MedLAN: Compact Mobile Computing System for Wireless Information Access in Emergency Hospital Wards

A thesis submitted for the degree of
Doctor of Philosophy

by

Konstantinos A. Banitsas
Bsc (Hons), Msc, MIEEE, MIEE

Department of Electronic and Computer Engineering

Brunel University

May 2004

Abstract: As the need for faster, safer and more efficient healthcare delivery increases, medical consultants seek new ways of implementing a high quality telemedical system, using innovative technology. Until today, teleconsultation (the most common application of Telemedicine) was performed by transferring the patient from the Accidents and Emergency ward, to a specially equipped room, or by moving large and heavy machinery to the place where the patient resided. Both these solutions were unpractical, uneconomical and potentially dangerous. At the same time wireless networks became increasingly useful in point-of-care areas such as hospitals, because of their ease of use, low cost of installation and increased flexibility.

This thesis presents an integrated system called **MedLAN** dedicated for use inside the A&E hospital wards. Its purpose is to **wirelessly** support high-quality live video, audio, high-resolution still images and networks support from anywhere there is WLAN coverage. It is capable of transmitting all of the above to a consultant residing either inside or outside the hospital, or even to an external place, thorough the use of the Internet. To implement that, it makes use of the existing IEEE 802.11b wireless technology.

Initially, this thesis demonstrates that for specific scenarios (such as when using WLANs), DICOM specifications should be adjusted to accommodate for the reduced WLAN bandwidth. Near lossless compression has been used to send still images through the WLANs and the results have been evaluated by a number of consultants to decide whether they retain their diagnostic value.

The thesis further suggests improvements on the existing 802.11b protocol. In particular, as the typical hospital environment suffers from heavy RF reflections, it suggests that an alternative method of modulation (OFDM) can be embedded in the 802.11b hardware to reduce the multipath effect, increase the throughput and thus the video quality sent by the MedLAN system.

Finally, realising that the trust between a patient and a doctor is fundamental this thesis proposes a series of simple actions aiming at securing the MedLAN system. Additionally, a concrete security system is suggested, that encapsulates the existing WEP security protocol, over IPSec.

To my loving father, Athanassios, whose death
could have been avoided if technology like this existed.

Contents

1. Introduction 1

1.1 Telemedical needs 1

1.2 Basic WLAN concepts 2

1.3 Existing applications 4

1.4 Thesis objectives 7

1.5 Contribution to knowledge 7

1.6 Dissertation structure 9

2. Applications of Telemedicine 11

2.1 Definition of Telemedicine 11

2.2 Divisions of Telemedicine and Telecare 11

2.2.1 Teleconsultation 11

2.2.2 Tele-education 13

2.2.3 Telemonitoring 14

2.2.4 Telesurgery 15

2.3 Advantages and limitations of Telemedicine 16

2.4 Ethical and legal aspects 18

2.4.1 Confidentiality and patients expectations 18

2.4.2 Data Protection Act 19

2.4.3 Common problems and risks 20

2.4.4. Engineering concerns 21

2.4.5 NHS principles 22

2.5 Structure of a telemedical system 23

2.5.1 Text 24

2.5.2 Audio 24

2.5.3 Still images 25

2.5.4 Video 26

2.5.5 Image compression 27

2.5.6 Communication lines 29

2.6 Summary and conclusions 31

3. Wireless LANs 33
3.1 Introduction 33
3.2 Wireless evolution 33
3.3 Applications of WLANs 35
3.4 Benefits, concerns and challenges of WLANs 36
3.5 WLAN frequency bands 39
3.6 WLAN trends and versions 40
3.6.1 IEEE 802.11 40
3.6.2 ETSI HiperLAN 41
3.7 Physical characteristics of 802.11b 43
3.7.1 Mapping 802.11b into the ISO-OSI 7 layer model 43
3.7.2 Wireless media 44
3.7.3 Medium Access Control layer (MAC) 48
3.7.4 A general WLAN model: sequence of operations 49
3.8 Installation considerations 51
3.8.1 Topologies of WLANs 51
3.8.2 Frequency planning 53
3.8.3 The hidden station problem 55
3.8.4 Interference by other 2.4GHz devices 56
3.9 IEEE 802.11b services 58
3.10 Summary and conclusions 61

4. The MedLAN System 63
4.1 Introduction 63
4.2 Current and future medical needs 63
4.3 System description 65
4.3 System services and performance 69
4.3.1 Video 70
4.3.2 Audio 74
4.3.3 Still images 76
4.3.4 Connecting to an external device 78
4.3.5 Wireless network access 80
4.3.6 Using a PDA at the consultant’s site 80
4.4 Range and scalability of the MedLAN system 82

4.5 Interference with medical equipment 85
4.6 Testing phase evaluation 89
4.6.1 Doctors in the A&E ward 89
4.6.2 Consultants 90
4.6.3 Nurses / healthcare personnel 90
4.6.4 Patients 91
4.6.5 Overall results 91
4.7 Conclusions 92

5. Adjusting DICOM Specifications in a Wireless LAN System 93
5.1 Introduction 93
5.2 DICOM recommendations 94
5.2.1 Scope of DICOM 94
5.2.2 Goals of DICOM standards 95
5.2.3 Structure of DICOM standards 96
5.2.4 DICOM image format 98
5.3 Image and video compression 99
5.3.1 JPEG 100
5.3.2 MPEG 104
5.4 DICOM's approach to compression 108
5.5 Defining the problem 110
5.5.1 Bandwidth requirements 111
5.5.2 Wireless capabilities 111
5.5.3 Searching for the "golden rule" 112
5.6 Methodology 113
5.6.1 Using test patterns to evaluate performance 113
5.6.2 Using expert's opinion to empirically evaluate performance 115
5.7 Results and discussion 116
5.8 Conclusions 117

6. OFDM over IEEE 802.11b Hardware for Telemedical Applications 119
6.1 Introduction 119
6.2 Existing technologies 120
6.3 OFDM 124

6.4 Methodology 129
6.4.1 Physical layer simulation 131
6.4.2 Upper layer simulation 133
6.5 Results 135
6.6 Summary and conclusions 138

7. Securing a Wireless Telemedical System 140
7.1 Introduction 140
7.2 Current security standards 141
7.3 WEP 143
7.3.1 WEP encryption / decryption process 143
7.3.2 WEP implementation 146
7.3.3 WEP overhead benchmark 147
7.4 WEP vulnerabilities 148
7.4.1 Risk of keystream reuse 149
7.4.2 Message authentication 150
7.4.3 Future improvements: AES and WPA 152
7.4.4 Concerns and unjustified fears of WLAN security 154
7.5 Management and human issues of telemedical security 155
7.5.1 Management issues 155
7.5.2 Human issues 157
7.6 Creating a set of countermeasures 157
7.6.1 Immediate Actions 158
7.6.2 Configuration and Management Actions 159
7.7 IP Secure (IPSec) 160
7.7.1 IPSec architecture and function 161
7.7.2 IPSec key advantages 162
7.7.3 Authentication and key management 163
7.7.4 Using IPSec 163
7.8 Securing a telemedical WLAN 166
7.8.1 Methodology 166
7.8.2 Discussion 168
7.9 Conclusions 169

8. Conclusions 171
8.1 Summary and conclusions 171
8.2 Future directions 174

Appendices 178
A. IEEE 802.11 modulation 178
B. Timing of IEEE 802.11 frames 179
C. Specifications of the MedLAN system 180
D. Range of the MedLAN system in CMH A&E 181
F. Structure of DICOM standards 183
G. Modalities supported by DICOM 184
H. ACR/NEMA Equipment Specification 185
I. Modalities used 188
J. Doctor's Questionnaire 190
K. VisSim modules 191
L. Using a Radius server: sequence of events 192
M. IPSec modes 193

Glossary 194

References 198

Publications 206

List of figures and tables

Fig. 1.1 Wireless Telemedicine in use: drug subscription using a WLAN.....2
Fig. 1.2 A variety of WLAN architectures find increased acceptance.....3

Fig. 2.1 Videoconferencing is the most commonly used application of.....12
Fig. 2.2 Using telemedical links to enhance education of healthcare personnel.....14
Fig. 2.3 A patient suffering from hypertension is using a digital device.....15
Fig. 2.4 A specialist performs remote surgery by controlling a robotic arm 16
Table 2.1 Examples of telemedical data with their typical sizes 24
Table 2.2 Typical medical modalities in original and compressed form 28
Table 2.3 Communication line options for telemedical uses 31

Table 3.1 ISM and UNII unlicensed bands used in most of WLAN networks.....40
Table 3.2 Comparison of WLAN standards and technologies today.....42
Fig. 3.1 The IEEE 802 model compared to the 7-layer OSI model for the 802.1 43
Fig. 3.2 A typical infrared configuration. Several IR networks can be set up.....45
Fig. 3.3 Frequency Hopping Spread Spectrum uses a pseudo random.....46
Fig. 3.4 Direct Signal Spread Spectrum adds redundant information.....47
Fig. 3.5 MAC frame and LLC PDU format of 802.11.....48
Fig. 3.6 MAC frame of IEEE 802.11 as it is actually transmitted over the medium .49
Fig. 3.7 Clockwise sequence of events within the lower layers of both OSI.....50
Fig. 3.8 Wireless ad-hoc topology with no need for an AP 51
Fig. 3.9 Infrastructure mode: each AP creates a cell (BSS). Multiple APs 52
Fig. 3.10 Wireless bridges connect networks from different buildings 53
Fig. 3.11 802.11b has 11 partially overlapping channels.....53
Fig. 3.12 By establishing the range of each AP, the same frequencies.....54
Fig. 3.13 By having eight, instead of three independent channels, 802.11a.....54
Fig. 3.14 The hidden station problem 55
Fig. 3.15 By using RTS/CTS commands, the hidden station problem is eliminated.55
Fig. 3.16 IEEE 802.11b with Bluetooth interferer at 10m and at 10cm. 57
Fig. 3.17 Authentication, de-authentication, association, disassociation.....60

Fig. 4.1 A modern videoconferencing system including 64
Fig. 4.2 The MedLAN system 65
Fig. 4.3 The MedLAN prototype trolley while communicating 66
Fig. 4.4 Block diagram of the operation of the MedLAN system.....69
Fig. 4.5 Microsoft NetMeeting videoconference settings:.....71
Fig. 4.6 By using simple Java scripts, live video can be transmitted). 73
Fig. 4.7 comparison between the transmissions of MNM (right) and TeVeo (left)...74
Table 4.1 Sound compressors available on the MNM 75
Fig. 4.8 MedLAN still image transmission: a. macro detail of a patient. 76
Table 4.2 Still image file sizes depending on resolution and level of compression ..77
Fig. 4.9 Still images were better captured using “manual exposure”. 78
Fig. 4.10 The MedLAN system is capable of connecting to an external 79
Fig. 4.11 Mobile PDA viewing a DICOM image b. zooming into the ROI 81
Fig. 4.12 Site survey tools provided by Cisco systems indicate signal strength.....83
Fig. 4.13 The range of two APs as revealed after a site survey of the CMH.....84
Fig, 4.14 Basic structure of North West London Hospital network. 85
Fig. 4.15 Worst-case EM emissions recorded from five measurement sites 87
Table 4.3 Interference of IEEE 802.11b WLAN 88
Table 4.4 Interference of IEEE 802.11b WLAN in NWLH 89

Fig. 5.1 Scope of DICOM in medical informatics.....95
Fig. 5.2 Relationship of the first nine parts of the DICOM standards. 97
Fig. 5.3 Mapping the OSI 7-layer model to the DICOM model: two more.....97
Fig. 5.4 Zig-zag scan used by the JPEG algorithm.....101
Fig. 5.5 JPEG baseline codec: sequence of events.....101
Fig. 5.6 Detail of an original image. b. The square represents the detai.....102
Fig. 5.7 PSNR over bpp for JPEG, JPEG 2000, PCM (uncompressed) 104
Fig. 5.8 VO1 and VO2 are the moving foreground while VO3 is the stable.....106
Fig. 5.9 Performance comparison of various codecs when compressing medical...109
Table 5.1 Space required for storing a 10-bit colour image using different. 111
Table 5.2 Time required for sending a 10-bit colour image through a WLAN 112
Table 5.3 A simple comparison between the DICOM popular format.....112
Fig. 5.10 Comparison between an original SMPTE pattern (a).....114
Fig. 5.11 Detail of an electronically created SMPTE pattern used.....115
Table 5.4 Evaluation of the MedLAN’s outputs (still images, video and sound)....116

Fig. 6.1 Multipath effect: the signal is reflected on various surfaces. 121
Fig. 6.2 WLAN range comparison between 802.11a and 802.11b inside the A&E 123
Table 6.1 Transmission and Reflection values of common materials for ISM.....124
Fig. 6.3 FDM Access in a typical landline exchange centre: many users share 125
Fig. 6.4 In OFDM, carriers are carefully selected so they would be. 126
Fig. 6.5 Transmitter design of an OFDM system. 127
Fig. 6.6 OFDM encoding / decoding sequence.....127
Fig. 6.7 When a subcarrier arrives later than expected.....128
Table 6.2 Comparison table between IEEE 802.11b, a and g in terms of data rates130
Table 6.3 PHY layer parameters of the model.....132
Fig. 6.8 Defining the noise sources of the model: an AWGN generator 132
Fig. 6.9. Block diagram representation of the physical layer of 802.11b, ...133
Fig. 6.10 Model of the A&E room of the Central Middlesex Hospital: 134
Fig. 6.11 Eb/No of the signal versus BER for various scenarios:) 136
Fig. 6.12 An average increase of 1 Mbps was observed in the simulation.....137

Fig. 7.1 SSID and MAC filtering process in an infrastructure WLAN 142
Fig. 7.2 Encryption and decryption process of the WEP algorithm.....144
Fig. 7.3 Encrypted WEP frame 145
Fig. 7.4 Through a web page, the key (k) can be set for use by the AP.....146
Fig. 7.5 Setting the WEP key on the MT's side.....147
Table 7.1 Effects of WEP encryption on the IEEE 802.11b throughput 148
Fig. 7.6 Using a Radius server as an interim solution between the existing WEP ..154
Fig. 7.7 Treating the WLAN system as external: placing the AP behind.....159
Fig. 7.8 Implementing IPSec in a standard network:.....164
Fig. 7.9 running the MMC program permits the user to select the kind of security 167
Table 7.2 Overheads introduced while transferring various size files.....168

Acknowledgements

I would like to acknowledge my deep gratitude to the following persons:
Prof. Yong Hua Song who acted as my supervisor and allowed me the freedom that I needed to complete this project.
Dr. Sapal Tachakra and the whole North West London Hospitals trust fund, both for their valuable guidance and for their financial support.
Prof. Stephen Watts who embraced this project and believed at its potential.

1. Introduction

In recent years, there has been a rapid growth in the use of Wireless Local Area Networks (WLAN). They found their way into offices, campus, factories, airports, coffee shops and even hospitals, providing users with freedom of movement and allowing applications to operate in a mobile environment [Fig. 1.1]. One can safely assume that the trend our technological society is following, would dictate a transition from the wired to the wireless environment, as there is a profound need for mobility in our everyday applications.

1.1 Telemedical needs

The medical needs that influenced the creation of the Telemedical system described in this dissertation belong mainly within the sphere of **Telemedical videoconferencing**. An increasingly large number of videoconferencing systems are being used by the hospitals for a number of reasons, varying from Teleconsultation to Telesurgery. Up until today the way that any of these applications were performed was by either transferring the patient, often in a critical state, to a videoconferencing room where a number of heavy and large videoconferencing systems were installed, or transferring these machines into another part of the hospital; usually the A&E room. Both of these solutions came with a number of disadvantages:

- The equipment was usually very heavy and required the need for at least two persons to carry it.
- There were a large number of cables that had to be connected and run over a distance in the A&E ward. That makes the current systems both unpractical and potentially dangerous in a fast moving environment like the emergency ward.
- A considerable amount of time was needed to reset and reconnect the system; not to mention special communication lines (usually triple ISDN lines) had to be installed to the A&E rooms, as well.
- In the case that the patient was to be carried to the videoconferencing room, valuable time would be lost in that transfer; sometimes critical for the patient.

- The videoconferencing rooms were usually not properly suited for patient care but mostly for accommodating the communication needs of the videoconferencing system (there is usually lack of proper patient facilities, critical life support equipment and generally medical tools that are available in the treating sections of the hospital).
- Current videoconferencing systems usually rely on the use of Integrated Services Digital Network (ISDN) lines that have higher cost of ownership and relatively lower bandwidth in comparison with standard network lines (a triple ISDN line can support 3x128 Kbps=384 Kbps in comparison with a standard 100 Mbps network line).

Fig. 1.1 Wireless Telemedicine in use: drug subscription using a WLAN

Regardless of the above problems, the issue still remains: It is very often that a doctor treating a patient from the A&E ward would require the opinion and consultation of another doctor either within or outside the hospital. The way that the technology was utilised until now is far from satisfactory as it left space for errors, delays and accidents and could even be accused of neglecting the patient needs for fast and safe diagnosis.

1.2 Basic WLAN concepts

Wireless LANs came to bridge the gap of applications like those that are described above. However, they are not limited to that small sector of science [Fig. 1.2]

WLANs are much like any radio system like TV and radiophone. They utilise the airwaves to transmit and receive signals but unlike conventional radio waves, they

do so in a digital manner so binary information can flow between them while minimising the need for wired connections.

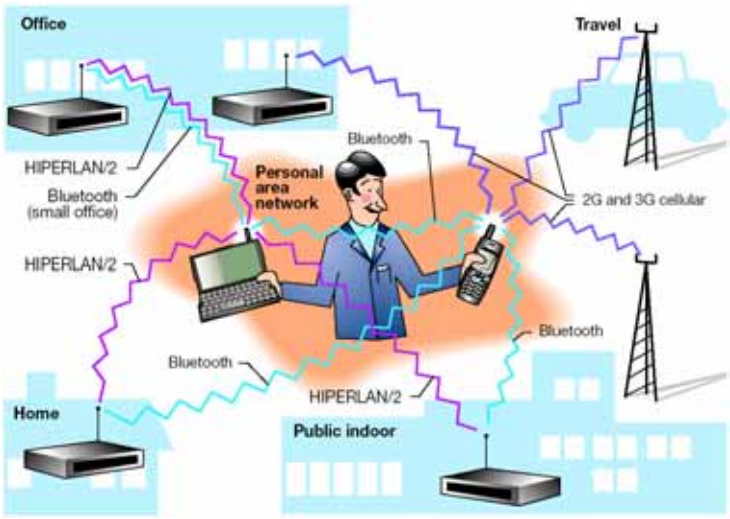


Fig. 1.2 A variety of WLAN architectures find increased acceptance in our every day life

WLANs have a number of properties that make them increasingly popular [Khu00]:

- Their range can cover an office space of about 100m radius and, depending on the product and the antennae used, can extend to a distance of 20 km.
- Their throughput, although smaller than that of the wired LANs, is between 11 and 54 Mbps and in some cases, has the additional support of Quality of Service (QoS).
- WLANs maintain interoperability with the existing wired structure as they only define the lower two layers of the ISO model and are transparent to the overall network.
- They allow for seamless handover between cells so the coverage area can be extended infinitely.
- They apply techniques that eliminate interference among them and reduce external noise within the wireless path.
- WLANs can be easily operated by non-specialised users but can also be efficiently maintained by network administrators (even in remote operation).
- They are secure enough and in critical applications, can become even more secure by incorporating specialised security patches on them.

- They have a low cost of ownership and an even lower cost of maintenance when compared to the wired LANs.
- Their topology can be user defined (change the backbone and architecture of the network).
- Finally, they have been proven to be safe (conforming to every safety rule) and interference free, especially in a sensitive environment like that of the hospitals.

A conclusion that can be drawn by reading the last two sections, is that the needs of specific Telemedical applications bind perfectly with the advantages and characteristics that WLANs have to offer.

1.3 Existing applications

Several pieces of substantial work related to the MedLAN project have been carried out, related both to the Telemedical and to the communicational part of it [Kyr02]:

- One of the first wireless Telemedical projects was developed by the **Johns Hopkins** hospital in 1999. The project was not designed to transfer real-time data and was using mostly store and forward methods to update patient records and issue drug prescriptions. Consequently, it was unable to transfer live video and audio for use in medical teleconference. The research included three different WLAN technologies with three different frequency ranges. Several Access Points (AP) were placed in a single hospital floor to give the ability to the treating personnel to roam between APs. The results were satisfactory and opened up the way for the use of WLANs within hospitals. [Lom97]
- Another project that started in Jan 2001 is **Mobi-Dev**: Mobile Devices for Home Care Applications. This project will provide clinical staff with portable devices (based on palm PCs) wirelessly connected to different information databases, able to perform real time data management. An Internet-based system is set up to exchange clinical data between the Mobi-Dev portable devices and various kinds of relevant information databases. The palm PC with microphone is integrated with a smart card reader, a Bluetooth and a UMTS transceiver [Inc03]. This project, although using wireless techniques, is limited both in bandwidth (about

one tenth of basic WLAN bandwidth) and in the variety of possible applications and does not include video transfer or videoconferencing.

- The National Technical University of Athens has developed two projects using wireless GSM networks: the **Ambulance** and **Emergency-112**. The aim of the Ambulance project was the development of a portable emergency telemedicine device that supports real-time transmission of critical biosignals as well as still images of the patients, using GSM links. EMERGENCY-112, an extension of the Ambulance project, aimed at developing an integrated portable medical device for Emergency Telemedicine. The system enables the transmission of critical biosignals (ECG, BP, HR, SpO_2, temperature) and still images of the patient, from the emergency site to an Emergency call centre; thus enabling physicians to direct pre-hospital care in a more efficient way, improving patients outcome and reducing mortality rates. The system was designed in order to operate over several communication links such as satellite, GSM, POTS and ISDN. In Emergency-112 emphasis was given on maximising the system's future potential application, through the utilisation of several communication links (both fixed and wireless), as well as through the increase of the overall system's usability, focusing on advanced user-interface and ergonomics. The Emergency-112 system has been used successfully since 1998 in three European Countries (Greece, Italy, and Cyprus). Nevertheless, as the above projects mainly use a slow GSM link (9.6kbps), it cannot incorporate video along its transmission nor can it support high resolution imaging. [Pav98a], [Pav98b]
- One other project of major importance is **Speedwave**. Manchester city has unveiled the first urban wireless network based on Bluetooth and wireless local area networking (WLAN) technology. The pilot network is designed to offer residents high-speed access to the Web and communications services as they go about the city. Initially, the network will be installed in hotels, restaurants, the Manchester Business School, and the University of Manchester. The wireless network will feature both Bluetooth and 802.11b technologies and will be expanded to serve the city council and 70 other sites. Users of wireless portable appliances will be able to connect to base stations from up to 100 meters. The service is offered on a pay-as-you-go basis. This kind of infrastructure is not designed specifically for telemedical application but can easily support the

roaming of systems like MedLAN well beyond the boundaries of the hospital and will permit for the consulting doctor to be anywhere while still having access to medical data. [Agn01]

- Finally, one of the projects closest to MedLAN, is a commercial application of a medical trolley that has the ability to transfer data over an ISDN link, the **Darby** trolley [Rco04]. Much like MedLAN, it is specifically designed for use in hospitals and clinics where there is a requirement for remote consultation or second opinion through wireless videoconferencing. However, its technical characteristics are inferior to those of MedLAN: it uses a slower wireless link (2Mbps) and requires ISDN lines to transfer the live stream into another hospital. It weights about 30-40 kg, it accepts no changes or improvements to its existing infrastructure and does not have the ability to send high-resolution still images.

On the communicational side of MedLAN, there has been much research mainly related to the wireless networks.

- The Institute of Electrical and Electronic Engineering (IEEE) has developed a work group, called 802.11. Several versions have been developed since then, that address different network properties: IEEE 802.11a, b, g, e, i, deal with speed, compatibility, combination of both, QoS and security respectively [IEEE99]. From these, undoubtedly the most well used around the world is the IEEE 802.11b offering a top speed of 11Mbps. This technology has already been incorporated in handheld computers, PDAs and even mobile phones.
- The European Telecommunication Standards Industry (ETSI) is the European equivalent of the IEEE. They have also developed a set of wireless transmission protocols called HiperLAN (HIgh PERformance LAN). With its two versions, HiperLAN/1 and HiperLAN/2, it competes with the IEEE protocols offering not only speeds in excess of 50Mbps but also procedures to differentiate and prioritise the traffic sent over the wireless link, in order to impose QoS rules onto the wireless network.

Each of the above architectures addresses a part, but not all of the needs that a wireless Telemedical system would have. As a paradigm, IEEE 802.11b works in a frequency range that is more desirable for an average office space while IEEE 802.11a offers a substantial increase of speed while sacrificing the available range of

the WLAN. On the other hand, as desirable as many of the HiperLAN/2 properties might sound, no such system is as yet commercially available to use.

1.4 Thesis objectives

The contents of this dissertation describe a two-fold application: a Telemedical and a Communicational application. In the Telemedical part, a mobile system would be described, dedicated for use within the Accidents and Emergency (A&E) wards of a hospital. The communication part will investigate novel ways for enhancing the operation of the above Telemedical system.

In general, the objectives of this dissertation are:

- To enhance the mobility of a videoconference system dedicated for Telemedical use.
- To add additional properties on that system that will make it desirable to the health care personnel.
- To investigate the security issues of such a system.
- To improve the communicational properties of such a system so this change will reflect a positive step in its Telemedical properties, too.
- To enhance the Quality of Service (QoS) parameters of that system.
- To create a user-friendly system that can be easily operated by any computing platform without the use of any specialised software.
- To do all the above in a manner that would be financially feasible and more affordable compared with the current trends and techniques.

1.5 Contribution to knowledge

This thesis makes several contributions to both the Telemedical and the communication science:

The MedLAN system itself is a novel system. Depending on the version, it either consists of a light mobile trolley (containing a laptop computer, a high quality video camera, a small hardware encoder and a WLAN card) or in a newer version it can be in a size that a doctor can carry in his / her pocket. Several alterations were made to

the above prototype including the replacement of the laptop computer with a PDA. As the project has already been completed, doctors in the A&E room can already use this system to wirelessly communicate with a consultant either within or outside the hospital.

Adjusting DICOM (Digital Imaging and Communications in Medicine) **specifications** to meet the requirements of wireless networks was also an original task. WLANs offer reduced bandwidth in comparison with wired LANs. Accordingly, still images have to be slightly compressed to fit efficiently into the wireless channel. This kind of compression eventually loses a small part of the original information. An extensive study of the validity of the output images was made using a number of images and videos. Finally, a clinical research was carried out with the collaboration of several consultants to determine if this method retains enough image quality to make a safe diagnosis.

Suggesting an alternative modulation to that of IEEE 802.11b for use in Telemedical applications. Orthogonal Frequency Division Multiplexing (OFDM) is proven to be more tolerant to multipath interference, often caused by the operation of WLANs in spaces with thick walls and reflecting surfaces. Old hospitals are the ideal terrain for examining this problem. By applying OFDM into the existing 802.11b modulation, the multipath noise was reduced and there was an increase of the available bandwidth. This allowed for lower compression levels in both still images and live video that in turn resulted in an increased diagnostic ability.

In the course of development of the MedLAN project, a number of other tasks were developed that were not original but novel in their application to Telemedical science:

A **complete model** was developed for the Central Middlesex Hospital (CMH) A&E and its connection to the surrounding hospitals belonging to the North West London Hospitals (NWLH) network. In there, the whole operation of the MedLAN system, the WLAN and its connection to the wired hospital network was simulated and research was made into the assumption that OFDM would perform better in these specific conditions.

Additionally the overall **security of a WLAN** system using the 802.11b protocol was investigated. Following recent concerns on the possible attacks that were made to the above WLAN protocol, a set of countermeasures were researched and

proposed, specifically designed for a Telemedical system. The data overhead of such techniques was also investigated as it reflects on the quality of medical information sent over the wireless channel.

1.6 Dissertation structure

The remainder of this dissertation is organised as follows:

Chapter 2 introduces Telemedicine as a science and separates it from its variations (Telehealth, Telemonitoring, Telesurgury, etc). Then, it describes a modern Telemedical system like MedLAN, explaining basic issues like videoconference, compression, communications lines, etc. It concludes with an overview of the legal and ethical dilemmas that such a project may pose to both the health care personnel and to the engineers involved in developing such an application.

Chapter 3 is an overview of the basic WLAN technology and includes the major IEEE and ETSI protocols. There, the most well known WLAN architectures are presented along with an investigation of the impact they have on the last two ISO layers (physical and data-link). Issues like topology, signal encoding, Medium Access Control (MAC), services, range, interference and security are being presented along with some of the most well known problems that WLANs have.

Chapter 4 and onwards is the contribution of this thesis to Telemedicine. In **Chapter 4** there is a complete presentation of the MedLAN system and its capabilities. It describes the contents of the mobile trolley, the way that the system is working, the outputs it produces and the general performance of the system. It also describes how symbiotic the system is with existing medical instruments, especially those found in A&E wards.

Chapter 5 investigates the concept of compressing still images and live video to reduce the bandwidth and enable a more efficient transmission of these data through a wireless link. This is an alternative to the recommendations of the DICOM organisation that usually calls for uncompressed data. An extensive library of various medical images, sounds and video has been processed and the results are analysed and evaluated by a number of consultants.

Chapter 6 introduces OFDM modulation and the possible advantages that this may have on reducing multipath interference. It then suggests that Telemedical

applications could benefit by using OFDM as an alternative modulation. This notion is supported by means of simulation using three different simulation packages that eventually model the complete ISO 7-layer model of the system. The results are compared to those using the original 802.11b modulation to show that the proposal is beneficiary for certain kinds of applications.

Chapter 7 begins by outlining the security procedures involved in WLANs today. It summarises Wired Equivalent Protocol (WEP) and addresses the current concerns about its safety. It suggests a series of countermeasures that a Telemedical system might take to ensure privacy and confidentiality, emphasising the use of security protocols like IPSec as a means to achieve the above. It concludes by measuring the overhead that such action might impose on the bandwidth and therefore on the output quality of a Telemedical system.

Finally, **Chapter 8** concludes with the main contribution of this thesis and describes some possible future research directions.

2. Applications of Telemedicine

2.1 Definition of Telemedicine

It is always useful to clarify the boundaries of the term “telemedical” science especially as over the years, the meaning of the term has changed and keeps on changing.

The first part of the word “Tele-medicine” derives from the Greek word “tele” that means “at a distance”. An easy way of defining Telemedicine, would be to consider it as “medicine delivered at a distance”. However, since the “tele” implies at least the existence of a telecommunication path (often being a digital one) and considers medicine at its broader sense, we can perceive Telemedicine to be a science that “utilises information and telecommunication technology to deliver medical information for diagnosis, therapy and education” [Nor02]. A term very closely related to Telemedicine is “telecare”. Telecare utilises information and communication technologies to transfer medical information for the diagnosis and therapy of patients in their place of domicile. It is especially important for a specific group of patients with long-term chronic conditions such as mental illness, disability or simply old age, which reduce their freedom of movement [Ist01b].

2.2 Divisions of Telemedicine and Telecare

The scope and categorisation of Telemedicine and Telecare is in constant change. Presently we can distinguish four main categories depending on their features [Nor02]:

2.2.1 Teleconsultation

Since the medical consultation is one of the most important factors in clinical practice, it is obvious that Telecosultation would be the most frequent example of Telemedicine. Studies have shown that Teleconsultation accounts for 35% of the

usage of telemedical networks [ATA02]. Teleconsultation also represents the application area for projects like MedLAN as the basic task that it achieves is the communication between a doctor in the A&E ward and a consultant residing somewhere else [Ban02a].

A teleconsultation can take place between two or more health care personnel or between them and a patient. It can extend from a distance as small as different rooms in the same hospital, up to running a telemedical link between different countries. It can also use a variety of communication media; from a simple telephone line to a satellite video link.

The most frequent case of Teleconsultation is a video link between a patient and his or her doctor [Fig. 2.1]. By default, this link is based on a real-time communication channel as opposed to store-and-forward techniques that usually deal with still images (x-rays, etc).

Fig. 2.1 Videoconferencing is the most commonly used application of Teleconsultation. Above, a doctor is consulting a specialist using a telemedical link [Sha03]

In the process of running a teleconsultation link, the following procedures have been suggested in order to maximise the benefits of this procedure [Tac99]

- Agree on the purpose of the teleconsultation. For example, is the session to be used to diagnose a condition, to monitor the progress of treatment or to develop the skills of healthcare workers?
- Establish the process and content of the teleconsultation. Whatever its main purpose, the consultation should focus in a natural and continuous way on the relevant healthcare issues. It should avoid irrelevancies and discontinuities as well as distractions such as the need to adjust technology settings.
- To achieve the above, one must ensure practitioners are trained in the use of equipment.
- Formalise the delegation of clinical responsibilities. A doctor who participates in a teleconsultation must be satisfied that any healthcare worker who accompanies the patient at the other end of the link, can carry out any medical procedures that are needed.
- Decide on documentation. All healthcare professionals involved in the teleconsultation should document the procedure and the outcomes and make sure that a suitable note is made in the patient's medical record.

2.2.2 Tele-education

With the term tele-education we refer to the use of telemedical links to deliver educational material. Depending on the recipient of this information, we can distinguish the following tele-educational categories:

- Clinical education using Teleconsultation: whenever there is a Teleconsultation link between a health care worker and a consultant, there is always an opportunity for education to occur. In a conventional scenario, the non-expert person is at close vicinity to the patient, with the consultant being at the other end of the communication link. This presents the non-expert with several opportunities: to help the patient to articulate and interpret his or her symptoms, to enhance his diagnostic abilities by observing the expert at work, and have hands-on experience especially if the non-expert is at the early stages of practice. In general, this triangle (non-expert, patient, consultant) offers an opportunity for education that is not normally presented in the classical referral process (patient, GP).

- Clinical education using the Internet: healthcare workers can obviously update and extend their knowledge and medical skills using sources from the Internet. Clinicians have specialised access to some excellent web and other online resources, which are ideal for this purpose. Examples include national sites such as the UK's National Electronic Library for Health (NELH) [NEL04] and the USA's National Library of Medicine (NLM) [NLM04]. There are also specialised databases or literature searching tools such as MEDLINE to retrieve evidence-based information from which to enhance self-skills and improve the treatment of patients.
- Academic study via the Internet: tele-education also deals with the support of distance learning courses that lead to recognised qualifications. These courses are usually at a postgraduate level and are made by doctors for doctors. Some examples include EuroTransMed (ETM) [Rao99] and IT-EDUCTRA [Has97], [Man97] [Fig. 2.2]

Fig. 2.2 Using telemedical links to enhance education of healthcare personnel

- Public Education via Telemedicine: this implies the education of the community at large, about matters of public health. Examples include issues of diet, exercise and hygiene, and information on specific diseases and conditions, such as cancer or diabetes. The information can be presented in a controlled way to a target audience via a kiosk in a shopping mall, health centre or home or can even be accessed by anyone using the web.

2.2.3 Telemonitoring

Telemonitoring is the procedure when telecommunications links are used to repeatedly collect data about a patient's condition. This procedure of data accumulation can be either manual (every given interval a care taker gathers data from the patient's charts and sends them into a collection point for evaluation using

phone, fax or a computer) or it can be entirely automatic (machines will send these data in a predefined time using either real time or store-and-forward processes).
In most of the cases, the purpose of Telemonitoring is to decide if an adjustment is needed in the patient's treatment. This adjustment can be implemented either by manual means (like instruct either the patient or the caregiver to take an action), or in a more automatic way, by the treating doctor remotely controlling medical instruments on a two-way communication system. Perfect examples of Telemonitoring home-based patients are the monitoring of hypertension [Fig. 2.3] [Fri96] and diabetes [Ahr92], [Goy95].

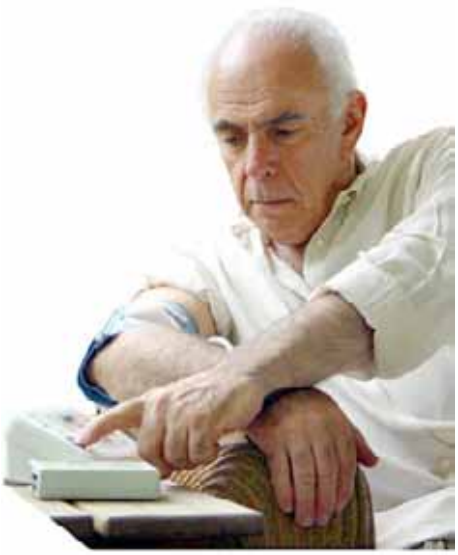


Fig. 2.3 A patient suffering from hypertension is using a digital device
to forward his daily readouts to his treating GP

2.2.4 Telesurgery

Compared to the above, Telesurgery is a relatively newer application. It can be applied in the following ways:

- By having Telemonitoring as the basis, a doctor can enjoy the assistance of a specialist that views the operation from a distance (audio and video) using a telemedical link. The above notion also promotes Tele-education.
- By a specialist controlling a robotic arm and actually performing a surgical operation from a remote place. In this case, other medical personnel are in the actual place of the operation, to assist the remote surgeon. Because of the delicate operations required for such an action, it is not uncommon to scale down

the movements of the robot in order to avoid hand tremor and increase accuracy. [Fig. 2.4]. However, and in the case that a satellite link is to be used, one of the fundamental problems of Telesurgery is the delay introduced by the signal bouncing back from the satellite, that can vary from half a second to more than one second [Moo02]

Fig. 2.4 A specialist performs remote surgery by controlling a robotic arm

2.3 Advantages and limitations of Telemedicine

It is obvious by reading the previous sub-chapter that Telemedicine in general can offer us with a number of advantages. Below is a list of some of them [Nor02]:

- Better access to healthcare: extending the healthcare to disadvantaged communities that would have problematic access to hospitals or doctors [Elf97], [Mit98]. In that sense, more convenient methods of health care delivery can be implemented to both the doctor and the patient: the patient avoids unnecessary journeys and the doctor saves time in between consultations.
- Access to better healthcare: in comparison with the conventional methods of treatment, using Telemedicine can offer the patient with the opportunity of consulting a specialist, as opposed to his or her personal GP [Got95].
- Improved communication between carers: with the transition to digital information exchange the healthcare staff can benefit by more accurate, more complete and faster access to patients information [Hje99]

- Healthcare personnel continuing education: an easy access to increasingly bigger information databases assists the carers to continue their education and to have experience in subjects that would have been next to impossible in the past.
- Better access to information: patients can enjoy better access to information while taking advantage of home-based telemedical advances. These include downloading information from the Internet or uploading personal data to specific databases.
- Better resource usage: it is uneconomical to have the same information stored in several places. It makes much more sense to set up the minimum number of resource sites and make them available through telemedical links.
- Reduced cost: cost has always been one of the fundamental drivers of Telemedicine and the right use of the technology can reduce the health care cost considerably. Clear cost savings have been demonstrated to modalities like teleradiology, which have been around long enough to permit the extraction of such conclusions [Bal99]

Unfortunately, nothing good comes without some negative aspects. Telemedicine can have the following repercussions:

- Poor patient-carer relationships: there might be a breakdown of communication between the patient and the carer, especially if there are concerns of confidentiality from the patient's side [Hje99], [Col96]. This will be discussed at a later stage within this chapter.
- Poor relationships between healthcare staff: telemedicine can be a threat to the conventional ways that some carers have been used to. It can also be a potential drawback when an over-enthusiastic party will try to convince a more conservative co-worker.
- Impersonal technology: some patients (mostly elderly) will fear the technology itself. That can lead to the patient feeling uneasy and can jeopardise the validity of the examination.
- Organisational disruption: the adoption of new technologies can lead to some disruption on the normal working pattern that might consume some extra time from the carers, especially in the implementation period as then, there is a profound need for education into the new technologies [Yel99], [WGA98]

- Potential low rates of utilisation: there is always the risk of installing a telemedical system in much enthusiasm and then leaving it unused. On the opposite side, there is also the risk of a telemedical link becoming so popular that the staff will overuse and render it obsolete.

2.4 Ethical and legal aspects

Telemedicine still has many barriers to overcome until it can be satisfactorily utilised within the healthcare system. Some of these include the optimum usage of telecommunication infrastructure standards, (described later on in this chapter), the cost effectiveness of the telemedical systems and the compliance with the national policy and strategy. Finally, yet most importantly, it has to overcome some ethical and legal dilemmas.

2.4.1 Confidentiality and patients expectations

The basic principle behind the term “confidentiality” is that the patient’s information should remain confidential, if upon the release of such information, there is the potential danger of harming a person either physically or emotionally. This concept dates back to Hippocrates and applies regardless to if a contract or any other formal relationship exists between a doctor and a patient [BMA93]. The current thinking in medical record keeping is that the healthcare organisation “owns” the physical form of the information (e.g. an x-ray film) but the patient “owns” the information contained in it. In summary, the following three rules describe the patient’s expectations regarding medical confidentiality [AMA96]:

- There is a basic right of patients to privacy of their medical information.
- Patient’s privacy should be respected unless waived in a meaningful way, or when it will counter the public interest.
- The information that is kept should be limited only to the portion needed to fulfil the specific purpose.

It is obvious that the concept of confidentiality is at the core of the patient-doctor relationship: patients who reveal information to their doctors must be sure that no information will leak to others, either intentionally or even incidentally [Tac96]. This “incidental” disclosure of information is a fundamental issue when dealing with

projects like MedLAN, as this assumes the transmission of information through a WLAN link. However, the techniques to overcome this problem will be discussed in a later chapter.

2.4.2 Data Protection Act

In order to form a legal framework and regulate any possible misuse of information, the UK government formed a list of "rules" concerning the safekeeping and exchange of personal information; the Data Protection Act. Initially activated in 1984 it required the registration of individuals and organisations (including the NHS Trusts) that hold personal information in digital form and introduced criminal penalties to those not obeying these rules. By its revision in 1998, the Data Protection Act, among other things, becomes more specific in its concepts, includes manual keeping of records and strengthens the rights of individuals even more. In essence, there are eight fundamental rules included in the original Act:

1. *The information to be contained in personal data shall be obtained, and personal data shall be processed fairly and lawfully.*
2. *Personal data shall be held only for one or more specified and lawful purposes.*
3. *Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.*
4. *Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.*
5. *Personal data shall be accurate and where necessary kept up to date.*
6. *Personal data held for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.*
7. *An individual shall be entitled: (a). At reasonable intervals and without undue delay or expense: To be informed by any data user whether he holds personal data of which that individual is a subject; and access to any such data held by the data user; and (b). where appropriate, to have such data corrected or erased.*
8. *Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data.*

When applied to the healthcare sector, principle 3 describes the patient's expectations.

2.4.3 Common problems and risks

One can distinguish the problems that arise from the use of telemedical equipment, in two major categories: problems that are caused due to the technology itself and problems due to the personnel involved [Nor02]. For the former, we can consider technology risks like:

- Quality of images: of major issue is the amount of difference (often expressed as noise) that a still image can suffer before producing unacceptable clinical results. This implies that a set of rules must exist for images used in radiology, pathology, dermatology, etc to ensure the levels of "change" this image can undergo through when transmitted over a telemedical link. This will be dealt with in detail in a future chapter.
- Lack of proper equipment: describes the absence of suitable tools to effectively practice Telemedicine and includes worn-out or incompatible devices, lack of servicing, poor documentation, etc
- Malfunctioning equipment: when telemedical equipment suffers some form of breakdown or is poorly connected and configured.
- Inadequate guidelines: this refers to both the procedures and protocols that govern a telemedical session and to the documentations applied by the engineer developing the telemedical application.

For the case of operational risks due to personnel, we can consider:

- Poor verbal communication: what makes problematic audio and video transmission even worse is the human factor due to the personal nature of the personnel involved. This includes native language, dialect, accent and even factors like age and culture.
- Limited ability: medical personnel that are under-qualified or even unqualified, is a source of errors for practicing Telemedicine [Vin88]
- Poor training: the training of consultants used in telemedical scenarios is crucial. It is inconceivable that in today's fast evolving world, some medical personnel are only educated in the clinical aspects of the treatment and do not undergo training in the effective use of technology.

- Improper delegation: the delegation of responsibility to personnel with either less qualifications or personnel belonging to sciences different than those of the healthcare sector, is often a source of medical malpractice. That often includes the use of engineers to develop a telemedical project (much like MedLAN). In contrast with medical personnel, an engineer is not governed by the same rules for confidentiality.
- Unclear responsibility: the fact that a telemedical link often requires the involvement of a greater number of people (sometimes changing in the process) often leads to an unclear responsibility when an error occurs.

2.4.4. Engineering concerns

In view of the above concerns on the ethical and legal aspects of Telemedicine, there are a number of responsibilities that rely on the engineer developing the telemedical application. Apart from the ones related to the technical risks of the equipment involved (discussed in the previous section), there are always security concerns involved, if a telemedical system is to be used without reservations. A security policy has to be created by answering the following questions [Nor02], [Owe01]

- How sensitive are the data we wish to protect? Are we dealing with a crucial piece of medical information or mostly with demographic data?
- What are the consequences of a breach of security? Is it likely that this will result in an unpleasant situation for the patient, or harm them severely, either physically or emotionally?
- Who are the authorised users of the telemedical system? There has to be a list of authorised personnel restricting the use of the system through a set of usernames, passwords and other security measures.
- How vulnerable is the data? Is it likely to be intercepted easily (unprotected data over a WLAN link) or are they well secured on their own (data through a Virtual Private Network)?
- What are the technical issues that will govern the safe exchange of data? Is it likely that the additional cost of security will overcome the benefit of the system?
- Do we wish to eliminate, minimise or reduce the threat of unauthorised access? Not all telemedical applications need the same level of security. For

example, an exchange of medical ideas through a tele-educational link needs much less security than a delicate tele-surgery procedure [Owe01]

- How do we balance the needs of authorised users with the constraints imposed by security? This becomes an even bigger issue in projects like MedLAN created for use in fast moving environments like the A&E wards, when even a portion of time required for the proper authentication of a user, can be proven fatal to a patient.

2.4.5 NHS principles

In the United Kingdom, the above engineering considerations gave rise to an extended discussion between the NHS and the British Medical Association. That led to a review of the existing NHSnet structure. The improved network promised a more effective access of medical information to all interested parties with emphasis on security. This approach initiated a “code of connection”; rules that organisations should obey if they wished to have access to the NHSnet [NHS95]. The basic rules were:

- Access of the network is being protected by at least one level of authentication (like username / password).
- Controls are placed between non-NHS organisations wishing to access the NHSnet.
- A specific person is made responsible for the security of a specific connecting point.
- Both the engineering and the healthcare staff are made aware of their responsibilities.
- Physical access to the NHS network equipment (routers, HUBs, wall plugs) is controlled.
- Any misuse of the system or any security breach is reported and dealt with.

The above rules soon found their place as a standard to any internal NHS network access. However, as the NHSnet was designed long before the Internet revolution, these rules imposed a handicap to future developments. Newer techniques had to be set to allow more people (often non-specialists individuals like patients) to be able to have access to the new telemedical trends. Diabetic patients needed to fill in their data into their record, overweight people were looking for advice through custom-

made NHS web pages and engineers needed to experiment using NHSnet to develop new medical applications.

The above scenarios indicated the need for a specialised tool, controlling the access to the NHSnet through the Internet. Such a tool is called a “firewall”. A firewall acts like a filter allowing legitimate access through the Internet while blocking (and reporting) unwanted traffic. There are two kinds of firewalls: a network-level firewall, resides on a router and makes decisions on which traffic should pass and which should not, based on the IP (Internet Protocol) address of the computer requesting the traffic. An application–level firewall is a piece of software running on a PC and controlling two ports; an input and an output. It works by allowing outside users to access specific pages inside the network (like web pages) while blocking any other outside-to-inside activity of unauthorised users.

Along with the need for controlled access, NHSnet had to facilitate the need for secure telemedical transactions by encrypting the transmitted data in such a way that they would be meaningless to an intruder. Moreover, they had to ensure that the data transmitted from both ends would belong to the alleged users and not any third party. The former concept describes the use of encryption and cryptography, while the latter deals with the use of authentication through digital signatures.

One of the fundamental future applications of MedLAN is allowing the consultant to communicate through videoconference, with the A&E ward, while being on the move outside the hospital and, possibly, using a WLAN deployed by an independent service provider. It is within these kinds of scenarios that the above rules had to be fulfilled, so the consultant can penetrate through the NHSnet and its firewall and authenticate him or herself as a legitimate user. However, this also will be described in detail in a later chapter.

2.5 Structure of a telemedical system

After separating Telemedicine in its divisions and examining some basic telemedical issues like ethics, confidentiality and security, the most important factor to consider (and definitely the one that the developing engineer is mostly concerned about) is the actual structure of the telemedical system and the properties of its components.

Before describing the alternative telemedical structures, it would be useful to understand that since not all systems have the need for the same type of telemedical data, not all systems would have the same requirements. In essence, there are four major categories of telemedical data: text, sound, still images and video. Each of those utilise the communication line differently and have different requirements for Quality of Service. In summary:

Type of data	Example	Typical file size
Text	Patient record	1-5 KB
Audio	Heartbeat through an electronic stethoscope	2-4 KB/sec
Still image	x-ray, MRI, US, etc	500KB-2MB
Real time video	Ultrasound, videoconferencing	200KB-1MB/sec

Table 2.1 Examples of telemedical data with their typical sizes

Following, is a summary of the basic characteristics of each of the above four types of data.

2.5.1 Text

There are two ways of storing text information in an electronic patient record. The first is by directly entering the text in digital form into a PC (typing the data) and storing it in a central system for retrieval. The second is by scanning a hand-written text and storing it as an image. As the later has the disadvantage of not creating editable text, there is the option of converting the hand-written text into data through an OCR (Optical Character Recognition) program. Unfortunately, these programs have a relatively low rate of success converting handwritten text, especially when the text is badly written. The first option usually occupies 0.5-2KB while the image of the handwritten text occupies about 50-200KB

2.5.2 Audio

Apart from the obvious use of the telephone network to facilitate a conference between two doctors, there is always the need for transmitting audio signals (other than speech) to a remote destination, through a telemedical link.

In the case of speech, the voice is travelling through the PSTN (Public Switch Telephone Network) in an all-analogue form. The limitations of the telephone

network are imposed on both the frequency range and in the overall sound quality of the audio transmission.

However, newer trends require newer techniques for transmission. An electronic stethoscope for example, is capable of transmitting heart and lung murmurs over a Plain Old Telephone System (POTS). The disadvantage of that method is that depending on the distance and the intermediate links of the phone call, the sound can be so degraded that it would be rendered obsolete.

The solution for the above problem is to convert the analogue data into a digital data stream and send it in an error-free manner so it can be received, stored and reproduced without losing any of its original information. This is done by sampling the amplitude of the analogue signal in small time intervals and finally digitising it into a discrete form. The smaller these time intervals are, the more accurate the digital output is, in respect to the original analogue signal. Obviously, regardless of how small the intervals are, there will always be a small difference between the analogue and the digital signal. This is called a “quantisation noise” and is perceived by the human ear as a “metallic” variation of the original sound. A sampling “resolution” of 16 bits (creating 2^{16}=65536 different amplitude levels) and a sampling rate of 44kHz is considered sufficient to avoid distortion and to perfectly reproduce frequencies ranging from 0 to 22kHz (half of the sampling rate) [Nyq28]. As the human ear can generally hear the sound range 20Hz-20kHz, the above settings are considered more than enough. The above are also the settings that the music industry uses to record music on CDs. However, this produces the need for 44000 x 16=704000 kbits=85.9KB/sec available bandwidth, that in an average situation is much more than what a PSTN line can offer. This leads to two alternatives: either use lower sampling frequency and resolution, or compress the audio signal. As compression will be presented in a more analytical way later, it is just worth mentioning that one of the most commonly used techniques for converting and transmitting digital sound over low data rate lines is the International Telecommunication Union (ITU) G.723.1

2.5.3 Still images

Still images represent the majority of the telemedical uses. They extend from simple x-rays to Magnetic Resonance Imaging (MRI) and from still Ultrasound (US) to

Computed Tomography (CT). Their quality is initially defined by their resolution and their colour “depth”. Resolution is the number of pixels than can fit in a given area (e.g. an inch) and is measured as dots per inch (dpi). The more dots per inch, the better the result. A typical scanner can scan a still image at 600-1200 dpi. However, this produces a very large output file, so less resolution is usually used.

If we perceive the still image file as a two-dimension table with pixels, a third dimension could be added to the table to represent the colour (depth). By having eight bits per pixel to describe that dimension, we can create 2^8=256 alternative colours. Usually, a “colour depth” of 16 or 24 bits is proven more than efficient for still medical images. As grey-scale images, like x-rays, have no need for colour information, they are mostly limited to 2^8=256 shades of grey.

The American College of Radiologists (ACR) has contributed to the definition of a set of rules that will be explained further in a later chapter. The Digital Imaging and Communication in Medicine (DICOM) set of standards define a framework of interconnection between medical devices. Although DICOM is merely a set of suggestions, many hardware manufacturers conform to these proposals.

As an example of still images, ACR’s DICOM calls for two categories of teleradiology images: a small matrix (low resolution) images with 500 x 500 pixels and 8 bit colour depth and a large matrix (high resolution) with 2000 x 2000 pixels and 12 bits colour depth. The former generates usually a file size of about 200KB while the latter takes more than 4MB. If the whole 24 bits of colour information were to be used, the same file would exceed 12MB.

Finally, it is worth mentioning that apart from using specialised scanners in order to digitise still images, there is also the option of directly capturing the image (film or paper) through a digital camera. Although not as precise as the scanner solution, the digital camera is very fast, handy and easy to use. This method of capturing stills is used by the MedLAN system.

2.5.4 Video

The benchmark for measuring the quality of a telemedical videoconferencing system is usually in relation to television broadcasting. While PAL, the predominant European standard, calls for a vertical resolution of 625 lines and 25 frames per second (fps) the output of a videoconferencing system is usually lower than that.

However, through special techniques (like compression or transmitting only that part of the image that has changed since the last frame) it can be improved considerably so the human eye can assume that it is viewing a television.

The usual resolutions that a typical videoconferencing system has, is 260 x 144 pixels, 320 x 200 or even higher. The frame rate varies from 5 to 25 fps. Both resolution and frame rate are heavily dependant on the amount of available bandwidth. The higher the bandwidth, the more data can fit within the given channel and so, the more pixels, colours and frames can travel at a given time. A PSTN connection is usually deemed poor to handle that kind of traffic while a triple ISDN (3 x 128=384 Kbps) is considered the standard for today's videoconference. A dedicated T line (1 to 2 Mbps) produces even better results.

2.5.5 Image compression

As the number of medical applications that require the use of computer imaging increases, so does the required storage space (and thus the bandwidth demand for transferring a file within a network) for these applications. Increased complexity high-efficiency algorithms have been developed to compress the data before they are stored or transferred.

When applied in still imaging, these algorithms are divided into lossless (a procedure that after decompression, regenerates the exact same image as the original) and lossy (a procedure that loses some part of the original quality but achieves a much better compression). The first scheme uses techniques that try to find similarities within the image and pack them together in order to save space (thus transfer time). The second works in the same way but it extends its operation onto creating similarities when the image components are so close, that the difference would not be visible to the end-viewer. The user is able to adjust this "forcing" of similarities [Ban03]. The most well used compression technique that uses the above scheme, was proposed by the Joint Pictures Expert Group (JPEG).

Doctors tend to agree that a lossless compression is more suitable for medical image interchange as it retains all its original quality and makes diagnosis more accurate. This is generally true if an extremely large storage space is offered, coupled with a very large bandwidth. Some would even argue that grouping very similar image components may result in reducing the "grain-of-rice" noise effect (when the

elements that make up an image on a film, are particularly visible to the viewer. This granular effect can be usually seen in photographs when using a fast film). [Tob02], [Ban03]

When dealing with video, one can imagine that the storage / transmission problem is multiplied by the frame rate. For European PAL system it has to have 720 x 570 pixels with a 24 bit colour depth, 25 times per second (fps). For a 90 minutes movie, this translates into: 720 x 570 x 24 x 25 x 60 x 90 = 1329696000000 bits (approximately 1.2TB). Luckily, compression algorithms for video applications have been developed, that can reduce this amount considerably. These algorithms, created by the Moving Pictures Expert Group (MPEG) rely too, on aggressively creating similarities on the image. However, and in newer version of this MPEG algorithm, the preceeding and succeeding frames of the video are taken into account to create an inter-frame compression and result into reducing the size of the file into as much as 200 times while still perceived as “perfect” to the eye of the observer. One can think of the MPEG codec (coder-decoder) as a combination of a sequence of JPEGs running along an audio stream.

Below is a table summarising some typical compression ratios for telemedical applications [Del99]

	Image size	**Uncompressed (MB)**	**Compressed (KB)**	**Compression ratio**
x-ray	2000 x 2000 x 12	5.7	285	20:1
Pathology (microscope)	800 x 600 x 24	1.44	96	15:1
Dermatology	1280 x 1024 x 24	3.9	980	4:1
CT (20 images)	256 x 256 x 8	1.3	650	2:1

Table 2.2 Typical medical modalities in original and compressed form

As the use of video compression increased, several videoconferencing algorithms (codecs) were developed (mainly by ITU). H.320, H.323, H.324, H.261 and H.263 being some of them. The last one, H.263, is the codec used by the MedLAN system. It combines high compression based on an MPEG-4 codec and is versatile enough to be used in a variety of communication lines, from PSTN to T lines.

2.5.6 Communication lines

Regardless of the telemedical data to be transferred through the communication link, the link itself always deserves serious consideration. As mentioned above, if the link can accommodate a large enough amount of data, less compression is needed and the data suffer less distortion. Unfortunately, bandwidth is an expensive commodity. The developing engineer has to balance these two factors and produce the best result with the available means.

Below is a list of the most well known communication lines along with their major characteristics:

- PSTN lines present the standard medium for communication through POTS. With a minimum amount of monthly rental, they can operate in a maximum speed of 56Kbps (with an actual speed of 44-50 Kbps) for download and 33.6Kbps for upload (V.90 protocol). The use of modems involve the conversion of a digital stream into an analogue form, in order to pass through the analogue line. Newer protocols (V.92) allow for an increase of upload speed to about 40Kbps. Although good for everyday slow Internet access, PSTN lines are not suitable for telemedical applications as the speed for uploading video is limited to 33.6Kbps
- Until today, ISDN lines dominated the videoconferencing world and were extensively used in telemedical applications. They come in forms of Basic Rate (BR) having 2 x 64Kbps=128 Kbps channel, or Primary Rate (using 30 x 64Kbps channels in Europe) having a total bandwidth of about 2Mbps. In their basic rate they are relatively cheap to rent and they can guarantee the available bandwidth that they advertise. This is the main reason that a triple ISDN (3 x 128=384 Kbps) were chosen as a standard for videoconferencing. Newer developments involve the use of Broadband ISDNs (B-ISDN) to facilitate the transmission of bandwidth demanding applications like live video, high quality audio, etc. This, however, is done with the use of fibre optics.
- Asymmetric Digital Subscriber Lines (ADSL) is one of many threads of the DSL family lines. Using the same PSTN copper lines and more advanced modulation techniques like OFDM, they manage to dramatically increase the bandwidth offered to the end user from 56Kbps to 512-2048Kbps for

download and 384-1024 Kbps for upload. The only disadvantage is the fact that their bandwidth is dictated by the distance the end-user has from the private branch exchange (PBX); the greater the distance, the lower the bandwidth. DSL lines offer an excellent cost-to-performance ratio and are setting the status for Small Office – Home Office (SOHO) use. This technology is the best choice for doctor's or patient's home, when connected to a central point, (like a hospital) in order to run telemedical applications.

- Satellite communications are becoming increasingly popular. They offer a link between source and destination with fewer intermediate providers, thus minimising delays and bandwidth limitations. However, as in its popular form the satellite connection is usually one-way (download), it requires the co-existence of at least one other communication form (PSTN, ISDN, etc) to upload data. Their major disadvantages are both the cost of installation (satellite dishes and decoders have to be installed) and their running cost. However, their use in certain circumstances (like marine telemedicine) is de-facto.
- Leased lines have always been the standard form of connection for bigger enterprises, including hospitals. They have a wide variation of available bandwidth, ranging from 64Kbps to 50Mbps and constant operation that makes them the tool of choice for Internet Service Providers (ISP). Their cost of ownership, however, is high enough to render them uneconomical if not utilised properly. In the case of the healthcare sector, this is usually the way that hospitals are connected together.
- Wireless connections are becoming increasingly popular as they combine high bandwidth, low cost of ownership, installation flexibility and, most of all, mobility for the end users. They operate in the unlicensed ISM bands (2.4GHz and 5 GHz in Europe) and can reach speeds in excess of 50Mbps depending on the protocol and modulation used. Two major technologies dominate the market: IEEE 802.11 for the US and HiperLAN for Europe. Wireless technologies and their applications in Telemedicine will be examined in more detail in the next chapters.

- Several other communication lines exist with various other properties: high-speed microwave links, ATM, DSVD, etc. The table below summarises the above technologies [Fal99]

Communication line	Bandwidth	Characteristics
PSTN	56 Kbps	Cheap, ubiquitous, slow, not suitable for high resolution
ISDN (BRI)	128 Kbps	Cheap, flexible, slow
ISDN (PRI)	< 2Mbps	Fast, high quality, expensive
Satellite	< 2Mbps	High quality, remote access, need for extra line, expensive
Wireless	2-24 Mbps	Convenience, free movement, unclear standards
Microwave	< 20Mbps	Good quality, inexpensive to run, expensive to install, line of sight only, short distances
Leased lines	64Kbps – 50Mbps	Reliable, expensive, inflexible
ATM, DSVD	155Mbps	High bandwidth, expensive
ADSL	384Kbps-4Mpbs	High bandwidth, dependence on user distance

Table 2.3 Communication line options for telemedical uses

2.6 Summary and conclusions

During the previous chapter it was mentioned that this thesis described a two fold project: telemedical and communicational. Within chapter 2, some basic concepts of Telemedicine have been presented: it began with the definition and the divisions of Telemedicine, and continued by presenting some obvious advantages and limitations of that science. It then moved on to describe the ethical and legal maters that both healthcare personnel and developing engineers should consider when designing and using a telemedical system. Finally, there was a presentation of some basic structures and procedures that a telemedical system might use when dealing with a variety of modalities and concluded with a list of communication lines used in telemedical scenarios [Ist01a]

In all the above, emphasis was given to the specific properties and techniques that the MedLAN system uses, along with their obvious advantages: telemedical

videoconferencing, wireless access, mobility and security to overcome ethical and legal dilemmas.

In the following chapter, there will be a similar presentation of basic wireless LAN properties, with emphasis on the specific technologies used by the MedLAN system.

3. Wireless LANs

3.1 Introduction

In just the past few years, wireless networks have come to play an increasingly important role in the LAN market. Organisations found that wireless infrastructures are much more convenient and dynamic and can satisfy the needs for mobility, relocation, wide coverage and restructuring, much better than wired networks [Sta01]. Consequently, the field of wireless communication is one of the fastest growing sectors of the telecommunication industry.

When trying to grasp the meaning of this "wireless revolution" it is a common misconception to separate "wireless" and "radio" networks into two different categories. From 1896, when Marconi invented the wireless telegraph, until 3rd generation mobile phones (3G), there are fundamental issues that remain the same: radio or wireless systems utilise electromagnetic waves to transmit or receive signals over a distance. Conclusively, apart from "wireless" usually addressing digital data transmission and "radio" more often referring to analogue transmission, there is not much difference between these two terms.

3.2 Wireless evolution

From 1946, when the first mobile telephone was introduced, there were many attempts to improve the services of mobile networks and increase their efficiency, mostly in the areas of telephony. Listed below, is a short timeline of the most important of these stages [Sta01]:

- In 1946, Mobile Telephone System (MTS) was established in 25 cities in the US. It was a uni-directional communication system that utilised a high-power transmitter and due to its volume was usually mounted in vehicles. The communication had to be established manually through telephone operators. As an enhancement, Improved MTS (IMTS) started operating in the late 60s

offering full-duplex communication while eliminating the need for operators. It was clear, however, that the spectrum efficiency of that system was very low: it could accommodate a finite number of users per base station (23) and could not extend its coverage by reusing the same frequency band.

- First generation analogue cellular telephony came to resolve the above problem. By dividing the frequency range into a number of channels, each channel could be reused, as long as the Base station (BS) using that frequency was sufficiently far away from another BS using the same frequency. That introduced the concept of frequency planning and site survey. Analogue systems were based in that architecture to extend their coverage space and include whole countries. Examples of analogue mobile telephony include Advance Mobile Phone System (AMPS) in the US and Total Access Communication System (TACS) in UK and other parts of Europe.
- The second generation of cellular telephony (2G) used an analogue to digital converter to convert the data into a digital stream. It also used a combination of Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM) to divide the available spectrum into a number of channels. Working in an all-digital environment presented a number of advantages: ease of encryption, reduced interference, better spectrum utilisation and many new applications (SMS, data transfer, etc). As good as the initial plan for GSM was, it still remained the problem of higher speed data rates: GSM was only capable of transmitting 9.6Kbps; a speed considered very low for today's applications. Solution came with the introduction of what was called 2.5G: High Speed Circuit Switched Data (HSCSD) and General Packet Radio Service (GPRS). Utilising circuit switching and packet switching respectively, these additions to GSM managed to increase the data speed to 57.6 and 115.2 Kbps respectively. The basic technique behind this increase of bandwidth is the use of additional time slots (slots that other users would use with their mobile phones). This, however, results either in additional charging, or in reduced battery autonomy.
- The latest addition to mobile telephony is the third generation system (3G). Using a number of alternative techniques (EDGE, cdma2000, WCDMA) it

manages to elevate data transfer speeds up to 2Mbps (using a mobile device in a fixed position). Having that much bandwidth opens up the way to an exciting number of new applications: two-way videoconferencing, multimedia messaging that includes video, high quality audio playback, high resolution picture exchange, city mapping, etc. 3G is at its beginning. Time will tell if it will completely replace 2G and 2.5G devices (like 2G did for analogue telephones) or it will just be an alternative for bandwidth demanding applications, leaving 2G to play its well-deserved role in standard mobile telephony.

- Studying the above timeline, one can distinguish a **constant shift** from standard applications to bandwidth demanding applications: initially mobile telephony was more than adequate to cover the user's needs, while in today's world people request an increase amount of data speed for their applications. The above requirement gave birth to Wireless Local Area Networks (WLANs). Unlike mobile telephony, WLANs are not designed to carry out voice (although this is also feasible) and are usually deployed in a smaller area, like an office, a building or a campus. Novel projects, however, have shown that they can also effectively cover a city area [Ang01]. What WLANs do in essence, is cover the need for high-speed data communication without the nuisance of wires.

3.3 Applications of WLANs

Apart from the obvious need for mobility, an emerging number of applications (even some that were not conceived during the birth of wireless networks) are taking advantage of WLANs today. WLANs are often being added to the existing wired network, providing the last few meters of connection. The ongoing decrease in pricing and the increase of integrated WLAN technology in PCs and mobile computing, has further accelerated the growth of wireless networking at home, in the enterprise environment and also in public spaces like hotel lounges, cafes, airports, Universities campus, libraries, etc.

Below is a short list of some of the basic applications that were only made possible through the use of WLANs [Ani02]

- By using WLANs in dynamic environments, network managers minimise the overhead caused by moves, extensions to networks and other changes, and can redefine the network topology dynamically.
- Network managers installing networked computers in older buildings (like old hospitals) find that Wireless LANs are a cost-effective network infrastructure solution as they eliminate the need for aggressive environment change (holes in the walls, lengthy cables, etc)
- Wireless LANs are the ideal solution for temporary networks (exhibitions, seminars, etc)
- Warehouse workers use wireless devices to exchange information with central databases, thereby increasing productivity and reducing the need for unnecessary movement.
- Network managers implement Wireless LANs to provide backup for mission-critical applications running on wired networks.
- Office workers can roam from meeting to meeting throughout the building, remaining constantly connected to the enterprise network.
- University students can be constantly connected to the network and the Internet while in class and can move from one building to another while roaming between WLAN cells.
- Health care workers can take advantage of WLANs to offer better quality services, faster diagnosis and treatment and in general, more efficient ways of caring for the patient.

3.4 Benefits, concerns and challenges of WLANs

By taking into account the above applications of WLANs, we can identify a number of emerging benefits for either the user or the enterprise [Ani02]:

- Mobility of users within the organisation promotes user satisfaction and improves productivity as the user can have real time access to information from any point, and consequently save time.
- By using a simple wireless architecture, managers can cut the cost of installing, adding, changing or moving network infrastructure. They can also

eliminate the cost and burden of pulling wires or cables through walls, installing new plugs, etc.

- Relocation and reorganisation of offices, departments or even campuses, is made much easier using WLANs. Once the Access Points (APs) are set to strategic places, very little has to be changed to accommodate for the new office structure.
- New applications like mobile videoconferencing and mobile telephony using WLANs can seriously benefit the enterprise and reduce the cost of communications
- Finally, WLANs have a low running and ownership cost and can guarantee a short-term return of investment [Pro99].

Unfortunately, nothing good comes without any negative aspect and that applies to WLANs, as well. Various concerns and challenges have been documented, ranging from health issues and interference to questionable security and range. These issues vary between different WLAN versions but can be generally summarised below regardless of the WLAN standard: [Sta01]:

- In contrast with wired networks that guarantee accessibility and bandwidth, wireless networks, by nature, cannot offer that advantage. This is due to the significant attenuation and distortion the signal undergoes while transmitted over the air and can be attributed to reflections, lack of line-of-sight (LOS), multiple signal path, movement, etc. As most of these distortions are of random nature, the wireless systems include techniques that “hide” these problems from the higher layers protocols and consequently from the user.
- Spectrum is a valuable commodity. License exempt spectrum is of vital importance to small and medium companies that desire the use of WLANs. If they were required to pay for air-time it would pose a serious handicap to the WLAN deployment. The spectrum regulation committees over the world recognised the obvious need for some bands to be license-free but unfortunately failed to agree on the exact same frequencies. This was mainly due to the fact that frequency bands have been reserved for other uses in the past. As an example, US GSM operates in 1.9GHz instead of the standard 900MHz or 1.8 GHz, as these frequencies have been in use by the US army

for a number of years. Consequently, techniques for world-wide operation of WLAN equipment are necessary.

- This license-free nature of WLANs means that other products can operate in the same frequency and potentially interfere with the wireless network (microwave ovens, Bluetooth devices). However, special techniques have been developed to reduce that problem. They include Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) and will be described in a later part of this chapter.
- Security is probably the first concern that comes to mind when talking about wireless networks. Enterprises have to be certain that they can trust WLANs as much as they would trust wired ones. To accomplish that, there is a need for encrypting the transmitted data and controlling the access of the users (will be dealt with in detail, in a later chapter). Finally, contrary to wired networks, where terminals can be located in a fixed position, wireless networks offer the ability of roaming between cells thus constantly changing the current topology and work grouping.
- Health concerns have always been an issue when using radio frequencies. People tend to confuse health issues concerning cellular telephony, with those concerning WLANs. Cellular transmissions are quite different as they operate in a different frequency, they are used by mobile phones operating very close to the human brain and they are of “bursty” nature (transmission on fixed time intervals that explain the characteristic sound of amplifiers and TVs when mobile phones are in close proximity). This is very different from the transmission of WLANs. Most of them are operating in a 2.4GHz frequency band; the exact same band that water molecules resonate and the same band that microwave ovens use. In contrast with the microwave ovens, though, that output a power of about 700-1000W, WLANs output merely 30-50mW and relatively away from the human brain. There have been a great number of studies on the effects that these frequencies have on the brain: it has been suspected that prolonged use of such radio frequencies (GSM, WLAN) can gradually raise the average temperature of the brain and cause long term diseases. However a final answer is yet to be given as these studies result in different conclusions: some say that there is no scientific proof that

these combinations of power and frequencies can be harmful to the brain, while others indicate that there is no proof to the contrary. The overall situation resembles the first days of electricity when people were worried about damaging their health when power cables were passing through their houses. It is the writer's opinion that a number of years must pass until we can draw a definite scientific conclusion of the above problem. Nonetheless, various health and radio regulatory bodies all over the world, issued conservative guidelines in order to protect consumers from possible side effects (ANSI/IEEE C95.1-1992) [Ent02]. They have set a maximum power level for these kinds of devices. These rules are obeyed (or made even stricter) by hardware manufacturers today.

- Finally, power management also plays an important role in the operation of WLANs. As many of the terminals operate using battery power, the electrical consumption of the WLAN hardware dictate the autonomy of the overall system. Having this in mind, hardware manufacturers keep reducing the power consumption of WLAN equipment by embedding several techniques: beacon instead of constant transmission, sleep mode, power saving mode.

3.5 WLAN frequency bands

One of the basic reasons that supported the rapid growth of WLAN during the last five years, was proven to be the fact that there was no need for any license to operate in the frequency bands that WLAN use [Kap02a].

Local regulatory bodies around the world (ETSI for Europe, FCC for US) deregulated small portions of spectrum to be used without the need of licenses. This spectrum is commonly called ISM (Industry, Science and Medicine) on the 2.4GHz and UNII (Universal Networking Information Infrastructure) on the 5GHz band [Table. 3.1]. As mentioned above, spectrum is a valuable resource and the frequency bands that were deregulated were always the least desirable ones for any other kind of applications, due to the coexistence of common noise sources: the 2.4GHz band is the same band where microwave ovens operate, while the 5GHz band is crowded with older satellite signals and military radar.

Below is a summary of the unlicensed frequency bands that WLANs use:

2.4 GHz band	**ISM:** 2.4 – 2.4835 GHz				
11 channels	1W				
5 GHz band	**UNII-1:** 5.15-5.25 GHz	**UNII-2:** 5.26-5.35 GHz	5.36-5.47 GHz	5.471-5.725 GHz	**UNII-3** 5.726-5.825 GHz
12 channels (US)	50 mW	250 mW	reserved	reserved	1 W
19 channels (EU)	200 mW		reserved	1 W	Reserved

Table 3.1 ISM and UNII unlicensed bands used in most of WLAN networks (max power indicated)

Both ISM and UNII bands have different regulations on the maximum power level depending on the distance and application to be used: UNII, for example, consists of three separate bands: UNII-1 for indoor use, UNII-2 for either indoor or outdoor use and UNII-3 for outdoor bridging only.

3.6 WLAN trends and versions

With Europe and the US competing on WLAN technology, two major trends appear in the market today: IEEE 802.11 and ETSI HiperLAN; the former being the most dominant around the world. Both these trends have several similarities but are separated by major differences, as well.

3.6.1 IEEE 802.11

In 1997 the IEEE 802.11 task group issued the first set of specifications describing the physical (PHY) and Medium Access Control (MAC) layer of a wireless network capable of working at speeds of 1 and 2 Mbps. It used either Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) operating at 2.4 GHz ISM or Infrared (IR) light at a wavelength of 850 and 950 nm. After a short period, it was clear that greater speeds were needed if WLANs were to gain popularity. From then on, IEEE 802.11 groups created several task groups named a, b, g, e, h, i, to address the different needs of users for security, speed, quality of service, etc. A short mention of the basic characteristics of each follows:

- **IEEE 802.11b** is undoubtedly the most popular WLAN standard today. Its success is mainly contributed to the WECA's Wi-Fi alliance that permits wireless Network Identification Cards (NICs) of any vendor, to work with an

AP of another vendor. It operated in the 2.4 GHz band providing a maximum speed of 11Mbps that automatically falls down to 5.5, 2 and 1 depending on the distance and interference of the channel.

- Despite its name, **IEEE 802.11a** is a newer addition to the 802.11 family. It is a high-speed LAN capable of providing speeds up to 54Mbps in the 5GHz band. In contrast with 802.11b it uses OFDM modulation to reduce the multipath interference. 802.11a products are not compatible with 802.11b.
- The above incompatibility gave rise to the development of another product in the 802.11 series; **IEEE 802.11g**. 802.11g can be considered as an extension of the 802.11b in the 2.4GHz ISM band. Due to its superior modulation (combination of OFDM and Complementary Code Keying, CCK) it can support speeds of up to 54Mbps. Commercial products of 802.11g are just beginning to be available in the market.
- **IEEE 802.11e** came to fill the need for Quality of Service (QoS). Many real time applications (like videoconferencing, voice over IP, etc) need to have higher priority over standard network traffic. 802.11e creates different classes of transmission for different types of data transmitted over a wireless link.
- **IEEE 802.11h** is an enhancement of 802.11a standard that improves coexistence with other WLANs operating in the 5GHz band. This is particularly important in Europe, as ETSI promotes HiperLAN/2 that operates in the 5GHz band (explained later).
- **IEEE 802.11i** addresses some security issues that become very significant after several successful attacks made on the standard 802.11b encryption with weak or improper configuration. However, this will be explained in Chapter 7.
- Finally, a very new task group, **IEEE 802.11n** is developing special protocols to increase the bandwidth of 802.11 to at least 100Mbps. This, however has not been standardised yet.

3.6.2 ETSI HiperLAN

Alongside IEEE, its European counterpart, ETSI, was developing similar protocols to facilitate the use of WLANs. Two majors versions exist [Khu00]:

- ETSI started developing HIgh PERformance LAN type 1 (**HiperLAN/1**) in 1997, mainly for use in ad-hoc topologies (computer to computer). The standard mainly supports asynchronous data transfer and uses CSMA/CA techniques. Its maximum speed is 22Mbps.
- From 1999 until today, ETSI has been developing a complement of the above protocol; **HiperLAN/2**. Using OFDM for modulation, it can support speeds up to 54Mbps in a distance of about 150m. Its internal coding schemes and characteristics are very similar to IEEE 802.11a [Dou02], however HiperLAN/2 also supports for traffic differentiation; a fundamental prerequisite for QoS: each connection is assigned one out of five specific priority levels (in terms of bandwidth, delay, jitter, BER, etc) relative to other connections [San02]. Unfortunately, and despite years of anticipation, HiperLAN/2 is still not commercially available today.

Table 3.2 summarises some of the major characteristics of the most popular wireless technologies today.

	IEEE 802.11b	**IEEE 802.11a**	**IEEE 802.11g**	**Hiperlan/1**	**Hiperlan/2**
Frequency band	2.4GHz	5GHz	2.4GHz	5GHz	5GHz
License (ISM)	No	No (Not applicable in Europe)	No	No	No (not applicable in Japan)
Frequencies	2.4-2.483 GHz, 3 non overlapping channels	5.15-5.30 & 5.47-5.725 (Non-Europe) 12 channels	2.4-2.483 GHz, 3 non overlapping channels	5.15-5.30 GHz 5 channels	5.15-5.30 & 5.47-5.725 (Europe)
Max capacity	11Mbps	54Mbps	54Mbps	24 Mbps	54Mbps
Intermediate speeds	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 12, 24 Mbps	6, 9, 12, 18, 27, 36, 54 Mbps
Modulation	DBPSK, QPSK, CCK, DSSS	BPSK, QPSK, 16QAM, 64QAM	CCK-OFDM, DSSS	GMSK	BPSK, QPSK, 16QAM, 64QAM
MAC	Ethernet based	Ethernet based	Ethernet based	Ethernet based	ATM based
Typical Power	30mW	25mW	50mW	0.1-1W	25mW
QoS	Low	Low	Low	Medium	High
Possible Interference	Microwave ovens, cordless phones, Bluetooth, fluorescent lamps	Satellite (not for open environments), HiperLAN	Microwave ovens, cordless phones, Bluetooth, fluorescent lamps	Satellite (not for open environments)	Satellite
Types of applications	WLAN, real-time	WLAN, real-time	WLAN, real-time	WLAN	WLAN, video, broadcast, MPEG
Typical radius	30-200m	20-100m	30-200m	20-100m	20-100m
Cost today	Low	Low	Medium	Medium	N/A

Table 3.2 Comparison of WLAN standards and technologies today

The IEEE 802.11b is the most widely used protocol and is the network of choice for the development of the MedLAN project. The remaining of the chapter investigates details of installation considerations, physical characteristics and services of a WLAN. It is assumed that all the above address primarily the 802.11b.

3.7 Physical characteristics of 802.11b

The characteristics of the physical layer (PHY) specifications of IEEE 802.11b, extend to great detail and cover several volumes of specifications. From those, the most basic procedures and techniques will be mentioned.

3.7.1 Mapping 802.11b into the ISO-OSI 7 layer model

The International Standards Organisation (ISO) has established a seven-layer model for Open Systems Interconnection (OSI), that governs the connection of homogeneous and heterogeneous networks. It includes the following layers: Physical, Data link, Network, Transport, Session, Presentation and Application. It is beyond the scope of this thesis to get into greater detail on the ISO layers. It is worth mentioning though, that layers 3 or 4 and above are independent of network architecture and are applicable to LANs, MANs and WANs. In that way, a discussion of LAN protocols (wired or wireless) is primarily concerned with the lower layers of the OSI model [Nor98]

On the other hand, the IEEE 802 group (that deals explicitly with the lower layers) has developed its own architectural model that has found great acceptance to organisations; the 802.11 reference model [Fig. 3.1].

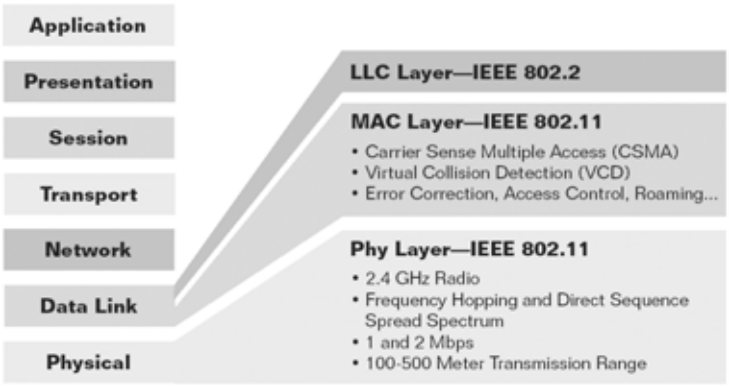


Fig. 3.1 the IEEE 802 model compared to the 7-layer OSI model for the 802.11 protocol

The PHY layer of the IEEE 802 reference model includes functions like encoding and decoding of signals, preamble generation and removal, bit transmission and reception, etc.

Above the PHY layer are functions that deal with providing LAN services to the users and include the following:

- Assemble the data into frames with address and error detection fields.
- Disassemble frames and perform address recognition and error correction.
- Govern access to the LAN transmission medium (wired or wireless).
- Provide an interface to the higher layers and perform flow and error control.

Of these four items, the first three are treated as a separate layer (or sub-layer) by the IEEE 802 model, and form the Medium Access Control (**MAC**) sub-layer, perhaps the most important part of the wireless networks. The fourth item is separate and creates a Logical Link Control (**LLC**) sub-layer, something that is not described efficiently in the data link layer of the OSI model (especially for managing a shared-access medium). It is also worth mentioning that for the same LLC, several MAC options may be provided.

3.7.2 Wireless media

There are three wireless media defined in the original IEEE 802.11 protocol:

Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) and Infrared (IR).

Although fully defined, **Infrared** transmission is the least favourable way of transmitting. Nevertheless it possesses a number of advantages like: the unregulated medium worldwide due to its nature (light), easily securable rooms using IR as light cannot penetrate walls and finally the fact that light colour objects can be used as mirrors to reflect the IR beams [Fig. 3.2] [Sta01]

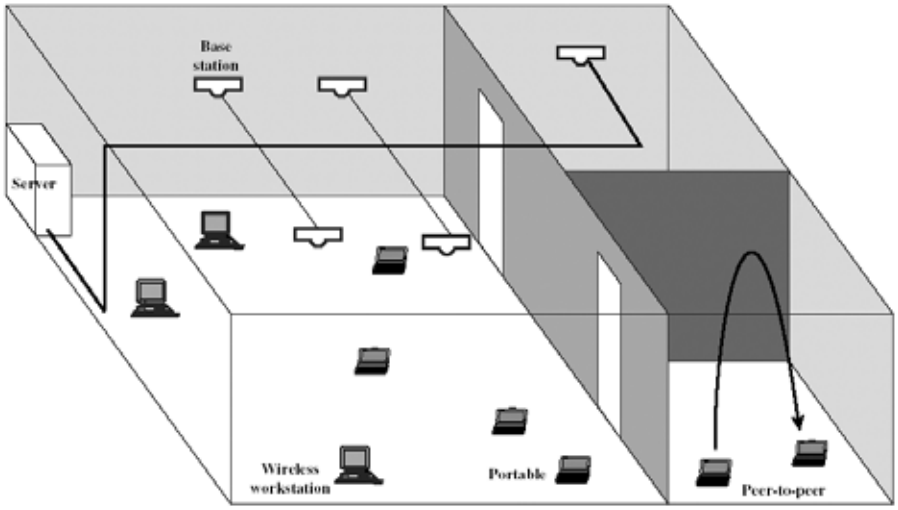


Fig. 3.2 A typical infrared configuration. Several IR networks can be set up in different rooms as light from one room does not interfere with any other IR network in another room

There are three alternative transmission techniques for IR:

directed beam to create point to point links

diffused, where all IR transmitters are focused on a diffusely reflecting ceiling

omnidirectional, that involves a base station within the range of all other Mobile Terminal (MT) (usually on the ceiling). This last scheme, omnidirectional, is the most commonly used one and achieves a maximum range of 20m [Sta01].

Despite some advantages that IR transmission has, its low range coupled with the inability of the system to transmit through solid objects (walls, etc) makes it useful only for a small number of applications (low cost communication, microwave sensitive environment, etc). Finally, two data rates are possible: 1 Mbps (using a 16-Pulse Position Modulation, PPM) and 2 Mbps (using 4-PPM).

Excluding IR transmission, essentially leaves the users with a choice between one of the two previously mentioned spread spectrum techniques, FHSS and DSSS.

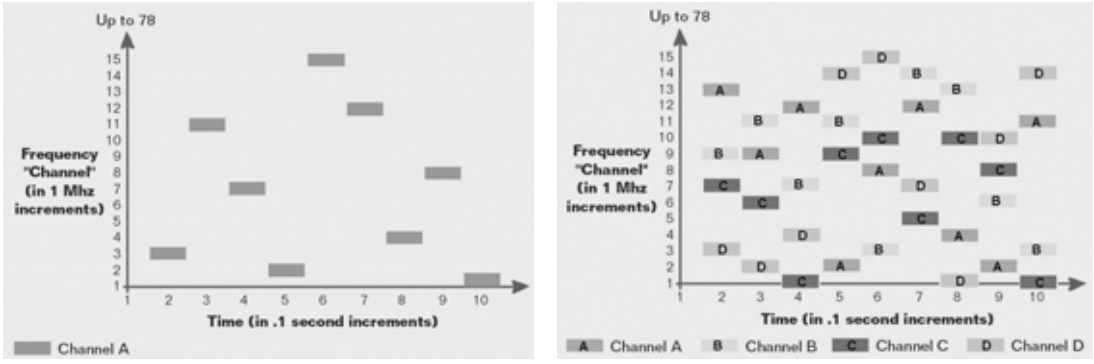
Generally, in a spread spectrum system the transmission bandwidth used is much greater than that required to transmit the signal. The way this is done, is by spreading the information signal over a larger bandwidth, before transmission. This is a totally opposite approach than the conventional method used by radio, television, etc, where the “station” occupies a specific narrowband channel.

The spreading of the signal is governed by a spreading code, independent of the information of the signal. At the receiving end, the signal is de-spread using the same spreading code to recover the information. This process reduces the harmful effects

of noise, as noisy sources usually affect a specific part of the frequency spectrum. It also enhances security, as the receiver must possess the spreading key in order to de-spread the data. This latest ability made the system ideal for military applications when it was initially launched in the 1950s. Later, as the advantages of spread spectrum became known, it was applied in a number of commercial applications like cellular telephony. Below is a summary of the advantages of spread spectrum [Sub98]:

- Low probability of intercept and enhanced security as the transmitter and the receiver share a common, secret spreading code.
- Combats multipath interference since the receiver can "lock" into one of the arriving paths.
- Allows for multiple access within the same channel with more than one users transmitting in the same frequency range but using different spreading codes. The "other" signals would be considered as noise.

Frequency Hopping Spread Spectrum is a process when a radio transmits and receives a packet of data at a specific frequency, for a short period of time, before changing (hopping) into a different frequency. The message is fully received only if the intended receiver knows the hopping sequence (usually different for each hardware vendor). To the intruder, these transmissions are perceived as random unintelligent beeps [Fig. 3.3]. Most FHSS systems divide the ISM band into 78 separate 1 MHz channels and "hop" between these channels ten times every second using a pseudo-random algorithm [Sta01].

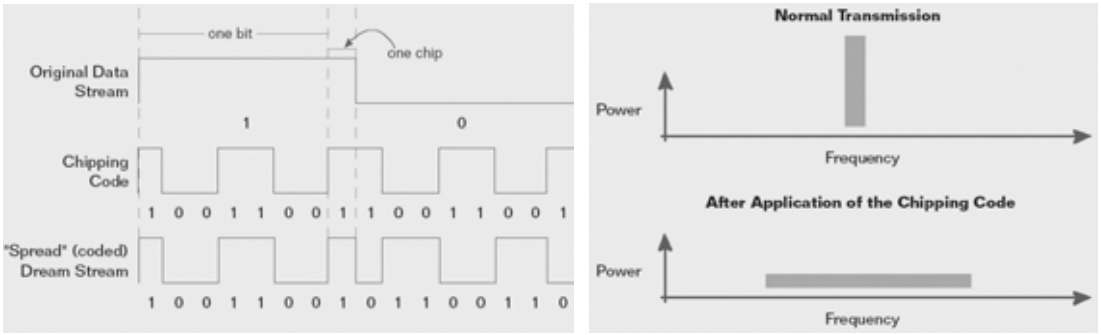


a b

Fig. 3.3 a. Frequency Hopping Spread Spectrum uses a pseudo random algorithm to "hop" from one frequency to another. b. Several transmissions can share the same frequency band

FHSS has two distinct benefits: electrical noise caused by random electromagnetic signals will only affect a small part of the useful signal. Furthermore, the effects of other legitimate transmissions in the ISM band will be held to a minimum. In any such case, error detection mechanisms will be engaged and a retransmission of a small part of the signal will take place automatically.

Direct Sequence Spread Spectrum is by far the most common method used by WLANs today. A direct sequence modulator takes input bits and ads redundant data bits to them, creating "chips" [Fig. 3.4.a]. At least 10 redundant bits are added (with 11 to 20 being a more realistic value). An example of an 11-bit chip might be: 0=10010010110 and 1=01101101001. This repeated pattern of chips is called "chipping sequence" or "Barker sequence". A good spread spectrum code has a low cross-correlation value with other spread spectrum codes issued by other radios in the same vicinity, in order to achieve the minimum interference among them.



a b

Fig. 3.4 a. Direct Signal Spread Spectrum adds redundant information to each bit transmitted, using a "chipping code". b. the power of the transmission is "spread" to minimise the interference

Similar to FHSS, a DSSS receiver must know the transmitter's spreading code in order to properly restore the original signal. The different spreading codes are what allow multiple DSSS transceivers to operate in the same area, without causing interference to each other, even though their channels will operate in overlapping frequencies [Fig. 3.4.b].

When comparing the two, FHSS radios generally use less power than DSSS and cost less as they have reduced complexity in their design. However, DSSS have a practical raw data rate of 8 Mbps (and by using advanced techniques can achieve even greater speeds) while FHSS have a practical limit of 2 Mpbs and generally

reduced range. That is the main reason why FH was used widely in the first version of 802.11, while the newer versions favoured DS.

In conclusion, if a small inexpensive wireless adapter is needed without, the demand for a wider distance range, a FH system will be sufficient. On the other hand, as applications become more demanding, DS will meet these needs better. With either method, the result will be a secure system that minimises the interference with other wireless systems and provides sufficient bandwidth for data [Appendix A].

3.7.3 Medium Access Control layer (MAC)

As mentioned before, the MAC layer is the building block of a WLAN. It receives a block from the LLC layer and performs functions related to the medium access and to the transmission of the data. The LLC in its turn is responsible for supporting the multi-access shared-medium nature of the link thus relieving the MAC layer from that task. The data that the MAC layer handles at a time form the Protocol Data Unit (PDU), is often referred to as the MAC PDU.

The format of the MAC frame for the IEEE 802.11is illustrated in Fig. 3.5. The timing of the MAC sequence of 802.11 exists in Appendix B.

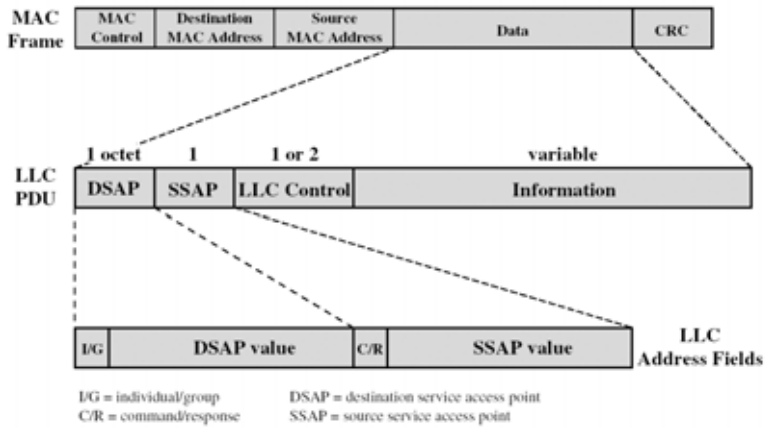


Fig. 3.5 MAC frame and LLC PDU format of 802.11

- Cyclic Redundancy Check (CRC) is used for error detection.
- Data represents the body of the MAC frame and can be data from a higher layer (like LLC) or MAC control information.

- Source and destination MAC addresses are unique values set by the manufacturer of each network device. These can be used as filters by the APs for limiting the access of unauthorised users to the WLAN.
- Finally the MAC frame control contains a series of information needed for the functioning of the MAC protocol. Fig. 3.6 illustrates an analysis of this field [Sta01].

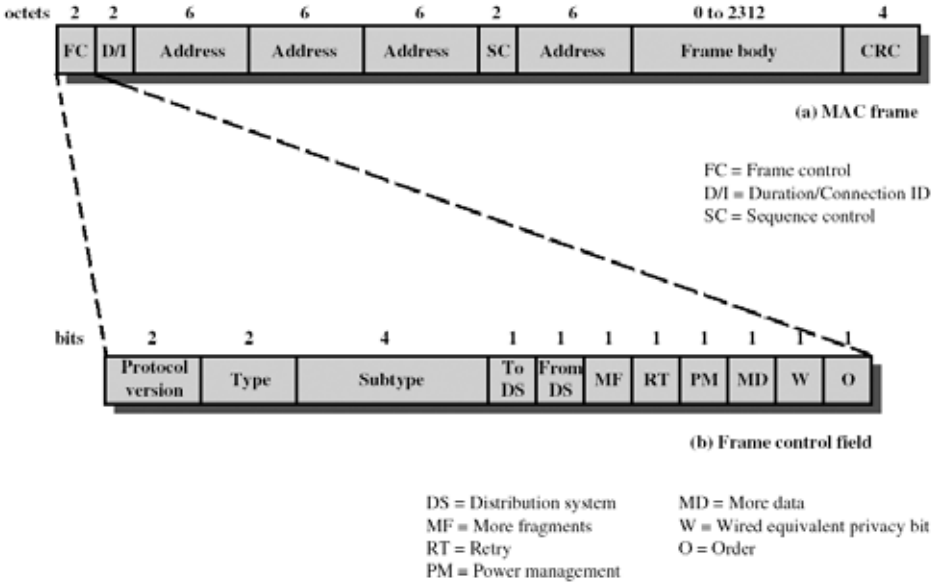


Fig. 3.6 MAC frame of IEEE 802.11 as it is actually transmitted over the medium

3.7.4 A general WLAN model: sequence of operations

Summarising all the above procedures, Fig 3.7 displays the sequence of events on the lower layers of the IEEE 802 reference model.

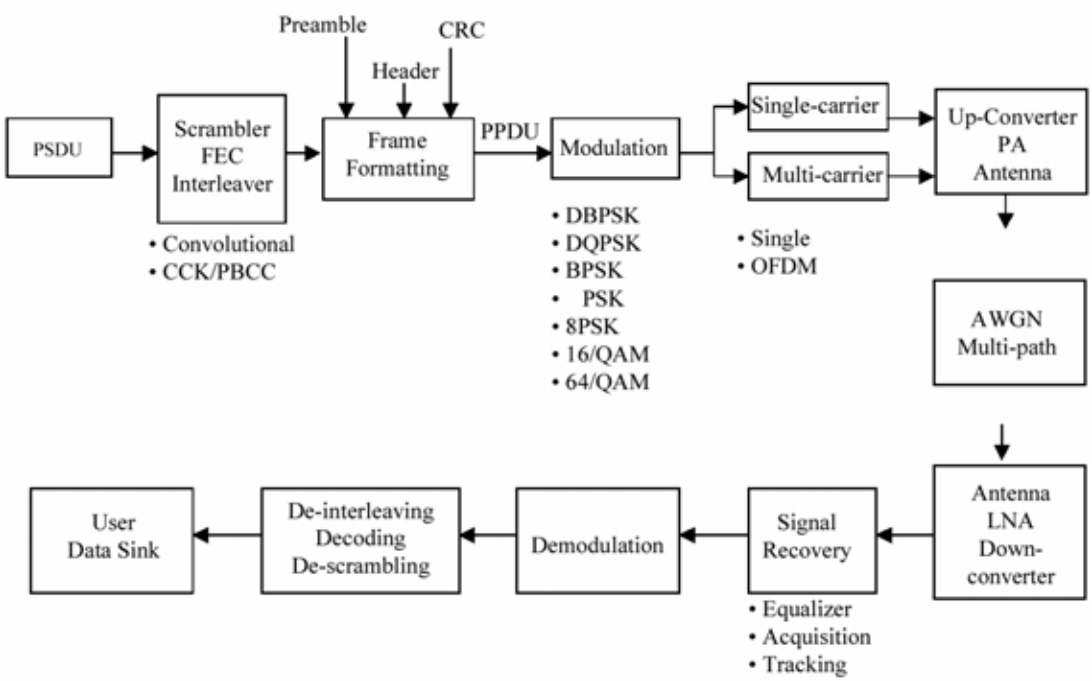


Fig. 3.7 Clockwise sequence of events within the lower layers of both OSI and IEEE reference model

The raw data to be transmitted, is stored within the PSDU that is input to a scrambler whose job is to prevent long runs of 1s and 0s. Most WLAN systems scramble the data with a length 127 pseudo-random sequence. The scrambled data is input to a convolutional or to a CCK/PBCC encoder. The coded data is interleaved in order to prevent error bursts to affect the decoding procedure. Preamble, header and CRC are added to the signal and then the coded data is mapped to data symbols using BPSK, Quadrature PSK (QPSK), 16 QAM, 64 QAM, etc. Finally comes the choice of carrier: single carrier for 802.11b or multi carrier for 802.11a or HiperLAN/2, usually using OFDM modulation [Dou02]. The whole signalling train is transmitted over the air and noise is inevitably added to the channel (Additive White Gaussian Noise, multipath noise, frequency selective fading, etc). The receiving antenna picks up the signal and after equalisation (band pass filtering) it demodulates it, removes the interleaving sequence, decodes and descrambles the signal.

The above procedure is common to almost all existing wireless protocols today with some variations on the details.

3.8 Installation considerations

After deciding on the technology and version of WLAN to be used, one should consider some basic installation parameters: topology, frequency planning, the hidden station problem and the possible interference with other devices using the same frequency band.

3.8.1 Topologies of WLANs

Wireless LANs can operate in the following topologies:

Ad-hoc mode (also referred to as Independent Basic Service Set) is very similar to a home or office, peer-to-peer network, where no single node plays the role of a server. It includes a number of wireless terminals that communicate with each other with no need for an AP or any connection to a wired network [Fig. 3.8]. This topology is ideal in situations where no wireless infrastructure exists (or is not required). Typical examples are conferences, hotels, airports, etc [Cis01].

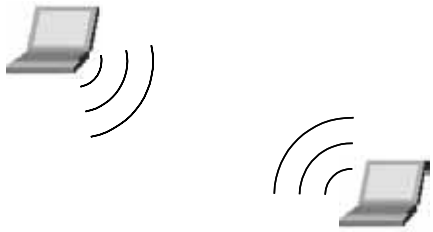


Fig. 3.8 Wireless ad-hoc topology with no need for an AP

Infrastructure mode (also called Basic Service Set) is the most commonly used topology. It includes at least one AP that acts as a server for a single WLAN cell. This AP is usually connected to the wired network infrastructure allowing the AP to act as a bridge between the wireless and the wired network (e.g. 802.3 and 802.11). Communication between mobile terminals flows from the source terminal to the AP and from then on, to the destination terminal. This topology can be extended to use several overlapping APs and form an Extended Service Set (ESS). APs are connected together through the wired network [Fig. 3.9]. The major advantage of this scenario is that a mobile terminal is permitted to roam from one cell to another seamlessly, without losing connection to the network and without the user being aware of this procedure.

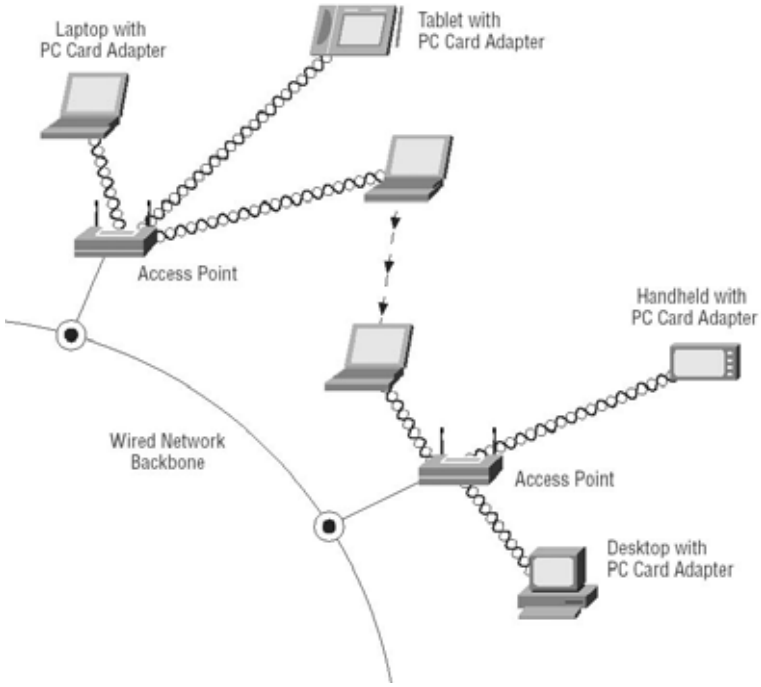


Fig. 3.9 Infrastructure mode: each AP creates a cell (BSS). Multiple APs are connected to the wired network allowing mobile terminals to roam among them (ESS)

Bridge mode is not as commonly used as the above topologies, but is gaining popularity as wireless bridge devices are becoming more affordable. In Bridge mode, entire wired networks use wireless links to connect to other networks in relatively close vicinity. A perfect example is the use of wireless bridges to interconnect two or more offices of a company that are in close proximity. This eliminates both the need for wires and the expenses for renting leased lines (most leased lines have considerably lower bandwidth capacity than WLANs) [Fig. 3.10]. The distance between buildings can vary from 3-25km, with the use of parabolic antennae and usually requires a relatively clear line-of-site. Wireless bridges can operate in point-to-point and point-to-multipoint mode.

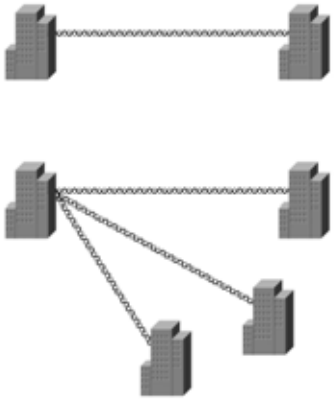


Fig. 3.10 Wireless bridges connect networks from different buildings
either in point-to-point or in point-to-multipoint mode

3.8.2 Frequency planning

Before installing a wireless network it is highly recommended that a full site survey would be performed. This would not only reveal possible leaks of wireless signal outside the region of interest (that would eventually be considered as security threats) but would also help to establish the precise range of each of the APs. This will lead to a better utilisation of the available spectrum as one can place the APs in such a way that the interference between them will be minimised.

In IEEE 802.11b the available spectrum is divided into 11 partially overlapping channels (2.4-2.48 GHz) [Sta01]. From those 11 channels, three are non-overlapping (channels 1, 6, 11) [Fig. 3.11]

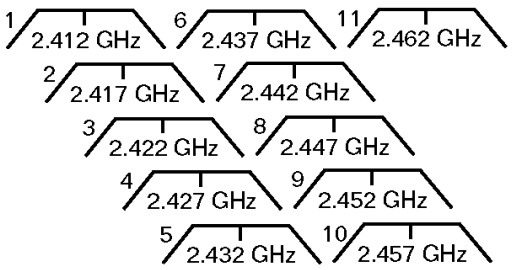


Fig. 3.11 802.11b has 11 partially overlapping channels. From them 1,6, and 11 are non-overlapping

The above means that by carefully placing several APs in a way that the range of the first one (using channel 1) will not extend to interfere with the range of the fourth one (reusing channel 1), one can extend the WLAN coverage infinitely and include whole buildings in a cell-like structure [Fig. 3.12]. The transmitted power of the APs can also be adjusted to vary the size of the cell, much like in GSM structure.

Alternatively, three APs operating in channels 1, 6 and 11 can be used in close proximity to triple the available bandwidth (3x11=33Mbps) where there is such a need (busy office location, café shop, etc), without causing any interference to each other.

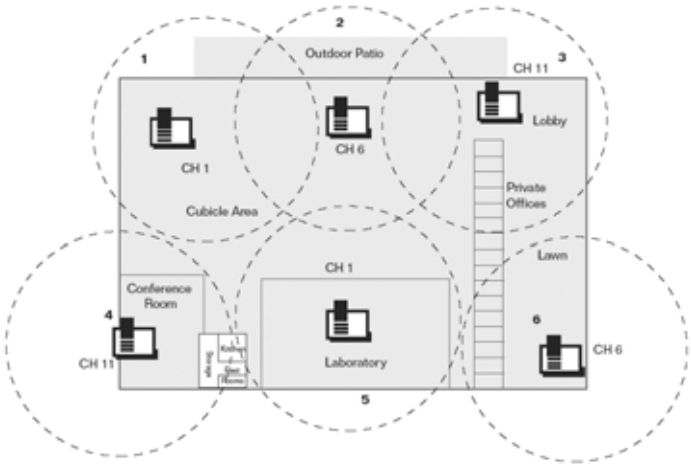


Fig. 3.12 By establishing the range of each AP, the same frequencies can be reused to extend the coverage of the WLAN

It is worth mentioning that IEEE 802.11a has a definite advantage over 802.11b as it supports eight independent channels. That makes frequency planning much easier and reduces Co-Channel Interference (CCI) considerably [Che01]. Although the range of the 802.11a cells are practically much shorter that those of 802.11b, Fig. 3.13 demonstrates the above notion.

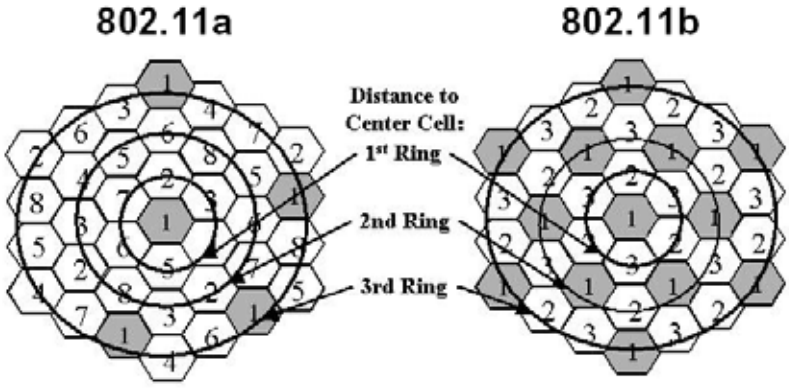


Fig. 3.13 By having eight, instead of three independent channels, 802.11a can reduce Co-Channel Interference by placing AP cells, using the same frequency, further apart from each other

3.8.3 The hidden station problem

A significant difference between the wired and the wireless networks is the fact that in the latter case one cannot assume connectivity between terminals: a mobile node can get out of the range of the WLAN. This gives rise to the “hidden station” problem, very often encountered in infrastructure topology, with multiple mobile terminals [Fig. 3.14]

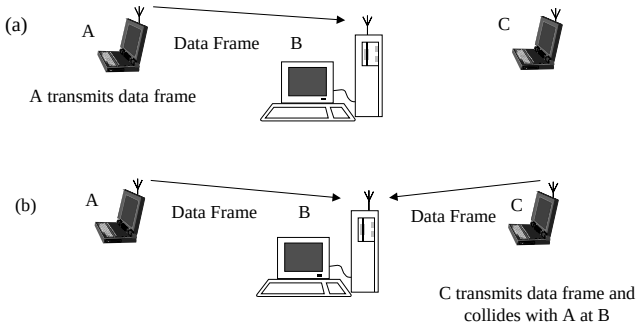


Fig. 3.14 The hidden station problem

Mobile terminal A (MT A) is outside the range of MT C but they can both communicate with AP B. While MT A transmits a data frame, MT C cannot “hear” this transmission and assumes the medium is free [Fig. 3.14.a]. As MT C tries to transmit at the same time, both packets collide and are destroyed [Fig. 3.14.b] [Gar00].

The solution comes by varying the principles of Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA): the controlling part of the wireless network (AP) introduces the use of Request To Send / Clear To Send (RTS / CTS) commands. Using that technique, MT A sends a RTS frame to B (about 30 bytes containing the length of the data to follow). MT B replies with a CTS (frame contains the length from the RTS) and immediately after MT A begins transmission [Fig. 3.15]

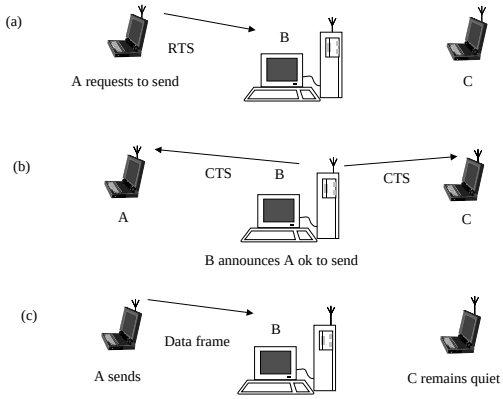


Fig. 3.15 By using RTS/CTS commands, the hidden station problem is eliminated

Any other station hearing the RTS (close to MT A) and any station hearing the CTS (close to MT B) must remain silent. Even in extreme cases when collision occurs, stations back off for random time and retransmit [Gar00]. RTS / CTS is an effective mechanism to combat interference from hidden terminals. RTS and CTS data packets are very small (20 and 14 bytes respectively) compared to the maximum 802.11 data frame of 2346 bytes, thus cause negligible overhead. As a result, when collisions occur, less bandwidth is wasted compared to standard 802.11 transmissions. This does not apply in an environment characterised by a great number of MTs using small data packets.

3.8.4 Interference by other 2.4GHz devices

As mentioned in previous subchapters, the 2.4GHz band was intentionally included to the ISM band because it was, by nature, a very noisy frequency band. Hardware manufacturers had to overcome this problem by applying DSSS and FHSS techniques.

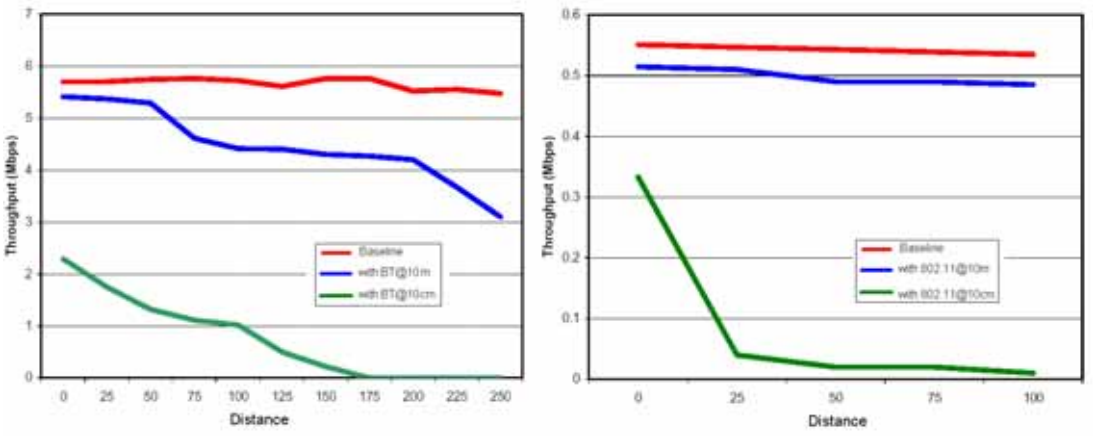
Despite the obvious gain of spreading the available data into a frequency channel, 2.4GHz still suffer from interference from other sources. The most commonly known are microwave ovens and other devices operating in the same frequency and sharing the same band; 802.11g and Bluetooth.

Microwave ovens operate in a very specific frequency (2.448GHz); a frequency that resonates water molecules and heats up the water. Unlike any narrowband wireless connection that would have been devastated by such high power interferer, 802.11 operates at the exact same frequency bands and suffers very little degradation from channel noise. Practical experiments have shown that by introducing a microwave oven in full operation at a distance of 20cm between two WLAN MTs, resulted in a 11% loss at 1Mbps and 8% loss at 11Mbps. That comes as no surprise at any spreading system: when the WLAN is using DSSS only a small part of the signal is being affected (and errors are usually corrected through the use of Error Correction), while when using FH with an average of 78 hops, only 1-2 packets will be totally destroyed and need to be retransmitted [Fli03].

Bluetooth can be considered as a “light” WLAN. It, too, is capable of bi-directional transmission of digital data using the 2.4GHz band. Contrary to the WLAN structure, though, it uses FHSS and lacks central structure (infrastructure mode). It is mostly

used as a wireless alternative to cables, when low-speed communication is involved (printer, mouse, mobile phone, PDA, etc) with a top speed of about 0.8Mbps.

Several simulations and practical experiments concluded that the coexistence of Bluetooth and 802.11b does not pose major problems nor does it reduce the speed of either considerably [Zyr99], [Sho01]. Obviously, this degree of interference is highly dependent on the loading, the density and the distance between the Bluetooth and the 802.11b terminals. A typical degradation of the available bandwidth of both Bluetooth and 802.11b, is shown in Fig. 3.16 when an interferer is either in very close proximity (10cm) or in average distance (10m).



a b

Fig. 3.16 a. IEEE 802.11b with Bluetooth interferer at 10m and at 10cm.
b. Bluetooth with 802.11b interferer at 10m and 10cm

It is obvious that for a typical scenario, the level of interference among 802.11b and Bluetooth is negligible.

Finally, **IEEE 802.11g** and any future wireless protocols using the 2.4GHz band, are not expected to create considerable interference among them. The reason is that by using different spreading keys, spread spectrum behaves very well when two or more transmissions use the same frequency band. Furthermore, hardware manufacturers promote dynamic channel selection on newer wireless products, which automatically select the least busy and corrupted channel from the ISM band.

3.9 IEEE 802.11b services

In order for the wireless networks to be able to perform basic functions (registering into a cell, communication, verification of data, moving from one cell to another) nine different services (procedures) were established. Four of them belong to the station services group (MT) and the remaining five to the distribution group. The **station services** are of particular interest and include: authentication, de-authentication, data delivery and privacy [Oue01]

- The authentication service defines the identity of the wireless device and without this specific function the mobile device is not allowed to connect to the wireless network. Apart from the unique WLAN identity of each MT, authentication can be made using a list of MAC addresses that can be stored either inside the AP's memory or somewhere in the wired network. It is worth mentioning that a MT can authenticate itself to more than one AP to allow for faster roaming from one cell to another.
- The opposite procedure, de-authentication, is initiated when a MT is either shutting down or is moving away from the range of the AP (to free up resources to accommodate other MTs). After this procedure the MT can no longer access the wireless network.
- Much like wired networks, WLANs need to specify a data delivery service to ensure that the data frames are reliably transmitted between MAC layers. This level consists of several procedures:
    - The DCF / PCF functions and the RTS / CTS mechanisms: Distributed Coordination Function (DCF) is mostly used when multiple MTs are operating without an AP. This is a "best effort" delivery system where if the channel is occupied, the terminal wishing to transmit will back off and wait for a random amount of time. Point Coordination Function (PCF) uses an AP that acts as a central controlling element to the wireless traffic. The AP periodically "beacons" the MTs to check if they have outgoing traffic. On both DCF and PCF, Request To Send and Clear To Send (RTS / CTS) is used to implement a CSMA/CA procedure. Finally, it is important to mention that since wireless is an unreliable medium by nature, higher

layer protocols, like TCP, usually guarantee the safe receiving and compilation of all data packages.

- Data Acknowledgement is an essential part of CSMA/CA. In an environment highly susceptible to noise, the MAC layer needs to be informed if a transmitted packet arrived at its destination safely. The receiving station has the obligation to send an ACKnowledgement frame (ACK) to inform the sender of successfully receiving the packet. If this is not received in a predefined time (usually less than a second) it is assumed that the packet is lost and resending procedures are initiated [Appendix B].
- As mentioned above, the wireless environment is highly undependable. When an error occurs within a data packet, regardless of the number of bits corrupted, the whole packet has to be resent. Thankfully 802.11b gives the user the opportunity to vary the size of the packets (from 1 to 2346 bytes) to adapt to the current environment: in a noisy environment smaller packets are used to save time in case of retransmission, while in more reliable scenarios, the packet size is increased to reduce the overhead-to-data ratio.

In contrast with station services, the **distribution services** make the decisions of where to send the data initiated by a MT. They include the procedures of association, re-association, disassociation, distribution and integration.

- In association, the MT, through the AP, establishes a logical connection with the network devices and determines dynamically the path that its signal must take to reach other mobile devices. Association is very different from authentication. In the latter, the MT is accepted by the AP but without the knowledge of where the other network devices are, the distribution service cannot know how to deliver data to them.
- When the MT is moving outside the range of the AP (or if the AP is shutting down) it will lose connection and become disassociated. The MT has to find another AP to associate with.
- If in the above case either the AP is back into operation, or more commonly, the MT returns within the range of the AP, it is re-associated. In the case of

roaming between APs, the re-association procedure informs the new AP on the number of devices that the previous MT was associated to.

- The distribution procedure informs the APs whether the data frame in hand is to be sent to another AP or it is destined to the wired network.
- Finally, the integration service resides within the APs and acts like a bridge between the wired and the wireless network. It translates and reformats packets from 802.11 protocol, into the protocol used by the wired network (usually 802.3).

Fig. 3.17 illustrates most of the above services.

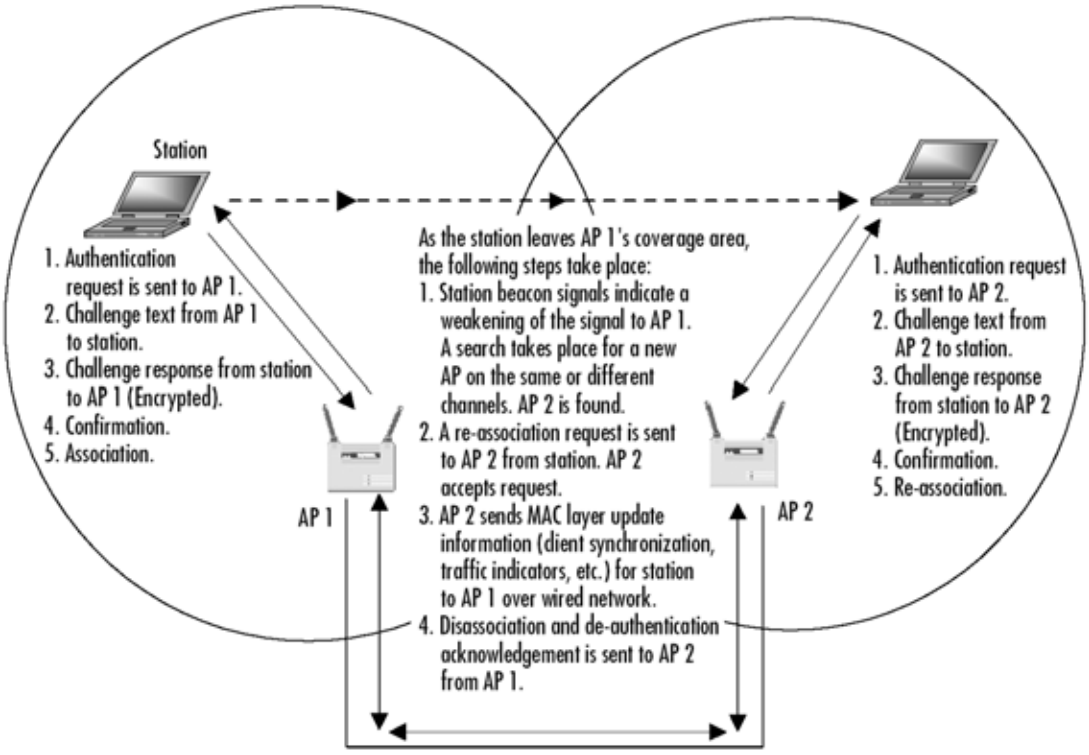


Fig. 3.17 authentication, de-authentication, association, disassociation and re-association of MTs while roaming in a multi AP environment.

Although privacy and security will be analysed in a later chapter, it is worth mentioning some basic security principles that IEEE 802.11b uses.

The privacy service that 802.11b uses to protect data utilises the RC-4 algorithm that has been used for encryption for a number of years. **It is not** intended for an end-to-end encryption (MT to another terminal; wired or wireless) or to be used as the sole means of network protection. Its initial design was to provide a protection equivalent to the wired networks, hence its name: Wired Equivalent Protocol (WEP). However, and due to their nature, wireless networks have always been more prone to security

threats in comparison to their wired equivalent as in the latter, the lack of physical access can prevent potential attacks.

Initially 802.11b provides three ways to increase security on the wireless part of the network. A network administrator can use any (or all) of these methods:

- Withholding the Service Set Identifier (SSID) in the frame that is beaconed regularly by the APs and is needed by the MTs to associate themselves with the network. SSID can be considered as a unique name of each AP.
- Controlling the MTs that associate with the APs, based on their MAC addresses.
- Using the above mentioned WEP algorithm to encrypt the transmitted data, with either a 40-bit or a 128-bit key.

Even by using all the above techniques, there is still a chance that an attacker would perform a passive attack. These kinds of attacks exploit some fundamental vulnerabilities of the WEP algorithm and the way that it creates and maintains the keys, and in some cases can lead to the attacker decrypting the data transmitted and gaining access to the wireless network. This would be examined in further detail within chapter 7.

3.10 Summary and conclusions

This chapter concludes the introductory part of this thesis. The same way chapter 2 dealt with the introduction of some Telemedical aspects to the reader, this chapter offers some fundamental knowledge of wireless LANs and the way they operate.

Within this chapter, we have examined the need that gave birth to WLANs and discussed the benefits, concerns and challenges that WLANs pose to the users. We have listed the most well known technologies of WLANs today and gave emphasis on the IEEE 802.11b, the technology used by the MedLAN system. We also considered the physical parameters of a wireless system and the services that are performed within it and finally elaborated on some installation considerations and procedures.

As our world keeps shifting into “mobile”, WLANs, without a doubt, will play a leading role in that aspect. It is the author’s opinion that in some years from now

wired LANs will not cease to exist, but will provide a fast backbone service to connect the ever increasing number of WLANs.

MedLAN is one of the novel projects that take advantage of the numerous benefits of WLANs that are stated in this chapter. As presented in the next chapter, it uses an infrastructure mode (APs and clients) and multiple APs to allow for one or more MT to roam from one cell to another and cover a vast hospital area.

The following chapters will deal with the original contribution to knowledge starting with describing the physical characteristics and capabilities of the MedLAN system.

4. The MedLAN System

4.1 Introduction

One of the first issues that come to mind when talking about the applications of Telemedicine and Telecare is Teleconsultation. Teleconsultation accounts for a third of the use of Telemedical networks and usually defines the procedure of using communication links to provide an audio / video bridge between the patient's side and a place where a consultant resides. The most frequent example is a videoconference link between a patient in a hospital and a doctor at another hospital.

As Teleconsultation is one of the fastest evolving divisions of Telemedicine, it is expected that it will constantly embrace new technologies with the objective of making the health care delivery faster, more reliable and more accessible. The MedLAN system represents one of these new trends in the Teleconsultation field.

4.2 Current and future medical needs

A Teleconsultation system used in hospitals today usually consists of a relatively heavy trolley that includes a monitor (usually CRT) a desktop computer supported also by an Uninterruptible Power Supply (UPS) with keyboard and mouse, an ISDN modem supporting a triple ISDN line (3x128=384Kbps), a camera and a set of microphone and speakers [Fig. 4.1]. The same equipment has to be present on both sites, patient and consultant. The whole system weights about 30-90kg and during normal operation has to be powered by the mains. Due to its volume, weight and delicate nature, it is usually kept in a special room close to the consultant's office.

The procedure dictates that if a patient is in need of a Teleconsultation, the treating doctor communicates with the consultant via a conventional manner (a telephone call) and both initiate the procedure for the two teleconference machines to link together. The charging of the ISDN communication is usually done based on connection time. Call initiation has to take place and some time has to pass for the two systems to negotiate connection protocols and settings.

It is obvious that due to its weight and volume, the trolley is hard to manoeuvre and this can be a serious handicap, especially on the patient's side. An alternative would be to transfer the patient (usually from the Accidents and emergency room) to the consultation side of the hospital that he or she is treated in.

Fig. 4.1 A modern videoconferencing system including
monitor, desktop computer (inside), camera and ISDN modem

Despite the fact that the above procedure would produce the desired result (and has done for many years now), that does not necessarily mean that it cannot be considerably improved:

- Transferring the patient from the A&E room to another place in the hospital wastes precious time (assuming the best-case scenario when the patient can actually be moved without endangering his or her condition).
- In the case that one of the teleconsultation systems has to get to the patient's site, one or more persons have to be charged with this responsibility (wasting man-hours), as the system is heavy and usually has to be set-up by an expert.
- Lengthy cables in a fast moving environment like the A&E room do not just limit the range of the system but also pose a potential danger to the staff operating in there.
- Finally, ISDN lines operate on an "on-demand" charging system. That means that it would be financially infeasible to retain a constant ISDN connection between hospitals thus a connection procedure has to be initiated every time a new consultation is needed. Furthermore, the ISDN communication model usually addresses similar communication systems and not computers that exist in remote hospitals.

Both doctors and consultants recognised the above vulnerabilities of the present systems and requested for an improvement that would be more autonomous within the A&E room, be less costly to build, easier to operate and would reduce the running communication costs of teleconsultation. By answering those needs (freedom of movement inside the Accidents and Emergency area while transmitting high quality video), the MedLAN system was created.

4.3 System description

MedLAN consists of two main parts [Fig. 4.2]: A mobile trolley that exists in the open plan Accident & Emergencies area (A&E) and a consultation point, within the hospital.

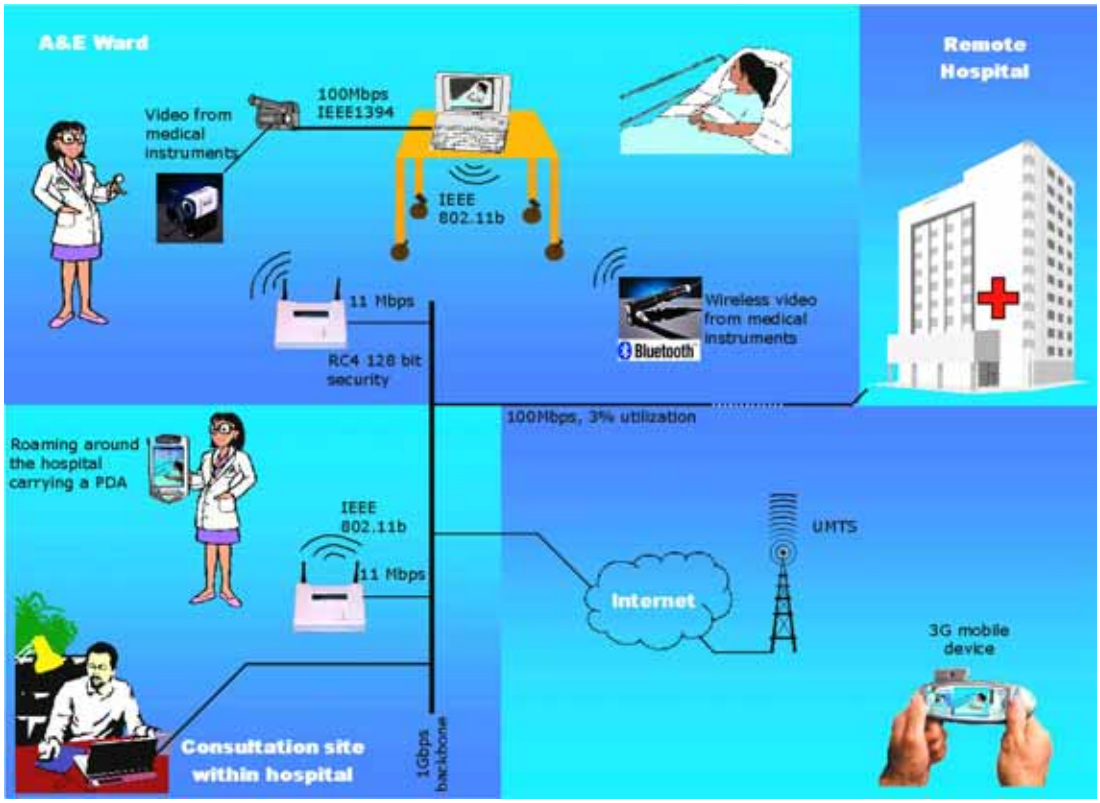


Fig. 4.2 The MedLAN system

The mobile trolley uses a wireless LAN to connect to the hospital's network and can be freely moved to anyplace within the hospital, as long as there is coverage by the WLAN. It can also seamlessly roam from cell to cell without interrupting the teleconference procedure (although this scenario is rarely needed). Within the mobile

trolley exists a high-end laptop computer and a camcorder capable of transmitting both video and still images. The doctor that operates the system can either point the camera directly to the patient, or to any medical information (ECG, hardcopy outputs, films, CRT screens, details of the patient, etc) available at the time. As explained in chapter 5 the procedure of directly viewing the medical data presents several advantages while retaining the diagnostic quality.

The system can also be connected to several medical equipment (digital stethoscope, otoscope, dermascope, endoscope, etc) that produce video or audio (digital or analogue) convert and forward their output into the network. This connection can be made by using cables (AV or S-Video) or by using Bluetooth medical devices.

A consultant either exists at another part of the hospital, or in another hospital connected to the NHSnet. High quality still images along with video and sound can reach the consultant's computer to perform the teleconference procedure [Fig. 4.3]. There is the option of establishing a WLAN in the consultant's site to allow the consultant to freely move around his or her hospital while giving advice.

a b

Fig. 4.3 a. The MedLAN prototype trolley while communicating wirelessly with the consultant. Newer versions do not require the use of a trolley. b. The consultant's side

The overall system is very light and flexible. In its initial version, the contents of the trolley weight just above 3Kg while an even newer version has been tested, having the digital camera embedded in the mobile computer, which the doctor can carry in his or her pocket and can be considered wearable as it weighs less than a kilo.

Furthermore, the use of Personal Data Assistants (PDAs) with wireless support on the consultant's side can enhance consultant's mobility even more and detach him or her from the consultant's offices. The above will be explained in further detail within this and other chapters. Below is a summary of the basic system components for the first version of MedLAN:

- A light portable computer (laptop) that will be the central node of the system. Most laptops available on the market today have sufficient computational power to accommodate the needs of a videoconferencing session.
- A digital camcorder performing a two-fold function: it can be used as a camera for the teleconference part and it can also take high-resolution photographs and sending them to the consultant. The most important characteristics of the camera are: the quality of the camera lens, the ability of focusing to distances close to zero (macro lens), the automatic reduction of hard tremor ("steady shot") the fast and automatic while-balance and the ability to perform under poor lighting conditions. The camcorder also includes a video / audio-in port to connect third-party medical equipment while being able to perform real-time analogue to digital conversion of their signals.
- A hardware video encoder stands between the camcorder and the laptop. It is a very light USB device that accelerates the compression procedure and alleviates that task from being performed by the computer. The alternative would be to directly input an IEEE 1394 (Firewire) signal from the digital camcorder, to the computer but compacting a 100Mbps high quality video and audio signal into a data stream less than 1Mbps requires extra computational time that translates to delay between receiver and transmitter or audio / video desynchronisation.
- The data to be transmitted is processed by the mobile computer and fed into the network path. A WLAN card (that can be embedded inside the laptop) transmits the data into an infrastructure WLAN. The optimum speed is 11Mbps that falls down to 5.5, 2 and finally 1 Mbps as the MT is moving away from the AP. About 40% of the nominal speed is actually available to the MedLAN system with the rest being used by the controlling mechanisms of the WLAN system [chapter 3].

- Access points are strategically placed in the A&E ward (and to anywhere else deemed necessary), pick up the signals from the MTs and forward them to the wired hospital network. From then on (and depending on the location of the receiving station) the data is routed either to a computer within the same domain (hospital or hospital group) or to any other computer in the NHSnet.
- The consultant's computer will receive the video, audio and other medical information having no need of any special software. This computer is also able to respond with any of the above kinds of data.

It is important to understand that this thesis has demonstrated that both the practical and the theoretical capabilities of this system are very broad. Experiments performed have shown that the system is also capable of:

- Accommodating more than one MT in the A&E ward while sharing the 11Mbps wireless capacity.
- Having up to three MTs in the same vicinity, with each one enjoying 11Mbps of bandwidth. This takes advantage of the three independent channels supported in the ISM band.
- Forwarding the data into the Internet to be useful to the consultant, even when he or she is at home or in any place that can access the Internet. This generally requires the use of broadband connections (e.g. ADSL) in the consultant's residence.
- Accessing the data through a mobile computer being connected to Internet using General Packet Radio Service (GPRS) while on the move.
- Accessing the data through the high-speed links offered in the third generation mobile phones (3G) and performing consultations on the run.
- Using high-quality, wireless-ready PDAs to allow the consultant to be in constant communication with the A&E room (always connected) and perform a novel videophone function.
- Wirelessly linking hospitals that are close together and have line-of-site (LOS) to implement an all-wireless, independent telemedical network and reduce communicational costs.

The following block diagram explains further the sequence of events while using the MedLAN system [Fig. 4.4]

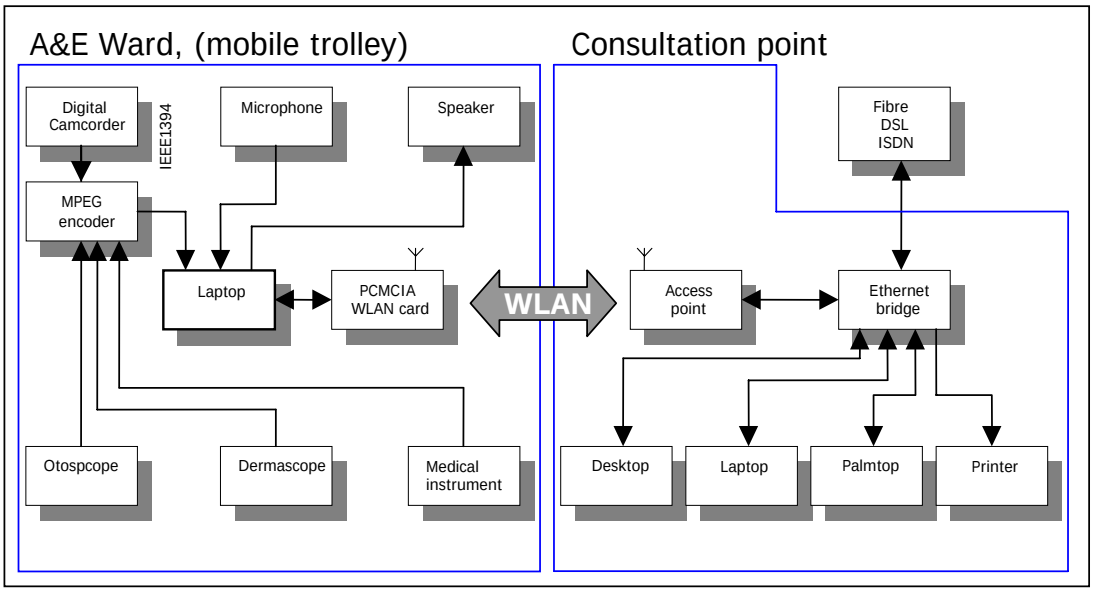


Fig. 4.4 Block diagram of the operation of the MedLAN system

The data initiated from the camcorder and the microphone (videoconferencing mode) flows to the hardware video encoder. Both can have other telemedical equipment as their input. The digital videostream of the MPEG encoder is input to the mobile computer in the MedLAN trolley. Through videoconferencing software, the laptop is able to send audio and video to a specific IP, using a PCMCIA WLAN card (can be embedded in the laptop). The WLAN card acts as a transceiver (transmitter and receiver) to the infrastructure network and is constantly connected to an AP, or roams between APs. The AP is connected in its turn to the wired network of the hospital, along with the consultant's computer, who can eventually view the video and audio sent, based on its IP address. Since this is an all-IP network, outside connections can be supported to send the data anywhere in the world through the use of broadband connections (fibre, DSL, etc). Patient's data can also be forwarded, recorded, and even stored in the patient's file.

4.3 System services and performance

The MedLAN system is capable of handling video, audio still images, video from other sources and wireless access to the hospital's network. Each of these issues will be presented separately.

4.3.1 Video

To accommodate the basic needs for teleconsultation the MedLAN system acts as a mobile videoconferencing system. A high quality camera is input to a hardware encoder that, in its turn, feeds the data to software responsible for recompressing the video and audio stream and transmitting it to the specified IP of the consultant. Assuming that the destination computer would be in the same network domain (NHSnet in this case), the same software can also pick up the data from the network, decompress and display them on screen on the consultant's side.

Several commercially available software packages suitable for videoconferencing, were tested and evaluated. Each had its unique set of advantages and disadvantages:

- **Microsoft NetMeeting v.3** (MNM) was proven to be one of the most reliable software packages. Its greatest advantage was the fact that it is embedded to any Microsoft Windows environment (all available versions from Windows 95 to Windows XP) that seem to monopolise the industry today and is even offered in Linux operating systems. This kind of cross-platform compatibility was proven essential, as sometimes the treating doctor in the A&E ward has no knowledge about the operating environment of the destination computer.

  The system is capable of sending and receiving video in three different resolutions: 160x120, 320x240 and 640x480 pixels. The highest resolution (640x480) is the most suitable for medical applications. Within the available resolutions, the compression factor of the video can be adjusted to increase the quality of the video:

  MNM uses an H.263 video transmission protocol. This is very similar to the MPEG4 compression algorithm where, apart from finding similarities to each frame and grouping them together, the algorithm tries to find similarities in preceding and succeeding frames in order to achieve an even better compression. Furthermore, when the chromatic differences of the pixels are not that high, the algorithm considers those pixels to have the same colour thus compressing the video output even more. The more the compression factor, the less bandwidth has to be used, but the lower the video quality. MNM always tries to take advantage of most of the available bandwidth. It also gives the user the opportunity to select between faster video and clearer video. Selecting clearer video is best suited for delicate operations when the

remote camera is in a relatively stable position and there is not much movement. Faster video behaves better for moving situations, transmitting images straight from a CRT or LCD screen (ECG, EEG, etc) and plain videoconferencing with either the patient or the treating doctor. The “golden rule” was proven to be a setting relatively closer to “faster video” [Fig. 4.5]. The overall compression procedures would be analysed further in chapter 5.

Fig. 4.5 Microsoft NetMeeting videoconference settings:
balancing between faster video and better quality.

The communication procedure begins by powering up the laptop and camera on the mobile trolley and initiating wireless connection to the hospital’s network, through the WLAN card and the AP in the A&E room. About half a minute later, the mobile computer has received an IP address from the DHCP server of the hospital. The case is even easier when a static IP is associated with the specific network plug. By possessing any of the two IP numbers, (MedLAN’s or the consultant’s) one MNM software can page the other to initiate the communication. The receiving computer is prompted to accept the “call” and after doing so, two video windows are displayed on both screens (local and remote video).

As the bandwidth available by the WLAN usually fluctuates, the number of frames per second (fps) changes and both users experience this as a temporary “freezing” of the video. This is more apparent when the mobile

trolley roams from one cell to another (disassociating from one AP and associating with another). In normal operation, this freezing effect is less than 100-200ms for the former case but can reach up to 10 sec while roaming from cell to cell. This, however, is rarely needed as it would mean that the MedLAN trolley had to follow a patient moving from the A&E ward into another hospital room. Generally, the system displays an average of 13-18 fps when a single MT is used inside each AP [Fig. 4.6 middle left side]. As the number of MT terminals increases, the available fps decrease dramatically, mainly due to the conflicting packets of the WLANs: eight fps for two MTs and less than three for three MTs.

Finally, it is worth mentioning that as the compression factor is getting higher, more succeeding frames have to be taken into account to search for inter-frame similarities and achieve a better compression. This however does not apply for the sound that accompanies the video. As the number of frames increases, so does the delay between audio and video; something that is usually referred to as AV delay. There are software tricks that synchronise audio and video by actually delaying the audio as much as the video. This obviously introduces further delays than those already imposed by the transport layer. The relatively small AV delay of the MedLAN system (50-230ms) is considered low enough not to justify the use of the above AV-sync patches.

- An alternative to the MNM is the TeVeo Vidio Suite. Unlike MNM this program does not offer a complete videoconferencing solution as it can only handle video and not audio. It too, compresses the videostream to reduce the bandwidth needed but it also uses a relatively simple Java script to transmit the video directly to an Internet browser (Internet explorer, Netscape, etc) capable of supporting Java scripts. Since Microsoft Windows version 2000 and above have an embedded support for the Internet through the Internet Explorer) and these versions of IE include the ability of running Java scripts), TeVeo can transmit video to any computer or PDA that can run an Internet browser: the consultant simply has to know the unique IP of the treating doctor’s computer and type it in the address bar of his or her browser. The transmitting side would have already run the TeVeo client to monitor the videostream sent. In the case that the videoconferencing is needed to be both

ways (two video windows in each computer) the above procedure is repeated for the consultant's computer [Fig. 4.6]

Fig. 4.6 By using simple Java scripts, live video can be transmitted to any computer running an Internet browser by just knowing the transmitter's IP (top left).

The major advantage of this alternative is that a basic teleconsultation procedure can be initiated very quickly, without the receiving side having to have any special software or needed to install or configure any applications (like MNM). The disadvantage is that Java scripts do not usually support sound transmission so alternative means have to be used (landlines, mobile phones or even voice over IP software).

- Several other software packages were tested, including CUSeeMe, WebCam, ISpy, etc. Java scripts were either created or altered to investigate their usefulness in telemedical applications. With the exception of CUSeeMe which seems to have better settings control (it allowed the user to select or change the basic settings for the video and audio compression algorithm), other software fell into two categories. Videoconferencing software where both parties needed special software installed on their computer, or Java scripts that only require the transmitting party to run any special software.

Overall, MNM was proven to perform relatively well and coped better with bandwidth fluctuations introduced by the WLAN system than any of the alternatives. TeVeo was simple to use and introduced the lowest overall delay between sender and receiver, as it did not buffer any frames: as soon as the frames were ready to be transmitted, TeVeo sent them to the application layer. This, however, was only done at the cost of high frame rate fluctuation. Fig. 4.7 illustrates this problem.

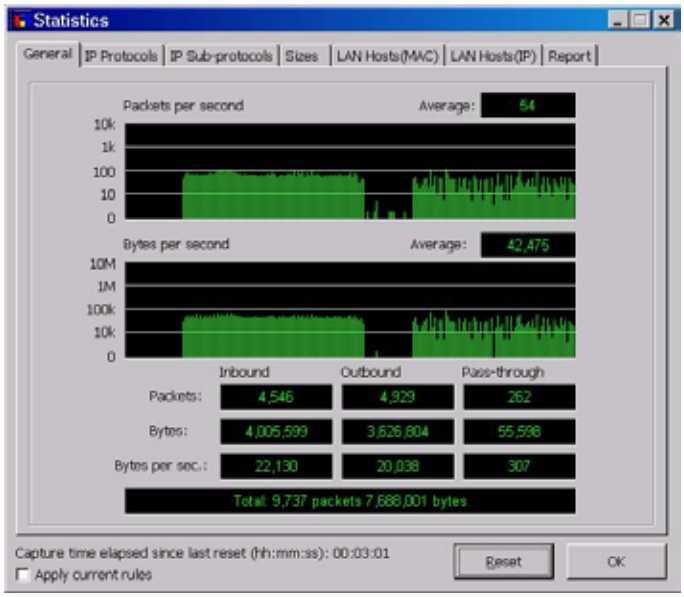


Fig. 4.7 comparison between the transmissions of MNM (right) and TeVeo (left) in terms of bandwidth fluctuation.

MNM buffered a sufficient number of frames, to be able to transmit video and audio with much less fluctuation, in comparison with TeVeo.

4.3.2 Audio

The audio of the MedLAN system is usually transmitted alongside the video when software like MNM is used. It, too, is compressed to limit the amount of bandwidth used and/or improve the audio quality within a limited bandwidth.

As MNM has an integrated solution for videoconferencing, it also supports compressed sound transmission. The user is given the opportunity to either leave the computer to decide the suitable compression algorithm, or set one manually using the advanced sound settings. From those available G.723 is a standard audio compressor sampling a single sound channel at 8KHz and output 6.4Kbps of sound

data [ITU96]. This compression algorithm was proven sufficient for average scenarios when the two doctors needed only to verbally communicate among them.
In the case that an external sound source was connected to the system (electronic stethoscope, ultra sound monitor, etc), alternative compressors performed better. Adaptive Differential Pulse Code Modulation (ADPCM) and CCITT's A-law and u-law produced less noise and clearer sound outputs, as judged by the doctors. Below is a table of the available sound compressors with their corresponding data rates.

	Sampling rate	**Bits**	**Max frequency transmitted**	**Bandwidth occupied**
G. 723	8kHz	8	4kHz	6.4kbps
ADPCM	8kHz	4	4kHz	8kbps
A-law	8kHz	8	4kHz	8kbps
u-law	8kHz	8	4kHz	8kbps

Table 4.1 Sound compressors available on the MNM

MNM also supports full duplex communication (transmit and receive sound simultaneously). This function depends on the sound card used, although most sound cards today support this feature. Furthermore, it can automatically adjust the sound level to accommodate for very high or very low level sounds. Finally, it detects silence by allowing the user to set a threshold below which, the programme assumes that no sound is being generated. This has the advantage of saving bandwidth and limiting the background noise in a noisy environment but also introduces the danger of not transmitting a low level sound.
The overall audio quality is dependant on the electronic properties of the audio hardware used including microphone, cables, earphones, etc. Using a low quality microphone with an unshielded cable led to the system picking up noise from various sources and retransmitting them to the channel. Not only was the sound unclear, but since the noise was constant, the sound threshold control could not get into effect thus wasting precious bandwidth. This bandwidth was eventually taken from the bandwidth destined for the video, thus reducing video quality.
Finally, and despite the relatively low sampling frequency of the sound, the system performed very well in retransmitting audio from other sound sources. Heart and lung murmurs have a low maximum frequency. Nyquist theorem states that when

digitising a sound, the maximum frequency reproduced is half the sampling rate. As in most cases the sound is sampled at 8kHz, the reproduced sounds can vary from 0-4kHz; much more than needed for heart and lung sounds (a telephone line permits frequencies up to 2.4kHz).

4.3.3 Still images

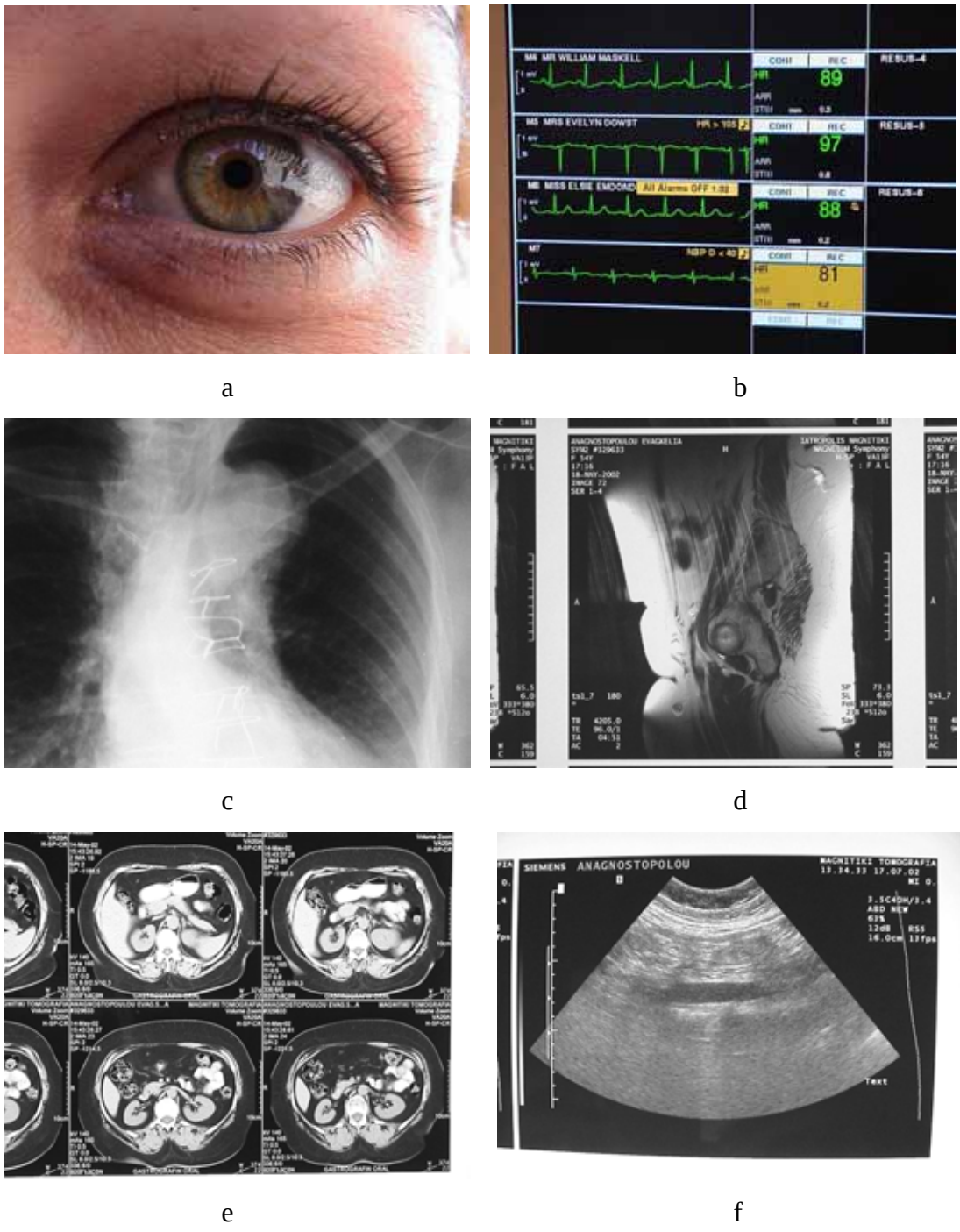


Fig. 4.8 MedLAN still image transmission: a. macro detail of a patient. b. camera pointing on a TFT ECG screen. c. chest x-ray. d. Computed Tomography. e. Magnetic Resonance. f. Ultra sound film

One of the most highly used functions of the MedLAN system is its ability to send high quality still images to the consultant's side. These images can be films (x-ray, MRI, CT), images directly taken from a patient (skin, injury, various details) or images pointing at an object (ECG monitor, hardcopy results, patient records, etc) [Fig. 4. 8]

This procedure elevates the teleconsultation procedure into a higher level: up until today the consultant has often found that the resolution and general quality of the videostream did not provide support for accurate diagnosis as it was usually poor in quality and limited to the resolution of a television (720x576=0.4 Mega pixels). By having a quality digital camera to take snapshots of images and transmit them to the consultant, he or she can deliver easier, faster and safer diagnosis.

The use of a high quality camera pointing directly to the observed object permitted total mobility of the MedLAN system by eliminating the need for wires, and also performed better than initially expected (the use of direct cameras in telemedical applications has been proven very valuable [Kru00]).

The system uses a high quality Carl-Zeiss lens capable of auto focusing from zero to infinity and features auto white balancing in all lightening conditions. It has a CCD with a maximum resolution of one Mega pixel and can optically zoom 6x (independently of the 4x digital zoom). Its output is compressed as a JPEG with the user having the choice of three alternative compression levels and two available resolutions. Its maximum file size is just over half a MB. Below is a table summarising all the available resolutions, compressions and file output sizes of the still images.

	1152 x 864	**640 x 480**
Low compression (5.5:1)	520KB	180KB
Medium compression (10.3:1)	220KB	100 KB
High compression (14.3:1)	100KB	55KB

Table 4.2 Still image file sizes depending on resolution and level of compression

These images can also be converted to any other file format (including the DICOM format). Additional information can also be added and they can be stored into a patient's record. Further information about compression and DICOM compatibility will be given at chapter 5.

The way these images are transmitted is the store-and-forward method: the digital camera stores the images in its internal memory (it can vary from 4MB to 2GB being able to accommodate thousands of images of various resolutions, according to Table 4.1) and then retransmits the image, as a file to the consultant's computer. From then on, the consultant can use any image viewer to view, zoom, enhance, and generally process the image. He or she can easily use this image to amend patient records or, (since it is already digital), forward it as an attachment to an email.

Generally, the quality of the images was very satisfactory. The worst-case scenario was when capturing x-ray films (and generally black and white films with variety of grey scaled areas). As the system tried to compress the image, it created some similarities when there were none. This, however, was done in a very small scale and the output retained its diagnostic value. Finally, as the black and white films needed to be placed in a transparency viewer (fluorescent light) to be photographed, it was often better to adjust the brightness of the camera manually, to bring out the details of the film as the camera tended to get "fooled" by any remaining light from the transparency viewer [Fig. 4.9].

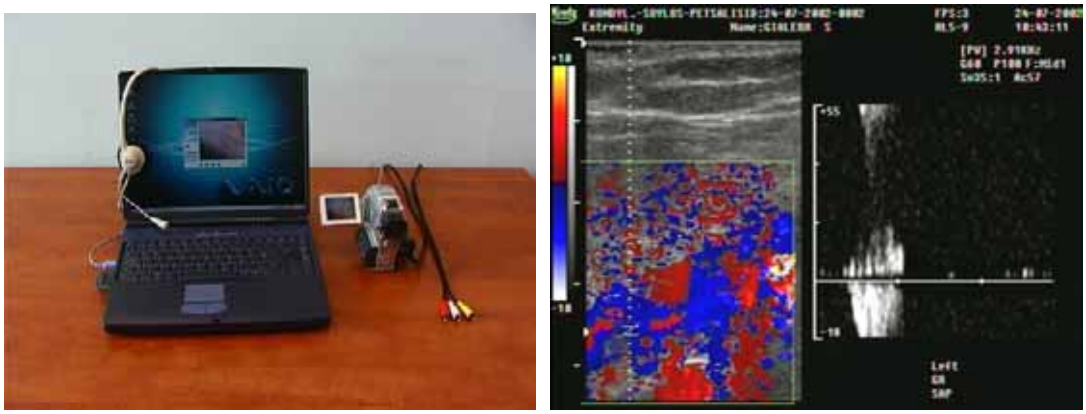
Fig. 4.9 Still images were better captured using "manual exposure" as escaping light for the transparency viewer (right) tends to "fool" the camera's auto-brightness function.

4.3.4 Connecting to an external device

The MedLAN system also has the ability to connect to an external medical device and transfer video, audio and still images from that device to anywhere in the network. Obviously, by connecting to any device through wires the MedLAN system will lose its mobility. Nevertheless, having a very light device that freely moves

around the A&E ward **until** it gets connected to any device also presents advantages as the cables will only be connected at the last possible moment.

These kinds of devices were usually ultra sound monitors, endoscopes, electronic stethoscopes, etc. With the exception of the latter (being small and mobile), the remaining devices usually could output a video signal either through a RCA (coaxial) video cable or through a S-Video cable. Both of these cables can be input to the MedLAN system. One sound channel can also be carried through a RCA coaxial cable [Fig. 4.10].



a b

Fig. 4.10 a. The MedLAN system is capable of connecting to an external device and retransmit video, audio and still images. b. Connecting to an ultra sound monitor and wirelessly retransmitting its video

The overall performance of the system while connected to an external device, followed precisely that of when the system was operating on its own. The real-time hardware video encoder does not differentiate between these two scenarios, so as far as it was concerned it was just transmitting video.

There was a visible improvement when using the S-Video cable instead of the classic coaxial RCA to carry the video signal. That is attributed to the fact that S-Video achieves a better signal to noise ratio by transmitting the chrominance and luminance signals separately so the need for composite signal filtering is eliminated.

Finally, high-resolution still images of the external devices can also be taken by the digital camera by connecting internally in the device's output and without having to point the camera to the output screen. Unfortunately, as these images are destined to be viewed on a television monitor (720 x 576 pixels) the resolution cannot be as high as the digital camera can support.

4.3.5 Wireless network access

In addition to the above services, MedLAN also permits its user to wirelessly access the hospital network and perform any task that would require the use of a computer connected to the wired part of the network (file transfer, print, amend record, access the Internet, etc). This presents a significant advantage, especially in the A&E ward where the computer access sometimes becomes a problem: too many people demand access to a computer for emergency needs, while there is usually lack of space to accommodate a greater number of terminals. That, coupled with the fact that cables present a potential danger in the A&E rooms, makes the MedLAN system ideal for these kinds of applications.

The system connects at a nominal speed of 11Mbps (as all IEEE 802.11b WLANs) but has an actual speed of about a third of that (3-4Mbps). That permits for fast file transfer or any other kind of bandwidth demanding application.

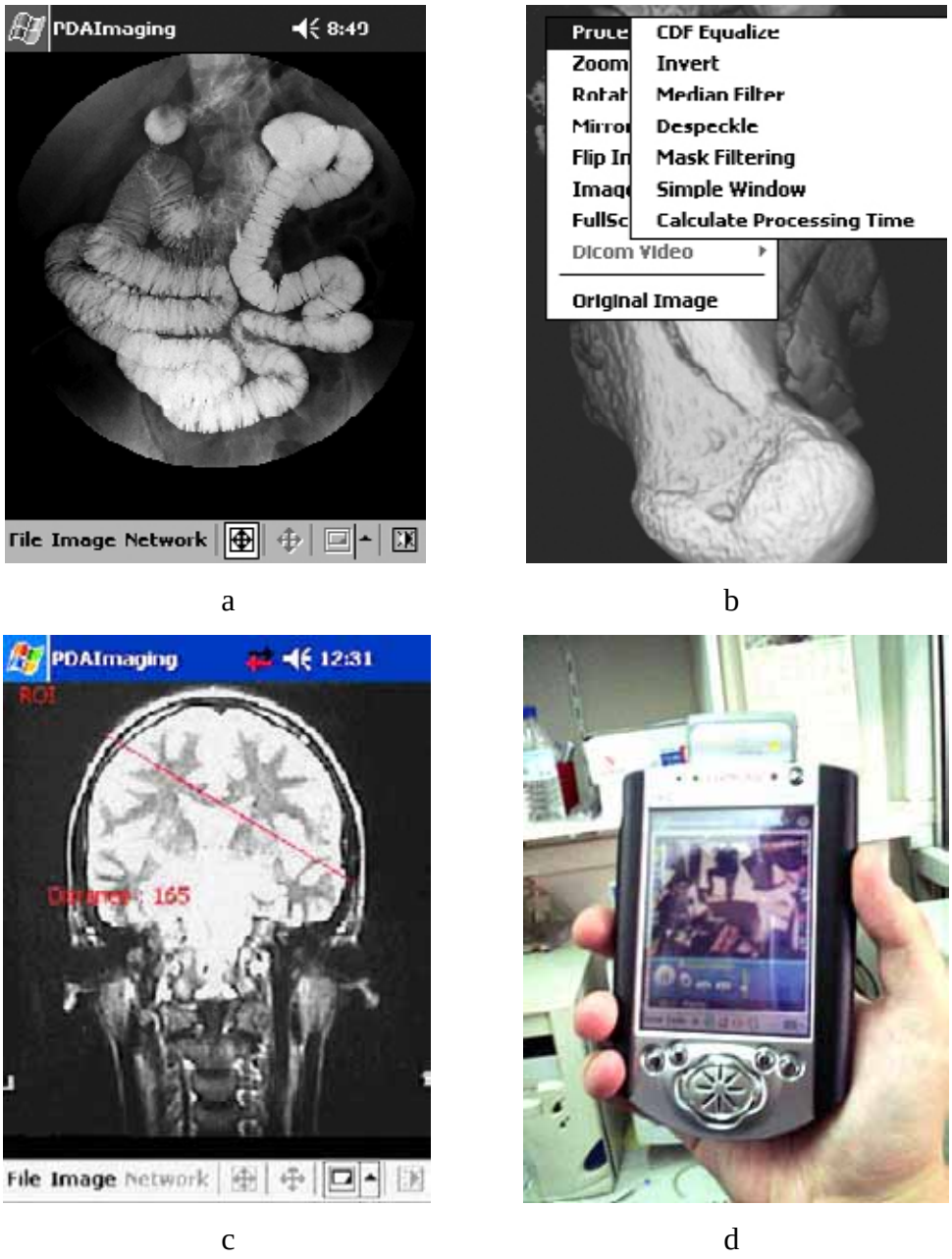
As the above procedures have no need for QoS, the users reported that wireless network access performed very satisfactorily fulfilling any potential need in the A&E ward.

4.3.6 Using a PDA at the consultant's site

Further to the consultant viewing the MedLAN output on a computer screen, there is scope for providing the end user with the same mobility advantages as in the A&E ward. In that sense, a Personal Data Assistant (PDA) device can be used by the consultant as a communication device. Using a PDA has a number of advantages:

- It is very light (150g) and thus can be carried easily.
- It supports a resolution of 320 x 200 x 16 colour depth that can handle live video, audio, and still images.
- Newer PDA versions have internal IEEE 802.11b support so no additional PCMCIA WLAN card is needed.
- It can perform all the necessary functions usually performed by a desktop computer (save, open, zoom, pan, etc).

Concerning the network coverage, there are two solutions: either extend the WLAN to the entire hospital by placing multiple APs and performing frequency planning (as explained in the previous chapter) or install an AP close to the consultant's office to allow for mobility on a radius of about 50m [Fig. 4.11].



a b

c d

Fig. 4.11 a. mobile PDA viewing a DICOM image b. zooming into the ROI c. performing basic measuring tasks in the PDA's screen d. streaming wireless video viewed in the PDA screen

The PDA component runs a Pocket PC 2002 operating system that supports Windows Media Player 9 (WMP) for viewing video and audio. Images are transmitted in the usual manner as files though the WLAN and can be panned to allow their full detail to be examined. Video, however, can have two alternatives: it can either be transmitted as a Java script output while the PDA's Internet browser connects to the A&E's IP, or it can be slightly buffered and transmitted in a fast

store-and-forward technique. The former is a simple solution but unfortunately does not output the quality needed as the frame rate of the video tends to fluctuate heavily. The most feasible solution that was dictated through experimentation, was to store a number of frames, compress them and them transmit them all together. Unfortunately, this introduced a 5-6 sec video delay due to compression but the frame rate was much more stable (up to 20 fps) and the video could also be accompanied by one-way sound.

Finally, several filters were embedded on the still-image viewing software of the PDA, in order to enhance the ability of the system to view DICOM images and perform basic processes on them [Fig. 4.11.a,b,c]

Overall, the use of PDA on the consultant's side was proven a valuable application that permitted mobility to the consultant at a range that was only limited by the range of the APs. Java scripts were developed in order for the videostream to be compatible with what the PDA expected. Unfortunately, sound and video could only be transmitted one way (A&E ward to consultant) as the PDA lacked the ability to handle real-time audio and video transmission. During the experimental phase this was compensated for, by using a mobile phone.

4.4 Range and scalability of the MedLAN system

As mentioned in the previous chapter, IEEE 802.11b allows clients to roam from one AP to another while retaining their connection to the network. This means that multiple APs can be placed in strategic locations around a hospital wards, or even cover the entire hospital, so MTs can roam around seamlessly while running real-time applications. It was also mentioned that 802.11b supports three independent channels. By carefully placing the APs to specific locations so they would not interfere with each other when the same frequencies are reused, the coverage can extend to include vast areas, much like the structure of GSM cellular telephony [Ban02b].

This introduces the concept of site survey and frequency planning: before any WLAN installation, specific tools that reveal the signal strength in the region of interest have to be used. Following that, the three independent frequencies have to be assigned in a way that the range of the AP using the first independent frequency,

does not collide with the range of the distant AP reusing the same frequency [Fig. 3.11]. Newer WLAN hardware has the ability to automatically select the least busy channel alleviating this burden from the communications engineer. Most of the site survey processes can be performed using software that comes with the WLAN client card [Fig. 4.12]

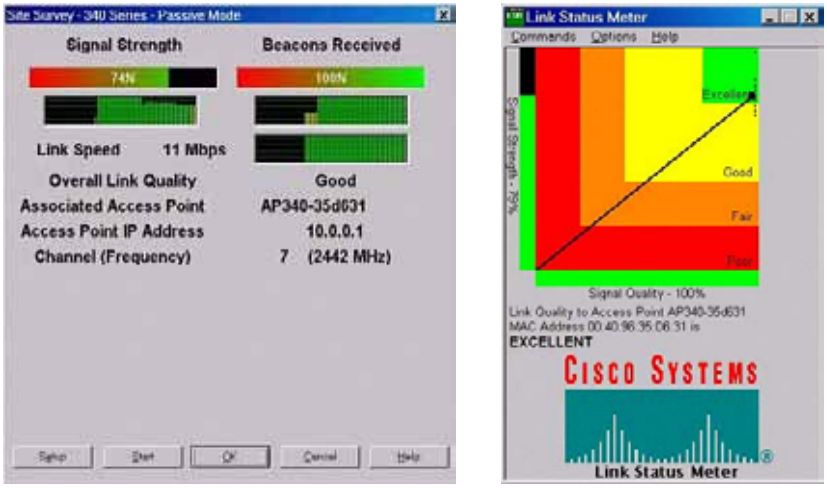


Fig. 4.12 Site survey tools provided by Cisco systems indicate signal strength and signal quality.

It is also important for both the management of the hospital and the developing engineer to note that [Ban02b]:

- The range of the WLAN system is directly related to the security of the system: the designer of the system should know which area needs protection.
- The range that the manufacturer suggests is much higher than the actual range of the WLAN.
- Although the PCMCIA card's transceiver will only work in the effective range, by the use of special antennae this range can be widely extended.
- It is only with a site survey tool and with the use of practical means that the developer can estimate the effective range of the WLAN. Simulation and modelling tools fail to take into account small details (walls, furniture, metallic surfaces) that greatly affect the WLAN range.
- As the signal quality of the WLAN is reduced, IEEE 802.11b falls-back in a lower speed to preserve the signal integrity. The fallback speeds from 11 Mbps are 5.5, 2 and 1 Mbps.

The site survey was the first action to take place in the Central Middlesex Hospital A&E ward when the WLAN was installed. Fig. 4.13 illustrates the range of two APs (marked in black circles), one installed in the majors (adults) and one in the minors (children) area of the A&E. The ranges overlap each other but without causing any interference as the lower user channel 6 and the higher (minors) uses channel 11. The specific range displayed in the figure represents connection at 1Mbps. As the need for speed increases, the range of the system decreases. Maps of the various WLAN speeds and ranges can be found in Appendix D.

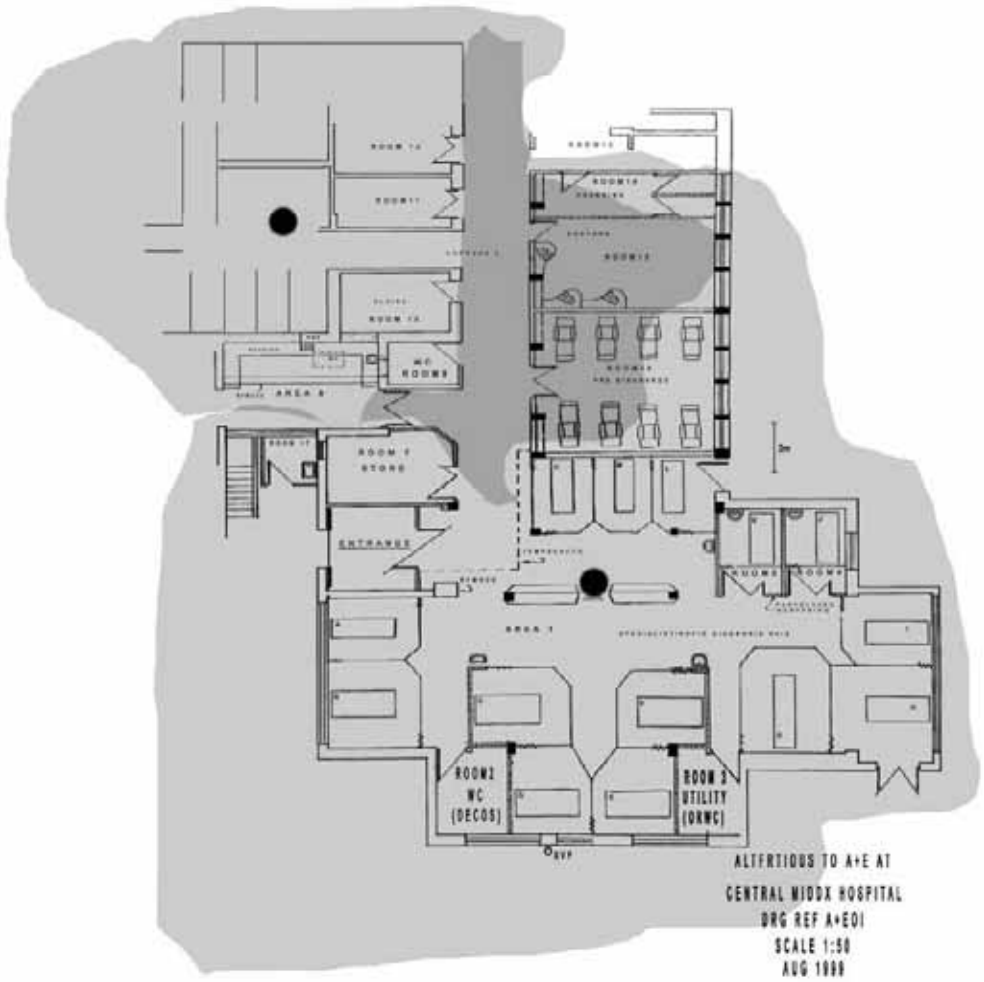
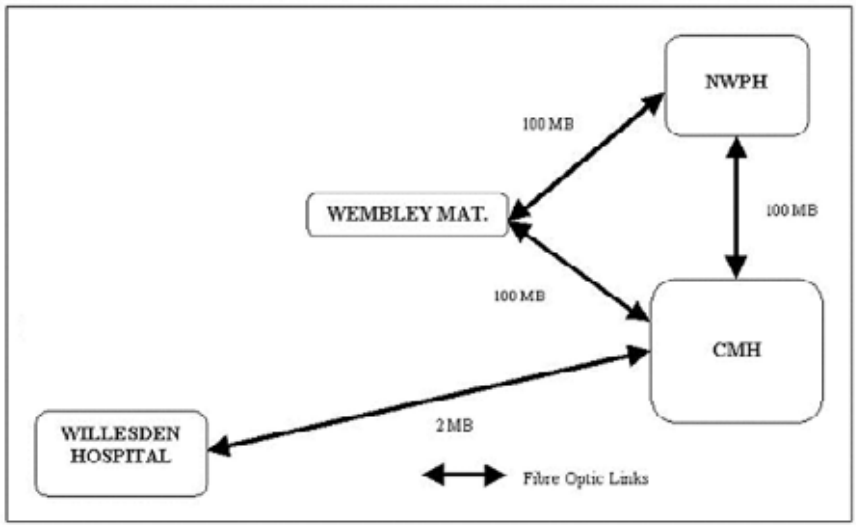


Fig. 4.13 The range of two APs as revealed after a site survey of the CMH A&E ward. The black circles indicate the position of the APs and the grey area indicate their range at 1Mbps

Both the APs are connected to the wired network of the CMH hospital and from then on, to the network of North West London Hospitals (NWLH) that includes NorthWick Park Hospital (NWPH), Wembley MAT and Willesden Hospital [Fig. 4.14].



Fig, 4.14 Basic structure of North West London Hospital network.
The MedLAN system can directly operate between any of those two hospitals.

Any teleconsultation operation that can take place within one of these hospitals using WLANs, can also be performed between any other two, as they all belong to the same network. All experiments (site survey, frequency planning, videoconferencing, etc) that were performed in CMH were also tested in NWPH and Wembley MAT. The results were the same (if not better) as in the CMH case, yielding that the MedLAN system performs adequately regardless of the environment. As an exception, NWPH enjoyed an even better reception of the radio signal. That is attributed to the fact that NWPH's A&E ward is built as a single room with no walls in between, in contrast with the thick walls of CMH's A&E.

4.5 Interference with medical equipment

The increasing number of wireless personal systems (WLANs, PDAs, mobile phones, pagers, etc) has led to an increasing concern of the possible interference that these systems might have with the existing medical equipment. No medical personnel or hospital administration could accept a system that might have an effect on the reliability of the existing medical instruments and thus on the safety of the patients.

Several studies so far have dealt with this both in the practical and theoretical aspects of the problem. It is however clear that unless practical measurements are taken in

the actual hospital environment, one cannot be certain of the effects that these electromagnetic frequencies might have on the medical hardware [Boi97], [Vla95], [Pha00], [You97].

Initially, it is crucial to distinguish between Electro-Magnetic Interference (EMI) caused by the use of narrowband radio transmitters, and that caused by spread spectrum radios. When referring to EMI from mobile radio, it is a common misconception to consider only mobile phones, especially GSM. Contrary to spread spectrum, GSM phones use a combination of Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA). They separate the available bandwidth to 128 channels (using FDMA) and each of these channels into eight time slots (TDMA) and assign one slot for each user operating his/her mobile phone at the time. This means that the mobile phone only transmits “bursts” of signals every eighth of the time turning its radio amplifier on and off continuously. This causes interference to any amplifier, speaker, radio, television and of course, some medical equipment built to amplify weak signals and consequently are sensitive to this kind of EMI [Fig. 3.4.b].

This is very different from the case when WLANs operate. As explained in the previous chapter, WLANs use a spread spectrum technique (usually DSSS) to spread their signal to the entire available frequency band. As they continuously transmit their low power signal, the chance of interfering with any device (medical or not) is minimal and always favours DSSS over FHSS.

Nevertheless, the US FDA developed a set of rules recommending that non life supporting medical electrical equipment should be resistant to background electric fields in the frequency range of 80MHz to 2.5GHz of 3 V/m (130 dBuV/m), increasing to 10 V/m (140 dBuV/m) for life supporting medical equipment [EMC01].

An extensive study of the possible effects of 2.4GHz WLAN operation into the hospital environment took place during 2003 in two US hospitals: the Virginia-Maryland Regional College of Veterinary Medicine (VMRCVM) at Virginia Tech and the Carilion Roanoke Memorial Hospital (CRMH) in Roanoke, Virginia giving emphasis to locations such as Emergency Rooms, Intensive Care Units, Surgery blocks and Radiology. [Kri03]

After setting up an infrastructure WLAN and with the help of a measurement test-bed (vertical dipole, sleeve antenna, low noise power amplifier and finally a spectrum analyser), the system took continuous readings of various floors and wards of both hospitals, for the duration of the day. The results, illustrated in Fig. 4.15, indicate that the worst-case emissions of WLANs are far below the levels of resistance proposed by the FDA (the curve found in the 2.44GHz frequency is due to the often operation of a microwave oven).

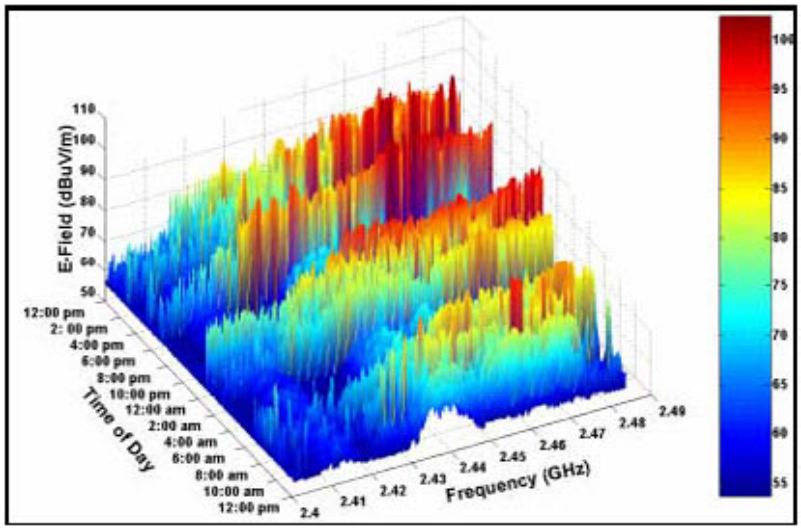


Fig. 4.15 worst-case EM emissions recorded from five measurement sites on the South section of the Carilion Roanoke Memorial Hospital over a period of 24h. All measurements fall under 130 dBuV/m

A past study in the Johns Hopkins Hospital performed in 1999, also dealt with the same issue. This study was performed at the dawn of the WLAN revolution and investigated the use of WLANs to fulfil patient record updates, while on the move. Several APs were placed inside the hospital and there was an emerging concern on the possible effects that these radio frequencies might have on the medical hardware. Contrary to the previous one, this study followed a different, yet effective path: it placed the WLAN radios near (or in contact with) several medical equipment and asked both doctors and engineers to check if they could witness any change in the operation of the medical instrument. Table 4.2 summarises the results yielded by this experiment.

Medical equipment	Power at 2.4GHz	Hospital	Effect
Bunnel ventilator monitor	100 mW	John Hopkins	No visible interference
Escort MDE remote EKG	100 mW	John Hopkins	Readings affected 5-120 cm depending on the radio position
Fenwal blood warmer	100 mW	John Hopkins	No visible interference
Healthdyne infant monitor	100 mW	John Hopkins	No visible interference
HP 78173A ECG	100 mW	John Hopkins	No visible interference
Imed Gemini PC-2 infusion pump	100 mW	John Hopkins	No visible interference
Marquette physiological monitor	100 mW	John Hopkins	No visible interference
Nellcor pulse oximeter	100 mW	John Hopkins	No visible interference
SensorMedics 3100A oscillator ventilator	100 mW	John Hopkins	No visible interference

Table 4.3 Interference of IEEE 802.11b WLAN
with existing A&E medical devices in John Hopkins Hospital

Using the same procedure, the same experiment was performed in both CMH and NWPH during spring of 2002:

- Each of the devices usually found in an A&E ward or Resuscitation Room was tested with emphasis on oscilloscopes, as these tend to be the most vulnerable to EMI.
- Both the client PCMCIA card and the access point were placed in a number of different positions near or on the device in question.
- To ensure realistic conditions, all the above devices were connected to one or more patients and possible changes in their vital signs were examined both by doctors and by technicians.

Below is a table that summarizes some of the most frequently used equipment that can be found within an A&E room along with the possible interference that the MedLAN system could cause in such equipment. No visible interference was noticed in all the medical equipment tested in CMH and NWPH.

Medical equipment	Power at 2.4GHz	Hospital	Effect
HP 78353 BU	30 mW / 50mW	CMH A&E	No visible interference
VDU monitors	30 mW / 50mW	CMH A&E	No visible interference
HP Page Writer Xli	30 mW / 50mW	CMH A&E	No visible interference
LIFEPAK 8 cardiac monitor	30 mW / 50mW	CMH A&E	No visible interference
Agilent Page Writer 300pi	30 mW / 50mW	CMH A&E	No visible interference
Nova SI and Profig Nutra	30 mW / 50mW	CMH resuscitation	No visible interference
Passport XG Datascope	30 mW / 50mW	CMH resuscitation	No visible interference
Propaq encore	30 mW / 50mW	CMH resuscitation	No visible interference

Table 4.4 Interference of IEEE 802.11b WLAN
with existing A&E medical devices in CMH and NWPH

Conclusively, several experiments (both practical and theoretical) indicate that the emerging concern about the possible effects that WLAN emissions might have in hospital equipment is unfounded. This is attributed to the use of spread spectrum technologies by the WLAN hardware (especially DSSS) and is very different than TDMA used by mobile phones.

4.6 Testing phase evaluation

Overall, a great number of visits were made to all NWLHs and in all of them various parts, procedures and alternatives of the MedLAN system were tested, along with all tests made to the laboratory. In all of these visits and from the moment the first MedLAN prototype was used in CMH's A&E ward, a record was kept of the opinion of the various personnel using the system, along with the opinion that the patient had when using MedLAN on them. Below is a summary of these records indicating the general acceptance of the system. The results concerning the validation of the specific system's outputs will be presented in the next chapter.

4.6.1 Doctors in the A&E ward

Treating doctors seem to be the most enthusiastic group. They understood the system as something new and original in the Telemedical application field. As they were the ones working in the A&E ward, they looked at the system as something that has the potential to alleviate some of the burden of the A&E procedures since mobility leads to effectiveness and better time utilisation.

As some of these doctors had basic computer training and experience, they were eager to try the system out and to provide all necessary sources for the test. They were, however, reluctant towards the possibility of jeopardising the confidentiality of the patient and often requested the support and cover of the upper management.

4.6.2 Consultants

Consultants were very positive in their initial comments. As they were they ones suggesting the system in the first place, after witnessing its development from birth, they were contempt when the prototype of the system began operation. Their first observation was regarding the frame rate fluctuation and the small delay between the sender and receiver that was made noticeable as at that time, landline phones were also used to verify correct operation.

After some of the glitches were corrected, they continuously requested for system improvements, as they understood that the potential of the system was greater than initially planned. Some of their requests include the transmission of the MedLAN's output at their home through the use of DSL lines, being able to use 3G mobile device to view video and having access to the MedLAN system from outside the NHSnet.

Most of the problems were regarding the system's output quality of films (x-rays, US, MRI, CT). Doctors felt uncertain that finer details will be able to be recognised as they were long used to viewing films on transparency viewer. After some brightness adjustments experiments, the results were satisfactory (Chapter 5).

4.6.3 Nurses / healthcare personnel

Most of the nurses did not seem to grasp the potential of the system and remained distant from its use. They were more active in providing initial care for the patients in the A&E, rather than investing time to learn about a system that would be used in the future. The fact that in its initial stage, the system tended to take some precious space in the A&E benches, made their feeling towards the system slightly negative.

4.6.4 Patients

As expected, patients were reluctant about the possibility of using MedLAN to transmit their data to a distant point. This can be attributed to several reasons: Initially, being in the A&E room as patients inclined them to worry more about their current health, rather than the potential of the system. Additionally, when explaining to them that their images and video will be transmitted to a distant location there was concern about the overall security of the system and of the possibility of others viewing their personal data. Finally, it was difficult to explain to some of the patients the basic procedures that the system uses. All the above were made even worse when dealing with older people. There were of course, many patients that were enthusiastic about the possibility that a system so technologically advanced will be used for their own benefit.

To avoid any mishaps and to ensure the legality of the hospital's actions against the patient, a "patient acceptance form" was developed to be signed by the patient [Appendix E]

4.6.5 Overall results

From the testing phase and by using both the feedback forms and the subjective opinion of all the groups previously mentioned, a summary of the acceptance of the MedLAN system could be created. The population used to create this output, included 7 consultants, 15 doctors and 23 nurses from the A&E department and more than 35 patients. All of these groups were asked to evaluate different aspects of the MedLAN system: among other questions, consultants and doctors were asked about the effectiveness, ease and fidelity of the system. Nurses were asked about the practicality of the system and the degree at which it might interfere with their work. Finally, patients were called to answer if the use of the system increased their uneasiness or their concern regarding security.

Of the above groups, the entire population of both doctors and consultants evaluated MedLAN as a system that can have a positive effect in treating a patient. Most of the nursing staff (70%) felt that this was a positive step; the rest were mainly concerned about the possible effects that the deployment of such a system might have in their working environment. Finally, an average of 60% of the patients thought that they

would benefit by the use of such a system, while the rest either did not fully understood its potential, or seemed slightly intimidated in trying new technology.

4.7 Conclusions

When evaluating a telemedical system, the objective is to prove that the healthcare data provided by telemedicine is as useful as those provided by conventional means [Nor02]. As the MedLAN system was developed as an improvement to existing videoconferencing systems, our task was to prove that it works as well as (or even better than) these conventional systems.

In that sense, we have presented the system and its abilities and gave a general description of its components and the way the data flows from one end to another. We have then elaborated on the services that the system can offer (live video, audio, still imaging, connection to external sources and wireless network access) along with its performance in each of these cases. We have also discussed the possibility of MedLAN interfering with existing medical equipment, before we discharged it as not applicable in the case of DSSS WLANs. Finally, we have presented a record of the remarks and opinions from the persons using the system.

Overall, the MedLAN system proved that it can perform satisfactorily in a variety of scenarios and can outperform existing telemedical systems while having a relatively low cost of installation and maintenance. This, coupled with the fact that it is completely open-sourced and easily upgradeable (in order to adapt to new trends in communication technology), makes the system ideal for use in a number of healthcare applications.

Although the main characteristics of the system were evaluated (mostly using practical means and observations), a detailed comparison between MedLAN's outputs and conventional means used until today will be presented in the next chapter, with emphasis on the still imaging of the system.

5. Adjusting DICOM Specifications in a Wireless LAN System

5.1 Introduction

As the need for electronic transfer and storage of medical images seemed to increase over the years, there was a definite need for standardisation of the format of those images. Up until some years ago, the scenery of medical imaging seemed hazy with medical images extended to different formats, resolutions, frame rates (video), colour depth, contrast, etc. Digital Imaging and Communications in Medicine (DICOM) standard has been developed to serve the needs of manufacturers and users of medical imaging equipment, for interconnection of devices on standard networks [DIC01]. Its multiple parts provide a means of expansion and updating.

The design of the standard aimed at allowing simplified development of all types of medical imaging. It also described a hierarchical structure of communication between medical and storage / retrieval devices, as well as specifications on patient records. Simply put, DICOM provides a set of specifications for interconnection of medical devices.

In the MedLAN case, however, the limited available throughput of a WLAN system makes the use of high demanding specifications, such as DICOM, problematic especially when no compression during transmission is used.

In this chapter, there will be a description of the DICOM specifications and the consequences that this poses to a transport layer of a WLAN. More specifically, transmission of still images (x rays, CT, MR, etc), video (patient live video, ultra sound scan, etc) and sound (heart, lung murmurs) over a WLAN link will be investigated and will be contrasted with the DICOM recommendations. Specific attention will be given to still images [Ban03].

5.2 DICOM recommendations

After the introduction of Computed Tomography (CT) and other medical modalities some years ago, the American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA) recognised the need for information exchange between medical devices. (until then, devices by different manufacturers produced a variety of different file formats). For that reason, ACR and NEMA formed a joint committee in 1983 (ACR-NEMA) to develop standards to [DIC01]:

- Promote communication of digital image information, regardless of device manufacturer.
- Facilitate the development and expansion of Picture Archiving and Communication Systems (PACS) that can also interface with other systems of hospital information.
- Allow the creation of diagnostic information databases, which can be interrogated by a wide variety of devices distributed geographically.

These standards were later referred to as DICOM.

It is important to understand that DICOM standards keep evolving by applying enhancements proposed by members and other interested parties. This is crucial in order to accommodate for future developments in technology. One such "adaptation" of the DICOM standards will be presented in this chapter and concerns the use of WLANs in medical image transmission.

5.2.1 Scope of DICOM

The DICOM Standard facilitates interoperability of medical imaging equipment by specifying [DIC01]:

- A set of protocols to be followed by devices claiming conformance to the Standard.
- The syntax and semantics of Commands and associated information, which can be exchanged using these protocols.
- Information that must be supplied with an implementation for which conformance to the Standard is claimed.

However, the DICOM Standard does not specify for the implementation details of any features of the standard on a device claiming conformance, the overall set of

features and functions to be expected from that system, nor a testing / validation procedure to assess an implementation's conformance to the standard.

In essence, DICOM standards deal with the field of medical imaging and within that field it addresses the exchange of information between medical imaging equipment [Fig. 5.1]

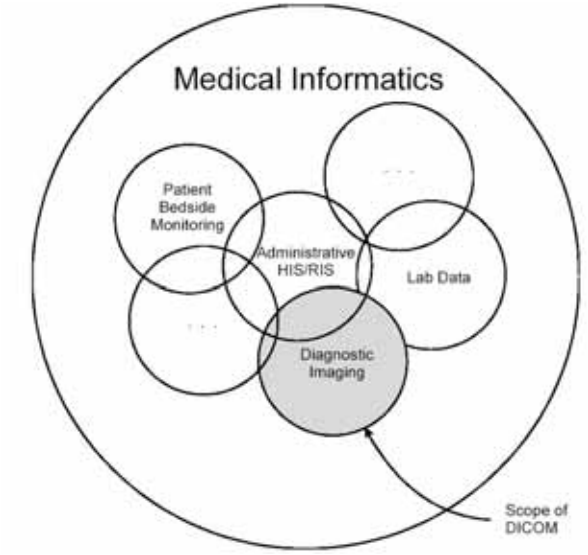


Fig. 5.1 Scope of DICOM in medical informatics

5.2.2 Goals of DICOM standards

From the moment of their creation, DICOM standards offered a basis for interoperability of medical devices conforming to the DICOM suggestions. More specifically DICOM [DIC01]:

- Addresses the semantics of interoperation commands and associated data (for devices to interact, there must be standards on how these devices are expected to react to commands and associated data).
- Is explicit in defining the conformance requirements of implementations of the Standard. In particular, a conformance statement must specify enough information to determine the functions for which interoperability can be expected with another device claiming conformance.
- Facilitates operation in a networked environment.
- Is structured to accommodate the introduction of new services, thus facilitating support for future medical imaging applications.
- Makes use of existing international standards wherever applicable.

5.2.3 Structure of DICOM standards

The DICOM standards are structured as a multi-part document. Depending on the application used, some or all of these parts are to be used to ensure conformance and interoperability. In summary, the following sixteen parts describe its possible operations (a more detailed description can be found in Appendix F):

1. Introduction and Overview
2. Conformance
3. Information Object Definitions
4. Service Class Specifications
5. Data Structure and Encoding
6. Data Dictionary
7. Message Exchange
8. Network Communication Support for Message Exchange
9. Point-to-Point Communication Support for Message Exchange
10. Media Storage and File Format for Data Interchange
11. Media Storage Application Profiles
12. Storage Functions and Media Formats for Data Interchange
13. Print Management Point-to-Point Communication Support
14. Grayscale Standard Display Function
15. Security Profiles
16. Content Mapping Resource

Number 8, “Network Communication Support for Message Exchange “, number 5, “data structure and encoding” and more specifically, number 10, “media storage and file format for data interchange”, deal with the way that images are displayed, stored and compressed. This will be explained further during this chapter and will be contrasted against the abilities of the transport layer of a WLAN.

All the above parts, and the way they are combined together, are illustrated in Fig. 5.2

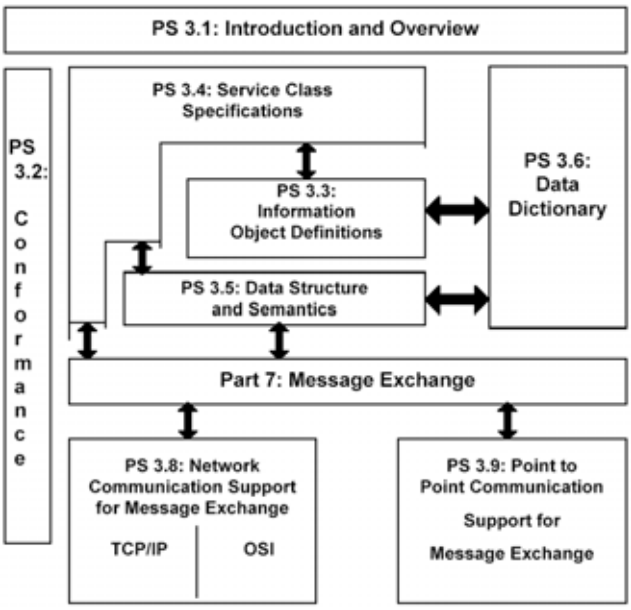


Fig. 5.2 Relationship of the first nine parts of the DICOM standards as they appear on the specification manuals. Depending on the application, some or all of them are used.

In general, the operations of the DICOM model can be mapped to the seven OSI layer model described in chapter 3 [Fig. 5.3].

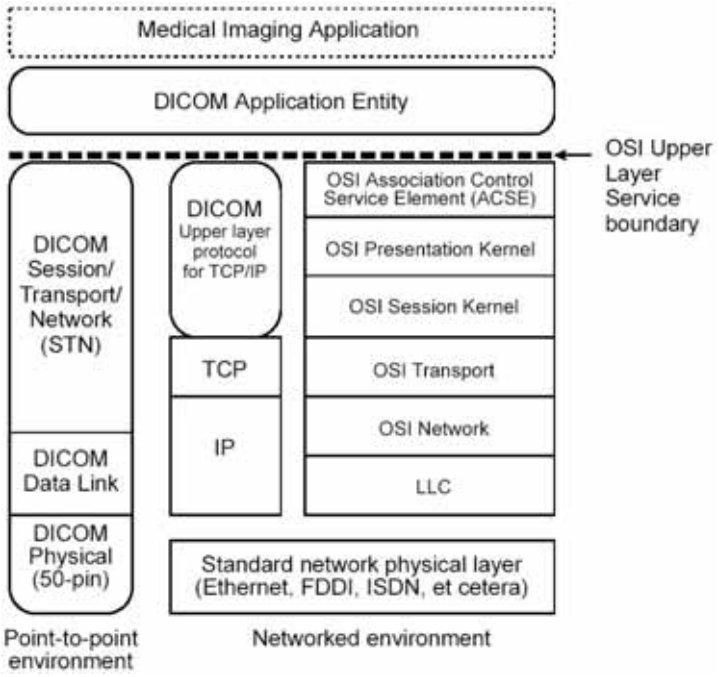


Fig. 5.3 Mapping the OSI 7-layer model to the DICOM model: two more layers exist in the DICOM

5.2.4 DICOM image format

By far, the most valued DICOM application is the representation and storage of still images (x-rays, CT, MRI, etc) and limited frame rate videos (angiography, ultrasound, etc). All modalities supported by DICOM, along with their specific characteristics, are presented in Appendix G. Network access to patient record and medical equipment interoperability are also important tasks but will not be discussed in this chapter.

One of the changes that DICOM imaging has introduced, is the use of a composite image: apart from the actual image information, there exists a text file about a page long, that offers information about the image: modality, size, data, time, operating doctor, patient's name, findings, etc. This has been proven crucial to the effective use of medical images as it can include information on actual image metrics. It can also eliminate the danger of the image being mistaken or misplaced. The initial DICOM versions kept this additional text file as a separate document, so each medical image stored was represented by two files: one *.hdr and one *.img (analyse format). Newer versions contain both header and image data on the same file. The image data can also be compressed using lossy or lossless variants of JPEG as well as run-length encoding format. An analysis of a modern DICOM header (single file) reveals its basic structure: the first 794 bytes are used for the DICOM header that describes the dimensions of the image to follow, along with other details (mentioned above). The image data follows the header information, as they are stored under the same file.

DICOM requires a 128-byte preamble (usually set to zero) followed by the letters "D", "I", "C", "M". After that comes the header information that is organised in groups; group 0002h, for example, is the meta file information group and contains three elements: group length, file version and transfer syntax. The DICOM elements that are required to effectively view a modality (described in part 3) depend on the image type. As an example, the image modality "MR" should have an element in its header describing the MRI echo time. Absence of this kind of information is a violation of the DICOM standard, however, most DICOM viewers will still consider these images as valid and allow proper display.

ACR-NEMA has proposed guidelines for equipment, covering two basic categories of teleradiology: small matrix size (e.g., computed Tomography (CT), magnetic resonance imaging (MR), ultrasound, nuclear medicine, digital fluorography, and digital angiography) and large matrix size (e.g., computed radiography and digitised radiographic films). A small matrix is typically 512 x 512 resolution at minimum 8-bit depth for processing, manipulation, and subsequent display. A large matrix allows a minimum of 2.5 lp/mm spatial resolution at minimum 10-bit depth (translating to about 2048x2048 pixels).

Furthermore, ACR/NEMA also suggested that reversible or irreversible compression could be applied to those image matrices, to reduce their storage size and facilitate easier transmission, as long as there is no reduction of information necessary for a diagnosis. However, the current trend concerning DICOM images is that there is benefit in storing uncompressed medical images, as the possibility of losing valuable information is minimised. (Further suggestions made by the ACR-NEMA concerning still image capture and storage, can be found in Appendix H [ACR99])

5.3 Image and video compression

Before further discussing the compression of DICOM images, it is useful to explain some fundamentals of image and video compression.

In a number of applications, our needs tend to grow much faster than the technology can keep up with: the demands for speed in the Internet connection, CPU processing ability, transmission of high quality video and audio, higher media storage capacity, etc. One can consider the example of a plain video stream being transmitted over a digital channel: for a European PAL system it has to have 720 x 570 pixels with a 24 bit colour depth, 25 times per second (fps). For a 90 minute movie, this translates into: 720 x 570 x 24 x 25 x 60 x 90 = 1329696000000 bits (approximately 1.2TB); a volume too large to be handled by today's storage media. For that reason, the need for compressing data (multimedia or other kind) became apparent, especially during the last fifteen years.

Compression algorithms in general, fall into two categories: **entropy encoders** that manipulate bits regardless of their meaning while being fully reversible and **source encoders,** which take advantage of the bits properties to provide better compression

while sacrificing some of the original information. For obvious reasons, the former algorithm is preferred for data applications while the latter is more desirable for multimedia. An example of a fully reversible algorithm, would be the operation of a widely-used compressor; ZIP (Winzip or PKZIP) to reduce the size of a program file: it will search throughout the file for groups of similar bytes and will store the group's contents and the places where these group appears. This procedure reduces the size of the file by an average factor of 0.5 (50%). The reverse procedure creates a file identical to the original.

Even with this definite gain though, it would be impossible to fit most of multimedia applications in conventional storage media. For that reason, more advanced techniques came in use.

Source encoding usually applies to images or image sequences (video). Like the entropy encoder, it also manipulates the image bits searching for groups of similar properties (chrominance and luminance) to pack them together thus reducing the image size to about a half. The major difference is that if it does not find any similarities, it **creates** some by forcing pixels that have similar properties to act as a group of pixels with the **same** properties. This "forcing" of similarities is controlled by the user and it balances quality over size: the higher the compression, the less the file size. The less file size, the less image quality, as the loss of the original information is apparent.

In general, image formats that use a fully reversible procedure include: .TIFF, .PCX, .GIF, .BMP while formats that usually lose some information during decompression are: .PNG, .JPG, with the latter being the most widely used format, as it is the de-facto form for Internet images.

It is obvious that if an image has a high percentage of similarities (areas with the same colour or brightness) the compression algorithm will perform better than in a case of high detail and smooth colours. This introduces the term "entropy" that simply describes the "randomness" of things. The higher the entropy in an image, the lower the compression.

5.3.1 JPEG

JPEG (Joint Photographic Expert Group) group provides the syntax and the method for compressing still images [Ric02]. The JPEG standard includes a set of features

designed for a wide range of applications. Further optional modes are defined to extend the capabilities of the baseline codec.

JPEG operates in the following way: the image to be compressed is divided into several 8 x 8 pixel blocks and each is processed in a zig-zag manner [Fig. 5.4]

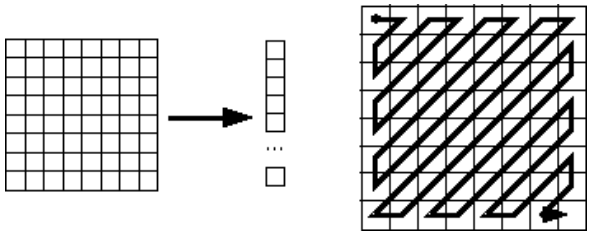


Fig. 5.4 zig-zag scan used by the JPEG algorithm

This allows for the grouping of low frequency coefficients in top of vector and the transformation of the 8 x 8 blocks into a single 64-element vector. Colour components (RGB or chrominance and luminance) may be represented separately or interleaved. Each of the 8 x 8 blocks is coded using the procedure illustrated in Fig 5.5.

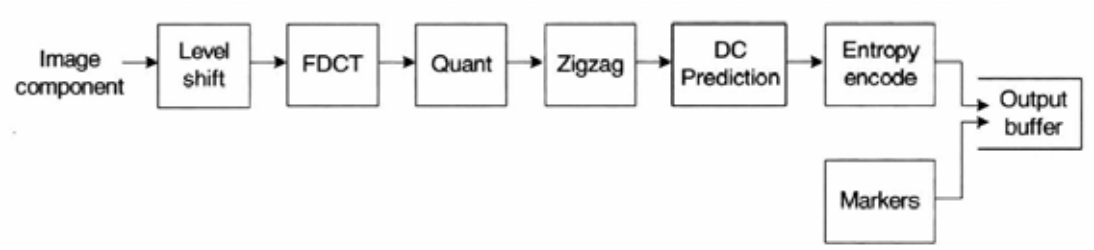


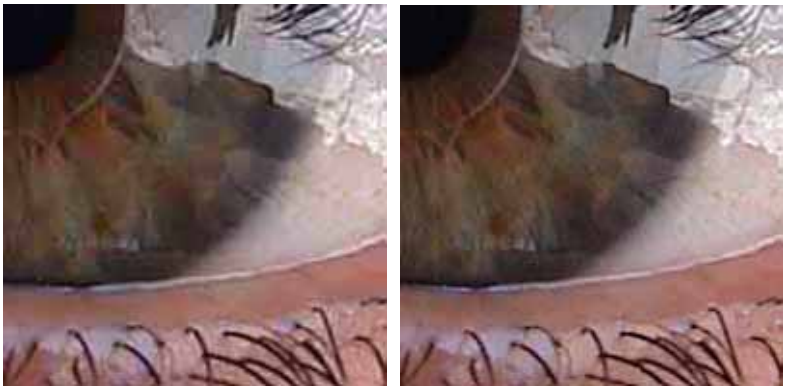
Fig. 5.5 JPEG baseline codec: sequence of events

- Level-shift shifts the data to a value evenly distributed about zero
- Forward DCT transforms the image to 8 x 8 block
- In the quantiser, each of the 64 DCT coefficients (C_{ij}) is quantised by an integer division Cq_{ij}=round (C_{ij}/Q_{ij}). Q_{ij} is a quantisation parameter and Cq_{ij} is the quantised coefficient. Larger values of Q_{ij} yield for higher compression as more coefficients are set to zero after quantisation. This is the parameter controlled by the user to set the compression ratio. The 64 values of Q_{ij} are stored in a quantisation map and can be “weighed” so that low frequency coefficients are quantised more than high frequency ones. That achieves a better visual result as higher contrast areas are represented in more detail.

- Zig-zag reordering rearranges the 8 x 8 block coefficients so that low frequencies are grouped together at the start of the array.
- DC differential prediction attempts to guess the coefficients of neighboured blocks, based on the properties of preceding blocks.
- In the entropy encoding, the differential DC and AC coefficients are encoded.
- Finally, an optional "marker encoding" can be embedded into the entropy-coded data sequence to describe several image properties. This is also called "metafile" and can contain information on the camera or scanner that took that picture, lens distance, speed of shutter, etc

Figure 5.6 demonstrates the effects of various levels of compression applied in a medical image. The "block" effect is evident in the images that were stored using higher compression [Fig. 5.6.c]

a b



c d

Fig. 5.6 a. detail of an original image. b. The square represents the detail of the original uncompressed image c. image compressed as a JPEG with 30:1 compression ratio having a PSNR of 26.2dB. The "block" effect and forcing of similarities are apparent. d. same detailed compressed at 5.5:1 with no visible loss of information (PSNR is 21.4 dB)

Decompressing the image has the exact reverse procedure as compression. As some of the detail is inevitably lost during JPEG conversion, multiple savings of the same image (usually after processing it) further degrades the image quality as more coefficients are rounded to their nearest integer.
It is worth mentioning that JPEG also defined a lossless encoding / decoding algorithm using a DPCM technique. Lossless JPEG guarantees image quality, but only at the expense of poor compression performance.

From the moment of their creation, many coding schemes have been shown to outperform baseline JPEG. The need for better performance and higher compression ratios led to the development of **JPEG 2000**, the latest addition to the JPEG family. JPEG 2000 is based on a wavelet transform and generally supports [Ric02]:

- Better compression performance at high compression rates.
- Efficient compression of mixed images (photographs and text).
- A choice of lossless or lossy compression.
- Progressive transmission (to improve transmission over a slow network link).
- Region Of Interest (ROI) coding allowing for the encoder to specify a region within the image that will be treated differently during encoding (better quality). That is particularly useful to telemedical applications as in several modalities (more often films) there is a demand for the highest detail in a very specific part of the image, to facilitate safer diagnosis.
- Error resilience tools that improve the safety of transmission.
- Open architecture that allows for future addition to the standard.

A typical objective metric scale for measuring the quality of an image is by using the Peak Signal to Noise Ratio of the JPEG reconstructed image, against the original. Fig. 5.7 illustrates the difference in performance of JPEG, JPEG 200, PCM (no compression) and Differential PCM, for a range of bits per pixel [Lag02]

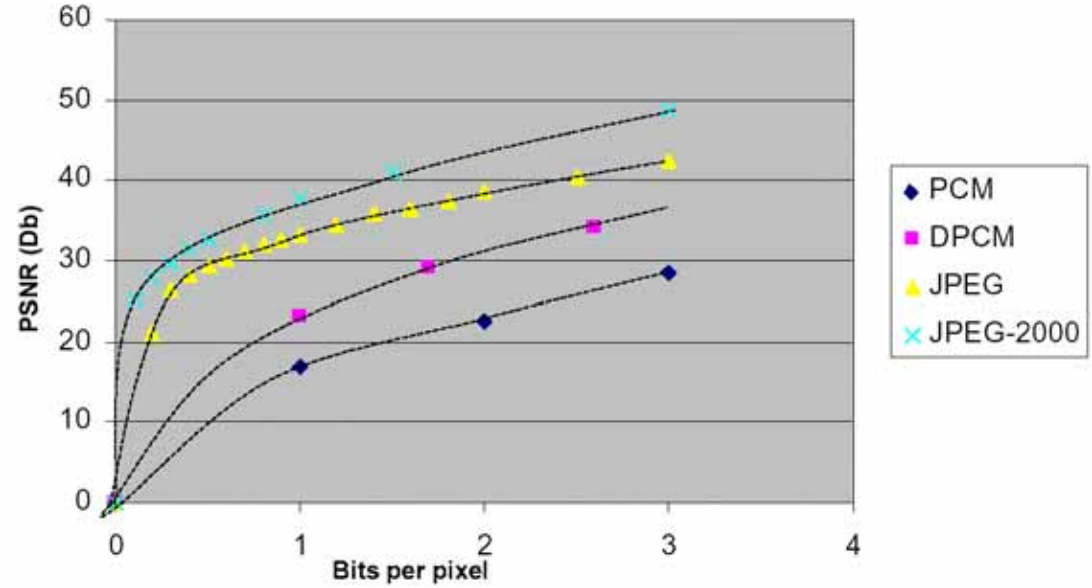


Fig. 5.7 PSNR over bpp for JPEG, JPEG 2000, PCM (uncompressed) and Differential PCM: For the same value of bpp, JPEG 2000 outperforms JPEG

Finally, a "motion JPEG" (MJPEG) has also being defined. It is a series of JPEG-compressed images run as a sequence to mimic motion pictures. Although this technique has been used in the early days of JPEG compression, nowadays it is deemed obsolete, as it does not exploit inter-frame redundancy and achieves a poor compression rate, especially compared to the MPEG algorithm.

5.3.2 MPEG

The first standard produced by the Moving Pictures Expert Group (MPEG) was **MPEG-1** and aimed at providing sufficient compression to accommodate 74 minutes of compressed video and audio, in a standard CD format; later described as Video-CD (VCD). VCD was never a commercial success as the quality improvement over conventional VHS tape was not sufficient. Moreover, the irritating break of the movie on the 74th minute made things even worse. However, MPEG-1 was considered valuable for two good reasons: it introduced consumers to the idea of digital video storage and transmission (over the Internet) and also opened up the way for improvements, such as MPEG-2. Until today, MPEG-1 is considered a fail-safe compression algorithm; something that almost all digital devices can reproduce (digital cameras, computers, DVD players, etc) [Ric02]

Details of the operation of the MPEG algorithms are too vast to be mentioned within this chapter [Ric02]. However, it is worth mentioning that MPEG-1 encoder works

with a typical resolution of 352 x 288 or 352 x 240 pixels. Each frame of video is processed in units of "macroblock" corresponding to a 16 x 16 pixel area in the frame that explains the "squaring" effect of a rapidly moving scene encoded using MPEG-1. The major advantage of this algorithm over MJPEG, is that it takes into account the preceding and succeeding frames to achieve a considerably better compression. More specifically, it uses "P-pictures" to forward-predict the next frame, based on a reference picture.

With the dawn of digital television some years ago, came the need for an even more efficient video compression algorithm. **MPEG-2** was designed to support larger frame sizes (720 x 576 or 720 x 480) and coding for interlaced video, in contrast with MPEG-1 that treated the video frame progressively. This function was proven useful when dealing with television frames that were inherently interlaced. MPEG-2 is considered as a superset of MPEG-1; MPEG-2 decoders can effectively decode MPEG-1 video.

Its major advantages can be summarised below:

- Efficient coding of television video: its core functions address television frames and can efficiently compress and reproduce a television videostream with an average bit rate of about 3-5 Mbps
- Support for coding of interlaced video: encodes separately the two half-frames that make up the television image. Using that technique, a better performance is achieved as the frames are captured at typically 1/50 of a second.
- Scalability: apart from base layer (performing basic encoding functions) MPEG-2 supports a set of four enhancement layers (spatial, temporal, SNR and data partitioning) to effectively improve the quality of the decoded sequence.
- Support for different profiles and levels: to enhance interoperability between different applications, MPEG-2 supports for profiles (simple, main, 4:2:2, SNR, spatial and high) and for each of those, four different levels (low, main, high-1440 and high). As an example, the "main" profile combined with the "main" level describes a digital television transmission with a frame resolution of 720 x 576 and 30 fps.

MPEG-2's efficient architecture opened up the way for a new set of exciting applications: DVD video, satellite television, cable television, direct recording from digital cameras, digital video recording, etc. It is the compression algorithm used by all DVDs and it seems that it will be the de-facto compressor for high quality video transmission over digital lines, as long as they can handle the high bandwidth demands.

With the exception of MPEG-3 that deals exclusively with audio compression, **MPEG-4** was designed to extend the capabilities of its predecessors.
The characteristics that make MPEG-4 particularly desirable are summarised below:

- Support for low bandwidth applications: MPEG-1 and 2 perform satisfactorily at bit rates above 1Mbps. However, for applications like Internet videoconferencing over POTS or ISDN, or Video on Demand (VoD), only MPEG-4 demonstrates efficient compression.
- Support for object-based coding: probably the most important feature of MPEG-4, which separates it from conventional codecs, is the shift towards object coding. Using that technique, the scene is handled as a set of "foreground" and "background" objects. This opens up a wide range of possibilities as the "foreground" objects are usually the ones that are moving and require better representation through the compression algorithm, while the "background" objects remain relatively stable and can be coded at a lower rate. Fig. 5.8 demonstrates these properties [Ric02]

Fig. 5.8 VO1 and VO2 are the moving foreground while VO3 is the stable background. By distinguishing between the two, MPEG-4 can achieve better compression

The basis of the MPEG-4 algorithm is the Video Object (VO). Fig. 5.8 consists of a background VO and two foreground VOs. As VO1 and VO2 move into the background about 50% of the whole scene remains unchanged. MPEG-4 takes advantage of this property thus achieving a superb compression rate relative to the previous compressors. This, however, means that a much more complicated algorithm has to be performed to render this idea, translating to an increased compression time (a videostream compressed with MPEG-4 requires 5-8 more computational time).

- Toolkit-based coding: contrary to previous compressors, MPEG-4 is organised so that new coding tools can be added incrementally as new versions of the standards are developed, thus giving the standard an increased level of flexibility.

MPEG-4 compression also forms the basis for a compression algorithm known as DiVx. DiVx is able to recompress a 8GB movie stored in a DVD, into a file as small as half a GB (1:16 compression ratio), with a visual degradation only perceived by an expert's eye. That supports new applications like video storing, Video on Demand through broadband lines and video sharing through the Internet.

Finally, from the wide variety of applications that MPEG-4 supports, the most popular element is the **core low bit rate codec** that is almost identical to the ITU-T **H.263** standard that is widely used for videoconferencing over ISDN and other slow or unpredictable communication links. This is also the codec of choice for the MedLAN system, used to transmit video through the WLAN, through a variety of software packages (Chapter 4.3.1). The codec is based on an MPEG-4 algorithm, thus explaining MedLAN's inferior performance in fast moving situations when both foreground (patient) and background images keep changing.

H.263 was designed as an improvement of the H.261 compressor. It provided increased flexibility along with a greater set of available frame sizes. The target application was a low bit rate, low delay, two-way video communication. H. 263 can support video communication at bit rates as low as 20 Kbps, but only at the cost of visually limited quality. This, however, represents the basis for newly emerged applications, like video telephony over 3G mobile phones.

5.4 DICOM's approach to compression

Based on the above information, ACR-NEMA (and eventually DICOM) was called to decide on an appropriate compression technique, especially when dealing with still images. Instead of making a specific decision (and by realising that medical imaging is a very sensitive subject), the task group limited itself on merely suggesting a set of procedures for image storage and transmission. They also allowed a wide range of techniques to be used, provided the result is medically acceptable. For obvious reasons however, it favoured schemes that produced a lossless result, so information would be lost only from the first level of image acquisition (e.g. scanning an x-ray film would inevitably introduce some noise, however, saving the output image in an uncompressed format would limit the information loss to just the scanning operation).

As mentioned above, DICOM standards are still evolving. Apart from the widely used JPEG, DICOM considers a wide variety of other versions and formats, including the JPEG 2000, JPEG LS, PNG and many others.

An independent study of the quality of DICOM alternatives was performed in 2002 with the objective of finding a balance between the increasingly demanding medical applications, the facilities available in an average hospital and the need for accurate medical diagnosis [Clu99]. Within this study, 3679 single frame greyscale images from multiple anatomical regions, modalities and vendors, were tested.

The effectiveness of the alternative compression methods was judged based on two methods: objective and subjective:

Using **objective** methods, both the compression ratio and the time for the completion of the operation were recorded. Fig. 5.9 displays the results of compressing 3679 medical images of various modalities in respect to the performance of the compression algorithm (the higher, the better).

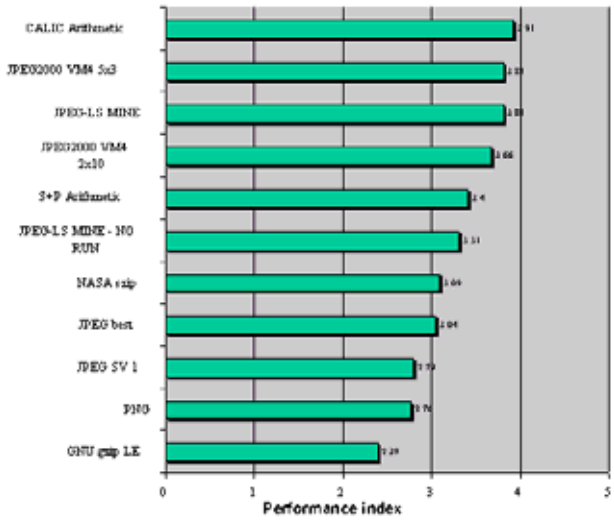


Fig. 5.9 Performance comparison of various codecs when compressing medical images (the higher, the better)

JPEG-LS and JPEG 2000 performed equally well (3.81), almost as well as CALIC (3.91), which was only used as a benchmark. Both outperformed existing JPEG (3.04 with optimum predictor choice per image, 2.79 for previous pixel prediction as most commonly used in DICOM). Dictionary schemes performed poorly (gzip 2.38), as did image dictionary schemes without statistical modelling (PNG 2.76). Proprietary transform based schemes did not perform as well as JPEG-LS or JPEG 2000 (S+P Arithmetic 3.4, CREW 3.56). JPEGLS compressed CT images (4.00), MR (3.59), NM (5.98), US (3.4), IO (2.66), CR (3.64), DX (2.43), and MG (2.62). CALIC usually achieved the highest compression. JPEG-LS outperformed existing JPEG for all modalities.

Considering the time required for the operations, JPEG, JPEG-LS, and SZIP codecs were noticeably faster than the others were and CALIC was noticeably slower due to the design of the algorithms. CALIC was included in the comparison as it is the "gold standard" for the effectiveness of lossless compression, but is considered unpractical for most applications.

Objective performance evaluation methods include quantitative metrics based on the analysis of the image pixels and include Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). Contrary to those methods, **subjective** performance evaluation methods rely on the human factor to empirically judge the quality and usefulness of the output. During the above study, it was found that the observers opinion did not correlate well with the objective metrics of the image. Metrics based

on models of human visual perception are still in their infancy and unfortunately, the observer performance is rarely exhaustively tested since there are many potential tasks, and findings from studies of one task may not be applicable to another. Furthermore, significant degrees of inter-observer and intra-observer variation on particular tasks may reduce the power of experiments on both lossless and lossy compression.

Considering studies like the above, (and for the sake of interoperability and wider acceptance) DICOM has decided to include compressed image formats in its standards [DICOM standards 8.2.1]. However, it applies strict rules before accepting these images, for a variety of their characteristics: size, colour depth, compression algorithm, etc [DICOM standards 8.2.1 a, b, c]. Furthermore, (indicating that medical imaging standardisation is a delicate procedure) it states: "*The context where the usage of lossy compression of medical images is clinically acceptable is beyond the scope of the DICOM Standard. The policies associated with the selection of appropriate compression parameters (e.g. compression ratio) for JPEG lossy compression is also beyond the scope of this standard*".
Conclusively, despite DICOM accepting lossy compression schemes, there is a high demand by the medical profession for lossless, uncompressed codecs that are perceived to offer a better representation of medical images. However, due to their high demand for storage space and bandwidth, the use of lossless compressors is not always feasible.

5.5 Defining the problem

By comparing the DICOM recommendations discussed so far, with the services that WLANs can offer (chapter 3) and the capabilities of the MedLAN system (chapter 4), it is apparent that a gap exists between what is required and what can be offered, in regards to the quality, size and speed of telemedical information.

5.5.1 Bandwidth requirements

As the number of medical applications that require the use of computer imaging increases, so does the required storage space (and thus the bandwidth demand for transferring the file within a network) for this application [Ban03]

As shown, increased complexity, high-efficiency algorithms have been developed to compress the data before they are stored or transferred. When applied in still imaging, these algorithms are divided into lossless and lossy.

Doctors tend to agree that a lossless compression is more suitable for medical image interchange as it retains all its original quality and makes diagnosis more accurate. This notion is further supported by DICOM. This is generally true if an infinite storage space is offered coupled with a very large bandwidth (although some may argue that grouping very similar image components may result in reducing the "grain-of-rice" noise effect) [Tob02]. However when trying to make use of the image, especially while using wireless networks, the problem becomes apparent. Table 5.1 below, summarises the space required to store an image of various sizes.

Size	**Storage space required (KB)**		
	Uncompressed	Lossless	Lossy
2048x2048	5120	2048-2512	1400-1700
1024x1024	1280	500-740	100-500
512x512	327	150-170	30-70

Table 5.1 Space required for storing a 10-bit colour image using different compressions.

5.5.2 Wireless capabilities

As discussed in chapter 3 and 4, the wireless network that has been used by the MedLAN system is the IEEE 802.11b; the most standard WLAN in Europe having a maximum data rate of 11Mbps.

Unfortunately, and for the best-case scenario of 11Mbps, a relatively small portion of it is available to the user. Specifically only 2.3 to 2.8 Mbps are available while the rest of the bandwidth is occupied by signalling data, protocols, encapsulation, etc.

It is apparent that with the average of 2.5Mpbs, transferring the images listed in Table 5.1 would require a considerable amount of time. This, combined with the fact that the MedLAN system is specifically designed to operate in an Accidents and Emergency Department, would render the system problematic. Table 5.2 summarises the time required to send an image of various sizes.

Size	Time required (sec)		
	Uncompressed	Lossless	Lossy
2048x2048	16	6-8	4-5
1024x1024	4	1-2	0.5-1.5
512x512	1	0.5-0.6	0.1-0.2

Table 5.2 Time required for sending a 10-bit colour image through a WLAN link operating at 11Mbps. Times triple in actual operation as the advertised speed is much higher than the actual.

Due to several factors like protocol collision and network congestion, all the above times increase dramatically when the image file is transferred simultaneously with a live video stream.

There are newer WLAN trends, like IEEE 802.11a that operates in a maximum speed of 54Mbps. However, in contrast with the IEEE 802.11b that uses the 2.4GHz band, 802.11a uses the 5GHz band thus considerably limiting the range of each AP [Ara02]. This means that a much greater number of APs have to be installed in order to cover the same space. In a mobile system, this leads to an increase of the hand-over time (time to disconnect from one AP and connect to another) that varies from 5 to 15 seconds.

5.5.3 Searching for the "golden rule"

The MedLAN system is trying to combine a diagnostic acceptable quality with the present limitations of the WLAN systems. Therefore, a new set of specifications were developed, tested and finally validated by the doctors.

The basic idea behind these new sets of rules is that a well-compressed image, even while being slightly loosely compressed, can maintain its diagnostic value while saving a considerable amount of bandwidth and time.

As a result, the MedLAN system can output images in three different compression ratios, to accommodate for different available network speeds: 5.5:1, 10.3:1 and 14.3:1. Keeping the best (5.5:1) as a default, Table 5.3 summarises some of the properties of the system, compared with the DICOM specifications.

	DICOM	MedLAN
Image resolution	512x512 to 2048x2048	640x 480 to 1152x864
Colour depth	10 bits minimum	16 bits
Image format	DICOM	JPEG
Average size	2048KB	512KB

Table 5.3 A simple comparison between the DICOM popular format and MedLAN outputs

The same rules were used when transferring video and sound: Video stream resolution is 320x240 pixels and the frame rate is dynamically adjusted depending on the available bandwidth. This means that if a high quality image is being transferred, the frame rate (fps) will be reduced. Typical frame rate is about 13-18 fps. Sound is being compressed using CCITT A-Law or u-Law with 8 KHz sampling rate, 8 bits per sample and monophonic audio transmission. Since heart and lung murmurs use the lower band of the acoustic spectrum, 8KHz sampling rate was proven adequate.

5.6 Methodology

To evaluate the system's performance a series of steps were taken involving both **objective** measurement techniques (SNR between original and compressed image, compression ratio, Mean Square Error, etc) and the **subjective** evaluation of the results by experts [ITU-T P.910 (9/99)]

Although the subjective evaluation of decoded video quality is quite fuzzy, compared to the calculation of numerical values of the objective quality evaluation, it is still preferable especially for low bit rate compression because of the inconsistency between the existing numerical quality measurements and the human perception of the outputs.

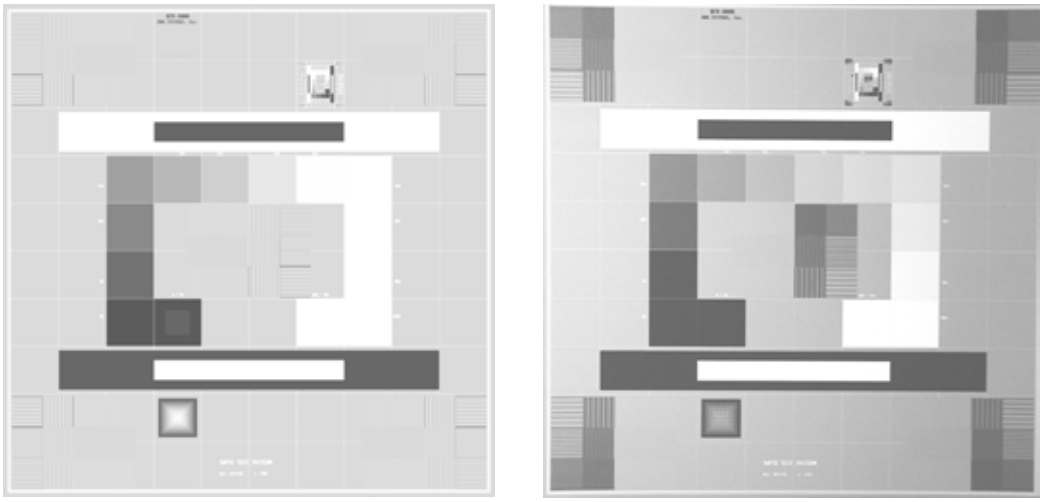
Furthermore, in error-prone environments, errors might corrupt the coded video stream in a way that causes a merge or split to the transmitted video frames. In this case an objective numerical method would lead to an inaccurate evaluation of the codec performance while a subjective measurement would certainly yield a fairer and more precise evaluation of the decoded video quality [Sad02].

5.6.1 Using test patterns to evaluate performance

Society of Motion Picture and Television Engineers (SMPTE) patterns have long been used by television technicians to isolate faults in television sets and establish the quality of video reproduction. SMPTE test patterns have also been used in Telemedicine to yield the overall quality of the telemedical system against the more conventional approach [Tob02].

In the case of the MedLAN system, SMPTE patterns were both photographed and videoed using the system's high quality camera. The results were then evaluated

with respect to their fidelity. Fig. 5.10 illustrates two SMPTE patterns. The first one is electronically created while the second one was photographed deliberately under average lighting conditions using the MedLAN system.



a b

Fig. 5.10 Comparison between an original SMPTE pattern (a) and one transmitted using the MedLAN system (b)

One can see that despite some change in the image brightness and a small loss in visual information when it comes to finer details (smooth grey-scale variants in the edges of the pattern), the reproduction of the image retains the greatest part of the original's information. There was also a marginal addition of noise due to digitisation (apparent in the grey areas on the right side of the second pattern) creating a grain-like effect. Overall, the Peak Signal to Noise Ratio (PSNR) of the reconstructed image was 26.4 dB, yielding a highly accurate reproduction procedure (JPEG outputs vary around 18-30 dB; the latter is the best-case scenario when the image is almost uncompressed) [Joh98]

In the case that a videostream was transmitted, greater sacrifices had to be made to ensure efficient fps values. As the video compression index increased, the H.263 algorithm (part of MPEG-4) forced more similarities, both in the current frame and between preceding and succeeding frames.

Fig 5.11 illustrates the video quality degradation of a real-time videostream while transmitted using an average (2Mbps) and a very narrowband (32kbps) channel. By considering both reconstructions just as a still images, the first one has a PSNR value of 25.2 dB while the second has a considerably lower value of 18.4 dB.

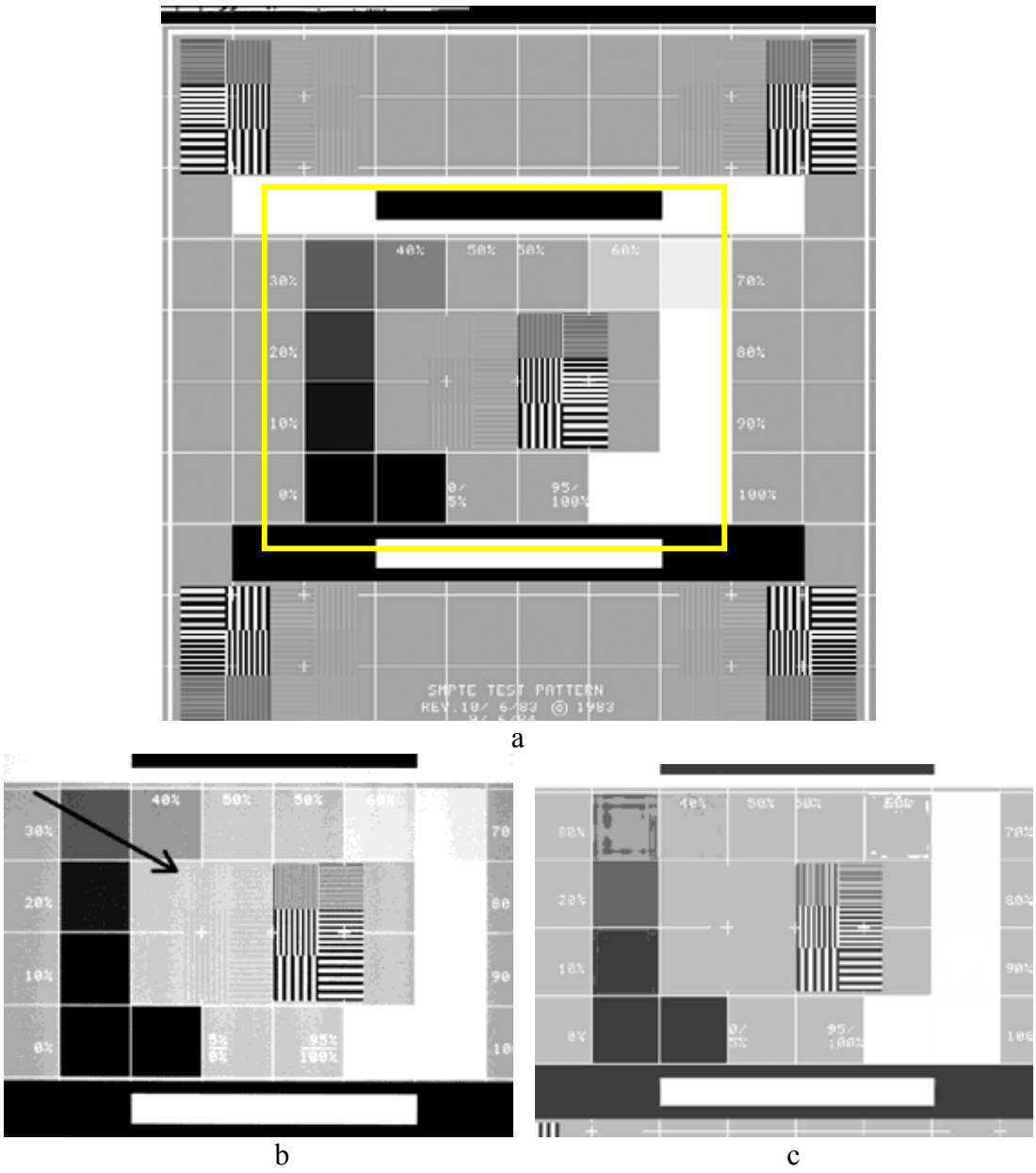


Fig. 5.11 a. Detail of an electronically created SMPTE pattern used for evaluation of video transfer through a WLAN link. b. 2Mbps WLAN channel indicates some visual loss in fine grey-scaled areas (arrow). c. a 32 kbps channel displays severe image degradation due to high compression.

5.6.2 Using expert's opinion to empirically evaluate performance

As mentioned previously, even by establishing a relatively low ratio of noise in the image or video to be transmitted, it does not guarantee that the output would have high diagnostic value. Inevitably, the people that will eventually judge the system and benefit from it would be the healthcare experts and it is their opinion that has greater value rather than absolute numbers. For that reason, a series of steps were

taken to supply doctors with enough material to form a safe opinion of the system's performance:

- a large number of x-rays, CT and MR have been captured and stored from four different hospitals.
- Several videos were recorded, including connecting the MedLAN system to external devices.
- Numerous heart and lung murmurs were captured and transmitted. Both electronic stethoscopes and pre-recorder sounds were used for that matter.

In total, five consultants within the NHS were asked to evaluate: more than 110 still pictures, 28 videos and 45 different sounds. The list of the modalities used exists in Appendix I. In the case that the images were converted to DICOM after being wirelessly transmitted, the composite DICOM format was chosen (header and image information exist in the same file), as it was the predominant standard in the NWLH group. In each of the above, three different compression rates were used to define the level of medical acceptable quality. The questionnaire included the following subject: image clarity, colour fidelity, depth versatility, sound quality, image/sound delay, total delay and x-ray grey-scale clarity [Appendix J]. Table 5.4 summarises the results of the doctors' evaluation. For convenience, the **average** of all the above factors are recorded in the appropriate cells.

Compressed sample	Quality	Poor %	Acceptable %	Good %
Still images	low compression 5.5:1	0	15	85
	medium compression 10.3:1	0	30	70
	high compression 14.3:1	5	80	15
Video	20 fps	0	50	50
	15 fps	10	55	35
	10 fps	20	50	20
Sound	low compression	0	8	92
	high compression	5	80	15

Table 5.4 Evaluation of the MedLAN's outputs (still images, video and sound) performed by a number of consultants.

5.7 Results and discussion

Clearly, Table 5.4 indicates that even when the medical data are compressed in a non-reversible way (some information is sacrificed in order to limit the size of the

files) the files maintain their diagnostic ability. Especially when low compression rates are used, none of the files falls below the “acceptable” threshold.

The most difficult part was proven to be the acquisition of x-rays. This was because the camera was “fooled” by both the low contrast of the film, the room lighting and the escaping light from the transparency viewer. Setting a non auto-brightness level resulted in the best outputs [chapter 4.10]

An important point to make is that after the files / videos / sounds have been received, the consultant can convert them into a DICOM format by adding additional information to the file (such as patient data, dates, diagnosis, etc) and creating the DICOM header. This way, files can be stored in a larger format that will follow DICOM specifications, but having already saved critical time while being transferred.

Finally, it is essential to understand that medical QoS is a very delicate matter that has always been hard to establish. The level of confidence in a pioneering system or a new proposal is directly related to the depth of the clinical trials that this has gone through. Although the above video and image samples represent a large portion of the consultant’s application area, further experimentation with additional data will strengthen the proposed notion.

5.8 Conclusions

The use of wireless LANs in hospitals is becoming increasingly apparent. However, along with their ease of use, there come some limitations that are directly related with their operation: lower bandwidth, security, administration, etc [Ban02b]

On the other hand, standards like ACR-NEMA’s DICOM, try to impose specific rules that are necessary for the interoperability between different medical architectures but also stating that the final word concerning the usefulness of a telemedical system belongs to the doctors. Furthermore, there is a considerable difference between the QoS as defined by objective measurements and that as perceived by humans, therefore, it is more important to evaluate the quality of medical service, based on human perception, as they would be the end-users of the whole procedure.

Based on the above, it is apparent that there has to be a balance between the standardisation (that often means additional overhead) and the flexibility of the system. This is especially true in time-critical environments like the Accidents and Emergency Departments.
The MedLAN system is dedicated for use within A&E departments. It tries to balance the standardisation of medical procedures and the flexibility of the system that has to respond promptly in such a demanding environment. For that reason a new set of specifications were tested and finally suggested, that reduce considerably the amount of information sent and thus the time before the consulting doctor has the data available, while maintaining the information necessary to make a valid diagnosis. Within the suggested framework and by using a low compression rate, 100% of the samples fall within the category of either “acceptable” or “good”.

In this chapter, we have presented some fundamentals of the DICOM standards while explaining the need for medical standardisation. Then we moved on to explaining some basic compression principals for most kinds of data (images, video and sound). Using the low-compression JPEG format as a stepping-stone, we have proved that a lossy compression can be very effective (especially in use with WLANs) and suggested an alternative / addition to the existing DICOM standards while using the MedLAN system.
The DICOM standards are not carved in stone. According to ACR they are “*not rules, but guidelines that attempt to define principles of practice that should generally produce high-quality care. The physician and medical physicist may modify an existing standard as determined by the individual patient and available resources”* [ACR99].

6. OFDM over IEEE 802.11b Hardware for Telemedical Applications

6.1 Introduction

Using a wireless Local Area Network (WLAN) to transmit live high-quality video suitable for a telemedical application presents many challenges, including ensuring sufficient Quality of Service (QoS) for the end-user to be able to make an accurate diagnosis. One of the many problems that exist when developing such a system, is the multipath effect caused by the reflections of the transmitted signals on various surfaces including walls, floors, furniture and people [Fig. 6.1]. This degrades the signal quality and reduces the amount of available bandwidth and thus, the quality of the image and video, as higher levels of compression are needed.

Specifically on the MedLAN system, several problems had to be resolved before the WLAN system can operate successfully. In Chapters 3 and 7 the problems of range, speed, security and interference of a wireless system, are examined. Especially on the range issue, several factors can influence the transmission and reception of the signal and affect the overall quality of the application.

In contrast with wired systems that have no range problems (apart from the ones dictated by the protocols used and are always predictable), wireless LANs suffer from a variety of factors that can influence their active range, with the operating terrain being one of the most important. Wireless product vendors acknowledge this fact and try to implement as many techniques as possible to ensure that the signal will eventually be correctly received.

As explained in Chapter 3, the most widely used wireless protocol today is the IEEE 802.11b. Being on the market since 2000, it usually uses Complementary Code Keying (CCK) and Direct Signal Spread Spectrum (DSSS) techniques to spread its signal over a frequency range and avoid interference while achieving a top speed of 11 Mbps. As sophisticated as this technique is, it behaves relatively poorly in

multipath environments when compared with newer modulation schemes like Orthogonal Frequency Division Multiplexing (OFDM).

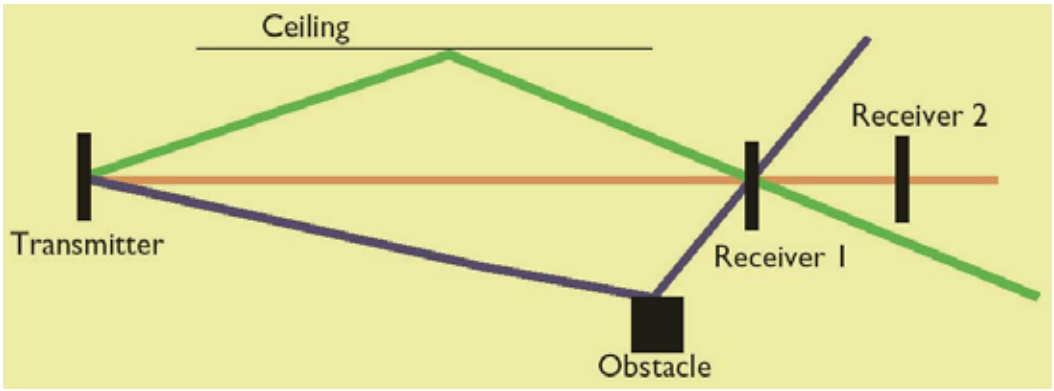
In this chapter, the balance between wider WLAN range (due to the use of a lower frequency band) and higher speed will be presented, along with the effects that an average hospital environment will have at the higher frequency spectrum (5 GHz).

Furthermore, the advantages of using OFDM over IEEE 802.11b hardware will be investigated with emphasis on the benefits that the end-users will enjoy when working with telemedical applications. The above suggestion will be supported by means of simulation using three different simulation packages [Ban04]

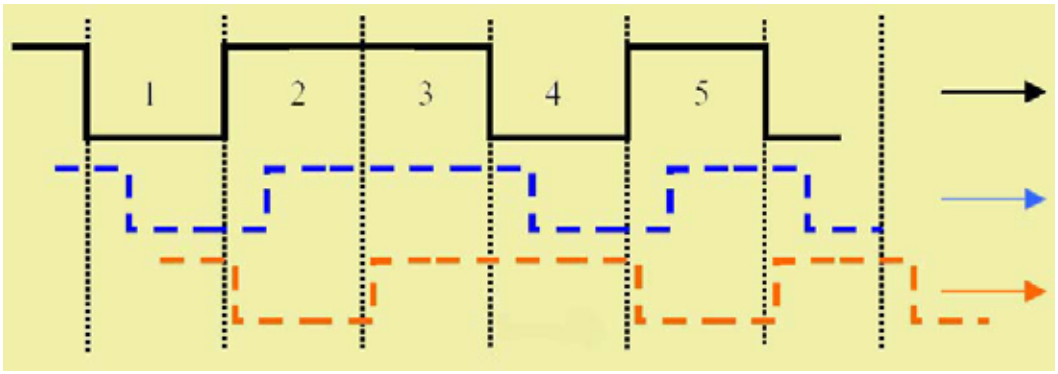
6.2 Existing technologies

In a medical system like MedLAN (Chapter 4), QoS plays a critical role. The system would be deemed useless if it could not guarantee the level of service necessary for accurate diagnosis. Despite the fact that none of the IEEE 802.11 protocols have guaranteed QoS, there are several parameters that a developer can optimise in order to keep a high operational level of the wireless network. Some of these include: connection establishment delay, throughput, transit delay, residual error rate, protection, priority and resilience. While protection refers to the security that the system applies to the transmitted data [Chapter 6], throughput and resilience are definitely some of the most important QoS parameters in a WLAN. In order to maximise the throughput one has to minimise the number of errors that appear in the communication channel. One of these erroneous factors is the multipath phenomenon:

In most wireless communications, the signal does not travel through a straight line from transmitter to receiver. Mountains, buildings, floors, ceilings, furniture and even people reflect the signal [Fig. 6.1.a] and that is much depends on the operating frequency. The lower the frequency, the more it can penetrate through objects and not get reflected. The higher the frequency, the more reflections take place and a multipath effect is more dominant [Kap02b].



a



b

Fig. 6.1 a. Multipath effect: the signal is reflected on various surfaces.
b. The receiver receives altered versions of the signal (different timing, strength and quality)

During the multipath effect, the receiver not only receives the signal directly from the transmitter, but also receives all the reflections of that signal. What makes this an undesirable effect is that since the straight-line transmission arrives the earliest, all other packet transmissions arrive with a time delay and collide with next-frame data [Fig. 6.1.b]. Depending on the distance between receiver and transmitter and the number of reflected paths, the signal can be rendered useless, even though its power would be sufficient.

Multipath delay also causes the information symbols represented in an IEEE 802.11 stream to overlap, something that confuses the receiver. This is often referred to as Inter-Symbol Interference (ISI). As the demodulator tries to decode the signal, bit errors in the packet will occur and the Cyclic Redundancy Check (CRC) will not compute correctly. In response to bit errors, the receiving station will not send an ACK to the source, so the entire packet will eventually be retransmitted thus lowering the throughput of the WLAN system. 802.11 signals in homes or small

offices experience a multipath delay of about 50 ns while in a manufacturing plant with a lot of reflecting surfaces, this delay can go as high as 300 ns [Dub03]

Chapter 3 mentioned some basic trends and versions of wireless networks including the IEEE 802.11 and the HiperLAN families. Table 3.2 summarises the different properties of the most widely use WLAN systems along with their basic characteristics. There was an obvious trade-off between the data speeds offered by the IEEE 802.11a and the extended range of IEEE 802.11b. To complicate matters even further, IEEE 802.11a operates in the 5GHz spectrum; a frequency band that is regulated in most European countries and therefore much less populated than ISM. It is only until very recently when some countries including UK and The Netherlands deregulated this band and although the feeling is that some time in the near future the 5GHz spectrum will be licence exempt, most of Europe is still awaiting this decision from the ETSI.

Apart from the obvious decrease of active WLAN range in the IEEE 802.11a, reflections are much more apparent in the 5 GHz spectrum so any kind of reflective surface can have devastating effects on signal quality. The most visible consequence of the above two problems (lower range and higher reflections) is when trying to cover a space with APs, a lot more are needed if 802.11a is used, compared to 802.11b [Fig. 6.2], [Ban02b], [Ara02].

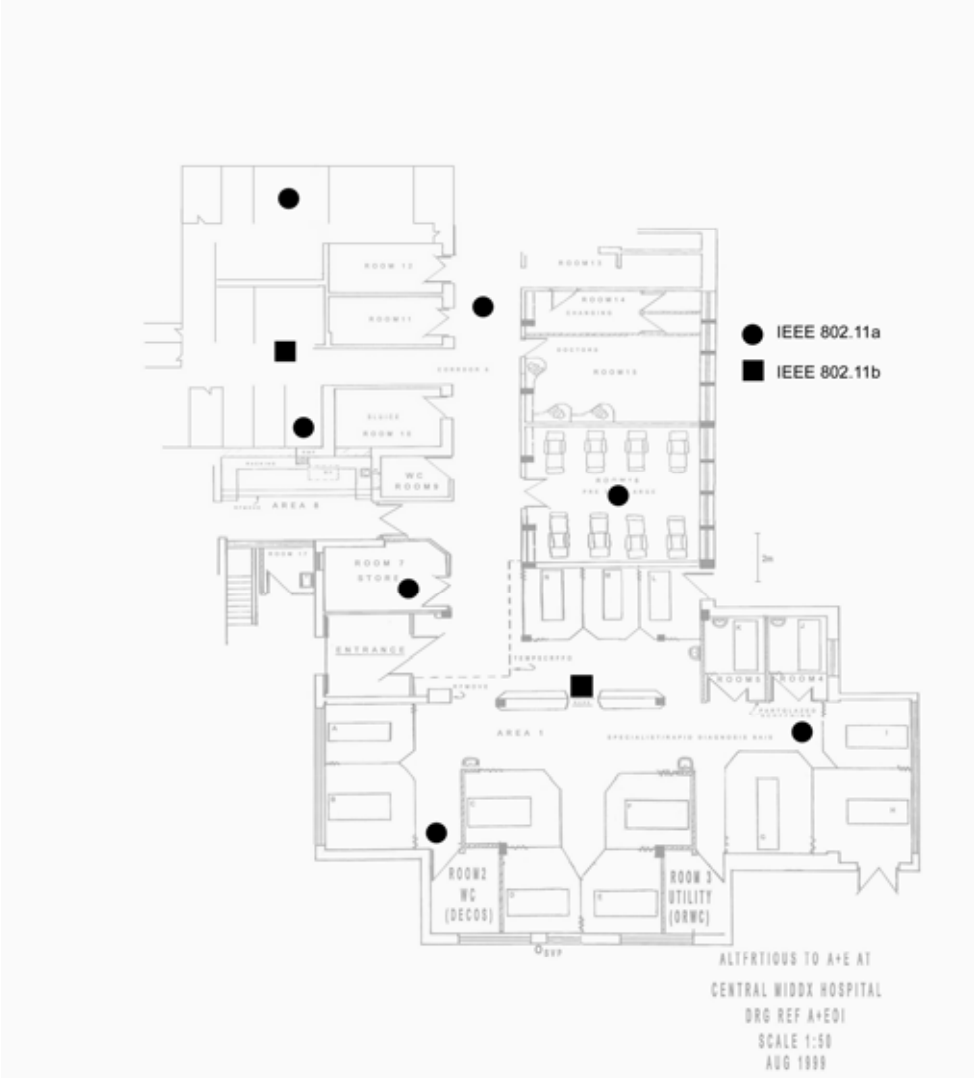


Fig. 6.2 WLAN range comparison between 802.11a and 802.11b inside the A&E room of CMH Hospital. Squares are 802.11b and circles 802.11a APs

Fig. 6.2 shows results of an experiment that took place in Central Middlesex Hospital (CMH) that investigated the number of APs needed to cover the Accidents and Emergency ward using both 802.11a and b technologies. Squares indicate APs using 802.11b while circles show APs using IEEE 802.11a. It is clear that using 802.11a a greater number of APs (7 APs) are required to cover the same space, compared to 802.11b (2 AP).

Furthermore, (and as mentioned above), 802.11a suffers from signal deterioration due to reflecting surfaces. Several studies of the reflection of common materials agree that the reflections in the 5 GHz band (UNII) are more severe than in the 2.4 GHz band (ISM). Table 6.1 summarises some of these effects in both frequency bands [Che02], [Wils02].

	T (dB)		R (dB)	
Material	ISM	UNII	ISM	UNII
Dry red brick	-4.43	-14.62	-12.53	-8.98
Drywall (12.8mm)	-0.49	-0.51	-12.11	-11.50
Drywall (9mm)	-0.50	-0.84	-12.03	-8.87
Body of water	-14.2	-3.8	-10.50	8.91

Table 6.1 Transmission and Reflection values of common materials for ISM and UNII bands

It is clear that since thick red brick walls (often found in hospitals) have a greater reflection index than concrete walls, they create a stronger multipath phenomenon as the operating frequency increases. Note that a body of water simulates the human body that mainly consists of water and might move in between the communications path. Since the ISM band operates at 2.4 GHz, the transmitted energy is absorbed much more by water molecules than in the 5GHz band. However, reflections due to water obstacles (and thus human bodies) tend to be less of a factor in the ISM band.
Conclusively, the potential gains of a UNII 802.11a system due to reduced interference (caused by the less populated 5GHz band), are balanced by the increased path loss caused by standard obstacles such as walls, floors and water / people. Although IEEE 802.11a uses a different modulation technique to combat multipath interference, **none of the two systems** seems to include the optimum solution between range and speed.

6.3 OFDM

Orthogonal Frequency Division Multiplexing (OFDM) represents a different design approach than CCK [IEC03], [Arm02], [Edf96]. It can be thought of as a combination of both modulation and a multiple-access technique that divides the channel in such a way that the users can share it (similar to TDMA dividing the channel in time and CDMA according to spreading codes). OFDM techniques and advantages spread far beyond the scope of this thesis. In this chapter, only an introduction to OFDM will be made, necessary to appreciate the research novelty that is introduced.

Although OFDM was proposed as far back as 1950, it is recent developments in VLSI chips and the increased computational power of Digital Signal Processing (DSP) that have made it realizable. Due to its advanced nature OFDM found an increasingly high number of possible applications in modern communications systems. HiperLAN/2 IEEE 802.11a, DSL communication lines and digital TV are only a small part of its area of applications.

To begin with, Frequency Division Multiplexing (FDM) systems separate the available bandwidth in a number of intermediate channels. To accommodate hardware imperfection and different distances and speeds between transmitter and receiver, FDM introduces a number of guard bands (gaps) between each of the channels so signal frames do not overlap each other [Fig. 6.3]. Unfortunately, these guard bands can sometimes take up to 50% of the available spectrum thus reducing the spectrum efficiency.

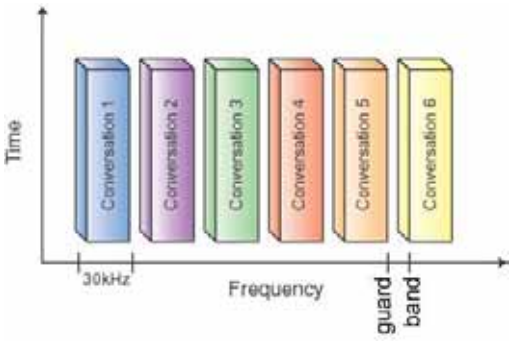
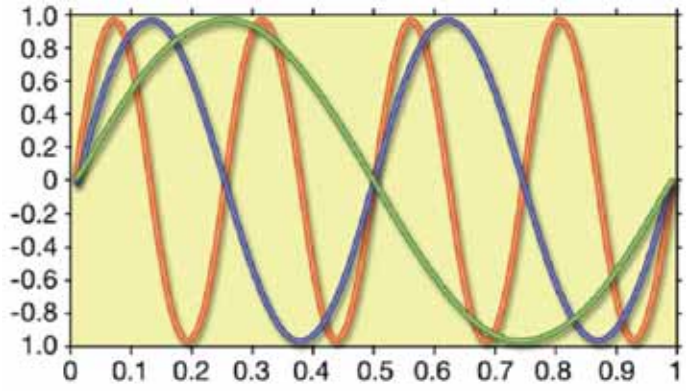


Fig. 6.3 FDM Access in a typical landline exchange centre: many users share the same line occupying different frequencies and leaving guard bands between their frequency bands

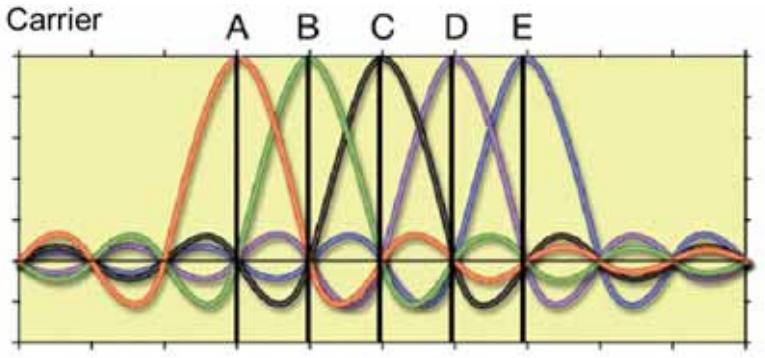
Much like FDM, OFDM also separates the channel into a number of intermediate frequencies channels (approx. 2000-8000 for digital TV and 48 for Hiperlan/2). However, in contrast with FDM, OFDM systems do not have any guard bands. In fact, OFDM overlapping subcarriers is a desirable characteristic.

This is done by a careful selection of the frequencies used (subcarriers) so that they are orthogonal to each other [Fig. 6.4.a]. Consequently, subcarriers are easily separated without causing any interference among them [Fig. 6.4.b]. This special property prevents adjacent subcarriers from interfering with each other much like the human ear clearly distinguishing each of the tones created by neighbouring keys of a piano. This technique (incorporated with a small amount of guard time in each

symbol) preserves the orthogonality between subcarriers in the presence of multipath. In Fig. 6.4.b, notice that the peak of each one of the five subcarriers corresponds to a zero level energy of any other subcarrier, resulting in zero interference between them as, when the receiver samples at the centre frequency, there is no other energy present than that of the desired signal.



a



b

Fig. 6.4 a. In OFDM, carriers are carefully selected so they would be orthogonal to each other. b. by having orthogonal subcarriers, the peak of each one corresponds to a zero level energy of any other.

The way that OFDM is modulated is by applying changes in each of the carriers: varying its phase, amplitude or both. Typically, high-level modulation techniques, such as Quadrature Amplitude Modulation (QAM) are employed to distribute the data over the carriers spaced at precise frequencies.

At the implementation level, OFDM systems take a serial data stream and convert it into N parallel data series. Each of these series is then modulated into a subcarrier at a unique frequency and then the subcarriers are combined to produce a serial stream of transmitted signal.

In the core of the OFDM transmitter, theoretically exists N modulators, one for every frequency component used [Fig. 6.5].

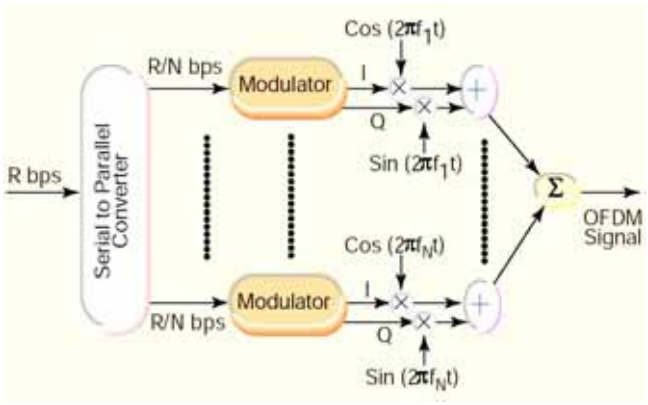


Fig. 6.5 Transmitter design of an OFDM system. The N modulators are replaced by an IFFT operation

In practice, the operation of the multiple modulators can be replaced by an Inverse Fast Fourier Transform operation (IFFT) that converts the frequency components into the time domain [Hug02]. The decoding procedure involves the exact opposite sequence [Fig. 6.6].

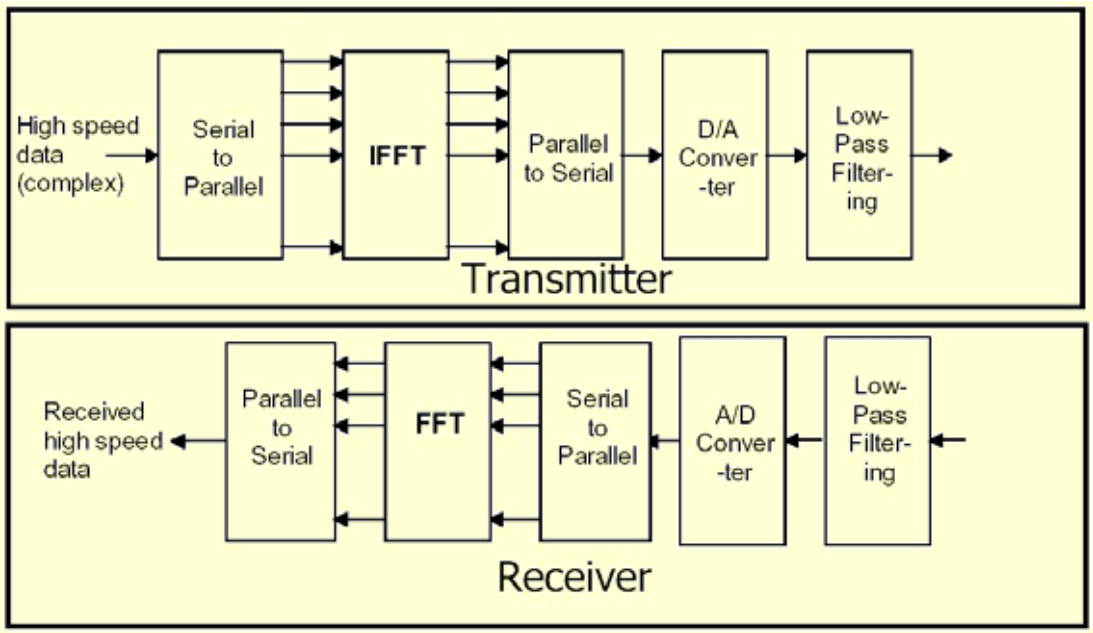
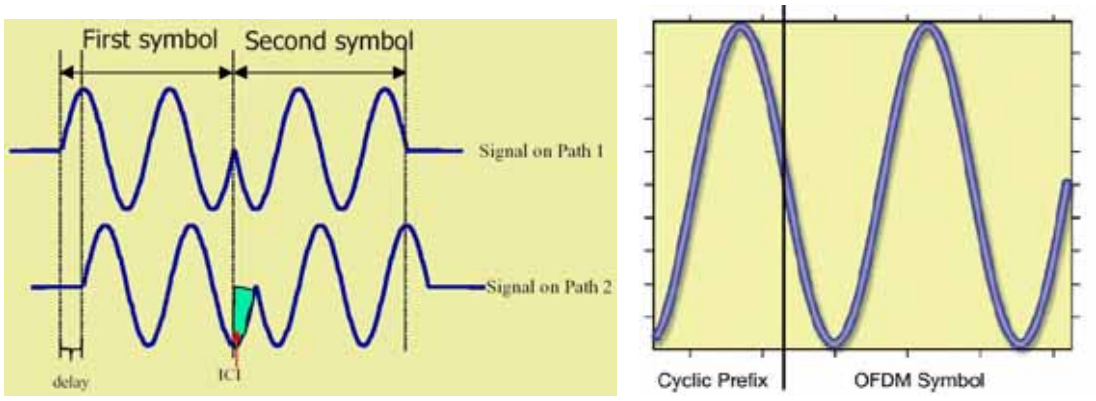


Fig. 6.6 OFDM encoding / decoding sequence. The modulator takes a serial data stream and convert it into N parallel data streams using an IFFT algorithm.

Since OFDM transmits data in blocks, multipath delay will cause blocks of signals to collide with each other causing an Inter-Channel Interference (ICI) as some paths

take longer to arrive at the receiving end. This eventually leads to Inter-Symbol Interference (ISI) [Fig. 6.7.a] [Keo03]. To address this issue, OFDM uses an additional signal that is added to the beginning of each symbol. This added signal does not contribute any useful information but acts as a guard band to combat channel delay. The most commonly used method of achieving this is the Cyclic Prefix where the last useful part of the signal is copied to the start of the signal. As a result, the periodicity of the signal is preserved [Fig. 6.7.b]



a b

Fig. 6.7 a. When a subcarrier arrives later than expected (signal on path 2), the orthogonality between all the subcarriers is destroyed causing ICI and eventually ISI. b. Cyclic Prefix repeats the "tail" of an OFDM symbol as a header. This redundant information serves as a guard band to combat ISI

The cyclic prefix is sized appropriately to serve as a guard time against ISI. This is accomplished, as the time dispersion from the channel is smaller than the duration of the cyclic prefix. A fundamental trade-off is that the cyclic prefix must be long enough to accommodate for the anticipated multipath delay imposed on the system. As the cyclic prefix increases, so does the amount of the overhead imposed on the useful bandwidth.

As mentioned above, in OFDM systems data streams are transmitted in parallel and thus require a longer symbol period allowing the system to cope a lot better in multipath environments. For example, in Hiperlan/2, that uses 48 different parallel streams, the symbol period is 48 times as long as if it would be transmitted in a single stream. This, combined with the Cyclic Prefix, improves considerably the tolerance that the signal has against multipath interference: instead of transmitting a very fast single stream, multiple streams are transmitted at a much lower frequency

so that interference can only affect a very small portion of the symbol during its initial part. However, the affected part is made up by redundant information introduced by the Cyclic Prefix.
OFDM is also the base of a multiple access system called OFDM Access (OFDMA). Here, each user can be assigned a specific number of subcarriers (having a predefined bandwidth) or a variable number of subcarriers (having bandwidth on-demand). This is the basic technique for transmission over DSL lines [IEC03]
OFDM can also be combined with frequency hopping to create a spread spectrum system that will include the advantages of frequency diversity and interference averaging (as in CDMA). By switching frequencies at a high rate, the losses due to frequency selective fading are minimised.
Conclusively, OFDM provides the best of two worlds: TDMA, (as users are orthogonal to each other) and CDMA, (as mentioned above) while avoiding the limitations of each, that includes frequency planning, equalisation and multiple access interference [Nee00].

6.4 Methodology

Based on the first two subchapters, it is easy to realise that there is a fundamental gap between QoS (specifically in a hospital environment) and speed : IEEE 802.11b is the standard for most of Europe and has a definite advantage in regards to its range of operation as it uses the 2.4GHz spectrum that suffers less from reflections. IEEE 802.11a, on the other hand experiences more reflections as it is operating in a higher frequency but uses an advanced modulating technique to reduce multipath interference. 802.11a has not been yet cleared for operation around Europe. Furthermore, its range of operation is considerably lower than this of 802.11b.
Even at 11Mbps it is evident that 802.11b will either support low speeds and consequently have low multipath distortion or operate at a higher speed but suffer from multipath interference.

It is worth mentioning that a new version of wireless networking, IEEE 802.11g promises speeds as high as 54 Mbps, at the ISM frequency band. Unfortunately, in order to maintain compatibility with both 802.11a and 802.11b, it was forced to

adapt all available modulation schemes, along with Packet Binary Convolution Coding (PBCC) making the hardware considerably more expensive [Table 6.2]. This system is in the process of standardisation, however hardware has already been commercially available.

Speed (Mbps)		802.11b		802.11g		802.11a	
	carrier	mandatory	optional	mandatory	optional	mandatory	optional
1	Single	Barker		Barker			
2	Single	Barker		Barker			
5.5	Single	CCK	PBCC	CCK	PBCC		
6	Multi			OFDM	CCK-OFDM	OFDM	
9	Multi				OFDM, CCK-OFDM		OFDM
11	Single	CCK	PBCC	CCK	PBCC		
12	Multi			OFDM	CCK-OFDM	OFDM	
18	Multi				OFDM, CCK-OFDM		OFDM
22	Single				PBCC		
24	Multi			OFDM	CCK-OFDM	OFDM	
33	Single				PBCC		
36	Multi				OFDM, CCK-OFDM		OFDM
48	Multi				OFDM, CCK-OFDM		OFDM
54	Multi				OFDM, CCK-OFDM		OFDM

Table 6.2 Comparison table between IEEE 802.11b, a and g in terms of data rates and modulations

In this subchapter, the alternative of using OFDM over 802.11b technology will be investigated, with emphasis on the telemedical applications. The idea of OFDM over the 2.4GHz band is not very new and has been investigated for a number of years and addressed within the IEEE 802.11g. However, there is very little research both on the use of this modulation in telemedical applications and on the financial advantages of applying OFDM to the existing 802.11b systems, instead of replacing them entirely with new 802.11g hardware.

Fortunately, most wireless hardware (APs and client cards) on the market today offer the user the ability to upgrade the firmware (software inside ROM) of the system in order to support different technologies. In addition, today's hardware has embedded microprocessors that can perform a wide variety of tasks, including IFFT and FFT, necessary for OFDM modulation.

The simulation that follows investigates the advantages that OFDM modulation would have, compared to CCK in 802.11b, with regard to both the signal-to-noise ratio and the total speed achieved by the wireless network. Three different simulation packages will be used to do the simulation.

In order to justify the proposed use of OFDM over 802.11b hardware for telemedicine applications, models have been built and tested in various simulation

environments. For the lower OSI layers (physical) Matlab 6.5 and VisSim Comm 5 were used. These software packages can simulate the PHY layer very well and allow the user to introduce several variations to the communications channel like multipath noise, Rice / Rayleigh effects, selected frequency fading etc.

For the upper OSI layers (up to the presentation layer) OPNET Modeler 9.1 was used, and allowed the opportunity to adjust data links (wired to wireless), transport sessions (the priority the video stream will have over other data flowing into the network), even the presentation environment (video resolution and frame rate).

These software tools complement each other as OPNET Modeler had insufficient representation of the PHY layer and the multipath environment while Matlab and VisSim describe the lower level very effectively but fail to give the user the ability to investigate changes at higher levels. In summary, VisSim and Matlab simulation supports the proposal of using OFDM over 802.11b while OPNET Modeler investigates the practical results that this notion would have in a telemedical application such as MedLAN.

Due to the complexity of the tasks involved, both the simulating environments mentioned above have a great number of parameters that have to be set. It would be outside the scope of this chapter to mention all of them, thus only the basic settings will be included for reference purposes.

6.4.1 Physical layer simulation

In general, the PHY layer of any IEEE 802.11 protocol that uses OFDM, follows this sequence, from Data-link layer to PHY bursts:

Scrambling → ½ rate convolutional coding → puncturing → interleaving → mapping → OFDM

Fig. 6.8 describes how the model was built in VisSim Comm 5 (some modules were taken from Matlab): A random bit generator passes its output to a standard 802.11 scrambler. The scrambled data is input to a convolutional encoder consisting of a ½ rate initial code and subsequent puncturing. The coded data is interleaved to avoid error bursts to be input to the convolutional decoding process. The interleaved data is subsequently mapped to data symbols (using BPSK, QPSK, etc). Finally, the output is fed into an OFDM complex modulator consisting of 48 data and 4 pilot subcarriers and converted using a 64-point FFT. After that, the whole train is transmitted over

the air. It is worth mentioning that the above procedure is also fundamental for the operation of both IEEE 802.11a and HiperLAN/2. Table 6.3 summarises the basic parameters of the system:

Parameter	Value
Modulation	BPSK, QPSK
Coding rate	½
Coded bits per subcarrier	2
Coded bits per OFDM symbol	96
Data bits per OFDM symbol	48
Number of data subcarriers	48
Number of pilot subcarriers	4
FFT size	64
OFDM output rate (11*64/48)	14.666 MHz
Guard time duration	0.8 us
Number of paths	2 (multipath noise)
Power of additional path	10, 20% of original

Table 6.3 PHY layer parameters of the model

Inside the AWGN box and for the single-path experiment, is a white Gaussian noise generator with a noise level equal to the value of the EbNo box. For the multipath environment simulation, a multipath noise generator was added alongside the AWGN one [Fig. 6.8].

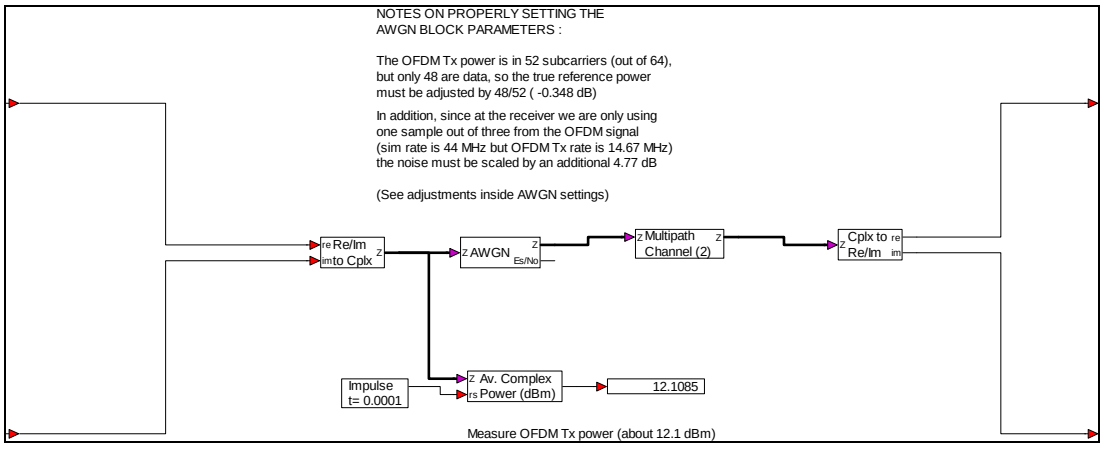


Fig. 6.8 Defining the noise sources of the model: an AWGN generator with a value that is user defined, followed by a multipath generator having two or three alternative paths.

Although the number of multipaths is user defined, as their number increased, the simulation time of the system increased exponentially. To simplify matters, there were either one or two reflected paths defined. During the first scenario, the reflected

path had 10% of the power of the main transmission. In the second scenario, the first reflected path had 20% and the second 10% of the power of the main path.

Much like Matlab, VisSim consists of a number of modules that work jointly with each other [Fig. 6.9]. The contents of each of the modules / procedures involved, can be found in Appendix K.

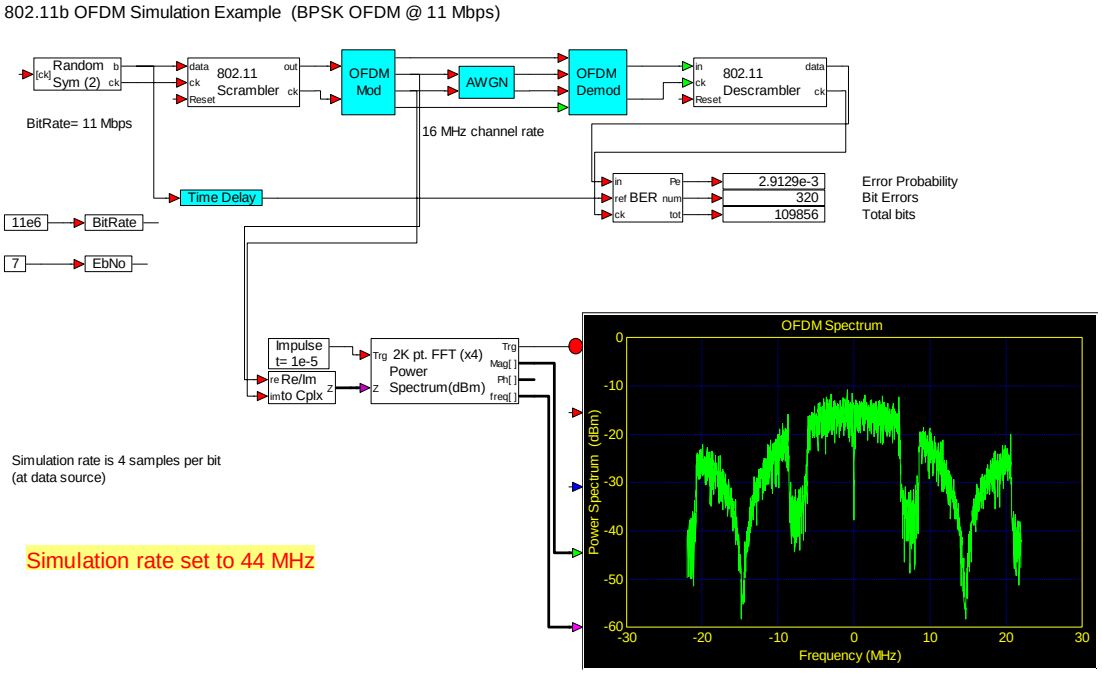


Fig. 6.9. Block diagram representation of the physical layer of 802.11b, using OFDM modulation

On the demodulating side, the reverse procedure was applied. The Bit Error Rate (BER) was measured against the original signal and a power spectrum analyser displayed the original signal before it went over the noisy channel.

Overall, the transfer of a file of about 14KB (110 Kbits) was simulated at a speed of 11Mbps. Larger files produced the same average BER.

6.4.2 Upper layer simulation

A complete model of the MedLAN hospital environment was built using OPNET Modeler. The model represents the Accidents and Emergency (A&E) ward for both majors and minors, of the Central Middlesex Hospital (CMH), West London [Fig. 6.10]. To simplify matters, only one AP was modelled, even though there is an option to use two (one in the majors and one in the minors) or more to extend the WLAN cover space. [Ban01b]

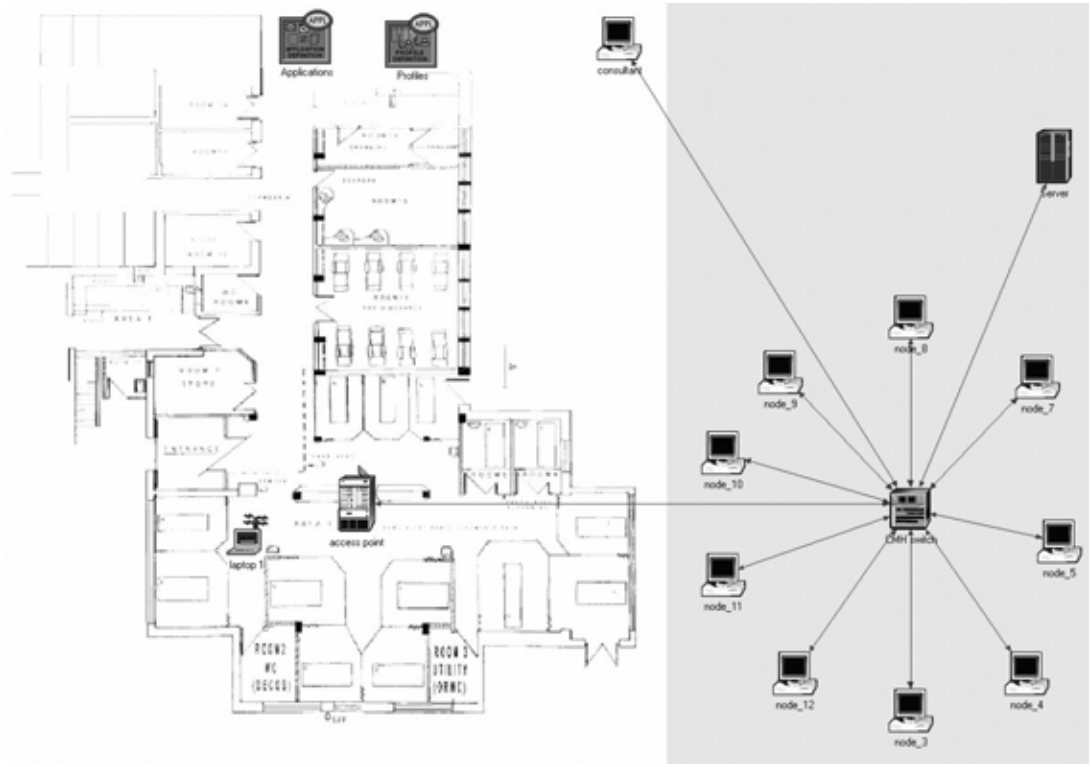


Fig. 6.10 Model of the A&E room of the Central Middlesex Hospital:
The WLAN is installed in that ward, and is connected to the rest of the hospital via the wired network

As described in chapter 4, the simulated environment is a hospital requiring a wireless videoconferencing application between the A&E department and a consultation point either within or outside the hospital. The rooms suffer from signal deterioration that can be attributed to both reflected signals due to the thickness of the walls (CMH is an old hospital) and to the existence of several noisy sources (medical equipment, microwave ovens, etc).

The AP is located in the centre of the A&E ward and a mobile client is free to move around the room while being in communication with the AP, which in turn, is connected via wire to the hospital backbone. Several other hospital computers are also connected to the same backbone running various other applications (www browsing, email, ftp, etc). All these details are described in the “Applications” and “Profiles” boxes of the model. One of these computers is the “consultant” that resides within the same hospital. Alternative scenarios have investigated the effect of having the “consultant” computer placed in another hospital that belonged to the NWLH domain [Fig. 4.15]. Since the lines used to connect these hospitals run on fibre optics (thus having adequate capacity) and their utilisation index is very low (2-

5% on an average day), practically the same results were output by the simulator regardless of if the “consultant” resides in the CMH or in another NWLH hospital.

The path of the mobile client was chosen to be non-static with an average distance of 15m between the client and the AP. The initial 802.11 modulation is QPSK and thereafter OFDM. Power was set to a standard 30mW to simulate a standard Cisco 340 AP, although newer APs offer power in excess of 100mW thus improving the range considerably. Background noise levels were set to 5 dB to simulate an average A&E environment. To maintain comparability, frames are not fragmented and no RTS/CTS commands are used as it is assumed that the mobile client would be in constant communication with the AP and there will only be one MT associated with the AP.

For the upper layers, a videoconferencing application was chosen having a VCR quality and a frame rate of 30 frames per second (fps). Every effort was made to keep the simulation parameters for both environments (CCK and OFDM) precisely the same. This, however, cannot be extended to every small detail like the buffer of the OFDM scenario that had to be bigger to accommodate for the IFFT calculations.

The whole model was run to simulate 300 seconds of real time communication and took about 30 minutes to run on a P-III/850MHz/256MB RAM. However, the above figure depended a lot on the alternative scenarios used, as well as on the version of OPNET Modeler. Some of these alternative scenarios included transmitting data through a DSL line to the doctor’s home or using 3G telephony to stream the video into the doctor’s mobile phone while he/she is on the move. However, in these scenarios, the destination terminals experienced reduced bandwidth availability, so using OFDM modulation played little or no role at all.

Finally, it is worth mentioning that the first 100 sec had zero network traffic to simulate the setting up of networking hardware. That explains the flat lining of the first 100 seconds in Fig. 6.11.

6.5 Results

For the above simulation environment, both the single-path and multi-path alternatives were investigated either with standard 802.11b modulation (QPSK/CCK

at 11Mbps), or with the addition of the OFDM modulation (QPSK/OFDM at 11Mbps).

Fig. 6.11 displays the BER vs. Eb/No of the transmitted data stream over a channel that is affected by both AWGN and multi-path noise under three different modulations: QPSK/OFDM, BPSK/OFDM and QPSK/CCK, the last being the standard modulation for 802.11b at 11Mbps. It is evident that when there is no multipath noise, OFDM modulation behaves similarly to standard 802.11b modulation [Fig. 6.11.a].

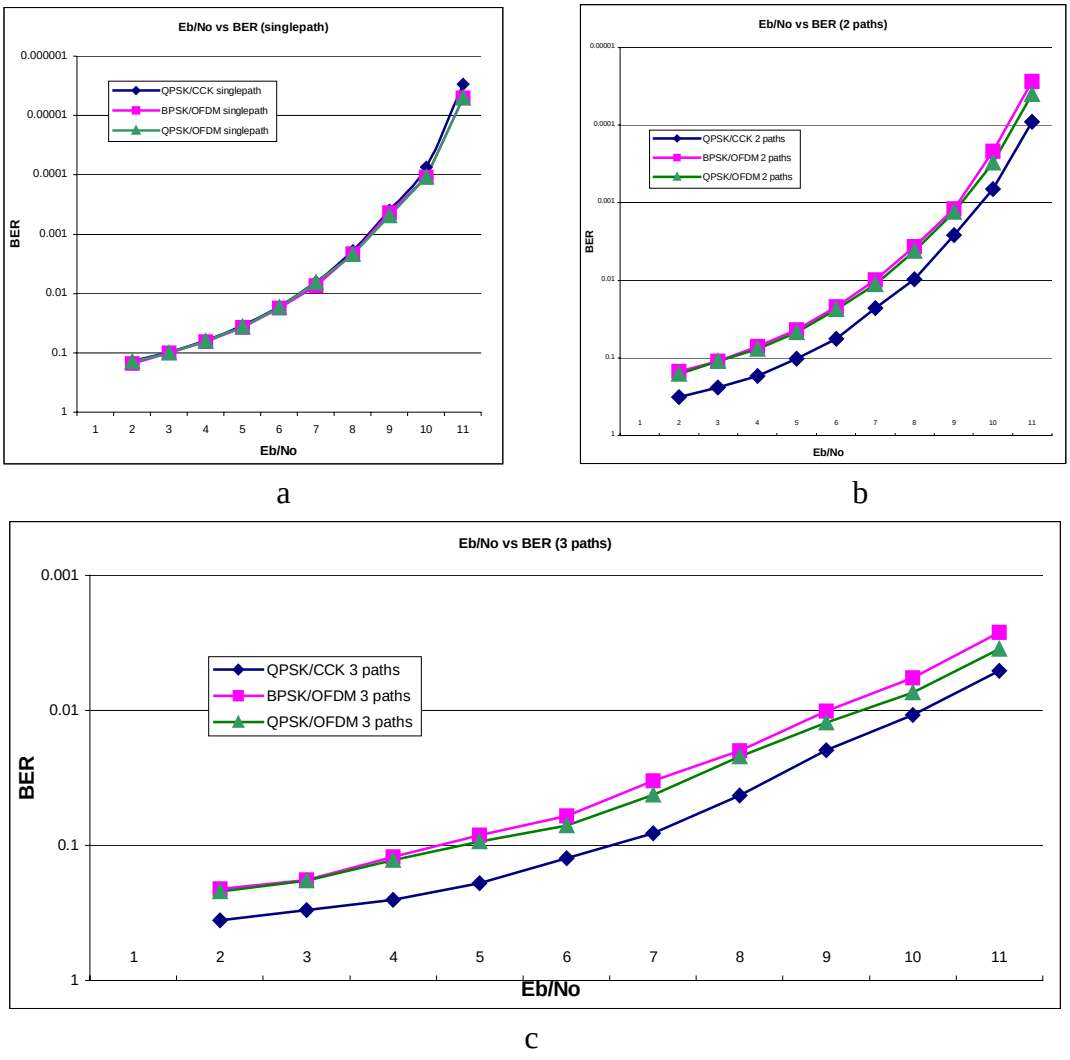


Fig. 6.11 Eb/No of the signal versus BER for various scenarios: a. no multipath noise; just AWGN, b. two paths (second is 10% of main path), c. three paths (second is 20% and third 10% of original)

On the multipath noise scenario [Fig. 6.11.b and c] noise values ranging from 1 to 10 dB were tested with 7dB being a typical noise figure in an average environment. For the above values, it can be seen that a clear 1 dB difference exists in favour of the

QPSK/OFDM modulation, something that is attributed to the more effective way that the OFDM deals with multipath interference. Both BPSK and QPSK behave similarly with QPSK having just a slight (but constant) advantage [Fig. 6.11.b].
As more paths were added the gap between the CCK and OFDM modulation grew even bigger and in some cases reached up to 2 dB [Fig. 6.11.c]. This also applies for different kinds of noise (frequency selective fading, Rice / Rayleigh effects having 250ns RMS delay spread in a NLOS environment, etc), or a combination of noise sources. The above simulation set was run multiple times and yielded an average statistical error between measurements, of 4.5%. This is an expected variance as the input to the modulator was random numbers.

For the upper layers that were simulated in OPNET, a great variety of statistical outputs were available, including throughput, delay, gain (dB), noise, videoconferencing delay, load for any of the network components (both wired and wireless) and many others. However, the throughput of the wireless client and the AP is of great importance, as it summarises many of these outputs and indirectly yields the overall videoconferencing quality: the higher the available bandwidth, the lower the compression and thus the higher the image quality.

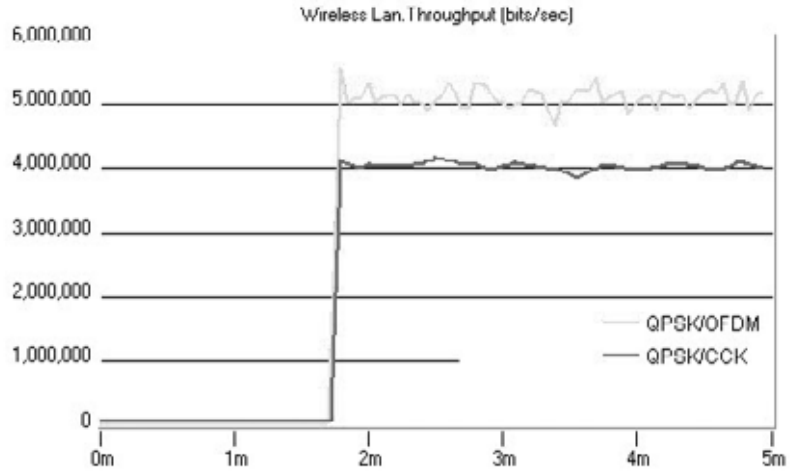


Fig. 6.12 An average increase of 1 Mbps was observed in the simulation, while using OFDM in a multipath environment

An average of 1Mbps improvement in the throughput was observed mainly due to the increase of Eb/No ratio described in the last paragraph [Fig. 6.12].

The above improvement would mean that more data can safely go through the communication channel and, for the specific telemedical application, a better video quality can be transmitted and consequently the doctors can make a more accurate diagnosis.

6.6 Summary and conclusions

In chapter 3 we presented several versions of WLANs that are on the market today, with IEEE 802.11a being one of the most recent to be commercially available in Europe and concluded that regardless of the countries that will deregulate the 5 GHz band (necessary to operate 802.11a) the dominance of 802.11b all over Europe today, is undisputable.

Based on that, in the current chapter we tried to suggest an alternative modulation technique for 802.11b that will offer distinct benefits to telemedical applications. Doing so, we started by identifying some typical problems that affect the QoS of a WLAN; namely the multipath interference and the relation between operating frequency and range or, in other words, the effects that reflecting paths have in the WLAN operation. We continued by laying out the basics for an advanced modulation technique (OFDM) and presented the benefits of using that modulation in an average healthcare environment.

This chapter continued with showing that for specific applications like Telemedicine, the best of the two worlds can be combined: from the 802.11b, we can use the extended range it has, its increased compatibility with radio regulatory committees all over the world and its relatively cheap hardware and from the 802.11a we can use its higher tolerance to multipath noise, a factor that affects extensively the signal quality and speed of the WLAN. The way this can be done is by replacing IEEE 802.11b's modulation with that of IEEE 802.11a thus using OFDM modulation instead of CCK.

Since 802.11a and 802.11b do not internally support QoS, real time applications are left to the mercy of the transport layer that, in turn, is highly dependent on the physical layer of the system. Real time applications would benefit considerably by minimising the number of errors due to signals being reflected over various surfaces and decreasing the quality of the communication channel.

Telemedical applications like MedLAN could take advantage of this “safer” communication environment and could be able to deliver a larger amount of data (in a highly reflective terrain like an old hospital) that would result in safer and more accurate diagnosis.
To implement the above most hardware manufacturers give end-users the ability to upgrade (flash) their firmware to include newer modulation techniques and advances, at no cost and through their support web pages. Provided that these hardware manufacturers will make such alternative firmware available, it would only take hospital network managers a small amount of time and no cost to include OFDM to the available IEEE 802.11b modulations. This offers a great advantage compared with the costly and time-consuming procedure of replacing and reconfiguring the entire WLAN with either IEEE 802 or the newer IEEE 802.11g: a compete replacement of APs is needed in the former, while in the latter the cost of the newly released hardware is considerable.

The above proposal has been modelled using two different simulation packages that specialise in different OSI layers. The conclusion based on the simulations is that despite the slightly increased computational power required of the WLAN’s CPUs, **using OFDM modulation** over IEEE 802.11b hardware, can **reduce** considerably the **multipath noise** thus increasing the available bandwidth.

During the next chapter, we will deal with the task of securing a wireless telemedical system. We will present a spherical approach to the problem, identifying some basic weaknesses of the existing WLAN protocols. We will then attempt to find easy and reliable ways to overcome these problems. We will also set a multiple-step procedure for securing a telemedical WLAN that deals not only with the lower layers of the system (MAC) but with the administrational aspect as well.

7. Securing a Wireless Telemedical System

7.1 Introduction

When using a WLAN system in a medical environment, the issue of confidentiality is instantly raised. Within chapter 2, it was made clear that in a telemedical session, security and confidentiality between the treating doctor and the patient is vital and must be preserved at almost any cost. Moreover, the NHSnet, responsible for supplying the data communication foundation of telemedical applications within the United Kingdom, has revised a set of rules to govern the various issues of exchanging medical information over its network and more specifically to ensure that these exchanges have adequate security.

As the MedLAN system relies on the use of WLANs to facilitate data exchange, there has to be a way of securing these data transmitted over the wireless link. WLAN vendors offer a set of four security measures for that purpose: SSID, MAC filtering, authentication and Wired Equivalent Privacy (WEP). Of those, WEP has by far raised a lot of ambiguity lately as, based on several publications, attacks on its basic encryption algorithm (RC4) can be proven successful thus destroying the overall system security.

This chapter will attempt to shed some light into some fundamental problems of securing a WLAN system, especially when this is addressing a medical environment. It will start by explaining some of the basic procedures of WEP along with some of its fundamental flaws that were discovered. It will argue that despite the recent mistrust of the WEP system, there are easy ways of minimising the risks that it poses. Furthermore, for implementing the highest level of security an alternative model will be presented, that will include the encapsulation of WEP over IPSec; an encryption algorithm that is used for implementing Virtual Private Networks (VPN). Practical experiments and benchmarks will reveal the advantages of this method along with any overhead imposed on the system. This approach is not novel in networking, but its application to a wireless system like MedLAN contributes in the Telemedical science.

7.2 Current security standards

Now that WLANs have become mainstream, organisations look positively on the benefits that they provide and are willing to deploy them in their working environment. However, network managers are reluctant or unwilling to accept this change without being sure that this innovation will offer the same amount of security found in wired LANs.

Security usually consists of privacy and access control. The former ensures that the data travelling within the WLAN can only be received and understood by the intended receiver. The latter ensures that data can only be accessed by authorised users [Cis00].

In wired LANs data travels through a cable and access to the LAN is governed by access to an Ethernet port. This means that privacy cannot be compromised unless there is a physical interception to the network hardware carrying the data. Contrary to wired LANs, WLANs data are broadcasted over the air and can be received by any potential client. As radio waves often extend outside the vicinity of the enterprise, installing a WLAN might seem like putting Ethernet ports everywhere, including the parking lot or the cafeteria across the street!

IEEE 802.11 task force recognised early the need for data security to ensure access control and privacy to the nominal users of these systems. For that reason, four basic security mechanisms are embedded into all modern IEEE 802.11 networking hardware: SSID, MAC filtering, WEP and authentication. Each of those will be explained, with emphasis on WEP.

- Service Station IDentifier (SSID) can simply be considered as the name of an AP. Naming APs is mandatory in an IEEE 802.11 network and its usefulness becomes apparent when several APs are deployed, that might be running on different properties.

  Mobile terminals are requested to log in to the AP by using its SSID name. If this information is not known, the association procedure with the AP cannot be initiated and therefore the AP denies service to the MT.

  The sole use of the SSID, however, is not considered a strong security method for two reasons: Unlike passwords, the SSID name tends to leak out to public (as a lot of people possess that information). Moreover, to simplify the installation and connection procedure, vendors tend to ship WLAN

hardware with the SSID turned to “broadcast” mode; transmitting its name along with every packet sent.

- Using MAC filtering is yet another way to control the access of users in a WLAN system: Each LAN hardware (LAN cards, routers, WLAN MTs, etc) has a unique six-byte identifier embedded in its hardware by the manufacturer, called “MAC address”. This is used to uniquely identify the hardware, especially in large networks or the Internet. The user can create a list of nominal MAC addresses (or MAC address ranges) that will be allowed to connect to the WLAN, while excluding any others [Fig. 7.1]. The downside of this is that when the WLAN system is rapidly expanding, the network manager is constantly obligated to add new users to the list. Furthermore, there exist programs on the market that can masquerade the MAC address of one hardware into another thus rendering this method of security inefficient.

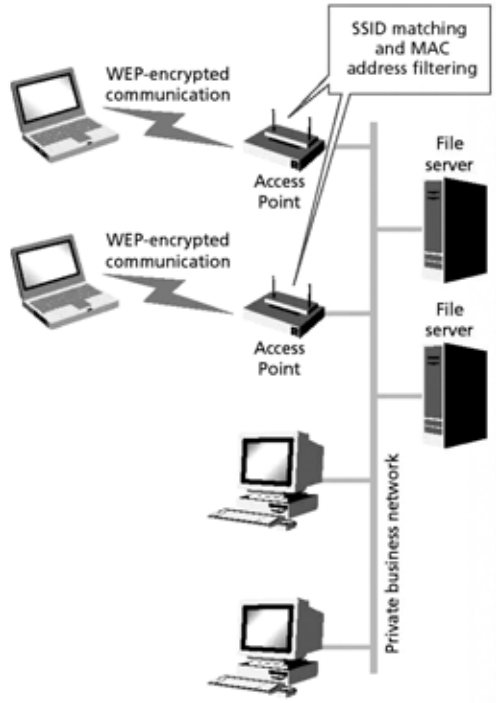


Fig. 7.1 SSID and MAC filtering process in an infrastructure WLAN

- WEP offers an integrated security mechanism that is aimed at providing the same level of security experienced in wired networks. The goals of WEP include: **Access control**, that prevents unauthorised users who luck the correct key to gain access to the network and **privacy** to protect WLAN data

streams by means of encryption, allowing decryption only to users possessing the correct key. WEP will be explained further during the next subchapter.

- Another mechanism for controlling the access of users to the WLAN, is the **authentication** procedure, as defined in chapter 3.9 IEEE 802.11 provides two types of authentication: **Open system authentication** simply permits the interacting parties to exchange their identities within the MAC control frame. This method provides no security benefits. Alternatively, **shared key authentication** requires the two parties to share a secret key, not shared by anyone else. The authenticating procedure for parties A and B is as follows:
    - A sends a MAC authentication frame that contains an authentication algorithm along with the SSID.
    - B responds with a 128-octet challenge text created using the WEP pseudo random number generator.
    - A transmits an authentication frame that includes the challenge text received from B and the entire frame is encrypted using WEP.
    - B receives the encrypted text and decrypts it using WEP and the secret key. If CRCs match, it means that the decryption is successful so B compares the output text with the one that was sent as a challenge. If the two match, then the procedure is authenticated.

7.3 WEP

To ensure access control, privacy and data integrity, WEP uses an encryption algorithm based on the RC4 [Sta01]. RC4 is a well-established algorithm that is currently used to encrypt data in e-commerce transactions and is considered adequately safe.

7.3.1 WEP encryption / decryption process

Fig. 7.2 shows the encryption process [Sta01]. The integrity algorithm is simply the 32-bit CRC check that is embedded at the end of each MAC frame [Fig. 3.5].

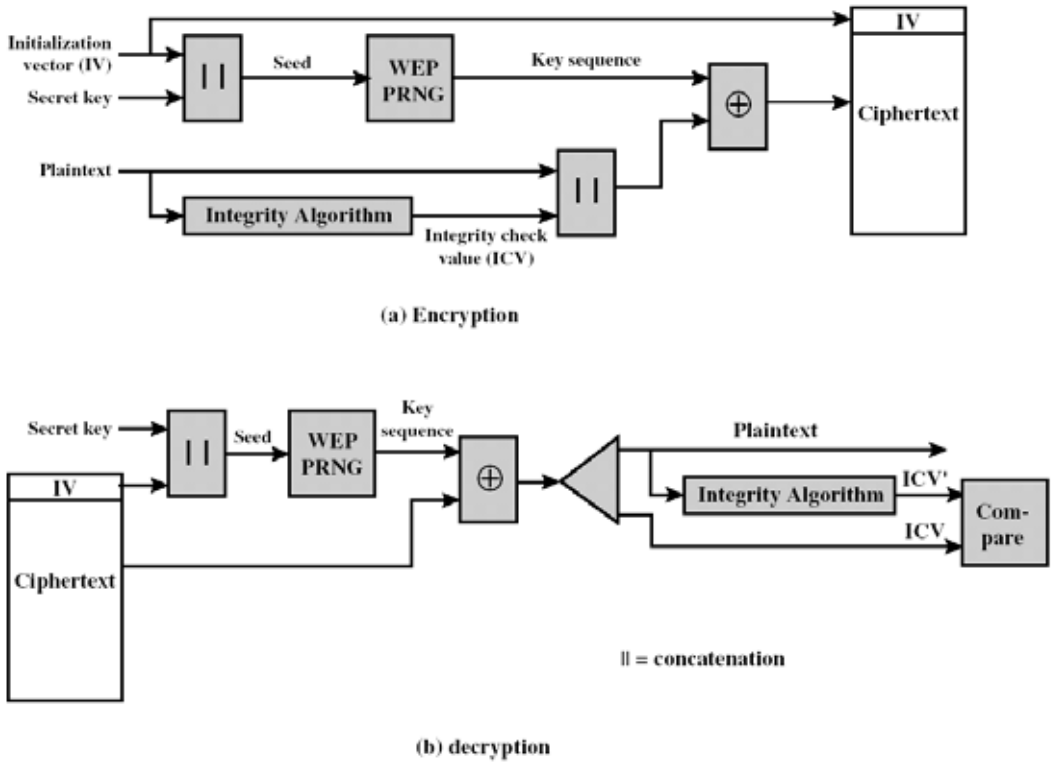


Fig. 7.2 Encryption and decryption process of the WEP algorithm based on an RC4 encryption.

For the encryption process, a 40 or 128 bit key is shared by both receiver and transmitter. An Initialisation Vector (IV) is created using this key (explained later). The output is fed to the Pseudo Random Number Generator (PRNG) defined in RC4 thus generating a bit sequence with the same length as the MAC frame plus the CRC. A bit by bit XOR between the MAC frame and the PRNG outputs the ciphertext. The IV is attached to the ciphertext and the whole train is transmitted [Fig. 7.2.a]. The IV is changed periodically (can change as often as each packet transmission depending on the hardware used). The more frequent the change of the IV is, the harder it becomes for an eavesdropper to decode the sequence.

At the receiving end, the receiver retrieves the IV from the data block and concatenates this with the shared key to generate the same key sequence as the sender. The output is XORed once again against the incoming block to recover the plaintext, taking advantage of the property of XOR: $A \oplus B \oplus B = A$ [Fig. 7.2.b]. Finally, the receiver compares the incoming CRC, with the CRC calculated at the receiver to ensure data integrity.

When defining the above procedure mathematically, the following procedures take place: [Bor01]

- A secret key “k” is selected and shared between sender and receiver.
- Having the message M, its checksum is computed c(M). The concatenation of the two yields the plaintext: P={M,c(M)}. Note that c(M) and thus P does not involve the secret key k.
- As a second stage, the P is encrypted using the RC4 algorithm: an IV “v” is chosen and RC4 generates a long pseudorandom sequence as a function of v and k denoted as RC4(v,k). Then, the plaintext is XORed with the above sequence: C=P⊕RC4(v,k).
- Finally, the IV and the ciphertext is transmitted over the air [Fig. 7.3]:

$$A \rightarrow B: v,\{(P \oplus RC4(v,k)\}$$

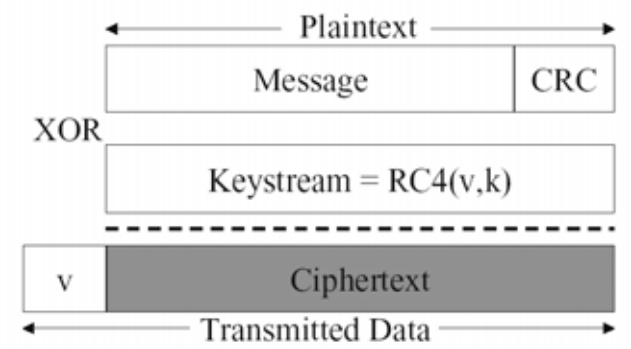


Fig. 7.3 Encrypted WEP frame

The decryption process is the exact opposite of the encryption as RC4 is a symmetric algorithm:

The keystream RC4(v,k) is generated and is XORed against the ciphertext to recover the initial plaintext:

P’=C⊕RC4(v,k)

={P⊕RC4(v,k)}⊕RC4(v,k)

=P

(M is the message, P is the plaintext and C is the ciphertext)

Finally, the receiver verifies the CRC checksum of the decrypted plaintext P’ by splitting it into the form (M’, c’), recalculating its checksum c(M’) and checking that it matches the received c’ to ensure that only frames with a valid checksum will be accepted by the receiver.

7.3.2 WEP implementation

To render the above encryption, hardware manufacturers ship their products with software suitable for changing and administering WEP keys. In the MedLAN case, the WLAN hardware used were produced by Cisco. Both 340 and 350 WLAN series were used, either on a stand-alone basis, or in collaboration with each other. This hardware has an extended Read Only Memory (ROM) embedded in the main board so an advanced firmware (software inside ROM) can be used to perform all necessary tasks.

Each AP gets a unique IP (either by the user, or by the DHCP server). The way to administer it is to use an Internet browser and direct it to the AP's IP address. Administering the AP through a web page simplifies the procedure for the novice user and does not decrease the level of functionality required by an expert user. Most of WLAN manufacturers use this web-page method for setting up their hardware.

One of the administration pages existing in the AP's firmware is "AP radio data encryption" [Fig. 7.4]

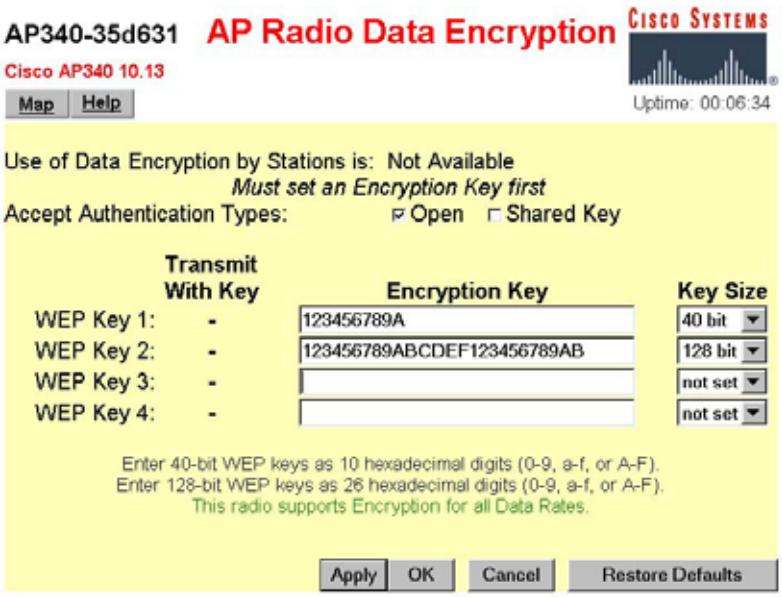


Fig. 7.4 Through a web page, the key (k) can be set for use by the AP. The key can either be 40 or 128 bits long in form of bytes. Note the "open" or "shared key" authentication method selection.

This allows the user to set up to four different keys (k) with either 40 or 128 bits of security. As inserting 128 bits can be proven confusing, the key's elements are organised in bytes. Only one of the four keys can be used at a time. Keys are being

kept secret (even to the nominal user) after being inserted to the AP. Keys can be deleted but not altered.

On the MT side, a similar procedure takes place: the user, having possessed the key (k) must enter it using a special program in order to establish communication with the AP. The MT card has an EEPROM memory that can store this key, even in the absence of electrical power. In other words, the key is permanently stored in the card; something that may be considered as a security risk.

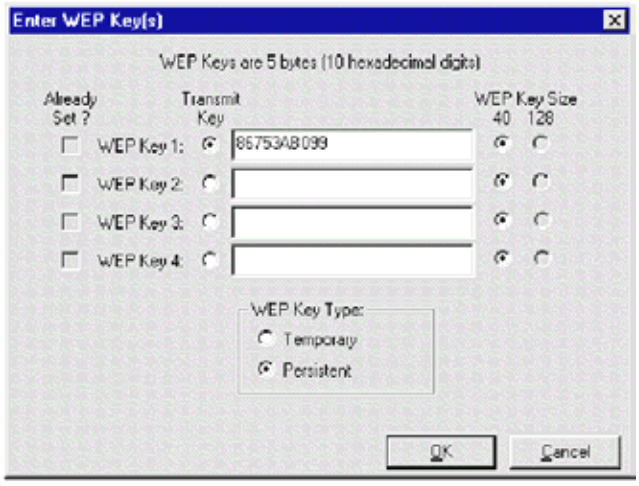


Fig. 7.5 Setting the WEP key on the MT's side

Some hardware vendors give the user the ability of setting either a "persistent" (constantly stored in the card) or "temporary" key that will be lost after rebooting the machine [Fig. 7.5].

7.3.3 WEP overhead benchmark

Considering Fig. 7.3, it is expected that since the procedure of using a WEP key generates additional traffic, it will have some effect on the performance of the wireless network throughput. Unfortunately, metric procedures for these kinds of operations are in their infancy, so one has to rely more on practical measurements [Wil01].

A number of publications have considered this issue and almost all of them tend to agree that the use of WEP has the effect of increasing the computational power of the hardware (handled by the WLAN), rather than the throughput itself. Table 7.1 illustrates this notion [Wil01], [Fli03].

Speed (Mbps)	No WEP	40-bit WEP	128-bit WEP
1	1048576	1175773	1178175
2	2128106	2120282	2116391
5.5	3673355	3627149	3650106
11	4164020	3857637	3806711

Table 7.1 Effects of WEP encryption on the IEEE 802.11b throughput

The experiment was conducted while receiver and transmitter had a nine meter distance through three walls and a solid wood door. Notice that for low speeds, the use of WEP plays almost no role at all. On the maximum speed of 11Mbps, a decrease of 8-16% was observed. The same experiment was repeated at CMH producing similar results.

Conclusively, despite the general feeling that WEP use can produce a high volume of unnecessary overhead, experiments tend to agree that this is actually kept to a minimum.

7.4 WEP vulnerabilities

In the past two years, various research groups have published a number of papers indicating that the IEEE 802.11 is open to attacks by attackers using relatively easy methods [Arb01], [Bor01], [Flu01], [Stu01]. These papers also indicated that poor authentication implementations and bad management could further decrease the level of security in a WLAN. Some of them went further to suggest ways to improve security and even countermeasures against the attackers [Wil02], [Joh02]. Articles on the researchers' findings appeared in the Wall Street Journal, among other publications, and raised the concern of the public who, up until then, considered WEP as a solid security solution. The articles reported that these attacks tend to undermine the ability of 802.11 to perform adequately on its basic objectives: confidentiality, access control and data integrity.

In the remaining of this subchapter, there will be a basic description of the flaws embedded in the WEP implementation, along with the corresponding attacks that can be performed by taking advantage of these flaws. Note also that WEP has been

implemented in two versions: 40-bit and 128-bit key. The 40-bit key was defined in the standard to accommodate for US regulations. Unfortunately, by applying a brute-force attack, 40-bit keys can be broken in a modest time frame. 128-bit key, on the other hand, seem to be invulnerable to brute force attacks, although shortcut methods can be used.

7.4.1 Risk of keystream reuse

As WEP uses a stream cipher (RC4), that operates by expanding a secret key into an arbitrary long keystream of pseudo random bits, encryption is performed by XORing the generated keystream with the plaintext. A well-known disadvantage of those ciphers is that encrypting two messages under the same IV can reveal information about both messages [Bor01]:

If $C_1 = P_1 \oplus RC4(v,k)$

and $C_2 = P_2 \oplus RC4(v,k)$

then $C_1 \oplus C_2 = \{ P_1 \oplus RC4(v,k)\} \oplus \{ P_2 \oplus RC4(v,k)\} = P_1 \oplus P_2$

meaning that by XORing C_1 and C_2, the result is the XOR of P_1 and P_2

This can lead to a number of attacks, especially if any part of the text in known [Daw96]. The trick to avoid this is to have the ability to change the IV with every packet sent; something that is suggested in the WEP specifications. Unfortunately, these specifications fail to indicate how to do so, thus many implementations do it very poorly: with a starting value of zero, the IV is incremented by one every time a packet is sent. When the hardware is powered off, the procedure begins once again from zero. Even worse, as the IV is always 24 bit wide and with a speed of 11Mbps and a packet size of 1500 bytes, it is guaranteed that the same IV will appear every about 12 hours.

Once two packets encrypted by the same IV are discovered, various methods of attacks can be applied to recover the plaintext:

- Many fields of the IP traffic are predictable and so are many initial states of the login procedure (e.g. a remote computer usually displays the word “password” while initialising a connection).
- Another way to do so is to cause a known plaintext to be transmitted over the air (for example send some IP traffic directly to the mobile host using the Internet).

- Finally, even if no plaintext is known, some analysis is still possible by performing an educated guess about the traffic.

After the plaintext of a packet becomes known by using any of the above methods, the attacker can use this same keystream to decrypt any other message encrypted with the same IV. By persistent work, a complete dictionary of IVs and corresponding plaintexts can be built having a modest size of about 2^{24}=24GB. This way, an attacker can take advantage of the low frequency that the keys are renewed in the system and immediately decrypt any broadcasted message.

Finally, it is worth mentioning that there is no standardisation as to the way that the keys (k) are distributed among the users. Since there is usually a single key for all MTs, the task of key insertion is performed by the network administrators manually, something that poses a great deal of managerial overhead.

7.4.2 Message authentication

CRC is a field used by WEP to ensure that the contents of the packet have not been modified during transmission. This CRC-32 is embedded in the encrypted part of the packet.

CRC, however, is not a cryptographically secure algorithm and leaves the system open to a number of malicious attacks, described below:

"**Message modification**" means that contrary to security goals, a message can be modified during transmission, without disrupting the checksum. This method takes advantage of the linearity properties of WEP: $c(x \oplus y)=c(x) \oplus c(y)$ for all choices of x and y. Let us assume that C corresponds to some unknown message M so that $C=RC4(v,k) \oplus \{M,c(M)\}$. There can be a C' that decrypts M' where $M'=M \oplus D$ and D can be chosen by the attacker. Then the attacker can substitute C with C' thus the recipient will receive a modified message M' with the correct CRC. To obtain C' from C (so that C' decrypts to M' instead of M) we use the following equation:

$C'=C \oplus \{D, c(D)\}$

$= RC4(v,k) \oplus \{M,c(M)\} \oplus \{D.c(D)\}$

$= RC4(v,k) \oplus \{M \oplus D,c(M) \oplus c(D)\}$

$= RC4(v,k) \oplus \{M',c(M \oplus D)\}$

$= RC4(v,k) \oplus \{M',c(M')\}$

"**Message injection**" refers to the ability of an attacker to inject arbitrary data into a message. This takes advantage of the fact that CRC can also be computed by the attacker who has intercepted the message: if an attacker knows the plaintext corresponding to a frame of transmitted data, it will be possible to inject arbitrary data into the network.

As shown earlier, knowledge of both plaintext and ciphertext reveals a keystream that can be reused to create a new packet using the same IV:

$P \oplus C = P \oplus \{P \oplus RC4(v,k)\} = RC4(v,k)$.

A message M' can be constructed, where

$C' = \{M', c(M')\} \oplus RC4(v,k)$.

Note that the rough message uses the same IV as the original. However, it is a fundamental property of WEP that older IVs can be reused. This property allows for packets that were delayed in transport to be considered valid by the system. Not accepting older IVs will risk no compliance with the WLAN system. This is considered a fundamental flaw of the WEP implementation.

Furthermore, the same technique can be used during an authentication procedure, using a shared-key: if the attacker posseses a set of plaintext / ciphertext (after monitoring a legitimate authentication sequence), it is trivial to derive the keystream used to encrypt the response. Since all authentication responses are of the same length, the recovered keystream will be sufficient to create a proper response for a new challenge, and subsequently, authenticate oneself into the network.

In "**message decryption**", the attacker tries to decrypt the entire ciphertext. As a direct attack on the cryptography of WEP is pointless, the trick is to have another device that can perform this task. Such a device is the AP that is obligated to possess the key and the ability to decipher the encrypted message. Basically, in this type of attack, the adversary uses the AP as an aid to perform the attack.

One way to do so, is to modify the destination address of an IP packet, so the AP will send it to an address that is controlled by the attacker. Since most firewalls limit incoming traffic but allow for outgoing traffic, this should not be so difficult.

The easiest way to modify the IP address is to try to guess a nominal destination address; something that is not as hard as it sounds: most traffic have a small range of destinations. The trick is to be able to inject the new IP address without alarming the CRC checksum of the packet; something feasible and documented in the bibliography [Bor01].

Another way to implement message decryption is to use a fundamental property of the TCP protocol (most network communications rely on using this). In this kind of attack, the reaction of the TCP protocol is monitored: whenever a nominal TCP packet is accepted (having the correct checksum), a fixed-length response is being transmitted from the receiver to the sender. This response, although encrypted, is easily detected by its format.

In the attack, a ciphertext (v,C), with an unknown P, is intercepted. A few bits of C are flipped and CRC is adjusted accordingly to obtain a new ciphertext C'. After transmitting the C' the attacker monitors if the AP will send an ACK packet back or it will discard the packet completely.

The trick is to cleverly choose the bit positions that are flipped, so the TCP checksum remains undisturbed exactly when the one-bit condition $P_i \oplus P_{i+16}=1$ on the plaintext, holds. Thus, the presence or absence of a ACK packet will reveal one bit of information on the unknown plaintext P. By repeating the attack for many choices of i, one can learn almost all of the plaintext P [Bor01].

7.4.3 Future improvements: AES and WPA

Following the concern the above mentioned vulnerabilities of WEP caused to the public, the newly formed IEEE 802.11i task group was charged by standardising a better, more secure method for operating WLANs. The 802.11i is a work in progress and is just beginning to publicise some of its recommendations. Final standards are not expected before mid 2004.

This standard promises to completely revamp the architecture of WLAN security environment by upgrading the entire secure-key procedure. The RC4 algorithm will be abandoned and will be replaced by the newer Advanced Encryption Standard (AES) (it must be clear that the RC4 algorithm does not suffer from any fundamental flaws and is still used by banks to perform secure on-line transactions; it is its implementation inside the WEP protocol that was poorly designed).

AES is a relatively new cryptographic algorithm that can be used to protect electronic data. Specifically, AES is an iterative, symmetric-key block cipher that uses keys of 128, 192, and 256 bits long, and encrypts and decrypts data in blocks of 128 bits (16 bytes). Unlike public-key ciphers, which use a pair of keys, symmetric-key ciphers use the same key to encrypt and decrypt data. Encrypted data returned by

block ciphers have the same number of bits that the input data had. Iterative ciphers use a loop structure that repeatedly performs permutations and substitutions of the input data [Caf03].

AES is the successor to the older Data Encryption Standard (DES). DES was approved as a Federal standard in 1977 and remained viable until 1998 when a combination of advances in hardware, software, and cryptanalysis theory allowed a DES-encrypted message to be decrypted in 56 hours. Since that time numerous other successful attacks on DES-encrypted data have been made and DES is now considered to have past its useful lifetime. It has been calculated that if a machine could recover a DES key in a second (i.e., try 2^{55} keys per second), then it would take that machine approximately 149 trillion years to crack a 128-bit AES key [NIS04]

AES was created in 1999, using the "Rijndael" algorithm, created by researchers Daemen and Rijmen [Dae99]. It was selected by the NIST as the proposal that best met the design criteria of security, implementation efficiency, versatility, and simplicity. AES is widely expected to become the de facto standard for encrypting all forms of electronic data including data used in commercial applications such as banking and financial transactions, telecommunications, and private and Federal information [NIS04], [Caf03].

Until the IEEE 802.11i standard comes into effect, the Wi-Fi alliance recommends a subset of the 802.11i standard to replace the current WEP implementations. The Wi-Fi Protected Access (WPA) is an interim solution that will increase security over current WLANs and open the way to 802.11i future developments [Wil02]

WPA will work like the authentication system in 802.1x. MTs and APs must both support WPA and the access point will need to be connected to a Radius server, (that supports 802.1x and EAP) to perform an authentication procedure. The Radius server will then provide the same authentication service performed by dial-up modem users: it will block all access to WLAN until the client has been authenticated, usually through a login procedure (username and password). Once this procedure has been completed, the Radius server sends the WEP session key to the client and both MT and AP use this key for that WLAN session [Fig. 7.6]. The complete sequence of events using a Radius server, can be found in Appendix L [Cis00], [Cis02a], [Cis02b].

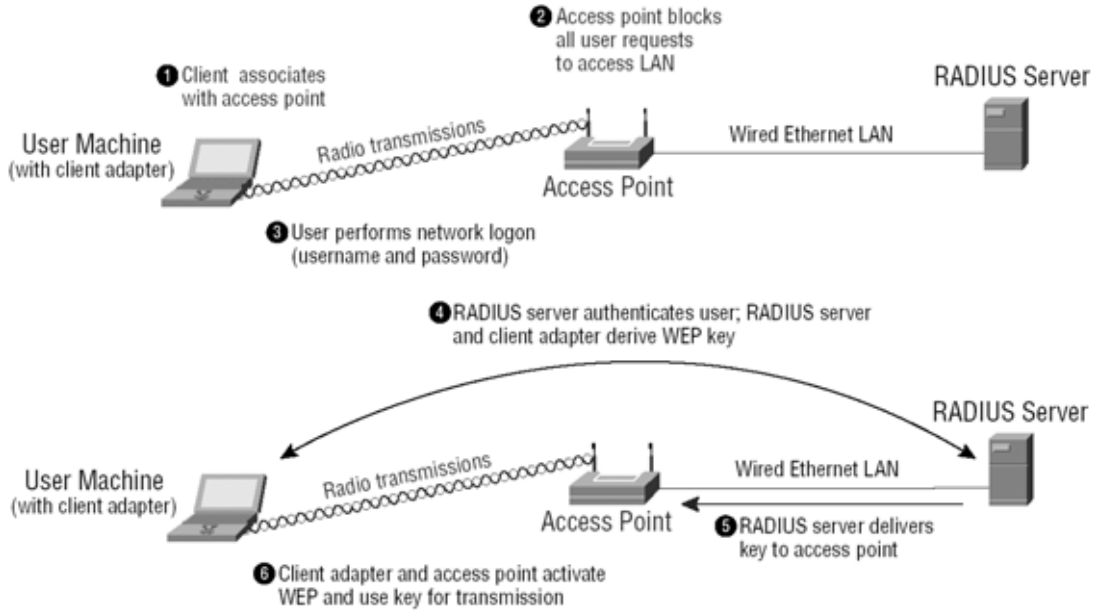


Fig. 7.6 Using a Radius server as an interim solution between the existing WEP and the future 802.11i: sequence of events

The advantage of this approach is that it relies on user-memorable information (password) rather than keys permanently stored on a card. The drawback, on the other hand, is that it requires the existence of a separate Radius server to authenticate the user; a luxury that SOHO users cannot usually afford.

7.4.4 Concerns and unjustified fears of WLAN security

It is important at this point to make a clear distinction between the theory and the practice of WLAN security attacks: it is one issue to be able to prove that under given circumstances there is a mathematical chance of penetrating the WLAN WEP security, and a very different issue to prove that this is generally feasible and relatively easy to implement.

Almost all of the above mentioned studies, were basing their conclusions on a number of prerequisites: using a low-end WLAN card, using weak keys, not changing the session keys, partial knowledge of the text, assumption that it is **text** that is sent over the WLAN, adversaries that are extremely well equipped or even no existence of WEP. Even if one of these circumstances did not apply, the attack would not be successful.

It is the author's opinion that some fundamental weaknesses of the WEP implementation were exaggerated and over-publicised by the press using fearsome titles like "Your WLAN security has no cloths". This approach raised a partially unnecessary concern to the public that has no specific knowledge on how WLANs work and sometimes resulted in enterprises shutting down their WLANs in a state of panic.

To make matters worse, these concerns were shared by some of the doctors and patients while the prototype MedLAN system was under development. This seriously undermined the trust between the treating doctor and the patient; a trust that is **fundamental** during any telemedical procedure [chapter 2.4.1].

At the risk of investing a considerable amount of time to explain to every user of the system the particularities of the MedLAN system and the many reasons why MedLAN is tolerable to these kinds of attacks, the security of the MedLAN system was improved even further, to ease the concerns of both the healthcare personnel and the patients.

7.5 Management and human issues of telemedical security

It would be pointless to view the security of a telemedical system while giving concern only to the mathematical and technical properties of the system. To address the issue spherically, one should be concerned with the possibilities of security threats via other means that are not referred to in the bibliography so often. What good is a very efficient encryption algorithm, if a password can be easily leaked by an unhappy employee, or if a spy camera can be placed near the operation terrain of the WLAN?

Moreover, it is imperative to understand that network security should not only be handled by a qualified engineer but should be documented with the help of the management of the enterprise. **They** are the ones who will give guidance and will set the rules that the security policy should follow.

7.5.1 Management issues

To understand how to secure wireless links, it is necessary to understand how the system can be attacked [Owe01]. In rare circumstances, and even if the encryption

cannot be broken, it can be forced to be weak by interfering with the key generation system on purpose. It may even be possible to make the WLAN cards radiate the unencrypted wireless message or a subliminal channel could be added to make the cards leak the keys onto a predefined destination. These attacks could be put into place during product design and development, before the cards are shipped to the hospital, or during maintenance and system upgrades. Despite this scenario resembling a scientific fiction movie, there is a **much higher** probability of this happening rather than breaking a properly configured WEP encryption, as it is today. There are a number of other things that can be done that do not directly involve the secure wireless link. Bugs can be installed inside the computer or in the A&E room. The people using the system can be bribed and so forth. The hospital management cannot reasonably expect the secure wireless links to be able to deal with such threats.

Implementing a **security policy** is the only way to address the problem spherically. A security policy for a system defines the aims goals and addresses the threats and provides a framework for selecting and implementing countermeasures against these threats. A single written policy forces every employee to its guidelines. Such policy should clearly state who is responsible for what (implementation, enforcement, audit review). Finally, a hospital's data security policy would have to be expanded to accommodate for future telemedical systems when they are introduced.

After a risk has been identified, one of three things can be done: the risk can be **accepted**, **reduced**, or it can be **insured against**. **Security does not have to be perfect but the risks have to be manageable.** Technical solutions mitigate risk to the point where it is insurable. The need to insure the security of the data handled by the MedLAN system will have to be budgeted for on a yearly basis. Counterintelligence is the only way to stay abreast of what is really going on. Insurance will handle the residual risk but it is the job of the experts to keep being informed of new securities and security threats.

In the near term, it is expected that a variety of outsourced security services will become available. Managed security monitoring is required, as someone has to monitor security products in real time and respond to events as they occur. The same person has to be able to maintain the security products in the face of an ever-changing network and ever-changing services running on the network. Hospitals

cannot do this for themselves and the demand for such services, generated by the MedLAN system, will have to be budgeted for on a yearly basis.

7.5.2 Human issues

For some time, there has been the problem of confidentiality in telemedicine. [Tac96]. In a public opinion survey, it was found that patients were very concerned that details of their illness could be available to relatives or strangers. One comment was: “how do I know that someone won’t scoop an armful of videos and laugh at a whole lot of patients?”. These comments were further aggravated by the recent publication of the WEP security flaws, giving rise to further concerns.

There is also the risk of the teleconsultation being physically overheard. Luckily, one of the great advantages of a WLAN system like the MedLAN is the ability of the trolley to be wheeled around a ward area so that the above risk is reduced.
During the following subchapter, there will be an analytical description of the problem of securing a medical WLAN, the concerns, the attitude to follow and the steps that were taken to ensure against such attacks. Overall, a set of countermeasures for the attacks described below will be presented, along with a complete security solution, realisable using currently available technology.

7.6 Creating a set of countermeasures

As mentioned above, there exist a number of indirect attacks that can take place, to compromise the security of a WLAN. Apart from the attacks to the RC4 implementation, a malicious party can also go into extreme lengths: theft of already set hardware, bribe disloyal or unhappy personnel, or even place rough APs to disrupt the operation of the WLAN. (A possible attack to the system could be made by placing a dummy AP close to the existing WLAN. As clients will always try to associate with the AP that offers the best signal to noise ratio, they will connect to the dummy AP losing contact to the valid network. However, a simple site survey reveals the “hidden” APs) [Ban02b]
A summary of simple steps that both the developing engineer and the management can take to reduce considerably the security risks, are listed below [Joh02]:

7.6.1 Immediate Actions

- Regardless of any problems that WEP might have, use it to encrypt the transmitted data.
- Change the default SNMP community strings (passwords). The common management protocol used to manage all Access Points is SNMP (Simple Network Management Protocol). SNMP stores its management information in a special database called a MIB. Access to the MIB is controlled with a password (officially called a community string). Every manufacturer configures its products with a default community string that should be changed as soon as possible (e.g. username: admin, password: admin)
- Change the default Access Point SSID. To start a connection (authenticate and associate) with an Access Point, the client needs to know its SSID. This information can be possessed in a number of ways:
    - It is revealed by the network administrator.
    - the AP is broadcasting it.
    - the AP has been set to a NULL SSID and will accept connections from any MT.
    - the AP SSID has not been changed since it was taken out of the box and it still has the one set by the manufacturer.
- Disable the broadcast SSID feature of the AP (unless really needed in cases like internet cafes or public access WLANs where is necessary)
- Change the default password for administrative access to your Access Point. All manufacturers have default passwords that are public knowledge. It should be changed (and should have strong password quality characteristics) as soon as possible to prevent unauthorised users from connecting to the AP and making unauthorised configuration changes that can lead to them taking over the control of the WLAN.
- Survey your site to understand how far the APs are actually broadcasting their signals. If it is a multi-floor building, one must remember to map the vertical coverage too. Account for rough APs that can disable the normal WLAN operation.
- To restrict the signal, one can change the placement of the APs or to consider the use of more specialised (directional) antennae.

- There is also the option to restrict the strength of the antenna signal, if the manufacturer of your AP allows it. This will reduce the overall coverage area (e.g., to keep it within your physical boundaries and not radiate past the walls). Nevertheless, one should also keep in mind that the adversary might utilise a sophisticated antenna with a longer range than found on a typical 802.11 configuration [Stu01].
- Given the ease of deploying wireless network extensions and the current state of wireless insecurity, it is vital to monitor for unauthorised or inappropriate traffic.
- If sensitive data is going to be transmitted to or from the clients, one needs to look into some type of end-to-end security solution to protect it (explained later in this chapter).

7.6.2 Configuration and Management Actions

- Consider the use of MAC level (Ethernet) address filtering to limit the number of clients the AP will "pay attention" to.
- Treat all systems connected via a 802.11 as external. Consider placing the AP in the De-Militarised Zone (DMZ) (as opposed to being attached directly to your internal networks) and in front of a firewall. Having a firewall between the internal network and the Access Point is always a good practice because it gives the management flexibility and control [Fig. 7.7]

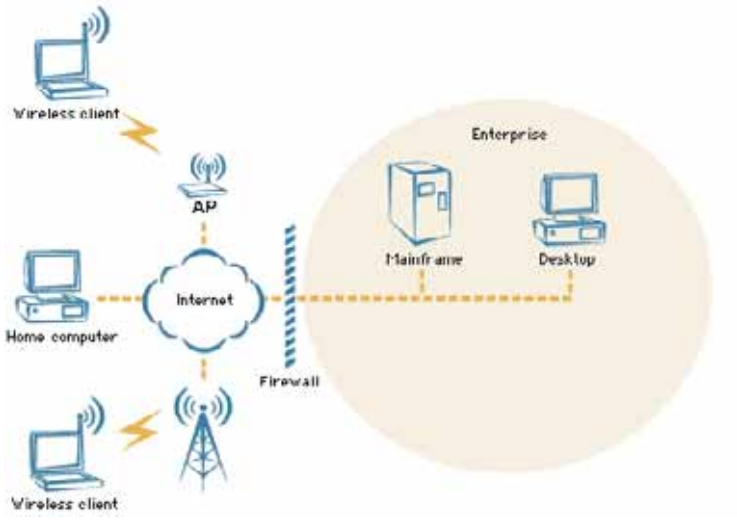


Fig. 7.7 Treating the WLAN system as external: placing the AP behind the enterprise's firewall.

- Consider configuring the Access Point so that it will not respond to “probe-response” requests. This means that clients will have to explicitly know the Access Point connection information beforehand. The publicly available “war driving” tools use this technique; they constantly send out “probe-response” packets on all channels and record all Access Points responses.
- Consider whether the AP should offer DHCP for new clients. While most AP manufacturers provide the capability for the device to offer dynamic IP addresses via the DHCP protocol, enabling this feature means that any client will also be offered this service to connect to the network infrastructure.
- Support mutual authentication between a client and an authentication server using Radius servers described above [Cis00].
- Base WLAN security on device-independent items such as usernames and passwords, on top of existing WLAN security.
- Use WEP keys that are generated dynamically upon user authentication, not static keys that are physically associated with a client. Furthermore, support for session-based WEP keys.

7.7 IP Secure (IPSec)

Designed by the Internet Engineering Task Force (IETF) as the security architecture for the Internet Protocol (IP), IPSec defines IP packet formats and related infrastructure to provide end-to-end strong **authentication, integrity, anti-replay**, and (optionally) **confidentiality** for network traffic. It is specified by a set of IETF standard documents (RFCs 2401 to 2411 and 2451), which define an architecture for encryption. An on-demand security negotiation and automatic key management service is also provided using the IETF-defined Internet Key Exchange (IKE), (RFC 2409). IKE is used to set up the trust relationship between two peers [Tah03].

IPSec is a **framework of open standards** for ensuring secure private communications over Internet protocol networks. Open standards means that IPSec does not specify exactly which encryption algorithms must be used by its applications, but instead provides an empty infrastructure (shell) where the desired algorithms can be set. This actually is an efficient design, as it allows the

implementations to be modular, customisable for specific problems (WLANs) and easily upgradeable with new algorithms. That is the reason why IPSec is the basic algorithm of Virtual Private Networks (VPN).

Depending on which devices it is deployed, the implementation of IPSec takes the form of one of the following typical scenarios:

- Host-to-host communication: IPSec is deployed on each host that requires secure communication services. Each host-pair negotiates its own IPSec parameters and establishes its own connection. This would be typically the case when two users wish to share a private connection over the WLAN and will be explained later in reference to the MedLAN system.
- Gateway-to-gateway communication: IPSec is deployed on network gateways, which can be either routers or special firewalls. Each pair of security gateways establishes a secure tunnel over which all the hosts in the LAN send protected packets. This is completely transparent to the hosts, hence it is well suited for connecting distant LANs over the Internet or over the insecure WLAN 802.11b.
- Host-to-gateway communication: IPSec is deployed both on a security gateway (already defined above) and on a host (typically, a mobile station) that remotely connects to it. In this scenario, a remote user (e.g. a tele-worker or a WLAN user) is able to reach a private / backbone LAN, without requiring a dedicated connection as the IPSec environment between the station and the gateway ensures that all the packets are protected.

7.7.1 IPSec architecture and function

The security services within IPSec are provided by one of two protocols, the **Authentication Header** (AH) and the **Encapsulation Security Payload** (ESP). Each of these provides certain services and may be used separately or together.

- AH packets are IP packets with the purpose of providing data source verification, packet integrity and replay protection, but not data or traffic flow confidentiality. Connectionless data integrity means that the original IP packet was not modified in transit from the source to the destination. Data source verification confirms the source of the data. Together these two combined services are referred to as “authentication”. The AH is either

inserted between the original IP packet header and payload, e.g. TCP header + data, for the “Transport Mode”, or prefixed to the original header along with a new IP header in “Tunnel Mode” (more details concerning IPSec modes can be found on Appendix M). The AH contains a cryptographic checksum. The default cryptographic algorithms for calculating the checksum are **hash-based message authentication code** (HMAC) coupled with the **Message Digest 5** (MD5) hash function or HMAC coupled with the SHA-1 hash function.

A hash algorithm is a one-way mathematical function that takes a variable-length message and produces a unique fixed-length value. SHA-1 is considered a stronger hash function as it produces a 160-bit authenticator value (cryptographic checksum), versus a 128-bit authenticator produced by MD5. AH also provides an anti-replay service that can be used to counter an attack based on an attacker’s intercepting a series of packets and then replaying them.

- ESP packets are similar to AH packets. ESP provides data confidentiality, as well as authentication and anti-replay capabilities. Under the right circumstances, it can also provide some traffic flow confidentiality.

  Confidentiality is achieved through encryption. ESP supports a variety of symmetric encryption algorithms for the encryption of the data. The default algorithm, Data Encryption Standard (DES), has been in use for about 20 years now. DES uses a 56-bit key. However, because it has shown to be cracked by brute-force attacks, Triple DES (3DES), is considered better. In addition, the newer, faster, and more secure standard encryption algorithm, (AES) can be implemented within IPSec.

7.7.2 IPSec key advantages

In an earlier subchapter, there was a mention of a fundamental flaw of WEP encryption: the limited number of possible IV keys (2^{24}) can lead to IV collision.

In contrast with WEP, IPSec uses a **unique key for each direction of each session over each** (virtual) **link**. As it uses 3DES with an effective key strength of 112 bits, there must be about $2^{56}/2=2^{55}$ sessions before there is any significant chance of collision between two randomly generated keys. An attacker has to assemble a very

large database of cipher texts before a hope of discovering a collision. Furthermore, 2^{55} translate to about 2^{36} (64 billion) new sessions, each second for over twenty years.

When using 3DES, each session takes its IVs from a 64-bit space (128-bit space when AES is used). This means there is no significant chance of randomly selected IV collision until after about 2^{32} packets so IPSec renders such a collision probability too unlikely to worry about.

IPSec also allows a single key to encrypt 2^{32} packets at most, so the probabilities add up against an attack.

7.7.3 Authentication and key management

Similar to WEP, the whole IPSec architecture is based on the presence of some common secret keys on both peers. Because all keys have to be exchanged in order for the parties to communicate securely, key exchange and management is an important part of IPSec. Contrary to WEP, which uses manual methods of doing so, two methods of handling key exchange and management are specified within IPSec: manual keying and Internet Key Exchange (IKE).

The first method (similar to WEP) has proved to be deficient when the key length is high and the number of stations sharing the same key is growing. Therefore, to handle the key problem, IPSec uses the Internet Key Exchange (IKE) protocol that automates the keying and re-keying processes.

A Diffie-Hellman exponentiation is used to assist in generating a strong initial key. Before IKE proceeds, the potential parties must agree on a way to authenticate themselves to each other. This authentication method is negotiated during the IKE phase main mode exchange. **Digital certificates** involve the use of a trusted third party, called a Certificate Authority (CA), to validate the authentication of each peer. Digital certificates offer the added benefit of no repudiation, in the sense that a peer can verify that communication actually took place [Tah03], [Sta02]

7.7.4 Using IPSec

IPSec consist of a set of rules along with their corresponding actions and settings. Rules determine which types of traffic IPSec must examine, how traffic is treated, how to authenticate an IPSec peer, and various other settings.

An IPSec policy consists of one or more rules that determine IPSec behaviour. Each IPSec rule contains the primary following configuration items:

- Filter list: A single filter list contains one or more predefined packet filters that describe the types of traffic to which the configured filter action for this rule is applied.
- Filter action: A single filter operation that includes the type of action required (permit, block, or secure) for packets that match the filter list. For the secure filter action, the negotiation data contains one or more security methods that are used (in order of preference) during IKE negotiations and other IPSec settings. Each security method determines the security protocol, the specific cryptographic algorithms and session key regeneration settings used.
- Authentication methods: One or more authentication methods are configured (in order of preference) and used for authentication of IPSec peers during main mode negotiations. One of the available authentication methods is the Kerberos V5 protocol that is used in cases of a certificate issued from a specified certification authority, or a pre-shared key.

Fig. 7.8 illustrates a practical example of using IPSec: a user on Host A is sending a message to a user on Host B assuming that IPSec has been employed for both computers. At the user level, the process of securing the IP packets is transparent.

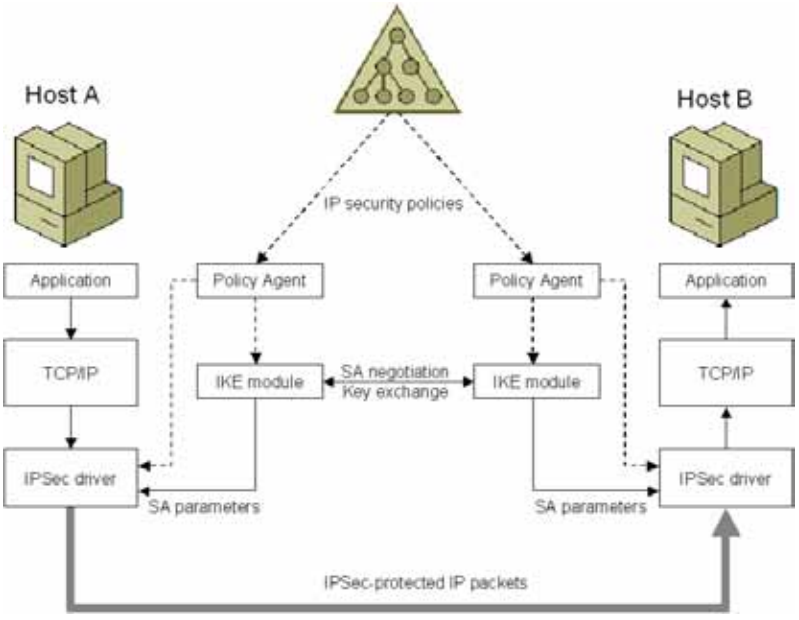


Fig. 7.8 Implementing IPSec in a standard network:
the procedure is transparent to both users as IP packets are encapsulated within IPSec

The IPSec policies assigned to the domain system containers of Host A and Host B determine the level of security for the communication. The IPSec policies are retrieved by the IPSec Policy Agent and passed to the IKE module and the IPSec driver. The IKE module on each computer uses the negotiation settings of the IPSec policy to perform computer-level authentication, determine the secret key and how to negotiate the protection of IPSec traffic and IPSec-secured traffic. The IPSec driver uses the IP filter settings of the IPSec policy to determine what types of traffic are to be protected.

Assuming that Host A and Host B are not already communicating securely and a message that Host A sends to Host B must be secured, IPSec works in the following way [Fig. 7.8]:

- User on Host A wishes to sent a message to the user on Host B. The message is passed to TCP/IP and is intercepted by the IPSec driver on Host A.
- The IPSec driver on Host A checks its IP filter lists to determine whether the message should be secured.
- The IPSec driver notifies the IKE module to begin negotiations.
- The two computers use IKE to authenticate each other and determine the secret keying material, the type of protection for future IKE traffic, and the type of protection for the message that is being sent.
- The sets of parameters that determine the protection, known as Security Associations (SAs), are sent to the IPSec driver. The IPSec driver uses SA information to protect the message.
- The IPSec-protected message is forwarded to Host B.
- The IPSec-protected message is received by the IPSec driver on Host B.
- The IPSec driver on Host B validates authentication and integrity and, if required, decrypts the message.
- The IPSec driver passes the validated and decrypted message to TCP/IP, which passes it to the receiving application on Host B.

7.8 Securing a telemedical WLAN

By reading the previous subchapters, the following conclusions can be drawn:

- Using WEP to secure WLANs systems has been the recipient of a number of negative remarks.
- Not all of these remarks, on the possible attacks to the WEP protocol, are considered to pose a clear and realistic danger, as many of these attacks require specific prerequisites.
- There are simple ways to secure a network using WLANs
- There is an ongoing fear of the general population as to the possible attacks that were publicised recently. Furthermore, these concerns are also shared by the patients and the healthcare workers.

The trust between doctor and patient should remain on the highest level of priority, for any research project like MedLAN. This dictated that any fears and insecurities of both patients and doctors should be addressed before the successful deployment of a system like MedLAN.

As proved, IPSec offers a superb level of security; much higher than previously set by WEP. By using (encapsulating) WLAN data into IPSec frames (with or without WEP security), the WLAN level of security is increased and the confidence to the overall MedLAN system is retained. Below, the methodology and results of this experiment will be explained.

7.8.1 Methodology

A number of different topologies, both wired and wireless, were secured using IPSec protocol in tunnel mode, with a primary intention of investigating the possible overhead that such a protocol would impose on a system. The interest, in particular, was focused on the possible effects that this kind of encapsulation would pose in a real time videoconferencing system; specifically one destined for telemedical use.

As the overhead added by the IPSec protocol increases, the bandwidth available for the videoconferencing application decreases (the overall speed remains the same). This means that (as the available bandwidth that the video compression algorithm can use decreases) the compression must increase and the quality eventually is degraded.

The theoretical overhead of IPSec is about 15-20% of the data packets (at any given speed). Practical experiments reveal the actual overhead.

For these experiments, three different scenarios were chosen for a node-to-node communication: wired, wireless without AP (ad-hoc mode) and wireless with AP (infrastructure mode). For each of those, variable-sized files were used (small and large) in order to define the effect that IPSec would have. 100% was defined as the time that a wired network (using a cross-wired cable to avoid any delays introduced by the HUBs and switches or by packet collisions) takes to transfer a large file from one computer to another, using the same speed as the WLANs (the maximum IEEE 802.11b speed of 11Mbps). The file simulates the constant videoconferencing data stream introduced while videoconferencing.

The testbed included two computers (a laptop and a desktop) that run Windows XP Professional and supported internally the use of the IPSec protocol. The MMC command was used to add the IPSec protocol and configure the security policies [Fig. 7.9] [Dix03]

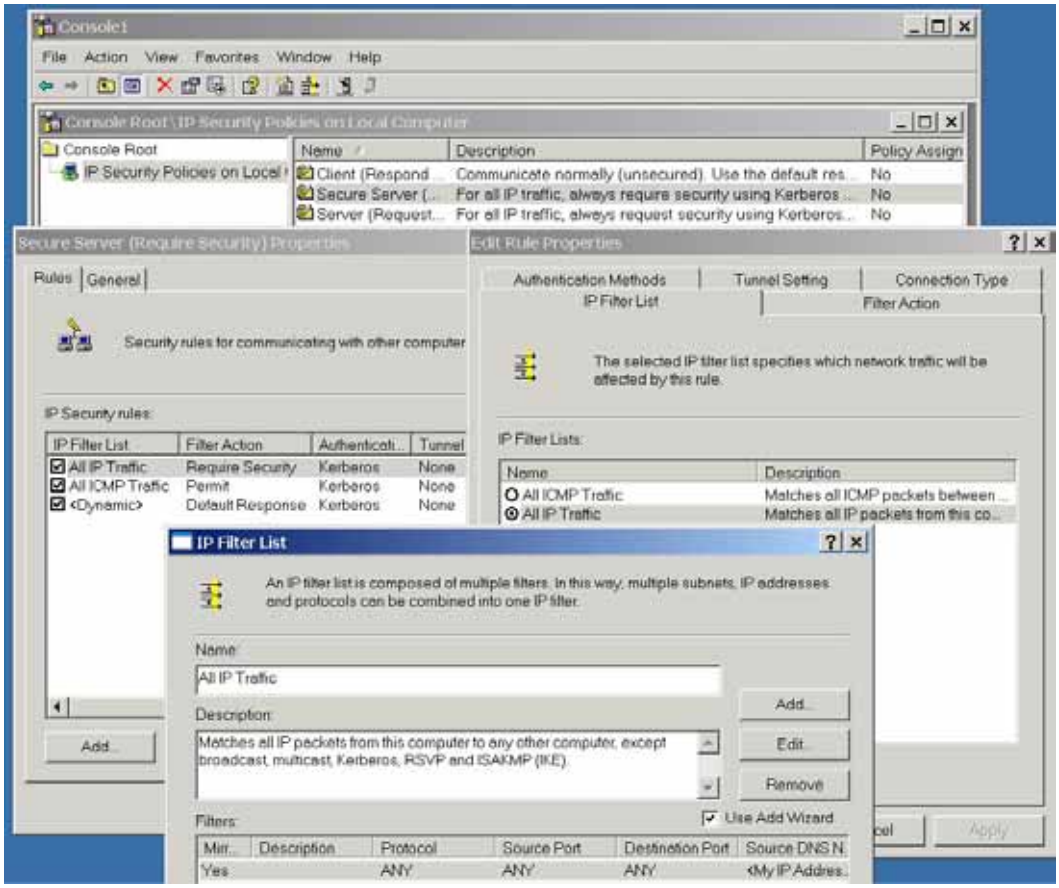


Fig. 7.9 running the MMC program permits the user to select the kind of security and the settings (rules) to which it applies.

Several scenarios were tested, having different security properties. For the most common scenario, both clients were running under IPSec, the negotiation has already taken place and normal communication between them has been established. The overall procedure was transparent to the users. (there is a great level of detail involved in establishing and configuring IPSec, but for reasons of simplicity, only the most common procedures are mentioned).
The following table indicates the IPSec overhead:

File size (in MB)	83.70	73.00	47.20
FTP time	276 sec	232 sec	152 sec
FTP time with WEP	296 sec	268 sec	160 sec
FTP time with IPSec	292 sec	254 sec	205 sec
FTP time with WEP and IPSec	303 sec	348 sec	214 sec
Overheads for WEP	117.20%	115.51%	110.5%
Overheads for WEP and IPSec	110.9%	115%	114%

Table 7.2 Overheads introduced while transferring various size files by using WEP, IPSec or a combination of both.

7.8.2 Discussion

By taking into account the experiment results, the following remarks can be made:

- Both the overhead of WEP and IPSec remain in a relatively low level. This means that for an average WLAN traffic, both solutions do not impose a considerable burden into the data stream. Consequently, either method can be used without any major problems.
- Despite the fact that the speed of the WLAN is 11Mbps, the actual speed left to be used is about 2.5-3Mbps. Of this, only about half is being occupied by the videoconferencing application of MedLAN. As the overhead of the above security solutions is about 12%, that means that no visible degradation of the videostream will take place. This notion has been verified through practical experimentation.
- There was no measurable delay introduced to the system while using WEP, IPSec or both. The reason for that was that WEP additional calculations are handled by the WLAN hardware. IPSec, on the other hand, is handled by the computer CPU, which seemed able to perform this task in real-time without any additional delay.

- Initially it seems that encapsulating IPSec over WEP is an unnecessary task, as IPSec offers a greater level of security and is considered superior to the WEP service. However, in contrast with IPSec, which requires a rather expert installation and configuration, WEP can be enabled or disabled easily by the user of the WLAN system. Furthermore, it is more common for WLAN hardware to be WEP-enabled, than to be configured to run under IPSec as sometimes this service may not be available.
- Finally, as the overhead introduced was not big enough to cause any significant delays or overloads to the WLAN traffic, the integrity of the MedLAN system operation was preserved, while the security level was increased.

7.9 Conclusions

During this chapter, we have presented a brief overview of the existing security techniques, embedded in the IEEE 802.11 WLANs. Apart from SSID and MAC filtering, further attention was given to the WEP security protocol and the way it is implemented and configured.

We also discussed the possible vulnerabilities that the WEP implementation has (using the RC4 algorithm), as they were presented recently to the press. That led to an increased concern about the security of WLANs. It is the author's opinion that this concern is exaggerated and overestimated. There are poor implementations of several details of the WEP protocol. However, a list of simple rules to be followed has also been included in this chapter; rules that render wireless security equal to wired security.

Nevertheless, as non-expert users tend to jump to conclusions regarding the security of the WLANs, a complete and integrated security solution was added to this chapter, to ease these concerns (especially these of the patients, that seem to worry the most). This solution proposes the encapsulation of WEP inside the IPSec security architecture; something that has been proven reliable over the years and has been exploited within VPNs. The encapsulation of WEP over IPSec is not a unique concept, however by the methods described in this thesis, it contributes to an

increase of security in a wireless telemedical system by means of a carefully balanced integration.

The experiments carried out in the hospital, illustrated that this solution is not only feasible and relatively easy to implement, but also adds no significant overhead to the wireless datastream, used by the MedLAN system to carry video and data.

Another important point to mention is that apart from the data security due to the advantages or disadvantages of the algorithm, there are also managerial issues that can pose bigger challenges than technical issues. These should be anticipated, decided, documented and delegated, before the start of the operation of any telemedical system.

In conclusion, like most advances, WLANs pose both opportunities and risks [Sym02]. This technology can represent a powerful complement to a healthcare-sector networking capabilities enabling fast and effective delivery of care when it is needed, while reducing cost. To minimise the risks, network administrators can implement a range of measures and practices, while being confident that this expanding technology is as safe as possible.

8. Conclusions

8.1 Summary and conclusions

MedLAN is a system dedicated for use in the hospital accidents and emergency wards. It has been developed to serve the need for mobile videoconferencing and wireless network access of healthcare personnel.

A number of reasons contributed to the need of such a system, with the main ones being: the need for mobility inside the A&E rooms to increase the healthcare quality and the productivity, the need for consulting an expert that can reside inside or outside the hospital, the inefficiency (or even potential danger) of moving the patient to a room dedicated for videoconferencing, and finally the high cost and reduced flexibility of the existing ISDN videoconferencing systems.

Within this thesis, the overall concept of such a wireless medical system was presented, along with its advantages and its potential limitations. As this thesis presented a two-fold application (Telemedical and communicational), it attempted to keep a balance between those two.

In summary, we started by introducing some basic concepts of Telemedicine and Telecare along with a list of properties that a telemedical system should possess. We continued by introducing the reader to basic WLAN principles before moving on to the actual operation and properties of the MedLAN system. Next, we presented an alternative method of transferring images over a wireless channel; something that was proven essential for the operation of a wireless system such as the MedLAN. On the communicational side, we also presented a modulation alternative to that of the IEEE 802.11b, which was proven to cope better within a multipath environment often caused by thick hospital walls. Finally, we have presented some potential security problems that the 802.11 system suffers from and proposed not only a simple list of countermeasures that can be adopted, but also an integrated security solution that guarantees the confidentiality and integrity, when using a telemedical system such as MedLAN.

Chapters three to eight include one or more contributions to knowledge, as defined in the beginning of this thesis. Below is a summary of the conclusions that can be drawn from the entire thesis:

- The MedLAN system was developed to fill in the space of some very specific needs, as set by the doctors. However, its specifications and its range of applications were extended far beyond those initially set by doctors. The resulting prototype is capable of handling live videostream, high quality still images, sound, patient data, and allows the operator to be wirelessly connected to the hospital's network while roaming around the A&E room. Further development showed that the system could also exist in handheld versions, to allow complete autonomy of the healthcare personnel.

  The majority of the tests performed in the hospital proved that the system behaves very well, is easy to use, it costs less than the existing systems and, more importantly, can **effectively assist to save lives.** Furthermore, it poses no danger due to the use of radio waves, both to the people in close proximity, and to the existing medical instruments.
- As the most interesting feature of the MedLAN system is its ability to send still images and video, there was the problem of standardisation of its outputs. DICOM has proposed a detailed list of specifications for the DICOM-compliant hardware. These specifications, however, do not take into account the particularities of wireless systems and more specifically the low bandwidth available to wireless networks, compared to their wired equivalent.

  Within this thesis, an alternative set of specifications was suggested, that allowed for a small percentage of compression of medical images while saving a considerable percentage of storage space and transfer time. The images that were compressed using this technique were evaluated by several doctors that verified that their quality maintains its diagnostic abilities, despite their lossy nature.
- On the communication part of the thesis, there was an apparent dilemma regarding the physical layer of the wireless system. The choice was either to select a protocol that would cope better with multipath noise but have a limited range of operation (due to the frequency band used), or to have a

wide radius of coverage but allow for signal degradation due to reflecting surfaces, often found in hospitals.

What was proposed is to take the best of the two worlds: increased range and better immunity to multipath noise. OFDM modulation was applied to the existing IEEE 802.11b protocol in order to prove the above suggestion. The whole notion was supported by means of simulation using various simulation packages. The result was a system that is tolerable to multipath noise and maintains its increased range of coverage, while operating in the 2.4GHz spectrum.

This alternative suggestion is highly effective for use in Telemedical systems such as MedLAN, where the available bandwidth also defines the level of compression of the video and images sent, and thus the overall quality. Under the above scheme, a clear 2dB noise reduction was experienced; something that translated to a throughput increase in the order of 1Mbps.

- Finally, as the data handled by the MedLAN system is of a very delicate nature, it had to be proven that the system could maintain a high level of security and confidentiality, which is the cornerstone of any patient - doctor relationship. The fact that the MedLAN system uses the IEEE 802.11b protocol gave rise to a number of concerns regarding the effectiveness of its encryption algorithm; WEP. Based on recent publications, WEP has been found to suffer from a number of vulnerabilities that an attacker can take advantage of, to extract information out of the wireless data stream. Despite the fact that to perform such actions very specific prerequisites had to exist, there was an increased concern from both patients and healthcare personnel. To address this issue, an alternative to WEP security was suggested: encapsulating IPSec over WEP. This is not a novel approach, but is uniquely applied in a wireless telemedical system.

  The experiments carried out in the hospital showed that this operation offers the highest level of security for a telemedical system like MedLAN. Furthermore, the overhead introduced by both WEP and IPSec remains in such low levels, that it does not interrupt the normal operation of MedLAN: an average of 12% reduction of the available wireless bandwidth had no effect on the videoconferencing system that only used 50% of the wireless link.

8.2 Future directions

As expected with this kind of research projects, the more the research was progressing, the more opportunities arise for expanding its capabilities to meet additional telemedical needs. This was made apparent at the early stages of development and consequently many more functions were added to MedLAN than those originally planned.

This kind of application opened many new opportunities for both doctors on the move and patients in need of care; many more than those described in this thesis. A short list of additional paths that can be followed to complement or expand MedLAN's capabilities is given below:

- **Expand the WLAN coverage to include the entire hospital**: Although this kind of application has been applied some years ago in the Johns Hopkins Hospital, it was limited into just supporting the transmission of data at low speeds to accommodate for patient record update. The MedLAN system dealt with only covering a limited part of the hospital, mainly the A&E ward and the areas surrounding it, along with the A&E offices. For that reason it used a limited number of APs. The majority of the hospital area, however, remained uncovered. By performing a careful network planning (regardless of the WLAN technology that will be used) and by placing a large number of APs to cover the entire hospital area, new applications can emerge:
    - Videoconferencing between healthcare personnel, while being on the move inside the hospital.
    - Voice over IP conversations.
    - Freedom of movement of any computer or network equipment (modern ECG, etc) within the vicinity of the hospital.
    - Access / update of patient records from anywhere inside the hospital.
    - Easy network expansion while avoiding needless infrastructure (lengthy cables, holes in the hospital walls, etc).
    - Increased network capacity while avoiding bottlenecks in crowded areas.

- **Use PDAs for an all-wireless hospital**: a number of benefits exist of using PDAs, as demonstrated in the MedLAN example. Alternatively, the entire

hospital staff can be equipped with small and light PDAs that can internally support WLAN connection. Assuming that the hospital would already be covered with APs, this project will revolutionalise the order of operations in the entire hospital. Some of the benefits include:

- Healthcare personnel will be in constant contact with each other while only carrying a device weighing less than 200g.
- Health care delivery will be faster and more efficient.
- PDAs can have access to any kind of data or software that a desktop computer can.
- Video and audio conversation can take place between two or more participants.
- Intranet and Internet access will be even easier.
- An adequate level of confidentiality and security.
- The running cost of such an operation is minimal.

- **Take advantage of the growing WLAN infrastructure**: Many telecommunication companies around the world have announced the deployment of WLAN infrastructures to cover a range of areas, from hotspots, to entire cities. As the future of communications is undoubtedly wireless, it is more than certain that this project will one day cover a vast area of a country, much like GSM evolved.

  By taking advantage of such infrastructures, the operation of MedLAN, and every other wireless system, can be extended outside the hospital. This way, the consultant (or even the patient) can be reached at any location covered by WLAN access. This kind of innovation will radically change the view of health care delivery as we understand it today.

  Nevertheless, there are fundamental problems to be resolved before this notion can take off. Some of these include:

  - Security of the system, as the link will be handled by an “outside” provider. Some kind of encapsulation (possibly IPSec) should take place to ensure confidentiality of patient data.
  - Link quality: As many other users will share the same link, the bandwidth available for telemedical purposes will fluctuate heavily. There needs to be a method of ensuring constant bandwidth.

- The running cost of the system would be relatively high, as large amounts of data have to be transferred for a successful videoconferencing session.

- **Use of 3G mobile devices to perform teleconsultation**: As the deployment of WLAN as MANs is still under development, the intermediate solution for mobile videoconferencing is the use of the growing 3G infrastructures.
  3G cells offer a high speed connection to MTs that can extend up to 2Mbps, when in a stable position. The actual speed falls to about 64-128 Kbps for normal use in order to maintain the financial feasibility of the system. Even at those speeds, however, the healthcare staff can still initiate a proper teleconference session. Furthermore, and as the system supports IP packet transmission, a consultant can be connected to the MedLAN system (operating inside the A&E) and perform an all-mobile teleconsultation. A mobile computer, PDA or even a 3G mobile telephone at the consultant's end can perform this function adequately.
  Similar problems with the use of WLAN MANs (described above) regarding the security and bandwidth of the system exist in this notion and have to be researched before successful operation.

- **Use of newer and faster protocols**: While writing this thesis, an improvement to the existing IEEE 802.11a and b was added to the WLAN family; IEEE 802.11g. "g" promises speeds up to 54 Mbps at an operating frequency of 2.4GHz, while employing advanced modulation techniques.
  By having almost four times as much bandwidth as the 802.11b available, several applications can be improved or emerged altogether (especially in relation to the deployment of APs around the entire hospital space):
  - Telemedical videoconferencing can enjoy increased bandwidth. This translates to lower video compression and thus higher video and image quality.
  - Network administrators can look favourably to complement / replace the existing wired LANs with wireless ones, as the speed of the 802.11g is more than half of the standard 100Mbps Ethernet.

- Wireless bridges supporting IEEE 802.11g can be deployed between hospital campuses, to link hospitals together and cut the cost of leased lines.

Overall, by using open-ended architectures, the MedLAN system has not only proven that it can effectively assist the healthcare personnel to perform a range of duties better, faster and safer, but it also has limitless possibilities for future expansions.

Appendices

A. IEEE 802.11 modulation

(a) Direct sequence spread spectrum

Data rate	Chipping code length	Modulation	Symbol rate	Bits/symbol
1 Mbps	11 (Barker sequence)	DBPSK	1 Msps	1
2 Mbps	11 (Barker sequence)	DQPSK	1 Msps	2
5.5 Mbps	8 (CCK)	DBPSK	1.375 Msps	4
11 Mbps	8 (CCK)	DQPSK	1.375 Msps	8

(b) Frequency-hopping spread spectrum

Data rate	Modulation	Symbol rate	Bits/symbol
1 Mbps	Two-level GFSK	1 Msps	1
2 Mbps	Four-level GFSK	1 Msps	2

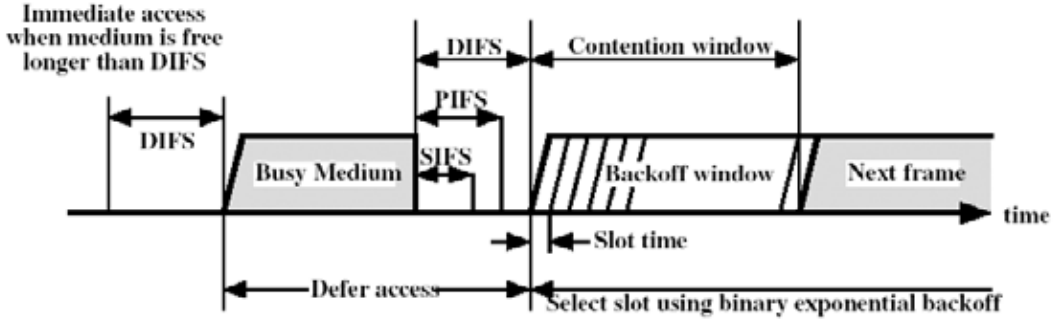
(c) Infrared

Data rate	Modulation	Symbol rate	Bits/symbol
1 Mbps	16-PPM	4 Msps	0.25
2 Mbps	4-PPM	4 Msps	0.5

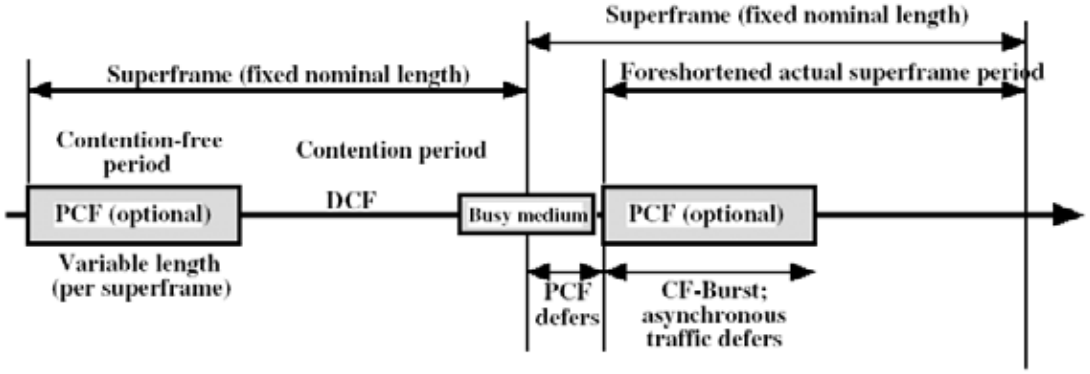
(d) Orthogonal FDM

Data rate	Modulation	Coding rate	Coded bits per subcarrier	Code bits per OFDM symbol	Data bits per OFDM symbol
6 Mbps	BPSK	1/2	1	48	24
9 Mbps	BPSK	3/4	1	48	36
12 Mbps	QPSK	1/2	2	6	48
18 Mbps	QPSK	3/4	2	96	72
24 Mbps	16-QAM	1/2	4	192	96
36 Mbps	16-QAM	3/4	4	192	144
49 Mbps	64-QAM	2/3	6	288	192
54 Mbps	16-QAM	3/4	6	288	216

B. Timing of IEEE 802.11 frames



(a) Basic Access Method



(b) PCF Superframe Construction

C. Specifications of the MedLAN system[1]

	Mobile computer	Video camera	WLAN
Type	Sony VAIO PCG SRX 51	Sony DCR-PC110E	Cisco 350 series
CPU	P-III / 800MHz		
RAM	256MB		2MB EEPROM
Additional functions	DVD, IEEE 1394, LAN, modem, Internal IEEE 802.11b	DV in/out, memory stick, IEEE 1394, video in/out	Line-in power, DHCP, 128 bit WAP, remote configure
Storage	30GB HD	64MB memory stick	
O.S.	Windows XP Pro		
Video	Inter 815	PAL colour CCIR standards	
Audio	Yamaha sound Max	PCM quantisation 12, 16 bits	
Resolution	1024 x 768, 10.4" TFT	1.070.000 active pixels	
Lens		Carl-Zeiss Vario sonar	
Zoom		10x optical, 40x digital	
Focal lengths		40-480mm	
Focus		0-infinity	
Illumination		7 lux minimum, 0 lux in night shot	
WLAN speeds			1,2,5.5, 11 Mbps
Typical range			400m@1Mbps 90m@11Mbps
Operating temperature	0-40 C	0-40 C	0-55 C
Power consumption	10W (LCD half on)	4.1W (LCD screen) 3.5W (viewfinder)	5V, 800mA Max power output: 50mW
Weight	1200g (including battery)	690g (including battery)	350g
Autonomy (on battery)	180-240 min while videoconferencing	160 min	

[1] There exist a number of combinations between mobile computer, video camera, WLAN, etc, to fit various needs and budgets. A number of specifications depend on the combination selected.

D. Range of the MedLAN system in CMH A&E

Coverage of a single AP (at 1Mbps) placed in the A&E majors room (marked white)

Coverage of a single AP (at 1Mbps) placed in the A&E minors room (marked white)

E. Patient acceptance form

North West London Hospitals are devoted to constantly improve the quality of services offered to patients. For that reason, NWLH has funded a project called MedLAN. It is a telemedical system that will allow easy teleconsultations between the hospital that you are in now, and a consultant in a different hospital (mostly within NWLH). The purpose of the system is to provide a second opinion from an experienced doctor, without having to move you to another part of the hospital or use any big and heavy teleconference equipment inside the Accidents and Emergency department. The MedLAN system is a very light and convenient system and most of all it is wireless so it can freely roam around the department.
The system is in its second year of development and as the prototype is already built and tested, there is the obvious need to test it in real life situations. In that sense, by allowing the hospital staff to use this system in your case not only you would be contributing towards research but you would gain by being examined twice: once by the doctor next to you and another by a consultant in another hospital.
Here are some points to ease your mind:

- It is only a video-conferencing system
- There will be no physical contact between you and the system
- You would feel absolutely nothing
- It uses radio frequencies of very low power to transmit the signal. These have been tested extensively and do not interfere with any of the hospital equipment (unlike mobile phones do)
- The system uses a highly sophisticated encryption algorithm that makes sure that the videoconference is limited only between you and the remote doctor.
- No recording is made of the consultation.

Your help will be much appreciated

I authorize the use of the Telemedical equipment to allow for the Teleconsultation between the hospital that I am in and a remote hospital. All my personal data will be jealously protected and I expect the minimum inconvenience.

Patient name:_____ Patient signature:_____

Date: _____

F. Structure of DICOM standards

The DICOM standard is composed of 13 parts:

PART 1: Introduction and Overview
Describes the overall structure of the Standard
PART 2: Conformance
Specifies the general requirements which must be met by implementations claiming conformance and defines contents of a Conformance Statement
PART 3: Information Object Definitions
Specifies the structure and attributes of objects, which are operated upon by Service Classes (Part 4).
These objects include images, studies, and patients
PART 4: Service Class Specifications
Defines the operations that can be performed on instances of Information Objects (Part 3) to provide a specific service. These services include image storage, retrieval and printing.
PART 5: Data Structure and Semantics
Specifies the encoding of the data content of messages, which are exchanged to accomplish the operation used by the Service Classes (Part 4).
PART 6: Data Dictionary
Defines the individual information attributes that represent the data content (Part 3) of instances of Information Objects.
PART 7: Message Exchange
Specifies the operations and protocol used to exchange messages. These operations are used to accomplish the services defined by the Service Classes (Part 4).
PART 8: Network Communication Support for Message Exchange
Defines the services and protocols used to exchange messages (Part 7) directly on OSI and TCP/IP networks.
PART 9: Point-to-Point Communication Support for Message Exchange
Defines the services and protocols used to exchange messages (Part 7) directly on the DICOM 50-pin interface (obsolete).
PART 10: Media Storage and File Format (Supplement 1)
Defines the logical formats for storing DICOM information on various media.
PART 11: Application Profiles (Supplement 2)
Defines a means for users and vendors to specify a selection of Media among those in Part 12 and of Information Objects among those defined by DICOM Part 3.
PART 12: Media Formats and Physical Media for Data Interchange (Supplement 3)
References industry specifications for the Physical Media and Media formatting file systems. It includes 5 types of Media: CD-R 650 Mbyte, 5.25" MOD 650 Mbytes, 5.25" MOD 1.3 Gbyte, 3.25" MOD 128 Mbyte, and the 3.5" Floppy Disk.
PART 13: Print Management Point-to-point Communication Support (Supp 4)
PART 14: Grayscale Standard Display Function
PART 15: Security Profiles illustrating possible security scenarios to ensure privacy
PART 16: Content Mapping Resource

G. Modalities supported by DICOM

Computed Radiography (CR)
Multiframe, etc.: No
Bits Allocated: Unrestricted
Bits Stored: Unrestricted
High Bit: Unrestricted
Pixel Representation: Any
Samples per Pixel: Any (1,3,4 defined)
Planar Configuration: Any
Coordinate System: Unspecified

Computed Tomography (CT)
Multiframe, etc.: No
Bits Allocated: 16
Bits Stored:12 to 16
High Bit: Bits Stored - 1
Pixel Representation: Any
Samples per Pixel: 1
Coordinate System: Frame of reference, Image Plane

Magnetic Resonance (MR)
Multiframe, etc.: No
Bits Allocated: 16
Bits Stored: Anything up to 16
High Bit: Anything that fits Bits Stored within the 16 bits allocated
Pixel Representation: Any
Samples per Pixel: 1
Coordinate System: Frame of reference, Image Plane

Nuclear Medicine (NM)
Multiframe, etc.: Yes
Bits Allocated: 8 or 16
Bits Stored: Bits Allocated
High Bit: Bits Stored - 1
Pixel Representation: Any
Samples per Pixel: 1
Coordinate System: Frame of Reference with Projection angles, patient or table based

Secondary Capture (SC)
Multiframe, etc.: No
Bits Allocated: Unrestricted
Bits Stored: Unrestricted
High Bit: Unrestricted
Pixel Representation: Any
Samples per Pixel: Any (1,3,4 defined)
Coordinate System: Unspecified

Ultrasound (US)
Multiframe, etc.: Yes
Bits Allocated: 8 or 16
Bits Stored: Bits Allocated
High Bit: Bits Stored - 1
Pixel Representation: Any
Samples per Pixel: 1,3
Coordinate System: Unspecified

H. ACR/NEMA Equipment Specification

Specifications for equipment utilised in teleradiology will vary depending on the individual facility's needs but, in all cases, should provide image quality and availability appropriate to the clinical need.
Compliance with the ACR/NEMA (National Electrical Manufacturers Association) Digital Imaging and Communication in Medicine Standard (DICOM) is strongly recommended for all new equipment acquisitions and consideration of periodic upgrades incorporating the
expanding features of that standard should be part of the ongoing quality-control program.
Equipment guidelines cover two basic categories of teleradiology when used for rendering the official interpretation: small matrix size (e.g., computed tomography (CT), magnetic resonance imaging (MR), ultrasound, nuclear medicine, digital fluorography, and digital
angiography) and large matrix size (e.g., computed radiography and digitised radiographic films).
Small matrix: A data set should provide full-resolution data (typically 512 x 512 resolution at minimum 8-bit depth) for processing, manipulation, and subsequent display.
Large matrix: A data set allowing a minimum of 2.5 lp/mm spatial resolution at minimum 10-bit depth should be acquired.

A. Acquisition or Digitisation Initial image acquisition should be performed in accordance with the appropriate ACR modality or examination standard.
1. Direct image capture
The image data set produced by the digital modality both in terms of image matrix size and pixel bit depth should be transferred to the teleradiology system. It is recommended that the DICOM standard be used. This is the most desirable mode of digital image acquisition for primary diagnosis.
2. Secondary image capture
a. Small matrix images. Each individual image should be digitised to a matrix size as large or
larger than that of the original image by the imaging modality. The images should be digitised to a bit depth of 8 bits per pixel or greater. Film digitisation or video frame grab
systems conforming to the above specifications are acceptable.
b. Large matrix images. These images should be digitised to a matrix size corresponding to 2.5 lp/mm or greater, measured in the original detector plane. These images should be digitised to a bit depth of 10 bits per pixel or greater. Film digitizers will generally be
required to produce these digital images.
3. General requirements
At the time of acquisition (small or large matrix), the system must include:
Annotation capabilities including patient name, identification number, date and time of examination, name of facility or institution of acquisition, type of examination, patient or anatomic part orientation (e.g., right, left, superior, inferior, etc.), amount and method of data compression. The capability to record a brief patient history is desirable.

B. Compression
Data compression may be performed to facilitate transmission and storage. Several methods, including both reversible and irreversible techniques, may be used, under the direction of a qualified physician, with no reduction in clinically diagnostic image

quality. The types and ratios of compression used for different imaging studies transmitted and stored by the system should be selected and periodically reviewed by the responsible physician to ensure appropriate clinical image quality.

C. Transmission

The type and specifications of the transmission devices used will be dictated by the environment of the studies to be transmitted. In all cases, for official interpretation, the digital data received at the receiving end of any transmission must have no loss of clinically significant information. The transmission system shall have adequate error-checking capability.

D. Display Capabilities

General: Display workstations used for official interpretation and employed for small matrix and large matrix systems should provide the following characteristics:

1. Luminance of the gray-scale monitors should be at least 50 foot-lamberts.
2. Care should be taken to control the lighting in the reading room to eliminate reflections in the monitor and to lower the ambient lighting level as much as is feasible.
3. Provide capability for selection of image sequence.
4. Capable of accurately associating the patient and study demographic characterisations with the study images.
5. Capable of window and level adjustment, if those data are available.
6. Capable of pan functions and zoom (magnification) function.
7. Capable of meeting guidelines for display of all acquired data.
8. Capable of rotating or flipping the images, provided correct labelling of patient orientation is preserved.
9. Capable of calculating and displaying accurate linear measurements and pixel value determinations in appropriate values for the modality (e.g., Hounsfield units for CT images), if those data are available.
10. Capable of displaying prior image compression ratio, processing, or cropping.
11. Elements of display that should be available include: a. Matrix size. b. Bit depth. c. Total number of images acquired in the study.

There may be less stringent guidelines for display systems when these display systems are not used for the official interpretation.

E. Archiving and Retrieval

If electronic archiving is to be employed, the guidelines listed below should be followed:

1. Teleradiology systems should provide storage capacity capable of complying with all facility, state, and federal regulations regarding medical record retention. Images stored at either site should meet the jurisdictional requirements of the transmitting site. Images interpreted off-site need not be stored at the receiving facility, provided they are stored at

the transmitting site. However, if the images are retained at the receiving site, the retention period of that jurisdiction must be met as well. The policy on record retention should be in writing.

2. Each exam data file must have an accurate corresponding patient and examination database

record, which includes patient name, identification number, exam date, type of examination, facility at which examination was performed. It is desirable that space be available for a brief clinical history.

3. Prior examinations should be retrievable from archives in a time frame appropriate to the clinical needs of the facility and medical staff.

4. Each facility should have policies and procedures for archiving and storage of digital image data equivalent to the policies that currently exist for the protection of hard-copy storage media to preserve imaging records.

F. Security

Teleradiology systems should provide network and software security protocols to protect the confidentiality of patients' identification and imaging data. There should be measures to safeguard the data and to ensure data integrity against intentional or unintentional corruption of the data.

G. Reliability and Redundancy

Quality patient care depends on availability of the teleradiology system. Written policies and procedures should be in place to ensure continuity of care at a level consistent with those for hard-copy imaging studies and medical records within a facility or institution. This should include internal redundancy systems, backup tele-communication links, and a disaster plan.

I. Modalities used

- **Images, sounds and video for MEDLAN**
  Radiology Images (JPEG, forced DICOM, originals)
  1 CT scan of knee consisting of 1 image
  1 CT of elbow consisting of 4 images
  1 CT of elbow consisting of 6 images
  1 MRI transverse cut of abdomen with Gastrographin) 1 image
  1 MRI transverse cut of abdomen with Gastrographin) 12 images
  1 MRI transverse cut of abdomen with Gastrographin) 4 images
  1 ultrasound abdomen consisting of 1 image
  1 ultrasound of abdomen consisting of 4 images
  I ultrasound of limb consisting of 1 image
  Ultrasound of limb consisting of 1 image
  Ultrasound of limb consisting of 1 image

- **Plain X-rays (B&W, colour, forced DICOM)**
  Cervical and thoracic spine consisting of 1 image
  Mammogram consisting of 1 image
  Lateral view of chest consisting of 1 image
  PA view of chest consisting of 1 image
  AP view of chest consisting of 1 image
  Gastrographin study of stomach consisting of 1 image
  Gastrographin view of duodenum consisting of 1 image
  Gastrographin study of jejunum consisting of 1 image
  Gastrographin study of jejunum consisting of 1 image
  X-ray of both feet consisting of 1 image
  Subcutaneous emphysema chest PA chest consisting of 1 image
  Subcutaneous emphysema chest AP consisting of 1 image
  Nail plate of hip consisting of 1 image
  Nail plate of hip consisting of 1 image
  Nail plate of hip consisting of 1 image
  Charnley hip replacement consisting of 1 image
  Elbow AP with healed fracture of midshaft of ulna consisting of 1 image
  Elbow lateral view of healed fracture of midshaft of ulna consisting of 1 image
  AP view of ankle consisting of 1 image
  Multiple myeloma of long bone consisting of 1 image
  Multiple myeloma of bone consisting of 1 image

Salter-Harris fracture lateral of wrist consisting of 1 image
Salter-Harris fracture lateral of wrist consisting of 1 image
Salter-Harris fracture of wrist with gross displacement consisting of 1 image
Salter-Harris fracture of wrist with displacement consisting of 1 image
Sacro-iliac joints on AP film
Supra-condylar fracture humerus oblique consisting of 1 image
Supracondylar fracture of humerus lateral view consisting of 1 image
Supra-condylar fracture of humerus AP view consisting of 1 image
Supra-condylar fracture of humerus AP view consisting of 1 image
Orthopantomogram consisting of 1 image
Orthopantomogram consisting of 1 image
Pelvis AP consisting of 1 image
Pelvis & hips consisting of 1 image

- **Pictorial images**
  Skin
  Eye
  Close-up of hair
  Fingernail

- **ECGs**
  Echocardiogram with 1 client
  Echocardiogram with 2 clients
  Echocardiogram with 3 clients

- **Videos**
  Videos of conversation with 1 client
  Videos of conversation with 2 clients
  Videos of conversation with 3 clients

- **Heart sounds [ADPCM (Adaptive Differential Pulse Code Modulation), CCITT's A-law, CCITT's Original]**
  Normal heart sounds
  Mid-systolic click
  Gallop rhythm
  Split first sound
  Split second sound
  Split first and second sounds

J. Doctor's Questionnaire

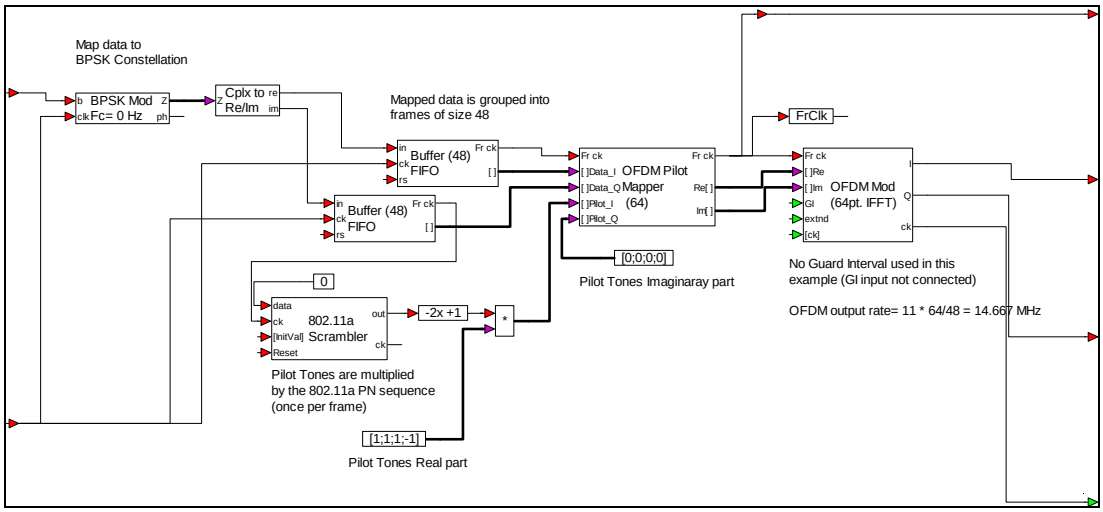
MedLAN
wireless videoconference system

Date	
Time	
MedLAN site	
Remote site	

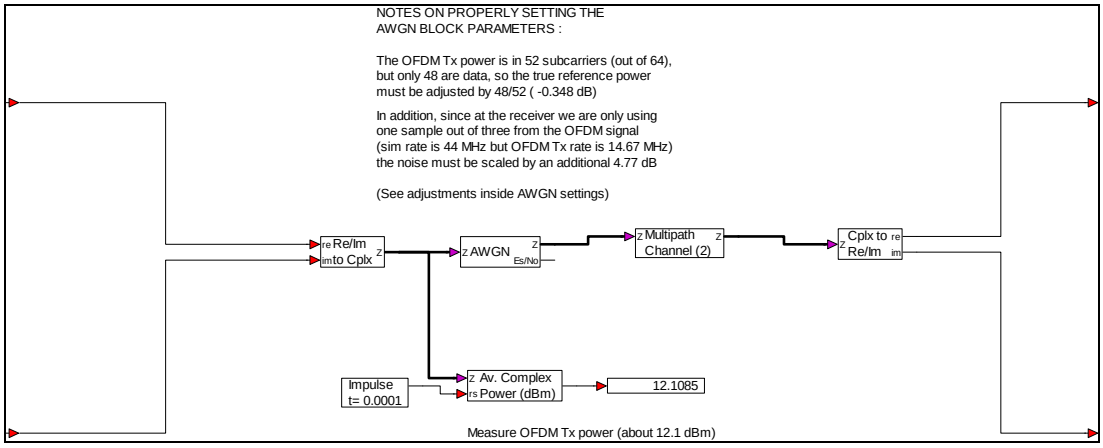
Name of Doctor in MedLAN site	
Name of Doctor in Remote site	

	Poor	**Acceptable**	**Good**	**N/A**	**Notes**
Image clarity					
Colour					
Depth versatility					
Sound					
Image / sound delay (lip synch)					
Total delay					
X-ray detail					

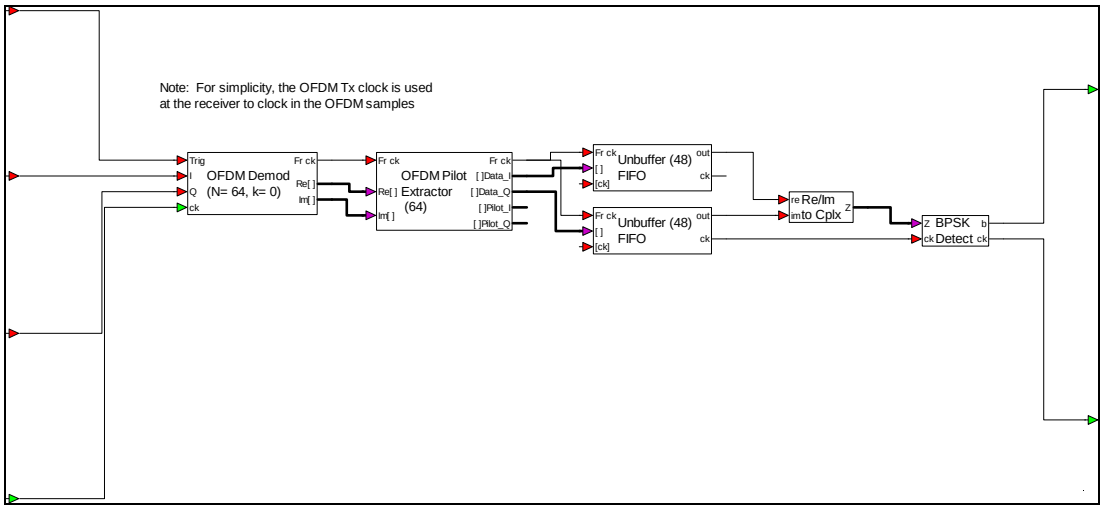
K. VisSim modules



OFDM modulator

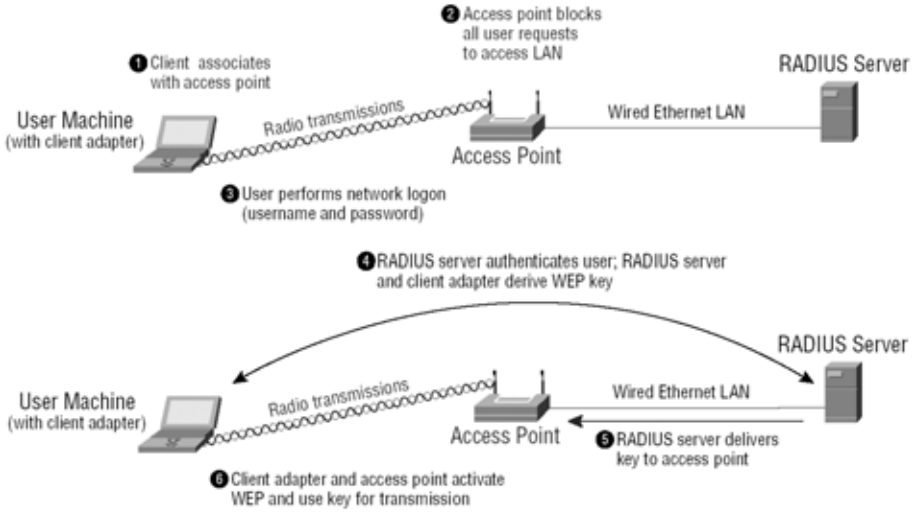


Channel noise



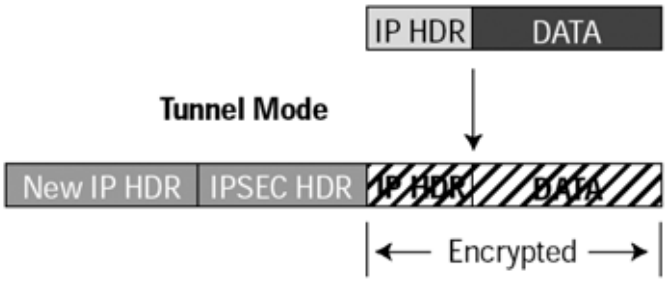
OFDM demodulator

L. Using a Radius server: sequence of events

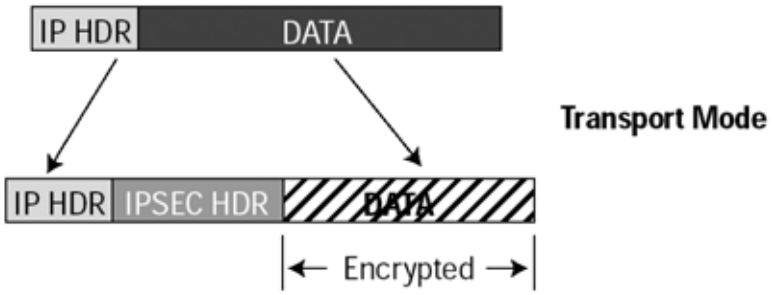


- Using open authentication, a wireless client associates with an access point.
- The access point blocks all attempts by the client to gain access to network resources until the client logs on to the network.
- The user on the client supplies a username and password in a network logon dialog box or its equivalent.
- Using 802.1x and EAP, the wireless client and a RADIUS server on the wired LAN perform a mutual authentication through the access point. As part of the authentication process, the client passes the username and a one-way hash of the password to the RADIUS server. The RADIUS server checks the username and one-way hash of the password against a database of valid usernames and passwords to determine if it should authenticate the client.
- When mutual authentication is successfully completed, the RADIUS server and the client determine a WEP key that is distinct to the client and provides the client with the appropriate level of network access, thereby approximating the level of security inherent in a wired switched segment to the individual desktop. The client loads this key and prepares to use it for the logon session.
- The RADIUS server sends the WEP key, called a session key, over the wired LAN to the access point.
- The access point encrypts its broadcast key with the session key and sends the encrypted key to the client, which uses the session key to decrypt it.
- The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session [Cis00]

M. IPSec modes



- Tunnel mode is used when one or both sides of the IPSec connection is a security gateway and the actual destination hosts do not support IPSec.
- In Tunnel mode, entire IP packets are encapsulated within AH or ESP, and then a new IP header is placed around it.
- Traffic analysis can only determine that encrypted data are traversing the network between two tunnel endpoints.



- Transport mode is for host-host communications.
- In transport mode, only the original packet's payload is sent. The AH or ESP is placed after the original IP header.
- Third party traffic analysis (eavesdropping) can determine IP protocol types and port numbers.

Glossary

Communication terms

3G	Third Generation
ACK	ACKnowledgment
ADPCM	Adaptive Differential Pulse Code Modulation
ADSL	Asymmetric Digital Subscriber Lines
AES	Advanced Encryption Standard
AH	Authentication Header
AMPS	Advance Mobile Phone System
ANSI	American National Standards Institute
AP	Access Point
ATM	Asynchronous Transfer Mode
AV	Audio Video
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPSK	Binary PSK
BR (ISDN)	Basic Rate
BS	Base Station
BSS	Basic Service Set
CA	Certificate Authority
CCD	Charge Coupled Device
CCI	Co-Channel Interference
CCITT	Comité Consultatif International Téléphonique et Télégraphique
CCK	Complementary Code Keying
CRC	Cyclic Redundancy Check
CRT	Cathode Ray Tube
CSMA/CD	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DCF	Distributed Coordination Function
DCT	Discrete Cosine Transfer
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIVX	DIgital Video eXpress
DMZ	De-Militarised Zone
DPCM	Discrete Pulse Code Modulation
Dpi	Dots per inch
DSP	Digital Signal Processing
DSSS	Direct Sequence Spread Spectrum
DSVD	Digital Simultaneous Voice and Data
DVD	Digital Versatile Disc or Digital Video Disc
E_b/N_o	Energy per bit to the spectral Noise density
EDGE	Enhanced Data for Global Evolution
EEPROM	Electrical Erasable / Programmable ROM
EMI	Electro-Magnetic Interference
ESP	Encapsulation Security Payload
ESS	Extended Service Set
ETSI	European Telecommunication Standards Industry
FCC	Federal Communications Commission
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access

FHSS	Frequency Hopping Spread Spectrum
Fps	Frames per second
GPRS	General Packet Radio Service
GSM	Global System Mobile
HIPERLAN	HIgh PERformance LAN
HMAC	Hash-Based Message Authentication Code
HSCSD	High Speed Circuit Switched Data
ICI	Inter-Channel Interference
IEE	Institute of Electrical Engineers
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IFFT	Inverse Fast Fourier Transform
IKE	Internet Key Exchange
IMTS	Improved Mobile Telephone System
IP	Internet Protocol
IPSec	IP Secure
IR	InfraRed
ISDN	Integrated Services Digital Network
ISI	Inter-Symbol Interference
ISM	Industry Science and Medicine
ISO	International Standards Organisation
ISP	Internet Service Providers
ITU	International Telecommunication Union
IV	Initialisation Vector
JPEG	Joint Pictures Expert Group
LCD	Liquid Crystal Display
LLC	Logical Link Control
LOS	Line Of Site
MAC	Medium Access Control
MD	Message Digest
MIB	Management Information Base
MMC	Microsoft Management Console
MNM	Microsoft NetMeeting
MPEG	Moving Pictures Expert Group
MSE	Mean Square Error
MT	Mobile Terminal
MTS	Mobile Telephone System
NEMA	National Electrical Manufacturers Association
NIC	Network Identification Card
OCR	Optical Character Recognition
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PACS	Picture Archiving and Communication Systems
PBCC	Packet Binary Convolution Code
PBX	Public Box eXchange
PC	Personal Computer
PCF	Point Coordination Function
PCM	Pulse Code Modulation
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Data Assistant
PDU	Protocol Data Unit
PHY	Physical layer
POTS	Plain Old Telephone System
PPM	Pulse Position Modulation
PR (ISDN)	Primary Rate

PRNG	Pseudo Random Number Generator
PSK	Phase Shift Keying
PSNR	Peak Signal to Noise Ratio
PSTN	Public Switch Telephone Network
QoS	Quality of Service
QPSK	Quadrature PSK
RFC	Request For Comments
RGB	Red Green Blue
ROM	Read Only Memory
RTS	Request To Send
SA	Security Associations
SMPTE	Society of Motion Picture and Television Engineers
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SOHO	Small Office / Home Office
SpO_2	Oxygen saturation
SSID	Service Station IDentifier
TACS	Total Access Communication System
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
UMTS	Universal Mobile Telecommunication Services
UNII	Universal Networking Information Infrastructure
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VCD	Video Compact Disc
VO	Video Object
VoD	Video on Demand
VPN	Virtual Private Networks
WCDMA	Wide Code Division Multiple Access
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Networks
WMP	Windows Media Player
WPA	Wi-Fi Protected Access

Medical terms

A&E	Accidents and Emergency
ACR	American College of Radiologists
BP	Blood Pressure
CMH	Central Middlesex Hospital
CT	Computed Tomography
DICOM	Digital Imaging and Communications in Medicine
ECG	ElectroCardioGram
EEG	ElectroEncephaloGram
ETM	EuroTransMed
FDA	Food and Drug Administration
GP	General Physician
HR	Heart Rate
MRI	Magnetic Resonance Imaging
NELH	National Electronic Library for Health
NHS	National Health Service
NWL	National Library of Medicine
NWLH	North West London Hospitals
NWPH	NorthWick Park Hospital
ROI	Region Of Interest
US	Ultra Sound

References

(web page access dates are shown in square brackets at end of reference)

[ACR99] American College of Radiology, *Standards for Teleradiology*, 1-1-1999, www.acr.org/departments/stand_accred/standards/pdf/teleradiology.pdf, [15-5-2004]

[Agn01] Agnew Richard: *Manchester launches first urban WLAN*, Netimperative news, 2001, www.netimperative.com/cmn/viewdoc.jsp?cat=news&docid=BEP1_News_0000057339, [15-5-2004]

[Ahr92] Ahring K, et al.: *Telephone modem access improves diabetes control in those with insulin-requiring diabetes*, Diabetes Care, 15, pp. 971-975, 1992

[AMA96] American Medical Association, CME Resource Guide: *The Promotion of Quality Telemedicine*, Chapter 7, Section 2, Part 11, 1996.

[Ani02] Anixter white paper: *Introduction to wireless local area networks*, Anixter 2001/2002, www.itpapers.com/abstract.aspx?kw=verizon+wi-fi&dtid=1&sortby=comp&docid=27241, [15-5-2004]

[Ara02] S. Laxminarayanan, D. Molta: *Perfect harmony*, Network computing magazine, pp. 58-69, June 2002

[Arb01] Arbaugh, William A., et al.: *Your 802.11 Wireless Network has No Clothes*, Wireless Communications, IEEE, Vol. 9 , Issue 6 , pp.44 – 51, Dec. 2002

[Arm02] J. Armstrong: *OFDM – Orthogonal Frequency Division Multiplexing*, La Trobe University, 2002, www.ieeevic.org/events/docs/72_armstrong_ofdm.pdf, [15-5-2004]

[ATA02] American Telemedicine Association: *E-xecutive Summary*, The Global Application of Video Conferencing in Health Care, www.atmeda.org/news/globalexe.html, [15-5-2004]

[Bal99] Baldwin G.: *Attention shoppers*, American Medical News, 19-4-1999, www.ama-assn.org/amednews/1999/net_99/tech0419.htm, [15-5-2004]

[Ban01b] Banitsas A. Konstantinos., et al.: *Modelling issues of Wireless LANs for Accident and Emergency Departments*, IEEE EMBC conference, Istanbul, vol. 4, pp. 3540-3543, Oct 2001

[Ban02a] Banitsas A. Konstantinos, Robert S. H. Istepanian, Sapal Tachakra: *Applications of Medical Wireless LAN Systems (MedLAN)*, Inter. Journal of Medical Marketing journal, Vol. 2, no. 2, pp.136-142, Sep 2000

[Ban02b] Banitsas A. Konstantinos, Sapal Tachakra, Robert S. H. Istepanian: *Operational Parameters of a Medical Wireless LAN: Security, Range and Interference issues*, Presented at IEEE EMBS conference, vol. 3, pp. 1889-1890, Oct 2002, Houston

[Ban03] Banitsas A. Konstantinos, Sapal Tachakra, Yong Hua Song, *Adjusting DICOM Specifications When Using Wireless LANs: The MedLAN example*, presented to IEEE EMBC conference, Cancun, Mexico, vol. 4, pp. 3661-3664, Sep 2003

[Ban04] Banitsas A. Konstantinos, Yong Hua Song, Thomas J Owens: *OFDM over IEEE 802.11b hardware for Telemedical applications*, International Journal of Mobile Communications, Vol.2, No. 3, 2004

[BMA93] British Medical Association, *Medical Ethics Today: Its Practice and Philosophy*, BMJ Publishing Group, London, 1993

[Boi97] Boivin, W.S., et al.: *Measurement of Electromagnetic Field Strengths in Urban and Suburban Hospital Operating Rooms*, IEEE 19th Annual International Conference on Engineering in Medicine and Biology, November 1997, vol.6, pp. 2539 -2542.

[Bor01] Nikita Borisov, Ian Goldberg, David Wagner: *Intercepting Mobile Communications: The Insecurity of 802.11*, Mobicom 2001 conference, pp. 180-189, July 2001

[Caf03] James McCaffrey: *Keep Your Data Secure with the New Advanced Encryption Standard*, MSDN Magazine, November 2003,msdn.microsoft.com/msdnmag/issues /03/11/aes, [15-5-2004]

[Che01] James C. Chen: *Measured Performance of 5-GHz 802.11a Wireless LAN Systems*, Atheros Communications, 2001, epsfiles.intermec.com/eps_files/eps_wp/Atheros RangeCapacityPaper.pdf, [15-5-2004]

[Che02] D. Cheung, C. Prettie: *A path loss comparison between the 5 GHz UNII band (802.11a) and the 2.4 GHz ISM band (802.11b)*, Intel labs, Jan 2002, impulse.usc.edu/resources/802_11a-vs-b_report.pdf, [15-5-204]

[Cis00] Cisco Systems white paper, *Wireless LAN security*, *Overview*, 2000, www.osws.com/pdf/CISCO_Aironet_Wireless_%20Security.pdf, [15-5-2004]

[Cis01] Cisco AP340/350, 340/350 wireless PCMCIA card *operating manual*, Cisco, 2001

[Cis02a] Cisco Bulletin: *Cisco Aironet Security* Solution Provides *Dynamic WEP* to Address *Researchers' Concerns*, Cisco, 2002, www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm, [15-5-2004]

[Cis02b] Cisco Bulletin No. 1327: *Cisco Comments on Recent WLAN Security Paper* from *University of Maryland*, Cisco, 2002, www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a008009246e.html, [15-5-2004]

[Clu99] David A. Clunie: *Lossless Compression of Grayscale Medical Images - Effectiveness of Traditional and State of the Art Approaches*, Quintiles Intelligent Imaging, SPIE 99 conference proceedings pp. 3662-10, Feb 1999

[Col96] Collins B and Sypher H.: *Developing better relationships in telemedicine practice: organizational and interpersonal factors*. Telemedicine Today, 4-2, pp. 27-42, 1996.

[Dae99] J. Daemen, V. Rijmen: *AES Proposal: Rijndael*, *The Rijndael block cipher*, 3-9-1999, csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael-ammended.pdf, [15-5-2004]

[Daw96] E. Dawson and L. Nielsen: *Automated cryptanalysis of XOR plaintext strings*. Cryptologia, (2), pp. 165–181, Apr. 1996.

[Del99] Della Mea V, Wootton R and Craig J.: *Pre-recorded telemedicine*. Introduction to Telemedicine, Royal Society of Medicine, London, 1999, Chapter 3

[DIC01] ACR-NEMA *DICOM specifications PS 3.1-2001* (Part 1 to Part 16), medical.nema.org, [19-5-2004]

[Dix03] Dixon W., Wong D., Scambray J: *Using Microsoft Windows IPSec to help secure an internal corporate network server*, Microsoft Press, 2003, www.foundstone.com/resources/whitepapers/Foundstone_IPSec_W2K_XP.pdf, [15-5-2004]

[Dou02] A. Doufexi, et al.: *A comparison of the Hiperlan/2 and IEEE 802.11a wireless LAN standards*, IEEE Communications magazine, pp. 172-179, May 2002

[Dub03] Vern A. Dubendorf: *Wireless Data Technologies*, John Wiley & Sons, Ltd, 2003

[Edf96] Ove Edfors, et al.: *An introduction to orthogonal frequency division Multiplexing*, Research Report TULEA 1996:16, Div. of Signal Processing, Luleå University of Technology, Luleå, Sept. 1996

[Elf97] Elford D R.: *Telemedicine in northern Norway*, Journal of Telemedicine and Telecare, 3, pp. 1-22, 1997

[EMC01] Regulatory Compliance Analysis EMC Standard, IEC *(EN)60601-1-2* (2001 Edition).

[Ent02] Enterasys white paper: *Health and Safety of RoamAbout 802.11*, Enetrasys networks 2002, www.enterasys.com/products/whitepapers/health-wpaper0499.html, [15-5-2004]

[ETSI00] Broadband Radio Access Networks (BRAN); *HIPERLAN Type 2; System Overview*, DTR/BRAN-00230002, ETSI, 2000

[Fal99] Falconer J, Wootton R and Craig J.: *Telemedicine systems and telecommunications*, Introduction to Telemedicine, Royal Society of Medicine, London, 1999, Chapter 2

[Fli03] R. Flickenger: *Performance test 802.11b*, 2003, www.oreillynet.com/lpt/a/713, [15-5-2004]

[Flu01] Scott Fluhrer, Itsik Mantin, and Adi Shamir: *Weaknesses in the Key Scheduling Algorithm of RC4*, 8th Annual International Workshop on Selected Areas in Cryptography, pp. 1-24, Springer-Verlag, London, 2001

[Fri96] Friedman R H, et al.: *A telecommunications system for monitoring and counseling patients with hypertension*, American Journal of Hypertension, 9, pp. 285-292, 1996

[Gar00] Leon- Garcia & Widjaja, *Communication Networks*, McGraw Hill, 2000

[Got95] M. Gott: *Telematics for health: the role of telemedicine in homes an communities*, Oxford: Radcliffe Medical Press, 1995

[Goy95] G. Coyle, L. Boydell, and L. Brown: *Home telecare for the elderly*, J. Telemedicine and Telecare, vol. 1, pp. 183-185, 1995.

[Has97] Hasman A and Albert A.: *Education and training in health informatics: guidelines for European curricula*, International Journal of Medical Informatics, 45 (1-2), pp. 91-110, 1997

[Hje99] Hjelm M., Wootton R and Craig J.: *Benefits and drawbacks of telemedicine*, Introduction to Telemedicine, Royal Society of Medicine, London, 1999, Chapter 10

[Hug02] Hughes software systems, *Multi-carrier code division multiple access*, white paper, 2002, www.hssworld.com/whitepapers/whitepaper_pdf/service4.pdf, [15-5-2004]

[IEC03] The International Engineering Consortium, white paper: *OFDM for mobile data communications*, 2003, www.iec.org/acrobat.asp?filecode=179, [15-5-2004]

[IEEE99] IEEE 802.11, 1999 Edition (*ISO/IEC 8802-11: 1999*) IEEE Standards for Information Technology, 1999

[Inc03] Francesca Incardona and Clive Tristram: *Handheld Devices for Healthcare*, Int. Symposium on Handheld devices for Healthcare, Italy, 2003, www.mobi-dev.arakne.it/symposium/main.htm, [15-5-2004]

[Ist01a] Robert S.H. Istepanian, Sapal Tachakra, Konstantinos A. Banitsas *Medical Wireless LAN Systems (MedLAN). State of the Art, Challenges, and Future Directions*, eHealth conference, City University, pp. 43-49, April 2001

[Ist01b] Robert S. H. Istepanian, Sapal Tachakra, Konstantinos A. Banitsas *Health and Mobility: Current Status and Future Paradigms*, IEEE International Workshop on Enterprise networking and computing in Healthcare Industry - HealthCom2001, pp. 77-79, L'Aquila, Italy, June-1st. July 2001.

[ITU96] ITU *G.723 specifications* Annex A, 1996, www.itu.int/rec/dologin.asp?lang=e&id=T-REC-G.723.1-199611-I!AnnA!ZPF-E&type=items, [15-5-2004]

[Joh02] Brad C. Johnson: *Wireless 802.11 LAN Security: Understanding the Key Issues*, System Experts white paper, 2002, www.systemexperts.com/tutors/wireless-issues.pdf, [15-5-2004]

[Joh98] Brad Johanson: *Optimizing Perceptual Quality in JPEG Coded Images*, Stanford University final project, March 1998, ise.stanford.edu/class/psych221/projects/98/jpeg/brad/, [15-5-2004]

[Kap02a] S. Kapp: *802.11a more bandwidth without the wires*, IEEE Internet computing, July-Aug 2002, pp. 75-79

[Kap02b] Steve Kapp: 802.11: *Leaving the Wire Behind*, IEEE Internet Computing magazine, Jan-Feb 2002, pp. 82-85

[Keo03] Peh Keong Teh, Seyed A. Zekavat, *A Merger of OFDM and Antenna Array Beam Pattern Scanning (BPS): Achieving Directionality and Transmit Diversity*, IEEE 37th Asilomar conference on Signals, Systems and Computers, Asilomar, CA, pp. 512-516, Nov 2003

[Khu00] Jamshid Khun-Jush, et al.: *HIPERLAN type 2 for broadband wireless Communication*. Ericsson review 2000 pp.108-119, 2000

[Kri03] Seshagiri Krishnamoorthy, et al.: *Characterization of the 2.4 GHz ISM Band Electromagnetic Interference in a Hospital Environment*, IEEE EMBS conference 2003, Cancun, Mexico, vol. 4, pp. 3245-3248, Sep. 2003

[Kru00] Elizabeth Krupinski at al.: *Evaluation of a Digital Camera for Acquiring Radiographic Images for Telemedicine Applications*, Telemedicine Journal and e-Health, Volume 6 Number 3 Issue 1, pp.297, Sep 2000

[Kyr02] E. Kyriacou, et al.: *Wireless Telemedicine Systems: A Brief Overview*, 2002, IEEE Antennas and Propagation Magazine 44(2): pp. 143-153.

[Lag02] R. L. Lagendijk: *Image Compression*, Center for image compression white paper, 2002, www-etsi2.ugr.es/depar/ccia/mia/complementario/video/Image Compression 2001.pdf, [15-5-2004]

[Lom97] J. S. Lombardo, M. McCarty, R. A. Wojcik: *An evaluation of mobile computing for information access at the point of care*, Biomedical instrumentation & technology, pp. 465-475, September / October 1997

[Man97] Mantas, J.: *Health Telematics Education, State of the Art Report on Education and Telematics in the Health Care Sector*, Studies in Health Technology and Informatics, v.1 41, 10s Press, Amsterdam, pp. 3-7, 1997

[Mit98] Mitchell J.: *Fragmentation to Integration: National Scope Study for the Telemedicine Industry in Australia*, Department of Industry, Science and Tourism, Canberra, ACT, 1998.

[Moo02] Samuel K. Moore: *Extending Healthcare's Reach*, IEEE Spectrum magazine, vol. 38, issue 1, pp.66-71, Jan 2002

[Nee00] Richard van Nee, Ramjee Prasad: *OFDM for wireless multimedia communications*, Artech house, 2000

[NEL04] National Electronic Library of Health, www.nelh.nhs.uk, [15/3/2004]

[NHS95] NHS Executive: *NHS-wide Networking Programme Security Project*, Department of Health, London, 1995

[NIS04] NIST Advanced Encryption Standard (AES) *Questions and Answers*, www.nist.gov/public_affairs/releases/aesq&a.htm, [16/3/2004]

[NLM04] National Library of Medicine, www.nlm.nih.gov, [15/3/2004]

[Nor02] A. C. Norris: *Essentials of Telemedicine and Telecare*. John Wiley & Sons Ltd, 2002

[Nor98] Nortel white paper: *IEEE 802.11 standard for wireless LANs*, Nortel 1998, www.cdt.luth.se/net/courses/01-02/smd088/links/3189.pdf, [16-5-04]

[Nyq28] H. Nyquist: *Certain topics in telegraph transmission theory*, Trans. AIEE, vol. 47, pp 617-644, April 1928

[Oue01] Eric Ouellet, et al.: *Building a Cisco Wireless LAN*, Syngress - Callisma publications, 2001

[Owe01] Thomas J. Owens, Sapal Tachakra, Konstantinos A. Banitsas, Robert S. H. Istepanian, *Securing a Medical Wireless LAN System*, IEEE EMBC conference, Istanbul, vol. 4, pp. 3552-3555, Oct 2001

[Pav98a] Pavlopoulos S., Kyriakou E., Berler A., Koutsouris D.: *Emergency telemedicine applications using mobile and internet communication links - The AMBULANCE Project,* Proceedings of EURO-MED NET 98 Conference, Nicosia, Cyprus, pp. 281-282, 1998

[Pav98b] Pavlopoulos, S, et. al: *A novel emergency telemedicine system based on wireless communication technology - AMBULANCE*, Information Technology in Biomedicine, IEEE Transactions on , Vol. 2 , Issue: 4 , pp. 261-267, Dec. 1998

[Pha00] Phaiboon, S., and Somkuarnpanit, S., *Modeling and Analysis the Effect of Radio-Frequency Fields in Hospitals to the Medical Equipment*, IEEE TENCON 2000, vol.1, pp.92-95, 2000

[Pro99] Proxim white paper: *Selecting and Implementing a Wireless Network in the Healthcare Environment*, Proxim 1999, www.proxim.com/learn/library/appnotes/mobile_healthcare.pdf, [2-2-2003]

[Rao99] Rao M.: *Internet is an Emerging Key Component of Telemedicine Infrastructure in Developing Nations*, 1999, oneworld.org/news/reports99/telemedicine.htm, [13-3-2004]

[Rco04] Remote connections Ltd: *The Darby Trolley*, www.rconnections.com/products.htm, [15/3/2004]

[Ric02] lain E. G. Richardson: *Video Codec Design Developing Image and Video Compression Systems*, John Wiley & Sons, Ltd, 2002

[Sad02] Sadka H. Abdul, *Compressed video communications*, John Wiley publications, 2002

[San02] Asuncion Santamaria, Francisco Lopez-Hernandez: *Wireless LAN Standards and Applications*, Artech house, April 2002, pp.138

[Sha03] Lorna Sharpe: *Doctors at a distance*, IEE review, pp.44-47, October 2003

[Sho01] Matthew B. Shoemake: *Wi-Fi (IEEE 802.11b) and Bluetooth Coexistence Issues and Solutions for the 2.4 GHz ISM Band*, Texas Instruments, 2001, www.techonline.com/community/related_content/21476?li=0, [18-5-2004]

[Sta01] William Stallings: *Wireless Communications & Networks*, Prentice Hall, 1st edition, 2001

[Sta02] Frank Stajano: *Security for ubiquitous computing*, John Wiley & Sons, 2002

[Stu01] Adam Stubblefield, John Ioannidis, Aviel D. Rubin: *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, Rev. 2, AT&T Labs Technical Report TD-4ZCPZZ, Aug 2001, www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/stubbl.pdf, [18-5-2004]

[Sub98] Madhavi Wunnava Subbarao: *On Optimizing Performance in Mobile Packet Radio Networks*, PhD thesis, Johns Hopkins University, 1998

[Sym02] Symantec white paper: *Wireless LAN Security*, Symantec, 2002, securityresponse.symantec.com/avcenter/reference/symantec.wlan.security.pdf, [16-5-2004]

[Tac96] Tachakra S, et al,: *Confidentiality and ethics in Telemedicine*, Journal of Telemedicine and Telecare, 2(1), pp. 68-71, 1996

[Tac99] Tachakra S, Haig. A. *How to do a telemedical consultation*, Introduction to Telemedicine, Royal Society of Medicine, London, 1999

[Tah03] Placide M. Tahou : *Using IPSec to further secure an 802.11b WLAN*, MSc dissertation, Brunel University, 2003

[Tob02] Michael Tobin, *Effects of lossless and lossy image compression and decompression on archival image quality in a bone radiograph and an abdominal CT scan*, May 2002, www.mikety.net/Articles/ImageComp/ImageComp.html, [19-5-2004]

[Vin88] Vincent C F, et al.: *Accuracy of detection of radiography anomalies*, Archives of Emergency Medicine, 5, 101-109, 1988

[Vla95] Vlach, P., et al.: *The Electromagnetic Environment due to Portable Sources in a Typical Hospital Room*, IEEE 17th Annual Engineering in Medicine and Biology Society Conference, vol.1, pp. 683 –684, September 1995

[WGA98] Western Governors' Association: *Telemedicine Action Report*, 1994 and 1998.

[Wil01] Joseph Williams: *The IEEE 802.11b Security Problem, Part 1*, IEEE IT Pro, Nov-Dec 2001, pp. 91-95

[Wil02] Joseph Williams: *Providing for Wireless LAN Security, Part 2*, IEEE IT Pro, Nov-Dec 2002, pp. 44-47

[Wils02] R. Wilson: *Propagation losses through common building materials: 2.4 vs 5 GHz*, Magis network, Aug. 2002, www.siliconrfsystems.com/Papers/Making%20OFDM%20Work%20Webpage%20Part3.pdf, [18-5-2004]

[Yel99] Yellowless P., Wootton R, Craig J.: *How to be successful at telemedicine.* Introduction to Telemedicine, Royal Society of Medicine, London, 1999, Chapter 7

[You97] Young, C., Ahmed Saoudy, S., Budwill, S., *EMI Levels at a 'Patient Care Location' in a Hospital*, IEEE Canadian Conference on Electrical and Computer Engineering, May 1997, vol. 2, pp. 625-628.

[Zyr99] Jim Zyren: *Reliability of IEEE 802.11 Hi Rate DSSS WLANs in a High Density Bluetooth Environment*, Intersil Co., 1999, www.wlana.org/learn/reliabwlan.pdf, [18-5-2004]

Publications

Journal Papers

- **Konstantinos A. Banitsas**, R.S.H. Istepanian, Sapal Tachakra, "Applications of Medical Wireless LAN Systems (MedLAN)", International Journal of Medical Marketing, Vol. 2, no. 2, pp.136-142, Sep 2000
- **Konstantinos A. Banitsas**, Yong Hua Song, Thomas J Owens, “OFDM over IEEE 802.11b hardware for Telemedical applications”, International Journal of Mobile Communications, Vol.2, No. 3, July 2004

Self presented Conference Proceeding Papers

- R.S.H. Istepanian, Sapal Tachakra, **Konstantinos A. Banitsas** "Medical Wireless LAN Systems (MedLAN). State of the Art, Challenges, and Future Directions", eHealth conference, City University, pp. 43-49, April 2001
- **Konstantinos A. Banitsas**, Robert S. H. Istepanian, Sapal Tachakra and Thomas J. Owens, "Modelling issues of Wireless LANs for Accident and Emergency Departments", IEEE EMBC conference, Istanbul, vol. 4, pp. 3540-3543, Oct 2001
- Thomas J. Owens, Sapal Tachakra, **Konstantinos A. Banitsas**, Robert S. H. Istepanian, "Securing a Medical Wireless LAN System", IEEE EMBC conference, Istanbul, vol. 4, pp. 3552-3555, Oct 2001
- **Konstantinos A. Banitsas**, Sapal Tachakra, R.S.H. Istepanian, "Operational Parameters of a Medical Wireless LAN: Security, Range and Interference issues", IEEE EMBC conference, Houston, vol. 3, pp. 1889-1890, Oct 2002
- **Konstantinos A. Banitsas,** Sapal Tachakra, Yong Hua Song, "Adjusting DICOM Specifications When Using Wireless LANs: The MedLAN example", IEEE EMBC conference, Cancun, Mexico, vol. 4, pp. 3661-3664, Sep 2003

Conference papers

- Robert S. H. Istepanian, Sapal Tachakra, **Konstantinos A. Banitsas** "Health and Mobility: Current Status and Future Paradigms", IEEE International Workshop on Enterprise networking and computing in Healthcare Industry - HealthCom2001, pp.77-79, L’Aquila, Italy, June-1st. July 2001.