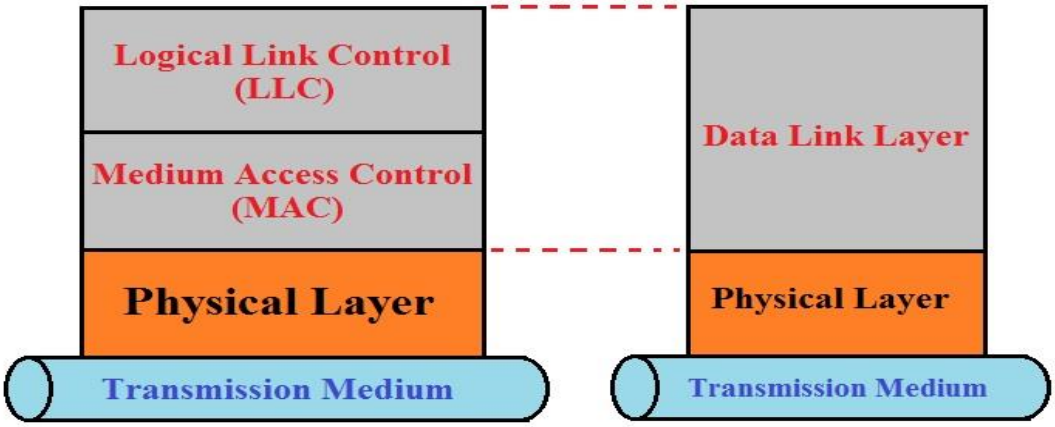
UNIT-2
Medium Access Control

Syllabus:
(Wireless) Medium Access Control (MAC) : Motivation for a specialized MAC (Hidden and exposed terminals, Near and far terminals), SDMA, FDMA, TDMA, CDMA, Wireless LAN/(IEEE 802.11)

Medium Access Control (MAC):

- Media access control (MAC) is a sublayer of the data link layer (DLL) in the seven-layer OSI network reference model.
- MAC is responsible for the transmission of data packets to and from the network-interface card, and to and from another remotely shared channel.
- The basic function of MAC is to provide an addressing mechanism and channel access so that each node available on a network can communicate with other nodes available on the same or other networks. Sometimes people refer to this as the MAC layer.
- Medium Access Control (MAC) acts as an interface between physical layer and Logical Link Channel(LLC).



Motivation for a specialized MAC:

- The main question in connection with MAC in the wireless is whether it is possible to use elaborated MAC schemes from wired networks, for example, CSMA/CD as used in the original specification of IEEE 802.3 (Ethernet) networks.
- Consider **carrier sense multiple access with collision detection, (CSMA/CD)** which works as follows.
- A sender senses the medium (a wire or coaxial cable) to see if it is free. If the medium is busy, the sender waits until it is free. If the medium is free, the sender starts transmitting data and continues to listen into the medium.
- If the sender detects a collision while sending, it stops at once and sends a jamming signal.
- This scheme fails in wireless networks? CSMA/CD is not really interested in collisions at the sender, but rather in those at the receiver.
- If a collision occurs somewhere in the wire, everybody will notice it. The situation is different in wireless networks. Strength of a signal decreases proportionally to the square of the distance to the sender.

- The sender may now apply carrier sense and detect an idle medium. The sender starts sending – but a collision happens at the receiver due to a second sender (hidden terminal problem).
- The same can happen to the collision detection. The sender detects no collision and assumes that the data has been transmitted without errors, but a collision might actually have destroyed the data at the receiver.
- Collision detection is very difficult in wireless scenarios as the transmission power in the area of the transmitting antenna is several magnitudes higher than the receiving power.
- So, this very common MAC scheme from wired network fails in a wireless scenario.
- The following sections show some more scenarios where schemes known from fixed networks fail.

Hidden and exposed terminals:

- Consider the scenario with three mobile phones as shown in below Figure. The transmission range of A reaches B, but not C (the detection range does not reach C either).
- The transmission range of C Reaches B, but not A. Finally, the transmission range of B reaches A and C, i.e., A cannot detect C and vice versa.
- A start sending to B, C does not receive this transmission. C also wants to send something to B and senses the medium. The medium appears to be free, the carrier sense fails.
- C also starts sending causing a collision at B. But A cannot detect this collision at B and continues with its transmission. A is **hidden** for C and vice versa.
- While hidden terminals may cause collisions, the exposed terminals effect only causes unnecessary delay.

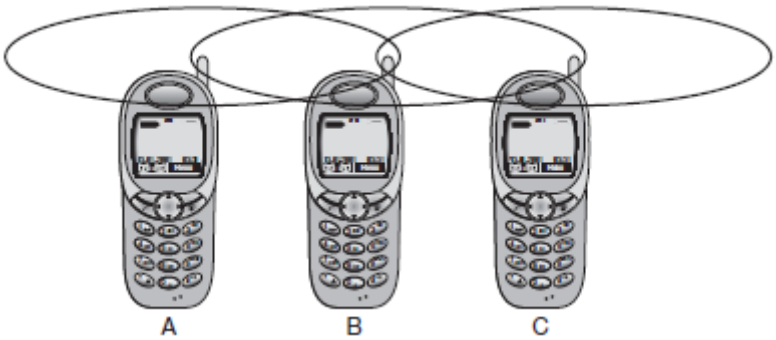


Fig: Hidden and exposed terminals

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

Near and far terminals:

- Consider the situation as shown in below Figure. A and B are both sending with the same transmission power.
- As the signal strength decreases proportionally to the square of the distance, B's signal drowns out A's signal. As a result, C cannot receive A's transmission.
- Now think of C as being an arbiter for sending rights. In this case, terminal B would already drown out terminal A on the physical layer. C in return would have no chance of applying a fair scheme as it would only hear B.
- The **near/far effect** is a severe problem of wireless networks using CDM.

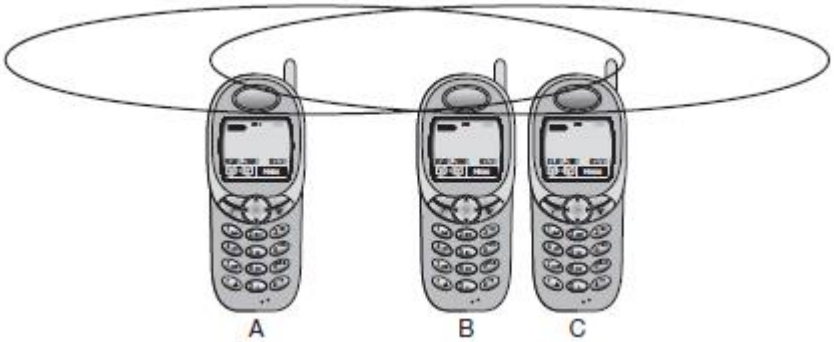
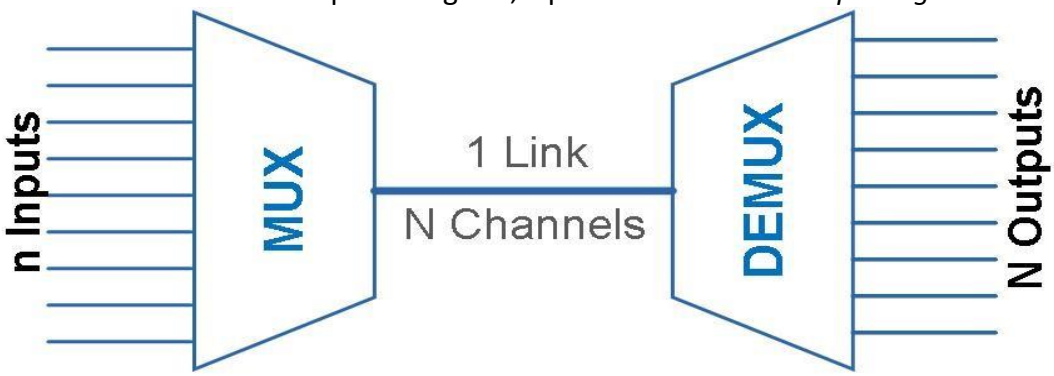


Fig: Near and far terminals

Multiple Access techniques:

- Multiplexing is a way of sending multiple signals or streams of information over a communications link at the same time in the form of a single, complex signal; the receiver recovers the separate signals, a process called *demultiplexing*.



- Generally, four types of multiple access techniques are there,
  - **SDMA: Space Division Multiple Access**
  - **FDMA: Frequency Division Multiple Access**
  - **TDMA: Time Division Multiple Access**
  - **CDMA: Code Division Multiple Access**

SDMA: Space Division Multiple Access

- **SDMA** is used for allocating a separated space to users in wireless networks. A typical application involves assigning an optimal base station to a mobile phone user.
- The mobile phone may receive several base stations with different quality.
- A MAC algorithm could now decide which base station is best, taking into account which frequencies (FDM), time slots (TDM) or code (CDM) are still available (depending on the technology).
- Typically, SDMA is never used in isolation but always in combination with one or more other schemes.
- The basis for the SDMA algorithm is formed by cells and sectorized antennas which constitute the infrastructure implementing **space division multiplexing (SDM)**.
- A new application of SDMA comes up together with beam-forming antenna arrays. Single users are separated in space by individual beams. This can improve the overall capacity of a cell tremendously.

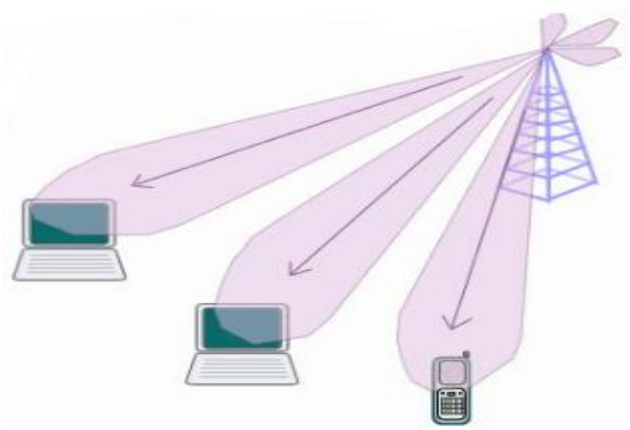
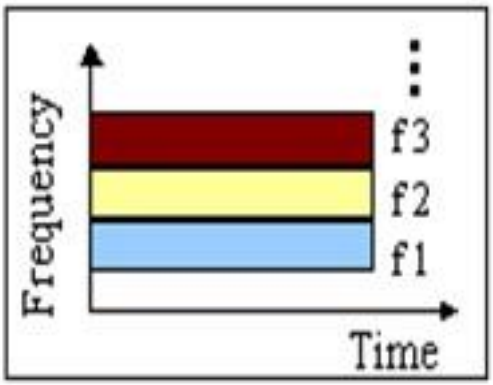


Fig: Beam forming antenna

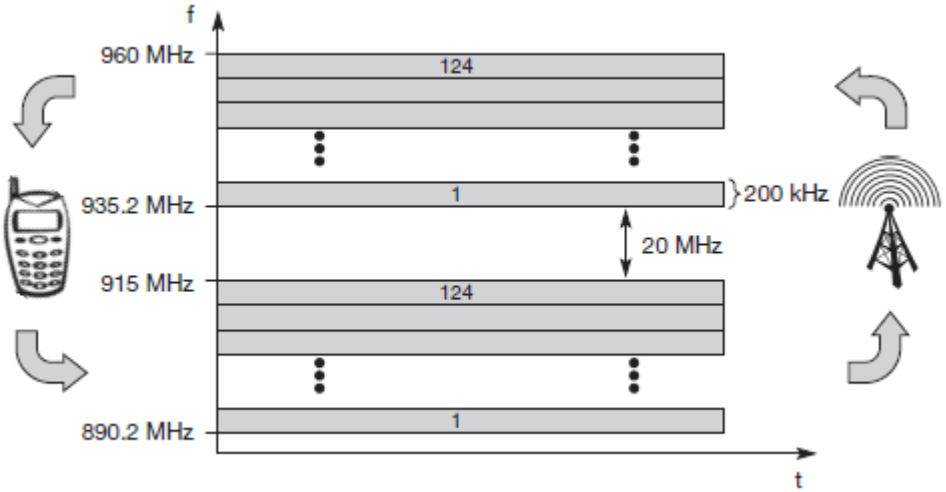
FDMA: Frequency Division Multiple Access

- **Frequency division multiple access (FDMA)** comprises all algorithms allocating frequencies to transmission channels according to the **frequency division multiplexing (FDM).**
- Allocation can either be fixed or dynamic.
- Channels can be assigned to the same frequency at all times, i.e., pure FDMA, or change frequencies according to a certain pattern, i.e., FDMA combined with TDMA.

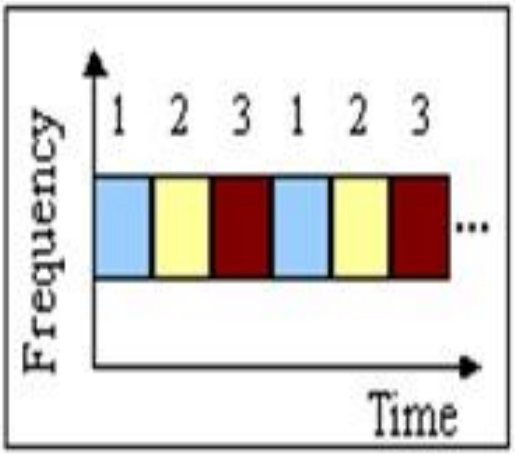


- Common practice for many wireless systems to circumvent narrowband interference at certain frequencies, known as **frequency hopping**.
- Sender and receiver have to agree on a hopping pattern, otherwise the receiver could not tune to the right frequency.
- Furthermore, FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks.
- Here the two partners typically establish a **duplex channel**, i.e., a channel that allows for simultaneous transmission in both directions. The two directions, mobile station to base station and vice versa are now separated using different frequencies.

- This scheme is then called **frequency division duplex (FDD)**.
- The two frequencies are also known as **uplink**, i.e., from mobile station to base station or from ground control to satellite, and as **downlink**, i.e., from base station to mobile station or from satellite to ground control.



TDMA: Time Division Multiple Access



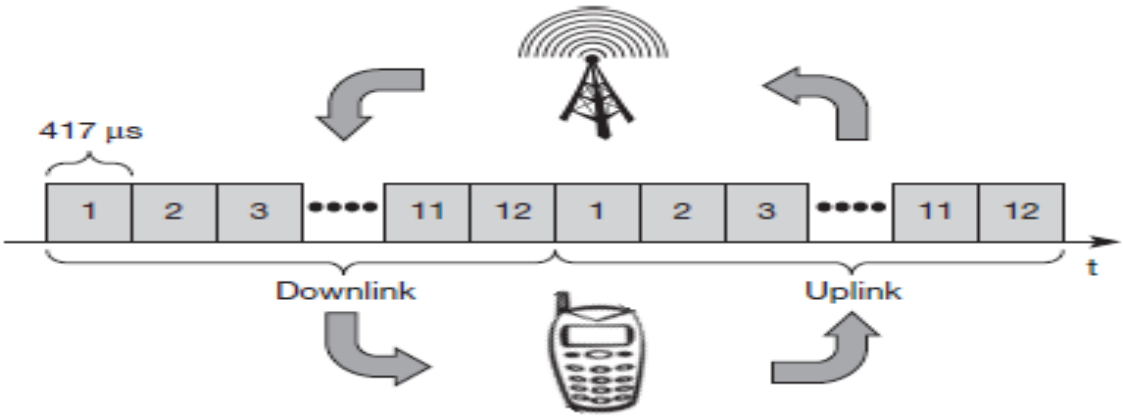
- Compared to FDMA, **time division multiple access (TDMA)** offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication, i.e., controlling **TDM**.
- Now tuning into a certain frequency is not necessary, i.e., the receiver can stay at the same frequency the whole time.
- Using only one frequency, and thus very simple receivers and transmitters, many different algorithms exist to control medium access.
- Listening to different frequencies at the same time is quite difficult, but listening to many channels separated in time at the same frequency is simple.
- Almost all MAC schemes for wired networks work according to this principle, e.g., Ethernet, Token Ring, ATM etc.
- Now synchronization between sender and receiver has to be achieved in the time domain.
- This can be done by using a fixed pattern similar to FDMA techniques, i.e., allocating a certain time slot for a channel, or by using a dynamic allocation scheme.

Other schemes of TDMA:

- The following schemes of fixed and dynamic schemes as used for wireless transmission. Typically, those schemes can be combined with FDMA to achieve even greater flexibility and transmission capacity.
    - Fixed TDM
    - Classical Aloha
    - Slotted Aloha
    - Carrier sense multiple access (CSMA)
    - Demand assigned multiple access (DAMA)
    - Packet reservation multiple access (PRMA)
    - Reservation TDMA
    - Multiple access with collision avoidance (MACA)
    - Polling
    - Inhibit sense multiple access (ISMA)

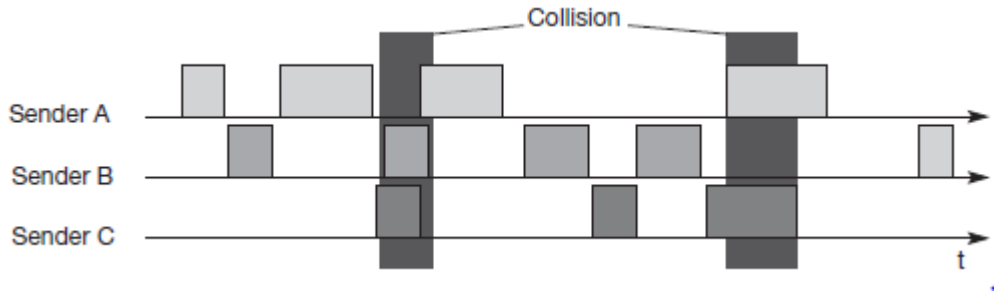
Fixed TDM:

- The simplest algorithm for using TDM is allocating time slots for channels in a fixed pattern. This results in a fixed bandwidth and is the typical solution for wireless phone systems.
- The fixed pattern can be assigned by the base station, where competition between different mobile stations that want to access the medium is solved.
- Fixed access patterns (at least fixed for some period in time) fit perfectly well for connections with a fixed bandwidth.
- TDMA schemes with fixed access patterns are used for many digital mobile phone systems like IS-54, IS-136, GSM, DECT, PHS, and PACS.
- Fixed TDM patterns are used to implement multiple access and a duplex channel between a base station and mobile station.
- Assigning different slots for uplink and downlink using the same frequency is called **time division duplex (TDD)**.
- As shown in the figure, the base station uses one out of 12 slots for the downlink, whereas the mobile station uses one out of 12 different slots for the uplink. Uplink and downlink are separated in time.
- Up to 12 different mobile stations can use the same frequency without interference using this scheme. Each connection is allotted its own up- and downlink pair.
- In the example below, which is the standard case for the DECT cordless phone system, the pattern is repeated every 10 ms, i.e., each slot has a duration of 417 μs.



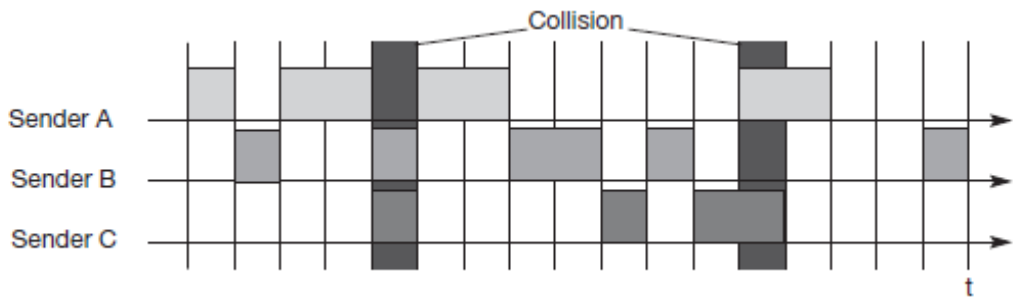
Classical Aloha:

- Classical Aloha scheme was invented at the University of Hawaii and was used in the **ALOHANET** for wireless connection of several stations.
- Aloha neither coordinates medium access nor does it resolve contention on the MAC layer.
- Instead, each station can access the medium at any time as shown in Figure. This is a random-access scheme, without a central arbiter controlling access and without coordination among the stations.
- If two or more stations access the medium at the same time, a **collision** occurs and the transmitted data is destroyed.
- Resolving this problem is left to higher layers (e.g., retransmission of data).
- The simple Aloha works fine for a light load and does not require any complicated access mechanisms.
- In Classical aloha data packet arrival follows a Poisson distribution, maximum throughput is achieved for an 18 per cent.



Slotted Aloha:

- The first refinement of the classical Aloha scheme is provided by the introduction of time slots (**slotted Aloha**).
- In this case, all senders have to be **synchronized**, transmission can only start at the beginning of a **time slot** as shown in Figure. Still, access is not coordinated.
- Under the assumption stated above, the introduction of slots raises the throughput from 18 per cent to 36 per cent, i.e., slotting doubles the throughput.
- As we will see in the following sections, both basic Aloha principles occur in many systems that implement distributed access to a medium.
- Aloha systems work perfectly well under a light load, but they cannot give any hard transmission guarantees, such as maximum delay before accessing the medium, or minimum throughput. Here one needs additional mechanisms, e.g., combining fixed schemes and Aloha schemes.
- However, even new mobile communication systems like UMTS have to rely on slotted Aloha for medium access in certain situation.



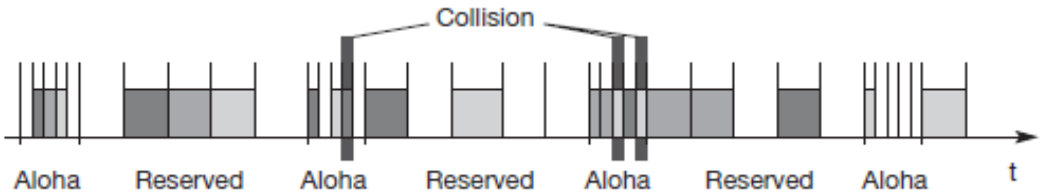
s.

Carrier sense multiple access (CSMA):

- The **carrier sense multiple access (CSMA)** scheme "Sensing the carrier and accessing the medium only if the carrier is idle decreases the probability of a collision".
- But hidden terminals cannot be detected, so, if a hidden terminal transmits at the same time as another sender, a collision might occur at the receiver.
- This basic scheme is still used in most wireless LANs. Several versions of CSMA exist.
- In **non-persistent CSMA**, stations sense the carrier and start sending immediately if the medium is idle. If the medium is busy, the station pauses a random amount of time before sensing the medium again and repeating this pattern.
- In **p-persistent CSMA** systems nodes also sense the medium, but only transmit with a probability of p, with the station deferring to the next slot with the probability 1-p, i.e., access is slotted in addition.
- CSMA with collision avoidance (**CSMA/CA**) is one of the access schemes used in wireless LANs following the standard IEEE 802.11.
- Another, very elaborate scheme is Elimination yield – non-preemptive multiple access (**EY-NMPA**) used in the HIPERLAN 1 specification.

Demand assigned multiple access (DAMA):

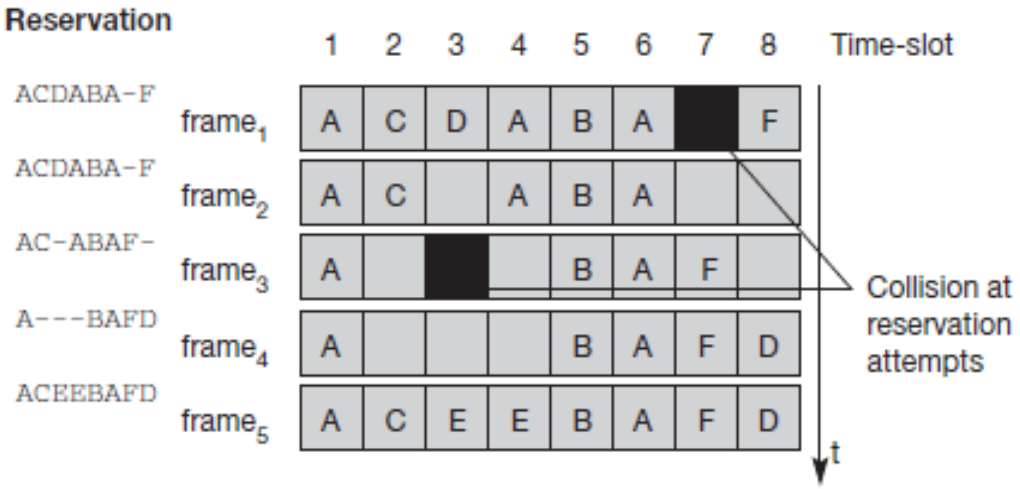
- A general improvement of Aloha access systems can also be achieved by **reservation** mechanisms and combinations with some (fixed) TDM patterns.
- **DAMA** typically have a reservation period followed by a transmission period. During the reservation period, stations can reserve future slots in the transmission period.
- In general, these schemes cause a higher delay under a light load (first the reservation has to take place), but allow higher throughput due to less collisions.
- **Demand assigned multiple access (DAMA)** scheme typical for satellite systems, also called **reservation Aloha**.



- Different stations on earth try to reserve access time for satellite transmission. Collisions during the reservation phase do not destroy data transmission.
- If successful, a time slot in the future is reserved, and no other station is allowed to transmit during this slot.
- The satellite collects all successful requests and sends back a reservation list indicating access rights for future slots.
- All ground stations have to obey this list. To maintain the fixed TDM pattern of reservation and transmission, the stations have to be synchronized from time to time.
- DAMA is an **explicit reservation** scheme. Each transmission slot has to be reserved explicitly.

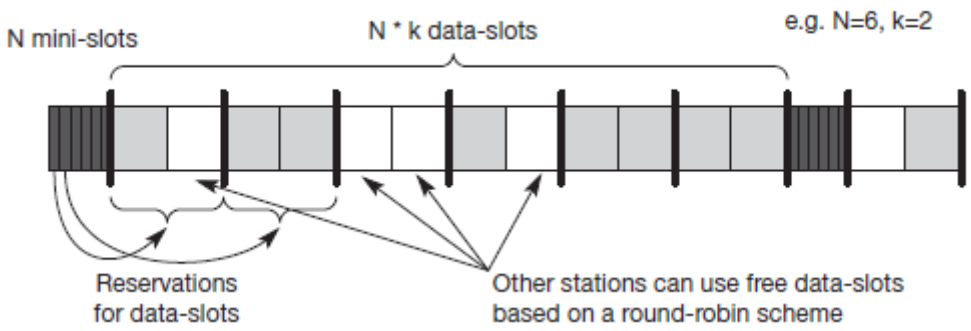
Packet reservation multiple access (PRMA):

- **Packet reservation multiple access (PRMA)** is an **implicit reservation** scheme.
- Slots can be reserved implicitly according to the following scheme. A certain number of slots forms a frame (Figure shows eight slots in a frame).
- The frame is repeated in time (forming frames one to five in the example), i.e., a fixed TDM pattern is applied.
- A base station, which could be a satellite, now broadcasts the status of each slot (as shown on the left side of the figure) to all mobile stations.
- A successful transmission of data is indicated by the station's name (A to F). In the example, the base station broadcasts the reservation status 'ACDABA-F' to all stations, here A to F.
- This means that slots one to six and eight are occupied, but slot seven is free in the following transmission.
- All stations wishing to transmit can now compete for this free slot in Aloha fashion. The already occupied slots are not touched.
- In the example shown, more than one station wants to access this slot, so a collision occurs.
- The base station returns the reservation status 'ACDABA-F', indicating that the reservation of slot seven failed (still indicated as free) and that nothing has changed for the other slots.
- Again, stations can compete for this slot. Additionally, station D has stopped sending in slot three and station F in slot eight. This is noticed by the base station after the second frame.
- Before the third frame starts, the base station indicates that slots three and eight are now idle.
- Station F has succeeded in reserving slot seven as also indicated by the base station. PRMA constitutes yet another combination of fixed and random TDM schemes with reservation compared to the previous schemes.
- As soon as a station has succeeded with a reservation, all future slots are implicitly reserved for this station. This ensures transmission with a guaranteed data rate.
- The slotted aloha scheme is used for idle slots only, data transmission is not destroyed by collision.



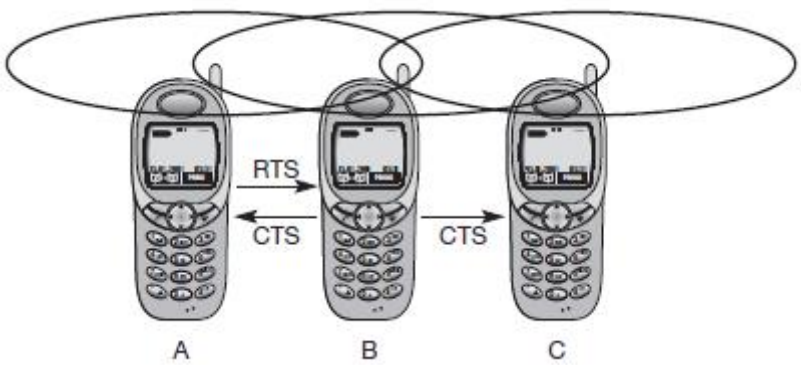
Reservation TDMA:

- An even more fixed pattern that still allows some random access is exhibited by **reservation TDMA**.
- In a fixed TDM scheme N mini-slots followed by N·k data-slots form a frame that is repeated.
- Each station is allotted its own mini-slot and can use it to reserve up to k data-slots. This guarantees each station a certain bandwidth and a fixed delay.
- Other stations can now send data in unused data-slots as shown.
- Using these free slots can be based on a simple round-robin scheme or can be uncoordinated using an Aloha scheme.
- This scheme allows for the combination of, e.g., isochronous traffic with fixed bitrates and best-effort traffic without any guarantees.



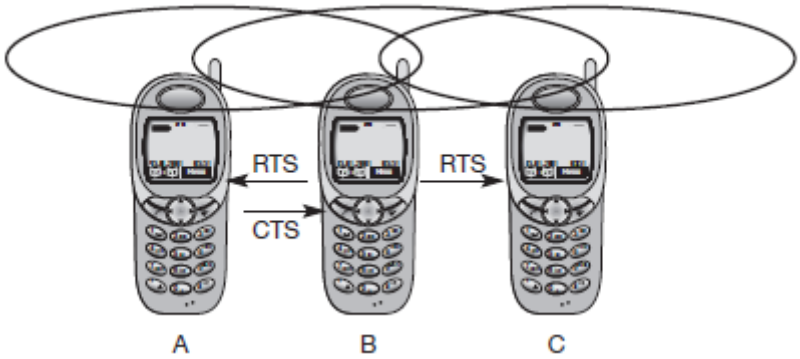
Multiple access with collision avoidance (MACA):

- **MACA** presents a simple scheme that **solves the hidden terminal problem**, does not need a base station, and is still a random-access Aloha scheme – but with dynamic reservation.
- In the hidden terminal problem. Remember, A and C both want to send to B. A has already started the transmission, but is hidden for C, C also starts with its transmission, thereby causing a collision at B.



- With MACA, A does not start its transmission at once, but sends a **request to send (RTS)** first. B receives the RTS that contains the name of sender and receiver, as well as the length of the future transmission.
- This RTS is not heard by C, but triggers an acknowledgement from B, called **clear to send (CTS)**.
- The CTS again contains the names of sender (A) and receiver (B) of the user data, and the length of the future transmission.

- This CTS is now heard by C and the medium for future use by A is now reserved for the duration of the transmission.
- After receiving a CTS, C is not allowed to send anything for the duration indicated in the CTS toward B.
- A collision cannot occur at B during data transmission, and the hidden terminal problem is solved.
- **MACA also help to solve the 'exposed terminal' problem**. Remember, B wants to send data to A, C to someone else. But C is polite enough to sense the medium before transmitting, sensing a busy medium caused by the transmission from B.
- C defers, although C could never cause a collision at A. With MACA, B has to transmit an RTS first containing the name of the receiver (A) and the sender (B).
- C does not react to this message as it is not the receiver, but A acknowledges using a CTS which identifies B as the sender and A as the receiver of the following data transmission.
- C does not receive this CTS and concludes that A is outside the detection range. C can start its transmission assuming it will not cause a collision at A.
- The problem with exposed terminals is solved without fixed access patterns or a base station.

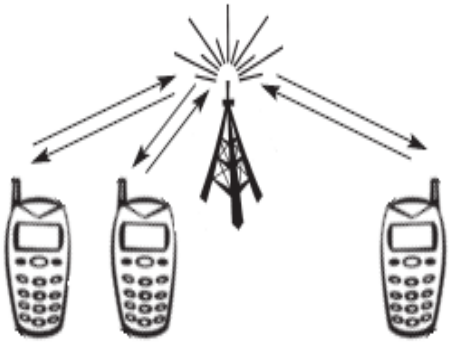


- MACA also assumes symmetrical transmission and reception conditions. Otherwise, a strong sender, directed antennas etc. could counteract the above scheme.

Polling:

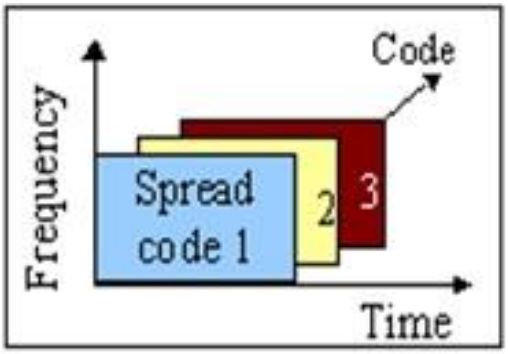
- **Polling** is a strictly centralized scheme with one master station and several slave stations.
- The master can poll the slaves according to many schemes: round robin, randomly, according to reservations etc.
- The master could also establish a list of stations wishing to transmit during a contention phase. After this phase, the station polls each station on the list.
- Similar schemes are used, e.g., in the Bluetooth wireless LAN and as one possible access function in IEEE 802.11 systems.

Inhibit sense multiple access (ISMA):



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

CDMA: Code Division Multiple Access



- Codes with certain characteristics can be applied to the transmission to enable the use of **code division multiplexing (CDM)**.
- **Code division multiple access (CDMA)** systems use exactly these codes to separate different users in code space and to enable access to a shared medium without interference.
- The main problem is how to find "good" codes and how to separate the signal from noise generated by other signals and the environment.
- The spreading a signal (e.g., using DSSS) directly controls the chipping sequence.
- But what is a good code for CDMA? A code for a certain user should have a good auto correlation and should be **orthogonal** to other codes.
- Two vectors are called orthogonal if their inner product is 0, as is the case for the two vectors (2, 5, 0) and (0, 0, 17): (2, 5, 0)*(0, 0, 17) = 0 + 0 + 0 = 0. But also vectors like (3, –2, 4) and (–2, 3, 3) are orthogonal: (3, –2, 4)*(–2, 3, 3) = –6 – 6 + 12 = 0.
- Now let us translate this into code space and good **autocorrelation** can be achieved by Barker code. This code is used for ISDN and IEEE 802.11
- the following example explains the basic function of CDMA
  - Two senders, A and B, want to send data. CDMA assigns the following unique and orthogonal key sequences:

    key $\mathbf{A_k = 010011}$ for sender A,

    key $\mathbf{B_K = 110101}$ for sender B.
  - Sender A wants to send the bit $\mathbf{A_d = 1}$, sender B sends $\mathbf{B_d = 0}$.

- To illustrate this example, let us assume that we code a **binary 0 as –**1, a **binary 1 as +1** (barker code).
- Now A_K = 010011 ➔ (–1, +1, –1, –1, +1, +1)
  B_K = 110101 ➔ (+1, +1, –1, +1, –1, +1)
- Spread signal for Sender A
  $A_S = A_d * A_K$= +1*(–1, +1, –1, –1, +1, +1) = (–1, +1, –1, –1, +1, +1)
- Spread signal for Sender B
  $B_S = B_d * B_K$ = –1*(+1, +1, –1, +1, –1, +1) = (–1, –1, +1, –1, +1, –1)
- Generate combined signal C is received at a receiver:
  $C = A_s + B_s$ = (–2, 0, 0, –2, +2, 0).
- If the receiver wants to receive data from sender A then applies A's code for dispreading:
  $C*A_K$ = (–2, 0, 0, –2, +2, 0) *(–1, +1, –1, –1, +1, +1) = 2 + 0 + 0 + 2 + 2 + 0 = 6.
  (The **result is positive**, so a **1** has been detected)
- If the receiver wants to receive data from sender B then applies B's code for dispreading:
  $C*B_K$ = (–2, 0, 0, –2, +2, 0) *(+1, +1, –1, +1, –1, +1) = –2 + 0 + 0 – 2 – 2 + 0 = –6.
  (The **result is negative**, so a **0** has been detected)

- Consider sender A that wants to transmit the bits 101. The key of A is shown as signal and binary key sequence A_K. In this example, the binary "0" is assigned a positive signal value, the binary "1" a negative signal value.
- After spreading, i.e., XORing A_d and A_K, the resulting signal is A_S.

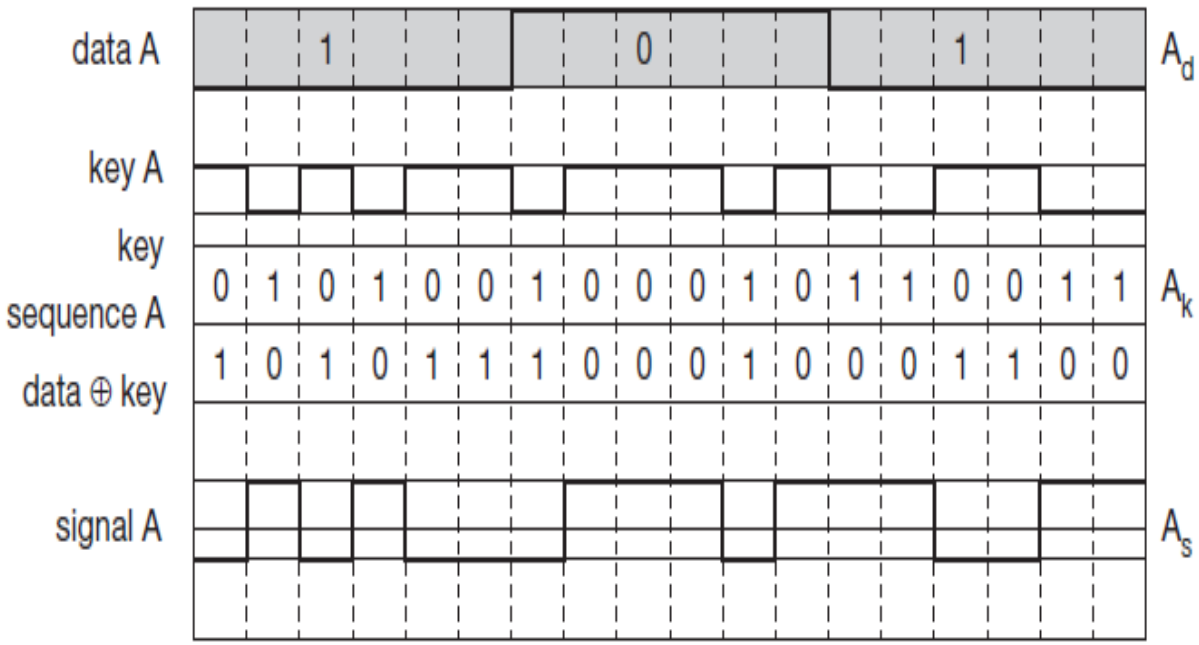


Fig: Coding and spreading of data from sender A

- The same happens with data from sender B, here the bits are 100. The result of spreading with the code is the signal B_S.
- A_S and B_S now superimpose during transmission (again without noise and both signals having the same strength). The resulting signal is simply the sum $A_S + B_S$.

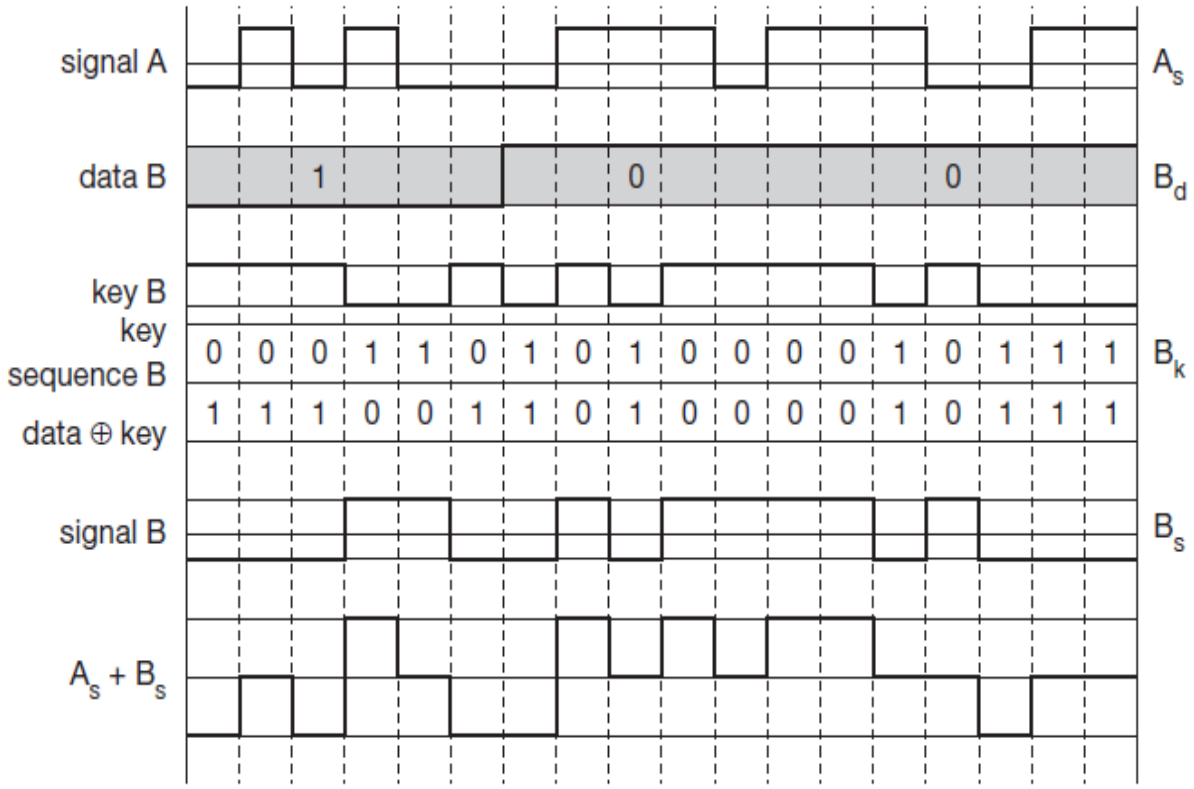


Fig: Coding and spreading of data from sender B

- If a receiver wants to receive A's data, then $(A_S + B_S) * A_K$

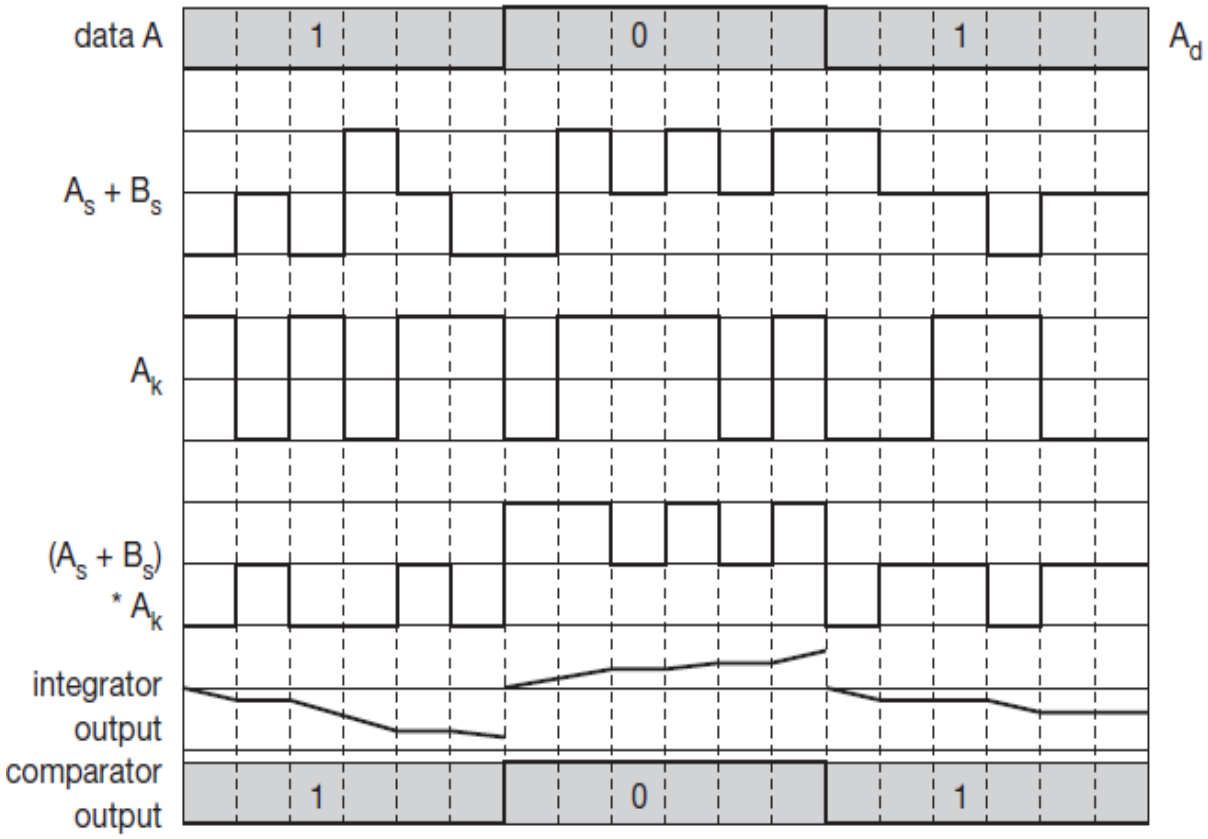


Fig: Reconstruction of A's data

- The same happens if a receiver wants to receive B's data, $(A_S + B_S) * B_K$

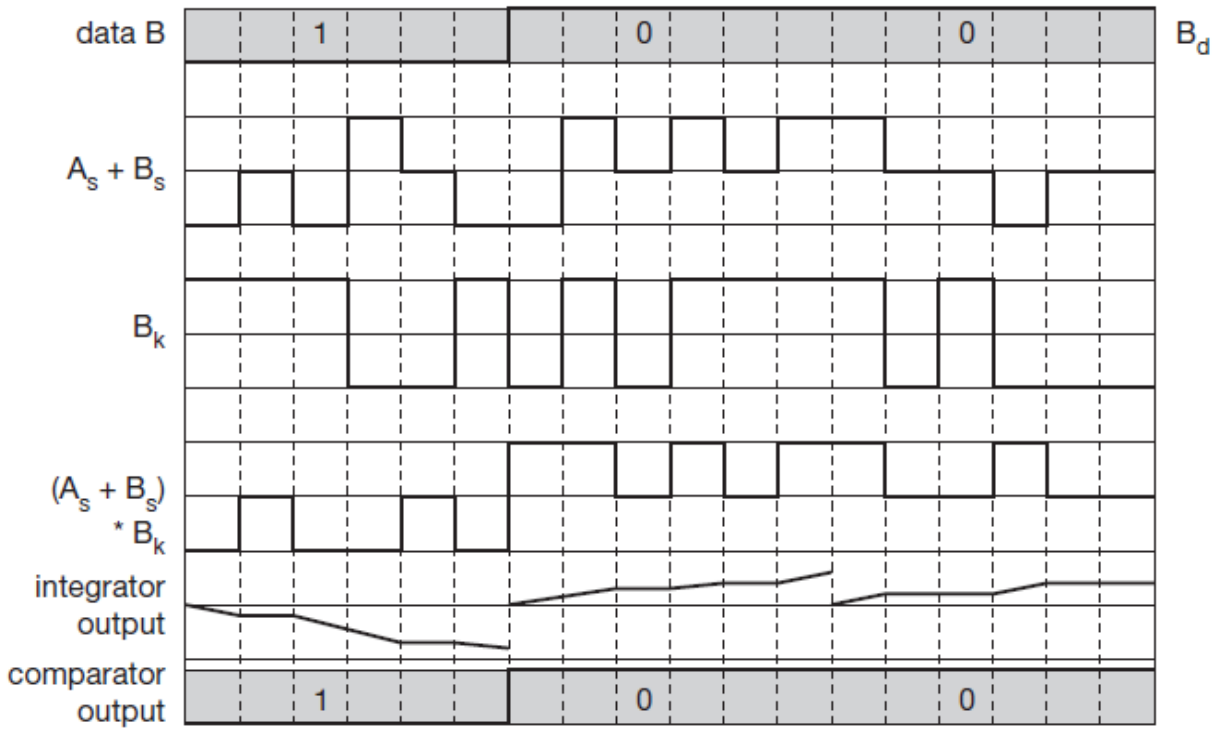
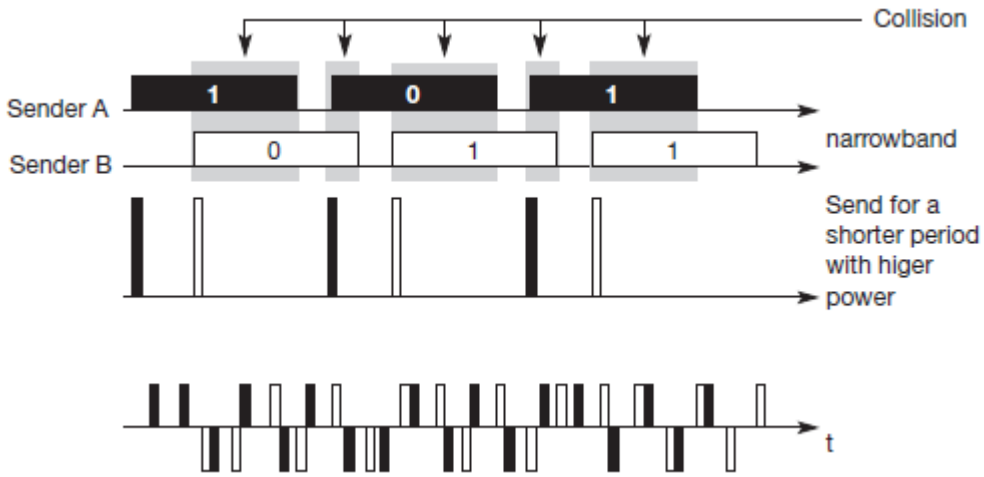


Fig: Reconstruction of B's data

Spread Aloha Multiple Access (SAMA):

- **Spread Aloha multiple access (SAMA)** and is a combination of CDMA and TDMA.
- SAMA works as follows: each sender uses the same spreading code (110101).
- The standard case for Aloha access is shown in the upper part of the figure. Sender A and sender B access the medium at the same time in their narrowband spectrum, so that all three bits shown cause a collision.
- The same data could also be sent with higher power for a shorter period as shown in the middle, but now spread spectrum is used to spread the shorter signals, i.e., to increase the bandwidth (spreading factor s = 6 in the example).



- Both signals are spread, but the chipping phase differs slightly. Separation of the two signals is still possible if one receiver is synchronized to sender A and another one to sender B.
- The main problem in using this approach is finding good chipping sequences. Clearly, the code is not orthogonal to itself – it should have a good autocorrelation but, at the same time, correlation should be low if the phase differs slightly.
- The maximum throughput is about 18 per cent, which is very similar to Aloha.
- The approach benefits from the advantages of spread spectrum techniques:
    - robustness against narrowband interference
    - simple coexistence with other systems in the same frequency bands.

Comparison between SDMA/TDMA/FDMA/CDMA

Approach	SDMA	TDMA	FDMA	CDMA
Idea	Segment space into cells/sectors	Segment sending time into disjoint time-slots, demand driven or fixed patterns	Segment the frequency band into disjoint sub-bands	Spread the spectrum using orthogonal codes
Terminals	Only one terminal can be active in one cell/one sector	All terminals are active for short periods of time on the same frequency	Every terminal has its own frequency, uninterrupted	All terminals can be active at the same place at the same moment, uninterrupted
Signal separation	Cell structure directed antennas	Synchronization in the time domain	Filtering in the frequency domain	Code plus special receivers
Advantages	Very simple, increases capacity per km^2	Established, fully digital, very flexible	Simple, established, robust	Flexible, less planning needed, soft handover
Disadvantages	Inflexible, antennas typically fixed	Guard space needed (multi-path propagation), synchronization difficult	Inflexible, frequencies are a scarce resource	Complex receivers, needs more complicated power control for senders

Wireless LAN (IEEE 802.11):

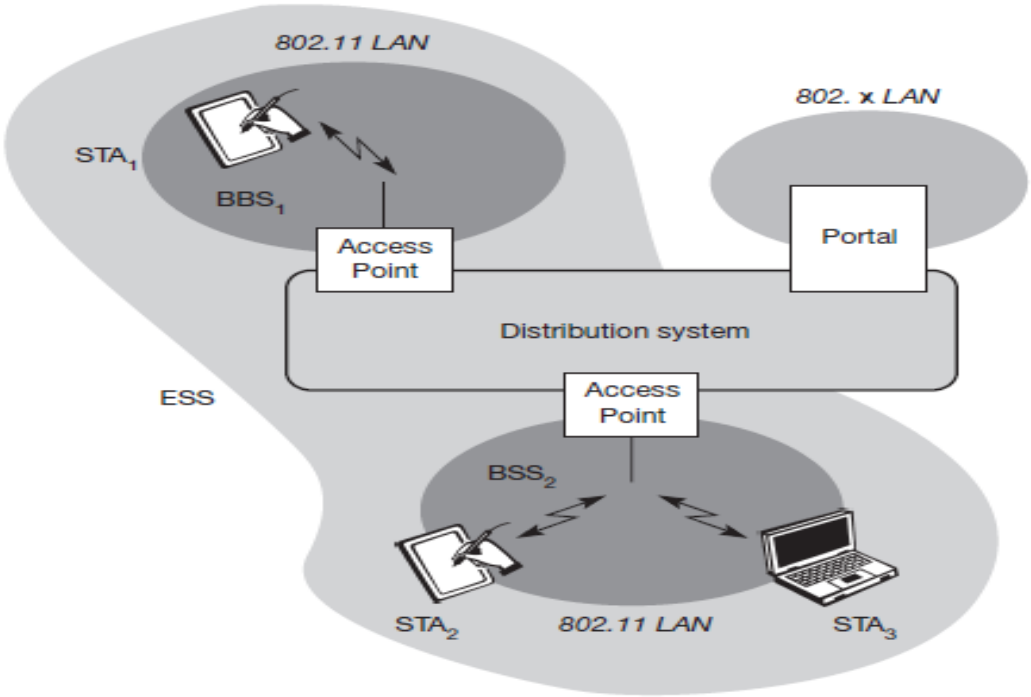
- The IEEE standard 802.11 (IEEE, 1999) specifies the most famous family of WLANs in which many products are available.
- As the standard's number indicates, this standard belongs to the group of 802.x LAN standards, e.g., 802.3 Ethernet or 802.5 Token Ring.
- This means that the standard specifies the physical and medium access layer adapted to the special requirements of wireless LANs, but offers the same interface as the others to higher layers to maintain interoperability.
- 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.
- Additional features of the WLAN should include the support of power management to save battery power, the handling of hidden nodes, and the ability to operate worldwide.

IEEE 802.11(WLAN) System architecture:

- Wireless networks can exhibit two different basic system architectures as,
  - Infrastructure-based
  - Ad-hoc based

Infrastructure-based:

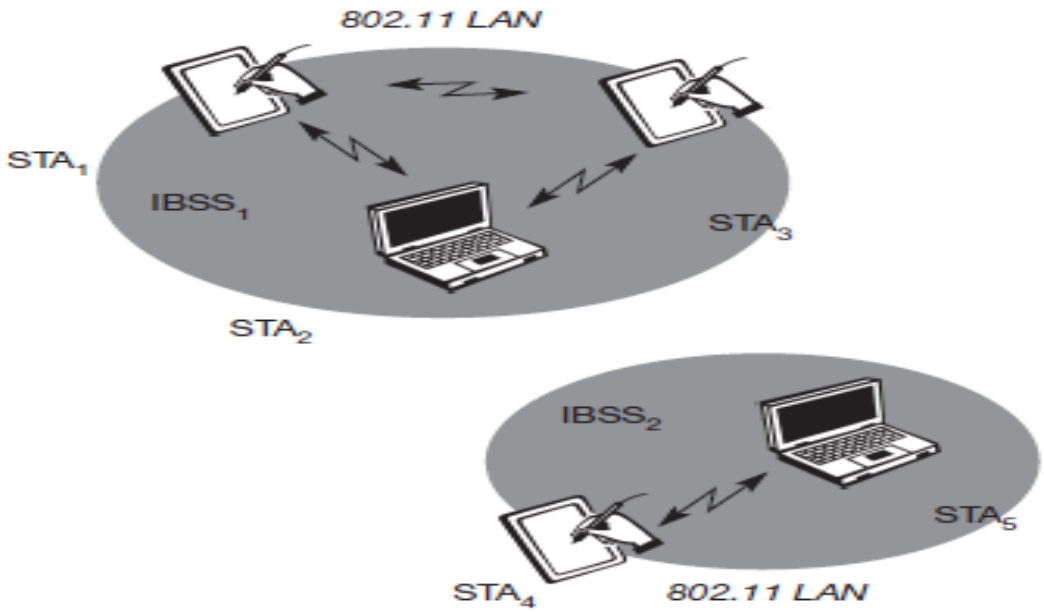
- The components of an infrastructure and a wireless part as specified for IEEE 802.11.
- Several nodes, called **stations (STAi)**, are connected to **access points (AP)**.
- Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP.
- The stations and the AP which are within the same radio coverage form a **basic service set (BSSi)**.



- The example shows two BSSs – BSS1 and BSS2 – which are connected via a **distribution system**.
- A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area.
- This network is now called an **extended service set (ESS)** and has its own identifier, the ESSID.
- The ESSID is the 'name' of a network and is used to separate different networks. Without knowing the ESSID it should not be possible to participate in the WLAN.
- The distribution system connects the wireless networks via the APs with a **portal**, which forms the interworking unit to other LANs.
- Access Point (AP),
    - Provide synchronization within a BSS,
    - Supports roaming, power management,
    - Control medium access to support time-bounded service.
- The distribution system handles data transfer between the different APs.

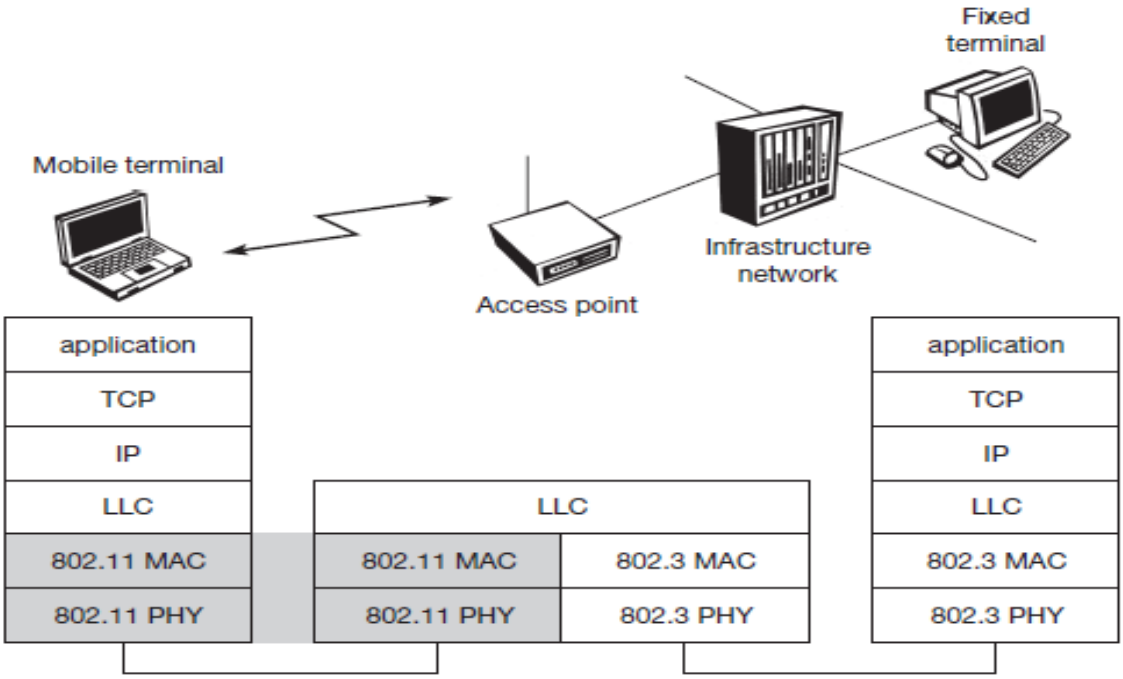
Ad-hoc based:

- In addition to infrastructure-based networks, IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSSs (IBSS) .
- In this case, an IBSS comprises a group of stations using the same radio frequency. Stations STA1, STA2, and STA3 are in IBSS1, STA4 and STA5 in IBSS2.
- This means for example that STA3 can communicate directly with STA2 but not with STA5.
- Several IBSSs can either be formed via the distance between the IBSSs or by using different carrier frequencies.
- IEEE 802.11 does not specify any special nodes that support routing, forwarding of data or exchange of topology information as, e.g., HIPERLAN 1 or Bluetooth.

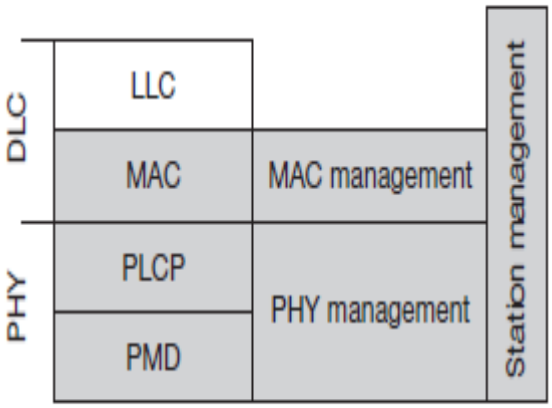


IEEE 802.11 Protocol architecture:

- IEEE 802.11 fits seamlessly into the other 802.x standards for wired LANs. Figure the most common scenario: an IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge.
- The WLAN behaves like a slow wired LAN. Consequently, the higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes.
- The upper part of the data link control layer, the logical link control (LLC), covers the differences of the medium access control layers needed for the different media.



- The IEEE 802.11 standard only covers the physical layer **PHY** and medium access layer **MAC** like the other 802.x LANs do.
- The physical layer is subdivided into the **physical layer convergence protocol (PLCP)** and the **physical medium dependent** sublayer **PMD**.
- The basic tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption.



- The PLCP sublayer provides a carrier sense signal, called clear channel assessment (CCA), and provides a common PHY service access point (SAP) independent of the transmission technology.
- The PMD sublayer handles modulation and encoding/decoding of signals.
- The **MAC management** supports the association and re-association of a station to an access point and roaming between different access points.
- It also controls authentication mechanisms, encryption, synchronization of a station with regard to an access point, and power management to save battery power.

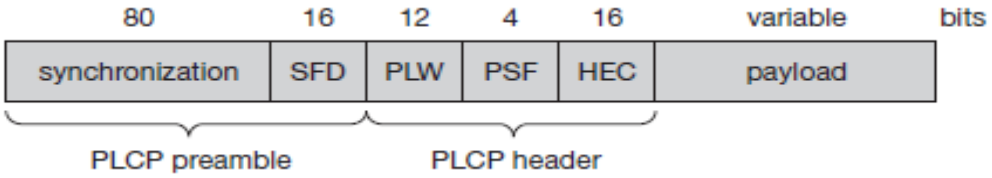
- MAC management also maintains the MAC management information base (MIB).
- The main tasks of the **PHY management** include channel tuning and PHY MIB maintenance.
- **Station management** interacts with both management layers and is responsible for additional higher layer functions (e.g., control of bridging and interaction with the distribution system in the case of an access point).

IEEE 802.11 Physical Layer:

- IEEE 802.11 supports three different physical layers:
  - one layer based on **infra-red** and
  - two layers based on **radio transmission** (ISM band at 2.4 GHz, which is available worldwide).
- 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 transmission technology determines exactly how this signal is obtained.
- The PHY layer offers a service access point (SAP) with 1 or 2 Mbit/s transfer rate to the MAC layer.

Frequency hopping spread spectrum (FHSS)

- Frequency hopping spread spectrum (FHSS) is a spread spectrum technique which allows for the coexistence of multiple networks in the same area by separating different networks using different hopping sequences.
- Below Figure shows a frame of the physical layer used with FHSS.
- The frame consists of two basic parts: **PLCP** part (preamble and header), **Payload** part.

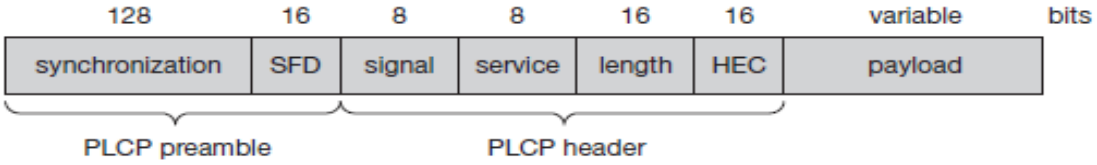


- The fields of the frame fulfill the following functions:

Synchronization:	The PLCP preamble starts with 80-bit synchronization, this pattern is used for synchronization of potential receivers and signal detection by the CCA.
Start frame delimiter (SFD):	The 16 bits indicate the start of the frame and provide frame synchronization. Pattern is 0000110010111101.
PLCP PDU length word(PLW):	This first field of the PLCP header indicates the length of the payload in bytes including the 32-bit CRC at the end of the payload.
PLCP signaling field (PSF):	The 4-bit field indicates the data rate of the payload following. All bits set to **zero (0000) indicates** the lowest data rate of **1 Mbit/s**. **2 Mbit/s is indicated by 0010** and the **maximum is 8.5 Mbit/s (1111)**.
Header error check (HEC):	The PLCP header is protected by a 16-bit checksum with the ITU-T generator polynomial $G(x) = x^{16} + x^{12} + x^5 + 1$.

Direct sequence spread spectrum (DSSS)

- DSSS is the alternative spread spectrum method separating by code and not by frequency.
- In the case of IEEE 802.11 DSSS, spreading is achieved using the 11-chip Barker sequence (+1, –1, +1, +1, –1, +1, +1, +1, –1, –1, –1).
- The key characteristics of this method are its robustness against interference and its insensitivity to multipath propagation (time delay spread). The implementation is more complex compared to FHSS.
- Below Figure shows a frame of the physical layer using DSSS.



- The frame consists of two basic parts: **PLCP** part (preamble and header), **Payload** part
- The fields of the frame have the following functions:

Synchronization:	The first 128 bits are not only used for synchronization, but also gain setting, energy detection (for the CCA), and frequency offset compensation.
Start frame delimiter (SFD):	This 16-bit field is used for synchronization at the beginning of a frame and consists of the pattern 1111001110100000.
Signal:	Only two values have been defined for this field to indicate the data rate of the payload. The value **0x0A indicates 1 Mbit/s (DBPSK)**, **0x14 indicates 2 Mbit/s (DQPSK).** Other values have been reserved for future use, i.e., higher bit rates.
Service:	This field is reserved for future use; however, 0x00 indicates an IEEE 802.11 compliant frame.
Length:	16 bits are used in this case for length indication of the payload in microseconds.
Header error check (HEC):	Signal, service, and length fields are protected by this checksum using the ITU-T CRC-16 standard polynomial.

Infra-red:

- The PHY layer, which is based on infra-red (IR) transmission, uses near visible light at 850–950 nm.
- Infra-red light is not regulated apart from safety restrictions (using lasers instead of LEDs).
- The standard does not require a line-of-sight between sender and receiver, but should also work with diffuse light. This allows for point-to-multipoint communication.
- This type of network will only work in buildings, e.g., classrooms, meeting rooms etc. Frequency reuse is very simple – a wall is more than enough to shield one IR based IEEE 802.11 network from another.
- Today, no products are available that offer infra-red communication based on 802.11.
- Alternatively, directed infra-red communication based on IrDA can be used (IrDA, 2002).

****