Information Technology

Mobile Computing

Module: MACA (Medium access control with collision avoidance)

Learning Objectives

- Understand need of medium access control is necessary in wireless environment
- Understand motivation behind separate MAC protocols for wireless environment
- Understand Hidden and Exposed terminal problem
- Understand Near and far terminal problem
- MACA algorithm to solve the problems due to CSMA/CD in wireless environment
- MAC protocols used in IEEE 802.11

Introduction

Medium Access Control, allow several users to share a common medium of communication simultaneously. An efficient MAC technique should have goal of maximum channel utilization with minimum interference and collisions and provide reliable point-to-point or multipoint connection between different devices on medium. The common MAC algorithms existing in wired networks cannot be simply replicated in wireless networks due to situations like Hidden and Exposed terminal problem and near and far terminal problem. Due to these problems, the existing MAC algorithms like CSMA/CD fails in wireless scenario. This module discusses these problems and presents the motivation behind need of specialized MAC algorithms in wireless scenario. The module also discusses some of the alternative algorithms to CSMA/CD which works well in the wireless environment like MACA, MACAW and virtual carrier sense.

Medium Access Control

Medium Access Control is protocol of data link layer. It is used to regulate the control of access among different users without or very less collisions. The transmission medium in wireless communication is air or atmosphere which is shared by multiple users or subscribers. In such a situation, simultaneous access by multiple users can lead to collisions. A good MAC algorithm should minimize the number of collisions hence increasing the throughput at the same time maintain fairness among the users.

The perfect analogy to this situation is Highway where more than one vehicle can arrive at same or different points of time. If the traffic on highway is not controlled in an efficient and systematic way, accidents can occur. Therefore different traffic control mechanisms should be applied. Similarly in wireless networks access to the transmission media should be controlled using different modulation and multiplexing techniques. Medium access control is one of the two sub-layers of Data Link layer of ISO/OSI reference model. The biggest challenge of medium access control is that wireless devices should transmit without interfering with the signals of neighboring wireless devices.

Need for Specialized MAC in wireless Communications

Let us now understand whether the standard MAC algorithms used in wired networks, can be replicated in wireless scenario. For this we first understand the basic CSMA/CD **Carrier Sense multiple access with collision detection** used in IEEE 802.3 wired networks. It works as follows:

- **Sense the medium**

Analogy: In a round table conference, different people participate and communicate. They sense through their eyes and ears to find if anyone is talking. If anyone senses someone talking, he remains quite i.e. “Listen before you talk”.

- **If free, transmit else wait**

Analogy: If it is found that no one is talking, press the button to initiate talk and start talking. For that time, others will sense the medium to be busy.

- **Continuously listen to the medium for any collisions**

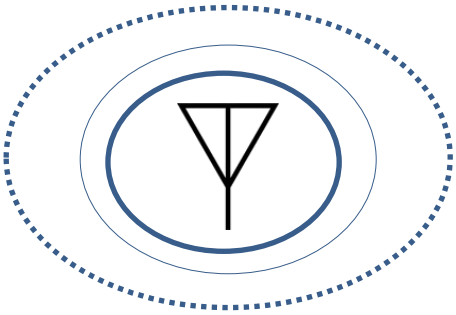
Analogy: Observe if the speech has coincided with some other person.

- **Stop in case of collision detection and sends a jamming signal**

Analogy: The person stops talking and repeats its previous speech.

The scheme works well in wired scenario. In wired communication, all devices are connected through wire and the strength of the signal is uniform throughout the wire hence all the devices can listen to the medium and detect the collision if it exists. But in wireless scenario there are many other issues which will not allow CSMA/CD to function properly. They are:

a) In wireless environment, signal propagates in omnidirectional way in all directions and the strength of the signal decreases inversely as square of distance from the transmitter.



b) The objects in the way from sender to receiver also offers various effects like reflection, scattering, diffraction leading to multipath propagation and many other undesirable effects which degrades the signal as shown in Fig. 1

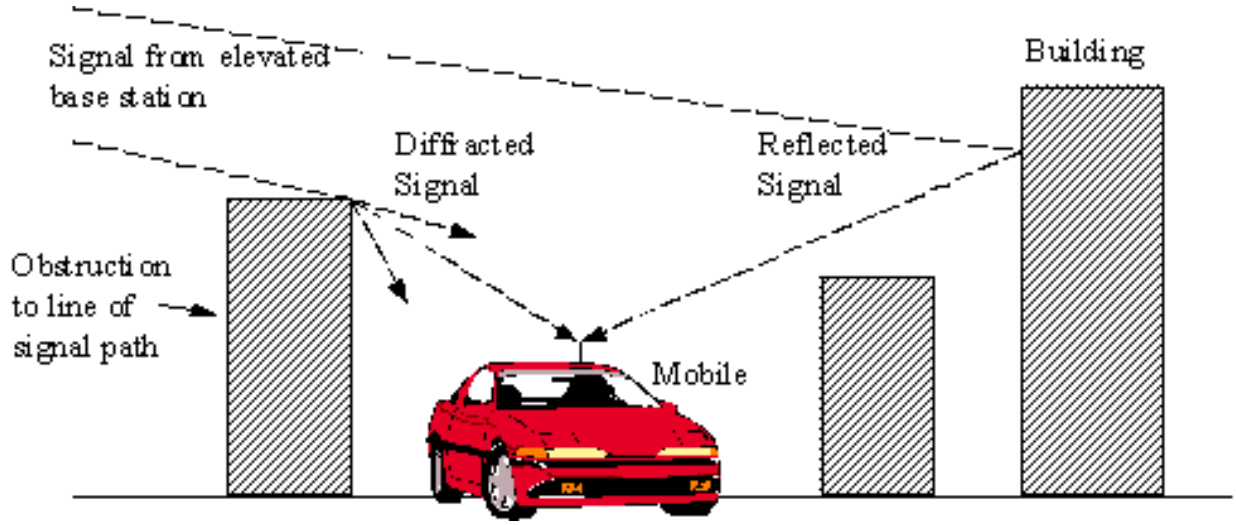


Figure 1: Various effects degrading the quality of the signal

c) The receiving power is very much less than transmitting power. Wireless transceivers can't send and receive on the same channel at the same time, so they can't detect collisions.

d) Hidden and exposed terminal problem and near and far terminal problem are other situations which fails the use of CSMA/CD in wireless networks.

Let us understand the hidden and exposed terminal problem and near and far terminal problem typical to wireless networks.

Hidden Terminal Problem

As the strength of the signal transmitting from a wireless device, decreases with distance, the transmission is limited to a certain area known as transmission range after which the signal diminishes. A device can listen only to those devices which are in its range others are said to be **hidden** from it.

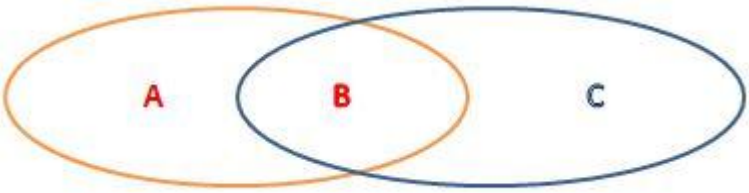


Figure 2: Hidden terminals A and C

In Figure 2, A is in transmission range of B. B is in transmission range of C but A&C are in not in transmission range of each other. A and C are said to be hidden from each other.

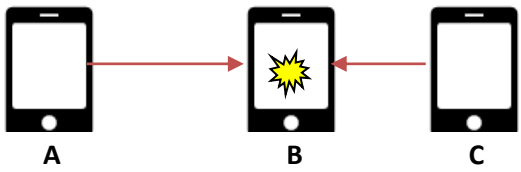


Figure 3: A and C are hidden from each other

Following sequence of events (Fig. 3) illustrate why CSMA/CD fails in hidden terminal situation:

- A wish to transmit, senses the medium, finds it to be idle.
- A transmits. C cannot hear transmission of A
- C wish to transmit, senses the medium, also finds it to be idle**.(Carrier sense fails)**
- Collision occurs at B
- Collision not heard by both A&C **(Collision detection fails)**
- Both Continue transmitting
- A and C are said to hidden from each other

Hidden terminal problem decreases the throughput because of collisions

Analogy: Two people want to talk to a third person but they cannot hear each other. So when one person is talking, other cannot sense it, finds the way free, he also talks and both the

conversation coincides. Further they do not even know that there is collision of speech and continue talking.

Exposed terminal problem

- B is transmitting to A, C can hear it
- D is in transmission range of C
- C wish to transmit to D
- C sense medium, finds it busy because of transmission of B
- C waits causing delay(Fig. 4)

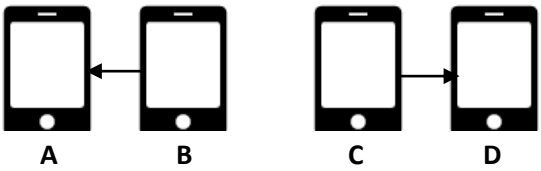


Figure 4: Exposed Terminal Problem

Near and far terminal problem

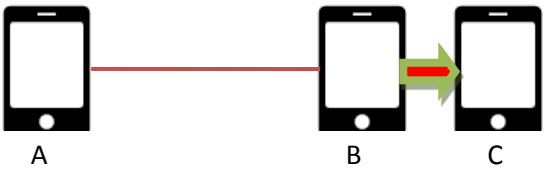


Figure 5: Near and Far Terminal Problem

To illustrate this problem, let us view a situation when three terminals A, B and C are such that B is farther from A and nearer to C as shown in Fig. 5. In this situation when A and B both transmit with equal power, but the strength of signal of A decreases as it reaches C due to distance from C. At the same time power of B is strong and it drowns signal of A. This problem is more acute in Code division multiplexing because all stations transmit with same power yet they are at different distance from the receiver. Hence the near terminals drown signal of far terminals. Therefore regular power regulation is required in CDM. E.g. UMTS regulates power 1,500 times in a second.

Analogy: People sitting in the same hall speak at the same time. The receiver gets all the signals. But the people who are sitting near to the receiver drowns the signal of the people sitting far apart.

Multiple Access with Collision Avoidance: A Solution to Hidden and exposed terminal problem

MACA is a scheme proposed by Karn in 1990 which solves the problem of hidden and exposed terminal problem. In this scheme instead of sensing the medium, consent of receiver is taken before transmitting. The receiver if free, signals transmission following which the sender transmit. This is accomplished by the use of two fixed length (32 bytes) additional signaling packets called request to send **(RTS)** and clear to send **(CTS).** They **are also called control packets.**

RTS: A control packet used by the sender to seek permission from the receiver to transmit. It contains name of sender, receiver of user data and duration of transmission.

CTS: A control packet used by the receiver to grant permission to the sender to transmit. It contains name of sender, receiver of user data and duration of transmission.

Whenever any station wants to transmit, it sends an RTS to the receiver. If receiver is free, it signals the transmission by sending CTS. Sender sends the packet and receiver on receiving the packet, sends the acknowledgement.

How MACA solves Hidden terminal problem

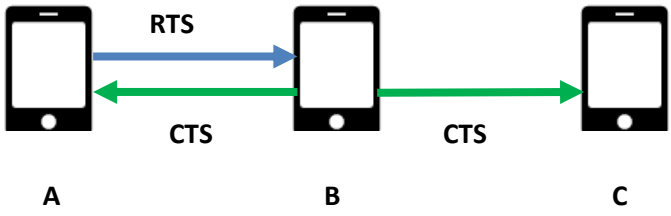


Figure 6: A and C are hidden from each other

A, B, C are 3 terminals where A and C are hidden from each other.
A wants to transmit to B. It broadcasts RTS to B (Figure 4). When broadcasted, the RTS will be heard by all the stations in its range so the RTS is heard by B but not by C (A&C are hidden) B sends CTS. C hears CTS (B&C are in transmission range).C is not allowed to transmit anything for the duration mentioned in RTS. **Hidden terminal problem is solved.**

How MACA solves exposed terminal problem

B wants to transmit to A. B sends RTS to A. (RTS heard by C)
A sends CTS, CTS not heard by C. C understands it is out of range with A.
C now starts transmission with D.

Exposed terminal problem is solved.

Limitations of MACA

MACA offered a three way handshake only.
MACA did not provide specifications about parameters
What are RTS, CTS packet sizes ?
Collisions of RTS may occur when more than one station send RTS at same time. In that case none of the stations gets CTS.

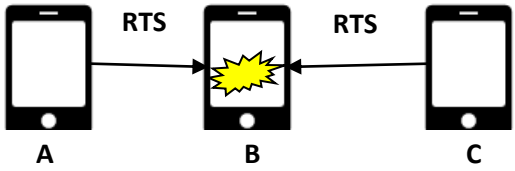


Figure 7: Collision of RTS from A and C at B

The overhead is affordable when data packets are large but in case of short and time-critical data packets this overhead can be quite expensive.

MACAW

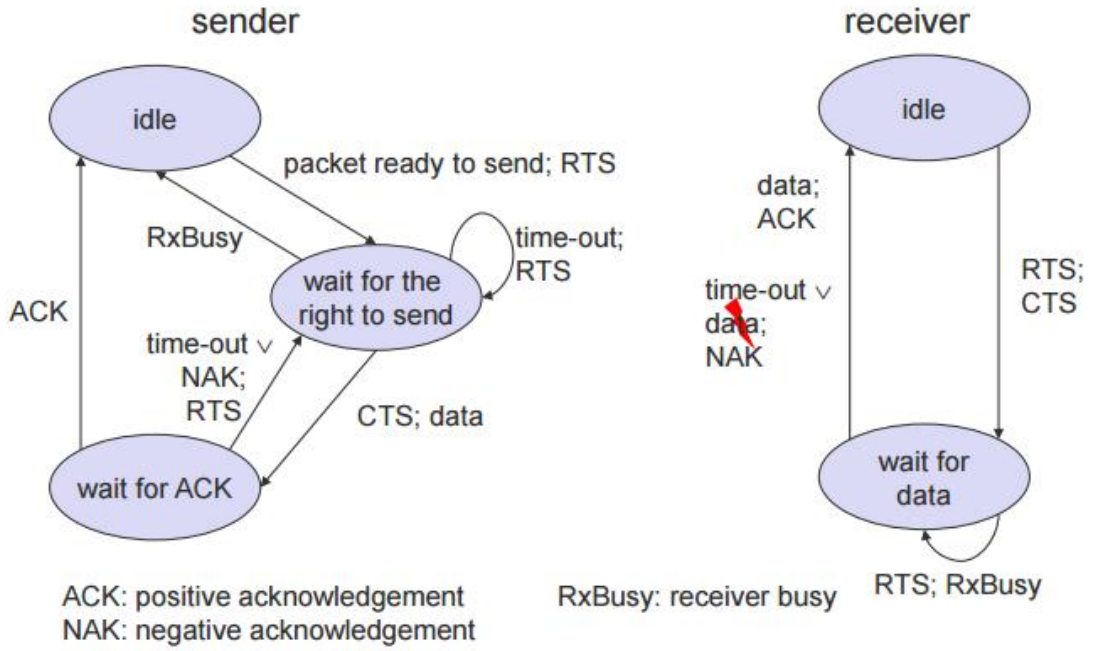
It is refined and extended MACA. Used Information sharing to achieve fairness. It supports

- Four-way handshake (reliable, recover at MAC layer)
- Five-way handshake (relieve exposed terminal problem)
- RRTS (unfairness)

It works as follows

- Sender sends Ready-to-Send (RTS)
- Receiver responds with Clear-to-Send (CTS)
- Sender sends DATA PACKET
- Receiver acknowledge with ACK
- RTS and CTS announce the duration of the transfer
- Nodes overhearing RTS/CTS keep quiet for that duration
- Sender will retransmit RTS if no ACK is received
- If ACK is sent out, but not received by sender, after receiving new RTS, receiver returns ACK instead of CTS for new RTS

Time State diagram of MACA algorithm



.

Figure 8: State diagram of MACA Algorithm: **Picture courtesy: Mobile communications by Joschen Schiller**

Figure 5 shows state diagram for sender in the MACA. The sender can be either in ***idle*** state, waiting for CTS state or ***waiting for acknowledgement*** state. When sender wishes to transmit, it sends RTS and moves in to ***wait for CTS*** state. If the receiver is idle, it will send CTS. Sender will transmit and move to **wait for ACK state** and receiver will go to **wait for data state**. If the receiver is busy or time-out for CTS has occurred, sender again goes to idle state. On receiving the data, receiver gives ACK, sender goes back to idle. In case of NACK, sender again sends initiates transmission and waits for CTS.

MACAW with five-way handshake

- Sender sends Ready-to-Send (RTS)
- Receiver responds with Clear-to-Send (CTS)
- Sender sends DATA SENDING (DS)
- Sender sends DATA PACKET
- Receiver acknowledge with ACK
- RTS and CTS announce the duration of the transfer
- Nodes overhearing RTS/CTS keep quiet for that duration