IV/IV B.TECH (REGULAR) DEGREE EXAMINATION

November 2017 Computer Science & Engineering

Seventh Semester Wireless Networks

14CS704

Answer Question No.1 compulsorily

Answer ONE Question from each unit.

1. Answer all questions
   a. Mention the functions of data link layer in wireless environment.
   b. Draw the phase domain representation of a signal.
   c. What is effect of inter symbol interference?
   d. Mention the GSM bearer services.
   e. How do inclination and elevation determine the use of a satellite?
   f. What are the disadvantages of WLANs?
   g. What is reverse tunneling?
   h. What is the reaction of standard TCP in case of packet loss?
   i. What are the advantages of snooping TCP?
   j. What are the services offered by Wireless Transaction Protocol to higher layers?
   k. What is inhibit sense multiple access scheme?
   l. Define selective retransmission.

UNIT - I

1.
   a. Define spread spectrum. How spreading is performed using DSSS? 6M
   b. Compare SDM, FDM and TDM multiplexing schemes. 6M

(OR)

2.
   a. Why specialized MAC is needed in wireless environment? 6M
   b. Describe PRMA and MACA schemes. 6M

UNIT – II

3.
a. Draw the function architecture of GSM and explain? 8M

b. Explain MTC and MOC in GSM. 4M

(OR)

4.
a. Write in detail about the main components of the UMTS reference architecture. 8M

b. List and explain different types of satellite orbits? 4M

UNIT – III

5.
a. Draw the IEEE 802.11 MAC packet structure and explain each field? 6M

b. Explain DFWMAC-DCF schemes with neat sketches? 6M

(OR)

6.
a. How packet delivery to and from the mobile is performed in mobile IP? 6M

b. Describe how a mobile node registration is performed. 6M

UNIT – IV

7.
a. With an example explain dynamic source routing algorithm? 8M

b. Write about indirect TCP. 4M

(OR)

8.
a. Explain about wireless session protocol? 8M

b. Explain about wireless datagram protocol? 4M

Scheme of Valuation

IV/IV B.TECH (REGULAR) DEGREE EXAMINATION

November 2017 Computer Science & Engineering

Seventh Semester Wireless Networks

14CS704

Answer Question No.1 compulsorily

Answer ONE Question from each unit.

1. Answer all questions

a. Mention the functions of data link layer in wireless environment.

The data link layer provides means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer.

FUNCTIONS OF DATA LINK LAYER:

Framing

Physical Addressing

Flow Control

Access Control

b. Draw the phase domain representation of a signal.

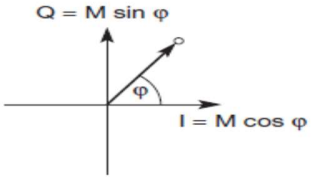


Figure 2.4 Phase domain representation of a signal

c. What is effect of inter symbol interference?

Intersymbol interference (**ISI**) is a form of distortion of a signal in which one symbol interferes with subsequent symbols. This is an unwanted phenomenon as the previous symbols have similar effect as noise, thus making the communication less reliable. The spreading of the pulse beyond its allotted time interval causes it to interfere with neighboring pulses. ISI is usually caused by multipath propagation or the inherent linear or non-linear frequency response of a channel causing successive symbols to "blur" together.

The presence of ISI in the system introduces errors in the decision device at the receiver output. Therefore, in the design of the transmitting and receiving filters, the objective is to minimize the effects of ISI, and thereby deliver the digital data to its destination with the smallest error rate possible.

d. Mention the GSM bearer services.

Bearer services are the telecommunication services to transfer data over the network. Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission.

Transparent bearer services only use the functions of the physical layer (layer 1) to transmit data. Data transmission has a constant delay and throughput if no transmission errors occur. The only mechanism to increase transmission quality is the use of **forward error correction (FEC)**, which codes redundancy into the data stream and helps to reconstruct the original data in case of transmission errors. Depending on the FEC, data rates of 2.4, 4.8, or 9.6 kbit/s are possible.

Non-transparent bearer services use protocols of layers two and three to implement error correction and flow control. These services use the transparent bearer services, adding a **radio link protocol (RLP)**. This protocol comprises mechanisms of **high-level data link control (HDLC)**, and specialselective-reject mechanisms to trigger retransmission of erroneous data.

e. How do inclination and elevation determine the use of a satellite?

The **inclination angle** δ is defined as the angle between the equatorial plane and the plane described by the satellite orbit. An inclination angle of 0 degrees means that the satellite is exactly above the equator. The **elevation angle** ε is defined as the angle between the center of the satellite beam and the plane tangential to the earth's surface.

f. What are the disadvantages of WLANs?

- Quality of service
- Proprietary solutions
- Restrictions
- Safety and security
- Cost

g. What is reverse tunneling?

A reverse tunnel is a tunnel that starts at the mobile node's care-of address and terminates at the home agent. A mobile node can request a **reverse tunnel** between its foreign agent and its home agent when the mobile node registers.

h. What is the reaction of standard TCP in case of packet loss?
Congestion

i. What are the advantages of snooping TCP?

- The End-to-end TCP semantic is preserved.
- The correspondent host does not need to be changed.
- It does not need a handover of state as soon as the mobile host moves to another foreign agent.

j. What are the services offered by Wireless Transaction Protocol to higher layers?

WTP offers a light-weight transaction service at the transaction SAP(TR-SAP). This service is efficiently provides reliable or unreliable requests and asynchronous transactions.

k. What is inhibit sense multiple access scheme?

This scheme, which is used for the packet data transmission service Cellular Digital Packet Data (CDPD) in the AMPS mobile phone system, is also known as digital sense multiple access (DSMA). Here, the base station only signals a busy medium via a busy tone (called BUSY/IDLE indicator) on the downlink. After the busy tone stops, accessing the uplink is not coordinated any further. The base station acknowledges successful transmissions; a mobile station detects a collision only via the missing positive acknowledgement. In case of collisions, additional back-off and retransmission mechanisms are implemented.

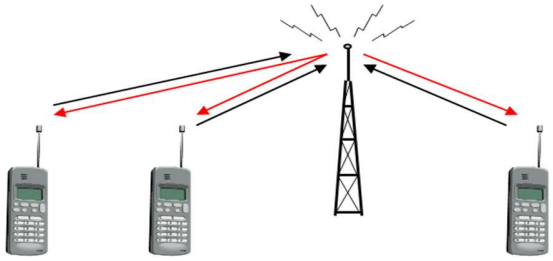


Figure 3.13 Inhibit sense multiple access using a busy tone

l. Define selective retransmission.

A very useful extension of TCP is the use of selective retransmission. TCP acknowledgements are cumulative, i.e., they acknowledge in-order receipt of packets up to a certain packet. If a single packet is lost, the sender has to retransmit everything starting from the lost packet (go-back-n retransmission). This obviously wastes bandwidth, not just in the case of a mobile network, but for any network. TCP can indirectly request a selective retransmission of packets. The receiver can acknowledge single packets, not only trains of in-sequence packets. The sender can now determine precisely which packet is needed and can retransmit it.

UNIT - I

9.

a. Define spread spectrum. How spreading is performed using DSSS? 6M

Spread spectrum techniques involve spreading the bandwidthneeded to transmit data – which does not make sense at first sight.Spreading the bandwidth has several advantages. The main advantage is theresistance to **narrowband interference**.

Direct sequence spread spectrum (DSSS) systems take a user bit stream and perform an (XOR) with a so-called chipping sequence as shown in Figure 2.35. The example shows that the result is either the sequence 0110101 (if the user bit equals 0) or its complement 1001010 (if the user bit equals 1). While each user bit has a duration t_b, the chipping sequence consists of smaller pulses, called chips, with a duration t_c. If the chipping sequence is generated properly it appears as random noise: this sequence is also sometimes called pseudo-noise sequence. The spreading factor $s = t_b/t_c$ determines the bandwidth of the resulting signal. If the original signal needs a bandwidth w, the resulting signal needs s*w after spreading. While the spreading factor of the very simple example is only 7 (and the chipping sequence 0110101 is not very random). Barker codes exhibit a good robustness against interference and insensitivity to multi-path propagation.

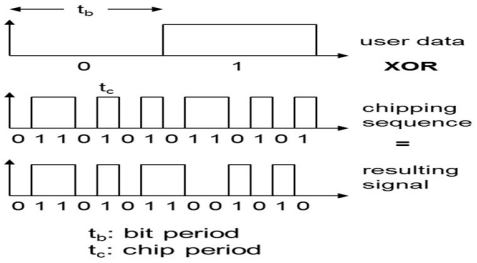


Figure 2.34 Spread spectrum to avoid narrowband interference

Transmitters and receivers using DSSS need additional components as shown in the simplified block diagrams in Figure 2.36 and Figure 2.37. The first step in a DSSS transmitter, Figure 2.36 is the spreading of the user data with the chipping sequence (digital modulation). The spread signal is then modulated

with a radio carrier. Assuming for example a user signal with a bandwidth of 1 MHz. Spreading with the above 11-chip Barker code would result in a signal with 11 MHz bandwidth. The radio carrier then shifts this signal to the carrier frequency. This signal is then transmitted.

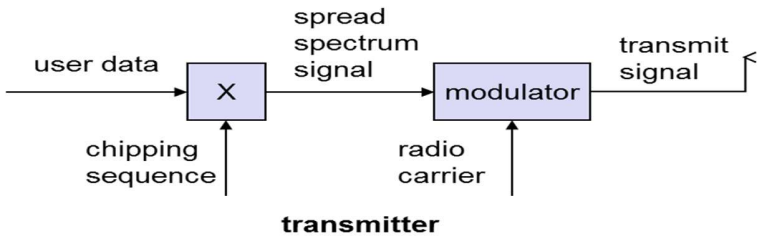


Figure 2.36 DSSS transmitter

The DSSS receiver is more complex than the transmitter. The receiver only has to perform the inverse functions of the two transmitter modulation steps. However, noise and multi-path propagation require additional mechanisms to reconstruct the original data. The first step in the receiver involves demodulating the received signal. This is achieved using the same carrier as the transmitter reversing the modulation and results in a signal with approximately the same bandwidth as the original spread spectrum signal. Additional filtering can be applied to generate this signal.

While demodulation is well known from ordinary radio receivers, the next steps constitute a real challenge for DSSS receivers, contributing to the complexity of the system. The receiver has to know the original chipping sequence, i.e., the receiver basically generates the same pseudo random sequence as the transmitter. Sequences at the sender and receiver have to be precisely synchronized because the receiver calculates the product of a chip with the incoming signal. This comprises another XOR operation, together with a medium access mechanism that relies on this scheme. During a bit period, which also has to be derived via synchronization, an integrator adds all these products. Calculating the products of chips and signal, and adding the products in an integrator is also called correlation, the device a correlator. Finally, in each bit period a decision unit samples the sums generated by the integrator and decides if this sum represents a binary 1 or a 0.

If transmitter and receiver are perfectly synchronized and the signal is not too distorted by noise or multi-path propagation, DSSS works perfectly well according to the simple scheme shown. Sending the user data 01 and applying the 11-chip Barker code 10110111000 results in the spread 'signal' 10110111000001001000111. On the receiver side, this 'signal' is XORed bit-wise after demodulation with the same Barker code as chipping sequence. This results in the sum of products equal to 0 for the first bit and to 11 for the second bit. The decision unit can now map the first sum (=0) to a binary 0, the second sum (=11) to a binary 1 – this constitutes the original user data.

In real life, the situation is somewhat more complex. Assume that the demodulated signal shows some distortion, e.g., 10100101000011010000111. The sum of products for the first bit would be 2, 10 for the second bit. Still, the decision unit can map, e.g., sums less than 4 to a binary 0 and sums larger than 7 to a binary 1. However, it is important to stay synchronized with the transmitter of a signal.

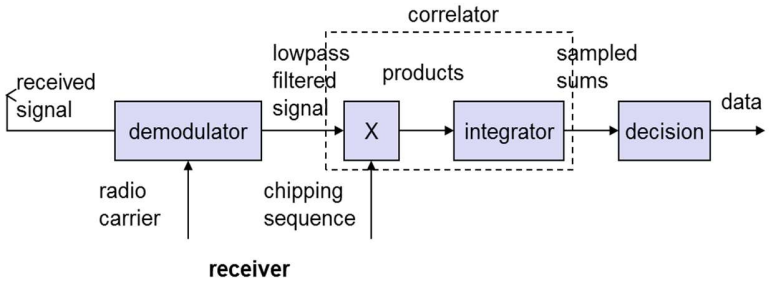


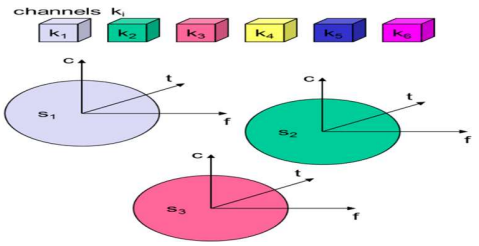
Figure 2.37 DSSS receiver

b. Compare SDM, FDM and TDM multiplexing schemes. 6M

Space Division Multiplexing is used for allocating a separated space to users in wireless networks. Single users are separated in space by individual beams. The basis for the SDMA algorithm is formed by cells and sectorized antennas which constitute the infrastructure implementing space division multiple access. SDMA is used in combinations of FDM, TDM or CDM.

The following diagram shows six channels K_i and introduces a three dimensional coordinate system. This system shows the dimensions of code c, time t, and frequency f. Here space is represented via circles indicating the interference range. The channels k_1 to k_3 can be mapped onto the three spaces s_1 to s_3 which clearly separate the channels and prevent the interference ranges from overlapping. The space between the interference ranges is sometimes called guard space. Such a guard space is needed in all four multiplexing schemes.

For the remaining channels (k_4 to k_6) three additional spaces would be needed. In wireless transmission, SDM implies a separate sender for each communication channel with a wide enough distance between senders. 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.

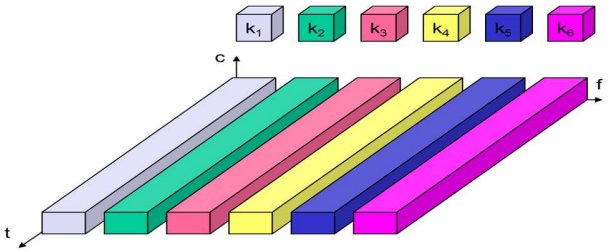


Frequency Division Multiplexing:
In this scheme separation of the whole spectrum into smaller frequency bands. A channel gets a certain band of the spectrum for the whole time.
Advantages:

- no dynamic coordination necessary
- works also for analog signals

Disadvantages:

- waste of bandwidth if the traffic is distributed unevenly
- inflexible
- guard spaces



Time Division Multiplexing

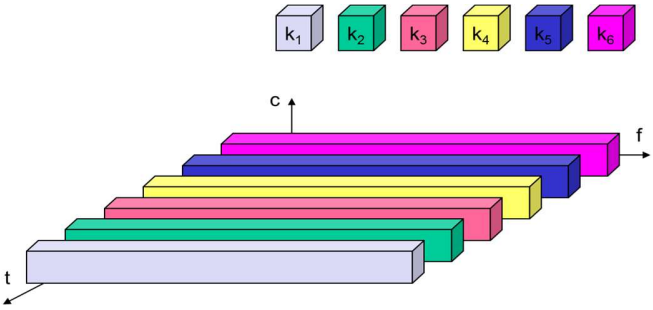
A channel gets the whole spectrum for a certain amount of time

Advantages:

- only one carrier in the medium at any time
- throughput high even for many users

Disadvantages:

- precise synchronization necessary



(OR)

10.

a. Why specialized MAC is needed in wireless environment? 6M

Carrier sense multiple access with collision detection, (CSMA/CD) which works as follows. A sender senses the medium (a wire or coaxial cable) to see if it is free. If the medium is busy, the sender waits until it is free. If the medium is free, the sender starts transmitting data and continues to listen into the medium. If the sender detects a collision while sending, it stopsat once and sends a jamming signal.

CSMA/CD is not reallyinterested in collisions at the sender, but rather in those at the receiver. Thesignal should reach the receiver without collisions. But the sender is the onedetecting collisions. This is not a problem using a wire, as more or less the samesignal strength can be assumed all over the wire if the

length of the wire stayswithin certain often standardized limits. If a collision occurs somewhere in thewire, everybody will notice it. It does not matter if a sender listens into themedium to detect a collision at its own location while in reality is waiting todetect a possible collision at the receiver.

The situation is different in wireless networks. Thestrength of a signal decreases proportionally to the square of the distance to thesender. Obstacles attenuate the signal even further. The sender may now applycarrier sense and detect an idle medium. The sender starts sending – but a collisionhappens at the receiver due to a second sender. The same can happen to the collision detection. Thesender detects no collision and assumes that the data has been transmittedwithout errors, but a collision might actually have destroyed the data at thereceiver. Collision detection is very difficult in wireless scenarios as the transmissionpower in the area of the transmitting antenna is several magnitudeshigher than the receiving power. So, this very common MAC scheme fromwired network fails in a wireless scenario.

1 Hidden and exposed terminals

Consider the scenario with three mobile phones. Thetransmission range of A reaches B, but not C (the detection range does notreach C either). The transmission range of C reaches B, but not A. Finally, thetransmission range of B reaches A and C, i.e., A cannot detect C and vice versa.

A starts sending to B, C does not receive this transmission. C also wants tosend something to B and senses the medium. The medium appears to be free,the carrier sense fails. C also starts sending causing a collision at B. But A cannotdetect this collision at B and continues with its transmission. A is **hidden** for Cand vice versa.

While hidden terminals may cause collisions, the next effect only causes unnecessary delay. Now consider the situation that B sends something to A and C wants to transmit data to some other mobile phone outside the interference ranges of A and B. C senses the carrier and detects that the carrier is busy (B's signal). C postpones its transmission until it detects the medium as being idle again. But as A is outside the interference range of C, waiting is not necessary.Causing a 'collision' at B does not matter because the collision is too weak to propagate to A. In this situation, C is **exposed** to B.

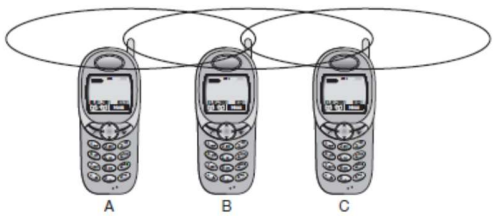


Figure 3.1
Hidden and exposed terminals

2 Near and far terminals

Consider the situation as shown in Figure 3.2. A and B are both sending with the same transmission power. As the signal strength decreases proportionally to the square of the distance, B's signal drowns out A's signal. As a result, C cannot receive A's transmission.

Now think of C as being an arbiter for sending rights. In this case, terminal B would already drown out terminal A on the physical layer. C in return would have no chance of applying a fair scheme as it would only hear B.

The **near/far effect** is a severe problem of wireless networks using CDM. All signals should arrive at the receiver with more or less the same strength. Otherwise a person standing closer to somebody could always speak louder than a person further away. Even if the senders were separated by code, the closest one would simply drown out the others. Precise power control is needed to receive all senders with the same strength at a receiver.

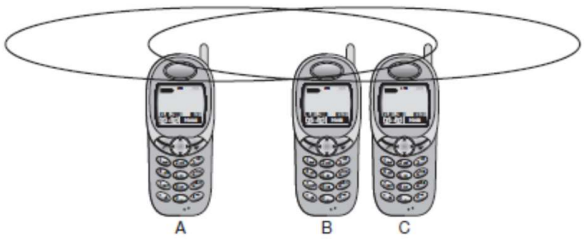


Figure 3.2
Near and far terminals

b. Describe PRMA and MACA schemes. 6M

PRMA (Packet Reservation Multiple Access)
An example for an implicit reservation scheme is PRMA. Here, slots can be reserved implicitly according to the following scheme. A certain number of slots forms a frame (Figure 3.8 shows eight slots in a frame). The frame is repeated in time (forming frames one to five in the example), i.e., a fixed TDM pattern is applied.

A base station, now broadcasts the status of each slot (as shown on the left side of the figure) to all mobile stations. All stations receiving this vector will then know which slot is occupied and which slot is currently free. In the illustration, a successful transmission of data is indicated by the station's name (A to F). In the example, the base station broadcasts the reservation status 'ACDABA-F' to all stations, here A to F. This means that slots one to six and eight are occupied, but slot seven is free in the following transmission. All stations wishing to transmit can now compete for this free slot in Aloha fashion. The already occupied slots are not touched. In the example shown, more than one station wants to access this slot, so a collision occurs. The base station returns the reservation status 'ACDABA-F', indicating that the reservation of slot seven failed (still indicated as free) and that nothing has changed for the other slots. Again, stations can compete for this slot. Additionally, station D has stopped sending in slot three and station F in slot eight. This is noticed by the base station after the second frame.

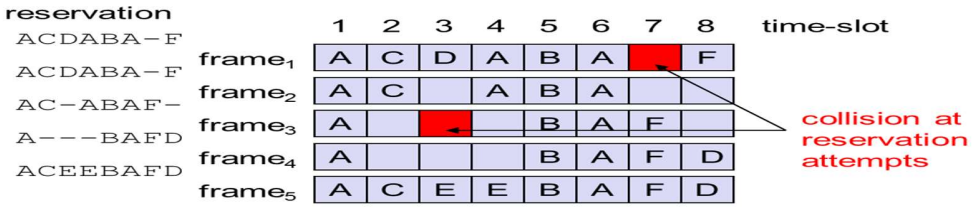
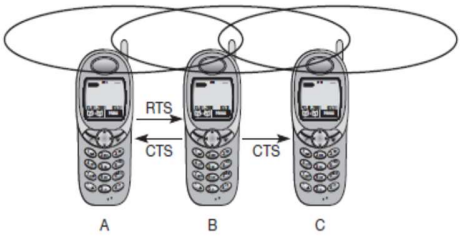


Figure 3.8 Demand assignment multiple access with implicit reservation

MACA (Multiple Access with Collision Avoidance)
Itpresents a simple scheme that solves the hidden terminal problem, does not need a base station, and is still a random access Aloha scheme – but with dynamic reservation. A and C both want to send to B. A

has already started the transmission, but is hidden for C, C also starts with its transmission, thereby causing a collision at B.

Figure 3.10
MACA can avoid hidden terminals



With MACA, A does not start its transmission at once, but sends a **request to send (RTS)** first. B receives the RTS that contains the name of sender and receiver, as well as the length of the future transmission. This RTS is not heard by C, but triggers an acknowledgement from B, called **clear to send (CTS)**. The CTS again contains the names of sender (A) and receiver (B) of the user data, and the length of the future transmission. This CTS is now heard by C and the medium for future use by A is now reserved for the duration of the transmission. After receiving a CTS, C is not allowed to send anything for the duration indicated in the CTS toward B. A collision cannot occur at B during data transmission, and the hidden terminal problem is solved – provided that the transmission conditions remain the same. (Another station could move into the transmission range of B after the transmission of CTS.)

Still, collisions can occur during the sending of an RTS. Both A and C could send an RTS that collides at B. RTS is very small compared to the data transmission, so the probability of a collision is much lower. B resolves this contention and acknowledges only one station in the CTS (if it was able to recover the RTSat all). No transmission is allowed without an appropriate CTS. This is one of the medium access schemes that is optionally used in the standard IEEE 802.11.

Remember, B wants to send data to A, C to someone else. But C is polite enough to sense the medium before transmitting, sensing a busy medium caused by the transmission from B. C defers, although C could never cause a collision at A.

With MACA, B has to transmit an RTS first (as shown in Figure 3.11) containing the name of the receiver (A) and the sender (B). C does not react to this message as it is not the receiver, but A acknowledges using a CTS which identifies B as the sender and A as the receiver of the following data transmission. Cdoes not receive this CTS and concludes that A is outside the detection range. C can start its transmission assuming it will not cause a collision at A. The problem with exposed terminals is solved without fixed access patterns or a base station. One problem of MACA is clearly the overheads associated with the RTS and CTS transmissions – for short and time-critical data packets, this is not negligible. MACA also assumes symmetrical transmission and reception conditions. Otherwise, a strong sender, directed antennas etc. could counteract the above scheme.

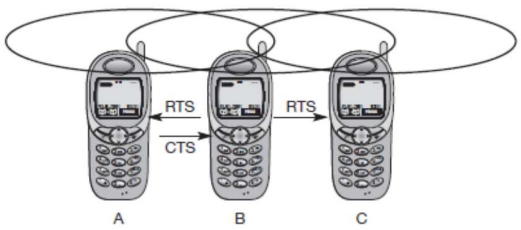


Figure 3.11
MACA can avoid exposed terminals

UNIT – II

11.

a. Draw the function architecture of GSM and explain? 8M

GSM comes with a hierarchical, complex system architecture comprising many entities, interfaces, and acronyms. A GSM system consists of three subsystems, the **radio sub system (RSS)**, the **network and switching subsystem (NSS)**, and the **operation subsystem (OSS)**. Generally, a GSM customer only notices a very small fraction of the whole network – the mobile stations (MS) and some antenna masts of the base transceiver stations (BTS).

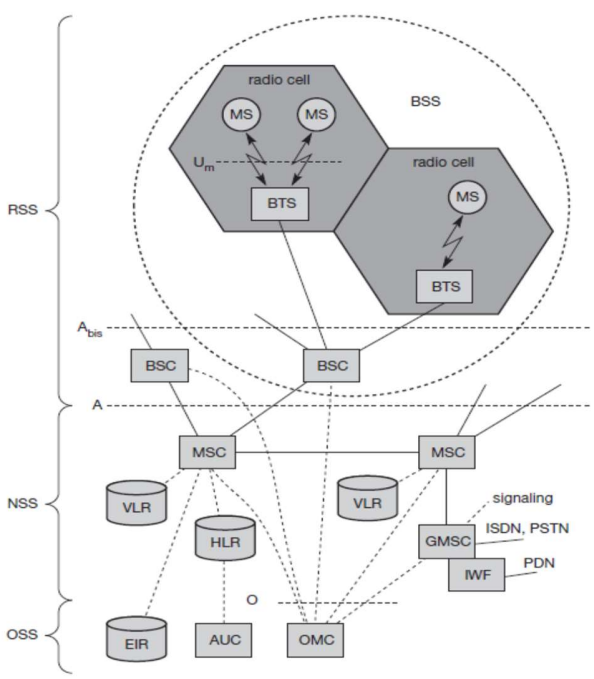


Figure 4.4
Functional architecture of a GSM system

1 Radio subsystem

The **radio subsystem (RSS)** comprises all radio specific entities, i.e., the **mobile stations (MS)** and the **base station subsystem (BSS)**. The above diagram shows the connection between the RSS and the NSS via the **A interface** (solid lines) and the connection to the OSS via the **O interface** (dashed lines). The A interface is typically based on circuit-switched PCM-30 systems (2.048 Mbit/s), carrying up to 30 64 kbit/s connections, whereas the O interface uses the Signalling System No. 7 (SS7) based on X.25 carrying management data to/from the RSS.

- **Base station subsystem (BSS)**: A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.
- **Base transceiver station (BTS)**: A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission. A BTS can form a radio cell or, using sectorized antennas, several cells, and is connected to MS via the **Um interface**, and to the BSC via the **A_{bis} interface**. The Um interface contains all the mechanisms necessary for wireless transmission and will be discussed in more detail below. The **A_{bis}** interface consists of 16 or 64 kbit/s connections. A GSM cell can measure between some 100 m and 35 km depending on the environment (buildings, open space, mountains etc.) but also expected traffic.
- **Base station controller (BSC)**: The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.
- **Mobile station (MS)**: The MS comprises all user equipment and software needed for communication with a GSM network. An MS consists of user independent hard- and software and of the **subscriber identity module (SIM)**, which stores all user-specific data that is relevant to GSM. While an MS can be identified via the **international mobile equipment identity (IMEI)**, a user can personalize any MS using his or her SIM, i.e., user-specific mechanisms like charging and authentication are based on the SIM, not on the device itself. Device-specific mechanisms, e.g., theft protection, use the device specific IMEI. Without the SIM, only emergency calls are possible. The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a **personal identity number (PIN)**, a **PIN unblocking key (PUK)**, an **authentication key Ki**, and the **international mobile subscriber identity (IMSI)**. The PIN is used to unlock the MS. Using the wrong PIN three times will lock the SIM. In such cases, the PUK is needed to unlock the SIM. The MS stores dynamic information while logged onto the GSM system, such as, e.g., the **cipher key Kc** and the location information consisting of a **temporary mobile subscriber identity (TMSI)** and the **location area identification (LAI)**. Typical MSs for GSM 900 have a transmit power of up to 2 W, whereas for GSM 1800 1 W is enough due to the smaller cell size. Apart from the telephone interface, an MS can also offer other types of interfaces to users with display, loudspeaker, microphone, and programmable soft keys. Further interfaces comprise computer modems, IrDA, or Bluetooth. Typical MSs, e.g., mobile phones, comprise many more vendor-specific functions and components, such as cameras, fingerprint sensors, calendars, address books, games, and Internet browsers. Personal digital assistants (PDA) with mobile phone functions are also available. The reader should be aware that an MS could also be integrated into a car or be used for location tracking of a container.

2 Network and switching subsystem

The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries. The NSS consists of the following switches and databases:

- **Mobile services switching center (MSC)**: MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the fixed backbone network of a GSM system. Typically, an MSC manages several BSCs in a geographical region. A **gateway MSC (GMSC)** has additional connections to other fixed networks, such as **PSTN** and **ISDN**. Using additional **interworking functions (IWF)**, an MSC can also connect to

public data networks (PDN) such as X.25. An MSC handles all signaling needed for connection setup, connection release and handover of connections to other MSCs. The **standard signaling system No. 7 (SS7)** is used for this purpose. SS7 covers all aspects of control signaling for digital networks (reliable routing and delivery of control messages, establishing and monitoring of calls). Features of SS7 are number portability, free phone/toll/collect/credit calls, call forwarding, three-way calling etc. An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.

- **Home location register (HLR)**: The HLR is the most important database in a GSM system as it stores all user-relevant information. This comprises static information, such as the **mobile subscriber ISDN number (MSISDN)**, subscribed services (e.g., call forwarding, roaming restrictions, GPRS), and the **international mobile subscriber identity (IMSI)**. Dynamic information is also needed, e.g., the current **location area (LA)** of the MS, the **mobile subscriber roaming number (MSRN)**, the current VLR and MSC. As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network. All these user-specific information elements only exist once for each user in a single HLR, which also supports charging and accounting. HLRs can manage data for several million customers and contain highly specialized data bases which must fulfill certain real-time requirements to answer requests within certain time-bounds.
- **Visitor location register (VLR)**: The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI, MSISDN, HLR address). If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR. This hierarchy of VLR and HLR avoids frequent HLR updates and long-distance signaling of user information.

3 Operation subsystem

The **operation subsystem (OSS)**, contains the necessary functions for network operation and maintenance. The OSS possesses network entities of its own and accesses other entities via SS7 signaling. The following entities have been defined:

- **Operation and maintenance center (OMC)**: The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing.
- **Authentication centre (AuC)**: As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission. The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR.
- **Equipment identity register (EIR)**: The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network. As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices. In theory an MS is useless as soon as the owner has reported a theft. Unfortunately, the blacklists of different providers are not usually synchronized and the illegal use of a device in another operator's network is possible (the reader may speculate as to why this is the case). The EIR also contains a list of valid IMEIs (white list), and a list of malfunctioning devices (gray list).

b. Explain MTC and MOC in GSM. 4M

Mobile terminated call (MTC), i.e., a situation in which a station calls a mobile station (the calling station could be outside the GSM network or another mobile station). Figure 4.8 shows the basic steps needed to connect the calling station with the mobile user. In step 1, a user dials the phone number of a

GSM subscriber. The fixed network (PSTN) notices (looking at the destination code) that the number belongs to a user in the GSM network and forwards the call setup to the Gateway MSC (2). The GMSC identifies the HLR for the subscriber (which is coded in the phone number) and signals the call setup to the HLR (3). The HLR now checks whether the number exists and whether the user has subscribed to the requested services, and requests an MSRN from the current VLR (4). After receiving the MSRN (5), the HLR can determine the MSC responsible for the MS and forwards this information to the GMSC (6). The GMSC can now forward the call setup request to the MSC indicated (7).

From this point on, the MSC is responsible for all further steps. First, it requests the current status of the MS from the VLR (8). If the MS is available, the MSC initiates paging in all cells it is responsible for (i.e. the location area, LA, 10), as searching for the right cell would be too time consuming (but this approach puts some load on the signaling channels so optimizations exist). The BTSs of all BSSs transmit this paging signal to the MS (11). If the MS answers (12 and 13), the VLR has to perform security checks (set up encryption etc.). The VLR then signals to the MSC to set up a connection to the MS (steps 15 to 17).

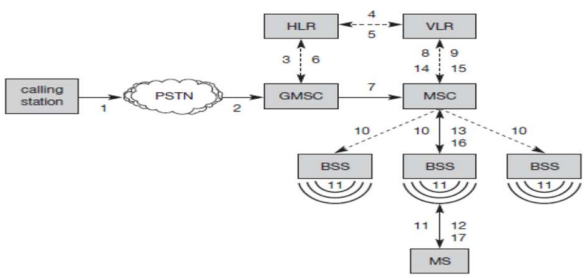


Figure 4.8
Mobile terminated call (MTC)

It is much simpler to perform a **mobile originated call (MOC)** compared to a MTC (see Figure 4.9). The MS transmits a request for a new connection (1), the BSS forwards this request to the MSC (2). The MSC then checks if this user is allowed to set up a call with the requested service (3 and 4) and checks the availability of resources through the GSM network and into the PSTN. If all resources are available, the MSC sets up a connection between the MS and the fixed network.

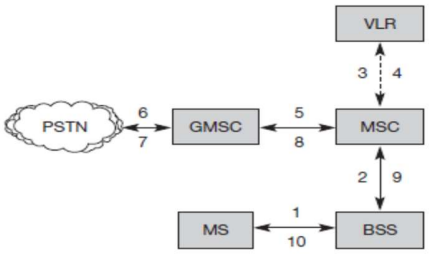


Figure 4.9
Mobile originated call (MOC)

(OR)

12.

a. Write in detail about the main components of the UMTS reference architecture. 8M

The following diagram shows the very simplified UMTS reference architecture. The **UTRA network (UTRAN)** handles cell level mobility and comprises several **radio network subsystems (RNS)**. The functions of the RNS include radio channel ciphering and deciphering, handover control, radio resource management etc. The UTRAN is connected to the **user equipment (UE)** via the radio interface **Uu**. Via

the **Iu** interface, UTRAN communicates with the **core network (CN)**. The CN contains functions for inter-system handover, gateways to other networks (fixed or wireless), and performs location management if there is no dedicated connection between UE and UTRAN.

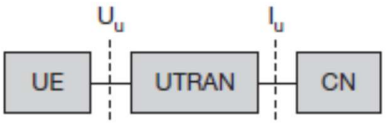


Figure 4.24 Main components of the UMTS reference architecture

b. List and explain different types of satellite orbits? 4M

Geostationary Earth Orbit: This orbit has a distance of almost 36,000 km to the earth. Three GEO satellites are enough for a complete coverage of almost any spot on earth. Life time of GEO satellites are 15 years. They don't need a handover due to large footprint. Examples are all TV and radio broadcast satellites, many weather satellites and satellites operating as backbones for the telephone network.

Low Earth Orbit: This orbit has a distance of 500-1500 km to the earth. LEO systems have a high elevation for every spot on earth to provide a high quality communication link. Each LEO satellite will only be visible from the earth for around ten minutes. For global coverage we need 50-200 or even more LEO satellites. The delay for packet delivery via a LEO is relatively low (approximately 10 ms).

Medium Earth Orbit: MEOs operates at a distance of about 5,000-12,000 km to the earth. This system requires a dozen satellites. These satellites move more slowly relative to the earth's rotation allowing a simpler system design. They cover larger populations, so requiring fewer handovers.

Highly elliptical orbit (HEO): This class comprises all satellites with noncircular orbits. Currently, only a few commercial communication systems using satellites with elliptical orbits are planned. These systems have their perigee over large cities to improve communication quality.

UNIT – III

13.

a. Draw the IEEE 802.11 MAC packet structure and explain each field? 6M

Figure 7.16 shows the basic structure of an IEEE 802.11 MAC data frame together with the content of the frame control field. The fields in the figure refer to the following:

- **Frame control:** The first 2 bytes serve several purposes. They contain several sub-fields as explained after the MAC frame.
- **Duration/ID:** If the field value is less than 32,768, the duration field contains the value indicating the period of time in which the medium is occupied (in μs). This field is used for setting the NAV for the virtual reservation mechanism using RTS/CTS and during fragmentation. Certain values above 32,768 are reserved for identifiers.
- **Address 1 to 4:** The four address fields contain standard IEEE 802 MAC addresses (48 bit each), as they are known from other 802.x LANs. The meaning of each address depends on the DS bits in the frame control field and is explained in more detail in a separate paragraph.
- **Sequence control:** Due to the acknowledgement mechanism frames may be duplicated. Therefore a sequence number is used to filter duplicates.
- **Data:** The MAC frame may contain arbitrary data (max. 2,312 byte), which is transferred transparently from a sender to the receiver(s).
- **Checksum (CRC):** Finally, a 32 bit checksum is used to protect the frame as it is common practice in all 802.x networks.

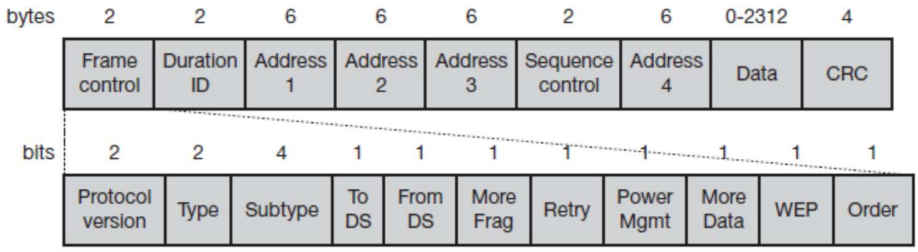


Figure 7.16 IEEE 802.11 MAC packet structure

The frame control field shown in Figure 7.16 contains the following fields:

- **Protocol version:** This 2 bit field indicates the current protocol version and is fixed to 0 by now. If major revisions to the standard make it incompatible with the current version, this value will be increased.
- **Type:** The type field determines the function of a frame: management (=00), control (=01), or data (=10). The value 11 is reserved. Each type has several subtypes as indicated in the following field.
- **Subtype:** Example subtypes for management frames are: 0000 for association request, 1000 for beacon. RTS is a control frame with subtype 1011, CTS is coded as 1100. User data is transmitted as data frame with subtype 0000. All details can be found in IEEE, 1999.
- **To DS/From DS:** Explained in the following in more detail.
- **More fragments:** This field is set to 1 in all data or management frames that have another fragment of the current MSDU to follow.
- **Retry:** If the current frame is a retransmission of an earlier frame, this bit is set to 1. With the help of this bit it may be simpler for receivers to eliminate duplicate frames.
- **Power management:** This field indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
- **More data:** In general, this field is used to indicate a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered. Or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.
- **Wired equivalent privacy (WEP):** This field indicates that the standard security mechanism of 802.11 is applied. However, due to many weaknesses found in the WEP algorithm higher layer security should be used to secure an 802.11 network.
- **Order:** If this bit is set to 1 the received frames must be processed in strict order.

MAC frames can be transmitted between mobile stations; between mobile stations and an access point and between access points over a DS. Two bits within the Frame Control field, '**to DS**' and '**from DS**', differentiate these cases and control the meaning of the four addresses used. Table 7.1 gives an overview of the four possible bit values of the DS bits and the associated interpretation of the four address fields.

to DS	from DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	–
0	1	DA	BSSID	SA	–
1	0	BSSID	SA	DA	–
1	1	RA	TA	DA	SA

Table 7.1 Interpretation of the MAC addresses in an 802.11 MAC frame

Every station, access point or wireless node, filters on **address 1.** This address identifies the physical receiver(s) of the frame. Based on this address, a station can decide whether the frame is relevant or not. The second address, **address 2**, represents the physical transmitter of a frame. This information is important because this particular sender is also the recipient of the MAC layer acknowledgement. If a packet from a transmitter (address 2) is received by the receiver with address 1, this receiver in turn acknowledges the data packet using address 2 as receiver address as shown in the ACK packet in Figure 7.17. The remaining two addresses, **address 3** and **address 4**, are mainly necessary for the logical assignment of frames (logical sender, BSS identifier, logical receiver). If address 4 is not needed the field is omitted.

For addressing, the following four scenarios are possible:

- **Ad-hoc network:** If both DS bits are zero, the MAC frame constitutes a packet which is exchanged between two wireless nodes without a distribution system. **DA** indicates the **destination address**, **SA** the **source address** of the frame, which are identical to the physical receiver and sender addresses respectively. The third address identifies the **basic service set (BSSID)**, the fourth address is unused.
- **Infrastructure network, from AP:** If only the 'from DS' bit is set, the frame physically originates from an access point. DA is the logical and physical receiver, the second address identifies the BSS, the third address specifies the logical sender, the source address of the MAC frame. This case is an example for a packet sent to the receiver via the access point.
- **Infrastructure network, to AP:** If a station sends a packet to another station via the access point, only the 'to DS' bit is set. Now the first address represents the physical receiver of the frame, the access point, via the BSS identifier. The second address is the logical and physical sender of the frame, while the third address indicates the logical receiver.
- **Infrastructure network, within DS:** For packets transmitted between two access points over the distribution system, both bits are set. The first **receiver address (RA)**, represents the MAC address of the receiving access point. Similarly, the second address **transmitter address (TA)**, identifies the sending access point within the distribution system. Now two more addresses are needed to identify the original destination DA of the frame and the original source of the frame SA. Without these additional addresses, some encapsulation mechanism would be necessary to transmit MAC frames over the distribution system transparently.

Figure 7.17 shows three control packets as examples for many special packets defined in the standard. The **acknowledgement packet (ACK)** is used to acknowledge the correct reception of a data frame. The receiver address is directly copied from the address 2 field of the immediately previous frame. If no more fragments follow for a certain frame the duration field is set to 0. Otherwise the duration value of the previous frame (minus the time required to transmit the ACK minus SIFS) is stored in the duration field.

For the MACA algorithm the RTS/CTS packets are needed. These packets have to reserve the medium to avoid collisions. Therefore, the **request to send (RTS)** packet contains the receiver address of the intended recipient of the following data transfer and the transmitter address of the station transmitting the RTS packet. The duration (in μs) comprises the time to send the CTS, data, and ACK plus three SIFS. The immediately following **clear to send (CTS)** frame copies the transmitter address from the RTS packet into its receiver address field. Additionally, it reads the duration field, subtracts the time to send the CTS and a SIFS and writes the result into its own duration field.

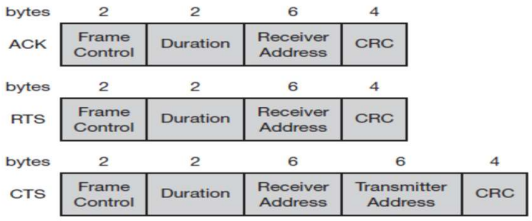


Figure 7.17
IEEE 802.11 special control packets: ACK, RTS, and CTS

b. Explain DFWMAC-DCF schemes with neat sketches? 6M

1 Basic DFWMAC-DCF using CSMA/CA

The mandatory access mechanism of IEEE 802.11 is based on **carrier sense multiple access with collision avoidance** (CSMA/CA), which is a random access scheme with carrier sense and collision avoidance through random backoff. The basic CSMA/CA mechanism is shown in Figure 7.10. If the medium is idle for at least the duration of DIFS (with the help of the CCA signal of the physical layer), a node can access the medium at once. This allows for short access delay under light load. But as more and more nodes try to access the medium, additional mechanisms are needed.

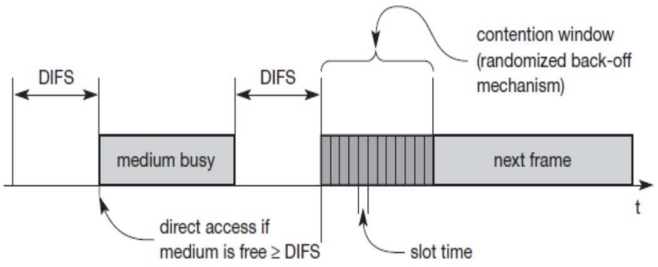


Figure 7.10
Contention window and waiting time

If the medium is busy, nodes have to wait for the duration of DIFS, entering a contention phase afterwards. Each node now chooses a **random backoff time** within a **contention window** and delays medium access for this random amount of time. The node continues to sense the medium. As soon as a node senses the channel is busy, it has lost this cycle and has to wait for the next chance, i.e., until the medium is idle again for at least DIFS. But if the randomized additional waiting time for a node is over and the medium is still idle, the node can access the medium immediately (i.e., no other node has a shorter waiting time). The additional waiting time is measured in multiples of the above-mentioned slots. This additional randomly distributed delay helps to avoid collisions – otherwise all stations would try to transmit data after waiting for the medium becoming idle again plus DIFS.

Obviously, the basic CSMA/CA mechanism is not fair. Independent of the overall time a node has already waited for transmission; each node has the same chances for transmitting data in the next cycle. To provide fairness, IEEE 802.11 adds a **backoff timer.** Again, each node selects a random waiting time within the range of the contention window. If a certain station does not get access to the medium in the first cycle, it stops its backoff timer, waits for the channel to be idle again for DIFS and starts the counter again. As soon as the counter expires, the node accesses the medium. This means that deferred stations do not choose a randomized backoff time again, but continue to count down. Stations that have waited longer have the advantage over stations that have just entered, in that they only have to wait for the remainder of their backoff timer from the previous cycle(s).

Figure 7.11 explains the basic access mechanism of IEEE 802.11 for five stations trying to send a packet at the marked points in time. Station3 has the first request from a higher layer to send a packet (packet arrival at the MAC SAP). The station senses the medium, waits for DIFS and accesses the medium, i.e., sends the packet. Station1, station2, and station5 have to wait at least until the medium is idle for DIFS again after station3 has stopped sending. Now all three stations choose a backoff time within the contention window and start counting down their backoff timers.

Figure 7.11 shows the random backoff time of station1 as sum of boe (the elapsed backoff time) and bor (the residual backoff time). The same is shown for station5. Station2 has a total backoff time of only boe and gets access to the medium first. No residual backoff time for station2 is shown. The backoff timers of station1 and station5 stop, and the stations store their residual backoff times. While a new station has to choose its backoff time from the whole contention window, the two old stations have statistically smaller backoff values. The older values are on average lower than the new ones.

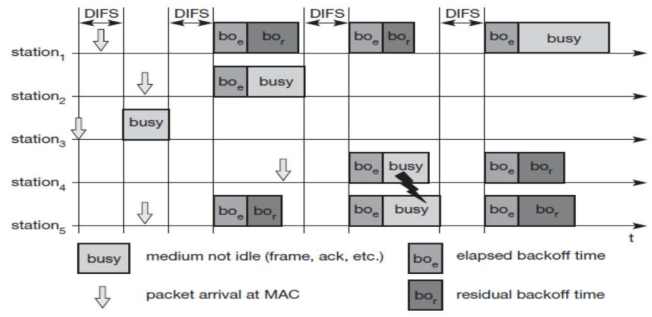


Figure 7.11
Basic DFWMAC–DCF with several competing senders

Now station4 wants to send a packet as well, so after DIFS waiting time, three stations try to get access. It can now happen, as shown in the figure, that two stations accidentally have the same backoff time, no matter whether remaining or newly chosen. This results in a collision on the medium as shown, i.e., the transmitted frames are destroyed. Station1 stores its residual backoff time again. In the last cycle shown station1 finally gets access to the medium, while station4 and station5 have to wait. A collision triggers a retransmission with a new random selection of the backoff time. Retransmissions are not privileged.

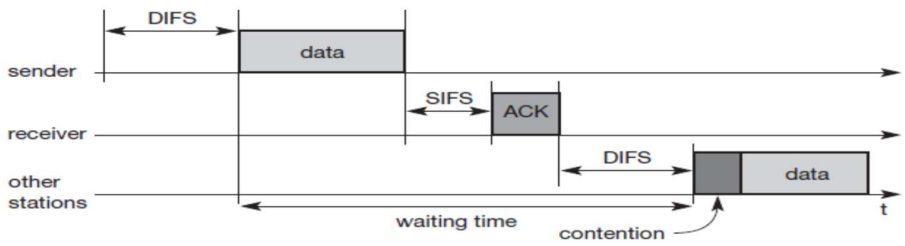
Still, the access scheme has problems under heavy or light load. Depending on the size of the contention window (CW), the random values can either be too close together (causing too many collisions) or the values are too high (causing unnecessary delay). The system tries to adapt to the current number of stations trying to send.

The contention window starts with a size of, e.g., CWmin = 7. Each time a collision occurs, indicating a higher load on the medium, the contention window doubles up to a maximum of, e.g., CWmax = 255

(the window can take on the values 7, 15, 31, 63, 127, and 255). The larger the contention window is, the greater is the resolution power of the randomized scheme. It is less likely to choose the same random backoff time using a large CW. However, under a light load, a small CW ensures shorter access delays. This algorithm is also called **exponential backoff** and is already familiar from IEEE 802.3 CSMA/CD in a similar version.

While this process describes the complete access mechanism for broadcast frames, an additional feature is provided by the standard for unicast data transfer. Figure 7.12 shows a sender accessing the medium and sending its data. But now, the receiver answers directly with an **acknowledgement (ACK)**. The receiver accesses the medium after waiting for a duration of SIFS so no other station can access the medium in the meantime and cause a collision. The other stations have to wait for DIFS plus their backoff time. This acknowledgement ensures the correct reception (correct checksum CRC at the receiver) of a frame on the MAC layer, which is especially important in error-prone environments such as wireless connections. If no ACK is returned, the sender automatically retransmits the frame. But now the sender has to wait again and compete for the access right. There are no special rules for retransmissions. The number of retransmissions is limited, and final failure is reported to the higher layer.

Figure 7.12
IEEE 802.11 unicast data transfer



2 DFWMAC-DCF with RTS/CTS extension

We discussed the problem of hidden terminals, a situation that can also occur in IEEE 802.11 networks. This problem occurs if one station can receive two others, but those stations cannot receive each other. The two stations may sense the channel is idle, send a frame, and cause a collision at the receiver in the middle. To deal with this problem, the standard defines an additional mechanism using two control packets, RTS and CTS. The use of the mechanism is optional; however, every 802.11 node has to implement the functions to react properly upon reception of RTS/CTS control packets.

Figure 7.13 illustrates the use of RTS and CTS. After waiting for DIFS (plus a random backoff time if the medium was busy), the sender can issue a **request to send (RTS)** control packet. The RTS packet thus is not given any higher priority compared to other data packets. The RTS packet includes the receiver of the data transmission to come and the duration of the whole data transmission. This duration specifies the time interval necessary to transmit the whole data frame and the acknowledgement related to it. Every node receiving this RTS now has to set its **net allocation vector (NAV)** in accordance with the duration field. The NAV then specifies the earliest point at which the station can try to access the medium again.

If the receiver of the data transmission receives the RTS, it answers with a **clear to send (CTS)** message after waiting for SIFS. This CTS packet contains the duration field again and all stations receiving this packet from the receiver of the intended data transmission have to adjust their NAV. The latter set of receivers need not be the same as the first set receiving the RTS packet. Now all nodes within receiving

distance around sender and receiver are informed that they have to wait more time before accessing the medium. Basically, this mechanism reserves the medium for one sender exclusively (this is why it is sometimes called a virtual reservation scheme).

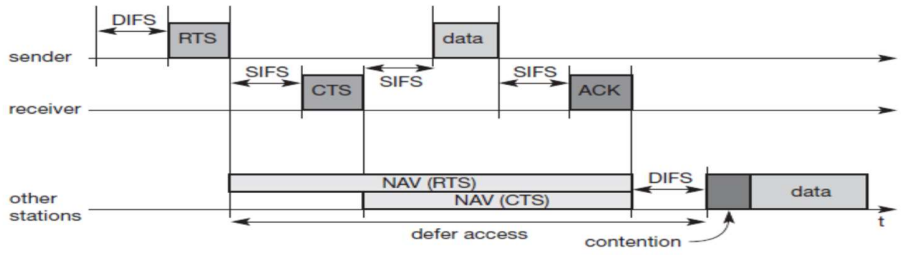


Figure 7.13
IEEE 802.11 hidden node provisions for contention-free access

Finally, the sender can send the data after SIFS. The receiver waits for SIFS after receiving the data packet and then acknowledges whether the transfer was correct. The transmission has now been completed, the NAV in each node marks the medium as free and the standard cycle can start again.

Within this scenario (i.e., using RTS and CTS to avoid the hidden terminal problem), collisions can only occur at the beginning while the RTS is sent. Two or more stations may start sending at the same time (RTS or other data packets). Using RTS/CTS can result in a non-negligible overhead causing a waste of bandwidth and higher delay. An RTS threshold can determine when to use the additional mechanism (basically at larger frame sizes) and when to disable it (short frames).

(OR)

14.

a. How packet delivery to and from the mobile is performed in mobile IP? 6M

IP packet delivery

Figure 8.2 illustrates packet delivery to and from the MN using the example network of Figure 8.1. A correspondent node CN wants to send an IP packet to the MN. One of the requirements of mobile IP was to support hiding the mobility of the MN. CN does not need to know anything about the MN's current location and sends the packet as usual to the IP address of MN (step 1). This means that CN sends an IP packet with MN as a destination address and CN as a source address. The internet, not having information on the current location of MN, routes the packet to the router responsible for the home network of MN. This is done using the standard routing mechanisms of the internet.

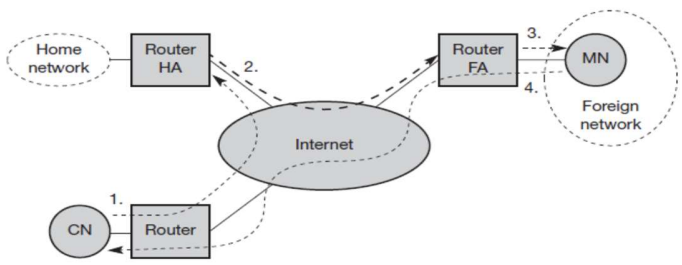


Figure 8.2
Packet delivery to and from the mobile node

The HA now intercepts the packet, knowing that MN is currently not in its home network. The packet is not forwarded into the subnet as usual, but encapsulated and tunnelled to the COA. A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet (step 2). The foreign agent now decapsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination to the MN (step 3). Again, for the MN mobility is not visible. It receives the packet with the same sender and receiver address as it would have done in the home network.

At first glance, sending packets from the MN to the CN is much simpler. The MN sends the packet as usual with its own fixed IP address as source and CN's address as destination (step 4). The router with the FA acts as default router and forwards the packet in the same way as it would do for any other node in the foreign network. As long as CN is a fixed node the remainder is in the fixed internet as usual. If CN were also a mobile node residing in a foreign network, the same mechanisms as described in steps 1 through 3 would apply now in the other direction.

b. Describe how a mobile node registration is performed. 6M

Having received a COA, the MN has to register with the HA. The main purpose of the registration is to inform the HA of the current location for correct forwarding of packets. Registration can be done in two different ways depending on the location of the COA.

- If the COA is at the FA, registration is done as illustrated in Figure 8.4. The MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now sets up a m**obility binding** containing the mobile node's home IP address and the current COA. Additionally, the mobility binding contains the lifetime of the registration which is negotiated during the registration process. Registration expires automatically after the lifetime and is deleted; so, an MN should reregister before expiration. This mechanism is necessary to avoid mobility bindings which are no longer used. After setting up the mobility binding, the HA sends a reply message back to the FA which forwards it to the MN.
- If the COA is co-located, registration can be simpler, as shown in Figure 8.4. The MN may send the request directly to the HA and vice versa. This, by the way, is also the registration procedure for MNs returning to their home network. Here they also register directly with the HA. However, if the MN received an agent advertisement from the FA it should register via this FA if the R bit is set in the advertisement.

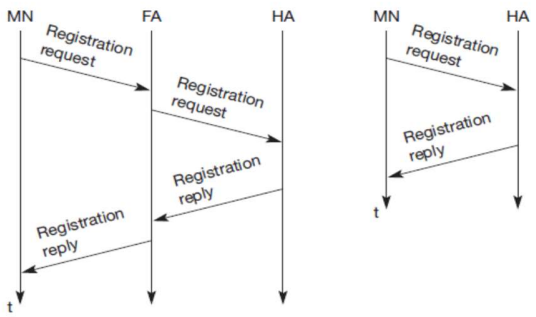


Figure 8.4 Registration of a mobile node via the FA or directly with the HA

UDP packets are used for **registration requests**. The IP source address of the packet is set to the interface address of the MN, the IP destination address is that of the FA or HA (depending on the location of the COA). The UDP destination port is set to 434. UDP is used because of low overheads and

better performance compared to TCP in wireless environments. The fields relevant for mobile IP registration requests follow as UDP data (see Figure 8.6). The fields are defined as follows.

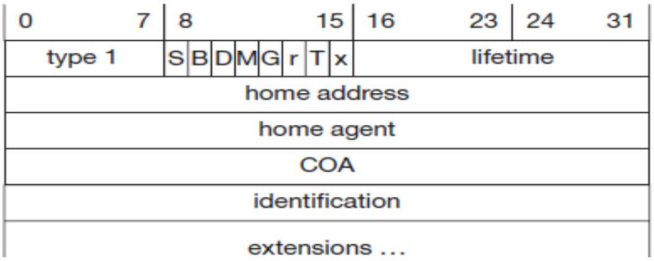
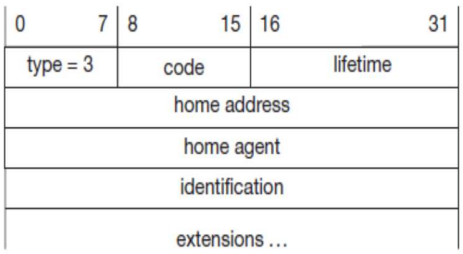


Figure 8.5
Registration request

The first field **type** is set to 1 for a registration request. With the **S** bit an MN can specify if it wants the HA to retain prior mobility bindings. This allows for simultaneous bindings. The following bits denote the requested behavior for packet forwarding. Setting the **B** bit generally indicates that an MN also wants to receive the broadcast packets which have been received by the HA in the home network. If an MN uses a co-located COA, it also takes care of the decapsulation at the tunnel endpoint. The **D** bit indicates this behavior. As already defined for agent advertisements, the following bits **M** and **G** denote the use of minimal encapsulation or generic routing encapsulation, respectively. **T** indicates reverse tunneling, **r** and **x** are set to zero.

Figure 8.6
Registration reply



Lifetime denotes the validity of the registration in seconds. A value of zero indicates deregistration; all bits set indicates infinity. The **home address** is the fixed IP address of the MN, **home agent** is the IP address of the HA, and **COA** represents the tunnel endpoint. The 64 bit **identification** is generated by the MN to identify a request and match it with registration replies. This field is used for protection against replay attacks of registrations. The **extensions** must at least contain parameters for authentication.

A **registration reply**, which is conveyed in a UDP packet, contains a **type** field set to 3 and a **code** indicating the result of the registration request. The **lifetime** field indicates how many seconds the registration is valid if It was successful. **Home address** and **home agent** are the addresses of the MN and the HA, respectively. The 64-bit **identification** is used to match registration requests with replies. The value is based on the identification field from the registration and the authentication method. Again, the **extensions** must at least contain parameters for authentication.

UNIT – IV

15.

c. With an example explain dynamic source routing algorithm? 8M

Dynamic source routing (DSR), therefore, divides the task of routing into two separate problems:

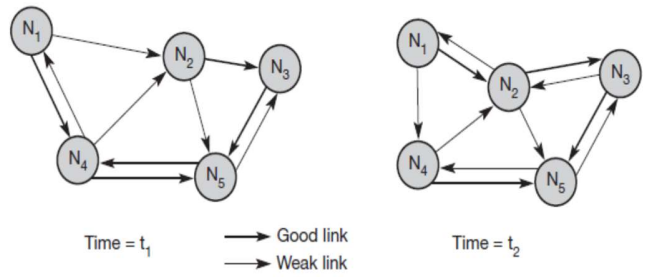
- **Route discovery:** A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.
- **Route maintenance:** If a node is continuously sending packets via a route,it has to make sure that the route is held upright. As soon as a node detectsproblems with the current route, it has to find an alternative.

The basic principle of source routing is also used in fixed networks, e.g.token rings. Dynamic source routing eliminates all periodic routing updates andworks as follows. If a node needs to discover a route, it broadcasts a routerequest with a unique identifier and the destination address as parameters. Anynode that receives a route request does the following.

- If the node has already received the request (which is identified using theunique identifier), it drops the request packet.
- If the node recognizes its own address as the destination, the request has reached its target.
- Otherwise, the node appends its own address to a list of traversed hops inthe packet and broadcasts this updated route request.

Using this approach, the router request collects a list of addresses representinga possible path on its way towards the destination. As soon as the requestreaches the destination, it can return the request packet containing the list tothe receiver using this list in reverse order. One condition for this is that thelinks work bi-directionally. If this is not the case, and the destination node doesnot currently maintain a route back to the initiator of the request, it has to starta route discovery by itself. The destination may receive several lists containingdifferent paths from the initiator. It could return the best path, the first path, orseveral paths to offer the initiator a choice.

Figure 8.20
Example ad-hoc network



Applying route discovery to the example in Figure 8.20 for a route from N1to N3 at time t1 results in the following.

- N1 broadcasts the request ((N1), id = 42, target = N3), N2 and N4 receivethis request.
- N2 then broadcasts ((N1, N2), id = 42, target = N3), N4 broadcasts ((N1, N4),id = 42, target = N3). N3 and N5 receive N2's broadcast, N1, N2, and N5receive N4's broadcast.
- N3 recognizes itself as target, N5 broadcasts ((N1, N2, N5), id = 42, target =N3). N3 and N4 receive N5's broadcast. N1, N2, and N5 drop N4's broadcastpacket, because they all recognize an already received route request (andN2's broadcast reached N5 before N4's did).
- N4 drops N5's broadcast, N3 recognizes (N1, N2, N5) as an alternate, butlonger route.

- N3 now has to return the path (N1, N2, N3) to N1. This is simple assumingsymmetric links working in both directions. N3 can forward the informationusing the list in reverse order.

The assumption of bi-directional links holds for many ad-hoc networks.However, if links are not bi-directional, the scenario gets more complicated. Thealgorithm has to be applied again, in the reverse direction if the target does notmaintain a current path to the source of the route request.

- N3 has to broadcast a route request ((N3), id = 17, target = N1). Only N5receives this request.
- N5 now broadcasts ((N3, N5), id = 17, target = N1), N3 and N4 receivethe broadcast.
- N3 drops the request because it recognizes an already known id. N4broadcasts ((N3, N5, N4), id = 17, target = N1), N5, N2, and N1 receivethe broadcast.
- N5 drops the request packet, N1 recognizes itself as target, and N2 broadcasts((N3, N5, N4, N2), id = 17, target = N1). N3 and N5 receive N2's broadcast.
- N3 and N5 drop the request packet.

Now N3 holds the list for a path from N1 to N3, (N1, N2, N3), and N1 knowsthe path from N3 to N1, (N3, N5, N4, N1). But N1 still does not know how to senddata to N3! The only solution is to send the list (N1, N2, N3) with the broadcastsinitiated by N3 in the reverse direction. This example shows clearly how muchsimpler routing can be if links are symmetrical.

The basic algorithm for route discovery can be optimized in many ways.

- To avoid too many broadcasts, each route request could contain a counter.Every node rebroadcasting the request increments the counter by one. Knowingthe maximum network diameter (take the number of nodes if nothing else isknown), nodes can drop a request if the counter reaches this number.
- A node can cache path fragments from recent requests. These fragments cannow be used to answer other route requests much faster.
- A node can also update this cache from packet headers while forwardingother packets.
- If a node overhears transmissions from other nodes, it can also use thisinformation for shortening routes.

After a route has been discovered, it has to be maintained for as long as thenode sends packets along this route. Depending on layer two mechanisms, differentapproaches can be taken:

- If the link layer uses an acknowledgementthe node can interpret this acknowledgement as an intact route.
- If possible, the node could also listen to the next node forwarding thepacket, so getting a passive acknowledgement.
- A node could request an explicit acknowledgement.

Again, this situation is complicated if links are not bi-directional. If a nodedetects connectivity problems, it has to inform the sender of a packet, initiatinga new route discovery starting from the sender. Alternatively, the node could tryto discover a new route by itself.

Although dynamic source routing offers benefits compared to other algorithmsby being much more bandwidth efficient, problems arise if the topologyis highly dynamic and links are asymmetrical.

d. Write about indirect TCP. 4M

Two competing insights led to the development of indirect TCP (I-TCP). One is that TCP performs poorly together with wireless links; the other is that TCP within the fixed network cannot be changed. I-TCP segments a TCP connection into a fixed part and a wireless part. Figure 9.1 shows an example with a mobile host connected via a wireless link and an access point to the 'wired' internet where the correspondent host resides. The correspondent node could also use wireless access. The following would then also be applied to the access link of the correspondent host.

Standard TCP is used between the fixed computer and the access point. No computer in the internet recognizes any changes to TCP. Instead of the mobile host, the access point now terminates the standard TCP connection, acting as a proxy. This means that the access point is now seen as the mobile host for the fixed host and as the fixed host for the mobile host. Between the access point and the mobile host, a special TCP, adapted to wireless links, is used. However, changing TCP for the wireless link is not a requirement. Even an unchanged TCP can benefit from the much shorter round trip time, starting retransmission much faster. A good place for segmenting the connection between mobile host and correspondent host is at the foreign agent of mobile IP (see chapter 8). The foreign agent controls the mobility of the mobile host anyway and can also hand over the connection to the next foreign agent when the mobile host moves on. However, one can also imagine separating the TCP connections at a special server, e.g., at the entry point to a mobile phone network.

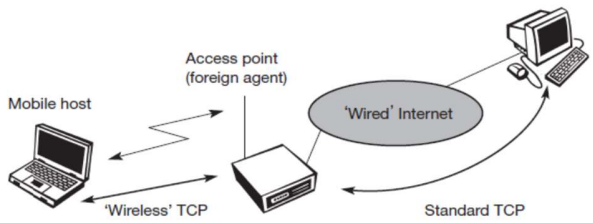


Figure 9.1
Indirect TCP segments a TCP connection into two parts

The correspondent host in the fixed network does not notice the wireless link or the segmentation of the connection. The foreign agent acts as a proxy and relays all data in both directions. If the correspondent host sends a packet, the foreign agent acknowledges this packet and tries to forward the packet to the mobile host. If the mobile host receives the packet, it acknowledges the packet. However, this acknowledgement is only used by the foreign agent. If a packet is lost on the wireless link due to a transmission error, the correspondent host would not notice this. In this case, the foreign agent tries to retransmit this packet locally to maintain reliable data transport.

Similarly, if the mobile host sends a packet, the foreign agent acknowledges this packet and tries to forward it to the correspondent host. If the packet is lost on the wireless link, the mobile hosts notice this much faster due to the lower round trip time and can directly retransmit the packet. Packet loss in the wired network is now handled by the foreign agent.

I-TCP requires several actions as soon as a handover takes place. As Figure 9.2 demonstrates, not only the packets have to be redirected using, e.g., mobile IP. In the example shown, the access point acts as a proxy buffering packets for retransmission. After the handover, the old proxy must forward buffered data to the new proxy because it has already acknowledged the data. After registration with the new foreign agent, this new foreign agent can inform the old one about its location to enable packet forwarding. Besides buffer content, the sockets of the proxy, too, must migrate to the new foreign agent located in the access point. The socket reflects the current state of the TCP connection, i.e., sequence

number, addresses, ports etc. No new connection may be established for the mobile host, and the correspondent host must not see any changes in connection state.

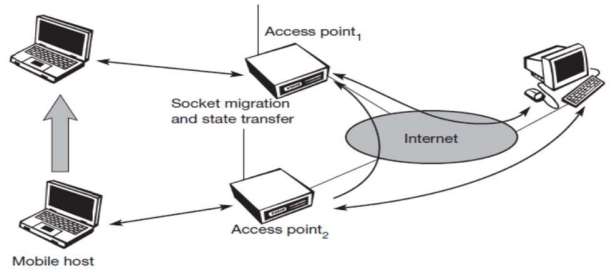


Figure 9.2 Socket and state migration after handover of a mobile host

(OR)

16.

a. Explain about wireless session protocol? 8M

The **WSP** has been designed to operate on top of the datagram service WDP or the transaction service WTP. For both types, security can be inserted using the WTLS security layer if required. WSP provides a shared state between a client and a server to optimize content transfer. HTTP, a protocol WSP tries to replace within the wireless domain, is stateless, which already causes many problems in fixed networks. Many web content providers therefore use cookies to store some state on a client machine, which is not an elegant solution. State is needed in web browsing, for example, to resume browsing in exactly the same context in which browsing has been suspended. This is an important feature for clients and servers. Client users can continue to work where they left the browser or when the network was interrupted, or users can get their customized environment every time they start the browser. Content providers can customize their pages to clients' needs and do not have to retransmit the same pages over and over again. WSP offers the following features needed for content exchange between cooperating clients and servers:

- **Session management:** WSP introduces sessions that can be **established** from a client to a server and may be long lived. Sessions can also be **released** in an orderly manner. The capabilities of **suspending** and **resuming** a session are important to mobile applications. Assume a mobile device is being switched off – it would be useful for a user to be able to continue operation at exactly the point where the device was switched off. Session lifetime is independent of transport connection lifetime or continuous operation of a bearer network.
- **Capability negotiation:** Clients and servers can agree upon a common level of protocol functionality during session establishment. Example parameters to negotiate are maximum client SDU size, maximum outstanding requests, protocol options, and server SDU size.
- **Content encoding:** WSP also defines the efficient binary encoding for the content it transfers. WSP offers content typing and composite objects, as explained for web browsing.

While WSP is a general-purpose session protocol, WAP has specified the **wireless session protocol/browsing (WSP/B)** which comprises protocols and services most suited for browsing-type applications. In addition to the general features of WSP, WSP/B offers the following features adapted to web browsing:

- **HTTP/1.1 functionality:** WSP/B supports the functions HTTP/1.1 offers, such as extensible request/reply methods, composite objects, and content type negotiation. WSP/B is a binary form of HTTP/1.1. HTTP/1.1 content headers are used to define content type, character set encoding, languages etc., but binary encodings are defined for well-known headers to reduce protocol overheads.

- **Exchange of session headers:** Client and server can exchange request/reply headers that remain constant over the lifetime of the session. These headers may include content types, character sets, languages, device capabilities, and other static parameters. WSP/B will not interpret header information but passes all headers directly to service users.
- **Push and pull data transfer:** Pulling data from a server is the traditional mechanism of the web. This is also supported by WSP/B using the request/response mechanism from HTTP/1.1. Additionally, WSP/B supports three push mechanisms for data transfer: a confirmed data push within an existing session context, a non-confirmed data push within an existing session context, and a non-confirmed data push without an existing session context.
- **Asynchronous requests:** Optionally, WSP/B supports a client that can send multiple requests to a server simultaneously. This improves efficiency for the requests and replies can now be coalesced into fewer messages. Latency is also improved, as each result can be sent to the client as soon as it is available.

As already mentioned, WSP/B can run over the transaction service WTP or the datagram service WDP. The following shows several protocol sequences typical for session management.

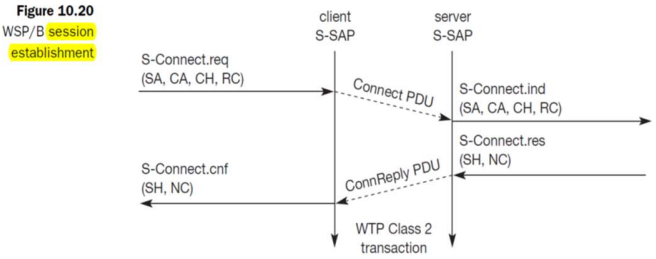


Figure 10.20
WSP/B session establishment

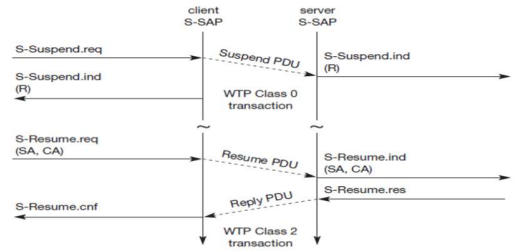


Figure 10.21
WSP/B session suspension and resume

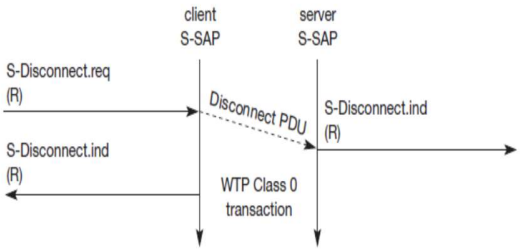


Figure 10.22
WSP/B session termination

b. Explain about wireless datagram protocol? 4M

The **wireless datagram protocol (WDP)** operates on top of many different bearer services capable of carrying data. At the T-SAP WDP offers a consistent datagram transport service independent of the

underlying bearer. Tooffer this consistent service, the adaptation needed in the transport layer candiffer depending on the services of the bearer. The closer the bearer service is toIP, the smaller the adaptation can be. If the bearer already offers IP services, UDPis used as WDP. WDP offers more or less the same services as UDP.

WDP offers **source** and **destination port numbers** used for multiplexing anddemultiplexing of data respectively. The service primitive to send a datagram is **TDUnitdata.req** with the **destination address (DA), destination port (DP),Source address (SA), source port (SP)**, and **user data (UD)** as mandatory parameters. Destination and source address are unique addresses for thereceiver and sender of the user data. These could be MSISDNs (i.e., a telephonenumber), IP addresses, or any other unique identifiers. The **T-DUnitdata.ind** serviceprimitive indicates the reception of data. Here destination address and portare only optional parameters.

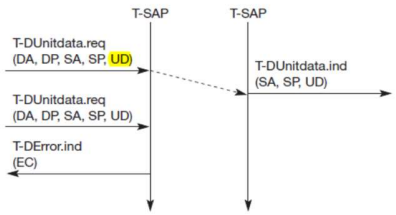
If a higher layer requests a service the WDP cannot fulfill, this error is Indicatedwith the **T-DError.ind** service primitive as shown in Figure 10.11. An**error code (EC)** is returned indicating the reason for the error to the higherlayer. WDP is not allowed to use this primitive to indicate problems with thebearer service. It is only allowed to use the primitive to indicate local problems,such as a user data size that is too large.

If any errors happen when WDP datagrams are sent from one WDP entityto another, the **wireless control message protocol (WCMP)**provides error handling mechanisms for WDP and shouldtherefore be implemented. WCMP contains control messages that resemble theinternet control message protocol (ICMP for IPv4, for IPv6) messages and can also be used for diagnostic and informational purposes.WCMP can be used by WDP nodes and gateways to report errors.However, WCMP error messages must not be sent as response to other WCMPerror messages. In IP-based networks, ICMP will be used as WCMP (e.g., CDPD,GPRS). Typical WCMP messages are **destination unreachable** (route, port,address unreachable), **parameter problem** (errors in the packet header),**message too big, reassembly failure**, or **echo request/reply**.

An additional **WDP management entity** supports WDP and provides informationabout changes in the environment, which may influence the correctoperation of WDP. Important information is the current configuration of thedevice, currently available bearer services, processing and memory resources etc.Design and implementation of this management component is consideredvendor-specific and is outside the scope of WAP.

If the bearer already offers IP transmission, WDP (i.e., UDP in this case) relieson the segmentation (called fragmentation in the IP context) and reassembly capabilitiesof the IP layer. Otherwise, WDP has toinclude these capabilities, which is, e.g., necessary for the GSM SMS. The WAP specificationprovides many more adaptations to almost all bearer services currentlyavailable or planned for the future.

Figure 10.11
WDP service primitives



Scheme prepared by
Mr. M.Rajesh Babu,
Dept. of CSE,
BEC, Bapatla
9441271567
mrb.csebec@gmail.com

Signature of faculty member
Prof. V. chakradhar
Dept. of CSE, BEC.

Signature of faculty member
E.Eesswni
Dept. of CSE, BEC.

Signature of HOD
Dept. of CSE

Signature of paper evaluators:

S.No.	Faculty Name	College Name	Contact Number	Signature