



جامعة الشرق الأوسط
MIDDLE EAST UNIVERSITY
Amman - Jordan عمان - الأردن

A Secure Home Appliances Remote Control Model

نموذج آمن للتحكم عن بعد في الأجهزة المنزلية

By:

Mohammed Mohammed Jasim

Supervisor

Dr. Oleg Viktorov

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Master Degree in Computer Science

Faculty of Information Technology

Middle East University

April 2014

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿ إِنَّهُمْ يَكِيدُونَ كَيْدًا ۖ ۝١٥ وَأَكِيدُ كَيْدًا ۖ ۝١٦ فَمَهْلُ الْكَافِرِينَ أَمَهُلُهُمْ رُويِدًا ۖ ۝١٧ ﴾

سورة الطارق - سورة ٨٦

الشمس شمسي والعراق عراقي

للشاعر كريم العراقي

الشمس شمسي والعراق عراقي..... ما غير الدخلاء من أخلاقي
 داس الطغاة على جميع مشاعري..... فتفجر الإبداع من أعماقي
 أجريت في الصخر العقيم جداولاً..... وحملت نور الله في أحداقي
 أنا منذ فجر الأرض ألبس خوذي..... ووصية الفقراء فوق نطاقي
 قدرتي بأن كل الحروب تحيئي..... مجنونة تسعى لشد وثاقي
 وتحالفت كل العصور لمقتلي..... فأغضتها بتماسكي الخلاق
 اسمع صهيل الحزن بين مفاصلي..... أضحي صديقي.. كنيتي.. ميثاقي
 وأنا الجميل السومري البابلي..... كانت يدي قيثارة العشاق
 هربت طيوري حين ضاع أمانها..... فكأنني شجر بلا أوراق
 لكنما همس العراق بمسمعي..... يفنى الأسى وجبين عزك باقي
 الشمس شمسي والعراق عراقي..... ما غير الدخلاء من أخلاقي

Dedication

This thesis is dedicated to all the people who never stopped

Believing in me

To my great father who never stopped supporting me during the

Journey of my life, to the father that made me the man I am.

To my great mother who raised me with passion.


To my brother and sister.

To my lovely wife, who cheered up my life.

إقرار تفويض

إننا محمد محمد جاسم أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي
للمكتبات أو المؤسسات أو الهيئات أو الأفراد عند طلبها.


التوقيع:



التاريخ: ١٢ / ٤ / ٢٠١٤

Authorization statement

I Mohammed Mohammed Jasim, Authorize the Middle East University to supply a copy of my Thesis to libraries, establishments or individuals upon their request.

Signature: 

Date: 2014-04-12

COMMITTEE DECISION

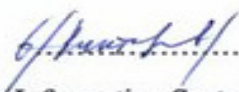
This is certifying that the thesis entitled "A Secure Home Appliances Remote Control Model" Was successfully defended and approved on April 12th 2014.

Examination Committee Members

Signature

Dr. Oleg Viktorov

Associate Professor, Department of Computer Information System
(Middle East University)



Dr. Mudafer M. Al-Jarrah

Associate Professor, Department of Computer science
(Middle East University)



Dr. Basem M.F. Al-Hadidy

Professor, Department of Computer Information System
(Al-Balqa University)



قرار للجنة المناقشة

نوقشت هذه الرسالة وعنوانها " نموذج أمن للتحكم عن بعد في الأجهزة المنزلية "

وأجيزت بتاريخ 2014 / 4 / 12.

التوقيع

لجنة المناقشة



رئيس اللجنة والمشرف (جامعة الشرق الأوسط)

١- د. أوليج فيكتوروف



عضو اللجنة الداخلي (جامعة الشرق الأوسط)

٢- د. مظفر منير الجراح



عضو اللجنة الخارجي (جامعة البلقاء التطبيقية)

٣- أ.د. باسم محمد الحنيدى

Acknowledgments

I would like to thank my father and my mother for their continuous support during my study. I also would like to thank my great supervisor Dr. Oleg Viktorov and Dr. Hussein H.Owaid Al-shimary for their support, encouragement, proofreading of thesis drafts, and for helping me throughout my studies, putting me in the right step of scientific research. I would like to thank the Information Technology Faculty members at the Middle East University. I would also like to thank my friends for their support throughout my academic journey and all of my family members.

Table of Contents

Table of Contents	x
List of Figures	xi
List of Tables	xii
List of Abbreviations	xii
الخلاصة.....	xiv
Abstract	xv
Introduction	1
1.1 Introduction	2
1.2 Problem Definition.....	3
1.2.1 Questions.....	4
1.3 Objective of this Study.....	4
1.4 Motivation	4
1.5 Thesis Organization	6
Literature Review and Related work	7
2.1 Introduction	8
2.2 Related Work	11
2.3 The Relationship between this study and the Previous Study	14
Methodology	15
3.1 Introduction	16
3.2 Presented Command Transaction System	20
3.3 Secure Shell (SSH).....	23
3.3.1 Functionality of Secure Shell	24
3.3.2 Protocol Basics of Secure Shell	24
3.3.3 Public Key and Private Key	24
3.3.4 Data Encryption	25
3.4 Presented System	26
3.4.1 System components.....	26

3.4.2 Message Transfer and Control Commands	28
Results	31
4.1 Performance Evaluation	32
4.2 Data Set	37
4.3 Experimental Result	40
4.3.1 Algorithm Robustness Testing Using Statistical and Logging Programs	40
4.3.2 Algorithm Analytical Results	44
Conclusion and	52
5.1 Conclusion	53
5.2 Future Work	55
References	56

List of Figures

Figure 3.1:The Sender Command Flowcharts	17
Figure 3.2:The Receive Command Flowchart	19
Figure 3.3: Block Diagram of the proposed system	20
Figure 3.4:Simulink Model	21
Figure 3.5:Forwarding passes authentication from the first SSH connection	25
Figure 3.6:Flowchart for the sender system	27
Figure 3.7:Flowchart for the receiver system	28
Figure 4.1:SSH Control Panel	34
Figure 4.2:SSH Setting	35
Figure 4.3:SSH Key Generator	35
Figure 4.4:PUTTY Program	37
Figure 4.5:Reliability of the proposed system	47
Figure 4.6:Internet only system	48
Figure 4.7:Results of applying a detection programs on test pattern of the encrypted message	50

List of Tables

Table 4.1: Text messages that were used in performance evaluation and result recording	39
Table 4.2: Results of applying a detection programs on test pattern of the encrypted message	42
Table 4.3: Comparison between the presented work and related works	46
Table 4.4: Experimental Results Comparison.....	51

List of Abbreviations

Abbreviation	Meaning
ISP	Internet Service Provider
GSM	Global Systems for Mobile Communications
SMS	Short Messages Service
DTMF	Dual Tune Multi Frequencies
ANSI	American National Standard Institute
OPC	Object Oriented Personal Computer
NSA	National Security Agency
NIST	National Institute of Standard Technology
DOD	Department of Defense
IDP	Identify Provider
CDMA	Code Division Multiple Access
IEEE	Institute of Electrical and Electronic Engineers

RSA	Responsible Service of Alcohol
DSA	Digital Signature Algorithm
UMTS	Universal Mobile Telecommunications System
DNS	Domain Name Server
NBS	National Bureau Standard
ATM	Auto Transfer Money
SSH	Secure Shell
CRC	Cyclic Redundancy Check
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
DCT	Discrete Cosine Transform
DSP	Digital Signal Processing
ADC	Analog to Digital Conversion
CWT	Continuous Wavelet Transform
PDA	Personal Data Assistant
ASCII	American Standard Code For Information Interchange

الخلاصة

التحكم في الأجهزة المنزلية أو البيوت الذكية هي فرع من فروع البحث ذات العلاقة بالازدهار التقني والتطور في مجال الحاسب الالي وأنظمة الأمان. العديد من الباحثين حاولوا تطوير طرق للتحكم المباشر في أتمتة المنازل، على سبيل المثال، التحكم بالمحركات، تجميع الإشارة، القياس، الخ. من ناحية أخرى العديد من الأنظمة تم تطويرها للوصول إلى وسيلة امنة ويمكن الاعتماد عليها لتناقل إشارات التحكم والقياس بواسطة أنظمة المنازل الذكية. في عصر تقنيات الانترنت الوسائل رخيصة جدا وسهلة البناء لتناقل إشارات التحكم والقياس بواسطة الانترنت. في الحقيقة، شبكة الانترنت في معظم الأحيان لا يمكن الاعتماد عليها، فهي تواجه العديد من الانقطاعات. لذلك استخدمنا الرسائل القصيرة في هذا البحث، هذه الرسائل تكون طريقة تحكم مؤقتة، و امنة ويمكن الاعتماد عليها. توفير وسيلة الاتصال المستمر بين المرسل والمستلم سيتم تحقيقها باستخدام الانترنت وشبكة الهواتف النقالة (الرسائل القصيرة). يتم نقل الايعازات عن طريق الانترنت وهو الطريق الرئيسي للتحكم في الأجهزة المنزلية ، ولكن في حال وجود أي مشكله في الانترنت او عدم توفره سيتم نقل الايعازات باستخدام شبكة الهاتف المحمول (الرسائل القصيرة) . بالإضافة الى ذلك تم تشفير الايعازات باستخدام خوارزمية اس اس اش ليكون أكثر امانا. وقسمنا الايعازات الى قسمين، الأول لا يحتاج تشفير والثاني يحتاج الى التشفير وهكذا حسنا في الوقت وعملنا نضام امن في نفس الوقت.

Abstract

Home automation or smart homes is a field of researches that is related to the rapid rise of the computer technology and security systems. Many researches are intended to develop the methodology of direct control in home automation, for example, actuator control, signal gathering, measurements, etc. On the other hand, many systems were developed to achieve security and reliable transfer of control and measurement signals via smart home automation. In the age of Internet technology, a very cheap, and easy to construct communication methodology is to transfer the control signals and measurements via Internet connection. However, in fact, the Internet connection in many cases is not reliable, while it comprises many disconnects per the day. Therefore, this thesis presents a wireless home security methodology that ensures both reliable transfer and secure transfer. The reliability will be achieved by mixing two communication media, Internet and GSM communication. The transmitter and receiver terminal acknowledges determines if the transfer using one media failed, then another media connection will be established and the message will be resent again. Also, in order to make the transmitted message secure; the is message encryption using SSH secret key encryption algorithm,. The proposed system was simulated on Simulink and the encryption algorithm was modelled on MATLAB, good results were obtained and solved the problems of security and reliability and the time at the same time.

Chapter One

Introduction

1.1 Introduction

Smart Home Technology is a collective term for information and communication technology at homes, where the components are communicating through a local network. The different technology might been used for monitoring, alarming and executing actions, according to the programmed criteria (Kucuk, 2010). They are state of the art technology in the two last decades, are becoming the most exciting and useful tools in our daily lives, which has brought a higher comfort and security level into our life. Future digital will been developed toward new environment with various structure, shape, function and design, and not been restricted by patterns or rules (Jahromi & Rajabzadeh, 2001). When it comes to the question of how smart house became an important aspect today, it is because of the rapid development in the fields of microelectronics, communication/networks and other related technologies enabled us to develop various kinds of wireless sensors. These sensor nodes are consisted of spatially distributed devices using sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants at different locations.

A sensor network provides easy access to information from anywhere at every time. This functionality is achieved by collecting, processing, analyzing and spreading data. So that, wireless sensor network plays an important role in creating smart environments effectively (Baydere, 2010).

Operating all such electronic/electrical instruments in a modern house might be difficult for the elderly as well as disabled people (Patil, Dhillon and Mitra, 2005). This rapid development of technology helps us to reduce accidents and risks that are

associated with theft, fire or faults, which may occur in the devices. Those risks could be very costly if are left unhandled. Fault-tolerant describes a computer system or component designed so that, in the event that a component fails, a backup component or procedure can immediately take its place with no loss of service. Fault Tolerance can be provided with software, embedded in hardware, or provided by some combination.

This work is trying to minimize risks and maintain the devices availability as much as possible, this is done by connecting sensors to the devices at home. The user will have the ability to control a smart house at any time, the proposed system will be safer and more secure than most smart homes available on the market nowadays.

1.2 Problem Definition

There are many applications of home appliances; the following problems have been identify in order to controls appliances by sending a message, which contains the device's name or code, providing the proper level of security:

1. Reliability problem is a critical issue in home automation, which ensures the reception of the control command and the log or the warning messages.
2. Some measures should been provided to make the system more fault tolerant .
3. Some security measures should been taken to prevent attackers from accessing the system.

1.2.1 Questions

This research aims at answering the following questions:

1. How the proposed system handles safety concerns?
2. What is the architecture of the proposed model?
3. What quality attributes the proposed system consider?
4. How to make the system fault-tolerant?

1.3 Objective of this Study

- 1- Facilitating the process of dealing with the home appliances remotely.
- 2- Main objective is to provide friendly human-machine interface.
- 3- If the Internet connection down or become unavailable, the system will provide the user with a text messaging service, to control appliances' devices temporary until the Internet connection was restored.
- 4- Design a security algorithm, to encrypt and decrypt the command messages.

1.4 Motivation

The digital communications becomes a daily used way for the most people in the world. This technology and its infrastructure enable to send secret and critical messages for a while, but with the diffusion of that technology, the security becomes very important and hard issues to achieve. This is what to lead to continuous development in data hiding for security. The most common and adaptive technique that could be adapted to be used in such application is the cryptography. In cryptography, the sender hides the secret message, in

order to be able to send it through the public network, while the rebuilding of the original message is possible if the receiver has the appropriate key.

The most researchers consider the control of domestic services and building management systems via mobile GSM and improve the methodologies to debug and commanding the actuators and action targets in the location of control. Hence, the most of their work are focusing on the control event itself and simple transfer by either GSM or even DTMF.

The fact that the control commands has to be very confidential and sometimes very critical for intrusion, leads to motivate this research to implement a cryptographic transfer of text command message using encryption and decryption algorithm that is mathematically proofed.

Another issue is the weakness of the communication networks including GSM and Internet networks. Therefore, the idea was that, the use of hybrid transmission media will significantly increases the accuracy and precision of the system. The hybrid network will use the local Internet service provider in addition to the GSM mobile communication to ensure a reliable transfer of the command messages and feedback messages from the location of measurement, weather it was a home, office, or even an outdoor location environment.

1.5 Thesis Organization

The work of this research is to demonstrate the technique that is used to add security to control messages that used in home domestic applications. In addition to create a strategy to ensure a backup transfer line for that control message(s) in the case of failure of one communication line that would be either GSM based Internet or GSM mobile communication.

This thesis was divided into five chapters. The first chapter illustrates the goals, concepts, contribution, and system design idea. In the second chapter, some related researches that shows literal survey were presented. The third chapter illustrates the scientific techniques that used in research work. The complete methodology and design steps will be presented in chapter four. The results of the proposed researches measured and discussed in chapter five. Finally, conclusion and future recommended researches .

Chapter Two

Literature Review and Related work

2.1 Introduction

Smart homes or an automated home plugs all appliances and devices in the home in a way that enable them to communicate with each other in addition to the homeowner. Any device that being used in a home by the means of electricity is capable to be put on the management system of the home and subjected to human command. Regardless of the command itself, or the input command type, the device should reacts. Most functions relate to home security, lighting, temperature and air control, alarms, entertainment, computer vision and others. Security represents an important criterion in the automated home functionality. Conventional systems of security always meet the condition of making people at home, and their own property, and secure from different intruders. A smart security system of a home, make many other benefits are available (Edwards, 2011).

In historical view, smart home technology was started in when a Scotch company had developed the X10 in 1975. The X10 allows compatible products to talk to each other over the already existing electrical wires of a home. The most of appliances and devices are being working as receivers. While the main control device that controls all these appliances remotely, like remote keypads or cell phones, are implementing transmitter functionality. If a person wants to switch the lighting on or off in another home area, the transmitter will send a control message that has a code of the needed required command (Patricio, 2009).

The control sequence should be considered to be achieved successfully in a very short time. The X10 faced many constraints. The communication and signal transfer over

electrical power lines considered to be not reliable and not efficient, because of that the lines is power and always has noise affecting the other devices. The X10 peripheral would interpret electromagnetic interference like a command and perform an action, or even it is possible not to understand the control command itself. Therefore, many researchers tries to work in different platform that the home original electrical power outlets, that should consider being reliable in automation of home (Patricio, 2009).

In addition, Z-Wave was created in the next phase, it uses a source routing algorithm to send the control and feedback messages to determine the fastest route for messages. Each Z-Wave device is embedded with a code, and when the peripheral is inserted in the system, the network controller recognizes the code, specifies its address and adds it to the structure of the network. When a control signal issued, the control device follows the algorithmic behaviors to specify how the data message should be transferred and what the command that should be performed. Therefore, the routing is possible take a lot of memory space on the network space. The Z-Wave has implemented hierarchy between the peripherals: Some controllers initiate messages, and some are slaves. That means they can only carry and respond to messages (Van, 2009).

The use of wireless network ensures more flexibility for appliances arrangement and installation, but as normal electrical signals lines, they are subjected to interference. the system that is connects the control system of home with the user was been adapted and named Insteon. It enables a methodology for the home network to have communication over radio channel in addition to the original home electrical wiring, thus, it is a dual

channel network. In this topology, the message has to be sent in one media, either it was a radio channel or even the power lines, so, when a fail in that media occurs, the system will re-establish another transfer using the other twin media. Insteon devices do not rout the message, but instead, it device is broadcasting the control message, and the peripherals pick up the signal and transfer it until the control action is achieved. The peripheral behaves as a peer. The "Insteon" device, which is installed on behave of the network, will comprise a stronger transfer of the message (Nasri, 2010).

In Jordan and Middle East, technology to equip homes with smart devices are concentrating on development of controlling the building management and get feedback and control of critical signals and status. No special protocol is being used to adopt the digital communication between smart devices. Instead, many common communication networks is being used for that purpose like GSM and Internet. Such link media connects the appliances to a central home / office communication and control system. It actually works as telephone line or terminal PC (Banerjee, 2011).

Nowadays, the rise of cellular communication and mobile systems pushed the home automation in advance. The mobile telephone networking usage in commercial applications becomes reliable in the rise of GSM wireless communications. In addition, the big revolution in the Internet in commercially used technology for home users makes the adaptation of special home automation networks so expensive with respect to those of GSM and Internet. Actually, the implementation of systems that depends on globally used wireless network will cost much less than any other networks and it is very reliable and

efficient in smart homes and automation. It is also very efficient in industrial automation. It starts with OPC server (object-oriented personal computer) to remotely control the industrial processes. Nowadays, we can reality and costless use either Internet or GSM mobile communication to control any automation event, and also, to get feedback from the automated system, which considered to be status or alarm signal (Sleman, 2009).

2.2 Related Work

Home automation becomes a high need in the age of technology rising up to controlling any feature in the human life using computer-based system. This literature review looks at the research that has been published in the area of cryptography as it relates to network data and global communications security. It contrasts and compares the researches taking into account the general scope in the researches that published during past years that related to this objective, which considered more related and more affecting. It studies the use of encryption / decryption algorithms that has taken place and is the concern of future and current technology that is related to security. This literature presents cryptography as basic theme of the home security that it ensures corporations, individuals and others in the recent of wireless networks and Internet technology. This thesis aims to build and implement a high security and high reliability cryptography based technique for wireless transfer over Internet and GSM communications.

In their work (Faisal and Beg , 2013) suggested two ways to control home automation system appliances. The first one is remotely via voice commands; the second one is using remote control to override the control of the appliances.

In work (Ahmad and Yakubu, 2011), a new strategy to manage and control home appliances using mobile phone, this method allows the users to control their home appliances from remote distance.

(Tafaraji, 2011) illustrated a concept of security developing of the code division multiple access (CDMA). The CDMA is considered to be widely implemented air linking wireless interfaces though the 3G communication. This work applied an encryption / decryption algorithm over the code of spreading. It also illustrates the cross correlation over encryption algorithm outputs which causing interference for multi user was demonstrated thoroughly, since the detection of multi user should be the CDMA inherent characteristic. An unencrypted and encrypted combination of M-sequences is used as the code of spreading to mitigate the performance of the system. A hidden direct sequence is the methodology that was proposed in this work, which aims to enhance the CDMA security systems via application of the algorithmic cryptography in the code of channelization. This method of spectrum spreading security prevents cross calling of eavesdroppers of intercepted message, and it prevents those from trying to decrypt the transfer.

In their work, (Rosmanith, 2010), introduced a home automation system based on Internet Protocol (IP) they designed a low cost hardware/software system to evaluate their approach, they used SSH protocol to carry one side of the transmitted commands, however, their results were not satisfied due to the huge number of lost packets.

(Hsiao-Han Chen, and Yi-Bing Lin, 2010), In this work a point and control scheme that enables selecting a home appliance by pointing the smart phone to the specific appliance. They showed the performance of their solution, which is able to achieve the remote control function effectively.

In their work (Aihab Khan and Malik Sikandar, 2009) focused in their work on controlling the appliances remotely and providing security for remote controlling the appliances. Their system is based on GSM SMS, to provide solution to the problem faced by homeowners in daily life.

(Rifat Shahriyar and Emanul Hoque, 2008), introduces a new mechanism in their work their approach leveraged the ordinary services of mobile phones to communicate and control home appliances to satisfy the smart home concept.

On the other hand, (Murthy, 2008), studied primary health-care management for the rural population. Their approach proposed the use of mobile web technologies to the rural population. The system involves the use of SMS and mobile phones technologies for information management, transactional exchange and personal communication.

In their work (Jawarkar, Ladhake and Thakare, 2008), This work a remote monitoring system using mobile technology also, they involved the use of spoken commands, which are generated and sent in the form of text SMS to the controller then to the microcontroller, based on SMS commands, their take the decision of particular task.

(Chris Rapier, 2005), In their work discuss the nature of this limitation, the functional barriers it imposes, a method by which it can be remedied, and introduces a high performance implementation based on the industry standard, OpenSSH. Additionally.

2.3 The Relationship between this study and the Previous Study

After studying the three proposed work of each of them and how one is a solution of the other, (Beg, et al, 2013), and (Jawarkar, 2008) and (Aihab Khan, 2009) previous benefits and enhanced using GSM and security in home automation is proposed.

This study is meeting with the three previous studies, (Beg, et al, 2013) using remotely via voice commands and using remote control to override the control of the appliances and (Aihab, 2009) using has based on GSM SMS, and (Jawarkar et al, 2008) using SMS commands. And in this studies using two Chanel that are internet and GSM and to security using SSH protocol.

Chapter Three

Methodology

3.1 Introduction

In computer and digital system, the computer technology added more complexity and flexibility in data communication. The messages become very easy to be transported. The cryptography using SSH were adapted in terms of data encryption and compression, to enable secret transfer and storage of confidential and critical messages.

The aim of the proposed system is to find a reliable solution to control home automation system remotely. The system is based on two channels, the Internet and the GSM SMS. When one channel goes down the traffic turn to the other channel. The system is enhanced with a security algorithm to secure the control messages. There are two subsystems; The user side, and the controller side. The flowchart 3.1 describes the system.

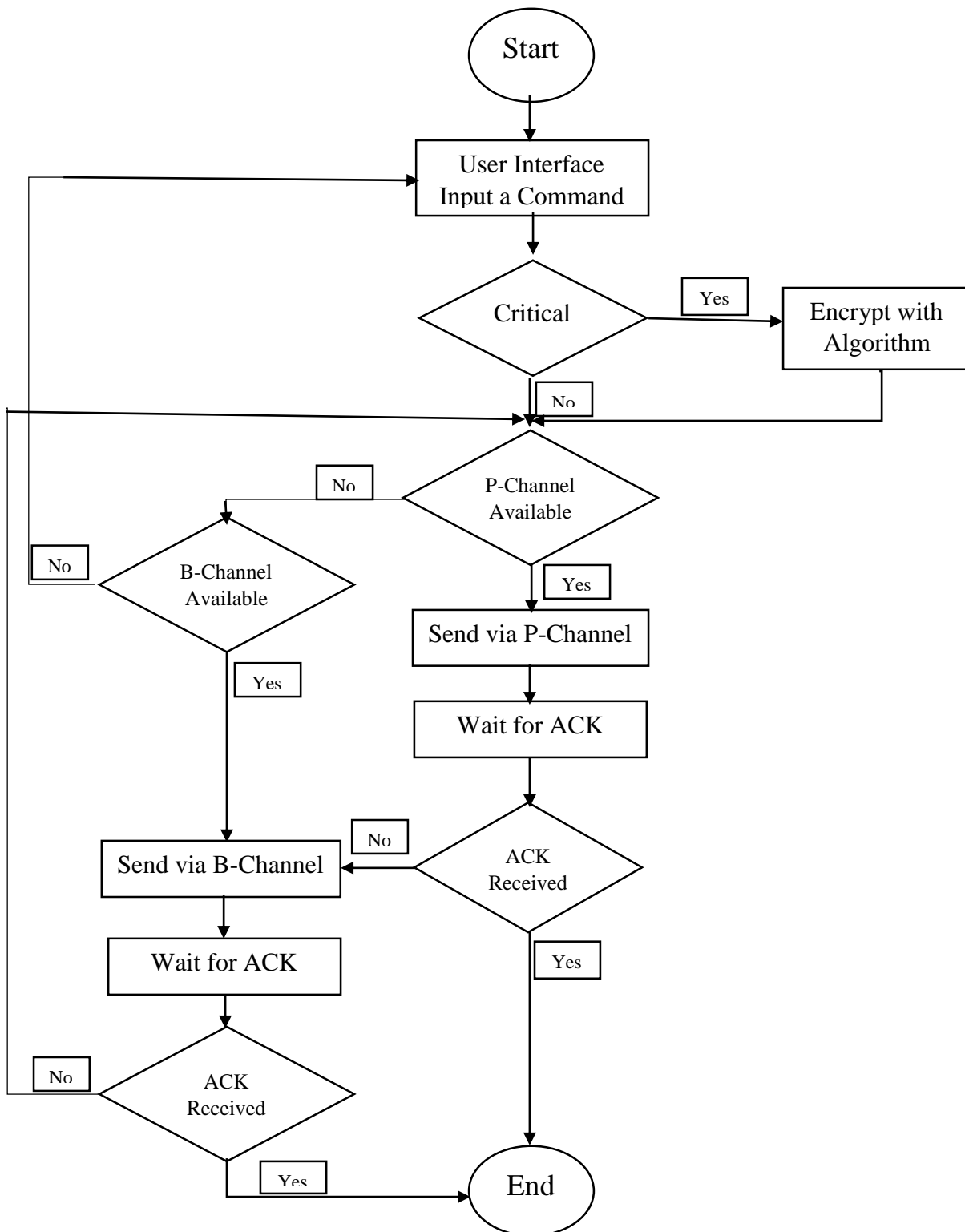


Figure 3.1 The Sender Command Flowchart

The flowchart 3.1 explains the proposed system as follows:

- Initially the user sends the control command to the system. This system contains two redefined databases, one for critical commands, and the an other for non-critical commands.
- The system determines if the entered command is critical or not.
- If it is critical, it in the critical database, the system applies the proposed Secure Sell (SSH) algorithm.
- Then the SSH algorithm, transfers the command into secret data and turns them into the transfer channel. In more details, the critical command will be transferred to the SSH algorithm to be encrypted, however, the non-critical command will be sent to the receiver without encryption, to reduce time and efforts.
- The Internet channel has the primary priority channel.
- The system will transfer the command (as explained in section 3.1) in the channel weather it is encrypted or not.
- Then after transmission, the sender waits the acknowledgment packet to ensure the reception of the signal.
- If it received and it is secure, the controller will send a log message via GSM SMS channel or the available channel, to inform the user that the action was taken.
- If it is received and it is non-secure, the controller will send a log message to the user via Internet or the available channel.
- The below flowchart explains the controller subsystem.

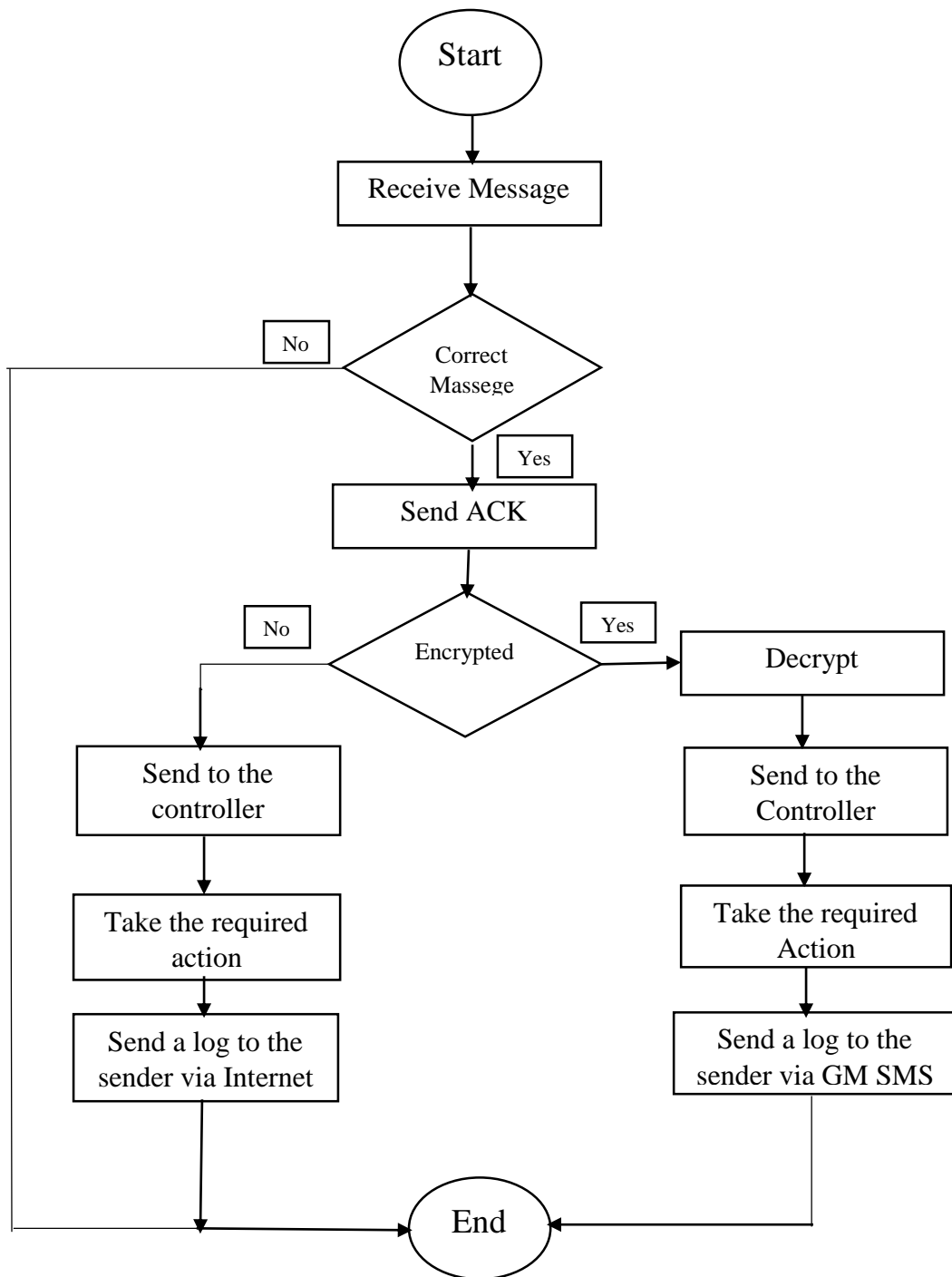


Figure 3.2 the Receive Command Flowchart

The flowchart 3.2 explains the receiver side, which contains the following tasks:

- Initially the system receives the signal,
- Then it determines if it is encrypted or not
- If it is encrypted with SSH it will decrypt it
- Then send it to the controller
- And send a confirmation message to the sender via SMS
- If it is not encrypted it will send the message to the controller
- And send a confirmation message to the sender via Internet

This approach solved the issues of reliability, security, in low cost and short time as will be shown in the results chapter.

3.2 Presented Command Transaction System

As mentioned previously, this thesis presents an enhanced method of controlling home automation system, this approach is based on two channels, which are the GSM SMS and the Internet, block diagram of the proposed system is shown in the figure below.

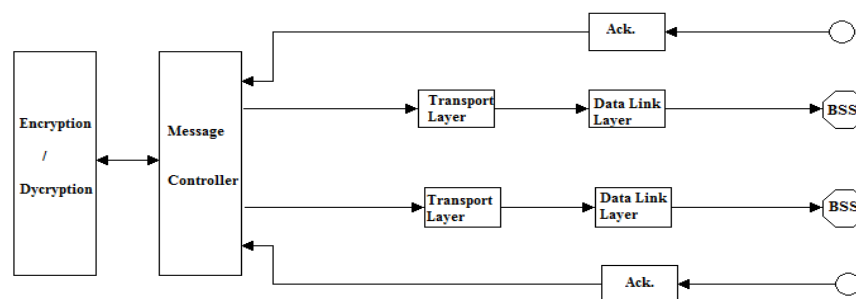


Figure 3.3: Block Diagram of the proposed system

To solve the reliability and security problem, this work presented a two redundant channel secure systems to carry the control commands. As shown in the figure 3.3, the transferred command initially encrypted using the SSH algorithm explained in section 3.6, then the message will be transferred through the internet initially, the sender will wait an acknowledgment from the receiver for a predefined period. In case of the time out without receiving the acknowledgment packet, the sender will resend the packet through the other channel, which is the GSM SMS.

The system model has simulated using Simulink.

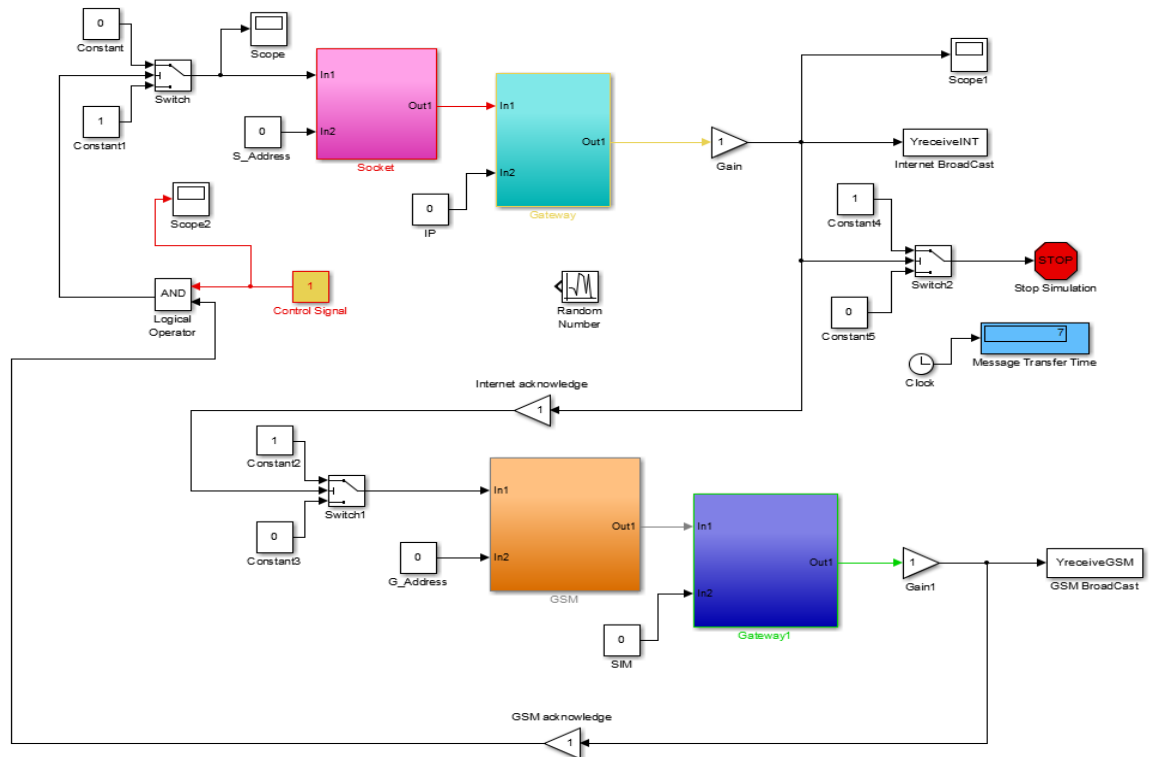


Figure 3.4: Simulink Model

As shown in the figure 3.4, two models were created, initially an Internet model is based on YreceiveINT broadcast, this model simulates the Internet network and transmission medium, and was created using DSP and Communication toolboxes. Gaussian noise was also added to the model to simulate the real world.

The other model is the GSM SMS, this is also model using the same toolboxes and the 2G communication standards, and this is the used standard in mobile voice and text communication without the use of Internet.

In this model, two options were created, the use of the Internet channel or the use of the GSM channel, the medium was not susceptible to noise thus as shown in the model above, a Gaussian noise block were added to the model. A feedback notification or acknowledgment log were add to the system, this was condition to the receiving of the command message by the receiver.

A preemption has been added to the system model algorithm, ensure the return to the primary channel, which been chosen as the Internet by using larger weights, however, this preemption ensures the return to the Internet after fixing a problem. The sender and receiver flowcharts, summarizes the transaction method.

Initially the command will be encrypted, and then send through the Internet, if it was received by the destination, it will be decrypted and sent to the controller, which is in return forward this command to the related device to be controlled. If the command message

cannot received by the destination, the sender will not receive an acknowledgment, then after the waiting period, the sender will resend the packet again, via the other channel.

After that, the system will resend the packet through the GSM SMS channel. In this case, the maximum time that it took the message to reach the controller is:

Transmission Time + Encryption Time + Decryption Time.

The system model simulates the Internet and GSM, and the proposed algorithm using both of them. Initially the Internet have divided into two parts, the socket, which represents the Network Interface Card, and the Gateway, which is the device that will route the signal to the Internet. The message then amplified and sent via a simulated antenna. It contains also an IP address model to ensure that the command it directed to the right destination.

The controller will connected to the Internet via Ethernet and to the GSM SMS via a modem. This controller will also contain the same application that runs the same algorithm. The results of this model is showing in the results chapter.

3.3 Secure Shell (SSH)

Secure Shell is a protocol to give encryption and authentication to the data integrity to secure network communications. SSH gives secure command-shell and allow remote access to TCP destinations. SSH is widely used in client-server environments.

SSH provides good answer to the data security problem sent in public network. SSH is used rather than using a traditional overnight courier can provide a substantial cost savings (Chris, 2005).

3.3.1 Functionality of Secure Shell

SSH, abilities are as follow:

- Secure command-shell.
- Secure file transfer.
- Port forwarding.

3.3.2 Protocol Basics of Secure Shell

The Secure Shell protocol provides the below benefits:

- User Authentication
- Host Authentication
- Data Encryption
- Data Integrity

3.3.3 Public Key and Private Key

SSH uses Public Key Authentication as a secure method. Public key uses a method of generating the key that is usually between 1024 and 2048 bits, As shown in the bwlo sample. The public key is useless except with the existence of the private key

Comment: my public key


```

AAAAB3NzaC1kc3MAAACBAKoxPsYlv8Nu+fncH2ouLiquUNGIJo8iZaHdpDABAvCvLZnjFPUN+SGPtzP9XtW+
+2q8khlapMUVJS0OyFWgl0ROZwZDApr2olQK+vNsUC6ZwuUDRPVfYaqFCHrjzNBHqgmZV9qBtngYD19fGcpaq
1xvHgKJfPeQOPaG3Gt64FAAAAFQCJfkGZe3alvQDU8L1AVebTUFi8OwAAAIBk9ZqNG1XQizw4ValQXREczII
N946Te/1pKUZpau3WiiDAXTFIK8FdE2714pSV3NVkWC4xlQ3x7wa6AUXIhPdLKtiUhTtxtcm1epPQS+RZKrRIXjw
KL71EO7UY+b8EOAC2jBNIRtYRy0Kxsp/NQ0YYzJPfn7bqhZvWC7uiC+D+ZwAAAIEAmx0ZY05jENA0linXGpc6
pYH18ywZ8CCI2QtPeSGP4OxxOusNdPskqBTe5wHjsZSiQr1gb7TCmH8Tr50Zx+EJ/XGBU4XoWBJDifP/6Bwryejo3
wwjh9d4gchaoZNvIXuHTCYLNPfO RKPx3cBXHJZ27khllsjzta53BxLppfk6TtQ= ---- END SSH2 PUBLIC KEY ----

```

Private keys are typically generated using a key generation utility. Both keys in the pair are generated at the same time and, while the two are related, a private key cannot be computed from a corresponding public key. In addition to authentication, keys can also be used to sign data. To access an account on a Secure Shell server, a copy of the client's public key must be uploaded to the server.



Figure 3.5 Forwarding passes authentication from the first SSH connection

3.3.4 Data Encryption

Encryption is the protection of data from disclosure to the attacker or eavesdropping on the wire. Ciphers, on the other hand, is the method of encrypting and decrypting SSH over wire. One of the most common symmetric key algorithms is block cipher (e.g. Blowfish, RSA, and Twofish).

These operate on a fixed size block of data, use a single, secret, shared key, and generally involve multiple rounds of simple, non-linear functions. The data at this point is “encrypted” and cannot be reversed without the shared key.

Session keys are the “shared keys” described above and they randomly generated by both the client and the server during establishment of a connection. Both the client and host use the same session key to encrypt and decrypt data although a different key have used for the send and receive channels (Rosmanith, 2004).

3.4 Presented System

3.4.1 System components

In the time of domestic services and home automation, the computer era becomes the motivated engine to all security researchers. This thesis implements a secure multichannel home automation system in order to create a high level of security to the transferred data via mobile and Internet communication using SSH standards. In fact, the Internet is the basic communication media. However, in case of failure the mobile communication will start to substitute the failure of Internet connection and create another new connection to ensure the reliable transfer of that message.

Figure 3.6 shows the flowchart for the transmission system where Figure 3.7 illustrated the receiver terminal flowchart the presented system. The implemented system is divided into two parts, the sender part and the receiver part.

The senders normally write a text short message that contains the command of the home automation control command. The message will be covered with SSH algorithm to be encrypted. In the proposed algorithm, not every command is encrypted via SSH, however, the message will be sent normally, except predefined important commands, that cannot be sent without encryption.

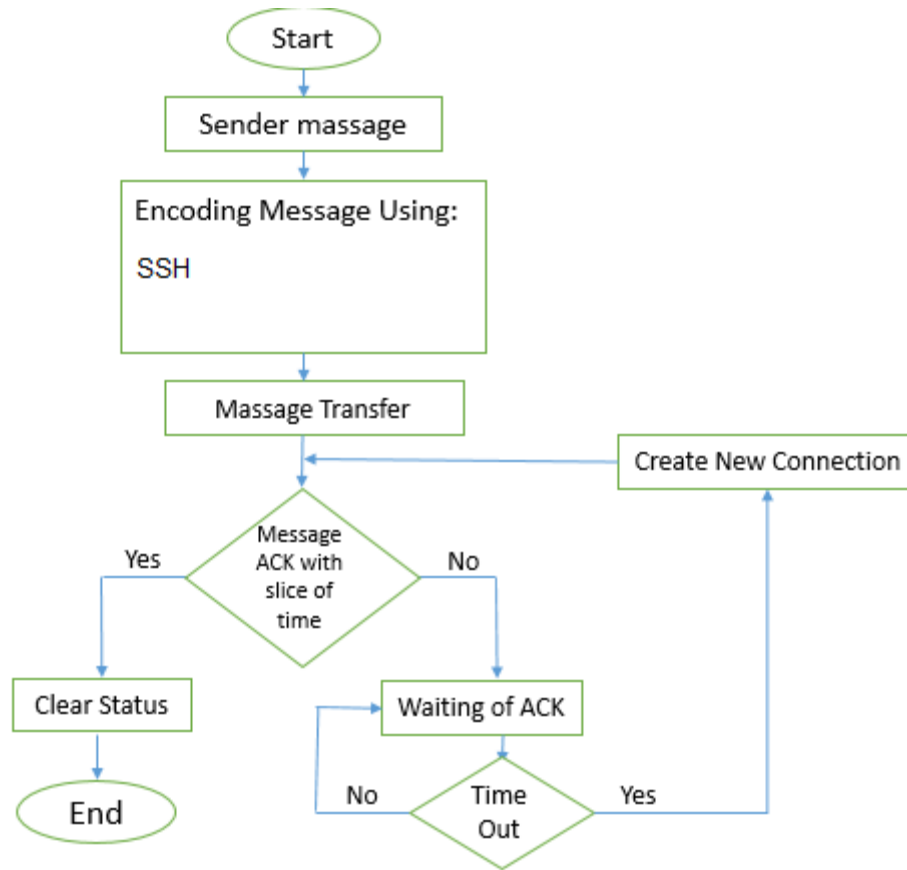


Figure 3.6: Flowchart for the sender system

The receiver terminal will apply these concepts in reverse way in order to extract the real text message from the received encrypted one. Once the message is being received,

(as will be described in Section 3.2) then the reversing of encryption procedure will extract the meaningful message.

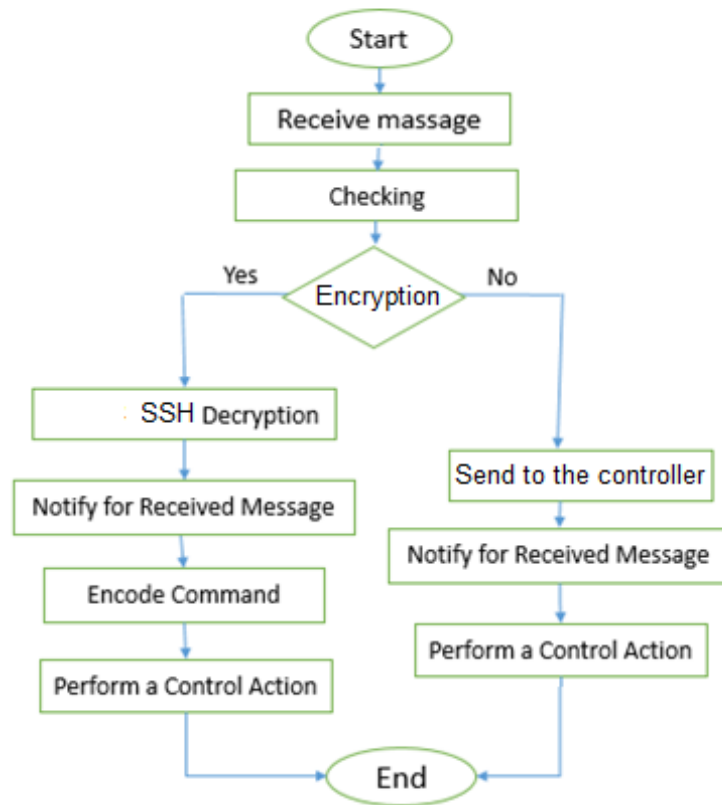


Figure 3.7: Flowchart for the receiver system

3.4.2 Message Transfer and Control Commands

The basic communication media is the Internet, the control commands and status message all are transferred via Internet. When any fail detected on the Internet communication media, the backup media will be activated to send the command and status via SMS instead of Internet.

Present research is intended to Short Message Service (SMS) from a sender terminal to the receiver terminal with high security trend. Such technology always enables the commercial user to send and receive fast messages in the pathway lies in between the GSM terminals. The short messages service was based on the Global System for Mobile (GSM) communication initially. However, it stays with the most modern communications that extended from GSM like UMTS and CDMA.

Initially, the user writes the command code that is capable to be interpreted and activate a control action in the target home. This command in the form of SMS will be decrypted depending on the algorithm that is described in this chapter and the result data will be loaded as a payload with the SMS header to format legal SMS that is capable to be sent via either Internet or GSM mobile communications.

Hence, the target is to control domestic home automation, the command will control one of the common home services. In order to make the command easier and add more redundancy to the receiver controller, which will make the event interpretation easier to generate the control signals and perform the control action, this

As shown in Fig. 3.6 and Fig. 3.7 the receiver calculates the SSH to check the validity of the received message. If so, the receiver returns acknowledgement to the sender. The sender transmits the message and waits for the acknowledgement. After specified reasonable time, the transmitter creates a new connection if the acknowledgement not received. The first connection is initially the local Internet by

default, and the new connection will be the local mobile communication network. The transmitter repeats this loop until receives an acknowledgement from the receiver or until the user cancels the control message. This will ensure that, the sender algorithmic system will continuously try to send the control message via different connections until a reliable connection passed and the messages to be received.

Then a recognizable message received, the receiver will acknowledge the message and start the exact control sequence. To prevent performing the same control command twice, the receiver will mark the message read once it was recognized and will delete it once the control action is performed.

This thesis simulation was done using MATLAB. MATLAB contains an essential toolbox (library) specialized for packets transformation, analysis, and its properties. This toolbox gives an ease to use and implement the packet transformation in different systems in case of simulation and algorithm development without any worry about the programming skills, computer specs, and any other issues that do not relate to the system and algorithm design.

Chapter Four

Results

4.1 Performance Evaluation

The aim of this research is to develop hybrid system for reliable transfer of domestic home automation control command to achieve high security, and high reliability of secret messaging and data transfer. This goal is being achieved by implementing a contributed algorithm that used SSH Protocol. The transfer has been done in two ways, Internet transfer and GSM short messages.

Initially, the results are being estimated on the same computer. Actually Three different personal computers were used to generate the control message. Then, those computers transfer resulted messages to another three terminal personal computers. The main way is to send the message via Internet by the use of direct email messaging; this uses the Internet transmission, by sending the control messages email from a transmitter PDA device to the receiver PDA terminal.

Those methods in transferring the control message on substitute need for hardware implementation and ensures that, this new algorithm is valid whether it transferred directly using digital storage media, or by Internet messaging. The messaging is the similar to GSM messaging with respect to its message structure and format. Those are the basic way that this thesis is intended to develop and design. While the use of separate personal computers, as receiver terminal will make some dependability of decision making for the receiver terminal program.

A specially designed programs is normally used to detect if the redundancy of the hacked message in order to achieve their goal by finding some consistency in the received bulk of data message. Actually, those commonly used detection programs are enterprise and not easy to use some of them legally. Because of their high cost and reasonability.

In fact, the detection programs are implicitly implements the concepts of message performance evaluation (i.e. the described above criteria) and measurement methodologies. Those detection programs that based on trials, the program use a huge amount of trial and tries to find some meaningful result in its trials. When this result is found, a hit is recorded and the method the location of hiding information is almost detected, after that, another methodologies should be applied to extract the real message if that is possible.

However, if cryptography detection program did not find any meaningful results, the image appears to do not have any information inside it.

To make server on ssh and using this protocol to send and receive the critical command we used the (Bitvis SSH Server) program. Use this start and stop Bitvis SSH server and manage its host key pairs, the password cache, and settings.

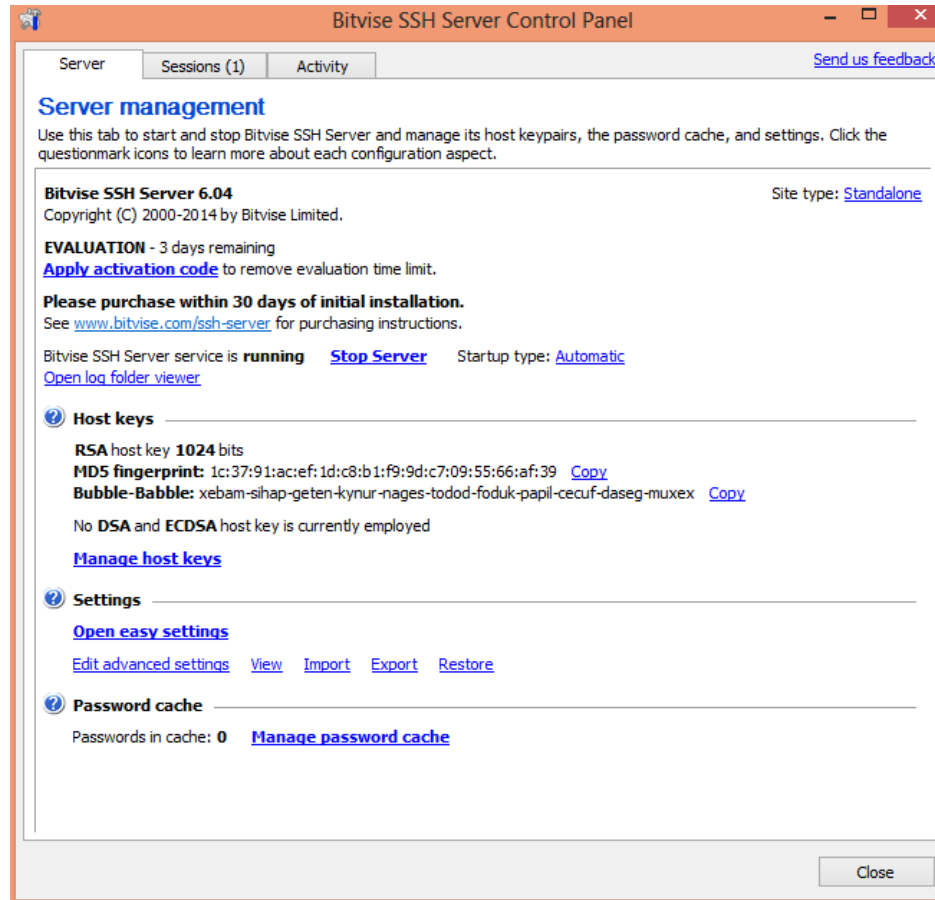


Figure 4.1 SSH Control Panel

open easy setting to chose port nummber of SSH. The dufalt portt 22 ,in this work we make spashil por (333). Before opening your firewall and router to outside connection to "local host" with an SSH client installed on the same machine.

Once you are satisfied with your configuration the SSH server to open the windows firewall and configure your route so that outside connection can be received.

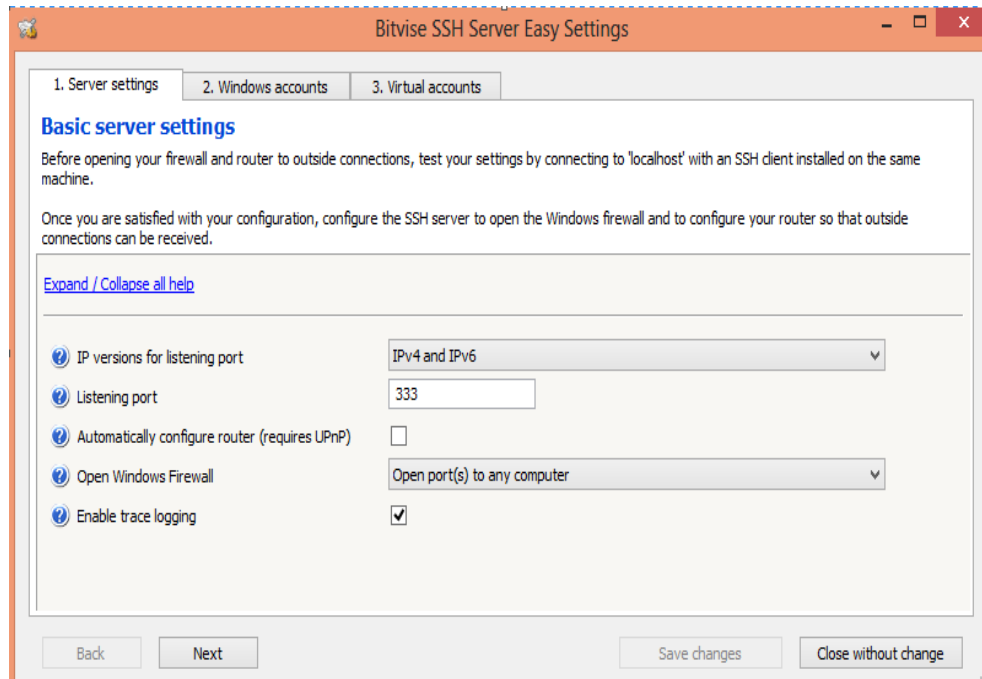


Figure 4.2 SSH Setting

"Manage host keys to create private key and public key and can choose type of key RSA 1024, 2048 or RSD 1024,2048.

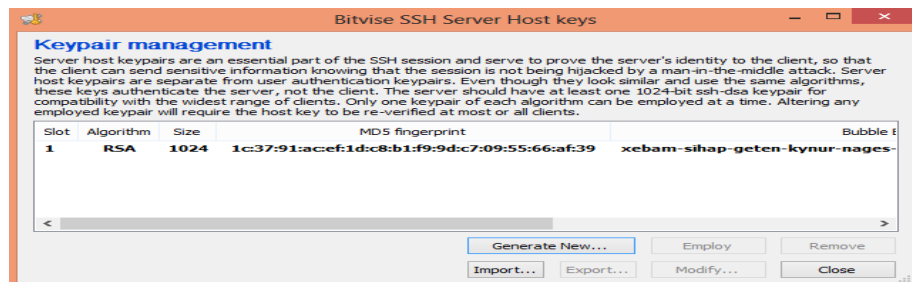


Figure 4.3 SSH Key Generator

Server host key pairs are an essential part of the SSH session and server to prove the server's identity to client. So that the client can send sensitive information knowing that the session is not being hijacked by a man-in-the-middle attack, server host keys authentication key pair. Even though they look similar and use the same algorithms, these keys authenticate the server, not the client. The server should have at least one 1024bit SSH DSA key pair for compatibility with the widest range of clients. Only one key pair of each algorithm can be employed at a time. Altering any employed key pair will require the host key to be re-verified at most or clients.

Now the server is ready to connect with the client to send and receive command, in this work used (PUTTY) program to connect with server. These settings SSH login rights and permission for local account that already exist in windows. If your server is part of domain, these settings also control login right and permissions for domain accounts.

To create or manage local windows account, use computer management in windows administrative tools, or User account in the windows control panel. If using domain account, do not forget to configure the windows domain order in advanced setting.

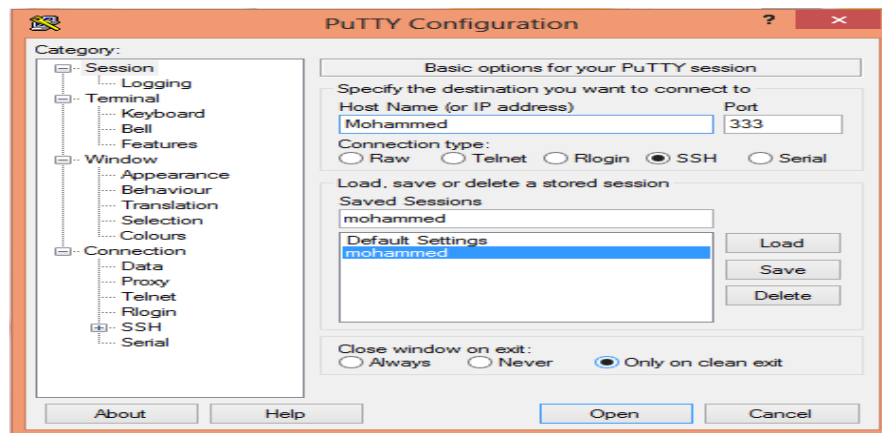


Figure 4.4 PUTTY Program

4.2 Data Set

In order to test the performance criteria and evaluation, a reasonable data set should been selected and tested. In this thesis, couple of messages in different conditions to perform the testing, evaluation and recording the result.

First, different messages where been selected to be decrypted. Those messages are differ in their contents to enable testing different message sizes, different structure of the string message (where the special characters may cause a problem in such systems), and there contents. This method enables to fix the bugs in the system, and ensure to handle the different messages the English language.

The messages that was used to been encrypted for testing are shown in table 4.1 bellow. This table contains 30 strings those used for testing purpose. It contains real control messages to test the real messaging state and to be sure about the secrecy of that

information. In addition, it contains a text only messages that mean nothing, it represents the simplest messages ever. Those messages do not contain any special characters, only English language meaningful characters.

Thus, it enables to test different formats of the message and its complex context and structure.

30 samples were enough to judge on the contributed algorithm, and to measure the security and reliability of the proposed algorithm, in addition to the required time, the robustness, and the security level. More than thirty messages could get more rigid results, and could ensure the consistency of the algorithm, but it will not so differ than the results that gotten by a thirty samples only.

Those samples are send from one computer to another, using three personal computer machines, to make some dependability of the gotten results. And to test the reality of the control message using Internet protocol, where the GSM is not really build because it's high cost of hardware.

Table 4.1: Text messages that were used in performance evaluation and result recording

No.	Message
1	First test message
2	Second test message
3	Test 5 4
4	Open condition 1
5	Close condition 2
6	Start TV 1
7	Start TV 2
8	Stop TV1
9	Stop pump 2
10	Speed up fan 1
11	Speed down fan 2
12	Stop fan 3
13	Zoom in cam1
14	Zoom out cam 2
15	Close cam 3
16	Focus in cam 4
17	Pan right cam 1
18	Pan left cam 2

19	Tilt up cam 1
20	Tilt up cam 3
21	Tilt down cam 4
22	Alarm on 1
23	$\cos x^2 + \sin x^2 = 1$
24	Is a >> 4 equals 5.3
25	What you doing!?
26	This is just for test 8425
27	Lemon is a tree 3
28	#define pi 3.14
29	$A \models 8 \ll 2$
30	$(3+4)^2 \% 5$

4.3 Experimental Result

4.3.1 Algorithm Robustness Testing Using Statistical and Logging Programs

As described in section 4.2, the sample images were random to test the effects of size, security, and the message quality. The messages , are encrypted by SSH and transferred to the receiver terminal. The same computer contains the software that is able to transmit and receive messages in the same time.

The result of this test shown in table 4.2. In fact, all images applied to all types of tests. At the result, all messages were subjected to at least two tests of the existed test in the

table 4.2. Some messages were subjected to four or more tests. These tests take a lot of time separately using separate personal computer machines.

The gotten result was as expected, it good, most test were unable to detect message inconsistency or possibility to load an intrusion data. This proves the assumptions those were made along the thesis. Where, the use of SSH security in addition to the work in two channels of transferring the message context information very rigid inside the carrier image.

Table 4.2 shows that, each test is done on at least half of the test sample messages. This ensures that, the message is robust with different fixture of its context. Some detection programs work in different signal measurements criteria.

Table 4.2: Results of applying a detection programs on test pattern of the encrypted message

Command	Transmission With SSH	Transmission Without SSH	The Proposed Algorithm
Open condition 1	1.406748	0.008039	0.008039
Close condition 2	1.305013	0.007041	0.007041
Start TV 1	1.414890	0.002033	0.002033
Close Main Gate	1,498761	0.002328	1,498761
Stop TV 1	1.313763	0.001959	0.001959
Stop pump 2	1.297849	0.002271	0.002271
Turn on Power Generator	1.402484	0.002291	1.402484
Speed down fan 2	1,351345	0.002025	0.002025
Stop fan 3	1,516306	0.002286	0.002286
Zoom in cam1	1,423879	0.002022	0.002022
Alarm on	1.502815	0.002025	1.502815
Focus in cam 4	1,385250	0.002000	0.002000
Speed up fan 1	1,448511	0.002372	0.002372
Turn off Main Power	1.520018	0.002049	1.520018
Zoom out cam 2	1,402942	0.001951	0.001951
Stop Alarm	1.471350	0.002030	1.471350
Stop TV 3	1.443733	0.002253	0.002253
Sum	23,919148	0,04902	5,8034542
Average	1,407008	00,288353	0,34137966

As shown in the previous result table, this contributed algorithm of dividing the messages into critical or non-critical messages enhanced the delivery time of the command to the controller, moreover, it enhanced its security and reliability. To go over the tradeoff between the time and security, we used the division system, in which the normal commands were transmitted without SSH encryption and the secure commands were transmitted with SSH encryption.

This division, were made based on the importance and accuracy of the commands; As shown in the table above, the Alarm is a very critical entity, and needs accurate treating. Thus, our algorithm force this command to be encrypted with SSH. On the other hand, the TV is not as important as the Alarm, thus, it will be sent without encryption.

The results above, compared between the transmission times, with SSH and without SSH, then compare the results with our work, which divide the commands. The table showed our enhanced results of securing the critical commands and transmitting the normal commands in short time. In comparison of other works that apply the security to every command or transfer all the commands without security; the disadvantage of the first one is the delay of transaction time, and the disadvantage of the second one is the lack of security.

However, the proposed contributed algorithm, solved the two issued in very smart way. For example; “ Stop TV 1” in the first method which uses the encryption on every command, takes “1.134 Sec.” all the way to reach the controller, while in this proposed

method it takes 0.002 Sec.” and because it is non-critical command, the proposed method handled the command with very short time.

On the other hand the “Stop Alarm” takes “0.002 Sec.” in the algorithm that does not use SSH in all the commands, but in the proposed algorithm, it takes “1.47 Sec. “; But this command is very critical and cannot be sent without encryption as the previous method has done. This in addition to the delay time, which is tradeoff, this method transmitted the command in a secure way. By reaching that, the proposed algorithm solved the security, reliability and delay time, in a very smart and contributed way.

This section shows the final complexity, security level, and robustness of the contributed algorithm. The next section illustrates the result of applying the algorithm on the sample text messages.

4.3.2 Algorithm Analytical Results

The contributed algorithm was implemented used MATLAB, as two stages program. One stage to encrypt the text command message using SSH and the other is to decrypt it. Both stages were implemented in a single program, which enables the communication terminal to both transmit and receive messages in the same time.

This result were gotten by applying the described methodology (see Chapter 3). Good result are shown previously in this chapter that shows the rigid work ad homogeneous system components selection and adaptability. The following chapter shows the conclusion

of this thesis work, and demonstrates some views of future work remarks that could be done in researches that is related to this thesis field.

The main contribution of this work is the use of two channels, which are the Internet and the GSM SMS, this system enhanced the reliability of previous systems such as the Internet only systems or the GSM only systems. This proposed system decreased the probability of the downtime of the entire system, such as when one channel goes down the traffic routs to the other channel, while in the previously mentioned systems that use one channel only, goes down when this channel goes down. Moreover it enhances the security and the delay transaction time, by applying the critical commands to SSH and transmit the non-critical ones without SSH.

Table 4.3: Comparison between the presented work and related works

Algorithm	Description	Advantages	Disadvantages
Fagin, 2008	Tries to increase the information related and cryptography products of security confidence	Aims to meet the information technology security evaluation common criteria	Do not solve the skepticism and it do not deal with the media connection that transfer the data.
Bhargav and Spantzel, 2007	It concerns user centricity management , and provides a taxonomy for management identification	Minimizes the redundancy and consistency	It concerns only internet transfer
Bohli, 2010	It uses common model for establishing public key, and keep the security in single malicious participant	It has variance of key establishment The model is secure in the sense of strictest	It ensures security only in single malicious participant not completely achieve requirements that is retained to it It concerns only on internet transfer
Tafaroggi, 2011	It aims to enhance the CDMA security systems via application of the algorithmic cryptography in the code	Handles 3G communication Handles multi-user	It only based on CDMA and cannot be expanded to different topologies. It consider single media transfer only
Pistoia, 2007	It concerns software system security though access control and information flow	It handles the access security by software only, thus, reduce the cost and complexity	It considered statistical analysis and design, but the statistics has no rigid security scheme It handles single media transfer only
Presented	It concerns on software security by software encryption / decryption algorithm and hardware control, by providing double transfer media; internet and mobile communication	It handles the security by software and ensure the sustainability of transfer medium through double transfer media Math model	

The main contribution of this work is the use of two channels, which are the Internet and the GSM SMS, this system enhanced the reliability of previous systems such as the Internet only systems or the GSM only systems. This proposed system decreased the

probability of the downtime of the entire system, such as when one channel goes down the traffic routs to the other channel, while in the previously mentioned systems that use one channel only, goes down when this channel goes down.

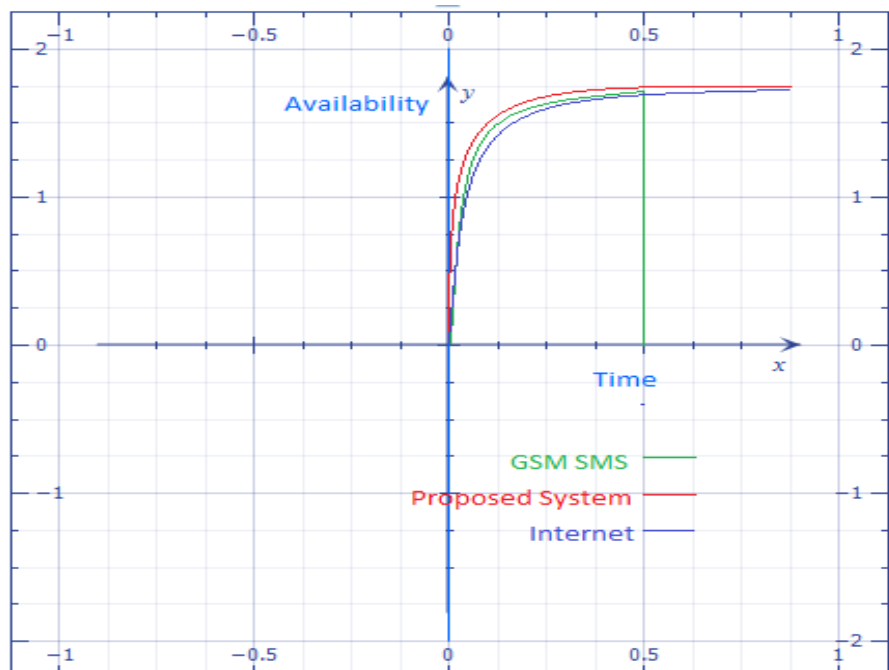


Figure 4.5: Reliability of the proposed system

Figure 4.5 shows the stability and availability of the proposed system. Initially the system used the GSM SMS channel, however, when this channel went down, the system quickly routed the traffic to the Internet channel; this allowed the system to remain up all the time. Then when the GSM SMS channel returns up, the system will return to use it to transfer the traffic.

On the other hand, the system in the figure 4.6 uses one channel only, and as shown in the figure, when this channel went down, unlike the proposed system, this one channel system goes down entirely, whether this system uses the Internet channel or the GSM SMS channel.

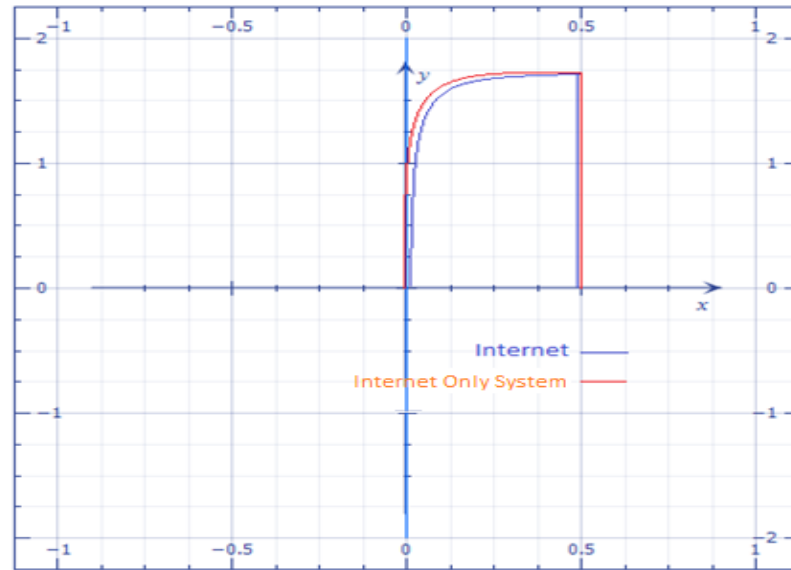


Figure 4.6: Internet only system

After applying this system on the Simulink several scenarios were conducted, in order to obtain the accurate results and evaluate the system. The table below summarizes the scenarios and their results.

The system was simulated on Simulink to deal with full message where the measurements consider that in the proposed security algorithm. However, there is no

significant time between transferring two messages, one of them is 1 character and the other is larger such as 160 character. The difference falls into milliseconds only.

In case of not receiving the ACK. from the sender (not changing the noise value). the transmission should be sent via GSM and the ACK received via GSM.

The simulation can show that when putting the value of ACK in the Internet as 0, this will turn the traffic through the SMS. Another scenario, when disconnecting the Internet it will turn the traffic to the GSM also. The GSM also work the same way.

To measure the encryption and decryption time, tic toc command was used before and after the algorithm. Different commands were used and tested, the average time for all of them is 1.40 sec.

Moreover the two channels simulation were tested several times to measure the full time of the algorithm with and without the security algorithm. The two analyses were studied on three laptops with different specifications.

Laptop 1:

- Dual Core
- Windows 7
- 2 G Ram

Laptop 2:

- Core I3.
- Windows 7

- 4 G Ram

Laptop 3:

- Core I5
- Windows 8
- 8 G RAM

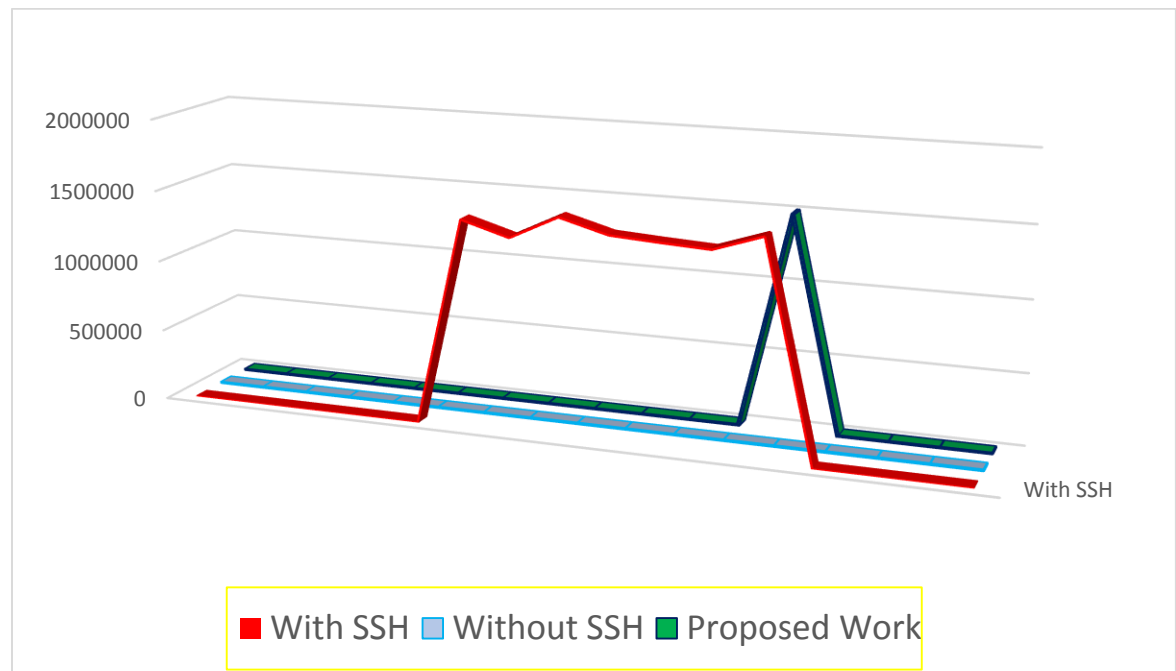


Figure 4.7 Results of applying a detection programs on test pattern of the encrypted message

Table 4.4: Experimental Results Comparison

No. Sample Messages Sent		No. of Text which are Received and Successfully Decoded and Separated		Success Rate		Failure Rate	
(Mousumi, 2010)	Proposed Work	(Mousumi, 2010)	Proposed Work	(Mousumi, 2010)	Proposed Work	(Mousumi, 2010)	Proposed Work
30	30	29	30	96.67%	98.20%	3.33%	1.80%
20	20	19	20	95.00%	97.00%	5.00%	3.00%
25	25	24	25	96.00%	98.90%	4.00%	1.10%
Average				95.89%	98.03%	4.11%	1.96%

From the obtained results, it noticed that the proposed system is more reliable than the system described by of Mousumi, (2010), because the proposed system uses two channels of transmission; and when where the primary channel goes down the secondary holds the traffic.

Chapter Five

Conclusion and Future Work

5.1 Conclusion

In the age of computer systems, Internet, and GSM mobile communications, the control of home devices and peripherals is much easier and cost efficient via communication networks rather than any new adapted or contributed methodology. Therefore, the adaption of common network home control system, should concentrate on different criteria; the permanent connectivity and the security. Hence, the Internet that is normally supplied by the local ISP is facing a lot of disconnecting and failure, the critical signals and messages may be loosed if it depends only on the Internet. The SMS services via GSM mobile communications are more rigid communication media than Internet, but in fact, it also has many failures and disconnects.

A double way control system in home automation for domestic services and smart buildings was implemented. The contributed systems are bases on both, GSM mobile communication in the package of SMS, in addition to local Internet services. Therefore, sending the control message to the smart home directly, that message will be sent by an established connection either GSM based SMS or even Internet based email. If the message sent successfully, the control action will been performed and the receiver device will acknowledge that message was received. In contrast, if the message does not reach the receiver for any cases such as failure in the communication, the other connection will be reestablish, and the control message will resent again.

This topology ensures reliable message transfer that lives in different environmental conditions and states, in addition to different server and host provider facilities. If the message received from source to the destination, then, the media problem is being solve. It

is the first contribution of this thesis.

On the other hand, the message that is being used to control home, it is capable to control factory, stock, or any critical complex. It is usually consider critical message and no one should hack it or interfere it. Therefore, the security of the transfer is very important issue. This thesis implements the security of the system using SSH algorithm. Enhanced the tradeoff between the security and the delay time by the contributed way of dividing the critical and non-critical commands.

After obtaining the results, it was clear that the commands without encryption were send in shorter time than those with encryption. This is solve by categorizing the commands into two groups, one that needs security to send them encrypted, and the other that needs to be sent in shorter time, which does not need an encryption algorithm.

5.2 Future Work

Future modification that could be suggested is to develop a common structure of the control command in a standard form to with header and expandable message format in order to make it usable in different environments with different applications and communication protocols.

Fault tolerance also, this encasement implies, the addition of other servers, to have two servers, at least, in order to enhance the reliability of the control server.

Moreover, this system could be enhanced by using the satellite services; in order to give more reliability of the system, in case both of the channels went down, the system uses the satellite service in order to remain up.

References

A. J. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon. (2011). Home Automation in the Wild: Challenges and Opportunities. CHI.

Anoh, O.O.; Ali, N.T.; Abd-Alhameed, R.; Jones, S.M.R.; Dama, Y.A.S. (2012), On the performance of DWT and WPT modulation for multicarrier systems, IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 348-352.

Bruce Schneier. (2008). The Blowfish Encryption Algorithm. Retrieved. <http://www.schneier.com/blowfish.html>

Chik, Z., T. Islam, S.A. Rosyidi, H. Sanusi, M.R. Taha, M.M. Mustafa. (2009). Comparing the performance of Fourier decomposition and wavelet decomposition for seismic signal analysis. European Journal of Scientific Research, 32 (3):.314-328

Chris Rapier, Benjamin Bennett.(2005). High Speed Bulk Data Transfer Using the SSH Protocol. Pittsburgh Supercomputing Center 300 South Craig Street Pittsburgh, PA 15213 1-412-268-4960.

C. Escoffier, J. Bourcier, P. Lalanda, and J. Yu. (2008). Towards a home application server .Consumer Communication & Networking Conference.

Escoffier, C.; Bourcier, J.; Lalanda, P.; Jianqi Yu. (2008). Towards a Home Application Server. Consumer Communications and Networking Conference. CCNC. 5th IEEE, vol., no., pp.321-325, 10-12 Jan.

E. Manhas, G. Brante, R. Souza and M. Pellenz. (2012). Energy-Efficient Cooperative Image Transmission Over Wireless Sensor Networks. In Proc. the 2012 IEEE Wireless Communications and Networking Conference : Mobile and Wireless Networks, Vol. 2, pp. 2014-2019.

Faisal Baig, Saira Beg and Muhammad Fahad Khan. (2013). Zigbee Based Home Appliances Controlling Through Spoken Commands Using Handheld Device. Federal Urdu University of Arts, Science and Technology, COMSATS Institute of Information and Technology, Val.7, No.1, PP.19-26.

G. Quéllec, M. Lamard, G. Cazuguel, B.Cochener, and C. Roux. (2010). Adaptive Nonseparable Wavelet Transform via Lifting and its Application to Content-Based Image Retrieval. Image Processing, IEEE Transactions on , vol.19, no.1, pp.25-35.

Hsiao-Han Chen, Yi-Bing Lin, Yingrong Coral Sung, and Ren-Huang Liou.(2010). Direction-based Wireless Remote Controller: A Smartphone Application, International Journal of Computer Science and Information Security, Vol.2, No.2, PP.33-47.

H.-S. Lee, (2009). A photon modeling method for the characterization of indoor optical wireless communication. Progress In Electromagnetics Research, vol. PIER 92, pp. 121-136.

I. Ahmad. Yakubu, A. Bagiwa, I. Abdullahi. (2011). Remote Home Management. World of Computer Science and Information Technology Journal, Vol.1, No.4, PP.144-147.

IEEE. Ieee 802.15.4 (2011). wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (lr-wpans). Technical report, Park Avenue, New York, USA: IEEE.

Alkar, A. Z., Roach, J., & Baysal, D. (2010). IP based home automation system. *Consumer Electronics, IEEE Transactions on*, 56(4), 2201-2207.

Jawarkar, N. P., Ahmed, V., Ladhake, S. A. & Thakare. (2008). Micro-controller based Remote Monitoring using Mobile through Spoken Commands. Journal of Networks, PP.58-63.

KakaliChatterjee, Asok De, and Daya Gupta. (2011). Software Implementation of Curve based Cryptography for Constrained Devices. *International Journal of Computer Applications*,24(5):18–23.

Kalaoja, J. (2006). Analysis of vocabularies for Amigo home domain. to be presented as a poster and published in the proceeding of 8th International Conference on Enterprise Information Systems 23 - 27, Paphos - Cyprus.

L. Bauer, L. Cranor, R. W. Reeder, M. K. Reiter, and K. Vaniea. (2008). A user study of policy creation in a flexible access-control system. InCHI.

Malik Sikandar Hayat Khiyal, Aihab Khan, and ErumShehzadi.(2009). SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security Software. *Engineering Dept*, Vol.6, PP.886-894.

M. El-Hadedy, D. Gligoroski, and S.J. Knapskog. (2008). High performance implementation of a public key block cipher-mqq, for fpga platforms. *Reconfigurable Computing and FPGAs. ReConFig'08. International Conference on*, pages 427–432. IEEE.

Mei, J., Li, S., Tan, X.: (2009). A Digital Watermarking Algorithm Based on DCT and DWT. In: *Proceedings of the International Symposium on Web Information*

Systems and Applications (WISA), Nanchang, P. R. China, May 22-24, pp. 104–107.

M. L. Mazurek, J. Arsenault, J. Breese, N. Gupta, I. Ion, C. Johns, D. Lee, Y. Liang, J. Olsen, B. Salmon, R. Shay, K. Vaniea, L. Bauer, L. F. Cranor, G. R. Ganger, and M. Mousumi, F., & Jamil, S. (2010). Push Pull Services Offering SMS Based m-Banking System in Context of Bangladesh. *Int. Arab J. e-Technol.*, 1(3), 79-88.

K. Reiter. (2010). Access Control for Home Data Sharing: Attitudes. Needs and Practices. CHI.

LIU, B., & WANG, Z. (2010). Application of Office Automation Based on SSH Framework [J]. *Computer Technology and Development*, 1, 039.

M. Nasri, A. Helali, H. Sghaier and H. Maaref, (2010) Adaptive image transfer for wireless sensor networks (WSNs) In Proc. 2010 International Conference on Design & Technology of Integrated Systems in Nanoscale Era, Vol. 1, pp:1 – 6.

Murthy, M. V. R. (2008). Mobile based primary health care system for rural India. W3C workshop on Role of Mobile Technologies in Fostering Social Development.

N. Banerjee, S. Rollins, and K. Moran. (2011). Automating Energy Management in Green Homes. SIGCOMM Workshop on Home Networks (HomeNets).

N. Watthanawisuth, N. Tongrod, T. Kerdcharoen and A.Tuantranont. (2010). Real-Time Monitoring of GPS-Tracking Tractor Based on ZigBee Multi-Hop Mesh Network In Proc. the Electrical Engineering/Electronics Computer Telecommunications and Information Technology, Vol. 1, pp. 580-583.

N. Zeldovich, S. Boyd-Wickizer, and D. Mazieres. (2008). Securing distributed systems with information flow control. In NSDI.

O. Ardakanian, S. Keshav, and C. Rosenberg. (2011). Markovian Models for Home Electricity Consumption. SIGCOMM Workshop on Green Networking.

P. Rigole, C. Vandervelpen, K. Luyten, Y. Vandewoude, K. Coninx, and Y. Berbers, A component-based infrastructure for pervasive user interaction (2005) Proceedings of Software Techniques for Embedded and Pervasive Systems (Varea, M. and Cortes, L., eds.), pp. 1-16.

Patricio, G.; Gomes, L., (2009). Smart house monitoring and actuating system development using automatic code generation. Industrial Informatics. DIN2009. 7th IEEE International Conference on, vol., no., pp.256-261, 23-26.

Rajbhandari, S., Z. Ghassemlooy and M. Angelova. (2009). “*Effective denoising and adaptive equalization of indoor optical wireless channel with artificial light using the discrete wavelet transform and artificial neural network*”. IEEE-Journal of Lightwave Technology, 27(20): 4493-4500. DOI: 10.1109/JLT..2024432.

Rosmanith, H., KRANZLMULLER, D.(2010). “glogin - A Multifunctional, Interactive Tunnel into the Grid,” grid, Fifth IEEE/ACM International Workshop on Grid Computing, pp. 266- 272.

Rifat Shahriyar, Enamul Hoque, S.M. Sohan, Iftekhar Naim, Md. Mostafa Akbar & MasudKarim Khan. (2008). Remote Controlling of Home Appliances using Mobile Telephony. 1,2,3,4,5.Department of Computer Science & Engineering, Bangladesh University of Engineering & Technology, Vol.2, No.3, PP.37-54.

R. E. Grinter, W. K. Edwards, M. Chetty, E. S. Poole, J.-Y.Sung, J. Yang,A.Crabtree, P. Tolmie, T. Rodden, C. Greenhalgh, and S. Benford. (2009). The ins and outs of home networking: The case for useful and usable domestic networking. ToCHI, 16(2).

R. S. Manzoor, R. Gani, V. Jeoti, N. Kamel, and M. Asif. (2008). Implementation of FFT using discrete wavelet packet transform (DWPT) and its application to SNR estimation in OFDM systems. IEEE International Symposium on Information Technology, Kuala Lumpur, Malaysia.

Renal Struik. (2011). Cryptography for highly constrained networks. NIST - CETA Workshop.

Shish Ahmad, Mohd. Rizwan beg, and Qamar Abbas. (2010). Energy Saving Secure Framework for Sensor Network using Elliptic Curve Cryptography. IJCA Special Issue on MobileAd-hoc Networks, pages 167–172.

Sleman, A.; Alafandi, M.; Moeller (2009). Integration of Wireless Fieldbus and Wired Fieldbus for Health Monitoring. R.; Consumer Electronics. ICCE '09. Digest of Technical Papers International Conference on 10-14 Jan. Page(s):1 - 2

S. Prasanna Ganesan. (2010). An Authentication Protocol for Mobile Devices Using Hyperelliptic Curve Cryptography. International J. of Recent Trends in Engineering and Technology, 3(2):2–4.

S.Z.S. Idrus, S.A.Aljunid, S.M.Asi. (2008). Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1. PP 20-25.

W. Granzer, W. Kastner, G. Neugschwandtner, and F. Praus. (2006). A modular architecture for building automation systems. in Proc. 6th IEEE WFCS , pp. 99–102.

W.S.Elkilani, H.m.Abdul-Kader. (2008). Performance of Encryption Techniques for Real Time Video Streaming, IBIMA Conference, PP 1846-1850

Van Nguyen, T.; Jin Gook Kim; Deokjai Choi. (2009). ISS: The Interactive Smart home Simulator. Advanced Communication Technology. ICACT. 11th. International Conference on, vol.03, no., pp.1828- 1833, 15-18.

W. K. Edwards, R. E. Grinter, R. Mahajan, and D. Wetherall. (2011). Advancing the state of home networking. Communications of the ACM, 54.

W. Saad, N. El-Fishawy, S. EL-Rabaie and M. Shokair. (2010). An Efficient Technique for OFDM System Using Discrete Wavelet Transform. Springer-Verlag Berlin Heidelberg, pp. 533–541.

Xuan Hung Le, Ravi Sankar, Murad Khalid, and Sungyoung Lee. (2010). Public Key Cryptography - based Security Scheme for Wireless Sensor Networks in Healthcare. 4th International Conference on Ubiquitous Information Management and communication, pages 1–7.