

COMP28411 Computer Networks

Lecture 15

Nick Filer

Link Layer - 2

Some material from:

Kurose & Rose – Chapter 5 + Slides

Overview

- More about Switches, Routing and Local Area Network (LAN) addresses.
- Multiple access – sharing a network.
- Collisions and channel partitioning.
- Random Access protocols:
 - Aloha
 - Slotted Aloha
 - Carrier Sense Multiple Access (CSMA) with Collision Detection (CD) – hence CSMA/CD
 - CSMA with Collision Avoidance (CA) – hence CSMA/CA
 - Used in wireless IEEE 802.11 (WiFi).

Multiple Access

Two main types:

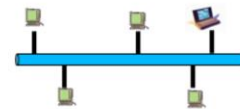
- **Point-to-Point (P2P)**

- Single sender + single receiver direct.
- Point to Point (PPP) and High Level Data Link Control (HDLC) protocols over ADSL (PPPoA) or VDSL (PPPoE)

- **Broadcast**

- Single shared broadcast channel.
- Ethernet (up to 100Mbps) and Wireless
- Everybody could speak or transmit at the same time – interference.
- Analogies:
 - **Party:** Lots of people talk at the same time.
 - Rely on Signal to Noise and Interference ratio (SNIR) to listen and understand.
 - **Classroom:** Teacher and students (mostly) take it in turns to talk.
 - Mainly – Half Duplex.

PPP extends the older HDLC. More later



24/11/2016

COMP28411 Link Layer

37

The switches we talked about last time we used to interconnect multiple devices to form a network. We also briefly mentioned half-duplex and full-duplex.

Our networks are mainly made from either point 2 point (P2P) links or from broadcast links. The medium for P2P was almost always an isolated via insulation of some form wire which we only allow to have connections at each end. Most mediums are in fact broadcast in nature. It is by constraining the use of the broadcast medium that we build unicast or P2P links. Some mediums are easier to constrain than others. For wireless, the medium is usually the air, water and other objects around us but it can be vacuum such as space.

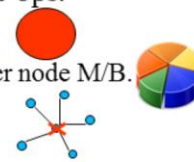
In any medium we need some rules to decide who can transmit when. These can be very simple such as whenever you have data, transmit it straight away. Or the rules can be more complex requiring a node to wait until the medium is unused before sending. Shared mediums lead to collisions when several users send at the same time. When this happens inevitably some data is lost. Where we can schedule transmission to avoid collisions we do this as it is both efficient and sensible. However, scheduling requires warning that data will be available or waiting with data to tell a controller to allocate a transmission opportunity and then when told by the controller, to actually transmit the data.. In a seldom used medium, scheduling may be more trouble than it is worth as collisions will almost never happen. Different environments and applications will have different needs. To meet these needs many solutions are generic and work well in many scenarios. Other solutions are bespoke designed to work with particular applications in pre-specified environments.



Collision



- **On a broadcast channel:** whenever more than 2 nodes transmit at the same time.
 - This is wasted resource. Will have to throw away or re-transmit.
 - More nodes + more traffic = more collisions = wasted bandwidth!
 - Therefore need coordination – Medium Access Control (MAC) protocol.
 - Three main categories of MAC:
 1. **Channel partitioning**
 2. **Random access**
 3. **Turn taking**
- Ideal Characteristics for channel with bandwidth B bps:
 - Only one node with data – uses total bandwidth B .
 - M nodes with data sharing – average throughput per node M/B .
 - Decentralized – no single point of failure.
 - Simple – inexpensive.



24/11/2016

COMP28411 Link Layer

38

When someone transmits (anything) they create some noise that receivers will try to listen to. At the receiver there is after attenuation (losses) there is an amount of power which the receiver hears. However, the receiver actually hears the sum or all the power (in Watts) from all transmitters currently transmitting in the medium. In most current computer networks transmissions use the electromagnetic spectrum. Losses due to attenuation are relatively small in wired/fiber media but will be much larger if the medium is air or a vacuum. In air or a vacuum losses are proportional roughly to the inverse square of the distance between a transmitter and receiver – Inverse square law $1/d^2$.

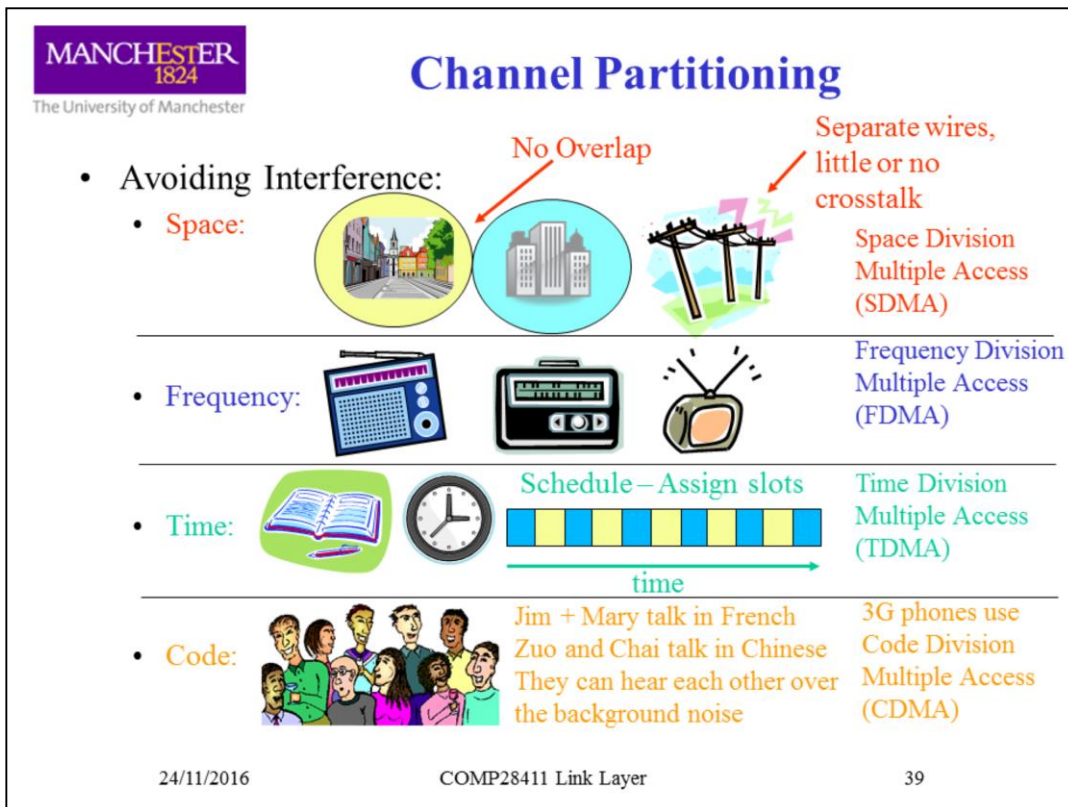
When an electromagnetic radiation travels through any medium it travels at the speed of light (SoL) for that medium. For air or a vacuum this is approximately $3 \times 10^8 \text{ms}^{-1}$. The SoL is fast but it still introduces delay. These delays mean that often, even if a transmitter listens to the medium before transmitting and hears nobody, when it decides to transmit someone else made the same decision at the same or almost the same time. This means that in a distributed or uncontrolled environment collisions are inevitable. To try and avoid collisions we try to control when and how nodes access the medium.

When there is plenty of space the channel can be partitioned to avoid all collisions sometimes with no extra delay e.g. by partitioning into different frequency channels.

Where no central control system can decide who can use the medium when (distributed and unlicensed) then, to try and minimize the probability of collisions we can use random numbers in various ways to distribute traffic but almost always with an extra delay cost if we assume the frequency and geographic location are already decided.

When nodes can be either forced (e.g. mobile phones) or decide it is a good idea to collaborate then turn taking systems can vastly reduce the number of collisions but again at the cost of extra delay.

It is very rare to get anywhere near the idealized channel discussed in the slide!



In our lives we experience many different channel partitioning systems without much thought about them. The International Telecommunications Union, allows most countries to decide how large blocks of the electromagnetic spectrum are allocated or shared. Thus the ITU allows the frequencies between 88 and 108MHz to be used for Frequency Modulated (FM) transmissions in many places. In the UK, because these frequencies do not bend and follow the spherical curvature of the Earth they have a limited distance of reach of around 30 miles (to the horizon). Thus, the same frequency can be re-used at say 70 miles transmitter to transmitter separation with almost zero experienced interference between stations. Putting signals inside wires, limits the space these signals reach. Space partitioning is a very effective way to share !

There are also agreements that particular frequencies can only be used for pre-defined purposes. So, within the 88 to 108MHz FM band, stations are allocated reserved bandwidth allowing many stations to broadcast and reach us with separation between them (The separation was Marconi's big contribution to 20th century telecommunications!).

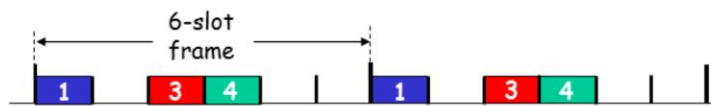
We share, lecture theatres, toilets, railway tracks and wireless spectrum by using timetables with slots in time allocated for use by different users or services. The 2G GSM mobile phone systems works with 8 slots per channel allowing 8 telephone calls to continue side-by-side with no interference on a single wireless channel (actually two channels – one for uplink and one for downlink).

A more complex sharing method relies on non interfering codes or patterns. By only tuning in to a given spoken language at a party and ignoring other languages we tune into a conversation. Luckily for you the mathematics behind its use in networks is not part of this course!

Channel Partitioning MAC protocols: TDMA

TDMA: Time Division Multiple Access

- Access to channel in "rounds".
- Each station gets fixed length slot (length = packet TX time) in each round.
- Unused slots go idle.
- "2G" mobile phones, GSM uses TDMA with 8 slots per channel. But often several channels in a given space = cell.
- Example: 6-station LAN, 1,3,4 have pkt, slots 2,5,6 idle



24/11/2016

COMP28411 Link Layer

40

TDMA is an example of time partitioning. Typically a system will divide a period of time into several equal sized slots which can be allocated to different users based on their needs or value. If there is no user for a slot it may be idle or wasted. If demand is high enough, then there could be auctions for usage of slots or other marketing tools used to maximize profit from this spectrum resource.

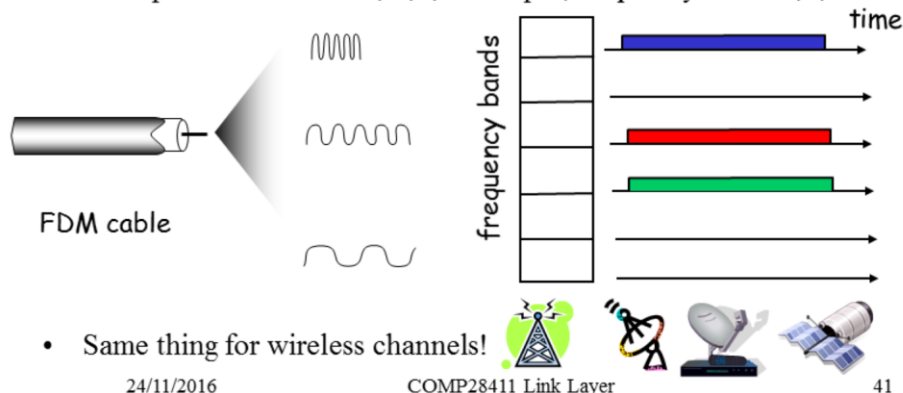
In 2G GSM, the mobile phone operators installed transceivers based on the demand in an area for the service. They sold spectrum access to many people and balanced allocation of resources based on usual usage. When usage was very high for some reason, e.g. match days at Manchester United, they might increase the number of available transceivers temporarily but almost always demand could and often would exceed supply so some users were unable to make calls or had calls dropped as they moved around because no spare resources to handle mobility were available for the short time period of the arrival, match and departure of the fans. Because a variety of techniques could be used to increase the number of users who could share the spectral resource in a small area such as simply using smaller cells it is not really possible to state a maximum number of users per area.

Channel Partitioning MAC protocols: FDMA

FDMA: Frequency Division Multiple Access

- Channel spectrum divided into frequency bands.
- Each station assigned fixed frequency band.
- Unused transmission time in frequency bands go idle.
- Example: 6-station LAN, 1,3,4 have pkt, frequency bands 2,5,6 idle.

Remember: we use frequency in cables as well as for wireless.



24/11/2016

COMP28411 Link Layer

41

The frequency given for most systems is the central frequency. Around this central frequency half the quoted bandwidth is therefore above and the other half below the central frequency. One reason for choosing high frequencies for data networks is to have more bandwidth available. Between 100Hz and 200Hz there is just 100Hz of bandwidth. Between 2 and 3 GHz there is 1GHz of bandwidth. So not surprisingly many data networks use the highest economical frequencies where we have suitable technologies available.

Today that is, for the mass market with wireless systems between around 1GHz and 5GHz and we now allocate e.g. 20MHz for relatively low data rate applications up to say 300Mbps using MIMO (Look it up! You do not need to know this yet!) technology or 54Mbps using SISO technology.

Ethernet Cat-5 cables carrying Ethernet 100BaseT at 100Mbps are actually working at 125Mbps or 125MHz ($10/8 \times 100$) because they use an encoding called 8B/10B where every 8 bits of data are sent as 10 bits on the cable.

Strangely, Gigabit Ethernet runs on the same 125MHz cat-5 cable!

It does this by coding 2 bits into each signal using 4 voltages for 00, 01, 10, 11 instead of 2 voltages for 0 and 1. The result is made from 125Mhz x 2 bits per signal x 4 cable pairs = 1000Mbps. The modulation actually uses 5 voltages not 4 and is called 4D-PAM5. So Gigabit Ethernet runs at 125MHz not 1000MHz/1GHz. Ideally it needs a PCI Express point-to-point bus running at 250MBps to run at maximum rate. On PCI which shares its 133MBps between everything connected it is unlikely to get anywhere near full data rates. But I diverge.

10Gigabit Ethernet runs at 833.3MHz over Cat-6a cables up to 100m(ideally), Cat-6 for just 55m or Cat-5e for very short distances. It uses 3 bits per signal again over 4 cable pairs. So $3 \times 4 \times 833.3 = 10\text{Gbps}$. The coding is called PAM-16 DSQ128 coding – no details needed here!

Random Access Protocols

- **When node has packet to send**
 - **Transmit at full channel data rate R .**
 - **No *a priori* coordination among nodes**
- Two or more transmitting nodes = “collision”
- **Random access MAC protocol** specifies:
 - How to detect collisions
 - How to recover from collisions (e.g., via delayed retransmissions)
- Examples of random access MAC protocols:
 - **ALOHA**
 - Slotted ALOHA
 - CSMA, CSMA/CD (Old Ethernet), CSMA/CA (WiFi)

Useful when:

Must share
Not much traffic.
Collisions not very likely.
Control difficult
Cheap/simple

24/11/2016

COMP28411 Link Layer

42

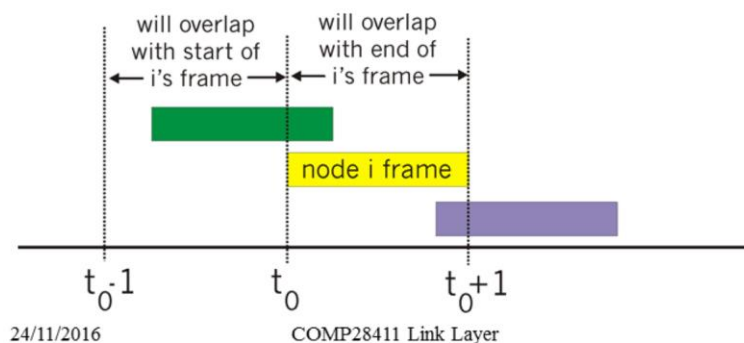
Random access protocols will experience collisions whenever two or more stations have data to send that overlaps. There are many possible ways to respond to collisions. In wired networks because there is very little attenuation of signals the power level of receivers is similar to the power transmitted. Therefore, for example, in shared 10Mbps and lower data rate wired Ethernets nodes that are transmitting can listen to the cable themselves and if they hear only their own transmission right through to its end can assume no collision took place. This is used by CSMA/CD or Carrier Sense Multiple Access with Collision Detection.

In wireless, the attenuation of signals is massive meaning that receivers have to be many times more sensitive than transmitters. This means that a receiver placed adjacent to a transmitter would be destroyed by the very large signal it would be exposed to (you can imagine adapting the hardware for this). In wireless systems the signal expected at the receiver is tiny compared to the power of the transmitted signal. A fairly small signal but large enough to cause errors at the receiver may be totally unheard at the transmitter even if it was able to listen whilst transmitting. Wireless senders only know about collisions if somebody tells them! In WiFi using CSMA/CA or Carrier Sense Multiple Access with Collision Avoidance, transmitters only know their signal was heard correctly if an acknowledgement is sent and received. The acknowledgement may be immediate or sometime later. It might acknowledge one or more received messages. It is often sent over the same wireless channel as the message itself but it could be sent by some other means.

The simplest random MAC protocol is called ALOHA. The very slightly more complex but still random MAC protocol Slotted ALOHA is still used by mobile phones!

Pure (unslotted) ALOHA


- Pure Aloha: no synchronization!
- When frame first arrives
 - Transmit immediately
- Collision probability:
 - Assuming fixed sized frames.
 - Frame sent at t_0 collides with other frames sent in $[t_0-1, t_0+1]$
 - Each frame is vulnerable to collision for twice its length!



This is called ALOHA after the “Hello” greeting used on the Hawaiian islands . It was first implemented to provide wireless data networking between islands. It is very simple. Using a shared channel, a node with data to send simply sends the data as soon as it arrives. Other nodes are assumed to be listening whenever they themselves are not sending data. Pure ALOHA does not make any assumptions about e.g. having the same size packets but this assumption makes illustrating what happens much simpler.

A fixed size frame received at time t_0 will collide with any other frame received less than one frame size earlier. Similarly, the frame received at time t_0 will collide with any other frame received less than one frame size later. For these fixed size frames, the receiver is vulnerable to a collision for just (infinitesimally) less than $2t$ representing frames from before and after.

Why did I talk about receivers and not transmitters? Almost always, ALOHA and slotted ALOHA are described talking about transmitters and in the wired connection theoretical world where receivers start and finish hearing transmission at exactly the same time it makes no difference. But in the real world or with wireless



MANCHESTER
1824
The University of Manchester

Pure Aloha Efficiency

Few users or little traffic:

Very successful as few collisions. With more users and traffic.....

$P(\text{success by given node}) = P(\text{node transmits}) \times \text{times}$

Probability series independent events is $p(1) \times p(2) \times \dots \times p(n)$ which is p^n .

$P(\text{no other node transmits it's in } [t_0-1, t_0] \text{ times})$
 $P(\text{no other node transmits it's in } [t_0, t_0+1])$
 $= p * (1-p)^{N-1} * (1-p)^{N-1}$
 $= p * (1-p)^{2(N-1)}$

... choosing optimum p and then letting $N \rightarrow \text{infinity}$...

$= 1/(2e) = .18$ or roughly 18% efficiency (= success rate!).

$e \approx 2.71828 \approx \sum 1/n!$
Is Euler's number.

Lots of nodes.

1/e is the answer to the secretary problem. See: http://en.wikipedia.org/wiki/Secretary_problem. Here we select 2 secretaries. For slotted Aloha only 1 secretary so the analogy is much easier to see.

At best: channel used for useful transmissions 18% of time!

!

24/11/2016
COMP28411 Link Layer
44

We have N nodes. We want to calculate the probability of successful transmission of a packet by a node. Clearly the probability of a node transmitting is for ALOHA the probability of a packet's worth of data arriving to be sent. This has to be combined with the probability that within 1 packet length before our node's transmission no other nodes had enough data to form a packet arrive; this is because if enough data did arrive it would be transmitted and cause a collision. The same applies to the time just after the packet is sent. We can write this equation quite easily. Then we have to allow for N varying right up to infinity with an optimum data arrival rate setting the probability that a node sends a packet.

This simplifies to $1/2e$.

You do not need to know this but it is a useful relationship for the more mathematically minded amongst you: The secretary problem has been studied extensively in the fields of applied probability, statistics, and decision theory. It is also known as the marriage problem, the sultan's dowry problem, the fussy suitor problem, the googol game, and the best choice problem. Always reject the first n/e people then accept the 1st person who is better than everybody seen so far. This will be the best candidate $1/e = 37\%$ of the time! If you need two secretaries then it will be the best candidate $1/2e = 18\%$ of the time. See <http://tinyurl.com/q82udoz> or <http://tinyurl.com/nbkhhkm>.

Slotted ALOHA

Assumptions:

- All frames same size
- Time divided into equal size slots (time to transmit 1 frame)
- Nodes start to transmit only at slot beginning
- Nodes are synchronized
- If 2 or more nodes transmit in the same slot, all nodes detect a collision.

Operation:

- When node obtains fresh frame, transmits in next slot
 - *If no collision:* node can send new frame in next slot
 - *If collision:* node retransmits frame in each subsequent slot with probability P until success

Implies shared or central clock to ensure synchronization.

24/11/2016

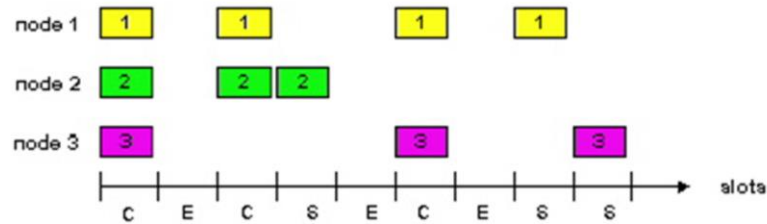
COMP28411 Link Layer

45

This is a slightly more complex variation of ALOHA. Now all transmissions start in synchronized slots. Nodes can only start to transmit at the start of a slot. Therefore, data may have to wait for up to 1 slot length of delay before being transmitted.

Complete synchronization is required so that for a slot at time t , everybody with data to transmit would start to transmit at exactly the same time and/or be heard by the receivers at exactly the same time.

Slotted ALOHA



Pros

- Single active node can continuously transmit at full rate of channel.
- Highly decentralized: only slots in nodes need to be in sync.
- Simple.

Cons

- Collisions, wasting slots
- Idle slots
- Nodes may be able to detect collision in less than time to transmit a packet.
- Clock synchronization

24/11/2016

COMP28411 Link Layer

46

It is clear in this illustration that the rules for slotted ALOHA for fixed size packets or slots cause each slot to have either 0 = idle time, 1 = transmit OK time or 2+ transmission sat the same time. With 2+ simultaneous transmissions these are assumed to collide and cause complete data lose.

So, now each packet is vulnerable to collision for exactly 1 slot time rather than the 2 slot times are pure ALOHA.

Slotted Aloha efficiency

Efficiency : Long-run fraction of successful slots (many nodes, all with many frames to send)

- Suppose: N nodes with many frames to send, each transmits in slot with probability p
- Probability that given node has success in a slot = $p(1-p)^{N-1}$
- Probability that *any* node has a success = $Np(1-p)^{N-1}$

- Max efficiency: find p that maximizes the value of $Np(1-p)^{N-1}$
- For many nodes, take limit of $Np(1-p)^{N-1}$ as N goes to infinity (∞), gives:
Max efficiency = $1/e = .37$

At best: channel used for useful transmissions 37% of time!



24/11/2016

COMP28411 Link Layer

47

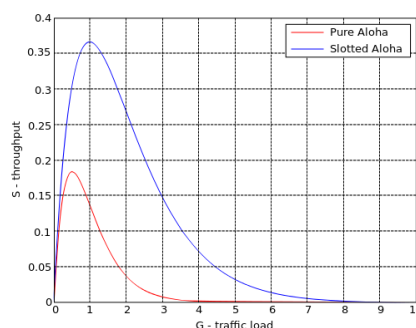
Doing the same sums to those used to analyze pure ALOHA we now find the channel can successfully transmit twice as much data. This is a very useful gain. For distributed random arriving data it is very hard to reach this maximum performance of up to 37% successful transmission.

With both ALOHA and slotted ALOHA if there is little traffic and the traffic is not clustered then the success rate will be close to 100%. As the amount of traffic increases ALOHA very quickly approaches its maximum. However, the traffic arrival rate can continue to increase twice as far before slotted ALOHA also approaches its maximum.

If no traffic is ever thrown away then if the arrival rate exceeds the maximum possible efficiency then nothing gets through. i.e. the network saturates and until the traffic load drops no traffic is delivered!

In practice, we do allow data to be thrown away. By throwing away old data or data we have nowhere to store networks can still not exceed their maximum possible performance. But if the arrival rate exceeds the maximum then some packets get through though the number that succeed drops.

We can show this by plotting generated (arriving) traffic against successfully sent/received traffic. Image from: http://commons.wikimedia.org/wiki/File:Aloha_SvG.PNG



CSMA (Carrier Sense Multiple Access)

Instead of central control and synchronization.

CSMA: Listen before transmit:

If channel sensed idle: Transmit entire frame

- If channel sensed busy, defer transmission – queue.

- Human analogy: don't interrupt others!



24/11/2016

COMP28411 Link Layer

48

ALOHA is not a polite protocol. Others can be talking successfully and an ALOHA node will but in rudely just because it has data to send. In the real world, you and I listen to conversations between others and we normally only talk when the other parties to our conversation stop talking. The 300ms figure for the maximum round trip for VoIP traffic is based on this . We seem to need a gap of around 150-200ms in speech before we will interrupt and start speaking.

For data networks, a similar idea is often used where nodes listen for an idle medium before sending their data. While waiting to send data because others are sending theirs the nodes might build up quite a queue of data which has to be stored.

When whosoever is currently using the medium stops. All the nodes with queued data want to send their data. If they all send at the same time there is a much higher likelihood of collisions. Therefore, there are various schemes whereby those with data to send when a medium becomes free compete to be the one who sends data first.

The most common mechanism is one whereby each node generates a random number with a fixed range. The nodes then each count down to zero , stopping if they hear anybody using the medium and restarting when the medium becomes idle again until they reach zero. Then they can send their data. By generating mainly different random numbers for back-off the competing nodes are spread out to void collisions. Of course, we can come up with fair back-off schemes and unfair schemes. Nodes can cheat.

Whilst the probability of collision is reduced, collisions will still happen. After a collision, nodes can of course try again or give up on the data they were trying to send.

CSMA collisions - 1

Collisions *can* still occur:

Propagation delay means two nodes may not hear each other's transmission.

Collision:

Entire packet transmission time is wasted. *Always?*

Note:

Role of distance & propagation delay in determining collision probability.

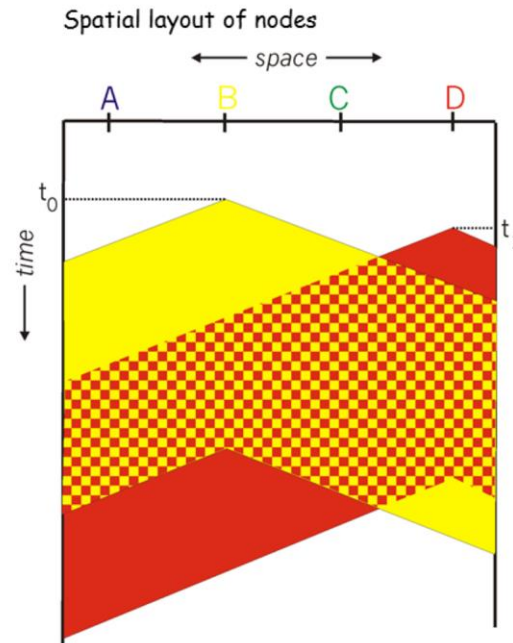
Scenario:

B starts at t_0 . D starts at t_1 before hearing B.....

24/11/2016

COMP28411 Link Layer

49



At time t_0 node B has a packet to send. It hears nothing on the medium so decides to send its data. Node D has data ready to send a little later than B. Being polite, D also listens to the medium and hearing nothing it starts to transmit its packet of data at time t_1 .

Meanwhile, the data from B has been propagating through the medium and has reached A and C what looks to be a little after time t_1 . A and C start to receive the nice clean data from B. If they are using CSMA/CD introduced just before and repeated in a moment, B is hearing B's own data being sent and D is hearing D's own data being sent. So for a short time everybody is happy!

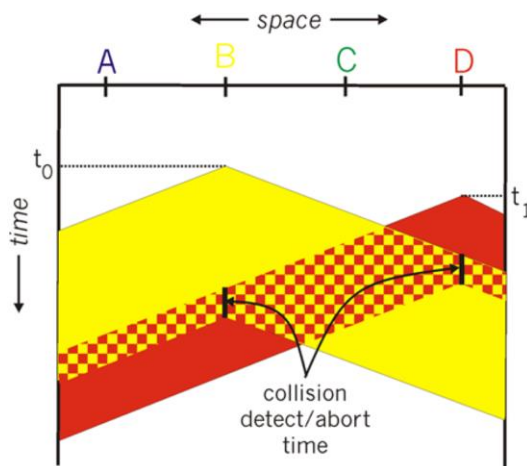
The first node to detect a problem is C but having heard the headers clearly, it will do nothing about it until either it hears what it thinks is the end of the frame or an idle channel. Ethernet uses a length field in the header so C will be counting bytes using the length of the frame from B, at the end it will find the CRC fails due to lots and lots of errors.

Shortly after C starts to receive rubbish, D will notice that what it is sending no longer matches what it sent. This is because it listens to its output. So D now knows there is a problem. D aborts its send and instead sends a jamming sequence to almost always ensure everybody listening gets errors. After the jamming sequence D stops sending, generates a random wait time and waits for this counter to count down before starting to send again.

A similar process will take place at B when it hears the collision.

Node A will hear a mixture of good signal, collision signal and jamming signals. It will throw any incoming data away because it has heard rubbish and the CRC will fail.


CSMA/CD collision detection - 2

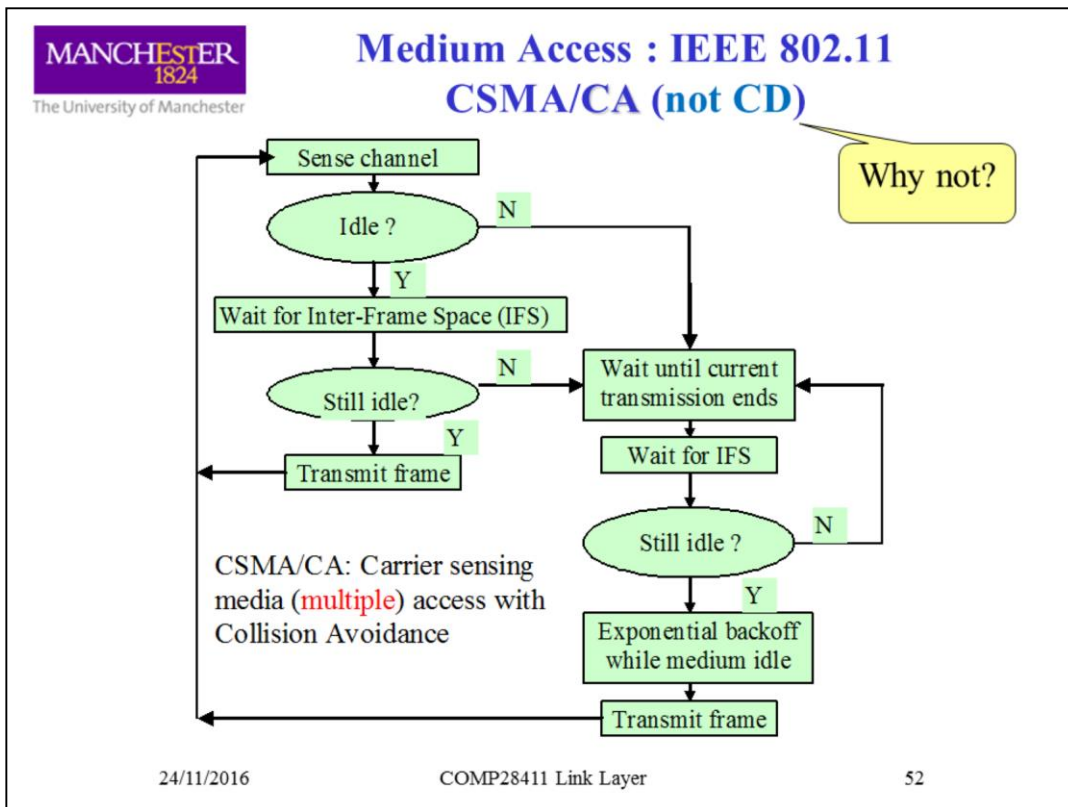


- Both B and D are Idle.
- Both start to send leading to **collision**!
- CD detects overlap – 2 signals at same time – Change in signal strength.
- Can cut short the now useless transmission.
- How ensure others know a collision occurred?

CSMA/CD (Collision Detection)

CSMA/CD: Carrier sensing, deferral as in CSMA.

- Used in Ethernet. Required at start so wire could be shared. 100Mbyte and above speeds do not share anymore!
- Collisions *detected* within short time. By listening 
- Colliding transmissions aborted, reducing channel wastage.
- Collision Detection (CD):
 - Easy in wired LANs: Measure signal strengths, compare transmitted and received signals – Not much difference = OK
 - Difficult in wireless LANs: Received signal strength overwhelmed by local transmission strength – Due to inverse square law!
- On wireless use **CA** (Collision Avoidance)
 - **If listen to own transmission will destroy the transmitter due to too much power.**
 - Listen, random back-off after busy medium BUT **cannot detect collisions at the transmitter** until someone else tells you! e.g. No ACK



This is a simplified flow chart for CSMA/CA as used in WiFi. This type of state chart and its underlying finite state machine is how most protocols are implemented in hardware. There are notations for state machines such as SMC (you do not need to study SMC) whose manual is at <http://tinyurl.com/ne9ca9t> and which translates to efficient code in many programming languages.

The state machine above only handles frame transmission. In most devices it would be extended to also deal with receiving frames, checking frames and all the other necessary processes to implement the protocol. The code to run an IEEE 802.11n or ac transceiver is very large and complex!

Medium Access : IEEE 802.11 CSMA/CA

- Is a distributed de-centralized method.
- Cannot use CD as high transit power would destroy the sensitive semiconductors.
- Listen at transmitter **but interference happens at receiver!**
 - The world (noise) at the receiver cannot be perceived directly at the transmitter.
- Works best if TX and RX are close to each other.
 - This happens at high data rates due to needing high power to receive data correctly.
 - But, large exclusion area so as not to interfere. E.g. at 54Mbps exclusion area is 1000 (30dB) times the coverage area.

24/11/2016

COMP28411 Link Layer

53

CSMA/CA operates mainly at the transmitter to sense that the wireless medium is idle before transmitting a frame. However, interference and errors do not effect transmitters they only effect receivers. If the receiver is close to the transmitter then it is likely that any noise the transmitter hears the receiver will also hear and vice versa. However, as the distance between the transmitter and the receiver increases so does the difference in the noise environments they are both in. A transmitter has no accurate idea what a distant receiver is experiencing as noise. So, in practice, CSMA/CA works well with close by devices and much less well with distant devices.

In order to understand high data rate information receivers' need high power from the incoming signal. For example, WiFi at its lowest data rate may only need 0-10dB separation between the incoming signal and the sum of all other noise sources in order to be clearly and error free understood. At higher data rates the noise separation will be 20, 30 or more dB. Where 20dB is a factor of 100 and 30dB a factor of 1000 in loudness. Remember that dB is a unit less power ratio given in logarithmic form. $\text{dB} = 10 \log (\text{Power1} / \text{Power2})$.

The problem of needing large power ratios to successfully work is that the exclusion distance where nobody else can transmit while the current frame is being received around the receiver is massive its area being proportional in size to the power ratio needed at the receiver to clearly hear the data error free. In low density usage everything works well. In high density spaces, CSMA/CA will have high numbers of collisions resulting lots of re-transmissions which increase the number of collisions. WiFi uses much longer (larger) back-off times in high density networks to try and reduce the number of collisions but at the cost of considerable added latency.

“Taking Turns” MAC protocols - now mainly for wireless

Channel partitioning MAC protocols:

- Share channel *efficiently* and *fairly* at high load
- Inefficient at low load: Delay in channel access, $1/N$ bandwidth Allocated even if only 1 active node! Redundancy.



Random access MAC protocols

- Efficient at low load: single node can fully utilize channel
- High load: High collision probability and overhead – re-send.



“Taking turns” protocols

Look for best of both worlds!



24/11/2016



COMP28411 Link Layer



54

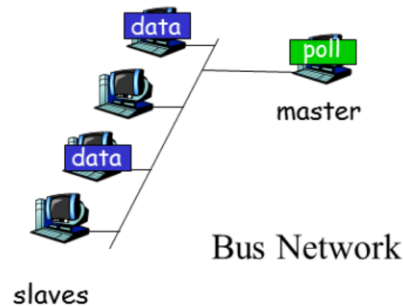
Whenever nodes are able and willing to cooperate with one another the collision problems in random based protocols can be avoided. Cooperation can be by taking turns with either centralized control from e.g. an Access Point (AP) or via distributed control by, for example passing a “your turn” token from node to node. Aside from time needed to arrange the cooperation, tell one another what data each has waiting so the turns can be scheduled or the order of having the “your turn” token can be decided, the rest of the time can be used for data transfers. These systems can therefore achieve much higher successful transfer rates than random access protocols sometimes approaching towards 100% channel occupancy with successful data transfers.

“Taking Turns” MAC protocols

A2

Polling:

- Master node “invites” slave nodes to transmit in turn.
- Typically used with “dumb” slave devices – *not necessarily though*.
- Concerns:
 - Polling overhead
 - Latency/delays
 - Single point of failure (master)



24/11/2016

COMP28411 Link Layer

55

In this variant of turn taking, a master node asks each slave node one by one if it wants to transfer any data. It polls them. Clearly there is overhead for this process where nodes with no data need to be asked just as much as nodes with data which adds latency. Because, it uses turn taking, if some data has just missed a turn it may have to wait some time before getting its next chance to be broadcast which may lead to real-time data transfer jitter problems.

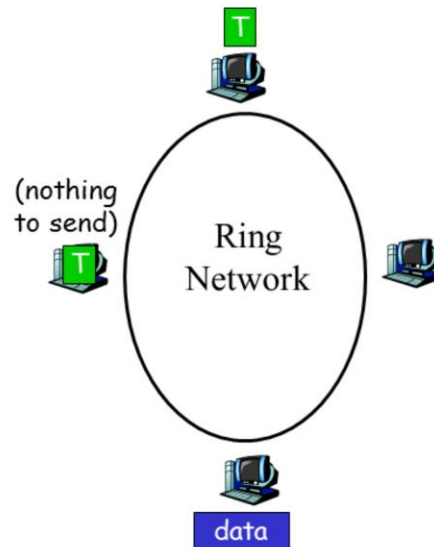
If the master controller dies for any reason the system dies. One solution though is for another node to step up and take over the control tasks but this probably needs some negotiation and will take a little time.

An example of this type of network is Bluetooth where a network can have one master, up to 7 active slaves and up to 255 parked (non active but can quite quickly become active) slaves.

“Taking Turns” MAC protocols

Token passing:

- Control **token** passed from one node to next sequentially.
- Token message
- Concerns:
 - Token overhead
 - Latency/delays
 - Single point of failure
 - Token
 - Broken ring



24/11/2016




COMP28411 Link Layer

56

One idea that was used for network control was the token ring. This is very similar to a round-robin system. A token is passed around the ring from node to node. When a node has the token it can send its data.

Token rings have largely disappeared because they are more complex and expensive than Ethernet which has become the default standard for almost all local area networks.

Summary of MAC Protocols

- **Started by looking at MAC addressees and the IP to/from MAC mapping called ARP.**
- **Channel partitioning**, by space, time, frequency or code
 - Space Division, Time Division, Frequency Division, Code Division - Multiple Access – SDMA, TDMA, FDMA, CDMA.
- **Random access** (dynamic),
 - ALOHA, Slotted-ALOHA, CSMA, 
 - Carrier sensing: easy in some technologies (wire), hard in others (wireless) 
 - CSMA/CD used in Ethernet
 - CSMA/CA used in 802.11. CA = Collision Avoidance.
 - Why not CD? 
- **Taking turns**
 - Polling from central site, token passing
 - Bluetooth, FDDI, IBM Token Ring

Questions ?

- Why are collisions very unlikely when Gigabit Ethernet is used?
- What does CSMA stand for?
- What does CDMA stand for? (Not “Collision”!)
- Why is SDMA so useful for wireless systems?
- If random access protocols are so inefficient, why are they used?
- When does a mobile phone use:
 - TDMA?
 - What other multiplexing methods does it also use?
 - CDMA?
 - What other multiplexing methods does it also use?
 - Slotted Aloha?