Air Sniffing: Positioning Devices

When capturing over the air packets, proper positioning of the ComProbe hardware and the Devices Under Test (DUTs) will result in the best possible captures and will mitigate sources of path loss and interference. The following procedures will help optimize the capture process especially if you are have problems obtaining reliable …captures.

Problems with indoor radio propagation

Even in free space, it is well understood that radio frequencies attenuate over distance. The free-space rule-of-thumb dictates that radio energy decreases in strength by 20 dB by each 10-to-1 increase in range. In the real-world, the effects of objects in an outdoor environment cause reflection, diffraction, and scattering resulting in greater signal losses. Indoors the situation can be worse. Reflections occur from walls and other large flat surfaces. Diffraction occurs from objects with sharp edges. Scattering is produced from objects with rough surfaces and from small objects. Also any object directly in the path of the radiation can present a hard or soft partition depending on the partition's material properties. Path losses from partitions are difficult to estimate.

Estimating indoor propagation loss

One estimate of indoor path loss, based on path loss data from a typical building, provides a $\frac{1}{range^{3.5}}$ power rule. At 2.4 GHz, the following relationship provides an approximate estimate of indoor path loss:

$$\textit{Indoor Path Loss (in dB)} = 40 + 35\textit{Log}_{10}\textit{(range, in meters)}$$

This approximation is expected to have a variance of 13 dB.

Mitigating path loss and interference

Bluetooth device design contributes to mitigating environmental effects on propagation through spread spectrum radio design, for example. However, careful planning of the testing environment can also contribute to reliable data capture process.

The first step to ensuring reliable air-sniffing data capture is to understand the RF characteristics of the Devices Under Test (DUTs). The *Bluetooth* Class, antenna types, and radiation patterns are all important factors that can affect the placement of the DUTs and the ComProbe analyzer. Radiation patterns are rarely spherical, so understanding your device's radiation patterns can greatly enhance successful data capture. Position devices to avoid radiation attenuation by the surroundings.

This step is optional: Consider conductive testing to establish a baseline capture. Conductive testing isolates the DUTs and analyzer from environmental effects.

The next step is to ensure that the testing environment is as clutter-free as possible.

- Line-of-sight obstructions should be eliminated between the ComProbe hardware and the DUTs because they cause a reduction in signal strength. Obstructions include, but are not limited to: water bottles, coffee cups, computers, computer screens, computer speakers, and books. A clear, unobstructed line-of-sight is preferred for DUT and ComProbe hardware positioning.
- If using an analyzer connected to a computer, position the computer on an adjacent table or surface away from the analyzer and DUTs, taking advantage of the cables' length. If this is not possible, position the computer behind the analyzer as far away as possible. If using the ComProbe FTS4BT, which is a dongle, either use an extension USB cable or position the computer such that the dongle is positioned towards the DUTs.
- The preferred placement is positioning the DUTs and the ComProbe hardware at the points of an equilateral triangle in the same horizontal plane, i.e. placed on the same table or work surface. The sides of the triangle should be between 1 and 2 meters for Bluetooth transmitter classes 1 and 2. The distance for transmitter class 3 should be 1/2 meter.

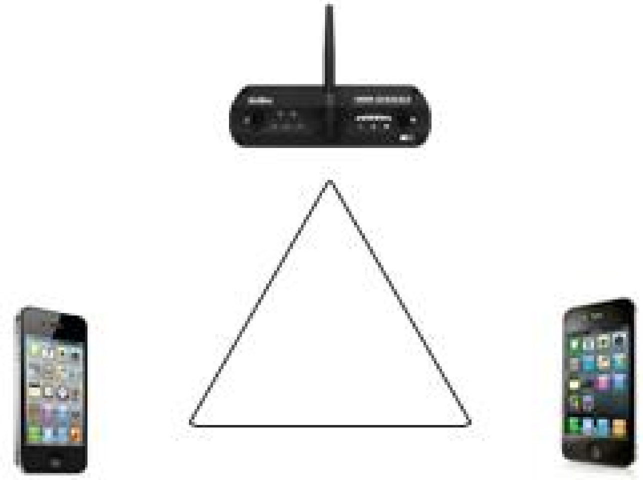

Figure 1 - Devices Equally Spaced in the Same Horizontal Plane

Finally, eliminate other RF sources.

- Wi-Fi interference should be minimized or eliminated. *Bluetooth* shares the same 2.4 GHz frequency bands as Wi-Fi technology. Wi-Fi interference can cause loss of packets and poor captures. In a laboratory or testing environment do not place the DUTs and ComProbe hardware in close proximity with Wi-Fi transmitting sources such as laptops or routers. Turning off Wi-Fi on the computer running the ComProbe software is recommended.

Positioning for wideband capture

Frontline's Wideband Bluetooth Protocol Analyzer, Sodera, can capture from multiple devices, which requires a different approach to position the DUTs and the analyzer. When testing more than two devices arrange the DUTs on the perimeter of a circle 1-2 meters in diameter for Bluetooth transmitter Class 1 and 2 devices. For transmitter Class 3 DUTs, the circle should be 1/2 meter in diameter. Equally space the DUTs on the perimeter. Place the Sodera in the center of the circle. If not using the Sodera Excursion mode, connect the computer and place it outside the circle as far away from the DUTs as possible.

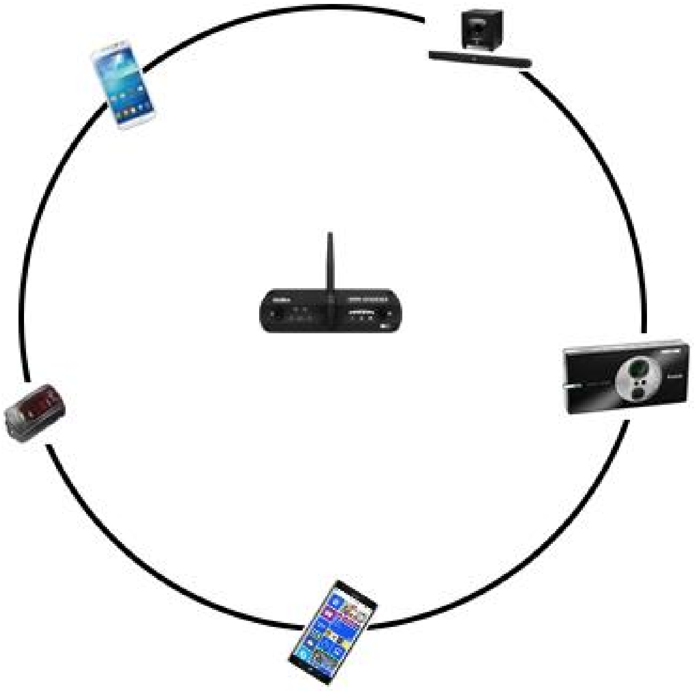

Figure 2 - Wideband Capture: Devices Equally Spaced in the Same Horizontal Plane

Positioning for audio capture

The Bluetooth Audio Expert System provides analysis of audio streams and can assist in identifying problems with capture methods including positioning and environment because it will point out missing frames. For hands-free profile data captures both DUTs send and receive data. Therefore, position the devices following the equilateral triangle arrangement as mentioned above.

However, in A2DP data capture scenario, the equilateral positioning of devices is not optimum because, normally, only one device is sending data to the other. It is recommended that the ComProbe hardware be positioned closer to the device receiving data so that ComProbe better mimics the receiving DUT. Position the DUTs 1 -2 meters apart for Class 1 and 2 transmitters, and 1/2 meter apart for Class 3 transmitters.

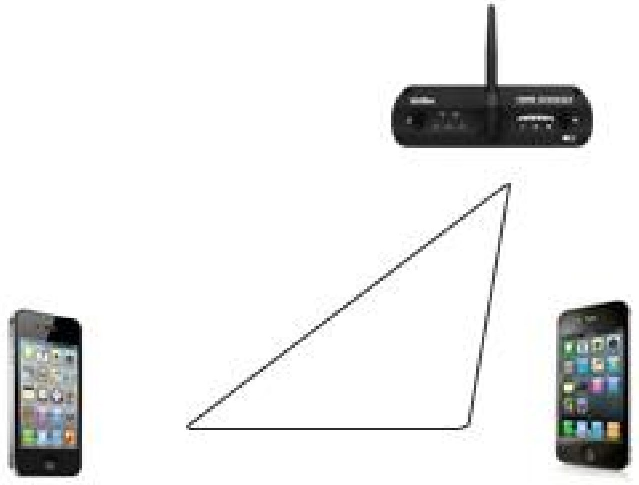

Figure 3 - For Audio A2DP, Position Closer to SINK DUT

Poor Placement

A poor test configuration for the analyzer is placing the DUTs very close to each other and the analyzer far away. The DUTs, being in close proximity to each other, reduce their transmission power and thus make it hard for the analyzer to hear the conversation. If the analyzer is far away from DUTs, there are chances that the analyzer may miss those frames, which could lead to failure in decryption of the data.

Obstacles in close proximity to or in between the analyzer and the DUTs can interfere and cause reduction in signal strength or interference. Even small objects can cause signal scattering.

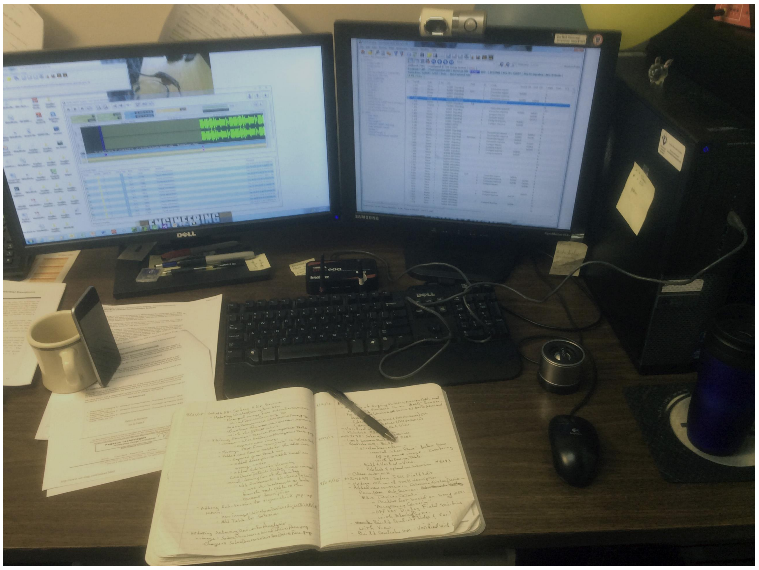

Figure 4 - Example: Poor Capture Environment