Bluetooth® low energy technology

Bluegiga Technologies

Topics

- Background
- What is *Bluetooth* low energy?
- Basic concepts
- Architecture
- Differentiation and comparison
- Markets and applications

Background

18/11/11

Background

2001:

- First ideas from Nokia: BTLite

2006:

- Nokia, Suunto, Nordic Semiconductor etc. form Wibree Forum to further develop the technology

June 2007:

- Bluetooth SIG together with Nokia agreed that the Wibree Forum is merged with the Bluetooth SIG

- Wibree addresses devices with very low battery capacity and as it could be easily integrated with *Bluetooth* technology, it will round out *Bluetooth* technology's wireless Personal Area Networking (PAN) offering

Background

December 2009:

- First version of the core specification was released

July 2010:

- First version of the host specification was released

March 2011:

- First Bluetooth LE profiles adopted

2011:

- First *Bluetooth* low energy devices appear on the market bluegiga

What is *Bluetooth* low energy?

18/11/11

What is *Bluetooth* low energy?

***Bluetooth* low energy is a NEW, open, short range radio technology**

- Blank sheet of paper design
- Different to *Bluetooth* classic (BR/EDR)
- Optimized for ultra low power
- Enables coin cell battery use cases
  - < 20mA peak current
  - < 5uA average current

What is *Bluetooth* low energy?

However...

- Must reuse as much Bluetooth RF as possible
  - Same antenna and RF components
  - Can time division multiplex with *Bluetooth*
- Must reuse Bluetooth HCI
  - Same physical host interfaces: UART, USB and SDIO
  - Same HCI packet format
  - Same HCI OS drivers
- Must reuse Bluetooth L2CAP
  - A known packet multiplexing point

What is *Bluetooth* low energy?

Has same benefits as *Bluetooth* classic:

- Robust
- Interoperable
- Global
- Royalty free
- Small size
- Secure
- Connectivity to mobile phones and PCs

Except:

- Lower power
- Lower cost

Basic concepts

18/11/11

Basic concepts

Everything is optimized for lowest power consumption

- Short packets reduce TX peak current
- Short packets reduce RX time
- Less RF channels to improve discovery and connection times
- Simple state machines
- Single protocol
- Etc.

Why?

- Coin cell batteries will be the main source of power
  - < 20mA peak current
  - < 5uA average current

Basic concepts

Memory is expensive

- Memory requires silicon area, which costs money
- Memory increases leakage current and reduces battery life

So minimize memory requirements

- Short packets require less buffering
- Simple protocol requires less states
- Simple services require less memory

Basic concepts

Peripherals are simple and resource constrained

- Optimize peripherals

Central devices have more resources and power

- Not so critical to optimize
- e.g. mobile phones and PCs

bluegiga

Basic concepts

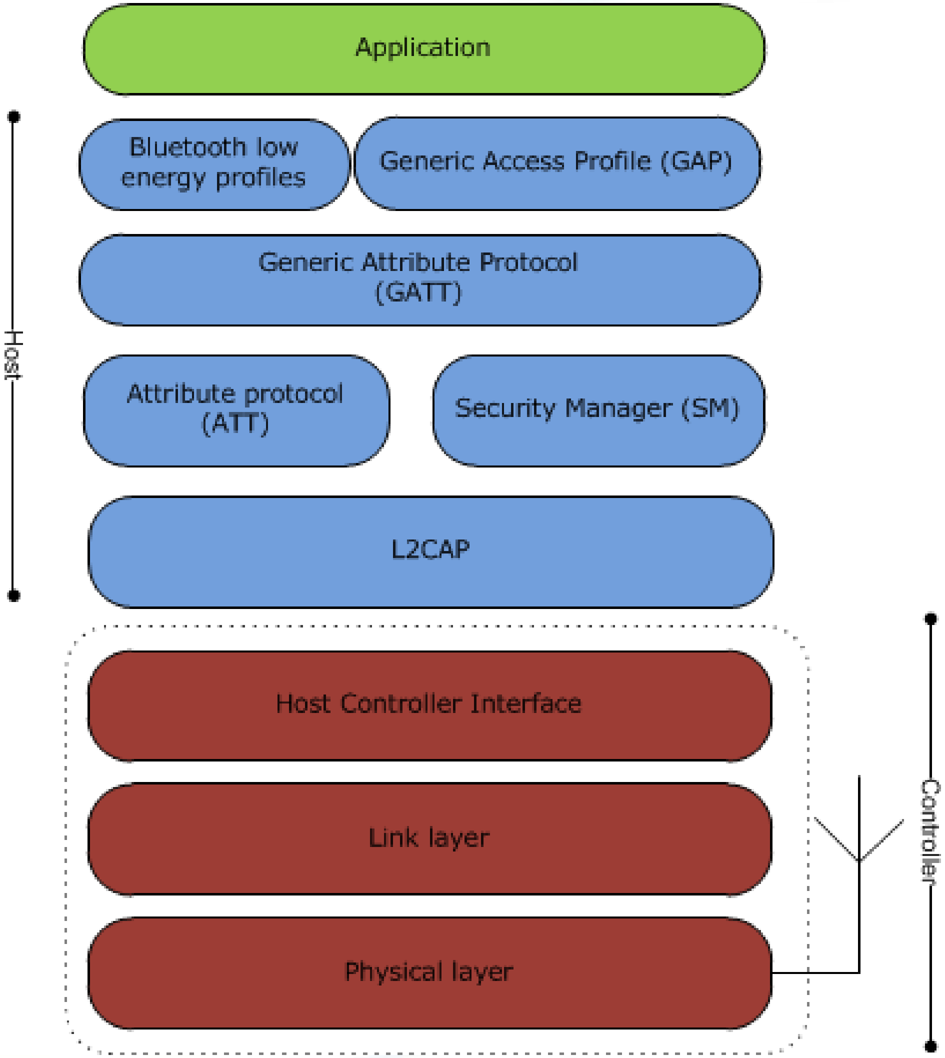
Design for success

- Ability to discover thousands of devices
- Unlimited number of slaves connected to a master
- State of the art encryption
- Security including authentication, authorization and privacy
- Robustness and data integrity

Architecture

18/11/11

Layered architecture


Application
Bluetooth low energy profiles
Generic Access Profile (GAP)
Generic Attribute Protocol (GATT)
Attribute protocol (ATT)
Security Manager (SM)
L2CAP
Host
Host Controller Interface
Link layer
Physical layer
Controller

Profiles

- Application specific data

GAP

- Device discovery, connections

GATT

- Organization of data

ATT

- Data access protocol

L2CAP

- Multiplexer

HCI

- Interface between host and controller

Link layer

- Packets and radio control

Physical layer

- Transmission/reception of bits

Device modes

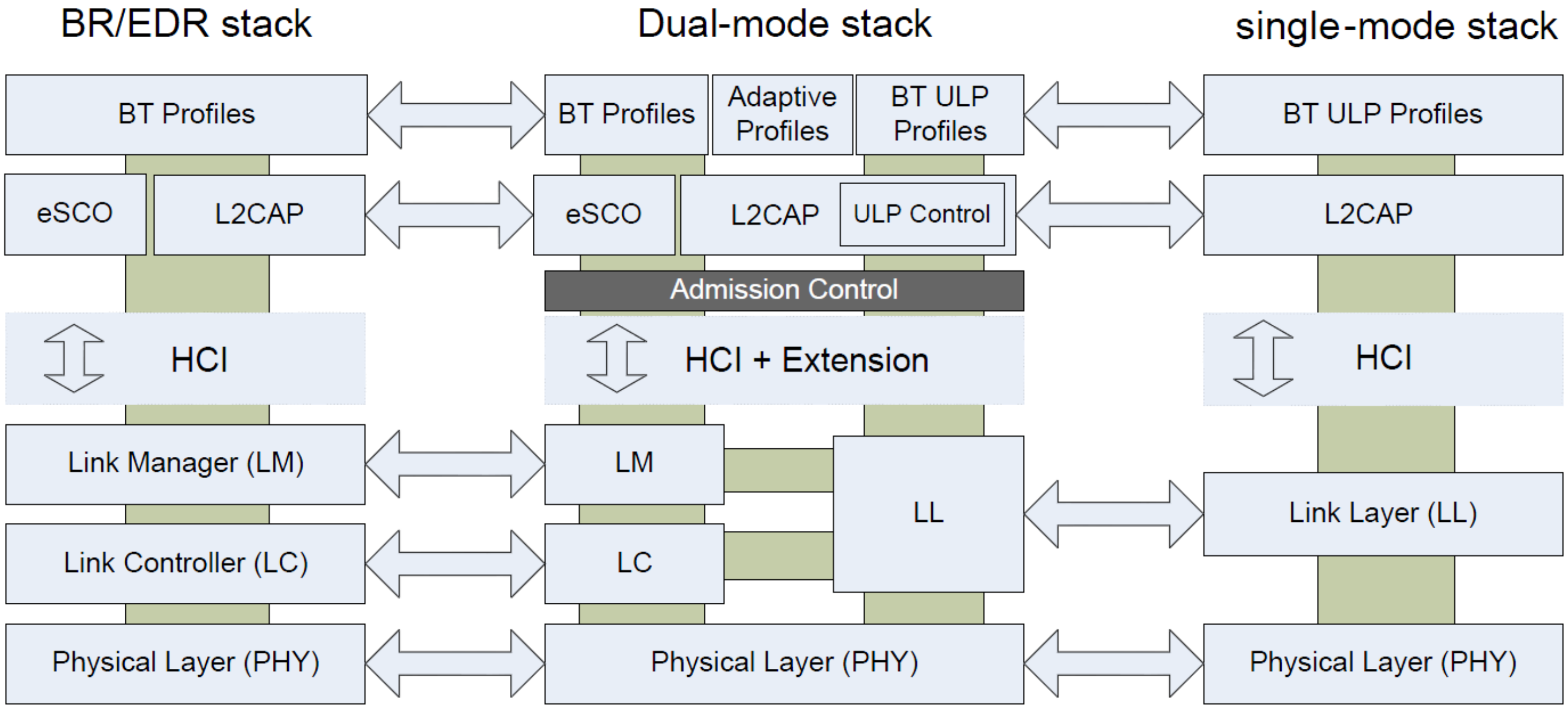
Dual mode

- Implements *Bluetooth* BR/EDR and *Bluetooth* low energy
- Can be used everywhere, where *Bluetooth* is used today

Single mode

- Implements only *Bluetooth* low energy
- Will be used in new devices / applications

Device modes



Physical layer

2.4 GHz transciever

- Industrial Scientific Medical (ISM) band
- 2400 MHz to 2483,5 MHz
- License free

GFSK modulation

- Modulation index 0.5
- -> Improvide SNR and therefore better range

Bandwidth

- 1 Mbps

40 channels

- 2 MHz channel spacing
- 2402 MHz to 2480 MHz

Physical layer

Minimum transmit power

- 0.01mW (-20 dBm)

Maximum transmit power (regultaroty limit)

- 10mW (+10 dBm)

Minimum receiver sensitivity

- -70 dBm (Bit Error Rate 0.1%)

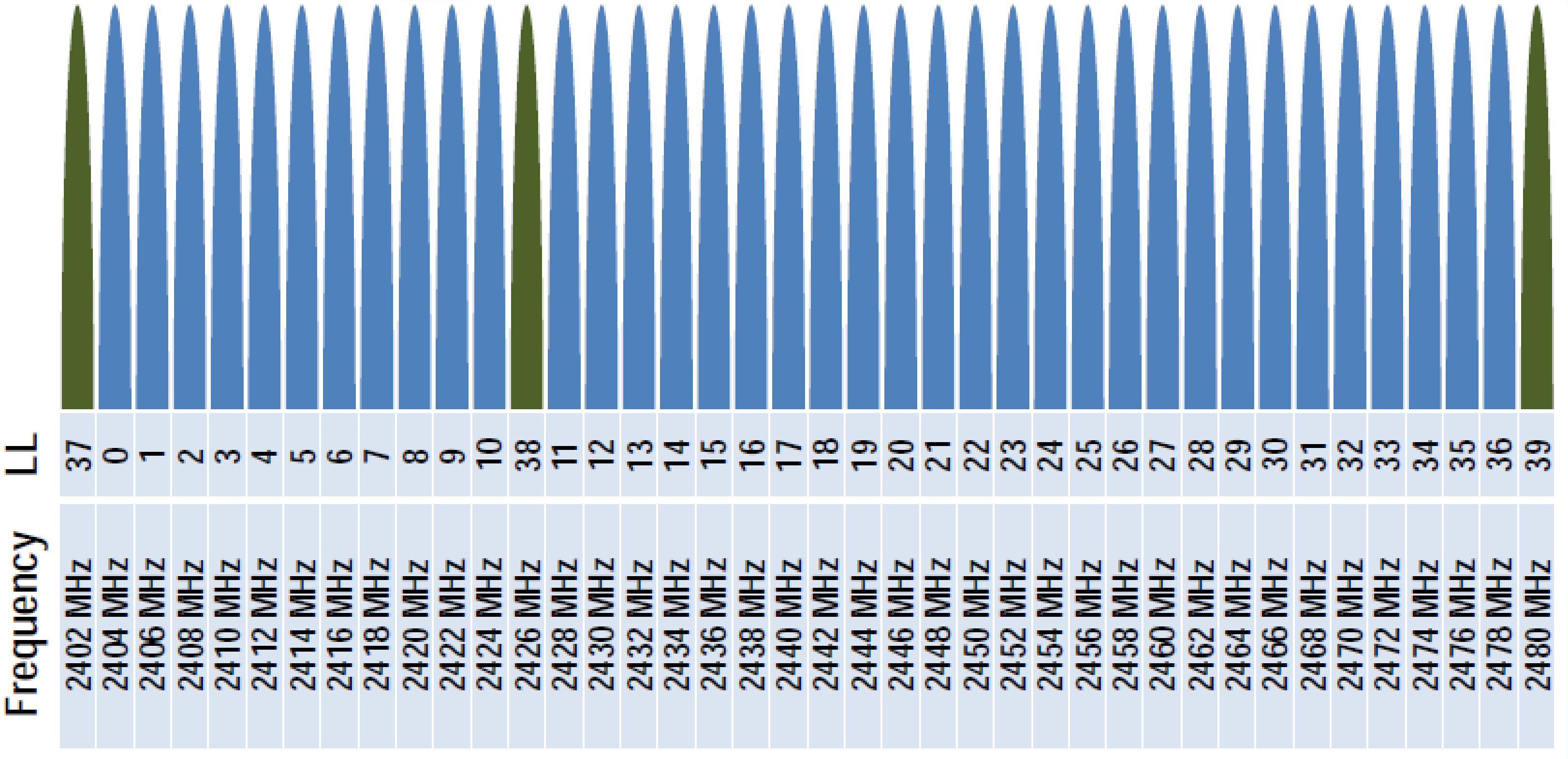
Range

- 0dBm TX power and -70dBm RX sensitivity
- ~ 30 meters
- 10dBm TX power and -90dBm RX sensitivity
- 100+ meters

Typically devices have:

- 0-4 dBm TX-.power
- -85 to -90 dBm sensitivity

Physical layer



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

Link layer

A simple state machine

Channels

- Advertising and data channels

Packets

- Advertising and data packets

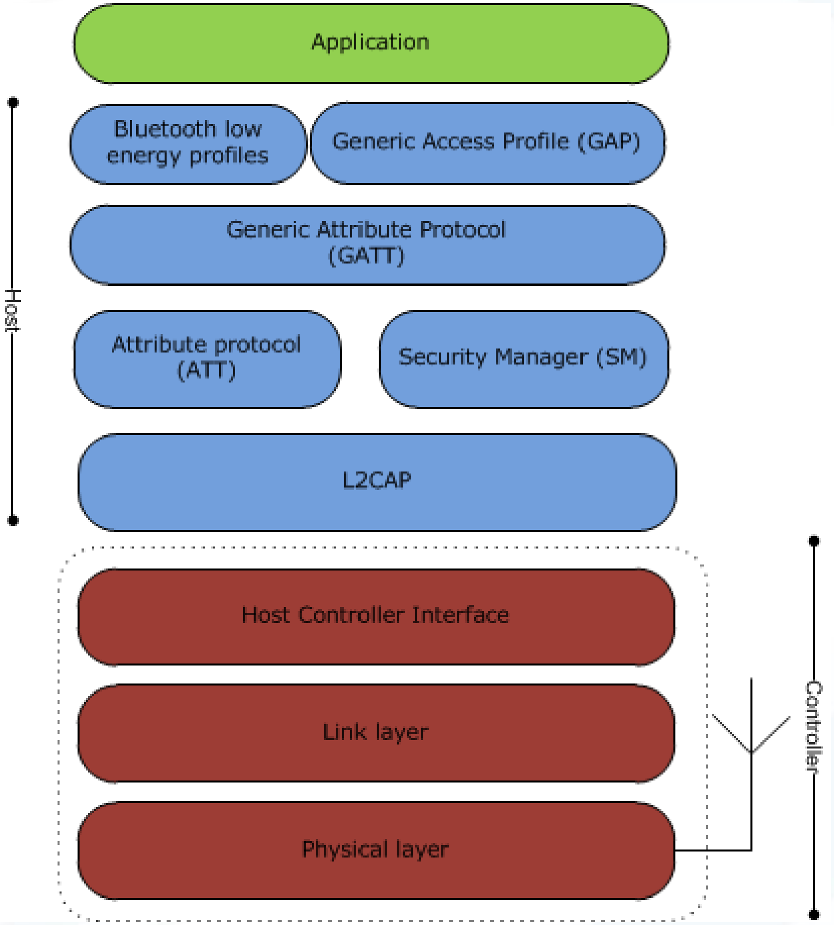
Link layer procedures

- Advertising
- Scanning
- Initiating connections
- Connected

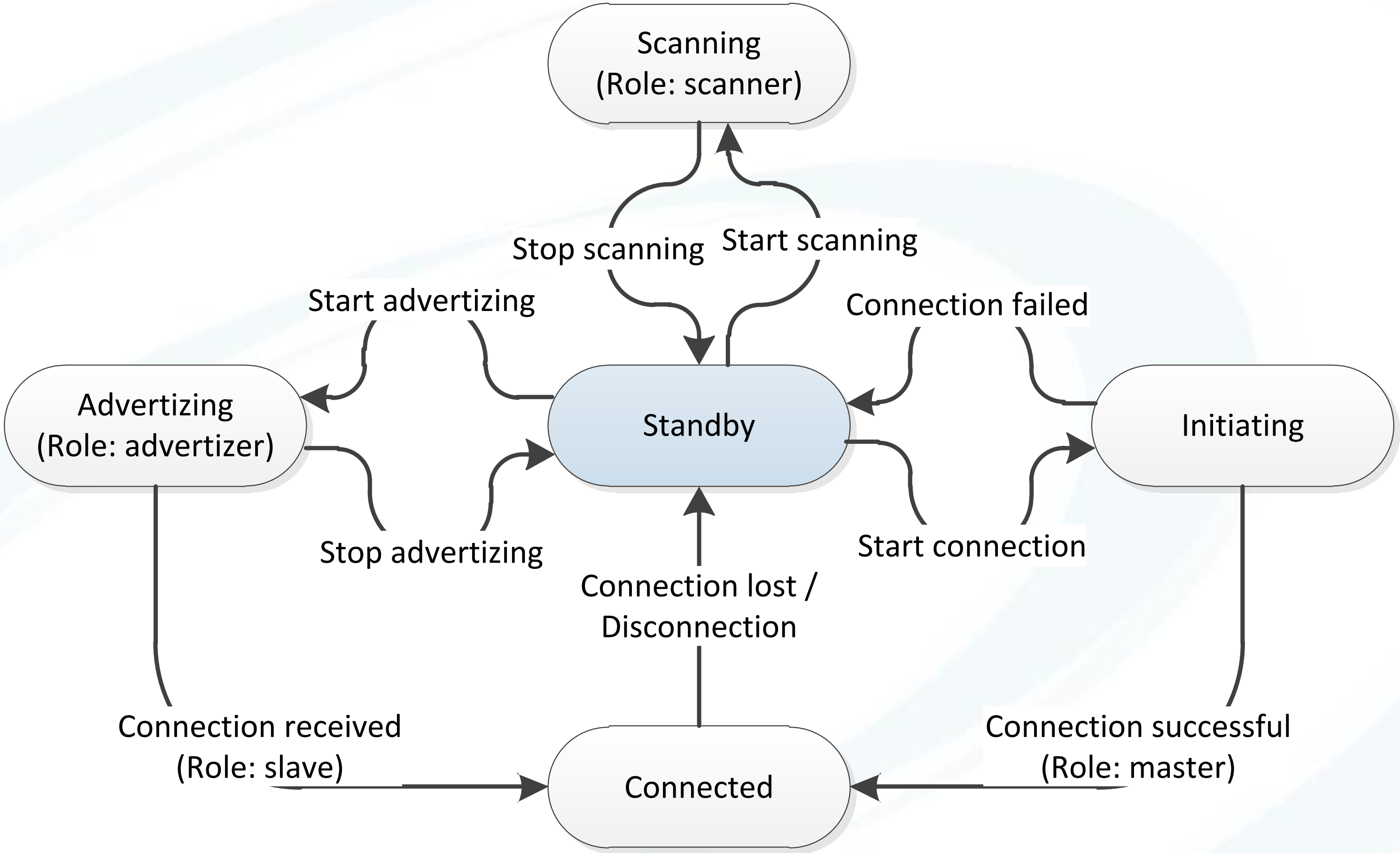
Topologies

- Point-to-point
- Star

Link layer security


Application
Bluetooth low energy profiles
Generic Access Profile (GAP)
Generic Attribute Protocol (GATT)
Attribute protocol (ATT)
Security Manager (SM)
L2CAP
Host
Host Controller Interface
Link layer
Physical layer
Controller

Link layer state machine



Link layer channels

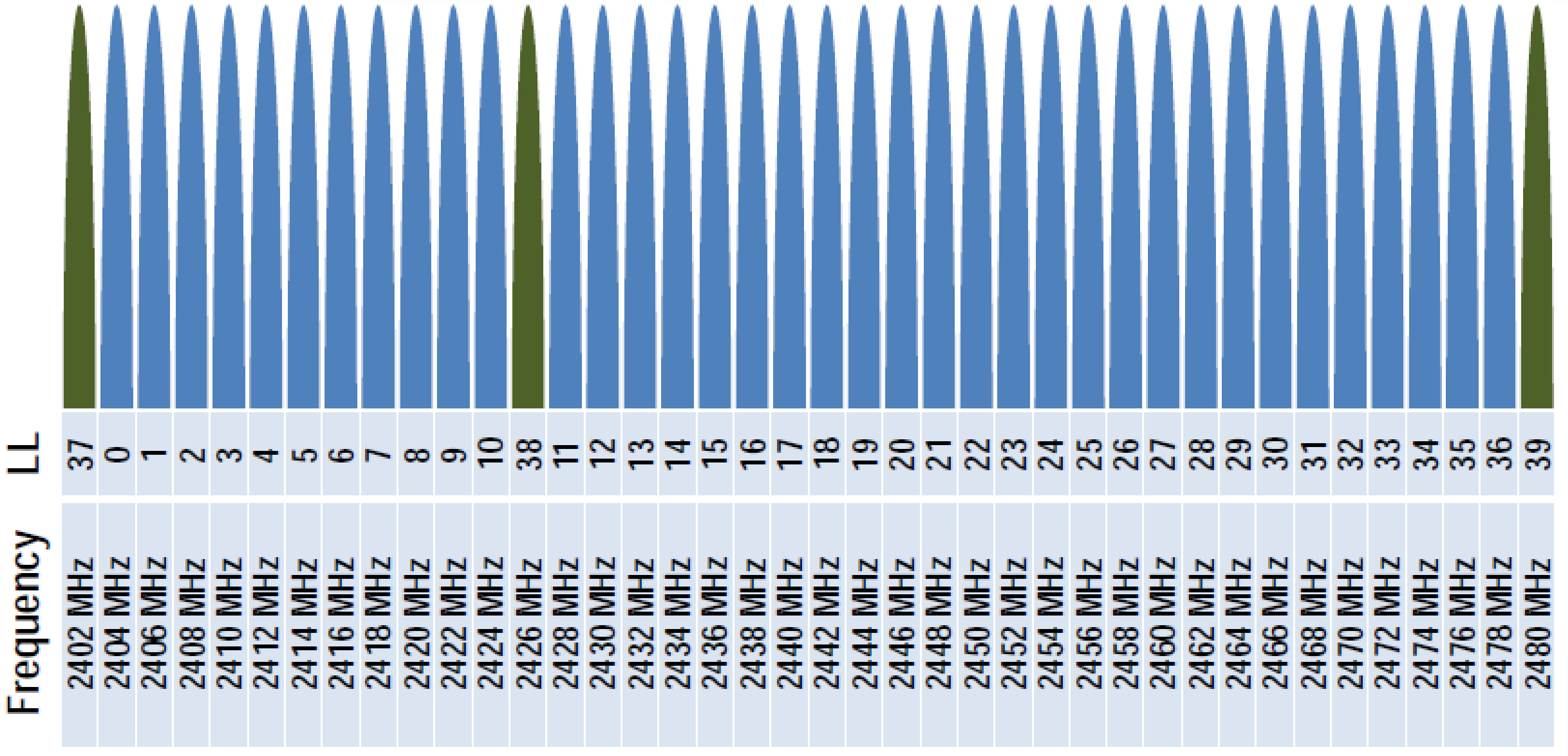
3 advertising channels

- Used for discoverability and connectability
- Used for broadcasting
- Avoid known 802.11 frequencies

37 data channels

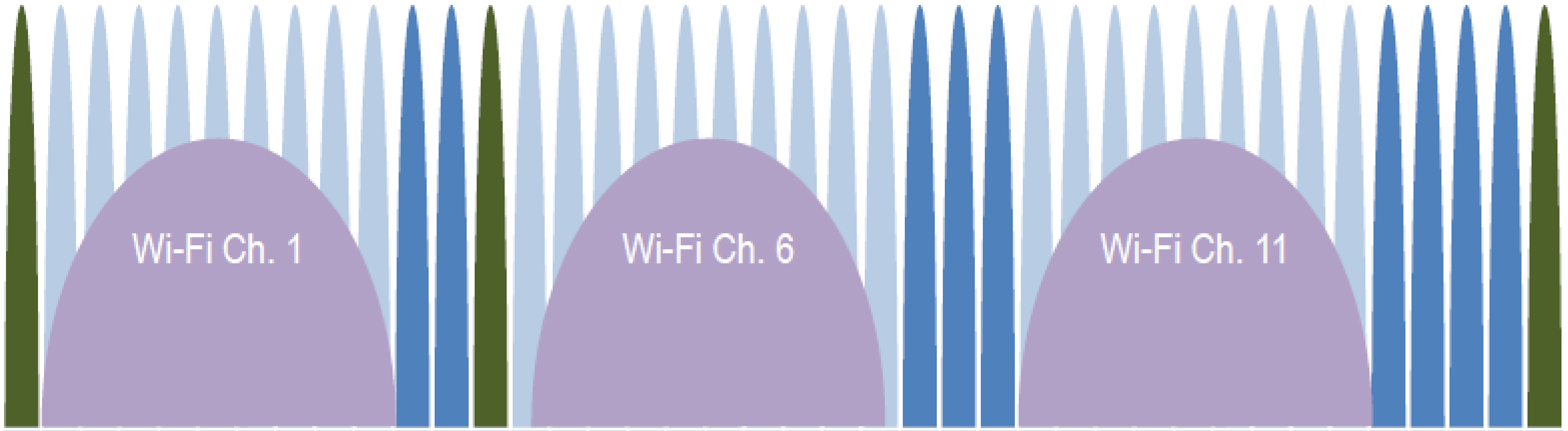
- Used to reliably send application data in a connection
- Use Adaptive Frequency Hopping for co-existence and robustness

Link layer



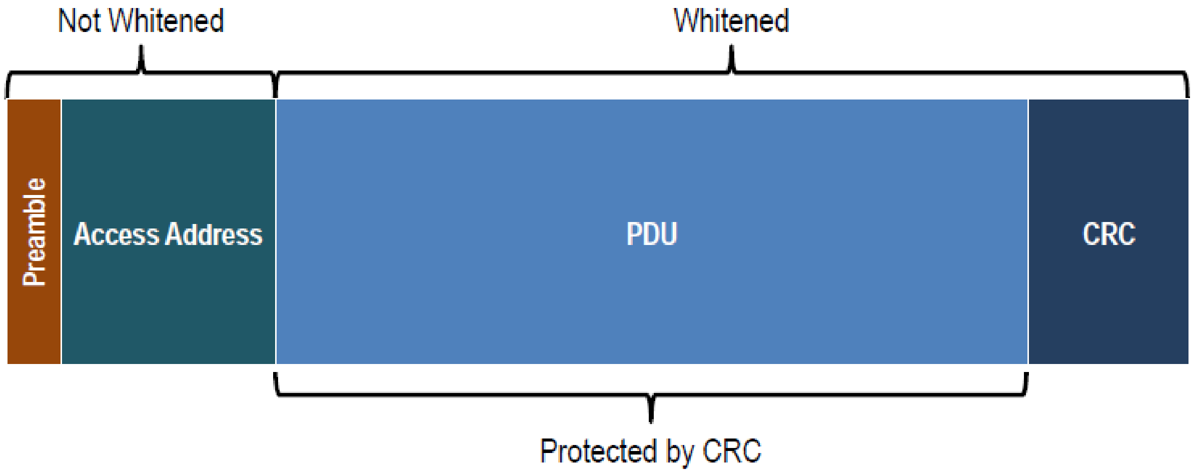
LL	Frequency
37	2402 MHz
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	2426 MHz
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz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

Link layer



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

Link layer packets



Single packet format

- Preamble used to synchronize AGC
- Access address identifies advertising PDUs or device pairs
- PDU contains application data
- 24-bit CRC protects agains errors
    - Better than Bluetooth BT/EDR

Link layer packets

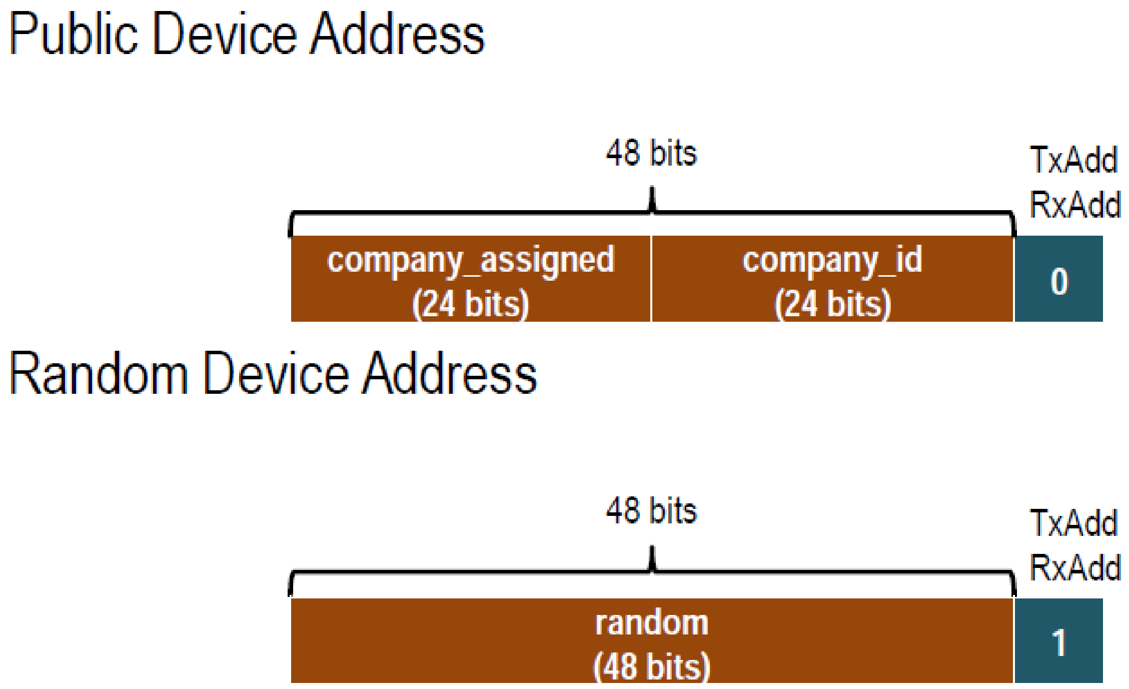
Advertising PDUs

- Used to find devices, get additional information or open connections
- 7 PDU types

Data PDU

- Carries application data reliably

Device address



Public Device Address

48 bits

TxAdd
RxAdd

company_assigned
(24 bits)

company_id
(24 bits)

0

Random Device Address

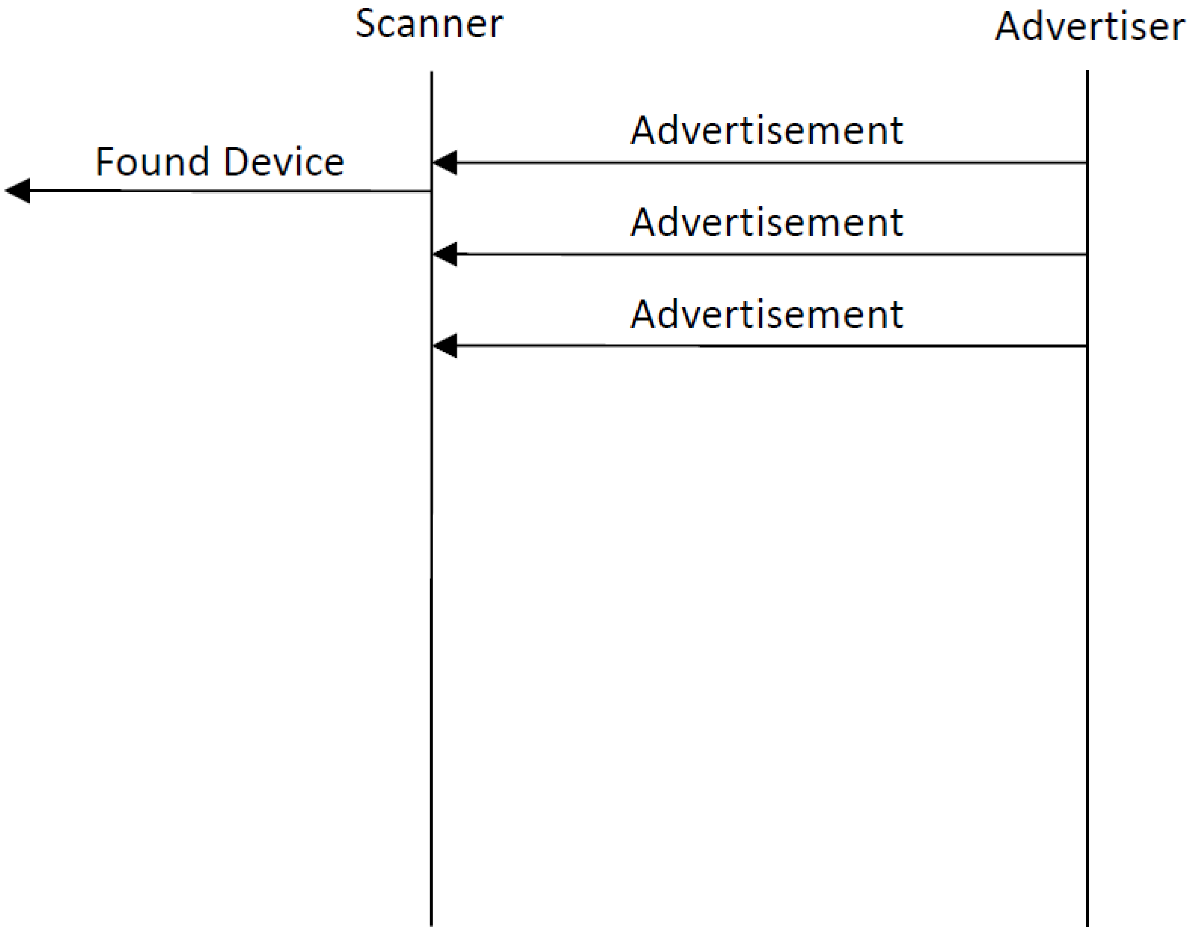
48 bits

TxAdd
RxAdd

random
(48 bits)

1

Link layer: Passive scanning



Advertising

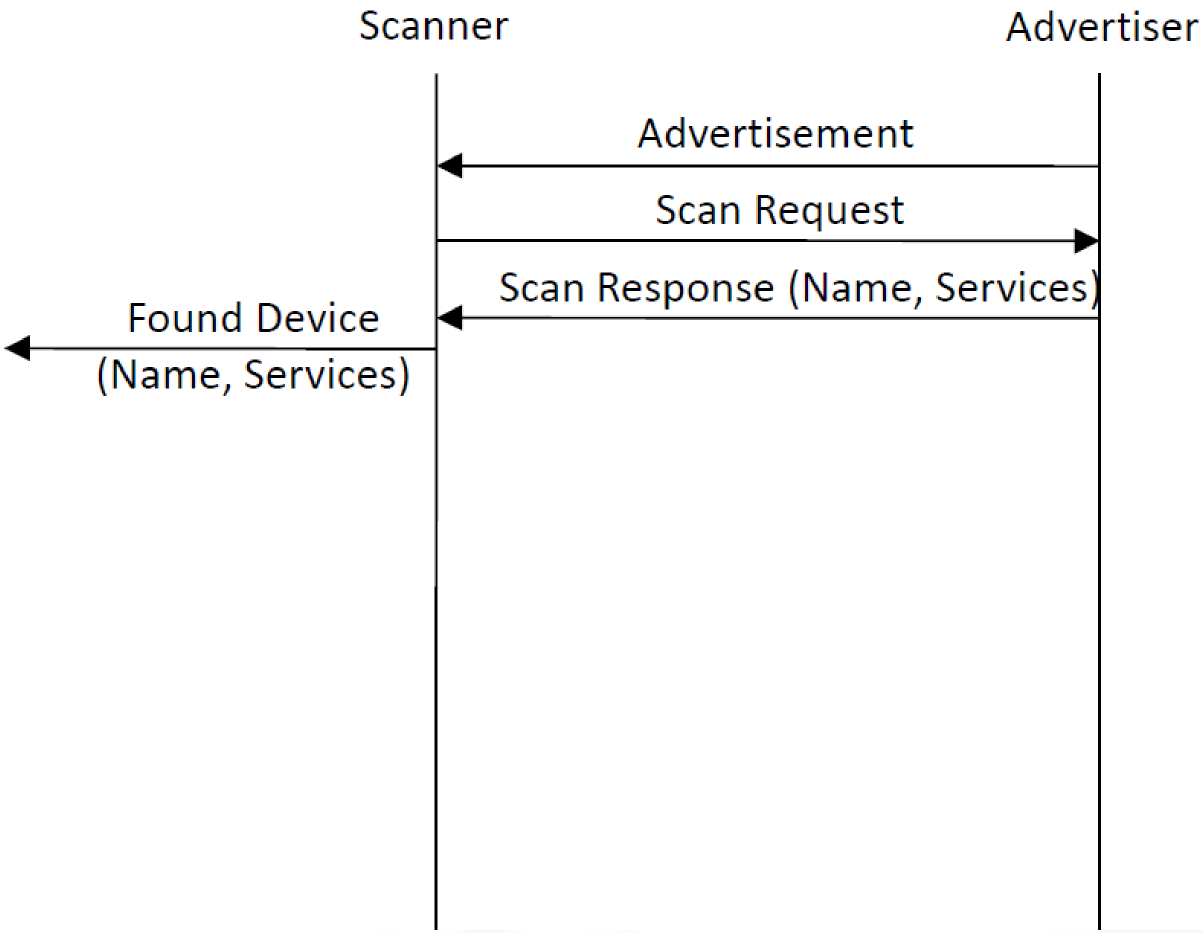
Advertising data

- ”I’m connectable and bondable”
- ”My trasmit power is 0 dBm”
- ”I support heart rate, manufacturer and battery services”

Why advertise?

- Takes around 1.5 ms of time
- 20 x lower power then *Bluetooth* classic

Link layer: Active scanning



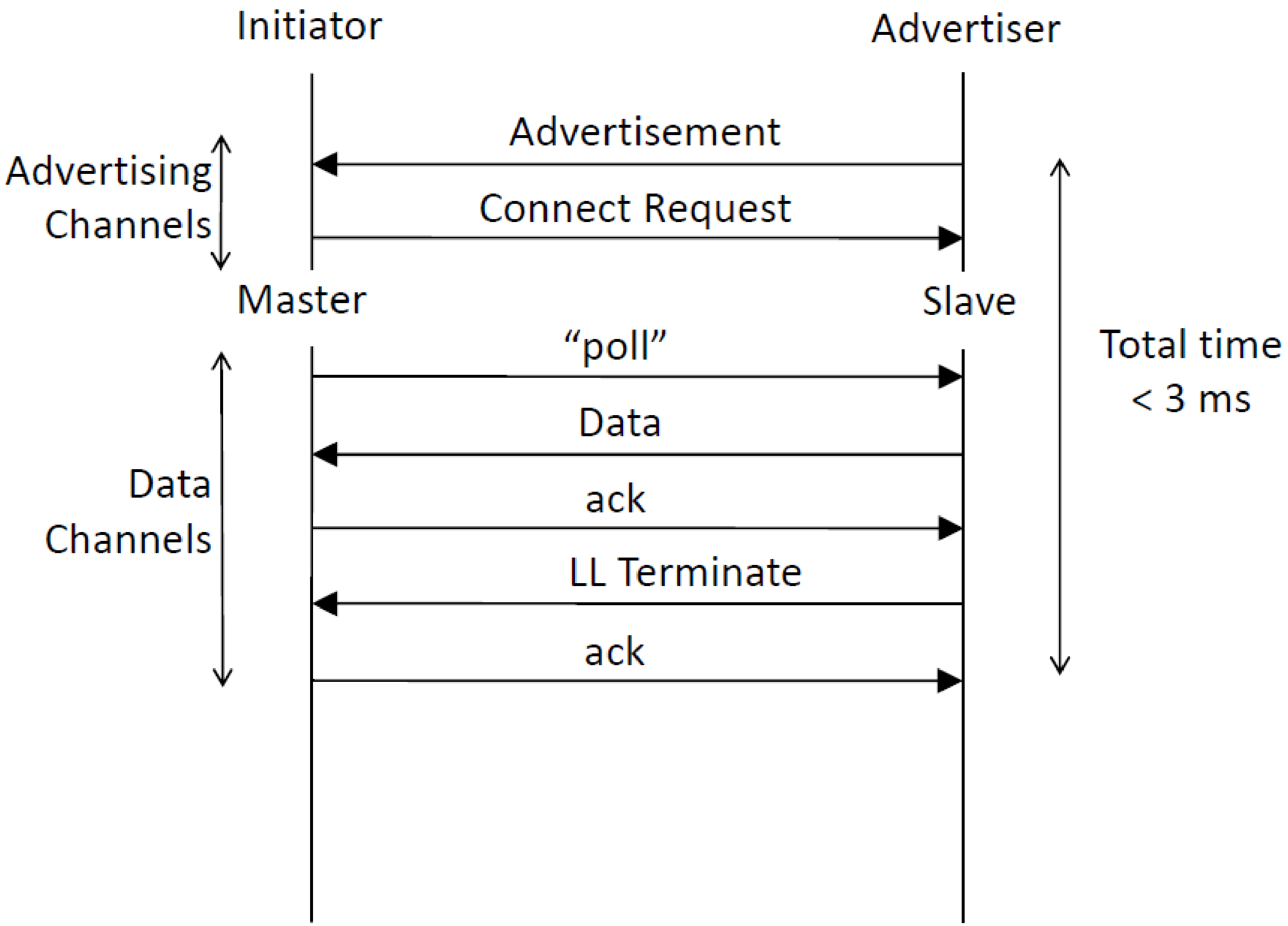
Active scanning

Active scanning used to get more data from the advertiser

Scan response data

- Device name is ”Indoor thermostat”
- Device supports thermometer and battery services

Link layer: Connection



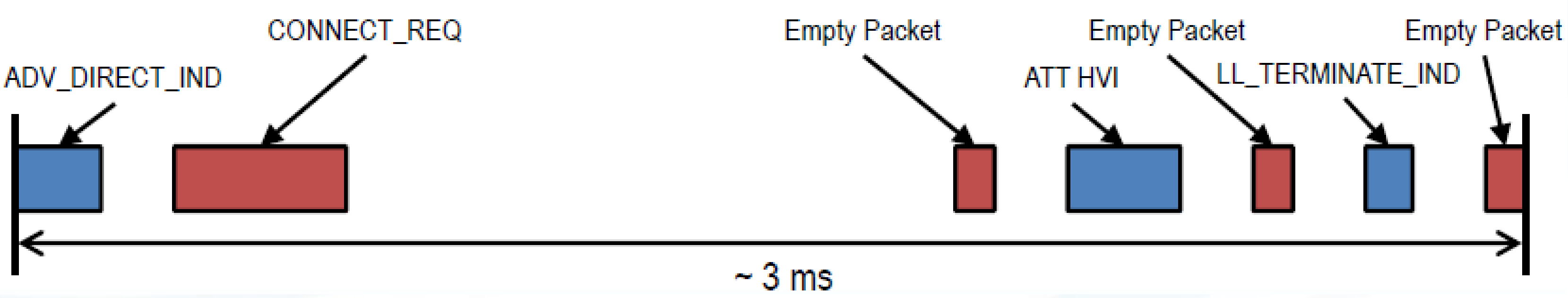
Connections

- **Master always transmits at known “anchor points”**
  - Known as connection interval
  - Starts a connection event
  - From 7.5ms to 4.0s

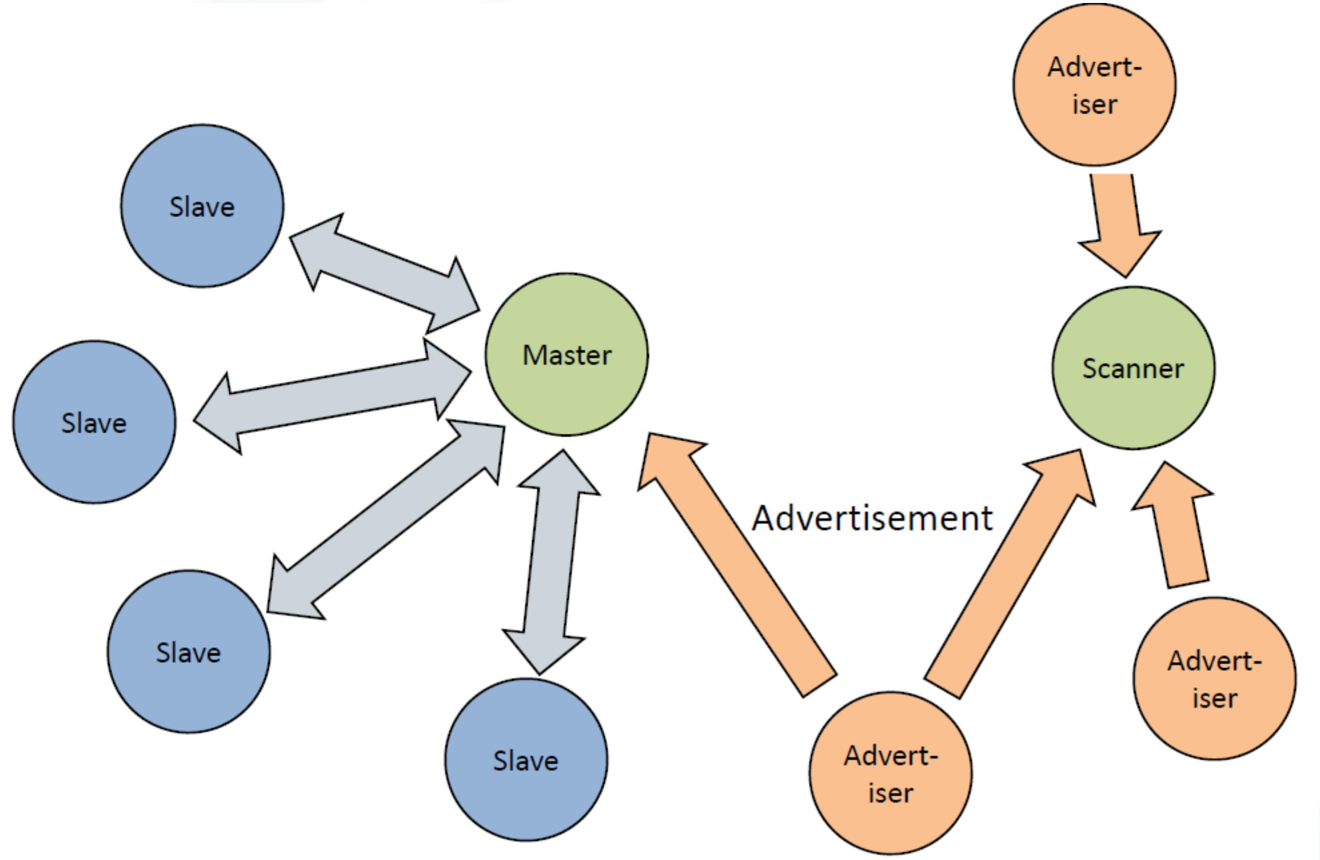
- **Slave is able to listen / communicate**
  - Slave latency allows slave to save power if it has nothing to send
  - Slave can skip N anchor points

- **Automatically extends when**
  - More data bit set by either device

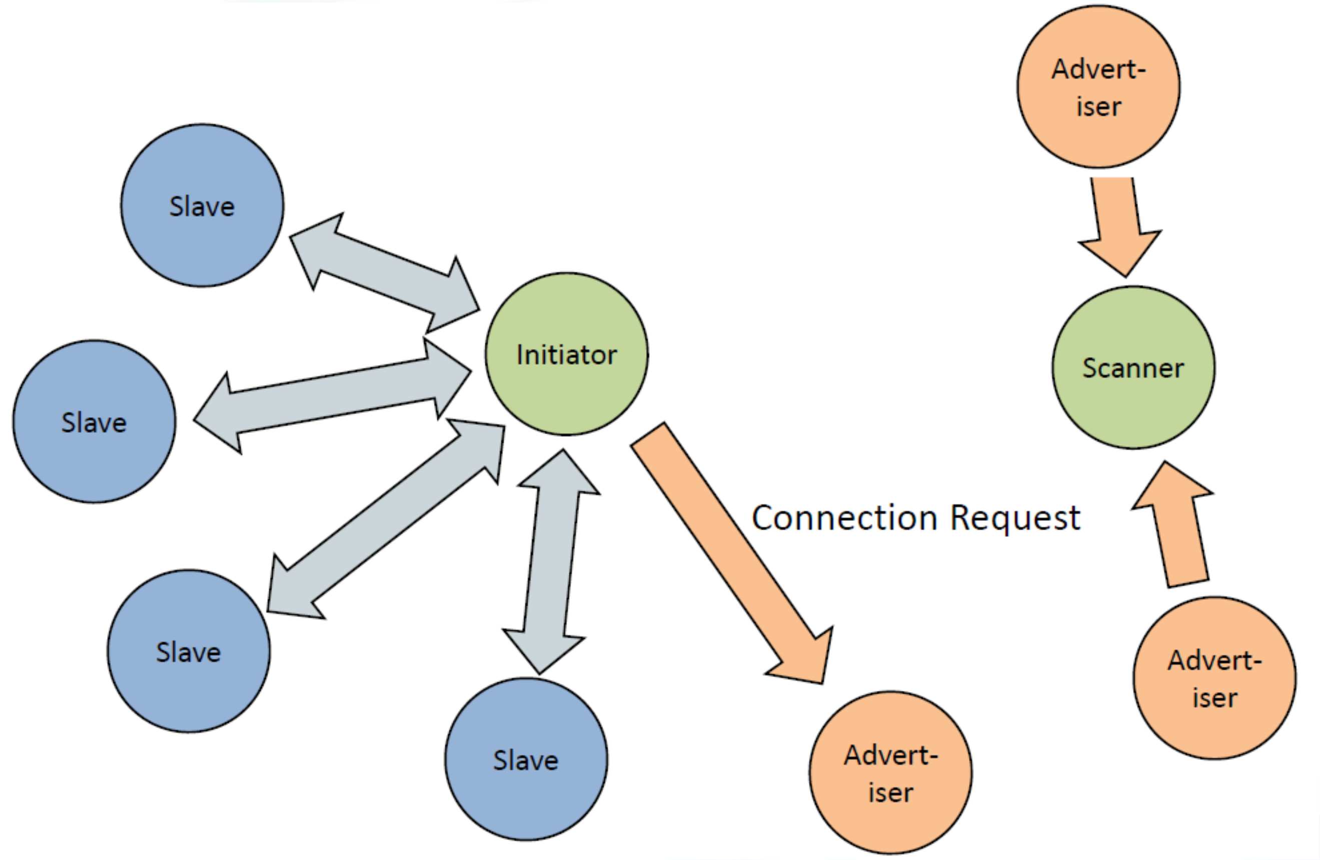
- **Automatically ends when CRC errors received**
  - Move to another channel at next connection event



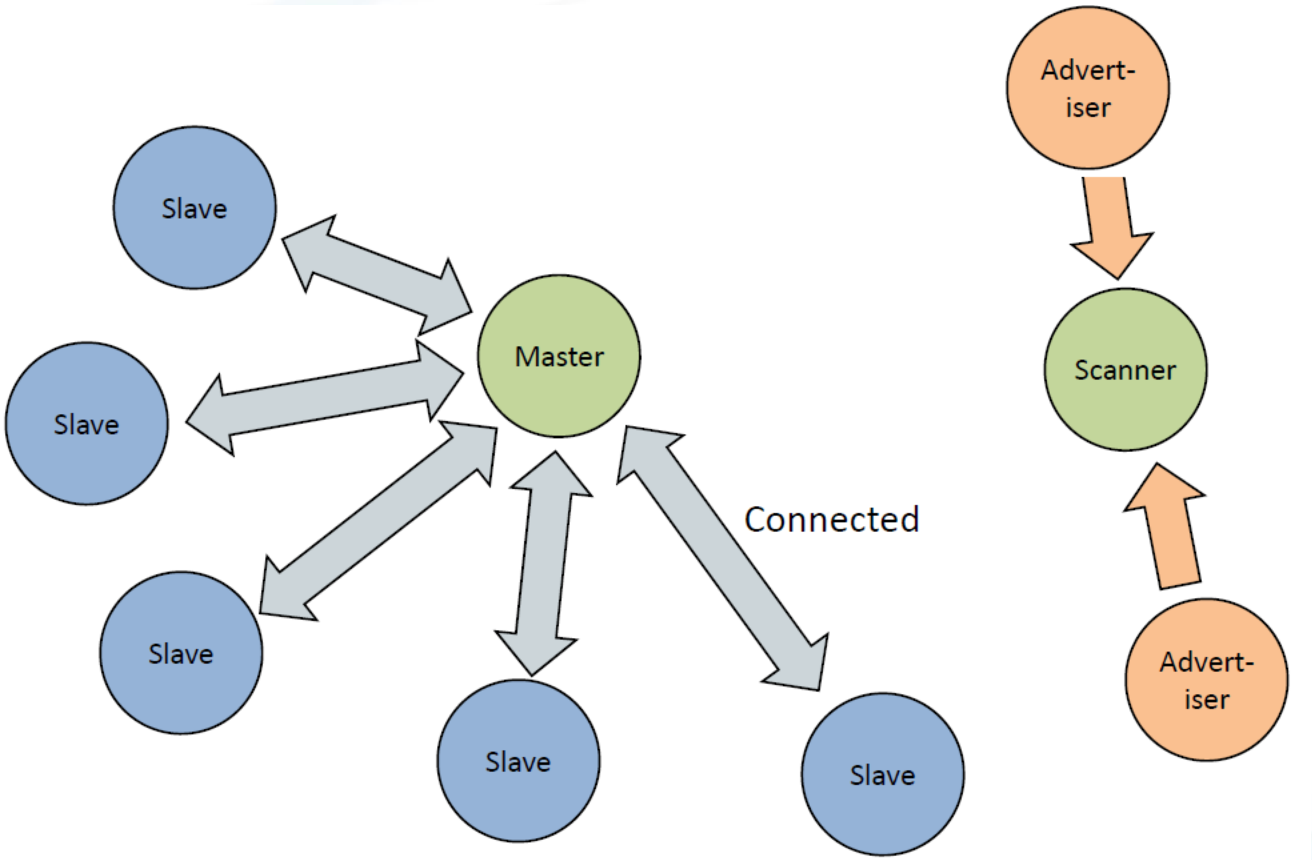
Link layer: Topologies



Link layer: Topologies



Link layer: Topologies



Topology limits

A single master can address ~2^{31} slaves

- ~ 2 billion addressable slaves per master

Max Connection Interval = 4.0 seconds

- Can address a slave every ~ 5 ms (assuming 250 ppm clocks)
- ~ 800 active slaves per master

Note:

Devices RAM may limit the number of connections

Link layer security

AES-128 is the encryption engine of choice

- Used by most other secure wireless standards

Link Layer uses CCM (Counter Mode CBC-MAC) (RFC 3610)

- Encryption and Authentication of Data
- MIC added to end of payload to authenticate data
- Authentication does not have to be done in real-time
  >Saves power

Limits:

- 13.5 Terabytes / connection
- ~12 years at maximum data rate

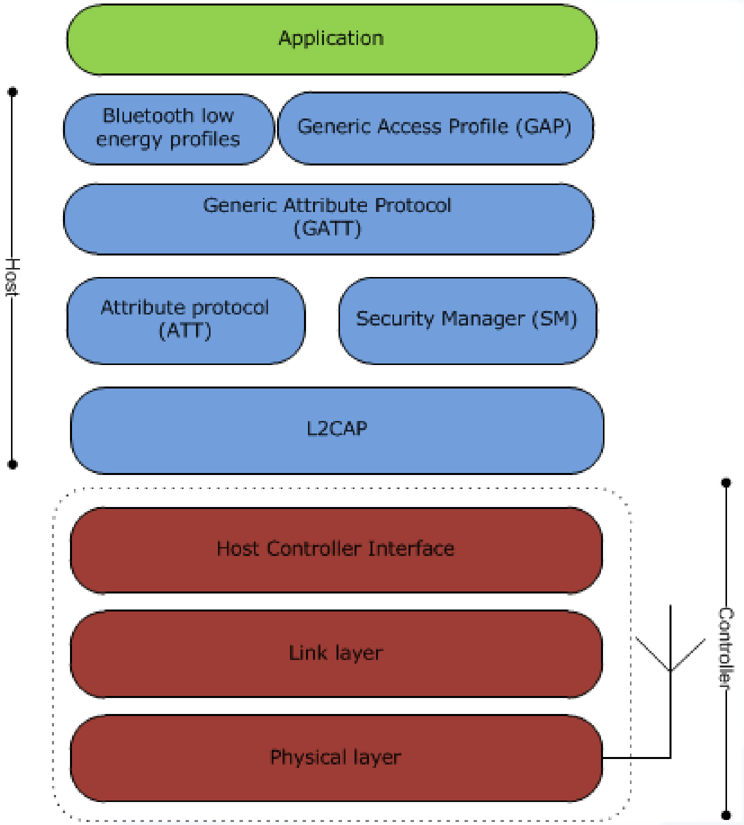
Host Controller Interface

Transport layer

- UART
- USB
- SDIO
- 3 wire UART

Functional layer

- HCI commands
- HCI events
- Data


Application
Bluetooth low energy profiles
Generic Access Profile (GAP)
Generic Attribute Protocol (GATT)
Attribute protocol (ATT)
Security Manager (SM)
L2CAP
Host
Host Controller Interface
Link layer
Physical layer
Controller

New commands added for *Bluetooth* LE

18/11/11

L2CAP

Logical Link Control and Adaptation Protocol

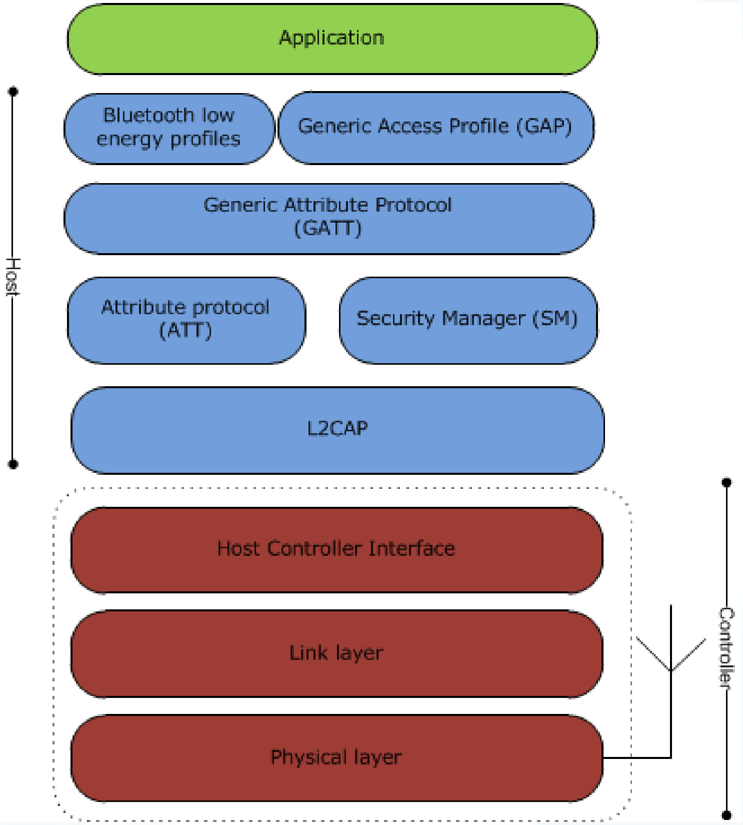
Acts as a protocol multiplexer

- Segmentation and reassmebly of packets

All application data is sent using L2CAP

Three fixed channels for Bluetooth LE

- Attribute protocol
- LE L2CAP signalling protocol
- Security Manager protocol


Application
Bluetooth low energy profiles
Generic Access Profile (GAP)
Generic Attribute Protocol (GATT)
Attribute protocol (ATT)
Security Manager (SM)
L2CAP
Host
Host Controller Interface
Link layer
Physical layer
Controller

18/11/11

Security Manager

Used for pairing and key distribution

Use distributing key model

- Slave generates and distributes key information to master
- Master can use this key information when reconnecting

Pairing

- Authentication based on their capabilities / security requirements
- Side effect is encrypted link / key distribution

Signing Data

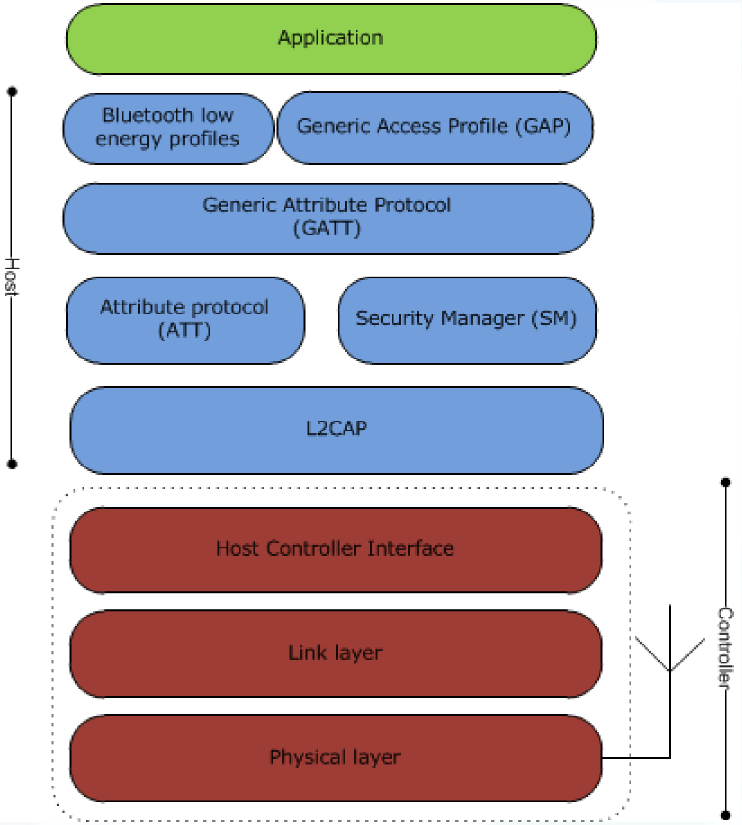
- Signing allows authentication of sender without encryption

Uses several keys

- Short term key
- Long term key
- Identity resolving key

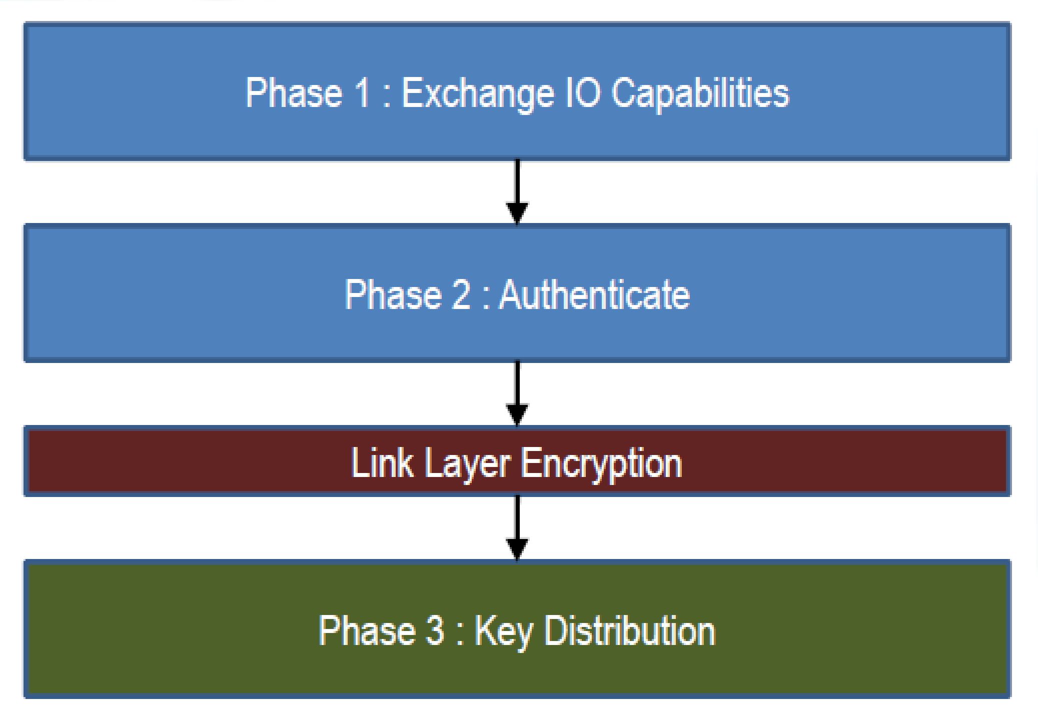
Bonding

- GAP concept – device save keys for bonded devices


Application
Bluetooth low energy profiles
Generic Access Profile (GAP)
Generic Attribute Protocol (GATT)
Attribute protocol (ATT)
Security Manager (SM)
L2CAP
Host Controller Interface
Link layer
Physical layer
Host
Controller

18/11/11

Security Manager



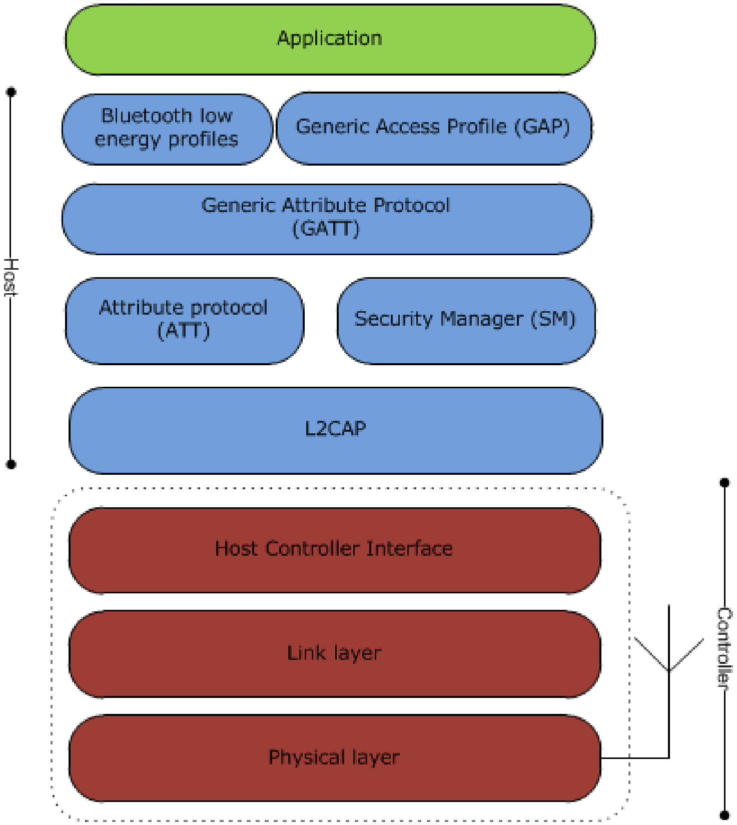
Phase 1 : Exchange IO Capabilities

Phase 2 : Authenticate

Link Layer Encryption

Phase 3 : Key Distribution

Attribute Protocol (ATT)


Application
Bluetooth low energy profiles
Generic Access Profile (GAP)
Generic Attribute Protocol (GATT)
Attribute protocol (ATT)
Security Manager (SM)
L2CAP
Host Controller Interface
Link layer
Physical layer
Host
Controller

18/11/11

Attribute Protocol (ATT)

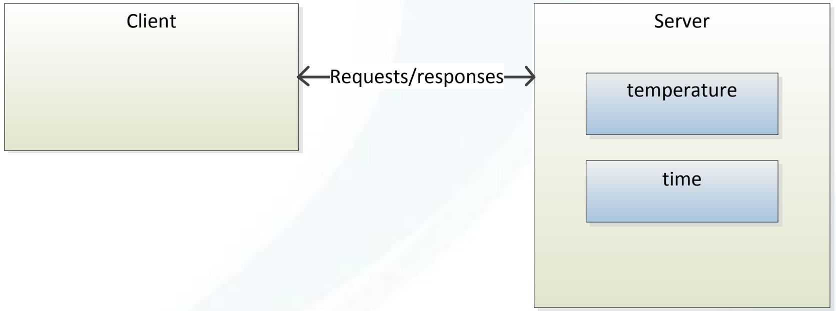
The only protocol used in *Bluetooth* low energy

Uses client server architecture

- servers store data
- clients request data from server
- clients writes data to server

Protocol Methods

- Client to server: Read, write
- Server to client: Notify, indicate



Attribute Protocol

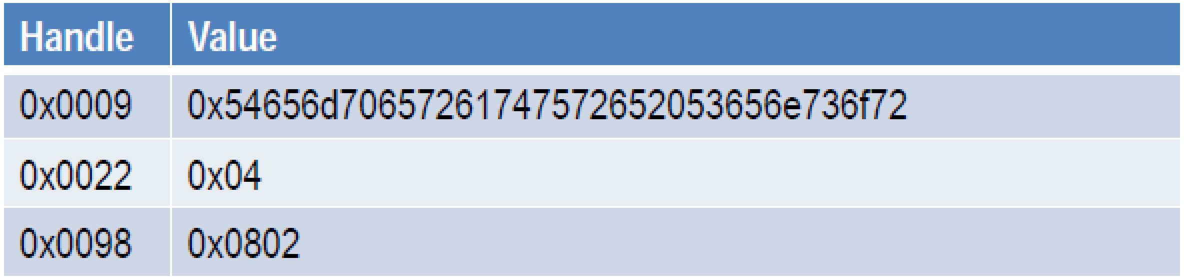
The data is exposed as attributes

- Attributes have values
- 0 to 512 octets
- Fixed or variable length

Attributes have handles

- Used to address individual attributes

Read 0x0022 -> 0x04



Handle	Value
0x0009	0x54656d70657261747572652053656e736f72
0x0022	0x04
0x0098	0x0802

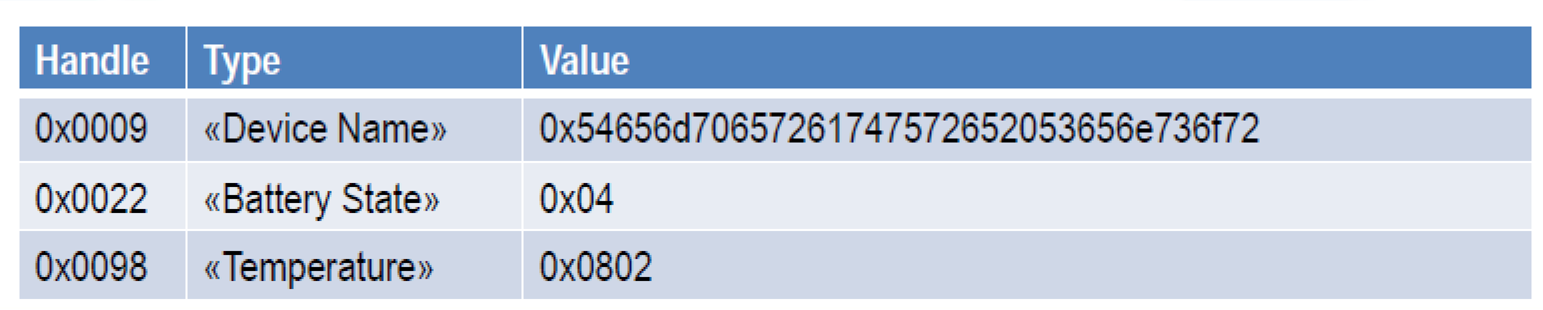
Attribute Protocol

Attributes have a type

- Identified by UUIDs
- UUIDs are 16-bit (Bluetooth SIG assigned) or 128-bit (manufacturer proprietary)

Types are defined is specifications

- Characteristics specifications
- Generic Access Profile
- Generic Attribute Profile



Handle	Type	Value
0x0009	«Device Name»	0x54656d70657261747572652053656e736f72
0x0022	«Battery State»	0x04
0x0098	«Temperature»	0x0802

0x54656d70657261747572652053656e736f72 = “Temperature Sensor”

Attribute Protocol

Attributes have permissions:

- Readable / not readable
- Writeable / not writeable
- Readable & writeable / not readable & not writeable

Attribute values may require:

- Authentication to read / write
- Authorization to read / write
- Encryption / pairing to read / write

These are defined in *Bluetooth* LE profile specifications

Attribute Protocol

Attribute Protocol is stateless

Transactions:

- Request -> Response
- Command
- Notification
- Indication -> Confirmation

Attribute Protocol is sequential

- Only one request at a time

Simple!

Attribute Protocol

- **Attribute operations: notify**

  Server sends the data when it changes

- **Attribute operations: indicate**

  Server sends the data when it changes

  Client confirms that is has received the data

Attribute Protocol

- **Attribute operations: read**

  Client requests data when it needs it

  Client polls server for attribute value

  – This may be inefficient if data doesn't change often

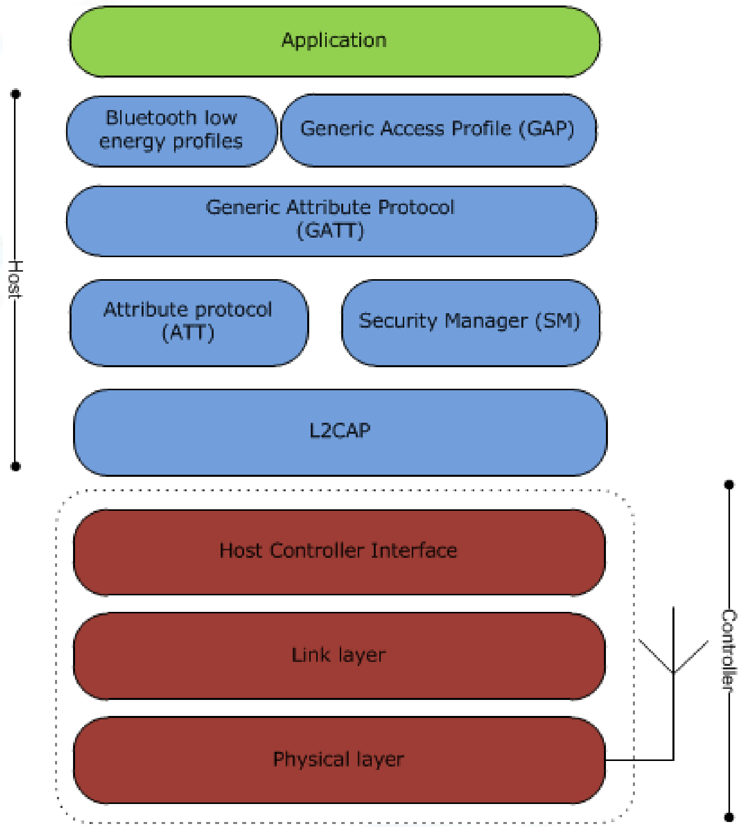
  – Shouldn't be used for frequently changing data that you are monitoring

- **Attribute operations: write**

  Client can set attributes to configure a server

  – E.g. set the room temperature to 22ºC

Generic Attribute Profile (GATT)


Application
Bluetooth low energy profiles
Generic Access Profile (GAP)
Generic Attribute Protocol (GATT)
Attribute protocol (ATT)
Security Manager (SM)
L2CAP
Host
Host Controller Interface
Link layer
Physical layer
Controller

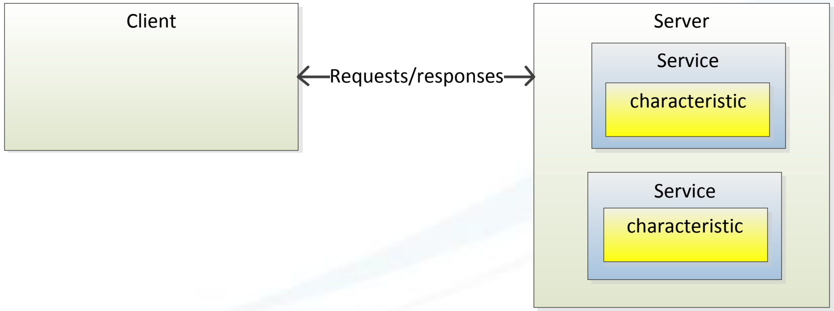
Generic Attribute Profile

GATT defines concepts of

- Service group
- Characteristic group
- Declarations
- Descriptors

Same client server architecture as in ATT, except:

- Data is encapsulated in services
- Data is exposed in characteristics



GATT : Generic Attribute Profile

- **Attribute Protocol is just a flat structure**
  - Profiles require hierarchical structures

- **GATT defines how to group attributes**
  - Groups of attributes in a “Service”
  - Groups of attributes within a “Service” – Sub-Services
  - Groups of attributes by client

Generic Attribute Profile (GATT)

A service is:

- A collection of characteristics
- References to other services

Primary Service

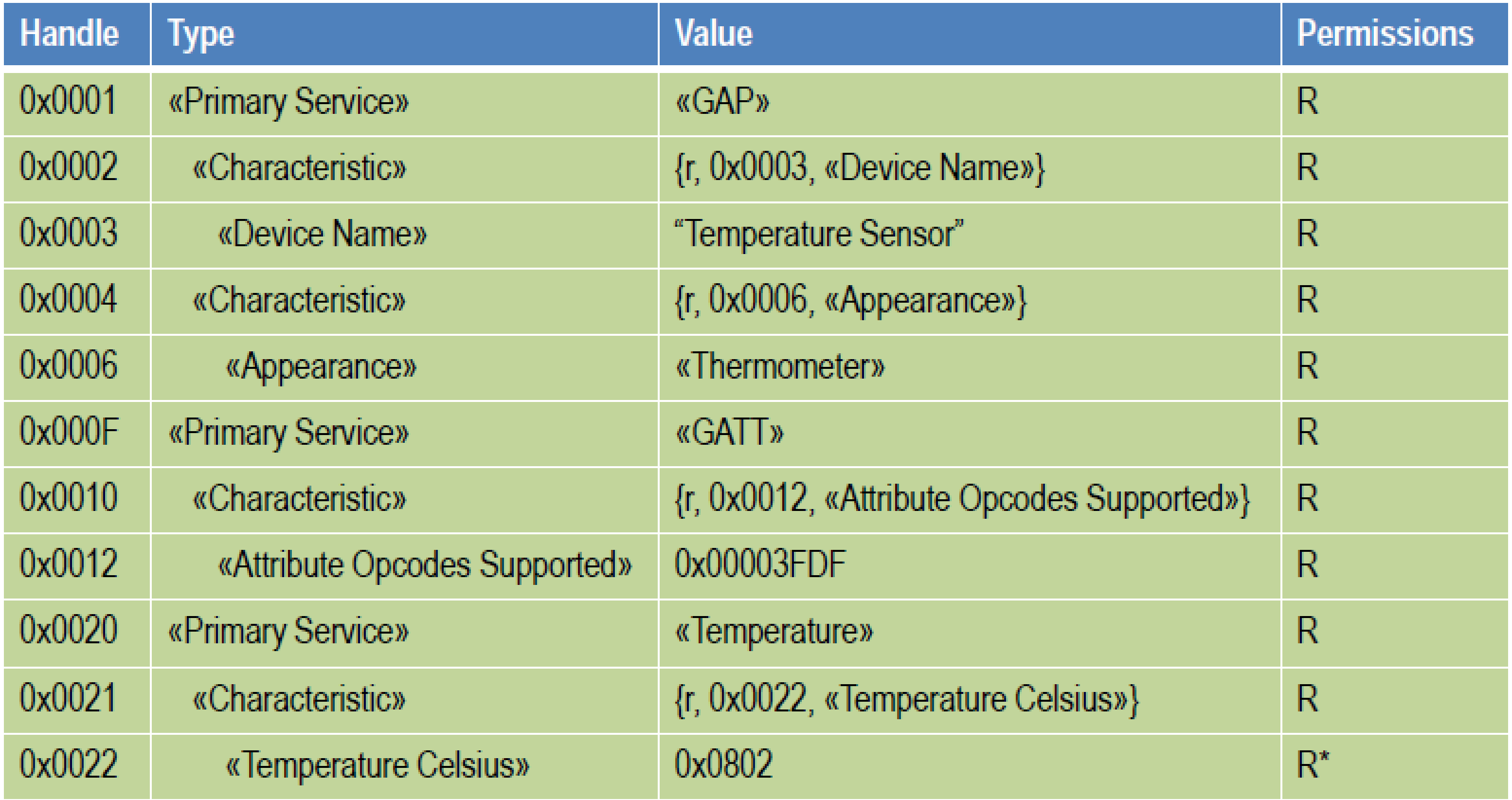
- A primary service is a service that exposes primary usable functionality of this device. A primary service can be included by another service

Secondary Service

- A secondary service is a service that is subservient to another secondary service or primary service. A secondary service is only relevant in the context of another service.

Generic Attribute Profile (GATT)

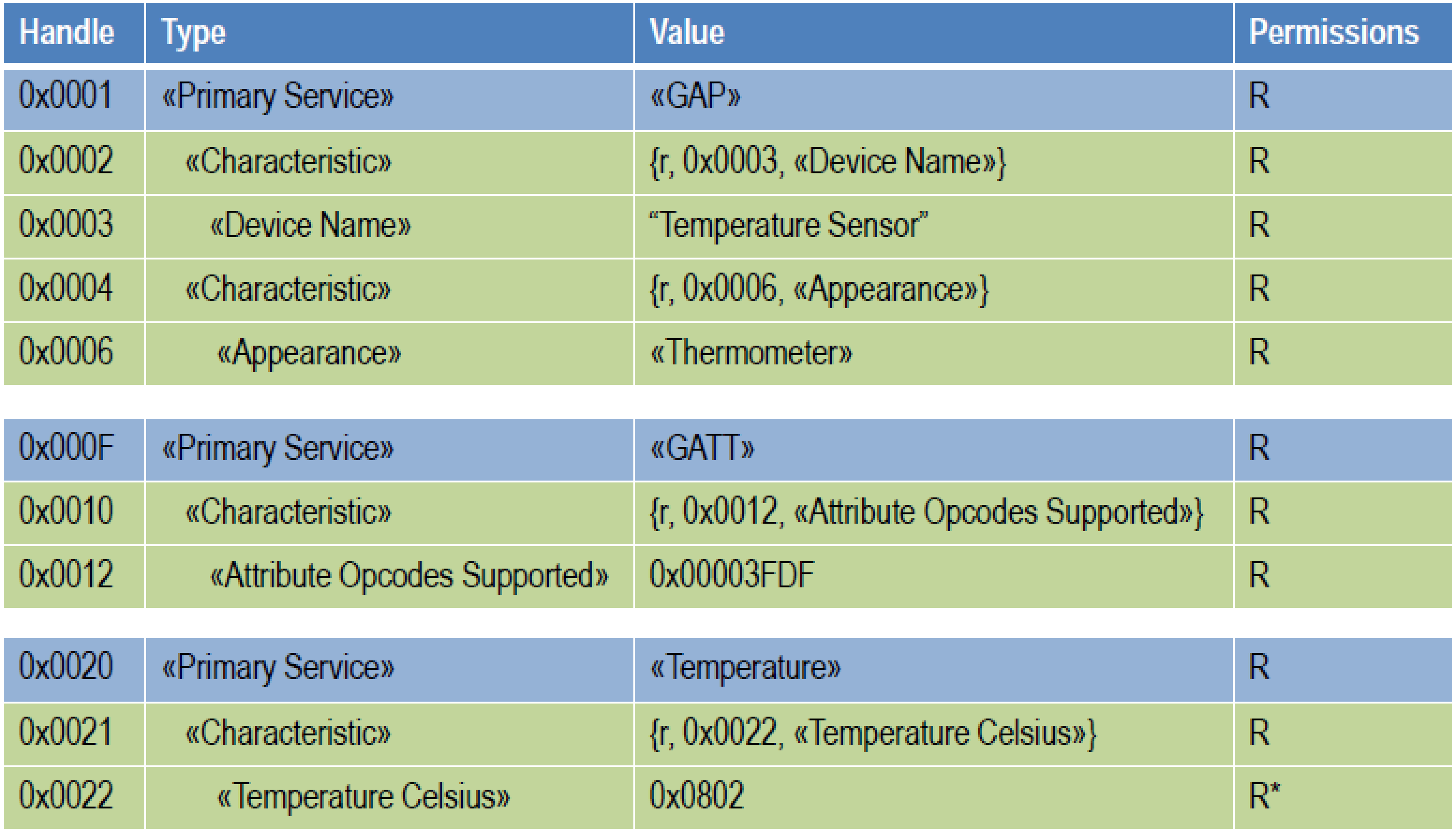
Attributes are flat



Handle	Type	Value	Permissions
0x0001	«Primary Service»	«GAP»	R
0x0002	«Characteristic»	{r, 0x0003, «Device Name»}	R
0x0003	«Device Name»	“Temperature Sensor”	R
0x0004	«Characteristic»	{r, 0x0006, «Appearance»}	R
0x0006	«Appearance»	«Thermometer»	R
0x000F	«Primary Service»	«GATT»	R
0x0010	«Characteristic»	{r, 0x0012, «Attribute Opcodes Supported»}	R
0x0012	«Attribute Opcodes Supported»	0x00003FDF	R
0x0020	«Primary Service»	«Temperature»	R
0x0021	«Characteristic»	{r, 0x0022, «Temperature Celsius»}	R
0x0022	«Temperature Celsius»	0x0802	R*

Generic Attribute Profile (GATT)

Grouping gives structure



Handle	Type	Value	Permissions
0x0001	«Primary Service»	«GAP»	R
0x0002	«Characteristic»	{r, 0x0003, «Device Name»}	R
0x0003	«Device Name»	“Temperature Sensor”	R
0x0004	«Characteristic»	{r, 0x0006, «Appearance»}	R
0x0006	«Appearance»	«Thermometer»	R
0x000F	«Primary Service»	«GATT»	R
0x0010	«Characteristic»	{r, 0x0012, «Attribute Opcodes Supported»}	R
0x0012	«Attribute Opcodes Supported»	0x00003FDF	R
0x0020	«Primary Service»	«Temperature»	R
0x0021	«Characteristic»	{r, 0x0022, «Temperature Celsius»}	R
0x0022	«Temperature Celsius»	0x0802	R*

GAP : Generic Access Profile

Defines Profile Roles

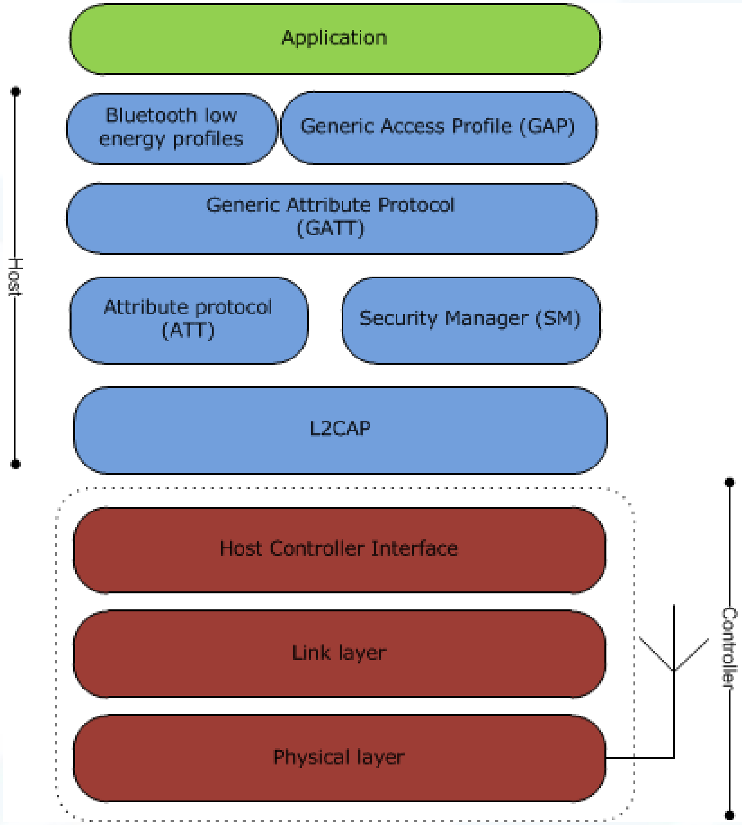
- Broadcaster, Observer, Peripheral, Central

Defines Modes

Discoverable	General discoverable, non-discoverable, limited discoverable
Connectable	Connectable, non-connectable
Bondable	Bondable, non-bondable

Privacy

- Non-Resolvable and Resolvable Private Addresses



Application
Bluetooth low energy profiles
Generic Access Profile (GAP)
Generic Attribute Protocol (GATT)
Attribute protocol (ATT)
Security Manager (SM)
L2CAP
Host
Host Controller Interface
Link layer
Physical layer
Controller

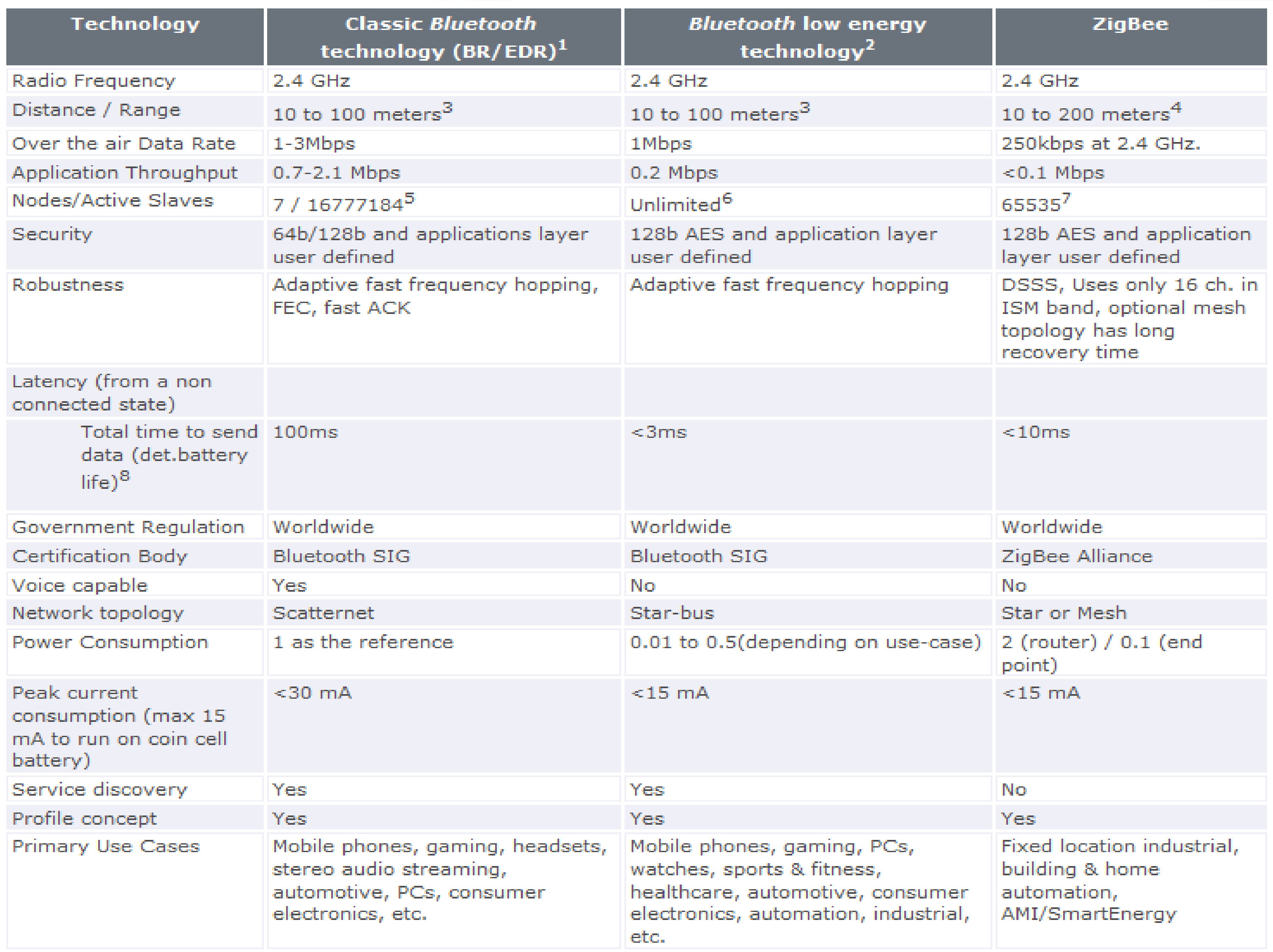
Differentation & Comparison

18/11/11

Differentiation

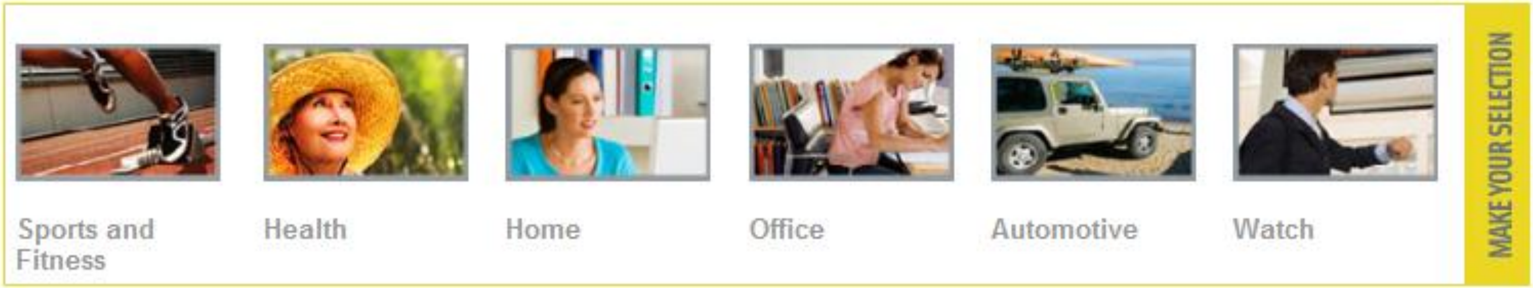
- Simple star topology reduces implementation complexity significantly
- Very small silicon footprint and thereby very low cost
- Very robust through frequency hopping compared to other wireless technologies
- Very secure through 128 bit AES encryption
- Very low power – always OFF technology
- No competitors (*Bluetooth* is already in phones)

Comparison



Technology	Classic *Bluetooth* technology (BR/EDR)[1]	*Bluetooth* low energy technology[2]	ZigBee
Radio Frequency	2.4 GHz	2.4 GHz	2.4 GHz
Distance / Range	10 to 100 meters[3]	10 to 100 meters[3]	10 to 200 meters[4]
Over the air Data Rate	1-3Mbps	1Mbps	250kbps at 2.4 GHz.
Application Throughput	0.7-2.1 Mbps	0.2 Mbps	<0.1 Mbps
Nodes/Active Slaves	7 / 16777184[5]	Unlimited[6]	65535[7]
Security	64b/128b and applications layer user defined	128b AES and application layer user defined	128b AES and application layer user defined
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive fast frequency hopping	DSSS, Uses only 16 ch. in ISM band, optional mesh topology has long recovery time
Latency (from a non connected state)			
Total time to send data (det.battery life)[8]	100ms	<3ms	<10ms
Government Regulation	Worldwide	Worldwide	Worldwide
Certification Body	Bluetooth SIG	Bluetooth SIG	ZigBee Alliance
Voice capable	Yes	No	No
Network topology	Scatternet	Star-bus	Star or Mesh
Power Consumption	1 as the reference	0.01 to 0.5(depending on use-case)	2 (router) / 0.1 (end point)
Peak current consumption (max 15 mA to run on coin cell battery)	<30 mA	<15 mA	<15 mA
Service discovery	Yes	Yes	No
Profile concept	Yes	Yes	Yes
Primary Use Cases	Mobile phones, gaming, headsets, stereo audio streaming, automotive, PCs, consumer electronics, etc.	Mobile phones, gaming, PCs, watches, sports & fitness, healthcare, automotive, consumer electronics, automation, industrial, etc.	Fixed location industrial, building & home automation, AMI/SmartEnergy

Markets


Sports and Fitness
Health
Home
Office
Automotive
Watch
MAKE YOUR SELECTION

Sports & fitness

- Heart rate
- Cadence
- Watches
- Pedometers

Assisted living

- **Sensors**
  - Temperature
  - Humidity
  - Alarms

- **Collectors**
  - Collect information from sensors
  - Display information to user

Consumer medical

- Weight scales

- Blood pressure meters

- Blood glucose meters

Entertainment

- Remote controllers
- Gaming controllers

Automation

- **Industrial automation**
  - Robots
  - Motors
  - Processes

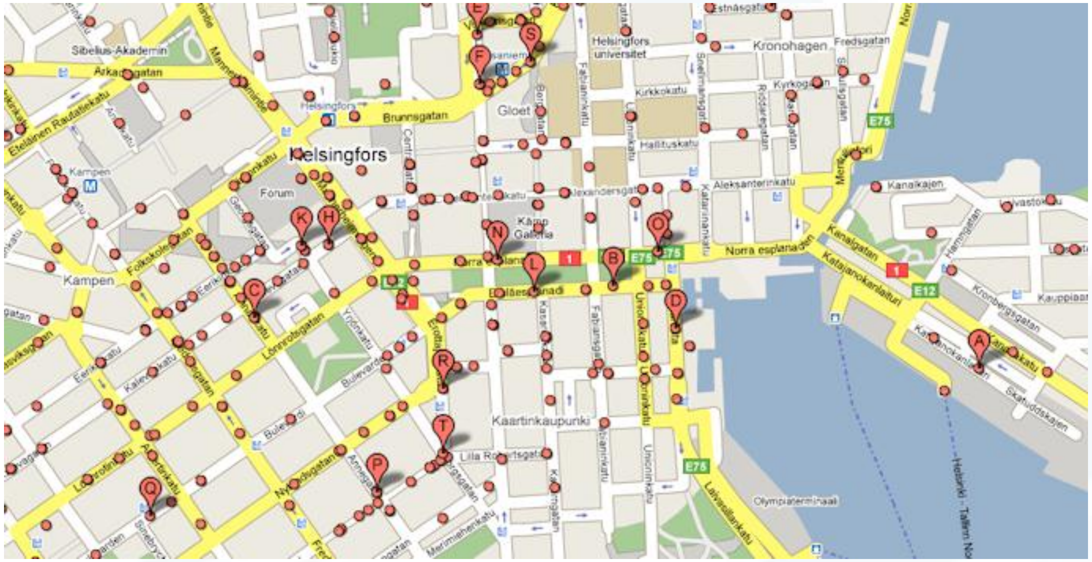
- **Home automation**
  - Temperature
  - Humidity
  - Lights

Security

- Key fobs
- Proximity monitors
- Electrical keys
- Mobile phone keys

Broadcast advertising

- Information points
- Indoor GPS
- Advertisements
- Maps of facilities
- Fire exits



18/11/11

Summary

18/11/11

Summary

***Bluetooth* low energy is a new technology**

- Blank sheet of paper
- Optimized for low power

***Bluetooth* low energy is designed to be low power**

- 10-20 times less power consumption compared to *Bluetooth* classic
- Low silicon area and memory requirements
- Enables coin cell battery use cases

***Bluetooth* low energy is designed for new applications**

- Health
- Fitness
- Automation
- Security
- Watch

Summary

***Bluetooth* low energy is designed to be secure and robust**

- AES-128 with CBC/MAC
- Simple pairing
- Privacy support
- Adaptive Frequency Hopping
- Reliable connections

It’s still *Bluetooth!*

- Reuse of RF, HCI and L2CAP
- Royalty free
- Developed and driven by Bluetooth SIG (~14000 members)
- Bluetooth already in mobile phones and PCs
- Qualification and interoperability
- ~3 billion sold devices already

bluegiga

Questions?

www.bluegiga.com