Wireless Protocols for IoT Part I: Bluetooth and Bluetooth Smart

Raj Jain
Professor of CSE
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this class lecture are available on-line at:
http://www.cse.wustl.edu/~jain/cse574-18/

Overview

1. Bluetooth: Packet Format, Energy Management
2. Bluetooth Protocol Stack, Application Profiles
3. Bluetooth LE: Protocol Stack, PHY, MAC
4. Bluetooth and WiFi Coexistence

Note: This is 1st in a series of lectures on WPANs. ZigBee and other networks are discussed in subsequent lectures.

Bluetooth

- Started with Ericsson's Bluetooth Project in 1994 for radio-communication between cell phones over short distances
- Named after Danish king Herald Blatand (AD 940-981) who was fond of blueberries
- Intel, IBM, Nokia, Toshiba, and Ericsson formed Bluetooth SIG in May 1998
- Version 1.0A of the specification came out in late 1999.
- IEEE 802.15.1 approved in early 2002 is based on Bluetooth Later versions handled by Bluetooth SIG directly
- Key Features:
  - Lower Power: 10 mA in standby, 50 mA while transmitting
  - Cheap: $5 per device
  - Small: 9 mm^2 single chips

Bluetooth Versions

- **Bluetooth 1.1**: IEEE 802.15.1-2002
- **Bluetooth 1.2**: IEEE 802.15.1-2005. Completed Nov 2003. Extended SCO, Higher variable rate retransmission for SCO + Adaptive frequency hopping (avoid frequencies with interference).
- **Bluetooth 2.0** + Enhanced Data Rate (EDR) (Nov 2004): 3 Mbps using DPSK. For video applications. Reduced power due to reduced duty cycle
- **Bluetooth 2.1** + EDR (July 2007): Secure Simple Pairing to speed up pairing
- **Bluetooth 3.0**+ High Speed (HS) (April 2009): 24 Mbps using WiFi PHY + Bluetooth PHY for lower rates
- **Bluetooth 4.0** (June 2010): Low energy. Smaller devices requiring longer battery life (several years). New incompatible PHY. Bluetooth Smart or BLE
- **Bluetooth 4.1**: 4.0 + Core Specification Amendments (CSA) 1, 2, 3, 4
- **Bluetooth 4.2** (Dec 2014): Larger packets, security/privacy, IPv6 profile

Ref: ITL, "Security of Bluetooth Systems and Devices," http://csrc.nist.gov/publications/nistbul/august-2012_itl-bulletin.pdf

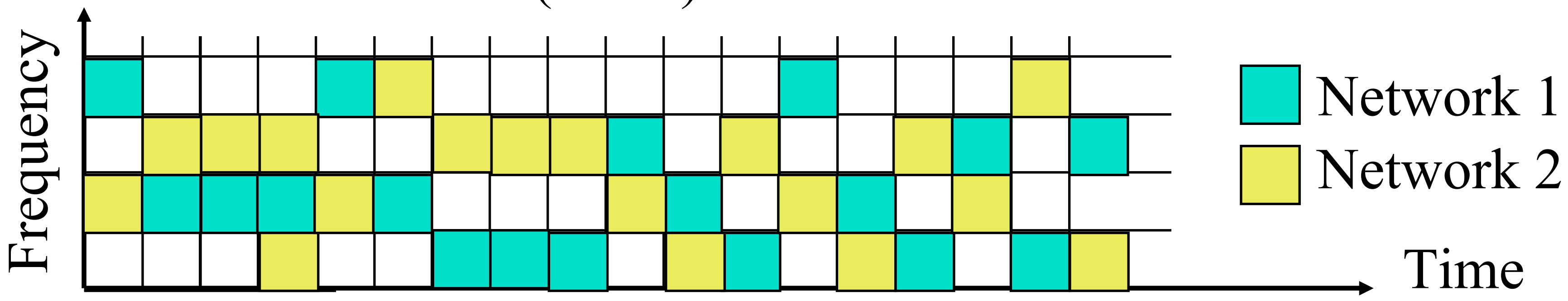
Bluetooth 5

- 2X Data rate using a new modulation
- 4X range using a special coding
- 8X broadcast capacity by changing the advertising procedure
- +20 dBm transmit power available

Ref: Rohde & Schwarz, “Bluetooth phusicall layer evolution: From cable replacement to the IoT,” http://www.rohde-schwarz.com/appnote/1MA108

Bluetooth: Details

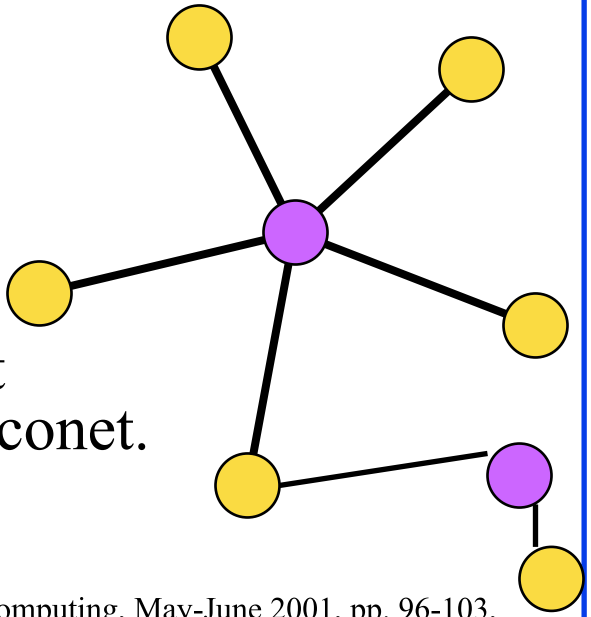
- **Frequency Range:** 2402 - 2480 MHz (total 79 MHz band) 23 MHz in some countries, e.g., Spain
- **Data Rate:** 1 Mbps using 1 MHz (Nominal) 720 kbps (User)
- **Radio Frequency hopping:** 1600 times/s ⇒ 625 ms/hop
- **Security:** Challenge/Response Authentication. 128b Encryption
- **TX Output Power:**
  - Class 1: 20 dBm Max. (0.1W) – 100m
  - Class 2: 4 dBm (2.5 mW)
  - **Class 3**: 0 dBm (1mW) – 10m



Ref: http://www.bluetooth.com/, http://www.bluetooth.org/, http://grouper.ieee.org/groups/802/15/index.html

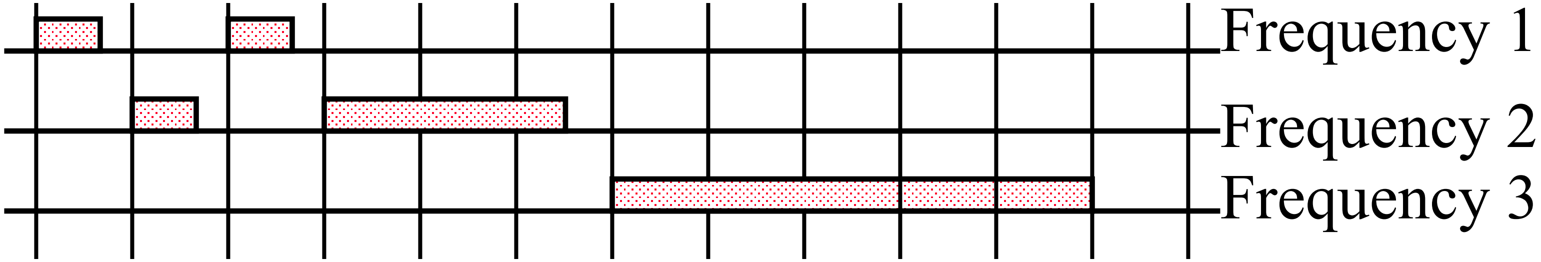
Piconet

- Piconet is formed by a master and many slaves
  - Up to 7 active slaves.
    Slaves can only transmit when requested by master
  - Up to 255 Parked slaves
- Active slaves are polled by master for transmission
- Each station gets a 8-bit parked address
  ⇒ 255 parked slaves/piconet
- The parked station can join in 2ms.
- Other stations can join in more time.
- **Scatter net**: A device can participate in multiple Pico nets ⇒ Timeshare and must synchronize to the master of the current piconet. Routing protocol not defined.



Ref: P. Bhagwat, "Bluetooth Technology for short range wireless Apps," IEEE Internet Computing, May-June 2001, pp. 96-103, bluetooth.pdf (Must read)

Frequency Hopping Sequences



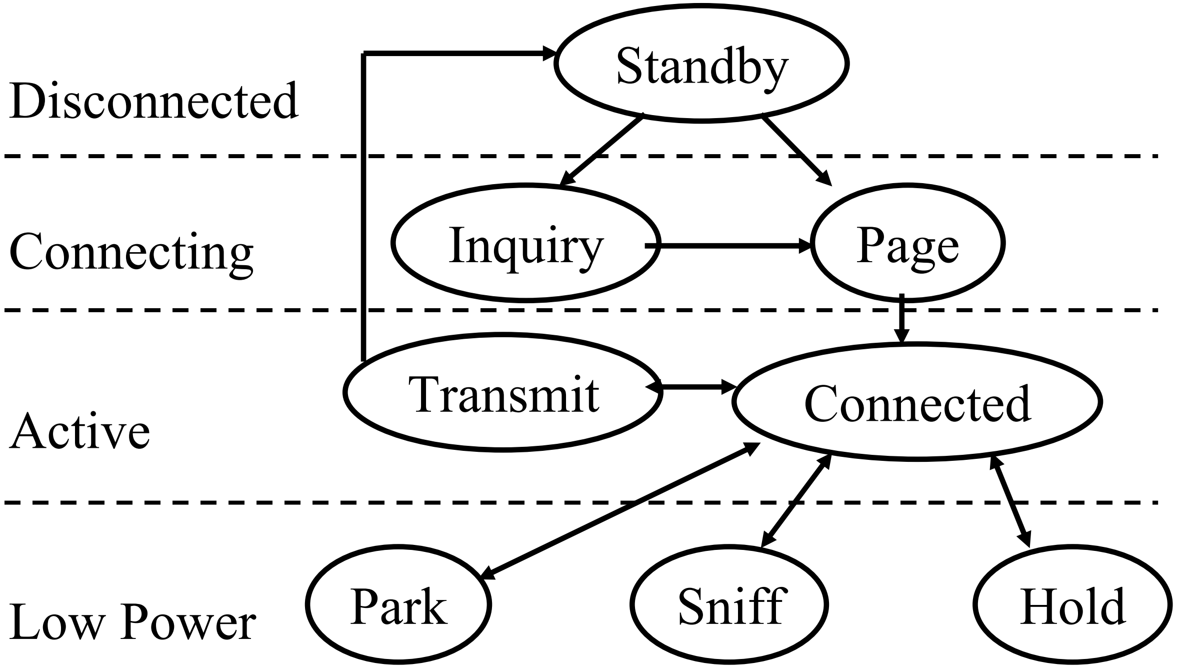
- 625 ms slots using a 312.5 ms clock
- Time-division duplex (TDD)
  ⇒ Downstream and upstream alternate
- Master starts in even numbered slots only.
- Slaves start in odd numbered slots only
- Slaves can transmit in one slot right after receiving a packet from master
- Packets = 1 slot, 3 slot, or 5 slots long
- The frequency hop is skipped during a packet.

Bluetooth Packet Format

Access Code	Baseband/Link Control Header	Data Payload
72b	54b	0-2745b

- Packets can be up to five slots long. 5 slots =3125 bits.
- Access codes:
  - Channel access code identifies the piconet
  - Device access code for paging requests and response
  - Inquiry access code to discover units
- Header: member address (3b), type code (4b), flow control, ack/nack (1b), sequence number, and header error check (8b) 18b Header is encoded using 1/3 rate FEC resulting in 54b
- Synchronous traffic has periodic reserved slots.
- Other slots can be allocated for asynchronous traffic

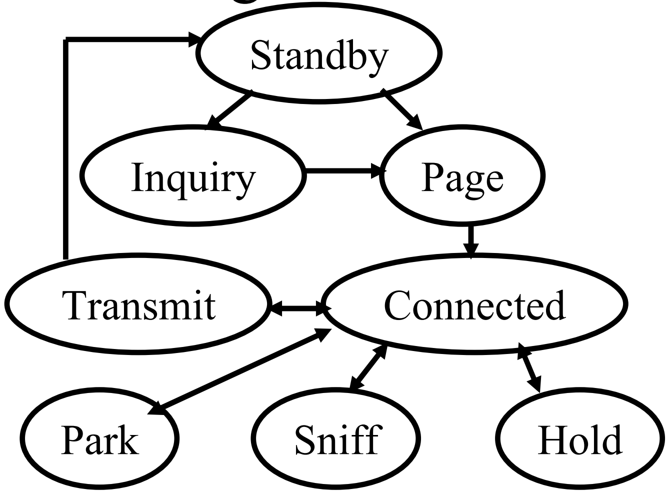
Bluetooth Operational States



- **Standby**: Initial state
- **Inquiry**: Master sends an inquiry packet. Slaves scan for inquiries and respond with their address and clock after a random delay (CSMA/CA)

Bluetooth Operational States (Cont)

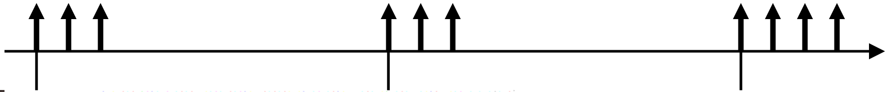
- **Page**: Master in page state invites devices to join the piconet. Page message is sent in 3 consecutive slots (3 frequencies). Slave enters page response state and sends page response including its device access code.
- Master informs slave about its clock and address so that slave can participate in piconet. Slave computes the clock offset.
- **Connected**: A short 3-bit logical address is assigned
- **Transmit**:



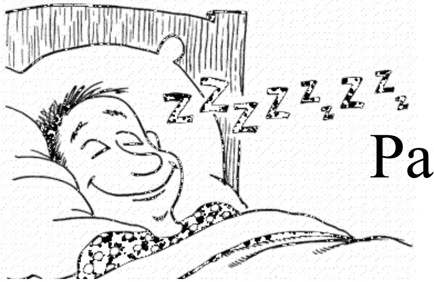
Energy Management in Bluetooth

Three inactive states:

1. **Hold**: No Asynchronous Connection List (ACL). Synchronous Connection Oriented (SCO) continues.
   Node can do something else: scan, page, inquire
2. **Sniff**: Low-power mode. Slave listens after fixed sniff intervals.
3. **Park**: Very Low-power mode. Gives up its 3-bit active member address and gets an 8-bit parked member address. Wake up periodically and listen to beacons. Master broadcasts a train of beacons periodically

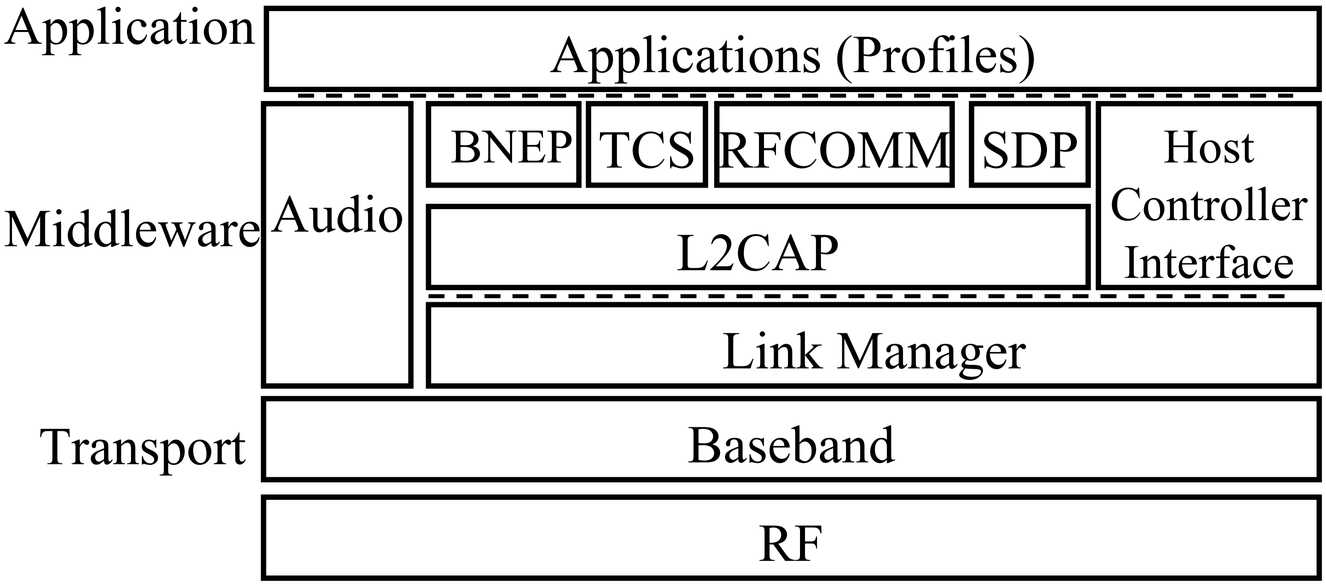


Sniff

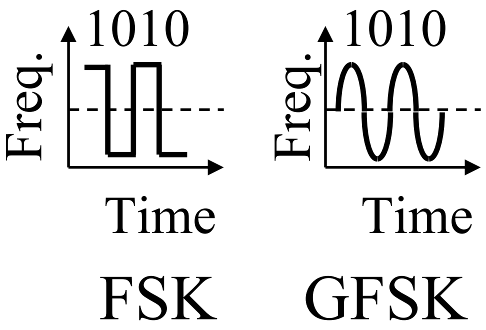


Park

Bluetooth Protocol Stack



- **RF**: Frequency hopping Gaussian Frequency Shift Keying (GFSK) modulation
- **Baseband**: Frequency hop selection, connection, MAC



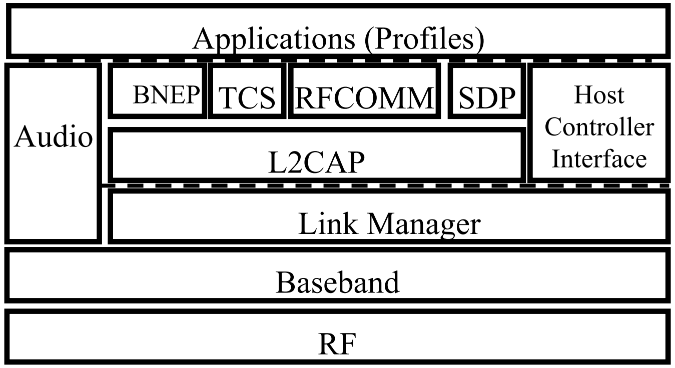
Baseband Layer

- ❑ Each device has a 48-bit IEEE MAC address
- ❑ 3 parts:
  - ➢ Lower address part (LAP) – 24 bits
  - ➢ Upper address part (UAP) – 8 bits
  - ➢ Non-significant address part (NAP) - 16 bits
- ❑ UAP+NAP = Organizationally Unique Identifier (OUI) from IEEE
- ❑ LAP is used in identifying the piconet and other operations
- ❑ Clock runs at 3200 cycles/sec or 312.5 ms (twice the hop rate)

Upper Address Part	Non-sig. Address Part	Lower Address Part
8b	16b	24b

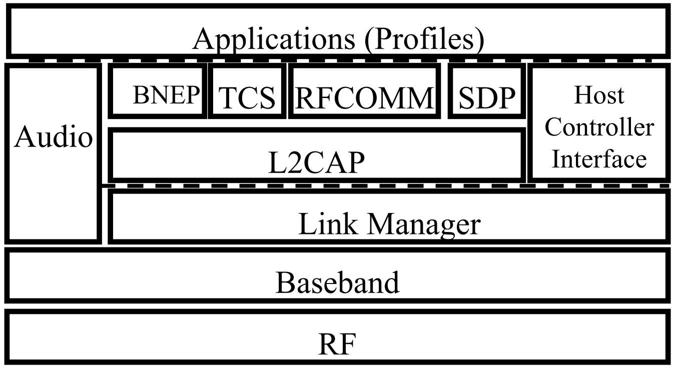
Bluetooth Protocol Stack (Cont)

- **Link Manager:** Negotiate parameters, Set up connections
- **Logical Link Control and Adaptation Protocol (L2CAP)**:
  - Protocol multiplexing
  - Segmentation and reassembly
  - Controls peak bandwidth, latency, and delay variation
- Host **Controller Interface**: Chip independent interface to Bluetooth chip. Allows same software to run on all chips.
- **RFCOMM Layer**: Presents a virtual serial port
  - Sets up a connection to another RFCOMM
- **Service Discovery Protocol (SDP):** Devices can discover the services offered and their parameters



Bluetooth Protocol Stack (Cont)

- **Bluetooth Network Encapsulation Protocol (BNEP):** To transport Ethernet/IP packets over Bluetooth
- **IrDA Interoperability protocols**: Allow existing IrDA applications to work w/o changes. IrDA object Exchange (IrOBEX) and Infrared Mobile Communication (IrMC) for synchronization
- **Audio** is carried over 64 kbps over SCO links over baseband
- **Telephony control specification binary (TCS-BIN)**: Call control including group management (multiple extensions, call forwarding, and group calls)
- **Application Profiles**: Set of algorithms, options, and parameters.



Application Profile Examples

- Headset Profile
- Global Navigation Satellite System Profile
- Hands-Free Profile
- Phone Book Access Profile
- SIM Access Profile
- Synchronization Profile
- Video Distribution Profile
- Blood Pressure Profile
- Cycling Power Profile
- Find Me Profile
- Heart Rate Profile
- Basic Printing Profile
- Dial-Up Networking Profile
- File Transfer Profile

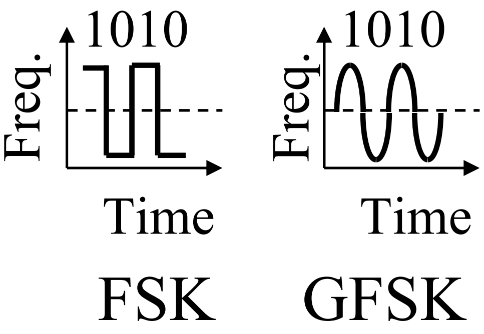
Ref: Bluetooth SIGn, "Adopted Bluetooth Profiles, Services, Protocols and Transports," https://www.bluetooth.org/en-us/specification/adopted-specifications

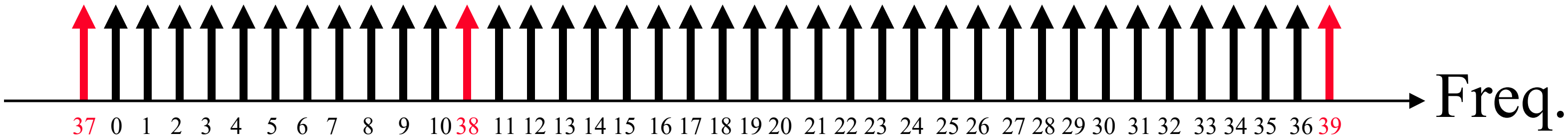
Bluetooth Smart

- **Low Energy**: 1% to 50% of Bluetooth classic
- **For short broadcast**: Your body temperature, Heart rate, Wearables, **sensors**, automotive, industrial.
  Not for voice/video, file transfers, …
- **Small messages**: 1Mbps data rate but throughput not critical.
- **Battery life**: In years from coin cells
- **Simple**: Star topology. No scatter nets, mesh, …
- **Lower cost** than Bluetooth classic
- New protocol design based on Nokia's **WiBree** technology
  Shares the same 2.4GHz radio as Bluetooth
  ⇒ Dual mode chips
- All new smart phones (iPhone, Android, …) have dual-mode chips

Bluetooth Smart PHY

- ❑ 2.4 GHz. 150 m open field
- ❑ Star topology
- ❑ 1 Mbps Gaussian Frequency Shift Keying
  Better range than Bluetooth classic
- ❑ Adaptive Frequency hopping. 40 Channels with 2 MHz spacing.
- ❑ 3 channels reserved for advertizing and 37 channels for data
- ❑ Advertising channels specially selected to avoid interference with WiFi channels

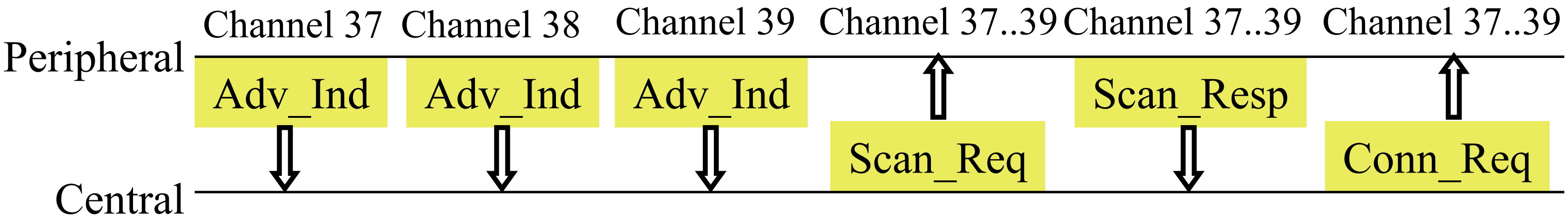




Ref: J. Decuir, "Bluetooth 4.0: Low Energy," 2010, https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205-Decuir.pdf

Bluetooth Smart MAC

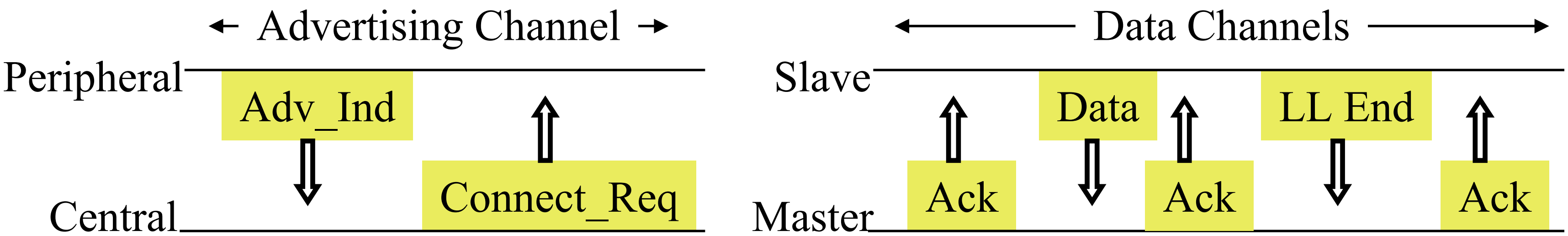
- Two Device Types: "**Peripherals**" simpler than "**central**"
- Two PDU Types: Advertising, Data
- **Non-Connectable Advertising**: Broadcast data in clear
- **Discoverable Advertising**: Central may request more information. Peripheral can send data without connection
- **General Advertising**: Broadcast presense wanting to connect. Central may request a short connection.
- **Directed Advertising**: Transmit signed data to a previously connected master



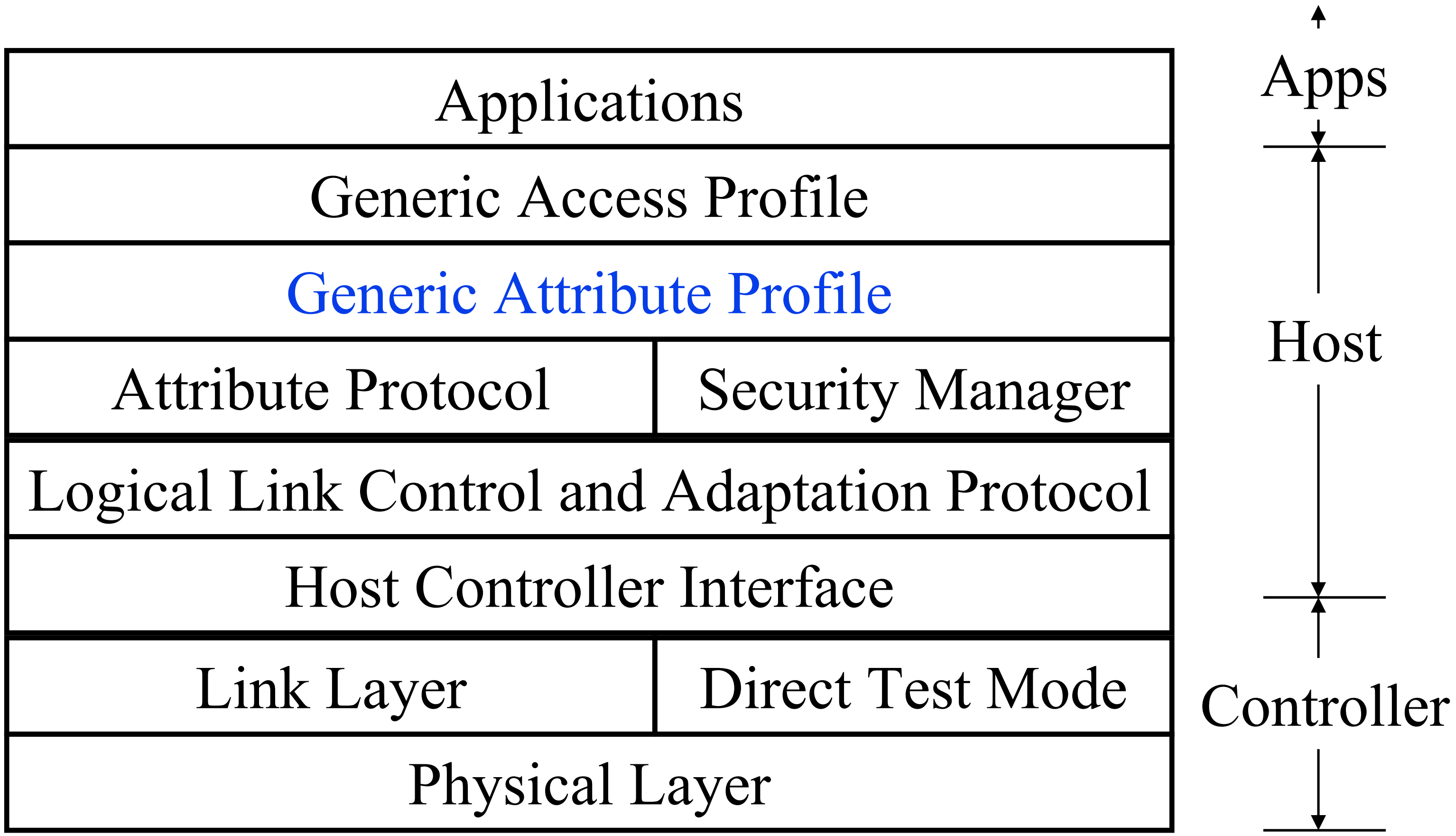
Ref: J. Decuir, "Bluetooth 4.0: Low Energy," 2010, https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205-Decuir.pdf

Bluetooth Smart MAC (Cont)

- ❑ After connecting, master tells slave about hopping sequence and wake up cycle
- ❑ All subsequent data transfers in 37 data channels
- ❑ Both devices can sleep between transactions
- ❑ Data can be encrypted.
- ❑ ~3 ms per transaction, 15 mW Power = 10 mA using 1.5V
  ⇒ 30mAs/transaction
  ⇒ 21.6 M transactions using 180 mAh battery
  ⇒ 41.1 years with 1 transaction/minute



Bluetooth Smart Protocol Stack



Applications

Generic Access Profile

Generic Attribute Profile

Attribute Protocol | Security Manager

Logical Link Control and Adaptation Protocol

Host Controller Interface

Link Layer | Direct Test Mode

Physical Layer

Apps

Host

Controller

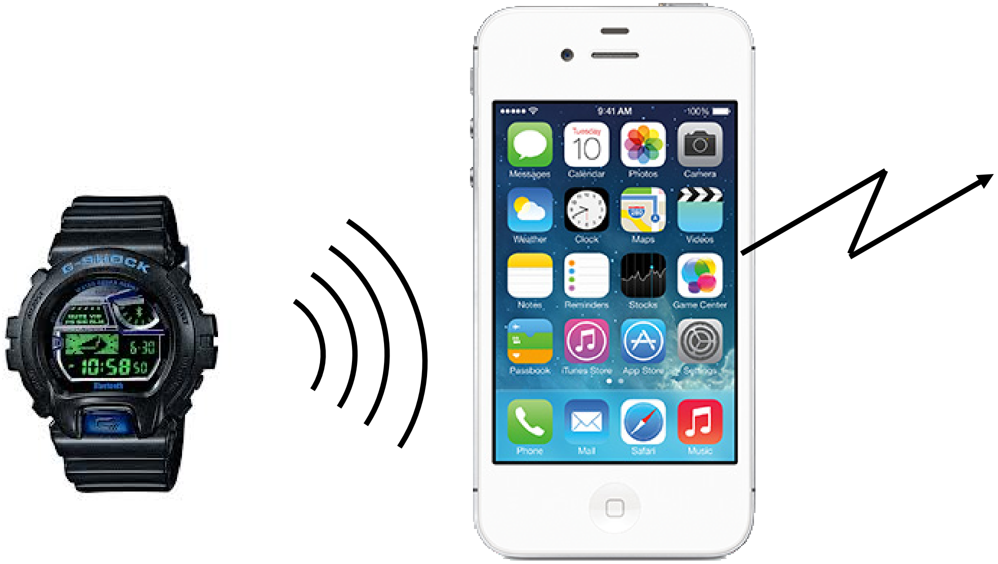
Ref: J. Decuir, "Bluetooth 4.0: Low Energy," 2010, https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205-Decuir.pdf

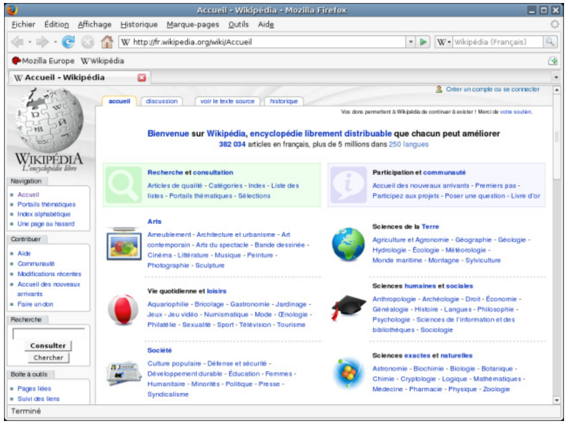
Generic Attribute (GATT) Profile

- Defines data formats and interfaces with the Attribute Protocol
- Type-Length-Value (TLV) encoding is used
- Each attribute has a 16-bit Universally Unique ID (UUID) standardized by Bluetooth SIG
- 128-bit UUID if assigned by a manufacturer
- Allows any client to find a server, read/write data
  Allows servers to talk to generic gateways
- Allows security up to AES-128
- Each to encode in XML
- Makes profile (application) development easier

Bluetooth Gateway Devices

- A gateway device helps connect a Bluetooth device to the Internet. Smart phone, Tablets, PC, …
- A generic app can forward the data to the URL sent by the device




Accueil - Wikipédia - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils Aide
http://fr.wikipedia.org/wiki/Accueil
Wikipédia (Français)
Mozilla Europe
Wikipédia
Accueil - Wikipédia
Créer un compte ou se connecter
accueil
discussion
voir le texte source
historique
WIKIPÉDIA
L'encyclopédie libre
Consulter
Chercher
Terminé

Vos dons permettent à Wikipédia de continuer à exister ! Merci de votre soutien.

Bienvenue sur Wikipédia, encyclopédie librement distribuable que chacun peut améliorer

382 034 articles en français, plus de 5 millions dans 250 langues

Navigation
- Accueil
- Portails thématiques
- Index alphabétique
- Une page au hasard

Contribuer
- Aide
- Communauté
- Modifications récentes
- Accueil des nouveaux arrivants
- Faire un don

Recherche

Boîte à outils
- Pages liées
- Suivi des liens

Recherche et consultation

Articles de qualité - Catégories - Index - Liste des listes - Portails thématiques - Sélections

Participation et communauté

Accueil des nouveaux arrivants - Premiers pas - Participez aux projets - Poser une question - Livre d'or

Arts

Ameublement - Architecture et urbanisme - Art contemporain - Arts du spectacle - Bande dessinée - Cinéma - Littérature - Musique - Peinture - Photographie - Sculpture

Sciences de la Terre

Agriculture et Agronomie - Géographie - Géologie - Hydrologie - Écologie - Météorologie - Monde maritime - Montagne - Sylviculture

Vie quotidienne et loisirs

Aquariophilie - Bricolage - Gastronomie - Jardinage - Jeux - Jeu vidéo - Numismatique - Mode - Œnologie - Philatélie - Sexualité - Sport - Télévision - Tourisme

Sciences humaines et sociales

Anthropologie - Archéologie - Droit - Économie - Généalogie - Histoire - Langues - Philosophie - Psychologie - Sciences de l'information et des bibliothèques - Sociologie

Société

Culture populaire - Défense et sécurité - Développement durable - Éducation - Femmes - Humanitaire - Minorités - Politique - Presse - Syndicalisme

Sciences exactes et naturelles

Astronomie - Biochimie - Biologie - Botanique - Chimie - Cryptologie - Logique - Mathématiques - Médecine - Pharmacie - Physique - Zoologie

Bluetooth Smart Applications

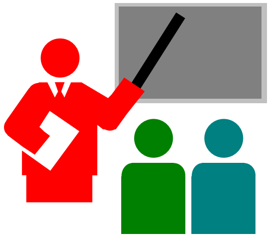
- Proximity: In car, In room 303, In the mall
- Locator: Keys, watches, Animals
- Health devices: Heart rate monitor, physical activities monitors, thermometer
- Sensors: Temperature, Battery Status, tire pressure
- Remote control: Open/close locks, turn on lights

Ref: E. Vlugt, "Bluetooth Low Energy, Beacons and Retail," Verifone White paper, 2013, 12 pp., https://www.slideshare.net/verifone/bluetooth-low-energy-beacons-and-retail-final

Beacons

- ❑ Advertizing based on proximity
- ❑ Peripherals (your phone) broadcasts its presence if Bluetooth is turned on
- ❑ Primary aim of these broadcasts is to allow device discovery
- ❑ Advertising packets consist of a header and max 27B of payload with multiple TLV-encoded data items
  - ➢ May include signal strength Þ Distance
- ❑ iOS7 iPhones can send/received iBeacons
- ❑ Can be used for customized advertising, indoor location, geofencing
- ❑ PayPal uses this to identify you.
  You can pay using a PIN and your phone.

Summary



1. Bluetooth basic rate uses frequency hoping over 79 1-MHz channels with 1, 3, 5 slots packets.
2. Three inactive states: hold, sniff, park. Has a fixed set of applications called "Profiles"
3. Bluetooth and WiFi co-exist by time-sharing or adaptive frequency notching
4. Bluetooth Smart is designed for short broadcasts by sensors. 40 2-MHz channels with 3 channels reserved for advertising. One or two-message exchanges
5. Generic attribute profile allows new applications using UUID for data types

Homework 11

- Submit answer to the following Problem:
  Assume that in one slot in Bluetooth 256 bits of payload could be transmitted. How many slots are needed if the payload size is (a) 512 bits, (b) 728 bits, and (c) 1024 bits. Assume that the non-payload portions do not change.

Reading List: Bluetooth

- Kevin Townsend, Carles Cufí, Akiba, Robert Davidson, "Getting Started with Bluetooth Low Energy," O'Reilly Media, Inc., May 2014, 180 pp., ISBN:978-1-4919-4951-1 (Safari Book), Chapter 2.
- J. Decuir, "Bluetooth 4.0: Low Energy," 2010, 62 pp., https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205-Decuir.pdf
- E. Vlugt, "Bluetooth Low Energy, Beacons and Retail," Verifone White paper, 2013, 12 pp., https://www.slideshare.net/verifone/bluetooth-low-energy-beacons-and-retail-final
- P. Bhagwat, "Bluetooth Technology for short range wireless Apps," IEEE Internet Computing, May-June 2001, pp. 96-103, http://ieeexplore.ieee.org/xpl/abstractKeywords.jsp?arnumber=935183
- Logitech, "Bluetooth FAQ," http://www.logitech.com/images/pdf/userguides/bluetooth-faq.pdf

References

- Bluetooth SIG, http://www.bluetooth.com/lowenergy
- Bluetooth SIG, “BLUETOOTH 4.1 Features and Technical Description,” 2013, https://www.bluetooth.org/en-us/Documents/Bluetooth%204.1%20Technical%20Description.pdf
- Bluetooth SIG, "Adopted Bluetooth Profiles, Services, Protocols and Transports," https://www.bluetooth.org/en-us/specification/adopted-specifications
- http://whatis.techtarget.com/definition/Bluetooth-20EDR
- ITL, "Security of Bluetooth Systems and Devices," http://csrc.nist.gov/publications/nistbul/august-2012_itl-bulletin.pdf
- E. Ferro and F. Potorti, ""Bluetooth and Wi-Fi wireless protocols: a survey and a comparison", Volume: 12 Issue: 1, Pages: 12-26, IEEE Wireless Communications, 2005, http://ieeexplore.ieee.org/iel5/7742/30466/01404569.pdf?tp=&arnumber=1404569&isnumber=30466

References (Cont)

- P. McDermott-Wells, "What is Bluetooth?", Volume 23, Issue 5, Page(s):33 - 35, IEEE Potentials, 2005, http://ieeexplore.ieee.org/iel5/45/29958/01368913.pdf?tp=&arnumber=1368913&isnumber=29958
- K.V.S.S.S.S. Sairam, N. Gunasekaran, and S.R. Redd, "Bluetooth in wireless communication" Volume 40, Issue 6, Page(s):90 - 96, IEEE Communications Magazine, June 2002, http://ieeexplore.ieee.org/iel5/35/21727/01007414.pdf?tp=&arnumber=1007414&isnumber=21727
- B. Chatschik, "An overview of the Bluetooth wireless technology", Volume 39, Issue 12, Page(s):86 - 94, IEEE Communications Magazine, 2001, http://ieeexplore.ieee.org/iel5/35/20896/00968817.pdf?tp=&arnumber=968817&isnumber=20896

Acronyms

ACL	Asynchronous Connection List
AD	Anno Domini (Latin for *in the year of the Lord*)
AES-128	Advanced Encryption Standard w 128 bit keys
BIN	Binary
BLE	Bluetooth Low Energy
BNEP	Bluetooth Network Encapsulation Protocol
CAP	Connection Access Profile
CSA	Core Specification Amendment
dBm	Deci-bel milli-watt
DPSK	Differential Phase Shift Keying
EDR	Enhanced Data Rate,
FEC	Forward Error Correction
FSK	Frequency Shift Keying
GATT	Generic Attribute
GFSK	Gaussian Frequency Shift Keying
GHz	Giga Hertz
HS	High Speed,

Acronyms (Cont)

IBM	International Business Machines
ID	Identifier
IEEE	Institution of Electrical and Electronics Engineers
iOS	Apple's idevices Operating System
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
IrDA	Infrared Data Association
IrMC	Infrared Mobile Communications
IrOBEX	Infrared Object Exchange
LAN	Local Area Network
LAP	Lower address part
LE	Low Energy
LL	Logical Link
MAC	Media Access Control
MAN	Metropolitan Area Network

Acronyms (Cont)

MHz	Mega Hertz
mW	milli Watt
NAP	Non-significant address part
OUI	Organizationally Unique Identifier
PAL	Protocol Adaptation Layer
PC	Personal Computer
PDU	Protocol Data Unity
PHY	Physical Layer
PIN	Personal Identification Number
RF	Radio Frequency
RFCOMM	Radio Frequency Communication
RFID	Radio Frequency Identifier
SCO	Synchronous Connection Oriented
SDP	Service Discovery Protocol
SG	Study Group
SIG	Special Interest Group

Acronyms (Cont)

SIM	Subscriber Identity Module
TCS	Telephony Control Specification
TDD	Time-division duplex
TLV	Type-Length-Value
TV	Television
TX	Transmit
UAP	Upper address part
UCD	Unicast Connectionless Data
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
uW	Micro-Watt
WAN	Wide Area Network
WBS	Wide Band Speed
WiFi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WPAN	Wireless Personal Area Networks

Acronyms (Cont)

WRAN	Wireless Regional Area Network
XML	Extensible Markup Language

Scan This to Download These Slides

Raj Jain

http://rajjain.com

Related Modules

CSE567M: Computer Systems Analysis (Spring 2013), https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011), https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw

Recent Advances in Networking (Spring 2013), https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5

CSE571S: Network Security (Fall 2011), https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u

Video Podcasts of Prof. Raj Jain's Lectures, https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw