Bluetooth Low Energy : BLE

Prof SRN Reddy, IGDTUW

BLE: Bluetooth Low Energy

GAP: Generic Access Profile

GATT: Generic Attribute Profile

ATT: Attribute Protocol (ATT)

Bluetooth Low Energy (BLE) Introduction

- Wireless technology standard designed Personal Area Network
- Simple and easy to use model.
- Small bursts of data for low power consuption.
- Impressive battery life , operating for “months or years” on a button cell .
- Small size and Low cost.
- Works on free 2.4 Ghz band.
- Ideal for sensors/ IoT.
- Target for Applications: Home automation, healthcare, fitness, and home entertainment
- BLE is not same as BT classic
- BT 5 Bluetooth mesh used for Industrial applications

Components of BLE

- There are two devices
  - Central Devices: Rich recourses in terms of CPU power, memory and power
  - Peripheral Devices: Constraint Recourses of CPU power, memory and power

It uses Asymmetric Technology: Central devices will handle CPU computational load more then the Peripheral Device to provide more battery life for the Peripheral Devices

Advantages of BLE

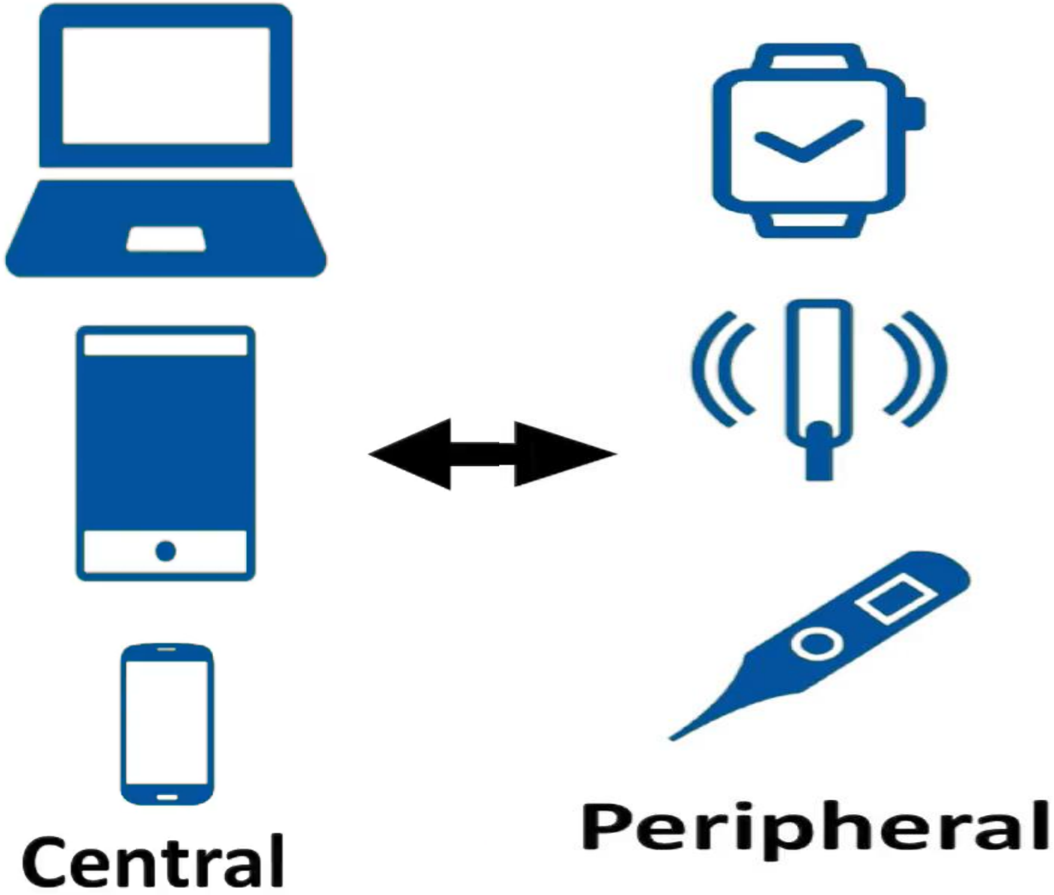
- Lowest Power Consumption
- Free Technical Specifications
- Low-cost Chipset
- BLE is available in almost all Smartphones to use diff. Applications

How to achieve Low Power

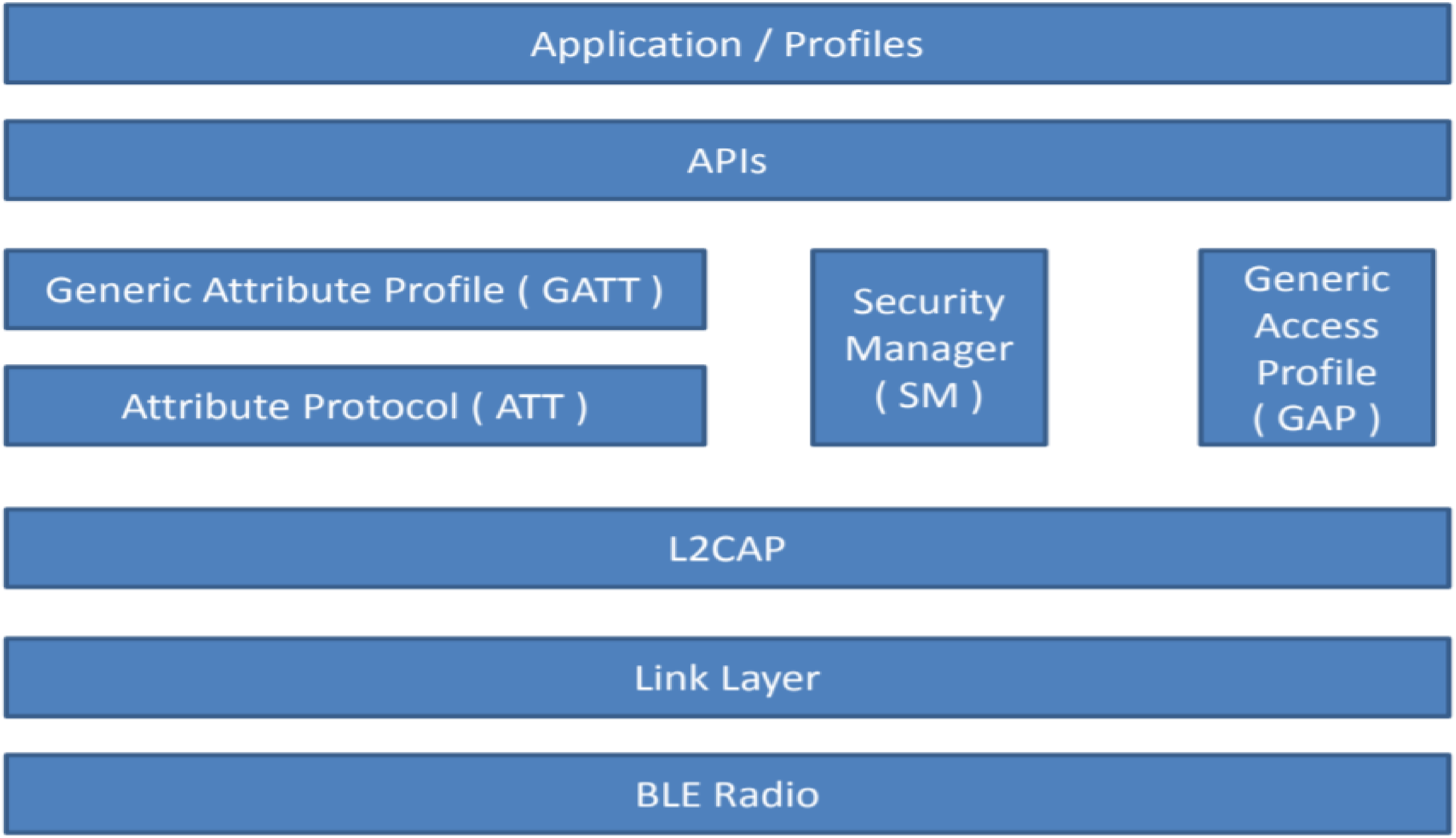
- Radio off for longer
- Low burst data transfers
- Operate at Low speeds

- Note: BLE is not suitable for applications for large amount of data transfers and long distances
- BLE is suitable for small amount of data eg. Sensor data in IoT

BLE Devices



Architecture



Application / Profiles

APIs

Generic Attribute Profile (GATT)

Attribute Protocol (ATT)

Security Manager (SM)

Generic Access Profile (GAP)

L2CAP

Link Layer

BLE Radio

BLE Radio Layer

- Operates in 2.4 GHz ISM (Industrial Scientific Medical) band
- 40 RF Channels with 2 MHz Spacing
- 3 out of 40 channels are advertising:
  - Used for device discovery
  - connection establishment
  - broadcast
- Advertising channel frequencies are selected to minimize the interference
- All physical channels use GFSK – Gaussian Frequency Shift Keying modulation to reduced peak power consumption
- Range is typically 0 – 50 meters from smart phone

BLE Link Layer

- First level of control & data structure over raw radio operations
- Bit stream transmission & Reception
- State machine & state transitions
- Data & Advertisement Packet formatting
- Link Layer operations
- Connections, packet timings, retransmission
- Link Layer level security

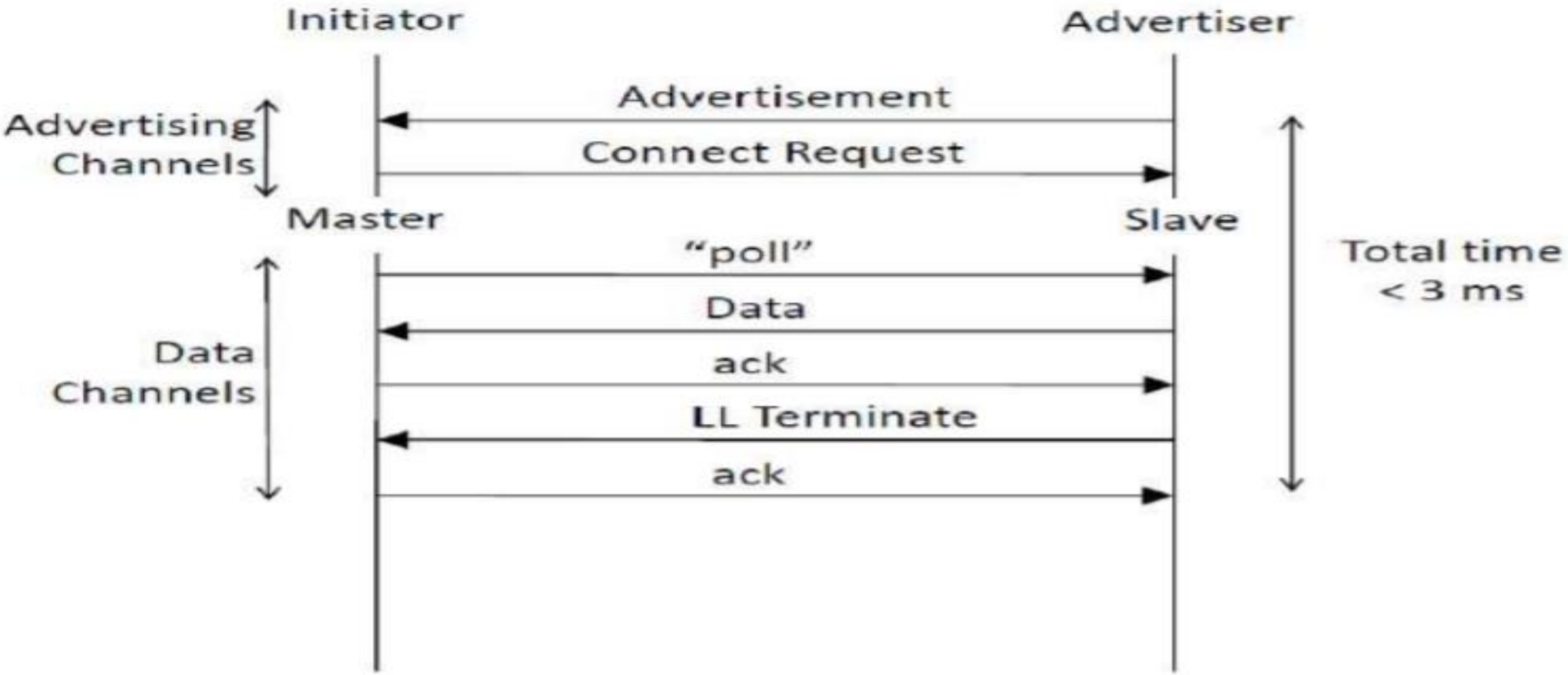
Logical link control and adaptation protocol (L2CAP)

- Advertisement
- Scanning
- Connection Establishment

Advertisement

- Provides a way for devices to broadcast their presence
  - Allows connection to be established
- Broadcast data like the list of supported services, device name and TX Power Level
- Device will send advertising broadcast packets to one or multiple advertisement channels, which remote devices will pick up

BLE L2CAP – Connection



Connection, transmission of packet, and connection termination

Network Topology

Advertiser – Broadcasts advertisement packets

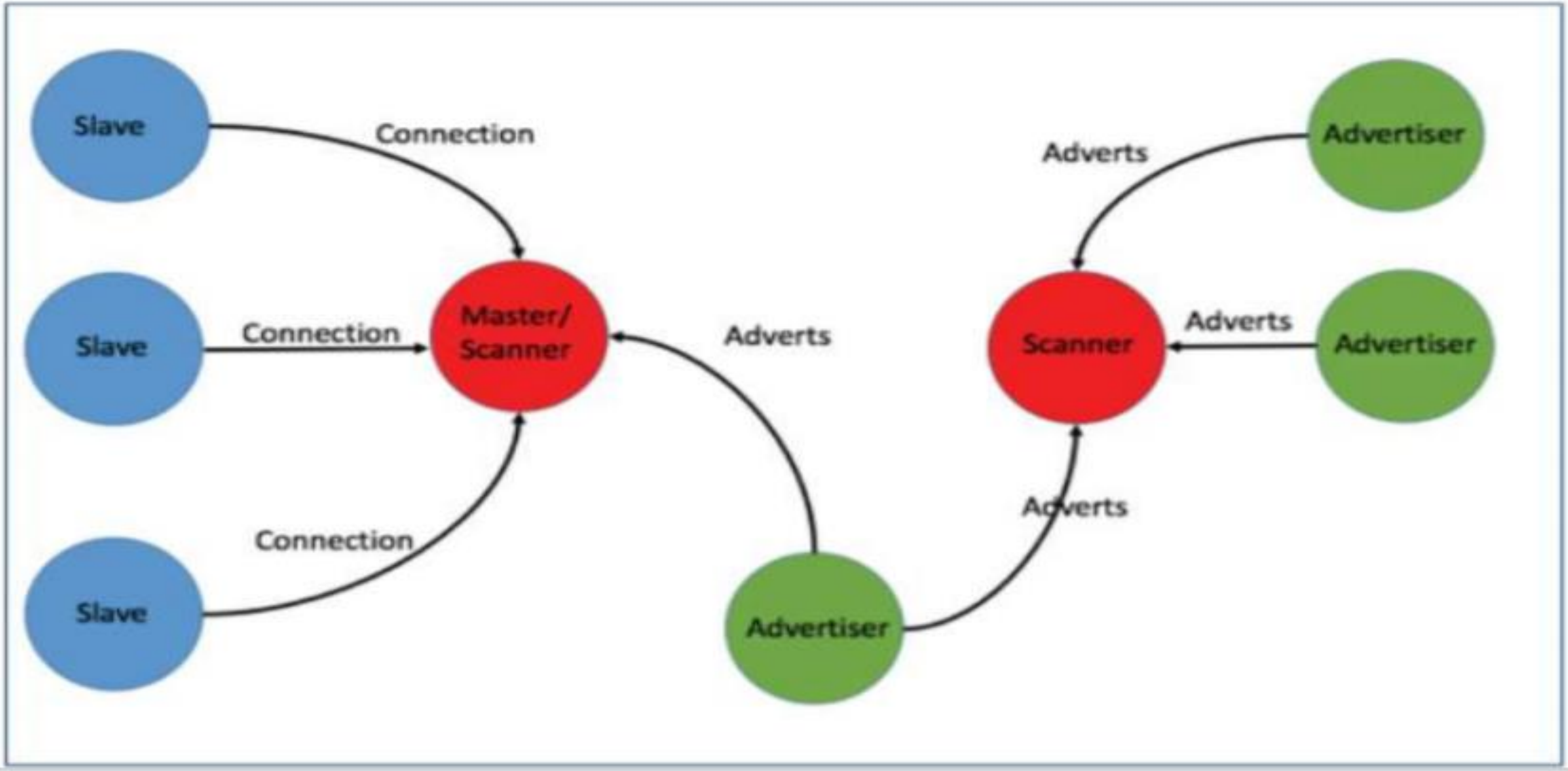
Scanner – Only listen for advertisements, can connect to advertiser

Slave – Device connected to master

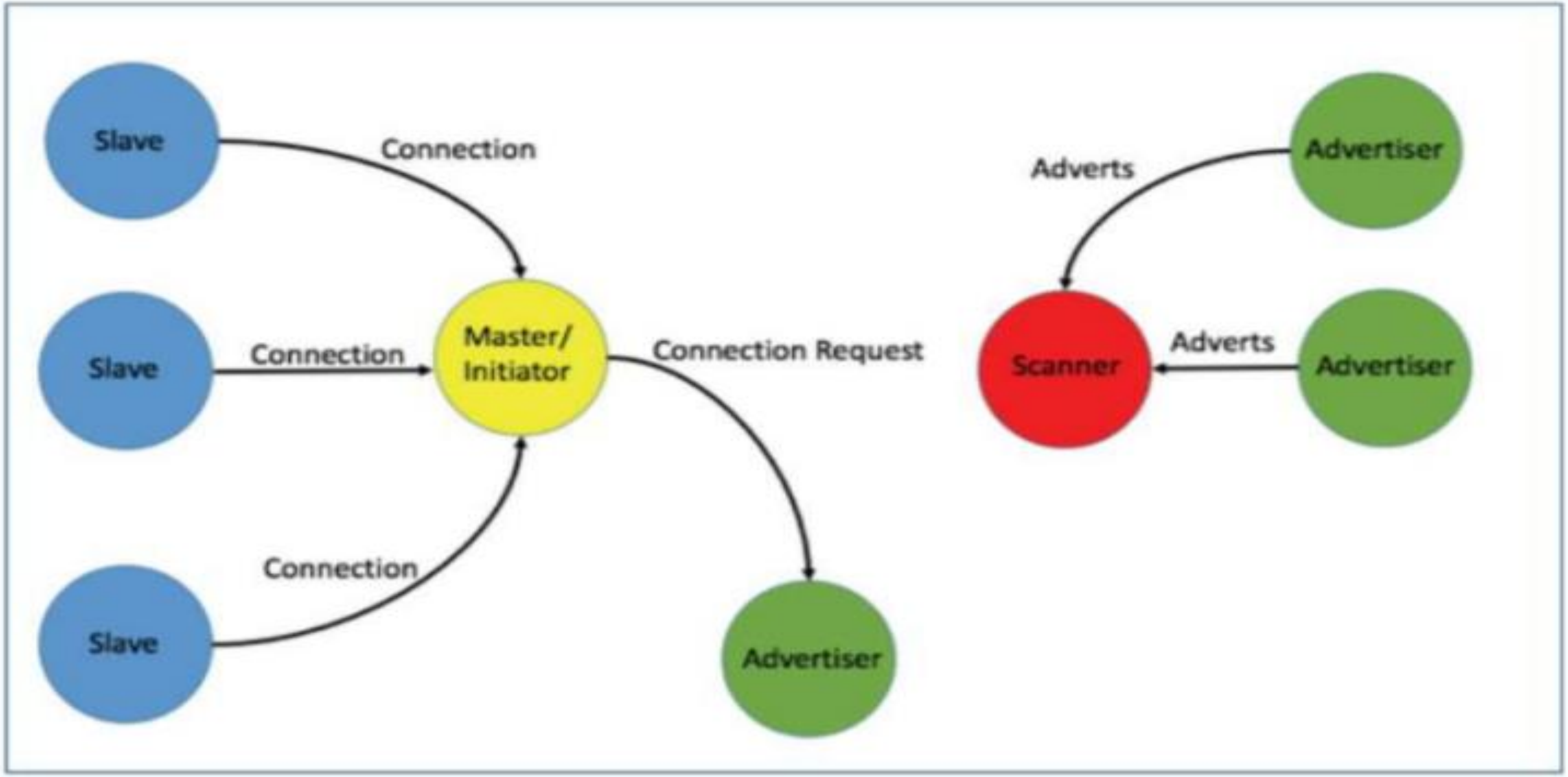
Master – Device connected with one or more slaves – Master can connect upto 4 – 8 slaves at a time

Hybrid – Device advertise and scan at the same time – Connected to a master and advertise or scan simultaneously

Connection


Slave
Connection
Slave
Connection
Slave
Connection
Master/
Scanner
Adverts
Advertiser
Adverts
Scanner
Adverts
Advertiser
Adverts
Advertiser
Adverts
Advertiser

Topology Change



BLE Generic Attribute Profile

- Provides access to the link layer operations related to
  - Device discovery
  - Connection establishment & termination
  - Connection timing control
- GAP defines roles
  - Broadcaster : Sends advertising & broadcast data
  - Observer : Listens for advertising events
  - Peripheral : Always slave, is connectable & advertising
  - Central : Always master, never advertise
  - Device can have more than one role, only one role can be adopted at a given time

BLE Modes

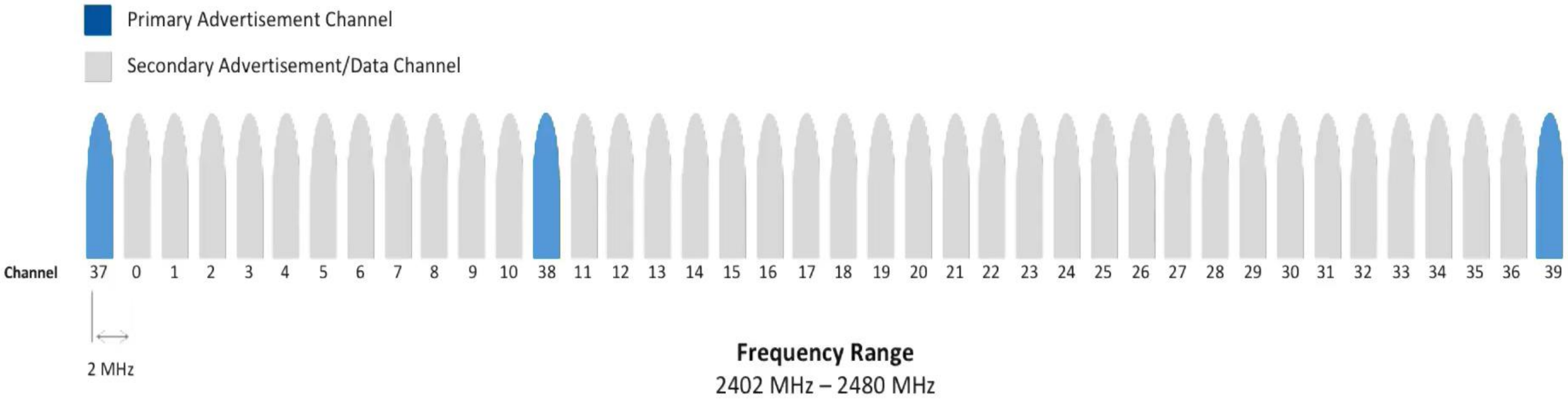
- There are Two Modes : 1. Advertising Mode 2. Connection Mode

1. Advertising Mode: Communication Broadcasts and Unidirectional data Transfer
2. Connection Mode: Used to connect the devices and Bidirectional Data transfer

Note: The Broadcaster first uses advertise mode to advertise and then uses connection mode to connect

There are two types of applications: Broadcast oriented and connection oriented

BLE Channels: 40 [3 Primary and 37 Sec]



ellisys
Better Analysis

GAP Roles

Broadcaster
Observer

Peripheral
Central

GAP Roles

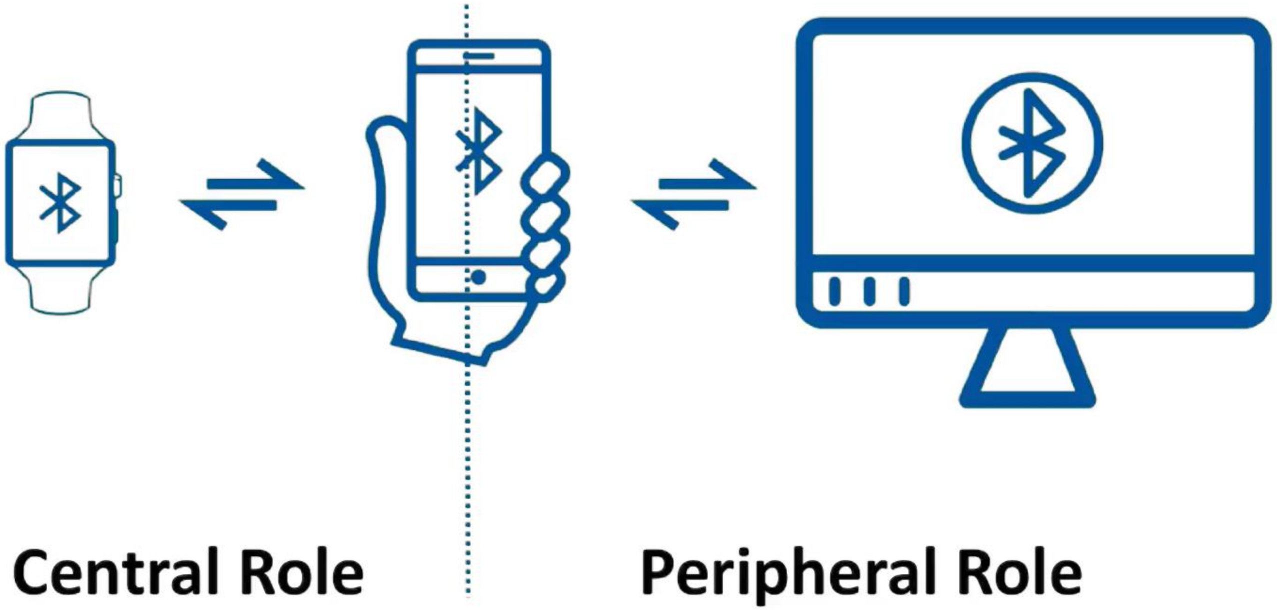
Broadcaster

Observer

Peripheral

Central

Simultaneous GAP Roles



Broad Caster and observers can only broad or observe and do not establish the connections.
Peripheral and central devices scan and establish the connections

GAP Modes

- Broadcast
- Discoverability
- Connectability
- Bonding
- Periodic advertising

GAP Modes

- Connectable
  - Can make a connection.
  - Not connectable, connectable
- Discoverable
  - Can be discovered (is advertising)
  - None, limited, general
- Bondable
  - If connectable, will pair with connected device for a long term connection
  - Bondable, Non Bondable

GAP Procedures

- Name Discovery – Find the name of other device
- Device Discovery – Find address & name of devices; Define device role
- Link Establishment– Instruct link layer to send a CONNECT_REQ

  – Service discovery, device authentication
- Service Discovery – Find services available on the peer devices

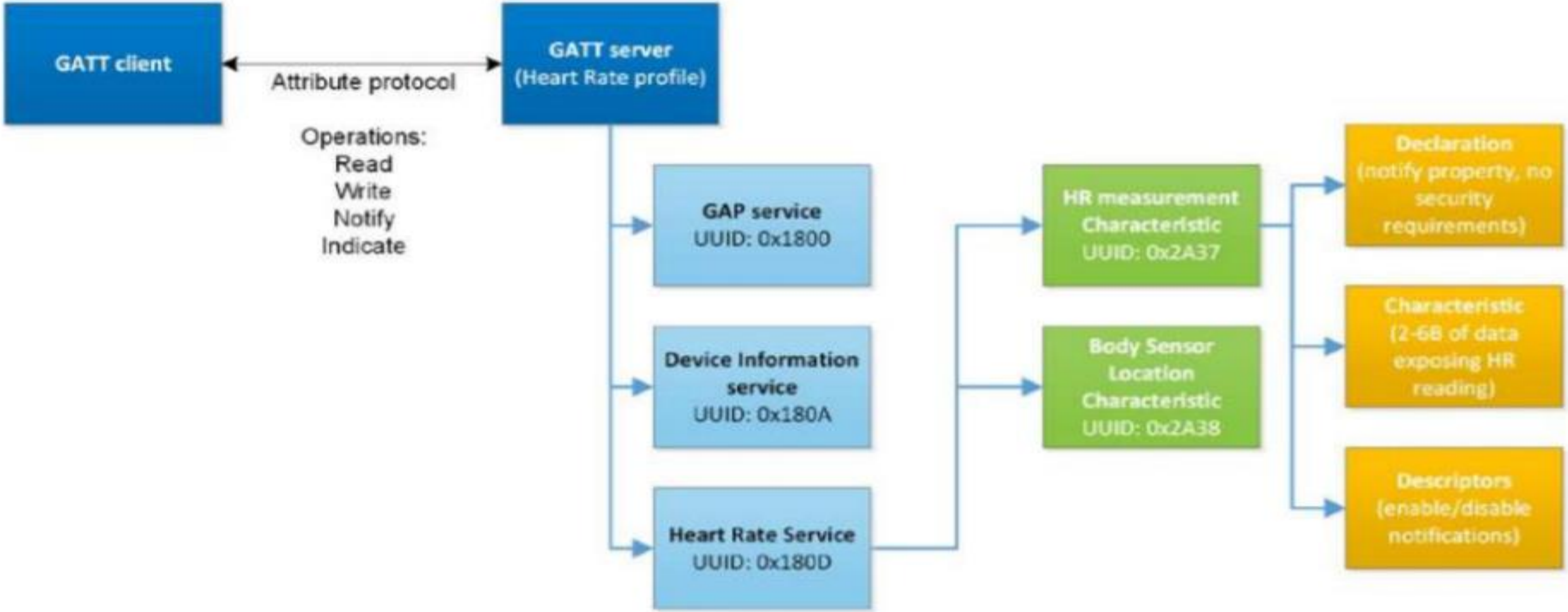
Attribute Protocol

- Defines communication between two devices playing the roles of server & client
- ATT Protocol defines two roles
  - Server : device that stores the data as one or more attributes
  - Client : Collects the information for one or more servers

BLE GATT

- Built on top of Attribute Protocol
- Establishes common framework for data transported & stored
- GATT defines two roles
    - Server
    - Client
- Attributes – Transported by Attribute protocol
    - Formatted as services & characteristics
- Service – Contain collection of characteristics
- Characteristics – Contain single value and any number of descriptors

BLE GATT Data Structure



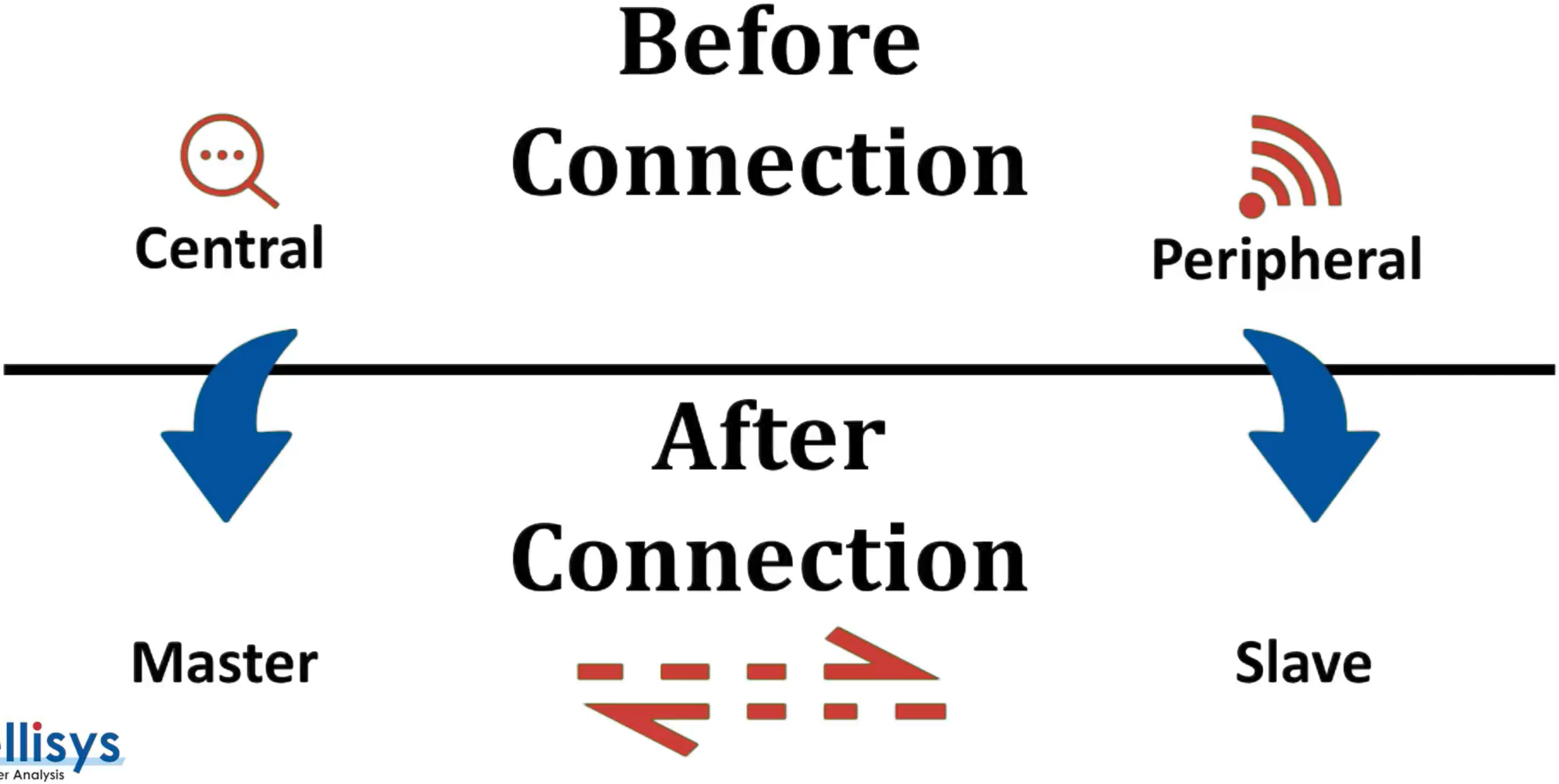
GATT data structure and operation

Connections

Persistent

Synchronized

Data Exchange



Before Connection

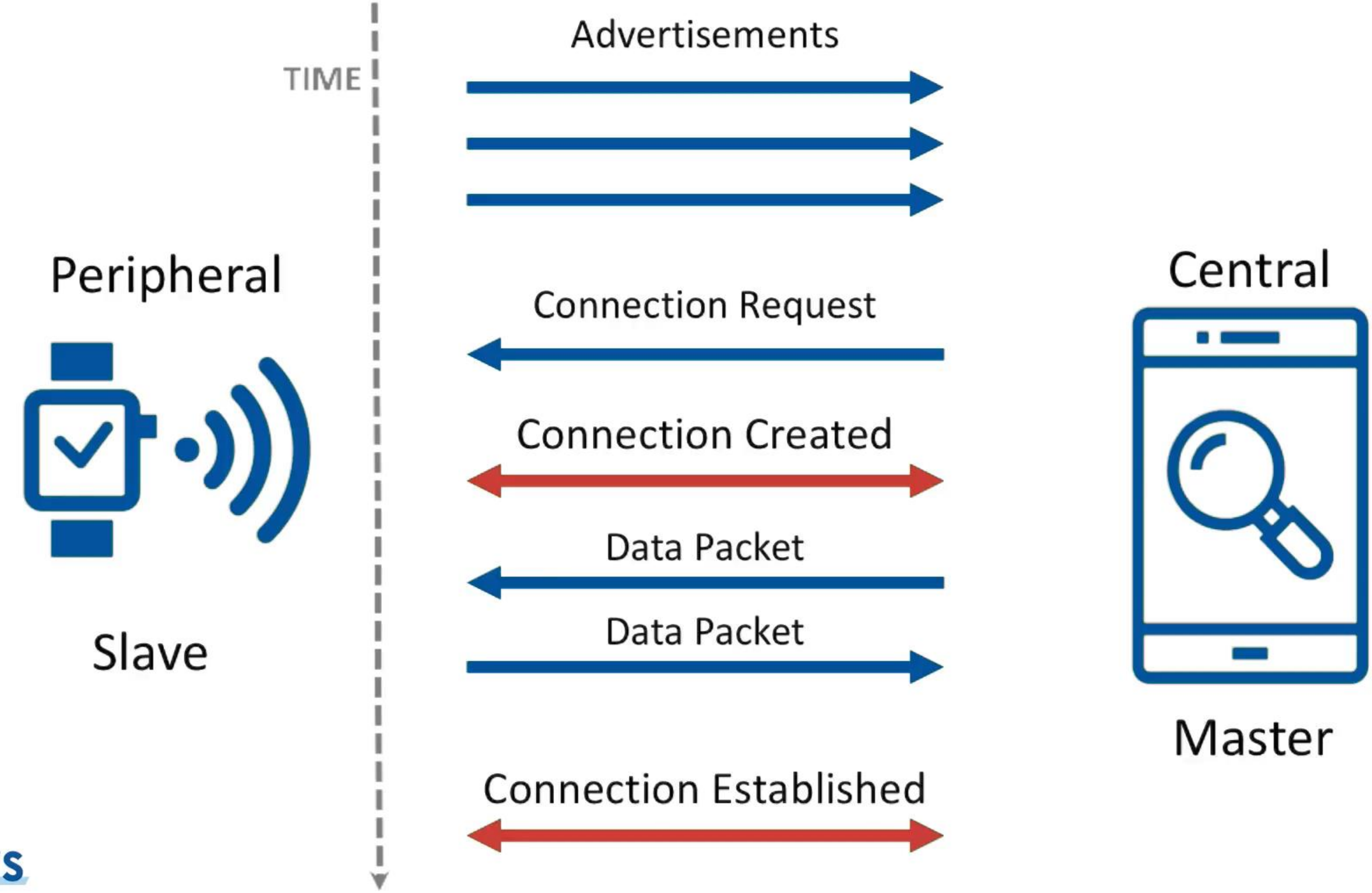
Central

Peripheral

After Connection

Master

Slave



ellisys
Better Analysis

Security

- Encryption (128 bit AES)
- Pairing (Without key, with a shared key, out of band pairing)
- Passive eavesdropping during key exchange
- Many products are building their own security on top of BLE
- Check out Mike Ryan (iSec partners) work on security

References

- https://www.jfokus.se/jfokus15/preso/Intro%20to%20BLE.pdf
- file:///C:/Users/S%20R%20N%20REDDY/Downloads/bluetoothlowenergy-170617090747.pdf
- https://datatracker.ietf.org/meeting/interim-2016-t2trg-02/materials/slides-interim-2016-t2trg-2-7
- https://www.bluetooth.com/bluetooth-resources/?types=paper [Applications]
- https://www.youtube.com/watch?v=eZGixQzBo7Y [Good Video by Ellisys]