Bluetooth [in]security

Security Center of Excellence

#whoami

Jiggyasu Sharma

- A secuirty N00b
- I hack for bread and b33r
- I write [crape]
- I shoot [by camera]

Agenda

- To discus whatever we all know

Bluetooth

- **Bluetooth** is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). (wiki)

History

- Named on 10th century king Herald Bluetooth
- Proposed by Jim Kardach
- In 1997
- A system which communicate b/w phone and comp
- BSIG

Capability

- Wireless
- Short Range
- Less energy
- Cheap
- Personal
- Easy
- Multipoint
- Frequency hopping
- [in]secure

Where is being used

- Phone/Computer/Camera/Speaker
- Watch/Fitness Band/Car/door locks
- Cooker/coffee machine/trimer/dryer
- Medical devices : ventilator/blood glucose monitor
- Payment solution
- 7 Million Devices

Types

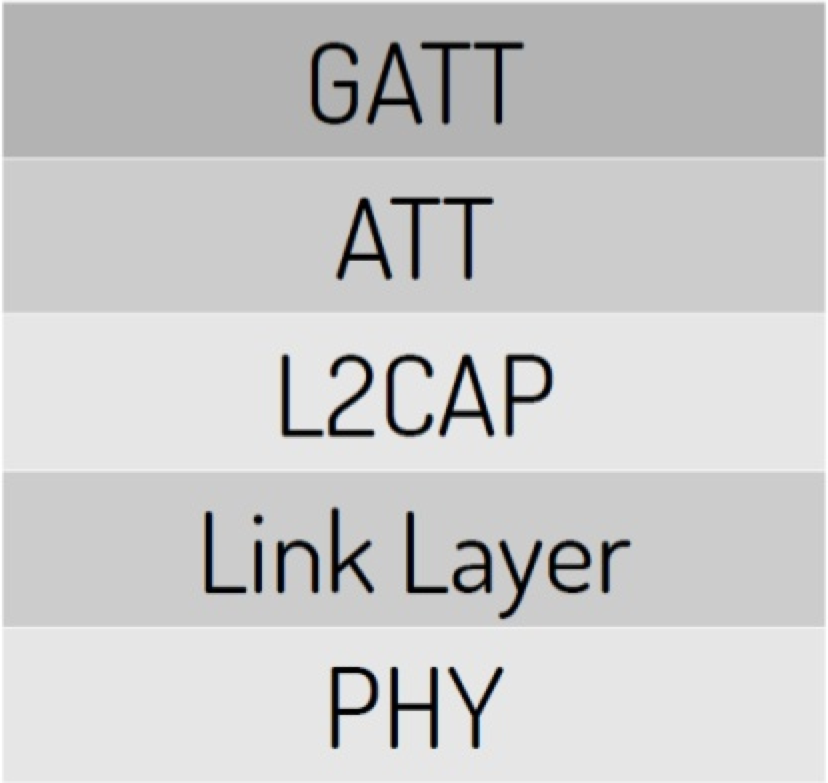
- Classic (since 1997)
    - V-1
    - V-2
    - V-3
- Smart (since 2010)
    - V-4.0
    - V-4.1
    - V-4.2

Difference

- Both can not communicate to each other
- PHY and DLL are completely difference
- High level protocol reuse [L2CAP…]

Bluetooth Low Energy

Protocol Stack



GATT

ATT

L2CAP

Link Layer

PHY

PHY Layer

- FSK, +/- 250 kHz, 1 Mbit/sec
- 40 channels in 2.4 GHz
- Hopping

PHY Channels

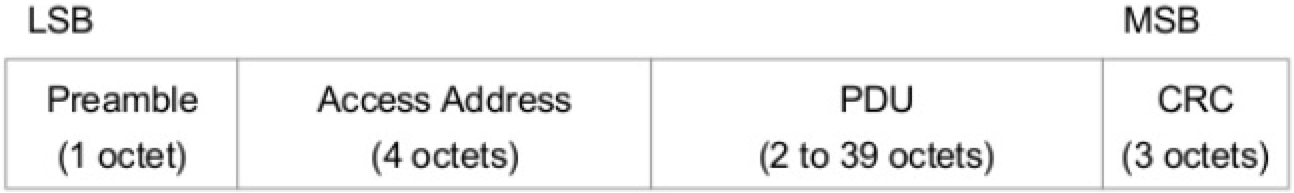
- 40 channels
- 0-39
- Advertising – 3
- Data -37

Hoping

- Hope along 37 data channels
- One data packet per channel
- Next channel = (channel + hop increment) mod 37

- 3 → 10 → 17 → 24 → 31 → 1 → 8 → 15 → …
    - hop increment = 7

Link Layer



LSB			MSB
Preamble (1 octet)	Access Address (4 octets)	PDU (2 to 39 octets)	CRC (3 octets)

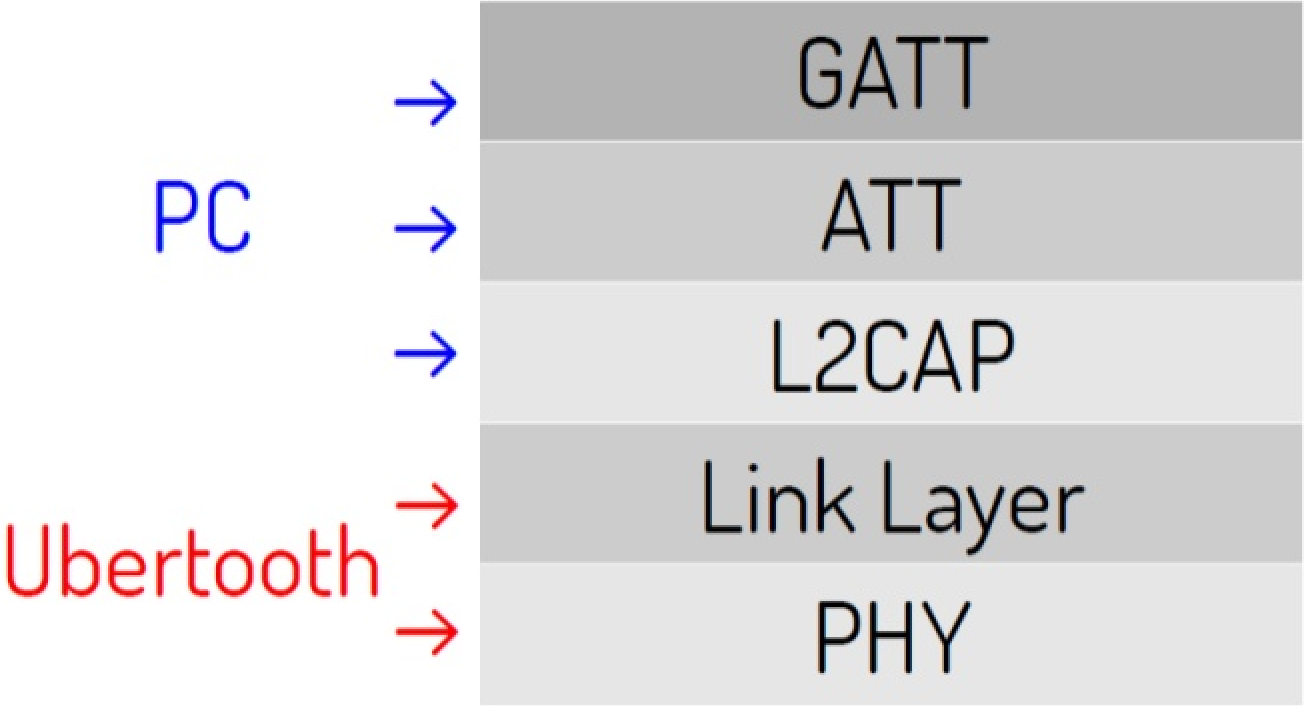
Figure 2.1: Link Layer packet format

How to sniff

- Its Hard (actually)

Ubertooth

- Open source h/w
- Bluetooth sniffer
- Ubertooth One
- Cheapest in existing solutions



PC

Ubertooth

GATT

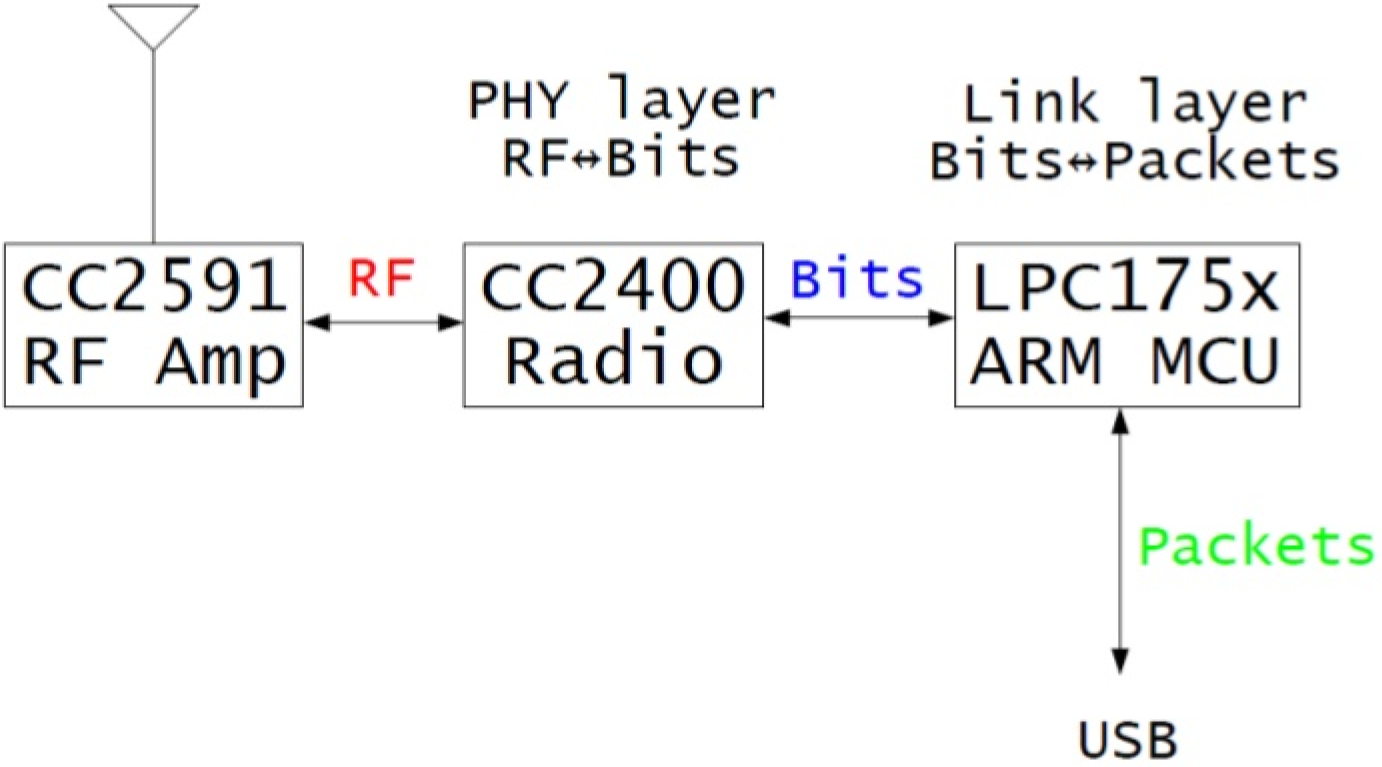
ATT

L2CAP

Link Layer

PHY

Block diagram



Capturing Packates

- Configure CC2400
- Follow connections according to hop pattern
- Hand off bits to ARM MCU