Capturing Bluetooth, The Right Way

Debugging Complex Topologies

Sniffer Overview

We are often asked what we mean by “wideband” or “whole-band” sniffing, the capture methodology used by all of our Bluetooth analyzer products. This Ellisys Expert Note explains at a high level how Ellisys Bluetooth analyzers capture Bluetooth traffic using this technique, an approach pioneered by Ellisys. The wideband technique can be described simplistically as the ability to capture all Bluetooth channels (BR/EDR and Bluetooth LE) both asynchronously and concurrently. This approach eliminates the many drawbacks of synchronous channel (hopping) sniffing approaches.

Hopping Sniffers

Before we introduced wideband sniffing to Bluetooth developers, capturing Bluetooth traffic was difficult, due to its advanced communication techniques, such as frequency hopping, whitening, privacy, and encryption. For security reasons, Bluetooth was actually designed to be difficult to sniff.

A Bluetooth radio uses from 40 (low energy) to 79 (classic) channels pseudo-randomly, according to a hopping sequence defined at the piconet’s connection time. This makes sniffing Bluetooth a challenge and greatly affects the ability to analyze, characterize, and troubleshoot.

Prior to our introduction of the wideband approach, the hopping sniffer was the most common sniffing method and was used by all sniffers introduced on the market from Bluetooth’s inception.

A hopping sniffer tries to actively synchronize on a specific hopping sequence, and captures the packets only after a successful synchronization. This kind of sniffer has several inherent limitations, making it more difficult to use, less reliable, and usable only in a limited set of scenarios.

As depicted in **Figure 1**, this sniffing method involved **listening to just one of the available channels at any given time.** For example, as Bluetooth devices use a different channel every 625µs, this sniffing method needed to know precisely when and where to listen in order to capture the packets from a given piconet.

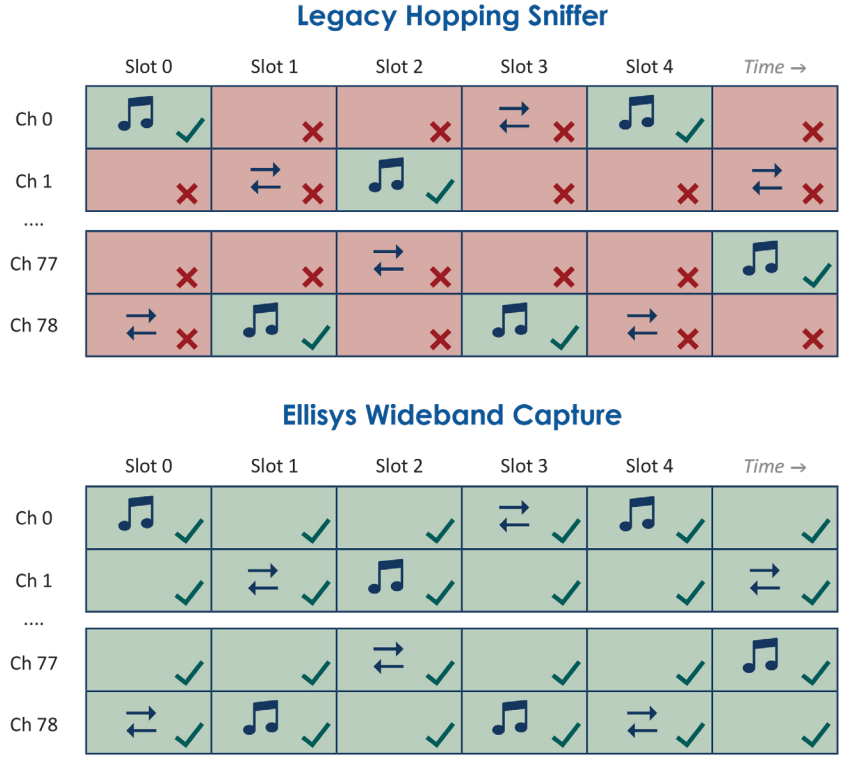

Figure 1 Legacy Hopping vs. Wideband.

As the hopping sniffing method can be implemented with a standard radio chip and specific firmware, it acts similarly to a standard Bluetooth device. It follows the hopping sequence of the selected piconet, and captures the packets in each slot; however, before even being able to capture any packets, it requires synchronization to the piconet of interest. The hopping sniffer managed this synchronization just as any device would - it actively paged the master of the piconet by sending ID packets.

HELPFUL HINT: A hopping sniffer tries to actively synchronize on a specific hopping sequence and captures the packets only after a successful synchronization. The wideband capture approach is as simple as it is powerful: instead of listening to just a few channels, the sniffer captures all channels concurrently.

When the master saw these packets, it transmitted an FHS packet in response. An FHS packet contains the information required to sync to the master and to follow its hopping sequence. From this point, and only from this point, the hopping sniffer can receive packets from this piconet. While this worked, this sniffing approach was quite limited as compared to wideband sniffing.

Wideband Sniffers

Of course, as you've figured out by now, a more interesting and practical way to sniff Bluetooth is to listen to all Bluetooth channels concurrently, using wideband concurrent channel sniffing. Instead of trying to follow a hopping sequence, such a sniffer will **listen to all channels**, and as soon as any packet is transmitted on any channel, it will be captured. This way, the sniffer hardware doesn't have to worry anymore about piconets and it can just **capture any traffic, statelessly, without any configuration.** All intelligence compilations, and these are both numerous and exceedingly complex, are then managed by fast and sophisticated software routines.

Refer to **Figure 2**, again using our Instant Piconet feature, where the image represents packets involving several piconets captured by an Ellisys wideband sniffer.

Such sophistication cannot be achieved with standard Bluetooth radio chips. From scratch, Ellisys engineers designed a **proprietary wideband radio**, including a test equipment grade RF front-end, concurrent-channel digital radio, and baseband.

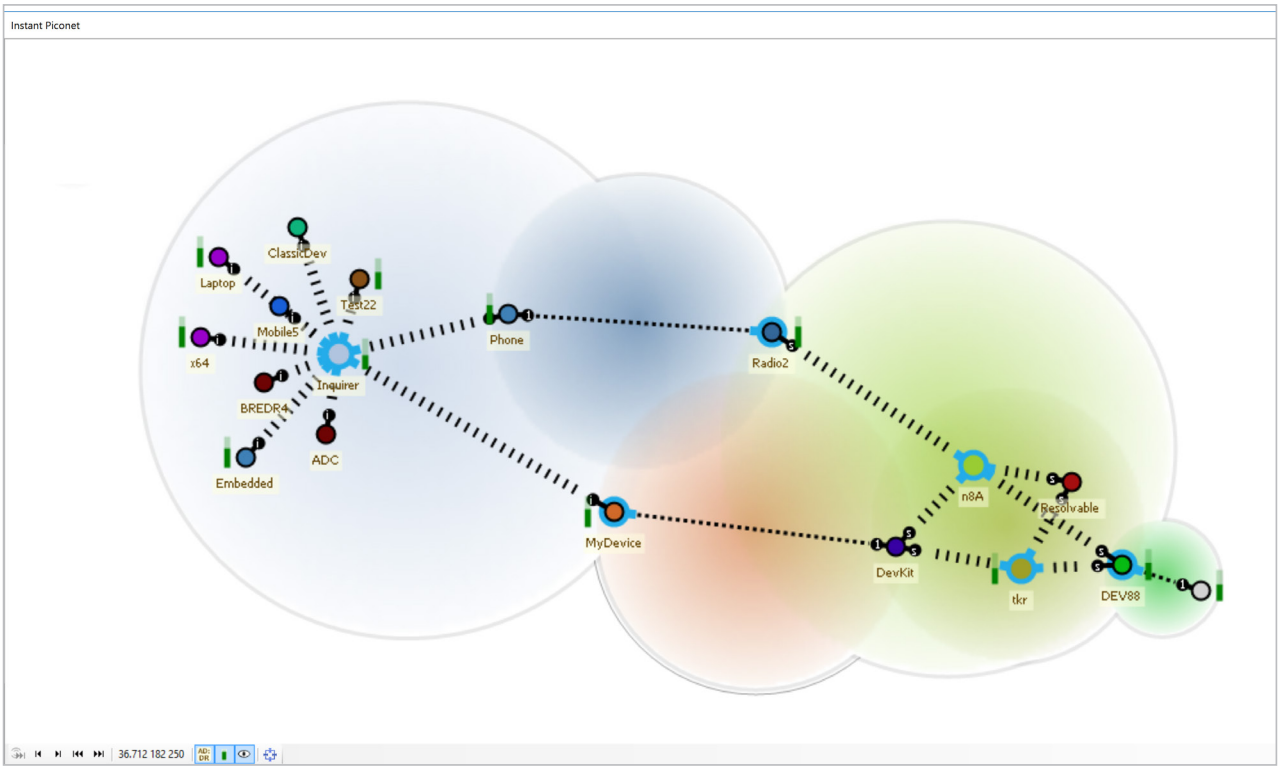

Figure 2 Instant Piconet Feature.

HELPFUL HINT: The Ellisys wideband sniffer will listen passively to all nearby Bluetooth piconets, scatternets, and other topologies, such as mesh, without any required configuration and without being intrusive.

Advantages of Wideband Sniffers

Using this approach is quite significant as it makes the Ellisys analyzers particularly **future-proof.** The Bluetooth technology is evolving in many directions and at an amazing pace. New paging techniques, baseband improvements, security enhancements, added protocols & profiles, and other new features can be accommodated with software updates alone, without changing anything in the hardware. This gives the hardware a longer life and translates to savings and convenience for the customer.

Another great advantage of wideband sniffing is that capturing **asynchronous traffic** is no longer an issue, see **Figure 3**.

Paging and inquiries can be captured flawlessly. This capture method is intrinsically insensitive to role switches, adaptive frequency hopping, paging schemes, etc. Capturing marginal traffic is also not an issue: **even if a packet is transmitted before, at the limit, or after the time slot, it will still be captured.**

And with its sub-symbol 125ns timing precision, the wideband approach provides maximum fidelity. Its super-precise, temperature-stabilized internal oscillator makes it the perfect reference when measurements have to be made between various devices.

This approach also opened up new possibilities when capturing encrypted connections. As the Ellisys wideband sniffer does not need to interpret Bluetooth traffic, it can also capture encrypted traffic and decrypt it immediately, or afterwards, in post-processing.

This allows for automatic determination of PIN-codes, capture of SSP Debug Mode devices, and capture of SSP pairings, followed by decryption of 100% of the traffic by simply providing the link key, which is not possible with other sniffing techniques.

HELPFUL HINT: The Ellisys analysis software automatically extracts any link key exchanged over HCI and uses it to decrypt the wireless traffic, all without any user interaction.

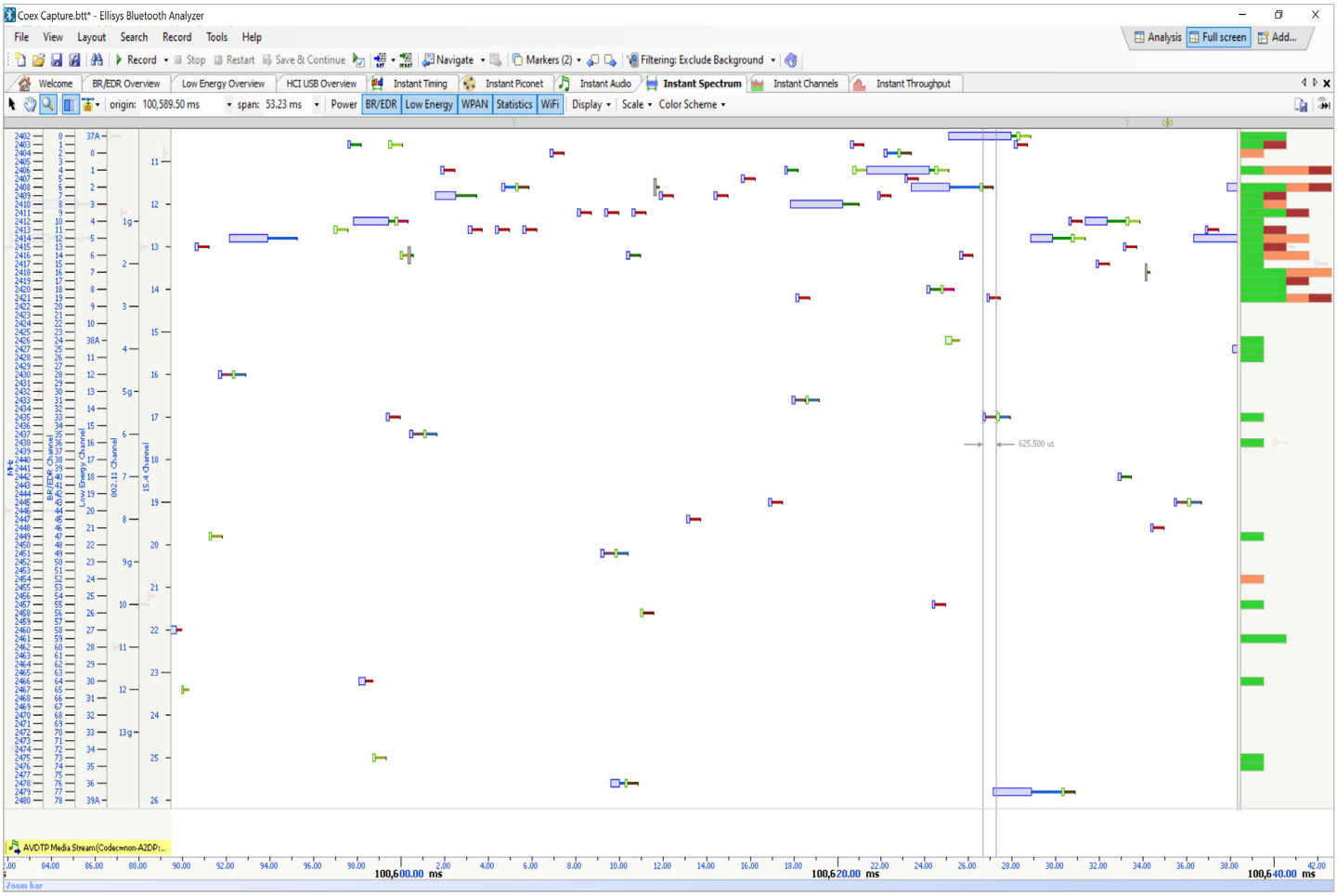

Figure 3 Instant Spectrum Feature.

Last but not least, this sniffer method enables capture of not just a single piconet, but **all piconets and scatternets in the neighborhood.** Debugging complex topologies is becoming more and more important as use cases have been steadily evolving from simple point-to-point connections to multi-profile, complex topologies, such as Bluetooth mesh.

Conclusion

Wideband sniffing changes everything, enabling Bluetooth debugging and interoperability testing that wasn't previously possible. Wideband sniffing provides a much more elegant approach, allowing the user to capture everything immediately and then hone in on any potential issues using the powerful filtering of the popular Ellisys analyzer software application.

Visit ellisys.com or email support@ellisys.com for more information.

Other Interesting Reading

- EEN_BT03 - Your First Wideband Capture
- EEN_BT06 - Bluetooth Security - Truths and Fictions
- EEN_BT07 - Secure Simple Pairing Explained

More Ellisys Expert Notes available at:
www.ellisys.com/technology/expert_notes.php

Feedback

Feedback on our Expert Notes is always appreciated. To provide comments or critiques of any kind on this paper, please feel free to contact us at expert@ellisys.com

Sales Contact:

USA: +1.866.724.9185
Asia: +852 2272 2626
Europe: +41 22 777 77 89

sales@ellisys.com

www.ellisys.com

Connect with us.