Embedded wireless networking using Bluetooth & 802.11: state-of-the-art and research challenges

Pravin Bhagwat
pravin@acm.org
http://www.winlab.rutgers.edu/~pravin

16th ACM Supercomputing
New York, NY
June 22, 2001
Bluetooth

- A cable replacement technology
- 1 Mb/s symbol rate
- Range 10+ meters
- Single chip radio + baseband
  - at low power & low price point ($5)

Why not use Wireless LANs?
- power
- cost
802.11

- Replacement for Ethernet
- Supported data rates
  - Current: 11, 5.5, 2, 1 Mbps
  - Future: 20+ Mbps in 2.4 GHz and up to 54 Mbps in 5.7 GHz band
- Range
  - Indoor 20 - 25 meters
  - Outdoor: 50 – 100 meters
- Transmit power up to 100 mW
- Cost:
  - Chipsets $ 35 – 50
  - AP $200 - $1000
  - PCMCIA cards $100 - $150
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?

P. Bhagwat
Questions I hope to answer

- What are the key design differences between Bluetooth and 802.11?
  - At PHY, MAC, and System level
- How do Bluetooth and 802.11 compare?
  - Cost, Range of communication, performance
- Why is Bluetooth supposed to be low cost and low power? Can 802.11 achieve the same price and performance target?
- Is Bluetooth more secure than 802.11?
- Reality Vs. hype
- Can the two systems co-exist?
## Tutorial Overview

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:00 – 3:00 pm</td>
<td>Introduction, Bluetooth applications,</td>
</tr>
<tr>
<td></td>
<td>basic radio concepts, Bluetooth RF</td>
</tr>
<tr>
<td>3:00 - 3:45 pm</td>
<td>Bluetooth Baseband</td>
</tr>
<tr>
<td>3:45 - 4:15 pm</td>
<td>LMP, Security, Scatternets</td>
</tr>
<tr>
<td>4:15 - 4:30 pm</td>
<td><em>Break</em></td>
</tr>
<tr>
<td>4:30 - 5:30 pm</td>
<td>802.11 specifications overview, PHY &amp; MAC</td>
</tr>
<tr>
<td>5:30 - 6:00 pm</td>
<td>Bluetooth &amp; 802.11 comparison, Conclusion</td>
</tr>
</tbody>
</table>
New Applications
Synchronization

User benefits

- Automatic synchronization of calendars, address books, business cards
- Push button synchronization
- Proximity operation
Cordless Headset

User benefits
- Multiple device access
- Cordless phone benefits
- Hands free operation
Usage scenarios examples

- Data Access Points
- Synchronization
- Headset
- Conference Table
- Cordless Computer
- Business Card Exchange
- Instant Postcard
- Computer Speakerphone
Bluetooth Specifications
Bluetooth Specifications

A hardware/software/protocol description
An application framework
Interoperability & Profiles

- Represents default solution for a usage model
- Vertical slice through the protocol stack
- Basis for interoperability and logo requirements
- Each Bluetooth device supports one or more profiles
Bluetooth Radio Specification

Applications

Data

Control

RF

Baseband

Link Manager

L2CAP

RFCOMM

SDP

IP

Audio

P. Bhagwat
Propagation characteristics are different in each frequency band.
**Unlicensed Radio Spectrum**

<table>
<thead>
<tr>
<th>Frequency Range</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>902-928 MHz</td>
<td>cordless phones, baby monitors, Wireless LANs</td>
</tr>
<tr>
<td>2.4-2.4835 GHz</td>
<td>802.11, Bluetooth, Microwave oven</td>
</tr>
<tr>
<td>5.725-5.785 GHz</td>
<td>unused</td>
</tr>
</tbody>
</table>

λ: 33 cm, 12 cm, 5 cm
Bluetooth radio link

- frequency hopping spread spectrum
  - 2.402 GHz + k MHz, k=0, …, 78
  - 1,600 hops per second
- GFSK modulation
  - 1 Mb/s symbol rate
- transmit power
  - 0 dbm (up to 20dbm with power control)
**Design considerations**

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

Goal

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

Noise, interference

Recovered data signal
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

- SiGe or GaAs
- Analog
- Digital
- CMOS

P. Bhagwat
Radio architecture: Bluetooth
Receiver sensitivity & range of comm.

- BT
- 802.11

- C/I > 21 dB
- C/I > 12 dB
Radio: cost, power, range tradeoff
Review of basic concepts
Understanding wireless communication

• How does signal propagate?
• How much attenuation take place?
• How does signal look like at the receiver?
Radio Propagation

Three basic propagation mechanisms

- **Reflection**: $\lambda \ll D$
- **Diffraction**: $\lambda \approx D$
- **Scattering**: $\lambda \gg D$

- At 2.4 Ghz, leaves, lamp-posts can cause scattering
**dB (relative measure)**

- **Bill**: $100B, $10^{11}$, 40 dB, 10,000 times
- **Steve**: $10M, $10^7$, 30 dB, 1,000 times
- **Grad**: $10K, $10^4$,

\[ dB = 10 \log (\text{times}) \]

- $10,000 \times 1,000 \text{ times} = 10,000,000 \text{ times}$
- $40 \text{ dB} + 30 \text{ dB} = 70 \text{ dB}$
**Path loss in dB**

Path loss from source to d2 = 70dB

\[
\text{dB} = 10 \log \left( \frac{P_1}{P_2} \right)
\]
dBm (absolute measure of power)

- 10 W = 40 dBm
- 1 mW = 0 dBm
- 1 µW = -30 dBm

\[ \text{dBm} = 10 \log \left( \frac{P_1}{1 \text{mW}} \right) \]
Radio propagation: path loss

path loss = 10 \log \left( \frac{4\pi r^2}{\lambda} \right) \quad r \leq 8m

= 58.3 + 10 \log \left( \frac{r^{3.3}}{8} \right) \quad r > 8m
Radio Propagation: Fading and multipath

Fading: rapid fluctuation of the amplitude of a radio signal over a short period of time or travel distance

Effects of multipath

• Fading
• Varying doppler shifts on different multipath signals
• Time dispersion (causing inter symbol interference)
Baseband

- Applications
- Control
- Data
- Audio
- L2CAP
- Link Manager
- Baseband
- RF
- SDP
- RFCOMM
- IP
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
Connection Setup

- Inquiry - scan protocol
  - to learn about the clock offset and device address of other nodes in proximity
Inquiry on time axis

Slavel1

Master

Slave2

Inquiry hopping sequence
**Piconet formation**

- **Page - scan protocol**
  - to establish links with nodes in proximity
Addressing

- Bluetooth device address (BD_ADDR)
  - 48 bit IEEE MAC address

- Active Member address (AM_ADDR)
  - 3 bits active slave address
  - all zero broadcast address

- Parked Member address (PM_ADDR)
  - 8 bit parked slave address
Piconet channel

FH/TDD

f1  f2  f3  f4  f5  f6

m

S1

625 λsec

1600 hops/sec
**Multi slot packets**

Data rate depends on type of packet
Physical Link Types

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

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

Diagram showing the allocation of SCO and ACL connections over time.
Packet Types

Control packets

- ID*
- Null
- Poll
- FHS
- DM1

Data/voice packets

Voice

- HV1
- HV2
- HV3
- DV

Data

- DM1
- DM3
- DM5
- DH1
- DH3
- DH5
Packet Format

72 bits 54 bits 0 - 2744 bits

Access code Header Payload

Voice
No CRC
No retries
FEC (optional)

header Data CRC

ARQ
FEC (optional)

625 µs

master
slave

P. Bhagwat
Access Code

Access code

72 bits

Header

Payload

Purpose

- Synchronization
- DC offset compensation
- Identification
- Signaling

Types

- Channel Access Code (CAC)
- Device Access Code (DAC)
- Inquiry Access Code (IAC)
Packet Header

54 bits

Access code | Header | Payload

Purpose

- Addressing (3) → Max 7 active slaves
- Packet type (4) → 16 packet types (some unused)
- Flow control (1)
- 1-bit ARQ (1) → Broadcast packets are not ACKed
- Sequencing (1) → For filtering retransmitted packets
- HEC (8) → Verify header integrity

---

Total 18 bits

Encode with 1/3 FEC to get 54 bits
## Data Packet Types

<table>
<thead>
<tr>
<th></th>
<th>Symmetric</th>
<th>Asymmetric</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DM1</strong></td>
<td>108.8</td>
<td>108.8</td>
</tr>
<tr>
<td><strong>DM3</strong></td>
<td>258.1</td>
<td>387.2</td>
</tr>
<tr>
<td><strong>DM5</strong></td>
<td>286.7</td>
<td>477.8</td>
</tr>
<tr>
<td><strong>DH1</strong></td>
<td>172.8</td>
<td>172.8</td>
</tr>
<tr>
<td><strong>DH3</strong></td>
<td>390.4</td>
<td>585.6</td>
</tr>
<tr>
<td><strong>DH5</strong></td>
<td>433.9</td>
<td>723.2</td>
</tr>
</tbody>
</table>
Inter piconet communication

Cordless headset

Cell phone

mouse

Cordless headset

Cell phone

Cordless headset

Cell phone

P. Bhagwat
Scatternet, scenario 2

How to schedule presence in two piconets?

Forwarding delay?

Missed traffic?
TDD, frequency hopping physical layer
Device inquiry and paging
Two types of links SCO and ACL links
Multiple packet types (multiple data rates with and without FEC)
Link Manager Protocol

Setup and management of Baseband connections

- Piconet Management
- Link Configuration
- Security
Piconet Management

- Attach and detach slaves
- Master-slave switch
- Establishing SCO links
- Handling of low power modes (Sniff, Hold, Park)
Low power mode (hold)

Hold offset

Slave

Hold duration

Master
**Low power mode (Sniff)**

- Sniff offset
- Sniff duration
- Sniff period

- Traffic reduced to periodic sniff slots

---

P. Bhagwat
**Low power mode (Park)**

- Power saving + keep more than 7 slaves in a piconet
- Give up active member address, yet maintain synchronization
- Communication via broadcast LMP messages
**Link Configuration**

- Quality of service
  - Polling interval
  - Broadcast repetition
- Power control
- Packet type negotiation
- Multi-slot packets

![Diagram showing Master and Slave with Paging and LMP_quality_of_service and LMP_not_Accepted messages]
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
Authentication

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

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

![Diagram of Pairing Process]

- PIN + Claimant address
- Random number
  - Challenge
  - Response
  - Accepted

- PIN + Claimant address
- Random number

P. Bhagwat 58
Encryption

- Encryption Key (8 – 128 bits)
- Derived from the Link key
## Link Manager Protocol Summary

- Piconet management
- Link configuration
  - Low power modes
  - QoS
  - Packet type selection
- Security: authentication and encryption
L2CAP provides

- Protocol multiplexing
- Segmentation and Re-assembly
- Quality of service negotiation
Bluetooth Service Discovery Protocol

RF
Baseband
Link Manager
L2CAP
Audio
SDP
RFCOMM
IP
Data
Applications
Serial Port Emulation using RFCOMM

Serial Port emulation on top of a packet oriented link
• Similar to HDLC
• For supporting legacy apps
LAN access point profile

Why use PPP?
- Security
  - Authentication
  - Access control
- Efficiency
  - Header and data compression
- Auto-configuration
- Lower barrier for deployment

IP
PPP
RFCOMM
L2CAP
Baseband
Bluetooth Network Encapsulation Protocol (BNEP) provides emulation of Ethernet over L2CAP

- BNEP defines
  - a frame format which includes IEEE 48 bit MAC addresses
  - A method for encapsulating BNEP frames using L2CAP
- Option to compress header fields to conserve space
- Control messages to activate filtering of messages at Access Point
802.11 specifications overview
802.11 Specifications

- Specification of layers below LLC
- Associated management/control interfaces
802.11 Specifications

MAC sublayer

PLCP Sublayer

PMD Sublayer

MAC Layer Management

PHY layer Management

MAC Service Interface

PHY Service Interface

MAC Mgmt Service Interface

PHY Mgmt Service Interface

LLC

MAC

WEP

MAC Mgmt

MIB

PHY

DSSS

FH

IR

OFDM
802.11 Specifications

**PHY Layer**
- FH (clause 14)
- DSSS (clause 15)
- Infrared (clause 16)
- OFDM (clause 17)
- High rate DSSS (clause 18)

**MAC Sublayer**
- MAC framing (clause 7)
- MAC operation (clause 9)
- WEP (clause 8)
- State Machines (Annex C)

**PHY Management**
- MIBs (Annex D)

**MAC Management**
- Protocols (clause 11)
- State Machines (Annex C)
- MIBs (Annex D)

**MAC Service Interface** (clause 6)

**PHY Service Interface** (clause 12)

**MAC Mgmt Service Interface** (clause 10)

**PHY Mgmt Service Interface** (clause 13)

**LLC**
802.11 System 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
802.11 PHY

Applications

Control

PHY

DSSS  FH  IR  OFDM

MAC Mgmt

MAC

WEP

LLC

P. Bhagwat
802.11 PHY

Sender

MAC Protocol Data Unit (MPDU)

PLCP header

MAC Protocol Data Unit (MPDU)

Physical Media Dependent (PMD) layer

Frequency Hopping Spread Spectrum (FHSS) PHY
1, 2 Mbps

Higher rate (DSSS) PHY
20+ Mbps

802.11g

Direct Sequence Spread Spectrum (DSSS) PHY
1, 2 Mbps

High rate (DSSS) PHY
11, 5.5 Mbps

802.11b

5.7 GHz

Physical Media Dependent (PMD) layer

PMD layer

Infrared (IR) PHY
1,2 Mbps

Orthogonal Frequency Division Multiplexing (OFDM) PHY
6,9,12,18,24,36,48,54 Mbps

802.11a

2.4 GHz

802.11 PHY
Baseband signal is spread using Barker word (10 dB processing gain)
Spread signal occupies approximately 22 Mhz bandwidth
Receiver recovers the signal by applying the same Barker word
DSSS provides good immunity against narrowband interferer
CDMA (multiple access) capability is not possible
- **Direct sequence spread spectrum**
  - Each channel is 22 Mhz wide
- **Symbol rate**
  - 1 Mb/s with DBPSK modulation
  - 2 Mbps with DQPSK modulation
  - 11, 5.5 Mb/ps with CCK modulation
- **Max transmit power**
  - 100 Mw
802.11 MAC

Applications

Control

MAC

WEP

LLC

MAC Mgmt

PHY

DSSS FH IR OFDM

MIB
802.11 MAC

- **Carrier sensing (CSMA)**
  - Rules:
    - carrier ==> do not transmit
    - no carrier ==> OK to transmit
  - But the above rules do not always apply to wireless.
    - Solution: RTS/CTS
- **Collision detection (CD)**
  - Does not work over wireless
  - Therefore, use collision avoidance (CA)
    - random backoff
    - priority ack protocol
**802.11 MAC protocol: CSMA/CA**

- Use CSMA with collision Avoidance
  - Based on carrier sense function in PHY called Clear Channel Assessment (CCA)
- Reduce collision probability where mostly needed
- Efficient backoff algorithm stable at high loads
- Possible to implement different fixed priority levels
802.11 MAC: Contention window

For DSSS PHY
Slot time = 20 µs
CSMA/CA + ACK protocol

- Defer access based on carrier sense
- Direct access when medium is sensed free longer than DIFS
- Receiver of directed frames to return an ACK immediately when CRC is correct
  - When no ACK received then retransmit frame after a random backoff
Problems with carrier sensing

Exposed terminal problem

Z is transmitting to W

Y will not transmit to X even though it cannot interfere

Presence of carrier $\Rightarrow$ hold off transmission
Problems with carrier sensing

Hidden terminal problem

W finds that medium is free and it transmits a packet to Z

no carrier $\Rightarrow$ OK to transmit
Solving Hidden Node problem with RTS/CTS

- listen RTS
- wait _long enough_ for the requested station to respond with CTS
- if (timeout) then ready to transmit

- listen CTS
- wait _long enough_ for the transmitter to send its data

listen RTS ==> transmitter is close to me
listen CTS ==> receiver is close to me

Note: RTS/CTS does not solve exposed terminal problem. In the example above, X can send RTS, but CTS from the responder will collide with Y’s data.
802.11 MAC sublayer Management
A station can first scan the network and discover the presence of BSS in a given area.

Scanning:
- Passive: listen for beacons on each channel
- Active: send probe and wait for response on each channel

Beacon and probe response packets contain:
- AP timing information,
- Beacon period,
- AP capability information,
- SSID,
- PHY parameter set,
- Traffic Indication Map (TIM)
- SSID (Service set identifier) identifies an ESS or IBSS
MAC Mgmt : Authentication & Association

With respect to an access point, a station can be in one of the following three states:
- Unauthenticated/Unassociated
- Authenticated/Unassociated
- Authenticated/Associated

A station can pre-authenticate with several access points in advance to speedup roaming.

A station can be associated with only one AP at a given time.

Association state is used by the distribution system to figure out the current location of the station within the ESS.
A station which is synchronized with an AP clock can wake up periodically to listen for beacons.

Beacon packets contain Traffic Indication Map (TIM), a bit vector, which indicates whether a station has a packet buffered at AP.

The station sends a PS-Poll message to the AP asking the AP to release buffered packets for the station.

All broadcast and multicast frames are transmitted following beacons with DTIM flag set.
### 802.11 Frame Format

<table>
<thead>
<tr>
<th>Frame control</th>
<th>Duration ID</th>
<th>Addr 1</th>
<th>Addr 2</th>
<th>Addr 3</th>
<th>Seq ctrl</th>
<th>Addr 4</th>
<th>Frame body</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>0 - 2312</td>
</tr>
</tbody>
</table>

- 802.11 frame has more fields than other media type frames
- 30 bytes frame header appears too long!
- All fields are not present in all frames
Frame Control Field

<table>
<thead>
<tr>
<th>bytes</th>
<th>bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2 2 4 1 1 1</td>
</tr>
</tbody>
</table>

- Prot Ver
- Type
- Subtype
- To DS
- From DS
- More Frag
- Retry
- Pwr Mgmt
- More Data
- WEP
- Order

Mgmt: 00
Control: 01
Data: 10
Reserved: 11

- Association req
- Association resp
- Re-association req
- Re-association resp
- Probe req
- Probe resp
- Beacon
- Announcement Traffic
  - Indication Request (ATIM)
- Disassociation
- Authentication
- De-authentication

- Power save (PS)-poll
- Request to Send (RTS)
- Clear to send (CTS)
- Acknowledgement (ACK)
- Contention free (CF)-END
- CF-END + CF-ACK
- Data
- Data + CF+ACK
- Data + CF-Poll
- Data + CF-ACK + CF-Poll
- Null
- CF-ACK
- CF-Poll
- CF-ACK + CF-Poll
802.11 Privacy and Authentication
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

Provide same level of security as a physical wire
802.11 security design goals

**Authentication**
- Protect identity theft

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

**Accounting**
- Accurate usage monitoring

**No red tape**

**No queues**

**Anonymity**

**Confidentiality**

**No fraud**

**Scalability**

**Efficiency**

**Low cost**

**Audit trails**

**Service Provider’s concerns**

**Equipment vendor’s concerns**

**User concerns**

Unfortunately, WEP fails on all three counts
WEP design: adding privacy

A secret key is shared between a sender and a receiver
- Using the secret key the sender generates a random key stream
- XOR plain text with the random key stream
- XOR the cipher text with the same random key stream to recover the plain text
- An eavesdropper cannot compute the plain text by inspecting the cipher text
- New key streams are refreshed periodically
  - Use initialization vector (IV) in conjunction with shared key
  - Transmit IV in clear text along with the cipher text
The problem is that cipher text can be modified without any knowledge of the key:
- Just flip some bits in the cipher text
- After decrypting the cipher text, receiver will not know that the plain text has been corrupted

Solution:
- Compute 32 bit CRC of plain text and append it with plain text before generating the cipher text
- If cipher text is modified, CRC check will fail and the frame will be discarded
**WEP design: adding Authentication**

Summary
- Shared secret keys are distributed out of band
- AP sends a challenge to the station
- Station responds with a WEP encrypted packet
- AP verifies station’s response

Sender

K

Distributed out of band

K

AP

Sender

AP

shared key

Challenge (Nonce)

Response (Nonce encrypted with secret key)

Decrypted response OK?
Where is the problem?

Problem #1: improper use of stream ciphers

- Two messages should never be encrypted using the same key streams.
- Suppose $P_1$ and $P_2$ are encrypted using the same key stream.
  - $C_1 = P_1 \oplus b$
  - $C_2 = P_2 \oplus b$
- Adversary can compute $C_1 + C_2 = P_1 + b + P_2 + b$
  - $= P_1 + P_2$
- Usually XOR of two plain texts is enough to recover both plain texts.
- Moreover, if one plain text is known other can be computed trivially.
Key stream reuse in WEP

- Key stream is a function of secret key and initialization vector
- IV vector is only 24 bits long; since there are only 16 million combinations, eventually key streams will be recycled
- Since IV vector is transmitted in clear text, Key stream reuse is easy detect by passive eavesdropping
- An eavesdropper can record all instances of key stream reuse
  - Require 1K * 16 million = 16 GB space
- Worse yet, most 802.11 cards when reset start counting IV from 0
  - so, key streams are recycled more frequently
Possible attack: Message decryption

- Inject known plain text in the network by e-mail spamming, or ping
- Passively record encrypted packets
- By computing XOR of known plain text with encrypted packet, it is possible to compute the RC4 key stream that was used to encrypt the known plain text
- Build a dictionary of key streams
  - Map each value to IV to its associated key stream
- Once this dictionary is built, any packet can be decrypted
  - Record the packet
  - Inspect the IV
  - Pull out the key stream associated with the observed IV from the dictionary
  - XOR the key stream with the encrypted packet and obtain the plain text
- The same dictionary can also be used to inject any message in the network
Possible attack: Breaking Authentication

The previous attack relies on finding a known plain text and its encrypted version to compute the key stream. By snooping 802.11 Authentication protocol, this pair can be collected for free. Using this key stream, an adversary station can respond to any new challenge from the AP!
Integrity check value (ICV) is good at detecting random bit errors, not intentional modifications to the packet.

An adversary can modify an encrypted packet such that those changes cannot be detected by CRC test at the receiver. This is possible because encryption function (XOR) as well as CRC are both linear operations.

\[(M, c(M)) \oplus (R, c(R)) = (M \oplus R, c(M \oplus R))\]

The modified message after decryption will pass the CRC test!
WEP current status

- Note that attacks don’t try to deduce the key. Knowledge of key stream is enough to launch all sorts of attacks

- **Possible Solutions**
  - Long IV’s which never repeat for the lifetime of the shared secret
  - Replace CRC by a strong message authentication code which depends on the key and IV

- WEP2 addresses the first problem, but not the other

- A recent paper by Fluhrer, Mantin, and Shamir has discovered many inherent weaknesses in RC4 stream cipher. They have shown that RC4 is completely insecure when used used in a way prescribed by WEP, in which a fixed secret key is concatenated with known IV modifiers.

- 802.11i working group is now looking into using AES instead of WEP. AES will fix both problems of WEP
  - AES is a block cipher
  - AES includes a strong keyed message authentication code

- Bill Arbaugh’s web-page (http://www.cs.umd.edu/~waa/wireless.html) is good source of info on this topic.
802.11 current status

- **802.11i**
  - Security

- **802.11f**
  - Inter Access Point Protocol

- **802.11e**
  - QoS enhancements

---

**PHY**

- **DSSS**
- **FH**
- **IR**

- **OFDM**

---

**MAC**

- **Mgmt**

---

**MAC**

- **WEP**
  - Inter Protocol

---

**MIB**

---

**802.11b**

- 5.11 Mbps

---

**802.11g**

- 20+ Mbps

---

**802.11a**

- 6,9,12,18,24 Mbps
- 36,48,54 Mbps

---

P. Bhagwat 102
Bluetooth is a (top down) market driven consortium
- Business interests take precedence over technical considerations
- Designed primarily for voice; data an afterthought

802.11 is a (bottom up) open standard effort
- Good piece of engineering except for WEP
- Designed primarily for data; voice an afterthought
Bluetooth Vs. 802.11: Radio issues

Radio is typically the most costly component in a wireless network interface

- **Bluetooth** radio is (will be) inexpensive because
  - It is a frequency hopper (which is relatively easy to build)
  - Its sensitivity is poor
  - It uses very simple modulation technique (GFSK) (requires less silicon)
  - It is possible to package both baseband and radio in a single chip
  - Potentially market for Bluetooth radios is (will be?) large if every mobile phone vendors decide to embed Bluetooth in their products

- **802.11** DSSS radios are costly today, but
  - if market for 802.11 continues to grow, their price may become competitive to Bluetooth
  - DSSS radios are superior to Bluetooth in terms of range, speed, BER performance
  - Due to better range, it may be cheaper to cover an area with 802.11
  - 802.11 can be operated at 0 dBm to reduce power consumption
802.11 Market drivers: Business Users

Trend #1: Need for wireless access inside office building

Trend #2: Growth of Wireless LAN access in hotels, airports, etc.

Trend #3: Replacement of wired phones with VOIP over wireless phones

Trend #4: Dual mode phones

Traveling

Inside office
Bluetooth Value chain

Conspicuously missing

Wireless Carriers

Stack providers

Integrators

Software vendors

Silicon

Radio

<image>
**Bluetooth Vs. 802.11: Market Issues**

<table>
<thead>
<tr>
<th></th>
<th>Bluetooth</th>
<th>802.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</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>Market size</td>
<td>Potentially huge if every consumer electronic device is Bluetooth enabled</td>
<td>It is unlikely that 802.11 will penetrate the consumer electronic device market in the near future</td>
</tr>
<tr>
<td>Form factor</td>
<td>Smaller due to single chip integration</td>
<td>Multi chip solution</td>
</tr>
<tr>
<td>Power consumption</td>
<td>Lower due to low power transmitter and tight integration</td>
<td>Will reduce in the future</td>
</tr>
<tr>
<td>Interoperability</td>
<td>The biggest problem of Bluetooth at present</td>
<td>802.11 is a more mature technology</td>
</tr>
<tr>
<td>Applications</td>
<td>Still looking for a killer app.</td>
<td>TCP/IP</td>
</tr>
</tbody>
</table>
Concluding remarks

- Will Bluetooth survive?
  - 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 a tough competition from 802.11
  - Scatternet is still a difficult technical 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