Lab 07 – BLE Introduction

Author: Raymond Ng
Course Number/Section: IS 3413-006
Date: October 25, 2022

INTRODUCTION

The purpose of this lab was to allow the user to experiment with Bluetooth connectivity and describe basic Bluetooth Low Energy (BLE) terminology and components. Moreover, the user will use Windows Bluetooth Virtual Sniffer and Wireshark to scan for BLE devices.

PROCESS

Step 1:

The most notable difference between Bluetooth and BLE is that BLE requires less power in applications that do not require large amounts of data and can run on battery power much longer than Bluetooth classic. Bluetooth classic can handle a lot of data, but quickly consumes battery life. Bluetooth classic costs more than BLE. [1]

BLE operates in the 2.4Ghz ISM Band, same spectrum as Bluetooth classic and Wi-Fi. [2]

BLE typically finds its use in home automation applications (i.e. smart door locks, smart appliance, smart lighting systems), fitness devices (i.e. wearables, trackers), indoor location technology (when GPS is not available), medical and personal health devices. [2]

In BLE, central devices (i.e. laptops, tablets, smart phones) are usually the more capable devices in terms of CPU power, memory, or battery capacity whereas the peripheral device (i.e. Bluetooth accessories) is much more resource constrained especially when it comes to battery capacity. BLUE is an asymmetric technology, meaning much of the heavy lifting and processing responsibility is put on the central device versus on the peripheral which actually allows the peripheral device to sleep for longer periods of time turn, consuming less power. Range limiting factors include surrounding environment, antennae design, and orientation of the devices that are talking to each other. [2]

BLE range is approximately 150ft (50m) within line of sight distance; however, with obstacles in between range decreases significantly, approximately 30ft (10m). Bluetooth 5.0 can range up to 2600ft (800m) line of sight distance. [2]

Step 2:

Using Windows Bluetooth Virtual Sniffer, coupled with Wireshark, I was able to capture one of my devices connected via Bluetooth, my Logitech mouse. I did not see any other Bluetooth devices that were not my own. Looking at *Figure 1*, the only protocol that was captured was Attribute (ATT) protocol. ATT is a protocol in the BLE protocol stack. It defines how data is represented in the BLE server database and the methods by which that data can be read or written [3]. From RFwireless-world.com, I learned that the BLE protocol stack architecture consists of two parts, controller and host (Figure 2). Both are interfaced using Host to Controller Interface (HCI). Examining the host, I learned about the following protocols in the BLE stack:

Generic Access Profile (GAP): The layer that defines how to discover and connect services to a Bluetooth device, also involved with security.

General Attribute Profile (GATT): Service protocol that defines the attributes and services of a BLE device; when the profile is setup by GAP the attributes are assigned to a particular service.

Security Manger Protocol (SMP): Used for pairing, or the method of listening to a BLE device and communicating with the other device.

Logical Link and Adaptation (L2CAP): A protocol that works int eh background with GAP for the purpose of defining a set of rules for BLE device discovery and links to other low energy devices

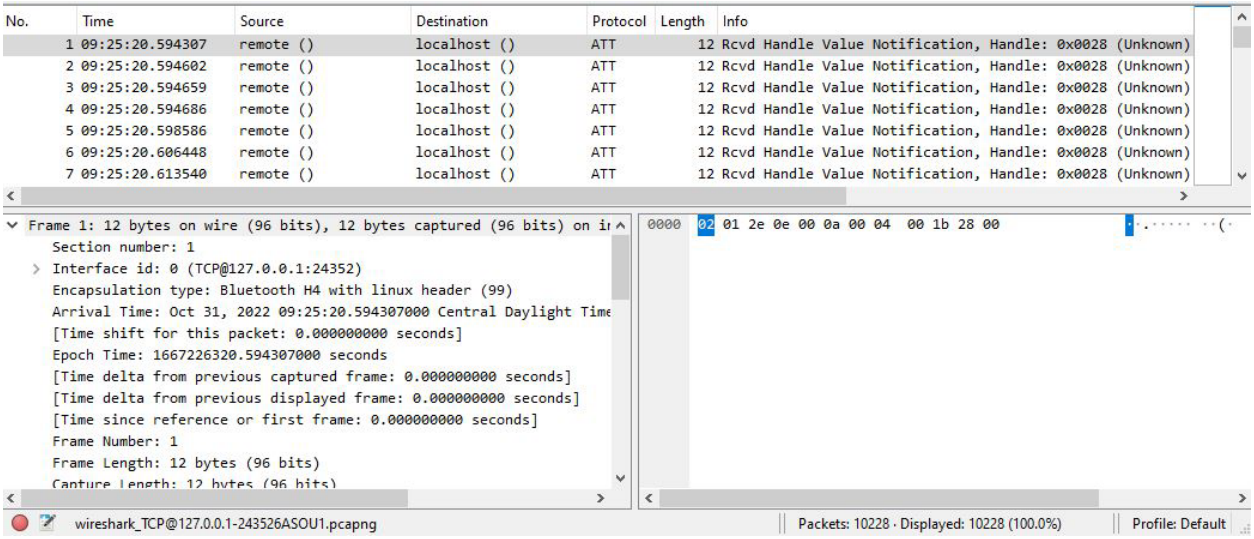

Figure 1: BTVS Wireshark capture

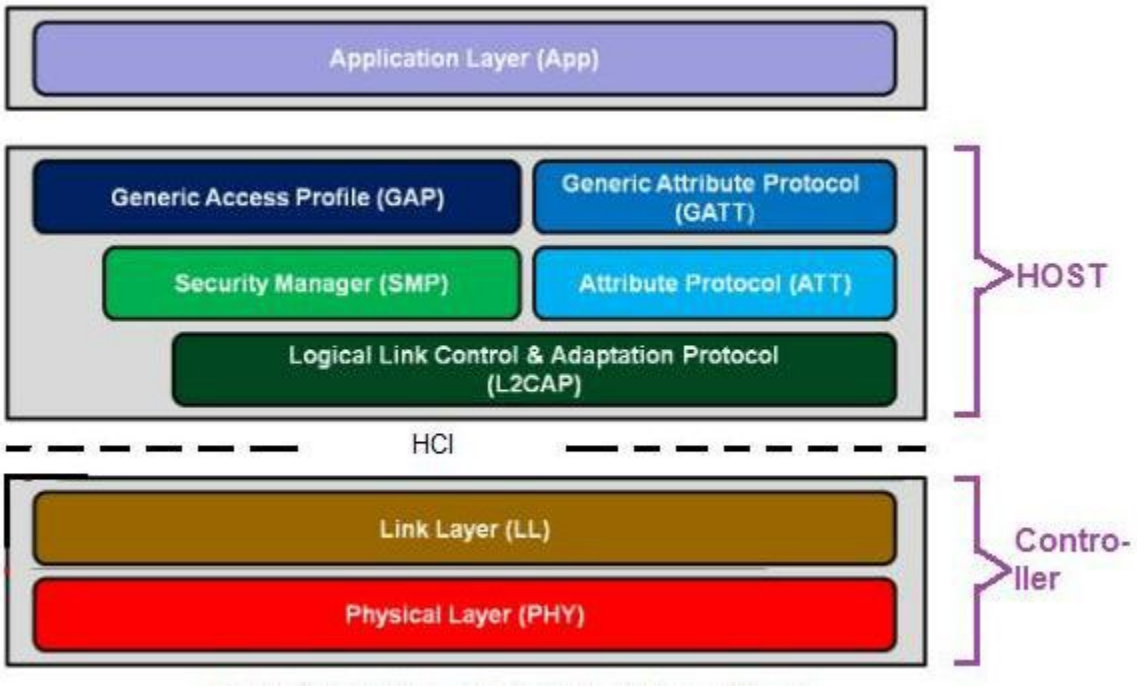

Figure 2: BLE Protocol Stack, graphic sourced from rfwireless-world.com

LIMITATIONS/CONCLUSION

There were minimal limitations to this lab. Everything was executed in a live environment. The biggest takeaway from this lab was learning about the BLE stack and the different protocols/attributes associated with it.

REFERENCES

[1] GeeksForGeeks [Online]. "Bluetooth vs Bluetooth Low Energy", May 18, 2022. Available: https://www.geeksforgeeks.org/bluetooth-vs-bluetooth-low-energy/ [Accessed: 27-Oct-2022]

[2] Bluetooth SIG Inc [Online]. "Intro to Bluetooth Low Energy", 2022. Available: https://www.bluetooth.com/bluetooth-resources/intro-to-bluetooth-low-energy/ [Accessed: 27-Oct-2022]

[3] Car Rental Gateway [Online]. "Attribute Protocol (ATT)", 2022. Available: https://www.carrental gateway.com/glossary/attribute-protocol/ [Accessed: 31-Oct-2022]

[4] RF Wireless World [Online]. "BLE Protocol Stack | BLE System Architecture", 2012. Available: https://www.rfwireless-world.com/Terminology/BLE-Protocol-Stack-Architecture.html [Accessed: 31-Oct-2022]

[5] Symmetry Electronics [Online}. "A Bluetooth Low Energy Application: Defining the BLE Stack", December 9, 2014. Available: https://www.symmetryelectronics.com/blog/a-bluetooth-low-energy-application-defining-the-ble-stack/ [Accessed: 31-Oct-2022]

COLLABORATION

The entirety of this lab was executed independently by the author. No additional collaboration to report.