BLUETOOTH SECURITY
Logical Link Control and Adaptation Protocol

Asish Chandra Choudhury

Roll. 710CS1027

under the supervision of

Prof. Suchismita Chinara

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela – 769008, India

Bluetooth Security Logical Link Control and Adaptation Protocol

Dissertation submitted in

MAY 27

to the department of Computer Science

and Engineering of

National Institute of Technology Rourkela

in partial fulfillment of the requirements

for the degree of

Master of Technology

by

Asish Chandra Choudhury

(Roll. 710CS1027)

under the supervision of

Prof. Suchismita Chinara

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela – 769 008, India

Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela-769 008, India. www.nitrkl.ac.in

Feb 13, 2015

Certificate

This is to ensure that the work in the theory entitled Bluetooth Security by Asish Chandra Choudhury, bearing move number 710CS1027, is a record of a unique exploration work did by him under my watch and direction in halfway satisfaction of the necessities for the recompense of the level of Master of Technology Dual Degree in Computer Science and Engineering Department. Neither this theory nor any piece of it has been submitted for any degree or scholastic grant somewhere else.

Dr. Suchismita Chinara
Associate Professor
Department of CSE
NIT, Rourkela

Acknowledgment

As a matter of first importance, I might want to express my profound feeling of appreciation and appreciation towards my boss Prof. Suchismita Chinara, who has been the controlling compel behind this work. I need to say thanks to her for acquainting me with the field of Bluetooth Security and issuing me the chance to work under her. Her unified confidence in this point and capacity to draw out the best of explanatory and functional abilities in individuals has been important in extreme periods. Without her priceless guidance and help it would not have been workable for me to finish this postulation. I am significantly obliged to her for her steady consolation and significant exhortation in every part of my scholastic life. I think of it as my favorable luck to have got a chance to work with such a brilliant individual.

I thank our H.O.D. Prof. Santanu Kumar Rath for his consistent backing in my proposal work. They have been extraordinary wellsprings of motivation to me and I express gratitude toward them in the name of all that is holy.

I might likewise want to thank all employees, PhD researchers, my seniors and youngsters and all partners to give me their standard proposals and supportive gestures amid the entire work.

At last yet not the slightest I am owing debtors to my family to bolster me frequently amid my tough times.

I wish to thank all employees and secretarial staff of the CSE Department for their thoughtful collaboration.

Asish Chandra Choudhury

Abstract

The point of our work is to assess security dangers in Bluetooth-empowered frameworks. Our exploration work focuses on handy parts of Bluetooth security. It can be generally isolated into four sections. First and foremost, shortcomings of Bluetooth security are mulled over taking into account a writing survey, and a Bluetooth security research center environment for actualizing Bluetooth security assaults by and by has been manufactured. Also, distinctive sorts of assaults against Bluetooth security are researched and the possibility of some of them are shown in our exploration lab. Countermeasures against every sort of assault are likewise proposed. Thirdly, a portion of the current Bluetooth security assaults are upgraded and new assaults are proposed. To do these assaults by and by, Bluetooth security investigation devices are executed. Countermeasures that render these assaults unreasonable are likewise proposed. At long last, a relative examination of the current Man-In-The-Middle assaults on Bluetooth is displayed, a novel framework for distinguishing and forestalling interruptions in Bluetooth systems is proposed, and a further arrangement of Bluetooth-empowered specially appointed systems is given.

Contents

List of Figures

Chapter 1

Introduction

Bluetooth[5] is an innovation for short range remote information and realtime two-way voice exchange giving information rates up to 3 Mb/s. It can be utilized to unite any gadget to another gadget. Bluetooth[5]-empowered gadgets, for example, cell telephones, headsets, PCs, portable PCs, printers, mice, and consoles, are generally utilized everywhere throughout the world. As of now in 2006, the one billionth Bluetooth gadget was sent, and the volume is relied upon to increment quickly soon. The objective volume for 2010 is as high as two billion Bluetooth[5] gadgets. Hence, it is imperative to stay up with the latest. As an interconnection innovation, Bluetooth[5] needs to address all conventional security issues, no doubt understood from conveyed systems. Likewise, security issues in remote adhoc systems are a great deal more intricate than those of more customary wired or brought together remote systems. Besides, Bluetooth[5] systems are shaped by radio connections, which implies that there are extra security viewpoints whose effect is not yet surely knew. The L2CAP[2] (Logical Link Control and Adaptation Protocol) is a product module that typically lives on the host. The ACL[1] connection gives a parcel exchanged association between the expert and all dynamic slaves in the piconet. Diffie-Hellman key[6] trade is taking into account the utilization of discrete logarithm. The L2CAP[2] (Logical Link Control and Adaptation Protocol) is a product module that typically lives on the host. The ACL[1] connection gives a bundle exchanged association between the expert and all dynamic slaves in the piconet. Diffie-Hellman key[6] trade is in view of the utilization of discrete logarithm

1.1 Bluetooth versions

The preparatory work for creating Bluetooth[5] innovation began in 1994, when Ericsson started exploring the conceivable methods for supplanting links in the middle of adornments and portable telephones with remote connections. Ericsson immediately understood the potential business for Bluetooth items, yet overall collaboration was required for the items to succeed. Along these lines, the Bluetooth SIG [Blu07b] was established in February 1998 by Ericsson, Nokia, IBM, Intel and Toshiba. 3Com, Lucent, Microsoft and Motorola joined the Bluetooth SIG in December 1999.These nine individuals from the Bluetooth SIG are known as the Bluetooth SIG Promoters. They are in charge of upper-level SIG organization, and for giving labor to run the advertising, capability and lawful procedures. At present, the Bluetooth SIG has more than 10000 part organizations.

1.1.1 First Version

The primary open adaptation of Bluetooth[5] particular, Bluetooth 1.0A [Blu99a], was discharged in July 1999. Numerous gadget producers experienced issues in making their Bluetooth 1.0A good items interoperable. Consequently, the Bluetooth 1.0B particular [Blu99b] was discharged later around the same time (December 1999) to alter the interoperability issues. The Bluetooth 1.1 particular [Blu01] was discharged in February 2001. It altered numerous mistakes that were found in the Bluetooth
1.0B particular and included backing for decoded correspondence and additionally bolster for RSSI (Received Signal Strength Indicator).RSSI is an estimation of the got radio sign quality that is utilized for controlling power as a part of Bluetooth gadgets. It can likewise be utilized for Bluetooth situating purposes, for instance.

The Bluetooth 1.2 specification [Blu03] was launced in November 2003. It included major modifications such as: [Blu03]

- AFH (Adaptive Frequency Hopping): AFH further modifies the original Bluetooth frequency hopping method FHSS (Frequency Hopping Spread Spectrum) by ignoring the use of channels that suffer from interference. A maximum of 59 ”bad” channels can be turned off during the communication session, i.e. only 20 different ”good” channels are essential. AFH too serves higher transmission speeds in practice by decreasing the demand for retransmissions.

- eSCO (extended Synchronous Connection-Oriented): eSCO modifies the voice quality of Bluetooth audio links by allowing retransmissions of corrupted packets.

- Optional QoS (Quality-of-Service) improvements : QoS improvements further improve the scope for error detection, flow controlling and synchronization.

1.1.2 Further Version

The Bluetooth 2.0+EDR (Enhanced Data Rate) determination [Blu04a] was discharged in November 2004. The fundamental change was the presentation of EDR, which gives information rates up to 3 Mb/s. The first Bluetooth information rate before EDR was 1 Mb/s. As per the Bluetooth SIG, EDR has the accompanying impacts on Bluetooth correspondence: [Blu04a,Blu04b]

- Three times better transmission speed (up to 10 times in certain cases).

- Lower power consumption by a reduced duty cycle.

- Simplification of multilink scenarios due to more present bandwidth

- Further improved BER (Bit-Error-Rate) performance.

1.1.3 New Version

New Bluetooth forms are in reverse perfect with the more seasoned variants. The most recent open rendition of Bluetooth determination, Bluetooth 2.1+EDR [Blu07a], was discharged in July 2007. It gives numerous upgrades, for example, [Blu07a]

- Encryption Pause Resume: Encryption Pause Resume will further upgrade security by permitting scrambled connections to change their encryption keys intermittently. Expert slave role switches (Section 2.2 clarifies the expert slave relationship) will likewise be conceivable on an encoded connection.
- Extended Inquiry Response: Extended Inquiry Response will give more data, for example, the name of the gadget and a rundown of bolstered administrations, amid the request method, permitting better gadget sifting before the association is built up.
- SSP: SSP fundamentally enhances the Bluetooth matching background by simplifying the blending procedure from the client's perspective. It will likewise expand the quality of security by giving the assurance against both detached listening in assaults and MITM assaults (dynamic spying assaults). The Bluetooth SIG expects that this highlight will essentially build the utilization of Bluetooth innovation.
- NFC (Near Field Communication) [NFC08] as an OOB (Out-Of-Band) channel: In order to give assurance against MITM assaults, SSP either utilizes NFC as an OOB channel or requests that the client look at two six-digit numbers. Such a correlation can also be thought as an OOB channel which is not controlled by the MITM. However,when NFC radio interface is accessible, SSP bolsters the programmed formation of secure Bluetooth associations.
- Sniff Subrating: Sniff Subrating will further lessen the force utilization of Bluetooth gadgets. For instance, it will build the battery life of HID (Human

Interface Devices) gadgets, for example, mice and consoles, by 3 to 10 times contrasted and the battery life times of more seasoned Bluetooth HID gadgets.

1.2 Bluetooth communication

Connection sorts define the ways Bluetooth devices can exchange data. Bluetooth has three connection sorts: ACL[1] (Asynchronous Connection-Less), SCO[1] (Synchronous Connection-Oriented) and eSCO.

1. SCO connections are symmetric (greatest of 64 kb/s for both headings) and are utilized for transferring realtime two-way voice. Retransmission of voice bundles is not utilized. Accordingly, when the channel BER is high, voice can be twisted.

2. eSCO connections are likewise symmetric (most extreme of 864 kb/s for both headings) and are utilized for exchanging realtime two-way voice. Retransmission of bundles is utilized to guarantee the trustworthiness of information (voice). Since retransmission of parcels is utilized, eSCO connections can likewise convey information bundles. Then again, they are basically utilized for exchanging realtime two-way voice. Bluetooth 1.2 (or later) gadgets can utilize eSCO joins, yet they should likewise bolster SCO connections to provide backward-similarity.

ACL connections are for symmetric (greatest of 1306.9 kb/s for both bearings) or unbalanced (greatest of 2178.1 kb/s for send and 177.1 kb/s for get) information exchange. Retransmission of parcels is utilized to guarantee the honesty of information.

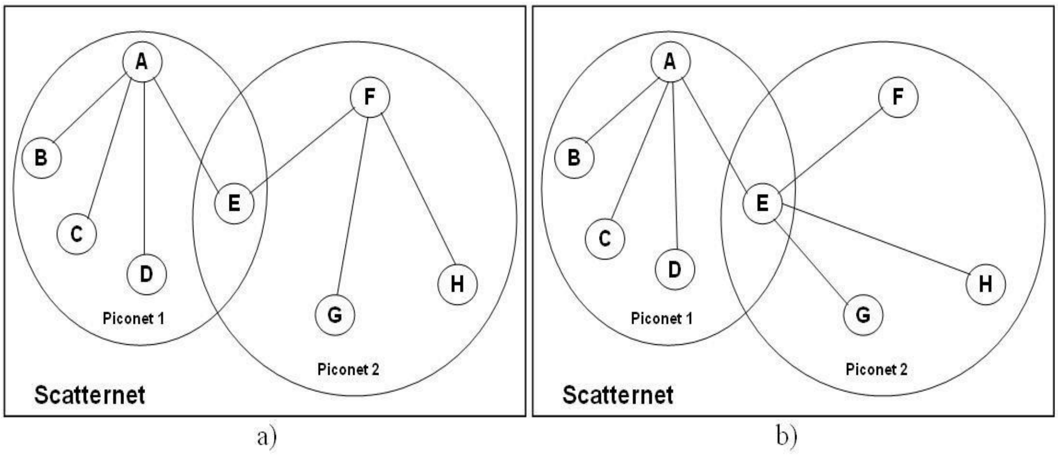
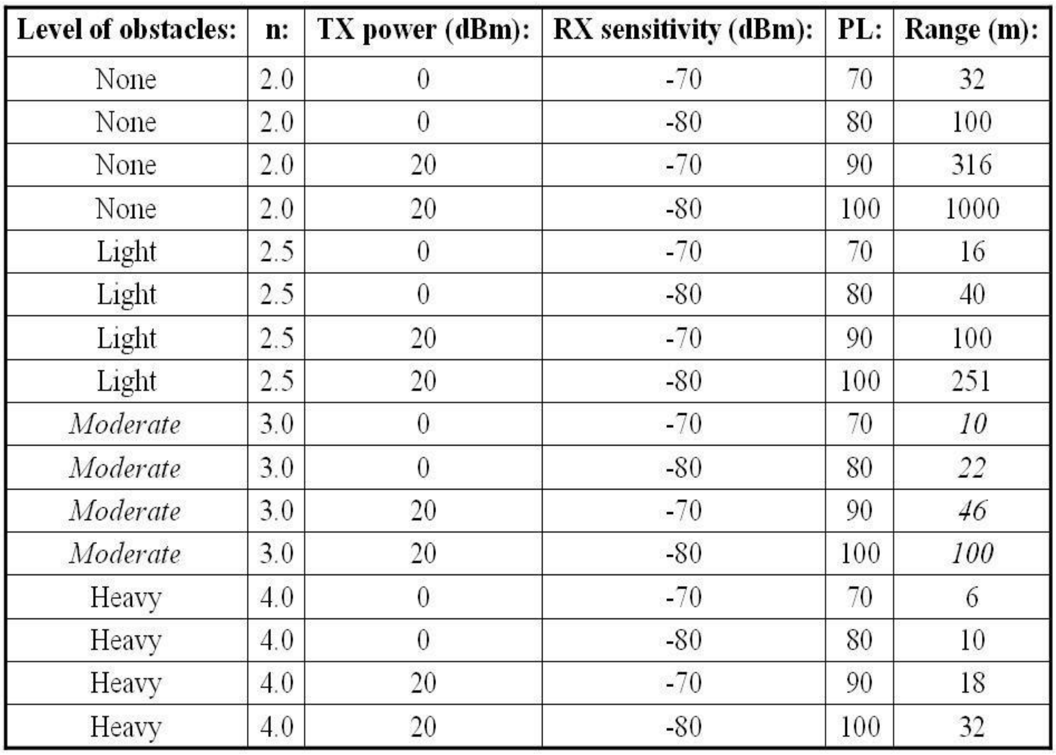


Figure 1.1: a) Bluetooth topology when ACL links are used. b) Bluetooth topology when SCO or eSCO links are used.

1.3 Special characteristics of the Bluetooth medium

Bluetooth is a remote RF correspondence framework utilizing chiefly omnidirectional antennas.Communication with other Bluetooth gadgets is conceivable inside of the reach, and no direct lineof-sight between the imparting Bluetooth gadgets is needed. This capacity makes Bluetooth correspondence much simpler to use than the conventional link based correspondence or short range direct viewable pathway infrared correspondence, however then again it too makes spying much less demanding.Bluetooth devices can create ad-hoc networks of several devices in which no fixed infrastructure is required.

There are three Bluetooth gadget classes: class 1, class 2 and class 3. The greatest transmit powers for class 1, class 2 and class 3 gadgets are 100 mW (20 dBm, i.e. 20 decibels relative to one milliwatt), 2.5 mW (4 dBm), and 1 mW (0 dBm) individually. As indicated by the Bluetooth particular [Blu07a], the reference affectability level of a Bluetooth gadget needs to be -70 dBm or



Level of obstacles:	n:	TX power (dBm):	RX sensitivity (dBm):	PL:	Range (m):
None	2.0	0	-70	70	32
None	2.0	0	-80	80	100
None	2.0	20	-70	90	316
None	2.0	20	-80	100	1000
Light	2.5	0	-70	70	16
Light	2.5	0	-80	80	40
Light	2.5	20	-70	90	100
Light	2.5	20	-80	100	251
Moderate	3.0	0	-70	70	*10*
Moderate	3.0	0	-80	80	*22*
Moderate	3.0	20	-70	90	*46*
Moderate	3.0	20	-80	100	*100*
Heavy	4.0	0	-70	70	6
Heavy	4.0	0	-80	80	10
Heavy	4.0	20	-70	90	18
Heavy	4.0	20	-80	100	32

Figure 1.2: range of bluetooth devices

better.

The scope of Bluetooth[5] gadgets relies on upon the class of gadgets at both closures, the affectability levels at both closures, and the level of obstructions. The amount n is the supposed PL (Path Loss) example that can be conformed to record for the measure of disarray in the way between the transmitter and the beneficiary. The level of hindrances can be generally separated into four classifications: none (a free space without disarray in the transmit-get way; n=2.0), light (a gently jumbled way, for example, an office situation with moveable dividers; n=2.5), moderate (a reasonably jumbled way, for example, an office domain with altered dividers; n=3.0), or overwhelming (a vigorously jumbled way in which the thickness of the materials utilized as a part of the building’s development is high; n=4.0).

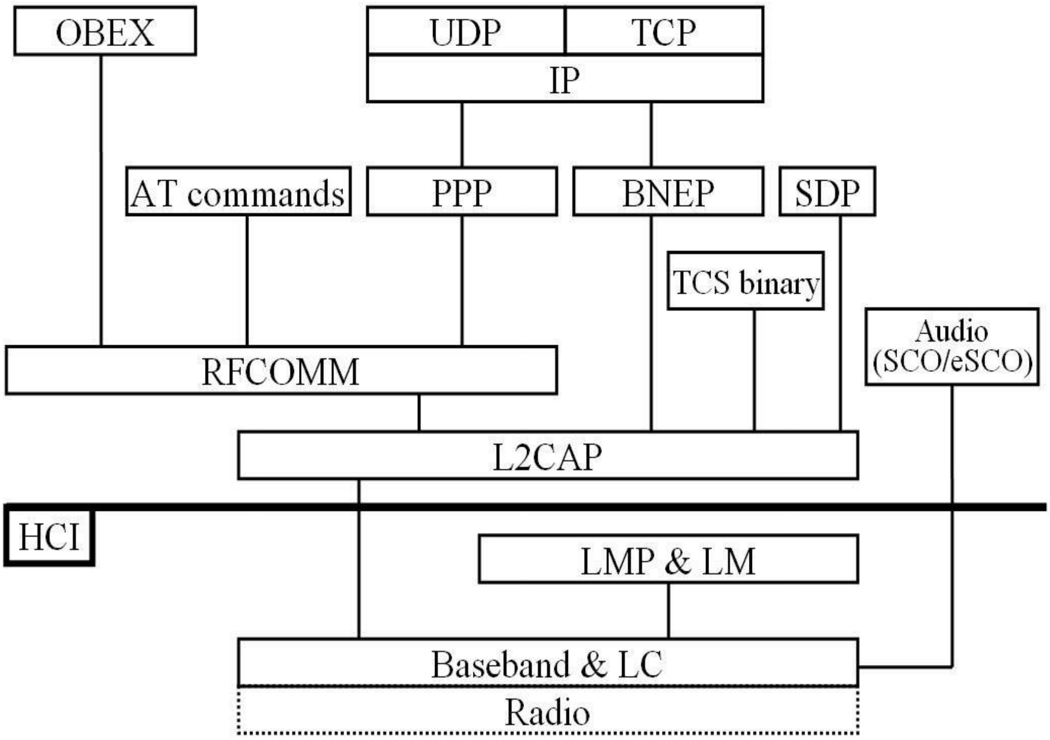


Figure 1.3: Bluetooth protocol stack.

1.3.1 Protocols

- Protocols beneath the HCI (Host Controller Interface)are assembled into the Bluetooth microchip, and conventions over the HCI are situated as a piece of the host gadget’s product bundle. A HCI is required between the equipment and programming conventions. The reason for the HCI is to empower the maker autonomous consolidating of Bluetooth chips (Host Controller) and the genuine host gadget. The HCI deals with security correspondence between the host and the Bluetooth module.
- Baseband and LMP (Link Manager Protocol)together empower the physical RF connection.The LC (Link Controller) is a state machine that characterizes the current condition of the Bluetooth gadget. A Bluetooth gadget can be in low-control mode for sparing batteries, in the

associated state for ordinary piconet operation, or in the paging state for the expert to convey new slaves to the piconet, for instance. The LC has a pseudorandom number era ability, techniques for overseeing security keys, and the capacity for giving the scientific operations expected to verification and encryption.

- The LM (Link Manager)acts as a contact between the application and the LC on the neighborhood gadget, and it likewise speaks with the remote LM by means of PDUs (Protocol Data Units) utilizing the LMP, i.e. the LM corresponds with three unique substances amid a Bluetooth session: the nearby host through the HCI, the neighborhood LC (nearby operations), and the remote LM (join arrangement, join data, and connection administration operations). The PDU is recognized at the Baseband level, yet it is followed up on by the LM. The neighborhood LM ordinarily lives on the Bluetooth module as a complete host-module execution. The remote LM can be characterized as the LM at the flip side of the Bluetooth join. The LM additionally has a few summons for taking care of security issues. [Blu07a, Mor02]
- SCO[1]and eSCO[1]links are utilized for exchanging realtime two-way voice.They are built up specifically from the Baseband level, so the overhead of upper layer conventions does not bring about any postponements for realtime two-way voice associations. Four parcel sorts have been characterized for SCO joins, though eSCO connections bolster seven bundle sorts [Blu07a]. One of these 11 parcel sorts, SCO join's HV1 (High-quality Voice 1), is truly fascinating from the security perspective, in light of the fact that one single HV1 SCO connection holds all Bluetooth piconet assets and subsequently makes different DoS (Denial-of-Service) assaults conceivable.
- TheL2CAP[2] (Logical Link Control and Adaptation Protocol)is a product module that ordinarily lives on the host. It fits upper

layer conventions to the Baseband, i.e. it goes about as a channel for information on the ACL connection between the Baseband and host applications. The L2CAP[2] additionally offers CO (Connection-Oriented; from expert to one slave and from slave to ace) and CL (Connection-Less; from expert to different slaves) administrations, and it is characterized just for ACL joins. Lower layer conventions don't need to know how layers over the L2CAP[2] work and viceversa. The L2CAP[2] can start security systems when a CO or a CL channel association endeavor is made.

- The SDP (Service Discovery Protocol)is used to discover the administrations of Bluetooth gadgets in the range.RFCOMM (Radio Frequency Communication)emulates serial ports over the L2CAP, what's more, along these lines it is conceivable to utilize existing serial port applications through Bluetooth.
- The OBEX (Object Exchange Protocol)is used to trade items, for example, schedule notes, business cards and information documents, between gadgets by utilizing the customer server model. The OBEX underpins six straightforward and obvious operations: Connect (pick your accomplice, arrange capacities and build up association), Disconnect (end association), Put (push articles to the server), Get (draw objects from the server), (prematurely end an article trade that is in advancement), and SetPath (set server's index way to another worth).
- The TCS (Telephony Control convention Specification)binary characterizes the call control flagging for the foundation/arrival of discourse and information calls between Bluetooth gadgets. It too gives usefulness to trading flagging data that is irrelevant to continuous calls. Numerous AT orders are additionally upheld for transmitting control signals for telephony control.
- The BNEP (Bluetooth Network Encapsulation Protocol)is used to give organizing abilities for Bluetooth gadgets. It permits IP (Internet

Protocol) parcels to be conveyed in the payload of L2CAP bundles. The IP is a system layer convention in the TCP/IP (Transmission Control Protocol/Internet Protocol) convention suite. TCP and UDP (User Datagram Protocol) are transport layer center conventions utilized as a part of the TCP/IP convention suite. PPP (Point-to-Point Convention) can likewise be utilized to give TCP/IP organizing abilities for Bluetooth gadgets,yet, it is slower, i.e. it meets expectations over RFCOMM while BNEP lives up to expectations straightforwardly over the L2CAP,what's more, along these lines PPP is once in a while utilized at this point.

Chapter 2

Litreture Survey

2.1 Cryptography

The primary ideas of the general population key encryption plan are::

(a) Plaintext : The plaintext is the initial understandable message or information sustained into the encryption algorithm as input.

(b) Encryption algorithm : The encryption algorithm performs different changes on the plaintext

(c) Public key: The public key is required for encryption.

(d) Private key: The private key is essential for decryption.

(e) Cipher text: The ciphertext is a scrambled message produced as an output that takes into account the plaintext and the public key.

(f) Decryption algorithm : The decryption algorithm receives the ciphertext and the matching private key, and gives the original plaintext.

2.2 Analysis of existing schemes

Diffie-Hellman key[6] exchange relies on the use of discrete logarithm. Pick a prime p and a number g¡p, which is a primitive base of p. We know numbers p and g are public.

(a) User A chooses the private key $S_A < p$ and calculates the public key
S_A
$J_A = g^{S_A} \mathrm{mod} p$. Hence, the whole public key of user A is (p, g, J_A).

(b) The public key is used for sharing a common secret key by the given way:

- User A sends the public key (p,g,J_A) to user B and user B sends (p,g,J_B) to user A too.
- User A computes $J_B^{S_A} = g^{S_B S_A}$, and user B computes $J_A^{S_B} = g^{S_A S_B}$ too.
- $g^{S_A S_B}$ is their common secret key (to be used for symmetric encryption), that is difficult for outsiders to invent, even if they know p, g, J_A and J_B.

2.2.1 Security

The security of a symmetric cryptosystem relies on upon two things: the quality of the calculation and the length of the key. There are two general methodologies for assaulting a symmetric encryption plan:

- Cryptanalysis: Cryptanalytic assaults depend on the way of the calculation and maybe some learning of the general qualities of plaintext or even some example plaintext-ciphertext sets. The fundamental point is to adventure the qualities of the calculation trying to find a particular plaintext or to reason the key being utilized. On the off chance that the key (or even a piece of the key) is found, all future and past messages encoded with that key are traded off.

– Brute force attack: An assailant tries each conceivable key esteem on a bit of ciphertext until a comprehensible interpretation into plaintext is acquired. All things considered, 50conceivable key qualities must be attempted to make progress.

2.3 Connections in Bluetooth

Connections sorts characterize the ways Bluetooth gadgets can trade information. Bluetooth[5] has three connection sorts:

(a) ACL[1] (Asynchronous-Connection-Less), SCO (Synchronous-Connection-Oriented) and eSCO. SCO connection is utilized to exchange of constant administrations (mostly voice application).

(b) ACL[1] connection is expected for exchanging of nonconcurrent activity (information application, for example, document exchange, astounding sound/feature exchange etc.

(c) Bluetooth Baseband convention bolsters both SCO connection and ACL connection, while Logical Link Control and Adaptation Protocol (L2CAP[2]) just bolster ACL join.

(d) All the Bluetooth ACL information applications or higher layer conventions use L2CAP[2] to correspond with the Baseband.

The essential part of the L2CAP[2] layer is to shroud the normal for the lower layer transport conventions from the higher layers in the convention stack.

2.3.1 Protocol Specification:

Logical Link Control and Adaptation protocol (L2CAP)[2] is layered over the Baseband Protocol and dwells in the information connection layer. The convention gives association situated and connectionless information administrations to upper layer conventions. Useful necessities for L2CAP[2] are convention multiplexing, division and reassembly, and gathering management.L2CAP[2] depiction is taking into account the idea of ’channels’. Consistent channel endpoint on the gadget is spoken to with channel identifier(C1D).

Logical Link Control and Adaptation convention (L2CAP) is layered over the Baseband Protocol and lives in the information connection layer. The convention gives association situated and connectionless information administrations to upper layer conventions. Utilitarian necessities for L2CAP[2] are convention multiplexing, division and reassembly, and gathering administration.L2CAP[2] depiction is taking into account the idea of ’channels’.Logical channel endpoint on the gadget is spoken to with channel identifier.In this paper we concentrate on a setup process for transaction of the channel parameters. Setup stage must be entered preceding information trade, and may be re-entered if channel parameters need to be renegotiated amid information transmission.

Chapter 3

Proposed Scheme

3.1 Diffie-Hellman Protocol

Diffie-Hellman[6] key exchange is based on the use of discrete logarithm.

– Choose a prime p and a number $g < p$, which is a primitive root of p. Numbers p and g are public.

– User A chooses the private key $S_A < p$ and computes the public key $S_A J_A = g^{S_A} \mathrm{mod} p$. Therefore, the whole public key of user A is (p, g, J_A).

– The public key can be used for sharing a common secret key in the following way:

– User A sends the public key (p,g,J_A) to user B and user B sends (p,g,J_B) to user A.

– User A computes $J_B^{S_A} = g^{S_B S_A}$, and user B computes $J_A^{S_B} = g^{S_A S_B}$.

$g^{S_A S_B}$ is their common secret key (to be used for symmetric encryption), which is difficult for others to invent, even if they know p,g,J_A and $J_{B.}$.

3.2 Bluetooth security architecture

The different types of connectability and discoverability capabilities can be split into three categories, or security levels:

- Silent : The device will not accept any connections. It simply checks Bluetooth traffic.
- Private : The device can never be discovered, i.e. it is hence so-called non-discoverable device. Connections are accepted only if the BD$_A$DDR (Bluetooth Device Address) of the device is known to the prospective master. A 48-bit BD$_A$DDR is generally unique and refers as a whole to only one individual Bluetooth device.
- Public: The device is both discoverable and connected to. It is hence called a discoverable device.

.

There are also four different security modes that a device can implement. In Bluetooth technology, a device can be in only one of the following security modes at a time:

- Nonsecure : The Bluetooth device does not initiate any security measures.
- Service-level enforced security mode: Two Bluetooth devices can establish a nonsecure ACL link. Security procedures, namely authentication, authorization and optional encryption, are initiated when an L2CAP CO or an L2CAP CL channel request is made.
- Link-level enforced security mode: Security procedures are initiated when an ACL link is established.
- Service-level enforced security mode: This mode is similar to mode 2, except that only Bluetooth devices using SSP can use it, i.e. only Bluetooth 2.1+EDR (or later) devices can use this security mode.

3.2.1 Authentication

Authentication is used for supplying the identity of one piconet device to another. The output of authentication are used for determining the client's authorization level, which can be implemented in several distinct ways: for example, access can be granted to all services, only to a subset of services, or to some services while other services require extra authentication. Encryption is utilized for encoding the information being exchanged between Bluetooth devices in such a way that eavesdroppers cannot decipher its contents. Bluetooth security is developed on building a chain of events, none of which provides meaningful information to an eavesdropper, and all events must occur in a distinct sequence for security to be created successfully. Two Bluetooth devices begin pairing with the same textitPIN (Personal Identification Number) code that is used for generating several 128-bit keys. PIN code selection, for example in a private Bluetooth network environment, i.e.when a Bluetooth network consists of various Bluetooth devices such as a mobile phone, a printer, a DVD (Digital Versatile Disc; also known as Digital Video Disc) player, a mouse and a keyboard, can be done by using the same PIN code for all Bluetooth gadgets, because the user owns and hence also trusts all Bluetooth devices that are used in his private Bluetooth network. However, each master-slave pair can have a distinct PIN code for supplying trusted relationship between the devices. Therefore, PIN code selection, for example in a conference environment where two ”friends” meet and want to generate a Bluetooth network between their gadgets, should be done by using a distinct PIN code for each master-slave pair, because otherwise all other Bluetooth connections that are utilizing the same PIN code may be compromised, i.e. it is possible that the ”friend” will use the PIN code for eavesdropping or for attacking purposes. SAFER+ with a 128-bit key is used as an algorithm for Bluetooth authorization and key generation.

An initialization key (Kinit) is generated when Bluetooth devices unite for the first time and it is used for securing the generation of other more secure 128-bit keys, which are generated during the next phases of the security chain of events. The Kinit is generated from a 128-bit pseudorandom number IN_{RAND}, an L-byte PIN code, and a BD_{ADDR}. It is important that the IN_{RAND} is sent through air in unencrypted form. The product of a certain key generation function can be defined in terms of the function itself and its inputs. The Kinit is derived in both devices using the formula Kinit=E22(PIN’,L’,IN_{RAND}). The PIN code and its length L are enhanced into two different quantities called PIN’ and L’ before sending them to the E22 function. If the PIN is less than 16 bytes, it is joined by appending bytes from the device?s BD_{ADDR} until the PIN’ either reaches a total length of 16 bytes or the entire BD_{ADDR} is joined, whichever comes first. If one gadget has a fixed PIN code, the BD_{ADDR} of the other gadget is used. If both gadgets can support a variable PIN code, the BD_{ADDR} of the gadget that received the IN_{RAND} is used. The Kinit is used to encrypt a 128-bit pseudorandom number (RAND or LK_{RAND}), i.e. RAND⊕Kinit or LK_{RAND}⊕ Kinit, exchanged in the next phase of the security chain of events where a link key (a unit key or a combination key) is created. A unit key (KA) is generated from the information of only one device (device A) by using the formula A=E21(BD_{ADDRA},RANDA). Gadget A encrypts the KA with the Kinit, i.e. KA ⊕ Kinit, and sends it to gadget B. Gadget B decrypts the KA with the Kinit, i.e. (KA ⊕ Kinit) ⊕ Kinit=KA, and now both gadgets have the same KA as a link key. Only gadgets that have limited resources, i.e. no memory to store several keys, should utilize the KA, because it provides only lower level of security. Therefore, Bluetooth specifications do not recommend using

KA. A combination key (KAB) is subordinate on two devices and hence it is originated from the information of both gadgets. The KAB is generated in both devices using the formula $KAB=E21(BD_{ADDRA},LK_{RANDA})\oplus E21(BD_{ADDRB},LK_{RANDB})$. It is important that generating the KAB is nothing more than a simple bitwise XOR between two unit keys, i.e. $KAB=KA \oplus KB$. Each gadget can generate its own unit key and each gadget also has the BD_{ADDR} of the other gadget. Hence, two gadgets have to exchange only their respective pseudorandom numbers in order to produce each other?s unit key. Gadget A encrypts the LK_{RANDA} with the current key K, i.e. $LK_{RANDA} \oplus K$ where K can be the Kinit, the KA or the KAB that was created earlier, and sends it to gadget B. The K is the Kinit if the gadgets create a link key for the first time together. The K is the KA if the link key is being upgraded to a combination key, and it is the KAB if the link key is being changed. ZGadget B decrypts the LK_{RANDA} with the K, i.e. $(LK_{RANDA} \oplus K) \oplus K = LK_{RANDA}$, and can now generate the KA. Accordingly, gadget B encrypts the LK_{RANDB} with the K, i.e. $LK_{RANDB} \oplus K$, and sends it to gadget A. Gadget A decrypts the LK_{RANDB} with the K, i.e. $(LK_{RANDB} \oplus K) \oplus K = LK_{RANDB}$, and produces the KB. Finally, both gadgets can generate the KAB by XORing the KA with the KB, i.e. $KAB = KA \oplus KB$. The next phase of the security chain of events is the challenge-response authentication in which a claimant's memory of a secret link key is verified. During each authentication, a new 128-bit pseudorandom number $AU_{RAN\ D}$ is exchanged through air in unencrypted format. Other inputs to the authorization function E1 are the BD_{ADDR} of the claimant and the current link key (KA or KAB).

Chapter 4

Implementation Of Proposed Scheme

4.1 Details regarding implementation

32feet.NET is also known as InTheHand

(a) Makes a direct data connection.

    i. Adds Virtual Serial Port

(b) Does an OBEX transfer.

(c) Has the Bluetooth stack and/or the OS connect to and use a remote service.

(d) Makes a direct data connection using the L2CAP protocol.

(e) Checks whether a particular device is in range.

OBEX utilizes a client-server model and is free of the transport mechanism and transport API.

A Bluetooth[5] empowered device needing to set up an OBEX communication session with another device is thought to be the client device.

The OBEX protocol also characterizes a folder-listing object, which is used to browse the contents of folders on remote gadget. RFCOMM is used as the fundamental transport layer for OBEX.

OBEX empowers applications to work over the Bluetooth technology protocol stack as well as the IrDA stack.

For Bluetooth empowered gadgets, only connection-oriented OBEX is supported. Three application profiles have been produced using OBEX which incorporate SYNC, FTP and OPP.

There are two sorts of OBEX operations: a PUT and a GET. The PUT operation is to send an article from the customer to the server and the GET operation is to give back an item from the server to the customer.

4.2 IrMC

IrMC Server The gadget that provides an object exchange server. Typically, this gadget is a mobile phone or PDA.

IrMC Client The gadget which contains a sync engine and pulls and pushes the PIM data from and to the IrMC Server. Usually, the IrMC Client device is a PC

4.3 RFCOMM

The RFCOMM protocol emulates the serial cable line settings and status of an RS-232 serial port and is used for providing serial data

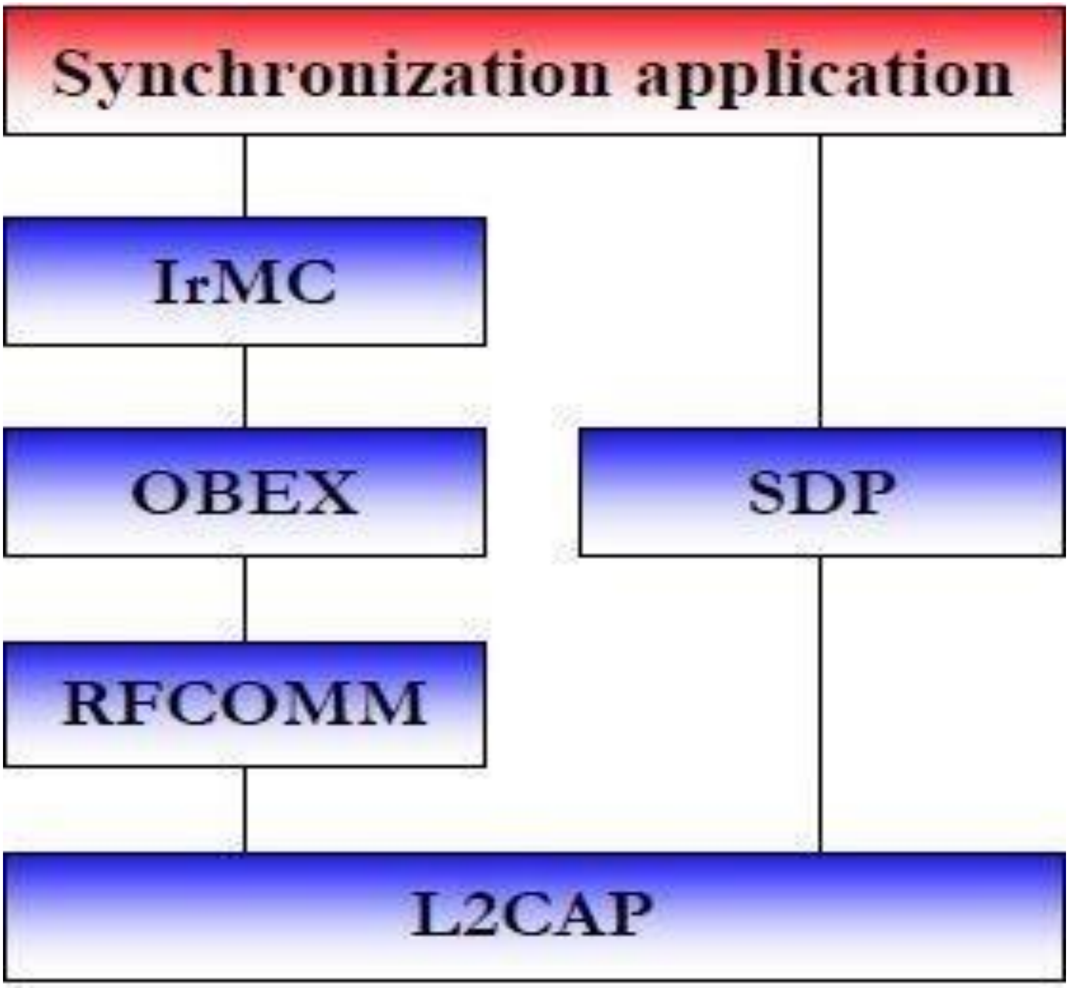


Figure 4.1: Synchronisation Application

transfer. RFCOMM connects to the lower layers of the Bluetooth protocol stack through the L2CAP layer.

4.4 Bluetooth Application Profiles Using OBEX

– Synchronization:Basically, the synchronization means comparing two object stores, deciding their differences, and then binding these two object stores.

– File Transfer:At the least, the File Transfer profile is intended for sending and retrieving generic files to and from the Bluetooth gadget.

– Ob ject Push:The Object Push profile is the extraordinary case of the File Transfer Profile for bearing objects and alternatively pulling the default objects

4.5 Modules

4.5.1 Bluetooth Connectivity(Pairing)

The RFCOMM protocol copies the serial cable line settings and status of an RS-232 serial port and is used for providing serial data transfer. RFCOMM joins the lower layers of the Bluetooth protocol stack through the L2CAP layer.

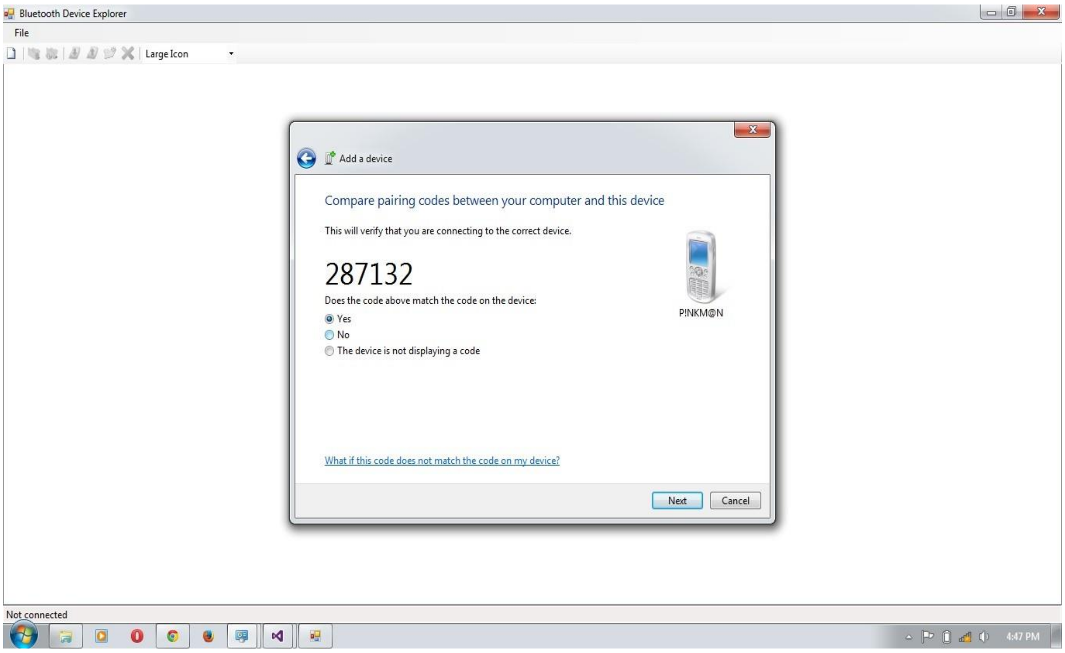
4.5.2 Bluetooth Key Authentication

Basically, the synchronization means contrasting two object stores, determining their differences, and then binding these two object stores.

4.5.3 Bluetooth Data Transmission

There are two sorts of OBEX operations: a PUT and a GET. The PUT operation is to send an article from the customer to the server and the GET operation is to give back an item from the server to the customer.

4.6 Screen shots



Compare pairing codes between your computer and this device

This will verify that you are connecting to the correct device.

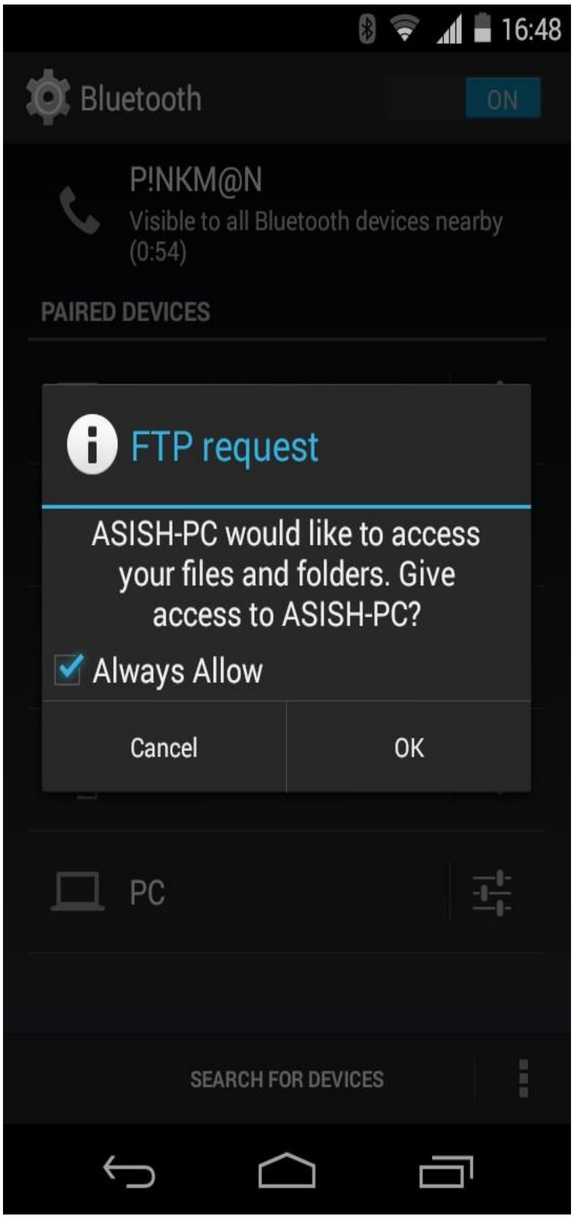
287132

Does the code above match the code on the device:

● Yes
○ No
○ The device is not displaying a code

What if this code does not match the code on my device?

Figure 4.2: Comparing pairing codes between two devices.



16:48

Bluetooth ON

P!NKM@N

Visible to all Bluetooth devices nearby (0:54)

PAIRED DEVICES

FTP request

ASISH-PC would like to access your files and folders. Give access to ASISH-PC?

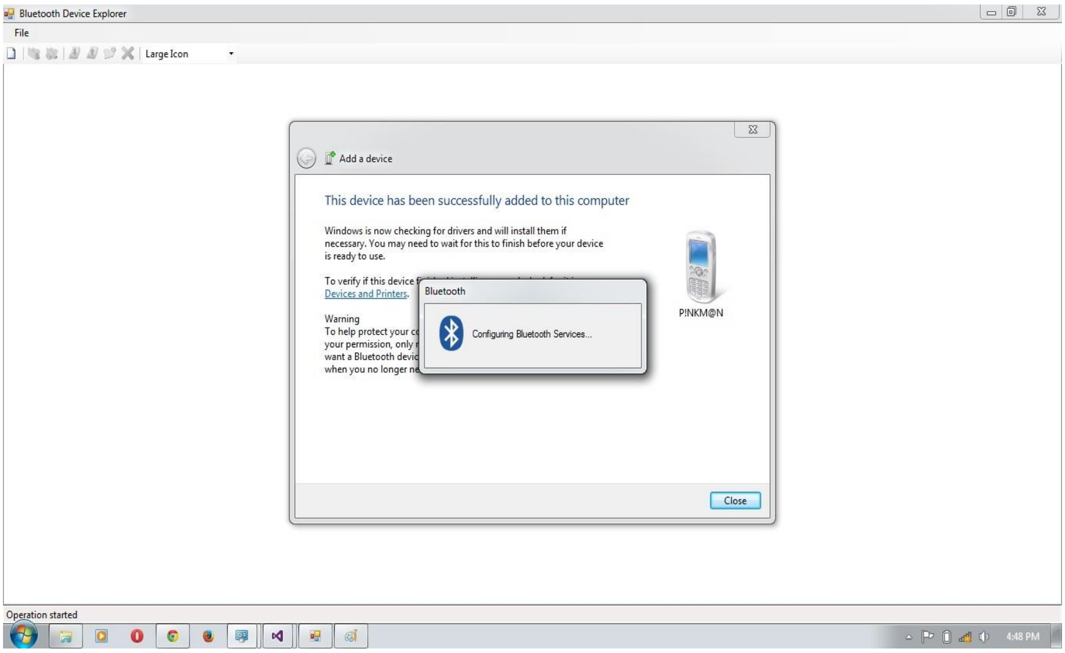
☑ Always Allow

Cancel OK

PC

SEARCH FOR DEVICES

Figure 4.3: Determining their inequalities and unifying these two object stores



This device has been successfully added to this computer

Windows is now checking for drivers and will install them if
necessary. You may need to wait for this to finish before your device
is ready to use.

To verify if this device f
Devices and Printers.

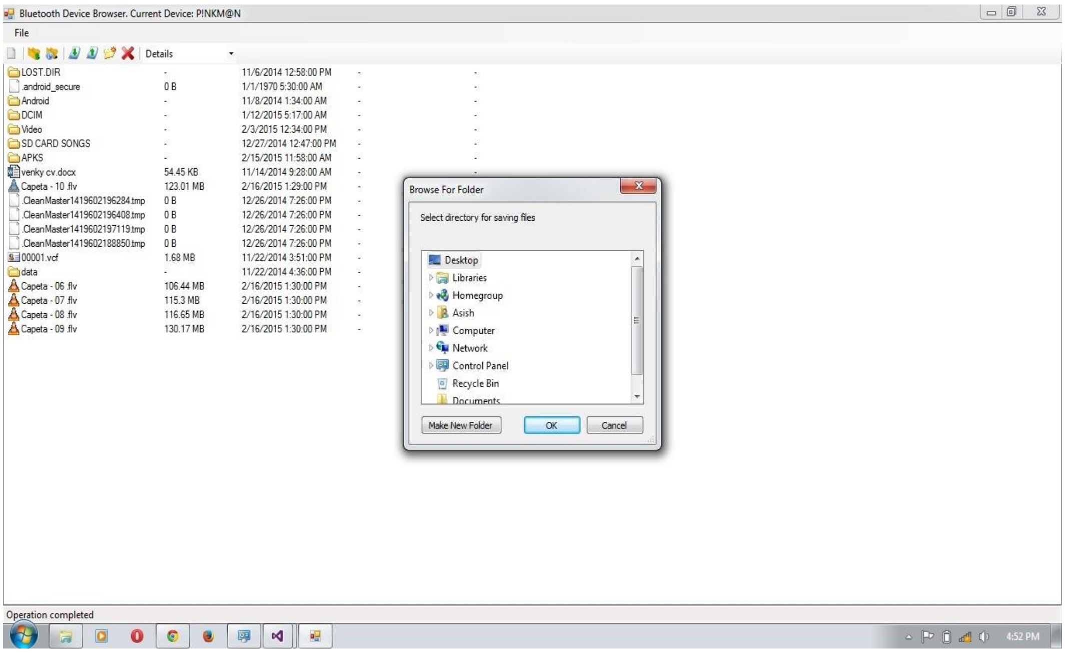
Warning
To help protect your c
your permission, only r
want a Bluetooth devic
when you no longer ne

Bluetooth

Configuring Bluetooth Services...

P!NKM@N

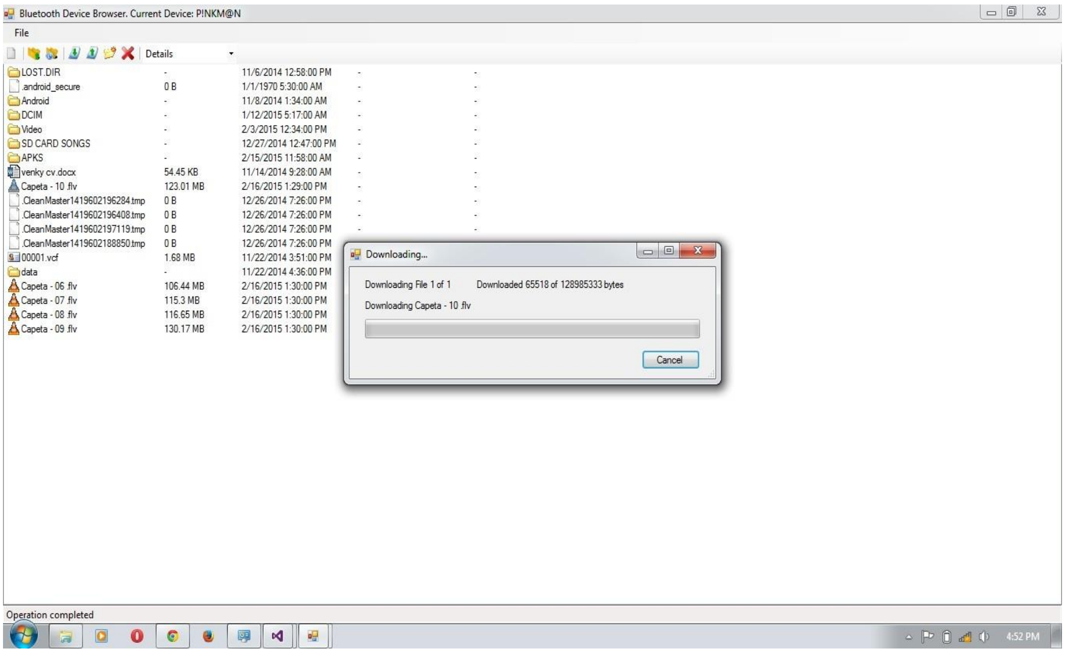
Figure 4.4: Synchronization



LOST.DIR	-	11/6/2014 12:58:00 PM	-	-
.android_secure	0 B	1/1/1970 5:30:00 AM	-	-
Android	-	11/8/2014 1:34:00 AM	-	-
DCIM	-	1/12/2015 5:17:00 AM	-	-
Video	-	2/3/2015 12:34:00 PM	-	-
SD CARD SONGS	-	12/27/2014 12:47:00 PM	-	-
APKS	-	2/15/2015 11:58:00 AM	-	-
venky cv.docx	54.45 KB	11/14/2014 9:28:00 AM	-	-
Capeta - 10 .flv	123.01 MB	2/16/2015 1:29:00 PM	-	
.CleanMaster1419602196284.tmp	0 B	12/26/2014 7:26:00 PM	-	
.CleanMaster1419602196408.tmp	0 B	12/26/2014 7:26:00 PM	-	
.CleanMaster1419602197119.tmp	0 B	12/26/2014 7:26:00 PM	-	
.CleanMaster1419602188850.tmp	0 B	12/26/2014 7:26:00 PM	-	
00001.vcf	1.68 MB	11/22/2014 3:51:00 PM	-	
data	-	11/22/2014 4:36:00 PM	-	
Capeta - 06 .flv	106.44 MB	2/16/2015 1:30:00 PM	-	
Capeta - 07 .flv	115.3 MB	2/16/2015 1:30:00 PM	-	
Capeta - 08 .flv	116.65 MB	2/16/2015 1:30:00 PM	-	
Capeta - 09 .flv	130.17 MB	2/16/2015 1:30:00 PM	-	

Select directory for saving files

Figure 4.5: File Transfer



Bluetooth Device Browser. Current Device: P!NKM@N

LOST.DIR	-	11/6/2014 12:58:00 PM	-	-
.android_secure	0 B	1/1/1970 5:30:00 AM	-	-
Android	-	11/8/2014 1:34:00 AM	-	-
DCIM	-	1/12/2015 5:17:00 AM	-	-
Video	-	2/3/2015 12:34:00 PM	-	-
SD CARD SONGS	-	12/27/2014 12:47:00 PM	-	-
APKS	-	2/15/2015 11:58:00 AM	-	-
venky cv.docx	54.45 KB	11/14/2014 9:28:00 AM	-	-
Capeta - 10 .flv	123.01 MB	2/16/2015 1:29:00 PM	-	-
.CleanMaster1419602196284.tmp	0 B	12/26/2014 7:26:00 PM	-	-
.CleanMaster1419602196408.tmp	0 B	12/26/2014 7:26:00 PM	-	-
.CleanMaster1419602197119.tmp	0 B	12/26/2014 7:26:00 PM	-	-
.CleanMaster1419602188850.tmp	0 B	12/26/2014 7:26:00 PM		
00001.vcf	1.68 MB	11/22/2014 3:51:00 PM		
data	-	11/22/2014 4:36:00 PM		
Capeta - 06 .flv	106.44 MB	2/16/2015 1:30:00 PM		
Capeta - 07 .flv	115.3 MB	2/16/2015 1:30:00 PM		
Capeta - 08 .flv	116.65 MB	2/16/2015 1:30:00 PM		
Capeta - 09 .flv	130.17 MB	2/16/2015 1:30:00 PM		

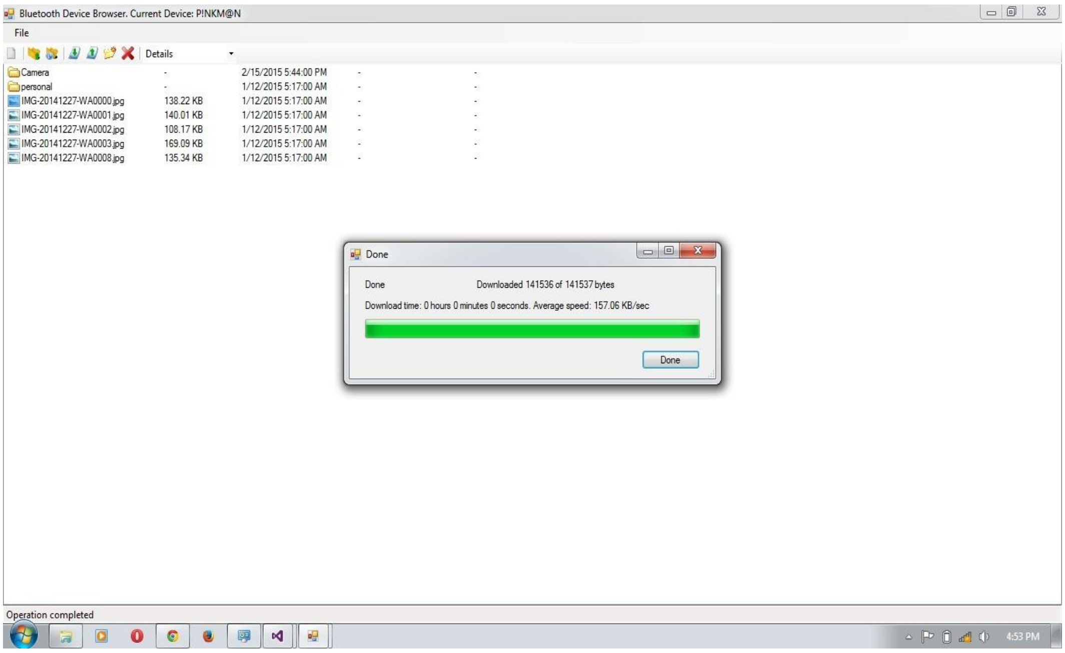
Downloading...

Downloading File 1 of 1 Downloaded 65518 of 128985333 bytes

Downloading Capeta - 10 .flv

Operation completed

Figure 4.6: Sending generic files



Bluetooth Device Browser. Current Device: P!NKM@N

Camera	-	2/15/2015 5:44:00 PM	-	-
personal	-	1/12/2015 5:17:00 AM	-	-
IMG-20141227-WA0000.jpg	138.22 KB	1/12/2015 5:17:00 AM	-	-
IMG-20141227-WA0001.jpg	140.01 KB	1/12/2015 5:17:00 AM	-	-
IMG-20141227-WA0002.jpg	108.17 KB	1/12/2015 5:17:00 AM	-	-
IMG-20141227-WA0003.jpg	169.09 KB	1/12/2015 5:17:00 AM	-	-
IMG-20141227-WA0008.jpg	135.34 KB	1/12/2015 5:17:00 AM	-	-

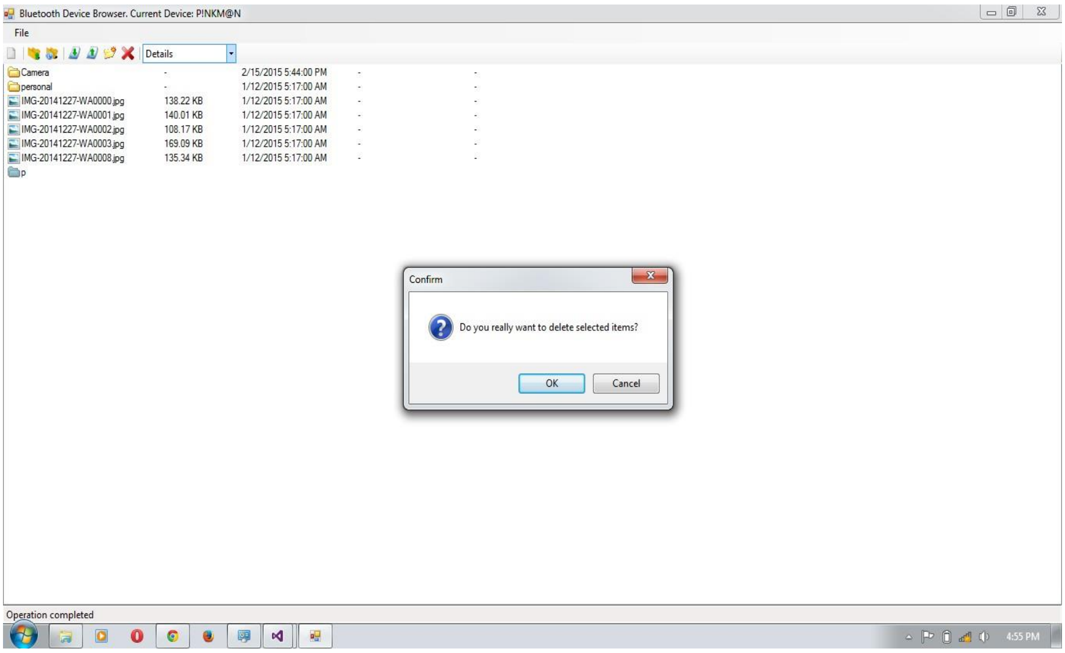
Done

Done Downloaded 141536 of 141537 bytes

Download time: 0 hours 0 minutes 0 seconds. Average speed: 157.06 KB/sec

Operation completed

Figure 4.7: Retrieving generic files from Bluetooth Devices



Bluetooth Device Browser. Current Device: P!NKM@N

Camera	-	2/15/2015 5:44:00 PM	-	-
personal	-	1/12/2015 5:17:00 AM	-	-
IMG-20141227-WA0000.jpg	138.22 KB	1/12/2015 5:17:00 AM	-	-
IMG-20141227-WA0001.jpg	140.01 KB	1/12/2015 5:17:00 AM	-	-
IMG-20141227-WA0002.jpg	108.17 KB	1/12/2015 5:17:00 AM	-	-
IMG-20141227-WA0003.jpg	169.09 KB	1/12/2015 5:17:00 AM	-	-
IMG-20141227-WA0008.jpg	135.34 KB	1/12/2015 5:17:00 AM	-	-
p				

Confirm

Do you really want to delete selected items?

Operation completed

Figure 4.8: Bearing objects and optionally pulling the default objects

Chapter 5

Future Scope and Conclusion

To better understand the total impact of Bluetooth on future pervasive computing applications (e.g., performance, reaction to noise, and interferences in a piconet or scatternets),

To create Bluetooth Transmission safer

5.1 Security Analysis

Due to inclusion of Authentication mechanism, the improved Diffie-Hellman[6] Key exchange protocol can stand up to replay attack, impersonation attack and man-in-the-middle attack. The simulation outputs in the LAN prove that authentication using hash function has the fewer computing quantity and the faster computing speed than the other public key and symmetric key encryption algorithm. It has a high practical worth in creating a secure communication channel of symmetric key.

5.2 Performance Evaluation

As long as the Diffie-Hellman[6] problem is difficult to decode, no eavesdropper can make out the secret key from the publicly known intelligence.

Bibliography

[1].Kapoor, R. ; Ling-Jyh Chen ; Lee, Y.-Z. ; Gerla, M. ” Bluetooth: carrying voice over ACL links” Mobile and Wireless Communications Network, 2002. 4th International Workshop on DOI: 10.1109/MWCN.2002.1045792 Publication Year: 2002

[2].Yang Hua ; Yuexian Zou ;“Analysis of the packet transferring in L2CAP layer of Bluetooth v2.x+EDR” Information and Automation, 2008. ICIA 2008. International Conference on DOI:10.1109/ICINFA.2008.4608099 Publication Year: 2008,

[3].Choonhwa Lee ; Helal, A;” Ns-based Bluetooth LAP simulator” Local Computer Networks, 2001.Proceedings. LCN 2001. 26th Annual IEEE Conference on DOI: 10.1109/LCN.2001.990832 Publication Year: 2001

[4].Pek, E. ; Bogunovic, Nikola ;” Formal verification of logical link control and adaptation protocol” Electrotechnical Conference, 2004. MELECON 2004. Proceedings of the 12thIEEE Mediterranean Volume:2 DOI: 10.1109/MELCON.2004.1346997 Publication Year: 2004 ,

[5]. Bluetooth, S. I. G. "Specification of the Bluetooth System, version 1.1."*http://www. bluetooth. com* (2001).

[6]. Research on Diffie-Hellman Key Exchange Protocol, Nan Li, Information Engineering Teaching and research section, The People’s Armed Police Force Academy of China, Langfang Hebei 065000, China

[7]. Papakonstantinou, Yannis, Hector Garcia-Molina, and Jennifer Widom. "Object exchange across heterogeneous information sources." *Data Engineering, 1995. Proceedings of the Eleventh International Conference on*. IEEE, 1995.