

TECHNIVCAL OVERVIEW

Robin Heydon, CSR plc.



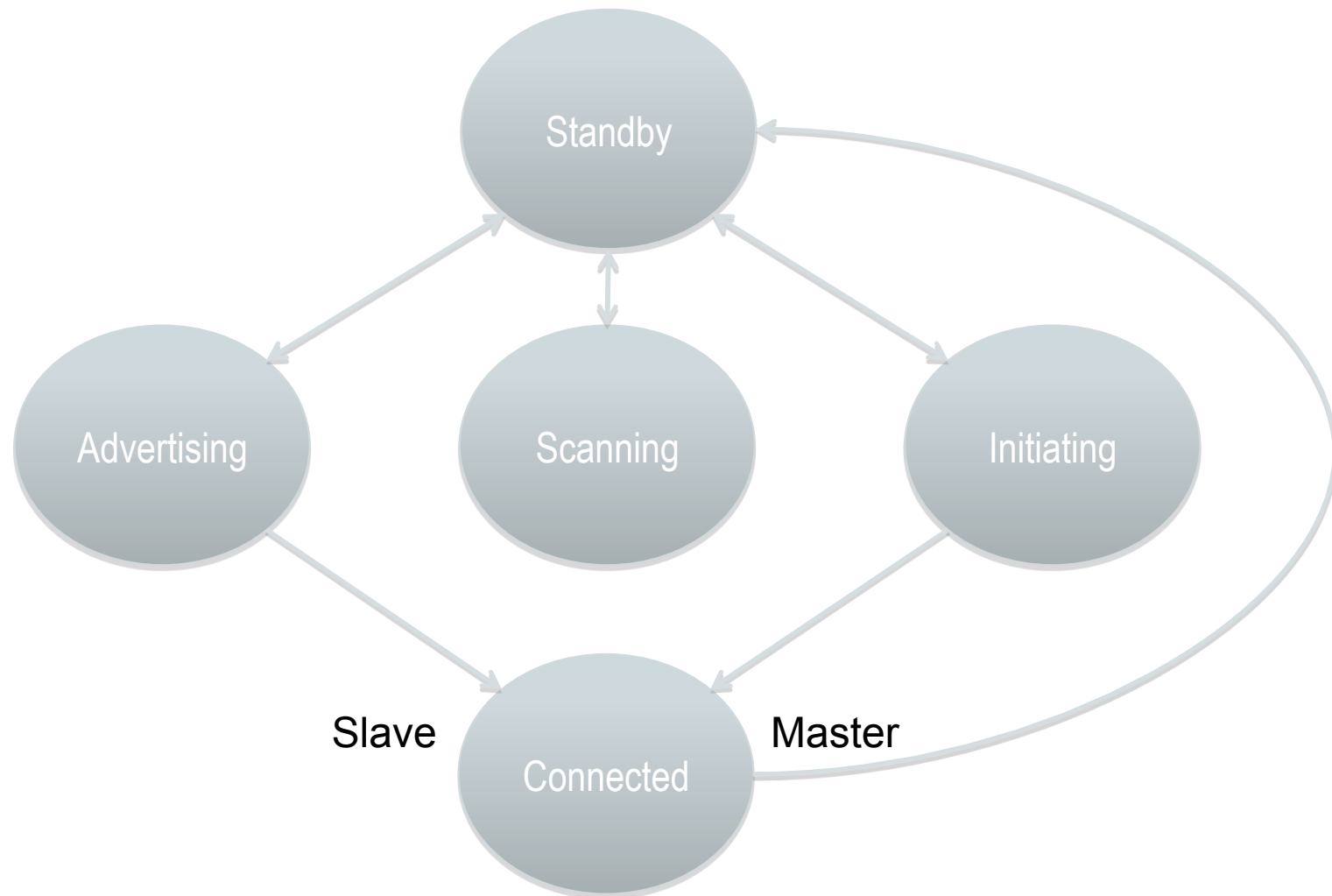
TECHNICAL OVERVIEW

- Radio
- Link Layer
- L2CAP
- Attributes
- Profiles

RADIO

- GMSK
 - Modulation Index = 0.5
- 40 Channels
 - 3 Advertising Channels for Discoverability and Connectability
 - 37 Data Channels using Adaptive Frequency Hopping (AFH)

LINK LAYER STATES AND ROLES



LINK LAYER STATES AND ROLES

- Advertising State
 - Discoverable / Connectable / Broadcasting
- Scanning State
 - Active or Passive Scanning
- Initiating State
 - Initiates a Connection to an Advertiser
- Connected State
 - Initiator becomes Master Role
 - Advertiser becomes Slave Role

WHY ADVERTISE?

- Up to 20x less power than *Bluetooth* BR
- Advertise for < 1.5 ms
 - Instead of scanning for 20ms to be connectable & discoverable
- Privacy concerns solved with “random device address”
 - Hashed random number using AES 128 bit encryption engine

LINK LAYER PACKET

- One Packet Structure
 - Preamble used to synchronize radios / AGC
 - Access Code used to identify device pair
 - PDU contains application information
 - 24 bit CRC protects PDU against bit errors

Preamble	Access Code	PDU	CRC
1 octet	4 octets	2 to 37 octets	3 octets

TWO TYPES OF PDU

- Advertising PDU
 - Used on to find devices, get additional information, initiate connections
 - ADV_IND, ADV_DISCOVER_IND, ADV_NONCONN_IND
 - ADV_DIRECT_IND
 - SCAN_REQ, SCAN_RSP
 - CONNECT_REQ
- Data PDU
 - Used to send application data reliably

WHEN CONNECTED...

- All communication is done in Connection Events
 - Just like *Bluetooth* Sniff Subrating – but lower power !!!
- “More Data” bit used to save power when no more data ready
- “Lazy Ack” bit used to acknowledge data using lower power

EVERYTHING IN *BLUETOOTH* LOW ENERGY TECHNOLOGY IS SIMPLIER !!!

Feature	<i>Bluetooth</i> BR/EDR	<i>Bluetooth</i> low energy technology
Packet Types	5 mandatory 13 BR packet types 10 EDR packet types	1 packet structure 2 packet formats (Adv / Data)
LM/LL Control Messages	75 LMP messages	8 LL Control messages
Protocols	9 (RFCOMM, BNEP, AVCTP, AVDTP, HCRP, TCSBIN, MCAP, OBEX, HID, SDP)	1 (Attribute)

L2CAP

- We use L2CAP packet formats
- We do not use connection oriented channels
- We use only Fixed channels for:
 - Attribute Protocol
 - Security Management Protocol
 - LE L2CAP Signalling

SECURITY MANAGEMENT PROTOCOL

- Security Management is now in Host
 - More flexible
- Builds on Secure Simple Pairing from *Bluetooth* BR/EDR v2.1
 - Exchange Device IO
 - Create trust (authentication)
 - Encrypt connection (security)
- Security is based off Long Term Keys – indexed by a Diversifier
 - Requires less memory (power) on slave device

IS *BLUETOOTH* LOW ENERGY TECHNOLOGY SECURE?

- Industry standard AES 128 bit encryption
 - 32 bit Message Integrity Check on every packet
- Secure Simple Pairing reused
 - v1.1 will also include ECC
- 128 bit Encryption Root used to derive Long Term Key
 - Reduces memory requirements for single mode slaves






ATTRIBUTES

- An attribute is just “Data”
 - Referenced by a Handle
 - Identified by a Type (UUID)
- Attributes can be
 - Read / Written / Indicated / Set / Discovered

ATTRIBUTE PROFILE

- Groups attributes together based on Handle
 - Handles are sorted
 - Attributes near group attributes are associated with that group
- Groupings include
 - Services and Profiles
 - Meta-Attributes – additional data about an attribute
 - Clients – which client “owns” this attribute

EVERYTHING IS DESIGNED FOR LOW POWER

Feature	Lower Power	Why
GMSK Modulation		More efficient transmission of data Uses less power to get data across
Advertising		10x to 20x lower power than BR/EDR Uses less power to be discoverable Uses less power to be connectable
Instant Sniff Mode		All data sent in Connection Events subrated to save even more power on slave
Fast Connections		Make connection, send data, get acknowledgement in 3 ms
Attribute Protocol		Connectionless protocol No state required Efficient Handle Value Indications

SUMMARY

- *Bluetooth* low energy technology is technically complete now
 - Interoperability testing has started
- Designed for “Low Power” above all other goals
- Complexity has been reduced to the minimum
 - While providing features customers want