Bluetooth Low Energy

What is BLE?

- Bluetooth 4.0
  - BR/EDR ("classic"): compatible subset
  - >> BLE: incompatible with classic, but very low energy
- Device modes
  - Dual mode: BR/EDR + BLE
  - Single mode: BLE only

Low Energy

- Simpler than BR/EDR, short packet, 40 RF channels
- Connection interval: Short Rx, average 5μA, Sleep 1μA
  - 1 year battery life (3V / 220 mAh) on CR2032
- Low peak power
  - Peak 15mA, compatible with CR2032 coin cell
- Good for transmitting state (commands, low-rate data)
  - Not as suitable for streaming (no SCO)

Who is using BLE?

- Smartmobiles and PC: "Dual-mode" (BluetoothSmart-Ready)
  - Since iPhone 4S (Fall 2011)/ iPad 3, Android 4.3 (2013)
  - Macs since mid-2011, Windows 8, Linux, …
  - Intel Edison (WiFi + BT4.0)

- Many new IoT products!
  - 162 products on official BLE web (IoT, not PC/ phone)
  - http://www.bluetooth.com/Pages/Bluetooth-Smart-Devices-List.aspx

Targeted devices

- Health & Fitness Wearable sensors
  - odometers, altimeters, sports watch

- Medical and home monitoring
  - heart-rate monitor, glucose meter, blood pressure, weight scale, light switches
- Appliance remote control
- Proximity tags
- Remote-controlled toys
- Mobile payment, shopping coupon
- Indoor navigation

BLE Certified Product Categories

- Observations
  - Sports + fitness = 45%
- Will look very different in a year
  - Proximity is fastest growing (both tags and beacons)
  - Many new IoT applications, esp. wearable, home, health,

Example: Personal & Fitness

- Personal activity tracker
  - Nike Fuel Band; FitBit
- Heart Rate Monitor (HRM chest strap)
  - Adidas miCoach, SmartRun HRM watch

- BostonMarathonTreadmills
- Wahoo Blue SC & Cadence Sensor (bike speed sensor)

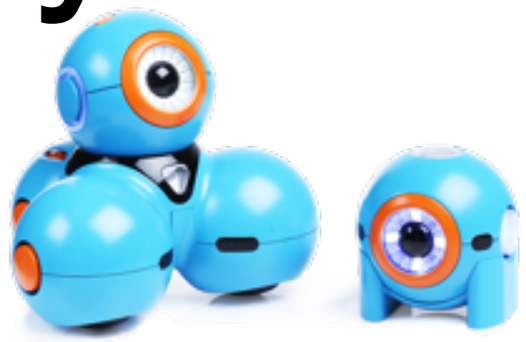
- Baby monitors…
- Weight scale, breath analyzer,

Example: BLE personal tags

Place a StickNFind on your pet's collar to get an alert if she wanders out of range.

- Example: Stick'N'Find, TinyFinder, TrackR…
  - BLE tag on personal objects, pets, key chair control, luggage
- Works with smartphones
  - As GUI + "reader" for finding object
  - Alerts on smartphone when walking away
  - Can work with iBeacon or compatible
- Long battery life
  - 1 year on coin-cell battery; 2-3 years on larger battery

Example: BLE Toys

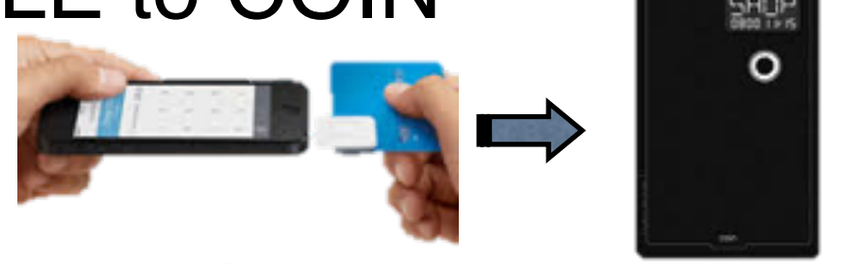


- Bo and Yana (play-i.com)
  - Children's programmable robots via iPad
- PowerUp 3.0 (poweruptoys.com)
  - BLE module & motor add-on to paper airplanes

- ANKI Drive (anki.com)
  - AI toy race cars with BLE

Example: Mobile payment

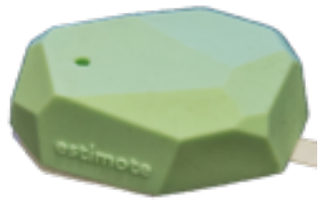
- Coin: Clones your existing credit cards (up to 8)
  - Swipe to read card into iPhone (via Square reader) and transfer card info via BLE to COIN
  - Use COIN as a credit card!
  - Bonus: acts as a BLE tag: rings phone when left behind



- PayPal BLE Beacon –
  - pay with PayPay app (competes w/NFC)!

BLE Beacons

- iBeacon (Apple)
  - Provides info on nearby products; indoor localization
- EstiMote



- Gimbal (QualComm): iBeacon compatible, $5 indoor, $10 outdoor
- ShopBeacon (ShopKick.com)

  - used in Macy's for product info; iBeacon compatible
- Enterprise Beacon (StickNFind): for indoor localization, iBeacon compatible
- BlueBite: For workout room

History of BLE

- Started in 2001 by Nokia Research
  - Bluetooth Low End Extension (2004)
- Nordic Semiconductor made nRF2401 RFIC
  - Shockburst MAC, renamed Wibree (2006)
    => very popular in wireless kb/mouse
  - ANT protocol built on this MAC (2005) nRF24AP1
    - Dynastream, now subsidiary of Garmin
    - ANT+: Used in health and fitness
- Part of Bluetooth SIG (2007), finalized 2010.

Application space

	voice	data	audio	video	state
Wi-Fi	Yes	Yes	Yes	Yes	?
Bluetooth	SCO	ACL	ACL	-	?
BLE	-	-	-	-	Yes
ZigBee	-	-	-	-	Yes
ANT	-	-	-	-	Yes

state means low-bandwidth, low-latency data and requires very low power

Topology space

	P2P	Piconet	Cluster Tree	Infrastructure	Mesh
Wi-Fi	Wi-Fi Direct	Wi-Fi Direct	-	Yes	-
Bluetooth	Yes	Yes	Scatternet	-	-
BLE	Yes	Yes	-	-	-
ZigBee	Y*	Yes	Yes	-	Yes
ANT	Y*	Yes	Yes	-	-

Y*: yes but with limited security

Wireless Comparison

	BLE	ANT+	ZigBee	RF4CE	Wi-Fi	NFC
Topology	Broadcast, Star, Scan, P2P, No mesh	Broadcast, Mesh, Scan, P2P	Mesh, Star, Scan, P2P, no broadcast	Mesh, Star, Scan, P2P, no broadcast	Star, P2P.	P2P only
Cost (1-10ku)	$1.95	$3.33 + MCU	$3.20	$2.75	$3 + MCU	$1 + MCU
PCB size (mm^2)	20	125	306	305	60	100
MCU	Integrated	Low-end, sep.	Integrated	Integrated	High-end, sep.	High-end sep.
Need Regulator?	No	No	No	No	Yes ($1.50)	Yes ($0.33)
Energy per bit	153 nJ	710 nJ	185,900 nJ	(~ZigBee)	5.25 nJ	(reader side)
Peak Current	12.5 mA	17 mA	40 mA	40 mA	116 mA	50 mA
Coin battery life @120 B/s	191 days	52.64 days	(too high)	(to high)	(too high)	(too high)
Distance	100 m	30 m	100 m	100 m	150 m	5 cm
Coexistence	Freq. hopping (37)	Fixed channel (1/8)	Freq. agility (1/16)	Fixed	Active coexistence	None (short burst)
Throughput	305 Kbps	20 Kbps	100 Kbps	100 Kbps	6 Mbps (11b)	424 Kbps
Latency	2.5 ms	< ms	20 ms	20 ms	1.5 ms	1 second
Direct to Smartmobile	Yes	(few)	No	No	Yes	(few)

Source: http://www.csr.com/sites/default/files/white-papers/comparisons_between_low_power_wireless_technologies.pdf

Spec Comparison

Technology	BT BR/EDR	BLE	ZigBee
Data rate	1-3Mbps	1Mbps	250Kbps
App.thruput	.7-2.1 Mbps	.2 Mbps	<.1 Mbps
Nodes / slaves	7 / ~2^{24}	unlimited	2^{16}
Security	64b/128b	128b AES	128b AES
Robustness	AFFH, FEC	AFFH	DSSS
Latency	100ms	<3ms	<10ms
Power ratio	1	0.01-0.5	2 / 0.1
Serv.Discovery	Yes	Yes	No

How BLE achieves low energy?

- Short packets to reduce Tx peak duration
- Hardware-supported connection interval to minimize idle Rx
- Fewer RF channels to improve discovery
- Simple state machine
- Single protocol

How BLE achieves low energy?

- Hardware-supported connection interval
  - Transaction time 3ms
  - Interval from 6ms to 20s
- Optimized to CR2032 coin cell battery
  - peak 15mA, average 5μA, sleep 1μA
  - 1 year minimum (3V/220mAh)

Power Consumption

- Different metrics
  - Peak power: when RF is on
  - Average power: energy ÷ time
- Both affect battery life
  - Can't really reduce peak, but can minimize peak-power duration
  - BLE's "low energy" => low average power

Where is RF power spent?

- Tx: depends on
  - The amount of data and the Tx gain.
  - Can turn off Tx when no data to transmit
- Rx:
  - Idle listening: burns power even when no data is received!
  - Solution: duty-cycle Rx to reduce idle listening

BLE factsheet

Range	~150m open field
Max current	~15 mA
Latency	3ms
Topology	Star
Connections	> 2 billion
Modulation	GFSK 2.4GHz
Robustness	Adaptive Frequency Hopping, 24b CRC
Security	128b AES CCM
Sleep current	~1μA
Data Rate	1Mbps

BLE Architecture

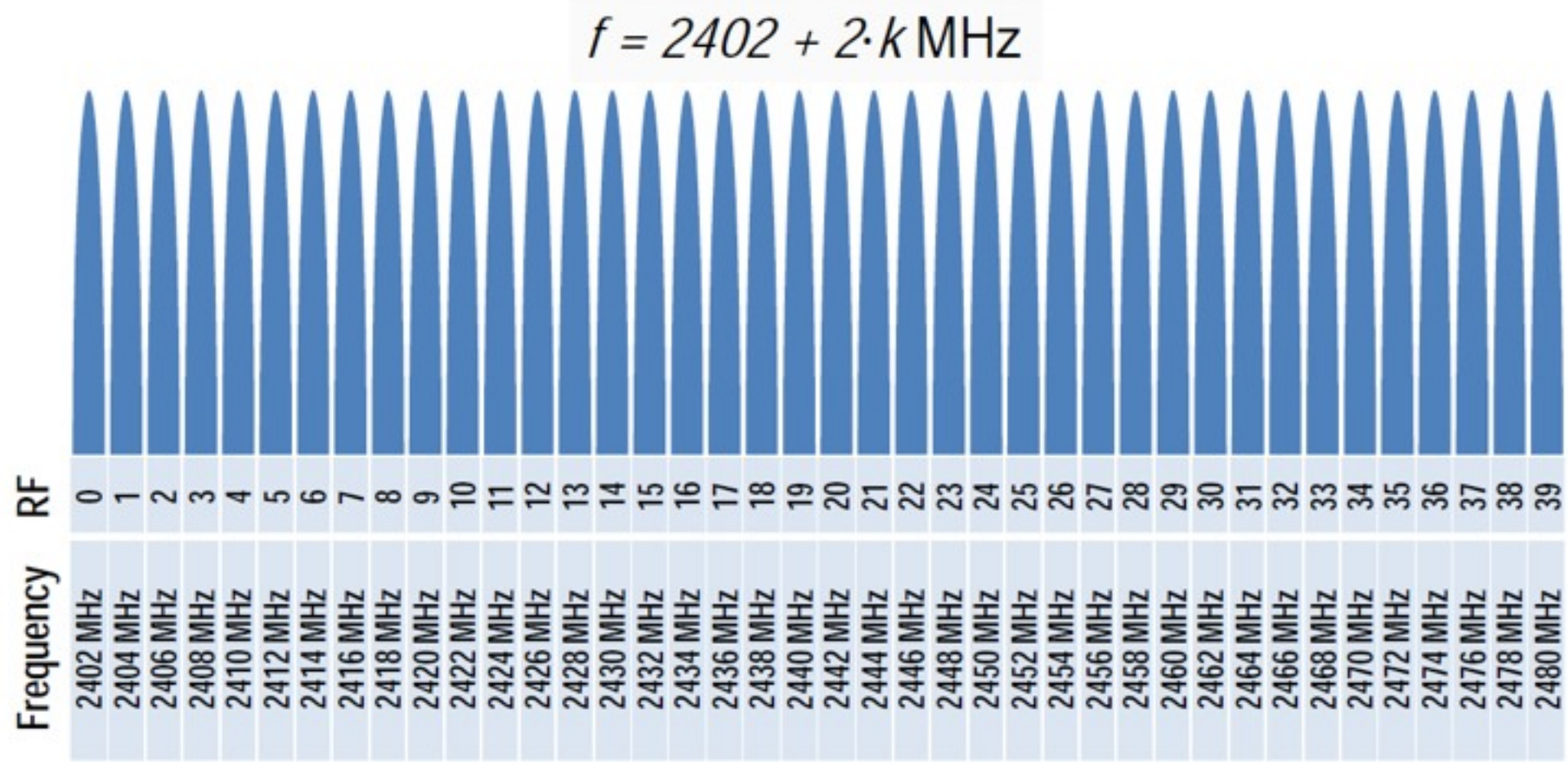
Applications								Application
PUID	Proximity	Simple RC	Battery	Temperature	Heart Rate	Blood Pressure	Time Update	Profiles
Generic Access Profile (GAP)								Host
Generic Attribute Profile (GATT)								
Attribute Protocol (ATT)					Security Manager (SMP)			
Link Control and Adaption Protocol (L2CAP)								
Host Controller Interface (HCI)								Link Controller
Link Layer (LL)					Direct Test Mode			
Physical Layer (PHY)								

Layers of BLE

- PHY: transmit/receive bits
- LL: packets and control
- L2CAP: Link multiplexor
- GAP: Discovery and Link management
- SMP: Link security
- ATT: Protocol for accessing data attributes
- GATT: Data attribute organization
- Profiles: Application-specific protocol between devices

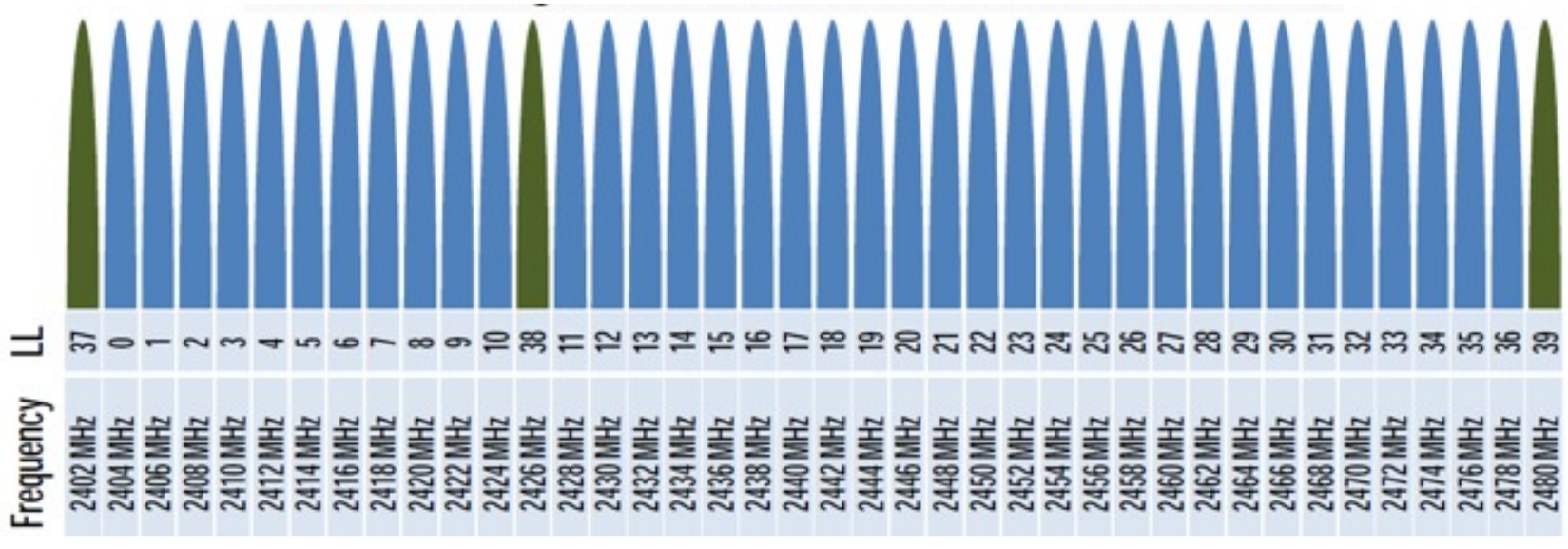
Physical Layer

- 2.4 GHz ISM band
- 1Mbps GFSK: Larger modulation index than Bluetooth BR (=> better range)
- 40 Channels on 2 MHz spacing



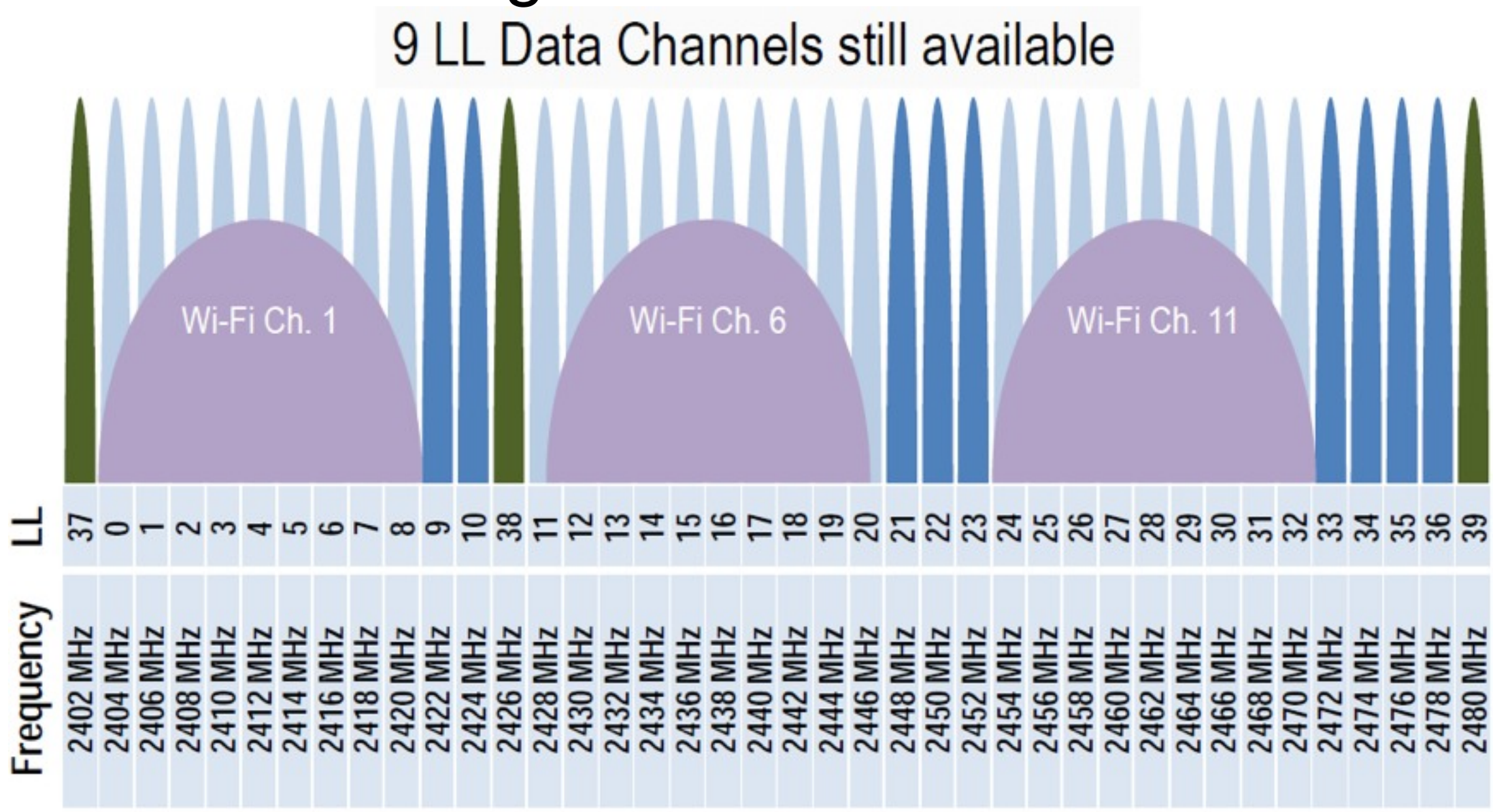
Physical Channels

- 3 fixed "advertising" channels
  - broadcast, connect, discover,...
- 37 dynamic "data" channels
  - application data (paired)



Physical Channels

- Advertising channels avoid 802.11

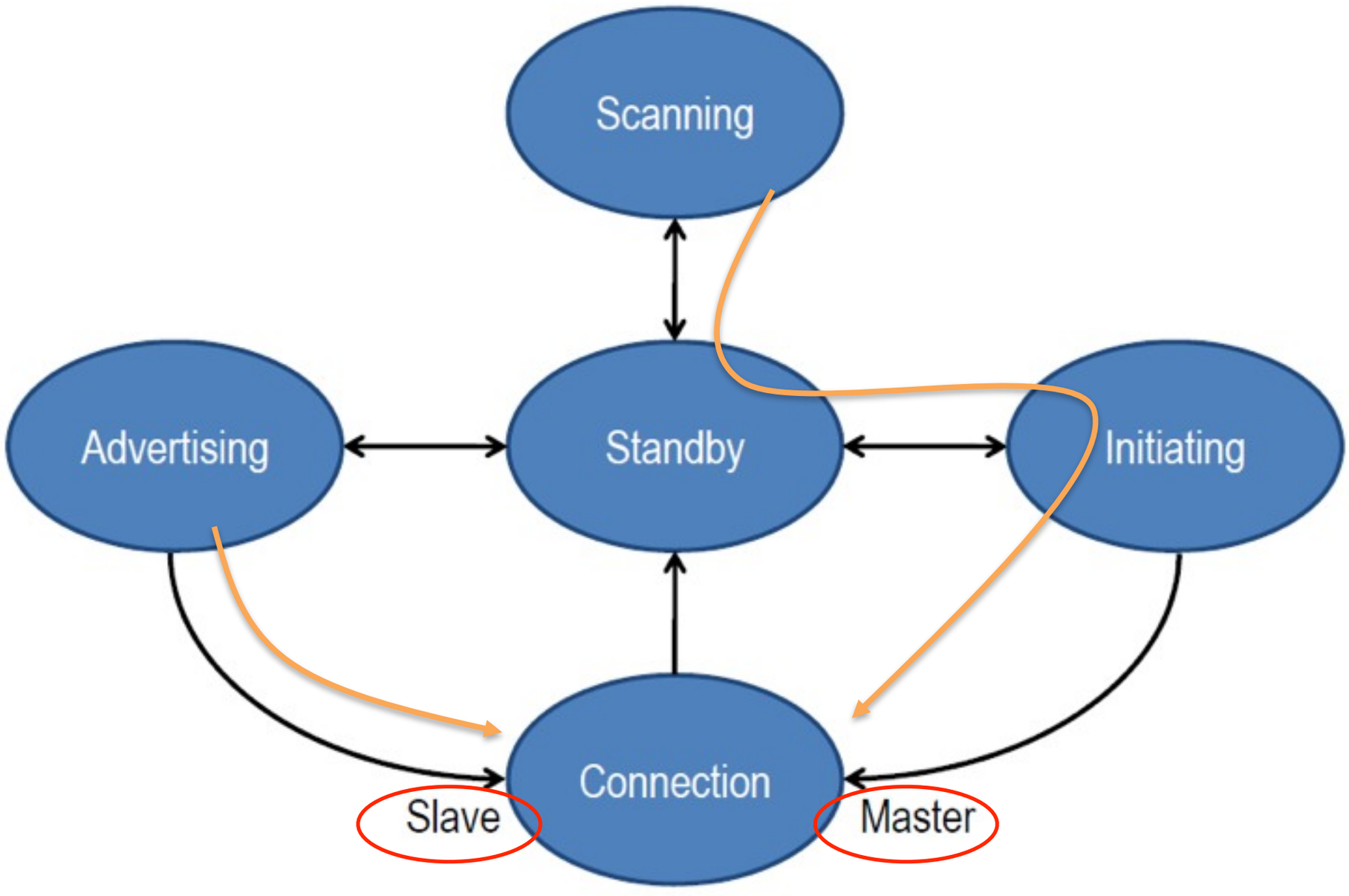


RF characteristics

- Tx: -20 dBm to +10 dBm
- Receive sensitivity
  - -70dBm, but -90dBm expected
- Modulation index
  - 0.5 for BLE, compared to 0.25 for BR/EDR
- Frequency hopping
  - No FH in advertise/scan
  - FH only in connections, but not required.

Link Layer

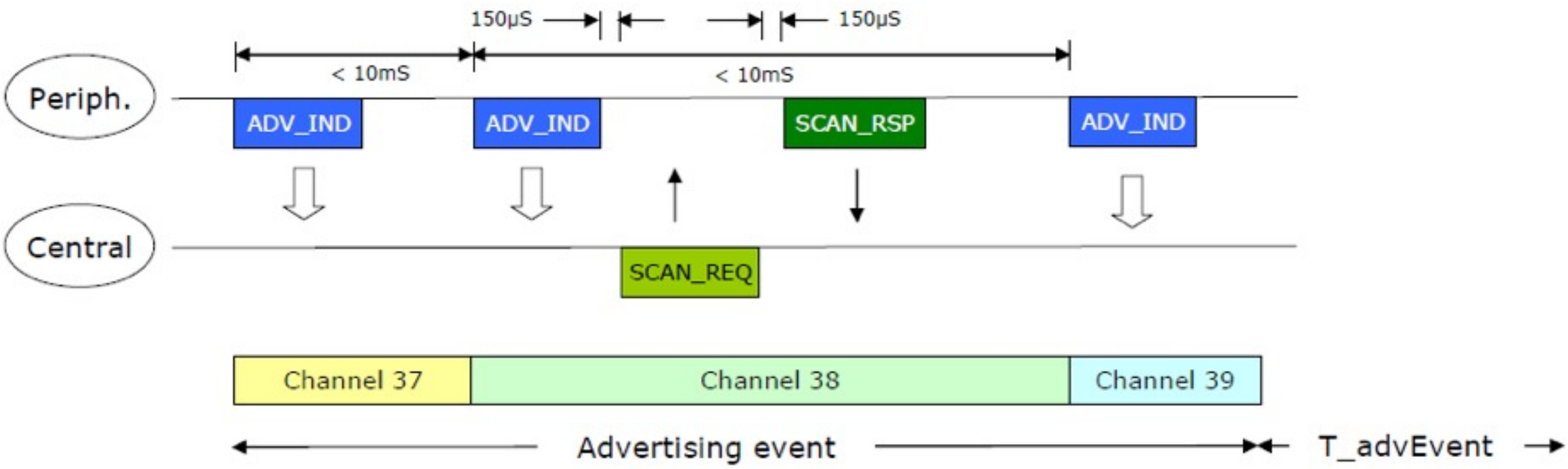
- Link Layer state machine



Pairing

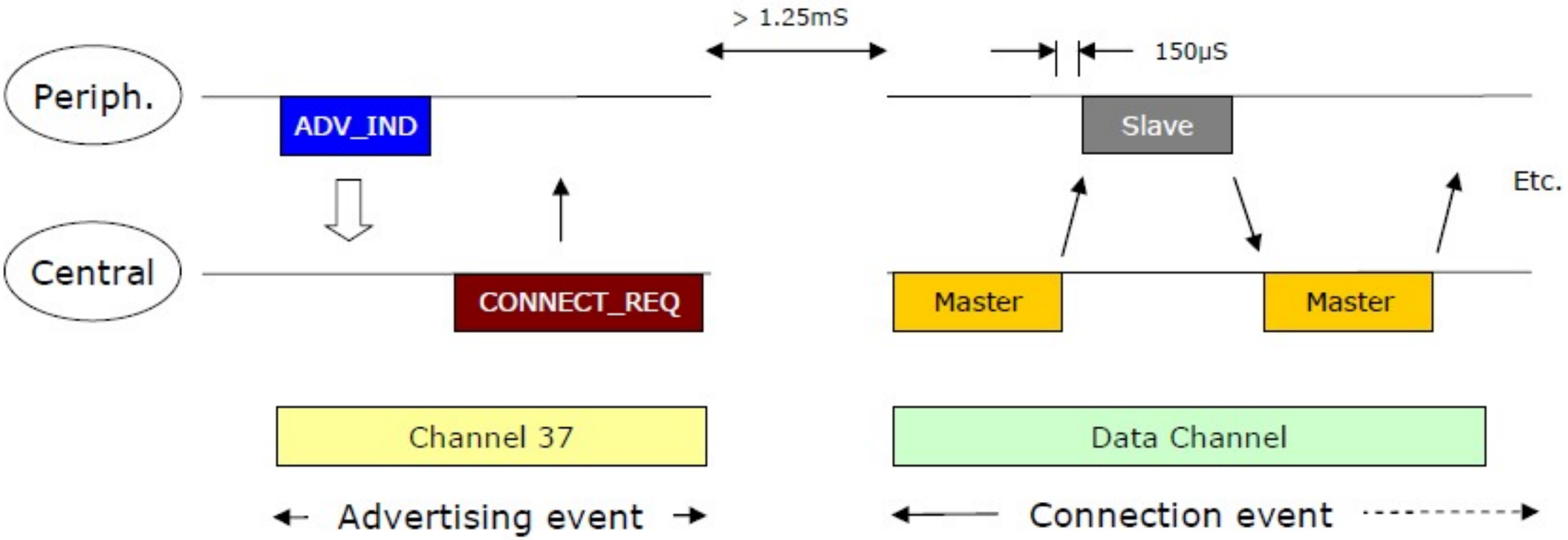
- Initially unpaired
  - Advertiser: "potential slave looking for master" / broadcaster
  - Scanner: "looking for slaves, but no commitment" / observer
- Pairing
  - Initiator: master sending connection request to advertiser
  - Exchange control info (crypto key, frequency hop)
- When paired
  - Slave can be paired to at most one master
  - a BLE node can't be both master and slave at the same time (4.0). But can in 4.1 and up.

Advertising



- Devices can advertise for a variety of reasons:
  - To advertise their presence to a device wanting to connect
  - To broadcast promiscuously (piggybacked data)
  - To transmit signed data to a previously bonded device
  - To reconnect asynchronously due to a local event

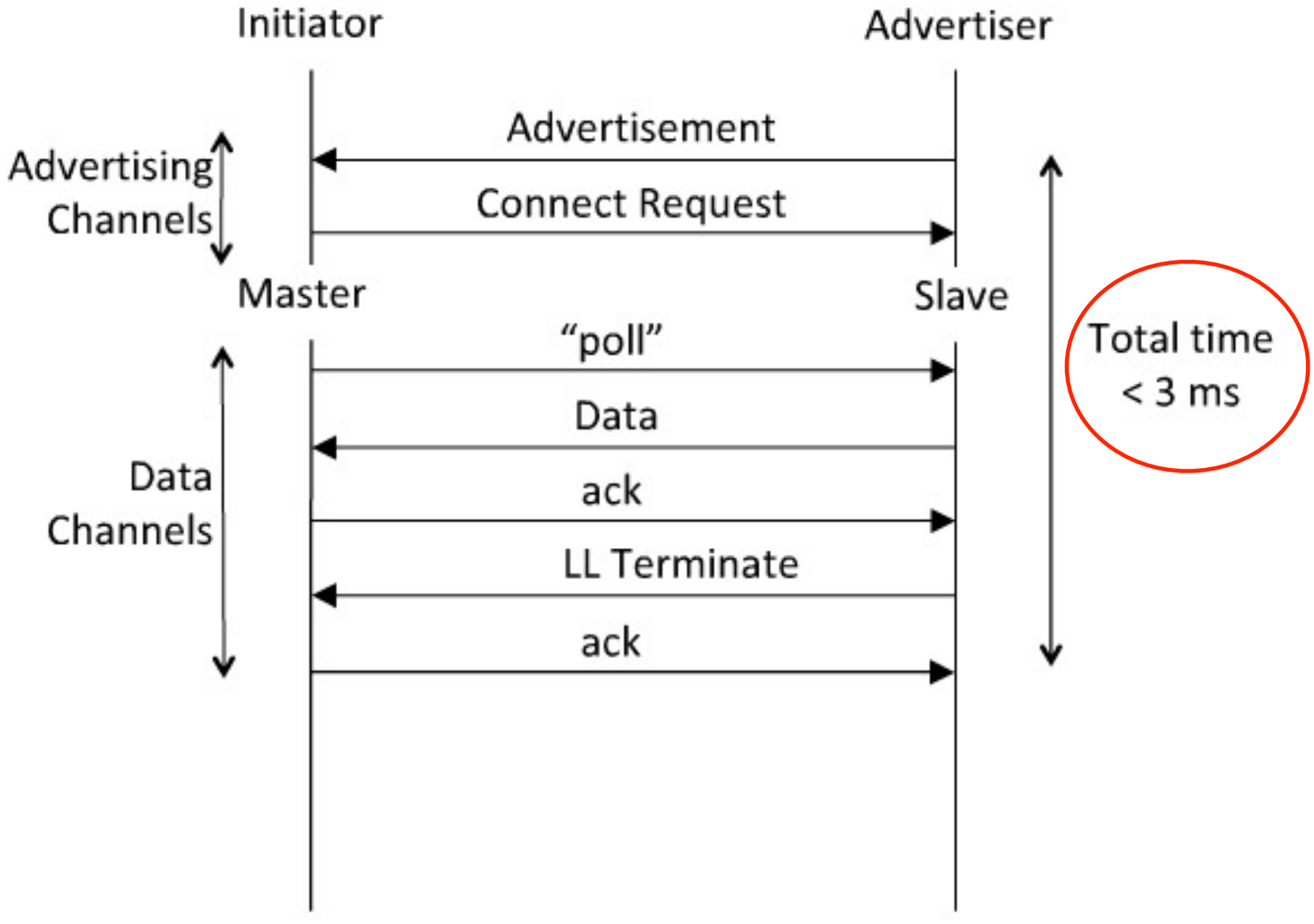
Data transactions



- Once a connection is made:
  - Master informs slave of hopping sequence and when to wake
  - All subsequent transactions are performed in the 37 data channels
  - Transactions can be encrypted
  - Both devices can go into deep sleep between transactions

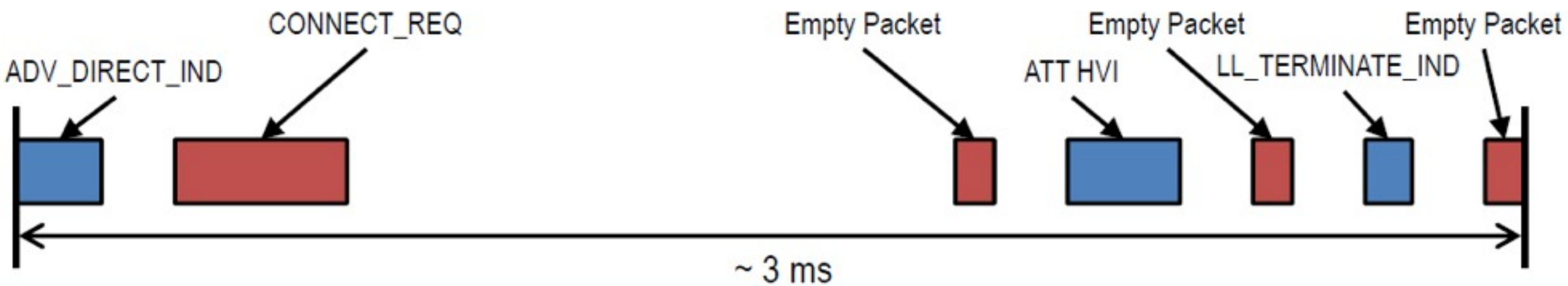
Link Layer Connection

- Very low latency connection



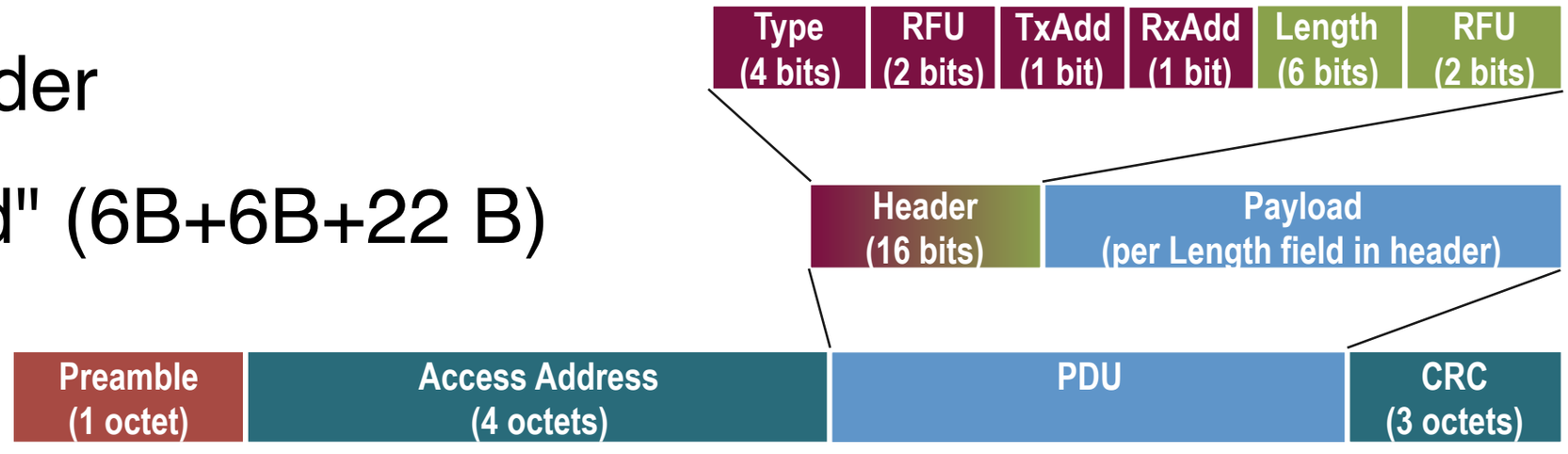
Time From Disconnected to Data ~ 3ms

Time (us)	Master Tx	Radio Active (us)	Slave Tx
0		176	ADV_DIRECT_IND
326	CONNECT_REQ	352	
1928	Empty Packet	80	
2158		144	Attribute Protocol Handle Value Indication
2452	Empty Packet (Acknowledgement)	80	
2682		96	LL_TERMINATE_IND
2928	Empty Packet (Acknowledgement)	80	



Link-Layer Packet Format

- Preamble (1 byte): 0x55 or 0xAA (01010101 or 10101010)
- Access Address (4 B)
  - 0x8389bed6 for advertising
  - other addresses for each LL connection
- Packet Data Unit (PDU) (2-39 B)
  - 2-B header
  - "payload" (6B+6B+22 B)
- CRC (3 B)



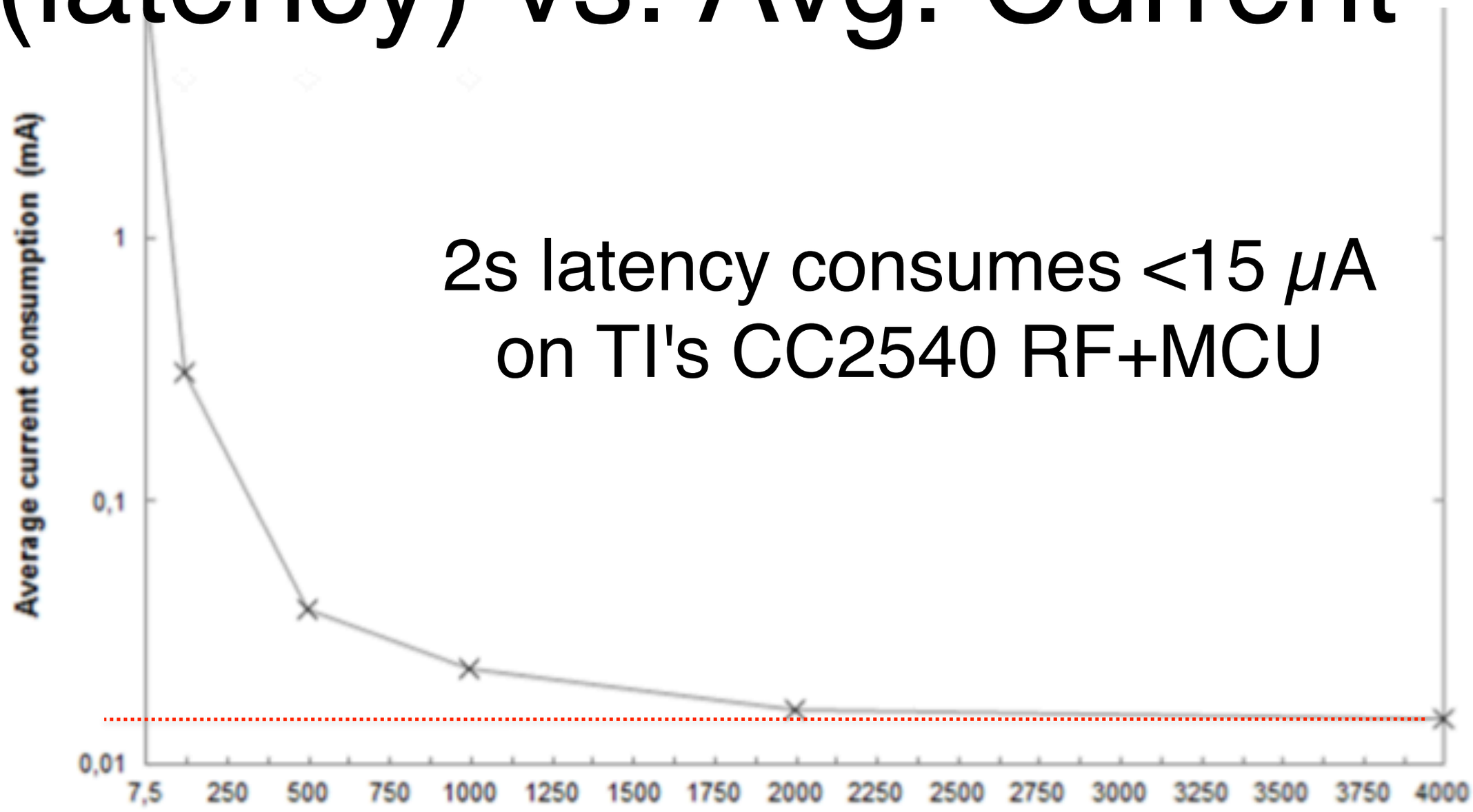
LL Device Filtering

- Devices maintain a white-list
- Advertiser:
  - default: allow all scan/connect requests
  - Filter: limit scan/connect from white list (separate lists for scan or connect)
- Scanner and initiator
  - defaults to all advertising, but can limit to white list

Low-power Wakeup

- Problem: how to wake a deep-sleeping node
  - Keep radio on => waste 15mA all the time
  - Use out-of-band radio or RFID
    - "Low-power listening" (duty cycle Rx by software)
- BLE solution: Connection interval
  - Master/slave agree on Connection interval
  - Hardware does synchronized Rx checking, wakes MCU if actually receiving packet
  - Can trade between power and latency

Connection Interval (latency) vs. Avg. Current



2s latency consumes <15 μA
on TI's CC2540 RF+MCU

Source: C. Gomez, J. Oller, J. Paradells, Sensors, vol. 12, 2012. 11734—11753. doi: 10.3390/s120911734. http://www.mdpi.com/1424-8220/12/9/11734/pdf

RF Power Consumption of CC2540

- Transmit (Tx): 25mA typical
  - -23 dBm => 21.1 mA
  - 0 dBm => 27 mA
  - 4 dBm => 31.6 mA
- Receive (Rx)
  - Standard gain: -87dBm => 19.6 mA
  - High gain: -93dBm => 22.1 mA

Average Power Consumption

Chip used: Nordic nRF8001 (excluding MCU)

Interval	Connected mode	Advertising mode
2 sec	10μA	29μA
1 sec	17μA	56μA
250 ms	55μA	110μA

HCI

- Inherit from BR
  - Keeps the existing HCI format
- Added LE commands
  - Scanning, Advertising
- Reuses existing transports
  - e.g., UART, USB, SDIO, 3wire, SPI, ...

Profile Roles

- BLE-defined minimum-set of LL features
- Four required
  - broadcaster
  - observer
  - peripheral
  - central

broadcast/listen

paired master/slave

- A device may support one or more roles

Profiles

- "Domain-specific service protocols"
  - Packet format and meaning of values
- Attributes = "data with meaning" & access
  - value, type, access permission, security requirements
  - addressed by a handle
- Purpose: multivendor interoperability

Attributes

- Value: up to 512 octets, fixed or variable length
- Handle: address of an individual attribute by client
- Type
  - UUID to determine meaning (e.g., °C)
  - Defined by GAP, GATT characteristic specification
- Permission
  - Read, Write; may require authentication

Generic Access Profile (GAP) in BLE

- Handling device access modes procedures
  - Device Discovery, link establishment and termination
  - Security features (fixed or random passcode)
  - Device configuration
- Roles
  - Unpaired: broadcaster, observer
  - Paired: peripheral, central
- Connection interval, slave latency, and supervision timeout

Generic Attribute Profile (GATT) in BLE

- Roles
  - GATT Client: initiates read/write the data
  - GATT Server: owns data, serves request
- Provides "Services"
  - mandatory GAP service: device/vendor name
  - mandatory GATT service: info about this GATT server
  - Application-defined services

Access Patterns on attributes

- Read and Write
  - Client sends requests to Server
  - Client may read/write an attribute via a handle (adders) or using UUID; once or multiple
- Notification (of characteristic value)
  - Client sets up and then does not pull; Server sends data (as defined by profile).

BLE Profiles

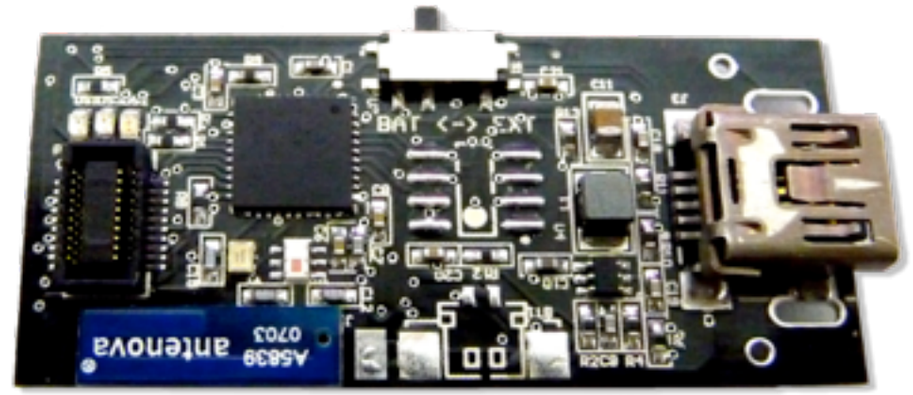
- MedWG
  - Body Temperature
  - Blood Pressure
  - Weight Scale
  - Glucose
  - Pulse Oximeter
  - Heart Rate
- Pedometer
  - Speed
  - Distance
- HID WG
  - Keyboard
  - Mouse
  - Game controller

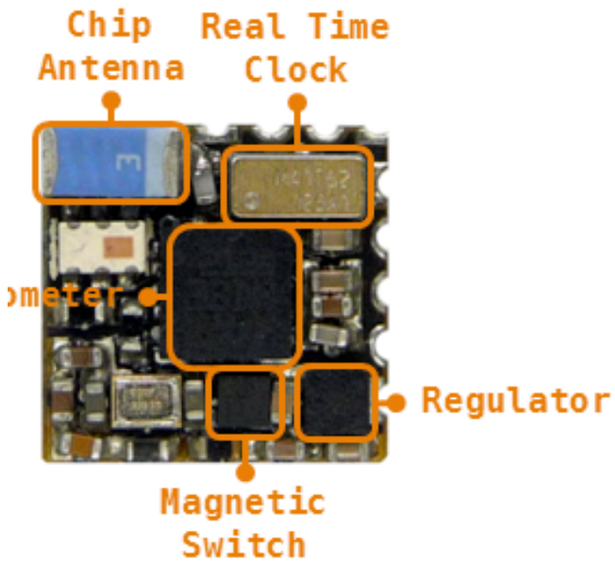
RFICs & Modules Available

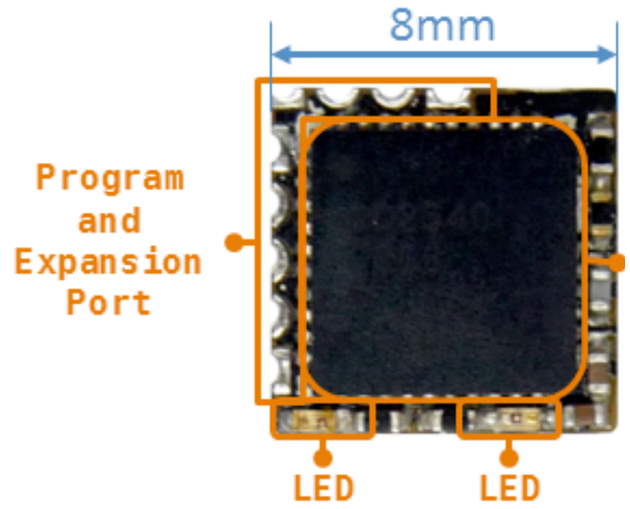
- Single Mode BLE
  - TI CC2540 (BLE + 8051), 2541, ...
  - Nordic nRF8001 (BLE coprocessor), nRF51822 (BLE + ARM Cortex M0 core)
  - CSR 1000 and 1001
- Multi-protocol modules
  - TI CC2564,2569 (BR EDR, BLE, ANT)

Development Kit at NTHU: EcoBT

- SuperNode
  - CC2540 MCU:
    8051 core, 8KB SRAM,
    256KB flash, on-chip
    ADC & Volt.comparator,
    USB2 slave
  - MicroSD, digital accelerometer, RTC
- Simple Node
  - 8x8 mm^2, Acc + RTC







Interfaces on CC254x

- BLE Stack -- host or peripheral
- two USARTs (UART or SPI)
  => connected to accelerometer
- I2C (on CC2541; emulated on CC2540)
  => connected to RTC
- USB slave (on CC2540)
- ADC channels

How to program CC254x

- Official Option
  - Compiler: IAR Embedded Workbench
  - TI: OSAL, BLE stack; + user code
- Our option
  - Compiler: SDCC for user code
  - Link with existing image made by IAR