Chad Ballay

**Week 5**

**Explain how RF wireless transmissions work for wireless networks. Note some common RF bands and their uses.**

RF transmissions typically are governed by measuring the behavior of a couple of properties of the signal. You can establish a standard around the shifting if the amplitude, frequency and even just the duration of a signal or absence of a signal. (Modulation, n.d.) DSSS,MIMO-OFDM, and OOK are the primary standards for 802.11 series of standards. (IEEE\_802.11 Protocol, n.d.)

For most of our RF wireless transmissions the bands that matter the most would lie in the ISM(Industrial, Scientific, Medical) bands. 900 mhz, 2.4 ghz, and 5ghz specifically for WiFi. RFID/NFC on 13.56 mhz is probably the next biggest band of importance. (ISM Band, n.d.)

**Describe wireless network interface cards (WNICs) as the means by which a wireless device communicates with a wireless network. Give examples of the different types of interfaces available for WNICs, such as PCI or USB.**

WNIC’s exist on the layer 1 and layer 2 of the OSI model. Drivers allow for device and operating system to communicate to either other wireless nodes (adhoc mode) or access points(infrastructure mode). (Wireless Network interface Controllers, n.d.) Like any device we have a range of implementations. From onboard chips that are built into the computer’s motherboard, to internal cards installed into expansion slots like PCI, on to external hardware that is connected through universal buses like USB, Bluetooth, etc…. At this point this hardware has become commonplace and ubiquitous. Especially as the age of IoT is pushing more and more the boundaries on ubiquitous connectivity.

**Research and explain what types of electronic devices or other obstacles can cause interference. Some objects will be obvious sources of interference, but others such as fluorescent lights and hearing aid devices, may be less obvious.**

Ironically, my own body as a source of interference has been yet another reason to lose weight. After years of not protecting my hearing, I’ve had to begin wearing hearing aids. The specific ones I have also act as Bluetooth receivers from my phone. A rather annoying aspect of that connection is that when I put my phone in my pants pocket only the hearing aid on the same side of my body will be able to maintain a consistent connection the cross body hearing aid just isn’t able to power through all my layers….

Another personal experience with interference came early in my career at Walmart. We would develop dead zones in and around the Electronics section during the initial rollout of the Nintendo Wii. The instore demo units for the original Wii were unique in that it was one of the first demo units to try and show customers how the motion tracking controllers worked. To help ensure that it worked these demo units had some custom circuitry in them. Unfortunately, it was a very finicky bit of hardware and in some stores our employee paging system would just intermittently not work. It took weeks to narrow it down. The visualization tools from 13-ish years ago just weren’t capable for finding this and it really was a case of identifying where in the store the pagers failed, then powering off likely suspects one by one until we at least figured out what was generating the interference.

**Explain the difference between WPA and WPA2 in personal security and enterprise security modes. Include how 802.1x or a preshared key is used for security.**

This table is a handy overview of the differences between WPA and WPA2 and with either of them in personal or enterprise mode. (Randy Weaver)

A screenshot of a cell phone

Description automatically generated

In personal mode a preshared key is used. This is some string of text that has to be known by every user of the network. For a small network this is manageable for coordination. (Temporal Key Integrity Protocol, n.d.)This doesn’t scale at all which partly led to the adoption of the 802.1x authentication standard. This shifts the authentication component to using a RADIUS server. A much more complicated setup but certainly more secure. (IEEE\_802.1x, n.d.)

# Bibliography

*IEEE\_802.11 Protocol*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/IEEE\_802.11#Protocol

*IEEE\_802.1x*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/IEEE\_802.1X

*ISM Band*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/ISM\_band

*Modulation*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Modulation#Digital\_modulation\_methods

Randy Weaver, D. W. (n.d.). *Guide to Network Defense and Countermeasures.*

*Temporal Key Integrity Protocol*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Temporal\_Key\_Integrity\_Protocol

*Wireless Network interface Controllers*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Wireless\_network\_interface\_controller