UNIT 16 FUTURISTIC LOOK OF COMMUNICATION SYSTEMS

Structure

16.1 INTRODUCTION

This last unit gives you a peek into the future of communication technology. You will see a glimpse of the exciting new work that is going on in this field and some of the new technological trends that are being adopted in this area. Quite a bit of this is already available, some of it commercially. So we will look at things that have been technologically proven, more or less, but whose business success might not be clear yet. These technologies have been adopted by a large number of users and many companies are engaged in research in these areas. Several products have been launched and have found favour with users.

The *killer app* in the realm of mobile telephony has been the **Short Message Service** (SMS). Its popularity is comparable to the use of e-mail over the Internet. It has many of the advantages of e-mail. It started off as a service that allowed a person with a mobile phone to send a short text message of about 750 characters to another person with a mobile phone. Later there emerged Internet websites that allow you to send an SMS message to a mobile phone Like e-mail, an SMS message can be replied to or forwarded on to another phone. It has the advantage of being asynchronous, and the receiver can look at the message at leisure. Even if the phone is off or out of range, the service mechanism ensures that the message is delivered later, when the recipient's phone is on or available again. There is now a demand for SMS over fixed lines phones as well, and some providers have already started supporting the service.

Radio Frequency Identification (RFID) tags are small chips that emit a signal over a radio frequency. Each chip has a unique number that can be ascertained by a receiver of the signal. They are very useful in tagging assets in a company or items for sale in a store. They have several advantages over conventional bar coding. First, they are active and no specific action is required to find out the identity of the asset. Secondly, in addition to the asset type, they can also contain information that can identify the asset uniquely. With increasing usage, their costs are coming down to very affordable levels.

If we look at the history of computing, the biggest change after the personal computer revolution has been the advent of computer networks. People realised that expensive resources could be shared by several people, thereby improving utilisation and bringing down the average cost for each user. This way, resources that were out of reach of all but large, affluent organisations, soon became available to smaller ones. These included peripherals such as high quality printers and scanners.

Then came the Internet, which brought large parts of the world together into one big network. The World Wide Web has now become the newest means of mass communication. It grew from infancy to becoming an essential part of modern life within a decade. You are already familiar with the technologies involved in bringing this about.

In this unit we will see the direction in which networks are growing and are tending to branch out. There are three major leaps or evolutionary paths that we can see after the World Wide Web, each of which liberates devices from some constraint.

- Networks are evolving to accommodate mobile devices like laptops, handheld computers and mobile phones. Devices are breaking free from the constraints of being fixed and of being limited to wire based communication.
- Networks are evolving to liberate devices from the tyranny of wires. Today a computer set up is a maze of wires – a cable to connect to the printer, another for the scanner, yet another for the handheld.
- Networks are evolving from a client/server model to a peer to peer model that has several advantages. This frees up a large amount of computing resources to contribute to the network – today these resources are provided only by a comparatively small number of servers.

Each of these evolutionary directions is addressed by a different set of technologies and protocols. These are:

- The Wireless Application Protocol (WAP) for mobile devices which freed the devices from fixed IP address;
- Bluetooth for connecting peripherals without wires; and
- Peer to Peer (P2P) networking protocols which allow even distribution of computing power and network traffic.

Each of these is complementary to the others, and brings more power to computers and computing devices. We take an overview of WAP in Sec.16.2. We also look at the architecture of WAP in some detail and go on to discuss WAP applications and entities required to implement them. Sec. 16.3 gives details about Bluetooth technology – its method of communication, design criteria and application. Sec.16.4 looks at peer to peer networking. Here we discuss the architecture of some common P2P standards and its applications. We end this Unit by discussing the influences of advances in communication technology on our society in Sec.16.5

Objectives

After studying this unit, you should be able to:

- envisage the directions in which computer networks of the future could evolve and the factors that lead to those directions;
- describe the basic architecture of the Wireless Application Protocol and some of its applications;
- explain the basic concepts of Bluetooth technology and its possible uses;

- enumerate the basic features of a peer to peer Networking architecture, called JXTA, introduced by Sun Microsystems; and
- discuss the pros and cons of technological development in the field of communication.

16.2 WIRELESS APPLICATION PROTOCOL

For long, computers had been large, fixed devices. Even the advent of personal computers did not change this situation materially since computers were still bulky enough to require a fixed location. The advent of laptop computers started to change this. These could be carried around by a user and provided several advantages as a consequence. New challenges emerged even as old problems got solved. For example, mobility of a computer meant that it could no longer have a fixed Internet Protocol address. It had to take on the IP address provided by whatever network it had to plug in to.

The coming of cell phones, palm tops and personal communicators brought mobile computing into focus. The older communication protocols that relied on fairly large computing power available on a host could not cater to a situation where a mobile phone had only a few kilobytes of memory and a minute controller as a CPU. This marked the advent of wireless data communication in a big way. The Wireless Application Protocol (WAP) was invented to take care of this situation.

WAP was created by the WAP forum which was formed in 1997 by leading mobile phone companies to provide Internet access from the devices. The idea was not just to be able to browse static content, but to be able to interactively transact business while on the move. It also gave birth to new ideas such as location based services. Since a cell phone service providers know approximately where you are, they could send out location specific information to you. This could be on restaurants or entertainment opportunities in the vicinity. Mobile phones can also be used for security – children and the elderly are a case in point. For example, mobile phones integrated with a global positioning system (GPS) device can be used to determine the exact coordinates of a person on the earth. If a child or elderly person is in trouble (because s/he is lost or is the victim of a crime) s/he can use the phone to call the police who will be able to determine her/his exact location and intervene much quicker than they could otherwise.

SAQ 1

How do mobile computing devices differ from conventional, fixed computers?

Spend 2 Min.

16.2.1 Overview of WAP

WAP was designed for devices with low computing power and with low bandwidth connections to the Internet. Also the protocols used in the web were kept in mind. WAP also uses a client-server paradigm. However, since the web uses HTTP, you need to have what is called a WAP gateway, which translates between the HTTP and WAP. So a phone connects over WAP to the gateway, which translates the request to HTTP and passes it on to the original webserver and a reverse translation occurs when the response comes back. This is how the mobile phone is able to access the Internet. The gateway is set up and maintained by the service provider.

How does the phone initiate a service request in the first place? If you guessed that there is some sort of a browser on the phone, you are right! Such a browser is called a WAP browser or a microbrowser. It has to take into account the very limited screen size, possible lack of colour screens, difficulties in accepting input and navigating and other constraints imposed by the phone. So you should not expect to be able to see a website the same way as you do on a PC. In fact there are emulators available that will let you see a website on a PC the way it would be seen by a particular phone using WAP. These are useful for designing the websites.

Some websites are designed with mobile users in mind. They can tailor their response to the device, PC or WAP. This is possible because the Markup language used with WAP is Wireless Markup Language (WML), based on Extensible Markup Language (XML). Such an implementation is better than relying entirely on the WAP gateway to do the translation because the results are often less than scintillating. A WAP gateway will also need to be able to bill users. This can be done because it has information on the phone that connected to it and all other details about the session.

The WAP users would want rapid responses because of the comparatively higher cost of airtime as opposed to a cable or dial-up Internet connection from a PC. They would also be less tolerant of errors because of the difficulties involved in navigation. Most mobile phones do not have keyboards or pointing devices (though some of the newer models have keyboards) and even when using a communicator, the size of the keys is usually too small to type comfortably. Moreover, mobile devices might need to be used while standing or walking – the user might not be able to sit at a desk. So it is important to have a quick and reliable connection. A "page not found" error is likely to exasperate a mobile users and they might just give up on the attempt to browse the site. What would be a mere irritant to the PC users can be a problem for the mobile users.

16.2.2 Uses of WAP

Though we talk here mainly in the context of mobile phones, the uses of WAP are not limited to them. It can be applied to any mobile device such as a handheld computer or a Personal Digital Assistant (PDA) that is compliant with the protocol. The WAP specifications do not make any assumptions about the client device.

A WAP portal is like a portal in the computer world. It serves as a gateway to several destination sites. These sites could be simply informative, but it is more likely that these would be interactive sites that allow the user to transact while on the move. If the user only wanted to see a website, s/he is likely to do it on a PC! A user will perhaps use the Internet only when s/he wants to do something immediately and cannot wait to get to office or home. Portals can be very useful in the WAP context because you do not have to know all the sites you want to access – they are conveniently available to you from one place. Also you will want to try and avoid having to enter a complete URL from your WAP client because you want to minimise input. Sites would be stored as bookmarks or accessed from your portal.

WAP sites can provide services such as those needed by a traveller - hotel bookings and flight timings. They could allow buying and selling of goods, participation in trading and on-line auctions as well as ordering services like taxis. You could also perform banking transactions that you are not able to postpone and need to do immediately. News and entertainment information are also well suited for WAP users. Services based on the current location of a person are also good candidates for WAP application.

Because of the limitations of the client devices, there are many challenges in designing good WAP applications. You cannot rely on the availability of colour (though colour screens on mobile phones are now becoming common), sound or images, let alone video or animation. Also it is hard to navigate as there is no mouse or other pointing device. Entry of data is tough because there is no keyboard.

Electronic mail gains in reach and is one of the central applications that will be used from a mobile device. Though it might be difficult to send more than a short reply, users will want the flexibility of being able to read their mail on the move. However, it might not be possible to read attachments or long messages. Also elaborate graphics cannot be shown on the devices. The same holds good for messenger services.

Here you might be thinking of the highly popular Short Message Service (SMS). This does not use WAP. But there are services on offer that allow you to send SMS messages from a PC using the Internet to a mobile phone. These are especially convenient if you want to communicate with a mobile phone in a distant country and your phone company does not support SMS to that country.

SAQ 2

What is a WAP portal?

Spend 3 *Min.*

16.2.3 WAP Architecture

Let us now take a look at the architecture of WAP and see the constituents of the WAP protocol stack. We first look at WAP version 1.1 and later we will see the changes introduced by WAP 2.0. The stack consists of five layers as shown in Fig. 16.1. Each layer provides a service to the layer above it and makes use of services provided by lower layers. A higher layer does not need to know anything about the internals of the layers below it. You are already familiar with the 7-layer OSI model, which is similar to this.

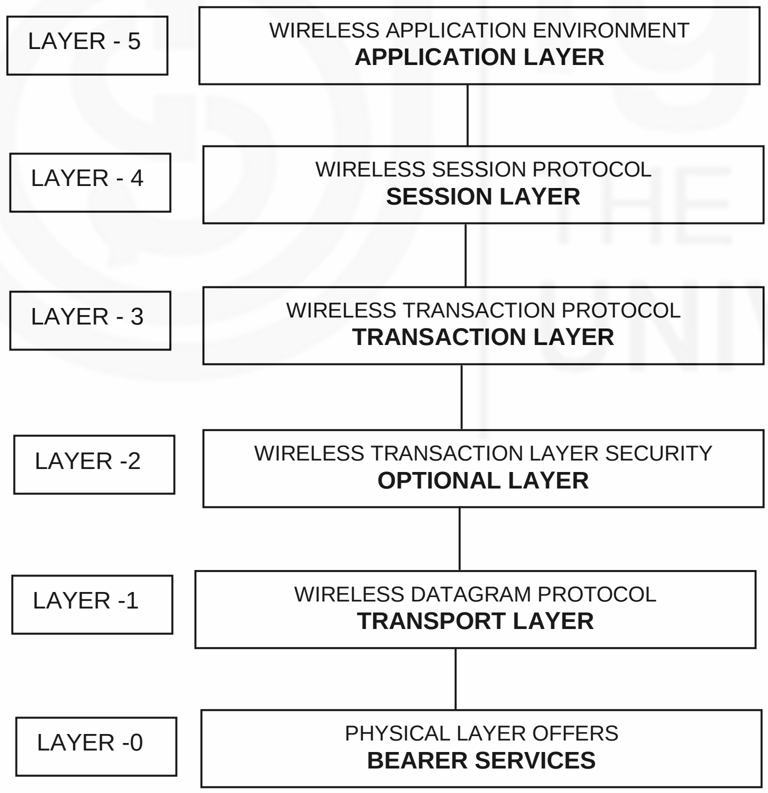

Fig. 16.1: WAP layers

These 5 layers are on top of the physical medium (indicated by 0^{th} layer) and the technologies and protocols used for the actual transmission. For example, the underlying data transfer could be done using a GSM or a CDMA phone or any other

A *lightweight protocol* means the one that is not computationally intensive or is otherwise simple. WAP can be used by slow networks and is less complex than TCP/IP-the protocol used over the Internet.

bearer. The mechanism used here does not affect the WAP stack. This is in keeping with the layered approach.

A feature of the WAP design is that it is lightweight. This is necessary because it is meant for networks that have low bandwidth and hence low data transfer rates. Also the latency in the networks is fairly high as compared to the wired Internet. That was the motivation for the development of WAP in the first place.

a. Wireless Application Environment (WAE) Layer

The top layer of the WAP stack is the WAE or the Wireless Application Environment layer. This is the layer with which application developers will interact. Also an application executes at this layer. So this layer has all the building blocks needed to create and run applications. Depending on the specific device in use, the developer will design and build the application. A WAP client has two user agents – a WAE user agent and a WTA (Wireless Telephony Application) user agent. A user agent is software or functionality that is available on the mobile device, that is, to the user. A typical wireless application environment is shown in Fig. 16.2.

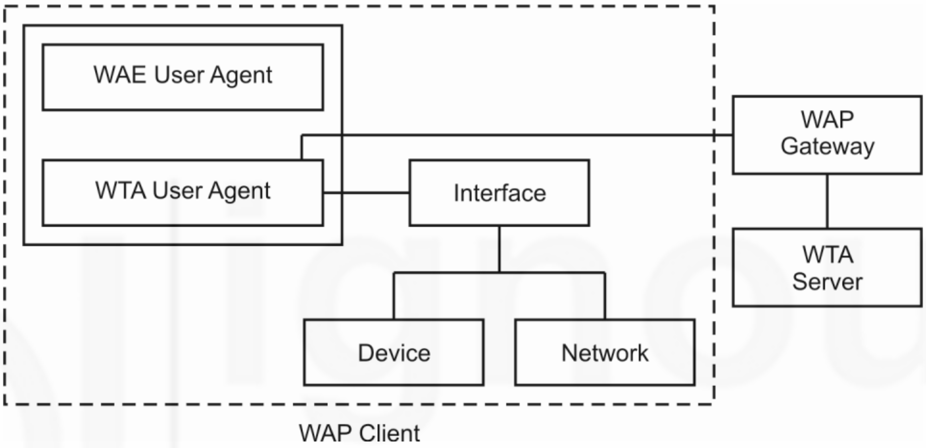

Fig. 16.2: Wireless application environment

The WAE user agent consists of facilities such as the editor used for editing text messages. The microbrowser is also a part of the WAE. As mentioned earlier, the WAE specifications do not make any assumptions about the actual client device being used. They only talk of things like formats of images or text that the user agent must support. These formats were designed with the specific aim of being able to display content on devices that have only rudimentary capabilities.

The WTA user agent was defined as a part of the WAP version 1.1 specifications. However no implementations were available on practical devices at the time. The basic idea here is to allow the functionality of the mobile device to be used from the Internet. This is the converse of using the Internet from the mobile device. For example, it would be possible to change phone settings from the Internet, or to add an entry into the phone book of a particular cell phone. Such features can be provided by having the WTA user agent on the mobile client device interact with the WTA server located on the wireless network. The client device and the network functionality work together using a WTA interface (WTAI). Network functionality includes capabilities that use the network, such as the ability to make or receive a call.

Apart from WTA, the WAE includes a markup language called Wireless Markup Language (WML). This is akin to HTML but is much more lightweight. Its main thrust is on displaying text. The content is specified by WML and a lot of the rendering decisions are left to the microbrowser. This is unlike the current state in PCs, where the browser has a more limited role to play in the rendering decisions since most of the actual display is already specified by the HTML code itself. A WML document consists of several *cards*. Each card is displayed on one screen and the entire set of cards is called a *deck*.

There is also a lightweight scripting language called WMLScript. It is based on JavaScript and is useful in preventing unnecessary connections to the server. This is done by providing the client device with local intelligence in the form of the ability to validate user input and being able to perform some limited calculations through the use of libraries. This saves the server from having to deal with invalid data and also saves the client from making connections to the server for every little computation. It can also display error messages and make use of local data such as addresses from the client device.

b. Wireless Session Layer (WSL)

This is the fourth layer in the WAP stack that is just below the application layer. It allows data to be exchanged in the form of sessions, thereby providing an organisation to the whole set of transmit sessions. It serves to group data exchange into a single related entity. The layer provides several primitives that can be exchanged between client and server. Each of them is a request for some facility and goes towards providing a service.

Sessions can be connection oriented or connectionless, just as in TCP/IP. Connection oriented sessions allow data to be exchanged in a reliable manner. They use the third layer of the WAP stack, the Wireless Transaction Layer that is described below. Such a session can be abandoned temporarily if the quality of the transmission becomes particularly poor. It can then be restarted later on. In a typical connection oriented session, a client begins by sending a connect primitive to the server. This requests the creation of a connection between them. This primitive requires the sending of various parameters, for example, the server address. The other services that are asked for can be then provided by the server in a confirmed or unconfirmed manner.

A *primitive* is a command that is directly understood by a device. It does not have to be broken down into any simpler instructions.

In a confirmed service, the server is notified by the client that it has received the data. Here the client sends the server a request primitive, at which the server sends a confirm primitive to the client. The server then sends a response primitive and receives an indication primitive from the client. This is not done in an unconfirmed service. In that case the server sends only indication primitives while clients send only request primitives.

The protocol is actually similar to the Hyper Text Transfer Protocol (HTTP), but with all transmission being in binary. You may wonder, what is meant by binary transmission. We are here looking at phenomena at different levels of abstraction. At higher levels we abstract away the details and complexities of the lower levels. Fundamentally, all transmission is by electromagnetic signals that ultimately have an analog waveform. What we call digital transmission is really an analog transmission of pulse trains with a waveform such that they have more or less only two significant amplitudes that we interpret as 0s or 1s. So at the physical level all transmission is always binary. But when we organise the bits into octates (bytes) and then into packets in keeping with a protocol specification, we begin to assign meaning to the bit stream. The ASCII code is commonly used to assign alphabetic or numeric symbols to certain combinations of bits. The TCP/IP protocol suite specifies packets in terms of the contents of octets. On the other hand, WAP specifies packet organisation in terms of bits only. This allows transmission to occur with lower overhead because fewer bits are required to describe packet information. This is required to keep the protocol lightweight, in tune with the characteristics of the medium that has low bandwidth, poor Signal to Noise ratio and high delay or latency. It can also be used to obtain information on the client so that the data can be formatted to suit the user agent the client runs.

c. Wireless Transaction Layer (WTL)

This is the third layer of the WAP stack, just below the Wireless Session Layer (WSL). It provides transaction services to the WSL. These can be reliable or unreliable requests. The former can also be accompanied by a result message. A reliable transaction consists of a message followed by an acknowledgement from the recipient. An unreliable transaction is completed simply by the transmission of a request to the user agent or the content server depending on who the initiator is.

In reliable transaction an acknowledgement can be transmitted back by the responding machine for some time if required by the originator. A reliable transaction with a result message has three data exchanges. First, the originator sends a request to the responding machine. This sends a result back to the originator. The sending of the result is an implicit acknowledgement of having received the request, as otherwise the result would not have been sent. The originator then sends an acknowledgement back to the responder, confirming having received the result.

d. Wireless Transaction Layer Security (WTLS)

SSL is a protocol developed by Netscape Communication Corporation to provide security and privacy over the Internet. It is application independent allowing protocols like HTTP, FTP and Telnet to be layered on top of it.

This is the second layer in the WAP stack and is the only optional layer. It is not a part of the WAP architecture and is invoked only when required. The wired Internet has been plagued by security issues and many horror stories of security breaches and consequential losses and damage are to be heard. If present, this layer operates over the first layer – Wireless Datagram Protocol. The WTLS layer is based on the Secure Sockets Layer (SLL) Protocol. Security is as important in WAP as on the Internet because of the ease with which wireless transmissions can be intercepted and read. If mobile devices are to be promoted as convenient and always available, this assurance must come with the assurance of at least the same level of security as is provided by the Internet.

Just like the other layers in WAP, this layer is also designed to be lightweight and to deliver the functionality of SSL within the bandwidth limitations and high latency of current wireless transmissions. As in any secure transmission, the use of SSL in this layer ensures that,

- Only authorised clients have access to the server. This is enforced using a password mechanism.
- Servers can be authenticated to be what they claim they are. It is not unknown for spurious servers to come up, claiming to provide services – thereby gathering data about clients and unsuspecting users. This authentication could be done using a certificate mechanism.
- Data cannot be altered during transmission without the fact being detected. This is necessary to safeguard against the transmission being read and altered, and the receiver getting only the doctored version of the transmission.
- Finally the basic premise is that the data cannot be read, at least not easily, even if it is intercepted. Encryption of the transmission from end to end is required to ensure this. Privacy of the transmission is thus assured.

When a mobile device initiates a connection to the server, the WAP gateway and the device communicate using WTLS, and the WAP gateway and the server communicate using SSL. The translation between WTLS and SSL occurs in the memory of the WAP gateway. The plaintext transmission is not stored anywhere on the gateway.

e. Wireless Datagram Protocol (WDP)

The Wireless Datagram Protocol is the first layer of the WAP stack. This is the layer responsible for providing much of the portability and bearer channel independence that the upper layers are able to use. It encapsulates the physical data being transmitted into packets that are then sent as units and shield the upper layers from the physical layer.

At the lowest level is the physical layer or the bearer channel that could use any of a variety of communication technologies.

SAQ 3

Spend
2 *Min.*

Why is security important in WAP?

16.2.4 WAP Constituents and Applications

An important constituent of a WAP application in use is a WAP gateway that translates between Internet protocols and WAP. This is depicted in Fig. 16.3. Apart from the protocols being different, WAP uses WML and WMLScript for application coding, which are suitable for the low resource devices typically used in WAP.

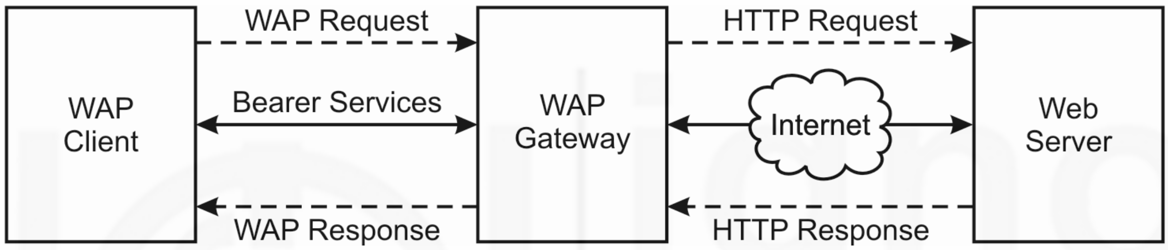

Fig. 16.3: WAP Gateway

The underlying consideration in the design of WAP is that it caters to low transmission speed networks that have high latency. So the protocols are lightweight. This is in contrast to the Internet protocols that assume much better networks and hence lay great stress on ensuring that correct data is transmitted. They are therefore able to take the higher overhead necessitated by the larger number of retransmissions.

Also the Internet protocols were designed for an environment where packets could arrive by different routes and therefore could arrive out of sequence. This problem does not exist in the world of WAP because the protocol applies only as the packets travel from the mobile device to the server. This path is only one hop and multiple routes are not possible. As a result the protocols are amenable to simplification.

WAP portals are a good way of visiting useful sites easily as one does not have to type in long URLs or even remember them. Also your provider is likely to connect you by default to a portal as soon as you initiate a connection.

The version 1.2 of WAP introduced the concept of **push technology**. Here a client receives content from the server without having made any request for it – the content is *pushed* to the client by the server. This would be required for many location based services that would send content based on the client location even though the client might not have asked for any. While this would certainly mean more traffic on the network, it would not really increase the latency as the push to the clients could be designed to take current network conditions into account. The push could be performed only when regular network traffic conditions are suitable.

After discussing the WAP which facilitates net connectivity of mobile devices, let us now take a brief overview of Bluetooth technology which helps in ridding the devices of wire connections.

16.3 BLUETOOTH TECHNOLOGY

The back of a computer can quickly become obfuscated by a maze of wires that connect it to various devices such as printers or a handheld. Bluetooth is a technology that allows computing and other electronic devices to be interconnected across short distances without the need for wires. This opens up exciting possibilities for applications such as exchanging files or distributing content across devices in localised areas, analogous to closed circuit television.

This technology was invented in 1994 by L.M. Ericsson of Sweden. It is named after a 10^{th} century Danish king whose name in English was Harold Bluetooth. He united a number of warring factions in Europe in his time in the Nordic regions. Bluetooth allows electronic devices to communicate with one another over short distances without any need for wires. It thus unites the devices just as the king united the kingdoms. This also opens up several possibilities for exciting applications.

16.3.1 Connecting Devices with Wires

The electronic devices of today, even those that we use everyday in our homes, have several components that need to be connected together in order to work. For example, a television set that we use as the screen for a DVD player has to be connected to it using some sort of cable. The DVD player itself will be connected by wires to a set of speakers depending on how sophisticated the sound system is. Each of them will have to be controlled independently – the DVD player for playing the intended video clipping properly and the TV set for the picture and sound settings.

The problem becomes more pronounced as we deal with more complex machines. A typical personal computer has several devices such as speakers, keyboard, printer, scanner, mouse and so on attached to it by wires. These often appear as a maze and the problem really manifests itself when we try to change a device or to unplug it.

Apart from the physical cables that are present, connecting up devices correctly can be a difficult task, especially for the layman. Fortunately, the cables are often all different, with different specifications and connectors, and often will only go into the correct points. But if there is any ambiguity about where a connector can fit in, you can have trouble. Limited lengths of connector cables also sometimes pose problems and one has to take resort to extension cords etc.

Moreover, these cables allow the devices to communicate using a variety of methods such as serial or parallel data transfer and a large number of protocols that are specific to the devices. The protocols are needed to ensure that the data sent has the same meaning to the sender and receiver.

16.3.2 Connecting Devices without Wires

There are ways of having devices communicate without having to use wires. One of these is to use infrared communication. This is the method used in most remote controlled electronic devices such as radios, air conditioners, television sets and stereos. There is a standard promoted by the Infrared Data Association for allowing computers to communicate with devices such as handheld computers, PDAs and mobile phones.

One characteristic of infrared communication is that it is line of sight, which is why you have to point your remote at your TV for it to work. You cannot control your TV through the walls from another room. This characteristic is also advantageous because it means that devices cannot easily interfere with one another if they are communicating using infrared.

Another feature of infrared is that you cannot have broadcast. Devices communicate with each other one on one. So even if you have several such devices close together you are not faced with the problem of interference between them.

The second way devices can communicate is by using radio waves. This obviates some of the problems of infrared. Radio communication is by nature in broadcast mode. It is not line of sight and is omni-directional. But these very same features come with some challenges. For one, in infrared there is no problem with interference between devices, while in radio communication it can be an issue. Secondly, when trying to connect up diverse devices together, they need to agree on a common protocol so that they can communicate.

16.3.3 Elements of Bluetooth

Bluetooth technology is meant to solve the problems of connecting devices together without the need for wires using radio transmission. Every device that is Bluetooth compliant would have a small radio transceiver that allows it to communicate by radio. Let us see how the difficulties faced in case of devices connected with wire are taken care of by Bluetooth.

Automatic Communication

Bluetooth uses the concept of a *piconet* or a *Personal Area Network* (PAN). This is a network of devices in a small area, within the range of the device radio. You do not have to do anything in order to get the devices to communicate. Whenever they come within range, the devices strike up a conversation automatically. In the course of this dialog they exchange information on whether they have anything to communicate to one another. A PAN would usually be confined to a house or room but it can be a very small distance, such as between a cell phone and a hands-free kit.

If you wonder how they can converse, it is because all Bluetooth devices use a common, agreed upon protocol. Any device can communicate with any other kind of Bluetooth device. This is because of agreement among companies and manufacturers. Currently the Bluetooth Special Interest Group (SIG) consists of over 3400 organisations, so that the standard is quite widely accepted.

Each type of device has an address that falls within an agreed upon range. A device knows what other devices it can communicate with, so that there is no conversation if the devices are not meant to be connected together. For example, a television set and cell phone will not interfere with each other. If you have a room with a PC and its peripherals, these will begin to communicate because the peripherals are meant to be attached to the PC. The cell phone in the room will be talking to the headset you wear on your head as a hands-free attachment. The television set will be able to talk to its remote and to the DVD player that it is meant to connect with. And if you have a cordless telephone set in the room, its base unit and handset will also be communicating with each other. But the base unit will not be trying to communicate with the DVD player, for instance.

How does this happen? The TV remote has an address and it knows which address range it has to try to communicate with. The TV and its remote both emit signals that enable them to recognise each other. Since the DVD player does not fall into the given address range, the TV remote will not try to send data to the DVD player.

Likewise the cell phone and its hands-free accessories know that they have to work together. Bluetooth device addresses are 12 digit hexadecimal numbers (48-bits), such as 00:04:76:b6:ba:9d.

So in the example that we have just taken, you have five piconets in the room – the TV and its remote, the DVD player and its remote, the PC and its peripherals, the cell phone and its hands-free kit and the cordless phone and its base unit. Let us now see how all of these are able to live together in the same room without confusing one another.

Spend
1 *Min.*

SAQ 4

How do you make devices in a PAN communicate?

Preventing Interference

Why does your TV remote kept in the drawing room not affect the TV set in your bedroom a few feet away? You must also be asking yourself why it does not affect the TV set in your neighbour's house. The standard was designed to take care of just these issues. First of all, the strength of the signals used by Bluetooth is quite low. The power of the transmitter is 1 mW, which is about a thousand times less than that of a typical cell phone.

The low power of the devices ensures that their range of communication is limited to about 10 m only. So they can talk to one another within, say a room or a section of a house or office. But they cannot affect other devices a long way off. This way, different piconets will not interfere with one another when they are not too near.

But what about devices those are in close proximity? Bluetooth devices communicate over the radio frequency spectrum from 2400 MHz to 2497 MHZ. This band has been set aside by international agreement for Industrial, Scientific and Medical devices (ISM). For example, most cordless phones make use of this band for communicating between the base unit and the handset.

Now besides the low power of the signals, another method used by Bluetooth technology is to randomly hop frequencies in the given band. So the devices in a piconet keep changing their frequencies from within a predetermined range (79 channels of 1 MHz in the US and Europe and 23 channels in Japan). This happens quite rapidly – about 1600 times a second. All devices in a piconet jump frequencies together so that they can continue to communicate. This synchronisation is controlled by the master device. Because of the combination of these two factors, the low power and the changing frequency of communication, two nearby piconets are extremely unlikely to interfere with each other. If by any chance they do happen to interfere because both are using the same frequency at the same time, the period for which the interference occurs will be very small. They will interfere only during one time slot of 625 microseconds after which both will change their frequencies again. The protocol provides for mechanisms to take care of such slots in which communication could not occur. The erroneous data that might have been received will be detected and discarded by the software and the data is requested again from the sender.

However, if there is an area that has a really high density of devices, there can be difficulties in communication and in their being able to work properly.

Some Bluetooth Specifics

There are two modes in Bluetooth transmission – synchronous and asynchronous. The former is given 3 reserved slots in every piconet. It is a connection oriented mode while the latter is connectionless. The reserved slots are set up by the master of the piconet to prevent collisions of data packets. There can be from 1 to 7 slaves in the network, of which 3 can use synchronous transmission.

In the asynchronous mode, the slaves transmit only when asked to do so by the master device. Communication is either to a slave or broadcast to all of them. A data packet can take up to 5 time slots. Each packet can be up to 2745 bits in length. They use slots not reserved by the master for synchronous links.

The Bluetooth standard has been deeply influenced by previous ones, such as the IrDA, IEEE 802.11 and others from Motorola (the Piano standard) and the Digital Enhanced Cordless Telecommunications (DECT) standard. Each of these has brought in some significant component of Bluetooth's capabilities. For example, the piconet or PAN concept comes from Piano. However, it also has developed its own unique and innovative ideas.

The *Piano standard* from Motorola is meant to allow mobile devices to form networks automatically at short distances. This is done using a high bandwidth wireless connection among them.

Because of the many different places where things have been left to individual vendors, there are some problems of interoperability between different implementations of Bluetooth. Because the technology is wireless, there is the risk of the data exchange between devices being intercepted and manipulated, posing a security concern.

SAQ 5

Spend 2 Min.

How many channels are available to a piconet? What is the bandwidth of each?

16.3.4 Bluetooth Applications

One major application of Bluetooth is connecting computers to peripherals wirelessly as shown in Fig. 16.4. If peripherals were to be connected without wires then it would make the back of the computer an uncluttered place and save connecting or disconnecting a device from becoming a bewildering task. The use of cables brings about many limitations such as

- Placement of devices is constrained;
- Clutter and inconvenience are caused; and
- Cables can sometimes interfere with the task at hand.

Please remember that even if communication within devices is wireless in the case of Bluetooth, still the power cables to supply power to each device cannot be done away with.

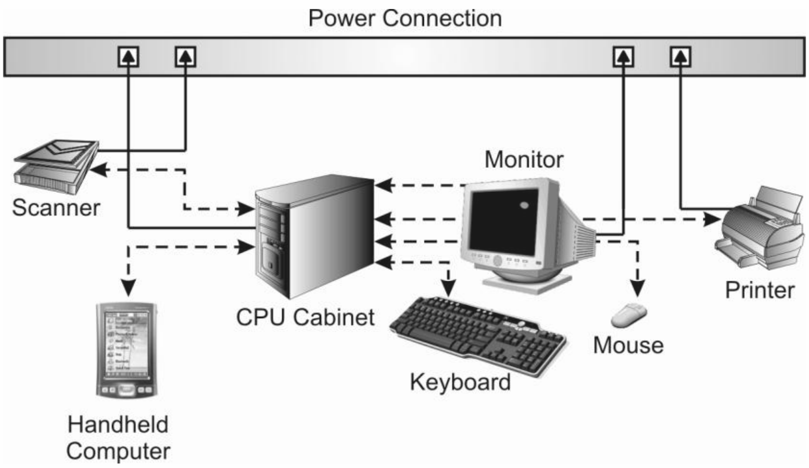

Fig. 16.4: A typical Bluetooth setup

The original goal of Bluetooth was in fact connecting devices without wires. However, the uses of Bluetooth are not confined to this. It can be used to let devices communicate with one another and several applications can come out of this ability. For example, in a closed area like an airport or shopping mall, you can have your own web server that gives out information relevant to that location, say flight times or sales schemes.

You can think of several possible applications. In a meeting, where different people come together for a short while, exchanging files amongst the various computers can be done easily. For example, a person making a presentation can give it out to all who attend. People can discuss matters and change files and all present can have the same changes happen to their copy of the files. The various computers that these people use need not be configured in any way for this to happen. This changing, ad-hoc nature of a Bluetooth network is a big strength of the technology.

So you can see how Bluetooth technology can make it much easier for devices to work together. However, it is not without competition. There are other standards being worked upon that aim to be as inexpensive as Bluetooth, with much higher data transfer speeds and longer range, while retaining all its advantages.

Spend
3 *Min.*

SAQ 6

Specify any three other applications of Bluetooth technology.

Let us now discuss another emerging trend in the computer networks viz. Peer to Peer networks.

16.4 PEER TO PEER (P2P) NETWORKING

You know that the World Wide Web is based on a client/server paradigm. There are server machines that host content or provide other services. These are comparatively few in number. These servers are typically accessed by a much larger number of client machines that make use of these services.

For applications such as file transfer, the model is point to point communication between two machines. The actual route taken by the data packets that are exchanged can be quite different at different periods, depending on the available routes and the traffic on the network at the time. Similarly when a web server makes content available on the Internet, the model is a client/server model whereas the other machines that access the web server are client machines.

While the client/server architecture is appropriate in many situations, it also has some disadvantages. Most servers are lightly utilised while a few well-known ones, the *hot spots*, see very heavy traffic. The servers need to have a large amount of computing power. Because of this, some routes on the network (those that lead to the popular web sites) are prone to congestion while large areas of the Internet see little activity. A very large amount of computing power available on the client machines is only sparsely used.

These deficiencies are addressed in a peer to peer (P2P) networking model where a computer can provide services as well as use them. It makes known to others the services that it offers and computers that require a service can then discover where to find it. This could make for a much more even distribution of computing power and network traffic.

16.4.1 Evolution of Peer to Peer Applications

The most significant revolution caused by P2P was the birth of applications such as the popular *SETI@home* project. This tapped into the idle computing power of millions of PCs and performed analysis and computations that aid in the search for extra-terrestrial intelligence. This was not on-line collaboration, though. The popular instant messaging and conferencing services are another example of a move towards working together on-line. All of these represent a move forward in tapping the potential of connected machines in collaboration.

Napster was a true peer to peer networking application that allowed users to share song files over the Internet without the need for any central server or arbitrator. Gnutella was another file sharing application. However, these and other older applications had some limitations and disadvantages

- they often worked on a single platform;
- they served only a single purpose; and
- different such applications cannot interoperate or collaborate.

Activity

Find out about the experiments presently on-going/planned using P2P distributed computing similar to the *SETI@home* described above.

16.4.2 Characteristics of Peer to Peer Applications

With the runaway success of peer to peer applications, there is the exciting possibility of a quantum leap in Internet usage. Such applications can offer features that are not in wide use at present. For example in searching for files or information, you can have searches that are broad as well as deep and that have several threads running in parallel. Even the best search engines of today would have visited only a small fraction of the available sites or computers on the Internet. What is more, current searches can look through only web servers, while the fact is that there is a wealth of information residing on the machines of individual users who have not put it out on a web server. It is not as if these individuals would always be unwilling to share the information, but they would not want to go through the trouble of maintaining a web site. Such information can become available to the community without much special effort on the part of the owner. It would also mean some change in the way of thinking about our PCs. People will have to become comfortable with the idea of sharing information for common good – especially as they themselves could be the beneficiaries in another case.

A similar situation holds good in the case of sharing computing power. Most PC users use only a small fraction of their processing power except for brief periods. The available computing power on all idling computers in the world would be a very large number. As in the *SETI@home* project, this power can be used to solve complex problems that would otherwise require supercomputers. If properly used, the available power would far exceed the capacity of any other computer on earth – after all we are talking of the combined might of the entire world here! Of course, there would be a need for precautions in the interests of security and privacy, but the potential is very large.

Peer to peer will enable applications that are based on collaborating and on exchange of information. This means that the same application with the same input data can give different answers based on up-to-the-minute real world situations. For example, buying and selling can become more like a physical marketplace, with people interacting directly and comparing bargains. This would be different from the current auction model that is used by websites.

Another feature is that the applications will have high availability. Even if some peer that provides a service is unavailable at a given point in time, there will surely be others who can provide the service, in contrast to a client/server situation where if a server is down, the service might not be available. High availability is traditionally provided through complex fail-over mechanisms, but in peer to peer networking, high availability is a natural side effect of the application paradigm.

It should be understood that peer to peer networking is not meant to replace the current client-server model in vogue, but only to complement it. You will still have websites and use their services. Peer to peer networking will only open up the new world that was previously non-existent.

16.4.3 The Sun JXTA Architecture

In an initiative to realise the potential offered by peer to peer networking, Sun Microsystems developed an architecture for such applications, with inputs from the software community. Here we will look at it briefly and see how it overcomes the limitations of earlier peer to peer applications.

General Approach

The aim here is to tap the large amount of resources available on the Internet that are currently not utilised. These include:

- computing power on PCs, laptops and handheld devices;
- content that is available on a large number of computers that are not web servers;
- programming expertise that is not tied to any organisation; and
- applications in different domains that can be written to use the new dispensation.

The architecture is designed to be scalable and flexible. It had to allow different platforms to interoperate and to be tolerant of failure. Also applications should work in parallel over many different threads. It must also be easy to implement peer groups and security has to be ensured. Collaboration cannot mean invasion of privacy or threats to one's own resources – the collaboration has to be with one's permission! Moreover, it must be easy to configure and set up applications or administer such security settings or alter groupings.

What the architecture does is to provide a set of building blocks in the form of protocols that can be used by any programmer to write applications. These protocols allow for the creation of discovery of peers on the network, provide the ability to create virtual network groups that might exist only for that application and the ability to request for services from other peers. An implementation of the protocols is available on the open source model to be used by any peer who wants to participate. The architecture consists of three main layers which reside on top of any working peer computer on the network. It uses open standards like Java, XML and many concepts from the UNIX operating system to enable collaboration.

a. Core

The core consists of the basic support for the mechanisms of JXTA. You can group peers into peer groups. Membership of a group is governed by policies for various aspects such as security, naming conventions, communicating with other peer groups, allowing or disallowing membership to a peer who seeks to join, removal of a peer from the group and for making known to the rest of the network the existence of the peer group. You can also discover what other peer groups are present and then enter into communication with nodes in that group, if allowed.

Communication between peers is done using a mechanism called **peer pipes**. These allow for security options to be exercised to take care of matters of privacy and integrity of the data. For this, the interchange is structured using XML. You can transfer any kind of data over a peer pipe (normal content, data or code) that the other peer might want to execute. In addition, there are mechanisms for administration. These include prioritisation for peers, allowing or rejecting access and also for load balancing.

This layer only provides mechanisms without enforcing any specific choices. For example, you can choose to send data over cleartext, that is, without any encryption. But if you want encryption, the core gives you the means to do so.

b. Services Layer

The services layer builds on the basic mechanisms of the core to provide facilities of various kinds. This layer provides basic facilities such as searching, indexing and so on. They are features that applications can draw upon without having to go through the labour of writing complex codes for the purpose. These services therefore make the task of application developers easier by providing ready to use functionality.

One example of a service is searching. You can have a deep search performed across a network, such as within the boundaries of a company intranet. Here the query can be processed in parallel by peers in the network. This would provide results that are based on content available within the intranet. If you want to now use the resources of the entire Internet, you can let the query be sent to different peer groups outside your company. In between the extremes lies the possibility of using the networks of your partners such as suppliers or clients in the search. This can be done safely by controlling access to your peer group and by using encrypted transmission.

The search engines on the Internet today cannot locate content that might be generated dynamically. Peer to peer searches can do this better because they would work on a near real time mode rather than reproduce results from previously trawled content. The core and the services layer are the ones where Sun provides support.

c. Applications

Finally, the applications are what developers and the domain experts write to provide functionality for end users. They are left to their imagination and vision, and are written using the lower level facilities from the core and the services layer. We have already discussed some possible applications.

You could have buyers and sellers come together directly and agree on a mutually acceptable price. This could be done by both having a strategy for quoting. This strategy could itself be a simple application. The difference between this kind of trade and the currently available auctions are that there is no central engine that mediates. Similarly instant messaging applications can be written so as to work directly between peers without any central server.

Besides new and better ways of implementing currently available applications, there are undoubtedly a whole lot of new applications that are waiting to be dreamt up by the users and programmers of tomorrow. The JXTA framework allows the quick development of applications using ready mechanisms and tools so that programmers do not have to do the basic things again from scratch. They can thus concentrate on thinking up and implementing useful applications that will work across all platforms and be valuable to the entire community.
You may like to attempt an SAQ before proceeding further.

SAQ 7

Spend 3 *Min.*

What are the functions of the core in Sun JXTA?

This was only an introductory discussion of futuristic trends in communication field and one cannot do justice to any of the above topics in just one unit. However, the objective is to stimulate interest in you and pave the way for further reading on the subject.

After reading about all these technological advances in the communication field, we now briefly discuss their impact on our every-day life and society in general.

16.5 WHERE ARE THE TECHNOLOGICAL ADVANCES HEADING US?

In this course on Communication Physics, we described the various technological developments taking place in the field of communication and their uses in our day-to-day life. However the impact of these new facilities on our life is also worth mentioning.

As you know, the advancements in the field of communication technology have been the factor instrumental in bringing the whole world closer with ease of access to information and its fast exchange. A letter that could have taken days or weeks to reach a destination reaches in a matter of seconds in electronic form. The mobile telephony has made even remote villages connectable without any efforts to install cables. However some points should be remembered while using these technologies.

The computers are networked world over via the Internet. However if proper security measures (in the form of firewalls etc.) are not taken, the computer *virus* or *worms* also find their route into our computers along with the legitimate information that we may be accessing. The viruses reside in the computer, causing harm to the functioning of the computer. The worms are the software programmes, which have a property of self replicating and getting spread through the e-mails sent from the host machine. The menace of spread of these softwares can be stopped only by proper anti-virus programmes and network securities.

Another aspect related to wide access allowed by Internet is the spread of malicious messages, which could affect the moral standards of society. Same has been the case with the *Multimedia Messaging System* (MMS) supported by the cellular mobile handsets. Though both the technologies mentioned here were initially meant for efficient and cost effective information exchange, some miscreant elements of society have put it to use for malicious motives.

One aspect to be taken care of while using the information available on the World Wide Web is to protect the rights of the rightful owner of that information. The authors of any literary and artistic work have a *copyright* in their creation. This right has to be respected while using the information created by them. This was the very reason for stopping the song-swapping platforms like Napster and Grokster used by P2P network users.

The Internet access has given rise to a more serious type of crime known as *Cyber Crime*. Since the information exchange is happening in electronic form, it is quite easy to tap these signals and use them for malicious aims. A good encryption/coding of signals is the solution for stopping any unauthorised tapping of signals.

Normally access to computer is protected by the password given to each authorised user. However it is possible to break the password and gain unauthorised access into the system. This is called *hacking*. There are many cases where a secrete data was stolen or modified by computer hackers and has caused enormous damage.

This list can be unending but the point we wish to make here is that we should be very careful while adapting to new technologies. We should know their pros and cons and take proper precautions while using them so that maximum benefit is derived out of the capabilities of these technologies without causing any ill effects.

Let us now summarise the points we discussed in this unit.

16.6 SUMMARY

- In this unit you have seen three directions in which computer networks are evolving viz. WAP, Bluetooth and P2P.
- Each of these complements the other and they can all co-exist. You can have a wireless application running on a mobile device that connects to hardware for printing or synchronisation using Bluetooth and that is itself part of a peer to peer networking application.
- The use of technology must be done judiciously keeping in mind its pros and cons.

16.7 TERMINAL QUESTIONS

Spend 20 *Minutes*

1. How are mobile software applications different?
2. What are the limitations of WAP applications?
3. What function does the WDP layer serve?
4. What are the disadvantages of connecting devices together with wires?
5. What are the advantages of peer to peer networking?

16.8 SOLUTIONS AND ANSWERS

Self Assessment Questions

1. Mobile computing devices have:
   - low computing power; and
   - limited data storage capability.

2. A WAP portal is similar to a portal on the Internet. It acts as a door or gateway to several destination sites that offer useful services to the user. These sites could be informative or interactive, allowing the user to transact business such as dealing in shares, making travel bookings and so on.

3. Security is important in WAP because wireless transmissions can be intercepted much more easily than wired transmissions. In mobile applications, security needs to be at least at a level as is available on the Internet. Without this assurance, such applications will not be used for financial transactions or where privacy is required, thereby limiting their utility.

4. You do not have to do anything to make the devices in a PAN communicate. As soon as Bluetooth devices come within radio range of another device, they initiate a connection and carry on further conversation if they need to communicate.

5. In the US and Europe 79 channels are available with a bandwidth of 1 MHz each. In Japan there are only 23 channels, with the same bandwidth.

6. Following are some of the applications of Bluetooth technology:

   - Wireless peripherals such as a keyboard or mouse need not be connected to the computer by a cable or connector.
   - A printer can be connected to the computer and used without worrying about the right cable or connector.
   - A cell phone can have a hands-free attachment connected to it without wires.
   - You can synchronise your handheld computer with your PC without the need for a cradle or a cable.

7. The core provides basic services such as grouping peers into groups with policies that allow for membership. Groups can be discovered and you can communicate with them if they permit.

Terminal Questions

1. Mobile applications need to be useful while the user is moving around. The user should be able to perform business transactions conveniently on these scaled down devices. Applications that use knowledge of the user's physical location are also possible with such devices.

2. WAP applications have to take into account the constraints of the client devices that will run them. So though there are no specific constraints on the complexity of WAP applications, they need to consider the probable absence of colour displays and sound or image capability, let alone animation of video. Also navigation and data entry are cumbersome on the client devices. However, some of the higher end mobile phones and communicators available today are better endowed and come with keyboards, pointing devices and colour screens.

3. The Wireless Datagram Protocol layer insulates the upper layers from the physical layer, where actual data transmission occurs. The physical layer could use any of several technologies with different characteristics.

4. The main problems of wire connecting devices are:

   - Clutter caused by a maze of wires;
   - Different kinds of connectors and cables required for each set of devices;
   - Several different protocols depending on the device operation; and
   - The difficulty a layman would face to connect devices.

5. Peer to peer networking could unlock the large amount of computing power available on the computers in the world that is currently underutilised. It can also lead to a more even distribution of traffic on the Internet and obviate the need for popular servers to have a large amount of computing power.

Reference Material:

1. *Computer Networks* by Tanenbaum, A.S.; (IV Edition) (Prentice Hall of India.)
2. *Introduction to Data Communication and Networking* by Forouzani, Behrouz; (IV Edition) (Tata McGraw-Hill)
3. *Data Communications and Networks*, by Godbole, Achyut; (Tata McGraw-Hill)
4. www.webopedia.com/
5. www.wikipedia.org/