Wireless Networks
(CSC-7602)
Lecture 6
(08 Oct. 2007)

Seung-Jong Park (Jay)
http://www.csc.lsu.edu/~sjpark

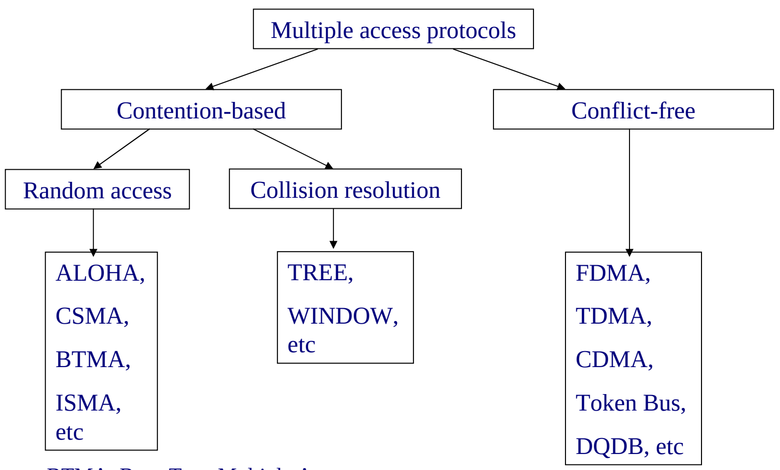
Wireless MAC

Wireless MAC

- CSMA as wireless MAC?
- Hidden and exposed terminal problems make the use of CSMA an inefficient technique
- Several protocols proposed in related literature – MACA, MACAW, FAMA
- IEEE 802.11 standard for wireless MAC

CSC7602 – S.J. Park

Reminder: MAC Protocols over Wired Network



BTMA: Busy Tone Multiple Access
ISMA: Internet Streaming Media Alliance

DQDB: Distributed Queue Dual Bus

CSMA/CD (CSMA with Collision Detection)

- In CSMA, if 2 terminals begin sending packet at the same time, each will transmit its complete packet (although collision is taking place).
- Wasting medium for an entire packet time.
- CSMA/CD

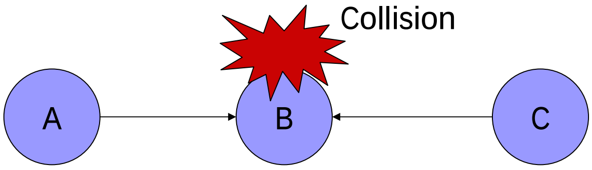
  Step 1: If the medium is idle, transmit

  Step 2: If the medium is busy, continue to listen until the channel is idle then transmit

  Step 3: If a collision is detected during transmission, cease transmitting

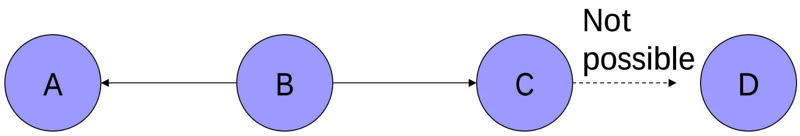
  Step 4: Wait a random amount of time and repeats the same algorithm

Hidden Terminal Problem



- A talks to B
- C senses the channel
- C does not hear A’s transmission (out of range)
- C talks to B
- Signals from A and B collide

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)

Hidden and Exposed Terminal Problems

- Hidden Terminal
  - More collisions
  - Wastage of resources
- Exposed Terminal
  - Underutilization of channel
  - Lower effective throughput

MACA[1]

- Medium Access with Collision Avoidance
- To reduce the probability of data packet collisions caused by hidden terminal problem
- CSMA/CA (Localtalk) uses a "dialogue" between sender and receiver to allow receiver to prepare for receptions in terms of allocating buffer space or entering "spin loop" on a programmed I/O interface

MACA[1]:
- P. Karn, "MACA – A New Channel Access Method for Packet Radio," in ARRL/CRRL Amateur Radio 9th Computer Networking Conference, pp134-140, ARRL, 1990

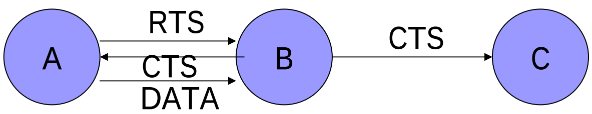
Basis for MACA

- In the context of hidden terminal problem, "absence of carrier does not always mean an idle medium"
- In the context of exposed terminal problem, "presence of carrier does not always mean a busy medium"
- Data carrier detect (DCD) useless!
- Get rid of CS (carrier sense) from
  CSMA/CA – MA/CA – MACA!!!!

MACA

- Dialogue between sender and receiver:
  - Sender sends RTS (request to send)
  - Receiver (if free) sends CTS (clear to send)
  - Sender sends DATA
- Collision avoidance achieved through intelligent consideration of the RTS/CTS exchange
- When station overhears an RTS addressed to another station, it inhibits its own transmitter long enough for the addressed station to respond with a CTS
- When a station overheads a CTS addressed to another station, it inhibits its own transmitter long enough for the other station to send its data

Hidden Terminal Revisited ...



- A sends RTS
- B sends CTS
- C overheads CTS
- C inhibits its own transmitter
- A successfully sends DATA to B

Hidden Terminal Revisited

- How does C know how long to wait before it can attempt a transmission?
- A includes length of DATA that it wants to send in the RTS packet
- B includes this information in the CTS packet
- C, when it overhears the CTS packet, retrieves the length information and uses it to set the inhibition time

Exposed Terminal Revisited

- B sends RTS to A (overheard by C)
- A sends CTS to B
- C cannot hear A's CTS
- C assumes A is either down or out of range
- C does not inhibit its transmissions to D

Collisions

- Still possible – RTS packets can collide!
- Binary exponential backoff 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)

Drawbacks

- Collisions still possible if CTS packets cannot be heard but carry enough to cause significant interference
- If DATA packets are of the same size as RTS/CTS packets, significant overheads

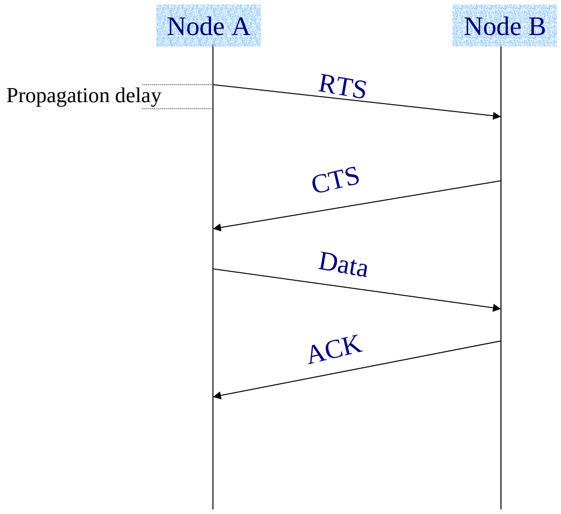
MACA Recap

- No carrier sensing
- Request-to-send (RTS), Clear-to-send (CTS) exchange to solve hidden terminal problem
- RTS-CTS-DATA exchange for every transmission

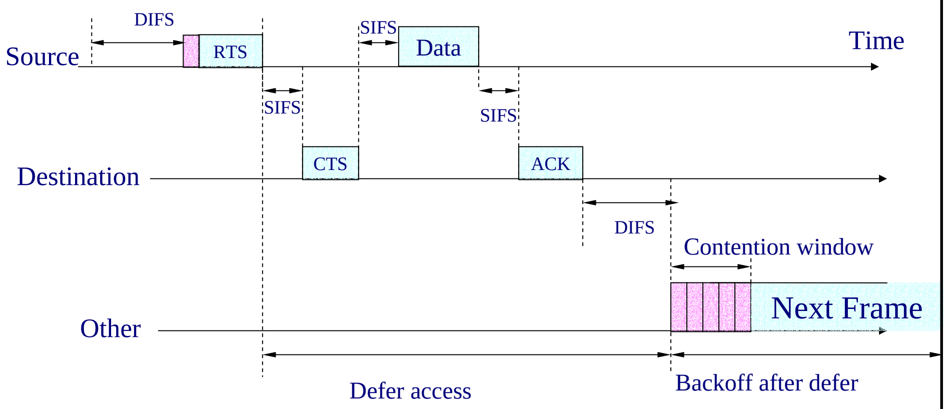
Other modifications (ACK)

- ACK packet exchange included in addition to RTS-CTS-DATA
  - Handle wireless (or collision) errors at the MAC layer instead of waiting for coarse grained transport (TCP) layer retransmission timeouts
  - For a loss rate of 1%, 100% improvement in throughput demonstrated over MACA

RTS/CTS



CSMA/CA with RTS/CTS (Cont'd)



MACAW

- Based on MACA
- Design based on 4 key observations:
  - Contention is at receiver, not the sender
  - Congestion is location dependent
  - To allocate media fairly, learning about congestion levels should be a collective enterprise
  - Media access protocol should propagate synchronization information about contention periods, so that all devices can contend effectively

Back-off Algorithm

- MACA uses binary exponential back-off (BEB)
- BEB: back-off counter doubles after every collision and reset to minimum value after successful transmission
- Unfair channel allocation!
- Example simulation result:
  - 2 stations A & B communicating with base-station
  - Both have enough packets to occupy entire channel capacity
  - A gets 48.5 packets/second, B gets 0 packets/second

BEB Unfairness

- Since successful transmitters reset back-off counter to minimum value
- Hence, it is more likely that successful transmitters continue to be successful
- Theoretically, if there is no maximum back-off, one station can get the entire channel bandwidth
- Ideally, the back-off counter should reflect the ambient congestion level which is the same for all stations involved!

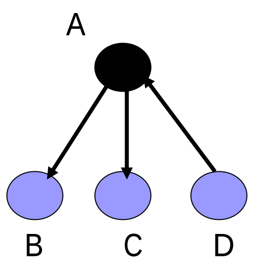
BEB with Copy

- MACAW uses BEB with Copy
- Packet header includes the BEB value used by transmitter
- When a station overhears a packet, it copies the BEB value in the packet to its BEB counter
- Thus, after each successful transmission, all stations will have the same backoff counter
- Example simulation result (same setting as before:
  - A gets 23.82 packets/second, B gets 23.32 packets/second

Other modifications (DS)

- In the exposed terminal scenario (ABCD with A talking to B), C cannot talk to D (because of the ACK packet introduced)
- What if the RTS/CTS exchange was a failure? How does C know this information?
- A new packet DS (data send) included in the dialogue: RTS-CTS-DS-DATA-ACK
- DS informs other stations that RTS-CTS exchange was successful

Accommodating Multiple Streams



- Problem
  - If A has only one queue for all streams (default case), bandwidth will be split as AB:1/4, AC:1/4, DA:1/2
  - Is this fair?
- Solution:
  - Maintain multiple queues at A, and contend as if there are two co-located nodes at A
  - One for transmitting and the other for receiving

MACAW Recap

- Backoff scheme
  - BEB with Copy
  - Multiple streams
- New control packets
  - ACK
  - DS
- Other changes (see paper)

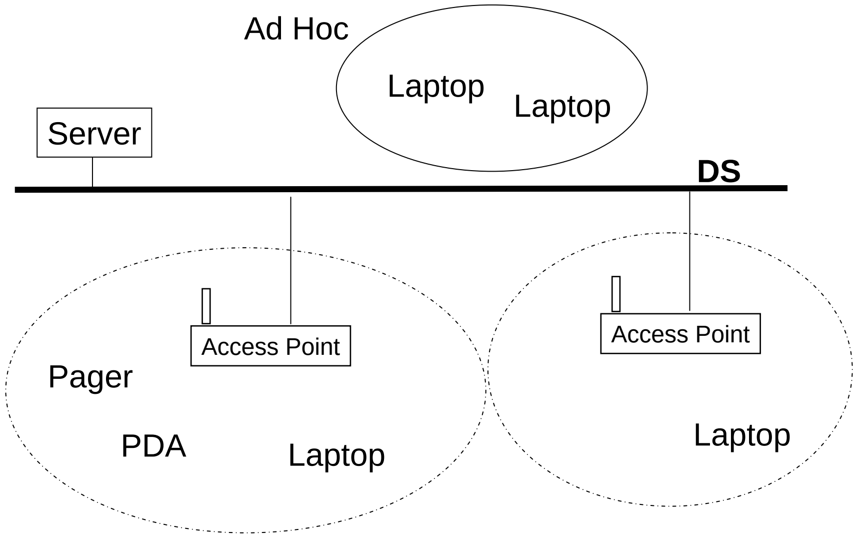
Other MAC Schemes

- FAMA
  - Floor Acquisition Multiple Access
  - Prevents any data collisions
- MACA-BI
  - MACA by invitation
  - No RTS but CTS retained
  - Suitable for multi-hop wireless networks
- Several other approaches ...

Wireless LAN

- Wish List
  - High speed
  - Low cost
  - No use/minimal use of the mobile equipment battery
  - Can work in the presence of other WLAN
  - Easy to install and use
  - Etc

Wireless LAN Architecture



IEEE 802.11

- The 802.11 standard provides MAC and PHY functionality for wireless connectivity of fixed, portable and moving stations moving at pedestrian and vehicular speeds within a local area.
- Specific features of the 802.11 standard include the following:
  - Support of asynchronous and time-bounded delivery service
  - Continuity of service within extended areas via a Distribution System, such as Ethernet.
  - Accommodation of transmission rates of 1, 2,10, and 50 Mbps
  - Support of most market applications
  - Multicast (including broadcast) services
  - Network management services
  - Registration and authentication services

CSC7602 – S.J. Park

IEEE 802.11

- The 802.11 standard takes into account the following significant differences between wireless and wired LANs:
  - Power Management
  - Security
  - Bandwidth
  - Addressing

IEEE 802.11 Topology

- Independent Basic Service Set (IBSS) Networks
  - Stand-alone BSS that has no backbone infrastructure and consists of at-least two wireless stations
  - Often referred to as an ad-hoc network
  - Applications include single room, sale floor, hospital wing
- Extended Service Set (ESS) Networks
  - Large coverage networks of arbitrary size and complexity
  - Consists of multiple cells interconnected by access points and a distribution system, such as Ethernet

IEEE 802.11 Logical Architecture

- The logical architecture of the 802.11 standard that applies to each station consists of a single MAC and one of multiple PHYs
  - Frequency hopping PHY
  - Direct sequence PHY
  - Infrared light PHY
- 802.11 MAC uses CSMA/CA (carrier sense multiple access with collision avoidance)

IEEE 802.11 MAC Layer

- Primary operations
  - Accessing the wireless medium (!)
  - Joining the network
  - Providing authentication and privacy
- Wireless medium access
  - Distributed Coordination Function (DCF) mode
  - Point Coordination Function (PCF) mode

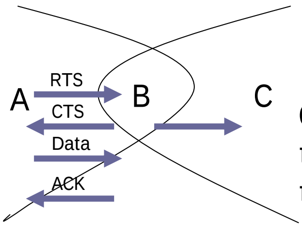
IEEE 802.11 MAC (contd.)

- DCF
  - CSMA/CA – A contention based protocol
- PCF
  - Contention-free access protocol usable on infrastructure network configurations containing a controller called a point coordinator within the access points
- Both the DCF and PCF can operate concurrently within the same BSS to provide alternative contention and contention-free periods

CSMA with Collision Avoidance

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Control packet transmissions precede data packet transmissions to facilitate collision avoidance
- 4-way (RTS, CTS, Data, ACK) exchange for every data packet transmission

CSMA/CA (Contd.)



C knows B is listening to A. Will not attempt to transmit to B.

Hidden Terminal Problem Solved through RTS-CTS exchange!

CSMA/CA (Contd.)

- Can there be collisions?
  - Control packet collisions (C transmitting RTS at the same time as A)
  - C does not register B's CTS
  - C moves into B's range after B's CTS

CSMA/CA Algorithm

- Sense channel (CS)
- If busy
  - Back-off to try again later
- Else
  - Send RTS
  - If CTS not received
    - Back-off to try again later
  - Else
    - Send Data
    - If ACK not received
      - Back-off to try again later
    - Next packet processing

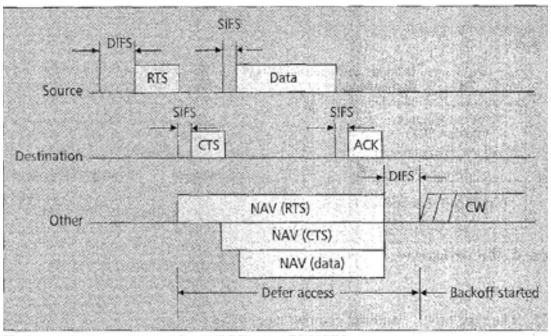


Figure 6. *Transmission of an MPDU using RTS/CTS.*

CSMA/CA Algorithm (Contd.)

- Maintain a value CW (Contention-Window)
- If Busy,
  - Wait till channel is idle. Then choose a random number between 0 and CW and start a back-off timer for proportional amount of time (Why?).
  - If transmissions within back-off amount of time, freeze back-off timer and start it once channel becomes idle again (Why?)
- If Collisions (Control or Data)
  - Binary exponential increase (doubling) of CW (Why?)

IEEE 802.11 MAC Frame Format

- Overall structure:
  - Frame control (2 octets)
  - Duration/ID (2 octets)
  - Address 1 (6 octets)
  - Address 2 (6 octets)
  - Address 3 (6 octets)
  - Sequence control (2 octets)
  - Address 4 (6 octets)
  - Frame body (0-2312 octets)
  - FCS (4 octets)

Bytes:								
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame Body	CRC

802.11 MAC Header (Frame Control through Addr 4)

Recap

- Random Access MAC Schemes
  - CSMA
  - MACA
  - MACAW
  - IEEE 802.11 Standard

MAC for Wireless Networks

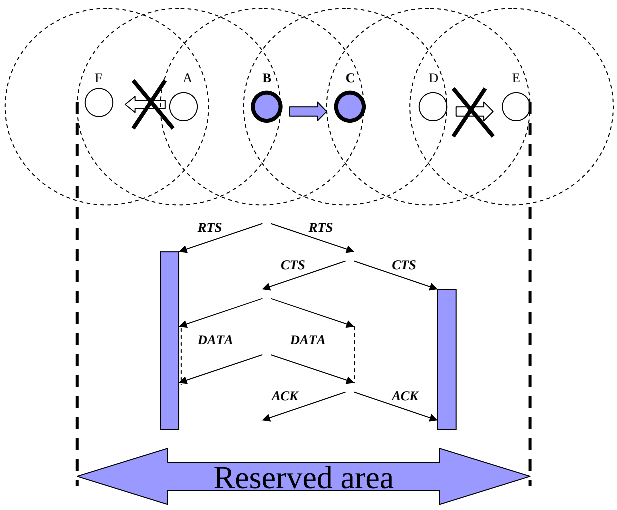
Directional MAC for Directional Antenna

SMAC for Sensor Networks

D-MAC Protocol

[Ko2000Infocom]

IEEE 802.11



Directional MAC (D-MAC)

- Directional antenna can limit transmission to a smaller region (e.g., 90 degrees).
- Basic philosophy: MAC protocol similar to IEEE 802.11, but on a per-antenna basis

D-MAC

- IEEE802.11: Node X is blocked if node X has received an RTS or CTS for on-going transfer between two other nodes
- D-MAC: Antenna T at node X is blocked if antenna T received an RTS or CTS for an on-going transmission
- Transfer allowed using unblocked antennas
- If multiple transmissions are received on different antennas, they are assumed to interfere

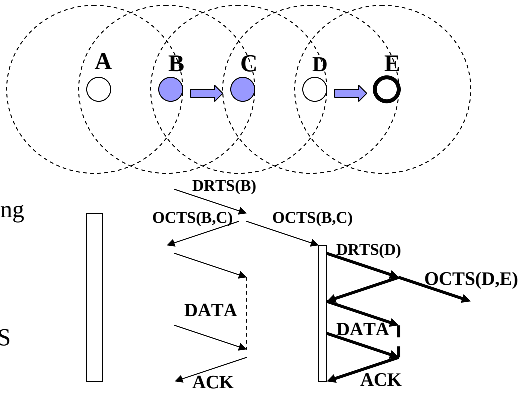
D-MAC Protocols

- Based on location information of the receiver, sender selects an appropriate directional antenna
- Several variations are possible

D-MAC Scheme 1

- Uses directional antenna for sending RTS, DATA and ACK in a particular direction, whereas CTS sent omni-directionally
- Directional RTS (DRTS) and
  Omni-directional CTS (OCTS)

D-MAC Scheme 1: DRTS/OCTS

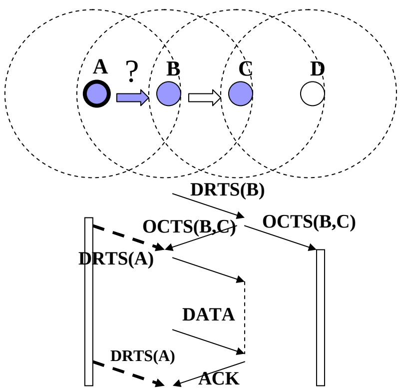


DRTS(B) - Directional RTS including location information of node B

OCTS(B,C) – Omni-directional CTS including location information of nodes B and C

Drawback of Scheme 1

- Collision-free ACK transmission not guaranteed



D-MAC Scheme 2

- Scheme 2 is similar to Scheme 1, except for using two types of RTS
- Directional RTS (DRTS) / Omni-directional RTS (ORTS) both used
  - If none of the sender's directional antennas are blocked, send ORTS
  - Otherwise, send DRTS when the desired antenna is not blocked

D-MAC Scheme 2

- Probability of ACK collision lower than scheme 1
- Possibilities for simultaneous transmission by neighboring nodes reduced compared to scheme 1

Variations

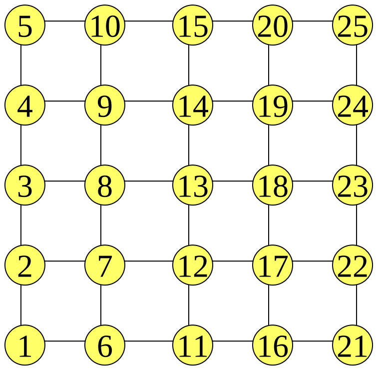
- Paper discusses further variations on the theme
  - Reducing ACK collisions
  - Reducing wasteful transmission of RTS to busy nodes

Performance Comparison

- Which scheme will perform better depends on
  - location of various hosts
  - traffic patterns
  - antenna characteristics

Performance Evaluation

- Mesh topology
- No mobility
- Bulk TCP traffic
- 2 Mbps channel

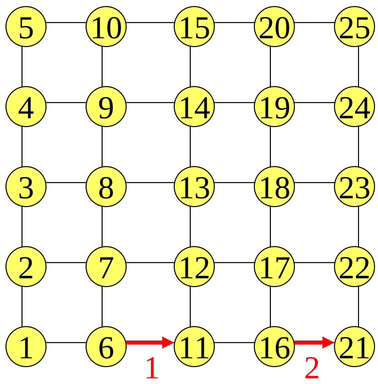


Performance Measurement

- Reference throughput of single TCP connection using IEEE 802.11
  - 1 hop (1383 Kbps)
  - 2 hops (687 Kbps)
  - 3 hops (412 Kbps)
  - 4 hops (274 Kbps)

Performance Measurement

- Scenario 1

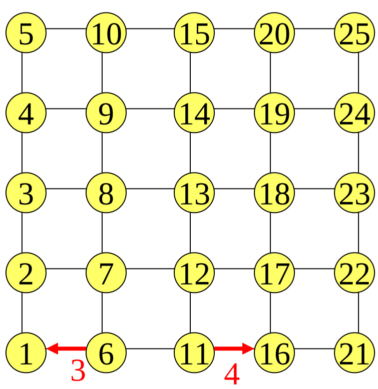


Connections	IEEE802.11	Scheme1	Scheme2
No.1	1130.42	771.27	51.03
No.2	214.57	1040.21	1303.64
Total Throughput	**1344.99**	**1811.48**	**1354.67**

Performance Measurement

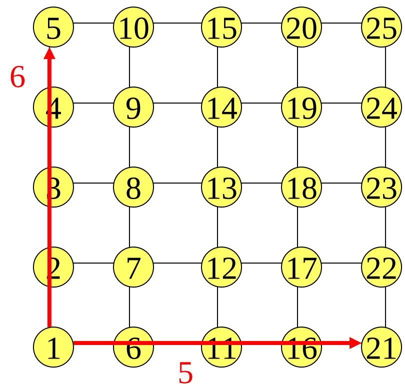
- Scenario 2: Best case for scheme 1

Connections	IEEE802.11	Scheme1	Scheme2
No.3	653.64	1250.14	884.82
No.4	634.58	1251.64	867.69
Total Throughput	**1288.22**	**2501.78**	**1752.51**



Performance Measurement

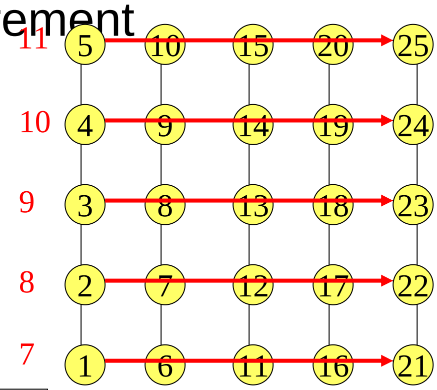
- Scenario 3



Connections	IEEE802.11	Scheme1	Scheme2
No.5	179.66	207.41	210.20
No.6	179.46	209.53	216.53
Total Throughput	**359.12**	**416.94**	**426.73**

Performance Measurement

- Scenario 4



Connections	IEEE802.11	Scheme1	Scheme2
No.7	157.50	146.73	165.89
No.8	89.90	85.31	81.30
No.9	22.00	91.39	105.03
No.10	89.29	82.30	82.83
No.11	157.94	153.30	163.37
Total	**516.63**	**559.03**	**598.42**

Limitations of D-MAC

- No guarantee of collision-free ACK
  - Some improvements suggested in paper
- Inaccurate/outdated location information can degrade performance

Conclusion

- Benefit: Can allow more simultaneous transmissions by improving spatial reuse
- Disadvantage: Can increase Ack collisions

- Alternatives for determining location information should be considered
- Location information does not always correlate well with direction

SMAC Protocol

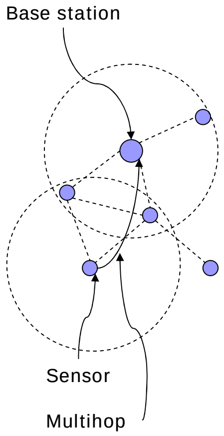
[Ye 2002 Infocom]

SMAC for Sensor Networks

- The characteristics of sensor networks
- Issues of MAC protocols for sensor networks
- Proposed solution for MAC protocols
  - S-MAC (Sensor-MAC)

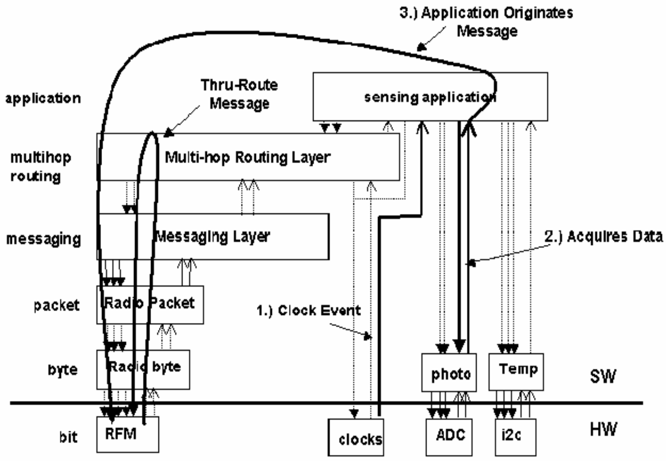
The characteristics of sensor networks

- Tight constraints
  - Computation power
  - Storage
- Primary functions
  - Sample the environment for sensory information
  - Propagate data back to the infrastructure
- Traffic pattern
  - Little activity in lengthy period
  - Intensive traffic in short time
  - Highly correlated traffic
  - End to end flows are required to be fair



The characteristics of sensor networks

- Networking component stack for sensor networks



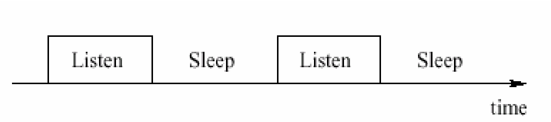
Complete TinyOS application component graph

Issues in MAC protocols for sensor networks

- Issues
  - Energy efficiency
  - Fairness of end to end flows
- Related work
  - IEEE802.11
    - High energy consumption when the nodes are in the idle mode
  - CSMA
    - To improve the energy consumption by avoiding overhearing among neighb oring nodes
  - TDMA
    - No contention-introduced overhead and collisions
    - Not easy to manage the inter-cluster communication and interference
    - Not easy to dynamically change its frame length and time slot assignment
  - PAMAS
    - Power off radio when not actively transmitting and receiving packet

S-MAC (Sensor-Networks)

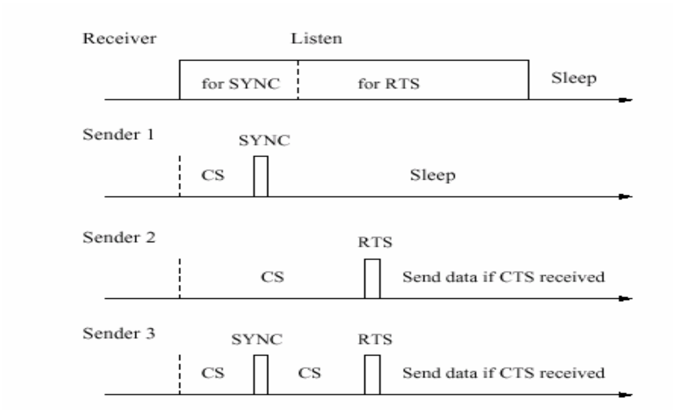
- Trade Off
  - Energy efficiency ⟷ Node-level fairness & Latency
- Basic Scheme: Periodic Listen and Sleep



- Choosing schedule
  - The node randomly choose a time to go to sleep.
  - The node receives and follows its neighbor's schedule by setting its schedule t o be the same.
  - If the node receives a different schedule after it select its own schedule, it adop ts both schedules.

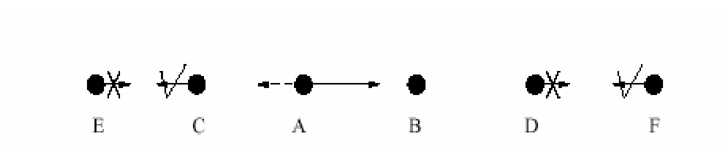
S-MAC (Sensor-Networks)

- **Maintaining Schedule**
  - To update schedule by sending a SYNC packet periodically



S-MAC (Sensor-Networks)

- **Collision Avoidance**
  - Virtual carrier sense
    checking the keeping silent time recorded in the NAV (network allocation vector)
  - Physical carrier sense
    Listening to the channel for possible transmission
  - RTS/CTS exchange
- **Overhearing Avoidance**
  - Let interfering nodes go to sleep after they hear an RTS or CTS packet



S-MAC (Sensor-Networks)

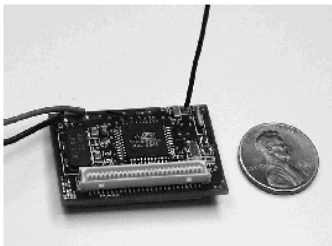
- Message passing
  - Only one RTS packet and one CTS packet are used
    - To avoid large control overhead and long delay
  - ACK would be sent after each data fragment
    - To avoid fragment loss or error
    - To Prevent hidden terminal problem
  - After the neighbor node hears the RTS and CTS, it will go to sleep for the time th at is needed to transmit all the fragments (using the duration field)

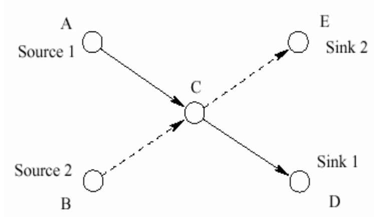
S-MAC (Sensor-Networks)

- Energy Saving vs. Increasing latency (Multi-hop Network)
  - Carrier sense delay
    Determined by the contention window size
  - Backoff delay
    Because the node detects another transmission or the collision occurs
  - Transmission delay
    Determined by channel bandwidth, packet length and the coding scheme adopted
  - Propagation delay
    Determined by the distance between the sending and receiving nodes
  - Processing delay
    Depends on the computing power of the node and the efficiency of in-network data processing al gorithms
  - Queuing delay
    Depends on the traffic load
  - Sleep delay
    Caused by the nodes periodic sleeping

S-MAC (Sensor-Networks)

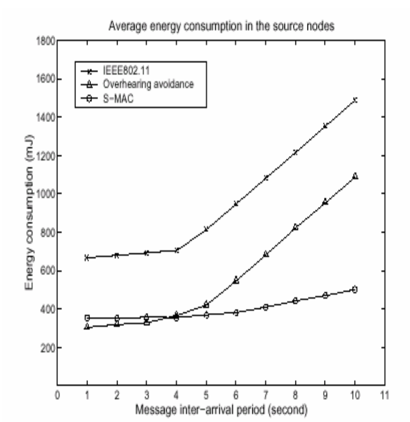
- Testbed
  - Used Rene Motes as the develop ment platform and testbed
  - TinyOS
  - 3 working modes: receiving, tran smitting and sleep
- Topology used in the experiment
  - 3 MAC modules on the mote and TinyOS platform
  1. Simplified IEEE802.11 DCF
  2. Message passing with overhearin g avoidance
  3. The complete S-MAC





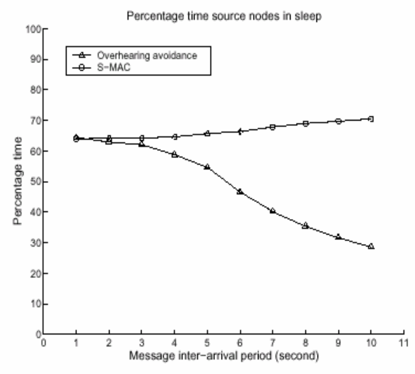
S-MAC (Sensor-Networks)

- The energy consumption result on the source nodes A and B
  - When the traffic is heavy (the inte r-arrival time<4s), S-MAC achieve s energy saving mainly by avoidin g overhearing and efficiently trans mitting a long message
  - When the traffic is light, the period ic sleep plays a key role for energ y savings



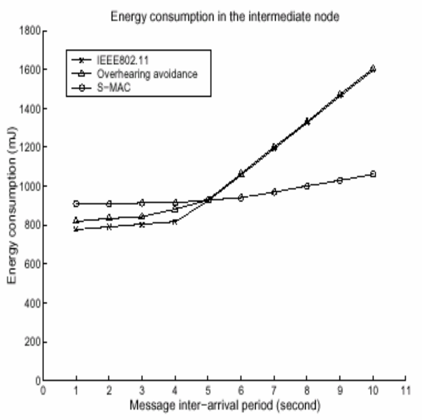
S-MAC (Sensor-Networks)

- The percentage of time that the so urce nodes are in the sleep mode
  - The S-MAC protocol adjusts the sl eep time according to the traffic p atterns
  - The Module of message passing with overhearing avoidance spend more and more time in idle listenin g when the traffic is light



S-MAC (Sensor-Networks)

- Energy consumption in the interm ediate nodes
  - When the traffic is light, S-MAC sti ll outperforms 802.11 MAC
    - Reason1:S-MAC has synchroniz ation overhead of sending an d receiving SYNC packets
    - Reason2:S-MAC introduces mor e latency and actually uses m ore time to transmit the same amount of data



S-MAC (Sensor-Networks)

- Conclusion
  - This new MAC protocol has very good energy conserving compared with IEEE80 2.11.
  - This new MAC protocol has the ability to make trade-offs between energy and lat ency according to the traffic conditions.