KINGSTON UNIVERSITY

Bluetooth

Digital Communications CIM242

Amarpreet Singh Saini
K1051678
12/10/2010

Bluetooth is a wireless technology that was conceived in the year 1998. Since then it has amassed an astoundingly huge user base most of which is due to the mobile telephony market. This calls for new methods to be developed which can make use of this huge penetration that Bluetooth has today. In this paper we discuss the Bluetooth specification and its implementation along with some issues plaguing it.

1. INTRODUCTION

Bluetooth is a wireless technology protocol conceived by the telecommunication company Ericsson in the year 1994. It was originally developed as a solution to eliminate the need for cables for short distance communications, enabling devices to form a personal area network which also support a high degree of security. Multiple devices can form a personal area network or PAN which can eliminates several issues associated with traditional methods and protocols. Bluetooth is maintained by a body SIG (Bluetooth Special Interest Group), which is a non-profit trade organisation formed in 1998. SIG oversees the activities related Bluetooth standards such as development and licensing of the trademarks and technologies to the manufacturers.

The name of the protocol Bluetooth comes from King Harald I of Denmark, who managed to unify the divided and fragment Danish tribes into a single kingdom.

Bluetooth Logo. [1]

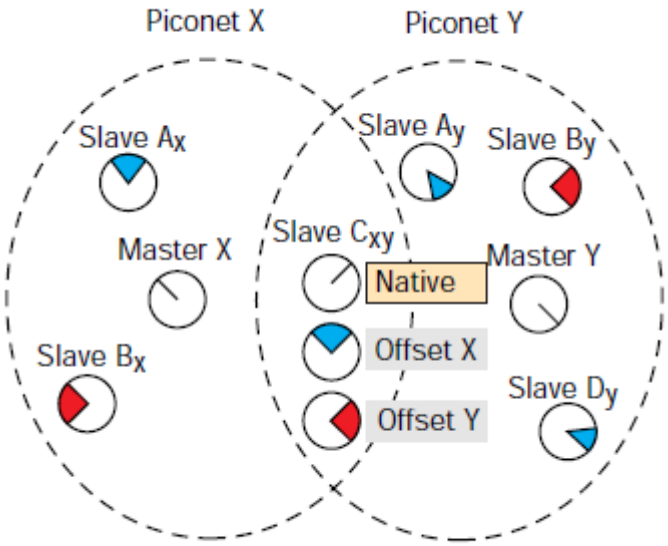
2. IMPLEMENTATION

Bluetooth is based on the concept of Frequency-Hopping Spread Spectrum (FHSS). Data is transmitted in chunks onto 79 bands each of 1 MHz in the range of 2402-2480 MHz. It can be seen that this range falls under the 2.4 GHz short range band, which is globally unlicensed for Industrial, Scientific and Medical purposes. A variant of FHSS called AFH is used in Bluetooth implementation due to its resistance to radio interference which can occur frequently in the unlicensed band. Additional mechanisms and strategies are combined with AFH, in order to obtain a noise free communication.

Initially the GFSK or the Gaussian frequency-shift keying modulation was the only technique used by the Bluetooth standard but later on techniques like π/4-DQPSK and 8DPSK were also implemented when the 2.0 and 3.0 standards were made available. A device is said to be in BR or Basic Rate mode when GFSK mode is used. The maximal transfer rate that can be attained with this mode is 1 Mbit/s. A device is said to be in EDR or Enhanced Data Rate mode when π/4-DQPSK and 8DPSK are used. The maximal transfer rate attainable using these is 2 and 3 Mbit/s respectively. Modern devices are capable of using all the above mentioned modes so as to attain compatibility with legacy devices. Such devices have a radio BR/EDR which is a combination of both the Basic and Enhanced modes.

In essence the Bluetooth protocol is a master-slave, packet based protocol. A master can communicate with 7 other devices termed as slave in a network, all of which share the master's clock. This network of master and slaves is termed as a piconet. The master can choose which slave will it transfer data to, and does this in a round robin algorithm fashion. All data transfer takes place according to the clock of the master in a piconet which ticks at a time interval of 312.5 µs. Packets are transferred in this time slot depending on the transfer scheme adopted. In a simplified example, the master transmits in even slots and receives in odd slots whereas the slaves receive in even slots and transfer in odd slots.

Multiple piconets can be combined with several devices acting as bridges to form a scatternet. The bridges are devices which act as masters in one piconet and slaves in the others.



[2] Participation of slaves in two piconets

3. SPECIFICATION

The following table describes the classes of devices that implement Bluetooth.

Class	Maximum Permitted Power		Range (approximate)
	mW	dBm	
Class 1	100	20	~100 meters
Class 2	2.5	4	~10 meters
Class 3	1	0	~1 meters

[1]

One thing to note is that the devices needn't have a line of sight due to the technology being a radio broadcast one.

The following table shows the versions of the Bluetooth specification along with their maximal transfer caps.

Version	Data Rate
Version 1.2	1 Mbit/s
Version 2.0 + EDR	3 Mbit/s
Version 3.0 + HS	24 Mbit/s

[1]

Although there are versions such as 1.0 and 2.1 but the above mentioned ones represent a giant leap with regards to the prior version.

3.1 Features of Bluetooth v1.2

AFH or Adaptive frequency-hopping spread spectrum was implemented in this version which helps in eliminating interference occurring due to other devices in the unlicensed 2.4 band. Also eSCO's or Extended Synchronous Connections were introduced allowing for retransmission of corrupted packets along with flow control for L2CAP.

3.2 Features of Bluetooth v2.0

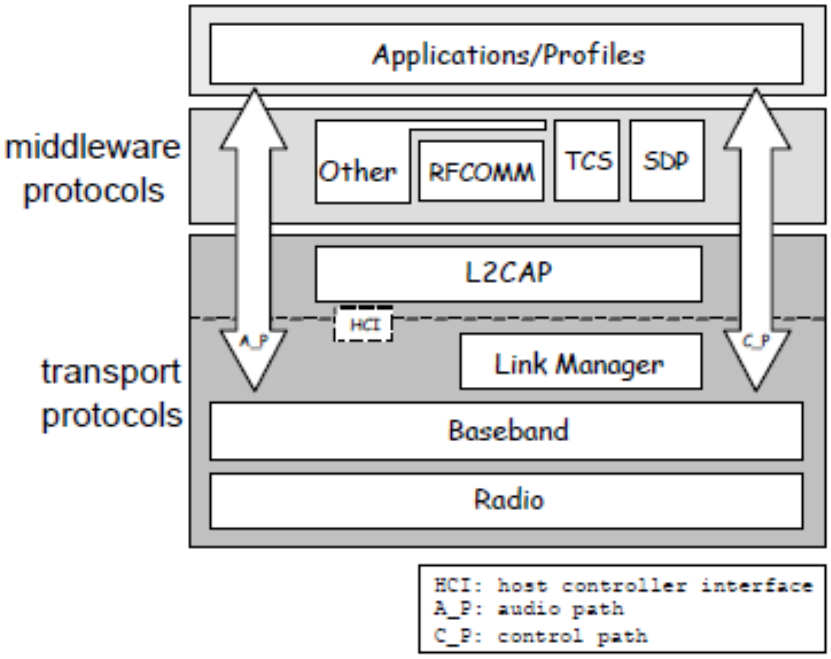
The main feature in v2.0 is the addition of EDR or Enhanced Data rate which allows for a theoretical transfer rate of 3.0 Mbit/s although 2.1 Mbit/s is the practically attainable rate. Also EDR is an addition to the already existing Bluetooth protocol, which means that the existing modulation techniques from the earlier versions are still available resulting in backwards compatibility.

3.3 Features of Bluetooth v3.0

Version 3.0 adopted by SIG on April 21, 2009 allows for a theoretical data transfer cap of 24 Mbit/s. This although is not done over the Bluetooth link which is only used for the negotiation and other communication. The transfer takes place over an 802.11 link which is implemented as AMP (Alternate MAC/PHY). This is called the HS or High Speed but is not required if one of the devices does not support it.

An implementation of the Bluetooth protocol in the operating system is termed a Bluetooth Stack. There are 2 categories of Bluetooth stacks:

- General purpose: Written with user interface and feature variety in mind. These are usually for desktop computers where resources such as power and computational power are abundant. Examples are Widcomm, BlueSoleil.
- Embedded system: Written for devices where resources such as power are limited. I.e. Bluetooth headsets. Examples are Bluemagic, Bluetopia.



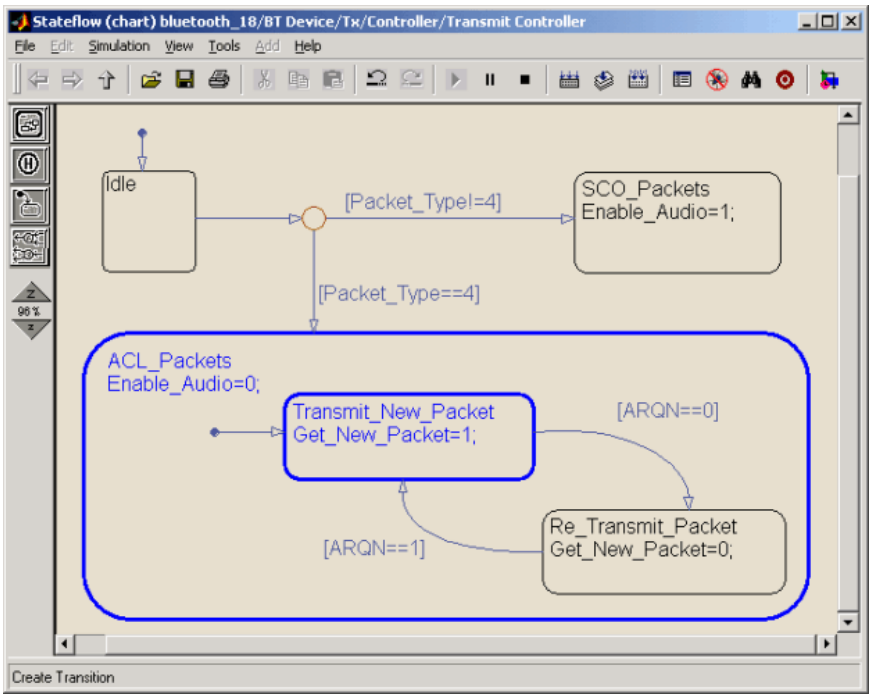
[3]

The following protocols have been adopted by SIG in the Bluetooth implementation.

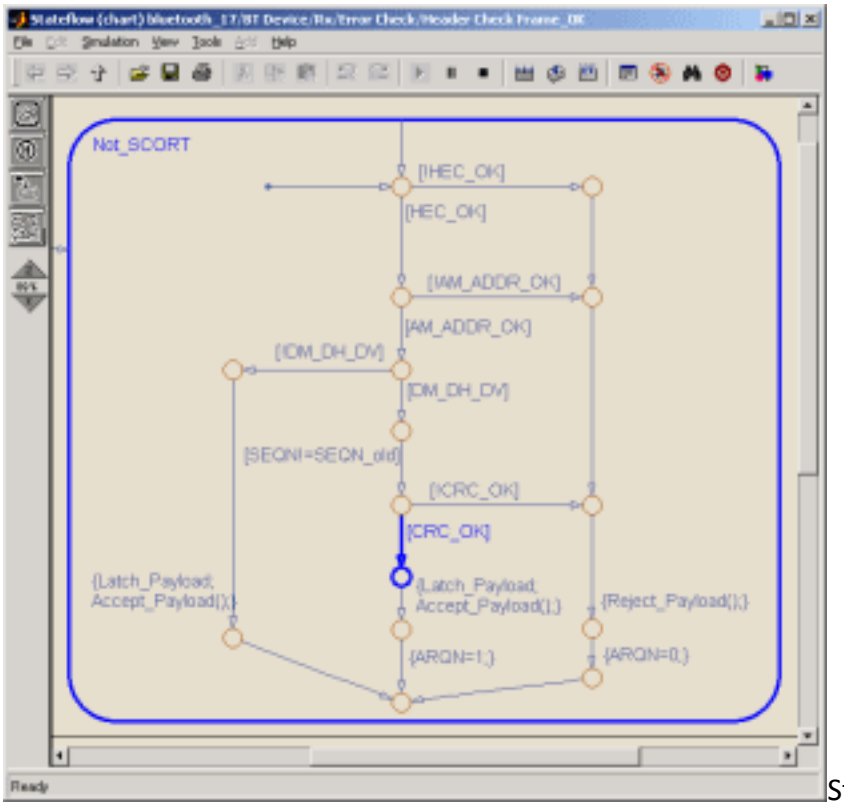
Protocols	
Audio/Video Control Transport Protocol (AVCTP)	describes the transport mechanisms to exchange messages for controlling A/V devices. More ...
Audio/Video Distribution Transport Protocol (AVDTP)	defines A/V stream negotiation, establishment and transmission procedures. More ...
***Bluetooth* Network Encapsulation Protocol (BNEP)**	is used to transport common networking protocols over the *Bluetooth* media such as IPv4 and IPv6. More ...
Object Exchange (OBEX)	a transfer protocol that defines data objects and a communication protocol two devices can use to exchange those objects. More ...
Telephony Control Protocol (TCP)	defines the call control signaling for the establishment of speech and data calls between *Bluetooth* devices. More ...
RFCOMM with TS 07.10	emulates the serial cable line settings and status of an RS-232 serial port and is used for providing serial data transfer. More ...

[4]

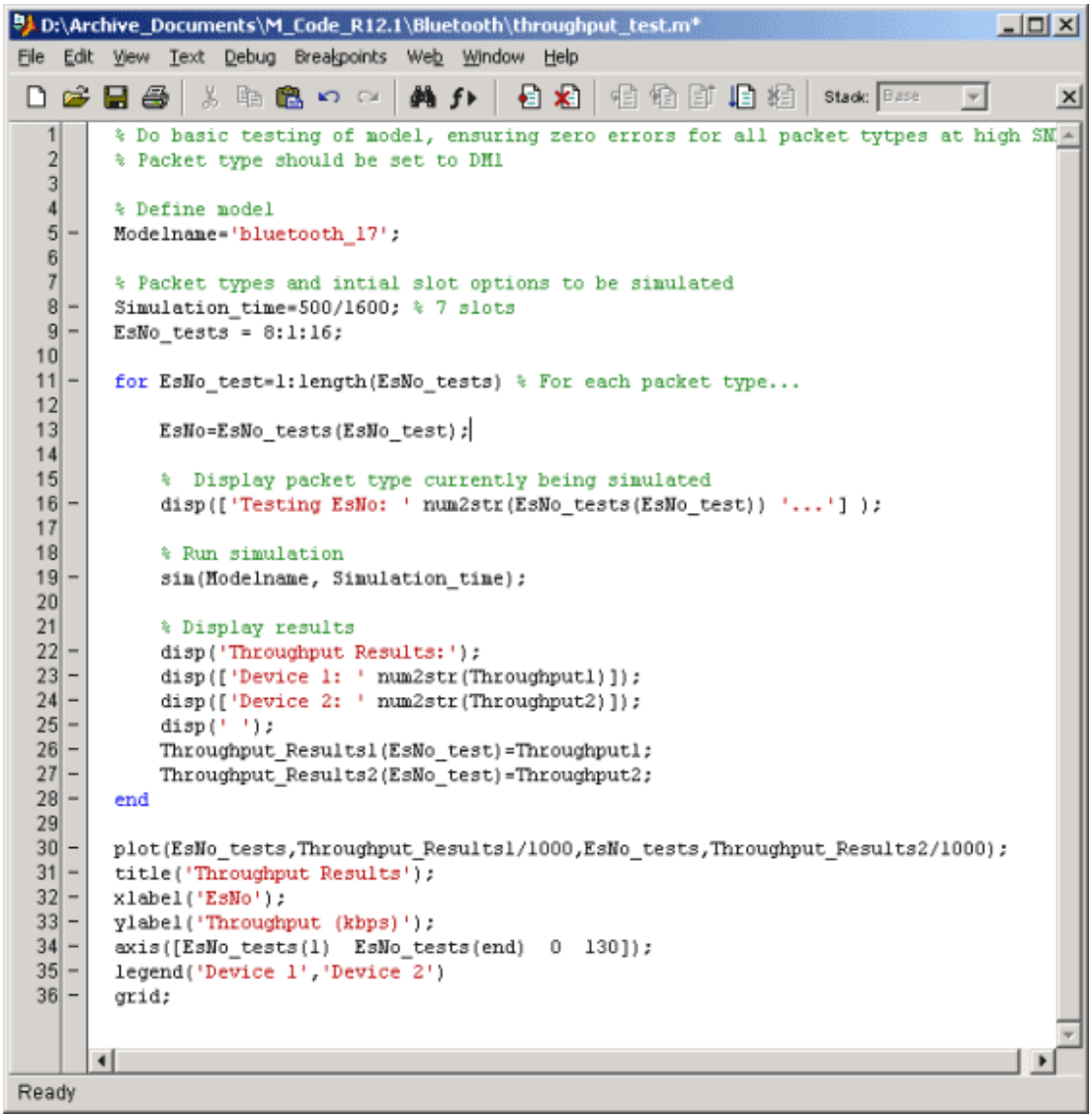
Using the article published in MATLAB digest in Sept 2002, we demonstrate the transmission rate between 2 devices using the v1.0 specification of Bluetooth. [9]



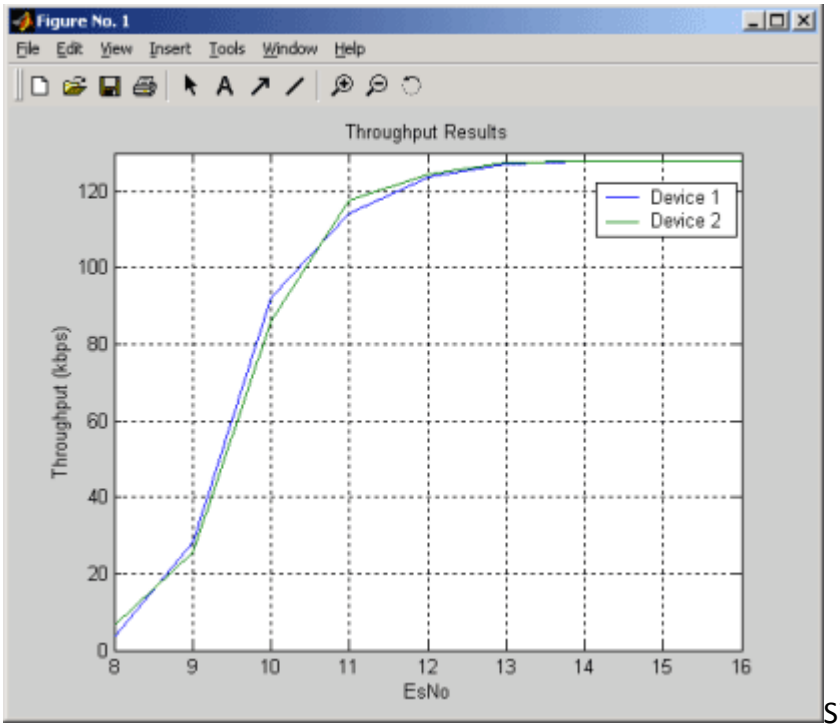
Stateflow diagram for data acknowledgement in transmitter.



Stateflow diagram for data acknowledgement in receiver.



Throughoutput_test.m



Simulation result

As it can be seen, data rate is 1 Mbit/s in case of no noise or interference. The model was recreated as given in the article and tested at a range of noise levels EsNo to calculate throughput.

4. USES

For a device to be able to use Bluetooth, it must be able to decipher what is called a Bluetooth profile. A Bluetooth profile is an interface specification which allows for communication between devices. These profiles may or may not be dependent on the version of the Bluetooth implementation running on the devices wishing to communicate. The profiles provide a standard which can then be followed by the device manufacturers so that consistency is maintained amongst all the devices supporting that particular profile.

A typical Bluetooth profile contains the following –

- Dependencies on other profiles
- User interface formats.
- Parts of the Bluetooth protocol stack required by the profile.

The Bluetooth profiles are implemented on the top of the Bluetooth specification and any other required protocols. The following profiles have been accepted by SIG.

Profiles	
Advanced Audio Distribution Profile (A2DP)	describes how stereo quality audio can be streamed from a media source to a sink. More ...
Audio/Video Remote Control Profile (AVRCP)	is designed to provide a standard interface to control TVs, stereo audio equipment, or other A/V devices. This profile allows a single remote control (or other device) to control all A/V equipment to which a user has access. More ...
Basic Imaging Profile (BIP)	defines how an imaging device can be remotely controlled, how an imaging device may print, and how an imaging device can transfer images to a storage device. More ...
Basic Printing Profile (BPP)	allows devices to send text, e-mails, v-cards, images or other information to printers based on print jobs. More ...
Common ISDN Access Profile (CIP)	defines how ISDN signaling can be transferred via a *Bluetooth* wireless connection. More ...
Cordless Telephony Profile (CTP)	defines how a cordless phone can be implemented over a *Bluetooth* wireless link. More ...
Dial-Up Network Profile (DUN)	provides a standard to access the Internet and other dial-up services via *Bluetooth* technology. More ...
Fax Profile (FAX)	defines how a FAX gateway device can be used by a terminal device. More ...
File Transfer Profile (FTP)	defines how folders and files on a server device can be browsed by a client device. More ...
General Audio/Video Distribution Profile (GAVDP)	provides the basis for A2DP and VDP, which are the basis of the systems designed for distributing video and audio streams using *Bluetooth* technology. More ...
Generic Object Profile (GOEP)	is used to transfer an object from one device to another. More ...
Hands-Free Profile (HFP)	HFP describes how a gateway device can be used to place and receive calls for a hand-free device. More ...
Hard Copy Cable Replacement Profile (HCRP)	defines how driver-based printing is accomplished over a *Bluetooth* wireless link. More ...
Headset Profile (HSP)	describes how a *Bluetooth* enabled headset should communicate with a *Bluetooth* enabled device. More ...
Human Interface Device Profule (HID)	defines the protocols, procedures and features to be used by *Bluetooth* keyboards, mice, pointing and gaming devices and remote monitoring devices. More ...
Intercom Profile (ICP)	defines how two *Bluetooth* enabled mobile phones in the same network can communicate directly with each other without using the public telephone or cellular network. More ...
Object Push Profile (OPP)	defines the roles of push server and push client. More ...
Personal Area Networking Profile (PAN)	describes how two or more *Bluetooth* enabled devices can form an ad-hoc network and how the same mechanism can be used to access a remote network through a network access point. More ...
Service Discovery Application Profile (SDAP)	describes how an application should use SDP to discover services on a remote device. More ...
Service Port Profile (SPP)	defines how to set-up virtual serial ports and connect two *Bluetooth* enabled devices. More ...
Synchronization Profile (SYNC)	used in conjunction with GOEP to enable synchronization of calendar and address information (personal information manager (PIM) items) between *Bluetooth* enabled devices. More ...
Video Distribution Profile (VDP)	defines how a *Bluetooth* enabled device streams video over *Bluetooth* wireless technology. More ...

[4]

Various uses that Bluetooth is used for –

- Transfer of streaming of audio. E.g. a Bluetooth headset and a mobile phone.
- Use in remote control devices. Sony PS3 uses Bluetooth in their controllers.
- Communication between a PC and various input and output devices such as wireless keyboards, mice, printers etc.

- An application where wireless is a desirable property rather than a high bandwidth channel. Such as low-distance transfer of media between mobile devices.
- Internet access via dialup networking for compatible devices.

A Bluetooth device can advertise all the services that it is compatible with on discovery. When a Bluetooth devices is requested, it provides a few details to the requesting device –

- Name of the device
- Class of the device
- List of services
- Other technical information like manufacturer, version of the Bluetooth implementation running.

However in order to use the services of the device, a procedure known as pairing must be established, which involves acceptance of the request by the owner of the that device. Every device has a unique 48 bit address associated with it. However, this address is hidden and instead a custom set name is advertised when a device is in discoverable mode. The 48 bit address is instead when a device operates in hidden mode, and only devices knowing this address can establish connections to it. This offers a degree of security to the involved parties when they are exchanging information in an insecure environment. However this is more of a hindrance if a determined attack is made against a Bluetooth device, using a brute force technique.

5. PAIRING

Pairing is the mechanism that occurs before devices can start using services over the Bluetooth link. Pairing is a necessary step that must occur, as only authorized devices are to be given access to the services of a device. Also once a device is paired, further connections can be initiated amongst the devices without any user intervention, thus offering convenience.

First of all, a device is put into discoverable mode. This enables it to be seen by other devices, which can trigger connections to it. Pairing then automatically occurs when a device connects to another for the first time. The devices can then remember this pairing relationship by storing the unique 48 bit address for each other along with other pairing data. This way connection can be made to the device in future even if it is in hidden mode. The pairing relationship can be removed by any of the two devices which will result in the pairing being broken. Even if one of the devices still has the pairing data stored, it will need to re-establish pairing the next time it wishes to communicate with the said device.

The pairing data that each device stores for every pairing relationship is a secret shared key. Storing of this key essentially means that the devices are paired or bonded. The authenticity of the device can be checked using this secret key, which must be provided by the device requesting the connection in future. This is thus a challenge-response type scenario, where the device being requested for the connection challenges the other device for its key. Also this key can be used to encrypt the data that is transferred between the two devices so that sniffing of data by a third party in the near vicinity, leads to no compromise of critical information.

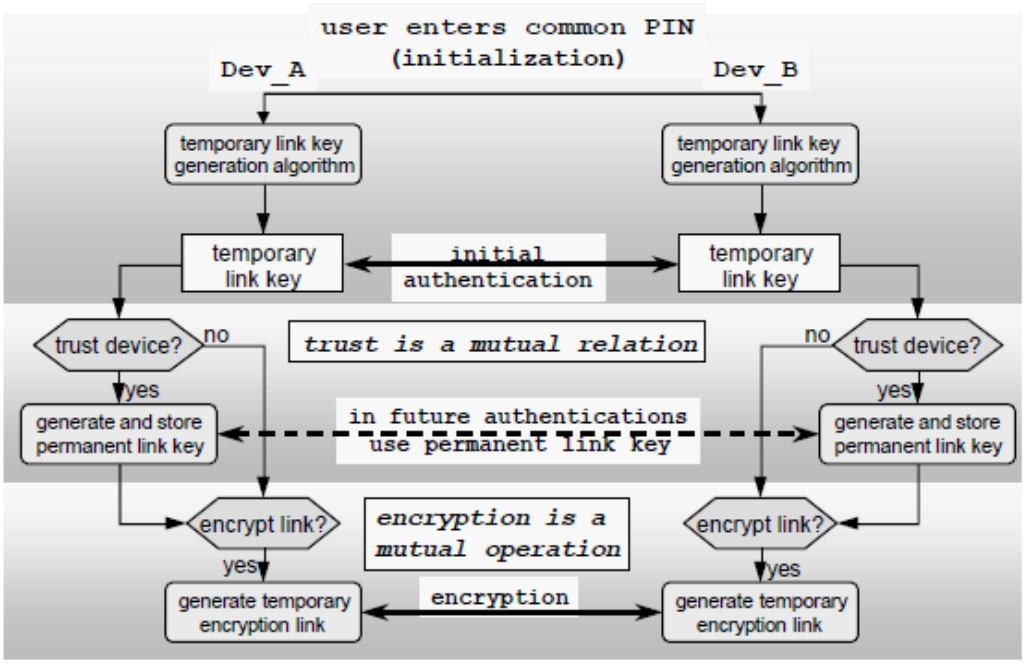
Two type of pairing mechanisms are generally used –

- Legacy: This method has been implemented before the 2.1v specification came out. Entering a PIN code is the only way to successfully establish a bond.
- Secure Simple Pairing: This was made available with the advent of Bluetooth specification 2.1v. SSP uses a variant of public-key cryptography.

6. CONCERNS ASSOCIATED WITH BLUETOOTH

There are a various concerns associated with Bluetooth technology, notably security and health related. We discuss a few of these.

6.1 Security



[3]

Although various security mechanisms are implemented in the Bluetooth specification there are various security related concerns plaguing it. Exploits have been discovered time and again in various aspects of the implementation. Exploits have been found out and used in the pairing mechanism, the encryption techniques, and stack level and so on. The introduction of v2.1 of the Bluetooth specification addressed several loopholes in the implementation such as mandatory encryption, pairing mechanisms such as SSP etc. Sniffing of data being exchanged is one of the more challenging issues surrounding Bluetooth. This is because mobile devices have limited processing power due to power concerns and using a more powerful device one can essentially brute force the encrypted data to obtain the unencrypted data.

Various tools have been made freely available over the internet which exploits various loopholes in the Bluetooth specification. Some of the more popular ones are –

- Bluesniff: A tool which detects hidden devices
- Bloover: Used to send messages to unwary device owners.

Martin Hefert from trifinite.group demonstrated an attack vulnerability called Bluebug at CeBIT fairgrounds, which exposed the risk which the Bluetooth devices were facing. [5] In June 2004, a proof of concept virus named Cabir was demonstrated, which further exposed the flaws in the Bluetooth specification and implementation. [6] Although it was a proof-of-concept, it proved that the vulnerability could be exploited by a malicious coder which could cause significant

damage due to the mobile nature of the Bluetooth devices. Cabir however was only written for devices running Symbian OS. Yaniv Shaked and Avishai Wool demonstrated an attack to successfully obtain the PIN that was used during the pairing process by using a custom hardware setup to initiate a passive attack. [7] Markus Jakobsson and Susanne Wetzel of Bell Labs demonstrate in their paper a few problems plaguing the Bluetooth specification where they demonstrate attacks to steal the PIN's, locating of a device's geographic location and a few attacks on the cipher used to encrypt the data transfer taking place. [8]

6.2 Health

Although Bluetooth devices emit radiation they have specifically not been linked to any health hazards. Bluetooth uses the microwave frequency range from 2.4 GHz to 2.4835 GHz. The emitted power varies from 1 to 100 mW.

7. CONCLUSION

Bluetooth is primarily designed for short range communication amongst devices where power efficiency is a major concern. Mobile devices are the primary example where Bluetooth technology is put to use. Although recently Wi-Fi is being implemented in mobile devices but continuous use of Wi-Fi drains battery at an extremely rapid pace. Bluetooth can thus be used for simple communication and has a vast variety of uses in such areas. The penetration of cell phones in today's times means this can also be used for many potential future technologies such as near-field technology. There are endless uses that Bluetooth can be put to use only limited by human ingenuity. Also Bluetooth is less susceptible to interference than 802.11, which makes it more preferable for such short sporadic communication although it can also be used as an always on link if desired.

8. REFERENCES

1. en.wikipedia.org/wiki/Bluetooth
2. Jaap Haartsen. BLUETOOTH—The universal radio interface for ad hoc, wireless connectivity. Ericsson review 1998
3. Chatschik Bisdikian. IBM Research Report – An overview of Bluetooth Wireless Technology. Ieee Commun Mag, 2001
4. http://www.bluetooth.com/English/Technology/Works/Pages/Profiles_Overview.aspx
5. http://trifinite.org/trifinite_stuff_bluebug.html
6. http://www.theregister.co.uk/2004/06/15/symbian_virus/
7. Yaniv Shaked, Avishai Wool (2005-05-02). *Cracking the Bluetooth PIN*. In Proceedings of the 3rd international conference on Mobile systems, applications, and services *(MobiSys '05).*
8. Markus Jakobsson and Susanne Wetzel. *Security Weaknesses in Bluetooth* Lecture Notes in Computer Science, 2001, Volume 2020/2001, 176-191
9. Stuart McGarrity *Bluetooth Control Logic Design with Stateflow* MATLAB digest, Sept 2002