Bluetooth Low Energy Controller in Zephyr OS

Vinayak Kariappa Chettimada
Consultant, Nordic Semiconductor ASA
SixOctets Systems, Bengaluru
@vkchettimada
Introduction
Vinayak Kariappa Chettimada

- Over 16 years in the industry
- Primary contributing maintainer of Zephyr BLE controller subsystem
  - Original author
- Architect and lead developer Bluetooth Software Stacks
  - nRF8001/2 firmware, SoftDevices for nRF51 Series and latest nRF52 series
- Prior experiences with leading mobile phone and automotive manufacturer
  - Headset, Handsfree, Advanced Audio support in car kits and their IOP with phones
- Windows applications and web technologies
- Linux user and developer since a student
Bluetooth

- Short range, low-power
- Frequency hopping spread spectrum (FHSS)
- 2.4 GHz ISM band
- Bluetooth Special Interest Group formed in 1998
- 20 Years
- Billions of products shipped
- 33000+ SIG member companies
Bluetooth Low Energy (BLE)

- Ultra Low Power
- Optimized for short burst data transmission
  - Small packets
  - Short RX and TX windows
- Race to idle
  - Turn radio on as seldom as possible
  - Turn radio off as soon as possible
- Fast connection in 6 ms and teardown
- Simple stateless operation
  - Data in form of parameter-value
- Low memory footprint
- Coin-cell battery 1+ year
Technology
BLE Stack

Profiles
- HID over GATT
- Proximity
- Battery
- Thermometer
- Heart Rate
- Blood Pressure
- Speed & Cadence...

Host
- GATT
- GAP
- ATT
- SMP
- L2CAP

Controller
- Host Controller Interface (HCI)
- Link Layer (LL)
- Physical Layer (PHY)
- 2.4 GHz free ISM band
- 1 Mbit/s and 2 Mbit/s signalling rate
- GFSK modulation
- +20 dBm maximum transmit power
- 40 RF channels
- 3 advertising channels reserved for:
  - Broadcast
  - Discover
  - Connect
- 37 data channels
BLE: Link Layer

- **Advertising**: connectable and non-connectable
- **Scanning**: active or passive
- **Slave and Master**: connection role
- **31 bytes** legacy advertising payload size
- **255 bytes** extended advertising on data channels with additional chaining
- **27-255 bytes** maximum payload size per PDU
- **AES-128** built-in encryption
- **CCM**
  - Counter with
  - Cipher Block Chaining
  - Message Authentication Code
Advertising and Scanning

Scanner scan interval = 50 ms
Scanner scan window = 25 ms

Advertising on 37, 38 and 39

Advertiser advertising interval = 20 ms
Topology
Connection

Selectable Connection Interval: 7.5 ms to 4 s
Advertising, Scanning, slave and master

• Demo using Zephyr OS
  – samples/bluetooth/peripheral
  – samples/bluetooth/central_hr
Advertising, Scanning, slave and master
Controller
Conformance
Features

• BLE 5.0 compliant
• Unlimited role and connection count, all roles supported
• Concurrent multi-protocol support ready
• Intelligent scheduling of roles to minimize overlap
• Portable design to any open BLE radio, currently supports Nordic Semiconductor nRF51 and nRF52 Series
Architecture

- **Zephyr**
  - Threads, fifo, semaphore

- **HCI**
  - Host Controller Interface, Bluetooth standard
  - Provides Zephyr Bluetooth HCI Driver

- **HAL**
  - Hardware Abstraction Layer
  - Vendor Specific, Replace with Zephyr Driver

- **Ticker**
  - Soft real time radio/resource scheduling

- **LL_SW**
  - Software-based Link Layer
  - States and Roles, control procedures, packet controller

- **Util**
  - Bare metal memory management
  - Queues of variable count, lockless
  - FIFO, fixed count, lockless, ISR-ISR-Thread
  - Mayfly
Multi-vendor execution contexts

- Vendor Specific Lower Link Layer (LLL)
  - Open or closed source
  - Bare-metal
  - High priority Direct ISR
- Open source Upper Link Layer (ULL)
  - Mayfly ISR infrastructure
  - Ideally use Kernel features
Mayfly

- Multi-instance scalable ISR execution contexts
- Mayfly is to ISR, as Work is to Thread
- Race-to-idle execution
- Priorities map to IRQ priorities
- Cross context scheduling
- Lock-less, bare metal
Scheduling

HTML content is not available.
Data Path: Tx

- Host thread
  - Scheduler
  - Event prepare (LLCP)
  - Event/Rx/Tx done
  - Tx PDU pool
  - Rx PDU pool
  - Rx demux
  - Rx packets per role

- Pointer to Tx packet
  - Pointer to Tx packet (carries link element to be freed + pool association)
  - Pointer to Tx packet
  - Pointer to Tx packet

- Link element points to Tx packet (carries data/control pool association)
- FIFO event queue
- FIFO tx queue
- FIFO tx_link queue (s)
- FIFO tx_done queue
- FIFO ticker
- User ops insert/remove
- Scheduler Event prepare/remove
- Memq Linked List
- ULL isr (tasklet)
- LLL isr (and HW)
- LLCP Baseband timer (HAL/HW)
- RTC
- Interrupt
- Role enable/disable
- HCI
- HCI driver
- Role enqueue
- Tx PDU release
- Notify host and release
- Forward to host
- Tx done
- Event done
- Event Rx done
- Rx done
- Rx packets
- Rx POIU release
- Rx POIU pool
- Rx POIU receive
- Event/Rx/Tx done
- LLLCP/ULL control procedures
- Rx demux
- Rx link pool
- Rx ultralink pool
- Tx queue
- Tx enqueue
- Transmission
- Packet Controller
Demonstrations with Q&A
Zephyr Continuous Scan with Advertising Event
Continuous events for continuous scanning and directed advertising
- Are truly continuous with very low Radio Idle when switching Tx/Rx state or channels
- Radio idle time: Min. 70us to Max. 300us

Events extend into unreserved time space

Reserved time space events pre-empt overlapping unreserved time space events
- Pre-emptor is placed in a pipeline to perform the pre-emption just-in-time to the event’s Radio start

Pre-emptee event can decide to resume after pre-emptor
Thank You