Wireless Media Access Protocols

© CS/ECE 439 Staff, University of Illinois

Wired Communication

- Pros
  - Very reliable
    - For Ethernet, medium HAS TO PROVIDE a Bit Error Rate (BER) of 10^{-12} (one error for every trillion bits!)
      - Insulated wires; wires placed underground and in walls
      - Error Correction Techniques
  - Very high transfer rates - currently up to 100 Gbit/s
  - Long distance - Up to 40km in 10-Gbit/s Ethernet
- Cons
  - Expensive to set up infrastructure
  - Infrastructure is fixed once set up
  - No physical mobility

© CS/ECE 439 Staff, University of Illinois

Wireless Communication

- Pros
  - Allows mobility
  - Much cheaper and easier to deploy, change, and upgrade!
- Cons
  - Exposed (unshielded) medium
    - Susceptible to physical phenomena (interference)
    - Variable BER – Error correction may not suffice in all cases
  - Slower data rates for wider distances
  - Link layer, and higher-layers, designed for wired medium
    - E.g. TCP assumes loss = congestion
    - Difficult to “hide” underlying behavior
  - Security: anyone in range hears transmission

© CS/ECE 439 Staff, University of Illinois

Wireless

- FCC oversees all wireless communication
- Licensed Bands
  - Cellular phones, 3G,4G, AM/FM radio, broadcast television, satellites, WiMax
  - Use of resources left to "owner" of band
- Unlicensed Bands
  - 802.11, Bluetooth, ZigBee, IR, WiMax
  - No license needed – free for all!
  - Restrictions to limit interference
    - Limit on transmission power
    - Spread spectrum communication

Unlicensed Bands
900 MHz
  Industrial, Scientific and Medical (ISM)
2.4 GHz
5.4 GHz
10 – 66 GHz

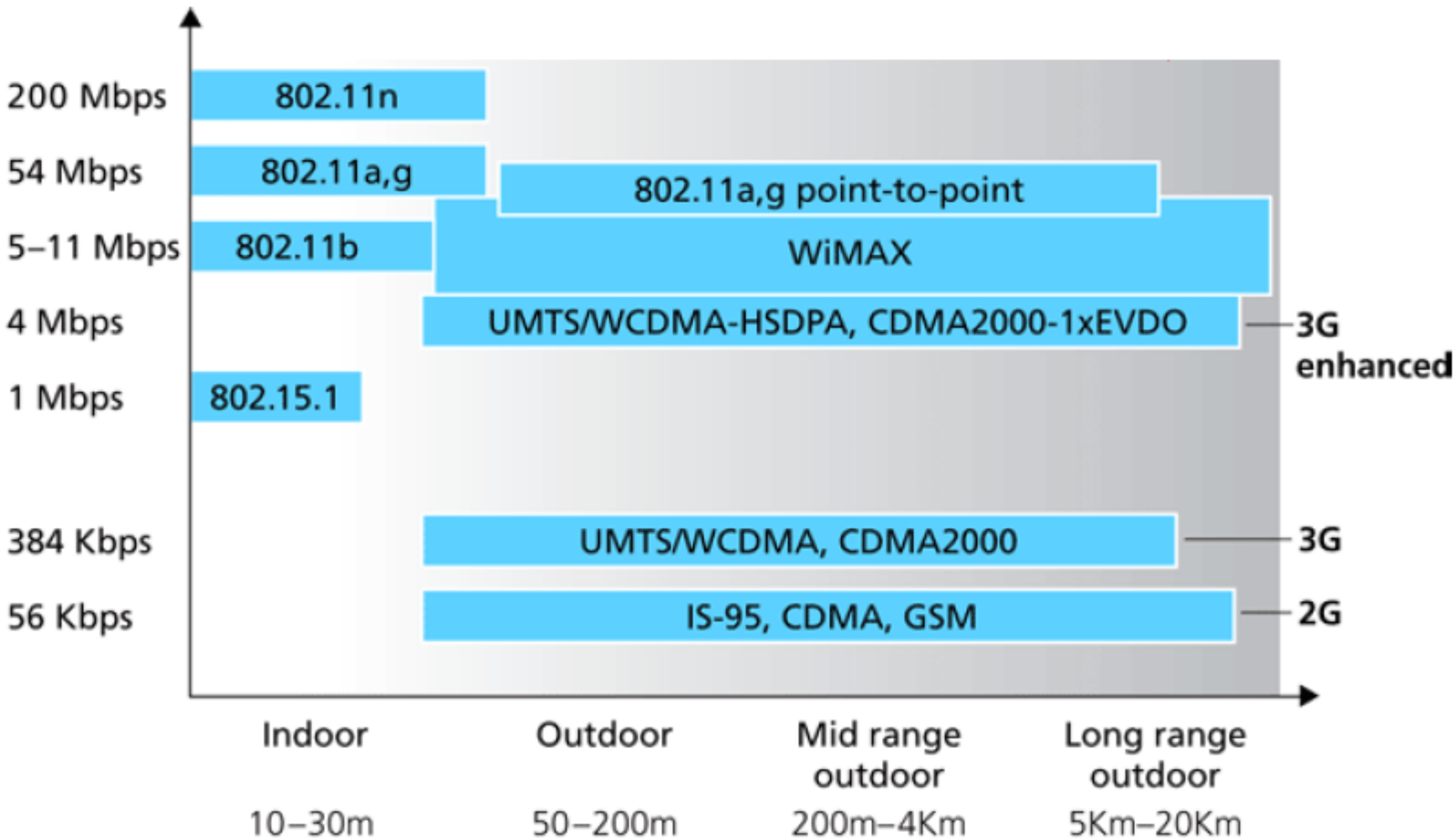
© CS/ECE 439 Staff, University of Illinois

Wireless Communication Standards (Alphabet Soup)

- Cellular (2G): GSM, CDMA, GPRS
- 3G: CDMA2000, W-CDMA, EDGE
- 4G: WiMAX, LTE
- IEEE 802.11
  - A: 5.0Ghz band, max 54Mbps
  - B: 2.4Ghz band, max 11Mbps
  - G: 2.4Ghz, max 54Mbps
  - N: 2.4/5Ghz, max 600Mbps
  - Many other versions
- IEEE 802.15 – lower power wireless
  - 802.15.1: 2.4Ghz, max 2.1 Mbps (Bluetooth)
  - 802.15.4: 2.4Ghz, max 250 Kbps (Sensor Networks)

© CS/ECE 439 Staff, University of Illinois

Wireless Link Characteristics



© CS/ECE 439 Staff, University of Illinois

Challenges of wireless

- Path loss
  - Signal attenuation as a function of distance
  - Signal-to-noise ratio (SNR—Signal Power/Noise Power) decreases, make signal unrecoverable
- Multipath propagation
  - Signal reflects off surfaces, effectively causing self-interference
- Internal interference (from other users)
  - Hosts within range of each other collide with one another's transmission
- External interference
  - Microwave is turned on and blocks your signal

© CS/ECE 439 Staff, University of Illinois

Spread Spectrum

- Direct Sequence Spread Spectrum
  - Spread the signal over a wider frequency band than required
  - Originally designed to thwart jamming
  - Original 802.11 uses 83 MHz in 2.4 GHz band
- Frequency-Hopped Spread Spectrum
  - Uses 80 1MHz sub-bands in 2.4 GHz band
  - Transmit over a random sequence of frequencies

© CS/ECE 439 Staff, University of Illinois

Spread Spectrum

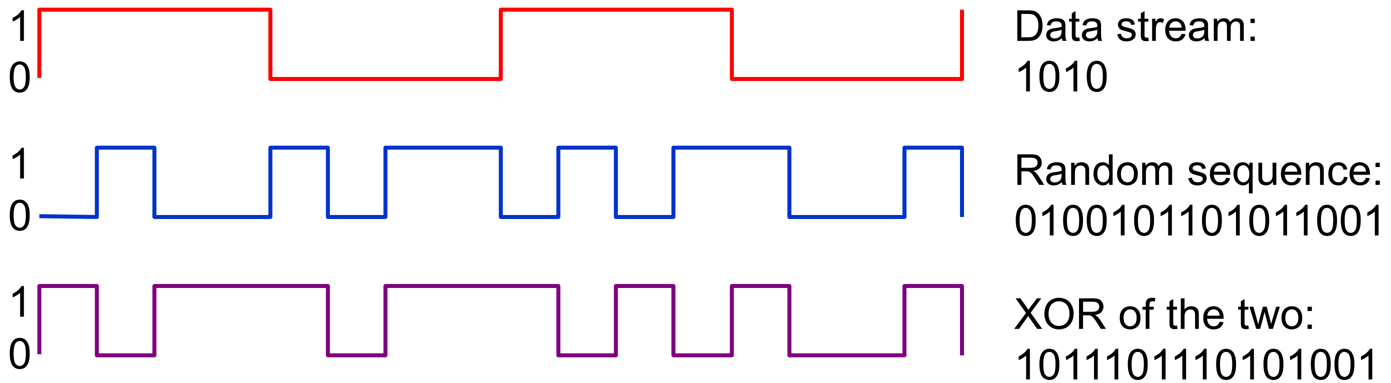
- Direc
  - Sp
    th
  - O
  - O
- Freq
  - Us
  - Tr
    fre

- Frequency hopping had many inventors
  - 1942: actress Hedy Lamarr and composer George Antheil patented Secret Communications System
  - Piano-roll to change between 88 frequencies, and was intended to make radio-guided torpedoes harder for enemies to detect or to jam
  - The patent was rediscovered in the 1950s during patent searches when private companies independently developed Code Division Multiple Access, a civilian form of spread-spectrum

© CS/ECE 439 Staff, University of Illinois

Direct Sequence Spread Spectrum

- Spread Spectrum
  - For each bit, send XOR of that bit and n random bits
  - Random sequence is known to both sender and receiver
  - Called n-bit chipping code (802.11 uses 11bit code)



© CS/ECE 439 Staff, University of Illinois

Communication Characteristics

- Rate
  - Defines the communication speeds
- Frequency
  - Defines the behavior in the physical environment
- Range
  - Defines the physical communication area
- Power
  - Defines the cost in terms of energy

© CS/ECE 439 Staff, University of Illinois

Communication Characteristics

- Rate
  - Defines the communication speeds
  - Channel Bandwidth
    - Defined by the specifications of the technology
  - Available Bandwidth
    - Defined by the current use of the communication channel
      - Channel competition – MAC layer
      - Bandwidth competition – Transport layer

© CS/ECE 439 Staff, University of Illinois

Communication Characteristics

- Frequency/signal characteristics
  - Defines the behavior in the physical environment
    - Does the signal go through walls?
    - Is the signal susceptible to multipath fading?
  - Challenge
    - Many technologies use the same frequency

© CS/ECE 439 Staff, University of Illinois

Communication Characteristics

- Range
  - Defines the physical communication area
  - May be affected by buildings, walls, people
  - May be affected by distance

© CS/ECE 439 Staff, University of Illinois

Communication Characteristics

- Power
  - Defines the cost in terms of energy
  - Power can be adapted to save energy
    - Inversely affects range

© CS/ECE 439 Staff, University of Illinois

Communication Characteristics

- Rate
  - Defines the communication spee
- Frequency
  - Defines the behavior in th sical environment
- Range
  - Defines the physi nmunication area
- Power
  - Defines the t in terms of energy

Everything is inter-related!

© CS/ECE 439 Staff, University of Illinois

Current Wireless Technologies

- IEEE 802.11
  - Wireless LAN (WLAN)
  - MAC layer based on Ethernet
    - Originally called "wireless Ethernet"

	Max Rate	Frequency	Range	Energy
Pre-802.11	2 Mbps	900 Mhz	100 m	100 mW
IEEE 802.11b	11 Mbps	2.4 GHz	35/150 m	100 mW
IEEE 802.11g	54 Mbps	2.4 GHz	35/150 m	100 mW
IEEE 802.11a	54 Mbps	5 GHz	10 /120 m	100 mW
IEEE 802.11n	600 Mbps	2.4/5 GHz	70 /250 m	100 mW

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 - Physical Layer

- IEEE 802.11 b
  - Direct Sequence Spread Spectrum
    - Uses 83 MHz in 2.4 GHz band
    - Spread the signal over a wider frequency band than required
    - Originally designed to prevent jamming
  - 3 orthogonal channels
- IEEE 802.11 g
  - Frequency-Hopped Spread Spectrum
    - Uses 80 1MHz sub-bands in 2.4 GHz band
    - Transmit over a random sequence of frequencies
      - Hop 10 times a second
    - Originally designed to avoid snooping
  - 3 orthogonal channels

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 - Physical Layer

- IEEE 802.11 a
  - Orthogonal Frequency Division Multiplexing (OFDM)
  - 13 orthogonal channels
- IEEE 802.11 n
  - Works on both 802.11a and 802.11g spectrum
  - MIMO – Multi-input, Multi-output antenna
    - Up to 4 antenna

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 - Physical Layer

- Channel Rate vs. Signal strength
  - All versions of IEEE 802.11 can reduce the rate to increase the signal strength
    - IEEE 802.11 b — 1, 2, 5.5, 11 Mbps
    - IEEE 802.11 a, g — 6, 9, 12, 18, 24, 36, 48, or 54 Mbps
  - Increased range → lower signal → lower rate

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 Extensions

- IEEE 802.11e
  - Enhancements: QoS, including packet bursting
- IEEE 802.11i
  - Enhanced security
- IEEE 802.11p
  - WAVE - Wireless Access for the Vehicular Environment
- IEEE 802.11s
  - ESS Mesh Networking
- IEEE 802.11u
  - Interworking with non-802 networks (for example, cellular)
- IEEE 802.11 ac
  - Provides high throughput in the 5 GHz band
  - Wider RF bandwidth, more streams (up to 8), and high-density modulation (up to 256 QAM)

© CS/ECE 439 Staff, University of Illinois

Current Wireless Technologies

- BlueTooth – IEEE 802.15.1
  - Originally designed as a cable replacement technology
  - Master/Slave configuration
  - Bluetooth Low Energy (BLE) for low power discovery

	Max Rate	**Frequency**	**Range**	**Energy**
BlueTooth	3 Mbps	2.4 GHz	100 m	100 mW
			10 m	2.5 mW
			1 m	1 mW

© CS/ECE 439 Staff, University of Illinois

BlueTooth

- Physical Layer
  - Frequency-Hopped Spread Spectrum
    - Uses 79 1MHz sub-bands in 2.4 GHz band
    - Transmit over a random sequence of frequencies
      - Hop 1600 times a second
    - 5 orthogonal sub-hopping sets
- MAC Layer
  - Slotted
    - Managed by the master
    - Single slot packet
      - Max data rate of 172Kbps
    - Multislot frames
      - Support higher rates of 721Kbps

© CS/ECE 439 Staff, University of Illinois

Current Wireless Technologies

- ZigBee – IEEE 802.15.4
  - Low power, short range
    - Sensor networks
    - Personal area networks

	Max Rate	Frequency	Range	Energy
ZigBee (IEEE 802.15.4)	250 kbps	2.4 GHz	10 - 100 m	1 mW
	40 Kbps	915 MHz	10 - 100 m	1 mW
	20 Kbps	868 MHz	10 - 100 m	1 mW

© CS/ECE 439 Staff, University of Illinois

ZigBee

- Physical Layer
  - Direct Sequence Spread Spectrum
    - 2.4 GHz – 16 orthogonal channels
    - 915 MHz – 10 orthogonal channels
    - 868 MHz – 1 channel
- MAC Layer
  - CSMA/CA
  - Battery Life Extension (BLE) mode
    - Limit the back-off exponent to max 2

© CS/ECE 439 Staff, University of Illinois

Current Wireless Technologies

- InfraRed
  - Directional

	Max Rate	Frequency	Range	Energy
InfraRed – IrDA	9600 bps – 16 Mbps		< 1 m	Low

© CS/ECE 439 Staff, University of Illinois

Current Wireless Technologies

- RFID
  - Passive technology
  - Used for inventory control

	Max Rate	Frequency	Range	Energy
RFID – Near Field			< 10 cm	Self-powered
RFID – Far Field			< 3 m	Self-powered

© CS/ECE 439 Staff, University of Illinois

RFID

- RFID Basics
  - Reader powers the “tag”
  - Antenna “captures” the energy for a response
  - Simple MAC
    - All tags respond
  - Contention-based MAC
    - Use ALOHA or Tree-splitting algorithm to avoid collisions
- Near field
  - Magnetic induction
    - Range < 10 cm
- Far field
  - Electromagnetic wave capture
    - Range < 3 m

© CS/ECE 439 Staff, University of Illinois

Current Wireless Technologies

- WiMAX – IEEE 802.16
  - Wireless Metropolitan Area Networks (WMAN)
  - May require line-of sight (LOS)

	Max Rate	Frequency	Range	Energy
WiMAX –LOS	70 Mbps	10-66 GHz	50 km	Very high
WiMAX Non-LOS	~14 Mbps	2-11 GHz	~10 km	Very high

© CS/ECE 439 Staff, University of Illinois

Current Wireless Technologies

- WiMAX – IEEE 802.16
  - Transmissions to/from base station by hosts with omnidirectional antenna
  - Base station-to-base station backhaul with point-to-point antenna

	Max Rate	Frequency	Range	Energy
WiMAX –LOS	70 Mbps	10-66 GHz	50 km	Very high
WiMAX Non-LOS	~14 Mbps	2-11 GHz	~10 km	Very high

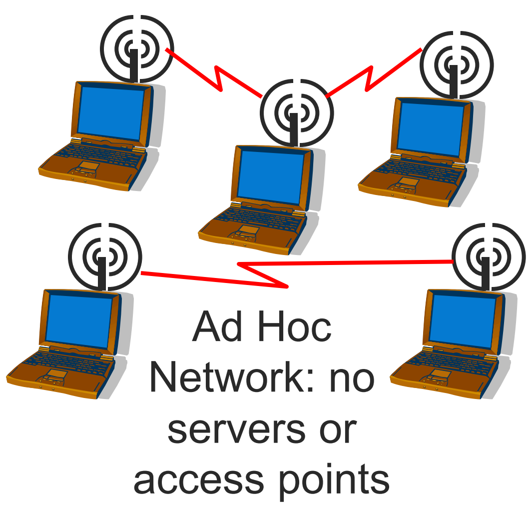
© CS/ECE 439 Staff, University of Illinois

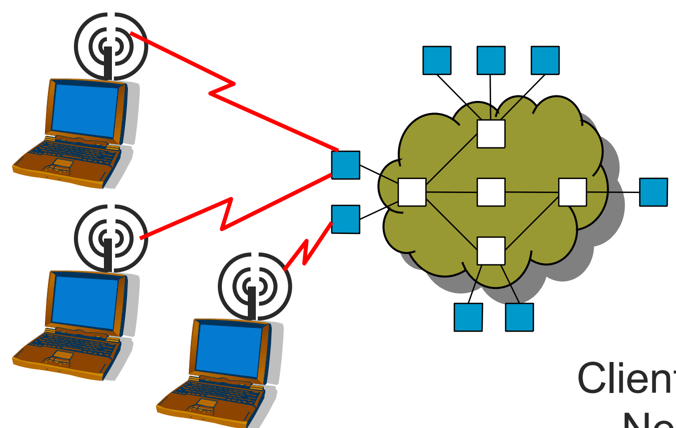
Media Access Control Protocols

© CS/ECE 439 Staff, University of Illinois

Medium Access Control

- IEEE 802.11
  - A physical and multiple access layer standard for wireless local area networks (WLAN)





Client Server
Network

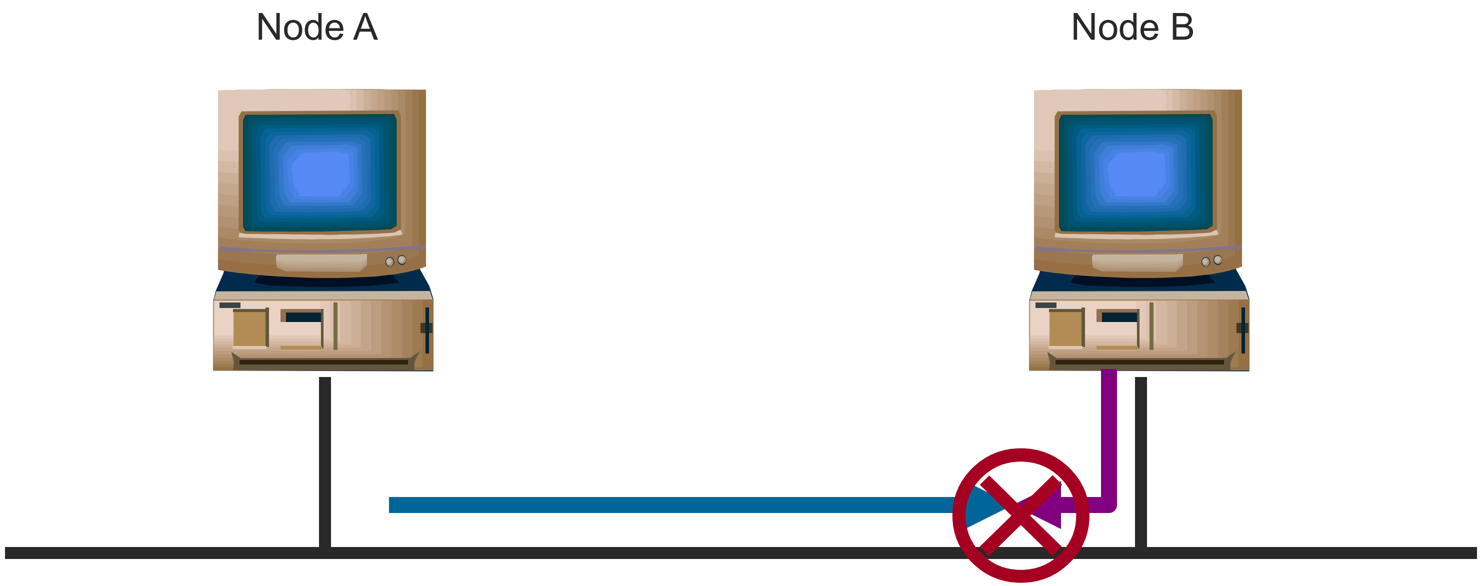
© CS/ECE 439 Staff, University of Illinois

Medium Access Control

- Wireless channel is a shared medium
- Need access control mechanism to avoid interference
- Why not CSMA/CD?

© CS/ECE 439 Staff, University of Illinois

Ethernet MAC Algorithm

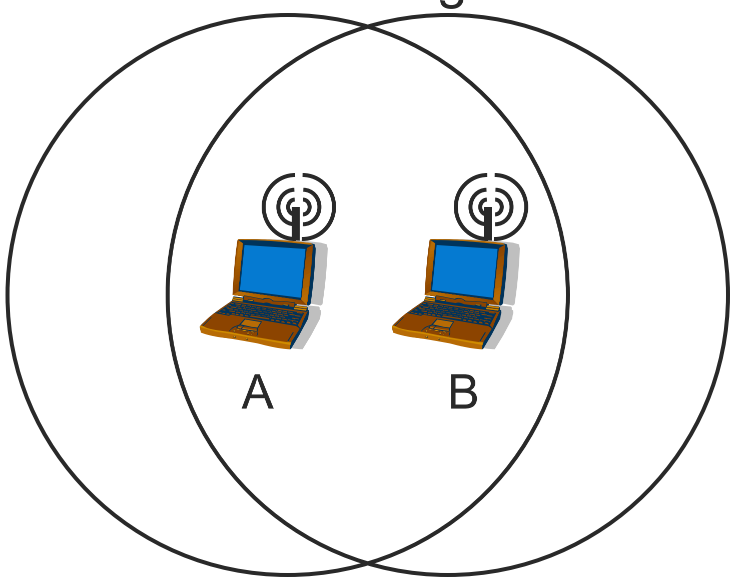


- Listen for carrier sense before transmitting
- Collision: What you hear is not what you sent!

© CS/ECE 439 Staff, University of Illinois

CSMA/CD in WLANs?

- Most (if not all) radios are half-duplex
  - Listening while transmitting is not possible
- Collision might not occur at sender
  - Collision at receiver might not be detected by sender!



© CS/ECE 439 Staff, University of Illinois

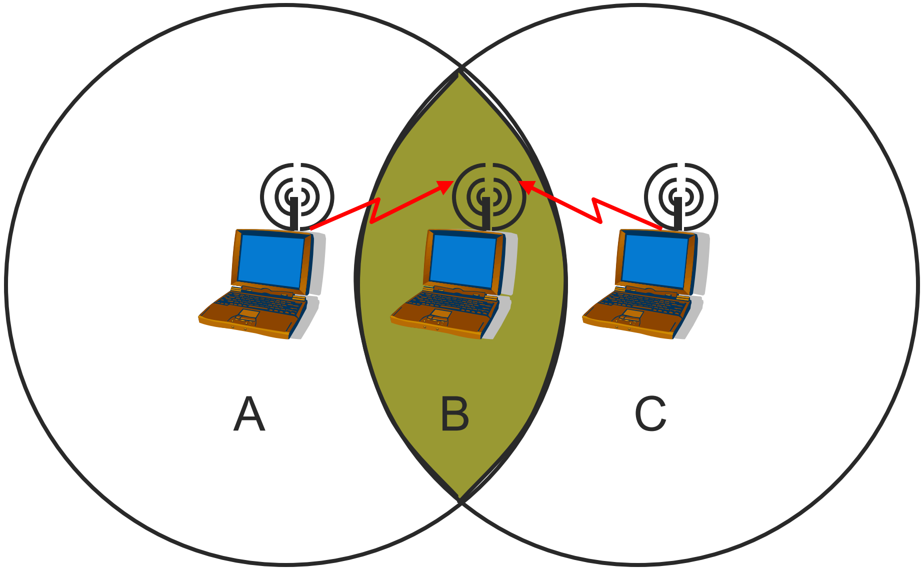
Wireless Ethernet - CSMA/CA

- CS – Carrier Sense
  - Nodes can distinguish between an idle and a busy link
- MA - Multiple Access
  - A set of nodes send and receive frames over a shared link
- CA – Collision Avoidance
  - Nodes use protocol to prevent collisions from occurring

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 MAC Layer Standard

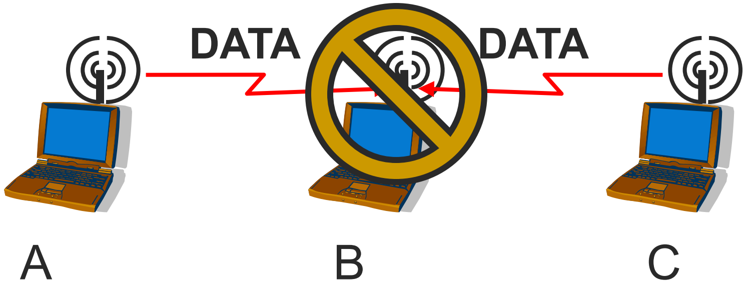
- Similar to Ethernet
- But consider the following:



© CS/ECE 439 Staff, University of Illinois

Hidden Terminal Problem

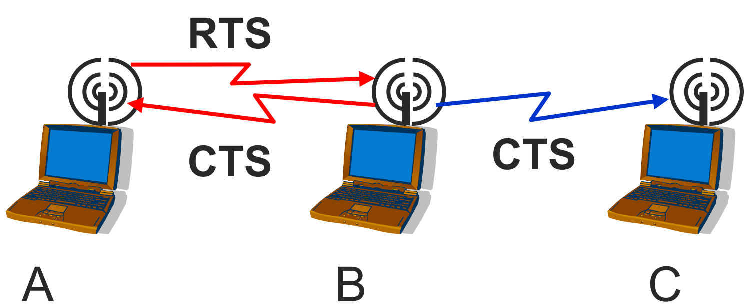
- Node B can communicate with both A and C
- A and C cannot hear each other
- When A transmits to B, C cannot detect the transmission using the carrier sense mechanism
- If C transmits, collision will occur at node B



© CS/ECE 439 Staff, University of Illinois

MACA Solution for Hidden Terminal Problem

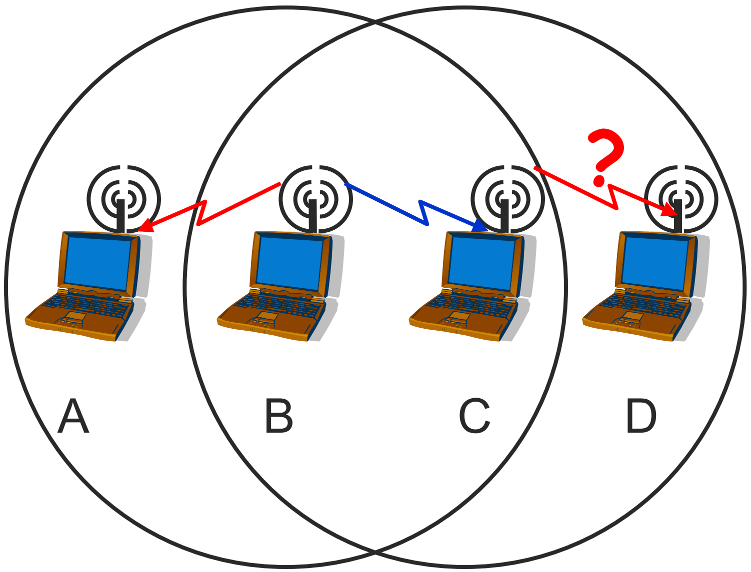
- When node A wants to send a packet to node B
  - Node A first sends a Request-to-Send (RTS) to A
- On receiving RTS
  - Node A responds by sending Clear-to-Send (CTS)
  - provided node A is able to receive the packet
- When a node C overhears a CTS, it keeps quiet for the duration of the transfer



© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 MAC Layer Standard

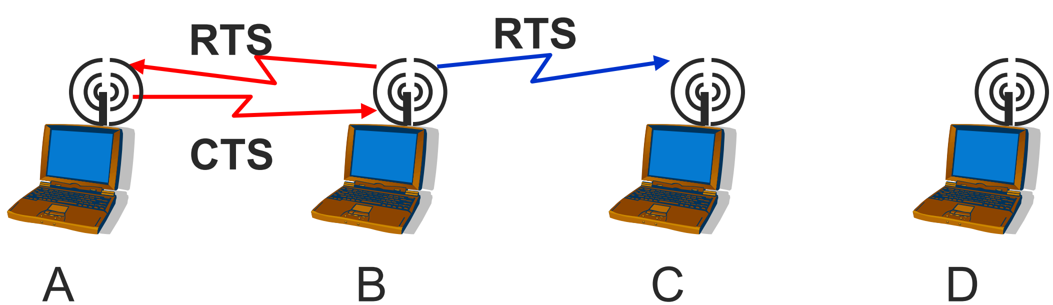
- But we still have a problem



© CS/ECE 439 Staff, University of Illinois

Exposed Terminal Problem

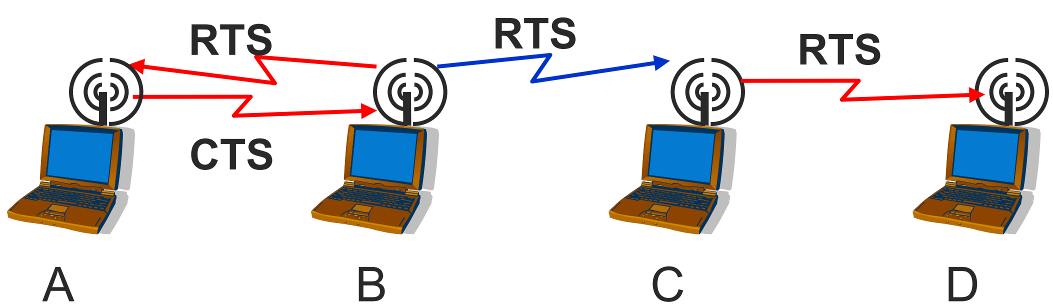
- B talks to A
- C wants to talk to D
- C senses channel and finds it to be busy
- C stays quiet (when it could have ideally transmitted)



© CS/ECE 439 Staff, University of Illinois

MACA Solution for Exposed Terminal Problem

- Sender transmits Request to Send (RTS)
- Receiver replies with Clear to Send (CTS)
- Neighbors
  - See CTS - Stay quiet
  - See RTS, but no CTS - OK to transmit



© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 MAC Layer Standard

- MACAW – Multiple Access with Collision Avoidance for Wireless
  - Sender transmits Request to Send (RTS)
  - Receiver replies with Clear to Send (CTS)
  - Neighbors
    - See CTS
      - Stay quiet
    - See RTS, but no CTS
      - OK to transmit
  - Receiver sends ACK for frame
    - Neighbors stay silent until they hear ACK

© CS/ECE 439 Staff, University of Illinois

Collisions

- Still possible
  - RTS packets can collide!
- Binary exponential backoff
  - Backoff counter doubles after every collision and reset to minimum value after successful transmission
  - Performed by stations that experience RTS collisions
- RTS collisions not as bad as data collisions in CSMA
  - Since RTS packets are typically much smaller than DATA packets

© CS/ECE 439 Staff, University of Illinois

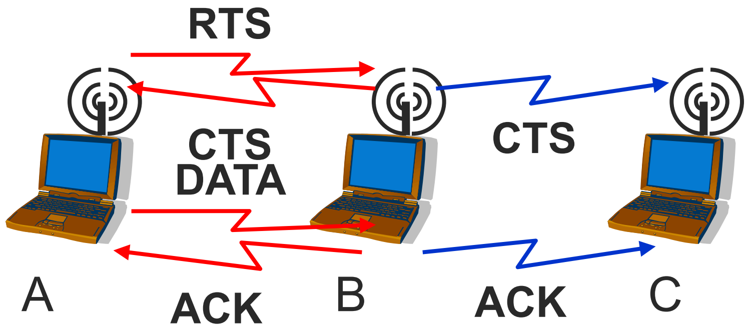
Reliability

- Wireless links are prone to errors
  - High packet loss rate detrimental to transport-layer performance
- Mechanisms needed to reduce packet loss rate experienced by upper layers

© CS/ECE 439 Staff, University of Illinois

A Simple Solution to Improve Reliability - MACAW

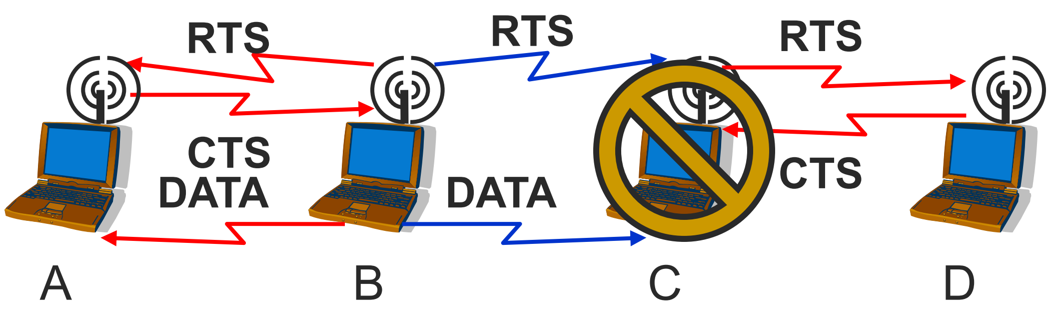
- When node B receives a data packet from node A, node B sends an Acknowledgement (ACK)
- If node A fails to receive an ACK
  - Retransmit the packet



© CS/ECE 439 Staff, University of Illinois

Revisiting the Exposed Terminal Problem

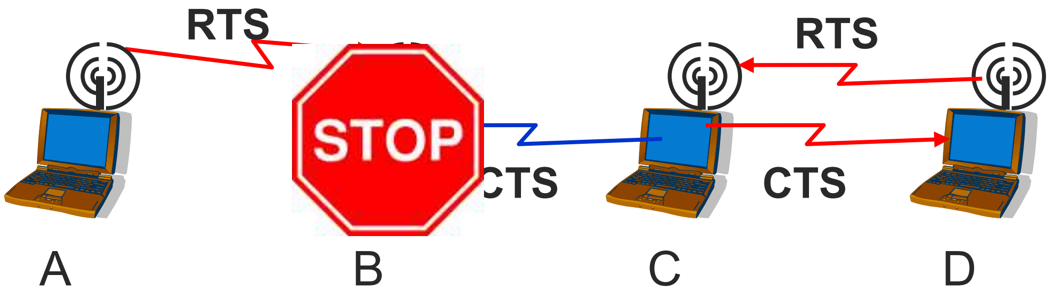
- Problem
  - Exposed terminal solution doesn't consider CTS at node C
- With RTS-CTS, C doesn’t wait since it doesn’t hear A’s CTS
  - With B transmitting DATA, C can’t hear intended receiver’s CTS
  - C trying RTS while B is transmitting is useless



© CS/ECE 439 Staff, University of Illinois

Deafness

- For the scenario below
  - Node A sends an RTS to B
    - While node C is receiving from D,
  - Node B cannot reply with a CTS
    - B knows that D is sending to C
    - A keeps retransmitting RTS and increasing its own BO timeout



© CS/ECE 439 Staff, University of Illinois

Broadcast/Multicast

- Problem
  - Basic RTS-CTS only works for unicast transmissions
- For multicast
  - RTS would get CTS from each intended receiver
  - Likely to cause (many) collisions back at sender

© CS/ECE 439 Staff, University of Illinois

Multicast - MACAW

- Sort-of solution
  - Don't use CTS for multicast data
- Receivers recognize multicast destination in RTS
  - Don't return CTS
  - Sender follows RTS immediately by DATA
  - After RTS, all receivers defer for long enough for DATA
- Helps, but doesn't fully solve problem
  - Like normal CSMA, only those in range of sender will defer
  - Others in range of receiver will not defer

© CS/ECE 439 Staff, University of Illinois

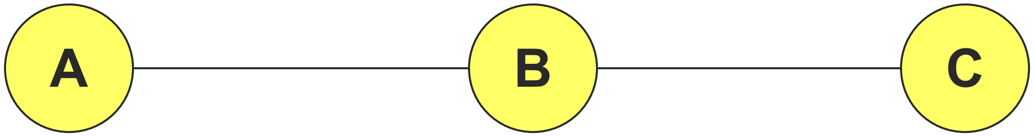
IEEE 802.11 Wireless MAC

- Distributed and centralized MAC components
  - Distributed Coordination Function (DCF)
  - Point Coordination Function (PCF)
- DCF suitable for multi-hop ad hoc networking
- DCF is a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 DCF

- Uses RTS-CTS exchange to avoid hidden terminal problem
  - Any node overhearing a CTS cannot transmit for the duration of the transfer
- Uses ACK to achieve reliability
- Any node receiving the RTS cannot transmit for the duration of the transfer
  - To prevent collision with ACK when it arrives at the sender
  - When B is sending data to C, node A keeps quite



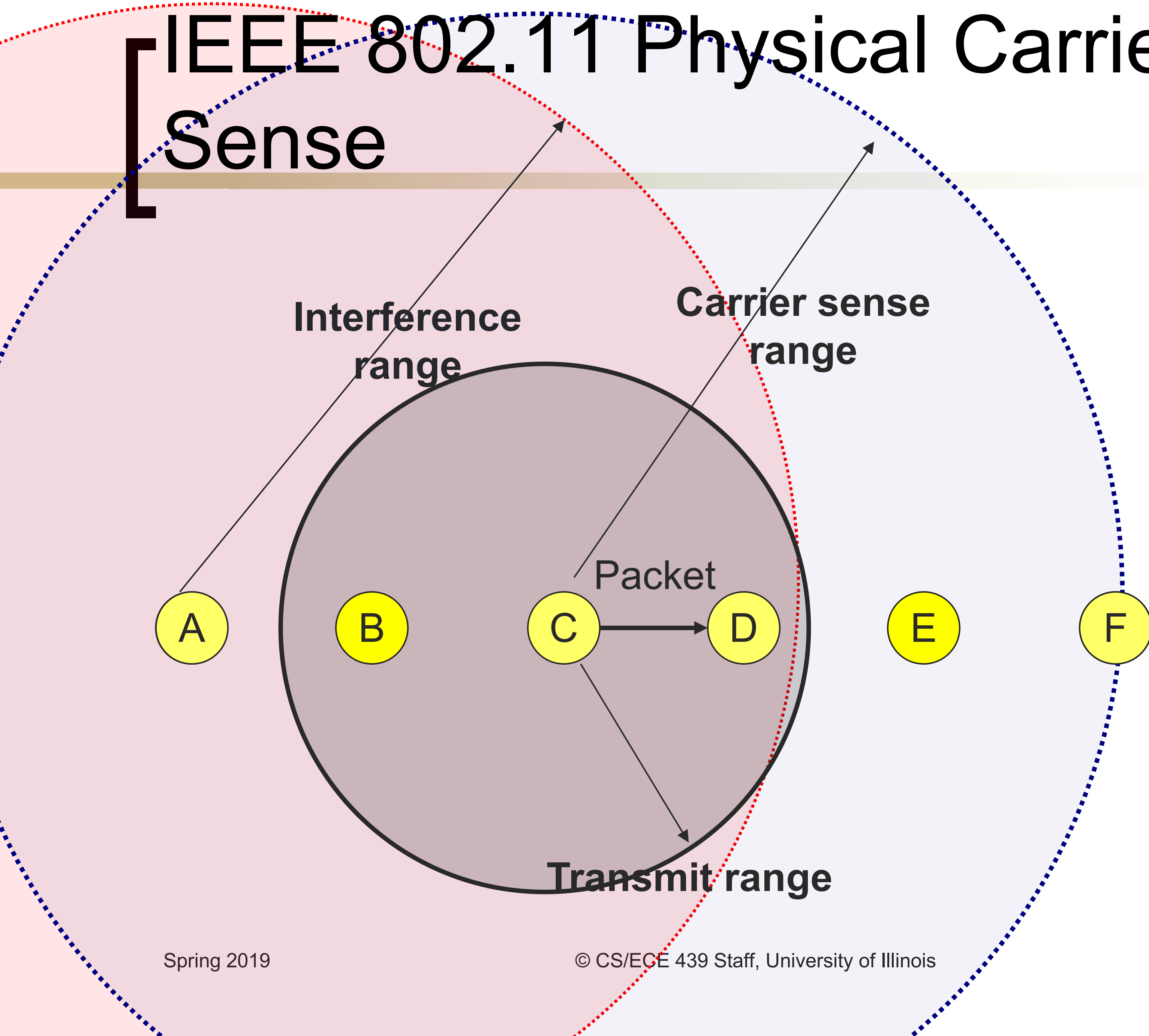
© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 CSMA/CA

- Nodes stay silent when carrier sensed
  - Physical carrier sense
  - Virtual carrier sense
    - Network Allocation Vector (NAV)
    - NAV is updated based on overheard RTS/CTS/DATA/ACK packets, each of which specified duration of a pending transmission
- Backoff intervals used to reduce collision probability

© CS/ECE 439 Staff, University of Illinois

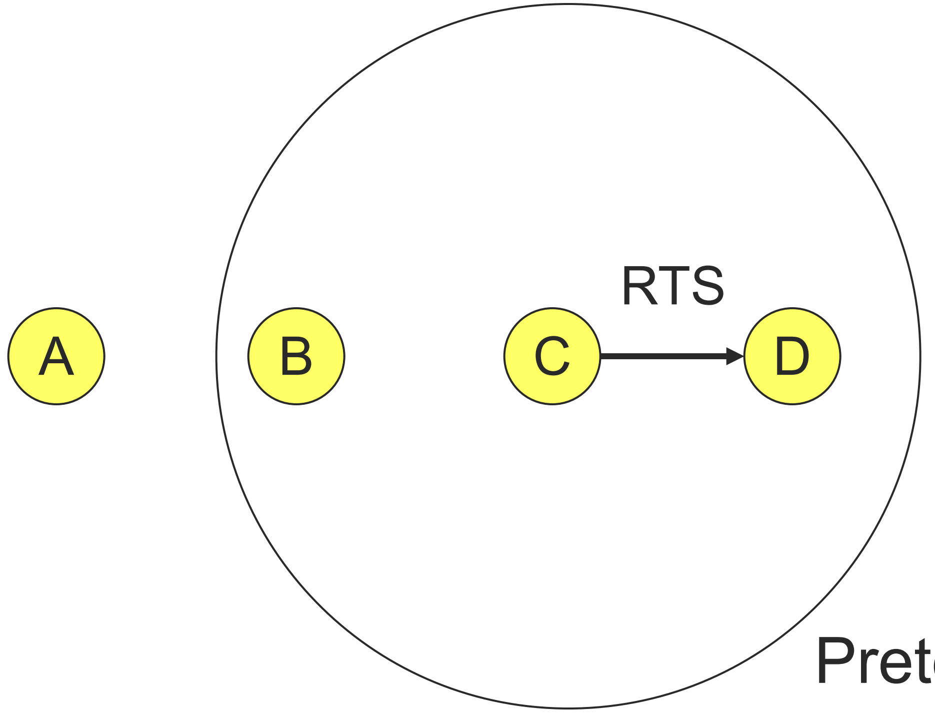
IEEE 802.11 Physical Carrier Sense



© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 Virtual Carrier Sense

RTS = Request-to-Send



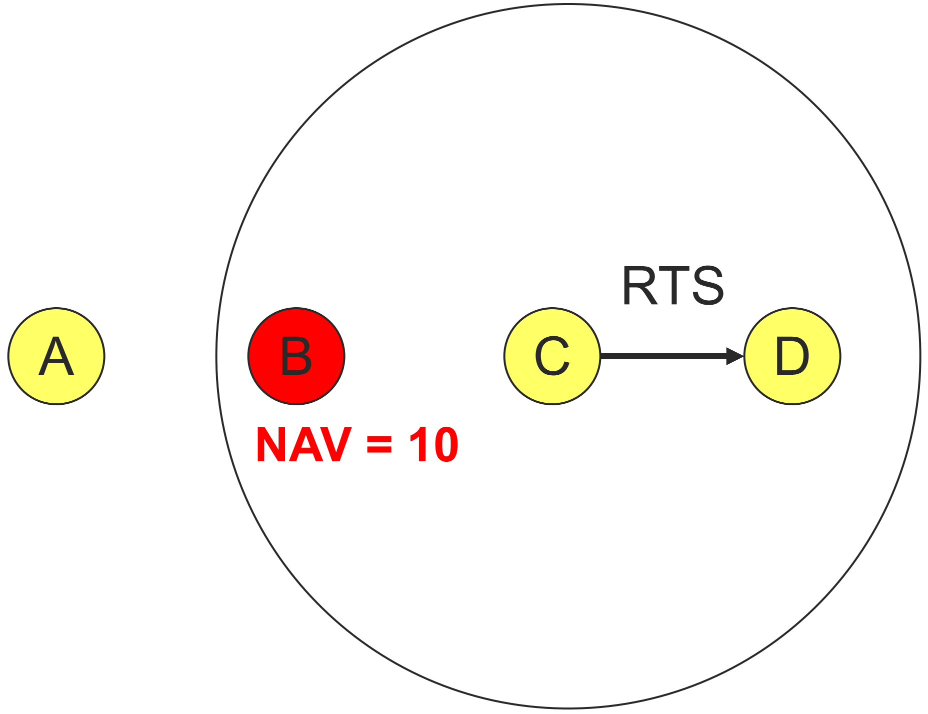
Pretending a circular range

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 Virtual Carrier Sense

NAV = remaining duration to keep quiet

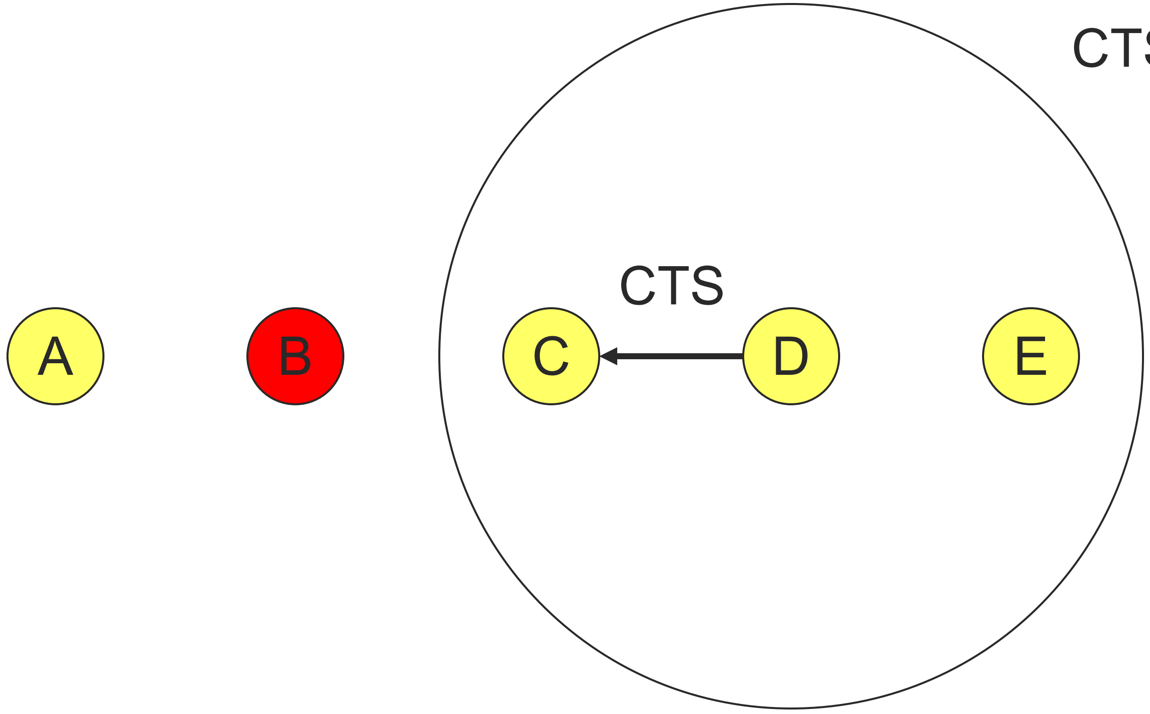
RTS = Request-to-Send



© CS/ECE 439 Staff, University of Illinois

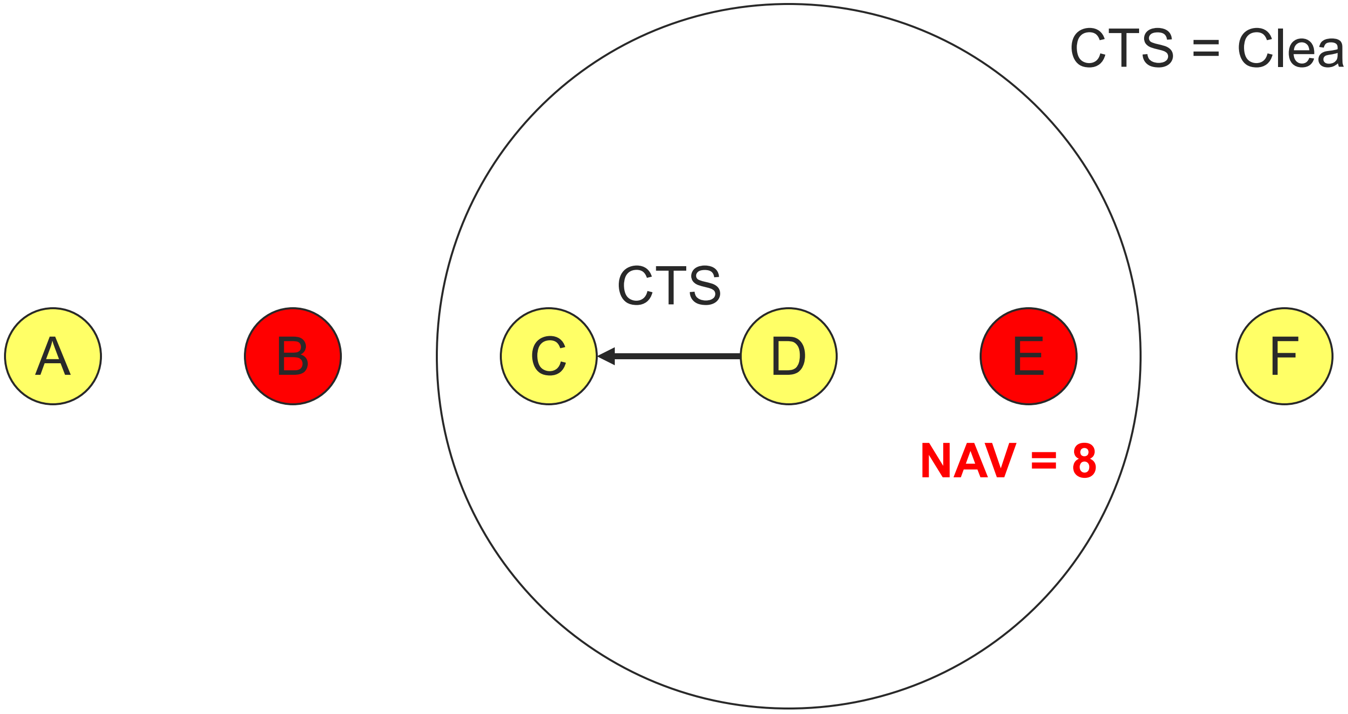
IEEE 802.11 Virtual Carrier Sense

CTS = Clear-to-Send



IEEE 802.11 Virtual Carrier Sense

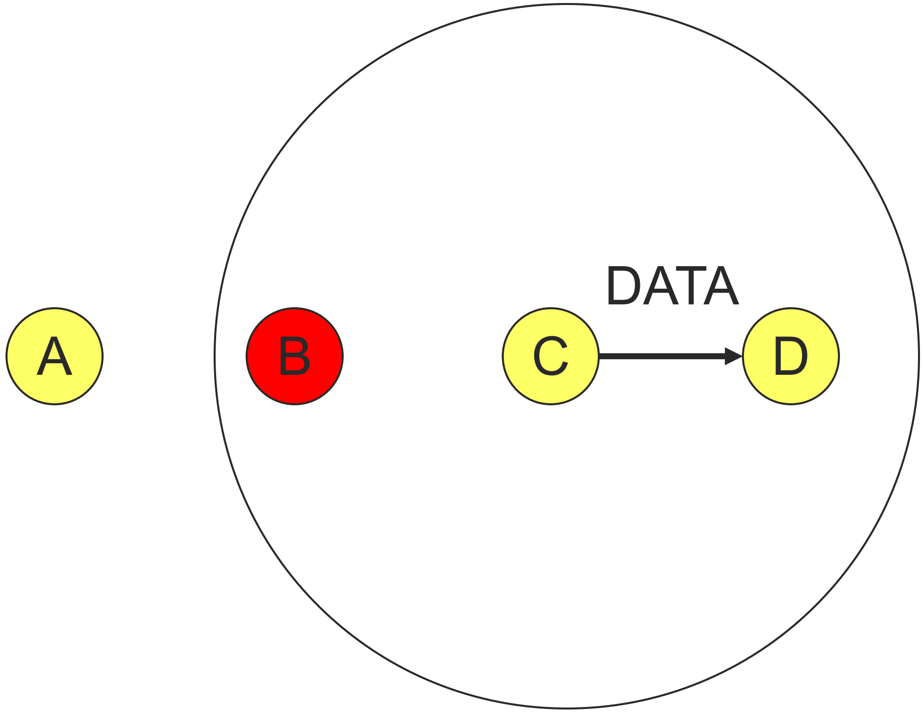
CTS = Clear-to-Send



© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 Virtual Carrier Sense

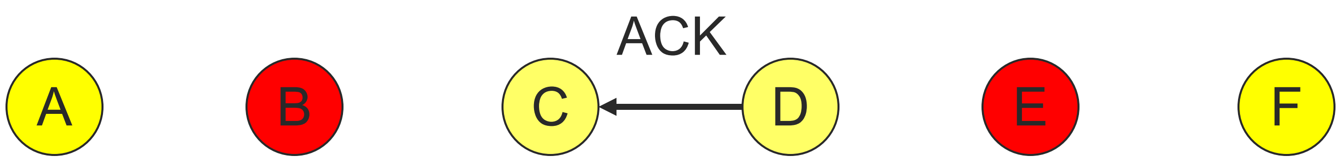
- DATA packet follows CTS



© CS/ECE 439 Staff, University of Illinois

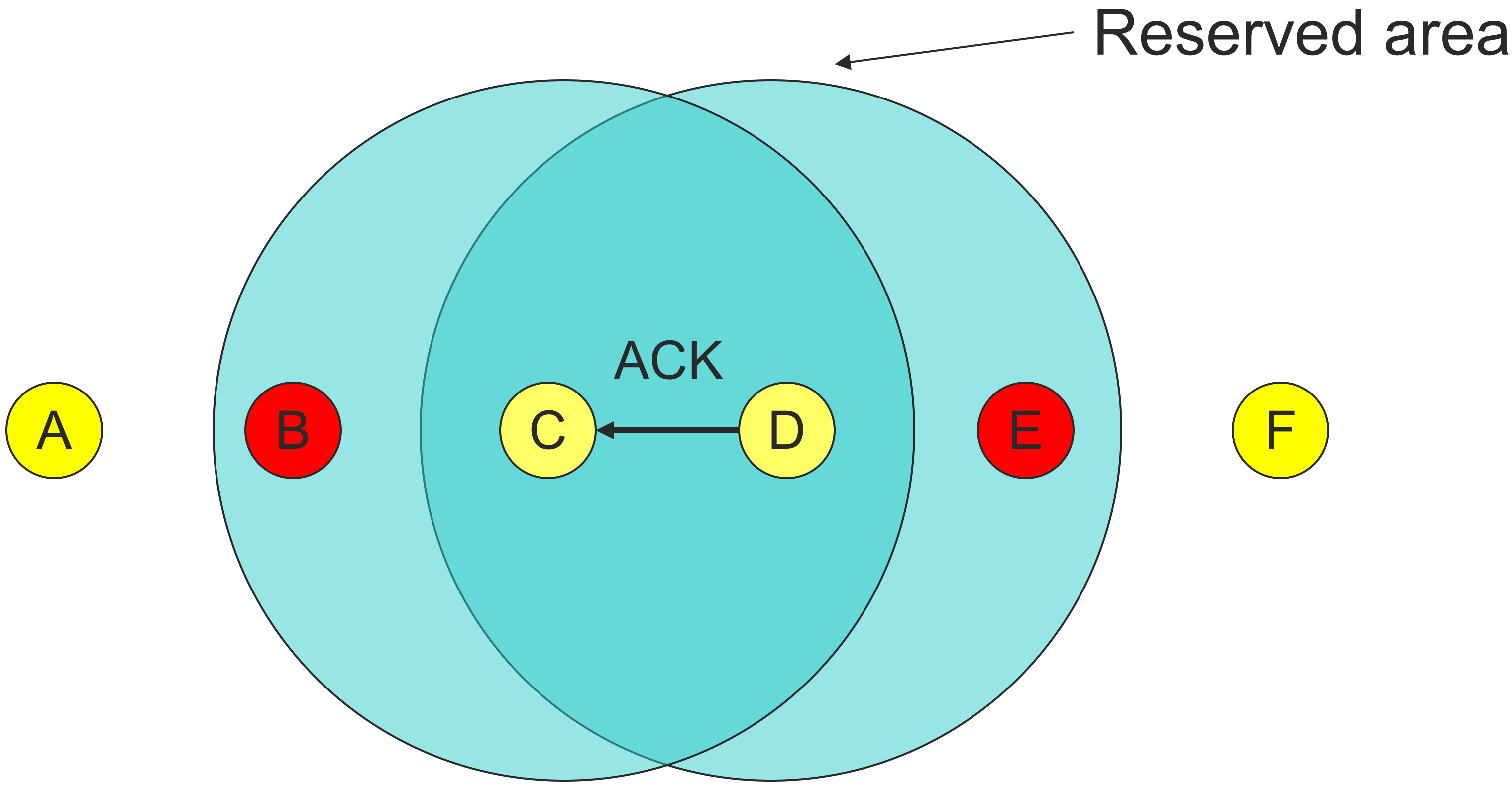
IEEE 802.11 Virtual Carrier Sense

- Successful data reception acknowledged using ACK



© CS/ECE 439 Staff, University of Illinois

IEEE 802.11



© CS/ECE 439 Staff, University of Illinois

Ethernet vs. IEEE 802.11

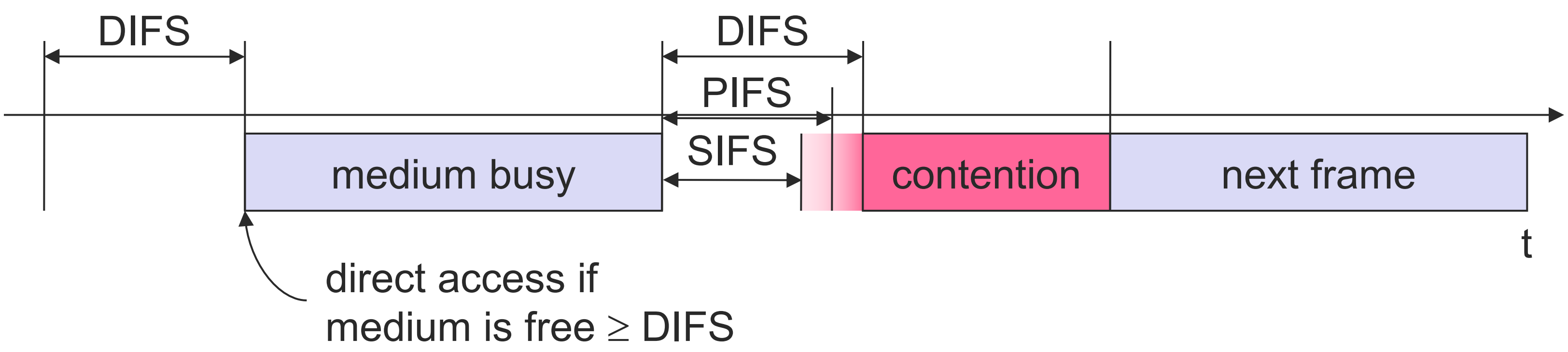
- If carrier is sensed
  - Send immediately
  - Send maximum of 1500B data (1527B total)
  - Wait 9.6 μs before sending again

- If carrier is sensed
  - When should a node transmit?

© CS/ECE 439 Staff, University of Illinois

Interframe Spacing

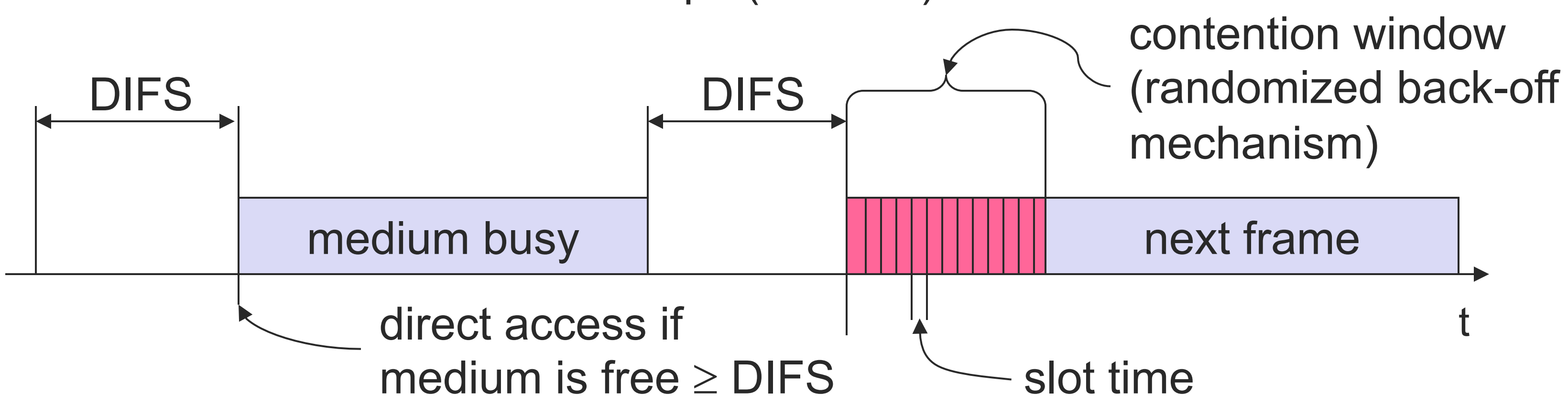
- Interframe spacing
  - Plays a large role in coordinating access to the transmission medium
- Varying interframe spacings
  - Creates different priority levels for different types of traffic!
- 802.11 uses 4 different interframe spacings



© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 - CSMA/CA

- Sensing the medium
- If free for an Inter-Frame Space (IFS)
  - Station can start sending (IFS depends on service type)
- If busy
  - Station waits for a free IFS, then waits a random back-off time (collision avoidance, multiple of slot-time)
- If another station transmits during back-off time
  - The back-off timer stops (fairness)



© CS/ECE 439 Staff, University of Illinois

Types of IFS

- SIFS
  - Short interframe space
  - Used for highest priority transmissions
  - RTS/CTS frames and ACKs
- DIFS
  - DCF interframe space
  - Minimum idle time for contention-based services (> SIFS)

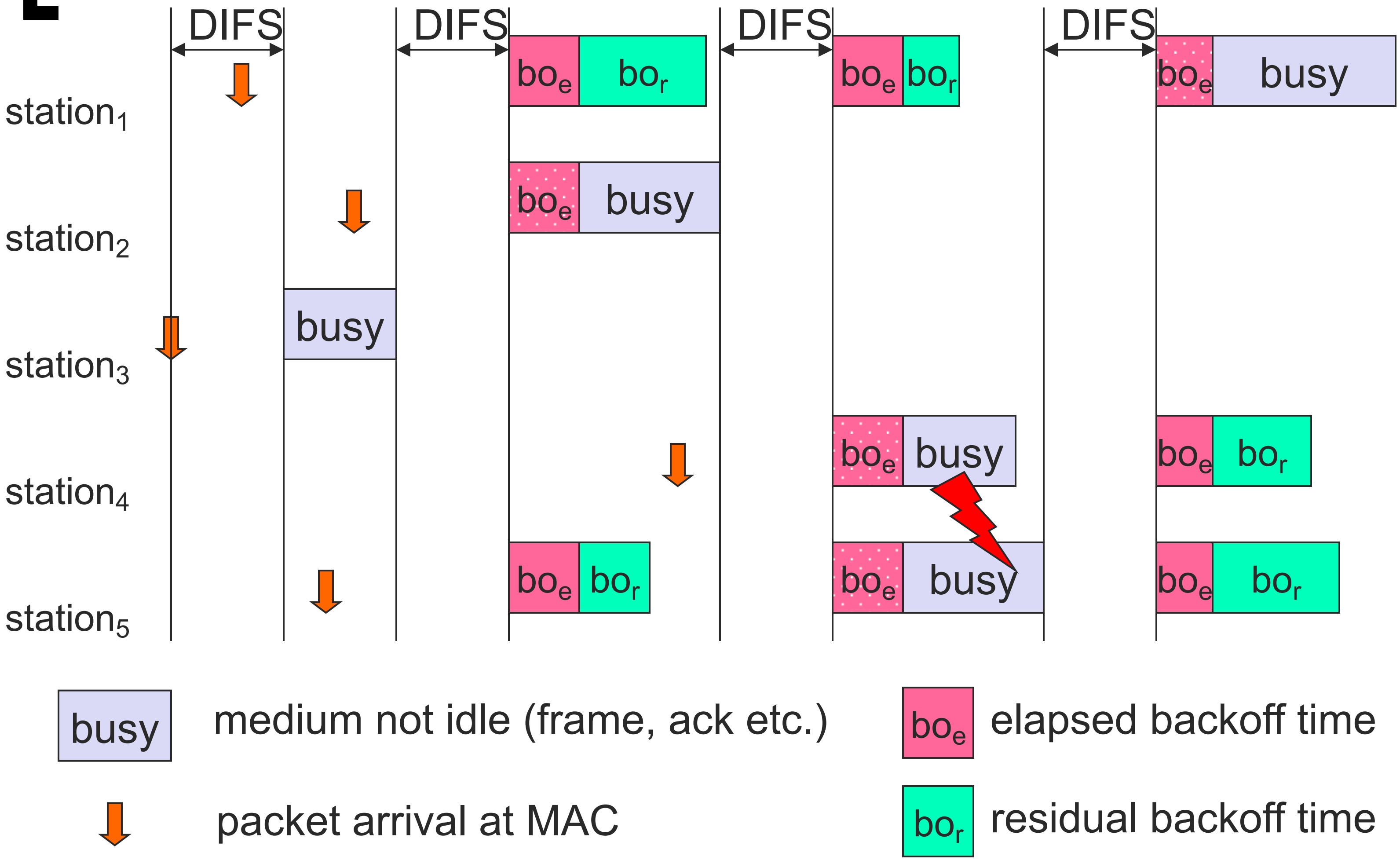
© CS/ECE 439 Staff, University of Illinois

Types of IFS

- PIFS
  - PCF interframe space
  - Minimum idle time for contention-free service (>SIFS, <DIFS)
- EIFS
  - Extended interframe space
  - Used when there is an error in transmission

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 - Competing Stations

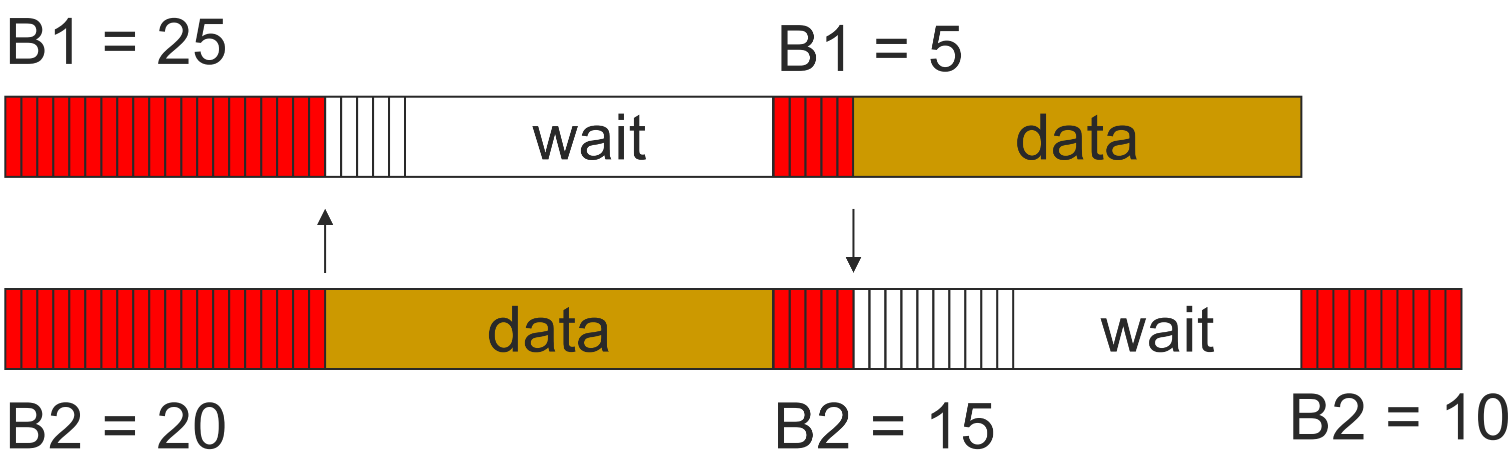


Backoff Interval

- When transmitting a packet, choose a backoff interval in the range [0,CW]
  - CW is contention window
- Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
- When backoff interval reaches 0, transmit RTS

© CS/ECE 439 Staff, University of Illinois

DCF Example



CW = 31

B1 and B2 are backoff intervals at nodes 1 and 2

© CS/ECE 439 Staff, University of Illinois

Backoff Interval

- The time spent counting down backoff intervals is a part of MAC overhead
- Large CW
  - Large backoff intervals
  - Can result in larger overhead
- Small CW
  - Larger number of collisions (when two nodes count down to 0 simultaneously)

© CS/ECE 439 Staff, University of Illinois

Backoff Interval

- The number of nodes attempting to transmit simultaneously may change with time
  - Some mechanism to manage contention is needed
- IEEE 802.11 DCF
  - Contention window CW is chosen dynamically depending on collision occurrence

© CS/ECE 439 Staff, University of Illinois

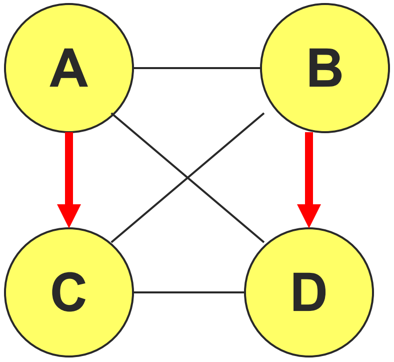
Binary Exponential Backoff in DCF

- When a node fails to receive CTS in response to its RTS, it increases the contention window
  - cw is doubled (up to an upper bound)
- When a node successfully completes a data transfer, it restores cw to CW_{min}
  - cw follows a sawtooth curve

© CS/ECE 439 Staff, University of Illinois

Fairness Issue

- Many definitions of fairness plausible
- Simplest definition
  - All nodes should receive equal bandwidth

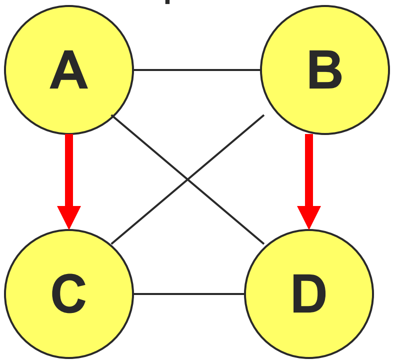


Two flows

© CS/ECE 439 Staff, University of Illinois

Fairness Issue

- Assume that initially, A and B both choose a backoff interval in range [0,31] but their RTSs collide
- Nodes A and B then choose from range [0,63]
  - Node A chooses 4 slots and B choose 60 slots
  - After A transmits a packet, it next chooses from range [0,31]
  - It is possible that A may transmit several packets before B transmits its first packet



Two flows

© CS/ECE 439 Staff, University of Illinois

Fairness Issue

- Unfairness occurs when one node has backed off much more than some other node
- MACAW Solution
  - When a node transmits a packet
    - Append the cw value to the packet
    - all nodes hearing that CW value use it for their future transmission attempts

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 Amendments

- IEEE 802.11-1997:
  - Originally 1 Mbit/s and 2 Mbit/s
  - 2.4 GHz RF and infrared (IR)
- IEEE 802.11a:
  - 54 Mbit/s, 5 GHz standard (2001)
- IEEE 802.11b:
  - Enhancements to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c:
  - Bridge operation procedures;
  - Included in the IEEE 802.1D standard (2001)
- IEEE 802.11d:
  - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e:
  - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11g:
  - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h:
  - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i:
  - Enhanced security (2004)
- IEEE 802.11j:
  - Extensions for Japan (2004)
- IEEE 802.11-2007:
  - Updated standard including a, b, d, e, g, h, i and j. (2007)

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 Amendments

- IEEE 802.11k:
  - Radio resource measurement enhancements (2008)
- IEEE 802.11n:
  - Higher throughput improvements using MIMO (multiple input, multiple output antennas) (September 2009)
- IEEE 802.11p:
  - WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (2010)
- IEEE 802.11r:
  - Fast BSS transition (FT) (2008)
- IEEE 802.11s:
  - Mesh Networking, Extended Service Set (ESS) (2011)
- IEEE 802.11u:
  - Improvements related to HotSpots and 3rd party authorization of clients, e.g. cellular network offload (2011)
- IEEE 802.11v:
  - Wireless network management (2011)
- IEEE 802.11w:
  - Protected Management Frames (2009)
- IEEE 802.11y:
  - 3650–3700 MHz Operation in the U.S. (2008)
- IEEE 802.11z:
  - Extensions to Direct Link Setup (DLS) (2010)

© CS/ECE 439 Staff, University of Illinois

IEEE 802.11 Amendments

- IEEE 802.11-2012:
  - New release including k, n, p, r, s, u, v, w, y and z (2012)
- IEEE 802.11aa:
  - Robust streaming of Audio Video Transport Streams (2012)
- IEEE 802.11ac:
  - Very High Throughput < 6GHz
  - Potential improvements over 802.11n: better modulation scheme (expected ~10% throughput increase), wider channels (estimate in future time 80 to 160 MHz), multi user MIMO (2012)
- IEEE 802.11ad:
  - Very High Throughput 60 GHz (~ February 2014)
  - IEEE 802.11ae:
  - Prioritization of Management Frames (2012)
- IEEE 802.11af:
  - TV Whitespace (February 2014)

© CS/ECE 439 Staff, University of Illinois

In process amendments

- IEEE 802.11ah:
  - Sub 1 GHz sensor network, smart metering. (~March 2016)
- IEEE 802.11ai:
  - Fast Initial Link Setup (~November 2015)
- IEEE 802.11aj:
  - China Millimeter Wave (~June 2016)
- IEEE 802.11aq:
  - Pre-association Discovery (~July 2016)
- IEEE 802.11ak:
  - General Links (~ May 2016)
- IEEE 802.11mc:
  - Maintenance of the standard (~ March 2016)
- IEEE 802.11ax:
  - High Efficiency WLAN (~ May 2018)
- IEEE 802.11ay:
  - Enhancements for Ultra High Throughput in and around the 60 GHz Band (~ TBD)
- IEEE 802.11az:
  - Next Generation Positioning (~ TBD)

© CS/ECE 439 Staff, University of Illinois

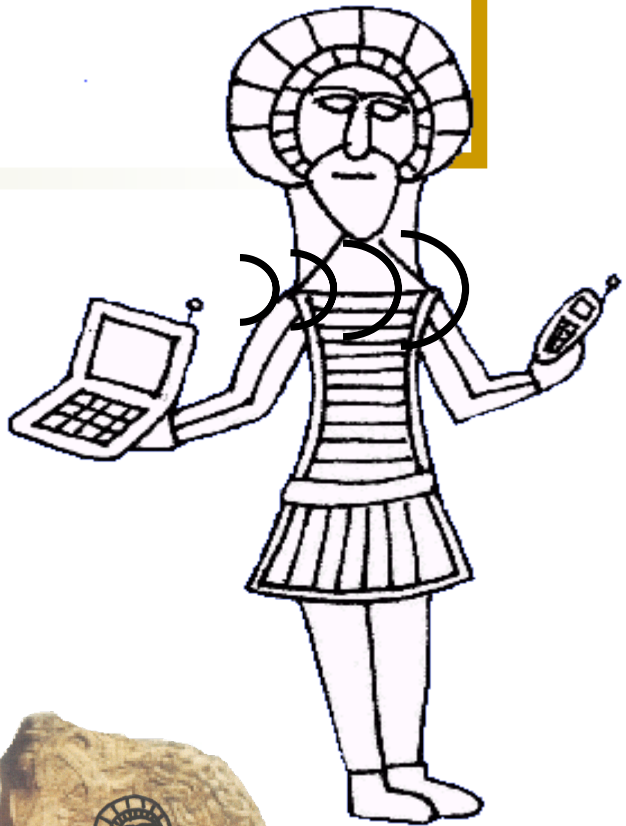
Other Technologies

- IEEE 802.15 Wireless PAN
- IEEE 802.15.1
  - Bluetooth certification
- IEEE 802.15.2
  - IEEE 802.15 and IEEE 802.11 coexistence
- IEEE 802.15.3
  - High-Rate wireless PAN (e.g., UWB, etc)
- IEEE 802.15.4
  - Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)
- IEEE 802.15.5
  - Mesh networking for WPAN
- IEEE 802.15.6
  - Body area network
- IEEE 802.16
  - Broadband Wireless Access (WiMAX certification)

© CS/ECE 439 Staff, University of Illinois

Bluetooth

- Harald Blaatand “Bluetooth” II
  - King of Denmark 940-981 AC
- Runic stones in his capital city of Jelling
  - The stone’s inscription (“runes”) says:
    - Harald Christianized the Danes
    - Harald controlled the Danes
    - Harald believes that devices shall seamlessly communicate [wirelessly]



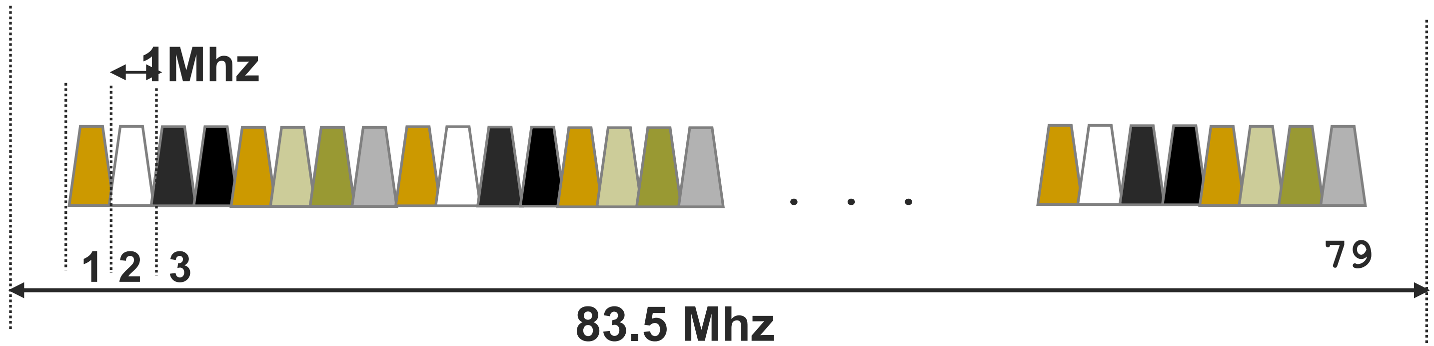
© CS/ECE 439 Staff, University of Illinois

Classic Bluetooth

- Cable replacement
  - 2.4 GHz
  - FHSS over 79 channels (of 1MHz each), 1600hops/s
  - 1Mbps
  - Coexistence of multiple piconets
  - 10 meters (extendible to 100 meters)

© CS/ECE 439 Staff, University of Illinois

Bluetooth Radio

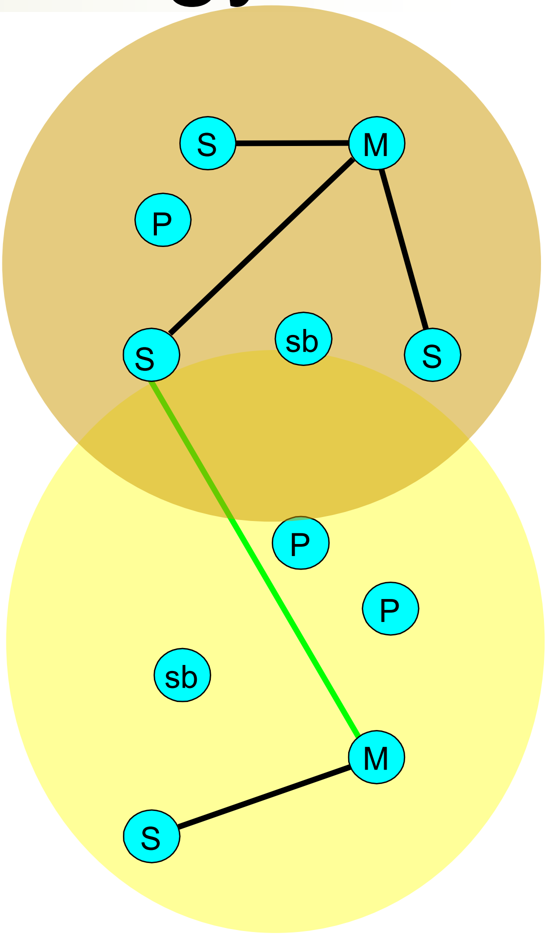


- MA scheme: Frequency hopping spread spectrum.
  - 2.402 GHz + k MHz, k=0, …, 78
  - 1,600 hops per second.
  - 1 Mb/s data rate.

© CS/ECE 439 Staff, University of Illinois

Bluetooth Network Topology

- Radio designation
  - Connected radios can be master or slave
  - Radios are symmetric (same radio can be master or slave)
- Piconet
  - Master can connect to 7 simultaneous or 200+ inactive (parked) slaves per piconet
  - Each piconet has maximum capacity (1 Mbps)
  - Unique hopping pattern/ID
- Scatternet
  - High capacity system
  - Minimal impact with up to 10 piconets within range
  - Radios can share piconets!



© CS/ECE 439 Staff, University of Illinois

Bluetooth – Contention-free MAC

- Master performs medium access control
  - Schedules traffic through polling.
- Time slots alternate between master and slave transmission
  - Master-slave
    - Master includes slave address.
  - Slave-master
    - Only slave chosen by master in previous master-slave slot allowed to transmit.
  - If master has data to send to a slave, slave polled implicitly; otherwise, explicit poll.

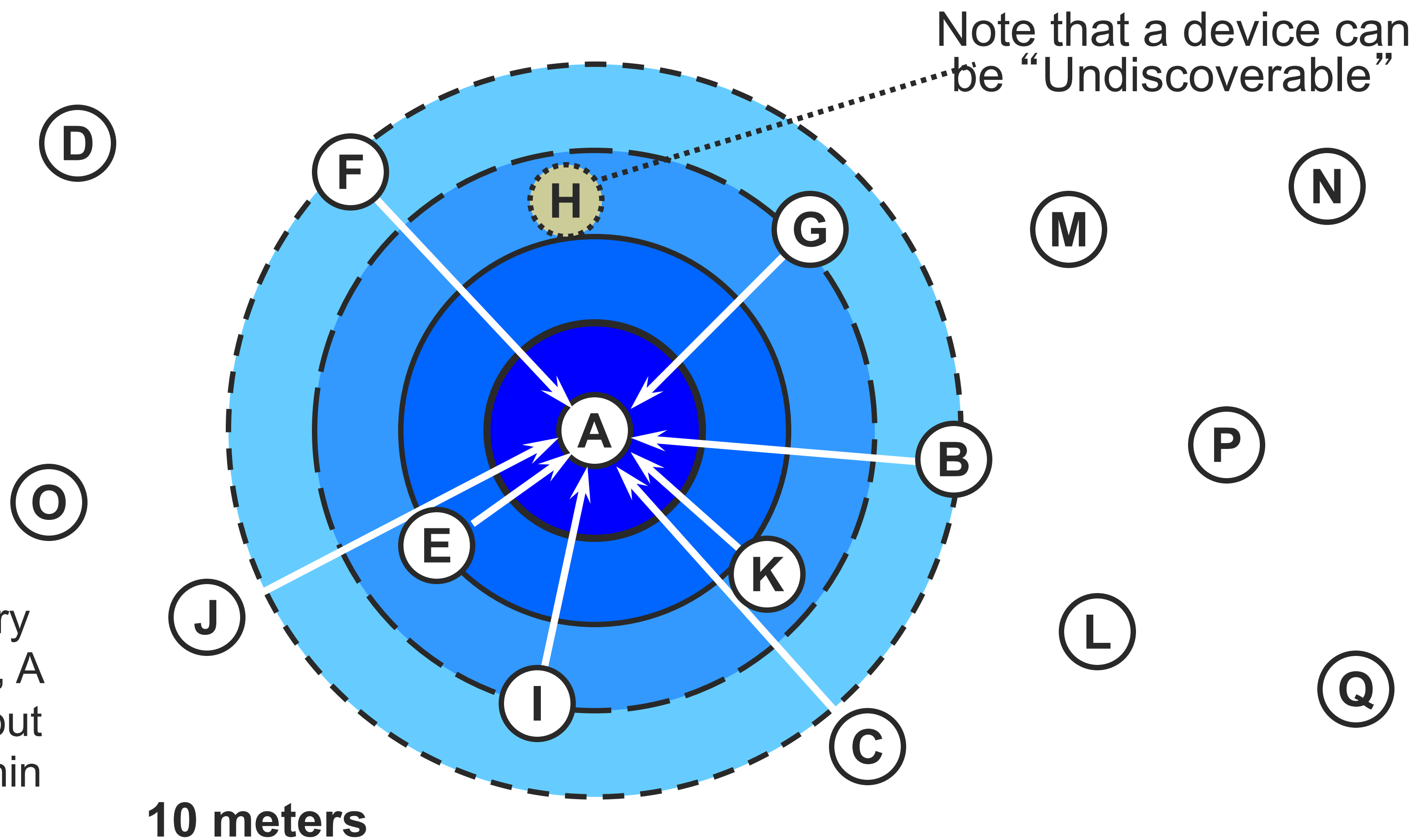
© CS/ECE 439 Staff, University of Illinois

Bluetooth Device Discovery - Inquiry

- Device discovery
  - Sends out an inquire, which is a request for nearby devices (within 10 meters)
  - Devices that allow themselves to be discoverable issue an inquiry response
  - Listeners respond with their address
  - Can take up to 10.24 seconds, after which the inquiring device should know everyone within 10 meters of itself

© CS/ECE 439 Staff, University of Illinois

Bluetooth Device Discovery - Inquiry



After inquiry procedure, A knows about others within range

© CS/ECE 439 Staff, University of Illinois

Bluetooth Inquiry

- Sender
  - Inquiry sent on 16 different frequencies
  - 16 channel train
    - about 1.28 seconds per channel
    - One full 16 channel train takes 10ms
- Receiver (device in standby mode)
  - Scans long enough for an inquiring device to send the inquiry on 16 frequencies
  - Scan must be frequent enough to guaranteed wake up during a 16 channel train
    - Enters inquiry scan state at least once every 1.28 seconds, and stays in that state for 10ms

© CS/ECE 439 Staff, University of Illinois

Bluetooth Inquiry - Reliability

- Challenge
  - Noisy channels
  - Lost packets
    - Train scan is repeated up to 4 times for each train (10.24 seconds)
    - Designed to successfully communicate at least once with all devices within range

© CS/ECE 439 Staff, University of Illinois

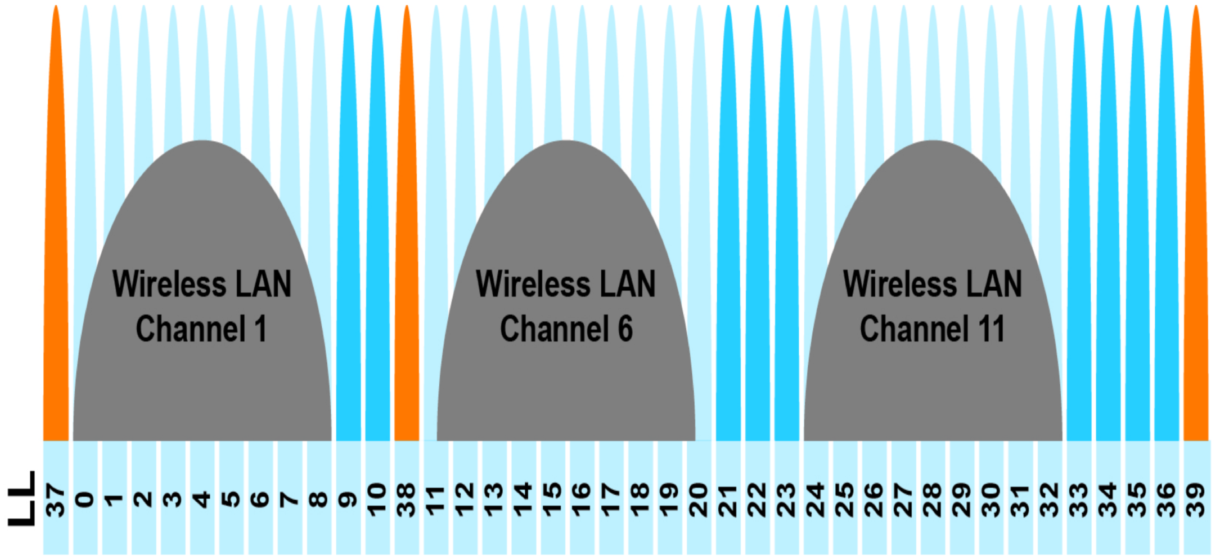
BLE Highlights

- Shared wireless channel
  - BLE operates in the 2.4 GHz ISM band with Wi-Fi and other technologies (phones, microwave ovens …)
- BLE = Bluetooth Low Energy
  - Improved discovery
  - Key component: Beacons
    - Tags send out advertising beacons (typ. dist 30ft)
    - Phones scan for beacons

© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Channel Use and Coexistence with Wi-Fi

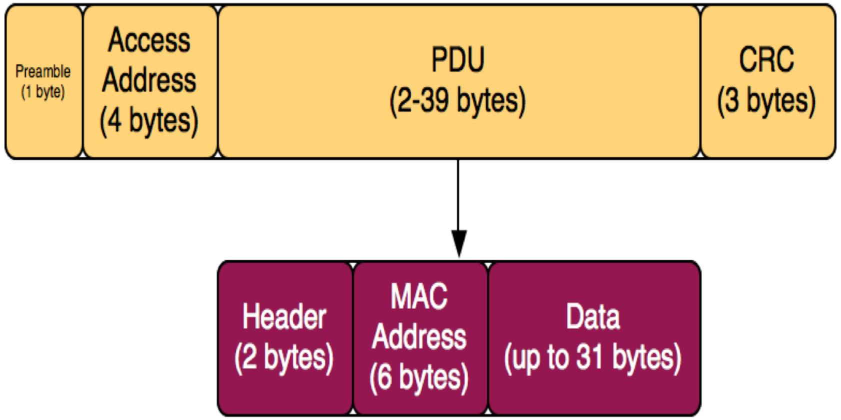
- Separate advertising and connected channels
  - Key: Three disjoint advertising channels (37, 38, 39)
  - Positioned between Wi-Fi channels (1, 6, 11)



© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Advertising

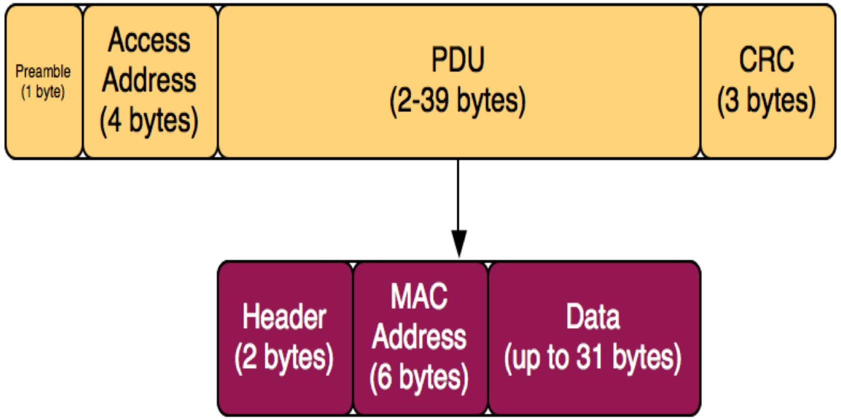
- Advertising Tags
- Advertising Messages
  - Header + MAC Address + up to 31 Bytes of data
    - ~200 - 400 usec per packet
  - Two types: Non-scannable, Scannable

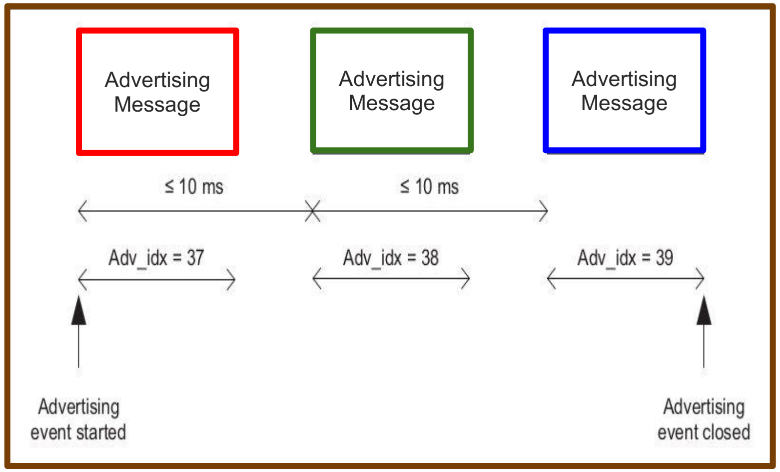


© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Advertising

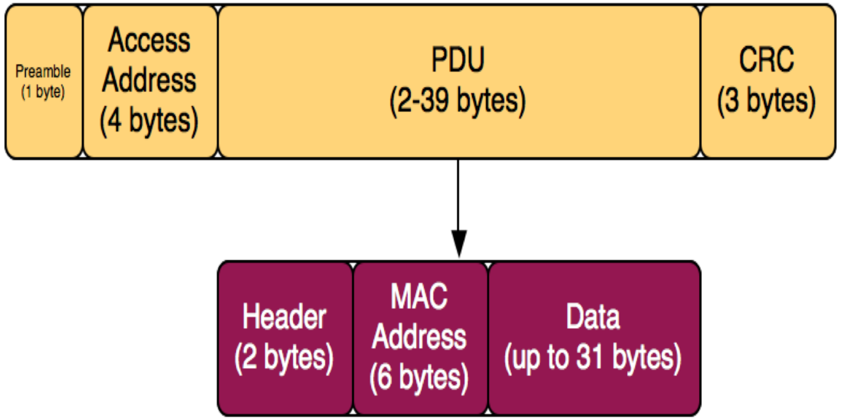
- Advertising Tags
- Advertising Messages
  - Header + MAC Address + up to 31 Bytes of data
    - ~200 - 400 usec per packet
  - Two types: Non-scannable, Scannable
- Advertising Event
  - One advertising message sent out on each advertising channel (37, 38, 39)



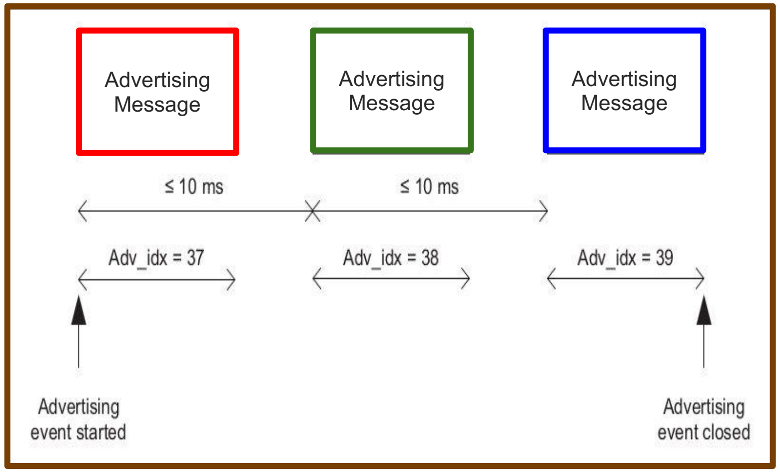


© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Advertising



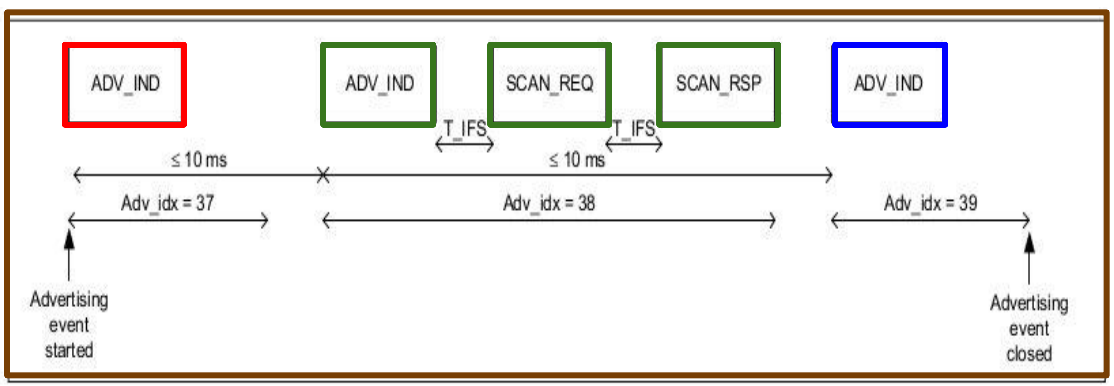
- Advertising Tags
- Advertising Messages
  - Header + MAC Address + up to 31 Bytes of data
    - ~200 - 400 usec per packet
  - Two types: Non-scannable, Scannable
- Advertising Event
  - One advertising message sent out on each advertising channel (37, 38, 39)
- Advertising Interval
  - One advertising event per advertising interval, e.g., every 1 sec or 100 msec

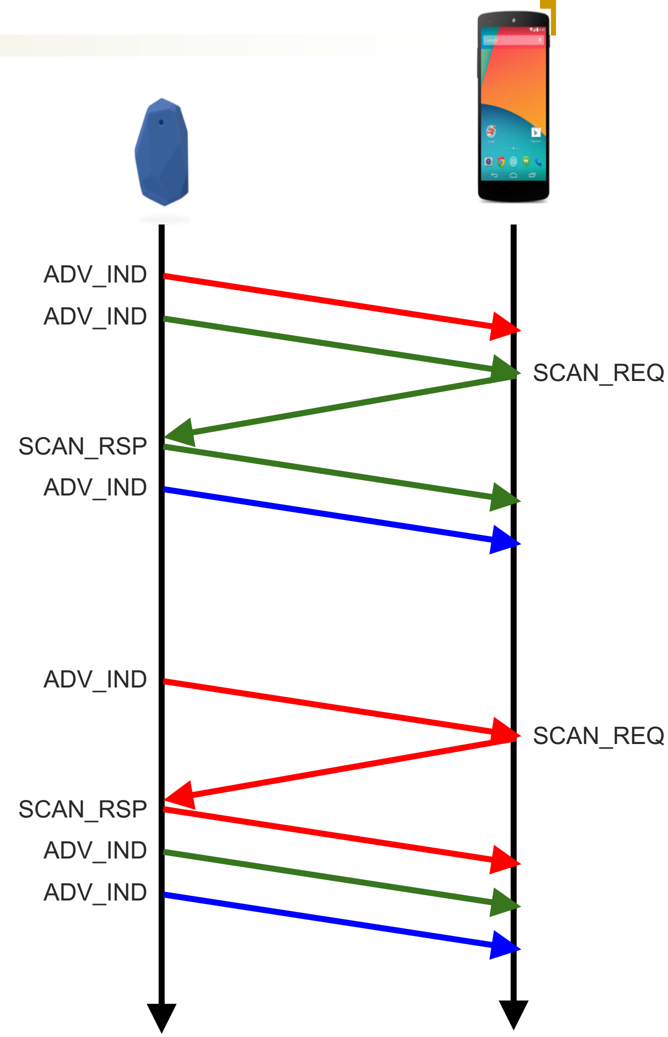


© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Tags Types - Scannable

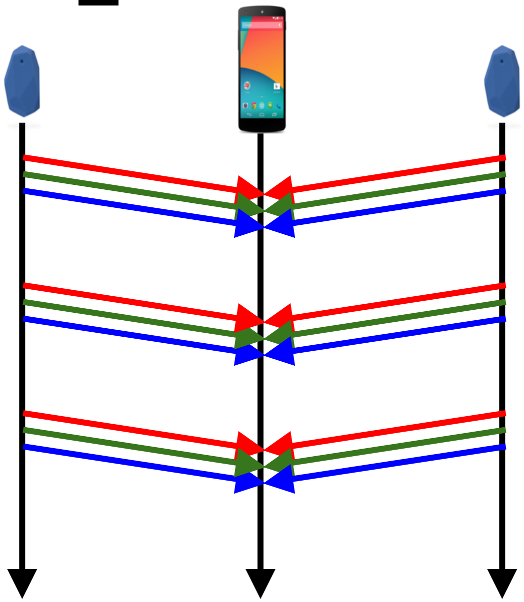
- Scannable Tags
  - Tags send ADV_IND messages
  - Scanners respond with SCAN_REQ message
  - Tags respond with SCAN_RSP message
    - Up to 31 Bytes of extra data
  - Tags wait ~150 usec for a request after beacon





© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Advertising and Collisions

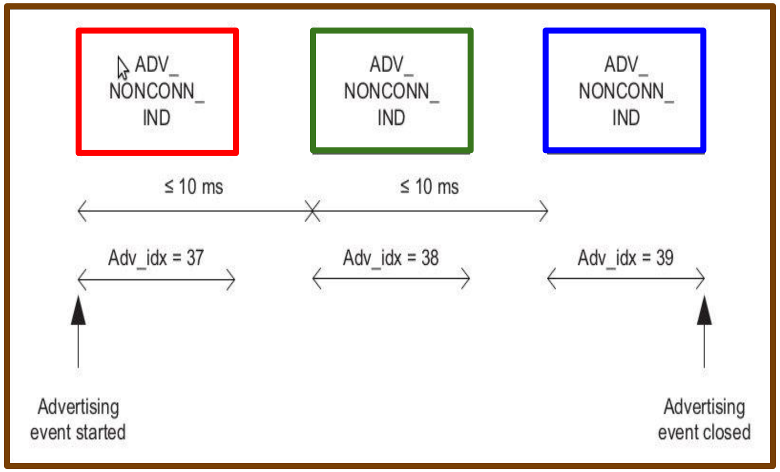


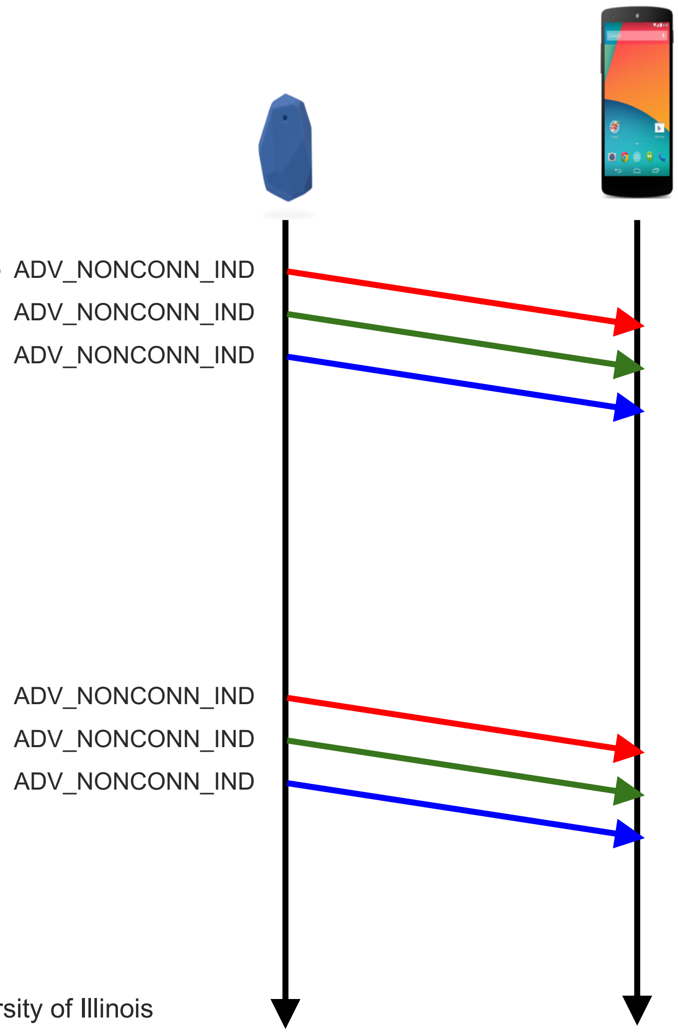
- If tags get synchronized, all advertising messages will collide

© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Tags Types - Non-Scannable

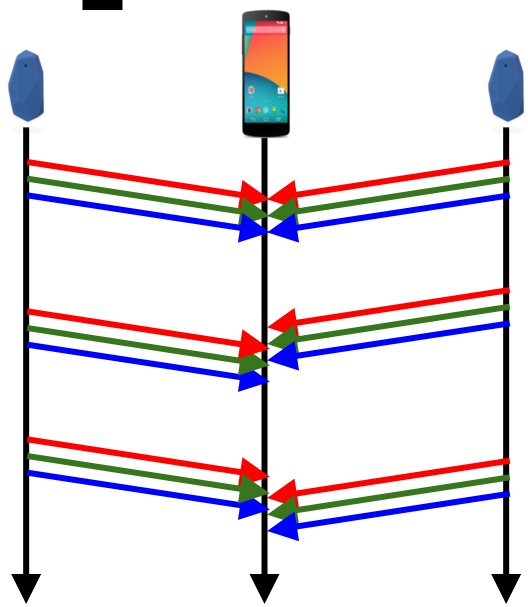
- Non-Scannable Tags
- Ex. gBeacon v3, iBeacon (?)
- Tags send ADV_NONCONN_IND messages
- Typically sent back-to-back
- Scanners listen, but do not respond

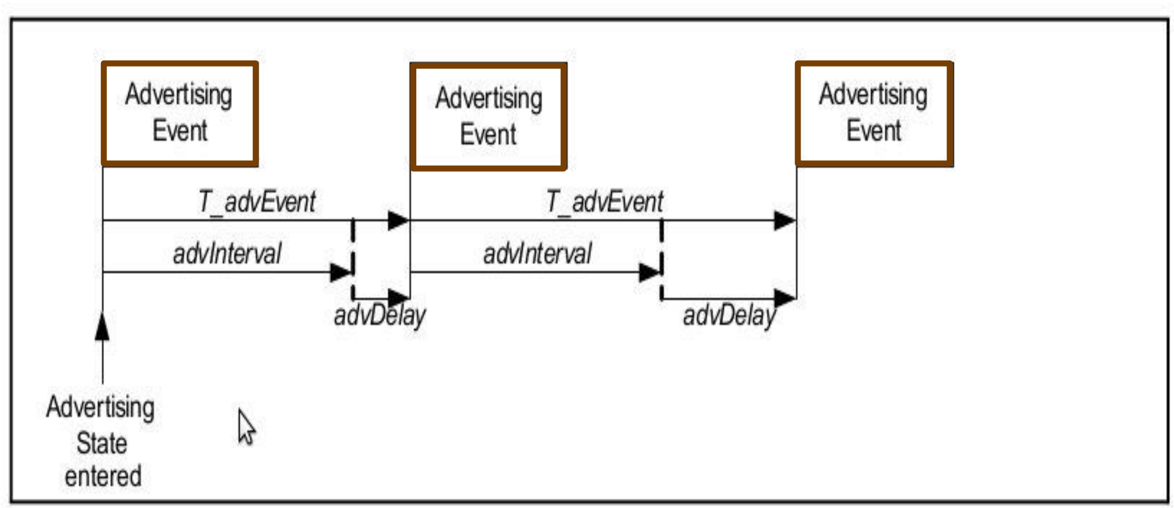




© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Advertising and Collisions



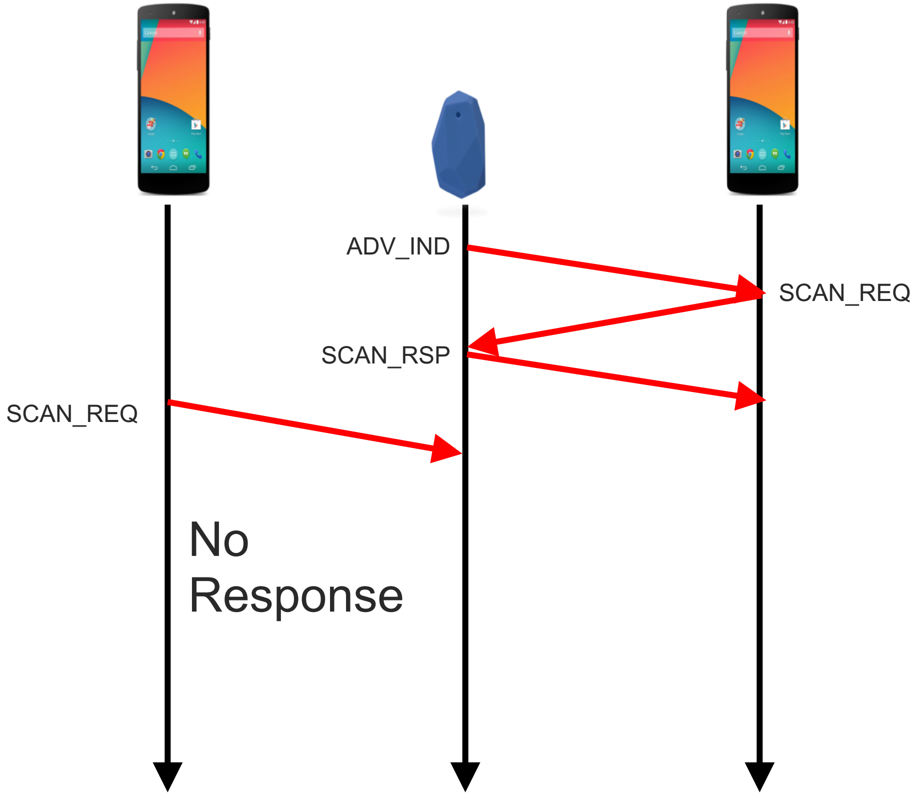


- Collision avoidance
  - Jitter advertising times
  - advDelay is added on to the end of each advertising event
  - advDelay = rand [0,10ms]

© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Scannable Tags

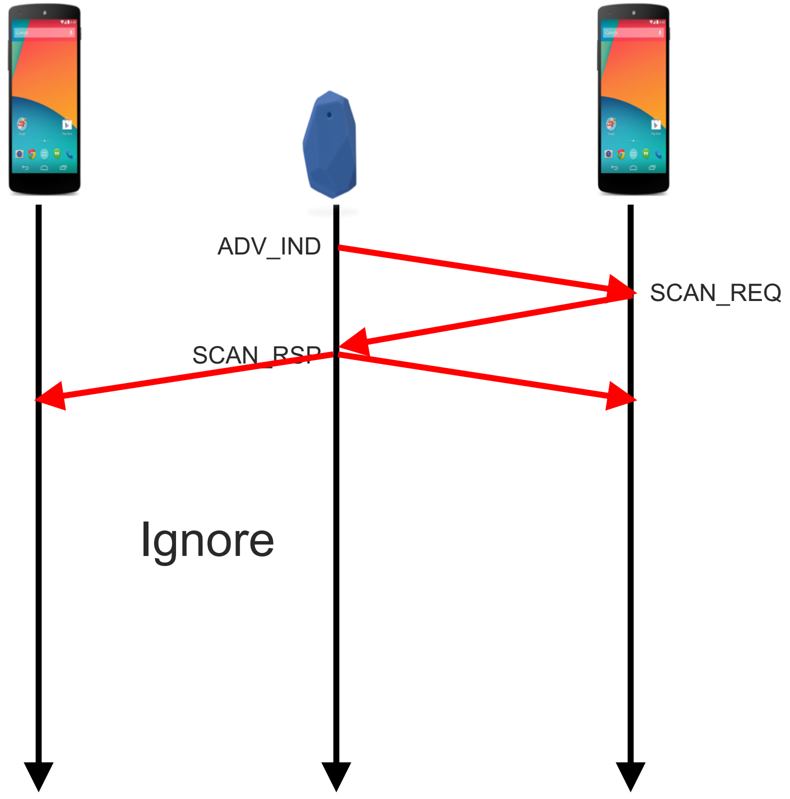
- One SCAN_RSP per channel per advertising event



© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Scannable Tags

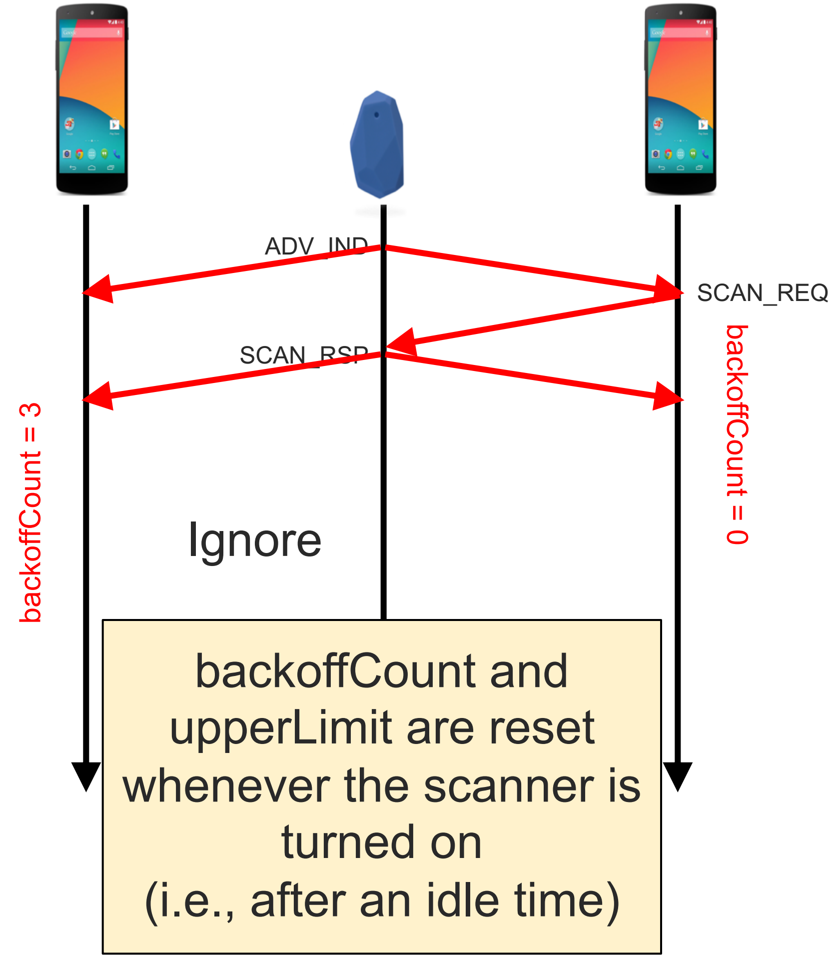
- ONLY accept SCAN_RSP if SCAN_REQ was sent to that tag on that channel during that advertising event
- Some collision tolerance
  - Any requesting scanner can receive a SCAN_RSP as long as one SCAN_REQ is received and the tag responds
  - BUT, No SCAN_RSP if all SCAN_REQs collide



© CS/ECE 439 Staff, University of Illinois

BLE Highlights: SCAN_REQ Collision Avoidance

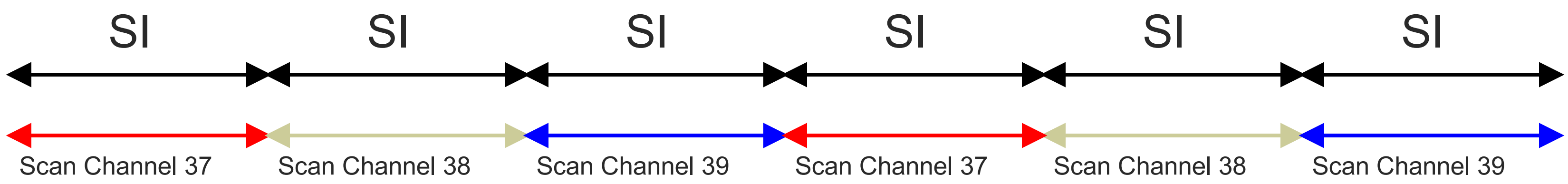
- Scanner backoff procedure
  - Two parameters
    - backoffCount, upperLimit
  - On starting scan
    - upperLimit = 1, backoffCount = 1
  - Decrement backoffCount on receipt of ADV message
    - Only send SCAN_REQ if backoffCount == 0
  - Adapt upperLimit based on success or failure of receipt of SCAN_RSP
    - Reset backoffCount
    - backoffCount = rand (1, upperLimit)



© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Low-level Scanning

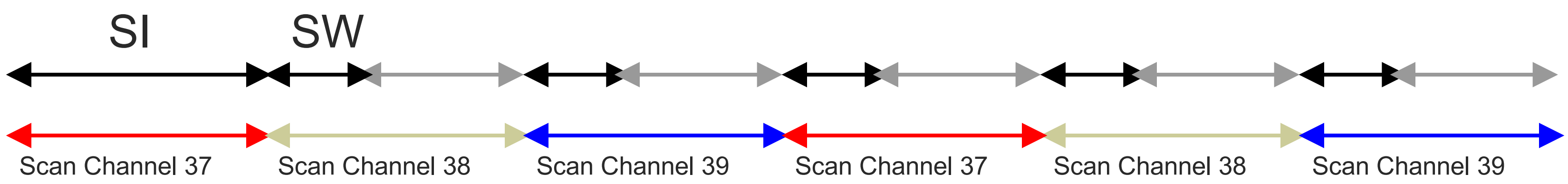
- Scanners
- Scan for tags on sequential channels (37, 38, 39)
- Scan Interval (SI)
  - Time spent on a channel



© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Low-level Scanning

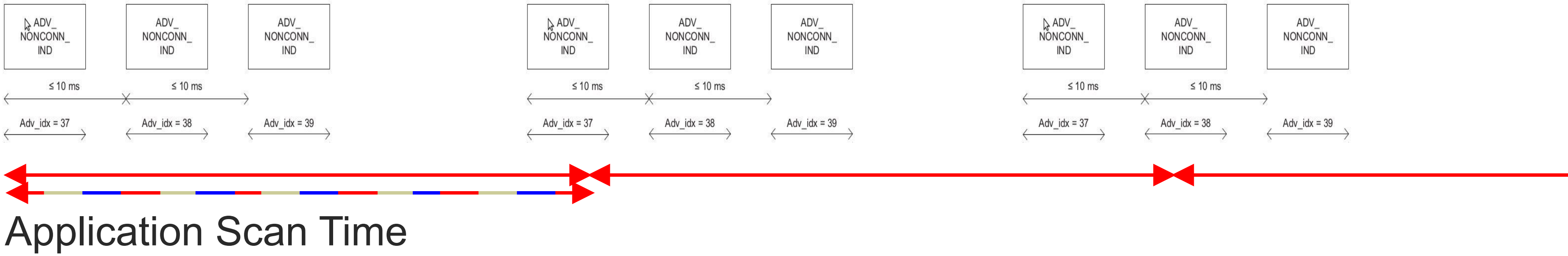
- Scan Time
  - Scan Int == Scan Window ⇒ Always on
- Scanners
- Scan for tags on sequential channels (37, 38, 39)
- Scan Interval (SI)
  - Time spent on a channel
- Scan Window (SW)
  - Time spent scanning at beginning of Scan Interval



© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Application-level Scanning

- Scanners
- Application Scan Time
  - > Tag Advertising Interval

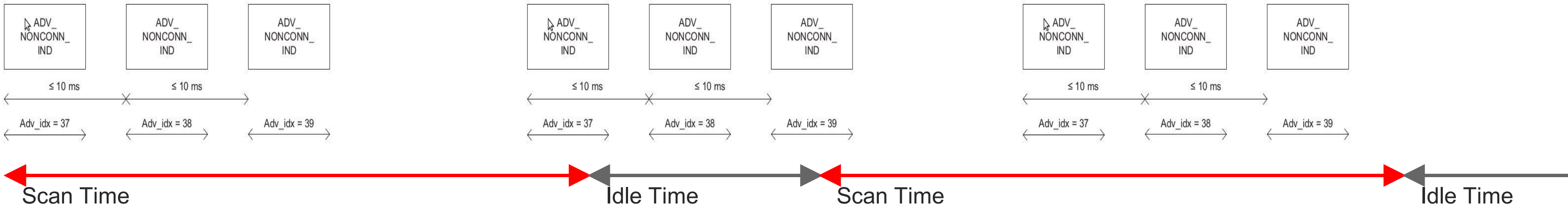


© CS/ECE 439 Staff, University of Illinois

BLE Highlights: Application-level Scanning

- Scan Time
  - 100% on Idle Time = 0
- (Continuous scanning)
  - 10% on Idle Time = 10 * Scan Time

- Scanners
- Application Scan Time
  - > Tag Advertising Interval
- Application Idle Time



© CS/ECE 439 Staff, University of Illinois

BLE Highlights: MAC Behavior

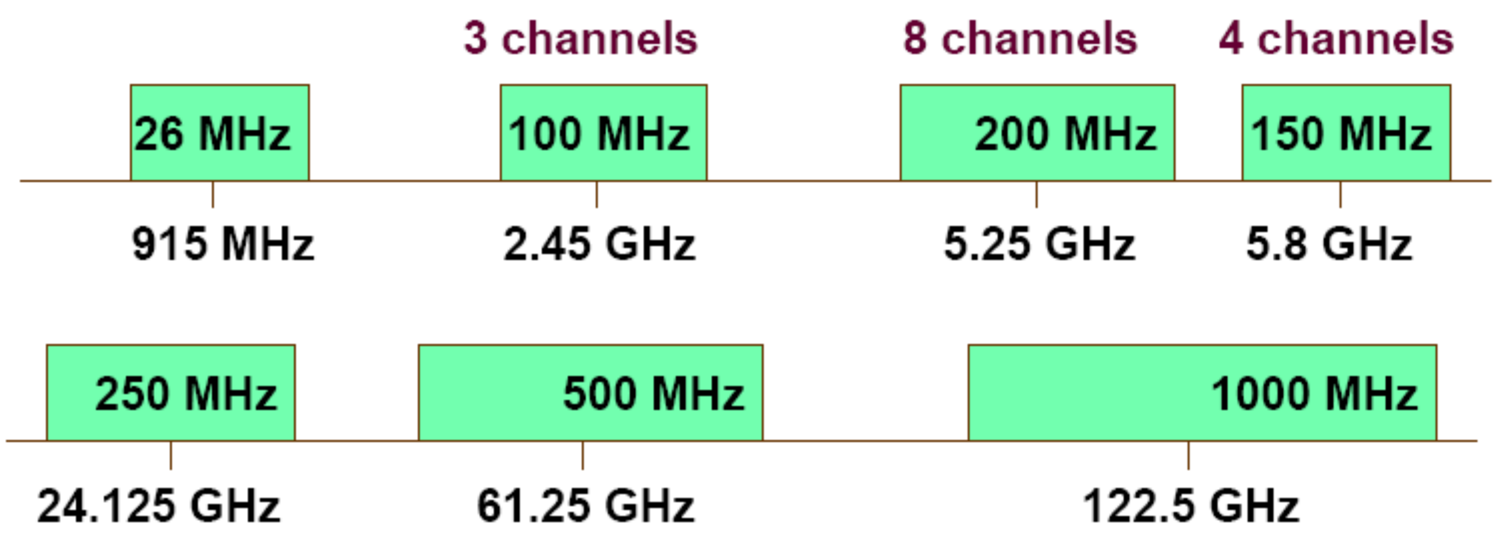
- No Carrier Sense
  - Tag does not listen for a clear channel before sending any message
- Minimal Contention Avoidance
  - Jitter length of advertising interval + rand [0, 10 ms]
  - Backoff for sending SCAN_REQ

- Other parameters
  - Inter-frame spacing 150us (from spec)
  - Channel switching delay 274us (from Nordic)
  - Scan Interval 11.25ms (from spec/Nexus 5)
  - Scan Window 11.25ms (continuous scanning)

© CS/ECE 439 Staff, University of Illinois

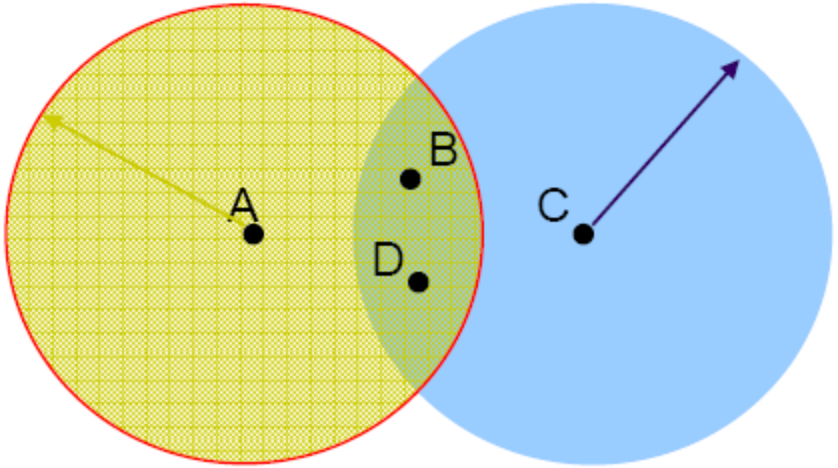
Channelization of spectrum

- Typically, available frequency spectrum is split into multiple channels
- Some channels may overlap



© CS/ECE 439 Staff, University of Illinois

Preventing Collisions Altogether



- Frequency Spectrum partitioned into several channels
  - Nodes within interference range can use separate channels
  - Now A can send to B while C sends to D without any interference!
  - Aggregate Network throughput doubles

© CS/ECE 439 Staff, University of Illinois

Using Multiple Channels

- 802.11: AP’s on different channels
  - Usually manually configured by administrator
  - Automatic Configuration may cause problems
- Most cards have only 1 transceiver
  - Not Full Duplex: Cannot send and receive at the same time
- Multichannel MAC Protocols
  - Automatically have nodes negotiate channels
    - Channel coordination amongst nodes is necessary
    - Introduces negotiation and channel-switching latency that reduce throughput

© CS/ECE 439 Staff, University of Illinois

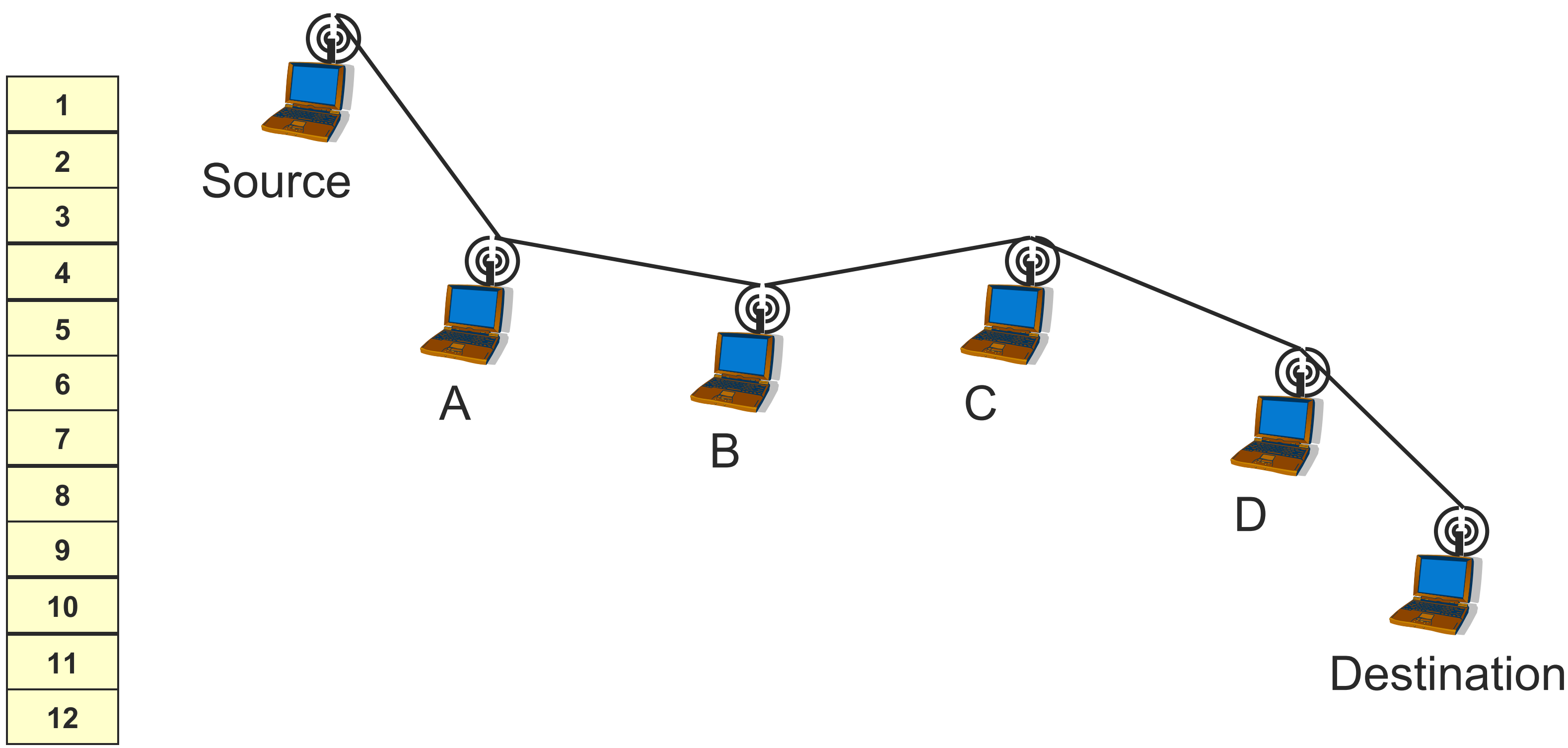
Wireless Multihop Networks

- Vehicular Networks
  - Delay Tolerant (batch) sending over several hops carry data to a base station
- Common in Sensor Network for periodically transmitting data
  - Infrastructure Monitoring
    - E.g., structural health monitoring of the Golden Gate Bridge
- Multihop networking for Internet connection sharing
  - Routing traffic over several hops to base station connected to Internet

© CS/ECE 439 Staff, University of Illinois

Multi-Hop Wireless Networks

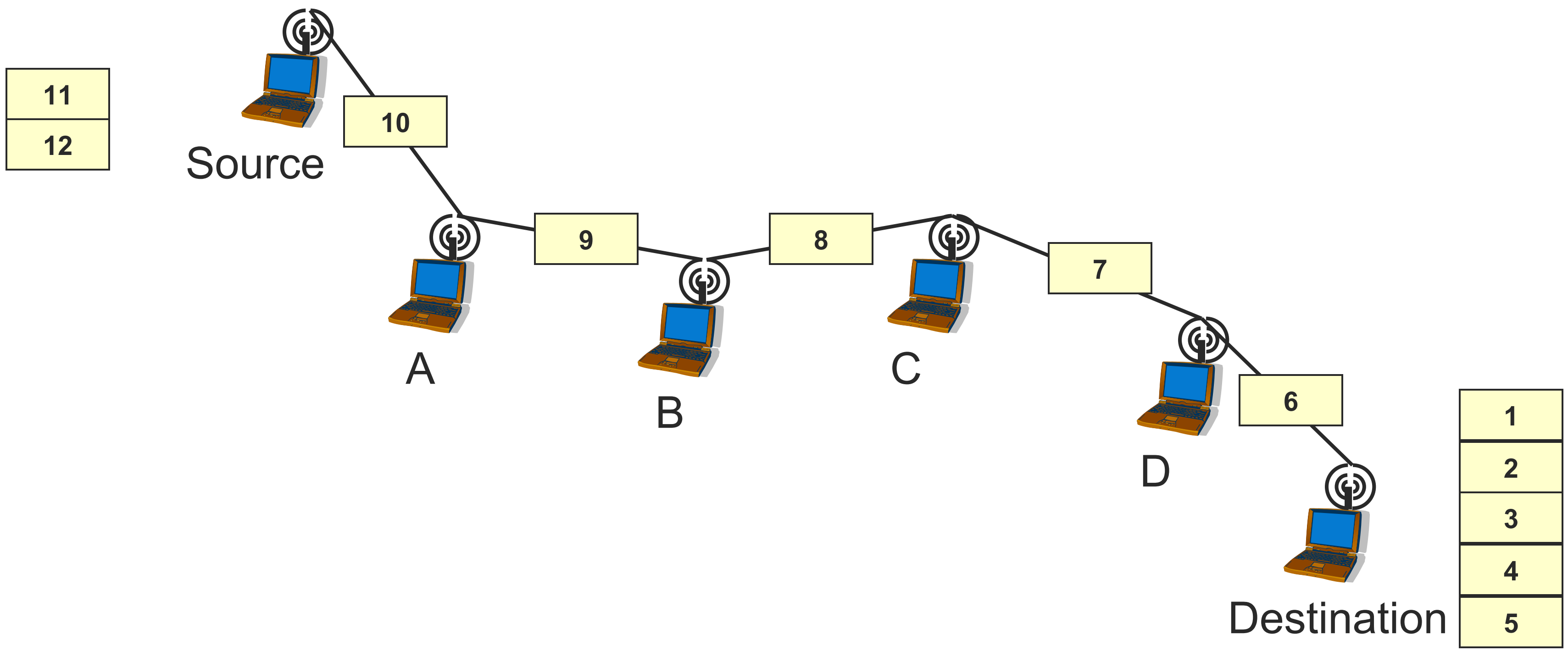
- In an ideal world …



© CS/ECE 439 Staff, University of Illinois

Multi-Hop Wireless Networks

- In an ideal world …

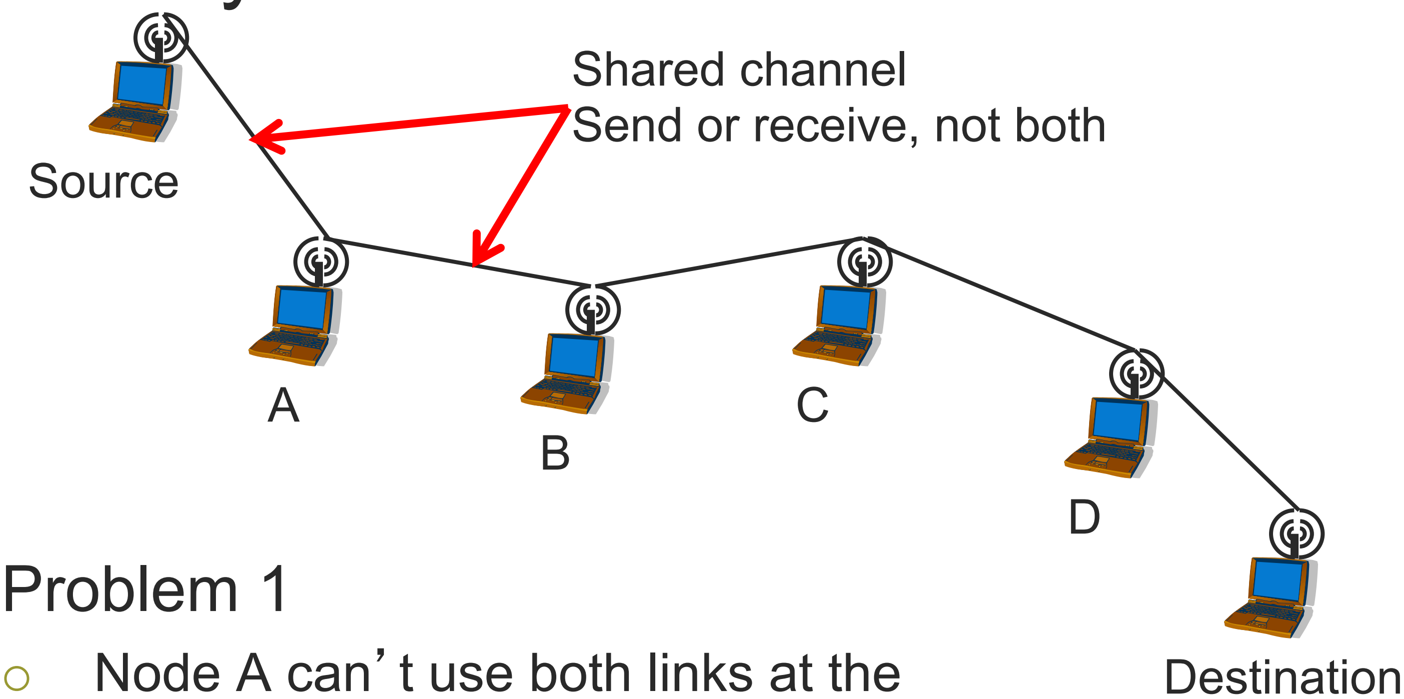


© CS/ECE 439 Staff, University of Illinois

Multi-Hop Wireless Networks

- Reality check …

1
2
3
4
5
6
7
8
9
10
11
12



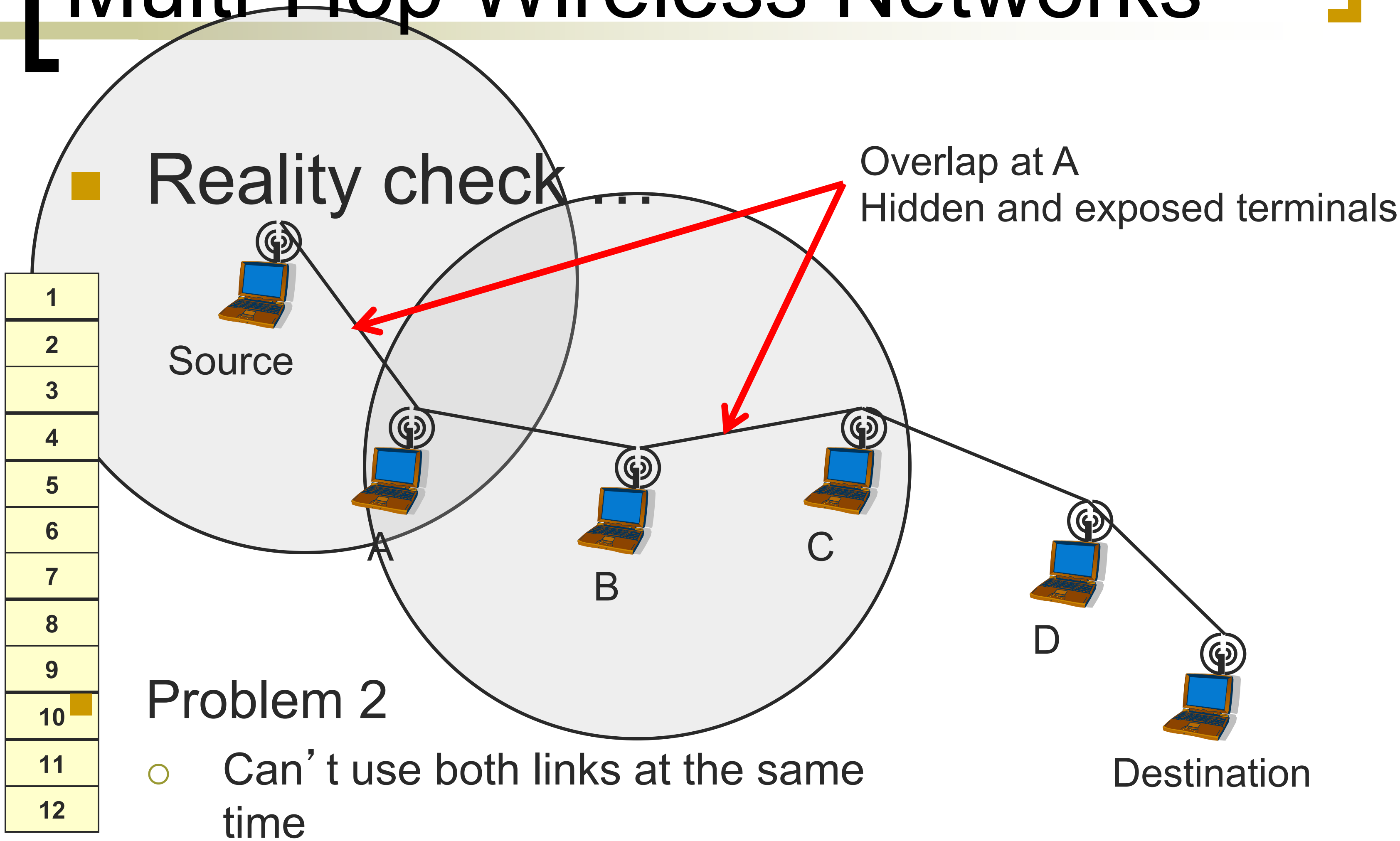
Problem 1

- Node A can't use both links at the same time

© CS/ECE 439 Staff, University of Illinois

Multi-Hop Wireless Networks

- Reality check …



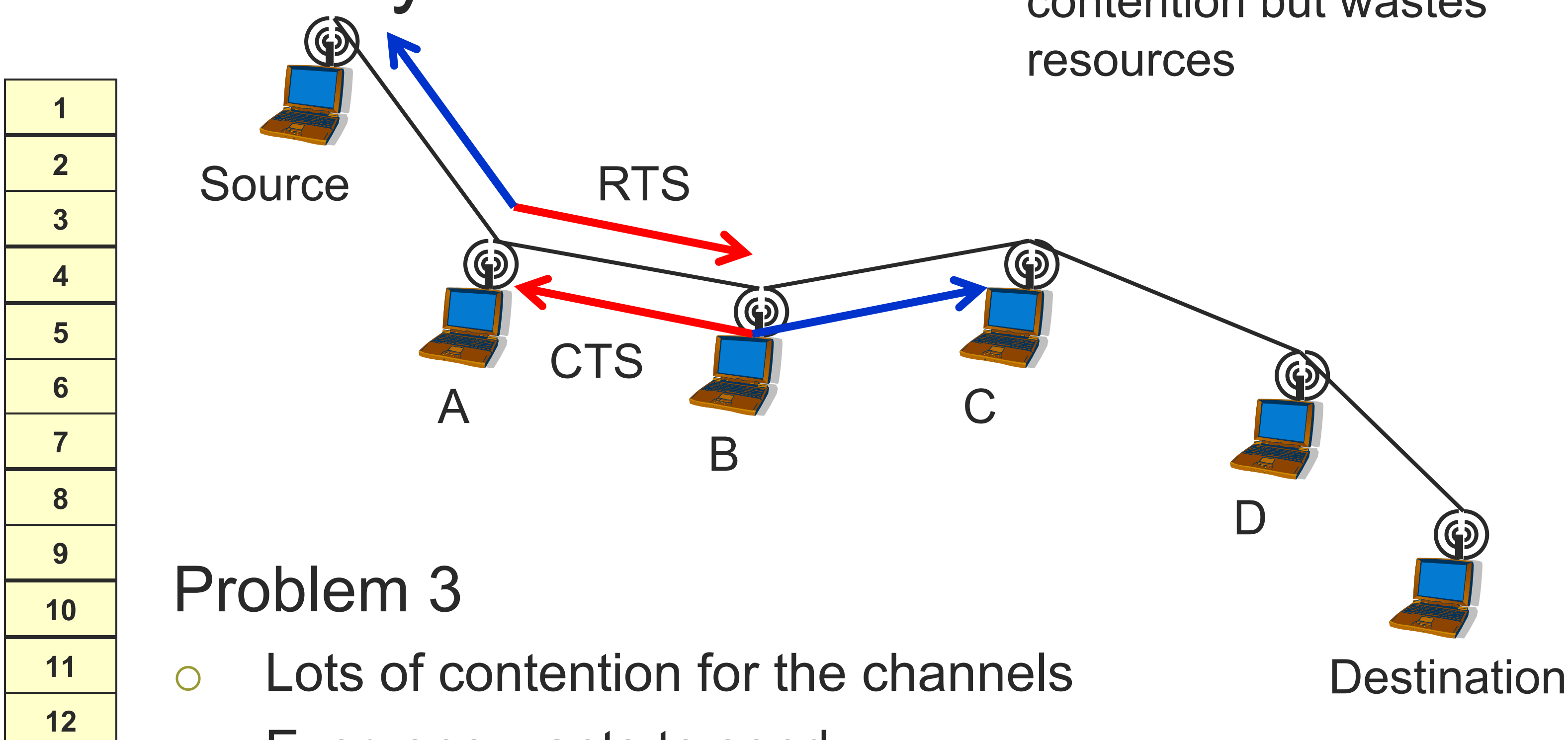
- Problem 2
  - Can't use both links at the same time

© CS/ECE 439 Staff, University of Illinois

Multi-Hop Wireless Networks

- Reality check …

RTS/CTS helps with contention but wastes resources



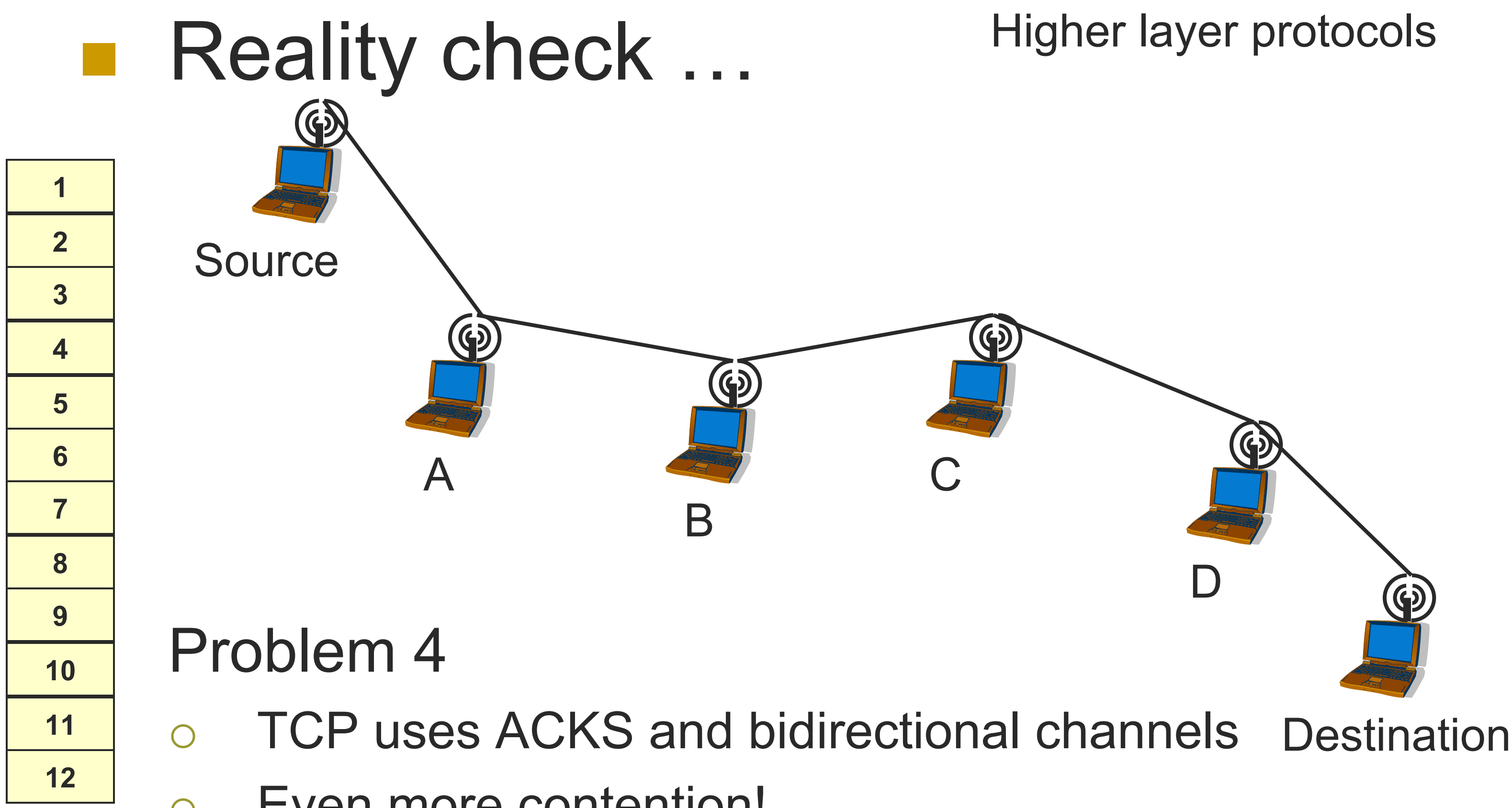
Problem 3

- Lots of contention for the channels
- Everyone wants to send

© CS/ECE 439 Staff, University of Illinois

Multi-Hop Wireless Networks

- Reality check …



Problem 4

- TCP uses ACKS and bidirectional channels
- Even more contention!

© CS/ECE 439 Staff, University of Illinois