IT8602 MOBILE COMMUNICATION L T P C 3003
B.Tech(IT) 6TH SEMESTER - 2017 Regulations
UNIT I INTRODUCTION 9
Introduction to Mobile Computing – Applications of Mobile Computing- Generations of Mobile Communication Technologies - MAC Protocols – SDMA- TDMA- FDMA- CDMA

Wireless Communication

Contents :

1. **Cellular systems**
2. **Frequency Management and Channel Assignment**
3. **Types of handoff and their characteristics**
4. **MAC**
5. **SDMA**
6. **FDMA**
7. **TDMA**
8. **CDMA**
9. **Cellular Wireless Networks**

Pre requisite Discussion :

In this unit we discuss what is cellular systems and how the frequency and channels are allocated. Medium access control tells how to reduce traffic in the network and we discuss about frequency , time, space and code division multiple access.

1. Cellular Systems:

Concept :

Cellular telephone systems must accommodate a large number of users over a large geographic area with limited frequency spectrum, i.e., with limited number of channels. If a single transmitter/ receiver is used with only a single base station, then sufficient amount of power may not be present at a huge distance from the BS. For a large geographic coverage area, a high powered transmitter therefore has to be used. But a high power radio transmitter causes harm to environment. Mobile communication thus calls for replacing the high power transmitters by low power transmitters by dividing the coverage area into small segments, called cells. Each cell uses a certain number of the available channels and a group of adjacent cells together use all the available channels. Such a group is called a cluster. This cluster can repeat itself and hence the same set of channels can be used again and again.

Each cell has a low power transmitter with a coverage area equal to the area of the cell. This technique of substituting a single high powered transmitter by several low powered transmitters to support many users is the backbone of the cellular concept.

Significance :
In order to know how mobile is made this is necessary.

2. Frequency Management and Channel Assignment:

Concept:
Channel Assignment Strategies

With the rapid increase in number of mobile users, the mobile service providers had to follow strategies which ensure the effective utilization of the limited radio spectrum. With increased capacity and low interference being the prime objectives, a frequency reuse scheme was helpful in achieving this objectives. A variety of channel assignment strategies have been followed to aid these objectives. Channel assignment strategies are classified into two types: fixed and dynamic.

Fixed Channel Assignment (FCA)

In fixed channel assignment strategy each cell is allocated a fixed number of voice channels. Any communication within the cell can only be made with the designated unused channels of that particular cell. Suppose if all the channels are occupied, then the call is blocked and subscriber has to wait. This is simplest of the channel assignment strategies as it requires very simple circuitry but provides worst channel utilization. Later there was another approach in which the channels were borrowed from adjacent cell if all of its own designated channels were occupied. This was named as borrowing strategy. In such cases the MSC supervises the borrowing process and ensures that none of the calls in progress are interrupted.

Dynamic Channel Assignment (DCA)

In dynamic channel assignment strategy channels are temporarily assigned for use in cells for the duration of the call. Each time a call attempt is made from a cell the corresponding BS requests a channel from MSC. The MSC then allocates a channel to the requesting the BS. After the call is over the channel is returned and kept in a central pool. To avoid co-channel interference any channel that in use in one cell can only be reassigned simultaneously to another cell in the system if the distance between the two cells is larger than minimum reuse distance. When compared to the FCA, DCA has reduced the likelihood of blocking and even increased the trunking capacity of the network as all of the channels are available to all cells, i.e., good quality of service. But this type of assignment strategy results in heavy load on switching center at heavy traffic condition.

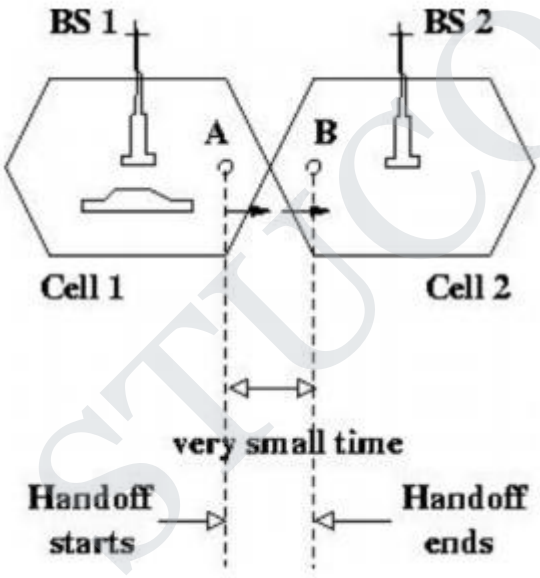
Significance:

This is used to know how the frequency is assigned to cells and how the channels are clustered in heavy and less traffic conditions.

3. Handoff Process

Concept:

When a user moves from one cell to the other, to keep the communication between the user pair, the user channel has to be shifted from one BS to the other without interrupting the call, i.e., when a MS moves into another cell, while the conversation is still in progress, the MSC automatically transfers the call to a new FDD channel without disturbing the conversation. This process is called as handoff. Processing of handoff_ is an important task in any cellular system. Handoffs must be performed successfully and be imperceptible to the users. Once a signal level is set as the minimum acceptable for good voice quality (Prmin), then a slightly stronger level is chosen as the threshold (PrH)at which handoff has to be made, as shown. A parameter, called power margin, defined as quite an important parameter during the handoff process since this margin can neither be too large nor too small. If is too small, then there may not be enough time to complete the handoff and the call might be lost even if the user crosses the cell boundary. If it is too high o the other hand, then MSC has to be burdened with unnecessary handoffs. This is because MS may not intend to enter the other cell. Therefore it should be judiciously chosen to ensure imperceptible handoffs and to meet other objectives.



Significance:

Handoff is used to know how the call is continued without any interrupt when the mobile node moves from one base station to other.

4. MAC:

Concept:

MAC is a data communication protocol. It is a sub layer of the data link layer, which itself is layer 2. The MAC sub layer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. It is also referred to as a medium access controller.

CSMA /CD

The Carrier Sense Multiple Access (CSMA) with Collision Detection (CD) protocol is used to control access to the shared Ethernet medium. A switched network (e.g. Fast Ethernet) may use a full duplex mode giving access to the full link speed when used between directly connected two NICs, Switch to NIC cables, or Switch to Switch cables.

Significance:

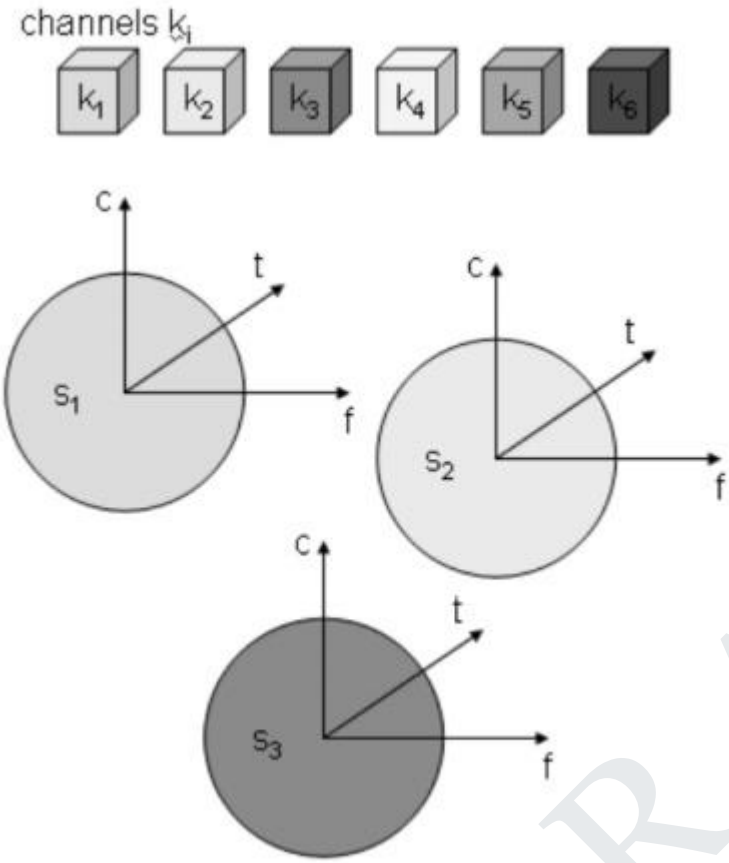
It is used for mobile nodes to communicate without any infrastructure. Overcomes the Near and Far terminal and Hidden-Exposed terminal problems

SDMA FDMA TDMA SDMA

5. Space Division Multiplexing

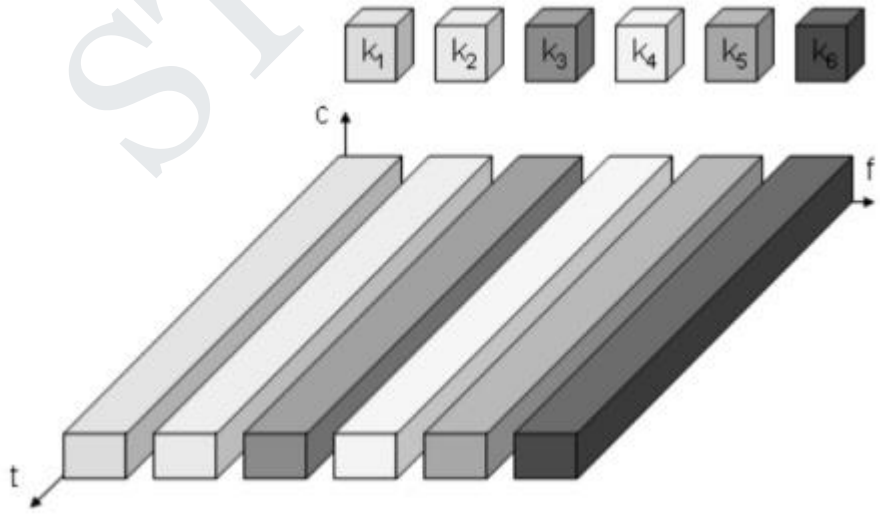
Six channels ki introduces a three dimensional coordinate system.

It shows the dimensions of code c, time t and frequency t. Space division multiplexing (SDM) the (three dimensional) space si is also shown. The channels k1 to k3 can be mapped onto the three spaces s1 to s3 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 4 multiplexing schemes presented. The remaining channels(k4 to k6) 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.



6. Frequency Division Multiplexing (FDM)

FDM schemes to subdivide the frequency dimension into several non-overlapping frequency bands.Each channel k1 is now allotted its frequency band as indicated. Senders using a certain frequency band can use this band continuously. Guard spaces are needed to avoid frequency band overlapping called adjacent channel interference.



This is used in radio stations within the same region where each radio station has its own frequency.

Significance:

No dynamic coordination necessary
Works also or analog signals

Disadvantages
Waste of bandwidth if the traffic is distributed unevenly

7. Time Division Multiplexing (TDM)

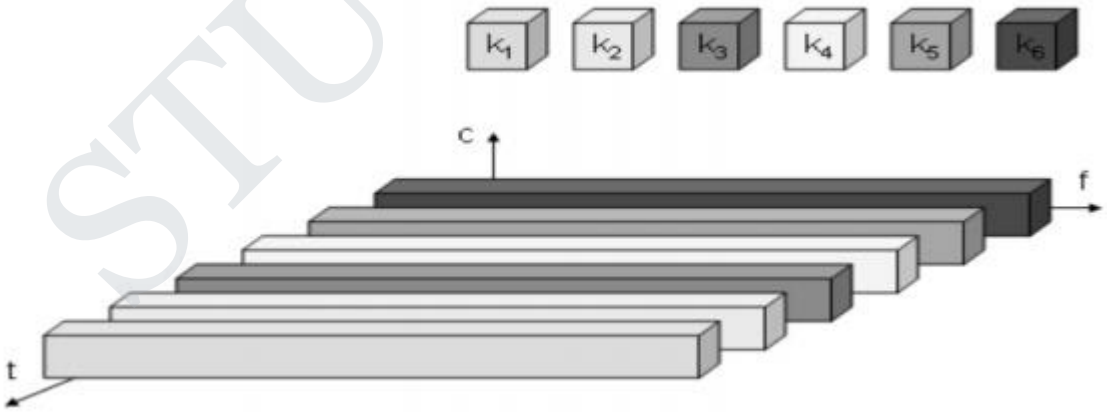
Here channels k1 is given the whole bandwidth for a certain amount of time i.e all senders use the same frequency but at different point of time Guard spaces which represent time gaps have to separate the different periods when the senders use the medium. If two transmissions overlap in time this is called co-interference. To avoid this type of interference precise synchronization between different senders is necessary.

Significance:

Only one carrier in the medium at any time
Throughput high even for many users

Disadvantages

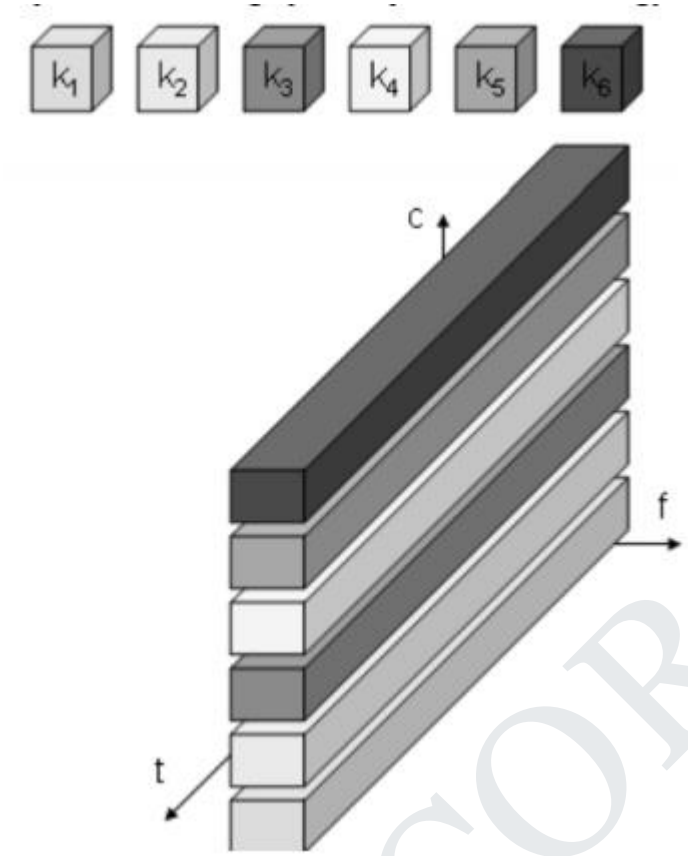
Precise synchronization necessary



8. Code Division Multiplexing

Each channel has a unique code
All channels use the same spectrum at the same time

Guard spaces are ralises by using codes with the necessary distance in code space Ex. Orthogonal codes
Implemented using spread spectrum technology



Significance:
Bandwidth efficient
No coordination and synchronization necessary
Good protection against interference and tapping

Disadvantages
Varying user data rates
More complex signal regeneration

9. Cellular Wireless Network

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 as explained in section 3.5, 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,. 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, however, the situation is somewhat more complex. Assume that the demodulated signal shows some distortion, e.g., 101**0**01**0**10000**1**101000111.

Additionally, the different paths may have different path losses. In this case, using so-called rake receivers provides a possible solution. A **rake receiver** uses n correlators for the n strongest paths. Each correlator is synchronized to the transmitter plus the delay on that specific path. As soon as the receiver detects a new path which is stronger than the currently weakest path, it assigns this new path to the correlator with the weakest path. The output of the correlators are then combined and fed into the decision unit. Rake receivers can even take advantage of the multi-path propagation by combining the different paths in a constructive way

Significance:

Used real time in organizations and used in smart phones. GPS in Taxies, Emergency alerts, etc

Application:

- ∑ Mobile Communication
- ∑ GPS systems
- ∑ Emergency System

IT8602 MOBILE COMMUNICATION L T P C 3003
B.Tech(IT) 6TH SEMESTER - 2017 Regulations
UNIT II MOBILE TELECOMMUNICATION SYSTEM 9
GSM – Architecture – Protocols – Connection Establishment – Frequency Allocation – Routing – Mobility Management – Security –GPRS- UMTS- Architecture

Mobile Communication Systems

Contents: 1. GSM Architecture-Location tracking and call setup 2. Mobility management 3. Handover-Security-GSM 4. SMS International roaming for GSM 5. Call recording functions-subscriber and service data mgt 6. Mobile Number portability 7. VoIP service for Mobile Networks 8. GPRS Architecture-GPRS procedures 9. Billing

Mobile Communication Systems

Contents:

1. **GSM Architecture-Location tracking and call setup**
2. **Mobility management**
3. **Handover-Security-GSM**
4. **SMS International roaming for GSM**
5. **Call recording functions-subscriber and service data mgt**
6. **Mobile Number portability**
7. **VoIP service for Mobile Networks**
8. **GPRS Architecture-GPRS procedures**
9. **Billing**

Pre requisite Discussion :

In this unit we discuss Digital cellular networks are the segment of the market for mobile(GSM) and wireless devices which are growing most rapidly. They are the wireless extensions of traditional PSTN or ISDN networks and allow for seamless roaming with the same mobile phone nation or even worldwide. Today, these systems are mainly used for voice traffic. However, data traffic is continuously growing and, therefore, this chapter presents

1. GSM: Architecture

Concept:

Global system for mobile communication founded in 1982. Most successful Digital Mobile Telecommunication System. Used by over 800 million people in more than 190 countries. System Architecture

Radio subsystem

Network and switching subsystem Operation Subsystem

SMS Concept:

A useful service for very simple message transfer is the **short message service (SMS)** which offers transmission of messages of up to 160 characters.

SMS messages do not use the standard data channels of GSM but exploit unused capacity in the signalling channels.

Sending and receiving of SMS is possible during data or voice transmission. SMS was in the GSM standard from the beginning

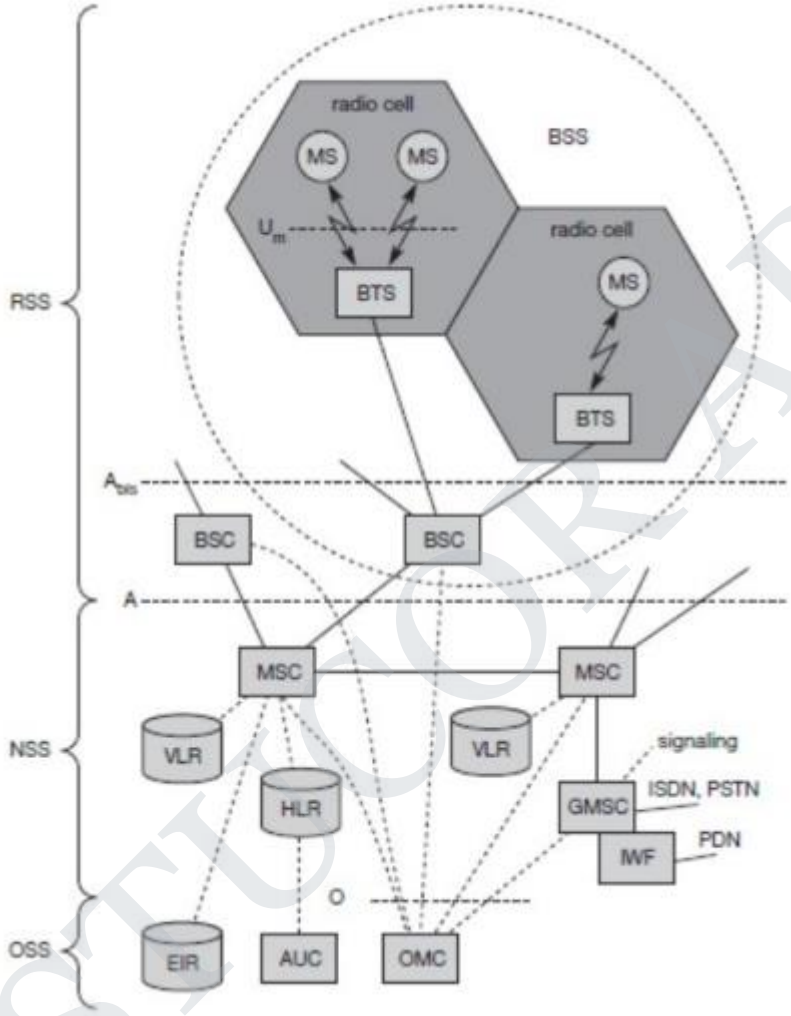
The successor of SMS, the **enhanced message service (EMS)**, offers a larger message size (e.g., 760 characters, concatenating several SMs), formatted text, and the transmission of animated pictures, small images and ring tones in a standardized way EMS never really took off as the **multimedia message service (MMS)** was available.

MMS offers the transmission of larger pictures (GIF, JPG, WBMP), short video clips etc. and comes with mobile phones that integrate small cameras.

Another non-voice tele service is **group 3 fax**, which is available worldwide.

In this service, fax data is transmitted as digital data over the analog telephone network according to the ITU-T standards T.4 and T.30 using modems.

Typically, a transparent fax service is used, i.e., fax data and fax signaling is transmitted using a transparent bearer service.



Mobile station (MS):

The MS comprises all user equipment and software needed for communication with a GSM network.

Significance:

Provides an interrupted connection between two or several users

2. Mobility Management:

Concept:

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.3 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)**

Significance:

The most advantageous thing is that while moving between one base station to other base station it provides an uninterrupted connection

3. GSM HANDOVER

Concept:

Cellular systems require handover procedures, as single cells do not cover the whole service area. The smaller the cell size and the faster the movement of a mobile station through the cells The more handovers of ongoing calls are required. A handover should not cause a cut-off, also called call drop. GSM aims at maximum handover duration of 60ms. 2 Basic Reasons for a Handover

The mobile station moves out of the range of a BTS of a certain antenna of a BTS respectively.

The received signal level decreases continuously until it alls below the minimal requirements or communication.

The error rate maygrow due to intererance, the distance to the BTS may be too high.

All these effects may diminish the quality of the radio link and make radio transmission impossible in the near future.

The wired infrastructure (MSC, BSC) may decide that the traffic in one cell is too high and shift some MS to another cells with a lower load. Handover may be due to load balancing.

Types of Handover in GSM 4 Possible Handover Scenarios in GSM

1. Intra-Cell Handover

2. Inter-Cell,Intra BSC Handover

3. Inter BSC,Intra-MSC Handover

4. Inter MSC Handover

1. Intra-cell handover: o Within a cell

o Narrow band interference could make transmission at a certain frequency impossible. o The BSC could then decide to change the carrier frequency.

2. Inter-cell, intra BSC handover:

o The mobile station moves from one cell to another, but stays within the control of the same BSC.

o The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one .

3. Inter BSC, intra MSC handover: o BSC controls a limited number of cells;

o GSM also has to perform handovers between cells controlled by different BSCs.
o This handover then has to be controlled by the MSC.

4. Inter MSC handover:

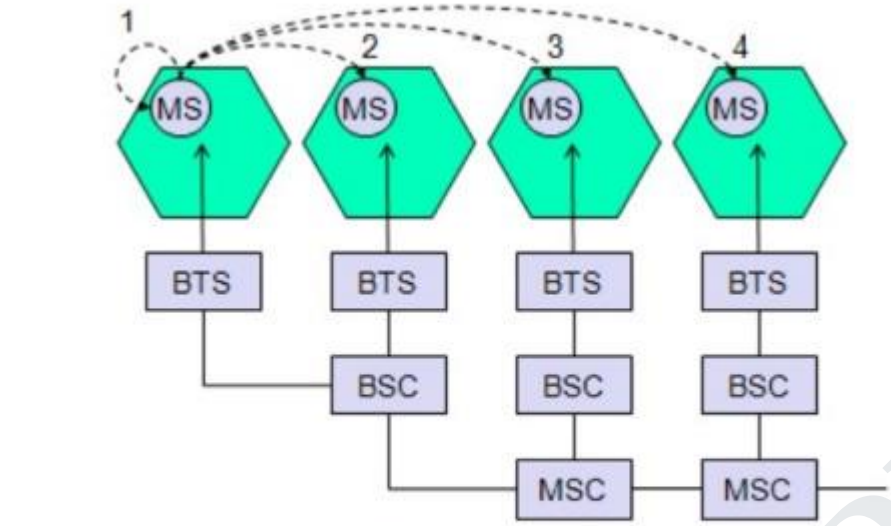
o A handover could be required between two cells belonging to different MSCs.
o Now both MSCs perform the handover together.

Necessary Information for a Handover

To provide all the necessary information for a handover due to a weak link

MS and BTS both perform periodic measurements of the downlink and uplink quality respectively. (Link quality comprises signal level and bit error rate.)

Measurement reports are sent by the MS about every half second and contain the quality of the current link used for transmission as well as the quality of certain channels in neighboring cells (the BCCHs).



Significance:

The most advantageous thing is that while moving between one base station to other base station it provides an uninterrupted connection

4. SMS International roaming for GSM Concept:

GSM offers several security services using confidential information stored in the AUC and in the individual SIM.

The SIM stores personal, secret data and is protected with a PIN against unauthorized use.

The security services offered by GSM are

Access control and authentication:

The authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM.

The next step is the subscriber authentication. This step is based on a challenge-response scheme.

Confidentiality:

All user-related data is encrypted.

After authentication BTS and MS apply encryption to

Voice

Data and

Signaling

This confidentiality exists only between MS and BTS.

Significance:

All data is encrypted before transmission, and user identifiers.

GSM transmits a temporary identifier (TMSI), which is newly assigned by the VLR after each location update.

5. Call recording functions-subscriber and service data mgt Concept:

Call recording is becoming increasingly important, with technology changing and working habits becoming more mobile. Addressing mobile recording is now the subject of many financial regulators' recommendations. It is also increasingly important to business continuity planning, especially for pandemic planning.

The actual recording takes place on a recording system with software for the management of calls and security of recordings. Most call recording software

applications rely on an analogue signal via either a call recording adapter or a telephony board.

Digital lines cannot be recorded unless the call recording system can capture and decode the proprietary digital signaling, which some modern systems can. Sometimes a method is supplied with a digital PBX that can process the proprietary signal (usually a conversion box) before being channeled to a computer for recording. Alternatively a hardware adapter can be used on a telephone handset as the digital signal is converted at that point to analogue.

VoIP Recording is usually restricted to streaming media recorders or software developed by the soft phone or IP PBX creator. There are also solutions which use packet capture technology to passively record VoIP phone calls on the LAN.

Hardware is required to make the voice signal available to the computer equipment. Some of today's call recording software is sold as a turn-key solution with hardware.

Direct recording of mobile phone calls requires a hardware adapter connected to the handset. There are many other ways to record mobile phone calls. One approach is to route calls via a new PBX system linked to the recorder. However, such systems are typically expensive to purchase and change the way that calls are made, incurring running costs. Another approach links directly into existing recording systems from a PDA phone. Both of these approaches allow recordings to be time stamped, often required for legal reasons. Recording directly onto mobile devices does provide a legally valid recording in many countries.

Significance:

- ∑ Records the call for future use(References)

- ∑ Manages the Call whenever the user seems busy

∑ Service provided(data) can be monitored in a fair manner

6. Mobile Number Portability:

Concept:

MNP is a boon to the customer as he is allowed to keep the same mobile number even he switches over to other operator.

3 options : Service portability Location Portability Number portability

MNP Priniciple in INDIA:

Applicable only for mobile Numbers

Applicable only in intra licensed area

Applicable irrespective of Technology

LRN based routing DoT

Significance:

All mobile users can use MNP to get best tariff and network coverage without changing the number.

7. VOIP Service for mobile networks

Concept:

Voice over Internet protocol is simply the transmission of voice traffic over ip ased networks. Mobile VOIP is delivered by a third party service provider a WIFI or 3G network cellular network that a mobile device is connected to.

Mobile VOIP service providers typically require a user to download software onto their mobile device in order to gain access to their service.

Voip sends your calls across the internet

Phone calls are sent through VOIP phone adaptor to regular or cordless telephone.

Significance:

Used by all network service providers for help purposes ncluding toll free numbers.

8. GPRS SYSTEM ARCHITECTURE

Concept:

The GPRS architecture introduces two new network elements, which are called

GPRS support nodes (GSN) and are in fact routers.

All GSNs are integrated into the standard GSM architecture, and may new interfaces have been defined .

GGSN - Gateway GPRS Support Node :-

The gateway GPRS support node (GGSN) is the inter working unit between the GPRS network and external packet data networks (PDN).

This node contains routing information for GPRS users, performs address conversion, and tunnels data to a user via encapsulation.

The GGSN is connected to external networks (e.g., IP or X.25) via the Gi interface and transfers packets to the SGSN via and IP-based backbone network (Gn interface).

Other New Element **SGSN** **Serving GPRS Support Node :-**

The other new element is the serving GPRS support node (SGSN) which supports the MS via the Gb interface.

The SGSN, for example, requests user address form the GPRS register (GR), keeps track of the individual Mss location, is responsible for collecting billing information (e.g., counting bytes), and performs several security functions such as access control.

The SGSN is connected to a BSC via frame relay and is basically on the same hierarchy level as an MSC.

GPRS Register (GR)

The GR, which is typically a part of the HLR, stores all GPRS relevant data. GGSNs can be compared with home and foreign agents, respectively, in a mobile IP network.

As shown in figure below, packet data is transmitted form a PDN, via the GGSN and SGSN directly to the BSS and finally to the MS.

The MSC, which is responsible for data transport in the traditional circuit switched GSM, is only used for signaling in the GPRS scenario.

Before sending any data over the GPRS network, an MS must attach to it, following the procedures of the mobility management.

CKSN Cipher key sequence number (CSKN)

The attachment procedure includes assigning a temporal identifier, called a temporary logical link identity (TLLI), and a ciphering key sequence number (CKSN) for data encryption.

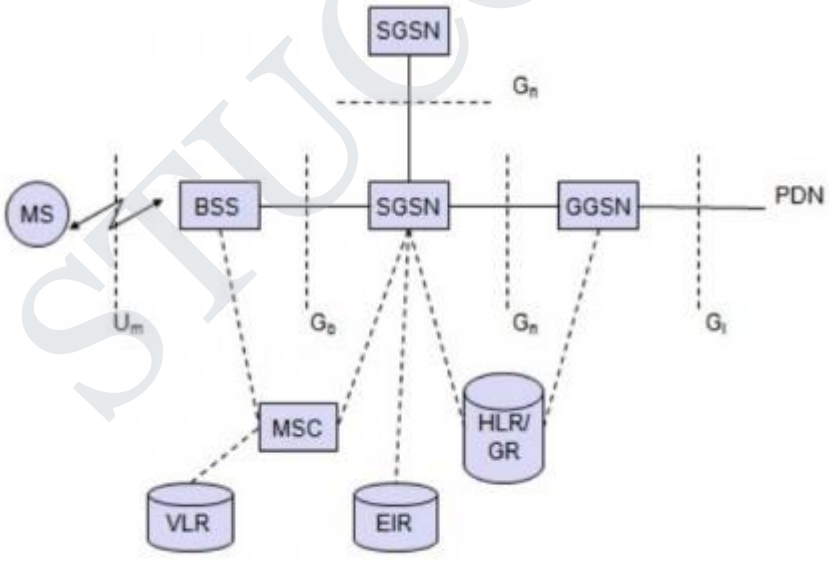
For each MS, a GPRS context is set up and stored in the MS and in the corresponding SGSN. This context comprises the status of the MS (which can be ready, idle, or standby), the CKSN, a flag indicating if compression is used, and routing data (TLLI, the routing area RA, a cell identifier and a packet data channel, PDCH, identifier).

Besides attaching and detaching mobility management also comprises functions for authentication, location management, and ciphering (here, the scope of ciphering lies between MS and SGSN, which is more than in standard GSM).

In idle mode an MS is not reachable and all contexts is deleted.

In the standby state only movement across routing areas is updated to the SGSN but not changes of the cell. Permanent paging.

The update procedure in standby mode is a compromise. Only in the ready state every movement of the MS is indicated to the SGSN.



Significance:

Provides Data connection for several Mobile Stations from the Base Stations.

9. Billing:

Concept:

As you travel, each network you access data or phone calls through sends a bill to your carrier back home. One your bills start coming in, your carrier mails it to you. Sometimes it can take several months to reconcile all the charges you've racked up while traveling. I've completely switched my travel calls to You Roam since I travel a lot. It lets you make and receive calls on your own number over Wi-Fi, 3G or a local sim anywhere in the world for free or really cheap.

Significance:

Allows the network provider companies, to process their billing procedures with their code of conduct.

Application:

- ∑ Provides the GSM architecture for nowadays Mobile usage.
- ∑ This is mainly used in the Voice IP call features

IT8602	MOBILE COMMUNICATION	[Btech(IT) 6TH SEM-2017Reg]
UNIT III	WIRELESS NETWORKS	9

Wireless LANs and PANs – IEEE 802.11 Standard – Architecture – Services – Blue Tooth- Wi-Fi – WiMAX

Wireless Networks

Contents:

1. **Wireless LAN**
2. **IEEE 802.11 Standards**
3. **Architecture**
4. **Services**
5. **Mobile Ad hoc Networks**
6. **WiFi and WiMAX**
7. **Wireless Local Loop**

Pre requisite Discussion :

In this chapter we present several wireless local area network (WLAN) technologies. This constitutes a fast-growing market introducing the flexibility of wireless access into office, home, or production environments. WLANs are typically restricted in their diameter to buildings, a campus, single rooms etc. and are operated by individuals, not by large-scale network providers The global goal of WLANs is to replace office cabling, to enable tether less access to the internet and, to introduce a higher flexibility for ad-hoc communication in, e.g., group meetings. The following points illustrate some general advantages and disadvantages of WLANs compared to their wired counterparts.

1.Wireless LAN :

Concepts:

WLAN Some advantage of WLAN (or) Characteristics of WLAN

Flexibility

Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere. Sometimes wiring is difficult if firewalls separate buildings. Penetration of a firewalls is only permitted at certain points to prevent fire from spreading too fast.

Planning

Only wireless ad-hoc networks allow for communication without previous planning any wired network needs wiring plans. As long as devices follow the same standard they can communicate. For wired networks, additional cabling with the right plug and probably interworking units such as switches have to be provided

Design

Wireless networks allow for the design of small, independent devices which can for example be put into a pocket. Cables not only restrict users but also designers of small PDAs, notepads etc. Wireless senders and receivers can be hidden in historic buildings. i.e., current networking technology can be introduced without being visible.

Robustness

Wireless networks can survive disasters e.g., earthquakes or user pulling a plug. If the wireless devices survive people can still communicate. Networks requiring a wired infrastructure will usually break down completely.

Cost

After providing wireless access to the infrastructure via an access point for the first user, adding, additional users to a wireless network will not increase the cost.

Significance:

This helps to know the characteristics and features of using Wireless LAN

2. IEEE 802.11

The three main sections of this chapter present the IEEE standard for WLANs, IEEE 802.11, the European ETSI standard for a high-speed WLAN with QoS support

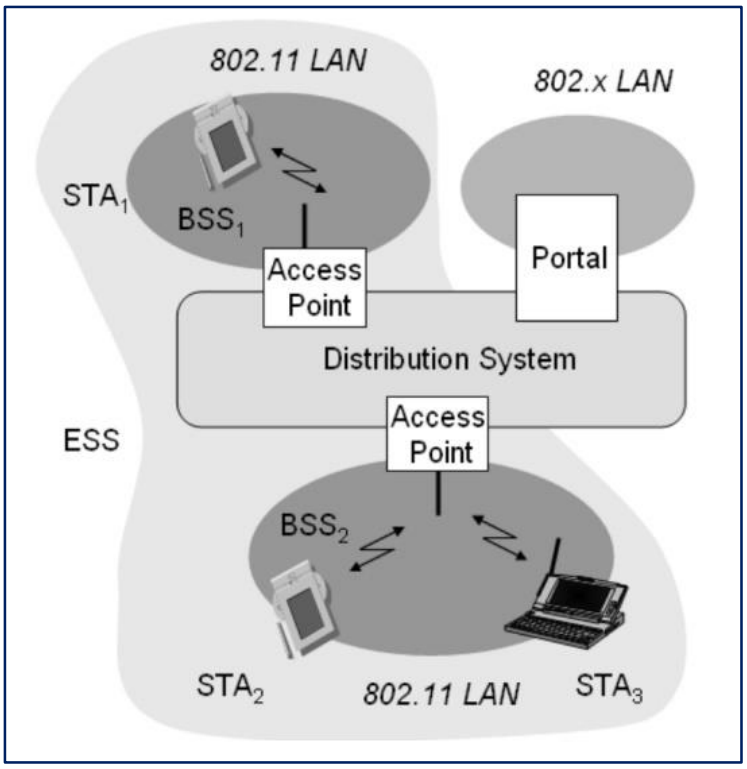
3. SYSTEM ARCHITECTURE

Wireless networks can exhibit two different basic

Information Based

Ad0-hoc

Infrastructure based:



STA (Station)

Several nodes called stations (STA)

STA are connected to access points (AP) stations (or) terminals with access mechanisms to the wireless medium and radio contact to the AP.

BSS (Basic Service Set)

A Group of stations using the same radio frequency..

The example two BSSs (i.e.) BSS1 and BSS2 - which are connected via a distribution system.

AP (Access Point)

A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area.

Distributed System

Interconnection network to form one logical network (ESS :- Extended Service Set) based on several BSS.

Extended service set (ESS) has its own identifier, the ESSID.

The ESSID is the name of a network and is used to separate different networks. Without knowing the ESSID it should not be possible to participate in the WLAN.

Portal

Bridge to other wired networks.

Significance:

The distribution system connects the wireless networks via the APs with a portal which forms the **interworking unit to other LANs.**

4. Services

Concept:

Stations can select an AP and associate with it.

The APs support roaming ie. Changing access points

Significance:

The distribution system handles data transfer between the different APs.

APs provide

Synchronization within a BSS

Support power management and

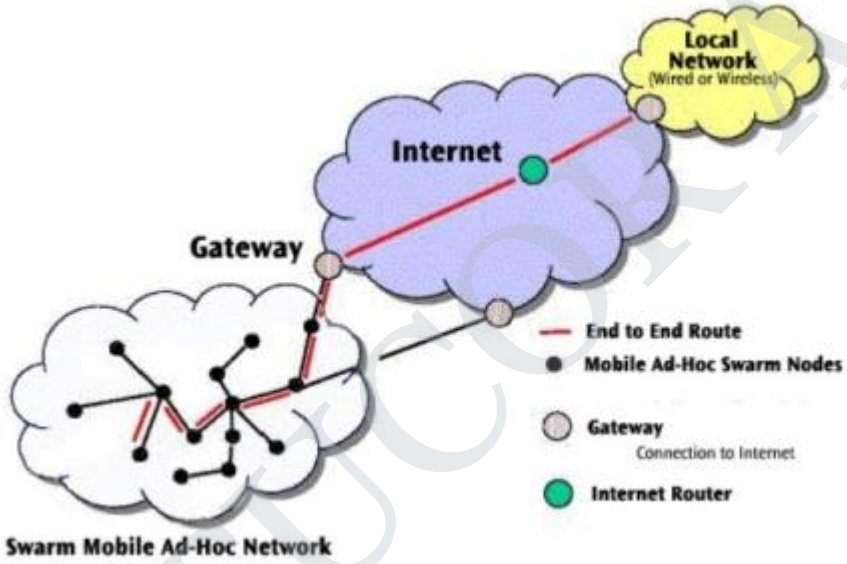
Can control medium access to support time bounded service

5. Mobile Ad hoc Networks Concept:

An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other. In Latin, *ad hoc* literally means "for this," meaning "for this special purpose" and also, by extension, improvised or impromptu.

The Ad Hoc Networks is an international and archival journal providing a publication vehicle for complete coverage of all topics of interest to those involved in ad hoc and sensor networking areas. The Ad Hoc Networks considers original, high quality and unpublished contributions

addressing all aspects of ad hoc and sensor networks. Specific areas of interest include, but are not limited to:



- Mobile and Wireless Ad Hoc Networks
- Sensor Networks
- Wireless Local and Personal Area Networks
- Home Networks
- Ad Hoc Networks of Autonomous Intelligent Systems

- Novel Architectures for Ad Hoc and Sensor Networks
- Self-organizing Network Architectures and Protocols
- Transport Layer Protocols
- Routing protocols (unicast, multicast, geocast, etc.)
- Media Access Control Techniques
- Error Control Schemes
- Power-Aware, Low-Power and Energy-Efficient Designs
- Synchronization and Scheduling Issues
- Mobility Management
- Mobility-Tolerant Communication Protocols
- Location Tracking and Location-based Services
- Resource and Information Management
- Security and Fault-Tolerance Issues
- Hardware and Software Platforms, Systems, and Testbeds
- Experimental and Prototype Results
- Quality-of-Service Issues
- Cross-Layer Interactions
- Scalability Issues
- Performance Analysis and Simulation of Protocols

Significance:

It is used for mobile nodes to communicate without any infrastructure.

6. WIFI and WIMAX :

Concepts:

These are used for data transfer and wireless communication such like Bluetooth, but it can connect devices in higher range. WiMAX is similar to the wireless standard known as Wi-Fi, but on a much larger scale and at faster speeds. A

nomadic version would keep WiMAX-enabled devices connected over large areas, much like today.s cell phones. We can compare it with Wi-Fi based on the following factors.

Range

Wi-Fi typically provides local network access for around a few hundred feet with speeds of up to 54 Mbps, a single WiMAX antenna is expected to have a range of up to 40 miles with speeds of 70 Mbps or more. As such, WiMAX can bring the underlying Internet connection needed to service localWi-Fi networks.

Scalability

Wi-Fi is intended for LAN applications, users scale from one to tens with one subscriber for each CPE device. Fixed channel sizes (20MHz).

WiMAX is designed to efficiently support from one to hundreds of Consumer premises equipments (CPE)s, with unlimited subscribers behind each CPE. Flexible channel sizes from 1.5MHz to 20MHz.

Bit rate

Wi-Fi works at 2.7 bps/Hz and can peak up to 54 Mbps in 20 MHz channel. WiMAX works at 5 bps/Hz and can peak up to 100 Mbps in a 20 MHz channel.

Quality of Service

Wi-Fi does not guarantee any QoS but WiMax will provide your several level of QoS. As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks. Wi-Fi does not provide ubiquitous broadband while WiMAX does.

Significance:

Used real time in organizations and used in smart phones.

7. Wireless Local Loop

Concept:

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 as explained in section 3.5, 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,. On the receiver side, this signal is XORed bit-wise after demodulation with the same Barker code as chipping sequence.

Applications:

- ∑ Used to provide data coverage to a small area with high speed with WiMax
- ∑ Provides an infrastructure for establishing a mobile communication

UNIT IV	MOBILE NETWORK LAYER	9
Mobile IP – DHCP – AdHoc– Proactive and Reactive Routing Protocols – Multicast Routing Vehicular Ad Hoc networks (VANET) –MANET Vs VANET – Security		

Mobile Network and Transport Layers

Mobile Network and Transport Layers

Contents: 1. Mobile IP 2. Dynamic Host Configuration Protocol 3. Mobile Ad Hoc Routing Protocols 4. Multicast routing 5. TCP over Wireless Networks 6. Indirect TCP 7. Snooping TCP 8. Mobile TCP 9. Fast Retransmit / Fast Recovery 10. Transmission/Timeout Freezing-Selective Retransmission 11. Transaction Oriented TCP- TCP over 2.5 / 3G wireless Networks

Contents:

1. **Mobile IP**
2. **Dynamic Host Configuration Protocol**
3. **Mobile Ad Hoc Routing Protocols**
4. **Multicast routing**
5. **TCP over Wireless Networks**
6. **Indirect TCP**
7. **Snooping TCP**
8. **Mobile TCP**
9. **Fast Retransmit / Fast Recovery**
10. **Transmission/Timeout Freezing-Selective Retransmission**
11. **Transaction Oriented TCP- TCP over 2.5 / 3G wireless Networks**

Pre requisite Discussion :

In this unit we discuss what is cellular systems and how the frequency and channels are allocated. Medium access control tells how to reduce traffic in the network and we discuss about frequency , time, space and code division multiple access.

1. Mobile IP:

Concept:

Goals For Mobile IP

The Internet is the network for global data communication with hundreds of millions of users. The reason is quite simple:

You will not receive a single packet as soon as you leave your home network, ie., The network your computer is configured for, and reconnect your computer (wireless or wired) at another place. A host sends an IP packet with the header containing a destination address besides other fields.

The destination address not only determines the receiver of the packet, but also the physical subnet of the receiver.

Routers in the Internet now look at the destination addresses of incoming pack-ets and forward them according to internal look-up tables.

To avoid an explosion of routing tables, only prefixes are stored and further optimizations are applied.

Otherwise a router would have to store the addressed of all computers in the Internet which is obviously not feasible.

As long as the receiver can be reached within its physical subnet it gets the packets as soon as it moves outside the subnet, no packet will reach it anymore.

Thus a host needs a so called topologically correct address.

Solutions:

Assigning the computer a new topologically correct IP address.

So moving to a new location would also mean assigning a new address.

Now the problem is that nobody knows of this new address.

It is almost impossible to find a (mobile) host in the Internet which has just changed its address. Especially the Domain Name System (DNS) needs some time before it update its internal tables necessary for the mapping of a logical name to an IP address.

This approach does not work if the mobile node moves quite often. Furthermore the Internet and DNS have not been built for frequent updates.

Significance:

- ∑ IP packet Delivery
- ∑ Path Delivery

2. DYNAMICHOST CONFIGURATION PROTOCOL

Concept:

The Dynamic Host Protocol (DHCP,RFC 2131) mainly used

TO simply the installation

Maintenance of networked computers

- ∑ If a new computer is connected to a network DHCP can provide it with all the necessary Information for full system integration into the network e.g:-Addresses of DNS server and Default router Subnet Mask Domain name IP address
- ∑ Providing an IP address makes DHCP very attractive for mobile IP as well source of care-of address.

Basic DHCP configuration

DHCP clients send a request to a server to which the server responds.

A client sends requests using MAC broadcasts to reach all devices in the LAN.

A DHCP relay might be needed to forward requests across inter-working units to a DHCP server.

Client Initialization

The client broadcasts a DHCP DISCOVER into subnet. There may be relay to forwards this broadcast.

Two servers receive this broadcast and determine the configuration they offer to the client. Servers reply to the client s request with DHCPOFFER and offer a list of configuration parameters.

The client can now choose one of the configurations offered.

The client in turn replies to the servers accepting one of the configurations and rejecting the others using DHCP REQUEST.

If a server receives a DHCP REQUEST with a rejection it can free the reserved configuration for other possible clients.

The server with the configuration accepted by the client now confirms the configuration with DHCP ACK.This completes the initialization phase.

If a client leaves the subnet it should release the configuration received by the server using

DHCP RELEASE.

Now the server can free the context stored for the client and offer the configuration again.

The configuration a client from a server is only leased for a certain amount of time it has to be reconfirmed from time to time.

Otherwise the server will be free the configuration. This timeout of configuration helps in the case of crashed nodes or nodes moved away without realizing the context.

DHCP Features

DHCP supporting the acquisition of care-of-address for mobile nodes

A DHCP server should located in the subnet of the access point of the mobile note.

DHCP relay should provide forwarding of the Messages.

RFC 3118 specifies authentication for DHCP messages which id needed to protect mobile nodes from malicious DHCP servers.

Significance:

Provides a protocol for the countries where the calls and IPs are dynamically allotted.

3. Mobile Adhoc Routing:

Concept:

In wireless networks using an infrastructure cells have been defines. within a cell the bse station can reach all mobile nodes.

In -hoc networks each node must be able to forward data for other nodes. At a certain time t1 the network topology consists of five nodes N1 to N5.

Nodes are connected depending upon the current transmission characteristics between them. In this network N4 can receive N1 over a good link.

But N1 receive N4 via a weak link.

Links do not necessarily have the same characteristics in both directions.

Reason:

Different antenna characteristics or transmit power. N1 cannot receive N2 at all

N2 receives a signal from N1. At a certain time t2 the network topology consists of five nodes N1 to N5.This situation can change quite fast N1 cannot receive N4 any longer

N4 receives N1 only via a weak link.

But N1 has as asymmetric but bi-directional link to N2 that did not exist before.

The Fundamental differences between wired networks and ad-hoc networks related to routing.

Asymmetric Links

Node A receives a signal from node B.

But this does not tell anything about the quality of the connection in reverse. Node B might

Receive nothing

Have a weak link

Even have a better link than the reverse direction.

Routing information collected for one direction is of almost no use for the other direction.

Redundant Links

Wired networks too have a redundant links to survive link failures.

There is only some redundancy in wired networks which additionally are controlled by a network administrator.

In ad-hoc networks nobody controls redundancy so there might be many redundant links up to the extreme of a completely meshed topology.

Routing algorithms for wired networks can handle some redundancy but a high redundancy can cause a large computational overhead for routing table updates.

Signifiacance:

Gives a protocol for configuring the mobiles.

4. Multicast Routing:

Concept:

Multicast IP Routing protocols are used to distribute data (for example, audio/video streaming broadcasts) to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.

A multicast group identifies a set of recipients that are interested in a particular data stream, and is represented by an IP address from a well-defined range. Data sent to this IP address is forwarded to all members of the multicast group.

Routers between the source and recipients duplicate data packets and forward multiple copies wherever the path to recipients diverges. Group membership information is used to calculate the best routers at which to duplicate the packets in the data stream to optimize the use of the network.

A source host sends data to a multicast group by simply setting the destination IP address of the datagram to be the multicast group address. Any host can become a source and send data to a multicast group. Sources do not need to register in any way before they can begin sending data to a group, and do not need to be members of the group themselves.

There are many different multicast protocols and modes of operation, each optimized for a particular scenario. Many of these are still at an early stage of standardization. However, they all operate in the same general way, as follows.

- A **Multicast Group Membership Discovery** protocol is used by receiving hosts to advertise their group membership to a local multicast router, enabling them to join and leave multicast groups. The main Multicast Group Membership Discovery protocols are Internet Group Management Protocol (IGMP) for IPv4 and Multicast Listener Discovery (MLD) for IPv6.

- A **Multicast Routing Protocol** is used to communicate between multicast routers and enables them to calculate the multicast distribution tree of receiving hosts. Protocol Independent Multicast (PIM) is the most important Multicast Routing Protocol.

The multicast distribution tree of receiving hosts holds the route to every recipient that has joined the multicast group, and is optimized so that

- multicast traffic does not reach networks that do not have any such recipients (unless the network is a transit network on the way to other recipients)

- duplicate copies of packets are kept to a minimum.

Significance:

This one provides a protocol for sending the call/data from one mobile station to several other stations.

5. TCP over Wireless networks:

Concept:

Slow Start

TCP s reaction to a missing acknowledgement is quite drastic but it is necessary to get rid of congestion quickly.

The behavior shows after the detection of congestion is called **Slow start.** The sender always calculates a Congestion window for a receiver.

The start size of the congestion window is one segment (TCP Packet). The sender sends one packet and waits for acknowledgement.

If this acknowledgement arrives the sender increases the congestion window by one now sending two packets (congestion window=2)

After arrival of the two corresponding acknowledgements now the congestion window equals 4. This scheme doubles the congestion window every time the acknowledgements come back which takes one **Round Trip Time (RIT**).This is called the exponential growth of the congestion window in the slow start mechanism.

It is too dangerous to double the congestion window each time because the steps might become too large. The exponential growth stops at the **Congestion Threshold.**

The congestion window reaches the congestion threshold further increase of the transmission rate is only linear by adding 1 to the congestion window each time the acknowledgements come back.

Linear increase continues until a time-out at the sender occurs due to a missing acknowledgement or until the sender detects a gap in transmitted data because of continuous acknowledgements for the same packet.

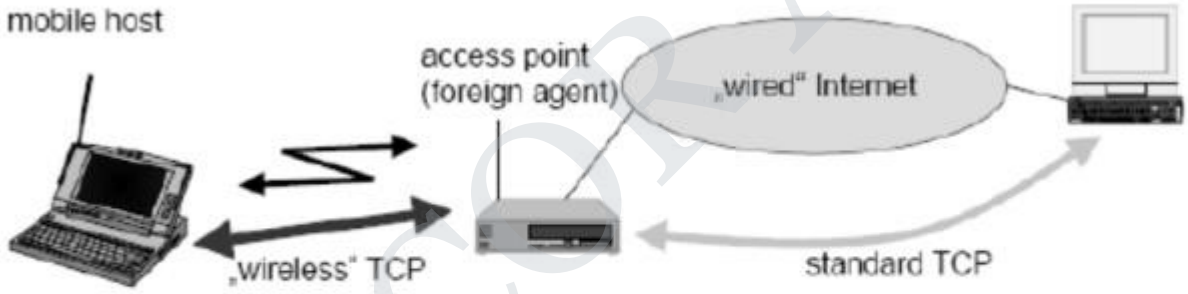
In either case the sender sets the congestion threshold to half of the current congestion window. The congestion window itself is set to one segment and the sender starts sending a single segment.

The exponential growth starts once more up to the new congestion threshold then the window grows in Linear fashion.

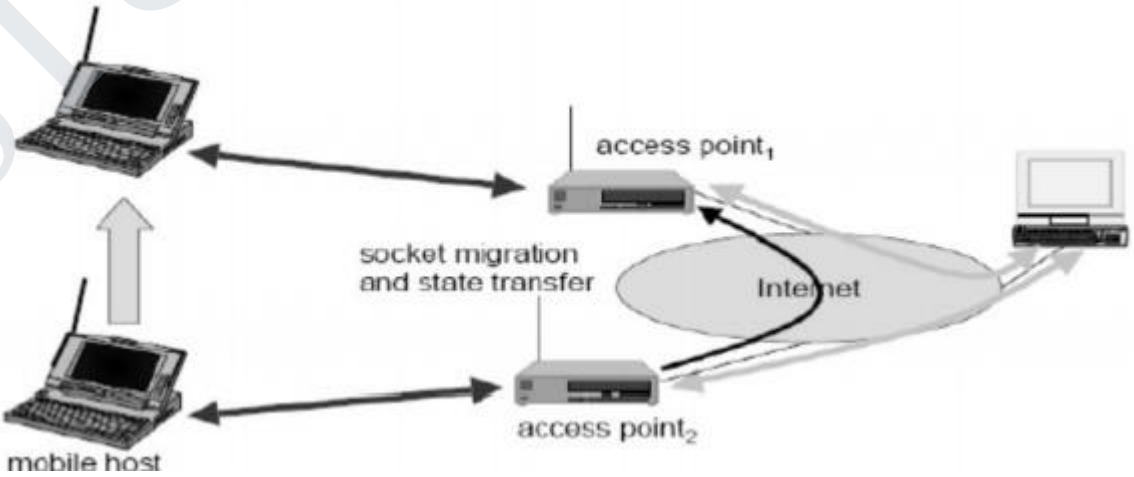
Significance:

Can be used in wireless communications too.

6. Indirect TCP or I-TCP Concept:



I-TCP socket and State migration



Indirect TCP Advantages and Disadvantages

Disadvantages

Loss of end-to-end semantics, an acknowledgement to a sender does now not any longer mean that a receiver really got a packet, foreign agents might crash.

Higher latency possible due to buffering of data with the foreign agent and forwarding to a new foreign agent

High trust at foreign agent; end-to-end encryption impossible

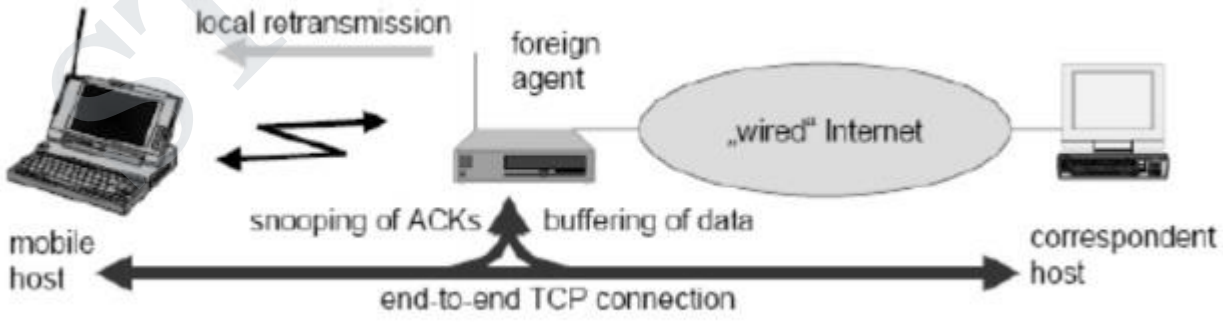
Significance:

No changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work

Transmission errors on the wireless link do not propagate into the fixed network simple to control, mobile TCP is used only for one hop, between a foreign agent and a mobile host Therefore, a very fast retransmission of packets is possible, the short delay on the mobile hop is known

7. Snooping TCP

Concepts:



The foreign agent buffers all packets with D**estination mobile host.**

Additionally snoops the packet flow in both directions to recognize acknowledgements.

The reason for buffering the packets toward the mobile node is to enable the foreign agent to perform a local transmission in case of packet loss on the wireless link.

The foreign agent buffers every packet until it receives an acknowledgement from the mobile host.

If the foreign agent does not receive an acknowledgement from the mobile host within a certain amount of time either the **packet** or the **acknowledgement** has been lost.

Alternatively the foreign agent could receive a duplicate ACK which also shows the loss of a packet.

Now the foreign agent

- Retransmits the packet directly from the buer.
- Performing a much faster retransmission completed to the correspondent host.
- The time out for acknowledgements can be much shorter because it reflects only the delay of one hop plus processing time.
- To remain transparent the foreign agent must not acknowledge data to the correspondent host.
- The correspondent host believe that the mobile host had received the data would violate the end-to end semantic in case of a foreign agent failure.
- The foreign agent can filter the duplicate acknowledgements to avoid unnecessary retransmissions of data from the correspondent host.

If the foreign agent now crashes the time-out of the correspondent host still works and triggers a retransmission.

The foreign agent may discard duplicates of packets already retransmitted locally and acknowledged by the mobile host.

Significance:

This avoids unnecessary traffic on the wireless link.

8. Mobile TCP Concept:

Special handling of lengthy and/or frequent disconnections

M-TCP splits as I-TCP does unmodified TCP fixed network to supervisory host (SH)

optimized TCP SH to MH Supervisory host no caching, no retransmission monitors all packets, if disconnection detected l set sender window size to 0

l sender automatically goes into persistent mode q old or new SH reopen the window Disadvantages

loss on wireless link propagated into fixed network adapted TCP on wireless link

Significance:

maintains semantics, supports disconnection, no buffer forwardin

9. Fast Retransmit / Fast Recovery

Concept:

Reduction of the congestion threshold

A sender receiving continuous acknowledgements for the same packets. This informs the sender of two things. One is that the receiver got all packets up to the acknowledged packet in sequence.

Fast Retransmit

In TCP a receiver sends acknowledgement only if it receives any packet from the sender.
Receiving acknowledgements from a receiver also shows that the receiver continuous receives something from the sender.

The gap in the packet stream is not due to severe congestion but a simple packet loss due to transmission error.

The sender can now retransmit the missing packet(s) before the timer expires. This is calle **Fast Retransmit.**

Fast Recovery
The receipt of acknowledgements shows that there is no congestion to justify a slow start.
The sender can continue with the current congestion window.
The sender performs a **Fast Recovery** from the packet loss.
This mechanism can improve the efficiency of TCP dramatically.

The other reason for activating slow start is a time-out due to a missing acknowledgement. TCP using Fast Retransmit / Fast Recovery interprets this congestion in the

network and activates the slow start mechanism.

10. Transmission / Timeout Freezing-Selective Retransmission

Concepts:

Mobile hosts can be disconnected for a longer time

no packet exchange possible, e.g., in a tunnel, disconnection due to overloaded cells or mux. with higher priority traffic TCP disconnects after time-out completely

TCP freezing

MAC layer is often able to detect interruption in advance MAC can inform TCP layer of upcoming loss of connection TCP stops sending, but does not assume a congested link MAC layer signals again if reconnected

Disadvantage

TCP on mobile host has to be changed, mechanism depends on MAC layer

Significance:

Scheme is independent of data

11. Transaction Oriented TCP- TCP over 2.5 / 3G wireless Networks

Concepts:

Fine tuning today s TCP Learn to live with

_ Data rates: 64 kbit/s upstream, 384 kbit/s downstream (UMTS release99); asymmetry: 3-6, but also up to 1000 (broadcast systems), periodic allocation/release of channels

_ High latency, high jitter, packet loss Suggestions

_ Large (initial) window size, large maximum transfer unit, selective acknowledgement, explicit congestion notification, timestamps, no header compression

Already in use _ i-mode in Japan

_ WAP 2.0 (TCP with wireless profile) Transport layer

_ Local retransmissions and acknowledgements Additionally on the application layer

_ Content filtering, compression, picture downscaling _ E.g., Internet/WAP gateways

_ Web service gateways?

Big problem: breaks end-to-end semantics _ Disables use of IP security!

More issues

RFC 3150 (slow links)

_ Recommends header compression, no timestamp RFC 3155 (links with errors)

_ States that explicit congestion notification cannot be used In contrast to 2.5G/3G recommendations!

Significance:

Used to differentiate the 2.8G/3G over the TCP

Applications:

- Fine tuned for Mobile usage over the TCP

o Almost all the Devices Makes use of this layer for sending the data o Used for the Mobile devices that are designed these days either2.5/3G

IT8602 MOBILE COMMUNICATION	
UNIT V MOBILE TRANSPORT AND APPLICATION LAYER	9
Mobile TCP– WAP – Architecture – WDP – WTLS – WTP –WSP – WAE – WTA Architecture – WML	

Chapter: Mobile Communication

| Study Material, Lecturing Notes, Assignment, Reference, Wiki description explanation, brief detail |

Application Layer

1. WAP Model 2. Mobile Location based services 3. WAP Gateway 4. WAP protocols 5. WAP user agent profile 6. caching mode 7. wireless bearers for WAP 8. WML WMLScripts 9. WTA- iMode-,SyncML

APPLICATION LAYER

1. **WAP Model**
2. **Mobile Location based services**
3. **WAP Gateway**
4. **WAP protocols**
5. **WAP user agent profile**
6. **caching mode**
7. **wireless bearers for WAP**
8. **WML WMLScripts**
9. **WTA- iMode-,SyncML**

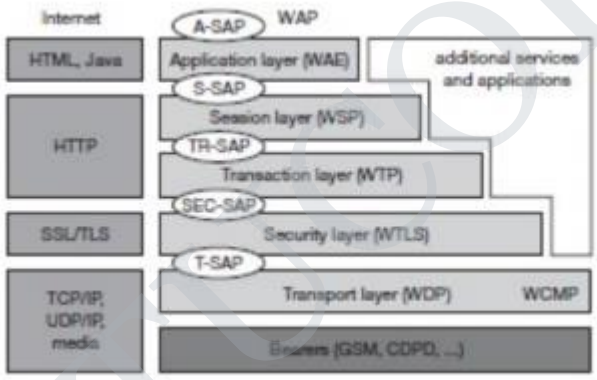
Pre requisite discussion:

The growth of the internet, internet applications, and mobile communication led to many early proprietary solutions providing internet services for mobile, wireless devices. Some of the problems these partial solutions face were discussed in section

1.WAP Model

Concept:

Figure below gives an overview of the WAP architecture, its protocols and components, and compares this architecture with the typical internet architecture when using the world wide web. This comparison is often cited by the WAP Forum and it helps to understand the architecture (WAP Forum, 2000a). This comparison can be misleading as not all components and protocols shown at the same layer are comparable. For consistency reasons with the existing specification, the following stays with the model as shown in Figure below The basis for transmission of data is formed by different **bearer services**. WAP does not specify bearer services, but uses existing data services and will integrate further services. Examples are message services, such as short message service (SMS) of GSM, circuit-switched data, such as high-speed circuit switched data (HSCSD) in GSM, or packet switched data, such as general packet radio service (GPRS) in GSM. Many other bearers are supported, such as CDPD, IS-136, PHS. No special interface has been specified between the bearer service and the next higher layer, the **transport layer** with its **wireless datagram protocol (WDP)** and the additional **wireless control message protocol (WCMP),** because the adaptation of



these protocols are bearer-specific (WAP Forum, 2000u). The transport layer offers a bearer independent, consistent datagram-oriented service to the higher layers of the WAP architecture. Communication is done transparently over one of the available bearer services. The **transport layer service access point (T-SAP)** is the common interface to be used by higher layers independent of the underlying network. The next higher layer, the **security layer** with its **wireless transport layer security** protocol **WTLS** offers its service at the **security SAP (SEC-SAP)**. WTLS is based on the transport layer security (TLS, formerly SSL, secure sockets layer) already known from the www. WTLS has been optimized for use in wireless networks with narrow-band channels. It can offer data integrity, privacy, authentication, and (some) denial-of-service protection. The WAP **transaction layer** with its **wireless transaction protocol (WTP)** offers a lightweight transaction service at the **transaction SAP (TR-SAP)**. This service

efficiently provides reliable or unreliable requests and asynchronous transactions. Tightly coupled to this layer is the next higher layer, if used for connection-oriented service. The **session layer** with the **wireless session protocol (WSP)** currently offers two services at the **session-SAP (S-SAP)**, one connection-oriented and one connectionless if used directly on top of WDP. A special service for browsing the web (WSP/B) has been defined that offers HTTP/1.1 functionality, long-lived session state, session suspend and resume, session migration and other features needed for wireless mobile access to the web. Finally the **application layer** with the **wireless application environment (WAE)** offers a framework for the integration of different scripting languages, special markup languages, interfaces to telephony applications, and many content formats adapted to the special requirements of small, handheld, wireless devices. Figure 10.9 not only shows the overall WAP architecture, but also its relation to the traditional internet architecture for www applications. The WAP transport layer together with the bearers can be (roughly) compared to the services offered by TCP or UDP over IP and different media in the internet. If a bearer in the WAP architecture already offers IP services (e.g., GPRS, CDPD) then UDP is used as WDP. The TLS/SSL layer of the internet has also been adopted for the WAP architecture with some changes required for optimization. The functionality of the session and transaction layer can roughly be compared with the role of HTTP in the web architecture. However, HTTP does not offer all the additional mechanisms needed for efficient wireless, mobile access (e.g., session migration, suspend/resume). Finally, the application layer offers similar features as HTML and Java. Again, special formats and features optimized for the wireless scenario have been defined and telephony access has been added. WAP does not always force all applications to use the whole protocol architecture. Applications can use only a part of the architecture. For example, this means that, if an application does not require security but needs the reliable transport of data, it can **directly** use a service of the transaction layer. Simple applications can directly use WDP. Different scenarios are possible for the integration of WAP components into existing wireless and fixed networks (see Figure 10.10). On the left side, different fixed networks, such as the traditional internet and the public switched telephone network (PSTN), are shown. One cannot change protocols and services of these existing networks so several new elements will be implemented between these networks and the WAP-enabled wireless, mobile devices in a wireless network on the right-hand side.

Significance:

- **interoperable,** i.e., allowing terminals and software from different vendors to communicate with networks from different providers;

- **scaleable,** i.e., protocols and services should scale with customer needs and number of customers;

- **efficient,** i.e., provision of QoS suited to the characteristics of the wireless and mobile networks;

- **reliable,** i.e., provision of a consistent and predictable platform for deploying services; and

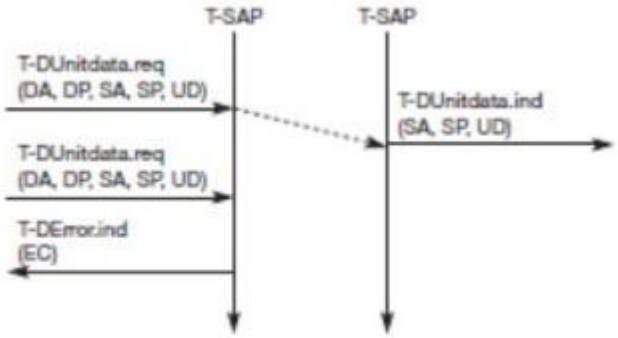
- **secure,** i.e., preservation of the integrity of user data, protection of devices and services from security problems.

2. Mobile Location based services

Concept:

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 (WAP Forum, 2000b). To offer this consistent service, the adaptation needed in the transport layer can differ depending on the services of the bearer. The closer the bearer service is to IP, the smaller the adaptation can be. If the bearer already offers IP services, UDP (Postel, 1980) is used as WDP. WDP offers more or less the same services as UDP. WDP offers **source** and **destination port numbers** used for multiplexing and demultiplexing 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 the receiver and sender of the user data. These could be MSISDNs (i.e., a telephone number), IP addresses, or any other unique identifiers. The **T-DUnitdata.ind** service primitive indicates the reception of data. Here destination address and port are only optional parameters.



If a higher layer requests a service the WDP cannot fulfill, this error is indicated with the **T-DError.ind** service primitive as shown in. An **error code (EC)** is returned indicating the reason for the error to the higher layer. WDP is not allowed to use this primitive to indicate problems with the bearer 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 entity to another (e.g. the destination is unreachable, no application is listening to the specified destination port etc.), the **wireless control message protocol (WCMP)** provides error handling mechanisms for WDP (WAP Forum, 2000r) and should therefore be implemented. WCMP contains control messages that resemble the internet control message protocol (ICMP (Postel, 1981b) for IPv4, (Conta, 1998) 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 WCMP error 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 information about changes in the environment, which may influence the correct operation of WDP. Important information is the current configuration of the device, currently available bearer services, processing and memory resources etc. Design and implementation of this management component is considered vendor-specific and is outside the scope of WAP. If the bearer already offers IP transmission, WDP (i.e., UDP in this case) relies on the segmentation (called fragmentation in the IP context) and reassembly capabilities of the IP layer as specified in (Postel, 1981a). Otherwise, WDP has to include these capabilities, which is, e.g., necessary for the GSM SMS

Significance:

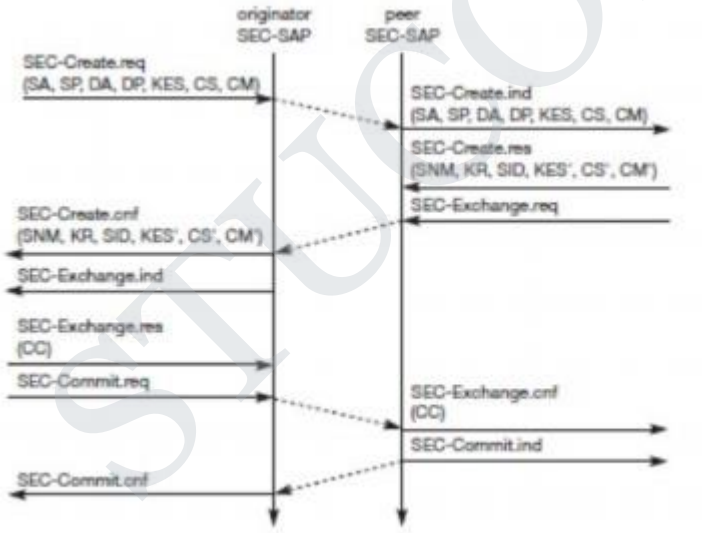
Makes the Mobile systems faster.

The WAP is applied in almost all the Base Station infrastructures.

3. WAP Gateway

Conept:

If requested by an application, a security service, the **wireless transport layer security (WTLS)**, can be integrated into the WAP architecture on top of WDP as specified in (WAP Forum, 2000c). WTLS can provide different levels of security (for privacy, data integrity, and authentication) and has been optimized for low bandwidth, high-delay bearer networks. WTLS takes into account the low processing power and very limited memory capacity of the mobile devices for cryptographic algorithms. WTLS supports datagram and connection-oriented transport layer protocols. New compared to, e.g. GSM, is the security relation between two peers and not only between the mobile device and the base station (see chapter 4). WTLS took over many features and mechanisms from TLS (formerly SSL, secure sockets layer (Dierks, 1999)), but it has an optimized handshaking between the peers.



Before data can be exchanged via WTLS, a secure session has to be established. This session establishment consists of several steps: illustrates the sequence of service primitives needed for a so-called full handshake (several optimizations are possible). The originator and the peer of the secure session can both interrupt session establishment any time, e.g., if the parameters proposed are not acceptable. The first step is to initiate the session with the **SEC-Create** primitive.

Parameters are **source address (SA), source port (SP)** of the originator, **destination address**

(DA), destination port (DP) of the peer. The originator proposes **a key exchange suite (KES)**

(e.g., RSA (Rivest, 1978), DH (Diffie, 1976), ECC (Certicom, 2002)), a **cipher suite (CS)** (e.g., DES, IDEA (Schneier, 1996), and **a compression method (CM)** (currently not further specified). The peer answers with parameters for the **sequence number mode (SNM)**, the **key refresh** cycle (**KR**) (i.e., how often keys are refreshed within this secure session), the **session identifier (SID)** (which is unique with each peer), and the selected **key exchange suite (KES), cipher suite (CS), compression method (CM** .The**)** peer also issues a **SEC-Exchange primitive**. This indicates that the peer wishes to perform public-key authentication with the client, i.e., the peer requests a **client certificate (CC)** from the originator. The first step of the secure session creation, the negotiation of the security parameters and suites, is indicated on the originator s side, followed by the request for a certificate. The originator answers with its certificate and issues a **SEC-Commit.req** primitive. This primitive indicates that the handshake is com pleted for the originator s side and that the originator now wants to switch into the newly negotiated connection state. The certificate is delivered to the peer side and the SEC-Commit is indicated. The WTLS layer of the peer sends back a confirmation to the originator. This concludes the full handshake for secure session setup. After setting up a secure connection between two peers, user data can be exchanged. This is done using the simple **SEC-Unitdata** primitive as shown in the figure below. SEC-Unitdata has exactly the same function as T-DUnitdata on the WDP layer, namely it transfers a datagram between a sender and a receiver. This data transfer is still unreliable, but is now secure. This shows that WTLS can be easily plugged into the protocol stack on top of WDP. The higher layers simply use SEC-Unitdata instead of T-DUnitdata. The parameters are the same here: **source address (SA), source port (SP), destination address (DA), destination port (DP),** and **user data (UD)**. This section will not discuss the security-related features of WTLS or the pros and cons of different encryption algorithms. The reader is referred to the specification (WAP Forum, 2000c) and excellent cryptography literature e.g., (Schneier, 1996), (Kaufman, 1995). Although WTLS allows for different encryption mechanisms with different key lengths, it is quite clear that due to computing power on the handheld devices the encryption provided cannot be very strong. If applications require stronger security, it is up to an application or a user to apply stronger encryption on top of the whole protocol stack and use WTLS as a basic security level only. Many programs are available for this purpose. It is important to note that the security association in WTLS exists between the mobile WAP-enabled device and a WAP

server or WAP gateway only. If an application accesses another server via the gateway, additional mechanisms are needed for end-to-end security. If for example a user accesses his or her bank account using WAP, the WTLS security association typically ends at the WAP gateway inside the network operator s domain. The bank and user will want to apply additional security mechanisms in this scenario. Future work in the WTLS layer comprises consistent support for application level security (e.g. digital signatures) and different implementation classes with different capabilities to select from.

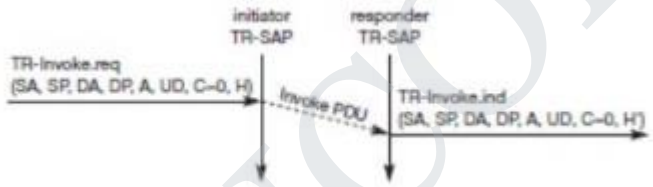
4. WAP protocols Conept:

The **wireless transaction protocol (WTP)** is on top of either WDP or, if security is required, WTLS (WAP Forum, 2000d). WTP has been designed to run on very thin clients, such as mobile phones. WTP offers several advantages to higher layers, including an improved reliability over datagram services, improved efficiency over connection-oriented services, and support for transaction-oriented services such as web browsing. In this context, a transaction is defined as a request with its response, e.g. for a web page. WTP offers many features to the higher layers. The basis is formed from three **classes of transaction service** as explained in the following paragraphs. Class 0 provides unreliable message transfer without any result message. Classes 1 and 2 provide reliable message transfer, class 1 without, class 2 with, exactly one reliable result message (the typical request/response case). WTP achieves reliability using **duplicate removal, retransmission, acknowledgement**s and unique **transaction identifiers**. No WTP-class requires any connection set-up or tear-down phase. This avoids unnecessary overhead on the communication link. WTP allows for **asynchronous transactions, abort of transactions, concatenation of messages**, and can **report success or failure** of reliable messages (e.g., a server cannot handle the request). To be consistent with the specification, in the following the term **initiator** is used for a WTP entity initiating a transaction (aka client), and the term **responder** for the WTP entity responding to a transaction (aka server). The three service primitives offered by WTP are **TR-Invoke** to initiate a new transaction, **TR-Result** to send back the result of a previously initiated transaction, and **TR-Abort** to abort an existing transaction. The PDUs exchanged between two WTP entities for normal transactions are the **invoke PDU, ack PDU**, and **result PDU**. The use of the service primitives, the PDUs, and the associated parameters with the classes of transaction service will be explained in the following sections. A special feature of WTP is its ability to provide a **user acknowledgement** or, alternatively, an **automatic acknowledgement** by the WTP entity. If user acknowledgement is required, a WTP user has to confirm every message received by a WTP entity. A user

acknowledgement provides a stronger version of a confirmed service because it guarantees that the response comes from the user of the WTP and not the WTP entity itself.

WTP class 0

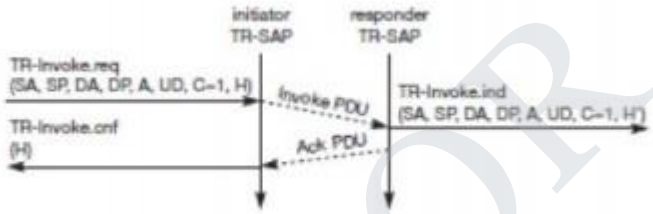
Class 0 offers an unreliable transaction service without a result message. The transaction is stateless and cannot be aborted. The service is requested with the **TR-Invoke.req** primitive as shown in Figure 10.14. Parameters are the **source address (SA), source port (SP), destination address (DA), destination port (DP)** as already explained in section 10.3.2. Additionally, with the **A** flag the user of this service can determine, if the responder WTP entity should generate an **acknowledgement** or if a user acknowledgement should be used. The WTP layer will transmit the **user data (UD)** transparently to its destination. The class type **C** indicates here class 0. Finally, the transaction **handle H** provides a simple index to uniquely identify the transaction and is an alias for the tuple (SA, SP, DA, DP), i.e., a socket pair, with only local significance.



The WTP entity at the initiator sends an invoke PDU which the responder receives. The WTP entity at the responder then generates a **TR-Invoke.ind** primitive with the same parameters as on the initiator s side, except for H which is now the local handle for the transaction on the responder s side. In this class, the responder does not acknowledge the message and the initiator does not perform any retransmission. Although this resembles a simple datagram service, it is recommended to use WDP if only a datagram service is required. WTP class 0 augments the transaction service with a simple datagram like service for occasional use by higher layers.

WTP class 1

Class 1 offers a reliable transaction service but without a result message. Again, the initiator sends an invoke PDU after a **TR-Invoke.req** from a higher layer. This time, class equals 1 , and no user acknowledgement has been selected as shown in Figure 10.15. The responder signals the incoming invoke PDU via the **TR-Invoke.ind** primitive to the higher layer and acknowledges automatically without user intervention. The specification also allows the user on the responder s side to acknowledge, but this acknowledgement is not required. For the initiator the transaction ends with the reception of the acknowledgement. The responder keeps the transaction state for some time to be able to retransmit the acknowledgement if it receives the same invoke PDU again indicating a loss of the acknowledgement. If a user of the WTP class 1 service on the initiator s side requests a user acknowledgement on the responder s side, the sequence diagram looks like the fig below. Now the WTP entity on the responder s side does not send an acknowledgement automatically, but waits for the **TR-Invoke.res** service primitive from



the user. This service primitive must have the appropriate local handle H for identification of the right transaction. The WTP entity can now send the ack PDU. Typical uses for this transaction class are reliable push services.

WTP class 2

Finally, class 2 transaction service provides the classic reliable request/response transaction known from many client/server scenarios. Depending on user requirements, many different scenarios are possible for initiator/responder interaction. Three examples are presented below. The basic transaction of class 2 without-user acknowledgement. Here, a user on the initiator s side requests the service and the WTP entity sends the invoke PDU to the responder. The WTP entity on the responder s side indicates the request with the**TR-Invoke.ind** primitive to a user. The responder now waits for the processing of the request, the user on the responder s side can finally give the result UD* to the WTP entity on the responder.

Wireless session protocol

The **wireless session protocol (WSP)** has been designed to operate on top of the datagram service WDP or the transaction service WTP (WAP Forum, 2000e). 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 general features needed for content exchange between cooperating clients and servers:

Significance:

● **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.

5. WAP user agent profile

Conept:

The schema for WAP User Agent Profiles consists of description blocks for the following key components:

HardwarePlatform: A collection of properties that adequately describe the hardware characteristics of the terminal device. This includes, the type of device, model number, display size, input and output methods, etc.

SoftwarePlatform: A collection of attributes associated with the operating environment of the device. Attributes provide information on the operating system software, video and audio encoders supported by the device, and user s preference on language .

BrowserUA: A set of attributes to describe the HTML browser application **NetworkCharacteristics:** Information about the network-related infrastructure and environment such as bearer information. These attributes can influence the resulting content, due to the variation in capabilities and characteristics of various network infrastructures in terms of bandwidth and device accessibility.

WapCharacteristics: A set of attributes pertaining to WAP capabilities supported on the device. This includes details on the capabilities and characteristics related to the WML Browser, WTA [WTA], etc.

Significance:

Faster when compared to all other user agent profiles.

6. Caching mode Conept:

Caching can reduce the bandwidth requirement in a mobile computing environment. However, due to battery power limitations, a wireless mobile computer may often be forced to operate in a doze (or even totally disconnected) mode. As a result, the mobile computer may miss some cache invalidation reports broadcast by a server, forcing it to discard the entire cache contents after waking up. In this paper, we present an energy-efficient cache invalidation method, called

GCORE (Grouping with COld update-set REtention), that allows a mobile computer to operate in a disconnected mode to save the battery while still retaining most of the caching benefits after a reconnection. We present an efficient implementation of GCORE and conduct simulations to evaluate its caching effectiveness. The results show that GCORE can substantially improve mobile caching by reducing the communication bandwidth (or energy consumption) for query processing

While a WSP session is established (whether active or suspended), the WAP gateway caches all Profile and Profile- Diff headers associated with that session. A third party host may issue a request for this CPI to, for instance, generate content that wil subsequently be pushed to the client device. The request is initiated from the third-party host and delivered to a Push Protocol Gateway (PPG). This specification defines neither a protocol for issuing this request nor a means for addressing the requested information. However, it is expected that such requests will typically be made to the WAP gateway using HTTP, as suggested by [WAP-PAP]. Upon receiving the profile request, the gateway accesses the cached Profile and Profile-Diff headers and resolves them to form a complete CPI profile. It responds to the CPI request with the resolved profile (a CC/PP document) using a MIME type of **text/xml**.

It is important to note that the WAP gateway has incomplete information about the current CPI. In particular, the gateway is not aware of any request-specific profile information that the client would have provided to the requesting third-party server. Moreover, the WAP gateway cannot incorporate attribute information from Profile-Diff headers that would have been added by intermediate proxies through which the request would have passed had it originated at the client device. Finally, if the WSP session is currently suspended, then the gateway may be caching out-of-date profile information.

7. Wireless bearers for WAP

Conept:

The above one defines properties for conformant User Agent Profiles, which are structured according to the CC/PP note [CC/PP], and correspondingly use RDF XML serialization syntax. This section defines a set of single-byte tokens corresponding to the attribute names and values of the RDF serialization

syntax. These tokens are distributed among three code pages. Code page zero (0) defines tokens for RDF serialization attributes. Code page one (1) defines tokens for properties in the core profile schema. Code page two (2) defines tokens for properties in the Browser useragent component of the schema. User agents or applications other than the browser may define additional attribute code pages for their own properties. Each user agent or application that wants to define properties for use in the user agent profile MUST first define a component to hold its properties. The name of the component MUST be globally unique. Each such user agent component is considered to have a unique namespace, so that, for example, the property BackgroundColor for User Agent A is a property distinct from the property BackgroundColor for User Agent B. See Section 7for more information. In addition, each user agent or application SHOULD define a series of token table code pages containing the properties from its component. If it chooses to define code pages, then it SHOULD define at least two: one in the "Tag" space and one in the "Attribute" space. The property names SHOULD be inserted into each page. Any wellknown values for the properties should be inserted into the "Attribute" page. Additional pages may be required if the component contains a large number of properties. A default user agent has been defined as part of the schema: the browser.

Significance:

These wireless bearers provides a major advantage of making a wireless telecommunication using the WAP

8. WML WMLScripts

Conept:

WML (Wireless Markup Language), formerly called HDML (Handheld Devices Markup Languages), is a language that allows the text portions of Web pages to be presented on cellular telephones and personal digital assistants (PDAs) via wireless access. WML is part of the Wireless Application Protocol (WAP) that is being proposed by several vendors to standards bodies. The Wireless Application Protocol works on top of standard data link protocols, such as Global System for Mobile communication, code-division multiple access, and Time Division Multiple Access, and provides a complete set of network communication programs comparable to and supportive of the Internet set of protocols.

WML is an open language offered royalty-free. Specifications are available at Phone.com's Web site. According to Phone.com, any programmer with working knowledge of HTML, common gateway interface, and Structured Query Language should be able to write a presentation layer using WML. A filter program can be written or may be available from a vendor that will translate HTML pages into WML pages.

Significance:

This WML is much more preferred than the HTML mainly because of its User interface

9. WTA- iMode-,SyncM

Conept:

The most common wireless technologies use radio. With radio waves distances can be short, such as a few meters for television or as far as thousands or even millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of applications of radio wireless technology include GPS units, garage door openers, wireless computer mice, keyboards and headsets, headphones, radio receivers, satellite television, broadcast television and cordless telephones.

Somewhat less common methods of achieving wireless communications include the use of other electromagnetic wireless technologies, such as light, magnetic, or electric fields or the use of sound.

Light, colors, AM and FM radio, and electronic devices make use of the electromagnetic spectrum. The frequencies of the radio spectrum that are available for use for communication are treated as a public resource and are regulated by national organizations such as the Federal Communications Commission in the USA, or Ofcom in the United Kingdom. This determines which frequency ranges can be used for what purpose and by whom. In the absence of such control or alternative arrangements such as a privatized electromagnetic spectrum, chaos might result if, for example, airlines didn't have specific frequencies to work under and an amateur radio operator were interfering

with the pilot's ability to land an aircraft. Wireless communication spans the spectrum from 9 kHz to 300 GHz.

Applications:

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet. Standardized as IEEE 802.11 a,b,g,n, Wi-Fi approaches speeds of some types of wired Ethernet. Wi-Fi has become the de facto standard for access in private homes, within offices, and at public hotspots.[19] Some businesses charge customers a monthly fee for service, while others have begun offering it for free in an effort to increase the sales of their goods.

Cellular data service offers coverage within a range of 10-15 miles from the nearest cell site. Speeds have increased as technologies have evolved, from earlier technologies such as GSM, CDMA and GPRS, to 3G networks such as W-CDMA, EDGE or CDMA2000.

Mobile Satellite Communications may be used where other wireless connections are unavailable, such as in largely rural areasor remote locations. Satellite communications are especially important for transportation, aviation, maritime and military use

Wireless Sensor Networks are responsible for sensing noise, interference, and activity in data collection networks. This allows us to detect relevant quantities, monitor and collect data, formulate meaningful user displays, and to perform decision-making functions.