Sniffle

A sniffer for Bluetooth 5 (LE)

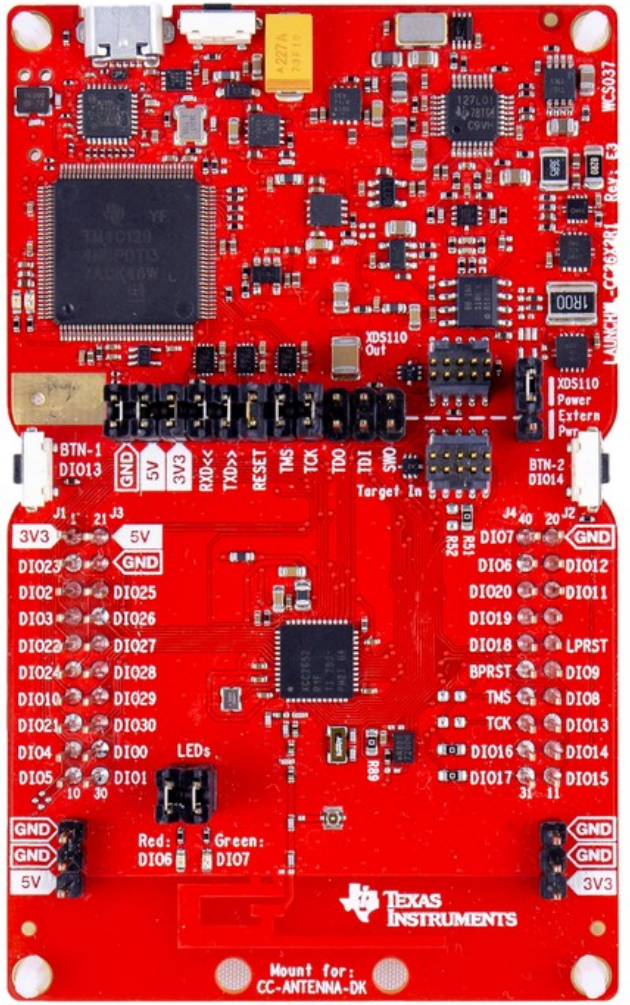
Hardwear.io Netherlands 2019

Sultan Qasim Khan

nccgroup

What is Sniffle?

- Sniffle is a packet sniffer for Bluetooth 5 LE (backwards compatible with 4.x)
- It runs on Texas Instruments CC13x2 and CC26x2 MCUs
- It supports new PHY modes in Bluetooth 5, including 2M and coded PHYs
- It supports Bluetooth 5 extended advertising
- It can display packets and record to PCAP files
- It is vastly more reliable than existing low cost BLE sniffers



Bluetooth Background

- Bluetooth Classic and Low Energy (LE) are very distinct protocols with little in common (except HCI and L2CAP)
- Both LE and Classic are frequency hopping spread spectrum (FHSS) in the unlicensed 2.4 GHz band, but use different PHYs
- Classic most commonly used for audio streaming and hands free calling, while most IoT devices use LE
- Both Classic and LE are part of the Bluetooth 5 standard, but the term Bluetooth 5 most commonly refers to Bluetooth 5 LE

Bluetooth LE

- Introduced in the Bluetooth 4.0 specification in 2010, originally intended as a low power protocol for devices with limited data throughput requirements
- Divides 2.4 GHz spectrum into 40 channels: 0-36 for data, 37-39 for advertising
- Upper layer communications built on GATT protocol, where clients can read, write, or subscribe to “characteristics” on a server
- BLE 4.0/4.1 have well known weaknesses in their pairing process which uses symmetric cryptography
- BLE 4.2 introduced an optional more secure ECDH pairing scheme
- BLE 4.2 added Data Length Extension (DLE), and BLE 5 added 2M PHY, both greatly increasing throughput

Bluetooth 5

- Introduced in 2017, with enhancements focused on LE
- New PHY modes for high throughput (2M) and long range (125k and 500k coded on 1M)
- New PRNG based channel hopping algorithm
- Greatly expanded advertising support, with advertising on secondary advertising (data) channels and connectionless data streaming (“periodic advertising”)
- Angle of Arrival (AoA) and Angle of Departure (AoD) measurement for location measurement using beacons (BLE 5.1)
- Randomized selection of primary advertising channels (BLE 5.1)
- These additions are optional

Problems With Existing Sniffers

- Sniffing only one advertising channel
  - Limits connection detection reliability to below 33%
  - All low cost sniffers have this limitation
- Missing or incomplete Bluetooth 5 support
  - New PHY modes, new channel hopping, advertising extensions
- Proprietary software and firmware
  - Windows only software, non-extensible software and firmware
- High cost

What Sniffle Does

- Uses the Bluetooth radio hardware built into Texas Instruments CC13x2/CC26x2 microcontrollers to capture Bluetooth LE traffic on any channel in any PHY mode
- Captures advertisements, can follow connections when connection establishment detected
- Target filtering by MAC and RSSI supported
- Handles updates to connection parameters, channel map, or PHY mode when following connections
- Streams captured traffic to a host PC over USB UART
- Host software displays and decodes traffic, and can save to PCAP too

Advertising Hopping Sequence

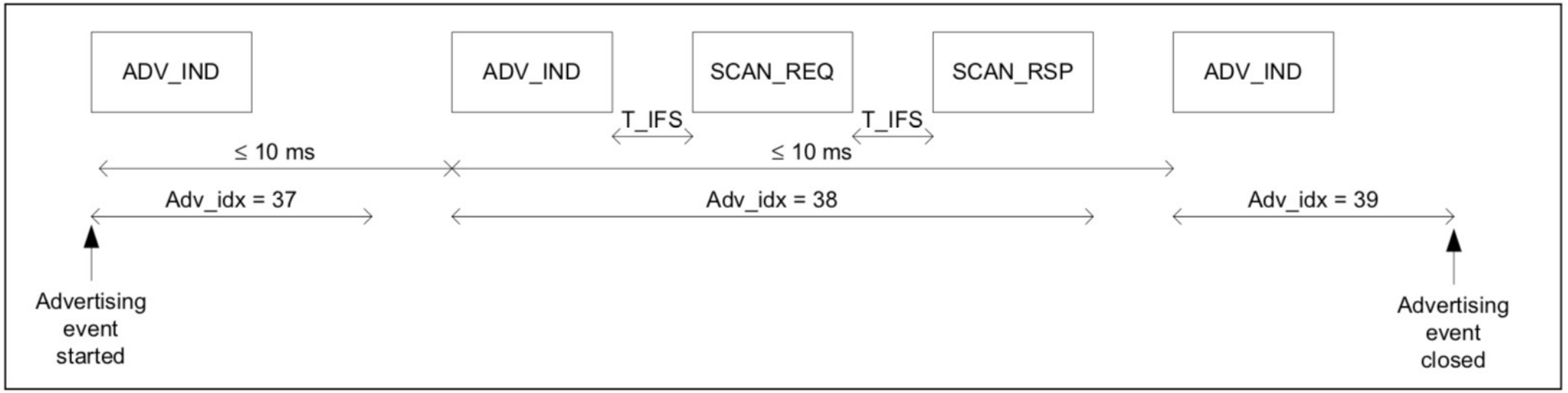


Figure 4.8: Connectable and scannable undirected advertising event with SCAN_REQ and SCAN_RSP PDUs in the middle of an advertising event

4.4.2.2 Advertising Events:
Advertising events are defined as one or more advertising PDUs sent on the primary advertising channel beginning with the first used advertising channel index and ending with the last used advertising channel index.

Figure and text from Bluetooth 5.0 Core Specification, Volume 6, Part B

Advertising Event Pattern

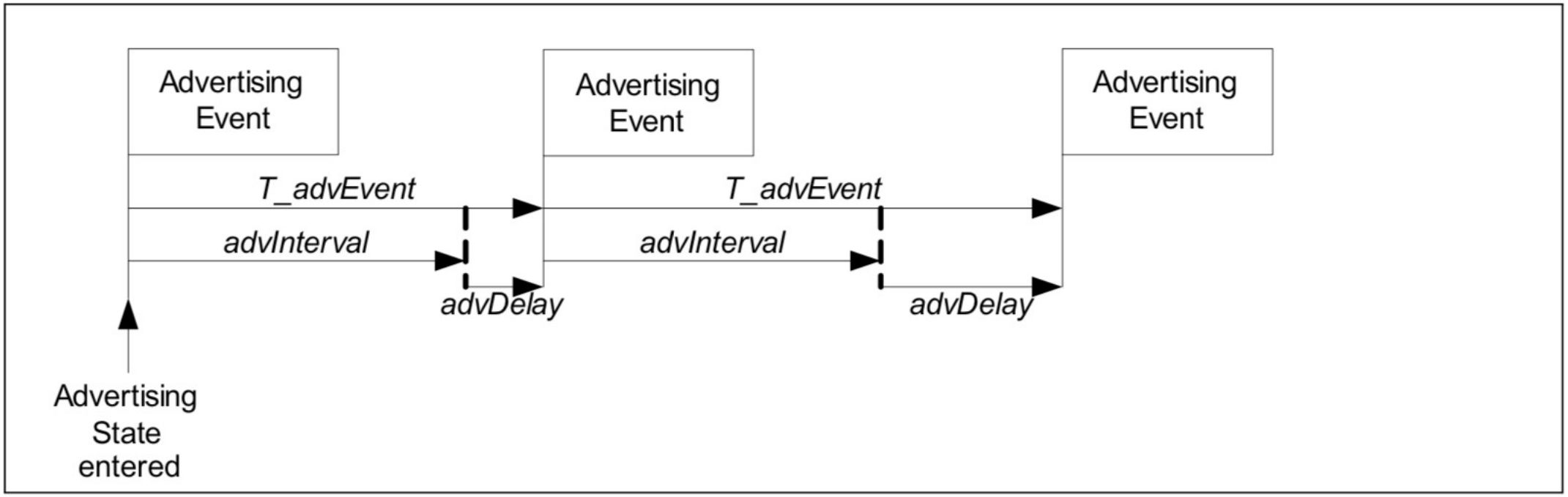


Figure 4.3: Advertising events perturbed in time using advDelay

Figure from Bluetooth 5.0 Core Specification, Volume 6, Part B

Sniffing All Three Advertising Channels

- Most sniffers only sniff one advertising channel, but connection initiation can happen on any of the advertising channels
- One workaround is to run three sniffers simultaneously
- Sniffle can follow the advertisement channel hopping of a BLE peripheral using a single radio
- It figures out the time spent on each advertising channel
- When Sniffle receives an advertisement on channel 37, it knows roughly when the next advertisement will be sent on channel 38
- The time spent on a channel can be extended by scan requests, so Sniffle adjusts accordingly when a scan request is received

Advertising Hop Parameter Detection

1. Wait for an advertisement from the target MAC address on channel 37
2. After receiving an advertisement on 37, immediately hop to channel 39, and wait for another advertisement from the target MAC
3. Record the time difference between advertisements on channels 37 and 39.
4. Repeat steps 1-3 to capture sufficient samples.
5. Sort the samples, and take half the 25th percentile as the base advertising hop interval.
   - We halve the value since 37->39 is two hops
   - We use 25th percentile instead of median because many intervals were extended from the base amount by scan requests/responses

Advertisement Hop Algorithm

1. Wait for an advertisement from the target on channel 37.
2. Schedule a hop to channel 38 one interval after the advertisement on 37 arrived.
3. Postpone the hop to 38 if we receive a scan request.
4. Wait for an advertisement on channel 38 for one hop interval.
5. Wait for an advertisement on channel 39 for one hop interval.

Note: Latency compensation omitted from description for simplicity

Caveat: Bluetooth 5.1 allows randomizing the advertising hop sequence

- However, BT 5.1 devices will usually connect on secondary channels using extended advertising, which Sniffle can sniff

Bluetooth 5 Extended Advertising

- Short advertisements on primary advertising channels point to longer auxiliary advertisements on secondary (data) channels
- Auxiliary packet pointers specify a channel, PHY, and offset
- Connection establishment occurs on the secondary channel
- Auxiliary advertising packets can be up to 255 bytes in length, and can be chained
- Auxiliary advertisements can point to periodic advertising trains for connectionless broadcast data streaming
- These additions greatly extend advertising bandwidth compared to Bluetooth 4.x LE

Extended Advertising Support in Sniffle

- Sniffle schedules hopping to secondary advertising channels as required to capture auxiliary advertising packets
- Sniffle can detect and follow connections established on secondary channels
- Sniffle's firmware currently does not support periodic advertising capture
  - Very few current devices actually support periodic advertising
  - Specification is vague on channel hopping for periodic advertising
  - Support can be implemented in the future (no hardware limitations)

When to Use a Sniffer

- Use local HCI Snoop logging where possible, since sniffers occasionally miss data
  - Standardized HCI Snoop logging captures all traffic between the host and BT controller
  - Often the only option for Bluetooth Classic, since low cost BT Classic sniffers are limited, and commercial sniffers are expensive
  - Be aware of transformations performed by the controller such as encryption
  - Sniffers provide a clear view of actual traffic over the air that can be helpful when diagnosing controller or stack level issues, or just identifying exactly what is encrypted
- For capturing BLE traffic between embedded devices with limited internal access, you need a sniffer
- You may need a sniffer to capture BLE advertisements more thoroughly than an ordinary BT adapter

Comparison to Low Cost Sniffers

	Sniffle	Ubertooth	TI Sniffer v1 (CC2540)	TI Sniffer v2 (CC26xx)	Nordic nRF51	Nordic nRF52	BtleJack 2
Cost	$40	$120	$40	$40	$40	$40	$15
Open Source	Yes	Yes	No	Yes	No	No	Yes
Data Length Extension	Yes	Yes	No	Yes	Yes	Yes	Yes
BT5 PHY	Yes	No	No	No	No	2M	No
BT5 CSA #2	Yes	No	No	No	No	No	Yes
BT5 Ext. Adv.	Yes	No	No	No	No	No	No
Sniff 37/38/39	Yes	No	No	No	No	No	No
Existing Conn.	No	Yes	No	No	No	No	Yes

Comparison to Commercial Sniffers

	Sniffle	Ellisys Bluetooth Tracker Pro	Frontline BPA LE	Frontline Sodera LE WB
Cost	$40	Over $10k	$5000	$10000
Open Source	Yes	No	No	No
Data Length Extension	Yes	Yes	Yes	Yes
BT5 PHY	Yes	Yes	No	Yes
BT5 CSA #2	Yes	Yes	No	Yes
BT5 Ext. Adv.	Yes	Yes	No	Yes
BT5 Per. Adv.	No	Yes	No	Yes
Sniff 37/38/39	Yes (hop)	Yes (full SDR)	Yes (simultaneous)	Yes (full SDR)

Where to Get Sniffle

- https://github.com/nccgroup/Sniffle
- GPLv3 licensed
- Installation and usage instructions are in the README
- Prebuilt firmware binaries available for those who don’t want to set up an embedded ARM GCC toolchain
- Also check out nOBEX, my tool for testing HFP and OBEX based profiles on Bluetooth Classic
  - https://github.com/nccgroup/nOBEX

Live Demo

Questions?

nccgroup