Bluetooth Vs. 802.11: state-of-the-art and research challenges

Pravin Bhagwat
ReefEdge, Inc.
pravin@reefedge.com or pravin@acm.org
http://www.cs.umd.edu/~pravin

WINLAB, Rutgers
Oct 28, 2001
**Emerging Landscape**

Licensed spectrum
- **Voice** continues to be the main revenue generator application
- **Data** services are trying to find a foothold

Unlicensed spectrum
- Enterprise environments
- Industry verticals
- Public spaces
- Personal area wireless networks

Potential for wireless carrier entry

Who will be the winner – 802.11 or Bluetooth?
Short Range Wireless: Emerging Landscape

802.11

New developments are blurring the distinction

- 802.11b for PDAs
- Bluetooth for LAN access

Designed for wired Ethernet replacement

Bluetooth

Cordless headset

Designed for cable replacement

- Which option is technically superior?
- What market forces are at play?
- What can be said about the future?
Bluetooth Specifications

- A hardware/software/protocol description
- An application framework

Profiles

Single chip with RS-232, USB, or PC card interface
802.11 Specifications

- Specification of layers below LLC
- Associated management/control interfaces
Bluetooth is a (top down) market driven consortium
  - Business interests take precedence over other considerations
  - Designed primarily for voice; data an afterthought

802.11 is a (bottom up) open standard effort
  - Designed primarily for data; voice an afterthought
  - Good piece of engineering except for WEP
Comparison Axes

- Business
- Application
- Network
- Link
- Radio
- Spectrum
Unlicensed Radio Spectrum

\[ \lambda \]

\begin{align*}
\text{33cm} & \quad \text{26 Mhz} \\
\text{902 Mhz} & \quad \text{928 Mhz} \\
\text{12cm} & \quad \text{83.5 Mhz} \\
\text{2.4 Ghz} & \quad \text{2.4835 Ghz} \\
\text{5cm} & \quad \text{125 Mhz} \\
\text{5.725 Ghz} & \quad \text{5.850 Ghz}
\end{align*}

cordless phones 802.11b Bluetooth
baby monitors 802.11a Microwave oven
Wireless LANs

Spectrum is free, but the right of way is not free
CMU’s spectrum sharing policy

“Computing Services will approach the shared use of the 2.4 GHz radio frequency in the same way that it manages the shared use of the wired network. While we will not actively monitor use of the airspace for potential interfering devices, we will seek out the user of a specific device if we find that it is actually causing interference and disrupting the campus network. In these cases, Computing Services reserves the right to restrict the use of all 2.4 GHz radio devices in university-owned buildings and all outdoor spaces on the Carnegie Mellon Campus”.

http://www.cmu.edu/computing/wireless/airspace.html
Spectrum War: Status today

Enterprise 802.11 Network

Wireless Carrier

Public 802.11
Spectrum War: Next phase of evolution

Enterprise 802.11 Network

Wireless Carrier

Public 802.11

- Market consolidation
- Entry of Wireless Carriers
- Entry of new players
- Footprint growth
Spectrum War: Eventual Steady State

- Enterprise 802.11 Network
- Wireless Carrier
- Public 802.11

- Virtual Carrier

- Emergence of virtual carriers
- Roaming agreements

10/29/2001
Pravin Bhagwat
Comparison Axes

- Business
- Application
- Network
- Link
- Radio
- Spectrum
Design considerations

- high bandwidth
- conserve battery power
- cost < $10

Goal
Radio: cost, power, range tradeoff

- Transmit power: \( \alpha d^n \)
- Battery life: \( \alpha \frac{1}{d^n} \)
- Access points (N): \( \alpha \frac{1}{d^2} \)

- Tradeoff between battery life & the cost of the overall system

\[ \text{battery life} \propto N^{0.5n} \]

for \( n = 4 \):
\[ 4x \quad 2x \]
Bluetooth Radio

- Low Cost
  - Single chip radio (minimize external components)
  - Today’s technology
  - Time division duplex

- Low Power
  - Standby modes: Sniff, Hold, Park
  - Low voltage RF
Radio architecture: 802.11b

Typically SiGe or GaAs

Analog

IF D/A

mixing

modulation

channel coding

CMOS

DSP

oscillators, PA filters
oscillators, LNA filters

demodulation

channel decoding

baseband signal

A/D IF

mixing
Radio architecture: Bluetooth

- Demodulation
- Channel decoding
- Mixing
- A/D conversion
- Baseband signal
- CMOS oscillators, LNA, filters
- Channel coding
- Mixing
- D/A conversion
- Baseband signal
- CMOS

IF

Analog

DSP
### Transmit power & receiver sensitivity

<table>
<thead>
<tr>
<th>Power Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 dBm</td>
<td>Tx power</td>
</tr>
<tr>
<td>-20</td>
<td>Rx power @ 10 cm</td>
</tr>
<tr>
<td>-70</td>
<td>Rx power @ 10m</td>
</tr>
<tr>
<td>-91</td>
<td>Noise floor</td>
</tr>
</tbody>
</table>

C/I = 21 dB
Comparison Axes

- Business
- Application
- Network
- Link
- Radio
- Spectrum
**Bluetooth Physical link**

- **Point to point link**
  - master - slave relationship
  - radios can function as masters or slaves

- **Piconet**
  - Master can connect to 7 slaves
  - Each piconet has max capacity (1 Mbps)
  - hopping pattern is determined by the master
Scatternet
**802.11 Architecture**

Basic Service Set (BSS): a set of stations which communicate with one another

- **Independent Basic Service Set (IBSS)**
  - only direct communication possible
  - no relay function

- **Infrastructure Basic Service Set (BSS)**
  - AP provides
    - connection to wired network
    - relay function
    - stations not allowed to communicate directly
Extended Service Set

ESS: a set of BSSs interconnected by a distribution system (DS)

- ESS and all of its stations appear to be a single MAC layer
- AP communicate among themselves to forward traffic
- Station mobility within an ESS is invisible to the higher layers
**Bluetooth MAC Layer**

FH/TDD

\[ \lambda \text{ sec} \]

\[ 625 \text{ hops/sec} \]

1600 hops/sec
Physical Link Types

- Synchronous Connection Oriented (SCO) Link
  - slot reservation at fixed intervals

- Asynchronous Connection-less (ACL) Link
  - Polling access method
**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

- direct access if medium is free $\geq$ DIFS
Comparison Axes

- Business
- Application
- Network
- Link
- Radio
- Spectrum
The Connectivity Problem

The same problem is being faced by all market segments and many solutions have been tried:

- PoE
- L2TP, PPTP
- GSM – smart card auth.
- EAP + 802.1x
- Mobile IP
- AAA
- IPSEC
- MS passport – Web sign on

Cable/DSL  3G  WLAN Bluetooth
Basic network access issues

**Authentication**
- Protect identity theft

**Access Control**
- Prevent masquerading, modification, and unauthorized access

**Accounting**
- Accurate usage monitoring

**Service Provider’s concerns**
- No fraud
- Scalability
- Efficiency
- Low cost

**Equipment vendor’s concerns**
- No queues
- No fraud
- Scalability
- Efficiency
- Low cost

**User concerns**
- Anonymity
- Confidentiality
- Audit trails

- No red tape
- No queues
- No fraud

10/29/2001  Pravin Bhagwat
Connection establishment & Security

Goals
- Authenticated access
  - Only accept connections from trusted devices
- Privacy of communication
  - Prevent eavesdropping

Constraints
- Processing and memory limitations
  - $10 headsets, joysticks
- Cannot rely on PKI
- Simple user experience

Diagram:
- Master
  - LMP_host_conn_req
  - Security procedure
  - LMP_setup_complete
- Slave
  - LMP_Accepted
  - LMP_setup_complete

Paging
**Authentication**

- Authentication is based on link key (128 bit shared secret between two devices)
- How can link keys be distributed securely?

![Diagram showing authentication process with challenge, response, and accepted arrows between two devices linked by a link key.]
Pairing (key distribution)

- Pairing is a process of establishing a trusted secret channel between two devices (construction of initialization key $K_{\text{init}}$)
- $K_{\text{init}}$ is then used to distribute unit keys or combination keys

**Diagram:**
- PIN + Claimant address to Verifier
- Random number to Claimant
- Challenge to Verifier
- Response to Claimant
- Accepted to Verifier
- $K_{\text{init}}$ to both sides
Wired Equivalent Privacy (WEP)

- **Design Objectives**
  - Confidentiality
    - Prevent others from eavesdropping traffic
  - Data Integrity
    - Prevent others from modifying traffic
  - Access Control
    - Prevent unauthorized network access

Unfortunately, WEP fails on all three counts
Comparison Axes

- Business
- Application
- Network
- Link
- Radio
- Spectrum
Synchronization and Push

- More bits over the air
- Utilization of unused capacity during non-busy periods
- Higher barrier for switching service providers
Cell phone as an IP gateway

- More bits over the air
- Enhanced user experience
  - Palmpilot has a better UI than a cell phone
- Growth into other vertical markets
Voice Call Handoff

Threat or opportunity?

- More attractive calling plans
- Alleviate system load during peak periods
- Serve more users with fewer resources
Bluetooth Value chain

Conspicuously missing Wireless Carriers

Stack providers

Integrators

Software vendors

Silicon

Radio
Biggest challenges facing Bluetooth

- Interoperability
  - Always a challenge for any new technology
- Hyped up expectations
- Out of the box ease of use
- Cost target $5
- Critical mass
- RF in silicon
802.11 Current Status

- **802.11i** security
- **802.11f** Inter Access Point Protocol
- **802.11e** QoS enhancements

### Phy Layers
- **DSSS**, **FH**, **IR**
- **OFDM**

### MAC Layers
- **MAC Mgmt**
- **WEP**
- **LLC**

### 802.11 Standards
- **802.11b**: 5, 11 Mbps
- **802.11a**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11g**: 20+ Mbps

**802.11i** security

**802.11f** Inter Access Point Protocol

**802.11e** QoS enhancements

**802.11b** 5, 11 Mbps

**802.11a** 6, 9, 12, 18, 24, 36, 48, 54 Mbps

**802.11g** 20+ Mbps
# Bluetooth Vs. 802.11: MAC issues

<table>
<thead>
<tr>
<th></th>
<th>Bluetooth</th>
<th>802.11</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Method</strong></td>
<td>TDD</td>
<td>CSMA</td>
</tr>
<tr>
<td></td>
<td>Good for voice, but difficult for data</td>
<td>Good for data, but difficult for voice</td>
</tr>
<tr>
<td><strong>Robustness to</strong></td>
<td>ARQ</td>
<td>ARQ</td>
</tr>
<tr>
<td><strong>interference</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hidden nodes</strong></td>
<td>Not an issue</td>
<td>RTS/CTS</td>
</tr>
<tr>
<td><strong>Power Management</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Power Control</strong></td>
<td>Possible</td>
<td>Not possible</td>
</tr>
<tr>
<td><strong>Paging</strong></td>
<td>Possible</td>
<td>Possible, but not yet defined</td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
<td>Limited</td>
<td>Stable at high loads</td>
</tr>
<tr>
<td><strong>Future safe?</strong></td>
<td>Not sure</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# Bluetooth Vs. 802.11: Market issues

<table>
<thead>
<tr>
<th></th>
<th>Bluetooth</th>
<th>802.11</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost</strong></td>
<td>Potential for low cost implementation exists but the market size will eventually determine the price point</td>
<td>Technology advances and market growth can reduce cost, even if tight single integration is not achieved in the near term</td>
</tr>
<tr>
<td><strong>Market size</strong></td>
<td>Potentially huge if every consumer electronic device is Bluetooth enabled</td>
<td>It is unlikely that 802.11 will penetrate the cosumer electronic device market in the near future</td>
</tr>
<tr>
<td><strong>Form factor</strong></td>
<td>Smaller due to single chip integration</td>
<td>Multi chip solution</td>
</tr>
<tr>
<td><strong>Power consumption</strong></td>
<td>Lower due to low power transmitter and tight integration</td>
<td>Will reduce in the future</td>
</tr>
<tr>
<td><strong>Interoperability</strong></td>
<td>The biggest problem of Bluetooth at present</td>
<td>802.11 is a more mature technology</td>
</tr>
<tr>
<td><strong>Applications</strong></td>
<td>Still looking for a killer app.</td>
<td>TCP/IP</td>
</tr>
</tbody>
</table>
Concluding remarks

Future of Bluetooth

- Bluetooth is ideal for cable replacement
- Initial applications of Bluetooth will exploit its point-to-point or point-to-multipoint connectivity feature
- Attempts to turn it into a LAN technology will face very tough competition from 802.11
- Multi-hop over Bluetooth is a challenging research problem
- Higher chance of success in Europe and Asia

802.11

- Will continue to grow in
  - Public spaces, home, industry vertical, and enterprise market
- 802.11 will provide a viable alternative to 3G in public places
Thank You