**Report on Wireless Network Analysis**

End of Semester Assignment for ET4004 TCP/IP Networking

**Name:** Nathaniel Teskey

**Student ID:** 20247672

*University of Limerick*

**May 2022**

**Introduction**

When creating an Internet of Things (IoT) application, one of the most important things that must be considered is the choice of wireless protocol. There are many established wireless protocols out there such as Bluetooth, Bluetooth LE, ZigBee, Z-Wave, 6LoWPan, Thread, NFC, RFID, LoRaWAN and 5G. Each of them have their own specific benefits and drawbacks. In the first part of this report I will give an in-depth comparison of three wireless protocols that interest me the most. They are Bluetooth LE, Z-Wave and ZigBee. To make it easier to digest I will then summarise my findings in a table for easy comparisons at a glance.

In the second part of this report I will step into the shoes of a network engineer on a site using wireless networks such as Wi-Fi, 5G and Bluetooth. I will outline the procedure of carrying out a wireless site survey while discussing how I would assess a wireless network in a building. I will also highlight the tools I would use to benchmark the network along with the software required to carryout the audit. I will describe the process of simulating data on the network and explain how I would test for interference along with highlighting the values that should be measured to test for interference. I will then make a recommendation on equipment to buy within different budgets.

In the final part of this report I will calculate the throughput of a WIFI network with certain characteristics and different amounts of users. I will then justify my answers by explaining throughput and how network resources/ bandwidth are distributed among users.

**PART 1 (Section 1)**

There are many wireless communication protocols but the three that interest me the most, aside from Wi-Fi are Bluetooth LE, Z-Wave and ZigBee. I chose these three protocols as they are most commonly used in IoT devices in the home. It amazes me that they can co-exist in harmony with each other, however I have always wondered if one protocol can replace all three.

Bluetooth Low Energy (LE) is the power-conserving variant of Bluetooth. It was specifically designed for use in IoT devices thanks to its very minimal energy requirements. This is handy as form factor is key for an IoT device and most of the time it is the battery that takes up the majority of the space, however with Bluetooth LE the battery size can be greatly reduced allowing for a more seamless experience. Bluetooth LE which was also marketed as Bluetooth Smart, was introduced originally in 2004 but massive improvements have been made, especially in the last number of years making this a practical protocol for IoT devices. Some new Bluetooth LE IoT devices can easily operate for one or two years on a 20-cent coin sized battery. Bluetooth LE is a key player in the IoT market as its low implementation cost, long battery life and ease of deployment make it a really attractive choice for short-range wireless data communication. [[1]](#endnote-1) Bluetooth LE also has the ability to use mesh profiles to communication with other Bluetooth LE devices since the release of Bluetooth 5.0. This means that one smartphone has the ability to turn off all of the lights in an entire building, because each Bluetooth LE device will pass the message on to the next device. Bluetooth LE uses frequency hopping to mitigate interference. Bluetooth LE benefits from a sleep mode, this means that it can be asleep until it needs to connect and transmit data and after that it can go back to sleep again to conserve battery. The best part of this is that the user doesn’t even know![[2]](#endnote-2)

Z-Wave and ZigBee are protocols mainly used in IoT devices in the office or home. Both protocols allow for the connected devices to have excellent battery life and they are mainly used in meshed high-density point to multipoint or multipoint to multipoint networks. This is where ZigBee and Z-Wave have a slightly upper hand as they have been using meshing well for a number of years whereas Bluetooth LE has just adopted it since the recent release of Bluetooth 5.0. Meshing lets you increase network range with every additional device that you add because its radio can act as a transceiver. However it isn’t easy to do well on low power networks as every device has to be ready to wake up at the same time and immediately start routing lots of packets to the required destinations. ZigBee mostly uses the 2.4GHz frequencies so it shares similarities to Wi-Fi and Bluetooth in this regard. Zigbee is freely available with many chips available and uses flexible protocols too. You can even make your own profiles! ZigBee is very cheap but in order to connect devices to the internet you need a gateway. Z-Wave is a more proprietary protocol as it is designed for use in the home however to make Z-Wave compatible devices you must purchase the silicon chips from a single supplier. In a way Z-Wave have made their own ecosystem like Apple, in order to maximise profit as you have to use their proprietary chips. Z-Wave operates on the 900 MHz frequency so it offers a little bit more range than Bluetooth LE and ZigBee as sub-1GHz frequencies penetrate concrete easier.[[3]](#endnote-3) The main benefit to going with Z-Wave apart from its slightly increased real world range is that you are joining 100+ companies that provide cross compatible support, however as I said previously this is also a drawback as it can be more expensive than Bluetooth LE and ZigBee, as Z-Wave only use a single chip supplier.

**PART 1 (Section 2)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Variable** | **Bluetooth LE** | **Z-Wave** | **ZigBee** |
| Range | 60 – 100 meters | 30 – 65 meters | 10 – 20 meters |
| Cost | Very Low Cost | High Cost | Low Cost |
| Latency | 6ms | 1000ms | 100ms |
| Energy Consumption | Very Low  ~1mA / 1uA when asleep | Low  ~2.5mA | Low  ~40mA |
| Data Rate | 2 Mbit/s | 40 kb/s | 250 kb/s |
| Frequency | 2.4 GHz | 908 MHz | 2.4 GHz |
| Security | 128-bit AES with counter mode CBC-MAC[[4]](#endnote-4) | 128-bit AES and ECDH key exchange[[5]](#endnote-5) | 128-bit AES |

**PART 2 (Section 1)**

The first thing I would do when asked to carry out a wireless site survey is, I will identify the wireless needs. This means figuring out what speed and bandwidth the client wants, how many devices will be accessing the network at once, how much transmission power will the wireless radios have and which Wi-Fi standard will I be using. Ideally all of this should be discussed with the client at the start of the survey to gain an insight into the needs of the business.

The next step in carrying out the wireless survey is to obtain a floorplan. The blueprints are ideal but any map of the layout of the building will do. Here I will need to note the locations of dense walls or other elements that can be hard / impossible for wireless signal to penetrate. Examples of these are elevator shafts, stairwells or garage doors. There are apps available that can import blueprints or site layouts onto an iPad or android tablet so you don’t have to deal with paper flapping around.

Now I am ready to perform a walkthrough of the entire building. The plans of the building tell some of the story but not the whole story so for that reason a walkthrough is key. Here I will take note of metal walls or equipment racks that can block or weaken the wireless signal.

While I am walking around, I am making notes of where the current wireless access points are and where new ones can be mounted. Ideal places for mounting of these access points are on the ceiling or high up on wall if the ceiling is not a viable option.

Next it is time to categorise all of the rooms and areas on the site. I will ask myself questions such as, “Which rooms need the highest bandwidth?” In my head I already know that offices, meeting rooms and canteens are key. It is also important to ask yourself where else you need good coverage. I will mark out the server rooms and other utility rooms that may contain wireless equipment on the floor plan also. It is important not to neglect these rooms. It is also important to be very strategic when planning out the layout of the network as this is key to a high-performance network. In many cases a well-planned network can also be cheaper for the customer as it is more efficient.

After taking all of this into account I will then begin to decide where to place the wireless access points. I will check the coverage range on the access points and allow for some overlap between neighbouring access points. This guarantees a seamless experience throughout the site. This also allows for dynamic load balancing and network resiliency, so if one hotspot stops working then another will be close by that can carry the users of the broken access point until it is restored. It might not have the best performance but it will be good enough to support the operation of the devices connected to it until their main access point has been fixed.

Next its time to run a wireless site survey. The main options here are installing survey software on your laptop or buying a specialized tool to carry out the survey, this tool is typically a modified tablet. Next walk I will walk around the site again and place my wireless access points in each location and then approach them with the survey tool to gather data on the network. The software records the SSID of the access point it is connected to and also the transmission rate, signal strength and connection quality. Some wireless survey tools can even generate a real time coverage map on your survey device, it does this after completing a site walk and loading all of the data into its software.

Now after consulting with the software it is time to refine the location of the access points. At this point I will play around with the locations of the access points until I find their optimum location. It is key to experiment at this stage a it will pay off when the network is up and running properly.[[6]](#endnote-6)

Wireless site survey tools are needed to benchmark the network. Wireshark is one of the most widespread tools for network benchmarking. Here the network engineer can make notes of the state of the network in different places on the site and save them too as Wireshark files. This is a very useful tool when benchmarking networks. Other tools that are frequently used are TCPdump, Netpref, MGEN, Kismet Spectrum Tools and GNU Radio toolkit. Wireshark can also be used for auditing Bluetooth networks and it also has capabilities that allow it to perform some 5g network tests too such as a trace visualizer. SolarWinds is a company widely known for its top of the line network monitoring systems, that can supply an all in one approach with a nice GUI. One of their most popular applications is the Network Performance Monitor that provides Wi-Fi heatmaps as mentioned previously, they help to better plan your network layout. It allows for custom heatmaps based on signal strength and it easily identifies dead zones. It adjusts to improve wireless coverage and it can locate all mobile devices connected to the Wi-Fi network provided it is within three meters from your network. These are really handy features for assessing a Wi-Fi network and the software starts at a price of about $3,000. An alternative to SolarWinds NPM could be Ekahau Heatmapper and Netspot, however these are not as good as SolarWinds NPM as they lack key features.[[7]](#endnote-7) To test the 5G services on the site a tool called RantCell could be used however this is more of a private use tool as it runs on an android phone, as 5G networks become more common we will see a rise in 5G network benchmarking tools.[[8]](#endnote-8)

To simulate the data on the network I would need to use a Network Simulation Tool. The tool that I am most familiar with is Cisco Packet Tracer. This allows to us to build simple or complex networks inside the Packet tracer and then we can simulate network scenarios and run tests without damaging the computer hardware. I believe it is a very useful tool, however if you aren’t a fan of Cisco packet tracer then GNS3 can be used. Another more basic network simulator, but still very useful is called PuTTY which allows for SSH, Telnet login and raw socket connection along with some more stuff.[[9]](#endnote-9)

To test for interference I would use heat mapping software to determine what access points were overlapping and then check the channels that they are on and change them to the least congested channels. Microwaves, cordless phones, poorly shielded cables and poorly wired satellite dishes can all causes network interference. Microwaves operate on the 2.4GHz network and so does the cordless phone. An easy way to carry out an interference test is by using a spectrum analyser to observe the entire radio frequency band to detect non 802.11 signals which may result in network interference.

**PART 2 (Section 2)**

If I was a network engineer with a very low budget of €1000, I would only be able to provide a basic level of service and might not get much work but for the sake of this question I will outline what I would recommend the client to buy anyway. For the €1000 budget I would instruct the customer to use TP-Link AV600 Powerline adapters. These adapters use the initial wiring in the walls to run the Wi-Fi signal along. It is similar to how fibre optic cable works in that is converts the signal to pulses on the line and then translates it back with the box on the other side in order to boost the signal. They cost about €50 a piece and one in each important room would really improve the signal around the building. At this price point wireless access points are out of range as they need to be installed and wired up to ethernet. This is a lot more hassle than simply plugging in the Powerlink adapters into the existing infrastructure within the walls of the building.

With a budget of €5000 I would be able to implement a good wireless infrastructure within the company. With this budget I would buy 20 access points which would cost me about €1500. Next, I would buy 3 305-meter ethernet cable rolls. This is necessary for wiring up the access points to the switches and routers in the networking room. I would wire all the access points from each floor into a switch each. So one switch for the top floor and one for the bottom floor. I would place all of these items on server racks which would aid with cooling. Then I would then have to connect the two switches to a router and the router would then be connected to a modem to give it internet access. The router costs about €1500 which brings the total to €3000 so far. Considering for the two switches they are about €500 a piece so that brings us up to €4000 and then the rolls of ethernet cable were €80 each and when that is multiplied by 3 it is €240. So we are currently sitting at €4240 of stuff and to make up the remainder we still have to pay for the server racks, modem and fans in the network room.

Finally, with a €30,000 budget I would designate a switch to every department in the company e.g. IT department, finance department, reception, HR etc. I would buy 5 rolls of Cat 6 ethernet cable giving me 2000 meters of cable for €400. The 5 switches would cost €2500 along with a router for each department to give each department its own group of IP addresses. They would then be connected to a modem and to the internet. I would have a wireless network all around the site using about 40 access points so every location is covered. The access points are costing me about €3000 now so my current total is €6000 plus the 5 routers which are €7500 it is now €13,500. Next, I would install a server room on site, which stored a backup of every piece of data on every computer. I would keep it in a firesafe on site in a different building in case of a fire. Everything would be backed up to metallic rolls and stored in a firesafe off site for 10 years before they are destroyed. The servers would cost me about €10,000 along with the infrastructure such as metal fire safes and server racks along with cooling we would be close to out €30,000 budget. This is in my opinion the perfect network, as it is perfectly organised with everything backed up too.[[10]](#endnote-10)

**PART 3 (Section 1)**

The internet link has a download rate of 10 Mb/ s and the wireless network has a bandwidth or peak rate of 54 Mb / s. The fastest throughput possible is 10 Mb/s as that is the maximum download rate of the internet link. The throughput is capped at that speed even though the wireless network

supports a peak rate of 54 Mb/s.

**PART 3 (Section 2)**

If there was 10 users connected to the Wi-Fi network then the maximum throughput for each user would be 54 Mb /s divided by 10 which is 5.4 Mb/s. So the maximum throughput with 10 users could only be 5.4 Mb/s as that is the weakest link on the network and it is slower than the 10 Mb /s download rate. The network “bandwidth” gets divided by 10 when 10 users join the network so it is not as efficient as when only 1 user is active on the network at a time.

**Conclusion**

In conclusion I feel like I addressed all the questions that needed to be answered in this report. I believe my answers were effective and I believe that all of my findings will be beneficial to other students, especially myself as a refresher to look back upon this work. I feel like I successfully dissected the three wireless protocols that I picked to dissect. They were Bluetooth Low Energy, ZigBee and Z-Wave. These were all kind of related in a way as they are often used in IoT devices in the office and the home. I explained how they all had their own benefits and drawbacks. If I was to choose one to rule them all I would choose Bluetooth LE as it has really come on leaps and bounds in its most recent form and it can now compete with ZigBee and Z-Wave when it comes to meshing, which is a key feature for IoT devices. I spoke about the prices and features of each and laid out my results in a table as required. I then had to assume that I was a network engineer and discuss how I would carry out a Wireless Site Survey. I spoke about how I would assess wireless networks in a building such as Bluetooth, 5G and Wi-Fi. I obviously went into the most detail about Wi-Fi as it is much more common. I then had to explain how I would test for interference and what I would measure to test for interference. In this case a spectrum analyser must be used which is able to analyse the entire radio frequency band. I then outlined how I would distribute funds in a company and how I would designate money to upgrading of the network equipment. In the final part of the report I outlined what I knew about throughput and preformed some calculations. I feel like this report was tricky to write at times but the information that I learned through research and reading will stick with me throughout my career.

**References**

1. https://www.techtarget.com/iotagenda/definition/Bluetooth-Low-Energy-Bluetooth-LE [↑](#endnote-ref-1)
2. https://learn.adafruit.com/introduction-to-bluetooth-low-energy [↑](#endnote-ref-2)
3. https://learn.adafruit.com/introduction-to-bluetooth-low-energy [↑](#endnote-ref-3)
4. https://www.arrow.com/en/research-and-events/articles/bluetooth-low-energy-technology-is-ideal-for-iot [↑](#endnote-ref-4)
5. https://aeotec.com/z-wave-home-automation/ [↑](#endnote-ref-5)
6. https://www.turn-keytechnologies.com/blog/article/the-ultimate-wireless-site-survey-checklist/ [↑](#endnote-ref-6)
7. https://www.netadmintools.com/best-wifi-heat-map-software#wbounce-modal [↑](#endnote-ref-7)
8. https://rantcell.com/ [↑](#endnote-ref-8)
9. <https://www.imedita.com/blog/top-10-list-of-network-simulation-tools/>) [↑](#endnote-ref-9)
10. https://www.corporateshields.com/small-business-network-setup-checklist/ [↑](#endnote-ref-10)