A Thesis

Entitled

A Secure and Low-Power Consumption Communication Mechanism for IoT

(Internet of Things) and Wireless Sensor Networks

by

Ashutosh Bandekar

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the

Master of Science Degree in

Electrical Engineering

_____

Dr. Ahmad Y. Javaid, Committee Chair

_____

Dr. Mansoor Alam, Committee Member

_____

Dr. Hong Wang, Committee Member

_____

Dr. Amanda Bryant-Friedrich, Dean
College of Graduate Studies

The University of Toledo

August 2017

An Abstract of

A Secure and Low-Power Consumption Communication Mechanism for IoT (Internet of Things) and Wireless Sensor Networks

by

Ashutosh Bandekar

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the Master of Science Degree in Electrical Engineering

The University of Toledo

August 2017

Internet of Things (IoT), the newer generation of traditional wireless sensor network devices, offer wide variety of applications in various areas including military, medicine, home automation, remote monitoring, etc. Due to their wide usage and recent large-scale DDoS (distributed denial of service) attacks using millions of these devices, security of these devices have become an important aspect to address. Additionally, security implementation needs to be power efficient considering the limited power resource available to these wireless devices. Since users, as well as attackers, can control or access IoT devices remotely using smartphone or a computer, any attack on these devices can result in disasters.

This thesis is directed towards development and implementation of a secure and power-efficient communication mechanism on these low-power devices. First, we performed a detailed analysis of the power consumption of these devices for different environment variables including temperature, lighting and location (in/outdoor), to understand effects of these parameters on device power consumption. Second, we proposed and implemented a novel security algorithm to detect and mitigate RPL (routing

protocol layer) attacks in IoT networks. We evaluated changes in the behavior of IoT devices before and after the implementation of our proposed algorithm in terms of the change in battery life and power consumption. The proposed security implementation has the novel approach of using the RSSI (received signal strength indicator) tunneling to detect and mitigate RPL (routing protocol layer) attacks. Finally, we conducted experiments in simulation as well as on first generation real-world sensor nodes (Zolertia Z1 motes) to evaluate the power efficiency of our proposed algorithm. We conclude the thesis with insights on (a) the effect of interference present in the atmosphere on battery life, (b) security provided by the proposed algorithm, and (c) power-efficiency of the proposed security algorithm for IoT devices.

Acknowledgements

Every work is source which requires support from many people and areas. It gives me proud privilege to complete Thesis report on “A Secure and Low-Power Consumption Communication Mechanism for IoT(Internet of Things) and Wireless Sensor Networks” under valuable guidance Dr. Ahmad Y. Javaid. I appreciate his inputs and guidance, which are utterly important for thesis. I am also extremely grateful to our respected Department Chair (Electrical Engineering and computer science Dept.) Dr. Mansoor Alam and Dr. Hong Wang for to taking out time to sever as a thesis committee from their busy schedule.

At last I would like to thank all the unseen authors of various articles on the Internet, helping me become aware of the research currently ongoing in this field and all my colleagues for providing help and support in my work.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

DODAG……....Destination Oriented Directed Acyclic Graph
DIO ……..DODAG Information Object
RPL……Routing Protocol
6LoWPAN……IPv6 over Low power Wireless Personal Area Networks.

Chapter 1

Introduction

1.1 Wireless Sensor Networks (WSNs):-

Wireless Sensor Networks (WSNs) known as, wireless sensor and actuator network (WSAN) is a device which collectively works as an autonomous network itself to monitor or collect information from different conditions such as physical or environmental. These devices primarily developed for the use of military applications. Wireless sensor networks are usually will be functional in the form of several nodes. These nodes will form a network together and will communicate with each other for efficient functionality.

Wireless sensor network devices are usually made up of different types of sensors such as temperature sensors. These devices also consists of radio transreceiver, microcontroller, etc. WSNs can form different types of topologies: Star topology, Mesh topology or Tree network topology based on user's specification. These nodes possess an ability to communicate with each other in the network or directly with base station. These are low powered devices which can work on batteries. The deployment of these devices is very easy and economic as we can just drop these sensors in the required fields or can be deployed manually. These wireless sensor network devices are generating interests in

many field of application viz. medical, military application mainly due to the characteristics they possess.

The Wireless sensor networks devices possess following characteristics [1].

1. Low power consumption: - As most of these devices work on batteries hence these devices have low power consumption.
2. Resilience: - These devices also has an ability to provide the required services to the user in case of node or device failures. This ability is called as resilience.
3. Mobility: - Wireless sensor network devices provides user mobility, due to which user can deploy these devices anywhere according to the user's specification or requirement of an application.
4. Heterogeneity: - These devices provides heterogeneity to users so that many different nodes with different architecture can work together
5. Scalability: - WSNs can be deployed anywhere in small scale to large scale as these devices scalability
6. Cross- layer design: - This characteristic of these devices helps us to make the optimal modulation to improve overall network's performance in terms of energy efficiency, QoS (Quality of Service), etc.
7. Flexibility: - All wireless sensor network devices are flexible in terms of designing of the topology, deployment of these devices, etc. This characteristic of these devices provides user

8. Ruggedness: - These devices primarily developed for medical purposes. So their basic architecture is rugged. These devices can work in any environment and in any situation.

Each of these devices separately also known as sensor nodes or mote are capable of performing some computational algorithms or used for the communication purposes. All of these devices share typical architecture, which includes power source, microcontroller, transreceiver, ADC, external memory and some external sensors to

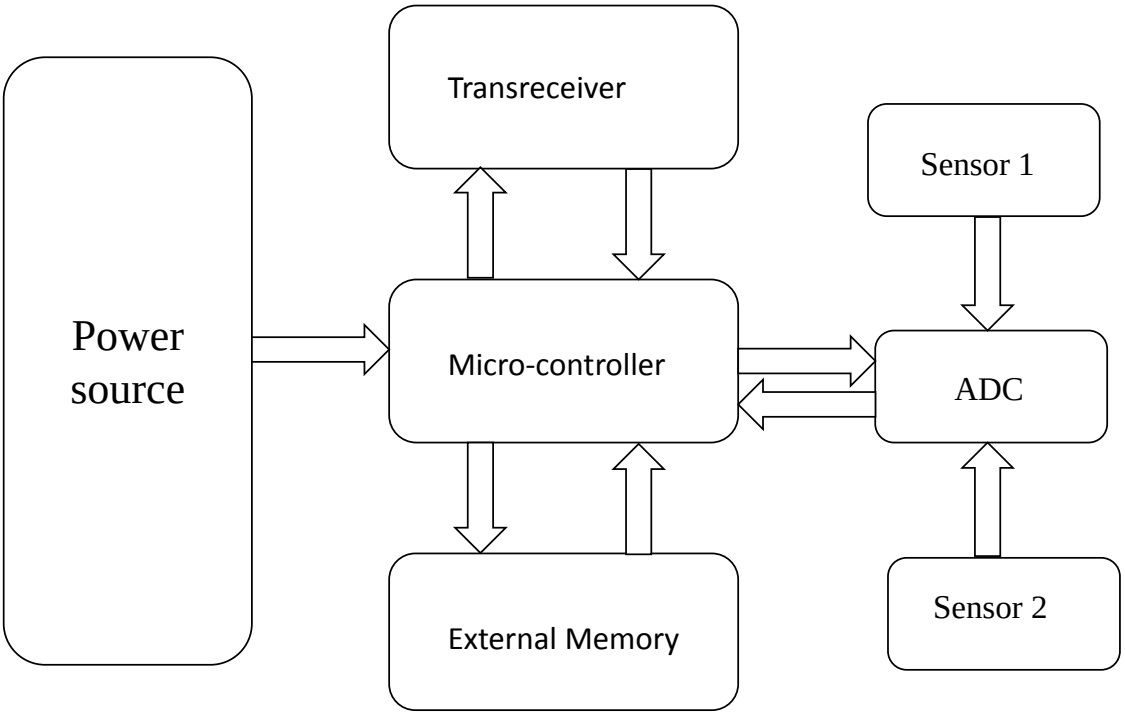


Figure 1 Typical Architecture of Wireless sensor network devices [1]

complete the application requirements. We can observe the typical architecture from figure 1 and the detailed description is as follows: -

Microcontroller: - To perform many operations these devices requires computational capabilities. These requirements can be accomplished using digital signal processors, FPGA, microprocessors and the most commonly used are microcontrollers. Microcontrollers usually are used in all the sensors or in embedded systems. These microcontrollers can be reprogrammed and can be optimized according to the requirement of the deployment.

Transreceiver: - Every sensor node requires radio connectivity or wireless connectivity to communicate with the devices which might have same or different architecture. Transreceiver provides these devices with the capabilities so that they can communicate with each other. Transreceiver in these sensor nodes makes use of ISM band usually which gives free radio spectrum and makes the nodes available globally.

Sensors: - These devices are equipped with many sensors to capture or read the data from the environment in which they have been deployed. These sensors are basically hardware which are incorporated with the WSNs according to the user's requirement. These sensors measure the data from the environment and send it to the neighboring node or base station. There are many sensors which are compatible with these devices such as Temperature Sensors, Accelerometer, etc. Most of these sensors are small, easy to deploy and due to this they can be very helpful in monitoring the environmental or any geographic changes.

1.1.1 Application of Wireless Sensor Networks (WSNs)

In modern times WSNs devices are gaining popularity amongst many manufacturers and researchers due to their compact and robust architecture. These devices have many application ranging from environmental monitoring, military application to health care monitoring. Following are some of the applications for wireless sensor network devices [1] [2]: -

Environmental Surveillance: - As WSN devices are compact and battery operated, they are very easy to deploy anywhere regardless of any geographic conditions. Also as they can operate in the form of network, we can monitor or we can deploy monitoring system for the large part of the geographic region. Through environmental surveillance we can deploy landslide detection system, forest fire detection system, etc.

We can even deploy these devices to monitor air pollution, water pollution. WSN devices have been deployed in many cities of the world to monitor pollution in the environment such as in Stockholm, London and in Brisbane these devices have been deployed to monitor the concentration of the poisonous gasses in the air. Through WSNs we can monitor the quality of water of many water resources such as dams, rivers, lakes, oceans and underground water reserves.

Health Care Monitoring: - The WSN can be used for many medical application such as vital monitoring of the patients, any implanted or wearable device, etc. Implanted devices are the devices which are inserted inside of the human body and wearable devices are the devices which are used to measure vital through the surface of the human body. With the help of these wireless sensor network devices we can create body area network altogether also called as WBAN. WBAN is the network though which we can monitor human body

vitals continuously through the various sensors implanted inside the human body or any wearable devices such as heart rate monitor, body temperature sensors, and blood pressure sensors, etc. This wireless body area network (WBAN) consists of many of these wireless sensor network devices though which all of biosensors will be connected to each other wireless connection to collect and process data regarding patients vitals [3].

Industrial Monitoring: - As the popularity of these wireless sensor network devices is increasing these devices can also be deployed for industrial monitoring. Through these devices we can deploy machine health monitoring system. As these sensors provides user the significant cost saving with the full functionality compare to any other devices. As these devices possesses scalability as characteristic, they can be deployed in large number of network. We can use these devices for data center monitoring, data logging, waste water monitoring, etc. As wireless sensor network device has cross layer compatibility, they can be deployed in almost any environment or situation.

Military Application: - Wireless sensor network devices were developed primarily for military purpose. The architecture of these devices are much more rugged and can get adapted in any environment. Through these devices we can deploy are monitoring system. These devices can detect any enemy intrusion on battlefield and also can send distress signal to base station, any military personnel can monitor the on-going activities with the help of these sensor devices.

1.2 Internet of Things (IoT)

Internet of things are the physical computing devices which are interconnected, they can also be referred as connected or smart devices. These devices primarily offers

advanced connectivity amongst each other. Mostly IoT devices are embedded in system and interconnection of these devices will usher automation in all fields which helps us in building smart cities, smart grid, smart home, etc. These devices basically collects data from other devices and make that data flow between other devices autonomously.

In Internet of Things(IoT), thing can be person with any biosensor implanted on his body, any industry, etc. Machine to machine communication can be made easily with the help of these devices. Essentially IoT devices are the next generation of the wireless sensor network devices.

Wireless sensor network devices were not that much equipped compared to IoT devices. As WSNs evolved they became more and more equipped with an integration of enhancements such as wireless technologies, micro services, and micro electrochemical systems, etc. These enhancements allowed the data flow between unstructured machines generated data. Due to which analyzing data flow between different machines became easier.

Due to IoT devices several machines gains an ability to communicate between two or more devices. These devices also help to create new promising business models which will improve all the business processes. Deployment of these devices also reduces cost and risk as they are getting evolved and gaining popularity. According to one study there will be almost 20.8 billion devices will be in use by 2020 [4]. All these devices will be interconnected via internet. As these devices works with limited microprocessor resources, memory and power requirement, they finds applications in every field. Also according to the reports from Cisco IoT devices will generate $14.4 trillion in value amongst all the industries in next decade.

1.2.1 Application of IoT services

Internet of Thing (IoT) devices brought new wave of inter connected devices which has many application. Due to accelerated use, these devices will bridge the gap between physical devices and digital world. As these devices could be the main aspect in data aggregation and segregation. As these devices have vast application, following will be an overview of some of the most important applications provided [5].

Smart Homes: - With the use of Internet of Things devices there is an immense and constant evolution in the field of home automation. All these devices will communicate each other via wireless connectivity or internet and altogether make a smart home. Smart home enhances the security of those and also the owner of the house can control the environment of the house. It is also energy efficient as these devices works on limited resources and are dedicated to their programmed activity. Google smart home, Amazon, Belkin and Philips are the prominent manufacturers of these devices. Also Nest learning thermostat is one revolutionary device which is self-learning device.

Wearables: - Wearables are one of the most used or popular products. All of these wearable devices comes with embedded IoT devices and these devices are broadly expanding to health monitoring and other entertainment areas. As all the wearables battery operated, IoT devices could be an appropriate choice. Manufacturers such as Apple, Samsung, Fitbit, Jawbone, etc. are the giant manufacturers in the field of wearables.

Environmental Monitoring: - IoT devices can be deployed to monitor as environmental monitoring systems. Through this system we can monitor water quality, atmospheric condition and soil condition. Also due to the deployment of these devices we can monitor environmental pollution, also early warning systems for natural calamities such as earthquakes, tsunami, etc.

Agriculture: - IoT devices contributes towards adopting new and innovative techniques in the field of agriculture. The convergence of physical devices, wireless or internet connectivity, cloud platforms will help farmers to collect data or vital information regarding environmental or agricultural conditions of the area. With the deployment of these devices farmer can now detect whether the land is dry or whether it is has been fertilized or not. IoT devices can help farmers in predicting the future yields too.

Medical and Healthcare: - IoT devices performs an important part in Wireless Body Area Network. Through this network we can monitor patient's vital information regarding Hear Rate, blood pressure, etc. remotely. Also some specialized sensors can be deployed to monitor the health of senior citizen or new born infants. Also in some hospitals smart beds have been deployed. These beds can track the movement of the patient.

Transportation: - Nowadays automotive industry is more dedicated towards the self-driving or connected cars. As through IoT devices aggregation of data becomes easier, these devices will be the most formal choice. Through these devices collected data can be monitored in a continuous manner, these IoT initiative in automotive industries promises to reduce accidents and save live, also reduces pollution, etc. Manufacturers like BMW, Ford, Google, Tesla Inc. are the manufacturers which are promising self-driving car.

With the help of Internet of Things devices self-driving car is now becoming a reality. Also smart traffic control, smart parking, road assistance, etc. is possible due to utilization of Internet of Things devices.

1.3 Thesis Outline

The thesis is organized in following manner:-

In chapter 1, we disussed an introduction regarding Wireless sensor network, and IoT also there is application and there literature surveyd in the document along with the thesis outline

Chapter 2 provides detailed overview of security issues regarding IoT devices and brief introduction to proposed algorithm

Chapter 3 gives detailed description regarding proposed methodology and implemented attacks.

Chapter 4 outlines the overview and security analysis of the algorithm. Also this chapter explains the technical approach we adopted.

Chapter 5 summarizes the results from all conducted experiments.

Chapter 6, Concludes the whole research with future work related to the subject

Chapter 2

IoT Security Issues

2.1 A survey on IoT security issues

Origination of wireless sensor network devices brought immense evolution in wireless networking devices. This evolution brought the next generation of these wireless sensor network devices which we call as Internet of Thing devices which are next generation of the wireless sensor network devices. Due to its continuous evolution these devices are accumulating popularity from different industry manufacturers such as home automation service providers, etc. As users from all over the world seek automation in their everyday work these devices are becoming part of many household appliances too such as bulbs, microwave, etc.

These IoT devices are interconnected through the internet and they are low powered. As these devices are connected to each other via internet continuously, they are vulnerable to the most of the cyber-attacks. The conception of IoT devices is not veteran compared to other wireless networking devices, there is still lot of research is going on considering the security of these devices. These devices also shares almost similar network protocol as that of the tradition al network. But as these devices possess

constrained resources the security implementation to thwart any cyber-attack should be efficient in terms of power consumption.

Recently there was report published regarding the security of these devices. According to this report, 70 percent of these devices have vulnerabilities [6]. IoT devices has constrained resources attacks such as distributed denial of service attacks (DDOS) will render the whole network. Also there have been several incidents reported regarding DDOS attacks on IoT devices. In the specific cited case, millions of IoT devices, packaged with an insecure operating system, were used to send requests to a DNS provider called Dyn, leading to disruption in services of providers like Netflix, CNN, and Twitter [7]. According to survey conducted in 2014, 39% of the people were more concerned about security of these devices in adopting IoT technology [4].

Also in January 2014 one of the author from Forbes also stated that through these IoT devices hackers can spy on people in their home as smart home technology is becoming popular everywhere [8]. In 2008 hackers' demonstrated remote insulin pump by hacking these IoT device enabled biosensor [9]. In 2016 hacker took down DNS provides and major websites and the hackers deployed distributed denial of service attack by IoT devices which were running Mirai malware [5]. Mirai is the malware which will turn any device connected to internet its slave or bot and affected devices will be the part of the large network of botnets. Also the researchers from the University of Michigan launched successful attack on Samsung SmartThings platform and they were able to control the installed home automation system and also they employed an eavesdrop to accumulate the PIN code used for the same devices [4]. Most of the communication protocol followed by these devices are same as conventional wireless devices. But unlike

those devices firewall, security updates and any anti malware system is not suitable for these smaller devices with limited resources. All of these devices has low cost, they are simple to install, yet they do not have all the required safety measures which can thwart any attack or at least it will detect or alarm the user for possible intrusion. As nowadays these devices have been deployed in many cars to make them more of a self-driving car, so by hacking in to these devices intruder can control the vehicle remotely and the result will disastrous. Similar type of incident happened in [10]and they took control of that vehicle. This carjacking incident is an eye opener for all the security analyst and the manufacturers of the IoT devices. Also there many studies regarding the applications of cryptography. Elliptical curve cryptography is the most suitable technique amongst them as it requires limited resources and time to encrypt messages but accommodating these techniques with any security implementation will be challenging as it will increase the resource consumption of the network. [11] [12] [13] [14]

2.2 Overview of Received signal strength indicator (RSSI)

Received signal strength indicator is term used in telecommunication to measure the power present in received signal. Generally, it is invisible to the user. It has also been proved that this signal strength can affect the wireless connectivity. RSSI primarily provides the actual power level being received at the receiver side. Hence, RSSI number is directly proportional to the strength of the signal. This technique measures the quality of the received signal from the receiver device.

RSSI was primarily introduced in an IEEE 802.11 system but due to optimization of RSSI for IEEE 802.15.4, it can be used for all wireless network sensor networks.

Integration of RSSI module in IoT devices will give the distance between the two or more nodes in the network. It is possible to convert RSSI value into the distance and vice versa.

2.3 Proposed algorithm based on Received signal strength indicator (RSSI)

Monitoring of the whole network is necessary to mitigate cyber-attack. To provide security against any intrusion the proposed technique combines network layer parameters with the packet encapsulation. This security implementation detect several DDOS attacks such as wormhole attack, hello flooding, rank attack, etc.

The network layer parameters used for the implementation includes RSSI,

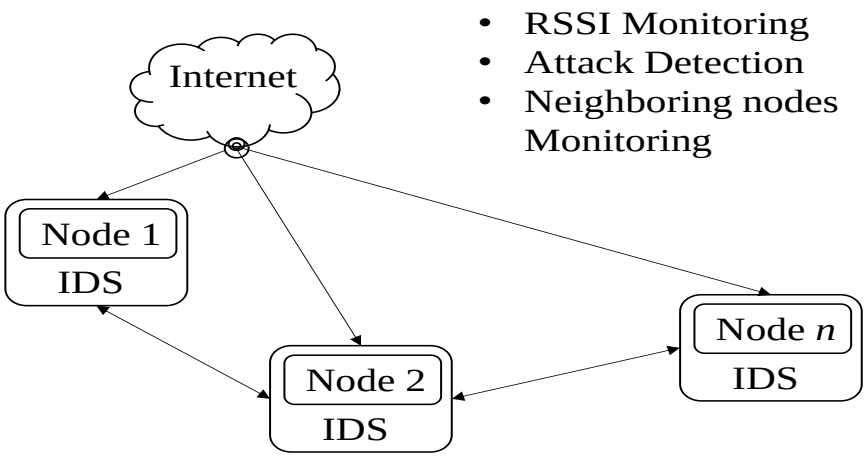


Figure 2. The general architecture of the proposed security [16]implementation

localization, etc. From figure we can observe the general architecture of the proposed implementation. From figure 2 we can observe the general architecture and the working of the proposed security implementation. From the observation we can notice that all the nodes communicating with each other via internet with the help of IPv6 network protocol

also it has one anchor node which will monitor the neighboring nodes within network. Through this we can monitor neighboring nodes within the network. The implementation works in a step by step manner considering all the parameters we are considering the network layer. First it will monitor the neighboring node, RSSI values collection and monitoring and attack detection. The detailed explanation about the proposed algorithm will be in further sections.

2.4 Chapter Summary

This Chapter provides you with the survey of the IoT devices, and their security issues. This chapter introduces you with vulnerabilities these devices possess and also provides you with potential vulnerabilities these devices we might face in the future. There are also documented and recent incidents regarding cyber-attack on these IoT devices.

Further there is an overview of the Received Signal Strength Indicator (RSSI), the mechanism which we adopted in our cyber-attack mitigation algorithm. Also, since the conception of RSSI mechanism it was compatible with IEEE 802.11 but how it is possible with modification in certain modules of RSSI it is compatible with IEEE 802.15.4.

As we proceed towards the next section, we can observe the illustration of the RSSI tunneling mechanism through the figure.2 In next section we will discuss the further step of our adopted methodology which is the validation of the algorithm through power consumption analysis. This analysis will prove the efficiency of any security implementation in terms of resource consumption.

Chapter 3

Analysis of Secured Low Power Consumption Communication

3.1 Proposed Methodology

To analyze the impact of an algorithm considering the mitigation of the cyber-attacks essentially we have to contemplate deviation in the power consumption of the IoT or WSNs devices. As we are dealing with the devices which works on constrained resources, we have to consider the consumption of those resources as an important aspect.

As these devices procuring popularity amongst most of the researchers and manufacturers, as a result they are becoming a critical part of many the systems which have high computational capabilities. Higher the computational requirements, higher the consumption of the resources, resulting more power consumption. Deviation in power consumption can be observed due to many important factors such as interference. Interference in the communication occurs due to some external factors other than any intruder or on-going cyber-attack such as environmental interference, electrical interference or magnetic interference etc. These external factors has an impact on the power consumption of the device or the whole network according to the type of the

interference present during on-going communication. As there is deviation in power consumption of these devices the battery life of these devices will also get affected.

The presented research in this thesis was conducted in step-by-step manner. Fundamentally we conducted many experiments considering the operating environment, lighting conditions and topology of the network created with Zolertia Z1 mote. These devices shares similar architecture with newer generation of these devices called as Internet of Things (IoT) devices. As these devices also operates on constrained resources, becomes prime choice for these experiments.

As these devices requires drivers to upload programs and to operate usually, we considered Contiki operating system. As Contiki OS is an efficient operating system developed for the wireless sensor networks devices such as Zolertia Z1, Tmote, Sky mote, etc. This operating provides many examples and features such as calculating power consumption of the connected devices or the whole network, monitoring RSSI value of the targeted device, etc. Equipped with the power consumption program analysis of the power consumption of the low powered devices is achievable. This module will check the on-going power consumption periodically. In the next section we will discuss about the analysis of power consumption methodology.

3.2. Power consumption analysis methodology:-

Since the genesis of IoT devices there have been many studies which rationalizes the deviation in power consumption but most of those studies are not unreservedly trustworthy as most of those studies are simulation based. As IoT devices has constrained resources, before any surety implementation power consumption is our priority.

Implementation itself will increase the power consumption and in addition to that there will be interference present in the atmosphere which will increase the deviation in power consumption. In most of the previous studies analysis presented is through simulation and very few are real world analysis. We are uploading the powertrace example in Zolertia z1 mote which is already present as one of the predefined examples in Contiki OS which we are using for the required drivers for the first generation of IoT device which we are using. The purpose of this analysis is to predict the battery life of the device before the implementation of proposed algorithm and compare the results after the implementation to validate the proposed security implementation.

For analysis we considered different environment and lighting conditions and conducted an experiment in indoor lab, auditorium, and basketball arena in different lighting conditions. This powertrace example provides detailed results in various modes such as Tx, Rx, idle mode and active mode. With powertrace we are also uploading different examples such as broadcast and unicast or one-to-one communication to validate the results of the change in power consumption. The accuracy of power trace has been proven experimentally with the accuracy rating of 94%. This module estimates the consumption of the power on the node level. [15]

After collecting the data from the various experiments the we estimated the battery of IoT devices. The battery life estimation will assist in verifying the impact of interference on the battery life of the device. We conducted several experiments without any security implementation in different environment and lighting conditions in real world with identical topology for all the experiments. With same topology we ran simulations with powertrace example with broadcast and unicast or one-to-one

communication. But according to our analysis we concluded that the simulated results and the results from the real world experiments were contrast to each other. To validate the efficiency implementation of the proposed algorithm in terms of the resource consumption we cannot rely on the simulated results, real world mote analysis is required to observe the behavior of the devices in different conditions.

As we are proposing the security implementation for IoT devices, implementation of cyber-attacks are required. To legitimize the working of the security implementation we implemented some cyber-attacks discussed in the next section.

3.3. Implemented Attacks:-

To corroborate the cyber-attack mitigation algorithm or proposed intrusion detection system, on-going cyber-attacks are required. Following are some of the implemented cyber-attacks which we deployed on the network.

1. **Wormhole Attack**:-

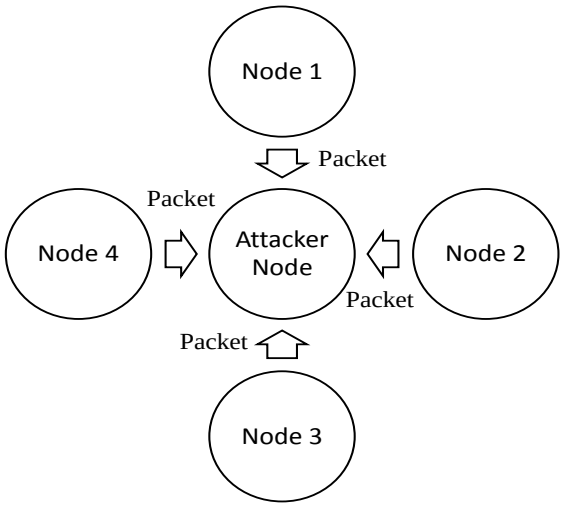


Figure 3. General Topology of Wormhole Attack

In wormhole attack attacker creates fake rout for node communication purpose. This rout or path will pose itself as shorter route or path compared to other route within the network. This will create confusion amongst the node routing mechanism and compels all other nodes to follow the compromised route. Attacker can introduce one or more malicious nodes and this attack also provides the attacker to create the tunnel with the help of the malicious nodes.

During wormhole attack can node can captures the transmitted packet and transits

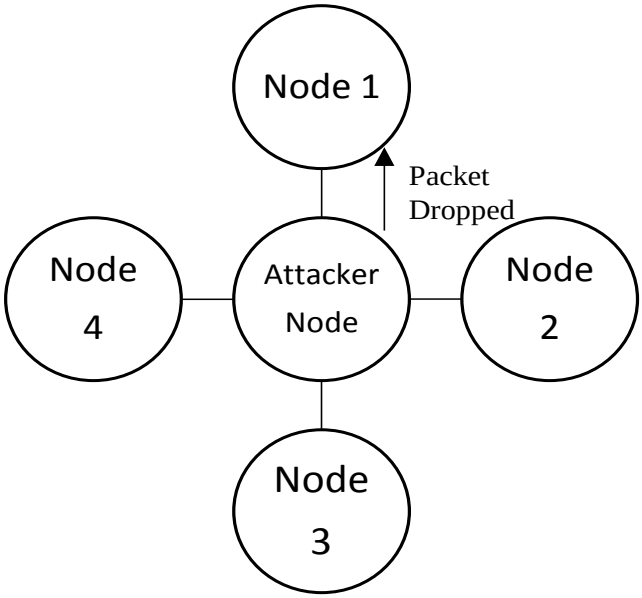


Figure 4. General Topology of Wormhole Attack

them to malicious node which will locate at distant node and it will transmits all the captured packets to the compromised location or node. It is possible to launch an attack for the attacker on the network which will compromise the whole network or any legit node or it can even help the attacker to break through the cryptographic implementation implemented on the network.

This attack primarily targets towards dropping the packets, which were supposed to be forwarded by the node. This attack categorized into the denial of service attacks. If the attacker node is placed precisely within the network, then it will help the attacker to isolate the targeted node from the network. With this attacks it is possible to filter some of the applied protocols and increase the power consumption of the whole network. It is also possible to launch this attack with several denial of service attacks.

Mitigation: - To mitigate this attack there several solutions but the easiest amongst them is to luxate the routes between the source and destination of the nodes. But it will be difficult if we are dealing with large number of nodes. Analyzing the application level traffic flow between the nodes and implementing security or cryptographic implementations is possible for small network and also for the large network consisting of the large number of no. of devices.

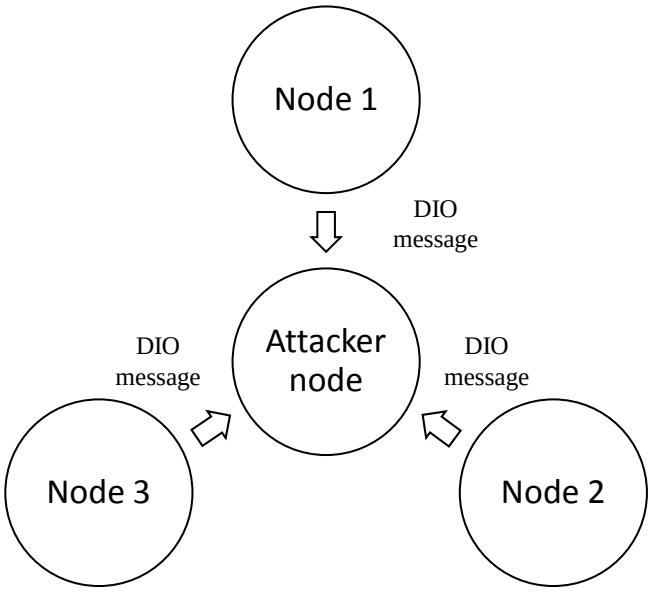


Figure 5. Brief working of flooding

Hello flooding: - Hello flooding attack also can be categorized as Denial of service attack.During on-going hello flooding attack attacker can generate huge traffic flow through duplicated packets or messages, which will cause the nodes within the network to send destination oriented directed acyclic information object (DIO) message and this causes these nodes to reset their trickle timers. This attack is possible with the combination of different RPL attacks. Figure A and B represents the graphical representation of the working or mechanism of the flooding attack.

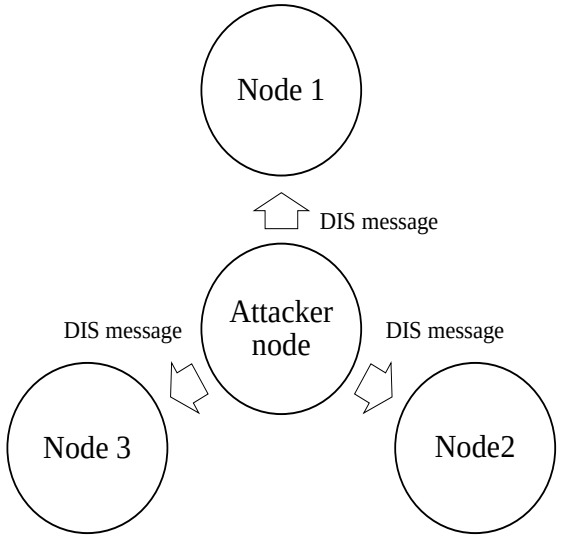


Figure 6. Brief working of flooding attack

Mitigation: - Solution for these type of attacks it to check bidirectional communication link between nodes for each packet or message. If there is no reception of acknowledgements, then the route chosen to send packet is compromised.

Rank Attack: - Ranks of a network is which within destination oriented directed acyclic graph will define nodes position with respect to destination directed acyclic graph. In rank attack attacker will broadcast the lower rank to its neighboring node within the

network and make the un-compromised nodes to connect to destination oriented directed acyclic graph via the compromised node. This attack can become the primary step for the initiation of other distributed denial of service attacks such as Wormhole attacks, Sinkhole attack, etc.

Mitigation: - To mitigate this attack there are several mechanism but the most popular amongst them are VeRa and TRAIL mechanisms.

3.4.Chapter Summary: -

This chapter provides outlines the methodology adopted to conduct experiment to validate the efficiency of the algorithm in terms of resource consumption. Initially we discussed about the chosen hardware for experiments which Zolertia Z1. As we proceeded further there a discussion about the advantage of the power consumption analysis and experiment.

To implement the cyber-attack mitigation algorithm there should be on-going attack on the network and there is a detailed diagrammatic explanation which explains the exact mechanism of the implemented attacks. We have even mentioned some of the popular mitigation techniques for those attacks.

In next chapter there will detailed explanation regarding the proposed cyber-attack mitigation algorithm. We have also elucidated all the aspects such as an operating environment, hardware and lighting conditions chosen for conducting experiments.

Chapter 4

Cyber Attack Mitigation Algorithm Using RSSI Localization Tunneling Mechanism

4.1 **Overview**: -

In chapter 2 we had brief explanation of the proposed cyber-attack mitigation algorithm. As we discussed in previous section to validate the efficiency of the algorithm there has to be an on-going attack or attacks only. This approach will make our understanding about IoT devices better. Also from figure 2 we can we can notice that there is on anchor node to observe the data communication within the network.

The proposed implementation will work in three steps such as RSSI monitoring, neighboring node monitoring and attack detection while connecting with all the nodes within network via internet using IPv6 protocol. Figure 2 show the general architecture of the mitigation algorithm.

As discussed earlier there is one anchor node to collect the neighboring node information, monitor RSSI values and attack detection. The algorithm follows the following approach [16]:-

a. Determining the distance between each node in the network

b. Collecting the information regarding the neighboring node such as the distance of the neighboring nodes from the anchor nodes.

c. If the neighboring in not in the range of the anchor node then

i. Generate alert

ii. If corrupted node is present then, monitoring of the whole IPv6 stack initiated

d. RSSI monitoring is initiated

e. Determine the RSSI values

f. Determining the nodes that are in the range considering the error while determining RSSI values.

g. Node which not in range while considering the errors in RSSI values considered as suspected node

h. Again, running the algorithm to check the probability of being that is suspected node

i. Higher the probability, higher the chances of being attacker node.

j. Then, suspected node is declared as Attacker node.

By modifying algorithm we can detect and track the location of compromised node or node in the network as this algorithm follows localization based approach. Following is the proposed algorithm based on the approach we discussed [16].

Algorithm 1 Cyber-attack Mitigation in IoT Devices

Input: Node = N to n, Distance = di, Range = D, Vn = Victim Node
Output: Vn, An = attacker node

```
for i = 1 to n do
    for j = 1 to n except i do
        Calculate dij = distance (Ni, Nj)
        D = distance through RSSI
        monitoring;
        if D>di then
            Attacker Flag=1
            set Vn = Ni
            Go to step 1
        else
            Attacker Flag = 0;
        continue
        end if
    end fo
end for
```

Algorithm 1 Cyber-attack Mitigation in IoT Devices

Input: Node = N to n, Distance = di, Range = D, Vn = Victim Node
Output: Vn, An = attacker node

```
1 : for i = 1 to n do
2 :     for j = 1 to n except i do
3 :         Calculate dij = distance
          (Ni, Nj)
4 :         D = distance through
          RSSI monitoring;
5 :         if D>di then
6 :             Attacker Flag=1
```

Above algorithm is modified version of the existing IDS which was designed for wormhole attack. This proposed algorithm is modified considering the architecture and the constrained resource consumption of the Zolertia Z1. As the main goal of the research is to enhance security of the device considering the power consumption of it. So analyzing the impact of the implementation is more important.

To analyze and validate the efficiency of the algorithm we conducted several experiments with and without cyber-attacks and also with implementation of the IDS As

this algorithm is successful in detecting cyber-attacks, to substantiate its competence against the deviation of the power consumption several experiments has been conducted. In next section we elaborated the technical approach adopted for conducting experiments.

4.2 Security analysis of proposed algorithm

In chapter 2 we discussed about the implemented attacks. And had a brief overview of an algorithm. We are proposing an algorithm for DDOS attacks detection. We implemented flooding attack, rank attack and wormhole attack for the analysis purpose the algorithm. As through wormhole attack it is possible to launch several denial of service attacks we are presenting security analysis implementing wormhole attack. This attack allows attacker to launch cryptal analysis attack. The wormhole attack has several following symptoms which we can target to adopt them in any security implementation:-

- Drastic reduction in hops
- Longer delays in paths
- Increased Propagation delays
- Data reception from node located far from the network
- Receiving duplicate messages

4.2.1 Analysis of the security algorithm

Wormhole attacks brings change in within the network when it gets activated in it. These change can affect the performance metrics of network as generally through this

attack it’s possible to disrupt the network or exhaust the resources of the devices. If this kind of attack was place on the network consisting of IoT devices then these devices will not be operative and the results will be disastrous. So the proposed system has been designed considering the architecture of the IoT devices.

In previous chapter there is a brief introduction about the proposed algorithm in the graphical form. This algorithm work in three modules Monitoring RSSI values, neighboring information collection, validation, RSSI value collection, comparing probabilistic model, attack detection.

Internet of Things concept thriving in many industries in a very fast pace. As it is growing up in the industry their applications also gaining popularity and it is changing the human lives as well. IoT is a multifaceted system and it may consists of many different devices with many different architectures. Due to its heterogeneous structure it difficult to maintain its security at many different layers and it is challenging. Also IoT is a system which works with several different aspects such as internet, they are limited resources and lossy communication link. These devices uses few different protocols compares with the traditional computer network. IoT devices works with protocols such as 6LoWPAN, RPL, etc. There are several attacks possible on these devices such as any DDOS attacks. There are several DDOS attacks which we are concerned about such as Hello flooding, wormhole, rank attack, Sybil attack, etc.

If launched these attacks disastrous effects on these low powered devices. Out of all RPL attacks we are considering wormhole as this can be launched on any network with the combination of several different DDOS attacks. [17] As of now there is there is

no cyber-attack mitigation algorithm present which will be energy efficient as well. As these devices has constrained resources implementation of any mechanism which will consume more of the resources and it will act as denial of service itself. The proposed algorithm is a generic algorithm but according the architecture of the devices present within network and scalability of the network optimization required before the implementation.

Network Layers	***Traditional Network***	***IoT Network***	***Contiki Layers***
Application Layer	HTTP, FTP, SMTP,etc.	CoAP, MQTT, XMPP, AMQP	Application
Transport Layer	TCP/UDP	UDP, DTLS	Transport
Network Layer	IPv6, IPv4, IPSec	IPv6/IP, 6LoWPAN	Network
Link Layer	802.3, 802.11, 802.15.4	802.15.4 MAC/PHY, sicslowpan	RDC/MAC
Physical Layer	Ethernet, DSL, ISDN, WLAN, etc.	CC2420	Radio

Figure 7. Network protocols and layers shared by IoT, Contiki and traditional network [33] [22] [32]

4.2.2 Protocol Layers in IoT and security analysis

Internet of Things conception work with few different protocols. 6LowPAN is relatively new protocol introduced in wireless sensor network (WSNs). It is compressed in IPv6 protocol designed for low powered wireless devices. This protocol is compatible with different IoT devices as these devices share multifaceted structure.

The proposed algorithm is designed considering RPL attacks. As we are dealing with RPL attacks which has no specific mechanism to protect it. We implemented packet relay wormhole attack on the network it is possible to launch an attack through RPL. Wormhole detection mechanism can be categorize hardware based, RTT based and statistical analysis, clock based, etc. As we are dealing with low powered devices hardware mechanism will not be suitable for the implementation. The proposed mechanism is software based as this approach provides flexibility while optimization. We have implemented packet relay wormhole attack. During this type of wormhole attack attacker node performs its malicious activities on radio interface and the packet remain the same but it will be encapsulated. From figure7 we can observe layers present in the Contiki operating system. All the packets to be transmitted gets relayed during unicast, broadcast, etc. This will occur in RDC layer in Contiki operating system. This layer also known as sicslowmac in Contiki. By encapsulating packets at every node this attack creates tunnel in sicslowmac layer. By applying RSSI technique in this layer it will again trace back the attacker node through the tunnel which was created by the attacker node. As most of the RPL attacks requires RDC layer to send and receive DIO (DODAG information object) messages which are based on the DODAG(Destination oriented directed Acyclic Graph) which will be generated by the root. During cryptographic implementation also these attacks works. Due to this kind of behavior of these attacks, there is required implementation which will detect an attack considering energy efficiency. The proposed mechanism will detect an attack through few possibilities. If this mechanism is integrated with software it will send an alert to user, otherwise it will

monitor through the deviation in power consumption. Next section provides detailed description regarding the technological approach.

4.3 Technological Approach: -

In previous section we discussed several aspects about IoT devices and proposed security implementation. This section will provide detailed description of the technological approach about the hardware, software, etc.

4.3.1 Hardware: -

This research mainly directed towards the real-world implementation of the impact of proposed algorithm and behavior of the IoT devices, we considered Zolertia Z1 mote. Zolertia Z1 mote is wireless sensor network device which one of the first or primary generation of the IoT devices. For the experimental setup low power Zolertia Z1 device is being employed. Zolertia Z1 shares the similar architecture as that of the modern IoT devices. It is equipped with Microcontroller MSP430F2617 which is low power microcontroller. In addition to this microcontroller it also consists of CC2420 transreceiver, which operate at 2.4 GHz and follows the IEEE 802.15.4. This transreceiver is also 6LowPAN and Zigbee compliant. This devices is also equipped with few different sensors such as 3- axis gyroscope, ±2/4/8/16 g digital accelerometer which is ADXL345, and a digital temperature sensor TMP102 which provides ± 0.5ºC accuracy. The operating range for this device is 0.3-3.6V, but it can also operate on 1.5V AA batteries [20]. These devices are equipped with 8Kb RAM and 92Kb flash memory [18]. [19]

Figure. 8 Hardware used Zolertia Z1

Experimental setup consists of nine Zolertia Z1 devices. We created the test bed of these nine devices and a new set of batteries were used for each of the experiment. This test bed follows the topology consisting of 15ftX5ft grid of eight motes in which broadcasting and one-to-one communication examples were uploaded. The ninth mote was equipped with power trace example that will track the power consumption of the whole network. This approach was adopted to observe the behavior of the devices with attack and without attack in different operating environment and lighting conditions. The congruent process was followed by converting one of the mote as an attacker and echoed the same approach by implementing mitigation algorithm.

For the purpose of comparison and validation we have to simulate the results. In the next section there will be detailed description used for the simulation using Cooja Contiki. [20] [21]

4.3.2. **Software**: -

Contiki OS is an operating system which designed and developed for IoT devices. It is a very efficient operating system for all low-powered devices such as WSNs or IOT devices. Due limited memory size of these devices this operating system is suitable for these low powered devices and the code size required for the processing is also limited. Kernel, libraries, the set of program loader and some set of processes are required to run the Contiki operating system. User can implement any kind of topology for these device according to the user's requirement. Basically, this operating system supports C

	Traditional Network	***IoT Network***
Application Layer	HTTP, FTP, SMTP,etc.	CoAP, MQTT, XMPP, AMQP
Transport Layer	TCP/UDP	UDP, DTLS
Network Layer	IPv6, IPv4, IPSec	IPv6/IP, 6LoWPAN
Link Layer	802.3, 802.11, 802.15.4	802.15.4 MAC/PHY
Physical Layer	Ethernet, DSL, ISDN, WLAN, etc.	CC2420

Figure 9. Implementation in Regular Network, IoT network and Contiki layer

programming language and it is also compatible with MSP430 microcontroller.

Contiki OS provides drivers for IoT devices. We can observe the protocols in figure 9 which are followed by IoT devices and regular network. Through this figure we can observe all the layer of the network and every detailed protocols required for the communication of these devices and traditional network. Proposed implementation will work on network layer as we are working with 6LowPAN, IPv6 protocols [22] [23] [24].

Contiki OS has the simulator for low powered wireless communication devices. As we are conducting experiments by employing Zolertia Z1 devices. We can run simulation for the same devices adopting any topology which will be suitable for the network. We are simulating all the experiment with the same topology we discussed and used in real-world experiments. We echoed the same procedure in simulation as real-world experiment by uploading broadcasting, unicast or one-to-one examples on eight nodes and for the remaining ninth node we uploaded powertrace example. We simulated results with and without attacks to observe the impact on devices and deviation in power consumption [2] [25].

As we are discussing about the security implementation and its impact on these low powered devices we also simulated results with implementing proposed implementation. These simulated results will help us to compare the results from real-world experiments. As COOJA simulator provided by Contiki OS has many predefined libraries, visualization of the functioning network is possible [20]. As COOJA simulator is optimization friendly, with some optimization it is possible to modify these libraries and make it compatible with chosen device's architecture and any implementation.

In next section, we will discuss and give insights regarding the operating environments chosen for experimental setup.

4.2.3 Operating Environment: -

Interference present in the atmosphere will cause the deviation in the power consumption. Power consumption will change according the change in environment and the lighting conditions. To conduct experiment we chose Parking lot, basketball arena, auditorium and working lab space. In lab space due to the presence electronic equipment there is electrical, magnetic disturbance in the atmosphere [26]. These types of interference will have adverse effect on the communication link between these devices.

Auditorium is also an indoor environment but it has large halogen lights which can create a lot of interference. Also there are several electrical instruments present in an auditorium. With electrical interference there will be an addition of the interference created by the presence large halogen lights power consumption of these devices will also deviate and there will be increase in power consumption. Same with basketball arena as arena has same lighting conditions but with huge lighting setup and electrical equipment they will also create an interference during on-going communication.

Parking lot is an open space, so an interference present will not be limited to only electrical or magnetic interference there also will be an atmospheric interference such as wind, temperature, etc. So there will also be a significant increase in power consumption.

During Indoor experiments we conducted experiments with lights on and lights off to observe the effect of interference on the energy consumption. But for outdoor

experiment conducted experiments were during daylight and nighttime. We also conducted experiments during high temperature and low temperature.

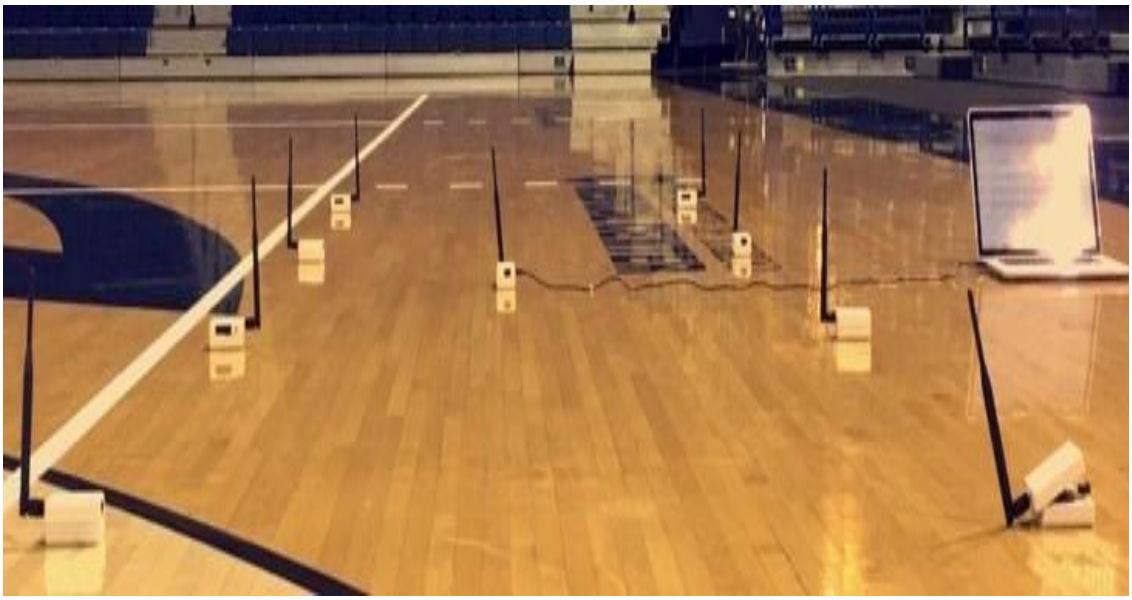


Figure.10 Topology used in real world environment [26]

As simulator does not provide any facility to choose environment and lighting condition, conducting real-world experiments will be the only option for validation of the results. Simulator provides the behavior of these low powered device in an ideal environment, so we cannot rely completely on the results taken from simulator. From figure 9 we can observe the adopted topology during real world experiments.

4.2.4 Experiments Conducted: -

We followed step-by-step approach to conduct all the experiments. As the primary, step we chose Zolertia Z1 as hardware which will be a proper choice for experiments. Then creating an identical topology for all the experiments as we created

testbed of these devices consisting of 15ftX5ft grid [26]. As drivers will be required for these devices to operate. There are several operating system such as Contiki, Tiny OS, [24] etc.

As discussed in previous section we can conclude that Contiki OS will be suitable for the Zolertia Z1 devices which are low powered wireless sensor network devices. According to previously conducted experiments we concluded that interference present in the atmosphere has an adverse effects on-going communication between these nodes. We adopted specific methodology where we deployed these devices in different operating environment such as indoor working lab space, basketball arena, and auditorium. As each

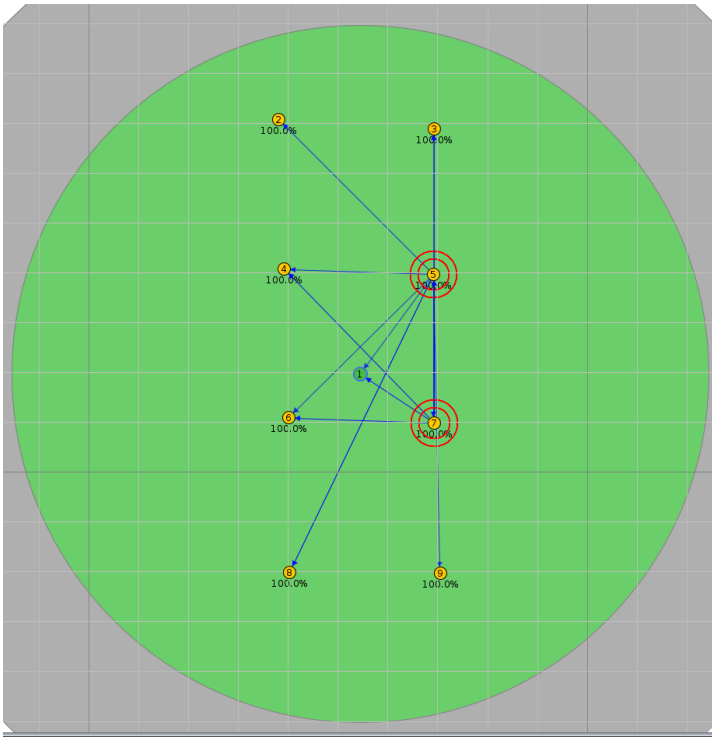


Figure 11. Topology Used during Simulation [26]

of these have adverse effect on the communication between these devices [4]. Examples such as broadcast, unicast and powertrace which are predefined in the Contiki OS, we

uploaded these examples on WSNs we are using and deployed them in different environment and varying lighting conditions.

WSNs we deployed to conduct experiments were equipped with broadcast, unicast and powertrace examples. Primarily we chose broadcast as an example to observer the power consumption without any going on attack. Same procedure was followed for unicast example. Testbed we created for conducting an experiment consists of eight mote in grid we specified previously and the ninth mote will be monitoring the on-going power consumption through power trace example. After the implementation of the attacks the same methodology was echoed and also the same procedure was repeated for the security implementation on these devices. The results we accumulated from these several experiments conducted shows the change in power consumption. As change in power consumption is inversely proportional to the battery life of these devices, battery life estimation of these devices will helpful for the analysis.

Contiki OS has an inbuilt simulator named as COOJA simulator for wireless

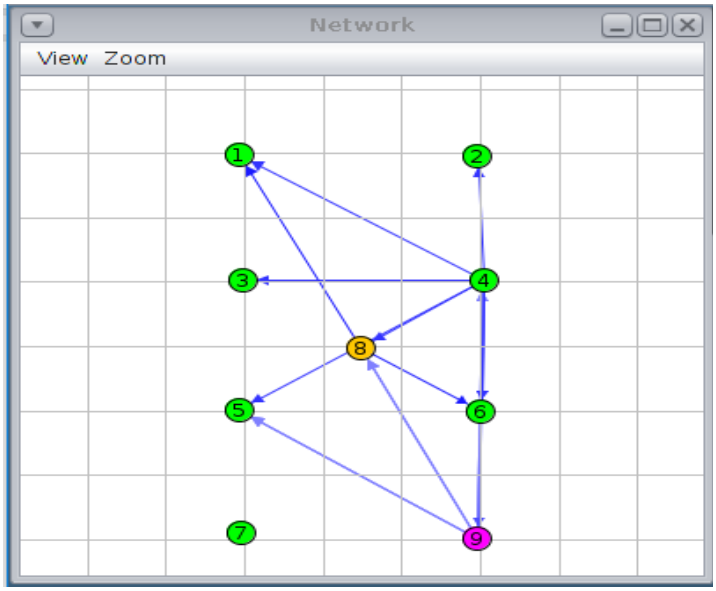


Fig 12. Topology used in simulation during ongoing attack [16]

sensor network devices. Through this simulator it is possible to analyze the behavior of these devices in an ideal environment, as this simulator does not provide any facility to choose operating environment and lighting condition.

We simulated the results with and without attack first and then with implemented IDS or proposed implementation. From figure 11 we can observe the simulation while the attack is going on.

4.3 Chapter Summary: -

Chapter 4 outlines an elaborated information regarding the actual algorithm. In further sub section there is detailed description about the technical approach adopted to conduct the experiments. We elucidated the basis of choosing the different environment, selecting Zolertia Z1 as hardware and Contiki operating system which has an in built simulator named as COOJA simulator

Also we have diagrammatic explanation of the topology used in real world and in simulation. In next section we compared all the result regarding the power consumption analysis and battery life estimation.

Chapter 5

Results and Discussion

This section provides you with the details of the impact of the proposed implementation on these devices through power consumption analysis in different operating environment and battery life estimation.

Table 1. Operating States of Zolertia Z1 [38]

Operating States	**Ratings**	**Unit**
MCU on	18.8	mA
MCU on	17.4	mA
MCU idle	0.1	μA
MCU standby	0.5	μA
Voltage	3.6	V

5.1 Power Consumption Analysis

The primary focus of this research is to enhance the security of IoT devices but these devices are low powered and has constrained resources. The impact analysis of interference present in the atmosphere, any cyber –attack and security implementation is also necessary. To analyze the impact of these implementations we are conducting several experiments and presenting the data or the results regarding the power consumption analysis and battery life estimation of these devices. As after the implementation cyber-attack mitigation algorithm the analysis of the resource consumption is necessary otherwise this implementation itself will be harmful without any analysis. As described in previous sections power consumption is directly proportional to the battery life. So more the power consumption, more the battery life and this will be harmful for the whole network.

To monitor the on-going power consumption we are using powertrace example which is predefined in the Contiki OS. Powertrace example will be helpful to evaluate the efficiency of the algorithm in terms of the resource consumption. This code will provide with the accurate data regarding the power consumption of the whole network. The calculation of the energy consumption is possible with the standard equation and parameters from the figure are considered for the accurate calculation [26],

$$Energy(mJ) = \frac{CPU * 0.5 + LPM * 0.0005 + Tx * 17.4 + Rx * 18.8) * 3}{32768}$$

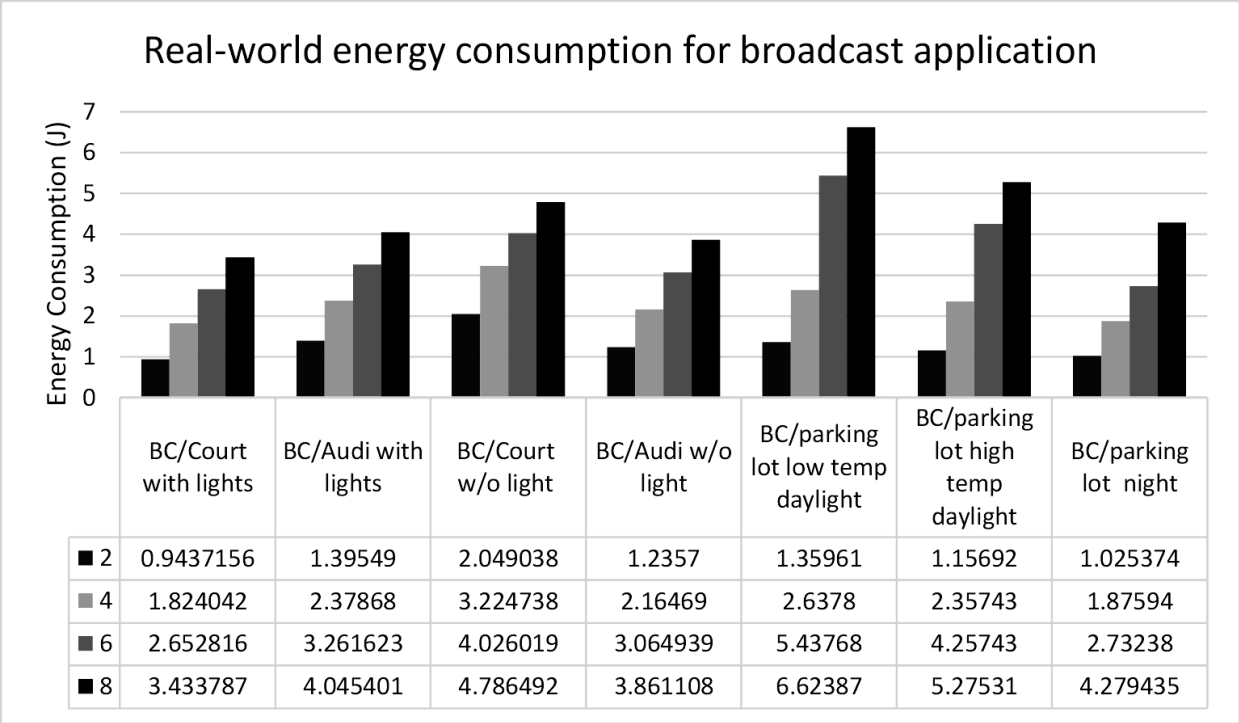
Where,

CPU = Time for which mote was active,

LPM = Total Time for the active low power mode,

Tx = Total transmission time,

Rx = Total listening time,



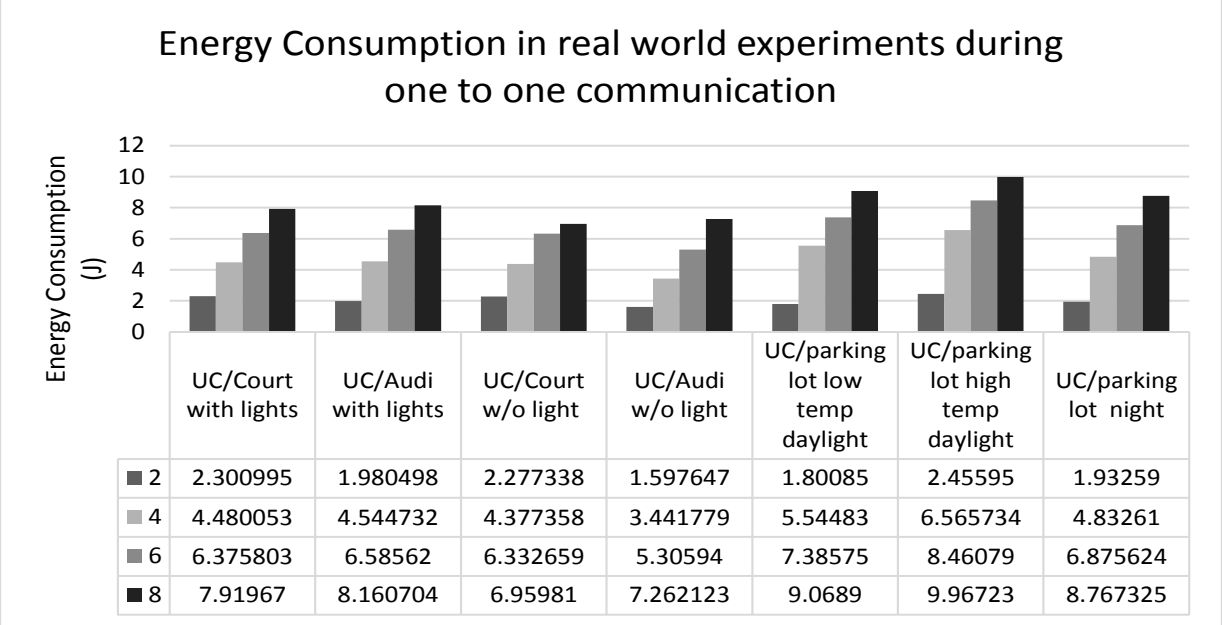
	BC/Court with lights	BC/Audi with lights	BC/Court w/o light	BC/Audi w/o light	BC/parking lot low temp daylight	BC/parking lot high temp daylight	BC/parking lot night
2	0.9437156	1.39549	2.049038	1.2357	1.35961	1.15692	1.025374
4	1.824042	2.37868	3.224738	2.16469	2.6378	2.35743	1.87594
6	2.652816	3.261623	4.026019	3.064939	5.43768	4.25743	2.73238
8	3.433787	4.045401	4.786492	3.861108	6.62387	5.27531	4.279435

Figure 13. Real-world energy consumption for broadcast application [16]

In this section we are presenting result for topology we discussed in previous sections without attack in different operating environment, lighting conditions and several different examples such as broadcast, unicast or one-to-one communication and powertrace to monitor the on-going energy consumption.

According to the discussion in the previous sections, we use nine Zolertia Z1 devices to conduct an experiment. A broadcast example code was implemented on eight of the nine devices. This broadcast program sends eight byte packet during on-going communication. Powertrace example was uploaded on the ninth mote to monitor the power consumption of the traffic flow the whole network. [15] From the figure we can

observe the deviation in energy or power consumption with change in the number of devices. As discussed earlier we have used broadcast example for the communication purpose. This example sends and receive eight byte packets from all the nodes in the network. Through this figure we can compare energy consumption in different operating environment and different lighting conditions. If we observe this figure, we can notice the significant change in energy consumption during on-going communication with change in number of nodes that is from two to eight nodes. Energy consumption will be higher when all the eight nodes are involved in the communication and as we reduce the number of nodes energy consumption will also get reduced. From the above figure we can conclude that the energy consumption 3.5 times greater compared to the two nodes in the



	UC/Court with lights	UC/Audi with lights	UC/Court w/o light	UC/Audi w/o light	UC/parking lot low temp daylight	UC/parking lot high temp daylight	UC/parking lot night
2	2.300995	1.980498	2.277338	1.597647	1.80085	2.45595	1.93259
4	4.480053	4.544732	4.377358	3.441779	5.54483	6.565734	4.83261
6	6.375803	6.58562	6.332659	5.30594	7.38575	8.46079	6.875624
8	7.91967	8.160704	6.95981	7.262123	9.0689	9.96723	8.767325

Figure 14. Energy consumption during real-world for one-to-one communication [16]

network.

During one-to-one communication, we use the same set of Zolertia Z1 devices but with brand new 1.5V standard AA batteries. We echoed the similar procedure we used

during broadcast example. One-to-one example was uploaded on eight nodes and the remaining ninth node was equipped with powertrace example to observe the power consumption of the devices. We can observe the same phenomenon that the energy consumption we higher when eight nodes were involved and it was reduced as we reduced the number of devices. From this figure 14 we can observe that at the primarily power consumption was less. But as we proceeded in the experiment we can notice the significant change in the power consumption as during experiment conducted in

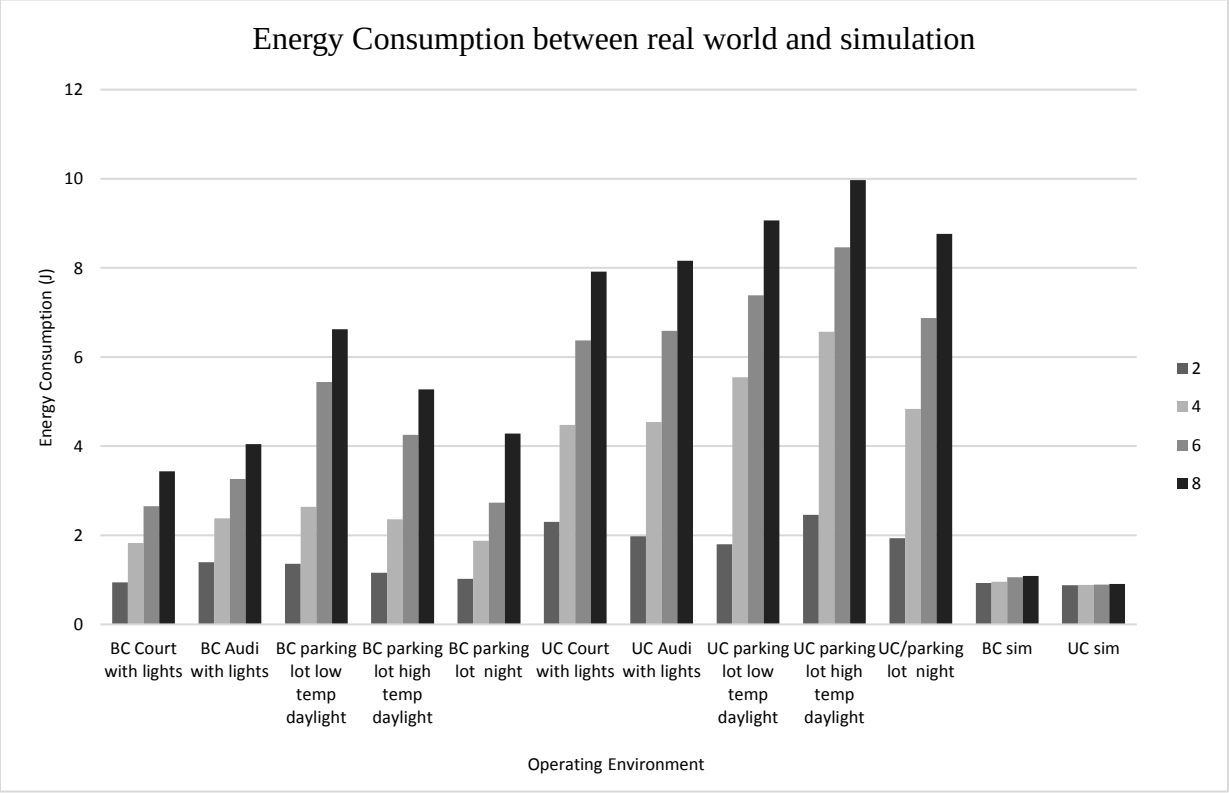


Figure 15. Energy consumption comparison between various real-world scenarios and simulation results [16]

auditorium, increase in power consumption has been observed compared to basketball arena. This significant change is due to the interference from the huge halogen lights.

Similarly we can notice that lower the temperature of the atmosphere, greater is the interference present in the atmosphere.

If we compare both the figures 14 and 15 presented data can be analyzed and can be concluded that one to one communication requires more energy compared to broadcast. This is possible due to the fact that every devices involved in the network has to establish the communication with every other device. Resulting increase in power consumption of the whole network during one to one communication.

Above figure represents the results from the real-world experiments and simulated through COOJA simulator. From this figure it is obvious that in simulation broadcast requires more energy compared to one to one communication. Contrary to simulation the real world experiments show drastic difference in results. As simulator provides an ideal environment for the operation of the network of these devices and in real world communication gets affected because of interference present in the atmosphere. Through our analysis it is clear that simulation results are not reliable all the time due to absence of path loss, interferences and some other parameters.

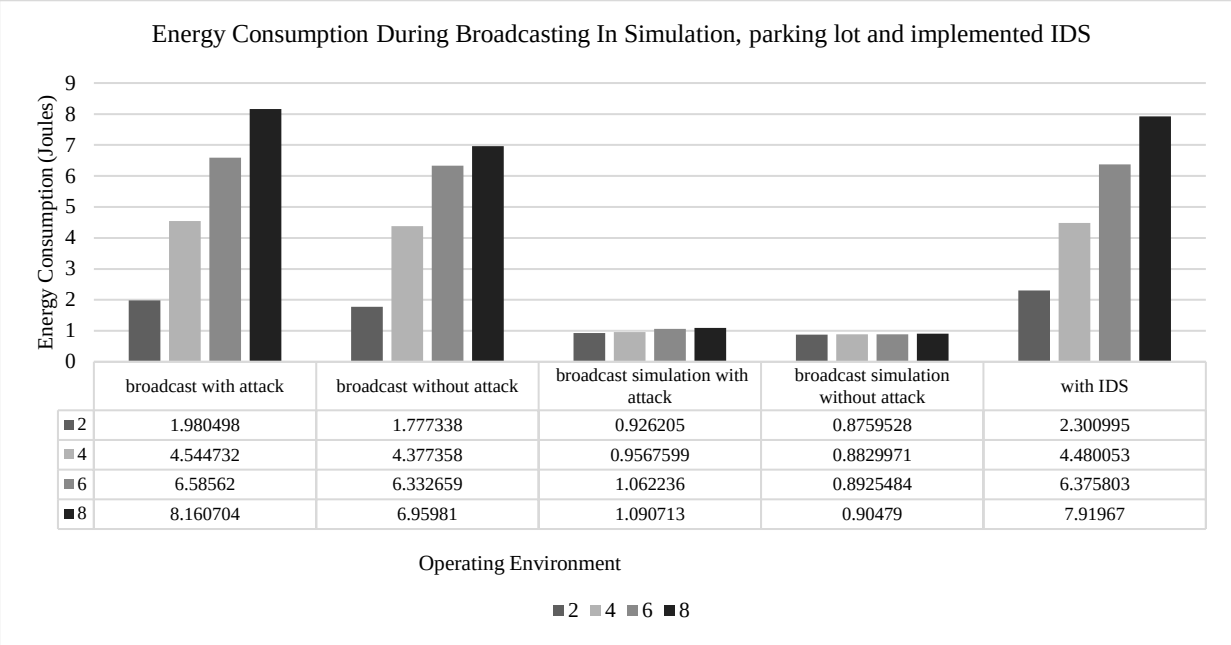


Figure 16. Energy Consumption during broadcasting in Simulation and working lab space [16]

As previously discussed this research mainly focused on security enhancement of these devices

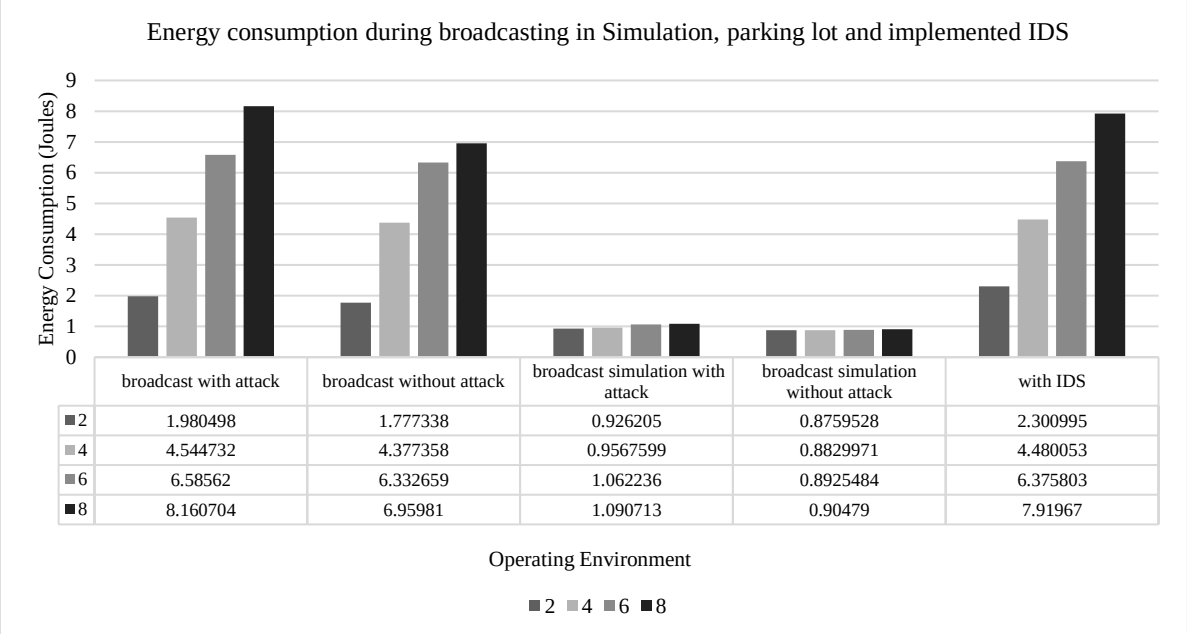
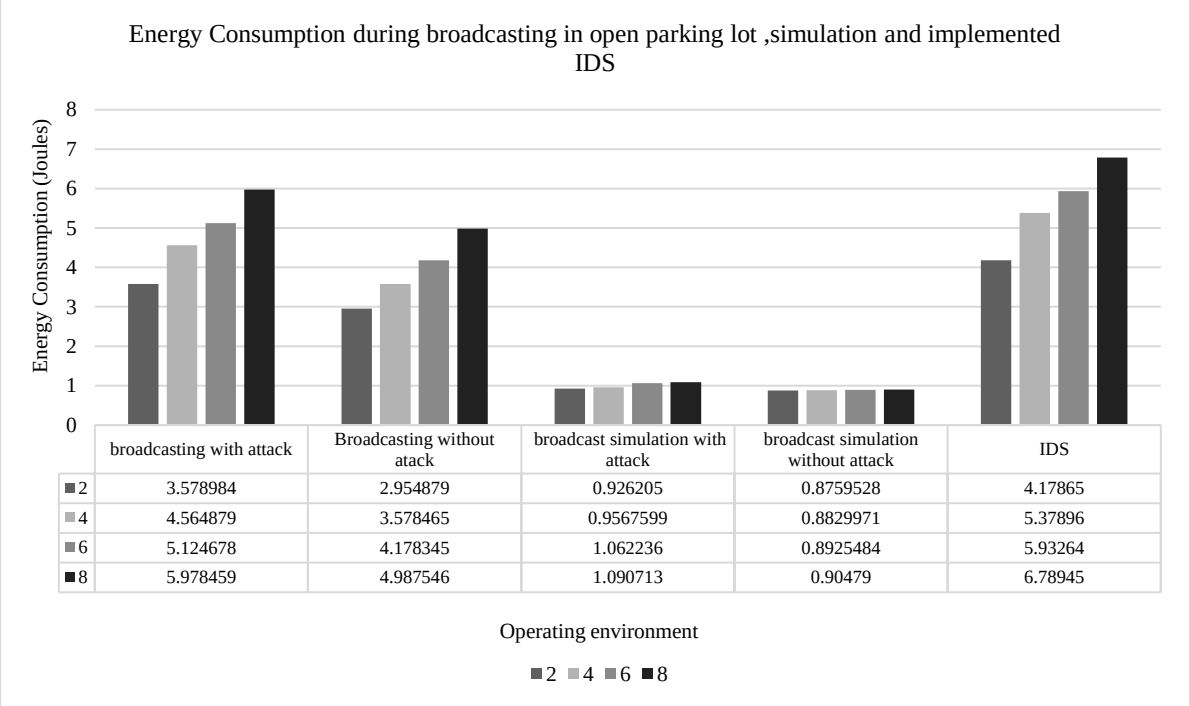


Figure 17. Energy Consumption During One to One communication in Simulation and lab space [16]

After analyzing the effects of the interference during broadcast and one to one communication, further we are presenting the results which we accumulated after implementing attacks and security implementation.

From the figure15 we can compare the energy consumption during broadcasting in simulation and in working lab space with and without attack and also an implemented IDS or cyber-attack mitigation algorithm. As we observed previously, the energy consumption increases with the increase in the number of nodes. Also there is significant change in energy consumption with an attack going on in the network compared to the network without attack. Also similar trend can be observed in simulation. Through figure 16 it is possible to observe that after the implementation of IDS there is no noticeable change in the energy consumption. The energy consumption results we are presenting

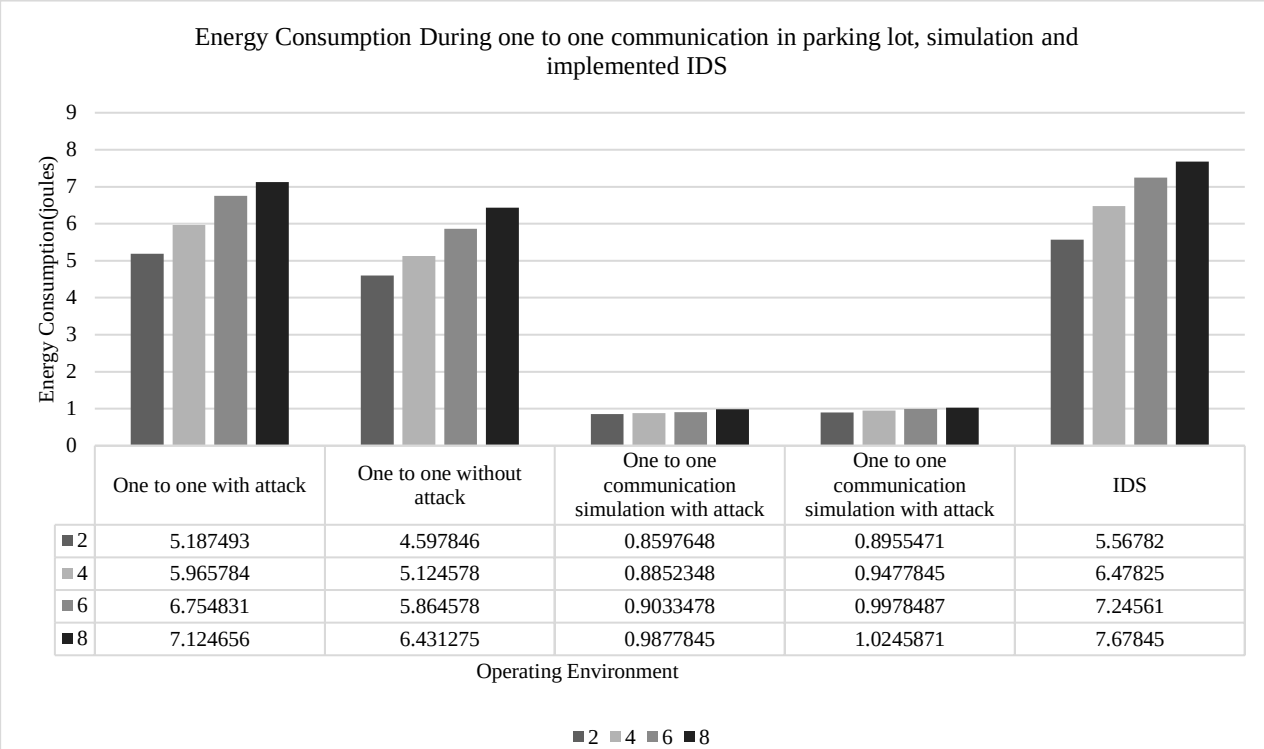


	broadcasting with attack	Broadcasting without atack	broadcast simulation with attack	broadcast simulation without attack	IDS
2	3.578984	2.954879	0.926205	0.8759528	4.17865
4	4.564879	3.578465	0.9567599	0.8829971	5.37896
6	5.124678	4.178345	1.062236	0.8925484	5.93264
8	5.978459	4.987546	1.090713	0.90479	6.78945

Figure 18. Energy Consumption during broadcasting in open parking lot and simulation [16]

also consists of interference present in the lab environment such as electrical interference and magnetic interference.

Figure 17 represents the results accumulated during one to one communication in simulation and in working lab space. It is possible to compare energy consumption between simulation and real world experiments which is experiment conducted in



	One to one with attack	One to one without attack	One to one communication simulation with attack	One to one communication simulation with attack	IDS
2	5.187493	4.597846	0.8597648	0.8955471	5.56782
4	5.965784	5.124578	0.8852348	0.9477845	6.47825
6	6.754831	5.864578	0.9033478	0.9978487	7.24561
8	7.124656	6.431275	0.9877845	1.0245871	7.67845

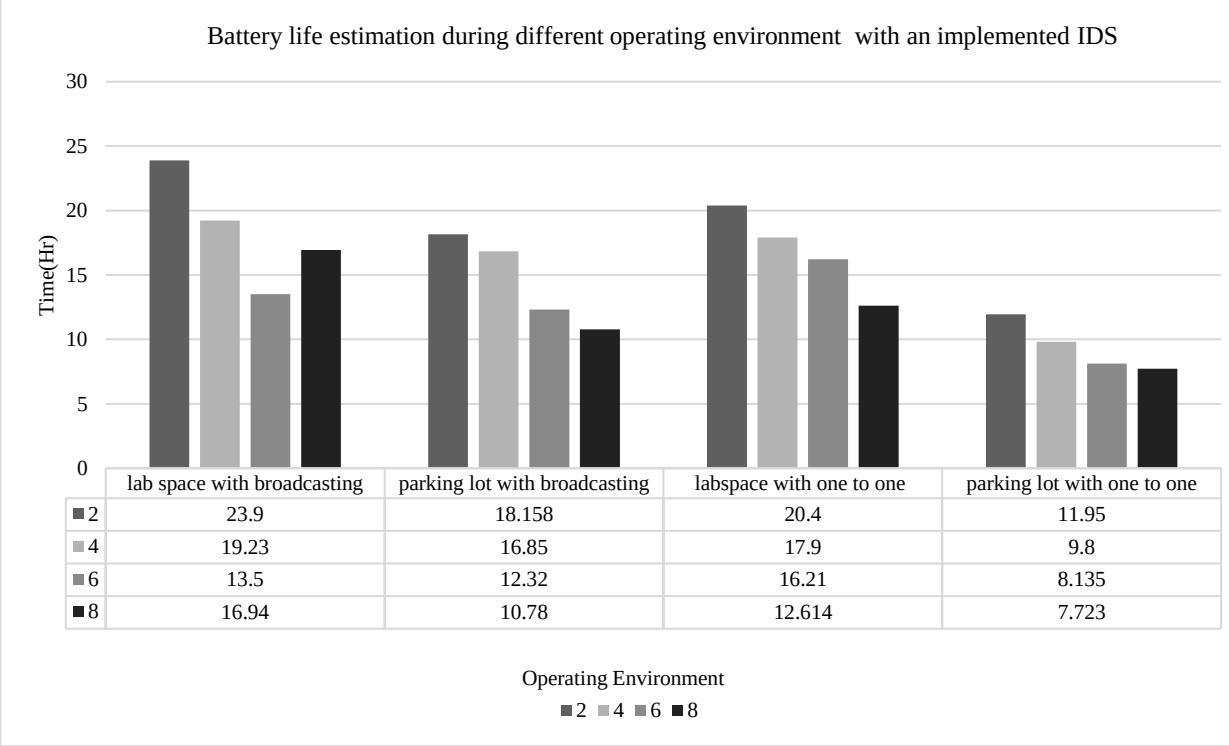
Figure 19. Energy Consumption during one-to-one communication in parking lot and simulation [16]

working lab space. Results represented in this figure shares similar trend as we have noticed during broadcast communication. But by comparing figures 17 and 18 we can again conclude that in real world experiments one to one communication requires more energy compared to broadcasting unlike simulation results.

From figure 17 and 18 we can analyze the results during broadcasting and one to one communication in parking lot and simulation. We can simultaneously analyze those results for the interference present and the effects of ongoing attack and implemented IDS. As we are considering open parking lot as an environment for the experiment, the results presented consist the effects of atmospheric interference such as wind, temperature, etc. Again similar pattern was observed for the both the figure during real world experiment s and simulation. As in simulation one to one communication requires less energy compared to broadcasting. But contrary to that we can observe that during real world experiments one to one communication requires more energy.

During our power consumption analysis we can observe that with attack going in all the experiments there in noticeable increase in the power consumption compared to that of the results we accumulated during communication going on without any attack. As the purpose of the research is to analyze the impact of security implementation with attacks going on, we can observe that there is no significant increase in the power consumption during all the conducted experiments.

As discussed earlier power consumption is inversely proportional to battery life of the devices, in the next section there will in-depth analysis of the battery life estimation of wireless sensor network devices. Power consumption analysis provides the basis for the battery life estimation.



	lab space with broadcasting	parking lot with broadcasting	labspace with one to one	parking lot with one to one
2	23.9	18.158	20.4	11.95
4	19.23	16.85	17.9	9.8
6	13.5	12.32	16.21	8.135
8	16.94	10.78	12.614	7.723

Figure 20. Average battery life estimation [16]

5.2 Battery Life Estimation

Previous section provide us the basis for the battery life estimation through power consumption analysis. As per our research we can conclude that interference has an adverse effect on the communication of these low powered wireless network sensor devices. We calculate the battery life in hours with the help of following equation (2):-

$$E = \sum_{i=0}^{n} Vi * Ii * Ti$$

Where,

E = Energy in Joules; I = Current drawn; T = Time; V = Voltage required,

From figure 19 we notice and get the exact idea of the battery life estimation with implemented IDS and ongoing attacks. Generally during broadcasting with implemented IDS we can observe that the battery life of these devices is more compared to one to one communication with an implemented IDS. We can again notice the same pattern as the lesser the number of node greater the battery life of the devices. So, from all the conducted experiments we can conclude that there is no significant energy change while IDS was implemented but during broadcasting and implemented IDS the energy consumption is less compared to one to one communication.

5.3 Discussion

We conducted several experiments considering different environments and lighting conditions to observe the effects of interference on communication of wireless sensor network devices primarily. The approach of this research is such the firstly we observe the effect of the interference without any attack and any implementation. After the observation of these effects, attacks were implemented with intrusion detection system to observer the impact of these attacks and security implementation on these devices. We concluded that considering all the parameters the proposed implementation is efficient for the selected device. Also our experiment proved that the simulated results are not always reliable as these IoT devices are nowadays are being used for medical

health monitoring, home automation systems. To validate any data or any improvement real-world validation is required for these low powered devices.

Chapter 6

Conclusion and future work

Internet of Things devices or IoT devices are becoming prevalent in many fields. Before we employ these devices for several different and crucial applications such as health monitoring, military application, area monitoring, etc. an efficient security implementation is required. These implementations should have efficiency considering the resource consumption and enhancing the network security. In this research we analyzed an impact of the proposed IDS or intrusion detection system considering different operating environment and simulation. As we have concluded previously for the results that simulated results are not reliable all the time. We required more research regarding our cyber-attack mitigation algorithm to provide security for these IoT devices and also to provide energy efficient encryption.

Hence, there is requirement of an efficient algorithm based on our proposed IDS considering the absence of security implementation and detection mechanisms. According to our analysis we still required more research considering the proposed algorithm as to develop its generalized version as we have targeted only Zolertia Z1 device. With more research and iteration it is possible to enhance the security of these

devices which will be more efficient considering constrained resources of these low powered IoT devices.

6.1 Publications

List of Publications are as follows: -

- A. Kotian, A. Y. Javaid and A. M. Bandekar, ""Comparative Analysis of Simulation and Real-world Energy Consumption for Battery-life Estimation of low-power IoT deployment in Varying Indoor Lighting Conditions using Zolertia Z1 motes," in *7th EAI International Conference on Sensor Systems and Software*, Nice, France,, 2016.
- A. M. Bandekar and A. Y. Javaid, "Cyber-attack Mitigation and Impact Analysis," in *IEEE Cyber-2017*, Hawaii, 2017.

References

[1] P. Pongle and G. Chavan, "Real Time Intrusion and Wormhole Attack Detection in Internet of Things(IoT)," *International Journal of Computer Applications,* July 2015.

[2] "Wikipedia/wirless sensor network," [Online]. Available: https://en.wikipedia.org/wiki/Wireless_sensor_network. [Accessed 20 july 2017].

[3] A. M. Bandekar and A. Y. Javaid, "Cyber-attack Mitigation and Impact Analysis," in *IEEE Cyber-2017*, Hawaii, 2017.

[4] A. Kotian, A. Y. Javaid and A. M. Bandekar, ""Comparative Analysis of Simulation and Real-world Energy Consumption for Battery-life Estimation of low-power IoT deployment in Varying Indoor Lighting Conditions using Zolertia Z1 motes," in *7th EAI International Conference on Sensor Systems and Software*, Nice, France,, 2016.

[5] G. Anastasi, A. Falchi, A. Passarella, M. Conti and E. Gregori, "Performance Measurements of Motes Sensor Networks," *ACM MSWiM,* pp. 174-181, 2004.

[6] S. Al-Janabi, A.-J. Samaher , I. Al-Shourbaji, M. Shojafar and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area network".

[7] "businessinsider," [Online]. Available: http://www.businessinsider.com/internet-of-things-survey-and-statistics-2015-1. [Accessed 20 july 2017].

[8] "Wikipedia/ Internet of Things," [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things. [Accessed 20 july 2017].

[9] 3 March 2017. [Online]. Available: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WMkZHBsrKUk.

[10] "http://dyn.com/," [Online]. Available: http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/. [Accessed 11 May 2017].

[11] "forbes," [Online]. Available: https://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home/#5c28d42bb859. [Accessed 20 july 2017].

[12] "technewsworld," [Online]. Available: http://www.technewsworld.com/story/83969.html. [Accessed 20 July 2017].

[13] "wired," [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[14] S. Ruben , K. Aerts, M. Nele, D. Singelee and A. , "A cryptographic key management architecture for dynamic 6LowPan networks".

[15] G. De Meulenaer, F. Gosset and F.-X. Standaert, "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks," 2008.

[16] S. Guicheng and Y. Zhen, "Application of Elliptic Curve Cryptography in Node Authentication of Internet of Things," 2013.

[17] K. Piotrowski, P. Langendoerfer and S. Peter, "How Public Key Cryptography Influences Wireless Sensor," 2006.

[18] J. Borgeson, S. Schauer and H. Diewald, "Benchmarking MCU power consumption for ultra-low-power applications," Texas Instruments, Nov 2012.

[19] T. Zhang and X. Li, "Evaluating and Analyzing the Performance of RPL in Contiki.," *MCSS '14 first international workshop on Mobile sensing, computing and communication,* pp. 19-24, 2014.

[20] Advancare, "Zolertia Z1 Datasheet," March 2010. [Online]. Available: http://zolertia.sourceforge.net/wiki/images/e/e8/Z1_RevC_Datasheet.pdf. [Accessed 16 September 2016].

[21] "http://zolertia.sourceforge.net," [Online]. Available: http://zolertia.sourceforge.net/wiki/images/e/e8/Z1_RevC_Datasheet.pdf. [Accessed 10 May 2017].

[22] K. Roussel, Y. Song and O. Zendra, "Using Cooja for WSN Simulations: Some New Uses and Limits," in *International Conference on Embedded Wireless Systems and Network - EWSN '16*, Feb 2016.

[23] A. Sehgal, "Using the Contiki Cooja Simulator," Oct 2013.

[24] T. Tsvetkov, "RPL: IPv6 Routing Protocol for Low Power and Lossy Networks," 2011.

[25] Q. M, A. H, Y. M. B and A.-D. A, "Performance Evaluation of RPL Objective Functions," in *IEEE International Conference on Computer and Information*

Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015.

[26] Contiki, "Contiki: The Open Source OS for the Internet of Things," Contiki, 2002. [Online]. Available: http://www.contiki-os.org/index.html. [Accessed 18 September 2016].

[27] A. Dunkels, J. Eriksson, N. Finne and T. Tsiftes, "Powertrace: NetworkLevel Power Profiling for Low-Power Wireless Networks," 2011.