JEPPIAAR INSTITUTE OF TECHNOLOGY

"Self-Belief | Self Discipline | Self Respect"

DEPARTMENT

OF

COMPUTER SCIENCE AND ENGINEERING

LECTURE NOTES

CS 8601 - MOBILE COMPUTING

(Regulation 2017)

Year/Semester: III / 06 CSE

2020 – 2021

Prepared by

Dr J FARITHA BANU

Professor / CSE

UNIT I

UNIT I INTRODUCTION: Introduction to Mobile Computing – Applications of Mobile Computing- Generations of Mobile Communication Technologies- Multiplexing – Spread spectrum -MAC Protocols – SDMA- TDMA- FDMA-CDMA.

Introduction to Mobile Computing :

Mobile computing sometimes called **ubiquitous computing** or **nomadic computing**. **Mobile computing** is widely described as the ability to compute remotely while on the move. Enable people to access information from anywhere and at anytime.

Mobile computing as encompasses two separate and distinct concepts: mobility and computing .

1. **Mobility:** provides the capability to change location from one place to other without any interuption. User move locally or even to far away
2. **Computing** means processing related to service invocations on a remote computer.

Mobile Computing vs. Ubiquitous Computing/Pervasive Computing

- ***Mobile Computing*** is a generic term describing the application of small, portable, and wireless computing and communication devices.

  This includes devices like laptops with wireless LAN technology, mobile phones, wearable computers and Personal Digital Assistants (PDAs) with Bluetooth or IRDA interfaces, and USB flash drives.

- ***Ubiquitous computing*** (ubicomp, or sometimes ubiqcomp) integrates computation into the environment, rather than having computers which are distinct objects.

- ***Pervasive computing is*** embedding computation into the environment would enable people to move around and interact with computers more naturally than they currently do.

Challenges in Mobile Computing

1. Disconnection
2. Low bandwidth
3. High bandwidth variability
4. Low power and resources Security risk
5. Wide variety terminals and devices with different capabilities
6. Device attributes
7. Fit more functionality into single, smaller device

Wireless networking

Wireless networks can be classified **into two basic types**. They are single hop and multi hop. The other type of wireless network is an ad hoc network and Bluetooth technology.

Single Hop: It uses fixed infrastructures such as base stations to provide single hop wireless communication with a wired network as illustrated in Fig. 1.1.

One popular example of a fixed infrastructure wireless network is a Wireless LAN (WLAN) that implements the IEEE 802.11 protocol. Observe from Fig. 1.1 that only the last hop is through the wireless medium. **An access point (AP)** provides the last hop connectivity of the mobile nodes to a wired network. All communication goes through APs which **perform bridging** between the wireless and the wired mediums.

A station must be recognized by an AP to be able to connect to the network. The AP may require authentication and this in turn is used as the basic means to keep out the unauthorized users.

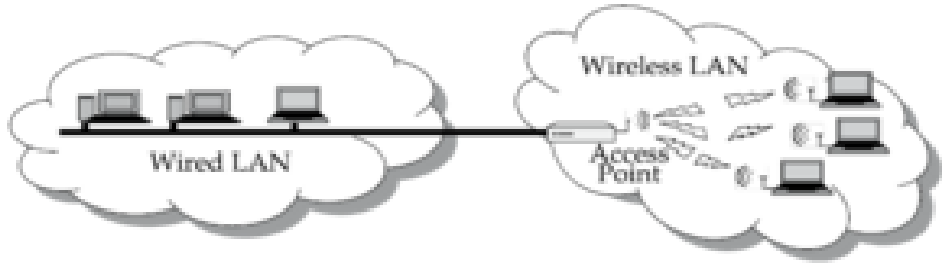


Fig. 1.1 wireless network based on fixed infrastrucure

Two-hop: wireless cellular communication with another mobile as illustrated in Fig. 1.2.

It has three main components: **the core network, the radio access network, and the mobile phones**. Mobile handsets communicate over the radio access network. The radio access network is primarily composed of the base stations which communicate with the mobile phones using radio frequency electromagnetic waves. As shown in Fig. 1.2, the coverage area is decomposed into hexagonal cells. In each hexagonal cell, one base station is located.

Two types of radio channels are usually involved in the communication between a base station and the cell phones: **control channels and voice channels**. Control channels typically use frequency shift keying (FSK) and are used for transferring control messages (data) between the mobile phone and the base station. Voice channels typically use frequency modulation (FM).

A base station typically has two antennas of different characteristics. One antenna is used for receiving and the other for transmitting. The use of the two different types of antennas at the base station increases the ability of the base station to receive the radio signal from mobiles that use very low transmitter power levels. On the other hand, **mobile handsets typically use the same antenna** for both receiving and transmitting.

The **core network interconnects the base stations**, switches the mobile switching centre (MSC), and also provides an interface to other networks such as the traditional telephone

network (PSTN) and the Internet. The interconnect used in the core network is required to provide high-speed connectivity. Therefore, usually **fiber optic cables are used as the interconnect in the core network**. But based on the terrain conditions, microwave communication is also sometimes used.

This interconnection in the core network must allow both voice and control information to be exchanged between the switching system and the base station. The core network is responsible for transmitting voice calls, SMS (Short Message Service), etc. from one phone to another through switches. The core network also maintains a database that contains information about the subscribers and the information about billing.

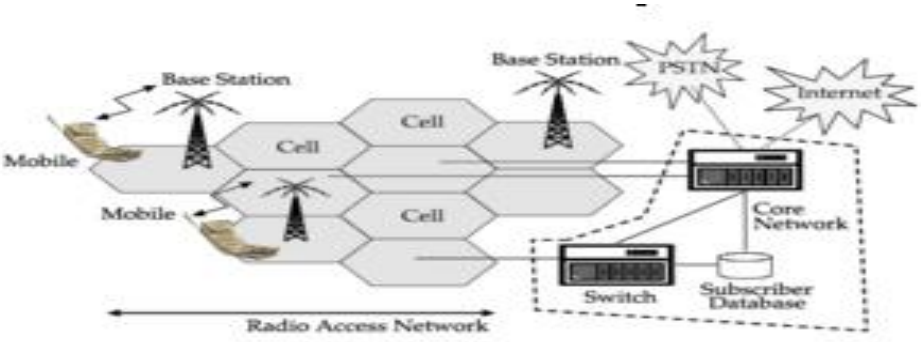


Fig. 1.2 Two hop wireless network

The other type of wireless network is an ad hoc network.

Ad hoc: network does not use any fixed infrastructure and is based on multi-hop wireless communication as shown in Fig. 1.3. An ad hoc network is also known as a Mobile Ad hoc Network (MANET). It is a collection of mobile nodes that form a network on the fly without requiring the support of any fixed infrastructure. Wireless sensor networks are a special type of wireless ad hoc networks.

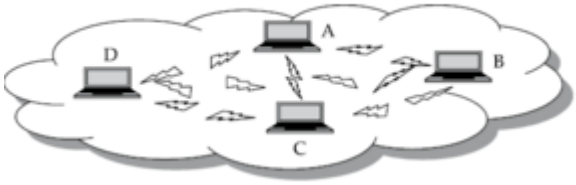


Fig. 1. 3 wireless network having no fixed infrastrucure

In an infrastructureless network, the communication between hosts occurs directly or via a few intermediate nodes that form the hops. For example, station A in Fig. 1.3 can communicate with station C using either the hops A–B, B–C or A–D, D–C.

Bluetooth technology

A development of wireless networking is Bluetooth technology. The Bluetooth technology can also be used to establish direct wireless connection of cell phones with devices such as

printers, cameras, scanners, laptop and desk computers. Bluetooth is gradually replacing cables and infrared as the dominant way of exchanging information between devices.

One of the objectives of the Bluetooth technology is to enable users to easily connect to a wide range of personal computing and telecommunication devices, without the need to buy, carry, or lay out cables.

In fact, the Bluetooth technology enables setting up of **personal area networks (PANs) known as piconets and ad hoc networks known as scatternets**. It provides opportunities for rapid deployment of ad hoc connections, and the possibility of automatic, transparent connections between devices.

Mobile Computing Applications

1. **Send or extract information while on the move**: For example, a stock broker travelling in a car may wish to issue stock transaction orders from a mobile phone or to receive share price quotations.

2. **Ease of deployment and scalability in data transmissions**: over the wireless medium. But, it is not without some shortcomings. When data is being transmitted on air, all the wireless devices present in the transmission range can receive the data. This, therefore, opens up very difficult security issues that must be overcome to ensure privacy of data.

Other APPLICATIONS

1. Vehicles

- transmission of news, road condition, weather, music via Digital Audio Broadcasting (DAB)
- personal communication using Global System for Mobile Communication (GSM)
- position via (Global positioning System) GPS
- forms local ad-hoc network with vehicles close-by to prevent accidents, guidance
- system, redundancy
- vehicle data (e.g., from busses, high-speed trains) can be transmitted in advance for maintenance

2. Emergencies

- early transmission of patient data to the hospital, current status, first diagnosis
- Replacement of a fixed infrastructure in case of earthquakes, hurricanes, fire etc. crisis, war, ...
- Nurses/Doctors in Medical offices are now using Wireless Tablet PCs/WLAN to collect and share patient information.

3. Business - Travelling salesmen

- direct access to customer files stored in a central location
- consistent databases for all agents

- mobile office -
- Sales representatives are using Tablet PCs with Smart phones for presentation, transmitting/access information among office, hotel, and customer location

4. Replacement of fixed networks

- remote sensors, e.g., weather, earth activities
- flexibility for trade shows
- LANs in historic buildings

5. Entertainment, education,

- outdoor Internet access
- intelligent travel guide with up-to-date location dependent information
- ad-hoc networks for multi user games

6. **Location dependent services**

- Location aware services : what services, e.g., printer, fax, phone, server etc. exist in the local environment
- Follow-on services : automatic call-forwarding, transmission of the actual workspace to the current location
- Information services : „push": e.g., current special offers in the supermarket
  „pull": e.g., where is the Black Forrest Cherry Cake?
- Support services : caches, intermediate results, state information etc. "follow" the mobile device through the fixed network Privacy

Characteristics of Mobile Computing

A computing environment is said to be "mobile", when either the sender or the receiver of information can be on the move while transmitting or receiving information.

The following are some of the important characteristics of a mobile computing environment.

Ubiquity: means present everywhere. In the context of mobile computing, ubiquity means the ability of a user to perform computations from anywhere and at anytime.

For example, a business executive can receive business notifications and issue business transactions as long he is in the wireless coverage area.

Location awareness: A hand-held device equipped with global positioning system (GPS) can transparently provide information about the current location of a user to a tracking station. Many applications, personalized services require location-based services.

For example, a person travelling by road in a car, may need to find out a car maintenance service that may be available nearby. He can easily locate such a service through mobile computing where an application may show the nearby maintenance shop.

A few other example applications include traffic control, fleet management and emergency services. In a traffic control application, the density of traffic along various roads can be dynamically monitored, and traffic can be directed appropriately to reduce congestions.

In a fleet management application, the manager of a transport company can have up-to-date information regarding the position of its fleet of vehicles, thus enabling him to plan accurately and provide accurate information to customers regarding the state of their shipments.

Location awareness can also make emergency services more effective by automatically directing the emergency service vehicles to the site of the call.

Adaptation: Adaptation in the context of mobile computing implies the ability of a system to adjust to bandwidth fluctuation without inconveniencing the user.

In a mobile computing environment, adaptation is crucial because of intermittent disconnections and bandwidth fluctuations that can arise due to a number of factors such as handoff, obstacles, environmental noise, etc.

Broadcast: Due to the broadcast nature of the underlying communication network of a mobile computing environment, efficient delivery of data can be made simultaneously to hundreds of mobile users. For example, all users at a specific location, such as those near a railway station, may be sent advertising information by a taxi service operator.

Personalization: Services in a mobile environment can be easily personalized according to a user's profile. This is required to let the users easily avail information with their hand-held devices. For example, a mobile user may need only a certain type of information from specific sources. This can be easily done through personalization.

Structure of Mobile Computing Application

A mobile computing application is usually structured in terms of the functionalities implemented. The simple three-tier structure of a mobile computing application is depicted in Fig. 1.4.

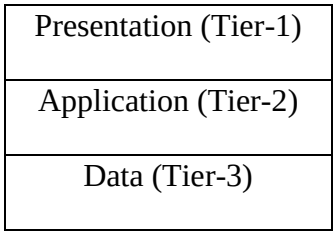


Fig. 1. 4 Three-tier structure of a mobile computing application

As shown in these figures, the three tiers are named presentation tier, application tier and data tier.

Roles and functionality of the three tiers structure of a mobile computing application:

Fig. 1.5 show the Roles and functionality of the three tiers.

Presentation tier: The topmost level of a mobile computing application concerns the user interface. A good user interface facilitates the users to issue requests and to present the results to the them meaningfully. Obviously, the programs at this layer run on the client's computer.

This layer usually includes web browsers and customized client programs for dissemination of information and for collection of data from the user.

Application tier: This layer has the vital responsibility of making logical decisions and performing calculations. It also moves and processes data between the presentation and data layers.

We can consider the middle tier to be like an "engine" of an automobile. It performs the processing of user input, obtaining information and then making decisions. This layer is implemented using technology like Java, .NET services, cold fusion, etc. The implementation of this layer and the functionality provided by this layer should be database independent. This layer of functionalities is usually implemented on a fixed server.

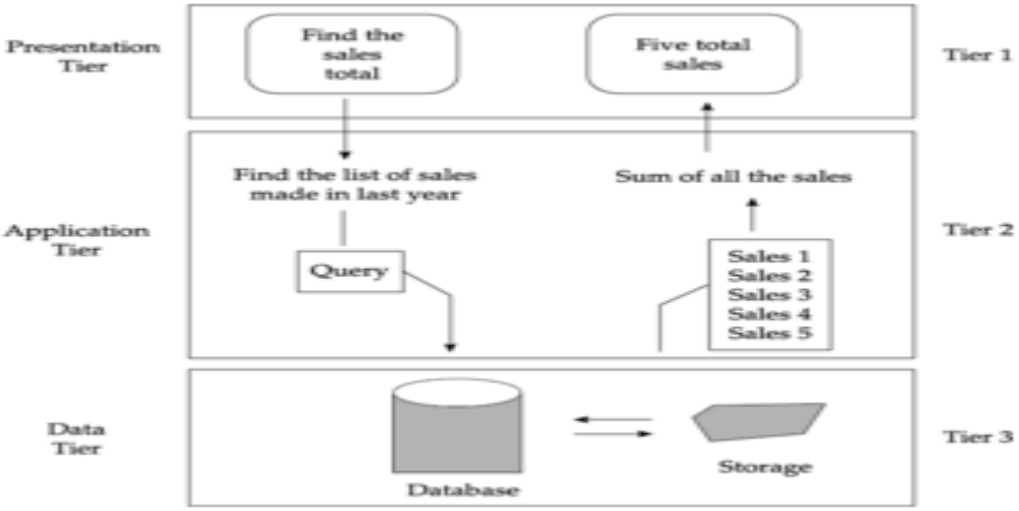


Figure 1.5 Functionalities provided by each tier structure of a mobile computing application.

Data tier The data tier is responsible for providing the basic facilities of data storage, access, and manipulation. Often this layer contains a database. The information is stored and retrieved from this database. But, when only small amounts of data need to be stored, a file system can be used. This layer is also implemented on a fixed server.

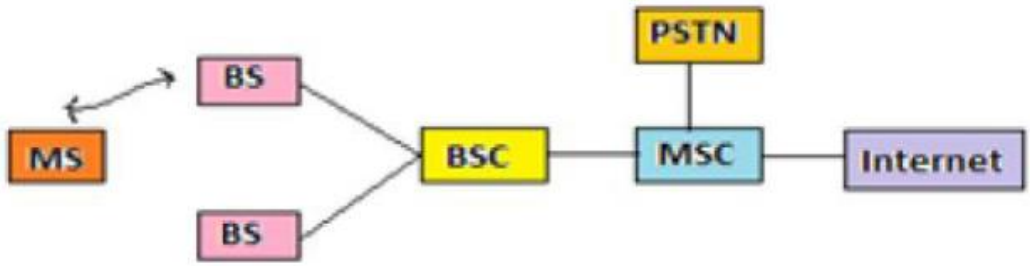
Generations of Mobile Communication Technologies

Mobile communication has become more popular in last few years due to fast reform from 1G to 5G in mobile technology. This reform is due to requirement of service compatible transmission technology and very high increase in telecoms customers. Generation refers change in nature of service compatible transmission technology and new frequency bands. In 1980 the mobile cellular era had started, and since then mobile communications have undergone considerable changes and experienced massive growth.

A. First Generation

- 1G These phones were the first mobile phones to be used, which was introduced in 1982 and completed in early 1990.

- It was used for voice services and was based on technology called as Advanced Mobile Phone System (AMPS). The AMPS system was frequency modulated and used frequency division multiple access (FDMA) with a channel capacity of 30 KHz and frequency band of 824- 894MHz
- It introduces mobile technologies such as Mobile Telephone System (MTS), Advanced Mobile Telephone System (AMTS), Improved Mobile Telephone Service (IMTS), and Push to Talk (PTT)



Architecture of Advanced mobile phone system

B. Second Generation (2G)

- 2G refers to the **second generation based on GSM** and was emerged in late **1980s**.
- It uses **digital signals for voice transmission**. Main focus of this technology was on digital signals and **provides services to deliver text and picture message** and MMS (Multimedia message) **at low speed (in kbps**).
- It use the **bandwidth of 30 to 200KHz**.
- Data speed was upto 64kbps
- Unable to handle complex data such as videos.

C. Third Generation (3G)

- 3G is **based on GSM and was launched in 2000**. The aim of this technology was to **offer high speed data** communication using packet switching.
- **It also offers data services, access to television/video, new services like Global Roaming.**
- It operates at a **range of 2100MHz and has a bandwidth of 15-20MHz** used for High-speed internet service, video chatting.
- Send/receive large email messages
- High speed web/more security/video conferencing/3D gaming
- This generation phones are typically called as smart phones
- **Later, 3G mobile system implemented based on GSM, UMTS(Universal Mobile Telecommunication System).** TD-SCDMA. WCDMA is the air-interface technology used for UMTS

D. Fourth Generation (4G)

- 4G offers a downloading speed of **100Mbps**.

- 4G provides same feature as 3G and additional services like **Multi-Media Newspapers, to watch T.V programs with more clarity and send Data much faster than previous generations** .
- **LTE (Long Term Evolution**) is considered as 4G technology.
- 4G is being developed to accommodate **the QoS and rate requirements** set by forthcoming applications like wireless broadband access, **Multimedia Messaging Service (MMS), video chat, mobile TV, HDTV content, Digital Video Broadcasting (DVB), minimal services like voice and data,** and other services

E. Fifth Generation (5G)

- 5G refer to Fifth Generation which was started from late 2010s.
- Facilities that might be seen with 5G technology includes far better levels of connectivity and coverage.
- The main focus of 5G will be on world-Wireless World Wide Web (WWWW).
- It is a complete wireless communication with no limitations.
- Multi-media newspapers, watch TV programs with the clarity(HD Clarity)
- Large phone memory, dialing speed, clarity in audio/video

Comparison of all generations of mobile Technologies

Technology	1G	2G	3G	4G	5G
Start/Deployment	1970-80	1990-2004	2004-10	Now	Soon (probably by 2020)
Data Bandwidth	2Kbps	64 Kbps	2 Mbps	1 Gbps	Higher than 1 Gbps
Technology	Analog	Digital	CDMA 2000, UMTS,EDGE	Wi-Max, Wi-Fi, LTE	WWWW
Core Network	PSTN	PSTN	Packet N/W	Internet	Internet
Multiplexing	FDMA	TDMA/CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit,Packet	Packet	All Packet	All Packet
Primary Service	Analog Phone Calls	Digital Phone Calls and Messaging	Phone calls, Messaging, Data	All-IP Service (including Voice Messages)	High speed, High capacity and provide large broadcasting of data in Gbps
Key differentiator	Mobility	Secure, Mass adoption	Better Internet experience	Faster Broadband Internet, Lower Latency	Better coverage and no droped calls, much lower latency, Better performance
Weakness	Poor spectral efficiency, major security issue	Limited data rates, difficult to support demand for internet and e-mail	Real performance fail to match type, failure of WAP for internet access	Battery use is more, Required complicated and expensive hardware	?

Multiplexing in Mobile Computing

Multiplexing describes how several users can share a medium with minimum or no interference. It is concerned with sharing the frequency range amongst the users. Frequency Bands are split into channels with Guard Space (gaps between allocations)

Four main ways of assigning channels

• Space Division Multiplexing (SDM): allocate according to location

• Time Division Multiplexing (TDM): allocate according to units of time

• Frequency Division Multiplexing (FDM): allocate according to the frequencies

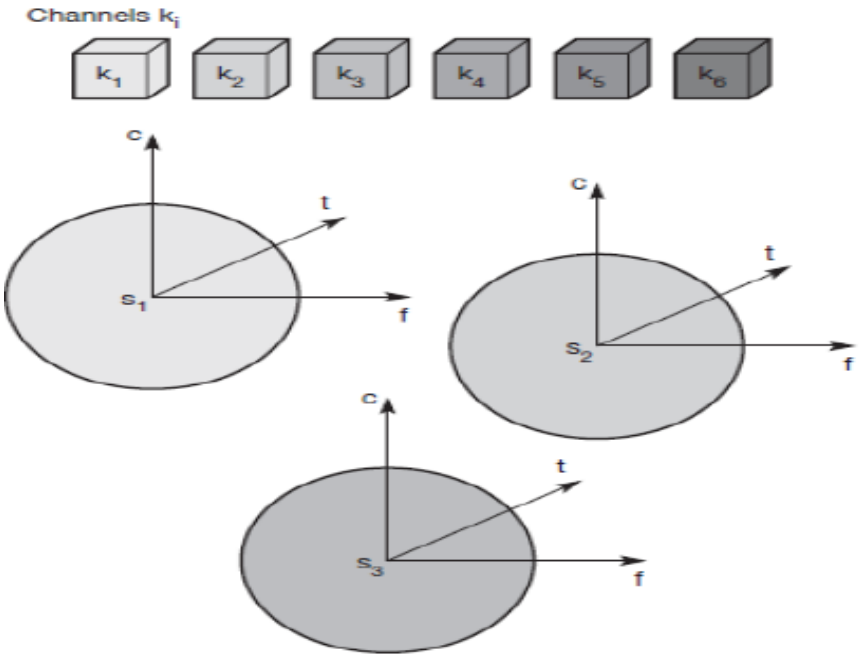
• Code Division Multiplexing (CDM) : allocate according to access codes

Space division multiplexing

- This is the basis of frequency reuse
- Each physical space is assigned channels
- Spaces that don't overlap can have the same channels assigned to them
- Example: FM radio stations in different countries

This multiplexing scheme is used, for example, at FM radio stations where the transmission range is limited to a certain region, many radio stations around the world can use the same frequency without interference

Below figure shows six channels ki and introduces a three dimensional coordinate system. This system shows the dimensions of code c, time t and frequency f. For this first type of multiplexing, space division multiplexing (SDM), the (three dimensional) space si is also shown. Here space is represented via circles indicating the interference range



For the remaining channels (k4 to k6) three additional spaces would be needed. In our highway example this would imply that each driver had his or her own lane.

Drawback

Although this procedure clearly represents a waste of space, this is exactly the principle used by the old analog telephone system: each subscriber is given a separate pair of copper wires to the local exchange. In wireless transmission, SDM implies a separate sender for each communication channel with a wide enough distance between senders.

Frequency division multiplexing

- Separation of the whole spectrum into smaller non overlapping frequency bands (guard spaces are needed)
- A channel gets a certain band of the spectrum for the whole time – receiver has to tune to the sender frequency

Time division multiplexing

- Here a channel ki is given the **whole bandwidth for a certain amount of time**, i.e., all senders use the same frequency but at different points in time.
- Only one carrier in the medium at any time
- Throughput high even for many users

Code division multiplexing

- All channels ki use the same frequency at the same time for transmission.
- **Separation is now achieved by assigning each channel its own 'code'**,
- **guard spaces are realized by using codes with the necessary 'distance' in code space, e.g., orthogonal codes**.
- **Implemented using spread spectrum technology.**

Spread Spectrum in Mobile Computing

Problem of radio transmission: frequency dependent fading can wipe out narrow band signals for duration of the interference. To overcome this Spread Spectrum is utilized.

Spread Spectrum means **spread the narrow band signal into a broad band signal using a special code**

- protection against narrow band interference

Usage of Spread Spectrum

There are many reasons to use this spread spectrum technique for wireless communications. The following are some reasons:

- It can successfully establish a secure medium of communication.

- It can increase the resistance to natural interference, such as noise and jamming, to prevent detection.
- It can limit the power flux density (e.g., in satellite down links).
- It can enable multiple-access communications.

There are two main types of spread spectrum multiple access techniques −

- Frequency hopped spread spectrum (FHSS)
- Direct sequence spread spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS)

For frequency hopping spread spectrum (FHSS) systems, the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels. Transmitter and receiver stay on one of these channels for a certain time and then**.** hop to another channel. This system implements FDM and TDM.

The pattern of channel usage is called the hopping sequence, the time spend on a channel with a certain frequency is called the dwell time. FHSS comes in two variants, slow and fast hopping.
In slow hopping, the transmitter uses one frequency for several bit periods. **For fast hopping** systems, the transmitter changes the frequency several times.

Direct Sequence Spread Spectrum (DSSS)

This is the most commonly used technology for CDMA. In DSSS, the message signal is multiplied by a Pseudo Random Noise Code. This spreading code has a higher chip rate (this the bitrate of the code), which results in a wideband time continuous scrambled signa.

Each user is given his own code word which is orthogonal to the codes of other users and in order to detect the user, the receiver must know the code word used by the transmitter.

DSSS significantly improves protection against interfering (or jamming) signals, especially narrowband and makes the signal less noticeable. It also provides security of transmission if the code is not known to the public. These reasons make DSSS very popular by the military. In fact, DSSS was first used in the 1940s by the military.

DSSS can also be used as a multiple access technique, whereby several different pseudo random spreading codes are being used simultaneously.

Space Division Multiple Access (SDMA)

Space Division Multiple Access (SDMA) is the basis of frequency reuse. **Space Division Multiple Access (SDMA)** is used for allocating a separated space to users in wireless networks.

A typical application involves assigning an **optimal base station to a mobile phone user**. The mobile phone may receive several base stations with different quality.

 A MAC algorithm could **now decide which base station is best**, taking into account which frequencies (FDM), time slots (TDM) or code (CDM) are still available.

 The basis for the SDMA algorithm is **formed by cells and sectorized antennas** which constitute the infrastructure implementing **space division multiplexing (SDM).**

 SDM has the unique advantage of not requiring any multiplexing equipment.

 It is usually combined with other multiplexing techniques to better utilize the individual physical channels

SDMA has the following features,

- All users can communicate at the same time using the same channel.
- SDMA is completely free from interference.
- A single satellite can communicate with more satellites receivers of the same frequency.
- The directional spot-beam antennas are used and hence the base station in SDMA, can track a moving user.
- Controls the radiated energy for each user in space.

Note: (For Detailed SDMA answers include Space Division Multiplexing)

MEDIUM ACCESS CONTROL (MAC)Protocols

In a wireless network, multiple nodes may contend to transmit on the same shared channel at the same time. In this situation, the transmitted **data would get garbled** unless a suitable medium access arbitration scheme is deployed.

The medium access control (MAC) protocol is a sublayer of the data link layer protocol and used to control the shared channel access mechanisam.

The primary responsibility of a MAC protocol is to **enforce discipline in the access of a shared channel when multiple nodes contend to access that channel**.

Two other objectives of any MAC protocol are **maximization of the utilization of the channel and minimization of average latency of transmission**.

However, a MAC protocol must be fair and ensure that no node has to wait for an unduly long time, before it is allowed to transmit.

Properties required for MAC protocol

In a general sense a good MAC protocol needs to possess the following features:

- It should implement some rules that help to enforce discipline when multiple nodes contend for a shared channel.
- It should help maximize the utilization of the channel.
- Channel allocation needs to be fair.

- No node should be discriminated against at any time and made to wait for an unduly long time for transmission.
- It should be capable of supporting several types of traffic having different maximum and average bit rates.
- It should be robust in the face of equipment failures and changing network conditions.

At present, IEEE 802.11 has emerged as a popular and standard MAC protocol for wireless networks. IEEE 802.11-based network cards and routers are available in the market that can be used to inexpensively and easily set up wireless LANs (commonly referred to as Wi-fi hotspots).

Wireless MAC Issues

A MAC protocol in a wireless medium is much more complex than its wired counterpart. First, a collision detection scheme is difficult to implement in a wireless environment, since collisions are hard to be detected by the transmitting nodes. Also, in infrastructure-less networks, the issue of hidden and exposed terminals make a MAC protocol extremely inefficient unless special care is taken to overcome these problems. We elaborate the hidden and exposed terminal problems in the following:

The Hidden and Exposed Terminal Problems in an Infrastructure-less Network

The hidden terminal problem arises when at least three nodes (A, B, and C), as shown in Fig. 1.6, communicate among each other. As shown in this figure, B is in the radio range of A, and B is also within the radio range of C. However, the nodes A and C are not in the radio range of each other. Note that if both A and C start to transmit to B at the same time, the data received at node B would get garbled.

Such a situation can arise because A and C are "hidden" from each other, because they are outside each other's transmission range. In this situation, when one node starts to sense the medium before transmission, it cannot sense that the other node is also transmitting. This creates a very difficult and important arbitration problem that a MAC protocol needs to resolve.

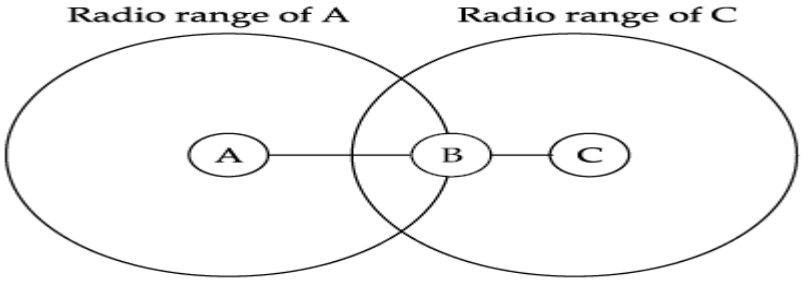


Fig. 1.6 Hidden Terminal Problem

A related problem called exposed terminal could arise in a scenario such as that depicted in Fig. 1.7 MAC protocols usually inhibit transmission when transmission from another terminal is detected. As a result, node A will not be able to transmit to any node when B is transmitting to C. On the other hand, had A transmitted to D, it would have been received correctly by D and B's transmission would have also been correctly received at C.

The problem arose only because A and B are within each other's transmission range, though the destination nodes are in the transmission range of only one of the nodes. In other words, the problem occurs because A is exposed to B's transmission. The overall effect of this problem is that it leads to inefficient spectrum usage as well as unnecessary transmission delays unless these are carefully addressed by a wireless MAC protocol.

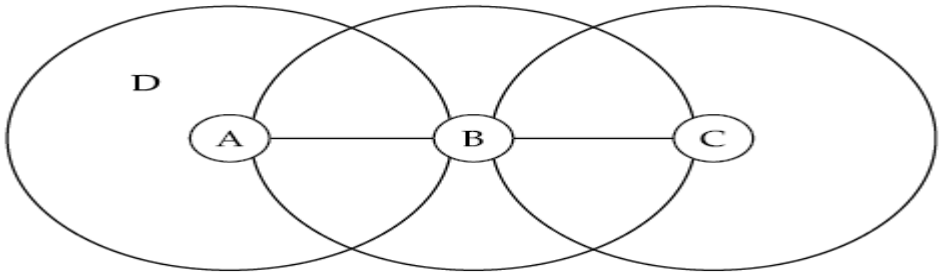


Fig. 1.7 Exposed Terminal Problem

A Taxonomy of MAC Protocols

A large number of MAC protocols have been proposed. These MAC protocols can be broadly divided into the following three categories: (i) Fixed assignment schemes (ii) Random assignment schemes (iii) Reservation-based schemes

The fixed assignment schemes are usually called circuit-switched schemes. In the fixed assignment schemes, the resources required for a call are assigned for the entire duration of the call. On the other hand, the random assignment schemes and the reservation schemes are called packet-switched schemes.

The random assignment schemes are comparable to the connection-less packet-switching schemes. In this, no resource reservations are made, the nodes simply start to transmit as soon as they have a packet to send.

In the reservation schemes, a node makes explicit reservation of the channel for an entire call before transmitting. This is analogous to a connection-based packet-switching scheme. The reservation-based MAC schemes are suitable to handle calls with widely varying traffic characteristics. In the following sections, we discuss these three categories of MAC protocols in some more detail.

Fixed Assignment Schemes

A few important categories of fixed assignment MAC protocols are the following:

- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
- Code Division Multiple Access (CDMA)

Frequency Division Multiple Access (FDMA)

In FDMA, the available bandwidth (frequency range) is divided into many narrower frequency bands called channels. Figure 1.8 shows a division of the existing bandwidth into many channels (showns as Ch 1, Ch 2, etc.). For full duplex communication to take place, each user is allocated a forward link (channel) for communicating from it (mobile handset) to the base station (BS), and a reverse channel for communicating from the BS to it.

Thus, each user making a call is allocated two unique frequency bands (channels), one for transmitting and the other for receiving signals during the call. Obviously, when a call is underway, no other user would be allocated the same frequency band to make a call. Unused transmission time in a frequency band that occurs when the allocated caller pauses between transmissions, or when no user is allocated a band, goes idle and is wasted. FDMA, therefore, does not achieve a high channel utilization.

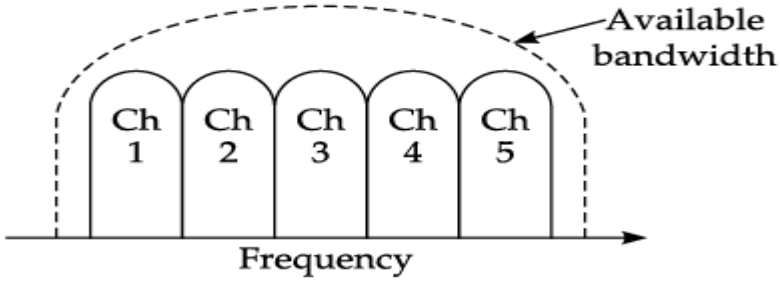


Fig. 1.8 Channels in Frequency Division Multiple Access (FDMA) scheme.

Time Division Multiple Access (TDMA)

TDMA is an access method in which multiple nodes are allotted different time slots to access the same physical channel. That is, the timeline is divided into fixed-sized time slots and these are divided among multiple nodes who can transmit. Note that in this case, all sources use the same channel, but take turns in transmitting. Figure 1.9 shows the situation where time slots are allocated to users in a round robin manner, with each user being assigned one time slot per frame. See Box 3.2. Obviously, unused time slots go idle, leading to low channel utilization.

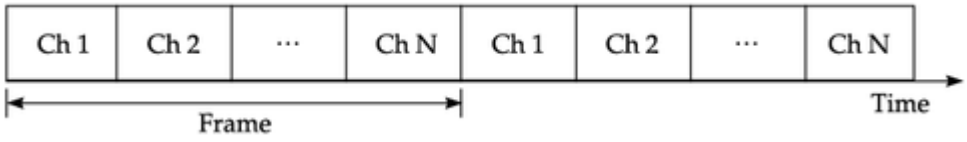
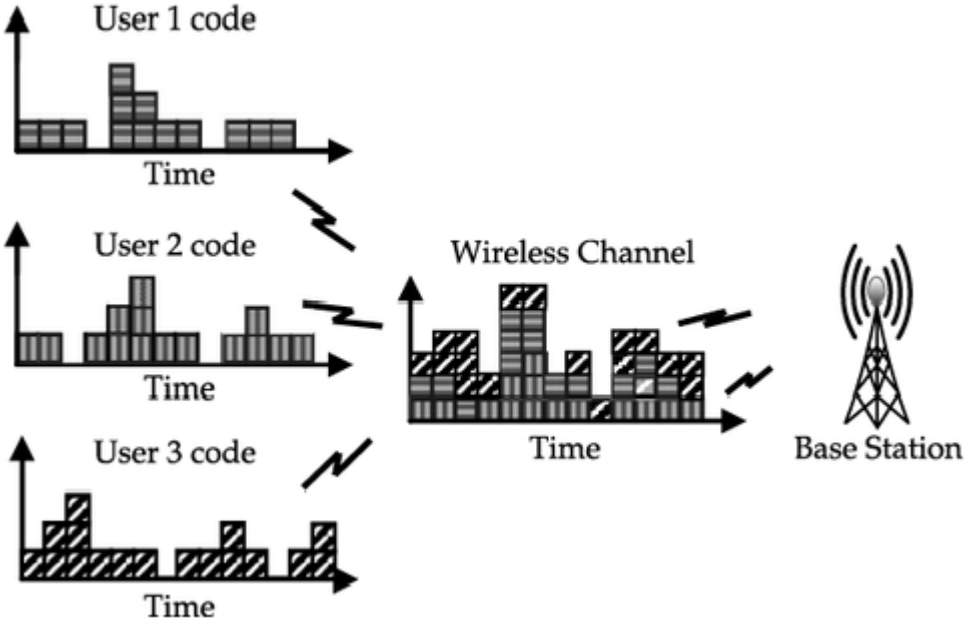


Fig. 1.9 Channels in Time Division Multiple Access (TDMA) scheme.

Code Division Multiple Access (CDMA)

In CDMA, multiple users are allotted different codes that consist of sequences of 0 and 1 to access the same channel. As shown in Fig. 1.10, a special coding scheme is used that allows signals from multiple users to be multiplexed over the same physical channel. As shown in the figure, three different users who have been assigned separate codes are multiplexed on the same physical channel.



(Or)

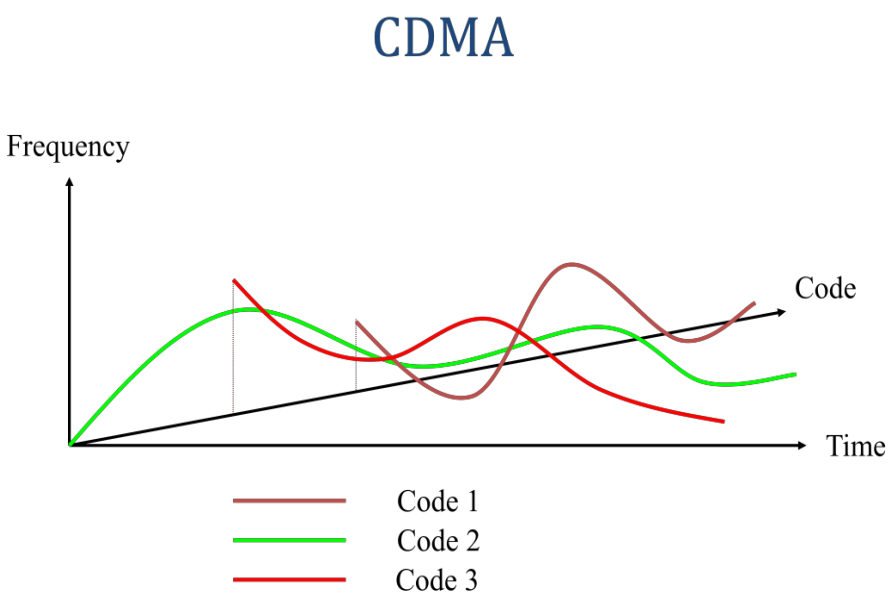


Fig. 1.10 Schematic of operation of Code Division Multiple Access (CDMA).

In the following, we elaborate the CDMA technology. In CDMA, multiple users use the same frequency at the same time and no time scheduling is applied . All the senders send signals simultaneously through a common medium. The bandwidth of this medium is much larger than the space that would be allocated to each packet transmission during FDMA and the signals can be distinguished from each other by means of a special coding scheme that is used. This is done with the help of a frequency spreading code known as the m -bit pseudo-noise (PN) code sequence. Using m bits, $2^m - 1$ different codes can be obtained. From these codes, each user will use only one code.

It is possible to distinguish transmissions from different nodes by ensuring some properties on the codes. A code for a user should be orthogonal (that is, non-interfering) to the codes assigned

to other nodes. The term "orthogonal" means that the vector inner product is zero, and good autocorrelation uses the bipolar notation where a code sequence of binary 0 is represented as –1 and binary 1 is represented as +1. See Box 3.3. On the receiving end, only the same PN sequence is able to demodulate the signal to successfully convert the input data .

For simplicity, we assume that all nodes transmit on the same frequency at the same time using the entire bandwidth of the transmission channel. Each sender has a unique random number key, and the sender XORs the signal with this random number key. The receiver can "tune" into this signal if it knows the pseudorandom number.

Consider an example, where X, Y are the transmitters and Z is a receiver. Sender X_data = 1 and X_Key = (010011). Its autocorrelation representation is (–1, +1, –1, –1, +1, +1).

Sender:

The signal to be calculated at sender X is Xs = X_data * X_key = +1 * X_key = (–1, +1, –1, –1, +1, +1).

Similarly, sender Y_data = 0 and Y_key = (110101) and the signal to be sent at Y is Ys = –1 * Y_key = –1 * (+1, +1, –1, +1, –1, +1) = (–1, –1, +1, –1, +1, –1).

The signal received by receiver Z is Xs + Ys = (–1, +1, –1, –1, +1, +1) + (–1, –1, +1, –1, +1, –1) = (–2, 0, 0, –2, +2, 0).

Receiver:

At the receiver, in order to receive the data sent by sender X, the signal Z is dispread.

So now if Z wants to get information of sender X data, then Z * X_key = (–2, 0, 0, –2, +2, 0) * (–1, +1, –1, –1, +1, +1) = 2 + 0 + 0 + 2 + 2 + 0 = 6 > 0 (positive), that is the original bit was a 1.

Similarly, the information of sender Y data may be obtained as Z * Y_key = (–2, 0, 0, –2, +2, 0) * (+ 1, +1, –1, +1, –1, +1) = –2 + 0 + 0 – 2 – 2 + 0 = – 6 < 0 (negative). So the Y data original bit was a 0.

Random Assignment schemes

There are a number of random assignment schemes that are used in MAC protocols. A few important ones are the following:

ALOHA

Slotted ALOHA

CSMA

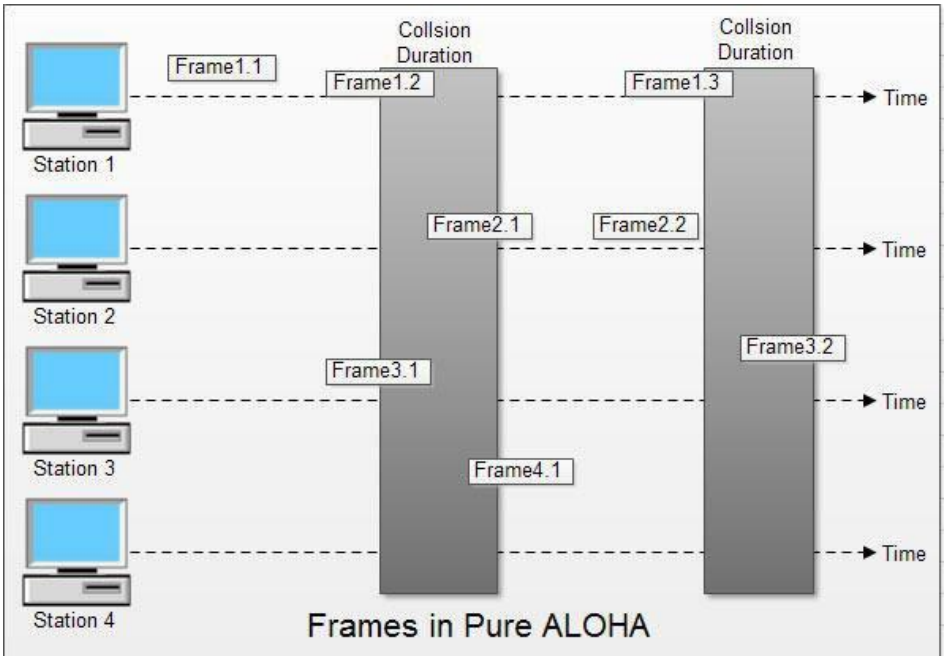
CSMA/CD

CSMA/CA

ALOHA Scheme

It is a simple communication scheme that was developed at the university of Hawaii. The basic (also called pure) ALOHA scheme, is a simple protocol. If a node has data to send, it begins to transmit. Note that the first step implies that Pure ALOHA does not check whether the channel is busy before transmitting. If the frame successfully reaches the destination (receiver), the next frame is sent. If the frame fails to be received at the destination, it is sent again.

The simple ALOHA scheme works acceptably, when the chances of contention are small (i.e., when a small number of senders send data infrequently). However, the collisions can become unacceptably high if the number of contenders for transmission is high.



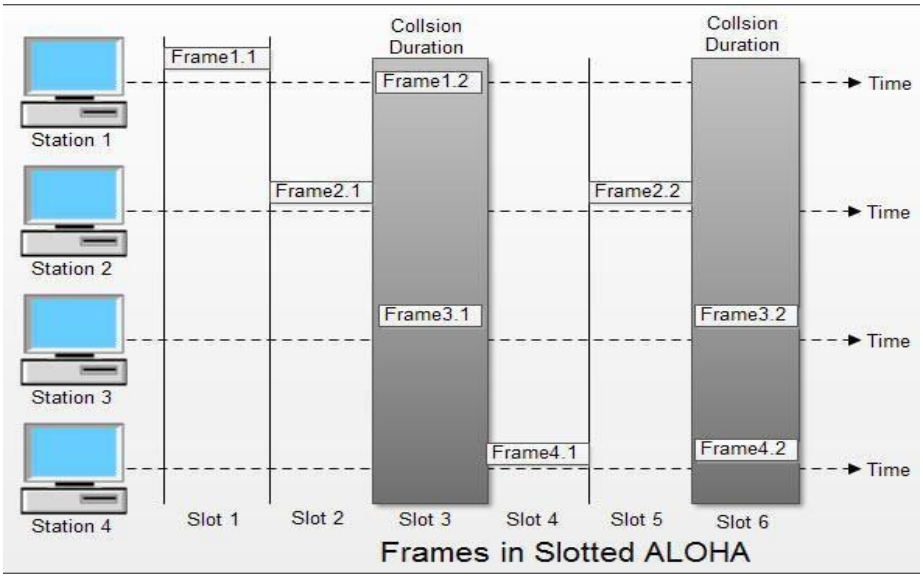
In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.

Slotted ALOHA Scheme

An improvement over the pure ALOHA scheme is the slotted ALOHA.

In the slotted ALOHA scheme, the chances of collisions are attempted to be reduced by enforcing the following restrictions. The time is divided into equal-sized slots in which a packet can be sent. Thus, the size of the packet is restricted. A node wanting to send a packet, can start to do so only at the beginning of a slot.

The slotted ALOHA system employs beacon signals that are sent at precise intervals that mark the beginning of a slot, at which point the nodes having data to send can start to transmit. Again, this protocol does not work very well if the number of stations contending to send data is high. In such cases, the CSMA scheme (described next) works better.



In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.

The CSMA Scheme

A popular MAC arbitration technique is the Carrier Sense Multiple Access (CSMA). In this technique, a node senses the medium before starting to transmit. If it senses that some transmission is already underway, it defers its transmission. Two popular extensions of the basic CSMA technique are the collision detection (CSMA/CD) and the collision avoidance (CSMA/CA) techniques.

The CSMA/CD Scheme

Unlike that in a wired network, in a wireless network the CSMA/CD technique does not work very well.

In the CSMA/CD technique, the sender starts to transmit if it senses the channel to be free. But, even if it senses the channel to be free, there can be a collision (why?) during transmission.

In a wired network, the implementation of a collision detection scheme is simple. However, in a wireless network it is very difficult for a transmitting node to detect a collision, since any received signal from other nodes would be too weak compared to its own signal and can easily be masked by noise. As a result, a transmitting node would continue to transmit the frame, and only the destination node would notice the corrupted frame after it computes the checksum. This leads **to retransmissions and severe wastage of channel utilization**. In contrast, in a wired network when a node detects a collision, it immediately stops transmitting, thereby minimizing channel wastage.

In a wireless network, a collision avoidance scheme works much better compared to a collision detection-based scheme.

The CSMA/CA Scheme

A collision avoidance scheme is based on the idea that it is necessary to prevent collisions at the moment they are most likely to occur, that is, when the bus is released after a packet transmission.

We explain the reason for this in the following. During the time a node is transmitting on the channel, several nodes might be wanting to transmit. These nodes would be monitoring the channel and waiting for it to become free. The moment the transmitting node completes its transmission, these waiting nodes would sense the channel to be free, and would all start transmitting at the same time.

To overcome such collisions, in the **collision avoidance scheme, all nodes are forced to wait for a random time and then sense the medium again, before starting their transmission**. If the medium is sensed to be busy, a node waiting to transmit waits for a further random amount of time and so on. Thus, the chance of two nodes starting to transmit at the same time would be greatly reduced.

Note :

(CSMA/CD) Carrier Sense Multiple Access with Collision Detection is suited for wired networks because, **It sends as soon as the medium is free, listen into the medium if a collision occurs as in IEEE 802.3.**

Why CSMA/CD not suit for wireless networks?

- **signal strength decreases proportional to the square of the distance**
- the sender would apply CS and CD, but the collisions happen at the receiver
- it might be the case that a sender cannot "hear" the collision, i.e., CD does not work
- furthermore, CS might not work if, e.g., a terminal is "hidden"

Reservation Base Schemes

A basic form of the reservation scheme is the RTS/CTS scheme. In an RTS/CTS scheme, a sender transmits an RTS (Ready to Send) packet to the receiver before the actual data transmission. On receiving this, the receiver sends a CTS (Clear to Send) packet, and the actual data transfer commences only after that. When the other nodes sharing the medium sense the CTS packet, they refrain from transmitting until the transmission from the sending node is complete.

In a contention-based MAC protocol, a node wanting to send a message first reserves the medium by using an appropriate control message. For example, reservation of the medium can be achieved by transmitting a "Ready To Send" (RTS) message and the corresponding destination node accepting this request answers with a "Clear To Send" (CTS) message.

Every node that hears the RTS and CTS messages defers its transmission during the specified time period in order to avoid a collision. An examples of RTS-CTS based MAC protocols are MACA, MACAW protocols.

In the following, we discuss MACA as a representative protocol belonging to this category of protocols.

MACA

MACA stands for Multiple Access Collision Avoidance. MACA solves the hidden/exposed terminal problems by regulating the transmitter power. A node running MACA requests to use the medium by sending an RTS to the receiver. Since radio signals propagate omni-directionally, every terminal within the sender's radio range will hear this and then refrain from transmitting. As soon as the receiver is ready to receive data, it responds with a CTS.

Figure 1.11 schematically shows how MACA avoids the hidden terminal problem. Before the start of its transmission, it sends a Request To Send (RTS). B receives the RTS that contains the sender's name and the receiver's name, as well as the length of the future transmission . In response to the RTS, an acknowledgment from B is triggered indicating Clear To Send (CTS). The CTS contains the names of the sender and receiver, and the length of the planned transmission. This CTS is heard by C and the medium is reserved for use by A for the duration of the transmission.

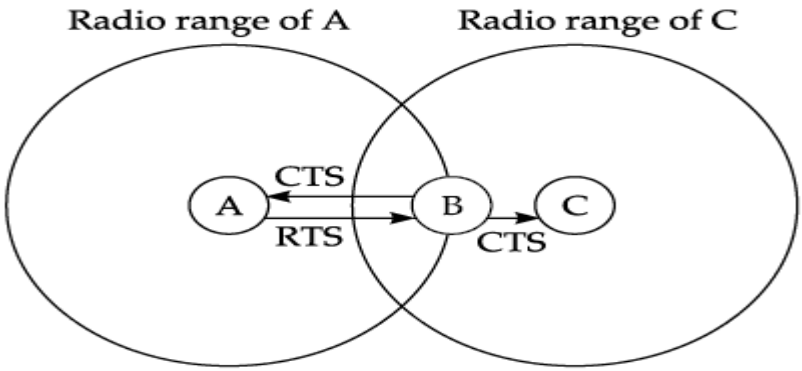


Fig.1.11 Hidden terminal solution in MACA.

On receipt of a CTS from B, C refrains from transmitting anything for the time indicated in the CTS. Thus a collision cannot occur at B during data transmission, and the hidden terminal problem is solved. Though this is a collision avoidance protocol, a collision can occur during the sending of an RTS. Both A and C could send an RTS at same time. But an RTS occurs over a very small duration compared to the duration of data transmission.

Thus the probability of collision remains much less. B resolves this contention problem by acknowledging only one station in the CTS. No transmission occurs without an appropriate CTS.

Figure 1.12 schematically shows how the exposed terminal problem is solved in MACA. Assume that B needs to transmit to A. B has to transmit an RTS first as shown in Fig. 1.12. The RTS would contain the names of the receiver (A) and the sender (B). C does not act in

response to this message as it is not the receiver, but A responds with a CTS. C does not receive this CTS and concludes that A is outside the detection range. Thus C can start its transmission assuming that no collision would occur at A.

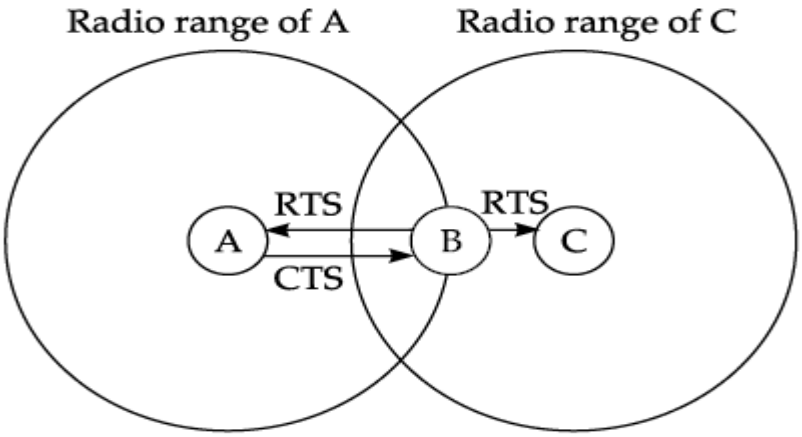


Fig.1.12 Exposed terminal solution in MACA.