

WestminsterResearch

<http://www.westminster.ac.uk/westminsterresearch>

**An Energy Aware and Secure MAC Protocol for Tackling Denial of
Sleep Attacks in Wireless Sensor Networks**

Udoh, E.

A PhD thesis awarded by the University of Westminster.

© Dr Ekereuke Udoh, 2019.

The WestminsterResearch online digital archive at the University of Westminster aims to make the research output of the University available to a wider audience. Copyright and Moral Rights remain with the authors and/or copyright owners.

Whilst further distribution of specific materials from within this archive is forbidden, you may freely distribute the URL of WestminsterResearch: (<http://westminsterresearch.wmin.ac.uk/>).

In case of abuse or copyright appearing without permission e-mail repository@westminster.ac.uk

An Energy-Aware and Secure MAC Protocol for Tackling Denial-of-Sleep Attacks in Wireless Sensor Networks

Ekereuke Udoh

A thesis submitted in partial fulfilment of the requirements of the
University of Westminster for the degree of Doctor of Philosophy

September, 2019

Abstract

Wireless sensor networks which form part of the core for the Internet of Things consist of resource-constrained sensors that are usually powered by batteries. Therefore, careful energy awareness is essential when working with these devices.

Indeed, the introduction of security techniques such as authentication and encryption, to ensure confidentiality and integrity of data, can place higher energy load on the sensors. However, the absence of security protection could give room for energy-drain attacks such as denial-of-sleep attacks which have a higher negative impact on the life span (availability) of the sensors than the presence of security features.

This thesis, therefore, focuses on tackling denial-of-sleep attacks from two perspectives – A security perspective and an energy-efficiency perspective. The security perspective involves evaluating and ranking a number of security-based techniques to curbing denial-of-sleep attacks. The energy-efficiency perspective, on the other hand, involves exploring duty-cycling and simulating three Media Access Control (MAC) protocols – Sensor-MAC, Timeout-MAC and TunableMAC – under different network sizes and measuring different parameters such as the Received Signal Strength (RSSI) and Link Quality Indicator (LQI), Transmit power, throughput and energy-efficiency. Duty cycling happens to be one of the major techniques for conserving energy in wireless sensor networks and this research aims to answer questions with regards to the effect of duty cycles on the energy efficiency as well as the throughput of three duty-cycle protocols – Sensor-MAC (SMAC), Timeout-MAC (TMAC) and TunableMAC, in addition to creating a novel MAC protocol that is also more resilient to denial-of-sleep attacks than existing protocols.

The main contributions to knowledge from this thesis are the developed framework used for evaluation of existing denial-of-sleep attack solutions and the algorithms which fuel the other contribution to knowledge – a newly developed protocol tested on the Castalia Simulator on the OMNET++ platform. The new protocol has been compared with existing protocols and has been found to have significant improvement in energy efficiency and also better resilience to denial-of-sleep attacks. Part of this research has been published - Two conference publications in IEEE Explore and one workshop paper.

Table of Contents

Abstract	1
List of Figures	4
Author’s Declaration	6
Definitions	7
Published Work	8
Acknowledgements	9
Chapter 1: Introduction	10
1.1. Background	11
1.2. Sensors	14
1.3. Wireless Sensor Networks	16
1.4. Problem Statement.....	17
1.5. Research Aim	18
1.6. Research Objectives.....	18
1.7. Contributions to Knowledge	19
1.8. Research Methodology	19
Chapter 2: Literature Review	21
2.1. Relevance of the MAC layer.....	22
2.2. Sources of energy loss.....	23
2.3. Classification of MAC protocols	24
2.3.1. Contention-free protocols	24
2.3.2. Contention-based protocols	26
2.3.3. Hybrid Protocols.....	29
2.4. Mobile Wireless Sensor Network Applications.....	30
2.4.1. How mobility can enhance energy-efficiency.....	30
2.5. Other Energy-related solutions.....	30
2.6. Security	32
2.6.1. Autonomous Access control	32
2.6.2. Device based authentication	33
2.6.3. Quantum-cryptography based authentication	33
2.6.4. Authorization	34
2.6.5. Smart Object Lifecycle-based access control.....	34
2.6.6. Threats, Vulnerabilities and Solutions to the IoT from a CIA perspective	35
2.6.7. IoT architectures and their security implications	36
2.7. Denial-of-Sleep Attacks.....	37

2.7.1. State-of-the-art	38
2.7.2. Research approach.....	43
2.7.3. Qualitative Analysis.....	46
2.7.4. Ranking using weighted scoring model	47
2.7.5. Simulation using OMNET++ and Castalia.....	47
Chapter 3: A Proposed approach for Tackling Energy-Drain Attacks.....	51
3.1. Introduction	52
3.2. Comparisons and Simulation for Security Based solutions.....	52
3.2.1. Ranking using Weighted Scoring Model	55
3.2.2. Wireless Sensor Network Simulation for TunableMAC protocol.....	57
3.2.3. Analysis and Discussion.....	66
3.3. Comparisons and Simulations for Energy-based approaches	67
3.3.1. Methodology for comparison and simulation	68
3.3.2. Energy-based approaches.....	72
3.3.3. Simulation Results and Analysis.....	77
3.4. Proposed Approach.....	85
3.4.1. High Level Constituents of the Approach	86
Chapter 4: Layered-MAC: Development of Energy-aware and Secure MAC Protocol.....	90
4.1. Introduction	91
4.2. Related Work	92
4.3. Development Methodology.....	95
4.4. Protocol Implementation.....	97
4.5. Experiments	107
4.6. Results and Analysis.....	114
4.6.1. Simulation results for the protocols under attack.....	118
4.7. PROPOSED AUTONOMOUS APPROACH.....	123
4.8. CONCLUSION	124
Chapter 5: Results and Future work.....	126
5.1. INTRODUCTION	127
5.2. Algorithms.....	129
5.3. Simulation Results.....	132
5.4. Future work.....	136
Chapter 6: Conclusions.....	139
References.....	145
Appendix A.....	157

List of Figures

Figure 1: Conceptual Model of intended research	15
Figure 2: OSI Reference Model	22
Figure 3: Security Mechanisms for M2M communication [8]	31
Figure 4: ZTIC Architecture[9]	33
Figure 5: Risk Landscape for IoT [1]	35
Figure 6: Protocol Architecture[22]	37
Figure 7: MAC Protocol Performance Results [24]	38
Figure 8: Research Focus and Context	45
Figure 9: Conceptual model for proposed research	45
Figure 10: Qualitative analysis of Denial of Sleep defence techniques	55
Figure 11: Ranking of Denial-of-Sleep Defence techniques based on WSM scores	56
Figure 12: Effect of duty cycle on Value propagation	58
Figure 13: Effect of duty cycle on Energy Consumption	59
Figure 14: Effect of duty cycle on Transmitted Packets.....	60
Figure 15: Effect of beacon fraction on value propagation	61
Figure 16: Effect of beacon fraction on consumed energy.....	62
Figure 17: Effect of beacon interval fraction on transmitted packets.....	63
Figure 18: Effect of TX power on value propagation	64
Figure 19: Effect of TX power on energy consumption (Consumed energy in mJoules).....	65
Figure 20: Effect of TX power on transmitted packets	66
Figure 21: Ranking of Green-oriented approaches.....	76
Figure 22: Simulation Parameters.....	81
Figure 23: Tunable MAC energy consumption	82
Figure 24: Comparing SMAC, TMAC and TunableMAC.....	82
Figure 25: Reception Ratio for Tunable MAC	83
Figure 26: Tunable MAC Total packets	83
Figure 27: SMAC, TMAC and TunableMAC compared	84
Figure 28: Total number of packets	84
Figure 29: Proposed Wireless Sensor Network Architecture for Intelligent Agents (Sensors).....	88
Figure 30: Model for Energy-efficiency and Security.....	88
Figure 31: Flow chart showing MAC layer Setup	101
Figure 32: Conceptual model of components of proposed proactive energy-efficient MAC protocol.	102
Figure 33: TMAC parameters	105
Figure 34: IEEE 802.15.4 parameters.....	106
Figure 35: Energy Consumption for 40m, 200m and 1000m Bridge	110
Figure 36: Energy Comparison for SMAC, TMAC and Layered-MAC on 40m, 200m and 1000m Bridge.	111
Figure 37: Reception for SMAC, TMAC and Layered-MAC on 40m, 200m and 1000m Bridge.....	113
Figure 38: RSSI for SMAC protocol under three network sizes.....	114
Figure 39: LQI for SMAC under three network sizes.....	115
Figure 40: RSSI for TMAC under three network sizes	115
Figure 41: LQI for TMAC under three network sizes.....	116
Figure 42: RSSI for TunableMAC under three bridge sizes	116
Figure 43: LQI for TunableMAC under different bridge sizes	117
Figure 44: Comparing RSSI for SMAC, TMAC and TunableMAC	117
Figure 45: Comparing LQI for SMAC, TMAC and TunableMAC.....	118

Figure 46: Energy Efficiency for SMAC, TMAC and LayeredMAC.....	119
Figure 47: Throughput for SMAC, TMAC and LayeredMAC under Denial-of-sleep attack.....	119
Figure 48: Proposed WSN architecture for intelligent agents	123
Figure 49: Energy Consumption for TunableMAC at varied duty cycles and bridge sizes.....	132
Figure 50: Energy Consumption for TunableMAC, SMAC and TMAC at varied bridge sizes	133
Figure 51: Reception ratio for TunableMAC at varied duty cycles and bridge sizes.....	133
Figure 52: Total packet for TunableMAC at varied bridge sizes	134
Figure 53: Reception ratio for TunableMAC, SMAC and TMAC at varied bridge sizes	134
Figure 54: Total packets for TunableMAC, SMAC and TMAC at varied bridge sizes	134
Figure 55: Conceptual model of components of proposed proactive energy-efficient MAC protocol	135

Author's Declaration

I declare that all the material contained in this thesis is my own work.

Definitions

MAC- Media Access Control

WSN- Wireless Sensor Networks

IoT- Internet of Things

SMAC- Sensor MAC

TMAC- Timeout MAC

LMAC – Layered MAC

GMAC – Gateway MAC

DoS – Denial-of-sleep

GAS – Green Autonomous Security

ICT – Information and Communication Technology

M2M – Machine-to-Machine

CIA – Confidentiality Integrity Availability

USB – Universal Serial Bus

DTLS – Datagram Transport layer security

RSSI – Received Signal Strength Indicator

LQI – Link Quality Indicator

Published Work

1. E. Udoh, V. Getov, A. Bolotov, "Sensor Intelligence for Tackling Energy-Drain Attacks on Wireless Sensor Networks," Proc. Of 23rd Workshop on Automated Reasoning: Bridging the Gap between Theory and Practice, University of Liverpool, 2016, <http://westminsterresearch.wmin.ac.uk/17129/1/ARW-16-Udoh-Getov-Bolotov.pdf>.
- [2] E. Udoh, V. Getov, "Performance Analysis of Denial-of-Sleep Attack-Prone MAC Protocols in Wireless Sensor Networks" UKSim: AMSS 20th International Conference on Modelling & Simulation, Cambridge, UK, 27 to 29 March 2018, IEEE. <https://research.westminster.ac.uk/file/e6d2e59414547dc8c07d34cf3586c205b6e34c9df44a27f28b98cba250011964/285789/UKSIM-Paper-Udoh-Getov.pdf> (Presented at the University of Cambridge, UKSIM2018)
- [3] E. Udoh, V. Getov, "Proactive Energy-Efficiency: Evaluation of Duty-Cycled MAC Protocols in Wireless Sensor Networks", Proc. Of 2018 International Conference on Computer, Information and Telecommunication Systems, Colmar, France, 11 to 13 July 2018, IEEE. <https://research.westminster.ac.uk/file/4cfa3295114ca5327e531d484926e6dfb29cf5ac15cc520523abfdb09284ab93/277319/CITS%202018%20Paper-Udoh-Getov.pdf>

Acknowledgements

I would like to dedicate this piece of work to my lovely wife (Christiana) and new-born son (Noah-James) who came into my life towards the finish line of the project. They contributed immensely through their emotional support which gave me an energy-boost that carried me to the end of the project. I would also like to thank my supervisor Prof. Vladimir Getov for his remarkable support throughout the research period, even during my low moments. One of the important lessons I learned from him was the significance of having good sleep. What a coincidence that my research is on denial-of-sleep attacks. My appreciation also goes to the University of Westminster for awarding me a half-fee waiver scholarship and my parents who also supported me in every way. Finally, and most importantly, I would like to thank God who gave me the grace to reach my goals.

Chapter 1: Introduction

“I am intelligent because I know that I know nothing...”

Socrates

This chapter begins with a background context - Internet of Things, and then goes on to emphasize on its enormous potential based on statistics on the predicted growth of the IoT as well as its potential application areas. The chapter then becomes more specific as emphasis is placed on the core component of the IoT – a sensor. The sensors can communicate via a **wireless sensor network** which forms the basis upon which a problem statement is built. After the problem statement, research aim and objectives are highlighted. This is followed by an explanation of the contributions to knowledge as well as the methodology used to achieve them.

1.1. Background

About a decade ago, who would have thought that a car, wristwatch, refrigerator or even non-electronic objects would be on the internet? In the past, one would think of the internet as a network of just personal computers, mini-computers, super computers, mainframes and maybe mobile phones, at most. However, this is no longer the case. An animal can be part of the internet, simply by placing a sensor on its body with which its location can be tracked. A car can now be on the internet and its owner can start the car from their mobile phone and even control the heating of the car. With a smart watch, the owner can also check the fuel level of the car. This new concept of having everything on the internet with the ability to communicate with other devices is called the internet of things.

The term “Internet-of-things” was devised by Kelvin Ashton who defined it this way: *“The Internet of Things means sensors connected to the Internet and behaving in an Internet-like way by making open, ad hoc connections, sharing data freely and allowing unexpected applications, so computers can understand the world around them and become humanity’s nervous system.”* In [60] it is defined as *“...the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.”* The IoT, in my definition, could be seen as the inter-connection of a wide variety of computing/electronic devices for the purpose of sensing, propagating and processing of data in order to increase productivity for humans. The internet-of-things therefore creates a more accommodating platform for fields like robotics and artificial intelligence.

Growth Statistics

The internet-of-things (IoT), also regarded as the internet-of-everything or the smart internet, is gradually gaining more grounds. This is evidenced by a 2014 report from Accenture which reveals that nearly two-thirds of consumers plan to own a wearable device by 2015. As at 2014, research showed that seven percent of consumers owned a wearable device, while 4 percent owned an in-home IoT device and that this figures weren’t higher mainly because of lack of awareness by the public that these devices existed [51] With regards to the future, the internet of things is predicted to be widely adopted by 2019 based on current trends which reveals that half of retailers are currently applying it to their businesses. Among the many uses of the IoT, 72% of business are involved in in-order, controlling building temperatures

and lighting, remote monitoring and indoor-location based services [54] Indoor-location based services which involves tracking shoppers 'paths inside stores happens to be a new industry with a predicted growth of up to \$23 billion by 2021 [55].

IoT Application Areas

To better understand what the IoT is all about, it is pertinent to look closely at the application areas of the IoT asides from the few mentioned earlier. Predicting 20 billion devices to be on the internet by 2020, [56] categorize the application areas for the IoT into 12 sections named as follows:

Smart Cities. This involves using the IoT to automate the infrastructure in a city. This could range from roads cars and traffic to lighting and waste management. Smart parking, for example, can enable the monitoring of parking spaces availability thereby making it easy for cars to smartly locate parking spaces. The structural health of bridges can be monitored using sensors thereby preventing any collapse. In areas where bars and night clubs are plenty, the noise levels can be monitored in real time. Highways can become intelligent by displaying warning messages that relate to climate conditions, accidents and traffic jams. IoT can also be used in management of waste by monitoring the rubbish levels in waste bins in order to enhance trash collection. Smart lighting which is currently applicable in modern cars can also be applied to street lights allowing them to adapt their brightness to the weather conditions. IoT can help road users to avoid traffic congestions by suggesting alternative routes based on intelligence derived from monitoring vehicle and pedestrian levels. The presence of devices such as smartphones can be detected in an environment using IoT.

Smart Environment. IoT can be applied to the environment focusing on aspects to do with environmental disasters such as forest fires, air pollution, earthquake detection, landslide prevention and snow level monitoring.

Smart Water. The quality of tap water can be monitored using IoT. Factories can produce wastes or could have leaking pipes laid under water which could pollute rivers. IoT sensors can detect such leakages and wastes. Swimming pool conditions can be controlled remotely

using IoT. Water levels in rivers, dams and reservoirs can also be monitored using IoT to prevent flooding.

Smart Metering. This involves the smart grid where energy consumption is monitored and managed. Performance in solar energy plants can also be monitored and optimized.

Security and Emergencies. IoT can also be applied to security to track criminals and prevent them from going beyond a certain area.

Retail. In retail, goods can be protected using sensors which could trigger an alarm if a customer attempts to steal a product.

Logistics. IoT can be used for logistics with regards to the tracking of goods as they are being moved between locations.

Industrial control. In industries, air quality can be monitored for oxygen levels as well as the detection of toxic gas in order to ensure that workers and other assets are safe. The location of assets can also be tracked using active and passive tags such as Zigbee and RFID/NFC respectively. In food factories, during the drying meat process, ozone levels can be monitored and managed. The temperature of industrial and medical fridges can also be controlled and managed.

Smart Agriculture. In agriculture, quality of wine produced from grapes can be enhanced by monitoring the moisture of the soil in order to control the amount of sugar in the grapes. Micro-climate conditions can also be managed in order to enhance the quality of fruits and vegetables. Weather conditions can also be studied to forecast rain, drought or snow and these could be very helpful for farmers.

Smart Animal Farming. Animals in the wild can be tracked by those who monitor their movements for the purpose of research. Animal offspring need certain environmental conditions to survive. IoT can be used to monitor and manage such environments to ensure the health and survival of the offspring.

Domestic and home automation. Intrusion detection systems can be implemented using motion sensors for example which can then alert the authorities or the home owner in the case of any breach.

eHealth. IoT can also be applied in hospitals and to elderly and disabled people. Sensors can be used to monitor conditions of patients both inside and outside the hospital. The ultraviolet radiation of the sun could also be monitored in order to inform people when to avoid being exposed. For elderly or disabled people who live alone, the IoT can also be used for fall detection. It is also useful for monitoring vital signs in sportsmen in order to enhance their performance.

1.2. Sensors

Basically, all of the aforementioned categories have their semantics underpinned by a device called a **sensor**. Just like humans have five senses (smell, touch, sight, hearing and taste) which helps them to sense their environment and take action, so also are there different kinds of sensors which sense different properties in the environment and then use such information to enhance productivity in some way. Examples of sensors include temperature sensors, motion sensors, light sensors, proximity sensors, etc. A proximity sensor, for example, will be applicable for use on driverless cars to enable them avoid obstacles or collision of any kind.

Sensors, in order to cover a wide area of the environment, are usually installed in large numbers and made to talk to each other. This interconnection between the sensors is called a sensor network. Initially, the connection medium between these sensors was wired but that wouldn't allow for mobility and ease of installation. Hence, the need arose for a wireless sensor network (WSN). WSNs form a major part of the architecture of the IoT mainly for the sensing and propagation of data. The part of the sensor used for data propagation is usually called the actuator.

The Internet of Things forms the macro-domain for which this project is based. The internet-of-things is an emerging trend which is predicted to rapidly expand in the nearest future. In the simplest terms, the IoT represents the concept of having literally anything as part of the internet. While the current internet is somewhat limited to the conventional computers such as desktop computers, laptops, tablets and mobile phones, the IoT would consist of sensor-based devices thereby allowing for any device with a sensor to be connected to the internet. While the internet consists of human-to-machine communication, the IOT includes machine-to-machine communication as these devices may need to talk to each other in certain contexts. This then makes IoT applicable to many sectors such as agriculture, medicine, manufacturing, education, transport and many other sectors.

If, practically, any device can be connected to the internet, then a number of challenges exist such as that of interoperability, scalability, security, performance, intelligence, energy-efficiency etc. This research narrows the focus to three of these concerns: Energy-efficiency, autonomy and security. More emphasis is placed on the relationship between them rather than considering each of them individually, although a relationship cannot be established without first understanding the individual components. While security focuses on the confidentiality, integrity and integrity of information on the IoT, energy-efficiency would focus on ensuring that the presence of security does not pose a threat to the energy consumption of the devices on the IoT considering their resource-constrained nature. Autonomy on the other hand, takes into consideration the complexity of the IoT and introduces some form of intelligence in handling security. The challenge then lies in how security can be made intelligent while ensuring energy-efficiency.

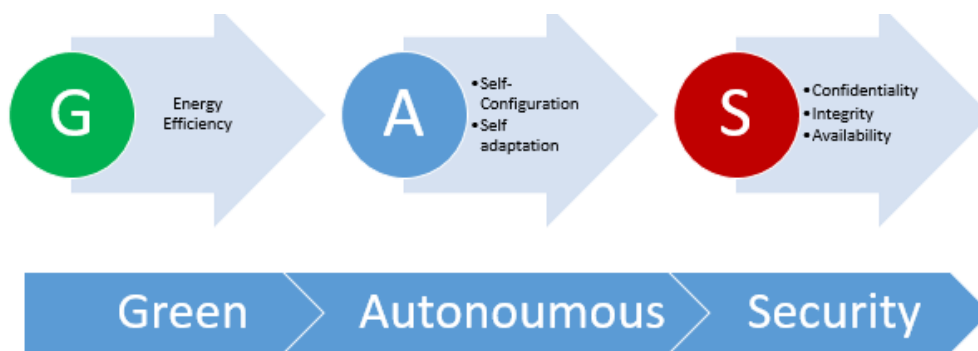


Figure 1: Conceptual Model of intended research

The above figure conceptualizes the entire research in the context of the IoT. The arrows depict the main focus of the research, being security; but then security is not considered singularly. By considering security in the context of the IoT, the problem of complexity then arises which could be handled through autonomy. Furthermore, the problem of resource-constrained devices on the IoT, such as that of wireless sensor networks then arises thereby creating the need for energy-efficiency all for the purpose of enhancing security on the IoT.

The novelty of this research lies in the **multi-disciplinary approach** to security on the internet of things by combining energy-efficiency and autonomy to enhance the confidentiality, integrity and availability of information on the IoT.

The Internet-of-things (IoT) is predicted to expand exponentially in the subsequent years to come in terms of the number of inter-connected devices. With its application in sectors such

as the medical, transport, industry and other aspects of everyday life, the need for security becomes of top priority as these safety and time-critical systems are vulnerable to attacks because of the wide attack surface of any system that makes use of the internet.

1.3. Wireless Sensor Networks

One of the major components of the IoT is a Wireless Sensor Network (WSN) which consists of resource-constrained sensor nodes that usually sense different types of data from the environment and then transmit to a base station. Because of their resource-constrained nature, they are very prone to certain attacks called denial-of-sleep attacks.

Denial-of-sleep attacks are considered to be one of the most dangerous attacks which can reduce the life span of sensors from years to days [65]. Sensors usually go into sleep mode as a way of conserving energy. These attacks work by keeping the nodes awake and preventing them from going into sleep mode thereby draining the energy of the nodes [67].

Various methods are used to carry out a denial-of-sleep attack. These are commonly classified as sleep deprivation, barrage, synchronization, replay, collision and broadcast attacks [68]. These attacks take advantage of vulnerabilities such as frame collisions, message overhearing and idle listening [66]. On the other hand, various approaches have been proposed to detect and prevent denial-of-sleep attacks. Existing comparisons of these approaches are qualitative in nature with a focus on their strengths and weaknesses [68].

Wireless sensor networks which form part of the core of the Internet of things consists of resource constrained sensors that are usually powered by batteries. Hence, there is need for energy-awareness when working with these devices. The presence, as well as the absence of security can have negative effects on energy consumption of these sensors. While the introduction of security techniques such as authentication and encryption in order to ensure confidentiality, integrity of data could place more load on the sensors, the absence of security could also give room for energy-drain attacks such as denial-of-sleep attacks which has a higher negative impact on the life span (availability) of the sensors than the presence of security techniques.

With regards to energy-efficiency, the MAC layer plays a very important role in the consumption of energy. Existing MAC protocols use various approaches such as CSMA, collision avoidance and adaptive duty cycling to achieve energy-efficiency, however majority of these protocols do not consider mobility of the sensors. Hence, the information with which

these protocols work is usually pre-defined before the start of the network with the assumption that the network nodes are static. With recent applications of the WSNs such as driverless cars where mobility is a major part, these existing protocols may not be suitable for such scenarios.

1.4. Problem Statement

Sensors are battery-powered and usually have a limited lifetime as well as a limited memory and processing capacities. This then implies that energy-consumption is a major challenge in wireless sensor networks. In [74] emphasis is placed on the fact that energy-efficiency would have to be increased in order to meet the exascale computing speeds of the future. The radio in a sensor plays a huge role in energy consumption and it is responsible for transmitting, receiving and listening for signals. Unlike a wired network where the medium is end-to-end, the wireless sensor network using a shared wireless medium and this means that one node can overhear signals meant for other nodes. There could also be collision between signals leading to loss of data and consequently loss of energy in retransmitting this data. Even when a sensor is not transmitting nor receiving, it could lose energy from listening for activity on the network. Control packets overhead are also another source of energy loss. All of these sources of energy loss have been tackled with solutions like CSMA, adaptive duty cycling, collision avoidance, time-division multiplexing, frequency division multiplexing and code-division multiplexing. In time-division multiplexing, each sensor node is assigned a time slot for which it can transmit data. Hence, two sensors cannot transmit at the same time thereby preventing any form of collisions. In frequency-division multiplexing, different frequencies are assigned to different nodes, hence two nodes can communicate at the same time but on different frequencies which prevents any form of interference. Code division multiplexing uses spread spectrum to allow multiple access to the same channel. However, most of these solutions were not designed with the mobility of sensors and topological changes in mind. Sensor mobility is becoming more popular in application areas such as underwater surveillance where sensors can move underwater to detect debris; driverless cars whereby sensors on a moving vehicle transmit data about their environment to the cloud. Mobility of sensors would always lead to frequent changes in topology thereby requiring solutions that are not just traffic-adaptive but topology-adaptive. One example of an application of mobile wireless sensor networks is animal monitoring where sensors are attached to animals to track

their migration patterns. Considering that the animals are mobile, these changes the position of the sensors hence requiring changes to aspects like routing of data.

Asides energy-consumption in WSNs, an equally important aspect to be aware of is the fact that the more IoT is adopted, the more vulnerable systems and people on the internet become. Considering that, the internet was not designed with security in mind, it is therefore plausible to combine energy efficiency and security and they tend to overlap and care has to be taken not to implement one at the expense of the other. Security can only expand with energy-efficiency. In other words, the more energy-efficient a WSN is, the more the chances of introducing stronger security techniques. Information security can be viewed in the context of confidentiality, integrity and availability. The availability aspect which involves ensuring that information is accessible to authorised users as at when they need it. Availability overlaps with energy-efficiency in that if a sensor is not energy-efficient, then a sensor can quickly exhaust its lifetime thereby making information unavailable for its intended purpose.

1.5. Research Aim

The main aim of this project is to improve the energy-efficiency and security of a wireless sensor network with focus on the MAC layer, in a way that creates a balance between energy-efficiency and security

1.6. Research Objectives

- To investigate the relevance of the MAC layer with regards to energy-efficiency in a wireless sensor network
- To evaluate existing energy-efficient MAC layer protocols using simulation experiments
- To compare and evaluate existing solutions to tackling denial-of-sleep attacks
- To explore how a balance can be established between energy-efficiency and security in WSNs
- To arrive at a framework/tool for tackling denial-of-sleep attacks
- To develop an energy-efficient prototype/protocol for tackling denial-of-sleep attacks
- To test the developed prototype under denial-of-sleep attacks in comparison with other existing protocols

1.7. Contributions to Knowledge

- One of the main contributions to knowledge was the framework developed as part of the novel MAC layer prototype. The framework served as a basis for the development of algorithms to improve on the energy-efficiency of the wireless sensors by incorporating a layered model which applies virtual clustering, RSSI/LQI measurements, adaptive duty cycling and cluster head rotation.
- Another contribution to knowledge is the development of the novel MAC protocol which was based on the algorithms. The algorithms and the protocol were implemented on OMNET++ simulator, on top of the Castalia framework for WSNs. Aspects of the algorithm tested include the energy efficiency and throughput. The protocol was tested against other existing MAC layer protocols (SMAC and TMAC). The results showed the new MAC protocol showed about twice as much reception at the sink node than the two existing protocols with the same amount of energy. The algorithm was also tested under denial-of-sleep attacks in comparison with other protocols and showed the same level of energy-efficiency.

1.8. Research Methodology

Simulation and real-device experiments were the main approaches used in this project. More specifically, the methodology for this research included the following stages:

- Evaluate existing solutions to denial-of-sleep attacks. This stage involved carrying out an extensive review of the literature to identify existing solutions to denial-of-sleep attacks. This included techniques, approaches, frameworks, models and protocols.
- Development and Application of GAS (**Green Autonomous Security**) model as a high-level approach to tackling denial-of-sleep attacks.
- Use OMNET++ and Castalia to observe effects of various parameters such as duty-cycling, sample interval, transmit power on energy-efficiency on existing protocols. This stage involved investigating the energy consumption of SMAC and TMAC under different network conditions.
- Use OMNET++ and Castalia to do a performance analysis by observing parameters such as RSSI/LQI and the effect on throughput. This stage involves measuring the performance of

SMAC and TMAC which included not just energy consumption measurements but throughput measurements.

- Use insight from the simulation results as well as evaluation to propose an approach for tackling denial-of-sleep attacks. Based on the results from the simulations as well as the evaluation of existing solutions, a layered model was developed.
- Develop a MAC layer protocol based on the proposed approach and test this protocol against existing protocols e.g. SMAC and TMAC. The aforementioned layered model was then used as an input into the development of the algorithms as part of the MAC-layer protocol (Layered-MAC).
- Test the MAC layer protocol by comparing it with existing MAC protocols based on energy-efficiency and throughput and based on their reaction under denial-of-sleep attacks.

Chapter 2: Literature Review

“Creativity is knowing how to hide your sources”

Albert Einstein

This chapter begins with an introduction to the MAC layer and the role it plays in a wireless sensor network. The MAC layer is also discussed in terms of the role it plays in energy consumption and the various sources of energy loss are discussed. MAC protocols have then been classified based on whether they allow multiple access to a medium or not. Mobility of the sensors was also considered in terms of the impact on energy consumption. Beyond the MAC layer and its protocols, other solutions to do with security, autonomy and energy-efficiency are considered.

Most of the below literature was taken from [58] and gives an overview of the wireless sensor networks and the MAC layer in particular.

2.1. Relevance of the MAC layer

Wireless network mediums are always shared by all the nodes in that network and hence require some form of access control to the medium. The shared medium gives rise to noise and interference, multiple nodes accessing the medium at the same time, fading of signals and unidirectional links.

- Noise
- Interference
- Simultaneous medium access
- Signal Fading
- Unidirectional Links

The MAC layer plays a role in the reliability and efficiency of transmissions on the WSN. In other words, the function of the MAC layer is to resolve any conflicts that may arise when a node is about to send data on the shared medium alongside other competing nodes. It can correct errors in communication and is also responsible for flow control, framing and addressing. The MAC layer is part of the OSI model which categorises a network into layers. The MAC layer is the 2nd layer directly on top of the physical layer. It is a sub-layer of the data-link layer which has the logical link control layer as its other sub-layer.

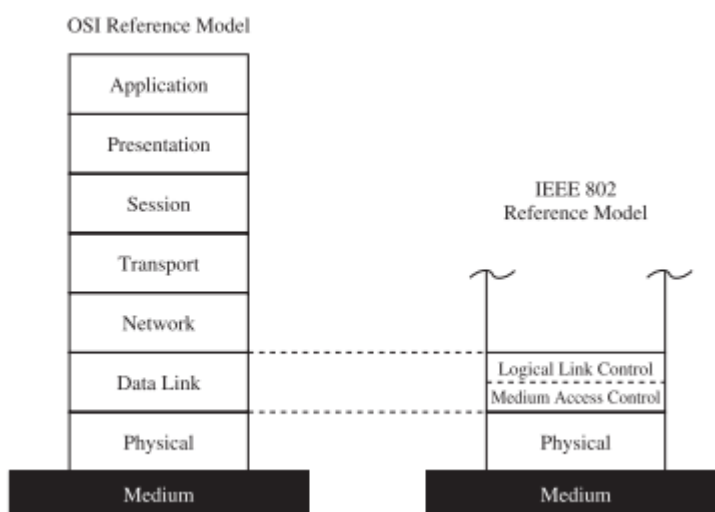


Figure 2: OSI Reference Model

2.2. Sources of energy loss

The MAC layer is also important aspect of wireless sensor networks when energy-efficiency is the main concern. To enhance energy-efficiency, it is important to know the sources of energy loss in WSNs. These include:

- **Transmission and reception of data.** Nodes lose energy while transmitting data either as a unicast or a broadcast. The same goes for receiving data from another node.
- **Idle listening.** When nodes are neither transmitting nor receiving, they could still be listening for activity in preparation to either receive or transmit data. This listening especially when it is idle also drains energy
- **Collisions leading to data retransmissions.** Packets being transmitted at the same time by two or more nodes may collide thereby leading to loss of data. The data will then need to be retransmitted thereby leading to energy loss.
- **Packet overheads.** The size of the packet could still be an overhead and still cause some energy loss, depending on the amount of data being transmitted.
- **Control Packet transmissions.** Control packets are different from data packets and contain meta-data and can be used as beacons to wake-up sleeping nodes, for synchronization of time across nodes and for extra information about the network. The more information contained in the control packets, the more energy required to transmit these control packets alongside the data packets.
- **Transmit power levels.** Radios have transmit power levels which have an effect on the throughput of the network. The higher the transmit power level, the more energy is consumed. Sometimes the transmit power level can be higher than what is required to send the data thereby leading to energy loss.

2.3. Classification of MAC protocols

MAC protocols are classified based on how they control access to the medium. The categories are as follows:

2.3.1. Contention-free protocols

These set of protocols ensure that only one node can access the medium at a time. Therefore, a node would have to reserve a slot exclusively for its transmission. The slots can either be fixed for all nodes at the start or they could be assigned on-demand. Contention-free protocols are further classified into Fixed and dynamic assignment classes.

Fixed Assignment Classes

These are classes that prevent collisions by setting fixed reservation slots for all nodes beforehand. Below are three techniques used by fixed assignment classes:

- **Time division.** Each node is assigned a time-frame. A time-frame consists of a fixed number of transmission slots. The disadvantage of this is that, if slots are of fixed sizes, then very large packets may not be delivered leading to reduced throughput. On the other hand, very small packets would use only a little of the time frame thereby leading to increased latency. If there's a change in network topology, then the slots need to be reassigned.
- **Frequency Division.** In this class, the frequency band is broken down into smaller frequency bands. Nodes that could interfere with other nodes are made to use different frequency bands thereby preventing interference.
- **Code Division.** In this class, multiple access is possible but without collision because of nodes allowed to use different codes. If there is an interference due to same frequency of nodes, these can be corrected at the receiving node using forward error correction through the use of the codes.

Dynamic Assignment Classes

Unlike fixed assignment classes which are rigid in nature as they are not able to adapt to topological changes, dynamic assignment classes only assign slots when they are needed. Below are three techniques used

- **Polling.** In polling, a base station is responsible for asking each node if they have any data to send. The base station moves to the next node if the previous node doesn't have any data to send.
- **Token-passing.** Although token-passing is similar to polling, the main difference is that in polling, there's a centralised way of checking whether a node has data to send, whereas in token-passing the nodes make poll request to each other using frames called tokens which are passed to each other in a round-robin fashion. A node is able to transfer data when it has the token.
- **Reservation-Based.** In this class, static time slots are used to reserve future access for nodes to access based on demand. Although the slots are static, they are only reserved on demand. This reservation is done by toggling a reservation bit.

Below are examples of contention-free MAC layer protocols which use one or more of the aforementioned techniques from either fixed or dynamic assignment classes:

- **TRAMA.** This protocol uses a distributed election scheme which is based on traffic information to determine when nodes can transmit. The benefit of this is that slots are not assigned to nodes without traffic thereby increasing throughput. Furthermore, nodes can also be aware of when they can become idle thereby allowing them to sleep.
- **Y-MAC.** This protocol uses TDMA-based medium access. Time is divided into frames and slots and each frame contains both a broadcast period and a unicast period. Synchronous low-power listening is used by the nodes and the contention during broadcasts is resolved through random back-off times and preambles.
- **DESYNC-TDMA.** Based on TDMA, this protocol uses a self-organising desynchronization algorithm. It improves on TDMA by not using a global clock and is also traffic-adaptive. The desynchronization process ensures that tasks are distributed evenly among sensors.
- **LEACH.** This is a combination of TDMA with a clustering algorithm. One benefit of the clustering algorithm is that it enhances data aggregation and also reduces the amount of data sent to the base station for processing. LEACH consists of two phases: Setup

phase and steady-state phase. In the set-up phase, the cluster heads are selected and the cluster head role is distributed among the sensors to ensure that the energy-usage is distributed evenly among the sensors. If new sensors join the network, they decide which cluster to join based on their received signal strength indicator (RSSI). The steady-state phase is the phase where the sensor can communicate only with its cluster head. One of the setbacks of leach is that it makes an assumption that all nodes have access to the base station and this is not always the case especially when the network gets larger. Even though clustering can improve energy-efficiency, more energy could still be wasted if a cluster head is far from the base station.

- **LMAC.** In this protocol, slots are not assigned centrally but rather assigned by the nodes themselves using a distributed algorithm. One of the downsides is that it is possible for more than one node to select the same slot which can lead to collisions. One variation of the LMAC protocol is the mobile LMAC which goes further to support mobile wireless sensor networks where nodes can frequently join and leave the radio range of other nodes. The MLMAC adapts to changes in the topology of the network. Another downside of both LMAC and MLMAC is that they both create fixed slot sizes which can lead to inefficiency in bandwidth usage.

2.3.2. Contention-based protocols

Unlike contention-free protocols where collision is prevented because there is no chance of collisions because there is no contention among nodes, contention-based protocols allow nodes to access the medium simultaneously, although with a mechanism for reducing collisions or recovering from them. Below are examples of contention-based protocols.

- **ALOHA.** If a broadcast is made by a node, ALOHA uses acknowledgments to confirm that the broadcast transmission was successful. Collisions are addressed through **exponential back off**. This is a form of algorithm that allows some level of delay in transmission of data packets to avoid collisions. A slightly better version of ALOHA called the slotted-ALOHA requires time synchronisation among the nodes as the nodes have to only transmit data at predefined points in time.
- **Carrier Sense Multiple Access (CSMA).** CSMA has two variations: CSMA with collision avoidance (**CSMA/CA**) and CSMA with collision detection (**CSMA/CD**). In the case of

the latter, the node doesn't immediately transmit data, it senses the medium to check whether it is idle or busy. If the medium is busy, it backs off; else it begins transmission. However, the **hidden terminal problem** can lead to collisions at the receiver which the sender won't detect. This hidden terminal problem is not detected by this technique, however, CSMA/CA avoids collisions by sensing the medium just like in the case of collision detection but then it goes further not to transmit even when the medium is idle. Rather it waits for a period of time called DCF inter-frame space (DIFS) in addition to a random back-off value. This could lower the chances of collisions from the hidden terminal problem but does not completely eliminate it.

- **Multiple Access with Collision Avoidance (MACA).** This is achieved through request-to-send (RTS) and Clear-to-send messages (CTS) whereby a node sends an RTS message to the receiving node. If the node responds with a CTS message, then the sender can transmit data. This addresses the hidden terminal problem.
- **Multiple Access with Collision Avoidance for Wireless LANs (MACAW).** In this protocol, an acknowledgement (ACK) control message is sent once a packet has been received correctly. Apart from the CTS and RTS, a data sending (DS) message is also sent to also help with collision avoidance.
- **Power Aware Multi-Access with Signalling.** Reducing energy consumption caused by overhearing is the major focus of this protocol. PAMAS is similar to the MACA protocol in that it uses RTS and CTS messages. It also uses two separate channels for transmission to avoid collisions. To achieve the use of separate channels, two radios have to be used which then leads to increase in energy consumption.
- **SMAC.** SMAC is a duty-cycle based MAC protocol which has a fixed listen interval. One of the disadvantages of this is that if there is very low traffic the energy is wasted during the listen phase. On the other hand, if there is very high traffic, throughput may be hindered as the listen time may not be enough. Therefore there is a need to have an adaptive listen time which TMAC provides. Another challenge with SMAC is that the duty cycle parameters are decided in advance and this may not be suitable for networks with rapidly changing topologies. Another challenge is that it does not

have random offset and therefore there may be collisions during broadcasts and RTS/CTS does not work for broadcasts.

- **TMAC.** This protocol has two major strong areas. One of them is the adaptive listening interval which adapts the listen interval according to the traffic level. Another strong point is the future-request-to-send technique which addresses the early sleeping problem. However, TMAC in order to conserve energy sends messages between small periods of time and this may have an effect on throughput in high traffic-load networks.
- **Pattern MAC.** Similar to T-MAC, sleep schedules are adapted based on the traffic of the node and its neighbours. PMAC uses patterns to describe sleep and wake times of nodes. While this helps save energy by putting nodes to sleep when there is no activity, this pattern is usually shared with other nodes during a period called the Pattern Exchange Time Frame. During this exchange of patterns, collisions are likely to occur.
- **Routing-Enhanced MAC.** This focuses on improving end-to-end latency and also reduces energy through duty cycles. For a node to send data to a destination node, the data has to pass through other nodes on a route to get to its destination. RMAC aligns the sleep and wake periods based on this route.
- **Data Gathering MAC.** This protocol is focused in the fact that most WSNs use a tree-like communication pattern. Therefore, its goal is to deliver data along this tree with very low latency and high energy-efficiency.
- **Preamble Sampling and WiseMAC.** WiseMAC protocols focuses on communications from a base station to a sensor. It uses a technique called preamble sampling where on one hand a node first sends a preamble as a form of alert to the receiver before actually transferring the original message. On the other hand, all nodes sample the medium by listening to the channel for as long as the channel is busy. The nodes only sleeps only when the channel is idle or a data frame is received. The benefit of this is that it enhances throughput as no node is likely to miss their packet due to sleeping at wrong times. A downside is the size of the preamble could still have a negative

effect on throughput and devices that are not intended receivers are still kept awake thereby affecting energy-efficiency negatively.

- **Receiver-Initiated MAC.** In this protocol, a transmission is always initiated by the receiver of the data. The receiving node broadcasts a beacon message if the medium is idle. The purpose of the beacon message is to create awareness of its readiness to receive data. A node which has information to send then transmits the information the moment it receives a beacon message from its intended receiver. The beacon message sent by the receiver also contains some extra information useful for handling any issues to do with multiple senders contending to send a message to the receiver. While this has an advantage on the receiver end by reducing overhearing, the overhearing seems to be increased on the sender side thereby increasing energy costs.

2.3.3. Hybrid Protocols

These are protocols have the characteristics of both fixed and dynamic assignment classes.

- **Zebra MAC.** This uses combination of CSMA and TDMA approach for low-traffic and high-traffic scenarios respectively. ZMAC has a setup phase which allows a node to find its neighbours and obtain its slot in the TDMA frame. The slots are assigned based on information about the node's 1-hop and 2-hop neighbours thereby ensuring that two nodes within a 2 hop neighbourhood cannot have the same slots. Z-MAC is also flexible enough to allow nodes to set the length of their time slots. While this protocol may be efficient in preventing collisions, a lot of energy is spent during the setup phase.
- **Mobility Adaptive Hybrid MAC.** This protocol takes mobility into consideration by combining the TDMA-style slots with mobile slots. The mobility of the sensor is detected through the RSSI of the node. Mobility information has to also be distributed to neighbours through a mobility beacon. MHMAC is better than LMAC in that one node can have more than one slot in a frame thereby increasing bandwidth and reducing latency.

2.4. Mobile Wireless Sensor Network Applications

Most of the research in WSN's focus on the static WSNs where the nodes are not mobile. Such research solutions may not be suitable for mobile WSN's and therefore would need to be improved. Before delving deeper into mobile WSNs, it is important to be aware of the existing application areas for mobile WSNs. The following are application areas for which mobile WSNs can be applied:

- Underwater monitoring. This involves deploying sensors on ocean beds to detect debris from plane crashes
- Small-scale robot squads. This involves deploying coordinated robots to search for earthquake victims under a rubble for example.
- Tracking sensors. Sensors can be attached to humans or equipment to monitor their location.
- Wearable sensors for independent assisted living. Wearable sensors can be part of eHealth systems which can help in assisting elderly people.

2.4.1. How mobility can enhance energy-efficiency

A certain problem called the sink's neighbours problem is discussed in [57] which is a problem that occurs with nodes which are closest to the sink. These nodes are usually the first to die in a network because they always relay information from the sensors to the sink and vice versa. Hence, their energy drains away faster than other nodes. By making the nodes mobile, especially the sink and relay nodes, then the energy usage can be distributed evenly among the sensor nodes. Ahmad et al (2014) introduce a way of conserving energy in mobile WSNs through load-based allocation and time allocation leister techniques.

2.5. Other Energy-related solutions

ICT accounts for about 2.5 percent of all harmful emissions with regards to global carbon emissions. Two aspects are highlighted that contribute to energy saving: Reliability and Efficiency [1]. From a CIA perspective, while efficiency has to do with availability, reliability has to do with integrity.

IoT Communication is identified as one of the areas that dominates energy consumption and efficiency can be enhanced by reducing transmission power to the barest minimum, applying the right algorithms to design communication protocols and activity scheduling [2].

Prasad and Kumar[1] also suggest that redundancy technologies could be very helpful in handling reliability issues which could be present not only during transmission, as in the case of efficiency, but also during sensing and processing by IoT sensor nodes.

Asides reliability and efficiency, security is another variable that has to be considered when making a trade-off as an energy-efficient and reliable IoT would not be termed as successful if there is no security[3].

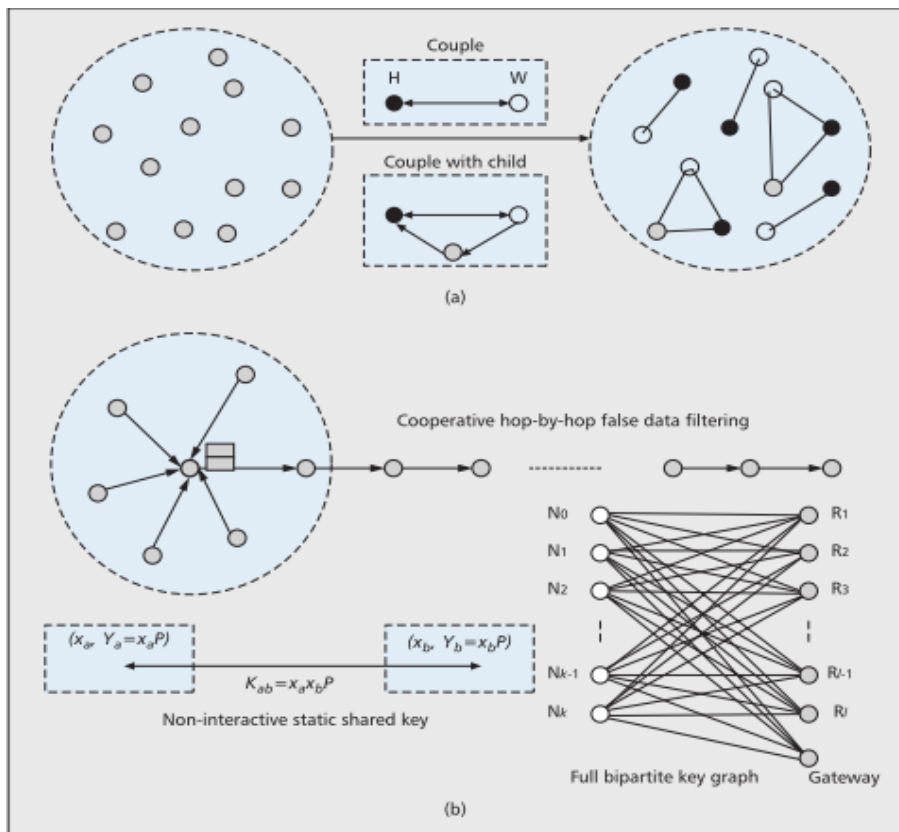


Figure 3: Security Mechanisms for M2M communication [8]

The above figure shows two mechanisms: Early detecting node compromise with couple and bandwidth cooperative authentication to filter false data.

The first mechanism works by coupling nodes together either in Husband(H) and Wife (W) mode or husband (H)-Wife(W)-Child(C) mode and having them exchange beacon messages

that could help them detect a compromise on one of the nodes[3]. While this enhances security, more energy is being utilized. The case could also be vice versa, where energy-efficiency is enhanced and security becomes compromised like in the case where a node is compromised by an attacker without being detected because the node has been put in sleep mode to save energy.

The second mechanism is a bandwidth co-operative authentication that involves a collective authentication by a number of nodes is proven to be very effective[4], however, on the condition that the transmission radius is well chosen as the en route filtering probability reduces as transmission radius increases[3].

Tourancheau et al[5] conclude based on their experiments that the energy cost is relatively low for sensor devices in a wireless sensor network although this is restricted to IEEE 802.15.4 security features and does not take other aspects of security into consideration.

The question then lies in how a balance can be ensured between efficiency, reliability and security.

2.6. Security

2.6.1. Autonomous Access control

One of the challenges identified for self-configurable IoT systems is energy awareness. Considering the envisioned scale of IoT growth of about 20 billion devices in 2020[6], it is worthwhile to consider energy as a constraint when building self-configurable systems as this could help improve the life-span of sensor devices as well as provide more support for critical applications[7]. Other challenges identified include development of suitable metrics, coordinated contextual intelligence, resilience to failures, outages and attacks, application integration and incentives for self-management.

In [8], an identity authentication and capability-based access control model (IACAC) is proposed and is said to protect against man-in-the-middle, replay and denial of service attacks. Certain criteria are considered to be very important in the context of the IoT when developing authentication and access control models. These include mutual authentication, lightweight solution, attack resistance (Denial of service, Man in the middles, Replay attacks), Distributed nature and access control. The IACAC model achieves all of the

aforementioned criteria except the lightweight criteria which is synonymous with energy efficiency.

2.6.2. Device based authentication

The IBM Zone Trusted Information Channel (ZTIC)[9] is a specialised hardware device intended to protect against certain man-in-the-middle attacks through malicious software that cannot be prevented by two-factor authentication approach.

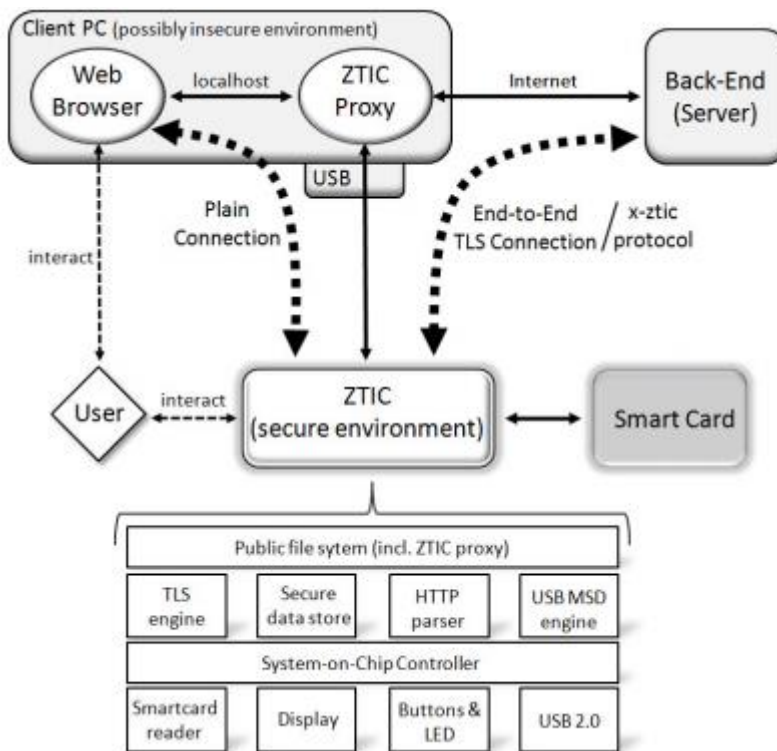


Figure 4: ZTIC Architecture[9]

The above figure shows how the ZTIC technology works by creating a secure connection to the bank server through a proxy on the USB device. This means that all communication between the ZTIC proxy and the server is outside of the client PC and is protected via end-to-end TLS connection.

2.6.3. Quantum-cryptography based authentication

Based on quantum cryptography, a quantum-secure authentication is proposed in [10] as having the following characteristics:

- A key that cannot be physically emulated
- Secure against digital emulation attacks

- Is not dependent on secret data
- Is not dependent on unproven mathematical assumptions
- Its implementation is straightforward

The benefit of quantum cryptography is that, unlike digital keys where their theft can go undetected, a physical object (physical unclonable function) which is based on quantum-physical principles makes it impossible for an attacker to typify the incident light pulse which in turn prevents the attacker from being able to mimic the expected optical response.

2.6.4. Authorization

In [11], an OAuth-based authorization service (OAS) architecture, which is targeted at machine-to-machine applications (IoT), is proposed. The open-authorization is beneficial in that it is third-party in nature; hence reducing the load on the resource-constrained devices on the IoT, allowing for scalability and remote customization of access policies.

However, one of the setbacks of the OAS architecture is that its energy consumption is on the high side particularly due to the radio transmission.

On the other hand, in [12], a secure and efficient authentication and authorization architecture is proposed which reduces communication overhead by 26% and communication latency by 16% by using a smart gateway to ensure a distributed form of authentication and authorization based on the certificate-based DTLS handshake protocol.

2.6.5. Smart Object Lifecycle-based access control

It is important to consider security in the context of the smart “thing” and ensure that security is addressed at each phase of the lifecycle from when power is first introduced to when the device is in operation, thereby making security fundamental to the device’s proper functioning rather than just being an add-on[13].

In [14], certain attacks are classified based on what phase of the lifecycle they happen. At the initial stage, a compromise of root of trust can occur as well as modification of credentials and keys at the manufacturing phase. At the deployment phase, server impersonation and denial-of-service attacks could occur while physical capture of devices could occur at the operational phase.

2.6.6. Threats, Vulnerabilities and Solutions to the IoT from a CIA perspective

According to E&Y [15], 7 in 10 devices on the IoT are vulnerable. They emphasize on the idea that the cyber threat to the IoT should not be seen just as a technological issue but as a business-wide issue. Hence, the figure below illustrates the 8 facets which constitute the



entire risk landscape with regards to cyber threat on the IoT.

Figure 5: Risk Landscape for IoT [1]

Information security can practically not be discussed without putting the CIA (confidentiality, security and availability into perspective). The literature is discussed with a risk assessment approach in mind which is quantitatively calculated by multiplying the threats, vulnerabilities and assets.

Thus, in carrying out a proper risk assessment, one needs to understand not only the threats and vulnerabilities involved but also the assets being compromised, with information being the asset in this context.

Kumar and Lee [16] discuss possible threats to the IoT with specific considerations to the healthcare application domain. Although the threats are discussed in a healthcare domain context, these threats can still be applied to other domains as pointed out by other researchers [17]. A number of threats have been identified as follows:

Monitoring and Eavesdropping

Kumar and Lee [16] describe this as the most common threat to patient privacy. From a CIA context, this breaches the confidentiality of information. Alsaadi and Tubaishat[18] make a

distinction between data ownership and data control/access illustrating that the owner of the data may not necessarily be the only one with access to the information using Google as an example who may use another individual's data for their predictive analysis in the case of Google Trends; which poses a huge challenge.

Denial-of-Service attacks

Roman *et al.* [19]; Alsaadi and Tubaishat [18] discuss on denial-of-service attacks with more emphasis on distributed-DOS attacks perpetrated through the use of botnets. With regards to the CIA, this mainly affects the availability of information.

Energy Drain Attacks

In [20], emphasis is placed on wireless sensor networks are being the target for energy-drain attacks because of their resource-constrained nature of the sensor nodes. Considering that these energy-drain attacks take advantage of the MAC layer, different MAC layer implementations are considered such as Sensor MAC, Timeout MAC, Berkeley MAC and Gateway MAC.

2.6.7. IoT architectures and their security implications

There are different IoT architectures and the architecture adopted determines the kind of security vulnerabilities that could be exploited which in turn determines what kind of solutions that should be in place.

It is also important to look at access control in the context of the cloud as the centralized IoT architectures include the cloud. Security as a Service (SecaaS) is a relatively new approach which stems from the need to outsource security services as well as the need for Managed Security Service providers to have a centralized security service from the cloud[21].

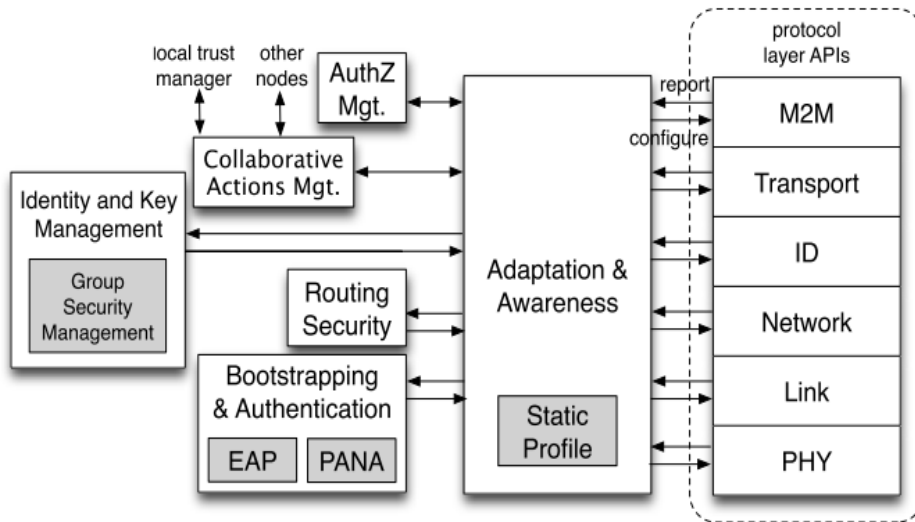


Figure 6: Protocol Architecture[22]

The above figure shows the architecture of an IoT protocol. On the rightmost part are the protocols responsible for the connectivity of the IoT device and this is similar to the Open Systems Interconnect (OSI) Model but has some slight differences. While the OSI model has 7 layers, this model has 6 layers. The lowest three layers stay the same for both models (Network, Link and Physical layer). An ID layer is present and is unique to the IOT protocol architecture and is not found in the OSI model and is intended for identification of IoT resources.

Both quantitative and qualitative methods are used for the evaluation. One of the quantitative methods used for the evaluation is a weighted scoring model. One of the benefits of this method is that it is easy to present and understand however it has its down sides. One of the downsides is that the values assigned to the solutions are mostly subjective. Hence, if this same method were to be used by someone else, the results might be totally different. This therefore had to be combined with some simulations were necessary. Simulations were used to validate some of the solutions that had their simulation models available. The use of simulations were also limited as not all solutions had the models that could be simulated.

2.7. Denial-of-Sleep Attacks

Denial of sleep attacks are mentioned in [20] as one the major attacks that could be targeted towards sensors due to their inherently limited energy sources. They conclude that battery-drain attacks could have negative impacts on the node life span as well as network capability.

More specifically, these attacks include a sleep-deprivation attacks whereby a node is prevented from entering into sleep mode thereby reducing its life span.

2.7.1. State-of-the-art

In [23], denial-of-sleep attacks are classified based on the attack strategy used and these includes sleep deprivation, barrage attack, synchronization attack, replay attacks and broadcast attacks.

Existing Defences for Denial-of-Sleep attacks

- **Gateway-MAC (GMAC)**

MAC Protocol	Network Lifetime (days)			
	Empty Network (no traffic)	Regular Unicast Traffic	Regular Broadcast Traffic	Denial of Sleep Broadcast Attack
802.11	6	6	6	6
S-MAC	63	88	63	63
B-MAC	244	87	87	87
T-MAC	295	130	108	108
G-MAC	480	455	203	478

Figure 7: MAC Protocol Performance Results [24]

The solutions above show that GMAC has the highest network lifetime thereby saving the most energy through the technique of centralized cluster management. One of the reasons for this is that, unlike the other protocols in which all nodes first receive a message before authentication, G-MAC only receives the message through one gateway node, which then authenticates the packet before sending it to the gateway node. This technique does a better job than the other protocols in guarding against broadcast denial-of-service attacks[24]. The 802.11 WLAN uses a MAC protocol called Distributed Coordinated Function which was also tested and found to have lowest network lifetime of 6 days because of its 100% duty cycle hence, lifetime stays the same across all scenarios. 802.11 is used for devices not as resource-constrained as wireless sensor networks, hence energy-efficiency is not given a high priority. While GMAC may have outperformed the other protocols, it does not take other network metrics such as throughput and packet delivery ratio into consideration. Therefore, while it may have a high-network lifetime under attack, there is no evidence of how much throughput/packet delivery is achieved.

- **Hash-based scheme**

The hash-based scheme proposed by Pirretti et al in [25] was an improvement of the initial round robin scheme they developed which in turn was an improvement of the random vote scheme. The hash-based scheme is intended to protect against barrage attacks and sleep deprivation attacks. This scheme overcomes the lack of scalability problem as well as the overhead present in the previous schemes. However, the hash-scheme only protects against intrusion directed at cluster heads.

- **Clustered Adaptive Rate Limiting**

Raymond and Midkiff [26], on the other hand, suggest the Clustered adaptive rate limiting (CARL) technique which unlike the conventional intrusion detection mechanisms is lightweight in nature and works by classifying incoming packets as either legitimate or malicious based on whether they pass authentication and anti-replay checks or not.

- **Threshold-based defence scheme (synchronization attack)**

In [27], a threshold-based defence scheme is proposed which works by using an expected clock drift threshold to ignore any SYN messages with a relative time to sleep that is larger than the clock drift threshold.

- **Fake schedule switch scheme**

In [28] Chen et al propose a security scheme which works with the aid of the Received signal strength indicator (RSSI) in protecting specifically against collision, exhaustion and broadcast attacks and even jamming attacks. However, this solution is not energy-efficient and network throughput is also negatively affected.

- **Four-component Defensive framework**

As a way of preventing denial of sleep attacks, in [29] a defensive framework is proposed which is made of four components:

- Strong link-layer authentication

While [29] suggest that the authentication at higher protocol layers such as the link layer provide integrity and confidentiality, [23] propose a mechanism that

not only considers availability through its cross-layer approach (physical and link layer) but is also energy efficient.

- **Anti-replay protection**

Clustered Anti-replay Protection (CARP) is suggested to be an energy-efficient technique which not only uses anti-replay messages at the data link layer but also takes advantage of the network-layer neighbor information which restricts the neighbor information maintained by a node thereby saving energy.

- **Jamming identification and mitigation**

In [30], a jam detection technique is proposed based on signal strength and location consistency checks.

- **Broadcast attack defense**

A light-weight intrusion detection technique is suggested which operates at the physical layer by classifying each packet based on whether it has passed the authentication and anti-replay checks.

- **Distributed wakeup scheduling scheme**

One of the ways through which power can be drained is through data collection from sensors. In [31], a scheme is proposed that helps nodes to periodically switch between sleep mode and active mode. They do this in a way that not only saves energy but also maintains network latency.

- **Secure wake-up scheme**

In [32], Falk proposes a secure wake-up scheme which verifies that pending messages are authenticated and legitimate without the node having to change to an active state.

- **Two Phase Security System**

In [33], Zhao and Nygard propose a two-phase security system which makes use of Markov Chain Monte Carlo methods and a Tabu Search technique to track and search for intruders respectively.

- **AMC Model for Denial-of-sleep detection**

In [34], Bhatassali and Chaki propose a mathematical model based on Absorbing Markov Chain (AMC) whereby the considered expected death time of a sensor network is used to determine whether there is a denial-of-sleep attack or not.

- **Hierarchical Collaborative model**

In [35] a hierarchical framework is proposed which uses anomaly detection technique to detect denial-of-sleep attacks. This method takes throughput into consideration by distributing the workload among components thereby increasing the energy-efficiency of the method.

- **Cross-layer energy efficient security mechanism**

In [23], Boubiche and Bilami propose a mechanism that takes advantage of the network, MAC and physical layers of the OSI model, hence the reason why it is cross-layer. This mechanism protects against six attacks (Sleep deprivation, barrage, synchronization, replay, collision and broadcast attacks). They achieve this by using the routing information at the MAC layer in combination with the Received Signal Strength Indicator (RSSI) which helps prevent replay attacks. The mechanism is designed to work with the SMAC protocol.

- **Isolation of low-energy nodes**

In [36], Kaur and Atallah propose a secure method that involves setting the detection mode for in sleep schedule and isolating the nodes with lower energy from attacks.

- **Anomaly-based Defense Algorithm**

In [37], a defence mechanism is proposed which forces nodes to enter into a deep sleep mode when any anomalies are detected. While this algorithm seems to defend against denial of sleep attacks, a challenge of reduced network throughput exists due to the fact that nodes are in deep sleep mode and cannot transfer information.

- **Two-tier Energy-efficient secure scheme**

In [38], Hsueh et al proposes a two-tier secure transmission scheme which uses a hash-chain to ensure energy conservation, low complexity, mutual authentication,

symmetric encryption, dynamic session key generation and counter the replay attack and forge attack while integrating with the MAC protocol (XMAC).

- **Selective Authentication**

In [39], Goudar and Kulkarni propose a selective authentication process which makes use of a selected number of nodes as firewalls through bootstrapping to prevent attacker nodes from successfully broadcasting their messages. This scheme focuses more on protecting against broadcast attacks. The selective authentication process is preceded by two steps: network organization and identification of malicious nodes.

- **Zero Knowledge Protocol**

In [40] the zero knowledge protocol is proposed for authenticating the sensor nodes that try to alter the sleep schedule of the nodes. This protocol used in combination with the interlock protocol for key transfer is aimed at tackling man-in-the-middle and replay attacks.

Compared to the conventional wired and wireless networks (IEEE 802.3 and IEEE 802.11), wireless sensor networks have less mature defences against malicious attacks because of the constraints applied in keeping the hardware simple enough to reduce cost and also increase durability. Sensor nodes, because of their energy-constrained nature, are usually put to sleep when they are idle. A denial-of-sleep attack is capable of depriving a sensor from sleep mode and thereby draining its energy sources [41].

In the quest to find ways to prevent denial-of-sleep attacks, it is important to identify and analyse the vulnerabilities that could be exploited by these attacks. Three vulnerabilities are identified by [41] and they include: **Frame collisions, Message overhearing and idle listening.**

Frame collisions which occur as a result of interference of one frame by another frame can lead to data loss which demands resending of the message thereby causing loss of energy. By jamming, and attacker can cause collision between frames and drain energy from the sensors in the process of retransmission. The solution to this is usually contention-based backoff algorithms. Message overhearing, although used in networks that are not energy-constrained, is not ideal for wireless sensor networks because it involves the participation of all the nodes in receiving a message that was intended for one node only. The solution to this

is usually early rejection and message passing. Idle listening occurs when a node is idle and listens for traffic, which consumes more energy than when it is receiving data. An attacker can take advantage of a node's idle time between transmission periods.

In addition to the three vulnerabilities mentioned above, [29] includes Control packet overhead whereby control packets which are usually meant to be received by all nodes are exploited by an attacker and sent to all nodes thereby draining their energy.

A few reviews have been done with regards to denial-of-sleep defence mechanisms. In [42], Vinodsharma while comparing denial-of-sleep solutions mentions only six solutions. Mahalakshmi and Subathra in their survey [43] of 11 solutions conclude that the solutions are unrealistic because they require large scale alterations.

2.7.2. Research approach

The methodology for this research is experimental in nature but first begins with a review of state-of-the-art proposed solutions regarding energy-efficiency in wireless sensor networks as well as a review of state-of-the-art solutions regarding security in wireless sensor networks. This then follows with an evaluation of these solutions in order to find the pros and cons of these solutions and then find gaps that can be filled.

Systematic Review of state-of-the-art energy-efficiency solutions for WSN

- Latency-Throughput-Network Lifetime

Latency is the measure of the delay in transmitting a packet from one point to another. It can be measured either one way (time taken from source to destination) or round-trip (time taken from source to destination and back to source). Throughput is how much of information is transferred from one point to another within a given time period. Hence, it is measured in bits/sec. Network lifetime is very important for WSNs as the nodes have a limited lifetime. Network lifetime is the time between when a WSN is put to use and when one of the nodes fail. Although these three aforementioned parameters do not measure energy, they are closely connected with energy efficiency and contribute to the overall performance of a network. The relationship energy-efficiency and these parameters will be analyzed in order to establish a trade-off between them all.

- OSI/TCP-IP layer of operation

Similar to security, energy-efficiency can be applied at various layers of the network model. Most solutions focus on the MAC layer mainly because access to the radio is managed by this layer and the radio is known to be one the highest consumers of energy on the WSN.

Systematic Review of state-of-the-art security solutions for WSN

- Confidentiality-Integrity-Availability (CIA)

This has to do with what aspect of information is being protected. Confidentiality involves privacy of information and not allowing an unauthorised user to have access to the information. Integrity has to do with maintaining the correctness of data while it is stationary or in transit. Availability has to do with ensuring that data is available for use by authorised users at the time they want it.

- Preventive-Detective

Some security techniques could be preventive in that, when they are implemented, they prevent an attack from being successful. On the other hand, some security techniques could be detective in nature, in that they do not prevent an attack but could detect an attack and notify the owner of the information. Other security techniques could play both roles.

- OSI/TCP-IP layer of operation

The older OSI model is logical model of how data moves from one node to the other on a network and consists of 7 layers namely Application layer, Presentation layer, Session layer, Network layer, Transport layer, Data link layer and Physical layer. The TCP/IP mode is a newer model than OSI and consists of four layers which are more like a compression of the 7 layers of the OSI model into 4. The four layers include application layer, transport, internet layer and network interface layer. Most security protocols operate on one or more of these layers and such information is necessary

as this helps further understand the semantics and effectiveness of the technique or protocol.

- WSN Attacks type handled by security solution

Most security techniques are aimed at curbing at least one type of attack or threat, be it preventive or detective. It is important to know what attacks have solutions and what attacks don't. For the attacks that have solutions, it is also important to know how effective they are in their protection role.

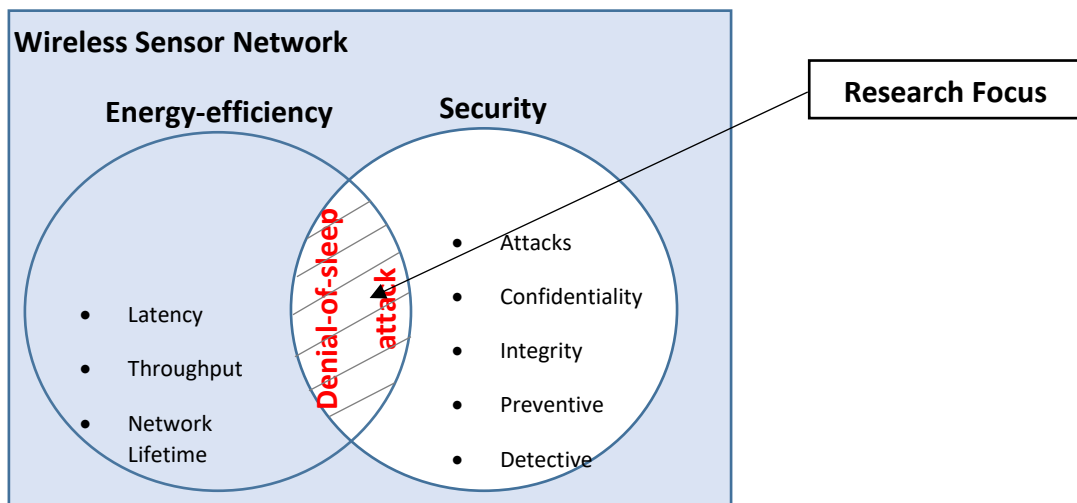


Figure 8: Research Focus and Context

The above figure highlights the main focus of this research as well as the energy-efficiency and security properties that would be looked into.

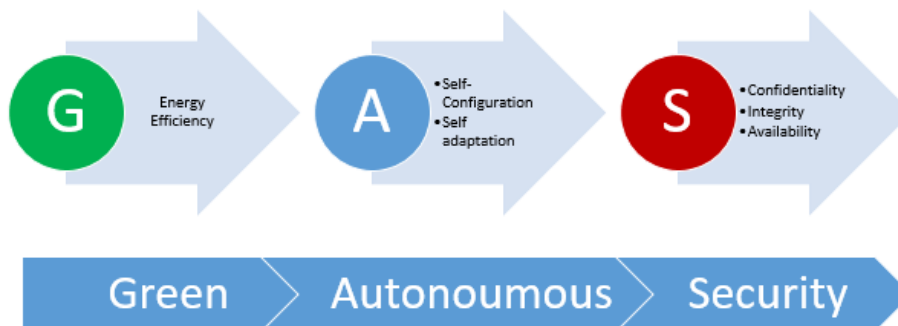


Figure 9: Conceptual model for proposed research

The above figure is a conceptual model which also shows the direction of the research. It begins with an investigation into energy efficiency and how this can be achieved using some form of autonomy which may involve self-configuration and self-adaptation. By improving the energy-efficiency, more room is then left to introduce security solutions that are also energy-efficient. This then gives rise to the term GAS (Green Autonomous Security) which forms the blueprint for this research.

The methodology is divided into three parts:

- Qualitative Analysis
- Ranking using Weighted Scoring Model
- Simulation using OMNET++ and Castalia

2.7.3. Qualitative Analysis

The first part is a qualitative analysis of a number denial-of-sleep defence techniques. This analysis is based on a set of criteria:

- Chronology

The solutions were discussed in a chronological manner beginning from the earliest to the latest.

- Protocols

Most of the solutions are either associated with existing protocols or are even protocols themselves, like in the case of the GMAC protocol

- Level of autonomy

With the increasing vulnerabilities as well as attacks strategies that could be used to carry out energy-drain attacks (in this case, denial-of-sleep attacks), it is important to introduce autonomy or intelligence into the solutions being proposed. One way to identify the level of autonomy in a solution is by looking at the assumptions made while developing the solutions. If the assumptions phase out certain vulnerabilities, then the solution is likely to be low on its level of autonomy.

- Effect on network lifetime (energy-efficiency)

The network lifetime is a strong indicator of how energy-efficient a solution is, because it has to do with how long a sensor can stay alive on its batteries before they run out. Energy efficiency is classified in terms of high and low. With high signifying that energy-efficiency has been considered to a great extent and vice versa.

- Attacks which are defended against

Most of the solutions are targeted towards certain attacks, meaning that some solutions may not be able to prevent all forms of denial-of sleep attacks.

2.7.4. Ranking using weighted scoring model

The second part of the methodology consists of using a multi-criteria decision making method (weighted scoring model) to give scores to these techniques based on a set of criteria. Besides the weighted scoring model, other similar models were also considered before a choice was made. Two of these models include the Best-Worst Method (BWM)[44] and the evidential reasoning approach[45]. A weighted scoring model seemed to be simpler than the other methods. Considering that the reason for the ranking of the techniques wasn't to choose a technique to implement but rather to establish a gap or baseline for further research, it was not necessary to go for a complex decision making method. Hence, the weighted scoring model was chosen.

The third part involves a simulation using OMNET++ and Castalia framework.

2.7.5. Simulation using OMNET++ and Castalia

The WSN MAC protocols had to be evaluated based on their performance. Certain metrics had to be used and these metrics include:

Latency: This has to do with any form of delay that happens during communication in the wireless sensor network. Latency is measured in units of time e.g. seconds

Throughput: As mentioned earlier, this has to do with the amount of data successfully transferred from the source to destination within a given period of time. The unit for throughput is bits/second. However in the simulator, this is referred to as the transmitted packets per time it took to transmit those packets.

Consumed energy: This is the total amount of energy used to transmit data from a source to its destination. The unit for consumed energy is joules/bit.

Network Lifetime: This is how long the nodes on a network can stay alive from the point when they start working to the point where the nodes fail.

Tunable MAC Parameters

- Duty cycle

A node can either be listening for any transmissions or sleeping. Considering that nodes consume a lot of energy while listening, the duty cycle is one of the most important parameters as it plays a major role in reducing the listening time of nodes. The duty cycle is expressed as a percentage or fraction of time for which the node listens or for which the node is active in duty. For example, if the duty cycle is 20% or 0.2, this means that the node listens for 20% of the time during its cycle of listen and sleep. For Castalia the duty cycle is expressed as a floating point value (double).

- Listen interval

It's important to understand that there's a difference between the duty cycle and listen interval. While duty cycle is a fraction of time the node listens, listen interval is the actual time for which the node listens. With the duty cycle and the listen interval, the sleep interval can then be calculated. The listen interval has an effect on both throughput and latency. If the listen interval is small, then the sleep interval will also be small and this can lead to minimised latency as the delay is reduced because of the small intervals. On the other hand, if the listen interval is too small, then throughput may be reduced meaning that packets may not deliver completely and the node may transition into sleep mode before the packets finish delivering. The listen interval is an integer and is measured in milliseconds.

- Beacon Interval Fraction

The presence of a duty cycle means that a node that wants to transmit to sleeping nodes needs to wake up those nodes. This can be done using beacons as a form of preamble before sending the actual message. The beacon interval fraction is the fraction of the sleep interval for which the beacons will be sent. The higher the

fraction, the more energy is consumed. This parameter also has a great impact on energy consumption. The beacon interval fraction is also expressed with the double data type between 0.0 and 1.0.

- Probability of transmissions

This is used alongside the number of transmissions or retransmissions to calculate the expected number of successful transmissions per node. It works by assigning a number between 0 and 1 as a probability of transmission. Probability of transmissions is expressed as a double value in the simulator.

- Number of transmissions

This has to do with the number of times data is transmitted. The more transmissions, the more energy consumed. With more transmissions, better performance is guaranteed. On the other hand, the lesser the number of transmissions, the lesser the energy consumed but performance may also be reduced as data may not reach all the required nodes. Number of transmissions is expressed as an integer value.

- Random Transmission Offset

This is the random time for which a node delays before information is transmitted. This delay is a random value which ranges from 0 (which is the default value) to the transmission offset. The aim of the transmission offset is to avoid collisions by ensuring that two or more nodes do not broadcast at the same time. This is stored with an integer data type in the simulator.

- Retransmission Interval: This is the interval between transmissions and is also expressed as an integer data type.

- Backoff Type: This has to do with carrier sensing.

- Backoff Base value

- CSMA Persistence

- Transmit all packets in free channel

- Sleep during backoff

TunableMAC Limitations

- No security to prevent denial-of-sleep attacks as a nodes can be kept awake through a stream of beacons

- Does not support unicast

Still this leads to a waste of energy as information is always sent to all neighbouring nodes.

- Does not support RTS/CTS: Therefore there is no form of collision avoidance

After getting the results from the simulations the next step is to then find a gap in the current solutions that can be improved on. The simulator will then be used to run different experiments trying out different parameters to see which best fills the gap. This gap could be a gap in energy-efficiency or security.

Mobility of the sensors is not explicitly considered in this research because it broadens the scope of the project and requires a lot of detailed testing which could be another research area on its own. It has therefore been identified as one of the areas of future consideration. Although part of the outputs of this research may favor mobility, no explicit tests are carried out in relation to mobility.

Chapter 3: A Proposed approach for Tackling Energy-Drain Attacks

*“You can't connect the dots looking forward; you can only connect them
looking backwards.”*

Steve Job

3.1. Introduction

In this chapter a framework [73] is proposed for intelligent agents (sensors) on a Wireless Sensor Network to guard against energy-drain attacks in an energy-efficient and autonomous manner. This is intended to be achieved via an energy-harvested Wireless Sensor Network using a novel architecture to propagate knowledge to other sensors based on automated reasoning from an attacked sensor. The proposed framework is based on comparisons of existing energy and security-based approaches, a weighted score model ranking and simulation-based review of TunableMAC protocol.

Wireless Sensor Networks (WSN) form part of the architecture of the Internet of Things (IoT) and are known particularly for their resource-constrained nature due to the fact that these sensors are usually powered by batteries alongside their low processing power. This makes the WSN prone to energy-drain attacks, one of which is known as denial-of-sleep attack [61]. A number of approaches exists which aim to tackle these attacks; however these approaches rarely take into consideration the future scale of the IoT as predicted to expand exponentially in the coming years [62]. The implication of this is that approaches would need to be, not just energy-efficient but, autonomous in nature in order to withstand the variety of attacks that may arise as a result of a larger network where there is a wider attack surface.

3.2. Comparisons and Simulation for Security Based solutions

In order to arrive at a proposed approach, comparisons of existing approaches have been done as well as simulations involving some of the existing protocols. The results from the comparisons and simulations have fed into the proposed approach.

Technique	Year	Protocol specific	Level of autonomy	Energy-efficiency	Attack focus
------------------	-------------	--------------------------	--------------------------	--------------------------	---------------------

GMAC	2005	GMAC	Low -An assumption is made that cluster nodes only respond to a gateway node which may not always be the case.	High	Broadcast attack
Hash-based scheme	2006	None	Low Designed for cluster based networks only and don't consider other topologies	Low	Barrage and sleep deprivation attacks
Clustered Adaptive rate limiting	2007	BMAC	Low Network throughput may not be maintained and it is tailored to the BMAC protocol	High	Broadcast attacks
Fake schedule switch scheme	2009	None	Low Assumption is made that attackers have limited power capability	Low Broadcast of fake schedule could bring more overhead	Collision and broadcast attacks

Secure wake-up scheme	2009	Nil	Low Authentication-based	High	General
AMC model for DoS detection	2012	Nil	Medium Uses a mathematical model (Absorbing Markov chain model)	Medium	General
Hierarchical collaborative model	2012	Nil	Low Uses leaf nodes which can be directly attacked by the intruder.	High	General
Cross-layer energy efficient security mechanism	2013	SMAC	Low Limited to the SMAC protocol	High	Replay attack
Two tier energy efficient secure scheme	2015	XMAC	Medium Uses hash chain	High	Replay attack and Forge attack

Zero knowledge protocol	2015	Nil	Low Authentication based. Uses interlock protocol for key transfer	Low	Man-in-the middle and replay attacks
-------------------------	------	-----	--	-----	--------------------------------------

Figure 10: Qualitative analysis of Denial of Sleep defence techniques

One of the findings is that a number of solutions are topology specific and attack- strategy specific. This means that some of the solutions cannot cater for all kinds of topologies and also cannot mitigate or prevent all kinds of denial-of-sleep attacks. Furthermore, some techniques are also protocol specific.

3.2.1. Ranking using Weighted Scoring Model

To use the weighted scoring model, the following formula is required:

$$A_i^{\text{WSM-score}} = \sum_{j=1}^n w_j a_{ij}, \text{ for } i = 1, 2, 3, \dots, m.$$

Where

w_j = relative weight of the criterion

a_{ij} = performance value of alternative A_i

m = number of alternatives

n = number of decision criteria

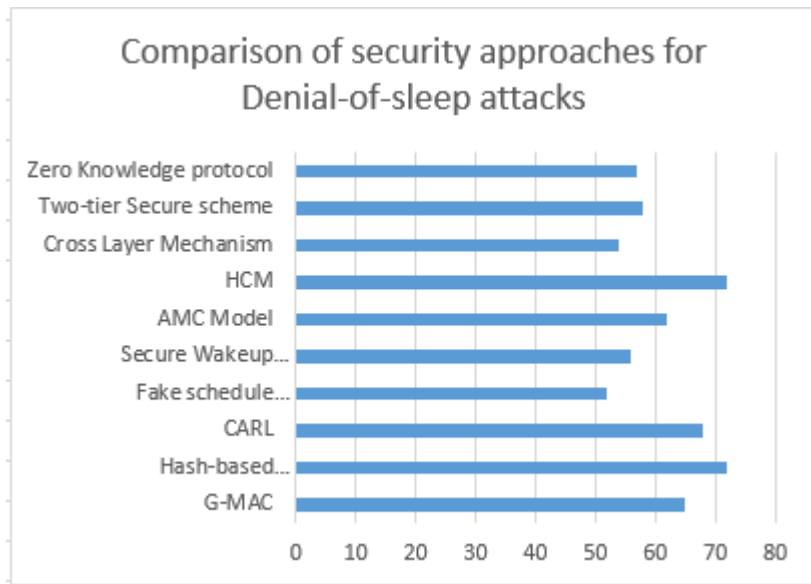


Figure 11: Ranking of Denial-of-Sleep Defence techniques based on WSM scores

Figure 11 shows the final weighted scores assigned to the techniques and the graphical representation of these scores. Four criteria have been used for the WSM: Energy-efficiency, level of autonomy, effect on throughput and attack focus.

Among the ten approaches, the hash-based scheme and the hierarchical collaborative model had the highest ranking based on the weighted scoring model with a score of 72 with energy efficiency being its strong point while the fake schedule switch scheme was the lowest at 52 with its weak point being the network throughput. The next best (CARL) is relatively lower on throughput due to its distribution of workload among components but at par with the hash-based scheme on its energy efficiency.

The weightings assigned to the approaches are based on a combination of qualitative and quantitative data about the approaches from their authors and other authors' reviews, as well as the researcher's point of view.

The results show how the approaches rank rather than just stating their strengths and weaknesses. Security frameworks are not included as part of the ten approaches compared because, unlike techniques, frameworks focus on the 'what' rather than the 'how' of the approach. Hence, the decision criteria used is limited to techniques and does not include frameworks.

The reason for the ranking is not to choose a technique to be applied but to understand the status quo of existing research so as to pinpoint where improvement can be made. Hence, a

simple multi-criteria decision making method is used. If the goal were to make a choice from the ten approaches to be applied to a given scenario, then a more advanced MCDM model would need to be used that allows for an extended decision criteria.

These findings are intended to fuel further research into how best to ensure an energy-efficient and autonomic security of the Internet of things.

3.2.2. Wireless Sensor Network Simulation for TunableMAC protocol

This simulation involves 16 temperature sensors arranged in the form of a grid. These sensors sample their temperature readings when it gets above 15 degrees. Any node that senses a value above the threshold then broadcasts this value. The value propagation which records how many of the nodes received the broadcasted value is then recorded for each node. Energy consumed by the node is also recorded as well as the number of packets transmitted by the nodes. In this scenario, only one node senses temperature beyond 15 degrees. The results are dependent on a number of parameters associated with the Tunable MAC protocol used in the scenario. The parameters include duty cycle, beacon interval fraction, and TX Power.

	Duty Cycle	Beacon Interval Fraction	TX Power
1	0.02, 0.05, 0.1, 0.5, 0.8	1.0	0dBm
2	0.1	0.02, 0.05, 0.1, 0.5, 0.8	0dBm
3	0.1	1.0	-15, -10, -5, -1, 0

Varying Duty Cycle

Application: got value – yes/no

Duty Cycle=0.02	Duty Cycle=0.05	Duty Cycle=0.1	Duty Cycle=0.5	Duty Cycle=0.8
0.992	0.975	0.992	0.933	0.867

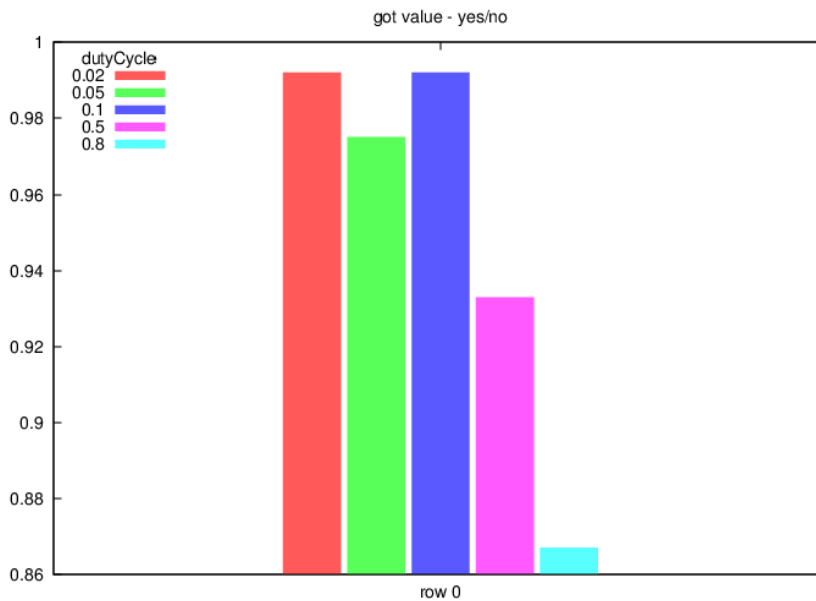


Figure 12: Effect of duty cycle on Value propagation

The above graph in Figure 12 shows the value propagation which indicates how many of the nodes received the propagated value as the duty cycle is varied. Each time a sensor senses a temperature above 15 degrees, it broadcasts a value. The average value of number of nodes that received the value is known as the value propagation. Value propagation is shown on the y-axis while the different duty cycles are shown on the x-axis. The significance of figure 12 is that more understanding about the relationship between duty cycles and their impact on value propagation can be seen. One point to note is that the change in value propagation is not linear and this is due to the variations and randomness in the start times of the nodes (lack of synchronisation of sleep cycles). In [46], one of the ways to ensure synchronization of schedules is for each node to send a SYNC message to other nodes to make them aware of its schedule. The main irregularity lies between the second and third bar from the left, where the duty cycle is 0.05 and 0.1 respectively. However, the graph still shows at large that the value propagation reduces as duty cycle increases. The lowest value is 0.867 which happens when the duty cycle is at the highest relatively (0.8). A duty cycle of 0.8 indicates that the node is listening for 80% of the time and sleeps for 20% of the time if it doesn't have anything to transmit.

Resource Manager: Consumed Energy

Duty Cycle=0.02	Duty Cycle=0.05	Duty Cycle=0.1	Duty Cycle=0.5	Duty Cycle=0.8
0.146	0.124	0.143	0.376	0.557

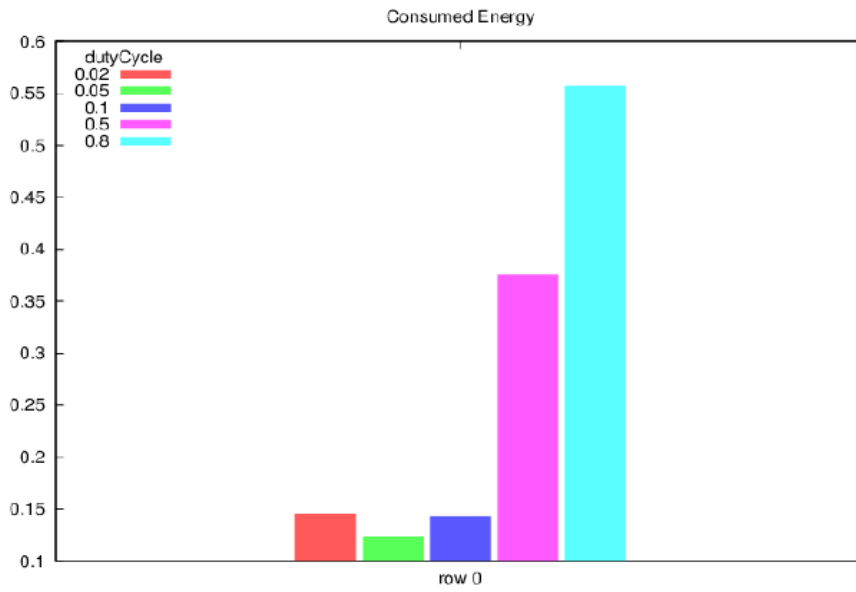


Figure 13: Effect of duty cycle on Energy Consumption

The above graph shows the effect of duty cycling on energy consumption. It is clear that energy consumption increases as the duty cycle increases meaning that the relatively highest consumed energy happens when duty cycle is 0.8. The more a node listens, the more energy it consumes. In [47], they conclude in their results and discussions that energy consumption increases as duty cycle increases. Among the three parameters (duty cycle, beacon interval fraction and transmit power), the duty cycle relatively has the greatest impact on energy consumption with its highest being 0.557.

Transmitted packets

Duty Cycle=0.02	Duty Cycle=0.05	Duty Cycle=0.1	Duty Cycle=0.5	Duty Cycle=0.8
117.017	45.825	22.808	3.733	1.733

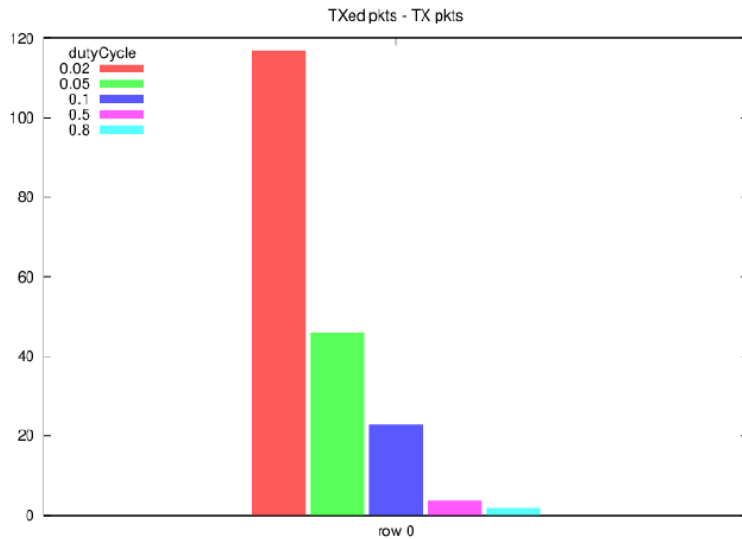


Figure 14: Effect of duty cycle on Transmitted Packets

The above graph shows the impact of the duty cycle on the transmitted packets. Apparently, the lower the duty cycle, the higher the transmitted packets. This is due to the fact that the node spends less time listening and therefore can send more data.

Varying Beacon

Application: got value - yes/no

BeaconFraction=0.02	BeaconFraction =0.05	BeaconFraction =0.1	BeaconFraction =0.5	BeaconFraction =0.8
0.183	0.242	0.304	0.813	0.912

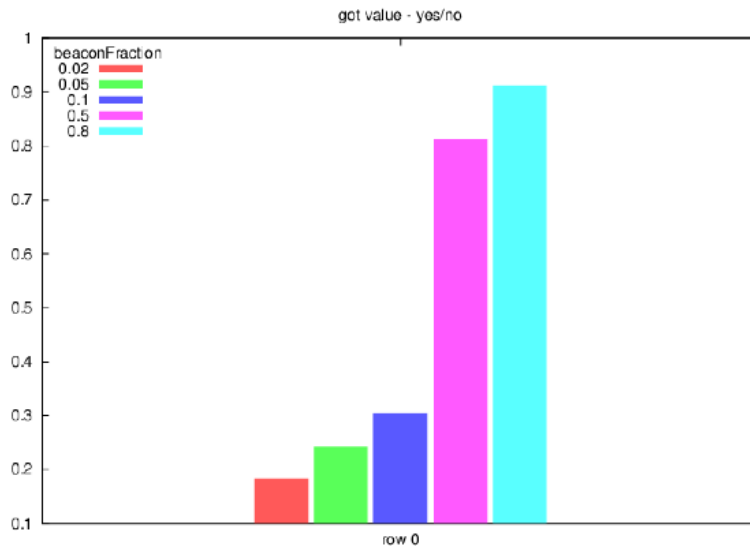


Figure 15: Effect of beacon fraction on value propagation

The above graph shows the effect of the beacon interval fraction on the value propagation. Value propagation increases as the beacon fraction increases. This means that more nodes are likely to receive the propagated value when more beacons are sent.

ResourceManager: Consumed Energy

BeaconFraction=0.02	BeaconFraction =0.05	BeaconFraction =0.1	BeaconFraction =0.5	BeaconFraction =0.8
0.134	0.135	0.135	0.137	0.142

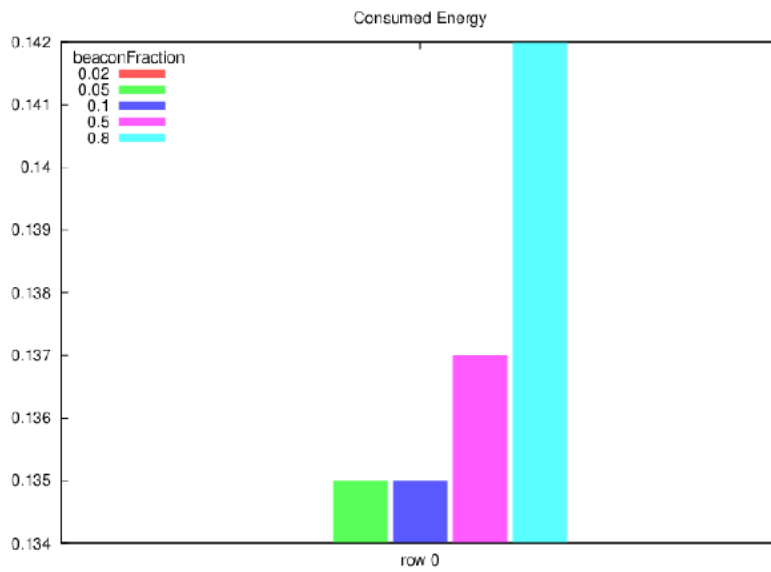


Figure 16: Effect of beacon fraction on consumed energy

The above graph shows the impact of the beacon interval fraction on the consumed energy. The higher the beacon interval fraction, the higher the energy consumed.

Transmitted Packets

BeaconFraction=0.02	BeaconFraction =0.05	BeaconFraction =0.1	BeaconFraction =0.5	BeaconFraction =0.8
0.367	0.725	1.217	9.75	17.337

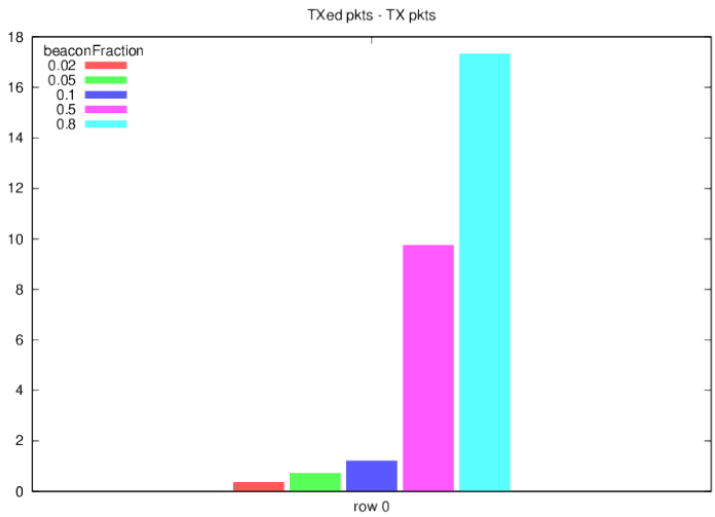


Figure 17: Effect of beacon interval fraction on transmitted packets

The above graph shows the effect of varying the beacon interval fraction on the transmitted packets. The higher the beacon interval fraction, the higher the number of transmitted packets.

The beacon interval fraction can be said to be directly proportional to the value propagation, consumed energy and transmitted packets.

Varying TX Power

Application: got value - yes/no

TX Power = -15dBm	TX Power = -10dBm	TX Power = -5dBm	TX Power = -1dBm	TX Power = 0dBm
0.063	0.113	0.558	0.954	0.979

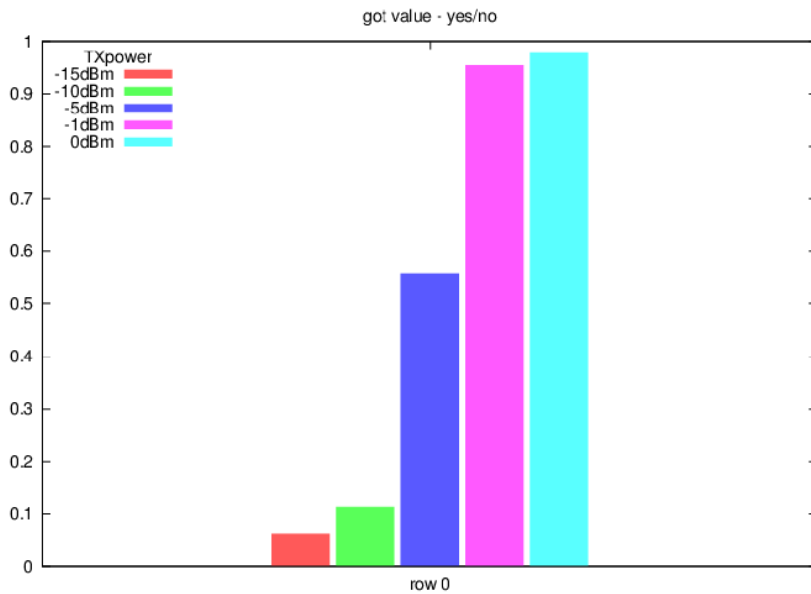


Figure 18: Effect of TX power on value propagation

The above graph shows the effect of varied transmitted packet on the value propagation and it clearly indicates that the value propagation increases as the radio transmit power increases. The value propagation is at its highest (0.979) when transmit power is at its highest (0dBm).

ResourceManager: Consumed Energy

TX Power = -15dBm	TX Power = -10dBm	TX Power = -5dBm	TX Power = -1dBm	TX Power = 0dBm
0.135	0.135	0.138	0.143	0.143

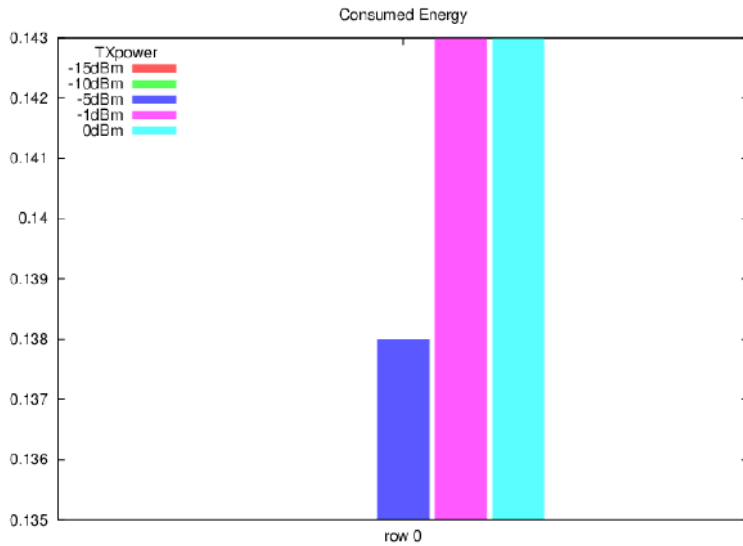


Figure 19: Effect of TX power on energy consumption (Consumed energy in mJoules)

The above graph shows the effect of the radio transmit power on the consumed energy. The simulator starts the y axis starts at 0.135 instead of 0. Hence, two of the bars with values of 0.135 are not showing on bar chart as both bars are on the line. The energy increases as the transmit power increases. Hence, the reason why most radios for wireless sensor networks do not exceed 0dBm of transmit power.

Transmitted Packets

TX Power = -15dBm	TX Power = -10dBm	TX Power = -5dBm	TX Power = -1dBm	TX Power = 0dBm
1.438	2.587	12.842	21.946	22.521

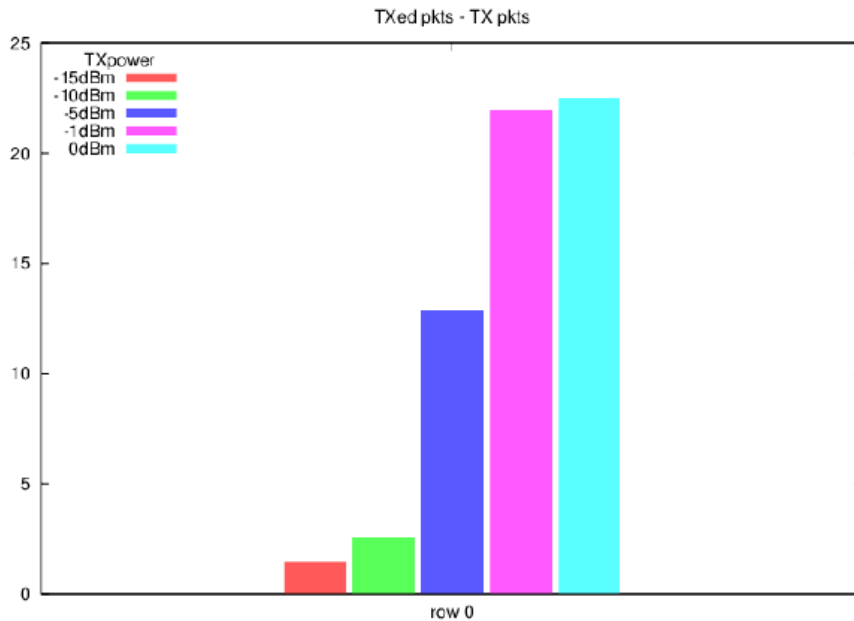


Figure 20: Effect of TX power on transmitted packets

The above graph shows the effect of varying the transmit power on the number of transmitted packets. It is evident that the higher the transmit power, the higher the packets transmitted. There's a huge difference between the change in TX packets from 15dBm to -10dBm and the change in TX packets from -10dBm to -5dBm.

Transmit power can be said to be directly proportional to the value propagation, consumed energy and transmitted packets.

3.2.3. Analysis and Discussion

Part of the relevance of this research is that it becomes easier to understand the impact of certain parameters on various aspects of a wireless sensor network thereby giving more insight as to where to focus on in terms of increasing energy-efficiency.

One important question that crops up is to find out which of the three parameters has the most impact on energy-efficiency assuming they have the same value propagation level. This then makes it easier to know which of the parameters to tune in order to increase energy-efficiency with minimal effect on throughput which can be measured from the value propagation.

Based on the above results, 117 packets are transferred with a duty cycle which consumes energy of 0.146. On the other hand, about 17 packets are transmitted with a beacon interval fraction which consumes 0.142. Finally about 23 packets are transmitted with a TX power

which consumes 0.143. This reveals that the duty cycle has more impact on energy efficiency considering the relatively huge amount of packets that were transmitted with relatively less energy, although latency was not taken into consideration in this analysis.

If self-adaptation and self-configuration has to be adopted into wireless sensor networks, then it is important to understand the effect of certain parameters on certain network performance metrics (latency, throughput, and energy-efficiency) so as to know what level of adaptation is required in certain circumstances. While parameters like transmit power are difficult to change while the network is live [48], parameters like duty cycle and beacon interval fraction can be optimised at runtime as evidenced in [49][50].

Areas for further research

Is there a more energy-efficient way to wake up sleeping nodes in order to transmit data to them, other than through beacons?

Is there a way to tell that these beacons are genuine and are not a form of denial of sleep attack?

How much impact would mobility have on the consumed energy of the sensors?

How can an energy-efficient and self-adaptive protocol which considers sensor mobility and protects sensors from energy-drain attacks (denial-of-sleep attacks) be developed?

3.3. Comparisons and Simulations for Energy-based approaches

Just like humans have five senses that make them intelligent and able to sense their environments, wireless sensor networks are networks of sensing devices which can sense their environments for various properties such as heat, light, sound, etc. and distribute this information via the network, to other destinations thereby making systems smarter. Hence, these wireless sensor networks can play a huge role in larger smart networks such as the Internet-of-Things (IoT). Similarly, just like humans can have viruses attack their senses and prevent them from functioning or even shorten their lives, WSNs can experience certain kind of attacks that can also prevent these sensors from functioning, except that these attacks are intentional and launched by humans. Because these sensors are mostly battery-

powered, these attacks can even reduce network lifetime enormously. One of such attacks is the denial-of-sleep attack.

Denial-of-sleep attack is a kind of denial-of-service attack which attacks the MAC layer of a WSN network and is considered to be one of the most dangerous attacks as it can reduce the life span of sensors rapidly[1]. Unlike jamming attacks whereby the attacker may use months to completely deplete the life of a sensor, with the denial-of-sleep attack, the attacker can achieve the same goal within few days[2]. Sensors usually go into sleep mode as a way of conserving energy. These attacks work by keeping the nodes awake and preventing them from going into sleep mode thereby draining the energy of the nodes[3].

Various methods are used to carry out a denial-of-sleep attack. These are commonly classified as sleep deprivation, barrage, synchronization, replay, collision and broadcast attacks[4]. These attacks take advantage of vulnerabilities such as frame collisions, message overhearing and idle listening[5]. On the other hand, various approaches have been proposed to detect and prevent denial-of-sleep attacks. Existing comparisons of these approaches are qualitative in nature with a focus on their strengths and weaknesses[4].

The aim of the research is to evaluate and review existing approaches to either preventing or reducing the impact of denial-of service attacks and rank them based on a set of criteria using a multi-criteria decision making (MCDM) method. A novel taxonomy is created which classifies the solutions into two groups: security-oriented approaches and energy-oriented approaches. This section, however, concentrates mainly on the energy-based approaches. Thus, a simulation experiment is carried out based on two of the existing energy-based protocols to monitor their effect on energy consumption as well as their effect on throughput. The section ends with a recommendation of a model for building an improved energy-aware protocol.

3.3.1. Methodology for comparison and simulation

Firstly, a taxonomy is proposed whereby existing approaches to tackling denial-of-sleep attacks are classified into two major groups (Security-oriented and Energy-oriented) because a denial-of-sleep attack threatens the energy of sensors by preventing them from sleeping. While the threat aspect calls for a security-oriented solution, the energy vulnerability calls for an energy-oriented solution. Therefore, the problem can be tackled either from a security

perspective or an energy-efficiency perspective. One justification for this classification is that it aligns with the GAS model discussed earlier. Existing approaches either directly aim to prevent the attacks from happening or indirectly reduce the impact of the attack by inherently saving energy where necessary to its barest minimum.

Preventing attack using security approach. In general, protecting information would always involve one of the three aspects: Confidentiality, Integrity and Availability. These approaches involve techniques that cover these three aspects with a major focus on availability. The security approaches are also further uniquely sub-categorised into five (5) groups based on their semantics and their advantages and disadvantages are then analysed. The categories are listed below as follows:

- Cluster-based (GMAC, HBS)
- Mathematical models (AMC)
- Measurement-based (FSSS, HCM, CLM)
- Authentication (CARL, SWS, ZKP)
- Cryptographic-based (HBS, TSS, AntiDoS, One-time password scheme)

Reducing impact using energy-aware approach. Besides from explicitly preventing the denial-of-sleep attacks using the aforementioned security approaches, below are the energy-based approaches that could play a role in reducing the impact of a denial-of-sleep attack. The classifications below are done in [6] and are all MAC layer protocols.

- Static scheduled protocols (SMAC)
- Adaptive group schedule (TMAC)
- Adaptive repeated schedule (SCP-MAC)
- Adaptive staggered schedule (DMAC)
- Adaptive reservation schedule (RMAC)

Weighted Score Model Approach. The approaches are compared based on 2 criteria. It is important that the security approach is not implemented at the expense of energy

conservation and the network performance and some level of adaptation should be included in the approach so as to create an optimum performance.

The criteria, therefore, include the throughput which has to do with how much information is transmitted from the sender to the receiver; and latency which has to do with delay (how long it takes for information to get delivered).

A weighted scoring model (WSM), among other multi-criteria decision models such as Best-worst method (BWM) and the evidential reasoning (ER) approach[7][8] was chosen to rank the proposed security techniques because of its simplicity.

The model works by first assigning weights in percentage to the criteria based on their importance and then assigning weights to the approaches for each criteria. The weights for the approaches and then multiplied by the weights for the criteria then summed up.

$$A_i^{\text{WSM-score}} = \sum_{j=1}^n w_j a_{ij}, \text{ for } i = 1, 2, 3, \dots, m.$$

Where

w_j = relative weight of the criterion

a_{ij} = performance value of alternative A_i

m = number of alternatives

n = number of decision criteria

Simulation. The simulation is done using OMNET++ and Castalia and involves simulation of SMAC, TMAC which seem to be the most popular among the duty-cycle based protocols and TunableMAC protocol under different network sizes while observing the energy consumption and reception.

Security-based approaches

A. Gateway MAC (GMAC). The Media Access Control (MAC) layer of the IEEE reference standard is usually exploited by denial-of-sleep attacks and the GMAC is a protocol developed to guard specifically against broadcast attacks[9]. GMAC saves a lot of energy via its centralised cluster management approach and has a better network lifetime than other protocols such as the SMAC, TMAC and BMAC. However, it is relatively low in terms of autonomy as it focuses on the MAC layer of the network. Here, there is high latency because of clusters.

B. Hash-based scheme (HBS). The hash-based scheme protects against barrage attacks and works by protecting cluster heads against intrusion[10]. Similar to GMAC, it works by protecting the cluster heads against intrusion which is energy-efficient but not autonomous enough to guard against attacks to sensors other than the cluster heads. This also has high latency.

C. Clustered Adaptive Rate Limiting (CARL). CARL classifies incoming packets based on authentication tests and anti-replay checks [3]. This is energy-efficient and relatively positive on throughput but has a relatively low autonomy because of its use of current host-based intrusion detection methods which do not take the distributed nature of sensors into consideration. If there is a high amount of traffic more than anticipated by the protection mechanism, then the rate limiting may go out of hand thereby even negatively affecting throughput. Low throughput is the case here.

D. Fake schedule switch scheme (FSSS). The FSSS uses received signal strength indicator (RSSI) measurement aid in protecting against collision, exhaustion and broadcast attacks[11]. It works by increasing the energy usage of the attacker which may affect throughput if the fake schedule switch is not done accurately. Although there is some form of autonomy in this method, throughput remains at stake.

E. AMC Model. Absorbing Markov Chain (AMC) is a mathematical model which is used in calculating the expected death time of a sensor network and using that to determine the presence of a denial-of-sleep attack[12]. While this may have some form of autonomy in its

approach, it may affect network throughput because of its procedural complexity and may sometimes not be energy-efficient.

SNo		Year	Category	Advantages	Disadvantages
1	GMAC	2006	Cluster-based	Centralised approach	May not work well in very large networks
2	HBS	2006	Cluster-based/Cryptographic		
3	CARL	2007	Authentication	Increases security by ensuring integrity and confidentiality	In a very high traffic, throughput may be affected especially in the CARL technique
4	FSSS	2009	Measurement-based		May have a negative impact on throughput
5	AMC	2012	Mathematical models		Throughput may be negatively affected

Other techniques include the secure wakeup scheme[13], zero knowledge protocol[14], cross layer mechanism[15] and

3.3.2. Energy-based approaches

1. **SMAC(Static-scheduled)**[16]. The SMAC protocol has a static schedule which is fixed during network setup. This means that nodes have a fixed duty cycle (sleep and listen durations are fixed). The implications of this is that in low traffic, energy may be wasted during the fixed listen durations whereby nodes will stay awake unnecessarily for the sake of completing the schedule, instead of sleeping. On the other hand, during

high traffic, the listen duration may not be enough thereby leading to increased latency. SMAC uses techniques such as Request-to-send (RTS) and Clear-to-send (CTS) which helps with collision avoidance and acknowledge (ACK) to contend for the medium. It involves three phases: the first phase is the SYNC phase where nodes synchronise their schedules by choosing a schedule or following schedules from other neighbouring nodes. The second phase is the active period and the third phase is the sleep period.

Algorithm for SMAC

Node listens to medium for a certain period (Carrier Sense)

If node receives schedule from neighbour, it chooses the schedule and becomes a follower *The node broadcasts its new schedule after a random delay*

Else, the node determines its own schedule and broadcasts it to neighbours

Node sends message using RTS by randomly selecting a time slot

If a node hears an RTS or CTS message, it goes to sleep

- 2. TMAC (Adaptive grouped schedule).** Unlike SMAC where the duty cycle is fixed, the TMAC allows for flexibility during a node's listen time according to the traffic density. The minimum time for which a node stays awake before going to sleep is the adaptive timeout (TA). Other packets used by TMAC include Data-send (DS) which is a dummy message sent when a node wants to transmit at the same time it hears a future RTS packet. This helps prevent collision by delaying transmission.

Algorithm for TMAC

Nodes wake up at the beginning of the slot

Node sleeps if no activity is observed

If a node overhears a CTS, it stays awake till the end of the transmission

At the end of the transmission, the node contends for the medium again and begins transmission if it wins the medium

If a node has pending data, it can inform its intended receiver using a future-request-to-send (future RTS) technique to avoid the early-sleeping problem

The receiver remains active until the message is received

If another node is about to make a transmission and overhears a future RTS packet, it sends DS to its receiver to delay transmission.

- 3. SCP-MAC (Adaptive repeated schedule).** This protocol improves the grouped schedule protocols by eliminating the early sleep problem by creating repeated small active periods in one slot.

Algorithm for SCP-MAC

Nodes performs carrier sense by randomly selecting a slot within the first contention window

If channel is idle

Sender transmits a short wake-up tone timed to intersect with the receiver's channel polling

After waking up the receiver, the sender transmits the data packet

Else node aborts transmission until next frame

- 4. DMAC (Adaptive Staggered Schedule).** This works very well with the tree-based topology and works in such a way that the schedule of one node is synchronised with the schedule of the next hop node.

Algorithm for DMAC

Node sends a packet to the next hop node on the route

The node awaits acknowledgment

The next hop node enters receiving state at the same time

If this next hop node is not the destination node

The node enters sending state to forward the packet

Else the final destination has been reached

If sender does not receive ACK

It queues the message until the next sending

If node has multiple packets to send

It increases its duty cycle

It requests other nodes along the sink route to increase theirs too

- 5. RMAC Algorithm (Adaptive reservation).** This protocol allows nodes to negotiate their schedules.

Algorithm for RMAC

During the SYNC phase, nodes synchronise their clocks.

During the data phase, the sender waits for a randomly chosen period of time plus an additional DIFS period

If no activity is detected, the sender transmits a Pioneer Control Frame (PION)

The next hop node along the route looks up the next hop and forwards the PION to it after waiting for a SIFS period

The process continues until destination is reached

Data transmission begins during sleep period

Each node returns ACK after receiving packet and returns to sleep mode

Process continues until data is received at destination

	Latency	Energy-efficiency	Weighted Score
Weight	40%	60%	
Static scheduled protocols	50	50	52
Adaptive group schedule	60	60	60
Adaptive repeated schedule	70	60	64
Adaptive staggered schedule	90	80	84
Adaptive reservation schedule	80	90	86

Figure 21: Ranking of Green-oriented approaches

Justification for above scores

The static scheduled protocols relatively has the highest latency and is also the poorest on energy efficiency because of the fixed duty cycle which then means that in networks with low traffic, the node may listen for longer than usual thereby leading to energy loss and also delay. Also, it provides no cross-layer support.

The adaptive grouped schedule has a relatively better performance during traffic fluctuation because of its (Future-request-to-send) FRTS feature and adaptive timeout which allows it to sleep when there's no traffic and stay awake when there's more traffic hence increasing energy efficiency. However, in very high traffic transmission may suffer from latency due to simultaneous access to the channel by nodes with grouped active schedules.

Adaptive repeated schedules are better in terms of end-to-end latency because of its periodic schedule channel polling thereby allowing for packet forwarding. However energy efficiency may not be improved because of its frequent channel polling using preambles. Per-hop latency may still be increased in very high traffic.

Adaptive staggered schedule further improves end-to-end latency better than other protocols because of its ability to synchronise the transmission time of a node to the wake-up time of the next hop node. It assumes the topology to be a unidirectional tree topology and this is one of its major limitation. Its converge-cast way of working may also lead to decreased energy-efficiency towards the sink due to the bottle neck problem.

Adaptive reservation protocols improves on the bottle neck challenge of the staggered schedule by allowing nodes to negotiate with their neighbours when to transmit and receive packets thereby improving energy efficiency.

3.3.3. Simulation Results and Analysis

Simulation was carried out using OMNET++ and Castalia framework. This simulation is a bridge test application whereby the structural health of a bridge is monitored, a 40 metre bridge with 7 nodes and a 200 metre bridge with 34 nodes. Each node is arranged in form of a grid is 20 metres apart from the next node, hence this explains the number of nodes which correspond with the length of the bridge. A sample interval of 1000ms is used. Consumed energy is measured in mJoules.

The first section of charts below show the total consumed energy used in the simulation. The other section of the charts show the reception of the nodes. A tree-based topology is being used whereby nodes use multi-path routing to propagate data to the sink. Three protocols were tested: SMAC, TMAC and TunableMAC. The aim of this experiment is to understand the relationship between delay and energy efficiency and how a balance can be created or if need be, the kind of trade-offs required.

TunableMAC

TunableMAC is a protocol that was provided along with the WSN Framework, Castalia[17]. As the name implies, this algorithm is tuneable and allows 12 of its parameters to be tuned. This protocol can simulate many duty-cycling protocols but it does not support unicast. It uses CSMA for its transmission, therefore its persistence and backing off policies can be tuned. Its duty cycle can also be tuned as well as the train of beacons that can be used to wake up potential receivers. Below are the 12 parameters that can be tuned:

- **Duty Cycle**

This is the fraction of time for which a node listens to the channel. The node sleeps the rest of the time. The default value is 1.0 meaning that the node listens for 100% of the time and hence no duty cycling.

- **Listen Interval**

While the duty cycle is expressed as a fraction, the listen interval is the exact duration of time for which the node listens and is expressed in milliseconds. The default value is 10 milliseconds.

- **Beacon Interval Fraction**

Unlike SMAC and TMAC, there is no schedule synchronisation and that means there has to be a way of getting the attention of the sleeping node before a broadcast is made. Beacons can be used to achieve this and the sending node sends a train of beacons for a period of time known as the beacon interval. However, this beacon

interval is expressed as a fraction of the sleeping interval and its default value is 1.0 meaning that the beacon interval for the whole of the sleeping interval.

- Probability of Transmission

Every transmission is made with a probability of 1 by default. It is used alongside with the number retransmissions to calculate the expected number of transmissions per node.

- Number of transmissions

The default number of transmissions is 1 and if this number is increased, then the energy consumed is also increased.

- Random Transmission Offset

This is the random time a node waits, after it has sensed that the channel is clear, in order to avoid any collisions. The default value for this parameter is 0 meaning that there is no randomness.

- Retransmission Interval

This is the time gap between retransmissions.

- Back-off Type

This is a CSMA feature and the default number is 1 meaning that the node backs off for a constant time each time the channel is not clear for transmission. If it is 0, the back-off timer is set to the duration of the sleeping interval. If set to 2, then the back-off timer is based on the number of consecutive times the channel was found not to be clear. Hence the back-off timer is equal to the back-off base value multiplied by the number of consecutive times the channel was off. Setting the parameter to 3 means the back-off timer is also based on the consecutive number of times the channel was not clear and is calculated by $(\text{backoffBaseValue})^{\text{times}}$.

- Back-off Base Value

This is the constant time for which a node backs off as discussed earlier. The default value is 16.

- CSMA Persistence

This determines how persistent the CSMA is. If it's non-persistent with the value of 0 (default) then it uses the back-off type and back-off base value. If it's persistent (1-persistent), then it does not back off and it keeps checking the channel until it's free for it to transmit. This requires that the node polls the channel every 0.128 msecs. Another type of CSMA persistence is the p-persistence. If it's p-persistent it also keeps polling until it finds the channel free for transmitting but it transmits only with the probability of p.

- Transmit all packets in free channel

This has a boolean value of either true or false and determines the behaviour of the nodes when the channel is free. With a default value of true, the node transmits all the packets in its buffer without the need to sense the channel. On the other hand a false value means that a node send only one packet from the MAC buffer and goes through the whole carrier sensing procedure again and sends beacons again to wake sleeping nodes. The disadvantage of the true value is that fairness is affected negatively.

- Sleep during back-off

With a duty cycle in place, a node will go to sleep when it backs off. The default value is false if there is no duty cycle as CSMA does not care about energy-efficiency.

TunableMAC Algorithm[17] (Uses CSMA)

Duty cycle of radio is set

Set the listen interval and other necessary parameters

Node senses the channel for a random period of time before transmitting

If the channel is not clear,

Then the node backs off based on CSMA

If sleepduringbackoff property is set to true

Node sleeps during the backoff period.

Else

A node broadcasts a train of beacons to wake up sleeping nodes

Comparing SMAC, TMAC and TunableMAC

Simulation Scenario

The TunableMAC protocol is used alongside two other protocols, SMAC and TMAC in the simulation to understand the energy consumption and reception under different network sizes. The bridge sizes include a 40m bridge, a 200m bridge and a 1000m bridge. The simulation is about the structural health monitoring of a bridge. Sensing nodes are placed in a grid with a sink node in the middle. A car moves on the bridge every five minutes and triggers nodes along its path. The sink node also distributes packets which signify an update software patch.

Bridge Size (metres)	No of nodes	Duty Cycle	Sample Interval(ms)
40	7	0.1 (10%)	1000
200	34	0.1 (10%)	1000
1000	154	0.1 (10%)	1000

Figure 22: Simulation Parameters

Energy Simulation

TunableMAC

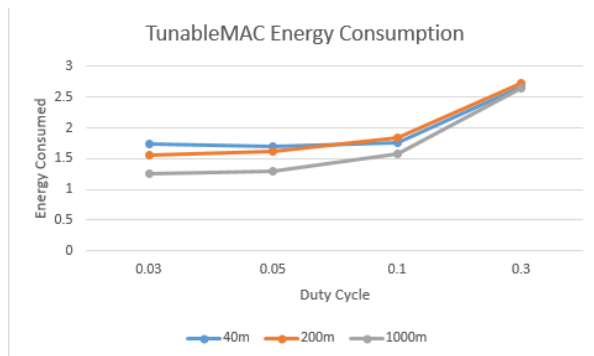


Figure 23: Tunable MAC energy consumption

Comparing TunableMAC with SMAC and TMAC

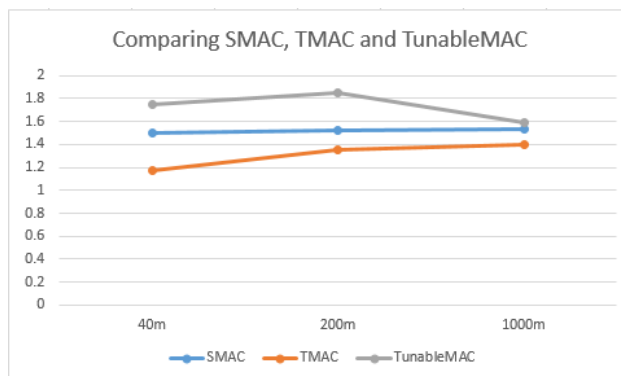


Figure 24: Comparing SMAC, TMAC and TunableMAC

The above three graphs show the energy consumption of SMAC, TMAC and TunableMAC under the different bridge sizes. SMAC increased from 1.505 in the 40m bridge to 1.521 in the 200m bridge and 1.531 in the 1000m bridge. TMAC increases from 1.169 to 1.358 to 1.399 for the 40m, 200m and 1000m bridge respectively. Based on the figures for SMAC and TMAC the energy consumption is directly proportional to the bridge sizes meaning the larger the bridge, the more energy consumed. However, this is not the case for TunableMAC where the energy consumption initially increases as the bridge size increases from 40m to 200m but then the energy decreases as the bridge size increases to 1000 metres hence making it not directly proportional as in the case of SMAC and TMAC. It starts

with 1.753 for the 40m bridge, then it increases to 1.848 for the 200m bridge and then finally ends in 1.587 for the 1000m bridge which is even lower than the 40m bridge.

Reception Simulation

TunableMAC

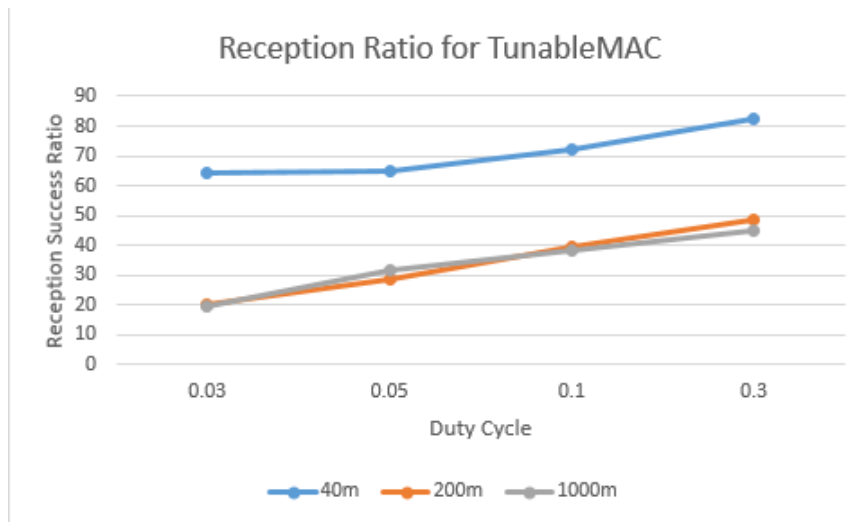


Figure 25: Reception Ratio for Tunable MAC

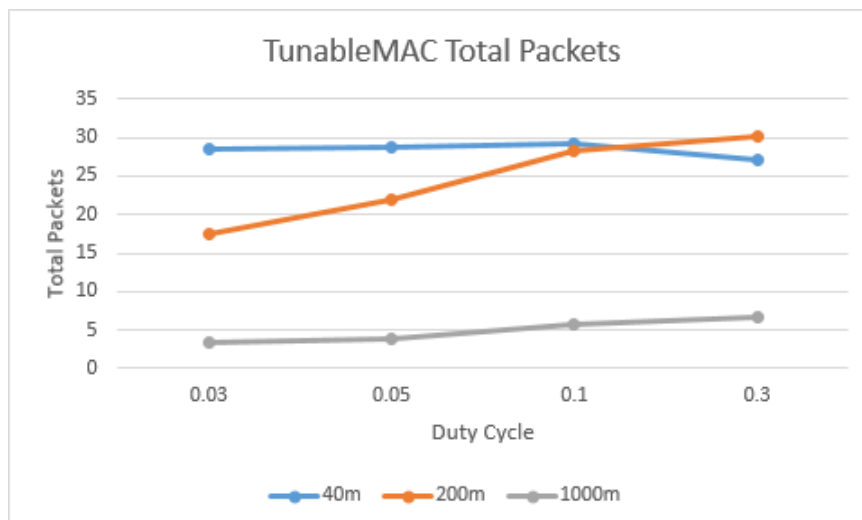


Figure 26: Tunable MAC Total packets

The above graph in figure 7 shows the reception of packets at the sink in a 40m bridge for varying duty cycle. The results show that the reception increases with a higher duty cycle. Success increases as the duty cycle increases while failures decrease as the duty cycle increases.

The above figure 8 shows the reception of packets at the sink in a 200m bridge using a TunableMAC protocol. The total number of packets reaching the sink is less compared to the 40m bridge in figure 7. However, the same pattern occurs in both scenarios whereby the reception (successful packets) increases as the duty cycle increases.

The above figure shows the reception for a 1000m bridge using the TunableMAC protocol. The packet reception also increases with an increase in duty cycle although in general the total number of packets received is less than the 40m and 200m bridges.

Comparing TunableMAC with SMAC and TMAC

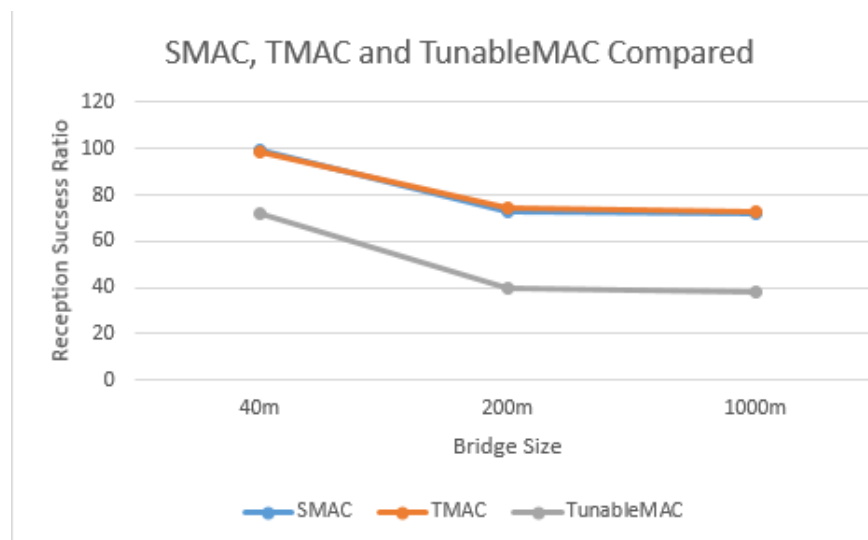


Figure 27: SMAC, TMAC and TunableMAC compared

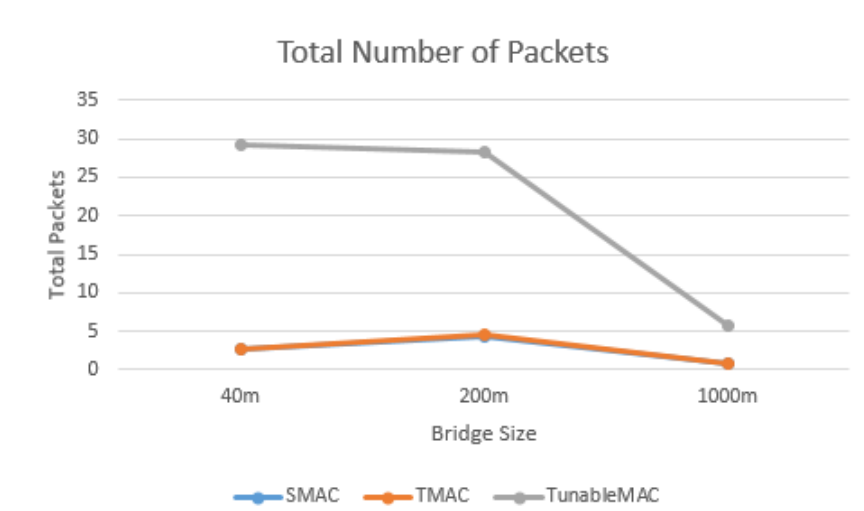


Figure 28: Total number of packets

The above figure compares SMAC, TMAC and TunableMAC in a 40m bridge and the results show that the TunableMAC receives more packets than SMAC and TMAC. SMAC and TMAC are similar in terms of their reception (2.683 and 2.633), although SMAC is slightly higher.

The above three graphs compare the reception levels of SMAC, TMAC and TunableMAC under different bridge sizes. In the 40 metre bridge, SMAC and TMAC have a much lower reception (2.683 and 2.633 respectively) than TunableMAC (21.05). In the 200 metre bridge, a similar situation occurs, even though SMAC and TMAC show an improvement in reception, the results are still very low compared to TunableMAC. In the 1000 metre bridge, there is a huge drop in packet reception for TunableMAC although it still has a higher reception than SMAC and TMAC. In summary, TunableMAC performs better than SMAC and TMAC in terms of reception.

Discussion and recommendation

The results show that TunableMAC performs better than SMAC and TMAC in terms of throughput but consumes more energy than both of them. However, it is important to note that the difference in energy consumption between TunableMAC and the two others (SMAC and TMAC) is significantly smaller than the difference in throughput (reception) between TunableMAC and the two others.

3.4. Proposed Approach.

The intended approach is an improvement of existing approaches - Gateway Media Access Control (GMAC) and Hierarchical Collaborative Model (HCM). While GMAC [63] and the hash-based scheme [4] use centralized approach via cluster heads, HCM [65] and the distributed wake-up scheme [66] use a distributed architecture. Although these approaches seem very useful, they do not take into consideration the size of the network especially on a large scale. Our proposed architecture is based on a combination of both the centralized and the distributed approach. It would involve the use of intelligent agents whereby each sensor becomes an agent which can sense data and take responsive action with the workload dynamically distributed among them. However, this would not function optimally with the

current battery-powered sensors, but rather an energy harvested IEEE 802.15.4 wireless sensor network [62]. This is necessary because the dynamic distribution would lead to an increase in processing power thereby consequently increasing energy costs. In [67], the concept of virtual clusters is introduced whereby nodes are grouped into the same subnet and presented as a single resource. The WSN will be dynamically divided into clusters with cluster heads appointed for each cluster. In this approach, if a sensor encounters or senses an attack, it immediately takes responsive action and also broadcasts the information to the rest of the appointed cluster heads via a “rumour” approach which may consume more bandwidth than processing power. The “rumour” approach is coined from the term “routing by rumour”, which explains the semantics of distance-vector routing protocols whereby each router sends messages to its nearest neighbour until the information propagates to all the routers. In this case, the cluster heads send information to the nearest cluster head and it continues that way until the information gets to all the cluster heads which then pass the information to their clusters. The cluster heads then relay this information to the sensors in their clusters.

3.4.1. High Level Constituents of the Approach

- Automated reasoning via intelligent agents

In [68] a management scheme based on automated reasoning whereby Bayesian reasoning is used during the learning phase, is proposed to help protect against intrusions and also enhance energy-efficiency on a wireless sensor network. Threshold analysis is also used prior to the reasoning. In [69], the BayesMob algorithm is used for self-healing in a case where one or more sensor nodes fail. In this thesis, we consider the Bayesian equation for predictive reasoning by sensors as a way of anticipating an attack and preventing it beforehand. More specifically, our model is based on the following Bayesian equation:

$$P(A|B) = \frac{P(B|A) P(A)}{P(B)},$$

where A and B are events

- P (A) and P (B) are the probabilities of A and B without regard to each other.

- $P(A | B)$, a conditional probability, is the probability of observing event A given that B is true.
- $P(B | A)$ is the probability of observing event B given that A is true.

In this context, for example, $P(A)$ is the base rate or prior probability that a sensor is under attack. This could be based on a threshold value of the amount of energy being consumed by the sensor. $P(B)$ could be the probability that the messages sent by the attacker have a certain size/frequency range. $P(B|A)$ would then be the probability that a sensor under attack is receiving a certain message size/frequency range.

- Choice of WSN architecture

A combination of centralised and distributed architecture is proposed. The centralised approach involves the use of clusters which are formed dynamically based on the location and proximity of sensors. Each cluster has a cluster head which not only serves the other sensors but also acts as a proxy thereby hiding the identity of the sensors. At the cluster level, a single-hop architecture is used while a multi-hop architecture is used for communication between cluster heads. Because of its centralised approach, the single-hop architecture has low delay and a high channel capacity, while the multi-hop architecture which is distributed in nature has a high energy-efficiency and high signal-to-noise ratio [72].

- Resource availability (via energy-harvesting rather than battery-powered sensors)

In [70], a relationship between autonomy and energy-efficiency is established whereby existing wireless sensor networks are limited by their battery power and therefore cannot be autonomous except more power is made available to them. Hence, energy-harvesting is proposed. In [71], the need for energy harvesting is also acknowledged considering that the existing battery-powered sensor nodes need periodic maintenance which contradicts with the characteristics of autonomous systems.

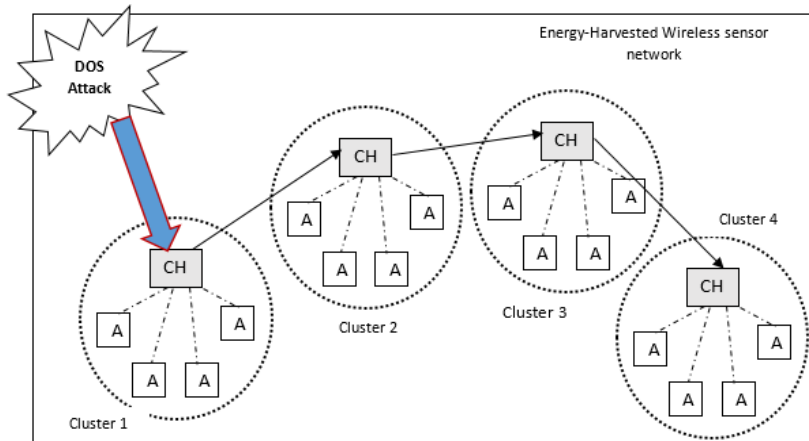


Figure 29: Proposed Wireless Sensor Network Architecture for Intelligent Agents (Sensors)

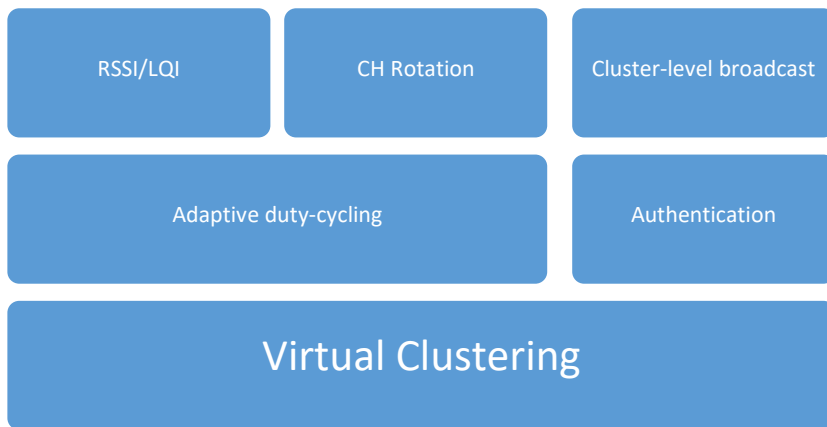


Figure 30: Model for Energy-efficiency and Security

Figure 29 above shows an attack being directed at a cluster head. The cluster head (CH) is an intelligent agent and also acts as a proxy for the member-nodes of its cluster. The moment it realizes it is under attack, it appoints one of its members as a cluster head and isolates itself from the network thereby allowing communication to continue. The learned information is then passed to other cluster heads to enable them to easily prevent the attack, in case they become the new target.

The novel architecture is intended to fit into the big picture of providing an energy-efficient and autonomous security on the IoT. This architecture builds on that of G-MAC which uses clustering to create a centralised architecture. With this architecture, the cluster heads act as a gateway, hence no communication can be made to the cluster nodes except through the gateway. However, one limitation of G-MAC is that the clusters are real and therefore do not consider mobility and change in topology. Hence the proposed architecture considers virtual

clusters. While GMAC considers energy-efficiency and network lifetime under denial-of-sleep attacks, there is no evidence of consideration of the effects on throughput and latency. The proposed architecture also intends to consider these aspects. Currently, the proposed approach is being tested on a simulator and the results will be analysed and discussed in the context of energy-efficiency and other existing approaches.

Apart from the focus on adaptability and autonomy, the proposed approach is based on a framework recommended in [3] which includes the following 4 components:

- Strong link layer authentication
- Anti-replay protection
- Jamming identification and mitigation
- Broadcast attack protection

The use of virtual rather than real clusters[18] is better in the sense that it is adaptable to any change in topology. Also, there'll also be rotation of cluster heads depending on their availability and resource consumption. Secondly, an adaptive duty cycling would then be incorporated into the virtual clusters. Thirdly, a measurement-based security technique such as RSSI can then be introduced to protect against any form of jamming. The presence of virtual clusters also be utilised to only allow cluster-level broadcasts rather than network-wide broadcasts.

Sources of energy loss

- Collision
- Overhearing
- Control Overhead
- Idle listening

Conclusion

One of the benefits of this research is that it shows the effect of duty cycling in MAC protocols and their effect on energy consumption. The interesting part is in the TunableMAC protocol which allows tuning of the duty cycle to see the energy levels. While it is obvious that energy

consumption is reduced with lower duty cycles, it is also important to know the cost involved in saving energy with regards to throughput and latency. This raised the question as to what degree of throughput is being traded to save energy. One way to answer this question is by measuring the report reception in the simulator. The results reveal that although SMAC and TMAC perform better than TunableMAC in terms of energy consumption, TunableMAC outshines them in terms of packet reception (throughput).

Chapter 4: Layered-MAC: Development of Energy-aware and Secure MAC Protocol

“You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete.”

Buckminster Fuller

4.1. Introduction

This chapter documents the development of a new MAC layer protocol which demonstrates an ability to tackle denial-of-sleep attacks better than the existing duty-cycled protocols discussed in previous chapters.

One of the goals is to compare the new protocol with three simulated protocols – Sensor-MAC (SMAC), Timeout-MAC (TMAC) and TunableMAC – based on performance metrics such as the Received Signal Strength Indicator (RSSI) and the Link Quality Indicator (LQI)

Battery-powered sensors usually have a network lifetime of 3.5 years. However, a successful denial-of-sleep attack can reduce the lifespan of these sensors to 3 days. Such significant loss of energy requires a deeper look into the problem, hence the need for a protocol that is energy-efficient and protects against these attacks. This protocol will be implemented on two different platforms: a simulated environment using OMNET++ [137] and a small proof-of-concept prototype using physical devices such as Sun SPOT [138]. More emphasis is placed on the simulation results rather than the real experiments using physical devices. This is because the simulation platform gives room for scalability allowing a variety of bridge sizes and numbers of nodes, whereas the physical platform is limited to just 3 devices. Hence, the physical devices are used as a proof-of-concept to support the simulation results. The created protocol also includes some inherent security features as part of the process of tackling denial-of-sleep attacks. The solution is evaluated based on how much of the sources of energy-loss it eliminates as well as how it responds in the event of a denial-of-sleep attack. These sources of energy loss include overhearing, idle listening, control packets overhead and collisions [120]. The new protocol tackles each of these sources of energy loss in a unique and secure way. The research begins by identifying the requirements of the protocol, specifying these requirements and prioritizing them using a technique called MoSCoW which indicates four priority categories – a) Must have; b) Should have; c) Could have; d) Would have [139]. Furthermore, different designs of the semantics of the protocol are produced and discussed. Algorithms are then produced for the protocol. These algorithms are implemented on the OMNET++ simulator and on a small test-bed with the Sun SPOT sensor devices. The language used for the simulation and device implementation are discussed critically based on different criteria. The chapter ends with a test plan on how

the two solutions will be tested in comparison to the requirements as well as in comparison to some selected existing MAC layer protocols.

Below are some research questions that underpin the new protocol presented and evaluated in this thesis:

- What happens when two nodes want to communicate with the cluster head simultaneously?
- How does this solution handle collision?
- How does this solution minimise control packets?
- How does this solution tackle overhearing?
- How does this solution minimise idle listening?
- What happens when two cluster heads want to talk to the sink at the same time?

The rest of this chapter is organised as follows. Section 4.2 provides a summary of related work elsewhere. Section 4.3 lays emphasis on the development methodology followed in arriving at this protocol. Section 4.4 gives details of the program development (construction phase) of the protocol. Section 4.5 shows the results of the experiments, both simulations and physical experiments.

4.2. Related Work

It is pertinent to note that in the context of DoS, a number of approaches exist to curb these attacks, however the majority of them are techniques that do not take energy-efficiency into consideration and even when they do, throughput becomes a trade-off which could become counter-productive in the long run. The most notable existing approaches include Gateway-MAC (GMAC) [143], Hash-based scheme [144], Clustered adaptive rate limiting [118], Fake schedule switch scheme [145], Absorbing Markov chain (AMC) model [146], Secure wakeup scheme [147], Zero knowledge protocol [148] and Cross layer mechanism [149].

Recent work [91] compares SMAC, TMAC and 802.11 in terms of energy consumption and the results show that TMAC saves 25% more energy than SMAC. In another project [92], the same protocols are compared, however, more performance metrics are looked into such as

end-to-end delay, packet delivery ratio and throughput and similarly, TMAC does better than SMAC. In [93], SMAC, TMAC and CSMA/CA are compared in terms of energy saving and peak load handling. The findings show that TMAC takes the lead in terms of energy saving but does not do as good as SMAC and CSMA/CA in terms of peak handling.

With respect to RSSI and LQI data, pattern recognition methodologies and clustering methods are used in [95] to process the data in order to find out the number of nodes in an unknown neighbouring WSN. This is done with the intention of maintaining network security. While RSSI indicates the strength of the signal, LQI indicates the quality of the signal. In [96], the limitations of RSSI which include being affected by environmental factors such as reflection, refraction, electromagnetic fields and diffraction are discussed. Hence, there's a need for another metric such as LQI, which is not affected by these environmental factors as much as RSSI. Combining these two metrics would guarantee more valid results.

One of the existing protocols that has geared towards energy-efficiency as well as security is the GMAC protocol. GMAC protocol uses the idea of a central management where nodes are divided into clusters and each cluster has a gateway node. One of the strategies used in tackling denial-of-sleep attacks is by understanding the impact of a failed node on the entire network lifetime. This is evidenced in [116] where the most critical node is assessed in terms of the impact of its elimination on the network lifetime. On the other hand, in [117] and [118], an intrusion detection scheme (IDS) is proposed whereby a DOS attacks are detected before it has any impact thereby making it preventive. In [126], focus is placed on creating hard-to-guess tokens/beacons which prevents attackers from easily guessing tokens that are aimed at depleting battery life. In [134], a cluster-based security protocol which uses digital signatures is proposed, however, this does not consider energy-efficiency. Another protocol is proposed in [135] and is based on Public key cryptography. However, this protocol seems to introduce a lot of overhead that comes with key exchange and management.

Protocols

The MAC layer of the OSI model is usually exploited by denial-of-sleep attacks and the Gateway-MAC (GMAC) is a protocol developed to guard specifically against broadcast attacks

[76]. GMAC saves a lot of energy via its centralised cluster management approach and has a better network lifetime than other protocols such as the SMAC, TMAC and Berkeley-MAC (BMAC).

Zero Knowledge Protocol (ZKP) works with the interlock protocol for key transfer and helps to tackle man-in-the-middle and replay attacks [73]. This protocol is not energy-efficient enough as it combines authentication and interlock protocol as part of its protection. It does not apply enough intelligence in tackling a variety of attacks

Schemes

The hash-based scheme protects against barrage attacks and works by protecting cluster heads against intrusion [71]. Similar to GMAC, it works by protecting the cluster heads against intrusion which is energy-efficient but not autonomous enough to guard against attacks to sensors other than the cluster heads. CARL classifies incoming packets based on authentication tests and anti-replay checks [67]. This is energy-efficient and relatively positive on throughput but has a relatively low autonomy because of its use of current host-based intrusion detection methods which do not take the distributed nature of sensors into consideration. If there is a high amount of traffic more than anticipated by the protection mechanism, then the rate limiting may go out of hand thereby even negatively affecting throughput. The fake schedule switch scheme uses the RSSI measurement aid in protecting against collision, exhaustion and broadcast attacks [75]. It works by increasing the energy usage of the attacker which may affect throughput if the fake schedule switch is not done accurately. Although there is some form of autonomy in this method, throughput remains at stake. The secure wake-up scheme finds a way to authenticate messages while ensuring that a node doesn't change to active state [72]. This is quite energy efficient in nature but due to its way of working may affect network throughput if proper authentication is not done in keeping a sensor from waking up which could negatively affect throughput. Two-tier secure scheme (TSS) integrates with a MAC protocol in addition to using a hash-chain to counter replay and forge attacks [74]. While this may affect more than one layer, it may have a negative effect on energy-consumption and even on throughput.

A. Models

The Absorbing Markov Chain (AMC) approach is a mathematical model which is used in calculating the expected death time of a sensor network and using that to determine the presence of a denial-of-sleep attack [77]. While this may have some form of autonomy in its approach, it may affect network throughput because of its procedural complexity and may sometimes not be energy-efficient. The hierarchical collaborative model (HCM) uses anomaly detection technique to detect denial-of-sleep attacks using a distributed approach whereby workload is spread across components in a hierarchical manner [65]. Its anomaly detection technique is quite static in nature and may not be intelligent enough to detect some attacks which may function below the threshold. Cross Layer Mechanism (CLM) focuses not just on the MAC layer as in the case of GMAC, but also focuses on the network and physical layers [68]. It also uses RSSI like in the fake schedule-switch scheme to prevent replay attacks. It is quite low on autonomy as it doesn't consider a variety of scenarios and can have a negative impact on throughput.

4.3. Development Methodology

Reverse engineering was one of the methods used to understand how one of the existing protocols works. The reverse engineering was done on a protocol called TunableMAC to understand the code components. TunableMAC was created using two languages- NED and C++. NED was used to define the network including its parameters and gates while C++ was used to define the behavior of the MAC protocol. The platform for these languages is OMNET++ and this was used alongside a framework for wireless sensor networks called Castalia. The C++ codes consisted of two files- a header file which contained a declaration of the variables and methods and another file which contained an initialization of the variables and implementation of the methods. The reverse engineering was done to understand the sequence and effect of the methods as well as the states of the variables. Hence a sequence diagram and state diagram are produced for the TunableMAC protocol. The diagrams provide a better understanding of where to insert the algorithms for the new protocol.

In building the new protocol, a traditional software development life cycle (SDLC) was used, particularly the **incremental model/iterative model**. This involved building the protocol in small increments. Each increment involved all the stages of the SDLC which are described briefly below:

- Requirements gathering/analysis. This stage involves understanding the problem and deciding on what needs to be done. In some cases, these two stages are split individually but considering the scope of this protocol, not much requirements are required. Hence the two stages can be combined into one. The requirement is then clearly specified.
- Design. This stage involves producing a blueprint of the internal workings of the system be it high-level or low-level design. One design could be a flow chart showing the flow of information in the protocol. Another design could be a sequence diagram showing the sequence of method calls for the new protocol. A class diagram showing the methods and variables of the new protocol is also an important design to include
- Implementation. At this stage, the coding will be done either for the simulator (in C++ and NED) or for the Sun SPOT sensor (in Java). This stage involves testing the codes to first check that they meet the requirements and that they perform better than existing protocols at tackling denial-of-sleep attacks.
- Existing approaches are classified in terms of their semantics and function and are then reviewed. Secondly, three protocols vulnerable to denial-of-sleep attacks are simulated in OMNET++ and Castalia framework to measure the RSSI and the LQI parameters of these three protocols under three network sizes. The simulation scenario is a bridge with three different sizes (40m, 200m and 1000m) and nodes (7 nodes, 34 nodes and 154 nodes respectively). The sizes and the number of nodes are increased in a linear fashion, however, this is limited to the topology of the scenario where there is one sink node in the middle. Other topologies could be considered as part of future work on mobility. The average value for the RSSI for all nodes is measured for each of the three MAC protocols under the three bridge sizes. The same is done for the LQI. The protocols simulated are discussed below:
- SMAC is a duty-cycle based MAC protocol which has a fixed listen interval. One of the disadvantages of this is that if there is very low traffic the energy is wasted during the listen phase. On the other hand, if there is very high traffic, throughput may be hindered as the listen time may not be enough. Therefore, there is a need to have an adaptive listen time which TMAC provides. Another challenge with SMAC is that the duty cycle

parameters are decided in advance and this may not be suitable for networks with rapidly changing topologies. Another challenge is that it does not have random offset and therefore there may be collisions during broadcasts and Request-To-Send/Clear-To-Send does not work for broadcasts [66].

- The TMAC protocol has two major strong areas. One of them is the adaptive listening interval which adapts the listen interval according to the traffic level. Another strong point is the future-request-to-send technique which addresses the early sleeping problem. However, in order to conserve energy, TMAC sends messages between small periods of time and this may have an effect on throughput in high traffic-load networks.
- TunableMAC [90] is a protocol that was provided along with the WSN Framework, Castalia. As the name implies, this algorithm is tuneable and allows 12 of its parameters to be tuned. This protocol can simulate many duty-cycling protocols, but it does not support unicast. It uses CSMA for its transmission, therefore its persistence and backing off policies can be tuned. Its duty cycle can also be tuned as well as the train of beacons that can be used to wake up potential receivers.

4.4. Protocol Implementation

A. *Requirements Identification*

- a) *Problem Statement.* Denial-of-sleep attacks can have a strong negative impact on the life span of battery-powered wireless sensors. Considering that the radio is the major source of energy loss, these attacks take advantage of the MAC layer, which is responsible for access to the radio, and use certain techniques to prevent the radio from sleeping thereby reducing the lifespan of the sensor. While there have been proposed solutions and techniques to tackling these attacks, only one of these solutions (GMAC) has been incorporated into a protocol and tested on a real device. There is therefore a need for more MAC layer protocols that have a form of security against denial-of-sleep attacks while aiming at maintaining the same or similar level of throughput and latency as protocols that do not have these security measures.
- b) *Protocol Requirements.* The protocol should be able to detect a denial-of-sleep attack and take measures to reduce its impact. In a case where the protocol is

not able to detect the denial-of sleep attack on time, it should take measures to reduce the other sources of energy loss that are not because of an attack. In this way the sensor can have enough energy to continue functioning until it detects the attack. To detect the attack, the first step is to understand the possible attack strategies that could be used:

- Attack from an unauthorized authenticated node - In this scenario, the node's identity is verified and valid, however the action of the node is not authorized.
- Attack from an authorized and authenticated node - This is a more dangerous scenario as it is more difficult to detect such a node. In this case the entire identity has been compromised. Sybil node attacks fall under this category.
- Attack from an unauthenticated and unauthorized node – This is the least dangerous of the three strategies.

The next step would be to identify the target of the attack. This is important because an attack on a sink node would have more impact than an attack on a cluster head. Similarly, an attack on a cluster head would have more impact than an attack on a normal node. After identifying the target, the next step is to get some data about the attacker node beginning with its address and RSSI and LQI for that node. After the node has been identified, the next step is to isolate the attacker and make the network inaccessible by that node.

The life cycle of the MAC layer is divided into four stages as follows:

- The start-up stage. This stage involves initializing the variables with start-up information about the packets, sensors and communication. This also involves getting the node to sleep if there is no information from the radio layer or there's nothing left in the buffer to send to the network layer. At this stage the cluster heads will also be set up.
- The transmit stage. This stage involves transmitting information received from the network layer to the radio layer or transmitting information received from the radio layer to the network layer.
- Carrier sensing stage. Before transmitting, a node may want to apply some CSMA techniques or use request-to-send or clear-to-send packets to avoid collisions and overhearing. While RTS/CTS could be helpful in avoiding collisions, it has one

disadvantage of increasing the control packet overhead which further increases the energy consumption. CSMA on the other hand has some back-off techniques that work based on probability and may not always be accurate and could lead to deadlock problems where a node is not able to transmit because it is waiting endlessly for an opportunity to transmit.

- The receive stage. This involves staying in a receive mode and waiting for information from the radio layer which is coming from another node. The data received has to be checked to know the type of data (control packet or actual data).

B. *Functional Requirements*

As mentioned earlier, the MoSCoW technique is used to prioritize the requirements based on the following categories:

Must Have

- The sink node should be able to get the RSSI and LQI values of every sensor it receives data from.
- Each node should know how far it is from the sink node and use that to decide who becomes a cluster head.
- The protocol should be able to adjust the duty cycle at run-time based on the traffic.
- The protocol should allow cluster heads to be appointed and rotated at intervals, if need be.
- The protocol should allow for a node to be isolated from the network when it has been discovered to be an attacker node.

Should Have

- Nodes should be able to find the least expensive route to communicate their data.
- Cluster heads should be able to communicate using code division multiple access.

Could Have

- Supervised learning could be applied on the data collected from the base station.

Would Have

- Nodes cannot be powered by Solar energy.

I. Program Development

i. Methods and Variables

Methods/Functions	Data requirements
getDistance()	Double distance
getRSSI()	Double RSSI
getLQI()	Double LQI
createClusterHeads() ()	int noOfClusterHeads
assessPackets()	Double packetSize
isolateNode()	int nodeID

A. *Algorithm for Proposed MAC Protocol*

- *MAC layer receives number of nodes from the application layer.*
- *Sink node gets the distance of all nodes.*
- *Sink node appoints the node with closest proximity as a cluster head.*
- *If a cluster head has more than 5 nodes assigned to it, then another cluster head is appointed.*
- *Nodes must only communicate to their cluster heads not to other nodes.*

- The cluster head then passes the information to the sink nodes. If the sink node is too far from the cluster head, then the data is passed to other cluster heads closer to the sink node.
- After every 5 minutes, a new cluster head is appointed to ensure security and to also manage the energy-efficiency.

B. Protocol Design

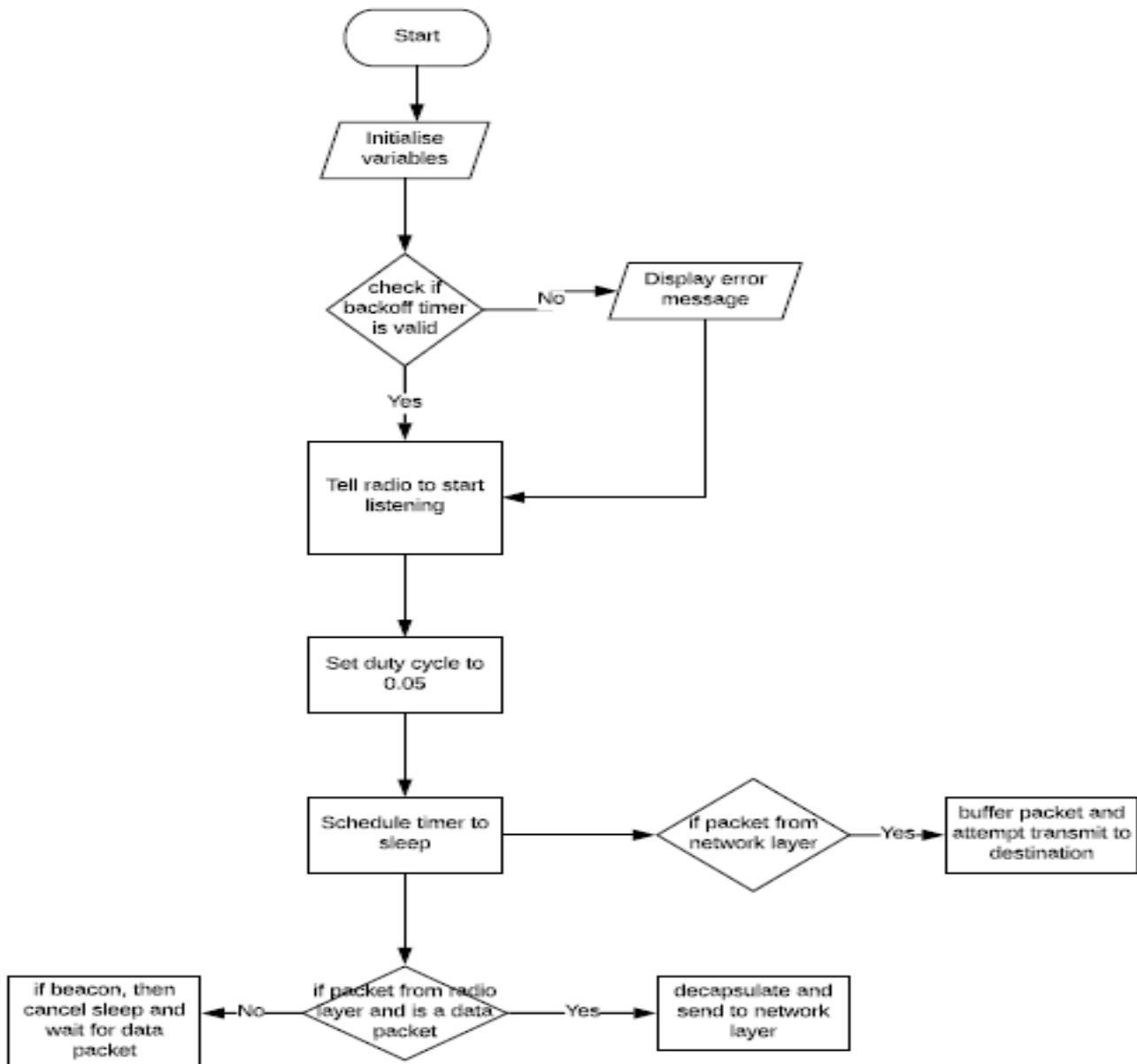


Figure 31: Flow chart showing MAC layer Setup

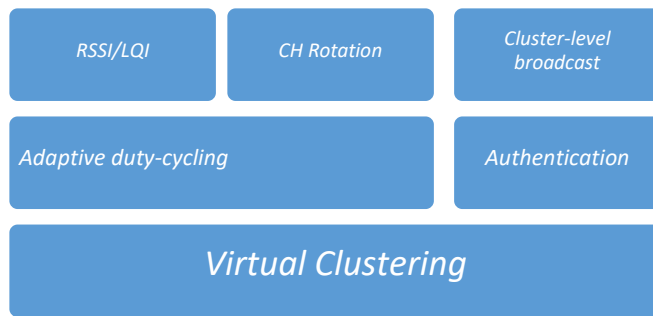


Figure 32: Conceptual model of components of proposed proactive energy-efficient MAC protocol.

Figure 32 shows the conceptual design of the protocol. The lowest layer is virtual clustering which involves grouping the sensors based on their proximity. The benefits of keeping the clusters virtual is that if the position of the sensor is changed, then the cluster can be reconfigured. The adaptive duty cycling is adopted from TMAC whereby the duty cycle automatically adjusts to the amount of traffic.

Getting the positions and distance between nodes

This involves using a points-based system/GPS to get the x and y coordinates of the sensor. After getting the x and y coordinates for each node, the next step would be to calculate the distance between the two nodes. The distance between the nodes is calculated using the following formula based on Pythagorean theorem:

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Where d = distance

x_2 = the x coordinate for node 2

x_1 = the x coordinate for node 1

y_2 = the y coordinate for node 2

y_1 = the y coordinate for node 1

One of the advantages of using GPS is its relative better accuracy at identifying the location of a device. However, this method may not work for sensors located in areas where the GPS may not work.

Another way to achieve this by using the Castalia framework is to get the Received Signal Strength Indicator (RSSI) and the Link Quality Indicator (LQI). However, this method has its

disadvantages. When using RSSI measurements, the channel model parameter variation could lead to dead spots, multi-path effect, interference and noise could affect the signal strength and link quality. One method of improving the accuracy is to combine both RSSI and LQI[141] is making measurements and this was the method used for this project.

Algorithm for position and distance of nodes

- *Each node waits for a random time and makes a broadcast.*
- *The broadcast packet contains the schedule and each node follows the schedule it receives.*
- *Each node also keeps the RSSI/LQI of the packet it receives.*
- *Get position of nodes.*
- *Base station creates a map of the distance between nodes using RSSI.*
- *Identify best distance from each node.*
- *Create Clusters based on best distance.*
- *Use CDMA to communicate between cluster heads.*
- *Stop.*

Base station creates a map of the distance between the nodes

This involves creating a matrix that maps the distance between each node. If there are ten nodes, each node maps the distance with 9 other nodes. The mapping is based on the RSSI and LQI values of the sensor nodes.

Identify best distance from each node

Based on the map created above, the best distance for each node is then calculated. The reason for using distance is to enhance the energy-efficiency in the nodes when transmitting data.

Create clusters based on best distance

Based on the best distance, the clusters are then created with cluster heads managing nodes within the closest distance. Only the cluster heads communicate directly with the base station/sink node. The cluster heads will be changed at intervals to increase security.

Algorithm for cluster creation

- *If nodes have the same schedule, they belong to the same cluster.*
- *Cluster nodes can only communicate with their cluster head.*
- *Cluster heads then communicate with the sink node.*

Use CDMA to communicate between cluster heads

Code division multiplexing is then used only for communication between cluster heads to ensure security and prevent denial-of sleep attacks. This stage has more to do with the physical layer.

Parameters for existing protocols (TMAC and 802.15 MAC)

In building the new protocol, parameters from existing protocols (Time-out MAC and 802.15.4 MAC) were used.

```
//mac layer parameters
int macMaxPacketSize = default (0);
int macPacketOverhead = default (14);
int macBufferSize = default (32);

bool enableSlottedCSMA = default (true);
bool enableCAP = default (true);
bool isFFD = default (false);
bool isPANCoordinator = default (false);
bool batteryLifeExtention = default (false);

int frameOrder = default (4);
int beaconOrder = default (6);
int unitBackoffPeriod = default (20);
int baseSlotDuration = default (60);

int numSuperframeSlots = default (16);
int macMinBE = default (5);
int macMaxBE = default (7);
int macMaxCSMABackoffs = default (4);
int macMaxFrameRetries = default (2);
int maxLostBeacons = default (4);
int minCAPLength = default (440);
int requestGTS = default (0);
```

Figure 33: TMAC parameters

Figure 33 shows the default parameters for TMAC in OMNET++ simulator. Figure 34 shows the parameters for IEEE 802.15.4 MAC on the OMNET++ simulator.

```

//mac layer packet sizes, these parameters are described in TMacFrame.msg file
int ackPacketSize = default (11);
int syncPacketSize = default (11);
int rtsPacketSize = default (13);
int ctsPacketSize = default (13);

//mac layer parameters
int macMaxPacketSize = default (0); //no limit on frame size
int macPacketOverhead = default (11); //DATA frame overhead is described in TMacFrame.msg
int macBufferSize = default (32); //buffer of 32 packets by default

//TMAC protocol parameters
int maxTxRetries = default (2);
bool allowSinkSync = default (true); //This parameter allows sink node to start synchronisation immediately
bool useFrts = default (false); //enable/disable FRTS (Future Request To Send), true value not supported
bool useRtsCts = default (true); //This allows to enable/disable RTS/CTS handshake
bool disableTAextension = default (false); //disabling TA extension effectively creates an SMAC protocol
bool conservativeTA = default (true); //conservative activation timeout - will always stay awake for
//atleast 15 ms after any activity on the radio

double resyncTime = default (6); // timer for re-sending SYNC msg, in seconds
double contentionPeriod = default (10); // 10 ms
double listenTimeout = default (15); // 15 ms, is the timeout TA (Activation event)
double waitTimeout = default (5); // timeout for expecting a reply to DATA or RTS packet
double frameTime = default (610); // frame time (standard = 610ms)

int collisionResolution = default (0); // collision resolution mechanism, choose from

```

Figure 34: IEEE 802.15.4 parameters

Table II shows the static design of the system which includes the classes required to build the program.

II. Classes

Cluster
-int ClusterID
-double distance
+createCluster
+addNodeToCluster()
+getDistance(String a, String b)

III.

Sensor
-int SesnsorID -String SensorAddress
+sleep() +wakeUp() +getRSSI() +getLQI() +getDistancefromSink()

4.5. Experiments

A. Test Plan

III. Test Cases and Corresponding Actions

ID	Test Case	Description	Actions
1	Collision	This checks that the protocol plays a role in reducing reduction	Compare the number of transmitted packets to the number of received packets.

2	Control Overhead	This checks that the protocol reduces the amount of control overhead	Track the size of data used for control overhead
3	Idle Listening	This checks that the protocol plays a significant role in reducing	Measure how long a node stays idle before transmitting data.
4	Overhearing	This checks that the protocol reduces the chances of a node hearing a packet that was meant for another node.	Measure how much energy is wasted listening to packets meant for other nodes.

Test Results from Simulator

In this section, the results from both the OMNET++ and Castalia simulator and the Sun SPOT devices are compared. Furthermore, these results from both simulator and device for the Layered-MAC protocol are then compared with the results from SMAC and TMAC. The results are shown below. GMAC has not been used in the comparisons for two reasons. Firstly because there is no model of it in the Castalia simulator and secondly because GMAC does not give any considerations to reception(throughput) at the sink.

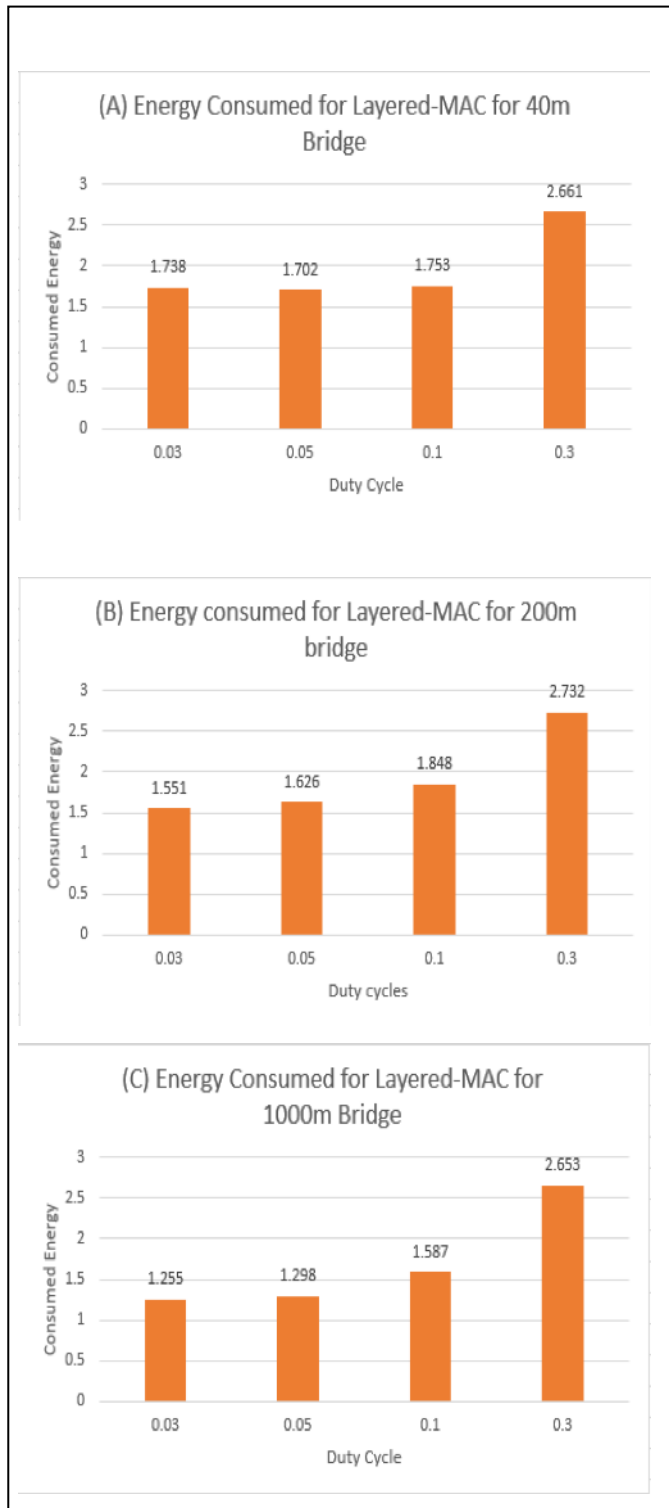


Figure 35: Energy Consumption for 40m, 200m and 1000m Bridge

- a) *Consumed Energy*. The first graph in Figure 35(a) shows the energy consumed for Layered-MAC under different duty cycles in a 40m bridge. The consumed energy

increases as the duty cycle increases. The second graph in Figure 35 shows the energy consumption for Layered-MAC in a 200m bridge. The energy consumed in the 200m appears less than the energy consumed in 40m bridge. The third graph in Figure 35 shows the energy consumption for the 1000m bridge for which energy consumption is the lowest.

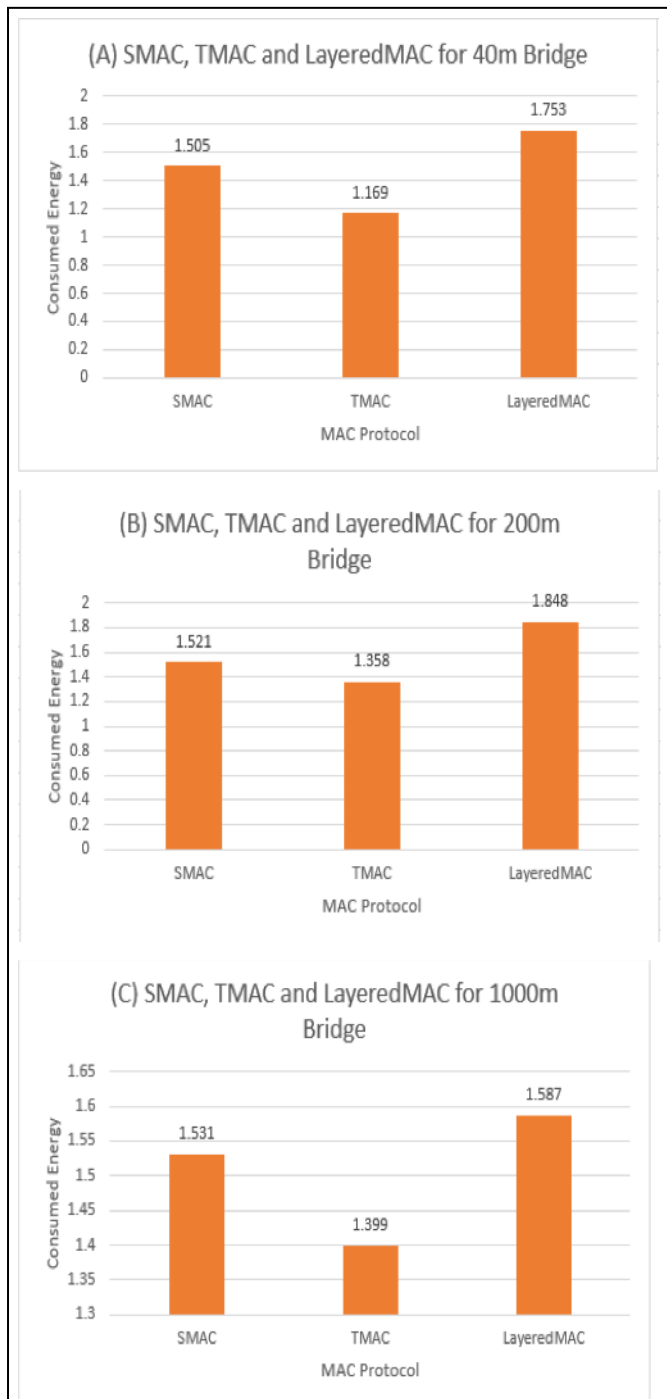


Figure 36: Energy Comparison for SMAC, TMAC and Layered-MAC on 40m, 200m and 1000m Bridge.

b) *Energy Comparisons.* The graphs in Figure 36 show a comparison of Layered-mac with two other protocols (TMAC and SMAC). The comparison is based on the energy consumption of the sensors. The graph in Figure 36(a) shows that TMAC consumes the least energy while Layered-MAC consumes the most energy. However, this does not take into consideration the packet reception at the sink. In the second graph, energy is compared on a 200m bridge for SMAC, TMAC and Layered-MAC and

Layered-MAC consumes the most energy at 1.848 while TMAC consumes the least energy at 1.358.

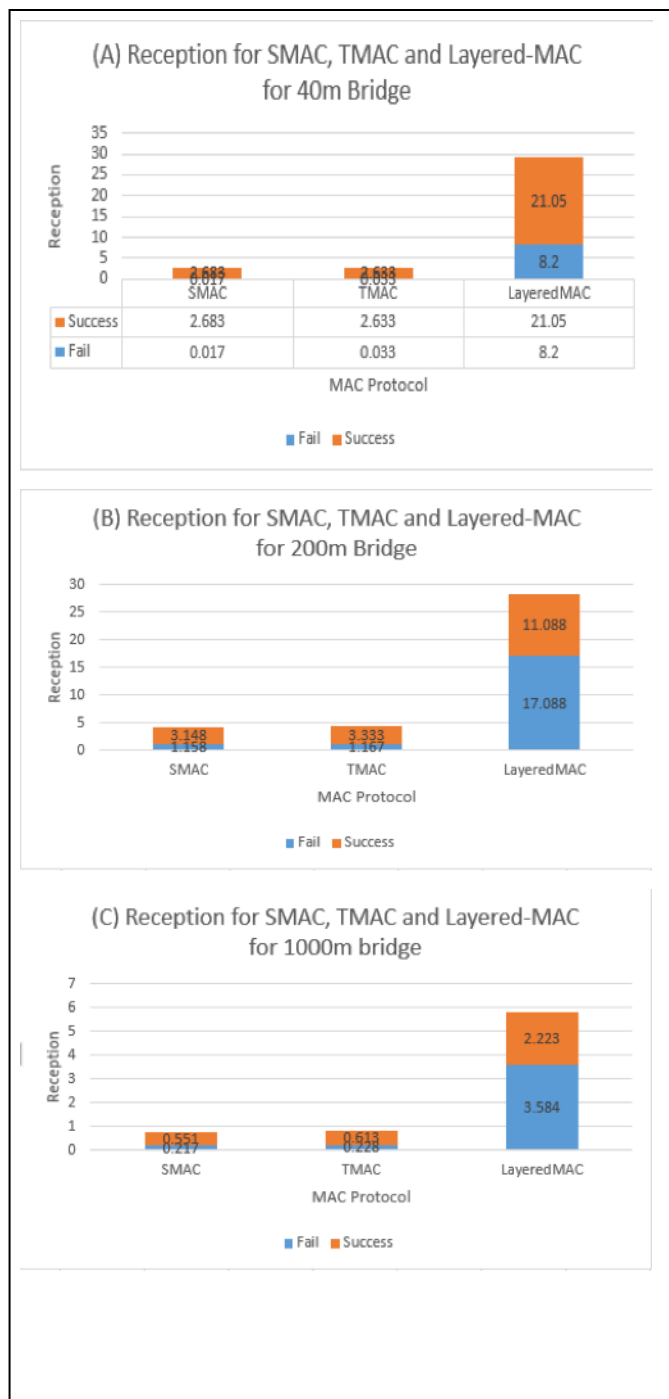


Figure 37: Reception for SMAC, TMAC and Layered-MAC on 40m, 200m and 1000m Bridge

c) *Reception Comparisons.* The second graph in Figure 37b shows that layered-MAC has a better reception at the sink in terms of data throughput with success of 11.088 and

failure of 17.088 compared to SMAC and TMC which are significantly lower. The third graph (Figure 37c) shows that layered-MAC has a better reception at the sink in terms of data throughput. There is a greater amount of succeeded and failed packets than in TMAC and SMAC.

In conclusion, while the energy consumption is total is higher for Layered-MAC than TMAC and SMAC, the receptions results show that Layered-MAC still does better in terms of performance and even energy consumption when measured in terms energy per successfully received packets received packets.

Another interesting observation is that although more energy is pent as the bridge size increases, the successfully received packets shows a downward trend for both TMAC and SMAC but is slightly different for Layered-MAC.

Hence, on a 40m bridge for LayeredMAC, 1.752 is spent for 21.05 received packets. On a 200m bridge, 1.848 is spent for 11.088 received packets and 1.587 for 2.223 received packets on a 1000m bridge. Summing up the received packets for TMAC and SMAC put together still doesn't get up to half the reception for Layered-MAC.

4.6. Results and Analysis

For RSSI, the higher the value, the higher the signal strength. For the LQI parameter, the lower the value, the better the quality. Figures 38-43 show the RSSI and LQI for SMAC, TMAC and TunableMAC respectively. Figures 44 and 45 show the three protocols in two graphs for RSSI and LQI respectively.

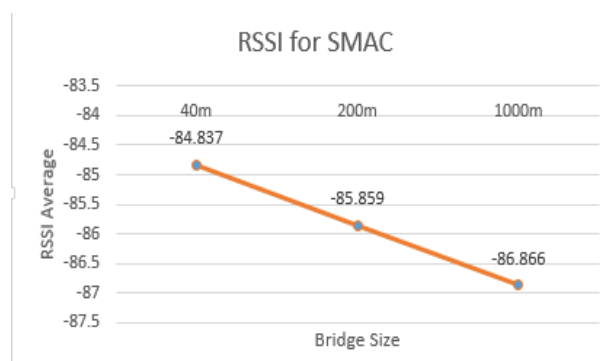


Figure 38: RSSI for SMAC protocol under three network sizes

Figure 38 shows how the RSSI parameter gets weaker as the network size increases for the SMAC protocol. It is important to note that SMAC has a fixed-duty cycle

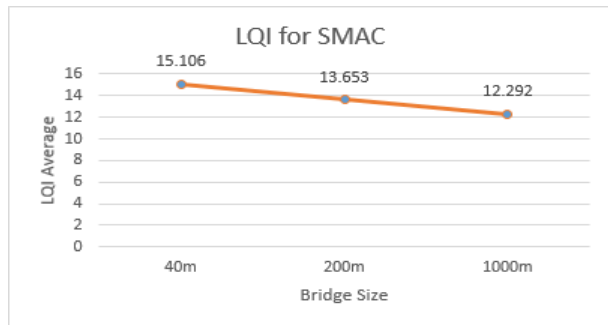


Figure 39: LQI for SMAC under three network sizes

Figure 39 shows how the link quality gets better with increase in network size for the SMAC protocol. While TMAC performs better than SMAC in terms of RSSI under the 40m bridge - as seen in Figures 38 and 40, SMAC performs better than TMAC in terms of LQI - as seen in Figures 39 and 41.

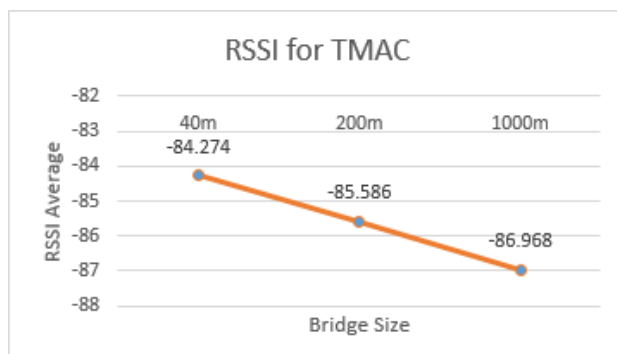


Figure 40: RSSI for TMAC under three network sizes

Figure 40 shows how the signal strength reduces as the network size increases. Compared to Figure 38, the RSSI parameter for the 40m bridge in Figure 40 is slightly stronger than that of Figure 38. The only exception is in the 1000m bridge where SMAC performs better.

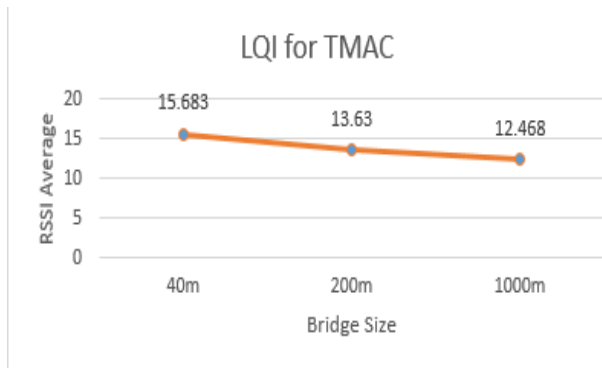


Figure 41: LQI for TMAC under three network sizes

Figure 41 shows how the link quality improves as the network size increases. Overall, the LQI for TMAC is lesser than that of SMAC.

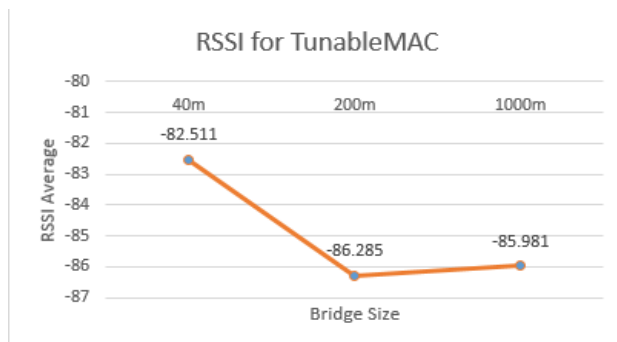


Figure 42: RSSI for TunableMAC under three bridge sizes

In Figure 42, signal strength weakens as the network size increases from 40m to 200m but then the signal strength slightly gets better with the 1000m bridge. The RSSI for the 40m bridge is stronger than in Figure 38 and Figure 40 and also stronger, overall, than SMAC and TMAC.

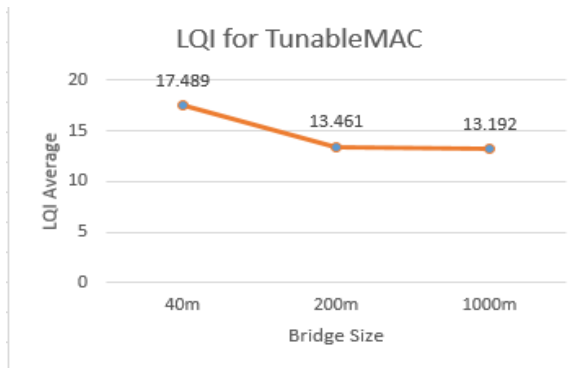


Figure 43: LQI for TunableMAC under different bridge sizes

In Figure 43, the link quality gets better as the network size increases. The overall LQI for TunableMAC is weaker than SMAC and TMAC.

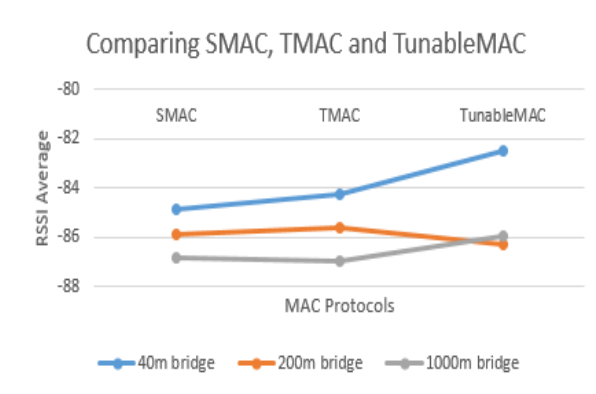


Figure 44: Comparing RSSI for SMAC, TMAC and TunableMAC

In Figure 44, RSSI is strongest in the 40m bridge with TunableMAC having the best performance. In the 1000m bridge, TunableMAC also has the strongest signal strength among the three protocols. Only in the 200m bridge does this trend with TMAC having the strongest RSSI parameter followed by SMAC.

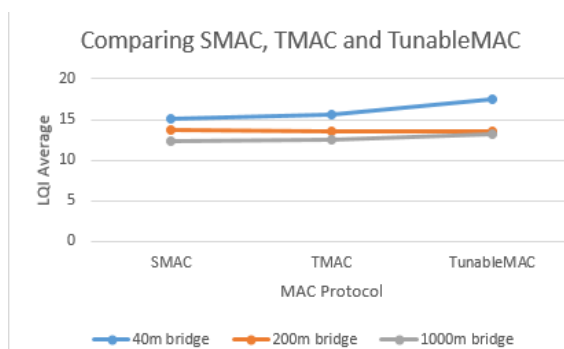


Figure 45: Comparing LQI for SMAC, TMAC and TunableMAC

In Figure 45, the 1000m bridge has the best link quality with SMAC having the strongest link quality. SMAC also maintains the strongest link quality in the 40m bridge but performs differently in the 200m bridge where TunableMAC has the best performance.

4.6.1. Simulation results for the protocols under attack

Simulation Scenario

The TunableMAC protocol is used alongside two other protocols, SMAC and TMAC in the simulation to understand the energy consumption and reception under an attack. For this scenario, a 200m bridge is used with 3 of the nodes as compromised malicious nodes which use a broadcast attack to stop nodes from sleeping. The broadcast attack is carried out by continuously flooding the network with broadcast messages from these three nodes. The simulation is about the structural health monitoring of a bridge. Sensing nodes are placed in a grid with a sink node in the middle. A car moves on the bridge every five minutes and triggers nodes along its path.

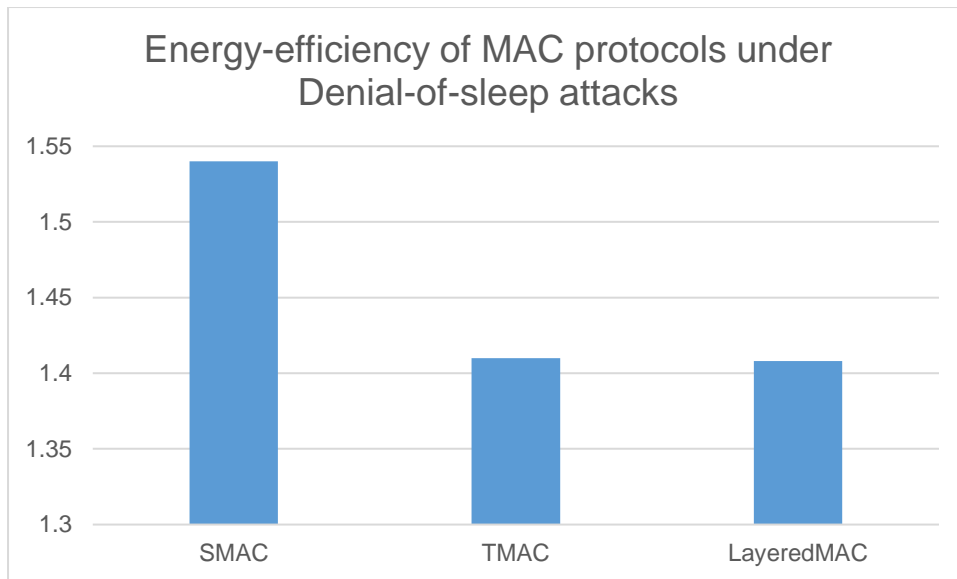


Figure 46: Energy Efficiency for SMAC, TMAC and LayeredMAC

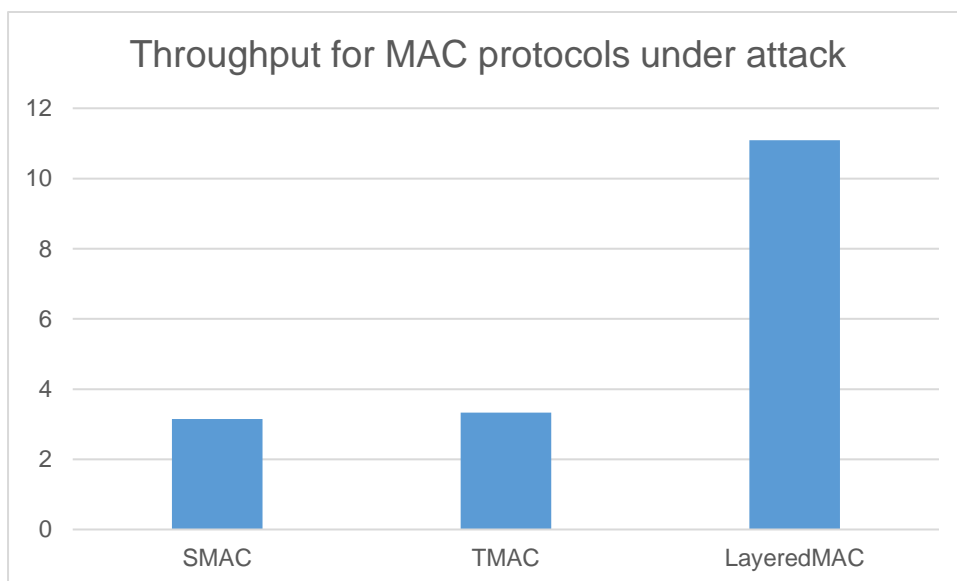


Figure 47: Throughput for SMAC, TMAC and LayeredMAC under Denial-of-sleep attack

Discussion of Results

Figures 46 and 47 show the energy-efficiency and throughput for 3 MAC protocols respectively, including the new protocol (LayeredMAC), under a denial-of-sleep attack. GMAC has not been used in the comparisons for two reasons. Firstly, because there is no model of it in the Castalia simulator and secondly because GMAC does not give any considerations to reception(throughput) at the sink.

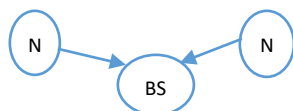
Figure 46 shows that under the DOS broadcast attack, SMAC consumes the highest amount of energy at 1.54 mjoules. TMAC consumes much lower energy than SMAC at 1.41 mjoules. LayeredMAC consumes the least energy slightly below TMAC at 1.408 mjoules. The fixed duty cycling for SMAC justifies the relatively high energy consumption. TMAC on the other hand supports adaptive duty-cycling, hence there is better energy-efficiency than SMAC. LayeredMAC on the other hand goes a step further than just adaptive duty-cycling to also detect signal strength and link quality, hence the slightly better energy-saving than TMAC.

In terms of throughput, figure 47 shows significant difference in throughput between LayeredMAC and TMAC and SMAC combined. This is partly because of LayeredMAC's ability to detect a malicious node and adjust duty cycling to bypass/isolate the malicious node.

Physical Device Experiments (Sun SPOT)

This section presents the experiments with three Sun SPOT devices. One of them is a base station and the other two are temperature sensors.

- a) *Centralized Architecture*. The first experiment was a centralized approach where one node was assigned the role of a sink node and the other two nodes had to forward temperature data sensed to the sink node. The layered-MAC protocol was implemented on the sensors using Java. Netbeans Integrated Development Environment was used for writing the Java codes.



Centralised Architecture Showing Connection Between Two Nodes and Base Station.

- b) *Ad-hoc Architecture*. The second experiment was a de-centralized approach whereby the sensor nodes may or may not be directly connected to the sink node depending on their distance from the sink node. The sensor nodes send the data to the nearest node to them.



Ad-hoc Architecture Showing Connection Between Two Nodes.

c) *Details of the Sun SPOT Sensors.* A Sun SPOT sensor consists of three basic elements:

- **Battery:** Has a lithium rechargeable battery
- **Processor Board:** This consists of a 32 bits ARM920T processor with a speed of 18 MHz. On the board is also a radio based on IEEE 802.15.4 standard. A RAM of 512KB as well as 4MB of flash memory is also present.
- **Sensor Board:** The sensor board consists of 3 axes accelerometer 2G/6G, a light sensor, a temperature sensor, two buttons, eight 24 bits RGB leds, 6 analog inputs, 5 general I/O pins and 4 high current output pins.



Sun SPOT Sensor.

In terms of software, a virtual machine called Squawk which is based on Java Micro Edition (J2ME) runs on the device. This software is designed for devices with limited memory. A transducer library exists which supports all the sensors and helps with energy-efficiency. Mesh networking is supported by this sensor.

d) *Setting up the Sensor Network.*

IV. Power Usage for a Typical Sun SPOT [27]

<i>Processor board state</i>	<i>Radio</i>	<i>Sensor Board</i>	<i>Current Draw</i>
Deep sleep mode ¹	Off	Any	~33 microamperes
Shallow sleep ²	Off	Not present	~24 milliamperes
Shallow sleep	On	Not present	~40 milliamperes
Awake, actively calculating	Off	Not present	~80 milliamperes
Awake, actively calculating	On	Not present	~98 milliamperes
Shallow sleep	Off	Present	~31 milliamperes
Shallow sleep	On	Present	~46 milliamperes
Awake, actively calculating	Off	Present	~86 milliamperes
Awake, actively calculating	On	Present	~104 milliamperes

1. In deep sleep, the processor and sensor board are both powered down.

2. Shallow sleep means devices active, but no active threads.

Table IV shows the power usage of the Sun SPOT in different modes. Considering that the goal is to improve the energy-efficiency of the sensors, it is important to understand the current draw of energy as shown in the figure above.

e) Carrying out the Experiments.

```
// locate a temperature sensor
ITemperatureInput temp =
    (ITemperatureInput)Resources.lookup(ITemperatureInput.class);

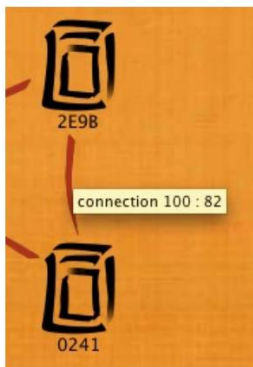
// define the callback
IConditionListener freezeListener = new IConditionListener() {
    public void conditionMet(ITransducer sensor, Condition condition) {
        System.out.println("Brrr... it's cold!");
    }
};

// define the condition - check temperature every 30 seconds
Condition freeze = new Condition(temp, freezeListener, 30 * 1000) {
    public boolean isMet() {
        if (((ITemperatureInput) sensor).getCelsius() <= 0.0) {
            stop(); // stop checking once temperature goes below freezing
            return true; // condition met: notify listeners
        } else {
            return false; // condition not met
        }
    }
};
freeze.start(); // start monitoring the condition
```

Code Snippet for Monitoring Temperature.

The code in Figure 11 was implemented to enable the sensors to sense the temperature and send a message when the temperature goes below 0 degrees.

f) Experimental Results.



Link Quality Between Nodes.

The above figure shows the link quality which works alongside the received signal strength indicator in helping with the measurement of distance between nodes as discussed in [142]. The power stats during experiment without Layered-MAC protocol are:

Power controller version: PCTRL-2.01

Battery charging current: 2 mA

Current drawn from battery: 90 mA

Max current drawn: 287 mA

Battery voltage: 3493 mv

Main board I/O voltage: 3118 mV

ARM CPU voltage: 1836mV

External Voltage: 0mV

USB voltage: 93 mV

Power fault status: No power fault

Reason for last interrupt: Cold boot, Button event, Sleep

Start-up time : 1986 us

Externally powered : false

The results show the energy consumption before the Layered-MAC protocol was introduced. After implementing the Layered-MAC protocol the current drawn from the battery was reduced from 90 mA to 87 mA for one sensor and the maximum current drawn was reduced from 287 mA to 278 mA. This seems like a small difference with one sensor but will have a huge impact when looking at a larger network of 1000 nodes as seen in the simulations done earlier.

4.7. PROPOSED AUTONOMOUS APPROACH

In addition to the aforementioned results, an approach is proposed that could help curb and minimize the impact of a denial-of-sleep attack.

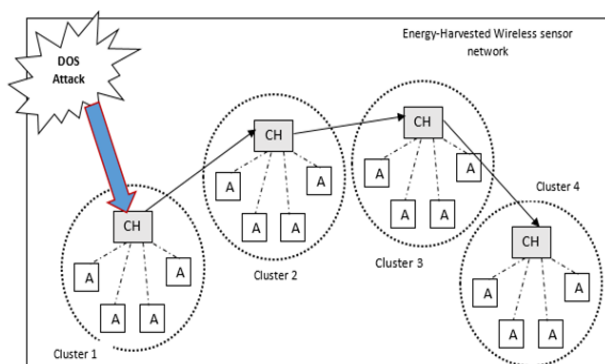


Figure 48: Proposed WSN architecture for intelligent agents

Figure 48 shows the architecture of the proposed approach [94] which is an improvement of two existing approaches – GMAC and HCM. As discussed earlier, while GMAC and the hash-based scheme use centralised approach via cluster heads, HCM and the distributed wake-up

scheme use a distributed architecture. Although these approaches seem very useful, they do not take into consideration the size of the network especially on a large scale.

Our proposed architecture is based on a combination of both the centralised and the distributed approach thereby taking advantage of the benefits of both GMAC and HCM. It would involve the use of intelligent agents whereby each sensor becomes an agent which can sense data and take responsive action with the workload dynamically distributed among them. However, this would not function optimally with the current battery-powered sensors, but rather an energy harvested IEEE 802.15.4 WSN [78]. This is necessary because the dynamic distribution would lead to an increase in processing power thereby consequently increasing energy costs.

Earlier work [79] introduced the concept of virtual clusters whereby nodes are grouped into the same subnet and presented as a single resource. The WSN will be dynamically divided into clusters with cluster heads appointed for each cluster. In this approach, if a sensor encounters or senses a denial-of-sleep attack, it immediately takes responsive action and also broadcasts the information to the rest of the appointed cluster heads via a “rumour” approach which may consume more bandwidth than processing power. The “rumour” approach is coined from the term “routing by rumour”, which explains the semantics of distance-vector routing protocols whereby each router sends messages to its nearest neighbour until the information propagates to all the routers. In this case, the cluster heads send information to the nearest cluster head and it continues that way until the information gets to all the cluster heads which then pass the information to their clusters. The cluster heads then relay this information to the sensors in their clusters.

4.8. CONCLUSION

It is important to look at how the research questions discussed in the introduction have been addressed. CSMA with collision avoidance is used to prevent collisions when two nodes are trying to communicate at the same time. Acknowledgements are not required to reduce the number of control packets. Minimizing the number of broadcasts by applying distance measurements and using a routing-by-rumor approach helps reduce overhearing. Idle listening is reduced by adaptive duty cycling. One of the benefits of this new protocol is that it is multi-layered and touches on different aspects. First it deals with virtual clustering [136], authentication, RSSI and LQI measurements which helps with security. It also measures the distance between nodes and supports adaptive duty-cycling which helps with

energy-consumption. Furthermore, the physical device experiments validate the results of the simulations as the energy measurements derived from the device have a correlation with the results from the Sun SPOT devices.

The novelty of this chapter lies in the simulation results and the comparisons between the three protocols as well as the new proposed architecture for tackling denial-of-sleep attacks. As discussed in Section II, although there have been comparisons of SMAC and TMAC, as well as analysis of RSSI and LQI data, however, no research to the best of our knowledge has compared these protocols in the context of what impact they have on RSSI and LQI values.

Chapter 5: Results and Future work

*“The proactive approach to a mistake is to acknowledge it instantly, correct
and learn from it.”*

Stephen Covey

5.1. INTRODUCTION

Media access control (MAC) protocols play a huge role in the energy-efficiency of wireless sensor networks (WSN) especially as these networks have resource-constrained devices which are mostly battery powered. The radio is the major source of energy consumption in these devices and access to radio is controlled by the MAC layer. Hence, the MAC protocols use duty cycling as one of the ways for saving energy by making nodes go to sleep when they are idle and having them only wake up when they need to transmit or receive data.

While duty cycling can save energy, it can also negatively affect throughput. This gives rise to the need to experimentally observe the effects of duty cycling on energy consumption and throughput in different MAC protocols to understand which other variables, beyond the duty cycles, could help to improve the energy-efficiency balance.

Understanding the various sources of energy loss such as collision, overhearing, idle listening, and control overhead is important as this would help give insight into what techniques other than duty cycling can help save energy.

Energy loss can be random or can be caused by an intentional attack, one of which is called a denial-of-sleep (DoS) attack [97], [98], [99], [115]. Various methods are used to carry out a DoS attack. These are commonly classified as sleep deprivation, barrage, synchronization, replay, collision and broadcast attacks [100]. These attacks take advantage of vulnerabilities such as frame collisions, message overhearing and idle listening [101]. On the other hand, various approaches have been proposed to detect and prevent DoS attacks. Existing comparisons of these approaches are qualitative in nature with a focus on their strengths and weaknesses [100].

It is pertinent to note that in the context of DoS, a number of approaches exist to curb these attacks, however the majority of them are techniques that do not take energy-efficiency into consideration and even when they do, throughput becomes a trade-off which could become counter-productive in the long run. The most notable existing approaches include Gateway-MAC (GMAC) [105], Hash-based scheme [106], Clustered adaptive rate limiting [99], Fake schedule switch scheme [107], Absorbing Markov chain (AMC) model [108],

Secure wakeup scheme [109], Zero knowledge protocol [110] and Cross layer mechanism [111].

The aim of this research therefore is to analyse the effects of duty cycling on energy efficiency and throughput in three MAC protocols and analyse the results to find clues as to how to create “proactive energy efficiency” – energy conservation that still supports throughput while minimising the impact of DoS attacks. Thus, a simulation experiment is carried out based on three duty-cycled protocols to monitor their effect on energy consumption as well as their effect on throughput. The analysis of the experimental results is then followed by a recommendation of a model for building an improved proactive energy-efficient protocol. The chapter concludes with plans for future work.

METHODOLOGY

A. Existing duty-cycle protocols

Duty cycling involves a cycle of an active period and a sleep period. However, these schedules need to be synchronised in some way to allow for harmony rather than counter-productivity. Hence, the need to consider several categories of MAC layer protocols [102] as listed below:

- Static scheduled protocols (SMAC);
- Adaptive group schedule (TMAC);
- Adaptive repeated schedule (SCP-MAC);
- Adaptive staggered schedule (DMAC);
- Adaptive reservation schedule (RMAC).

B. Simulation

The simulation was carried out using OMNET++ and Castalia framework [113]. It involves experiments with SMAC and TMAC which are the most popular among the duty-cycled protocols as well as the TunableMAC protocol, discussed later in Section III. Measurements were performed under different network sizes while observing the energy consumption and reception.

Our simulation experiments are based on a bridge test application whereby the structural health of a bridge is monitored, a 40-metre bridge with 7 nodes and a 200-metre bridge with 34 nodes as well as 1000-metre bridge with 154 nodes. Each node is arranged in the form of a grid is 20 metres apart from the next node, hence this explains the number of nodes which correspond to the length of the bridge. A sample interval of 1000ms is used, while the consumed energy is measured in megawatts. To reduce randomness in the results, a random seed value has been used and set to 10 which indicates the number of repetitions of the simulation. The value 10 was determined by using a 95% confidence interval along with manually checking the smoothness and precision of the results by trying out different seed values and observing the results.

5.2. Algorithms

A. SMAC (Static-Scheduled)

The SMAC protocol [112] has a static schedule which is fixed during network setup. This means that nodes have a fixed duty cycle (durations for sleep and listen are fixed). The implications of this is that in low traffic, energy may be wasted during the fixed listen durations whereby nodes will stay awake unnecessarily for the sake of completing the schedule, instead of sleeping.

Algorithm for SMAC

- Node listens to medium for a certain period by performing Carrier sense (CS).
- If node receives schedule from neighbour, it chooses it and becomes a follower.
- The node broadcasts its new schedule after a random delay.
- Else, the node determines its own schedule and broadcasts it to neighbours.
- Node sends message using Request-to-send (RTS) by randomly selecting a time slot.
- If a node hears an RTS or Clear-to-send (CTS) message, it goes to sleep.

B. TMAC (Adaptive Grouped Schedule)

Unlike SMAC where the duty cycle is fixed, the TMAC allows for flexibility during a node's listen time according to the traffic density. The minimum time for which a node stays awake before going to sleep is the adaptive timeout (TA). Other packets used by TMAC include

Data-send (DS) which is a dummy message sent when a node wants to transmit at the same time it hears a future RTS packet. This helps prevent collision by delaying transmission.

Algorithm for TMAC

- Nodes wake up at the beginning of the slot.
- Node sleeps if no activity is observed.
- If a node overhears a CTS, it stays awake till the end of the transmission.
- At the end of the transmission, the node contends for the medium again and begins transmission if it wins the medium.
- If a node has pending data, it informs its intended receiver using a future RTS technique to avoid the early-sleeping problem.
- The receiver remains active until the message is received.
- If another node is about to transmit and overhears a future RTS packet, it sends DS to its receiver to delay transmission.

C. SCP-MAC (Adaptive Repeated Schedule)

This protocol improves the grouped schedule protocols by eliminating the early sleep problem by creating repeated small active periods in one slot.

Algorithm for SCP-MAC

- Nodes perform CS by randomly selecting a slot within the first contention window.
- If channel is idle sender transmits a short wake-up tone timed to intersect with the receiver's channel polling.
- After waking up the receiver, the sender transmits the data packet.
- Else node aborts transmission until next frame.

D. DDMAC (Adaptive Staggered Schedule)

This works very well with the tree-based topology in such a way that the schedule of one node is synchronised with the schedule of the next hop node.

Algorithm for DMAC

- Node sends a packet to the next hop node on the route.
- The node awaits acknowledgment and the next hop node enters receiving state at the same time.
- If this next hop node is not the destination node, the node enters sending state to forward the packet.
- Else the final destination has been reached.
- If sender does not receive ACK, it queues the message until the next sending.
- If node has multiple packets to send, it increases its duty cycle and requests other nodes along the sink route to increase their duty cycles too.

E. RMAC (Adaptive Reservation)

This protocol allows nodes to negotiate their schedules.

Algorithm for RMAC

- During the Synchronisation (SYNC) phase, nodes synchronise their clocks.
- During the data phase, the sender waits for a randomly chosen time plus an additional DCF Inter-frame Space (DIFS) period.
- If no activity is detected, the sender transmits a Pioneer Control Frame (PION).
- The next hop node along the route looks up the next hop and forwards the PION to it after waiting for a Shortest Inter-frame space (SIFS) period.
- The process continues until destination is reached.
- Data transmission begins during sleep period.
- Each node returns acknowledgement (ACK) after receiving packet and returns to sleep mode.
- Process continues until data is received at destination.

F. TunableMAC

TunableMAC is a protocol that was provided along with the WSN Framework, Castalia [17].

Algorithm for TunableMAC

As the name implies, this algorithm is tuneable and allows 12 of its parameters to be tuned. This protocol can simulate many duty-cycling protocols, but it does not support unicast. It uses Carrier-sense multiple access (CSMA) for its transmission, therefore its persistence and backing off policies can be tuned. Its duty cycle can also be tuned as well as the train of beacons that can be used to wake up potential receivers.

5.3. Simulation Results

A. Energy Simulation

This section presents experimental results for energy consumption. This is done first for the TunableMAC and secondly, the three protocols (SMAC, TMAC and TunableMAC) are compared in terms of their energy consumption.

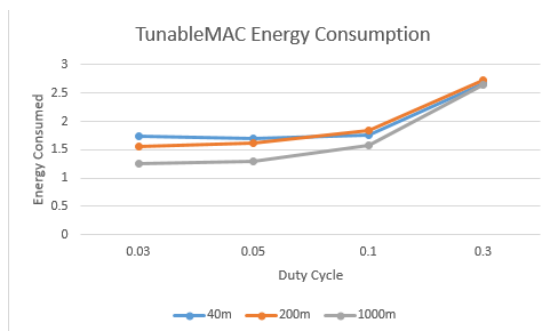


Figure 49: Energy Consumption for TunableMAC at varied duty cycles and bridge sizes

Figure 49 shows that the energy consumption increases in direct proportion to the duty cycle. The energy consumption is highest in the 200-metre bridge when the duty cycle is 0.3.

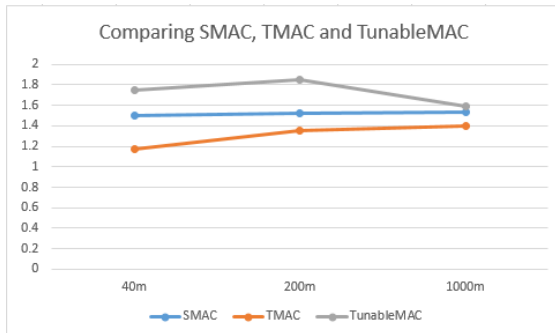


Figure 50: Energy Consumption for TunableMAC, SMAC and TMAC at varied bridge sizes

In Figure 50, SMAC appears more stable than TMAC and TunableMAC in terms of energy consumption. TunableMAC consumes the highest energy, followed by SMAC and then TMAC which consumes the least energy.

B. Reception Simulation

The reception simulation shows the ratio of the number of packets received at the sink to the total number of packets transmitted. Each packet has a maximum size of 128 bytes. The payload hasn't been considered as part of the scope of this project and therefore hasn't been investigated in terms of energy consumption. This could be considered as part of future research.

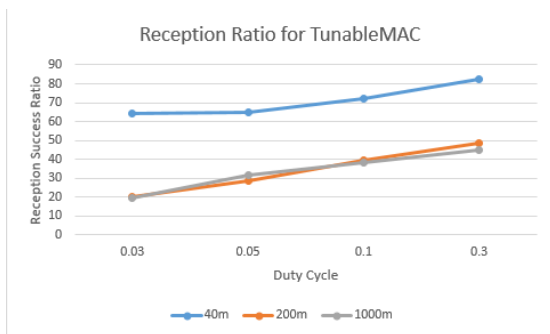


Figure 51: Reception ratio for TunableMAC at varied duty cycles and bridge sizes

Figure 51 shows that there is a higher reception in the 40-metre bridge with the 200m and 1000m competing for a lower reception.

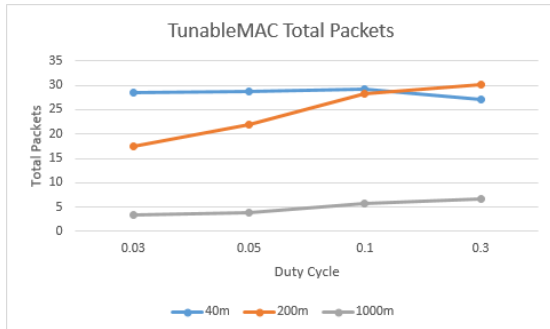


Figure 52: Total packet for TunableMAC at varied bridge sizes

In Figure 52, more packets are sent in the 40m bridge and this is followed closely by the 200m bridge and then the 1000m bridge takes the last position with relatively low number of packets transmitted.

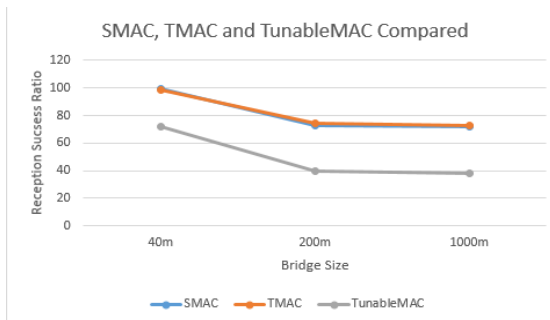


Figure 53: Reception ratio for TunableMAC, SMAC and TMAC at varied bridge sizes

In Figure 53, TMAC and SMAC have similar reception ratios while TunableMAC has a lower reception ratio.

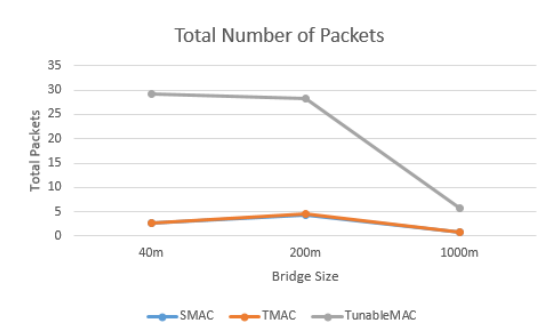


Figure 54: Total packets for TunableMAC, SMAC and TMAC at varied bridge sizes

In Figure 54, TunableMAC has the highest number of packets followed by SMAC and TMAC.

8.5. ANALYSIS

Figure 49 shows the changes in TunableMAC energy consumption as the duty cycles change. Energy is most consumed in the 40m bridge in total but at duty cycle 0.3, the 200m bridge

consumes the highest energy. Energy consumption increases proportionally to the duty cycle. Figure 50 compares SMAC, TMAC and TunableMAC and of all the three TunableMAC consumes the most energy. Figure 51 shows that reception is highest in a 40m bridge because of the distance. In Figure 52, throughput is highest in the 40m bridge although the 200m bridge seems to take over as duty cycle approaches 0.3. In Figure 53, SMAC and TMAC have a better reception ratio than TunableMAC, however in Figure 54, throughput is highest in TunableMAC. TunableMAC appears to spend a lot of energy without much productivity. On the other hand, TMAC and SMAC save more energy but transmit a very small number of packets.

Based on the above results and analysis, the following issues were identified:

- Too much energy consumption with less productivity. This is evident in the TunableMAC protocol which relatively consumes a lot of energy as shown in Figure 40 but has a relatively low reception ratio.
- Low energy consumption with little or no adaptability to a topological change.

In response to these issues, we propose a novel model based on the virtual clusters approach that is secure and proactively energy-efficient.

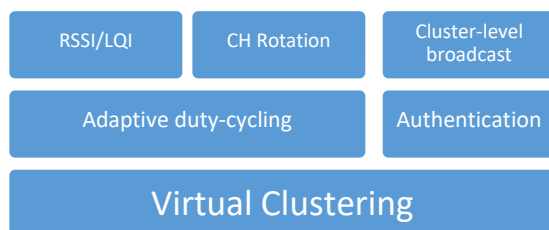


Figure 55: Conceptual model of components of proposed proactive energy-efficient MAC protocol

The proposed model is based on information gathered from the aforementioned literature. To solve the problem of little or no adaptability to topological changes, virtual clustering, cluster head rotation and adaptive duty cycling are proposed as part of the model. The use of virtual rather than real clusters [114] is better in the sense that it is adaptable to any change in topology. Also, there'll also be rotation of cluster heads depending on their availability and resource consumption. Secondly, an adaptive duty cycling would then be incorporated into the virtual clusters. One benefit of adaptive duty cycling in relation to the issues identified is that it can solve the problem of too much energy consumption with low

reception ratio by allowing the nodes sleep for longer when there is less traffic and also stay awake when the traffic is high. Hence, the duty cycle won't be fixed but adaptive based on traffic. To further improve energy-efficiency, a measurement-based security technique such as RSSI[141] can then be introduced to protect against any form of jamming. The presence of virtual clusters also be utilised to only allow cluster-level broadcasts rather than network-wide broadcasts.

5.4. Future work

In the future, the RSSI values would be used as a parameter in detecting denial-of-sleep attacks. This would be achieved via the following steps:

A. Use RSSI to measure distance between nodes

The RSSI parameter can be used to tell the distance between nodes and this can be useful in knowing how far a node is from the sink.

B. Use the distance measurements to assign nodes to real clusters

Knowing the distance between nodes can also enable clustering to be done among nodes. This would allow creation of real clusters and allows for nodes closest to each other to be in the same cluster

C. Establish a threshold value for the RSSI and go into deep sleep when there is an anomaly

Studying the RSSI values can also help detect a malicious node by observing an abnormal pattern in the RSSI values which would be detectable if there is a threshold value.

Furthermore, investigation can be done to ascertain why TunableMAC performs better than SMAC and TMAC in terms of packet reception at the sink. More research can be done in the TunableMAC protocol to find out what other parameters influence its high performance for the majority of the results. The TunableMAC is a good protocol to investigate especially because of its tuneable parameters which allows for a lot of experimenting to see the effect of certain changes. The throughput and latency aspects of the protocols can also be analysed to observe the relationship these parameters. Finally, this can lead to the development of an improved secure and energy-efficient WSN MAC protocol.

One of the areas for future work is to investigate how machine learning techniques can be applied to data collected by the sensor nodes. The algorithms will be run on the machine connected to the base station and then the output from the learning is then passed across to

the nodes as an update. Furthermore, a wireless sensor network based on raspberry Pis could be used in place of the Sun SPOT devices in order to keep up with the most recent trends in the field.

In the future, it could be useful to look into how to adapt TunableMAC by extending the concepts presented in Section VI and Figure 7. An impact analysis will be done on the other higher layers to analyse the overall energy-efficiency and throughput caused by changes to the MAC layer.

Alternative network architectures should be considered as an area for further research as more application areas of wireless sensor networks require topological changes to meet their goals. More complex alternative topologies such as mesh and hybrid topologies could be considered within the same context of energy efficiency and throughput. Mobility of sensors within the network is also another area that should be considered in order to cater for the variety of application domains that exist. It's pertinent to note that Castalia simulator provides support for the mobility of sensors and therefore could still be used for research around mobility of wireless sensor networks. Another area for future consideration is payload analysis as this has significant impact on latency, throughput and energy-efficiency of the WSN. Another area that could be looked into for mitigating denial-of-sleep attacks is machine learning. Algorithms like Bayes theorem could be explored to help calculate the probability of a denial-of-sleep attack based on measurement of certain metrics on the network. However, careful consideration should be given to ensure that more energy is not lost from introducing machine learning, than in mitigating the attacks.

The next phase would be to introduce the use of an Arduino board or a Raspberry pie to implement these sensors physically and go beyond the simulated environment to further demonstrate the proposed prototype. But before this is finalised the MAC protocol will need to have been developed fully on the simulator with the security features. It is important to bear in mind that the current prototype mostly handles energy efficiency and does not fully include security features. The security aspects would focus on the availability aspect of the CIA as this overlaps with energy-efficiency.

One of the future plans for the project is Machine learning and Data analytics. The current research uses a simulation approach whereby some tuning is done using the TunableMAC

protocol to save energy as well as wireless signal parameters such as RSSI and LQI to detect denial-of-sleep attacks. Although this is a great solution, the effectiveness of this protocol may reduce as the network size increases. For wireless sensor networks of thousands of nodes, a need arises for a much more autonomous solution for which machine learning can play a huge role. This properly fits with the original intended GAS (**G**reen **A**utonomous **S**ecurity) model discussed in chapter 3.

There has been research in the three aspects (Energy efficiency, autonomy and access control) and even research on the balance between energy efficiency and security but little or no research has been done on the trade-off between energy efficiency, autonomy and access control.

The expectation from research is that a technique be discovered that intelligently or autonomously achieves effective access control in an energy –efficient manner. While the research may seem broad in terms of cutting across three research areas, the narrowness lies in the novelty of seamlessly synchronising the three.

Chapter 6: Conclusions

“There is no real ending. It's just the place where you stop the story.”

Frank Herbert

This chapter aims to discuss how much of the intended objectives have been achieved, as well as the contributions to knowledge and strengths of the project. Further reflection is done on the challenges encountered during the project alongside the lessons learned from the project.

It's important to note that all seven objectives of the project were achieved although with some areas of improvement for future considerations. One of the objectives was to enhance the energy-efficiency of wireless sensor networks via the MAC layer and this was achieved. Another achieved objective was to minimize the impact of a denial-of-sleep attack and lastly, the objective of developing a MAC layer-based energy-efficient and secure prototype called LayeredMAC. The prototype was tested for its energy-efficiency and throughput under a denial-of-sleep attack in comparison with two other protocols.

By carrying out simulation experiments which involved comparing the effect of duty cycling on the energy consumption using SMAC and TMAC protocols, it was then possible to enhance energy efficiency by tuning certain parameters such as duty cycle, listen interval, transmit power and sample interval, all with the help of the TunableMAC protocol. By using the layered model which included virtual clustering, adaptive duty cycling, RSSI/LQI measurements and cluster head rotations, the objective of minimising the impact of a denial-of-sleep attack was achieved. The last objective was achieved by developing the MAC layer prototype called LayeredMAC which was then tested against SMAC and TMAC.

One of the main contributions to knowledge was the framework developed as part of the novel MAC layer prototype. The framework served as a basis for the development of algorithms to improve on the energy-efficiency of the wireless sensors by incorporating a layered model which applies virtual clustering, RSSI/LQI measurements, adaptive duty cycling and cluster head rotation. Another contribution to knowledge is the development of the novel MAC protocol which was based on the algorithms. The algorithms and the protocol were implemented on OMNET++ simulator, on top of the Castalia framework for WSNs. Aspects of the algorithm tested include the energy efficiency and throughput. The protocol was tested against other existing MAC layer protocols (SMAC and TMAC). The results showed the new MAC protocol showed about twice as much reception at the sink

node than the two existing protocols with the same amount of energy. The algorithm was also tested under denial-of-sleep attacks in comparison with other protocols and showed the same level of energy-efficiency.

One of the strengths of this research is that it shows the effect of duty cycling in MAC protocols and their effect on energy consumption. The interesting part is in the TunableMAC protocol which allows tuning of the duty cycle to see the energy levels.

While it is obvious that energy consumption is reduced with lower duty cycles, it is also important to know the cost involved in saving energy with regards to throughput and latency. This raised the question as to what degree of throughput is being traded to save energy. One way to answer this question was to measure the report reception (throughput) in the simulator. The results reveal that although SMAC and TMAC perform better than TunableMAC in terms of energy consumption, TunableMAC outshines them in terms of packet reception (throughput).

Another strength of the project is the GAS model proposed as a theoretical representation of how to understand and tackle denial-of-sleep attacks. Consisting of three aspects- Green (Energy-efficiency), Autonomy and Security, this model formed the basis for the simulation experiments and developed algorithms that led to the main contribution to knowledge.

Although the objectives were achieved, some areas of improvement were present. One area of improvement is in the testing of the new prototype. Although detailed tests were done on energy-efficiency and throughput as well as testing under denial-of-sleep attack, more tests could have been done to look into the effect of parameters such as the sample interval as this was part of the parameters used in the simulation scenario. Although tests were carried out under simulated denial-of-sleep attacks, it would have been good to see the impact of these attacks on different topologies with mobility of sensors as a factor.

There were many challenges encountered during the project, most of which had to do with the simulation environment. There was a steep learning curve with regards to the OMNET++ platform in terms of its installation and configuration. The same applied to Castalia simulator for wireless sensor networks which had to be installed on OMNET++ simulator.

There was no graphical user interface for Castalia simulator, hence commands had to be used on a Linux platform to operate the simulator which had to be learned from studying the only manual available for the tool. The graphical results produced from the simulator were not aesthetically pleasing, hence the values had to be transferred to Microsoft Excel and replotted all over again. Only a few existing models of MAC protocols such as TMAC and SMAC were available on the simulator. There was also very limited support on the use of the simulator, although the availability of a good number of simulation scenarios as well as its unique design specifically for wireless sensor networks made it worth considering. Another challenge is that Castalia had a limitation of not being platform-specific, hence it was a generic framework for the first order validation of an algorithm. Therefore, whatever code was written could not be directly implemented on a real sensor without substantial modifications. Although the objectives of the project were clear, a multi-disciplinary approach was considered in order to achieve the objectives and this posed the challenge of striking a balance between exploring different disciplines while keeping focus on the objective. The Sun SPOT sensors used for the real-device tests were relatively old and no support is currently being provided for them. However, they were chosen because they are based on Java and it was quicker to implement the algorithms developed on the simulator as Java was my area of expertise. The challenge with these devices was that they only worked with Windows XP and there was no support for new operating systems like Windows 10. One alternative would have been to use an Arduino board as a platform.

One of the initial challenges faced at the start of the project was how to narrow the research to become more specific than just the security of the internet-of-things. The literature study began with looking in the internet-of-things and its architecture. After much consideration, the research was then narrowed down to one of the components of the internet-of-things - Wireless sensor networks. Before narrowing down to wireless sensor networks, some literature review was done on current security techniques in general. The solutions were not suitable for wireless sensor networks as these networks usually contained resource-constrained sensors which require different security measures. In relation to IEEE, this meant moving from IEEE 802.11 to IEEE 802.15.4. The security solutions included models, techniques, frameworks and protocols. Each of these models tackled one of the following aspects of security (Confidentiality, integrity and Availability). Although security was the initial

focus, consideration had to be given to energy-efficiency as this played a huge role especially with the resource-constrained devices. Availability had more priority than confidentiality and integrity. The next step was then to rank the security solutions based on different criteria using a weighted scoring model.

Deciding on the project scope was also challenging especially in the aspects of whether to combine energy efficiency and information security or just pick one of them. To curb this challenge, the solution was to find a common ground between the two, where they overlap and then gradually expand from there.

One of the next strategies used was to decide on which simulator to use. Several simulators were considered before arriving at the final choice. Among the many simulators considered were OMNET++, JSim, OPNET(RiverBed), Matlab etc. Making a choice of simulator depended mainly on two aspects: skill level and relevance to research as discussed in chapter 3. OMNET++ was the chosen simulator mainly because of its support for the Castalia framework which was specifically designed for wireless sensor networks. Installing the simulator was challenging at first mostly because it was command-line based. Installation of the software was also a big challenge as the simulator wasn't fully compatible with the windows platform and did not work properly. After uncountable attempts, the solution was then to install Ubuntu OS on the Oracle VirtualBox which sits on a windows platform.

Scoping the literature review was also a challenge as there was an enormous amount of information surrounding energy efficiency and security of wireless sensor networks. The literature review surrounded areas such as the internet of things and its applications, wireless sensor networks architecture, design, energy efficiency and security.

Another major challenge was in the evaluation of MAC protocols. Most of the information about existing protocol were mainly theoretical and even the ones that were simulated didn't provide any of the files, and even if they did, it wouldn't be compatible with the simulator for this project (OMNET++). Hence, the plan was to develop models of this existing protocols afresh using the OMNET++ simulator but that seemed very painstaking and was therefore brushed aside. Although the OMNET++ simulator came with some pre-loaded existing MAC protocol models such as SMAC and TMAC but these were not exhaustive. However, a Tunable

MAC which was also part of the framework (Castalia) on OMNET++ allowed one to customise different parameters in a way that could represent several existing MAC Protocols.

Comparing various security approaches and protocols was a bit challenging for a number of reasons. One of the reasons was that some of them were full protocols while some were just techniques, some of which had not been tested. Furthermore, some of the protocols didn't have enough information about them in their journals to actually get enough information.

Considering that the bigger goal of this project would be to create a prototype MAC layer protocol which is energy-efficiency and secure, there was therefore a great need to find a gap in existing MAC layer protocols as well as existing security approaches and see how that gap can be filled through this research output.

The need to learn C++ programming language as well as NED language was paramount because the OMNET++ simulator was based on these languages. NED which stands for network definition was required to define the network topology while C++ handled the dynamic aspects of the network such as communication. Learning these languages and applying them to the current scenario was quite painstaking and kind of caused slight delays. Overall the project experience was a great one and the lessons learned are enormous.

References

1. S. S. Prasad and C. Kumar, "A Green and Reliable Internet of Things," *Communication Networks*, vol. 05, no. 01, pp. 44–48, 2013.
2. I. Stojmenovic, "Localized network layer protocols in wireless sensor networks based on optimizing cost over progress ratio," *IEEE Network*, vol. 20, no. February, pp. 21–27, 2006.
3. R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," *IEEE Community Magazine*, vol. 49, no. April, pp. 28–35, 2011.
4. Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, and Xuemin Shen, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," *IEEE Trans. Parallel Distributed System.*, vol. 23, no. 1, pp. 32–43, 2012.
5. B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "Energy Cost of Security in an Energy-Harvested," pp. 198–201, 2014.
6. Gartner, "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015," 2014. [Online]. Available: <http://www.gartner.com/newsroom/id/2905717>. [Accessed: 10-Dec-2015].
7. A. Athreya, B. DeBruhl, and P. Tague, "Designing for Self-Configuration and Self-Adaptation in the Internet of Things," *Proc. 9th IEEE International Conference Collaborative Computer Networking, Appl. Work.*, pp. 585–592, 2013.
8. P. Mahalle, "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things," *J. Cyber ...*, vol. 1, pp. 309–348, 2013.
9. T. Weigold and A. Hiltgen, "Secure Confirmation of Sensitive Transaction Data in Modern Internet Banking Services *," 2011.
10. S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. H. Pinkse, "Quantum-secure authentication of a physical unclonable key," *Optica*, vol. 1, no. 6, pp. 421–424, 2014.
11. S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios," *Sensors Journal, IEEE*, vol. 15, no. 2, pp. 1224–1234, 2015.
12. S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways," *Procedia Comput. Sci.*, vol. 52, no. 0, pp. 452–459, 2015.

13. M. Ulieru and P. Chapman, "Lessons from the past for the future Internet," *2008 First Conf. IT Revolutions*, 2008.
14. O. Garcia-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, and J. L. Torre-Arce, "A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO."
15. E&Y, "Cybersecurity and the Internet of Things," *E&Y*, no. March, 2015.
16. P. Kumar and H.-J. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2011.
17. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.
18. E. Alsaadi and A. Tubaishat, "Internet of Things: Features, Challenges, and Vulnerabilities," *Int. J. Adv. Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 1–13, 2015.
19. R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," *Computer (Long Beach. Calif.)*, vol. 44, no. 9, pp. 51–58, 2011.
20. A. Merlo, M. Migliardi, and L. Caviglione, "A survey on energy-aware security mechanisms," *Pervasive Mob. Comput.*, vol. 24, pp. 77–90, 2015.
21. V. Getov, "Cloud adoption issues: Interoperability and security," *Adv. Parallel Computing.*, vol. 23, pp. 53–65, 2013.
22. H. Ning and Z. Wang, "IoT-A Internet of Things Architecture," *Communications*, vol. 3, pp. 461–463, 2011.
23. D. E. Boubiche and A. Bilami, "A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks," *Journal of Emerging Technology and web Intelligence*, vol. 5, no. 1, pp. 18–27, 2013.
24. M. I. Brownfield, M. I. Brownfield, and N. J. Davis, "Energy-efficient Wireless Sensor Network MAC Protocol Energy-efficient Wireless Sensor Network MAC Protocol," *Management*, 2006.
25. M. Pirretti, S. Zhu, N. Vijaykrishnan, P. Mcdaniel, M. Kandemir, and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," *Int. J. Distrib. Sens. Networks Int. J. Distrib. Sens. Networks Int. J. Distrib. Sens. Networks*, vol. 2, no. 03, pp. 267–287, 2006.
26. S. Raymond, D.R.; Midkiff, "CLUSTERED ADAPTIVE RATE LIMITING : DEFEATING DENIAL-OF-SLEEP ATTACKS IN WIRELESS SENSOR NETWORKS David R . Raymond and Scott F . Midkiff Bradley Department of Electrical and Computer Engineering Virginia Polytechnic Institute and State University Blacksbu," *IEEE*, pp. 1–7, 2007.
27. X. Lu, M. Spear, K. Levitt, N. S. Matloff, and S. F. Wu, "A synchronization attack and defense in energy-efficient listen-sleep slotted MAC protocols," *Proc. - 2nd Int. Conf.*

Emerg. Secur. Inf., Syst. Technol. Secur. 2008, Incl. DEPEND 2008 1st Int. Work. Dependability Secur. Complex Crit. Inf. Sys., pp. 403–411, 2008.

28. C. Chen, L. Hui, Q. Pei, L. Ning, and P. Qingquan, "An effective scheme for defending denial-of-sleep attack in wireless sensor networks," in *5th International Conference on Information Assurance and Security, IAS 2009*, 2009.
29. D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 367–380, 2009.
30. W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *Proc. 6th ACM Int. Symp. Mob. ad hoc Netw. Comput. MobiHoc 05*, p. 46, 2005.
31. F. J. Wu and Y. C. Tseng, "Distributed wake-up scheduling for data collection in tree-based wireless sensor networks," *IEEE Commun. Lett.*, vol. 13, no. 11, pp. 850–852, 2009.
32. R. Falk and H. J. Hof, "Fighting insomnia: A secure wake-up scheme for wireless sensor networks," *Proc. - 2009 3rd Int. Conf. Emerg. Secur. Information, Syst. Technol. Secur. 2009*, pp. 191–196, 2009.
33. J. Zhao and K. E. Nygard, "A Two-Phase Security Algorithm for Hierarchical Sensor Networks," no. c, pp. 114–120, 2011.
34. T. Bhattasali and R. Chaki, "AMC Model for Denial of Sleep Attack Detection," *arXiv Prepr. arXiv1203.1777*, 2012.
35. T. Bhattasali, "Sleep Deprivation Attack Detection in Wireless Sensor Network," *Int. J. Comput. Appl.*, vol. 40, no. 15, pp. 19–25, 2012.
36. S. Kaur and M. Ataulloh, "Securing Wireless Sensor Network from Denial of Sleep Attack by Isolating Nodes," *Int. J. Comput. Appl.*, vol. 103, no. 1, pp. 975–8887, 2014.
37. D. M., Wainis; K., Kabalan; R., "COMMUN-31," 2014.
38. C. T. Hsueh, C. Y. Wen, and Y. C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," *IEEE Sens. J.*, vol. 15, no. 6, pp. 3590–3602, 2015.
39. C. P. Goudar and S. S. Kulkarni, "Mechanisms for Detecting and Preventing Denial of Sleep Attacks and Strengthening Signals in Wireless Sensor Networks," *Int. J. Emerg. Res. Manag. & Technology*, no. 46, pp. 2278–9359, 2015.
40. S. Naik and N. Shekokar, "Conservation of energy in wireless sensor network by preventing denial of sleep attack," in *Procedia Computer Science*, 2015.
41. M. Brownfield, Y. Gupta, and N. Davis IV, "Wireless sensor network denial of sleep attack," *Proc. from 6th Annu. IEEE Syst. Man Cybern. Inf. Assur. Work. SMC 2005*, vol. 2005, no. June, pp. 356–364, 2005.

42. V. Student and A. Professor, "A Survey on the Solutions for the Problems of Denial of sleep Attacks," *Int. J. Innov. Res. Comput. Commun. Eng. (An ISO Certif. Organ.,* vol. 3297, no. 1, 2007.
43. G. Mahalakshmi and P. Subathra, "A survey on prevention approaches for denial of sleep attacks in wireless networks," in *Journal of Emerging Technologies in Web Intelligence*, 2014.
44. J. Rezaei, "Best-worst multi-criteria decision-making method," *Omega*, vol. 53, pp. 49–57, 2015.
45. L. Xu and J. Yang, "Introduction to multi-criteria decision making and the evidential reasoning approach," *Isbn*, no. 0106, pp. 1–21, 2001.
46. F. Zorzi, M. Stojanovic and M. Zorzi, "On the Effects of Node Density and Duty Cycle on Energy Efficiency in Underwater Networks," *IEEE*, no. 10, pp. 10-13, 2010.
47. J. Saraswat and P. P. Bhattacharya, "Effect of Duty Cycle on Energy Consumption in Wireless Sensor Networks," *International Journal of Computer Networks & Communications (IJCNC)* , vol. 5, no. 1, 2013.
48. S. Panichpapiboon, G. Ferrari and T. O. K., "Optimal Transmit Power in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 10, pp. 1432 - 1447, 2006.
49. T. VanDam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in *1st ACM International Conference Embedded Network Sensor System*, Los Angeles, California, 2003.
50. R. Tahar, A. Dhraief, A. Belghith, H. Mathkour and R. Braham, "Autonomous and adaptive beaconing strategy for multi-interfaced wireless mobile nodes," *Wirel. Commun. Mob. Comput.*, vol. 16, no. 12, p. 1625–1641. doi: 10.1002/wcm.2638, 2016.
51. Accenture, "THE INTERNET OF THINGS: THE FUTURE OF CONSUMER ADOPTION," 2014. [Online]. Available: <https://www.accenture.com/gb-en/insight-internet-things-future-consumer-adoption>. [Accessed 6 March 2017].
52. Trustwave, "Trustwave Global Security Report," 2015. [Online]. Available: <http://www2.trustwave.com/rs/815-RFM->

- [693/images/2015_TrustwaveGlobalSecurityReport.pdf](#). [Accessed 13 December 2016].
53. Verizon Enterprise, "Verizon Data Breach Investigations Reports," 2015. [Online]. Available: <http://www.verizonenterprise.com/verizon-insights-lab/dbir/>. [Accessed 13 December 2016].
54. The Economist, "In-store detecting," 2016. [Online]. Available: <http://www.economist.com/news/business/21712163-there-money-be-made-tracking-shoppers-paths-inside-stores-new-industry-has-sprung-up>. [Accessed 6 March 2017].
55. C. Rigby, "Internet of Things set to see widespread adoption by 2019, with 49% of retailers now using it," 2017. [Online]. Available: <http://internetretailing.net/2017/02/internet-things-set-see-widespread-adoption-2019-49-retailers-now-using/>. [Accessed 6 March 2017].
56. Libelium, "50 Sensor Applications for a Smarter World," 2017. [Online]. Available: http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/. [Accessed 8 March 2017].
57. S. Basagni, A. Carosi, E. Melachrinoudis, C. Petrioli and Z. M. Wang, "Controlled Sink Mobility for prolonging wireless sensor network lifetime," Springer Science + Business Media, LLC , no. 14, pp. 831-858, 2008.
58. W. Dargie and C. Poellabauer, FUNDAMENTALS OF WIRELESS SENSOR NETWORKS THEORY AND PRACTICE, West Sussex, United Kingdom: John Wiley & Sons Ltd., 2010.
59. A. Ahmad, M. Rathore, A. Paul and B. Chen, "Data Transmission Scheme Using Mobile Sink in Static Wireless Sensor Network," *Journal of Sensors*, vol. 2015, no. Article ID 279304, 2015.
60. Gartner, "Internet of Things," 2017. [Online]. Available: <http://www.gartner.com/it-glossary/internet-of-things/>. [Accessed 6 March 2017].
61. A. Merlo, M. Migliardi, and L. Caviglione, "A survey on energy-aware security mechanisms," *Pervasive Mobile. Computing.*, vol. 24, pp. 77–90, 2015.

62. B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "Energy Cost of Security in an Energy-Harvested IEEE 802.15.4 Wireless Sensor Network," pp. 198–201, 2014.
63. M. I. Brownfield, M. I. Brownfield, and N. J. Davis, "Energy-efficient Wireless Sensor Network MAC Protocol Energy-efficient Wireless Sensor Network MAC Protocol," *Management*, 2006.
64. M. Pirretti, S. Zhu, N. Vijaykrishnan, P. Mcdaniel, M. Kandemir, and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," *Int. J. Distrib. Sens. Networks Int. J. Distrib. Sens. Networks Int. J. Distrib. Sens. Networks*, vol. 2, no. 03, pp. 267–287, 2006.
65. T. Bhattasali, "Sleep Deprivation Attack Detection in Wireless Sensor Network," *Int. J. Comput. Appl.*, vol. 40, no. 15, pp. 19–25, 2012.
66. F. J. Wu and Y. C. Tseng, "Distributed wake-up scheduling for data collection in tree-based wireless sensor networks," *IEEE Communication Letter*, vol. 13, no. 11, pp. 850–852, 2009.
67. S. Isaiadis and V. Getov, "Integrating Mobile Devices into the Grid: Design Considerations and Evaluation," *Proc. of Euro-Par 2005 Conference, LNCS*, vol. 3648, pp. 1080-1088, Springer, 2005.
68. H. Khalife and F. Krief, "Reasoning Services for Security and Energy Management in Wireless Sensor Networks," *Proc. 7th Int. Conf. Netw. Serv. Manag.*, pp. 520–524, 2011.
69. M. Coles, D. Azzi, and B. Haynes, "A self-healing mobile wireless sensor network using predictive reasoning," *Sens. Rev.*, vol. 28, no. 4, pp. 326–333, 2008.
70. R. Vullers, R. Schaijk, H. Visser, J. Penders, and C. Hoof, "Energy harvesting for autonomous wireless sensor networks," *IEEE Solid-State Circuits Mag.*, vol. 2, no. 2, pp. 29–38, 2010.
71. A. Lambebo and S. Haghani, "A Wireless Sensor Network for Environmental Monitoring of Greenhouse Gases," p. 2010, 2014.
72. A. K. Singh, S. Rajoriya, S. Nikhil, and T. K. Jain, "Design constraint in single-hop and multi-hop wireless sensor network using different network model architecture," *International Conference Computing Communication*, pp. 436–441, 2015.
73. E. Udoh, V. Getov, A. Bolotov, Sensor Intelligence for Tackling Energy-Drain Attacks on Wireless Sensor Networks, Proc. 23rd Workshop on Automated Reasoning: Bridging the Gap between Theory and Practice (ARW 2016), University of Liverpool, 2016.
74. V. Getov, A. Hoisie, P. Bose, New Frontiers in Energy-Efficient Computing, IEEE Computer, vol. 49(10), pp. 14-18, IEEE Press, 2016

75. T. Bhattasali, "Sleep Deprivation Attack Detection in Wireless Sensor Network," *Int. J. Comput. Appl.*, vol. 40, no. 15, pp. 19-25, 2012.
76. M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," *Proc. 6th Annual IEEE SMC Information Assurance Workshop*, pp. 356–364, IEEE Xplore, 2005.
77. D.R. Raymond and S.F. Midkiff, "Clustered Adaptive Rate Limiting: Defeating Denial-of-sleep Attacks In Wireless Sensor Networks," *Proc. of IEEE Military Communications Conference (MILCOM)*, pp. 1-7, IEEE Xplore, 2007.
78. D.E. Boubiche and A. Bilami, "A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks," *J. of Emerging Technologies in Web Intelligence*, vol. 5, no. 1, pp. 18–27, 2013.
79. J. Rezaei, "Best-Worst Multi-Criteria Decision Making Method," *Omega*, vol. 53, pp. 49-57, 2015.
80. L. Xu and J.B. Yang, "Introduction to Multi-Criteria Decision Making and the Evidential Reasoning Approach," Manchester School of Management, 2001, [https://php.portals.mbs.ac.uk/Portals/49/docs/jyang/XuYang MSM WorkingPaperFinal.pdf](https://php.portals.mbs.ac.uk/Portals/49/docs/jyang/XuYang_MSM_WorkingPaperFinal.pdf).
81. M. Pirretti, S. Zhu, N. Vijaykrishnan, P. Mcdaniel, M. Kandemir, and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense *Int. J. Distrib. Sens. Networks* *Int. J. Distrib. Sens. Networks*, vol. 2, no. 03, pp. 267–287, 2006.
82. R. Falk and H. J. Hof, "Fighting insomnia: A secure wake-up scheme for wireless sensor networks," *Proc. 2009 3rd Int. Conf. Emerg. Secur. Information, Syst. Technol. Secur.* 2009, pp. 191–196, 2009.
83. S. Naik and N. Shekokar, "Conservation of energy in wireless sensor network by preventing denial of sleep attack," *Procedia Computer Science*, vol. 45, pp. 370-379, 2015.
84. C.T. Hsueh, C.Y. Wen, and Y.C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," *IEEE Sens. J.*, vol. 15, no. 6, pp. 3590–3602, 2015.
85. C. Chen, L. Hui, Q. Pei, L. Ning, and P. Qingquan, "An effective scheme for defending denial-of-sleep attack in wireless sensor networks," *Proc. 5th Int.# Conference on Information Assurance and Security, IAS'09*, pp. 446-449, IEEE Xplore, 2009.
86. M.I. Brownfield, "Energy-efficient Wireless Sensor Network MAC Protocol," PhD Thesis, Virginia Tech, 2006, <http://hdl.handle.net/10919/26749>.
87. T. Bhattasali and R. Chaki, "AMC Model for Denial of Sleep Attack Detection," *Journal of Recent Research Trends*, pp. 1-4, 2012, <http://arxiv.org/abs/1203.1777>.

88. B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "Energy Cost of Security in an Energy-Harvested IEEE 802.15.4 Wireless Sensor Network," Proc. 3rd Mediterranean Conference on Embedded Computing (MECO) pp. 198–201, 2014.
89. S. Isaiadis and V. Getov, "Integrating Mobile Devices into the Grid: Design Considerations and Evaluation," Proc. of Euro-Par 2005 Conference, LNCS, vol. 3648, pp. 1080-1088, Springer, 2005.
90. B. A. Networks, "User's Manual," March, 2011.
91. A. Pratama, R. Munadi, and R. Mayasari, "Design and Implementation of Flood Detector Using Wireless Sensor Network with Mamdani's Fuzzy Logic Method", Proc. 2nd Int. Conference on Information Technology Information Systems and Electrical Engineering (ICITISEE), pp. 192-197, 2017.
92. A. Roy and N. Sarma, "Performance Evaluation of Synchronous Energy Efficient MAC Protocols for Wireless Sensor Networks," Proc. Of 2nd Int. Conference on Communication, Computing and Security [ICCCS-2012], pp. 806-813, Procedia Technology, 2012.
93. G.P. Halkes, T. van Dam, and K.G. Langendoen, "Comparing Energy-Saving MAC Protocols for Wireless Sensor Networks," Mobile Networks and Applications, vol. 10, no. 5, pp.783-791, Springer, 2005.
94. E. Udoh, V. Getov, A. Bolotov, "Sensor Intelligence for Tackling Energy-Drain Attacks on Wireless Sensor Networks," Proc. Of 23rd Workshop on Automated Reasoning: Bridging the Gap between Theory and Practice, University of Liverpool, 2016, <http://westminsterresearch.wmin.ac.uk/17129/1/ARW-16-Udoh-Getov-Bolotov.pdf>.
95. Y. Wang, I.G. Guardiola, X. Wu, "RSSI and LQI Data Clustering Techniques to Determine the Number of Nodes in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, 2014, <https://doi.org/10.1155/2014/380526>.
96. R. Grossmann, J. Blumenthal, F. Golatowski, D. Timmermann, "Localization in Zigbee-based Sensor Networks," Proc. 1st European ZigBee Developers Conference (EuZDC '07), München, Germany, 2007.
97. T. Bhattasali, "Sleep Deprivation Attack Detection in Wireless Sensor Network," Int. J. Comput. Appl., vol. 40, no. 15, pp. 19–25, 2012.
98. D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," IEEE Pervasive Comput., vol. 7, no. 1, pp. 74–81, 2008.
99. D. R. Raymond and S. F. Midkiff, "Clustered Adaptive Rate Limiting : Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks," IEEE, pp. 1–7, 2007.
100. D. E. Boubiche and A. Bilami, "A Defense Strategy against Energy Exhausting Attacks in Wireless Sensor Networks," J. Emerg. Technol. web Intell., vol. 5, no. 1, pp. 18–27, 2013.

101. M. Brownfield, Y. Gupta, and N. Davis IV, "Wireless sensor network denial of sleep attack," Proc. of 6th Annual IEEE Syst. Man Cybern. Inf. Assur. Work. SMC 2005, vol. 2005, pp. 356–364, June, 2005.
102. M. Doudou, D. Djenouri, N. Badache, and A. Bouabdallah, "Journal of Network and Computer Applications Synchronous contention-based MAC protocols for delay-sensitive wireless sensor networks : A review and taxonomy," J. Netw. Comput. Appl., vol. 38, pp. 172–184, 2014.
103. J. Rezaei, "Best-worst multi-criteria decision-making method," Omega, vol. 53, pp. 49–57, 2015.
104. L. Xu and J. Yang, "Introduction to multi-criteria decision making and the evidential reasoning approach," Isbn, no. 106, pp. 1–21, 2001.
105. M. I. Brownfield, M. I. Brownfield, and N. J. Davis, "Energy-efficient Wireless Sensor Network MAC Protocol Energy-efficient Wireless Sensor Network MAC Protocol," Management, 2006.
106. M. Pirretti, S. Zhu, N. Vijaykrishnan, P. Mcdaniel, M. Kandemir, and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," Int. J. Distrib. Sens. Networks Int. J. Distrib. Sens. Networks Int. J. Distrib. Sens. Networks, vol. 2, no. 3, pp. 267–287, 2006.
107. C. Chen, L. Hui, Q. Pei, L. Ning, and P. Qingquan, "An effective scheme for defending denial-of-sleep attack in wireless sensor networks," in 5th International Conference on Information Assurance and Security, IAS 2009, 2009.
108. T. Bhattasali and R. Chaki, "AMC Model for Denial of Sleep Attack Detection," arXiv Prepr. arXiv1203.1777, 2012.
109. R. Falk and H. J. Hof, "Fighting insomnia: A secure wake-up scheme for wireless sensor networks," Proc. 2009 3rd Int. Conf. Emerg. Secur. Information, Syst. Technol. Secur. 2009, pp. 191–196, 2009.
110. S. Naik and N. Shekokar, "Conservation of energy in wireless sensor network by preventing denial of sleep attack," in Procedia Computer Science, 2015.
111. C. T. Hsueh, C. Y. Wen, and Y. C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," IEEE Sens. J., vol. 15, no. 6, pp. 3590–3602, 2015.
112. W. Dargie and C. Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice. 2010.
113. B. A. Networks, "User's Manual," March, 2011.
114. S. Isaiadis and V. Getov, "Integrating Mobile Devices into the Grid : Design Considerations and Evaluation," Proc. of Euro-Par 2005 Conference, LNCS, vol. 3648, pp. 1080-1088, Springer, 2005.

115. A Merlo, M Migliardi, and L Caviglione, "A survey on energy-aware security mechanisms", *Pervasive and Mobile Computing*, vol. 24, pp. 77-90, 2015.
116. A. Yuksel, E. Uzun, and B. Tavli, "The impact of elimination of the most critical node on Wireless Sensor Network lifetime," *SAS 2015 - 2015 IEEE Sensors Applications Symposium, Proceedings*, pp. 1-5, 2015.
117. J. Wang, S. Jiang, and A. O. Fapojuwo, "A protocol layer trust-based intrusion detection scheme for wireless sensor networks," *Sensors (Switzerland)*, vol. 17, no. 6, 2017.
118. G. Vaseer, G. Ghai, and P. S. Patheja, "A novel intrusion detection algorithm: An AODV routing protocol case study," *Proceedings - 2017 IEEE International Symposium on Nanoelectronic and Information Systems, INIS 2017*, Vols. 2018-Febru, pp. 111-116, 2018.
119. J. Uher, R. G. Mennecke, and B. S. Farroha, "Denial of Sleep attacks in Bluetooth Low Energy wireless sensor networks," *Proceedings - IEEE Military Communications Conference MILCOM*, pp. 1231-1236, 2016.
120. P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," *Proceedings of IEEE International Conference on Signal Processing and Communication, ICSPC 2017*, Vols. 2018-Janua, no. July, pp. 288-293, 2018.
121. V. Shakhov and I. Koo, "Depletion-of-battery attack: Specificity, modelling and analysis," *Sensors (Switzerland)*, vol. 18, no. 6, 2018.
122. R. Schrader, T. Ax, C. Röhrig, and C. Fühner, "Advertising power consumption of bluetooth low energy systems," *Proc. 2016 IEEE 3rd Int. Symposium on Wireless Systems within the IEEE International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS-SWS 2016*, September, pp. 62-68, 2017.
123. L. Qiu, W. Jiang, W. Zhang, and P. Li, "Wireless Injection Attacks Based on Fake Data Injection in TinyOS," *Proceedings - International Symposium on Parallel Architectures, Algorithms and Programming, PAAP*, Vols. 2016-Janua, pp. 236-242, 2016.
124. P. M. Pawar, R. H. Nielsen, N. R. Prasad, and R. Prasad, "GSHMAC: Green and Secure Hybrid Medium Access Control for Wireless Sensor Network," *Wireless Personal Communications*, vol. 100, no. 2, pp. 267-281, 2018.
125. O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of Service Defence for Resource Availability in Wireless Sensor Networks," *IEEE Access*, vol. 6, pp. 6975-7004, 2018.
126. M. Montoya, S. Bacles-min, and J. J. A. Fournier, "SWARD: A Secure WAKE-up RaDio against Denial-of-Service on IoT devices," *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks - WiSec '18*, pp. 190-195, 2018.

127. C. Meinel, Konrad-Felix Krentz, and H. Graupner, "Denial-of-Sleep-Resilient Session Key Establishment for IEEE 802.15.4 Security: From Adaptive to Responsive," *Proc. 2018 Int. Conference on Embedded Wireless Systems and Networks*, pp. 25-36, 2018.
128. K.-F. Krentz, H. Graupner, and C. Meinel, "Countering Three Denial-of-Sleep Attacks on ContikiMAC," *Proc. 2017 International Conference on Embedded Wireless Systems and Networks*, pp. 108-119, 2017.
129. K. F. Krentz and C. Meinel, "Denial-of-sleep defenses for IEEE 802.15.4 coordinated sampled listening (CSL)," *Computer Networks*, vol. 148, pp. 60-71, 2019.
130. M. Gunasekaran and S. Periakaruppan, "GA-DoSLD: Genetic Algorithm Based Denial-of-Sleep Attack Detection in WSN," vol. 2017, no. i, 2017.
131. E. Gelenbe and Y. M. Kadioglu, "Battery Attacks on Sensors," *International Symposium on Computer and Information Sciences, Security Workshop*, pp. 1-10, Springer, 2018.
132. C. Gehrman, M. Tiloca, and R. Hoglund, "SMACK: Short message authentication check against battery exhaustion in the Internet of Things," *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2015*, pp. 274-282, 2015.
133. S. Rani and S. K. Naidu, "Mitigation of Energy Depletion in Wireless Ad-hoc Sensor Networks through Path Optimization," *Int. Journal of Computer Networks and Applications*, vol. 2, no. 1, pp. 1-11, 2015.
134. H. W. Ferng and N. M. Khoa, "On security of wireless sensor networks: a data authentication protocol using digital signature," *Wireless Networks*, vol. 23, no. 4, pp. 1113-1131, 2017.
135. A. T. Caposelle, V. Cervo, C. Petrioli, and D. Spenza, "Counteracting Denial-of-Sleep Attacks in Wake-up-radio-based Sensing Systems," *Proc. 13th Annual IEEE Int. Conference on Sensing, Communication, and Networking (SECON)*, 2016.
136. S. Isaiadis and V. Getov, "Integrating Mobile Devices into the Grid: Design Considerations and Evaluation," *Proc. of Euro - Par 2005 Conference, LNCS*, vol. 3648, pp. 1080-1088, Springer, 2005.
137. B. A. Networks, "User's Manual," March 2011.
138. Horveliu C. M. (2013) "Sun SPOTs: A Great Solution for Small Device Development". Available at: <https://www.oracle.com/technetwork/server-storage/ts-4868-1-159029.pdf> Accessed on: 20/11/2018.
139. Agile Business Consortium (2014). "The DSDM Agile Project Framework." Available at: <https://www.agilebusiness.org/content/moscow-prioritisation>. Accessed on: 20/11/2018.

140. E. Udoh and V. Getov, "Proactive Energy-Efficiency: Evaluation of Duty-Cycled MAC Protocols in Wireless Sensor Networks," *Proc. 2018 Int. IEEE CITS Conference*, pp. 1-5, IEEE, 2018.
141. E. Udoh and V. Getov, "Performance Analysis of Denial-of-Sleep Attack-Prone MAC Protocols in Wireless Sensor Networks," *Proc. UKSim:AMSS 20th International Conference on Modelling & Simulation*, pp. 1-6, IEEE, 2018. Oracle Labs, "Sun SPOT Programmers Manual," 2011. Available at: <https://bit.ly/2DlFFiy> Accessed on: 01/01/2019.
142. M. I. Brownfield, M. I. Brownfield, and N. J. Davis, "Energy-efficient Wireless Sensor Network MAC Protocol Energy-efficient Wireless Sensor Network MAC Protocol," *Management*, 2006.
143. M. Pirretti, S. Zhu, N. Vijaykrishnan, P. Mcdaniel, M. Kandemir, and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense," *Int. J. Distrib. Sens. Networks Int. J. Distrib. Sens. Networks Int. J. Distrib. Sens. Networks*, vol. 2, no. 3, pp. 267–287, 2006.
144. C. Chen, L. Hui, Q. Pei, L. Ning, and P. Qingquan, "An effective scheme for defending denial-of-sleep attack in wireless sensor networks," in *5th Int. Conference on Information Assurance and Security, IAS 2009*, 2009.
145. T. Bhattasali and R. Chaki, "AMC Model for Denial of Sleep Attack Detection," *arXiv Prepr. arXiv1203.1777*, 2012.
146. R. Falk and H. J. Hof, "Fighting insomnia: A secure wake-up scheme for wireless sensor networks," *Proc. 2009 3rd Int. Conf. Emerg. Secur. Information, Syst. Technol. Secur. 2009*, pp. 191–196, 2009.
147. S. Naik and N. Shekokar, "Conservation of energy in wireless sensor network by preventing denial of sleep attack," in *Procedia Computer Science*, 2015.
148. C. T. Hsueh, C. Y. Wen, and Y. C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," *IEEE Sens. J.*, vol. 15, no. 6, pp. 3590–3602, 2015.

Appendix A

Energy-efficient and autonomous access control on the Internet of Things

By

Ekereuke Effiong Udoh

Draft Research proposal to register

Course: MPhil/PhD Electronics and Computer Science

Director of Studies: Prof. Vladimir Getov

December, 2015

Table of Contents

Abstract	Error! Bookmark not defined.
List of Figures	Error! Bookmark not defined.
Author’s Declaration	Error! Bookmark not defined.
Definitions	Error! Bookmark not defined.
Published Work	Error! Bookmark not defined.
Acknowledgements	Error! Bookmark not defined.
Chapter 1: Introduction	Error! Bookmark not defined.
1.1. Background	Error! Bookmark not defined.
1.2. Sensors	Error! Bookmark not defined.
1.3. Wireless Sensor Networks	Error! Bookmark not defined.
1.4. Problem Statement.....	Error! Bookmark not defined.
1.5. Research Aim	Error! Bookmark not defined.
1.6. Research Objectives.....	Error! Bookmark not defined.
1.7. Contributions to Knowledge	Error! Bookmark not defined.
1.8. Research Methodology	Error! Bookmark not defined.
Chapter 2: Literature Review	Error! Bookmark not defined.
2.1. Relevance of the MAC layer.....	Error! Bookmark not defined.
2.2. Sources of energy loss.....	Error! Bookmark not defined.
2.3. Classification of MAC protocols	Error! Bookmark not defined.
2.3.1. Contention-free protocols	Error! Bookmark not defined.
2.3.2. Contention-based protocols	Error! Bookmark not defined.
2.3.3. Hybrid Protocols.....	Error! Bookmark not defined.
2.4. Mobile Wireless Sensor Network Applications.....	Error! Bookmark not defined.
2.4.1. How mobility can enhance energy-efficiency.....	Error! Bookmark not defined.
2.5. Other Energy-related solutions.....	Error! Bookmark not defined.
2.6. Security	Error! Bookmark not defined.
2.6.1. Autonomous Access control	Error! Bookmark not defined.
2.6.2. Device based authentication	Error! Bookmark not defined.
2.6.3. Quantum-cryptography based authentication	Error! Bookmark not defined.
2.6.4. Authorization	Error! Bookmark not defined.
2.6.5. Smart Object Lifecycle-based access control.....	Error! Bookmark not defined.
2.6.6. Threats, Vulnerabilities and Solutions to the IoT from a CIA perspective ..	Error! Bookmark not defined.

2.6.7. IoT architectures and their security implications	Error! Bookmark not defined.
2.7. Denial-of-Sleep Attacks	Error! Bookmark not defined.
2.7.1. State-of-the-art	Error! Bookmark not defined.
2.7.2. Research approach.....	Error! Bookmark not defined.
2.7.3. Qualitative Analysis.....	Error! Bookmark not defined.
2.7.4. Ranking using weighted scoring model	Error! Bookmark not defined.
2.7.5. Simulation using OMNET++ and Castalia	Error! Bookmark not defined.
Chapter 3: A Proposed approach for Tackling Energy-Drain Attacks.....	Error! Bookmark not defined.
3.1. Introduction	Error! Bookmark not defined.
3.2. Comparisons and Simulation for Security Based solutions.....	Error! Bookmark not defined.
3.2.1. Ranking using Weighted Scoring Model	Error! Bookmark not defined.
3.2.2. Wireless Sensor Network Simulation for TunableMAC protocol.....	Error! Bookmark not defined.
3.2.3. Analysis and Discussion.....	Error! Bookmark not defined.
3.3. Comparisons and Simulations for Energy-based approaches	Error! Bookmark not defined.
3.3.1. Methodology for comparison and simulation	Error! Bookmark not defined.
3.3.2. Energy-based approaches.....	Error! Bookmark not defined.
3.3.3. Simulation Results and Analysis.....	Error! Bookmark not defined.
3.4. Proposed Approach.....	Error! Bookmark not defined.
3.4.1. High Level Constituents of the Approach	Error! Bookmark not defined.
Chapter 4: Layered-MAC: Development of Energy-aware and Secure MAC Protocol	Error! Bookmark not defined.
4.1. Introduction	Error! Bookmark not defined.
4.2. Related Work	Error! Bookmark not defined.
4.3. Development Methodology.....	Error! Bookmark not defined.
4.4. Protocol Implementation.....	Error! Bookmark not defined.
4.5. Experiments	Error! Bookmark not defined.
4.6. Simulation results for the protocols under attack.....	Error! Bookmark not defined.
Chapter 5: Performance Testing of Denial-of-Sleep Attack-Prone MAC Protocols....	Error! Bookmark not defined.
7.1. Introduction	Error! Bookmark not defined.
7.2. Related Work	Error! Bookmark not defined.
7.3. Methodology.....	Error! Bookmark not defined.
7.4. Review Of Existing Approaches To Denial-Of-Sleep Attacks.....	Error! Bookmark not defined.
7.5. Results and Analysis.....	Error! Bookmark not defined.
7.5. PROPOSED AUTONOMOUS APPROACH.....	Error! Bookmark not defined.
7.6. CONCLUSION.....	Error! Bookmark not defined.

Chapter 6: Results Error! Bookmark not defined.
 8.1. Introduction **Error! Bookmark not defined.**
Chapter 7: Conclusions **139**
References..... Error! Bookmark not defined.
Appendix A..... Error! Bookmark not defined.

List of Figures

Figure 1: Research Contribution- A Green approach towards Autonomous Security	5
Figure 2: Security Mechanisms for M2M communication [8]	6
Figure 3: ZTIC Architecture[9]	7
Figure 4: Risk Landscape for IoT [1]	9
Figure 5: Conceptual Methodology of proposed research	10
Figure 6: Time Plan	13

List of Acronyms

IoT – Internet of Things

GAS- Green Autonomous Security

ICT – Information and Communication Technology

M2M – Machine-to-Machine

CIA – Confidentiality Integrity Availability

USB – Universal Serial Bus

DTLS – Datagram Transport layer security

Title of Proposed Investigation

Energy-efficient and autonomous access control on the Internet of Things

Research Objectives

To review access control attacks and vulnerabilities on different IoT application domains

To investigate autonomous computing and its implication to the IoT context

To develop a methodology that combines energy efficiency, autonomy and access control in a coherent way.

To develop an autonomous approach to achieve access control on the IoT

To experiment iteratively on the above approach in order to improve its energy efficiency

To critically discuss the development process and analyse the results

To build a prototype based on the results of the experiment

To test the prototype based on a 3 major test cases

To critically evaluate each step of the entire process and reach concrete conclusions

Research Questions

How can autonomy be used to enhance access control on the IoT?

How can an energy-efficiency be applied to an autonomic access control approach on the IoT?

Contribution to Knowledge

The core parts of this research are Energy-efficiency and Autonomous security. With the increasing need for security, there is plenty of focus on security improvement but this research draws attention to the resource-constrained nature of the devices on the IoT and therefore will bring security improvement that is energy-efficient. Furthermore, applying autonomy through artificial intelligence techniques to enhance security is another area currently being researched and is being driven by the fact that an exponential increase in the number of devices on the IoT is at hand and the complexity that comes with it can best be managed through autonomy.

This research contributes uniquely by combining energy-efficiency with autonomy in way that achieves a green security.

Another aspect that may likely have some potential contribution is access control, more specifically authentication. While much of the authentication techniques focus on human-to-machine interaction, the IoT consists of machine-to-machine or thing-to-thing communication which also requires authentication. This research is intended to lay more emphasis on the thing-to-thing communication and how access control can be enhanced.

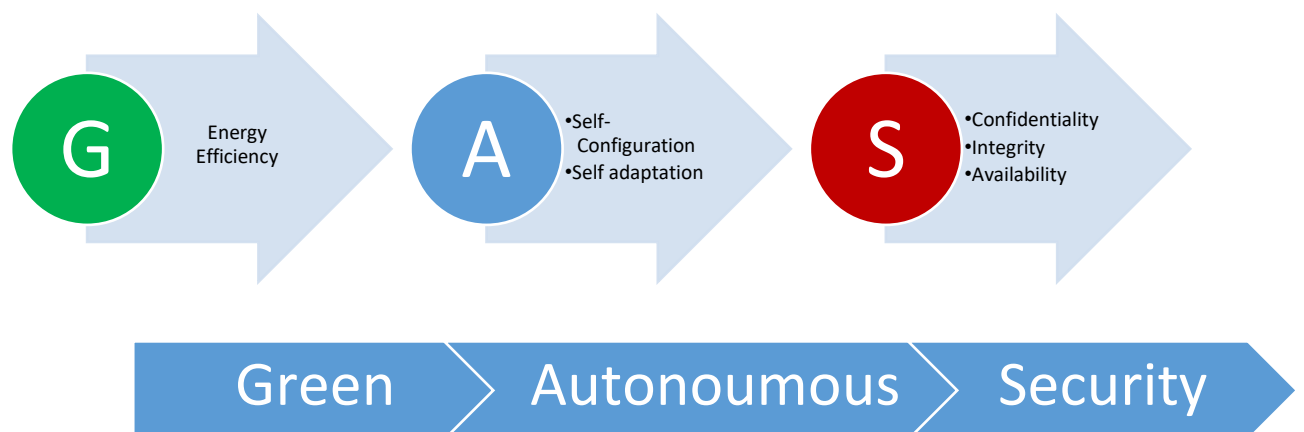


Figure 52: Research Contribution- A Green approach towards Autonomous Security

Literature Review (State-of-the-art)

Energy-related IoT issues and solutions

ICT accounts for about 2.5 percent of all harmful emissions with regards to global carbon emissions. Two aspects are highlighted that contribute to energy saving: Reliability and Efficiency [1]. From a CIA perspective, while efficiency has to do availability, reliability has to do with integrity.

IoT Communication is identified as one of the areas that dominates energy consumption and efficiency can be enhanced by reducing transmission power to the barest minimum, applying the right algorithms to design communication protocols and activity scheduling [2].

Prasad and Kumar[1] also suggest that redundancy technologies could be very helpful in handling reliability issues which could be present not only during transmission, as in the case of efficiency, but also during sensing and processing by IoT sensor nodes.

Asides reliability and efficiency, security is another variable that has to be considered when making a trade-off as an energy-efficient and reliable IoT would not be termed as successful if there is no security[3].

Energy-related security solutions

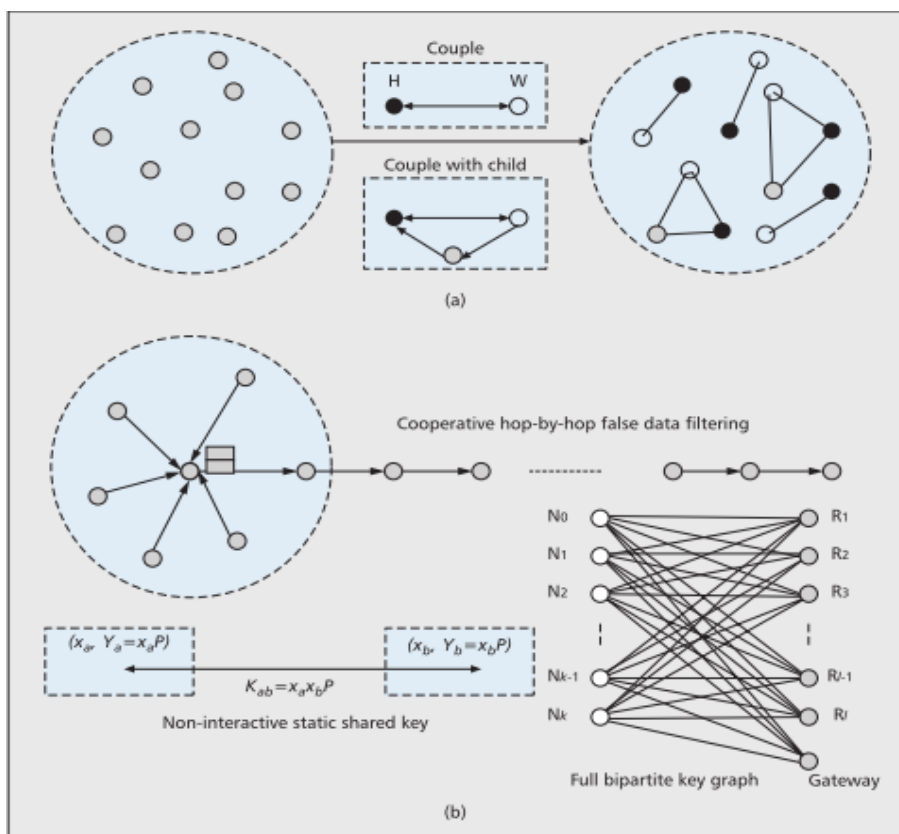


Figure 53: Security Mechanisms for M2M communication [8]

The above figure shows two mechanisms: Early detecting node compromise with couple and bandwidth cooperative authentication to filter false data.

The first mechanism works by coupling nodes together either in Husband(H) and Wife (W) mode or husband (H)-Wife(W)-Child(C) mode and having them exchange beacon messages

that could help them detect a compromise on one of the nodes[3]. While this enhances security, more energy is being utilized. The case could also be vice versa, where energy-efficiency is enhanced and security becomes compromised like in the case where a node is compromised by an attacker without being detected because the node has been put in sleep mode to save energy.

The second mechanism is a bandwidth co-operative authentication that involves a collective authentication by a number of nodes is proven to be very effective[4], however, on the condition that the transmission radius is well chosen as the en route filtering probability reduces as transmission radius increases[3].

Tourancheau et al[5] conclude based on their experiments that the energy cost is relatively low for sensor devices in a wireless sensor network although this is restricted to IEEE 802.15.4 security features and does not take other aspects of security into consideration.

The question then lies in how a balance can be ensured between efficiency, reliability and security.

Access control

Autonomous Access control

One of the challenges identified for self-configurable IoT systems is energy awareness. Considering the envisioned scale of IoT growth of about 20 billion devices in 2020[6], it is worthwhile to consider energy as a constraint when building self-configurable systems as this could help improve the life-span of sensor devices as well as provide more support for critical applications[7]. Other challenges identified include development of suitable metrics, coordinated contextual intelligence, resilience to failures, outages and attacks, application integration and incentives for self-management.

In [8], an identity authentication and capability-based access control model (IACAC) is proposed and is said to protect against man-in-the-middle, replay and denial of service attacks. Certain criteria are considered to be very important in the context of the IoT when developing authentication and access control models. These include mutual authentication, lightweight solution, attack resistance (Denial of service, Man in the middles, Replay attacks), Distributed nature and access control. The IACAC model achieves all of the

aforementioned criteria except the lightweight criteria which is synonymous with energy efficiency.

Device based authentication

The IBM Zone Trusted Information Channel (ZTIC)[9] is a specialised hardware device intended to protect against certain man-in-the-middle attacks through malicious software that cannot be prevented by two-factor authentication approach.

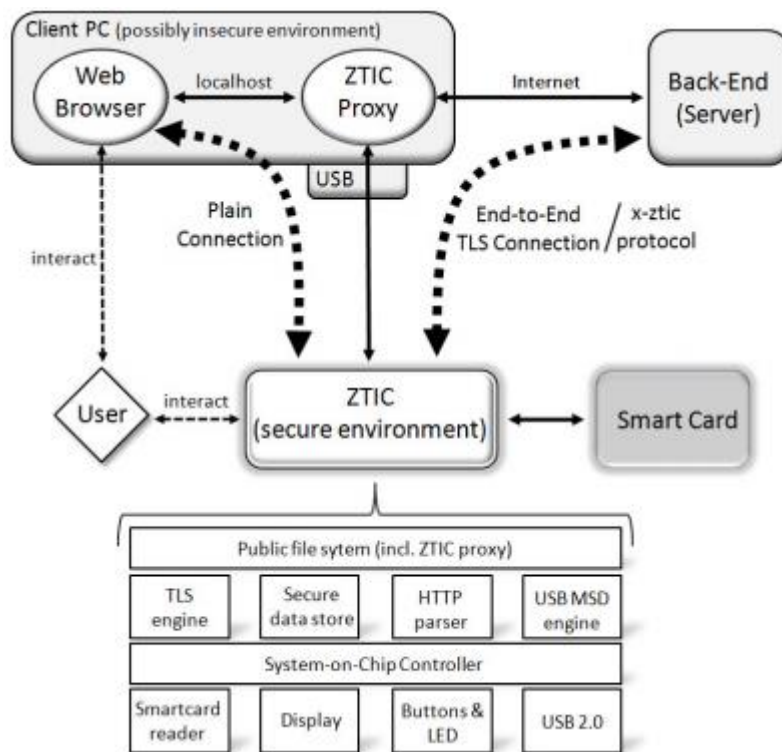


Figure 54: ZTIC Architecture[9]

The above figure shows how the ZTIC technology works by creating a secure connection to the bank server through a proxy on the USB device. This means that all communication between the ZTIC proxy and the server is outside of the client PC and is protected via end-to-end TLS connection.

Quantum-cryptography based authentication

Based on quantum cryptography, a quantum-secure authentication is proposed in [10] as having the following characteristics:

A key that cannot be physically emulated

Secure against digital emulation attacks

Is not dependent on secret data

Is not dependent on unproven mathematical assumptions

Its implementation is straightforward

The benefit of quantum cryptography is that, unlike digital keys where their theft can go undetected, a physical object (physical unclonable function) which is based on quantum-physical principles makes it impossible for an attacker to typify the incident light pulse which in turn prevents the attacker from being able to mimic the expected optical response.

Authorization

In [11], an OAuth-based authorization service (OAS) architecture, which is targeted at machine-to-machine applications (IoT), is proposed. The open-authorization is beneficial in that it is third-party in nature; hence reducing the load on the resource-constrained devices on the IoT, allowing for scalability and remote customization of access policies.

However, one of the setbacks of the OAS architecture is that its energy consumption is on the high side particularly due to the radio transmission.

On the other hand, in [12], a secure and efficient authentication and authorization architecture is proposed which reduces communication overhead by 26% and communication latency by 16% by using a smart gateway to ensure a distributed form of authentication and authorization based on the certificate-based DTLS handshake protocol.

Smart Object Lifecycle-based access control

It is important to consider security in the context of the smart “thing” and ensure that security is addressed at each phase of the lifecycle from when power is first introduced to when the device is in operation, thereby making security fundamental to the device’s proper functioning rather than just being an add-on[13].

In [14], certain attacks are classified based on what phase of the lifecycle they happen. At the initial stage, a compromise of root of trust can occur as well as modification of credentials and keys at the manufacturing phase. At the deployment phase, server impersonation and denial-of-service attacks could occur while physical capture of devices could occur at the operational phase.

Threats, Vulnerabilities and Solutions to the IoT from a CIA perspective

According to E&Y [15], 7 in 10 devices on the IoT are vulnerable. They emphasize on the idea that the cyber threat to the IoT should not be seen just as a technological issue but as a business-wide issue. Hence, the figure below illustrates the 8 facets which constitute the



entire risk landscape with regards to cyber threat on the IoT.

Figure 55: Risk Landscape for IoT [1]

Information security can practically not be discussed without putting the CIA (confidentiality, security and availability into perspective). The literature is discussed with a risk assessment approach in mind which is quantitatively calculated by multiplying the threats, vulnerabilities and assets.

Thus, in carrying out a proper risk assessment, one needs to understand not only the threats and vulnerabilities involved but also the assets being compromised, with information being the asset in this context.

Kumar and Lee [16] discuss possible threats to the IoT with specific considerations to the healthcare application domain. Although the threats are discussed in a healthcare domain context, these threats can still be applied to other domains as pointed out by other researchers [17]. A number of threats have been identified as follows:

Monitoring and Eavesdropping

Kumar and Lee [16] describe this as the most common threat to patient privacy. From a CIA context, this breaches the confidentiality of information. Alsaadi and Tubaishat [18] make a

distinction between data ownership and data control/access illustrating that the owner of the data may not necessarily be the only one with access to the information using Google as an example who may use another individual's data for their predictive analysis in the case of Google Trends; which poses a huge challenge.

Denial-of-Service attacks

Roman *et al.* [19]; Alsaadi and Tubaishat [18] discuss on denial-of-service attacks with more emphasis on distributed-DOS attacks perpetrated through the use of botnets. With regards to the CIA, this mainly affects the availability of information.

IoT architectures and their security implications

There are different IoT architectures and the architecture adopted determines the kind of security vulnerabilities that could be exploited which in turn determines what kind of solutions that should be in place.

It is also important to look at access control in the context of the cloud as the centralized IoT architectures include the cloud. Security as a Service (SecaaS) is a relatively new approach which stems from the need to outsource security services as well as the need for Managed Security Service providers to have a centralized security service from the cloud[20]

Methodology

The end goal of this research is to arrive at an energy-efficient approach to ensuring autonomous access control on the IoT. The methodology would generally revolve around identifying an IoT application domain, a systematic review existing domain specific techniques/approaches, a hypothetical design of an approach, an implementation of the approach in the chosen domain, a testing of the hypothetical design in certain energy contexts against the existing approaches and a critical review of the results and the process.

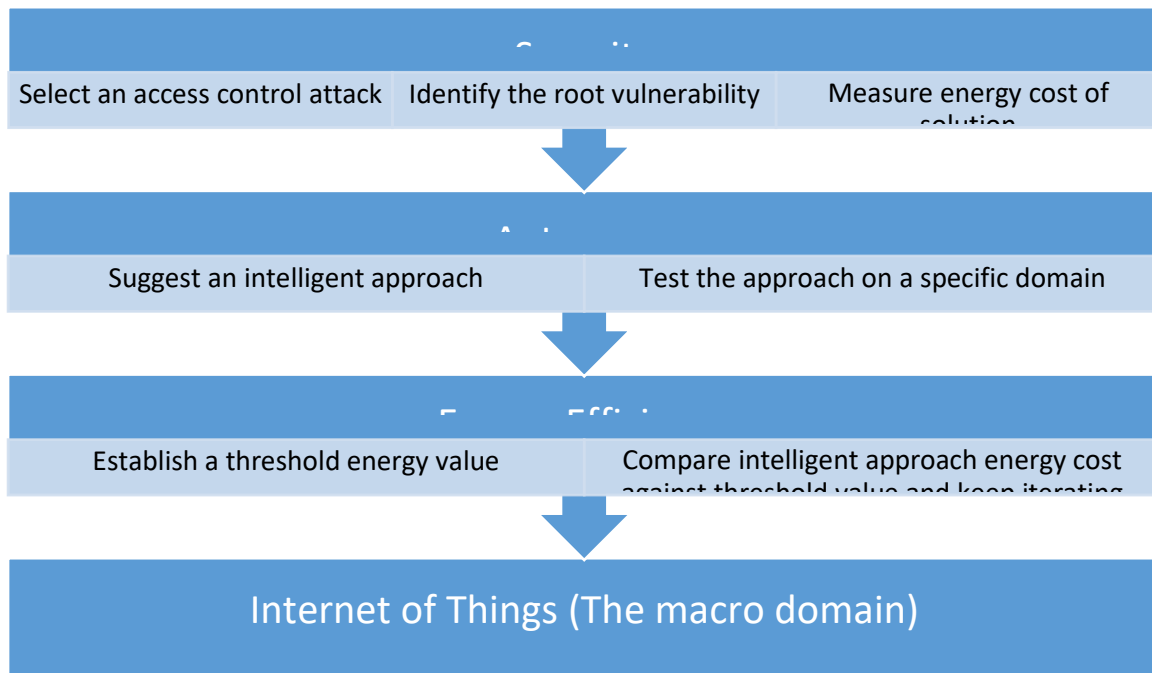


Figure 56: Conceptual Methodology of proposed research

Security

The first step involves the security aspects with focus on access control. Among the many access control attacks, one will be chosen as a point of focus for this research. Before making a choice, many access control attacks will be reviewed based on certain criteria. Since every attack exploits a vulnerability, the next task would be to identify the possible vulnerabilities that could give room to that attack and then analyse the possible solutions in terms of their energy efficiency.

The deliverable from this step could be published as a review of access control attacks, vulnerabilities and the energy efficiency of these solutions on the IoT.

Autonomy

The second step involves suggesting an intelligent or autonomous approach other than the possible solutions identified in the first step. The idea behind the intelligent approach is based on the anticipated expansion of the IoT in the nearest future and considering the level of interaction not just between human and machine but machine and machine, there has to be some form of autonomy in the way communication is made (in this case access control). The suggested intelligent approach will then have to be tested on a real network.

The deliverable from this step could be published as an autonomic approach towards access control on the internet of things.

Energy Efficiency

The third step which is actually inherent in all steps is the part which forms the critical success factor for the project. Based on analysis of existing solutions as well as review of secondary data, a particular threshold energy value would have to be reached against which the energy consumption of the intended intelligent approach will be compared until the threshold is reached or exceeded. Therefore, the second step (intelligent approach) would most likely be iterative and experimental in nature pending when the energy threshold value is reached.

Considering that certain energy-related issues are specific to certain contexts[3], it is necessary to identify an application domain such as E-healthcare, Smart home, environmental monitoring and industrial automation. Choosing a domain would be based on certain criteria such as ethical sensitivity, access to resources, level of energy consumption and level of need for security.

To achieve this, a review will need to be done of each domain through a set of qualitative methods:

Risk alternatives for methodology

In a case, where the aforementioned methods are not feasible, secondary data related to a specific application domain will be reviewed as part of the domain identification process.

Security issues in wireless healthcare applications using wireless sensor networks[16] gives specific information about security issues as it relates to healthcare organization with focus on specific IoT applications such as MobiCare, UbiMon, AlarmGate, and CodeBlue.

Information about smart city architecture as well as its security issues are also discussed with focus on specific applications such as ETSI M2M and 3GPP LTE-M[21].

Information about smart homes with focus on smart metering in a wired smart home instance with protocols such as M-bus and xDSL[22].

This stage involves reviewing all the possible approaches that can be applicable to the domain chosen in phase 1.

The deliverable from this step would be an energy-efficient autonomous approach to access control on the internet of things.

Time Plan

GANTT CHART
















	 Task Mode	Task Name	Duration	Start	Finish	Predecessors
1		To develop a draft research proposal	68 days	Thu 24/09/15	Mon 28/12/15	
2		To review access control attacks and vulnerabilities on different IoT application domains	45 days	Mon 04/01/16	Fri 04/03/16	
3		To investigate autonomous computing and its implication to the IoT context	43 days	Mon 07/03/16	Wed 04/05/16	2
4		To develop a methodology that combines energy efficiency, autonomy and access control in a coherent way	43 days	Thu 05/05/16	Mon 04/07/16	3
5		To publish a paper on a review of access control attacks , vulnerabilities and solutions	0 days			
6		To develop an autonomous approach to achieve access control on the IoT	67 days	Tue 05/07/16	Wed 05/10/16	4
7		To experiment iteratively on the above approach in order to improve its energy efficiency	60 days	Thu 06/10/16	Wed 28/12/16	6
8		To critically discuss the development process and the results	25 days	Thu 29/12/16	Wed 01/02/17	7
9		To publish a paper on an autonomous approach to access control on the IoT	0 days	Thu 02/02/17	Thu 02/02/17	8
10		To build a prototype based on the results of the experiment	80 days	Thu 02/02/17	Wed 24/05/17	8
11		To test the prototype based on a 3 major test cases	69 days	Thu 25/05/17	Tue 29/08/17	10
12		To critically evaluate each step of the entire process and reach concrete conclusions	86 days	Fri 01/09/17	Fri 29/12/17	
13		To publish a paper on energy-efficient autonomous access control on the IoT	0 days	Mon 01/01/18	Mon 01/01/18	12
14		Report Writing	152 days	Mon 01/01/18	Tue 31/07/18	

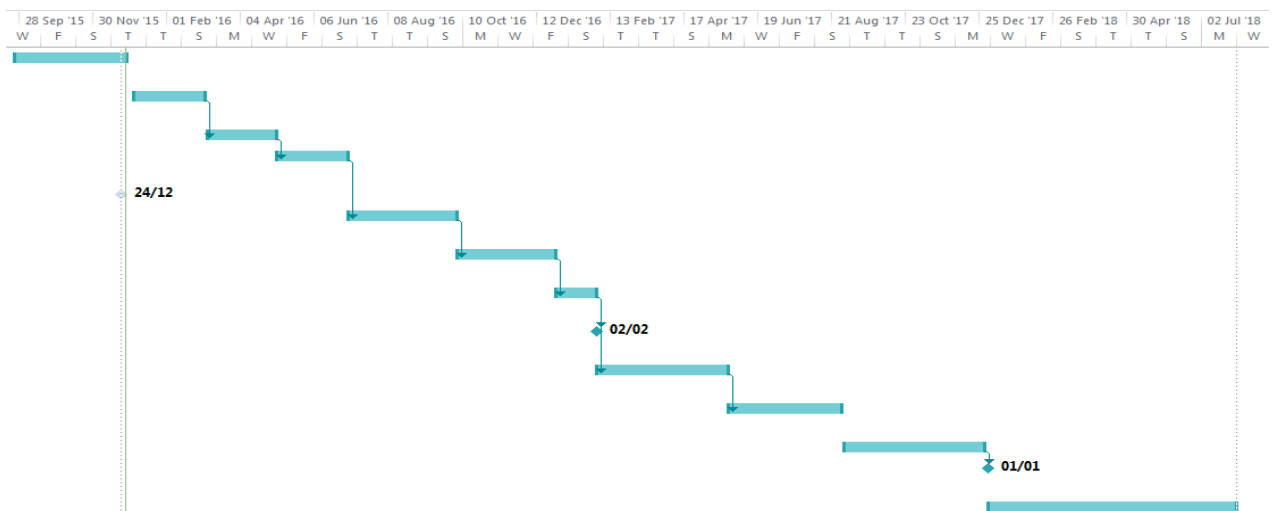
Figure 57: Time Plan

The time plan above spans a period of slightly less than 3 years (34 months) beginning from 24th September 2015 to 31st July, 2018.

Conclusion

There has been research in the three aspects (Energy efficiency, autonomy and access control) and even research on the balance between energy efficiency and security but little or no research has been done on the trade-off between energy efficiency, autonomy and access control.

The expectation from research is that a technique be discovered that intelligently or autonomously achieves effective access control in an energy –efficient manner. While the research may seem broad in terms of cutting across three research areas, the narrowness lies in the novelty of seamlessly synchronizing the three.



References

- [1] S. S. Prasad and C. Kumar, "A Green and Reliable Internet of Things," *Commun. Netw.*, vol. 05, no. 01, pp. 44–48, 2013.

- [2] I. Stojmenovic, "Localized network layer protocols in wireless sensor networks based on optimizing cost over progress ratio," *IEEE Netw.*, vol. 20, no. February, pp. 21–27, 2006.
- [3] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," *IEEE Commun. Mag.*, vol. 49, no. April, pp. 28–35, 2011.
- [4] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, and Xuemin Shen, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 1, pp. 32–43, 2012.
- [5] B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "Energy Cost of Security in an Energy-Harvested," pp. 198–201, 2014.
- [6] Gartner, "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015," 2014. [Online]. Available: <http://www.gartner.com/newsroom/id/2905717>. [Accessed: 10-Dec-2015].
- [7] A. Athreya, B. DeBruhl, and P. Tague, "Designing for Self-Configuration and Self-Adaptation in the Internet of Things," *Proc. 9th IEEE Int. Conf. Collab. Comput. Networking, Appl. Work.*, pp. 585–592, 2013.
- [8] P. Mahalle, "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things," *J. Cyber ...*, vol. 1, pp. 309–348, 2013.
- [9] T. Weigold and A. Hiltgen, "Secure Confirmation of Sensitive Transaction Data in Modern Internet Banking Services *," 2011.
- [10] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. H. Pinkse, "Quantum-secure authentication of a physical unclonable key," *Optica*, vol. 1, no. 6, pp. 421–424, 2014.
- [11] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios," *Sensors Journal, IEEE*, vol. 15, no. 2, pp. 1224–1234, 2015.
- [12] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, "SEA: A Secure and Efficient Authentication and Authorization Architecture for

IoT-Based Healthcare Using Smart Gateways,” *Procedia Comput. Sci.*, vol. 52, no. 0, pp. 452–459, 2015.

[13] M. Ulieru and P. Chapman, “Lessons from the past for the future Internet,” *2008 First Conf. IT Revolutions*, 2008.

[14] O. Garcia-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, and J. L. Torre-Arce, “A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO.”

[15] E&Y, “Cybersecurity and the Internet of Things,” *E&Y*, no. March, 2015.

[16] P. Kumar and H.-J. Lee, “Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey,” *Sensors*, vol. 12, no. 1, pp. 55–91, 2011.

[17] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[18] E. Alsaadi and A. Tubaishat, “Internet of Things: Features, Challenges, and Vulnerabilities,” *Int. J. Adv. Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 1–13, 2015.

[19] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of things,” *Computer (Long Beach. Calif.)*, vol. 44, no. 9, pp. 51–58, 2011.

[20] V. Getov, “Cloud adoption issues: Interoperability and security,” *Adv. Parallel Comput.*, vol. 23, pp. 53–65, 2013.

[21] A. Bartoli, J. Hern, J. Hernández-Serrano, and M. Soriano, “Security and Privacy in your Smart City,” *Cttc.Cat*, pp. 1–6, 2011.

[22] M. Schneps-Schneppe, A. Maximenko, D. Namiot, and D. Malov, “Wired Smart Home: Energy metering, security, and emergency issues,” *Int. Congr. Ultra Mod. Telecommun. Control Syst. Work.*, vol. 2020, pp. 405–410, 2012.

