Medium Access Control (MAC) Protocols for Ad hoc Wireless Networks - III

CS: 647
Advanced Topics in Wireless Networks

Drs. Baruch Awerbuch & Amitabh Mishra
Department of Computer Science
Johns Hopkins University
Distributed MAC Protocols

- Most distributed MAC protocols are based on the principle of carrier sensing & collision avoidance (CSMA/CA)
- Hidden terminals play very dominant role in CSMA/CA based protocols
  - Collisions that occur at the destination may not be heard by the sender
  - Therefore receiver has to send some kind of feedback to sender
Distributed MAC - Hidden Node Problem

- In the diagram simultaneous transmission will collide at B
- Half duplex operation of wireless terminals -->, transmission and listening simultaneously is not possible.
- A and C have no knowledge of this collision,
- Two ways A & C can know that collision has occurred at B
  1. A & C periodically stop transmission and listen for feedback from B
  2. B uses out of band signaling to inform A & C
Collision Avoidance Techniques

- First option is very difficult, second option is possible but (inefficient) because it requires additional channel

- Two well know approaches of collision avoidance (CA)
  - Out-of-band approach
  - Hand shaking approach
CA with out-of-band signaling (1)

- Busy Tone Multiple Access (BTMA) (Tobagi & Kleinrock, Haas) protocol uses out of band signaling to solve hidden terminal problem
- Any node hearing ongoing transmission, transmits busy tone
- All nodes hearing busy tone keep silent
- All nodes in 2R radius of the transmitter keep silence (R - range)
- Avoids interference from hidden terminals
- Requires a separate channel for busy tone
- Con: Eliminates hidden nodes, increases exposed nodes
CA with out-of-band signaling (2)

- Receiver Initiated Busy Tone Multiple Access (RI-BTMA) (S. Wu. & V.O.K. Li, 1988)
  - Only receiver transmits the busy tone
  - The receiver decodes the message and verifies the address that it is indeed the receiver
  - The nodes in the vicinity of the receiver (Radius R) are inhibited
  - Does not eliminate hidden terminal problem completely, but reduces the exposed nodes
CA with Control Handshaking - (MACA) - (1)

- Alternative to carrier sensing i.e. does not use CSMA
- Multiple access with collision avoidance (MACA) uses a three way handshake to avoid hidden terminal problem (Karn, 90)

- When node B wants to send a packet to node C, node B first sends a Request-to-Send (RTS) to C

- All nodes within one hop of the sending node hear the RTS and defer their transmissions.

- On receiving RTS, node C responds by sending Clear-to-Send (CTS), provided node C is able to receive the packet

- When a node (such as D) overhears a CTS, it keeps quiet for the duration of the transfer
  - Transfer duration is included in RTS and CTS both
Hidden Terminal Avoidance
**MACA examples**

- **MACA avoids the problem of hidden terminals**
  - A and C want to send to B
  - A sends RTS first
  - C waits after receiving CTS from B

- **MACA avoids the problem of exposed terminals**
  - B wants to send to A, C to another terminal
  - now C does not have to wait for it cannot receive CTS from A
CA with Control Handshaking - (MACA) (2)

- Does not completely solve the hidden terminal problem but does prevent to a large extent

- Enhancements to RTS-CTS control hand shaking and more complete single channel solutions [(MACAW (1997), Bhargavan] [Fullmer et al, (1995, 1997)]
  - MACA has no ACK but MACAW does

- In these techniques tradeoff is in the overhead of handshaking and the number of hidden nodes removed
Reliability

- Wireless links are prone to errors. High packet loss rate detrimental to transport-layer performance.

- MACA delegates packet loss recovery to transport layer → Higher delays
  - Better to perform at the MAC layer

- Mechanisms needed to reduce packet loss rate experienced by upper layers
A Simple Solution to Improve Reliability (MACAW)

- When node B receives a data packet from node A, node B sends an Acknowledgement (Ack). This approach adopted in many protocols [Bharghavan94,IEEE 802.11]

- If node A fails to receive an Ack, it will retransmit the packet
The Incompleteness of the RTS-CTS Method (1)
The Incompleteness of the RTS-CTS Method (2)
Using a directional antenna to resolve the exposed node problem
Outline

- Wireless MAC Issues
  - Hidden terminal problem
  - Exposed terminal problem
  - Capture

- MAC Performance Metrics

- Wireless MAC Classification

- Distributed Wireless MAC Protocols
  - CSMA/CA
  - 802.11 MAC
    - DCF
    - Backoff
  - Hiper Lan MAC
IEEE 802.11

RTS = Request-to-Send
IEEE 802.11

RTS = Request-to-Send

Diagram:

- Node A
- Node B
- Node C
- Node D
- Node E
- Node F

RTS connection between C and D.
IEEE 802.11

CTS = Clear-to-Send
IEEE 802.11

CTS = Clear-to-Send
IEEE 802.11
IEEE 802.11
The basic operation of CSMA protocol is as follows:

1. A node that has data to transmit, senses the channel for certain duration before transmitting
2. If the channel is busy, the node waits a random amount of time and tries to transmit at a later time
3. If the channel is idle, the node tries to acquire the channel
4. A successful acquisition is followed by transmission of data packet
5. If the acquisition attempt results in a collision, the colliding nodes try to resolve collision in an orderly fashion
6. Each packet transmission is acknowledged by the receiver
Distributed Random Access Protocols

- Two well known CSMA/CA protocols are:
  1. Distributed Foundation Wireless MAC (DFWMAC) - IEEE 802.11 Wireless LAN Standard
  2. Elimination Yield - Non Preemptive Priority Multiple Access (EY-NPMA) - HIPERLAN Standard
Minimal Frame Exchange Protocol

- Two frames
  - Frame sent from source to destination
  - Acknowledgement sent from destination back to source

- The exchange of this pair of frames is atomic in the MAC protocol -- cannot be interrupted

- If an acknowledgement is not received, the MAC will retransmit
  - Reduces latency compared to letting a higher layer protocol (e.g., TCP) detect the error and retransmit
**RTS-CTS Exchange Protocol (1)**

- Minimal frame exchange protocol does not address the hidden terminal problem
- IEEE 802.11 supports an RTS-CTS extension
  - Support is mandatory
  - Use is optional

![Diagram]

- **Cleared by RTS**
- **Cleared by CTS**

---

2-26
RTS-CTS Exchange Protocol (2)

- RTS-CTS used for frames longer than a Threshold
  - RTS-CTS overhead not efficient for short frames
  - Some environments may not find RTS-CTS useful, e.g. many infrastructure networks
  - Threshold variable can be tuned

- Virtual carrier sensing
  - Duration field in all frames, including RTS and CTS, monitored by every station
  - Duration field used to construct a network access vector (NAV)
  - Inhibits transmission, even if no carrier detected
Retry Counters

- Counter and timer for each frame
  - Short or long retry counter
  - Lifetime timer

- Retry counter
  - Incremented for each transmission attempt
  - Use of short versus long retry counter based on Threshold variable
  - Threshold limit
    - ShortRetryLimit for short retry counter
    - LongRetryLimit for long retry counter

- If threshold exceeded, frame is discarded and upper layer is notified via MAC interface
Basic Access Mechanism

- Basic access mechanism
  - CSMA/CA with collision avoidance
  - “Listen before talk” -- defers if medium is busy
    - Carrier sensing from PHY layer
    - Virtual carrier sensing based on NAV entries
  - Deferral based on a binary exponential back-off scheme
    - Random value selected from a contention window, starting with a PHY-defined minimum
    - Contention window doubles with each deferral up to a PHY-defined maximum
  - Back-off timer decrements only when the medium is idle
  - Retry counter incremented for each deferral
802.11 - MAC layer

Priorities

- Defined through different inter frame spaces
- No guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  - Highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - Medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  - Lowest priority, for asynchronous data service

![Diagram of MAC layer priorities and time frame](image-url)
 Timing Intervals (1)

- Timing intervals are defined that control a station’s access to the medium

- Slot time (SlotTime)
  - Specific value depends on PMD layer
  - Derived from propagation delay, transmitter delay, etc. (20micro-sec for DSSS and 50 for FHSS)
  - Basic unit of time for MAC, e.g., for backoff time is a multiple of slot time

- Short Inter-Frame Space (SIFS)
  - Shortest interval -- SIF < SlotTime e.g. 10 microsec for FHSS
  - Used for highest priority access to the medium, e.g., for ACK and CTS
  - Allows Data-ACK and RTS-CST to be atomic transactions
**Timing Intervals (2)**

- **Priority (or PCF) Inter-Frame Space (PIFS)**
  - PIFS = SIFS + SlotTime
  - Used for Point Coordination Function (PCF) access to the medium
  - Allows priority based access to the medium after ACKs but before contention based access

- **Distributed (or DCF) Inter-Frame Space (DIFS)**
  - DIFS = SIFS + 2×SlotTime
  - Used for Distributed Control Function (DCF) access to the medium
  - Results in lower priority access than using SIFS or PIFS
Timing Intervals (3)

- Extended Inter-Frame Space (EIFS)
  - EIFS = SIFS + (8×ACK) + PreambleLength + PLCPHeaderLength + DIFS
  - Used in the event that the MAC receives a frame with an error
  - Provides an opportunity for a fast retransmit of the error frame

- In summary ...
  - SIFS < SlotTime < PIFS < DIFS << EIFS
Outline

- Wireless MAC Issues
  - Hidden terminal problem
  - Exposed terminal problem
  - Capture

- MAC Performance Metrics

- Wireless MAC Classification

- Distributed Wireless MAC Protocols
  - CSMA/CA
  - 802.11 MAC
    - DCF
    - Backoff
  - Hiper Lan MAC
DFWMAC/IEEE 802.11

- It’s a derivative of MACA protocol \(\rightarrow\) MACAW

- It consists of four way exchange, RTS-CTS-DATA-ACK
  
  1. When a sender has a data to transmit, it picks a random wait period. The wait period is decremented if the channel is idle
  2. When this period expires, the node tries to acquire the channel by sending a RTS packet
  3. The Receiving node (destination) responds with a CTS packet indicating that its ready to receive the data
  4. The sender then completes the packet transmission
  5. If the packet is received without errors, the destination node responds with an ACK
DFWMAC/IEEE 802.11

6. If an ACK is not received, the packet is assumed to be lost and the packet is retransmitted.

7. If RTS fails, the node attempts to resolve the collision by doubling the wait period. (This is known as binary exponential back-off (BEB)).

8. Station trying to send an ACK is given preference over a station that is acquiring a channel (Different waiting intervals are specified).

9. A node needs to sense channel for Distributed Inter-Frame Space (DIFS) interval before making an RTS attempt and a Short Inter Frame Space (SIFS) interval before sending an ACK packet.
DFWMAC/IEEE 802.11

- Because SIFS is shorter than the DIFS interval, the station sending an ACK attempts transmission before a station sending a data packet.

- In addition to physical channel sensing, virtual carrier sensing is achieved due to NAV (Network allocation vector) field in the packets.

- NAV indicates the duration of current transmission.

- Nodes listening to RTS, or CTS messages back off NAV amount of time before sensing the channel again.

- Several papers describe this protocol and even suggest enhancements.
802.11 - CSMA/CA basic access method (DCF) without RTS/CTS

- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)
802.11 - CSMA/CA basic access method (DCF) without RTS/CTS

- Sending unicast packets
  - station has to wait for DIFS before sending data
  - receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - automatic retransmission of data packets in case of transmission errors
Sending unicast packets

- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS
IEEE 802.11 MAC Operation
Exponential Backoff Algorithm

- Select random number of slot times to defer transmission, keep as a state variable
- After channel has been idle for specified interval, decrement variable after each idle slot passes
- If carrier is sensed, freeze variable countdown, wait for channel to become idle again and resume countdown
802.11 - competing stations - simple version

- **DIFS**: Interframe Space
- **bo**: Backoff
- **bo\_e**: Elapsed Backoff Time
- **bo\_r**: Residual Backoff Time
- **busy**: Medium not idle (frame, ack etc.)
- **packet arrival at MAC**: Packet arrival at MAC

Station 1:
- DIFS
- bo\_e
- bo\_r
- busy

Station 2:
- DIFS
- bo\_e
- busy

Station 3:
- busy

Station 4:
- DIFS
- bo\_e
- busy
- bo\_e
- bo\_r

Station 5:
- DIFS
- bo\_e
- bo\_r
- bo\_e
- bo\_r
- bo\_e
- bo\_r

\( t \)
Exponential Backoff Algorithm

- No response from RTS or lost ACKs necessitates retransmission
  - Contention window is doubled, until reaching $CW_{max}$
- After successful transmissions
  - Contention window reset to $CW_{min}$
MAC Summary

- Designing MAC protocols for ad hoc networks is very difficult

- Issues to consider:
  - Hidden/exposed terminal
  - Collision avoidance
  - Congestion control
  - Fairness
  - Reliability
  - Energy efficiency

- IEEE 802.11 DCF (RTS/CTS/DATA/ACK) widely used, but many other protocols are proposed
What you should know ... (1)

- Wireless Mac issues
  - Half Duplex operation,
  - Time Varying Channel, Burst Errors
  - Performance parameters for MAC
  - Hidden Nodes
  - Exposed Nodes
  - Captured Nodes
  - MACA Mac Protocol
  - RTS-CTS Mechanisms
  - Limitations of RTS-CTS mechanisms
What you should know ... (2)

- Functions and operation of the MAC layer
  - Minimum frame exchange protocol
  - RTS-CTS extension

- Frame formats
  - Basic types and formats
  - Role of address fields

- Operation of access mechanisms
  - Operation of basic access mechanism
  - Role of timing intervals
  - Operation of DCF, DCF with RTS-CTS and PCF