

# VE489 Homework 4

Wei, Yinuo, 520370910103

July 2023

1. (a) Denote the transmission time for one frame  $A$  is  $X$  and it is sent at  $t_0$ . Then, the vulnerable period for ALOHA is  $[t_0 - X, t_0 + X]$  because another frame that begins to be sent by another station at this period will collide with this frame  $A$ .  
For slotted ALOHA, the vulnerable period is  $[t_0 - X, t_0]$ . Because for slotted ALOHA, new frames can only be sent at edges of slots. Thus, for other frames ready at  $[t_0 - X, t_0]$ , they will be sent at  $t_0$ , thus colliding with this frame  $A$ . However, frames ready at  $[t_0, t_0 + X]$  won't affect the transmission of this frame  $A$ , because they will be sent at  $t_0 + X$ , at which time this frame  $A$  would have finished transmission.
  - (b) The vulnerable period for CSMA is twice the propagation time. To make sure CSMA works better than ALOHA, we should ensure that the transmission time is longer than the propagation time.
  - (c) If detection of collision is enabled, the transmission can be aborted at the moment the collision is detected. However, without collision detection, transmission still goes on even if collision happens. This early abortion saves time.
2. (a) Virtual carrier sensing does not implement real carrier sensing in the physical layer. Instead, it is carried out in the following way. If a station  $A$  knows that other stations will occupy the channel for a fixed duration time to send data, station  $A$  will defer transmission for this duration. The value of the duration time is carried in the Duration field of RTS&CTS headers. Upon receiving frames, each station adjusts its Network Allocation Vector to indicate when the channel will idle again.  
Virtual Carrier Sensing is helpful for IEEE 802.11 MAC because of the following benefits.
    - In wireless network, detecting physical collision is hard because the energy level of collided signals and normal signals are not significantly differed. So, applying virtual carrier sensing enhance the carrier sensing and avoid collision.
    - Each station does not need to constantly sense the channel when the NAV value is not exhausted. So, it is power-saving.
    - It can keep listening to RTS&CTS control frames, so that even if there's hidden node which cannot be directly sensed, it can still determine if the medium is currently being used or reserved by other stations. So, it efficiently avoiding hidden node collision.
    - It can avoid collision due to mobility. If a station  $A$  is moving, and carrying NAV from station  $B$ , even if it cannot hear from station  $B$ , it will know that station  $B$  is still occupying the channel. So, it can still keep silent to avoid collision in the channel.
  - (b) If one node  $A$  cannot be sensed by another node  $B$  within the same access point service range, then node  $A$  is a hidden node for  $B$ . AP range is considered since different APs are designed to operate on different channels so that collision are mainly due to occupying the same channel within an AP. If node  $A$  is out of the sensing range of  $B$ , or there's physical obstacles in between,  $A$  cannot be sensed by  $B$ .  
If the sensing range is much bigger than the communication range, if  $A$  senses that  $B$  is

transmitting, *A* will stop transmission. However, *A* won't be interfered by *B* because they are too far and do not occupy the same medium. In this scenario, *B* is an exposed node to *A*. The network capacity will be low.

- (c) SIFS and DIFS reserve a time interval for frames with higher priority to transmit. They also decrease collision rate because frames with different priority cannot be transmitted simultaneously. Besides, these spaces allow the channel to stabilize and provide regular timing reference so that the transmission and reception can be more stable. Specifically, the space of SIFS is smaller than DIFS. Thus, important frames that wait for SIFS such as ACK, RTS and CTS can be transmitted efficiently. And these important frames are protected from being collided with lower priority frames.
- (d) Collision avoidance in IEEE 802.11 corresponds to the avoidance of simultaneous access to the same medium. Ready stations wait for completion of transmission and all stations must wait IFS. If channel is still idle after IFS period, ready station can transmit data. If channel becomes busy before DIFS, then station must schedule backoff time for reattempt. A station that completes a frame transmission is not allowed to transmit immediately. When station senses channel busy, it waits until channel becomes idle for DIFS period and then begins random backoff time. Station transmits frame when backoff timer expires. If collision occurs, recompute backoff over interval that is twice as long. ACK and timeout are used to find out collision.

Key mechanisms involve:

- Virtual carrier sense
- RTS/CTS
- Interframe Space
- Backoff and deferral: The contention window should dynamically change, so as to fit into the current situation. Besides, backoff count-down cnt will be frozen whenever the channel is busy.

Reference: Lecture Slides Chapter 4.

3. Stations in BSS can communicate with each other with an Access Point. Each access point is attached to ESS, and the distributed system provides services to transfer MAC SDUs between APs in ESS. Besides, it can also transfer MSDUs between portals and BSSs in ESS and transfer MSDUs between stations in the same BSS. Thus, a station in one BSS can transfer data to another BSS via the distributed system. Further, bridging and switching can transfer frames in layer 2. They can use table lookup and forward frames if source and destination are in different LAN. They can be used to connect different LANs and make them appear as a single logical LAN, via bridging, which allows devices in separate LAN segments to communicate as if they were part of the same LAN. Flooding is applied when the destination is unknown. Backward learning, adaptive learning and spanning tree algorithms can help to build the table.
4. PCF relies on DCF to some extent. PCF will first do polling. The NAV value is reserved for this polling period for every end users, just as how they use NAV in DCF. After polling, a contention period is reserved and end users can attempt to transmit just as how they do in DCF. Based on their traffic requirement and QoS needs, DCF and PCF can be applied together. PCF provides connection-oriented, contention-free service through polling. For high QoS needs, PCF can be used so as to be more predictable. For other services, DCF can be used.