Perytons

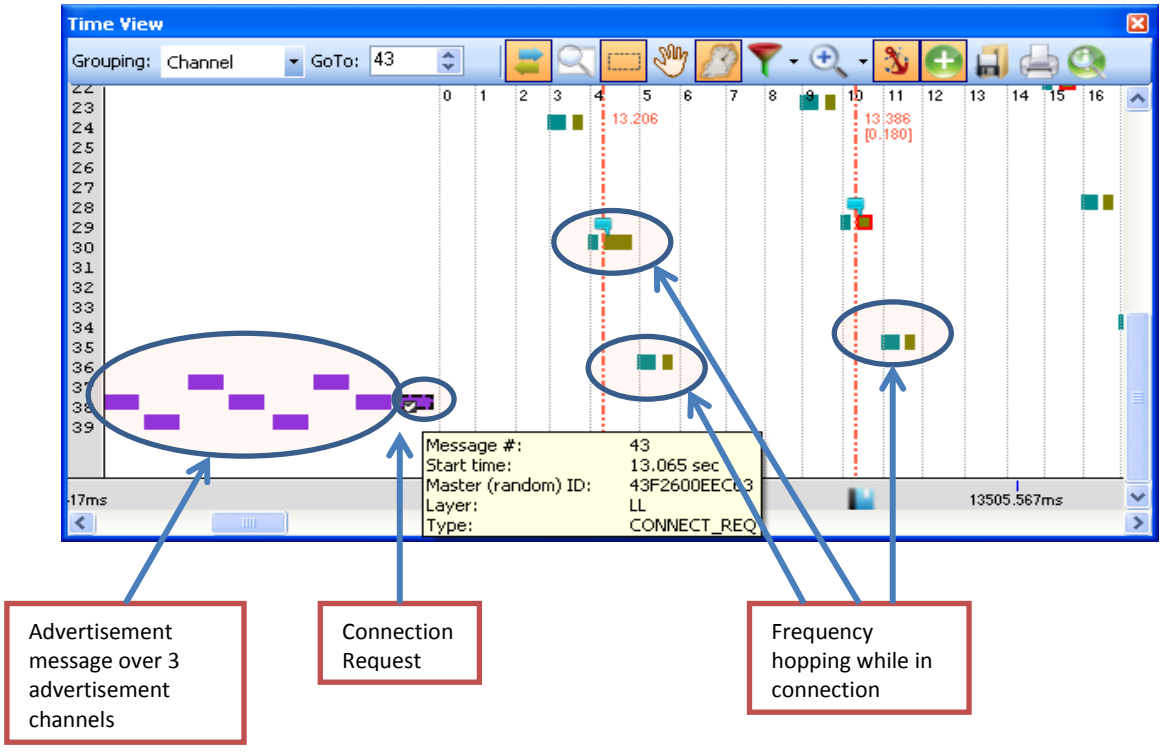
Single vs. Multi dongle capture of Bluetooth Low Energy Traffic

Background

Bluetooth Low Energy (also known as Bluetooth Smart, Bluetooth 4.0 or just BLE) uses 40 channels within the 2.4GHz band. 3 of these channels (numbered 37, 38 and 39) are defined as advertisement channels.

When a device (usually the Slave) wishes to set up a connection, it starts transmitting messages over the 3 advertisement channels (usually one after the other).

The other party (usually the Master) listens to the advertisement channels. Once it received the advertisement message sent by the initiating device, it replies with a Connection Request message. The Connection Request message defines the frequency hopping and other parameters of the connection. When receiving it, the initiating party starts frequency hopping sequence that matches the responder device parameters. The frequency hopping is done over the remaining 37 channels (numbered 0 to
36).



Sniffing a BLE network with a single receiver

In order to sniff a BLE network (i.e. listening to the network without taking active part in the sessions neither as Master or Slave), the sniffer must receive the Connect Request message,

extract the hopping parameters from it and then follow the network frequency hopping sequence, while receiving the messages transfferred over the connection.

Since the advertisement channel on which the Connection Request message is sent is chosen randomly out of the 3 channels, a single channel sniffer has a 1/3 (p = 33.33..%) probability to catch this message and be able to follow the connection.

In some setups (mainly during R&D phases in the lab), the user may control the responding party (Master) settings and force it to transmit the Connection Request on a specific advertisement channel. Then the sniffing receiver can be set to this channel, increasing the chances of successful connection detection to 100% (pending RF packet loss issues).

If this is not the case, the user may have to repeat the connection process several times until it will be detected by the analyzer.

The following table shows the probability of intercepting the connection with a single receiver:

Attempt # (n)	Probability for success ($P = 1 – (1 – p)^n$)
1	33.3%
2	55.6%
3	70.4%
4	80.2%
5	86.8%
6	91.2%
7	94.1%
8	96.1%
9	97.4%
10	98.3%

Sniffing to BLE network with multiple receivers

An alternative (and potentially better) solution is to have 3 dongles connected to the sniffer as front-ends. Each of the dongles will be set to capture messages sent on a different advertisement channel (37, 38 and 39 respectively).
Since the BLE session is initiated on one of these 3 channels, one of the three dongles will receive the Connection Request (with a 100% probability, pending RF packet loss issues) and follow the connection on the first attempt.

If, while the first connection is being captured, another connection is being set up, there is a 66.67..% chance that one of the two remaining dongles will receive it.

The following table shows the probability of intercepting a BLE connection with 3 USB dongles

Attempt #	Probability for success		
	1st connection	2nd connection ($P = 1 - p^n$)	3rd connection ($P = 1 - (1 - p)^n$)
1	100%	66.7%	33.3%
2	100%	88.9%	55.6%
3	100%	96.3%	70.4%
4	100%	98.8%	80.0%
5	100%	99.6%	86.8%
6	100%	99.9%	91.2%
7	100%	100%	94.1%
8	100%	100%	96.1%
9	100%	100%	97.4%
10	100%	100%	98.3%

Summary

Using Peryton-Smart with a single BLE USB dongle is good for users who can configure their Master device to transmit the Connection Request message on a known, predefined, advertisement channel, or for users that are willing to have a known trade-of between cost and the time needed when repeating the connection attempts in order to be able to analyze it.

Using Peryton-Smart3 is useful for users that would like a 100% chance to analyze each of the connections they have, or would like to be able to analyze more than one connection (up to 3) simultaneously.

Note: When a BLE session ends, the front-end receiving it is free again and gets' back to listening to the advertisement channel it was initially set to, allowing for additional BLE session to be received and sniffed in both the Peryton-Smart and Peryton-Smart3 models.