CS 480: MOBILE NETWORKS

Medium Access Control

29th November 2016

Topics Covered

- Introduction
- Motivation for a specialized MAC
  - Hidden and exposed terminals
  - Near and far terminals
- Space Division Multiple Access (SDMA)
- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
  - Fixed TDM
  - Classical Aloha
  - Slotted Aloha
  - Carrier sense multiple access (CSMA)
  - Polling
- Code division multiple access (CDMA)
  - Spread Aloha multiple access

Introduction (1)

- This lecture introduces **medium access control** (MAC) algorithms specifically adapted to the wireless domain
- MAC comprises all mechanisms that regulate user access to a medium
  - using Space Division Multiplexing (SDM), Time Division Multiplexing (TDM), Frequency Division Multiplexing (FDM), or Code Division Multiplexing (CDM).
- MAC is thus similar to traffic regulations in the highway.
  - The fact that several vehicles use the same street crossing in TDM, for example, requires rules to avoid collisions
  - one mechanism to enforce these rules is traffic lights.

Introduction (2)

- The previous lecture (Wireless transmission) mainly introduced mechanisms of the physical layer,
  - layer 1, of the ISO/OSI reference model
- MAC belongs to layer 2, the **data link control layer (DLC)**
- Layer 2 is subdivided into the MAC, layer 2a and logical link control (LLC), layer 2b.
- The task of the DLC is to establish a reliable point to point or point to multi-point connection between different devices over a wired or wireless medium.

Motivation for specialized MAC

Motivation for specialized MAC (1)

- Is it possible to use elaborated MAC schemes from wired networks?
  - such as CSMA/CD as used in the original specification of IEEE 802.3 networks (aka Ethernet)
- Consider carrier sense multiple access with collision detection (CSMA/CD) which works as follows:
  - A sender senses the medium (a wire or 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.
- Why does this scheme fail in wireless networks?

Motivation for specialized MAC (2)

- CSMA/CD is not interested in collisions at the sender, but in those at the receiver.
- The signal should reach the receiver without collisions, but the sender is the one detecting collisions.
- This is not a problem using a wire, as more or less the same signal strength can be assumed all over the wire
  - if the length of wire stays within certain often standardized limits.
- If a collision occurs along a wire, everyone will notice it.
- A sender can listen into the medium at its location to detect a collision that occurs at the receiver
- The situation is different in wireless networks.
  - The signal strength decreases proportionally to square of the distance to sender. Obstacles attenuate the signal even further.

Motivation for specialized MAC (3)

- The sender may now apply carrier sense and detect an idle medium.
  - The sender may now starts sending – but a collision happens at the receiver due to a second sender.
- 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 data at a 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.

Hidden and exposed terminals (1)

- Consider the scenario with three mobile phones as shown in Figure 1.
- 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.
- The transmission range of B reaches A and C,
  - i.e., A cannot detect C and vice versa.
- A starts sending to B, C doesn’t receive this transmission
- C also wants to send something to B and senses the medium.
- The medium appears to be free, the sense carrier fails.
- C also starts sending causing a collision at B.
  - But A cannot detect this collision at B and continues with its transmission.

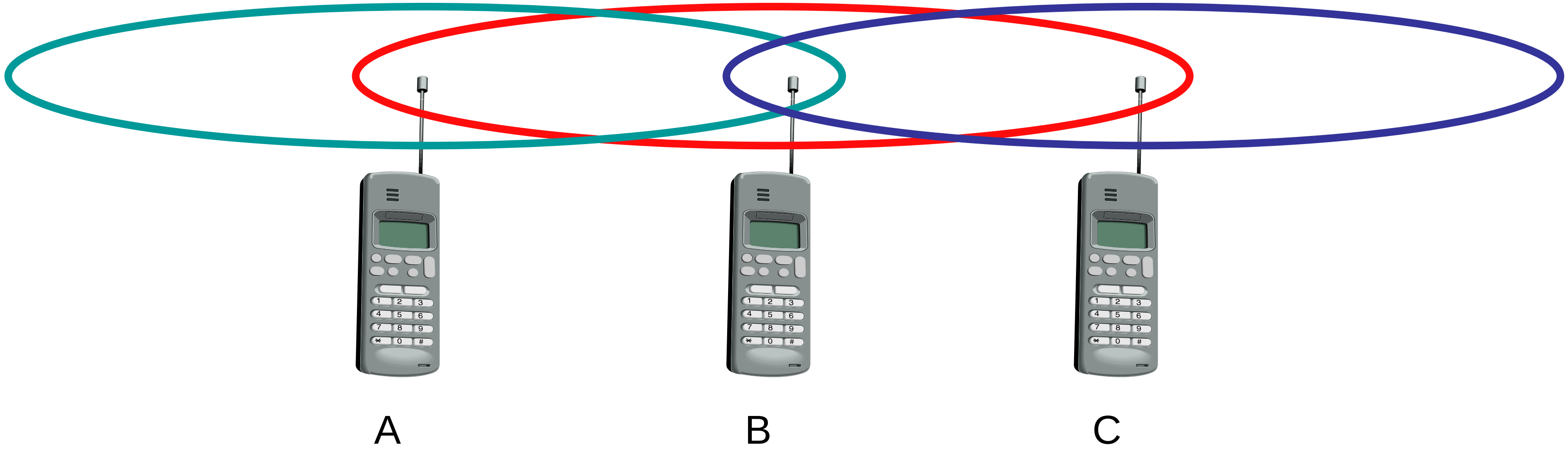


Figure 1: Hidden and exposed terminals

Hidden and exposed terminals (2)

- A is **hidden** for C and vice versa.
- While hidden terminals may cause collisions, the next effect only causes unnecessary delay.
- Consider a 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 (1)

- Consider the situation as shown in Figure 2.
- A and B are both sending with same transmission power.
- As 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.
- Think of C as being an arbiter for sending rights (e.g., C acts as a base station coordinating media access).
  - In this case, terminal B would already drown out terminal A on the physical layer.
- C in return would have no chance of applying a fair scheme as it would only hear B.
- The near/far effect is a severe problem of wireless networks using CDM.
  - All signals should arrive at the receiver with more or less the same strength.

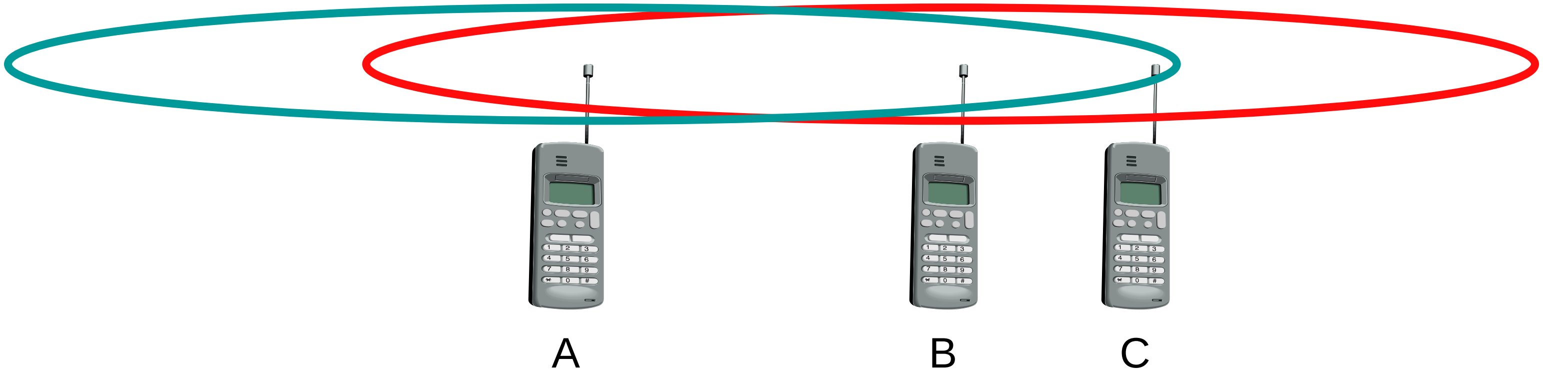


Figure 2: Near and far terminals

Near and far terminals (2)

- Otherwise a person standing closer to somebody could always speak louder than a person further away.
- Even if senders were separated by code, the closest one would simply drown out the others.
- Precise power control is needed to receive all senders with the same strength at a receiver.
- For example, the UMTS system adapts 1,500 times per second.

Space Division Multiple Access (SDMA)

SDMA (1)

- **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 medium access control (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
- Typically, SDMA is never used in isolation but always in combination with one or more other schemes

SDMA (2)

- 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 (e.g., measured in bit/s/m^2 or voice calls/m^2 tremendously).

Frequency Division Multiple Access (FDMA)

FDMA (1)

- To accommodate nodes inside a wireless network,
  - FDMA divides the available spectrum into subbands each of which are used by one or more users.
- FDMA comprises all algorithms allocating frequencies to transmission channels according to frequency division multiplexing (FDM) scheme.
  - Channels can be assigned to the same frequency at all times, i.e. pure FDMA, or change frequencies according to some pattern, i.e., FDMA combined with TDMA
- FDMA combined with TDMA is a 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

FDMA (2)

- FDM is often used for simultaneous access to a medium by base station and mobile station in cellular networks.
- The two partners typically establish a duplex channel,
  - i.e., a channel that allows for simultaneous transmission in both directions.
- Two directions, mobile station to base station and vice versa are now separated using different frequencies.
- This scheme is called frequency division duplex (FDD)
- Both partners have to know the frequencies in advance; they cannot just listen into the medium.

FDMA (3)

- The frequencies are also known as uplink (from mobile station to base station, or from ground control to satellite)
  - and as downlink (from base station to mobile station or from satellite to ground control).
- As for example FDM and FDD, Figure 3 shows the situation in a mobile phone network based on the GSM standard for 900 MHz.
  - The basic frequency allocation scheme for GSM is fixed and regulated by national authorities.
  - All uplinks use the band between 890.2 and 915 MHz, all downlinks use 935.2 to 960 MHz.

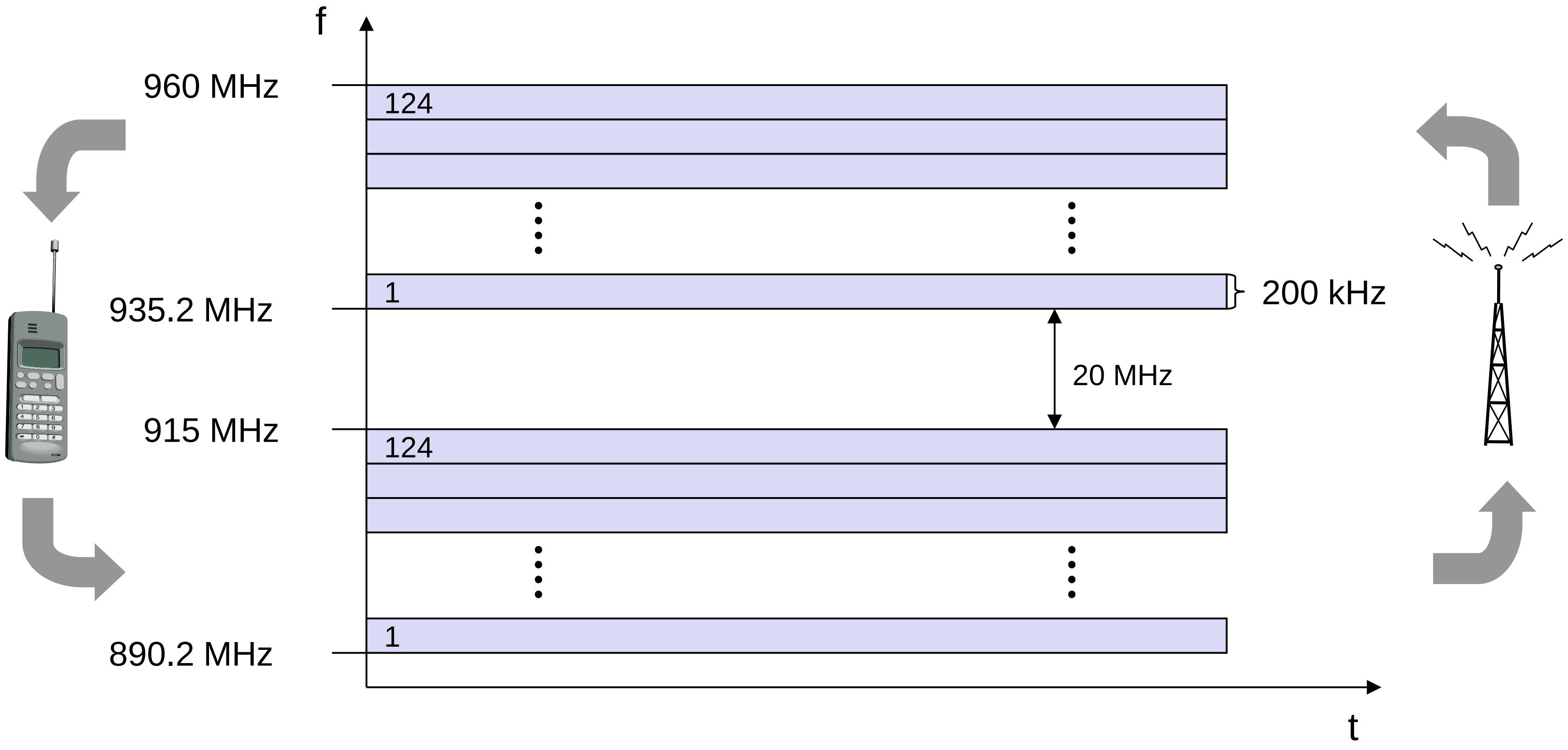


Figure 3: frequency division multiplexing for multiple access and duplex

FDMA (4)

  - According to FDMA, the base station allocates a certain frequency for up- and downlink to establish a duplex channel with a mobile phone.

- Similar schemes for FDD are implemented in
  - AMPS (Advanced Mobile Phone System),
  - IS (Interim Standard)-54, IS-95, IS-136,
  - PACS (Personal Access Communications System),
  - and UMTS (Universal Mobile Telecommunications System)

Time Division Multiple Access (TDMA)

TDMA (1)

- TDMA offers a much more flexible scheme than FDMA
- TDMA comprises all technologies that allocate certain time slots for communication
  - i.e., controlling TDM.
- Tuning in to 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 many channels separated in time at the same frequency is simple compared to listening to different frequencies at the same time

TDMA (2)

- Almost of medium access control (MAC) schemes for wired networks work according to this principle,
  - e.g. Ethernet, Token Ring, ATM etc
- Synchronization between sender and receiver has to be achieved in the time domain.
  - This is done by allocating a certain time slot for a channel, or by using a dynamic allocation scheme

Fixed TDM (1)

- 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
- Medium access control is quite simple;
  - the only crucial factor is accessing the reserved time slot at the right moment.
- 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 fit perfectly well for connections with a fixed bandwidth.

Fixed TDM (2)

- TDMA schemes with fixed access patterns are used in many digital mobile phone systems like GSM, DECT
- Figure 4 shows how fixed TDM patterns are used to implement multiple access and a duplex channel between a base station and a mobile station.
- Assigning different slots for uplink and downlink using the same frequency is called time division duplex (TDD)
- In Figure 4, the base station uses one of 12 different slots for the downlink,
  - the mobile station uses one of the 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.

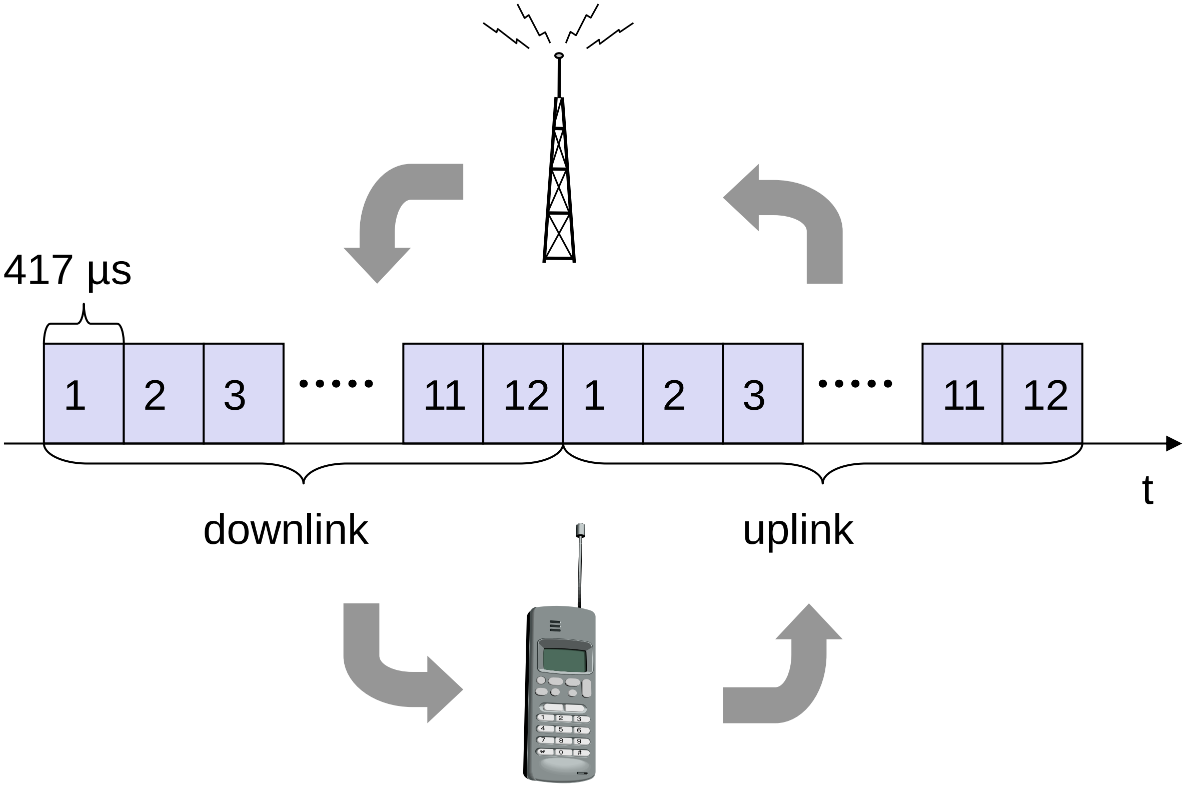


Figure 4: Time division multiplexing for multiple access and duplex

Fixed TDM (3)

- Each connection is allotted its own up- and downlink pair
- For DECT cordless phone system,
  - the pattern is repeated every 10 ms, i.e., each slot has a duration of 417 µs (=10ms/24)
- Fixed access patterns are suitable for connections with a constant data rate
  - e.g. classical voice transmission with 32 or 64 kbit/s duplex
- they are very inefficient for bursty data or asymmetric connections
- This scheme still wastes a lot of bandwidth,
  - it is too static, too inflexible for data communication.
- In this case, demand-oriented TDMA schemes can be used

Classical Aloha (1)

- TDMA comprises all mechanisms controlling medium access according to TDM.
- What if TDM is applied without controlling access?
  - This is exactly what the classical Aloha scheme does.
- This 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 medium access (MAC) layer
- Each station can access the medium at any time as shown in Figure 5.

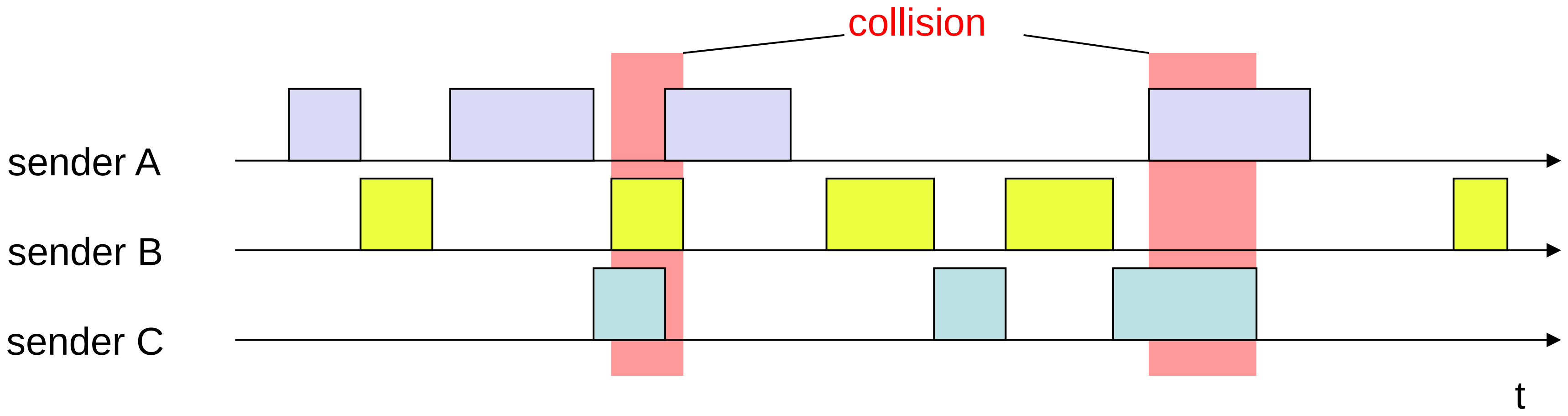


Figure 5: Classical Aloha multiple access

Classical Aloha (2)

- 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

Slotted Aloha (1)

- The first refinement of the classical aloha scheme is provided by introducing time slots (slotted aloha)
- In slotted aloha, all senders have to be synchronized,
  - transmission can only start at the beginning of a time slot as shown in Figure 6 but access is still not coordinated
- The introduction of time slots raises the throughput
  - from 18 per cent to 36 per cent, i.e. slotting doubles throughput
- 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 cannot give hard transmission guarantees such as maximum delay before accessing the medium or minimum throughput

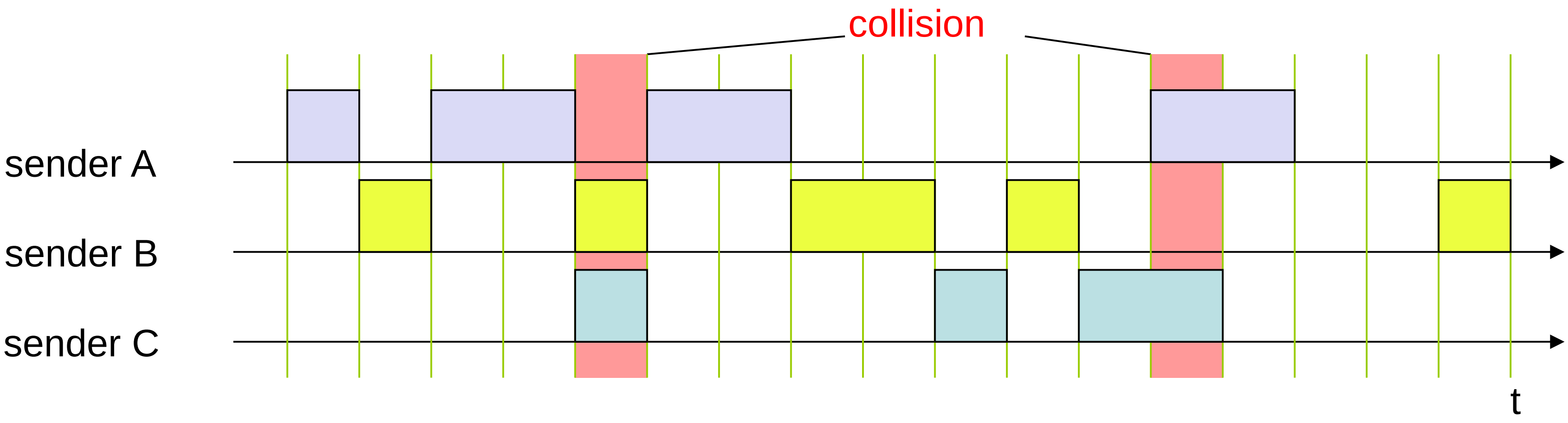


Figure 6: Slotted Aloha multiple access

Slotted Aloha (2)

- One thus needs additional mechanisms, e.g. combining fixed schemes and Aloha schemes
- New mobile communication systems like UMTS have to rely on slotted Aloha for medium access in certain situations.

Carrier sense multiple access (CSMA)

- One improvement to the basic Aloha is sensing the carrier before accessing the medium.
  - This is what CSMA schemes generally do.
- 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.
- 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.
  - Non-persistent CSMA
  - p-persistent CSMA
  - 1-persistent CSMA
  - CSMA with collision avoidance (CSMA/CA)
  - Eliminating yield non-preemptive multiple access (EY-NPMA)

non-persistent CSMA

- 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

p-persistent CSMA

- In *p-persistent CSMA* systems, nodes also sense the medium, but only transmit with a probability p, with the station deferring to the next slot with the probability 1-p

1-persistent CSMA

- In *1-persistent CSMA*, all stations wishing to transmit, access the medium at the same time, as soon as it becomes idle.
- This causes many collisions if many stations wish to send and block each other.
- To create fairness for stations waiting for a longer time, back-off algorithms can be introduced, which are sensitive to waiting time as this is done for standard Ethernet.

CSMA with collision avoidance (CSMA/CA)

- CSMA/CA is one of the access schemes used in wireless LANs following the standard IEEE 802.11.
- Sensing the carrier is combined with a back-off scheme in case of a busy medium to achieve some fairness among competing stations.

Eliminating yield non-preemptive multiple access (EY-NPMA)

- EY-NPMA is another very elaborate scheme used in HIPERLAN 1 specification
- Here several phases of sensing the medium and accessing the medium for contention resolution are interleaved before one “winner” can finally access the medium for data transmission
- Priority schemes can be included to assure preference of certain stations with more important data.

Multiple access with collision avoidance (MACA) (1)

- Consider one of the initial problems: hidden terminals.
- How do the previous access schemes solve this?
- To all schemes with central base stations assigning TDM patterns, the problem of hidden terminals is unknown.
- If the terminal is hidden for the base station it cannot communicate anyway.
- More or less fixed access patterns are not as flexible as Aloha schemes.
- What happens when no base station exists at all? This is the case in so-called ad-hoc networks.

Multiple access with collision avoidance (MACA) (2)

- Multiple access with collision avoidance (MACA) presents a simple scheme that solves the hidden terminal problem,
- The scheme does not need a base station, and is still a random access Aloha scheme
  - but with dynamic reservation.
- Figure 7 shows the same scenario as Figure 1, with the hidden terminals.
- Terminal A and C both want to send to B.
- Terminal 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.

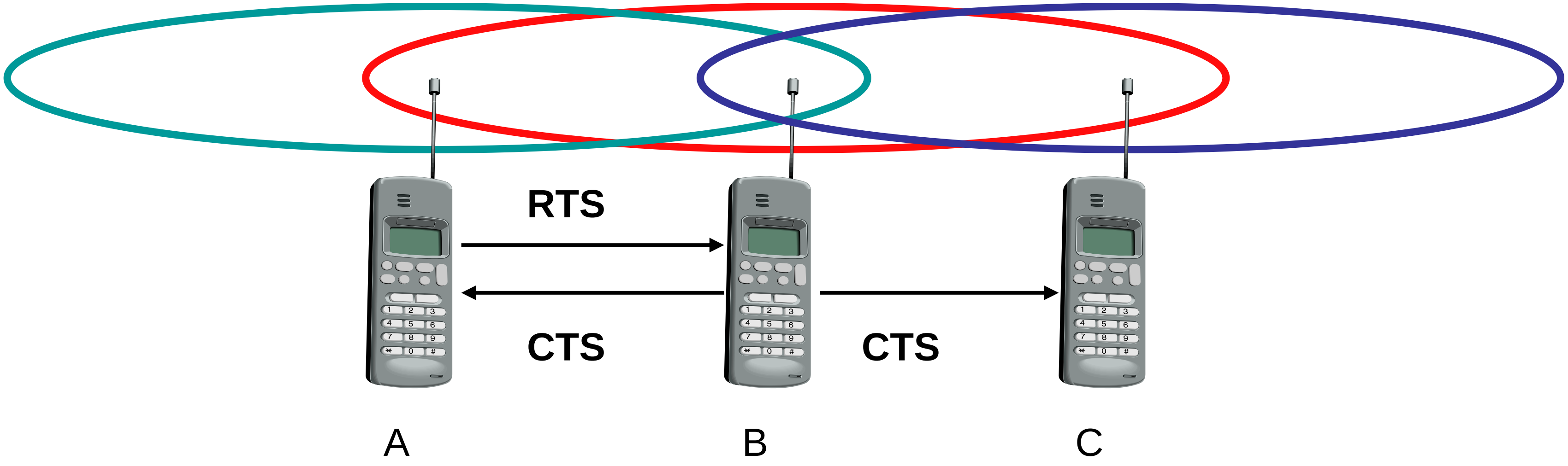


Figure 7: MACA can avoid hidden terminals

Multiple access with collision avoidance (MACA) (3)

- Terminal 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, 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 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.

Multiple access with collision avoidance (MACA) (4)

- A collision cannot occur at B during data transmission, and the hidden terminal problem is solved
  - provided that the transmission conditions remain the same.
- It is possible that another station could move into the transmission range of B after transmission of CTS.
- Still, collisions can occur during the sending of an RTS.
- Both A and C could send an RTS that collides at B.
- RTS is very small compared to the data transmission, so the probability of a collision is much lower.
- Terminal B resolves this contention and acknowledges only one station in the CTS (if it was able to recover the RTS at all).
- No transmission is allowed without an appropriate CTS.

Multiple access with collision avoidance (MACA) (5)

- This is one of the medium access schemes that is optionally used in the standard IEEE 802.11
- Can 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 (as shown in Figure 8) containing the name of the receiver (A) and the sender (B).

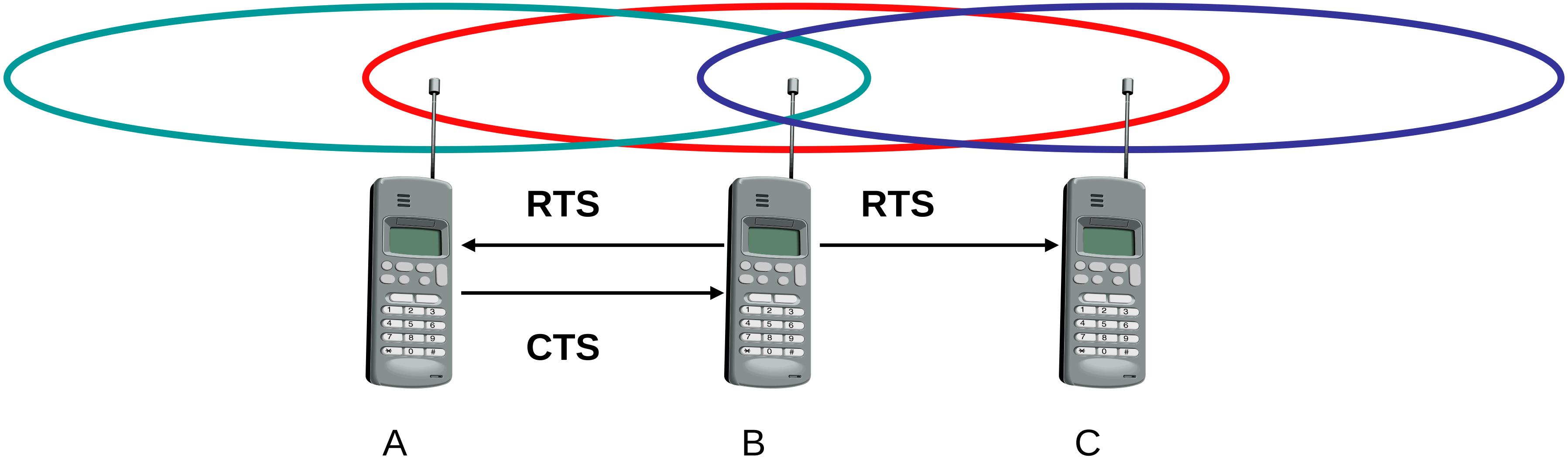


Figure 8: MACA can avoid exposed terminals

Multiple access with collision avoidance (MACA) (6)

- C does not react to this message as it is not the receiver,
  - but A acknowledges using a CTS which identifies B as a 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.
- The problem with exposed terminals is solved without fixed access patterns or a base station.
- One of the problem of MACA is clearly the overheads associated with the RTS and CTS transmissions
  - for short and critical data packets, this is not negligible.
- MACA also assumes symmetrical transmission and reception conditions.
  - Otherwise, a strong sender, directed antennas etc, could counteract the above scheme.

Polling

- Where one station is to be heard by all others (e.g., the base station of a mobile phone network or any other dedicated station) polling schemes can be applied
- Polling is a strictly centralized scheme with one master station and several slave stations.
- The master can poll slaves according to many schemes:
  - round robin (only efficient if traffic patterns are similar over all stations), randomly, according to reservations
- 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 of possible access function in IEEE 802.11 systems

Code Division Multiple Access (CDMA)

CDMA (1)

- Codes with certain characteristics can be applied to the transmission to enable the use of code division multiplexing (CDM)
- 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 code directly controls the chipping sequence
- A code for a certain user should
  - have good autocorrelation (large inner product with itself) and
  - be orthogonal (zero inner product with others) to other codes

CDMA (2)

- In CDMA all terminals send on the same frequency
  - probably at the same time and can use the whole bandwidth of the transmission channel
- Each sender has a unique random number,
  - the sender XORs the signal with this random number
- The receiver can “tune” into this signal if it knows the pseudo random number,
  - tuning is done via a correlation function
- Disadvantages of CDMA:
  - higher complexity of a receiver (receiver cannot just listen into the medium and start receiving if there is a signal)
  - all signals should have the same strength at a receiver

CDMA (3)

- Advantages of CDMA:
  - all terminals can use the same frequency, no planning needed
  - huge code space (e.g. 2^{32}) compared to frequency space
  - interferences (e.g. white noise) is not coded
  - forward error correction and encryption can be easily integrated

CDMA in theory (1)

Example 1: Two senders A and B, want to send data

- CDMA assigns the following unique and orthogonal key sequences:

  key A_k=010011 for sender A

  key B_k = 110101 for sender B

  - Sender A wants to send the bit A_d=1 and sender B sends B_d=0
  - Assume that we code a binary “0” as -1, a binary “1” as +1

- Both senders spread their signal using their key as chipping sequence
  - Spreading here refers to simple multiplication of the data bit with the whole chipping sequence
  - Sender A then sends signal $A_s = A_d*A_k = +1*(-1, +1, -1, -1, +1, +1) =(-1, +1, -1, -1, +1, +1)$

CDMA in theory (2)

- Sender B does the same with its data to spread the signal with the code:

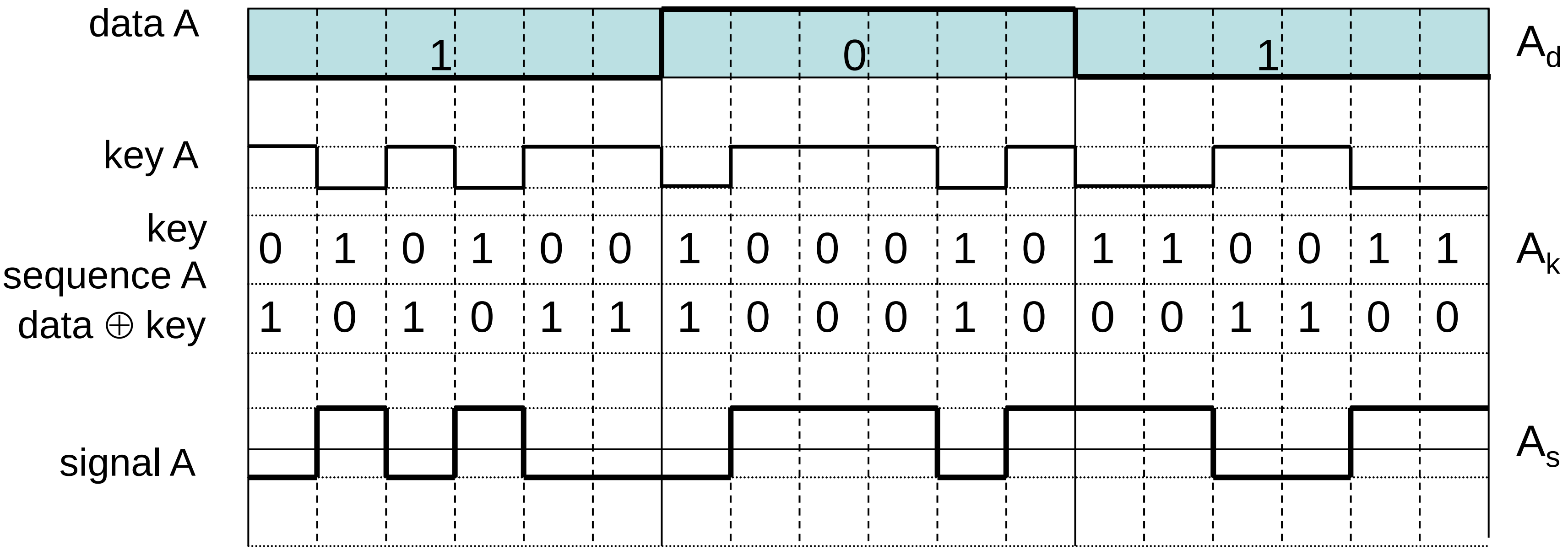
  $B_s = B_d * B_k = (-1, -1, +1, -1, +1, -1)$

- Both signals are transmitted at the same time using the same frequency, so they superimpose in space
  - Interference neglected (noise etc.)
  - Assuming signals have same strengths at the receiver, the following signal is received at a receiver: $C = A_s + B_s$ $= (-2, 0, 0, -2, +2, 0)$
- The receiver now wants to receive data from sender A and thus tunes in to the code of A
  - applies A’s code for despreading: $C * A_k = 2 + 0 + 0 + 2 + 2 + 0 = 6$
  - result greater than 0, therefore, original bit was “1”
  - tuning in to sender B, i.e. applying B’s code gives $C * B_k = -2 + 0 + 0 - 2 - 2 + 0 = -6$, i.e. “0”

CDMA in theory (3)

Example 2: Figure 9 shows a sender A that wants to send the bits 101.

- The key of A is shown as signal and binary key sequence A_k.
- The binary “0” is assigned a positive signal value, the binary “1” a negative signal value
- After spreading (XORing) A_d and A_k, the resulting signal is A_s.
- The same happens with data from sender B, here the bits are 100.
- The result of spreading with code is the signal B_s.

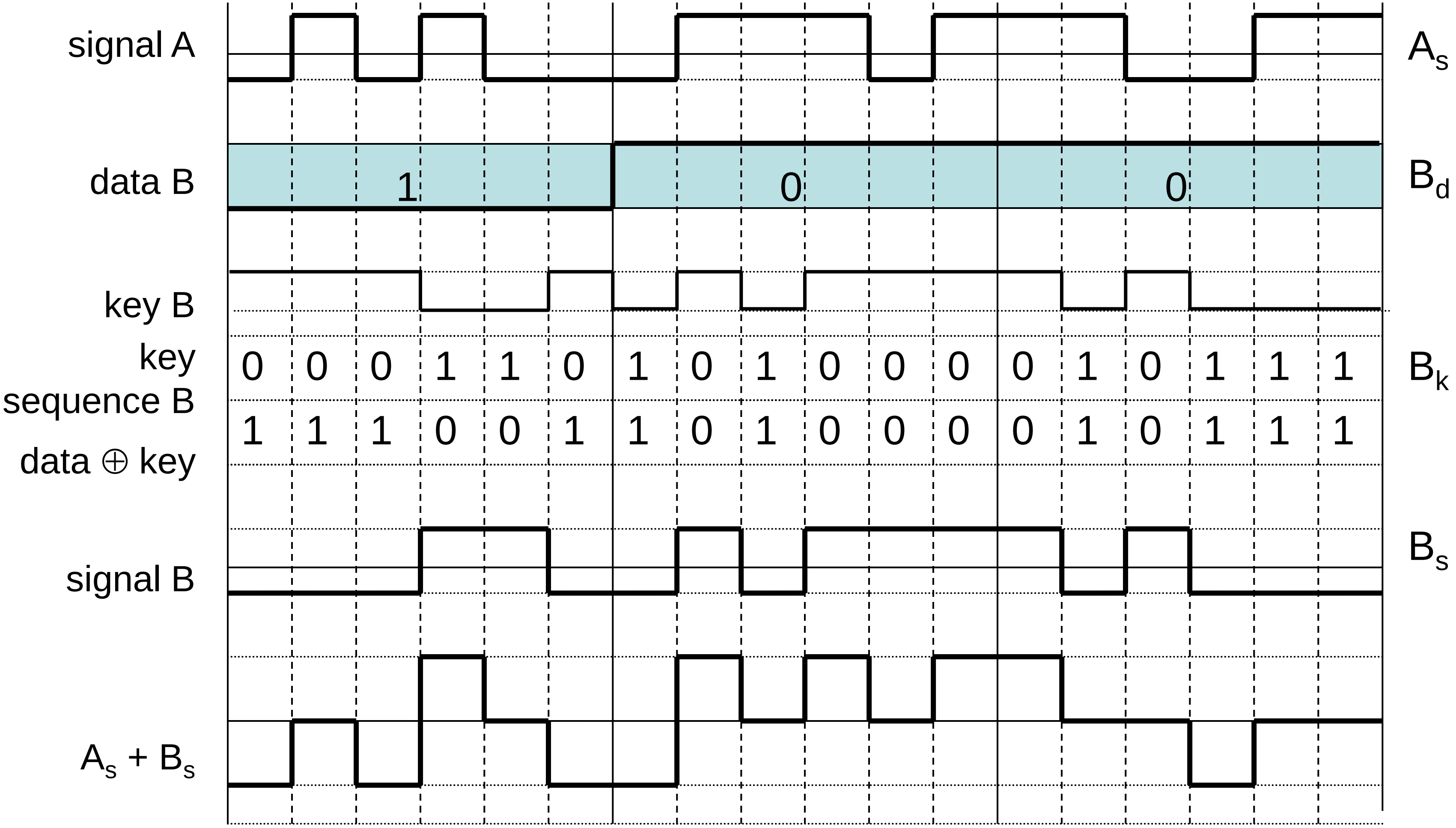


data A	1						0						1					
key sequence A	0	1	0	1	0	0	1	0	0	0	1	0	1	1	0	0	1	1
data ⊕ key	1	0	1	0	1	1	1	0	0	0	1	0	0	0	1	1	0	0

Figure 9: Coding and spreading of data from sender A

CDMA in theory (3)

- A_s and B_s now superimpose during transmission.
- The resulting signal is simply the sum A_s+B_s as shown in Figure 10.
- A receiver now tries to reconstruct the original data from A, A_d (see Figure 11)
  - A receiver applies A’s key, A_k to the received signal and feeds the results into an integrator
  - The integrator adds the products (calculates inner product)
  - A comparator then decides if result is 0 or 1
- The same happens if a receiver wants to receive B’s data (see Figure 12)



key sequence B	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	1	1	1
data ⊕ key	1	1	1	0	0	1	1	0	1	0	0	0	0	1	0	1	1	1

B_k

Figure 10: Coding and spreading of data from sender B

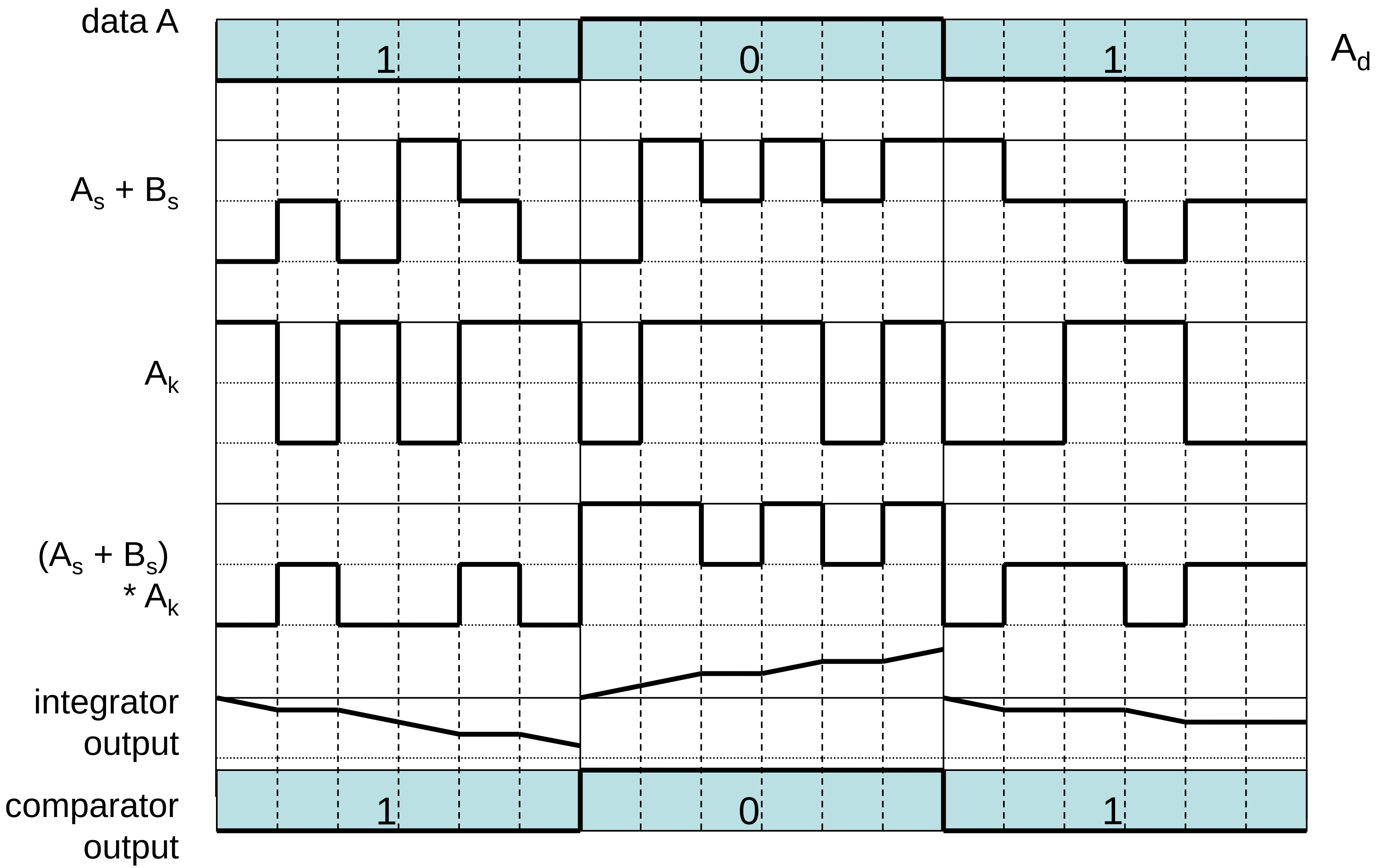


Figure 11: Reconstruction of A's data

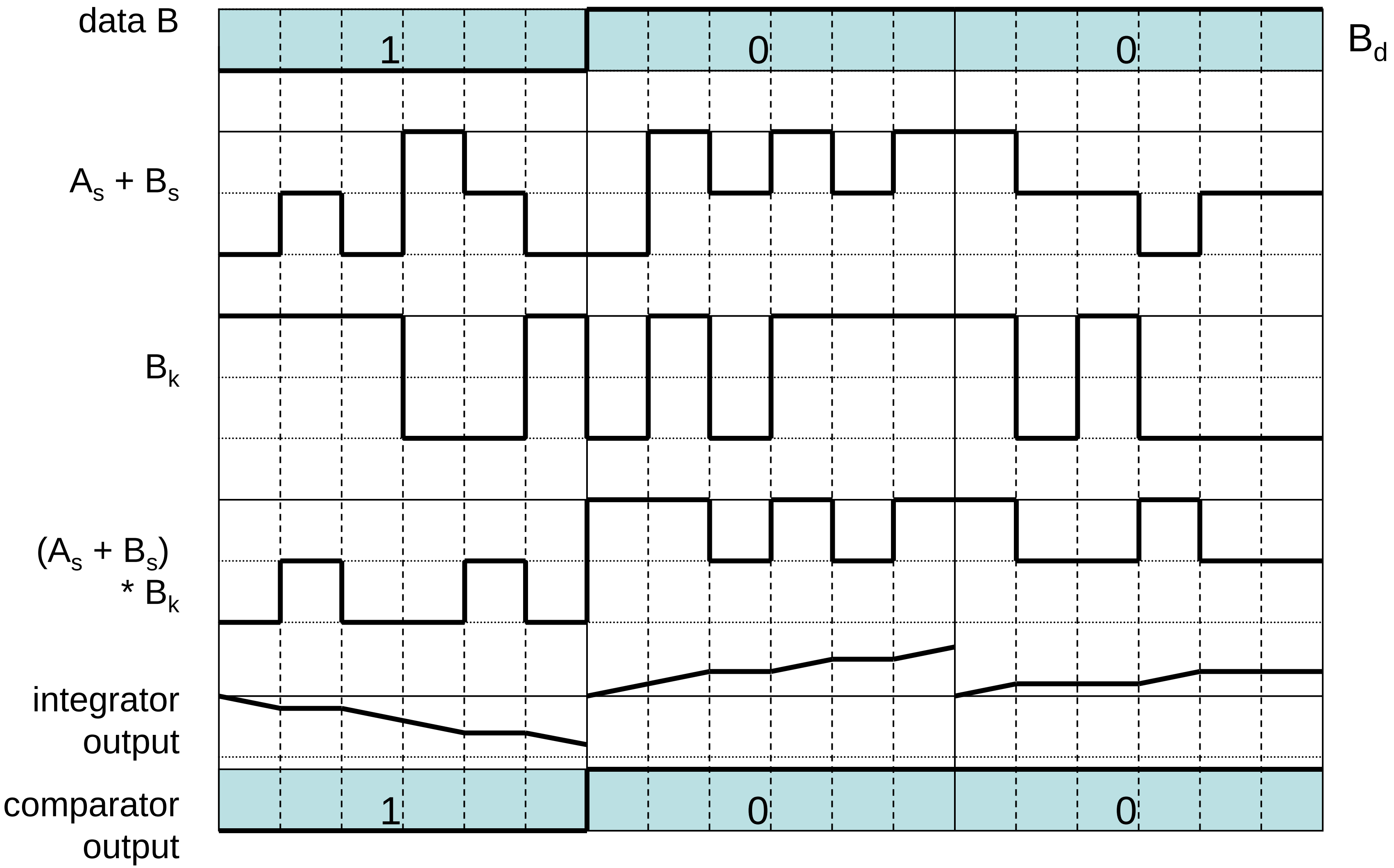


Figure 12: Reconstruction of B's data