Wireless Media

Anthony D. Joseph
CS 294-1

Lecture 3
September 13, 2000

Outline

- Wireless LAN Design Alternatives
  - David F. Bantz and Frederic J. Bauchot
- Wireless Data: Systems, Standards, Services
  - Antonio DeSimone and Sanjiv Nanda
- Bluetooth

Wireless LAN Design Alternatives

- Worldwide portable product
  - Not all countries have the same ISM bands!
- Low power consumption (physics limits)
- License free operation
  - Major problem with Motorola ALTAIR system
- Reliable, secure, private operation
- Multiple networks should co-exist
  - Think about a classroom
- Easy to manage and fix
  - How to find the rogue transmitter?
- Protection of investment

RF LAN Comparison

	Old RF	IEEE 802.11
Worldwide	No, many stds	Yes
Low Power Mode	No	Partial
License-free	Yes/No	Yes
Secure	Yes/No	Yes
Coexistence	Partial	Partial
Management	Limited	Limited

Design Choices

- Physical Layer: IR or RF?
  - Talk about RF today, IR next week
- Radio Technology: Direct-Sequence or Frequency-Hopping?
- Which frequency range to use?
- CSMA or TDMA?
- Peer-Peer architecture or Base-Station approach?

Physical Layer Alternatives

- IR
  - Simple circuitry, cost-effective, no regulatory constraints, no Rayleigh fading (multipath effects)
- RF
  - more complicated circuitry, regulatory constraints (ISM bands) in the U.S., very susceptible to Rayleigh fading and inter-symbol interference

IR versus RF

	IR	RF
Cost	< $10	< $20
Regulation	None	No license (ISM bands)
Interference	Ambient light	Radiators
Coverage	Spot	Wide area
Performance	Moderate	Depends on Bandwidth
Coexistence	Limited	Possible

Radio Technology

- Spread Spectrum technologies
  - Idea: make transmission look like noise!
  - Frequency Hopping: different channels used at different times
  - Direct-Sequence: Waveform frequency is XOR of information and a psuedorandom chipping sequence
  - Industrial, Scientific, and Medical bands
    - 902-928 MHz (¢¢), 2400-2483.5 MHz ($), 5725-5850 MHz ($$$$)
  - Very complex rules of use (and lots of lawsuits!)
- Non-spread spectrum requires license
  - But, no interference (maybe!)

Frequency Hopping vs Direct Sequence

- Direct Sequence
  - lower cost
  - More precise transmitter-receiver synch required
  - Hard to pick “good” orthogonal codes
- Frequency Hopping
  - higher capacity
  - interference avoidance capability
  - multiple networks can co-exist

ISM Bands Tradeoffs

	915 MHz	2.4 GHz	5.8 GHz
Bandwidth	26 MHz	83.5 MHz	125 MHz
Availability	U.S./Canada	World-wide (sort of)	U.S./Canada
Cost	Low (mass prod Si)	Medium (high vol Si)	High (low vol GaAs)
Transmit range	100%	95%	80%
Usage	High (very crowded)	Medium (getting busy)	Low (empty)

Media Access Control & Network Topology

- Why MAC?
- Same reason as for wired networks
  - Contention/floor control
- Code Division Multiple Access
  - Paper says not beneficial under current regulations, but Metricom chooses different FH sequences
- Frequency Division Multiple Access
  - Paper says inefficient spectrum utilization for bursty traffic, but 802.11 uses multiple (3) frequency channels
- Carrier Sense Multiple Access
  - Suitable for Peer-to-Peer architecture (no prior setup)
- Time Division Multiple Access
  - Base-Station/Remote-Station architecture (BS controls)

CSMA versus TDMA

- CSMA
  - Can be implemented on an Ethernet chipset (and often is – old WaveLAN)
  - Quality of Service issues (uneven delays)
  - IEEE 802.11 approach
- TDMA
  - Simple remote stations (unless remotes can be both master/slave)
  - Supports isochronous traffic
  - High power saving potential thru scheduling
  - Bluetooth approach

Peer to Peer versus Base Station

- Base Station Approach
  - No hidden terminals
  - Higher transmission range (radius vs diameter)
  - Easy expansion
  - Better approach to security
- Peer to Peer
  - Ad-hoc networking
  - Sensor networks

5-minute Break

Wireless Data

- Wireless LANs
  - Shared access to high speed link (1-11 Mb/s)
  - Alternative to wired LANs
  - Slow adoption
- CDPD
  - Contention based packet access on top of analog cellular
  - Used for low bandwidth vertical services
    - Ex: Palm OmniSky modem
- Short Message Service
  - Simple text messaging (>1 Billion messages/year!)
- Mobile IP

Problem Dimensions

- Media Access Control
- Link Layer Retransmissions
- Mobility Management

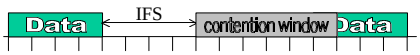
MAC Layer in Wireless Networks

- CSMA/CA
  - similar to CSMA/CD, why is it different?
- Can't simultaneously transmit and hear
- Cellular systems
  - Basestation manages access
- CDPD data channels
  - Unused voice channels are used for data
  - Packet based contention (non-persistent CSMA/CD)

CSMA/CA - IEEE 802.11

- Collision avoidance
  - Can't use detection, so small prob of error
- Based on slotted time algorithm
- After transmission,
  - Wait for Inter-Frame Spacing
  - Calculate random slot within a contention window (CW) in which to transmit
- On collision, increase CW exponentially
  - E.g., 2x to some fixed maximum

CSMA/CA Continued…



- Choice of parameters
  - Slot duration: depends on physical media
  - CW: optimal value depends on number of contending stations
  - Priority: Shortest IFS for ACKs, Priority IFS for control traffic

Augmented CSMA/CA

- MAC level acknowledgements & re-transmissions
- Special RTS/CTS frames for reservation
  - Addresses the hidden-terminal problem
- Different values of IFS to implement levels of priority
  - Can support isochronous traffic

MAC in Cellular Systems

- Basestation manages contention
- Different "send" & "receive" frequencies
  - May also have different timeslots (e.g., TDMA within FDMA)
- Basestation gives busy/idle feedback to terminals
  - This avoids the hidden-terminal problem
- MAC-level re-transmissions

Data Link Layer

- Need for Link-level recovery
- Methods of recovery
  - ARQ
  - Two-level recovery

Need for Link-level Recovery

- Error rate is high on wireless links (1%)
- End-to-end recovery is inefficient
- Paper claims:
  - Link-level retransmissions may actually decrease performance due to TCP timeouts
    - TCP does not perform well when the RTT is not stable
- Paper is wrong!
  - Local work demonstrates that link level recovery is very good [SIGMETRICS99]
  - Paper's result is due to inability to measure internals of the system and reliance on external measurements

ARQ-based Recovery

- Moderate size link-layer frames are retransmitted
- Based on receiver feedback
- Used in TDMA, GSM

Errors in Paper

- Papers' claims of spurious retransmission incorrect
  - Derived from external observation of the system
- We instrumented all layers of the protocol stack (MultiTracer)
  - We found unexpected, but not the expected problems !
  - Very easy to analyze large amounts of data (### hours of traces)
- Inefficient TCP/link layer interactions are rare
  - Depends on implementation of TCP!
  - Link is actually semi-reliable and authors used VJ header compression -> loss of an entire segment
- Other problems related to excessive link buffering
  - More later in the term

Two-level Recovery (CDMA)

- Small physical layer burst
- Re-transmission at link level does partial recovery
- TCP on top of this for complete recovery
- Recovery takes a long time
- What if TCP is running at a higher level too?

Mobility Management

- Circuit-switched cellular systems
  - Make routing decisions before call setup
  - Some systems support dynamic roaming (GSM), others do not (CDPD)
- Packet-switched (IP) world
  - Cannot make routing decisions per packet
- New mix: Packet-switched cellular
  - General Packet Radio Service in GSM

Mobile IP

- Mobile Node discovers Foreign Agent
- Registers care-of address with Home Agent
- Packets to the mobile are forwarded from the home network
- Issues
  - Route optimization
  - Security concerns

Mobile IP Routing

- Triangle routing problem
  - Packets from Correspondent Host are sent to Home Agent, then forwarded to Mobile Node
  - Packets from Mobile Node are sent directly to CH
- What happens when MN and CH are near, but HA is far away?
- Alternative (direct CH-MN) requires CH participation in Mobile IP protocol

Mobile IP Security

- Packets from MN to CH have wrong IP address for local network
  - Address from HA subnet
- Dropped by router security mechanisms
- How to authenticate MN to HA?
  - To FA? CH?
  - What about roaming agreements?

Mobility in Cellular Systems

- Every mobile host has an HLR entry in its home domain
- Mobile hosts have a VLR entry in the foreign domain
- HLR & VLR updates are made as the mobile moves

Bluetooth

- Goals
  - Ad-hoc wireless connectivity for everything!
- Original goal
  - Low-cost replacement for annoying wire between cellphone and headset
- Result: Two modes of operation
  - Point to point (serial wire replacement)
  - Point to multipoint (ad-hoc networking)

Bluetooth Devices

- Cellphones
- Headsets
- PDAs
- Laptops
- Two-way pagers
- Pads, tabs, etc…

Bluetooth Design Specs

- Price: single chip $15-20 today, <$5 in volume
- Frequency: 2.4 GHz ISM band
- Power
  - Transmit: 1 mW (0 dBm)
  - 30 uA sleep, 60 uA hold, 200 uA standby
- Range: 10 meters
- Hybrid DS and FH spread spectrum
  - 1600 hops/second!
- Rate: 721 + 56 Kbit/s per picocell
- Picocells:
  - 8 devices per picocell (3 voice or 7 data max)
  - 10 piconets in coverage area (w/ graceful degradation)
- Simple link layer security (encryption, authentication)

Bluetooth Reality: Frequencies

- ISM band is not the same everywhere!
- Smaller band in Japan
- Defense band in France!
  - How does radio know where it is and local laws?
- Airplanes and FAA
- Conflicts with 802.11
  - More powerful 802.11 stomps on Bluetooth

More Bluetooth Realities

- Cost
  - Hard to produce cheap single-chip radio
    - Mix of analog and digital circuits
  - Not meeting noise margin requirements
  - Currently requires two chips
    - Total redesign of boards/products!
- Ad-hoc networking is hard
  - Still lots of issues about networking protocols
  - First Bluetooth deployments will be P-to-P

More Bluetooth Realities

- Encryption
  - Bluetooth devices use short keys for link layer encryption (export issues)
- Authentication
  - How do two Bluetooth devices exchange keys?
- Push a button on both simultaneously
  - Small window of vulnerability
- What about ceiling mounted basestations?

Bluetooth Summary

- Will be very cool when it arrives
- Will enable low-cost ad-hoc wireless networking
- Lots of problems to be worked out first