



**Prifysgol Cymru**  
Y Drindod Dewi Sant  
**University of Wales**  
Trinity Saint David

# **Simulating Environmental IoT Sensor Networks for Wood Moisture**

by

Ethan Ridd

Supervisor: Carlene Campbell

Second Marker: Kapilan Radhakrishnan

Project submitted as part of the requirements for the  
award of MSc Computer Networks and Security

September 2019

## DECLARATION

I, Ethan Ridd declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

**Signed:** 

**Date:** 29/09/2019

## FORM OF CONSENT

I Ethan Ridd hereby consent that my Project, submitted in candidature for the MSc Computer Networks and Security degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

**Signed:** 

**Date:** 29/09/2019

## Table of Contents

|                                                                |    |
|----------------------------------------------------------------|----|
| <b>Abstract</b> .....                                          | 6  |
| <b>Chapter 1 – Introduction</b> .....                          | 7  |
| 1.1 Background.....                                            | 7  |
| 1.2 Aim .....                                                  | 8  |
| 1.3 Objectives .....                                           | 8  |
| 1.4 Project Structure.....                                     | 8  |
| <b>Chapter 2 – Literature Review</b> .....                     | 10 |
| 2.1 Introduction.....                                          | 10 |
| 2.2 What is the Internet of Things?.....                       | 10 |
| 2.3 IoT Protocols.....                                         | 12 |
| 2.4 Wireless Sensor Networks .....                             | 16 |
| 2.6 Simulating a Network .....                                 | 20 |
| 2.8 Related Works.....                                         | 22 |
| 2.9 Conclusion .....                                           | 24 |
| <b>Chapter 3 – Research Methodology</b> .....                  | 26 |
| 3.1 Introduction.....                                          | 26 |
| 3.2 Research Philosophy .....                                  | 26 |
| 3.3 Research Approach .....                                    | 26 |
| 3.4 Data Collection .....                                      | 27 |
| 3.5 Risks.....                                                 | 27 |
| 3.6 Conclusion .....                                           | 28 |
| <b>Chapter 4 – Design and Implementation</b> .....             | 29 |
| 4.1 Introduction.....                                          | 29 |
| 4.2 Problem Formulation .....                                  | 29 |
| 4.3 Design .....                                               | 29 |
| 4.4 Implementation .....                                       | 31 |
| 4.5 Conclusion .....                                           | 41 |
| <b>Chapter 5 – Data Analysis and Results discussions</b> ..... | 43 |
| 5.1 Introduction.....                                          | 43 |
| 5.2 IoT Results .....                                          | 43 |
| 5.3 WLAN Results.....                                          | 46 |
| 5.4 IoT and WLAN Comparison.....                               | 49 |
| 5.5 Result Discussions .....                                   | 51 |
| 5.6 Conclusion .....                                           | 52 |

|                                                          |    |
|----------------------------------------------------------|----|
| <b>Chapter 6 – Conclusions and Recommendations</b> ..... | 53 |
| <b>Chapter 7 – Reflections and Future Work</b> .....     | 55 |
| 7.1 Introductions .....                                  | 55 |
| 7.2 Reflections .....                                    | 55 |
| 7.3 Future Work.....                                     | 56 |
| References.....                                          | 58 |

## Table of Figures

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| Figure 1 - OFDM Frequency [14].....                                           | 13 |
| Figure 2 – Chart show the iteration of standard in 802.11 WLANs [15].....     | 13 |
| Figure 3 – Wireless Security Iterative Improvements[23].....                  | 15 |
| Figure 4 – Image showing ZigBee Topologies [48] .....                         | 18 |
| Figure 5 – Proposed Topology of Down to Earth Site.....                       | 30 |
| Figure 6 - Topology of IoT Network .....                                      | 32 |
| Figure 7 – General IoT Sensor Settings .....                                  | 33 |
| Figure 8 – IoT Sensor Network Settings.....                                   | 34 |
| Figure 9 – IoT Sensor Interface Settings.....                                 | 35 |
| Figure 10 – IoT Sensor Interface Settings Continued.....                      | 36 |
| Figure 11 – Topology of WLAN IoT Network.....                                 | 37 |
| Figure 12 – WLAN Sensor General Settings.....                                 | 38 |
| Figure 13 – WLAN Interface Settings .....                                     | 39 |
| Figure 14 – Simulation Noise Settings.....                                    | 40 |
| Figure 15 - Simulation Application Settings.....                              | 41 |
| Figure 16 – IoT Packet Loss showing simulations with and without noise.....   | 44 |
| Figure 17 - IoT Throughput showing simulations with and without noise.....    | 45 |
| Figure 18 - IoT Delay showing simulations with and without noise. ....        | 46 |
| Figure 19 – WLAN Packet loss showing simulations with and without noise. .... | 47 |
| Figure 20 - WLAN Throughput showing simulations with and without noise. ....  | 48 |
| Figure 21 - WLAN Delay showing simulations with and without noise. ....       | 49 |
| Figure 22 – Average per node packet loss of IoT and WLAN comparison.....      | 50 |
| Figure 23 - Average per node throughput of IoT and WLAN comparison .....      | 51 |
| Figure 24 - Average per node delay of IoT and WLAN comparison .....           | 51 |

**Abstract – The Internet of Things and Wireless Sensor networks have become a huge part of the networking space in recent years due to their ability to remote manage and gather data about many aspects of people lives. In this report the author designed a simulated network for the use of Down to Earth in measuring the wood moisture of newly constructed buildings. This report aimed to find the most suitable network for the site, considering performance and cost, WLAN and IoT WSN networks were simulated both with and without network interference. An in-depth analysis of the current literature surrounding the topics of IoT and WSN was performed and the research of others within the field critically reviewed. An experiment methodology was devised followed the positivist philosophy and deductive approach of the scientific method. The author used Netsim to simulate WLAN and IoT networks with a constant bit rate of data to understand how the networks would perform under this load of data and handle network interference. The range was considered to be a determining factor, so the network was simulated in accordance with the project manager of Down to Earths specification for the node placement. The data gathered from the simulations were irregular with some nodes especially on the IoT experiment showing that network interference improved performance. The author discussed this anomaly in the results and after seeking advice from other users it is most likely a bug within the program. Overall the results showed that the IoT has a massive increase in delay and packet loss with a decrease in throughput, whilst the WLAN showed the opposite. The author came to the assumption that the WLAN simulation showed the best results both with and without noise and this came to the conclusion that this would be the best network solution as it could also be a cost saving measure if the new network was integrated with the Wi-Fi already on site. A discussion on future work and reflections talked about in this report brought about the idea of simulating the nodes themselves and their functions such as data gathering and power draw as a possible avenue for continued work.**

## **Chapter 1 – Introduction**

### **1.1 Background**

With the rapid development of networking technology within the last 10 years the implementation of technologies such as the Internet of Thing (IoT) and Wireless Sensor Networks (WSN) have become vary widespread across the industry. IoT is a relative new technology that has rapidly become the forefront of many companies' future developments. IoT is the idea that numerous devices can be interconnected to share information and resources over a local network or even a wide area network. It has become a huge trend in recent years with numerous companies such as Philips and Nest creating devices for the commercial sector such as digital thermostats that can be altered from a mobile device or even lighting within homes or offices being controlled remotely through the use of devices such as Philips Hue technology. Wireless Sensor Network follows this trend but in a different direction instead of being able to control devices remotely, it follows the idea that a device can used to monitor or gather information from its surroundings using specialized protocols and Architectures. This has been popular in many areas of industry, such as the use in automation to monitor large industrial machines to measure metrics such as temperature, accuracy and service information of a machine such as a large automated lathe in engineers' facilities.

Down to Earth is an Eco-friendly company dedicated to exploring and teaching new methods of building that uses natural and environmentally friendly methods and materials. Recently they have developed a new site in south Wales with a building that is made primarily of Welsh Larch a native tree to Wales. The author and a few colleagues have been asked to implement a network that will monitor the wood moisture content of the structure to be used in further research by Down to Earth. The author will specifically focus on simulating the network to understand the best possible network for the building and gather performance metrics to support the recommendation of why the network should be built a particular way. This project could be used as a starting off point for a new area of development of IoT sensors that can be used on the construction site and in other eco-friendly projects. The author believes that the work being done within this report would allow for a more optimised and suitable network for the site and can allow for the actual network to be build from a steady bedrock.

## 1.2 Aim

The aim of this project is to gather an understanding of how a wireless sensor network designed for detecting wood moisture content using IoT sensors performs under the most optimal conditions.

## 1.3 Objectives

To achieve the aim of this project the author has created a set of achievable objectives to measure progression. They are as follows:

- I. Perform a comprehensive literature review into the numerous areas that this project touches upon, including IoT, Wireless Sensor and simulations.
- II. Develop an experiment methodology, that will be used to gather accurate result during experimentation
- III. Run the experiment in a simulation to gather a base mark of the best possible running condition and the network with noise generation.
- IV. Simulate other possible implementations for the network
- V. Make recommendations based on results of simulations.

## 1.4 Project Structure

The structure of this project is vital to ensuring that the aims and objective can be accomplished. This project will be split into numerous chapters to help illustrate the authors ideas and experiments, this will also help the author organise the ideas and thoughts in an understandable manner. The structure of the project is as follows:

- Chapter 1 – a basic introduction to the project, mainly highlight the overall aims and objectives of the project and what the author plans to achieve.
- Chapter 2 – A review of the current literature around the subjects of this projects and the numerous technologies that can be implemented throughout.
- Chapter 3 – An explanation of the way the author intends to conduct the research and experimentation whilst underlining an overall methodology for the project.
- Chapter 4 – An explanation of the network design in the simulation and in the real-life scenario, with appropriate justification of the design stating all

assumptions. This chapter will also review the areas of the implementation and testing and focus on areas where there might have been issues with the experiment.

- Chapter 5 – This chapter will involve the analysis of the data gathered and discuss the results. This will include a comparison of the simulation results from numerous technologies used and with noise
- Chapter 6 – Conclusions will be the focus of this chapter this will end the project by summarising everything learned from the project and make recommendation from the data gathered in the experimentation
- Chapter 7 – This final chapter will involve the author reflecting on the project and discuss area that could be improve if the project was to be repeated or expanded upon

## **Chapter 2 – Literature Review**

### **2.1 Introduction**

In this section of the report the author will outline the numerous aspects of IoT and WSNs whilst focusing on how the technologies work, the many protocols the technology uses and how they are implemented within many areas of industry. The author will also go through the current literature on simulations and their effectiveness in the use of modelling networks in optimal and suboptimal conditions. In the final section of this chapter the author will discuss the current literature of simulating and using Wireless Sensor Network to monitor environmental conditions and discuss how the current literature will affect the work being conducted within this project. The author will also review the literature in a critical manner and use the stated criticisms to improve or alter the project for a clearer and more conclusive report.

### **2.2 What is the Internet of Things?**

Internet of Things or IoT is the use of sensors and other devices connected over a network to gather data on numerous aspects of the environment and other machines. IoT is most popular in the use of monitoring energy efficiency, security, health and is even used in education[1]. IoT offers consumers the ability to access these sensors and devices remotely over the internet or locally through their own home network. IoT has widely been accepted by both consumers in the commercial sector and in the private sector with many companies offering heating solutions such as NEST which allows for the remote monitoring and control of heating systems within customers' homes which has increased energy saving of between 10-12% for its customers[2]. IoT has even begun to make a large impact on Automation within numerous industrial sectors around the world. With IoT becoming a major technological trend in recent years it is no surprise that security has become a major concern within the industry, with numerous devices gathering data on such a massive scale which has never been seen before it is vital that all data is protected.

### 2.2.1 Common Applications

IoT has become a very popular and has led to the development of numerous applications throughout the years, one such application is the development of smart cities. There is no clear definition of a smart city only the idea that a city can be improved for the community by the gathering of large amounts of data in real time through sensors and cameras[3]. This new technology allows for the monitoring and control of major city functions such as maintenance, this can be instrumental in ensuring the city runs efficiently through sensors that can detect when a public trash container is full requiring emptying or repairing city security cameras or streetlights[4]. Another area where smart cities can improve the running of a city is through public transport, this can potentially allow for accurate times of buses, trains or trams whilst also allowing users of the public transport to know of delays within the city. A third factor of a cities daily running that can be improved through implementation of a smart city is traffic control which allows for sensors to gather data on the areas of improvement of traffic flow and even regulate the frequency of traffic lights changing, which could potentially make the roads safer for pedestrians whilst maintaining optimal traffic flow[5].

Following the idea of smart cities, a smaller microscale version can be implemented within homes, this includes the controlling and gathering of data on key home facilities such as power usage, heating regulation and lighting. This can enable home owners to save money as reduce their carbon footprint as the smart home could automatically regulate the environment to suit the inhabitants needs through previously mentioned technology such as Nest or smart energy meters which can be acquired from the electricity service provider if they offer such technology[6]. Smart Agriculture is a similar technology following the trend of smart homes and smart cities. Smart farming is still relatively new in comparison to the other two applications of IoT previously mentioned but it is still nevertheless an area of great research. Development of such technology as automated feeding and watering for livestock through the use of microcontrollers, sensors such as humidity, gas and temperature alongside camera to notify the system when feed is low or when water needs to be supplied to the livestock[7]. Smart farms can also include automated irrigation and monitoring of crop growth with the use of moisture and humidity sensors to notify the network systems when to release water into the crops thus reducing water waste[8].

## 2.3 IoT Protocols

IoT has a wide range of protocols to facilitate connectivity, some of the protocols ensure low power consumption and reliability. Some IoT devices use common standards already available such as Bluetooth or Wi-Fi. For the purposes of this report the author is going to focus mainly on Wi-Fi and LoRa. The protocols help facilitate the communication and the transfer of data in a manner which allows devices to function with each other seamlessly. Some of the protocols allows for expansion of features and others allows for low power consumption and low latency.

### 2.3.1 Wi-Fi

Wi-Fi is an integral part of any network whether it be in the home or in the workplace this has led to the number of consumers that use Wi-Fi reaching an all-time high and many IoT device creators have used this already abundant technology to their advantage. In a report from the Internet Users Survey it is estimated that 88.6% of people use the internet in their home and is most likely through Wi-Fi[9].

Wi-Fi itself is defined by the Institute of Electronics and Electronic Engineers or IEEE. IEEE places Wi-Fi under the 802.11 standard[10], which itself has many sub standards each improving on the last. The 802.11 standard uses both the Media Access Control (MAC) and Physical (PHY) Layers of the OSI network model. The MAC layer is responsible for addressing of the network through MAC addresses and the multi-access support that Wireless Local Area Networks (WLAN) needs as numerous nodes can be connected at once, this layer also provides support for authentication, retransmitting of lost packets and the encryption of data being sent[11]. The PHY layer is responsible for the transmission rate (also known as speed) and transmission of data over the selected medium for the case of 802.11 it is radio frequencies, this includes the modulation of the bits in a binary signal to a radio frequency using sine waves and the demodulation of said sine waves back into a binary sequence[12].

802.11 wireless networks use a technology developed between 1960s -1970s called Orthogonal Frequency Division Multiplexing or OFDM. OFDM takes a single available wireless channel and separates it into multiple sub-channels that somewhat

overlap[Figure 1] and can all be used at the same time, this essentially allows for more channels for the signal to be transmitted without sacrificing pre-existing channels[13].

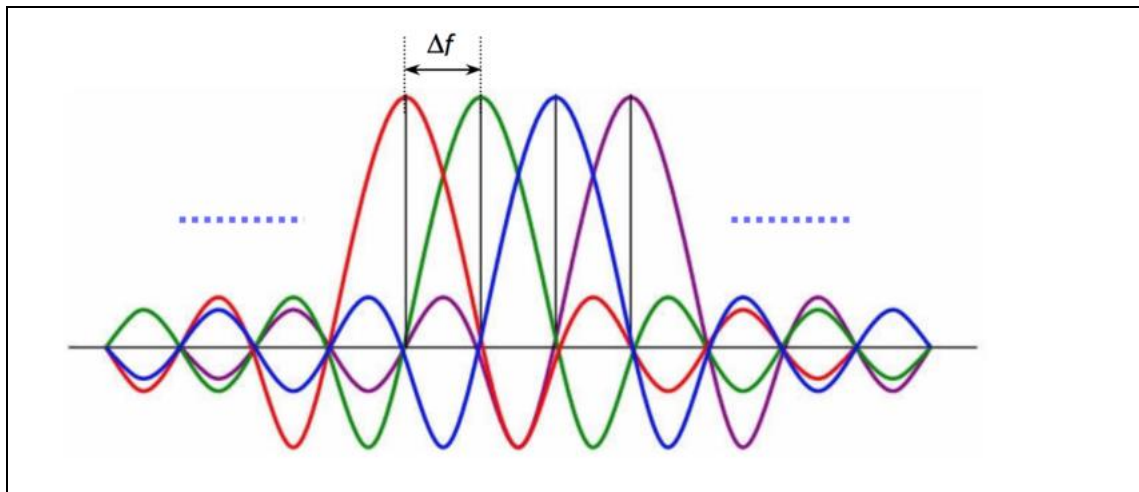


Figure 1 - OFDM Frequency [14]

As previously mentioned, 802.11 has numerous iterative sub standards this is best illustrated in figure 2. As can be seen below the iterations of the standard has led to massive improvement in both speed, and effective max range of the wireless signal. The most recent update coming in the form of Wi-Fi 6 (802.11ax) being made available to consumers they can expect almost a 187% increase in data rate at the same range over the previous 802.11af.

| IEEE Standard   | Year Adopted         | Frequency | Max. Data Rate                                | Max. Range            |
|-----------------|----------------------|-----------|-----------------------------------------------|-----------------------|
| 802.11a         | 1999                 | 5 GHz     | 54 Mbps                                       | 400 ft.               |
| 802.11b         | 1999                 | 2.4 GHz   | 11 Mbps                                       | 450 ft.               |
| 802.11g         | 2003                 | 2.4 GHz   | 54 Mbps                                       | 450 ft.               |
| 802.11n         | 2009                 | 2.4/5 GHz | 600 Mbps                                      | 825 ft.               |
| 802.11ac        | 2014                 | 5 GHz     | 1 Gbps                                        | 1,000 ft.             |
| 802.11ac Wave 2 | 2015                 | 5 GHz     | 3.47 Gbps                                     | 10 m.                 |
| 802.11ad        | 2016                 | 60 GHz    | 7 Gbps                                        | 30 ft.                |
| 802.11af        | 2014                 | 2.4/5 GHz | 26.7 Mbps – 568.9 Mbps (depending on channel) | 1,000 m.              |
| 802.11ah        | 2016                 | 2.4/5 GHz | 347 Mbps                                      | 1,000 m.              |
| 802.11ax        | 2019 (expected)      | 2.4/5 GHz | 10 Gbps                                       | 1,000 ft.             |
| 802.11ay        | late 2019 (expected) | 60 GHz    | 100 Gbps                                      | 300-500 m.            |
| 802.11az        | 2021 (expected)      | 60 GHz    | Device tracking refresh rate 0.1-0.5 Hz       | Accuracy <1m to <0.1m |

Figure 2 – Chart show the iteration of standard in 802.11 WLANs [15]

With the improvements over the years as previously mention it is an obvious that these updates would include updated security features to keep up to date with the latest

cybersecurity threats. 802.11 has many security features that have been updated over the years to include newer and more modern encryption techniques. The main form of security for an 802.11 wireless network is password encryption, there are numerous encryption techniques uses some more older and less used and many that have been specifically developed in the last few years to meet the security needs of a modern more technologically literate user. Wired Equivalent Privacy or WEP is a relatively old encryption technique developed by volunteers from IEEE wanting to develop a security technique that is in line with the 802.11 specification[16]. WEP takes the data that is to be transmitted and the checksum of the data for validation and integrity checks, the data packet is then generated at random 24-bit key called an Initialization Vector (IV). The IV and a shared key which is known by both transmitter and receiver is then used by a Rivest Cipher 4 or RC4[17] to encrypt the data. WEP is considered inadequate today due to many factors such as the IV and cipher being too short and the RC4 cipher being easily decipherable[18]. Wi-Fi Protected Access or WPA is a modern security technique that has had numerous updates. WPA similar to WEP but instead of using RC4 encryption it uses Advanced Encryption Standards also known as AES[19]. WPA also use TKIP encryption which allows longer IVs and a different encryption stream for each packet[20]. WPA also can use alphanumeric keys unlike WEP which can only use numeric, another secure differences is the pre-shared key is no longer transmitted over the air[21]. WPA has had 3 incremental improvements that increases security by improving and altering areas of the protocol such as key management methods and encryption techniques, as seen below. WPA has had a recent upgrade to WPA3 in recent years again with more improved security to tackle the growing threats to cybersecurity[22]. The Different Security standards used within Wi-Fi is best illustrated in Figure 3.

|                   | WEP                                   | WPA                                                   | WPA2                                                             | WPA3                                                                                                 |
|-------------------|---------------------------------------|-------------------------------------------------------|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Brief description | Ensure wired-like privacy in wireless | Based on 802.11i without requirement for new hardware | All mandatory 802.11i features and a new hardware                | Announced by Wi-Fi Alliance                                                                          |
| Encryption        | RC4                                   | TKIP + RC4                                            | CCMP/AES                                                         | GCMP-256                                                                                             |
| Authentication    | WEP-Open<br>WEP-Shared                | WPA-PSK<br>WPA-Enterprise                             | WPA2-Personal WPA2-Enterprise                                    | WPA3-Personal<br>WPA3-Enterprise                                                                     |
| Data integrity    | CRC-32                                | MIC algorithm                                         | Cipher Block Chaining Message Authentication Code (based on AES) | 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)     |
| Key management    | none                                  | 4-way handshake                                       | 4-way handshake                                                  | Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) |

*Figure 3 – Wireless Security Iterative Improvements[23].*

### 2.3.2 LPWAN and LoRa

In some cases, IoT can be extended to cover a large geographical area to control and monitor a large amount of sensor and devices wirelessly. The current distance restriction on Wi-Fi has led to the creation of a new form of wireless communication used in IoT this is called Low-Power Wide-Area Network or LPWAN and is a technology that is well suited for long range wireless communication[24]. A company called Sigfox first begun development in 2011 and has since been widely accepted as a suitable solution for long range low power wireless sensor communication[25]. Since then many other companies have begun adapting their own version of this technology to suit their own needs such as the LoRa Alliance and Ingenu. LPWAN Has many features that allow it to be useful for IoT and long-range sensor communication. LPWAN has very low power consumption this can enable remote sensors to preserve a large amount of their battery[26]. LPWAN allows for low cost as the hardware is simple and the deployment of such networks is relatively simple as they do not require much or any infrastructure[27]. LPWAN does has some down sides to the newly emerging technology and this mainly within the areas of data rate, the average data rate across the numerous types and LPWAN standards is roughly between 1kbps and 1000kbps[25].LPWAN is also very susceptible to signal interference from other devices that uses within the same frequency band even though LPWAN uses a very small amount of this band[28] this data rate is menial in terms of the data being transmitted so this downside is not as restrictive as it seems.

A Key technology within LPWAN is Long Range Wide Area Networks or LoRaWAN this is a specific adaptation of the technology used within IoT. LoRaWAN can cover an entire city with one base station which acts as a gateway for all network traffic to communicate through[29]. LoRaWAN acts as a normal wireless network using a star topology and standard Internet Protocols (IP) for network communication[30]. Interestingly LoRaWAN makes use of a network server which stores sensor data as a go between the application servers which take advantage of the data and the gateway[31]. As LoRaWAN is a new technology there are some considerations take must be taken into account in terms of security, due to the cost of the end devices being of relatively low cost this allows potential attackers to gain a way into the network with ease which could increase potential attack vectors[32]. To counter this potential flaw the LoRa alliance has implemented 128-bit AES encryption on both end devices and the gateway to ensure security but due to the low bandwidth nature of the technology more layers of security could hinder performance[33]. Security keys for the network come from the Key Management System or KMS which is stored on the network server and ensure consistent key distribution to authorized network end devices[34].

## 2.4 Wireless Sensor Networks

A large portion of IoT relies on a network technology called Wireless Sensor Networks or WSN. WSNs employ the use of a hub in which other wireless devices referred to as node can operate and transmit data to. These nodes are usually low power devices that typically rely on battery power to last a relative long time without human intervention. These devices also have low bandwidth and low processing overhead to keep power consumption low. WSNs can trace their development back to the 1950s when one was created by the use military to use sound to track and detect submarines used by the Soviet Union in the Cold war[35]. Since then the technology has made massive strides by being used in numerous ways most notably the National Aeronautics and Space Administration (NASA) in their sensor web technologies[36].

### 2.4.1 Common Applications

WSNs have numerous applications both in the public and private sectors of many areas of industry. One such application is the use in the smart grid. The power supply chain is vital to all countries and maintenance of these power lines can be a long and expensive

process. Sensor application to this industry can help monitor the powerlines for stresses cause by weather conditions such as erosion from rain and snow. This could potentially save money as the cost of hiring workers to manually perform maintenance checks [37]. Some other uses of a smart grid include allowing to monitor the system remotely and perform diagnostics at power junction boxes[38]. Another sector that can and does take use of Wireless Sensor Networks is healthcare. With the use of wireless sensors they can monitor the conditions of patients within a hospital whilst in postoperative care and in more intensive situations[39]. This technology could provide more mobility to patients whilst also improving reliability and response time of healthcare professionals[40]. There has been some discussion about WSNs for use in disaster recovery such as forest fire detection, this year alone a wild fire in California, USA has devastated many homes and as of writing this a forest fire in the amazon rainforest has devastated acres of the rainforest and destroying the habitats of hundreds of wild animals. This can be prevented with early warning systems provided by WSNs which can alert response teams and officials before the fires gain to much momentum to be controlled[41].

#### 2.4.2 Advantages/Disadvantages

There are numerous advantages to Wireless Sensor Networks due to their robustness. One such advantage is the mobility of the sensors due to the wireless nature of the network; the nodes can be mobile and thus can be used to monitor things such as vehicles or animals for conservation. Wireless Sensor Networks have no fixed infrastructure in the sense that the nodes can be placed in any location within range of the hub or other nodes that can forward the packets to the hub [42]. In some cases the network could be very cost effective with no need to invest in solid infrastructure such as wiring, power consumption or massive amount of expensive networking gear such as switches or routers[43].

As with advantages there are a few disadvantages that are present within a WSN, due to the wireless and low power attributes of WSNs it is understandable that they have shown to have less bandwidth and throughput in comparison to regular wireless networks [44]. Wireless signals cannot be sent to only specific nodes, this is not the nature of wireless signals, because of this the wireless signal can be a potential attack vector for hackers or attackers. The signal can be configured to hide broadcasts, but it is still possible to attack the signal and thus compromise the network and the data being transmitted within[45]. The interference cause by mobile devices or the natural electromagnetics involved with

other electrical devices can cause signal interference and negatively affect the network stability and data integrity.

#### 2.4.3 802.15.4 and Zigbee

Wireless Sensor Networks come from the same family of specifications as Wi-Fi, more specifically a part of the Bluetooth family for data transmission. 802.15.4 is an offshoot of Bluetooth specifically designed for wireless sensors networks, this standard boast scalability and low power usage[46]. These features are very useful when developing wireless sensor networks. 802.15.4 is a standard that mainly concerns itself with the Physical and Datalink Layer of the OSI model, this standard is capable of achieving a data rate of 250kbps in the 2.4Ghz band, but this is at the most and in real life scenarios the data rate is much low to account for network overheads such as routing and packet collision detection[47].

Zigbee Builds upon the 802.15.4 standards by applying standards to the Network and Application Layers of the OSI Model. This provides the user the ability to develop their own applications and uses for a Zigbee network whilst also building upon and taking advantage of the features 802.15.4 provides. The Zigbee network layer allows for multiple network configurations and network types, the three main network configurations are Star, Tree and Mesh as seen in Figure 4.

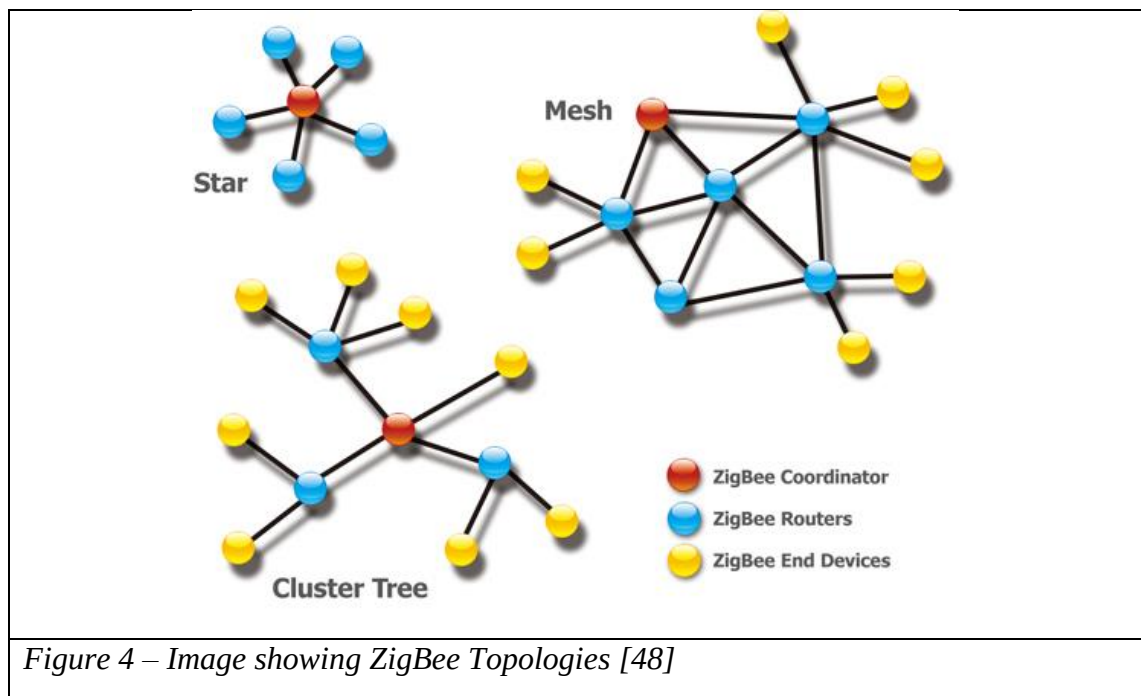


*Figure 4 – Image showing ZigBee Topologies [48]*

ZigBee uses different types of nodes to relay and route data transmissions. A ZigBee network has a coordinator which is responsible for controlling and organising the

network, this is a hub of sorts within the topology in which all data and nodes is accounted for. The ZigBee routers are responsible for multiple hop routing and allows other nodes to communication or route packets of information towards the co-ordinator. The end devices are the sensors which gather information and transmits it towards a ZigBee Router[46].

## 2.5 IoT and WSN Security

IoT has been successfully brought into the homes and workplaces of hundreds of thousands of consumers, these devices are constantly gathering data and utilizing it to complete numerous tasks. With this massive increase in data being gathered it is more important now than ever to consider the security of these device and how the data gathered can be protected from potential attackers, who would use this data for nefarious means. There are many methods that an attacker could use to gain access to the network and the data. The first of these attacks that the author is going to explore is a Sinkhole attack. A sinkhole attack occurs when a node that is not part of the network is sending data to make it seem like it is an authorized node and influences other nodes to send their packets to the sink node, this allows the attackers to disrupt the network flow by supressing network messages through selective forwarding[49]. A sinkhole attack can potentially lead to a wormhole attack which involves rouge nodes that act in tandem by reporting to the network that one node which is farther away from the hub is another node that may be closer this node is controlled by the attacker. This gives the network false routing information and can lead to the reduction of speed within the network, this is due to the nodes always looking for the fastest path to the hub[50]. The final attack is Man-in-the-Middle or MITM this attack involves a few sub attacks in order to work, first the attacker gain access to the network and then performs and Address Resolution Protocol (ARP) Poison attack or Domain Name Server (DNS) attack which sends faulty ARP or DNS info into the network making itself seem like a known node[51]. Once this stage has been established the attacker will then intercept packets being sent to a legitimate node by pretending to be that node, the information is then forwarded to the legitimate node, so the network doesn't think anything is wrong[52]. The attacker will take the information and replicate it before forwarding and decrypt it for further use. Most of the attacks mentioned rely on a wireless sensor network or IoT network to have a multi-hop routing system and a mesh topology.

## 2.6 Simulating a Network

When building a wireless network is it common practice within the industry to develop a working simulation of the proposed network to gather an understanding of how the network will perform in terms of speed, reliability and efficiency. A simulation allows an individual to create a model of the network using the same protocols and similar devices, once the model is created it also allows the individual to place some real life scenarios on the network such as modelling power consumption and network interference commonly referred to as noise there are numerous types of noise that can be added to the network this will be discussed in detail later. Simulation can often be used as a cost saving measure as it allows for someone to develop a proposed network and test what devices are needed to get the same efficiency thus reducing the cost that would be incurred in a trial and error format[53].

### 2.7.1 Common Programs for Simulations

There are numerous common applications used to simulate network of all types, many are developed for the industrial side of networking and not so much for the academic side, thus they require a licence which could restrict the author choice of simulation software. The author has 3 different network simulators that could potentially be used in this project, the first potential software is Network Simulator Version 2 or 3 or NS2 or NS3. These two network simulators are both event driven simulators capable of simulating both wired and wireless networks, this software is free, open source and mostly run on Linux or Unix based systems[54]. Whilst the software is very versatile it is very complex and requires patience and an understanding of C++ programming to use it effectively. The Second program the author is considering for use within this project is Netsim developed by Tetcos which is a more User-friendly network simulator capable of simulating various forms of wireless and wired network and their associated protocols. Netsim is often used by many educational institutions as well as military organisations, network manufacturers and network service providers[55]. This software also has the ability for integration with other software such as MATLAB which can be used to pass variables between the two for analysis or different experimentations. The third and final network simulation software that can be used in this experiment is the Graphical Network Simulator 3 or GNS3[56]. This software relies on running Virtual machines of common networking hardware such as Cisco switches and routers. Unfortunately, this software is restricted for use in wireless

networks as the operating systems for wireless devices are not often available for download. Another downside of GNS3 is the inability to easily gather metrics for results.

### 2.7.2 Network Noise

Network noise is the interference of the wireless signal from numerous other sources of wireless signals or common obstacles. One source of interference is the environment such as concrete walls and buildings, another source which is most common in heavily populated areas is interference from other wireless devices on the same band[57]. For example, a wireless device trying to communicate with the wireless hub could be interrupting or interfering with another node already communicating with said hub. With the world increasing its usage of wireless devices from mobile networks for long range communications and almost every home having a Wi-Fi network it makes wireless interference a real problem for signal congested areas. Radio Frequency interference is the most common form of interference this usually comes from devices both licenced such as commercial wireless devices or mobile phones and unlicensed such as amateur radio communication systems can result in unintentional interference[58]. In some cases, the interference can be intentional, as known as jamming this can act as a potential Denial of Service attack on Wireless users, these attacks are often seen to inconvenience users instead of gaining information.

### 2.7.4 Simulation Metrics

When a network is simulated it is common to primarily focus on 3 industry standard metrics the first being throughput, this is a measurement of the rate of speed in which the data that is being packaged into packets is being transmitted across the network medium whether it be wired or wireless. Throughput is the standard way of measuring if the network speed is reaching its specified transmission rate[59]. Measuring throughput is more difficult to measure than the other metrics in this research project, this metric would require a 3<sup>rd</sup> party program that would transmit dummy data and measure the speed, programs such as SolarWinds, Iperf3 and Netstress would be suitable for this in many instances. Packet Loss is another industry standard metric for analysing performance. This metric is self-explanatory as packets travel through a network it is possible that due to congestion within the network that certain devices will drop packets before they make it to their destination in order to free up available bandwidth for more important services that have been set by the administrator or by default within the network[60]. A good way

to measure packet loss is by pinging the IP address or domain name of the device or the site that is being tested, the ping test will output how many packets have been transmitted and the number of packets received by the destination, in some operating system this will include a percentage of the loss. This method works on almost all operating systems found in modern devices including Windows, MacOS and most likely all Linux distributions. Most network simulation software includes metric measurement functions within the system. Network delay or Network Latency is another metric used to monitor network performance. Latency is the amount of time it takes for a packet to reach its destination, with TCP networks that require a confirmation packet from the destination in order to transmit the next packet it is important that latency is as low as possible. To measure latency, it is possible to use the same ping method as mentioned before with testing Packet Loss as most operating systems also include a round trip time which is the measurement of how long did it take to receive a confirmation packet from the destination once the initial packet was sent[61].

## 2.8 Related Works

Although there has been much work done on Wireless Sensor Networks, it is difficult to find much research on simulating such network, the author has found a few papers that could be influential and helpful to this report.

In a paper published in 2014 by Faieza Hanum Yahaya and associates at Universiti Teknologi MARA in Malaysia titled “*Performance Analysis of Wireless Sensor Network*”[62], researchers performed an analysis of the potential performance of wireless sensor networks. In this report the author and associates created 2 models for the analysis of WSNs the first being a model where the 11 nodes are placed at random through the simulated environment, 1 of the nodes acted as a base station and another as a router for access to external networks. The second model was created similarly to the first, but numerous nodes were moved further away from the base station and others were moved closer. The researchers configured numerous settings from the MAC protocols to the battery model and modulation scheme. The researchers found that the further away a node was from the base station the less likely it is to attempt to transmit data and the increased likelihood of the node disconnecting. The report also showed that throughput is closely linked to the distance of the node to the base station. Yahaya and associates concluded that the distance, power and environment were all factors that should be considered when

developing a wireless sensor network. Though this report is relatively outdated as of 2019 the author still believes it holds merit in showing that numerous factors go into the planning and development of a wireless sensor network.; Yahaya et al has also give the author potential ideas on the configuration of the network from simulating power consumption to tweaking sensor variable for better performance. There are some areas where the author believes would not be useful for the experiments proposed in this project the first being the Constant Bit Rate used as test data, it is hard to assume that the data transmitted in a standard wireless sensor network will be constant and at the same packet size. The second factor the author believes would not help this report is the random locations of the modelled sensors this does not consider the static position of a node or account for an area where the node may not be placed due to obstacles or no mounting position. Yahaya et al also made no mention of interference from other electronic devices, that could affect the transmission signal. Overall Yahaya and associates work presents a best possible scenario for a wireless sensor network but is still helpful to this project as it helps build a foundation in which the author can build upon.

A second paper the author found that was relevant to the focus of this project is a paper written by N. Ahmed, H. Rahman and MD.I. Hussain, title “*A comparison of 802.11ah and 802.15.4 for IoT*”[63]. In this report the authors looked at how well both network types perform with increases in the number of sensors. The authors set strict parameters for the experiment but setting variables such as bandwidth and payload sizes to the same. The authors had nodes increase in increments of 100, the metrics used within this experiment was delay (Seconds), Throughput (Kbps) and Association time (Seconds). Association time is a metric that the author of this project didn’t think was relevant to some network but in this report the authors tested this metric and found that the 802.15.4 had lower association time in comparison to the 802.11 network. The throughput also showed that 802.11 performed a lot better than the 802.15.4 network as by the end of the testing of the author experiment the throughput of the 802.11 network was in the low 100Kbps and the 802.15.4 network was in the 10Kbps range. The delay results also reflect this with 802.15.4 showing a sharp increase in the amount of end to end delay experience as more nodes are added. From the results of N. Ahmed et al, it is apparent that with the 802.11 network largely outperformed on the 802.15.4 network. The author concluded that even though the performance was better “*802.15.4 demonstrates higher energy efficiency than 802.11ah*”[63]. It is the authors opinion that the report written by N. Ahmed et al. would be along the same lines as this report, the only areas where there is a difference is that the

author is attempting to understand how both technologies work under a specific scenario. The author think that the comparison of the association time is an important metric to consider for the experimentation of this project, whether the software the author plans to use will support this metric is unknown at this point.

The third and final piece of work that the author thinks is relevant to the work being done on this project is a paper called “*Comparison of IEEE 802.11 and IEEE 802.15.4 for Future Green Multichannel Multi-Radio Wireless Sensor Networks*[64]” written by Carlene Campbell, Jonathan Kok-Keong Loo and Heba A. Kurdi. In this report the authors looked at how 802.11 and 802.15.4 CSMA/AC performs under different data rates and ranges of distance. The authors simulated 50 nodes placed randomly in a 1000m<sup>2</sup> test environment and used a CBR to simulate data transmission within the network. The authors also had 2 range parameters, one at 10m and another at 50m and 2 data rate 100Kbps and 2Mbps. The authors focused on 3 metrics Access Delay (Seconds), Delivery Ratio and Average MAC Throughput (Kbps). The authors found that at 100Kbps both networks performed the same with 802.11 showing marginal increase in packet delivery and throughput. It was observed that as more nodes were added to the network delay began to increase and throughput and packet delivery ratio began to decrease. The authors concluded with at long range 802.15.4 performs poorly with data rates of both 100Kbps and 2Mbps, with 802.11 performing a little bit better at low data rates and node count of higher than 20. The authors concluded with “*Having investigating the performance between IEEE 802.11 and IEEE 802.15.4 it is feasible to focus the future WSN using 802.11 contention-based protocols.*[64]”. The author believes that the test bed for this experiment was solid, once again the author thinks that the research done in this paper would be along the same lines as this projects apart from the variance in the node ranges, in the authors simulation each node distance would be different respective to their requested location. The author thinks that the varying data rates would not be suitable for the work done on this project as the author is attempting to gain the most performance possible out of the simulations.

## 2.9 Conclusion

Throughout this chapter the author has conducted an in-depth investigation into the current research and work around IoT and its increase popularity and applications. The author investigated WSNs and specific protocols such as 802.15.4 and ZigBee which

build on 802.15.4. and Wi-fi Networks, the author has outlined how the technology works and how they are implemented across many industries. The many advantages and disadvantages of each technology were discussed, and the security methods and vulnerabilities in all these technologies were researched. The author looked at the surrounding technologies that are innovating IoT on a larger scale such as LPWAN and LoRa with their massive range capabilities allowing for large interconnected smart cities. The author has also discussed the ideas behind simulations and the various metrics used to measure simulation performance. The author has also review 3 pieces of related work that might be helpful with supporting or building the work being done in this report.

## **Chapter 3 – Research Methodology**

### **3.1 Introduction**

In this chapter the author will discuss the methodology behind this project, this will allow the author to fully flesh out how data collection and research will be conducted. Throughout this chapter the author will discuss the research philosophy which will underline how the author believes the data should be gathered and interpreted. The author will also talk about the research approach this will include how the author plans to solve the research problem formulated in the design section of this report. Finally, the author will talk about how data used within this report will be gathered in terms of primary and secondary sources, the author will also discuss potential risks that could be a hindrance to the project by causing delays or possible inconvenience.

### **3.2 Research Philosophy**

The research philosophy it is very important in understanding the way data will be collected and interpreted. The author has decided to take the positivist approach to the research. The Positivist approach also known as the scientific approach is the idea that the research should be conducted with a stable approach, that the testing should take place in isolated conditions and that only variables that should be in the experimentation is the variables the research is attempting to measure a reaction from[65]. The research involved within positivism is observable and repeatable with similar results, if they were not the theory would not be proven correct. The author believes that this will suit the purpose of this project as he believes that the results can be repeatable and thus hold weight when it comes to scrutiny.

### **3.3 Research Approach**

As the author plans the follows the positivistic philosophy it is naturally assumptive that the author will follow a deductive approach to the research. The deductive approach is based around a problem or hypothesis, this hypothesis is then tested through methods of experimentation to gather an outcome the proves or disproves the authors hypothesis. Deductive reasoning closely looks at the relationship between a set of variables and how they affect the outcome of the experiment. The end result of this approach to research is

either an confirmation of the hypothesis or a rejection either way the results still give information about how the isolated experiment reacts to variables[65].

### 3.4 Data Collection

The data that will be collected throughout this project shall come from numerous areas, Primary Sources of data is the data gathered by the investigator or researcher, the information gathered can be from numerous areas such as experimentation, case studies or surveys, if the data gathered is a first-hand account or encounter then it is a primary source. For the purpose of this project the primary sources of data will be gathered from an experiment which will be discussed in detail in Chapter 4, it is the authors belief that in order for a study to be effective and true then it must rely heavily on primary sources of information to give the research validity. Secondary sources of information are gathered from the reports and studies of other researchers this will help the author develop an understanding on what others in the field have found from their research and their experiments, this often helps validate research by showing it is repeatable. The author has already completed the research using secondary sources as seen in the literature review in Chapter 2. A Large portion of the secondary sources come from the IEEE digital library, this allows the author to access research papers written by other researchers in the field, the author also gathers information from books which while some might be outdated, they still can provide a good ground work for the literature review performed.

### 3.5 Risks

Understanding and identifying potential risk in any research project can allow the author to carefully predict and take precautions against any hinderance or such events from occurring. The author has identified a few risks that could potentially hinder the progression of the project, some of the risk can stop the project from making it to completion, by understanding these risks they can hopefully be avoided. The first of these risks is loss of access to the necessary tools such as network simulator or labs necessary to complete the experiment phase of this project. Another serious risk to the project is loss of data, the information gathered through the experimental stage will all be digital. This could result in data corruption or loss of data through other means, to prevent this the author will continually back up the data in multiple locations including the cloud.

### 3.6 Conclusion

To conclude this chapter the author has decided that the best approach for this project would be to follow the positivist philosophy, which is the tried and tested scientific method that has been the basis of the last few hundred years of research. In connection with the positivist philosophy the author will also follow the deductive approach which involves the testing of a hypothesis and either the rejection or acceptance of said hypothesis. The author has also discussed the numerous sources of information that have been and will be gathered for this project including primary sources from the experimentation and the secondary resources used within the literature review. Finally, the author discussed the numerous risks that could affect this project and cause many delays, the author has made suggestions on protocols that will be followed to minimize the risk to this project.

## **Chapter 4 – Design and Implementation**

### **4.1 Introduction**

Throughout this report the author has talked about IoT and Wireless Sensor Networks, in this chapter the author will fully develop the designs for the experiment and formulate the problem that this project hopes to resolve. The author will outline what tools will be used throughout the experiment, what the experiment hopes to achieve and what data will be gathered. Most importantly the author will bring focus to the areas of the topology and the protocol standards that have been proposed for the network.

### **4.2 Problem Formulation**

With the development of this new wireless sensor network there is always room for improvement, what the author is trying to solve is whether a wireless sensor network on the site with the proposed topology can be implemented with high performance. The author will also look at other network standards and protocols for the best way to implement the proposed network. The author believes that by comparing the results of both experiments accurate conclusions can be made to create the best performing network possible. The author will also make conclusions about which network standard should be implemented on the site for the best cost and the best performance.

### **4.3 Design**

The experiment is a key aspect of this project, so it is vital to gain as much information as possible. The author has decided that the experiment will have 2 areas of focus the first being simulating a conventional IoT Wireless Sensor Network both with and without noise. The second area of focus is to simulate a normal 802.11 wireless network again with and without noise. This simulation will try and get as close as possible to the real-life system in terms of node distance and interference levels. The author believes that by testing both of these systems, then good assumptions can be made about whether a new network should be put in place or if the Sensor Network can be integrated into the already existing Wi-Fi network on the site.

The topology of the network has already been developed in agreement with the project manager and what the wishes of the company are and the fellow colleague who will be developing the physical network. This topology can be seen below in figure 5. The topology is colour coded to reflect the location of the node, the orange nodes are to be installed outside and underneath attached to pillars which hold the first floor. The purple nodes are inside the building and attached to pillars that hold the roof, the green nodes are either outside or attached to a pillar which is partially exposed on the outside of the building. The reasoning for these positions is the project managers want to get as much data from multiple areas under different scenarios, for example the green would measure wood that has been in full or partial contact with the local weather and the orange does the same but under the building and closer to the ground to understand how the wood reacts to this change of environment. The hub for the network is place as close to the centre of the site as possible to get the best range for all the nodes on the network.

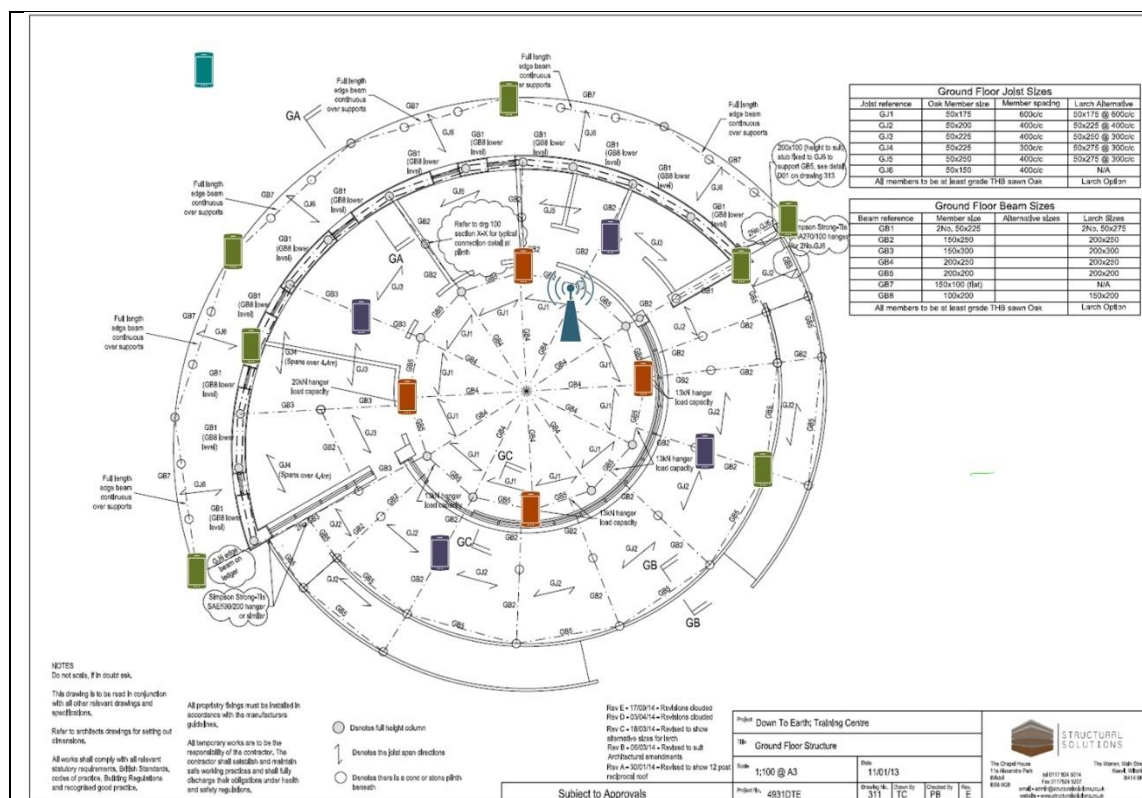


Figure 5 – Proposed Topology of Down to Earth Site

The Author plans to simulate all 16 of the proposed nodes, each running an application at the same time to understand how the network can handle the stress of so much data being sent at the same time. To simulate traffic the author will use the settings in Netsim to create a constant bit rate of traffic, this is to fully understand how the network handle stress during the moments in which all nodes will be transmitting their data to the hub.

The author will create a simulation with no network noise this is to get a base line reading on the best possible conditions.

Netsim currently supports the following noise types:

- Pathloss which is the loss of power in a signal that is being transmitted through the network. The author is using the Indoor Office Model implemented by Netsim. This model is best for indoor spaces where distances are smaller, and the variability is much higher.
- Fading is the altering of the signal strength based on outside variables such as geographical location. Rayleigh Model represents the variation of signal strength at the receiver, this form of fading occurs when there is no line of sight between the node and the hub
- Shadowing is the interference of the signal based on obstruction in the way of the transmitter and receiver such as walls and buildings. The author is going to use the constant model, this model is good for a simulation with little to no node mobility.

To make the simulations as accurate as possible the author has taken the schematics and calculated the node location in terms of X and Y co-ordinates to do this the author took a scale drawing with measures and place the nodes in their relative location and estimated the location of the X and Y location of the nodes, keep in mind that they may be some inaccuracy and the measurements might not be as precise.

#### 4.4 Implementation

Once the design was developed the author began to work on the Netsim Simulations, the first area to begin implementing the simulation was the placement of the nodes in the topology, following the proposed topology and the overall distances calculated previously. Figure 6 shows the final topology of the IoT network, as can be see the IoT network has a different way of connecting to the network sink using an Ad Hoc link. All

wireless connections link to the Ad Hoc link and the connects to the sink, which is then connected to the router and the data server in which all data will be transmitted to.

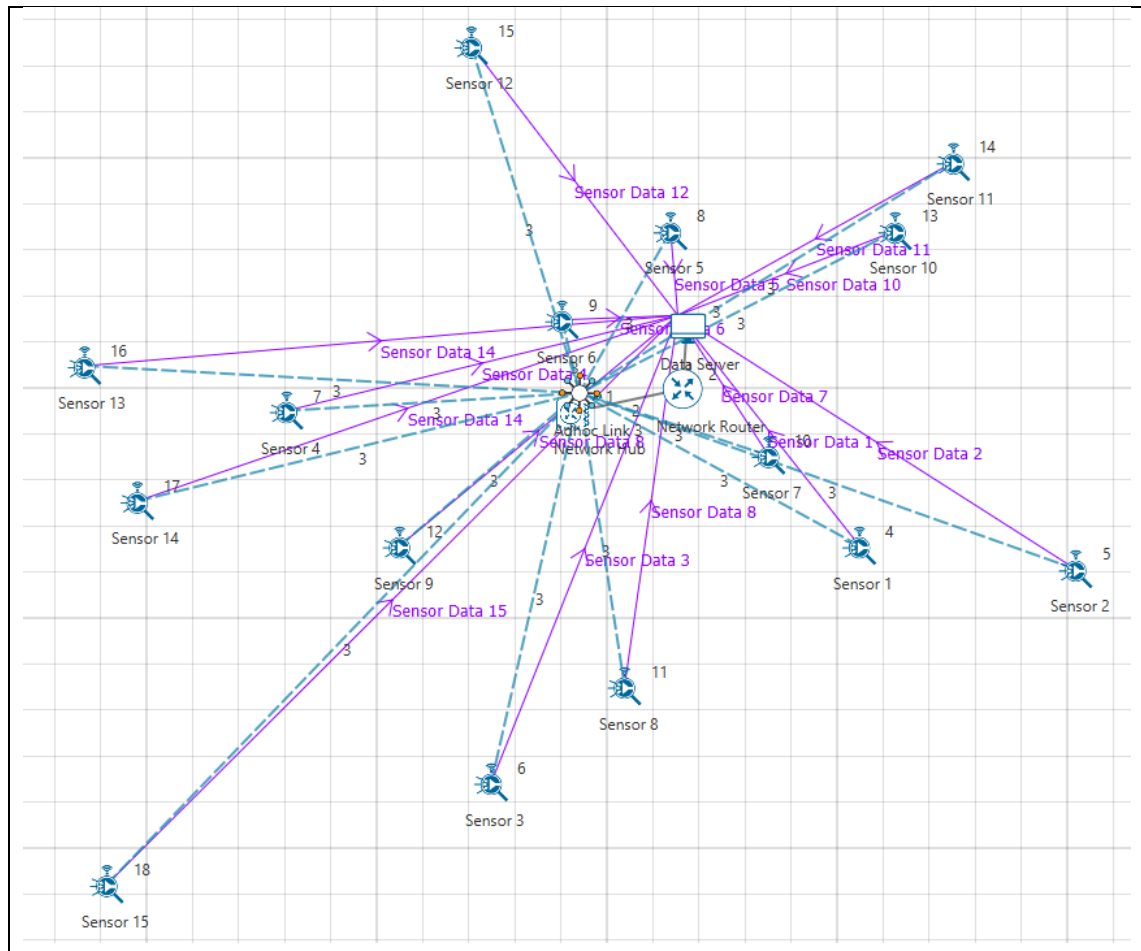


*Figure 6 - Topology of IoT Network*

Figure 7 shows the general settings of the sensors this includes the X and Y co-ordinates of the sensor node, this is done in relation to the schematics the author mentioned in the design section, each node will have a specific location across all simulations so that the result will be repeatable and comparable. The sensor also can be configured to move across the simulation space, but as all these sensor nodes are in static positions the author felt it was unnecessary to enable this function.

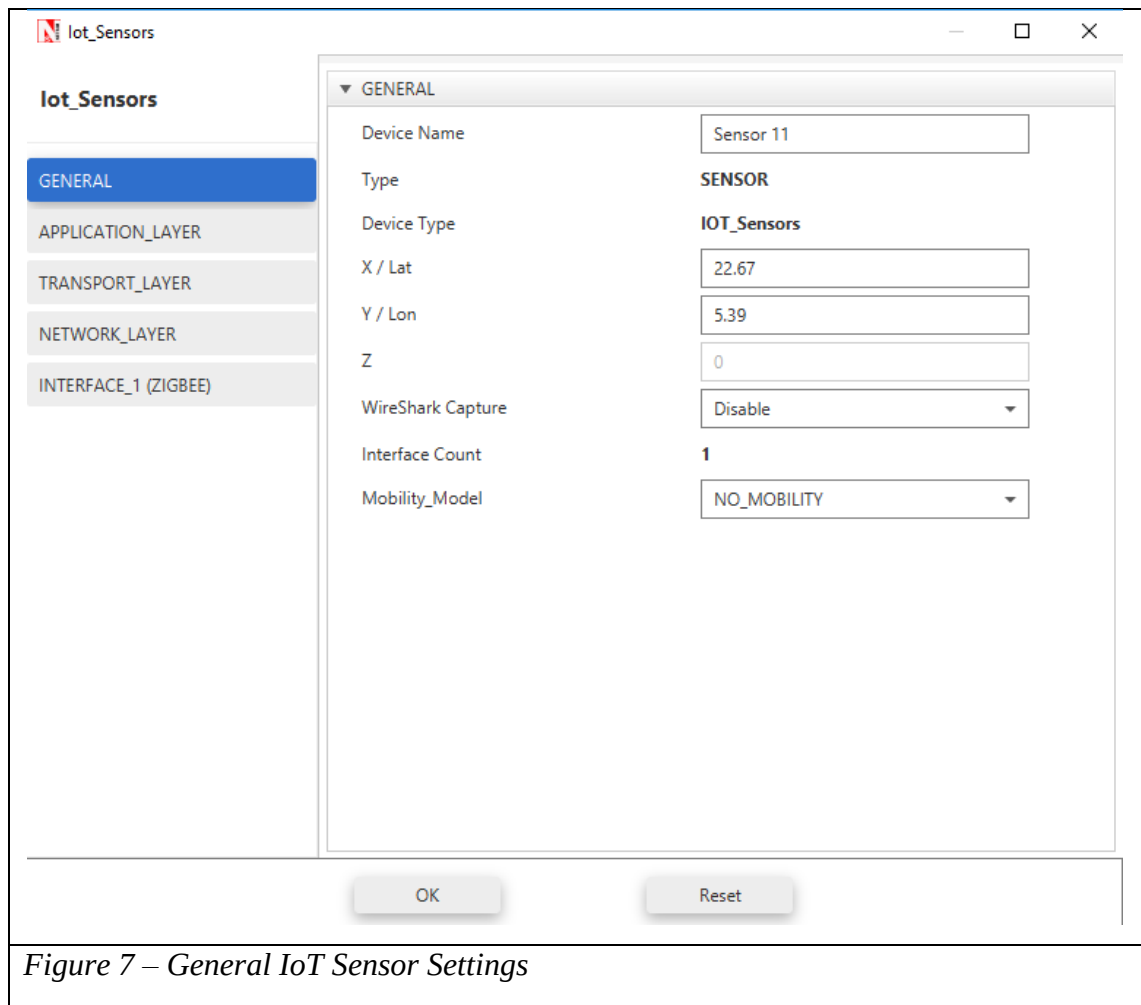


*Figure 7 – General IoT Sensor Settings*

Figure 8 shows the network configuration for the IoT network, the author has the option of 2 common WSN routing protocols DSR and AODV and from the author previous research into the area, it was discovered that AODV has superior performance across all metrics when compared to DSR[66]. This protocol will enable the network to communicate at the highest possible performance level.

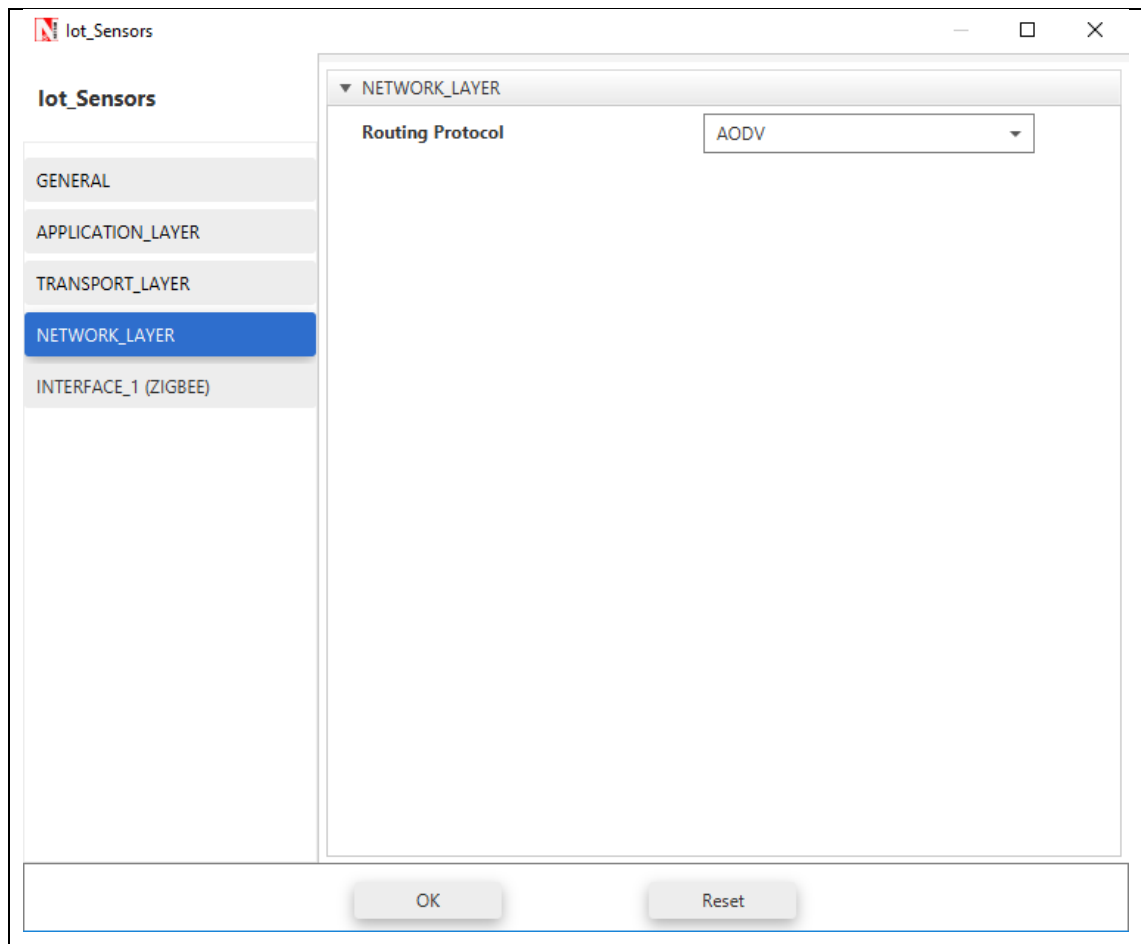


*Figure 8 – IoT Sensor Network Settings*

From Figure 9 there are very few settings that the author can change within the software. The protocol used is that standard IEEE 802.15.4 and is running in the 2.4GHz band. The highest potential data rate that the nodes can perform at is 250Kbps which is accurate as seen from the authors research. Figure 9 also shows that the modulation scheme for the nodes is Offset Quadrature Phase Shift Keying which is a modern scheme that allows for 4 symbols to be transmitted at the same time allowing for fast data transfers.

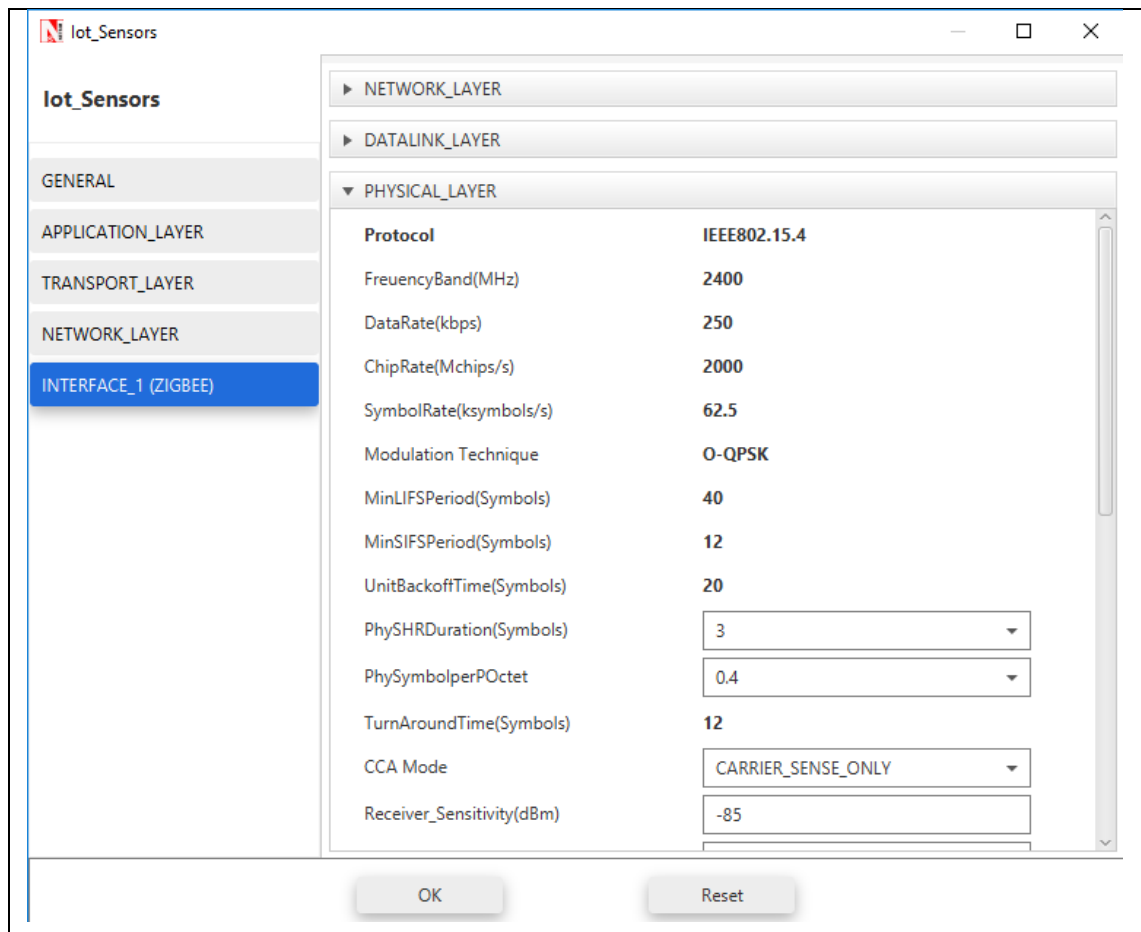


*Figure 9 – IoT Sensor Interface Settings*

In figure 10 the sensor interface settings have been continued, from this it can be seen that the author has configured the power source of the sensor nodes to be a battery with no energy harvesting as placing solar panels on some of the sensors could be a potential problem due to the lack of energy harvesting in low light while indoors. The author configured the sensor to have a 1000mAh battery which is the standard size rechargeable battery available on the market today. The other settings were left as default as the author felt that without a definitive sense of what batteries could be used, then an accurate assumption couldn't be made.

**IoT\_Sensors**

**IoT\_Sensors**

GENERAL

APPLICATION\_LAYER

TRANSPORT\_LAYER

NETWORK\_LAYER

**INTERFACE\_1 (ZIGBEE)**

NETWORK\_LAYER

DATALINK\_LAYER

PHYSICAL\_LAYER

TransmitterPower(dBm) 1

Antenna Gain 0

Antenna Height(m) 1

Connection\_Medium **WIRELESS**

Reference Distance d0(m) 8

**POWER**

PowerSource Battery

EnergyHarvesting Off

InitialEnergy(mAH) 1000

TransmittingCurrent(mA) 8.8

IdleModeCurrent(mA) 3.3

Voltage(V) 3.6

ReceivingCurrent(mA) 9.6

SleepModeCurrent(mA) 0.237

OK Reset

*Figure 10 – IoT Sensor Interface Settings Continued*

During the Design Phase the author decided that it would be beneficial to look at other potential network types for the sensor network. This would allow for the comparison of the different technologies and the different directions the network could take. The network has the same topology for the same reasons previously mentioned and it too has a data server but instead of an ad hoc link and a hub it relies on a standard 802.11 router as the network would be using the 802.11p standard.

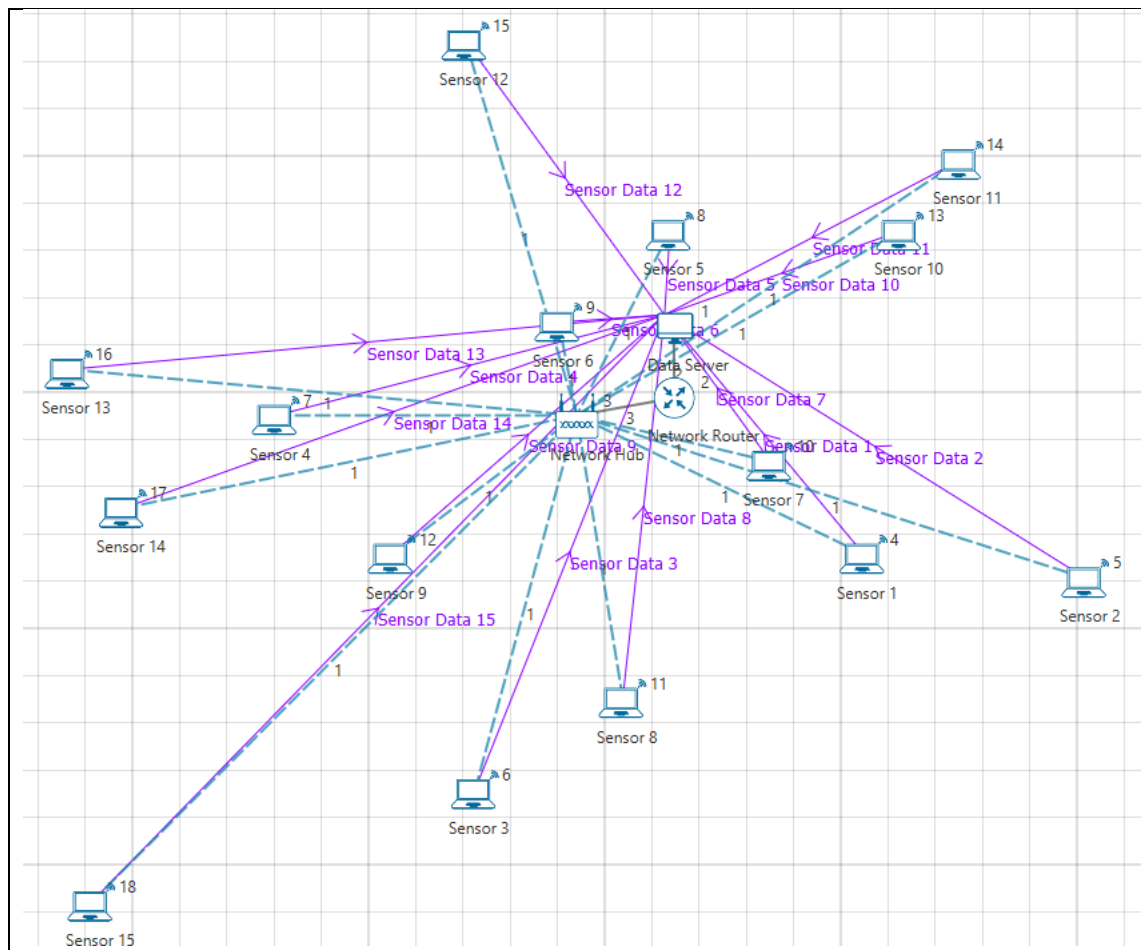


*Figure 11 – Topology of WLAN IoT Network*

As the topology for this network is also following the designs of the aforementioned topology the settings shall remain closely the same, the only downside to simulating 802.11 is the lack of mobility in the nodes, this is not a problem the author has any worries about as the nodes again are static and shall not move. Once again, the nodes are configured with an X and Y location in relation to the schematics mentioned earlier. This is highlighted in figure 12.

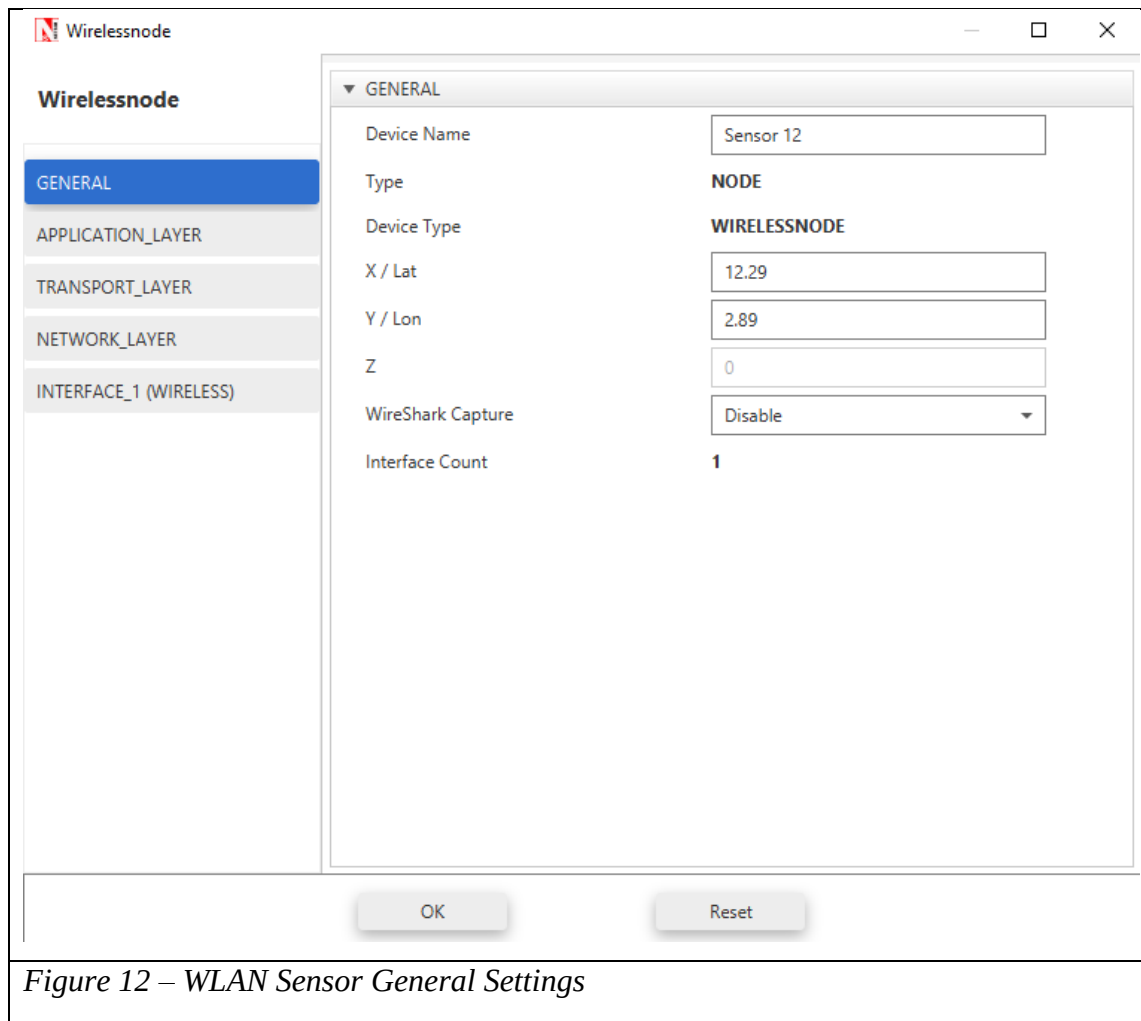


*Figure 12 – WLAN Sensor General Settings*

The settings of the nodes interface are simple. The author had decided to go with the 802.11p standard which is a recent iteration of the 802.11 standard which enables for the uses of vehicular networks. The transmission type is OFDM which the author covered in the literature review, the transmitter power and antenna setting remained at default. Unlike 802.15.4 simulation the 802.11 standard can run in the 5GHz frequency band which increase transmission speeds of the network. These settings are enabled on all the nodes and the access point for the network to ensure consistency of the network.

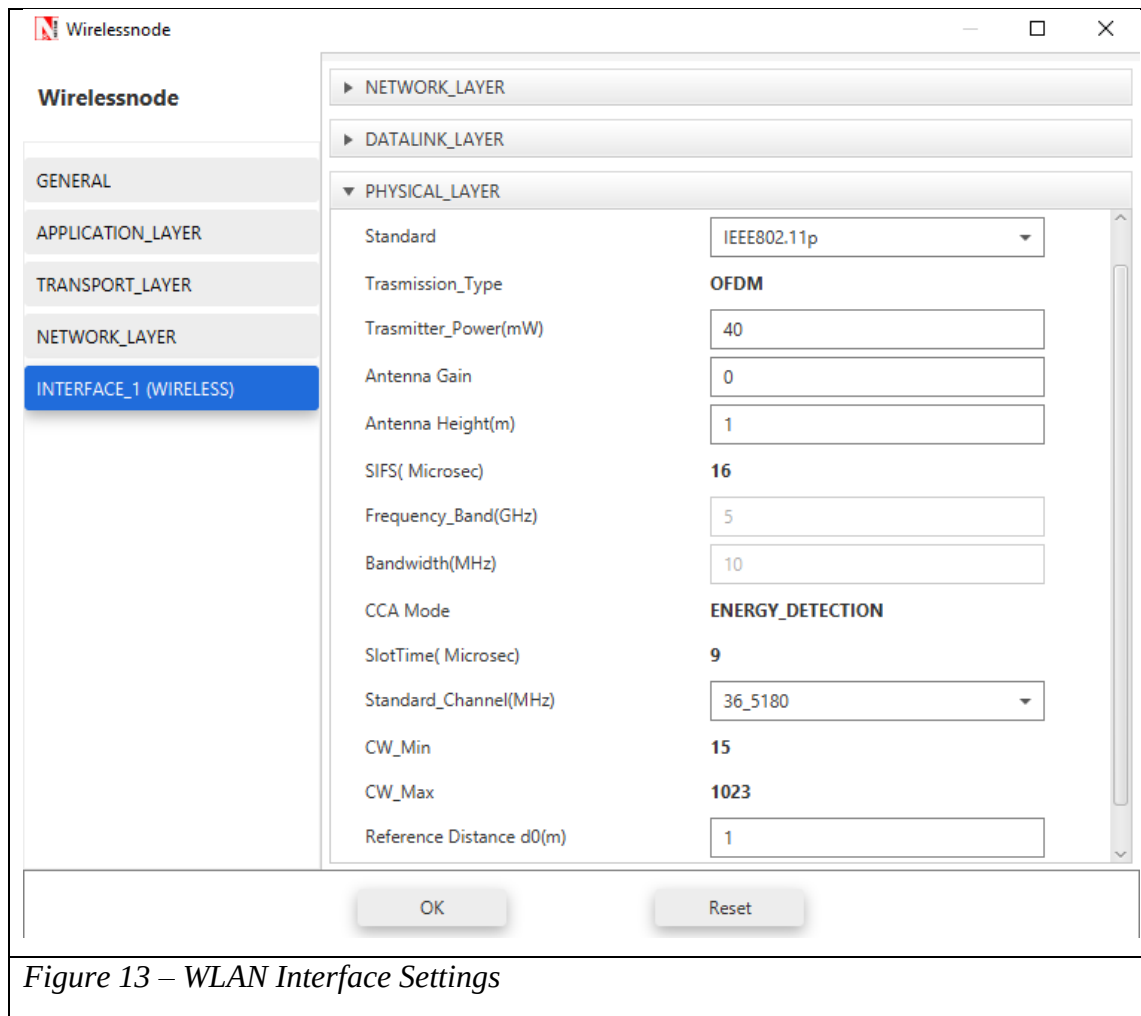


*Figure 13 – WLAN Interface Settings*

Figure 14 shows the setting for the network interference, as previously mentioned in the design section of this chapter the author has enabled the noise settings on both simulations. The author enabled the INDOOR\_OFFICE model and the RAYLEIGH fading model, with a standard deviation of 5, the author believes that it is a good midpoint of interference levels as the range for this software is 0-10.

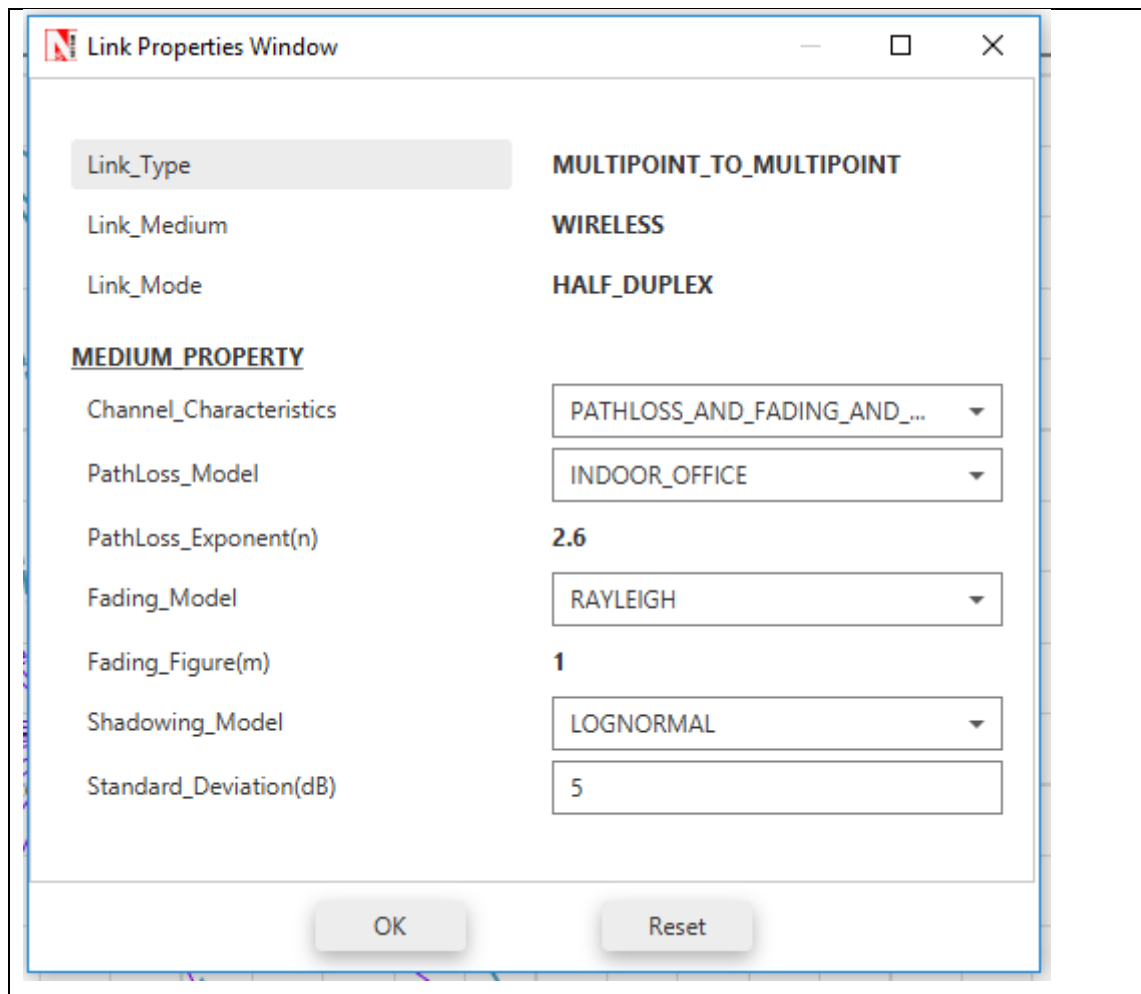


*Figure 14 – Simulation Noise Settings*

The applications of the two simulations was the same Constant Bit Rate (CBR) this will enable the author to gather an understanding of the metrics more reliably as the data will be constant and thus reflect the maximum performance of the network. The application was configured to transmit data to the data server through access point/IoT Sink, the author chose to disable encryption to ensure that the results wouldn't be affected by the higher processing overhead. The author set the start time and the end time to reflect the length of the running simulation so that the constant bit rate would not shutdown prematurely. The author also configured the packet size to be a constant size so that the results won't be affected by the variations of packet sizes.

| ▼ APPLICATION                    |               |
|----------------------------------|---------------|
| Application_Method               | UNICAST       |
| Application_Type                 | CBR           |
| Application ID                   | 1             |
| Application_Name                 | Sensor Data 1 |
| Source_Count                     | 1             |
| Source_ID                        | 4             |
| Destination_Count                | 1             |
| Destination_ID                   | 1             |
| Start_Time(s)                    | 0             |
| End_Time(s)                      | 100000        |
| Src to Dest                      | Show line     |
| Encryption                       | NONE          |
| Random_Startup                   | FALSE         |
| QoS                              | BE            |
| Priority                         | Low           |
| <b><u>PACKET SIZE</u></b>        |               |
| Distribution                     | CONSTANT      |
| Value(Bytes)                     | 1460          |
| <b><u>INTER ARRIVAL TIME</u></b> |               |
| Distribution                     | CONSTANT      |
| Value(micro sec)                 | 20000         |

*Figure 15 - Simulation Application Settings*

#### 4.5 Conclusion

In this chapter the author has outlined the plans for both sets of simulations, including the appropriate settings for both the IoT and WLAN network tests. In this chapter, the problem that this report is attempting to resolve was fleshed out and discussed in relation to how it might be solved in the most effective manner. The author has also discussed the network interference that has been used in the experiment and why certain levels were

chosen. The author has talk about all the design specifications set by the company and created a topology based on what was discussed in terms of varying range of data sources for Down to Earth. The author gave an explanation on how the data will be collected i.e. using a constant bit rate to gain a good overall understanding of the network performance. Finally, the author talked about all of the settings changed during the development of the simulations.

## **Chapter 5 – Data Analysis and Results discussions**

### **5.1 Introduction**

With the simulations successfully completed the data was collected and inputted into several spreadsheets for detailed analysis. In this chapter the author will analyse the results gathered and make assumption on the nature of the data and what they show, including trends and anomalies in the data. The author will do this for both simulations with and without interference. Once the data has been analysed the author will discuss the implications of the data and talk about the validity of said data in relation to this report.

### **5.2 IoT Results**

The first set of results the author will discuss is the IoT packet loss results. For the purpose of illustrating a clear trail of though the author will compare both the Noise and no noise simulations at the same time. In figure 16 when observing the no noise results only it can be said that the performance of the network is somewhat lacking as even with no interference the results show the highest percentage of packets being successfully delivered is that of node 1 with only 0.2638% of packets completing delivery. In some nodes on the no noise simulations there was no activity at all to be measured as seen with node 4, 9, 13 and 14. The lowest performing node on the no noise simulation minus the nodes that didn't even start up is node 10 with a success rate of only 0.0144% this is a disparity of 58.7543%.

When looking at the data with noise it can be said that in some cases certain nodes such as node nodes 5, 6, 7, 10 and 12 perform marginally better than the same nodes on the no noise simulation, this is an anomaly the author will discuss later in this chapter. The node effected with noise that manages to deliver the most packets is that of node 10, with a success rate of 0.056%, the IoT noise simulation only had one node that did not start up and that was node 8, besides node 8 the lowest performing node was node 3 with a success rate of 0.0022%, this is a difference of 184.88%. when looking at the disparity of the lowest performing node and the highest performing node on both simulations with and without noise, it is clear that the simulation has less disparity between the nodes and when looking at the average packet loss of the network as a whole the packet success rate of the network without noise is 0.0374 while the average success rate of the network with noise is 0.03, this shows that the network without noise has a better chance of successfully

delivering packets to the data server than that of the network with the noise even though it is marginal at best.

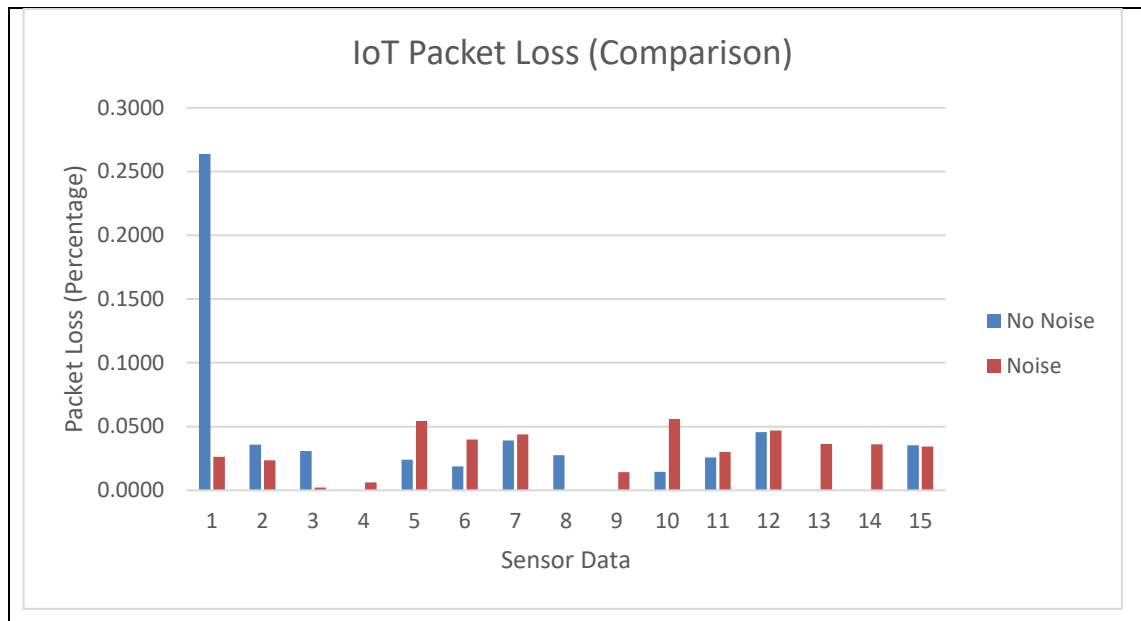


*Figure 16 – IoT Packet Loss showing simulations with and without noise.*

Figure 17 shows the throughput results of both simulations, from initial observations the throughput results of both simulations are abysmal with the best result just about reaching 0.0015Mbps. Once again, the results show irregularities compared to how the author would have predicted them. The highest throughput observable is that of node 1 which is to be expected based on the previous results, with a throughput of 0.001539Mbps when compared to the lowest throughput of an active node of 0.000085Mbps on node 10, which is a difference of 179.064%

When looking at the noise results it can be said that once again some nodes performed better with noise. Nodes 5, 6, 7, 10, 11 and 12 had higher recorded throughput on the noise simulations than their no noise counter parts. The highest recorded throughput on the noise simulation was again from node 10 at 0.000327Mbps and the lowest active node throughput was at 0.000013 on node 3, this results in a difference of 184.709% between the highest and lowest throughput for the noise simulation. When the author averages out the throughput of all the node on the network, it appears that the throughput is the same for both noise and no noise networks at 0.0002Mbps.

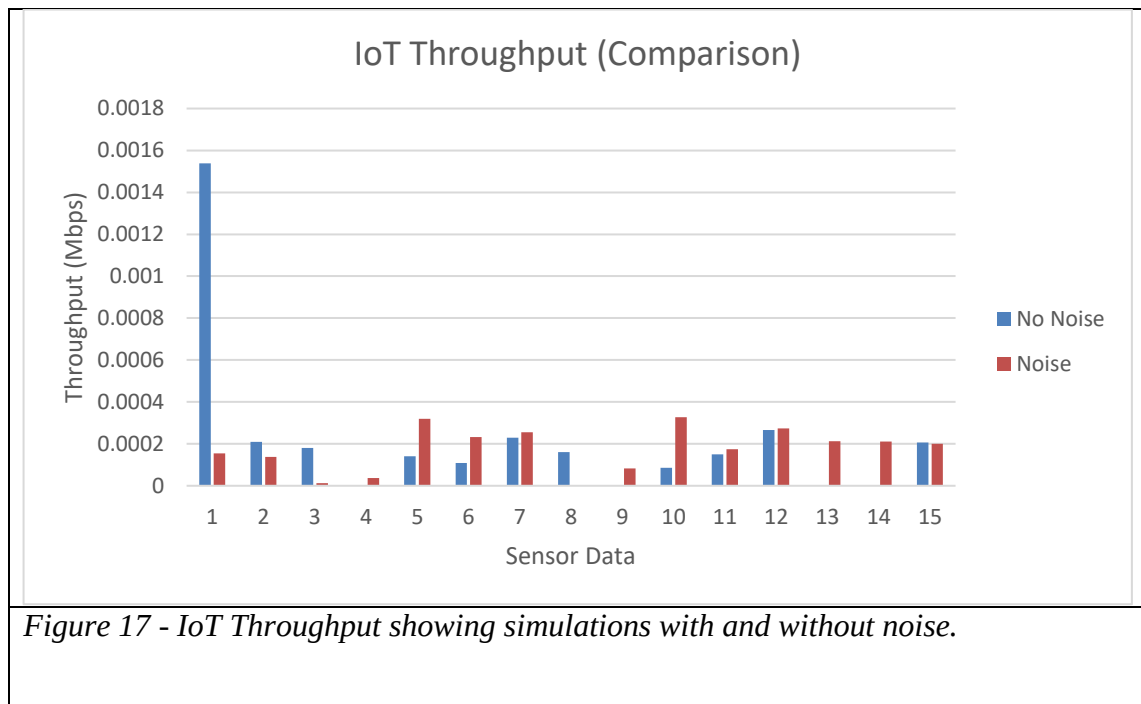
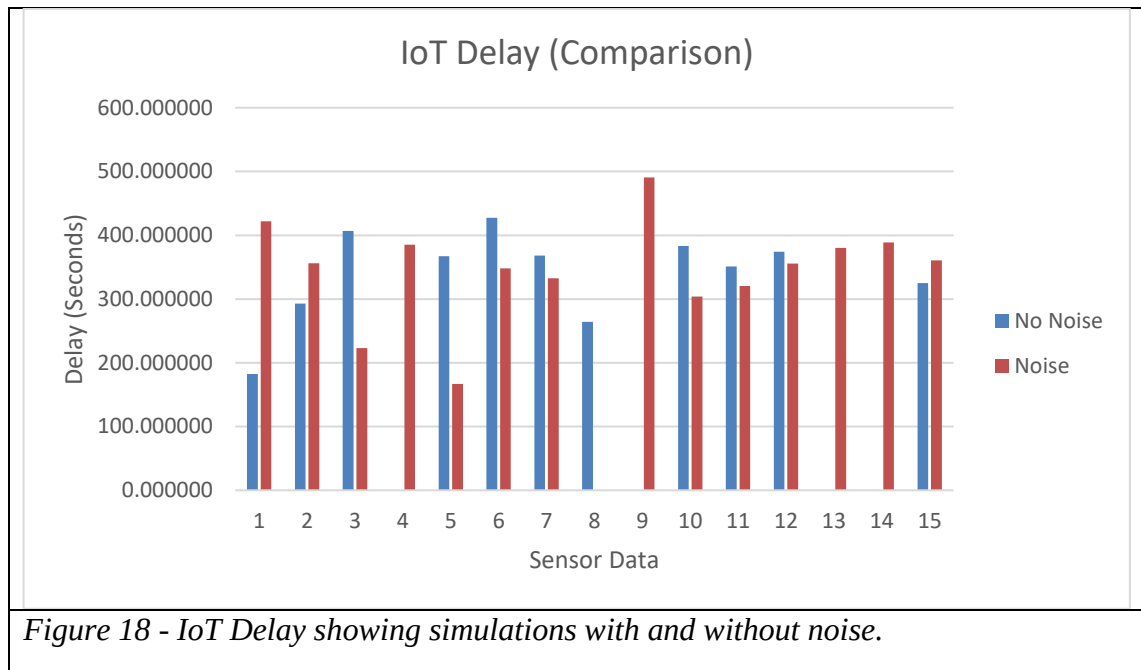


Figure 18 shows the comparison of delay on both networks, from an initial look at the data it is inconsistent with prior predictions but consistent with the rest of the metric for this network types. When looking at the no noise data the amount of delay through each node varies a lot, the that node experiences the highest delay with a time of 427.362888 seconds is node 6 whilst the node of on the no noise simulation with the least is node 1 with 182.375112 which reflects the throughput and the packet loss of previously studied data. With a difference 80.3584% which is a lot less of a difference when compared to the difference in percentage from throughput and packet loss.

When looking at the noise only data it can be said that node 5 experiences the least amount of delay amount the range of sensors, with a delay time 166.669028 seconds this is less than node 1 on the no noise simulation. The highest amount of delay comes from node 9 which manages to achieve a delay of 490.511148 seconds and is the highest delay from both simulations. This is a difference of 99.555% which again is a smaller amount of difference between the highest and lowest performing node than the rest of the recorded metrics of this simulation types. When the author averages out the network delay from both simulations, it becomes apparent that overall the no noise network experienced less delay with an average time to 249.5045 seconds than the noise based simulation which has an average time of 322.2286 seconds this is a percentage difference of 25.4399% this is to be expected as the noise influence simulation should perform worse.



So far, the author has review and pointed out some interesting areas within the IoT simulation, even with the anomalies in the data it is clear that the noise-based simulation performed worse, even if only by a small margin. The data overall also shows that some of the nodes perform better in some cases and when looking at the topology as seen in figure 6 of the design chapter there is no correlation between the performance of node and their relative distance as some of the node are closer to the network sink but still perform worse than those further away, the author will discuss this more in the discussion section of this chapter.

### 5.3 WLAN Results

As previously mentioned once the IoT simulation were run the author thought it was be useful to run a simulation using a conventional WLAN, this allows the author to make an informed decision about what type of network should be. Figure 19 shows the WLAN packet loss statistics, from an initial look it can be said that the packet loss for both networks is low. Looking at the no noise data only it can be said that most node performed well with the lowest performing node being node 15 still able to achieve a success rate of 95.7433%. The highest performing node was node 9 with a 100% success rate making the difference between highest and lowest performing nodes only 4.34927%. overall in terms of packet loss the WLAN network with no noise seem to perform as expected.

When it come to the network that include noises that when the data starts getting unusual. The noise-based network manages to have 2 nodes with the highest performance of 100% packet delivery which were nodes 13 and 14. The lowest performing node on the noise-based WLAN in terms of packets loss was node 10 with a successful delivery rate of 99.46% creating a difference of 0.541462%. Even though node 10 is the lowest performing it is still well above the lowest performing on the no noise simulation. The average packet loss for the no noise simulation is 99.3233% success rate but the average packet loss for the noise simulation was 99.8120% which even though it's a percentage increase of 0.4490822% it still shows the noise-based simulation performed better in terms of packet loss.

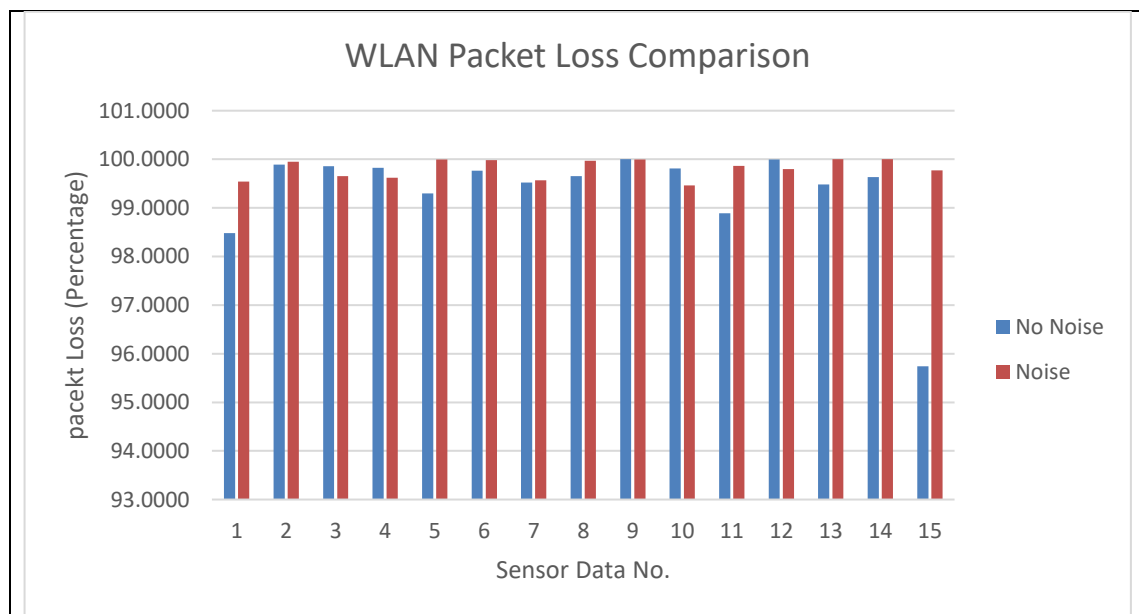


Figure 19 – WLAN Packet loss showing simulations with and without noise.

Figure 20 shows the throughput statistics for the WLAN experiments, once again the data is all over the place and require a deeper look into what it shows. By looking at only the no noise data it can be said that there is a lot of variability between the node the highest performing node was node 9 with a throughput of 0.584Mbps whilst the lowest performing node was node 15 with a throughput of 0.559141Mbps this makes the difference of 4.34924%, this shows the variability in the WLAN simulation.

From looking at the noise-based WLAN throughput once again the performance seems to be better with the interference added. The highest performing node on the noise-based simulation in terms of throughput was node 13 and 14 and with a throughput of 0.584Mbps. the lowest performing node on the noise-based simulation is sensor 10 with a throughput of 0.580846Mbps this is a percentage difference of 0.541531% compared to

the difference of the no noise simulation. The average throughput of the no noise simulation is 0.5800Mbps whilst the noise-based simulation average is 0.5828Mbps, this means the noise-based network perform 0.481596% better than the no noise simulation.

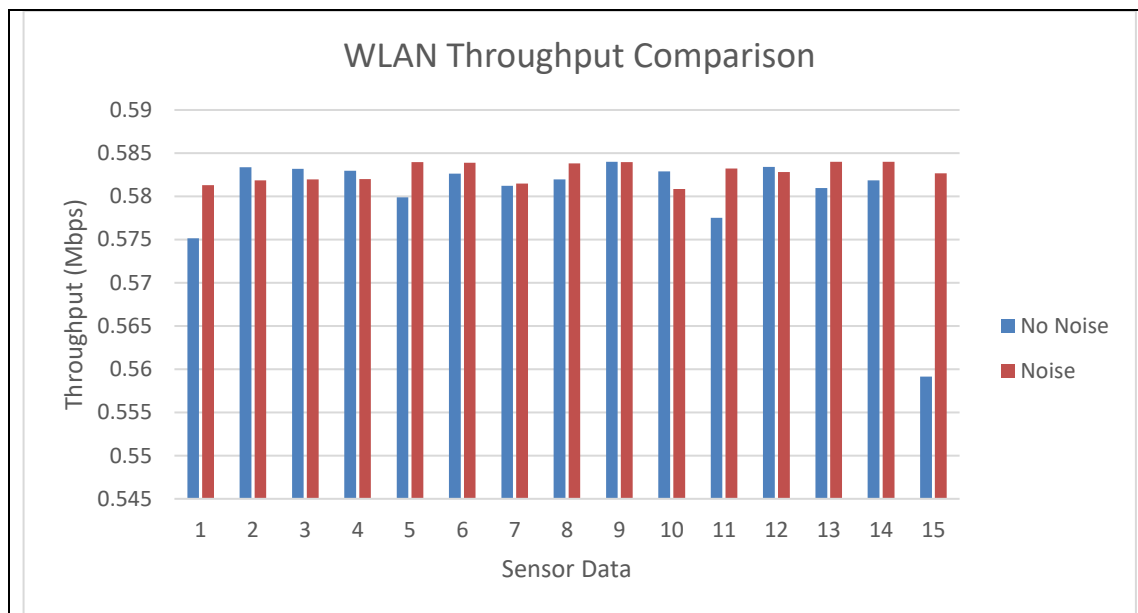
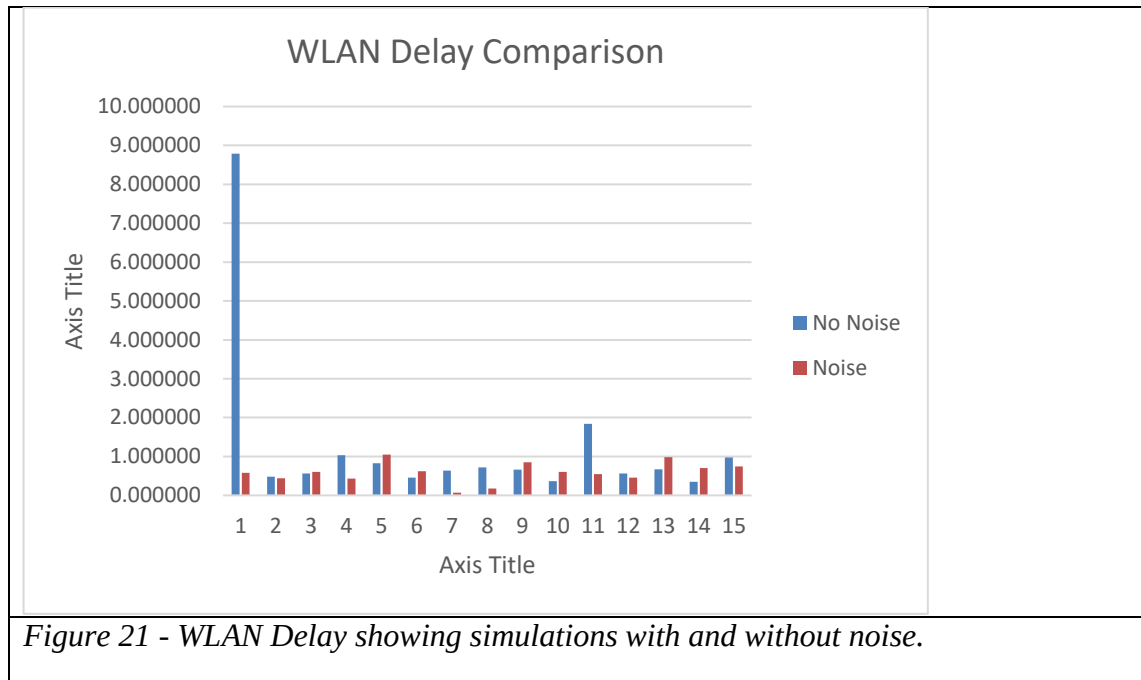


Figure 20 - WLAN Throughput showing simulations with and without noise.

Figure 21 shows the WLAN delay comparison statistics. The data is once again hard to make sense of. Just by looking at the no noise data it can be said that it experiences a lot of delay with the highest delay appearing on node 1 with 8.788343 seconds of delay, the lowest level of delay on the no noise network presented itself on node 14 with 0.346446 second. The calculated difference between the highest and lowest amount of delay was 184.83%.

Looking at the noise only data, it can be easily said that there is less delay, and this might be the case when looking at the other metrics mentioned so far. The highest amount of delay was experienced on node 5 with 1.046299 seconds which is low compared to the noise experienced on the no noise data. The lowest amount of delay was experience on node 7 with only 0.072955 seconds, that's and difference of 173.927%. which is a lower difference of delay than the no noise network. The average delay for the no noise network was 1.2621 seconds whilst the average on the noise-based simulation was 0.5916 seconds once again showing the simulation with noise performed better with a decrease in delay of 71.6823%



#### 5.4 IoT and WLAN Comparison

To gather a better understanding of the performance comparison of both the IoT and WLAN network the author took the simulation data with and without noise and averaged them to create a good midpoint of the data. With this the author was able to compare the results in a more realistic manner as the proposed network most likely will not suffer as much interference as simulated in the experiment.

Figure 22 shows the average packet loss comparison, this graph shows the massive disparity between the average IoT and the average WLAN statistics. The sensor nodes on the WLAN simulation all managed to achieve about 97% packet delivery on average of course, whilst the IoT network only managed to reach a 0.145% delivery of packets on the best performing node. This is a large gap with 199.40% difference between the two. The IoT network average for packets that successful transmitted through the network is 0.033696296%, whilst on the WLAN network the average for the whole network is 99.56166667% of packets successfully delivered. This is a massive increase of 199.865% in the packet delivery between IoT and WLAN.

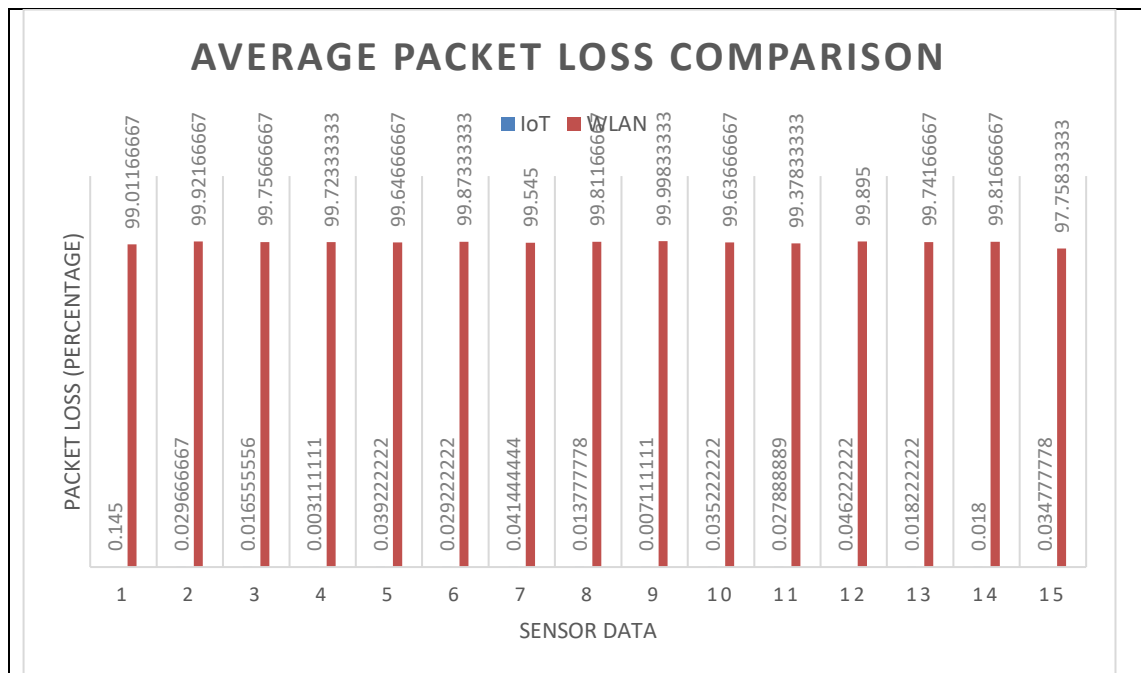


Figure 22 – Average per node packet loss of IoT and WLAN comparison

The throughput of the two networks averaged out shows very similar results to the packet loss as seen in figure 23 with the WLAN being able to reach 0.57Mbps on average at node one, which in comparison to the other nodes on the wireless local area network is low as the rest were able to reach 0.58Mbps on average. When looking at IoT network simulation the author has observed that highest throughput a node was able to reach was node 10 at 0.0008465Mbps which is a difference of 199.407% between the lowest throughput on WLAN and the highest on IoT. The total network average for throughput on the IoT simulation is 0.000196867Mbps, whilst on the WLAN network the average network throughput is 0.581401137Mbps which is calculated as a 199.865% difference between the two network averages.

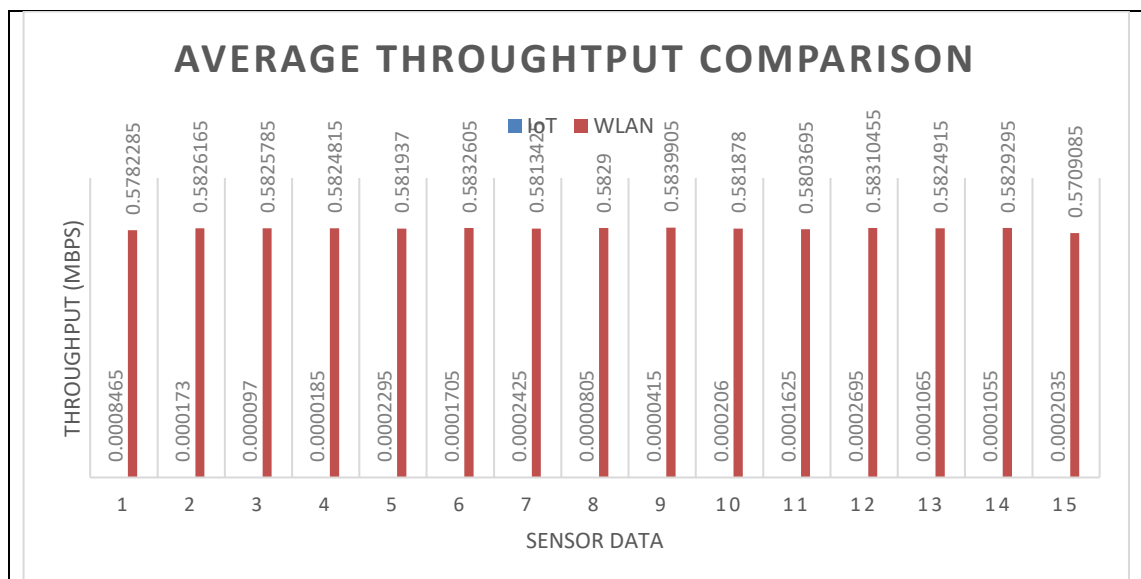


*Figure 23 - Average per node throughput of IoT and WLAN comparison*

The delay of both networks on a per node average shows results consistent with those previously mentioned in this section. The average per node delay on the WLAN simulation shows that it experiences a large decrease in delay in comparison to the IoT network. From figure 24 node 8 has the least delay in the IoT network but that is still a massive 132 seconds of delay on average. The highest amount of per sensor average delay on the WLAN is node 1 with an average delay of 4.6 seconds. This is a 186.53% difference between the two. The highest amount of delay experienced on the IoT network was 387 seconds, this is a large amount and can be problematic for the implementation of the proposed network. The average network delay for the IoT simulation is 285.8665281 seconds and the average network delay for the WLAN simulation was calculated at 0.926822551 seconds this is a 198.707% percent difference in the amount of delay experienced between both simulations.

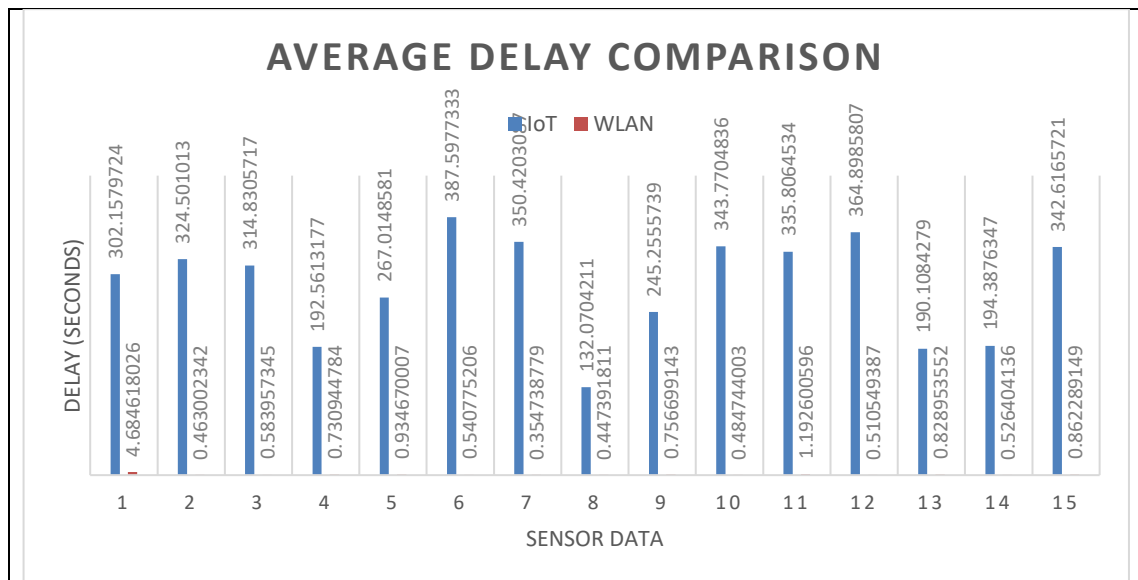


*Figure 24 - Average per node delay of IoT and WLAN comparison*

## 5.5 Result Discussions

From the results mentioned in this chapter there are many discrepancies within the both data sets. The author observed many instances where nodes in both the IoT and WLAN simulations performed better than the same nodes on the simulations without noise. The author ran these simulations numerous times and the same pattern was occurring, setting as we changed and even application types but still the issues presented itself. The author finally discussed the finding with a fellow colleague and discovered that the same problems were presenting on the work of others. The colleague contacted Tetcos, the

creator of the simulation software Netsim and support staff at Tetcos could not find the where the problems was coming from. The author has been assured that the problem would be solved in the next large update for the software, but this is a few months down the line, and this is time that the author does not have. Looking at the results the best option for the wireless sensor network is a WLAN as it boasts overall better metrics with a decrease of 198.707% of delay compared to the IoT, an increase of 199.865% in throughput and an increase of 199.865% in the packet delivery. This is a well-known fact but, in this case, it is supported by the experiment conducted and the work conducted by N. Ahmed et al[63] as mentioned in the related works section on this project . With the choice the author has made it is also possible to save on costs and the sensors can be integrated with the WLAN network already in place at the site. The author also knows that with a WLAN power consumption of the nodes increase and thus might be a downside, but the performance and stability of the network outweighs the power consumption. When taking into consideration the topology of the network it became clear that the distance played no part, the author initially believed that the IoT network would struggle with the distances but that was not the case, the author believes that the simulation software might have effected this measurement so topology and distances have not be discussed as much as the author would have liked. The authors decision for using a WLAN is supported by the work of another student who implemented a similar network and showed very favourable results of throughput between 9-28Mbps, packet loss of 0% and a delay of between 8 – 12 microseconds[67].

## 5.6 Conclusion

In conclusion the author has examined the result of both IoT and WLAN simulation with and without noise paying close attention to the anomalous data found, the results were inspected and statics on the average and the percentage defences were presented. The author then averaged out the noise and no noise results for each node on each network type and then compared them. The results clearly show that a WLAN would be best for the proposed sensor network. The author used the results to reinforce decisions made about the future types of network that would be best suited for down to earth. The author has decided that the best possible solution for the network based on the experiment is a WLAN network as it boasts better performance, even though it comes at a cost of power consumption.

## **Chapter 6 – Conclusions and Recommendations**

Throughout this report the author has conducted a lot of work based around research and experimentation. The author believes that the aim of this project which was to “*gather an understanding of how a wireless sensor network designed for detecting wood moisture content using IoT sensors performs under the most optimal conditions.*” Has been met. With the completion of all 5 objectives the author would regard this project as a success. The author conducted research around the common protocols used in IoT and Sensor Networks such as 802.15.4 and the technologies that build upon this standard such as Zigbee, from researching this area the author has learned that Zigbee provides a low power solution for wireless sensors at the cost of bandwidth, range and computational capacity of the nodes. The author also researched the newly developed LoRa technology which boasts a higher range than Zigbee and a slightly higher bandwidth and speed. Whilst looking into the other wireless technologies used the author mentioned the 802.11 standard which is widely used in sensor networks in homes, the security issues surrounding all these technologies were also discussed in relation to the potential attacks that could occur on these networks. The author performed some research on the practicality behind simulations and the common metrics used to measure performance. Finally, in the authors research were a few papers documenting the research of others in the field around simulating performance of wireless sensor networks, these were used to support the authors experimentation.

A strict methodology was developed which allowed for the accurate gathering of both primary and secondary sources of data and how the author would interpret that data, which as mentioned previous was the positivistic and deductive approaches research. For the experimentation, the designs of the networks were laid out including the topology and the technologies the author is attempting to measure, alongside a proper formulation of the problem that the author planned to solve within this project. within the design chapter includes a clear documentation of the implementation of the simulations, detailing the settings such as node settings and node positioning as well as the noise settings that were placed within the network.

Finally, the author took the results from the simulations and discussed the performance of both IoT and WLAN networks. The data was placed into a spreadsheet and displayed in graph form to analyse the data better. The author has some apprehensions about the data as mentioned in chapter 5 as there appears to be irregularities in what would normally be expected from these types of simulations

This chapter can be summarised as The IoT networks showed very low throughput but high packet loss and delay, whilst the WLAN network showed the opposite. Even though the data was not as expected with simulations showing that on some nodes the noise improved network performance and on others it degraded it as it should, the author believes that this data is good enough to support the recommendations that will be made in the end of this chapter.

From the work performed in this report the author recommends using an 802.11 based network preferably the most recent iteration of the protocol. The author recommends this due to the results from the experimentation, which clearly shows that with the network configuration that the company wishes to implement an 802.15.4 network would not only have to low of a performance but also the range might cause a decrease in network performance. Whilst 802.15.4 boasts more power efficiency, in an office environment when power is readily available then power consumption is not a big determining factor. With the implementation of an 802.11 network, costs can be saved as the nodes can be built into the already existing WLAN present at the site. The author also recommends further investigation through physical means as to the viability of an 802.15.4 network as the results shown have been skewed by the bugs in the simulation software.

## **Chapter 7 – Reflections and Future Work**

### 7.1 Introductions

In this final chapter the author will discuss the process of this project and reflect on areas on note that could be improved through different methods. The author will discuss the many aspects of this project such as the lessons that were learnt throughout the 3 months of time spent on this work. Improvements on this work will also be outlined in this chapter to understand where the author could have made this work better or more accurate. Discussions about the barriers experienced throughout this project will also be presented in this chapter as it is important to note where areas of this project could be streamlined with more forethought. Finally, the author will end this chapter by outlining ideas that could be implemented in future works to build off or help projects such as this.

### 7.2 Reflections

Throughout the project many lessons have been learnt that the author believes would be beneficial for future work. The first lesson learnt was time management, had the time of this project been managed more efficiently then the author might have been able to try many different methods of achieving the aim such as changing the simulation software, even though this would have taken more time as other programs are vastly more complex, had the authors time been managed properly then this might have been overcome. A second lesson learnt was to look at problem from a different perspective, when the simulation software showed anomalous results the author repeated the experiment many times and got similar results. Had the author reached out to other users within the university sooner, then the problem might have been discovered sooner and thus time could have been saved and appropriate action take.

The author experienced many barriers throughout the development of this project, the first being of course the access to the simulation software. As Netsim is only available in one lab within the university campus it makes constant access for the work being done difficult. This is made even more difficult when travel is considered as the author must travel a few miles to gain access. Fortunately, the author was able to overcome both barriers and bring the project to completion

Looking back on this project the author knows there are many areas where improvements can be made, or things done differently. The first improvement the author would have

made to this project is changing the simulation software. There are many different types of software on the market that perform the same function, but the author decided to go with Netsim due to familiarity and availability. Other programs that could have been used include NS3, a Linux based simulation that requires knowledge of the C programming language, while the author has no experience with this software looking back it would have been a good opportunity to learn. More simple programs such as OPNET/ Riverbed Model or Qualnet would have been suitable if they were available for a more reasonable price. The author would like to have performed more work on the energy consumption side of the network, while it is well known that 802.15.4 networks boast low power draw it would be beneficial to see how the two compare with performance to power over time. While this project is not technically constrained by power draw, future work or others using this work as a baseline might benefit from such detailed analysis. The final area of improvement would be to investigate a wider range of wireless technologies such as LoRa, Z Wave or LTE/4G/5G. The author knows that these technologies have increased in popularity over the years and investigating these might have increased the scope and relevancy of the work performed in this project.

### 7.3 Future Work

As with all projects and research it is important to look to the future and understand where this work can go if it was continued, the author has many thoughts on this. The first being that of simulating the actual nodes and what they could do in terms of data gathering. The author knows a few online tools that allows for the simulation of nodes using Raspberry Pi's and Arduino's such as Circuito.io or TinkerCAD, but they were not in depth or detailed enough to allow for actual testing of data and of the programming of the boards. It is the authors opinion that if this could be done then a more power efficient and better performing network could be implemented with the use of open sources designs.

Another area of future work the author is interested is the simulation software. There have been many issues with the current programs available on the market from the difficulty of the software to the inaccessibility due to the price range. The author has an idea to develop a more user friendly and open wireless network simulator using C or Python programming languages. With the ability to simulate many wireless network protocols, routing protocols, simulate real time data (including incremental i.e. every 5 mins) and with wider integration into programs such as MATLAB for noise or electrical engineering

suites such as TinkerCAD, Circuito.io, Autodesk Eagle or Virtual Box for testing and simulation of nodes or end users and host operating systems. While this is a lot of work it is the authors hope that such as task is implemented by other researchers in the future.

Finally, as this has been an attempt to find the best possible network solution for Down to Earth to monitor the structural integrity and moisture content of timber framed buildings it is natural that the next step in this work would be to implement the network using tools and equipment that would satisfy the criteria set by the company. Hopefully this will lead to the development of new methods and new technologies that could be brought into the wider world and expanded uses besides just moisture content.

## References

- [1] GSMA, “Understanding the Internet of Things (IoT),” 2014.
- [2] “Energy Savings from the Nest Learning Thermostat: Energy Bill Analysis Results.”
- [3] D. for B. I. & Skills, “SMART CITIES: Background paper,” 2013.
- [4] S. P. Mohanty, U. Choppali, and E. Kougianos, “Everything you wanted to know about smart cities,” *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 60–70, 2016.
- [5] D. Emc, “Smart Cities and Communities GDT Smart City Solutions on Intel ®-based Dell EMC infrastructure,” 2017.
- [6] T. Malche and P. Maheshwary, “Internet of Things (IoT) for building smart home system,” *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, no. February 2019, pp. 65–70, 2017.
- [7] M. H. et Al., “Internet of Things (IoT) Enabled Smart Animal Farm,” vol. 7, pp. 2067–2072, 2016.
- [8] S. Vaishali, S. Suraj, G. Vignesh, S. Dhivya, and S. Udhayakumar, “Mobile integrated smart irrigation management and monitoring system using IOT,” *Proc. 2017 IEEE Int. Conf. Commun. Signal Process. ICCSP 2017*, vol. 2018-Janua, pp. 2164–2167, 2018.
- [9] MCMC, “Internet Users Survey 2018.”
- [10] S. Banerji and R. S. Chowdhury, “On IEEE 802.11: Wireless LAN Technology,” *Orig. Publ. Int. J. Mob. Netw. Commun. Telemat.*, vol. 3, no. 4, 2013.
- [11] H. A. M. Saad, G. A. M. Abdu, M. A. Abbas, and H. Ali, “MAC Layer strategies in Cognitive Radio Networks DSA protocols for cognitive networks MAC Layer strategies in Cognitive Radio Networks DSA protocols for cognitive networks,” no. September, pp. 0–12, 2018.
- [12] D. Bertsekas and R. Gallager, “Second Edition Data Networks.”
- [13] M. S. Ghasst, *802.11 Wireless Networks*. 2005.
- [14] “PHY Basics: How OFDM Subcarriers Work — Revolution Wi-Fi.” [Online]. Available: <http://www.revolutionwifi.net/revolutionwifi/2015/3/how-ofdm-subcarriers-work>. [Accessed: 22-Aug-2019].
- [15] “Engineering Hub | Standards Showdown: 802.11 Standards Side-by-Side.” [Online]. Available: <http://www.l-com.com/blog/post/2017/07/20/Standards-Showdown-80211-Standards-Side-by-Side.aspx>. [Accessed: 20-Aug-2019].
- [16] S. Wong, “The evolution of wireless security in 802.11 networks: WEP, WPA

- and 802.11 standards,” *SANS Inst. Inf. Secur. Read. Room*, 2019.
- [17] M. Vanhoef, K. U. Leuven, and F. Piessens, “All Your Biases Belong To Us: Breaking RC4 in WPA-TKIP and TLS.”
  - [18] T. Sato and P. Moungnoul, “Hardware Amount Evaluation of the Improved WEP on an FPGA,” *2013 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, 2013. [Online]. Available: <https://ieeexplore-ieee-org.ezproxy.uwtsd.ac.uk/stamp/stamp.jsp?tp=&arnumber=6559629>. [Accessed: 22-Aug-2019].
  - [19] T. Ahmed, B. Gali, A. Babiker, and N. Mustafa, *A Comparative Study between WEP, WPA and WPA2 Security Algorithms*, vol. 4. 2013.
  - [20] S. Malgaonkar, R. Patil, A. Rai, and A. Singh, “Research on Wi-Fi Security Protocols,” 2017.
  - [21] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, “A survey on wireless security protocols (WEP,WPA and WPA2/802.11i),” *Proc. - 2009 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2009*, no. May 2014, pp. 48–52, 2009.
  - [22] A. Networks, “WPA3 AND ENHANCED OPEN: NEXT GENERATION WI-FI SECURITY.”
  - [23] G. Metric, “Wi-Fi Security Evolution - How we ended up in WPA3?” [Online]. Available: <https://www.grandmetric.com/2018/07/06/ended-wpa3-wi-fi-security-evolution/>. [Accessed: 22-Aug-2019].
  - [24] Actility, “LoRaWAN™: global standard for Low Power Wide Area IoT networks,” 2019.
  - [25] F. & Sullivan, “Growing Industry Applications of LPWAN Technologies A Frost & Sullivan White Paper.”
  - [26] C. V. and L. Bassang, “LoRa White Paper - Project NPR : LPWAN-VPN,” 2018.
  - [27] D. Ismail, M. Rahman, and A. Saifullah, “Low-Power Wide-Area Networks: Opportunities, Challenges, and Directions,” 2018.
  - [28] S. Ristov, “LOW POWER WIDE AREA NETWORKS: THE ANSWER TO THE IIOT’S CONNECTIVITY NEEDS?,” 2018.
  - [29] T. Rheinland, “A technical overview of LoRa ® and LoRaWAN ™ What is it?,” 2015.
  - [30] M. I. Muzamir, H. Z. Abidin, S. A. C. Abdullah, and F. H. K. Zaman, “Performance Analysis of LoRaWAN for Indoor Application,” 2019, pp. 156–159.

- [31] A. Lavric and V. Popa, "Internet of things and LoRaTM low-power wide- area networks challenges," in *Proceedings of the 9th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2017*, 2017, vol. 2017-January, pp. 1–4.
- [32] A. Gladisch, S. Rietschel, T. Mundt, J. Bauer, J. Goltz, and S. Wiedenmann, "Securely connecting IoT devices with LoRaWAN," in *Proceedings of the 2nd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2018*, 2019, pp. 105–112.
- [33] R. Sanchez-Iborra *et al.*, "Internet access for LoRaWAN devices considering security issues," in *2018 Global Internet of Things Summit, GIoTS 2018*, 2018.
- [34] "End-To-End Secure LoRaWAN: Secure Devices with Key Management from Provisioning to Operations."
- [35] "The Evolution of Wireless Sensor Networks Origin and History of Wireless Sensor Networks."
- [36] R. Sherwood and S. Chien, "Sensor Web Technologies: A New Paradigm for Operations."
- [37] "Internet of Things: Wireless Sensor Networks."
- [38] G. Tuna, V. C. Gungor, and K. Gulez, "Wireless sensor networks for smart grid applications: A case study on link reliability and node lifetime evaluations in power distribution systems," *Int. J. Distrib. Sens. Networks*, vol. 2013, 2013.
- [39] H. K. and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*. 2007.
- [40] Y. Li, B. Li, M. Qian, and L. Wang, "Application of wireless sensor networks in healthcare.," *Zhongguo Yi Liao Qi Xie Za Zhi*, vol. 37, no. 5, pp. 351–354, 2013.
- [41] H. Kaur, R. S. Sawhney, and N. Komal, "Wireless Sensor Networks for Disaster Management," *IJARCET J.*, vol. 1, no. January, pp. 129–134, 2012.
- [42] D. Bhattacharyya, T. hoon Kim, and S. Pal, "A comparative study of wireless sensor networks and their routing protocols," *Sensors*, vol. 10, no. 12, pp. 10506–10523, 2010.
- [43] M. Hamza Akhlaq, M. Arif, I. Ullah Khan, N. Azim, and S. Ahmad, "Advantages, Applications and Research Challenges in Wireless Sensor Networks," *Ijmca*, vol. 5, no. 2, pp. 041–046, 2017.
- [44] P. Tiwari, V. P. Saxena, R. G. Mishra, and D. Bhavsar, "Wireless Sensor Networks: Introduction, Advantages, Applications and Research Challenges Introduction to Wireless Networks," *HCTL Open Int. J. Technol. Innov. Res.*

- ISBN, vol. 14, pp. 2321–1814, 2015.
- [45] D. V. T. M. Logambal, “Applications of Wireless Sensor Networks: An Overview.”
  - [46] N. P. Mahalik, *Sensor Networks and Configuration*. 2007.
  - [47] E. al. Fabian Mieyeville, “Energy-Centric Simulation abd Design Space Exploration for Wireless Sensor Networks.”
  - [48] “Introduction to Zigbee Technology.”
  - [49] Y. X. Li, Lian-Qin, and Qian-Liang, “Research on wireless sensor network security,” in *Proceedings - 2010 International Conference on Computational Intelligence and Security, CIS 2010*, 2010, pp. 493–496.
  - [50] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Wormhole Attacks in Wireless Networks.”
  - [51] A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J.-C. Tsou, “Man-in-the-middle-attack: Understanding in simple words,” *Int. J. Data Netw. Sci.*, no. January, pp. 77–92, 2019.
  - [52] S. Gangan, “A Review of Man-in-the-Middle Attacks.”
  - [53] A. A.-F. Mohsen Guizani, Ammar Rayes, Bilal Khan, *Network Modeling and Simulation - A Practical Perspective*, 1st ed. Wiley, 2010.
  - [54] T. Issariyakul and E. Hossain, “Introduction to Network Simulator NS2.”
  - [55] “NetSim-Network Simulator & Emulator | Home.” [Online]. Available: <http://www.tetcos.com/>. [Accessed: 04-Oct-2017].
  - [56] Mike Fuszner, “Graphical Network Simulator 3.”
  - [57] L. Qiu, Y. Zhang, F. Wang, M. K. Han, and R. Mahajan, *A General Model of Wireless Interference*. 2007.
  - [58] “A Farpoint Group White Paper The Invisible Threat: Interference and Wireless LANs,” 2010.
  - [59] S. A. Jyothi, A. Singla, P. B. Godfrey, and A. Kolla, *Measuring and Understanding Throughput of Network Topologies*. .
  - [60] “How to Properly Measure and Correct Packet Loss.”
  - [61] ESOA, “How Latency Affects the User Experience.”
  - [62] G. S. Rani, T. S. S. Krishnan, V. Daiya, J. Ebenezer, and S. A. V. S. Murty, “Performance analysis of Wireless Sensor Network,” *Souvenir 2014 IEEE Int. Adv. Comput. Conf. IACC 2014*, no. December 2014, pp. 282–287, 2014.
  - [63] N. Ahmed, H. Rahman, and M. I. Hussain, “A comparison of 802.11ah and 802.15.4 for IoT,” *ICT Express*, vol. 2, no. 3, pp. 100–102, Sep. 2016.

- [64] C. E. Campbell, K. Loo, H. A. Kurdi, and S. Khan, “Future Green Multichannel Multi-radio Wireless Sensor Networks,” vol. 3, no. 1, pp. 96–104, 2011.
- [65] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods For Business Students*. .
- [66] E. Ridd, “Comparing the Performance of Routing Protocols on Mobile Ad Hoc Networks (MANET),” 2018.
- [67] S. Thomas, “Monitoring Environmental Effects on a Building’s Structure with the use of Wireless Sensor Network,” 2019.