Bachelor´s Thesis (UAS)

Information Technology

Networking and Programming

2011

IDAHOSA AKHANOLU

IMPLEMENTATION AND SECURITY OF BLUETOOTH TECHNOLOGY

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS (UAS) | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme in Information Technology

November 2011 | 69 pages

Instructor: Ossi Väänänen

Idahosa Akhanolu

Abstract

Implementation and Security of Bluetooth Technology

Bluetooth is a wireless technology that has the capability of handling data and voice transmissions simultaneously. It makes use of its wireless nature to eliminate wired connections between portable devices within a specific or defined range without requiring a line of sight to communicate with each other. This range however, depends on the Bluetooth adapters or devices in use.

Bluetooth is an industrial standard that specifies a low power radio frequency solution to transmit and receive information between compatible devices.

This unlicensed technology is an industrial specification that is implemented in two parts; the core specification that examines how the adhoc network works, and the profile specification which defines the specific use of the wireless technology.

The aim of this thesis is to illustrate the processes of implementing Bluetooth technology and its security issues. This thesis work covers the operational functionality of Bluetooth core specification, analyzing and demonstrating the various use of its profile specification and scrutinizing Bluetooth security application.

Bluetooth wireless technology popularity is increasing rapidly due to its suitability of exchanging relevant information between mobile devices, however, security problems are the major challenges faced by the end users of this new technology.

KEYWORDS: Bluetooth Technology

Acknowledgement

I would like to express my gratitude to my instructor Ossi Väänänen for his support and guidance while writing this thesis and secondly, special appreciation to my degree manager Patrick Granholm for his encouragement and advice throughout the period of my study and during the thesis work.

Finally, I would also like to thank my parents and friends who also gave me their warmest support all through my project work.

TABLE OF CONTENTS

PICTURES

FIGURES

TABLES

Notations

AR_ADDR	Access Request Address
AP	Access Point
AM_ADDR	Active Member Address
A2D	Advanced Audio Distribution
ACL	Asynchronous Connectionless Link
API	Application Programming Language
A/V	Audio/Video
ARR	Automatic Repeat Request
BD_ADDR	Bluetooth Device Address
BRI	Bluetooth Radio Interface
CAC	Channel Access Code
DCE	Data Circuit-terminating Equipment
DLL	Data Link Layer
DTE	Data Terminal Equipment
DAC	Device Access Code
EDR	Enhanced Data Rate
ESCE	External Security Control Entity
FHSS	Frequency Hopping Spread Spectrum
GFSK	Gaussian Frequency Shift Keying
GAP	Generic Access Profile
GOEP	Generic Object Exchange Profile
HEC	Head Error Check

HCI	Host Control Interface
HID	Human Interface Device
IrMC	Infrared Mobile Communication
ISM	Industrial Scientific Medical
IBM	International Business Machine
IP	Internet Protocol
IAC	Inquiry Access Code
LMP	Link Manager Protocol
L2CAP	Logical Link Control and Adaptation Protocol
LAP	Lower Address Part
LAN	Local Area Network
MAC	Media Access Control
NAP	Network Access Point
NSAP	None-Significant Address Part
OBEX	Object Exchange
OUI	Organizationally Unique Identifier
PAN	Personal Area Network
PANU	Personal Area Network User
PDA	Personal Digital Assistant
PIM	Personal Information Management
PDU	Protocol Data Unit
QOS	Quality of Service
RFCOMM	Radio Frequency Communication

SDP	Service Discovery Protocol
SNB	Sequence Number Bit
SPP	Serial Port Protocol
SIG	Special Interest Group
SCO	Synchronous Connection-Oriented
TCS	Telephone Control Specification
TDD	Time Division Duplex
TCP	Transmission Control Protocol
TCS	Transport Control Service
UAP	Upper Address Part
WUG	Wireless User Group

1. INTRODUCTION

Wireless technology is becoming popular and offers wide ranges of advantages over traditional networks in connecting multiple devices together. Its communication is one of the most appreciated telecommunication media that is globally used by individuals, business organizations, corporations, educational and research institutions as well as governmental organizations all in various geographical locations. Bluetooth is a type of the wireless technologies that provides a short-range wireless connection for many kinds of supported and compatible communication devices.

The fundamental strength of this technology allows alongside the communication between Bluetooth portable and compatible devices to simultaneously exchange voice and data. This technology allows users to quickly and easily connect to ranges of devices like cell phones, computers, digital cameras, printers and other types of portable and compatible mobile electronic devices. The technology operates in a license free frequency band of 2.4GHz to create a connecting link between devices by transmitting signals through the low radio frequency and uses the band frequency hopping spread spectrum to reduce interference with other wireless technologies during band sharing by hopping to a new frequency after transmitting or receiving packets. This is due to the fact that some industrial, scientific, and medical (ISM) radio signals are built into small microchips that are integrated into electronic devices for wireless operations within a short distance of 10m and 100m thus boosting the radio power.

Despite the fact that the wireless technology is free and open to the public, the rules and regulations of its use are governed by the Bluetooth special interest group. This group comprises of over 1200 companies with Ericsson, Nokia, IBM Corporation, Intel Corporation and Toshiba as the founding and leading member companies. Ericsson and Nokia represent the European continent in the group, IBM and Intel represents the American continent while Toshiba represents Asian continent to see to the regulations and use of the technology.

This low cost wireless network technology was named after the Danish King Harald Blåtand (Harald Bluetooth in English) who united Denmark and Norway during the 10th century. The name was connected to the king hence the technology has the ability to unite people wirelessly.

This thesis work is grouped into 3 sections which focus on the-step-by-step implementation of Bluetooth technology and its security application. The first section emphasizes how the wireless network performs its operation using the various layers of the protocol stack to control and enhance communications in the core specification. The second part covers the profile specification which makes use of the comprehensive functionality of layers of the protocol stack to provide different Bluetooth applications that meet the standard requirements of its end users. The last part of the thesis deals with the security application of Bluetooth, the security vulnerabilities and threats associated with Bluetooth devices during their use and the possible ways to minimize or prevent them.

This thesis work also highlights the advantages the technology provides to different vendors of Bluetooth compatible devices by implementing the capabilities of the layers of the protocol stacks in providing various application models. Moreover, improper implementations during its design would cause the devices to become vulnerable to threats, but these defects must be quickly rectified when discovered to ensure safe use.

2. FUNDAMENTALS OF BLUETOOTH TECHNOLOGY

Bluetooth-enabled devices can communicate with each other in an ad-hoc network known as a piconet. A piconet is a Bluetooth network topology that comprises of up to 8 devices which includes a master and 7 slaves together in the topology. The master device synchronizes all the slave nodes, provides the clock and implements frequency hopping sequence in the piconet. The addressing scheme is designed in such a way that the master devices initiates the communication link, and then transmit data to one, some or all of the devices. A piconet in which only one communication link exists between the slave and a master is called point-to-point and this is the simplest scheme as it involves only two devices with one device as a master and the other device as a slave as shown in **Fig**.**a** on **Figure 2.0**

The second case is known as a point-to-multi-point link type of piconet as this involves several devices having one of the device as a master and the other devices as slaves shown in **Fig.b** below. In this case, there can be up to seven active slaves that can only communicate with the master but never with each other directly and the communication bandwidth is shared between the devices and they are well timed to avoid jam.

The third case is the inter-connection of piconets that result to a larger network known as scatternet which supports the communication between devices that exceeds 8 in number as shown in **Fig.c** below. In this case, a device can be a master in one piconet and can also be acting as a slave in the other piconet and such a device can be involved in relaying data between both piconets in the ad-hoc network. This capability provide the ability of the scatternet to be expanded by joining more piconets to form a very large one and the size of the network can be beyond the range of Bluetooth. In fact, this is one of the proposed future applications of Bluetooth to potentially interconnect numerous wireless devices via a Bluetooth internet and can be capable of using it for the interaction between devices and autonomous robots. The major limitation to the application of scatternet is the degradation of performance during collision that occurs through the frequency-hopping spread spectrum [6].

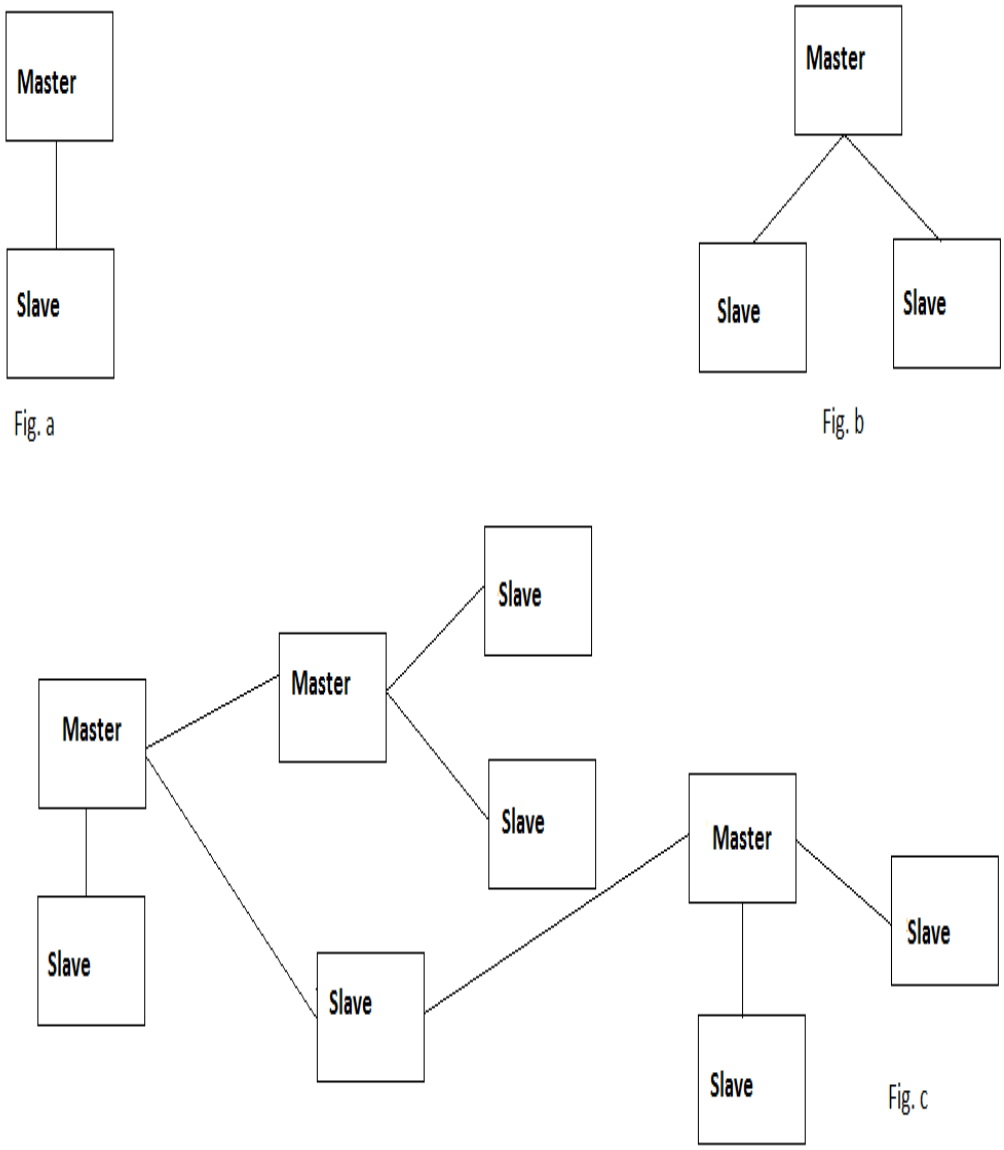


Figure 2.0 *Bluetooth Piconets*

2.1 Bluetooth Packets and Their Exchange

Bluetooth transmits data in packet format; the digital data are broken down into smaller packets from the source and are sent one by one to the destination. In a piconet, Bluetooth packets are sent directly to their destination master or slave from their source master or slave and these packets are transmitted one by one with the use of the frequency hopping system by using the advantage of time division duplexing (TDD) to provide an orderly exchange of data between master and slave in a piconet.

During transmission of packets, the destination master or slave checks each packet for data bit errors and requests the source master or slave for retransmission when errors are detected. In the case of digital voice packets, specific transmission time slots are assigned and repeat transmissions are not allowed. Packet information is sent in blocks with control and header information that enables the receiver to know the kind of information that is being sent and the order of transmission [5].

2.1.1 Bluetooth Links

Bluetooth specification can establish two different types of physical link between Bluetooth devices; these links are asynchronous connectionless link (ACL) and synchronous connection-oriented link (SCO). The former is used for data communication while the latter is used to support real-time voice and other multimedia traffic. In both cases, data and voice are transmitted in the form of packets and they can be sent simultaneously without jamming each other during transmission.

Asynchronous Connectionless Link

This is a point-to-point link that is established between a master and a slave in a piconet. In this type of link, the time between the creation of new packet at the source and the transmission of the packet to the destination is known as latency and it is more important than data integrity. In fact, latency ensures the transmission of scheduled packets in specific time slots and the packets are never retransmitted. On the other hand, excess of latencies can prevent communication between real-time two-way voice communications and in that case, a circuit-switch is needed to remedy the situation even if the voice communication can withstand a high percentage of bit errors.

Asynchronous connectionless link exchanges packets in pairs, that is, from master to slave and from slave back to the master [5].

Synchronous Connection-oriented Link

In this type of link, data integrity is more important than latency and packets are received with uncorrectable errors which are usually transmitted until they are free from error during packet switching. In an ACL master-to-slave time slot transmission, a slave can only transmit a packet to the master if and only if it was specifically addressed by the master.

This link can also be used for isochronous data transmission in which real-time two-way data are of less concern than data with timing issues, such as transferring streaming MP3 audio file that is playing during reception. In this case, the MP3 data is loaded to a buffer before playing which prevents sound interruption when some packets are retransmitted.

2.1.2 Packet Format

The general Bluetooth packet format is based on the capabilities of building the technology systems. There are three types of Bluetooth packet format which are: access code with 72-bits, a header with 54-bits and then a payload with information up to 2745 bits. The access code is used to signal other nodes that specify one of the following: Channel access code (CAC), Device access code (DAC) or Inquiry access code (IAC) and these access codes are divided into subgroups that contain a Preamble, a Sync word and a Trailer.

The header comprises of link information and has six various fields which are: Address field with 3 bits that provides address to one of the active member in a piconet; the 4 bit TYPE field provides specification to one of the four SCO packets or one of the seven ACL packets; the FLOW bit provides links for ACL, the Automatic Repeat Request use for signaling device that the transmitted data was received correctly; the Sequence Number bit ensures that data are put in a correct order and the Header Error Check field ensures that errors are checked properly in the header field.

The last part of the packet format is the Payload that comprises of a payload header consisting of 8- bytes to be transmitted to the payload body and the payload body consists of the data to be transmitted, while the cyclic redundancy check code field is used for checking errors in the payload.

ACCESS CODE	HEADER	PAYLOAD
72 Bits	54 Bits	0 – 2745 Bits

***Table 2.1.2**. Types of Packet Format. Source:[18]*

2.2 Bluetooth Specification

Bluetooth specification is the documentation of important information that provides detailed implementation of the wireless technology to make sure that all the Bluetooth devices can easily communicate with each other globally.

The documentation provided is used for product development to manufacture Bluetooth devices and content-centric applications for end users. However, the specification is split into two documents; the first part is called core specification that describes the base technology, that is, the way the technology works. Then, the second part is known as profile definitions which describe the particular use of the wireless technology for various applications by different manufacturers and to ensure interoperability between the different products [7].

2.2.1 Protocol Stack

Bluetooth protocol stack consists of the process of implementing the core specification. The stack provides services that control the core systems such as the modification of behavior and modes of Bluetooth devices, ensuring transport control services which create, modify and release traffic channels and links, and services that provide data submission and transmission over traffic bearers. Also, the stack ensures that Bluetooth devices can locate each other, exchange data and communicate with each other through different applications [13].

The protocol stack consists of different layers as shown in the diagram below.

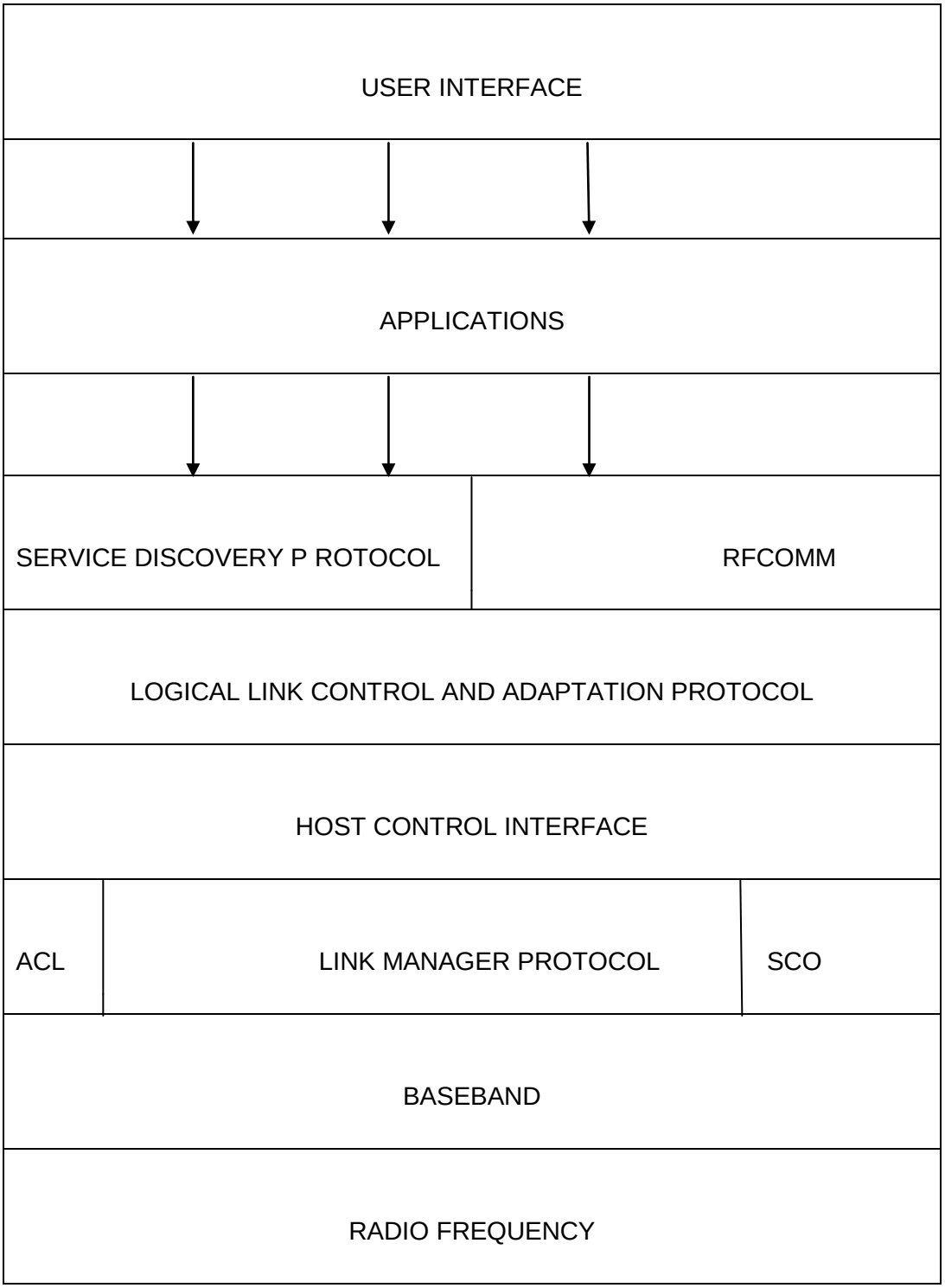


***Figure 2.2.1**. Different layers of protocol stack. Source:[21]*

Bluetooth Radio

In Bluetooth protocol stack levels, Bluetooth radio is the lowest layer that operates in a globally accepted ISM band of 2.4GHz. The radio band plays an integral part in the operation of Bluetooth devices that enables an electrical interface which is used for packet transfer by using its wireless modulated frequency system. More so, the radio layer defines the requirements and sensitivity levels of the radio transceiver that enable the process of using the frequency hopping spread spectrum and the power classification of Bluetooth devices. The devices power is classified into different classes and they are: power class 1 is used for bluetooth devices that use 100m long range with output power of 20dBm maximum; power class 2 is for used devices that use the standard range of 10m with a maximum power output of 4dBm; and power class 3 is used for Bluetooth devices that operate within a short range of 10cm with a maximum power of 0dBm and Bluetooth radio interface uses this as its antenna power.

The radio transceiver has a defined transmitter and receiver that are responsible for transmitting and receiving modulated electrical signals between Bluetooth devices. Moreover, the radio frequency modulation uses the Gaussian Frequency shift keying (GFSK) in which a positive frequency deviation is indicated as binary one and a negative frequency deviation is represented as zero.

Baseband Layer

The baseband layer is next to the radio frequency in the Bluetooth protocol stack which is also known as the physical layer. This layer is responsible for error correction, hop selection, Bluetooth security, data whitening and the management of physical channels and links control.

The baseband protocol implementation functions as a link controller that works with the combination of link manager to specifically perform routines such as linking connections with other Bluetooth devices, power control, flow control, synchronizing Bluetooth devices, controls address of the devices and channel control. Furthermore, baseband is also responsible for the management of both synchronous and asynchronous links, handling of packets and carrying out paging and inquiry for accessing and inquiring of Bluetooth devices within an environment through channel control.

Link Manager Protocol (LMP)

This is the layer that is next to the baseband in the Bluetooth protocol stack which is also known as data link layer protocol. Its enhancement includes link configuration and set-up, quality of service capabilities (QoS), security and security control, such as authentication and encryption control, power control and management of devices in different modes which include active mode, hold mode, park mode and sniff mode. More so, the link manager is also used for the negotiation of mode switching procedures and the master slave switch procedure.

The Link manager locates and discovers other link managers in other Bluetooth devices and links up with them through the link management protocol to carry out its functions. Nevertheless, the link manager responsibility also includes: establishment of asynchronous connection-less and synchronous connection oriented links, attachment of slaves to piconets as well as the allocation of their active member addresses and breaking down connections to detach slaves from a piconet when the connection is no longer needed.

Host Controller Interface (HCI)

The host controller interface is next to the link manager protocol which permits access to the baseband layer and link manager protocol for regulating and receiving information status through the provision of a command interface. This interface provides ways of accessing the Bluetooth baseband capabilities and configuration parameters.

The HCI exists in three parts. These are: HCI firmware which forms part of Bluetooth hardware, the HCI driver which is located in the software part of a Bluetooth device and the host controller transport layer which links the firmware to the driver. HCI firmware applies the HCI commands for Bluetooth hardware to access the hardware status registers, baseband commands, link manager commands and controlling registers and event registers. Afterwards, the HCI driver implementation is used in the host to exchange data and commands with the HCI firmware in the Bluetooth hardware. While the host controller transport layer implementation provides the tendency of transferring data without knowledge of the data [13].

Logical link Control and Adaptation Protocol (L2CAP)

The logical control and adaptation protocol is the layer that is above the host controller interface which is also known as data link layer that enables data to move from the higher layers and from the application layer of the Bluetooth protocol stack to the lower layers of the stack. This permits higher level protocols and applications to transmit and receive upper layer data packets that are up to 64 kilobytes. It enables the provision of data services to the upper level host protocols with protocol multiplexing capability, segmentation and reassembly tasks and group abstractions.

This link layer provides both connection-oriented and connectionless data services to the upper layer protocols and enhances per-channel flow control and retransmission through their modes.

Radio Frequency Communication (RFCOMM)

This is a protocol that is next to the L2CAP which links the layer to the lower layer in the Bluetooth protocol stack. RFCOMM provides the emulation of serial cable line setting and status of an RS-232 serial port that provides serial data transfer and supports legacy serial-port applications. In the communication between two Bluetooth devices, RFCOMM can supports up to 60 simultaneous connections and the number of connections that are simultaneously used in a Bluetooth device is implementation-specific.

RFCOMM complete communication path requires two applications that run on various devices having a communication segment between them. However, this protocol can accommodate two types of devices and they are:

Devices type 1 - These are Bluetooth wireless communication between devices like computers and printers.

Devices type 2 - These are types of devices which are part of communication segment, such as a modem.

The protocol can accommodate both types of devices and can support the information transferred between the two entities. In some cases, some information is only required by devices type 2 while other information is required to be used by both types.

Service Discovery Protocol (SDP)

The Service Discovery Protocol is the part of Bluetooth protocol stack that is used for the provision of available services to Bluetooth devices and also responsible for determining the characteristics of those available services in a Bluetooth environment. SDP performs its function by implementing a request/response model which is a process in which every transaction contains one request and response protocol data unit (PDU).

In another case, SDP relies on L2CAP links establishment to provide information of available services between the SDP server and client. The SDP server is a Bluetooth device used for the provision of services to other Bluetooth devices and has its own database for storing information of services rendered to its clients. SDP clients are those Bluetooth devices that use the services provided by the SDP server. However, there are some cases where devices can simultaneously be SDP servers and clients.

2.3 Bluetooth Addresses

Bluetooth addresses are plaintext names used for addressing Bluetooth devices. The addresses are in the binary number system which are represented in hexadecimal form, but are given a plaintext names for easy and better interface for human applications. The four types of addresses that can be assigned to Bluetooth devices are: Bluetooth device address (BD_ADDR), active member address (AM_ADDR), park member address (PM_ADDR) and access request address (AR_ADDR) [5].

The BD_ADDR has a 48-bit unique device address which is allocated to each Bluetooth transceiver. The device address consists of a 24-bit lower address part field (LAP), a 16-bit none-significant address part field (NAP) and a 8 bit upper address part field (UAP).

The LAP and UAP fields are used for piconet identification, paging Bluetooth devices and generating frequency hop set. The NAP field is used for Bluetooth hop channel set and also used for Bluetooth security application. More so, the NAP and UAP fields combine their bit to form a 24- bit entity known as company_id which is assigned as an organizationally unique identifier (OUI). The 24- bit LAP is company_assigned which is appended to the company_id to form BD_ADDR. Moreover, a company_id can be used to support over sixteen million Bluetooth devices and the total 48 bit BD_ADDR field is

big enough to the extent that each individual on earth can own over fifty thousand Bluetooth devices in the world.

Then, AM_ADDR is a 3-bit address which is assigned to slaves by the master in a piconet. The master uses this address space to address individual slave instead of using the 48-bit BD_ADDR that would consume a lot of transmitting time for the same purpose. The AM_ADDR is used to assign an address to each of the seven (maximum number of slaves in a piconet) slaves in a piconet using the bit values from 001 to 111 and reserving the 000 bit for broadcasting packets from the master to multi slaves. The AM_ADDR is sometimes called the Bluetooth unit MAC address.

While PM_ADDR is an 8-bit address field that can be assigned to up to 255 parked slaves. In a piconet, the maximum number of active slaves is seven, but there can be up to 255 parked slaves that are not active and are synchronized to the master´s packet timing and hop sequence and the parked slaves periodically listen for broadcast packets from the master. The master uses PM_ADDR to park an active slave and can used it to unpark the slave to be active again.

Also, AR_ADDR is assigned by a master to park a slave and the address is used by the slave in determining its access space for sending an unpark request to the master. This is regarded as the most powerful feature in the organization of Bluetooth piconet which is the ability of parked slaves to request an unparked command from their master.

2.4 Operational Procedures and Modes of Bluetooth

Bluetooth operational procedures and modes are applied to the various layers of the Bluetooth protocol stack used for different connections and communications between Bluetooth devices. Operational procedures are used to offer communications between devices in a piconet while the operational modes are used to connect Bluetooth-enabled devices together and for exchanging data with them. The operational procedures and modes that are used in an ad-hoc Bluetooth wireless technology are: the Inquiry procedure, Paging procedure, Active mode, Hold mode, Sniff mode and the Park mode.

The inquiry procedure is an asymmetric procedure used for enabling a device to search and discover devices that are in range, and then determines the addresses and clock for such devices. The procedure makes use of a special physical channel for inquiry

requests and responses. In fact, an inquiry device is a Bluetooth-enabled device that has the ability to discover other nearby devices and while discoverable devices are those devices that are available to be found by listening to inquiry device requests and sending responses to them.

Paging procedure is the process that uses a Bluetooth-enabled device address to establish an actual connection that follows immediately after the inquiry procedure. The device that is responsible for the page procedure will automatically be the master of the connection and has the knowledge of clock estimate to be able to set up the connection. The connectible devices make use of a special physical channel to listen and wait for connection request packets from the connecting device.

Active mode is a process of connection state in which Bluetooth enabled devices participates on the connected channel. The source master is responsible for scheduling the transmission that is based on traffic demands to and from the various destination slaves. In a Bluetooth piconet, active slaves listen and respond to master-to-slave slots for transmission packets and an active slave may become less active if and only if the slave is not addressed by the present master and then wait for the next new master to transmit packets.

The hold mode is a connection state in which synchronized devices in a piconet is entering power saving mode to reduce their transmission activities. In this process, the master source can put the destination slave on hold mode by running only its internal timer. In some cases, the slave can even request the master to put it on hold and data transmission will restart immediately after the slave hold mode expires. The hold mode has the medium power-saving efficiency of the three power-saving modes.

Sniff mode is another power-saving mode connection that reduces the transmission activities of synchronized devices in a piconet. The slave uses the sniff mode to listen to the master in the pconet at a lower rate by reducing its duty cycle. The sniff mode has the least power-saving efficiency of the three power-saving modes and its interval is programmable depending on the application.

The Park mode is another connection state whereby synchronized devices in a Bluetooth piconet do not participate in traffic transmission. Parked devices sometimes listen to the source master for re-synchronizing and checking for broadcast messages. This mode has the highest power efficient among the three power saving modes.

3. BLUTOOTH PROFILES

Bluetooth profiles can be defined as the general applications of Bluetooth technology and they also describe how the wireless technology can be used for specific devices. These profiles provide a minimum set of characteristics that allow communication between Bluetooth-enabled devices and are implemented to describe and support the functionality of end users models. Bluetooth device manufacturers make use of the underlying capabilities of the Bluetooth protocol stack to provide the end users of the devices with the ability to perform their various users' model functions. The device manufacturers do utilize the protocol stack features to define each profile depending on the feature requirements of the stacks and also provide the usage model. The stack provides an application programming interface (API) which defines the various profiles to achieve the user interface expectations. In general, the API enhances common operations that are viewable by the different manufacturers of Bluetooth-enabled devices and such operations include the following:

- Transmission and monitoring of events and exchanging of messages through the RFCOMM, L2CAP and SDP.
- Ability to use HCI or LM commands to simultaneously view and observe various operational data.
- Provision of protocol monitoring through the stack layers.

The application of specific Bluetooth profiles for the manufacturing of different products of Bluetooth-enabled devices is governed by SIG. Every manufacturer of these devices follows the SIG requirements to be able to achieve interpretability between the various manufactured Bluetooth devices. For one device to be compatible with another device, the two devices must have at least one of the same Bluetooth profiles.

Moreover, the minimum SIG requirement for a profile is its dependency on other profiles and its recommended user interface formats. The profiles are described by examining and specifying the implementation of the various features of the protocol stack. These features are assigned to profiles according to the following conformance requirements:

M: Mandatory implementation of certain features to conform to that particular profile.

O: Optional implementation of certain features to conform to that particular profile.

C: Conditional implementation of certain features based on performance criteria.

X: Excluded feature that is implemented based on its support, but never used in that profile.

N/A: Not Applicable feature to that particular profile.

The bluetooth profiles have a set of specifications that is categorically defined and classified into various groups. Such are the profiles that are based on Generic Access profile (GAP), Telephony profiles (3-in-1 model) that are based on Cellular telephone, Cordless Telephone and Intercom profile, profiles based upon Serial Port Profile (SSP), and the profiles based upon Generic Object Exchange Profiles (GOEP) [2].

3.1 Generic Access Profile (GAP)

The generic access profile forms the foundation of all profiles which defines the connecting mode procedures used for link management of Bluetooth-enabled devices, idle mode procedures for discovering other Bluetooth devices, and the security procedures that are applicable to various security levels of Bluetooth devices. In fact, the GAP is conformable to all other profiles and applicable for naming and addressing devices. Basically, two Bluetooth devices from different manufacturers should be able to connect to each other, hence they both support the GAP and even though they are not compatible or share any applications in common. The GAP is also responsible for specifying the required parameters needed in the user interface level such as the use of names and their definitions, values and coding schemes. The following applications are based upon the GAP usage models;

- Advanced Audio Distribution (A2D)
- Audio/Video Remote Control
- Video Distribution
- Hardcopy Cable Replacement
- Human interface Device (HID)
- Personal Area Networking (PAN)

The A2D usage model describes the process of distributing high quality mono or stereo audio content from the source (SRC) through an ACL channel to a sink (SNK). This profile defines the procedures for establishing, controlling and distributing of the streaming audio from the SRC to the SNK. The distribution of the streaming audio can only support point-to-point link, but cannot support the synchronized point-to-multipoint link. In the usage model scenario, the SRC device is the Bluetooth-enabled device that provides the digital audio stream which is delivered to the SNK. An example of such device is an MP3 player, while the SNK device is the Bluetooth-enabled device that receives the digital audio stream from the SRC and such example is a wireless headset. Some other Bluetooth-enabled devices that use A2D are mobile phones, stereo speakers, stereo adapters and many more.

Audio/Video Remote Control usage model provides a standard interface used for interpretability between Bluetooth-enabled devices by controlling their audio and video through A/V distribution commands. The interface provide the manipulation of action that is translated to the A/V control signal and sent by the controller to the targeted Bluetooth enabled devices. The controller is responsible for controlling the characteristics of streaming media such as volume control, starting, stopping, forwarding, playback, pausing and other remote control operations. Those controlling devices include mobile phone, personal computers, remote controller, personal and digital assistant while targeted devices can be a television set, headphone, amplifier, video monitor and audio or video player/recorder. This usage model also provides optional link-level security, but security authentication and encryption is mandatory.

The video distribution usage model offers a process that is intended to be used for streaming video between two Bluetooth-enabled devices. The combination of this and A2D can be used to send video with sound over a Bluetooth link. For video streaming, it can be used to stream a live video from a digital video camera to a home theater system.

Hardcopy Cable Replacement involves the process of a client-to-server communication in which the client, such as a laptop, is sending data to a server such as a printer. The purpose of this is to provide a simple wireless connection which is an alternative to a cable connection between devices like a laptop and a printer. In this case, data are

transferred through the driver on the client device and the profile does not support printing of pure images.

HID defines the process of describing the protocols, procedures, and features needed to operate Bluetooth-enabled human interface devices used by humans to control computer systems. Such HIDs include keyboard, mouse, joystick and other pointing devices. There are also other front-panel controls such as switches, buttons, sliders and knobs, so are complex gaming input/output devices such as special gloves and flight stimulator controls. On the other hand, there other HIDs which do not require human interaction, such as bar code readers. One of the usage scenario is using HID profile for conference room presentations which is controlled conveniently by using a Bluetooth-enabled HIDs to enable the presenter to conveniently move around the room during presentation instead of getting closer to the projector or the computer.

Bluetooth PAN is an ad-hoc network technology which is used for the creation of a wireless Ethernet network between devices such as personal computers, mobile phones and other numerous portable devices. The PAN gives wireless network access to all the Bluetooth enabled devices and computers that are connected to it. During a PAN connection, a transmission control protocol (TCP) and internet protocol (IP) is automatically created between computer and Bluetooth enabled devices or other computers. The profile is implemented by connecting to devices such as the personal area network user (PANU) device for the creation of an ad-hoc network that involves the personal computer and the device, the group ad-hoc network (GN) that involves a computer, the GN device and any other PANU devices which are connected to the same GN device and the network access point (NAP) device is used to connect the computer to a larger network like the Internet.

3.2 Telephony Profiles Based on 3-in-1 Model

The Telephony profiles are based on a 3-in-1 usage model which involves the ability of a single wireless phone to be used for three functions which are a cellular telephone, a cordless phone and an intercom. The function of the cellular is not Bluetooth enabled, while a profile exists for cordless and intercom which are based on a usage model of Telephone Control Specification Binary (TCS-BIN-Based). Moreover, the piconet of this network between devices does not necessary make use of master and slaves devices, but it rather uses the terminology of incoming and outgoing calls between the network and the user. The TCS usage model performs various functions such as call control,

group management and connectionless TCS. The call control is a process in which the LM established direct communication and release of SCO voice and data are used for point-to-point signaling calling process, such as making an outgoing call from a Bluetooth enabled mobile phone to a recipient. Then, the group management is used for the management of point-to-multipoint signaling of a group devices that are participating in a group call such as a base station that alerts other phones of incoming calls in the same range that is within the wireless user groups (WUG) and the connectionless TCS which involves the ability to exchange data or information between Bluetooth enabled devices without a call. The TCS functions are based on the following user models:

- Cordless Telephony
- Intercom

The Cordless Telephony is an implementation process in which a Bluetooth-enabled device can be used as a typical short-range cordless telephone. The authorization of phones from different manufacturers using this profile is able to communicate with any Bluetooth-enabled base station. This profile can be applicable to a cordless phone or a mobile phone that functions as a cordless phone when close to its base station. In the user scenario, mobiles phones are be able to use the Bluetooth gateway of the cordless telephone connected to an existing landline within the range of a home and can be connected to a mobile network when out of range of a home.

Intercom implementation is based on the symmetric use of Bluetooth link that relies on SCO to carry the audio and it is known as a walkie-talkie 3-in-1 phone usage model. In this case, the Bluetooth-enabled devices do not have any specific defined roles and every participating device is called a terminal. All the terminals use the inquiry and page procedures to connect to each other. A user scenario is voice calls between two Bluetooth-enabled mobile phones. In this type of profile, security application is optional.

3.3 Serial Port Profile (SPP)

Bluetooth wireless SPP is an emulation of a serial cable that is intended to replace the existing Recommended Standard (RS-232) that includes control signals used for a connection between Data Terminal equipment (DTE) and Data circuit-terminating Equipment (DCE).The profile implementation is based on RFCOMM protocol that sets up a port between Bluetooth-enabled devices to transfer data. The serial port is used

for the connection of devices within a Bluetooth range of one hundred meters such as serial printers, scanners or other portable devices that support this profile and GAP. Apart from the exchange of data between devices, the SPP usage model is based on the following applications:

- Dial-up Networking (DUN)
- Headset
- Hand-free
- LAN Access

The DUN usage model defines the protocols and procedures of using an Internet Bridge to establish a Bluetooth link that provides access to the Internet and other dial-up services and such devices are modems and cellular phones. In this application, the gateway device provides access to the Internet such as the cellular phone and the data terminal device uses the dial-up services of the gateway such as a personal computer. The user scenario involves a computer using a cellular phone as a wireless modem to dial-up internet access for network and a personal computer uses a cellular phone as a modem to make a point-to-point calls

The Headset is used for implementing the ultimate headset which is a process that defines the protocols and procedures required to support the use of headset. The commonest devices that use this model are headsets, cellular phones and personal computers. A device's role can either be used as an audio gateway device for providing gateway input and output audio such as the cellular phone, or as a headset device that provides a mechanism acting as the audio gateway´s remote audio input and output such as the headset. Both the audio gateway and headset use the RFCOMM to provide the Bluetooth wireless serial port emulation to transport the user data and control the signals and commands from the headset to the audio gateway. A security authentication and authorization procedure is an optional application to this model depending on the agreement between the devices. However, a pin code will be required to create link keys between devices for security purpose.

The Hand-free is one of the SPP usage model that defines the requirements that are specifically used for automotive application. This implementation is directed to the operation of a phone through an in-car device. It requires the use of Bluetooth link to control the mobile phone via the built in-car hand-free device that is embedded inside

the car. The embedded hand-free unit wirelessly provides a full duplex audio input and output mechanism with the combination of voice recognition, noise suppression and echo cancellation to connect to a mobile phone through the Bluetooth link. Various manufacturers of automobile are implementing this features provided by the Bluetooth in-car kits that enable the users to safely make and receive their calls when driving without operating the phone. As a matter of fact, Audi was the first car manufacturer to implement this technology in their Audi A8 car in 2002 and then followed by other manufacturers such as BMW, Acura, Toyota, Nissan, Volvo and many more.

The LAN Access implementation defines the process of accessing LAN with the use of point-to-point protocol (PPP) over RFCOMM. This application provides the means to access the services of a LAN with the use of PPP for Bluetooth enabled devices and also shows the process of using PPP mechanisms to create a network that has two Bluetooth-enabled devices. The Implementation of LAN access devices can either be a LAN access point (LAP) that provide access to a LAN such as fiber channel, token ring, cable modem and many more, or Data Terminal devices that make use of the services provided by the LAP such as laptops, personal computers, notebooks and so on. The user scenario involves a LAN access network for a single or multiple Bluetooth devices and network over serial cable emulation between two personal computers by using the PPP. Security application is mandatory for this usage model as it provides encryption of PPP traffic that is sent and received and authentication of Bluetooth devices during pairing by the users.

3.4 Generic Object Exchange Profile (GOEP)

The GOEP in compliance with SPP provides the requirements used to transfer objects between two Bluetooth-enabled devices. The capabilities of this profile can initiate an establishment of exchanging objects between two devices and such an object can be a small data file of a business card, picture, document and many more. Devices that are implementing this profile perform server/client roles, the server device plays the role of providing the object to be exchanged with the client that pulls or pushes the object while the client device performs the role of pushing or pulling the data object to or from the server. Moreover, this profile can only support point-to-point link and does not have fixed master-slave roles. A security procedure is required to initialize pairing and bonding during object exchange by the server and the client and authentication and encryption are required for authenticating establishment and encrypting all link level

data. The profile also supports the GAP requirement that provides interoperability with other profiles. The following application models are based on this GOEP:

- Object Push
- File Transfer
- Synchronization
- Basic Imaging

The Object Push utilizes the protocols and procedures of GOEP to push or send an object from one Bluetooth-enabled device into a designated folder of another Bluetooth enabled device. In fact, this application can also be used by a device to retrieve an object from another device that supports the pull operation and, to exchange objects between two devices. The Object Push operation provides the ability to push one or more objects to a push server, while the Object Pull operation provides the ability to pull an object from a push server and the exchange operation provides the ability to exchange objects with a push server. Such an application scenario involves sending a business card from the phone book of a mobile phone to a designated folder of another phone, pushing a picture to a laptop from a mobile phone and exchanging messages, business cards and documents between devices.

The File Transfer usage model provides an extended Object Push that enhances the ability of exchanging files between two Bluetooth enabled devices. This application uses the underlying GOEP to connect one device to another and perform functions such as browsing the file system to open and view the folder directories, transferring of file from one device to the other and manipulating files and folders by either creating, moving or deleting them. These functions are performed by both the server and the client device; the server provides the client with the file to be exchanged and the folder browsing capability while the client is responsible for pushing or pulling the file from the server.

The Synchronization application model defines the capability of connecting and updating files of two Bluetooth-enabled devices. This process can be automatically or manually initiated. An example is the connection of a personal computer to a personal digital assistant (PDA) to exchange personal information management (PIM) data. This usage model uses the infrared mobile communication (IrMC) to establish the Bluetooth link between the synchronizing devices. In this case, the device can either be an IrMC

server such as the PDA, or an IrMC client such as the personal computer and roles can be exchanged in order to meet the protocol and procedure requirements. The initialization sync mode is the process of using an IrMC server to manually discover, connect and pair the devices while the general sync mode is the process of using an IrMC server to automatically discover, connect and pair the devices together.

Basic Imaging describes the process of controlling, printing and transferring of images from a Bluetooth-enabled image device to a Bluetooth-enabled storage device. The Basic Imaging implementation does not guarantee interoperability between image devices unless they support at least one common image format. In this case, all the image devices should have the capability to receive JPEG thumbnail images and provide their stored images in JPEG thumbnail versions. The roles of the image devices can either be an imaging initiator which initiates the basic imaging feature to provide an object exchange client and server to support interoperability requirements, or can be an imaging responder that responds to the initiated imaging feature that also provides at least an object exchange client and server which then support interoperability requirements. An application scenario involves the process of browsing and retrieving of images stored on a digital camera with the use of a mobile phone.

3.5 Demonstration of Bluetooth Application Models

The real life application of Bluetooth profile specifications are implemented by the various manufacturers of compatible and connectible devices to be able to carry out end users functionality. The following application models are used to demonstrate and perform different types of Bluetooth technology usage:

3.5.1 Setting up of OBEX Object Push and File Transfer Application

The hardware used to demonstrate this Bluetooth setup includes a HP laptop with an embedded Bluetooth device and a Ubuntu10.10 operating system installed in it and a Nokia N70 mobile phone.

This process however, begins with the navigation to the terminal interface of the Ubuntu operating system via application > accessories > terminal and the use of sets of Linux commands on the interface.

Procedure

Step 1: The command below was used to configure the embedded Bluetooth of the laptop and as well display detail information installed in it.

```
akhanolu@idahosa:~$ hciconfig
hci0:   Type: BR/EDR  Bus: USB
        BD Address: 00:1E:37:A5:15:6A  ACL MTU: 1017:8  SCO MTU: 64:8
        UP RUNNING PSCAN ISCAN
        RX bytes:12527 acl:159 sco:0 events:340 errors:0
        TX bytes:3785 acl:73 sco:0 commands:74 errors:0

akhanolu@idahosa:~$
```

Picture 1. *Screen shot showing Bluetooth configuration parameters installed in the laptop*

The host control interface in the command line above provides the following configuration parameters:

type of Bluetooth known as Basic Rate/ Enhanced Data rate embedded USB; the embedded Bluetooth address also known as the MAC Address and establishment of Asynchronous Connectionless Link for data communication and Synchronous Connection-Oriented used for real time voice.

Step 2: The next process was to scan for Bluetooth devices within the range to search for the intended device and try to ping the device address for connection and communication to begin and to make sure the two devices are in discoverable mode. The following commands were applied on the interface;

```
akhanolu@idahosa:~$ hcitool scan
Scanning ...
        00:17:4B:1B:E4:53       N70
        00:60:57:AF:1C:EF       Nokia 6310i
akhanolu@idahosa:~$ sudo l2ping 00:17:4B:1B:E4:53
[sudo] password for akhanolu:
Ping: 00:17:4B:1B:E4:53 from 00:1E:37:A5:15:6A (data size 44) ...
0 bytes from 00:17:4B:1B:E4:53 id 0 time 501.81ms
0 bytes from 00:17:4B:1B:E4:53 id 1 time 35.68ms
0 bytes from 00:17:4B:1B:E4:53 id 2 time 24.77ms
0 bytes from 00:17:4B:1B:E4:53 id 3 time 32.76ms
0 bytes from 00:17:4B:1B:E4:53 id 4 time 33.74ms
Send failed: Connection reset by peer
akhanolu@idahosa:~$ sudo l2ping 00:17:4B:1B:E4:53
Ping: 00:17:4B:1B:E4:53 from 00:1E:37:A5:15:6A (data size 44) ...
0 bytes from 00:17:4B:1B:E4:53 id 0 time 468.35ms
0 bytes from 00:17:4B:1B:E4:53 id 1 time 24.70ms
0 bytes from 00:17:4B:1B:E4:53 id 2 time 15.77ms
0 bytes from 00:17:4B:1B:E4:53 id 3 time 30.76ms
0 bytes from 00:17:4B:1B:E4:53 id 4 time 16.74ms
Send failed: Connection reset by peer
akhanolu@idahosa:~$
```

Picture 2. *Screen shot showing scan and ping result of Nokia N70*

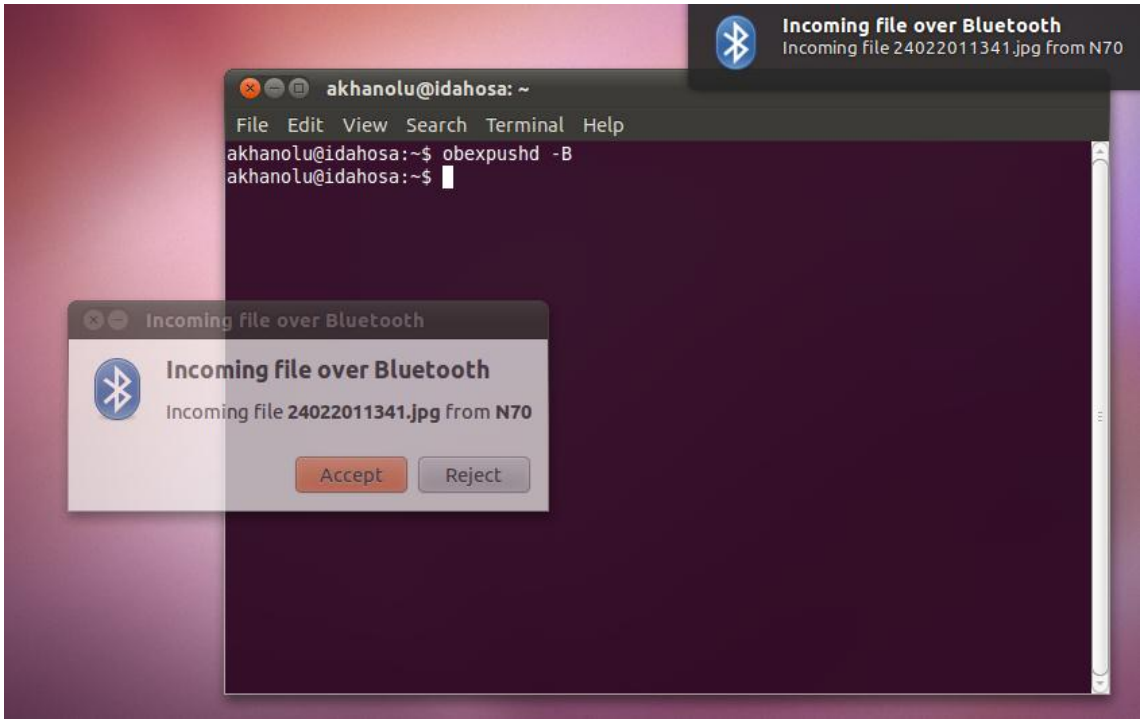
From Picture 2 above, the scan result showed two Nokia mobile phones and the address of the N70 was pinged from the laptop and responded by sending data to the system.

Step 3: The next step was to browse the available Bluetooth services in the mobile phone and to check if the OBEX is available in Nokia N70. This was achieved by using the sdptool browse command to browse the Bluetooth address of the phone (See appendix A);

The result in Appendix A showed the eight Bluetooth services that were available in the N70 which include the required OBEX file transfer and Object Push.

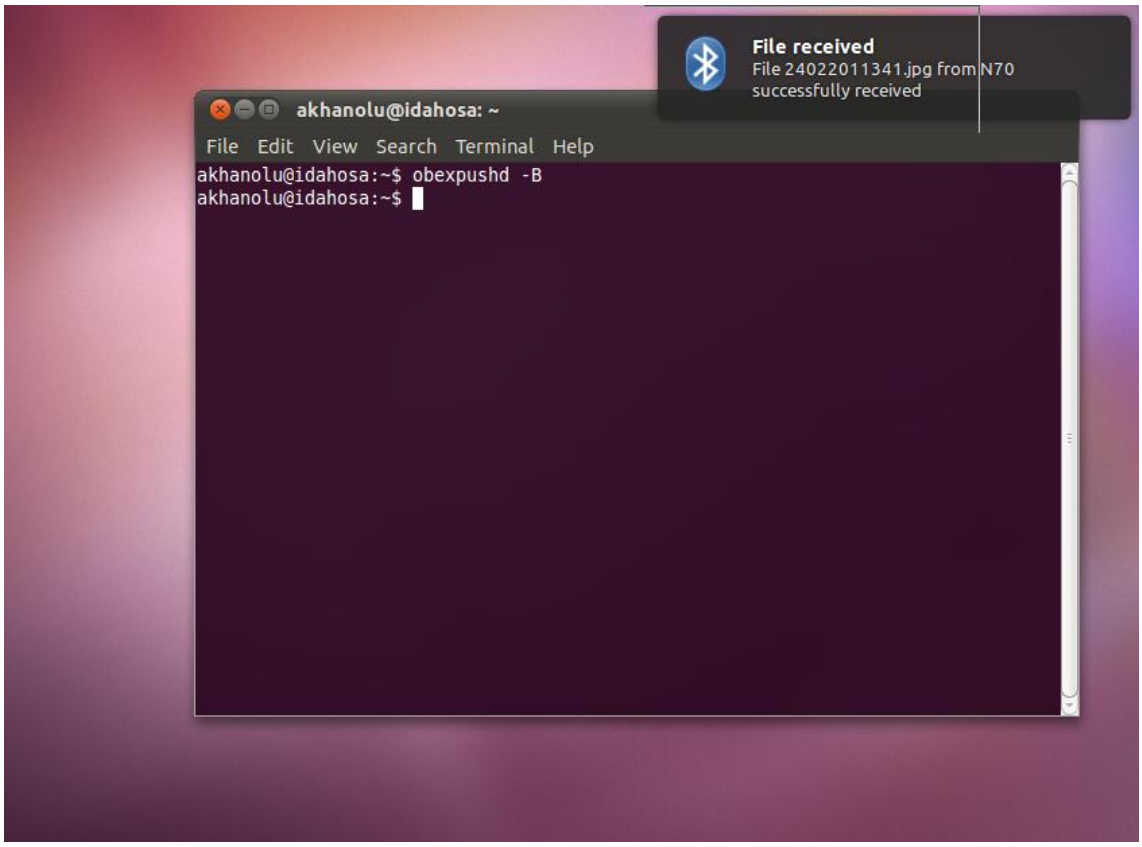
Step 4: The next step was sending the file from the mobile phone to the laptop running the Ubuntu operating system. This was achieved by applying the ‘obexpushd-B’ Linux command in the terminal to listen to incoming Bluetooth connection. A file name 24022011341.jpg was selected from the mobile phone which was then pushed or sent

to the laptop via Bluetooth and a screen shot of the resulted action was taken as shown in Picture 3 below.



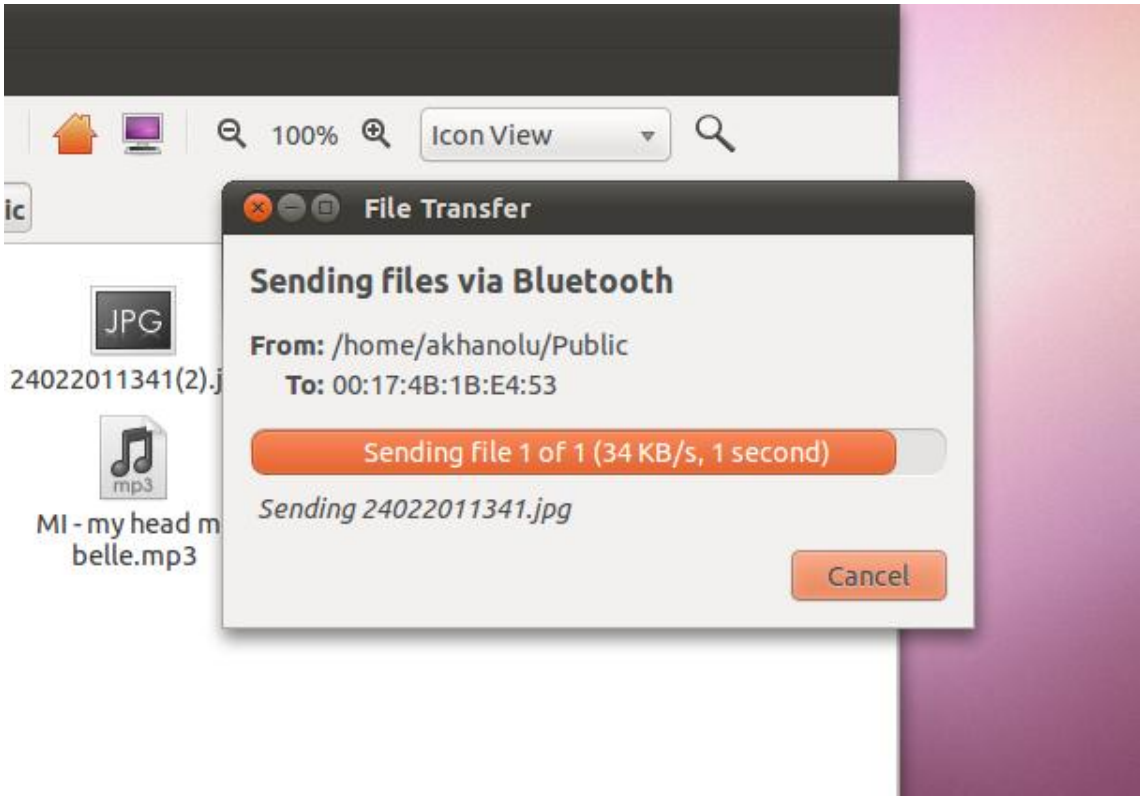
***Picture 3**. Screen shot showing incoming file. [Picture from the practical work]*

The use of Bluetooth devices requires various levels of security application to ensure usage. Protection requirements and Bluetooth security will be discussed in detail in the next chapter. From above, it can be noticed that the laptop used its built-in Bluetooth security manager to allow or deny the mobile device requested services. At that point, the incoming file from the N70 was accepted according to the security trust level and afterwards the file was successfully received by the laptop as demonstrated in Picture 4 below.



Picture 4. *Screen shot showing file received. [Picture from the practical work]*

Step 5: With both devices still connected and bound together with trust, the file that was sent and saved in the home folder of the laptop was transferred back to the mobile phone. At this stage, the file was selected by the user of the device and sent to the N70 by simply listening to its Bluetooth address without requiring any security procedures and the result is shown in Picture 5 below;



Picture 5. *Screen shot showing Bluetooth file transfer. [Picture from the practical work]*

Conclusively, the usage model is used to exchange or transfer small files between devices within the range of Bluetooth wireless network. The OBEX application model is mostly in mobile devices to share relevant data or files such as sending and receiving files for business purposes and sharing of pictures with friends and family, business cards for transferring phone contacts.

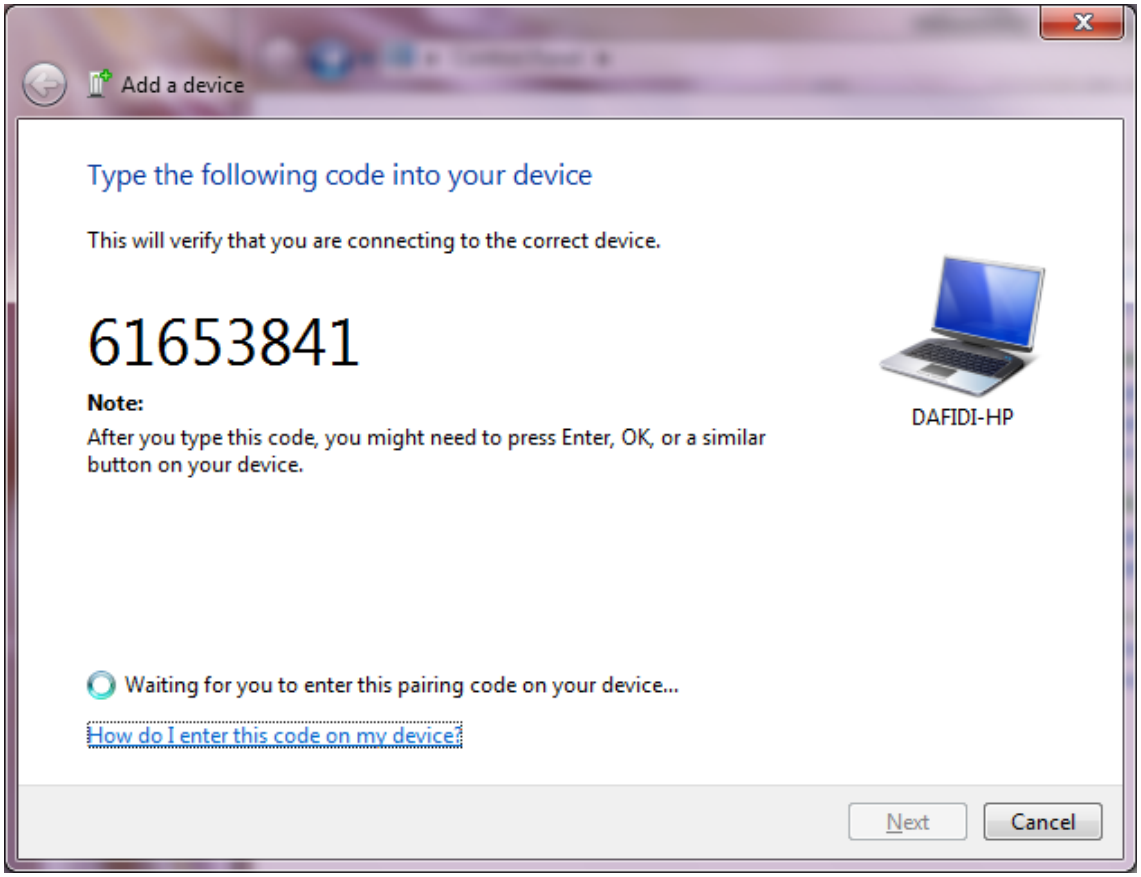
Furthermore, the major limitation of this model is the security downside of Bluetooth which makes it vulnerable to attack by hackers. The security vulnerability of Bluetooth is causing a lot of security threats in the usage of this model and it thus prevents users from using it to share concrete files. The threats can be minimized or prevented in many ways and one of them is to always make sure that the Bluetooth device is in non-discoverable mode when not in use. The other ways of threat minimization will be discussed in the next chapter of the thesis.

3.5.2 Personal Area Network Application Setup

The hardware used to illustrate the PAN set up were two laptops with computer names Idahosa-PC and Dafidi-HP, respectively. Both laptops had embedded Bluetooth adapters and had the Windows 7 operating system installed in them. The usage model was demonstrated graphically by using the graphical user interface of the operating system.

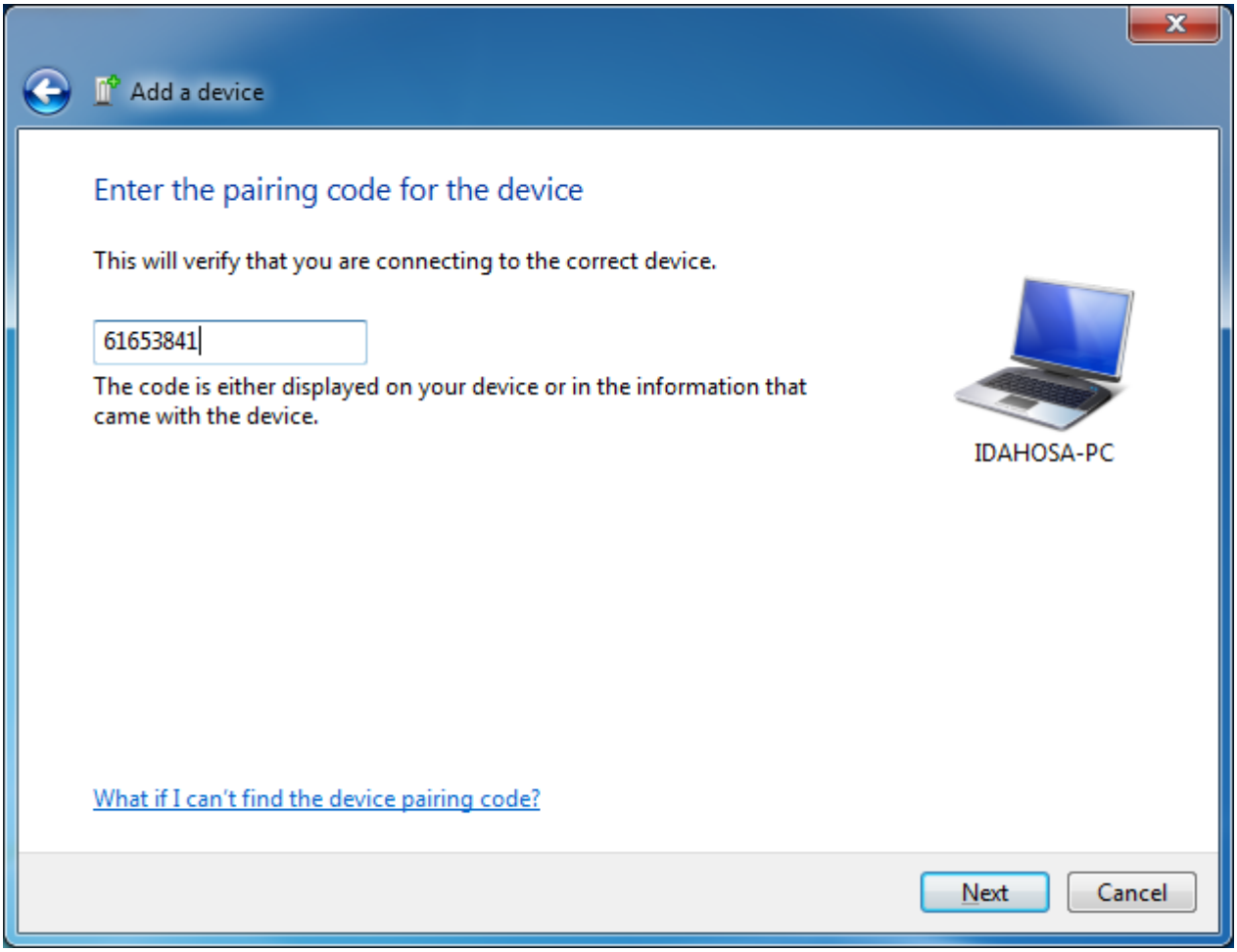
Procedure

Stage 1: The set up began by clicking the start button from Idahosa-PC and navigating via the control panel to the ‘hardware and sound’ and ‘add a Bluetooth device’ was selected under the device and printer tab. This action would display a dialog box that searches for available Bluetooth devices in range and afterwards lists all available Bluetooth devices including Dafidi–HP. The required Dafidi-HP was discovered and added by clicking on the device icon that showed in Idahosa-PC and then click next button to link them. At this stage, it is important to make sure that the discoverable mode is selected in both laptops so that they are able to discover each other. After discovering the device, a click on the device icon and then on next button would send a pairing request to Dafidi HP. During this process, a personal identification number (PIN) is generated in Idahosa-PC that will be shared with the other device as shown in the picture 6 below;



Picture 6. *Screen shot showing PIN pairing process on Idahosa-PC. [Picture from the practical work].*

The PIN shown in the above picture was entered into Dafidi-HP to conclude the pairing process as shown in Picture 7 below;

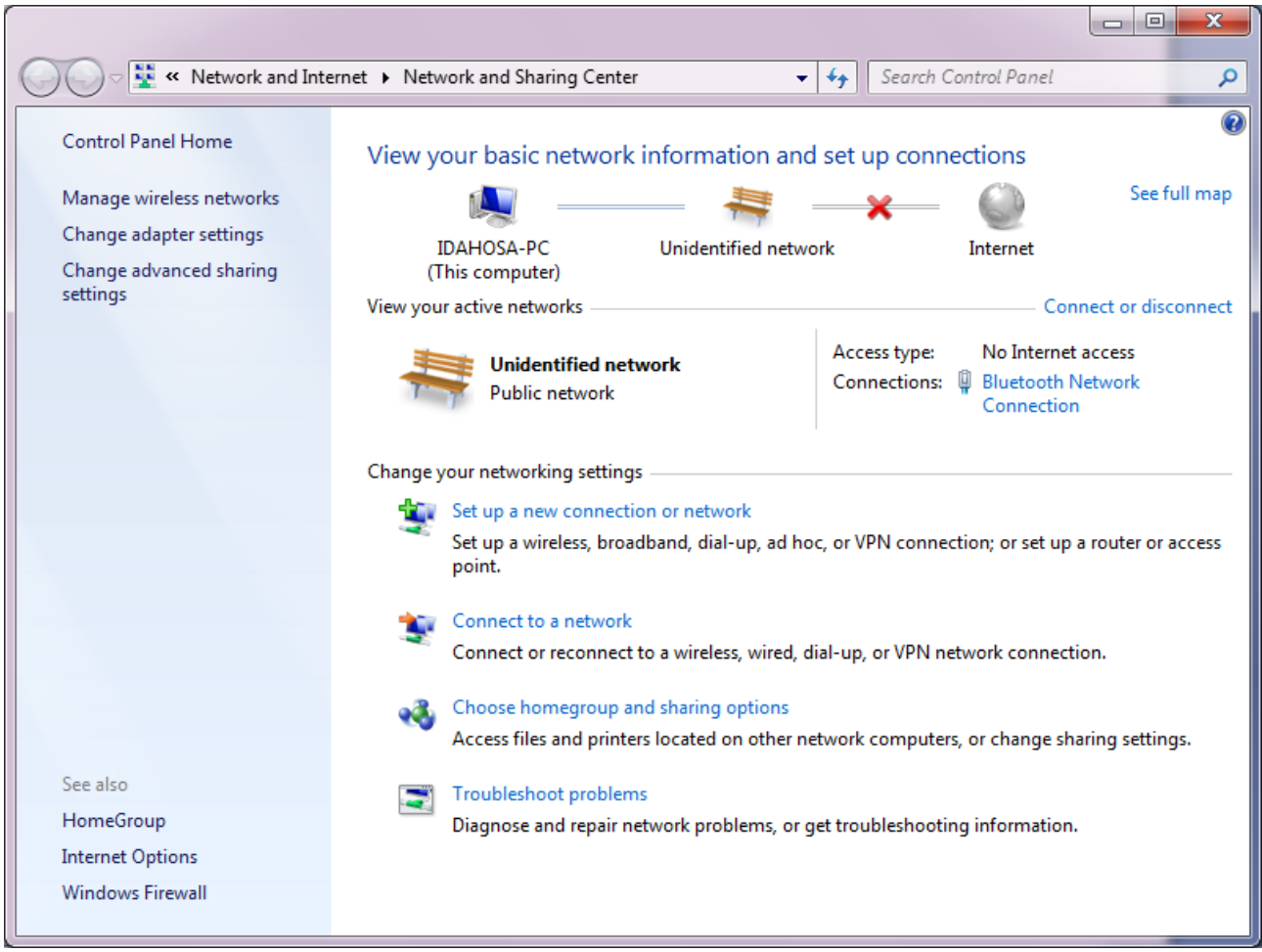


Picture 7. *Screen shot showing common PIN code sharing between pairing devices on DAfidi-HP. [Picture from the practical work].*

Clicking the next icon in the action box will exchange the PIN between the devices to generate an authenticated link key for future pairing. The pairing process completion does denote that an authenticated communication link was generated successfully between both Bluetooth devices as shown in Picture 8 below;

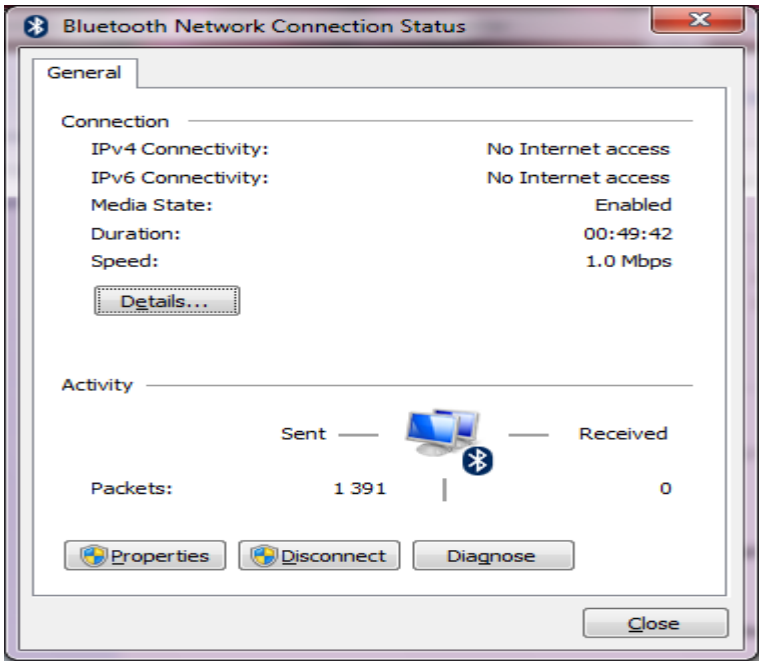
Picture 8. *Screen shot showing successful pairing process between two devices. [Picture from the practical work].*

Stage 2: After the pairing process, the next step is the setting up of a Bluetooth network in both devices. This was done by clicking on the start button and navigating to the 'network and sharing center' via the 'network and internet' tab on each device, clicking on network and sharing centre to view the basic network information and set up connections as shown in Picture 9 below .



Picture 9. *Screen shot showing Bluetooth network information on Idahosa-PC. [Picture from the practical work].*

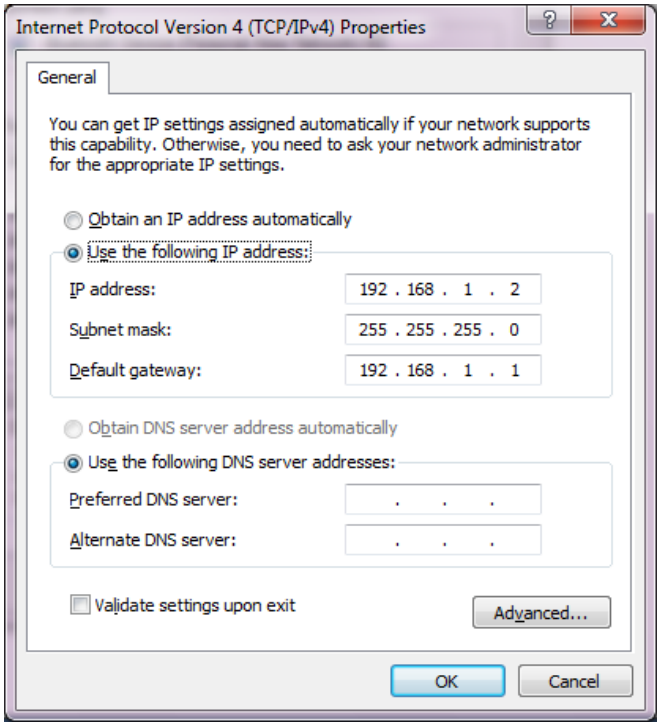
From picture 9 above, a click on the Bluetooth network connection would display details of Bluetooth network connection status. See picture 10 below.



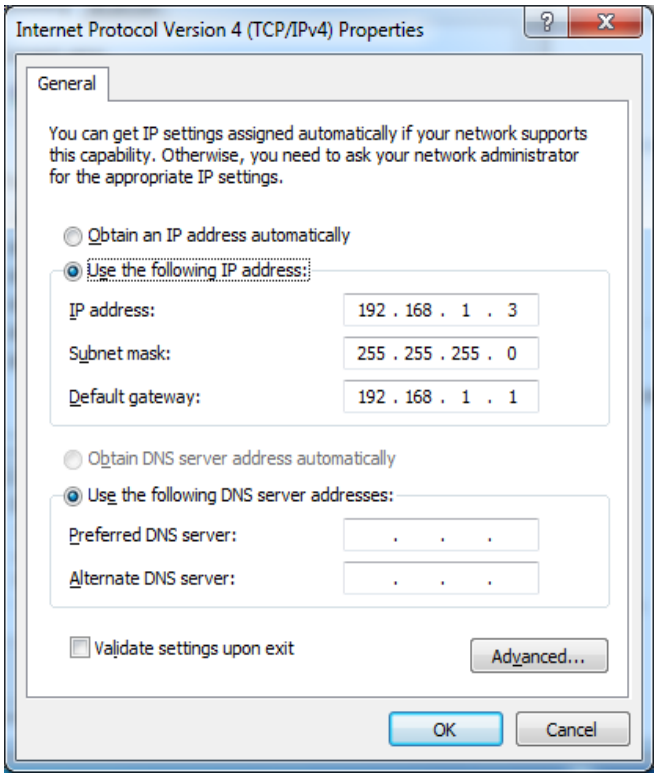
Picture 10. *Screen shot showing Network connection status on Idahosa-PC. [Picture from the practical work].*

Observing Picture 10 above carefully, it can be noticed that no active network is connected between the two devices. The received packet had a value of zero. This denotes that packets are not being received from each other.

However, the Bluetooth network connection was set up by double clicking on the properties shown in Picture 10 above on both devices to obtain an IP address manually or automatically.



Picture 11 *Assigning IP address to Idahosa-PC. [Picture from the practical work].*



Picture 12 *Assigning IP address to Dafidi-HP. [Picture from the practical work].*

Class C addresses were manually assigned to both devices with a subnet mask and a default gateway as shown in Picture 11 and 12 above and then the ‘ok’ tab was clicked to finalize the PAN set up.

Stage 3: This stage involves the use of Windows command line interface to verify the success of the configuration described above used to create a Bluetooth communication network link between the devices. This could be achieved by simply pinging the IP addresses of one of the device from the other pair and vice versa and the result was successful. See Appendix B and C.

From the observable results in the stages described above, it can thus be concluded that the Bluetooth PAN Application model is a convenient way to create an ad-hoc network with the use of PANU devices to connect and communicate with each other.

NB: During the PAN set up, it is very important to ensure that the choice Bluetooth IP address of the chosen device is different and preferably not on the same network as the LAN network address if there is an active LAN connection and the address can be obtain manually. This ensures that no IP address conflict and LAN network route problem as such problem could pose a risk to the entire LAN network. Also, the default gateway can be neglected when manually using TCP/IP version 4 to assign an IP address for the connection between both devices as this it does not have any effect on the ad-hoc network.

4. BLUETOOTH SECURITY

The use of Bluetooth wireless technology to exchange data between portable devices over a short distance range requires usage protection of the transmitted information. The built-in security protocols and procedures at the link level of the Bluetooth devices handle the security issues in a piconet. In fact, the incorporation of security measures into the Bluetooth devices ensures that user information or data are protected against various security threats. Bluetooth security is very important while using Bluetooth enabled devices to prevent attacks on wireless network such as leakage of transmitting information, denial of service attacks and integrity attacks that alter transmitting information.

The basic means of ensuring Bluetooth security are authentication, used for identification of devices in the piconet; authorization, used for granting authenticated client access to various services on the server; and encryption for encoding information to be exchanged. This basic security provisions are implemented within the various layers of the protocol stack. The link controller utilizes its random number generation capability used for managing security keys and provision of mathematical operations for authentication and encryption. Then, the link manager enhances several commands for handling security issues, while the L2CAP is used to initiate security procedures for channel connection. Also, HCI is used for handling security communication between Bluetooth devices.

The Bluetooth security usage model is applicable to the Bluetooth profiles and the generic access profile which forms the foundation of all the profiles where the security is organized. The security application can begin when the user of a device has options of discovering and connecting to another device to exchange information. The device can have options of being silent, private or public depending on the user options. In the silent option, the device can never enter the page scan or inquiry scan states and cannot accept any connections but it monitors the Bluetooth traffic. The private option enables the device to enter the page scan state periodically and not the inquiry scan state which prevents the device from being discovered by other devices but connections can be accepted if the Bluetooth address of the device is known. The public option enables the device to enter both page scan and inquiry scan states periodically and can as well be discovered and connected to other devices [5].

In Bluetooth security measures, the security levels of discovering, connecting and pairing of devices whether in silent, private or public access states are classified by the generic access profile into three security modes that provide security services to the devices and these modes are:

- **Bluetooth security mode 1**: This is a non-secure mode that does not require any security measures. Devices in this mode do not require the security mechanisms to prevent other Bluetooth devices from establishing connections and communication can occur without authentication or encryption. The Bluetooth security mode 1 can only support Bluetooth version 2.0 and enhanced data rate (EDR) devices.

- **Bluetooth security mode 2**: This is a service-level enforced security mode which uses a centralized security manager to control specified services and devices. The security manager applies security protocols and procedures for various trust levels with different security requirements to allow or restrict devices from available services. In security mode, authorization is applicable to grant access to a specific device by allowing it to have access to a particular service. Authentication and encryption security measures are applicable to this mode and they are implemented in the link manager protocol. In general, all the Bluetooth devices can support this security mode.

- **Bluetooth Security mode 3**: This is a link-level enforced security mode used by Bluetooth enabled devices for initiating security procedures before establishing any physical link. However, authentication and encryption in this mode are required for all the connections going and coming from the devices. During the process of pairing devices, authentication and encryption security measures apply a separate secret link key which is shared by the paired devices. The security mode can only support Bluetooth version 2.0 and (EDR) devices.

- **Bluetooth Security mode 4**: This security mode is used by Bluetooth devices for initiating security procedures after establishing a physical link. Security authentication and encryption are applicable to devices that support Bluetooth version 2.0 and (EDR) for key exchange and link key generation used for secure simple pairing.

  During the process of security applications for end users, improper implementation of security measures can provide access to unauthorized users which make Bluetooth devices vulnerable to attacks. Such vulnerabilities include: use of short personal identification number (PIN), weak and negotiable encryption key, improper storing of link keys, no user authentication existence and many more [4] .

4.1 Security Application Processes

Bluetooth security operates in a chain of events that involves the process of verification and identification of devices during communication, process of encrypting data to be exchanged for the purpose of confidentiality, and the process of authorizing or restricting devices for use in certain available services. In a point-to-point piconet security process, the master and the slave device communication begins with the use of a common personal identification number, and then the PIN is used for the creation of initialization key which in turn uses for the creation of link key to link the devices. This link key provides the process of authentication and it is also used to generate the encryption key. The creation of new key depends on the previous key in Bluetooth security chain of events and this process is illustrated in the diagram below;

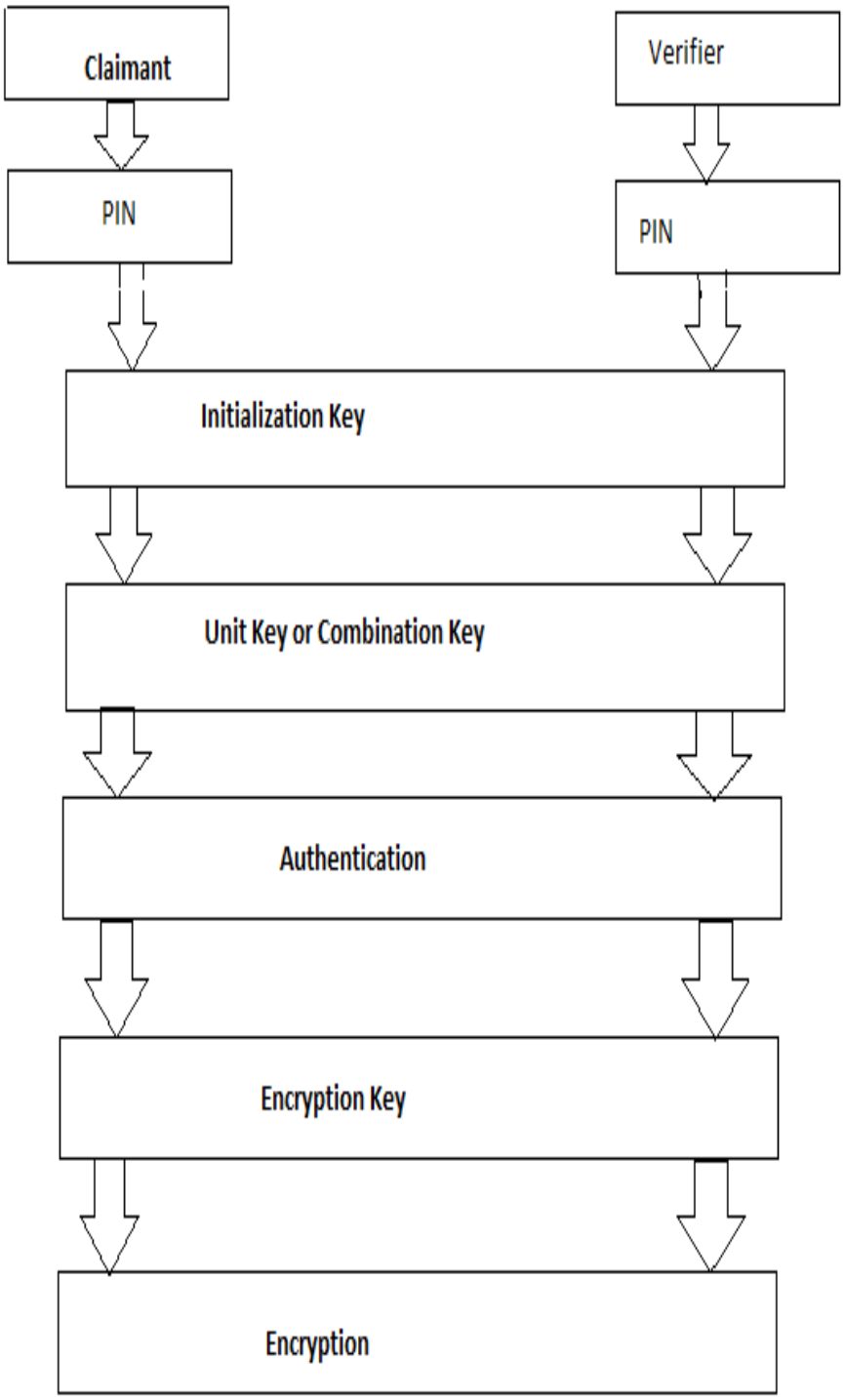


Figure 4.1.0. *Chain of events in security operation*

Link Keys

In Bluetooth security, the link key also known as authentication key is usually 128 bits long and it is used by a device to verify the identity of another device. The length and random nature of the link key ensures that it is almost impossible for an intruder to detect it and provide a secure link between the devices. The link key can be temporary used for one link session between devices, or can be continuously used for a defined period of time before it can be changed or completely removed. The link key can exist in four types such as initialization key, unit key, combination key, and master key. The initialization key is used as a link key in situations where the two devices discover each other for the first time and afterwards used for protection and generating other keys which are more secure. The unit key is used for a single Bluetooth device with limited resources and cannot store a large number of keys. The combination key is the unique link key generated by the two devices during connection and this key is more secure than the unit key. The master key is used for generating the encryption key in a piconet with multi-slaves to broadcast packets. The generated encryption key is used for encrypting information to be sent from one device to another.

4.1.1 Authentication

Bluetooth authentication can be described as a one-way process of authenticating security procedure that involves the verification of identity of a device by another device. This process requires a mutual challenge-respond action that can be repeated by reversing the roles of the devices. The device that verifies the identity of the other device is known as the verifier while the identified device that is verified by the verifier is known as the claimant. In this security mechanism, the verifier challenges the claimant by sending a random number to the claimant and the claimant responds to the challenge by returning the response to the verifier. This response produces an authentication output function that involves the random number, Bluetooth address of the claimant device, and the generated secret key during pairing. Nevertheless, the random number is forwarded back to the verifier from the claimant through the LMP packet for verification and if the sent number matches with the forwarded number, then the verifier can thus conclude that the claimant is in possession of the correct link key.

4.1.2 Encryption

The confidential transmission of information that can be accessed and viewed by authorized ad-hoc wireless Bluetooth devices can be provided by encrypting the data. The encryption process involves the transformation of plain text message into a random sequence of bits known as cipher text during transmission. The transformation is implemented by combining an encryption key with the plain text message as an input to an encryption algorithm and an output emerges as a cipher text that looks like a random sequence of bits. Then, the cipher text in the output is changed back to the plain text message with the use of the cipher key and a decryption key for another encryption algorithm. The Algorithm process can either be symmetric or asymmetric. The symmetric algorithm uses the same key for both encryption and decryption, but the security can be vulnerable in this process. A continuous increase in the number of devices that shares the key can thus makes the key and message easily intercepted. While the asymmetric process is based on a mathematical sequence whereby one key is used for encryption and another key is used for decryption. The two keys do not have anything in common and the knowledge of one key cannot provide information of the other key.

Furthermore, encryption process has three different encryption modes. The first one is the encryption mode 1 which does not require any encryption and all traffic in this mode is unencrypted. The second is encryption mode 2 and it requires encryption for point-to-point traffic with individual link keys and no broadcast traffic is encrypted. The third mode is encryption mode 3 which does requires encryption for both point-to-point traffic and broadcast traffic with the use of the same master link key and all traffic in this mode can be read by all the devices in the piconet, but they appear encrypted to all unauthorized viewers. Ideally, all parts of a Bluetooth packet are not encrypted to allow all the devices in the piconet to be able to recognize the packets that are meant for them. It is paramount to leave the access code part of a packet unencrypted as it ensures that the radio frequency signal is utilized by all the devices. An encryption key has 128-bits long and 8-bits short depending on the importation and exportation regulations of devices from one country to another as some countries do not permit the 128-bit encryption keys. The encryption keys are permanently programmed into Bluetooth devices which cannot be modified by end users [8].

4.1.3 Authorization

This is a security decision-making process that concerns the resource access control and requirements for authentication and encryption that are used for granting permissions to Bluetooth devices or the use of available Bluetooth services. It creates an instance in which devices or users are either allowed to use available services or not. The client-server process is used where the server acts as the verifier and the client acting as the claimant. Moreover, the client can link up with the server by authenticating itself to the server and request the server to grant access to its available services based on the permitted level. Bluetooth devices can be permitted to available services depending on the authorization level that is either granting access to the services or access to some part of the available services. Further access can be granted to some of the services with the use of external security control entity (ESCE) that require additional authentication by the user in the client device.

In general, the security chain of events of authentication, encryption and authorization processes are achieved with the use of security protocols and procedures to successfully pair and bond devices with levels of trust.

Pairing

This is a process that involves the communication and establishment of connection between two Bluetooth devices. The communicating devices agree to pair with the same PIN and generate keys which are used for identification purposes and to maintain relationship references with other devices. The keys are also used to generate device authentication and encryption keys. A PIN with a maximum of 128-bits used for pairing devices can either be variable or fixed. The variable passkey or PIN is determined during pairing through an input mechanism while the fixed key is determined before pairing. Secure Simple Pairing is another process of pairing devices which are meant to be flexible and easy to use for pairing by Bluetooth devices. This process exhibits far-ranging display and input capabilities. This system of pairing uses various application models which are the numeric comparison, out of band and just works. The numeric comparison is used to handle scenarios in which both communicating devices are capable of displaying a six digit number usually 000000 to 999999 and provide inputs to permit the user to enter a yes or no command. If the digit numbers are the same in the two communicating devices, then a yes command is entered in both devices and they would be paired successfully. Then, the out of band

pairing model is used for discovering Bluetooth devices and exchanging information during pairing and it requires the physical touching of the two devices together. While just work pairing model involves a situation in which one of the two devices to be pair cannot display the six digit numbers used for pairing process.

Bonding

This is a process that occurs when paired devices decide to store their link keys for subsequent authentications usage. The paired devices are not bonded if they decide to discard the link keys and repeat the pairing process each time they need to be connected. Devices can only be temporarily bonded together and the bonding ends immediately the link between the devices is disconnected after a certain period of time. The bonding process could be repeated after the pairing process repeating and the link key established would never be permanently stored by the bonded devices. This helps to prevent any stored link key attack. Devices can be either in a bondable mode or non-bondable mode. The bondable devices are in the modes that allow pair-ability with other devices, while the non-bondable devices are in the modes that do not request or respond to bonding and cannot pair with other devices.

Trust

This is a situation in which a device is authorized to access specified services on another device. A device can be trusted if the level of authorization in accessing available services is based on its previous authentication process. A device that is not trusted will require password despite it being authorized to access available services based on its initial authentication. Bluetooth devices can either be trusted or un-trusted depending on the trust levels. The trusted devices are devices that had been previously paired with another device and they have full access to the available services on the pair device. While the un-trusted devices could be devices that have either been previously paired with a pair device but the relationship has been discontinued, or a device that has never been paired with a pair device before and its access to the available device services is restricted to the device. On the other hand, Bluetooth available services could be accessed or restricted depending on the security levels such as service level 1, service level 2 and service level 3.The service level 1 requires manual authentication and authorization of devices before granting service access to un-trusted devices and automatic access to trusted devices. The service level 2 requires device authentication but does not require authorization to access the

services. While the service level 3 offers open services for all devices and no security is required.

In addition, trust implementation provides users with options of accepting or rejecting all connections that are globally applicable to incoming connections instead of access to certain services.

4.2 Security Problems

Bluetooth security weaknesses are causing a major setback which is delaying the global mass adoption of the technology. The end users are facing a lot of security problems while using Bluetooth enabled devices. Improper secure Bluetooth implementations by manufacturers could expose the devices to potential vulnerabilities as a result of insufficient security feature applications that could grant a false access to unauthorized users. Weaknesses in security application process such as authentication, encryption and authorization are rendering the devices vulnerable to attacks.

Furthermore, unauthorized users could take the advantage of improper security implementations to attack Bluetooth devices such as mobile phones. In turn, end users of the devices are facing other various security threats such denial of service attacks, disclosure threat, modification of messages, man-in-the-middle attacks and other related categories of Bluetooth hacking such as bluesnarfing, bluebugging and bluejacking.

4.3 Security Vulnerabilities

As stated in 4.2 above, the weaknesses in Bluetooth security applications are causing vulnerabilities in use of the devices and they are becoming a major concern to end users. Despite the fact that the various manufacturers are using the SIG standards to implement security features, the devices are liable to the following vulnerabilities:

4.3.1 PIN and Link Keys weaknesses

During the pairing process, the use of poorly secured PIN exchange between the initiating device and the responding device can provide an intruder with the ability to easily detect the shared PIN. This enables the attacker to be granted unauthorized access and thus could be able to retrieve the information that is being exchanged between the devices. Manufacturers are using very short PINs that could be easily

detected by intruders. Also, the use of random zeros as the default PIN and the physical entering of PIN code to devices can be visible to others. More so, weak implementations of link keys could provide access to an intruder and would expose the PIN as the unit key is known to others when reusable and can be exploited during sharing. A weak master key can be disclosed easily during sharing and improperly stored link keys can be modified if they are not protected through the access controls.

4.3.2 Authentication Weaknesses

An intruder could capitalize on repeated authentication process between verifier and claimant devices. The attacker could pose as a legitimate claimant to the verifier by disabling the repeated authentication attempts from the authorized claimant. Although this attack could sometimes be countered by exponentially increasing the waiting period for another authentication attempt after a failed attempt. This measure, however, is not wholly accepted as a measure to prevent intruders. In addition, there are cases in which manufacturers could only implement device authentication but not user authentication in the application security level. This could create access for unauthorized users. More so, in device authentication, the one way challenge-response key sharing between devices could be weak and could thus easily be subjected to an attack.

4.3.3 Encryption Weaknesses

In the encryption process, the use of symmetric stream cipher algorithm is too weak and does not provide strong encrypted text, hence the same key is used for the encryption and decryption process and this key can be shared by many devices. This key could be exploited by an intruder while performing a sequential search for the encryption key. The use of negotiable encryption key is the most known weakness especially when using a key shorter than 128 bits instead of using the whole bits for the key. For instance, a device with a shorter key could be restricted when negotiating an encryption process with a device having a longer key. The device with longer key length, however, must try to adjust to accommodate the shorter key before encryption can be enabled.

In general, devices that are in continuous discoverable or connectible modes are also prone to attacks and the specified minimal amount of time should have been implemented by the application developers to discover or connect the devices during pairing.

4.3.4 Bluesnarfing

This is a type of Bluetooth hacking in which a hacker takes advantage of firmware flaws to exploit the devices. The attacker could penetrate the device, gain access and also have full control of the data stored in the device. In fact, this attack could be deployed on a Bluetooth enabled mobile phone by using unauthorized means to bypass the usual pairing process and, thus, gain access and steal relevant data such as contacts in the phonebook, messages, access to calendar and any other important information stored in the phone memory. Devices can be less prone to this attack if they are in non-discoverable settings. Manufacturers of Bluetooth enabled mobile phones, like Nokia, are taking preventive measures to ensure that this threat is avoided in their newly produced phones.

4.3.5 Bluebugging

As a result of security vulnerabilities, attackers could gain access to Bluetooth devices and their commands. The hackers could gain full control of the target devices like mobile phones as if they are having physical access by sending commands to perform various actions. This is done without the knowledge of the authorized user to access stored data, send messages, make phone calls, adding, deleting and editing phone contacts, eavesdropping on phone user conversations and exploiting other services that are provided by the hacked device. For sake of manufacturers' reputation and end users data safety, the causes of security vulnerabilities in mobile phones have been taken into consideration and are resolved in the newer ones [25].

4.3.6 Bluejacking

This is another hacking technique that is used to attack Bluetooth enabled mobile devices. This attack is initiated by sending unsolicited messages to users without their consent. Hackers could initiate this hacking method by sending messages to mobile devices such as PDAs, smart phones and cellular phones and await the user response in some way that would open a gateway for the hackers. This attack could also be used to send a business card to another phone that is within the Bluetooth range. The message sending attack is equivalent to spam e-mail and an attempt to get access to relevant information by phishing the user. This attack is harmful if a user responds to

the sent message, but can also be prevented if the sent message is neglected or rejected by the device user.

4.3.7 Backdoor attack and other threats

The backdoor attack is a way that an attacker can use the pairing mechanism to exploit a device by establishing a link with another device, such as laptop that bases its connection with the attacker device on trust. The pairing process takes place without the knowledge of the user but it could be noticed if the screen of the hacked device is checked during an active connection with the hacker's laptop. The intruder can have full access to the data stored and available services of the hacked device immediately after the connection is established.

The Denial-of-Service is one of the threats to Bluetooth devices. Attackers use this technique to send a sudden commotion of pairing requests to the target device such as a mobile phone. The attack could cause annoyance to the user by sending unnecessary requests, paralyze the device and also drain the target device battery power. This threat could be avoided by simply walking away from the Bluetooth range.

Furthermore, the fuzzing attack is another type of attack that involves the sending of imperfectly formed data to the Bluetooth radio of the target device and keeps observing the device reaction to the data. If the device reaction to the data is slow or stops, then there is existence of vulnerability in the protocol stack of the device. Hackers can attack Bluetooth devices through disclosure threat to have unauthorized access to the target device to get leakage of information. Another way to attack Bluetooth devices is the use of integrity threat to deliberately alter the information to mislead the recipient.

4.4 Ways to Prevent Attacks

Despite the fact that Bluetooth security issues are a major concern in the use of Bluetooth technology, its security problems and vulnerabilities can be minimized or completely avoided during security implementations and also during the Bluetooth devices usage. With the continuous provision and updating of security standard by SIG to the various Bluetooth adapters manufacturers to tackle the improper implementation of Bluetooth security that causes vulnerabilities, the Bluetooth security threats are being countered. In order to achieve a maximum secure protection against any attack, the following security guidelines are recommendable while designing as well as during the usage of the Bluetooth devices:

- Manufacturers should ensure that Bluetooth devices are set by default to undiscoverable mode so that they will not be visible or discoverable to other Bluetooth devices within range unless they are previously paired and trusted devices. Bluetooth radio designers should make sure that the link keys are only based on combination key instead of using the unit keys that are prone to attacks.
- Radio designers should ensure that secure long and random PIN codes that would not be easily detected by an intruder are implemented instead of using static and weak PIN codes that can easily be known.
- Bluetooth device power level settings should be on a lowest considerable and sufficient level for transmissions to make sure that the range of access is not exceeded to unauthorized users.
- Various manufacturers of Bluetooth devices should provide users with detailed security guidelines for the proper use of their products to prevent attack.
- Device developers should ensure that user authorization is required for every incoming connection attempts and this would in turn allow the users to avoid connection with un-trusted users.
- Security mode 3 should be implemented for link level security to ensure initiation of Bluetooth authentication during connection between devices.
- Manufacturers should ensure that users of devices are restricted from manipulating security features to prevent alteration of security settings that can lead to vulnerability of the device.
- SIG should ensure that all manufacturers of Bluetooth devices are following the SIG standard and regulations to prevent the devices from being vulnerable to attacks and should as well make sure that all firmware, drivers and application software are constantly updated to standard.
- End users should ensure that they only enable the discoverable mode of their Bluetooth radio only when needed and should always disable them if they are not in use to prevent the devices from being visible to attackers.
- Users of Bluetooth devices should be conscious and constantly monitor device link and connection activities in the case of any attempt of unauthorized connection and they should implement visual check and have physical control of the devices regularly.
- Users should make sure that their devices are used in a secured environment and long and randomly generated PIN codes are used.
- End users should follow and obey the guidelines, policies, rules and regulations of using the Bluetooth enabled devices to avoid improper use of them.

- End users should always report any security issues that they are facing while using of Bluetooth devices to the manufacturers so that the manufacturers could quickly rectify such problems or provide guidelines.

5. CONCLUSION

Bluetooth Technology is rapidly growing in popularity due to its acknowledged usefulness, vast applications and reliability to conveniently exchange information between compatible mobile devices free of charge. The short range radio link of the wireless network enables the replacement of cables connections between point-topoint and point-to-multi-point of portable digital devices to transfer voice and data simultaneously.

The wireless technology is providing the developers of Bluetooth devices with the ability to easily penetrate the global market for sales of their products as a result of Bluetooth global availability and acceptability. More so, end users of Bluetooth devices are gaining confidence in the use of the technology as it is reliable, cheap, secure and easy to operate.

Based on the implementation of this technology, the reader of this thesis could see how vendors utilize the capabilities of the protocol stack with the functionality of its various layers to conveniently provide Bluetooth devices with different application models through Bluetooth profiles. Also, this thesis work analyzed the Bluetooth basic security applications that ensure the safe use of the technology, scrutinized the improper security implementation by vendors which result to vulnerabilities in Bluetooth devices and provide security tips on how end users of Bluetooth devices could minimize or eradicate the security threats associated with use of this technology.

Nevertheless, users of Bluetooth are utilizing and enjoying the advantages the technology has to offer them such as searching and transferring useful documents between mobile devices, for house furnishing and multimedia communication. Bluetooth technology affects and adds value to the daily lifestyles of the users with its numerous applications.

The SIG has been playing a vital role in the successful development and regulating the use of the technology. The group has made a significant impact on monitoring and controlling the implementation of the free wireless network.

Conclusively, considering the low cost of the vast reliable applications of Bluetooth and provision of security tips to minimize security threats, Bluetooth technology is definitely one of the useful wireless networks in the world today and in the future to come.

REFERENCES

[1] A Comprehensive Guide to Everything Bluetooth Related. 2011. Bluetooth History. Consulted 12.02.2011

http://www.bluetomorrow.com/about-bluetooth-technology/history-of-bluetooth/bluetooth-history.html

[2].Dean .A. Gratton. 2003. Bluetooth profiles (The Definitive Guide). consulted 10.5.2011

http://books.google.com/books?id=08eByqhzJ3wC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[3]. Christian Gehrman, Joakin Person, Ben Smeets. 2004. Bluetooth Security. British Library Cataloguing in Publication Data, Artech House Inc. 585 Canton Street Norwood, MA 02062.

[4]. Jun-Zhao Sun, Douglas Howie, Antti Koivisto, Jaako Sauvola. July 2001. Design, Implementing And Evaluation of Bluetooth Security. Media Team, Machine Vision and Media Processing Unit, InfoTech Oulu, University of Oulu, Finland.

[5]. Robert Morrow. February 2002. Bluetooth operation And Use. McGraw-Hill Companies, Inc. United States of America.

[6]. Axel Streicher, Charles Melear. July 2006. Introduction to Bluetooth Technology. Motorola Computer Group, Embedded Systems Conferences, Munich, Germany and Austin, Texas USA.

[7] The Wireless Directory. 2003. Bluetooth Specification. Consulted 21.02.2011

http://www.thewirelessdirectory.com/Bluetooth-Overview/Bluetooth-Specification.htm

[8] Karen Scarfone, John Padgette. September 2008. Guide to Bluetooth Security, Recommendations of the National Institute of the Standards and Technology. Consulted 13.05.2011

http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf

[9] Hewlett-Packard Development Company. 2004. Bluetooth Wireless Technology Basics.

Consulted 08.02.2011 http://www.dectrader.com/docs/set4/c00186949.pdf

[10] Wireless Developer Network. 2001-2010. An Introduction to Bluetooth. Consulted 26.02.2011

http://www.wirelessdevnet.com/channels/bluetooth/features/bluetooth.html

[11] Silan Liu. Bluetooth Technology. Consulted 05.03.2011

http://www.wirelessdevnet.com/channels/bluetooth/features/bluetooth.htm

[12] Palo Wireless Bluetooth Resource Centre. Bluetooth Specification Protocol Stack. Consulted 25.03.2011 http://www.palowireless.com/infotooth/tutorial

[13] A comprehensive guide to everything Bluetooth Related. 2011. Bluetooth Protocol Architecture.

Consulted 11.04.2011 http://www.bluetomorrow.com/about-bluetooth-technology/how-bluetooth-works/bluetooth-protocol-architecture.html

[14] A comprehensive guide to everything Bluetooth Related 2011, Listing of Bluetooth Profiles. Consulted 29.04.2011

http://www.bluetomorrow.com/about-bluetooth-technology/how-bluetooth-works/listing-of-bluetooth-profiles.html

[15] Markus Jacobsson, Susanne Wetzel. Security Weaknesses in Bluetooth. Consulted 24.05.2011 http://www.cs.stevens.edu/~swetzel/publications/bluetooth.pdf

[16] Tu C. Niem. GIAC Security Essentials Certification. Bluetooth and its Inherent Security Issues. April 2002.Consulted 10.06.2011

http://www.sans.org/reading_room/whitepapers/wireless/bluetooth-inherent-security-issues_945

[17] Types of Bluetooth Hacks and its Security Issues. 2011. Consulted 22.07.2011

http://hassam.hubpages.com/hub/Types-Of-Bluetooth-Hacks-And-Its-Security-Issues

[18] Justin Blasdel. April 2004. The Future of Bluetooth. Consulted 11.08.2011

http://faculty.mckendree.edu/kian_pokorny/Course_Pages/CSI490/Bluetooth.pdf

[19] Qusay H. Mahmoud. 2003. Wireless Application Programming with J2ME and Bluetooth. Consulted 21/08/2011

http://developers.sun.com/mobility/midp/articles/bluetooth1/

[20] Palo Wireless Bluetooth Resource Centre. Bluetooth Glossary. Consulted 30/08/2011

http://www.palowireless.com/infotooth/glossary.asp

[21] Palo Wireless Bluetooth Resource Centre. Bluetooth Baseband. Consulted 05/09/2011

http://www.palowireless.com/bluearticles/baseband.asp

[22] Wikipedia, the Free Encyclopedia. Bluetooth. Consulted 16/09/2011

http://en.wikipedia.org/wiki/Bluetooth

[23] Forum Nokia. 2003. Bluetooth Technology overview. Consulted 18/9/2011

http://lms.uni-mb.si/~meolic/ptk-seminarske/bluetooth2.pdf

[24] Tom Karygiannis, Les Owens. Wireless Network Security. 802.11, Bluetooth and Handheld Devices. Consulted 22/9/2011

http://www.artofhacking.com/tucops/hack/wireless/DRAFTWNS.PDF

[25] Hubpages. 2011. Types of Bluetooth hacks and its Security Issues. Consulted 29/9/2011 http://hassam.hubpages.com/hub/Types-Of-Bluetooth-Hacks-And-Its-Security-Issues

APPENDIX A

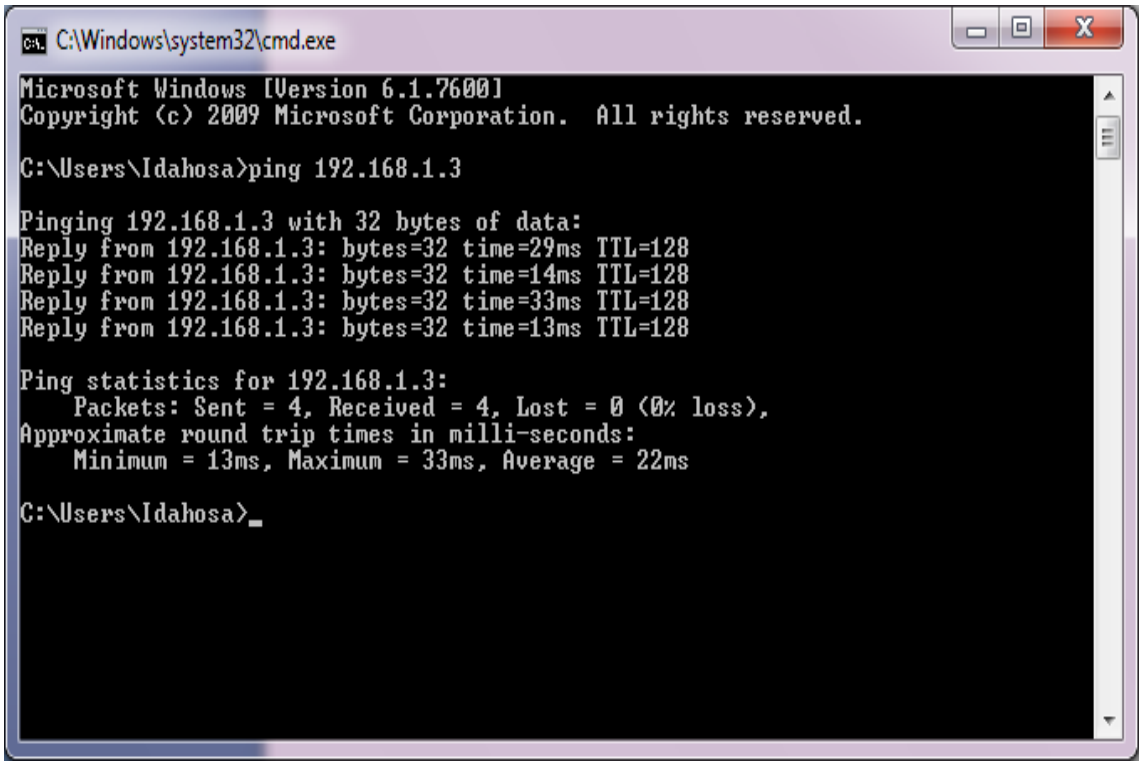
```
akhanolu@idahosa:~$ sdptool browse 00:17:4B:1B:E4:53
Browsing 00:17:4B:1B:E4:53 ...
Service Name: Hands-Free Audio Gateway
Service RecHandle: 0x10000
Service Class ID List:
  "Handsfree Audio Gateway" (0x111f)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 1
Language Base Attr List:
  code_ISO639: 0x454e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "Handsfree Audio Gateway" (0x111f)
    Version: 0x0101

Service Name: Headset Audio Gateway
Service RecHandle: 0x10001
Service Class ID List:
  "Headset Audio Gateway" (0x1112)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 2
Language Base Attr List:
  code_ISO639: 0x454e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "Headset" (0x1108)
    Version: 0x0100
```

```
Service Name: OBEX File Transfer
Service RecHandle: 0x10002
Service Class ID List:
  "OBEX File Transfer" (0x1106)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 10
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x454e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "OBEX File Transfer" (0x1106)
    Version: 0x0100

Service Name: OBEX Object Push
Service RecHandle: 0x10003
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 9
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x454e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0100
```

```
Service Name: SyncMLClient
Service RecHandle: 0x10004
Service Class ID List:
  UUID 128: 00000002-0000-1000-8000-0002ee000002
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 11
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x454e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "" (0x00000002-0000-1000-8000-0002ee000002)
    Version: 0x0100

Service Name: Imaging
Service RecHandle: 0x10005
Service Class ID List:
  "Imaging Responder" (0x111b)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 15
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x454e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "Imaging" (0x111a)
    Version: 0x0100
```

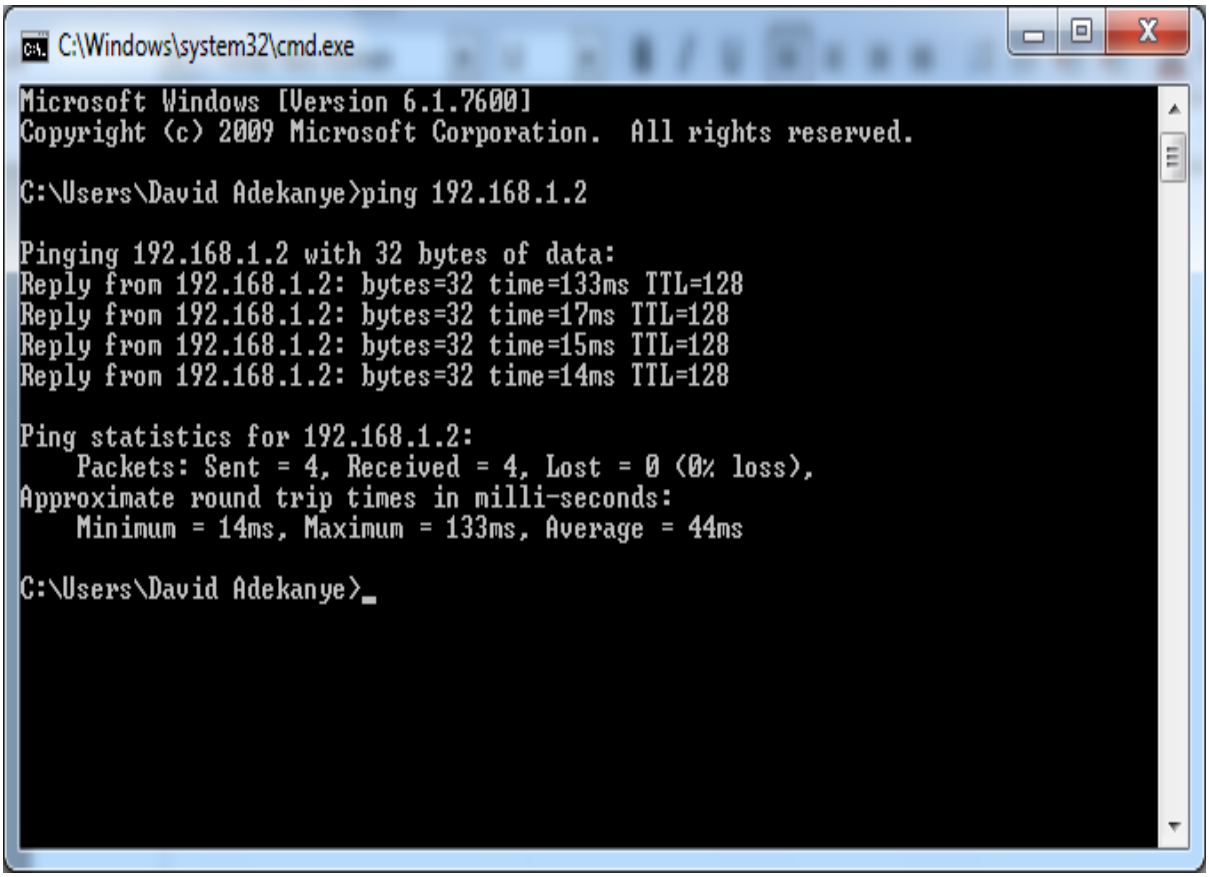
```
Service Name: Nokia OBEX PC Suite Services
Service RecHandle: 0x10006
Service Class ID List:
  UUID 128: 00005005-0000-1000-8000-0002ee000001
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 12
  "OBEX" (0x0008)
Language Base Attr List:
  code_ISO639: 0x454e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "" (0x00005005-0000-1000-8000-0002ee000001)
    Version: 0x0100

Service Name: Dial-Up Networking
Service RecHandle: 0x10007
Service Class ID List:
  "Dialup Networking" (0x1103)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 3
Language Base Attr List:
  code_ISO639: 0x454e
  encoding:    0x6a
  base_offset: 0x100
Profile Descriptor List:
  "Dialup Networking" (0x1103)
    Version: 0x0100

akhanolu@idahosa:~$
```

APPENDIX B



Picture 11. *Ping result for Idahosa-PC*

APPENDIX C



***Picture 12**. Ping result for Dafidi-HP*