CS 425: Computer Networks **Jan-Apr 2020**

Lecture 11: Computer Networks – February 7, 2020

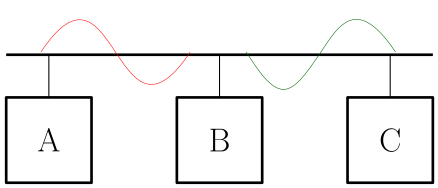
Lecturer: Swaprava Nath *Scribe(s): Akshay Bhola, Harsh Narang, Naman Jain, Shashwat Chaurasia*

Disclaimer: *These notes aggregate content from several texts and have not been subjected to the usual scrutiny deserved by formal publications. If you find errors, please bring to the notice of the Instructor.*

In the last lecture, we saw one of the randomized media access protocol ALOHA. Now, we will discuss another such protocol CSMA. CSMA protocol avoids clashes before they happen while Aloha protocol detects that a channel is busy only after a clash happens.

11.1 Carrier Sensing Multiple Access (CSMA)

In Aloha, we had senders transmitting the data whenever they want and expect an acknowledgement from the receiver if data is received correctly. Here, in CSMA, sender senses the channel before transmitting and does not use acknowledgement. If the channel is idle, the sender sends the data; otherwise, it waits till the channel becomes idle.



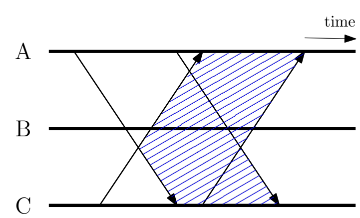


Figure 11.1: Mulitple Access of link

However, there is still a chance of collision. Consider the case in which station A sends the data after sensing channel to be idle. However, by the time the first bit of data reaches station C, C also sends the data finding the channel idle. This will result in a collision of data of A and C. When the collision occurs, a collision signal is generated and sent to all the stations on the link. Hence, the delay in A's signal reaching C is responsible for the collision.

11.1.1 CSMA with Collision Detection (CSMA/CD)

An improvement over CSMA is to stations quickly detecting the collision and abruptly stopping transmission (rather than finishing them) since it will anyways be garbled away. This strategy saves time and bandwidth. This protocol, known as CSMA/CD, is the basis for classic Ethernet LAN.

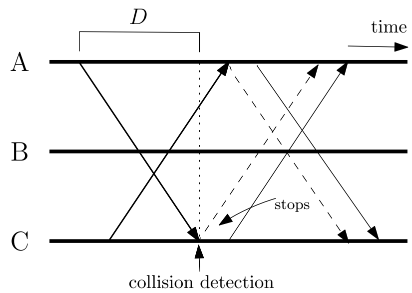


Figure 11.2: CSMA with Collison Detection

Principle: The transmission is said to be successful when the whole frame is transmitted with no collision being detected.

Ques: How long should the frame be transmitted to detect a collision?

Ans: Consider the worst case in which C starts transmitting just before the signal from A reaches it. Hence, the collision signal is generated at time D. This collision signal requires another D time to reach the sender A. Hence, the minimum time a frame should be transmitted is *2D*.

Ques: Suppose the maximum distance of a LAN is d meters, and velocity of the signal is v m/s. If the data rate is R bits/sec, at least how large the frame size has to be?

Ans: For collision to be detected, $T_f \geq 2D$ where D is the propagation delay. Hence,

$$\frac{L}{R} \geq 2\frac{d}{v}$$
$$L \geq 2\frac{d}{v}R$$

11.1.2 Access Modes

CSMA uses various algorithms to determine when to transmit to the channel. The distinguishing feature of these algorithms is how aggressively they are initiating transmission.

1. **1-persistent** This is an aggressive transmission algorithm. If the transmission medium is idle, then the sender sends immediately. If it is busy, then it continuously senses the channel until it becomes idle, then transmits the frame with certainty *(probability 1)*.

2. **non-persistent** This is a non-aggressive transmission algorithm. If the transmission medium is idle, then the sender sends immediately. If it is busy, then it waits for a random period and attempts transmission (sensing and transmission) again.

3. **p-persistent** This approach is between 1-persistent and non-persistent CSMA access mode algorithms. If the transmission medium is idle, then the sender sends immediately. If it is busy, then it continuously senses the channel until it becomes idle, then transmits the frame with probability p. In case it does not transmits (probability *1-p*), it waits for the next timeslot and transmits again with probability **p**. This back-off cycle continues until the channel is busy or the frame is transmitted successfully.

Ethernet, IEEE 802.3 LAN, IEEE 802.11 wireless LAN protocols are 1-persistent.

11.1.3 Throughput analysis

Renewal Reward Theorem

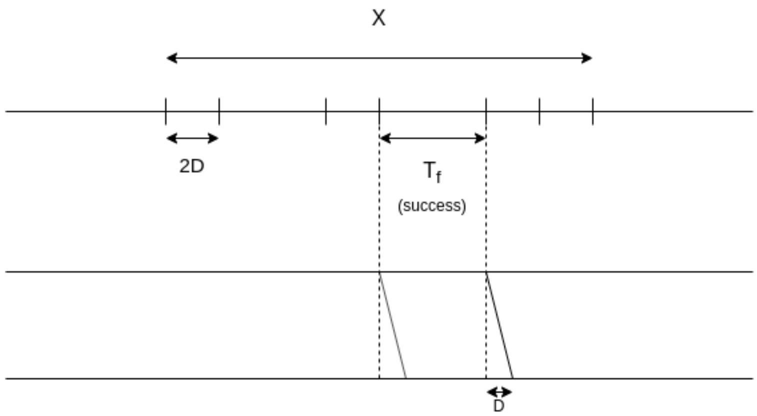


Figure 11.3: Depiction of general scenario of frame transmission over the time axis

The above figure represents the general scenario of frame transmission over the network. It constitutes collision with $2D$ interval in between. The successful frame transmission takes T_f time period.

$$\lim_{t\to\infty} \frac{R(t)}{t} = \frac{\mathbb{E}[R]}{\mathbb{E}[X]} = \frac{T_f}{\mathbb{E}[Y] \times 2D + T_f + D}$$

$R(t)$: Reward function
$\mathbb{E}[R]$: Expected reward
X : sequence of inter-arrival times (an independent, identically distributed sequence of random variables)
Y : number of collisions in the interval
$2D$: bad time (delay time)
T_f : time required to transmit a frame

Now analysing it in **Slot Level**.

Consider n nodes are attempting to access the channel with probability p.

E_i : Event that i^{th} packet was successfully transmitted in that $2D$ slot .

$$\begin{aligned} \text{P(atleast one packet is successfully transmitted)} &= P(\bigcup_{i=1}^{n} E_i) \\ &= \sum_{i=1}^{n} P(E_i) \\ &= np(1-p)^{n-1} \end{aligned}$$

Now, we want to maximise the above probability. Thus,

$$p_{succ} = max_p \; np(1-p)^{n-1}$$

Differentiating the equation wrt p and setting to zero.

$$
\begin{aligned}
&\Rightarrow p^* = \frac{1}{n} \\
&p_{succ} = n.\frac{1}{n}.\left(1 - \frac{1}{n}\right)^{n-1} \xrightarrow{n\to\infty} \frac{1}{e}
\end{aligned}
$$

In between the transmission, there are variable number of collision possible. Extending the above formulation, the expected number of collisions is given as:

$$
\begin{aligned}
\mathbb{E}[y] &= \sum_{i=1}^{\infty}(i-1)(1-p_{succ})^{i-1}p_{succ} \\
&= \frac{1}{p_{succ}} = e
\end{aligned}
$$

$$
\begin{aligned}
\text{Further, the efficiency of CSMA/CD (Ethernet)} &= \frac{T_f}{(1+2e)D + T_f} \\
&= \frac{1}{1 + (1+2e)(\frac{d}{v})(\frac{R}{L})} \\
&\approx \frac{1}{1 + 6.44(\frac{d}{v})(\frac{R}{L})}
\end{aligned}
$$

d : maximum distance between two nodes over the network
v : speed of the signal in the medium
R : rate of bit transmission over the network
L : size of the frame

Observations

Now, looking at the above expression carefully, there are some key observations mentioned below:

1. Efficiency decrease with increasing d
   - CSMA/CD is good for LANs, not for WANs
2. Efficiency increases with increasing L
   - not immune to malicious transmitters
   - Ethernet specifies max frame size of 1500 bytes

Ethernet Frame

- Ethernet uses 1-persistent CSMA/CD
- No Acknowledgements - media access is reliable
- Modern Ethernet is switched Ethernet

Preamble 8 Bytes	Destination Address 2/6 Bytes	Source Address 2/6 Bytes	Type 2 Bytes	Data 46-1500 Bytes	Frame Checksum 4 Bytes

Figure 11.4: Ethernet Frame

11.2 Wireless Multiple Access

CSMA/CD can not be used for wireless. Below we describe the issues that arise if CSMA/CD is used in wireless.

1. **Hidden Node Problem**

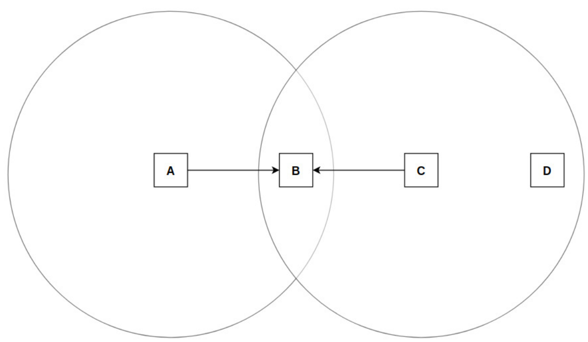


Figure 11.5: Hidden Node Problem

Consider a scenario where there are 3 nodes- A, B and C. B is in the middle of A and C and can communicate with both of them. A and C can not communicate with each other. Now, let us say both A and C want to send data to B at the same time, they both will start the transmission as they both will see the carrier to be idle. This is because when C is listening to the network, it will find it to be free as A's range is not enough to reach C. This may lead to a collision and still neither A nor C will be able to detect it. At the same time, B will receive 2 packets and may not be able to understand any of them. This is called "Hidden Node Problem" as A and C can be seen as hidden from one other.

2. **Exposed Node Problem**

Consider a scenario where there are 4 nodes- A, B, C and D. Let us say B is communicating with A and C wants to communicate with D. However, this transaction can take place in parallel, CSMA/CD will not allow it as C will hear B transmitting. This actually would not have created an issue for this transaction at A and D even if C had transmitted. Hence some nodes are silent even though that transaction was possible.

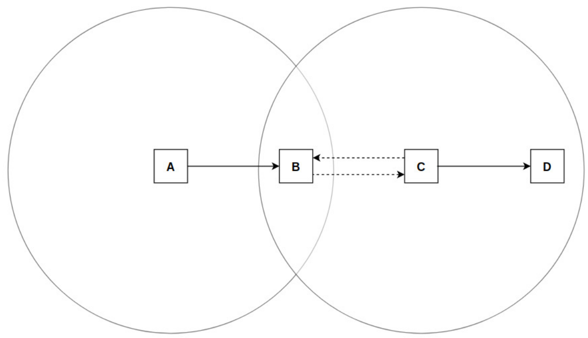


Figure 11.6: Exposed Node Problem

MACA

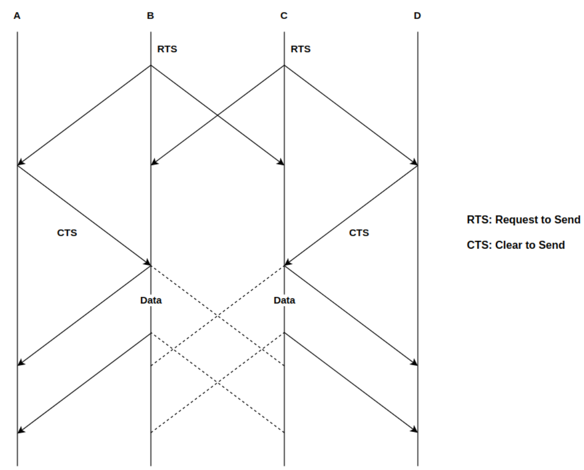


Figure 11.7: MACA

To tackle these two issues, we use an algorithm known as MACA(Multiple Access with Channel Acquisition). In this protocol, RTS(Request To Send) and CTS(Clear To Send) frames are used. The sender sends an RTS frame. The receiver responds with a CTS frame to the received RTS message. Any node that receives the RTS frame but not the CTS frame knows that it is not close to the receiver to interfere with it; hence it can transmit data. On the other hand, if a node receives a CTS message, then it must be close to the receiver; hence it cannot transmit data.

In the above diagram B and C send an RTS message. A response with a CTS to B's RTS and D responds to C's RTS. As A's CTS is not reaching C and D's CTS is not reaching B, both B and C are free to transmit data to their corresponding receivers A and D respectively.

References

[1] Tannenbaum, A. S., and D. J. Wetherall. "Computer Networks,(5-th edition)." (2010).

[2] https://www.geeksforgeeks.org/

[3] https://www.cse.iitk.ac.in/users/dheeraj/cs425/index.html