Mobile Computing

Unit 1 : Introduction

Outline

- Overview of Wireless and Mobile Infrastructure
- Preliminary Concepts
- Design Objectives and Performance Issues
- Radio resource Management
- Propagation and Path Loss Models
- Channel Interference and Frequency Reuse
- Cell Splitting
- Channel Assignment
- Overview of Generations

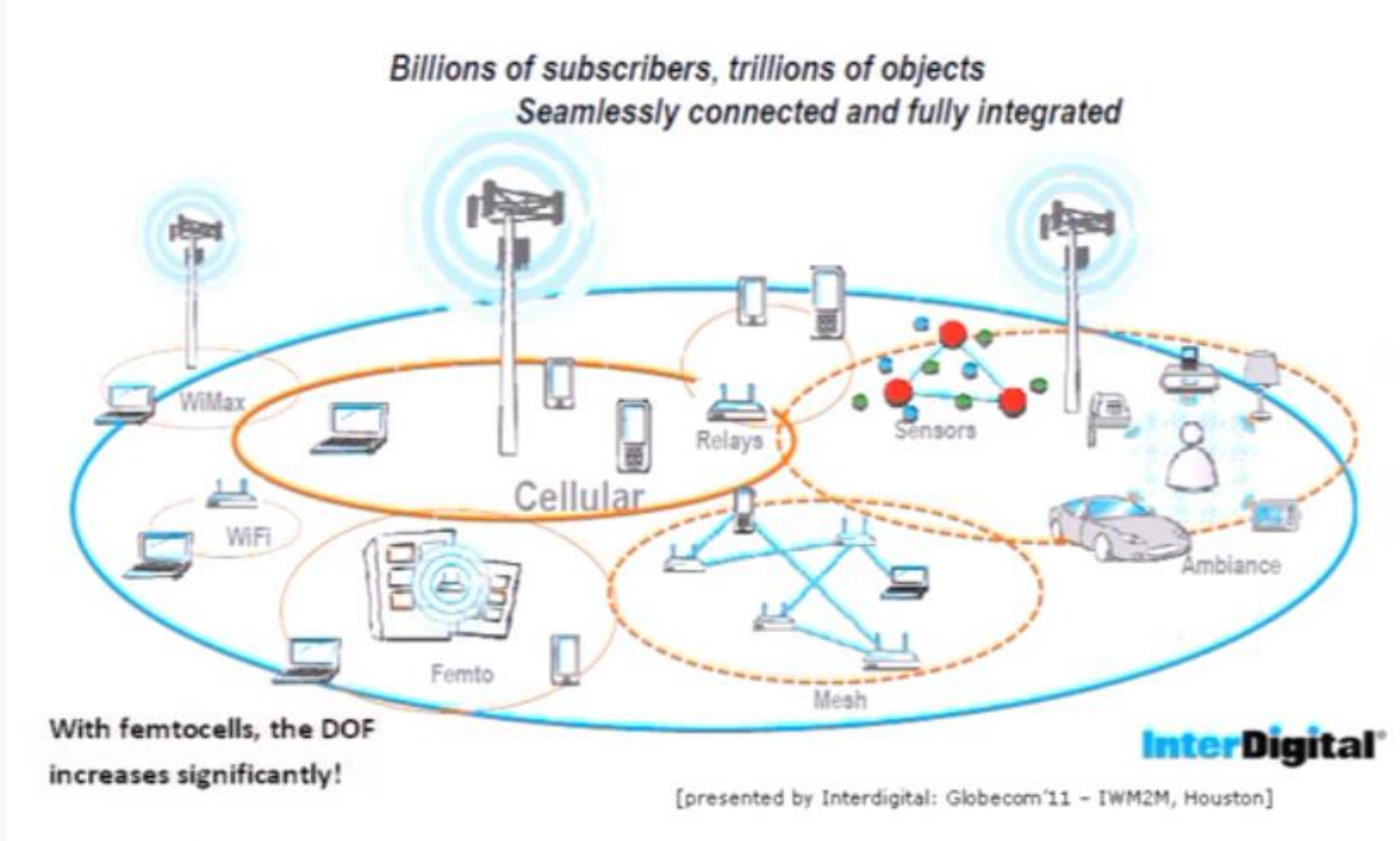
Why Mobile Computing?

- **Mobile refers to access in motion, no restriction on geographic location.**
- **With mobility comes lot of issues, techniques and solutions.**
- **80% of the world’s workforce is mobile.**
    - The demand for mobile communication creates the need for integration of wireless networks into existing fixed networks

Importance of Mobile Communication

- **Location Flexibility**
  - This has enabled users to work from anywhere as long as there is a connection established. A user can work without being in a fixed position.
- **Saves Time**
  - The time consumed or wasted while travelling from different locations or to the office and back, has been slashed
- **Enhanced Productivity**
  - Users can work efficiently and effectively from whichever location they find comfortable. This in turn enhances their productivity level.
- **Ease of Research**
  - Research has been made easier, since users earlier were required to go to the field and search for facts and feed them back into the system.
- **Entertainment**
- **Business processes are now easily available**

Heterogeneous



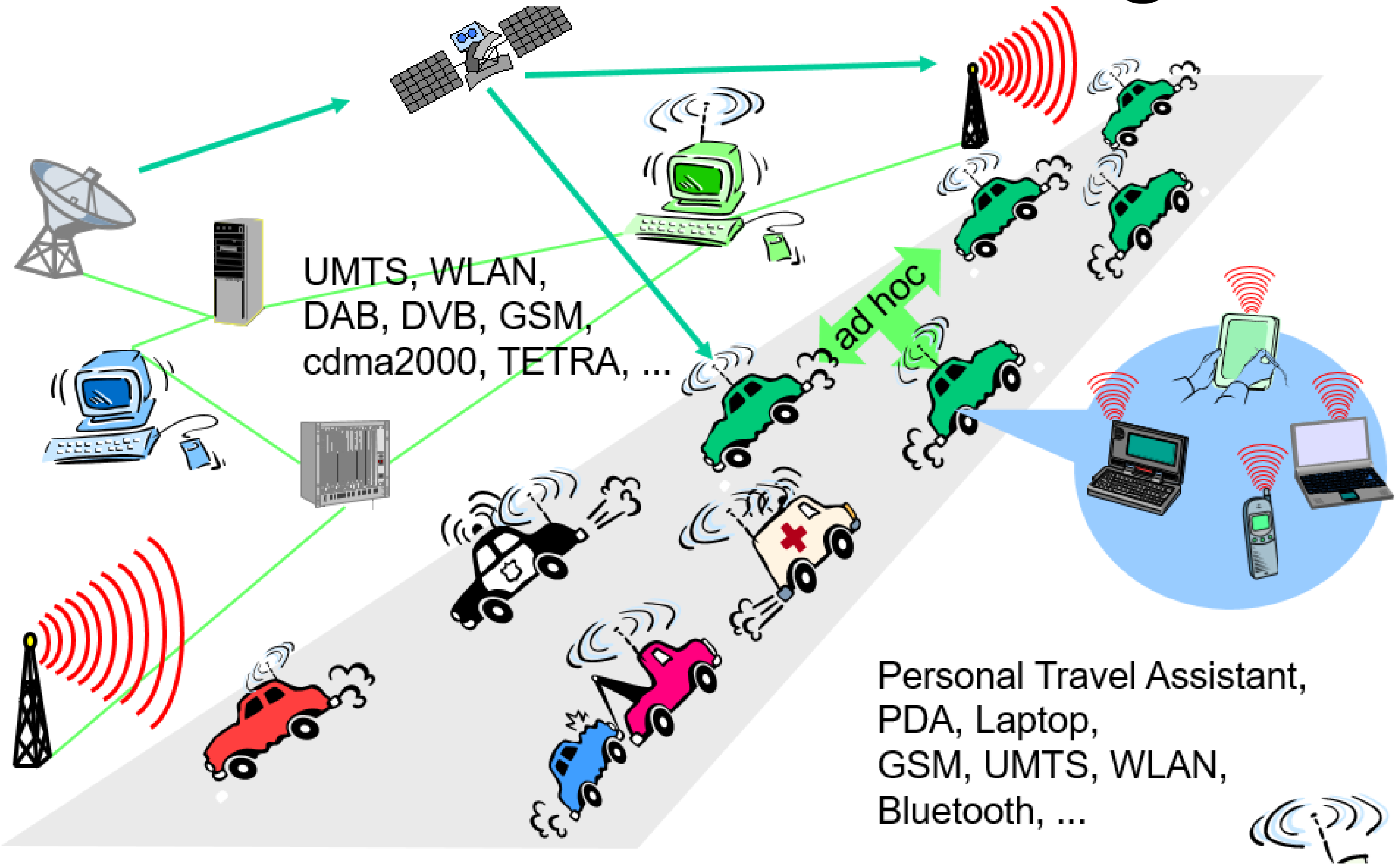
Applications

- Vehicles
  - transmission of news, road condition, weather, music via DAB
  - personal communication using GSM
  - position via GPS
  - local ad-hoc network with vehicles close-by to prevent accidents, guidance system, redundancy
  - vehicle data (e.g., from busses, high-speed trains) can be transmitted in advance for maintenance
- Emergencies
  - early transmission of patient data to the hospital, current status, first diagnosis
  - replacement of a fixed infrastructure in case of earthquakes, hurricanes, fire etc.
  - Disaster Management like crisis, floods, pandemic, ...

Applications

- Travelling salesmen
  - direct access to customer files stored in a central location
  - consistent databases for all agents
  - mobile office
- Replacement of fixed networks
  - remote sensors, e.g., weather, earth activities
  - flexibility for trade shows
  - LANs in historic buildings
- Entertainment, education, ...
  - outdoor Internet access
  - intelligent travel guide with up-to-date location dependent information
  - ad-hoc networks for multi user games

Example : Road Traffic Monitoring



Services Provided

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

Design Objectives of Mobile Computing

- Type of Application (Native or Mobile Web) : Before designing mobile application you need to determine type of application. ...
- Target device
- User experience
- Resource Constraint
- Multiple Platforms
- Security
- Network Communication

Issues in Mobile Computing

- Security, secrecy, and privacy
- Resource and spectrum utilizations
- Communication infrastructure
- Energy efficiency enhancement
- Integration of wireless information and power transfer
- Wireless access techniques
- Dynamic architecture and network functions analysis
- Coding and modulation
- Resource and interference management

https://www.frontiersin.org/articles/10.3389/frcmn.2020.00001/full

Different types of Mobile Networks

GSM : **Global System for Mobile communication**

- **(2G, 900MHz, 1900MHz Bands)**

LTE - Long Term Evolution

- (4G , for GSM *700, 750, 800 , 850 , 1800 , 1900 , 2100 , 2600 MHz*

HSDPA - High Speed Downlink Packet Access

- Advanced to 3G ,3.5 G

EV-DO – Evolution Data-Only.

- It mainly runs on CDMA Networks for 3G

CDMA – Code Division Multiple Access

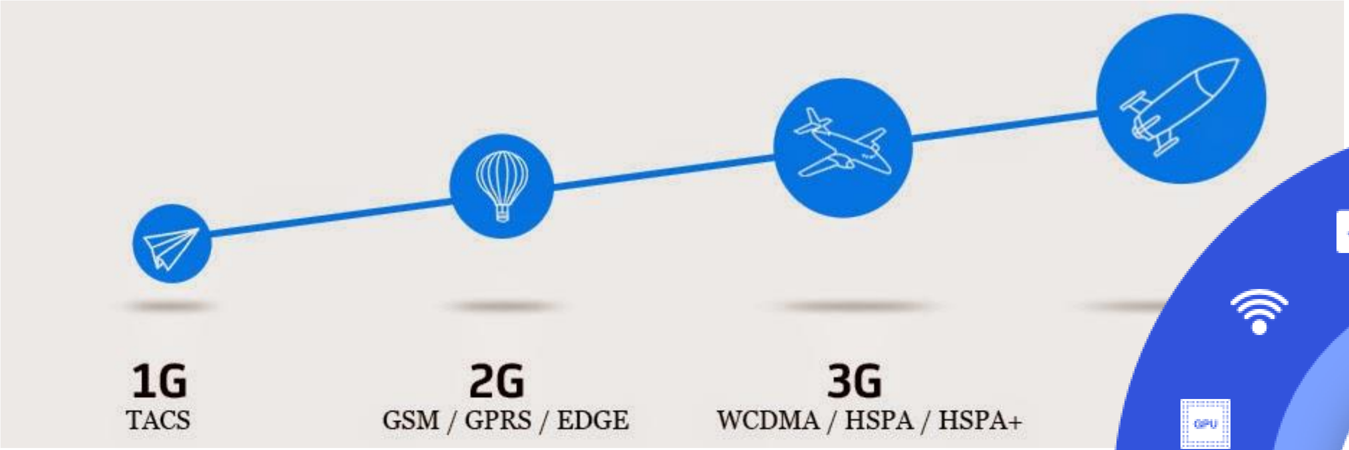
- **(3G Wireless, 450,800,1900MHz Bands)**

UMTS – Universal Mobile Telecommunications System

- (3G Technology WCDMA)

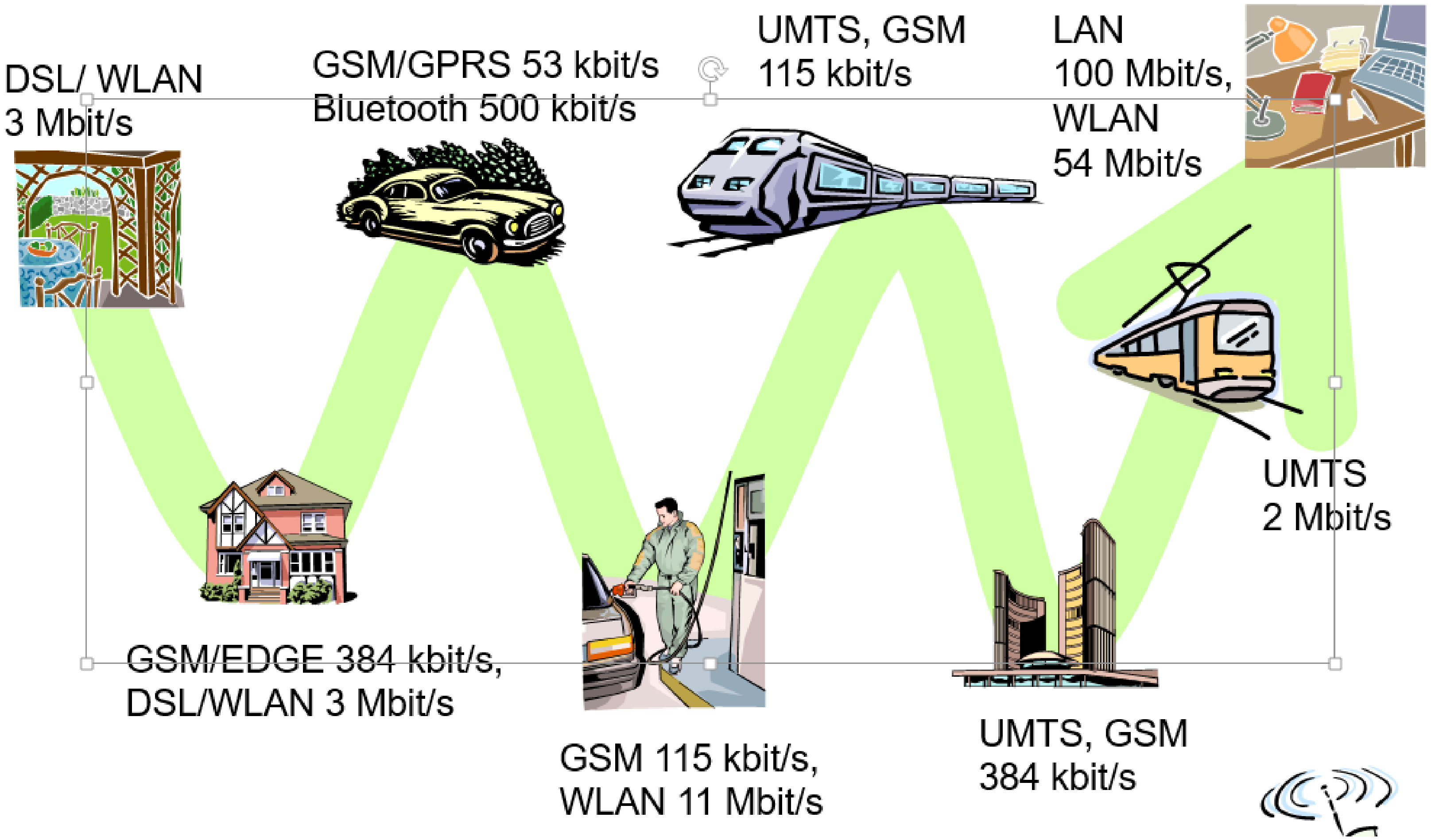
HSUPA – High Speed Uplink Packet Access

Types of Mobile Network



- Designed to connect virtually everyone and everything together including machines, objects, and devices.
- Deliver higher multi-Gbps peak data speeds

Mobile and Wireless Services



Two Aspects of Mobility

User Mobility	User mobility refers to a user who has access to the same or similar telecommunication services at different places, i.e., the user can be mobile, and the services will follow.
Device Portability	Device portability refers to the communication device moves (with or without a user). Many mechanisms in the network and inside the device have to make sure that communication is still possible while the device is moving. E.g; Mobile Phone System

Wireless	V/s	Mobile	Examples
✘		✘	stationary computer
✘		✔	notebook in a hotel
✔		✘	wireless LANs in historic buildings
✔		✔	Personal Digital Assistant (PDA)

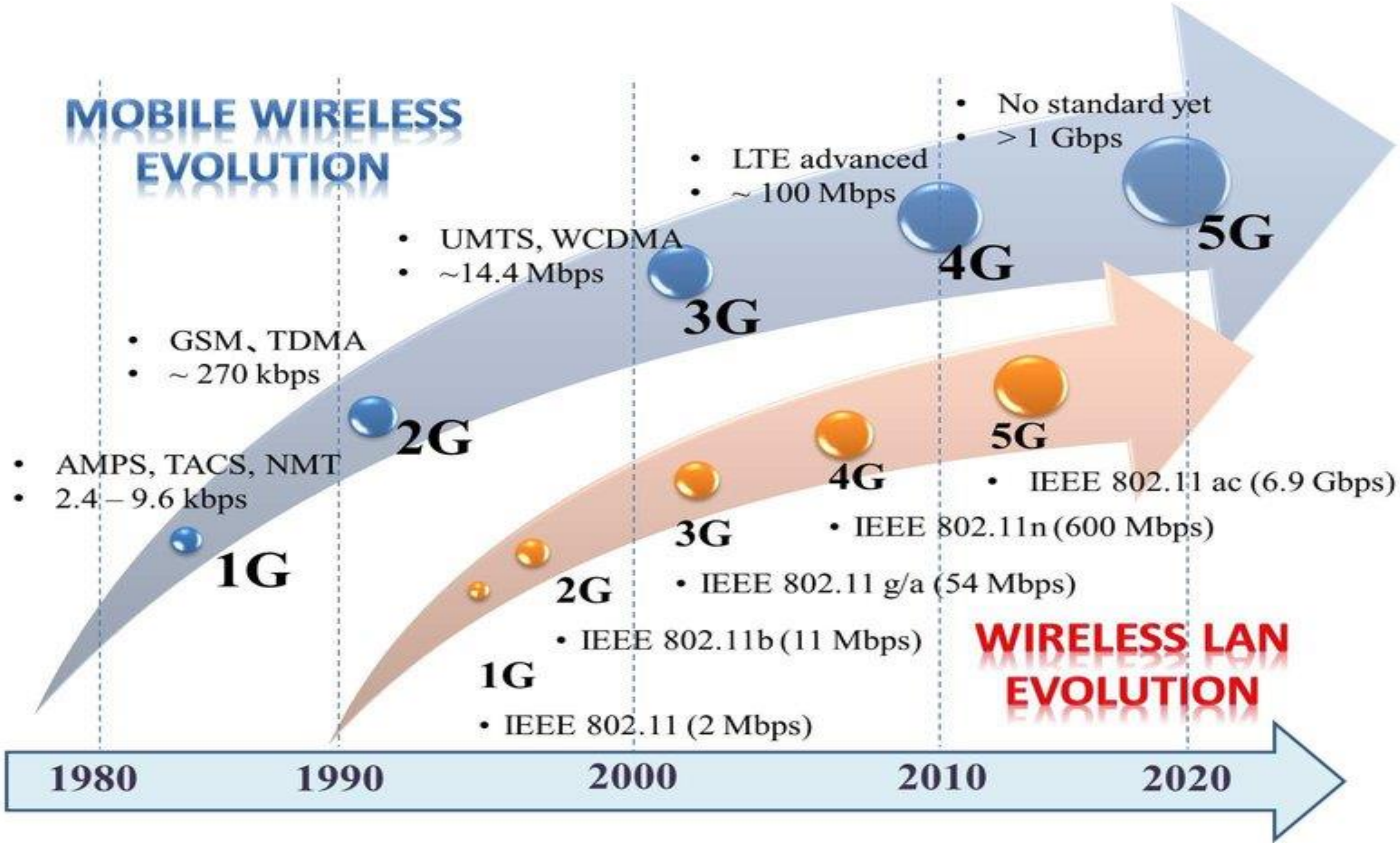
Effects of device Portability

- **Power consumption**
  - limited computing power, low quality displays, small disks due to limited battery capacity
  - CPU: power consumption ~ CV^2f
    - C: internal capacity, reduced by integration
    - V: supply voltage, can be reduced to a certain limit
    - f: clock frequency, can be reduced temporally
- **Loss of data**
  - higher probability, has to be included in advance into the design (e.g., defects, theft)
- **Limited user interfaces**
  - compromise between size of fingers and portability
  - integration of character/voice recognition, abstract symbols
- **Limited memory**
  - limited value of mass memories with moving parts
  - flash-memory or ? as alternative

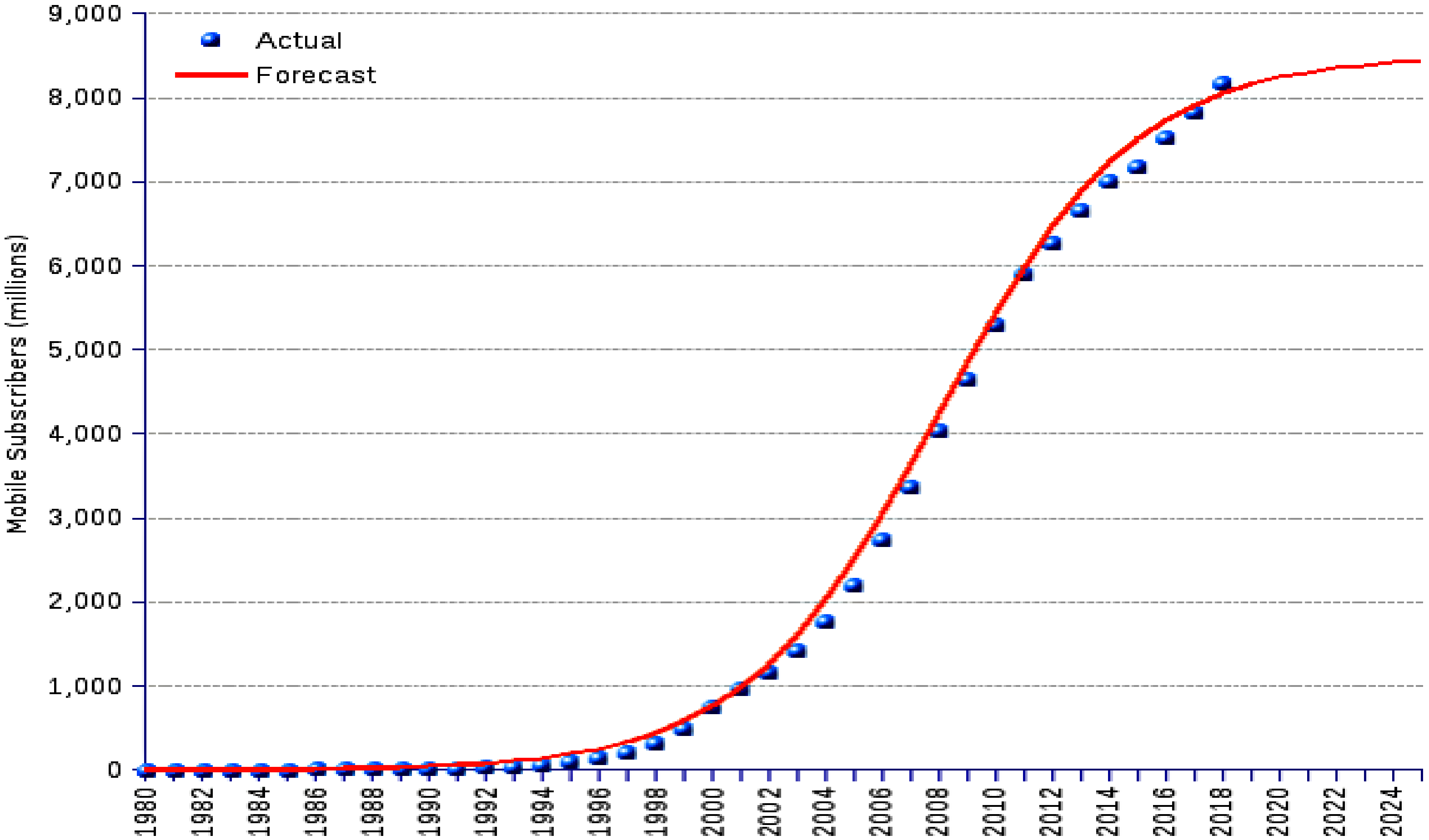
Wireless Networks in comparison with Fixed Networks

1. Higher loss-rates due to interference
    1. emissions of, e.g., engines, lightning
2. Restrictive regulations of frequencies
    1. frequencies have to be coordinated, useful frequencies are almost all occupied
3. Low transmission rates
    1. local some Mbit/s, regional currently, e.g., 53kbit/s with GSM/GPRS
4. Higher delays, higher jitter
    1. connection setup time with GSM in the second range, several hundred milliseconds for other wireless systems
5. Lower security, simpler active attacking
    1. radio interface accessible for everyone, base station can be simulated, thus attracting calls from mobile phones
6. Always shared medium
    1. secure access mechanisms important

History of Telecommunication

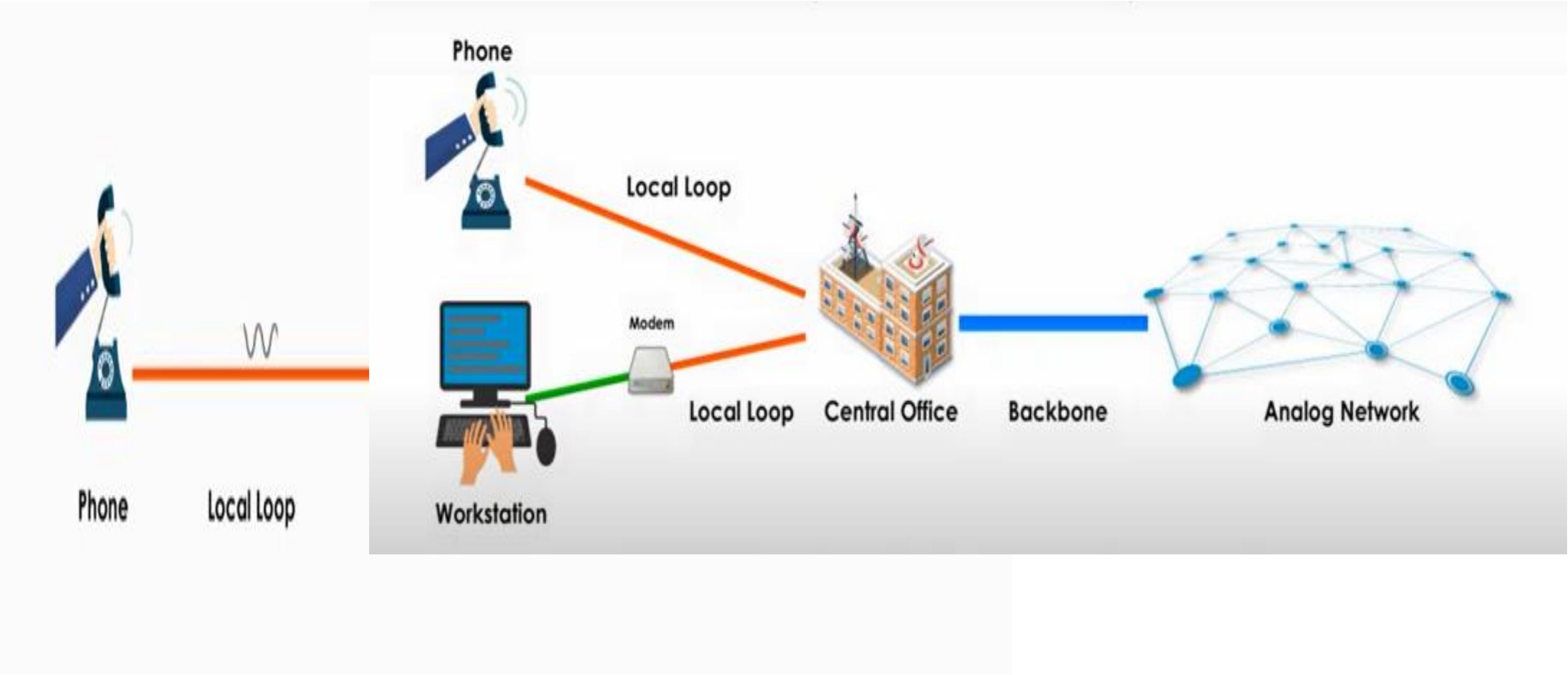


Cellular Subscribers World Wide



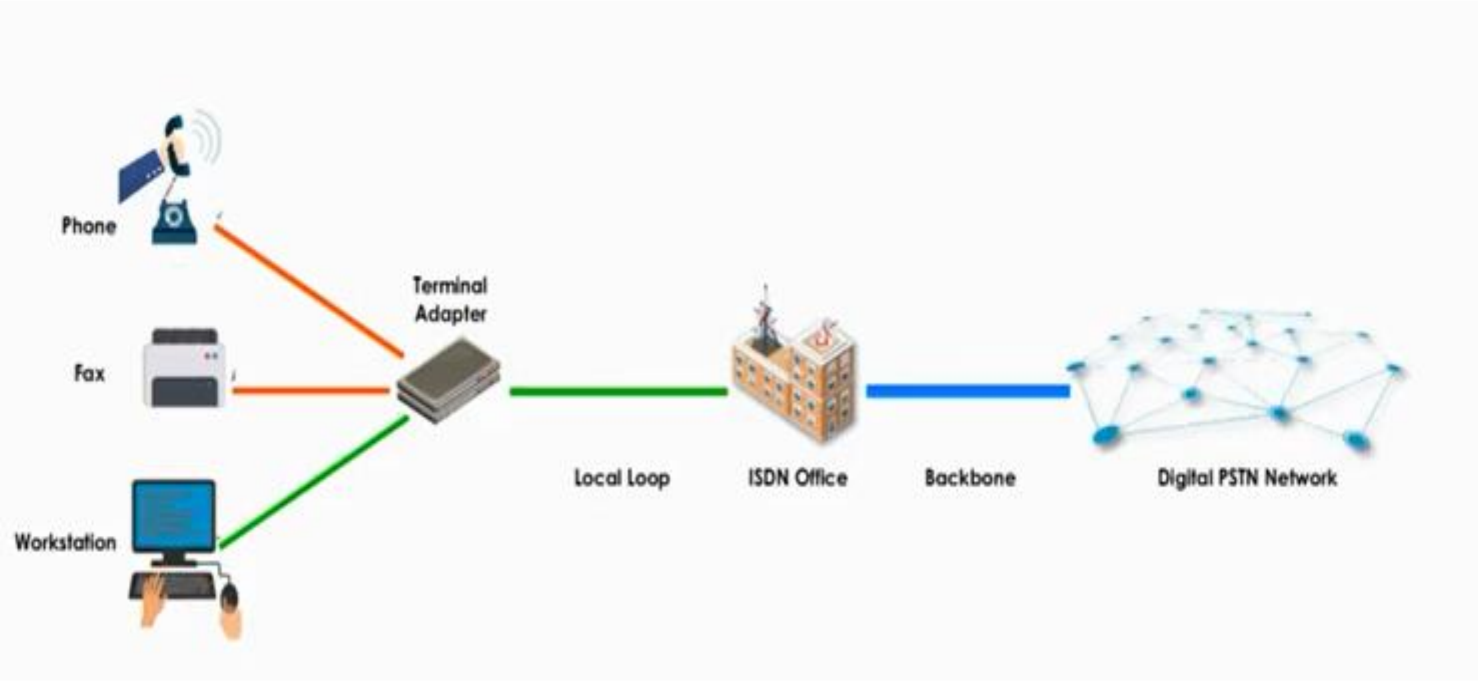
Common Services in Communication PSTN

USE of Analog Signals only



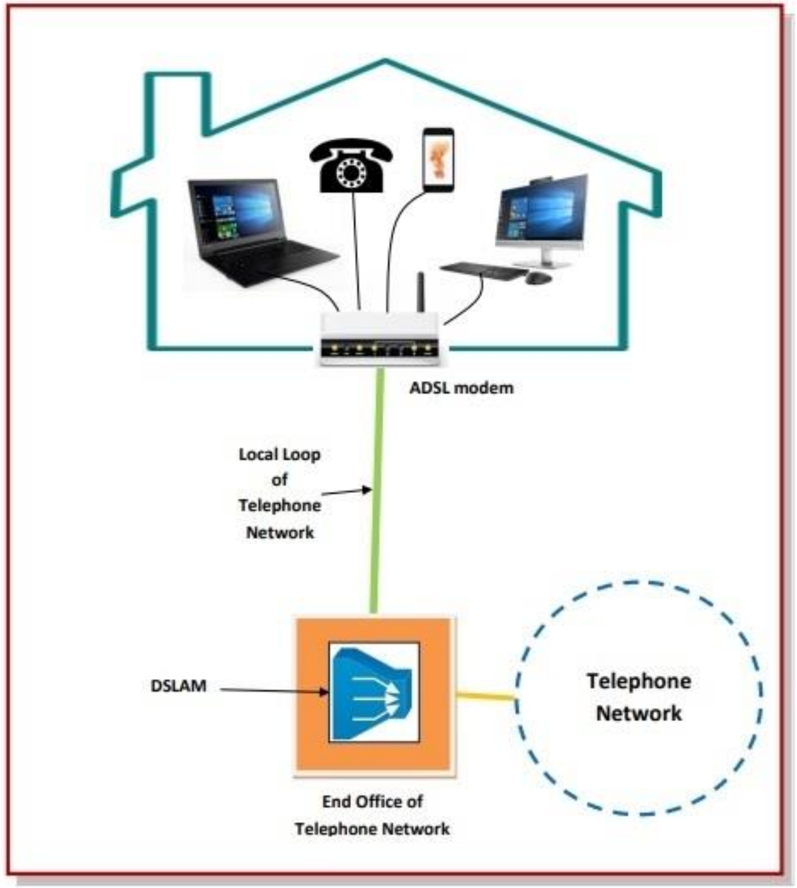
ISDN

- Digital network to transmit voice, image, video and text over circuit switched PSTN

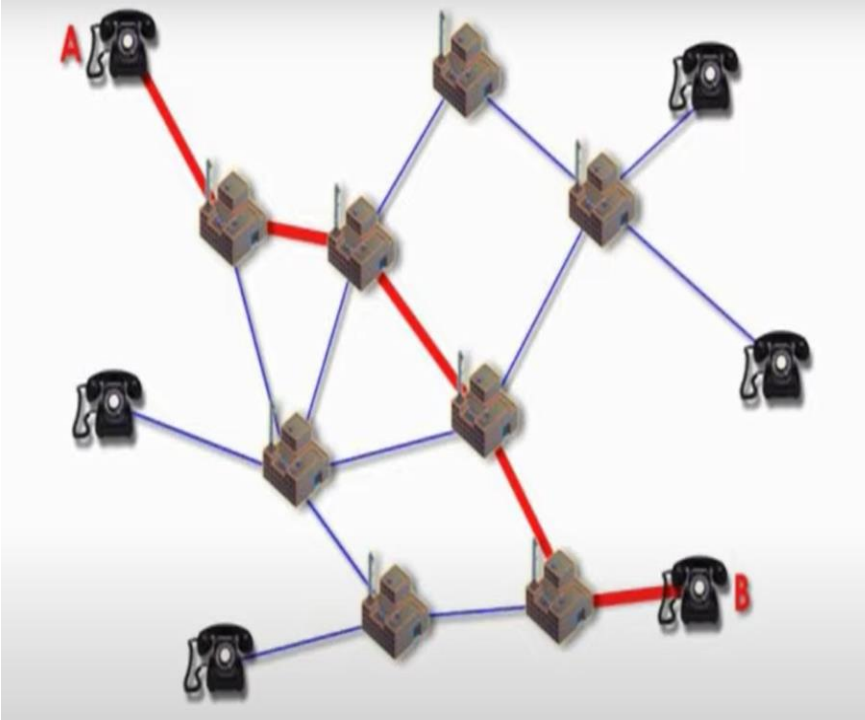


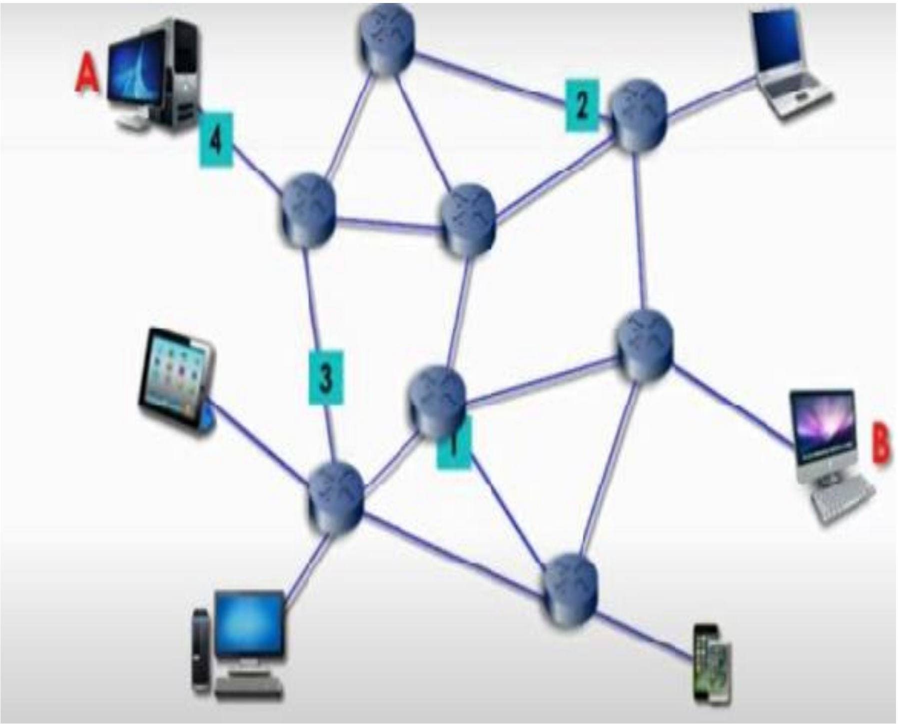
ADSL: *Asymmetric Digital Subscriber line*

- Type of Broadband internet connection.
- ADSL uses analog sinusoidal carrier waves for data transmission. The waves are modulated and demodulated at the customer premises with ADSL modems.



Circuit Switched V/S Packet switched

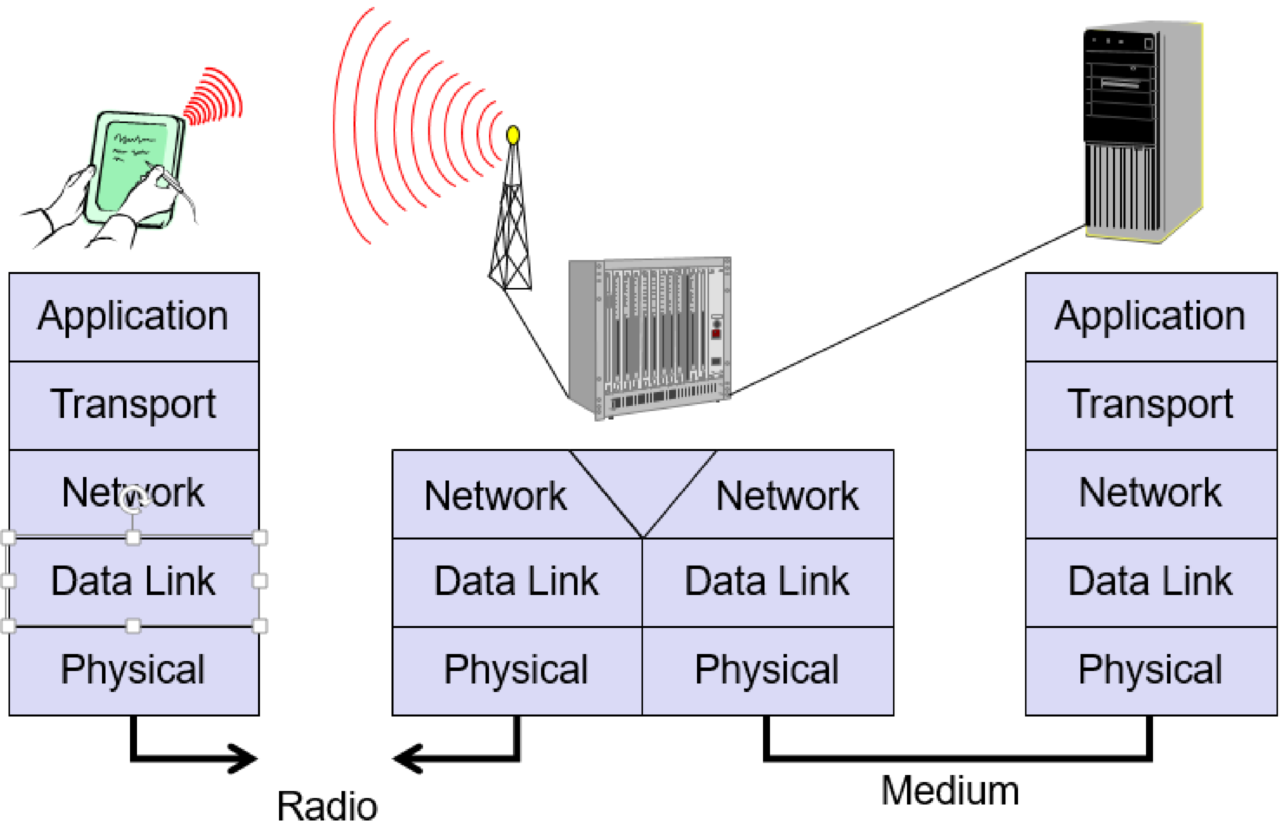




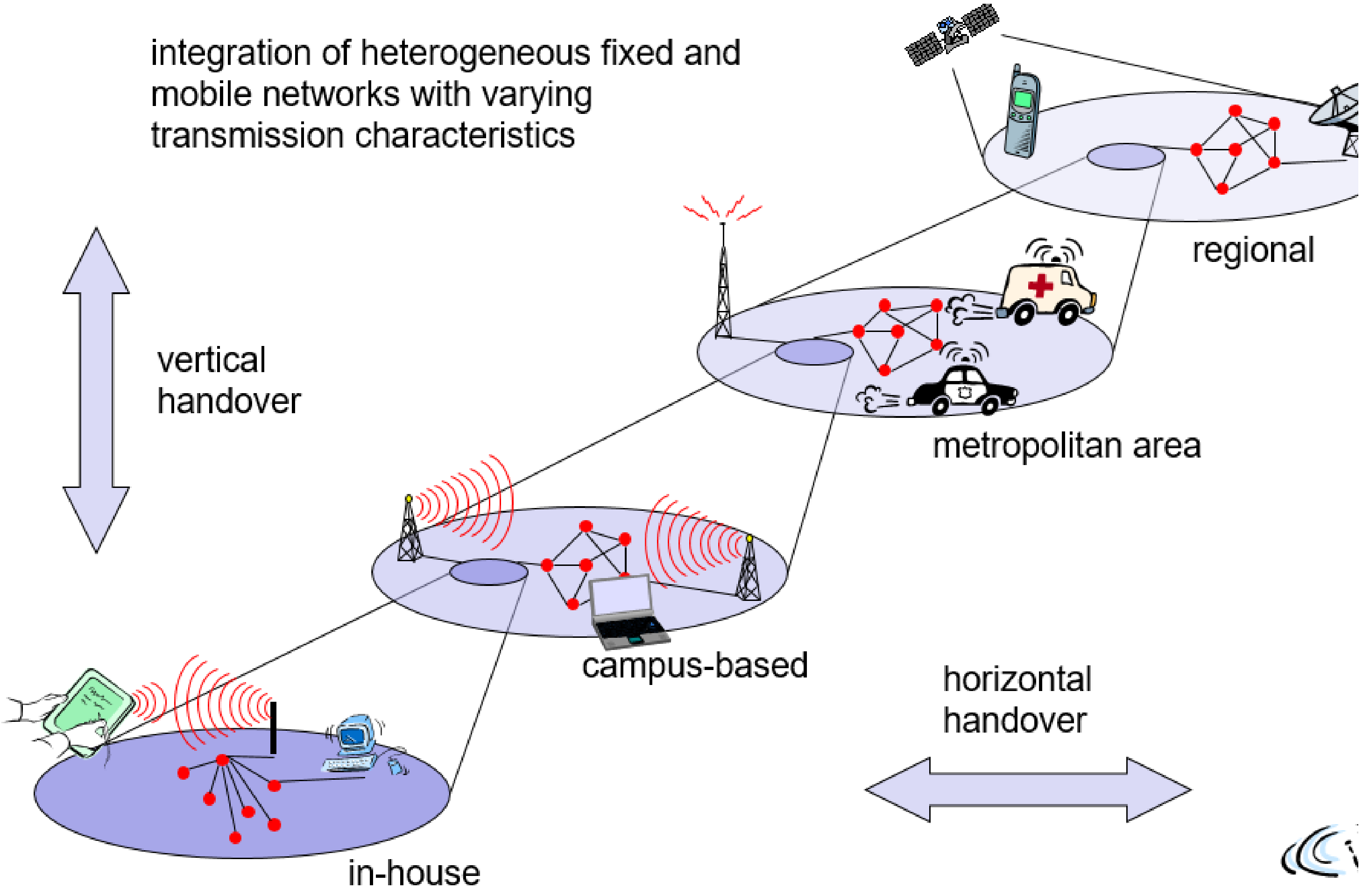
Circuit Switched Network

Packet Switched Network

Simple Reference Model



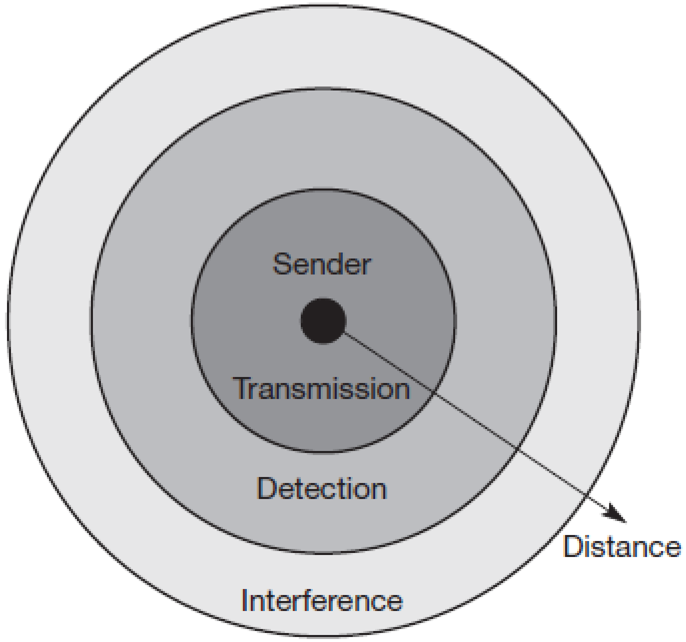
Overlay Networks: Global Goal



Radio resource management (RRM)

- **System level management of co-channel interference, Radio resources, and other radio transmission characteristics in wireless communication systems**.
- Cellular networks, wireless local area networks, wireless sensor systems, and radio broadcasting networks.

Signal Propagation



Transmission range: Within a certain radius of the sender transmission is possible, i.e., a receiver receives the signals with an error rate low enough to be able to communicate and can also act as sender.

● **Detection range**: Within a second radius, detection of the transmission is possible, i.e., the transmitted power is large enough to differ from background noise. However, the error rate is too high to

● **Interference range**: Within a third even larger radius, the sender may interfere with other transmission by adding to the background noise. A receiver will not be able to detect the signals, but the signals may disturb other signals.

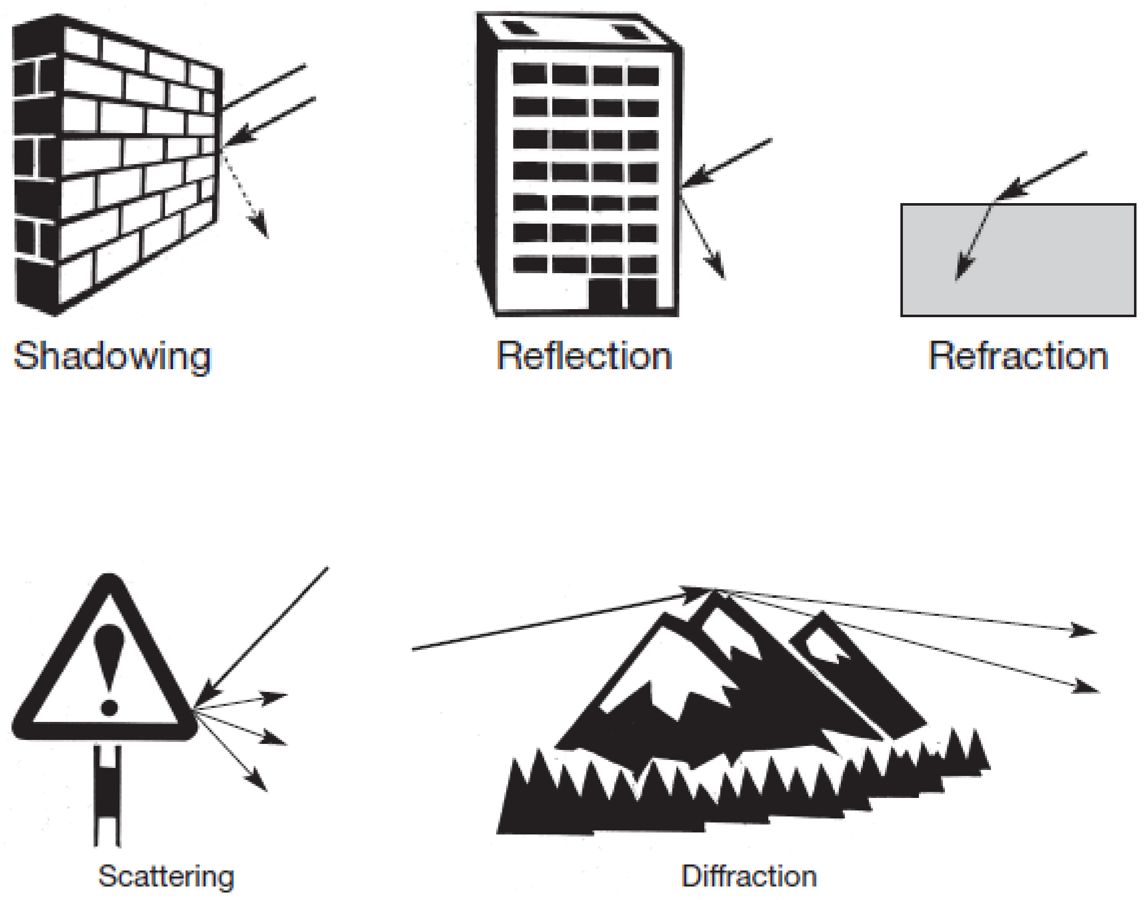
Path loss of radio signals

- In free space radio signals propagate as light.
- If such a straight line exists between a sender and a receiver it is called **line-of-sight (LOS)**.
- signal still experiences the **free space loss even in vacuum**
- Received power *Pr* is proportional to 1/*d*2 with *d* being the distance between sender and receiver. (**inverse square law**).
- radio transmission takes place through the atmosphere – signals travel through air, rain, snow, fog, dust particles, smog etc.
- While the **path loss** or **attenuation** does not cause too much trouble for short distances, the atmosphere heavily influences transmission over long distances.

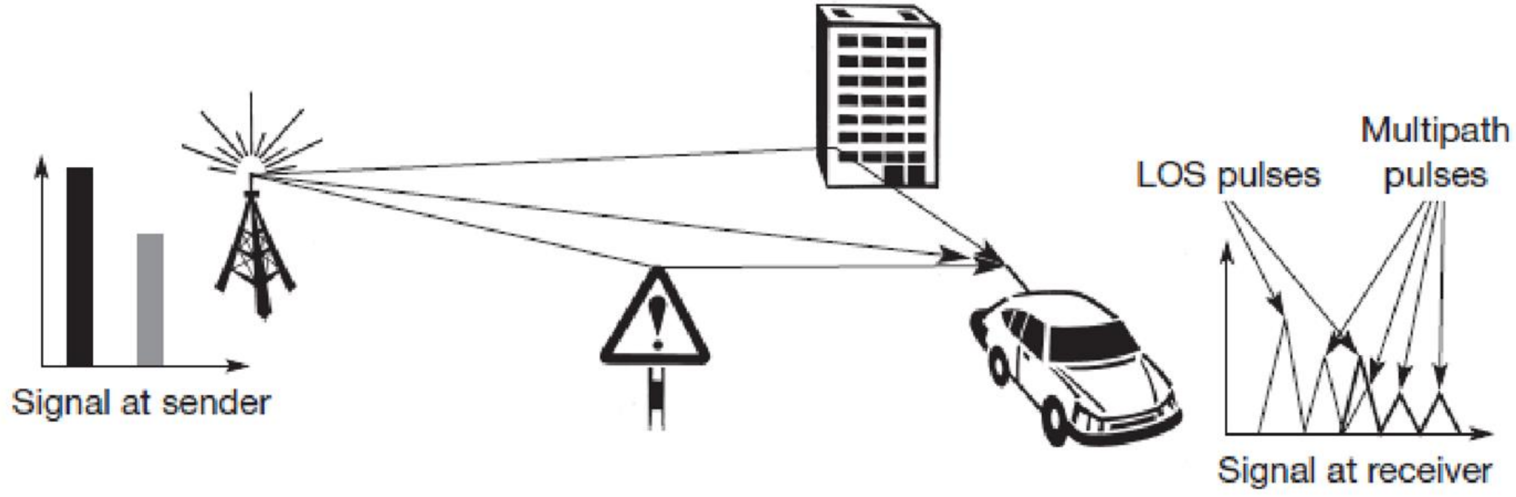
Radio Waves : Three Fundamental Propagations

Ground wave (<2 MHz): Waves with low frequencies follow the earth's surface and can propagate long distances. These waves are used for, e.g., submarine communication or AM radio.
Sky wave (2–30 MHz): Many international broadcasts and amateur radio use these short waves that are reflected2 at the ionosphere. This way the waves can bounce back and forth between the ionosphere and the earth's surface, travelling around the world.
Line-of-sight (>30 MHz): Mobile phone systems, satellite systems, cordless telephones etc. use even higher frequencies.

Effects of Signal Propagation



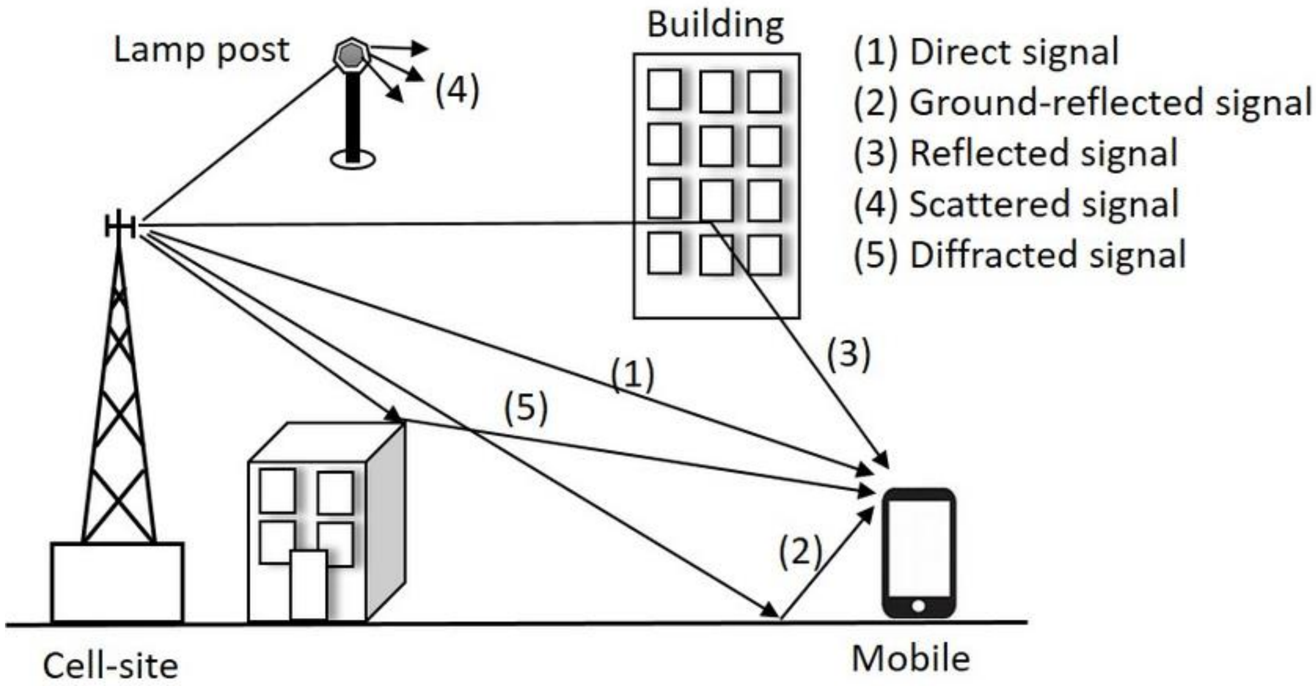
Multipath Propagation



Delay spread: the original signal is spread due to different delays of parts of the signal

Typical values for delay spread are approximately 3 μs in cities, up to 12 μs can be observed. GSM, for example, can tolerate up to 16 μs of delay spread, i.e., almost a 5 km path difference.

Multipath Propagation



Effects of Delay Spread

- Short impulse will be smeared out into a broader impulse, or rather into several weaker impulses.
- At the receiver, both impulses interfere, i.e., they overlap in time. The energy intended for one symbol now spills over to the adjacent symbol, an effect which is called **inter-symbol interference (ISI)**.
- ISI limits the bandwidth of a radio channel with multi-path propagation.

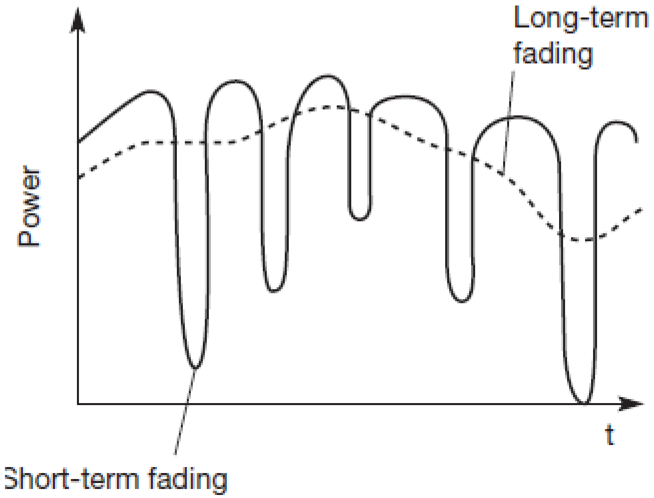
Avoid ISI:

1. Channel characteristics should be known.
2. Sender may first transmit a **training sequence** known by the receiver. The receiver then compares the received signal to the original training sequence.
3. Programs an **equalizer** that compensates for the distortion.

Effects of Signal Propagation

- ISI and delay spread already occur in the case of fixed radio transmitters and receivers, the situation is even worse if receivers, or senders, or both, move.
- Fading
  1. The power of the received signal changes considerably over time. These quick changes in the received power are also called **short-term fading.**
  2. **Depending on the different paths the signals take, these signals may have a different phase and cancel each other.**
  3. **The receiver now has to try to constantly adapt to the varying channel characteristics, e.g., by changing the parameters of the equalizer.**
  4. **If receiver is very fast, it cannot adapt fast enough and the error rate of transmission is high.**

Fading



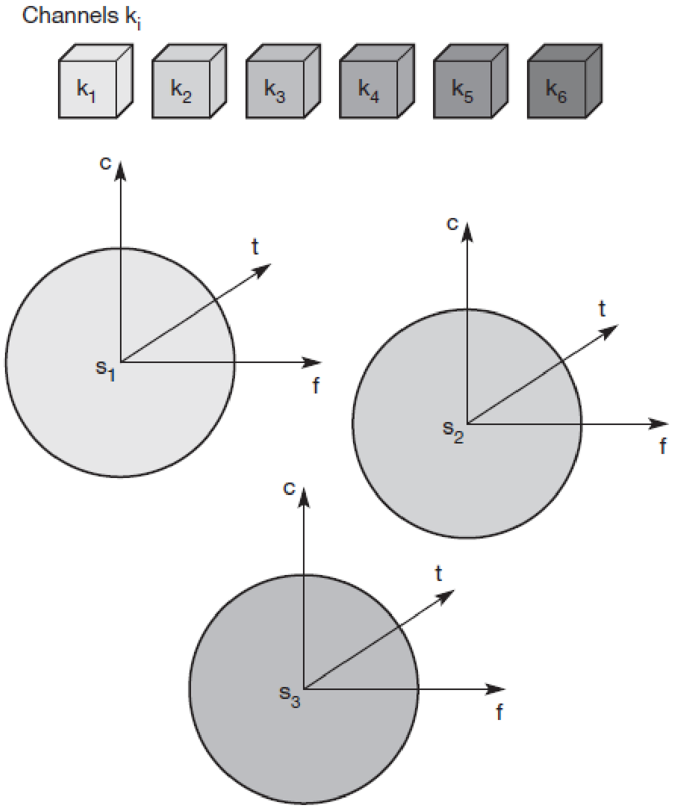
Quick changes in the received power are also called **short-term fading**.
Long-term fading, shown here as the average power over time.

Multiplexing

- In telecommunications and computer networks
    - Multiplexing is a method by which multiple analog or digital signals are combined into one signal over a shared medium.
- Multiplexing describes how several users can share a medium with minimum or no interference.
- Multiplexing can be carried out in four dimensions:

  space, **time**, **frequency**, and **code**

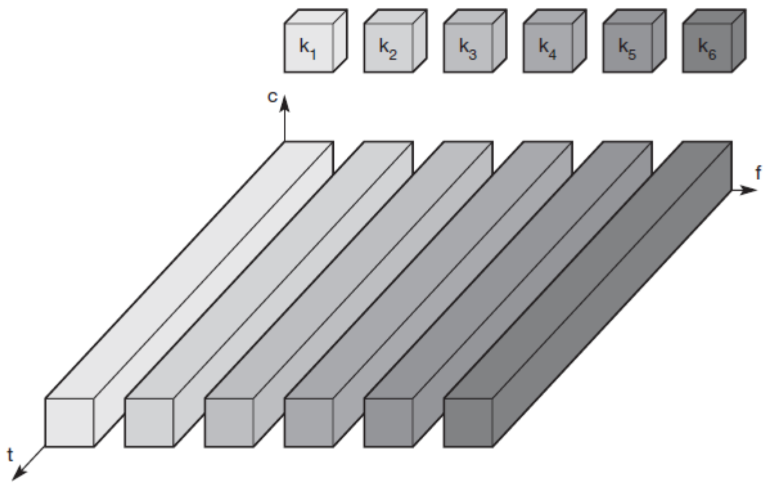
SDM : Space Division Multiplexing



- Space is represented via circles indicating the interference range.
- The space between the interference ranges is called **guard space**.
- In wireless transmission, SDM implies a separate sender for each communication channel with a wide enough distance between senders.
- Waste of space, principle used by the old analog telephone system.

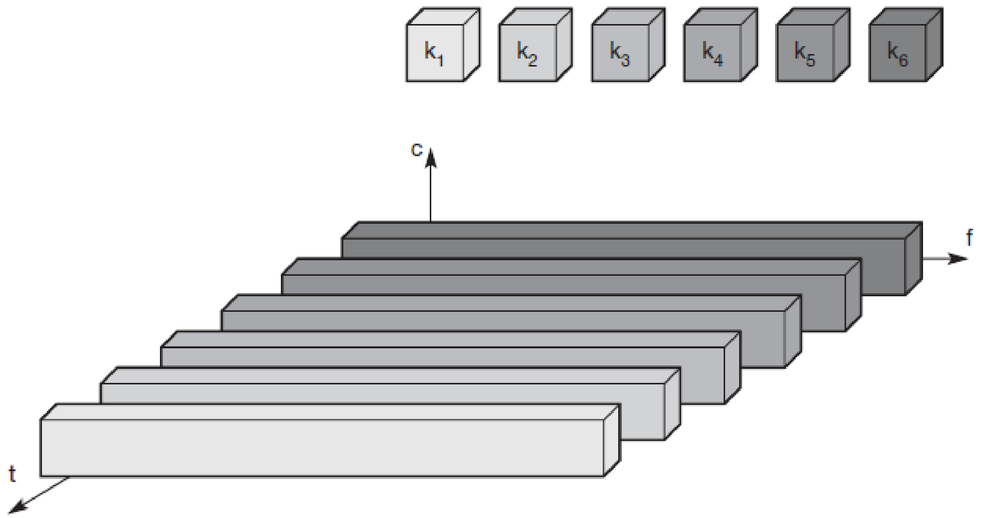
Frequency Division Multiplexing

1. **Frequency division multiplexing (FDM)** describes schemes to subdivide the frequency dimension into several non-overlapping frequency bands.
2. **Guard spaces** are needed to avoid frequency band overlapping (also called **adjacent channel interference**).
3. Scheme is used for radio stations within the same region, where each radio station has its own frequency.
4. Radio stations broadcast 24 hours a day, mobile communication typically takes place for only a few minutes at a time.
5. Assigning a separate frequency for each possible communication scenario would be a tremendous waste of (scarce) frequency resources.

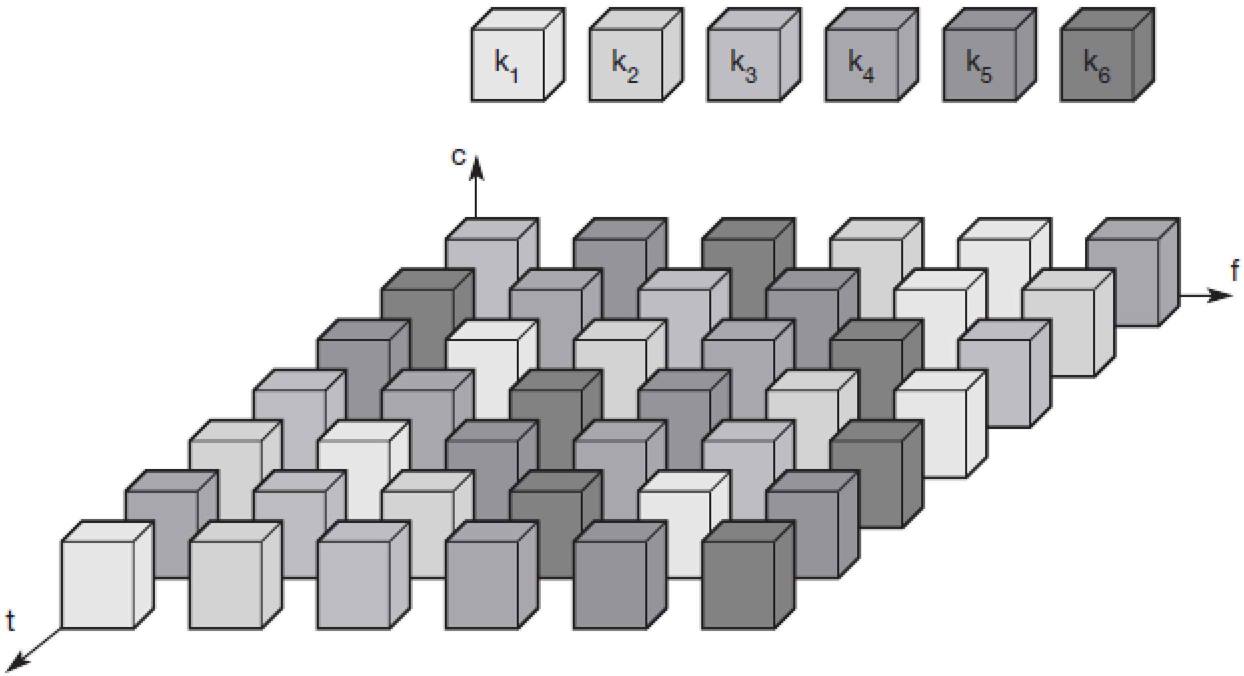


Time Division Multiplexing

1. Flexible multiplexing scheme for typical mobile communications is **time division multiplexing (TDM)**.
2. Channel ki is given the whole bandwidth for a certain amount of time, i.e., all senders use the same frequency but at different points in time.
3. Guard spaces, represent time gaps.
4. If two transmissions overlap in time, this is called co-channel interference.

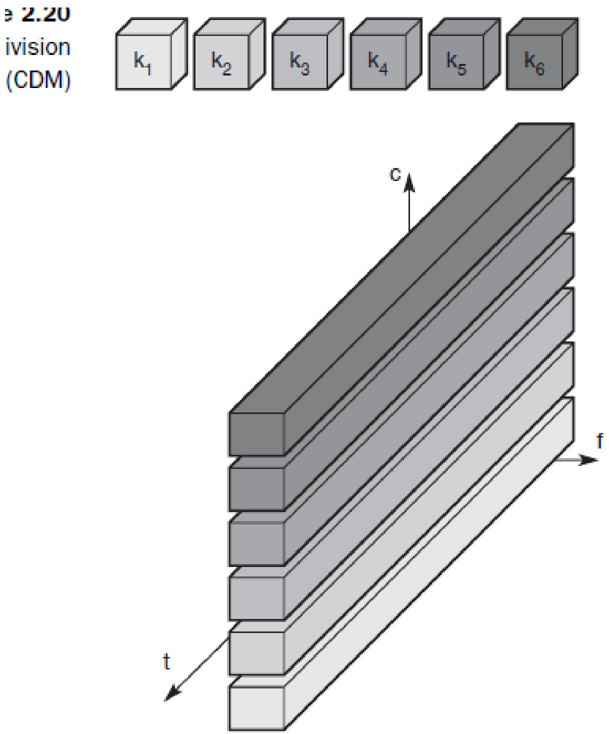


Time and Frequency Division Multiplexing (Used by GSM)



Code division multiplexing (CDM)

- Separation is now achieved by assigning each channel its own ‘code’, **guard spaces** are realized by using codes with the necessary ‘distance’ in code space, e.g., **orthogonal codes**.
- CDM for wireless transmission is that it gives good protection against interference and tapping.
- Receiver is highly complex.



Modulation Techniques

- $g(t) = A_t \cos(2\pi f_t t + \varphi_t)$ Signal Representation

  amplitude A_t, frequency f_t, and phase φ_t which may be varied in accordance with data or another modulating signal.
- **Digital modulation :** digital data (0 and 1) is translated into an analog signal (baseband signal). Required if digital data has to be transmitted over a medium that only allows for analog transmission.
- In wireless networks, digital transmission cannot be used.
- The binary bit-stream has to be translated into an analog signal first.
- Schemes used for this translation are:
  1. **amplitude shift keying (ASK)**
  2. **frequency shift keying (FSK)**
  3. **phase shift keying (PSK)**.
- digital modulation translates a 1 Mbit/s bit-stream into a baseband signal with a bandwidth of 1 MHz.
- In wireless transmission, an **analog modulation** that shifts the center frequency of the baseband signal generated by the digital modulation up to the radio carrier is needed

Brain Storming

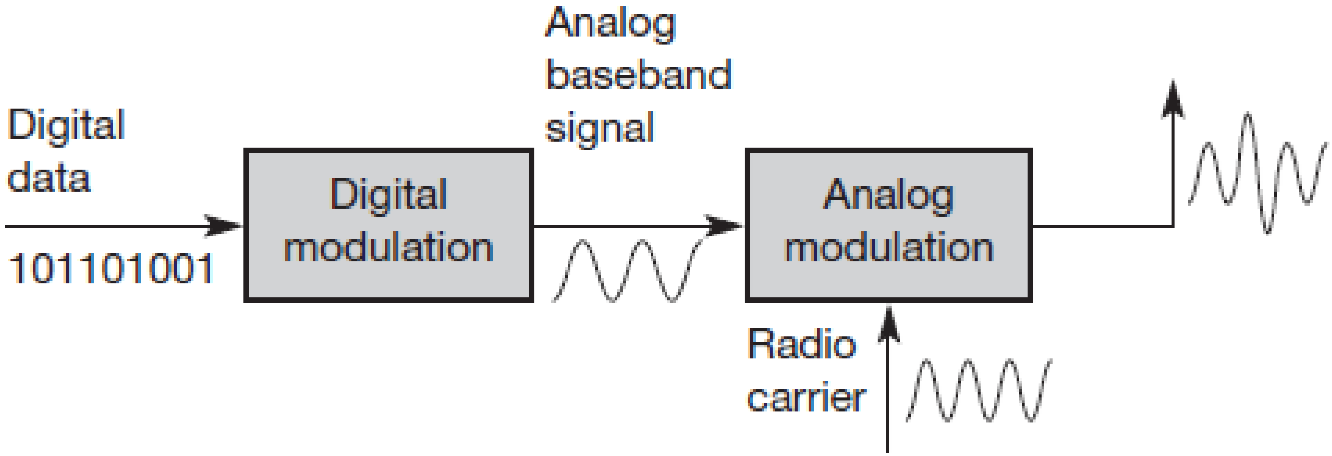
why
this baseband signal cannot be directly transmitted in a wireless system?

Reasons

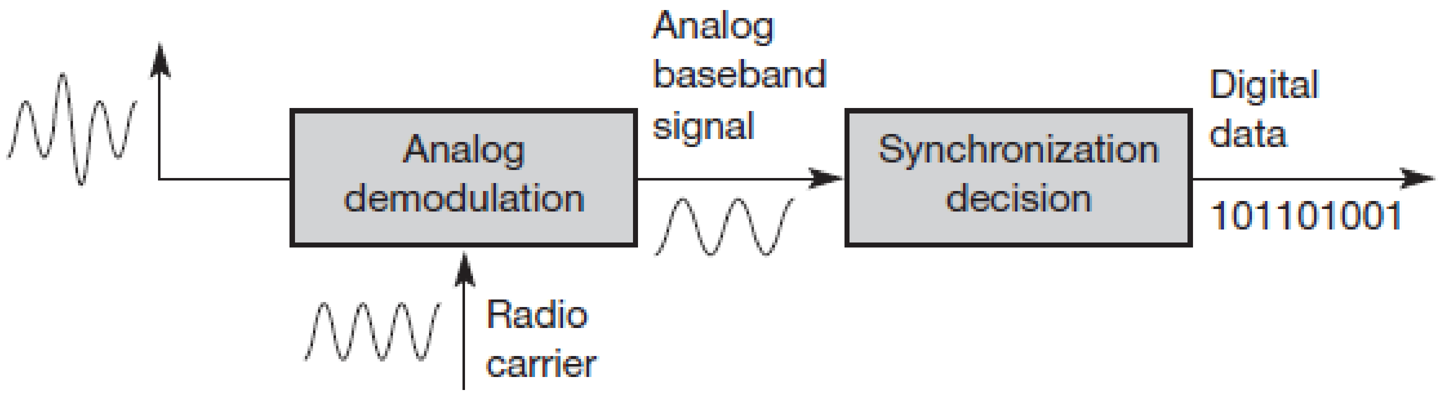
- **Antennas**: An antenna must be the order of magnitude of the signal’s wavelength in size to be effective. For the 1 MHz signal in the example this would result in an antenna some hundred meters high.
- **Frequency division multiplexing**: Using only baseband transmission, FDM could not be applied. Analog modulation shifts the baseband signals to different carrier frequencies. The higher the carrier frequency, the more bandwidth that is available for many baseband signals.
- **Medium characteristics**: Path-loss, penetration of obstacles, reflection, scattering, and diffraction –depend heavily on the wavelength of the signal.

Depending on the application, the right carrier frequency with the desired characteristics has to be chosen.

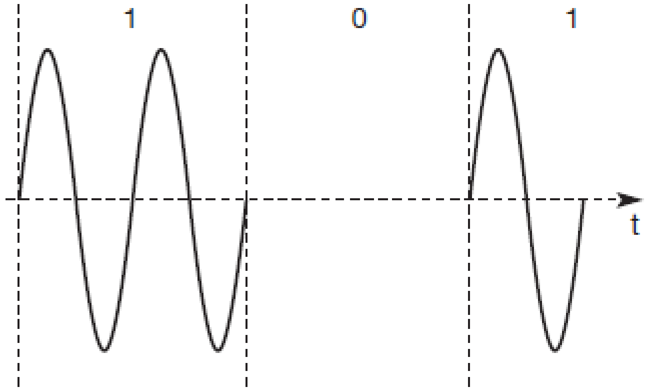
Modulation : Radio Transmitter for digital Data



Demodulation and data reconstruction in a receiver

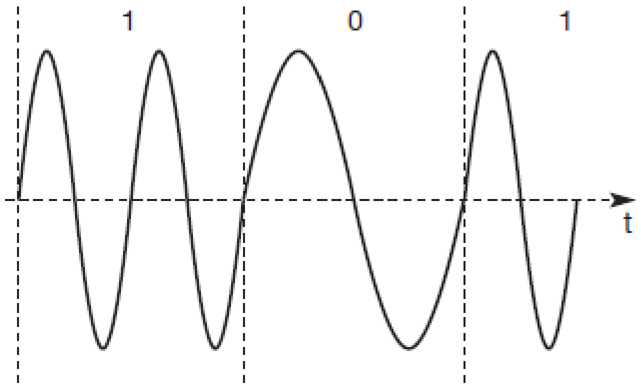


Amplitude shift keying (ASK), the most simple digital modulation scheme.



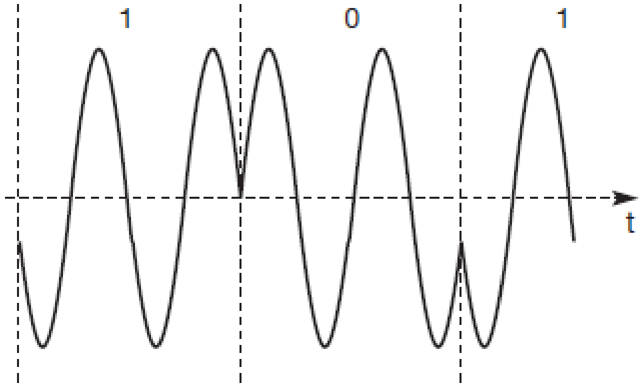
- The two binary values, 1 and 0, are represented by two different amplitudes.
- This simple scheme only requires low bandwidth, but is very susceptible to interference.
- Effects like multi-path propagation, noise, or path loss heavily influence the amplitude.

Binary FSK
(BFSK)



- One frequency f1 to the binary 1 and another frequency f2 to the binary 0.
- To implement FSK is to switch between two oscillators, one with the frequency f1 and the other with f2, depending on the input.

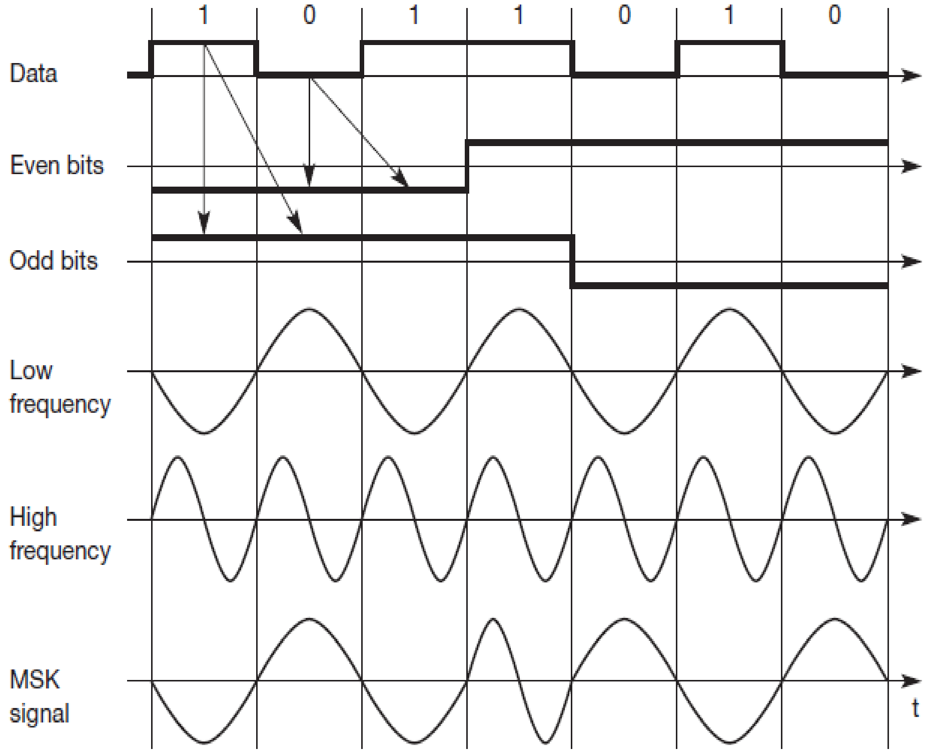
Phase shift keying (PSK)



- Phase shift of 180° or π as the 0 follows the 1.
- Shifting the phase by 180° each time the value of data changes, is also called **binary PSK (BPSK).**
- To receive the signal correctly, the receiver must synchronize in frequency and phase with the transmitter. This can be done using a **phase lock loop (PLL)**.

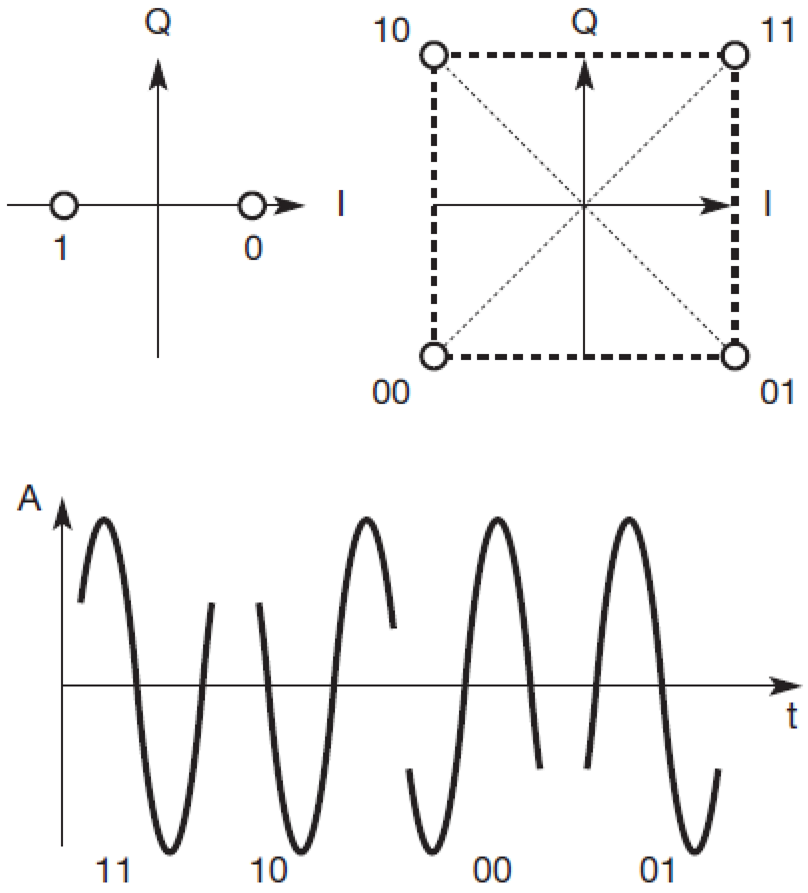
Advanced frequency shift keying

MSK is basically BFSK without abrupt phase changes.



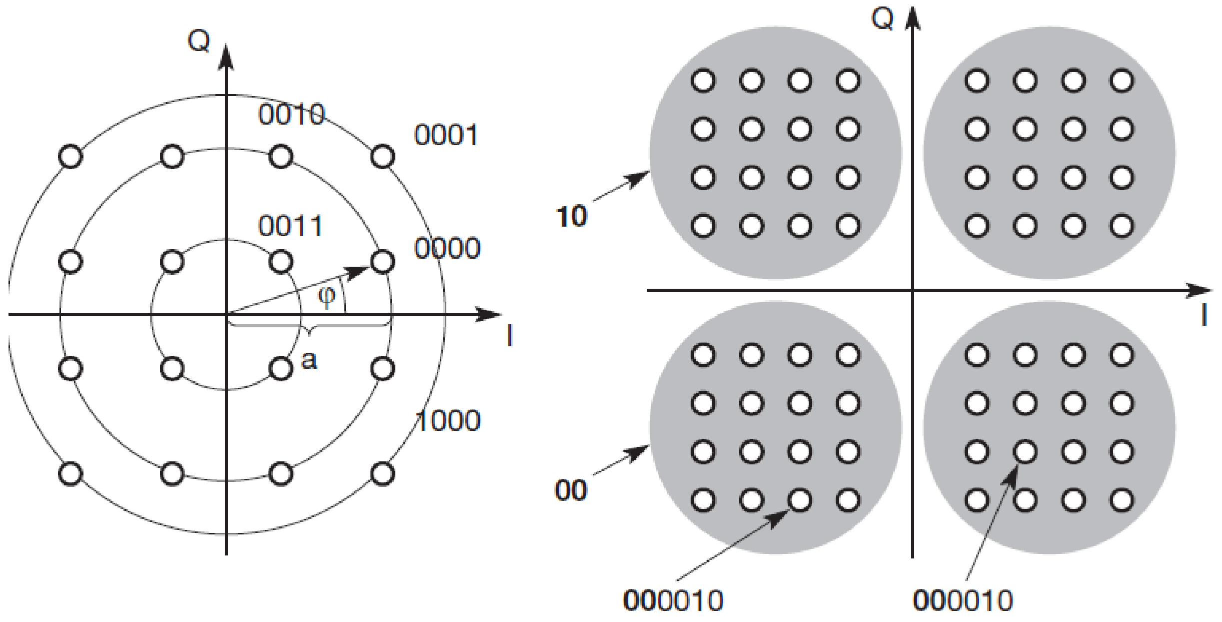
- data bits are separated into even and odd bits, the duration of each bit being doubled.
- The scheme also uses two frequencies: f1, the lower frequency, and f2, the higher frequency, with f2 = 2f1.
- if the even and the odd bit are both 0, then the higher frequency f2 is inverted (i.e., f2 is used with a phase shift of 180°);
  ● if the even bit is 1, the odd bit 0, then the lower frequency f1 is inverted.
- if the even bit is 0 and the odd bit is 1, as in columns 1 to 3, f1 is taken without changing the phase,
- if both bits are 1 then the original f2 is taken.

Advanced phase shift keying



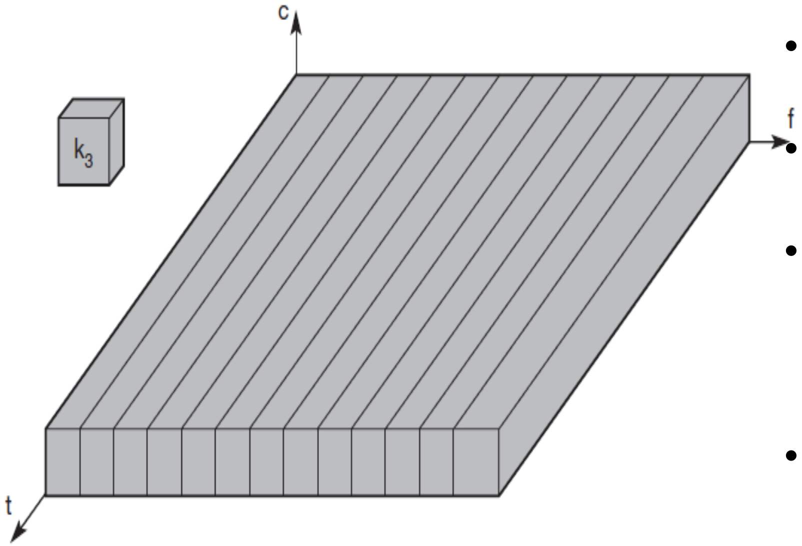
- QPSK (and other PSK schemes) can be realized in two variants.
- The phase shift can always be relative to a **reference signal** (with the same frequency).
- If this scheme is used, a phase shift of 0 means that the signal is in phase with the reference signal.
- A QPSK signal will then exhibit a phase shift of 45° for the data 11, 135° for 10, 225° for 00, and 315° for 01 – with all phase shifts being relative to the reference signal.

Quadrature amplitude modulation (QAM)

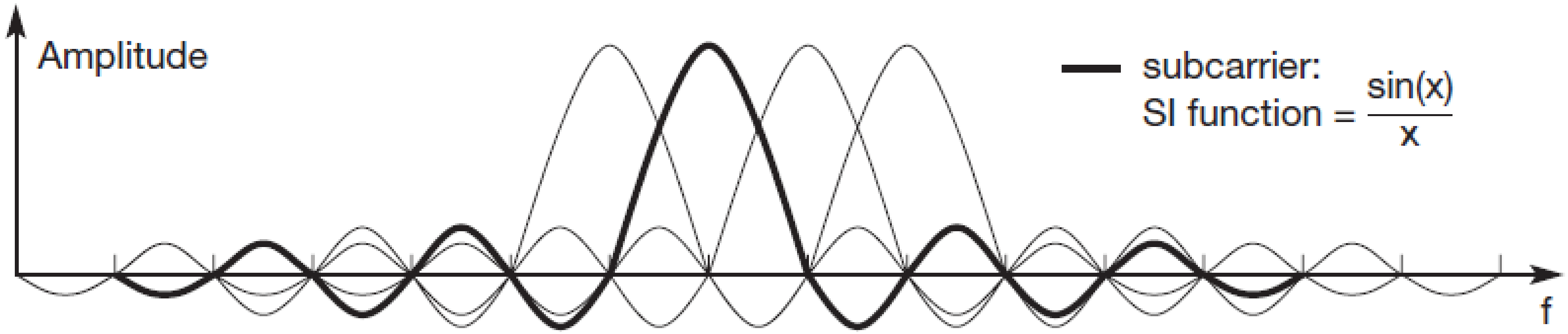


- Three different amplitudes and 12 angles are combined coding 4 bits per phase/amplitude change.
- The more ‘points’ used in the phase domain, the harder it is to separate them.

Multi-carrier modulation



- MCM has good ISI mitigation property.
- Higher bit rates are more vulnerable to ISI.
- MCM splits the high bit rate stream into many lower bit rate streams.
- Each stream is sent using an independent carrier frequency.
- If, for example, n symbols/s have to be transmitted, each subcarrier transmits n/c symbols/s with c being the number of subcarriers.
- One symbol could, for example represent 2 bit as in QPSK

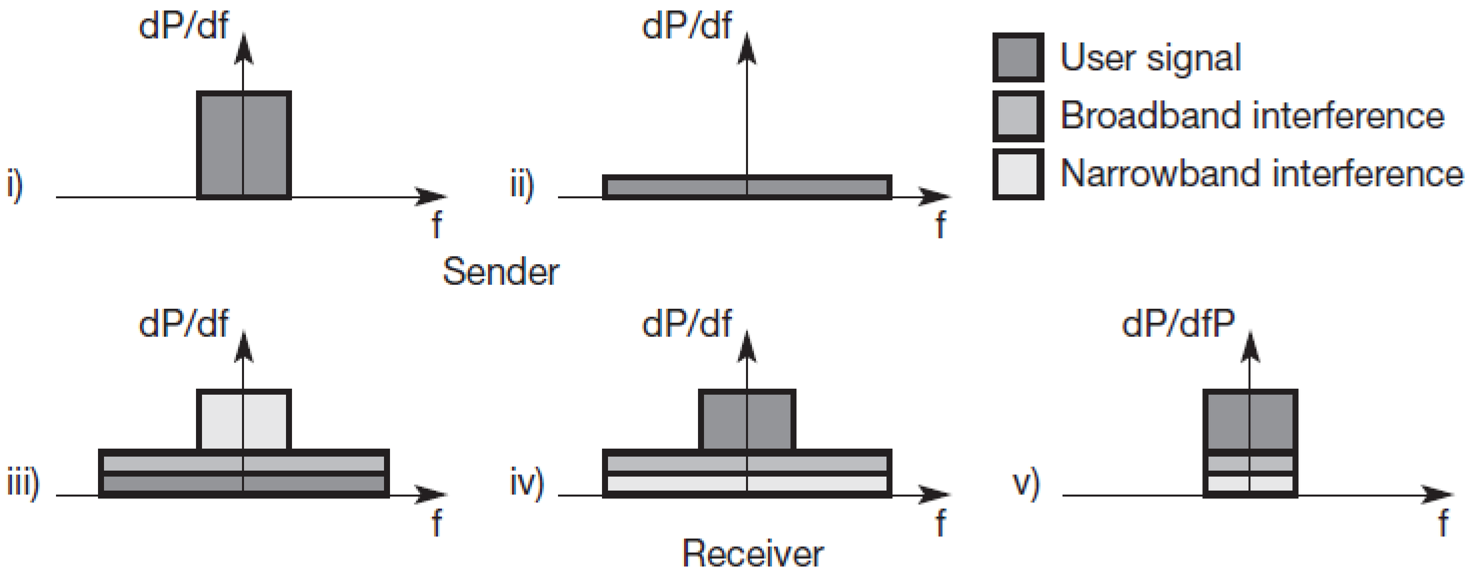


Spread Spectrum

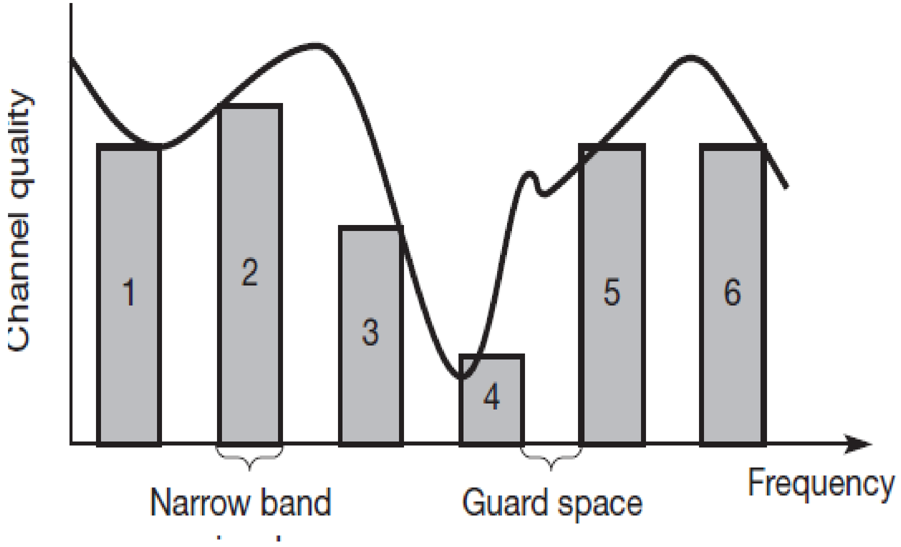
Spread spectrum techniques involve spreading the bandwidth needed to transmit data.

Advantages:

1. Resistance to **narrowband interference.**

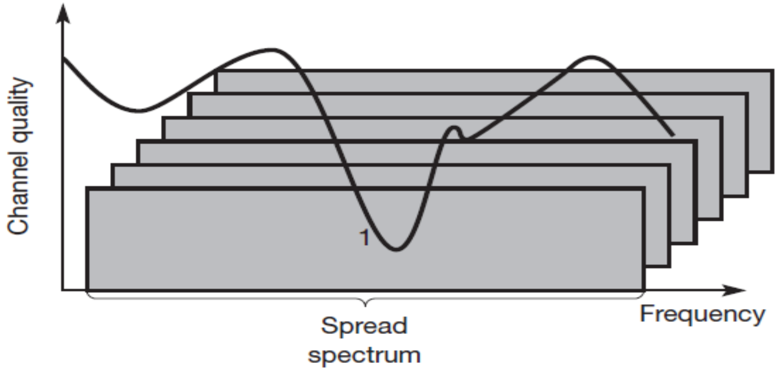


Narrow Band Interference without spread spectrum



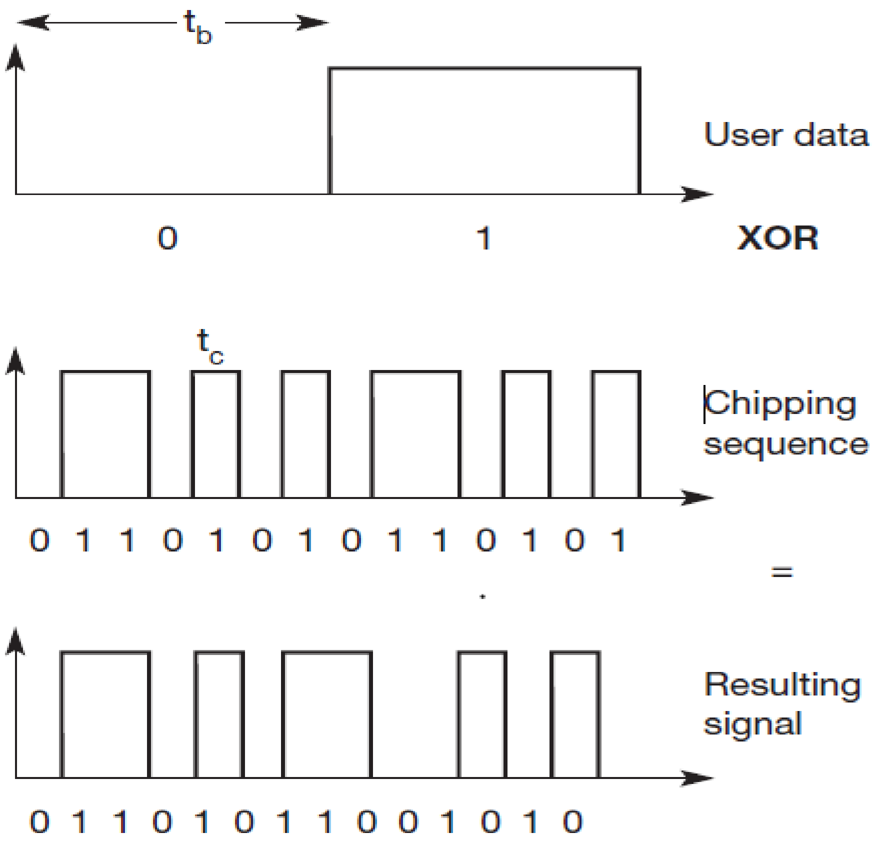
- Six different channels use FDM for multiplexing, each channel has its own narrow frequency band for transmission.
- Between each frequency band a guard space is needed to avoid adjacent channel interference.
- Channel quality also changes over time – the diagram only shows a snapshot at one moment.
- Narrowband interference destroys the transmission of channels 3 and 4.

Spread Spectrum to avoid Narrow Band Interference



- All narrowband signals are now spread into broadband signals using the same frequency range.
- Application shows the tight coupling of CDM and spread spectrum to recover signal at the receiver.
- One disadvantage is the increased complexity of receivers that have to despread a signal.
- Another problem is ,Large frequency band is needed due to the spreading of the signal.

Spreading the spectrum can be achieved in two different ways

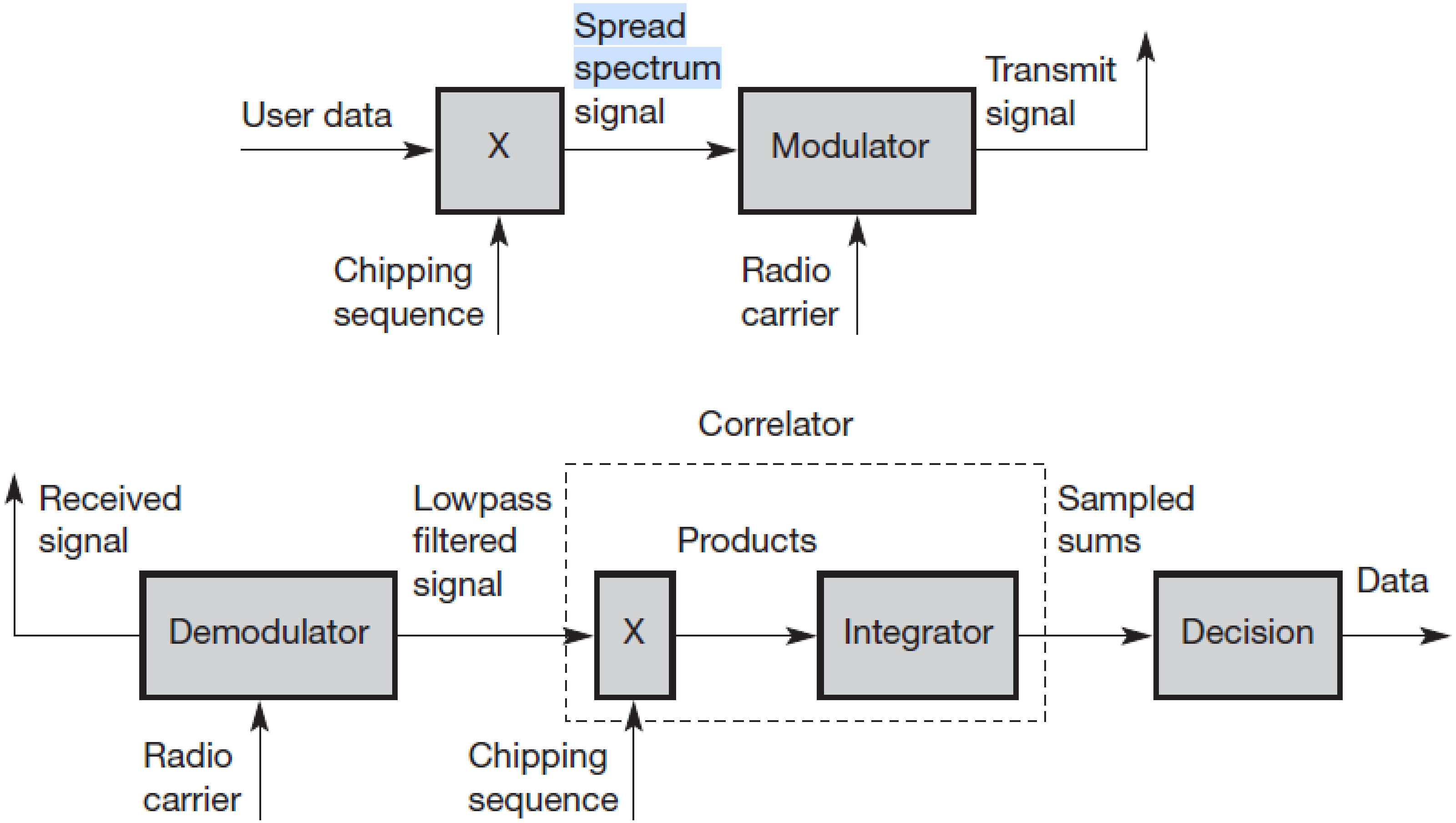


Direct sequence spread spectrum (DSSS): System take a user bit stream and perform an (XOR) with a so-called **chipping sequence.**

DSSS

- Result is either the sequence 0110101 (if the user bit equals 0) or its complement 1001010 (if the user bit equals 1).
- While each user bit has a duration tb, the chipping sequence consists of smaller pulses, called **chips**, with a duration tc.
- If the chipping sequence is generated properly it appears as random noise: this sequence is also sometimes called **pseudo-noise** sequence. The **spreading factor** s = tb/tc determines the bandwidth of the resulting signal.
- If the original signal needs a bandwidth w, the resulting signal needs s·w after spreading.

DSSS Transmitter and Receiver



Challenges in DSSS

- Receiver has to know the chipping sequence.
- Sequences at the sender and receiver have to be precisely synchronized because the receiver calculates the product of a chip with the incoming signal.
- Chip Sequence:

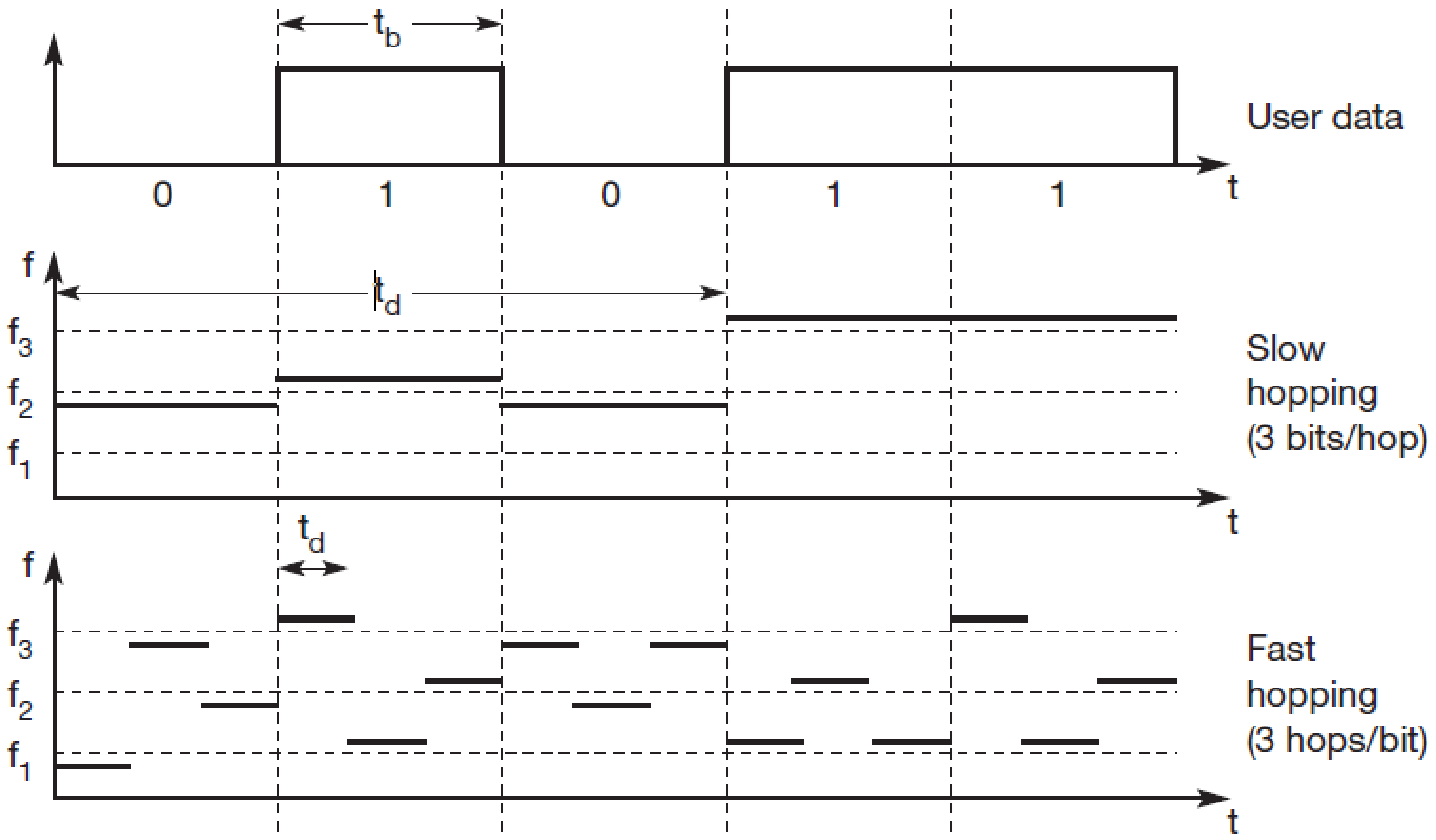
Sending the user data 01 and applying the 11-chip Barker code 10110111000 results in the spread ‘signal’ 0110111000010010001111.

There are several paths and signals due to multi path propagation, so there is need of rake receiver.

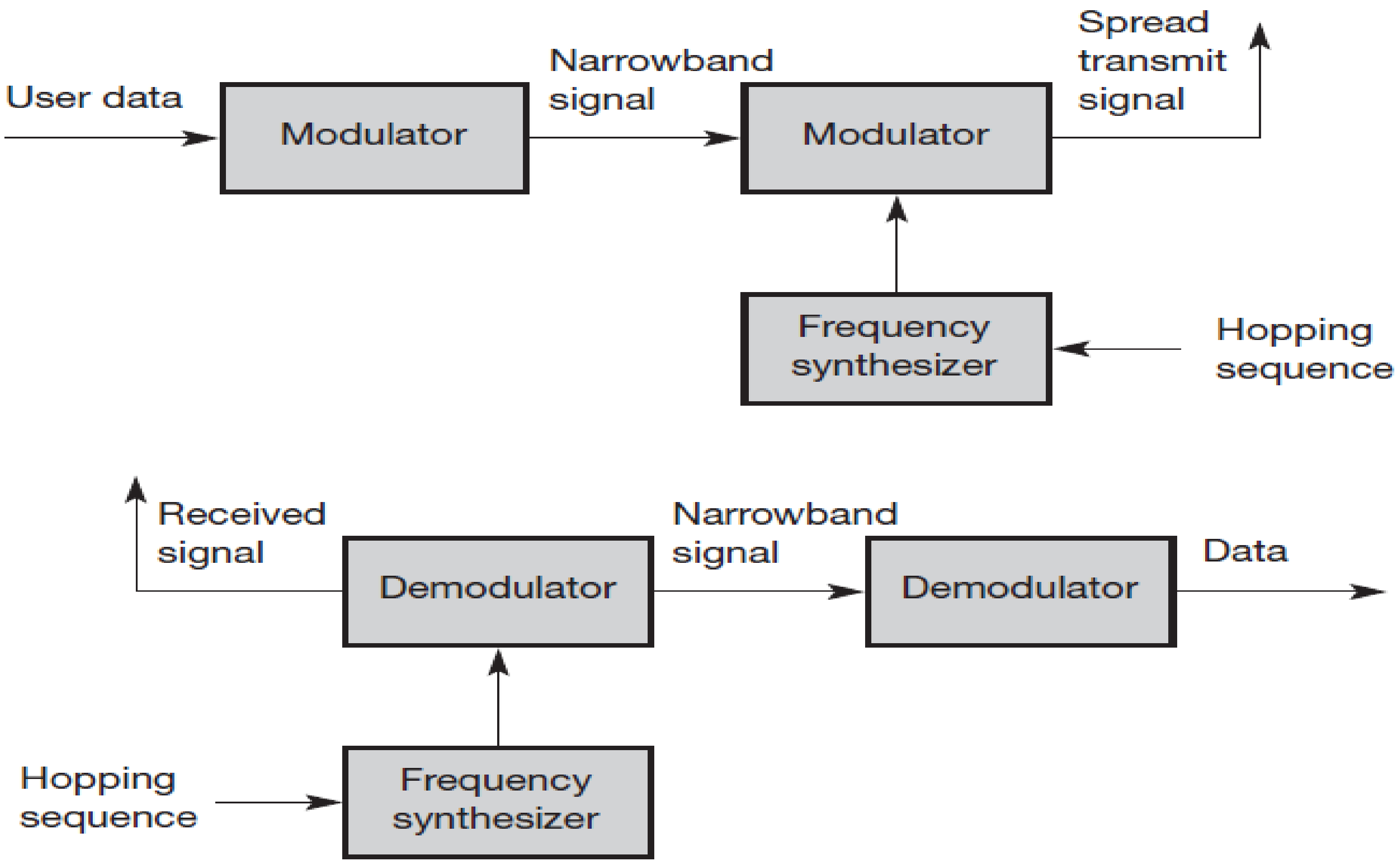
Frequency hopping spread spectrum (FHSS)

- Total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels.
- Transmitter and receiver stay on one of these channels for a certain time and then hop to another channel.
- The pattern of channel usage is called the **hopping sequence**, the time spend on a channel with a certain frequency is called the **dwell time**.

FHSS: Slow and Fast



FHSS: Transmitter & Receiver

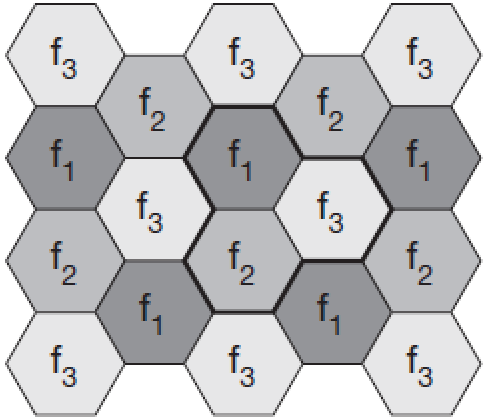


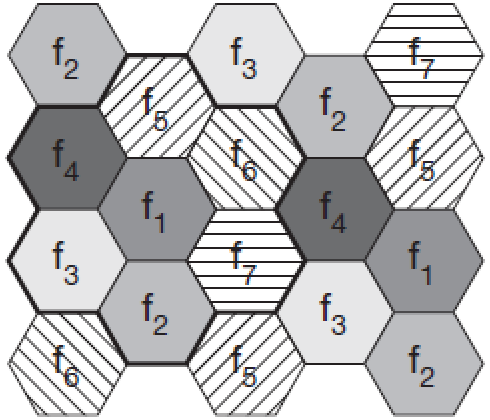
DSSS V/s FHSS

- FHSS systems only use a portion of the total band at any time, while DSSS systems always use the total bandwidth available.
- DSSS systems are more resistant to fading and multi-path effects.
- DSSS signals are much harder to detect – without knowing the spreading code, detection is virtually impossible.
- If each sender has its own pseudo-random number sequence for spreading the signal (DSSS or FHSS), the system implements CDM.

Cellular Systems – Frequency Reuse

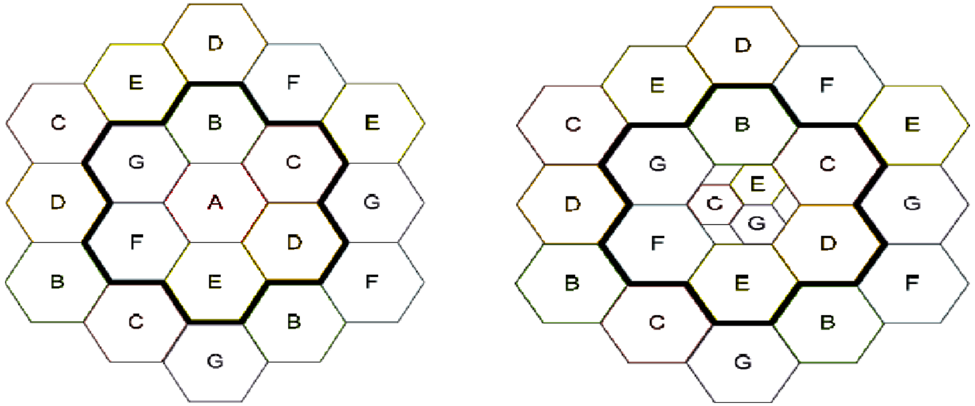
- Cellular systems for mobile communications implement SDM.
- Each transmitter, called a **base station**, covers a certain area, a **cell**.
- In Mobile telecommunication systems, a mobile station within the cell around a base station communicates with this base station and vice versa.





Cell Splitting

- Cell splitting is **the process of subdividing a congested cell into smaller cells, each with its own base station and a corresponding reduction in antenna height and transmitter power**.
- Cell splitting increases the capacity of a cellular system since it increases the number of times that channels are reused.



(a) Original cell distribution (b) After splitting cell A

Figure 1.5: Example of cell splitting

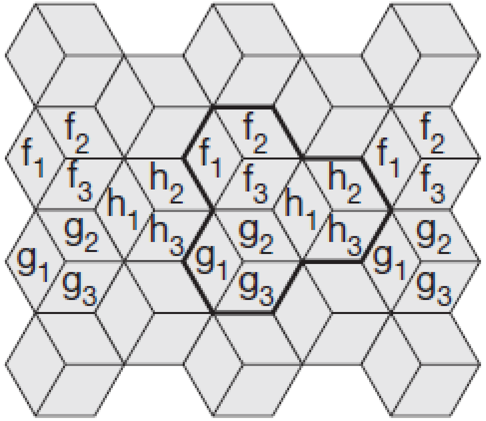
Advantages of Small Cells

- **Higher capacity**: Implementing SDM allows frequency reuse. As most mobile phone systems assign frequencies to certain users (or certain hopping patterns), this frequency is blocked for other users. But frequencies are a scarce resource and, the number of concurrent users per cell is very limited. **Huge cells do not allow for more users.**
- **Less transmission power**: A receiver far away from a base station would need much more transmit power than the current few Watts.
- **Local interference only**: With small cells, mobile stations and base stations only have to deal with 'local' interference.
- **Robustness**: Cellular systems are decentralized and so, more robust against the failure of single components.

Disadvantages of Small Cells

- **Infrastructure needed**: Cellular systems need a complex infrastructure to connect all base stations.
- **Handover needed**: The mobile station has to perform a handover when changing from one cell to another. Depending on the cell size and the speed of movement, this can happen quite often.
- **Frequency planning**: To avoid interference between transmitters using the same frequencies, frequencies have to be distributed carefully.

Channel Allocation-Cellular System with 3 Cell Cluster



- Fixed Channel Allocation
- Dynamic Channel Allocation
- Borrowing Channel Allocation

All cells within a cluster use disjointed sets of frequencies. One cell in the cluster uses set f_1, another cell f_2, and the third cell f_3.

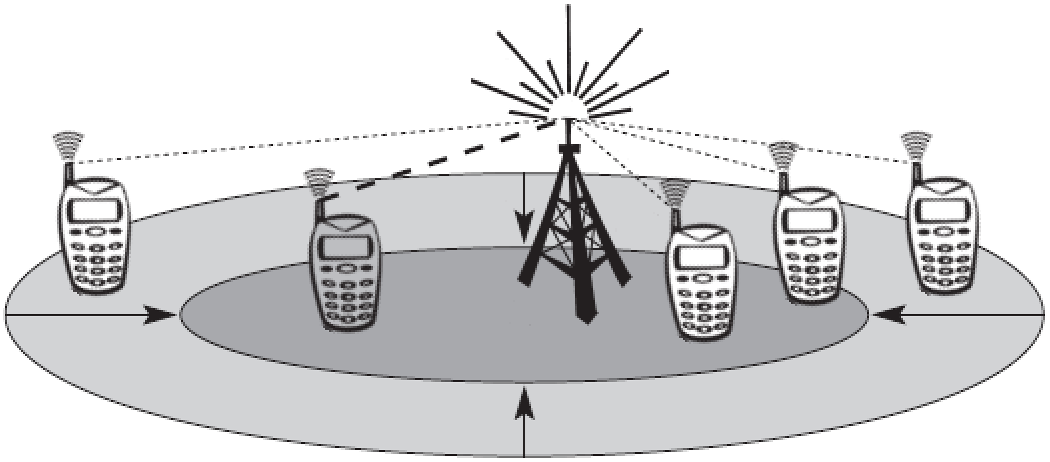
Cellular systems using CDM

Users are separated through the code they use, not through the frequency.

Cell size depends on the current load.

CDM cells are commonly said to '**breathe**'.

Cell can cover a larger area under a light load, it shrinks if the load increases.

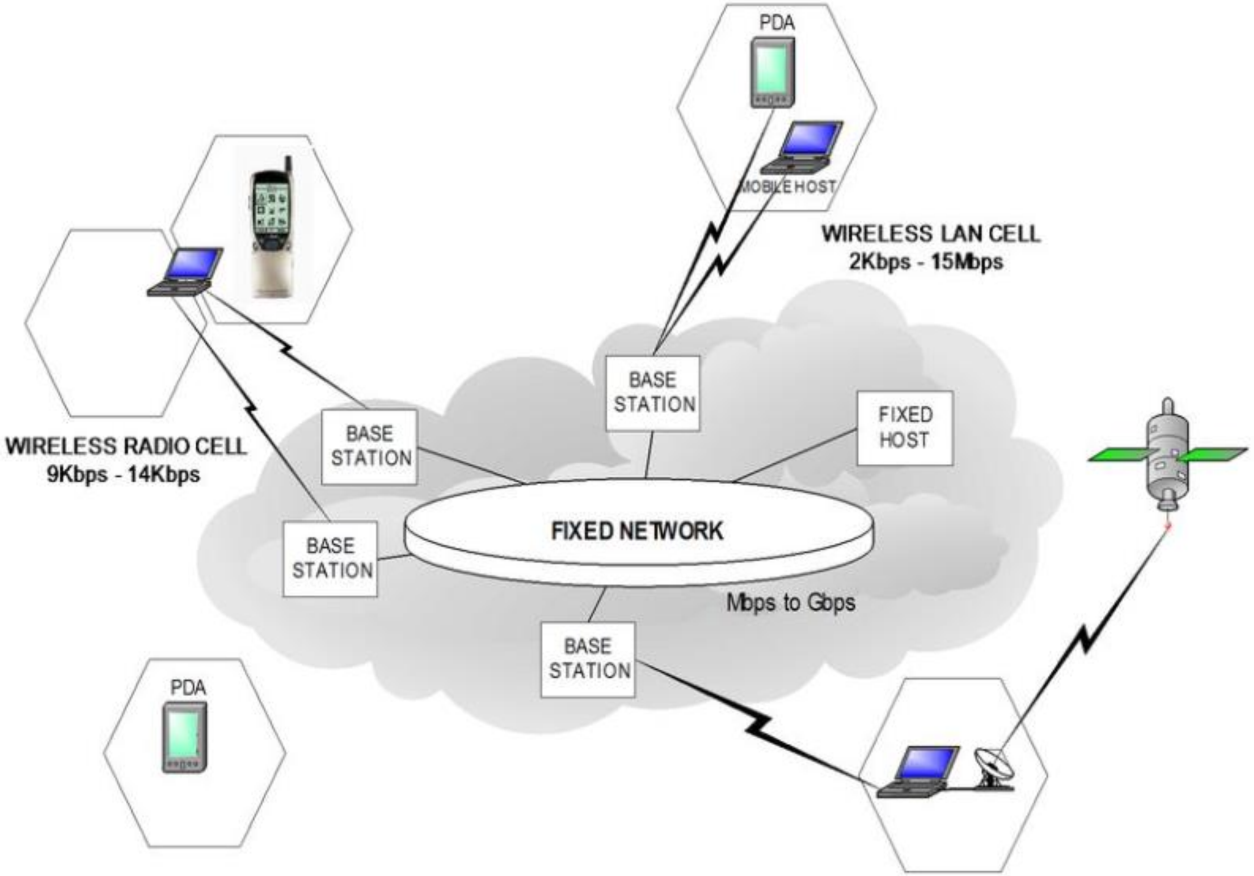


Thank You

Module 2

Location and Handoff Management

Mobile Network Architecture



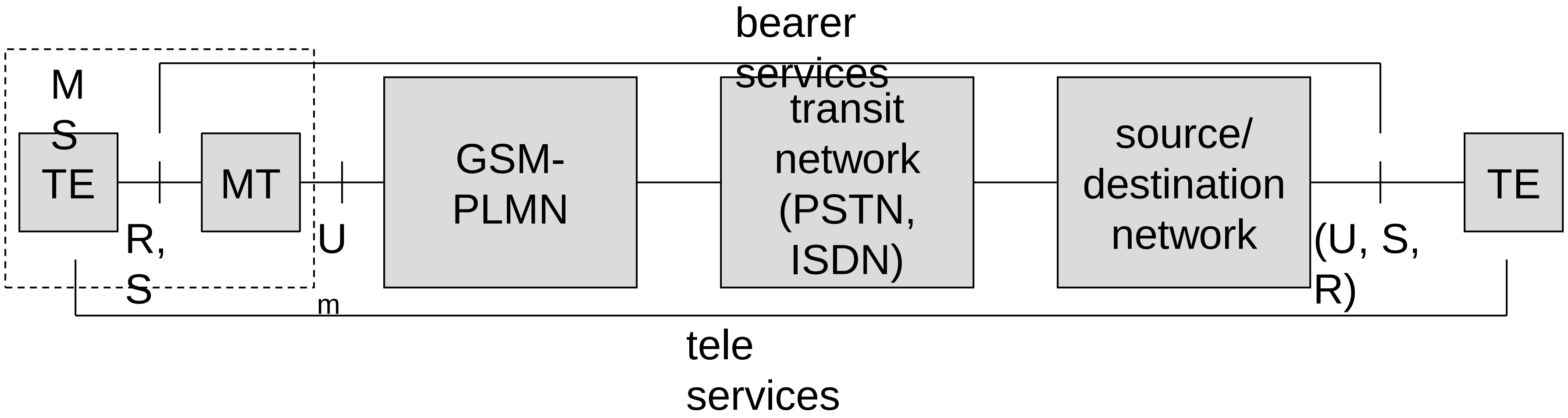
- GSM
  - formerly: Groupe Spéciale Mobile (founded 1982)
  - now: Global System for Mobile Communication
  - Pan-European standard (ETSI, European Telecommunications Standardisation Institute)
  - many providers all over the world use GSM (more than 130 countries in Asia, Africa, Europe, Australia, America)
  - more than 100 million subscribers

Performance characteristics of GSM

- Communication
  - mobile, wireless digital communication; support for voice and data services
- Total mobility
  - international access, chip-card enables use of access points of different providers
- Worldwide connectivity
  - one number, the network handles localization High capacity
  - better frequency efficiency, smaller cells, more customers per cell
- High transmission quality
  - high audio quality
  - uninterrupted phone calls at higher speeds (e.g., from cars, trains) – better handoffs and
- Security functions
  - access control, authentication via chip-card and PIN

GSM: Mobile Services

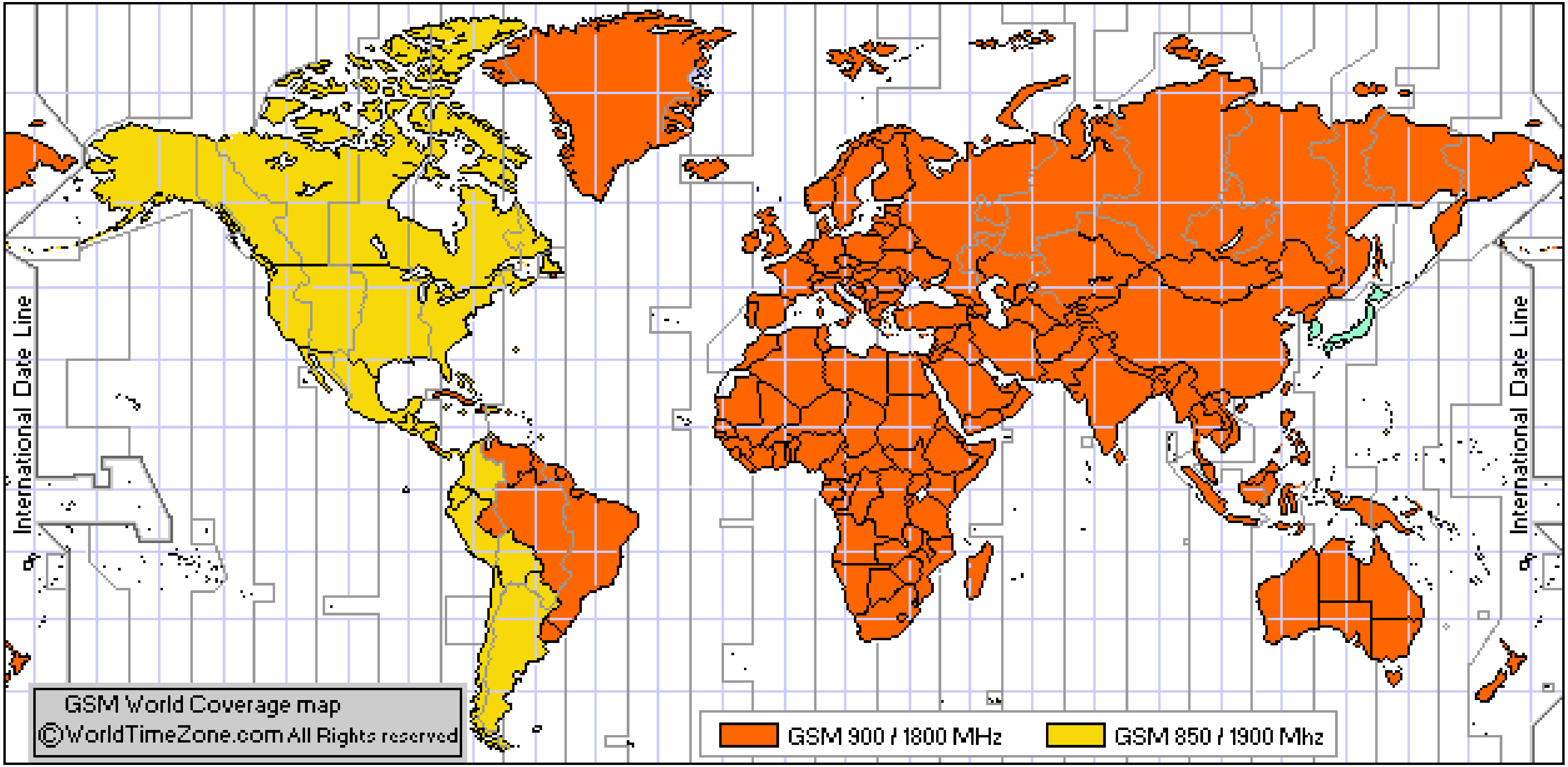
- ➢ GSM offers
- several types of connections
  - voice connections, data connections, short message service
- ➢ Three service domains
- **Bearer Services** – interface to the physical medium (transparent for example in the case of voice or non transparent for data services)
- **Telematic Services** – services provided by the system to the end user (e.g., voice, SMS, fax, etc.)
- **Supplementary Services** – associated with the tele services: call forwarding, redirection, etc.



Architecture of the GSM system

- GSM is a PLMN (Public Land Mobile Network)
  - *several providers setup mobile networks following the GSM standard within each country*
  - components
    - MS (mobile station)
    - BS (base station)
    - MSC (mobile switching center)
    - LR (location register)
- subsystems
    - RSS (radio subsystem): covers all radio aspects
    - NSS (network and switching subsystem): call forwarding, handover, switching
    - OSS (operation subsystem): management of the network

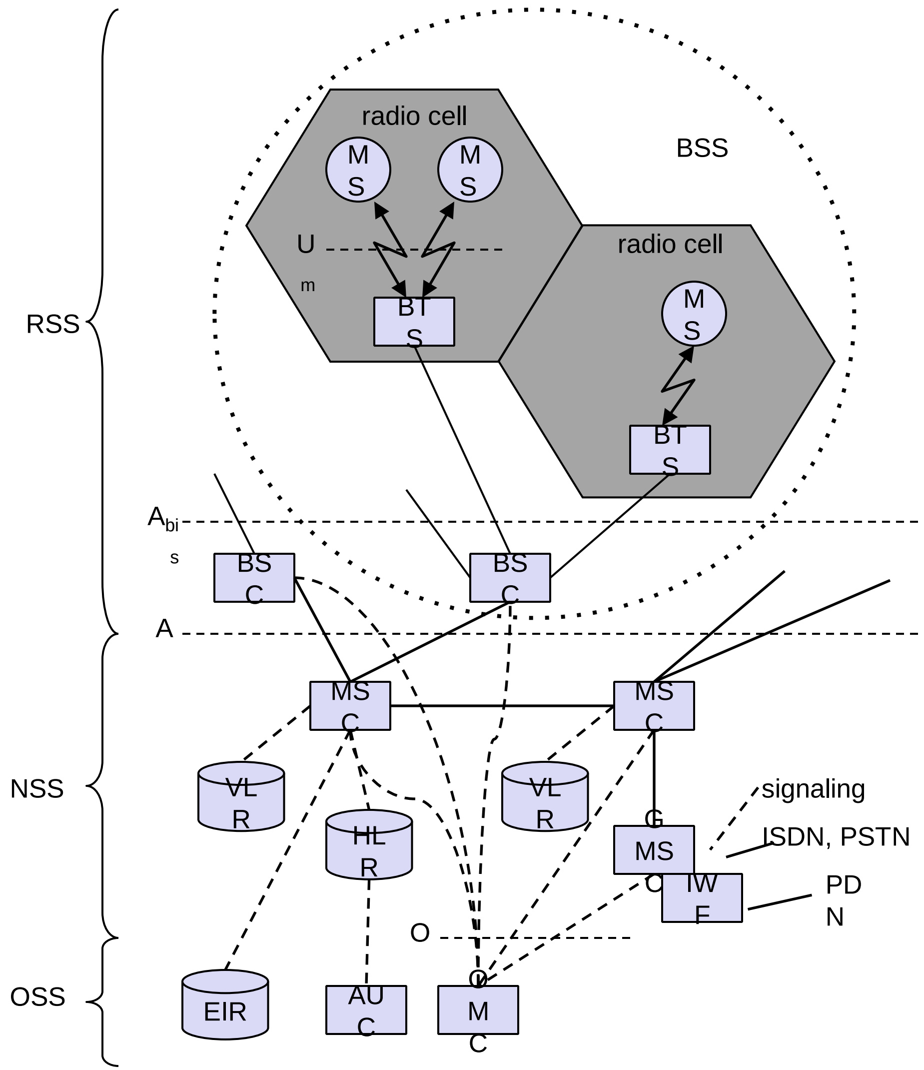
GSM World Coverage Map



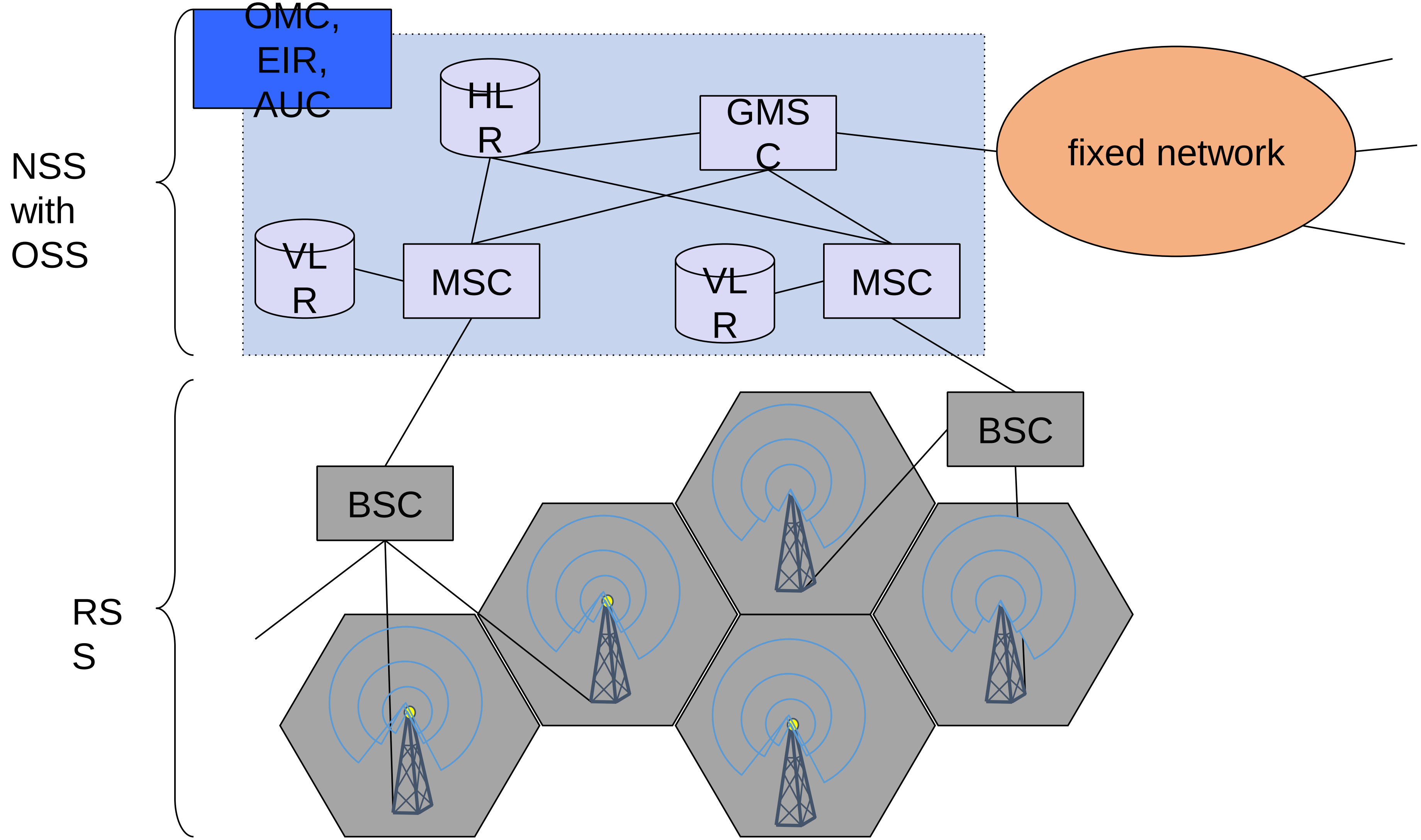
https://www.worldtimezone.com/gsm.html

India	900	1800	3G 900/2100 AirTel; 3G 2100 BSNL; 3G 2100 MTNL; 3G 2100 Tata Docomo; 3G 2100 Vodafone Idea LTD ;	4G LTE Vodafone Idea LTD 1800/2100/2500Mhz ; 4G LTE Bharti Airtel 1800/2100/2300Mhz; 4G LTE Jio 850/1800/2300mhz; 4G LTE BSNL 2500Mhz (trial); 4G LTE Tata DoCoMo Teleservices 900/1800/2100/2300Mhz ;

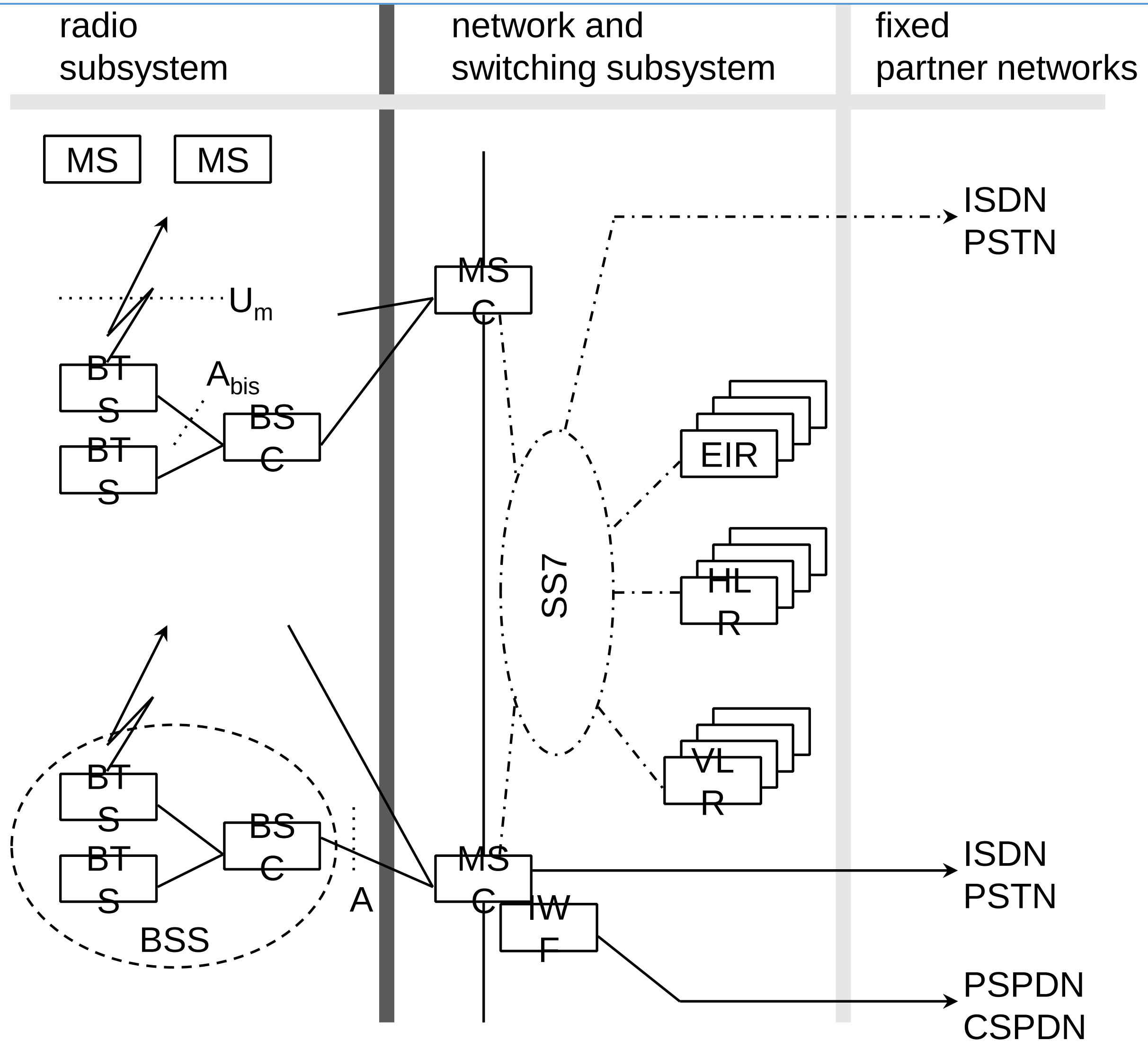
GSM: elements and interfaces



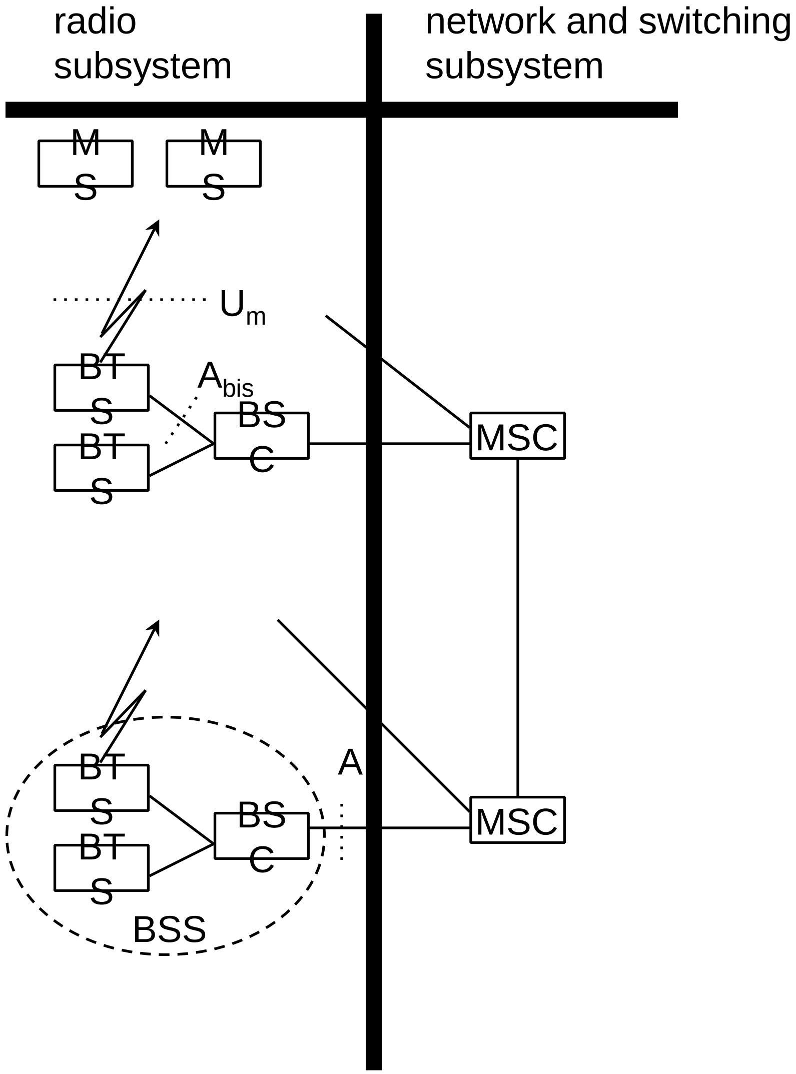
GSM: overview



GSM: System Architecture



System architecture: radio subsystem



- Components
  - *MS* (Mobile Station)
  - *BSS* (Base Station Subsystem): consisting of
    - *BTS* (Base Transceiver Station): sender and receiver
    - *BSC* (Base Station Controller): controlling several transceivers
- Interfaces
  - U_m : radio interface
  - A_{bis} : standardized, open interface with 16 kbit/s user channels
  - *A*: standardized, open interface with 64 kbit/s user channels

Radio subsystem

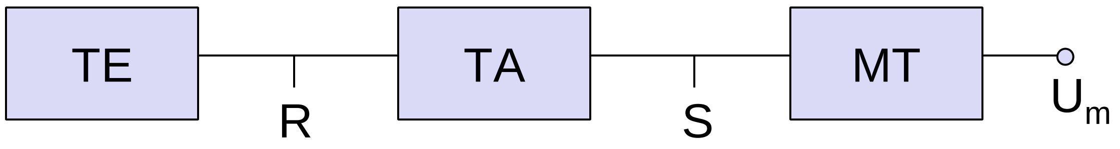
- *The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers*
- Components
  - **Base Station Subsystem (BSS):**
    - Base Transceiver Station (BTS): radio components including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
    - Base Station Controller (BSC): switching between BTSs, controlling BTSs, managing of network resources, mapping of radio channels (U_m) onto terrestrial channels (A interface)
    - BSS = BSC + sum(BTS) + interconnection
  - **Mobile Stations (MS)**

Mobile station

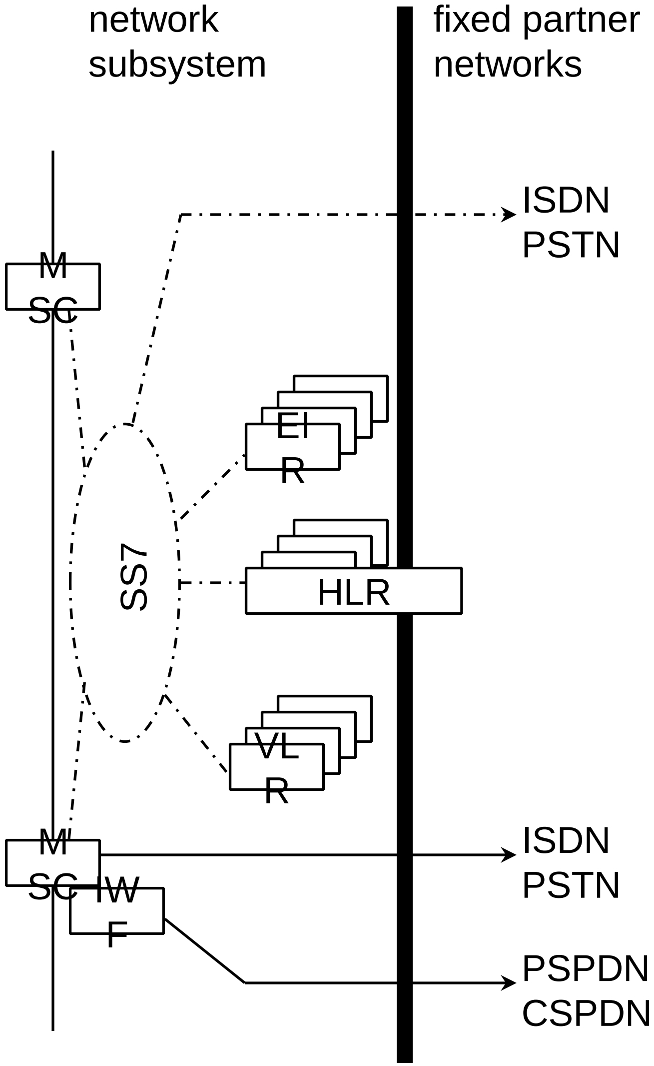
Terminal for the use of GSM services

A mobile station (MS) comprises several functional groups

- MT (Mobile Terminal):
    - offers common functions used by all services the MS offers
    - corresponds to the network termination (NT) of an ISDN access
    - end-point of the radio interface (U_m)
- TA (Terminal Adapter):
    - terminal adaptation, hides radio specific characteristics (TE connects via modem, Bluetooth, IrDA etc. to MT)
- TE (Terminal Equipment):
    - peripheral device of the MS, offers services to a user
    - Can be a headset, microphone, etc.
    - does not contain GSM specific functions
- SIM (Subscriber Identity Module):
    - personalization of the mobile terminal, stores user parameters



System architecture: network and switching subsystem



- Components
  - *MSC* (Mobile Services Switching Center):
  - *IWF* (Interworking Functions)

  - *ISDN* (Integrated Services Digital Network)
  - *PSTN* (Public Switched Telephone Network)
  - *PSPDN* (Packet Switched Public Data Net.)
  - *CSPDN* (Circuit Switched Public Data Net.)

- Databases
  - *HLR* (Home Location *R*egister)
  - *VLR* (Visitor Location *R*egister)
  - *EIR* (Equipment Identity Register)

Network and switching subsystem

- NSS is the main component of the public mobile network GSM
- switching, mobility management, interconnection to other networks, system control

Components

- **Mobile Services Switching Center (MSC)**
  controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC
- **Databases** (important: scalability, high capacity, low delay)
  - **Home Location Register (HLR)**
    central master database containing user data, permanent and semi-permanent data of all subscribers assigned to the HLR (one provider can have several HLRs)
  - **Visitor Location Register (VLR)**
    local database for a subset of user data - data about all users currently visiting in the domain of the VLR

Mobile Services Switching Center

- **The MSC (mobile switching center) plays a central role in GSM**
  - switching functions
  - additional functions for mobility support
  - management of network resources
  - interworking functions via Gateway MSC (GMSC)
  - integration of several databases
- **Functions of a MSC**
  - specific functions for paging and call forwarding
  - termination of SS7 (signaling system no. 7)
  - mobility specific signaling
  - location registration and forwarding of location information
  - provision of new services (fax, data calls)
  - support of short message service (SMS)
  - generation and forwarding of accounting and billing information

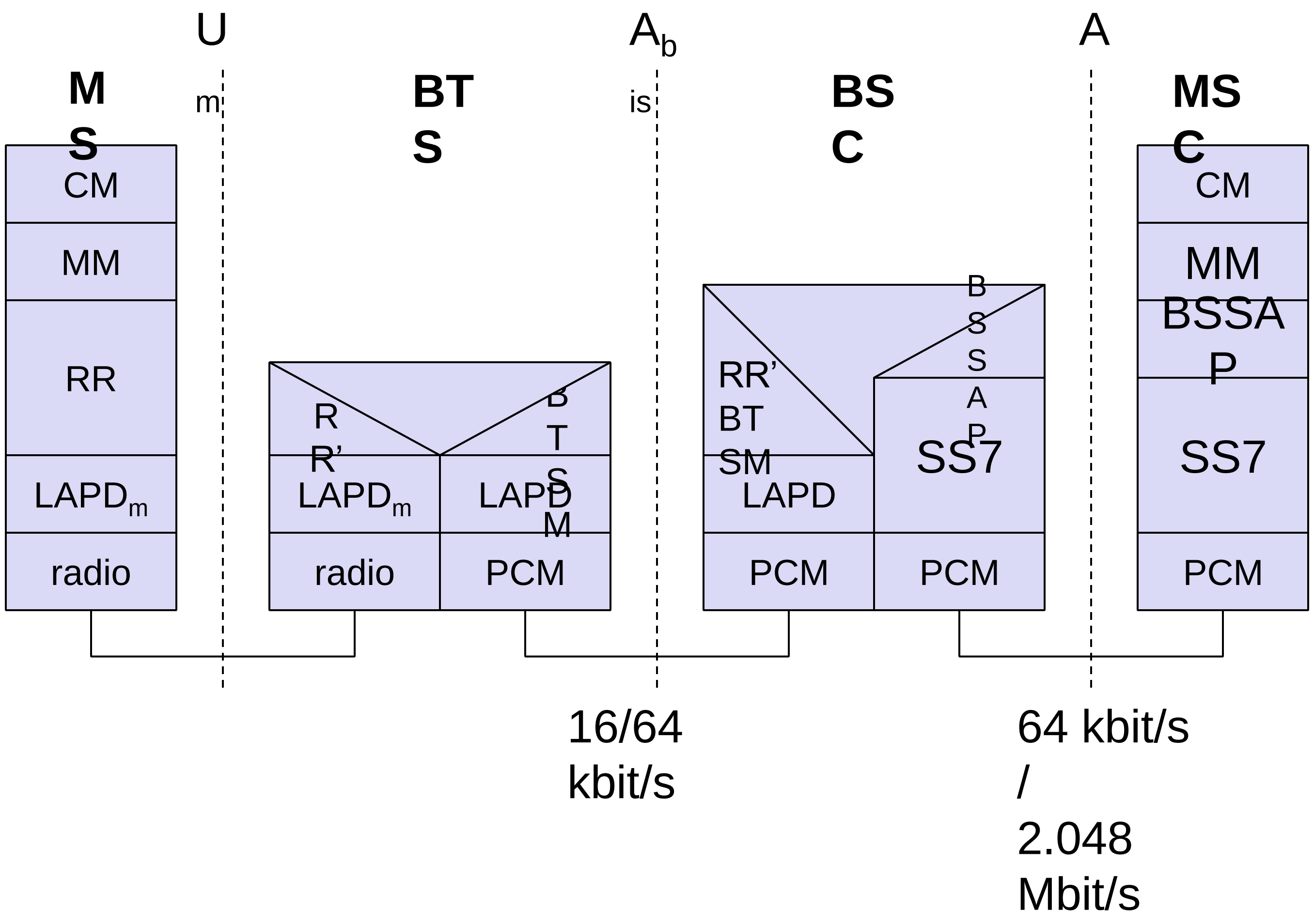
Operation subsystem

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems

- Components

- **Authentication Center (AUC)**
  - generates user specific authentication parameters on request of a VLR
- authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
- **Equipment Identity Register (EIR)**
  - registers GSM mobile stations and user rights
  - stolen or malfunctioning mobile stations can be locked and sometimes even localized
- **Operation and Maintenance Center (OMC)**
  - different control capabilities for the radio subsystem and the network subsystem

GSM protocol layers for signaling



Layer 1, the physical layer

- handles all radio-specific functions
  -includes the creation of bursts according to the five different formats,
  multiplexing of bursts into a TDMA frame, synchronization with the BTS,
  detection of idle channels, and measurement of the channel quality on the downlink.

- The physical layer at Um uses GMSK for digital modulation and performs encryption/decryption of data, encryption is between MS and BSS over the air interface.

- The main tasks of the physical layer comprise
  channel coding and error detection/correction, which is directly combined with the coding mechanisms.
  Channel coding uses forward error correction (FEC) schemes.
- The physical layer also contains special functions, such as voice activity detection (VAD), which transmits voice data only when there is a voice signal
- During periods of silence the physical layer generates a comfort noise to fake a connection but no actual transmission takes place.

Layer 2, LAPDm

- The LAPDm protocol has been defined at the Um interface .
- LAPDm, link access procedure for the D-channel (LAPD) in ISDN systems, . LAPDm is a lightweight LAPD
- LAPDm offers reliable data transfer over connections, re-sequencing of data frames, and flow control
- LAPDm has to obey the frame structures recurrence patterns etc. defined for the Um interface as there is no buffering between layer one and two,
- LAPDm provides segmentation and reassembly of data and acknowledged/unacknowledged data transfer.

layer 3,network layer

Comprises several sublayers as

- Radio resource management (RR).

Only a part of this layer, RR’, is implemented in the BTS, the remainder is situated in the BSC.

The functions of RR’ are supported by the BSC via the BTS management (BTSM).

The main tasks of RR are setup, maintenance, and release of radio channels.RR also directly accesses the physical layer for radio information and offers a reliable connection to the next higher layer.

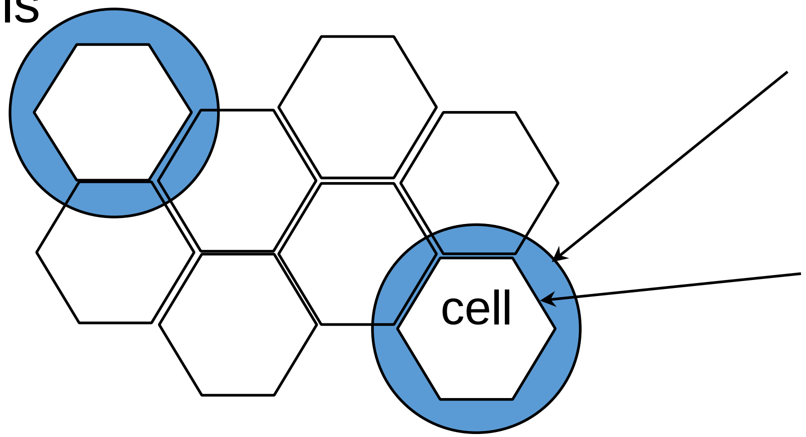
- Mobility management (MM)

registration, authentication, identification, location updating, and the provision of a temporary mobile subscriber identity (TMSI) that replaces the international mobile subscriber identity (IMSI) and which hides the real identity of an MS user over the air interface. MM offers a reliable connection to the next higher layer.

Call management (CM) layer contains three entities:

- call control (CC), short message service (SMS), and supplementary service (SS).
- SMS allows for message transfer using the control channels SDCCH and SACCH .
- CC provides a point-to-point connection between two terminals and is used by higher layers for call establishment, call clearing and change of call parameters.
- This layer provides functions to send in-band tones, called dual tone multiple frequency (DTMF), over the GSM network.
- These tones are used,e.g., for the remote control of answering machines or the entry of PINs in electronic banking and are, also used for dialing in traditional analog telephone systems. These are transferred as signals and then converted into tones in the fixed network part of the GSM system.

GSM: cellular network



- use of several carrier frequencies
- not the same frequency in adjoining cells
- cell sizes vary from some 100 m up to 35 km depending on user density, geography, transceiver power etc.
- hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)
- if a mobile user changes cells
  ⇒ handover of the connection to the neighbor cell

GSM: Identification

- Identification of Mobile Subscriber
  - International Mobile Subscriber Identity (IMSI)
  - Temporary IMSI (TMSI)
  - Mobile Subscriber ISDN number (MSISDN)
- Identification of Mobile Equipment
  - International Mobile Station Equipment Identification (IMEI)
  - Mobile Station Roaming Number (MSRN)

MSISDN

- “real telephone number” of a MS
- It is stored centrally in the HLR
- MS can have several MSISDNs depending on SIM
- It follows international ISDN numbering plan
  - Country Code (CC): upto 3 decimal places
  - National Destination Code (NDC): 2-3 decimal places
  - Subscriber Number (SN) : maximal 10 decimal places
    - MSISDN = CC + NDC + SN

IMSI

- International Mobile Subscriber Identity
- Stored in SIM, not more than 15 digits
    - 3 digits for Mobile Country Code (MCC)
    - 3 digits for Mobile Network Code (MNC)
        - It uniquely identifies the home GSM PLMN of the mobile subscriber.
    - Not more than 10 digits for National Mobile Station Identity (MSIN)
        - The first 3 digits identify the logical HLR-ID of the mobile subscriber
- MNC+MSIN makes National Mobile Station Identity (NMSI)

TMSI and LMSI

- Temporary Mobile Subscriber Identity
  - Has only local and temporal significance
  - Is assigned by VLR and stored there only
  - Is used in place of IMSI for security reasons
- Local Mobile Subscriber Identity
  - Is an additional searching key given by VLR
  - It is also sent to HLR
- Both are assigned in an operator specific way

Mobility Models

- Mobility models **characterize the movements of mobile users with respect to their location, velocity and direction over a period of time**.
- These models play an vital role in the design of Mobile Ad Hoc Networks(MANET)

Location and Handoff Management

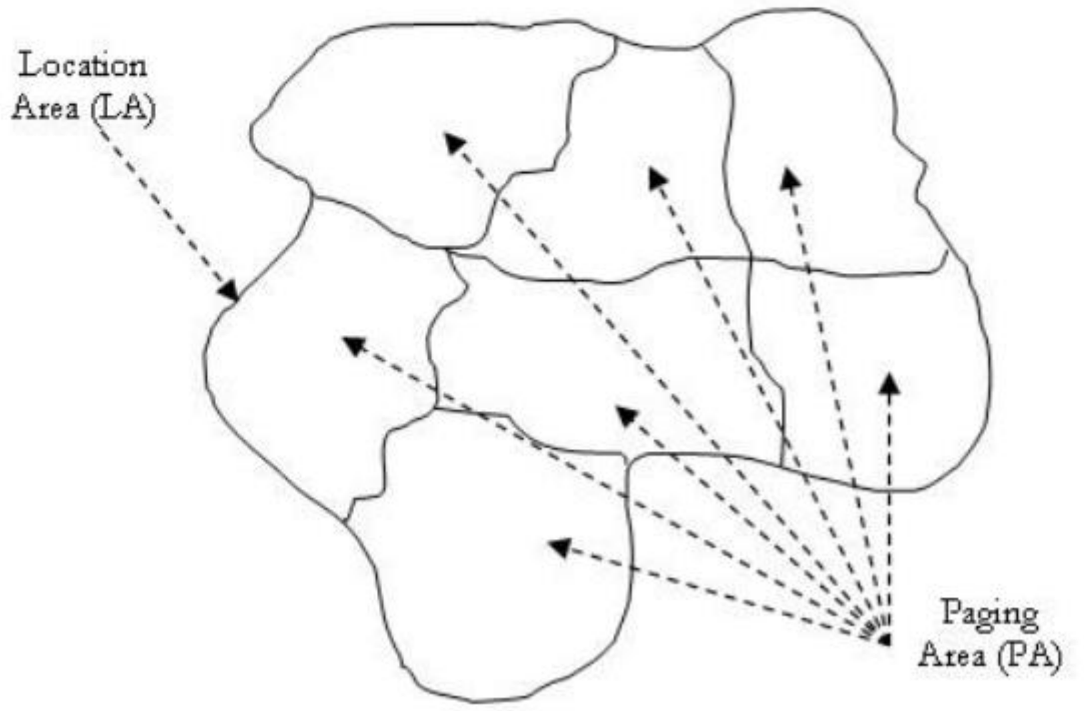
Module 2

Location Management

LM consists mainly of:

1. Location Tracking and Updating (Registration): A process in which an end-point initiates a change in the Location Database according to its new location.
    1. This procedure allows the main system to keep track of a user's location so that for example an incoming call could be forwarded to the intended mobile user when a call exists or maybe bring a user's profile near to its current location so that it could provide a user with his/her subscribed services.
2. Location Finding (Paging): The process of which the network initiates a query for an end-point's location.
    1. This process is implemented by the system sending beacons to all cells so that one of the cells could locate the user. This might also result in an update to the location register.

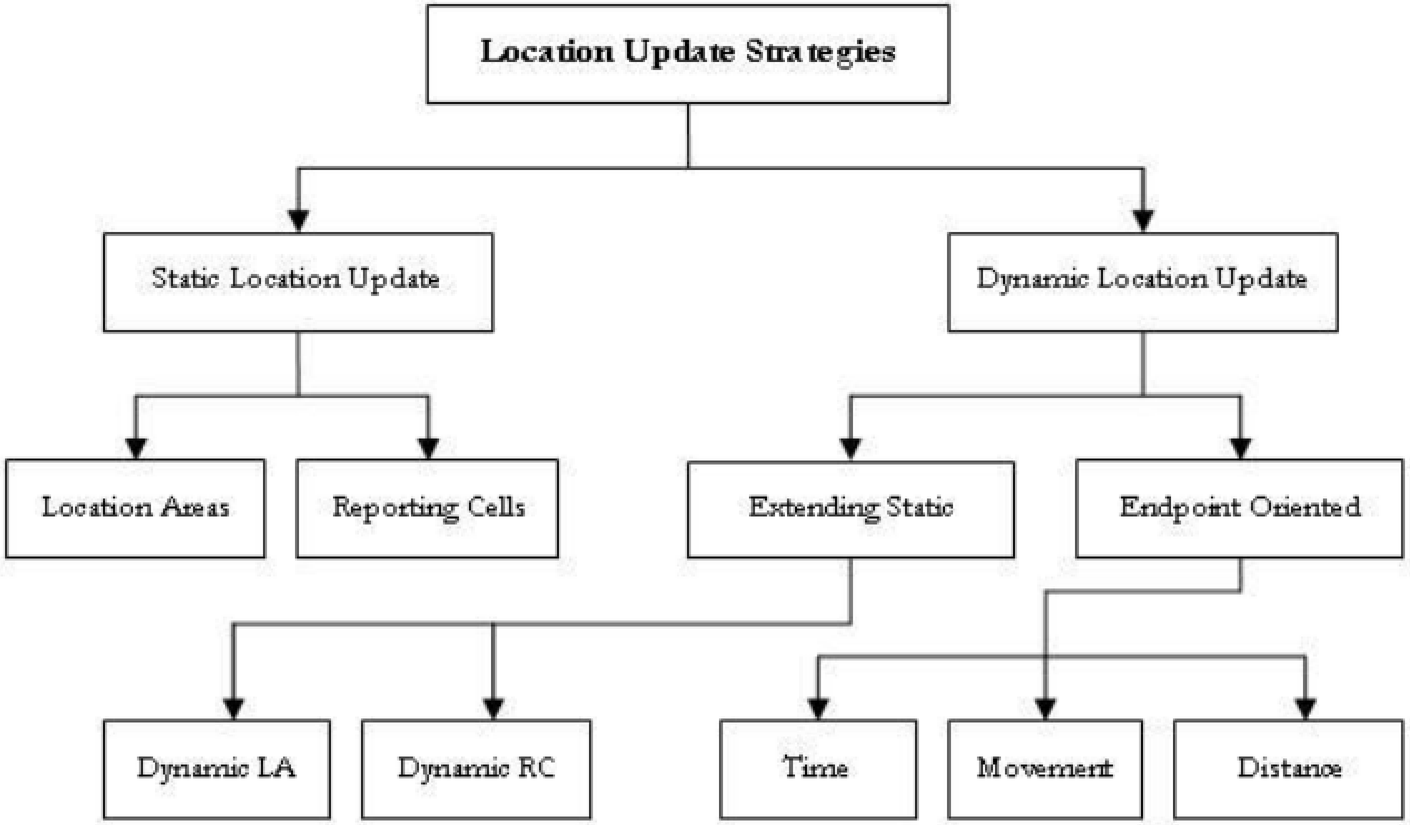
Concept of LA and PA



Location Management

- Cells in a network are grouped into Location Areas (LAs).
- Users can move within these LAs, updating their location with the network based upon some predefined standard.
- When a user receives a call, the network must page cells within the LA (also referred to as polling) to find that user as quickly as possible.
    - frequent Location Updates (LUs) to reduce polling costs by incurring increased time and energy expenditures from all the updates
    - only require rare LUs, storing less information about users to reduce computational overhead, but at a higher polling cost

Location Update Strategies



Issues in Location Management

- database architecture design
- transmission of signaling between various components of a signaling network
- security, dynamic database updates
- querying delays
- terminal paging methods
- paging delays

LM Schemes

Without Location Management

1. Is referred to as the Level 0 method.

2. The system doesn't track any mobile devices.

3. Searching for a user is done over the complete radio coverage area and within a specific time limit.

4. Is also referred to as the Flooding Algorithm.

5. It is used in paging

6. advantage-it is simple to implement because of the absence of a special database.

7disadvantage- is that it doesn't fit into large networks dealing with high number of users and high incoming data exchange rates.

Manual Registration in Location Management

1. Is referred to as the Level 1 method.

2. The system is simple to manage because it only requires the management of an indicator which stores the current location of the user.

3. The mobile is relatively simple since its task is limited to scanning the channels to detect paging messages. An example of such a system is telepoint cordless systems.

4. The main disadvantage of this method is that users have to re-register each time they move.

LM Schemes

Automatic Location Management using LAs

1. Is referred to as the Level 2 method.

2. Widely used and deployed in 1G and 2G cellular systems.

3. Since this method is a LA based method, a home database and several visitor databases are included in the network architecture.

Memoryless-Based Location Management Methods

- These methods depend mainly on the processing capabilities of the system. They are based on algorithms and the network architecture.

Memory-Based Location Management Methods

- The design of memory-based location management methods has been motivated by the fact that systems perform many repetitive actions which can be avoided
- if predicted.

Location Management in Next Generation Systems

- The next generation in mobility management will enable different mobile networks to interoperate with each other to ensure terminal and personal mobility and
- global portability of network services. However, in order to ensure global mobility, the deployment and integration of both wired and wireless components is necessary.
- These future systems will all depend on the usages of Mobile IP. For example, the aim of 4G cellular networks is to deploy Mobile IP in its infrastructure so that users can switch between different access technologies.

Static Location Management

- most LM schemes are static, where LUs occur on either periodic intervals or upon every cell change.
- static LAs incur great costs with the ping-pong effect.
  - When users repetitively move between two or more LAs, updates are continuously performed unnecessarily
- cells are constant in size, uniform, and identical for each user
- Three simple static Location Update schemes
  - being always-update : involves the user updating its location upon every inter-cell movement
  - never-update : never require the user to inform the network of intercell movements, only updating on LA changes, and is named never-update
  - static interval-based - each user within the network to update at static, uniform intervals.

Static Location Update Scheme

being always-update : involves the user updating its location upon every inter-cell movement

Limitations -

- incur significant energy and computational costs to both the network and the user,
- may be particularly wasteful, as if a user makes frequent, quick movements within an LA,
- beginning and ending at the same location, many LUs will occur that might be unnecessary, especially if few or no calls are incoming.

Advantage -

- network will always quickly locate a user upon an incoming call, and extensive paging will not be necessary.

Static Location Update Scheme

never-update : never require the user to inform the network of inter-cell movements, only updating on LA changes, and is named never-update

Limitations

resources are saved as constant updates are not required, but paging costs rise substantially

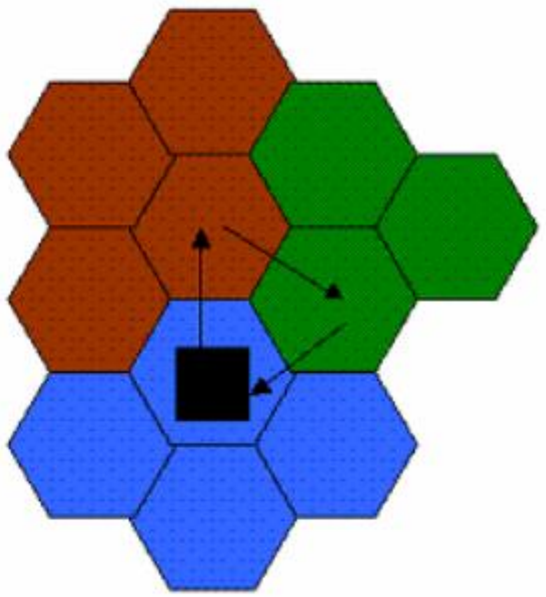
every cell within the user’s LA may need to be checked during paging due to the lack of information, which causes excessive overhead for users with a high incoming call frequency.

Static Location Update Scheme

- static interval-based - each user within the network to update at static, uniform intervals.
- balance between the extremes of the previous schemes, as the network will neither be overwhelmed with LUs nor wholly unaware of users' locations.
- Limitation-
  - users with rapid rates of movement may move into new LAs between updates, which causes locating that user to be very difficult.
  - an inactive user will not move at all, but will still regularly be sending unneeded LUs.

Static Location Areas

- Location Areas in static LM are static.
- They are effectively the easiest solution to physically dividing a network, providing the same LA to every user, without any customization.
- static LAs are set and cannot change
- If users repetitively move between two or more adjacent LAs, will cause a large number of LUs with a small or zero absolute cell distance moved.



Optimal LA size static Algorithm

- Fluid model: **This model assumes traffic flow to be like the flow of a fluid**. The amount of traffic flowing out of an area is proportional to the population density of the area, the average velocity of movement, and the length of the area boundary.
- The optimal static LA size algorithm, which uses a **Fluid-Flow mobility** model, states that in a network with uniform cell size, cell shape, and user movement speed, the ideal number of cells per LA is-
  -

$$N_{opt} = \sqrt{\frac{vC_{lu}}{\pi R C_{pg}}}$$

[Giner04]

- where R is the cell radius, v is the speed of a user, Clu is the LU cost, and Cpg is the paging cost per call.
- This equation states that high user speed and LU costs indicate that having a large number of cells per LA is preferable, while a large cell radius and high paging costs imply that a small number of cells per LA is optimal.

Static LM Standards/Implementation

- In current cellular telephone usage,
  - the Electronic and Telephone Industry Associations (EIA/TIA) Interim Standard IS-41, and the Global System for Mobile Communications (GSM) Mobile Application Part (MAP).
  - Both of these are quite similar, having two main tasks of Location Update and Call Delivery.

Two level hierarchical database scheme

- The Home Location Register (HLR) contains the records of all users' services, in addition to location information for an entire network.
- Visitor Location Registers (VLRs) download data from the HLR concerning current users within the VLR's specific service areas.
- Each LA has one VLR servicing it, and each VLR is designed to only monitor one LA.
- each VLR is connected to multiple Mobile Switching Centers (MSCs), which operate in the transport network in order to aid in handoffs and to locate users.

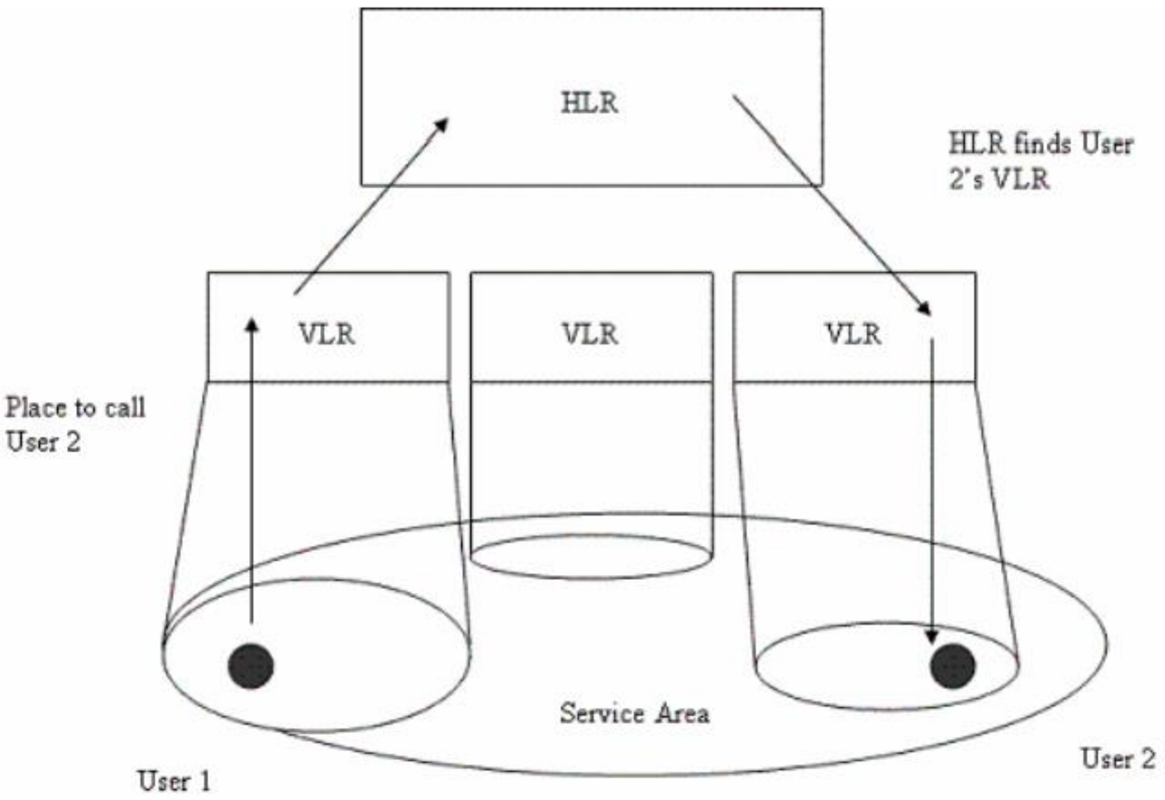


Figure 2: HLR/VLR architecture, Example of Call Process

Communication on a call

- All **inter-cell movements** cause an **update to the VLR**, while the HLR does not need any modification, as both the MSC and VLR that the user resides in remains constant.
- **Inter-MSC movements** within the **same LA** cause the **VLR to be updated** with the new cell address, and also cause an update to the HLR to modify the stored value of the user's MSC.
- Finally, **Inter-VLR movements** cause the new VLR to create a record for the user, as well as causing an **update to the HLR** where both **MSC and VLR fields** are updated.
- After this occurs, the old VLR's record for the user is removed. Figure 2 displays a symbolic high-level view of the HLR/VLR architecture, as well as demonstrating the methods of communication on a call.

Call Delivery with the help of SS7

- System database is queried to determine the LA or registration area of the user.
  - This is split into two steps; a fixed network interrogation is performed to find a region of cells containing the target, in which the HLR is queried to obtain the VLR of the called user.
  - Next, paging is used to poll cells within this region until the user is found.
- Currently, a system called Signaling System 7 (SS7) is used to transmit these locating messages.
- In this system, Signal Transfer Points (STPs) route messages through the network (as the HLR), while Service Control Points (SCPs) maintain the databases and information (as VLRs), and Service Switching Points (SSPs) help route calls (as MSCs).

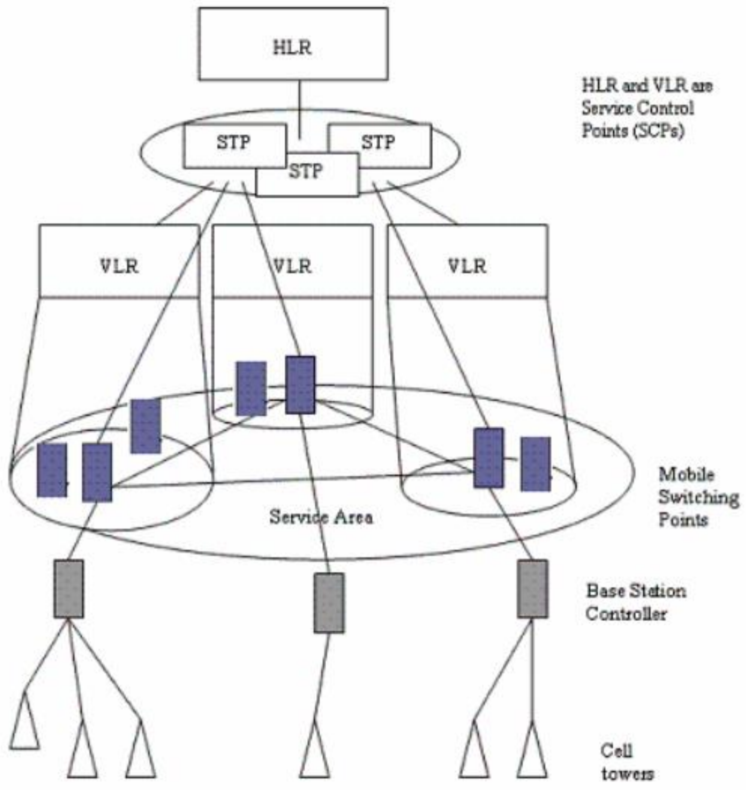


Figure 3: HLR/VLR architecture with SS7

Location Management Parameters

1. Paging
    - Simultaneous Paging-
        - every cell in the user's LA is paged at the same time in order to find the user
        - Quicker
        - Cost wise inefficient
    - Sequential Paging-each cell within an LA is paged in succession
        - poll the cells nearest to the cell of the most recent LU, and then continue outward if the user is not immediately found.
    - Intelligent Paging
        - calculates specific paging areas to sequentially poll based upon a probability matrix.
        - optimized version of Sequential Paging
2. Mobility Models

Mobility Models for Individual Node Movements

Mobility Model is **a model that describe the movement of mobile users and how their location, velocity and acceleration change over time**.

- The mobility metrics usually speaks about the mobility patterns.
- These include spatial dependence, temporal dependence, relative speed and geographic restrictions.

Random Walk

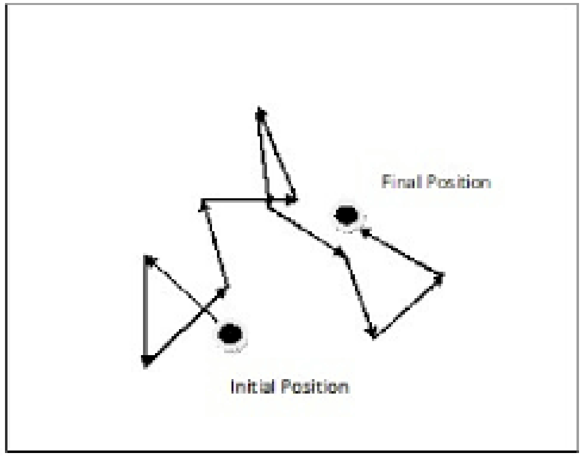
Markov

Fluid Flow

Activity Based

Mobility Models for Individual Node Movements

- Random Walk is a part of Indoor Mobility Models.
  - Indoor Mobility model, there are 3 parts- Random Walk, Random Way-Point, Random Direction.
  - 2D Random Walk is widely used in mobility.
  - It is memory-less mobility pattern.
  - Current speed is independent of its past.
  - This also generates unrealistic movements such as sudden stops and sharp turns.



Mobility Models for Individual Node Movements

- Gauss-Markov mobility model – Outdoor mobility model
  - Probabilistic version of Random walk
  - The model adapts to different levels of randomness.
    - In indoor mobility models, there are fixed simulation areas in which we can do whether random walk or random way-point or random direction.
    - In outdoor mobility model, there is no concept of the simulation area. It is purely random.
  - each mobile node is assigned a current speed and direction. It means that every node has its initial direction and initial speed and it can change itself randomly. It can move freely in and out.
  - The Gauss Markov model has both memory and variability.
  - The tunable alpha parameter determines how much memory and randomness you want to model.

Mobility Models for Individual Node Movements

Fluid Flow model - modelling users as a fluid; free particle (pedestrian) flow and the continuum (large crowd) flow approach

- use of fluid mechanics and transport theory to represent user mobility.
- A model based on viscous free irrotational fluid mechanics
- Empirical data from pedestrian and vehicular studies provide a means of creating realistic group movement characteristics with smooth non random trajectories and smooth continuous velocity.
- The model is used in an example to provide boundary crossing rates for users in a cellular network and optimising the size of cellular location areas.

Mobility Models for Individual Node Movements

- Activity Based Model – Extension of Markovian model
  - parameters such as time of day, current location, and predicted destination are also stored and evaluated to create movement probabilities.
  - a mobility model was developed with the goal of providing realistic mobility patterns for individual subscribers.
  - The model is based on activity pattern theory borrowed from related work in traffic engineering and social science, and using raw data from regional planning travel surveys.
  - The principle behind the model is that, through statistics derived from travel surveys, there are certain probabilities associated with one activity following another activity, based on certain parameters such as time of day and socioeconomic status.

Group based LM

- It is based on the assumption that the number of high cost location update messages from mobile hosts to the location server can be reduced by clustering mobile hosts with similar mobility into a set of groups.
- A single location report for the whole group is sent to the location server
- A leader will be selected to perform location updating on behalf of the whole group to the moving object database.
- positive consequence is that mobile hosts no longer need to possess the long range communication capability with the remote server; location information can be reported via the group leader.

Mobility models characterizing the movement of groups of nodes

1. Reference point based group mobility model

- RPGM model is based on RWP model
- Nodes are divided into groups
- Each group has a leader
- The leader's mobility follows RWP
- The members of the group follow the leader's mobility closely, with some deviation
- Examples:
  - Group tours, conferences, museum visits
  - Emergency crews, rescue teams
  - Military divisions/platoons

Mobility models characterizing the movement of groups of nodes

2. Community based group mobility model

- mobility model based on social network theory.
- each community is defined as a group of nodes that have strong social links with each other, and consequently a likelihood of being co-located together
- An interactionmatrix (IM) where each element has a value ranging from 0 to 1 (low to high) is used torepresent the degree of social interaction between any two nodes.
- the highly connected set of nodes will be grouped together to form a community.
- movements of the nodesare also influenced by the social links between them. A node will move to a randomlyselected location within a community

- *(PDF) A Review of Group Mobility Models for Mobile Ad Hoc Networks*. Available from: https://www.researchgate.net/publication/282535731_A_Review_of_Group_Mobility_Models_for_Mobile_Ad_Hoc_Networks [accessed Aug 07 2022].

Design Features of Group Mobility Models

- **Spatial constraints**: These refer to constraints imposed by the nodes' spatial environment that restrict their movements in a certain way. Such constraints may include roads, walkways, rail tracks, and transportation structures such as bridges andtunnels
- **Collision avoidance:** This refers to controlling the movement of a node to avoid physical collision with other nodes. GFMM introduces repulsion force between neighboring nodes to achieve this goal.
- **Stable group structure**: This refers to maintaining the relative distances and positions among the group members during a group movement, such as when a group of nodes(e.g. troops, tanks, robots) move in formation, or on-board a transport carriage (e.g.bus, truck, train).

Design Features of Group Mobility Models

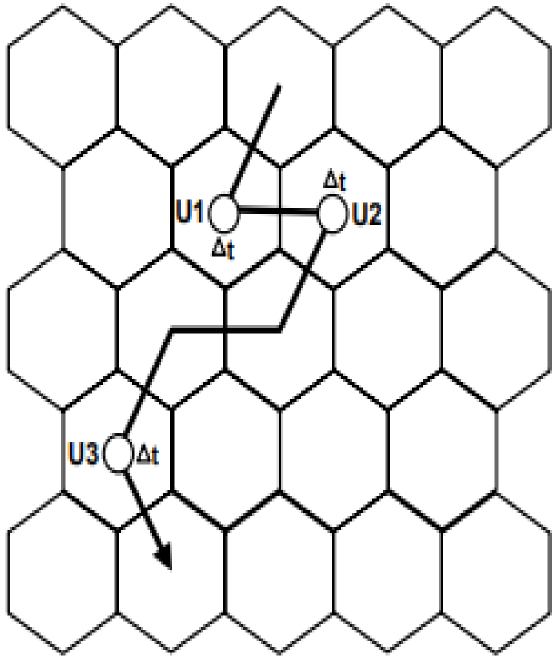
- Group destination: This refers to the target destination of a moving group, which can be randomly chosen or predefined.
- Group coordination: This refers to the existence of some cooperation or interaction among groups, which allows the movement of these groups to be coordinated. Such coordination exists in real-life scenarios such as that exhibited between groups when moving through a road traffic intersection.

Dynamic Location Management

- Dynamic location update schemes allow per-user parameterisation of the location update frequency.
- account for the dynamic behaviour of users and may result in lower location management costs than static schemes.
- Unlike static location management strategies, a location update may be performed from any cell in the network, taking into consideration the call arrival and mobility patterns of the user.

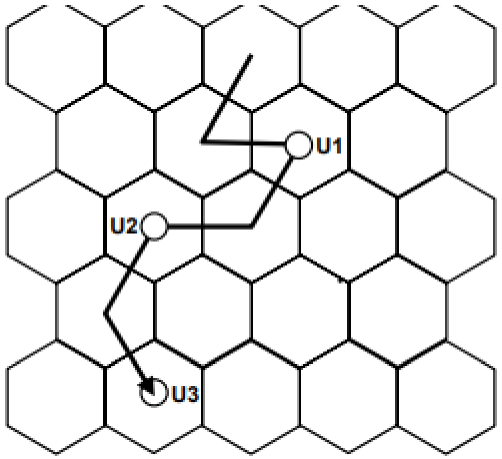
1. Time-based Update

- users update their location at constant time intervals.
- time interval be optimised per-user, to minimise the number of redundant update messages sent.
- requires the mobile device to maintain a simple timer, allowing efficient implementation and low computational overhead.
- a high degree of overhead
  - when a user has only moved a very small distance or
  - has not moved at all



2. Movement-based Update

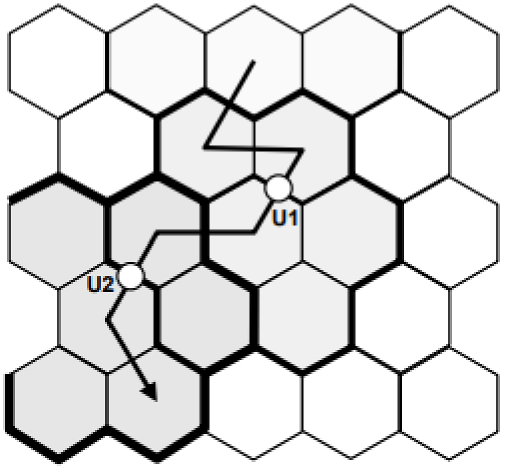
- mobile devices update their location after a given number of boundary-crossings to other cells in the network.
- optimised for individual movement and call arrival rates
- device updates its location every two crossings between cells
- The required paging area is restricted to a neighborhood of radius equal to the distance threshold around the last updated location.



- The paging area requirement is reduced through this scheme,
- although unnecessary updates may still be performed as a result of repeated crossings over the same cell boundary.

3. Distance-based Update

- mobile device performs a location update when it has moved a certain distance from the cell where it last updated its location.
- not requiring an update when a user repeatedly moves between a small subset of cells, provided these cells reside within the distance-threshold radius
- quite difficult to implement in a real-world network
- coordinate system is a non-trivial requirement in a heterogeneous network, where cell adjacencies and distances may not be clearly defined.



4. Profile-based

- the network maintains a profile for each user in the network, based on previous movements, containing a list of the most probable cells for the user to reside within.
- On a location update the network sends this list to the mobile device, forming what may be considered a complex location area.
- The mobile device updates its location only when entering a cell not contained in the list.
- high overhead of sending a large cell list to users outweighs the cost reduction provided by the profile-based scheme.

Adaptive

- predictive distance-based update scheme –
  - predicts a mobile's future location based on the location and velocity information registered during an update.
  - The shape of the assigned location area reflects the mobility patterns of the user, while the size of the area varies as a function of the incoming call rate.
- activity-based location update scheme –
  - The frequency of each cell movement between adjacent cells is measured along with the residence time at each cell
  - likelihood of residence in each cell is evaluated, with each cell added in decreasing probability order until the maximum location area size is reached

Terminal Paging

- mobile devices perform updates according to their location update scheme,
- the network needs to be able to precisely determine the current cell location of a user to be able to route an incoming call.
- This requires the network to send a paging query to all cells where the mobile device may be located, to inform it of the incoming transmission.
  - Simultaneous paging
  - Sequential paging
  - Intelligent Paging

Simultaneous paging (blanket paging)

- used in current GSM network implementations
- all cells in the users location area are paged simultaneously, to determine the location of the mobile device.
- requires no additional knowledge of user location but may generate excessive amounts of paging traffic
- Implementations of simultaneous paging favour networks with large cells and low user population and call rates.
- Not favorable in large networks

Sequential Paging

- Sequential paging avoids paging every cell within a location area by segmenting it into a number of paging areas, to be polled one-by-one.
- The number of cells per paging area is a factor which needs to be optimised and may lead to excessive call delays, particularly in large networks.
- several methods to determine the ordering of paging areas in a sequential scheme.
  - Purely random
  - paging areas located geographically closer to the previously updated location are found to further reduce the total number of paging messages required

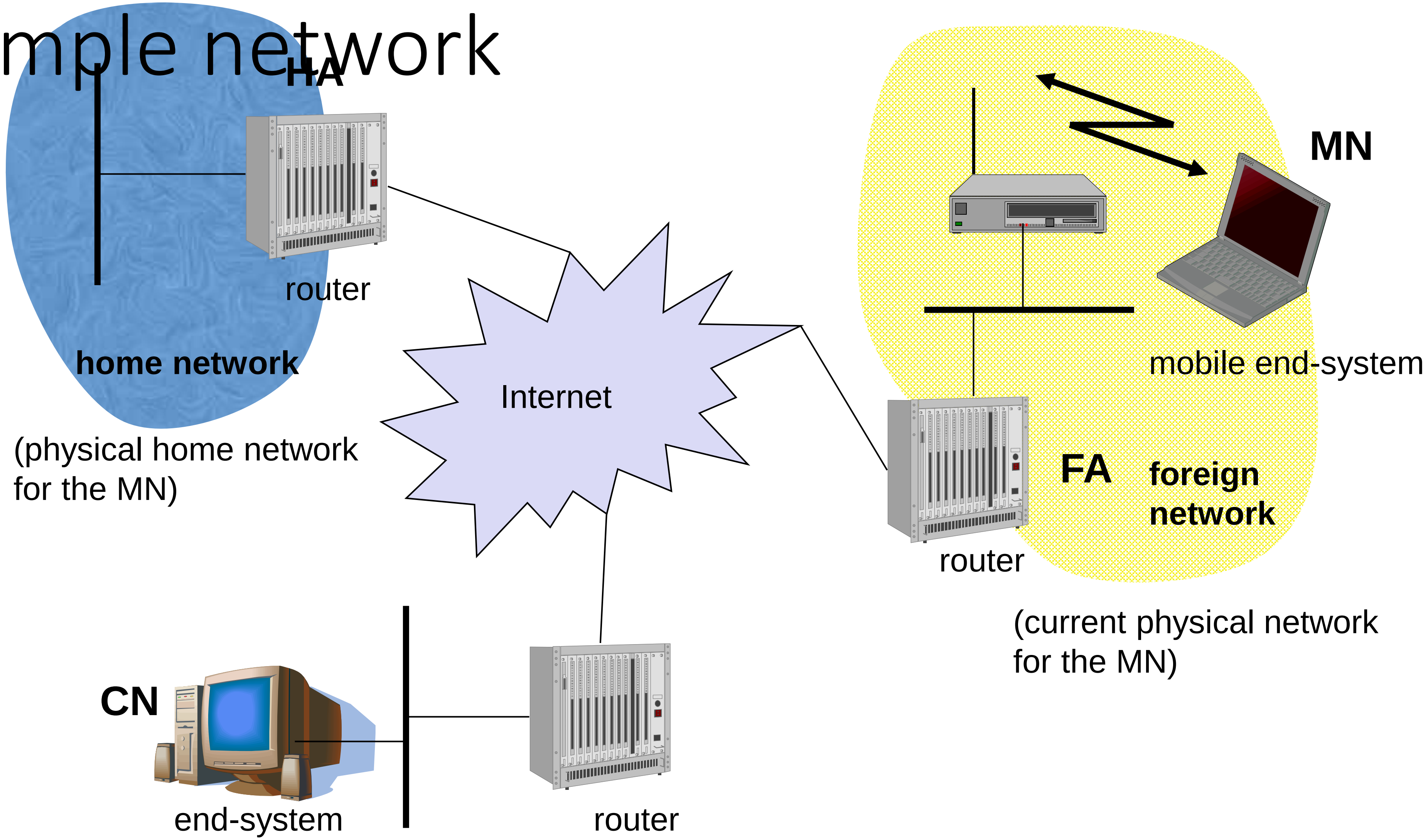
Intelligent Paging

- a variation of sequential paging, where the paging order is calculated probabilistically based on pre-established probability metrics
- s efficient ordering of paging areas requires a **comprehensive knowledge** of user residence probabilities.

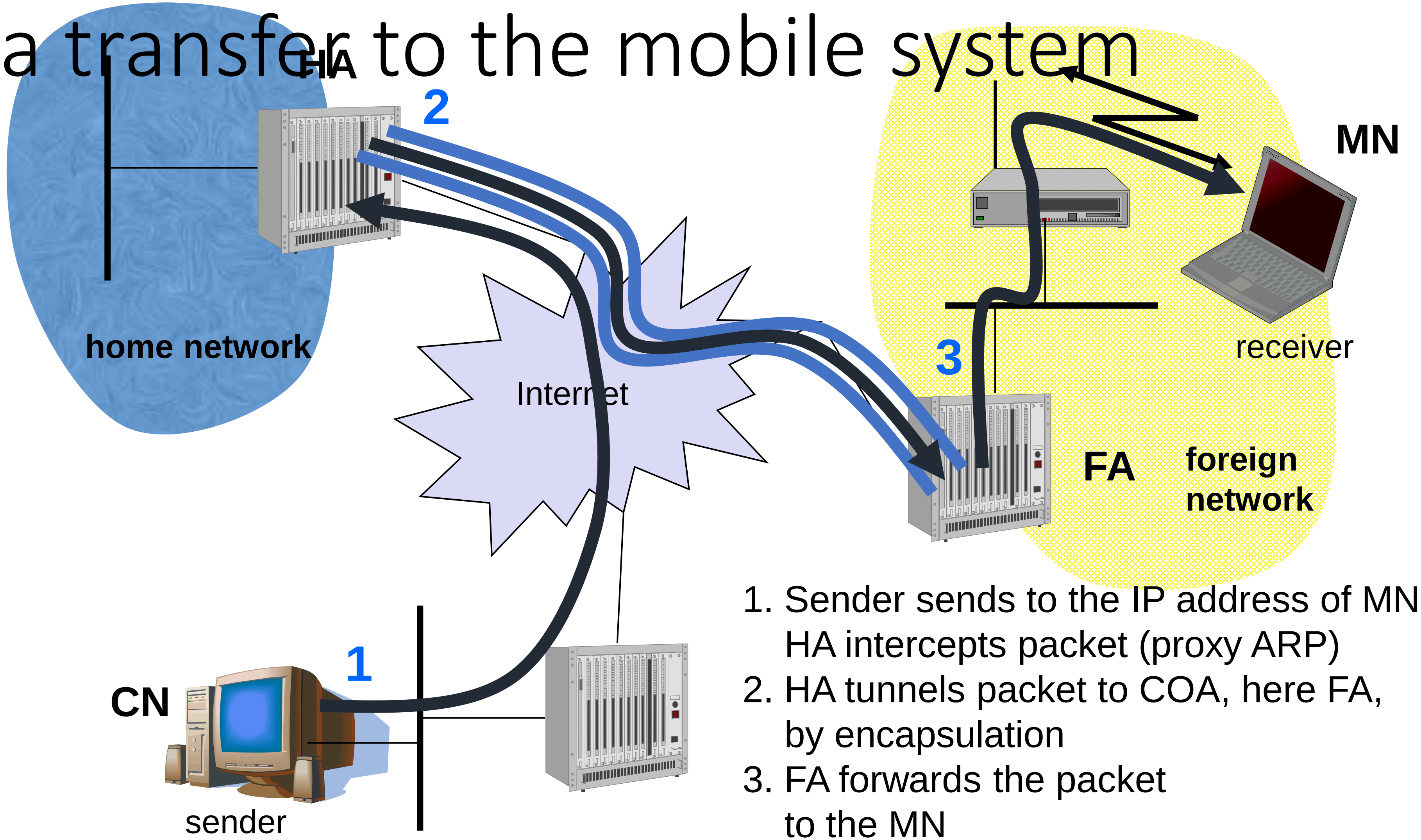
Basics of Mobile IP - Terminology

- Mobile Node (MN)
  system (node) that can change the point of connection
  to the network without changing its IP address
- Home Agent (HA)
  system in the home network of the MN, typically a router
  registers the location of the MN, tunnels IP datagrams to the COA
- Foreign Agent (FA)
  system in the current foreign network of the MN, typically a router
  forwards the tunneled datagrams to the MN, typically also the default router for the MN
- Care-of Address (COA)
  address of the current tunnel end-point for the MN (at FA or MN)
  actual location of the MN from an IP point of view can be chosen, e.g., via DHCP
- Correspondent Node (CN)
  communication partner

Example network

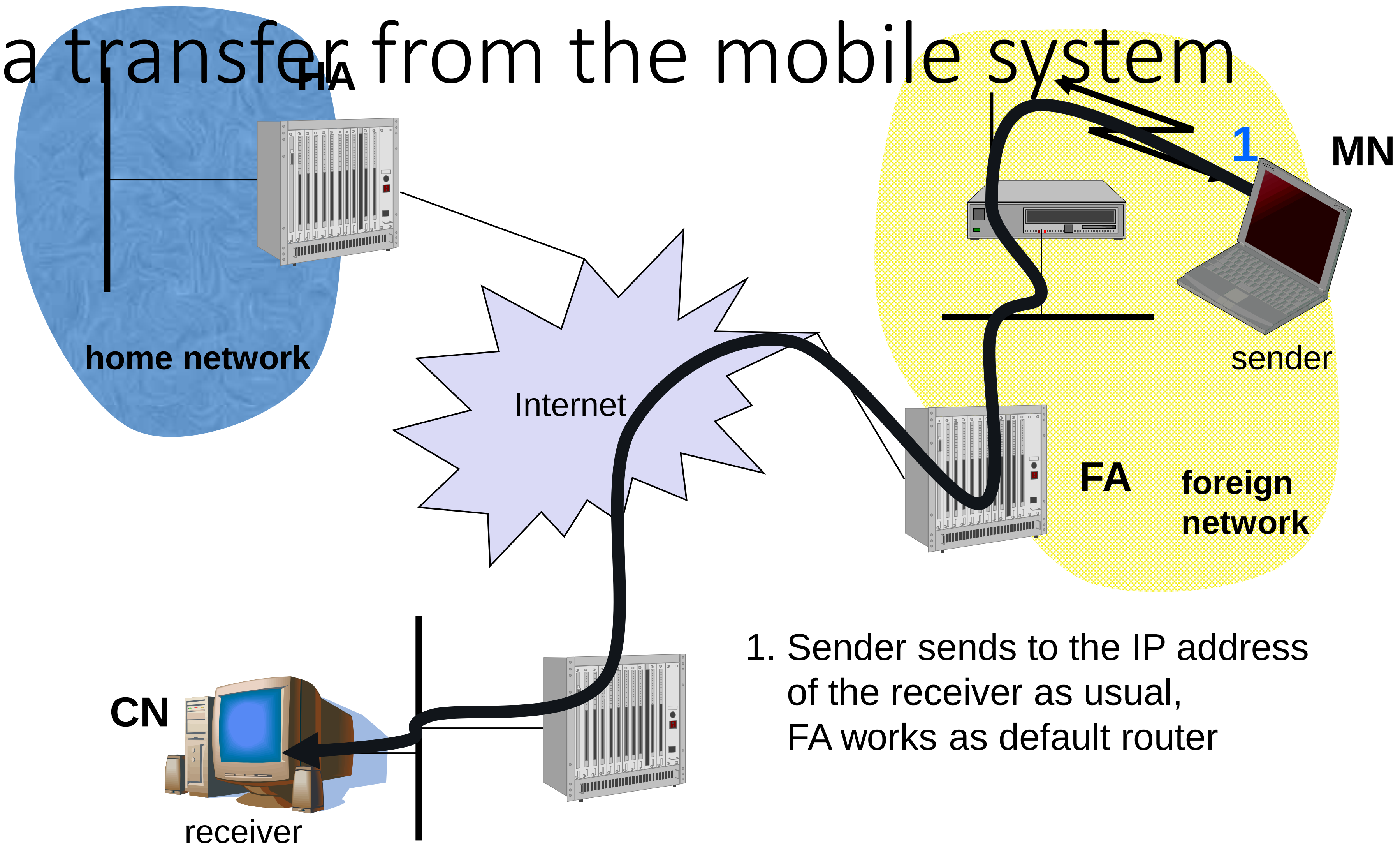


Data transfer to the mobile system



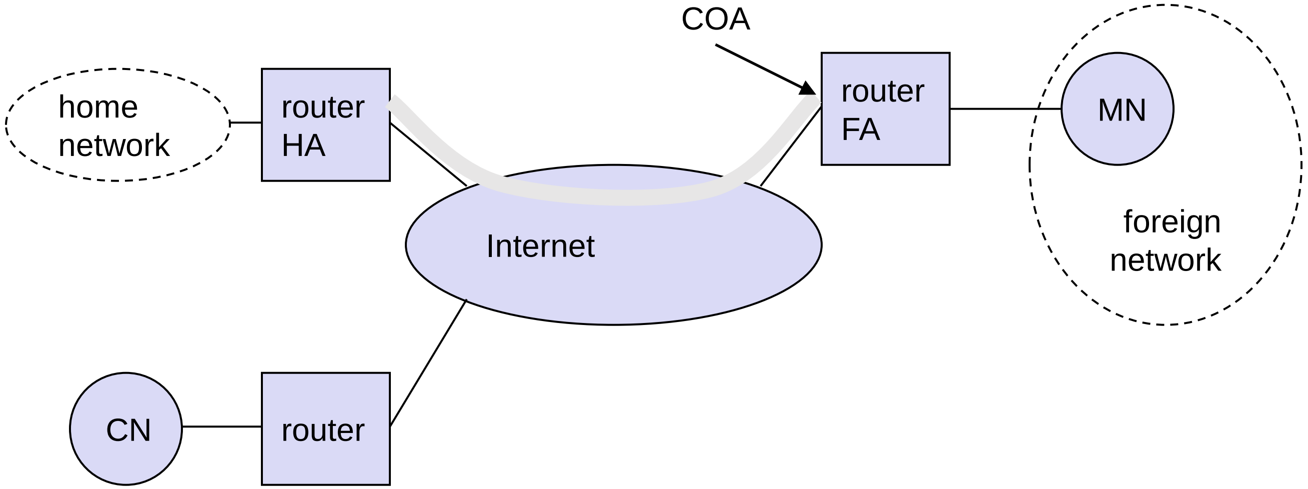
1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

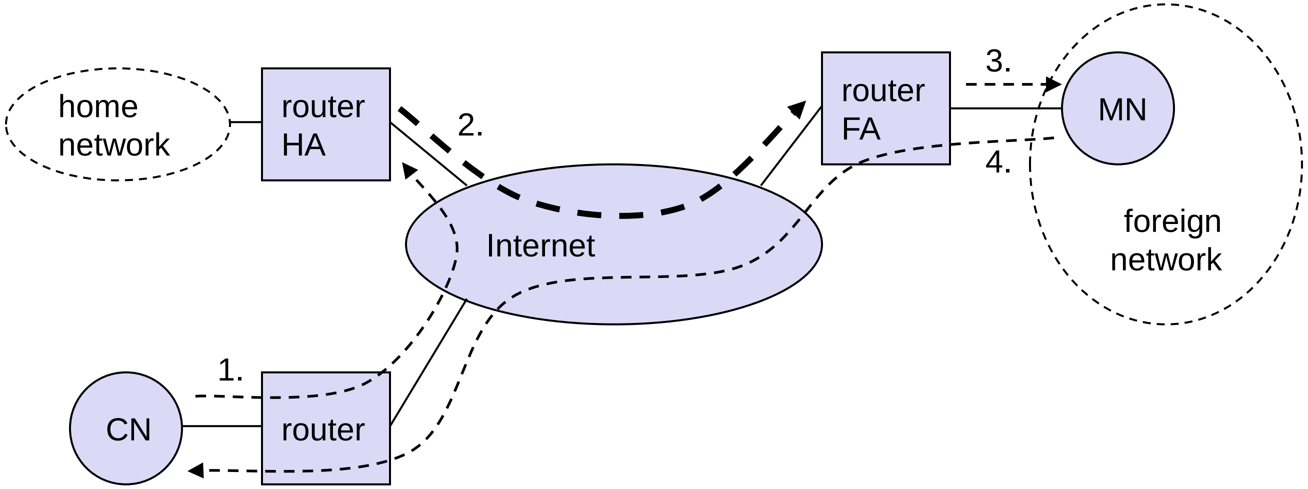
Data transfer from the mobile system



1. Sender sends to the IP address of the receiver as usual, FA works as default router

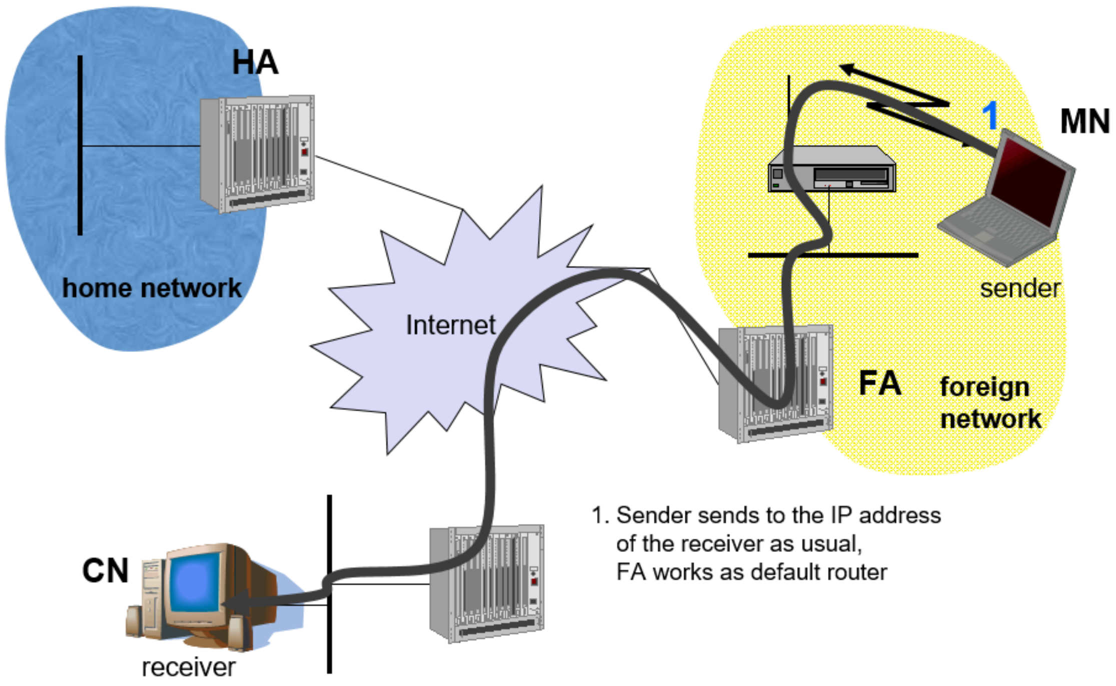
Overview





Packet Delivery to and from the mobile node

Reverse Tunneling



Problems Associated:

1. Firewalls: firewalls only allow packets with topologically correct addresses to pass. This provides at least a first and simple protection against misconfigured systems of unknown addresses.
2. **Multi-cast:** Reverse tunnels are needed for the MN to participate in a multicast group.
3. TTL:The TTL might be low enough so that no packet is transmitted outside a certain region.

Solution

Reverse tunneling now creates a triangular routing problem in the reverse direction. All packets from an MN to a CN go through the HA.

Location management and Mobile IP

- Mobile IP is a common standard to support global mobility of mobile hosts
- major problems for the Mobile IP is frequent location update and high signaling overhead
- To solve this problem, a regional registration scheme was proposed to employ the hierarchy of the foreign agents (FAs) and the gateway foreign agents (GFAs) to localize registration operation.
- hierarchical IPv6 addressing for LM and uses specialized mechanisms for handoff management. It eliminates packet redirection along correspondent node (CN) - mobile node (MN) path, rendering greater scalability and simplifying routing.
- a Hierarchical Mobile IPv6 (HMIPv6) scheme to improve the performance capability of Mobile IPv6 at handover. In HMIPv6, local entities named Mobility Anchor Points (MAPs) are distributed throughout a network to localize the management of intra-domain mobility

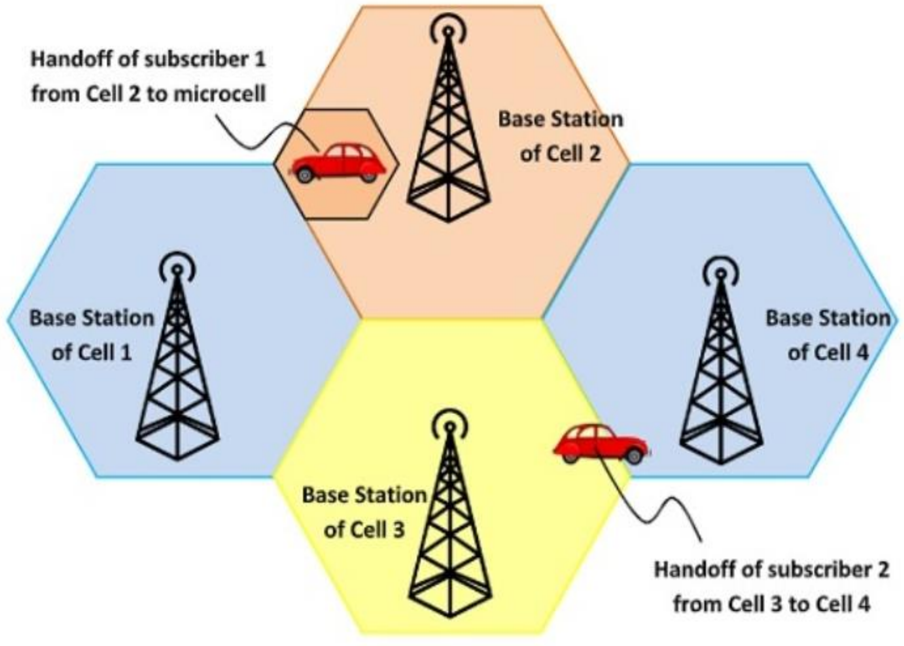
Handoff Management

- Overview of handoff process;
- Factors affecting handoffs and performance evaluation metrics; Handoff strategies;
- Different types of handoffs (soft, hard, horizontal, vertical)

https://www.youtube.com/watch?v=vJcyC1tJvD0

Handoff Process

- The term “handover” or “handoff” as used in the context of mobile or cellular phone systems would be more appropriate as it is simply a change of the active cell.
- Prevents loss of interruption of service.

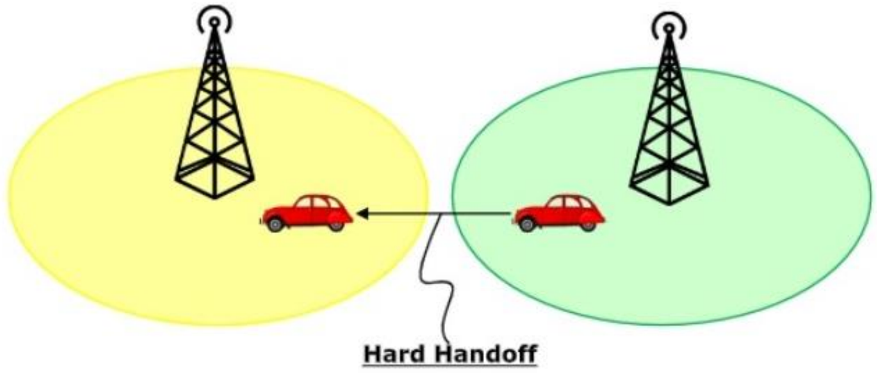


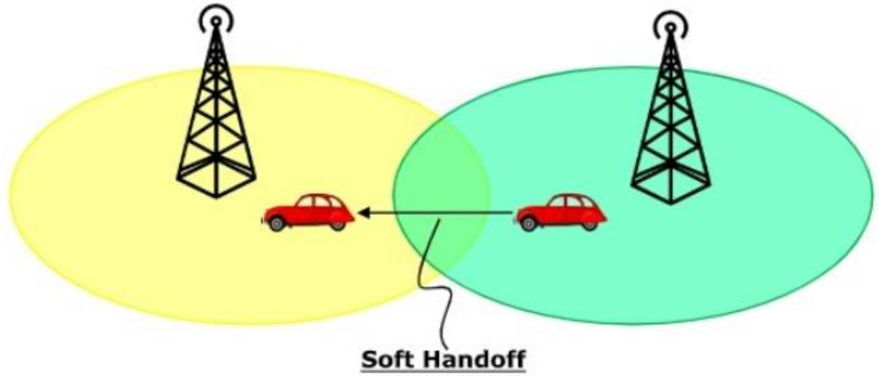
Handoff Scenarios

- If a subscriber who is in a call or a data session moves out of coverage of one cell and enters coverage area of another cell, a handoff is triggered for a continuum of service. The tasks that were being performed by the first cell are delineating to the latter cell.
- Each cell has a pre-defined capacity, i.e. it can handle only a specific number of subscribers. If the number of users using a particular cell reaches its maximum capacity, then a handoff occurs. Some of the calls are transferred to adjoining cells, provided that the subscriber is in the overlapping coverage area of both the cells.
- Cells are often sub-divided into microcells. A handoff may occur when there is a transfer of duties from the large cell to the smaller cell and vice versa. For example, there is a traveling user moving within the jurisdiction of a large cell. If the traveler stops, then the jurisdiction is transferred to a microcell to relieve the load on the large cell.
- Handoffs may also occur when there is an interference of calls using the same frequency for communication.

Types of Handoff

- **Hard Handoff** − In a hard handoff, an actual break in the connection occurs while switching from one cell to another. The radio links from the mobile station to the existing cell is broken before establishing a link with the next cell. It is generally an inter-frequency handoff. It is a "**break before make**" policy.
- **Soft Handoff** − In soft handoff, at least one of the links is kept when radio links are added and removed to the mobile station. This ensures that during the handoff, no break occurs. This is generally adopted in co-located sites. It is a "**make before break**" policy.



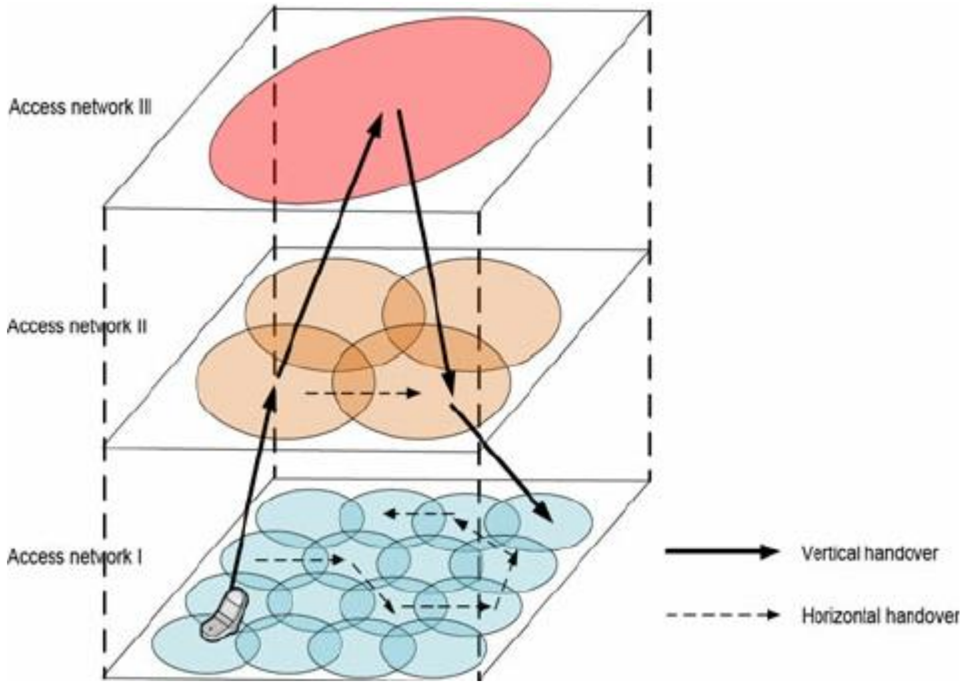


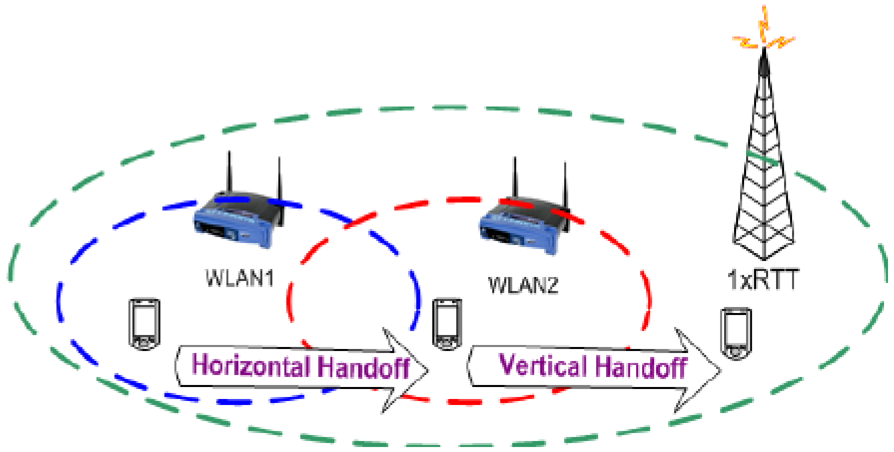
Mobile Assisted Handoff

- Mobile Assisted Handoff (MAHO) is a technique in which the mobile devices assist the Base Station Controller (BSC) to transfer a call to another BSC. It is used in GSM cellular networks. In other systems, like AMPS, a handoff is solely the job of the BSC and the Mobile Switching Centre (MSC), without any participation of the mobile device.

Handoff Types

- Depending on the movement of the mobile device, it may undergo various types of handoff. In a broad sense, handoffs may be of two types: (i) **intra-system handoff (horizontal handoff) and (ii) inter-system handoff (vertical handoff)**.
- Handover within same access networks (e.g., WLAN-to-WLAN) is referred to as horizontal handover or intra-domain handover,
- Handover across heterogeneous access networks (e.g., GSM-to- WiMAX) is referred to as the vertical or Inter-domain handover.





Factors Influencing Handoffs

- Transmitted power: as we know that the transmission power is different for different cells, the handoff threshold or the power margin varies from cell to cell.
- Received power: the received power mostly depends on the Line of Sight (LoS) path between the user and the BS. Especially when the user is on the boundary of the two cells, the LoS path plays a critical role in handoffs and therefore the power margin depends on the minimum received power value from cell to cell.
- Area and shape of the cell: Apart from the power levels, the cell structure also a plays an important role in the handoff process.
- Mobility of users: The number of mobile users entering or going out of a particular cell, also fixes the handoff strategy of a cell.

Wireless Transmission

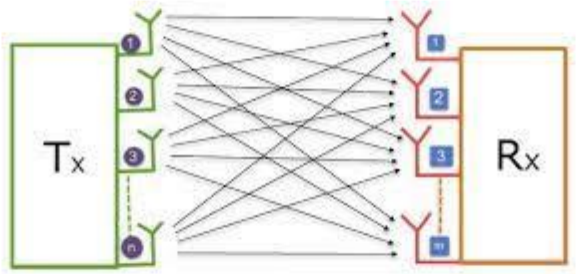
MIMO and OFDM

Wireless Transmission

- Introduction to MIMO;
  - MIMO Channel Capacity and diversity gain;
- Introduction to OFDM; MIMO-OFDM system;

MIMO

- Multiple-Input Multiple-Output (MIMO) is **a wireless technology that uses multiple transmitters and receivers to transfer more data at the same time.**
- All wireless products with 802.11n support MIMO. The technology helps allow 802.11n to reach higher speeds than products without 802.11n.
- an antenna technology for wireless communications in which multiple antennas are used at both the source (transmitter) and the destination (receiver).

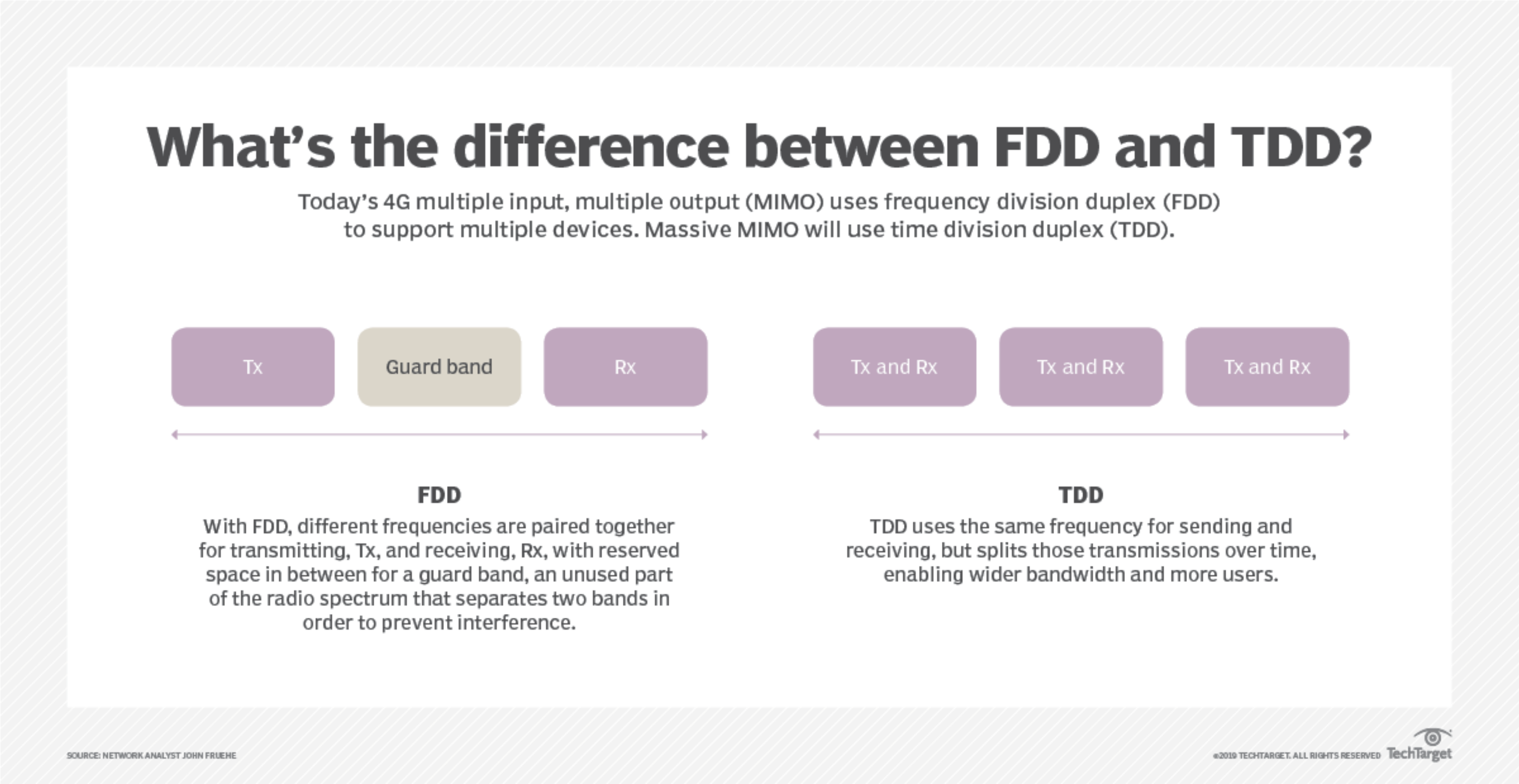


Basic Structure of a MIMO System

MIMO characteristics

- LTE uses MIMO and orthogonal frequency-division multiplexing (OFDM) to increase speeds up to 100 megabits per second (mbps) and beyond.
- These rates are double what was offered in previous 802.11a Wi-Fi.
- LTE uses MIMO for transmit diversity, spatial multiplexing (to transmit spatially separated independent channels), and single-user and multiuser systems.
- These massive 5G MIMO systems use numerous small antennas to boost bandwidth to users -- not just transmission rates as with third-generation (3G) and 4G cellular technology -- and support more users per antenna.
- Unlike 4G MIMO, which uses a frequency division duplex (FDD) system for supporting multiple devices,
- 5G massive MIMO uses a different setup called time division duplex (TDD). This offers numerous advantages over FDD (see image below).

FDD VS TDD

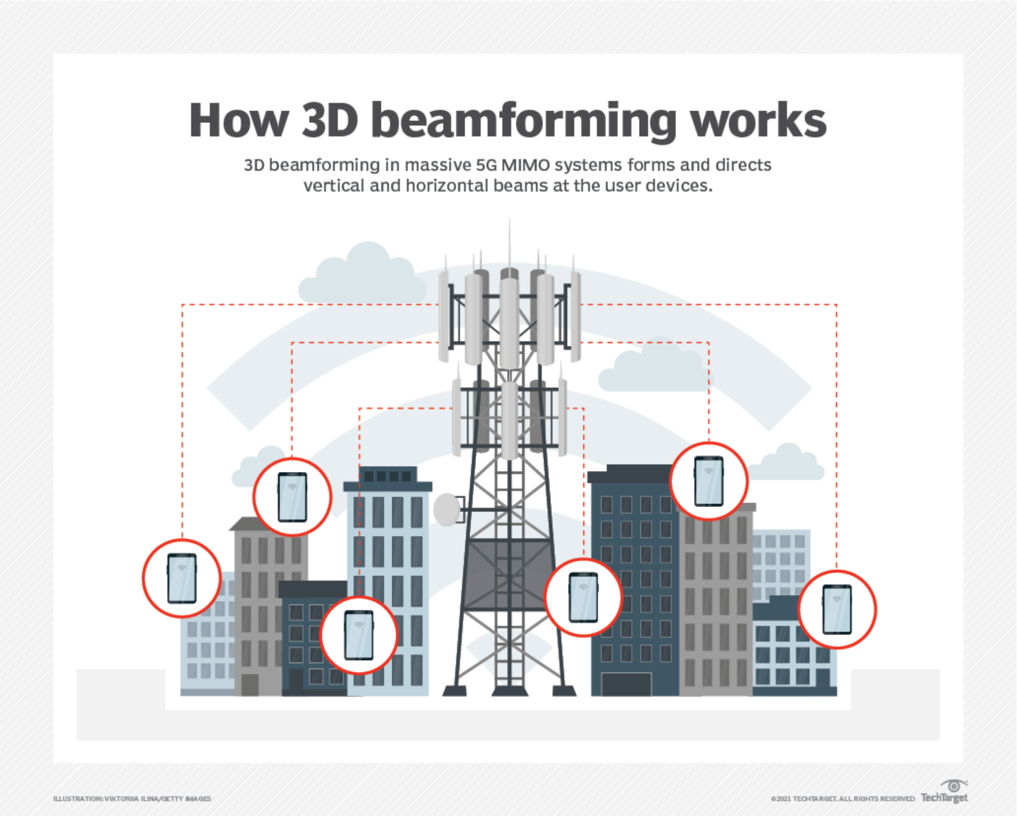

What's the difference between FDD and TDD?
Today's 4G multiple input, multiple output (MIMO) uses frequency division duplex (FDD) to support multiple devices. Massive MIMO will use time division duplex (TDD).
Tx
Guard band
Rx
Tx and Rx
Tx and Rx
Tx and Rx
FDD
With FDD, different frequencies are paired together for transmitting, Tx, and receiving, Rx, with reserved space in between for a guard band, an unused part of the radio spectrum that separates two bands in order to prevent interference.
TDD
TDD uses the same frequency for sending and receiving, but splits those transmissions over time, enabling wider bandwidth and more users.
SOURCE: NETWORK ANALYST JOHN FRUEHE
©2019 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

MIMO Beamforming

- Beamforming is an RF management technique that maximizes the signal power at the receiver by focusing broadcast data to specific users instead of a large area.
- With 5G, three-dimensional (3D) beamforming forms and directs vertical and horizontal beams at the user.
- These can reach devices even if they're at the top of a high-rise,

for example. The beams prevent interference with other wireless signals and stay with users as they move throughout a given area.

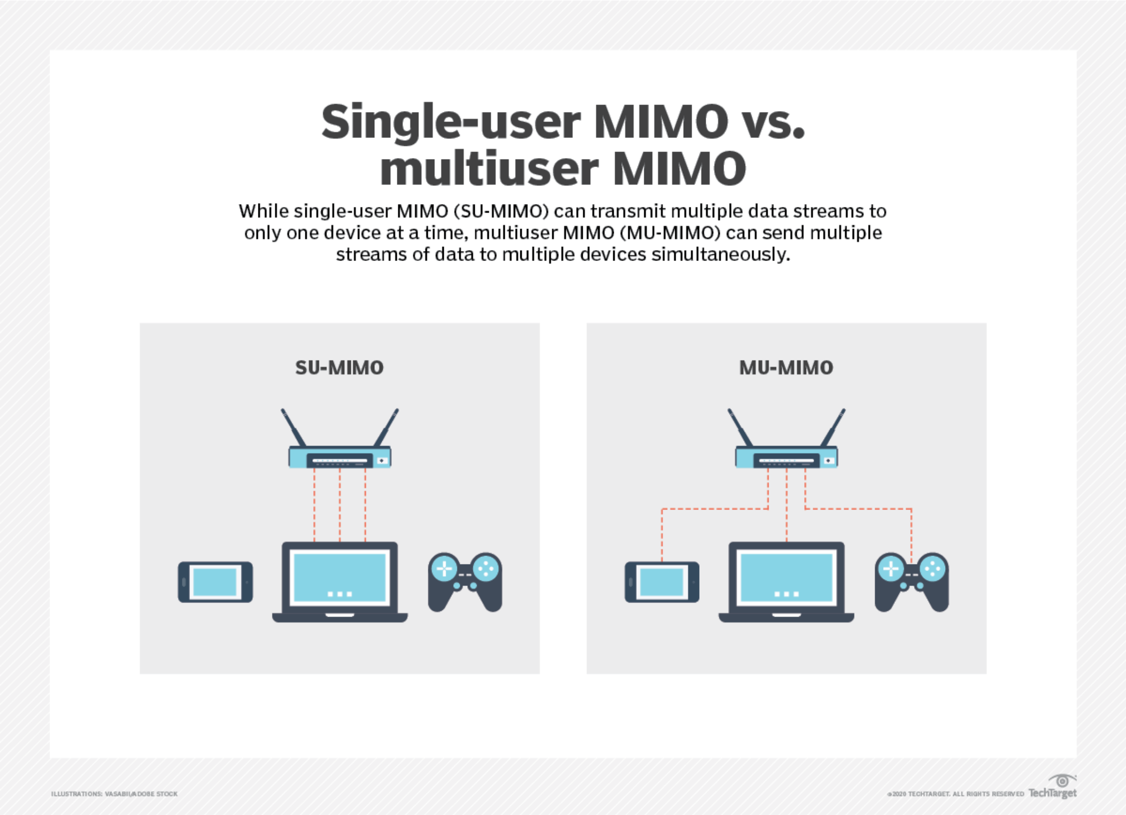
Beamforming in MIMO



Types of MIMO

- There are two primary types of MIMO: **single-user (SU) and multiuser (MU).**
- In SU-MIMO systems, data streams can only interact with one device on the network at a time. MU-MIMO systems, therefore, outperform SU-MIMO.
- Issues arise with SU-MIMO when many users attempt to use the network simultaneously. If one person is uploading video and another is conferencing, the data stream will choke, causing latency, or delays, to skyrocket.
- On the other end of the spectrum, MU-MIMO has the advantage of being able to stream multiple data sets to multiple devices at a time.

SU V/S MU MIMO



Single-user MIMO vs. multiuser MIMO
While single-user MIMO (SU-MIMO) can transmit multiple data streams to only one device at a time, multiuser MIMO (MU-MIMO) can send multiple streams of data to multiple devices simultaneously.
SU-MIMO
MU-MIMO
ILLUSTRATIONS: VASABII/ADOBE STOCK
©2020 TECHTARGET. ALL RIGHTS RESERVED

MIMO's primary advantages

- MIMO enables stronger signals. It bounces and reflects signals so a user device doesn't need to be in a clear line of sight.
- Video and other large-scale content can travel over a network in large quantities.
- This content travels more quickly because MIMO supports greater throughput.
- Many data streams improve visual and auditory quality. They also decrease the chance of lost data packets.

How massive MIMO systems are influencing the future

- MIMO is a primary tool for advancing all aspects of wireless communications. It plays a substantial role in 5G technology
- **High network capacities.** Data travels to more users through the deployment of 5G New Radio (5G NR). MU-MIMO and 5G NR enable more users to access data at the same frequency and time rates.
- **More coverage.** Users can soon expect high-speed data wherever they are, even at the edge of service areas. Using 3D beamforming, the coverage adapts to the user's movement and location.
- **Better user experience (UX).** Watching videos and uploading content is easier and faster. Massive MIMO and 5G technology transform UX.

MIMO Channel capacity

- In fading, capacity with both transmitter and receiver knowledge is the average of the capacity for the static channel, with power allocated either by an instantaneous or average power constraint.
- Under the instantaneous constraint power is optimally allocated over the spatial dimension only. Under the average constraint it is allocated over both space and time.

$$C = \min(M_t, M_r) B \log(1 + \rho).$$

capacity grows linearly with the size of the antenna arrays.

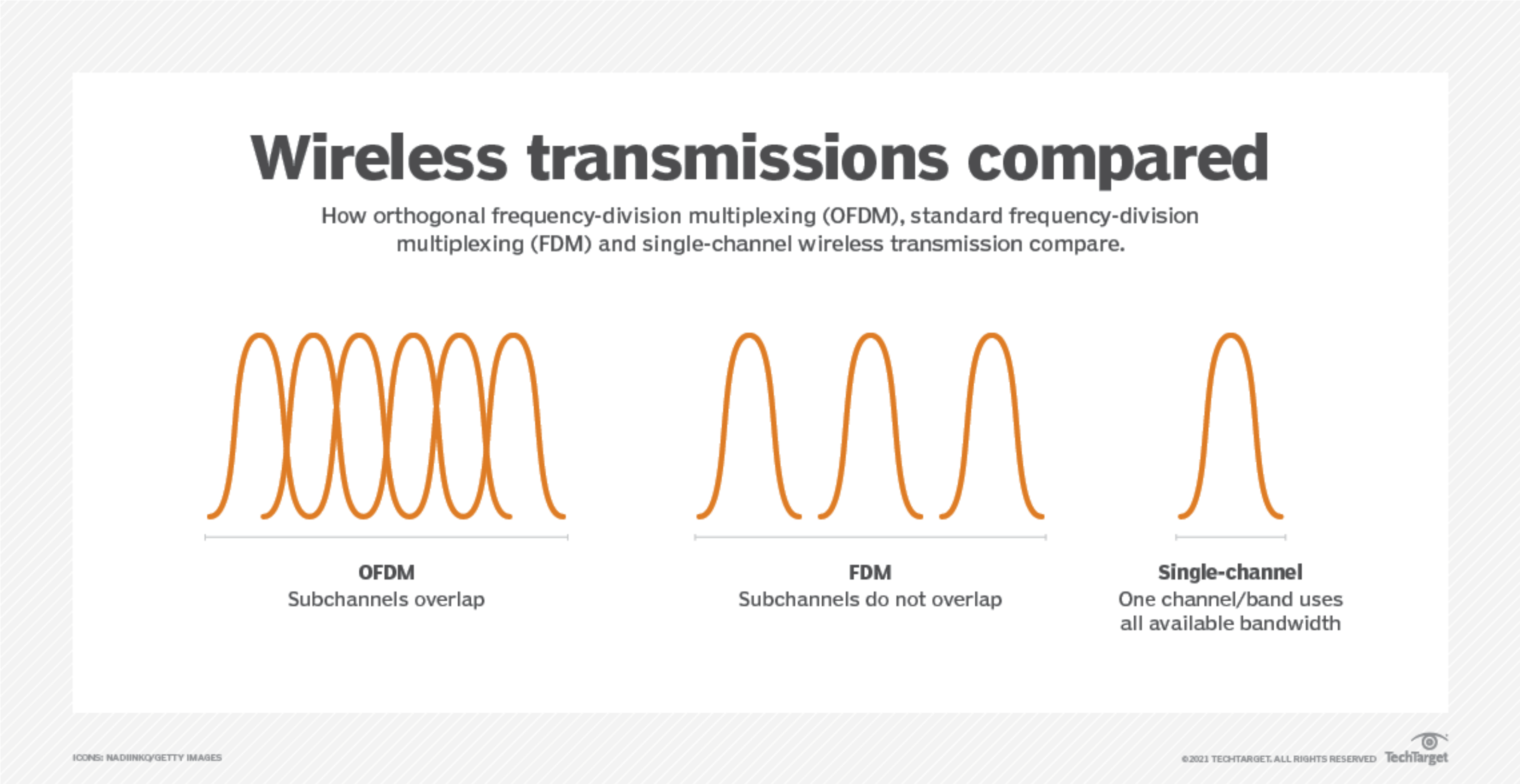
MIMO Diversity Gain

- Diversity gain is **the decreased required receive SNR for a given bit error rate (BER) averaged over the fading.**
- This is the reduction in fading margin that's obtained by reducing the fading with the smart antenna.

OFDM- Orthogonal frequency-division multiplexing

- method of data transmission where a single information stream is split among several closely spaced narrowband sub channel frequencies instead of a single Wideband channel frequency.
- It is mostly used in wireless data transmission but may be employed in wired and fiber optic communication as well.
- several bits can be sent in parallel, or at the same time, in separate substream channels.
- This enables each substream's data rate to be lower than would be required by a single stream of similar bandwidth.
- This makes the system less susceptible to interference and enables more efficient data bandwidth.

OFDM V/S FDM



Wireless transmissions compared
How orthogonal frequency-division multiplexing (OFDM), standard frequency-division multiplexing (FDM) and single-channel wireless transmission compare.
OFDM
Subchannels overlap
FDM
Subchannels do not overlap
Single-channel
One channel/band uses all available bandwidth
ICONS: NADIINKO/GETTY IMAGES
©2021 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

Working of OFDM

- In the traditional stream, each bit might be represented by a 1 nanosecond segment of the signal, with 0.25 ns spacing between bits, for example.
- Using OFDM to split the signal across four component streams lets each bit be represented by 4 ns of the signal with 1 ns spacing between.
- The overall data rate is the same, 4 bits every 5 ns, but the signal integrity is higher.

OFDM VS FDM

- OFDM builds on simpler frequency-division multiplexing (FDM).
- In FDM, the total data stream is divided into several subchannels, but the frequencies of the subchannels are spaced farther apart so they do not overlap or interfere.
- With OFDM, the subchannel frequencies are close together and overlapping but are still orthogonal, or separate, in that they are carefully chosen and modulated so that the interference between the subchannels is canceled out.

Advantages

- Primarily, OFDM is more resilient to electromagnetic interference, and it enables more efficient use of total available bandwidth because the subchannels are closely spaced. It is also more resistant to interference because several channels are available.
- Advanced error correction can be used to spread out the overall data and compensate for small errors. So, narrowband interference on a single subchannel will not affect the other channels, enabling the overall system to still operate.
- Frequency-selective interference fading due to multipath echo effects can also be corrected. The lower data rate on the individual subchannels enables guard intervals to be used between symbols, which eliminates intersymbol interference and helps with multipath errors.

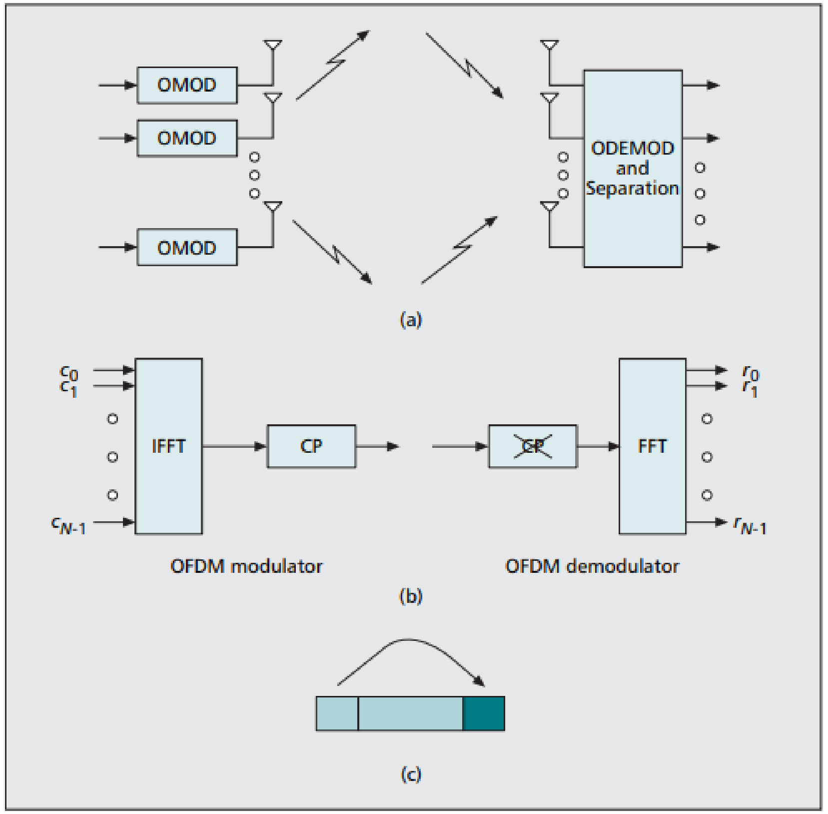
Disadvantages of OFDM

- OFDM systems must have closely tuned transmitters and receivers. This requires the timing on signal modulators and demodulators be closely matched and produced to tight tolerances.

Applications of OFDM

- Digital radio, Digital Radio Mondiale, and digital audio broadcasting and satellite radio.
- Digital television standards, Digital Video Broadcasting-Terrestrial/Handheld (DVB-T/H), DVB-Cable 2 (DVB-C2). OFDM is not used in the current U.S. digital television Advanced Television Systems Committee standard, but it is used in the future 4K/8K-capable ATSC 3.0 standard.
- Wired data transmission, Asymmetric Digital Subscriber Line (ADSL), Institute of Electrical and Electronics Engineers (IEEE) 1901 powerline networking, cable internet providers. Fiber optic transmission may use either OFDM signals or several distinct frequencies as FDM.
- Wireless LAN (WLAN) data transmission. All Wi-Fi systems use OFDM, including IEEE 802.11a/b/g/n/ac/ax. The addition of OFDMA to the Wi-Fi 6/802.11ax standard enables more devices to use the same base station simultaneously. OFDM is also used in metropolitan area network (MAN) IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX>) installations.
- Cellular data. Long-Term Evolution (LTE) and 4G cellphone networks use OFDM. It is also an integral part of 5G NR cellular deployments.

MIMO OFDM System



MIMO technology will predominantly be used in broadband systems that exhibit frequency-selective fading and, therefore, intersymbol interference (ISI).
OFDM modulation turns the frequency-selective channel into a set of parallel flat fading channels and is, hence, an attractive way of coping with ISI.

MIMO Wireless technology in combination with orthogonal frequency division multiplexing (MIMOOFDM) is an attractive air-interface solution for next-generation wireless local area networks (WLANs), wireless metropolitan area networks (WMANs), and fourth-generation mobile cellular wireless systems.

Unit 3
Wireless Transmission Fundamentals

Preeti Godabole

Topics

- Introduction to narrow and wideband systems;
- Spread spectrum;
- Frequency hopping;
- Introduction to MIMO;
  - MIMO Channel Capacity and diversity gain;
- Introduction to OFDM; MIMO-OFDM system;
- Multiple access control (FDMA, TDMA, CDMA, SDMA);
- **Wireless local area network;**
- Wireless personal area network (Bluetooth and ZigBee)

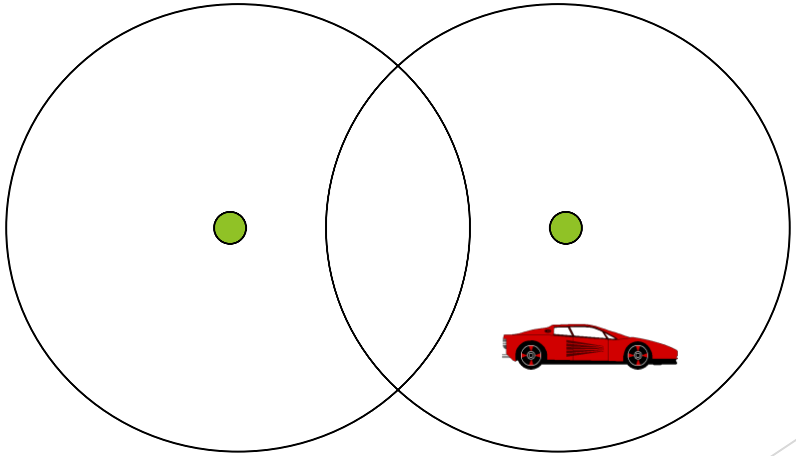
Goal of WLANs is to replace office cabling, to enable tetherless access to the internet and, to introduce a higher flexibility for ad-hoc communication in, e.g., group meetings.

Wireless networks

- Access computing/communication services, on the move
- Cellular Networks
  - traditional base station infrastructure systems
- Wireless LANs
  - infrastructure as well as ad-hoc networks possible
  - very flexible within the reception area
  - low bandwidth compared to wired networks (1-10 Mbit/s)
- Multihop Ad hoc Networks
  - useful when infrastructure not available, impractical, or expensive
  - military applications, rescue, home networking

Cellular Wireless

- Single hop wireless connectivity to the wired world
  - Space divided into cells, and hosts assigned to a cell
  - A base station is responsible for communicating with hosts/nodes in its cell
  - Mobile hosts can change cells while communicating
  - Hand-off occurs when a mobile host starts communicating via a new base station



Evolution of cellular networks

- First-generation: Analog cellular systems (450-900 MHz)
  - Frequency shift keying; FDMA for spectrum sharing
  - NMT (Europe), AMPS (US)
- Second-generation: Digital cellular systems (900, 1800 MHz)
  - TDMA/CDMA for spectrum sharing; Circuit switching
  - GSM (Europe), IS-136 (US), PDC (Japan)
  - <9.6kbps data rates
- 2.5G: Packet switching extensions
  - Digital: GSM to GPRS; Analog: AMPS to CDPD
  - <115kbps data rates
- 3G: Full-fledged data services
  - High speed, data and Internet services
  - IMT-2000, UMTS
  - <2Mbps data rates

Characteristics of wireless LANs

Advantages

- very flexible within the reception area
- Ad-hoc networks without previous planning possible
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...

Disadvantages

- typically very low bandwidth compared to wired networks (1-10 Mbit/s)
- many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11)
- products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions like, e.g., IMT-2000
- safety and security -may interfere with the equipments , eavesdropping much easier

Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary

Comparison: infrared vs. radio transmission

- **Infrared**
- uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)

Advantages

- simple, cheap, available in many mobile devices
- no licenses needed
- simple shielding possible

Disadvantages

- interference by sunlight, heat sources etc.
- many things shield or absorb IR light
- low bandwidth
- Example
- IrDA (Infrared Data Association) interface available everywhere

- **Radio**
- typically using the license free ISM band at 2.4 GHz

Advantages

- experience from wireless WAN and mobile phones can be used
- coverage of larger areas possible (radio can penetrate walls, furniture etc.)

Disadvantages

- very limited license free frequency bands
- shielding more difficult, interference with other electrical devices
- Example
- WaveLAN, HIPERLAN, Bluetooth

Wireless LANs

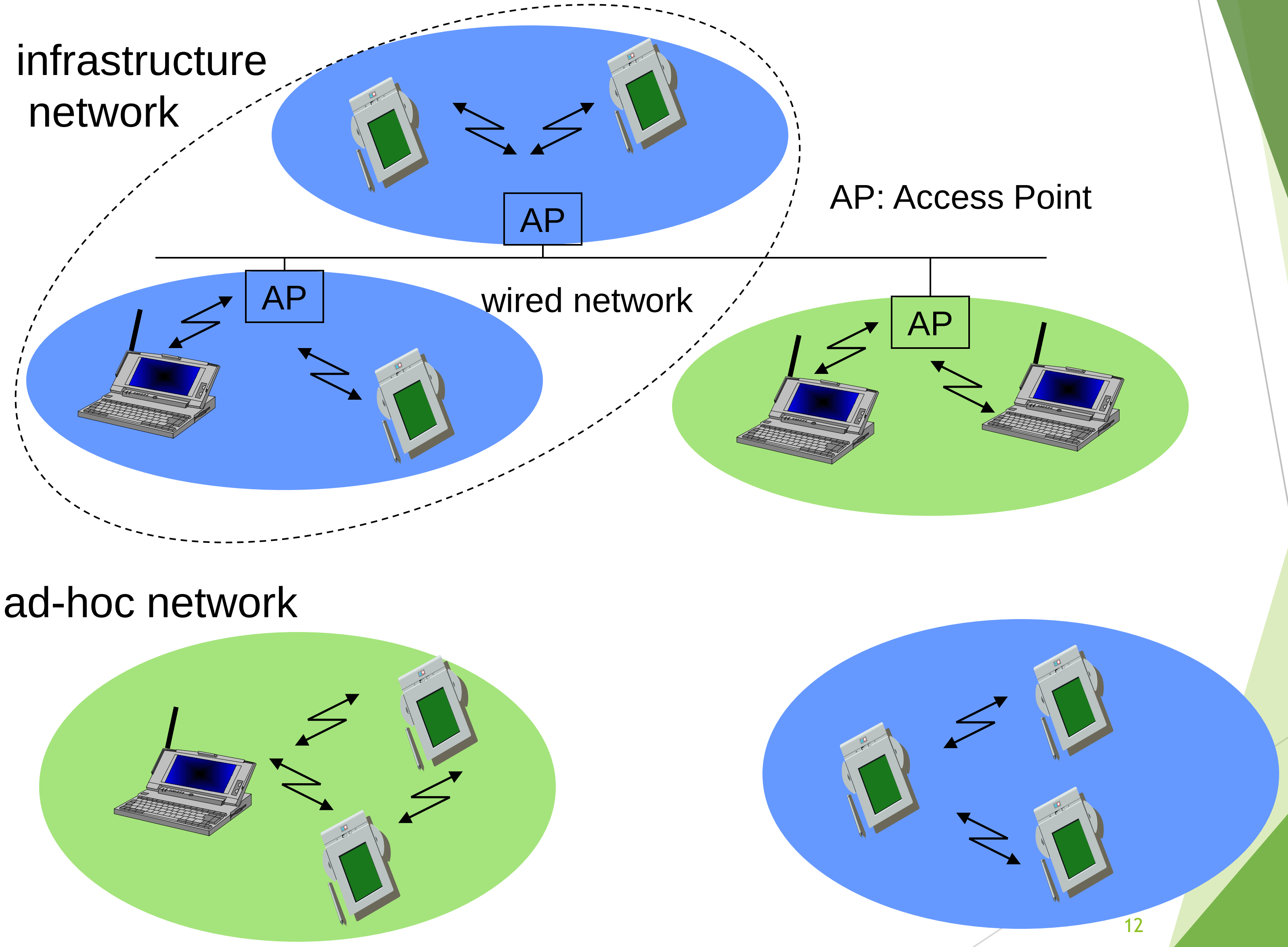
- Infrared (IrDA) or radio links (Wavelan)

- Advantages
  - very flexible within the reception area
  - Ad-hoc networks possible
  - (almost) no wiring difficulties
- Disadvantages
  - low bandwidth compared to wired networks
  - many proprietary solutions
    - Bluetooth, HiperLAN and IEEE 802.11

Wireless LANs vs. Wired LANs

- Destination address does not equal destination location
- The media impact the design
- wireless LANs intended to cover reasonable geographic distances must be built from basic coverage blocks
- Impact of handling mobile (and portable) stations
- Propagation effects
- Mobility management
- Power management

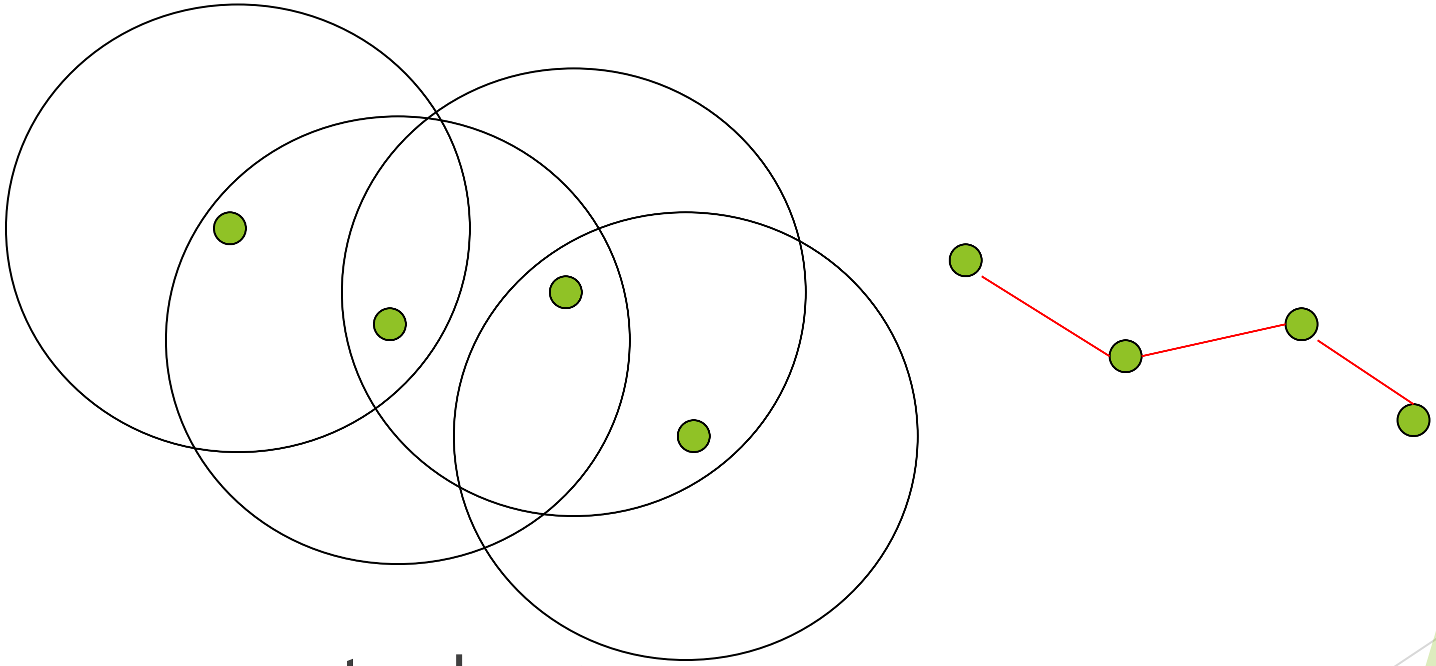
Infrastructure vs. Ad hoc WLANs



Source: Schiller

Multi-Hop Wireless

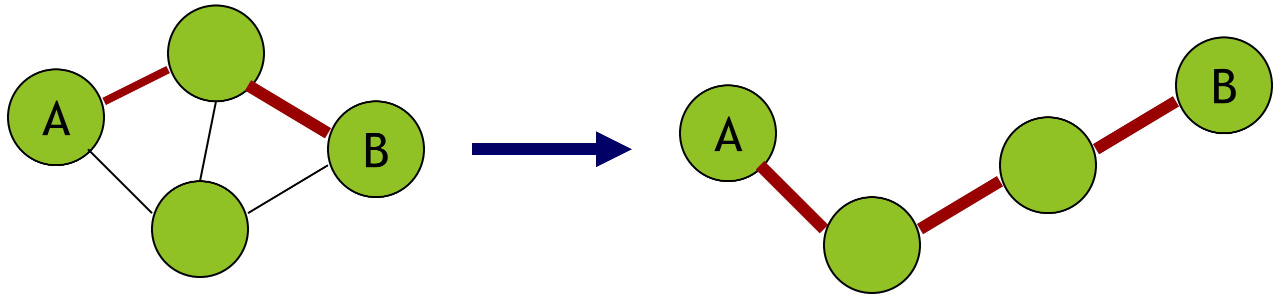
- May need to traverse multiple links to reach destination



- Mobility causes route changes

Mobile Ad Hoc Networks (MANET)

- Do not need backbone infrastructure support
- Host movement frequent
- Topology change frequent

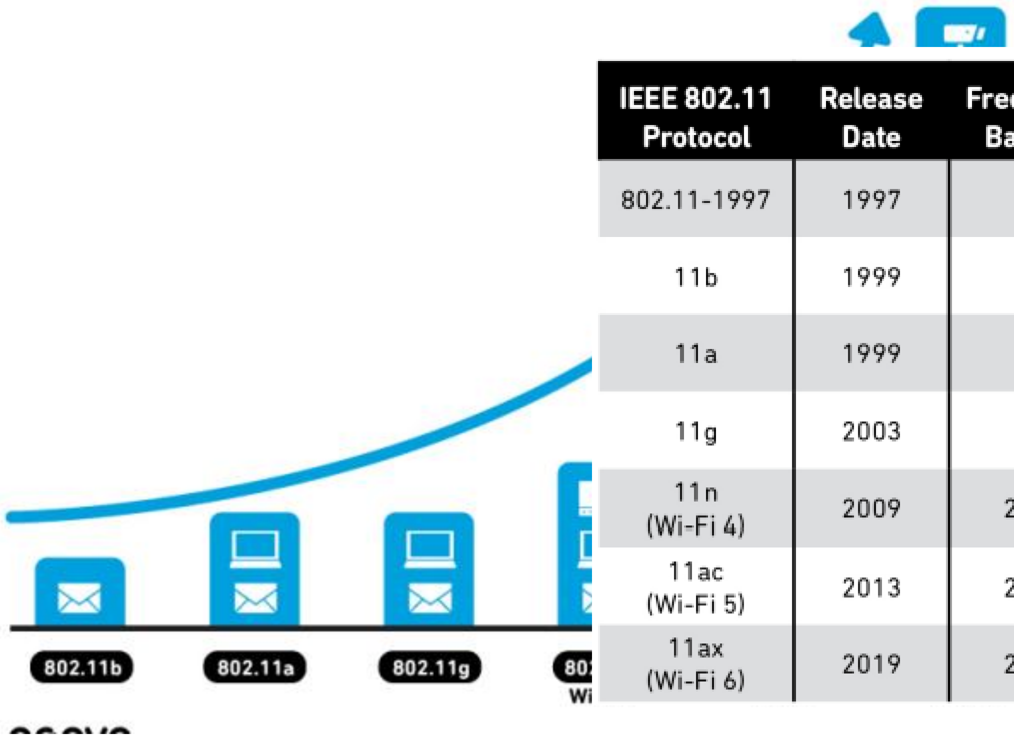


- Multi-hop wireless links
- Data must be routed via intermediate nodes

Applications of MANETS

- Military - soldiers at Kargil, tanks, planes
- Disaster Management – Orissa, Gujarat
- Emergency operations – search-and-rescue, police and firefighters
- Sensor networks
- Taxicabs and other closed communities
- airports, sports stadiums etc. where two or more people meet and want to exchange documents
- Presently MANET applications use 802.11 hardware
- Personal area networks - Bluetooth

Wireless Lan 802.11 Evolution



IEEE 802.11 Protocol	Release Date	Frequency Band(s)	Bandwidth	Max Throughput
802.11-1997	1997	2.4	22	2 Mbps
11b	1999	2.4	22	11 Mbps
11a	1999	5	20	54 Mbps
11g	2003	2.4	20	54 Mbps
11n (Wi-Fi 4)	2009	2.4/5	20/40	600 Mbps
11ac (Wi-Fi 5)	2013	2.4/5	20/40/ 80/160	6.8 Gbps
11ax (Wi-Fi 6)	2019	2.5/5	20/40/ 80/160	10 Gbps

Challenges of Wireless Communications

Wireless Media

- Physical layers used in wireless networks

- have neither absolute nor readily observable boundaries outside which stations are unable to receive frames are unprotected from outside signals
- communicate over a medium significantly less reliable than the cable of a wired network
- have dynamic topologies
- lack full connectivity and therefore the assumption normally made that every station can hear every other station in a LAN is invalid (i.e., STAs may be "hidden" from each other)
- have time varying and asymmetric propagation properties

Limitations of the mobile environment

- Limitations of the Wireless *Network*
- limited communication bandwidth
- frequent disconnections
- heterogeneity of fragmented networks

- Limitations Imposed by *Mobility*
- route breakages
- lack of mobility awareness by system/applications

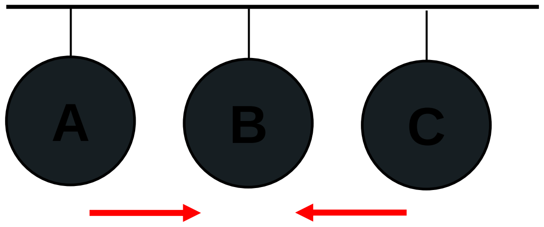
- Limitations of the Mobile *Device*
- short battery lifetime
- limited capacities

Wireless v/s Wired networks

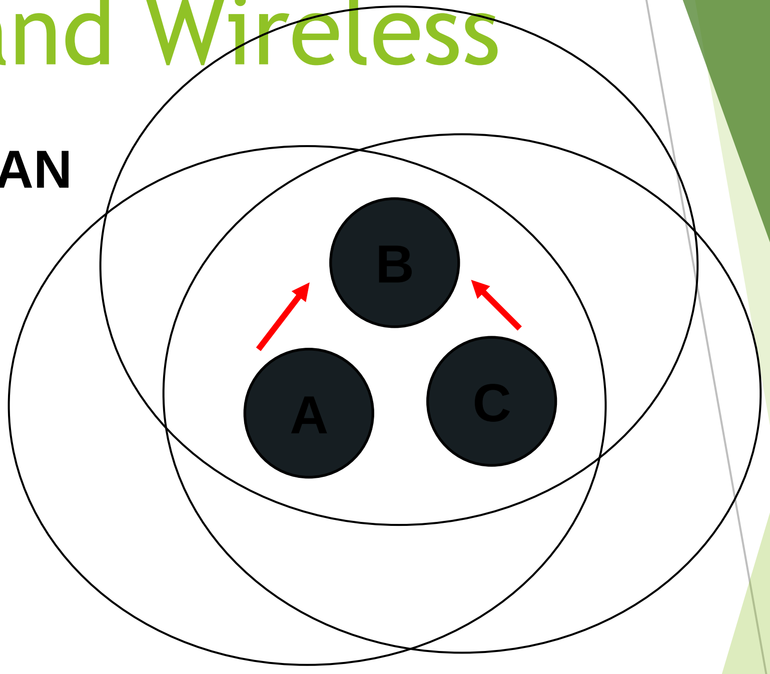
- Regulations of frequencies
  - Limited availability, coordination is required
  - useful frequencies are almost all occupied
- Bandwidth and delays
  - Low transmission rates
    - few Kbps to some Mbps.
  - Higher delays
    - several hundred milliseconds
  - Higher loss rates
    - susceptible to interference, e.g., engines, lightning
- Always shared medium
  - Lower security, simpler active attacking
  - radio interface accessible for everyone
  - Fake base stations can attract calls from mobile phones
  - secure access mechanisms important

Difference Between Wired and Wireless

Ethernet LAN



Wireless LAN



- If both A and C sense the channel to be idle at the same time, they send at the same time.
- Collision can be detected *at sender* in Ethernet.
- Half-duplex radios in wireless cannot detect collision at sender.

Effect of mobility on protocol stack

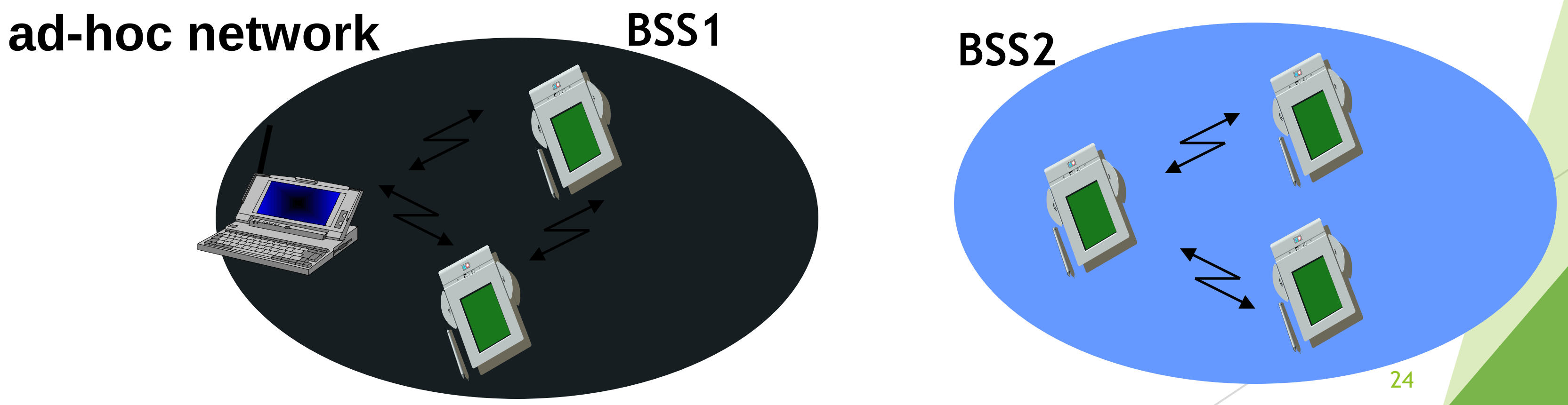
- Application
  - new applications and adaptations
- Transport
  - congestion and flow control
- Network
  - addressing and routing
- Link
  - media access and handoff
- Physical
  - transmission errors and interference

802.11-based Wireless LANs Architecture and Physical Layer

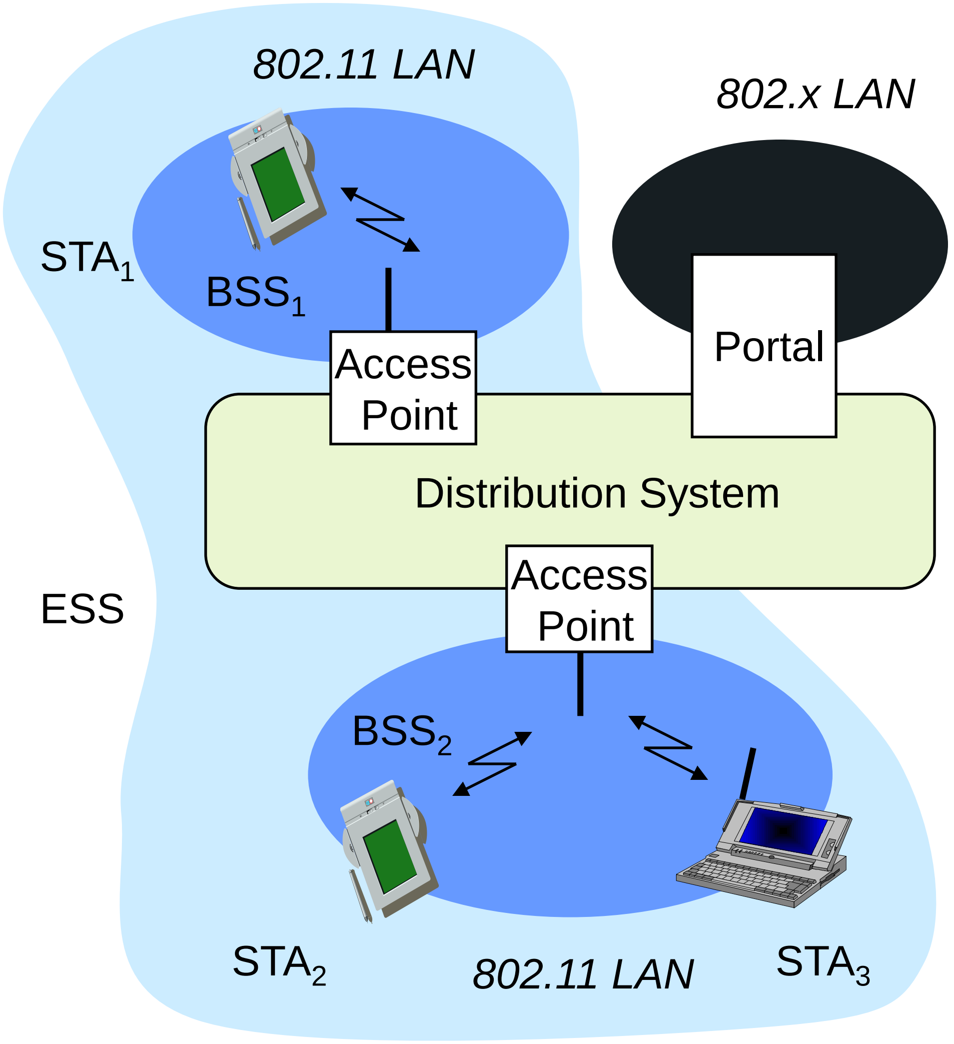
The **primary goal** of the standard was the specification of a simple and robust WLAN which offers time-bounded and asynchronous services. The MAC layer should be able to operate with multiple physical layers, each of which exhibits a different medium sense and transmission characteristic

Components of IEEE 802.11 architecture

- The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN
- The ovals can be thought of as the coverage area within which member stations can directly communicate
- The Independent BSS (IBSS) is the simplest LAN. It may consist of as few as two stations



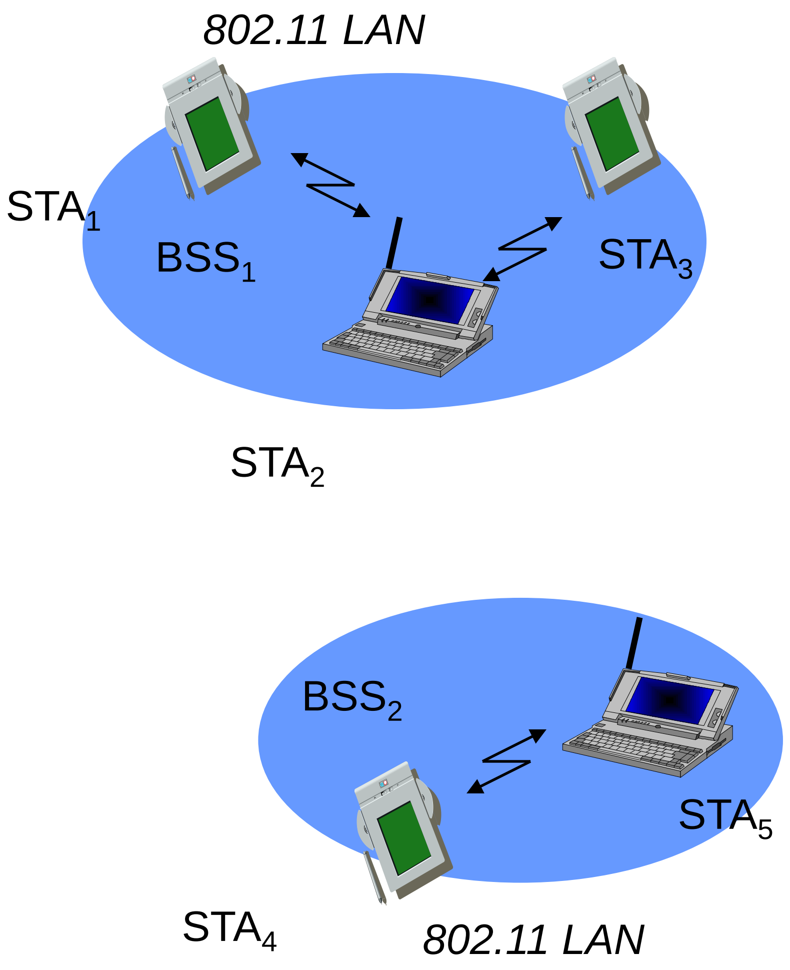
802.11 - infrastructure network



- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system Portal bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

Source: Schiller

802.11 - ad-hoc network



- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - Basic Service Set (BSS): group of stations using the same radio frequency

Source: Schiller

Distribution System (DS) concepts

- The Distribution system interconnects multiple BSSs
- 802.11 standard logically separates the wireless medium from the distribution system – it does not preclude, nor demand, that the multiple media be same or different
- An Access Point (AP) is a STA that provides access to the DS by providing DS services in addition to acting as a STA.
- Data moves between BSS and the DS via an AP
- The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity called the Extended Service Set network (ESS)

Extended Service Set network

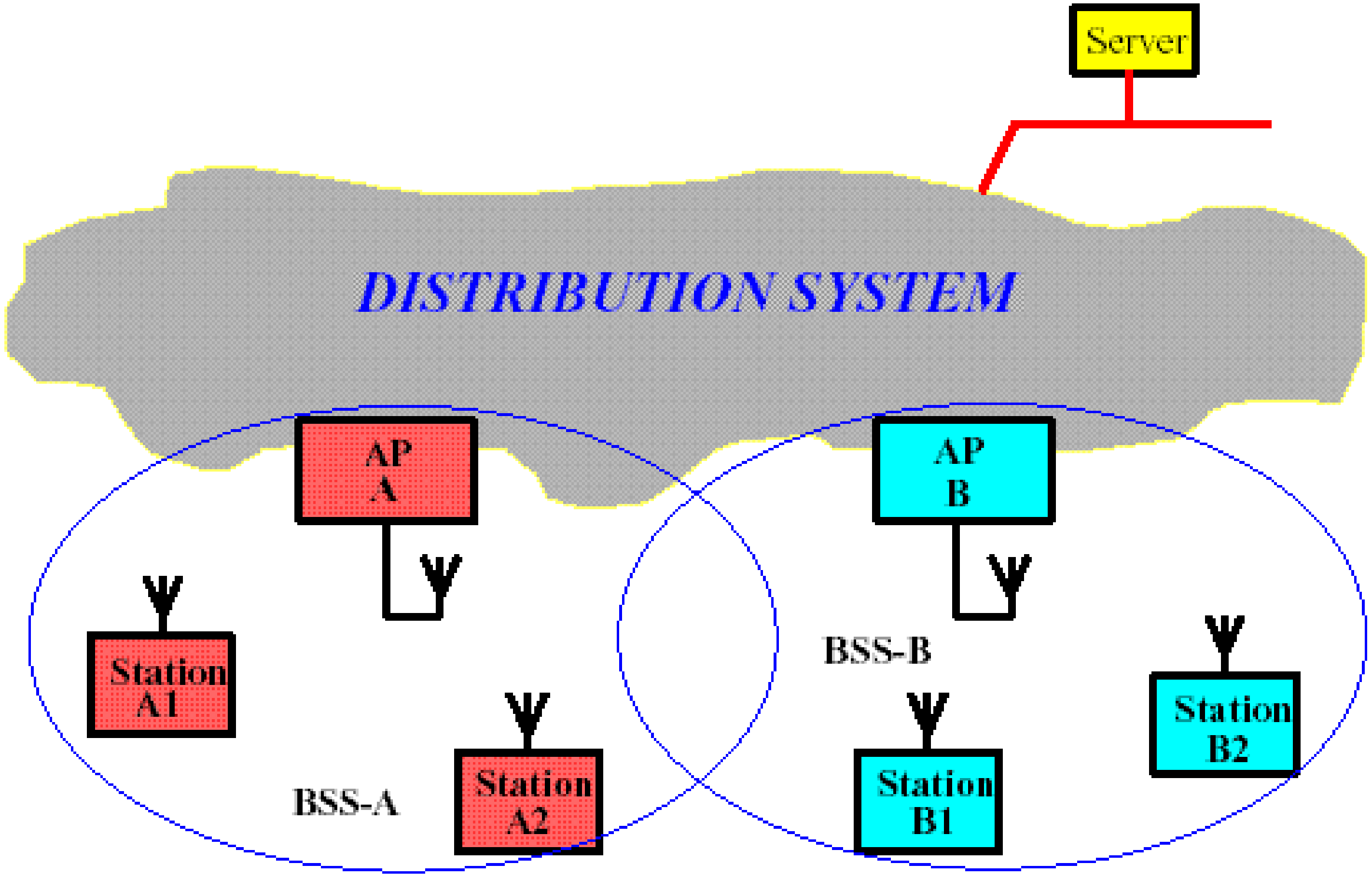
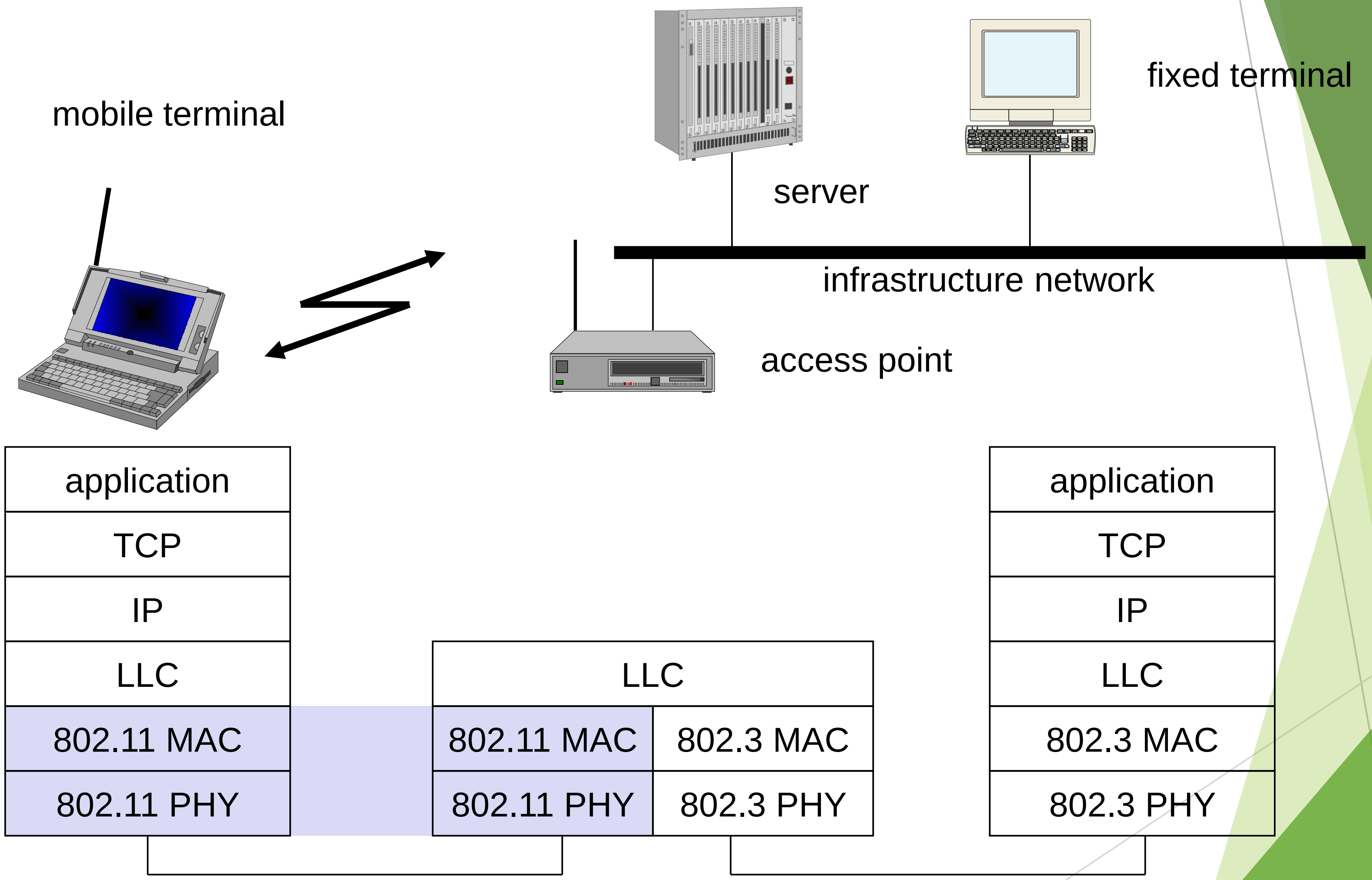


Figure 2 ESS Provides Campus-Wide Coverage

Source: Intersil

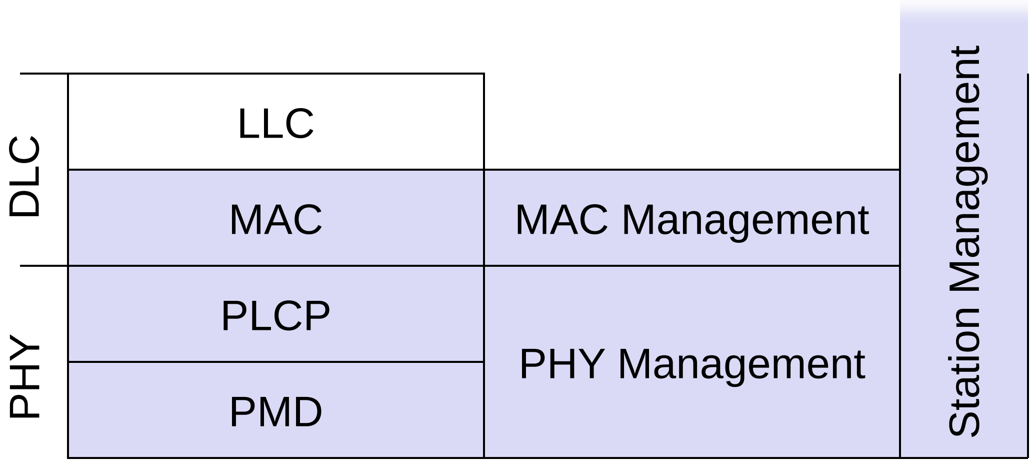
802.11- in the TCP/IP stack



802.11 - Layers and functions

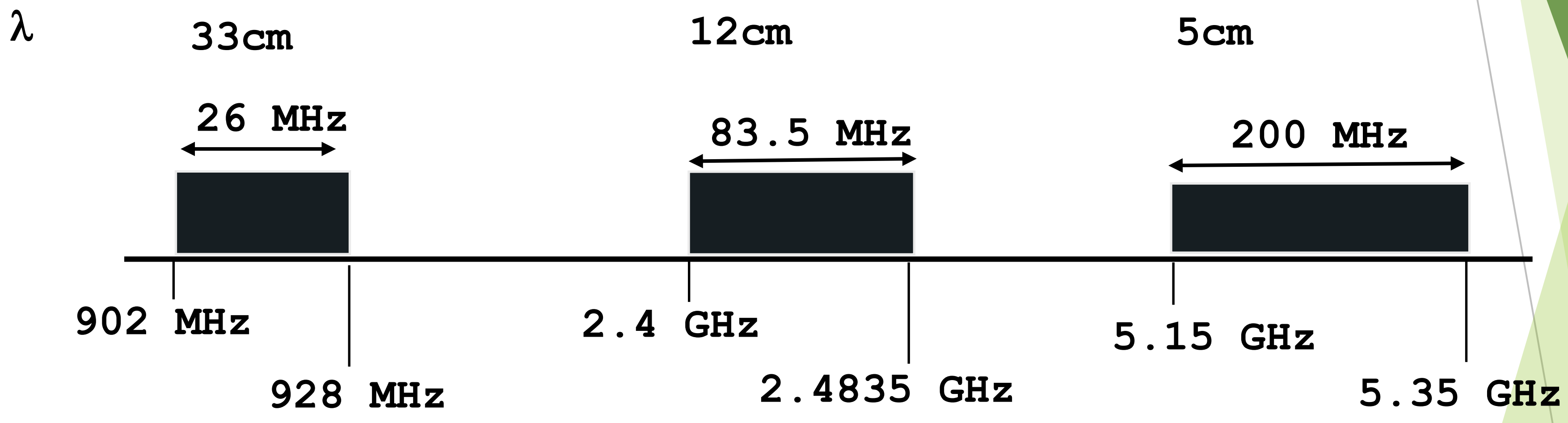
- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management

- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD
- Physical Medium Dependent modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions



IEEE 802.11

- Wireless LAN standard defined in the unlicensed spectrum (2.4 GHz and 5 GHz U-NII bands)



- Standards covers the MAC sublayer and PHY layers
- Three different physical layers in the 2.4 GHz band
  - FHSS, DSSS and IR
- OFDM based Phys layer in the 5 GHz band (802.11a)

802.11 - Physical layer

- All PHY variants include the provision of the clear channel assessment signal (CCA). This is needed for the MAC mechanisms controlling medium access and indicates if the medium is currently idle
- The PHY layer offers a service access point (SAP) with 1 or 2 Mbit/s transfer

  rate to the MAC layer (basic version of the standard).

3 versions of spread spectrum:

2 radio (typ. 2.4 GHz),

1 IR data rates 1 or 2 Mbps

1.FHSS (Frequency Hopping Spread Spectrum)

- spreading, despreading, signal strength, typically 1 Mbps min. 2.5 frequency hops/s (USA), two-level GFSK modulation

FHSS PHY packet format

$s(z): z^7+z^4+1$

- Synchronization

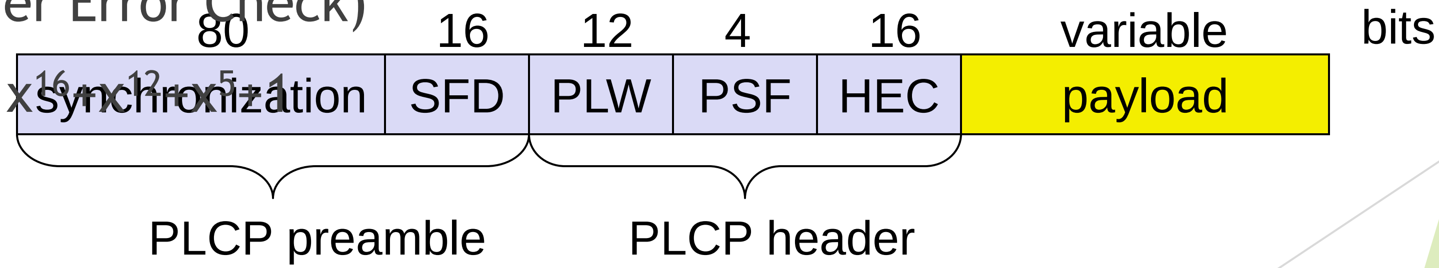
  synch with 010101... pattern
- SFD (Start Frame Delimiter)

  0000110010111101 start pattern
- PLW (PLCP_PDU Length Word)

  length of payload incl. 32 bit CRC of payload, PLW < 4096
- PSF (PLCP Signaling Field)

  data of payload (1 or 2 Mbit/s)
- HEC (Header Error Check)

  CRC with $x^{16}+x^{12}+x^5+1$



2.DSSS (Direct Sequence Spread Spectrum)

- DBPSK modulation for 1 Mbps (Differential Binary Phase Shift Keying), DQPSK for 2 Mbps (Differential Quadrature PSK)
- preamble and header of a frame is always transmitted with 1 Mbps, rest of transmission 1 or 2 Mbps
- chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

3.Infrared

- 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchronization

DSSS PHY packet format

- Synchronization

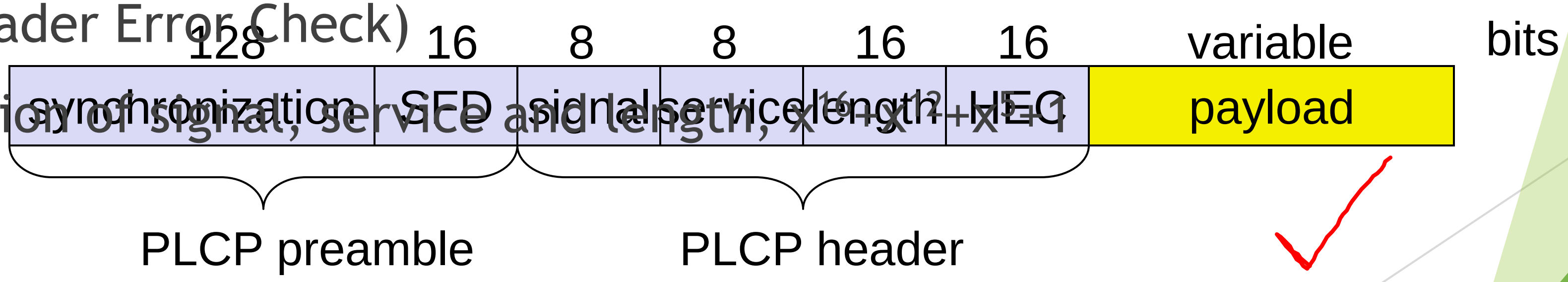
  synch., gain setting, energy detection, frequency offset compensation
- SFD (Start Frame Delimiter)

  1111001110100000
- Signal

  data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service Length

  future use, 00: 802.11 compliant length of the payload
- HEC (Header Error Check)

  protection of signal, service and length, $x^{16}+x^{12}+x^5+1$



Hardware

- Original WaveLAN card (NCR)
  - 914 MHz Radio Frequency
  - Transmit power 281.8 mW
  - Transmission Range ~250 m (outdoors) at 2Mbps
  - SNRT 10 dB (capture)
- WaveLAN II (Lucent)
  - 2.4 GHz radio frequency range
  - Transmit Power 30mW
  - Transmission range 376 m (outdoors) at 2 Mbps (60m indoors)
  - Receive Threshold = - 81dBm
  - Carrier Sense Threshold = -111dBm
- Many others….Agere, Cisco,………

802.11-based Wireless LANs MAC functional spec - DCF

802.11 - MAC layer I - DFWMAC

Traffic services

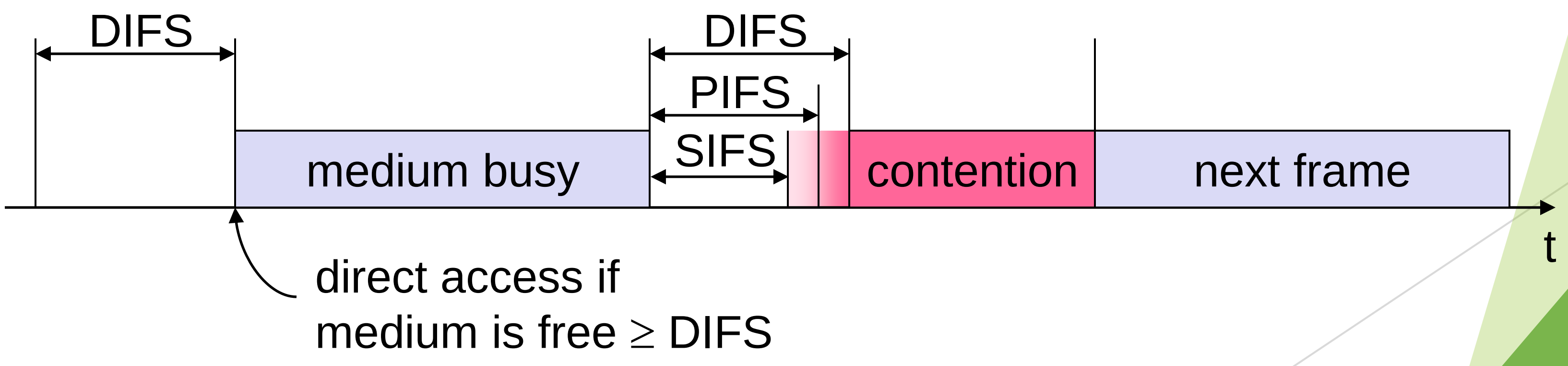
- Asynchronous Data Service (mandatory)
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - implemented using PCF (Point Coordination Function)

Access methods

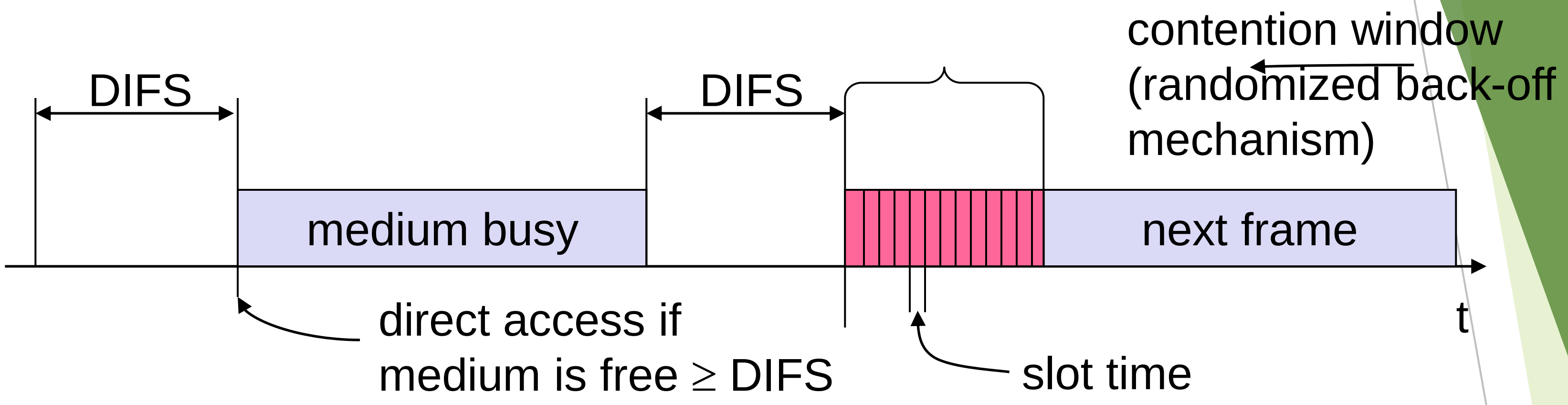
- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DFWMAC-DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem
- DFWMAC- PCF (optional)
  - access point polls terminals according to a list

802.11 - MAC layer II

- Priorities
  - defined through different inter frame spaces
  - no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  - lowest priority, for asynchronous data service



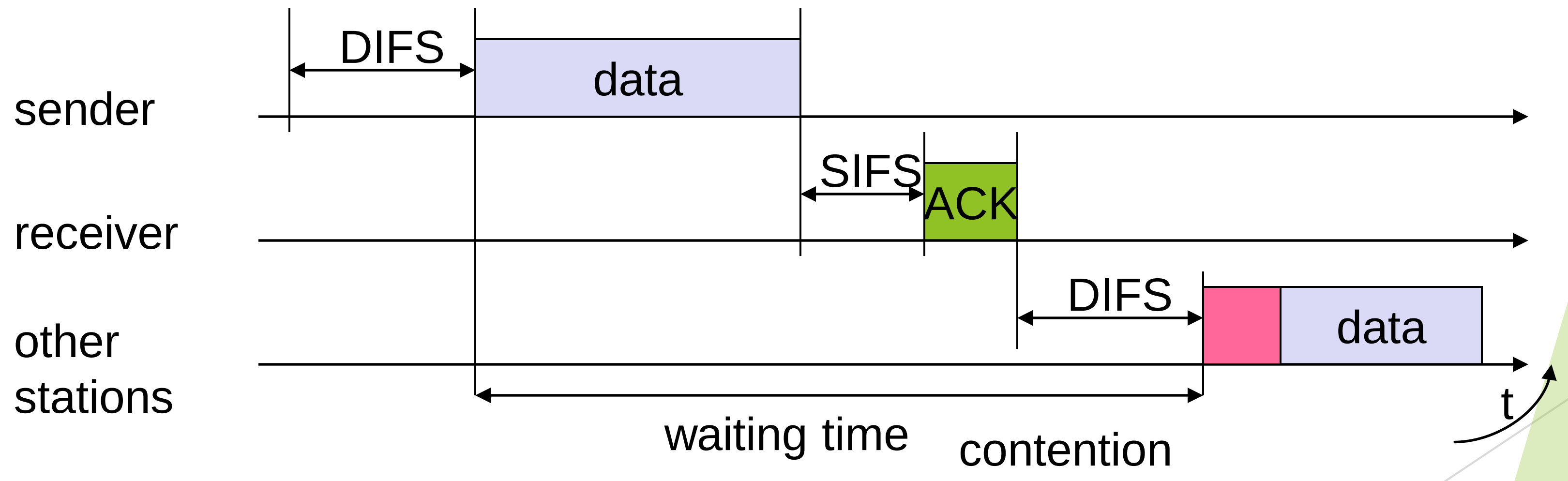
802.11 - CSMA/CA access method I



- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

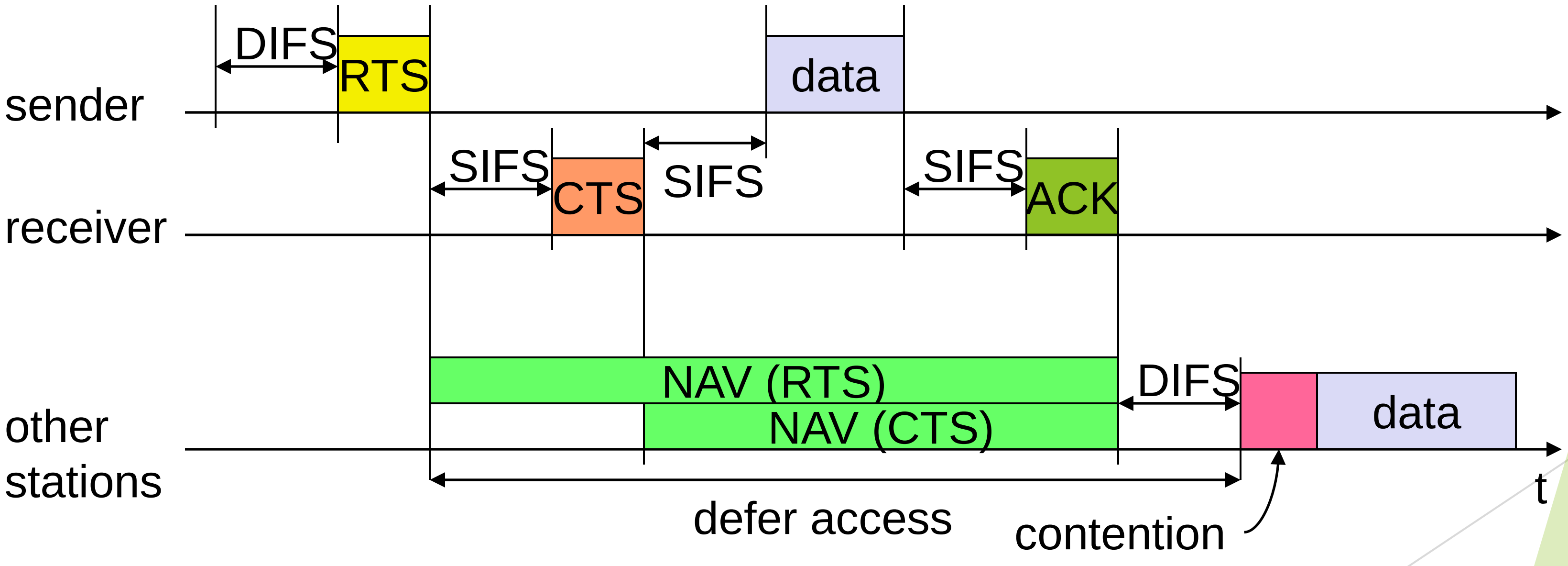
802.11 - CSMA/CA access method II

- Sending unicast packets
- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors



802.11 - DFWMAC

- Sending unicast packets
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS



802.11 - Carrier Sensing

- **In IEEE 802.11, carrier sensing is performed**
  - at the air interface (*physical carrier sensing*), and
  - at the MAC layer (*virtual carrier sensing*)
- **Physical carrier sensing**
  - detects presence of other users by analyzing all detected packets
  - Detects activity in the channel via relative signal strength from other sources
- **Virtual carrier sensing** is done by sending MPDU duration information in the header of RTS/CTS and data frames
- Channel is busy if **either** mechanisms indicate it to be
- Duration field indicates the amount of time (in microseconds) required to complete frame transmission
- Stations in the BSS use the information in the duration field to adjust their network allocation vector (NAV)

802.11 - Collision Avoidance

- If medium is not free during DIFS time..
- Go into Collision Avoidance: Once channel becomes idle, wait for DIFS time plus a randomly chosen backoff time before attempting to transmit
- For DCF the backoff is chosen as follows:
  - When first transmitting a packet, choose a backoff interval in the range [0,cw]; cw is contention window, nominally 31
  - Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - When backoff interval reaches 0, transmit RTS
  - If collision, then double the cw up to a maximum of 1024
- Time spent counting down backoff intervals is part of MAC overhead

802.11 - Congestion Control

- Contention window (cw) in DCF: Congestion control achieved by dynamically choosing cw
- *large* cw leads to larger backoff intervals
- *small* cw leads to larger number of collisions

- Binary Exponential Backoff in DCF:
  - When a node fails to receive CTS in response to its RTS, it increases the contention window
    - cw is doubled (up to a bound cwmax =1023)
  - Upon successful completion data transfer, restore cw to cwmin=31

802.11 - Frame format

- Types
  - control frames, management frames, data frames
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  - sending time, checksum, frame control, data

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

version, type, fragmentation, security, ...

Types of Frames

- Control Frames
  - RTS/CTS/ACK
  - CF-Poll/CF-End
- Management Frames
  - Beacons
  - Probe Request/Response
  - Association Request/Response
  - Dissociation/Reassociation
- Authentication/Deauthentication
  - ATIM
- Data Frames

802.11 - MAC management

- Synchronization

  try to find a LAN, try to stay within a LAN timer etc.
- Power management

  sleep-mode without missing a message

  periodic sleep, frame buffering, traffic measurements
- Association/Reassociation

  integration into a LAN

  roaming, i.e. change networks by changing access points

  scanning, i.e. active search for a network
- MIB - Management Information Base

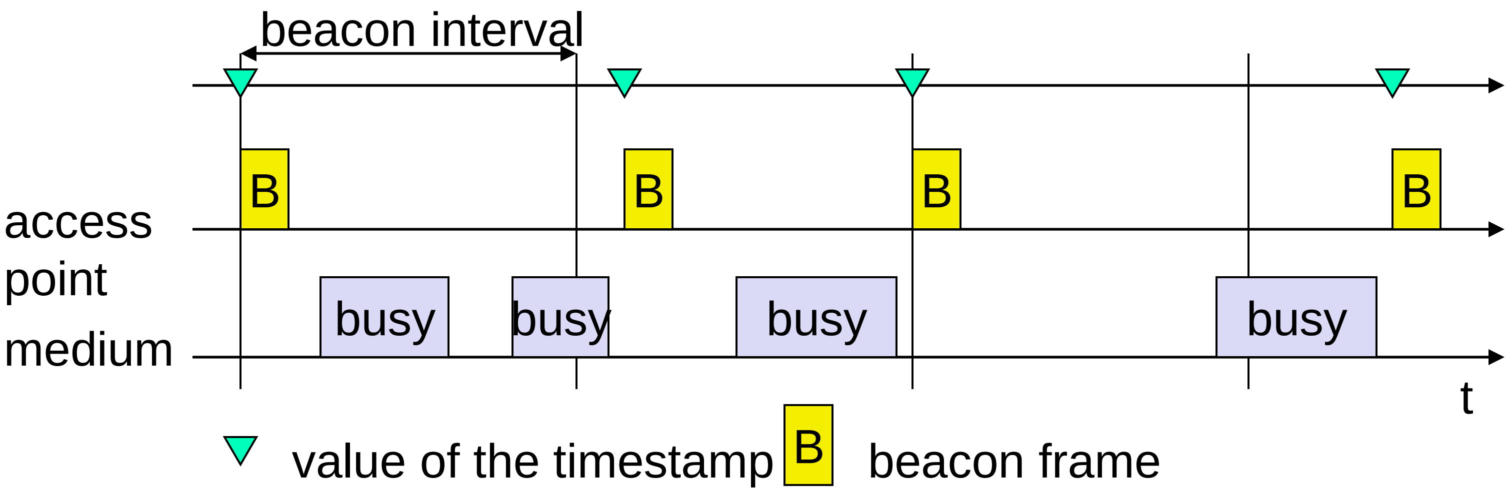
  managing, read, write

802.11 - Synchronization

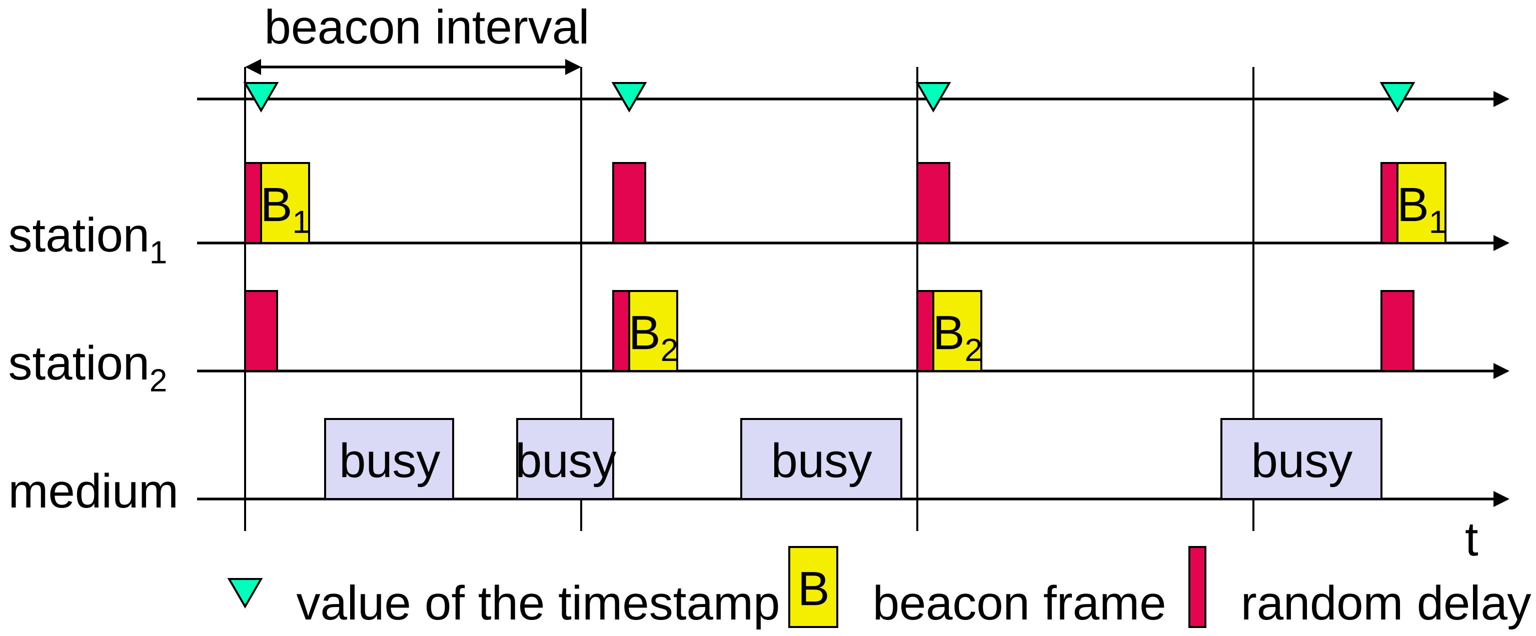
- All STAs within a BSS are synchronized to a common clock
- Infrastructure mode: AP is the timing master
  - periodically transmits Beacon frames containing Timing Synchronization function (TSF)
  - Receiving stations accepts the timestamp value in TSF
- Ad hoc mode: TSF implements a distributed algorithm
  - Each station adopts the timing received from any beacon that has TSF value later than
  - its own TSF timer

- This mechanism keeps the synchronization of the TSF timers in a BSS to within 4 μs plus the maximum propagation delay of the PHY layer

Synchronization using a Beacon (infrastructure)



Synchronization using a Beacon (ad-hoc)



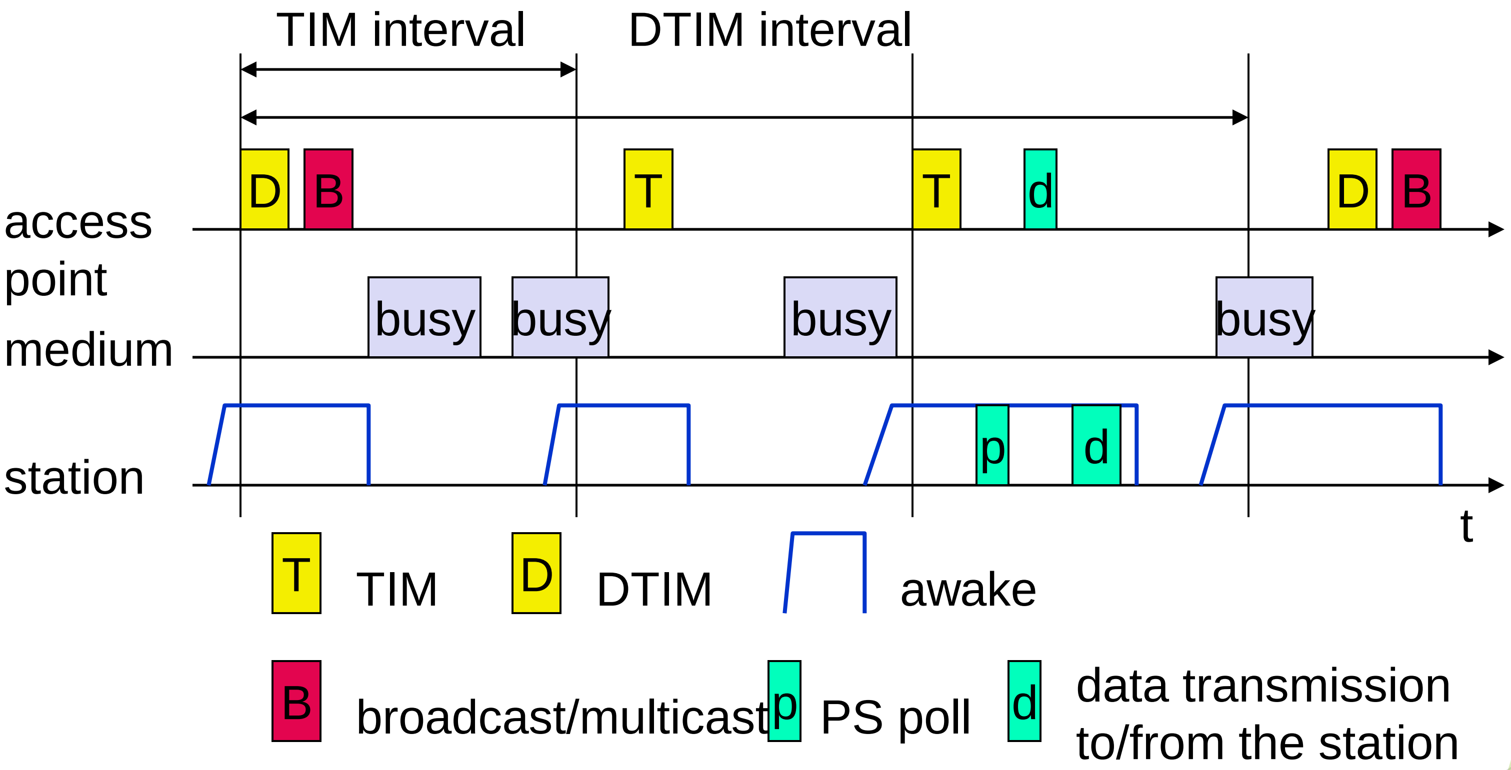
Power management

- Idea: switch the transceiver off if not needed

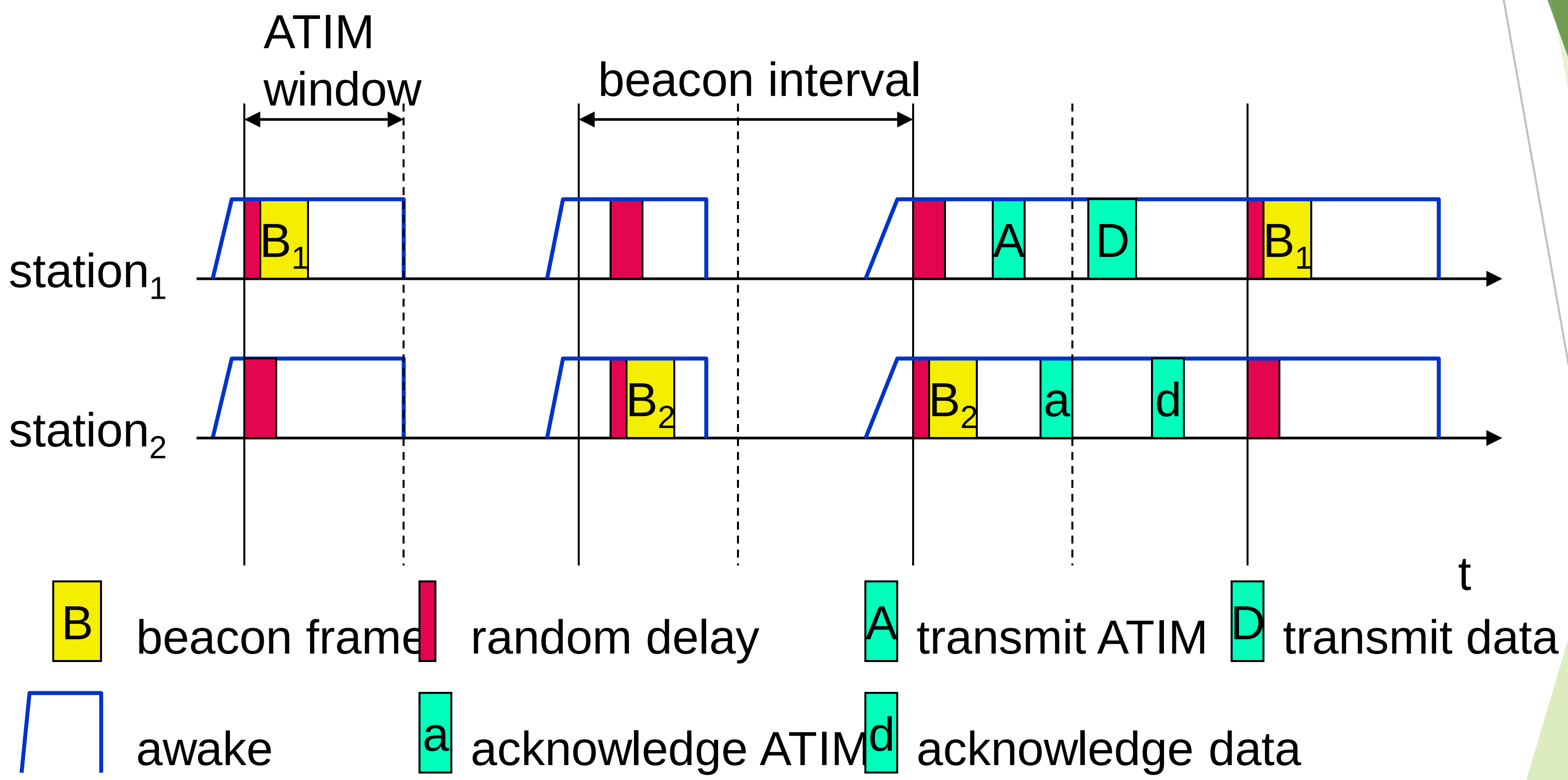
  States of a station: sleep and awake
- Timing Synchronization Function (TSF)

  stations wake up at the same time
- Infrastructure
  - Traffic Indication Map (TIM)
  - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
  - list of broadcast/multicast receivers transmitted by AP
- Ad-hoc
  - Ad-hoc Traffic Indication Map (ATIM)
  - announcement of receivers by stations buffering frames
  - more complicated - no central AP
  - collision of ATIMs possible (scalability?)

Power saving with wake-up patterns (infrastructure)



Power saving with wake-up patterns (ad-hoc)



802.11 - Roaming

- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources

IEEE 802.11 Summary

- Infrastructure and ad hoc modes using DCF
- Carrier Sense Multiple Access
- Binary exponential backoff for collision avoidance and congestion control
- Acknowledgements for reliability
- Power save mode for energy conservation
- Time-bound service using PCF
- Signaling packets for avoiding Exposed/Hidden terminal problems, and for reservation
  - Medium is reserved for the duration of the transmission
  - RTS-CTS in DCF
  - Polls in PCF

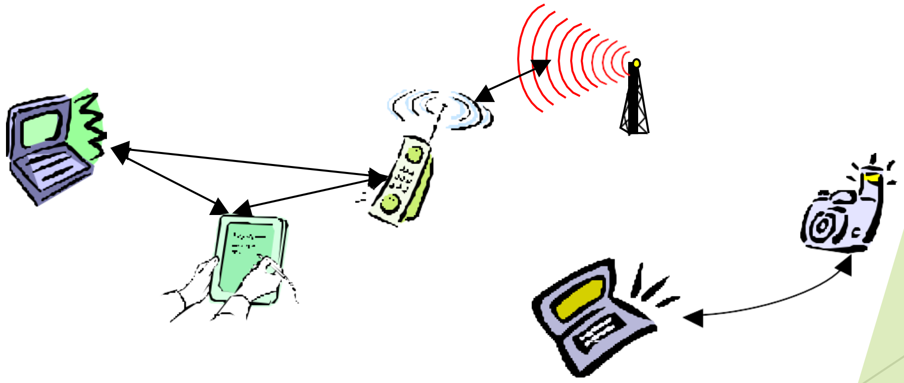
- IEEE WPAN (Wireless Personal Area Networks)
  - market potential
  - compatibility
  - low cost/power, small form factor
  - technical/economic feasibility
    - Bluetooth
    - Zigbee

Bluetooth

Idea

- Universal radio interface for ad-hoc wireless connectivity
- Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
- Embedded in other devices, goal: 5€/device (2005: 40€/USB bluetooth)
- Short range (10 m), low power consumption, license-free 2.45 GHz ISM
- Voice and data transmission, approx. 1 Mbit/s gross data rate

One of the first modules (Ericsson).



Prof. Dr.-Ing. Jochen Schiller, http://www.jochenschiller.de/

Bluetooth

History

- 1994: Ericsson (Mattison/Haartsen), “MC-link” project
- Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
- 1998: foundation of Bluetooth SIG, www.bluetooth.org (was: Bluetooth.)
- 1999: erection of a rune stone at Ercisson/Lund ;-)
- 2001: first consumer products for mass market, spec. version 1.1 released
- 2005: 5 million chips/week

Bluetooth™

Special Interest Group

- Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
- Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
- > 2500 members
- Common specification and certification of products

Characteristics

4. GHz ISM band, 79 (23) RF channels, 1 MHz carrier spacing
   - Channel 0: 2402 MHz … channel 78: 2480 MHz
   - G-FSK modulation, 1-100 mW transmit power

FHSS and TDD
   - Frequency hopping with 1600 hops/s
   - Hopping sequence in a pseudo random fashion, determined by a master
   - Time division duplex for send/receive separation

Voice link – SCO (Synchronous Connection Oriented)
   - FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched

Data link – ACL (Asynchronous ConnectionLess)
   - Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched

Topology
   - Overlapping piconets (stars) forming a scatternet

Piconet

Collection of devices connected in an ad hoc fashion

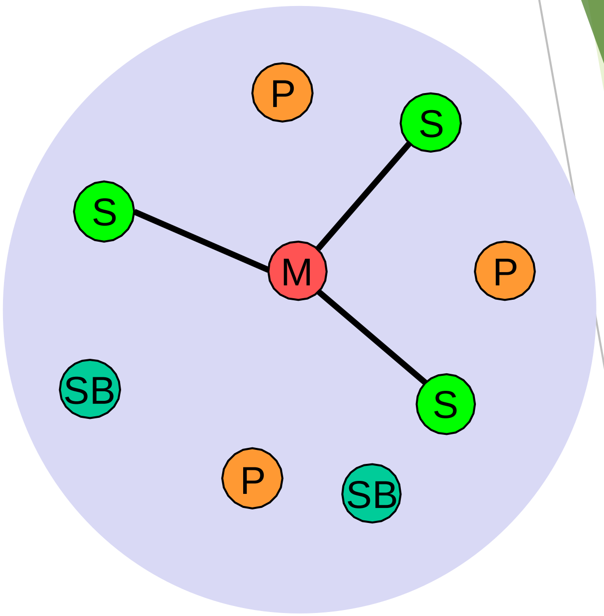
One unit acts as master and the others as slaves for the lifetime of the piconet

Master determines hopping pattern, slaves have to synchronize

Each piconet has a unique hopping pattern

Participation in a piconet = synchronization to hopping sequence

Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)



M=Master
S=Slave

P=Parked
SB=Standby

Prof. Dr.-Ing. Jochen Schiller, http://www.jochenschiller.de/

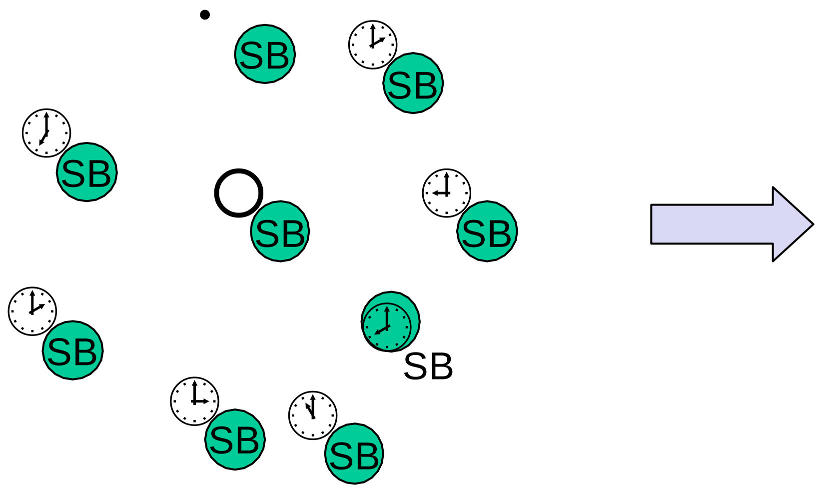
Forming a piconet

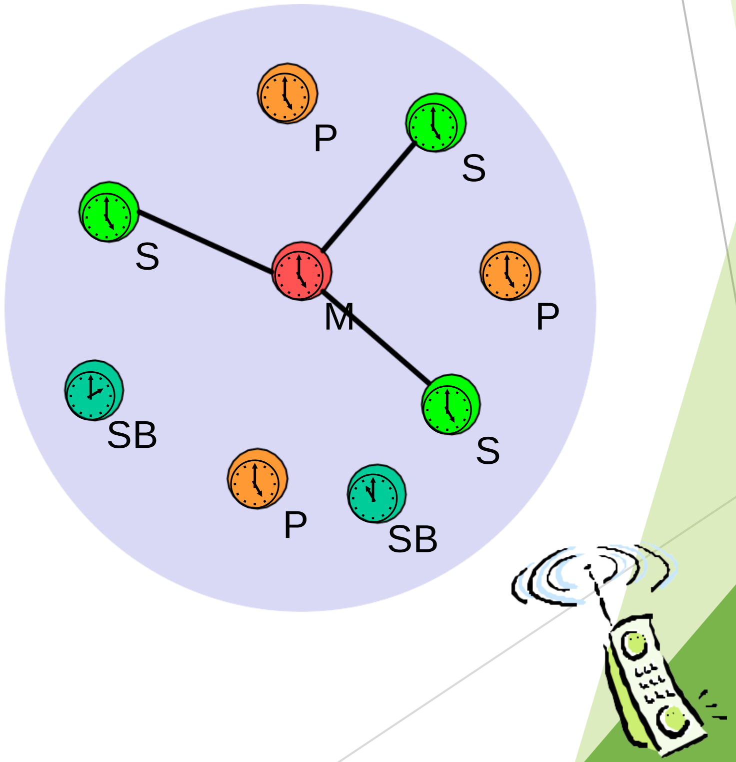
All devices in a piconet hop together

- Master gives slaves its clock and device ID
  - Hopping pattern: determined by device ID (48 bit, unique worldwide)
  - Phase in hopping pattern determined by clock

Addressing

- Active Member Address (AMA, 3 bit)
- Parked Member Address (PMA, 8 bit)





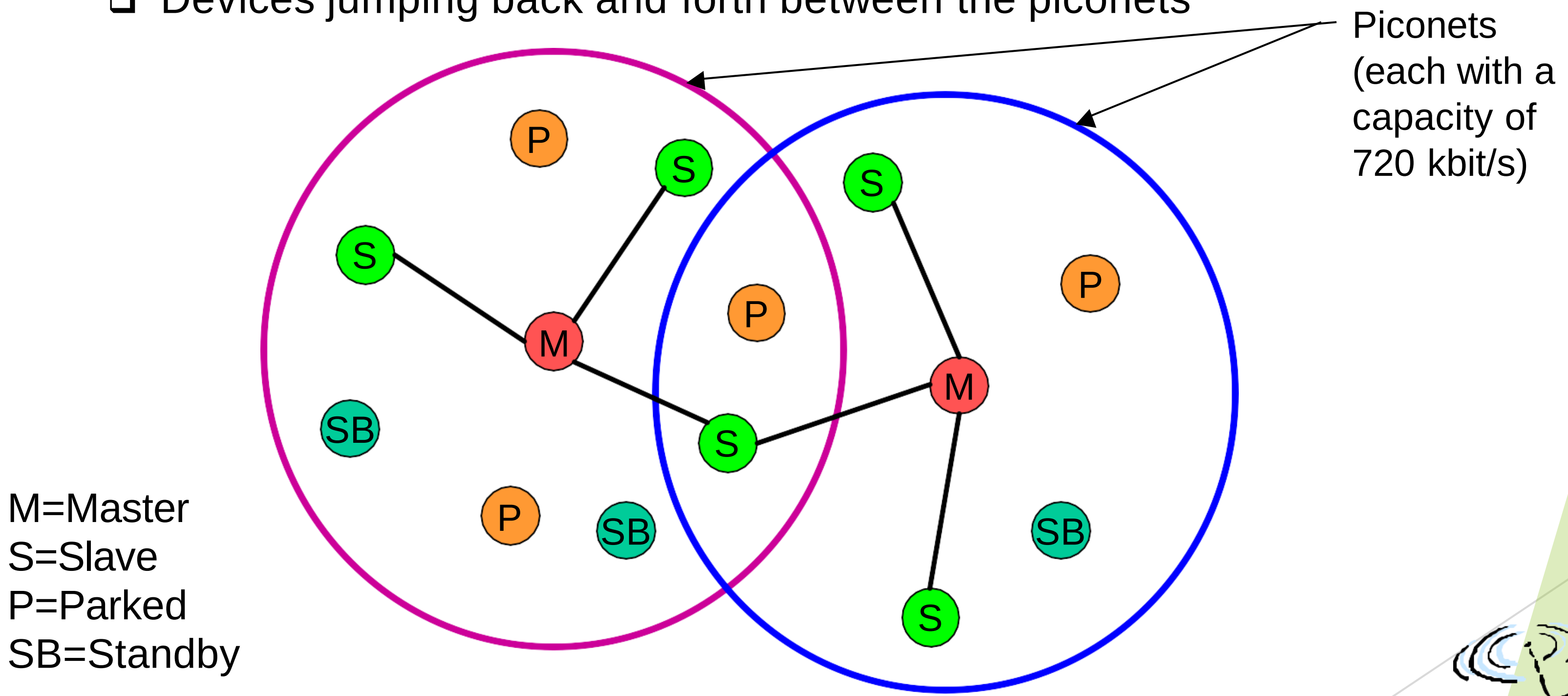
Scatternet

Linking of multiple co-located piconets through the sharing of common master or slave devices

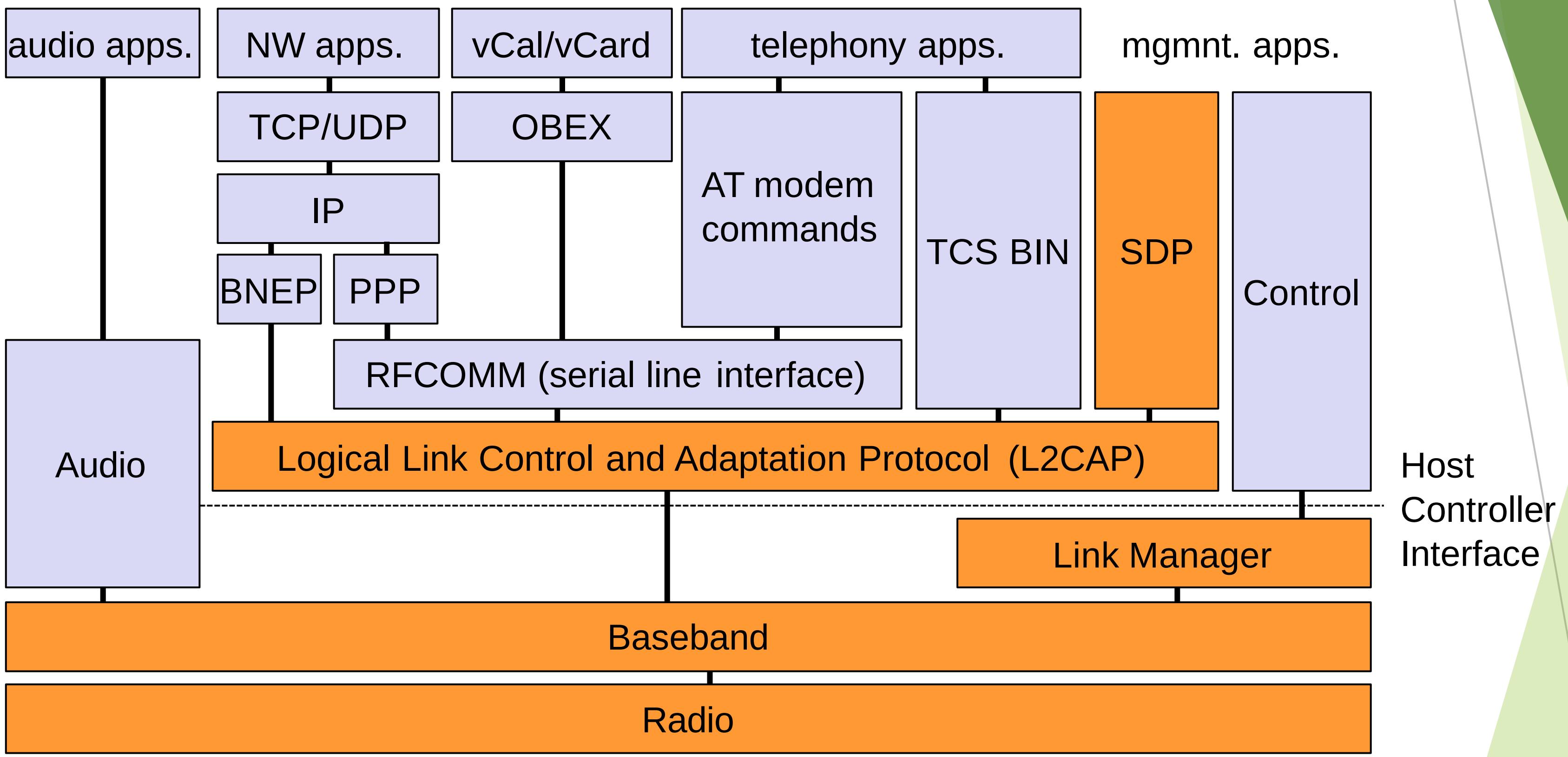
- Devices can be slave in one piconet and master of another

Communication between piconets

- Devices jumping back and forth between the piconets



Bluetooth protocol stack



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

Prof. Dr.-Ing. Jochen Schiller, http://www.jochenschiller.de/

Bluetooth Protocol Stack

- Radio: Specification of the air interface, i.e., frequencies, modulation, and transmit power
- Baseband: Description of basic connection establishment, packet formats, timing, and basic QoS parameters
- Link manager protocol: Link set-up and management between devices including security functions and parameter negotiation
- Logical link control and adaptation protocol (L2CAP): Adaptation of higher layers to the baseband (connectionless and connection-oriented services,
- Service discovery protocol: Device discovery in close proximity plus querying of service characteristics

Bluetooth Protocol Stack

- Cable replacement protocol RFCOMM that emulates a serial line interface following the EIA-232 (formerly RS-232) standards. RFCOMM supports multiple serial ports over a single physical channel.
- The telephony control protocol specification – binary (TCS BIN) describes a bit-oriented protocol that defines call control signaling for the establishment of voice and data calls between Bluetooth devices. It also describes mobility and group management functions. The host controller interface (HCI) between the baseband and L2CAP provides a command interface to the baseband controller and link manager, and access to the hardware status and control registers. The HCI can be seen as the hardware/software boundary.

L2CAP - Logical Link Control and Adaptation Protocol

Simple data link protocol on top of baseband

Connection oriented, connectionless, and signalling channels

Protocol multiplexing

- RFCOMM, SDP, telephony control

Segmentation & reassembly

- Up to 64kbyte user data, 16 bit CRC used from baseband

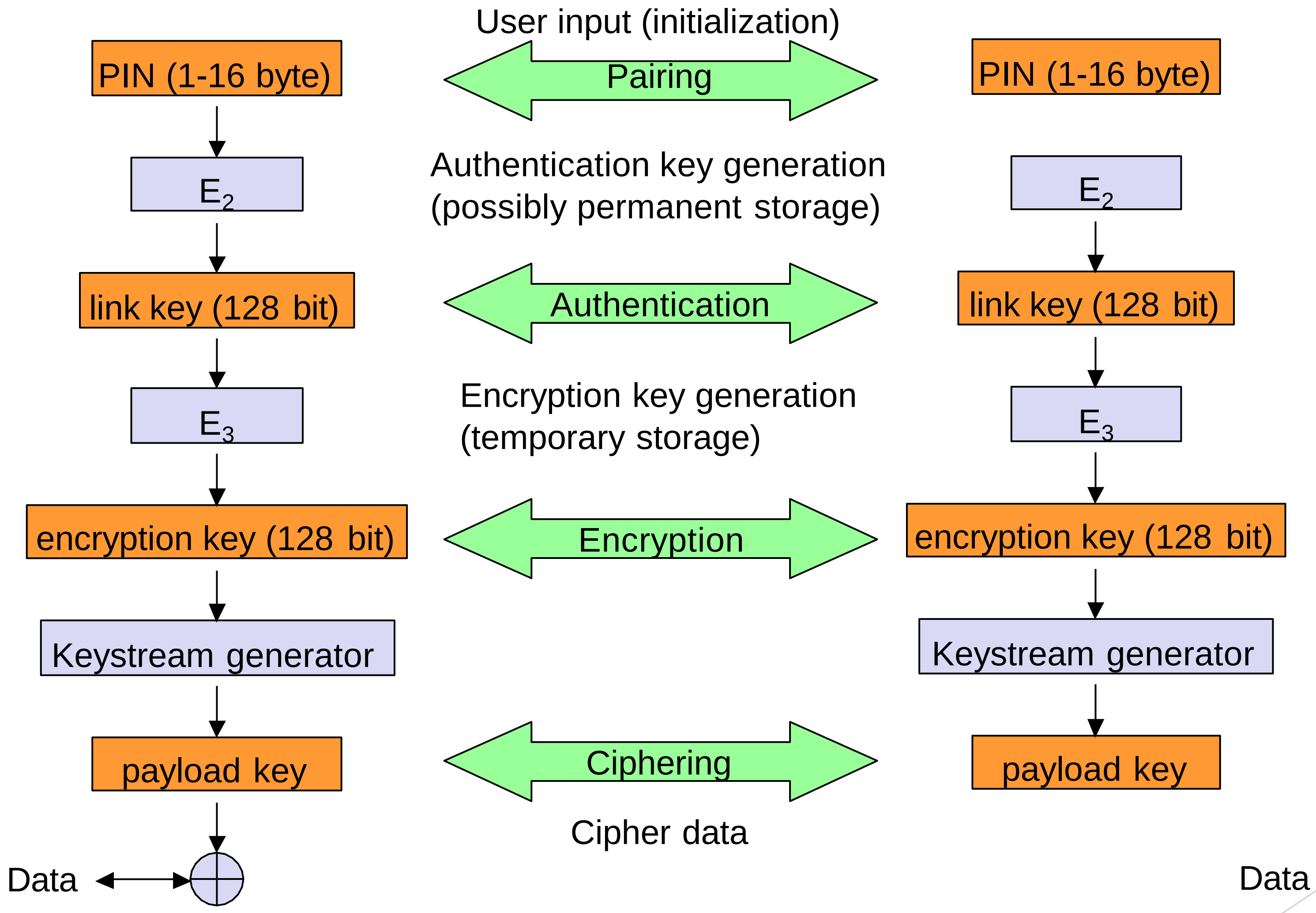
QoS flow specification per channel

- Follows RFC 1363, specifies delay, jitter, bursts, bandwidth

Group abstraction

- Create/close group, add/remove member

Security architecture of Bluetooth



Prof. Dr.-Ing. Jochen Schiller, http://www.jochenschiller.de/

LMP

- Authentication, pairing, and encryption: Although basic authentication is handled in the baseband, LMP has to control the exchange of random numbers and signed responses.
- Synchronization: Precise synchronization is of major importance within a Bluetooth network. The clock offset is updated each time a packet is received from the master. Additionally, special synchronization packets can be received.
- Capability negotiation: Not all Bluetooth devices will support all features that are described in the standard, so devices have to agree the usage of, e.g., multi-slot packets, encryption, SCO links, voice encoding, park/sniff/hold mode (explained below), HV2/HV3 packets etc.
- Quality of service negotiation: Different parameters control the QoS of a Bluetooth device at these lower layers. The poll interval, i.e., the maximum time between transmissions from a master to a particular slave, controls the latency and transfer capacity. Depending on the quality of the channel, DM or DH packets may be used (i.e., 2/3 FEC protection or no protection).
- Power control: A Bluetooth device can measure the received signal strength. Depending on this signal level the device can direct the sender of the measured signal to increase or decrease its transmit power.

SDP – Service Discovery Protocol

Inquiry/response protocol for discovering services

- ❑ Searching for and browsing services in radio proximity
- ❑ Adapted to the highly dynamic environment
- ❑ Can be complemented by others like SLP, Jini, Salutation, …
- ❑ Defines discovery only, not the usage of services
- ❑ Caching of discovered services
- ❑ Gradual discovery

Additional protocols to support legacy protocols/apps.

RFCOMM

- Emulation of a serial port (supports a large base of legacy applications)
- Allows multiple ports over a single physical channel

Telephony Control Protocol Specification (TCS)

- Call control (setup, release)
- Group management

OBEX

- Exchange of objects, IrDA replacement

WAP

- Interacting with applications on cellular phones

Power management

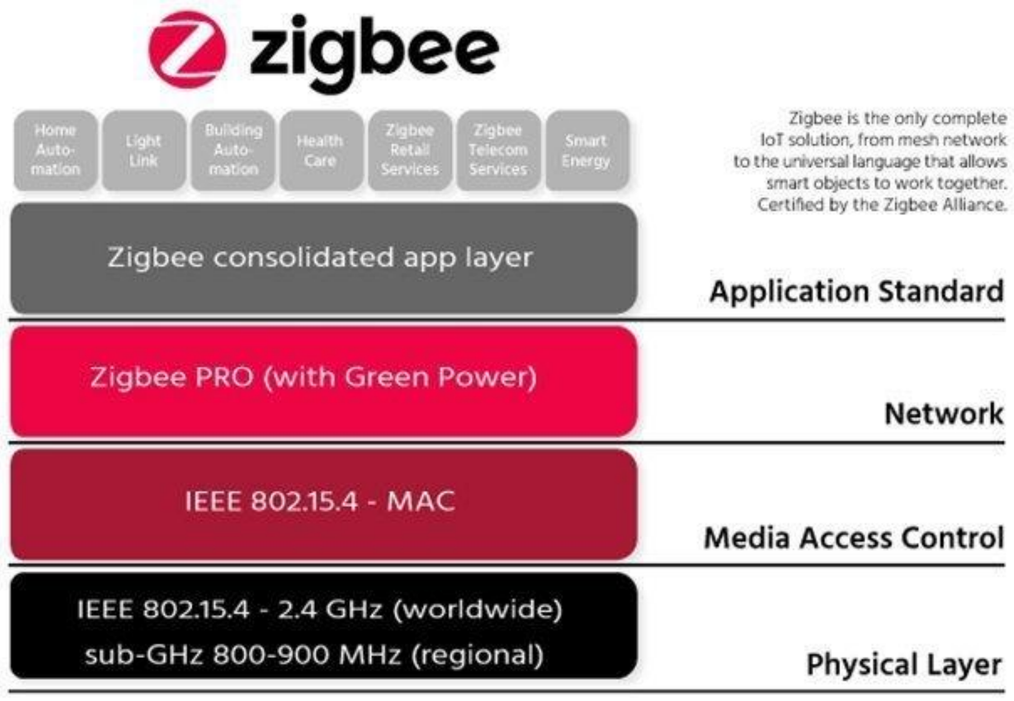
- . All devices being active must have the 3-bit active member address (AMA).
- To save battery power, a Bluetooth device can go into one of three low power states:
  - Sniff state: The sniff state has the highest power consumption of the low power states. Here, the device listens to the piconet at a reduced rate (not on every other slot as is the case in the active state).
  - Hold state: The device does not release its AMA . If there is no activity in the piconet, the slave may either reduce power consumption or participate in another piconet.
  - Park state: In this state the device has the lowest duty cycle and the lowest power consumption. The device releases its AMA and receives a parked member address (PMA). The device is still a member of the piconet, but gives room for another device to become active

Zigbee

- Zigbee is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks.
- Zigbee is for low-data rate, low-power applications and is an open standard.
- Zigbee products have been extended and customized by vendors and, thus, plagued by interoperability issues.
- In contrast to Wi-Fi networks used to connect endpoints to high-speed networks, Zigbee supports much lower data rates and uses a mesh networking protocol to avoid hub devices and create a self-healing architecture.
- IEEE 802.15.4 wireless standard for wireless personal area networks (WPANs). The Zigbee WPANs operate on 2.4 Ghz, 900 MHz and 868 MHz frequencies.

ZigBee Architecture

Zigbee Applications:
1.Home Automation
2.Medical Data Collection
3.Industrial Control Systems
4.meter reading system
5.light control system



Bluetooth v/s Zigbee

- **Bluetooth** was developed under IEEE 802.15.1, which is used for providing wireless communication through radio signals. The frequency range supported in Bluetooth varies from 2.4 GHz to 2.483 GHz. It covers less distance than Zigbee. In Bluetooth, GFSK modulation technique is used.
- **Zigbee**, BPSK and QPSK modulation techniques are used like UWB (Ultra-Wide Band). the frequency range supported in Zigbee is mostly 2.4 GHz worldwide, which means 2.4 GHz is not supported at all times. It covers more distance as compared with Bluetooth.

Bluetooth networks can be built using the point-to-point master-slave approach in which there is one master and up to seven slaves form a piconet, which leads to forming a scatter net which is a linking of two or more piconets.

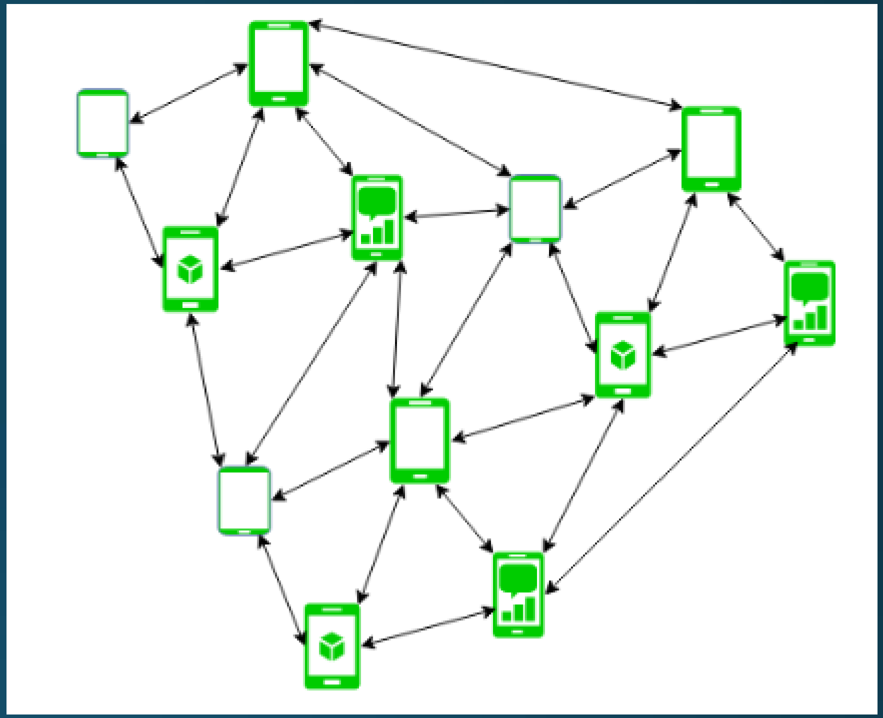
Zigbee devices can be networked in a variety of generic topologies, including a star, mesh, and others. A cluster can be created by connecting different Zigbee-based network topologies. Zigbee Coordinator, Zigbee Router, and Zigbee Endpoint nodes make up any Zigbee network.

Unit 4-Part1

MANETS

Content

- Mobile Ad-hoc networks
- Characteristics and applications
- Coverage and connectivity problems
- Routing in MANETs.



MANET

- MANET stands for Mobile Adhoc Network also called a wireless Adhoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.
- They consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure.
- MANET nodes are free to move randomly as the network topology changes frequently.
- Each node behaves as a router as they forward traffic to other specified nodes in the network.

Characteristics

- **Dynamic Topologies:**
  Network topology which is typically multihop may change randomly and rapidly with time, it can form unidirectional or bi-directional links.
- **Bandwidth constrained, variable capacity links:**
  Wireless links usually have lower reliability, efficiency, stability, and capacity as compared to a wired network
- **Autonomous Behavior:**
  Each node can act as a host and router, which shows its autonomous behavior.
- **Energy Constrained Operation:**
  As nodes rely on batteries or other exhaustible means for their energy. Mobile nodes are characterized by less memory, power, and lightweight features.

Characteristics

- **Limited Security:**
  Wireless networks are more prone to security threats. A centralized firewall is absent due to the distributed nature of the operation for security, routing, and host configuration.
- **Less Human Intervention:**
  They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature.

MANETS-PROS and CONS

Pros:

- Separation from central network administration.
- Each node can play both the roles ie. of router and host showing autonomous nature.
- Self-configuring and self-healing nodes do not require human intervention.
- Highly scalable and suits the expansion of more network hub.

Cons:

- Resources are limited due to various constraints like noise, interference conditions, etc.
- Lack of authorization facilities.
- More prone to attacks due to limited physical security.
- High latency i.e. There is a huge delay in the transfer of data between two sleeping nodes.

Types of MANETS

- **Vehicular Ad hoc Network (VANETs) –**
  Enable effective communication with another vehicle or with the roadside equipments. Intelligent vehicular ad hoc networks(InVANETs) deals with another vehicle or with roadside equipments.

- **Smart Phone Ad hoc Network (SPANC) –**
  To create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. Here peers can join or leave the network without destroying it.

- **Internet based Mobile Ad hoc Network (iMANETs) –**
  It supports internet protocols such as TCP/UDP and IP. To link mobile nodes and establish routes distributed and automatically.

Types of MANETS

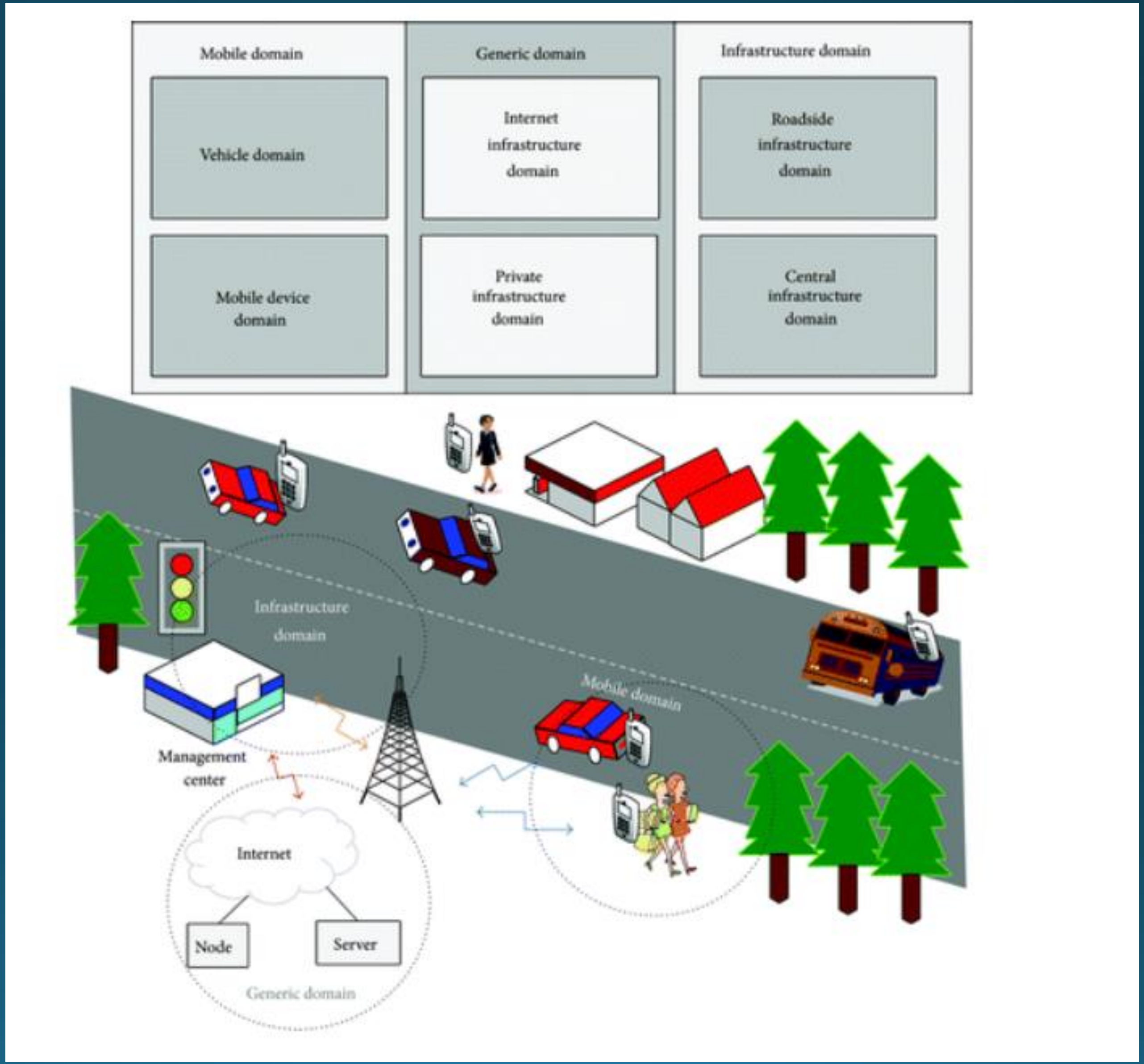
- **Hub-Spoke MANET:**
  Multiple sub MANET's may be connected in hub-spoke VPN to create a geographically distributed MANET. Normal Ad-hoc routing algorithm does not apply directly.

- **Military or Tactical MANETs –**
  This is used by the military units. Emphasis on data rate, real-time demand, fast re-routing during mobility, security, radio range, etc.

- **Flying Ad hoc Network (FANETs) –**
  This is composed of unmanned aerial vehicles (commonly known as drones). Provides links to remote areas and mobility.

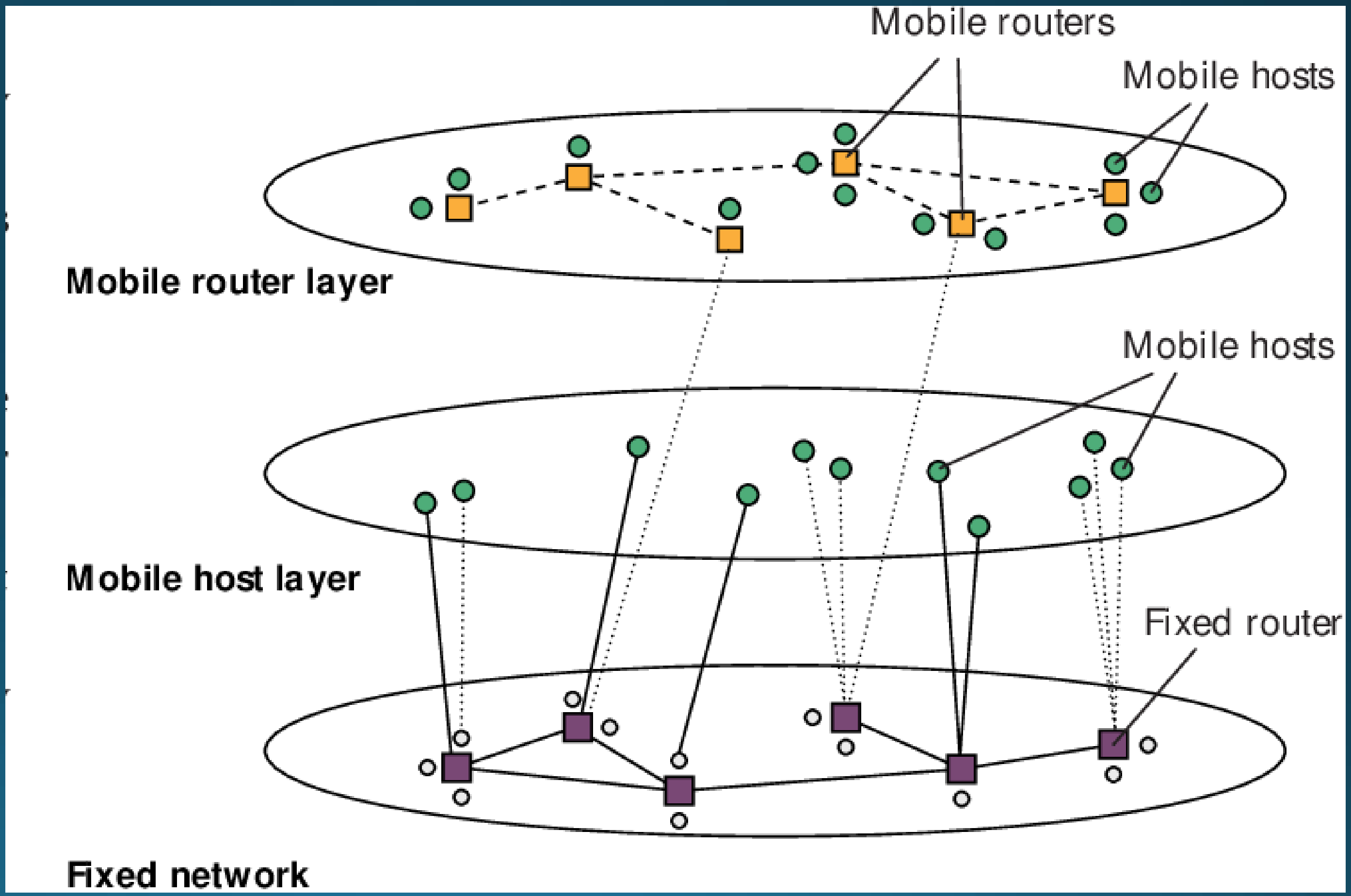
VANET

- The mobile domain consists of two parts: the vehicle domain and the mobile device domain.
- The vehicle domain comprises all kinds of vehicles such as cars and buses.
- The mobile device domain comprises all kinds of portable devices like personal navigation devices and smartphones.



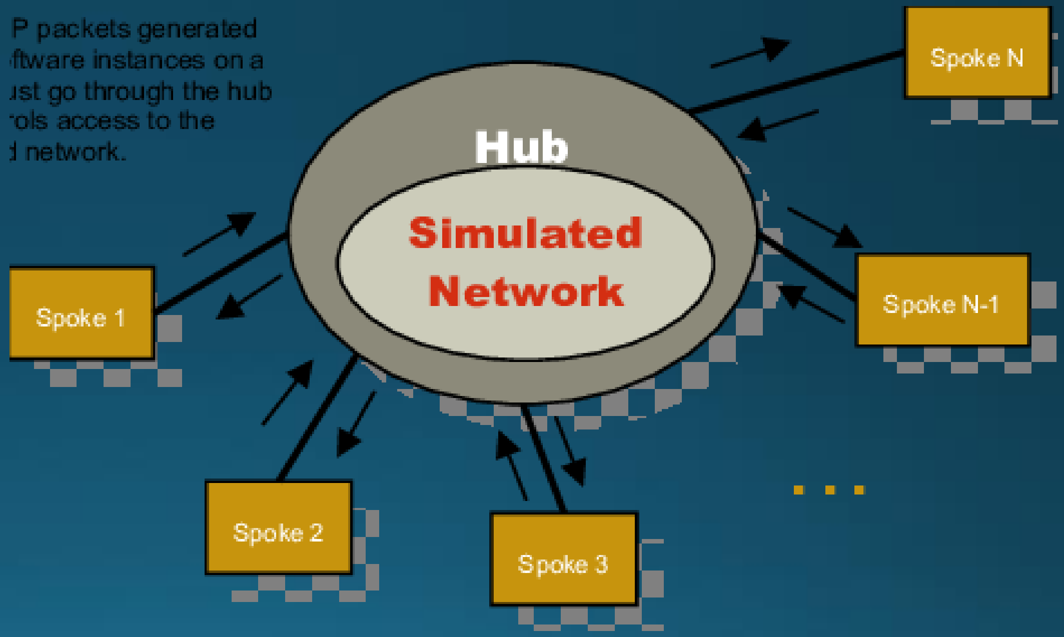
iMANETS

Internet based mobile ad hoc network (IMANET) is **an emerging technique that combines a wired network (e.g. Internet) and a mobile ad hoc network (manet) for developing a ubiquitous communication infrastructure**.

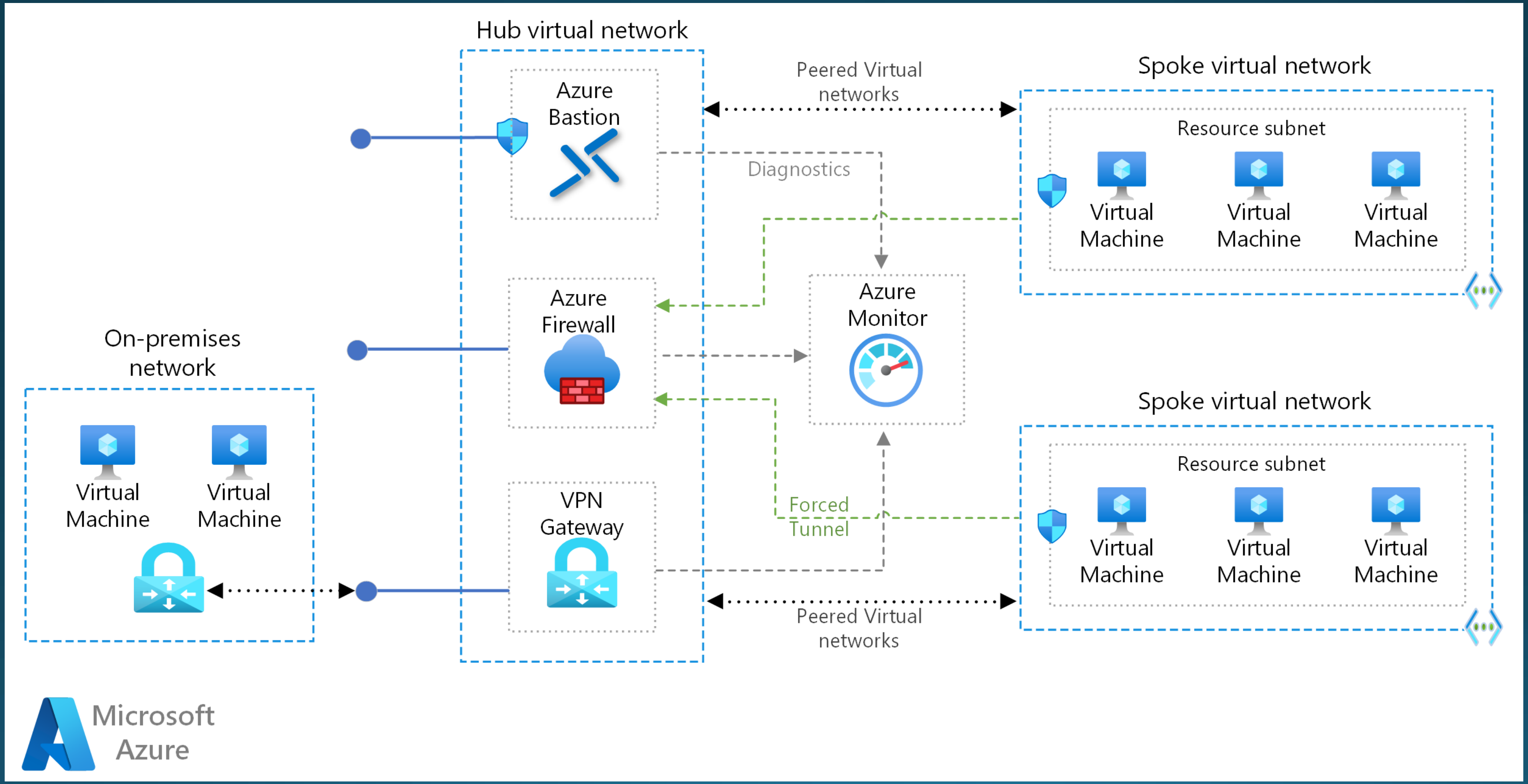


HUB-SPOKE MANETS

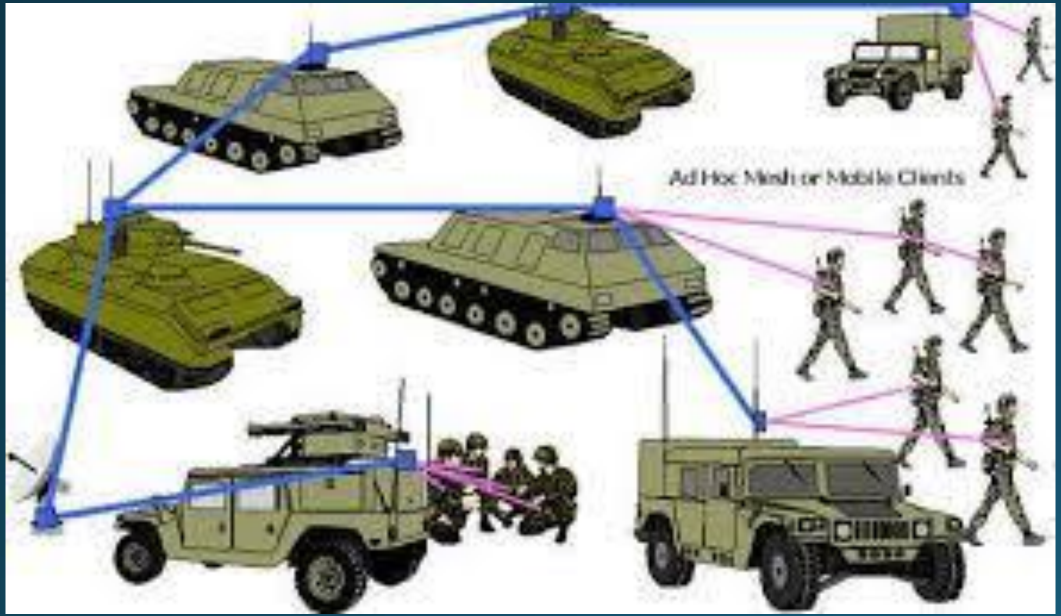
The communication is not made between pairs of applications, but between each application (spoke) and the central hub [1]. The broker functionalities include routing and messages transformation to the receiver spoke.



Azure with Hub-Spoke Architecture

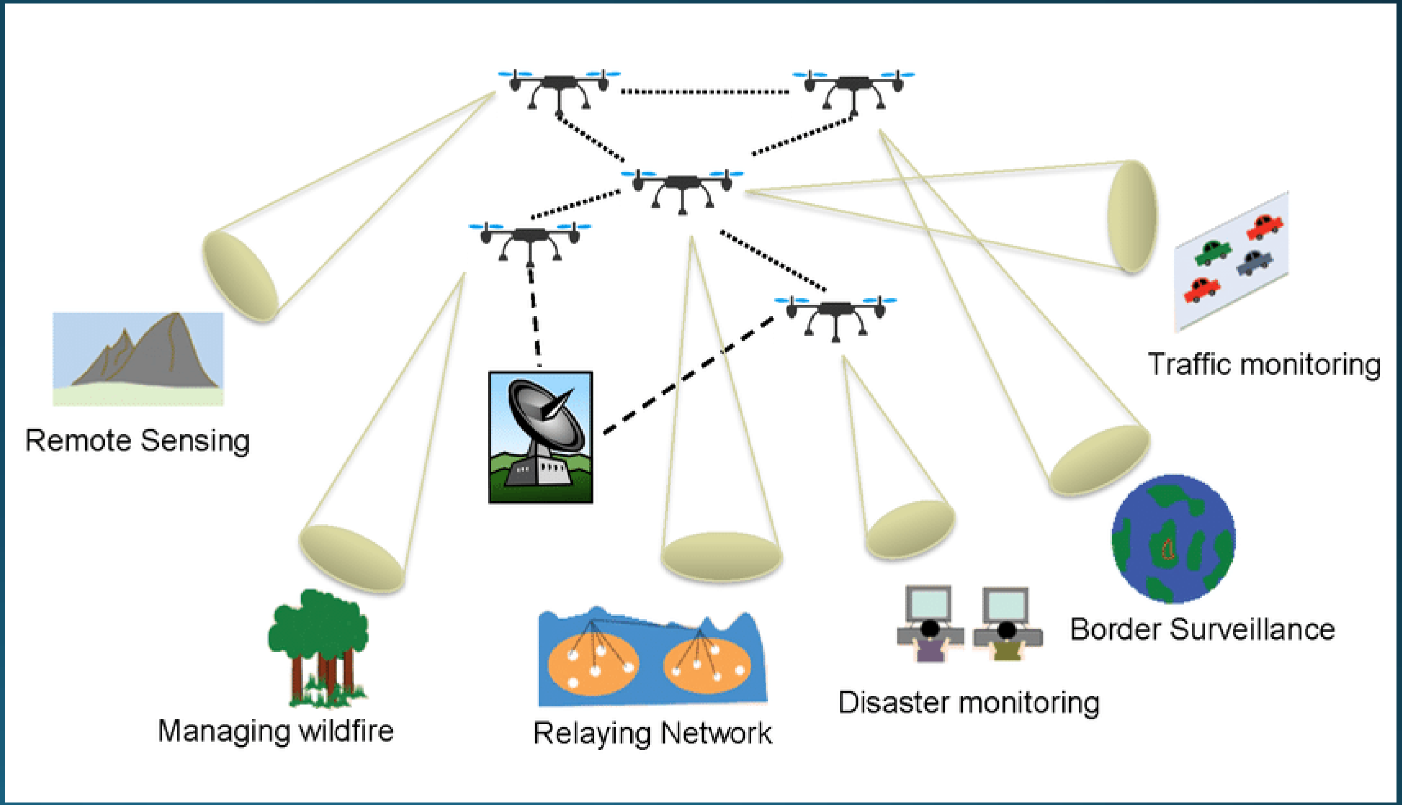


Tactical Manets



FANETS

- A Flying Ad hoc Networks (FANETs) is **such kind of network that consists of a group of small UAVs connected in ad-hoc manner, which are integrated into a team to achieve high level goals.**



Applications

- Military field: Ad-Hoc networking can permit army to exploit benefit of conventional network expertise for preserving any info network among vehicles, armed forces, and headquarters of information.
- Cooperative work: To facilitate the commercial settings, necessity for concerted computing is very significant external to office atmosphere and surroundings as compared to inner environment. People want getting outside meetings for exchanging the information plus cooperating with each other regarding any assigned task.
- Confined level: Ad-Hoc networks are able to freely associate with immediate, in addition momentary hypermedia network by means of laptop computers for sharing the info with all the contestants' e.g. classroom and conference. Additional valid and confined level application may be in domestic network where these devices can interconnect straight in exchanging the information.
- PAN and Bluetooth: A PAN is localized and tiny range network whose devices are generally belong to a specified individual. Limited-range MANET such as Bluetooth can make simpler the exchange among several portable devices like a laptop, and a cell phone.

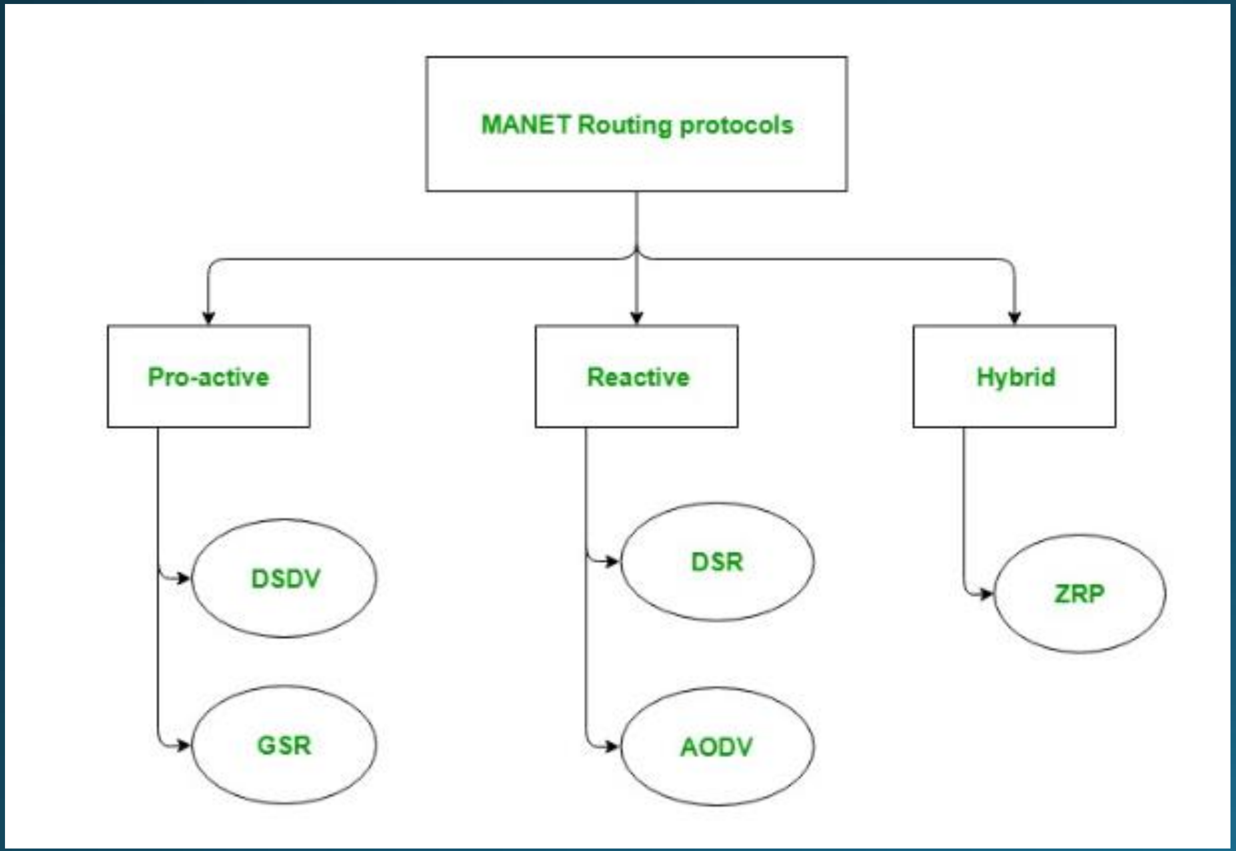
Applications

- Business Sector: Ad-hoc network could be used for rescuing and emergency processes for adversity assistance struggles, for instance, in flood, fire or earthquake. Emergency saving procedures should take place where damaged and non-existing transmissions structure and quick preparation of a transmission network is required .
- Sensor Networks: managing home appliances with MANETs in both the case like nearby and distantly. Tracking of objects like creatures. Weather sensing related activities.
- Backup Services: liberation operations, tragedy recovery, diagnosis or status or record handing in hospitals, replacement of stationary infrastructure.
- Educational sector: arrangement of communications facilities for computer-generated conference rooms or classrooms or laboratories [10] .

Routing in MANETS

- nodes do not know the topology of their network, instead they have to discover it by their own as the topology in the ad-hoc network is dynamic topology.
- The basic rules is that a new node whenever enters into an ad-hoc network, must announce its arrival and presence and should also listen to similar announcement broadcasts made by other mobile nodes.

Types of Routing



ProActive

- These are also known as table-driven routing protocols. Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes.
- Since the topology in the mobile ad-hoc network is dynamic, these routing tables are updated periodically as and when the network topology changes.
- It has a limitation that it doesn’t work well for the large networks as the entries in the routing table becomes too large since they need to maintain the route information to all possible nodes.

Reactive Routing

- These are also known as on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed.
- The process of route discovery occurs by flooding the route request packets throughout the mobile network.
- It consists of two major phases namely, route discovery and route maintenance.

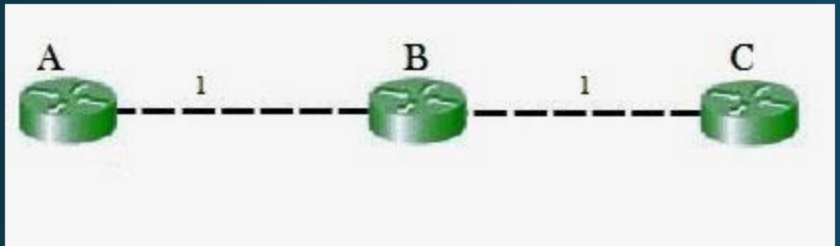
Hybrid Routing Protocol

- It basically combines the advantages of both, reactive and pro-active routing protocols. These protocols are adaptive in nature and adapts according to the zone and position of the source and destination mobile nodes. One of the most popular hybrid routing protocol is **Zone Routing Protocol (ZRP)**.
- The whole network is divided into different zones and then the position of source and destination mobile node is observed. If the source and destination mobile nodes are present in the same zone, then proactive routing is used for the transmission of the data packets between them. And if the source and destination mobile nodes are present in different zones, then reactive routing is used for the transmission of the data packets between them.

Proactive- DSDV protocol

- Distance vector routing protocol was not suited for mobile ad-hoc networks due to count-to-infinity problem.
- Hence, as a solution Destination Sequenced Distance Vector Routing Protocol (DSDV) came into picture.
  Destination sequence number is added with every routing entry in the routing table maintained by each node.
- A node will include the new update in the table only if the entry consists of the new updated route to the destination with higher sequence number.

Count to infinity Problem



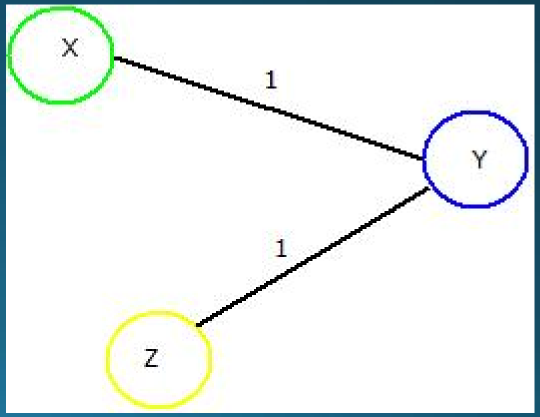
- B will know that it can get to C at a cost of 1, and A will know that it can get to C via B at a cost of 2.
- if the link between B and C is disconnected, then B will know that it can no longer get to C via that link and will remove it from its table.
- Before it can send any updates it’s possible that it will receive an update from A which will be advertising that it can get to C at a cost of 2.
- B can get to A at a cost of 1, so it will update a route to C via A at a cost of 3. A will then receive updates from B later and update its cost to 4.
- They will then go on feeding each other bad information toward infinity which is called as **Count to Infinity problem**.

DSDV

- DSDV protocol uses and maintains a single table only, for every node individually. The table contains the following attributes.
- Routing Table : It contains the distance of a node from all the neighboring nodes along with the sequence number(SEQ No means the time at which table is updated).
- This image describes the header format of Destination Sequenced Distance Vector Routing protocol
- Destination Sequenced Distance Vector Routing : Format
- This table is updated on every step and ensures that each node broadcast as well as receives correct information about all the nodes including their distance and sequence number.

DSDV working

- In DSDV, nodes broadcasts their routing tables to immediate neighbors with the sequence number.
- Every time any broadcasting occurs, the sequence number is also updated along with distances of nodes.
- Consider a network of 3 nodes having distances of "1" on each of the edges respectively. Below mentioned steps will let you know how DSDV works and routing tables are updated.



Routing tables at each node

For X:

Source	Destination	Next Hop	Cost	SEQ No
X	X	X	0	100-X
X	Y	Y	1	200-Y
X	Z	Y	2	300-Z

For Y:

Source	Destination	Next Hop	Cost	SEQ No
Y	X	X	1	100-X
Y	Y	Y	0	200-Y
Y	Z	Y	1	300-Z

For Z:

Source	Destination	Next Hop	Cost	SEQ No
Z	X	Y	2	100-X
Z	Y	Y	1	200-Y
Z	Z	Z	0	300-Z

If "Y" wants to broadcast the routing table. Then updated routing tables of all the nodes in the network will look like as depicted in the below tables where red marked cell denotes the change in sequence number.

For X:

Source	Destination	Next Hop	Cost	SEQ No
X	X	X	0	100-X
X	Y	Y	1	210-Y
X	Z	Y	2	300-Z

For Y:

Source	Destination	Next Hop	Cost	SEQ No
Y	X	X	1	100-X
Y	Y	Y	0	210-Y
Y	Z	Z	1	300-Z

For Z:

Source	Destination	Next Hop	Cost	SEQ No
Z	X	Y	2	100-X
Z	Y	Y	1	210-Y
Z	Z	Z	0	300-Z

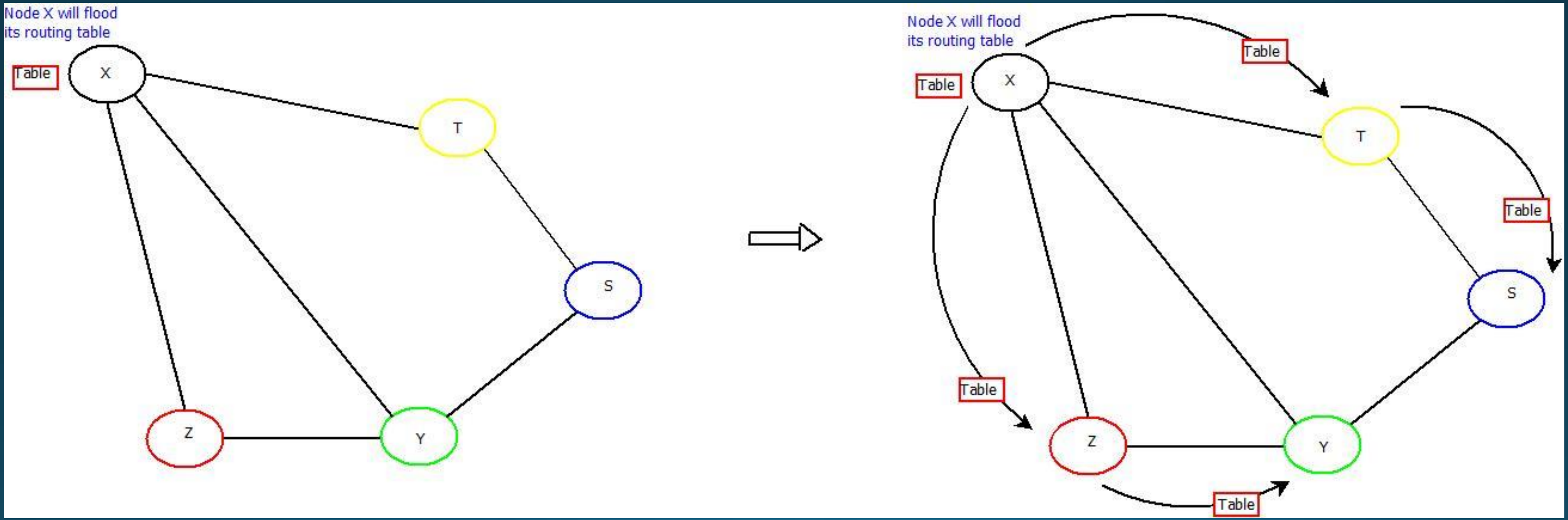
Pros and Cons

- <u>Advantages : Destination Sequenced Distance Vector Routing Protocol</u>
- Can't be implemented commercially or on larger scale.
- Efficient results will be produced if applied on small networks.
- <u>Disadvantages : Destination Sequenced Distance Vector Routing Protocol</u>
- Slower protocol processing time.
- Less bandwidth.
- Not suitable for large number of networks which are dynamic in nature.

GSR

- Global State Routing is based upon the fundamental concepts of link state routing.
- In Link State Routing(LSR), one of the node floods out a single routing table information to its neighbors and those neighbors floods out that table to further nodes. This process continue to take place until the routing table is received by all the nodes throughout the network.
- But in case of Global State Routing, the routing table of a particular node is broadcast-ed to its immediate neighbors only. Then initial tables of those neighboring nodes are updated. These updated tables are further broadcast one by one and this process continue to take place until all the nodes broadcasts their tables to each node in the network.
-

GSR working



Node X will flood
its routing table
Table
X
T
S
Z
Y
Node X will flood
its routing table
Table
Table
Table
Table
Table
X
T
S
Z
Y

GSR concept

- GSR protocol uses and maintains three tables for every node individually. These tables are:

1. Distance Table : This table contains the distance of a node from all the nodes in network.

Format :

Node	Distance

2. Topology Table : This table contains the information of Link state data along with the sequence number which can be used to determine when the information is updated last.

Format :	Node	Link State	Sequence

GSR concept

3. Next Hop Table : Next hop table will contain the information about the immediate neighbor of a particular node.

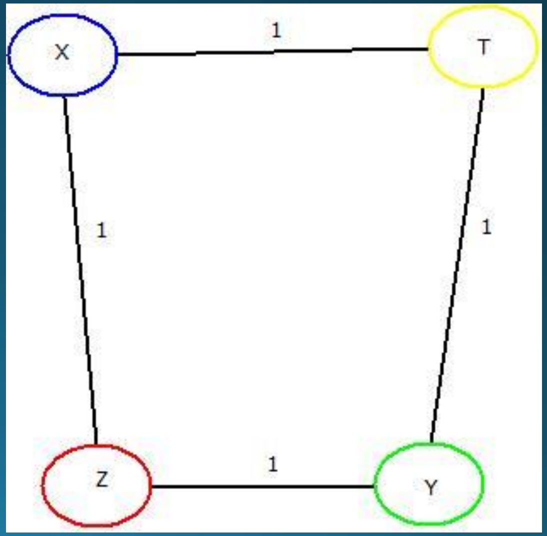
These tables are updated on every step and ensures that each node receives correct information about all the nodes including their distances.

Format :

Node	Next Hop

Example

- GSR broadcasts the routing tables to its immediate neighbors rather than flooding it to all the nodes as Link State Routing protocol does.
- Consider a network of 4 nodes having a distance of “1” on each of its edge. Below mentioned steps will let you know how GSR works and how its routing tables are updated.



GSR

- For Node "X" : Firstly three tables as mentioned above will be maintained which includes distance table, Topology table and Next hop tables. This same process will be done for rest of the nodes too.

Topology Table

Node	Link State	Sequence
X	{}	----
Y	{}	----
Z	{}	----
T	{}	----

Next Hop Table

Node	Link State
X	X
Y	-1
Z	-1
T	-1

Distance Table

Node	Distance
X	0
Y	Infinite
Z	Infinite
T	Infinite

GSR

- Secondly, broadcasting of all the tables will be done to all the immediate neighbors of “X” i.e. “Y” and “Z”.
- These tables are updated at “X”, “Y” & “T” nodes respectively.
- Same will be done for node “Y”. After first updation from “X”, node “Y” will broadcast the tables to its immediate neighbors i.e. “X” & “T” and those tables will be updated accordingly. This will be done for “T” & “Z” also.
- Once done, all the nodes “X”, “Y”, “Z” & “T” will be having the updated routing tables containing distances from each, with the help of which an optimal path can be chosen if data needs to be transferred from one node to other.

GSR updated tables

Node X

Distance Table

Node	Distance
X	0
Y	1
Z	1
T	∞

Next Hop Table

Node	Next
X	X
Y	Y
Z	Z
T	-1

Topology Table

Node	Link State	SEQ Number
X	{Y,Z}	1
Y	{}	----
Z	{X,T}	----
T	{}	----

Node Y

Distance Table

Node	Distance
X	1
Y	0
Z	∞
T	1

Next Hop Table

Node	Next
X	X
Y	Y
Z	-1
T	T

Topology Table

Node	Link State	SEQ Number
X	{}	----
Y	{X,T}	1
Z	{}	----
T	{}	----

Node Z

Distance Table

Node	Distance
X	1
Y	∞
Z	0
T	1

Next Hop Table

Node	Next
X	X
Y	-1
Z	-Z
T	T

Topology Table

Node	Link State	SEQ Number
X	{}	----
Y	{}	----
Z	{X,T}	1
T	{}	----

GSR

- Now, broadcasting of topology tables of “X” will take place to its neighbour i.e. “Y” & “Z” and updated tables will be like as mentioned below.

For Y:

Distance Table

Node	Distance
X	1
Y	0
Z	2
T	1

Next Hop Table

Node	Next
X	X
Y	Y
Z	X
T	T

Topology Table

Node	Link State	SEQ Number
X	{Y,Z}	1
Y	{X,T}	1
Z	{}	----
T	{}	----

For Z:

Distance Table

Node	Distance
X	1
Y	2
Z	0
T	1

Next Hop Table

Node	Next
X	X
Y	X
Z	Z
T	T

Topology Table

Node	Link State	SEQ Number
X	{Y,Z}	1
Y	{}	----
Z	{X,T}	1
T	{}	----

Similarly, these tables are further updated with topology tables of “Y”, “Z” & “T” as done in case of “X.

Pros and Cons

Advantages : Global State Routing Protocol

- Higher accuracy of GSR in generating optimal path as compared to LSR.
- Broadcasting reduces error rate as compare to flooding used in LSR.

Disadvantages : Global State Routing Protocol

- Large bandwidth consumption.
- Higher operational cost.
- Large Message size resulting in more time consumption.

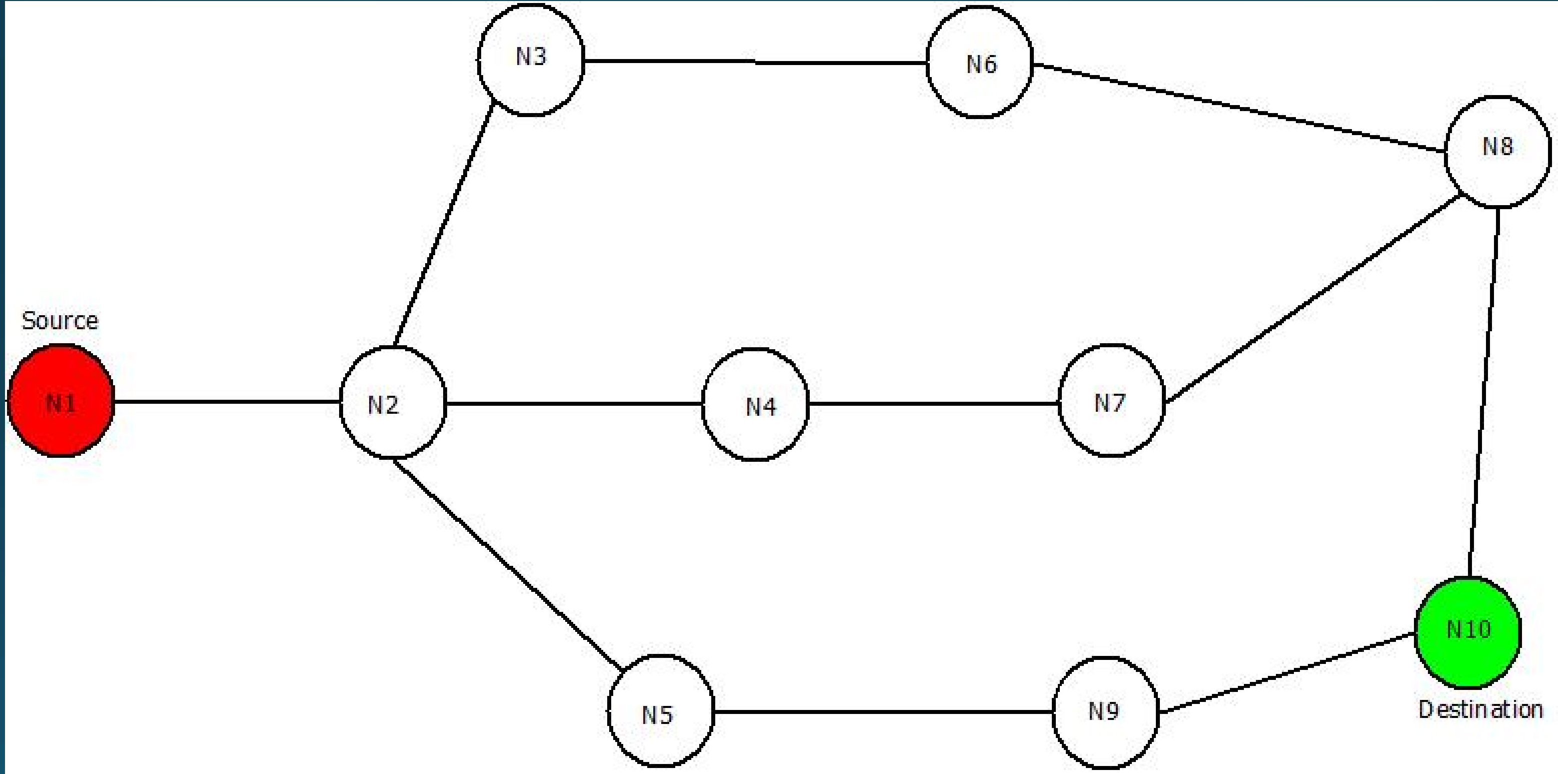
Reactive Protocols –Dynamic Source Routing

- Dynamic Source Routing (DSR) comes under the reactive routing protocol category, as it is capable of discovering the route from source to destination only when required and needed.
- Dynamic Source Routing protocol uses a process called "Route Discovery Mechanism" that is capable of discovering the route for data packets from source node to destination nodes using intermediate nodes.
- As like proactive routing protocols such as Global State Routing an Dynamic Sequence Distance Vector Routing no separate table is maintained.
- The major change in DSR as compare to GSR and DSDV is, in DSDV after asking a requirement of route from source to destination, path via intermediate nodes is checked for its length.
- Then a "Re-Request" packet is sent back from destination to source via the smallest route possible in the whole network. The "Re-Request" packet does contains its unique ID also.
- This process of separately sending a "Re-Request" packet from destination to source makes it easier for the sender to send the data packets on fixed path rather than sending it on multiple paths to check for total distance.

DSR working

- Dynamic Source Routing does broadcast the route to its neighbors but does not floods the information. It only trace the route by calculating the total distance or by calculating the number of nodes present in between source and destination nodes.
- Consider a network containing 10 nodes where node N1 being the source and node N10 being the destination nodes. Below mentioned steps will let you know how DSR protocol works and how Re-Request packet is transmitted through the network.

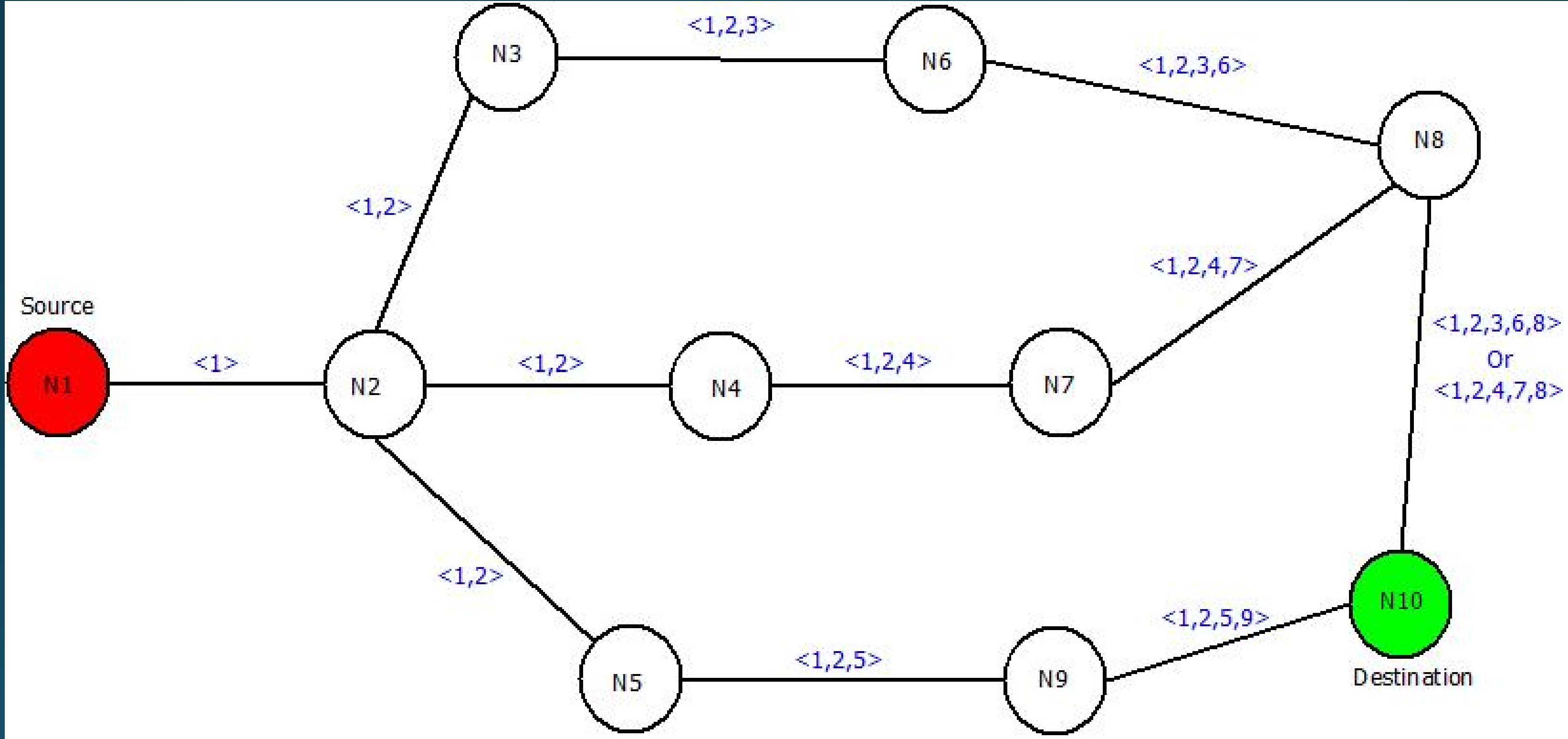
Example



DSR

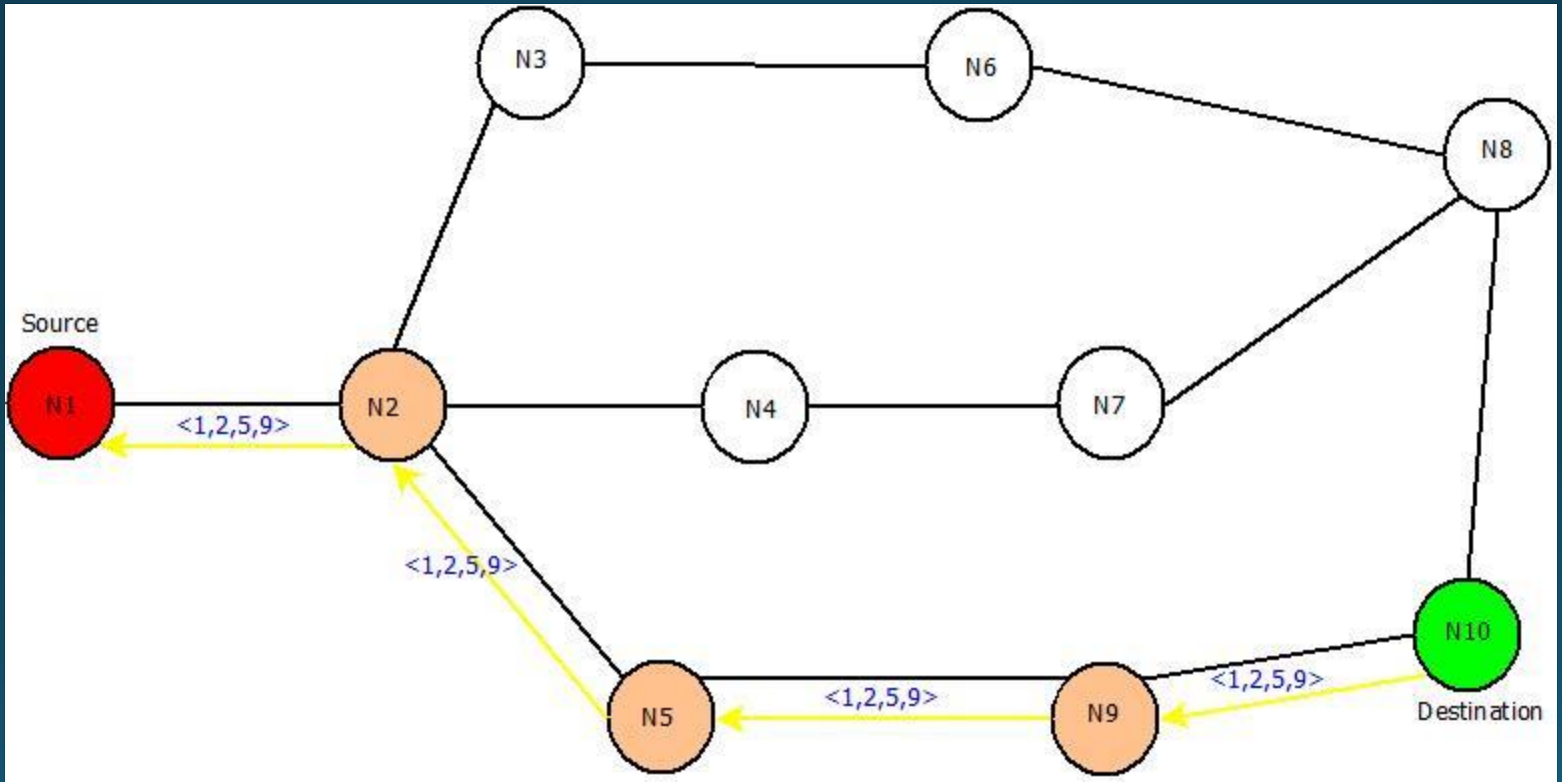
- Step 1: Start from source node N1 and broadcast the information about it to its neighbors i.e. in this case the route information is “<1>”, because of its one-to-one link between node N1 and N2.
- Step 2: Broadcast previous route information to neighbors of node N2 i.e. to node N3, N4, N5. The new route will remain same “<1,2>” in all the cases.
- Step 3: Take node N3 and broadcast previous route(<1,2>) to next neighboring nodes i.e. node N6. New route till node N6 will be “<1,2,3>” and same process can be done for other nodes i.e. Node N4 and N5.
- Step 4 : Further, broadcast the new routes i.e. <1,2,3,6> , <1,2,4> , <1,2,5> to nodes N8, N7 & N9 respectively.
- Step 5: Repeat the above steps until destination node is reached via all the routes.
- The updated routes will be as:

DSR-Updated Network



DSR

- After this, “Re-Request” packet will be sent in backward direction i.e. from destination node “N10” to source node “N1”. It will trace the shortest route by counting the number of nodes from route discovered in previous steps.
- The three possible routes are :
- Route 1: <1,2,3,6,8>
- Route 2: <1,2,4,7,8>
- Route 3: <1,2,5,9>
- Route 3 i.e. "<1,2,5,9>” will be chosen as it contains the least number of nodes and hence it will definitely be the shortest path and then data can be transferred accordingly.
- The Re-Request Packet route can be located as:



N3
N6
N8
Source
N1
N2
N4
N7
<1,2,5,9>
<1,2,5,9>
N10
<1,2,5,9>
<1,2,5,9>
N5
N9
Destination

Pros and Cons

Advantages : Dynamic Source Routing Protocol

- A perfect route is discovered always.
- Highly efficient.
- Low bandwidth Consumption.

Disadvantages : Dynamic Source Routing Protocol

- If the route gets broke, data transmission cannot happen.
- Time taking algorithm-Slow.
- If network is large , then it is impossible for the data packets header to hold whole information of the routes.

Ad-Hoc On Demand Distance Vector Routing Protocol(AODV)

- Another type of reactive routing protocol which does not maintain routes but build the routes as per requirements is Ad-Hoc On Demand Distance Vector Routing Protocol.
- AODV is used to overcome the drawbacks of Dynamic Source Routing Protocol and Distance Vector Routing Protocol i.e. Dynamic Source Routing is capable of maintaining information of the routes between source and destination which makes it slow. If the network is very large containing a number of routes from source to destination, it is difficult for the data packets header to hold whole information of the routes.
- In case of Dynamic Source Routing, multiple routes are present for sending a packet from source to destination but AODV overcomes this disadvantage too.

AODV

- In AODV, along with routing tables of every node, two counters including Sequence Number(SEQ NO) and broadcast ID are maintained also.
- The destination IP is already known to which data is to be transferred from source. Thus, the destination Sequence Number(SEQ NO) helps to determine an updated path from source to destination.
- Along with these counters, Route Request(RREQ) and Route Response(RRESP) packets are used in which RREQ is responsible for discovering of route from source to destination and RRESP sends back the route information response to its source.

AODV working

- In Ad-Hoc On Demand Distance Vector Routing, the source node and destination nodes IP addresses are already known.
- The goal is to identify, discover and maintain the optimal route between source and destination node in order to send/receive data packets and informative.
- Each node comprises of a routing table along with below mentioned format of Route Request(RREQ) packet.
- RREQ { Destination IP, Destination Sequence Number, Source IP, Source Sequence Number, Hop Count}

- Consider a network containing 5 nodes that are “X”, “Y”, “Z”,”T”,”D” present at unit distance from each other, where “X” being the source node and “D” being the destination node.

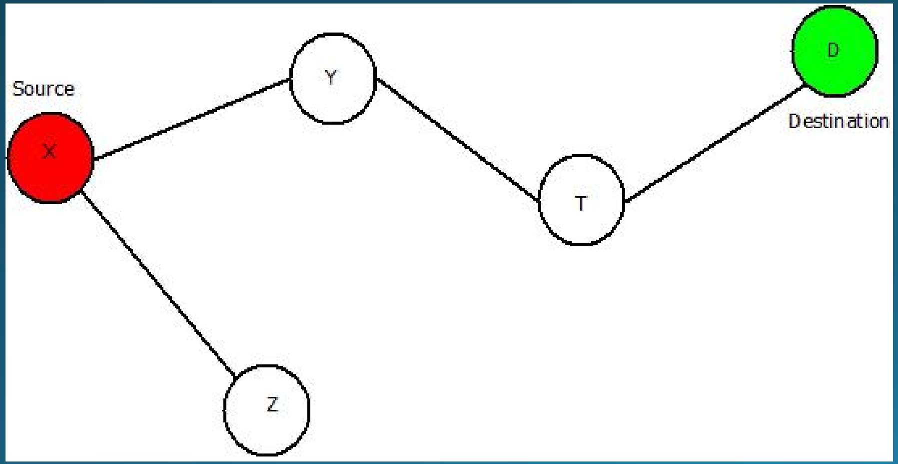
The IP addresses of source node "X" and destination node "D" is already known. Below mentioned steps will let you know how AODV works and concept of Route Request(REREQ) and Route Response(RRESP) is used.

Step 1: Source node "X" will send Route Request i.e. RREQ packet to its neighbours "Y" and "Z".

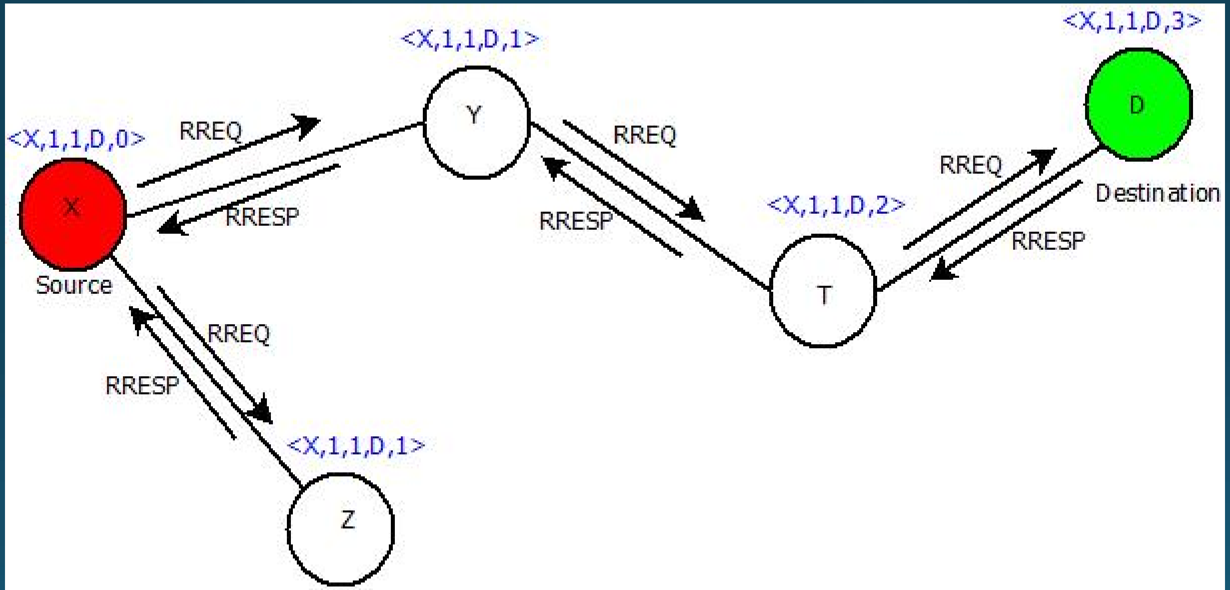
Step 2: Node "Y" & "Z" will check for route and will respond using RRESP packet back to source "X". Here in this case "Z" is the last node but the destination. It will send the RREQ packet to "X" stating "Route Not Found". But node "Y" will send RRESP packet stating "Route Found" and it will further broadcast the RRESP to node "T".

Step 3: Now the field of net hop in the RREQ format will be updated, Node "T" will send back the "Route Found" message to Node "Y" and will update the next hop field further.

Step 4: Then Node "T" will broadcast and RREQ packet to Node "D", which is the destination and the next hop field is further updated. Then it will send RRES packet to "T" which will further be sent back to the source node "X" via node "Y" and Node "T" resulting in generation of an optimal path. The updated network would be:



Adhoc on demand DSR network

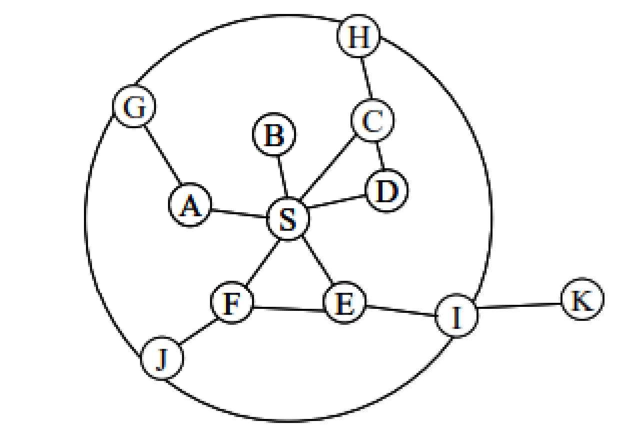


Pros and Cons

- Advantages : Ad-Hoc On Demand Distance Vector Routing Protocol
- Dynamic networks can be handled easily.
- No loop generation.
- Disadvantages : Ad-Hoc On Demand Distance Vector Routing Protocol
- A delayed protocol because of its route discovery process.
- High bandwidth requirement.

Hybrid - **Zone Routing Protocol (ZRP).**

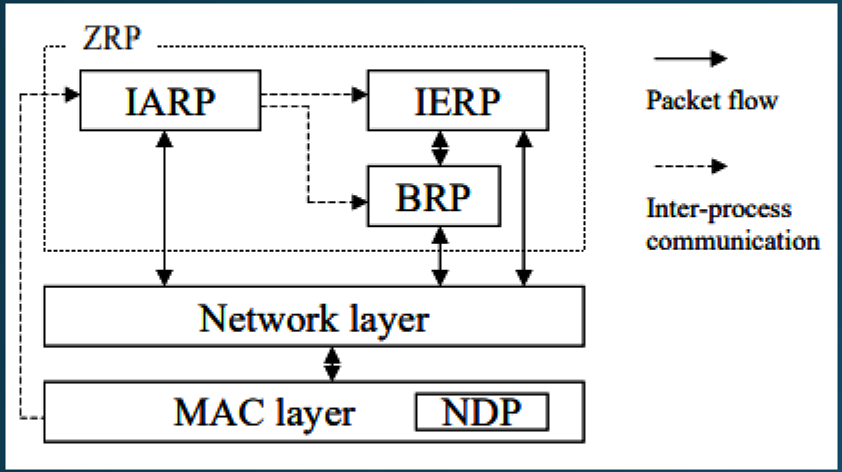
- The Zone Routing Protocol, as its name implies, is based on the concept of zones.
- A routing zone is defined for each node separately, and the zones of neighboring nodes overlap.
- The routing zone has a radius ρ expressed in hops. The zone thus includes the nodes, whose distance from the node in question is at most ρ hops.
- zone is defined in hops, not as a physical distance.



ZRP

- The nodes of a zone are divided into peripheral nodes and interior nodes.
- Peripheral nodes are nodes whose minimum distance to the central node is exactly equal to the zone radius

ZRP Architecture



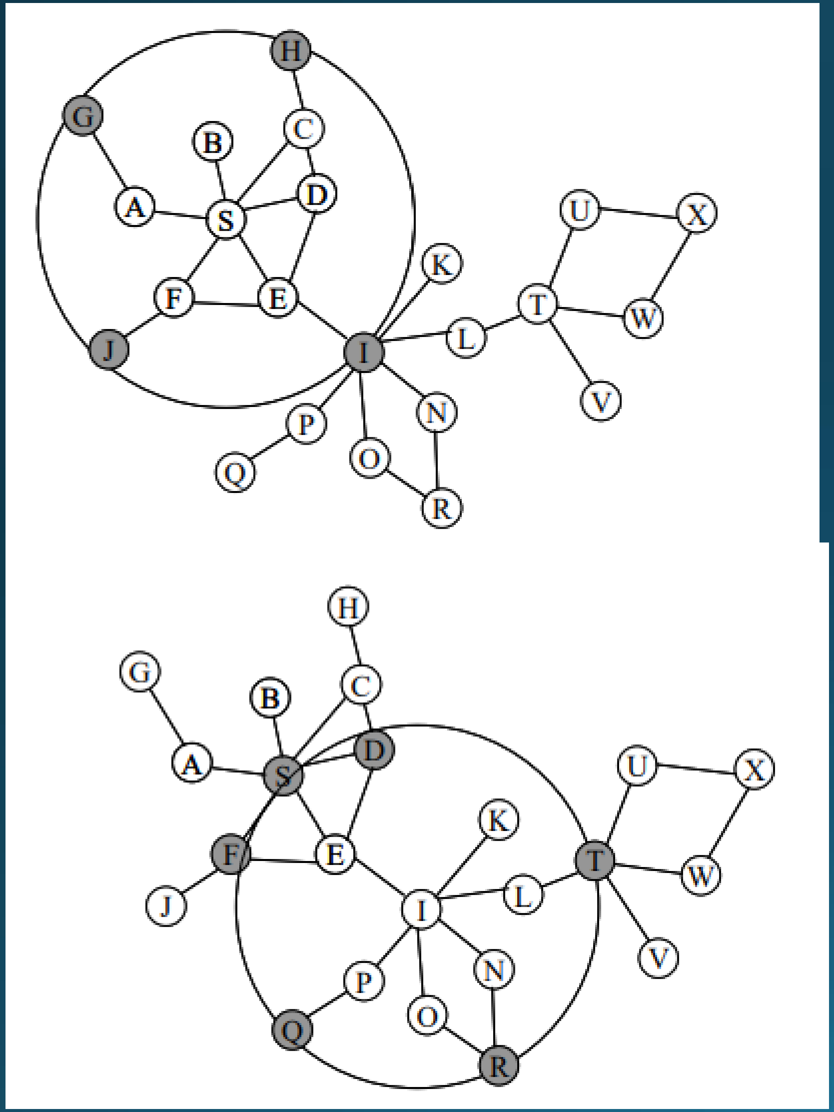
- ZRP refers to the locally **proactive routing** component as the IntrA-zone Routing Protocol **(IARP).**
- The globally reactive routing component is named IntEr-zone Routing Protocol (IERP).
- IARP is a family of limited-depth, proactive link-state routing protocols. IARP maintains routing information for nodes that are within the routing zone of the node.
- IERP is a family of reactive routing protocols that offer enhanced route discovery and route maintenance services based on local connectivity monitored by IARP.

Routing using ZRP

- A node that has a packet to send first checks whether the destination is within its local zone using information provided by IARP. In that case, the packet can be routed proactively.

- Reactive routing is used if the destination is outside the zone.

Example



The node S has a packet to send to node X. The zone radius is ρ=2.

- The node uses the routing table provided by IARP to check whether the destination is within its zone.
- Since it is not found, a route request is issued using IERP. The request is broadcast to the peripheral nodes (gray in the picture).
- Each of these searches their routing table for the destination
- Node I does not find the destination in its routing table. it broadcasts the request to its peripheral nodes.
- query control mechanisms, the request is not passed back to nodes D, F and S.
- Finally, the route request is received by node T, which can find the destination in its routing zone.
- Node T appends the path from itself to node X to the path in the route request. A route reply, containing the reversed path is generated and sent back to the source node.

Wireless Sensor Networks

Unit 4

Topics

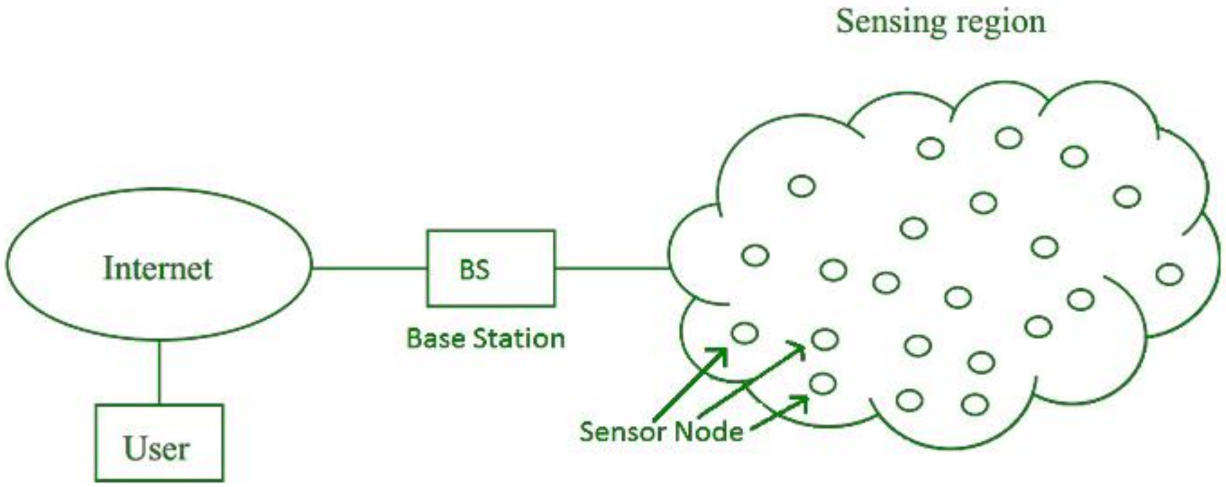
- Wireless sensor networks Concepts
- Basic architecture
- design objectives and applications
- Sensing and communication range
- Coverage and connectivity;
- Sensor placement;
- Data relaying and aggregation;
- Energy consumption;
- Clustering of sensors;
- Energy efficient Routing (LEACH).

Concept of WSN

- Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner
- Used to monitor the system, physical or environmental conditions.
- Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area.
- Nodes are connected to the Base Station which acts as a processing unit in the WSN System.
- Base Station in a WSN System is connected through the Internet to share data.

WSN-Components

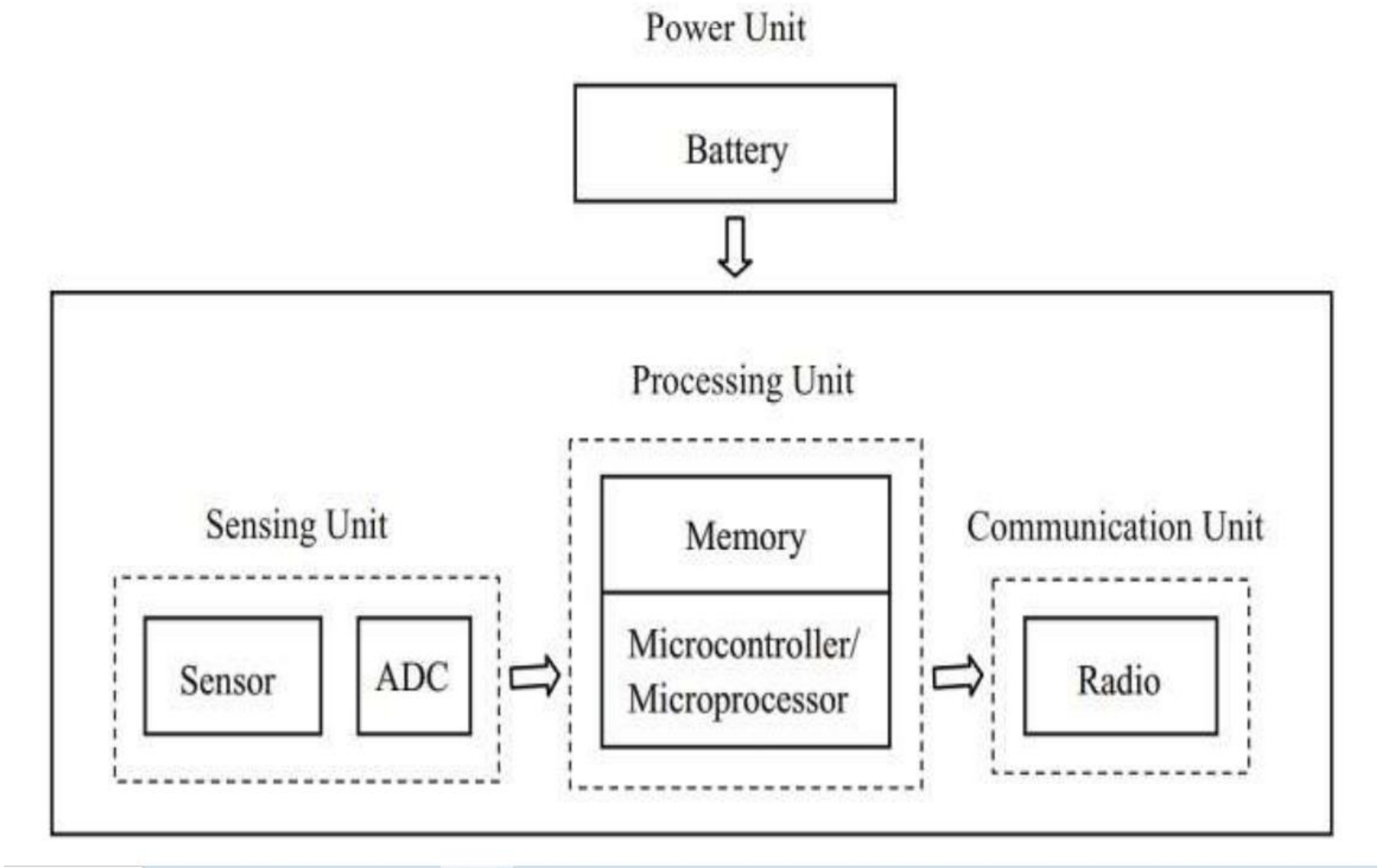
Sensors:
Sensors in WSN are used to capture the environmental variables and which is used for data acquisition.
Radio Nodes:
It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.
WLAN Access Point:
It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.
Evaluation Software:
The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.



WSN Components

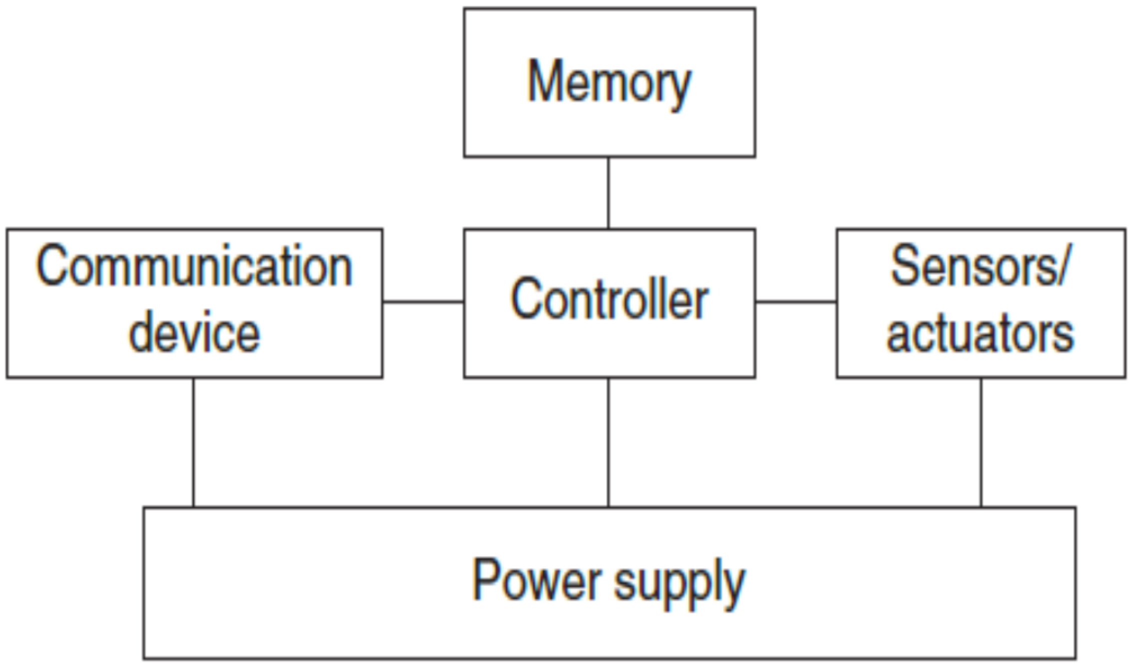
- A typical wireless sensor network can be divided into two elements. They are:
  - – Sensor Node
  - – Network Architecture
- A Sensor Node in a WSN consists of four basic components. They are:
  - – Power Supply
  - – Sensor
  - – Processing Unit
  - – Communication System

WSN Components



Overview of Sensor Node

- Controller: To process all relevant data
- Memory: To store programs and intermediate data.
- Sensors and actuators: Actual interface to the physical world to observe or control physical parameters of the environment.
- Communication: Device for sending and receiving information over a wireless channel
- Power supply: Some form of batteries necessary to provide energy and some form of recharging by obtaining energy from the environment as well.



Controller-core of a wireless sensor node.

- It is the Central Processing Unit (CPU) of the node
- It collects data from sensors, processes this data, receives data from other sensor nodes, and decides on the actuator's behavior.
- It has to execute various programs, ranging from time critical signal processing and communication protocols to application programs.
- Microcontrollers are suitable for WSNs since they can reduce their power consumption by going into sleep states where only parts of the controller are active

Memory in WSN

- There is a need for Random Access Memory (RAM) to store intermediate sensor readings, packets from other nodes etc.
- RAM is fast, but it loses its contents if power supply is interrupted.
- The program code can be stored in Read-Only Memory (ROM) or in Electrically Erasable Programmable ReadOnly Memory (EEPROM) or flash memory.
- Flash memory can also serve as intermediate storage of data when the power supply goes off for some time.

Communication Module

- The transmission medium
  - radio frequencies
  - Optical
  - Communication
  - ultrasound.
- Radio Frequency (RF)-based communication is vital requirement of most WSN applications.
  - It provides long range and high data rates, acceptable error rates at reasonable energy expenditure
  - does not require line of sight between sender and receiver.
- For a practical wireless, RF-based system, the carrier frequency has to be carefully chosen.
- The wireless sensor networks use communication frequencies between about 433 MHz and 2.4 GHz.

Transceivers

- For actual communication, both a transmitter and a receiver are required in a sensor node to convert a bit stream coming from a microcontroller and convert them to and from radio waves. Such combined devices are called transceivers.
- half-duplex operation is realized since transmitting and receiving at the same time on a wireless medium is impractical in most cases.

Types of Sensors

- **Passive Omni-directional sensors**: They can measure a physical quantity at the point of the sensor node without manipulating the environment by active probing. They obtain the energy directly from the environment – energy is only needed to amplify their analog signal. Typical examples include thermometer, light sensors, vibration, microphones, humidity, chemical sensors etc
- **Passive narrow-beam sensors**: They are passive but have a well-defined notion of direction of measurement. A typical example is a camera, which can “take measurements” in a given direction, but has to be rotated if need be.
- **Active sensors**: They probe the environment, for example, a sonar or radar sensor or some types of seismic sensors, which generate shock waves by small explosions.

Power Supply to sensor nodes

Traditional batteries - The power source of a sensor node is a battery, either non-rechargeable (primary batteries) or, if an energy scavenging device is present on the node, also rechargeable (secondary batteries).

Energy scavenging

- Some of the unconventional energy sources like fuel cells, micro heat engines and radioactivity – convert energy from stored secondary form into electricity in a easy way than a normal battery would do.
- The entire energy supply is stored on the node itself once the fuel supply is exhausted, the node fails.
- The energy from a node’s environment must be tapped into and made available to the node – energy scavenging should take place.

Power Supply to sensor nodes

- **Photo-voltaics** The solar cells can be used to power sensor nodes. The available power depends on whether nodes are used outdoors or indoors, and on time of day.
- **Temperature gradients** Differences in temperature can be directly converted to electrical energy.
- **Vibrations** Walls or windows in buildings are resonating with cars or trucks passing in the streets, machinery often has low- frequency vibrations, ventilations also cause it, and so on.

Applications of WSN

- Industrial Process Monitoring
- Health Monitoring
- Intelligent Agriculture and Environment Sensing
- Asset Tracking Supply chain management
- Military / security applications
- Home Automation

Network Performance Objectives

1. Low Power Consumption

- Wireless sensor network applications typically require network components with average power consumption that is substantially lower than currently provided in implementations of existing wireless networks such as Bluetooth.

2. Low Cost

3. Data Throughput

4. Message Latency

5. Security

6. World Wide Availability

Sensor Network Architecture

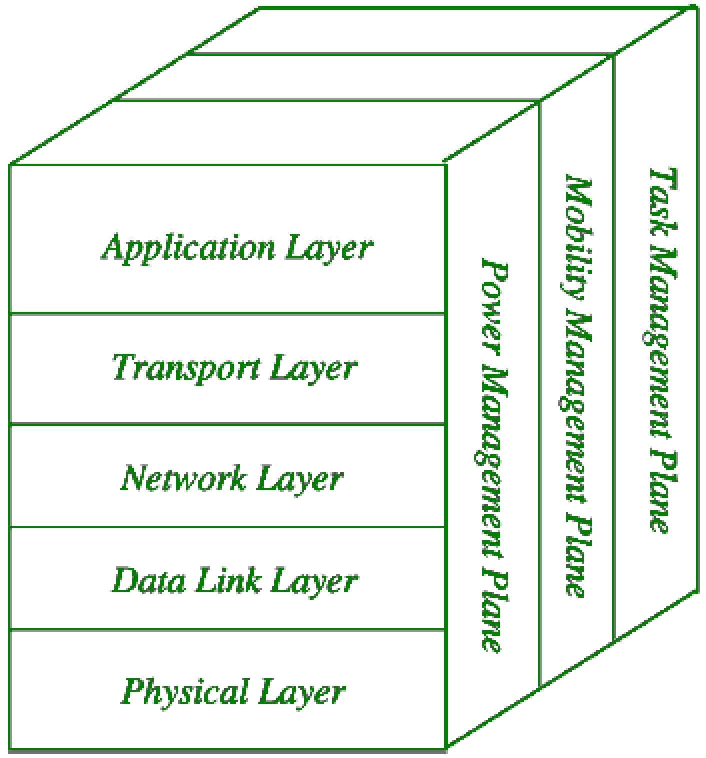
- It can be used in various places like schools, hospitals, buildings, roads, etc for various applications like disaster management, security management, crisis management, etc.
- There are 2 types of architecture used in WSN:
  - Layered Network Architecture,
  - Clustered Architecture.

. Layered Network Architecture:

Layered Network Architecture makes use of a few hundred sensor nodes and a single powerful base station. Network nodes are organized into concentric Layers. It consists of 5 layers and three cross layers.

The 5 layers are:

1. Application Layer
2. Transport Layer
3. Network Layer
4. Data Link Layer
5. Physical Layer



Advantages of Layered Architecture

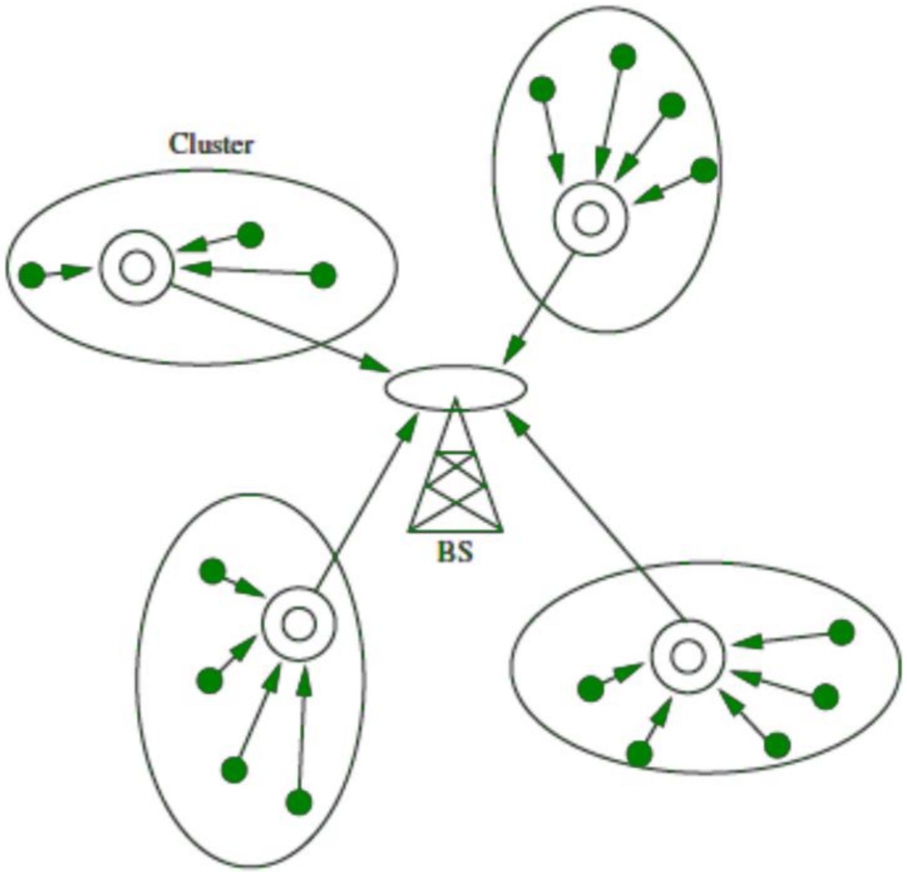
- Each node participates only in short-distance, low power transmissions to nodes of the neighbouing nodes because of which power consumption is less as compared to other Sensor Network Architecture.
- It is scalable and has a higher fault tolerance.

Clustered Architecture

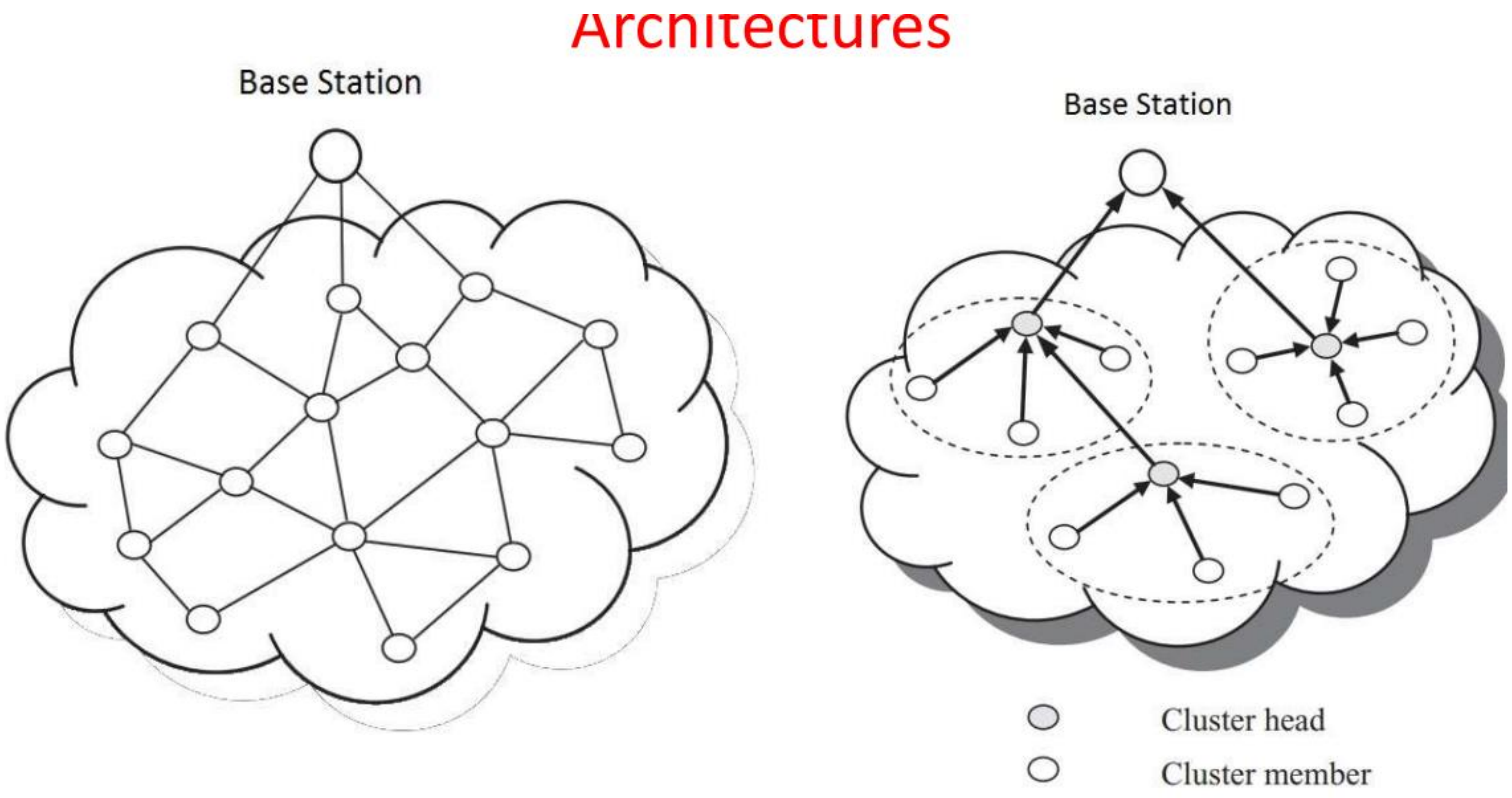
Sensor Nodes autonomously clubs into groups called clusters.
It is based on the *Leach Protocol* which makes use of clusters.
Leach Protocol stands for Low Energy Adaptive Clustering Hierarchy.

Properties of Leach Protocol:

- It is a 2-tier hierarchy clustering architecture.
- It is a distributed algorithm for organizing the sensor nodes into groups called clusters.
- The cluster head nodes in each of the autonomously formed clusters create the Time-division multiple access (TDMA) schedules.
- It makes use of the concept called *Data Fusion* which makes it energy efficient.



WSN Architectures-Flat and Hierarchical



Types of WSN

- Terrestrial WSNs
- Underground WSNs
- Underwater WSNs
- Multimedia WSNs
- Mobile WSNs

Topologies in WSN

1. Star Topology
    - In star topology, there is a single central node known as hub or switch and every node in the network is connected to this hub.
    - Star topology is very easy to implement, design and expand.
    - The data flows through the hub and plays an important role in the network and a failure in the hub can result in failure of entire network.

Topologies in WSN

2. Tree Topology

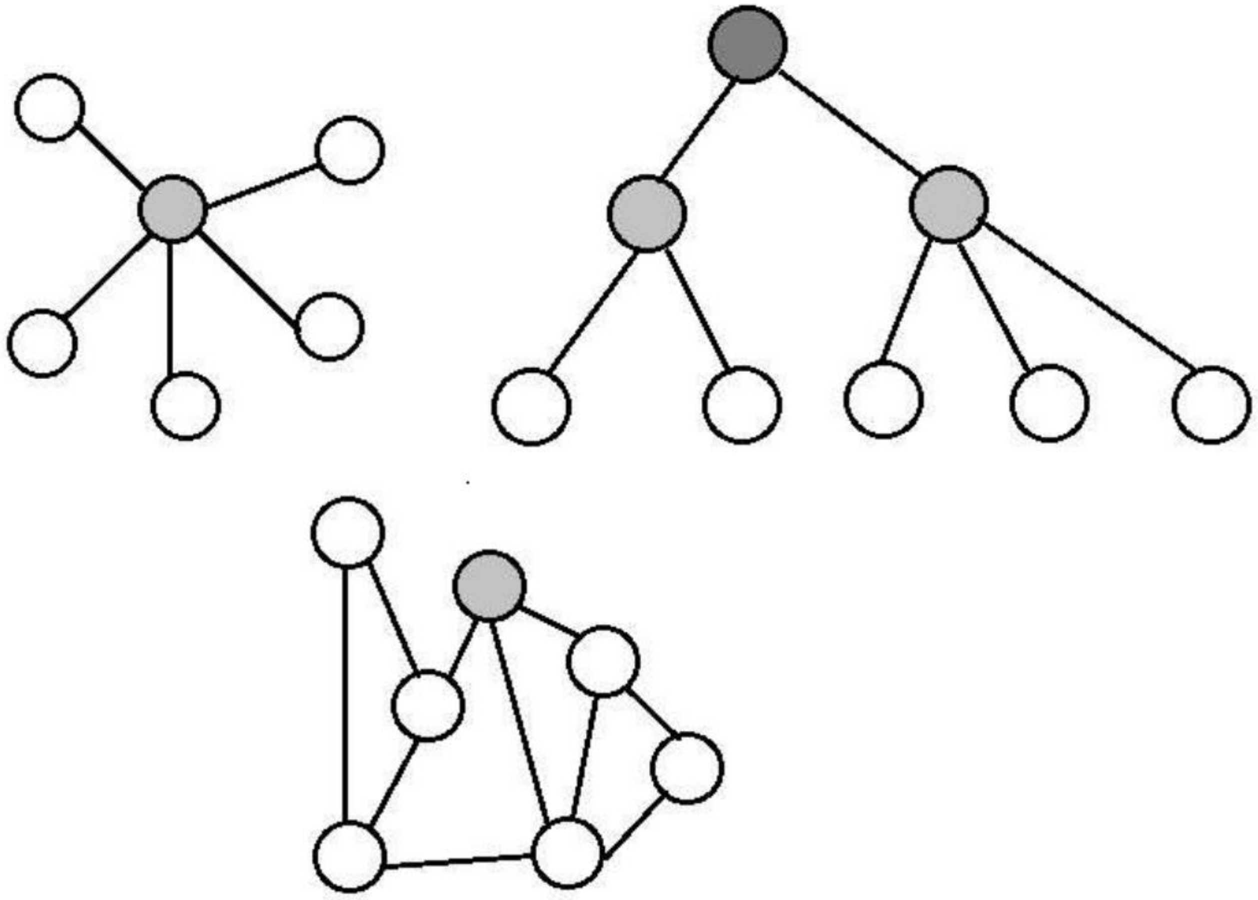
- A tree topology is a hierarchical network where there is a single root node at the top and this node is connected to many nodes in the next level and continues.
- The processing power and energy consumption is highest at the root node and keeps on decreasing as we go down the hierarchical order.

Topologies in WSN

3. Mesh Topology

- In mesh topology, apart from transmitting its own data, each node also acts as a relay for transmitting data of other connected nodes.
- Mesh topologies are further divided into Fully Connected Mesh and Partially Connected Mesh.
- In fully connected mesh topology, each node is connected to every other node while in partially connected mesh topology, a node is connected one or more neighboring nodes.

Topologies in WSN



Characteristics of WSN

- Type of service
- Quality of service
- Fault tolerance -The redundant deployment is necessary for WSN to tolerate the node failure and using more number of nodes will be necessary even if all nodes functioned correctly.
- Scalability
- Lifetime -the time until the first node fails as the network lifetime.
- Range of densities -the number of nodes per unit area that is the density of the network
- Programmability
- Maintainability -WSN has to monitor its own health and status to change operational parameters

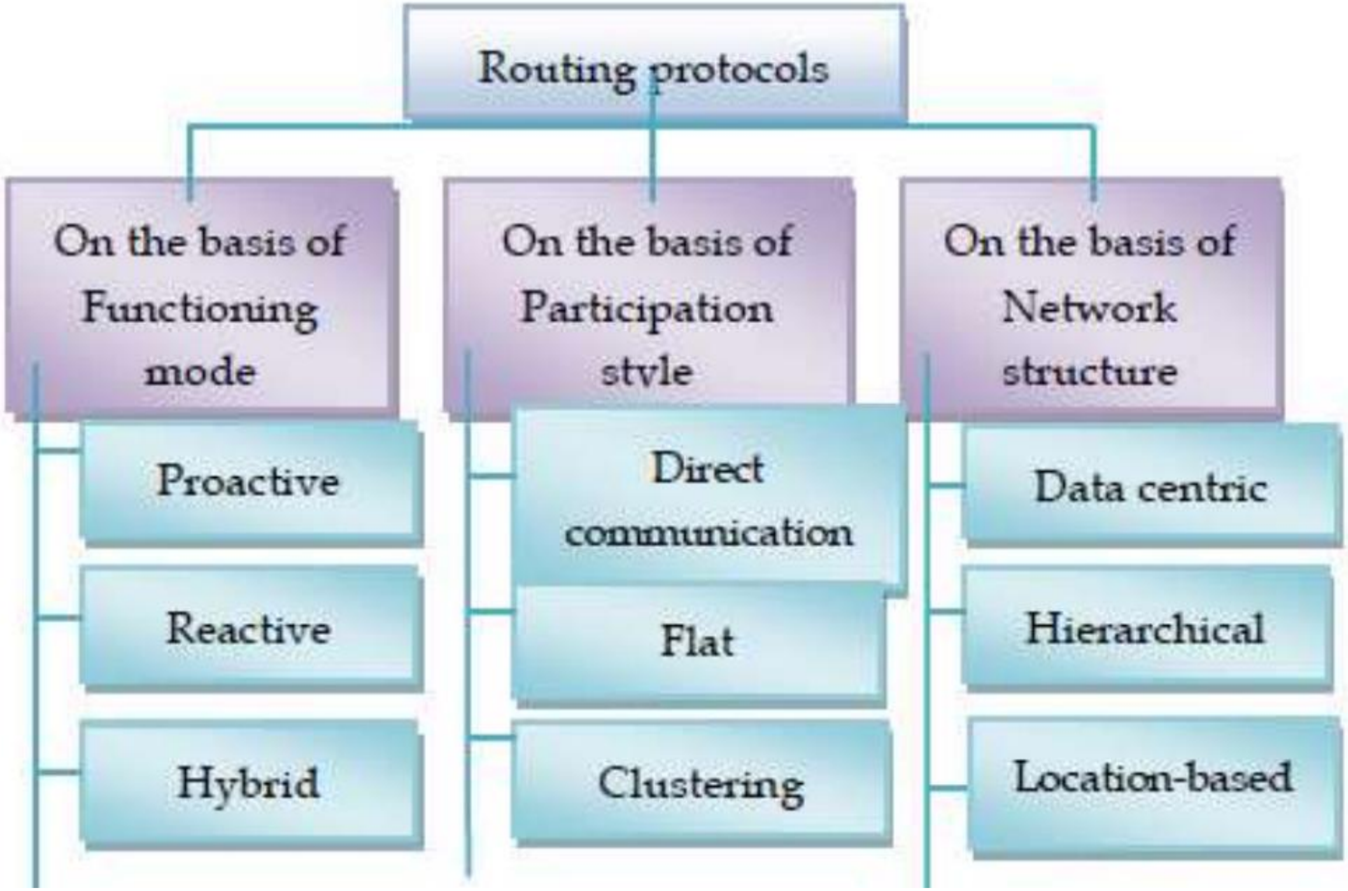
Address Centric v//s Data Centric

- Address centric - Traditional communication **networks are centered** around the **transfer of data** between two devices, equipped with network address
- Data Centric –
  - In a WSN, the nodes are deployed to protect against node failures or to compensate for the low quality of a single node's actual sensing equipment.
  - data-centric interaction will be to **request the average temperature** in a given location area, as opposed to requiring temperature readings from individual nodes.

Routing in WSN

- Routing strategies are required for transferring data between the sensor nodes and the base station.
- Routing in WSN is different than traditional IP network routing because it exhibits a number of unique characteristics to build a global addressing scheme for a large number of sensor nodes.
- Different routing techniques are proposed for remote sensor network and these conventions can be classifiedas per different parameters.

Routing Protocols



Routing types

- Direct Communication protocols: In this type of protocols the information sensed by nodes is sent directly to Base Station (BS). Example: SPIN
- Flat protocols: In this, the nodes search for the valid path and then transmit it to Base station. Example: Rumor routing protocol.
- Clustering Protocols: In this, the area is divided into clusters and Cluster heads are assigned to each cluster. All the nodes in the cluster send data to corresponding cluster heads and then cluster head sends it to Base station. Example: TEEN

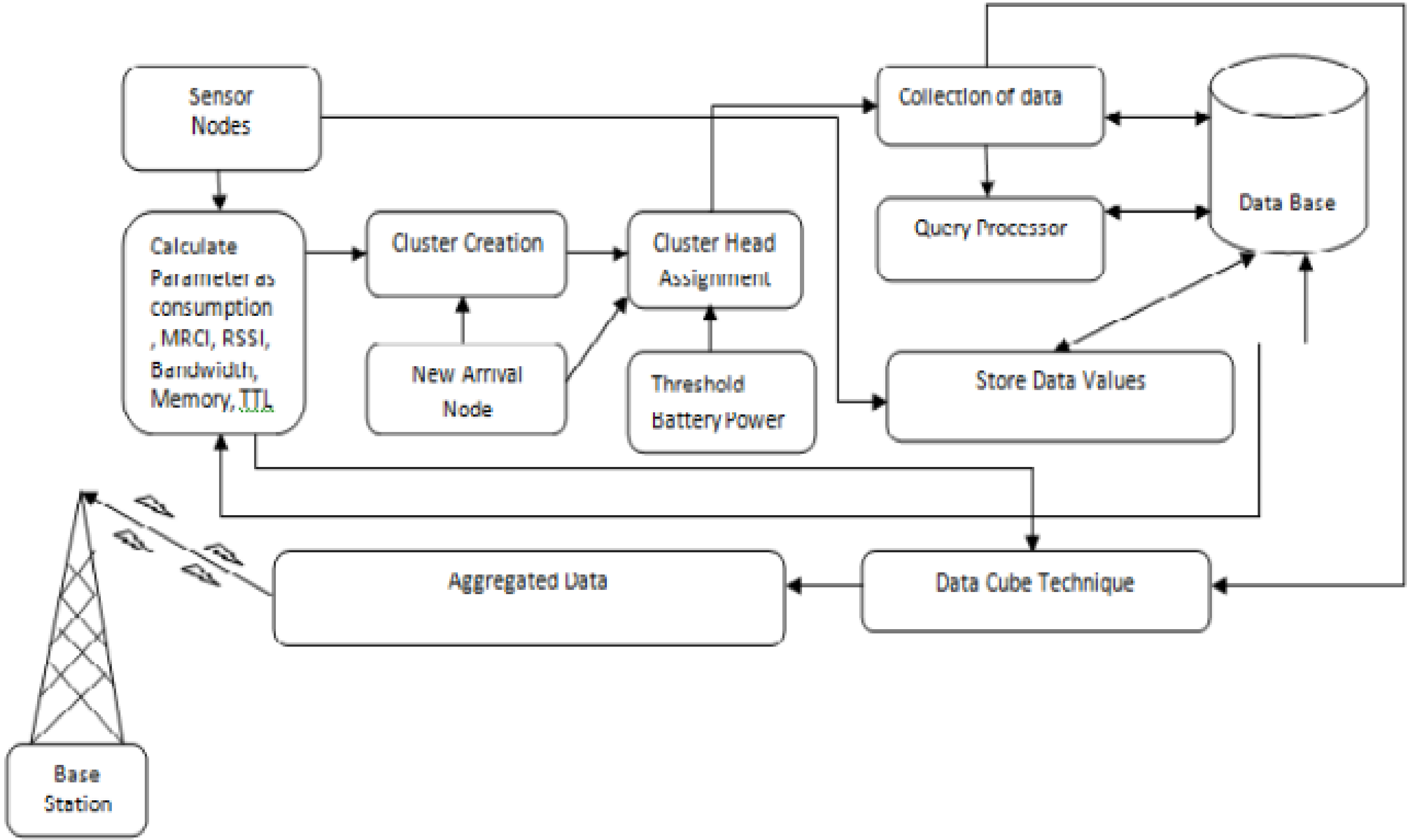
Network-based routing protocols

1. **Data Centric protocols**: These are **query based** and they depend on the naming of the desired data. The **BS sends queries** within a certain region to get information and waits for a reply from the nodes. Nodes in a particular region collect the specific data based upon the queries. Example: SPIN.
2. **Hierarchical protocols**: In this, the **nodes** with **lower energy** are used to **capture** information and nodes with **higher energies** are used to **process, transfer it** and it is used to perform energy efficient routing. Example: TEEN, APTEEN.
3. **Location Based**: In these, the **location of nodes** must be known to find an **optimal path** using flooding. To get the information about location of a particular node GPS is used. Example: GEAR.

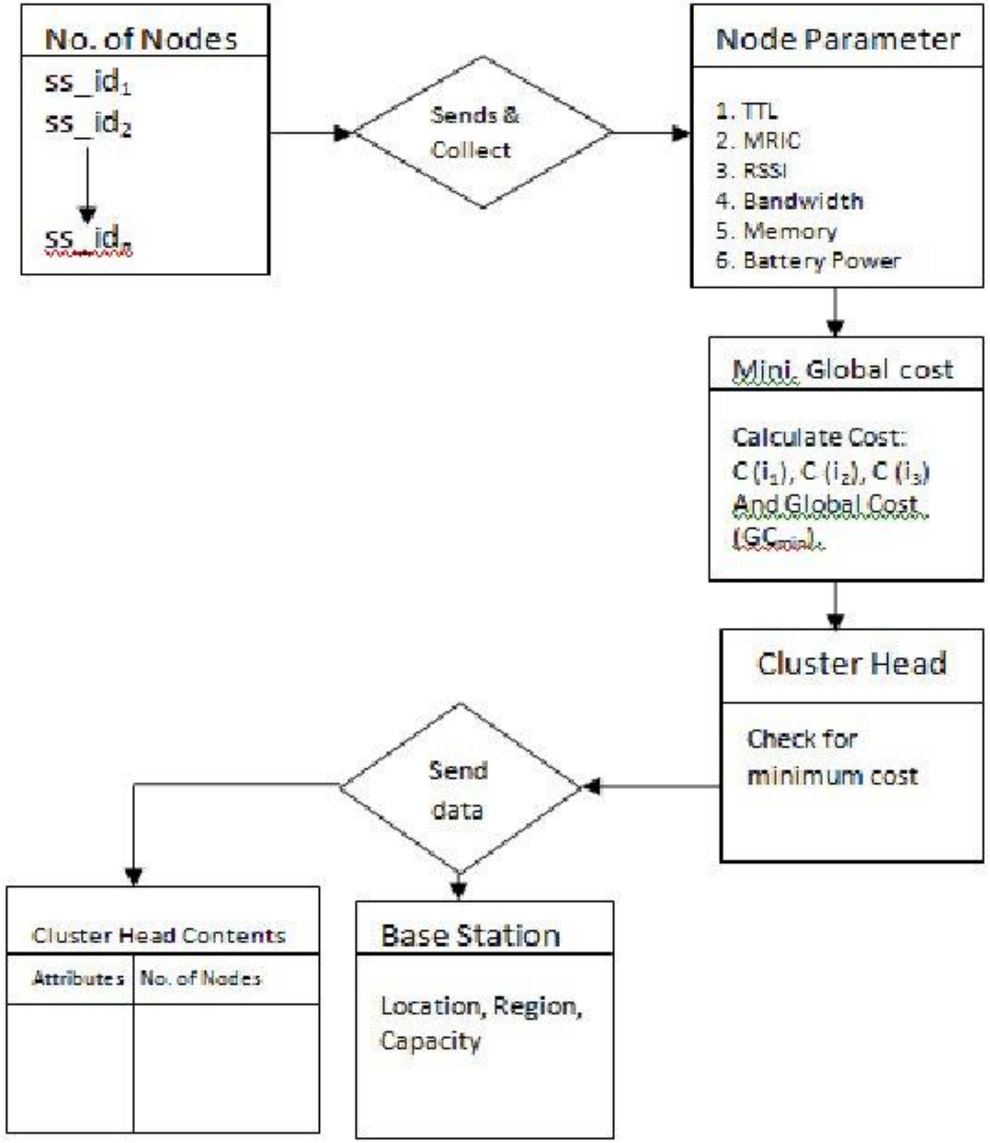
Routing Types

- **Energy efficiency** of a network is a significant concern in wireless sensor network. These days networks are becoming large, information gathered is becoming larger, which all consume a great amount of energy resulting in an early death of a node.
- Therefore, many energy efficient protocols are developed to lessen the power used in data sampling and collection to **extend the lifetime of a network.**
- The following are some of energy efficient routing protocols:
  - LEACH
  - PEGASIS
  - TEEN

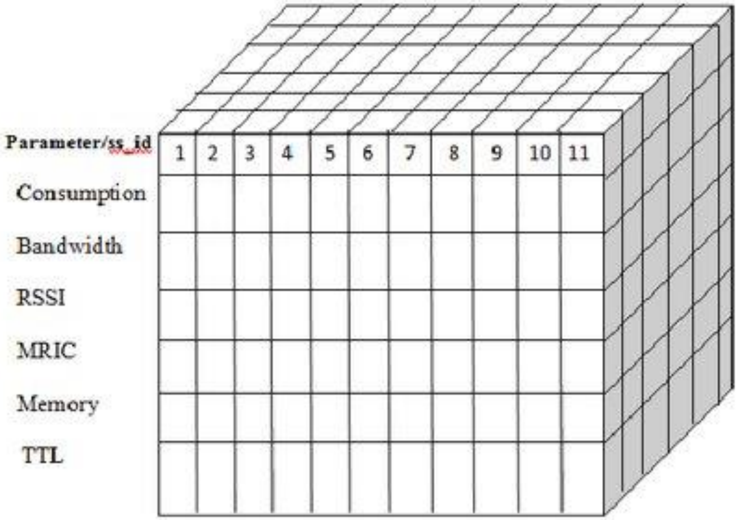
Data Collection and Aggregation



Data Cube Technique of Aggregation



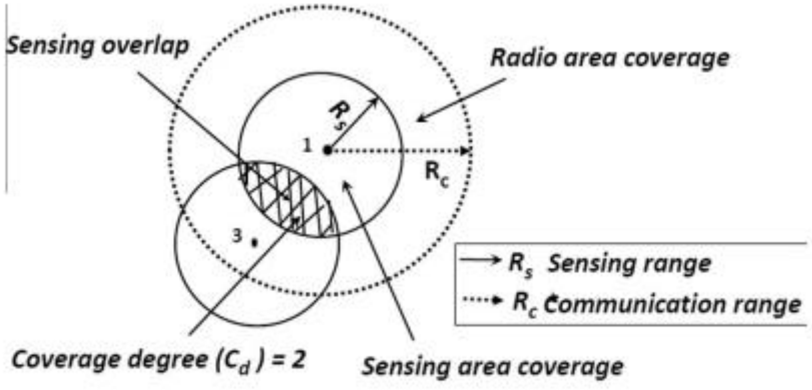
Parameter/ss_id	1	2	3	4	5	6	7	8	9	10	11
Consumption											
Bandwidth											
RSSI											
MRIC											
Memory											
TTL											



Data Aggregation: Working Principle

- starts working by choosing selecting of nodes and divided into clusters. These clusters can satisfy the intended parameter requirements and conditions. The parameters like RSSI, TTL, MRIC, bandwidth, battery consumption are accustomed verify the amount of nodes that will be considered in a cluster.
- a cluster head (CH) is selected among nodes lies within the each cluster. CH are going to be responsible for administration of all different nodes inside several cluster and collecting the data} from the nodes within the cluster and transferring the information to the neighboring cluster head for more information exchange and updation .
- The newly arrived nodes will be assigned as cluster head if the global cost of arrived node is minimum , otherwise other cluster nodes are going to be given opportunity to participate and global cost is once more recalculated.
- thereafter the data aggregation approach is presumed as the collection of data and numerous queries from the user end are checked and transformed into low level schemes by a query processor.
- All data collected and aggregated is stored at a storage location in database server.

Sensing and Communication range of sensor node



- Coverage degree (Cd) refers to the number of sensor nodes actively monitoring an area. Cd = n means n sensors are actively monitoring an area.
- Sensing void or hole occurs when no sensor actively monitors an area.
- To maximize the network lifetime it is essential to minimize the number of ACTIVE nodes while still achieving maximum possible sensing and radio coverage

- The sensing area coverage (or sensing coverage) is the region that a node can **observe or monitor** within its sensing range.
- The network coverage could be interpreted as the collective **coverage by all the ACTIVE sensor nodes** in the WSN.
- sensor node has a radio area coverage based on its communication range (Rc). The radio coverage bounded by Rc, is the region or area within which an **ACTIVE sensor node can communicate** with at least one other sensor node.
- Sensing coverage ensures proper event monitoring while radio coverage ensures proper data transmission within the WSN

Coverage

- Sensors are prone to be failure.
- The over-loading of working sensor nodes will cause easily exhausted and failed.
- In addition to possible hardware or software malfunctions, sensors may fail because of severe weather conditions or other hash physical environment in the sensor filed.
- It is therefore crucial to construct a fault-tolerant WSN that will continuously provide needed services despite sensor failures. This is the fault-tolerance requirement.

Coverage

The fault-tolerance requirement includes two types:

- coverage fault-tolerance
- connectivity fault-tolerance.

- The sensor coverage problem can be further divided
  - single coverage - In single coverage, each target or point in the area must be monitored by at least one working sensor
  - multiple coverage - In multiple coverage, each target or point in the area needs to be monitored by at least k different working sensors, which is called as the flat k-area-coverage problem for area coverage.

Area Coverage Problem

- A set of sensors are given and distributed over a geographical region to monitor a given area, an area coverage problem is to find a minimum number of sensors to work such that each physical point in the area is-
  - monitored by at least a working sensor.

Connected Area Coverage Problem

- A set of sensors are given and distributed over a geographical region to monitor a given area, an m-connected k-coverage problem is to find a minimum number of sensors to work such that each physical point in the area is-
  - monitored by at least k active sensors and
  - the active sensors form a m-connected graph

PEAS(**probing environment and adaptive sleeping**), a distributed, probing-based density control algorithm for robust sensing coverage.

- A **subset of sensor nodes** operative mode maintains coverage while **others** are put into sleep.
- Each sensor node has the same **probing range Rp** and may vary its transmission power and choose a power level to cover a circular area given a radius.
- In PEAS, each node has three operation modes:
  - **sleeping, probing and working.**
- Initially all sensor nodes are in the sleeping mode. Each node sleeps for an exponentially distributed duration generated according to a probability density function (PDF).
- When **sleeping time expires**, the **sensor enters the probing mode**.
- The **probing node** uses an **appropriate transmission power** to broadcast a PROBE message within its local probing range Rp.
- Any **working node(s)** within that range should **respond with a REPLY message**, also sent within the range of Rp. If the probing node **hears a REPLY**, it **goes back to the sleeping mode** for another random period of time.
- If the probing node does not hear any REPLY, it enters the working mode and starts monitoring until it fails or consumes all its energy

Clustering of Sensors

- Clustering of nodes plays an important role in conserving energy of WSNs.
- Clustering approaches focus on resolving the conflicts arising in effective data transmission.
- Modern energy-efficient clustering approaches to improve the lifetime of WSNs.
  - (i) fuzzy-logic-based cluster head election,
  - (ii) efficient sleep duty cycle for sensor nodes,
  - (iii) hierarchical clustering, and
  - (iv) estimated energy harvesting.
- Classical clustering approaches such as low energy adaptive clustering hierarchy (LEACH) is used.

LEACH

- LEACH is a hierarchical protocol in which most nodes transmit to cluster heads, and the cluster heads aggregate and compress the data and forward it to the base station (sink).
- Each node uses a stochastic algorithm at each round to determine whether it will become a cluster head in this round.
- LEACH assumes that each node has a radio powerful enough to directly reach the base station or the nearest cluster head, but that using this radio at full power all the time would waste energy.
- LEACH also uses CDMA so that each cluster uses a different set of CDMA codes, to minimize interference between clusters.
- LEACH addresses the **overloading of clusters** and it rotates the role of cluster heads among the sensor nodes present in a cluster.
- The significant **drawback** of this approach is that no weightage is given for the residual energy of the sensor nodes.

Unit 4:Cognitive Radio Networks

Preeti Godabole

Contents

- Fixed and dynamic spectrum access;
- Direct and indirect spectrum sensing;
- Spectrum sharing;
- Interoperability and co-existence issues;
- Applications of cognitive radio networks.

What is CR

- Cognitive radio (CR) is a form of wireless communication in which a transceiver
  - intelligently detect which communication channels are in use and which ones are not.
  - The transceiver then instantly moves into vacant channels, while avoiding occupied ones.
  - Helps to optimize the use of the available radio frequency (RF) spectrum.
  - minimizes interference to other users, by avoiding occupied channels, it increases spectrum efficiency and improves the quality of service (QoS) for users.

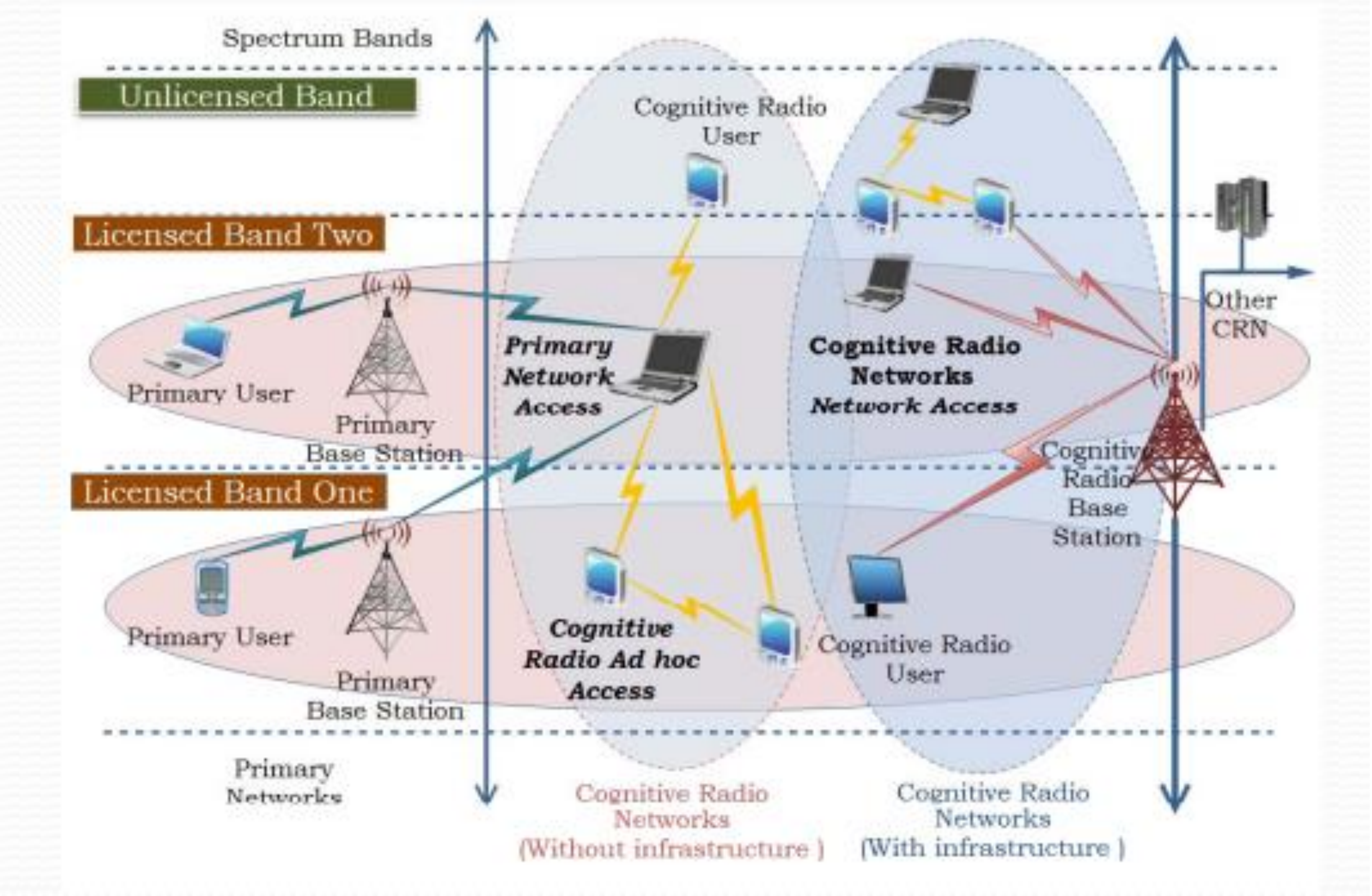
Wireless RF spectrum

- It is a limited resource, allocated through a licensing process
- The allocated (licensed) spectrum is not always used optimally.
- Some bands are overcrowded (e.g., GSM cellular networks), others are relatively unused (e.g., military).
- spectrum inefficiency limits the amount of data that can be transmitted to users and lowers service quality.
- Cognitive radio is an efficient way to use and share this resource intelligently, optimally and fairly.

cognitive radio network (CRN)

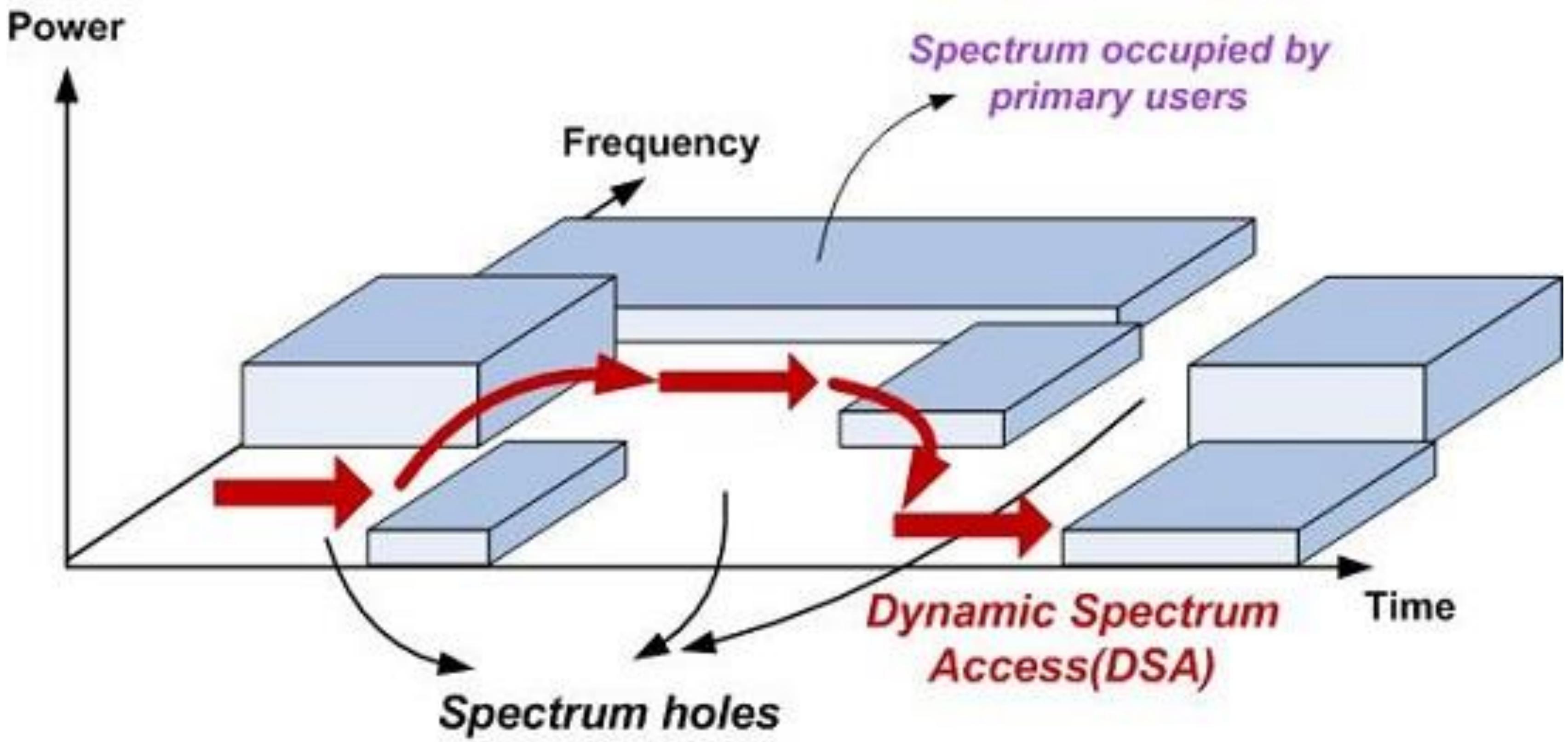
- CRN has two main networks, a primary network and a secondary network.
  - The primary network owns the licensed band and consists of the primary radio base station and users.
  - The secondary network shares the unused spectrum with the primary network. It consists of the cognitive radio base station and users.

- The three key capabilities that differentiate cognitive radio from traditional radio are:
  - Cognition: CR understands its geographical and operational environment.
  - Reconfiguration: CR can decide to dynamically and autonomously adjust its parameters.
  - Learning: CR can also learn from the experience, and experiment with new configurations in new situations.



Spectrum Bands
Unlicensed Band
Licensed Band Two
Licensed Band One
Cognitive Radio User
Primary User
Primary Base Station
Primary Network Access
Cognitive Radio Networks Network Access
Other CRN
Cognitive Radio Base Station
Primary User
Primary Base Station
Cognitive Radio Ad hoc Access
Cognitive Radio User
Primary Networks
Cognitive Radio Networks (Without infrastructure)
Cognitive Radio Networks (With infrastructure)

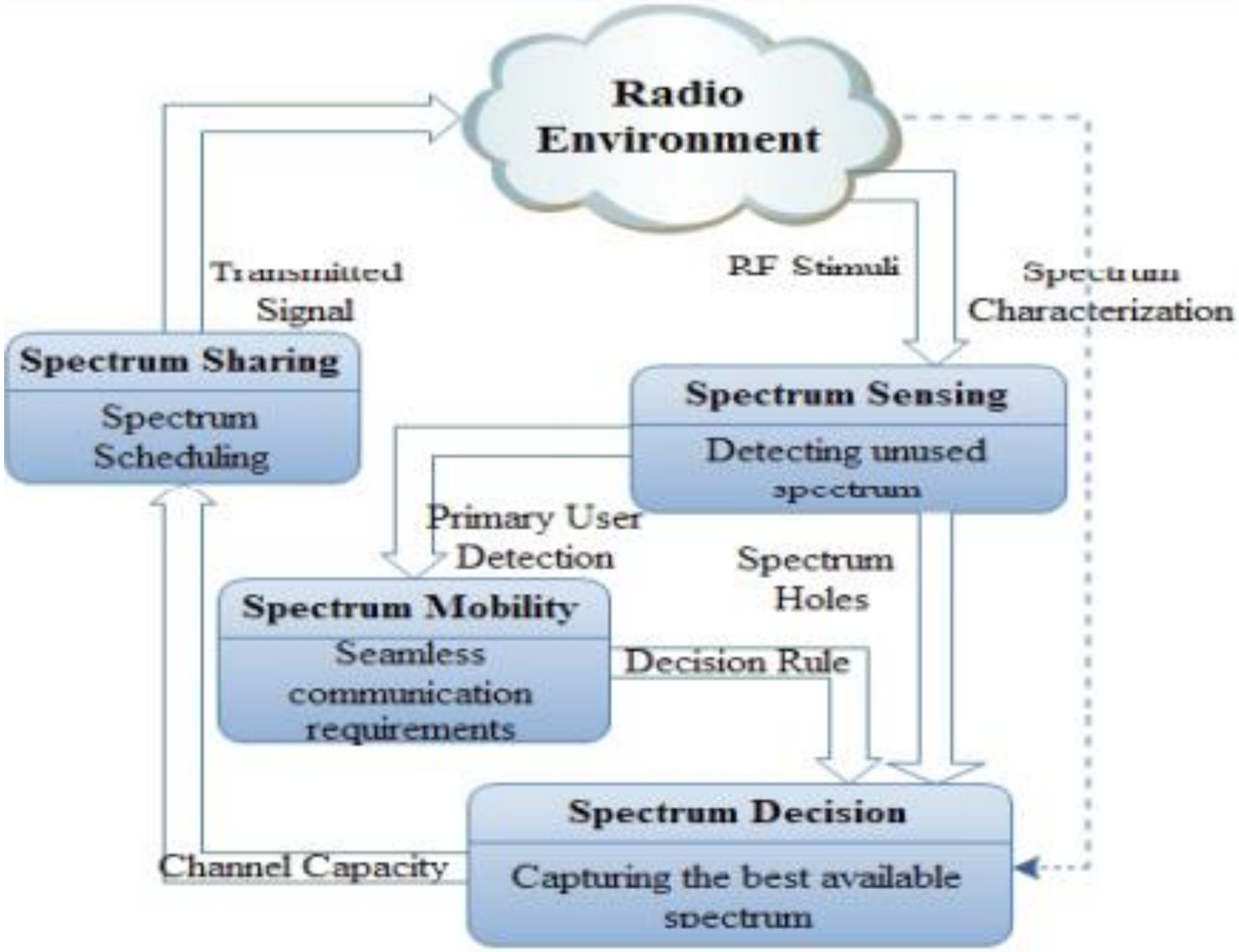
Spectrum Holes



Cognitive radio facets

- *spectrum sensing*
  - CR devices track the spectrum bands in their neighborhoods to identify users licensed to operate in that band.
  - look for unused portions of the RF spectrum known as white spaces or spectrum holes.
  - These holes are created and removed dynamically and can be used without a license.
- *spectrum database*
  - TV stations update their next week's use of the RF spectrum in a database that the FCC maintains. Cognitive radio devices can seek information about free spectrum from this database

CRN Life cycle



spectrum sensing is that the secondary users have to detect the presence of the primary users in the licensed spectrum and quit the frequency band as quickly as possible if the corresponding primary radio emerges so that the primary user does not face any interference.

. The Spectrum sensing techniques are classified into 3 main types,

- Transmitter Detection (Non Cooperative Sensing),
- Cooperative Sensing and
- interference based testing

Applications of CRN

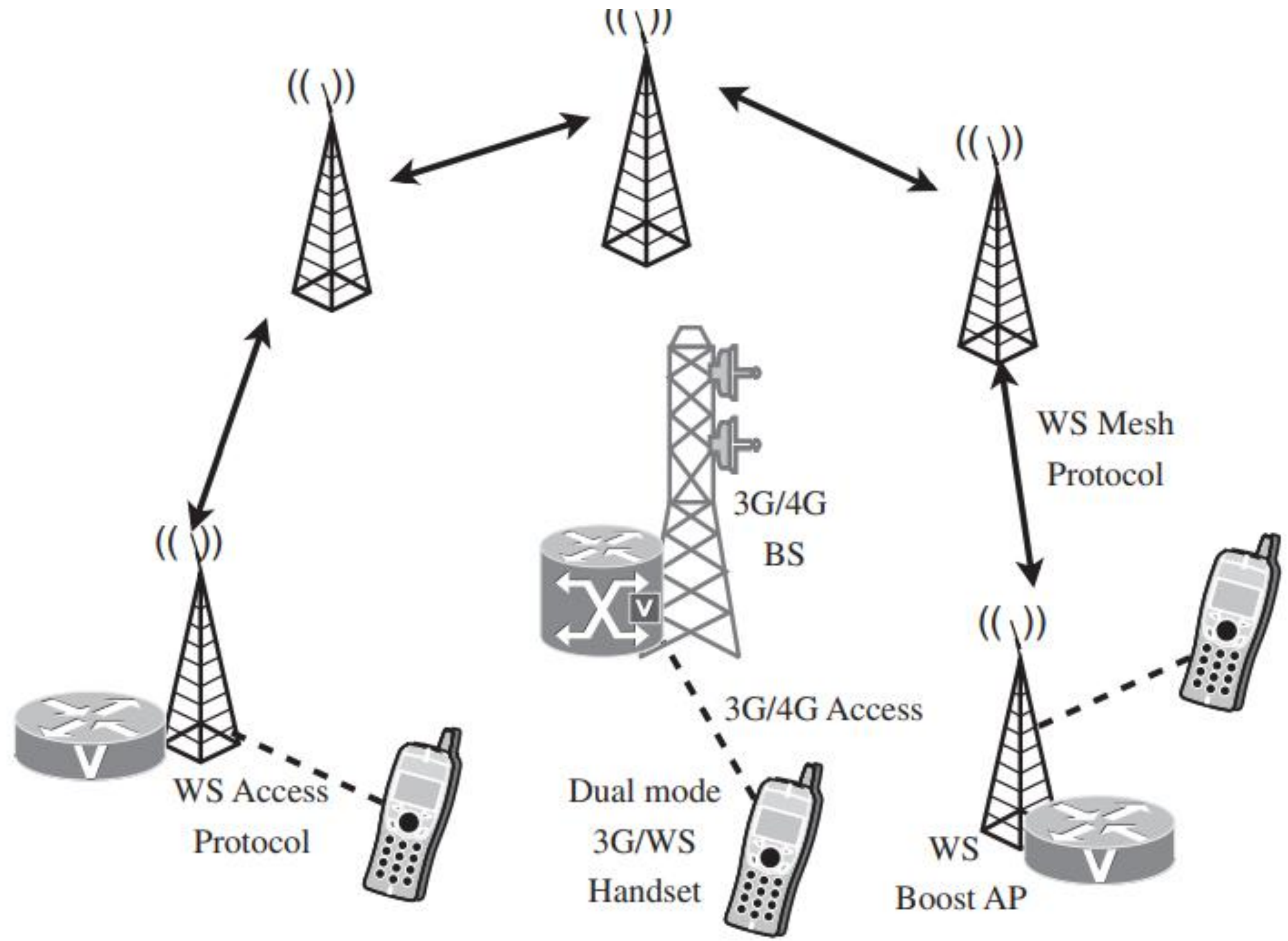
- CR is a disruptive new technology with many potential applications. This is why it is also known as a next-generation communication network.
- For example, CR can help address connectivity problems in rural areas. It can also optimize RF operations for smartphones and IoT devices, content delivery networks, also known as content distribution networks, and giant wireless hotspots.

Types of CRN

- *heterogeneous*
  - In heterogeneous CR, operators run several radio access networks (RANs) using the same or different radio access technology (RAT) protocols.
  - Heterogeneous cognitive radio uses a network-centric approach, and the frequency bands allocated to the various RANs are fixed
- *spectrum-sharing*
  - Several RANs share the same frequency band.
  - They also coordinate with each other to use unoccupied sub-bands intelligently and optimally.

DSA

- **The technique of dynamically accessing the unused spectrum band is known as Dynamic Spectrum Access (DSA)**. The dynamic spectrum access technology helps to minimize unused spectrum bands.
- To regulate the use of this limited resource, fixed spectrum access policy (FSA) was adopted by spectrum regulators. Under this policy, **a fixed piece of spec- trum is assigned for a dedicated purpose which is further distributed to the users for access to wireless services**.


WS Mesh
Protocol
3G/4G
BS
3G/4G Access
WS Access
Protocol
Dual mode
3G/WS
Handset
WS
Boost AP

cognitive radios : alleviate high loads on the cellular network.

- an overlay mesh network of white space hot-spots can carry non-real-time or delay tolerant data like mail, content, file transfer, etc.
- The hot-spots can operate either in the licensed or unlicensed band. Off-loading part of the delay tolerant data traffic from the cellular network helps operators to meet the quality of service (QoS) requirements of delay.
- The boost in the capacity comes at no additional cost, but from the detection of available white spaces and the opportunistic transmission over white spaces using the hot-spot mesh network

Issues in CRN

Interoperability challenges

- – CRN based device-to-device communications
- – CRN based device-to-network communications
- – CRN based machine-to-machine communications
- – CRN based service-to-service communications

Co-existence network technologies challenges

- – CRN based radio access
- – CRN based medium access control (MAC)
- – CRN based handover between multiple communication standards
- – CRN based channel hopping

Communications

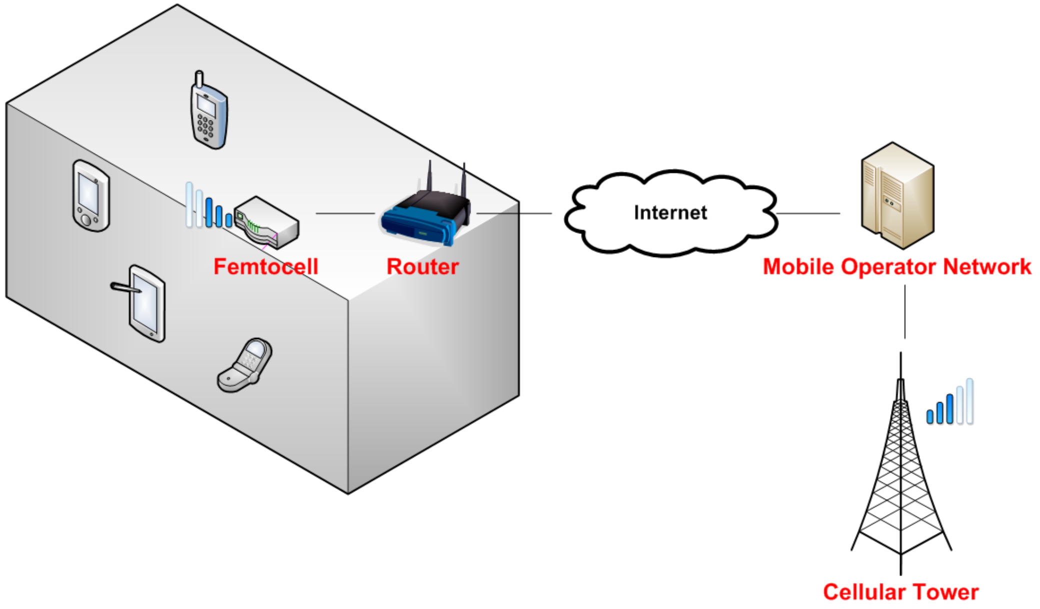
- M2M communications refer to **automated applications which involve machines or devices communicating through a network without human intervention**.
- Device-to-Device (D2D) communication refers to **a radio technology that enables devices to communicate directly with each other, that is without routing the data paths through a network infrastructure**.
- **The client can make a REST call to interact with other services**. The client sends a request to the server and waits for a response from the service (Mostly JSON over HTTP). <Service to service>

Applications of CRN

- It allows constructing a network of radio stations with the combination of cognitive radio nodes hence gives significant boost to the speed and availability of channels for the new secondary wireless networks.
- There are two possibilities to access vacant channel.
  - One, CR contact to multiple non CRs transmissions where femtocells get cognitive inspection, erect and then communicate with non CR mobiles.
  - Two, CR networks would like to contact to the network and operate through the cognitive radio network.

Femto Cells

- In telecommunications, a femtocell is a small, low-power cellular base station, typically designed for use in a home or small business. A broader term which is more widespread in the industry is small cell, with femtocell as a subset.

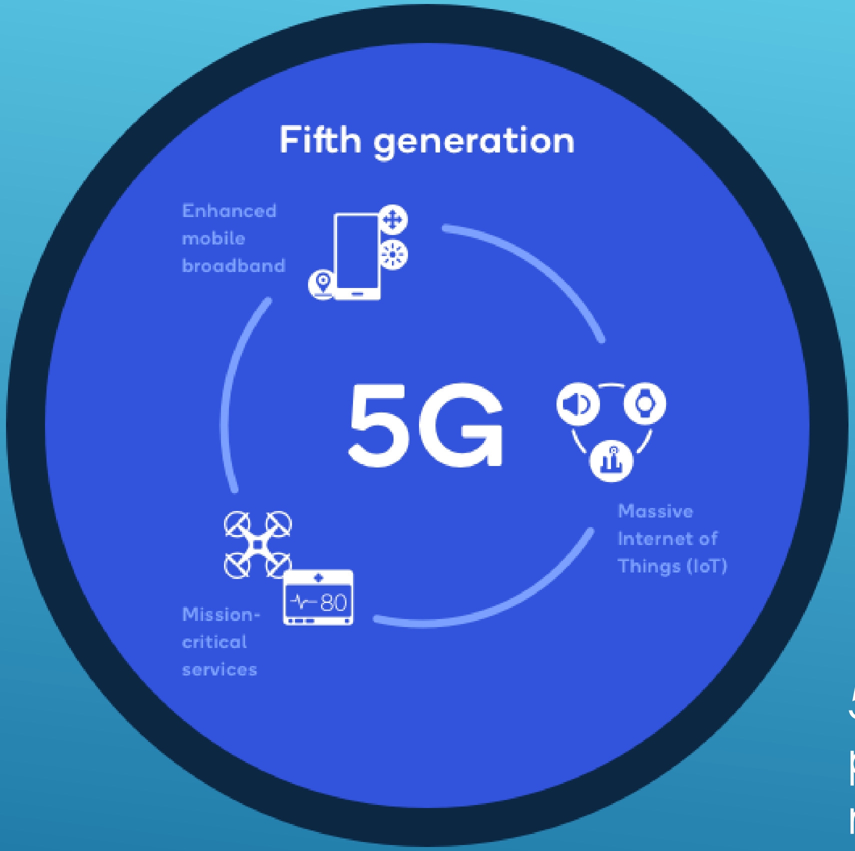


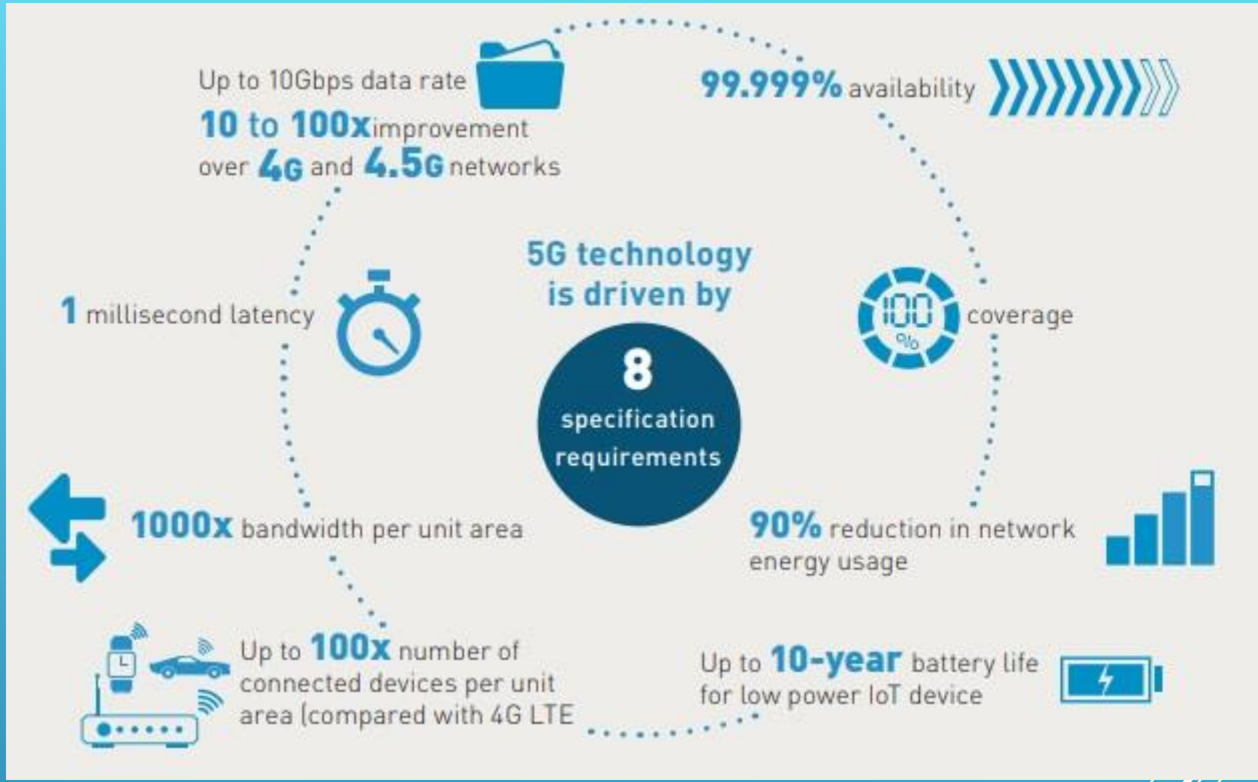
D2D COMMUNICATIONS IN 5G CELLULAR NETWORKS:

Prof. Preeti Godabole

CONTENT

- Introduction to D2D communications;
- High level requirements for 5G architecture;
- Introduction to the radio resource management, power control and mode selection problems;
- Millimeter wave communication in 5G.





5G wireless technology is meant to deliver higher multi-Gbps peak data speeds, ultra low latency, more reliability, massive network capacity, increased availability, and a more uniform user experience to more users. Higher performance and improved efficiency empower new user experiences and connects new industries.

WHAT IS 5G… SPECIFICATION REQUIREMENT

- Enhanced mobile broadband

In addition to making our smartphones better, 5G mobile technology can usher in new immersive experiences such as VR and AR with faster, more uniform data rates, lower latency, and lower cost-per-bit.

- Mission-critical communications

5G can enable new services that can transform industries with ultra-reliable, available, low-latency links like remote control of critical infrastructure, vehicles, and medical procedures.

- Massive IoT

5G is meant to seamlessly connect a massive number of embedded sensors in virtually everything through the ability to scale down in data rates, power, and mobility—providing extremely lean and low-cost connectivity solutions.

WHERE IS 5G USED

- 5G wireless has been assigned a new spectrum in low and mid bands (up to 6 gigahertz [GHz]) and in high bands (with millimeter wavelengths above 24GHz).
- Challenge for 5G antenna designs
  - Some devices need to operate in multiple bands.
  - Another is that millimeter wavelengths transmitted at cellular network power levels are subject to higher absorption by buildings, vegetation, and raindrops than low and mid bands.
  - This limits millimeter wavelength communications to line of sight, which necessitates small cell networks that can increase chances of edge interference between cells.

CHALLENGES THAT FOLLOW..

- active antenna arrays to provide better coverage, reduce interference, and increase data-carrying capacity.
- To operate in its full range of assigned frequencies,
  - 5G NR uses a scalable framework that functions at frequencies between 450 megahertz (MHz) and 6GHz (frequency range 1 [FR1]) and between 24.25 and 52.6GHz (frequency range 2 [FR2]).

MEETING 5G NR OBJECTIVES REQUIRES NEW ANTENNA DESIGNS

- 5G NR does this by using scalable orthogonal frequency-division multiplexing (OFDM) waveforms that allow different subcarrier signal spacing to fit the various channel widths that different frequency ranges provide.
- Higher frequencies provide wider channels and greater subcarrier spacing.
- Lower frequencies use smaller channel widths and narrower subcarrier spacing.
- Scaling subcarrier spacing to available channel widths enables the 5G framework to operate across a broad range of frequencies.
- The result makes it possible to deploy 5G in existing 4G Long-Term Evolution (LTE) networks.

5G ON EXISTING LTE

- challenge presented by the 5G specification is the need to support much higher densities of connected devices that are operating simultaneously at much higher data rates.
- require higher cell densities and more extensive use of the multiple-input, multiple-output (MIMO) antenna technologies already in use in 4G LTE networks.
- MIMO is an antenna array of multiple transmitting and receiving antennas (which in current LTE networks, often contains an 8 x 8 antenna array).
- MIMO uses spatial multiplexing to break a signal into encoded streams that it simultaneously transmits through different antennas in the array.

DEVICE DENSITY, DATA THROUGHPUT, AND MASSIVE MIMO

- **Communicate with higher throughput**
- Many variations of MIMO exist. A key variation for 5G is massive MIMO (mMIMO), an antenna design that packs many more antenna elements into a dense array than previous MIMO versions.
- Millimeter wavelengths work with much smaller antennas, which makes it possible to build mMIMO arrays in small packages.
- **Beamforming, Directionality, and User Equipment Tracking**
- High frequency (millimeter wavelength) 5G deployments will take advantage of adaptive arrays using larger mMIMO antennas with many more antenna elements and capable of tighter beamforming and real-time steering.

COMMUNICATE WITH MULTIPLE USERS AND DEVICES SIMULTANEOUSLY.

- **Downlink and Uplink Requirements**
- The 5G specification facilitates a maximum downlink data rate that is twice the uplink data rate in given use cases. In current deployment phases below 2.6GHz, 5G requires at least a 4 x 4 downlink MIMO and recommends at least a 2 x 2 uplink MIMO.
- **Antenna Designs for Different Use Cases**
- 5G deployments will require many antenna packages for indoor and outdoor use, small cell and macro-coverage, and many different kinds of terminal equipment.

COMMUNICATE WITH MULTIPLE USERS AND DEVICES SIMULTANEOUSLY

- **Base Stations**
- Most cell phone towers today are highly congested. Building compact 5G antennas that integrate lower and higher frequencies is the most cost-effective solution.
- In addition, placing antennas on light poles and corners of buildings for small cell coverage will require compact designs. Several telecom operators have begun deploying small 4G cells to address bandwidth and latency issues.

COMMUNICATE WITH MULTIPLE USERS AND DEVICES SIMULTANEOUSLY

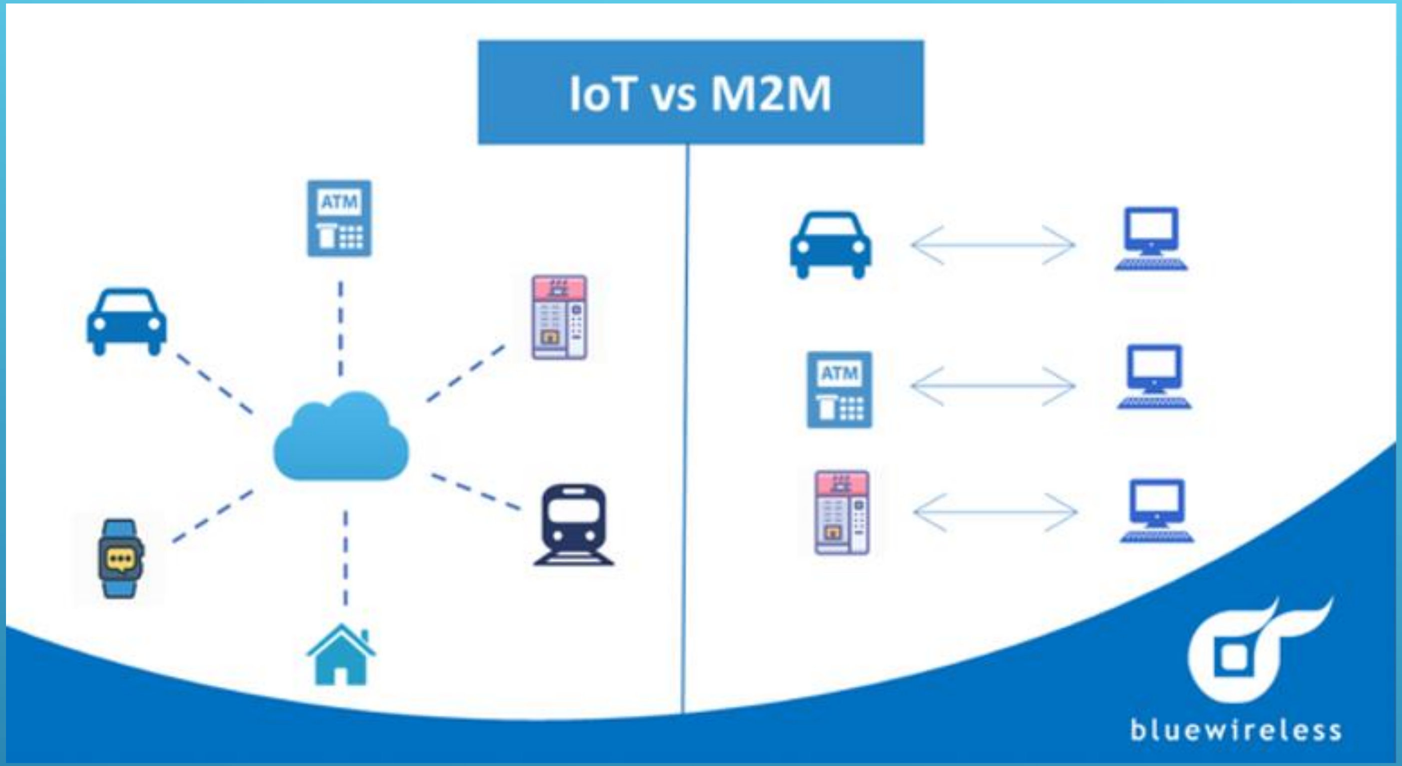
- **User and Terminal Equipment**
- Data, communication requirements, operational frequencies, and equipment design will dictate antenna designs in different 5G applications.
- **Cell Phones**
- Cell phones are already packed with antennas, so adding antennas to support the full range of 5G frequencies will be a challenge.
-

- Antenna designers typically begin with antenna simulation software
- A significant challenge in 5G antenna designs is antenna testing.
- 5G antennas are not static, omnidirectional devices. They are active, and they beam their transmissions to specific devices.
- Putting a 5G antenna in a test room and applying a static test does not show how it will perform when it is simultaneously communicating with a thousand moving devices in a noisy RF environment.
- Most antenna designers are not sure of the most effective means to test or validate performance for devices that use mMIMO arrays.
- Testing methods will likely involve scenario-based automated testing.

THE CHALLENGES OF 5G ANTENNA DESIGN

- IoT and M2M, both refer to the interconnection and sharing data between devices with embedded chips, sensors.
- There is a distinction between them.
  - IoT is a broader system of devices where every device has an IP address and can communicate over the internet platform
  - M2M concentrates on the direct flow of information between two devices and supports a point-to-point connection.
- An example of M2M could be a revolutions per minute (RPM) sensor on a mill sending data directly to only one smartphone.
- M2M also ships with some security features because of its characteristics:
  - End-to-end encryption because the communication is established between 2 devices.
  - When hackers attack, only information between some pairs of devices can be jeopardized.

M2M, IOT,D2D



IOT VS M2M

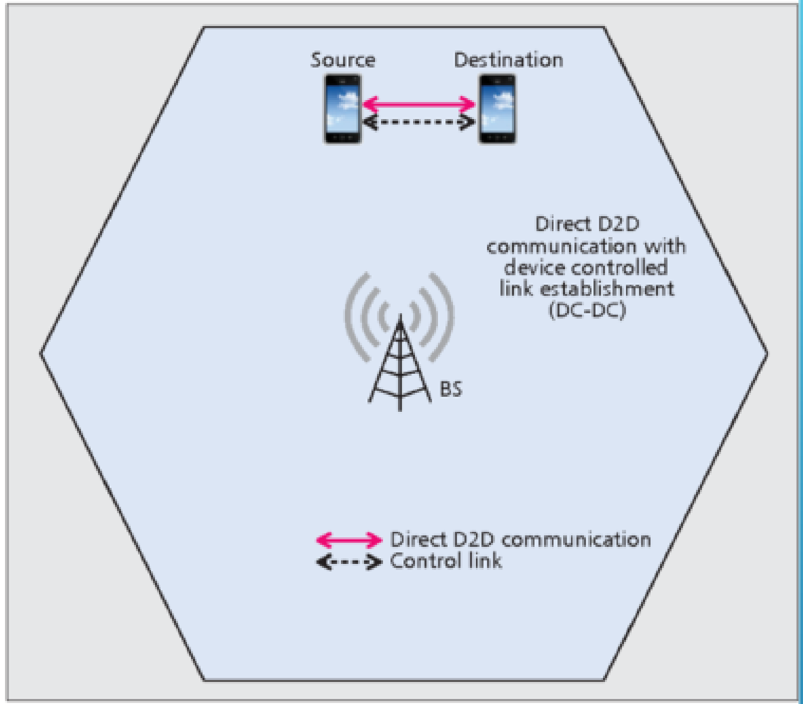


Figure 4. Illustration of direct D2D communication with device controlled

- The cellular network is one of the most blooming technologies recently with its fifth-generation (5G) which provides faster connectivity to the internet.
- Newer applications are introduced to the market and require fast multimedia-rich data exchange and the number of subscribers soared due to the popularity of smartphones.
- All of that huge data transfer required to travel through the base station or the core network which might create latency.
- D2D communication allows devices in close proximity to transfer data by creating a direct link and does not require that data to go through the base station.

D2D COMMUNICATION

- To enable D2D communication, we can rely on some existing wireless technologies used for transferring data in the near areas such as
  - Bluetooth,
  - WiFi direct
  - LTE direct.
- The listed wireless technologies however offer different ranges and speeds:
  - Bluetooth 5.0 offers a maximum data rate of 50Mbps and a range of 240m
  - WiFi Direct offers a 250 Mbps data rate and a range of 200m
  - LTE Direct offers up to 13.5 Mbps data rate and a range of 500m

D2D WITH EXISTING TECHNOLOGIES

- D2D provides a quick way to send data between devices that are nearby without going through Base Station (BS). That characteristic makes it an effective technique in many scenarios.
  - Local data services: D2D communication is fit and suitable to provide local data services for a small group of devices. It can support sending from one device to another device (unicast), or group of devices (group cast), or all devices (broadcast).
  - Information sharing: by using D2D links we can transfer files, videos, audio with high speed but using lower energy like using cellular channels. When disasters occur, the base stations may be destroyed, however, the D2D links can still work.
  - Data and computation offloading: Devices can act as hotspots that contain the same data as BS. Other devices with lower batteries then can get the data of those hotspots.
  - Machine-to-machine communication: Devices can leverage the power of D2D communication to directly transfer data with lower energy required and ultra-low latency. In some cases, M2M communication requires real-time data to be transmitted.
    - Automation cars need to exchange data with other nearby cars as fast as possible to make a decision instantly.

APPLICATIONS OF D2D

- The concept of D2D communications is to allow direct communications among the user equipment's (UEs) by reusing the cellular resources rather than using the uplink or downlink resources of the cellular networks .
- D2D communications can achieve four types of gain , <u>namely proximity gain, hop gain, reuse gain, and pairing gain.</u> In D2D communications, the UEs can operate in one of three traditional modes as follows.
  - • Reuse mode: D2D UEs directly transmit data among themselves by reusing some radio resources used by cellular UEs to enhance the spectrum utilization.
  - • Dedicated mode: D2D UEs directly transmit data among themselves by using a dedicated portion of spectrum to avoid interference with cellular UEs.
  - • Cellular mode: Similarly to cellular UEs, D2D UEs relay their data through the base station.

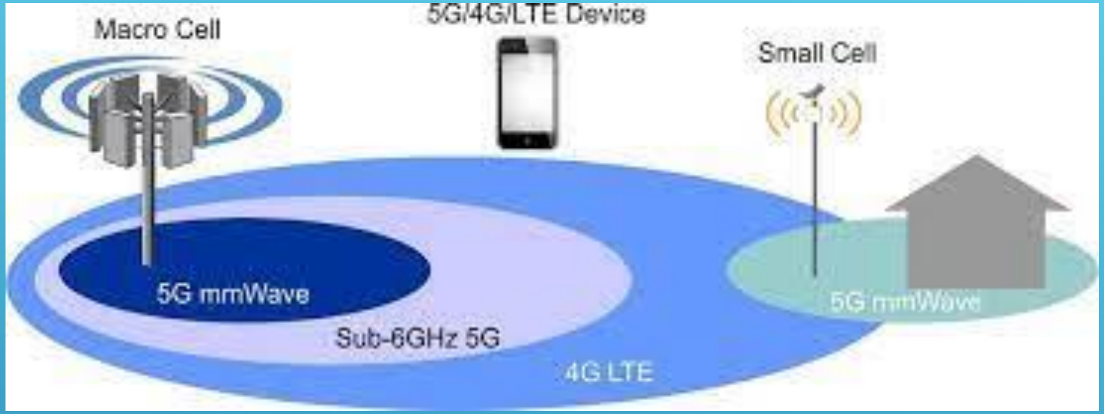
MODE SELECTION AND RESOURCE ALLOCATION

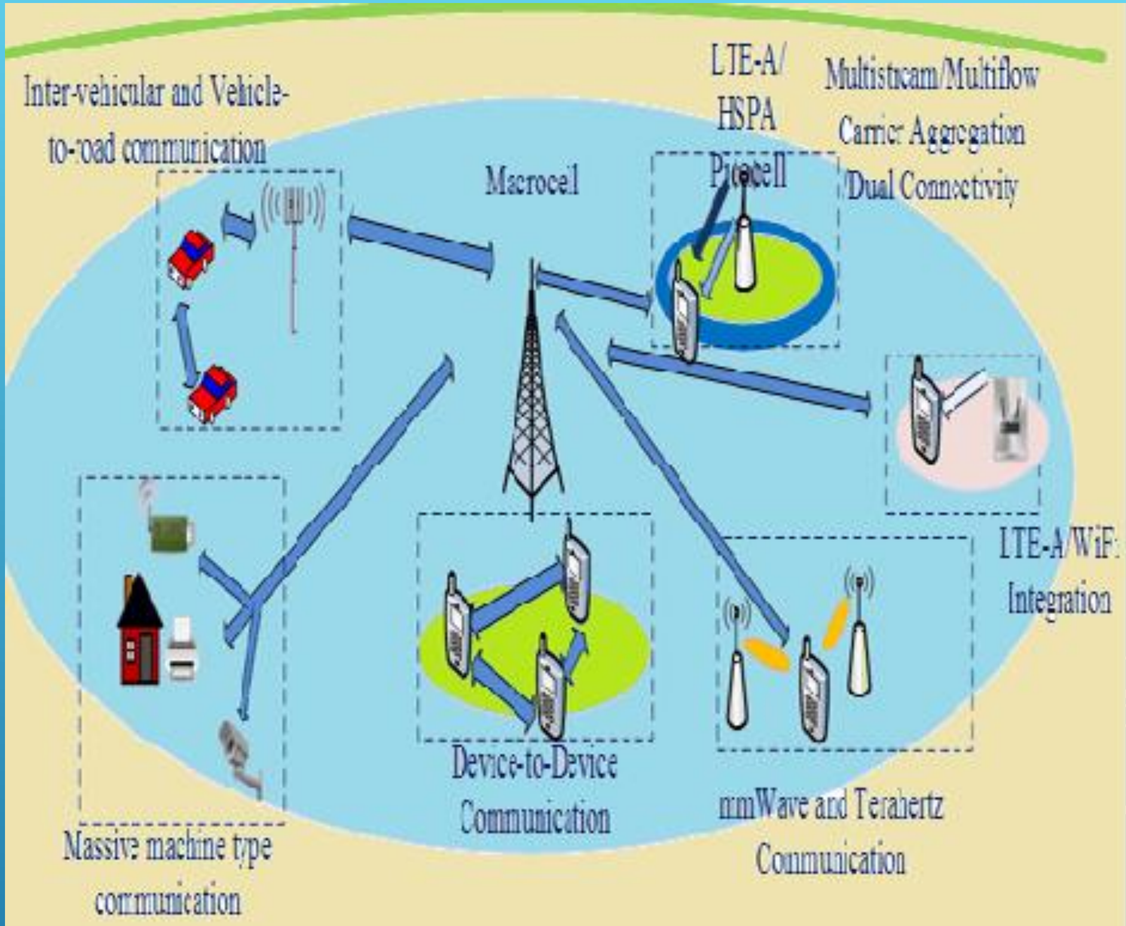
- In the cellular mode, more resources (e.g., the number of time slots) may be required for transmitting data to the receiver than in the reuse mode or dedicated mode;
- however, it is easier to manage interference with cellular users. The reuse mode can achieve a higher spectrum efficiency but D2D communications in this mode may interfere with cellular users and other D2D users using the cellular mode.
- By contrast, the dedicated mode can completely avoid interference, since some resources are reserved for the D2D communications; however, the spectrum utilization can be very poor in this mode.
- A simple method is to choose the mode by considering only the received signal strength over the D2D link or the distance between the terminals.
- However, the interference conditions and the differences between sharing cellular uplink and downlink also affect the overall network throughput.

HOW TO SELECT A TRANSMISSION MODE?

- high-frequency bands are often referred to as "mmWave" **due to the short wavelengths that can be measured in millimeters**.
- Although the mmWave bands extend all the way up 300 GHz, it is the bands from 24 GHz up to 100 GHz that are expected to be used for 5G.
- Modern 5G operates in the 3.5GHz frequency band that allows for higher capacity and lower latency.
- To achieve even higher frequency, longstanding mmWave technology can be utilized for next generation connectivity.
- **Pairing 5G with mmWave provides massive capacity and even lower latency to unlock the full 5G experience**.

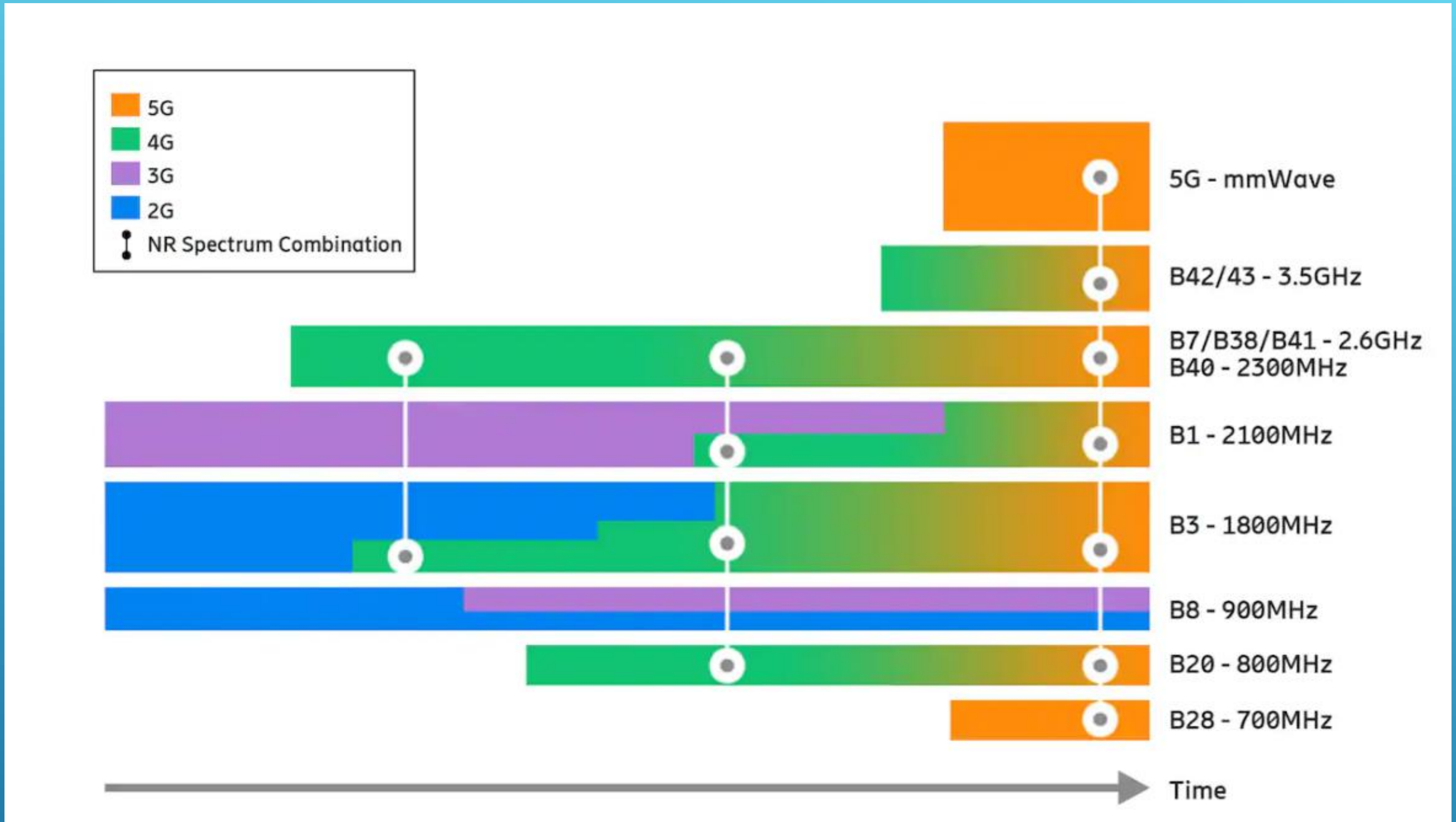
MILLIMETER WAVE COMMUNICATION IN 5G





Because of its high frequencies, mmWave has a limited range of only 300 to 500 feet and struggles to penetrate buildings

5G MMWAVE


5G
4G
3G
2G
NR Spectrum Combination
5G - mmWave
B42/43 - 3.5GHz
B7/B38/B41 - 2.6GHz
B40 - 2300MHz
B1 - 2100MHz
B3 - 1800MHz
B8 - 900MHz
B20 - 800MHz
B28 - 700MHz
Time

MMWAVE 5G

- https://www.qualcomm.com/research/5g/5g-nr/mmwave
- https://www.cambridge.org/core/books/abs/wireless-devicetodevice-communications-and-networks/mode-selection-and-resource-allocation-for-d2d-communications-underlaying-cellular-networks/77DB55E7E07FCE938A355CD4D6D538A0
- https://www.wevolver.com/article/5g-antenna-design
- https://www.speranzainc.com/what-is-machine-to-machine-device-to-device-internet-of-things/#:~:text=While%20IoT%20refers%20to%20a,of%20Machine%2Dto%2Dmachine.

WEB REFERENCES