BLUETOOTH LOW ENERGY

Flavia Martelli
flavia.martelli@unibo.it

Outline

- Introduction
- Applications
- Architecture
- Topology
- Controller specifications:
  - Physical Layer
  - Link Layer
- Host specifications: upper layers
- Products on the market

Introduction (1/2)

Bluetooth:

- Wireless technology for short-range communication
- Replacement to cables connecting portable and/or fixed electronic devices

- Key features:
  - worldwide operation
  - robustness
  - low power consumption
  - low cost
  - interoperability

Introduction (2/2)

Bluetooth Core Specification v4.0 (adopted 30 June 2010)

- Two main configurations
  1. Basic Rate (BR)
     - Optional Enhanced Data Rate (EDR) and Alternate MAC and PHY (AMP) extensions
  2. Low Energy (LE)
     - Lower power consumption → devices operated with coin cell batteries
     - Lower complexity
     - Lower cost
     - Lower data rates

Applications (1/7)

Automotive

Applications (2/7)

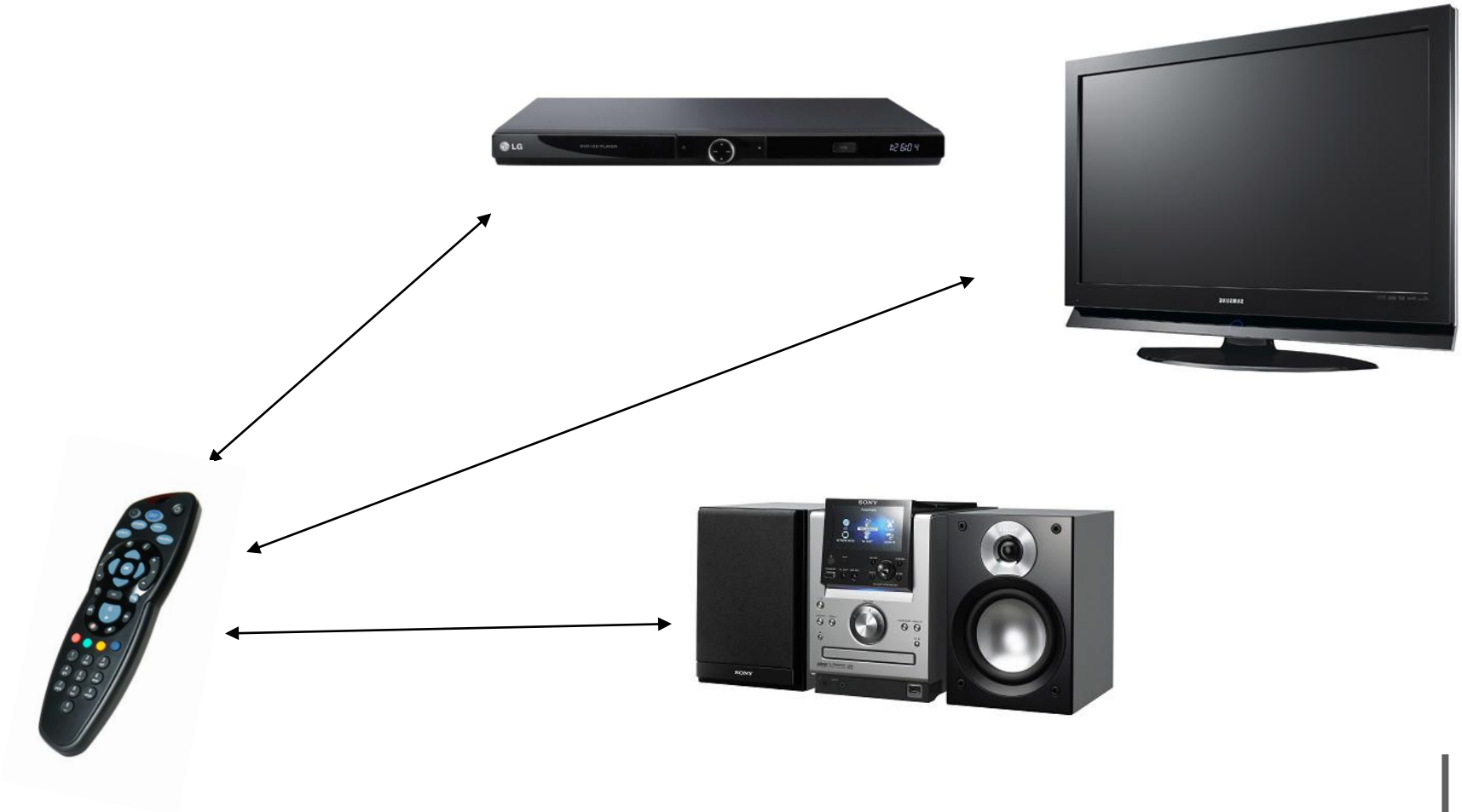
Sports and fitness

Applications (3/7)

Healthcare

Applications (4/7)

Entertainment



Applications (5/7)

Home automation








Applications (6/7)

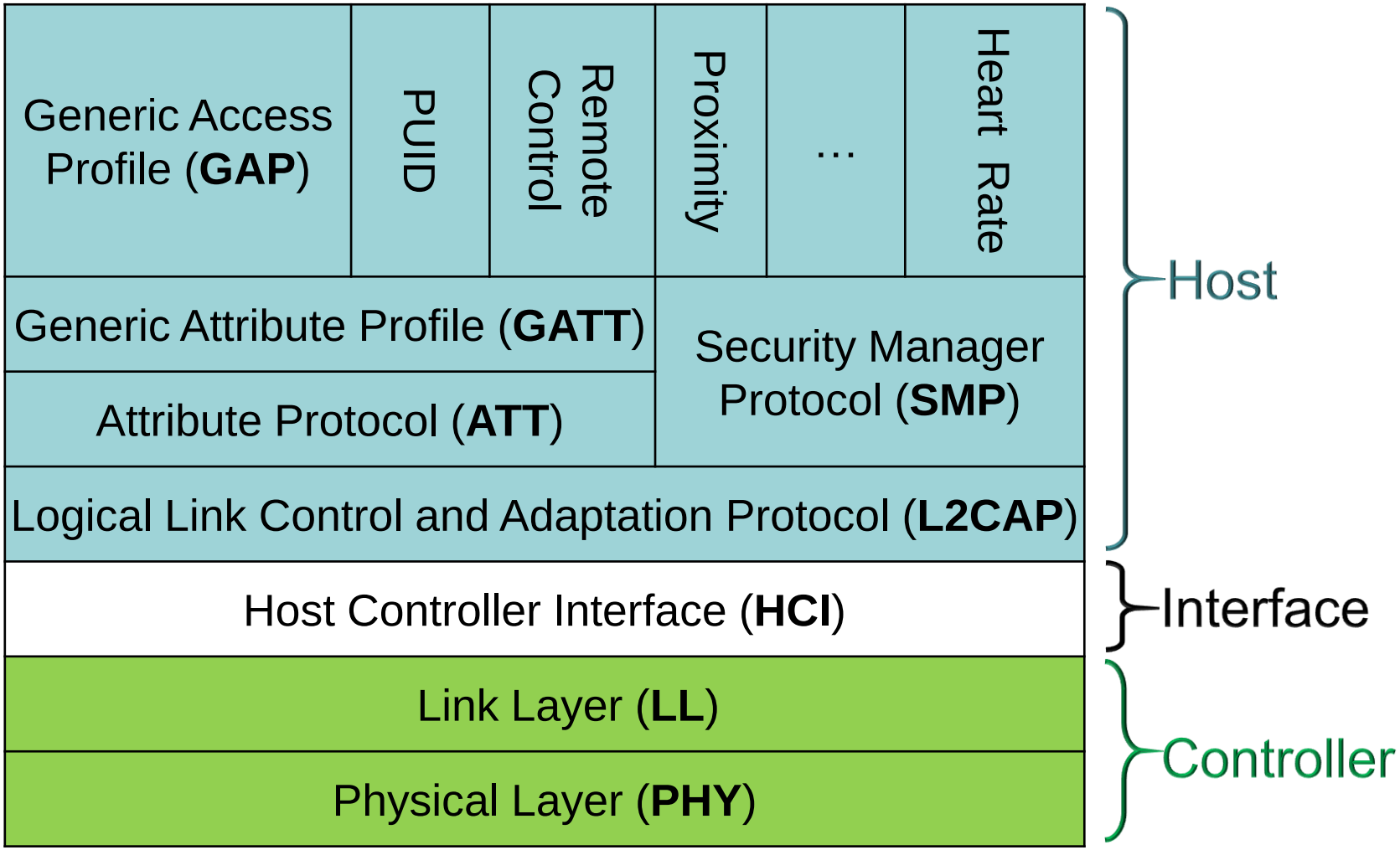
Security and proximity

Applications (7/7)

Advertising

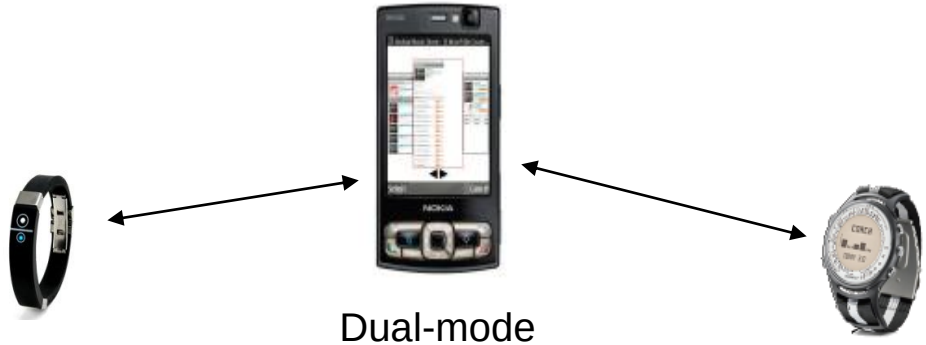
YOU ARE HERE

Architecture



Implementation modes

- ***Single-mode*** (stand-alone) implementation: targeted at low power consumption and small size devices
- ***Dual-mode*** implementation: extension to a classic Bluetooth radio, targeted at mobile phones and PCs



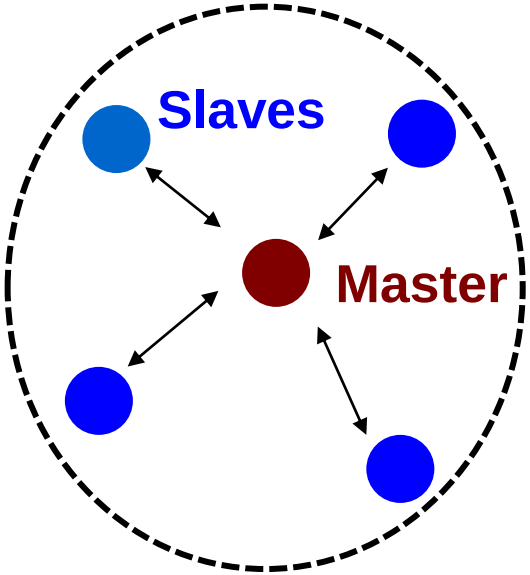
LE single-mode device

Dual-mode device

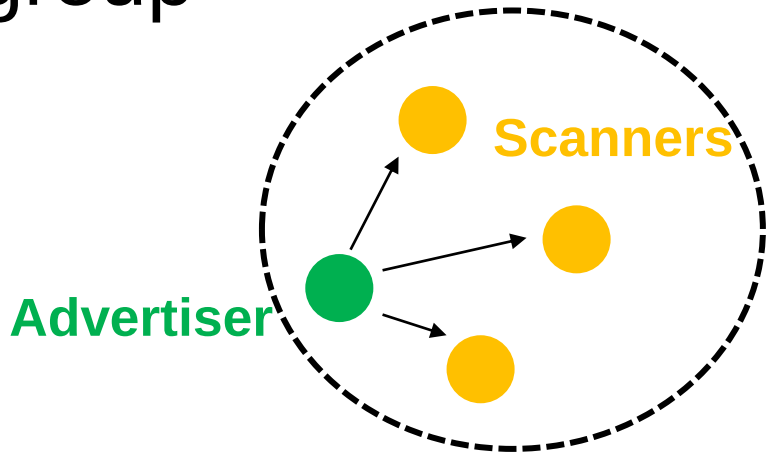
LE single-mode device

Network topology

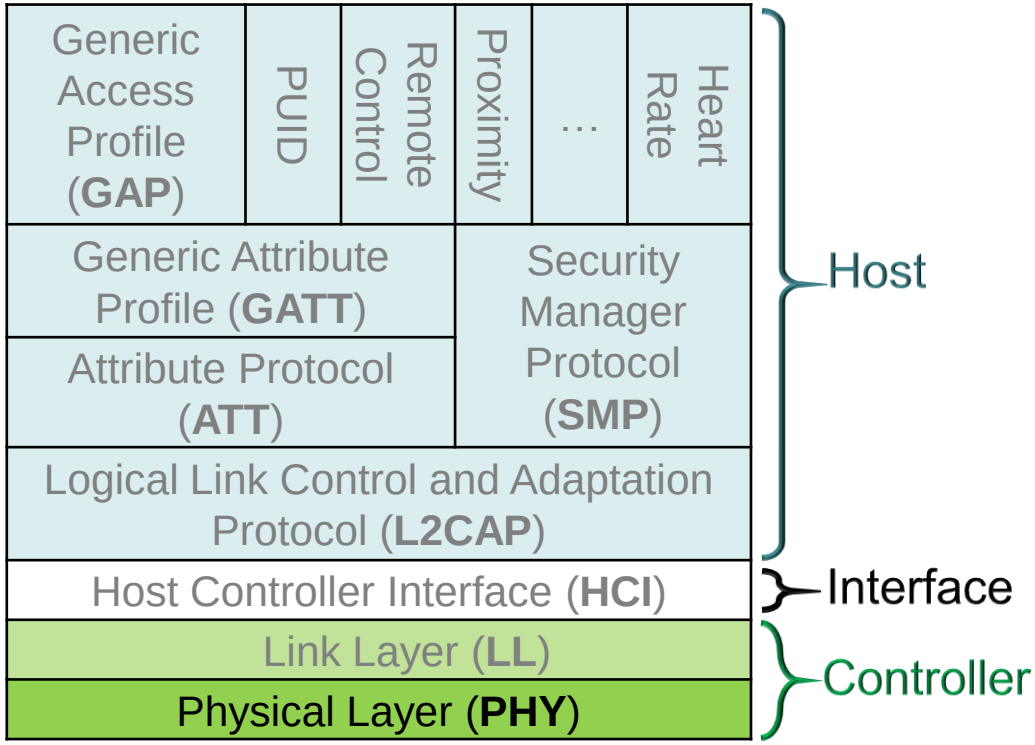
- Piconet: star topology



- Broadcast group



Controller specification



Physical Layer (1/2)

- **Modulation**: Gaussian Frequency Shift Keying (GFSK)
  - Bandwidth-bit period product: $BT = 0.5$
  - Modulation index: $0.45 < h < 0.55$
  - Bit-rate: $R_b = 1Mbit/s$

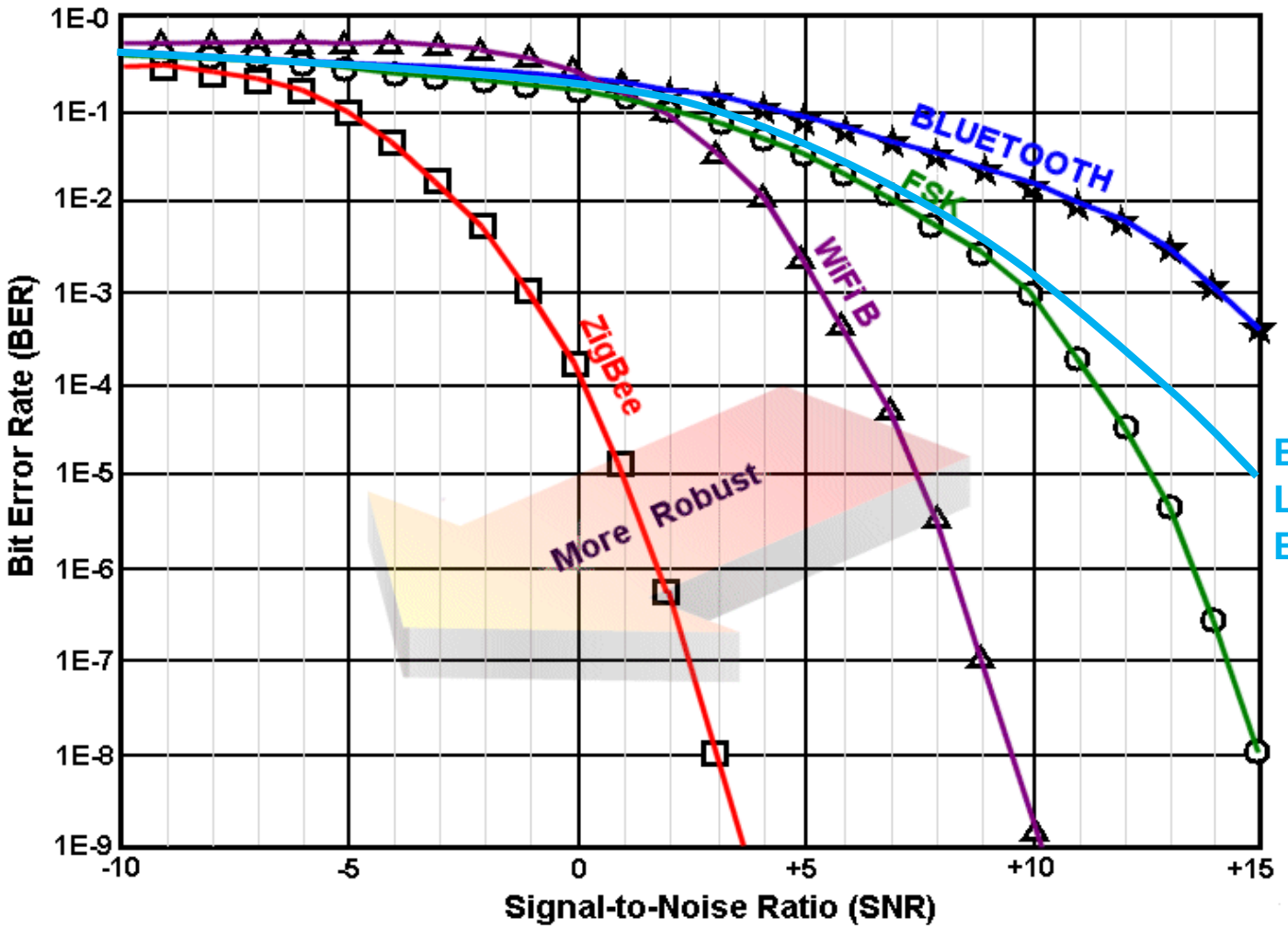
- **Transmission power**: $-20\ dBm < P_{tx} < +10\ dBm$
- **Receiver sensitivity**: $-70\ dBm$

  [BER < 0.1%]

Physical Layer (2/2)

- **Band**: ISM @ 2.4 GHz
  - 40 channels of 2 MHz
  - *f = 2402 + i*2 MHz, i=0,…,39*

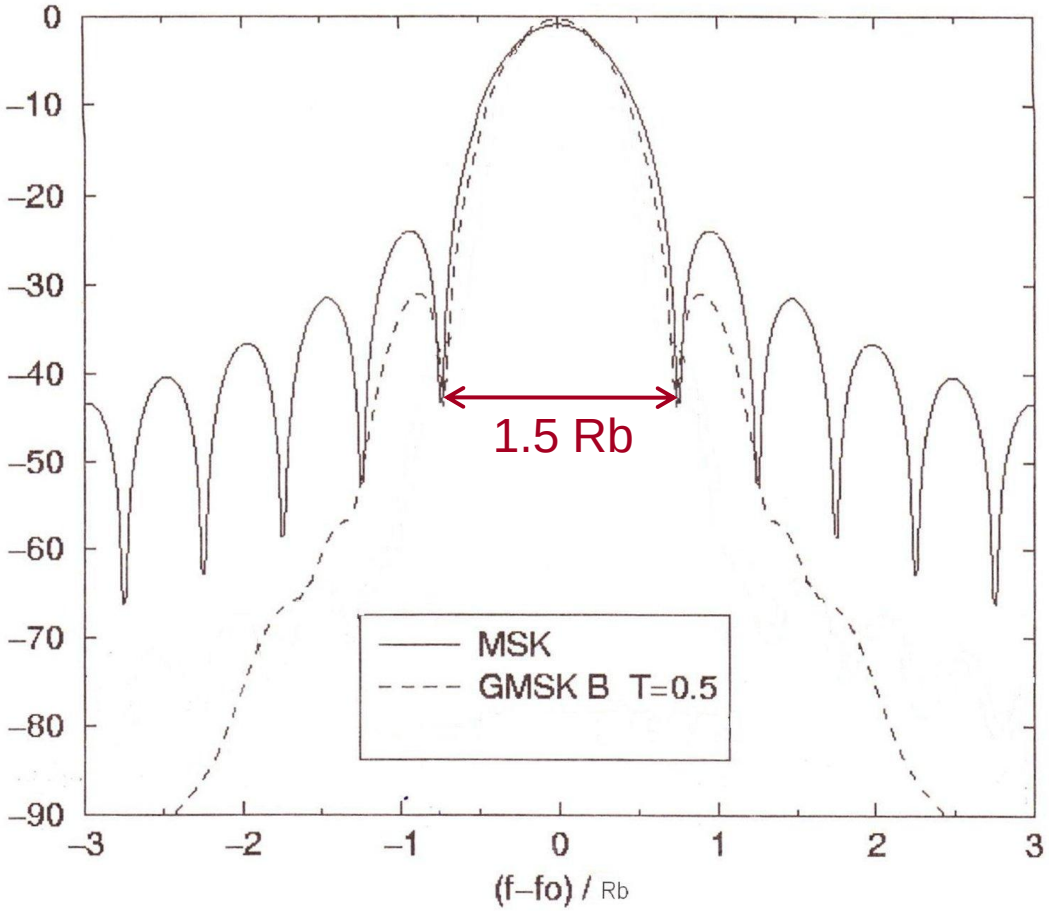
PHY performance (1/2)



BLUETOOTH LOW ENERGY

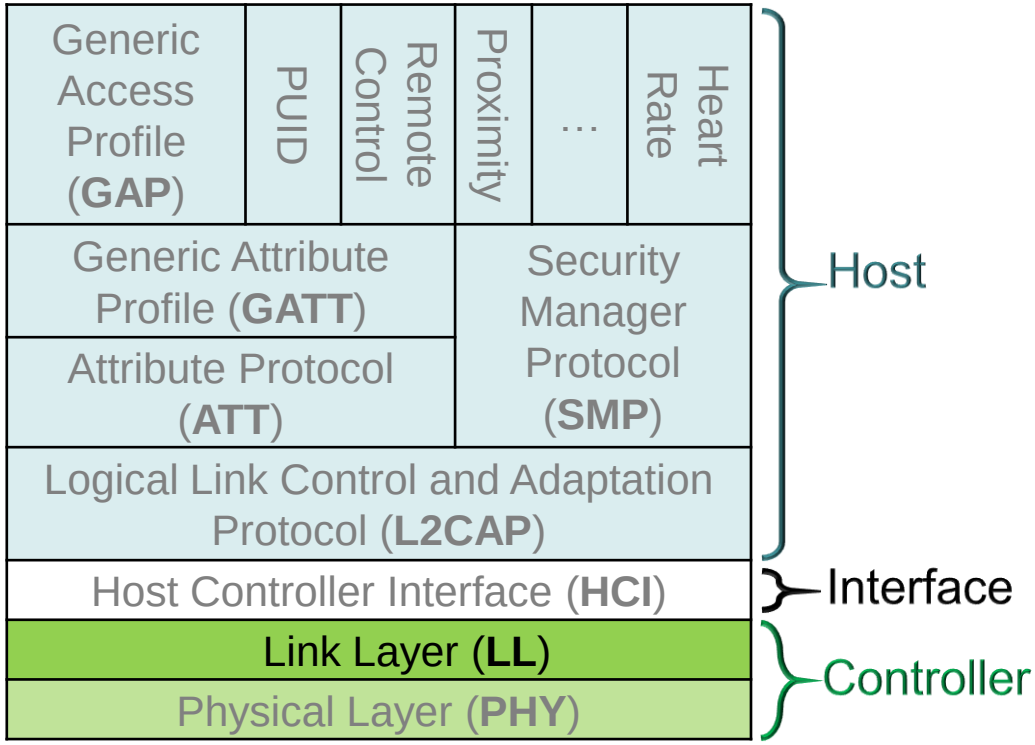
PHY performance (2/2)

Normalized power spectrum [dB]



802.15.4 → 3 MHz
Bluetooth LE → 1.5 MHz

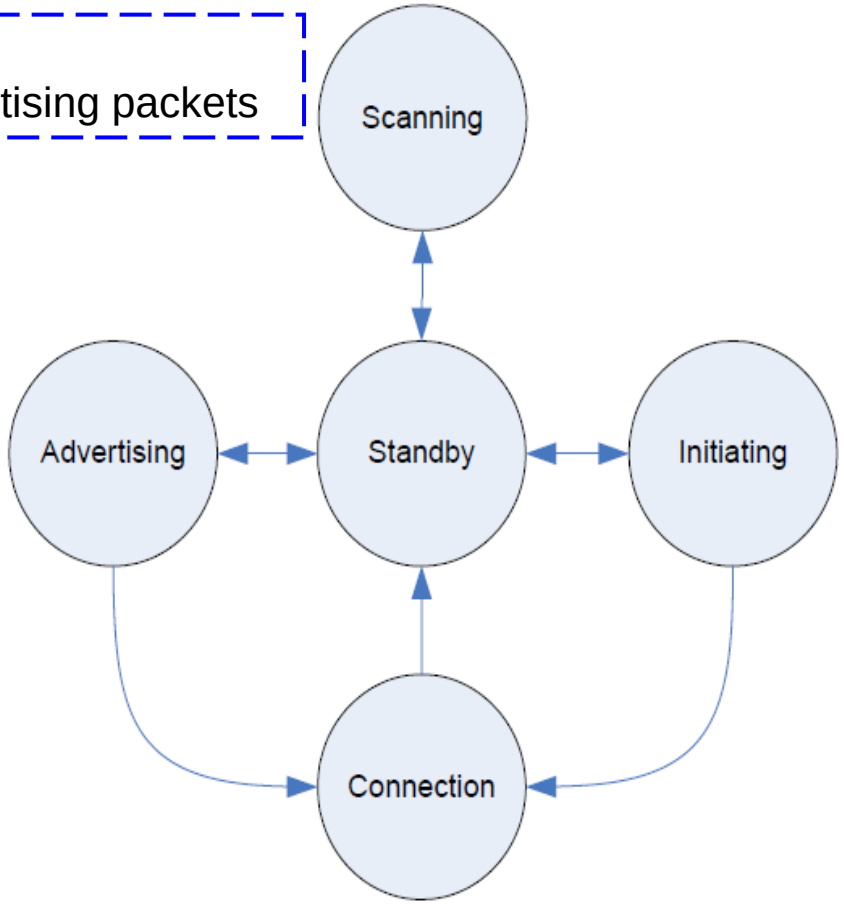
Controller specification



Link Layer: state machine

Scanner
Listen to Advertising packets

Advertiser
Tx Advertising packets



Initiator
Listen to Advertising packets and respond to initiate a connection

Slave/Master
Tx/Rx data packets

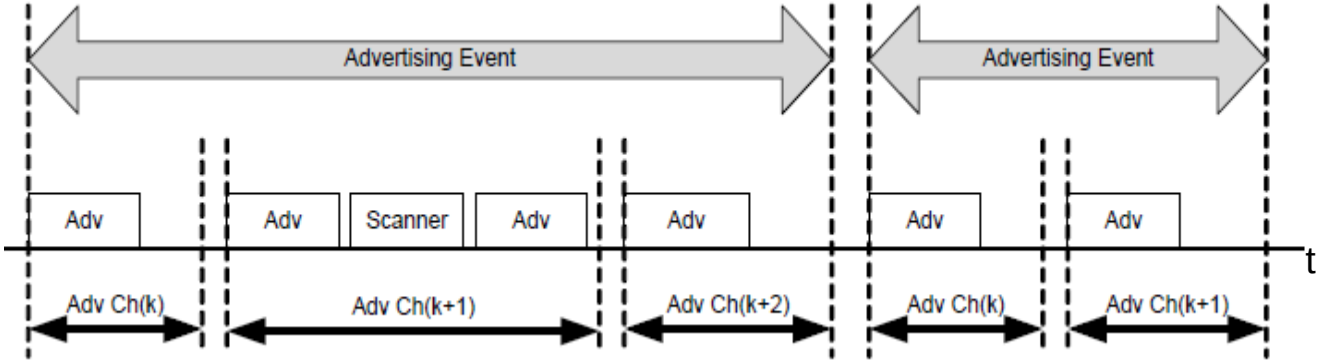
Link Layer: channels

- RF Channels are allocated into two types:
  1. ***Advertising physical channel*** (i = 0, 12, 39): discovering devices, initiating a connection, broadcasting data
  2. ***Data physical channel*** (the other 37 RF channels): communication between connected devices

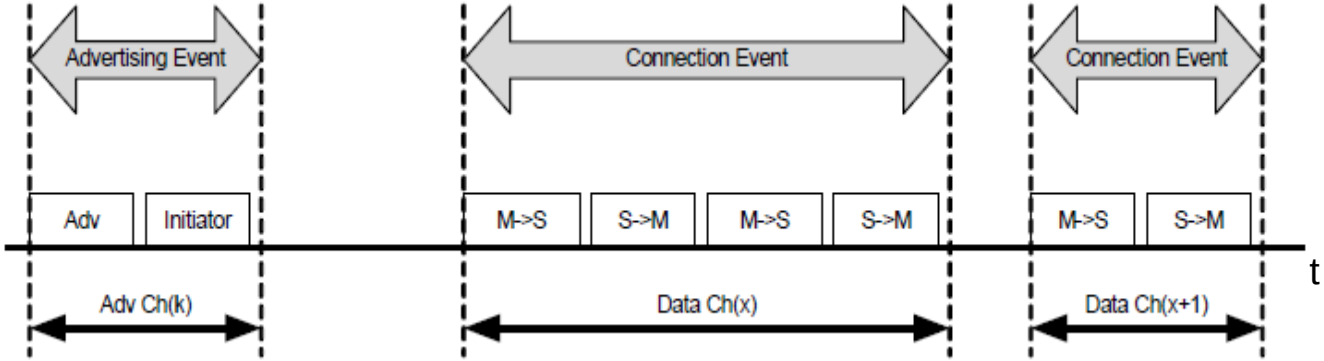
MHz	Adv	Data
2402	37	
2404		0
2406		1
2408		2
2410		3
2412		4
2414		5
2416		6
2418		7
2420		8
2422		9
2424		10
2426	38	
2428		11
2430		12
2432		13
2434		14
2436		15
2438		16
2440		17
2442		18
2444		19
2446		20
2448		21
2450		22
2452		23
2454		24
2456		25
2458		26
2460		27
2462		28
2464		29
2466		30
2468		31
2470		32
2472		33
2474		34
2476		35
2478		36
2480	39	

Link Layer: events

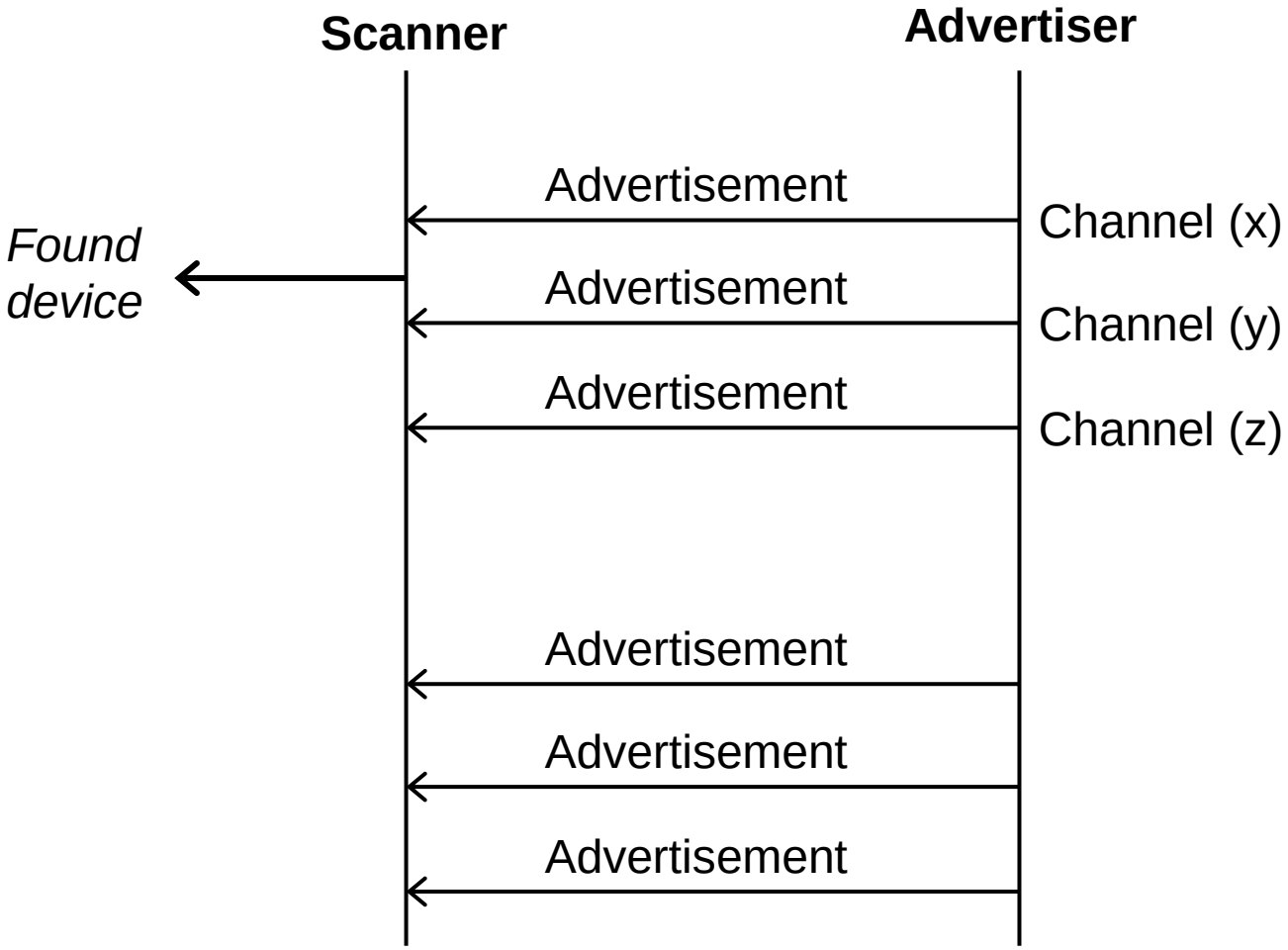
- ***Advertising events***



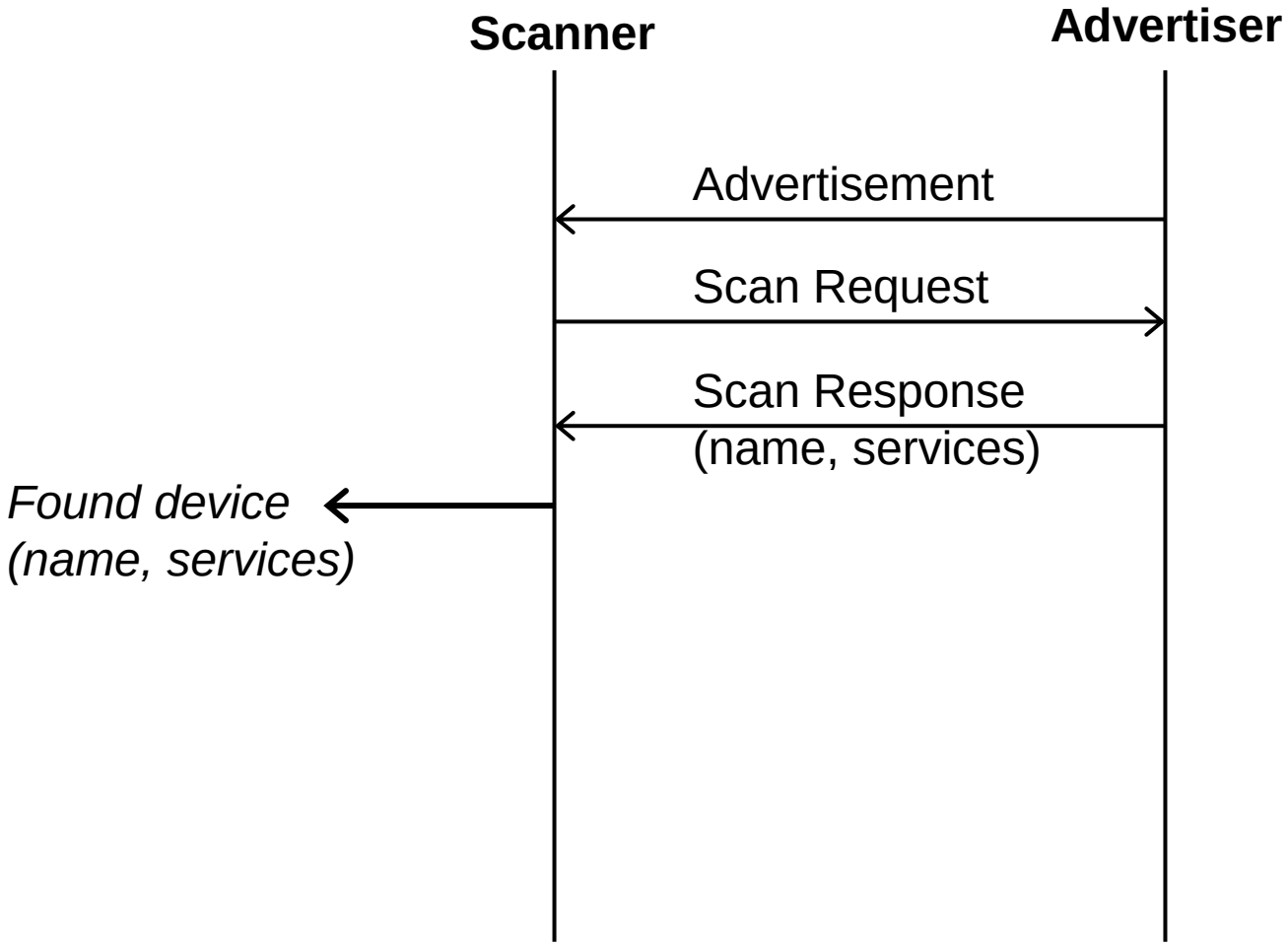
- ***Connection events***



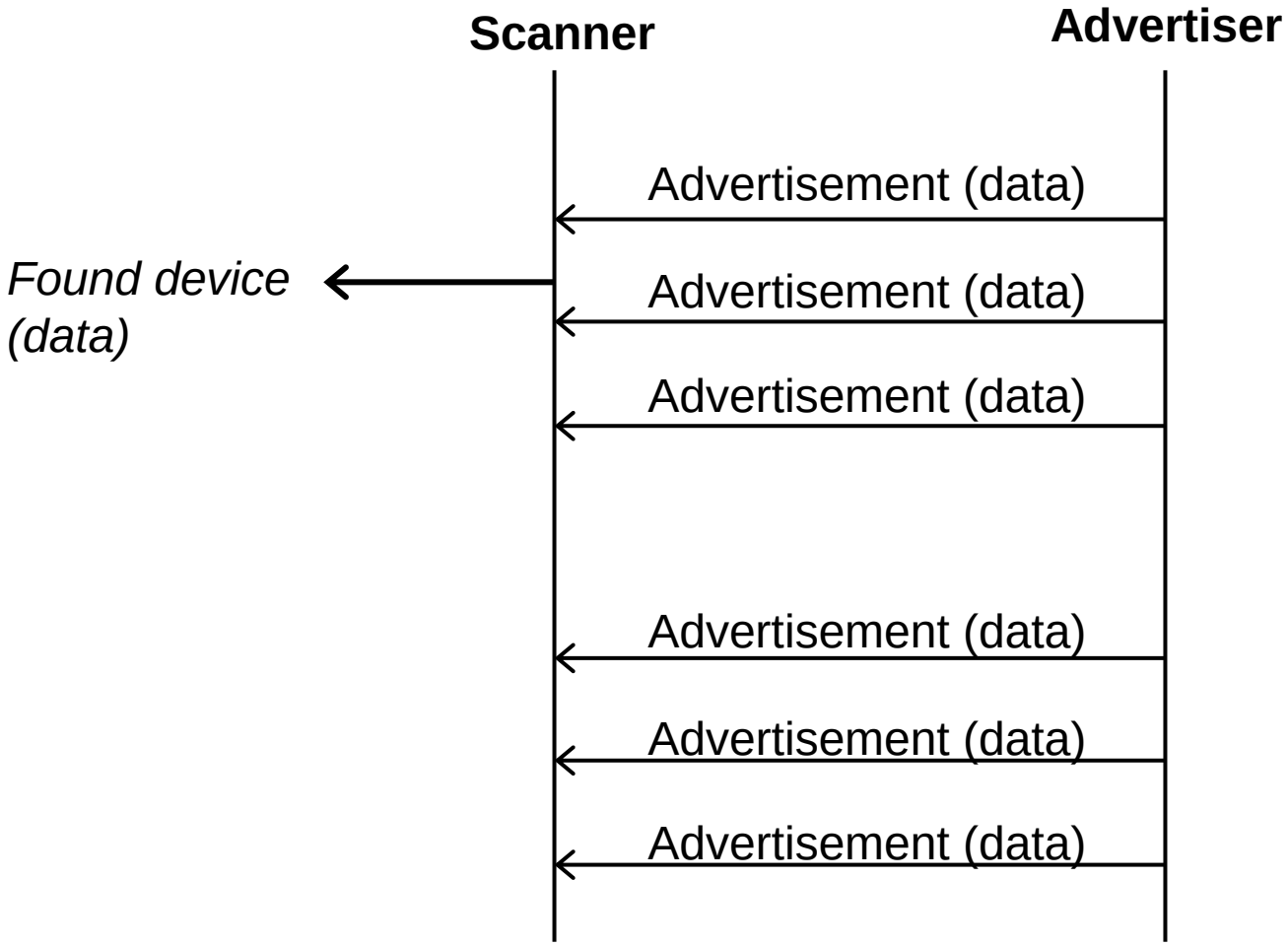
Passive scanning



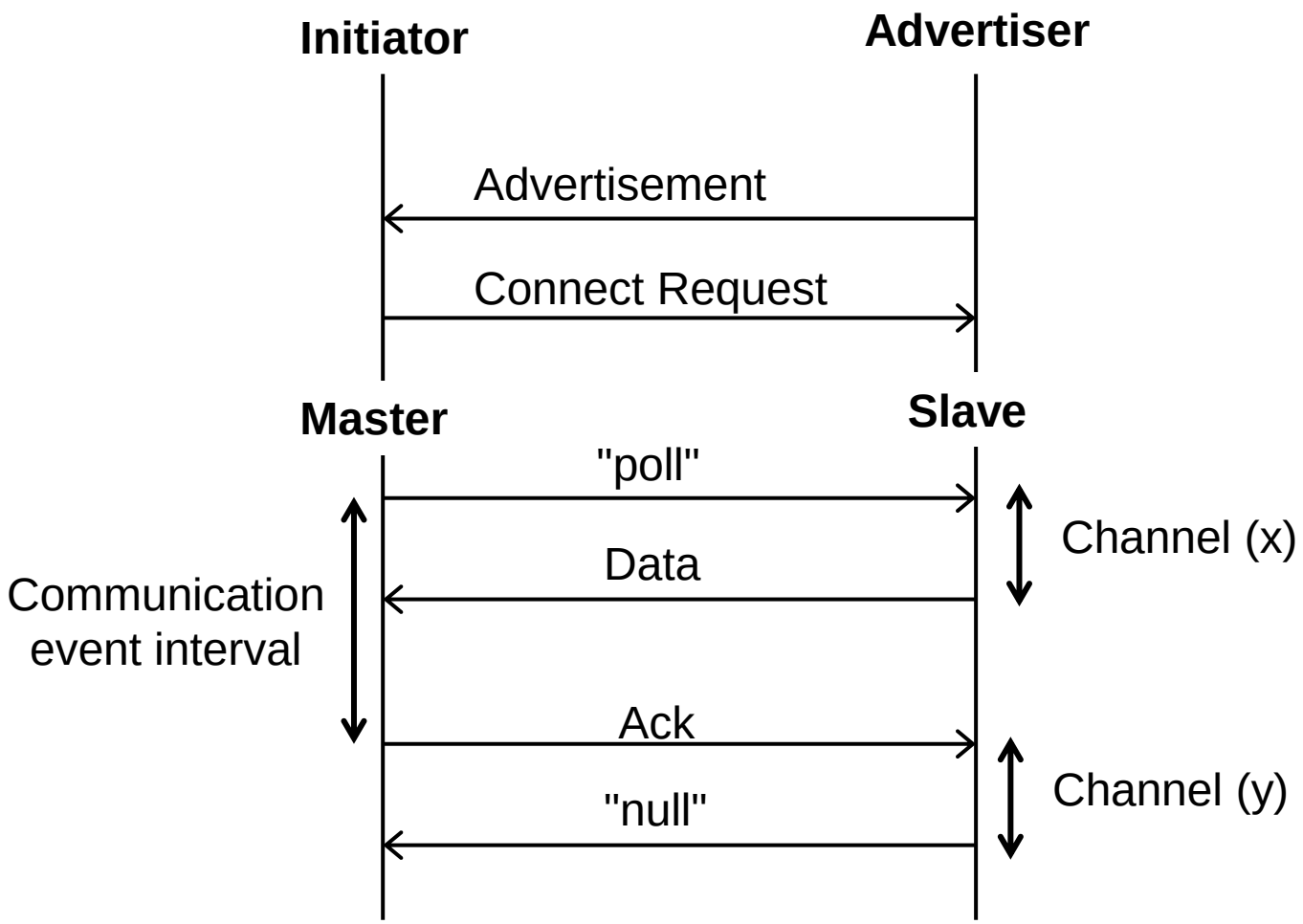
Active scanning



Broadcasting data



Initiating a connection



Link Layer: PDU

Preamble	Access Address	PDU Header	PDU Payload	CRC
1 byte	4 bytes	2 bytes	variable (0 – 37 bytes)	3 bytes

01010101
or
10101010

- Frequency synchronization
- Symbol timing estimation
- Automatic gain control

- Identifies a LL connection between two devices
- Fixed sequence for advertising PDUs

- Error checking

Link Layer: advertising PDU

Preamble	Access Address	PDU Header	PDU Payload	CRC
1 byte	4 bytes	2 bytes	variable (0 – 37 bytes)	3 bytes

PDU type	Res.	TxAdd	RxAdd	Length	Res.
4 bits	2 bits	1 bit	1 bit	6 bits	2 bits

PDU type	Packet name	PDU type	Packet name
0000	ADV_IND	0011	SCAN_REQ
0001	ADV_DIRECT_IND	0100	SCAN_RSP
0010	ADV_NONCONN_IND	0101	CONNECT_REQ
0110	ADV_SCAN_IND	other	Reserved

Link Layer: data PDU

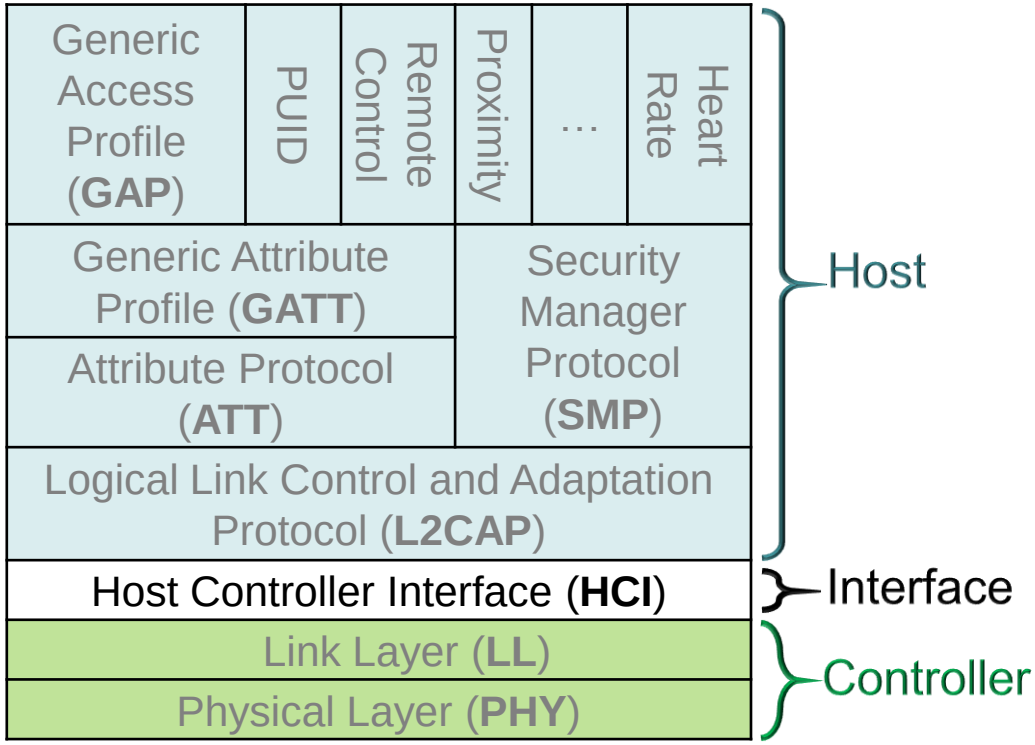
Preamble	Access Address	PDU Header	PDU Payload	CRC
1 byte	4 bytes	2 bytes	variable (0 – 37 bytes)	3 bytes

LLID	NESN	SN	MD	Res.	Length	Res.
2 bits	1 bit	1 bit	1 bit	3 bits	5 bits	3 bit

LLID	Packet type
00	Reserved
01	LL Data PDU: continuation fragment of an L2CAP message or empty PDU
10	LL Data PDU: start of an L2CAP message
11	LL Control PDU

ata bit

HCI specification

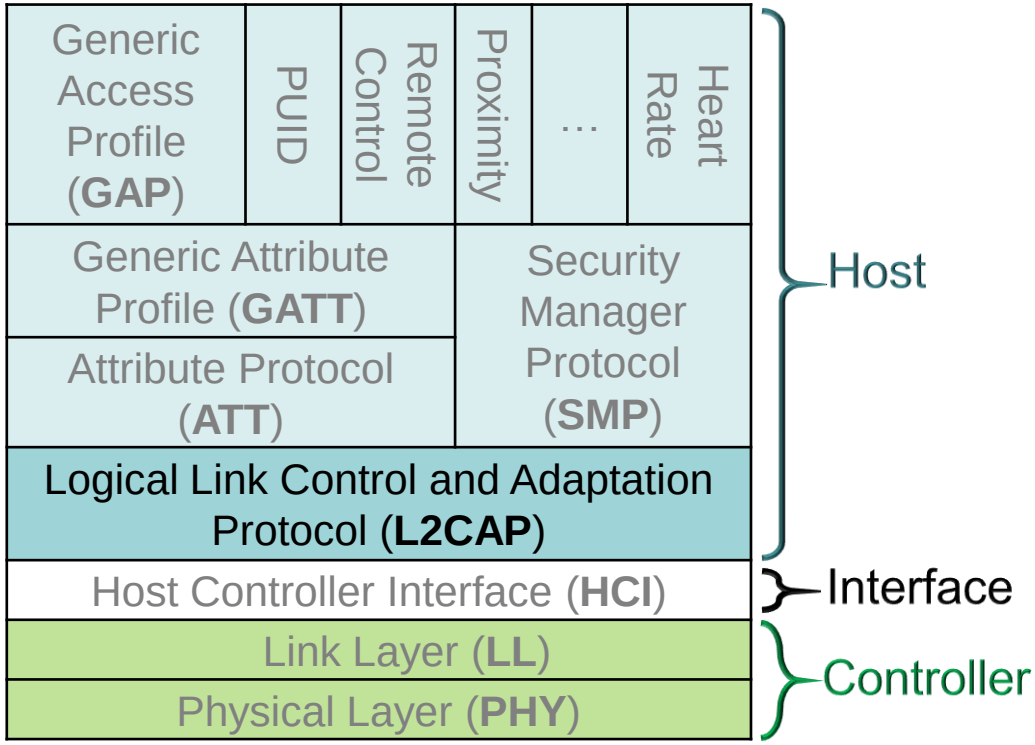


Host Controller Interface

- The HCI provides a uniform interface method of accessing Bluetooth Controller's capabilities (command PHY and LL, access hardware status, control registers)
- Optional implementation
- Possibility of realizing separate Host and Controller

  → interoperability of different subsystems

Host specification



L2CAP (1/2)

- L2CAP provides connection-oriented and connection-less data services to upper layer protocols
  - Protocol multiplexing capability (not in case of LE only Controller)
  - Segmentation and reassembly
  - Per-channel flow control and retransmission

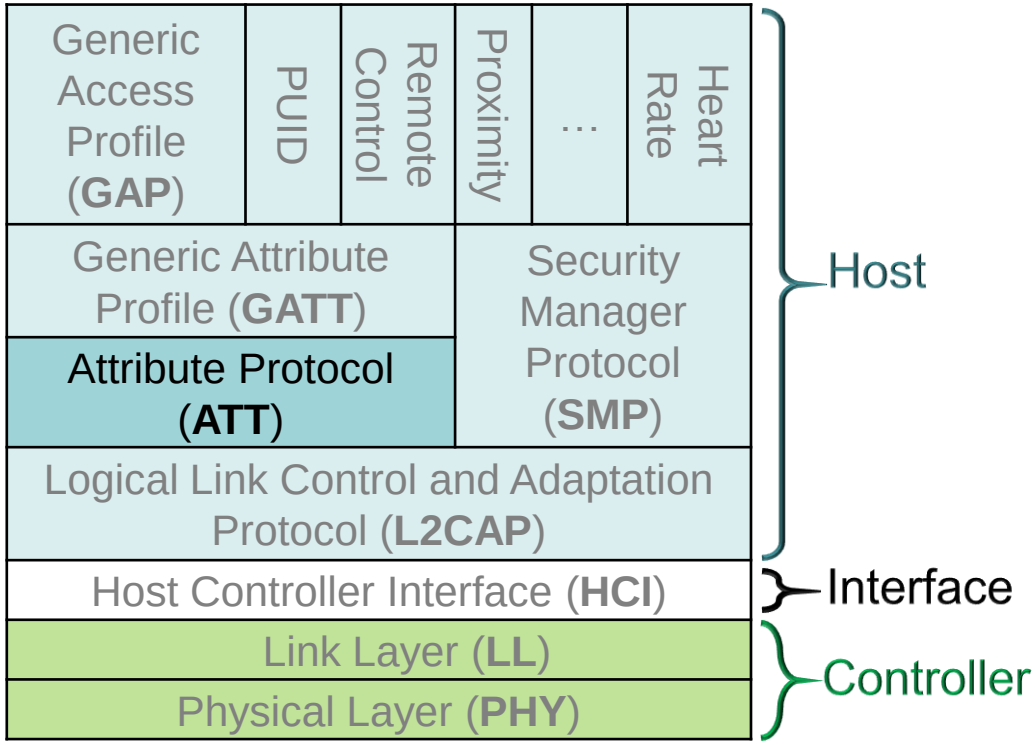
L2CAP (2/2)

- PDU format

Length	CID	Payload
2 bytes	2 bytes	Variable (as specified in ‘Length’)

- 0x0004 = Attribute Protocol
- 0x0005 = LE L2CAP Signaling channel
- 0x0006 = Security Manager Protocol

Host specification



Attribute Protocol (1/2)

- Attribute is ‘data’
  - Value with a meaning (UUID), permissions (read/write), that is addressable by a handle

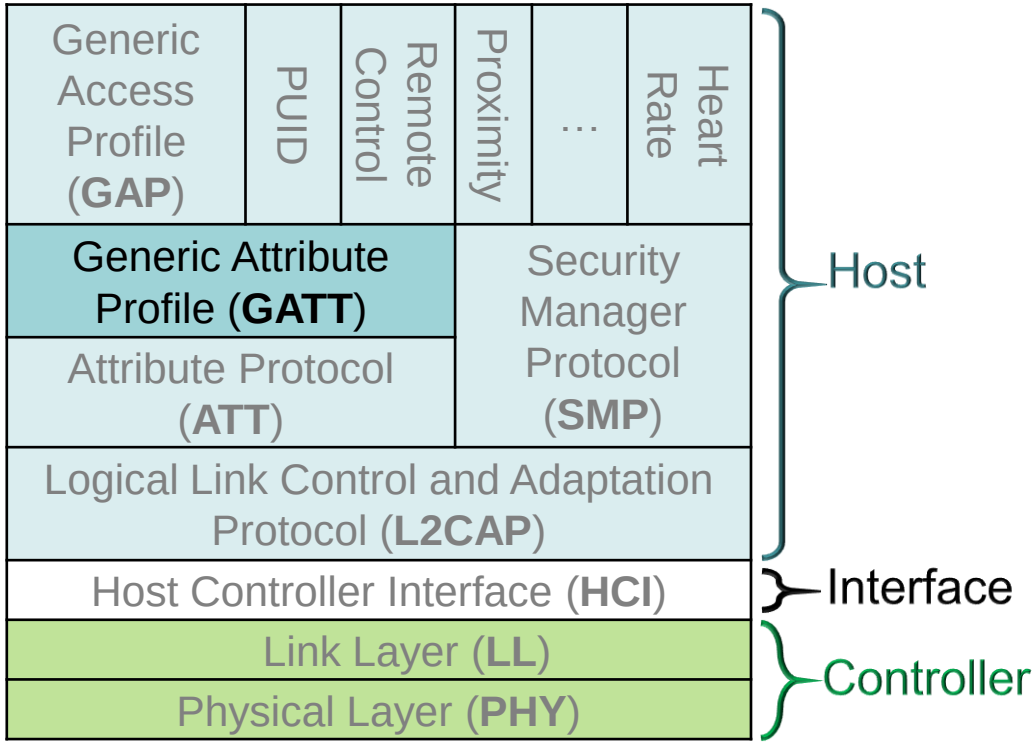
→Attributes expose data on a remote device

- ATT is a peer-to-peer protocol between a server and a client
  - *Server*: contains attributes, receives requests, executes, responds, can indicate values
  - *Client*: sends requests, commands, waits for responses, can confirm indications

Attribute Protocol (2/2)

- Operations on attributes
  - Push: the server sends the data to the client when it changes or according to configuration
  - Pull: a client request the data from the server when it needs it
  - Set: configuring a server (actuator)
  - Broadcast: the server periodically broadcast the data (using LL advertising PDUs)
  - Get: the client requests for attributes handles and UUID to discover the services that the server offers

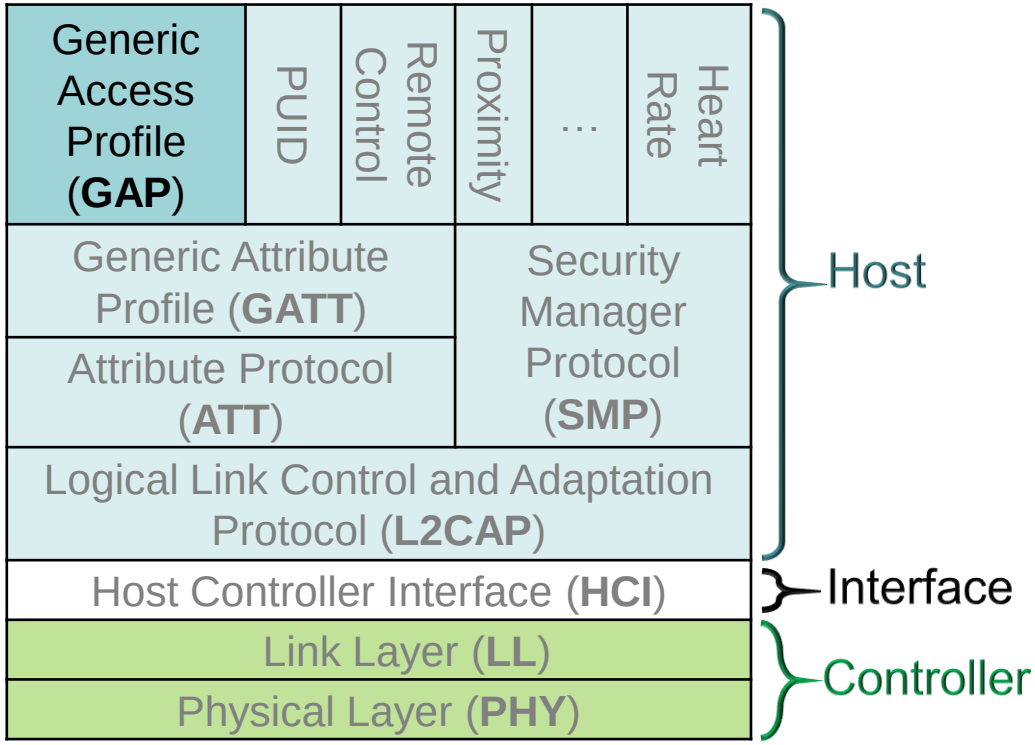
Host specification



Generic Attribute Profile

- The GATT profile is designed to be used by an application or another profile
- It defines how to use the ATT Protocol to discover, read, write and obtain indications of server attributes, as well as configuring broadcast of attributes
- Attributes are grouped in services
  - *service* = collection of data and associated behaviors
  - *characteristic* = value used in a service along with properties and descriptors (how it is accessed, displayed and represented)

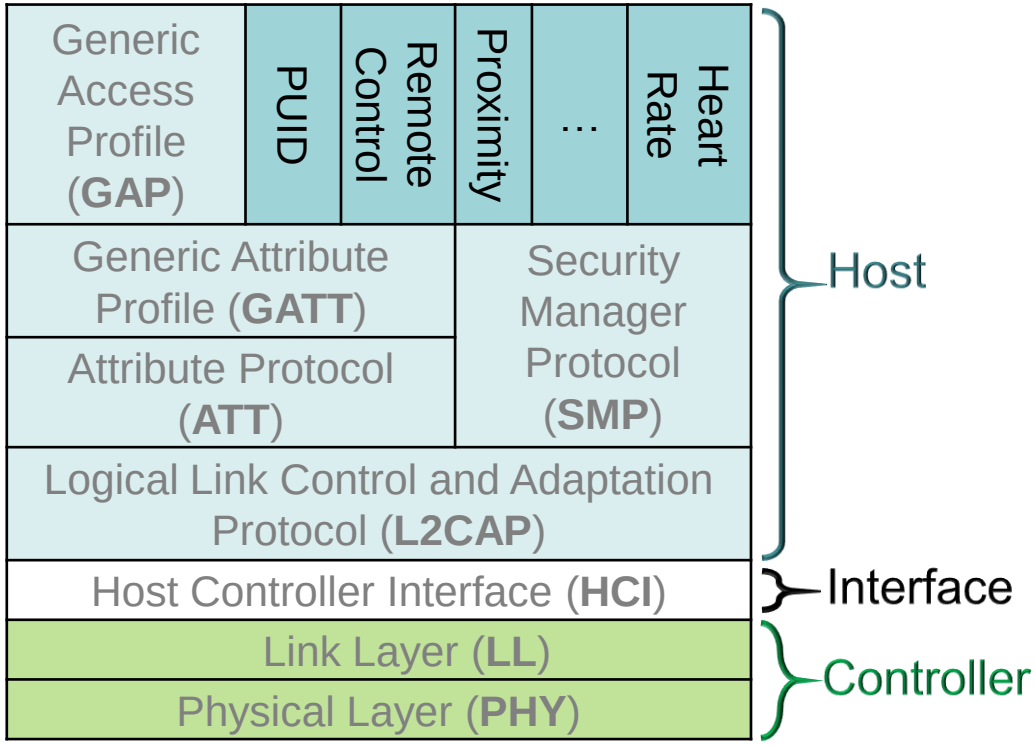
Host specification



Generic Access Profile

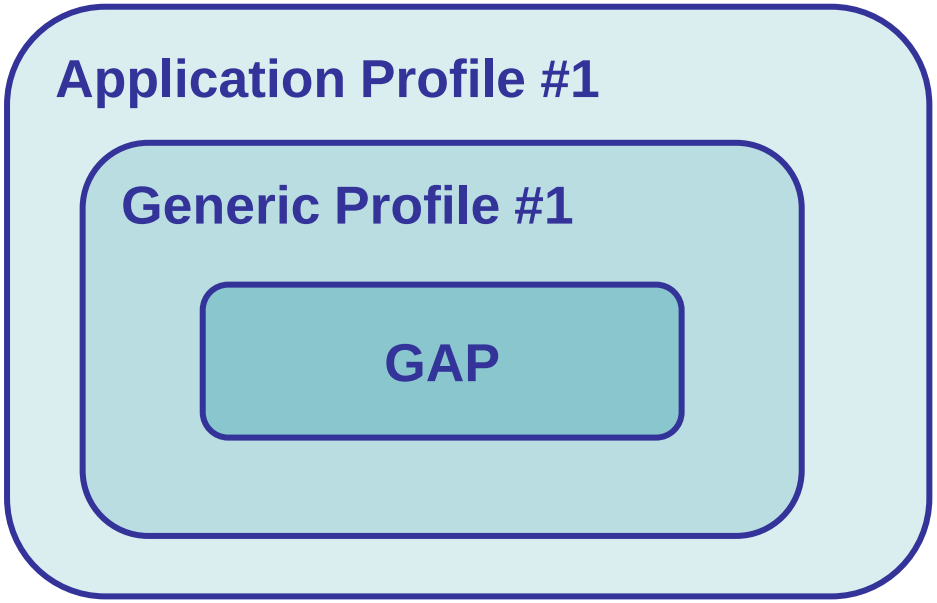
- A bluetooth *profile* defines the required functions and features of each layer in the Bluetooth system
- GAP: base profile implemented by all devices
  - Basic requirements of a device
  - Description of behaviours and methods for device discovery, connection establishment, security, authentication, association models, service discovery
  - Four LE device roles:
    - Broadcaster
    - Observer
    - Peripheral
    - Central

Host specification



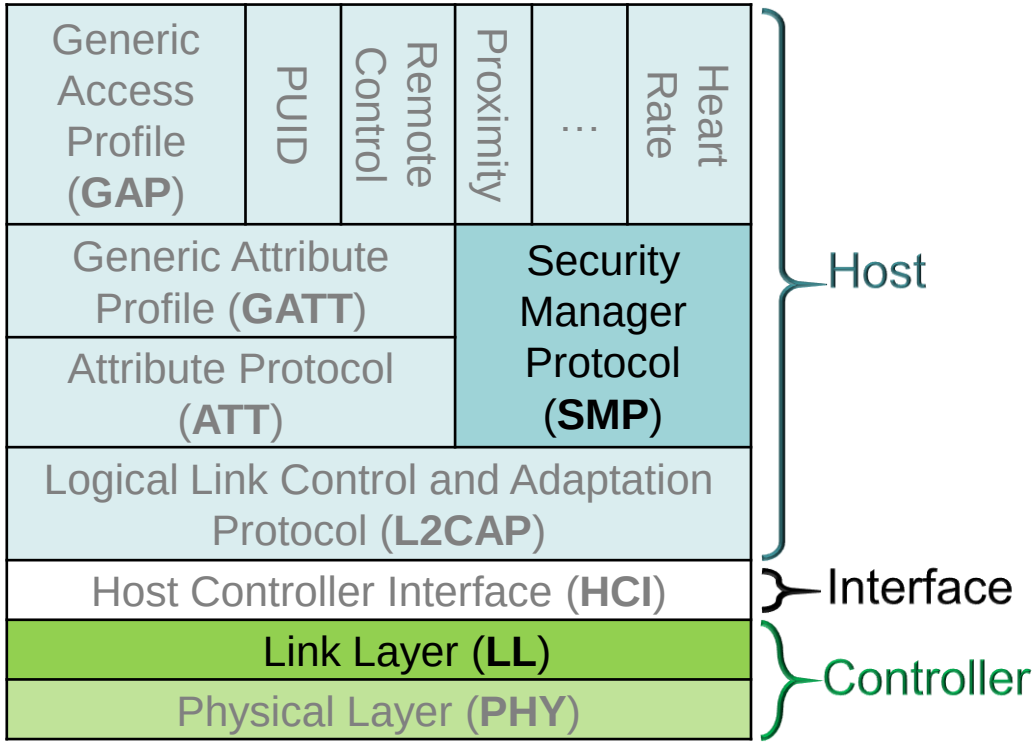
Device profiles

- Profiles can be organized in a hierarchy



- *Application profile*: top level profile that describes application interoperability

Security specifications



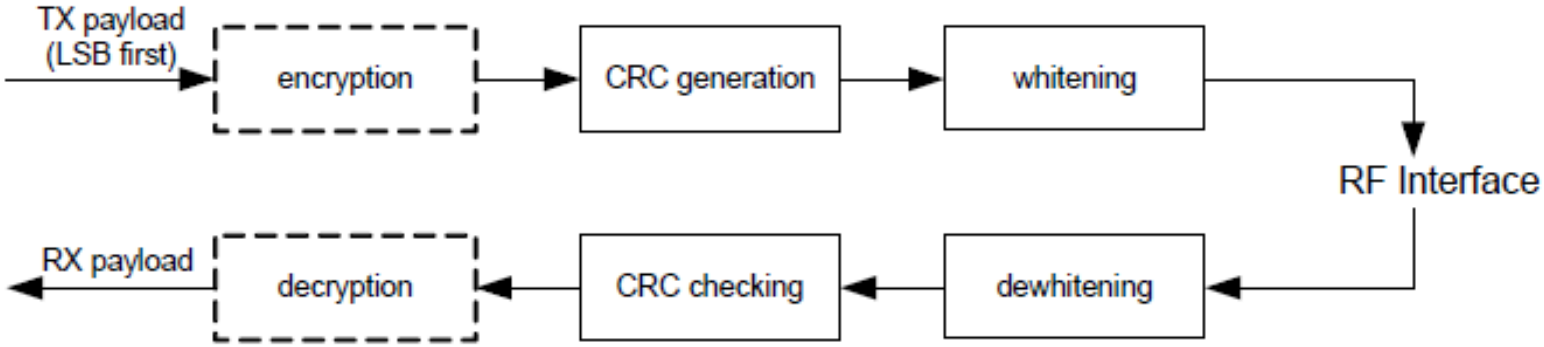
Security (1/4)

- Bluetooth Low Energy provides
  - Eavesdropping protection
  - Man In The Middle protection
  - Privacy of devices
- Security functions are split between host and controller
  - Controller → LL: encryption and authentication
  - Host → SMP: security protocol

Security (2/4)

Encryption and authentication

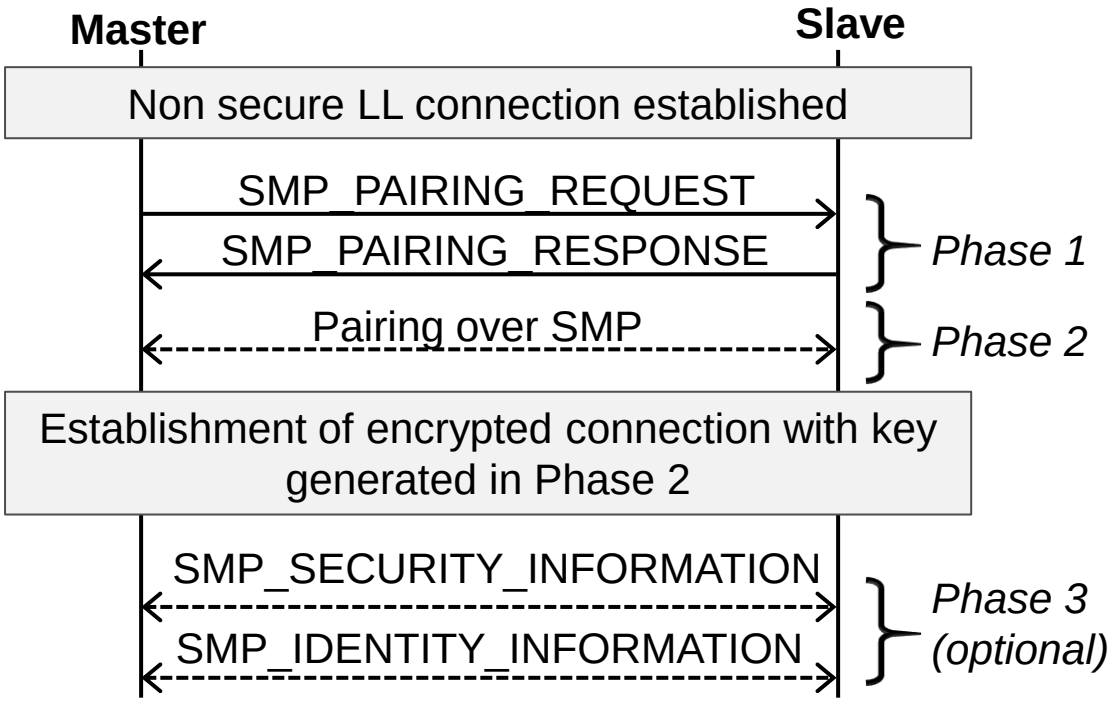
- AES128 – CCM cryptography
- Both hardware and software solutions
- A Message Integrity Check field is included in every encrypted PDU at the end of the payload
- Bit stream process:



Security (3/4)

SMP

- Defines how to setup a secure link
  - Key management and exchange



Security (4/4)

Privacy

- Feature used to prevent device tracking
- Two types of address
  1. *Public*: IEEE MAC address
  2. *Random*: obtained through a hash function from the IRK (Identity Resolving Key)
- Random addresses may be resolved only knowing the IRK
- Random addresses may be changed frequently in time

Products on the market (1/7)

- NORDIC nRF8001
  - Integrates both Controller and Host
  - Serial interface to support external application microcontrollers
  - Designed for Peripheral role devices
  - Temperature sensor

Products on the market (2/7)

- Texas Instrument CC2540
  - Integrates Controller, Host and Application
  - Peripherals to interface with analog and digital sensors
  - Single mode device
  - *Mini development kit* includes:
    - CC 2540 Keyfob (LE slave), with an accelerometer sensor
    - CC2540 USB Dongle (LE master)

    → 99 $

TEXAS INSTRUMENTS

Products on the market (3/7)

- BLUEGIGA BLE 112 *Low Energy Module*
  - Integrates Controller, Host and Application space for customer applications (no external processor needed)
  - Hardware interfaces to connect sensors and/or simple user interfaces
  - Single mode device
  - Designed for master and slave roles
  - Battery monitor and temperature sensor

Products on the market (4/7)

- BLUEGIGA BLED 112 *Low Energy USB Dongle*
  - Integrates Controller, Host and Application
  - Single mode USB device enabling LE connectivity for PCs and other devices having a USB port
  - BLE 112 Starter Kit includes:
    - 2 BLE112 Modules
    - 2 BLED112 USB Dongles

    → 440 $

Products on the market (5/7)

Device	Tx power [dBm]		Rx sensitivity [dBm]	Current consumption			Power supply [V]	
	min	max		Tx (@ 0 dBm)	Rx	sleep	min	max
NORDIC nRF8001	- 18	0	- 87	13 mA	14.5 mA	0.5 µA	1.9	3.6
TI CC2540	- 20	+ 4	- 93	27 mA	19.6 mA	0.4 µA	2	3.6
BLUEGIGA BLE 112 / BLED 112	- 23	+ 4	- 93	27 mA	22.1 mA	0.4 µA	2	3.6

Products on the market (6/7)

- Dayton Industrial Co. Ltd **Heart Rate Belt**
  - Based on nRF8001 chip
  - "*Heart rate monitors are one of the first and most sought after use cases for Bluetooth low energy*" [Johnson Chan, Product Engineering Manager at Dayton]

Products on the market (7/7)

- Casio G-SHOCK **Watch**
  - Automatic correct time update
  - Incoming calls and messages notification

References

- Specification of the Bluetooth System, version 4.0, available at www.bluetooth.org, June 2010
- www.bluetooth.com
- www.ti.com
- www.nordicsemi.com
- www.bluegiga.com
- http://world.casio.com/news/2011/watch_prototype/

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Flavia Martelli

flavia.martelli@unibo.it
+39 051 20 93549