

# Broadband Wireless Networks

*Benny Bing*

*School of ECE, Georgia Tech*

*Office: GCATT Room 270*

*Email: [benny@ece.gatech.edu](mailto:benny@ece.gatech.edu)*

*Phone/Fax: 404-385-0271*

*Homepage: <http://users.ece.gatech.edu/~benny>*

**Slides downloadable from**  
**[http://users.ece.gatech.edu/~benny/wireless\\_slides.pdf](http://users.ece.gatech.edu/~benny/wireless_slides.pdf)**

# Wireless Access Solution

- “Disruptive” technology capable of *pervasive* network access
  - Broadcast nature offers ubiquity and immediate access
  - Many phone companies are losing their landline business to wireless (just as they are losing business to VoIP)
- Quick, low-cost alternative to installing cable or leased lines
  - Allows long-distance carrier to bypass local service provider, thereby cutting down subscriber costs
- Allows fixed line operators to extend broadband networks
- Indispensable when wired interconnections are impractical
  - Rivers, rough terrain, private property, highways
- Reduce network config. complexity, dependence on gateways
- Eliminate overheads associated with moves, adds, changes
  - Removes labor, material, and equipment costs associated with cabling
  - Offers flexibility to reconfigure quickly or add more subscribers to network without much planning effort and cost of recabling (also increases reliability of network connectivity during catastrophic events)
  - Makes future expansion and growth inexpensive and easy

# Wireless Access Solution

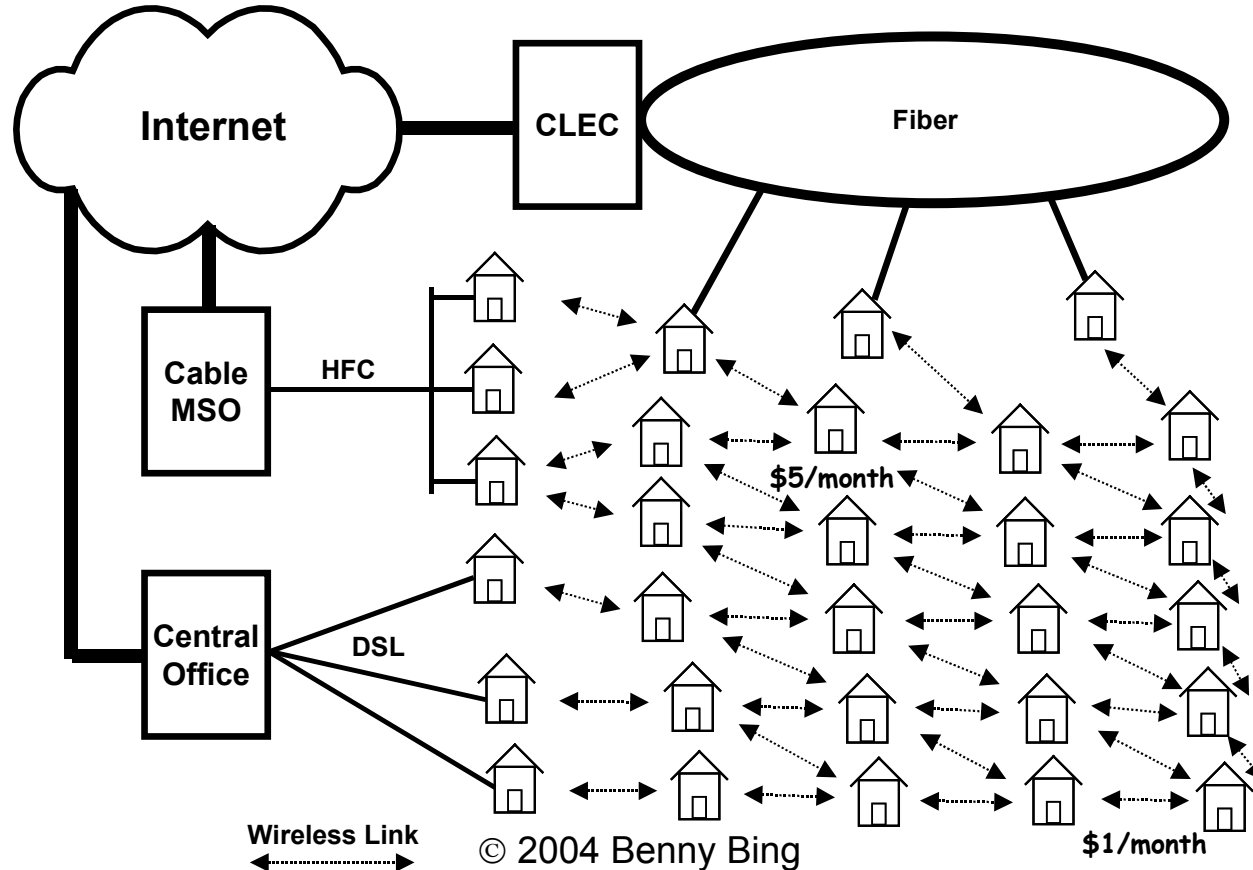
- Cannot compete with fiber in terms of bandwidth provisioning
  - Particularly with increasing operational range
- More prone to eavesdropping, security attacks, traffic analysis
- Performance fundamentally limited by signal interference among concurrent transmissions
  - A function of timing and spatial separation of transmissions
  - For wide coverage areas, a combination of wireless and wired infrastructure may still be required

# Emerging Wireless Technologies

- Have realized impressive efficiencies ( $\sim 10$  bits/s/Hz)
  - Unprecedented levels of individual and aggregate capacities in the order of Gbit/s wireless data rates
  - Compare current Wi-Fi or 802.11 technologies (0.5 bits/s/Hz for 802.11b, 2.7 bits/s/Hz for 802.11a/g)
- Radio spectrum getting increasingly deregulated
  - Can potentially lead to an abundance of bandwidth when spectrum is used (and reused) more efficiently and co-operatively
  - Capacity increase and efficiency are a direct result of being able to switch between different idle channels only for the period of usage
- Multihop (or mesh) and long-range wireless technologies have huge potential in enabling pervasive broadband access
  - Multihop wireless simplifies private network deployment for residential users
  - Long-range wireless can be an overlay complementing multihop technologies, OR can compete with local hotspots, 3G, and integrated cellphone/Wi-Fi for revenue

# Multihop Wireless Access

- Fixed wireless access point typically mounted on rooftop of subscriber's home
  - Creates a small wireless coverage area called a “hop”
  - Acts much like a router, automatically discovering neighboring access points and relaying packets across several wireless hops



# Advantages of Multihop Wireless

- Subscribers create local community networks on-demand
  - Allow residences to communicate directly with neighbors and enabling broadband applications between homes (e.g., neighborhood watchdog applications, medical/emergency response tasks, etc)
- Ownership of access network becomes decentralized
  - Provide degree of autonomy (just as network domains or autonomous systems do in the Internet today)
  - Lower subscriber costs through shared services/resources
  - KaZaA (a dominant online music swapping platform) has forced big recording labels to agree to offer music downloads for as little as \$1 a song
  - Need innovative approaches to digital rights management, which will ultimately help increase availability of high fidelity multimedia content
- Increased capacity, improved range performance
  - Lower transmit power (no need to transmit information all the way back to ultimate destination)
  - Results in a corresponding reduction in interference
  - Ability to reuse limited radio spectrum efficiently

# Disadvantages of Multihop Wireless

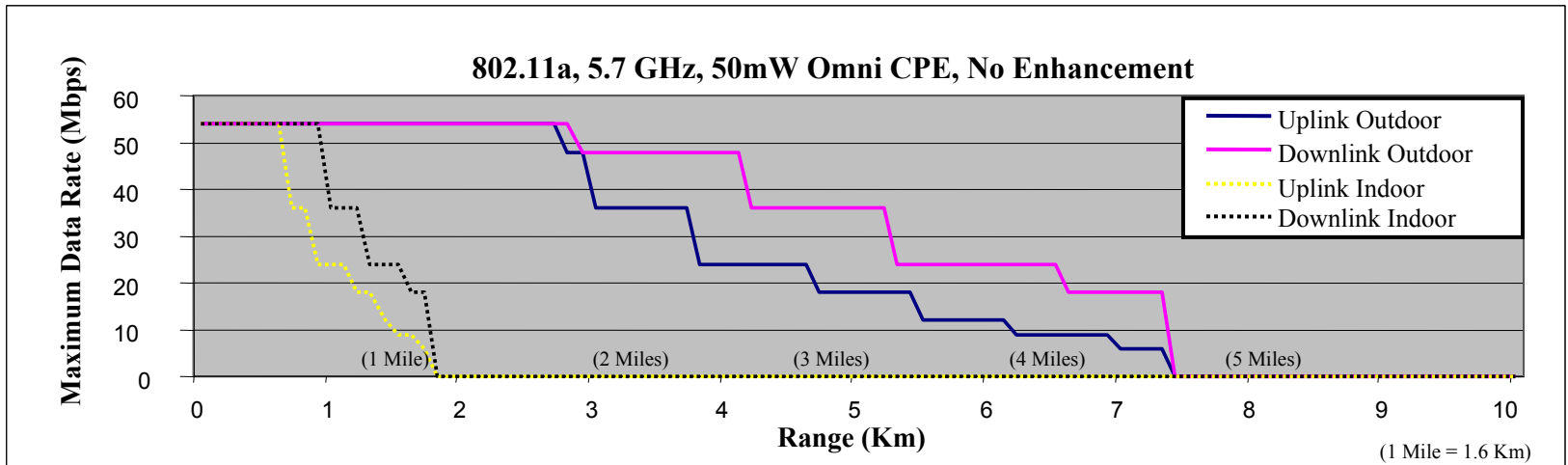
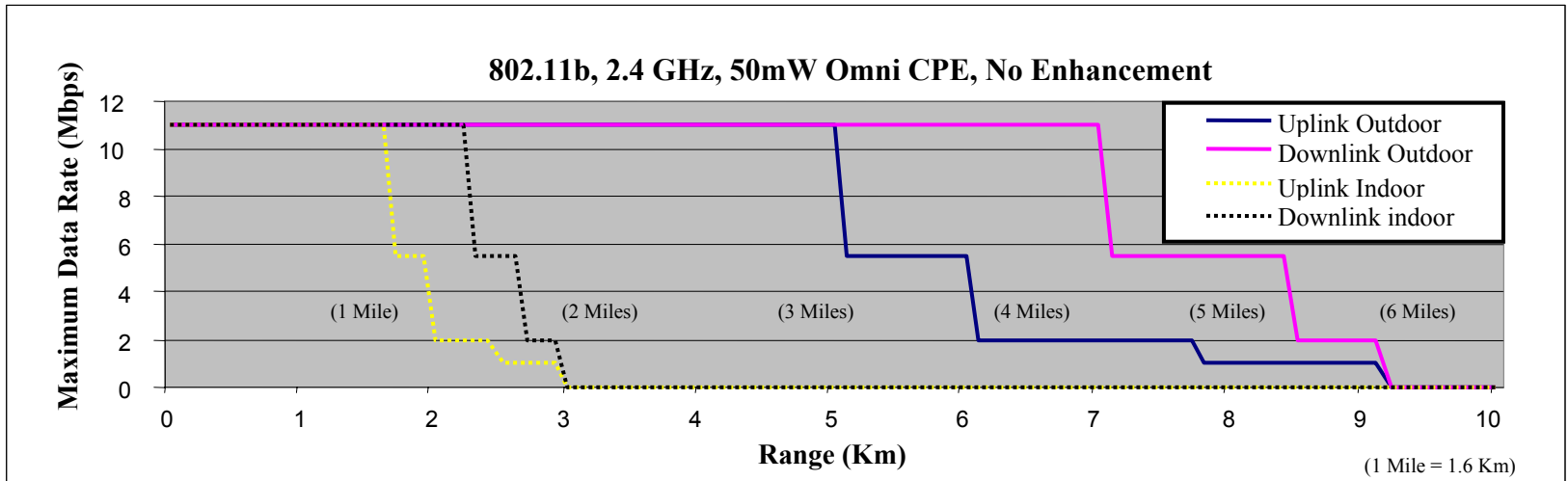
- Cooperation among subscribers required
  - Access point in each home must be “always on”
  - Difficult to guarantee security and QoS with always-on connections
- Congestion and interference generated by intermediate relay nodes in both upstream and downstream directions
  - Worse for nodes residing nearer to service provider in relay chain
- Store-and-forward delay for packets
  - Half-duplex radio transceivers
- Outdoor wireless transmission makes it easier for an intruder to masquerade as a wireless relay
  - Aggravate security problems in current Wi-Fi implementations
  - Rogue access points (i.e., unauthorized access points plugged into a legitimate wireless network)
  - Soft access points (i.e., devices masquerading as access points)
  - Can easily generate a security hole and compromise entire network connected to these access points

**Key solution to problems: A well-designed multihop routing protocol**

# Long-Range Wi-Fi Wireless Access

- May be more attractive than other long-range solutions
  - Can be easily integrated with Wi-Fi home networks which is experiencing staggering growth
  - According to In-Stat/MDR, shipments of Wi-Fi home adapters/access points increased 214% in 2003 (equivalent to sales of 22.7 million units)

# Long-Range Wi-Fi Wireless Access



Based on the Vivato™ Wi-Fi switch (reproduced with permission from Horwitz International LLC, GA, USA)

If directional high-gain antennas are used, then the operational range can extend up to 30 miles

Note: 555 MHz bandwidth available for 802.11a

# Long-Range Wi-MAX Wireless Access

- Based on IEEE 802.16 standard
  - Can potentially offer up to 150 Mbit/s in data rates using 25 MHz of radio spectrum
  - Data rate can be lowered to 100 Mbit/s or 50 Mbit/s if a longer operating range is desired
  - Unlike Wi-Fi, allows full-duplex communication
  - Focuses on frequency bands between 10 and 66 GHz (line-of-sight) and between 2 to 11 GHz (non line-of sight)
  - 10 to 66 GHz standard supports continuously varying traffic levels at many licensed frequencies (e.g., 10.5, 25, 26, 31, 38, and 39 GHz) for two-way communications
  - 2 to 11 GHz extension standard (802.16a) supports both unlicensed and licensed bands
  - TDMA MAC protocol supports multiple physical layer specifications customized for frequency band of use
  - Currently developing a client standard

# Medium Access Control

- Broadcast nature of wireless networks require a medium access control (MAC) protocol (or multiple access protocol) to resolve access contentions among the upstream transmissions from subscribers
  - Transforms shared upstream channel into a point-to-point link
- Key to designing *efficient* MAC protocols is the identification of subscribers with data to transmit
  - These are users who will use bandwidth

# Classification of MAC Protocols

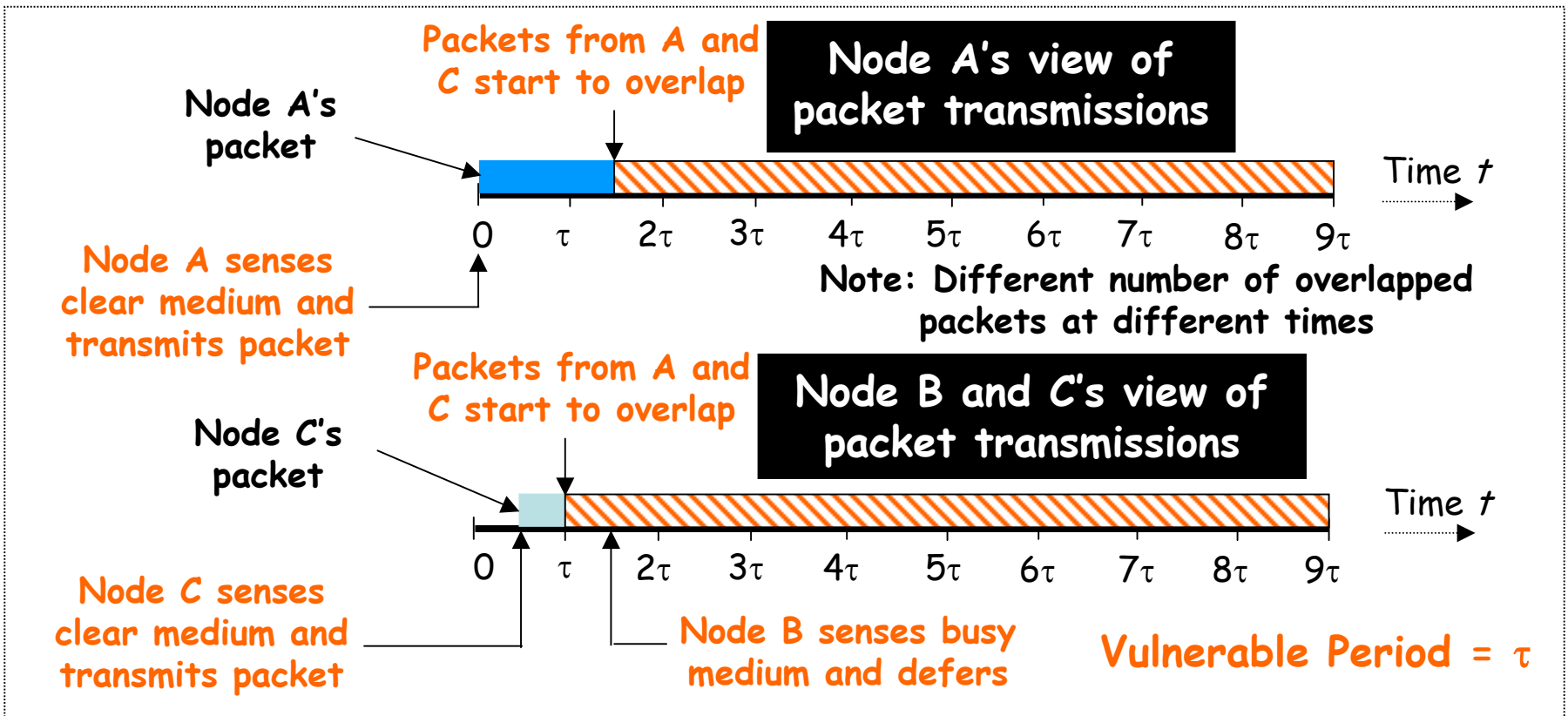
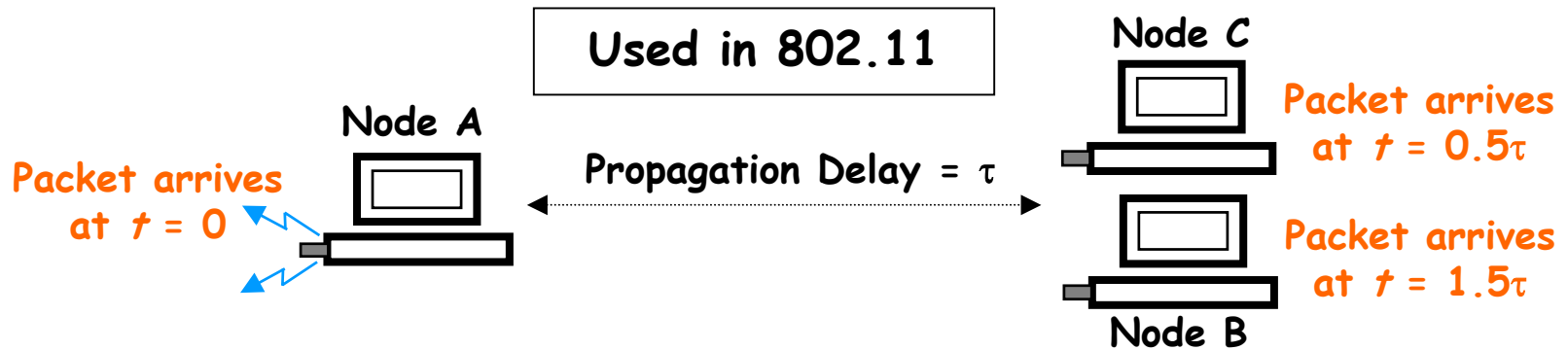
- MAC protocols can be categorized under contention, reservation, polling, and fixed allocation
  - Performance of contention and reservation techniques dependent on combined traffic from *all users* in network
  - Performance of fixed allocation and polling schemes strongly influenced by traffic requirements of *each individual user*

MAC Protocol	Collisions	Control Overhead	Idle Time
Contention	Yes	No	No
Reservation	No	Yes	No
Polling	No	Yes	No
Fixed Allocation	No	No	Yes

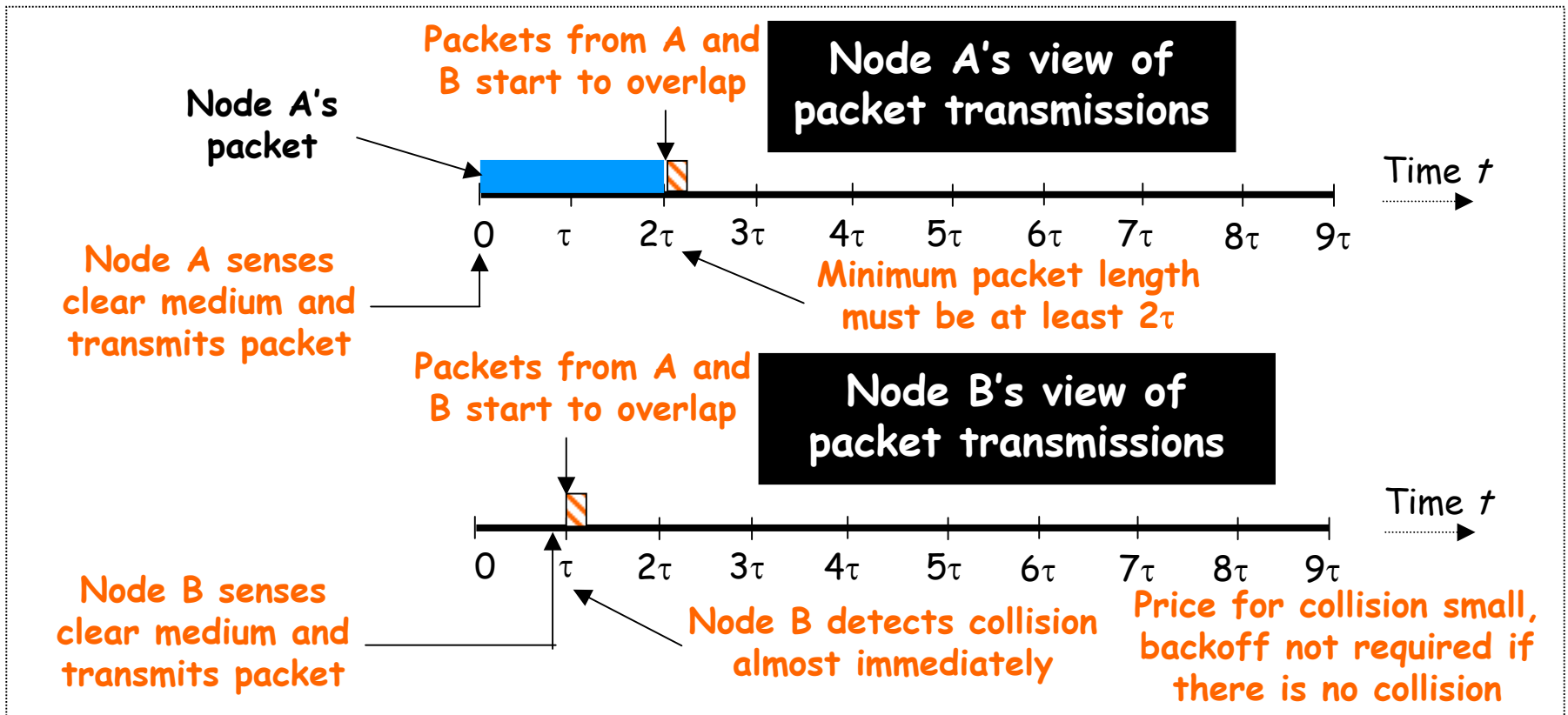
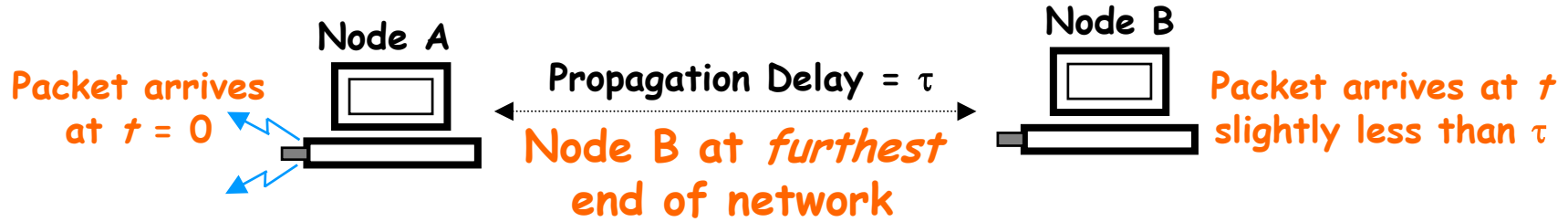
Contention-Free {

Examples of fixed allocation protocols include TDMA, FDMA, CDMA

# Carrier Sense Multiple Access

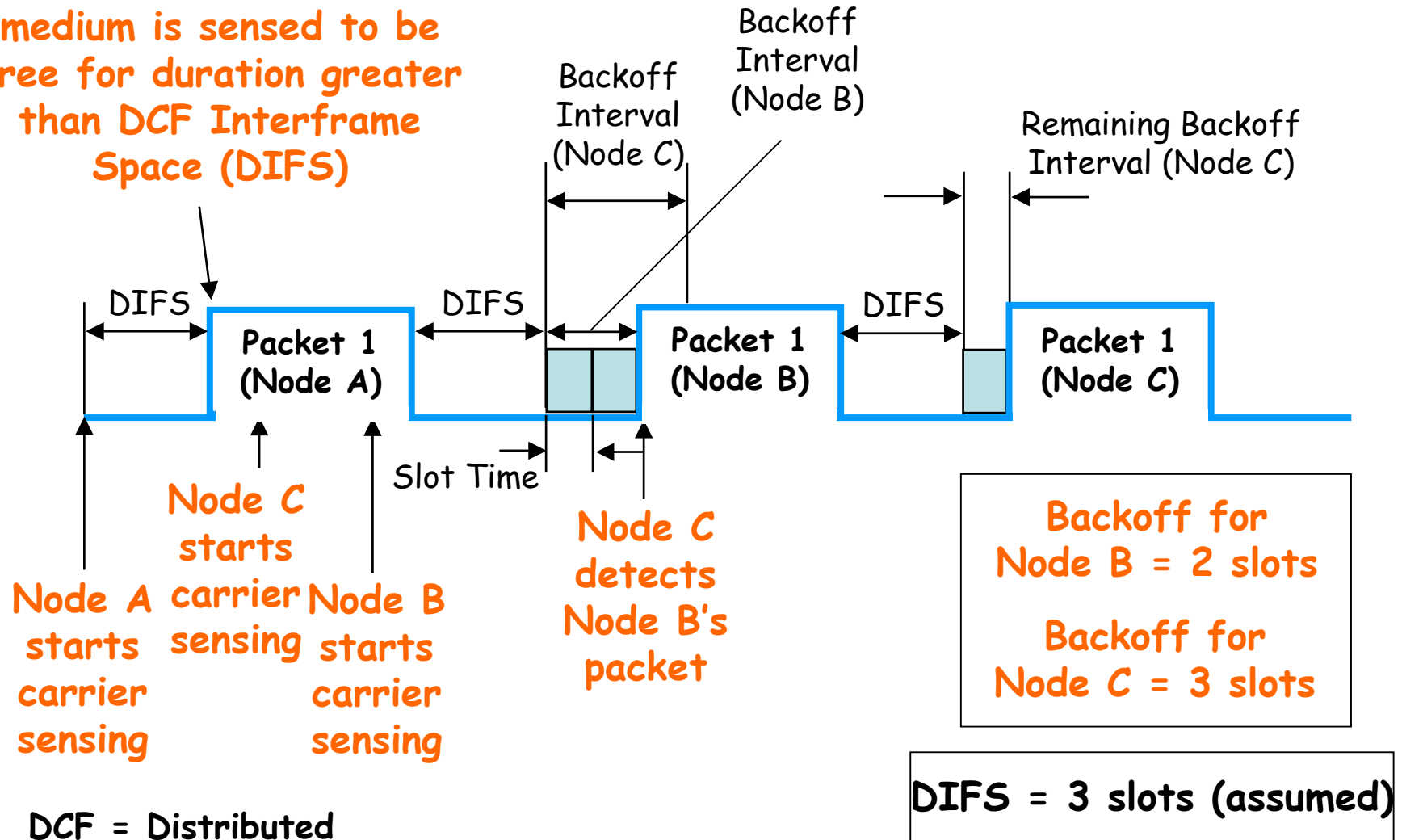


# Carrier Sense Multiple Access with Collision Detection

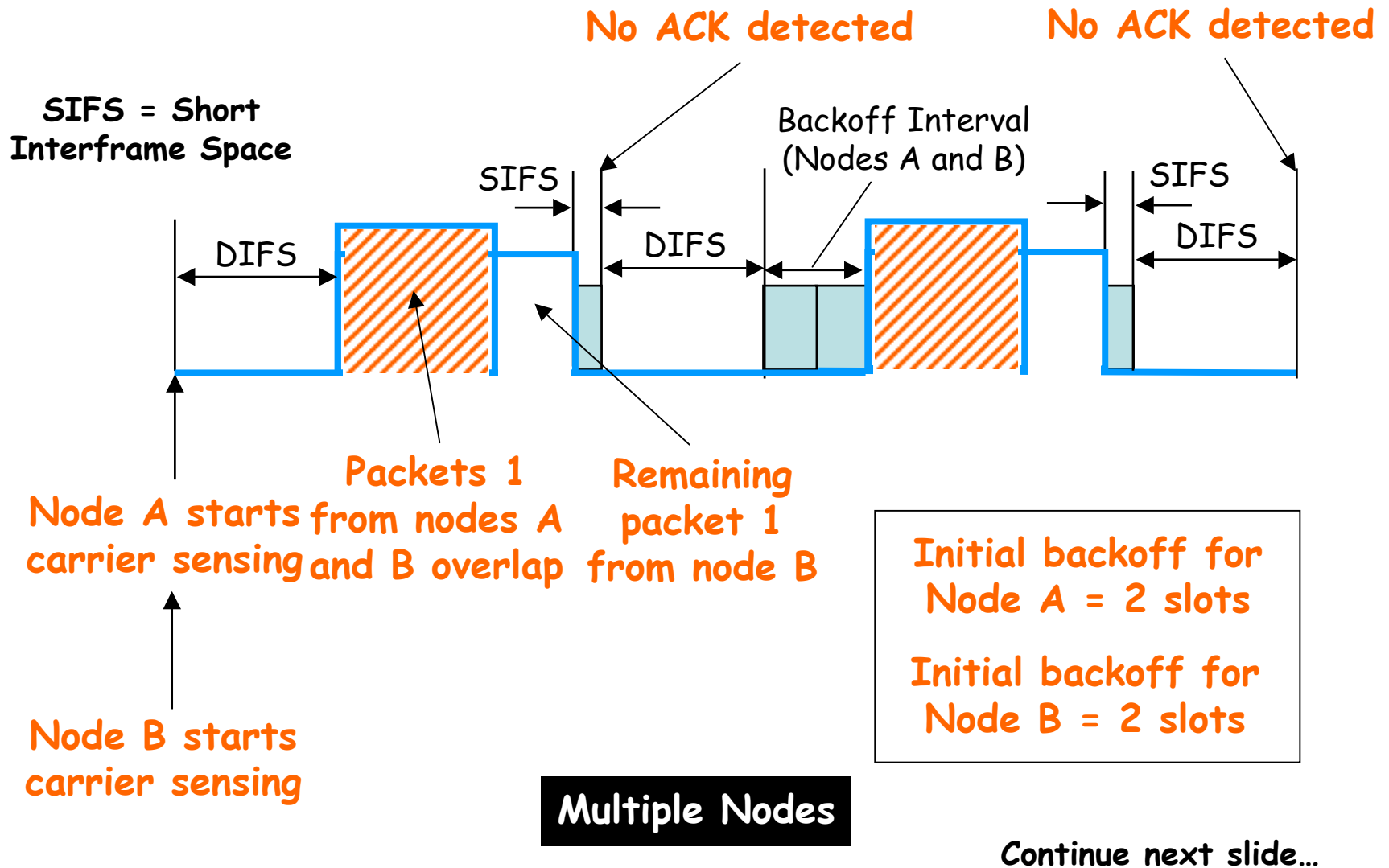


# Collision Avoidance using CSMA

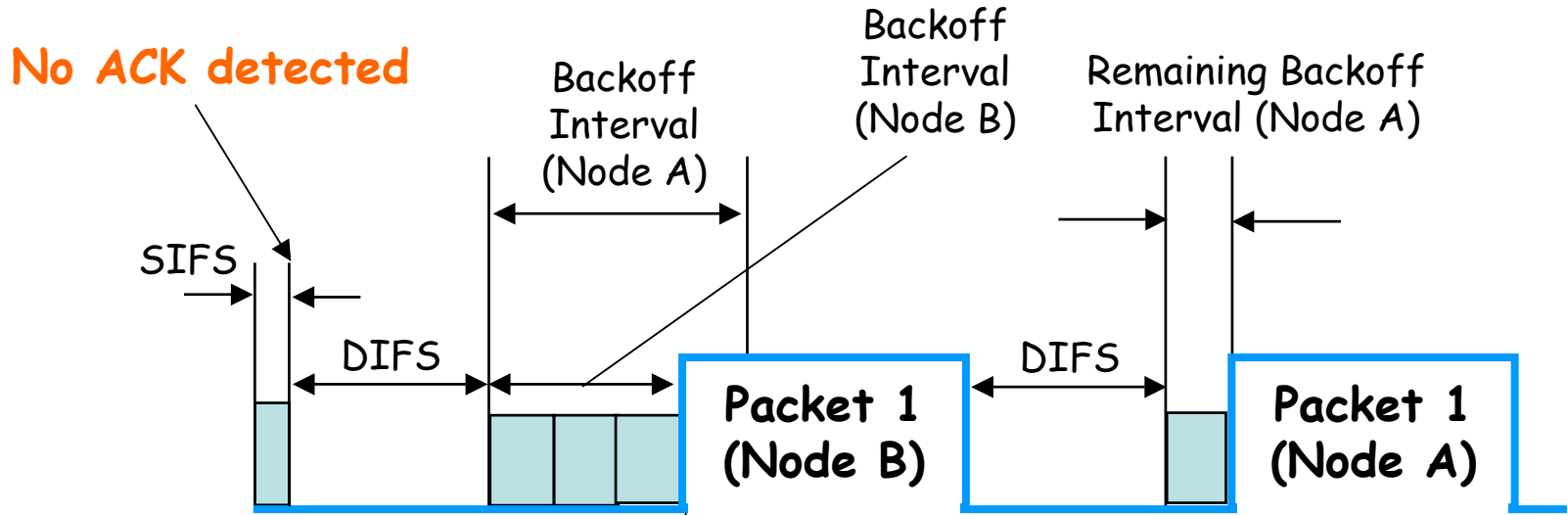
Immediate access when medium is sensed to be free for duration greater than DCF Interframe Space (DIFS)



# Collision Resolution using CSMA



# Collision Resolution using CSMA



No ACK detected

SIFS

DIFS

Backoff Interval (Node A)

Backoff Interval (Node B)

Remaining Backoff Interval (Node A)

Packet 1 (Node B)

DIFS

Packet 1 (Node A)

New backoff for Node A = 4 slots

New backoff for Node B = 3 slots

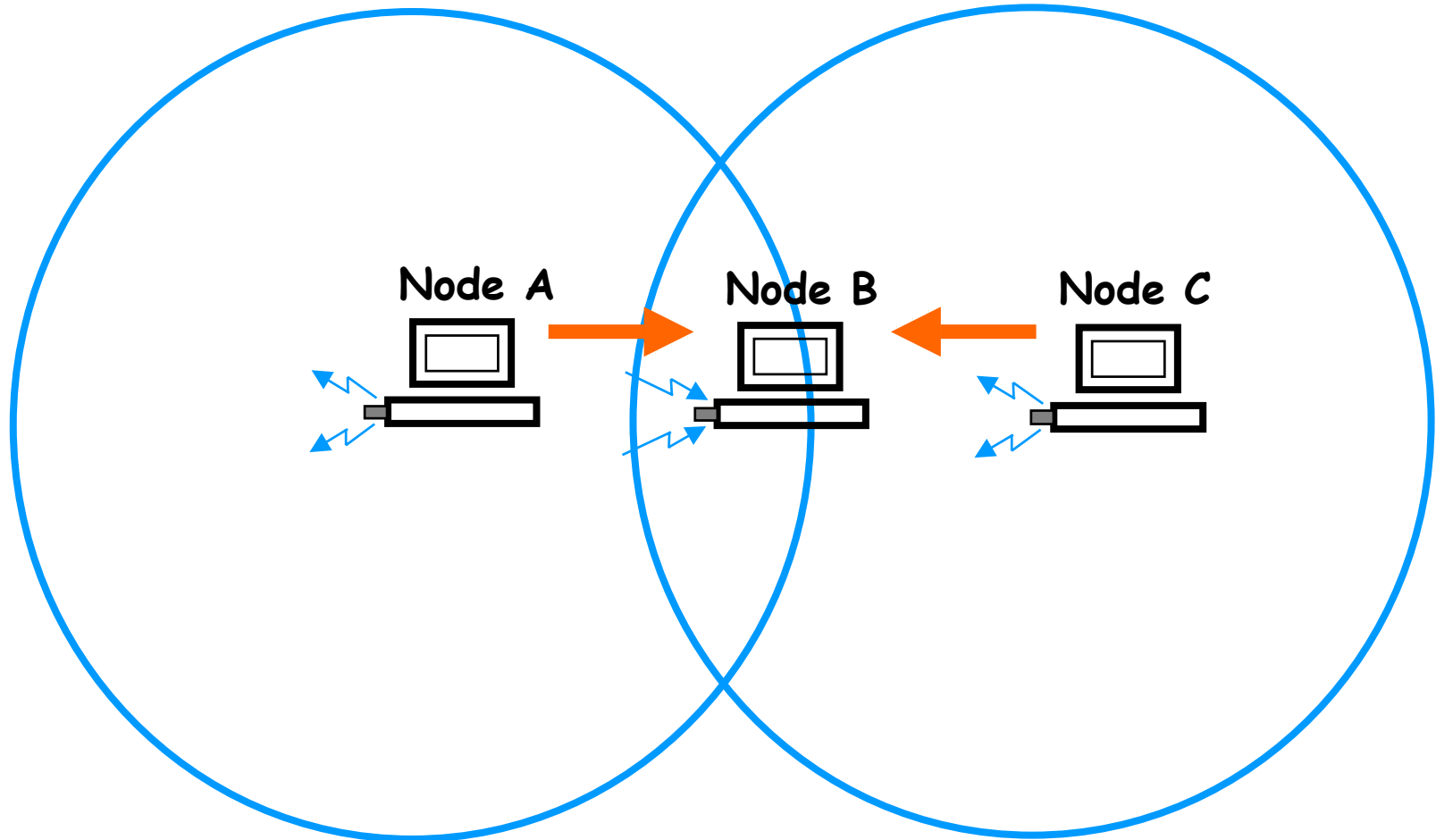
Node A detects Node B's packet

Backoff intervals are increased

Multiple Nodes

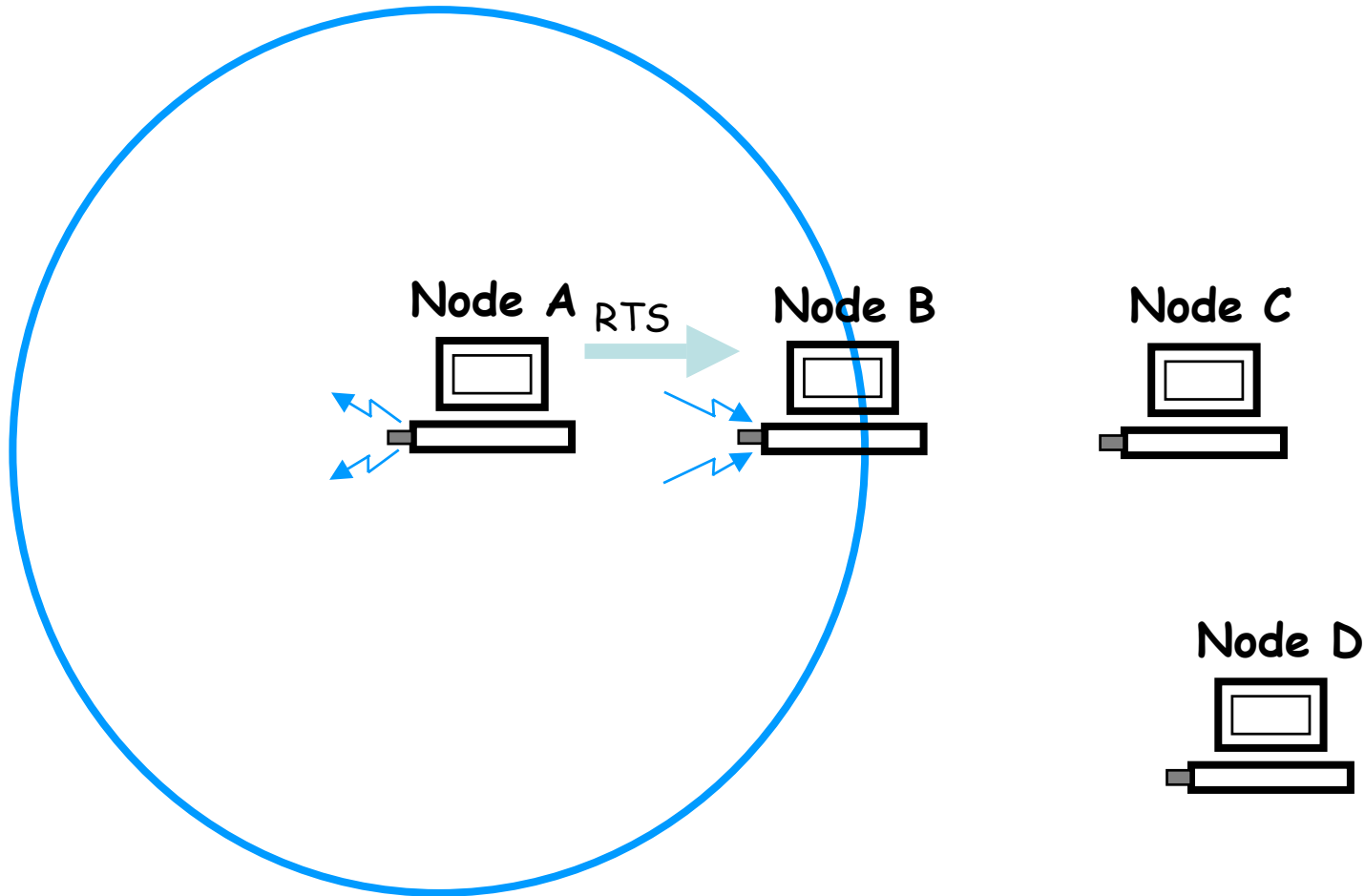
# Hidden Node (Spatial) Problem of CSMA

Nodes A and C are not in range but within range of node B



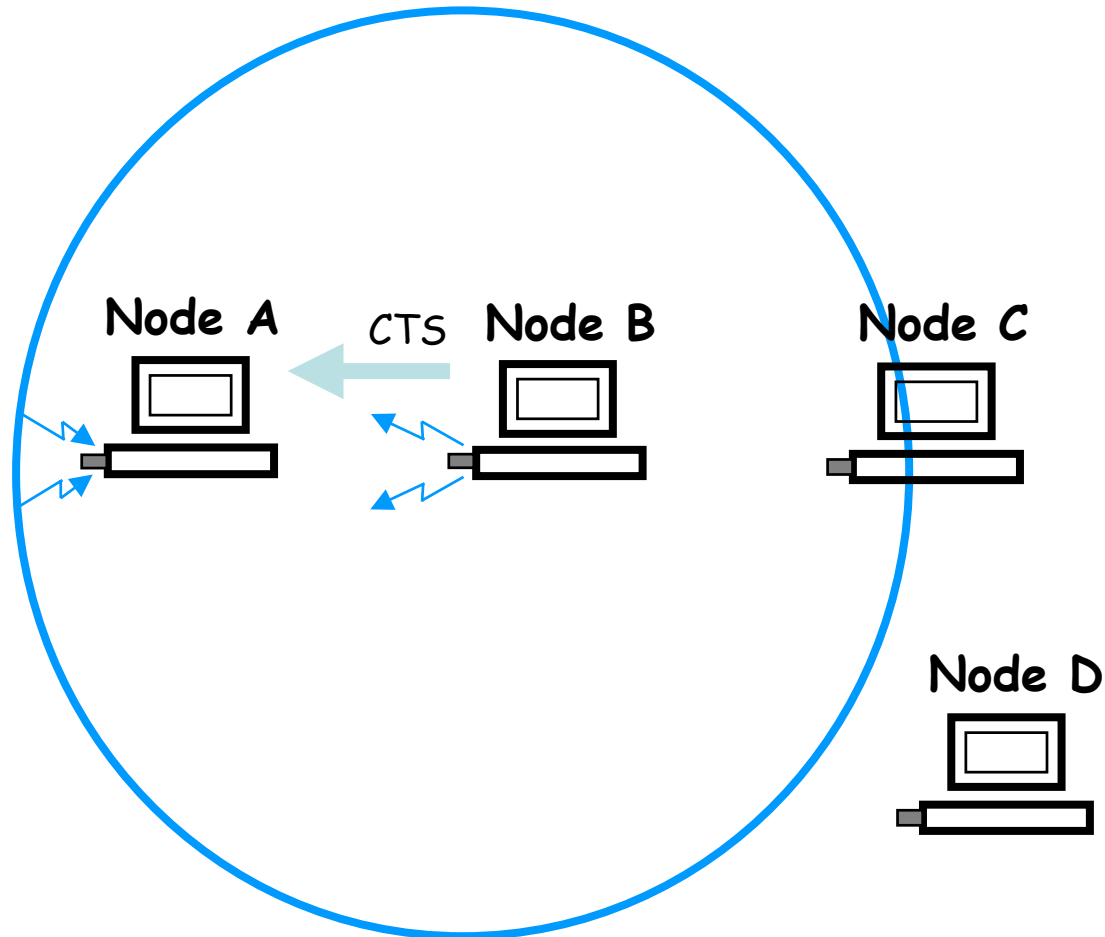
Nodes A and C are unaware of the collision (even with carrier sensing!), they are hidden from each other

# Hidden Node Problem



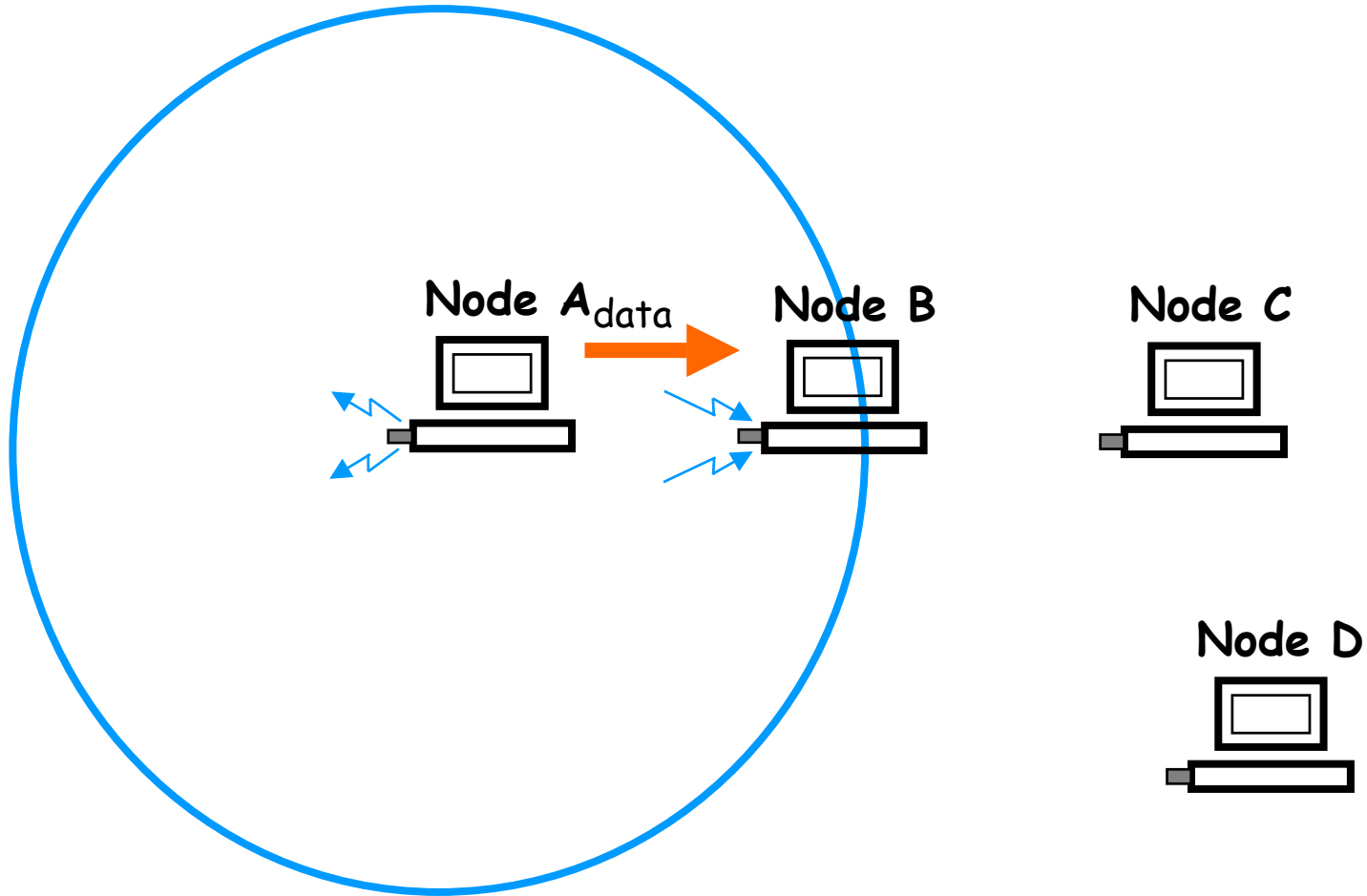
802.11 allows transmission of short control packets namely request to send (RTS) and clear to send (CTS)

# Hidden Node Problem



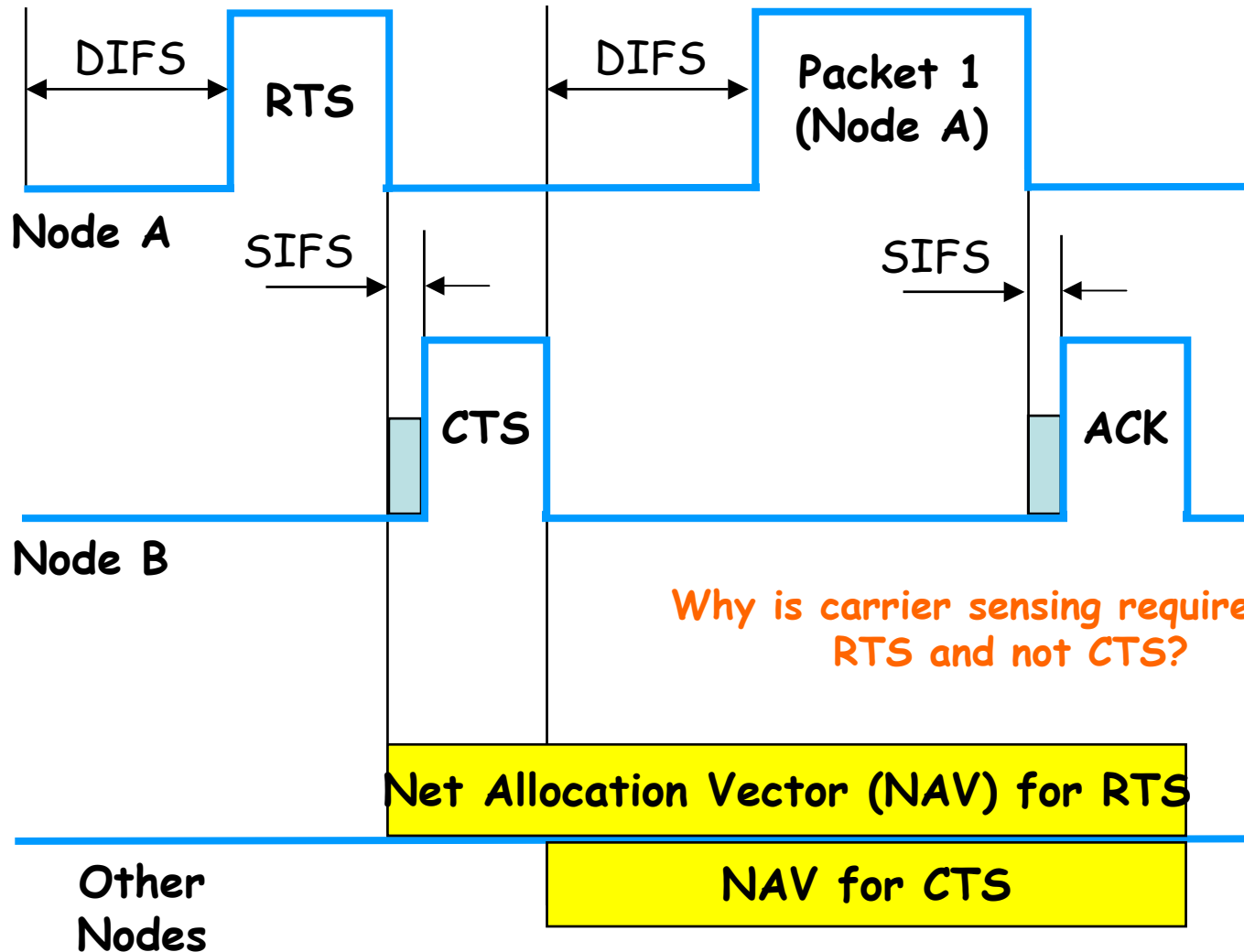
**CTS informs Node C of impending transmission from Node A i.e., it is CTS (and not RTS) that solves the hidden node problem**

# Hidden Node Problem

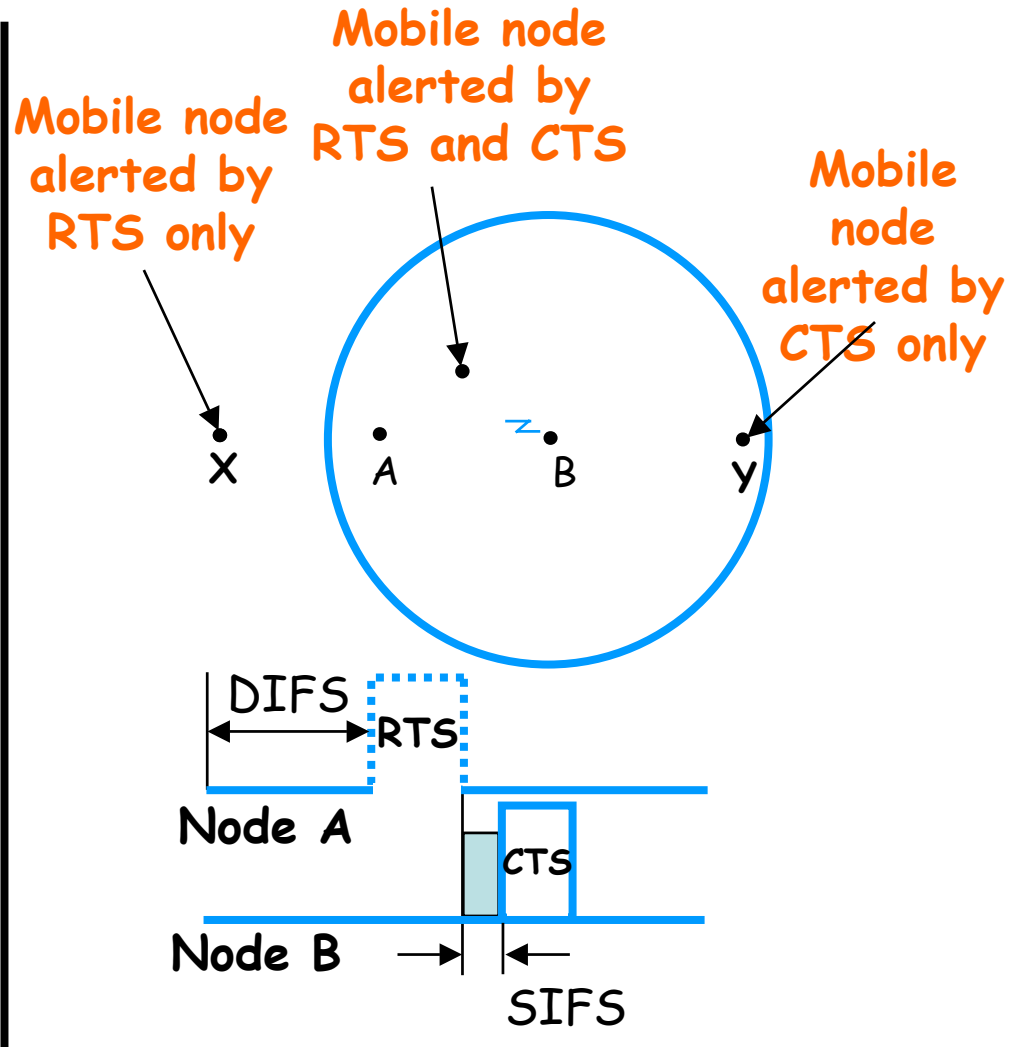
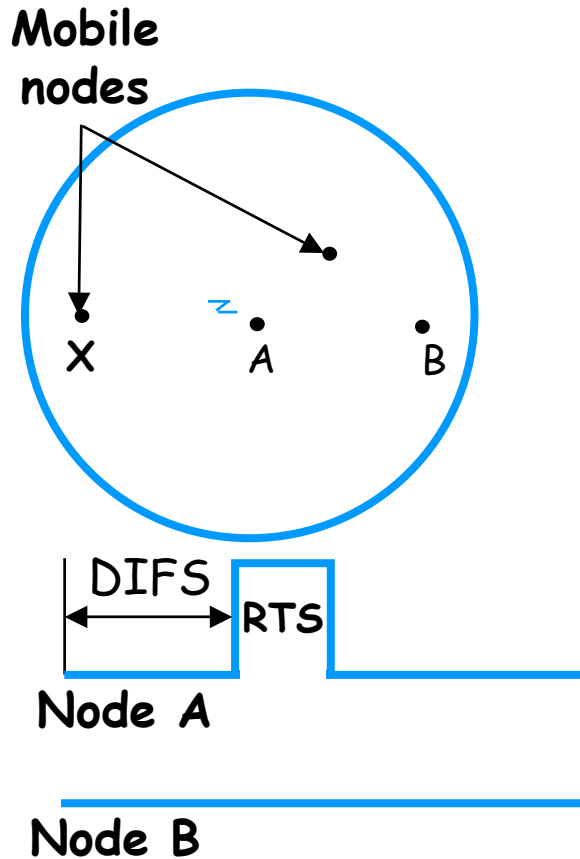


# Virtual Carrier Sensing

## Unicast Data Packet Transmission

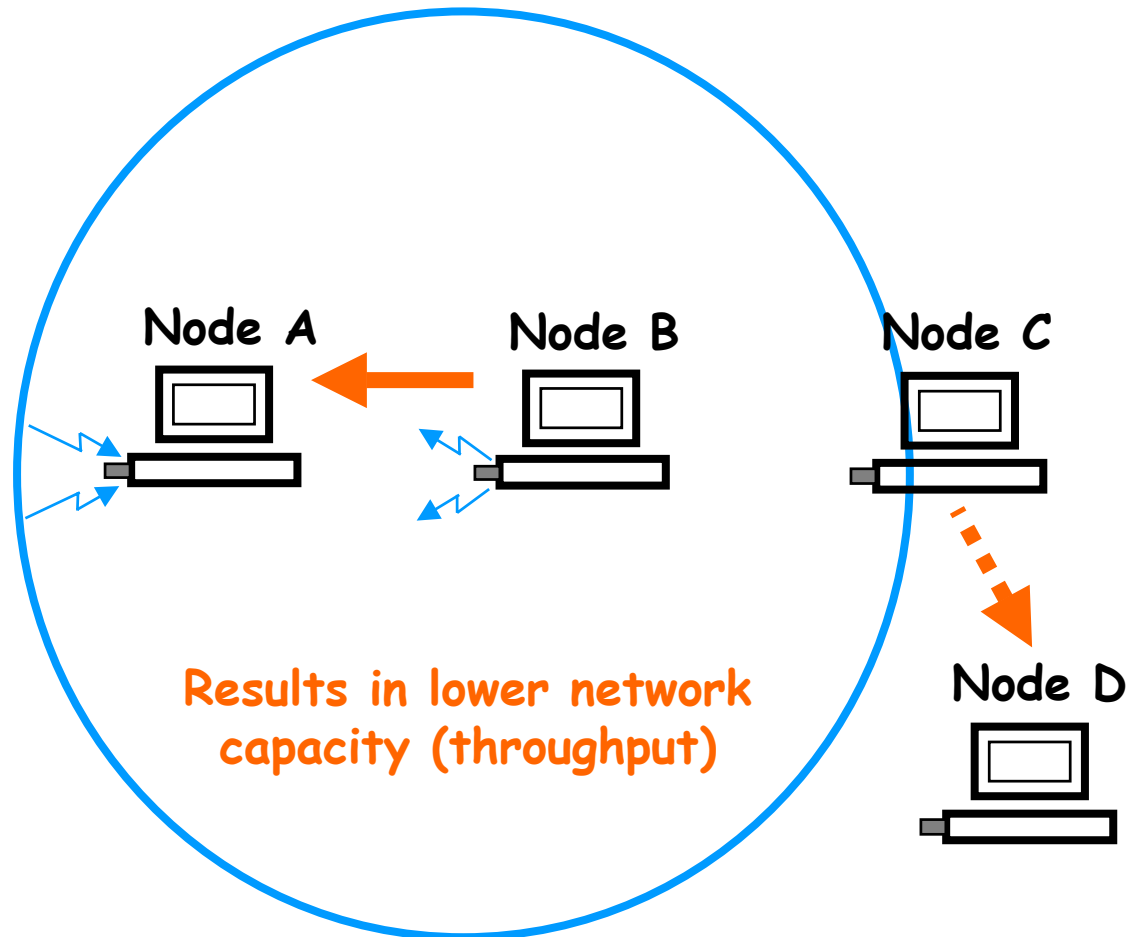


# Virtual Carrier Sensing



Which control packet solves the hidden node problem?

# Exposed Node Problem



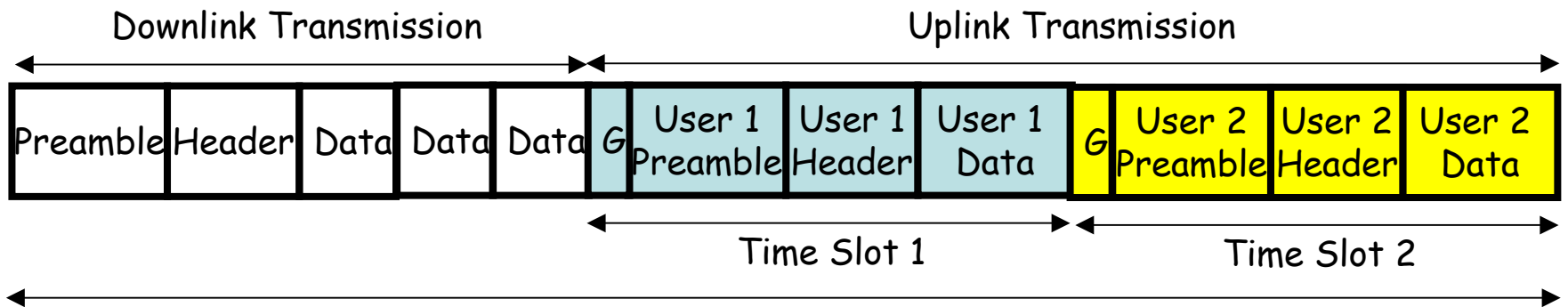
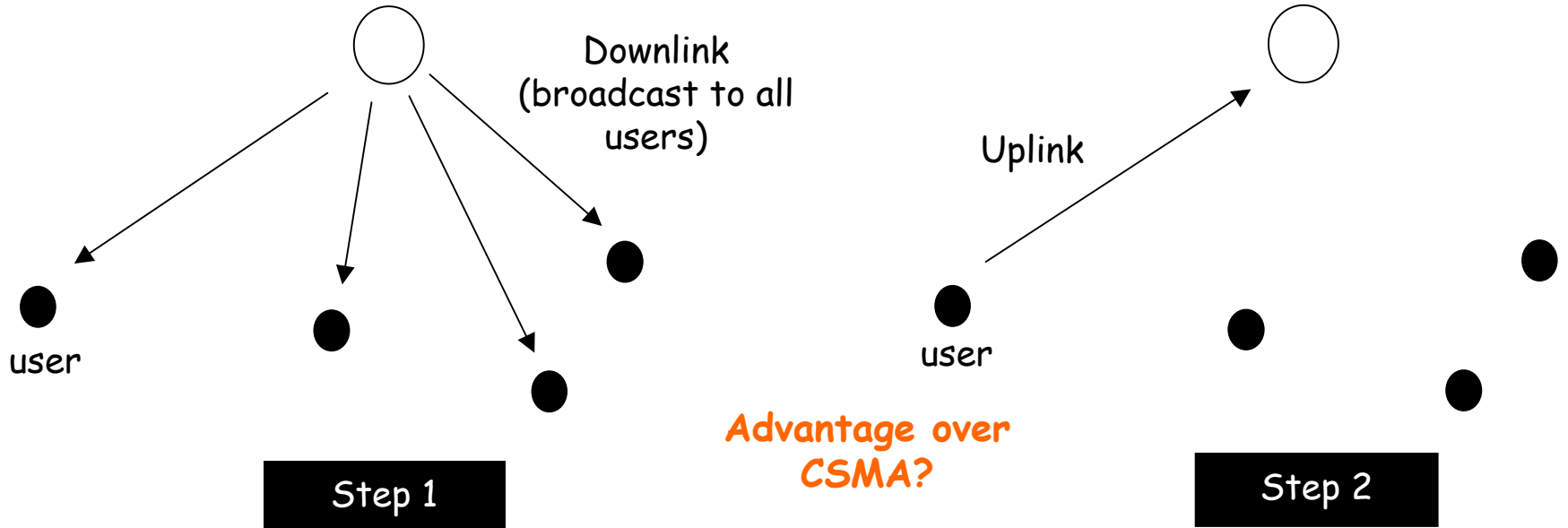
Node C inhibits transmission to node D even though node D is out of node B's range

# TDMA/TDD Operation

Controller/Base Station  
(with scheduler)

Used in 802.16

Controller/Base Station  
(with scheduler)



TDMA/TDD Frame Format

# IEEE 802.11 Wireless LAN Standard

- Also known as wireless Ethernet

- Network (rather than radio) standards
- Comprises a main standard supplemented by extensions
- All extensions based on a single MAC protocol
- 802.11b, 802.11g, 802.11a (Different PHY Specifications)
- 802.11e (Quality of Service)
- 802.11h (Transmit Power Control)
- 802.11i (Security)
- 802.11j (Japanese 5 GHz Standard)
- 802.11k (Radio Resource Measurement)
- 802.11m (Standard Maintenance)
- 802.11n (High Throughput)
- 802.11r (Fast Roaming)
- 802.11s (Extended Service Set)
- WAVE SG (Wireless Access Vehicular Environment)
- WIEN SG (Wireless Interworking with External Networks)
- WPP SG (Wireless Performance Prediction)
- WNG SC (Wireless LANs Next Generation)

**802.11b currently  
the most dominant**

**For large networks servicing  
diverse end-user devices, it is  
better to stick to standards  
rather than proprietary solutions**

# IEEE 802.11e

- Adds multimedia capabilities, QoS support and home wireless network features to existing 802.11 MAC functionality
- General enhancements
  - Allows one device to communicate directly with another even in the presence of an access point
  - A packet in a stream need not be acknowledged  
acknowledgments can be aggregated
  - Forward error correction using Reed-Solomon coding
  - Allows device to transmit multiple packets within a specified period
  - Supports contention-free polling mechanism for deterministic delays
  - Supports efficient polling using reservation requests
  - Allows changes to contention backoff on a per-priority basis
  - Traffic prioritization and parameterization

# IEEE 802.11h

- Spectrum management an important aspect of QoS support
  - Wireless error rates can vary dramatically as a result of obstacles and interferers (e.g., microwave ovens, cordless phones)
  - Can result in retransmissions that degrade bandwidth and QoS for time-sensitive applications
- Dynamic Channel Selection (DCS)
  - Allows a Basic Service Set (BSS) or wireless subnet to be moved to an adjacent channel that may offer better channel characteristics
  - Preserves QoS metrics
  - Provides a mechanism for overlapping (but different) BSSs (e.g., adjacent apartments) to avoid one another
- Transmit Power Control (TPC)
  - Enable nodes to communicate at the minimum power
  - Reduces interference between adjacent and overlapping BSSs using the same channel, thereby improving level of QoS for all BSSs

# IEEE 802.11i

- Stream Theft
  - Ability for an intruder to gain access to content that another individual is paying, without anyone's knowledge
  - Best addressed by improved encryption
- Encryption
  - Advanced Encryption Standard or AES (using elliptical encryption)
- Digital Rights Management
  - A problem in existing 802.11 standard because process for allocating and distributing encryption keys is not defined
- Upper Layer Authentication
  - Key distribution handled by layers above MAC sublayer
  - Effective owner of digital rights can determine who is and who is not to be given permission to receive a particular stream

# Extensible Authentication Protocol (EAP)

- Improves security of WEP significantly
  - An extension to Remote Access Dial-In User Service (RADIUS)
  - RADIUS's vendor specific attribute (VSA) allows a vendor to extend RADIUS operation to fit its own products without conflicting existing RADIUS attributes or other companies' VSAs
  - Defined in IETF's RFC 2284
  - Security framework enables multiple authentication methods (e.g., passwords, tokens, kerberos, and digital certification) which can be activated in sequence if desired
  - Creates a new key for *every* user and *every* new session
  - Provides *centralized* security management of thousands of users
  - Ideal for organizations with a large user base
- EAP framework can be extended to wired LANs
  - Enables an enterprise to use a *single* security architecture for every access method (wireless and wired)

# EAP with Transport Layer Security (EAP-TLS)

- An authentication and encryption protocol developed by Microsoft that succeeds SSL protocol
  - Defined in RFC 2246
  - Provides mutual authentication with non-repudiation, encryption, secure key negotiation, keyed message integrity checking
- Establishes WEP keys using certificate authority
  - When client requests access, authentication server responds with server certificate
  - Client responds with own certificate and validates server certificate
  - From certificate values, EAP-TLS derives session encryption keys
  - After validating client's certificate, authentication server sends session encryption keys to client

# Protected EAP (PEAP)

- Simplified version of EAP-TLS
  - Authenticates server only and hence avoids having to distribute user certificates for every client
- Provide mutual authentication between EAP client and server
  - Use TLS to authenticate authentication server to client
  - Use TLS key to protect channel
  - Use legacy method (e.g., MD5 challenge, GSM-SIM, etc.) protected by TLS key to authenticate client to authentication server