CSC8360

Wireless Networking

Faculty of Sciences

Study Book

Written by

David Fatseas and Ron Addie

Faculty of Sciences
The University of Southern Queensland

Distributed by

Distance Education Centre
The University of Southern Queensland
Toowoomba Qld 4350
Australia

http://www.usq.edu.au

Produced using LaTeX in a USQ style by the School of Agricultural, Computational, and Engineering Sciences.

Table of Contents

List of Exercises

List of Examples

List of Figures

List of Tables

Module 1

Introduction

Module contents

Objectives

- Gain a broad understanding of wireless communication.
- Gain an understanding of how to succeed in the course.

1.1 Wireless Communication

Australian Communications Authority (ACA) Elctromagnetic fields were discovered approximately 200 years ago, by Danish physicist Hans Christian Orsted, electromagnetic waves by Michael Faraday, in England. It took around another 100 years for the effect of transmission of electromagnetic waves to be harnessed for communication.

From almost this time on it has been highly important in military operations, in industry, and as a means for supporting human communication over distances for political, commercial, and social reasons. Australian Communications Authority (ACA) As a means for communicating between military units, especially during war, wireless communication has proved so useful that it has been often used even when its use risks revealing vital information to the enemies involved in the same conflict.

1.1.1 Waves

Australian Communications Authority (ACA)

All wireless communication makes use of electromagnetic *waves*, which can be described as oscillations of a magnetic and electrical field which can (and does) exists in free space (and even in space which is occupied by certain physical objects.

Waves of magnetic and electrical fields, just like sound waves or water waves, frequently appear to take the form of a steady oscillation at a certain frequency. In fact, it can be shown mathematically that all signals (taking the form of a voltage, for example, varying over time) can be decomposed into different oscillatory components, each component with a different *frequency*.

When wireless transmission was first used for communication, 100 years ago, the frequencies used were relatively low – below one million cycles per second. As our understanding of electromagnetic waves and the technology for their transmision and reception has improved, higher and higher frequencies have been used. Some of the frequencies currently used are shown in Table 1.1. A diagram listing the names of some of the frequency bands currently in use is shown in Figure 1.2.

Figure 1.1 shows the complete RF spectrum allocation chart specified by the Australian Communications Authority (ACA). More information regarding regulations for RF frequency allocations in Australia can be found at: `http://acma.gov.au`.

1.2 Succeeding in this course

This course can best be described as practical-based. The assignments, which comprise a major part of the assessment cover all the major topics of the course. These assignments can be successfully achieved by any student who completes all the practical work. There are practicals every week, which

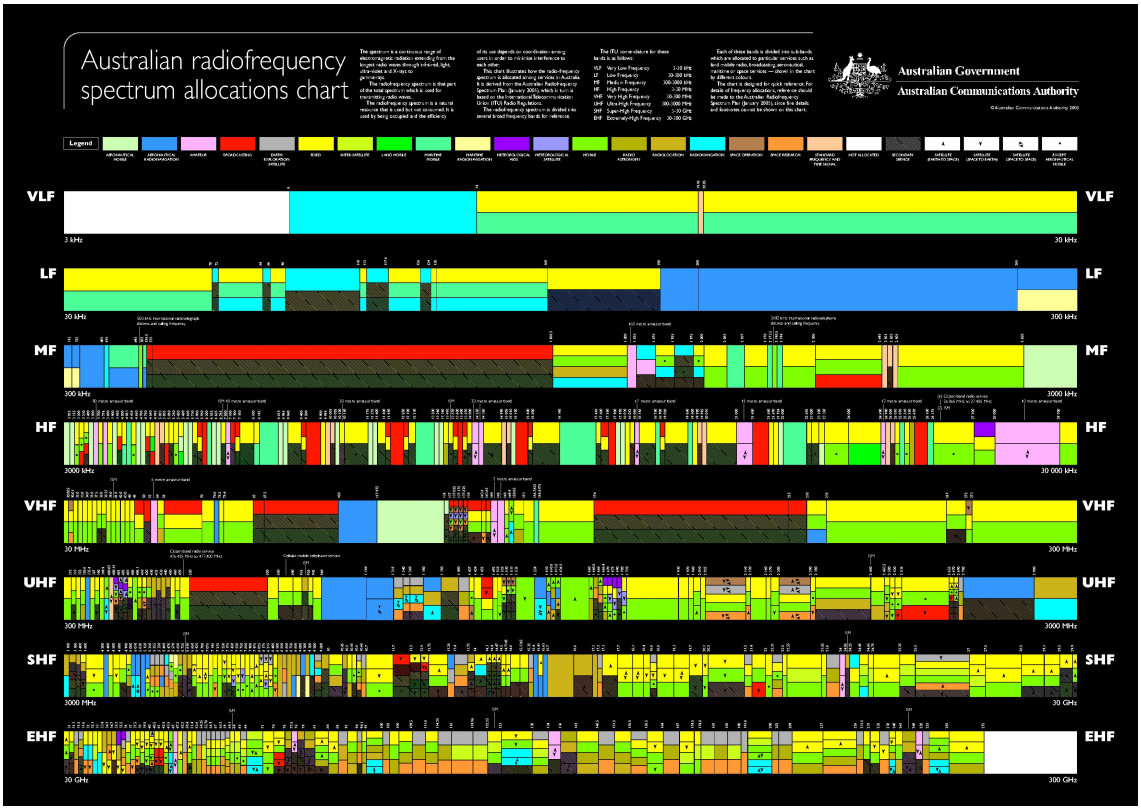

Figure 1.1: RF Frequency Allocation Chart, from http://aca.gov.au

Voice band:	300-3,400 Hz
Broadcast AM radio:	540-1,710 kHz
LF cordless telephone:	43-50 MHz
Broadcast VHF TV:	54-216 MHz (Channels 2-13)
Broadcast FM radio:	88-108 MHz
Broadcast UHF TV:	470-800 MHz
Analog mobile telephone:	824-894 MHz
Digital mobile telephone:	1,710-1,880 MHz

Table 1.1: Important frequency bands used in communication systems

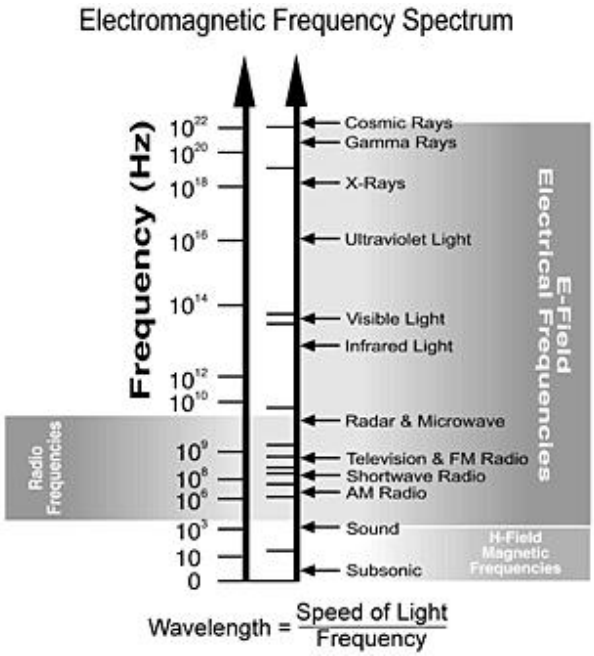

Figure 1.2: The Electromagnetic Frequency Spectrum (from http://www.glenair.com)

directly guide the students in how to complete the assignments. If students do all the practicals, they will be able to successfully complete, and gain a passing result in the assignments, and this will enable them to succeed in the course.

Module 2

History of Wireless Networking

Module contents

Objectives

- Gain an understanding and appreciation of the history and evolution of wireless communication.
- Develop insight into the sort of developments likely to take place in wireless communication in the next few years.

2.1 Wireless Chronology

A brief chronology for the discovery and development of electromagnetism and wireless communication is shown in Figure 2.1.

Year	Discovery / Development
1804	Joseph Fourier discovers that all signals can be decomposed into frequencies
1820	Danish physicist Hans Christian Orsted discovers electromagnetic fields
1831	British scientist Michael Faraday discovers electromagnetic induction
1864	Scottish mathematician and physicist James Clerk Maxwell discovers the partial differential equations for electromagnetic waves (which is later discovered to be the general form of light)
1888	Hertz produces, transmits, and receives electromagnetic waves
1895	Marconi transmits and receives a coded message at a distance of 1.75 miles
1899	Marconi sends the first international wireless message from England to France
1923	The decibel (1/10th of a bel, after A. G. Bell, inventor of the telephone) used to express loss (of power)
1924	The mobile telephone invented by Bell Telephone and introduced to NYC police
1932	The International Telecommunications Union (ITU) formed
1948	Branttain, Bardeen and Shockley build the junction transistor
1948	Claude Shannon develops the theoretical foundations of digital communications
1974	The beginning of TCP/IP
1978	AT&T Bell Labs test a mobile telephone system based on cells
1985	The FCC allows unlicensed use of the ISM band (enabling wifi)
1990	WWW developed
1997	First 802.11 standard for wifi released by IEEE

Table 2.1: Wireless Chronology (Microwave Journal (`microwavejournal.com`)

2.2 Mobile Telephony

As mentioned in the chronology, above, mobile phones were first used in 1924. However, it was not till much later, around 1978, that they became widespread.

Wireless signals lose strength approximately according to the inverse square law, which means that the loss (in power) over a certain distance is a factor of 4 greater if that distance is doubled. More generally, if the distance is increased by the factor a, the loss will be greater by the factor $\frac{1}{a^2}$.

This might seem a disadvantage, but in fact it is probably mostly beneficial, because it means that the signals of our neighours, and fellow citizens, cause

very little interference, with our communication, so long as they take place a little way off.

As a consequence, it makes sense to subdivide the region where wireless communication is taking place into *cells*. The frequencies in use in one cell can then be re-used in a cell that is not too close

2.3 The Modern Era of Wireless Communication

For the moment it seems to reasonable to call the history of wireless since the introduction of the Internet *modern*.

In 1985, the idea that some wireless spectrum can be *unlicensed* was introduced.

The only regulation is that no transmitter should use more than about 10 milliamps.

This allowed for the wifi standards: 802.11a, b, ...

2.3.1 Shared spectrum

The natural measure of capacity, of any transmission medium, is transmission speed, typically measured in bits per second (bits/s). To enable us to discuss transmission speed in a natural, intuitive manner, we also use mega-bits per second (Mbits/s), giga-bits per second (gb/s) and so on. Note that although it would also make sense to use bytes per second, this is not common practice, and therefore should generally be avoided.

The natural measure of *size* of a wireless medium, on the other hand, is the width of the range of frequencies that it makes use of, in cycles per second. Thus, if a wireless technology uses frequencies from 20 million cycles per second (20 MHz) to 100 million cycles per second (100 MHz), we say it has a *bandwidth* of 80 MHz.

It is also common to use the term *bandwidth* to refer to the transmission capacity of a medium. This is not strictly correct, and because the term already has a clear and precise meaning, it is potentially confusing. However, the use of "bandwidth" reveals that there was a widespread perception for a long time that the "natural" transmission capacity of a wireless medium is approximately the same as its bandwidth in the strict sense of the width of the range of frequencies it uses.

Amazingly, the precise relationship between transmission capacity and bandwidth was derived in 1948, before the explosion in use of wireless communication. The formula developed by Hartley and Shannon gives the maximum data rate in the presence of noise, as follows:

$$C \leq B \log_2(1 + S/N)$$

where C is the channel capacity (transmission speed in bits/s), B is the bandwidth, and S/N is the signal-to-noise ratio (SNR), which is the ratio of the power levels of the signal and the noise.

At the same time when spectrum for wireless communication was "liberated" by this de-regulation, the mathematical and technical breakthroughs for making optimal use of this spectrum were developed.

According to the formula of Shannon and Hartley, the maximum possible bit-rate through a wireless medium is not limited to the bandwidth, in cycles per second, but can be much higher. It depends, crucially, on the signal to noise ratio (SNR).

When the transmitter and receiver of a wireless signal are close together, the signal to noise ratio will be higher and hence so will be the transmission capacity. This means that as the density of users of wireless spectrum goes up, and the demand for spectrum increases, we can achieve higher and higher efficiency in its use by decreasing the average distance between transmitters and receivers. To some extent this will occur naturally, as the number of base stations or wireless access points which gather the communication from end users increases.

2.4 Where Wireless is Heading

Some general trends in wireless communication can be observed.

Higher and higher frequencies are coming into regular use. These higher frequencies have some disadvantages, such as being more easily blocked by obstacles, or atmospheric conditions. Also, because the wavelength of higher frequency signals is smaller than 1cm, and in some cases just a few millimetres, aerial designs need to be more complex in order to receive an adequate strength signal. However, a major advantage of higher frequencies is that as we move up the spectrum, the *quantity* of bandwidth becomes dramatically larger.

Module 3

WiFi and 802.11 Regulations, Standards, Organizations

Module contents

Objectives

- Know all the major standards organisations relevant to Wireless communication, and their role in its regulation and development
- Understand, in outline, the meaning and significance of the key standards for wireless LANs.
- Understand, at a high level, how wireless communication works.

3.1 The Standards Organizations

In the past, and still today, some *standards* form as a result of development of a product or service by a single company that subsequently becomes agreed, by the relevant industry, as the preferred way to package that service. Such standards, which do not necessarily stay the same over time, can pass from private to public ownership, or even become adopted as a standard by one of the existing standards organisations.

Another, increasingly common process, is that, once the need for a service or product has been identified, a committee, or group of specialists, is formed within one of the major standards organisations, which then develops a standard for that service, or product.

The most significant organisation in regard to standards in general is the *International Standards Organisation* (ISO). Most nations also have national standards organisations which are affiliated with the ISO. For example, Australia has *Standards Australian* [4].

Although these standards organisations are very important and do create standards relevant to communication, the specific standards organisations which have primarily guided each specific technology is somewhat different.

In telecommunications in general, the primary organization has, and continues to be the ITU (see §3.1.3). Many historical standards in mobile telephony have been developed by the ITU. However, one of the most significant steps in standardisation of mobile wireless was the development of the GSM standard [7], which was undertaken primariy by the European Telecommunications Standards Institute (ETSI) (See §3.1.7). For example, the original standard for SIM cards was developed as part of this standard.

3.1.1 Institute of Electrical and Electronic Engineers (IEEE)

The IEEE is one of the key players in the development and publishing of technical standards development. Some of the notable technical standards that fall under the umbrella of the IEEE 802 Local Area Network (LAN)technical standards include:

- IEEE 802.1 (Interworking - Routing, Bridging and Network-to-Network Communications)
- IEEE 802.2 (Logical Link Control - Error and flow control over data frames)
- IEEE 802.3 (Ethernet LAN - All forms of Ethernet media and interfaces)
- IEEE 802.4 (Token BUS LAN - All forms of Token Bus media and interfaces)
- IEEE 802.5 (Token Ring LAN - All forms of Token Ring media and interfaces)
- IEEE 802.6 (Metropolitan Area Network - MAN technologies, addressing and services)
- IEEE 802.7 (Broadband Technical Advisory Group - Broadband network media, interfaces and other equipment)
- IEEE 802.8 (Fiber Optic Technical Advisory Group - Fibre Optic media used in token passing networks like FDDI)
- IEEE 802.9 (Integrated Voice/Data Network - Integration of voice and data traffic over single network medium)
- IEEE 802.10 (Network Security - Network access controls, encryption, certification and security topics)
- IEEE 802.11(Wireless Networks - Various broadcast frequency and usage technique standards for wireless networking)
- IEEE 802.12 (High-Speed Networking - Various 100Mbps+ technology standards)
- IEEE 802.14 (Cable Broadband LANs and MANs - Standards for designing networks over coaxial cable based broadband connections)
- IEEE 802.15 (Wireless Personal Area Networks - Co-existence of wireless personal area networks with other wireless devices operating in the unlicensed frequency bands)

- IEEE 802.16 (Broadband Wireless Access - The atmospheric interface and related functions associated with Wireless Local Loop)

3.1.2 Internet Engineering Task Force (Internet Standards)

The IETF is the leading body responsible for development and publishing of Internet standards, which are known as Request For Comments (RFCs). The IETF aims to continuously improve the Internet and evolve the Internet architecture through the development and publication of open standards in collaboration with a large international community of network designers, network operators, software and hardware vendors and researchers.

Although the IETF is responsible for all Internet standards, when development of a standard in a new area is undertaken, it is likely that a committee targetted on that particular area will be formed to undertake the work. Members of the IETF and related committees are usually employed by other organisations with a strong interest in Internet standards and the work these individuals undertake will therefore typically be paid for by their employer.

3.1.3 The International Telecommunication Union (ITU)

The ITU has developed and managed standards for communications in general for many decades. They have developed hundreds of standards in this area, many of which are still in use.

ITU-T International Mobile Telecommunications (IMT) is responsible for all 5G non-radio segments as far as overall 5G architecture, network softwarization, integrated network management, fixed mobile convergence is concerned.

3.1.4 The International Standards Organization (ISO)

The International Standards Organization is the parent organization for national standards organizations, which are responsible for standards in every area of society, not excluding communications. The ISO and the ITU coordinate closely, and use similar procedures in the management of standards. In particular, both organizations use a coordinated naming convention of the form **A.123** (Roman letter, then '.', followed by three digit number).

The ISO, in particular, manages some standards in the area of video-conferencing and cryptography that are actively in use at the present time. For example **H.264** is a widely used standard for compression of video communication which is used in video-conferencing and the ISO is also responsible for some encryption standards, e.g. the **X.509** standard for certificates.

3.1.5 The 3rd-Generation Partnership Project (3GPP)

The 3GPP was formed in 1998 with the aim to produce technical specifications and technical reports for 3G Mobile Systems based on evolved GSM core networks and the radio access technologies) that support data speeds up to 2Mbit/s (downlink direction) and support the use both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes.

There are three Technical Specification Groups (TSG) in 3GPP and they are responsible for the production of specifications and technical studies. The areas of focus for these three TSGs are:

- Radio Access Networks (RAN),
- Services & Systems Aspects (SA),
- Core Network & Terminals (CT).

The evolution of 3G (UMTS) to 4G (LTE) to 5G (NR) over the years has been driven by the standards developed, ratified and published by 3GPP. An important requirement of these standards is the backward compatibility and interworking with earlier mobile system generations.

The evolution of mobiles systems is necessary to meet the ever increasing appetite by network subscribers to more reliably create and consume more content at lower latencies. This requirement will need to be supported through the standards which are published by the 3GPP.

3.1.6 The 5th-Generation Public Private Partnership Project (5GPPP)

In conjunction with the global activities undertaken by the 3GPP, the European Union (EU) is funding a 5GPPP project which aims to encourage both the public and private sectors in the EU to collaborate together in the development of 5G. 5GPPP projects range from physical layer to overall architecture, network management and software networks.

This is very important because 5G is not only a new radio but also a framework that integrates new with existing technologies to meet the requirements of 5G applications. The 5G Architecture Working Group as part of the 5GPPP initiative is looking at capturing novel trends and key technological enablers for the realization of the 5G architecture.

It also targets at presenting in a harmonized way the architectural concepts developed in various projects and initiatives (ie: not limited to 5GPPP projects only) so as to provide a consolidated view on the technical directions for the 5G architecture design.

3.1.7 European Telecommunications Standards Institute (ETSI)

Some standards have been developed or guided by the more European oriented standards organization, ETSI. In particular, the GSM [7] standard was developed primarily under the supervision of ETSI and SIM card standards have also been developed and managed by ETSI.

3.2 The WiFi Standard

Compliance with the IEEE 802.11 standard [3] makes possible interoperability between devices manufactured by any vendor within any wireless network type.

3.2.1 What is not regulated

Users do not need a license to use these bands. All users can use the same frequency bands "simultaneously".

3.2.2 What is regulated

IEEE 802.11 standard specifies the use of WiFi equipment operating in certain specific frequencies bands, primarily the unregulated 2.4GHz and 5GHz frequency bands.

User's must use the 802.11 standard. These standards specify use of CSMA which limits interference between nearby users.

Transmitted power must be below the specified level which in the country where the transmission occurs. The required power level is typically $\approx$ 20 dBm, or 100 mW.

3.2.3 The technical details

3.2.4 Evolution of the 802.11 standard

The first release of the IEEE 802.11 standard limited the capacity of WiFi to 2Mbit/s but the use of the regulated 5GHz frequency band saw this increased to 54Mbit/s and introduction the IEEE 802.11b standard saw this increased to 11Mbit/s using the lower unregulated 2.4GHz frequency band.

Both IEEE 802.11a and IEEE 802.11b enabled WiFi speeds to be equivalent or better than speeds offered by wireline Ethernet connectivity which was 10Mbits at that time. which was some of the benefits of using unregulated 2.4GHz frequency band include being able to keep the equipment manufacturing and operating costs down, good radio propagation characteristics and range. The main negative aspect of using unregulated frequency bands is the risk of interference.

While IEEE 802.11 standard specifies the unregulated or lightly regulated frequency bands that WiFi equipment can operate in, this standard does spell out the limits under which these frequency bands can operate. This includes reference to national legisative requirements (ie; ACMA) and international requirements (eg; ITU-R) which are both used to specify the frequency bands and associated channel spacings and the maximum transmit power (EIRP) that equipment can use. Regulation is used to ensure that everyone using WiFi can do so safely and can achieve some level of certainty when it comes to reliability and performance (ie; higher speeds and reduced interference).

In 1999, the IEEE developed and published the IEEE 802.11b specification, supporting devices operating in the unregulated 2.4GHz frequency band to achieve speeds of up to 11Mbit/s (comparable speeds to wireline Ethernet at 10Mbit/s).

By 2003, the new the IEEE 802.11g specification was released with the objective of combining the best capabilities IEEE 802.11a (5GHz)and IEEE 802.11b (2.4GHz). The combining of these two standards allow a single device to either have benefits of higher bandwidth speeds up to 54 Mbps when operating on the 5GHz frequency band or have the extended range benefits if operating on the 2.4GHz frequency band.

In 2009, the new the IEEE 802.11n specification was released which the focus on increased speeds being possible via the use of MIMO (Multi-Input, Multi-Output) Antenna technology. IEEE 802.11n supported speeds of up to 300Mbit/s. It is noted that IEEE 802.11n is backwards compatible with earlier standards.

The latest generation of WiFi devices are now manuafactured to support IEEE 802.11ac specification. This specification goes the next step and support dual-band simultaneous connections on both the 2.4 GHz and 5GHz channels. The IEEE 802.11ac standards allow a single device to be dual band connected with speeds of up to 1300 Mbit/s on the 5GHz band plus speeds up to 450 Mbps on 2.4 GHz band.

3.3 Other Standards Relevant to Wifi

The WiFi Alliance was established in the year 2000 with the aim to test and certify vendor products for compliance with IEEE 802.11 technical standards.

Exercise 3.1: Examine the Standard

Access and read the current 802.11 standard [3], from the IEEE, and find what it says concerning the maximum power which can be generated from a wireless access point. What other standards could be relevant to this question? [1].

Module 4

RF Fundamentals

Module contents

Objectives

To develop a sound, practical understanding of:

- radio frequency behaviour (propagation characteristics, frequency band selection and range);
- the variation in the relationship between power and distance for different frequencies;
- impact of Interference (sources of noise and interference);
- antenna systems (type selection);
- channel bandwidth (vs frequency bands);
- the Shannon-Hartley law
- system gain;
- reflection and refraction of wireless signals;
- multipath propagation and how OFDM overcomes it.

4.1 Wireless Signal Characteristics

4.1.1 Power vs distance

The power of an electromagnetic signal reduces over distance because, as the signal propagates through space, the energy it carries is spread over a larger area. This is illustrated in Figure 4.1.

From the principle illustrated in Figure 4.1, we can conclude, more precisely, that the power of a signal decreases in proportion to the square of the distance between the sender and the receiver:

$$P_d = \frac{1}{d^2} P_1, \tag{4.1}$$

in which P_d denotes the power of the signal received at distance d from the transmitter.

This assumes that the signal is not absorbed by the medium; for example, if the space between the sending antenna and the receiving antenna is completely empty – a vacuum – we can expect the inverse square law to be exact. But if the space has some contents, e.g. air, glass, water, mist, clouds, rain, etc, then there will be some absorption of energy in the intervening space and the inverse square law will not hold exactly.

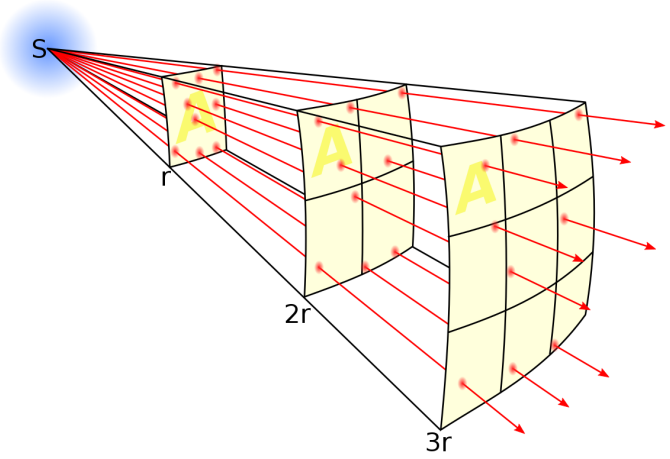

Figure 4.1: The inverse square law (By Borb, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=3816716)

4.1.2 Power vs Frequency

The atmosphere is not completely transparent for light. Some frequencies are absorbed more than others. The absorption of a proportion of the light passing through a medium, such as the atmosphere, which is not completely transparent, introduces additional loss which is also proportional to a power of the distance between the transmitter and the receiver. If the medium is completely transparent, the additional gain (although it is actually a loss, we refer to it as a gain less than 1 to simplify its numerical expression) due to the medium will be $d^0 = 1$, where d is the distance. If the media does introduce loss, this gain will be d^{-a} for some $a > 0$.

[David, here we need to introduce a figure which shows the loss, as this power of d, at different frequencies, due to oxygen, etc.

This would also be a good place to introduce a discussion of the spectrum used in Star Link, as an example of the sort of compromise which can be adopted, when a frequency has loss, but we can work with it.]

For best communication, we naturally prefer to use frequencies of light which have as little loss as possible. However, because modern communication technology is highly efficient, and there is so much commercial pressure to use the available spectrum (frequencies) for communication, we do not simply avoid using frequencies with higher loss, but instead we make use of the best methods of modulation, filtering and receiver designs so that we can make use of all frequencies by adapting to their characteristics.

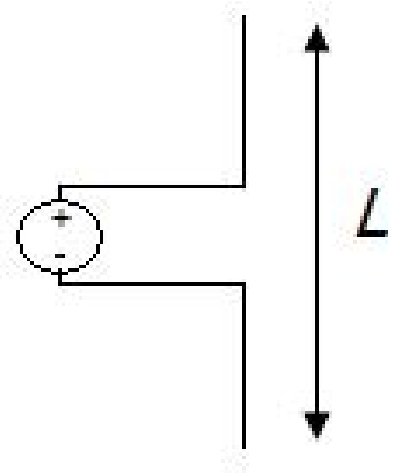

Figure 4.2: A short dipole antenna (from `https://www.antenna-theory.com/antennas/shortdipole.php`)

4.1.3 Noise and interference

Noise is present in all communication systems. It is caused by heat, which is present in all devices and media involved in a communication system, and by electromagnetic radiation, which is also present everywhere. Other communications taking place in the same, or a nearby, location will also cause interference, although in many cases such signals can also be treated as noise. The impact of noise on the capacity of a communication system has been precisely quantified in §4.3.

4.2 Antenna Design and Choice

Antenna design is tricky to explain, and to do. Fortunately, most of us do not need to *design* antennas, but merely to choose the appropriate one from a small range of alternatives, in a certain situation. Nevertheless, there some simple principles which we can easily learn that make it a lot easier to make these choices correctly.

4.2.1 Dipole Antennas

A short dipole antenna is depicted in Figure 4.2. When stimalated by an oscillating voltage at its centre, this antenna causes propagation of an electromagnetic signal. This is because, due to the physical law described by

Maxwell's equations, the *current* in the arms of the antenna directly cause a time-varyig magnetic field in the vicinity of these arms, which then, because it varies in time and space, also leads to a time-varying electrical field. Both these fields then propagate away from the antenna. These propagating fields constitute elemctromagnetic radiation, i.e. radio waves. If this field is, moreover, varied in time according to a *message*, this details of this message will be detectable at a receiver some distance away.

The strength of this signal is, naturally enough, proportional to the strength of the electrical signal at the source, and also to the length of the arms, so long as the antenna is *short*. An antenna is regarded as short only if it is shorter, in length, than a quarter of a wavelength, for the particular frequency of the original signal. As the antenna approaches a half wavelength, in size, the law of signal strength increasing with length of the antenna breaks down, and once the antenna is *longer* than half a wavelength, transmitted signal strength starts reducing.

Simple dipole antennas must, therefore, be of length in roughly the range 1/4 to 1/2 the wavelength of the signal.

4.2.2 Frequency dependence

The idea that the physical dimensions, and shape, of an antenna depends critically on the frequencies being transmitted, or received, is not only true for dipole antennas. If an antenna is designed for frequency f, but used for frequency $2f$, its performance will seriously oompromised.

4.2.3 Reciprocity

Reciprocity is the principle that transmission and reception of electromagnetic signals from an electrically stimulated (or monitored) antenna obey "exactly" the same physical principles. Here is one statement of this principle, from [2]:

> *Reciprocity is one of the most useful (and fortunate) property of antennas. Reciprocity states that the receive and transmit properties of an antenna are identical. Hence, antennas do not have distinct transmit and receive radiation patterns - if you know the radiation pattern in the transmit mode then you also know the pattern in the receive mode. This makes things much simpler, as you can imagine.*

Although it is not completely obvious how to apply this principle, the important takehome message is that our understanding of transmission, such as it is, can be used to help our understanding of reception of signals, and conversely. This is helpful. In particular, an antenna which is well designed for transmission, in a particular context (for example, for a certain frequency range, will also be well designed for receiving signals, in the same context.

4.2.4 Multiple Input Multiple Output (MIMO)

If a larger antenna than 1/4-1/2 wavelength is desired, while retaining the simplicity of the dipole structure, rather than making the dipole itself longer, it is necessary to use multiple antennas, each of which has the preferred 1/4-1/2 wavelength length. If the signals from these multiple antennas have to be combined by carefully selected coefficients, determined by measurements of the channel frequency response, the effective signal to noise ratio can be steadily improved as more antennas are added.

This is particularly important for signals with short wavelengths, because no single antenna will be able to receive a strong signal by itself. Thus, for higher frequencies, it is likely to be essential to use multiple antennas for both sending and receiving signals.

4.3 The Shannon-Hartley law

Supposing a communication channel is not noise free, but has noise with power level N, the error rate of the received signal will be non-zero. The formula of Hartley and Shannon takes this into account, and gives the maximum data rate in the presence of noise, as:

$$C \leq B \log_2(1 + S/N).$$

where C is the channel capacity, in bits/s, B is the bandwidth, in Hz, and S/N is the signal-to-noise ratio (SNR), which is the ratio of the power levels of the signal and the noise, at the receiver.

Example 4.1: The Shannon capacity of a channel

As an example consider we have a radio channel with bandwidth 10 MHz. Say the received signal level is 2 mW, and the noise level is 0.04 mW. What is the Shannon Capacity of the channel?

$$\text{SNR} = S/N = 2mW/0.04mW = 50.$$

$$C = 10 \times 10^6 \times \log_2(1 + \text{SNR}) = 10^7 \times 5.67 = 56.7\text{Mbit/sec.}$$

Note that this capacity value is higher than the Nyquist bandwidth of the channel. To achieve this high value of capacity it is necessary to use more than 2 voltage levels to represent bits ($M > 2$), this was rarely done in practice in the past, however, with the introduction of OFDM it has become more common to use modulation techniques like QPSK (Quadrature Phase Shift Keying) in which more than two symbols are transmitted per time slot, and hence it becomes possible to exceed the Nyquist rate.

The Shannon Capacity formula also provides a general idea of how much noise we can tolerate on a channel. Suppose we have a radio bandwidth of 30 MHz, as for example in the 802.11b channel, and we want to transmit data at 11 Mbit/sec. Then,

$$\begin{aligned} \text{SNR} &= 2(C/B) - 1 \\ \text{SNR} &= 2(11 * 10^6/30 * 10^6) - 1 \\ \text{SNR} &= 1.28 - 1 = 0.28 \end{aligned}$$

This corresponds to a signal *loss* of 5.38 dB, which indicates that the signal power can actually be *less than* the channel noise level.

Exercise 4.1: Using Shannon's capacity formula

Consider we have a channel with bandwidth 125 MHz. Suppose the received signal level is 5 mW, and the noise level is 1.2 mW. What is the Shannon capacity of the channel?

4.4 System Gain

4.4.1 Free space loss

4.4.2 Antenna gain

4.4.3 Feeder loss

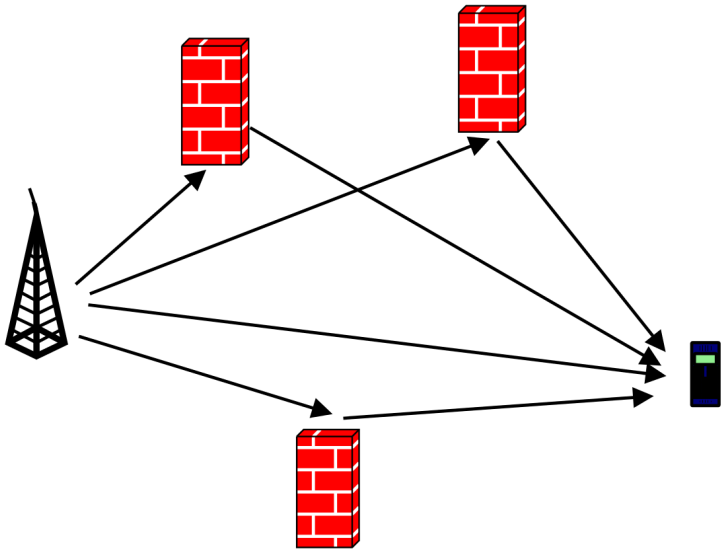

Figure 4.3: Multipath propagation

4.4.4 Transmitter power

4.4.5 Receiver sensitivity

4.5 Reflection and Refraction

4.5.1 Multipath Propagation

Wireless signals pass along multiple paths of different gain, and delay as shown in Figure 4.3. Each path can have a complex gain which depends on the types of reflections or refraction which occur along the path. Nevertheless, each frequency does, in general, have a well-defined complex gain, which can be estimated.

This is the multipath problem.

4.5.2 Orthogonal Frequency Division Multiplexing

OFDM solves the multipath problem. In brief, it works as follows:

- Divide spectrum up into bands
- Relative to a frame, bands are *orthogonal*

- Estimate the complex gain of each frequency
- This overcomes multipath interference
- Transmit over all frequencies at once
- Each frame must include a cyclic continuation

The OFDM concept was first discovered many decades ago, but was fully proved, with an implementation, first, by Australia's CSIRO. They were awarded a patent on the concept, which was adopted in 802.11 from 802.11a. 802.11b was the last non-OFDM wifi.

Module 5

Wireless LANs

Module contents

Objectives

To develop

-
-
-
-

5.1 Wireless Signal Characteristics

Module 6

Mesh, infrastructure mode, bridges, and other wireless modes

Module contents

Objectives

To develop

-
-
-
-

6.1 Wireless Signal Characteristics

Module 7

Wireless Security

Module contents

Objectives

To develop a sound, practical understanding of:

- the history and evolution of security in wireless networks;
- the different standards that can be used to provide encryption and authentication for 802.11 networks;
- why it is necessary to make use of services at layer 3 and higher to complement WiFi security;
- the protocols used to transfer security information during WiFi security setup.

7.1 History

The first of the IEEE802.11 series of standards for wireless communication was accompanied by the Wired Equivalent Privacy (WEP) standard for encryption of communication. Since IEEE802.11 is regarded as a layer 2 protocol (equivalent to Ethernet) it was originally felt that incorporating security at this layer is not appropriate.

In some situations, particularly if security is provided at higher layers, it is true that providing security as part of IEEE802.11 is unnecessary and inappropriate. However, there are also situations where providing security at this layer is by far the most natural and convenient way to do it.

The biggest weakness of the WEP protocol is that it uses a *shared key*. Thus, anyone who makes use of the wireless network is informed of the key that they should use, and they are therefore able to pass this information on to others who could exploit this information.

However, the use of a shared key is appropriate in some very limited use cases, for example in a home wireless network.

Not long after WEP was deployed it was discovered that it could be ”cracked” relatively quickly by listing to communication over the wireless medium and deducing what key has been used for encryption. The method for finding the key relies on the fact that the encryption process will usually be re-initialised with the start of each packet. Since there are many packets typically being sent, many of which will take a predictable form, the code is vulnerable to being cracked by a search through the possible codes.

In addition, the key-space is not all that large, so the search process does not need to be excessively long.

The software for finding out the shared key in use over the wireless network is readily obtainable from the Internet and can be used by anyone with the appropriate equipment (ie. WiFi capable laptop computer).

After these weaknesses were revealed and exploited on may occasions a revised security protocol known as WiFi Protected Access (WPA), and soon afterwards WPA2 was introduced when the the IEEE802.11i was released in 2004, along with subsequent amendments which all add to the robustness of wireless networks. The overall aim of this specification was to provide wireless networks with stronger authentication, confidentiality and integrity measures.

7.2 Wireless Security and Identity Management

WPA2 also provides the ability to encrypt communication using a code based on a shared key. Although this approach has its weaknesses, it is very convenient for domestic users, and in this situation the weakness of using a shared key is not a serious problem.

In addition, WPA2 can work with other systems which allow (or force) users to authenticate before they are able to use the wireless network. When this is included in the overall approach to security, there is no longer a problem of the shared key. WPA II has a much larger key space so that attacks by brute force searches through the range of possible keys are much more difficult.

The WPA2 standard also addresses the weakness of WEP in regard to re-initialization of the encryption at the start of each packet.

7.3 Client Authentication

The following methods of client authentication are available for use in WiFi networks:

(i) OPEN: No authentication is used when accessing the network and/or any of network elements forming part of the overall network. This method should not be considered for implementation in any form of network as it poses a significant security risk and would be wide open to any malicious attack.

(ii) Pre-Shared Key Extensible Authentication Protocol (EAP): Keys are manually distributed among clients and access points (AP) or the authentication server. A Pre-Shared Key simply means a key in symmetric cryptography [6]. This key is derived by some prior mechanism and shared between the parties before the protocol using it takes place. It is merely a bit sequence of given length, each bit of which has been chosen at random uniformly and independently. For EAP-PSK, the PSK is the long-term 16-byte credential shared by the EAP peer and server.

(iii) Lightweight EAP (LEAP): Cisco proprietary EAP method introduced to provide dynamic keying for WEP (depreciated).

(iv) EAP-TLS: This method employs Transport Layer Security (TLS); PKI certificates are required on AP and client devices.

(v) EAP-TTLS: The EAP-Tunneled Transport Layer Security (EAP-TTLS) protocol is an extension of the EAP-TLS mechanism. EAP-TTLS is different from EAP-TLS because it does away with the EAP-TLS requirement of a supplicant-side certificate. Only the authentication server component requires a digital certificate.

(vi) Protected EAP (PEAP): PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server.

(vii) EAP-FAST: EAP-FAST is an EAP method developed by Cisco that enables secure communication between a client and an authentication server by using Transport Layer Security (TLS) to establish a mutually authenticated tunnel.

7.4 Proxy-based Security

In some situations use of a security protocol embedded in Layer 2, the 802.11 layer, is really not appropriate. An example is shared use by patrons of a commercial Wifi network in a restaurant or hotel. In these situations a different approach which is widely used is to provide free unencrypted access to the wireless network, but to limit the pathways from this network.

The WiFi network is limited for use to gain access to a certain Proxy server.

The Proxy server is then configured to allow users from the wireless network to connect to hosts in the Internet at large only if they have authenticated at the Proxy server.

This limits the uses that the wireless network can be put to because Proxy servers have limited capabilities.

The big advantage of this configuration is that access can be controlled by a system installed on the Proxy server which is relatively self-managing. For example, this software might handle the registration of new users, and their payment for access over a period of time.

It should be kept in mind that in this arrangement, since the wireless network provides free access, it may be possible for users who have not registered to intercept communications of the users of the network. It should be possible to configure the Proxy server so that it forces all communication to be encrypted through the use of SSL, however it is doubtful that this is widely done in practise.

7.5 Virtual Private Networks

Another method for providing security for wireless networks at a higher layer is to provide limited access to the users of the wireless network unless they have connected to a Virtual Private Network (VPN).

A VPN is usually configured to require both authentication, using a database of user identities provided by a different system, and encryption. This approach therefore overcomes the weakness of the un-encrypted communication which arises with the use of Proxy servers.

7.6 MAC Address Registration

Yet another for limiting access to wireless networks is to require users to register the MAC address (Ethernet address, also known as Hardware address) with the Wireless Access Point before they are permitted access. Wireless access points can limit access to a list of registered MAC addresses.

This is a simple mechanism, however it does not really provide a big increase in security because software which allows users to masquerade as having a different MAC address than is really present in their computer is available. Also, this method is not idea from the point of view of convenience either, because it means that each user must go through an administrative procedure before gaining access to the network. In some situations a wireless network might only be used for a very brief period, in which case registering to use it before the first use might be infeasible.

Exercise 7.1: A scenario where you are a network administrator

Imagine that you are the network administrator of a small company, with approximately 80 employees, which provides wholesale and retail services to a small community at three locations. Some of the staff need to travel within the local region to visit clients for installation and maintenance of the services provided by your com- pany. Describe all the possible applications of wireless networking to your companies operations.

Exercise 7.2: Setting up a point-to-point link

In the same context as the previous question, suppose you need to establish communication between two buildings separated by two kilometres. One of the buildings is visible from the other and conversely. Describe how you would approach solving the problem of establishing cost-effective communication between these two sites, including:

(a) costing and selection of alternative technical solutions – including considerations of communication performance;

(b) description of all the protocol layers involved in the communication between the sites in your proposed solution;

(c) consideration of security – a description of the issues and your proposed solution;

(d) describe your plan for ongoing monitoring and maintenance of this facility.

7.7 Security Design

Traditionally design of networks has been viewed as a constrained optimization problem. The constraints in this problem are the security objectives – a statement concerning what conditions should be allowed, and what events or conditions should not be allowed. Subject to these constraints, the objective of the designer is to find the network with minimum cost.

It is not obvious that this framework applies to security. In particular, the question of how the security constraints can be *expressed* needs to be addressed.

Fortunately, this issue has been addressed in the security literature, and although there is no standard way to do it, much research adopts the idea that security constraints can be expressed by means of *rules* which are recorded either informally, or in a formal language, like XACML [5].

Security rules can sometimes, but not always, be *enforced*. When rules can be enforced, it helps to achieve the objective of minimising the likelihood of failures (like break-ins, data-loss, data-release). For example, limiting access to certain servers to users who already have access to certain other computers will reduce the chance of a break-in. However, rules that have not been technically enforced can still be useful. A good example of this is a rule, or collection of rules, which prescribe what types of access to user-data are allowed by system administrators.

Enforcing a rule which proscribes access to user data is probably not a good option, because the flexibility of allowing administrators such access can be convenient for the users. There may also be situations where preventing such access is warranted, and should be enforced.

It might seem that all security rules are about *preventing* undesirable outcomes. However, it is also useful to include rules which state what *should be allowed*, or *what must be possible*. For example, it is common to express a performance constraint like: *all users must be able to access their services 99.99% of the time*.

Rules which state what *should be allowed* are called *positive* rules.

In summary, we can break down the rules which define security of a network into four categories: (i) positive, enforced rules; (ii) positive, un-enforced rules; (iii) negative, enforced rules; and (iv) negative, un-enforced rules. Usually it will be clear in which category a rule falls, and it is helpful to make this sub-division in to different types of rules.

Consider a rule like: "User's should change their password at least once every 4 weeks". Such a rule should be described as positive because it states something that should (or perhaps must) be done. This rule can be enforced, however doing so might not be a good policy. It could offend some users, and most of its objective will be achieved by simply sending reminders, especially if this is only done when a password has not been changed for at least the target period of time.

Exercise 7.3: Security rules

It has become established practice to define network security by means of rules. These rules can take many different forms. Although security is often concerned with preventing access, good security requires

consideration of other aspects than merely preventing access. Rules may state what types of service or activity are not allowed, and also what should be allowed. Rules may take precedence over other rules. Complete set of rules for the following situations:

(a) A network of wireless access which is provided in a nationwide network of hotels;

(b) a university campus network (with three types of user – academics, admin, and students);

(c) a home wireless network. In each case, include both positive and negative rules, and also rules which are not simply about access, and attempt to ensure that the resulting set of rules is unambiguous, complete, and consistent.

Module 8

Wireless LAN design

Module 9

Wireless LAN troubleshooting

Module 10

Cellular and Fixed Wireless Networks

Module 11

Emerging Trends and ACS Code of Ethics

Bibliography

[1] Mohammad Kaisb Layous Alhasnawi, Shahab Abdulla, David Fatseas, and Ronald G. Addie. Spectral density constraints on wireless communication. *Heliyon*, 2020.

[2] antennatheory.com. The addition of explicit congestion notification (ecn) to ip, 2022. `https://www.antenna-theory.com/definitions/reciprocity.php#:~:text=Reciprocity%20states%20that%20the%20receive,pattern%20in%20the%20receive%20mode.`

[3] IEEE Standards Association et al. 802.11-2012-ieee standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *Retrieved from http://standards. IEEE. org/about/get/802/802.11. html*, 2012.

[4] Standards Australia. Standards australia, 2022. `https://www.standards.org.au/`.

[5] OASIS (Organization for the Advancement of Structured Information Standards). Oasis extensible access control markup language (xacml) tc, 2010. `http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml`.

[6] IETF. RFC4764 : Pre-shared key extensible authentication protocol, 2007. `https://datatracker.ietf.org/doc/html/rfc4764`.

[7] Wikipedia. Gsm, 2022. `https://en.wikipedia.org/wiki/GSM`.