香港開放教科書
Open Textbooks for Hong Kong

Free to use. 自由編輯運用
Free to change. 共享優質課本
Free to share.

ELEC S212 Network Programming And Design (Free Courseware)

香港公開大學
THE OPEN UNIVERSITY OF HONG KONG

Contents

Chapter 1 Introduction to wireless networks

1.1 About this module

Welcome to this free courseware module 'Introduction to wireless networks'!

This module is taken from the OUHK course *ELEC S212 Network Programming and Design (http://www.ouhk.edu.hk/wcsprd/Satellite?pagename=OUHK/tcGenericPage2010&c=C_ETPU&cid=191154024000&lang=eng&pri=2)*, a ten-credit, Middle level course that is part of the Bachelor of Science (BSc) or BSc (Hons) degree programme offered by the School of Science and Technology (http://www.ouhk.edu.hk/wcsprd/Satellite?pagename=OUHK/tcSubWeb&l=C_ST&lid=191133000200&lang=eng) of the OUHK. This course provides you with a firm foundation for understanding network programming and design.

ELECS212 is mainly presented in printed format and comprises ten study units. Each unit contains study content, activities, self-tests, assigned readings, etc for students' self-learning. This module (The materials for this module, taken from the print-based course ELECS212, have been specially adapted to make them more suitable for studying online, and multimedia elements have been added where appropriate. In addition to this topic on 'Introduction to wireless network', 'Wireless network protocols', 'Wireless LAN design models', 'Wireless access to the Internet' and 'Wireless network security' which are extracts from Unit 9 of the course, the original Unit 9 also includes the topics 'WAN (Wide Area Network) essentials' and 'Wireless LAN survey'.) retains most of these elements, so you can have a taste of what an OUHK course is like. Please note that no credits can be earned on completion of this module. If you would like to pursue it further, you are welcome to enrol in *ELEC S212 Network Programming and Design (http://www.ouhk.edu.hk/wcsprd/Satellite?pagename=OUHK/tcGenericPage2010&c=C_ETPU&cid=191154024000&lang=eng&pri=2)*.

This module will take you about **eight hours** to complete, including the time for completing the activities and self-tests (but not including the time for assigned readings).

Good luck, and enjoy your study!

1.2 Introduction

This module will enable you to understand various wireless technologies, especially those that have been infused into our daily lives. Also, a range of wireless network protocols and wireless LAN design models will be discussed.

Another topic that we cannot afford to miss is wireless network security, because wireless medium is more vulnerable to attack than physical medium. In addition, some labs on wireless technology, with reference to the textbook A Practical Approach to Internet Programming and Multimedia Technologies (Kwan, R, Tsang, P, Kwok, P, Koong, K, Mak, J and Wu, J (2009) A Practical Approach to Internet Programming and Multimedia Technologies, Hong Kong: Open University of Hong Kong Press.), have been incorporated into the module to help you consolidate what you have learned.

1.3 Introduction to wireless networks

As the name implies, wireless networks do not need to use wire lines to transmit signals. Rather, a wireless network uses the atmosphere as the network medium for transmitting data. But, considering that wired networks have been working so well for so far, why do we need to go wireless? What are the advantages of wireless networks?

In the following, we compare wireless networks with their wired counterparts, so that we can see the areas in which wireless networks work best, and those in which wired networks are more sutiable.

1.3.1 Comparison of wireless and wired networks

The most obvious advantage of wireless networking is **mobility**, and wireless networks typically have a great deal of **flexibility**.

Mobility of wireless networking

Wireless network users can connect to existing networks and are then allowed to roam freely. Wireless data networks free users from the tethers of an Ethernet cable at a desk. They can work in the library, in a conference room, in the airport, or even in the coffee house across the street. As long as the wireless users remain within the range of the base station, they can take advantage of the network.

Flexibility of wireless networking

The flexibility of wireless networks can translate into rapid deployment. Wireless networks use a number of base stations to connect users to an existing network. With the infrastructure built, adding a user to a wireless network is a matter of configuring the infrastructure, but it does not involve running cables, punching down terminals, and patching in a new jack as wired networks need to. Only could such flexibility make possible the public hot spot operation, through which public users can gain access to the network connections wirelessly provided by service providers in various locations or premises.

However, wireless networks do not replace fixed networks. Servers and other data centre equipment are very static in terms of their location; they may as well be connected to wires that do not move. And, the speed of wireless networks is **constrained** by the available bandwidth. Furthermore, while security on any network is a prime concern, it is more **critical** for wireless networks.

Speed constrain of wireless networks

Information theory (http://en.wikipedia.org/wiki/Information_theory) can be used to deduce the upper limit on the speed of a network. Wireless-network hardware tends to be slower than wired hardware. Unlike the 10-GB Ethernet standard, wireless-network standards must carefully validate received frames (A term for the unit of data transferred on a network; its size depends on the type of network implemented. See the Glossary at the end of this module for more information.) to guard against loss due to the unreliability of the wireless medium.

Security issues of wireless networks

On wireless networks, security is often a critical concern because the network transmissions are available to anyone within range of the transmitter with the appropriate antenna.

On a wired network, the signals stay in the wires and can be protected by strong physical-access control (locks on the doors of wiring closets, and so on). On a wireless network, sniffing is much easier because the radio transmissions are designed to be processed by any receiver within range.

Table 1.1 provides a comparison of the features of wireless and wired networks.

	Wireless networks	Wired networks
Mobility	High	Low
Flexibility	High	Low
Speed	Moderate	High
Security	Poor	good

Table 1.1: Comparison of wireless and wired networks

1.3.2 Wireless transmission

The following sections introduce some basic concepts relating to the operation of wireless networks, including data transmission.

The topics to be covered include:

- radio spectrum of wireless networks;
- access methods of wireless networks;
- association process of wireless networks.

Radio spectrum

Like all networks, wireless networks transmit data over a network medium. The medium is a form of electromagnetic radiation. The wireless spectrum is a continuum of electromagnetic waves used for data and voice communication. On the spectrum, waves are arranged according to their frequencies. The wireless spectrum spans frequencies 9KHz and 300 GHz, which is shown in Figure 1.1.

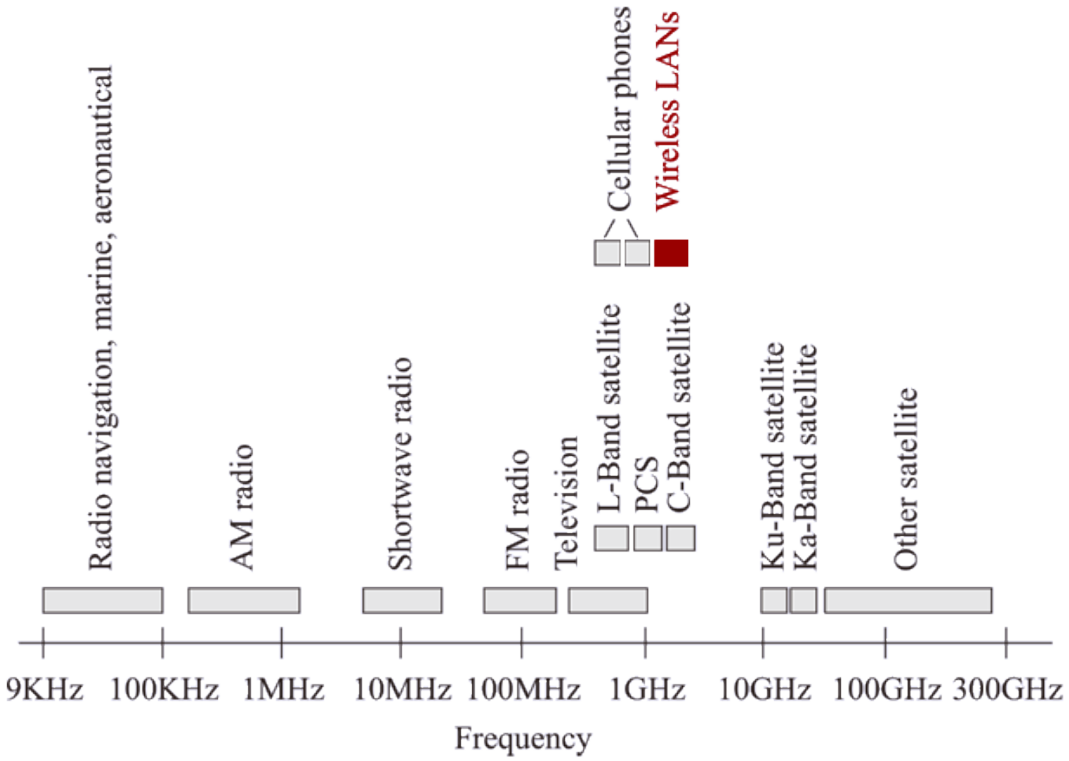

Fig. 1.1: The wireless spectrum

Radio waves can penetrate most office obstructions and offer a wider coverage range. It is no surprise that most, if not all, 802.11 products on the market use the radio wave physical layer.

Frequency bands used by 802.11 products

802.11b and 802.11g use the 2.4 GHz frequency band, while 802.11a uses the 5GHz frequency band.

802.11 divides each of the frequency bands into channels, analogously to how radio and TV broadcast bands are sub-divided, but with greater channel width and overlap. For example the 2.4000–2.4835 GHz band is divided into 13 channels each of width 22 MHz but spaced only 5 MHz apart, with channel 1 centred on 2.412 GHz and channel 13 on 2.472 GHz, to which Japan adds a 14th channel, i.e. 12 MHz above channel 13.

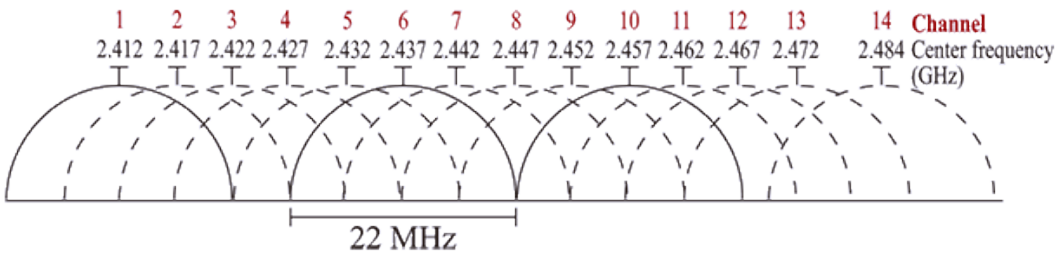

Fig. 1.2: 2.4 GHz Wi-Fi channels (802.11b or g)

Access methods

802.11 does not depart from the previous IEEE 802 (http://en.wikipedia.org/wiki/IEEE_802) standards in any radical way. The standard successfully adapts Ethernet-style networking to radio links. Like Ethernet, 802.11 uses a Carrier Sense Multiple Access (CSMA) (http://en.wikipedia.org/wiki/Carrier_sense_multiple_access) scheme to control access to the transmission medium. However, collisions waste valuable transmission capacity, so rather than implementing the collision detection (CSMA/CD) employed by Ethernet, 802.11 uses **collision avoidance (CSMA/CA)**. Also like Ethernet, 802.11 uses a distributed access scheme with no centralized controller. Each 802.11 station uses the same method to gain access to the medium.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

In CSMA/CA, before a node (End point of a network connection. Nodes include any device attached to a network such as file servers, printers, or workstations.) begins to send data, it checks the medium. If it detects no transmission activity, it waits a brief, random amount of time, and then sends its transmission. If the node does detect activity, it waits a brief period of time before checking the channel again. CSMA/CA does not eliminate the potential for collisions— it only minimizes them. This is the major difference between CSMA/CA and CSMA/CD (used by Ethernet).

In CSMA/CD, when a node finds out that the medium is idle, the node immediately starts to send data, but in CSMA/CA it waits for a brief, random amount of time before doing so.

The major differences between 802.11 and Ethernet therefore stem from the differences in the underlying medium. To tackle the vulnerability of wireless communications to external interference, 802.11 incorporates positive acknowledgments (meaning that all transmitted frames must be acknowledged) to ensure the reliable transmission of data.

Association

At any physical location – whether it is an Internet cafe, airport lounge, etc. — there could be many different wireless networks providing network coverage. A user therefore has to go through an association process to establish a link with a particular existing wireless network before he can use it to transmit data.

Association process of a wireless network

Click this link to watch the video:
http://www.opentextbooks.org.hk/system/files/resource/10/10308/10314/media/video0001.mp4

In order to establish a link with a particular existing wireless network for transmitting data, a user has to go through an association process.

Each wireless network is identified with a SSID (Service Set Identifier) — that is, a unique character string through which he can decide which wireless network he wants to associate with. During the association, the access point (A device used on wireless LANs that transmits and receives wireless signals to and from multiple nodes and retransmits them to the rest of the network segment. See the Glossary at the end of this module for more information.) (AP) of the wireless network may or may not (depending on how the security protection is configured) authenticate the user before granting him access to the network connectivity.

The security protection described in the animation will be discussed further in a later part of this module.

This web page (http://www.cisco.com/c/en/us/products/wireless/aironet-1200-series/index.html) shows you some information about an access point product, for your reference.

Now read the following material and attempt Self-test 1 (Page 8) afterwards. While Suggested answers to Self-test 1 (Page 8) are provided, you should always try to answer the questions on your own first. If you can't answer a particular question, this shows that you most likely need to review some of the material that you've worked through so far.

Reading

Dean (2010) (Dean, T (2010) Network+ Guide to Networks, 5th edn, Thomson Course Technology.) 364–73.

Do you know you can improve your Wi-Fi connection without spending much? See Activity 1 (Page 8) and have a try!

1.3.2.1 Self-test 1

1. What is an SSID?
2. What is the Access Point?
3. What frequency range is shared by the most popular type of wireless LAN?

1.3.2.1.1 Suggested answers to Self-test 1

1. Each wireless network is identified with a SSID (Service Set Identifier) — a unique character string — through which users can decide which wireless network they would associate with.
2. The AP is a device used on wireless LANs that transmits and receives wireless signals to and from multiple nodes, and retransmits them to the rest of the network segment. Access points can connect a group of nodes with a network or two networks with each other. They may use directional or omni-directional antennas.
3. 2.4–2.4835 GHz.

1.3.2.2 Activity 1

Do you know how to improve your Wi-Fi connection without having spending a lot of money?

In this short video (http://www.videojug.com/film/how-to-boost-your-wi-fi-signal), you can see how to make a parabolic reflector using some aluminium foil, and then use it to boost the reception of Wi-Fi signal by two bars on a Windows desktop.

1.4 Wireless network protocols

Wireless networking is a hot industry segment. Several wireless technologies have been targeted primarily for data transmission. The IEEE 802.11 standards define how wireless LAN should work. They are analogous to their wired counterpart 802.3

Ethernet standard (http://en.wikipedia.org/wiki/IEEE_802.3), which defines how wired network should work.

Bluetooth is another standard of wireless networking, which is used to build small networks between peripherals: a form of wireless wires, if you will. Infrared serves the similar purpose of Bluetooth, but is regarded as an older technology.

We will explore each of them in the following sections and walk through their major functions and features.

1.4.1 Wireless LANs (802.11 technologies)

802.11, also known as wireless LAN (WLAN) technology, goes by a variety of names, depending on who is talking about it. Some people call it 802.11 wireless Ethernet, to emphasize its shared lineage with the traditional wired Ethernet (802.3). The Wireless Ethernet Compatibility Alliance (WECA) has been pushing its **Wi-Fi (wireless fidelity) certification programme**. There are three principal wireless LAN technologies standards, namely **802.11b**, **802.11a** and **802.11g**.

Wi-Fi certification programme

Any 802.11 vendor can have its products tested for interoperability. Equipment that passes the test suite can use the Wi-Fi mark. So, today we often use the term 'Wi-Fi' interchangeably with the term 'wireless LAN.'

802.11b

The IEEE 802.11b standard is the dominant standard for WLANs. It reuses many of the Ethernet Logical Link Control (LLC) (http://en.wikipedia.org/wiki/Logical_Link_Control) components, and is designed to easily connect into Ethernet LANs. For these reasons, IEEE 802.11b is usually called ‘wireless Ethernet’, but its official name is wireless LAN. Some vendors selling 802.11b equipment have trademarked the name Wi-Fi to refer to 802.11b. There are two versions of 802.11b: frequency-hopping spread-spectrum (FHSS) (http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum) systems run at 1 Mbps and 2 Mbps; and direct-sequence spread-spectrum (DSSS) (http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum) systems run at 1 Mbps, 2 Mbps, 5.5 Mbps and 11 Mbps. DSSS systems dominate the marketplace because they are faster.

802.11a

The IEEE 802.11a standard for WLAN is newer than 802.11b. It operates in a 5-GHz frequency range. The total bandwidth is 300 MHz, substantially more than the 22 MHz of 802.11b. This means that it can transmit data faster than 802.11b. The possible data rates would be 6 Mbps to 54 Mbps. However, as it operates in 5-GHz range, it requires more power for transmission.

802.11g

The IEEE 802.11g comes after 802.11b and 802.11a. 802.11g is designed to combine many of the advantages of 802.11b and 802.11a. It can attain a transmission rate of 54Mbps, while it operates in the 2.4-GHz range and thus has more moderate power consumption than 802.11b. Currently, 802.11g is the most widely-used WLAN protocol.

802.11n is a recent amendment to previous 802.11 standards, and there is an **802.11i** standard for securing wireless networks.

802.11n

802.11n is a recent amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and many other newer features. Enterprises have begun migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal. An 802.11n network operates at either 5GHz or 2.4GHz frequency bands, achieving a sustainable throughput of 144Mbps and a peak transmission rate of 600Mbps. The maximum indoor and outdoor ranges go up to 300 feet and 500 feet, respectively.

The current state of the art supports a maximum transmission rate of 450 Mbps, with the use of three spatial streams at a channel width of 40 MHz. Depending on the environment, this may translate into a sustainable throughput for TCP/IP of 110 Mbps.

The IEEE 802.11n task group has completed their work, and the amendment was approved by IEEE in September 2009. It will be followed by publication in mid October 2009. In other words, the IEEE 802.11n standard will finally be released after six years' deliberation, which is an exceptionally long process of standardization in the telecommunications industry.

Major networking manufacturers have been releasing 'pre-N', 'draft n' or 'MIMO-based' products based on early specs. These vendors anticipated that the final version would not be significantly different from the draft, and in a bid to get the early mover advantage they pushed ahead with many of the new technologies. Depending on the manufacturer, a firmware update should make current 'Draft-N' hardware compatible with the final version. More importantly, the incompatibility issues among products from different manufacturers that have hindered the wide adoption of 802.11n will vanish gradually, and the era of 802.11n, representing high speed wireless LAN connectivity, will come soon.

802.11i

802.11i is a security protocol designed to protect the wireless network. It uses Extensible Authentication Protocol (EAP) (http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol) with strong encryption scheme, and dynamically assigns every transmission its own key to heighten the protection of the data in transmit against taping or tampering. With 802.11i enabled, logging on to a wireless network is more complex than with WEP (Wired Equivalent Privacy) and, in return, a higher level of security protection can be achieved.

We will cover this protocol further, together with the subject of wireless security, in a later part of this module.

1.4.2 Bluetooth

A wireless PAN (personal area network) (WPAN) (http://en.wikipedia.org/wiki/Personal_area_network#Wireless_PAN) provides hands-free connectivity and communications within a confined range and limited throughput capacity. Bluetooth (http://en.wikipedia.org/wiki/Bluetooth) is a perfect example of a wireless PAN technology that is both beneficial and that is in widespread use. Everything from Bluetooth mice to headsets are being used on a daily basis throughout the world.

Bluetooth has been codified by the IEEE in their 802.15.1 (http://en.wikipedia.org/wiki/IEEE_802.15) standard, which describes WPAN technology. A Bluetooth PAN is also known as a piconet (http://en.wikipedia.org/wiki/Piconet). The simplest type of piconet is one that contains one master and one slave, which communicate in a point-to-point fashion with each other.

1.4.3 Infrared (IR)

It is a common experience for us to use infrared (IR) (http://en.wikipedia.org/wiki/Infrared) signalling to change channels on a TV via a TV remote. IR signals depend on a line-of-sight transmission (http://en.wikipedia.org/wiki/Line-of-sight_propagation) path between the sender and receiver. This has in fact hindered the application of IR from advancing beyond remote controlling and peripherals connection. IR signals occur at very high frequencies, in the 300- to 300,000-Ghz range, just above the visible spectrum (http://en.wikipedia.org/wiki/Visible_spectrum) of light.

Table 1.2 offers a comparison of the common wireless networking standards, their ranges and throughputs.

Standard	Frequency range	Theoretical maximum throughput	Effective throughput (approximate)	Average geographic range
802.11b ("Wi-Fi")	2.4 GHz	11 Mbps	5 Mbps	100 meters (or approximately 330 feet)
802.11a	5 GHz	54 Mbps	11–18 Mbps	20 meters (or approximately 66 feet)
802.11g	2.4 GHz	54 Mbps	20–25 Mbps	100 meters (or approximately 330 feet)
Bluetooth ver. 1.x	2.4 GHz	1 Mbps	723 Kbps	10 meters (or approximately 33 feet)
Bluetooth ver. 2.0	2.4 GHz	2.1 Mbps	1.5 Mbps	30 meters (or approximately 100 feet)
IrDA	300–300,000 GHz	4 Mbps	3.5 Mbps	1 meter (or approximately 3.3 feet)

Table 1.2: Comparison of the common wireless networking standards

Source: Dean 2006 (Dean, T (2010) Network+ Guide to Networks, 5th edn, Thomson Course Technology). 4e

Now, read the following material to learn more about wireless network protocols:

Reading

Dean (2010) (Dean, T (2010) Network+ Guide to Networks, 5th edn, Thomson Course Technology.) 373–83.

To see if you have understood the topics we have covered so far, attempt Self-test 2 (Page 14) on your own before checking the Suggested answers to Self-test 2 (Page 14).

In practice, 802.11b and 802.11g wireless transmission technologies are more commonly used in business LANs than Bluetooth. Can you think of some underlying reasons? Complete Activity 2 (Page 14) and take a look at its Feedback to Activity 2 (Page 14) afterwards.

1.4.3.1 Self-test 2

1. In the 802.3 Ethernet, the IEEE specifies CSMA/CD as the access method. In the 802.11 standard, the IEEE specifies what type of access method?
2. What are the theoretical maximum throughputs of 802.11 a, b, g, and n?
3. What is MIMO?

1.4.3.1.1 Suggested answers to Self-test 2

1. CSMA/CA
2. 802.11a: 54Mbps, 802.11b: 11Mbps, 802.11g: 54Mbps, 802.11n: 600Mbps,
3. MIMO (multiple-input and multiple-output) is the use of multiple antennas at both the transmitter and receiver to improve communication performance. MIMO technology has to be used in wireless communications (e.g. 802.11n), since it offers significant increases in data throughput and link range without additional bandwidth or transmit power.

1.4.3.2 Activity 2

Investigate why the 802.11b and 802.11g wireless transmission technologies are more commonly used in business LANs than Bluetooth. This is an open question. You can try to come up with at least two reasons.

1.4.3.2.1 Feedback to Activity 2

This is an open question. You should come up with your own answer.

The following are some examples of the reasons:

1. 802.11 signals travel farther than Bluetooth signals.
2. 802.11 technologies transmit data at higher throughputs than Bluetooth.

1.5 Wireless LAN design models

To help you put together the pieces of information you have learned so far in this unit, this section presents how the WLAN models that have evolved over time.

We start with the first model implemented using IEEE 802.11 technology, and then progress through the second stage of WLAN design models.

1.5.1 Intelligent edge

The first devices to be released to the market were standard APs that are still used heavily today. This kind of AP contains the entire logic system needed to implement, manage, and secure (according to the original IEEE 802.11 specification) a WLAN. The benefit of this type of WLAN is that implementation is very quick when you are implementing only one AP.

The drawback to this type of WLAN is that implementation is very slow when you are implementing dozens or hundreds of APs. There are many networks around the world that have more than 1000 APs. You can imagine the time involved if you have to set up each AP individually. At stage one, intelligent edge, this is your only choice. The APs implemented in this model are also known as autonomous APs.

1.5.2 Wireless LAN management systems

When we arrive at stage two in the evolution of WLAN management, we encounter centralized configuration management with distributed intelligence. The devices and software that provide this functionality are known as a WLAN Network Management System (WNMS).

This stage provides much faster implementations of traditional APs, and works using SNMP (http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol) or other proprietary communication protocols to configure the APs across the network. The WNMSs usually supports the rollout of firmware (http://en.wikipedia.org/wiki/

Firmware) so that the APs can be updated without having to visit each one individually. This model provides scalability, but does not cause much impact to the topologies (The physical layout of the network, how the cables are arranged, and how the computers are connected.), and to the infrastructure cost of the APs. In short, this model centralizes management, but distributes processing.

1.5.3 A lab on setting up an ad hoc wireless network

Sometimes we need to create a network among a small group of notebook computers, for example, for file sharing or sharing an Internet connection, as shown in Figure 1.3.

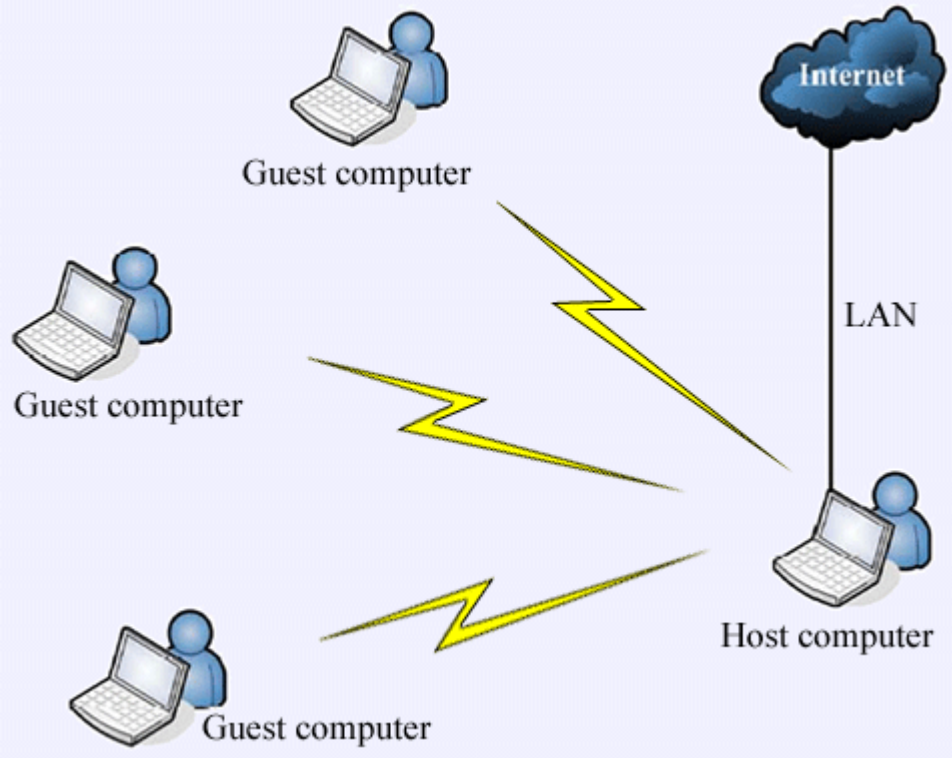

Fig. 1.3: An adhoc wireless network design

In the Activity 3 (Page 16), we will do this using *ad hoc* technology to temporarily create a Wi-Fi network that does not need other network devices such as routers and switches.

1.5.3.1 Activity 3

Complete 'Lab 5.2 – Creating a small network between notebook computers with *ad hoc* technology' from the textbook A Practical Approach to Internet Programming and Multimedia Technologies (Kwan, R, Tsang, P, Kwok, P, Koong, K, Mak, J and Wu, J (2009) A Practical Approach to Internet Programming and Multimedia Technologies, Hong Kong: Open University of Hong Kong Press.).

This exercise helps you learn how to make a connection between notebook computers directly through Wi-Fi, and to share the Internet connectivity among the users connected to the Wi-Fi network.

1.6 Wireless access to the Internet

The following sections introduce how wireless network access is implemented.

Basically, there are 3 ways of implementation, namely:

- Wi-Fi (Page 17)
- Hotspots (Page 18)
- WiMAX (Page 19)

1.6.1 Wi-Fi

Wi-Fi, also known as wireless broadband, wireless networking or wireless fidelity, simply means broadband without the wires. The advantage of small, portable devices such as laptops and PDAs is that they can be used anywhere around the house. But if you want to access the Internet on them as well, you'll need a Wi-Fi transmitter.

Wi-Fi has become very popular because once you have a base station, any number of desktop or laptop computers can be connected to your broadband service without the need for any cables or installing extra phone lines. So if you have a second computer in an upstairs room, or a laptop as well as a desktop, the same broadband service will be available on all your machines at the same time.

On the other hand, Wi-Fi is a trademark of the Wi-Fi Alliance for **certified products** based on the IEEE 802.11 standards.

Wi-Fi Certification

The Wi-Fi certification warrants interoperability between different wireless devices. In some countries the term Wi-Fi is often used by the public as a synonym for IEEE 802.11-wireless LAN (WLAN).

Not every IEEE 802.11 compliant device is certified by the Wi-Fi Alliance, which may be because of certification costs that must be paid for each certified device type. The lack of the Wi-Fi logo does not imply that a device is incompatible to certified Wi-Fi devices.

Wi-Fi is used by most personal computer operating systems, many video game consoles, laptops, smartphones, printers, and other peripherals.

1.6.2 Hotspots

A *hotspot* provides **wireless Internet access in public areas.** PDAs and laptops are usually the devices used to connect to hotspots.

Hotspots - natures and locations

Some hotspots are free and wide open, while others are free and secured. Yet other hotspots are subscription-based, pay-as-you-go, or a mixture of these.

Hotspots are found everywhere, from coffee shops to libraries to public parks.

It is important to remember that a hotspot is defined as a wireless network that is *intended to give* wireless Internet access either free or for a fee. There are many locations where you can connect to a wireless network, but many, if not most, of these are *inadvertently giving (Examples of these inadvertent networks include homes, businesses, and even government installations that are not properly secured.)* wireless Internet access.

Specialty devices have been created that can print receipts, authenticate users, and even disconnect users after time limits expire. These devices are often called hotspot gateways. There are many **business models** associated with the implementation of a hotspot.

Business models associated with hotspots

Following are a few examples business models associated with hotspots:

- ***Paid Access*** — This model profits from the fees for access to the Internet. This is very common today in airports, coffee shop, major shopping centres, etc..
- ***Traffic Generation*** — This model profits from the sales of items like coffee, books, music, and other items to the individual who come to the hotspot location for Internet access. The customers who patronize the shop will be provided a fixed-period of free or discounted access to wireless Internet connection.

1.6.3 WiMAX

Wireless MANs (metropolitan area networks) differ from wireless LANs and wireless PANs in that they are not usually implemented by the organization that wishes to use the network. Instead, they are generally implemented by a service provider, and then access to the network is leased by each subscribing organization. However, unlike with wireless WANs, this does not have to be the case. For example, 802.16 (http://en.wikipedia.org/wiki/IEEE_802.16) -compliant hardware could be purchased and frequency licenses could be acquired in order to implement a private wireless MAN, but the expense is usually prohibitive. WiMAX is the most commonly referenced wireless MAN technology.

WiMAX

In 2007, WiMAX solutions are just beginning to see production and installation. In fact, the first WiMAX Professional Certification training class was held in Hawaii, in January and February 2007.

WiMAX is based on the IEEE 802.16 standard (http://en.wikipedia.org/wiki/IEEE_802.16) and provides expected throughput of approximately 40 Mbps for fixed, line of sight connections and approximately 15 Mbps for mobile, non-line of sight connections. In addition to the throughput speeds, WiMAX incorporates QoS (http://en.wikipedia.org/wiki/Quality_of_service) mechanisms that help to provide greater throughput for all users and important applications using the network.

A **wireless Internet service provider (WISP)** is an Internet service provider (ISP) that is accessed using wireless technologies. WISPs often fulfil the need at the '**last mile**', which refers to the last section that must be spanned to reach remote customers. It can be very expensive and, without wireless, sometimes impractical. Sometimes these

WISPs lease bandwidth to businesses that require Internet access, but that are too far from DSL stations and have no other options.

Wireless technologies used by WISPs

WISPs may use IEEE 802.11 technologies for the entire delivery, or they may use other wireless technologies, like WiMAX (IEEE 802.16), from the operations centre to the delivery area and then use IEEE 802.11 technologies within the delivery area. Other WISPs use WiMAX all the way to the end destination, meaning it is then up to the subscriber whether to use IEEE 802.11 technologies within their house or business.

Since WiMAX and IEEE 802.11 use different frequencies (if the 802.11 devices use the 2.4 GHz spectrum), there should be no conflicts or interference.

Last-mile delivery

To help you understand last-mile delivery, consider the home where my friend grew up in West Virginia of the United States. They lived on a very old country road. It was not paved; it was a gravel road. They lived in the last house on the road, which was approximately 2.5 miles from the nearest paved road. They had to pay a large fee just to get electricity to the house. The electric company required such a fee since there were no other houses close to theirs.

This is an example of the problems related to last-mile delivery. It's no different for the Internet today than it was for electricity then. Wireless technologies provide an excellent solution to the problem of last-mile delivery of Internet access.

In Hong Kong, WiMAX's advantage of enabling last-mile deliveries to remote users economically may not be so convincing since the density of population is extremely high here, and ISPs have enough incentive to pave the last mile for nearly every household. But another strength of WiMAX that does apply to Hong Kong is that it can offer the last mile connection for those endpoints that are '**on the move**' (e.g. PDAs, notebooks, etc.) .

WiMAX's provision of last mile connection for mobile endpoints

As you might expect, this capability is well-received by local users, given the high popularity of handheld devices here. Currently, the wireless connections used by these handheld devices are mainly provided by the existing mobile networks. However, the throughput of the mobile networks, even 3G, can reach only a few mega bits per second, which is much lower than WiMAX (45Mbps). It is therefore foreseen that WiMax will have plenty of scope to develop in Hong Kong.

Please read the following material to learn more about 802.11 and 802.16 (WiMAX) Internet access:

Reading

Dean (2010) (Dean, T (2010) Network+ Guide to Networks, 5th edn, Thomson Course Technology.) 396–97.

Check if you have grasped the topics we have convered in this section by attempting Self-test 3 (Page 21). Remember, don't look at the Suggested answers to Self-test 3 (Page 21) before answering the questions.

In Hong Kong, the government has launched a programme to provide free wireless Internet access services to all citizens. Learn more about the programme by answering the questions in Activity 4 (Page 22) and reading the Feedback to Activity 4 (Page 22) afterwards.

1.6.3.1 Self-test 3

1. Which access technology(ies) is currently used to provide Internet access in wireless hot spots such as cafes and libraries?
2. What is the current status of WiMax development in Hong Kong? Do a desktop research on the Internet.

1.6.3.1.1 Suggested answers to Self-test 3

1. IEEE 802.11 (any of 802.11a, b or g).
2. In late 2008, OFTA issued Broadband Wireless Access licences to three local service providers, i.e. Genius Brand Ltd., CSL Ltd. And China Mobile Hong Kong Company Ltd. It is believed some of the providers will use WiMAX technology to deliver their wireless broadband service to the local community. The licensees will provide BWA services within five years from the date of the issue of the licenses.

1.6.3.2 Activity 4

The Government Wi-Fi Programme (GovWiFi) is one of the major initiatives under the 2008 Digital 21 Strategy to build Hong Kong into a wireless city. This programme aims to provide free wireless Internet access services to all citizens by installing Wi-Fi facilities at designated government premises. Its aims are as follows:

- People can surf the web freely for business, study, leisure or accessing government services whenever they visit the designated Government premises.
- Business organisations can extend their services to a wireless platform to reach and connect with their clients.
- ICT industry players can make use of this new wireless platform to develop and provide more Wi-Fi applications, products and supporting services to their clients, and open up more new business opportunities.
- Foreign visitors can enjoy Internet access at the designated tourist spots.

Visit GovWiFi (http://www.gov.hk/en/theme/wifi/program/index.htm) and answer the following questions:

1. How many government premises have been installed with Wi-Fi facilities?
2. What types of premises are included?
3. What kind of security protection is enabled?

1.6.3.2.1 Feedback to Activity 4

1. Around 350 premises, at June of 2009.
2. These premises include public libraries, public enquiry service centres, sports centres, cultural and recreational centres, cooked food markets and cooked food centres, job centres, community halls, large parks and Government joint-user buildings.
3. WPA2-Enterprise.

1.7 Wireless network security

Wireless communications are particularly susceptible to eavesdropping. For example, a hacker can search for unprotected wireless networks by driving around with a laptop configured to receive and capture wireless data transmission.

In this topic, therefore, we introduce to you some common protection mechanisms that apply to wireless networks. These include:

- Wired Equivalent Privacy (WEP)
- IEEE 802.11i (commonly known as "Wi-Fi Protected Access")

At the end of this section, you will have a lab activity in which you can capture and analyse some wireless LAN traffic.

1.7.1 WEP

By default, 802.11standard does not offer security, but it allows for optional encryption using WEP (Wired Equivalent Privacy). WEP uses keys both to authenticate network clients and to encrypt data in transit. When configuring WEP, you establish a character string required to associate with the AP, also known as the network key. When the client detects the presence of the AP, the user is prompted to provide a network key before the client can gain access to a network via the AP.

The early implementation of WEP allowed for 64-bit keys, which was not so secure. Current versions allows for 128-bit keys, which are relatively more secure. However, WEP's use of shared and static keys is still more susceptible to discovery than a dynamically generated, random, or single-use key, which is adopted by the WPA (Wi-Fi Protected Access) and will be introduced in the next section.

1.7.2 IEEE 802.11i and WPA

802.11i uses Extensible Authentication Protocol (EAP) (http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol) with strong encryption scheme and dynamically assigns every transmission its own key to heighten the protection of the data in transmit against taping or tampering. With 802.11i enabled, logging on to wireless network is more complex than with WEP.

WPA (Wi-Fi Protected Access) is a subset of 802.11i standard that is endorsed by the Wi-Fi Alliance, an international organization dedicated to ensuring the interoperability of 802.11-capable device.

Click this link to watch the video:
http://www.opentextbooks.org.hk/system/files/resource/10/10308/10341/media/video0001.mp4

In a wireless network secured with Wi-Fi Protected Access, the AP acts as proxy between a remote access server and station until the station has successfully authenticated with the remote access server. It requires mutual authentication — the station authenticates with the remote access server, and vice versa. After authentication, remote access server instructs AP to allow traffic from the client into network. Following that, the client and server agree on an encryption key for subsequent data transmission.

WPA2 is an updated version that has already gained wide support by commercial products.

Read the following material to learn more about wireless network security:

Reading

Dean (2010) (Dean, T (2010) Network+ Guide to Networks, 5th edn, Thomson Course Technology.) 611–14.

Now, attempt Self-test 4 (Page 24) to see if you have grasped the topics covered. After that, check your answers against the Suggested answers to Self-test 4 (Page 24).

1.7.2.1 Self-test 4

1. Let's say you are designing an 802.11g wireless network for a local cafe. You want the wireless network to be available to the cafe's customers, but not to anyone with a wireless NIC who happens to be in the vicinity. Which security measures would require customers to enter a network key to gain access to your network via the access point?
2. What is the main difference between WPA and WEP?

1.7.2.1.1 Suggested answers to Self-test 4

1. WEP
2. WPA dynamically assigns every transmission its own key to heighten the protection of the data in transmit against taping or tampering, while WEP uses a static key for all transmissions.

1.7.3 A lab on wireless network security

Network analysis (also known as traffic analysis, protocol analysis, packet analysis, packet sniffing and so on) is the process of capturing network traffic and examining it closely in order to deduce information from it. A packet sniffer (also known as a network analyser, protocol analyser or network protocol analyser) is a hardware device or software that captures, records and analyses network traffic. Network analysis can be used for both **good** and **evil**.

Proper uses of network analysis

A network administrator performs network analysis to monitor network usage, analyse network problems and debug client/server communications.

A network security practitioner performs network analysis to detect network intrusion attempts and violations against network usage policies.

Improper uses of network analysis

Hackers perform network analysis to gain information for effecting network intrusion and other unauthorized (and often illegal) activities.

An engineer (or a student like you) can also use network analysis to investigate, study and reverse engineer protocols used over the network.

In the Activity 5 (Page 25) you will use a powerful and free packet sniffer, Wireshark (https://www.wireshark.org/), to capture and analyse the traffic between your PC and selected remote hosts on the Internet. In addition, you will use a wireless networking tool, NetStumbler (http://www.netstumbler.com/), to detect the wireless LANs in your neighbourhood. You will be surprised that many people are not running their wireless LANs in secure mode and hence are vulnerable to wireless sniffing.

1.7.3.1 Activity 5

Complete the 'Lab 1.5 — Network Traffic Analysis and Wireless Network Security' from the textbook A Practical Approach to Internet Programming and Multimedia Technologies (Kwan, R, Tsang, P, Kwok, P, Koong, K, Mak, J and Wu, J (2009) A Practical Approach to Internet Programming and Multimedia Technologies, Hong Kong: Open University of Hong Kong Press.). This exercise will help you realize how easy it is to

intercept and analyse the data transmitted in networks and how to protect a wireless network.

1.8 References

Below are the resources referred to or cited by the developer(s) of the original unit:

Carpenter, T (2008) CWNA — *Certified Wireless Network Administrator Official Study Guide*, 4th edn, New York: McGraw Hill.

Dean, T (2010) *Network+ Guide to Networks*, 5th edn, Thomson Course Technology.

Kwan, R, Tsang, P, Kwok, P, Koong, K, Mak, J and Wu, J (2009) *A Practical Approach to Internet Programming and Multimedia Technologies*, Hong Kong: Open University of Hong Kong Press.

1.9 Conclusion

In this module you looked into a number of fundamental concepts and issues surrounding wireless LAN technologies.

We began by discussing the wireless LAN technologies that fall under the IEEE 802.11 series, including 802.11 a, b, g and, the latest member, n. After that, we covered Bluetooth and Infrared (IR), which are in common use for connecting peripherals to the main computer unit.

Next was a topic concerned with wireless LAN design. We concluded this part with a lab aimed at setting up an *ad hoc* wireless network. The Internet has become a mainstream use of the wireless network technologies. In addition to Wi-Fi, we also discussed WiMAX, an upcoming wireless broadband access technology, and made a brief note of the local development of the wireless broadband access service provisioning.

You then learned how network security is a very important topic that can't be separated from wireless communications, simply because of the plain fact that a signal transmitted over the air can be intercepted by anyone, including those with malicious intentions.

If you would like to learn more on this subject, you are welcome to enrol in *ELEC S212 Network Programming and Design (http://www.ouhk.edu.hk/wcsprd/Satellite?pagename=OUHK/tcGenericPage2010&c=C_ETPU&cid=191154024000&lang=eng&pri=2)* offered by the School of Science and Technology (http://www.ouhk.edu.hk/wcsprd/Satellite?pagename=OUHK/tcSubWeb&l=C_ST&lid=191133000200&lang=eng) of the OUHK.

1.10 Glossary

access point— A device used on wireless LANs that transmits and receives wireless signals to and from multiple nodes and retransmits them to the rest of the network segment. Access can connect a group of nodes with a network or two networks with each other. They may use direction or omni-directional antennas.

AP — See Access Point

bit — Binary digit in the binary numbering system. Its value can be 0 or 1. In an 8-bit character scheme, it takes eight bits to make a byte of data.

broadband — Sometimes also referred to as wideband. It's a term describing any network that allows multiple signals to be transmitted on a single cable at the same time. Different frequencies of electromagnetic waves are used to encode the signals, and transmissions do not interfere with each other. In LAN terminology, broadband refers to a system in which multiple channels access a medium, for example coaxial cable (http://en.wikipedia.org/wiki/Coaxial_cable), that has a large bandwidth using Radio Frenquency (RF) (http://en.wikipedia.org/wiki/Radio_frequency). This may allow the coaxial cable to carry multiple separate LANs whose transmission is being modulated at different frequencies. In cable television (CATV), broadband describes the ability to carry 30 or more TV channels and is synonymous with wideband.

CSMA/CD — Carrier Sense Multiple Access/Collision Detect, a common Ethernet protocol.

Ethernet — A network protocol invented by Xerox Corporation (http://en.wikipedia.org/wiki/Xerox) and developed jointly by Xerox, Intel (http://en.wikipedia.org/wiki/Intel) and Digital Equipment Corporation (http://en.wikipedia.org/wiki/Digital_Equipment_Corporation). Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps.

frame — A term for the unit of data transferred on a network; its size depends on the type of network implemented, hundreds or thousands of bytes long (any particular type of network will have a limit on the frame size, e.g. Ethernet 1500-byte limit). The terms cell, datagram, message, packet, and segment are also used to describe logical information groupings at various layers of the OSI reference model (http://en.wikipedia.org/wiki/OSI_model).

Hotspot — A hotspot is a physical location that offers internet access over a wireless LAN through the use of a shared internet connection and a single router. Hotspots can typically be found in coffee shops and various other public establishments throughout a city.

Internet — A global network of networks used to exchange information using the TCP/IP protocol. It allows for electronic mail and the accessing and retrieval of information from remote sources.

LAN — See Local Area Network.

Local Area Network — A network connecting computers in a relatively small area such as a building.

Mbps — Megabit per second.

Megabit — One million bits.

node — End point of a network connection. Nodes include any device attached to a network such as file servers, printers, or workstations.

point-to-point — A direct link between two objects in a network.

protocol — A formal description of a set of rules and conventions that govern how devices on a network exchange information.

WLAN — A short form of wireless LAN.