision domain, which is the geographical area that limits the overall throughput of the network. [JuSi03] analyses the capacity of WMNs based on the traffic behaviour at the MAC layer. Since their approach is not limited to a specific MAC scheme, one can compute the exact capacity of a

WMN for any MAC layer implementation. Most research effort for WMNs has been focussed on developing efficient strategies for routing, channel assignment and scheduling in order to maximise throughput [DrPZ04], [RaCh05], [RaGC04], [AlBL05].

The average delay is the expectation of packet delay over all packets and all possible network topologies. One way to measure the packet latencies is that each node in turn sends a specific number of ping packet with fixed length to each other node. In this way, it is possible to obtain the Round-Trip Times (RTTs) between any pair of nodes for the paths used by the specified protocol. The packet size used must to be typical for many Internet applications (for example, if the packet size is 1470 byte and the packet interarrival time is 0.01 s, then, it is equivalent to a sending rate of about 1.1 Mbps). Others measurement papers prefer broadcast packets [ABBJ04].

Chapter 3

Modelling

This chapter provides models on WLAN and WMNs relative to capacity estimation. The analytical approach provides also how to measure communication ranges, throughput, delay, and maximum number of VoIP users in WMN. Finally, a brief description of OPNET Modeler is provided, which is the software used to do simulations in this work.

3.1 Performance parameters

This section shows how to measure communication range, delay, throughput, and maximum number of VoIP users. The parameters that influence the communication range are power, sensitivity of the transmitter/receiver, distance between transmitter and receiver, and environment. The Delay is influenced by the number of hops, the number of users per MAP, the number of MAPs, and CW. Throughput depends mainly on the overhead of various protocols layers, on the payload length, and on the medium access times. The number of users varies on the basis of the data rate and the type of service used.

3.1.1 Communication Ranges

The maximum allowable output power is measured in accordance with practise specified by regulatory institutions [IEEE03]. [Cisc07] provides the typical maximum (Effective Isotropic Radiated Power) EIRP allowed for each data rate in the IEEE 802.11a/b/g, Table 3.1. One has to consider that the EIRP shown are the maximum values for outdoor communication.

Table 3.1. Maximum EIRP for IEEE 802.11a/b/g (extracted from [Cisc07]).

Standard	Maximum EIRP [dBm]
802.11a	30
802.11b	20
802.11g	20

Another important parameter is the equipment sensitivity, which depends on the bit rate, and, in the 802.11a case, on frequency. Table 3.2 shows typical sensitivity values for 802.11a/b/g.

In a wireless communication is necessary to consider that, to predict the behaviour of radio wave propagation, several empirical mathematical formulations exist for its characterization, as a function of frequency, distance and other conditions. The most elementary model is the free-space path loss. In this model L_0 is the loss in signal strength of an electromagnetic wave that would result from a LoS path through free space, with no obstacles nearby to cause reflection or diffraction.

Table 3.2. Typical receiver sensitivity for IEEE 802.11a/b/g (extracted from [Cisc07]).

Data Rate [Mbps]	Sensitivity in 802.11a [dBm]	Sensitivity in 802.11b [dBm]	Sensitivity in 802.11g [dBm]
1		-94	
2		-94	
5.5		-90	
6	-91		-91
9	-89		-89
11		-88	
12	-89		-89
18	-86		-86
24	-84		-84
36	-80		-80
48	-76		-76
54	-73		-73

In wireless communications, it is necessary to consider models to predict the behaviour of radio wave propagation as a function of frequency, distance, and other parameters. The most elementary model is the free-space path loss. From [Rapp96]:

$$L_{0[\mathrm{dB}]} = 20log\left(d_{[\mathrm{km}]}\right) + 20log\left(f_{[\mathrm{Mhz}]}\right) + 32.44_{[\mathrm{dB}]} \quad (3.1)$$

where:

- f : is the frequency.
- d : is the distance.

The free space propagation model can not be used when an obstacle exists. When, *e.g.*, the radio wave penetrates a wall, it is necessary to have others propagation models.

In both indoor and outdoor environments, the average large-scale path loss for an arbitrary transmitter-receiver separation is expressed as a function of the distance by using a path loss exponent, n. The value of n depends on the specific propagation environment, *i.e.*, type of construction material, architecture, and location within a building. n does not vary much with the frequency; Table 3.3 shows typical values of n. The Log-Normal Shadowing Model equation [Rapp96] considers random shadowing effects, and the average path loss *L* between a transmitter and

receiver, with separation, d is given by:

$$L_{[\mathrm{dB}]} = L\left(d_{0[\mathrm{km}]}\right) + 10n\log\left(d_{[\mathrm{km}]} / d_{0[\mathrm{km}]}\right) + \varepsilon_{[\mathrm{dB}]} \quad (3.2)$$

where:

- ε : is a zero-mean Gaussian distributed random variable with standard deviation σ_ε.
- d_0 : is the reference distance, which is the received-power reference point.

For applications operating at 1 to 2 GHz, d_0 is 1m for indoor environments and 100 m for outdoor ones. If the devices are stationary, it is possible to ignore ε. For in-building propagation, there is a model that considers floor attenuation [Rapp96].

Table 3.3. Typical values for the path loss exponent, n (extracted from [Rapp96]).

Environment	n
Retail store	2.2
Grocery sore	1.8
Office, hard partition	3.0
Office, soft partition	2.5
Factory, line of sight	2.0
Suburban, indoor street	3.0
Residential environment	3.3

3.1.2 Delay

In order to determine the delay of the system, it is necessary to analyse the MAC layer. 802.11a/b/g compliant data packet consist of preamble, header and payload. The payload in turn consists of data from the application, plus the overhead added at transport and IP layers. The transport mechanism can either be TCP or UDP. TCP adds more overhead compared to UDP, and also has inherent retransmission and flow control mechanisms.

The Delay depends on the time taken to transmit the packet, and in a WLAN this is determined by DCF. DCF enables the sharing of the medium among active nodes, based on physical sensing of the medium. In DCF, all directed packets are positively acknowledged (the ACK); retransmission occurs if there is a failure to receive an ACK. Thus, the time taken to transmit a packet with a particular

payload, $T_{PAY\,pkt}$, depends on the MAC ($T_{MAC\,hdr}$) and a PLPC headers ($T_{PHY\,hdr}$) [IEEE03]. Moreover, the packet can be transmitted only after an AIFS period (T_{AIFS}) plus a backoff (T_{BO}) one, which depends on the amount of CW in the network. Once executed, this transmission plus a SIFS period (T_{SIFS}), and Acknowledge packet (T_{ACK}) with a $T_{PHY\,hdr}$ is received. The network delay, D_{NET}, taken to transmit a packet is shown below [FCFN07].

$$D_{NET[\mu s]} = T_{BO} + T_{AIFS} + (T_{PHY\,hdr} + T_{MAC\,hdr} + T_{IP\,hdr} + T_{PAY\,pkt}) + T_{SIFS} + (T_{PHY\,hdr} + T_{ACK}) \quad (3.3)$$

From (3.3), one can see that throughput depends on the load in the network and on the received signal strength. Figure 3.1 shows an example of overhead in the transmission of a data packet.

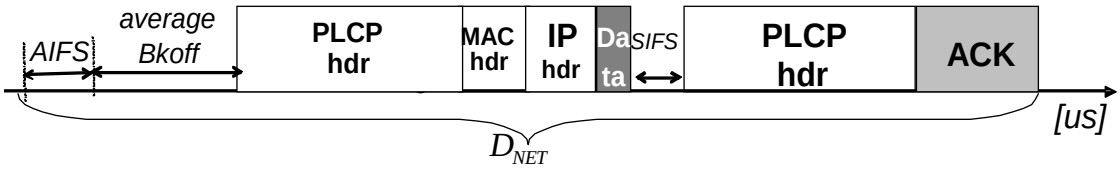


Figure 3.1. Example of overhead in 802.11 transmission (extracted from [FCFN07]).

A practical method to calculate D_{NET} is provided by [JuPe03]:

$$D_{NET[\mu s]} = \alpha_{\left[\frac{\mu s}{bytes}\right]} \times x_{[bytes]} + \beta_{[\mu s]} \quad (3.4)$$

where x is the payload, whereas α and β are two coefficients that depend on the type of standard used. Values for α and β are shown in Table 3.4, which also shows D_{NET} for a payload of 20 bytes (typical value in VoIP).

Table 3.4. Coefficients to compute network delay (extracted from [JuPe03]).

Data Rate [Mbps]	α [µs/bytes]	β [µs]	D_{NET} [µs]
6	1.33	230.17	256.84
12	0.66	194.00	207.33
24	0.33	177.67	184.34
54	0.15	167.00	169.96

When one wants to evaluate the performance in a voice application, the main parameter is the Voice Packet End-to-End Delay, E_{VPD}, which is the sum of network delay D_{NET}, encoding delay D_{ENtx}, the

decoding delay D_{DErx}, compression delay D_{COtx}, and decompression delay D_{DCrx} (the values for D_{ENtx}, D_{DErx}, D_{COtx}, and D_{DCrx} depend on the type of VoIP application used):

$$E_{VPD} = D_{ENtx} + D_{COtx} + D_{NET} + D_{DErx} + D_{DCrx} \quad (3.5)$$

This is true in a single hop network, whereas in a multihop one the analysis is more complex; details about network delay estimation in these kinds of networks are provided in [GoMM04].

Another parameter is the WLAN Delay, D_{WLAN}, which represents the End-to-End delay of all the packets received by WLAN MACs of all nodes in the network and forwarded to higher layers.

Others kinds of delay are useful to analyse a network. The first one is the Media Access Delay, D_{MAD}, which represents the global statistic for the total of queuing and contention delays of the data, management, delayed Block-ACK and Block-ACK Request frames transmitted by all WLAN MACs in the network.

Moreover, in this work, others parameters about the response time, RT, are considered:

- **HTTP response time, RT_{HTTP}:** it specifies the time required to retrieve the entire page with all the contained inline objects.
- **FTP response time, RT_{FTP}:** it is the time elapsed between sending a request and receiving the response packet, being measured from the time a client application sends a request to the server to the time it receives a response packet. Every response packet sent from a server to an FTP application is included in this statistic
- **E-mail response time, RT_{Email}:** it is the time elapsed between sending a request for e-mails and receiving e-mails from the e-mail server in the network. This time includes signalling delay for connection setup.

3.1.3 Throughput

TCP provides congestion control, which controls the rate of data entering the network, keeping the data flow below a rate that would trigger collapse. ACK for data sent is used by senders to implicitly interpret network conditions between the TCP sender and receiver. TCP receive windows size is the amount of received data (in bytes) that can be buffered during a connection. The sending host can send only up to that amount of data, before it must wait for an ACK and window update from the receiving host. When a receiver advertises the window size of 0, the sender stops sending data and starts the persist timer. The persist timer is used to protect TCP from the dead lock situation, which could be when the new window size update from the receiver is lost and the receiver has no more

data to send, while the sender is waiting for the new window size update. When the persist timer expires, the TCP sender sends a small packet so that the receivers ACKs the packet with the new window size, and TCP can recover from such situations.

A larger window size is recommended to improve TCP performance, in networks paths with large bandwidth and long-delay characteristics. The TCP windows size field controls the flow of data and it is limited from 2 to 65 535 bytes. This approach is not good for wireless networks, because the lost of packets is frequent, due to the unreliability of the wireless channels. The best approach is to increase the send rate, resending packet as quickly as possible. Unfortunately, standard algorithms for congestion control assume that a packet lost is equivalent to a congestion in the network, and the consequence is a rate reduction.

[JuPe03] provides a definition for the Theoretical Maximum Throughput, TMT, using the same coefficients values for α and β shown in Table 3.4. TMT is the ratio between the payload x and the network delay D_{NET} :

$$TMT_{[\text{bps}]} = \frac{8 \times x_{[\text{bytes}]}}{\alpha_{\left[\frac{\mu s}{\text{bytes}}\right]} \times x_{[\text{bytes}]} + \beta_{[\mu s]}} \times 10^6 \tag{3.6}$$

Table 3.5 shows TMT, considering a payload x of 536 bytes (default value in OPNET Modeler), where as payload one can considers the Maximum Segment Size (MSS) that the underlying network can carry without fragmenting.

Table 3.5. TMT values (extracted from [JuPe03]).

Data Rate [Mbps]	TMT [Mbps]
6	4.54
12	7.78
24	12.03
54	17.40

Another study [JuSi03] provides the maximum throughput available for a multi-hop network. Figure 3.2 shows a basic network topology with two nodes (1 and 2) that have the same offered load sent to the gateway. Ideally, as the load increases, both nodes have the same throughput but, in practice, the node 1 closest to the gateway is advantaged relative to node 2. If the load consists of a file download using FTP, then, the throughput considered in this case is the so-called FTP User Throughput, R_U ,

computed as the ratio between the file size and the average time to download the file. The average of all FTP user throughputs in a network is called R_A.

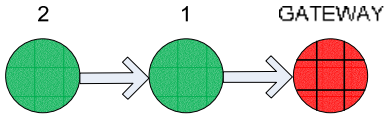


Figure 3.2. Fairness study of a two-node network (extracted from [JuSi03]).

Another kind of throughput used in this work is the WLAN Throughput, R_{WLAN}, which represents the total number of bits forwarded from WLAN layers to higher layers in all nodes of the network.

Moreover, in this work the WLAN Load, L_{WLAN}, was used, which is the total load submitted to wireless LAN layers by all higher layers in all nodes of the network.

In a network, not all packets arrive to destination, thus, an useful parameter to study is the number of dropped data, D_{DATA}. This parameter is the total size of higher layer data packets dropped by all the MACs in the network due to full higher layer data buffer, or the size of the higher layer packet, which is greater than the maximum allowed data size defined in the IEEE 802.11 standard.

3.1.4 Maximum number of VoIP users

As wireless networks see increasing public deployment, it is important for services providers to able to be ensure that access to the network by different users and applications remains equitable, so it is important focus on the problem of TCP fairness in a WLAN. Fairness issues in WLANs have been studied extensively [LuBh99], [VaBG00]. However, most of these solutions involve changes to the MAC layer, which is impractical, given the wide deployment of these networks. Also, while the focus of previous work has been on ensuring a particular QoS level for a given flow, it is interesting to analyse TCP fairness in the presence of both up- and downloads. Consider a typical installation of 802.11 based WLAN where the hosts access the network through an AP; since the 802.11 protocol allows equal access to media for all hosts, the AP and mobile hosts all have equal access to the medium; if the hosts are all senders or all receiver, then they each one has equal share of the total available bandwidth. However, consider the case when there is on sender and the rest are all receivers: in this case, the AP and the sender get equal access to media; this sender gets half of the channel bandwidth, and the remaining half is equally shared by all receivers; depending on the number of receivers, the sender can achieve several times the bandwidth of the receivers. Thus, the very equal access nature of the 802.11 media access protocol, when applied to the standard installation of access through a case station, results in significant unfairness.

Concerning the maximum number of VoIP users in a WMN, it is associated to the Voice Packet End-

to-End Delay, E_{vpd}. A VoIP application can not tolerate high delays; in fact, the maximum E_{vpd} has to be less than 400 ms, preferably under 150 ms.

The worst case happens when all the network users do simultaneously a VoIP call, and by considering this case, it is possible to find the maximum number of simultaneous VoIP users, N_{SV}. To find a rule to do this, one has to considers that the packet delay increases whenever a packet has to do a hop from one network node to another. Thus, in general to guarantee a good performance in a VoIP session to all users in the network, it is necessary that the users with the greatest hop distance from the gateway have an End-to-End Voice Packet Delay less then 400 ms. When all these users have the possibility to do calls with an acceptable delay, then, the maximum number of simultaneous VoIP users corresponds to the actual number of users in the network.

One idea to estimate a possible value for the maximum number of VoIP users, when they do not do simultaneously VoIP calls, is provided to use the Erlang B formula. Erlang B is the commonly used traffic model, and it is used to work out how many resources are required if the traffic during the busiest hour is know. The model assumes that calls are performed over Circuit Switching networks and that all blocked calls are immediately cleared. This is not the case for WLANs, but, still, this model can be used to provide a rough estimation. The probability of block B is expressed as:

$$B(N, A_{[\mathrm{Erl}]}) = \frac{\frac{A_{[\mathrm{Erl}]}^{N}}{N!}}{\sum_{i=0}^{N} \frac{A_{[\mathrm{Erl}]}^{i}}{i!}} \tag{3.7}$$

where:

- N : is the number of resources in the network.
- A : is the total amount of traffic offered.

Considering as number of resources the maximum number of simultaneous VoIP users, N_{SV}, and for a certain probability B, it is possible to compute the amount of traffic A. One can consider the traffic of a single user as:

$$A_{user[\mathrm{Erl}]} = \frac{N_{calls} \times T_{call[\mathrm{min}]}}{60} \tag{3.8}$$

where:

- N_{calls} : number of calls per hour.

- T_{call} : average holding time.

The ratio between the traffic A and the traffic per user A_{user} represents an estimation for the maximum number of VoIP users, N_V :

$$N_V = \frac{A}{A_{user}} \tag{3.9}$$

3.2 OPNET

OPNET Modeler [OPNE07] is a comprehensive software designed and manufactured by OPNET (Optimum Performance Network) Technologies. This software allows its user to design and study communication networks, devices, protocols, and applications. Modeler's object-oriented modeling approach and graphical editors mirror the structure of actual networks and network components. Modeler supports all network types and technologies. Among the many benefits of this development environment are: its hierarchical network models, its clear modeling paradigm, its finite state machine design capabilities, its integrated analysis tools, its comprehensive libraries of protocol, application, and network devices, its wireless, point-to-point, and multilinks functionality.

The main decision making process involved in design with the OPNET Modeler is the use and definition of each of the hierarchical models. OPNET models are structured hierarchically, in a manner that represents real network systems. The specialised editors allow modifications and configurations at each specified hierarchical level. The OPNET Modeler environment is categorised by modelling domains. The main modelling domains are the Network, Node, and Process Domains.

The Network Model defines the overall scope of a system to be simulated, specifying the objects in the system, their interconnections, and the system’s configurations. The network may be simple and contain one node, or more complex with many interconnected nodes and subnetworks. Network models are composed of the following building blocks:

- **Subnetworks**: encapsulate other network objects.
- **Communication nodes**: model network objects with definable internal structure.
- **Communication links**: mechanism to transport information in between communication nodes.

Subnetworks encapsulate other network objects, encompassing a set of nodes, fixed or mobile, and links that represent a grouping of objects, such as a LAN. Subnetworks may be organised hierarchically, creating parent/child relationships and/or reiterative complexity; they may also exist independent of each other, with no present interconnections. There are three types of interconnections: fixed, mobile, and satellite. Fixed subnetworks are statically placed, and their

x_position and *y_position* can not change during simulation. Mobile subnetworks have the capability to change positions during simulation; these changes are attributed to statically defined trajectory segments, by a vector trajectory, or by direct changes to subnetworks position attributes. A satellite has the ability to change during simulation via an assigned orbit; this orbit defines its orbital path through time.

Communication nodes exist within a subnetwork, representing a network device. The node model defines the actual function and behaviour of the node. Much like the subnetwork categorisation, there are three types of communication nodes: fixed, mobile, and satellite. Fixed nodes are unable to change its position during simulation; a fixed node is typically used to model static network devices, such as workstations, gateways, or ground stations, LAN nodes are special kinds of fixed nodes, and they have the ability to connect to all other objects with the same or different data rate and protocol. Mobile nodes have the ability to change positions during a simulation; a mobile node is typically used to model terrestrial network elements, such as automobiles, military vessels, etc. A satellite communication node has the ability to change position during simulation via an assigned orbit; every satellite node is located within a subnetwork object.

Communication links allow communication between nodes in the form of packets. A link is composed of several communication channels, each defining a connection between a transmitter and a receiver. OPNET Modeler supports three types of links: point-to-point, bus, and radio. Point-to-point links connect a single source node to a single destination node; the number of communication channels is static, since there is one channel between transmitter and receiver, and links have the ability to be simplex or duplex connections. A bus link is a constrained broadcast communication medium, connecting a fixed set of nodes to each other; nodes that require access to and from a bus must contain bus transmitters and receivers, and are attached to the bus via a tap (a simple element that is used to connect fixed node to a bus). A radio link may exist between any transmitter-receiver channel pair, and is dynamically established during simulation; radio links potentially allow all nodes to communicate with each other, based on dynamic evaluation; since radio is a broadcast technology, the transceiver pipeline must evaluate the possible connectivity between a transmitter and a receiver for each transmission.

The Node Model defines the internal structure of the communication nodes and communication links defined by the Network Model. A node model is composed of a series of connected blocks called modules, which represent all the various functional areas of a node. The types of modules that can be implemented in the node model are processors, queues, generators, receivers, transmitters, and antennas. The processor modules are used to perform the overall processing of the data packets transmitted through the node, serving as the primary building blocks of the node models. Processors can be connected to other modules to send and receive packets via any number of packet streams; typical processor receives the packet on the input stream, performs some processing, and sends the packet out on an output stream. Processor modules can also act as “controllers,” communicating through statistic wires or remote interrupts. The queue modules provide an extended functionality of

the processor module; the queue contains an additional set of internal resources, the subqueues, which facilitate buffering and managing a collection of data packets. The capacity of each subqueue to hold data is unlimited by default, and may be defined within a subqueue. The internal structure of the queue is set up as an array of subqueues. The access to each subqueue is determined by either a physical or abstract index number.

The transmitter modules are the interface between packet streams inside a node and the communication links outside the node, collecting all packets within the node and relaying them over a communication channel to the awaiting communication link. A packet received on an input stream is transmitted over the channel with same index number. Transmitter modules have an input packet stream, being considered to be a data sink; from the network model, the transmitter acts as the output port of the nodes to which the communication links are connected. Receiver modules serve as the interface between the external communication links and internal packet streams, distributing packets to one or more output packet streams upon reception; a receiver is considered to be a data source. Opposite of the transmitter modules, receiver modules have no input packet stream. There are three types of receivers, as well as transmitters: point-to-point, bus, and antenna.

The main objective of the Process Model is to define the behaviour of the processor and queue modules defined within the Node Model. A process model typically represents a behavioural model of a process, which are interrupt-driven execution and dynamic processes.

Interrupt driven executions occur when an event is delivered to a process. When this event is invoked, it is important to determine the type of interrupt that occurred; then, more detailed attributes are analysed including input streams or statistic wires. A process follows a cycle of invocation and rest periods, alternating Blocked and Active states; invocation may occur at random times based on the internal and external timing of generated events.

Dynamic processes, processes invoked by other processes, occur during execution, forming a process hierarchy and being added to the list of processes needing execution time. Multiple processes share memory architecture. Each parent-child pair can establish an independent block of memory for two-way communication. To eliminate inconsistent data structures, an external copy is stored in each process's header file.

OPNET Modeler contains a large library package of functions, consisting of several used for operations on Dynamic Processes. Functions are defined for the creation of an initial process, which places the process in the process hierarchy.

State Transitions Diagrams (STD) consists of states and transitions: states represent modes that the process can enter, while transitions specify the changes in state that are possible for the process. States consist of the state information it has chosen to retain; the executives of a state are split into the enter executive and the exit executive, which This functionality allows the states to execute two separate functions depending on its transition. States are classified as either forced or unforced; in an

unforced state, there is a Blocked state between the execution of the enter and exit executives, that waits for an interrupt; conversely, forced states do not allow the process to wait. Transitions describe the possible movement of a process from state to state. There are four components to a transition's specifications: a source state, destination state, condition expression, and an executive expression. Transitions may either occur from one node to another or back to itself. Condition expressions may include complex combinations, including, state variable values, boolean values, and interrupt attributes.

The OPNET Modeler networking environment allows users to simulate the models they have created in dynamic scenarios in order to study system behaviour and performance. The specific features of Simulation Design are specifying data collection, simulation construction, and simulation execution. Some statistics that may be considered for verification during early modeling phase are progress, flow of data, basic statistics, and key events. Others include application-specific and behavioural data. Simulation output can be collected and displayed in four distinct forms: output vectors, output scalars, animation, and proprietary reports and files.

All of the data that is collected during the Simulation Design phase may be analysed using the OPNET Modeler Analysis Tool. The general service of this tool is to display information in the form of graphs. Output scalar files combined the data collected through multiple simulations. The Analysis Tool allows the plot of several simulations to be graphed together. Overall, both the Simulation Design and Analysis Tool encompass a wide variety of functionality.

In OPNET, it is possible to define the profiles and applications that will be used by the network. A profile is applied to a workstation, server, or LAN, specifying the applications used by a particular group of users. Various profiles are available, like profiles for Marketing (heavy use of email, light use of FTP) and for Engineering (light use of email, heavy use of file transfer). An application be any of the common applications (email, FTP) or a customise application. Eight common applications are already defined: Database Access, Email, File Transfer, File Print, Telnet Session, Video conferencing, Voice over IP Call, and Web Browsing.

3.3 Path loss implementation in OPNET

The default path loss model provided by OPNET are not good for the scenarios to be analysed. In fact, the free space propagation model does not allow to implement a realistic scenario in which buildings are present, whereas the others models available in OPNET are not valid in the frequencies range used in 802.11 standard.

A new path loss propagation model was added in the OPNET Terrain Modeling [OPNE07]. This model considers the Log-Normal Shadowing Model, (3.2), being considered the outdoor model for a campus

environment with path loss exponent $n = 3.3$. With these values, in fact, it is possible to simulate an environment composed by several buildings and open areas.

To insert this model in the OPNET library it was necessary to create a Visual C++ file in which the model was developed. Once inserted the model, the communication range was found, *i.e*, the maximum distance in which two nodes are in radio visibility. In particular, the communication ranges for each data rate available in 802.11a and 802.11g standards were found.

Figure 3.3 and Figure 3.4 show the small differences between the theoretical values and the values obtained with OPNET. In 802.11a, a transmission power of 30 dBm was used, whereas for 802.11g the transmission power was 20 dBm (the maximum values for outdoor communication were used).

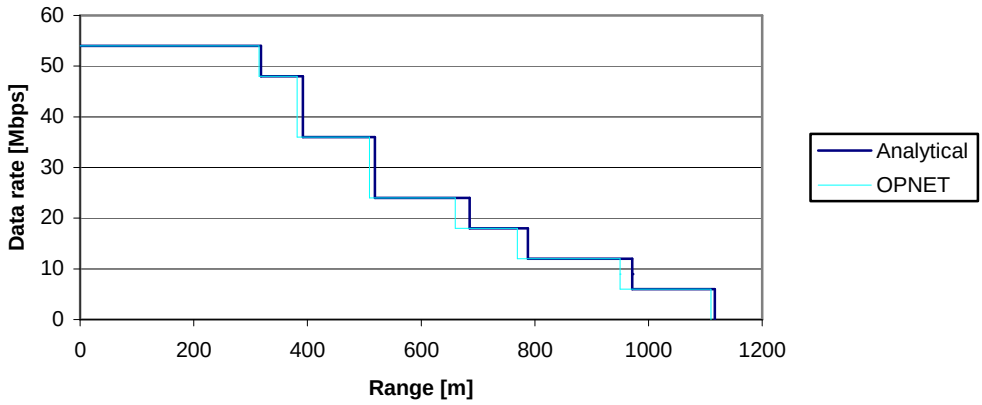


Figure 3.3. Log-Normal Shadowing Propagation Model, for 802.11a.

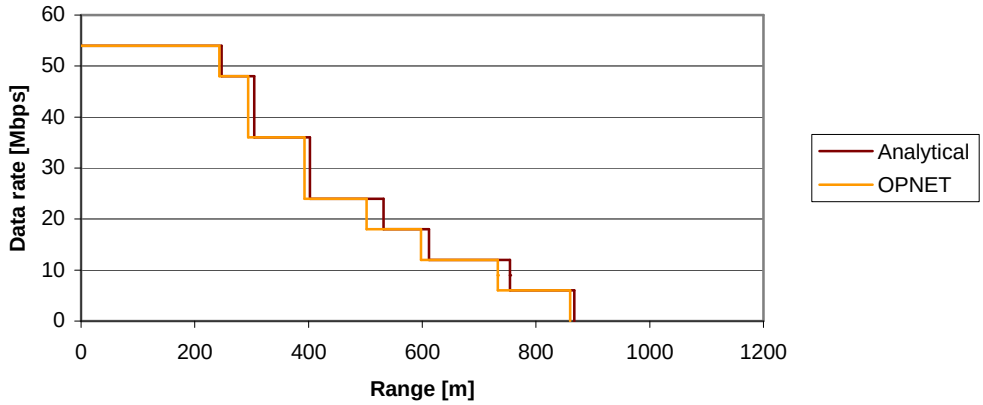


Figure 3.4. Log-Normal Shadowing Propagation Model, for 802.11g.

It is important to say that, in general, at parity of transmission power and sensitivity, 802.11g allows to reach distances longer then 802.11a, because 802.11g works with lower frequencies than 802.11a. Figure 3.3 and Figure 3.4 show the maximum coverage range values for each data rate, but, in some cases, it was necessary to reduce the values of the transmission power to build a coverage network with non-overlapped areas to avoid interference problems.

To do all the simulation it was used a Fujitsu Siemens AMILO M1450G with Intel Pentium M processor at 1.60 GHz and 1.23 GB of RAM at 1.60 GHz. The total time to do all the simulation was 239 h 32.

Chapter 4

Scenarios and Results

A Basic Scenario is studied in the beginning to understand the behaviour of a network that is possible to implement in a campus. FTP and VoIP are studied, given their different kind of applications. Then, the Campus Scenario is analysed, for HTTP, FTP, E-mail, and VoIP applications.

4.1 Scenarios description

4.1.1 Basic Scenario

The first step during network analysis is the study of the maximum user throughput available in a multihop network. Figure 4.1 shows a simple network topology with two nodes (1 and 2) that have the same offered load sent to the gateway.

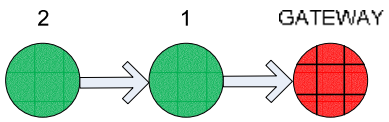


Figure 4.1. Fairness study of a two-node network.

The second step is the study of a basic scenario, which consists of a circular area with a radius of more or less 900 m. To cover this area, which contains only one internet gateway situated its centre, it is possible to use several topologies. The goal is to compare the performance of an ESS of one AP, with an ESS with several MAPs (1, 2, 3, and 4 rings topologies) connected via a WDS, using the cluster solution. In particular, 802.11g was used for the BSS and 802.11a for the WDS.

The idea is to increase the density of MAPs, which is related to the data rates and the coverage areas. Four solutions are proposed, and Table 4.1 showing the mains characteristics, where R_{BSS} is the BSS data rate, and R_{WDS} is the WDS data rate.

Table 4.1. Characteristics of the various topologies.

RINGS	# BSS	R_{BSS} [Mbps]	BSS Radius Coverage [m]	R_{WDS} [Mbps]	WDS Radius Coverage [m]
1	1	6	900	-	-
2	7	48	300	24	680
3	19	54	180	48	390
4	37	54	130	54	310

Before describing these topologies, it is necessary to address the interference problem. In fact, for a given transmission range, the interference range is more or less the double of the transmission one. A way to reduce the interference between devices is to use a different channel allocation. For example, in the BSS the reuse of the non-overlapping channels is possible, which in 802.11g standard are the 1, 6, and 11. The

solution consists of not using the same channel for neighbour cells. As a graphic representation of the different channels used in the areas to cover, different colours are used in what follows.

The first topology is the classical WLAN solution, where a single AP covers the entire region under study. It is used as a reference scenario, for comparison with the introduction of MAPs. To cover the region under study, of 900 m radius, Figure 4.2, the possible data rate for 802.11g is 6 Mbps for the BSS, which guarantees the required coverage. This range, shown also in Figure 3.4, is computed with the values shown in Table 3.1and Table 3.2.

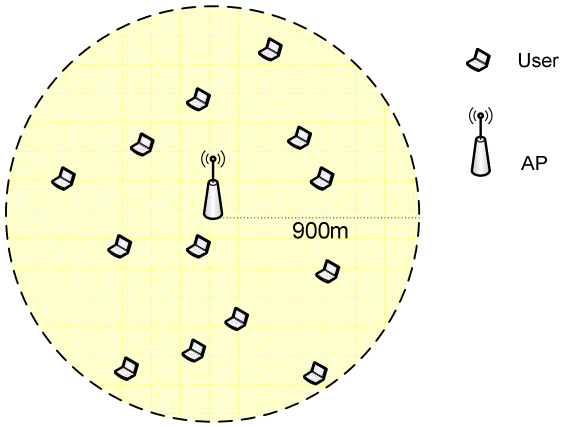
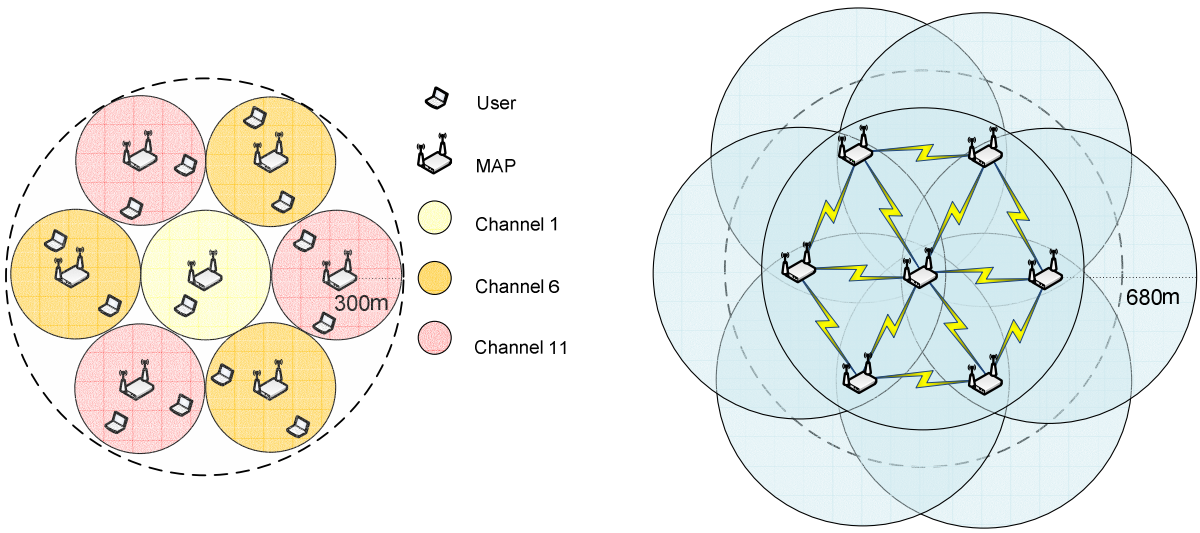


Figure 4.2. Topology with only one MAP – BSS coverage.

The second topology uses 7 MAPs to cover the same area, Figure 4.3. With 802.11g at 6 Mbps, it is possible to cover the whole area, but the lower data rate does not guarantee a good performance. To build this cluster using 7 MAPs, one has to consider that the BSS radius coverage of one single cell has to be 1/3 of the previous radius.



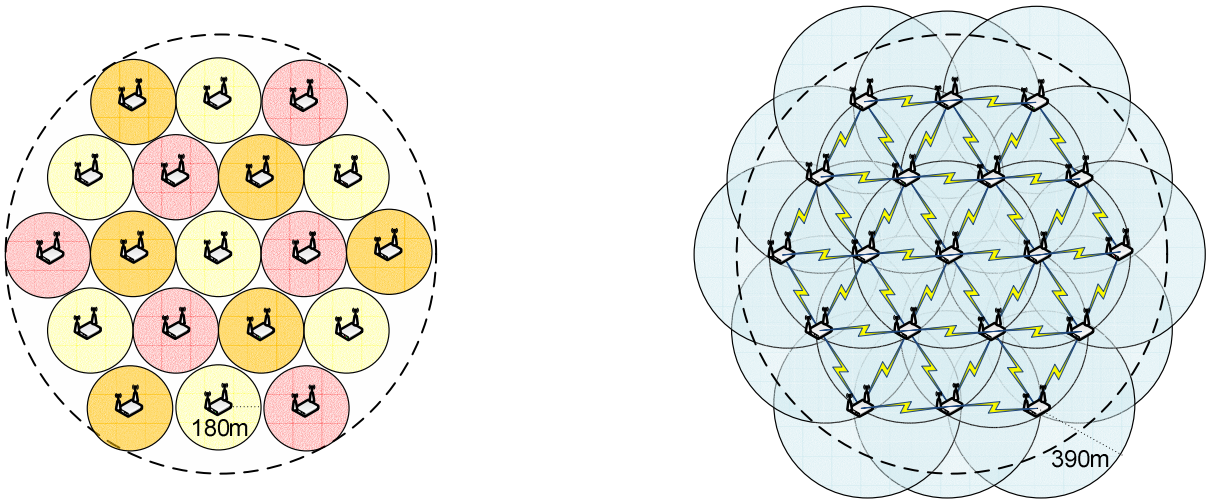
(a) BSS coverage. (b) WDS coverage.

Figure 4.3. Cluster of 7 MAPs – BSS and WDS coverage.

Using the transmission power and sensitivity in Table 3.1 and Table 3.2, it is possible to use a BSS at 48

Mbps, which allows a radius coverage of 300 m. In this case, the distance between two MAPs is of 600 m, and to guarantee that these MAPs are in radio visibility, it is necessary to use, for the WDS, a radius coverage better than 600 m. The first possibility to do it, is to use the 802.11a at 24 Mbps, which provides a radius coverage of 680 m. This topology is a WMN, in which each MAP can communicate with neighbour MAPs. The MAP that is also a Mesh Portal (MPP) has to communicate with a lot of MAPs, and this decreases the performance of the WMN. If there are more portals as possible gateways to the internet, performance will increase.

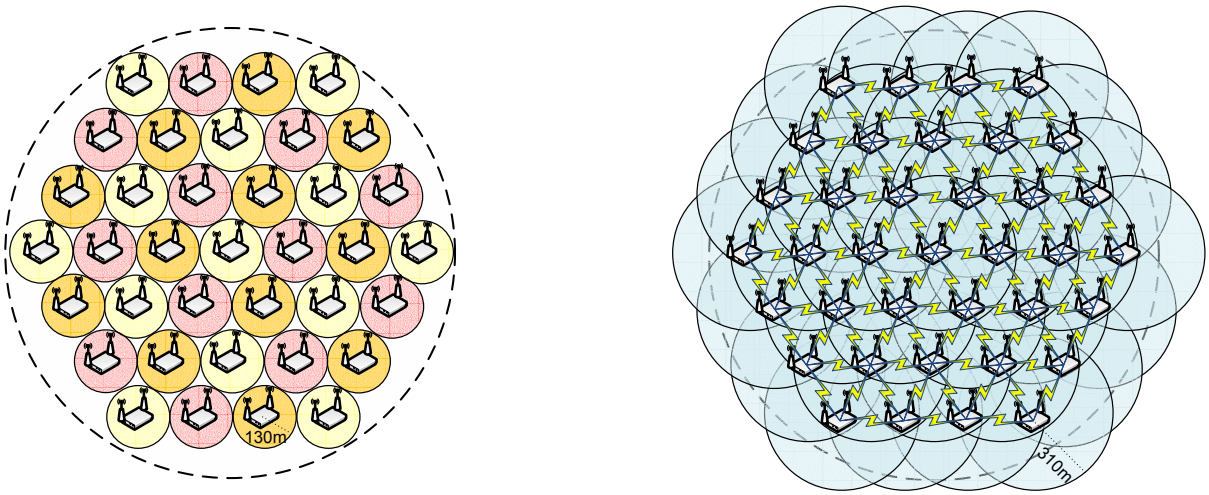
The third topology is shown in Figure 4.4, which contains 19 MAPs. In this case the access network is provided by 802.11g at 54 Mbps, and for the backhaul the 802.11a is used at 48 Mbps. To cover the area, using BSSs at 54 Mbps, without overlapped BSS areas it is necessary to reduce the MAP transmission power for the access network. By decreasing the transmission power from 20 to 15.5 dBm, it is possible to do non-overlapped BSS areas, the transmission range reducing from 250 to 180 m. To allow radio visibility between two MAPs, it is necessary to reach a coverage distance better then 360 m and so it is possible to use a WDS that works at 48 Mbps, which provides a radius coverage of 390 m.



(a) BSS coverage. (b) WDS coverage.

Figure 4.4. Cluster of 19 MAPs – BSS and WDS coverage.

The last topology, shown in Figure 4.5, uses the same data rate of 54 Mbps for BSS and WDS. In this case, it is necessary a distance between two MAPs less then 310 m, which is the maximum radius coverage for the WDS at 54 Mbps. To cover the area without overlapped BSS areas, it is necessary to decrease the BSS transmit power from 20 to 11 dBm because, the range coverage for 802.11g at 54 Mbps is of 130 m, thus, 37 MAPs are necessary to cover the whole area.



(a) BSS coverage. (b) WDS coverage.

Figure 4.5. Cluster of 37 MAPs – BSS and WDS coverage.

4.1.2 Campus Scenario

One of the main differences between the Basic Scenario and the Campus Scenario is that in the latter there are four types of services: HTTP, FTP, E-mail, and VoIP. Thus, there is a realistic traffic mix that, in a Campus Scenario, is distributed as shown in Figure 4.6.

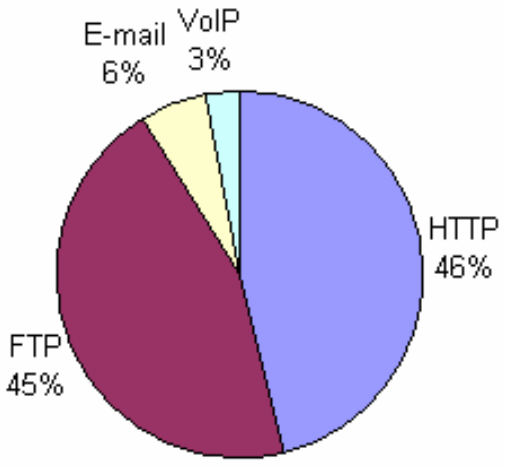


Figure 4.6. Services Distribution.

Another difference between the Basic and the Campus Scenarios is that in the latter data rates of BSS and WDS are always of 54 Mbps. This is possible because the Campus Scenario is deployed in an area of 400 m^2 and so, by reducing the BSS transmission power to avoid interference, it is possible to cover the whole campus area maintaining a high data rate.

The implemented topologies are three: 2, 3, and 4 rings, Figure 4.7, Figure 4.8, and 4.9.

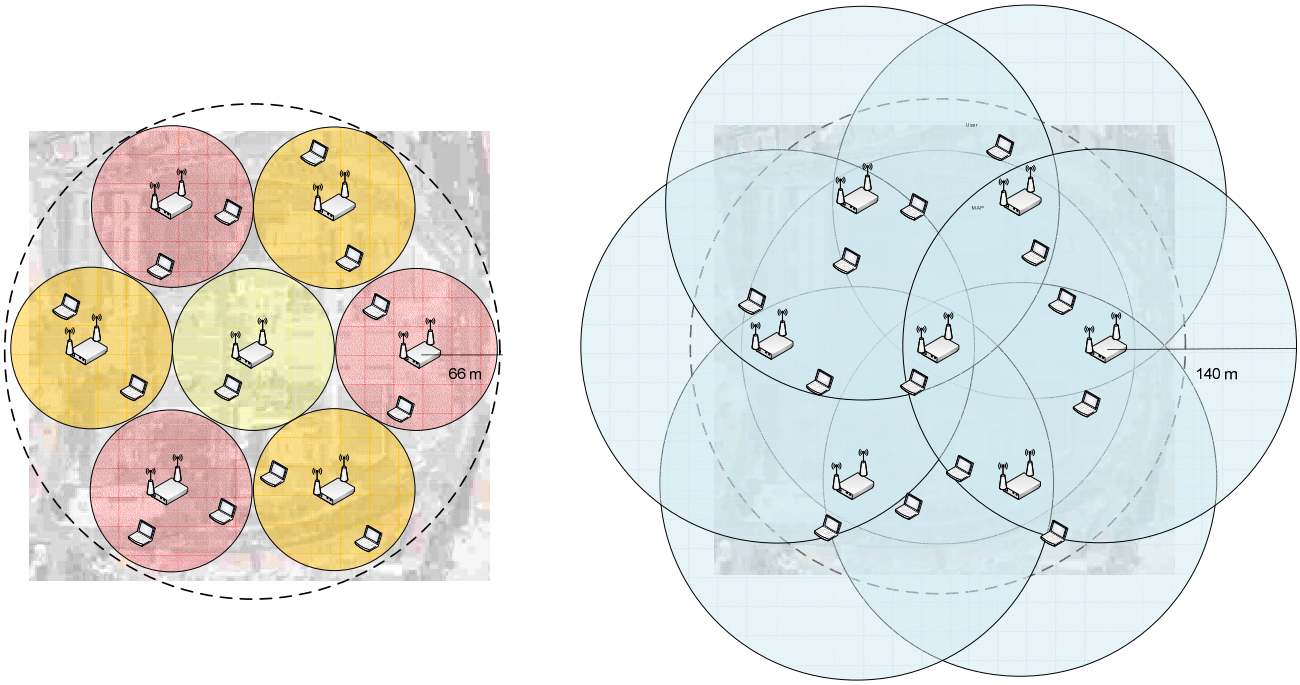


Figure 4.7. Campus Scenario – 2 rings topology.

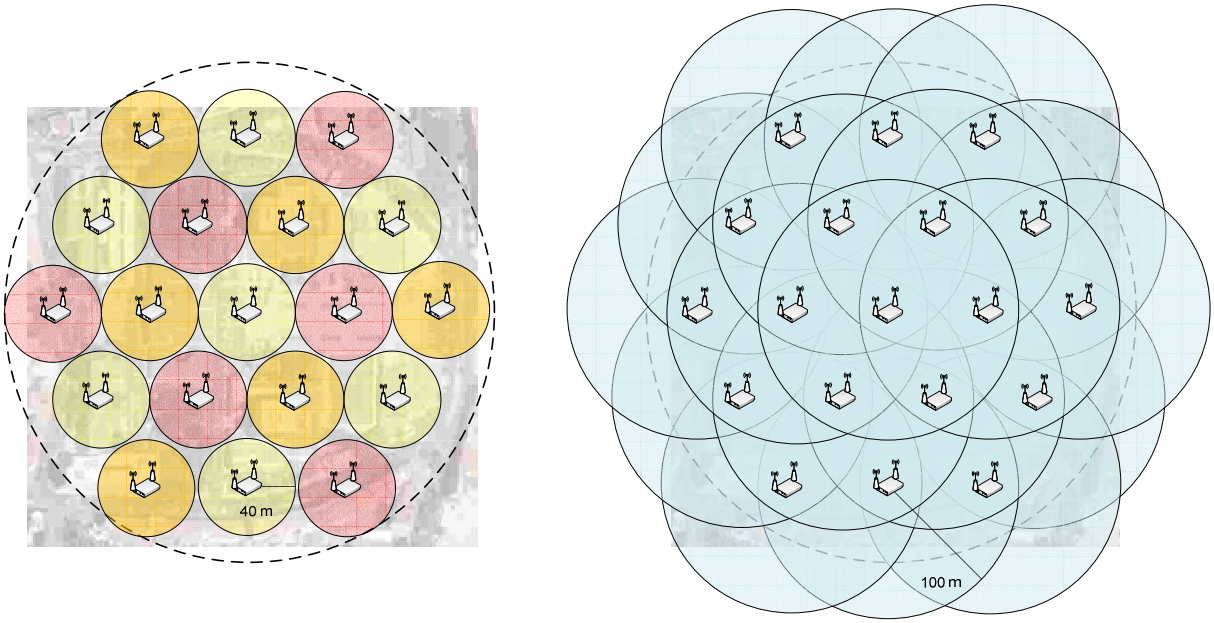


Figure 4.8. Campus Scenario – 3 rings topology.

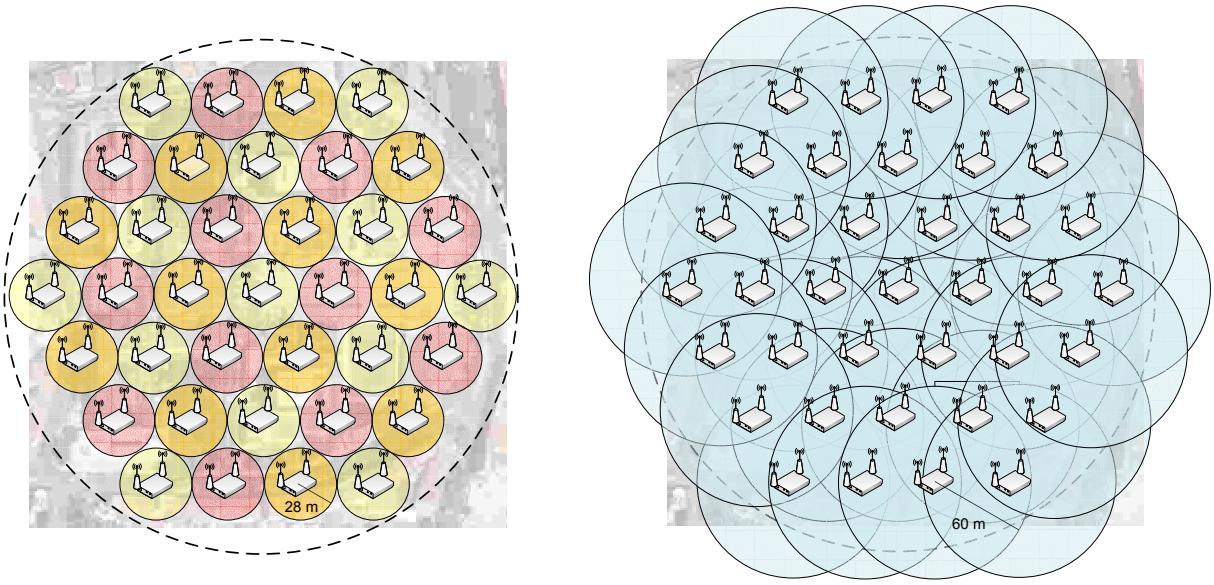


Figure 4.9. Campus Scenario – 4 rings topology.

The last difference between the Basic and the Campus Scenarios is that in the latter users do not transmit their data simultaneously only one time but they use profiles with different time behaviours, Table 4.2.

Table 4.2. Campus User Profile.

	HTTP	**FTP**	**E-mail**	**VoIP**
Operation Mode	Serial (Ordered)			
Start Time [s]	Uniform (0, 120)			
Profile Inter-repetition Time [s]	None			
Profile Number of Repetitions	None			
Duration [s]	End of Profile	End of Profile	End of Profile	Constant (100, 140)
Inter-repetition Time [s]	Exponential (600)			
Number of repetitions	Unlimited			

Once the scenario is defined, it is necessary to evaluate the simulation time and how many simulations must to done to have stable results, in order to have some statistical relevance. To do so, 10 different seeds for each scenario are performed, and simulations of one hour system are performed. Moreover, the first 5 minutes of each simulation are discarded, corresponding to the simulator set up time.

There are 74 users with uniform distribution on the area.

Table 4.3. Implementation Model for the Campus Scenario - Default setting.

RINGS	# BSS	# of user per BSS	R_{BSS} [Mbps]	BSS Radius Coverage [m]	R_{WDS} [Mbps]	WDS Radius Coverage [m]
2	7	10.57	54	66	54	140
3	19	3.89		40		100
4	37	2		28		60

4.2 Analysis of the Basic Scenario

4.2.1 Maximum throughput

In the analysis of the maximum throughput that a user can achieve in a two-node network, shown in Figure 4.1, only two users are in the network, each one downloading a file using FTP. One user is at one hop from the gateway, whereas the second one is at two hops. The study consists in the analysis of the user throughput, R_U , increasing the file size. The BSS data rate and the WDS data rate are the same at 54 Mbps.

As mentioned in Section 3.2.3, there is a Theoretical Maximum Throughput, TMT, that is of 17.4 Mbps when both data rates are of 54 Mbps, and an MMS of 536 bytes is used. This MMS value represents the default in OPNET Modeler. Ideally, as the load increases, both nodes have the same R_U , but, in practice, the user closest from the gateway (user 1) is in advantage to the other user (user 2), Figure 4.10. Only with low values of file size (up to 1 MB) both users have the same throughput, whereas for file sizes over 1 MB the absence of fairness mechanism causes a different performance for each user, benefiting the one hop user. Moreover, it is interesting to see how the throughput of the user closest to the gateway tends to the theoretical maximum value when increasing the file size.

Finally, it is possible to conclude that, in a network without fairness mechanism, traffic load influences network capacity. This is the consequence of the fact that 802.11a/g were not created to work in multihop wireless networks.

14 simulations of 10 minutes were done and for each simulation 10 different seeds were simulated. The average time to do all these simulation was 11h 37.

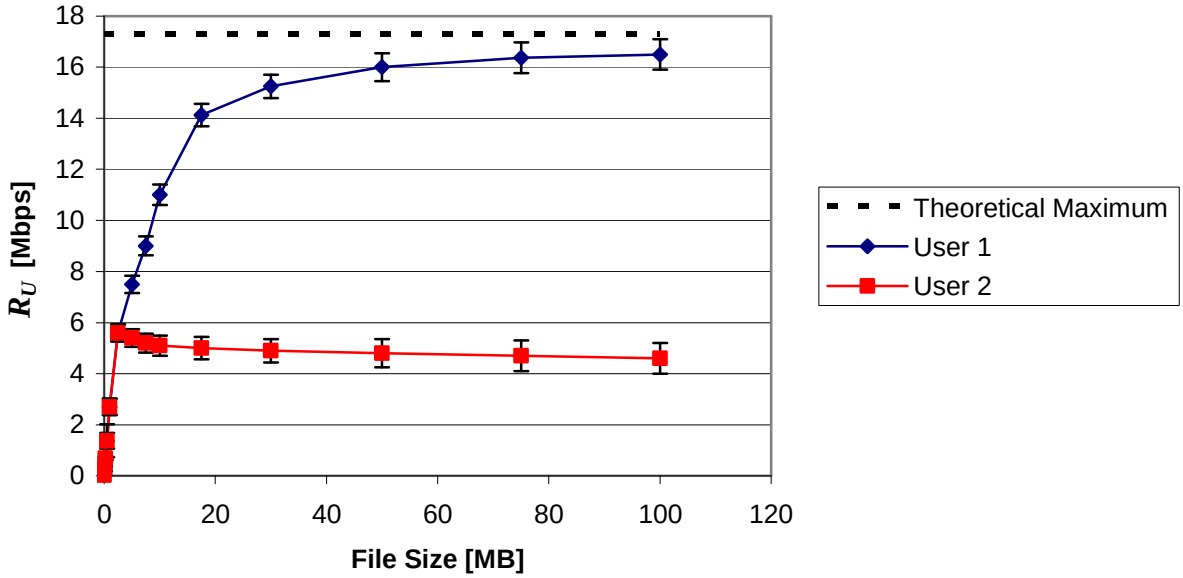


Figure 4.10. User throughput behaviour for a two-node network.

4.2.2 FTP single service

To analyse the network behaviour, one studied the FTP average throughput of all the users in the network, R_A. The hypothesis are that each user starts the file download more or less simultaneously with the others users, and that the file size is fixed and equal for users. R_A is computed as the ratio between the file size and the average time of download for all the users. For each configuration, 10 simulations of one hour were performed. The total time to do these simulations was 32h 30.

The effect of increasing the density of MAPs was studied. A configuration of 37 users was considered, with uniform distribution on the area, and a file size of 25 MB. Table 4.4 shows the results relative to the throughput, in terms of global average of all users, and of 1, 2, 3 and 4 hops, whereas Table 4.5 shows the FTP file download times. N_u is the average number of users per BSS.

Table 4.4. Simulation results – Average user throughput.

Ring	# MAPs	R_{BSS} [Mbps]	R_{WDS} [Mbps]	N_u	R_A [Mbps]				
					Global Average	1 hop	2 hop	3 hop	4 hop
1	1	6	-	37	0.129	0.129	-	-	-
2	7	48	24	5.3	0.616	1.852	0.426	-	-
3	19	54	48	1.9	0.620	2.315	0.988	0.282	-
4	37	54	54	1	0.549	2.778	1.466	0.434	0.175

Table 4.5. Simulation results – FTP download time.

Ring	FTP Download time [min]				
	Global Average	1 hop	2 hop	3 hop	4 hop
1	27.0	27.0	-	-	-
2	7.0	1.8	7.9	-	-
3	8.7	1.5	3.4	12.0	-
4	12.4	1.2	2.3	8.0	19.8

In Figure 4.11, one shows the average throughput R_A in each topology for each hop. The small standard deviation represents a good confidence around the values obtained. It is easy to understand that when only one AP (1 ring topology) is used performance is the worst. In fact, in this case, the low data rate of 6 Mbps is not sufficient to provide the adequate capacity to all users. Moreover, one has to consider that users have to contend the wireless access to only one BSS. These two factors cause a high network latency, *i.e.*, to download the file of 25 MB each user spends an average time of 27 minutes. So, the topology with only one AP to cover all the area is not a good solution.

With the 2 rings topology, there are performance improvements. Using this solution, we have a two hops network, but, the increment of the BSS data rate from 6 Mbps to 48 Mbps allows a capacity improvement. As the BSS data rate increases 8 times, one hop users throughput increases 14 times relative to the 1 ring topology. This is the positive consequence of the drastically reduction on the average number of users per BSS, from 37 in the 1 ring topology to 5.3 in the 2 rings one. One hop users can download the file in an average time of 1.8 minutes.

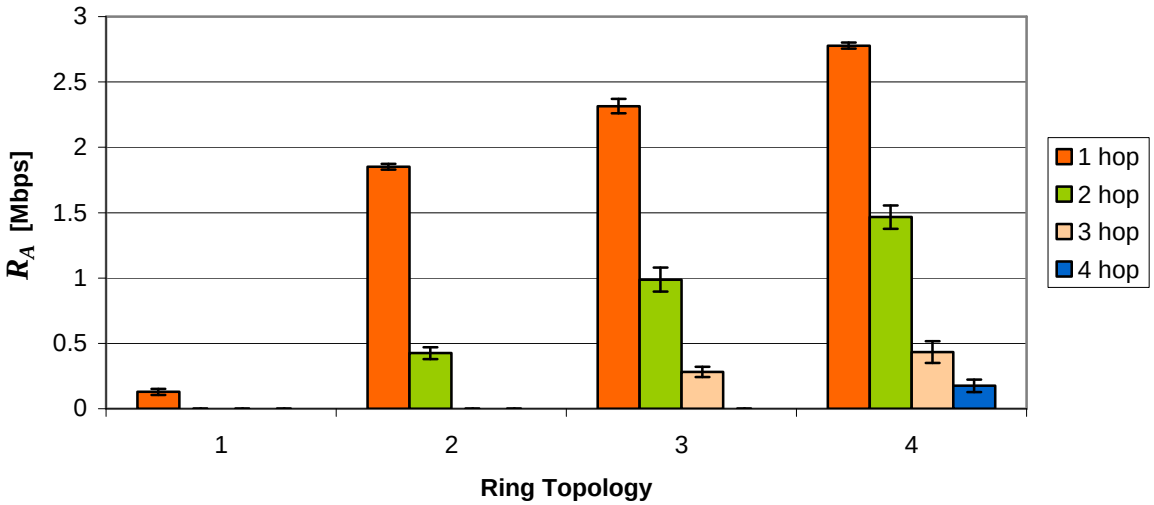


Figure 4.11. FTP average user throughput – Hop study.

Two hops users in the 2 rings topology have a lower throughput compared to one hop users, but, their throughput is better than the 1 ring users throughput. This throughput reduction is a consequence of the

lack of fairness management in the network; there is no equal performance among users closest to the gateway and others at two hops. On average, the download time for two hops users is 7.9 minutes.

In the 3 rings topology, the BSS data rate increases from 48 to 54 Mbps, while the WDS data rate goes from 24 to 48 Mbps. Relative to the 2 rings topology, one can observe that there are now better values of throughput as a consequence of the BSS and the WDS data rates increment. Moreover, the average number of users per BSS is 1.9, and so the medium access contention is relaxed. The 1, 2, and 3 hops users can download the file in 1.5, 3.4, and 12 minutes respectively. The 3 hops users have a low throughput, but it is greater than the throughput in 1 ring topology.

The 4 rings topology allows to reach a high throughput only by changing the WDS data rate from 48 to 54 Mbps, keeping the BSS data rate at 54 Mbps. There is a good performance for 1 and 2 hops users, and acceptable performance for 3 hops users, but 4 hops users have a low throughput comparable to 1 ring one. The download times are 1.2, 2.3, 8, and 19.8 minutes for 1, 2, 3, and 4 hops users respectively.

Figure 4.12 shows the R_A trend for each ring topology, as a function of the number of hops. In the 1 ring topology, only one point can be determined, because only one hop users exist. Generally, R_A decreases when the number of hops increases, and, as said previously, this is the consequence of the lack of fairness mechanisms.

The distinction between 3 and 4 rings topologies resides only in the WDS data rate (from 48 Mbps in 3 rings to 54 Mbps in 4 rings), while the BSS data rate is 54 Mbps. As consequence, one can see that the curves that represent the 3 rings and the 4 rings trends are parallel to each others. Moreover, once fixed the number of hops, the throughput increases for an increasing the number of MAPs, because there is data rate improvement.

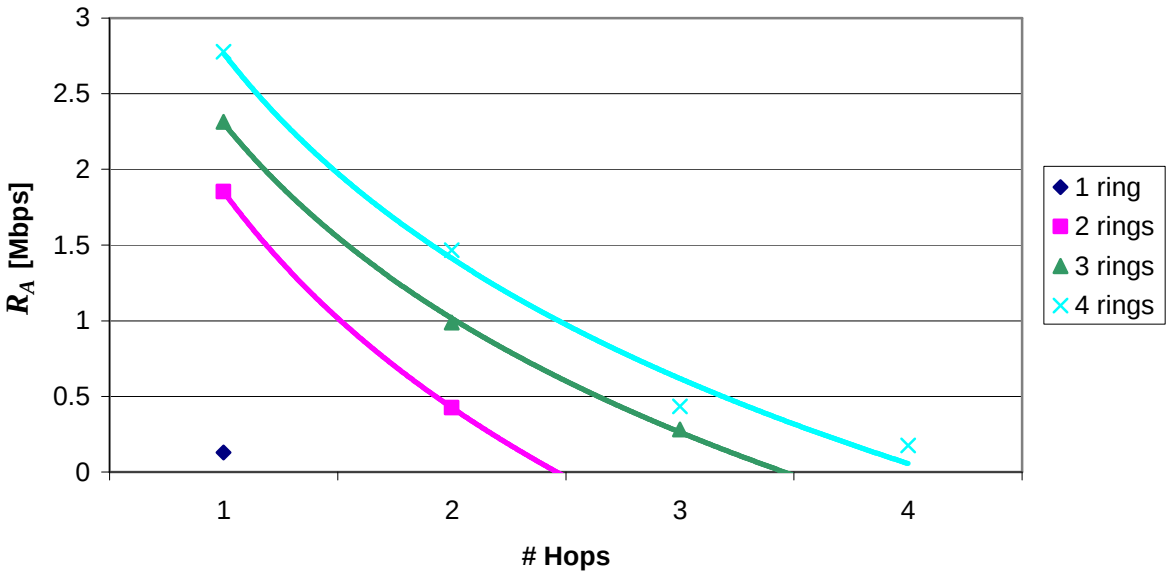


Figure 4.12. Trend of the FTP average user throughput – Hop study.

Table 4.6 shows the trend equations, and the values of the correlation coefficient, R^2, in each topology, relatively to average user throughput. One can see that there is a logarithmic trend, with a correlation coefficient that decreases when the number of rings increases.

Table 4.6. Trend equations and coefficient correlations – Average user throughput.

Rings	Equation	R^2
2	-2.057ln(x) + 1.852	1.0000
3	-1.857ln(x) + 2.304	0.9994
4	-1.955ln(x) + 2.767	0.9878

Figure 4.13 shows R_A for all 37 nodes in each topology. This figure allows to understand which is the average level of capacity provided by each topology. One has to consider that, by increasing the number of rings, most users will be situated in the lasts rings, as shown in Table 4.7.

Table 4.7. Average users per BSS at 1, 2, 3, and 4 hops.

Rings	Average users per BSS			
	1 hop	2 hops	3 hops	4 hops
1	37	-	-	-
2	5.3	31.7	-	-
3	1.9	11.7	23.4	-
4	1	6	12	24

It is possible to see that, relatively to the 1 ring topology, the throughput in 2 and 3 rings topologies increases because the BSS and the WDS data rates increase. In 2 and 3 rings topologies, users have, on average, more or less the same throughput. As shown in Figure 4.11, the 1 and 2 hops users in the 3 rings topology have a throughput better then similar users in the 2 rings topology, whereas the 3 hops users in the 3 rings topology have more or less the same throughput of 2 hops users in the 2 rings topology. In the 4 rings topology, there are a lot of users at 4 hops from the gateway, and the consequence is that the global average FTP user throughput in the 4 rings topology is lower than in 2 and 3 rings topologies.

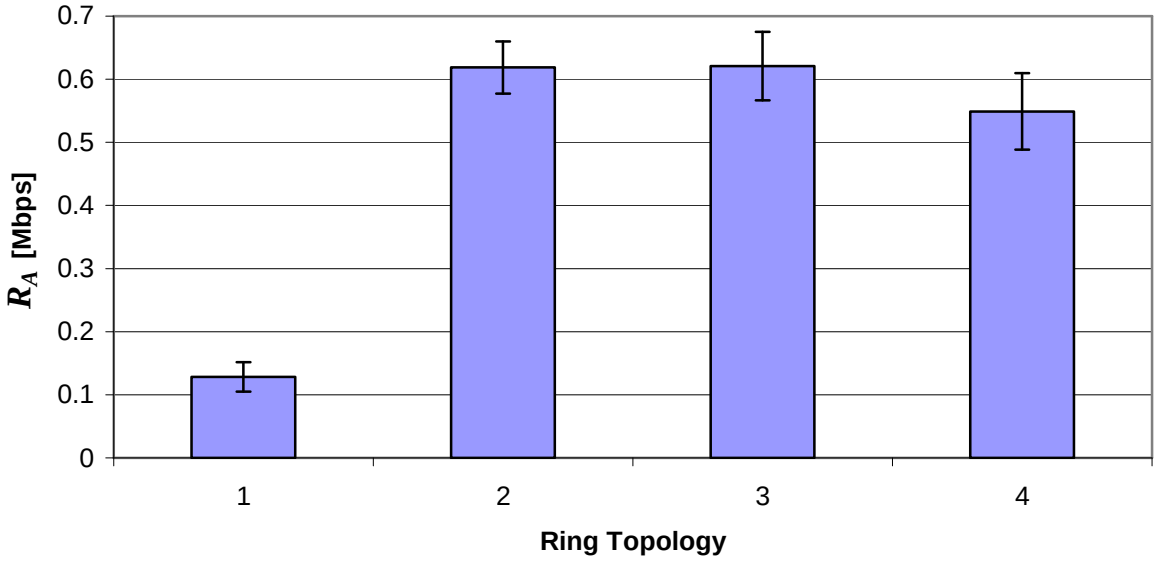


Figure 4.13. Global FTP average user throughput for each topology.

Another interesting result is shown in Figure 4.14, which represents the ratio between the global average throughput over the BSS data rate in each scenario (see Table 4.1). This representation, in fact, allows to see that the network usage, in terms of throughput, decreases when one changes topology from 1 to 4 rings.

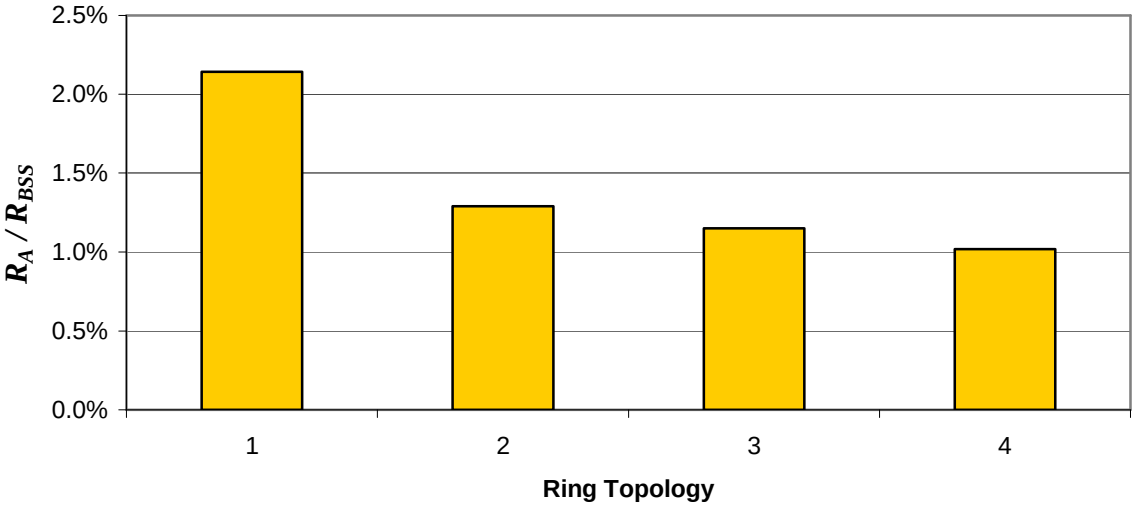


Figure 4.14. Global FTP average user throughput over BSS data rate for each topology.

So, concerning the FTP single service in the network, one can conclude that the kind of topology that it is possible to choose depends on the capacity that one wants to provide to users. For example, as one can see in Table 4.5, if each user has to download a file of 25 MB in a maximum time of 8 minutes the only solution is the 2 rings topology, whereas, if one can wait until 12 minutes it is also possible to choose the 3 rings solution.

It is interesting to see the traffic in the TCP layer, to understand how users communicate along time. Figure 4.15 shows the TCP traffic of four users, being possible to see the communication of the various users is

simultaneous.

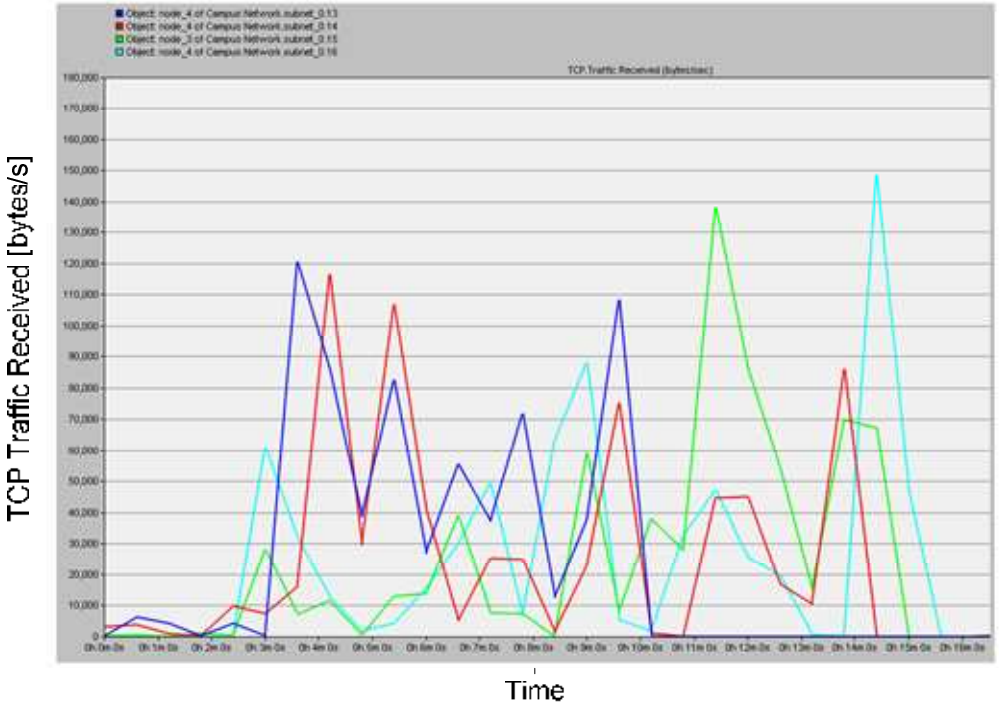


Figure 4.15. TCP traffic of four simultaneous users.

4.2.3 VoIP single service

The main parameter to evaluate the performance in a voice application is the Voice Packet End-to-End delay, E_{VPD}. This delay is caused by processing in the endpoint equipment (and in the network), the collection of voice samples to implement voice compression, and the collection of voice (compressed or uncompressed) into network packets. VoIP can not tolerate high delays; in fact, E_{VPD} has to be less than 400 ms, preferably under 150 ms.

Two different studies were done: the first one consists of the Voice Packet End-to-End delay analysis, for each topology, fixed the number of users, whereas the second study consists of finding the maximum number of simultaneous VoIP users, N_{SV}, in each topology. Simultaneous calls of one minute were simulated, and for each topology 10 seeds were run. To do the first study 7h 18 of simulations were spent, whereas 41h 48 for the second simulation set were used.

Figure 4.16 shows the average E_{VPD} per hop, when there are 34 users. With this high number of users in the network, it is possible to use VoIP only in the 2 rings topology (E_{VPD} is less then 400 ms for all users); in fact, in the others solutions, it is practically impossible to use VoIP, because there are delay very high. With only one AP, the E_{VPD} reaches 1.6 s, a totally unacceptable value, as it is for 2 and 3 hops users in the 3 rings topology, 2, 3, and 4 hops users in the 4 rings topology. It is also interesting to see that in the 2 rings topology there is not a lot of differences of Voice Packet End-to-End delay between 1 and the 2 hops users. It is possible to interpret this behaviour considering that when there are users at 3 or more hops, then

traffic determines an accumulation of voice packets in the buffer of the 2 hops MAPs, creating high delay values.

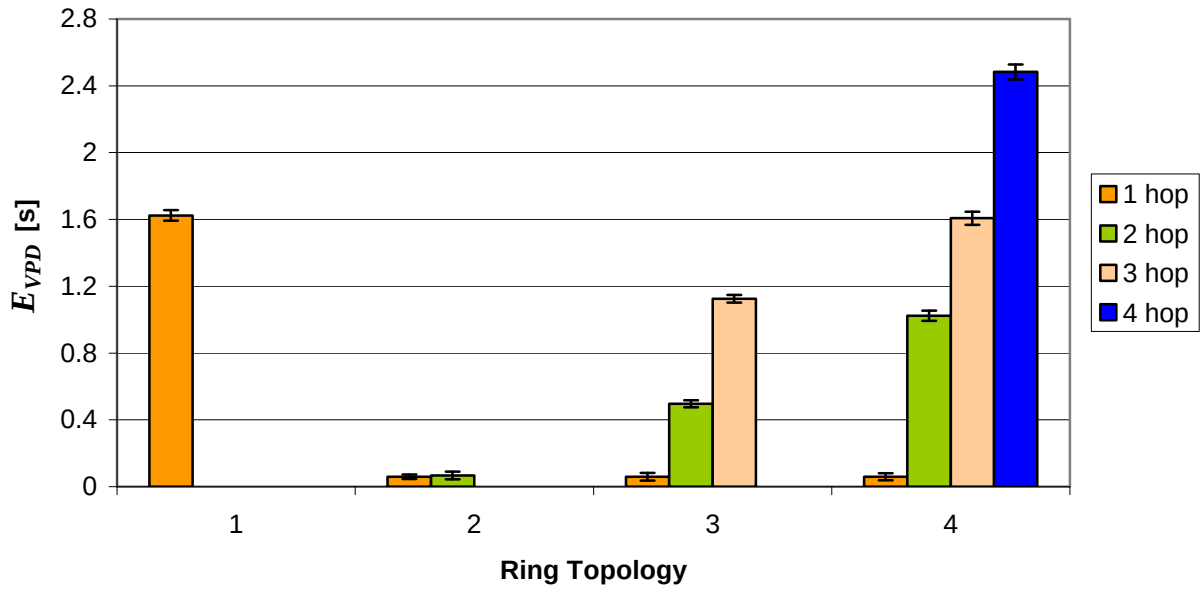


Figure 4.16. Average Voice Packet End-to-End delay for each topology.

Figure 4.17 shows the E_{VPD} trend for each ring topology, when the number of hops increases. There is only one point in the 1 ring curve, because there are only one hop users. One can see that, for a certain number of hops, E_{VPD} in the 4 rings topology is higher than in the 3 rings one, and so on. Only the 1 hop E_{VPD} is more or less equal in 2, 3, and 4 topologies, whereas it is unacceptable in the 1 ring one.

So, when there is a high number of MAPs, network performance, in terms of Voice Packet End-to-End Delay, decreases.

Figure 4.17. Trend of the average End-to-End Delay – Hop study.

Table 4.8 shows the trend equations and the values of the correlation coefficients, in each topology, relatively to Voice Packet End-to-End Delay.

Table 4.8. Trend equations and coefficient correlations – Voice Packet End-to-End Delay

Rings	Equation	R^2
2	$0.06\ x^{0.1462}$	1.0000
3	$0.06\ x^{2.7074}$	0.9901
4	$0.08\ x^{2.6879}$	0.9252

It is also interesting to compare the results from the simulations with the analytical approach provided in Section 3.2.2. In fact, considering, *e.g.*, the results from the 4 rings topology, the E_{VPD} in 1 hop users is more or less 60.20 ms. The analytical value of the network delay, D_{NET}, for this kind of network, is of more or less 170 µs. Considering a voice payload of 20 bytes, and the values of D_{ENtx}, D_{DErx}, D_{COtx}, and D_{DCrx}, provided in the Annex, than the analytical value of E_{VPD} is 60.17 ms, thus, the value from simulation compared with the analytical approach it is very similar.

Figure 4.18 shows, for each topology, E_{VPD} for all users in the network. As said previously, generally, it is practically impossible to use VoIP, excepting in 2 rings topology.

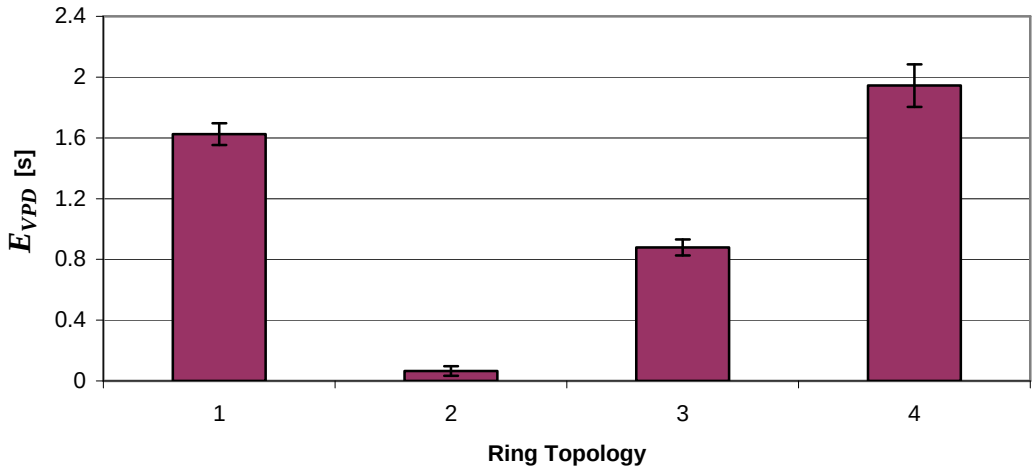


Figure 4.18. Global average Voice Packet End-to-End delay for each topology.

The second type of simulations provide the maximum number of simultaneous VoIP users, N_{SV}, in each topology, as shown in Figure 4.19. The rule to find this number is that the E_{VPD} of users with the greatest hop distance from the gateway has to be less then 400 ms. The maximum number of simultaneous VoIP users, when there is only one AP, is 24. With the 2 rings topology, it is possible to have 42 users. This improvement is due to the fact that, with this topology, there are on average 5.3 users per BSS, compared

to 37 users per BSS in the first topology. Moreover, the data rates are higher than 1 ring topology ones.

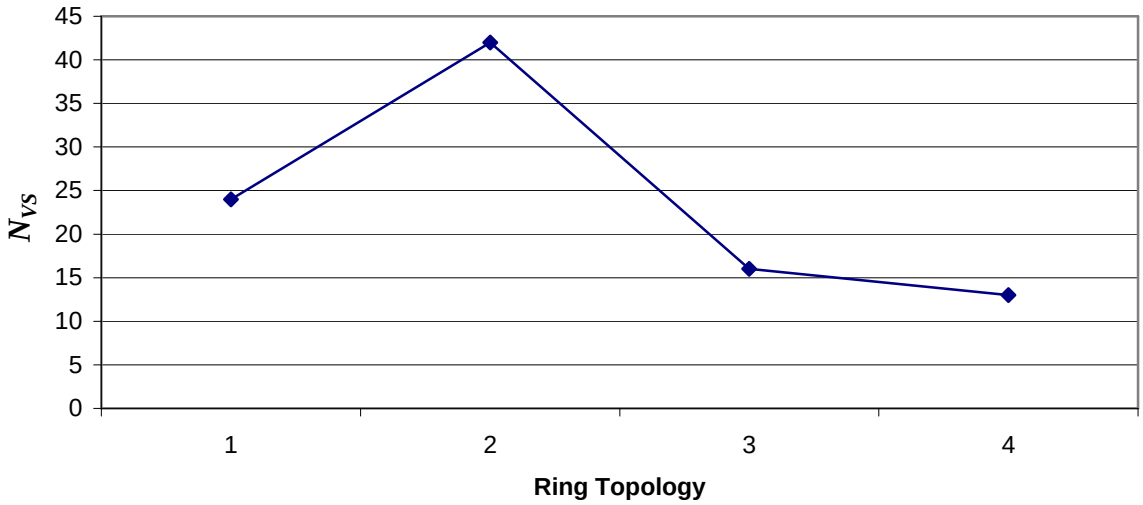


Figure 4.19. Maximum number of VoIP users in each topology.

There is no improvement in the 3 rings topology, where there are only 16 possible simultaneous calls, because 3 hops users are very penalised. With a 4 hops network, N_{SV} decreases even to 13. With the Erlang B model, is possible to estimate the maximum number of non simultaneous VoIP users; this analytical study is provided in the next section.

4.2.4 FTP and VoIP combined service

The last study of the Basic Scenario consists of the analysis of each topology, when the users give a mix of FTP and VoIP traffic to the network. In this case, it is interesting to evaluate the degradation in terms of number of possible simultaneous calls when there is an FTP traffic in background. Between these two kinds of applications, the main difference is that VoIP works wit as interactive as traffic class, whereas FTP uses the best effort traffic class. As a consequence, VoIP packets have priority relative to FTP ones, because VoIP is a real-time service.

As mentioned in the previous section, the rule to find the maximum number of simultaneous VoIP users is that the E_{VPD} for the users with the greatest hop distance from the gateway has to be less then 400 ms. Calls of one minute during an FTP download of a file of 25 MB, were simulated. To do all simulations 33h 48 were spent.

As expected, with FTP in background, the maximum number of simultaneous calls decreases. It is possible to see this decrease in Figure 4.20, which shows the comparison between N_{SV} in the network with only VoIP service and the N_{SV} in the network with VoIP and FTP combined services.

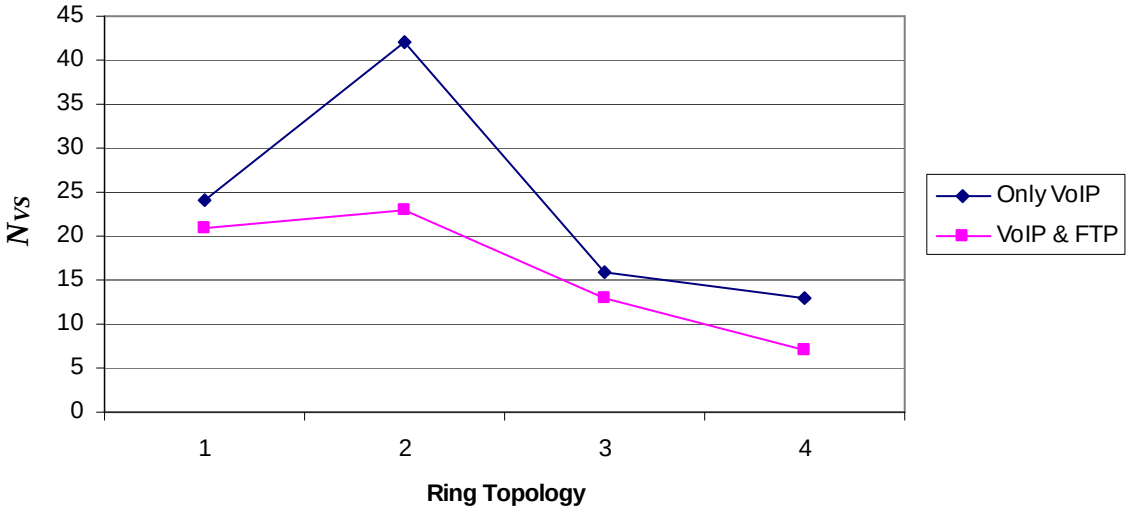


Figure 4.20. Maximum number of VoIP users with FTP traffic in background.

In the 1 ring topology, N_{SV} decreases from 24 to 21, whereas a great difference exists in the 2 rings case, where the maximum number of simultaneous VoIP users decreases from 42 to 23. In the 3 rings topology it is possible to have only 13 simultaneous calls, instead of 16. The last topology is the worst one, and, only 7 users can use simultaneously VoIP.

One idea to know a possible value of the maximum number of VoIP users, N_V, is provided by using the Erlang B model, which is an approximation to compute N_V. In fact, considering as number of resources the maximum number of simultaneous VoIP calls, and considering a probability of blocking of 1%, it is possible to compute the amount of traffic for each topology when only VoIP, or FTP and VoIP combined, are used. Then, the ratio between this traffic and the number of calls per hour is the maximum number of VoIP users, considering the Erlang B formula. It was considered that in one hour a user does one call of three minutes. In Table 4.9, one can see that it is possible to have a lot of users N_V in the network when there is only VoIP, whereas Table 4.10 shows the comparison between N_{SV} and N_V in the case there is an FTP and VoIP combined service.

Table 4.9. Maximum number of VoIP user considering the Erlang B model – Only VoIP service.

RINGS	A [Erl]	N_{SV}	N_V
1	15.25	24	305
2	30.75	42	615
3	8.85	16	177
4	6.60	13	132

Table 4.10. Maximum number of VoIP user considering the Erlang B model – FTP & VoIP combined service

RINGS	A [Erl]	N_{sv}	N_v
1	12.80	21	256
2	14.45	23	289
3	6.60	13	132
4	2.50	7	50

4.3 Analysis of the Campus Scenario

In this section, the results relative to the services mix used in the Campus Scenario are described. Totally, the time to do all simulations was 112 h 30.

Concerning the HTTP response time, RT_{HTTP}, the FTP response time, RT_{FTP}, and the E-mail response time, RT_{Email}, Figure 4.21 shows those results. As a consequence of the multihop network, it is possible to see that the RT in each application increases when the number of MAPs increases. The network in the 2 rings topology is very efficient in terms of RT; in fact, in a few milliseconds it is possible to open a web page, or to download an FTP file, or to download a E-mail. Relatively to the standard deviation, it is small in the 2 ring topology, and it become large in the last topology, because, when increasing the number of MAPs the packets can take different paths to reach the gateway, and this causes different response times.

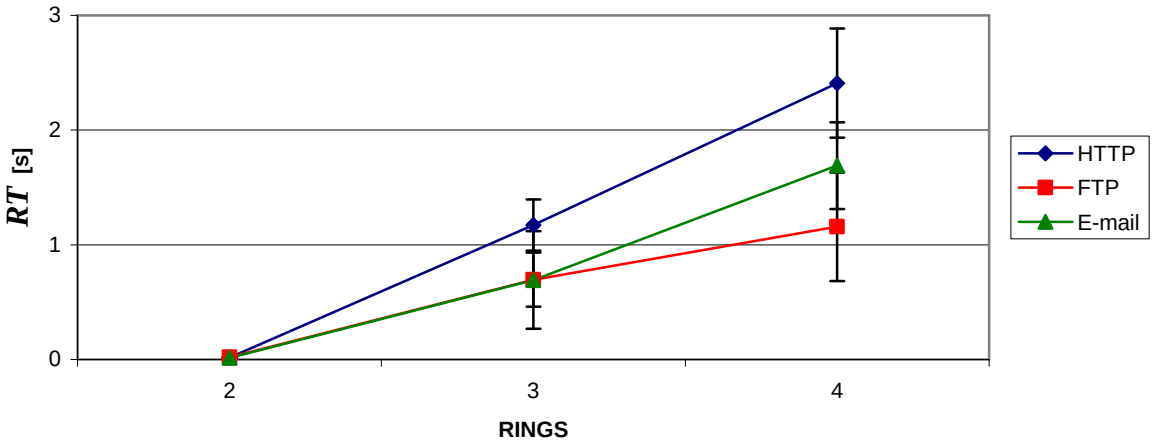


Figure 4.21. Response Time in HTTP, FTP, and E-mail applications.

Knowing that the 46% of the services are HTTP and the 45% are FTP, it is interesting to study in detail the response times for these applications. Figure 4.22 and Figure 4.23 show how HTTP and FTP response times vary, on average, for each user situated at 1, 2, 3, and 4 hops from the gateway. These figures help to explain how the multihop structure influences network performance in each ring. As previously mentioned for the Basic Scenario, users in the last rings are more penalised than the users closer to the gateway; *e.g.*,

the 4 hop users in the 4 rings topology have to wait 4.3 s to download the web page.

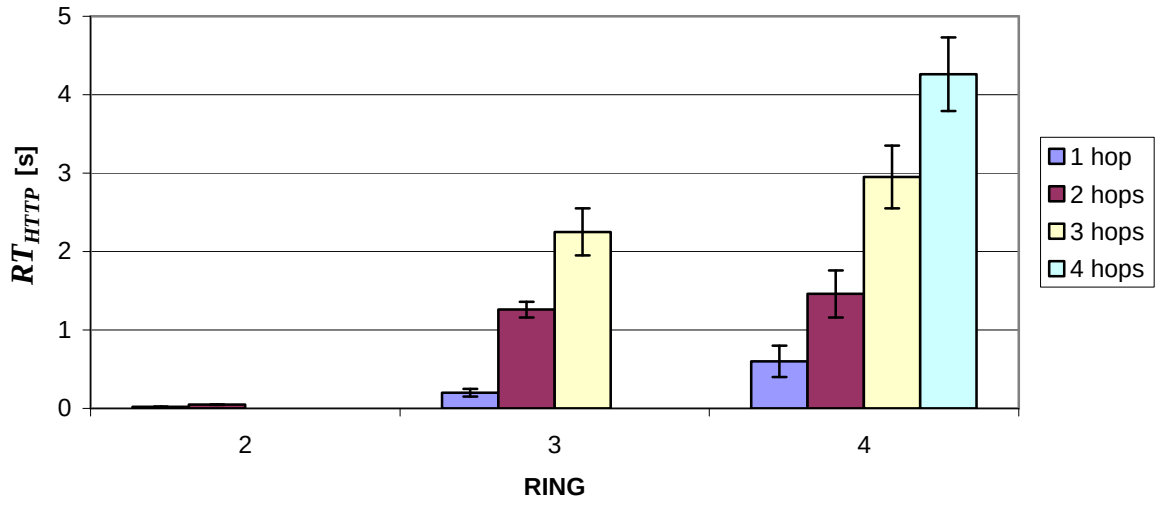


Figure 4.22. HTTP Response Time in each topology – Hop study.

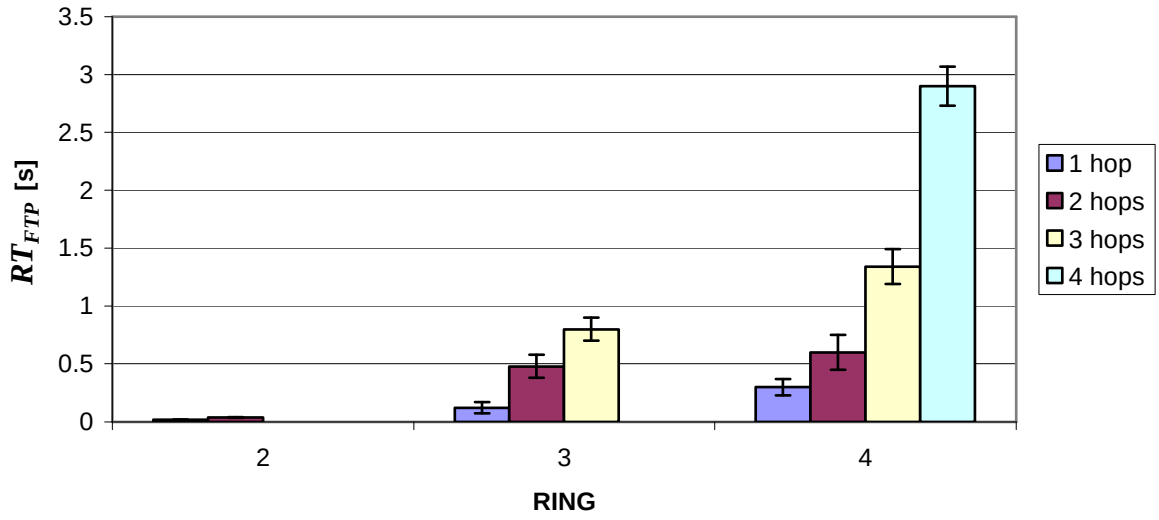


Figure 4.23. FTP Response Time in each topology – Hop study.

The RT_{HTTP} trend, expressed as function of the number of hops, is shown in Figure 4.24, while Table 4.11 shows the trend equations and the correlation coefficient, R^2. It is possible to see that, considering a certain number of hops, when the number of MAPs increases the RT_{HTTP} increases as well. Moreover, one can see the linear trend of RT_{HTTP}. Users in the 2 rings topology have excellent performance, independent of the hop distance from the gateway, whereas in 3 and 4 rings topologies only one hop users have a low RT_{HTTP}.

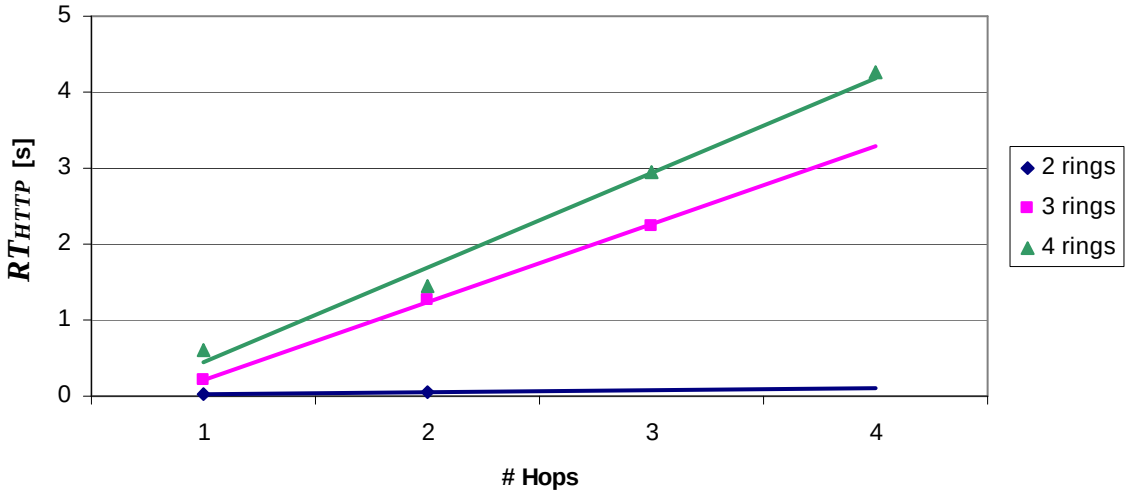


Figure 4.24. HTTP Response Time trend .

Table 4.11. Trend equations and correlations – HTTP Response Time.

Rings	Equation	R^2
2	0.027x – 0.007	1.0000
3	1.025x – 0.813	0.9996
4	1.247x – 0.800	0.9894

It is possible to see similar results also for RT_{FTP} , *i.e.*, 2 hops users have excellent performance, 3 hops users have acceptable performance, whereas 4 hops users have to wait until 2.9 s to download the file. Figure 4.25 shows as the RT_{FTP} trends are of the exponential type.

Figure 4.25. FTP Response Time in each topology trend.

It is possible to see the trend equations and the values of correlation, R^2, for the FTP Response Time in Table 4.12. One should expect this type of trend, because the RT_{FTP} is inversely proportional to the FTP throughput, R_A, studied in Section 4.2.2, which has a logarithmic trend.

Table 4.12. Trend equations and correlations – FTP Response Time.

Rings	Equation	R^2
2	$0.0084\ e^{0.7603x}$	1.0000
3	$0.0549\ e^{0.9403x}$	0.9356
4	$0.1365\ e^{0.7611x}$	0.9991

In a Campus Scenario, there is a low percentage of user that use VoIP (only the 3%), thus, as it is possible to see in Figure 4.26, the Voice Packet End-To-End Delay, E_{VPD}, is very low, providing a good quality of conversation during a call. In fact, the maximum E_{VPD} is 270 ms, thus, it is less than the threshold for an acceptable quality.

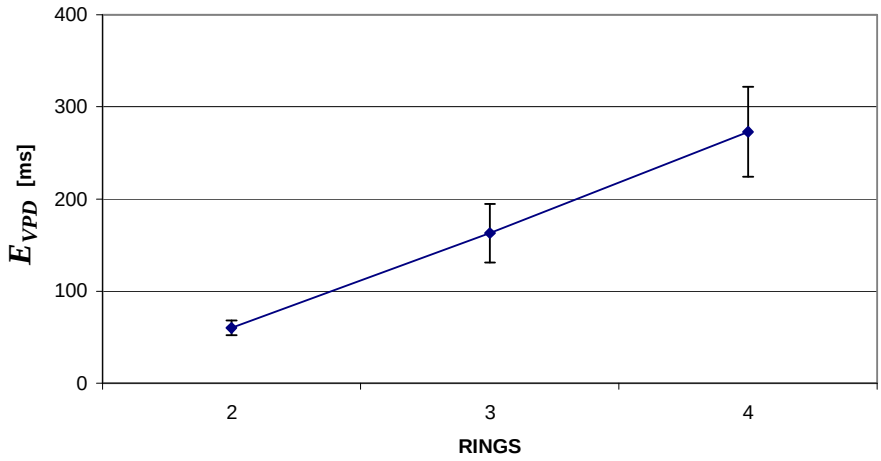


Figure 4.26. Voice Packet End-to-End Delay in each topology.

In Figure 4.27, the dropped data values, D_{DATA}, for each topology are shown. In the topology with a few number of MAPs, the data dropped values are residual, but, when the number of MAPs increases, one sees an increase in dropped data. Although the number of users per MAP decreases when the number of MAPs increases, and so there is a lower probability of access collision in the BSSs, the data dropped increases because in the WDS the number of hops that a packet can do increases, thus the probability that data are dropped increases too. It can happen because the data buffer of the higher layer is full, or because the size of the higher layer packet is greater than the maximum allowed data size defined in the 802.11 standard.

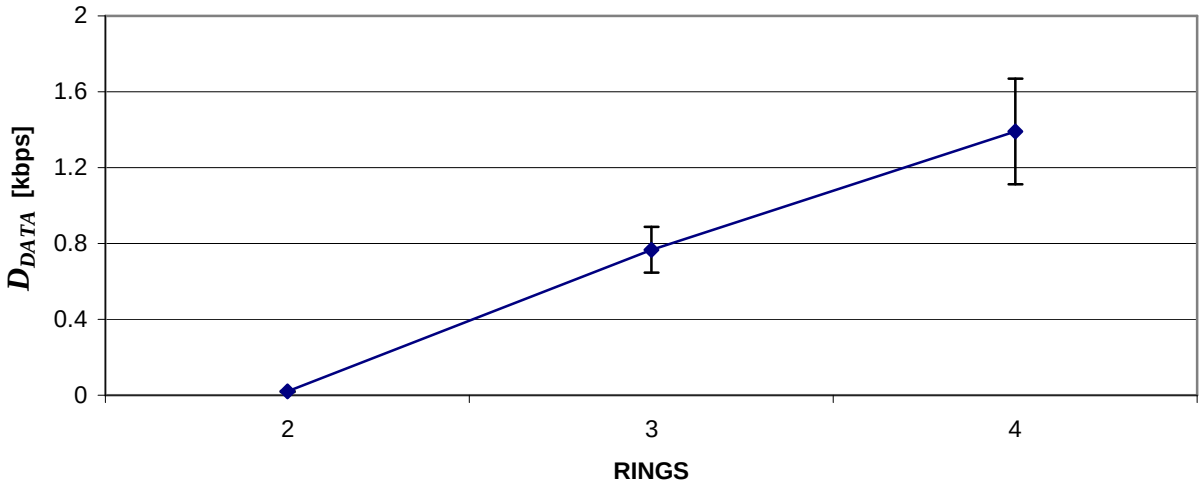


Figure 4.27. Data dropped in each topology.

Concerning the delay, the WLAN Delay, D_{WLAN}, and the Media Access Delay, D_{MAD}, were analysed, as shown in Figure 4.28. The WLAN Delay represents the End-to-End Delay of all packets received by the MACs of all nodes in the network, and forwarded to the higher layer. One can see that, varying the topology, there is only a small delay increment, and that this delay is always less than 1.5 ms. Considering the queuing and contention delays of the data, management, delayed Block-ACK and Block-ACK Request frames transmitted by all MACs in the network, it is possible to see that the maximum D_{MAD} reaches 1.7 ms, in the 4 rings topology.

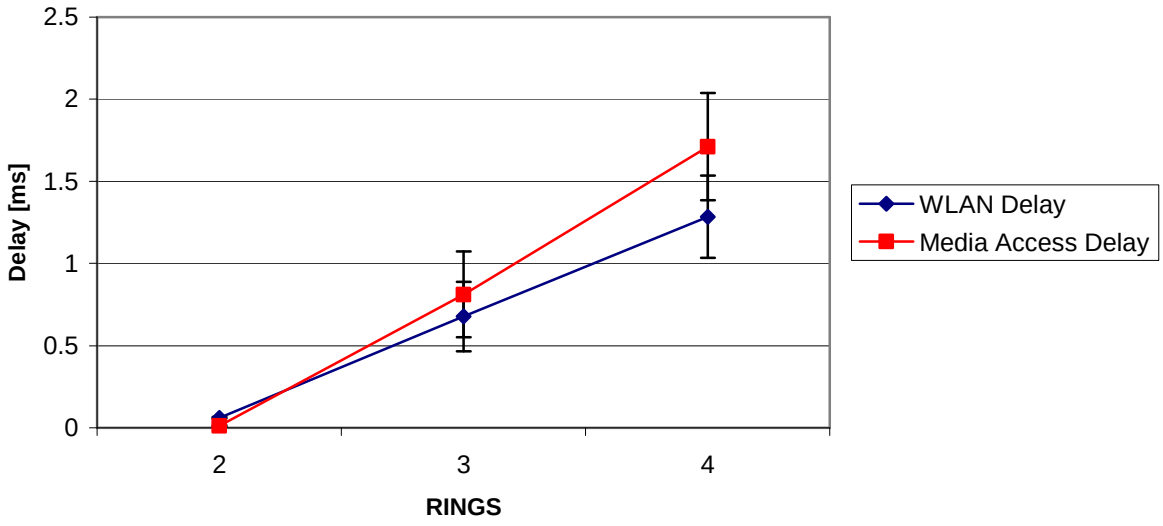


Figure 4.28. WLAN Delay and Media Access Delay for each topology.

Another output is the global load in the network, L_{WLAN}, which represents the total load submitted to WLAN layers by higher layers in all nodes of the network. L_{WLAN} values are shown in Figure 4.29 together with the WLAN throughput, R_{WLAN}, which represents the total number of bits forwarded from WLAN layers to higher layers in all nodes of the network. Load and throughput increase when the number of rings increases

because, using a lot of MAPs, the capacity per user provided by each MAP increases. However, if one sees the delay output in the network, it worsens when the number of MAPs increases, because the number of hops that a data packet can do increases too. As consequence, although the throughput is better, the delay component influence the response times of the various services, which increase, and so is not good performance for the users.

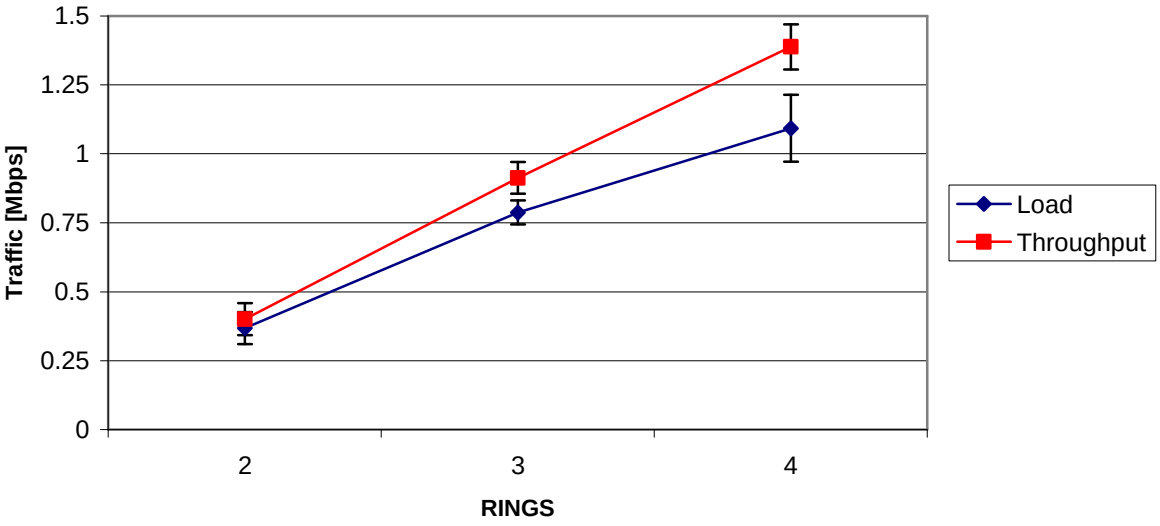


Figure 4.29. WLAN Load and WLAN Throughput for each topology.

Considering all the results obtained, the main conclusion is that, by using a multihop wireless network to cover an area it is possible to provide high performance only to users at 1 or 2 hops maximum from the gateway. In fact, generally, users in the lasts rings are penalised relative to users closer from to gateway. To decrease the average number of users per MAP it is useful to improve the user throughput, but the consequence is that, by increasing in this way also the number of hops, the delay can become too high, and moreover, there is an increment of dropped data.

It is possible to see this situation in Figure 4.24 and Figure 4.25, which show the HTTP and FTP Response Time trends as a function of the number of hops. Thus, having considered the topology with the minimum number of hops, one has to choose the 2 rings topology, which provides low response times for HTTP, FTP, and E-mail applications, and a minimum Voice Packet End-to-End Delay for VoIP applications.

Chapter 5

Conclusions

In this chapter, which finalises the work, some conclusions are provided. Moreover, some possible future works are presented.

This thesis focuses on wireless mesh infrastructure systems used to create large Wi-Fi access networks. In particular, this work is based on the study of the performance of a WMN placed in a Campus Scenario, which is composed by several buildings and open areas. This campus is located in a small area covered by most MAPs, which form the network backhaul. Several users in the campus provide a high traffic on the network. Each user executes the access on one MAP, which forwards the data in the backhaul so that data arrive to destination. This scenario is characterised by a lot of MAPs and one of this has a gateway functionality. In general, there is a high density of users per MAP, because the first characteristic of a campus network is to have a lot of users. This WMN scenario is characterised by several possible service mixes. Its performance was evaluated, considering several characteristics of the scenario, using OPNET Modeler Wireless Suite simulation tool.

Before simulating the scenarios in OPNET, it was necessary to implement a new path loss propagation model, because the models available in OPNET are not good for these scenarios. Thus, the Log-Normal Shadowing Model was inserted in the simulator to have realistic scenarios in which the various MAPs can be in radio visibility or less. This model considers that in both indoor and outdoor environments the average large-scale path loss for an arbitrary transmitter-receiver separation is expressed as a function of distance by using a path loss exponent, n. The value of n depends on the specific propagation environment, i.e., type of construction material, architecture, and location within a building. In this work, a propagation model for outdoor environment was used.

Once implemented the right path loss propagation model some studies to be acquainted with the simulator were done. Simple networks were simulated and the basic outputs, as throughput and delay, were analysed. Then, two different types of scenarios were studied:

- Basic Scenario
- Campus Scenario

The first one is useful to understand the behaviour of the network, consisting of a circular area with a radius of more or less 900 m with a uniform distribution of users (34 in all). To cover this area, which contains only one Internet gateway situated in its centre, several topologies are used, with various rings. Four topologies called 1, 2, 3, and 4 rings, which are relatively 1, 2, 3, and 4 hops networks, were implemented. The 1 ring topology is formed by only one BSS, the 2 rings topology has 7 BSSs, the 3 rings topology contains 19 BSSs, and finally, the 4 rings topology is composed of 37 BSSs. Each topology has certain BSS and WDS data rates, which depend on the cells dimension. In the Basic Scenario only two kinds of applications, FTP and VoIP, were studied. FTP represents a best effort service, which does not need real time to operate and, moreover, it uses TCP, whereas VoIP is a real time service that use UDP; thus, FTP and VoIP are very different applications. Separates studied implementing only either FTP, or VoIP were done. Then, an FTP and VoIP combined service study was done, to see how simultaneous users can call in the network while there is FTP traffic in background.

In the Campus Scenario, there are four types of available applications: HTTP, FTP, E-mail, and VoIP. Thus, there is a realistic traffic mix that is distributed as 46% for HTTP, 45% for FTP, 6% for E-mail, and 3% for VoIP. In this case, only three topologies were implemented: 2, 3, and 4 rings. Another difference with the Basic Scenario is that in the Campus Scenario the data rate in BSS and in WDS are the same, at 54 Mbps.

In the Basic Scenario, a preliminary study was done considering a 2 hops network to see the maximum throughout behaviour. Theoretically, both nodes have the same throughput, but, in practice, the node closest to the gateway is better. Finally, it is possible to conclude that, in a network without fairness mechanism, the traffic load influences the network capacity. This is the consequence of the fact that 802.11a/g were not created to work in multihop wireless networks.

The network study using only FTP was useful to analyse the network behaviour relative to the average user throughput. The hypothesis are that each user starts the file download more or less simultaneously with the other users, and that the file size is fixed and equal for all users. The average throughput was computed as the ratio between the file size and the average download time for all users. It is easy to understand that when only one BSS is used (1 ring topology) performance is the worst. In fact, in this case, the low data rate of 6 Mbps does not provide a sufficient capacity to all users, which have to contend the wireless access to only one BSS. These two factors cause a high network latency, and to download the file of 25 MB each user expends an average time of 27 minutes. So, the topology with only one AP to cover the whole area is not a good solution.

With the 2 rings topology there are improvements on performance. Using this solution, one has a 2 hops network, but, because the data rate in the BSS is increased from 6 to 48 Mbps, the system capacity increases too. This is the positive consequence of the drastically reduction of the average number of user per BSS from 37, in the 1 ring topology, to 5.3, in the 2 rings one. 2 hops users in the 2 rings topology have a lower throughput with respect to 1 hop users, but, anyway, the throughput is better than 1 ring users throughput. This throughput reduction is a consequence of the lack of fairness management in the network, and so there is not equal performance between users closest to the gateway and users at two hops.

In the 3 rings topology, the BSS data rate increases from 48 to 54 Mbps, while the WDS data rate goes from 24 to 48 Mbps. Relatively to the 2 rings topology, one can observe that there are now better values of throughput, as a consequence of the BSS and WDS data rates increment. Moreover, the average number of users per BSS is 1.9, and so the medium access contention is relaxed. 3 hops users have a low throughput, but it is greater than the throughput in the 1 ring topology.

The 4 rings topology allows to reach a high throughput only in changing the WDS data rate from 48 to 54 Mbps, leaving the BSS data rate at 54 Mbps. There is a good performance for 1 and 2hops users, and acceptable performance for 3 hops users, but 4 hops users have a low throughput compared with the 1 ring users throughput. So, relatively to the FTP single service in the network, one can conclude that the kind of topology that it is possible to choose depends of the capacity that one wants to provide

to users.

When only VoIP is used in the network, the main output parameter is the Voice Packet End-to-End delay, which has to be less than 400 ms, preferably under 150 ms. Taking as default 34 simultaneous VoIP users, the VoIP use is practically impossible, except in the 2 rings topology.

Thus, it was interesting to find the maximum number of simultaneous VoIP user available in each network topology. The rule to find this number is that the Voice Packet End-to-End delay for users with the greatest hop distance from the gateway has to be less then 400 ms. The maximum number of simultaneous VoIP users, when there is only one AP, is 24. With the 2 rings topology it is possible to have 42 users. This improvement is due to the fact that, with this topology, there are on average 5.3 users per BSS, compared to 37 users per BSS in the first topology. Moreover, the data rates are higher than the 1 ring topology ones. There is no improvement in the 3 rings topology, where there are only 16 possible simultaneous calls, because 3 hops users are very penalised.

The last study of the Basic Scenario consists of the analysis of each topology when users give a mix of FTP and VoIP traffic in the network. In this case it is interesting to evaluate the degradation in terms of number of possible simultaneous calls when there is n FTP traffic in background.

In the 1 ring topology, the maximum number of simultaneous users decreases from 24 to 21, whereas a great difference exists in the 2 rings case, where the maximum number of simultaneous VoIP users decreases from 42 to 23. In the 3 rings topology, it is possible to have only 13 simultaneous calls, instead of 16. The last topology is the worst, and, only 7 users can use simultaneously VoIP.

One idea to know a possible value of the maximum number of VoIP users it is provided by using the Erlang B model. In fact, considering as number for resources the maximum number of simultaneous VoIP calls, and considering a probability of blocking of 1%, it is possible to compute the amount of traffic for each topology when only VoIP, or FTP and VoIP combined, are used. Then, the ratio between this traffic and the number of calls per hour is the maximum number of VoIP users. It was considered that in one hour a user does a call of three minutes. Using the Erlang B model, one sees that, *e.g.*, in the 2 ring topology the maximum number of VoIP users, when there is FTP in background, can be 615.

As said previously, in the Campus Scenario a realistic traffic mix was implemented. As consequence of the multihop network, it is possible to see that the response time in each application increases when the number of MAPs increases. The network realised in a 2 rings topology is very efficient in terms of response time; in fact, in a few milliseconds it is possible to open a web page, to download an FTP file, or to download an E-mail.

The multihop structure influences the performance of the network in each ring. As said previously for the Basic Scenario, the users in the last rings are more penalised than the users closer to the gateway. Concerning HTTP and FTP trends, expressed as a function of the number of hops, it is possible to see that, considering a certain number of hops, when the number of MAPs increases the

response time increases too.

In a Campus Scenario, there is a low percentage of users that use VoIP (only the 3%), thus, the Voice Packet End-To-End Delay is very low, and this provides a good quality of conversation during a call. In fact, the maximum Voice Packet End-to-End Delay is of 270 ms, thus, it is less than the threshold to have an acceptable quality, which is 400 ms.

In the topology with few number of MAPs, data dropped values are residual, but, when the number of MAPs increases, one sees an increase in dropped data. Although the number of users per MAP decreases when the number of MAPs increases, and so there is a lower probability of access collision in the BSSs, the data dropped increases because in the WDS the number of hops that a packet can do increases, thus the probability that the data are dropped increases too. It can happen because the data buffer of the higher layer is full, or because the size of the higher layer packet is greater than the maximum allowed data size defined in the 802.11 standard.

Regarding delay, the WLAN Delay and the Media Access Delay were analysed. The WLAN Delay represents the End-to-End Delay of all packets received by the MACs of all nodes in the network, and forwarded to the higher layer. One can see that, varying the topology, there is only a small delay increment, and this delay is always less than 1.5 ms. Considering the queuing and contention delays of data, management, delayed Block-ACK and Block-ACK Request frames transmitted by all WLAN MACs in the network, it is possible to see that the maximum Media Access Delay reached is of 1.7 ms, in the 4 rings topology.

Others outputs are the global load in the network, which represents the total load submitted to WLAN layers by higher layers in all nodes of the network, and the WLAN throughput, which represents the total number of bits forwarded from WLAN layers to higher layers in all nodes in the network. Load and throughput increase when the number of rings increases because, using a lot of MAPs, the capacity per user provided by each MAP increases. However, if one sees the delay output in the network, it worsens when the number of MAPs increases, because the number of hops that a data packet can do increases too. As consequence, although the throughput is better, the delay component influence the response times of the various services, which increase, and so there is no good performance for users.

Considering all results obtained, the main conclusion is that, using a multihop wireless network to cover an area, it is possible to provide high performance only to users at 1 or 2 hops maximum from the gateway. In fact, generally, users in the lasts rings are penalised relatively to users closer to the gateway. To decrease the average number of users per MAP, it is useful to improve the user throughput, but the consequence is that, increasing in this way also the number of hops, then the delay can be too high, and moreover there is an increment of dropped data.

To do all the simulation it was used a Fujitsu Siemens AMILO M1450G with Intel Pentium M processor

at 1.60 GHz and 1.23 GB of RAM at 1.60 GHz. The total time to do all the simulation was 239 h 32 m.

Regarding future work, some ideas are suggested:

- With a small area to cover, as it is the campus one, it is possible to avoid a multihop network. As a consequence it is interesting to study the network performance when, more or less, each MAP is in radio visibility with the others.

- To study a protocol that avoids the unfairness problem caused by the multihop network. The goal is to have the same performance for each user, independent of the hop distance between the user and the gateway.

- To add user mobility, considering also the possibility of handover when the users leaves a BSS to connect to another.

Annex

Application Parameters

This annex provides an overview of the applications used in this work. In particular, one shows all the values for each application used in OPNET Modeler.

Table A.1. HTTP application specification.

HTTP Specification	HTTP 1.1
Page Interarrival Time [s]	exponential (60)
RSVP Parameters	None
Type of Services	Best Effort (0)

Table A.2. Page properties.

Object Size [byte]	**Number of Object**	**Location**	**Back-End Custom Application**	**Object Group Name**
Lognormal (20000, 50000)	Constant (1)	HTTP Server	Not used	Not used
Lognormal (14400, 252000)	Gamma (47.258, 0.232)	HTTP Server	Not used	Not used

Table A.3. FTP application specification.

Command Mix (Get/Total)	0.95
Inter-Request Time [s]	exponential (600)
File Size [byte]	Uniform_int (100000, 1000000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort (0)
RSVP Parameters	None
Back-End Custom Application	Not Used

Table A.4. E-mail application specification.

Send Interarrival Time [s]	Exponential (360)
Send Group Size	Uniform_int (1, 5)
Receive Interarrival Time [s]	Exponential (360)
Receive Group Size	Uniform_int (1, 5)
E-Mail Size [byte]	Lognormal (100000, 660000)
Symbolic Server Name	Email Server
Type of Service	Background (1)
RSVP Parameters	None
Back-End Custom Application	Not Used

Table A.5. VoIP application specification.

Incoming Silent Length [s]	Exponential (0.456)
Outgoing Silent Length [s]	Exponential (0.456)
Incoming Talk Spurt Length [s]	Exponential (0.854)
Outgoing Talk Spurt Length [s]	Exponential (0.854)
Encoder Scheme	G.729 A (silence)
Type of Service	Interactive Voice (6)
Compression Delay D_{COtx} [s]	0.02
Decompression Delay D_{DCrx} [s]	0.02

Table A.6. VoIP Encoder Scheme.

Codec Type	CS-ACELP
Name	G.729 A (silence)
Frame Size D_{ENtx} [ms]	10
Lookahead Size [ms]	5
DSP Processing Ratio	1.0
Coding Rat [kbps]	8
Speech Activity Detection	Enabled
Equipment Impairment Factor	Unknown
Packet Loss Robustness Factor	Default

References

[ABBJ04] D. Aguayo, J. Bicket, S. Biswas, G. Judd and R. Morris, “Link-level measurement from an 802.11b mesh network”, in *Proc. of the 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Portland, Oregon, USA, Aug. 04.

[AkWW04] I.F. Akyildiz, X. Wang and W. Wang, “Wireless mesh networks: a survey”, *Elsevier Journal of Computer Networks*, Vol. 47, No. 4, Mar. 2005, pp.445-487.

[AlBL05] M. Alicherry, R. Bhatia and L. Li, “Joint channel assignment and routing for throughput optimization in multi-radio wireless mesh networks”, in *Proc. of the 11th Annual International Conference on Mobile Computing and Networking*, Cologne, Germany, Sep. 2005.

[Bagh03] N. Baghaei, “IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients”, in *Proc. of ICON 2004 - 12th IEEE International Conference on Networks*, Singapore, Singapore, Nov. 2004.

[BelA07] http://www.belairnetworks.com, Oct. 2007.

[BABM05] J. Bicket, D. Aguayao, S. Biswas and R. Morris, “Architecture and evaluation of an unplanned 802.11b mesh network”, in *Proc. of the 11th Annual International Conference on Mobile Computing and Networking*, Cologne, Germany, Sep. 2005.

[BiFO96] G. Bianchi, L. Fratta and M. Olivieri, “Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LAN”, PIMRC’96 7th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Taipei, Taiwan, Oct. 1996.

[Cisc07] http://www.cisco.com, Oct. 2007.

[DrPZ04] R. Draves, J. Padhye and B. Zill, “Routing in multi-radio, multi-hop wireless mesh networks”, in *Proc. of the 10th annual international conference on Mobile computing and networking*, Philadelphia, USA, Aug. 2004.

[FCFN07] L.S. Ferreira, L. Caeiro, M. Ferreira and M.S. Nunes, *Qos Performance Evaluation of a*

WLAN Mesh vs. A WIMAX Solution for an Isolated Village Scenario, Instituto Superior Técnico/Instituto de Telecomunicações, Technical University of Lisbon, Lisbon, Portugal, 2007.

[GoMM04] S. Gobriel, R. Melhem and D. Mosse, "A Unified Interference/Collision Analysis for Power-Aware Adhoc Networks", in *Proc. of IEEE INFOCOM*, Mar. 2004.

[GrTs02] M. Grossglauser and D.N.C. Tse, "Mobility increases the capacity of ad hoc networks", *IEEE/ACM Transactions on Networking*, Vol. 10, No. 4, Aug. 2002, pp.477-486.

[GuKu00] P. Gupta and P.R. Kumar, "The capacity of wireless networks", *IEEE Transactions on Information Theory*, Vol. 46, No. 2, Mar. 2000, pp-388-404.

[Haen02] M. Haenggi, "Probabilistic analysis of a simple MAC scheme for ad hoc wireless network", in *IEEE Wireless Circuits and System Workshop*, Pasadena, California, USA, Sep. 2002.

[HoLe08] E. Hossain and K. Leung, *Wireless Mesh Networks Architectures and Protocols*, Springer, NY, USA, 2008.

[IEEE03] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications* , IEEE Standard 802.11-99, 2003 (http://www.ieee.org)

[JuPe03] J. Jun and P. Peddabachagari, "Theoretical maximum throughput of IEEE 802.11 and its applications", in Proc. of Network Computing and Applications, Raleigh, NC, USA, Apr. 2003.

[JuSi03] J. Jun and M.L. Sichitiu, "The nominal capacity of wireless mesh networks", *IEEE Wireless Communications*, Vol. 10, No. 5, Oct. 2003, pp.8-14.

[KiVa05] P. Kyasanur and N.H. Vaidya, "Capacity of multi-channel wireless networks: impact of number of channels and interferences", in *Proc. of the 11th annual international conference on Mobile computing and networking*, Philadelphia, USA, Sep. 2005.

[Liaw05] G.H. Liaw, *An Overview of 802.11e*, Oct. 2005, (netlab18.cis.nctu.edu.tw/html/wlan_course/powerpoint/802.11e.pdf).

[LCLM01] J. Li, C. Blake, D.S.J. De Couto, H.I. Lee, R. Morris, "Capacity of Ad Hoc wireless networks", *Conference on Mobile Computing and Networking*, Rome, Italy, Jul. 2001.

[LuBh99] S. Lu and V. Bharghavan, "Fair scheduling in wireless packet networks", *IEEE/ACM Transactions on Networking*, Vol. 7, No. 4, Aug. 1999, pp.473-489.

[NeTu01] G. Németh, Z.R. Turànyi and A. Valkò, "Throughput of ideally routed wireless ad hoc

network", *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol. 5, No. 4, Oct. 2001, pp.40-46.

[NGKI06] D. Niculescu, S. Ganguly, K. Kim and R. Izmailov, "Performance of VoIP in a 802.11 Wireless Mesh Network", in *Proc. of IEEE INFOCOM*, Barcelona, Spain, Jul. 2006.

[OPNE07] *OPNET Modeler 14.0 Documentation*, OPNET Technologies Inc., Bethesda, Maryland, USA, 2007 (http://www.opnet.com).

[RaCh05] B. Raman and K. Chebrolu, "Design and evaluation of a new MAC protocol for long-distance 802.11 mesh networks", in *Proc. of the 11th annual international conference on Mobile computing and networking*, Philadelphia, USA, Sep. 2005.

[RaGC04] A. Raniwala, K. Gopalan and T. Chiueh, "Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks", *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol. 8, No. 2, Apr. 2004, pp.50-65.

[Rani04] A. Raniwala, *Coverage and Capacity Issues in Enterprise Wireless LAN Deployment*, Technical Report TR-166, Stony Brook University, Computer Science Department, Experimental Computer System Lab, NY, USA, Nov. 2004.

[Rapp96] T.S. Rappaport, *Wireless Communications Principles and Practice*, Prentice Hall, New Jersey, USA 1996.

[Stall01] W. Stallings, "LAN QoS", *The Internet Protocol Journal*, Vol. 4, No. 1, 2001, pp.16-23.

[Trop07] http://www.tropos.com, Oct. 2007.

[VaBG00] N.H. Vaidya, P. Bahl and S. Gupta, "Distributed fair scheduling in a wireless LAN", in *Mobicom 2000*, Boston, Massachusetts, USA, Aug. 2000.

[WaMa06] B. Walke, S. Mangold and L. Berlemann, *IEEE 802 Wireless System*, John Wiley & Sons, West Sussex, UK, 2006.

[WiMA07] http://www.wi-mesh.org, Oct. 2007.