psm

by Muhammad Sayuthi Mohd Sobri

FILE	PSM_2_REPORT_VERSION_UNFULL.DOCX (824.59K)		
TIME SUBMITTED	21-AUG-2014 09:41PM	WORD COUNT	13721
SUBMISSION ID	444943073	CHARACTER COUNT	78054

CHAPTER I

INTRODUCTION

1.1 Background of the Study

Today's digital age offers great opportunities to enhance industrial applications related to security by using the wireless communication technology. Ubiquitous wireless communication technologies including Bluetooth, Wi-Fi, Wibree, WUSB, and Zigbee, is gaining acceptance and growing popularities in most developing countries (Erasala et al., 2002). Wireless communication allowing interchange by providing an alternative access without physical wire connections. Thus, this brings a new resolution to a great qualitative and quantitative management of information (Bellido et al, 2010). The main focused of these wireless communication technologies are the enhancement of short-medium range in communication system to be integrated in mobile devices with low cost and less power consumption (Bellido et al, 2008).

In general, security is counted as major concern in any configuration of wireless networking. With wireless technology, radio waves can be easily grab out of the air. Therefore, precaution and preventive measure need to be carried out to ensure there is no signal intercepted while sending sensitive and private information. Same goes to Bluetooth technology, if the network are not fully secured, it vulnerable to any harm involving access control and spying (Dipak et al., 2013). However, since most mobile devices utilize a protected and secure Bluetooth connection that requires authorization and authentication before accepting data from an unknown device.

On top of that, Bluetooth is known as inexpensive technology that can be implemented for various types of application including access control applications. In specific, secure access control for real time door locking mechanism allows activation, authorization, authentication and validation of user (Bellido et al., 2008). According to Dipak et al., (2013), smart phones with Bluetooth-enabled can establish an alternative for the locking and unlocking operations for a door. Thus, this advanced technology has the potential to resolves any problems significance to door lock management.

1.2 Problem Statement

- **Lack of research in the area of door locking management especially in Bluetooth-based mobile application.**

  There is a lot of Bluetooth based mobile application in several field of study but lack of research in door-locks domain area. Bluetooth features which mainly used for exchange of data should reinforce in more advanced features such as door locking management.

- **Current technology required a manual action to lock and unlock the door**

  Most access control solutions are implemented via the use of conventional technologies. This includes keys, bar-coded swipe cards, and access pin code numbers. With this physical security control, it is possible that keys might get duplicate when granting access to new users.

- **Safety procedures taken for intruder is weak and less secured**

  Intruder or trespassing into someone else's property has becoming more crucial issue and it has been reported almost every day on the news. Thus, an intensive safety procedures and protocols should be taken include the use of wireless technologies to provide adequate protection. Wireless technologies like Bluetooth has the built-in security features that include authentication protocols, encryption of data link and

comprehensive security features to attain highest levels of confidentiality, integrity and authentication.

- **Most physical security measures for door-locks come with high cost and difficult to maintain**

  The protection that provide by physical security are costly and time consuming. Biometric locks and keycard locks tend to be expensive with associated cost to implement and maintain such physical control. It also involves complex procedures such as documentation, training, troubleshooting and on-going maintenance. Furthermore, key loss require high cost for rekeying of all affected door locks.

1.3 Aim

The aim of this project is to develop smart lock system that will lock or unlock doors remotely through Bluetooth mobile application. Through this project, the security is one of the major requirement to enhance the protection level of door locking management.

1.4 Objective

This project was built with several objectives as the following:

- To develop an autonomous smart lock system using Bluetooth-based mobile application that will enhance the existing security measures for door locks operation
- To facilitate the use of Bluetooth technology in access control application for locking and unlocking the door using mobile device.
- To minimize the usage conventional keys to lock and unlock the door

- To understand the concept used for keyless entry using Bluetooth based mobile application.

1.5 Project Scope

This project will focus on the use of Bluetooth technology in access control application with the purpose to remotely locking and unlocking the door. This system works with mobile device with Bluetooth enabled and android application installed on the device. The system will work as stimulation for the physical door that can be implement on any operating system together with java and Bluetooth platform.

In addition, the security modes for this Bluetooth enabled device has the functionality with authentication and encryption to establish connection link with the door. Key derivation by entering the Personal Identification Number or PIN pairing that will generate the Bluetooth authentication and encryption procedures. This will ensure only authorize user can access the system to lock and unlock the door.

1.6 Target User

The target user of this system are busy families members and individuals that has limitation to access the door for locking and unlocking using physical keys entry. On top of that, this system can be useful for user that wish to experience with an innovative wireless technologies to perform a remotely lock or unlock doors through Bluetooth mobile application.

1.7 Limitations

The following is the summary of limitations of this project:

- The system is only available in English version
- Environmental condition may affect the Bluetooth maximum range and connections.
- Bluetooth may require uses of battery power of particular device in order for this application to operate.

1.8 Expected Outcome

The following is the expected outcomes of the system:

- A Bluetooth-based mobile application for door-lock operations.
- Manage to lock and unlock the door remotely using mobile devices with Bluetooth enabled.
- Enable only authorize user can access the system for door-lock operation using authentication and encryption.
- Succeed to retrieve status from the system (door) to be delivered to user on their mobile device.
- Manage to utilize the encryption and decryption process via secret key-based to establish secure Bluetooth connection.

1.9 Significance

9

- Eliminates time and costs associated with managing keys and implementing key control policies for organizations.

- Locks cannot be easily broken, picked or tampered with enhancing physical security measures via Bluetooth based application.
- Easy and more practical rather than having to carry lot of keys that might get stolen or misplaced.
- Reduce the risk of losing or misuse of keys when keys falling into the wrong hands.
- Simply let family members or trusted people enter the code and later if needed this code can be changed.
- Ease of installation with keyless entry application that are just as simple to install as standalone traditional locks.

1.10 Project Timeline

The development of this project involved several activities and tasks that are required to be carried out. A Gantt chart is commonly used in project management that provides useful ways of showing activities (tasks and event) displayed against time. This also help organize and work out practical aspects of this project including the minimum time required it will take to deliver and tasks need to be completed before others can start. Figure 1.1 shows the Gantt chart indicates the project timeline of this project.

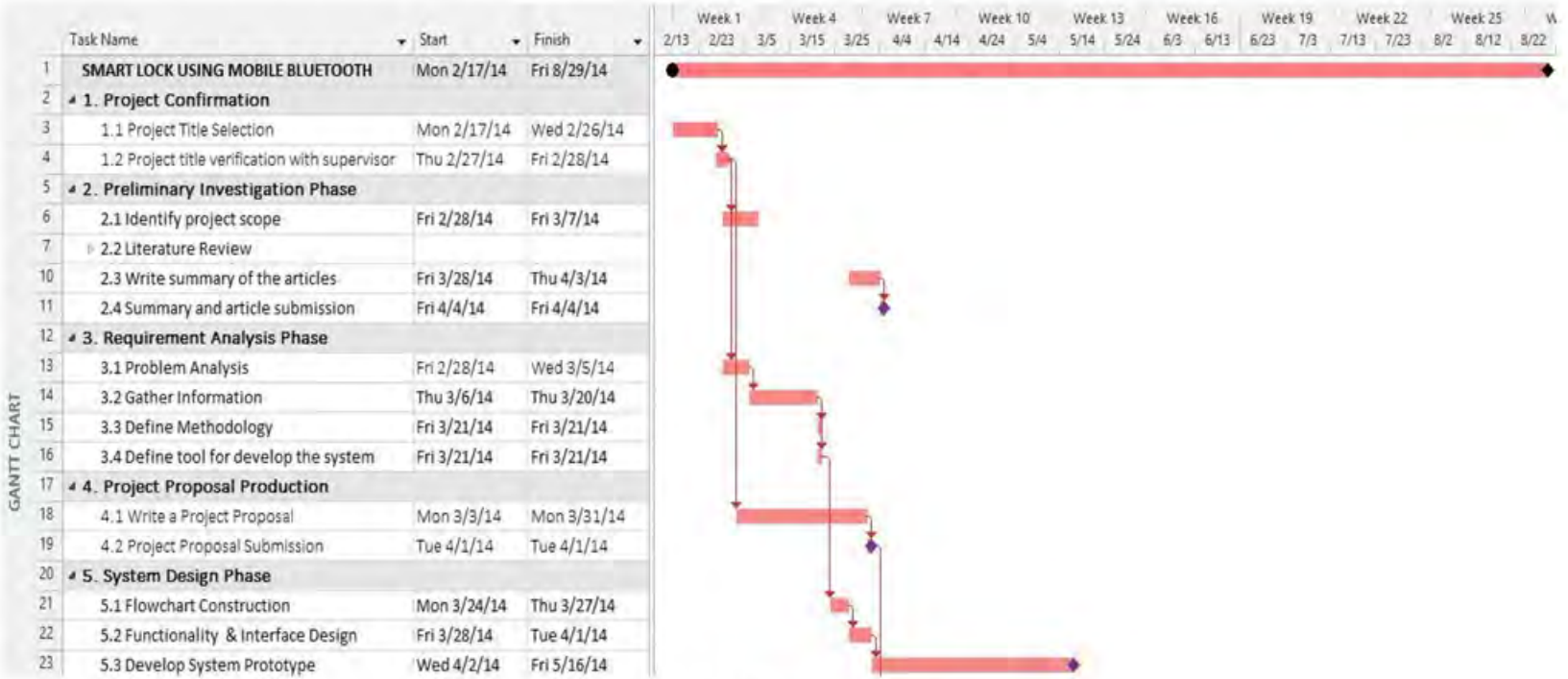
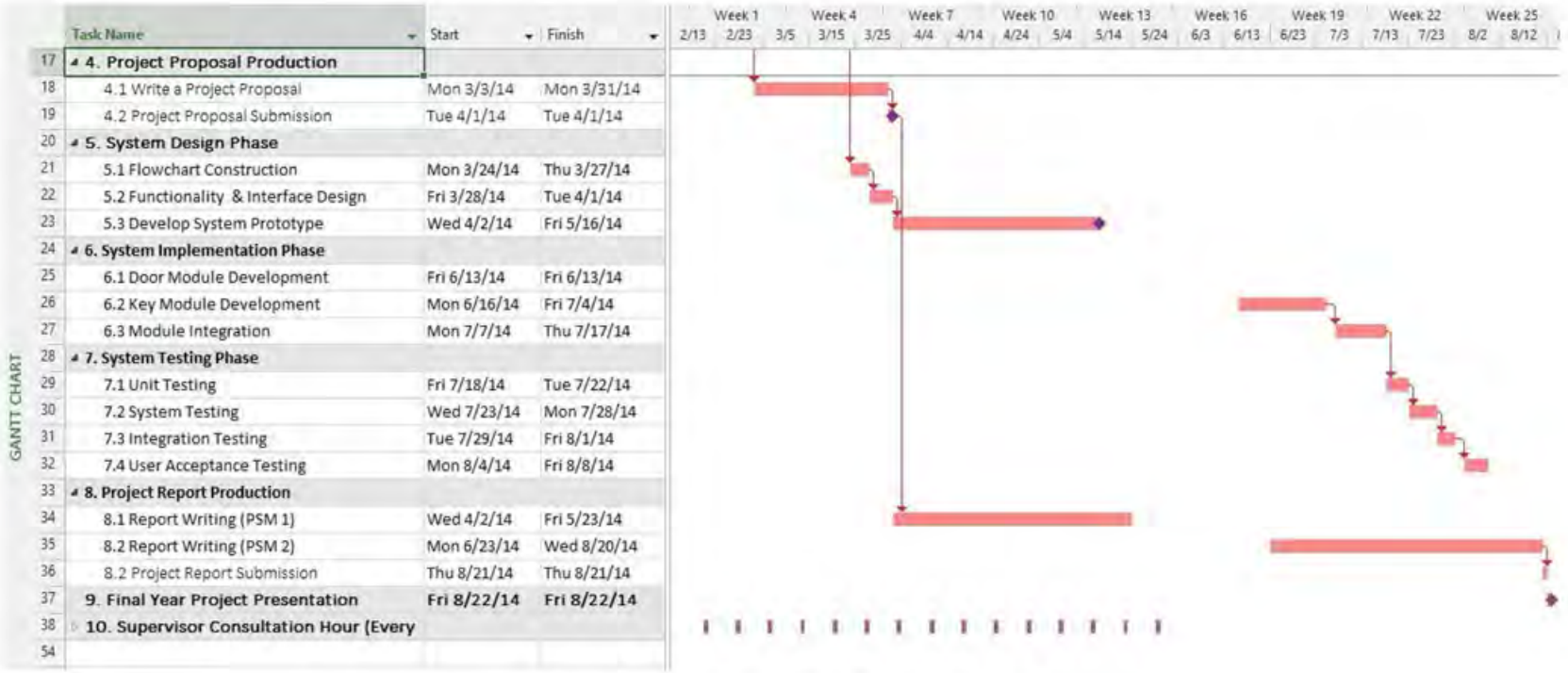


Figure 1.1: The Project Timeline



	Task Name	Start	Finish
17	4. Project Proposal Production		
18	4.1 Write a Project Proposal	Mon 3/3/14	Mon 3/31/14
19	4.2 Project Proposal Submission	Tue 4/1/14	Tue 4/1/14
20	5. System Design Phase		
21	5.1 Flowchart Construction	Mon 3/24/14	Thu 3/27/14
22	5.2 Functionality & Interface Design	Fri 3/28/14	Tue 4/1/14
23	5.3 Develop System Prototype	Wed 4/2/14	Fri 5/16/14
24	6. System Implementation Phase		
25	6.1 Door Module Development	Fri 6/13/14	Fri 6/13/14
26	6.2 Key Module Development	Mon 6/16/14	Fri 7/4/14
27	6.3 Module Integration	Mon 7/7/14	Thu 7/17/14
28	7. System Testing Phase		
29	7.1 Unit Testing	Fri 7/18/14	Tue 7/22/14
30	7.2 System Testing	Wed 7/23/14	Mon 7/28/14
31	7.3 Integration Testing	Tue 7/29/14	Fri 8/1/14
32	7.4 User Acceptance Testing	Mon 8/4/14	Fri 8/8/14
33	8. Project Report Production		
34	8.1 Report Writing (PSM 1)	Wed 4/2/14	Fri 5/23/14
35	8.2 Report Writing (PSM 2)	Mon 6/23/14	Wed 8/20/14
36	8.2 Project Report Submission	Thu 8/21/14	Thu 8/21/14
37	9. Final Year Project Presentation	Fri 8/22/14	Fri 8/22/14
38	10. Supervisor Consultation Hour (Every		
54			

Figure 1.1: The Project Timeline (continued)

1.11 Report Outline

This report outline is to give an overview of the major chapters involved during development of this project. The report is divided into three major chapters. The section below briefly describes on each chapter outline.

Chapter I: Introduction

This chapter introduces the background of the study, problem statement, aim, objectives, project scope, target user, limitations, significance, expected outcome, and project timeline.

Chapter II: Literature Review

Chapter two introduces Bluetooth and its concept with brief explanation on the topics and studies that are relevant to this project. The differences between Bluetooth and Other Wireless Technologies are discussed. Then, this chapter also cover comparisons on previous works/findings related with Bluetooth applications with Smart Lock Using Mobile Bluetooth.

Chapter III: Methodology

This chapter introduces various types of system development methodologies and also consists of knowledge acquisition and a thorough understanding and a usage of selected methodology for the system development and implementation. This chapter also includes the system analysis of the project.

Chapter IV: System Analysis & Design

This chapter covers the conceptual and technical design of the system. It covers the system architecture design, system functionality design, Data Flow Diagram (DFD), process flow chart and user interface design.

Chapter V: System Implementation

Chapter five discussed the overall processes involved in system development and implementation. It involves transforming of design into programming language and testing the system to assure the quality of the system and to fulfill the requirements.

The coding process begins at this phase whereby considerable amount of time is required for the system development. Therefore, the most important aspect of this phase will be the coding that is sets of sequenced instructions needed to run the system.

Chapter VI: System Testing & Evaluation

This chapter gives a brief description of testing and evaluation processes. It also involved the verification and validation of the software to ensure the effectiveness of the system and all functions work without any error or minimum level of error.

Chapter VII: Conclusion and Future Work

Chapter seven summarizes the whole system and discusses the limitation that exists in this project. This chapter also suggest future enhancements that can be incorporated into this system. The problem encountered during the development of the system will also be illustrated here. Finally, it ends with a conclusion of the whole project.

1.12 Chapter Summary

As a conclusion, this chapter has included the background of the study, problem statement, aim, project objectives, project scope, target user, limitations, expected outcomes, significance, project timeline and report outline. The main objective of this system is an autonomous smart lock system using Bluetooth-based mobile application that will enhance the existing security measures for door locks operation. It is hope that by creating the system, it will help and make a big impact in access control application using Bluetooth technology.

51

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

In a literature review of this project is very important as it places the project in the context of other projects which might have similar features and functionality. It can help the author to understand more the existing current systems features. The author can focus on learning the existing systems and enhance it to be more powerful and useful system.

2.2 What is Mobile Application?

According to Mobile Marketing Association (MMA), (2008), mobile application is defined as software application designed to runs on mobile devices such as a smartphone or tablet computers that perform certain tasks for the user of the mobile phone. Mobile applications are commonly on the most mobile phones that also known as downloadable, entry-level models and inexpensive. On top of that, mobile application is widely used due to the many functions performed by mobile application including

advanced services and entertainments, tools for downloading and reading blogs, providing user interfaces for basic telephony services and others (MMA, 2008). Thus, smartphones has gradually turned into multi-purpose mobile device with the dramatic increase in smartphone users that provide various mobile applications for their daily use (Adam et al., 2003).

Recently, an open source platform like Android Development Tools (ADT) has been widely used for developers to create and built new mobile applications for Android platform in Java (Chung et al., 2011). It is different from any other existing like iOS (iPhone OS) because of essential tools that it comes with which known as Software Development Kit (SDK) and also Application Programming Interfaces (APIs). In addition, Android platform has help to support Bluetooth network stack which provide a wireless communication in a sort range through Bluetooth enabled devices (Adam et al., 2003).

With the increasing number of mobile applications' developers and publishers, the higher quality and excellent products of mobile application can be delivered to its users (MMA, 2008). Thus, with an advanced wireless technology like Bluetooth that integrated with Android system, many mobile application are constructed and developed for the ease of people in modern and contemporary lifestyle (Min-Yan et al., 2013).

2.3 Bluetooth Overview

With the rapid development of advanced technologies, Bluetooth is one of the important wireless transferring technology that enables unlimited mobile communications between home, office and outside world (Naveen et al., 2002). Bluetooth technology was initially designed to support simple wireless networking of devices including cellular phones, personal digital assistants (PDAs), and wireless headsets (Salim et al., 2009). Nevertheless, technology of Bluetooth has been expose to various applications and effectively used in wide range of domain area such as personal

area networks, security specialization and others. According to Padgette et al., (2011), Bluetooth is known as a wireless technology standard for short-range wireless connection of radio frequency (RF) communication.

The main attributes offered by Bluetooth include ubiquitousness, low cost, and low power that can enhance security by automation of the operations and tasks that was previously controlled manually (Salim et al., 2009). The significant different between Bluetooth and other standards of wireless technology are the core specification of Bluetooth provides product developers both application layer and link layer definitions, that will assist data and voice applications (Bluetooth Special Interest Group [SIG], 2013). This fundamental strength of Bluetooth provides users with variety of innovation solutions include synchronization of mobiles phones and personal computers (PCs), hands-free headsets for voice calls, printing and fax capabilities and many more.

There been significant advancement in the field of access control, automation system, and security system by using wireless technologies. In specific, digital door lock for security and monitoring purpose has been found with the effective use of Bluetooth technology (Soo-Hwan et al., 2004; Tajika, 2003; Bellido et al., 2008). Bluetooth is invented by telecom vendor Ericsson in 1994 and its reveal to be potentially integrated with smartphones (Monson, 1999). According to Ming Yan et al., (2013), the main goal of Bluetooth technology is to allowing data to be exchanged wirelessly over relatively short-range distance using short-wavelength radio transmissions. With this technology, the conventional wired digital devices is transform into advanced wireless devices.

There are several versions of Bluetooth which are currently in use in trading devices. In year of 2003, Special Interest Group (SIG) of Bluetooth technology has released Bluetooth version 1.2 with data transmission speed up to 721 kbit/s. With adaptive frequency-hopping spread spectrum (AFH), which recovered confrontation to radio frequency interference by minimizing the use of crowded frequencies in the hopping sequence. Then a year later, Bluetooth version 2.0 was released. It is backward-compatibility the previous 1.2 version. The Enhanced Data Rate (EDR) was introduced for faster data rate. This 2.0 version has three times faster transmission speed up to 2.1Mbit/s.

Later on version 2.1 was adopted by SIG on July 2007. To allow better connection, this version provides more information during the inquiry procedure and uses sniff sub rating to reduce the power consumption in low-power mode. Then in 2009, Bluetooth version 3.0 was released and brought more speed in data transmission up to 24Mbits/s with the use of Wi-Fi connections. Next, the most recent version of Bluetooth 4.0 which features an essential strong power management skills of Low Power Consuming. It also enhance security level in data transmission compared to earlier version. Table 2.1 show the summary of data transmission rate of Bluetooth different versions.

Table 2.1 Summary of data transmission rate of Bluetooth different versions

Specifications	Bluetooth 1.0	Bluetooth 1.2	Bluetooth 2.0 + EDR (enhanced data rate)	Bluetooth 2.1 + EDR (enhanced data rate)	Bluetooth 3.0 + HS (high speed)
rate	721 kbit/s	721 kbit/s	2.1 Mbits/s	3 Mbits/s	24 Mbits/s
Adopted	2002	2005	2004	2007	2009
compatible		yes	yes	yes	yes
pairing		yes	yes	yes	yes
Adaption Layer (PAL)					yes
range			10 meters	10 meters	10 meters
Support 100m			yes	yes	yes

(Source from Bluetooth Special Interest Group [SIG], 2013)

2.4 Bluetooth Technology

The technology of Bluetooth allows data to be synchronize, permits mobile devices or computers to communicate with each other and establish high speed of Internet connection without cables or wires. Bluetooth technology can be separated into two major specification which are profile specifications and the core. The Bluetooth profiles specification concentrates on how to fulfill certain function that interoperate the devices using the core technology. Meanwhile, the core specification describes how the

technology works and operates in the usage model (Naveen, E., et al., 2002; Bluetooth

Profile **Usage model**

SIG, 2013).

Bluetooth SIG (2013) added that the core specification of Bluetooth has an essential features such as protocol stack, RF transceiver, and baseband. This will enables the interchange of several type of data classes and connection established on the devices. Most features provide by the core specification are optional and gives flexibility on the implementation of product. In 2010, a brand new name for Bluetooth Low Energy consumption named Bluetooth Smart Technology was introduced. This features was previously introduced and adopted from Bluetooth Core Specification. Bluetooth smart is a revolutionary technology that goes beyond simply application-friendly and also power-friendly. The technology is application-friendly in term of less cots and enhance application flexibility for creating Bluetooth Smart sensors applications that compatible with smartphones, tablets, or various consumer devices (Basil, 2012).

According to Malik, (2009), for Bluetooth profile specification, each devices must support at least one profile that will defined the particular messages and procedures from the Bluetooth specification. For instance, a mobile phone can communicate with another devices like headset if they have the same profiles. The main purpose of this profile being used is to reduce the problems related to interoperability among various consumer devices. Moreover, the profile is used by the Bluetooth certification authority to certify compliance and run a test. This is to ensure only granted permission that qualify the procedures defined in the profiles for the usage of Bluetooth logo to a specific products. Table 2.2 shows the list of several Bluetooth profiles and their usage model.

Cordless Telephony Profile (CTP)	To enable use of Bluetooth enable devices as cordless telephones
Dial-up Networking Profile (DUN)	To provide standard internet access and dial-up services over Bluetooth
File Transfer Profile (FTP)	To browse, transfer and manipulate of data as a whole file or folder
Headset Profile (HSP)	To enable communication of audio between Bluetooth devices
LAN Access Profile (LAP)	To enable Bluetooth device to have an access LAN, WAN or Internet via another physical connection to the network.
Message Access Profile (MAP)	To allow exchange of messages between several Bluetooth enabled devices.
Object Push Profile (OPP)	To enable data transferring over Bluetooth devices that follow the specification of the Bluetooth stack
Service Discovery Application Profile (SDAP)	To discover available services on any Bluetooth enabled remote device

Table 2.2 Bluetooth Profile and Usage Model

(Source from Bluetooth Special Interest Group [SIG], 2013)

2.5 Bluetooth Protocol Stack

In general, Bluetooth can be defined as layered protocol architecture involving core protocols, adapted protocols and cable replacement protocols. Figure 2.1 depict the core protocols with five-layer stack.

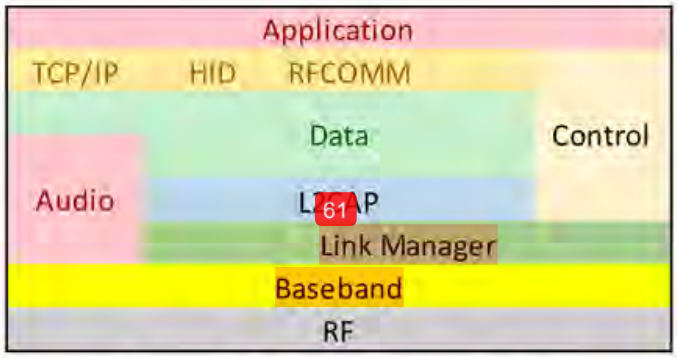


Figure 2.1 Bluetooth Protocol Stack

The following elements describes the five-layer stack of core protocols (Matt, 2008; Flynn, 2012):

- **Radio layer**

  Bluetooth generally work similar principles with other wireless technologies where data is transmitted over a radio frequency (RF) in the form of bits. The radio frequency assigned to Bluetooth is 2.4 GHz ISM (Industrial Scientific Medicine) band. The frequency band 2400 - 2483.5 MHz is used in most of the countries around the world. This radio layer specifies the air interface and frequency including the use of frequency hopping, transmit power and modulation scheme.

- **Baseband Layer**

  The baseband layer focusing on the protocols to establish connection within a piconet, channel codding, packet format, power control, addressing and timing. There are two type of connection established depending on the operating environment and type of application. These are an Asynchronous Connection Link (ACL) that emulate circuit switched connection for voice and data connection while a synchronous Connection Oriented (SCO) is defined for data bursts.

- **Link Manager Protocol (LMP)**

  This layer is performing establishment of link between Bluetooth enabled devices and ongoing link management. This protocols are important which includes security features to govern devices pairing, QoS, synchronization.

authentication and encryption, and the control and negotiation of baseband packet sizes.

- **Logical Link Control and Adaptation Protocol (L2CAP)**

  Responsible to adapt multiplexing layer to upper layer and also enabling adapts of upper layer protocols to the baseband layer. L2CAP gives both connectionless and connection-oriented services.

- **Service Discovery Protocol (SDP)**

  The SDP is defined as services available in the RF proximity and determine the attributes and features of those available services. The devices must have to support the same services in order to establish connection with each other.

RFCOMM is a cable replacement of transport protocol in Bluetooth specification that are used to emulate the RS 22 serial ports. In order to provide reliable in-sequence delivery of byte streams, RFCOMM has to rely on the Bluetooth baseband. Whenever physical serial port involved, the data rates of RFCOMM will be limited in the devices. The additional provisions of RFCOMM are as following (Bluetooth SIG, 2013):

- Remote port settings-Baud rate, parity, number of data bits
- Optional credit based flow control
- Parameter negotiation (frame size)
- Remote line status-break, overrun, parity
- Modern status-RTS/CTS, DSR/DTR, DCD, ring.

2.6 Bluetooth Network Topologies

According to Bisagni et al., (2002), the communication of Bluetooth has been possible by establish between a master device and slave devices. Any device has the potential to be a master or slave. This Bluetooth property has been useful for crating ad-hoc networks. Unlike WLAN, Bluetooth has special features that enable any Bluetooth enabled devices to communicate with other device in range by simply create a

connection between one of them as the master and the rest as slaves (Liron et al., 2002). The master is responsible to determine the pattern of frequency hopping based on its address. There are two type of topologies where the Bluetooth communication occurs that is Piconet and Scatternet.

2.6.1 Piconet

Piconet is the basic network topology via ad-hock network in which all devices have the same frequency hopping synchronization (Liron, et al., 2002). It contain collection of slave devices operating together and controlled by a master. A master is responsible to control and initiate the communication and to divide the whole bandwidth amongst the slaves by deciding when and how to communicate with each other. The slaves may request to become master when link is established (Basil, 2012). Each Piconet can have 8 units of active devices which include one master and seven slaves with the purpose to maintain high capacity link between all the units. One Piconet can be split into two Piconet by one slave becoming a master and this will cause the increase the aggregate throughput (Daniele et al., 2007).

2.6.2 Scatternet

Scatternet is the overlapping areas among multiple Piconet. A master can leave its own Piconet and join another Piconet as a slave. The main purpose of Scatternet is used to maximize the use of available spectrum (Basil, 2012). The hope sequence in Piconet is different while the entire unit of Scatternet share the same range of frequency with each other (Daniele et al., 2007). An effective way to optimize the capability of data transmission is to maintain the Piconet small (Basil, 2012). Figure 2.2 illustrate a Bluetooth Scatternet comprising of two Piconets (Liron et al., 2002).

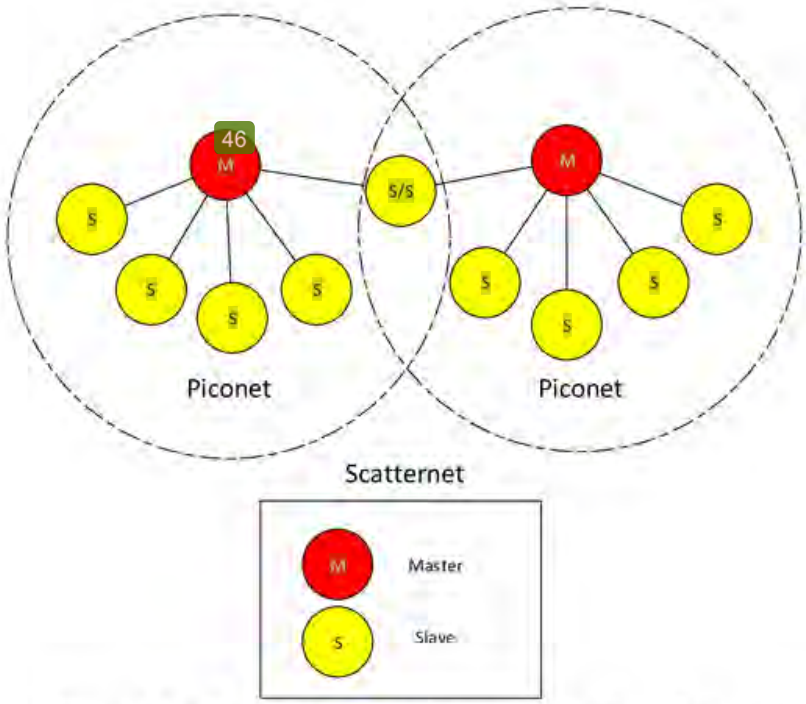


Figure 2.2 A Bluetooth Scatternet comprising of two Piconets

2.7 Bluetooth Security

The security is a major concern in any Bluetooth devices since they are commonly being used to communicate personal information through wireless technology. This will require for security functionality through the wireless solution (AU System, 2000). There are several security solution provided in Bluetooth specification include Pseudo-random frequency hopping, authentication and encryption (Mei, 2003).

2.7.1 Pseudo-Random Frequency Hopping

Pseudo-random frequency hopping is a method of radio transmission signal by rapidly change carrier amongst many Bluetooth frequency channels with intended for

noise resilience. This technique is a good way to avoid eavesdropping (Kaufman et al., 2009). Figure 2.3 shows how the Bluetooth channel frequency can change over time.

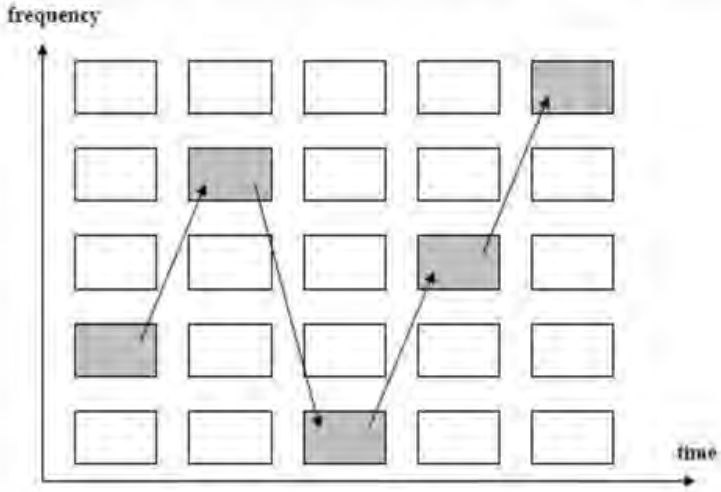


Figure 2.3 Bluetooth channel frequency changing pseudo-randomly

2.7.2 Authentication

Authentication is the process of proving one's identity (claimant) to someone else (verifier). The Bluetooth device authentication process is in the form of challenge-response procedures (Padgette et al., 2011). The following figure 2.4 illustrate the conceptual challenge-response verification process.

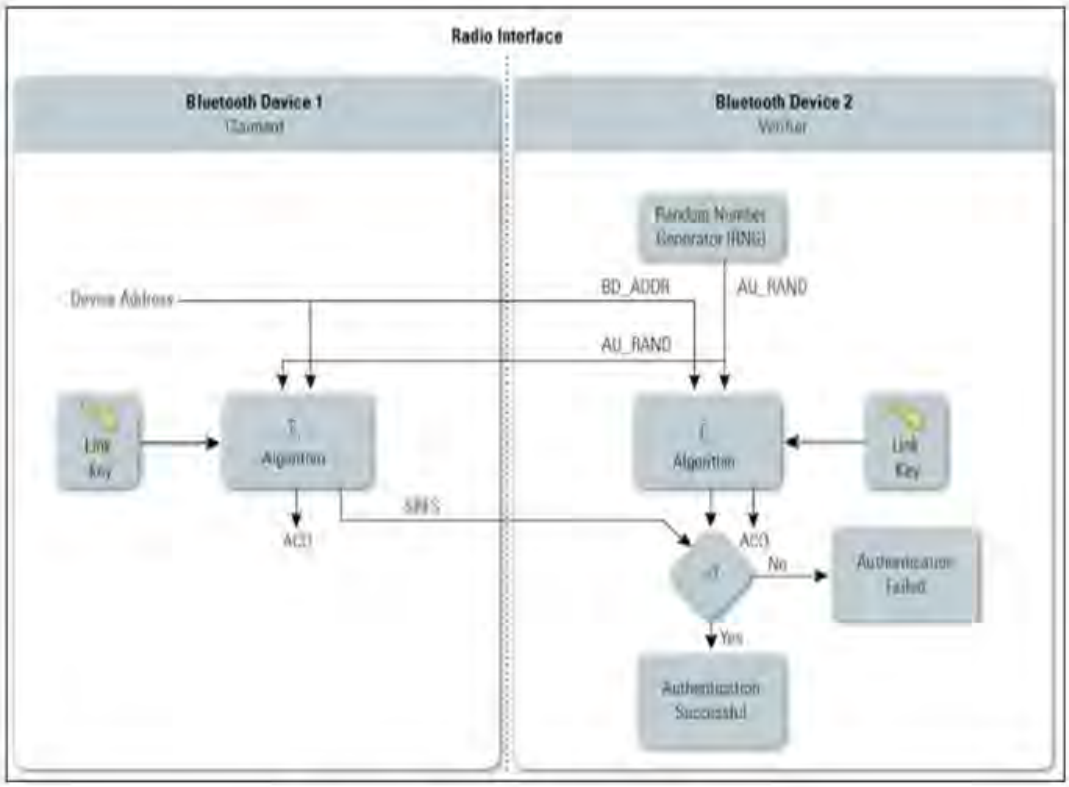


Figure 2.4 Bluetooth Authentication

The following steps are the Bluetooth authentication process involve as shown in Figure 2.4 (Padgette et al., 2011; Liron et al., 2002):

- **Step 1:** A 128bit random challenge was transmitted by the verifier to the claimant.
- **Step 2:** With the use of certain E_1 algorithm for computation, the claimant response to the authentication using his/her unique 48-bit Bluetooth device address. Then, the same computation will be performed by the verifier. The authentication process only use 32 most significant bits of E_1 output while the remaining bits will be used later as input to create Bluetooth encryption key.
- **Step 3:** The claimant return the 32 most significant bits of E_1 same as the response from the previous computation process to the verifier.

- **Step 4:** The respond from the claimant will be compared with the value that it computed by the verifier.
- **Step 5:** Authentication is considered as successful if the 32-bit values are equal meanwhile, the authentication is failed if the two 32-bit value are not equal.

By performing this authentication it has accomplishes one-way Bluetooth authentication. For mutual authentication, the steps mention above is repeated with the claimant and verifier switching its roles (Padgette et al., 2011).

2.7.3 Encryption

According to the National Security Agency (2007), Bluetooth ensures the data confidentiality across its medium through the encryption of the packets contents. Encryption is an optional features and only affects the packet payload. Bluetooth has four possible confidentiality modes though which an application can define the encryption requirements. The modes are as follows:

- **Encryption Mode 1**: specifies that no encryption is required on any type of traffic.
- **Encryption Mode 2:** requires that unicast traffic is encrypted using encryption keys based on individual link keys, but specifies that broadcast traffic is not encrypted.
- **Encryption Mode 3**: requires that both unicast and broadcast traffic are encrypted using an encrypted key based on master link key.
- **Encryption Mode 4:** specifies that encryption is required for all data, except for service discovery traffic.

In order to accomplish encryption process in the stream cipher system, Bluetooth SIG, (2013), has specifies three steps involve as shown in the following figure: