Better Analysis

Optimal Placement of your Analyzer

Capturing Bluetooth Traffic Flawlessly

Introduction

Capturing Bluetooth traffic with a wideband sniffer is as easy as clicking a button: just turn on your analyzer, start capturing and your traffic is displayed right away. With any wireless technology, some care must be taken to ensure that the analyzer is placed in an ideal position in order to robustly capture the traffic. This Expert Note will help to ensure that you get a flawless capture the first time by providing a few key best practices.

Position Setup

Preferably, the analyzer should be positioned in between the devices you would like captured, being mindful that the devices are not too close to the analyzer's antenna (as a signal that is too strong is not ideal). The ideal distance is about 1 meter (~40 inches) between the analyzer and each device as shown in **Figure 1.**

You will want to avoid placing the devices close to each other, and the analyzer far away (as shown in **Figure 2**). In this situation, the devices may reduce transmission power to a minimum, and the analyzer will receive a very small signal, which is increasingly subject to interferences.

Figure 1 Analyzer Positioning Set-up

Figure 2 Worst Possible Set-up

Case Involving a Bluetooth Vanguard™ with Capture Diversity™

Placement of your devices relative to the analyzer is a bit different with the Ellisys Bluetooth Vanguard analyzer. This analyzer uses an Ellisys innovation called "Capture Diversity" (as show in **Figure 3**.) This technique involves a co-operational replication of the Ellisys wideband capture engine intended to allow for increased spatial capture volume and reduced packet error rates.

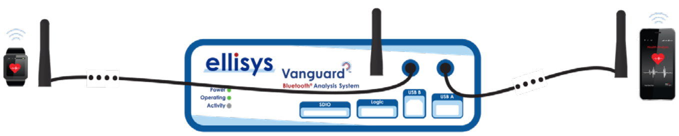

Figure 3 Capture Diversity.

Both antennas can be:

1. Angularly displaced on the analyzer unit <u>to diversify the physical characteristics</u> of the reception.
2. Externally cabled and placed at optimal locations to <u>improve the spatial volume</u> of the reception.
3. Placed nearer specific devices under test to *reduce packet error rate*.

Primarily, items 1 and 3 above are approaches that can be used to improve capture quality.

As additional background, Bluetooth packets can be degraded and missed by both Bluetooth test equipment and Bluetooth devices due to antenna positioning, signal strength issues, or RF interferences such as Wi-Fi and a variety of consumer electronics operating in the same band as Bluetooth. Certain packet exchanges are critical to Bluetooth connection sequences, encryption processes, and applications, and if missed can cause serious issues with communications between devices or characterizations provided by test and analysis equipment.

Capture Diversity involves smart software algorithms (developed by Ellisys engineers) that are applied to the dual capture channels, and when combined with spatial and angular flexibilities provided by this technique, can significantly improve the capture process and user experience.

Antenna Radiation Patterns

Having a basic understanding of your device's Bluetooth antenna radiation pattern is important. This often misunderstood concept can lead to poor reception, and it is difficult to detect as it is usually counter-intuitive.

In a few words, an antenna will not transmit power equally in all directions and, most of the time, little or no power will be transmitted into blind spots. For example, a typical mobile phone will transmit nicely in front and behind its screen; however, on each of its sides, it likely will transmit a poor signal.

If you place the mobile phone flat on a table, it will typically provide poor transmission quality, see Positioning Examples section. The receiving device will get a small signal, so it will ask the mobile phone to increase its power level, making the situation even worse, because the power transmitted into these blind spots is not only attenuated, but also distorted. The devices will manage to see each other and will likely be capable of communicating, but at a higher retransmission rate.

Capturing such traffic flawlessly is no longer possible as the analyzer cannot ask for retransmission, resulting in a poor quality trace. The analyzer can easily characterize retransmissions and other metrics – see below discussion on the Instant Channels feature.

Instant Channels Feature

The Instant Channels feature provides visual and statistical analyses on various per-channel transmission characteristics, including packet retransmissions, header errors, and payload errors. The user can use this feature to very quickly ascertain the quality of communications either in the aggregate, or between specific devices (when a device filter is set). This information can be useful in understanding where in the Bluetooth spectrum devices are communicating and the spectral areas (channels) they are avoiding, generally due to external interferences.

> HELPFUL HINT: Set a device filter to be sure the Instant Channels is characterizing just the devices that are of interest to you.

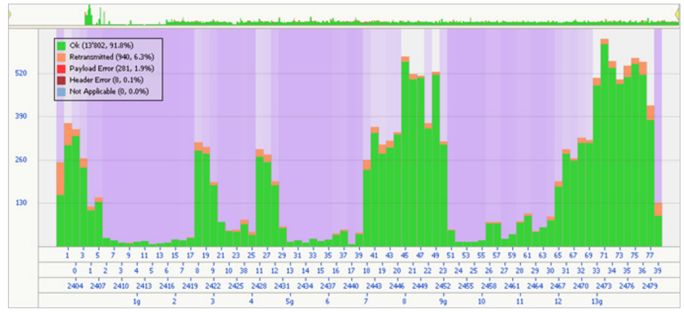

Figure 4 Instant Channel Features

This information is provided for the duration of an entire capture and can be configured to characterize all devices in the vicinity or specific devices.

In **Figure 4**, the Navigation Bar (horizontal bar across the top of the window) does not show any "window" selections, i.e., the entire capture is being characterized. The device filter (not displayed) is set to show only the devices of interest (in this case, a computer and an audio headset).

> HELPFUL HINT: Remove the OK packets with a right-click to improve the relative visibility of retransmissions, packet errors, and header errors.

Looking at the legend, we see that overall, the connection exhibits a retransmission rate of 6.3%. Payload errors and header errors are fairly small, **indicating that the analyzer is likely in a good position relative to the devices under test**. Considering the very busy (and strong) spectrum environment (see **Figure 3**), an "OK" packet rate of 91.8% as shown could be considered optimal. Note the prevalence of the magenta coloring across most of the channels. These indications characterize channel mapping or Adaptive Frequency Hopping (AFH).

Looking at the same capture in **Figure 5w,** but with a modified UI layout to add the Instant Spectrum view side-by-side with the Instant Channels view, we can see at a glance that the RF environment is quite busy. We can see that in the **Instant Channels** view, the user has selected a small window of 31.75 seconds (which can be panned left and right).

Looking at the Wi-Fi scale on the Instant Channels view, we can see that much of the avoidance is centered around strong emitters on Wi-Fi channels 1,6, 10, and 11. This is also apparent in the Instant Spectrum view.

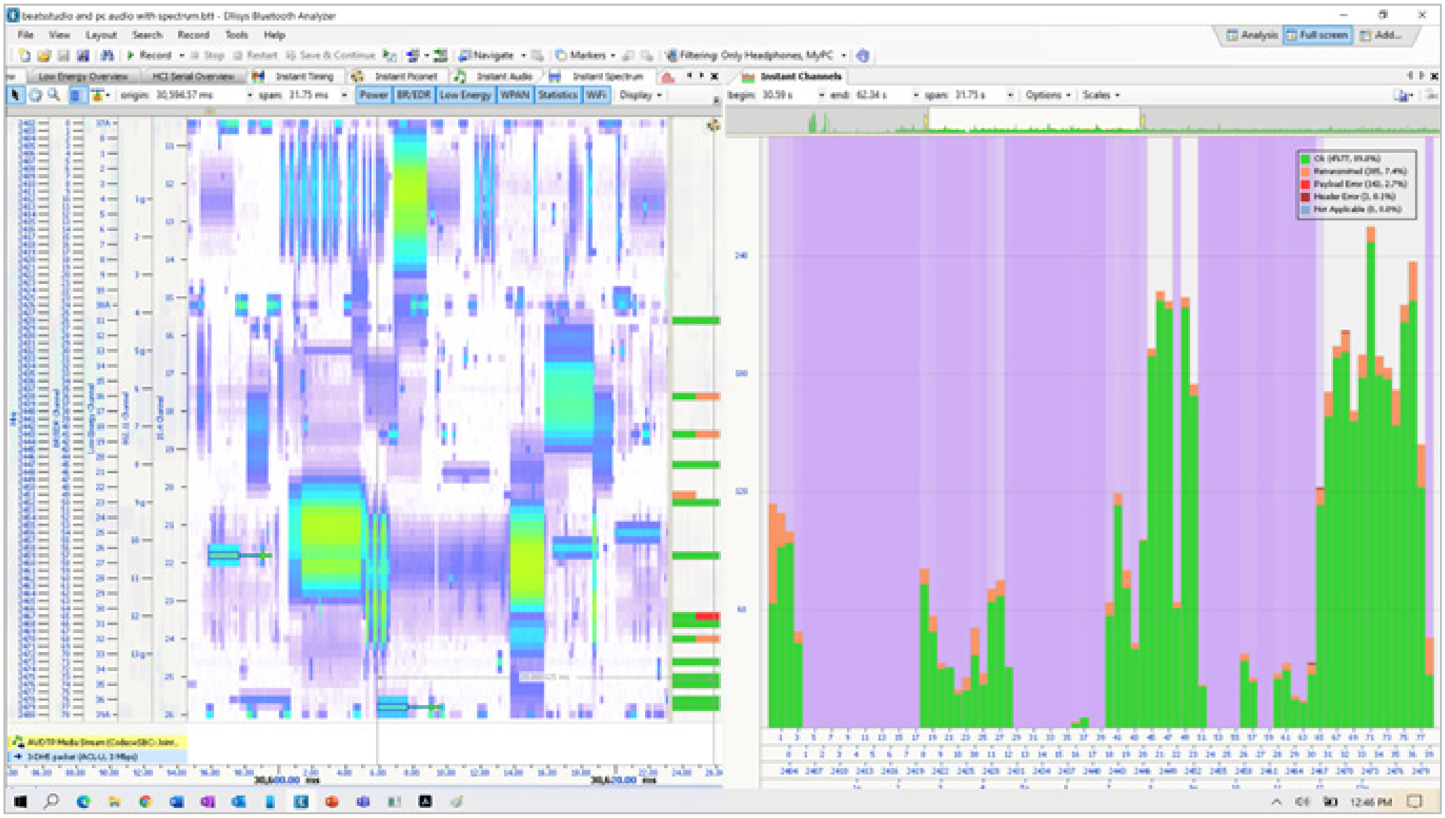

Figure 5 Instant Channel Features with Modified UI

HELPFUL HINT: The Instant Channels view, like all other features on the analyzer operates "live" during the capture. With your devices connected and communicating, you can vary the position of the devices, the relative location of the analyzer, or if you are using a Vanguard analyzer, experiment with angular displacement of the antennas and/or cabling of the antennas to your devices under test to "dial in" optimal physical placements/settings. Alternatively, make such physical adjustments on captures of similar length and connections of similar characteristics (e.g., data transfers) and then stop and save the captures before comparing results.

Other various electromagnetic sources that generate RF noise can also cause interference (e.g., microwaves, electric motors, security cameras, etc.)

So, even in a very busy RF environment, this Bluetooth connection is performing well, the devices are quite active in avoiding channels on which they find competing RF energy, and the analyzer is capturing packets optimally.

For more details about radiation patterns and antenna types, please review Expert Note, EEN_BT_05 on "Understanding Antenna Radiation Patterns."

Avoiding Interference

Interference can also cause issues while capturing Bluetooth traffic and it is not always intuitive in determining the source of the interference. For example, you have your analyzer next to your notebook on the table, with your devices on the left and right of the notebook, although this placement wouldn't appear to cause interference, it will because the Wi-Fi antennas are usually mounted along the edge of notebook screens.

Having the analyzer too close to the notebook screen with Wi-Fi turned on can cause an interference problem, resulting in the Wi-Fi transmitting a very strong signal into the analyzer's antenna. Therefore, positioning the Bluetooth devices further away from the Wi-Fi antenna source will ensure less disturbance within the frequency area. Additionally, notebook screens are also very good wireless shields, so it is good practice to avoid placing a screen in between your devices and the analyzer.

Positioning Examples

The following illustrations show examples of ideal positioning as well as positions to avoid. Please note that these drawings are conceptual examples and may not be correct with all such device models. Some mobile phones may be designed to work perfectly when lying flat on a table, while others may have awful performance in the same situation.

Mobile Phones Lying Flat: Two mobiles phones are lying flat on a table. If the chip antenna is not specifically designed to work this way, the Bluetooth radios on these mobile phones may have a hard time communicating.

Standing Mobile Phones: The most ideal antenna positioning for mobile phones is vertical rather than lying flat.

Vertical Dongle: The dongle is connected to the notebook with an adapter enabling the dongle to be operated vertically, thus positioning the antenna in its optimal position.

Wi-Fi Interferences from Laptop Screen: The analyzer is placed close to the laptop. This may appear just fine, however the laptop's Wi-Fi antenna, which is placed right at the edge of the screen, is smashing the lower intensity signal from the mobile phones .

Close Devices and Analyzer Far Away: If the two mobile phones are placed closely to each other, they may reduce their transmission power to the strict minimum. The analyzer, if placed far away, will receive a very weak signal, so it will be much more sensitive to interferences, increasing the capture's error rate.

Wireless Shield: A laptop screen can be used as a wireless shield. In this example, it will likely interfere with the two devices, reducing the transmission quality.

Horizontal Dongle: Most dongles use a chip antenna, which have good radiation patterns when vertical. When used horizontally, most dongles provide poor performance, which is counter-intuitive as dongles seem to be designed to work that way.

Fake Antenna Dongles: A warning about Bluetooth dongles. The model shown looks great with its movable antenna , allowing it to be positioned in the best possible way. Unfortunately, the antenna is a fake. It is just a piece of plastic with metal or wire to the radio chip, making it completely useless.

Analyzer Sensitivity

One last consideration to reach the optimal capture configuration is to verify that the analyzer's radio receives the signal in the usable range (not too strong and not too weak). The analyzer's radio has a fairly wide sensitivity range, but it is possible to tune the range further by adding attenuation or gain. This is configured in the **Record menu → Recording options → RF Gain**.

The default gain is 0 dB, meaning that there is no gain or attenuation. This works well in most cases, but some devices reduce their transmission power significantly to improve battery life, in which case some gain will help. There are three main indications in the software that help to optimize the RF Gain:

- When a packet is selected in the **Overview**, the **Details view** will contain a section called **Baseband Information** (for Bluetooth Classic BR/EDR) or **Link-Layer Information** (for Bluetooth low energy). Within the Sniffer Radio section, the RX Quality field will show the strength level. For best performance, adjust the sensitivity setting to place this field at Average or High.
- The **Instant Piconet** view also shows an indication of the RX strength (via the RSSI Indication) of the level next to each device. Preferably this level should be between the middle and the top of the indicator.
- Observe the Packet Error and Header Error indications in the **Instant Channels** view (discussed in the section above). The optimum sensitivity setting will produce the best possible error rates. Be sure to set a device filter so that you are characterizing the communications/devices of interest.

Conclusion

Capturing Bluetooth traffic flawlessly requires understanding a few good principles prior to recording the capture. This Expert Note emphasized the importance of adhering to the positioning of your devices relative to the analyzer, how antenna radiation patterns affect signal quality, how to reduce interference, and how to optimize the analyzer's sensitivity through attenuation and gain.

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

Other Interesting Reading

- EEN_BT02 - Analyzer Features Tour
- EEN_BT03 - Your First Wideband Capture
- EEN_BT05 - Understanding Antenna Radiation Patterns

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.