IOT DATA ENCRYPTION ALGORITHM FOR SECURITY

MARWAN KANAAN ISMAEL

A thesis submitted in
fulfilment of the requirement for the award of the
Degree Master of Electrical and Electronic Engineering
With Honours

Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

JANUARY 2020

ACKNOWLEDGEMENT

In the Name of **Allah**, The Most Merciful. The completion of this study was not possible without His blessings. Thank you for guiding me all the way around this time.

My appreciation and sincere thanks I bid to my supervisor, **Dr. DANIAL BIN MD.NOR** for her direction, advice and support throughout this study. Her understanding and personal guidance have provided a good basis for this research. Her detailed and constructive comments along with her professionalism motivate me to withstand throughout the journey of this study. Many thanks to my committee members (**Dr. NORFAIZA BINTI FUAD and TS.Dr.MOHD NORZALI BIN HJ MOHD** and **PROF.Dr. NOORSALIZA BINTI ABDULLAH**) for their helpful comments and careful review of this work.

I would also like to express sincere gratitude for my father, for his kind support and motivations during the period of completing this journey. Not forgetting my mother , who have always been patient with me during this period. They have understood me so much and they sacrifice their time with me especially when I am not at home even on holidays in order to finish this study. Without their prayers and advices, I would not be where I am today.

The writing of the thesis had been the most challenging task of my life to date. I could not have completed this work without the support and help of many people. I would also like to convey thanks to Universiti Tun Hussein Onn Malaysia for providing the laboratory facilities and my teachers

DEDICATION

To My Beloved Dad, Mr. kanaan ismael

To my mum

My brothers

My lectures and all my friends

Especially my supervisor, Dr. danial bin md.nor

For giving me support and showing faith in me.

Love you always.

I could have never done it without you

ABSTRACT

This research project is about encryption simulation for IoT data. It is important to enhance the security system when sending and receiving the IoT data. Some of these data, especially the health information for a particular person is very sensitive. Therefore, there is a need to encrypt and protect the data from malicious attack. The technique proposed in this research is using Hash function and encryption method to protect the data. To show the working of the encryption, a simulation is performed. The simulation used is a MATLAB coding. By inserting the number of bit and size of the data with random plain text, the system is able to encrypt the data. The simulation results showing that the encrypted data is completely different from the original data or the data haven't encrypted. Upon encrypted, the data being protected and will be unknown to the malicious. At the end of this research project, the result concluded that the waveforms will show the encryption process.

ABSTRAK

Projek penyelidikan ini adalah mengenai simulasi penyulitan untuk data IoT. Adalah penting untuk meningkatkan sistem keselamatan semasa menghantar dan menerima data IoT. Sebahagian daripada data ini, terutamanya maklumat kesihatan untuk orang tertentu sangat sensitif. Oleh itu, terdapat keperluan untuk menyulitkan dan melindungi data daripada serangan berniat jahat. Teknik yang dicadangkan dalam kajian ini menggunakan fungsi Hash dan kaedah penyulitan untuk melindungi data. Untuk menunjukkan kerja penyulitan, simulasi dilakukan. Simulasi yang digunakan adalah pengekodan MATLAB. Dengan memasukkan bilangan bit dan saiz data dengan teks kosong secara rawak, sistem dapat menyulitkan data. Hasil simulasi menunjukkan bahawa data yang disulik adalah sama sekali berbeza daripada data asal atau data yang tidak disulitkan. Apabila disulitkan, data yang dilindungi dan tidak diketahui oleh yang berniat jahat. Pada akhir projek penyelidikan ini, hasilnya menyimpulkan bahawa bentuk gelombang akan menunjukkan proses penyulitan.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

IOT	-	Internet of things
HAN	-	Home area network
CDMA	-	Coding division multiple access
AFH	-	Adaptive frequency hopping
WLAN	-	Wireless local area network
WSN	-	Wireless sensor network
BPSK	-	Binary phase shift keying
FH	-	Frequency hopping
Sd (t)	-	Modified BPSK with FH
A	-	Amplitude of the BPSK
FO	-	The base frequency
bi	-	Binary data
Di	-	Tip speed ratio
T	-	Bit duration
FHSS	-	Frequency hopping with spread spectrum
WCDMA	-	Wide code division multiple assess
LO	-	Local oscillator
WAN	-	WIDE AREA NETWORK
PID	-	Proportional intergrader and differentiator technique
AI	-	Artificial intelligent

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background of study

IOT security is important to prevent malicious attack. The malicious is a third party data destroyer who send a harmful packet that can destroy the data in a communication. The cause of malicious attack are [1].

- Data is unable receive by the recipients
- Data being delayed or block when trying to enter into the network
- Data flows is slow in the network

There are quite a number of solutions proposed to enhance the network security to avoid the malicious attack. Each solution proposed is unique to overcome the problem of malicious attack. However, the latest research is about the block-chain technology to enhance the network security. Other security scheme like frequency hopping also employed until today. This is because this scheme still found useful to avoid the malicious attack [2].

For HAN (Home Area Network) system using IoT, the network is small. Typical size will be around 100 m x 100 m. The network consists of wireless sensors, hot spot access point and other wireless communication devices. The HAN system is for future smart house where all the devices can be access remotely from far distance [3].

Because all the devices forming the HAN and they communicate to each other, so there is a need of security to protect the data flows in the network. HAN uses very low data rate and typical communication will use IPv6 (refers to IOT network). The network can be expanded if the number of devices are increase [4].

Since the HAN is not a big network, therefore encryption is proposed in to enhance the security. The proposed of encryption is to avoid malicious attack. It is believed that malicious often using some sort of frequency to detect the wireless data and hence jam the data transmission or locked into the system in order to destroy the data. By using encryption scheme, the network data will add with secrete code [5].

There are two transparent security systems that can be observed in the encryption system that based on CDMA. One is CDMA itself and second is frequency hopping. The CDMA generates random codes where it helps to protect the data. These codes are embedded into the data frame and will be extracted at the receiver when the receiver successfully recognize the data. The frequency hopping on the other hand provide randomly switches the carrier frequency in order to avoid the malicious attack and avoid other user who uses the same frequency. In the research, it is found that the tendency of frequency hopping scheme generates the frequency, which is similar to other user is very low or it can be said that it never happen or hardly to happen. Therefore, it is safe to use frequency hopping in the wireless communication to enhance the security system [6].

For this research, in order to show the encryption of CDMA scheme plays an important role to enhance the security system, MATLAB is used. [7].

MATLAB coding will be used to presents the CDMA coding. It is also used to present the waveform of CDMA and show how the CDMA randomly generates code to secure the communication. The core function of the MATLAB is to show the random pseudo code that embedded into the data frame signals [8].

Apart from showing the CDMA system, the MATLAB also will be used to present how the data can be extracted from the data frame. Again, this presentation of data extraction can be done by showing the waveform. All the demonstration parts in the MATLAB is using programming coding [9] [10][11].

.

1.2 Problem statement

For HAN (Home Area Network) system using IoT, the network is small. Typical size will be around 100 m x 100 m. The network consists of wireless sensors, hot spot access point and other wireless communication devices. The HAN system is for future smart house where all the devices can be access remotely from far distance [3].

Because all the devices forming the HAN and they communicate to each other, so there is a need of security to protect the data flows in the network. HAN uses very low data rate and typical communication will use IPv6 (refers to IOT network). The network can be expanded if the number of devices are increase [4].

Since the HAN is not a big network, therefore encryption is proposed in to enhance the security. The proposed of encryption is to avoid malicious attack. It is believed that malicious often using some sort of frequency to detect the wireless data and hence jam the data transmission or locked into the system in order to destroy the data. By using encryption scheme, the network data will add with secrete code [5].

1.3 Objectives

The main objectives of the research are:

i. To design and develop an IOT security system using encryption method
ii. To simulate the data for encryption an de-encryption to show data being protected and recovered when the noise is present.
iii. To analyse the model proposed IOT security system model.

The objective i refers to the security enhancement on the IoT data. This objective mainly focus on technical design and implementation of encryption system.

The objective ii refers to use the simulation or software to implement the encryption system. This objective will demonstrate how the data being encrypted and how it recovered at the receiver.

Objective iii will focus on analysis of the results, especially on the data waveform. This objective explain the data waveform before and after encryption.

1.4 Scope of study

The scope of the research will cover the following topics:

i. The encryption process for CDMA.
ii. The CDMA coding for HAN.
iii. The modulation environment and program use MATLAB.
iv. To design the encryption CDMA using MATLAB.

The most challenging part is not the theories about CDMA and encryption scheme, but is the software implementation of the system. This is because learning the MATLAB is not easy. The coding must write according to the equations of encryptions and test the coding to check the errors. This may incur many programming learning, therefore more time will be spend to learn the MATLAB.

The suggested tool to develop the CDMA encryption scheme are coding and run the coding in the command prompt of MATLAB to see the outcomes.

Research Problems

The research problems are:

i. How to protect data for IOT system.
ii. To identify input parameter for encryption in de-encryption.
iii. How to module in simulate the data encryption in IOT.

1.5 Overview of Thesis Arrangement

This report consists of five chapters. These chapters are introduction, literature review, methodology, results discussion and conclusion recommendation.

Chapter one is an introduction. This chapter introduces overall idea about the CDMA encryption scheme and how it helps to protect the user data in a wireless network HAN using IOT. The chapter also shows the objective, problem statements as well as the scope of the research.

Chapter two will present the theories about the encryption and other related research topics. The chapter will split the discussion between two. One is CDMA and second is data encryption. Many related researches where they had published will be presented in this chapter.

Chapter three will present the methodology of implementing the encryption scheme. This chapter will show the usage of MATLAB. The design flowchart and the programming coding will be presented in this chapter.

Chapter four will show the results and discussion. This chapter discuss the outcomes after running the simulation.

Chapter five presents the conclusion and recommendation. This chapter concludes the works done in the research summarize the important points about the data encryption against the malicious attack. The chapter also presents some of the suggested ideas to further improve the research.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents the reviews on theories of malicious attack in a network and how it happens. The chapter also presents few types of malicious which can hurt the user's computer. The computer protection schemes like antivirus and also the network protection systems also will be introduced in this chapter. The frequency hopping and its concept used to prevent the attack from the malicious will discuss in detail in this chapter. Finally, the chapter will end with few research papers that are used as references and support for this project.

2.2 Introduction to Harmful Malicious

Computer viruses and worms nowadays everywhere. They are exists in the network and created by computer hackers. The computer viruses and worms can hurt the computers and damage the hardware if the viruses and worms are programmed in that way. Today, the computer viruses and worms are designed based on the purposes of attack. The virus can direct destroy the computer or sending more advertisements to disturb the user's works [13].

In this century, most of the virus are belong to advertisement types. They advertise a fake company, release a fake information and serves two purposes. One is disturb the user's works and second is auto save the user credit card number and make illegal transaction.

In general, the malicious could be a virus or a worm. They are bad commands in programming. When computer executes these commands, the computer will goes into unstable mode and turn into troubles. Apart from worms and viruses, other malicious could be Trojan, hybrids or exotic, ransom ware, file less malware, adware and spyware. All these can be send through wireless or wired in a network [14].

A Trojan is a harmful executable program that normally executed by victim or receiver. This program usually reach the user computer via email or some pages that already infected by Trojan but user goes to visit the pages. Some Trojans can create a fake antivirus system and inform the user that his or her computer is affected by viruses. User will be baited and Trojan will root into the system. According to the virus researchers, Trojans can be stay longer in the network and it has no time limit. It is very hard to clean the network that contents Trojan. From time to time, the Trojan can infect the computers and hence it causes the following symptoms [15].

1. Computer slowdown in operation.
2. There are a lot of fake antivirus software appears on the desktop and disturb the user operation.
3. User files will be stolen and deleted.
4. The computer files become messy.
5. The browser will look different and hence limit the information searched by a user

The hybrid and exotic are the viruses that attack the rootkits or stealth programs. They can modify the content in the rootkits and this causes the software run unsmooth and cannot open at all.

The hybrid and exotic same like Trojan and they can be downloaded without knowing by computer user. This usually happen when user visited the infected websites or download a program that already infected by hybrid and exotic.

The great thing about hybrid and exotic is, they can duplicate themselves and make more and more in the network. Some of the firewalls can block them and some could not block them.

Ransomware is malware and it also a type of Trojan. This type of malware can prevent the user access into their file and make the file unable to open. Even user has successfully open, the contents in the file turned into other characters and letters which human could not understand.

Some ransomware can generates a message to get the payment from the user. User only can open his or her file once the payment is done. In fact, the payment is a fake. It is actually pay to the third party where it is not related to rescue the file.

Ransomware same like Trojan appears in the network for long time. It can be growth larger and larger when the user duplicate the infected files or sending the files over the internet network. The most commonly seen program that can infected by the ransomware is the websites and files that attached into email. Sometimes, the links send by people could also content ransomware. When user click on it, there is message pop up and guiding user to access into other pages. The moment user click and response to the message, then user's computer will infected by the ransomware immediately.

Ransomware also like Trojan where it can appears the fake antivirus software. This can cause user confuse and make payment to the third party in order to get a copy of antivirus software.

Another type of malware called file less malware. This malware not like other malware where they attack the file systems in the computer. The fileless malware does not attack the files of the computer, but it attack none files inside the computer like registry keys, scheduled task and memory. When filesless malware attack, it can causes the computer hang or suspend the operation. For example, if a registry keys are attacked, window cannot run and suspend the program.

Fileless malware is very hard to detect as the malware itself not appearing in the file system. Therefore, the firewall and antivirus software must be enhanced to detect such malware.

The most recent types of malware is called adware. This is a very annoying type of malware and until today, it adware still appears. The appearances not only in the computer but also in the Android smart phones.

Adware is about the advertisement virus. This virus uses other company brand to make advertisement and collect the transactions. Many user being baited due to the page pop up or appears in the desktop when it ask about the payment and solving the computer problems [16].

Adware can makes an advertisement really looks like a professional and legal advertisement. If user not aware on it, he or she might think this is a true advertisement and is secure to make a transaction.

Today, the adware infect the Android phone. They uses the company name like Alibaba, Shopee, Lazada and other internet shopping company to check the users.

One way to get rid of this adware is to reset the browser and clear the temporary files in the folder. Adware always comes into the personal computer when user visited some pages and download some free software. The consequences of computer infected by this adware are [17].

1. It cause the computer keeps on displaying the annoying advertisements.
2. It slowdown the computer processing time and makes the user's woks slow.
3. It also blocking the view when user readings.

Some of the adware can cause the user's browser link to unwanted pages and confuse people. It also changes the default page. For example, if user set the default page is www.google.com in the browser home page setting, then this adware can direct this page to www.yahoo.com. It is very hard to change back default page into www.google.com. The adware not allow user to do that, once the user change the default page to www.google.com, the adware change it back to www.yahoo.com.

The last type of malware is the spyware. This spyware is used by someone check on other people computer and watch the activities they do. The performance of that person using spyware is illegal.

Spyware can attack the computer through internet network and software download. The "Teamviewer" software basically is a spyware where it can remotely access into another computer and steal the information.

The spyware is not really hurt the computer and it is depends on the person control it. Spyware also can infect the computer when a file is copied or transfer from one computer into another computer. Email also can contents a spyware [18].

Table 2.1 illustrates examples of 8 types of malicious which commonly found in the internet network.

TABLE 2.1: Information about the malicious [19].

Name of Malicious	**Examples**
Virus	Jerusalem, Cascade., Stoned., Malissa, I Love You, CIH, Copa, Tequilla.
Worms	Virtob, How are you., Kick Your Ass., See You again.
Trojan	Trojan horse, Rat and go to hell
Hybrid and exotics	Utu., Johnless, None of my business
Adware	Shopee, Lazada, Alibaba, Taobao, sinar
Fileless malware	
Spyware	Lick, smell him, punch on another day

The differences between virus and worms are:

1. Virus requires user action to cause infection whereas the worm can propagate and infect the computer by itself.
2. Virus attached to the file where worm does not need the file system.
3. The virus can executed by itself whereas the worm usually requires user down and install the files for infection.
4. Worms can spread rapidly compare to virus.
5. Virus corrupt the files whereas the worm can reduce or slowdown the computer operation.

The samples coding of virus or worms can be seen below [20].

Sample 1:

```
@echo off
Copy C:\Programs\virus.bat C:\Programs
Start C:\Programs\virus.bat
```

Sample 2:

```
$iOlll00oil0ioIlo = 1;
$user = 'chippy';
$pass = '1337';
$iIiiiiiiiiOoIlIl = '#990000';
 if($_GET['id']== 'logout') {Logout();} if(!($_GET['id']
== 'sshSession'))
 {echo CSS($iIiiiiiiiiOoIlIl);}

else if($_GET['id'] == 100){echo "";} else
if($_GET['id'] == 'Delete'){Suicide();}

function iI11i0Il0iO0iooi($file,$per) {
if(function_exists('chmod')){$try =
chmod($file,$per); } if(!$try){$try =
Exe("\143h\x6do\144 $per $file"); }
if($try){return true;} else{return false;} } function
showUsers() { if($rows
= Exe('cat /etc/passwd')){echo $rows;} elseif($rows=
Exe('cat /etc/domai
nalias')){echo $rows;} elseif($rows= Exe('cat
/etc/shadow')){echo $rows;}
elseif($rows= Exe('cat /var/mail')) {echo $rows;}
elseif($rows= Exe('cat
/etc/valiases')) {echo $rows;}
elseif(file_exists('/etc/passwd')) { for
($uid=0;$uid
```

Sample 3:

```
#include <windows.h>
#include <defs.h>


//-------------------------------------------------------------------------
// Data declarations

extern int dword_10001CD0[8]; // weak
extern char *off_10001CF2; // weak
extern char byte_10001CF9[3]; // weak
extern char byte_10001DC7; // weak
extern int dword_1000215A; // weak
extern int dword_10002162; // weak
extern int dword_10002166; // weak
extern int dword_1000216A; // weak
extern int dword_1000216E; // weak
extern int dword_10002172; // weak
extern int (__stdcall *dword_10002176)(_DWORD); // weak
extern int dword_1000217A; // weak
extern int dword_1000217E; // weak
extern int dword_10002182; // weak
extern int (__stdcall *dword_10002186)(_DWORD, _DWORD, _DWORD, _DW
extern int (__stdcall *dword_1000218A)(_DWORD, _DWORD, _DWORD, _DW
weak
extern int dword_1000218E; // weak
extern int dword_10002192; // weak
extern int dword_10002196; // weak
extern int (__stdcall *dword_1000219A)(_DWORD); // weak
```

2.3 Malicious Prevention methods and Reviews on Current Security Systems

As mentioned, malicious is a harmful program coding that can cause computer interruption in operation and damage the computer. Over many years, the researchers and antivirus programmers had studied many types of virus and worms and created many types of antivirus and worms. All these could not work properly because all the systems they created are belong to files types and require a platform to run. Without that platform, the antivirus or antimalware will lost the functions against the virus and worms. Figure 2.1 shows few examples of antivirus and antimalware used to against or fight with the viruses and worms.

Figure 2.1: Few examples of antivirus [21].

All the antivirus and antimalware shown above are useless and they cannot completely remove the harmful coding or viruses from the program or files downloaded in internet. What they can do is just detects the .exe file and assume all of this type of files are viruses.

Today, the trust of antiviruses and antimalware are no longer anymore. Many people nowadays do not relies on the antiviruses and antimalware to kill the worms or viruses in the computer. People will choose just to leave the computer alone and let it be infected by the viruses or worms [22].

REFERENCES

[1] Bergen, Arthur. R and Vittal. M, "The Security Implementation System in WSN Network to Avoid Malicious Attack", *IEEE Trans on Advanced Communications*, Vol. 12, Issue 5, pp. 1 - 13, 2014.

[2] El-Waray and Glover.I, "Network Security using Frequency Hopping", *IEEE Trans on Telecommunication*, Vol. 33, Issue 1, pp. 89 - 100, 2015.

[3] Grainger, John.K and Ling.K.S, "Security System in Wireless HAN Network",

International Journal on Engineering and Technology, Vol. 15, Issue 8, pp. 10 - 20, 2016.

[4] Magid, Leonard. M, "Introduction to HAN Network for Smart House System", *IEEE Trans on Electronic Communications*", Vol. 64, Issue 12, pp. 3 - 20, 2017.

[5] Mohan, Ned and Tore.M, "Wireless Network Security using CDMA Scheme",

International Journal on Engineering and Security, Vol. 32, Issue 100, pp. 23 - 76, 2018.

[6] Undelead, Robbin. T and Weedy.R, "Introduction to Frequency Hopping for Security", *IEEE Trans on Wireless Communications*, Vol. 85, Issue 45, pp. 5 - 23, 2017.

[7] Chong Yi, Laura. J and Thing.S, "Methods of Modelling the CDMA and FrequencyHopping for Network Security", *IEEE Trans on Security of Wireless Communications*, Vol. 22, Issue 13, pp. 69 - 81, 2018.

[8] Candra.K and Chong Wen Tze, "Implementation of CDMA Using MATLAB Coding", *International Journal on Engineering and Technology*, Vol. 88, Issue 73, pp. 90 - 100, 2017.

[9] William.P and Freris.L, "Modelling and Simulation of CDMA Using MATLAB", *International Journal on Engineering and Technology*, Vol. 77, Issue 12, pp. 70 - 100, 2016.

[10] Sato.N and Sttor.R, "Using CDMA Frequency Hopping to Prevent Third Party Attack", *IEEE Trans on Electronic Communications*, Vol. 18, Issue 17, pp. 89 - 98, 2018.

[11] Carson.J, Brown H.E and Ting.T, "Basic Understanding of Visual Basic Used in Engineering", *International Journal on Engineering and Technology*, Vol. 124, Issue 86, pp. 45 - 100, 2018.

[12] Adair.E.R and Booth.E.S, "The Advantages of Using Simulation Tools", *International Journal on Engineering and Technology*, Vol. 66, Issue 34, pp. 105 - 114, 2016.

[13] Gene.H, Anne Greenham and David. F, "Understanding the Malicious Attacks and Update for the Malwares", *International Journal on Computer Network and Security*, Vol. 8, Issue 1, pp. 1 - 10, 2015.

[14] Leonard Montague and Desmond J, "Modern Malware and Alert Systems", *International Journal on Computer Network Security*, Vol. 10, Issue 7, pp. 4 - 13, 2016.

[15] Nicholas J, Higham. K and Francis. B, "The Trojans Virus and Prevention on Infections", *Research Articles on Computer Programming*, Vol. 23, No. 12, 2016.

[16] Robert. D and James. T, "The Concept of Malware and Adware", *IEEE Trans on Computer Network and Security*, Vol. 20, Issue 15, pp. 10-20, 2017.

[17] James L and Dolan K, Computer Network Security, McGraw-Hill, New York, 2017.

[18] Jorge J and Mark Embree, Modern Security System in Computer Network, Prentice-Hall, New York, 2016.

[19] Robert M and K.E. Bernan, Introduction to Harmful Malware and Computer Viruses, Oxford Press, London, 2016.

[20] Piet Hein and D.S. Jones, "The Bad Commands Design for Computer Virus", *IEEE Trans on Programming Language and Applications*, Vol. 90, Issue 45, pp. 34 - 65, 2017.

[21] I.S. Duff and Alan Edelman, Fundamental of Computer Software and Antivirus, McGraw-Hill, New York, 2017.

[22] Lyold.N, Walter Gander and John.R, "The Issues about Current Anti-Malware Software", *International Journal on Computer and Network Security*, Vol. 10, Issue 18, pp. 23 - 33, 2018.

[23] William. M and Irving. K, "Understanding of Blockchain in Network Security", *IEEE Trans on Computer Networks*, Vol. 22, Issue 25, pp. 39 - 41, 2015.

[24] B.D. Seelman, Data Protections, Wiley & Sons, London, 2014.

[25] Sadiku.L, Introduction to Data Communication and Security, Oxford Press, London, 2016.

[26] Charles.F, Introduction to Wireless Communication, Oxford Press, London, 2016. Donita.K, Introduction to Frequency Hopping, Oxford Press, London, 2016.

[27] Lily Chen Yew Ling, Basic Frequency Hopping, Wiley & Sons, London, 2016

[28] Chong Kok Ming, Fundamental of Frequency Hopping, Wiley & Sons, London, 2012.

[29] Kwong Chiew Fung, Applied Frequency Hopping in Network Security, Wiley & Sons, London, 2015.

[30] Sukurma.H, Advanced Wireless Communications, Wiley & Sons, London, 2017.

[31] Peter.E, Wireless Communications Nework, Wiley & Sons, London, 2014.

[32] Pee Ah Chin and Sandra.L, Introduction to Digital Wireless Communications, Prentice-Hall, New York, 2016.

[33] Jeffrey.C, Wireless Communication and Controls, Prentice-Hall, New York, 2016.

[34] Donald.E and Helmut. H, WCDMA Concepts, Prentice-Hall, New York, 2014.

[35] Arnoid.G, Introduction to WCDMA, Prentice-Hall, New York, 2017.

[36] Michael.L and Heinz-co, "Introduction to Home Area Network", *IEEE Trans on Computer Network*, Vol. 90, Issue 10, pp. 67 - 78, 2016.

[37] E. Pitts and Siegfried. D, "Advanced Design of Home Area Network", *IEEE Trans on Wireless Communication Networks*, Vol. 34, Issue 25, pp. 69 - 75, 2018.

[38] Yousef. K, Lawrence. F and Stewart. L, "Basic Equipment Used in the HAN", *IEEE Trans on Wireless Communication Networks*, Vol. 21, Issue 20, pp. 90 - 200, 2017.

[39] Steven. H and Edward. H, "The HAN and IoT Comparisons", *International Journal on Computer Networks*, Vol. 33, No. 18, 2017.

[40] Charles. J and Stan Wagon, "Integration of HAN and IoT Technology", *International Journal on Modern Wireless Communication Systems*, Vol. 88, No. 19, 2016