

COEN-4720 Embedded Systems Design

Lecture 08

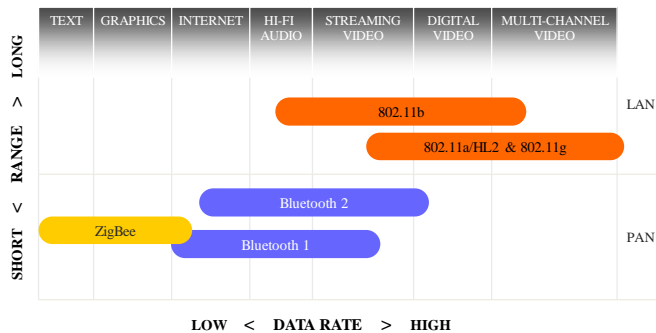
Wireless Technologies: BlueTooth

Cristinel Ababei
Dept. of Electrical and Computer Engineering
Marquette University

1

Wireless Technologies: BlueTooth

- WiFi
- **Bluetooth**
- Cellular
- 3G (3rd Generation)
- UWB (Ultra Wide Band)
- FSO (Free Space Optics)
- WiMAX
- ZigBee
- ...



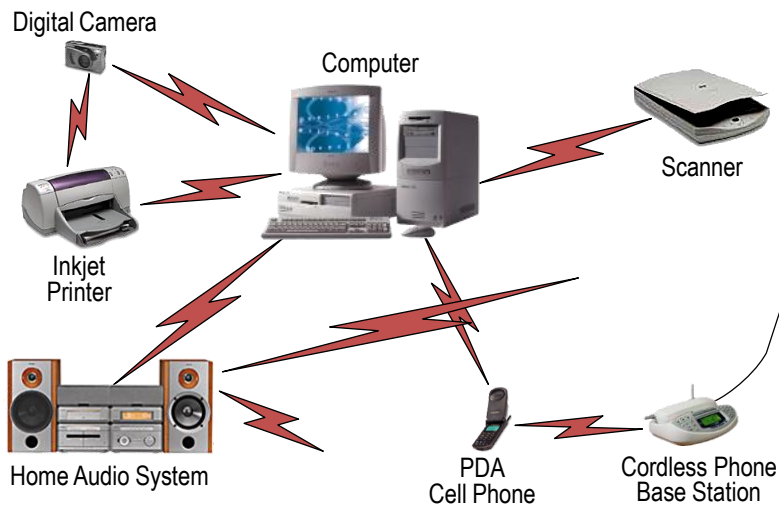
2

Outline

- BlueTooth
 - Motivation, releases
 - Introduction and Specs
 - Basic idea
 - Protocol stack
 - Network topology
 - Security
 - Antennas
 - Bluetooth vs. Wi-Fi
- HC-06 BlueTooth Module
- Example Application + Demo

3

BlueTooth - Motivation

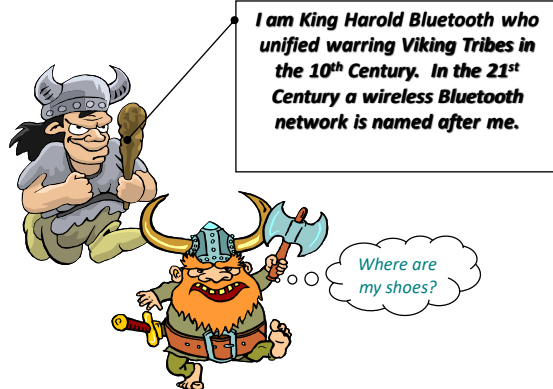


- Cable replacement
- Ad-hoc networking

4

The Name - Bluetooth?

- The name is attributed to Harald “Blatand” (“Bluetooth”) Gormsen [son of Gorm], King of Denmark in the 10th century
- Choosing this name for the standard indicates how important companies from the Baltic region (nations including Denmark, Sweden, Norway and Finland) are to the communications industry?

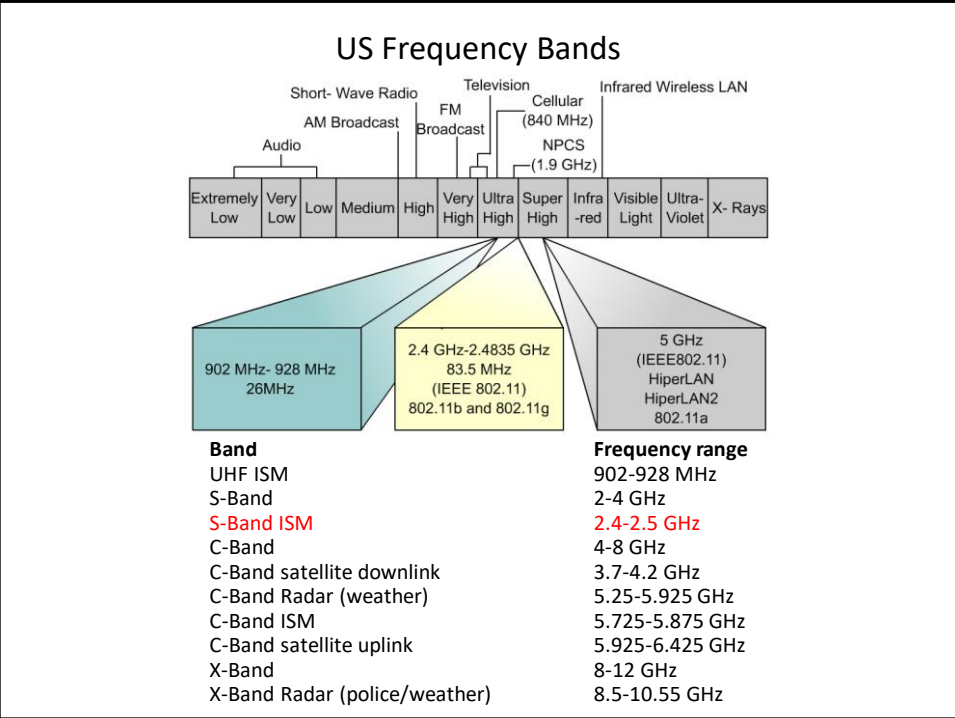


5

BlueTooth - Intro

- BlueTooth (BT) is a wireless technology standard
- Invented by Dutch electrical engineer Jaap Haartsen working for Ericsson in 1994
- Initially intended as wireless alternative to RS-232 cables
- IEEE 802.15 committee standardized the physical and link layers
- Managed by Bluetooth Special Interest Group (SIG); >30,000 member companies
- Short distances
- Short-wavelength UHF radio waves in **unlicensed ISM (industrial, scientific and medical) band**, 2.400 to 2.485 GHz
- Fixed and mobile devices
- Building personal area networks (PANs)

6



7

BLUETOOTH STANDARD RELEASES & TIMELINE HISTORY		
BLUETOOTH STANDARD VERSION	RELEASE DATE	KEY FEATURES OF VERSION
1.0	July 1999	Draft version of the Bluetooth standard
1.0a	July 1999	First published version of the Bluetooth standard
1.0b	Dec 1999	Small updates to cure minor problems and issues
1.0b + CE	Nov 2000	Critical Errata added to issue 1.0b of the Bluetooth standard
1.1	February 2001	First useable release. It was used by the IEEE for their standard IEEE 802.15.1 - 2002.
1.2	Nov 2003	This release of the Bluetooth standard added new facilities including frequency hopping and eSCO for improved voice performance. Was released by the IEEE as IEEE 802.15.1 - 2005. This was the last version issued by IEEE.
2.0 + EDR	Nov 2004	This version of the Bluetooth standard added the enhanced data rate (EDR) to increase the throughput to 3.0 Mbps raw data rate. Read more about Bluetooth 2.
2.1	July 2007	This version of the Bluetooth standard added secure simple pairing to improve security.
3.0 + HS	Apr 2009	Bluetooth 3 added IEEE 802.11 as a high speed channel to increase the data rate to 10+ Mbps
4.0	Dec 2009	The Bluetooth standard was updated to include Bluetooth Low Energy formerly known as Wibree

8

Bluetooth – Some Specs (1/2)

- Operates at frequencies between 2402 and 2480 MHz, or 2400 and 2483.5 MHz
- Uses radio technology called **Frequency-Hopping Spread Spectrum (FHSS)**
- **79 hops** (i.e., BT channels) separated by 1 MHz (i.e., each channel has a bandwidth of 1 MHz).
- Maximum frequency hopping rate: 1600 hops/sec
- Bluetooth Low Energy uses 2 MHz spacing, which accommodates 40 channels
- **Nominal range: 10 cm to 10 meters**
- Divides transmitted data into packets, and transmits each packet on one of 79 designated BT channels
- One complete data packet can be transmitted within each 625 μ s hop slot

9

Bluetooth – Some Specs (2/2)

- Bluetooth is a **packet-based protocol** with a master/slave architecture
- One master may communicate with up to 7 slaves in a piconet (ad-hoc computer network using BT technology)
- All devices share the master's clock
- Packet exchange is based on the basic clock (which ticks at 312.5 μ s intervals), defined by the master
- Two clock ticks make up a slot of 625 μ s
- Two slots make up a slot pair of 1250 μ s
- In the case of single-slot packets, the master transmits in even slots and receives in odd slots. The slave, conversely, receives in even slots and transmits in odd slots
- **Packets may be 1, 3 or 5 slots long**, but in all cases the master's transmission begins in even slots and the slave's in odd slots

10

Outline

- BlueTooth
 - Motivation, releases
 - Introduction and Specs
 - Basic idea
 - Protocol stack
 - Network topology
 - Security
 - Antennas
 - Bluetooth vs. Wi-Fi
- HC-06 BlueTooth Module
- Example Application + Demo

11

The Basic Idea

- Bluetooth is a standard for a small, cheap radio chip to be plugged into computers, printers, mobile phones, etc.
- Bluetooth chip is designed to replace cables; information is transmitted at a special frequency to a receiver Bluetooth chip.
- These devices can form a quick ad-hoc secure “piconet” and start communication.
- Connections in the “piconets” can occur even when mobile.

12

“Piconet”

- A collection of devices connected via Bluetooth technology in an ad-hoc fashion.
- A **piconet** starts with two connected devices, and may grow to eight connected devices.
- All Bluetooth devices are peer units and have identical implementations. However, when establishing a piconet, one unit will act as a **Master** and the other(s) as **Slave(s)** for the duration of the piconet connection.

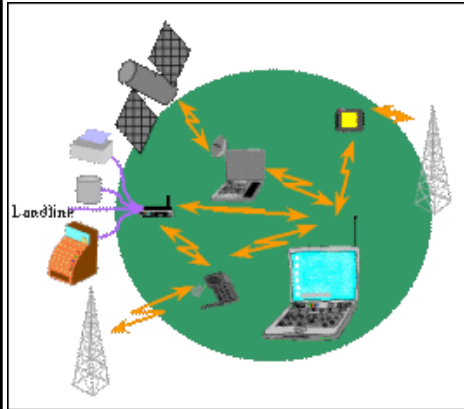
13

Requirements

- Low cost as cables – chip \$5
- Secure as cables – must support authentication and encryption
- Must support both data and voice.
- Must connect to a variety of devices.
- Must be able to function in a noisy environment.
- Data rates – 721kbps, using the 2.45GHz radio frequency band – ISM (industrial, scientific and medical)
- Must support many simultaneous and private “piconets”.
- Must be low power, compact and global.

14

Usage models - Voice/Data Access Points



- Connecting a computing device to a communicating device.
- Allows any device with a bluetooth chip to connect to the internet while located within the range of the access point.
- **Example** - a notebook could link to the internet using a mobile phone as an access point.

15

Usage models - Peripheral Interconnects



- Standard peripheral devices like keyboards, mice, headsets, etc. working over a wireless link.
- The same device can be used in multiple functions, e.g., a headset can access phones while in the office and can interface with a cellular phone when mobile.

16

Usage models - Personal Area Networking (PAN)



- Allows dynamic formation and breakdown of “PICONETS”: ad-hoc personal networks.

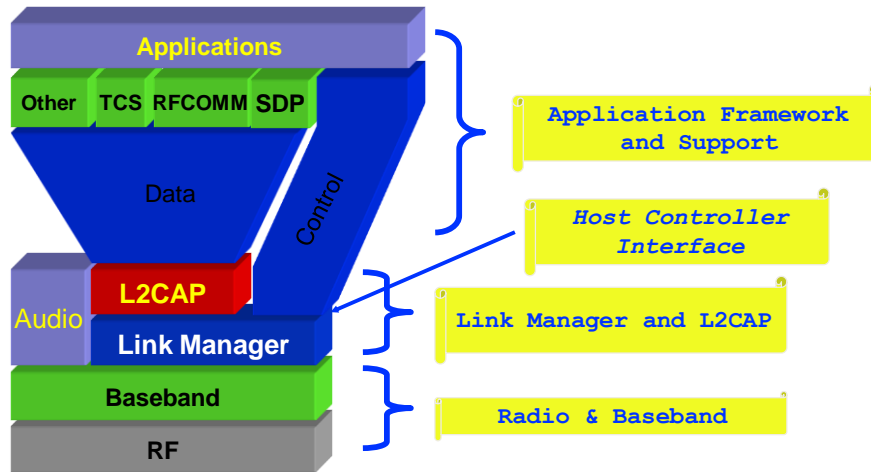
17

Outline

- Bluetooth
 - Motivation, releases
 - Introduction and Specs
 - Basic idea
 - Protocol stack
 - Network topology
 - Security
 - Antennas
 - Bluetooth vs. Wi-Fi
- HC-06 Bluetooth Module
- Example Application + Demo

18

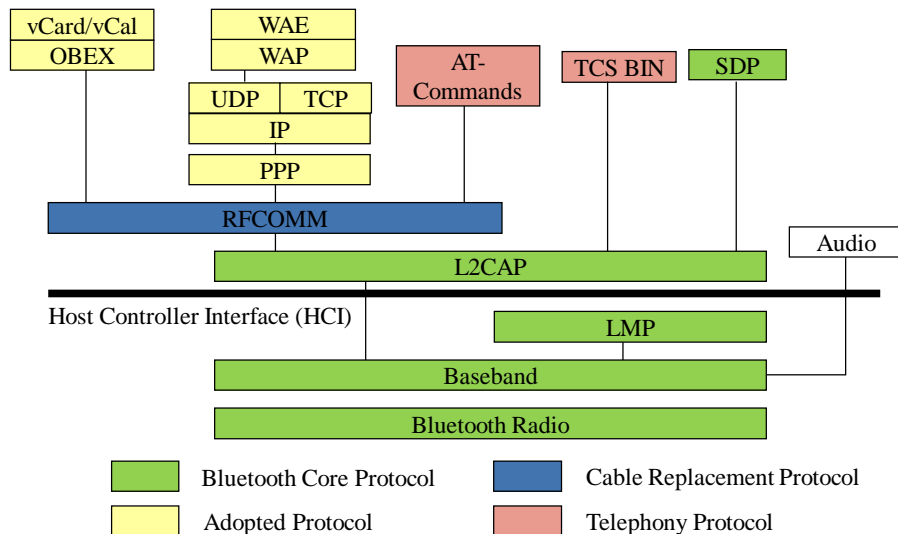
Bluetooth Protocol Stack



- A hardware/software description
- An application framework

19

Bluetooth Protocol Stack - Details



20

Layers

- Bluetooth Radio (RF Layer)
- Baseband
- LMP (Link Manager Protocol)
- HCI (Host Controller Interface)
- L2CAP (Logical Link Control and Adaptation Protocol)
- RFCOMM (Radio Frequency Communication)
- SDP (Service Discovery Protocol)

21

RF Layer

- The lowest defined layer of the Bluetooth specification
- It defines the requirements of the Bluetooth transceiver device operating in the 2.4 GHz ISM band
- It uses a packet switching protocol based on a technology called **Frequency-hopping spread spectrum (FHSS)** to spread the energy across the ISM band.

22

- In order to minimize interference, the nominal antenna power is 1 mW which can be extended to 100 mW.
- The low power limits the range to about 10 centimeters to 10 meters. With higher power of 100 mW range of 100 meters can be achieved.
- 3 different power classes
 - Power Class1: long range (100m,100mW)
 - Power Class2: mid range (10m,1-2,5mW)
 - Power Class3: short range (0.1-10m,1mW)

23

Frequency-hopping spread spectrum (FHSS)

- **FHSS** is a method of transmitting radio signals by shifting carriers across numerous channels with a pseudorandom sequence which is already known to the sender and receiver.
- Divides the designated range of the ISM-band (2.402GHz to 2.480GHz) into 79 of 1 MHz channels.
- Every frequency is **GFSK** (Gaussian frequency-shift keying) modulated with channel width of 1MHz.

24

Frequency-hopping spread spectrum (FHSS)

- A device will use 79 individual (pseudo)randomly chosen frequencies, changing from one to another on a regular basis.
- Communication between devices switches between available channels. The **frequency hopping** is done at a rate of 1600 times a second. This:
 - allows more devices to use the limited time slice
 - reduces the chance of two transmitters being on the same frequency at the same time.

25

Baseband Layer

- The physical layer of the Bluetooth that provides
 - Error correction
 - Flow control
 - Hopping sequence
 - Security
- Hopping through 79 channels
- Data is divided in **packets**
 - access code: e.g. timing synchronization
 - header: e.g. packet numbering, flow control, slave address
 - payload: voice, data or both

26

- Connection Modes
 - STANDBY: not connected in a piconet
 - ACTIVE: active participation on the channel
 - Power Saving Modes
 - SNIFF: slave listens to the channel at a reduced rate (decreasing of duty cycle) least power efficient
 - HOLD: data transfer is held for a specific time period, medium power efficient
 - PARK: synchronized to the piconet but does not participate in traffic

27

- Security Modes
 - non-secure
 - encryption enforced by application layer
 - encryption enforced by link layer
 - For devices
 - trusted device
 - untrusted device
 - For services
 - require authorization and authentication
 - require authentication
 - open to all devices

28

Audio

- Two codecs: PCM and CVSD
- Both at 64kbit/s
- Synchronous connection oriented (SCO) links
- Time-critical
- No retransmission
- Errors appear as background noise

29

LMP (Link Manager Protocol)

- The Link Manager carries out link setup, authentication, link configuration and other protocols.
- It discovers other remote LM's and communicates with them via the Link Manager Protocol (LMP).
- To perform its service provider role, the LM uses the services of the underlying Link Controller (LC).

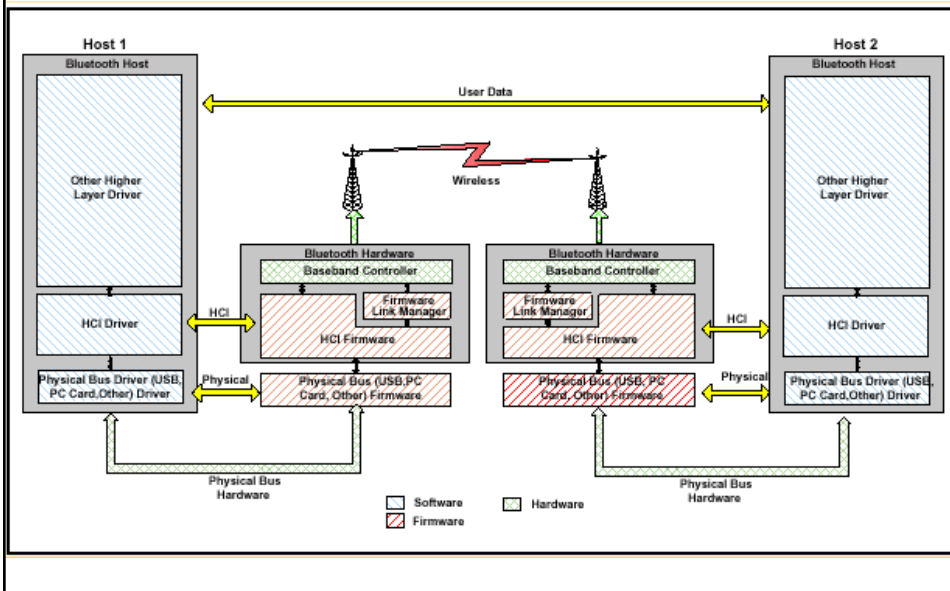
30

HCI (Host Controller Interface)

- HCI provides a command interface to baseband controller and link manager, and access to hardware status and control registers.
- Also to hardware status, control and event registers
- Bluetooth defined Host Controller Transport Layers:
 - UART (HCI over serial interface)
 - RS232 (HCI over serial interface)
 - USB (HCI over USB interface e.g. USB dongle)

31

HCI Functional Entities



32

L2CAP (Logical Link Control and Adaptation Protocol)

- L2CAP is layered over the Baseband Protocol and resides in the data link layer
- L2CAP provides connection-oriented and connectionless data services to upper layer protocols with quality-of-service functions using multiplexing, segmentation and reassembly
- Two link types are supported for the Baseband layer:
 - Synchronous Connection-Oriented (SCO)
 - Asynchronous Connection-Less (ACL)

33

RFCOMM (Radio Frequency Communication)

- Provides emulation of serial ports
- Supports up to 60 simultaneous connections
- Differentiates between two device types:
 - Type 1: communication end points (e.g. printer or headsets)
 - Type 2: devices which are part of communication (e.g. modems)
- But in the protocol itself no distinction is made, some information is for type 1 other for type 2

34

SDP (Service Discovery Protocol)

- Provides a means for applications to discover which services are available and to determine the characteristics of those available services
- Uses a request/response model where each transaction consists of one **request protocol data unit (PDU)** and one **response PDU**
- SDP is used with L2CAP
- Is optimized for the dynamic nature of bluetooth
- SDP does not define methods for accessing services

35

Outline

- BlueTooth
 - Motivation, releases
 - Introduction and Specs
 - Basic idea
 - Protocol stack
 - **Network topology**
 - Security
 - Antennas
 - Bluetooth vs. Wi-Fi
- HC-06 BlueTooth Module
- Example Application + Demo

36

Network Topology

- All units have a unique **global ID** address (48 bits)
- The unit that initializes the connection is assigned as the master which controls the traffic of the connection.
- A master can simultaneously connect up to 7 slaves.
- A device can be a master in only one “piconet” at a time.
- The master/slave roles can be swapped.

37

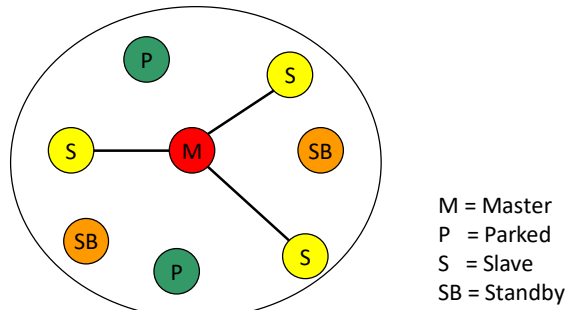
Network Topology

- **Piconet**
 - Each piconet has one master and up to 7 simultaneous slaves
 - Master: device that initiates a data exchange
 - Slave: device that responds to the master
- **Scatternet**
 - Linking of multiple piconets through the master or slave devices
 - Bluetooth devices have point-to-multipoint capability to engage in Scatternet communication

38

Piconet

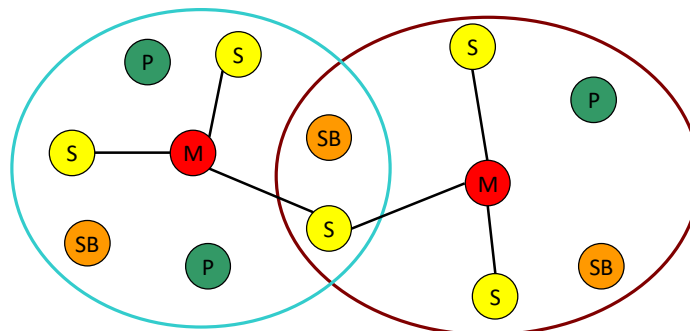
- All devices in a piconet hop together
 - Master gives slaves its clock and device ID
- Non-piconet devices are in standby



39

Scatternet

- Devices can be slave in one piconet and master of another



40

Forming a piconet

- Needs two parameters
 - Hopping pattern of the radio it wishes to connect.
 - Phase within the pattern, i.e., the clock offset of the hops.
- The global ID defines the hopping pattern.
- The master shares its global ID and its clock offset with the other radios which become slaves.
- The global ID and the clock parameters are exchanged using a **FHS (Frequency Hopping Synchronization)** packet.

41

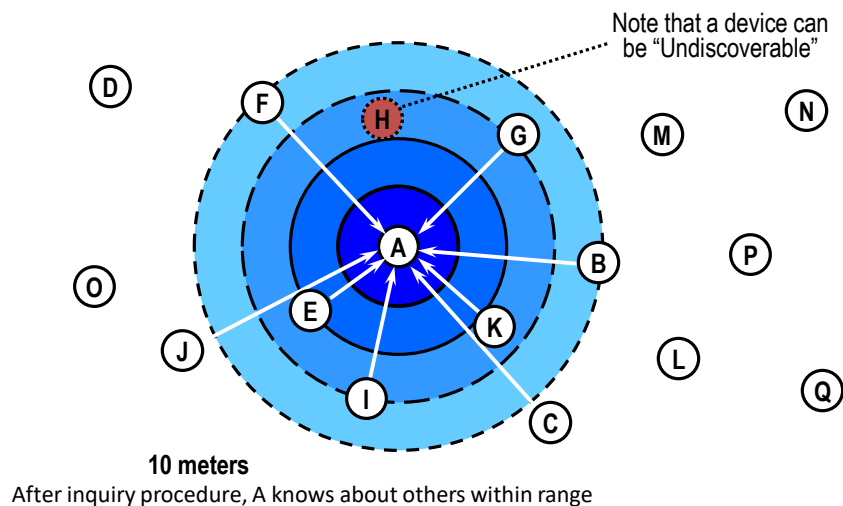
- Devices not connected to a piconet are in **STANDBY** mode, using low power.
- A connection is made by either a **PAGE** command if the address is known or by the **INQUIRY** command followed by a **PAGE**
- When a radio sends an **INQUIRY** command, all the listening radios respond with their FHS packets, which tells the inquiring radio of all the radios in the area.
- All listening radios perform a **page scan** and/or an **inquiry scan** every 1.25 seconds.
- The master radio sends an FHS to the paged radio.

42

- When a radio joins a piconet, it is assigned a 3 bit *Active Member Address (AMA)*.
- Once the piconet has eight radios, the master can put/assign a radio into the *PARK* mode.
- This is one of the low power states, in which the radio releases its AMA for a 8 bit *PMA* (Passive Member Address).
- The freed AMA can be assigned to another radio wishing to join the piconet.
- Though up to 256 radios can actively reside on a piconet, only 8 of them with AMA's can transfer data.

43

Device Discovery Illustrated



44

- Once a radio joins the piconet and has an AMA it can direct data to other devices on the piconet.
- In order to remain in the connected state within a piconet, the radio needs to maintain the frequency hopping pattern and offset while consuming low power.
- To achieve this the connected radios can be placed in either *PARK, HOLD* or *SNIFF* modes.

45

PARK MODE

- The device has given up the AMA and has become passive.
- The parked device will occasionally listen to see if the master has sent any broadcast data asking it to become active.

HOLD MODE

- When data needs to be transmitted very infrequently, thus conserving power.
- In this mode only an internal timer is running.
- No data is transferred when in HOLD mode.
- The master can put slaves on HOLD mode.

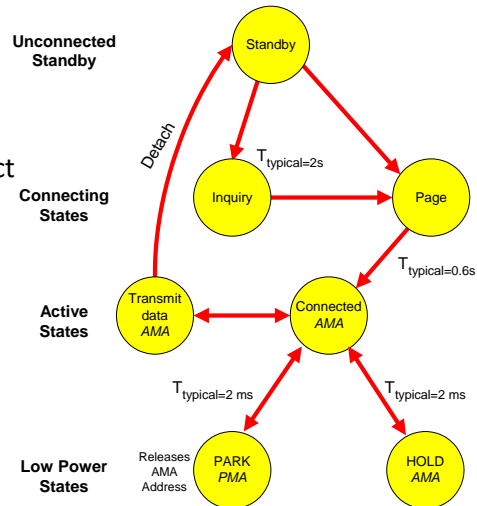
SNIFF MODE

- ❖ A slave device listens to the piconet at a reduced rate.
- ❖ The SNIFF interval is programmable.
- ❖ In both the HOLD and SNIFF states the device retains its AMA.

46

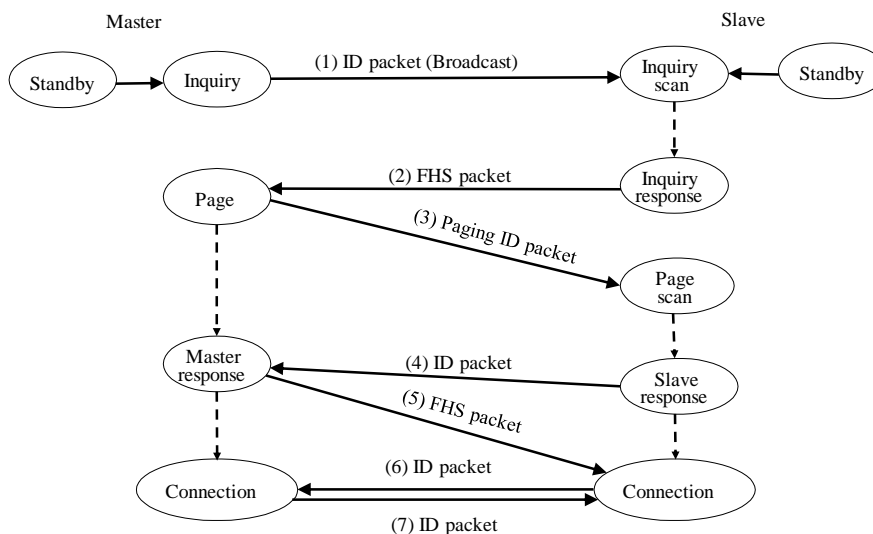
Functional Overview

- Standby
 - Waiting to join a piconet
- Inquire
 - Ask about radios to connect to
- Page
 - Connect to a specific radio
- Connected
 - Actively on a piconet (master or slave)
- Park/Hold
 - Low Power connected states



47

Connection: Inquiry and Paging



48

Two Types of Links

- The Baseband Layer handles two types of links:
 - Synchronous Connection Oriented (**SCO**)
 - Support symmetrical, circuit-switched, point-to-point connections
 - Typically used for voice traffic; do not use CRC and are not retransmitted
 - Data rate is 64 kbit/s
 - Asynchronous Connection-Less (**ACL**)
 - Support symmetrical and asymmetrical, packet-switched, point-to-multipoint connections
 - Typically used for data transmission
 - Up to 433.9 kbit/s in symmetric or 723.2/57.6 kbit/s in asymmetric

49

Outline

- BlueTooth
 - Motivation, releases
 - Introduction and Specs
 - Basic idea
 - Protocol stack
 - Network topology
 - **Security**
 - **Antennas**
 - **Bluetooth vs. Wi-Fi**
- HC-06 BlueTooth Module
- Example Application + Demo

50

Security

- Bluetooth relies on PIN codes to establish trusted relationships between devices
- Supports Unidirectional or Mutual Encryption based on a secret link Key (128 bit) shared between two devices
- Security defined in 3 modes
 - Mode1 - No security
 - Mode 2 - Service level security: not established before channel is established at L2CAP
 - Mode 3 - Link level security: device initiates security before LMP (link management protocol) link is setup
 - Devices and Services can be Set for Different Levels of Security
 - Two Trust Levels are Set for Devices
 - **Trusted Device:** Fixed Relationship and Unrestricted Access to All Services
 - **Untrusted:** No Permanent relationship and Restricted Services

51

Antennas

- Internal antennas
- External antennas



52

BlueTooth vs. Wi-Fi

- Similar applications
 - Setting up networks, printing, or transferring files
- Bluetooth
 - Intended for portable equipment and its applications (wireless personal area network, WPAN); ad-hoc connections
 - Also works for fixed location applications such as smart energy functionality in homes (thermostats, etc.)
 - Usually symmetrical, between two Bluetooth devices
 - Simple applications: headsets, remote controls, etc.
- Wi-Fi
 - Intended as replacement for high-speed cabling (wireless local area networks, WLAN)
 - Usually access point-centered, with asymmetrical client-server connection with all traffic routed through the access point
 - Applications where high speeds are required, especially for network access

53

BlueTooth vs. Wi-Fi

Figure 1.

Select the Best Wireless Standard for Your Application

	ZigBee 802.15.4	Bluetooth 802.15.1	Wi-Fi 802.11b	GPRS/GSM 1XRTT/CDMA
System resource	4-32 KB	250 KB+	1 MB ±	16 MB+
Battery life (days)	100-1,000+	1-7	0.1-5	1-7
Nodes per network	255/65,000+	7	30	1-1000
Bandwidth (KBps)	20-250	720	11,000+	64-128
Range (meters)	1-75+	1-10+	1-100	1000+

Figure 2.

Which Wireless Standard?

	Application Focus	Success Metrics
ZigBee	Monitoring and control	Reliable, secure networking Protocol simplicity Low power consumption
Bluetooth	Cable replacement	Low incremental cost Ease of use/convenience Moderate data rate
Wi-Fi	Web, email, and video	High data throughput Flexibility (work and home) Hot Spot connectivity
GPRS / GSM	Wireless voice and data	Broad geographic coverage Data-centric pricing plans Network build-out

54

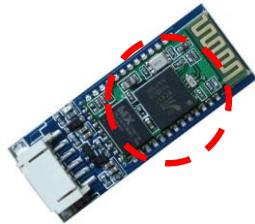
Outline

- BlueTooth
- **HC-06 BlueTooth Module**
- Example Application + Demo

55

HC-06 Module

- JY-MCU BT_BOARD V1.07 - referred to as **HC-06 Module**
 - Manual: http://www.ram-e-shop.com/ds/general/Bluetooth_TRx_Module_New.pdf
 - There are many similar others (including HC-03, HC-04, and HC-05)
- Wireless Bluetooth Transceiver Module – uses Bluetooth Specification v2.0
- Can work either as a master or a slave
- Built around the **BC417 Bluetooth-to-Serial** chip



56

HC-06 Pins

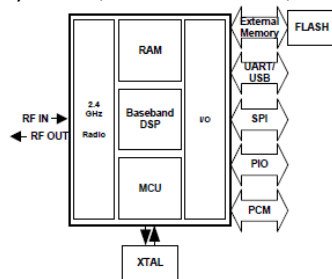
- The module has six pins:
 - VCC**: supply voltage with range 3.6 V to 6 V (BC417 chip needs 3.3V generated with the help of a voltage regulator on the same PCB).
 - GND**: ground.
 - RXD**: Serial RX - would be connected to the TX pin of the Arduino board for example.
 - TXD**: Serial TX - would be connected to the RX pin of the Arduino board.
 - KEY**: Not used.
 - STATE**: Not used.



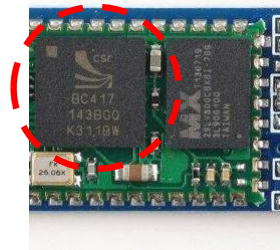
57

BC417 BlueTooth-to-Serial Chip

- Single chip radio and baseband IC for Bluetooth 2.4 GHz systems
 - Datasheet: <https://cdn.sparkfun.com/datasheets/Wireless/Bluetooth/CSR-BC417-datasheet.pdf>
- Enhanced data rates (EDR) to 3Mbps
- Loaded with features
 - 1.8V core, 1.8 to 3.6V I/O
 - UART interface with programmable baud rate up to 3M baud
 - Low Power 1.8V operation
 - USB and Dual UART Ports
 - By default, it works as a Slave, 9600 baudrate, N, 8, 1, and Pincode 1234



System Architecture



58

Outline

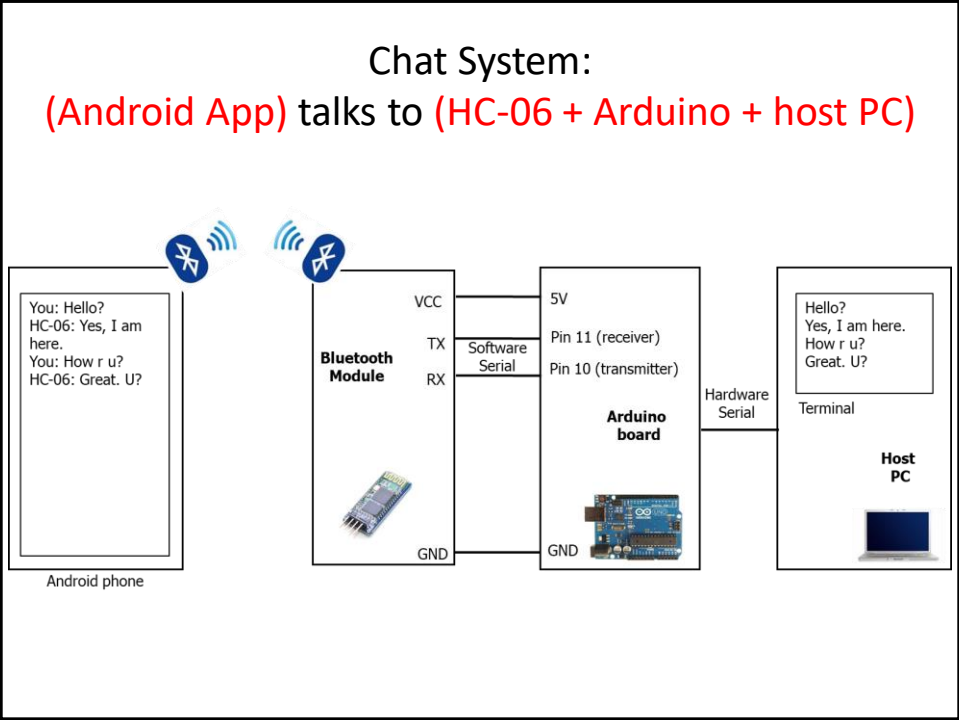
- BlueTooth
- HC-06 BlueTooth Module
- Example Application + Demo

59

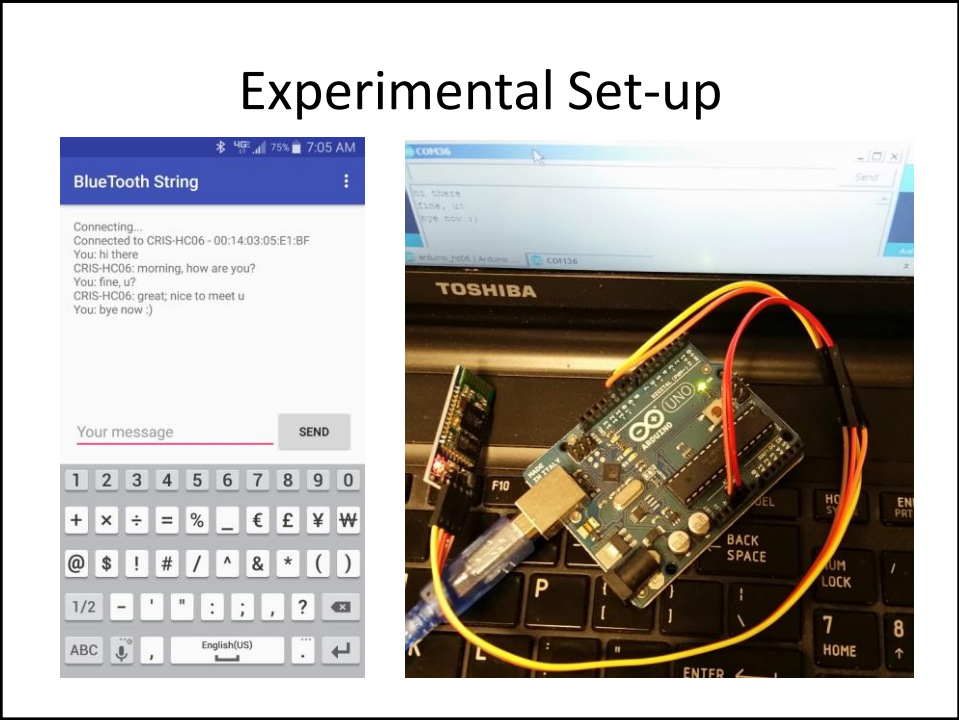
Examples of Projects that use HC-06

- Arduino based (can be ported to other MCU boards, such as LandTiger 2.0)
- Example #1
 - Send a text message from an MCU board to host PC
 - http://dejazzzer.com/geen1200/resources/G1200_EECE_Lab3.pdf
- Example #2
 - Wireless data acquisition system (send Temp./Humidity data to host PC)
 - http://dejazzzer.com/geen1200/resources/G1200_EECE_Lab3.pdf
- Example #3
 - Transmit and Receive Sensor Data and Messages from Arduino to Android App
 - If interested in whole source code let me know
- Example #4
 - Bluetooth Chat System: Android App “chit-chat”s with Arduino
 - Complete implementation, available on D2L

60



61



62

Credits, References

- Google ☺
- <https://en.wikipedia.org/wiki/Bluetooth>
- <https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics>
- https://www.amd.e-technik.uni-rostock.de/ma/gol/lectures/wirlec/bluetooth_info/radio.html
- http://www.radio-electronics.com/info/wireless/bluetooth/bluetooth_overview.php
- <https://vdocuments.mx/wireless-personal-area-networks-wpans-bluetooth-ian-f-akyildiz-broadband.html>
- <https://www.scientificamerican.com/article/experts-how-does-bluetooth-work/>
- Videos:
 - <https://www.linkedin.com/learning/ethical-hacking-wireless-networks/understanding-bluetooth>

63



64