Survey of Bluetooth and Applications

Arwa Kurawar, Ayushi Koul, Prof. Viki Tukaram Patil

***Abstract*[5]—Bluetooth is an open specification for short-range wireless communication and networking, mainly intended to be a cable replacement between portable and/or fixed electronic devices. The main aim of introducing Bluetooth is to connect two or more devices without any physical connection. This helps to reduce time and human efforts for transferring data. The specification also defines techniques for interconnecting large number of nodes in scatternets, thus enabling the establishment of a Mobile Ad hoc network (MANET). While several solutions and commercial products have been introduced for one-hop Bluetooth communication, the problem of scatternet formation has not yet been dealt with. This problem concerns the assignment of the roles of master and slave to each node so that the resulting MANET is connected. The range of Bluetooth is upto 60metres.So we are basically focusing on the idea to improve in some essential areas.In this paper we have included some important features like scatternet and piconet,Bluetooth Protocol Stack.We have also dealt with different versions of Bluetooth according to their date of release.Also we have discussed the fundamentals of communication and connection and pairing and bonding mechanisms.Our future scope area mainly focuses on power and energy saving in the future Bluetooth devices or any such equipments.In today's era we are having gadgets using different operating systems.The pairing between the devices is not upto the mark so also aim at presenting the idea of gathering opportunities to improve upon the compatibility feature.**

Keywords- *Bluetooth, MANET, .Protocol, Frequency, hopping, dongle, piconet, scatternet,* cryptography,spectrum topology,encryption.

INTRODUCTION

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz from fixed and mobile devices, and building (PANs). The Bluetooth wireless specification got its name from 10th-century Danish king who used diplomacy to negotiate a truce between two opposite parties. Invented by telecom vendor Ericsson in 1994 it was originally conceived as a wireless alternative to RS-232 data cables. **.**

Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 20,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. Bluetooth was standardized as **IEEE 802.15.1**, but the standard is no longer maintained. The SIG oversees the development of the specification, manages the qualification program, and protects the trademarks.To be marketed as a Bluetooth device, it must be qualified to standards defined by the SIG.A network of patents is required to implement the technology, which is licensed only for that qualifying device. Bluetooth is a connective convenience. It is a high-speed, low-power microwave wireless link technology, designed to connect phones, laptops, PDAs and other portable equipment together with little or no work by the user. Unlike infra-red, Bluetooth does not require line-of-sight positioning of connected units.

Manuscript received August 2014.

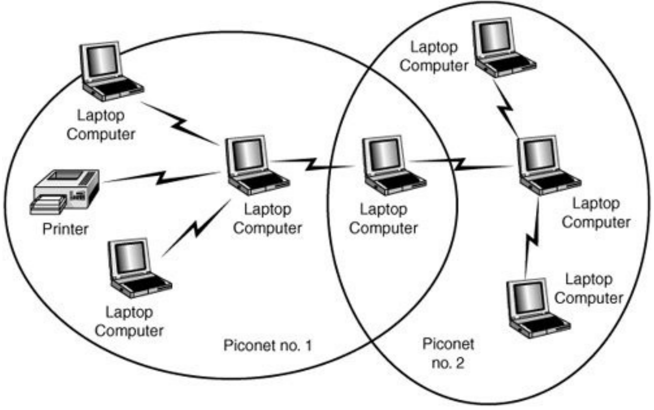
Arwa Kurawar, *Computer Science and Engineering, Mumbai University at MGMCET, Panvel, India,*
Ayushi Koul, *Computer Science and Engineering, Mumbai University at MGMCET,. Panvel, India.*
Prof. Viki Tukaram Patil *Computer Science and Engineering, Mumbai University at MGMCET, Panvel, 8691892111*

LOGO

The Bluetooth logo is bind rune merging the Younger Furthrak (□) and ᛒ Bjarkan (□), Harald's initials.
Meanwhile the Bluetooth logo was almost completely copied from the original design of the brand in 1970 Beauknit Textiles, a division Beauknit Corporation.
Implementation. It looks like:[1]

ARCHITECTURE

Bluetooth is a packet based control with a master slave structure. One master may communicate with up to seven slaves in a piconet all devices share the master's clock. Packet exchange is based on the basic clock, defined by the master, which ticks at 312.5 µs intervals. Two clock ticks make up a slot of 625 µs; two slots make up a slot pair of 1250 µs. In the simple case of single-slot packets the master transmits in even slots and receives in odd slots; the slave, conversely, receives in even slots and transmits in odd slots. Packets may be 1, 3 or 5 slots long, but in all cases the master transmit will begin in even slots and the slave transmit in odd slots.



Communication and connection

A master Bluetooth device can communicate with a maximum of seven devices in a piconet (an ad-hoc computer network using Bluetooth technology), though not all devices reach this maximum. The devices can switch roles, by agreement, and the slave can become the master (for example, a headset initiating a connection to a phone will necessarily begin as master, as initiator of the connection; but may subsequently prefer to be slave).

The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatternet, in which certain devices simultaneously play the master role in one piconet and the slave role in another.
At any given time, data can be transferred between the master and one other device (except for the little-used broadcast mode.]) The master chooses which slave device to address; typically, it switches rapidly from one device to another in a round robin fashion. Since it is the master that chooses which slave to address, whereas a slave is (in theory) supposed to listen in each receive slot, being a master is a lighter burden than being a slave. Being a master of seven slaves is possible; being a slave of more than one master is difficult.The specification is vague as to required behavior in scatternets.

Bluetooth profile[3]

To use Bluetooth wireless technology, a device has to be able to interpret certain Bluetooth profiles, which are definitions of possible applications and specify general behaviours that Bluetooth enabled devices use to communicate with other Bluetooth devices. These profiles include settings to parametrize and to control the communication from start. Adherence to profiles saves the time for transmitting the parameters anew before the bi-directional link becomes effective. There are a wide range of Bluetooth profiles that describe many different types of applications or use cases for devices.

APPLICATIONS

A. Wireless control of and communication between a mobile phone and a handfree headset. This was one of the earliest applications to become popular.

B. Wireless control of and communication between a mobile phone and a Bluetooth compatible car stereo system.

C. Wireless control of and communication with tablets and speakers such as iPad and Android devices.[2]

D. Wireless Bluetooth headset and Intercom diomatically, a headset is sometimes called "a Bluetooth".

E. Wireless networking between PCs in a confined space and where little bandwidth is required.

F. Wireless communication with PC input and output devices, the most common being the mouse, keyboard and Printer.

G. Transfer of files, contact details, calendar appointments, and reminders between devices with OBEX.

H. Replacement of previous wired RS-232 serial communications in test equipment, GPS receivers medical equipment, bar code scanners, and traffic control devices.

I. For controls where infrared was often used.

J. For low bandwidth applications where higher USB bandwidth is not required and cable-free connection desired.

K. Sending small advertisements from Bluetooth-enabled advertising hoardings to other, discoverable, Bluetooth devices.

L. Dial-up internet access on personal computers or PDAs using a data-capable mobile phone as a wireless modem.

M. Short range transmission of health sensor data from medical devices to mobile phone, SET TOP BOX or dedicated telehealth devices.

N. Real-time location systems (RTLS) are used to track and identify the location of objects in real-time using “Nodes” or “tags” attached to, or embedded in the objects tracked, and “Readers” that receive and process the wireless signals from these tags to determine their locations.

O. Personal security application on mobile phones for prevention of theft or loss of items. The protected item has a Bluetooth marker (*e.g.*, a tag) that is in constant communication with the phone. If the connection is broken (the marker is out of range of the phone) then an alarm is raised. This can also be used as a man overboard alarm. A product using this technology has been available since 2009.

P. Calgary, Canada’s Roads Traffic division uses data collected from travelers' Bluetooth devices to predict travel times and road congestion for motorists.

Bluetooth vs. Wi-Fi (IEEE 802.11)

Bluetooth and Wi-Fi have some similar applications: setting up networks, printing, or transferring files. Wi-Fi is intended as a replacement for high speed cabling for general LAN access in work areas. This category of applications is sometimes called WLAN. Bluetooth was intended for portable equipment and its applications. The category of applications is outlined as the WPAN. Bluetooth is a replacement for cabling in a variety of personally carried applications in any setting and also works for fixed location applications such as smart energy functionality in the home (thermostats, etc.).

Wi-Fi and Bluetooth are to some extent complementary in their applications and usage. Wi-Fi is usually access point-centered, with an asymmetrical client-server connection with all traffic routed through the access point, while Bluetooth is usually symmetrical, between two Bluetooth devices. Bluetooth serves well in simple applications where two devices need to connect with minimal configuration like a button press, as in headsets and remote controls, while Wi-Fi suits better in applications where some degree of client configuration is possible and high speeds are required, especially for network access through an access node. However, Bluetooth access points do exist and ad-hoc connections are possible with Wi-Fi though not as simply as with Bluetooth.

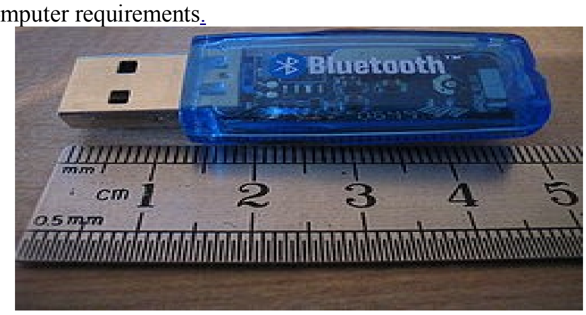
Device

A Bluetooth is a USB device with a 100 m range.

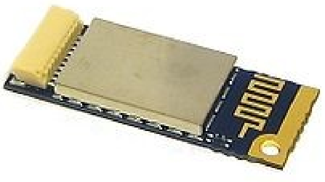
Bluetooth exists in many products, such as telephones, tablets, media players, robotics systems, handheld, laptops and console gaming equipment, and some high definition headsets, modems and watches. The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e., with a Bluetooth headset) or byte data with hand-held computers (transferring files).

Bluetooth protocols simplify the discovery and setup of services between devices. Bluetooth devices can advertise all of the services they provide.[1] This makes using services easier, because more of the security, network address and permission configuration can be automated than with many other network types.

Computer requirements.



A typical Bluetooth USB dongle.



An internal notebook Bluetooth card (14×36×4 mm)

Operating system implementation

Apple products have worked with Bluetooth since Mac OS Xv 10.2 which was released in 2002.

For Microsoft platforms, Windows XP Service Pack 2 and SP3 releases work natively with Bluetooth 1.1, 2.0 and 2.0+EDR. Previous versions required users to install their Bluetooth adapter's own drivers, which were not directly supported by Microsoft. Microsoft's own Bluetooth dongles (packaged with their Bluetooth computer devices) have no external drivers and thus require at least Windows XP Service Pack 2. Windows Vista RTM/SP1 with the Feature Pack for Wireless or Windows Vista SP2 work with Bluetooth 2.1+EDR Windows 7 works with Bluetooth 2.1+EDR and Extended Inquiry Response (EIR).

The Windows XP and Windows Vista/Windows 7 Bluetooth stacks support the following Bluetooth profiles natively: PAN, SPP, HID, HCRP. The Windows XP stack can be replaced by a third party stack which may support more profiles or newer versions of Bluetooth. The Windows Vista/Windows 7 Bluetooth stack supports vendor-supplied additional profiles without requiring the Microsoft stack to be replaced.

Linux has two popular Bluetooth Services,Blue Z and Affix. The BlueZ stack is included with most Linux kernels and was originally developed by Qualcomm. The Affix stack was developed by Nokia.

The Bluetooth specification was developed as a cable replacement in 1994. The specification is based on Frequency Hopping spread spectrum technology.

The specifications were formalized by the Bluetooth Special Interest Group (SIG). The SIG was formally announced on 20 May 1998. Today it has a membership of over 20,000 companies worldwide. It was established by Ericsson,IBM,Intel ,Toshiba and Nokia companies.

Versions

1. Bluetooth v1.0 and v1.0B

Versions 1.0 and 1.0B had many problems, and manufacturers had difficulty making their products interoperable. Versions 1.0 and 1.0B also included mandatory Bluetooth hardware device address (BD_ADDR) transmission in the Connecting process (rendering anonymity impossible at the protocol level), which was a major setback for certain services planned for use in Bluetooth environments.

A. Bluetooth v1.1

- Many errors found in the 1.0B specifications were fixed.
- Added possibility of non-encrypted channels.
- Received Signal Strength Indicator (RSSI)

B. Bluetooth v1.2

Faster Connection and Discovery

Adaptive Frequency Hopping spread spectrum (AFH), this improves resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence. Higher transmission speeds in practice, up to 721 kbit/s, than in v1.1.

- Extended Synchronous Connections (eSCO), which improve voice quality of audio links by allowing retransmissions of corrupted packets, and may optionally increase audio latency to provide better concurrent data transfer.

2. Bluetooth v2.0 + EDR

This version of the Bluetooth Core Specification was released in 2004. The main difference is the introduction of an Enhanced Data Rate (EDR) for faster data transfer. The nominal rate of EDR is about 3 Mbit/s, although the practical data transfer rate is 2.1 Mbit/s. EDR uses a combination of GFSK and Phase shift Keying modulation (PSK) with two variants, π/4-DQPSK and 8DPSK EDR can provide a lower power consumption through a reduced duty cycle.

The specification is published as "Bluetooth v2.0 + EDR" which implies that EDR is an optional feature. Aside from EDR, there are other minor improvements to the 2.0 specification, and products may claim compliance to "Bluetooth v2.0" without supporting the higher data rate. At least one commercial device states "Bluetooth v2.0 without EDR" on its data sheet.

C. Bluetooth v2.1 + EDR

Bluetooth Core Specification Version 2.1 + EDR was adopted by the Bluetooth SIG on 26 July 2007.

The headline feature of 2.1 is secure simple pairing (SSP): this improves the pairing experience for Bluetooth devices, while increasing the use and strength of security. See the section on Pairing below for more details.

2.1 allows various other improvements, including "Extended inquiry response" (EIR), which provides more information during the inquiry procedure to allow better filtering of devices before connection; and sniff subrating, which reduces the power consumption in low-power mode.

3. Bluetooth v3.0 + HS

Version 3.0 + HS of the Bluetooth Core Specification[1] was adopted by the Bluetooth SIG on 21 April 2009. Bluetooth 3.0+HS provides theoretical data transfer speeds of up to**24 Mbit/s,** though not over the Bluetooth link itself. Instead, the Bluetooth link is used for negotiation and establishment, and the high data rate traffic is carried over a collocated 802.11 link.

The main new feature is AMP (Alternative MAC/PHY), the addition of 802.11 as a high speed transport. The High-Speed part of the specification is not mandatory, and hence only devices sporting the "+HS" will actually support the Bluetooth over 802.11 high-speed data transfer. A Bluetooth 3.0 device without the "+HS" suffix will not support High Speed, and needs to only support a feature introduced in Core Specification Version 3.0 or earlier Core Specification Addendum .

4. Bluetooth v4.0

The Bluetooth SIG completed the Bluetooth Core Specification version 4.0 (called Bluetooth Smart) and has been adopted as of 30 June 2010. It includes *Classic Bluetooth*, *Bluetooth high speed* and Bluetooth low energy protocols. Bluetooth high speed is based on Wi-Fi, and Classic Bluetooth consists of legacy Bluetooth protocols.

Bluetooth Low Energy, previously known as Wibree, is a subset of Bluetooth v4.0 with an entirely new protocol stack for rapid build-up of simple links. As an alternative to the Bluetooth standard protocols that were introduced in Bluetooth v1.0 to v3.0, it is aimed at very low power applications running off a coin cell. Chip designs allow for two types of implementation, dual-mode, single-mode and enhanced past versions. The provisional names *Wibree* and *Bluetooth ULP* (Ultra Low Power) were abandoned and the BLE name was used for a while. In late 2011, new logos “Bluetooth Smart Ready” for hosts and “Bluetooth Smart” for sensors were introduced as the general-public face of BLE.In a single-mode implementation, only the low energy protocol stack is implemented.

Bluetooth v4.1

The Bluetooth SIG announced formal adoption of the Bluetooth 4.1 specification on 4 December 2013. This specification is an incremental update to Bluetooth Specification v4.0. The update incorporates Bluetooth Core Specification Addenda (CSA 1, 2, 3 & 4) and adds new features which improve consumer usability with increased co-existence support for LTE, bulk data exchange rates, and aid developer innovation by allowing devices to support multiple roles simultaneously.

New features of this specification include:

1. Mobile Wireless Service Coexistence Signaling
2. Train Nudging and Generalized Interlaced Scanning
3. Low Duty Cycle Directed Advertising
4. L2CAP Connection Oriented and Dedicated Channels
5. Dual Mode and Link Layer Topology
6. 802.11n PAL
7. Audio Architecture Updates for Wide Band Speech
8. Fast Data Advertising Interval
9. Limited Discovery Time.
10. Upgradeable .
11. Automatic.
12. Universally accepted.
13. Avoids interference from other wireless devices.

Bluetooth protocol stack

<table>
<tr><td>1.</td><td colspan="6">Application /Profiles</td></tr>
<tr><td rowspan="2">2.</td><td rowspan="2">Audio</td><td>Other
LLC</td><td>RFComm</td><td>Telephony</td><td>Service
Discovery</td><td rowspan="2">Control</td></tr>
<tr><td colspan="4">Logical link Control Adaptation Protocol
Link Layer</td></tr>
<tr><td>3.</td><td colspan="6">Baseband</td></tr>
<tr><td>4.</td><td colspan="6">Physical Radio</td></tr>
</table>

1. Application Layer

2. Middleware Layer

3. Data Link Layer

4. Physical Layer

Bluetooth Protocol Stack[1][2]

It is defined as a layer protocol architecture consisting of core protocols, cable replacement protocols, telephony control protocols, and adopted protocols. Mandatory protocols for all Bluetooth stacks are: LMP, L2CAP and SDP. In addition, devices that communicate with Bluetooth almost universally can use these protocols: HCI and RFCOMM.

Setting up connections

Any Bluetooth device in *discoverable mode* will transmit the following information on demand:

1. Device name
2. Device class
3. List of services
4. Technical information

Any device may perform an inquiry to find other devices to connect to, and any device can be configured to respond to such inquiries. However, if the device trying to connect knows the address of the device, it always responds to direct connection requests and transmits the information shown in the list above if requested. Use of a device's services may require pairing or acceptance by its owner, but the connection itself can be initiated by any device and held until it goes out of range. Some devices can be connected to only one device at a time, and connecting to them prevents them from connecting to other devices and appearing in inquiries until they disconnect from the other device.

Every device has a unique 48-bit address. However, these addresses are generally not shown in inquiries. Instead, friendly Bluetooth names are used, which can be set by the user. This name appears when another user scans for devices and in lists of paired devices.

Most cellular phones have the Bluetooth name set to the manufacturer and model of the phone by default. Most cellular phones and laptops show only the Bluetooth names and special programs are required to get additional information about remote devices. This can be confusing as, for example, there could be several cellular phones in range named T610.

Pairing and bonding

Many of the services offered over Bluetooth can expose private data or allow the connecting party to control the Bluetooth device. For security reasons it is necessary to be able to recognize specific devices and thus enable control over which devices are allowed to connect to a given Bluetooth device. At the same time, it is useful for Bluetooth devices to be able to establish a connection without user intervention (for example, as soon as they are in range).

To resolve this conflict, Bluetooth uses a process called *bonding*, and a bond is generated through a process called *pairing*. The pairing process is triggered either by a specific request from a user to generate a bond (for example, the user explicitly requests to "Add a Bluetooth device"), or it is triggered automatically when connecting to a service where (for the first time) the identity of a device is required for security purposes. These two cases are referred to as dedicated bonding and general bonding respectively.

Pairing often involves some level of user interaction; this user interaction is the basis for confirming the identity of the devices. Once pairing successfully completes, a bond will have been formed between the two devices, enabling those two devices to connect to each other in the future without requiring the pairing process in order to confirm the identity of the devices. When desired, the bonding relationship can later be removed by the user.

IMPLEMENTATION

During the pairing process, the two devices involved establish a relationship by creating a shared shift known as a *link key*. If a link key is stored by both devices they are said to be *paired* or *bonded*. A device that wants to communicate only with a bonded device can cryptographically authenticate the identity of the other device, and so be sure that it is the same device it previously paired with. Once a link key has been generated, an authenticated Asynchronous Connection Less ACL) link between the devices may be encrypted so that the data that they exchange over the airwaves is protected against eavesdropping

Link keys can be deleted at any time by either device. If done by either device this will implicitly remove the bonding between the devices; so it is possible for one of the devices to have a link key stored but not be aware that it is no longer bonded to the device associated with the given link key.

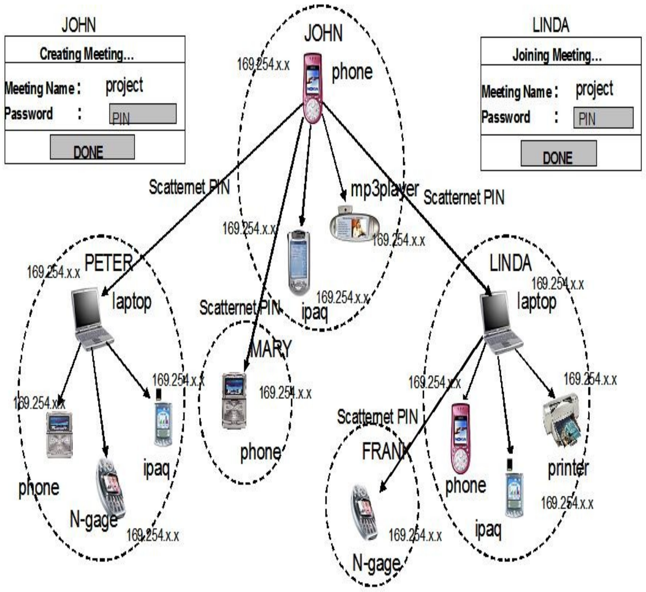
Bluetooth services generally require either encryption or authentication, and as such require pairing before they allow a remote device to use the given service. Some services, such as the Object Push Profile, elect not to explicitly require authentication or encryption so that pairing does not interfere with the user experience associated with the service use-cases.

Pairing mechanisms

Pairing mechanisms have changed significantly with the introduction of Secure Simple Pairing in Bluetooth v2.1. The following summarizes the pairing mechanisms:

- ➢ *Legacy pairing*: This is the only method available in Bluetooth v2.0 and before. Each device must enter a PIN CODE pairing is only successful if both devices enter the same PIN code. Any 16-byte UTF-8 string may be used as a PIN code; however, not all devices may be capable of entering all possible PIN codes.
- ➢ *Limited input devices*: The obvious example of this class of device is a Bluetooth Hands-free headset, which generally have few inputs. These devices usually have a *fixed PIN*, for example "0000" or "1234" that are hard-coded into the device.
- ➢ *Numeric input devices*: Mobile phones are classic examples of these devices. They allow a user to enter a numeric value up to 16 digits in length.
- ➢ *Alpha-numeric input devices*: PCs and smartphones are examples of these devices. They allow a user to enter full UTF-8 text as a PIN code. If pairing with a less capable device the user needs to be aware of the input limitations on the other device, there is no mechanism available for a capable device to determine how it should limit the available input a user may use.
- ➢ *Secure Simple Pairing* (SSP): This is required by Bluetooth v2.1, although a Bluetooth v2.1 device may only use legacy pairing to interoperate with a v2.0 or earlier device.SSP has the following characteristics:

- *Just works*: As implied by the name, this method just works. No user interaction is required; however, a device may prompt the user to confirm the pairing process. This method is typically used by headsets with very limited IO capabilities, and is more secure than the fixed PIN mechanism which is typically used for legacy pairing by this set of limited devices. This method provides no man in the middle (MITM) protection.
- *Numeric comparison*: If both devices have a display and at least one can accept a binary Yes/No user input, they may use Numeric Comparison. This method displays a 6-digit numeric code on each device. The user should compare the numbers to ensure they are identical. If the comparison succeeds, the user(s) should confirm pairing on the device(s) that can accept an input. This method provides MITM protection, assuming the user confirms on both devices and actually performs the comparison properly.
- *Passkey Entry*: This method may be used between a device with a display and a device with numeric keypad entry (such as a keyboard), or two devices with numeric keypad entry. In the first case, the display is used to show a 6-digit numeric code to the user, who then enters the code on the keypad. In the second case, the user of each device enters the same 6-digit number. Both of these cases provide MITM protection.



Disadvantages:[4]

1. Battery use is severely increased.

2. Outside the range of 60 metres the device is undiscoverable.

3. Device incompatibility due to usage of different operating systems.

4. Not so well developed like the Wi-Fi.

5. Bluetooth is omni-directional, so it can have problems when it's trying to discover a recipient device like a headsets, speakers, phones etc.

6. Bluetooth speed is lower than infrared.

Security concerns

Prior to Bluetooth v2.1, encryption is not required and can be turned off at any time. Moreover, the encryption key is only good for approximately 23.5 hours; using a single encryption key longer than this time allows simple XOR attacks to retrieve the encryption key.

- Turning off encryption is required for several normal operations, so it is problematic to detect if encryption is disabled for a valid reason or for a security attack.

Bluetooth v2.1 addresses this in the following ways:

- Encryption is required for all non-SDP (Service Discovery IProtocol) connections
- A new Encryption Pause and Resume feature is used for all normal operations requiring encryption to be disabled. This enables easy identification of normal operation from security attacks.
- The encryption key is required to be refreshed before it expires.[2]

Link keys may be stored on the device file system, not on the Bluetooth chip itself. Many Bluetooth chip manufacturers allow link keys to be stored on the device; however, if the device is removable this means that the link key will move with the device.

Bluejacking

Bluejacking[3] is the sending of either a picture or a message from one user to an unsuspecting user through *Bluetooth* wireless technology. Common applications include short messages, *e.g.*, "You've just been bluejacked!".Bluejacking does not involve the removal or alteration of any data from the device. Bluejacking can also involve taking control of a mobile device wirelessly and phoning a premium rate line, owned by the bluejacker. Security advances have alleviated this issue.

FUTURE SCOPE

Since the formation of the original group, more than 1800 manufacturers have joined the initiative worldwide. According to one market research report, Bluetooth technology is expected to be built into over 200 millions devices before the end of 2014.[4] As a result of success of WAP (Wireless Application Protocol), adoption of smart phones and handheld devices, Bluetooth will have tremendous effects on everyday life. Bluetooth is one of the key technologies that can make the mobile information society possible, blurring the boundaries between home, the office, and the outside world. The seamless connectivity promised by Bluetooth makes it possible to explore a range of interactive and highly transparent personalized services which were even difficult to dream of because of the complexity involved in making various devices talk to each other. Already many Bluetooth pilot products have rolled into the market backed by big vendors, which is a very healthy sign for the acceptance of the technology. The support for Bluetooth is not limited to companies developing Bluetooth enabled products only. Bluetooth applications can have far reaching impacts on many other industries as well. Bluetooth technology adoption is expected to be widespread throughout the computer and telecommunications industry. Implementation of the Bluetooth technology is expected to grow the market for personal mobile devices and indirectly increase airtime usage for wireless data. The current speed of Bluetooth is low and this needs to be incremented.The technologists are trying their best in this field.

CONCLUSION

Bluetooth is thus a powerful technology using air interface to make pairing possible between devices. It allows us to exchange files,, text,images ,etc over a network with range of about 60 meters. It can be used as portable or fixed device. Also the enhanced security techniques have built trustworthiness for data transfer. The cost and competition from other standards have hindered the widespread acceptance, but Bluetooth does offer a viable solution to many devices that might not have wireless connectivity without it.

REFERENCES

1. Bluetrees-scatternet to enable Bluetooth based ad-hoc networks by Eric Johansson School of Computer Science and Technology, Texas and Basagni.S
2. Demonstrating vulnerabilities in Bluetooth security by Hager C.T, Bradley Institute of Electronics and Telecommunication
3. Implementation of Bluetooth based wireless networks.
4. “BLUETOOTH TECHNOLOGY” Rajan Poddar & Vinita Singh.
5. www.creativeworld9.com/.../abstract-and-full-**paper**-on-**bluetooth**.html

ACKNOWLEDGMENT

“T. A. Author thanks Prof. V. Balachandran for his constant guidance for paper publishing also would like to thanks Prinicipal and Director General of MGMCET, Kamothe, Panvel for their Motivations.”

Arwa Kurawar is currently studying in Mumbai University at MGMCET, Kamothe, Panvel since 2011, currently pursuing B.E. in Computer Science and Engineering, with excellent Academics. She is having interest in Studying New Technologies, and Student Member of CSI. She has been topper since last 3 years consecutively.

Ayushi Koul is currently studying in Mumbai University at MGMCET, Kamothe, Panvel since 2011, currently pursuing B.E. in Computer Science and Engineering, with excellent Academics. She is having interest in Learning New Technologies, and Student Member of CSI. She has been among toppers since last 3 years consecutively.

Prof. Viki Tukaram Patil [M.Tech in Computer Science, VJTI] He is currently working in Mumbai University at MGMCET, Kamothe, Panvel since 2013 as Assistant Professor, He has Completed M. Tech from VJTI in 2013, earlier he has completed .B.E. from K. J. Somaiya C.O.E., Mumbai University with good Academic Grades. He has published more than 5 papers in National and International Journals. His Research Area is in Data Mining, Cloud Computing (Hadoop), Distributed Databases. He is Member of ISTE and IEI. He was Topper in his College for 2 years. He has completed many Certification Courses like Java, Oracle, CCNA, LINUX, HADOOP, and CLOUD COMPUTING Workshop by ANEKA.