Modelling and Performance Studies of Integrated Network Scenarios in a Hospital Environment

by

Xiaomin Kuang

A dissertation submitted to Auckland University of Technology
in partial fulfilment of the requirements for the degree
of Master of Computer and Information Sciences

2008

School of Computing & Mathematical Sciences
Primary Supervisor: Nurul I.Sarkar

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signature: ____________________

Xiaomin Kuang

Abstract

The hospital network is evolving towards a more integrated approach by interconnecting wireless technologies into backbone networks. Although various integrated network scenarios have been published in the networking literature, a generic hospital model has not yet been fully explored and it remains a challenging topic in practice. One of the problems encountered by network practitioners is the seamless integration of network components into healthcare delivery. A good understanding of the performance of integrated networks is required for efficient design and deployment of such technologies in hospital environments.

This dissertation reports on the modelling and evaluation of integrated network scenarios in hospital environments. The impact of traffic types (e.g. voice and video), traffic load, network sizes and signal strength on network performance is investigated by simulation. Three piloted case studies look at client performance in radiology Accident and Emergency (A & E) and Intensive Care Unit (ICU) scenarios. Each scenario reflects the need for various traffic types that end up distinct network behaviours. In the radiology scenario, email and File Transfer Protocol (FTP) traffic is found to perform well under medium-to-large networks. In the A & E scenario, Voice over Internet Protocol (VoIP) traffic generates very limited jitter and packet loss. This performance is aligned with the Quality of Service (QoS) requirements. In the ICU scenario, the performance of video conference degrades with network size, thus, a QoS-enabled device is recommended to reduce the packet delay and packet losses.

Acknowledgements

First of all, I am grateful to my supervisor Nurul I. Sarkar for giving this interesting topic as my dissertation research. With his guidance, I have learned a lot from the project and have overcome numerous issues regarding network modelling. Although the process is painful, it ends up a sense of success. In addition, I appreciate for his support and encouragements throughout this dissertation.

I am also grateful to my friends and co-workers, such as Wilford Gibson, Raffic Will, and Micheal Zheng for their sincere help.

Finally, I would like to appreciate my parents for their support overseas. Without their help, I cannot complete the dissertation on time.

Contents

List of Abreviations and Acronyms

AP	Access points
A & E	Accident & emergency
HR /DSSS	High rate / direct sequence spread spectrum
BSD	Berkeley software distribution
CT	Computed tomography
DSL	Digital subscriber line
DB	Database
ER	Emergency room
FTP	File transfer protocol
GPRS	Global packet radio service
HTTP	Hyper text transfer protocol
ICU	Intensive care units
IEEE	Institute of electrical and electronic engineers
ISM	Industrial, scientific, medical
IP	Internet protocol
PC	Personal computer
PACS	Picture archiving and communication system
PCF	Packet control function
PDA	Personal digital assistants
QoS	Quality of service
SSID	Service set identifier
TCP	Transfer control protocol
UDP	User datagram protocol
VoIP	Voice over internet protocol

VPN	Virtual private network
VLAN	Virtual local area network
WLAN	Wireless local area network
WPAN	Wireless personal area network

List of Figures

List of Tables

Chapter 1

Introduction

Over the past ten years, heterogeneous networks (wired and wireless) had tended to integrate seamlessly, offering effective and reliable service for medical operations. The major driver for adopting Wireless Local Area Network (WLAN) technology in hospital environments is accuracy enhancement [1]. An official report from the Institute of Medicine [2] shows that there are approx 1.5 million patients subject to medication errors throughout the US hospitals in 2006. To reduce the errors regarding drug delivery, Aspden, et al. [2] recommend high speed wireless technology for pharmaceutical track and trace. Other examples that harness Wireless Fidelity (WiFi) connectivity have been successfully implemented in [1, 3, 4].

The ease of use and mobility advantages of WLAN also significantly improves the efficacy of healthcare delivery. For instance, the patient records associated with monitoring can be acquired by authorized users using a Personal Digital Assistant (PDA). X-ray images are also retrievable in the forms of File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP) and Database (DB) query; thereby radiologists can share the information more effectively. Last but not least, it is quite common that doctors fulfil a consultation task through video conference or Internet Protocol (IP) telephony on a handheld device.

While 3G and Global Packet Radio Service (GPRS) cellular networks are high demanding in industries, they have shortcomings in capacity and would not be able to suite the real-time connectivity for tremendous amount of users [3]. Rather, WLAN technologies can be exploited to supply higher data rate connection within a relatively smaller coverage than cellular networks, to the designated medical applications in hospitals.

A misconception as to the hospital model development is to replace the entire wired backbone with the wireless architecture. This opinion is not realistic. Since the radio signal strength varies constantly with the surrounding environment, such as distance, source of interference (interior and exterior), and the protocol being used etc., its performance is not as stable as the wired networks. Literatures also reveal that Quality of Service (QoS) is not supported in current mainstream WLAN technologies (namely, 802.11a [5], 802.11b [6] and 802.11g [7]). Although 802.11e [8] is introduced as an emerging standard to provision QoS features on a contention-based channel access scheme, extensive testing is still required for the deployment in the medicine areas. Hence, a more integrated approach is expected to incorporate the wireless technologies into the existing backbone network, ensuring that the centralised service (including QoS) are still maintained by the wired infrastructure, while cable free flexibility and escalated bandwidth are achieved by WLAN technology to satisfy the peripheral mobile service as well as emerging medical services (e.g. heart monitor and telemetry).

A number of researchers [3, 9] have made effort in designing an intellectual Emergency Unit (EU) model that extends accessibility and interoperability against the legacy system, yet a generic hospital model is not fully developed. The complexity is due to the characteristics of hospital scenarios. Unlike the commercial and educational networks [10-12], a standard hospital normally involves life-critical application, multimedia application and office-oriented application, and therefore the network model requires more specific performance metrics to evaluate data, audio and video traffic under different conditions. Especially, in the emergency units, timely response to the biomedical signals and alarm is highly critical to saving lives, so mean packet delay and packet loss are sensitive at this point. As the network scenario switches to radiology room or intensive care unites, the tolerated range for mean packet delay and packet loss must be varied. The patterns of transmitting data, audio and video traffic are fully specified in [13]. Researchers can observe the network behaviours by means of simulation tools for data validity and verification purposes.

Out of the numerous design and modelling issues, the main ones encountered network practitioners include validity and feasibility of network architecture, network protocol and the strategies that figure out performance metrics, user capacity, and propagation environment. Presumably, the network architecture offers fast and reliable connectivity for hospital-wide applications. However, different traffic demands on different security and quality-based provision. Explicitly, voice and video traffic requires a robust gateway to maintain authentication and sufficient bandwidth for each session, while data traffic tends to more rely on backup, security policy and Virtual Private Network (VPN) technology dedicated for the remote users. Therefore, a preliminary feasibility research is required for deploying such technologies in the hospital scenarios. The network architecture is not validated until cost, availability, scalability and all performance data have met the predefined standards. Likewise, the high rate WLAN technologies (802.11a and 802.11g) need to be fully justified in terms of throughput, mean packet delay and packet drop, etc.

1.1 Objective of this research project

This dissertation aims to develop a generic hospital network model and evaluate its performance for the integrated network scenarios, including radiology room, Emergency (A & E) and Intensive Care Units (ICU). This dissertation makes use of computer simulation and discusses various aspects of the network design, so as to discover the performance behaviour pertaining to effect of traffic type, traffic load and network size. Intuitive insight is also sought to provide guidelines for novice users in developing hospital simulation models. In general, this dissertation considers the following research questions:

1. What are the key factors influencing the integrated network scenarios in a hospital environment?

2. How can the performance-constraint factors be quantified?

To achieve these objectives, OPNET simulation models have been exploited for performance analysis. The modelling process involves four discrete tasks. First, the wired backbone network is developed to interoperate with WLAN components. Second, traffic distribution and medical applications are defined using OPNET. Third, the effects of network size, traffic load and signal strength on network performance are evaluated individually through performance metrics, such as throughput, mean packet delay, fairness and packet loss. Comparative analysis among the integrated scenarios is then implemented. Through various simulation experiments, a fundamental overview is gained into the improvement towards efficient design and deployment of QoS delivery in a hospital environment. Fourth, validate the simulation model by means of observation and comparison with relevant studies.

This dissertation mainly contributes to the optimal settings of various applications in a hospital environment. By viewing the network behaviours under different traffic types (e.g. data, voice and video), .strategies pertaining to resource utilisation can be obtained. Since the upcoming multimedia services (such as VoIP and video conference) impose great challenges on medical network design, this dissertation also recommends on the optimised bandwidth utilization for QoS delivery.

1.2 Dissertation structure

The rest of the dissertation is organised as follows (Figure 1.1). Chapter 2 covers the fundamental overviews associated with network modelling and mechanism in hospital environments. Chapter3 articulates the proposed methodology for this dissertation, focusing on computer simulation and observation. Chapter 4 and Chapter 5 are the main contribution of research. The former devises the integrated network scenarios of generic hospital model. The latter interprets the network behaviours of various network scenarios and proposes improvements towards efficient network design and QoS delivery. The remarks and the future research are concluded in Chapter 6.

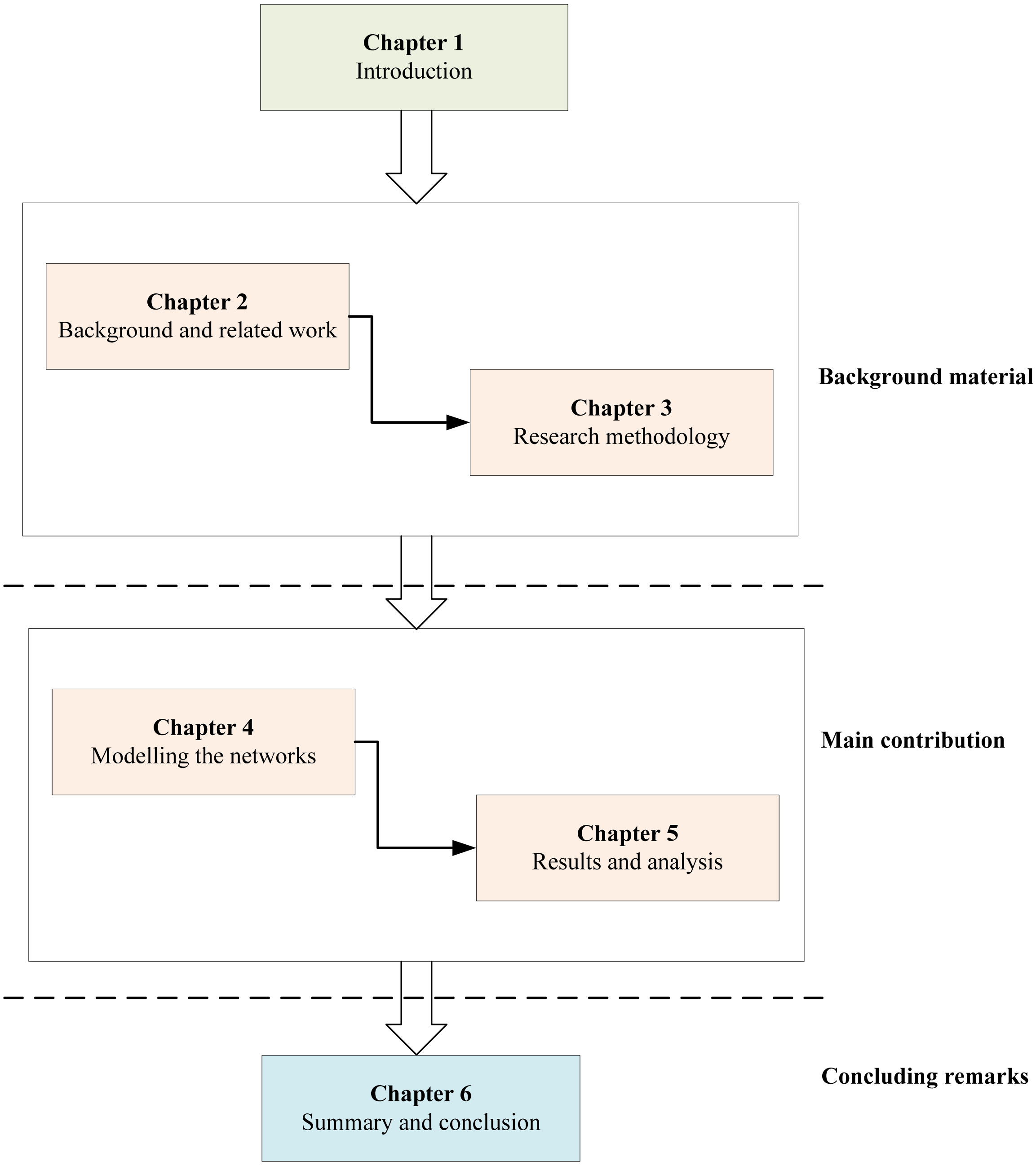


Figure 1. 1: Dissertation structure.

Chapter 2

Background and Related Work

In Chapter 1, the research objective was outlined. This chapter provides the background information for this dissertation. Section 2.1 presents the medical applications and scenarios intended for the integrated hospital model. Unlike the implementation of other types, the hospital network tends to rely on more advanced and reliable technologies. Section 2.2 elaborates the unique characteristics of hospital applications and identifies the key factors influencing network performance. Section 2.3 reports on the mainstream WLAN 802.11 standards with full justification of pros and cons. In section 2.4, several integrated network architectures are reviewed. Subsequently, the significant hospital models are discussed in section 2.5, followed by the designing issues and challenges that inspire further investigation in medical circumstances. Section 2.7 reports on the recommendation for operating parameters, performance threshold and security.

2.1 Medical applications and scenarios

Due to the increasing number of users and traffic types, medical applications will rely on more sophisticated, “interoperable integrated networks”[14]. The concept of “MedLAN” was originally proposed by Banitsas, et al. [15]. It refers to the network scenario explored for emergency care environments. With the progress of telecommunications, “MedLAN” is not restricted to the emergency department. Rather, more scenarios are expected to integrate into the legacy backbone network with advanced and reliable technologies. The major applications as illustrated in Figure 2.1, involve life-critical applications, on demand multimedia applications, office oriented application and distant control applications. Typical applications, such as videoconferencing, IP telephony and file transfer will not only run on the wired backbone network, but also interoperate with WLAN components which allow mobility and therefore trigger seamless communication and more effective heath care delivery [16]. As noted by Li, et al. [17], the integrated hospital networks will also open up opportunities for emerging applications, such as patient monitoring, alarm generation and remote device control.

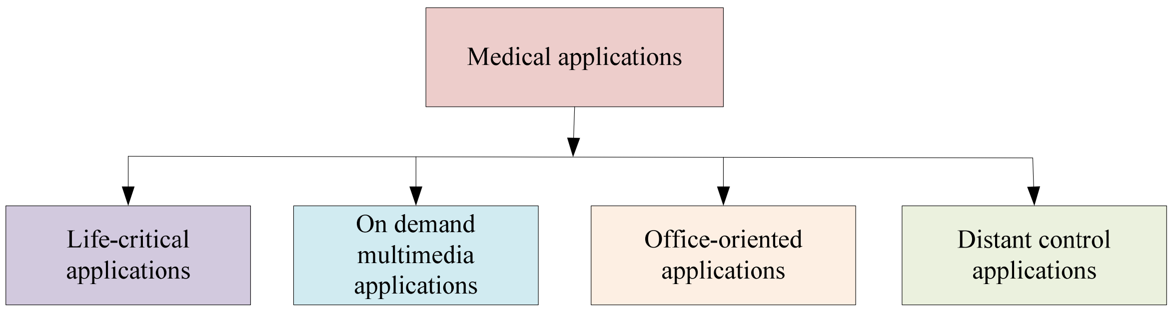


Figure 2. 1: Classification of the major medical applications

Figure 2.2 shows a typical hospital network which involves A & E ward, radiology and ICU scenarios. Each scenario demands on various applications and all interconnect with the wired backbone network providing high speed connectivity and centralised administration.

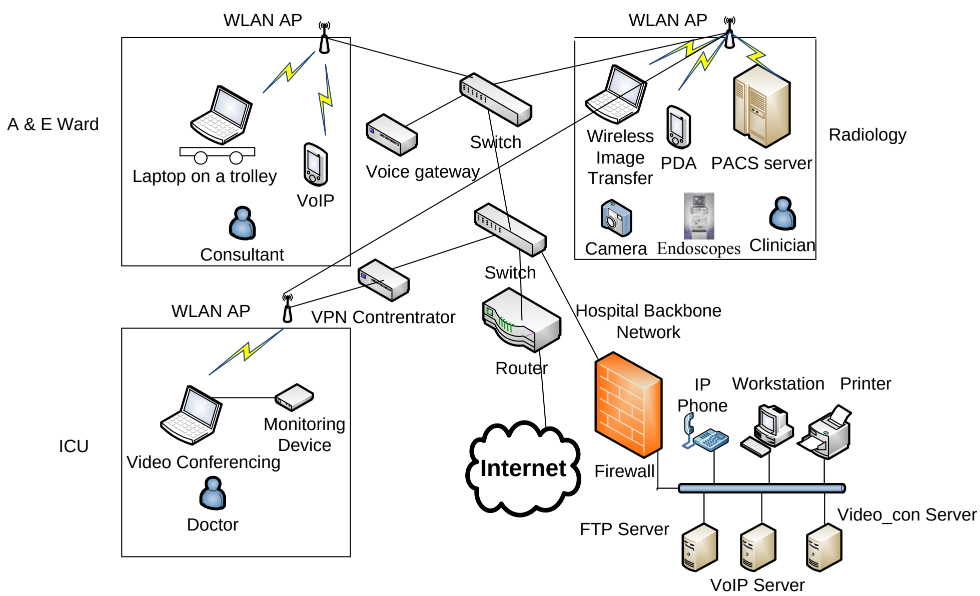


Figure 2. 2: Integrated network scenarios and the core applications in hospital settings.

The A & E ward is comprised of a laptop on a trolley and a PDA that is fully capable of WLAN transmission. The laptop is expected to capture the periodic biomedical data from remote device while roaming about in the emergency department. Meanwhile, it is linking to several specialized devices (such as high definition camera and endoscopes) which support WiFi connectivity, therefore high quality of video and audio data can be achieved for diagnosis purposes. The consultant on the other hand is free to obtain the analytical data, either from existing wired workstation or portable devices. In addition, IP telephony via a voice gateway is available, offering call forwarding and voice mail functionality.

The A & E ward in hospital can be considered as a kaleidoscope which reflects multiple functionalities as reported in [18]. E-prescription can be achieved by the use of handheld device equipped with voice-recognition functionality while doctors or specialists are right by the patient's bedside or roaming around the corridor area. The prescription record can be obtained by pharmacist who holds a tablet Personal Computer (PC). Meanwhile, additional information, such as patient's history, lab results and physiological data are available to track. The use of e-prescription has significantly speeded up the decision making process and cut down the extra work of reading doctors' cursive hand by pharmacists. Technically, there are a few concerns for the deployment of wireless technology: 1) instead of 802.11b, high rate wireless standard is required to transmit the medical data more efficiently; 2) minimise the interference with other wireless devices; and 3) the signal strength need to be fully investigated, ensuring the saturation range and link quality.

In the scenario of radiology, patients' records are maintained by applications, such as file sharing, database query and barcode scan. It also allows web browsing, email and image transfer for diagnostic purpose. Typically, Picture Archiving and Communication System (PACS) [19] is used to store X-rays and Computed Tomography (CTs) images electronically and allows sharing with other clinicians. According to Banitsas, et al. [20], the applications dealing with health care records are critical and normally require backup and authentication procedures. Although these applications are office-oriented, network load and ubiquity are always expected high.

ICU is another scenario that captures attention. This scenario consists of certain portable devices (like laptops and PDAs) that support web browsing, video conferencing and IP telephony. An AP here allows airborne transmission of various traffic types (e.g. data, video and voice). The embedded Virtual Private Network (VPN) ensures that only the authenticated users, such as doctors and nurses, can access and communicate with the training programs. Although similar scenarios are implemented by researchers Su & Shih; Cocoradal & Szekelyl [21, 22], efficient propagation scheme is still required for QoS delivery, in which performance improvement is the focus of this scenario.

As illustrated by Banitsas, et al.[23], futuristic medical scenario is expected to establish metropolitan connectivity, ideally covering the interior and exterior areas of hospital. With the use of fibre optics, Digital Subscriber Line (DSL) and WLAN infrastructures, doctors can effectively monitor the performance of medical device while he/she stays at home.

Bisain in [14] claim that the integrated network scenarios in hospital settings are intuitively linked to the ever-changing telecommunication industry and dynamics of “organizational learning”. Leveraging organizational collaboration is critical for medical network design. One illusion for project managers and directors is to accentuate on the technical functionality of intended project, and in a sense, ignore the clinical, educational and administrative or other issues that they claim to rectify. As a result of such misunderstanding, many researchers propose systemic validation methods [22]. The validation of medical network scenarios can be achieved through technology assessment, benchmarking schemes for medical pragmatics, and prototypes that begin with investigating “social medical, organizational, and social needs” and subsequently examines the added values, potential risks, and cost of substitute technologies or packages within this context [14].

2.2 Unique characteristics

Although the cost and technology advantages have triggered some exploration of integrated network scenarios [24], solid understanding as to the characteristics of hospital applications is still required. As described by Chigan and Oberoi [25], medical traffic can fall into two categories: constant report data which are transmitted in a regular predictable interval, and the emergency signal that has a highly arbitrary nature. The involvement of emergency signal imposes more challenges to the design of traffic distribution.

Earlier studies in [14] claim that bandwidth bounds and mean packet delay are the major concern with hospital application. Since the emergency signal is critical to saving lives, dedicated resource and robust QoS scheme should be provided, ensuring the important packets are transmitted in a timely manner. Golmie, et al. [26] argue that QoS is application-specific, and therefore a complete roadmap of QoS requirement should be investigated. Not only throughput and mean packet delay, but also packet drop and other factors should be taken into account [13]. Table 2.1 details the medical application and associated QoS requirements.

Table 2.1: QoS requirements of medical applications.

	Bandwidth	Delay	Packet drop	Reliability	Ubiquity	Security
Life-critical applications	Relatively low bandwidth is required. 10-100kb/s	Relatively low delays are required. 10-150 msec	Zero fault tolerance is expected	Very high reliability requireme nt	High ubiquity requirement	Authentica tion and confidential ity are expected
Non critical Multimedia applications	Voice: low requirement 10kb/s Video: high requirement 100kb/s	Low to moderate delays <300 msec	Low data loss is expected <0.0001	High reliability is expected	High ubiquity requirement	Authenticat ion and confidential ity are expected
Office-oriented applications	Relatively high bandwidth is required. 1-1Mb/s	Moderate to high delays <1 sec	Some recoverabl e data loss are tolerated <0.01	High reliability is expected	High ubiquity requirement	Authenticat ion, integrity and confidential ity are expected
Distant Control applications	<1 kb/s	Low delays <3-5 sec	Zero fault tolerance is expected	Very high reliability requireme nt	Not required	Integrity is required

Life-critical Applications – Typical applications contain alarm generation and patient monitoring. Due to the nature of salvation, this type of applications usually requires low bandwidth but hardly tolerate delay and packet loss. Reliability and mobility are required as well.

On demand multimedia applications – Image transfer, videoconferencing and IP telephony fall into this category. Unlike the life-critical applications, this category can bear small amount of packet loss but it is very sensitive to delay and confidentiality. Efficient mobility is required for the communication purpose.

Office-oriented applications – Typical applications contain web browsing, file sharing, database query, email. Although this type of applications requires relatively high bandwidth, some data corruption can be recovered by the backup facility. High level of confidentiality is required. In addition, mobility is also desirable so as to achieve efficient health care delivery anytime, anywhere.

Distant control applications – This category involves medical device monitoring, namely, alarm generator that monitors patient remotely and telemetry that copes with physiological functions.

2.3 Justification of current WLAN technologies

The advent of IEEE 802.11 standards significantly stimulates wireless connectivity in hospital circumstances [6]. Table 2.2 compares the key characteristics of 802.11 WLAN standards. Due to the Media Access Control (MAC) design, WLAN standards vary greatly in data rate, coverage, and other features. IEEE 802.11b resides in 2.4GHz frequency band and operates High Rate / Direct Sequence Spread Spectrum (HR-DSSS) as a MAC mechanism. Chu and Ganz [27] point out a fact that large hospitals are more likely to invest on wireless technologies than the smaller ones. The investment of wireless technologies is determined by fiscal budget, complexity of medical system and sophisticated communication need.

Although 802.11a and 802.11g infrastructures are relatively more expensive, they provides 4 times data rate faster than 802.11b. As reported by LeMay [28], Sydney Adventist

Hospital adopted 802.11a for the patient care solution. The great benefit is mitigating the interference with other devices operating on the popular 2.4 GHz ISM bands. In addition, 802.11a has greater number of channels compared to 802.11b and 802.11g, which addresses the issues as to hidden nodes. As reported by Lo [29], a hidden node refers to the node that cannot communicate with the others.

Table 2.2: Comparison of various WLAN standards

	802.11a	802.11b	802.11g
Frequency Band	5GHz	2.4GHz	2.4GHz
Channels	11 non-overlapping	3 non-overlapping	3 non-overlapping
Max data rate	54Mbps	11Mbps	54Mbps
Modulation	OFDM	HR-DSSS	OFDM
QoS	No	No	No
Possible Interference	Satellite signals	Microwave and Bluetooth devices	Microwave and Bluetooth devices
Types of Applications	Real-time, multimedia and typical IT applications	Real-time, multimedia and typical IT applications	Real-time, multimedia and typical IT applications
Typical coverage	10-50m	30-200m	30-200m
Cost	high	low	medium
Popularity	medium	medium	high

Since 802.11g is backward capable, concurrent implementation of 802.11b and g is possible. Nonetheless, Abdullah, Moinudeen and Al-Khateeb [30] find out the coverage range in concurrent implementation is smaller than that of standalone 802.11b. The aggregate throughput is also less than that of 802.11g.

Recent studies conducted by Branquinho, Reggiani and Ferreira [31] reveal that 802.11a supports the multimedia scenarios, with combination of voice, video and typical IT applications. Major advantages involve high data rate and low interference with other devices in the 2.4 GHz ISM bands, and also mobility support inside medical facility [31-34]. Unfortunately, QoS is not supported by IEEE 802.11 standard.

To investigate the optimal settings for hospital environments, a comparative study of 802.11a and g is required. This dissertation investigates 1) the impact of traffic load on WLAN performance; and 2) the impact of signal strength on WLAN performance.

2.4 Integrated network architecture

Figure 2.3 illustrates a typical WLAN architecture linked with a wired Distribution System (DS). The central DS provides flexibility to construct various sizes of WLANs. Multiple DSs and Basic Service Sets (BSSs) can build up hierarchical service architecture.

While WLAN architectures involve ad hoc mode and infrastructure mode, this dissertation focuses on the infrastructure mode. Explicitly, a Basic Service Set (BSS) consists of an AP as a reconciler among wireless stations. Certain BSSs can link to a DS so as to achieve corporate-wide coverage range (Figure 2.3). A DS [29] is a logical domain that propagates a variety of corporate services for multiple BSSs. It can be wired or wireless connection. A wireless DS requires linkage to peripheral BSSs and reconciliation among the APs.

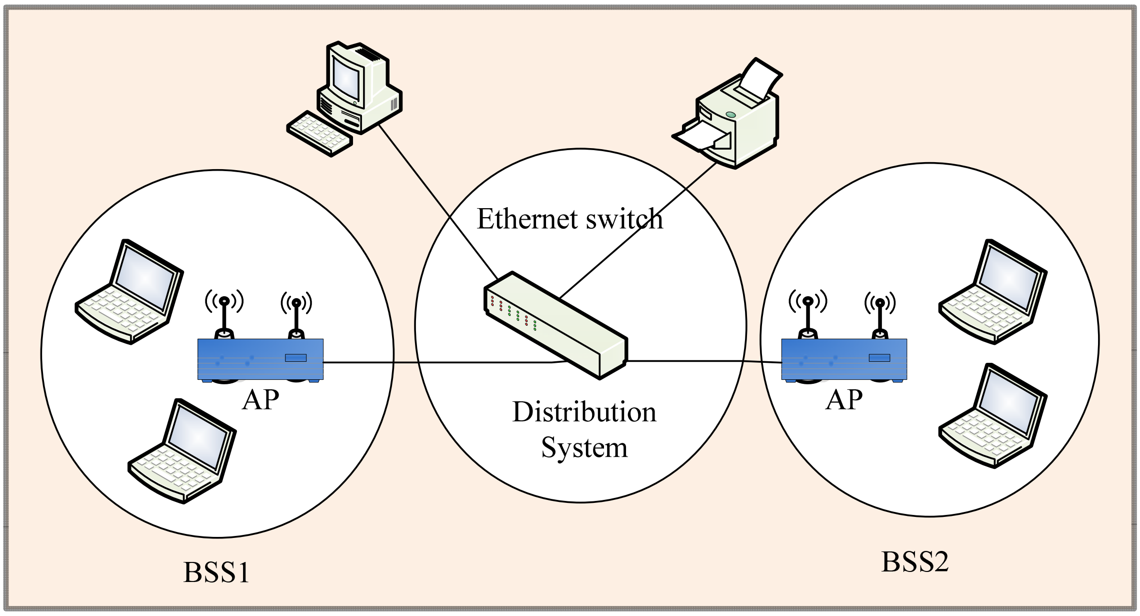


Figure 2. 3: WLAN linked with the wired DS.

In medical environments, a central switch is expected to provide gigabit connectivity as well as robust security (e.g. traffic monitoring, authentication and availability) for administrative purposes. The gigabit feature is shipped with the advanced products, such as 3Com 4007 and Cisco 4948. To maximise the system availability, an extra switch is committed to the failover tasks. If any fraud that leads to service down time is detected, the auxiliary switch will be activated promptly. Being a traffic coordinator, the central switch also needs to deal with VLAN technology, topology design and WLAN components.

- Virtual Local Area Network (VLAN) technology is essential to deliver medical applications to each department. It is commonly used for logical network design. The great advantages of using VLAN involve remarkable broadcast reduction and centralized administration. In addition, it enhances security by managing the access control lists (ACLs). For instance, Radiology users referred to vlan300, are only allowed to access email and FTP applications.
- Typical topology for a DS involves "gateway topology, wireless switch topology, and smart AP"[35]. The concern is with flexibility, scalability, budget, and security. The wireless switch, also known as thin switch, varies greatly from other kinds. These wireless switches provide coordination to thin APs which normally execute Ethernet translation from 802.11 to 802.3 and occasionally perform encoding/decoding. Other useful tasks implemented by the wireless switches involve filtering, authenticating and remote monitoring. As note in [31], the AP configuration resides at the powered on wireless switch. Whenever a thin AP is deactivated from the powered on wireless switch, its memory is eliminated. This is an extremely handy feature for securing configuration profiles and encryption keys from stealth or hostile attacks into the AP.
- Figure 2.4 demonstrates a typical hospital network architecture that supports WLAN technology. Authentication server is exploited to administer access to the wired backbone network. To avoid privilege abuse, network resources are only authorised to the users with reference to a hierarchical accountability framework. Such Authentication, Authorisation and Accountability model have been successfully implemented by a number of hospitals [36].

Since WLAN technology relies on radio propagation, a wireless network analyser is required to discover signal strength (clear channel) and to monitor radio link quality. The Wavelink's mobile manager [37] is embedded on the server end. It aims to administer the APs more effectively. Based on the predefined policies, the mobile manager is able to update the firmware periodically and generate alerts as soon as the configuration is changed. In addition, all the configuration profiles and encryption keys are stored in an inviolable memory, so that network administrators can retrieve the configuration file when outage occurs.

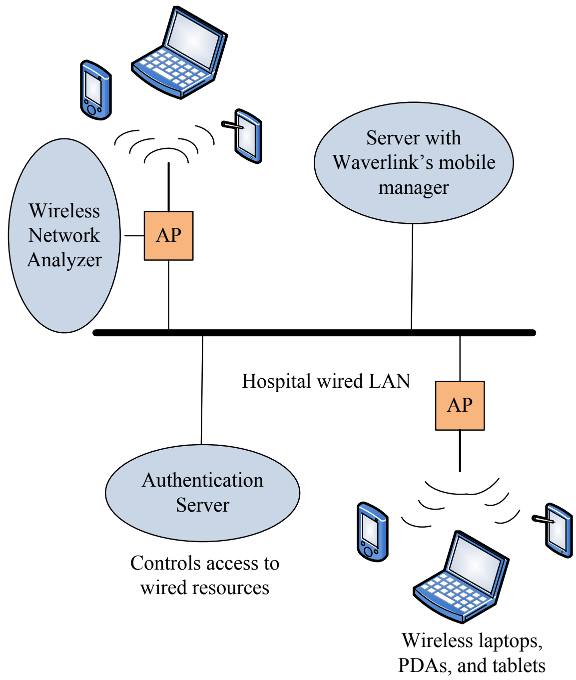


Figure 2. 4 : Typical hospital network architecture.

Hneiti and Ajlouni [36] suggest the fusion of XML and web service, in order to transfer the multimedia data more effectively and efficiently. This technology can be fulfilled by integrating member servers, such as Microsoft Share Point Server.

Several developments of hospital network models have been highlighted for further studies in the following section.

2.5 Related work on network modelling

Table 2.3 presents the leading researchers and their contribution in the design of integrated network scenarios. Empirical models tend to more focus on the development of Emergency Room (ER), such as [17, 20, 22, 38] . In addition, most of them utilize OPNET Modeller.

Table 2.3: Leading researchers and their contributions in the design of integrated network scenarios.

Researchers	Year	Contributions	Key concept descriptions
Assaad & Fayek [24]	2006	Build a multiple-site hospital network model for healthcare applications	Quantify the performance of server, workstation and router respectively
Banitsas, et al. [20]	2002	Propose a MedLAN scenario with the presence of OFDM-based IEEE 802.11b	Propose a novel MAC protocol and investigate the BER and throughput in multi-path wireless propagation environment
Li, et al. [17]	2006	Design a conceptual ER model for Katoomba Hospital	Evaluate the performance of existing ER systems
Su & Shih [22]	2003	Construct a multitask model for Emergency Care department	Verify the system performance with a pilot case study
Chu & Ganz [27]	2007	Devise a patient care model focusing on IEEE 802.11b	Investigate throughput, saturation limit, end-to-end delay and delay variation in various scenarios
Owens, et al. [39]	2001	Render modelling issues for MedLAN	Securing a medical integrated system
Zhen, et al [40].	2008	Establish a clear channel assessment model	Clear channel assessment in the integrated medical environments
Gunal, et al. [38]	2006	Create a model of ER department using real data from the patient admission system	Examine the performance in A&E department based on the multitasking behaviour and experience level of medical staff.
Golmie, et al. [26]	2004	Develop a coexistence model of WPAN and WLAN	Evaluate FTP and video performance trends and tradeoffs.

The MedLAN model, proposed in [20] contains a mobile device and a consultation point that links to the backbone network in ER. The novelty of this model is devising an 802.11b MAC protocol with Orthogonal Frequency Division Multiplexing (OFDM). While IEEE 802.11 standard does not support QoS by default, the promised performance can be achieved by parameter settings. Some of these include connection establishment delay, throughput, transit delay, residual error rate, protection, priority and resilience. Since the new protocol reduces Bit Error Rate (BER), the throughput was improved from 4mbps to 5mbps. Owens, et al. [39] extend the MedLAN research in the context of security. It is convinced that WLAN can perform safely, as long as robust authentication and security policy are deployed appropriately. Li, et al.[17] Indicate an interesting issue in the design of ER model. The authors emphasize the healthcare delivery should be integrated into the ER model seamlessly by interactive design approach and appropriate evaluation methodologies. Su and Shih [22] quantify the efficacy of medical task based on a ER paradigm. The results show that the performance improved by 3%.

As opposed to MedLAN, the patient care model, developed by Chu and Ganz [27] relies on heterogeneous wireless network. The primary objective is to achieve real time diagnostic data (text file, image and video) from the clinical site to remote control centre. Instead of 802.11b, 802.11g is adopted as high rate wireless standard. The scalability and performance results contribute to a more complex model design. Golmie, Cypher and Rebala [26] pinpoint the Quality of Service (QoS) requirement for WLAN and WPAN.

As an intelligent hospital network, wireless technology is not isolated from the wired backbone. Assaad and Fayek [24] build a multi-site hospital network model for healthcare applications. The authors accentuate the performance of server, workstation and router as a whole.

Cororadal and Szekelyl [21] examine the MAC protocol performance in multicast transmission mode. The proposed model demonstrates the fairness of IEEE 802.11g under various scenarios.

Mean packet delay and packet loss are the major concern in performance analysis of multimedia traffic. Varshney [9] examines the effect of mean packet delay and packet loss in medical application focusing on the UDP traffic over WLANs.

In view of the previous work, we can clearly conclude the criteria for developing a hospital network model: 1) designing less expensive and more realistic method to test the productivity of proposed scheme; 2) constructing better outcomes of quality delivery traffic characteristics and other variables that may affect outcomes; and 3) devising statistical or other that provide more meaningful and credible analysis of presentation of data.

2.6 Modelling issues and challenges

As a multiplexing hospital model, the implementation certainly presents some challenges. The major technical and performance issues involve:

- Integration of wireless components with healthcare delivery. Keep in mind that, the operating parameters should keep aligned to the QoS requirement throughout simulation.
- Bandwidth utilisation of wireless networking is a challenging issue for real time multimedia transmission. As published in [15], IEEE 802.11 provides relatively lower data rate than wired networks, thus the developer tends to adopt a more compromised solution: either reduce the file size or compress the image packets.
- Communication performance that varies constantly with the impact of signal strength, traffic load and interference. As stated in [18], radio signal senses as a curve and attenuates greatly while metallic object and microwave exist within the active range. To ensure devices do not interfere with other electronic equipments (e.g. heart monitors), Soomro and Cavalcanti [3] assert wireless spectrum has to be managed appropriately.
- Finding network devices that are credible and fulfil the QoS requirements, particularly catering the need of scalability and graphical capabilities. In addition, the ease of use, flexibility and security should be taken into account.

2.7 Recommendation

This section reports on the recommendation on operating parameters, performance threshold and security.

2.7.1 Operating parameters

Network performance normally depends on parameters tunings. The major challenges rest with backbone connectivity, application profile and WLAN settings. To make sure the backbone connectivity, one has to determine the source and destination preference, e.g. server IP and supported service. A test bed scenario is recommended in this respect. In addition, the traffic load, traffic distribution and file size need to be considered carefully, to respond to the requirement of the generic hospital model. Assumption making is an important technique that defines the model environment. Once the hospital model is established, one can validate the network performance by tuning/ optimizing the operating parameters until satisfactory results are achieved.

2.7.2 Performance threshold

To obtain a fundamental overview of hospital networks, the effect of network's size and traffic load need to be considered. Technically, the performance threshold reflects user requirement and future growth capacity. For example, with video conferencing, a heavy traffic load responds to the requirements for high resolution (352x240x15 fps) video streaming. Similarly, light traffic load is defined as low resolution (128x240x15 fps) video streaming. As pinpointed by Varshney [9], the combination of resolution, delay, throughput and general system stability impose an impact on the QoS of video streaming. As the user involvement increases, network performance may vary greatly. Hence, appropriate technique (e.g. compression for video conferencing) is required to maintain good quality transmission.

2.7.3 Security

Confidentiality has been a controversial topic as to whether all the patients' records are well protected. In addition, the exposure of patients' records via radio link is considered as potential abuse in hospital environments. Nonetheless, robust authentication and security policy can prevent system from hostile attacks. It is essential to understand how the hospital network model is possibly hacked, and determine what type of applications can be encrypted. Owens, et al. [39] suggests a session-based encryption Wired Equivalent Privacy (WEP) and encapsulation with other security protocol, e.g. IP Secure (IPSec). The authors also recommend a mutual authentication between a client and authentication server. Upon a weakness assessment of Service Set Identifier (SSID) and R4 algorithm,

A security policy defines the aims and goals for a system. As asserted by Banitsas, Tachakra, and Istepanian [15], a good security policy can significantly eliminate the threats by providing a holistic framework for the selection and implementation of countermeasure.

2.8 Summary

This chapter has covered the background material and related work on network modelling. A general requirement has been specified in terms of bandwidth, delay packet loss, reliability, mobility and security. This can be a useful guideline for designing an integrated Hospital network. In addition, each network segment is not isolated from the wired backbone. Thus, upfront assessment should be taken, ensuring the availability, scalability and security of the network infrastructure. Other challenges involve bandwidth utilisation and fairness of communication. To achieve the optimal settings in the hospital network model, a practical criterion has been made. The proposed research methodology is described in Chapter3.

Chapter 3

Research Methodology

Chapter 2 described on the background information and related work on network modelling. This chapter presents the proposed methodology and provides a guideline for performance investigation in a hospital environment.

In view of the previous network evaluation and analysis, performance data can be collected by: experimental measurement [29], analytical modelling [41], or computer simulation [21]. The pros and cons are discussed next.

3.1 Justification of research methodology

Experimental measurement is an effective method that gathers quantitative data of genuine system. Given research benchmarks, such as standard documents executed throughout an experiment, researchers are able to characterize network behaviour. However, a major challenge according to De Jongh, Hajian, and Ligthart [42] is identifying parameters that influence the results and acceptable deviation on the sought parameters. Although it is a costly and prolong process in data investigation, computational capability has been introduced to assist data collection Alvarez, Bustamante, Becker-szendy and Wilkes [43] patent in “interaction of loop” which aims to determine sought parameter values for a model of a data storage system.

The analytical model (mathematical model), is primarily used to predict performance of an emerging application. Although it facilitates parameter tuning and rollout of a new protocol, it cannot reflect the dynamics of data communication networks [44].

As noted in [45], computer simulation is an essential tool that assists practitioners and engineers to tune, debug and optimise network infrastructures. With the wide variety of simulation software, flexibility is significantly inspired in the course of model development while hardware cost is minimized [46]. As regard with a complex hospital network, computer simulation seems an attractive solution over experimental measurement and analytical modelling.

While computer simulation has gained increasing popularity in the recent years, it is still argued that a number of the network simulators tend to focus on solely specific network architecture, and therefore insufficient support are allocated in the domain of devising and analysing live network [47]. Page and Canova [48] also point out that mastering a complex simulation software requires expertise pertaining to building a right model (validation) and building the model in a right way (verification). Methods of validating and verifying a simulation model are fully specified in [49]. The key idea is to achieve sufficient accuracy for the model being built and also the data collected from the simulation process deduce meaningful results. As long as appropriate modelling techniques are used, credible results close to those of genuine systems can be obtained. These modelling techniques involve "observation, interactive participation, project specification and comparison (with real world and other models)" [49].

OPNET Modeller was chosen to study the performance of hospital networks, because it is a credible simulation package that has been tested by numerous researchers worldwide. In addition, it has an easy to use GUI interface and has an extensive library of network components for building simulation model more efficiently, which makes it preferable to other simulation tools, such as NS2 [47] and OMnet [50]. Users adopting OPNET are able to 1) create real-life network scenarios using an exponential number of commercially available network components; 2) reuse and modify network scenarios for volume comparison, saving a great deal of time and money; 3) propose a network protocol with coding capabilities; 4) manage system parameters of all scenarios in one file; 5) insert real time data from other software.

3.2 Model limitation

Adhered to the OPNET product specifications[1], there are still some limitations regarding the WLAN module.

• PCF (Packet Control Function) on noisy links — Not supported

• Power save mode — Not supported

• Authentication and security procedures — Not supported

• Variable transmission rate — Not supported

• Failure and recovery — Not supported

• Roaming and PCF. — Both of these features are implemented individually, but they cannot be used together.

3.3 Investigation guideline

This dissertation follows a step-by-step guideline for performance investigation (Figure 3.1). In the beginning, the key factors influencing network performance are identified through literature review. Step 2 specifies the assumptions on traffic-flow distribution and propagation environments. Step 3 and step 4 determine the performance thresholds and future growth capacity, respectively. By viewing figure 3.1, it is clear that the first four steps are closely related to each other and can be executed at the initial stage. The next step, network modelling is a recursive process that requires careful "deduction and validation" [51]. Upfront assessment as recommended by Salah [52], is applied to a simplified network model. Upon iterative modification and refining, a more complex model is then developed. Step 6 focuses on performance measurement, in which multiple experiments have been deployed to investigate the impact of various traffic types on network performance. By varying network size and traffic load independently, quantitative data, such as throughput, mean packet delay, and packet drop have been collected for data analysis in step 7.

[1] OPNET specifications are available at http://www.opnet.com

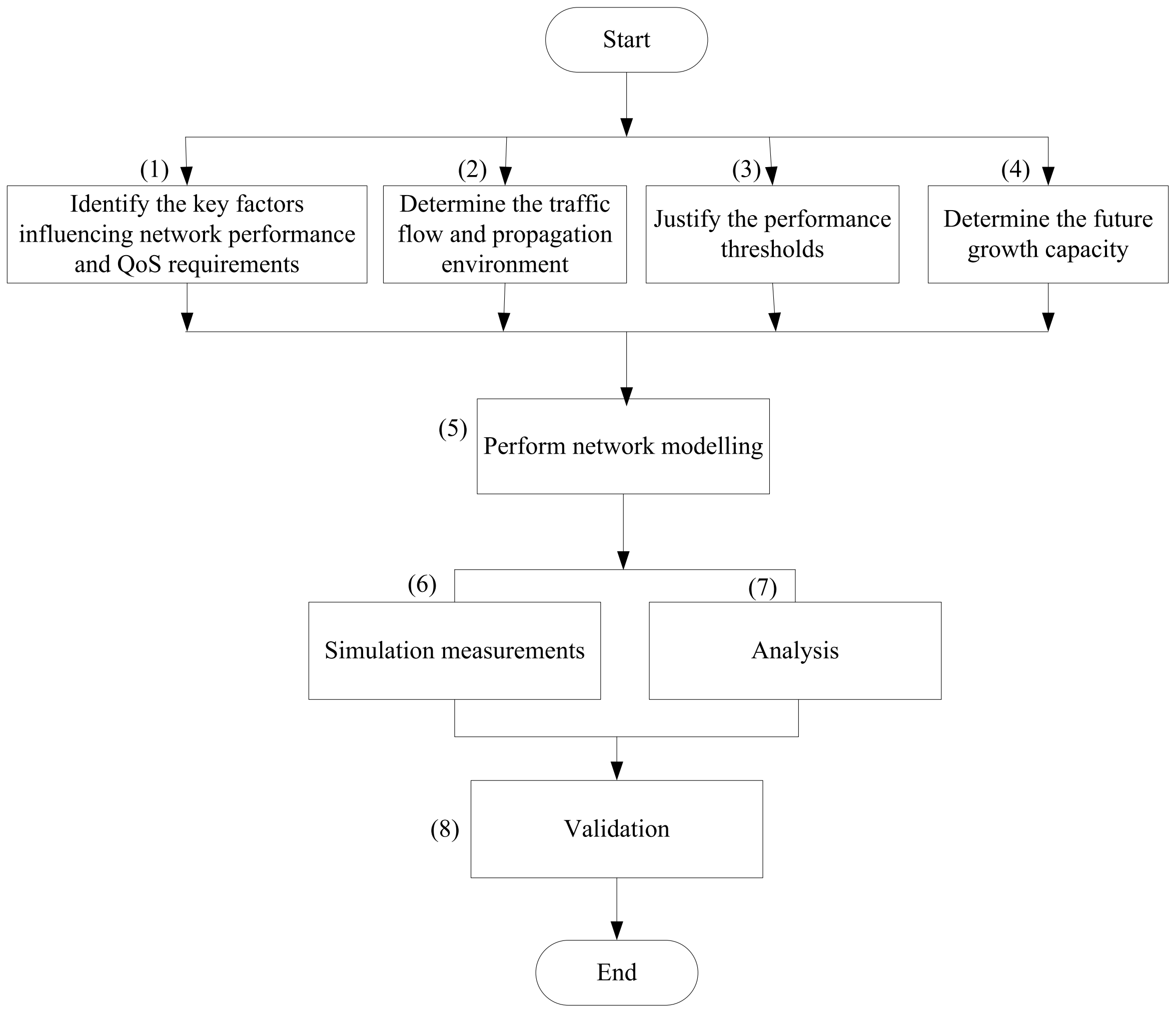


Figure 3.1: Flowchart for performance investigation.

Chapter 4

Modelling the Networks

The intended research methodology was outlined in Chapter 3. This chapter reports on the modelling and simulation of an integrated Hospital network. Due to the proliferation of multimedia service, a sophisticated interoperable network is required for efficient healthcare delivery. Section 4.1 describes on the hardware and software information that were used in the simulation study. Section 4.2 details the network topology and infrastructure which provide ergonomically sound performance for data, voice and video applications. To meet the need of future growth, each network segment is allowed to scale and modify. Detailed system profile and WLAN settings are presented in section 4.3 and section 4.4, respectively. In section 4.5, performance metrics, such as throughput, mean packet delay and packet loss are explained.

4.1 Hardware and software requirement

This section describes on the hardware and software information that were used in the simulation study.

4.1.1 Hardware equipment

A standalone work station was involved here to perform day-to-day maintenance of network simulation. It has met the system requirement adhered to the OPNET product specifications.

- Vendor: Cyclone
- Model: Sentinel
- CPU: INTEL Pentium D 3.00 GHz
- Memory: 2 GB

4.1.2 Software requirement

Hospital network models were developed using OPNET Modeller 14.0. The live license allows well functioning of model objects, while product specifications in general provide standard operation for novice users. With the data exported from OPNET Modeller, Matlab[2] was then used to generate graphics for observation and comparison purposes.

- OPNET Modeller 14.0 with live license
- OPNET Modeller product specifications
- Matlab 2008

4.1.3 Model objects

Model objects refer to a series of network components that allows attribute definition and tuning. Several model objects can somehow perform a functional network, such as a LAN. As more objects are involved, a more complex network can be established. Application config is an essential object that defines the data to be transmitted, file size and traffic load. In general, it supports common applications, namely, FTP, Email, VoIP, Video conferencing, telnet, print and database. Profile config on the other hand determines where the data is received by specifying the interaction between servers and clients. The following model objects involve wired and wireless network components

- Application config
- Profile config
- Server
- Switch
- LAN
- Wireless workstation (fixed and mobile)
- Wireless server (fixed and mobile)
- Wireless routers

[2] The software information is available at http://www.mathworks.com

4.2 Network design

This section presents the logics and building blocks for model establishment. In the beginning, a high speed backbone network was established to support a wide variety of medical applications and to interoperate with WLAN components. The parameter settings are described next.

As shown in Figure 4.1, the hospital network (1000m by 1000m) covers two buildings, each connected to a server segment. The central switch acts like a network coordinator, providing gigabit connectivity for all types of applications, as well as maintaining the centralized administration, performing tasks such as filtering, authenticating and fast failure recovery. The backend servers distribute voice, video and data traffic continuously, forming the core of the hospital network. VLAN technology was exploited here to deliver the predefined applications. It is commonly used for logical/ departmental network design. The great advantages of using VLAN relate to remarkable broadcast reduction and the ease of administration. In addition, it enhances security by managing the access lists. For instance, ICU users refer to vlan300, therefore they are only allowed to access video conferencing applications.

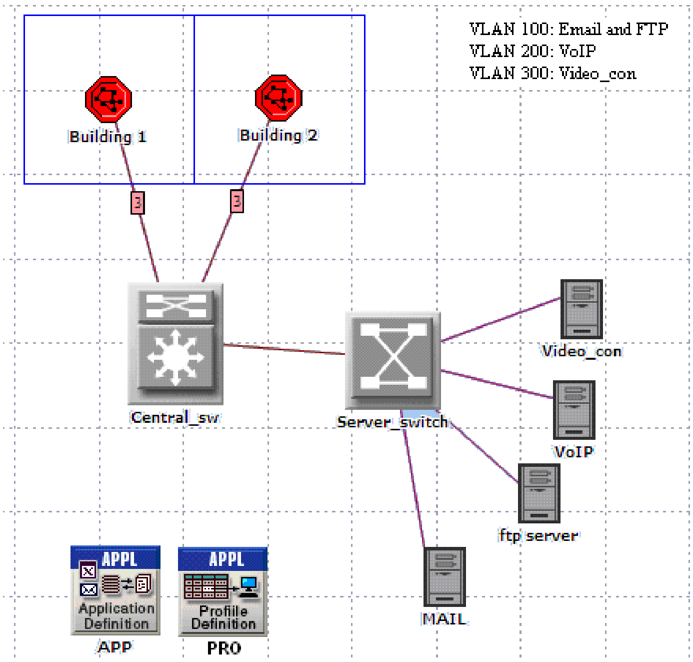


Figure 4.1: OPNET presentation of a typical hospital backbone netowork.

All the VLAN and application settings were maintained by application definition (APP) and profile definition (PRO) in OPNET. An application definition specifies the traffic flow distribution and supported service. As per the requirement for bandwidth utilization, each application was defined with light and heavy traffic load individually. The key attributes involve packet inter-arrival time and file size. A user profile, on the other hand, was built using various application definitions. In this study, email and FTP were created for data traffic analysis, denoted as vlan100. Real time applications, such as VoIP and video conference were mapped into vlan200 and vlan300 respectively, representing audio and video traffic. An application may have tasks; a task may have multiple phases. All the tasks and phases were determined by start time, offset start time, end time and repeatability.

The core layer of a tyical hospital network has been described above, this section continues the illustration of a building access submodule. As shown in Figure 4.2, a switched network design is used on each floor. The use of Ethernet swich ensures high-speed connectivity as well as dedicated bandwidth for demanding users. It is extremely handy for emergency applications which require a low rate but zero fraud toleration. For scalability reason, workstations and APs are plugged into a high-end Ethernet switch on each floor, which allows scalability when the port limit is esceeded. Since all the swithed LANs are uplinked to the central switch, network access and broadcast control can be achieved more resiliently. In each department, VLANs are activated for application assignment. According to the user profile, vlan100 refers to email and FTP applications, vlan200 and vlan300 refer to VoIP and video conferencing, respectively.

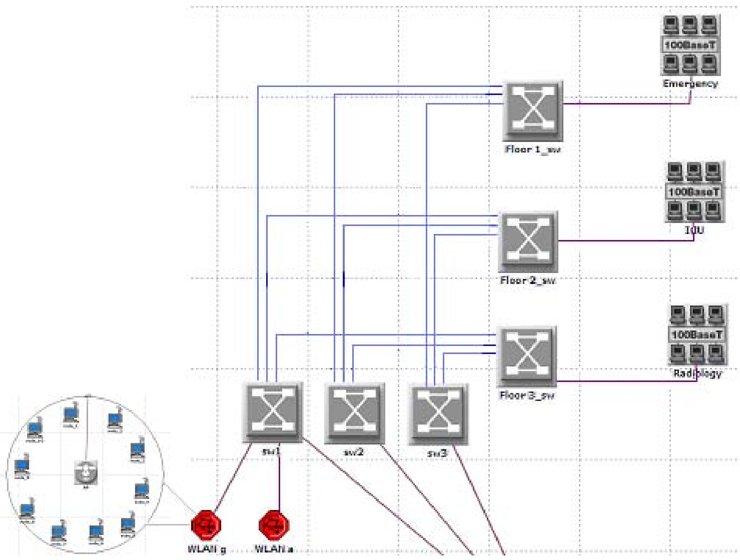


Figure 4.2: OPNET presentation of a building sub-module.

4.3 Traffic flow distribution

The duration considered for the simulation, pertaining to data, audio and video transmission is 20 minutes. As specified in [53], the time distribution for medical imaging has a constant exhibit. Accordingly, the time period can be denoted as **constant (t)**, in which **t** is the time spent in a simulation task. Likewise, the file size corresponds to **constant (b)**, in which **b** stands for the number of bytes. For trend prediction and fairness analysis purpose, all the traffic flows in this dissertation are implemented in a Constant Bit Rate (CBR) environment.

Table 4.2 shows the parameter settings for various types of application. Since email and FTP transfer files at a fixed interval, constant (3600) is assigned for light traffic load and constant (360) assigned for heavy traffic load. As explained in the OPNET product specifications, the start time for a file transfer session is computed by adding the inter-request time to the time that the previous file transfer started. We specified the start time as constant (2) and the repeatability time as constant (300). An interesting issue arise as to how badly the network reacts when the actual time taken for a file session is greater than the inter-request time. In view of this issue, the file size for email and FTP varies from constant (500) to constant (15000000).

Video_con on the other hand tends to rely on frame rate for the incoming and outgoing streams. The higher the frame rate, the higher the quality. Light video_con corresponds to a low quality stream with a combination of 10 fr/sec and 128x120 pixels. Similarly, Heavy video_con corresponds to a high quality stream with a combination of 15 fr/sec and 128x120 pixels.

Voice packets are generated in a very different way from others. Each packet encapsulates a certain number of encoded voice frames before being sent by the application to the lower layers. This dissertation follows the widely adopted guidelines of G.729 [54] for VoIP deployment. Two types of payload sizes are used: 10 ms and 20 ms, which correspond to 800 packets and 400 packets, respectively.

Table 4.1: Parameter settings for various types of application.

Application	**Distributed Interval**	**Encoder Scheme**	**File Size (byte / pixel /ms)**	**Compression delay (sec)**
Light email	Constant (3600) sec	-	Constant (500)	-
Heavy email	Constant (360) sec	-	Constant (2000)	-
Light FTP	Constant (3600) sec	-	Constant (50000)	-
Heavy FTP	Constant (360) sec	-	Constant (15000000)	-
Light video_con	10 fr/sec	-	128 x 120 pixels	-
Heavy video_con	15 fr/sec	-	128 x 240 pixels	-
Light VoIP	1fr/ packet	G. 729	10ms	0.02
Heavy VoIP	1fr/ packet	G. 729	20ms	0.02

4.4 WLAN configuration

In this dissertation, WLAN components were integrated into the wired backbone for performance investigation. It was assumed that all transmission tasks took place in an ideal environment where noise was minised. In addition, the interference between wireless devices was considered as zero. Since WLAN 802.11 a and g operated in varied spectrum bands, they would not interfer with each other.

Table 4.3 demonstrates the parameter settings used in a WLAN. It is clear that WLAN 802.11a and g vary in physical modulation. The received packet power threshold determines the signal strength in radio propagation environments. Presumably, the signal strength is set to -88dBm in line with the vendor standardization [55]. To maintain the efficient queuing scheme, the Rts threshold and fragmentation threshold are set to 2304 bytes and 2348 bytes respectively. Buffer size is another important attribute that influences the media streaming. It is set to 2468000 bits.

Table 4.2: Parameter settings of WLAN (802.11a / g).

802.11a/g parameters	Values
Physical Parameter	OFDM / Extended PHY
Data Rate (mbps)	54
Packet Reception-power Threshold (dBm)	-88
Rts Threshold (bytes)	2304
Fragmentation Threshold (bytes)	2348
Buffer size (bits)	2468000

4.5 Performance metrics

Performance metrics refers to a set of measures that quantify performance results for visualization and comparative purposes. As explained by Abdullah, Moinudeen, and Al-Khateeb [30], throughput, mean packet delay and packet drop have been widely used in data communication networks. Nonetheless, specific application demands on an own set of performance metrics. For instance, email and FTP rely on upload response time and download response time. VoIP and video conferencing are deemed to real time interaction and therefore sensitive to mean packet delay, packet delay variation and packet drop. More details of performance metrics used in this dissertation are described as follows:

Throughput: represents the efficiency of traffic successfully received and passed onto the upper layer. It is measured by kbps.

Mean packet delay: also known as "end-to-end delay", is important for audio and visual traffic [36]. End to end delay for a voice packet is measured from the time it is created to the time it is received. As noted by Latkoski, et al.[5], minimum end-to-end delay is always expected to achieve interactive real time session. In reality, natural human interaction is guaranteed by 80ms or less delay. More conservatively, 100ms is acceptable due to the encoding, decoding, compression and decompression process in the course of packet transmission [52]. The aggregate amount of end-to-end delay is denoted as delay in OPNET. Data can be dropped in the case of "buffer overflow" or "retransmission failed"[56]. It is measured by kbps.

Packet delay variation: measures the end-to-end delay variance of packets (either visual or audio) designated for one node.

Jitter: is a particular instance that works out the tendency of packet delay variation between two consecutive packets. It is reserved for voice packet only.

Packet drop: measures the number of dropped traffic within a time period. As explained in [54], packets can be dropped in occasion of full buffer or retransmission threshold exceeded. Video and voice stream are sensitive to packet drops.

Upload response time /download response time: are used to measure the performance of email and FTP traffic. Time elapsed between sending a request and receiving the response packet. 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.

4.6 Assumptions

Since the simulation model involved various applications and scenarios; environment control is expected to eliminate the unwanted factors. As pointed out by Sargent [57], good environment control can improve the accuracy of simulation model. Thus, a few assumptions were made prior to data collection.

A1 : All applications are running throughout the generic hospital model individually, so that the effect of variables (such as network size, traffic load and signal strength) can be observed clearly.

A2 : Data traffic (FTP and email) are presumably running in radiology scenario. VoIP and video conference traffic on the other hand are characterized as voice and video traffic respectively. The former is preferred in Accident & Emergency ward, while the latter is appointed to ICU scenario. Explicitly, the departmental solution is achieved by using VLAN design as introduced in chapter 4.

A3 : CBR traffic is defined as the distribution throughput the generic hospital model.

A4 : The generic hospital model is scaled as small network ($x \leq 50$ nodes), medium network ($50 \leq x \leq 100$ nodes) and large network ($x \geq 300$ nodes), respectively.

A5 : All traffic are running in an ideal propagation environment in which the radio interference can be ignored. The signal strength is otherwise determined by the active distance and received power only.

A6 : The signal strength thresholds are configured as -50, -70, -88 and -110, dBm in WLAN. Accordingly, strong ($s \geq -50$ dBm), medium ($-70 \leq s \leq -50$ dBm), fair ($-88 \leq s \leq -70$ dBm) and weak signal ($s \leq -110$ dBm) are defined for the radio propagation.

A7 : WLAN 802.11 a and g can coexist and produce accumulatively higher throughput.

4.7 Experimental design

The generic hospital model was established for internal network interaction, thus router performance for metropolitan network (site-to-site implementation) can be excluded in this case. More importantly, the performance of client, server and WLAN and their network behaviours were investigated.

Client Performance: As shown in Table 4.1, three piloted case studies look at client performance in scenario 1, 2, 3, respectively. Each scenario investigates the impact of a specific traffic type (e.g. data, voice and video) on network performance. By increasing the number of nodes and payload sizes, the network behaviours are observed as well. The performance is primarily measured by throughput and mean packet delay. However, depending on the traffic type, additional performance metrics are required. For instance, the quality of VoIP depends on jitter, packet delay variation, mean packet delay and throughput. FTP and email, on the other hand, prefer upload response time and download response time to reflect the efficacy.

Servers Performance: Scenario 4 -7 examine the traffic successfully sent by a server within a fixed time period. The primary performance metric employed is throughput. In most transmission tasks, TCP (Transfer Control Protocol) is exploited to examine the quality of traffic that departure from transport layer to other layers.

WLAN performance: in scenario 8, the WLAN performance is measured by throughput, delay and packet drop. By viewing the traffic behaviours in 802.11a and g, one can obtain a fundamental overview of wireless implementation in medical environments. In scenario 9, impact of signal strength threshold on network performance is investigated.

Table 4.3: Description of the experimental design.

<table>
<tr><th>Scenarios</th><th>Description of the experiments</th><th>Performance metrics</th></tr>
<tr><td>1</td><td>Investigated the impact of data traffic on network performance, by increasing the number of nodes and file size. Rich-text file and image file were denoted as light traffic load and heavy traffic load, respectively.</td><td rowspan="9">Email, FTP: upload response time and download response time.

VoIP: jitter, packet delay variation, mean packet delay and throughput.

Video_con: packet delay variation, mean packet delay, throughput.

Server: throughput.

WLAN: throughput, mean packet delay, and Packet drop.</td></tr>
<tr><td>2</td><td>Performed a simulation measurement of voice traffic under various sizes of networks. Voice payload sizes of 10ms and 20ms were used as light traffic load and heavy traffic load, respectively.</td></tr>
<tr><td>3</td><td>Conducted a comparative study to measure the network performance of video traffic under various traffic loads in a small, medium and large network, independently.</td></tr>
<tr><td>4</td><td>Quantified the traffic sent by a FTP server.</td></tr>
<tr><td>5</td><td>Quantified the traffic sent by an email server.</td></tr>
<tr><td>6</td><td>Quantified the traffic sent by a VoIP server.</td></tr>
<tr><td>7</td><td>Quantified the traffic sent by a video server.</td></tr>
<tr><td>8</td><td>Compared the network performance of WLAN 802.11a and 802.11g.</td></tr>
<tr><td>9</td><td>Investigated the impact of signal strength threshold on network performance. The signal thresholds110,-88, -70, -50 dBm) denotes as weak signal strength, medium signal strength and strong signal strength</td></tr>
</table>

4.8 Summary

This chapter reports on the modelling of an integrated hospital network and experimental design. Due to the proliferation of multimedia service, a sophisticated interoperable network is required for efficient healthcare delivery. The detailed network topology and infrastructure which provide ergonomically sound performance for data, voice and video applications were presented. To meet the need of future growth capacity, each network segment is allowed to scale and modify. Detailed system profile and WLAN settings are presented. Performance metrics, such as throughput, mean packet delay and packet loss are explained.

Chapter 5

Results and Analysis

In Chapter 4, the detailed hospital network modelling and experimental design were presented. This chapter explains experimental results for an integrated network scenario in the hospital settings Section 5.1 describes the network behaviours of client, server and WLAN, individually. The focus is to identify the optimal settings and potential issues for medical content delivery. Section 5.2 discusses the effect of traffic load, network size and signal strength on network performance. An insight has been gained into the futuristic network design and deployment of QoS provision. Model validation and proposed improvement are discussed in section 5.3 and 5.4, respectively.

5.1 Interpreting the results

Three simulation studies were investigated to observe the network performance of data, voice and video traffic under various performance conditions. The first study was carried out for examining the quality of client performance, including wired and wireless nodes. As per file size (FS) requirement, heavy and light traffic load were applied to small (N = 50), medium (N = 100) and large network (N = 300), individually. N was short for the number of nodes. In the second study, server performance was investigated, focusing on server throughput and system stability. In the third study, various signal strength thresholds (S) were used to identify the optimal settings of APs. Mean packet delay, throughput and packet drop were exploited for WLAN performance measurement. For verification reasons, the time series (x axis), in relation with connection initialization and distributed interval are observed, in comparison with the predefined parameters. If these time series are logically linked to the predefined parameters over a simulation time period, then the performance results (y axis) are realistic.

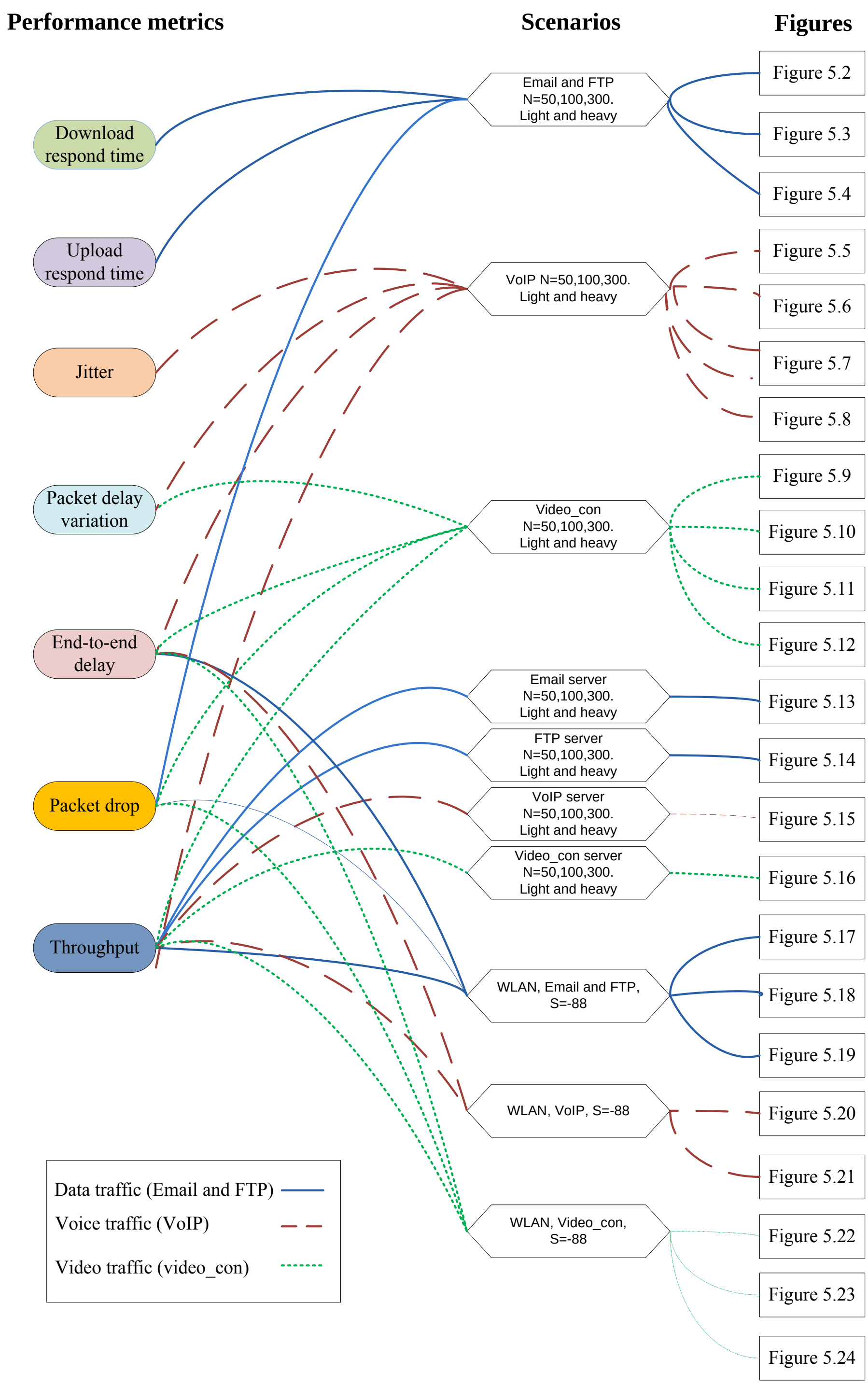


Figure 5.1: Summary of results.

Figure 5.1 provides overall information of performance metrics and figures used in various scenarios. As illustrated, email and FTP generate data traffic and primarily rely on download response time and upload response time for performance evaluation. VoIP and video conference belong to real time interactive applications and generate packets in a different way. Thus, their performance were measured by packet delay variation, end-to-end day delay, throughput and packet drop. For quality reason, VoIP also has requirement on jitter. All transmission tasks last for 20 minutes.

To achieve simulation accuracy, five replications were run with different initial seeds in OPNET. Five simulation replications were sufficient, as each simulation replication produced very similar graphical results.

5.1.1 Client performance

The impact of data traffic (N= 50, 100, 300 nodes; FS=500, 2000, 50000, 15000000 bytes)

This study was carried out to observe how FTP and email applications perform in radiology scenario. Light and heavy traffic loads were defined in OPNET, presenting the requirement for rich text files (e.g. patient's profile and lab test results) and graphical images (e.g. Xray images) respectively. The detailed parameter settings as regards with file size and distributed interval were described in Chapter4. For comparison reasons, the target applications were run in various sizes of networks (50, 100 and 300 nodes). Ultimately, the simulation results were validated using real life data obtained from previous studies.

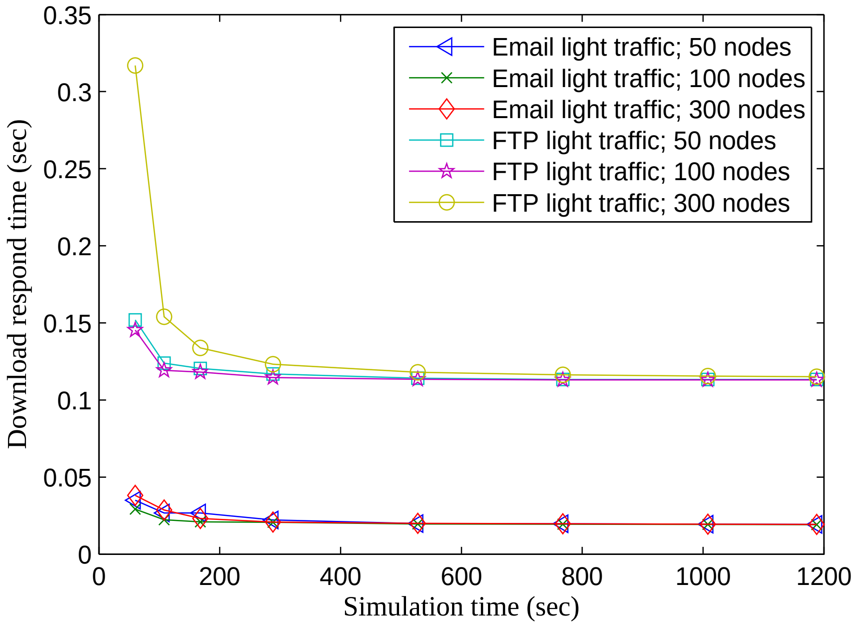
Download response time and upload response time are crucial to data traffic measurements, as they evaluate the efficiency and effectiveness of download / upload activities. The lower the value obtained, the faster the task proceeds.

Figure 5.2 illustrates the download response time (FTP and email). Y axis stands for download response time, while X axis stands for simulation time. It is found that all transmission tasks commenced within the first few seconds and tended to be steady in the long run, although a steep drop occurred in the beginning. The delay for the first generated packet is realistic because the encryption process (e.g. VPN enabled transmission) in reality is activated before the applications commence. Another interesting finding is that light FTP traffic accounted for higher response time when compared to email traffic. The margin between them was due to the file size and arrival interval configuration. In reality, email attachments are normally smaller than FTP files; therefore, Email transmissions run faster than FTP transmissions.

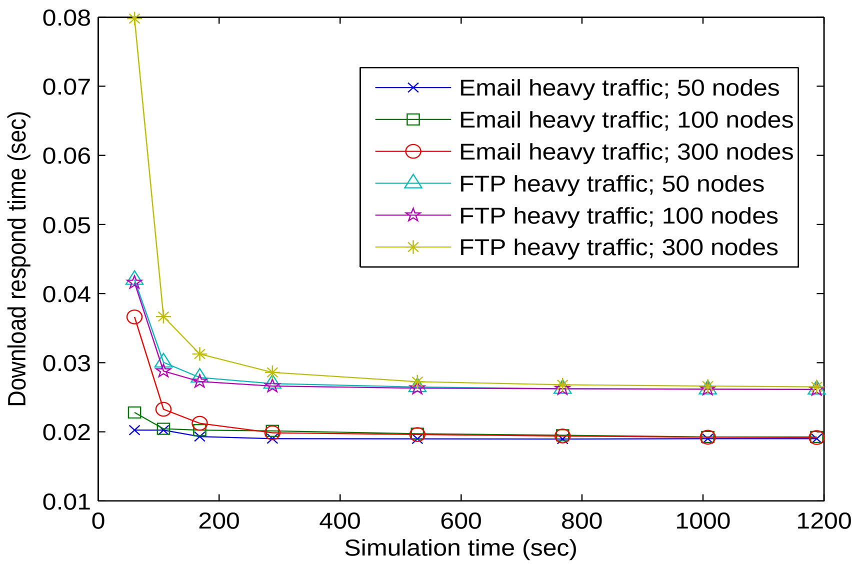
Provided all workstations start downloading simultaneously, extra load will be gained from the increased network size, which will eventually result in more response time to complete the task. From the observation in Figure 5.2a, a rich-text FTP file (50000 bytes) took 0.12 sec response time in a small network, 0.125 sec in a medium network and 0.14 sec in a large network. Similarly, the time taken for an email file (500 bytes) was 0.01 sec in a small network, 0.016 sec in a medium network and 0.021 sec in a large network, respectively. All download response time are less than one second, which is in keeping with the QoS requirements discussed in Chapter 2. Even when executing download task continuously, an operator will not feel overwhelmed.

The findings above revealed the performance of FTP and email applications when a light traffic was loaded. A comparative study was conducted to observe the effect of heavy traffic load, as outlined below.

Figure 5.2b demonstrates the download response time for transmitting an image files. In a small network, approx 1.6 times download response time (as much as light FTP traffic) was spent acquiring an image file (15000000 bytes). The same file was applied to a medium and large network, approx 0.8 and 0.95 times the response time were spent respectively. Likewise, an email image file (2000 bytes) resulted in 1.1 times for a small network, 1.15 times in a medium network and 1.5 times in a large network.



(a)



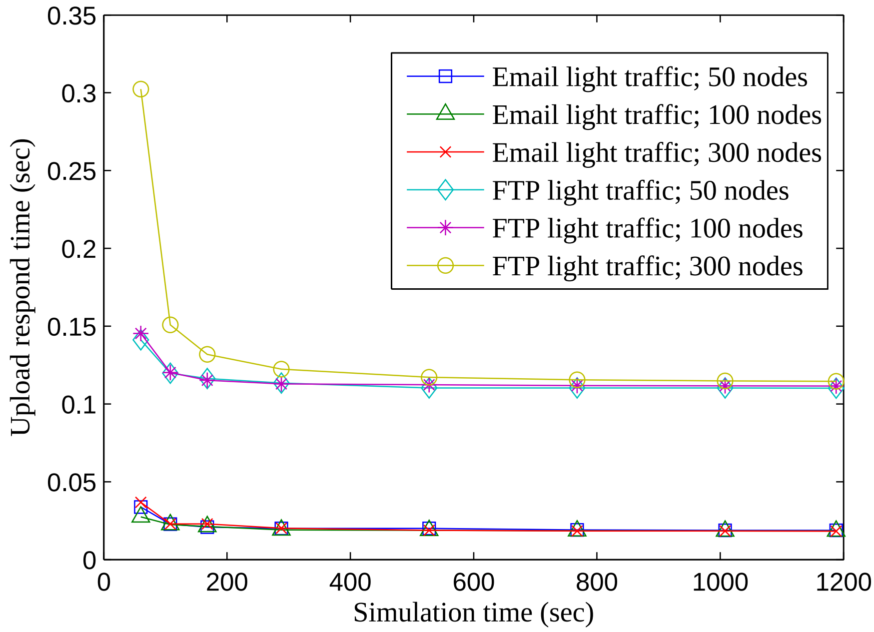
(b)

Figure 5. 2: Comparison of download response time of FTP and email: (a) Light traffic; (b) Heavy traffic.

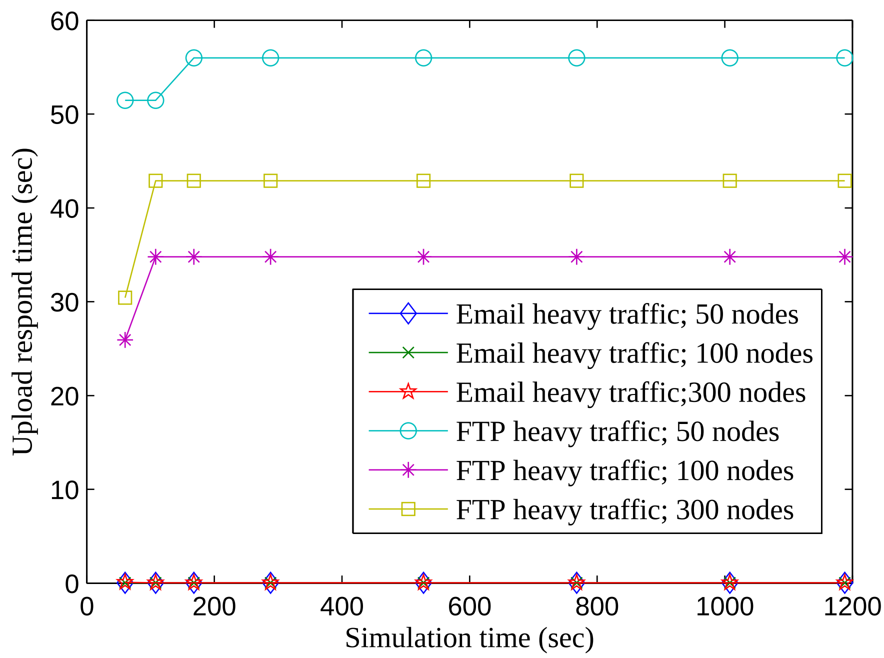
Figure 5.3 compares the upload response time of FTP and email respectively. As shown in Figure 5.3a, all upload response times reduced sharply within the first minute and then continued to stabilize until the end of the transmission tasks. In a small network, the average upload response time for FTP is approx 0.117 sec, which is approx 0.9 times as much as for a large network. In terms of email traffic, the average response time varied from 0.021 sec (small network) to 0.025 sec (large network). Corresponding to the QoS requirements, all upload response times are less than one second. In addition, no packet loss occurs in this scenario, since the received traffic curve overlaps with the sent traffic curve. Thus, smooth transmission can be ensured. Such light upload tasks considerably assist doctors' day-to-day operation.

The upload response time however varies greatly when adding heavy a traffic load. From the observation in Figure 5.3b, an image file (15000000 bytes) via FTP application resulted in a 56 sec response time in a small network, 35 sec in a medium network and 42 sec in a large network. Due to the limited uplink, a much higher response time was required in heavy traffic situations. It seems the small network cannot accommodate such a heavy traffic and behaved strangely. As a matter of fact, network performance degrades as the actual time taken for a file transfer session is greater than the inter-request time. To counter this, a file size restriction should be configured properly.

When uploading an image file (2000 bytes) via email, the results was different. Since the file size was smaller, the time spent was far less than FTP. All the upload response times were less than one second, regardless of the incremental network size.



(a)



(b)

Figure 5. 3: Comparison of upload response time of FTP and email: (a) Light traffic; (b) Heavy traffic.

Packet drop refers to the amount of traffic per second not successfully received by the clients. It occurs due to the retransmission threshold exceeded. Figure 5.4 explains the packet drop of email and FTP in various sizes of networks. Out of 6 scenarios, only FTP resulted in packet drop in a small network and none of others. Even light traffic did not incur any packet drop under the same network settings. The first packet drop for FTP was observed at the initial stage. As the simulation task proceeded, packet drop increased dramatically and reached a peak of 400 bps, followed by a reduction until end of simulation task. The average packet drop of FTP was approx 85 bps. By viewing back upon Figure 5.3b, it is found that packet drop led to the huge delay of upload response time in a small network.

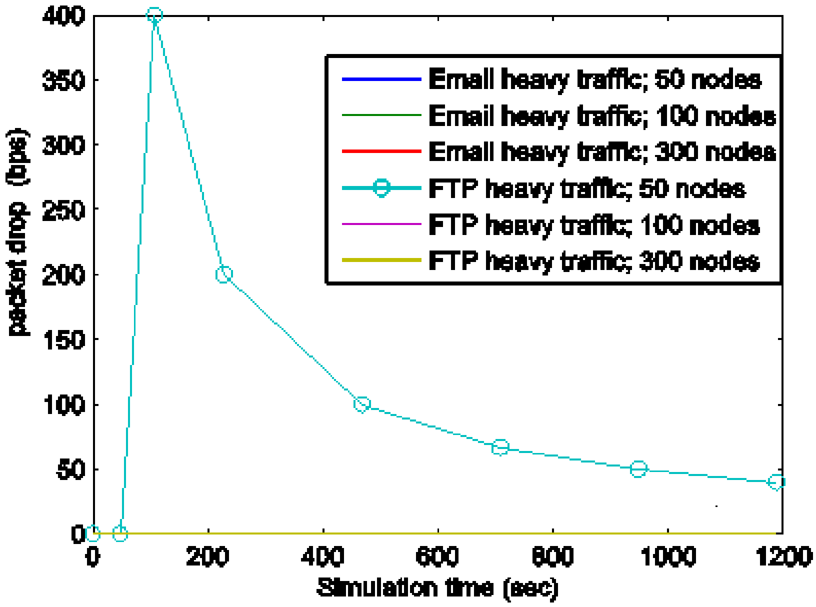


Figure 5.4: Comparison of FTP packet drop.

The impact of voice traffic (N= 50, 100, 300 nodes; FS=10, 20 ms)

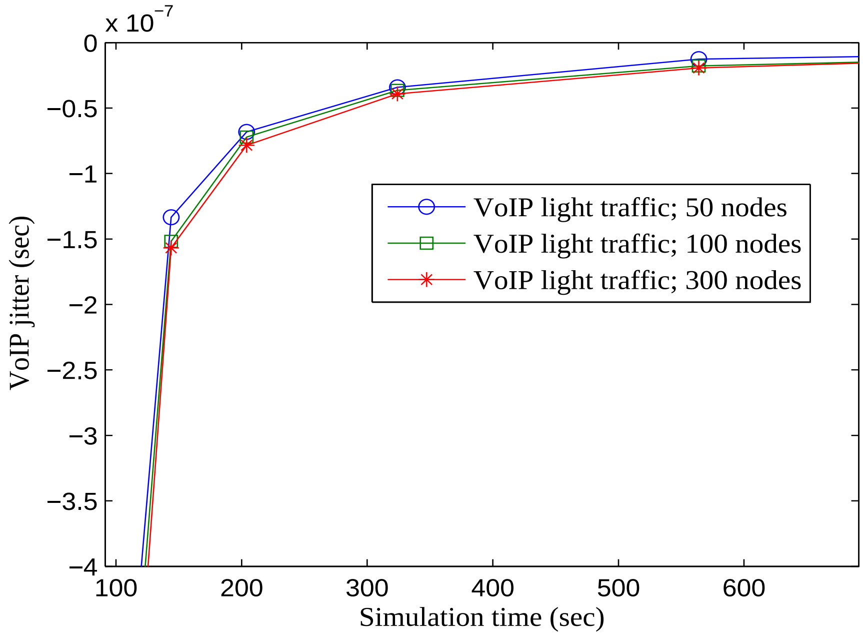
The performance of VoIP was examined by increasing the number of nodes as well as voice payload sizes. The popular G.729 standard has been selected because of its low bandwidth requirement. The voice payload sizes of 10 ms and 20 ms were denoted as light traffic and heavy traffic, respectively. In addition, the call distribution and the average number of calls per second were obtained from the call records during a peak hour in hospital. These numbers are used to adjust the application and profile settings. Detailed parameter settings were configured in Chapter 4.

The quality of VoIP depends on jitter, packet delay variation and end-to-end delay. Jitter can be exploited to measure a variety of signal qualities (e.g. voice and pulse width). Analogous to other periodic signals, voice packets are created at a fixed rate during conversation. However, jitter varies constantly as described by Broustis, et al. [32], which leads to play-out delay. To counter such play-out delay, VoIP normally employs play-out buffer with expense of extra delay of packet loss. Some researchers in [32] suggest using QoS embedded devices to guarantee a high quality connection.

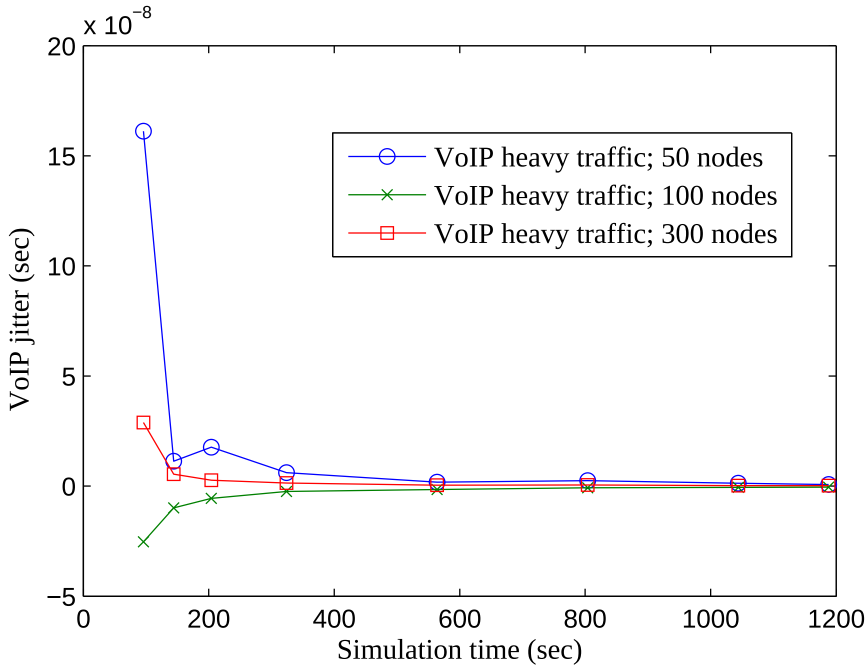
Figure 5.5a compares the VoIP jitter under various scenarios. The negative jitter here indicates the time difference between two consecutive packets at the destination node is less than that at the source node. Clearly, the average jitter in a small network was found to overwhelm others in medium and large networks. As the simulation proceeds, all the jitters are prone to reach zero after an exponential rise in the beginning. Such tendency is due to the encoding process activated for VoIP. Explicitly, each voice packet at the sending end encapsulates certain number of speech samples and adds the RTP, UDP, IP and Ethernet headers, which leads to variations or jitter in delay. A playback buffer at the receiving end however absorbs such variations or jitter and thereby provides smooth playout.

The findings above revealed the performance of jitter in each scale of network (small, medium and large). A comparative study was conducted to observe the effect of heavy traffic load on network performance, as outlined below.

As illustrated in Figure 5.5b, the jitter varied slightly as the number of nodes increased. In a small network, the jitter dropped abruptly from 17 x 10^{-5} ms to 0.2 x 10^{-5} ms. In medium network, the jitter started with -2 x 10^{-5} ms and then climbed up gradually until the end of simulation task. As opposed to the negative values derived from the medium network, positive values were found in a large network. The jitter varied from 3 x 10^{-5} ms and to 0.1 x 10^{-5} ms gradually. Although fluctuations were observed in the first few minutes, all jitters tended to get as closed to zero as possible.



(a)



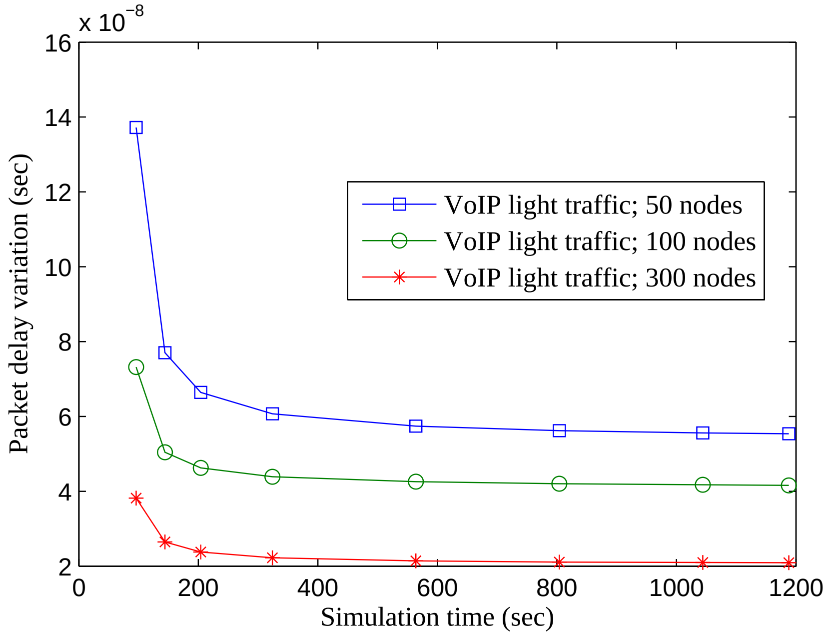
(b)

Figure 5. 5: Comparison of jitter of VoIP: (a) Light traffic; (b) Heavy traffic.

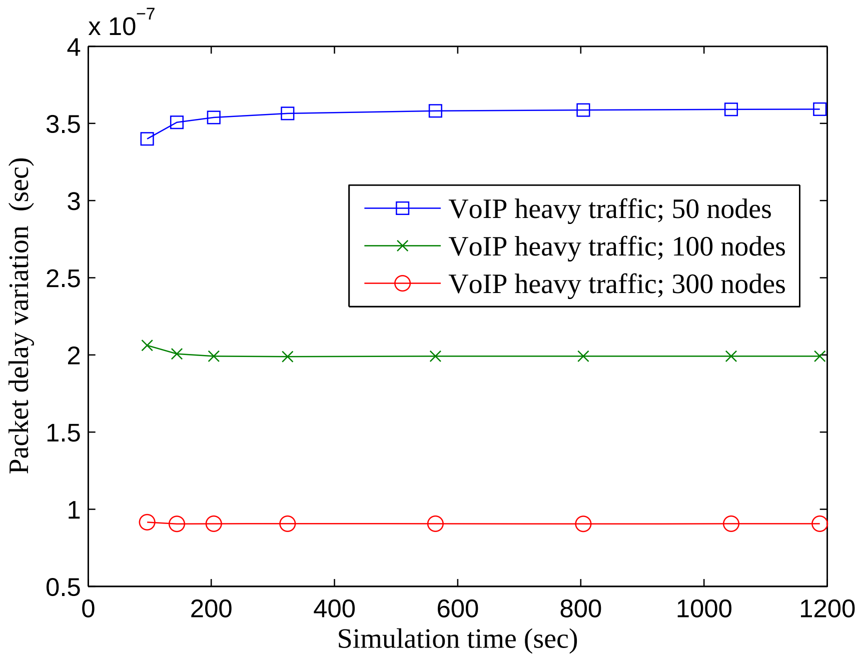
Figure 5.6 compares the packet delay variation derived from various scenarios. When a light traffic load was used, the highest packet delay variation was found in the beginning, approx 14 x 10^{-5} ms in a small network, 7.9 x 10^{-5} ms in a medium network and 4 x 10^{-5} ms in a large network. Subsequently, the curves dropped gradually and tended to stabilize until the end of simulation task. Among three transmissions tasks, the packet delay variation of small network exceeded others by 0.7 x 10^{-5} ms in medium and by 3.6 x 10^{-5} ms in large networks. Since the packet delay variation is far less than 30ms, it would not cause severe delay.

The findings above revealed the performance of packet delay variation in each scale of network. A comparative study was conducted to observe the effect of heavy traffic load on network performance, as outlined below.

Figure 5.6b shows the packet delay variation changed slightly under heavy traffic loads. In a small network, the packet delay variation started with 3.3 x 10^{-4} ms and then levelled up to 3.6 x 10^{-4} ms, followed by a plateau for the rest of time. Lower packet delay variation was found in the medium network, approx 2 x 10^{-4} ms. In parallel with that, the curve standing for large network tended to remain the same throughout the simulation task. The average packet delay variation was 0.8 x 10^{-4} ms. As opposed to the light traffic load, heavy traffic load yielded approx 6 times packet delay variation in the small network, 5 times in the medium network and 10 times in the large network, respectively. In other words, the packet delay variation is more aggressive in heavy traffic situations.



(a)



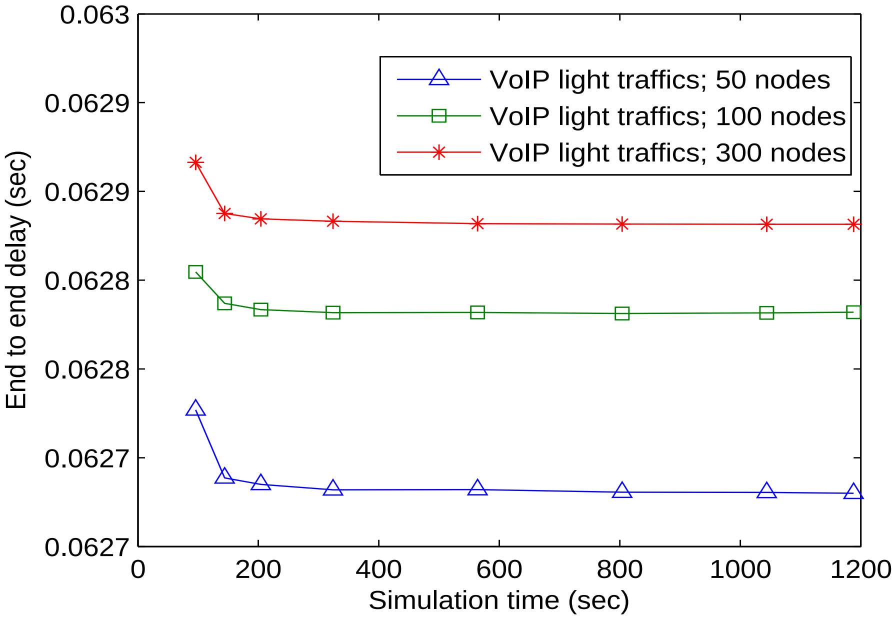
(b)

Figure 5. 6 : Comparison of packet delay variation of VoIP: (a) Light traffic; (b) Heavy traffic.

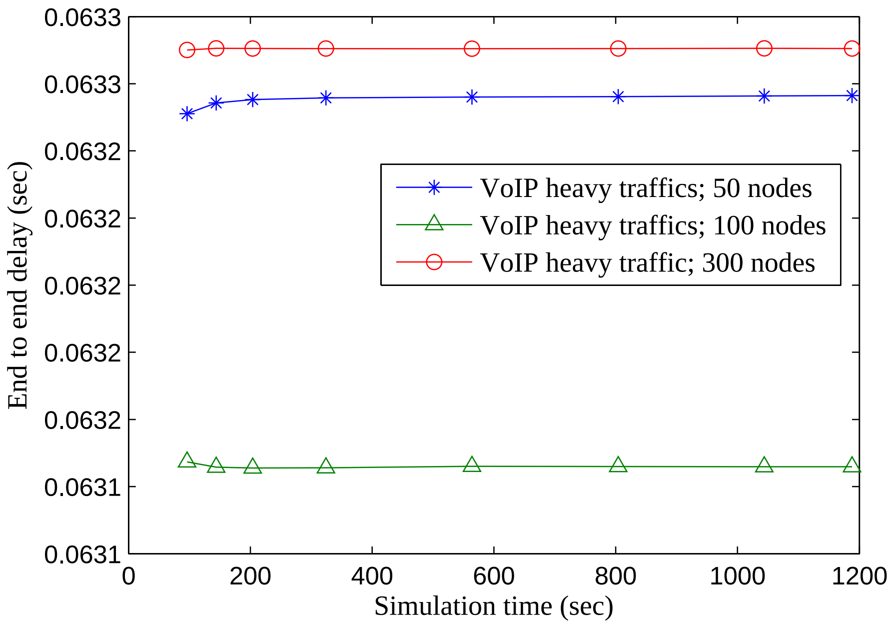
End-to-end delay for a voice packet is measured from the time it is created to the time it is received. High end-to-end delay indicates high chance of echo overlapped with the original voice.

Figure 5.7a shows the end-to-end delay among three VoIP scenarios. The highest end-to-end delay was observed in a large network, approx 62.9 ms. As the simulation proceeded, end-to-end delay dropped a tiny bit and tended to remain the same for the rest of time. Lower end-to-end delays were found in a medium network and small network, approx 62.8 ms and 62.7 ms, respectively. Since the end-to-end delay is less than 150 ms, smooth connectivity can be maintained for real time interactive communication.

Figure 5.7b on the other hand shows the end-to-end delay when heavy traffic overloaded. The highest end to end delay was also found in the large network, approx 63.33 ms. As the network size decreased, 63.31ms and 63.15ms were observed in the medium network and small network, respectively. Overall, the end-to-end delay is slightly higher than light traffic load, which is due to the increased volume of calls.



(a)



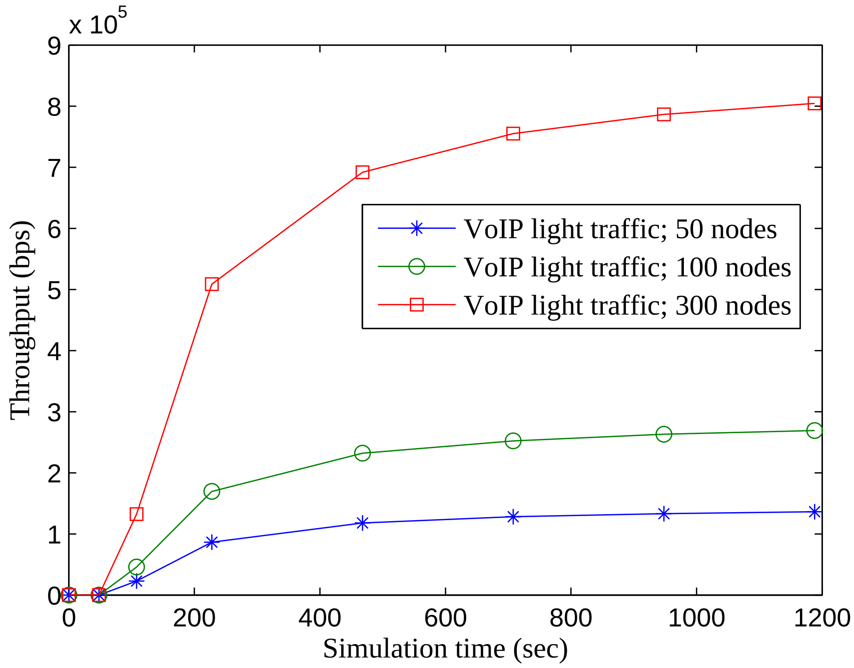
(b)

Figure 5.7: Comparison of end to end delay of VoIP:

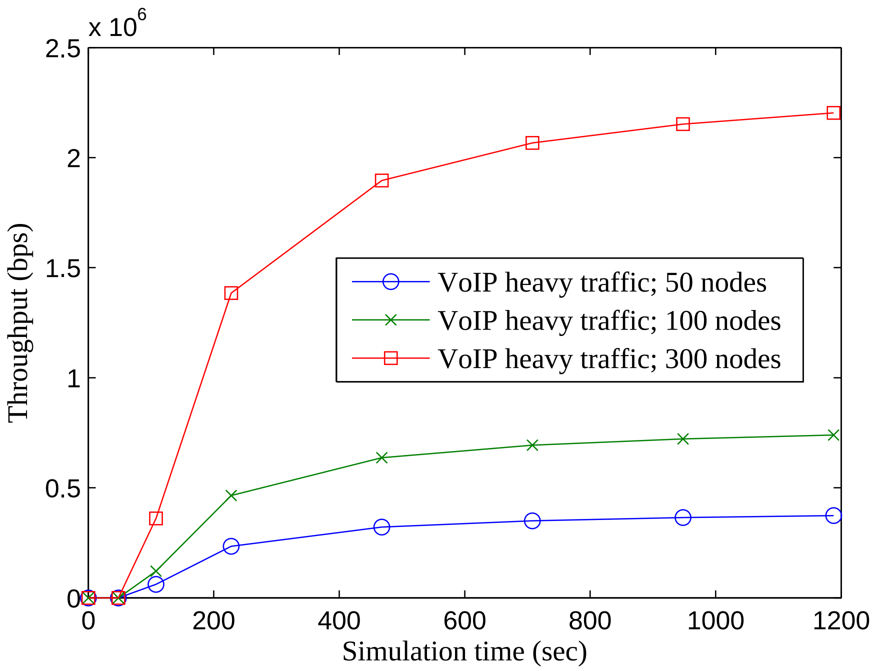
(a) Light traffic; (b) Heavy traffic.

Throughput refers to the amount of traffic successfully received by the destination node. The call capacity can be predicted by observing the throughput in the peak hour. Figure 5.8a compares the throughput derived from various network scenarios. The curve on top represents the throughput provided by a large network. From the very beginning, the throughput increased abruptly and attempted to exceed 800 kbps in the long run. As the network size shifted to medium, lower throughput was found. The average throughput was approx 270 kbps. Similarly, the throughput in a small network continued rising in the beginning and then stabilised until the end of simulation task. The average throughput was 130 kbps.

As shown in Figure 5.8b, increased throughputs were generated by heavy traffic loads, approx 2.4 mbps in a large network, 750 kbps in a medium network and 300 kbps in a small network, respectively. As discussed earlier, the data rate required for conveying VoIP packets is in general less than 100kbps. Hence, real time interactive communication can be fulfilled.



(a)



(b)

Figure 5. 8 : Comparison of throughput of VoIP: (a) Light traffic; (b) Heavy traffic.

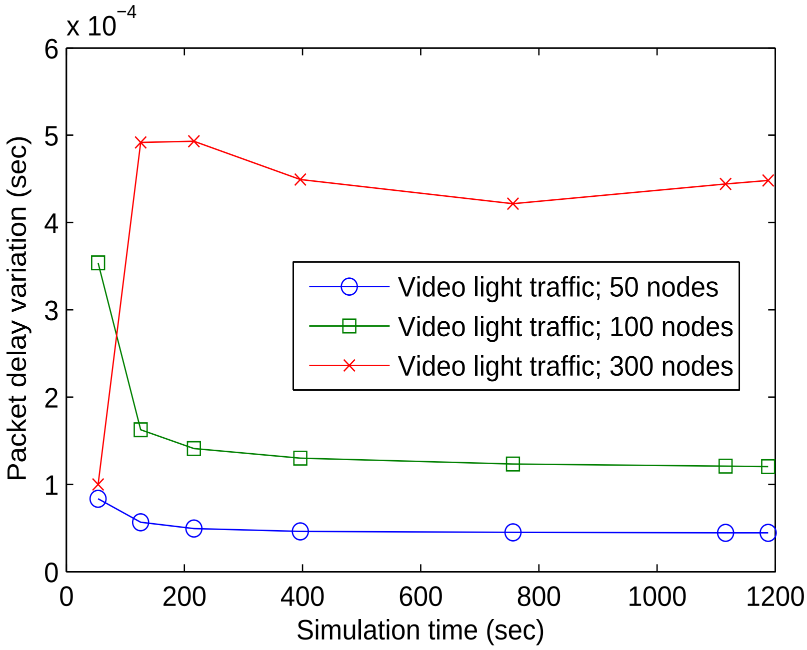
The impact of video traffic (N=50, 100, 300 nodes; FS= 128x 120, 128x240 pixels)

Two types of video conference applications were examined in this study, catering for the need for low resolution and high resolution. Low resolution quality is created by light traffic loads, while the counterpart is created by heavy traffic loads. Detailed parameter settings were configured in Chapter 4.

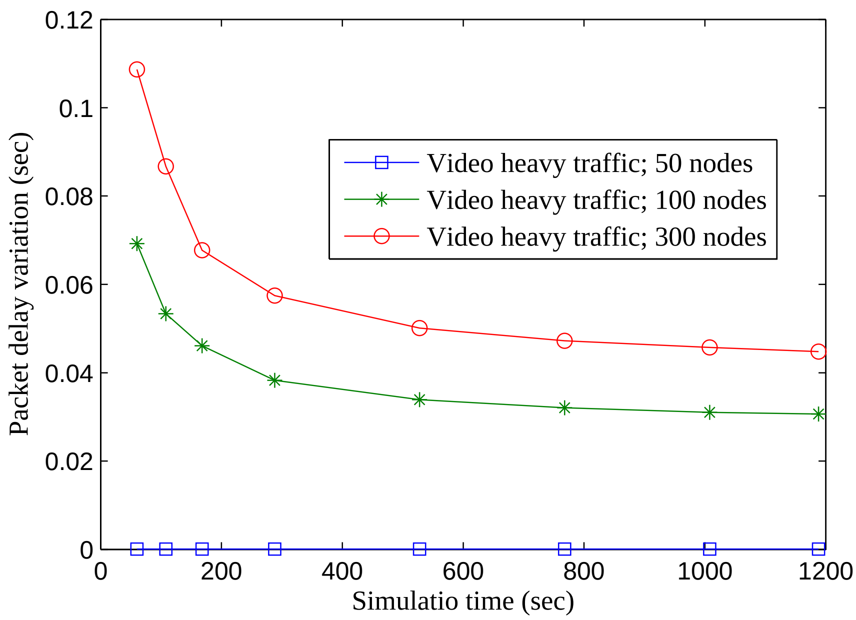
Figure 5.9a shows the packet delay variation of low resolution video conference corresponding to different network sizes. It would appear that a small network accounts for the lowest packet delay variation, which is approx 0.3 x 10^{-4}sec. As the network sizes shifted, more packet delay variations were generated, approx 1.2 x 10^{-4}sec in a medium network and 4.8 x 10^{-4} sec in a large network, respectively. Another interesting finding is the packet delay variation of a large network continued rising in most of time. All others, however dropped radically within the first two minutes and then remained steady.

The findings above demonstrate the performance of video light traffic. The effect of heavy loads to video conference is examined in the following section, so that one can observe the difference and perceive the notion of video transmission.

As mentioned earlier, the packet delay variation can be used to judge the continuity of a real time interactive application. It normally requires low packet delay variation (< 1 sec). As shown in figure 5.9b, all packet delay variations were less than one sec. In addition, all packet delay variations tended to remain steady although a sharp reduction occurred in the beginning. The large network was found overwhelm others. The average packet delay variations were 1 x 10^{-4} sec in a small network, 30 x 10^{-3} sec in a medium network and 43 x 10^{-3} sec in a large network. As opposed to the light traffic load, the heavy traffic load ended up 3.3 times packet delay variation in a small network, 250 times in a medium network and 90 times in a large network.



(a)

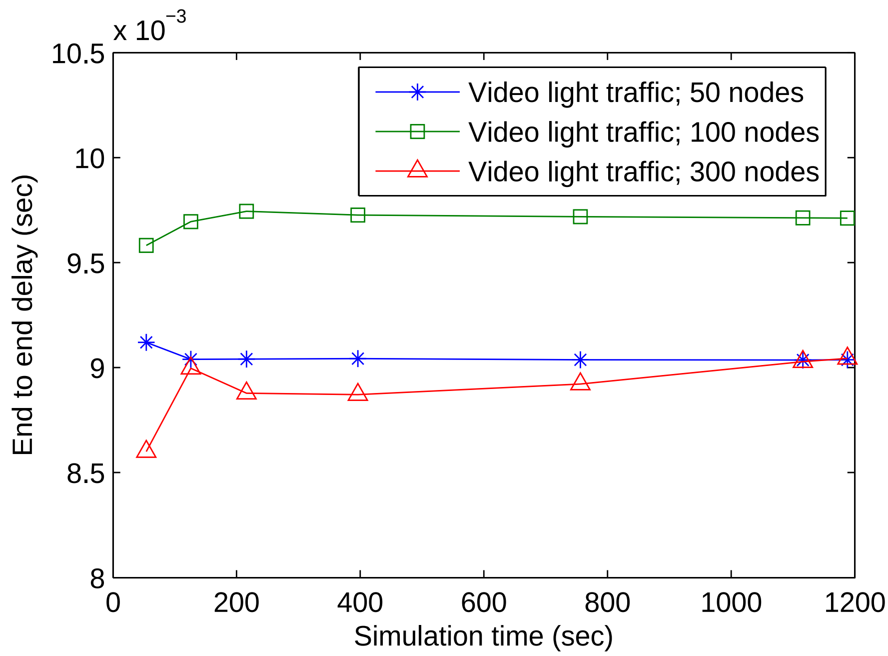


(b)

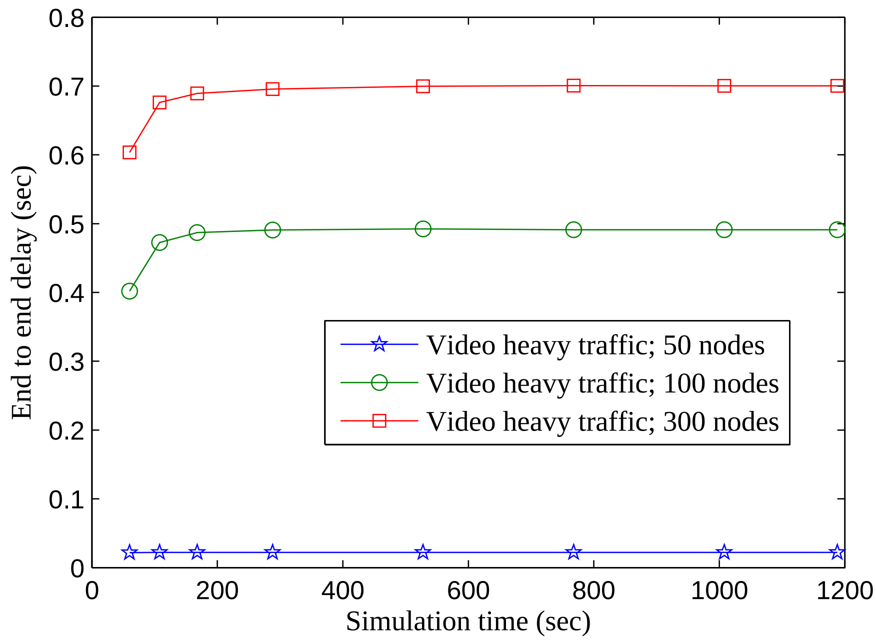
Figure 5.9 : Comparison of packet delay variation of video_con: (a) Light traffic; (b) Heavy traffic.

Figure 5.10a compares the end-to-end delay of three video conferencing scenarios when a light traffic load was used. Initially, the end-to-end delay in a medium network rose slightly from 9.6 to 9.8 x 10^{-3} sec. The second minute onwards, it tended to remain the same for the rest of time. Similarly, the end-to-end delay derived from a large network increased from 8.6 to 9 x 10^{-3} sec gradually. As the network size shifts to small, the end-to-end delay dropped by 3%.

Greater end-to-end delay was found in Figure 5.10b when a heavy traffic load was added. It would appear that the large network accounts for the highest end-to-end delay, which is approx 78 times as much as that of light traffic loads. The second highest end-to-end delay was observed in a medium network. It rose from 0.4 to 0.5 sec, indicating 51 times as much as that of light traffic loads. The lowest end-to-end delay in a small network is approx 0.02 sec throughout the simulation, which is increased by 120% as opposed to the light traffic loads.



(a)

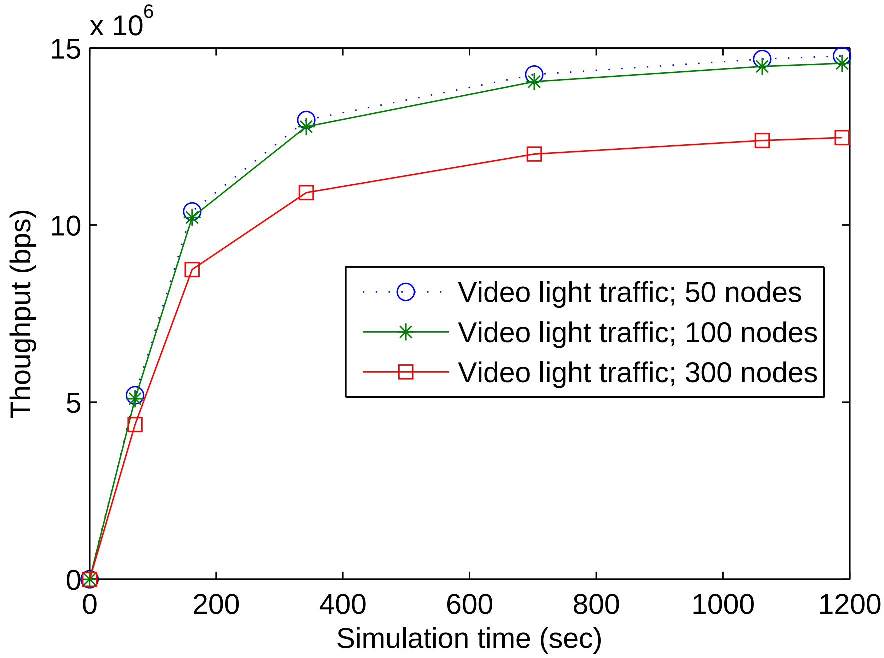


(b)

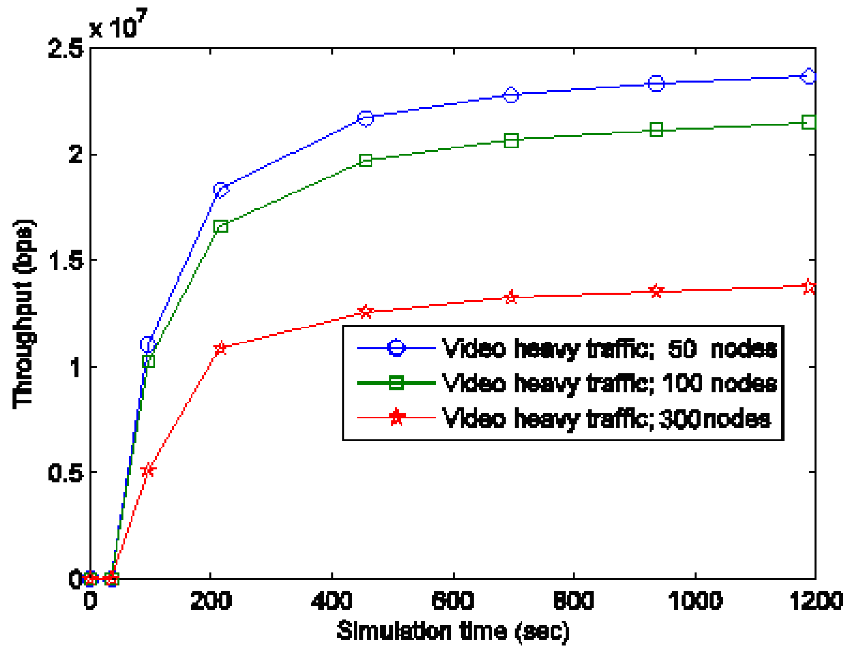
Figure 5. 10: Comparison of end-to-end delay of video_con: (a) Light traffic; (b) Heavy traffic.

Apart from packet delay variation and end-to-end delay, one can also determine the visual quality by viewing the throughput derived from various network scenarios. Figure 5.9a compares the throughputs when transmitting a low-resolution video file in a small, medium and large network, respectively. It is clear that the small network accounts for the highest throughput, approx 15 mbps. However, as the network size increases, lower throughputs are found in medium and large network, approx 14.8 mbps and 12.5 mbps, respectively. The reduction reaches up to 14%. Since the video streaming generated considerably larger payload than voice and data traffic, the throughput performs differently from others. It is estimated that the performance of video traffic will degrade when very large number of uses are involved.

Likewise, the highest throughput is also found in a small network when transmitting a high-resolution video file, which is approx 1.6 times as much as that of light traffic loads. The second highest throughput is found in a medium network. Although it increases dramatically in the beginning, the average throughput is still 9% less than the small network. As the network size shifts to a large network, the throughput ends up 14 mbps, which drops by 52% than the small network. However, as opposed to the light traffic loads, the throughput in each scale of network improves by 60%, 57%, 12%, independently.



(a)



(b)

Figure 5. 11 : Comparison of throughput of video_con **:** (a) Light traffic; (b) Heavy traffic.

5.1.2 Server performance

This section collected the average throughput of main servers. The pattern of traffic sent was observed as opposed to the counterparts in the client side. The effects of network size and traffic load were then presented. The simulation ended in 20 minutes. The detailed parameter settings can be found in Chapter4.

Figure 5.12 compares the throughputs of an email server. When a light traffic load was added, the email server generated 2 kbps in a small network, 2.6 kbps in a medium network and 6 kbps in a large network, respectively. When a heavy load was added, the email server generated approx 4 times, 9 times and 9.5 times in the corresponding networks.

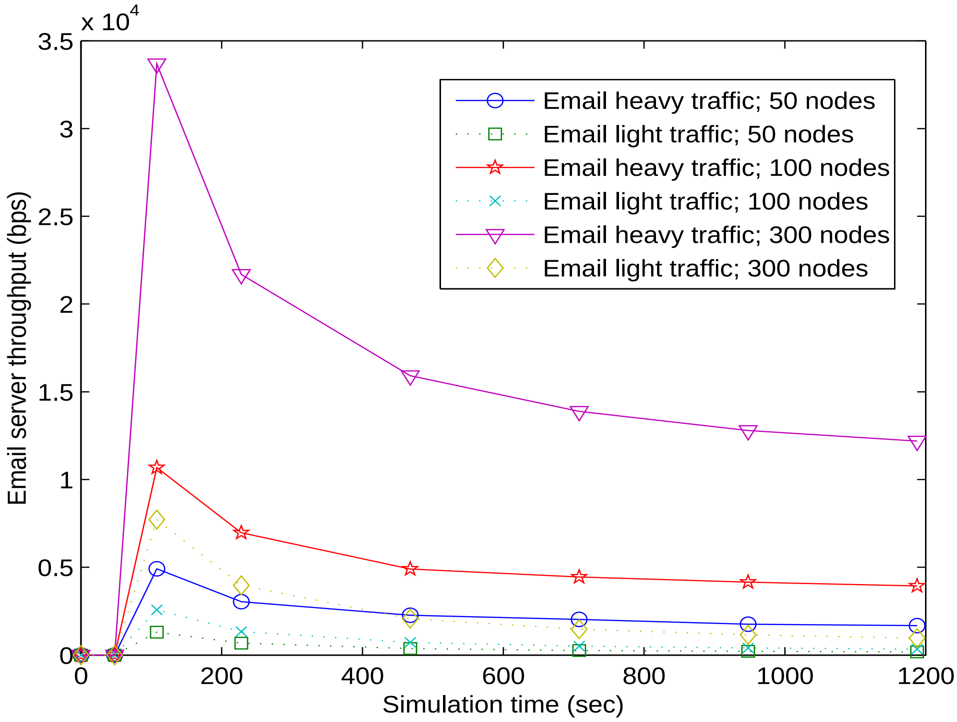


Figure 5. 12: Comparison of throughput derived from an email server.

Likewise, the FTP server provided incremental throughput as traffic load shifted from light to heavy. Clearly, the highest throughput was found in the large network, approx 2.5 mbps when a heavy traffic load was added. Very closed throughputs were also found in other scales of networks under the same traffic load settings

By viewing the traffic sent on the server side (Figure 5.13) and the packet drop incurred (Figure 5.4), one can measure the traffic received on the client side. Zero packet drops indicate all traffic is successfully received by the clients. Nonetheless, it is not always the case. An exception is transmitting an image file via FTP in a small network. Another interesting finding is higher chance of packet drop happens when the server throughput increases.

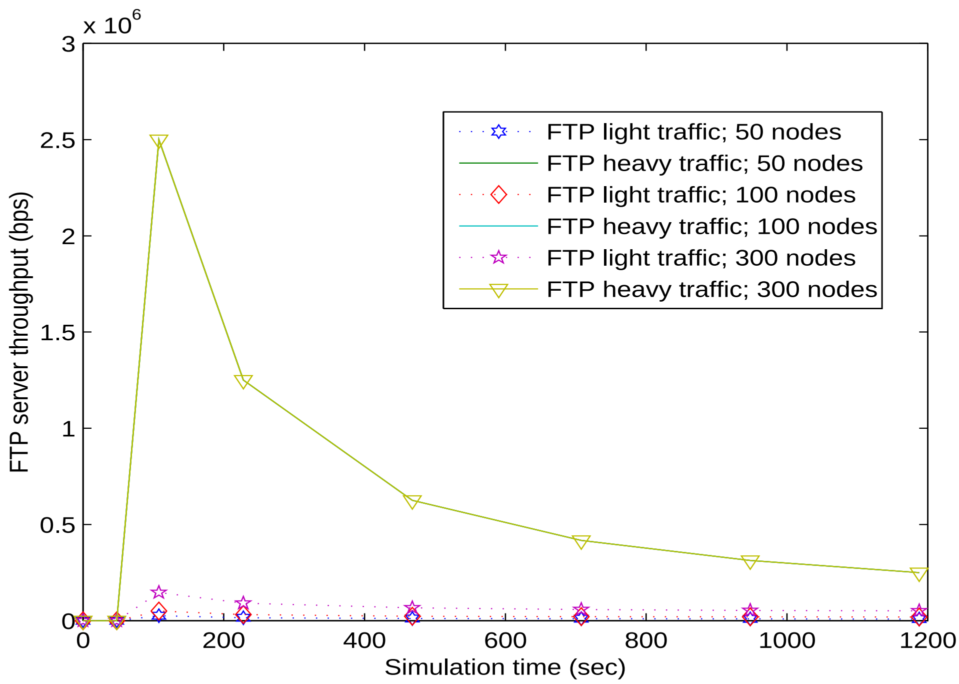


Figure 5. 13: Comparison of throughput derived from a FTP server.

Figure 5.14 compares the throughput of a VoIP server under various network scenarios. When a light traffic load was applied, VoIP server generated 200 kbps in a small network, 350 kbps in a medium network and 760 kbps in a large network. When a heavy load was applied, the VoIP server generated approx 2 times, 2.1 times and 3.2 times throughput in the corresponding networks.

Upon comparison of the traffic sent in Figure 5.14 and traffic received in Figure 5.8, no packet drop was observed, which indicate the packet switched network provides timely delivery of voice signals.

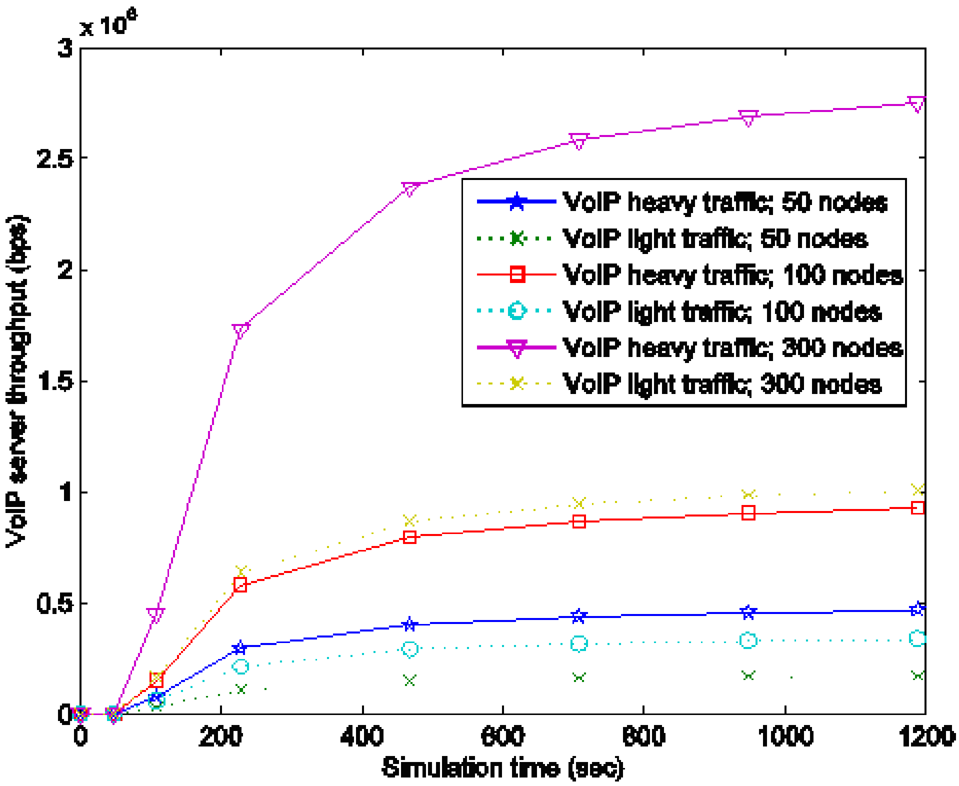


Figure 5. 14 : Comparison of throughput derived from a VoIP server.

Figure 5.15 demonstrates the throughputs derived from a video server. It is clear that the heavy traffic load results in higher throughput when compared to the counterparts. The margin between them is even greater as the network size increases. The highest throughput is found in the large network when a heavy traffic load was added. Under the same traffic load settings, the average throughput in a medium network is approx 8.9 mbps, indicating 10% reduction. Although there is an exponential rise in the beginning, the throughput in a small network is till less than others.

The light traffic load, on the other hand generates difference results. The highest throughput is found in a small network, approx 3.3 mbps. As the network size increases, slightly lower throughput is observed in a medium network. The reduction reached up to 9% when transmitting a video file in a large network.

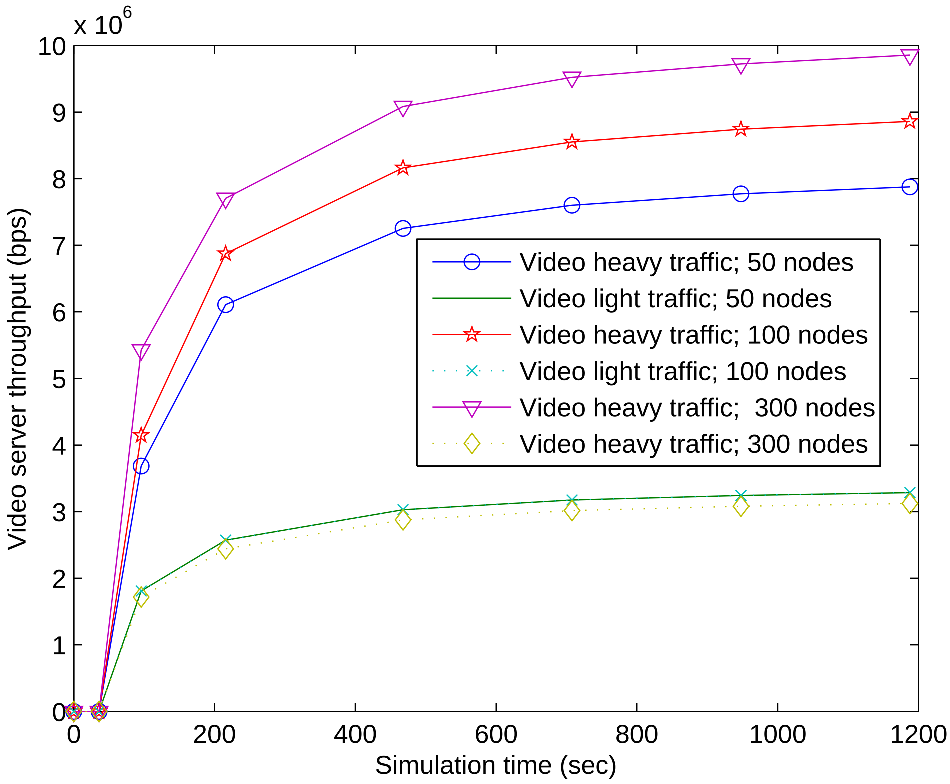


Figure 5. 15 : Comparison of throughput derived from a video server.

5.1.3 WLAN performance

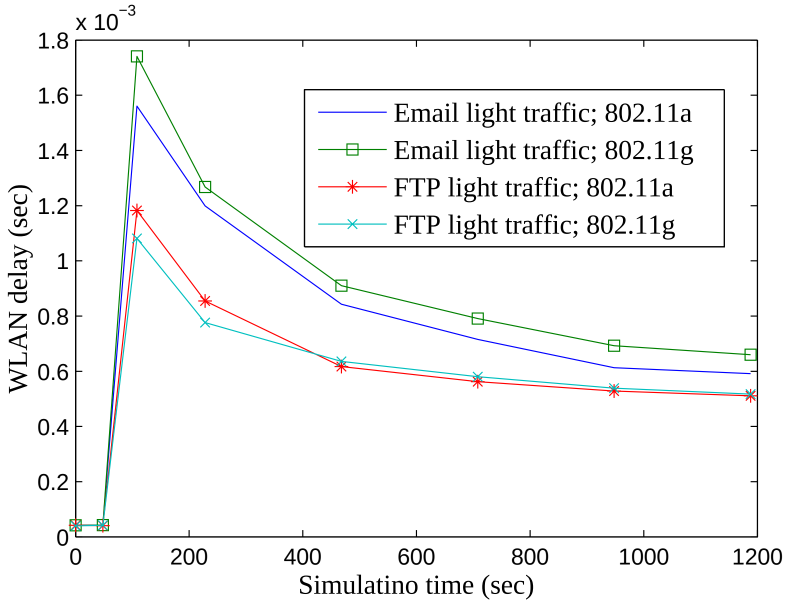
In WLAN, the impact of signal strength on network performance was investigated. The Received power threshold was used to detect the signal status for radio propagation, denoted as strong, medium, fair and weak. Theoretically, strong signal strength (s>-50 dBm) are always expected for packet transmission. However, the actual power consumption and clear channel assessment impose far more challenges in the MAC design. In addition, the signal strength changes constantly with the environmental condition, such as distance and the building concrete (walls, stairs, etc) through which the radio are sent. Thus, a more compromised scheme that allows medium signal strength (-88< s<-70 dBm) and less power consumption is preferred. This study first implemented the medium threshold (-88 dBm). Subsequently, a comparative analysis with other thresholds was presented. The collected results help quantify the performance in WLAN and eventually determine the optimal threshold of received power.

It is assumed that all wireless stations are placed in the random location. In addition, WLAN 802.11 a and g coexist side by side, in which case only the internal link interaction was taken into account.

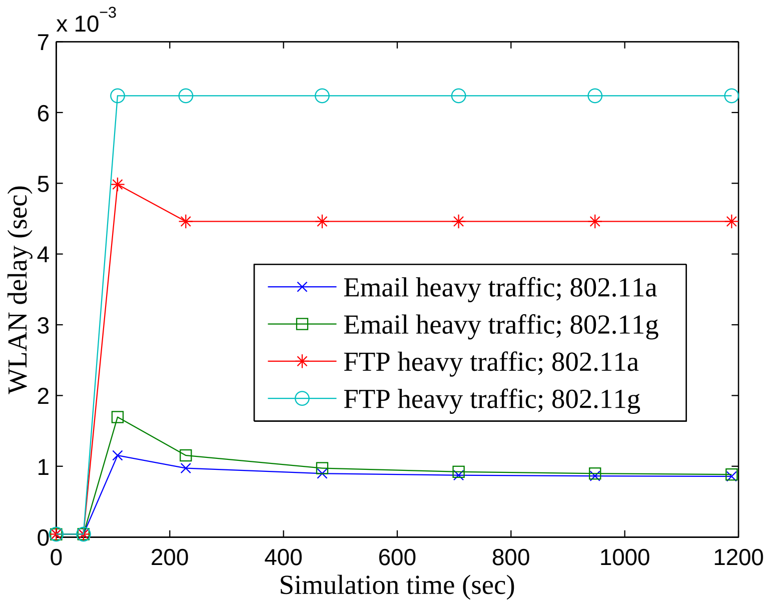
Mean packet delay, throughput and packet drop are used as performance metrics in WLAN. Mean packet delay refers to the amount of time taken a packet from the source to destination. Throughput in WLAN depends on the signal strength and the MAC standard used.

Figure 5.16 shows the mean packet delay of FTP and email in a WLAN. At first glance, all the mean packet delays increase dramatically and then reach a peak, followed by a gradual reduction. Transmitting a rich-text file (50000 bytes) via FTP generates approx a 0.52 ms delay in a WLAN 802.11a and 0.58 ms in a WLAN 80211g, respectively. When transmitting a rich-text email file (500 bytes), greater mean packet delay is found, approx 0.45 ms a WLAN 802.11a, 0.68 ms in a WLAN 80211g, respectively.

As opposed to the light traffic load, a greater mean packet delay is found when sending an image file via FTP. The average mean packet delay in a WLAN 802.11a is approx 4.4 ms, which is 9 times as much as light traffic load. As the network size increases, the mean packet delay rises to 6.2 ms in a WLAN 802.11g. Likewise, sending an image file via email also generates greater mean packet delay.



(a)

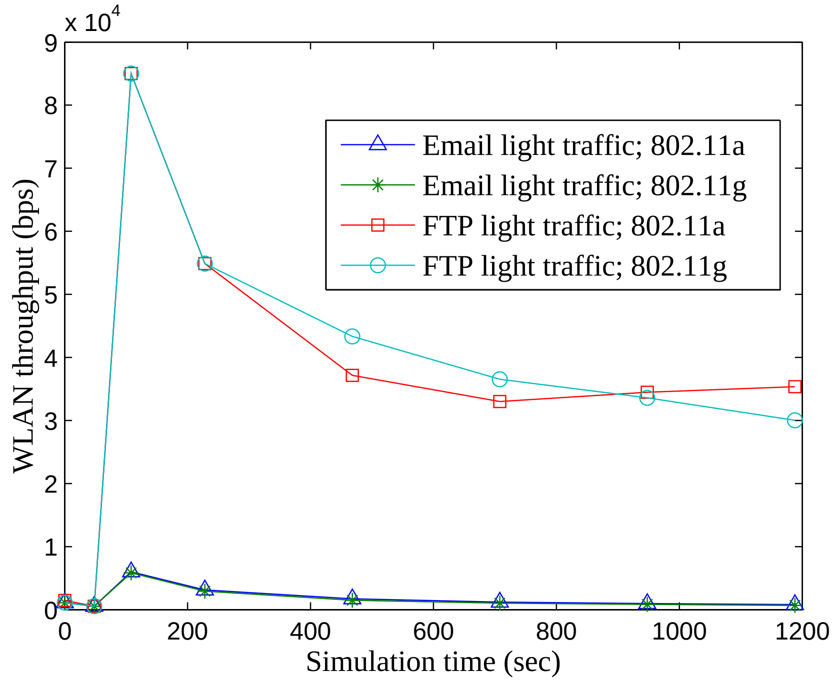


(b)

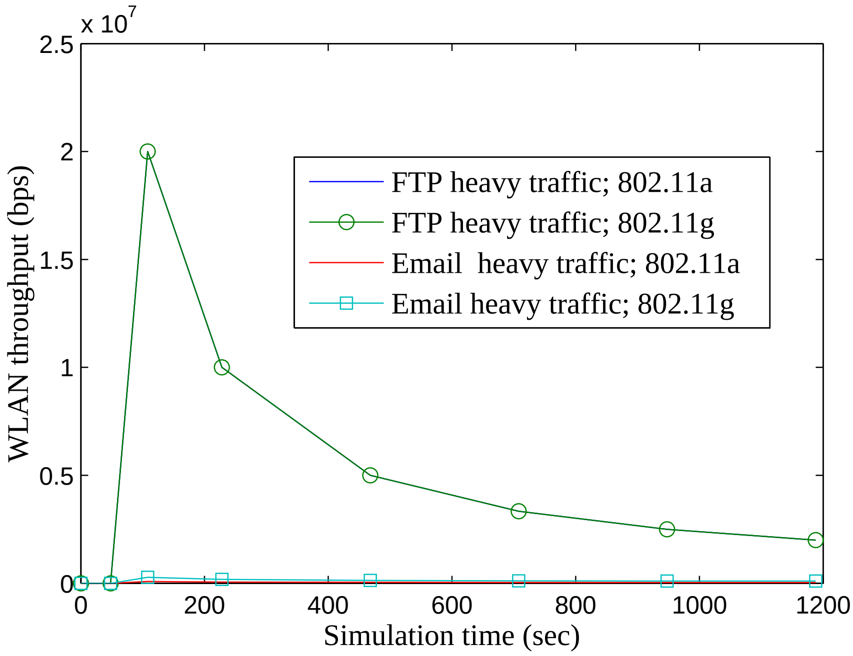
Figure 5. 16: Comparison of mean packet delay of FTP and email in the WLAN scenario: (a) Light traffic; (b) Heavy traffic.

The throughput in WLAN is measured by the number of packages successfully received by the destination node. It could be affected by traffic load and files size. Figure 5.17a shows the throughput derived from light FTP and email traffic in WLAN. Initially, all simulation tasks commenced with very low throughput and then increased dramatically until reaching a peak at approx 120 seconds. For the rest of time, the generated throughput tended to drop slightly. Transmitting a rich-text FTP file (50000 bytes) in a WLAN 802.11 g resulted in a 31 kbps throughput. Greater throughput was found in a WLAN 802.11 a, approx 36 kbps. Email traffic, on the other hand, was responsible for lower throughput compared to FTP, which was due to the file size configuration. When sending an email file (500 bytes), it generated approx 1.1 kbps in a WLAN 802.11 g, and 1.3 kbps in a WLAN 802.11 a, respectively.

Although increased throughputs were observed in Figure 5.17b, the gap among the various WLANs was reduced, which indicates 22 mbps is the highest throughput for FTP. Likewise, the maximum throughput for email is 800kbps, which is approx 533 times as much throughput compared to the light traffic.



(a)



(b)

Figure 5. 17: Comparison of throughput of FTP and email in the WLAN scenario: (a) Light traffic; (b) Heavy traffic.

Figure 5.18 demonstrates the packet drop associated with FTP and email in WLAN. One of the interesting findings is the packet drop here overlaps with that in Figure 5.4. In other words, the packet drop only takes place in WLAN and none of others.

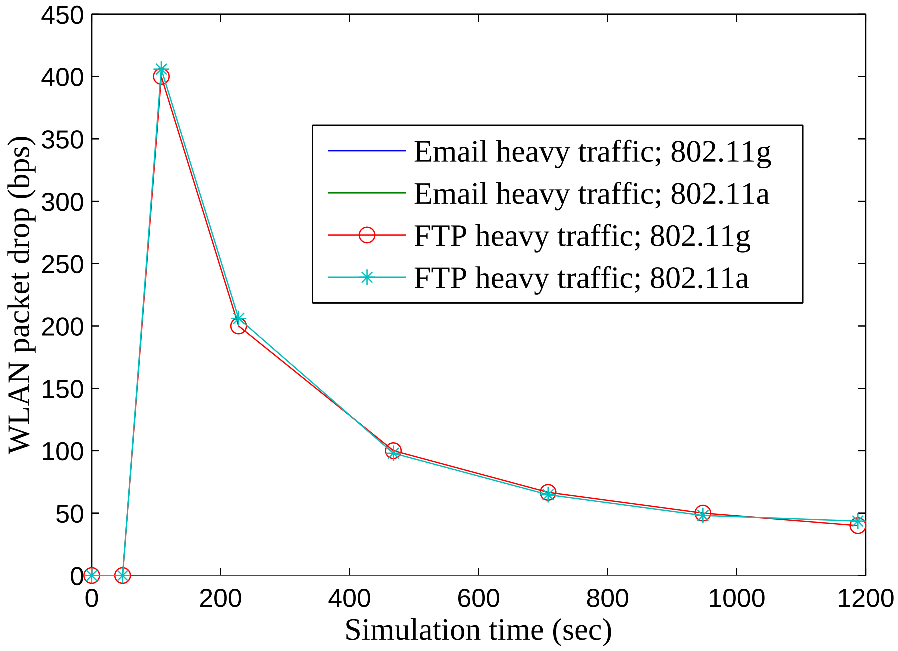
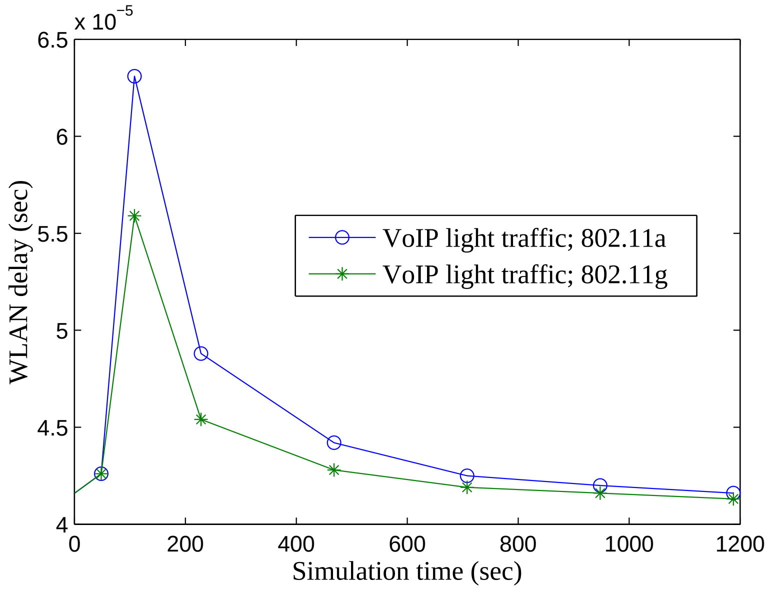


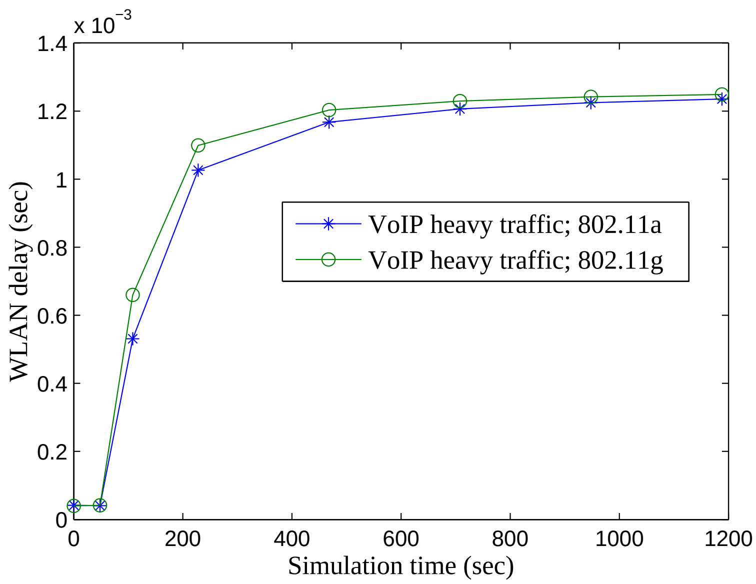
Figure 5. 18 : Comparison of packet drop of FTP and email in the WLAN scenario.

As a real time interactive application, VoIP is sensitive to end-to-end delay. Figure 5.19a compares the end-to-end delay of light VoIP traffic in WLAN. Out of three network scenarios, the WLAN 802.11a for the highest end-to-end delay, approx 0.064 ms. After reaching a peak at the second minute, the end-to-end delay tended to drop gradually and remain 0.042ms in the long run. Lower end-to-end delay was found in a WLAN 802.11g. Although there was an exponential rise in the beginning, the end-to-end delay varied from 0.056 to 0.041 ms.

When heavy traffic load was added, greater end-to-end delay was found in Figure 5.19b. In 802.11a, the average end-to-end delay was approx 1.2 ms, which is 17 times as much as light traffic load. Another interesting finding is the end-to-end delay in WLAN 802.11a and 802.11g are fairly closed, which is due to the concealment techniques in G.729 standard. Explicitly, each voice packet at the sending end encapsulates certain number of speech samples and adds the RTP, UDP, IP and Ethernet headers, which leads to variations or jitter in delay. A playback buffer at the receiving end however absorbs such variations or jitter and thereby provides smooth playout.



(a)

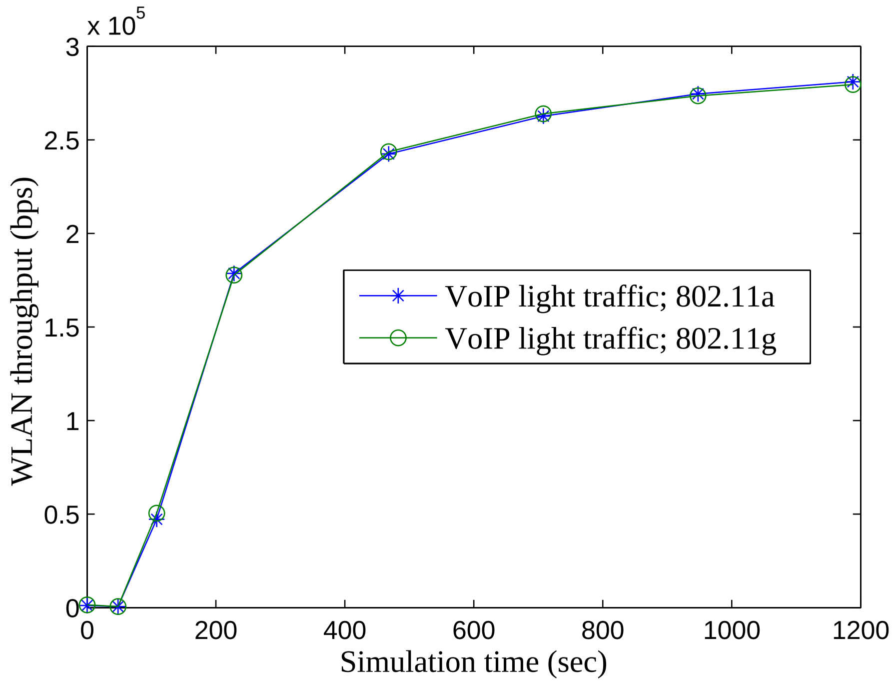


(b)

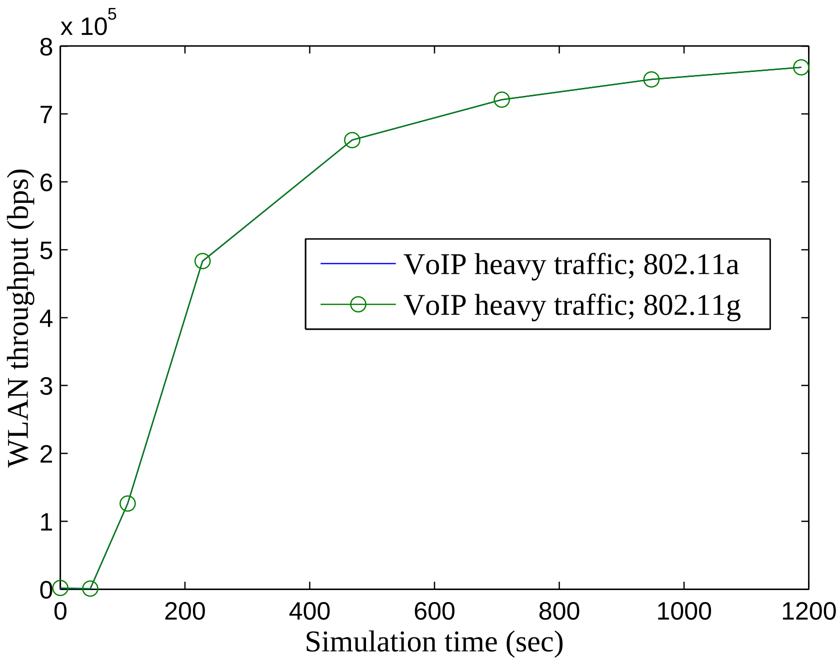
Figure 5. 19: Comparison of mean packet delay of VoIP in the WLAN scenario: (a) Light traffic; (b) Heavy traffic.

Figure 5.20 demonstrates the throughput of VoIP in a WLAN 802.11a and 802.11g, respectively. It is important to mention that all the wireless stations are placed arbitrarily. Each WLAN includes 10 nodes and 1 AP. Figure 5.20a corresponds to a light traffic load. It would appear that the throughput in a WLAN 802.11 a increases dramatically. As the simulation proceeds, it tends to remain the same, providing approx 1.4 mbps throughput. Likewise, in a WLAN 802.11g, there is an exponential rise of throughput initially, which is approx 5% greater than that of 802.11a. However, it is caught up by 802.11 a afterwards. The average throughput obtained from 802.11g is approx 1.3mbps. The highest throughput indicates the call capacity during a peak hour. Given an exact number of calls per second, the call capacity can be calculated.

Greater throughput is found in Figure 5.20b when heavy traffic load is added. In WLAN 802.11a, the average throughput is approx 2.7 mbps, which is 2 times as much as that of light traffic load. Closed throughput is found in WLAN 802.11g.



(a)



(b)

Figure 5. 20: Comparison of throughput of VoIP in the WLAN scenario: (a) Light traffic; (b) Heavy traffic.

Figure 5.21 shows that none packet drop occurs when transmitting a VoIP file in WLAN, which indicates good connectivity in WLAN. In addition, the quality of real time interaction can be ensured.

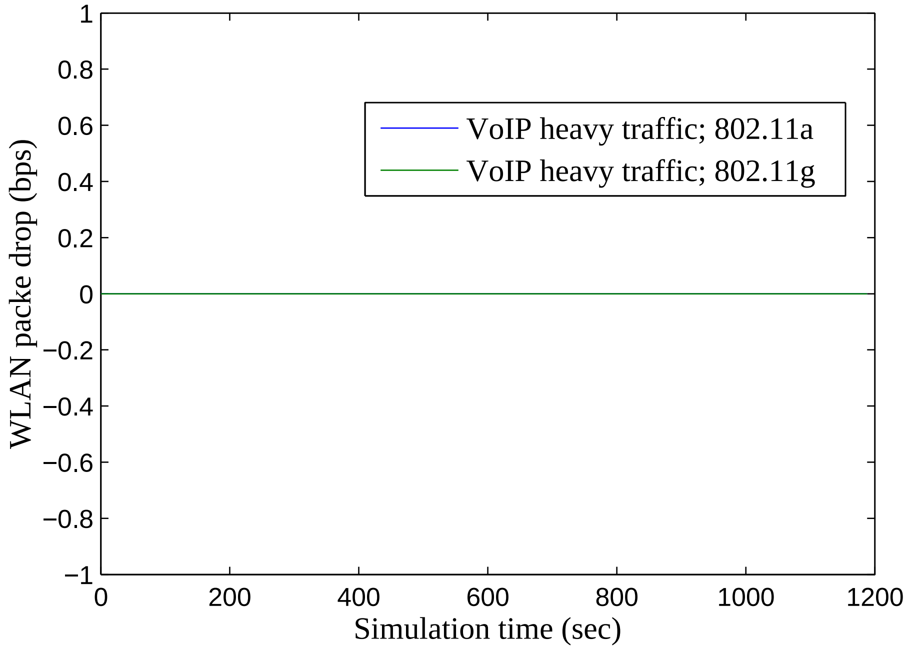
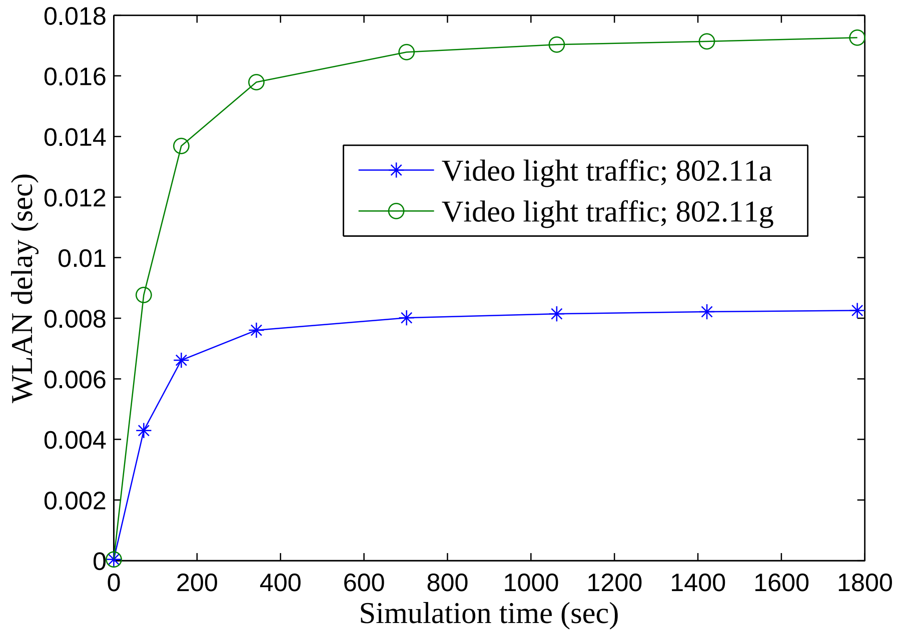
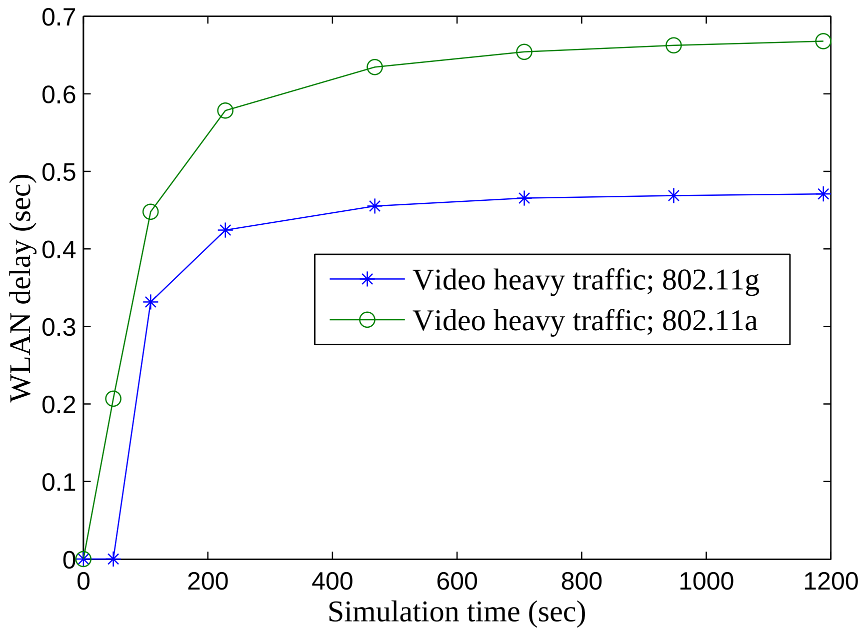


Figure 5. 21: Comparison of packet drop of VoIP in the WLAN scenario.

Video conference is also a kind of interactive applications which require high bandwidth and low values of mean packet delay, since massive delay could cause inconsistence of audio and visual traffic. Figure 5.22 shows the mean packet delay of video conference in WLAN. It is clear that the mean packet delay in WLAN 802.11a is greater than that of WLAN 802.11g. The difference between them is even greater when a heavy traffic load is added. The average mean packet delay for 802.11g is 0.017 sec under light traffic load and 0.68 sec under heavy traffic load, respectively. Given the same traffic load settings, the average mean packet delay in WLAN 802.11a, is 0.075 sec and 0.47 sec, respectively.



(a)

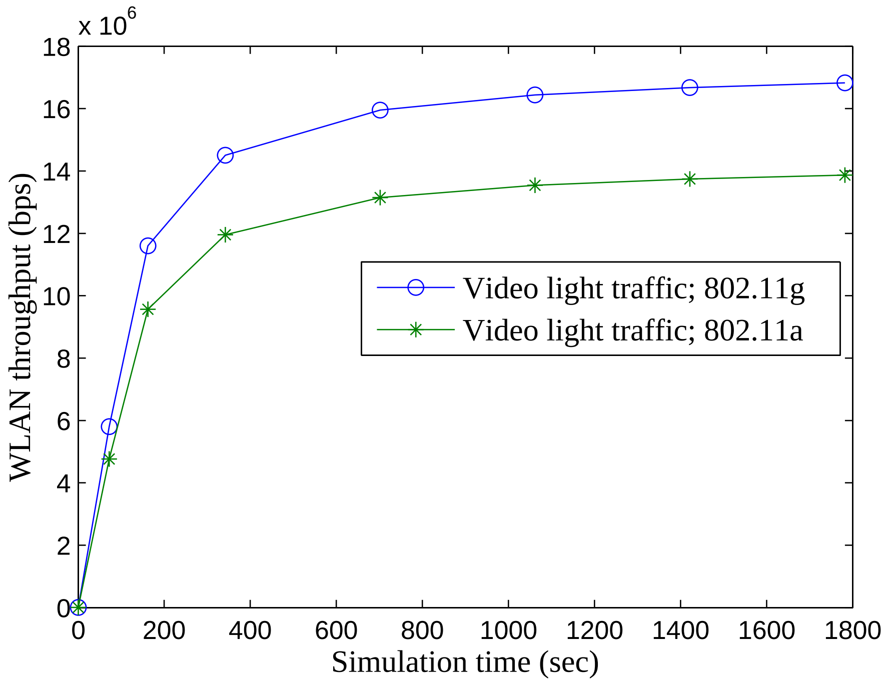


(b)

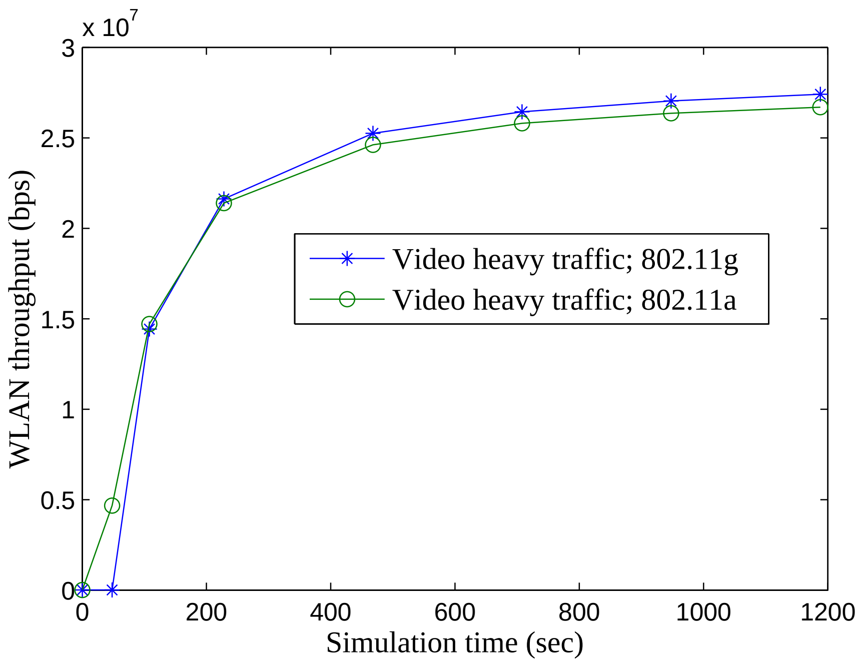
Figure 5. 22: Comparison of mean packet delay of video_con in WLAN: (a) Light traffic; (b) Heavy traffic.

Since video conference contains visual and audio traffic, greater throughputs were generated in WLAN 802.11a and 802.11g, respectively. By viewing the graph below, the average throughput reached 13.9 mbps in the WLAN 802.11a. As the traffic load increases, the throughput reached up to 27 mbps, indicating 94% improvement. 802.11g, on the other hand, provided generally greater throughput compared to 802.11a.

Another interesting finding is the maximum throughput in WLAN 802.11g is approx 27.6 mbps, which makes use of 50% of data rate (54Mbps). The great margin can be considered as overhead, which normally consists of request time, idle time, and PHY overhead. Out of the possible sources of overhead, request time and PHY overhead account for the majority of consumption, approx 30%, independently. Other overheads involve collisions, MAC overhead and TCP overhead. In practice, overhead can be reduced by environment control and mitigating possible interfering sources. A typical example is disabling unused services.



(a)

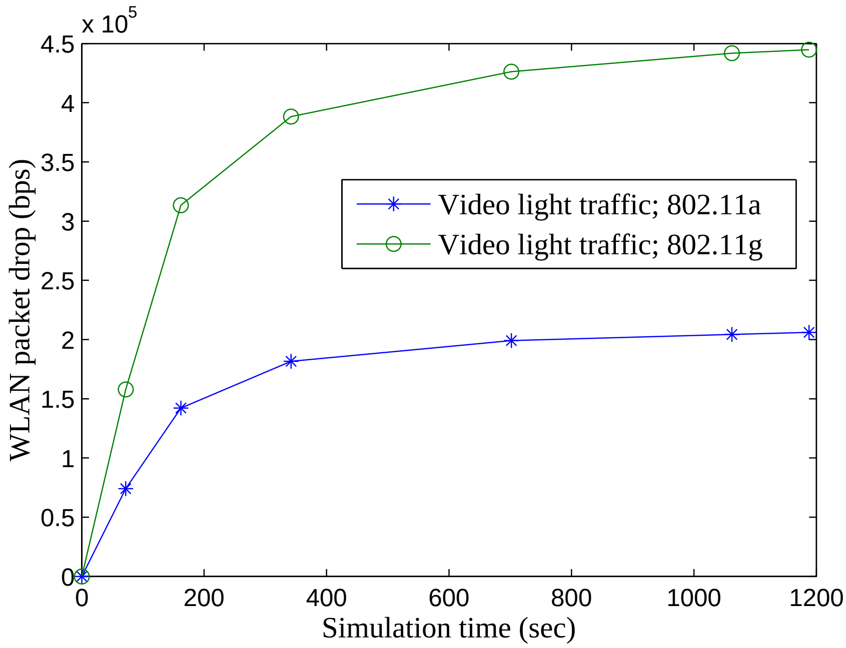


(b)

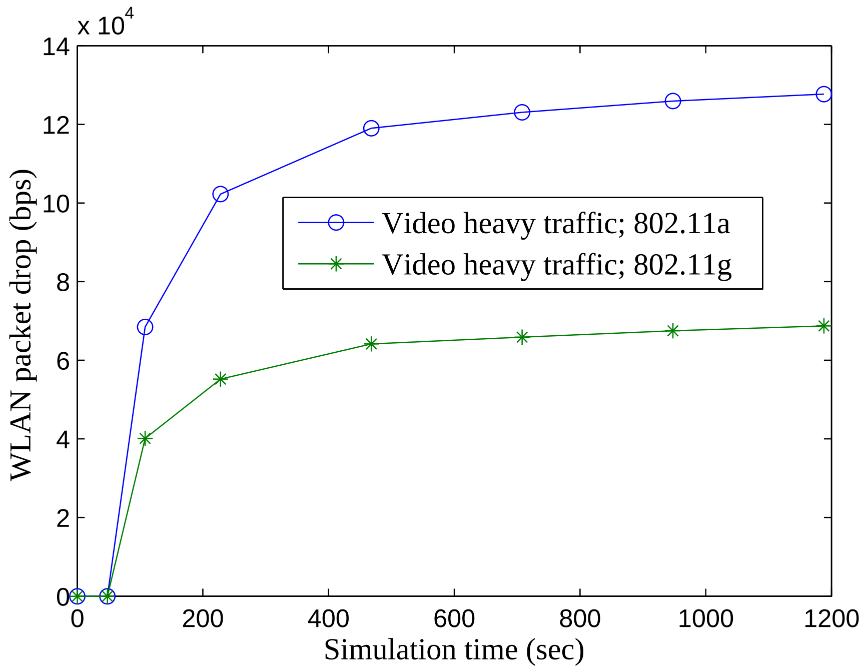
Figure 5. 23: Comparison of throughput of video_con in WLAN: (a) Light traffic; (b) Heavy traffic.

Packet drop occurs when exceeding the retry threshold. Figure 5.24 compares the packet drop of video conference in WLAN 802.11a and 802.11g, respectively. When transmitting a low-resolution file, there are approx 450kbps packet drop observed in WLAN 802.11g, indicating 2.6% drop rate out of the corresponding throughput. Given the same video file, 802.11a generates 200 kbps packet drop, which is approx 44% as much as 802.11g.

As the traffic load increases, lower packet drops were observed, approx 130 kbps in WLAN 802.11a and 70 kbps in WLAN 802.11g, respectively.



(a) Light traffic



(b) Light traffic

Figure 5. 24: Comparison of packet drop of video_con in WLAN:
(a) Light traffic; (b) Heavy traffic.

Reiterating the goal of this experiment is to figure out the best threshold of received power. Table 5.1 compares the average throughput among various applications running in WLAN. It turns out the medium thresholds (-88 dBm) generated remarkably more throughput than others. The gap between them was even greater when a heavy traffic load was added. In reality, -110 dBm was considered as unwanted threshold, as it allowed very weak signal for the transmission. Although it generated great throughput occasionally, -88 dBm overwhelmed others in most of the cases.

Table 5. 1: Comparison of throughput in WLAN (kbps)

Applications	Received power threshold (dBm)			
	-110	-88	-70	-50
Light FTP	1,350	1,400	80	20
Heavy FTP	4,100	4,200	150	30
Light email	280	300	0.6	0.1
Heavy email	360	370	2	1
Light VoIP	540	600	100	30
Heavy VoIP	760	780	110	20
Light Video_con	15,000	17,000	200	80
Heavy Video_con	22,000	25,000	600	280

Table 5. 2: Comparison of mean packet delay in WLAN (ms)

Applications	Signal strength threshold (dBm)			
	-110	-88	-70	-50
Light FTP	1.2	1.1	0.7	0.02
Heavy FTP	4.2	4.8	4.3	0.05
Light email	0.09	0.06	0.02	0.03
Heavy email	1	1.1	0.4	0.02
Light VoIP	0.03	0.02	0.01	0.01
Heavy VoIP	1.4	1.5	0.7	0.05
Light Video_con	0.07	0.05	0.01	0.01
Heavy Video_con	0.77	0.68	0.03	0.02

Table 5. 3: Comparison of packet drop in WLAN (kbps)

Applications	Signal strength threshold (dBm)			
	-110	-88	-70	-50
Light FTP	0	0	200	70
Heavy FTP	0	0	0.05	0.03
Light email	0	0	120	110
Heavy email	0	0	310	310
Light VoIP	0	0	130	180
Heavy VoIP	0	0	630	710
Light Video_con	16	16.2	2	1
Heavy Video_con	48053	47570	3.1	1.2

5.2 Discussion

5.2.1 The effect of traffic load

Observation and comparative analysis are the main techniques employed here to capture the traffic patterns. The ultimate objective is to achieve a fundamental overview of hospital network implementation. Three scenarios were piloted as case studies verification.

Email and FTP were deployed in the radiology scenario, in which heavy and light traffic represented the desire on rich text files and graphical image, respectively. It is interesting that upload and download stream are symmetric in radiology scenario, unlike the implementation of home network where download stream is greater than upload stream. Simulation results showed that heavy traffic can lead to performance degrade. For instance, FTP packets were dropped dramatically as the small network cannot accommodate such a heavy traffic load. To address this issue, network practitioners have to determine the performance threshold (e.g. packet size, network size and signal strength), by which the readiness and predictability can be improved.

Voice traffic relies on a number of coding standards and therefore performed distinctly from Email and FTP traffic. In the scenario of A & E, the average delay for VoIP is approx 62 ms, which is within the tolerated range as mentioned in Chapter 2. Regardless of the light or heavy traffic load, jitter was found very limited and there was even no packet drop. It is concluded that the voice traffic will cause no problems for the backbone network.

As a real time interactive application, video conference requires code division multiplexing that provisions constant bit rate. The major concern of code division multiplexing is implementation complexity and protocol overhead due to maintaining priority of packets. In the ICU scenario, only the interesting graphs that determine the QoS are selected. They are focusing on the combination of resolution, delay, frames rate (fps) and general stability of the system and the video throughput. The light traffic can offer in its best case but severely degrades the image quality from 352x240x30 fps to 128x120x10 fps. The heavy traffic on the other hand generated higher image output of 128x240x15 fps. In general, the traffic load has a significant effect to the network performance

5.2.2 The effect of network size

The generic hospital model was used to examine the performance of small, medium and large networks. By increasing the number of nodes, we can capture the fundamentals for user capacity.

It is found that different network size led to variant throughput and mean packet delay. As more users get involved, more response time was found when sending an email or downloading a file from the FTP server. Although such applications require high bandwidth, they generated relatively lower mean packet delay as compared to the audio and visual applications. More importantly, a robust backup device needs to be in place, ensuring all data are retrievable. As real time interactive applications, audio and video conference were found fairly sensitive to mean packet delay and packet drop. To guarantee efficient medical delivery, QoS enabled device is recommended in the large network.

5.2.3 The effect of signal strength in WLAN

The signal strength is determined by the received power of AP. Upon comparative analysis in experiment 4, the best threshold was found to be -88dBm. Theoretically, strong signal (s>-50 dBm) is expected for effective transmission. However, it relies on magnitude power consumption and clear channel environment. In reality, signal strength is associated with AP's location, active distance and the building concrete through which the radio waves are sent (walls, stairs, etc). Thus, a more compromised scheme that allows medium signal (-88< s<-70 dBm) and less power consumption is preferred. The average overhead found in this study reached 48%. As rendered by [36], the overhead can be reduced by environment control and mitigating possible interfering sources. Typical example is disabling unused services.

Unlike email and FTP, VoIP in a WLAN generates substantial RTP/UDP/IP overhead, which leads to unnecessary consumption of bandwidth. According to Rittenhouse and Zheng [54], voice payload refers to "voice signal and header information", which is typically between 20 and 40 bytes while data rate reaches 16kbps. In fact, this data rate is much smaller than the standard rate for transmitting email and FTP packets (0.5-2Mbps). Thus, efficient and robust header compression techniques dealing with MAC frame aggregation are required for the VoIP deployment.

5.3 Model validation and verification

The simulation results were compared with those of empirical models, focusing on the improvement, accuracy and fairness. The comparison also

5.3.1 Comparison with previous results

Assaad Fayek [24] propose a metropolitan hospital model which involves activities of email, FTP in the wired network and video conference in the WLAN. Banitsas, et al. [6] also construct an emergency department for video streaming. Although these network scenarios are regarding medical applications, the network design varies greatly in terms of VLAN, system capacity and AP configuration. This dissertation takes advantage of high rate WLAN technologies (IEEE 802.11a) instead of 802.11b, which introduces 2.8 times throughput to the heavy video conference (see table 5.1).

Table 5. 4 : Comparison of simulation results.

Applications	The prior results (kbps)	The current results (kbps)
Light FTP	710 [24]	400
Heavy FTP	1420 [24]	2000
Light Email	736 [24]	16
Heavy Email	1420.[24]	101
Light VoIP	-	800
Heavy VoIP	-	2240
Light video_con	-	18800
Heavy video_con	8294.4 [6]	23500

While the throughput varies a lot (owing to the configuration of file size and distributed interval), the response time regarding email and FTP under the light traffic load condition was found quite closed to the previous work. During the simulation time (20 min), the response time was generally less than one second. However, when a heavy traffic load was added to a small network, the response time (30 sec) terribly exceeded the acceptable range (< 1 sec), which indicates the small network cannot accommodate such a heavy traffic load. To address this issue, it is recommended to scale up current network devices which have 25% growth capacity.

5.3.2 Comparison with the real world data

Banitsas, et al. [23] undertook a usability test. It reveals that the video delay on the client side can be reduced by using faster processors and WLANs that supports higher bandwidth (IEEE 802.11a)

The performance of VoIP was verified with a real experiment conducted by Gunal and Pidd [38]. Similarly, the jitter and packet drop were found very limited. Thus, the implementation of VoIP imposes rare burden on the existing backbone network.

5.3.3 Simulation accuracy

Simulation accuracy is achieved by running five replications with different initial seeds in OPNET. The major guideline is discussed in [58]. The pseudo generator of OPNET is based on Berkeley Software Distribution (BSD)'s algorithm which allows safe random number, i.e. without overlapping of random number streams. Five simulation replications were sufficient. Each simulation replication produced very similar graphical results.

5.3.4 Simulation fairness

Traditional network fairness as stated in [33] focuses on treating uneven resource (such as bandwidth) allocation regarding TCP congestion control mechanisms. In the realm of medicine, a fair network ensures that the emergency nodes have higher priority to access the network resource (e.g. channel), while other nodes wait until the resource is available. Since the priority scheme can produce dominators in the system and cause the system to be unpredictable and unbalanced, we would like to propose a novel dual channel priority scheme in the future work as an extension to the current one.

5.4 Proposed improvement

Due to the unique hospital characteristics, providing QoS to the medical applications is extremely crucial. For the wired backbone network, QoS can be achieved by configuring the network devices (e.g. routers) and granting dedicated connection to the emergency department. However, the implementation of QoS in wireless environments is more complicated. The typical approaches as stated in [25] involve resource reservation, dedicated emergency channel, and exploring QoS protocol (e.g.IEEE 802.11e).

- In the resource reservation approach [59], channel access is given to the device that carries emergency message. Once the nearest AP with idle status is detected, it embarks on association with the AP. Subsequently, it contends for the channel access for transmitting the emergency data. The limitation of this approach is the steep latency introduced. Supposed the device cannot find the AP within tolerated delay period, the emergency message will lose the chance of getting channel access. Similarly, reserving a channel slot is achieved by sending a periodic signal. If a slot carrying emergency message is detected within a signal period, the channel access will be granted directly. Otherwise, the device needs to wait until the next signal comes. This approach also has latency issue as the channel reservation approach

- The dedicated emergency channel method [60] reserves an entire channel for conveying the emergency data. Nonetheless, it will result in significant wastage of resource, owing to the erratic nature of emergency data.

- The main concept of the QoS protocol (IEEE 802.11e) [61] is granting predefined priority for different nodes. Based on a polling scheme, the AP in the contention free phase analyses the traffic sent out by each node regarding their queue length. When it comes to the contention phase, all the nodes compete for the channel access via advanced coordination algorithm. In general, the approach seems feasible for a complex emergency model: if the AP is activated properly by the emergency demands, it can grant channel access to the associated nodes by sending out a beacon signal.

To provision QoS features for the emergency applications in a WLAN scenario, a dual channel priority scheme that exploits IEEE 802.11e is required. The design of dual channel enables bandwidth distributed among the main channel that is accessible to all data (urgent and regular) traffic, and the slim auxiliary channel that is committed to the transmission of concise emergency alert signals. As soon as the emergency event occurs, the medical application device senses a concise emergency alert signal via the auxiliary channel. With the alert received, the AP starts forwarding a beacon containing priority information to all the applications in the network. Since the auxiliary channel delivers small alert messages, very limited bandwidth is required, which in turn reduce the latency. The main challenge is to create an effective coordination algorithm for the contention phase. It is important to ensure that only the device with emergency demands and the AP itself obtain the dual channel access.

As an extension to the hospital model, voice packets needs to be delivered more effectively. The simulation results in this dissertation show that conveying VoIP packets consumes very low bandwidth (approx 780kbps out of 54mbps) in a WLAN compared to other applications. In order to improve the bandwidth utilization, an effective scheme that allows multiple frames integrated into one packet will be studied. This scheme takes advantages of high speed downlink packet access. The objective is to reduce the occurrence of bit-stuffing and improve resource efficiency. However, the design of such scheme will introduce extra buffer delay. Performance evaluation will look at the mean packet delay under different frame aggregation conditions.

The principle of QoS-compliant protocol and packet compression can be extended to video application. The performance evaluation will focus on throughput, mean packet delay, and packet drop under different conditions (e.g. traffic load and compression scheme).

5.5 Summary

This chapter interpreted the simulation results based on the generic hospital network. Experiment 1 investigated the performance of various types of traffic on the clients. The effects of traffic load and network size were discussed. Results showed that most applications performed well and kept aligned to the QoS requirement. One exception is small network that cannot accommodate heavy FTP traffic. To counter this issue, performance thresholds and future growth capacity need to be investigated thoroughly. In addition, voice and video streaming require QoS enabled device to ensure effective real time delivery. Experiment 2 measured the server throughput, by which one can observe the data loss and system stability. Experiment 4 evaluates the effect of signal strength in WLAN. -88 dBm was found to be the best signal strength threshold. The next chapter conclude the research remarks and guidelines for the future research.

Chapter 6

Summary and Conclusion

For the past ten years, hospital networks had been evolving towards more interoperable sophisticated solutions. The major driving force is to achieve efficient healthcare delivery and accuracy. Wireless technologies enable doctors and nurses access the medical records everywhere, using a handheld device. In addition, it is easily scalable by adding certain number of APs, with no concern of cabling. The escalated bandwidth requirement and medical regulation also motivate the integration of backbone network and WLAN. Although there are certain integrated network scenarios published in literatures, network modelling of medical environment remains a challenging topic in practice. A good understanding of integrated network performance is required for efficient deployment of such technologies in hospital environments.

This dissertation presents the characteristics of medical applications and scenarios. Accordingly, a holistic QoS requirement is explained with definition of the factors influencing network performance. Since biomedical and emergency signals are critical to lives, mean packet delay is sensitive. For multimedia applications, although minor packet delay and packet drop are acceptable, smooth connectivity is still expected. In terms of office oriented applications, bandwidth is the first and foremost. Overall, the QoS requirement in hospital environments is unique.

QoS requirement is the main guideline of building a hospital network model. Based on the desire of bandwidth, security and mobility, a simplified model was first established to examine the connectivity, denoted as feasibility study. Once the feasibility study is done, we can determine the network infrastructure, traffic distribution and performance thresholds for a more complex one. This dissertation overcomes the multi-storey design with VLAN, which improves the efficacy of broadcast and enhances security. Instead of IEEE 802.11b, this dissertation adopts high rate 802.11a and g as the wireless standard.

Three piloted case studies were deployed in this dissertation. Experiment 1,2,3 investigate the client performance in radiology, A & E and ICU scenarios individually. Each scenario was equipped with various applications. In the radiology scenario, email and FTP traffic perform well in medium and large network. Since small network cannot accommodate heavy traffic load, the performance of FTP degrades. In the A & E scenario, VoIP traffic generates very limited jitter and data loss, so it will not introduce severe burden on the existing backbone network. In the ICU scenario, the performance of video conference degrades as network size increases, thus, QoS enabled device is recommended to reduce the delay and data loss. Experiment 4-7 evaluations the performance of server sector, which proofs a good communication with all clients. Experiment 8 examines the effect of signal strength in WLAN. It is convinced that -88dBm is the best signal strength threshold. Although 802.11a generates slightly lower throughput than 802.11g, this issues can be addressed by placing more APs in the service area. It is convinced that 802.11a suits the hospital environments, because it mitigates interference on the popular 2.4GHz band where most wireless devices operate. It is important for medical devices which require future upgrade and Bluetooth deployment.

Upon completion of the simulation, it is observed that the throughput varies a lot, owing to the configuration of file size and distributed interval. The response time regarding email and FTP under the light traffic load condition was found quite closed to the previous work. During the simulation time (20 min), the response time was generally less than one second. However, when a heavy traffic load was added to a small network, the response time (30 sec) was much higher than the acceptable range (< 1 sec), indicating the small network cannot accommodate such a heavy traffic load. To address this issue, it is recommended to upgrade current network devices with appropriate growth capacity (e.g. 25%).

The performance of video conference and VoIP was verified with a real experiment. It reveals that the video delay on the client side can be reduced by using faster processors and

WLANs that supports higher bandwidth (IEEE 802.11a). In view of the VoIP traffic, the jitter and packet drop were found very limited. This phenomenon was supported in previous work, which indicates the correctness of the simulation results.

In this dissertation, a complex distribution system was considered as hospital network architecture. The data, audio and video traffic focused on peer-to-peer transmission. However, the simulation strategies and procedures presented in this dissertation can be extended and provided as a guide line on any generic hospital network. The simulation work presented here can also be extended to other popular and important multimedia networks.

To further examine the proposed improvement, a QoS-compliant scheme will be stated in the future work.

6.1 Future research

Due to the unique hospital characteristics, providing QoS to the medical applications is crucial. According to Golmie, Cypher, & Rebala [26], the implementation of QoS in wireless environments is more complicated compared to those in the wired one. The difficulties are due to the erratic nature of emergency data and the scarce of QoS mechanism compliant to the popular WLAN technology.

The typical approach for QoS provisioning involves resource preservation, dedicated emergency channel and exploring QoS protocols (e.g. IEEE 802.11e). Unlike voice streaming and multimedia traffic, emergency events in the medical application are unpredictable. Hence, preserving resource specifically for this kind of data can result in significant wastage. Although the emergency events occur in an erratic manner, the biomedical data needs to be sent across network as soon as possible. Thus, smooth network connectivity is still required for medical applications. As a QoS protocol, 802.11e enables personalized settings for typical applications (e.g. voice and video streaming) in wireless environments. Chigan and Oberoi [25] argue that it does not have the intelligence to detect the emergency signal. In the future research, a more efficient MAC protocol will be proposed to support the QoS of medical applications. The effort will be focusing on two areas.

1. **Create a dual channel priority scheme.** The design of dual channel enables bandwidth distributed among the main channel that is accessible to all data (urgent and regular) traffic, and the slim auxiliary channel that is committed to the transmission of concise emergency alert signals. As soon as the emergency event occurs, the medical application device senses a concise emergency alert signal via the auxiliary channel. With the alert received, the AP starts forwarding a beacon containing priority information to all the applications in the network. Since the auxiliary channel delivers small alert messages, very limited bandwidth is required, which in turn reduce the latency. The main challenge is to create an effective coordination algorithm for the contention phase. It is important to ensure that only the device with emergency demands and the AP itself obtain the dual channel access.
2. **Evaluate the network performance under various scenarios.** The performance evaluation will look at the impact of traffic loads, traffic types, and QoS control. The performance metrics involve mean packet delay, packet drop and throughput. Scenario 1 is observing the network behaviours of regular data traffic under a QoS-compliant condition. Scenario 2 is investigating the network behaviours of emergency data under QoS-compliant condition. Scenario 3 and scenario 4 are carried out to examine the network performance of voice and video traffic, individually.

Appendix A

Model configuration

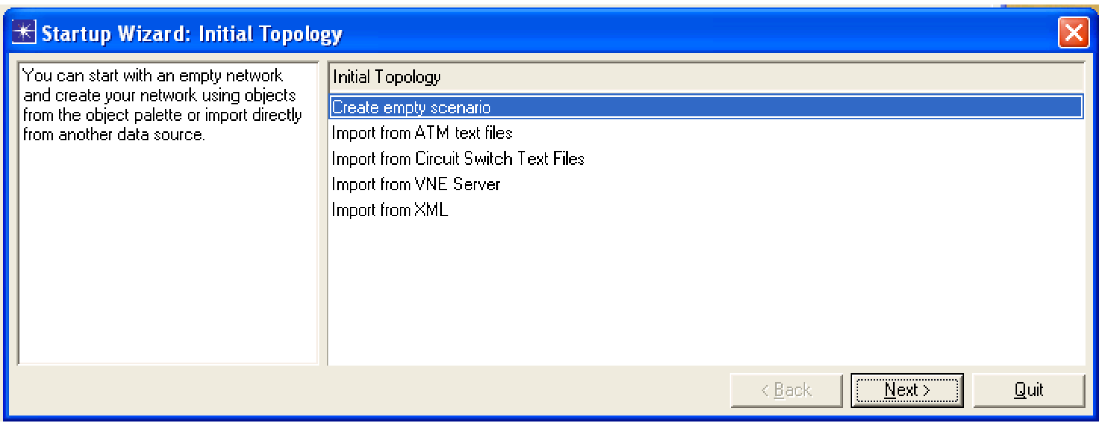


Figure A. 1: Create empty scenario.

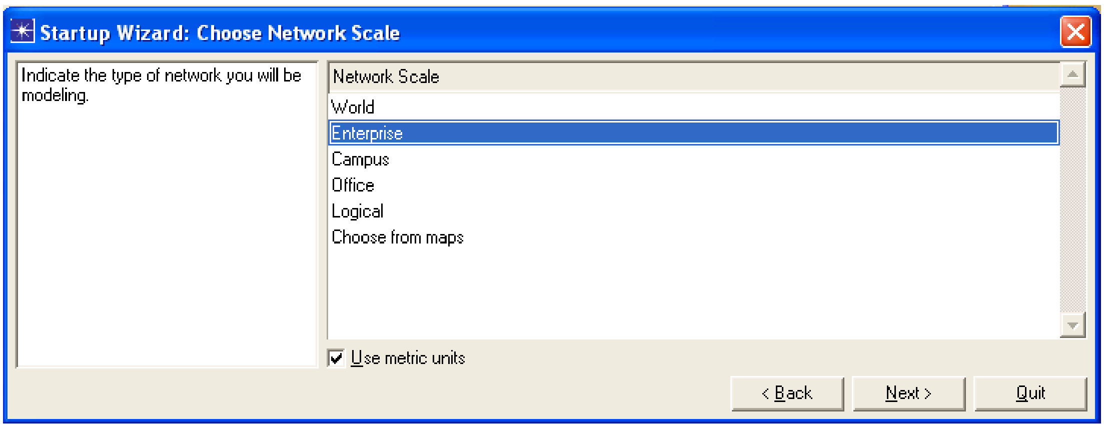


Figure A. 2: Create a hospital scenario with appropriate scale.

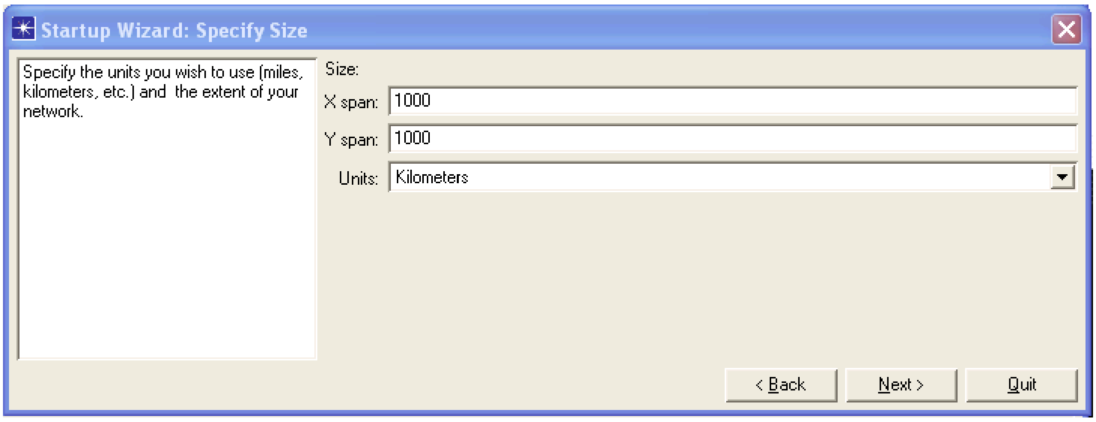


Figure A. 3: Specify the size and bounded area of a hospital model.

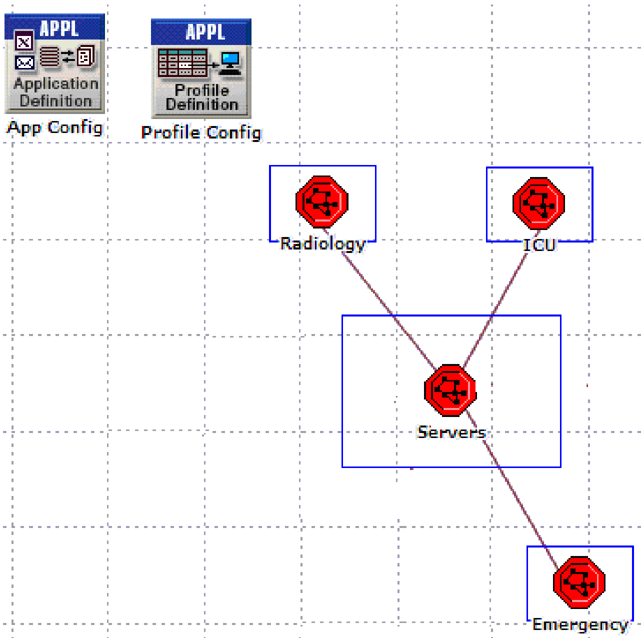


Figure A. 4: OPNET modelling of a simplified hospital network.

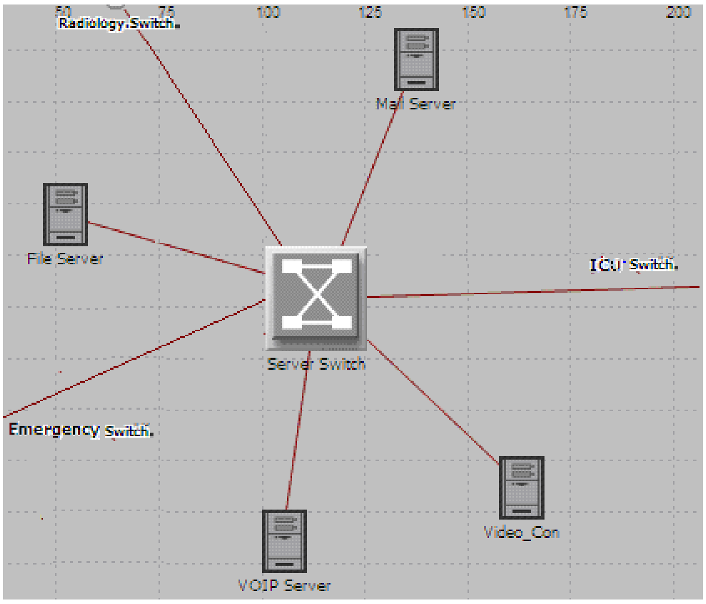


Figure A. 5: OPNET modelling of a server subnet.

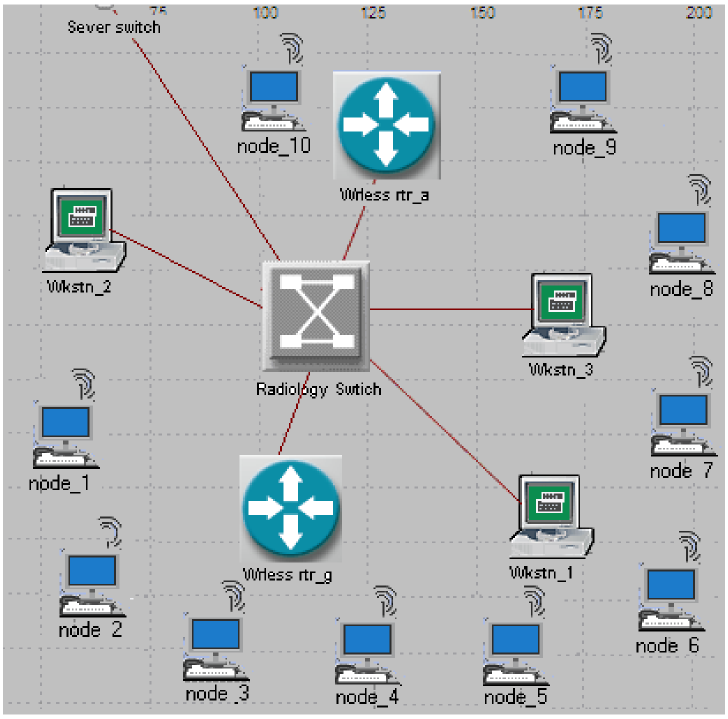


Figure A. 6: OPNET modelling of a radiology subnet with wired and wireless LAN.

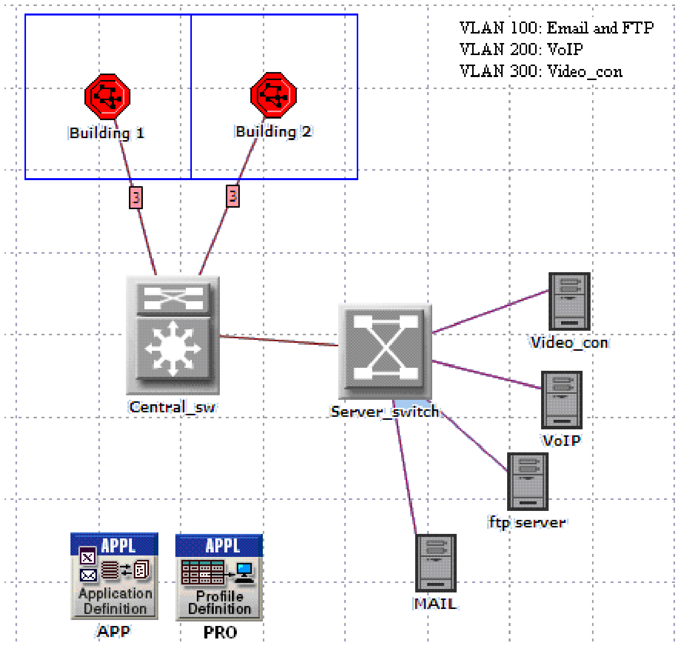


Figure A. 7: OPNET presentation of a complex hospital network.

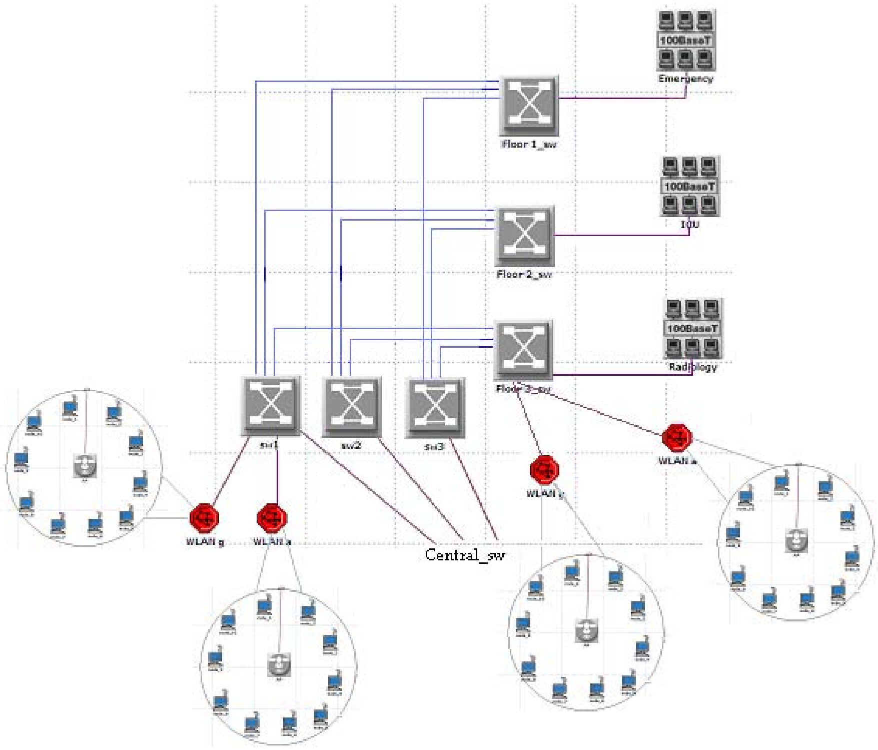


Figure A. 8: A building sub-module with wired and wireless LAN.

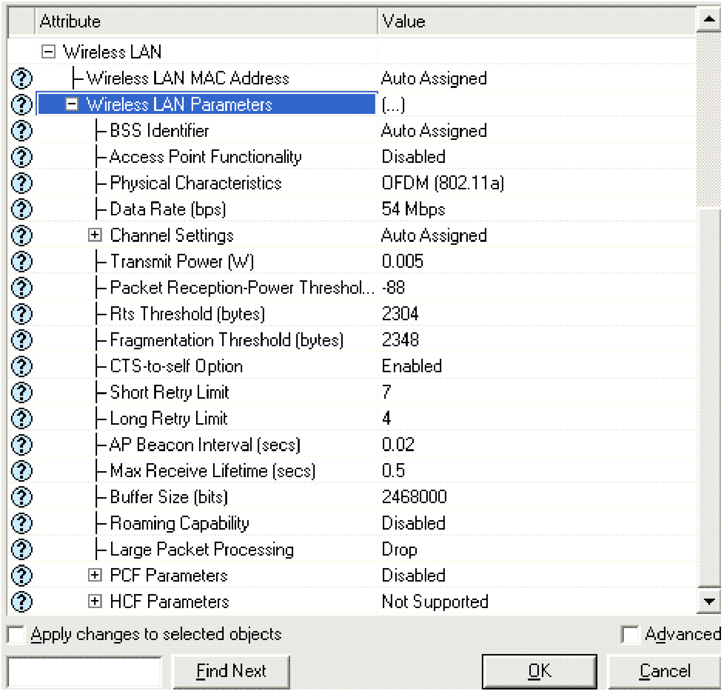


Figure A. 9: WLAN 802.11a attributes.

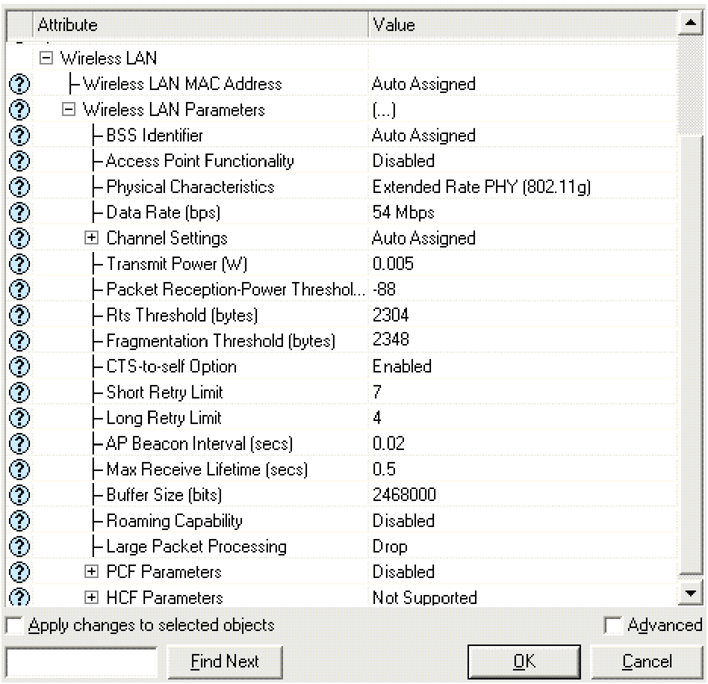


Figure A. 10: WLAN 802.11g attributes.

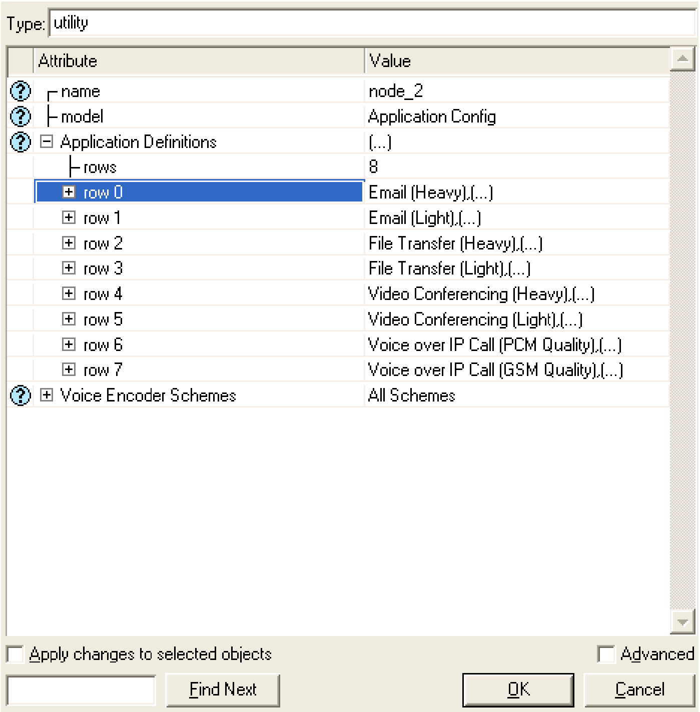


Figure A. 11: Application configuration.

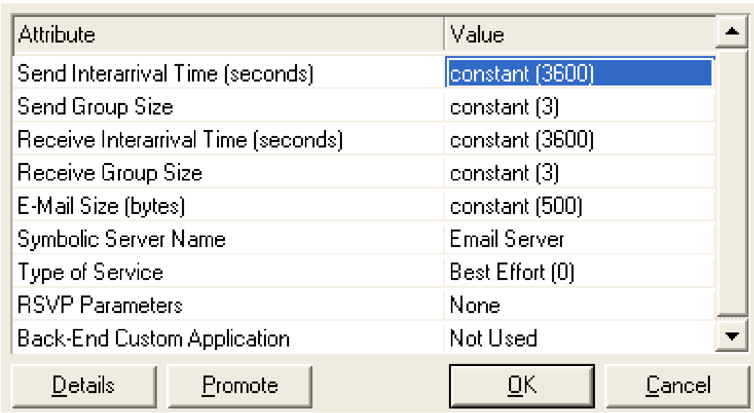
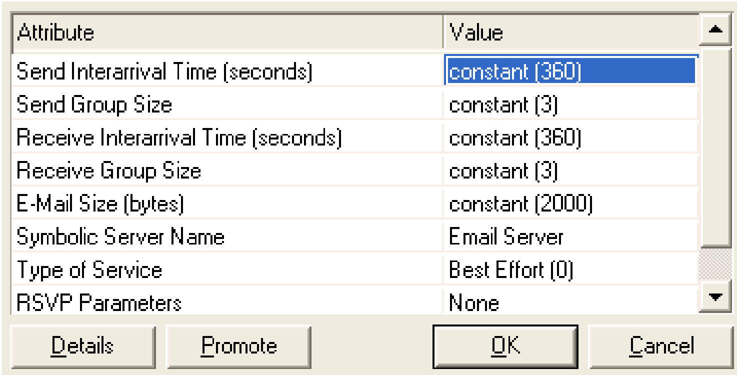
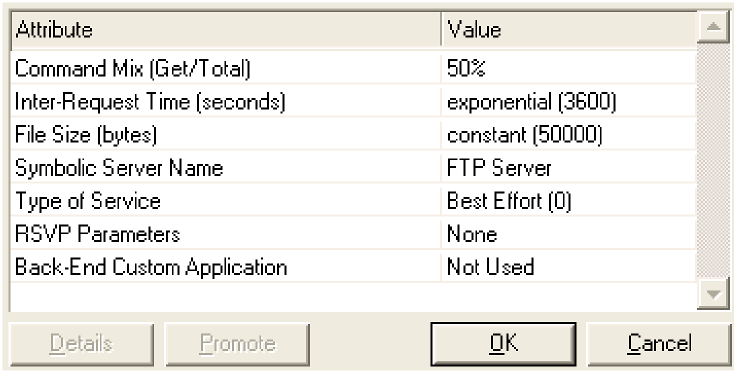


Figure A. 12: Email application attributes (light traffic).



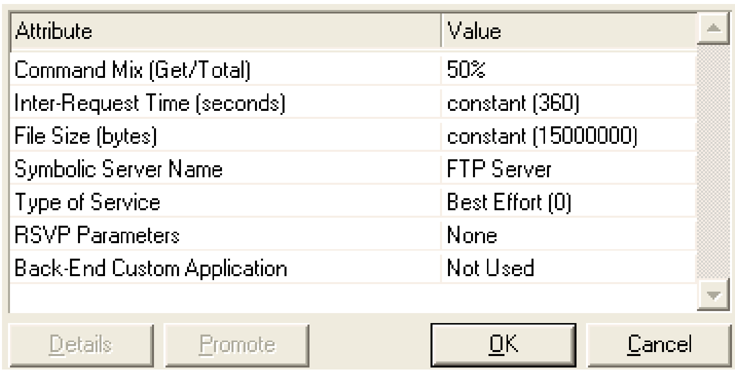
Attribute	Value
Send Interarrival Time (seconds)	constant (360)
Send Group Size	constant (3)
Receive Interarrival Time (seconds)	constant (360)
Receive Group Size	constant (3)
E-Mail Size (bytes)	constant (2000)
Symbolic Server Name	Email Server
Type of Service	Best Effort (0)
RSVP Parameters	None

Figure A. 13: Email application attributes (heavy traffic).



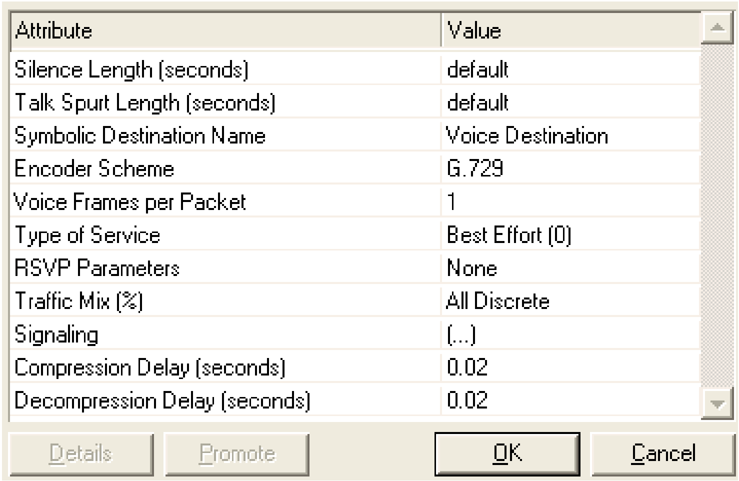
Attribute	Value
Command Mix (Get/Total)	50%
Inter-Request Time (seconds)	exponential (3600)
File Size (bytes)	constant (50000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort (0)
RSVP Parameters	None
Back-End Custom Application	Not Used

Figure A. 14: FTP application attributes (light traffic).



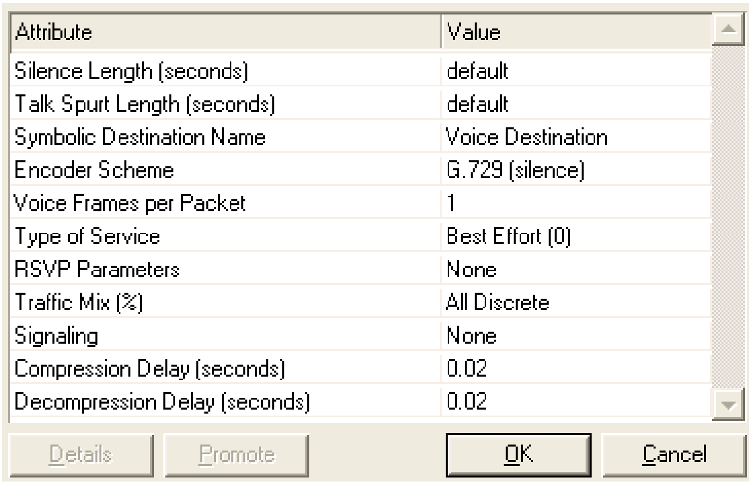
Attribute	Value
Command Mix (Get/Total)	50%
Inter-Request Time (seconds)	constant (360)
File Size (bytes)	constant (15000000)
Symbolic Server Name	FTP Server
Type of Service	Best Effort (0)
RSVP Parameters	None
Back-End Custom Application	Not Used

Figure A. 15: FTP application attributes (heavy traffic).



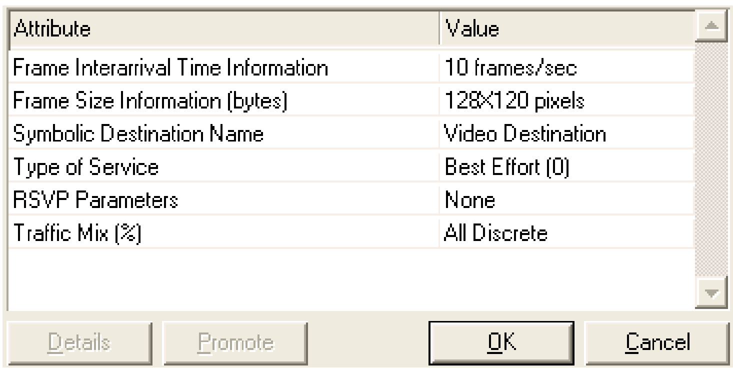
Attribute	Value
Silence Length (seconds)	default
Talk Spurt Length (seconds)	default
Symbolic Destination Name	Voice Destination
Encoder Scheme	G.729
Voice Frames per Packet	1
Type of Service	Best Effort (0)
RSVP Parameters	None
Traffic Mix (%)	All Discrete
Signaling	(...)
Compression Delay (seconds)	0.02
Decompression Delay (seconds)	0.02

Figure A. 16: VoIP application attributes (light traffic).



Attribute	Value
Silence Length (seconds)	default
Talk Spurt Length (seconds)	default
Symbolic Destination Name	Voice Destination
Encoder Scheme	G.729 (silence)
Voice Frames per Packet	1
Type of Service	Best Effort (0)
RSVP Parameters	None
Traffic Mix (%)	All Discrete
Signaling	None
Compression Delay (seconds)	0.02
Decompression Delay (seconds)	0.02

Figure A. 17: VoIP application attributes (heavy traffic).



Attribute	Value
Frame Interarrival Time Information	10 frames/sec
Frame Size Information (bytes)	128X120 pixels
Symbolic Destination Name	Video Destination
Type of Service	Best Effort (0)
RSVP Parameters	None
Traffic Mix (%)	All Discrete

Figure A. 18: Video_con application attributes (light traffic).

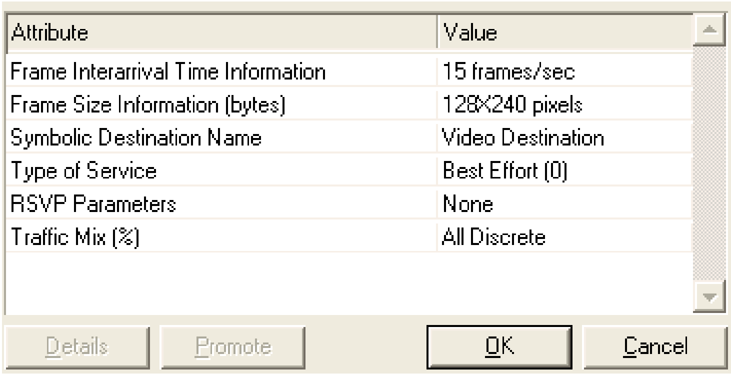


Figure A. 19: Video_con application attributes (heavy traffic).

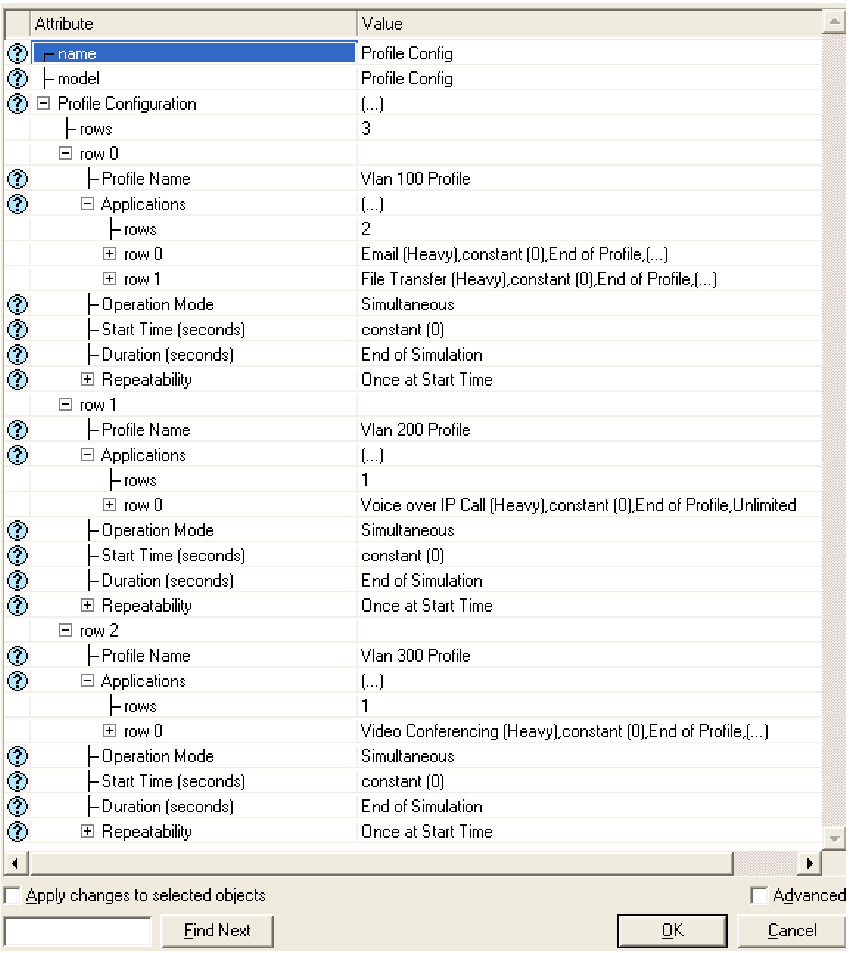


Figure A. 20: Profile attributes.

Appendix B

Additional results for Chapter 5

Table B.1: Average client performance under light traffic condition.

Traffic type	Nodes	Upload response time (s)	Download response time (s)	End-to-end delay (ms)	Packet delay variation (ms)	Jitter (ms)	Packet drop (kbps)	Throughput (kbps)
Email	50	0.02	0.021	-	-	-	-	-
	100	0.019	0.02	-	-	-	-	-
	300	19	0.021	-	-	-	-	-
FTP	50	0.11	0.12	-	-	-	-	-
	100	0.11	0.11	-	-	-	-	-
	300	0.12	0.12	-	-	-	-	-
Audio	50	-	--	62	5.5	0.003	0	3
	100	-	-	62	4.1	0.08	0	5
	300	-	-	63	2	1	0	8
Video	50	-	-	8	0.02	-	186	11254
	100	-	-	9	0.03	-	645	13153
	300	-	-	8	0.02	-	400	13348

Table B.2: Average client performance under heavy traffic condition.

Traffic type	Nodes	Upload response time (s)	Download response time (s)	End-to-end delay (ms)	Packet delay variation (ms)	Jitter (ms)	Packet drop (kbps)	Throughput (kbps)
Email	50	0.027	0.019	-	-	-	-	-
	100	0.026	0.02	-	-	-	-	-
	300	0.027	0.02	-	-	-	-	-
FTP	50	55	0.026	-	-	-	-	-
	100	34	0.027	-	-	-	-	-
	300	42	0.029	-	-	-	-	-
Audio	50	-	--	63	6.1	0.1	0	15
	100	-	-	63	5.7	0.07	0	63
	300	-	-	63	5	0.05	0	80
Video	50	-	-	12	510	-	1779	11633
	100	-	-	84	421	-	1423	18194
	300	-	-	22	579	-	6616	20012

Table B.3: Average server performance under light traffic condition.

Traffic type	Nodes	Traffic sent (kbps)	Traffic received (kbps)	Throughput (kbps)	Packet drop (kbps)
Email server	50	0.05	0.05	0.41	0
	100	0.10	0.10	0.81	0
	300	0.30	0.30	2.38	0
File server	50	68.73	68.73	68.73	0
	100	696.87	696.87	696.87	0
	300	701.03	701.03	701.03	0
VoIP server	50	13.24	13.24	13.24	0
	100	26.12	26.12	26.12	0
	300	78.1	78.1	78.10	0
Video server	50	2821.08	2635.08	2635.08	186
	100	3419.06	346.76	2774.06	645
	300	3174.06	346.76	2774.06	400

Table B.4: Average server performance under heavy traffic condition.

Traffic type	Nodes	Traffic sent (kbps)	Traffic received (kbps)	Throughput (kbps)	Packet drop (kbps)
Email server	50	2.3	2.30	2.30	0
	100	5.22	5.22	5.22	0
	300	16.3	16.30	16.30	0
File server	50	11.7	11.59	11.59	0.11
	100	23.93	23.93	23.93	0
	300	707.28	707.28	707.28	0
VoIP server	50	36.21	36.21	36.21	0
	100	71.71	71.71	71.71	0
	300	213.72	213.72	213.72	0
Video server	50	7782.98	6003.98	6003.98	1779
	100	8852.53	7429.53	7429.53	1423
	300	14933.7	8317.7	8317.70	6616

References

[1] R. Evans and N. Sarkar, "Mobile Commerce Implementation in the Hospital Environment: Issues, Challenges and Future Trends," *Bulletin of Applied Computing and Information Technology* vol. 2, no. 1, pp. 56-62, 2004.

[2] P. Aspden, J. A. Wolcott, J. L. Bootman, and R. Linda, "Quality Chasm Series," in *Preventing Medication Errors*. Washington, DC: Institute of Medicine, the National Academies Press 2006, pp. 480.

[3] A. Soomro and D. Cavalcanti, "Opportunities and Challenges in Using WPAN and WLAN Technologies in Medical Environments," *IEEE Communication Magazine*, vol. 45, no. 2, pp. 114-122, 2007.

[4] D. Watson. (2003). *Hospital goes to patient*. Retrieved August 12 2008, from Computer World Website http://www.computerworld.co.nz/webhome.nsf

[5] P. Latkoski, Z. Hadzi-Velkov, and B. Popovski, "Performance analysis of IEEE 802.11 a WLAN in block fading channel using SDL simulation," presented at the 7th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, Serbia and Montenegro, Nis, September 28-30 2005, pp. 97-100.

[6] K. A. Banitsas, Y. H. Song, and T. J. Owens, "OFDM over IEEE 802.11b hardware for tele-medical applications," *International Journal of Mobile Communications* vol. 2, no. 3, pp. 310-327, 2004.

[7] A. L. Wijesinha, Y. Song, M. Krishnan, V. Mathur, J. Ahn, and V. Shyamasundar, "Throughput measurement for UDP traffic in an IEEE 802.11g WLAN," presented at The Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SAWN '05). , Washington, DC, USA, 23-25 May 2005, 2005, pp. 220- 225.

[8] Y. Xiao, "IEEE 802.11e: QoS provisioning at the MAC layer," *IEEE Wireless Communications*, vol. 11, no. 3, pp. 72-79, 2004.

[9] U. Varshney, "Pervasive Healthcare and Wireless Health Monitoring," *Springer Mobile Networks.*, vol. 12, no. 2-3, pp. 113-127, 2007.

[10] W. Xiu-fang, D. Hong, W. Yu-heng, and J. Li-li, "Modelling and simulation of wireless local area network MAC access mechanism in oil field," presented at the IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '07), Shanghai, China, September 21-23 2007, pp. 2148-2151.

[11] N. I. Sarkar and K. W. Sowerby, "Wi-Fi Performance Measurements in the Crowded Office Environment: a Case Study," *International Conference on Communication Technologies (ICCT '06)*, no. 1-4, 2006.

[12] J. Potemans, J. Theunis, B. Rodiers, B. Van den Broeck, P. Leys, E. Van Lil, and A. Van de Capelle, "Simulation of a campus backbone network, a case study," presented at the OPNETWORK Conference, Washington D.C., Aug. 1, 2002, pp. 1-6.

[13] C. Chigan and V. Oberoi, "QoS in Ubiquitous Telemedicine Networks.," presented at the proceedings of the Four Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06). , March 2006, 2006, pp. 13-17.

[14] A. S. Bisain, "Intelligent network based wireless services for telemedicine," in *Master of Science Report, Dep. of System Engineering, Graduate School of the University of Maryland*, 1998, pp. 1-142.

[15] K. A. Banitsas, S. Tachakra, and R. S. H. Istepanian, "Operational parameters of a medical wireless LAN: security, range and interference issues," presented at the Proceedings of the Second Joint EMBS/BMES Conference, Houston, TX, USA, 23-26 October, 2002, pp. 23-26.

[16] D. Watson. (2002). *Patients go wireless at Dunedin Hospital*. Retrieved August 12 2008, from Computer World Website http://www.computerworld.co.nz/webhome.nsf

[17] J. Li, L. Wilson, S. Stapleton, and P. Cregan, "Design of advanced telemedicine system for emergency care," presented at the Proceedings of the 20th Conference of the Computer-human Interaction Special Interest Group (CHISIG). Sydney, Australia, November, 21-23, 2006, 2006, pp. 413-416.

[18] W. Fox. (2008). *Life-critical Wireless Networks*. Retrieved 16th Oct, 2008, from Welch Allyn Solution Website http://www.welchallyn.com/

[19] S. Bryan, G. C. Weatherburn, J. R. Watkins, and M. J. Buxton, "The benefits of hospital-wide picture archiving and communication systems: a survey of clinical users of radiology services," *The British Journal of Radiology*, vol. 72, no. 857, pp. 469-478, 1999.

[20] K. Banitsas, R. S. H. Istepanian, and S. Tachakra, "Applications of Medical LAN Systems (MedLAN)," *Journal of Health Marketing*, vol. 3, no. 1, pp. 112-117, 2002.

[21] S. Cocoradal and I. Szekelyl, "Simulation-based performance analysis of multicast transmissions in an 802.1 1g WLAN," presented at the International Symposium on Signals, Circuits and Systems (ISSCS 2007). in the International Symposium on Signals, Circuits and Systems (ISSCS'07). Iasi, Rumania July, 12-13, 2007, pp. 1-4.

[22] S. Su and C. L. Shih, "Modelling an Emergency Medical Services System Using Computer Simulation," *International Journal of Medical Informatics*, vol. 2003, no. 72, pp. 57-72, 2003.

[23] K. A. Banitsas, P. Georgiadis, S. Tachakra, and D. Cavouras, "Using handheld devices for real-time wireless tele-consultation," presented at the Proceedings of the 26th Annual International Conference of the IEEE EMBS, San Francisco, CA, USA, September 1-5, 2004, pp. 3105-3108.

[24] A. Assaad and D. Fayek, "General hospitals network models for the support of e-health applications," presented at the Tenth IEEE/IFIP Network Operations and Management Symposium (NOMS'06) Vancouver, Canada April 2006, 2006, pp. 1-4.

[25] C. Chigan and V. Oberoi, "Providing QoS in ubiquitous telemedicine networks," presented at the Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops(PERCOMW'06) Houghton, USA, March, 13-17 2006, pp. 1-5.

[26] N. Golmie, D. Cypher, and O. Rebala, "Performance analysis of low rate wireless technologies for medical applications," *Computer Communications* vol. 28, no. 10, pp. 1266-1275 2004.

[27] Y. Chu and A. Ganz, "WISTA: A Wireless Telemedicine System for Disaster Patient Care," *Mobile Network Applications*, vol. 12, no. 2-3, pp. 201-214, 2007.

[28] R. LeMay. (2006). *Sydney hospital plans unusual wireless network*. Retrieved July 28, 2008, from http://www.zdnet.com.au

[29] E. C. Lo, "An Investigation of the Impact of Signal Strength on Wi-Fi Link Throughput through Propagation Measurement," in *Master dissertation, School of Computing and Mathematical Sciences at Auckland University of Technology* 2007, pp. 1-163.

[30] A. N. M. Abdullah, H. Moinudeen, and W. Al-Khateeb, "Scalability and performance analysis of IEEE 802.11a," presented at the Canadian Conference on Electrical and Computer Engineering, Saskatchewan Canada May 1-4 2005, pp. 1626-1629.

[31] O. C. Branquinho, N. Reggiani, and D. M. Ferreira, "Mitigating 802.11 MAC anomaly using SNR to control backoff contention window," presented at the proceedings of IEEE International Conference on Wireless and Mobile Communications (ICWMC '06). Bucharest, Romania, July 29-31, 2006, pp. 590-593.

[32] I. Broustis, D. Papagiannaki, Krishnamurthy, M. Faloutsos, and V. Mhatre, "MDG: measurement-driven guidelines for 802.11 WLAN design," presented at the proceedings of the 13th annual ACM international conference on Mobile computing and networking (MobiCom '07). Montreal, Quebec, Canada, September 9–14, 2007, pp. 254-265.

[33] C. Y. Chang and H. R. Chang, "Power Control and Fairness MAC Mechanisms for 802.11 WLANs," *Computer Communications*, vol. 30, no. 7, pp. 1527-1537, 2007.

[34] S. Choi, K. Park, and C. Kim, "On the performance characteristics of WLANs: revisited," presented at the proceedings of the international conference on Measurement and modelling of computer systems (SIGMETRICS'05). Banff, Alberta, Canada., June 6–10, 2005, pp. 97-108.

[35] M. H. Manshaei and T. Turletti, "Simulation-based performance analysis of 802.11a Wireless LAN," presented at the International Symposium of Telecommunications IST, IRAN-Isfahan, August, 2003, pp. 221-226.

[36] W. Hneiti and N. Ajlouni, "Performance enhancement of wireless local area networks.," presented at the 2nd Information and Communication Technologies (ICTTA '06), Umayyad Palace, Damascus, Syria April 24-28 2006, pp. 2400-2404.

[37] L. Phifer, "Enabling Enterprise Wi-Fi," *Business Communications Review*, vol. 2, no. 2004, pp. 45-53, 2004.

[38] M. M. Gunal and M. Pidd, "Understanding accident and emergency department performance using simulation," presented at the Proceedings of the 2006 Winter Simulation Conference, Monterey, Canada, Dec. 3-6 2006, pp. 446-452.

[39] T. J. Owens, S. Tachakra, K. A. Banitsas, and R. S. H. Istepanian, "Securing a medical wireless LAN system," presented at the Proceedings of the 23rd Annual EMBS International Conference, Istanbul, Turkey, Oct. 25-28 2001, pp. 3552-3555.

[40] B. Zhen, H. B. Li, S. Hara, and R. Kohno, "Clear Channel Assessment in Integrated Medical Environments," *EURASIP Journal on Wireless Communications and Networking*, vol. 8, no. 3, pp. 1-8, 2008.

[41] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535-547, 2000.

[42] R. V. De Jongh, M. Hajian, and L. P. Ligthart, "Time Domain Antenna Measurements: Implementation and Verification of a Novel Technique," presented at the 27th European Microwave Conference and Exhibition 8-12 Sep 1997, 1997, pp. 470 - 475.

[43] G. Alvarez, F. E. Bustamante, R. Becker-szendy, and J. Wilkes. (2009). *Technique for programmatically obtaining experimental measurements for model construction* Retrieved 03/17/2009 from Free Patent Online Website: http://www.freepatentsonline.com/

[44] S. Xua and T. Saadawib, "Revealing the Problems with 802.11 Medium Access Control Protocol in Multi-hop Wireless Ad Hoc Networks.," *Science Direct Computer Networks* vol. 38, no. 4, pp. 531-548, 2002.

[45] R. M. Fujimoto, K. Perumalla, A. Park, H. Wu, M. H. Ammar, and G. F. Riley, "Large-scale network simulation: how big? how fast?," presented at the 11th IEEE/ACM International Symposium on Modelling, Analysis and Simulation of Computer Telecommunications Systems (MASCOTS'03), Atlanta, GA, USA, 12-15 Oct. 2003, 2002, pp. 116-123.

[46] D. M. Gaba, "The future vision of simulation in health care," *Quality and Safety in Health Care*, vol. 13, no. 2004, pp. 2-10 2004.

[47] N. I. Sarkar, "Simulation of Computer Networks: Simulators, Methodologies and Recommendations," presented at the 5th International Conference on Information Technology and Application (ICITA'08), Cairns, Queensland, Australia. , June 23-26, , 2008, pp. pp.420-425. .

[48] E. H. Page and B. S. Canova, "A Case Study of Verification, Validation, and Accreditation for Advanced Distributed Simulation," *ACM Transactions on Modelling and Computer Simulation*, vol. 7, no. 3, pp. 393-424, 1997.

[49] S. Robinson, "Simulation model verification and validation: increasing the users' confidence," presented at the Proceedings of the 29th conference on Winter simulation (WSC '97), Atlanta, Georgia, United States December 07-10, 1997, 1997, pp. 53-59.

[50] A. Varga, "The OMNET++ discrete event simulation system " in *the Proceedings of the European Simulation Multi-conference* Prague, Czech Republic: SCS - European Publishing House, 2001, pp. 319-324.

[51] K. Salah, P. Calyam, and M. I. Buhari, "Accessing readiness of IP networks to support desktop videoconferencing using OPNET," *Journal of Network and Computer Applications*, vol. 10, no. 2007, pp. 1-23, 2007.

[52] K. Salah, "On the deployment of VoIP in Ethernet networks: Methodology and case study," *Journal of Computer communications*, vol. 29, no. 2006, pp. 1039-1054, 2005.

[53] I. N. Bankman, "Handbook of medical imaging: Processing and Analysis," *Annals of Biomedical Engineering*, vol. 29, no. 8, pp. 729, 2000.

[54] G. Rittenhouse and H. Zheng, "Proving VoIP service in UMTS-HSDPA with Frame Aggregation," presented at the Proceedings of IEEE Acoustics, Speech and Signal Processing (ICASSP’05), Philadelphia, PA, March 18-23, 2005, 2005, pp. 1121-1124.

[55] I. Haratcherev and K. Langendoen, "Hybrid rate control for IEEE 802.11. ," presented at the proceedings of the second international workshop on Mobility management & wireless access protocols (MobiWac'04), , Philadelphia, Pennsylvania, USA., October 1,, 2004, pp. 10 - 18

[56] M. S. Obaidat and D. G. Green, "An Adaptive Protocol Model for IEEE 802.11 Wireless LANs," *Computer Communications* vol. 27, no. 12, pp. 1131-1136, 2004.

[57] R. G. Sargent, "Validation and verification of simulation models," presented at the Proceedings of the 2004 Winter Simulation Conference, Washington, DC, December 5-8 2004, pp. 39-48.

[58] N. Shetty, S. Choudhury, and J. Gibson, "Voice capacity under quality constraints for IEEE 802.11a based WLANs.," presented at the proceedings of the 2006 international conference on Wireless communications and mobile computing (IWCMC’06), Vancouver, British Columbia, Canada, July, 2006, pp. 1345-1350. .

[59] M. Li, B. Prabhakaran, and S. Sathyamurthy, "On flow reservation and admission control for distributed scheduling strategies in IEEE802.11 wireless LAN," presented at the Proceedings of the 6th ACM international workshop on Modelling analysis and simulation of wireless and mobile systems (MSWiM'03), San Diego, CA, USA, September 19, 2003, 2003, pp. 108-115.

[60] S. Shakkottai, T. S. Rappaport, and P. C. Karlsson, "Cross-layer design for wireless networks," *Communications Magazine*, vol. 41, no. 10, pp. 74-80, 2003.

[61] S. Mangold, C. Sunghyun, G. R. Hiertz, O. Klein, and B. Walke, "Analysis of IEEE 802.11e for QoS support in wireless LANs," *IEEE Wireless Communications*, vol. 10, no. 6, pp. 40-50, 2003.