

“Detection of Wood Moisture Utilising Environmental Sensors by simulating Internet of Things Sensors” - Project Proposal

by Ethan Ridd

FILE	2785_ETHAN_RIDD_DETECTION_OF_WOOD_MOISTURE_UTILISING_ENVIRONMENTAL_SENSORS_BY_SIMULATING_INTERNET_OF_THINGS_SENSORS__487176916.DOCX (183.29K)		
TIME SUBMITTED	08-MAY-2019 01:42PM (UTC+0100)	WORD COUNT	4667
SUBMISSION ID	106651808	CHARACTER COUNT	23710

“Detection of Wood Moisture Utilising
Environmental Sensors by simulating
Internet of Things Sensors”

Research Proposal

Ethan Ridd

Contents

1. Introduction.....	3
2. Aims and Objectives.....	3
3. Literature Review.....	3
4. Research Methods.....	7
4.1 Philosophy.....	7
4.2 Approach.....	7
4.3 Strategies.....	7
4.3.1 Experimentation.....	7
4.3.2 Document Review.....	7
4.4 Risks & Limitations.....	8
4.5 Data Evaluation.....	8
5. Resources & Planning.....	8
5.1 Resources Required.....	8
5.2 Gantt Chart.....	9
6. Conclusion.....	9
7. Reference List.....	9

1. Introduction

In recent years the process of monitoring and data collection has slowly moved in a more modern direction, through the uses of wireless sensors. This technological revolution has been branded the Internet of Things (IoT) and has been the focus of many companies in terms of technological development. IoT allows for the devices such as temperature and humidity sensors to be connected wirelessly or through cable to the internet. This allows for many systems or devices to be monitored remotely from anywhere if there is an internet connection[1]. IoT can offer many benefits to a company or person, such as the ability to monitor systems on the go with live reading this allows the user to adapt and act on any issues that might present itself whether its in a small scale like at home with the heating being left on or in a massive company where a server farm is not being cooled properly. As with everything in life there is a downside to IoT. With devices connected to the internet there is the potential risk of an attacker gaining access and either damaging the equipment or stealing data. There are also privacy concerns with IoT, since everything will be monitored at once. In this report the author will outline plan for a major project which will help towards a master's degree. The author has been asked by an outside company called the Down To Earth Project[2], which specialises in helping people through outdoor activities. The company is also involved in eco-Friendly development of buildings using welsh timber. Welsh timber previously has not been found suitable for construction. The author has been asked along with a research partner to create a sensor network for Down to Earth to measure the change in the moisture content of the wood. The company then plans to use the results as a measure of the structural integrity. Down to Earth plans to bring the research of the structural strength of the wood to the welsh assembly government to propose plan of using the wood in other projects. The author will provide research into the current literature around IoT and environmental sensors. The author will outline the planned methodologies and experiments in this report.

2. Aims and Objectives

The Aim of the project is to understand how a wireless sensor network used for wood moisture detection through IoT sensors performs under the most optimal and least optimal environment.

The author plans to achieve this aim by following a strict set of objectives. They are as follows:

1. Complete comprehensive research into the area of IoT sensors, Environmental monitoring and network simulations. This will be in the form of a literature review.
2. Gather an understanding about what Down To Earth wants to achieve and an understanding about the area in which the proposed network will be located.
3. Develop an experiment methodology, that will be capable of testing the network under varying conditions
4. Develop noise using MATLAB
5. Run the experiment and gather vital data for analysis.
6. Make recommendations to improve network performance based on data gathered

3. Literature Review

I. What is IoT

The Internet of Things has gained a lot of popularity within the last few years, with many companies developing new technologies that fall into the category of IoT. IoT allows for a different array of sensors or appliances to be connected with each other and with the internet, this gives a large degree of control and flexibility. IoT essentially allows one to monitor and get updates from devices over the internet and act accordingly. IoT has seen a large surge in usage from the industrial sector to monitor machinery thus improving maintenance time and most importantly automation making the processes involved in production more efficient and cost effective[3]. IoT has made its way into the Commercial sector as well with anyone able to invest in this technology at a low price. Look at the Smart Thermostat by Nest

for example, the device allows users to control and monitor the temperature of their home from anywhere whilst also monitoring energy usage in comparison to the temperature of the home[4].

a. Common uses

IoT has been widely adopted in many industries and in numerous aspects of society. With more and more companies developing their own IoT devices that are used daily by millions work wide. Companies such as Philips, Google and Nest creating IoT devices such as lighting, home assistants and smart temperature controls[4]. The applications of IoT are numerous, one such application is the use of IoT in Automation both in home and in industry. In industry IoT has been used to monitor and assess the performance of industrial production machines, thus optimizing them for improved production rates[5]. One large application of IoT is Smart Homes, this allows the automation of certain appliances in the home for example, environment monitoring possibly reducing the cost of certain aspects of the home[6]. Smart homes usually comprise of numerous systems connected to the internet router of the home, devices such as the before mentioned Nest can be used for monitoring energy and heating usage. Other devices such as home intrusion system and fire detection has been known to be used in smart homes[7]. Smart Homes were just the start of this technological revolution with some countries taking this technology a step further with the implementation of smart devices into a city's infrastructure. Focusing on many areas of services that a city might provide such as transportation through intelligent transportation systems which link the various aspects of city wide transportation such as cars, buses and even less conventional methods of transport such as water and air transport[8]. IoT covers a range of applications which are too numerous to mention in this short review.

b. Advantages

IoT has many advantages that make it a very useful and widely adopted technology. One such advantage the ability to monitoring and control certain systems without the need to visit each system individually. This is saves time for the employees and allows for quick response to system malfunctions and faults[9]. Another advantage is easy communication between devices, where once devices were isolated, and data was stored on the individual devices alone. IoT allows for the devices to have a centralised system of storage and can be configured to allows devices to be dependent on each other. A third advantage of IoT is allowing the users to remotely interact with the systems through the internet, there are numerous examples of IoT devices that can be monitored or altered from a smart phone, this adds and extra layer of functionality[9].

c. Disadvantages

As with all technologies there are several disadvantages to IoT. One disadvantage of IoT is the power consumption, smaller sensors require a power source if they are out in the open. This can be an issue as battery technology still isn't capable of lasting long periods of time and with the sensor becoming more and more complex and with more functionality power consumption is a key area of improvement[10]. With IoT in certain situations such as automated security on smart homes, privacy has become a potential risk. Many have discussed the idea that IoT in the home invites potential attackers an avenue to gain information they would not normally be able to access. This includes things such as home security information through camera and sensors, that could be used against the owner[11]. Due to the small and wireless nature of IoT devices, bandwidth is a restriction and is often a concern when implementing these networks. The Bandwidth itself is reliant on the power of the device, and as mention previously power consumption is a major concern. As new technologies and new protocols get developed the bandwidth restriction might be somewhat eliminated[12].

II. Wireless Sensor Networks

The Internet of Things is made up of many types of networks but the focus of many is a wireless sensor network. A wireless sensor network is comprised of mainly small low-cost nodes, that transmit sensor

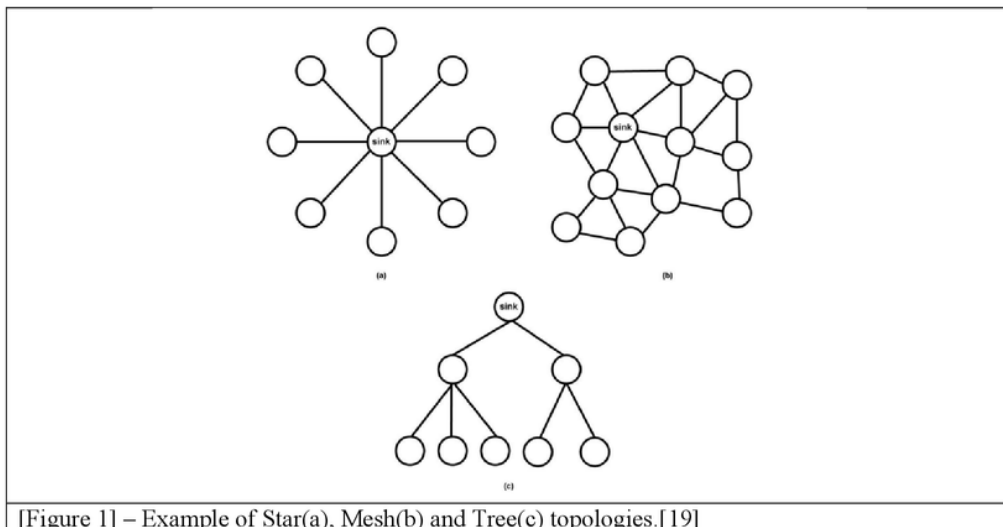
data to a hub. This is the basis of most IoT networks. These types of networks are suitable for all sorts of terrain from forests to the ocean. WSN can be structured into 2 architectures flat with the network connecting to a singular group of nodes, or hierarchical which organises the network into multiple layers[13]. There are many advantages of Wireless Sensor Networks such as the lack of fixed infrastructure reducing the costs of the network as the wireless nature of the network doesn't require costly cables[14]. There are also a few disadvantages of Wireless Sensor Networks as well such as the lack of security the access point is often exposed, and with more complex wireless configurations making it difficult to implement[15].

III. IoT Wireless Protocols

The popularity of IoT has led to the creation of many specialised wireless protocols. Many of these protocols boast low power and decent range. Wireless protocols allow for wireless devices to communicate with each other by sharing certain functions such as routing, addressing, neighbor discovery, modulation and transmission. Without the use of a wireless protocol the network would be unable to communicate, without standardised protocols the network would face numerous compatibility issues.

a. ZigBee

ZigBee is one such protocol developed specifically for the use of IoT devices, designed and developed by the ZigBee alliance as a low power solution for IoT devices following the 802.15.4 standard created and maintained by IEEE, though it is necessary to point out that these two are not the same protocol[16]. ZigBee boasts an interior range of 30m and an exterior (unobstructed) range of 100m, and an energy consumption of 25-35mA which compared to WIFI's 400mA is a major improvement and very suitable for IoT[17]. ZigBee employs the use of a network coordinator devices to maintain and control the nodes as ZigBee can support numerous nodes up to a theoretical 64,000. The coordinator is responsible for the information being transmitted over the network and the information about the numerous network devices[17]. ZigBee networks are very versatile with the network topology being able to be configured in numerous ways. The three most common topologies for Zigbee are Star, Mesh and Tree networks these topologies are best illustrated in Figure 1. Tree and Mesh network require the use of a ZigBee router to allow the nodes packets to be forwarded to the coordinator node[18].



[Figure 1] – Example of Star(a), Mesh(b) and Tree(c) topologies.[19]

ZigBee has been implemented worldwide in numerous IoT project and has seen numerous applications. Some applications currently in use include smart surveillance, light and heating controls, home security and even agricultural monitoring[20]. Zigbee has been very popular among IoT enthusiasts in the past

few years due to its flexibility and low power, but new technologies are always being developed and one such development is LoRa, Z-wave and even conventional WIFI networks are capable of supporting IoT

IV. IoT Security

As mentioned previously security and privacy are big issues for IoT, with the implementation of monitoring systems and sensors it is vital that the network is secured and able to prevent the loss of data and personal information to network attackers. Due to IoT being used in industrial, commercial and domestic environments, there is the potential for a security disparity to occur between the numerous settings. In this section the author will outline common attacks that are performed on IoT network and highlight some methods of securing the network.

a. Common attacks

As the size of the internet began to increase, so did the potential attack vectors through which an attacker can gain access to the networks. IoT has only increased the number of Intrusion points along with the number of devices that are susceptible to attacks. The author will outline 3 main attacks that commonly occur in IoT and Wireless Sensor Networks. The first common attack is Denial of Service or DOS, which involves the use of network flooding to prevent the use of the network. This can cause major disruption to the every day running of the network as legitimate packets are not able to pass through the network[21]. A blackhole attack is common, which works by an attacker impersonating a node within the network and intercepting the packets being transmitted, then just dropping the packets[22]. This makes it seem like there is a blackhole sucking in packets, causing a lot of disruption to the network effecting performance and potentially shutting the network down. A man in the middle attack is like a blackhole attack where a node is placed within the network and acts as a legitimate node[23]. Once this is complete the attacker will intercept packets that are meant to be router somewhere else and keep the data for malicious purposes. This is usually done in connection with an ARP Poisoning attack.

b. Securing IoT networks

The security of an IoT network is vital to ensuring the data is protected and secure from potential threats. There are many ways of securing the network from these potential threats mentioned previously. The data within the network could be encrypted, this would prevent the attacker from being able to use that data gathered from a man in the middle attack[24]. Another method of ensuring the network is secure is access control and authentication, this ensures that only those with the correct permissions can access the network thus preventing unauthorized access. Finally, for securing an IoT network it is good practice to have all devices updated with the latest firmware and security patches, this would hopefully prevent the weakness on a device level from being exploited.

V. Conclusion

In conclusion IoT has Rapidly become a major trend in the networking industry with numerous companies developing their own technologies such as nest or google home. IoT and WSN provide many advantages to the user with improved data gathering speed, data accuracy and the reduction of wasted time as sensor data is automatically transmitted over the network. With the increase in this new trend, new protocols have emerged such as ZigBee or LoRa. As is expected with new technologies there are many security issues that need to be accounted for such as blackhole attacks or man in the middle. The author has conducted a small amount of research into the field of IoT and Wireless Sensor Networks, as this is such a large field more in-depth research will be conducted into the field prior to the projects beginning.

4. Research Methods

The methodology to the authors research is very important as it defines the way that the research will be conducted. The author has investigated various aspects of research methods for the project. In this section the author will lay out plans for the research methodology.

4.1 Philosophy

When considering research philosophies, it is good to consider all possible approaches, there are 5 research philosophies that are used by researchers in various fields. For this research project the author has concluded that the work falls under the Positivism philosophy. Positivism follows the principle that the object or entity that is being observed is not likely to show change on its own, thus to observe change a variable must be altered[25]. Positivism is often referred to as the scientific method which relies on observable changes and facts, the values and personal ideas of the research would remain separate as the researcher would rely on the data collected to generate an answer to the hypothesis that has been formulated.

4.2 Approach

The research approach is how a research would come to conclusions, there are 2 main schools of thoughts that dominate research the first is inductive in which multiple tested facts are combined to conclude about an area of research. The second school of thought is Deductive which the author has decided would best suit this research project. The deductive approach is a method of reason that uses logical steps to conclude some research based of observations[26]. Research done under the deductive approach is often repeatable as it provides the steps that prove a hypothesis are logical and thoroughly tested, if the experiment proves a hypothesis wrong repeatedly then there is only one interpretation to be gained using the deductive approach[27].

4.3 Strategies

The research strategies are how a researcher intends to collect data to support the hypothesis or answer the research question. There are many strategies that depends on the field of research and whether the research is being conducted on living things which are subject to change or objects which are often not subject to change the author has Identified 2 strategies that could be used to collect data to achieve the aim.

4.3.1 Experimentation

The author has an idea of how he plans to meet the aim using an experiment in the form of a simulation. The simulation would be a digital version of the proposed network and following the approach and philosophies mentioned earlier the author would change variables such as noise to understand how the network would perform. The author has some experience using network simulations tools and has in past work noticed that the interference doesn't seem to be flexible enough, so the author has concluded that a less rigid way of adding interference must be used. The author has been told by fellow colleagues that a good way of creating network interference is using MATLAB Simulink software to generate noise and then push it into the network simulation program called Netsim.

4.3.2 Document Review

The Author will perform thorough research into the field of IoT, wireless sensor networks, Environmental Monitoring and simulation in general. To do this the author will look through many digital libraries such IEEE Xplore Library and Google Scholar. The author will also go through the universities digital library of research conducted by their own staff and PHD students. Despite the outdated information found in certain books the author believes that they can be used to conduct vital background research, as the universities library has a vast number of books on the topic the author will use this resource in the document review.

4.4 Risks & Limitations

With any research project there are naturally some risks and some limitations. To successfully complete a project, it is wise to look ahead and attempt to predict some risks and limitations. The author has thought about any potential risks that the project might create, fortunately as a result of the work mainly being a simulation there are few risks that involve others besides the author. One risk could be that the software or hardware would become unavailable or unstable for use at a point in the project, this could potentially cause some setbacks and thus delay the project past the due date. To counteract this the author will research numerous simulation programs and find alternatives as a backup just in case such an event could arise. The author has also considered that loss of any data collected could result in the project being unable to achieve its aims, thus the author must implement an air tight back up policy to prevent the data being lost and costing hours of work.

Limitations like risks must be seen before the project is implemented as at this stage is easy to mitigate the potential harm the limitations have on the project aim. The author has thought about some limitations of the software he plans to use, Netsim is available for use as it is provided by the university. This is a limitation as due to the licensing of the software the author can only use the software in 1 room as of May 2015, this could possible change in the future. This requires the author to plan the date and duration on when to use the equipment, as it could clash with the work of other students working on their own project or coursework. The author also has plans to create noise within the simulated network by designing it on MATLAB's Simulink package and pushing the code through to Netsim, as far as the author is aware this is possible with a moderate amount of complexity. Should any issues arise with this method then it could limit the range of interference that could be used to affect the network. To negate the limitation the author will go through many steps of research, implementation and testing of the integration between the two pieces of software before the simulation is run and data gathered.

4.5 Data Evaluation

The data gathered will be evaluated in a quantitative way, this means that when looking at the data the author will focus on the numerical values of the data and not the quality of how it was gathered. The data gathered will be Delay, Throughput and Packet Loss, these have been chosen by the author because they are the industry standard performance metrics when looking at a how well a network performs. The author will take the data and place it into a spreadsheet for easy evaluation and graph creation, this allows for the easy identification of trends and patterns within the data. Once the data has been collected and analysed the author will then attempt to make recommendations for improving the network performance, if any improvements can be made at all.

5. Resources & Planning

At this stage in the project it is sensible for the author to plan out when different stages of the project should be carried out and when the resources the author plans on using can be accessed. In this section of the report the author will outline any resources that will be needed and for what duration. The author will also detail a timeline of when certain parts of the project will need to be completed, this will allow the author to complete the project at a reasonable pace instead on rushing through and making potential mistakes.

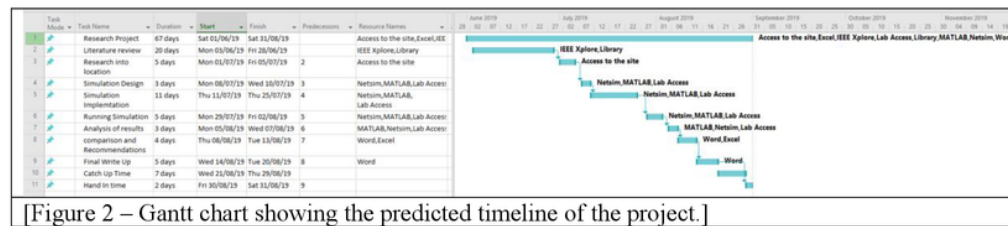
5.1 Resources Required

As mention previous the author plans on using a program called Netsim to simulate the network. This software is provided by the university and situated in one lab, the author will need to plan around the labs availability as not to disrupt other students work. The author also previously mentioned using MATLAB to create noise instead of using the built-in noise generation of Netsim. The university also provides MATLAB to students but fortunately the software can be downloaded on personal computers, this will allow the author the develop the noise without needing any extra resources such as lab space or workstations from the university. Some resources are simple and easy to access with no need for

prior planning resources such as access to the IEEE Xplore Digital Library, access to a computer and access to appropriate software to write the project report are all easily accessible to the author.

5.2 Gantt Chart

A good way to develop a project plan is to visualise it in a time line of sorts, this allows for easy interpretation. The author will use Microsoft Project to create a timeline in the form of a Gantt chart, this will display the predicted length of time for each section of the project. Figure 2 shows the produced Gantt chart the author has included areas for catch up in the event that certain task takes too long or if there are any setbacks.



[Figure 2 – Gantt chart showing the predicted timeline of the project.]

6. Conclusion

Throughout this report the author has outlined a plan for research including what the aim and objective are. The author also conducted a small amount of research into the field to gather a sense of what should be investigated in further research. Finally, the author outlined the plans and methodologies for the project including the research and experimentation methodologies and the data that will be collected. To summarise this the report the author plans to conduct research into IoT moisture sensors and how they perform in a perfect environment. The author has also stated the resources required to undertake this project as well as an evaluation of the risks and limitation that might hinder the project.

7. Reference List

- [1] V. Bhuvaneswari and R. Porkodi, "The internet of things (IOT) applications and communication enabling technology standards: An overview," *Proc. - 2014 Int. Conf. Intell. Comput. Appl. ICICA 2014*, no. October 2017, pp. 324–329, 2014.
- [2] "Down To Earth Project." [Online]. Available: <https://www.downtoearthproject.org.uk/>. [Accessed: 01-May-2019].
- [3] GSMA, "How Mobile IoT is Changing the Industrial Landscape."
- [4] NEST, "Nest Learning Thermostat How does it work?"
- [5] S. Kiran and S. B. Sriramoju, "A study on the applications of IOT," *Indian J. Public Heal. Res. Dev.*, vol. 9, no. 11, pp. 1173–1175, 2018.
- [6] V. Riquebourg, D. Menga, D. Durand, B. Marhic, L. Delahoche, and C. Logé, "The smart home concept: Our immediate future," *2006 1st IEEE Int. Conf. E-Learning Ind. Electron. ICELIE*, no. January, pp. 23–28, 2006.
- [7] 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.
- [8] 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.

- [9] A. Sarmah, K. Kailyan Baruah, and A. J. Baruah, "A Brief Review on Internet of Things," *Int. Res. J. Eng. Technol.*, 2017.
- [10] A. Haroon, M. Ali Shah, Y. Asim, P. Wajeeha Naeem, M. Kamran, and Q. Javaid, "Constraints in the IoT: The World in 2020 and Beyond," 2016.
- [11] A. Santhosh Reddy and C. Technology Solutions, "Reaping the Benefits of the Internet of Things."
- [12] R. Alur *et al.*, "Systems Computing Challenges in the Internet of Things," 2015.
- [13] D. Benhaddou and A. F. Ala, *Wireless sensor and mobile ad-hoc networks vehicular and space applications*, no. January 2015. 2015.
- [14] 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.
- [15] 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.
- [16] C. M. Ramya, M. Shanmugaraj, and R. Prabakaran, "Study on ZigBee technology," *ICECT 2011 - 2011 3rd Int. Conf. Electron. Comput. Technol.*, vol. 6, no. April 2011, pp. 297–301, 2011.
- [17] M. Bierlaire, "An Introduction to ZigBee," *Optimization*, pp. 1–82, 2005.
- [18] M. Hillman, "An Overview of ZigBee Networks A guide for implementers and security testers."
- [19] S. Environments, D. G. Reina, S. L. Toral, and F. Barrero, "Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence," vol. 460, no. January, 2013.
- [20] T. Obaid, A. Abou-Elnour, M. Rehan, M. Muhammad Saleh, and M. Tarique, "ZIGBEE TECHNOLOGY AND ITS APPLICATION IN WIRELESS HOME AUTOMATION SYSTEMS: A SURVEY," *Int. J. Comput. Networks Commun.*, vol. 6, no. 4, 2014.
- [21] T. Ho, "DDoS and IoT: How You Could Have Contributed to Breaking the Internet."
- [22] R. Kumar, "Computer Network and Information Security," *Comput. Netw. Inf. Secur.*, vol. 8, pp. 17–26, 2018.
- [23] S. Gangan, "A Review of Man-in-the-Middle Attacks."
- [24] "Security Overview Defining Basic Security Concepts Addressing Security Objectives ■ Recognizing Network Security Threats."
- [25] "Chapter Three: Research Methodology."
- [26] H. Zalaghi and M. Khazaei, "The Role of Deductive and Inductive Reasoning in Accounting Research and Standard Setting," *Asian J. Financ. Account. ISSN*, vol. 8, no. 1, 2016.
- [27] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods For Business Students*. .

“Detection of Wood Moisture Utilising Environmental Sensors by simulating Internet of Things Sensors” - Project Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

74/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

GRADING FORM: NEW ASSESSMENT

ETHAN RIDD

74

ENGAGEMENT WITH LITERATURE



There is lack of background information on the company and on the problem to be solved with them. Relevant information on the technology (wireless sensor) to be used. Appropriate sources used.

11

KNOWLEDGE AND UNDERSTANDING



The proposal reflect good level of knowledge and understanding. The conclusion could be better summed up what the expected outcomes should be.

11

COGNITIVE, INTELLECTUAL SKILLS



This was clearly highlighted and explained but could be more critically analysed.

10

PRACTICAL SKILLS



The appropriate method and approaches were discuss and aligned to the project. Clear Gantt chart figure need to be more visible. Ethics form completed.

35

TRANSFERABLE SKILLS



A presentable and well-structured work.

7