# Bluetooth Technology - Functionalities & Security Issues

Bhawna Singla
*Master of Computer Application*
*Ansal University, Gurgaon*
*Haryana, India*
bhawna1694@gmail.com

Vijaya Lakshmi Singh
*School of Engineering and Technology*
*Ansal University, Gurgaon*
*Haryana, India*
vijayalakshmisingh@ansaluniversity.edu.in

***Abstract*— Bluetooth is mainly used to establish Personal Area Network wireless communication. As Bluetooth Technology is gaining widespread popularity, vulnerabilities in its security is also increasing. Bluetooth is an inexpensive way to reduce the need of cabling between devices.This paper presents an overview of Bluetooth Technology, its functionalities and advantages. It also presents the security risks associated with Bluetooth which can be very dangerous for some users. Andfinally,the paper concludes with somesecurity recommendations that can be involved during data exchange between Bluetooth devices.**

***Keywords-Bluetooth Functionlity; Bluetooth Security;Malicious Attackers; Counter Measures; MIM; Privacy***

## I. INTRODUCTION

Bluetooth is a standard for short range, low power, robust and minimal effort remote correspondence that uses radio innovation. It was designed for data transfer between electronic devices without the need of cables.

Bluetooth is a very cost effective technology providing mechanism for establishing small wireless networks on ad hoc basis.

Bluetooth wireless technology (BWT) was created in 1994 at Ericsson in Sweden. The first motivation behind BWT was to dispose of the requirement for exclusive link associations between gadgets such as PDAs and scratch pad PCs. In February, 1998, five organizations, Ericsson, Nokia, IBM, Toshiba and Intel, established a Group of Special Interest (SIG). More than 2100 organizations around the globe as of now bolster Bluetooth innovation. Mobile phones, small PDAs and peripherals were the target markets. [1]

Figure1.The image of Bluetooth

As renowned as the name is the Bluetooth image. Everyone can perceive this image like the Bluetooth symbol, yet again few of them knows the starting point. Bluetooth's logo consolidates the representation of the Nordic runes Hagalaz (translated by 'H') and Berkana (deciphered by 'B') in the same image.

## II. ADVANTAGES OF BLUETOOTH TECHNOLOGY

The following are the advantages of using Bluetooth technology:

1. Wireless - Bluetooth technology can replace of cables/wires, for example those used for peripheral devices (mouse, keyboard, printers, headsets and many more). It even allows wireless synchronization.
2. Affordable Technology - The technology of Bluetooth is very low-cost. Its cost-effective for any individual or company to implement.
3. File sharing made easy - A Bluetooth device can support file sharing with other Bluetooth enabled devices such as cell phone, laptops etc. by forming a piconet.
4. Highly Compatibility Bluetooth offers high level of compatibility among various devices. Devices of different models can even connect to each other.
5. Low power consumption. Since Bluetooth uses low power signals, therefore the technology requires low power, very little energy and will use less battery.
6. Personal Network - Up to 7 Bluetooth devices can be connected to each other within a range of up to 30 feet, thereby forming a Personal Network.

## III. BLUETOOTH ARCHITECTURE

Bluetooth architecture defines two types of networks [2]:

*1)Piconet: It* comprises of two or more Bluetooth devices which are situated in a very close physical proximity. It operates on same channel and same frequency hopping sequence.

- It's a network that consists of one primary (master) node and 7 active secondary (slave) nodes.
- A piconet have up to 8 active nodes, i.e. 1 master and 7 slaves
- Communication between master and slave nodes can be one-to-one or one-to-many.
- Communication between slave-slave is not possible.
- A piconet can have up to 255 parked nodes. Parked nodes are secondary nodes. They cannot take part in communication until it is moved to active state.

*2) Scatternet:*

- It's formed by combining various piconets.
- A master in one piconet can also be a slave in another piconet, as shown in Figure3.
- Also, called as bridge slave. It can receive messages as slave node in one piconet and send in another piconet acting as master.
- Therefore, a station can be a member of two piconets.

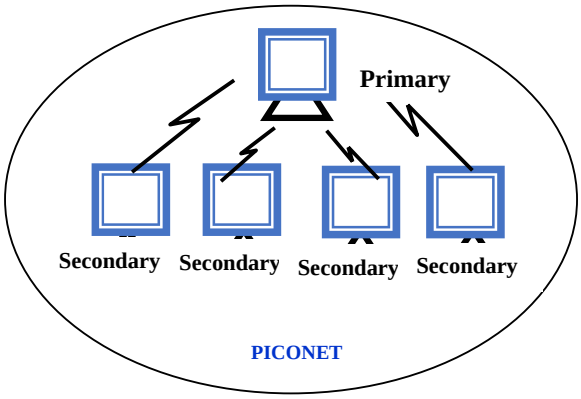



Figure 2. Piconet

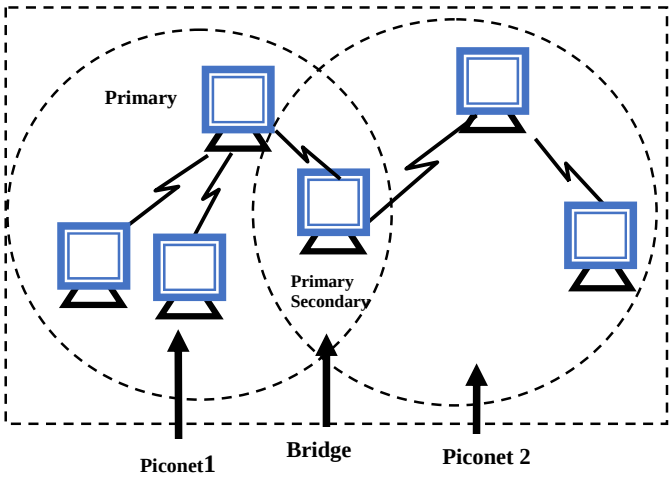



Figure 3. Scatternet

The Bluetooth GAP provides a framework in which Bluetooth devices can discover each other and make a connection. It enables a device to interact with the outside world, broadcast data and perform many other operations. It is also known as generic access protocol(GAP).

There are three discovery modes set by Bluetooth Gap:

a) General Discovery

b) Limited Discovery

c) Non-Discoverable

Bluetooth GAP is one of the most basic profiles, but every other foundation makes use of it to establish a link. It controls the formation of a connection and controls the use of security and encryption. [4]

## IV. BLUETOOTH PROTOCOL STACK

OBEX(OBjectEXchange): It is a session-layer protocol for the exchange of objects like business cards, notes and other such files.
TCS BIN (Telephony Control Service): It is a bit oriented protocol. It also used for exchanging signaling information between Bluetooth devices for the establishment of voice and data calls.
RFCOMM is a transport protocol which provides emulation of nine circuits of RS-232 serial ports. This protocol supports up to 60 connections at the same time between two Bluetooth devices.
WAE/WAP: Bluetooth Architecture also includes the wireless application environment and the wireless application protocol.
Host Controller Interface (HCI): It makes sure that a secured transmission takes place between a host and the Bluetooth module. Bluetooth microchip contains the protocols below HCI and the host device's software package contains the protocols above the HCI.
Service discovery protocol (SDP) is an important protocol that allows Bluetooth devices to create an ad hoc network. It also handles device data, search for services, and browses lists. It finds the services present in RF proximity and determine their characteristic.
Logical link control and adaptation protocol (L2CAP): This module usually resides in the host. It ensures both connectionless and connection-oriented services. Transmission from master to one slave is through connection oriented service whereas transmission from master to multiple slaves is through connectionless service. Whenever a connection oriented or connectionless request is placed, L2CAP begins its security procedures.
The link manager (LM) is used to create a connection between the application and the link controller (LC) residing on a local device. It can also be used for connecting with a remote Link Manager with the help of protocol data units (PDU) and the link manager protocol (LMP). [2][3][5]

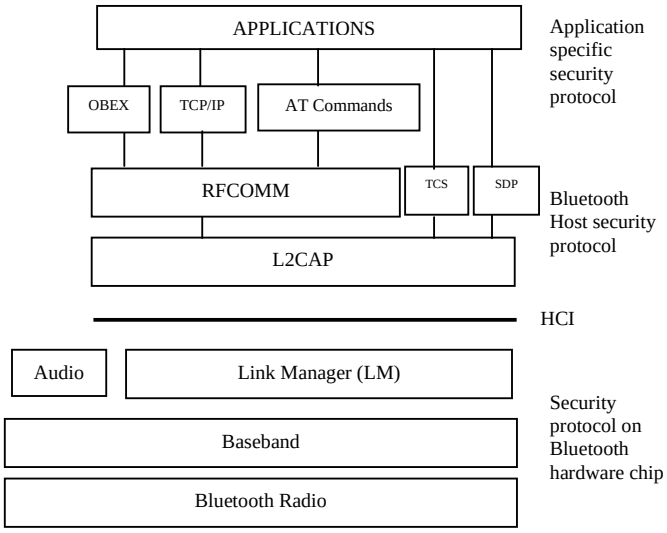


Figure 4. Bluetooth Protocol Stack

## V. HOW BLUETOOTH WORKS

BWT-empowered gadgets work in the unhindered 2.4-gigahertz (GHz) Industrial, Science, Medicinal (ISM) band. The ISM band ranges between 2.400 GHz and 2.483 GHz. BWT-empowered gadgets utilize seventy-nine 1-megahertz frequencies (from 2.402 to 2.480 GHz) in the ISM band.

BWT-empowered gadgets utilize a procedure called recurrence bouncing to minimize listening in and impedance from different systems that utilization the ISM band. With recurrence jumping, the information is partitioned into little pieces called bundles. The transmitter and collector trade an information parcel at one recurrence, and afterward they jump to another recurrence to trade another bundle. They rehash this procedure until all the information is transmitted. BWT gadgets arbitrarily jump between frequencies up to 1600 times each second—much speedier than different sorts of gadgets that utilization the ISM band. This implies if another gadget, for example, a 2.4-GHz cordless telephone, meddles with a BWT system at a specific recurrence, the impedance just endures for around 1/1600 of a second until the BWT gadgets jump to another recurrence. This gives BWT systems a high insusceptibility to obstruction from other 2.4-GHz gadgets.

There are three classes of BWT radio gadgets, each with an alternate greatest reach:

Class 1 (100 meters); Class 2 (50 meters); and Class 3 (10 meters). HP journals highlight Class 3 BWT radios, and HP printers highlight Class 1 radios.

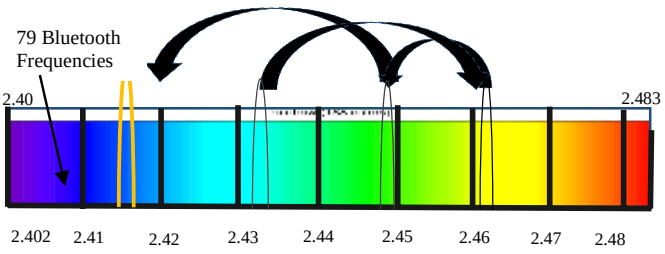



Figure 5.ISM Band Frequency Range(GHz)

### A. *Recurrence Bands*

The standard Bluetooth works in the band of 2,4 GHz. Even though around the world, this band is accessible, the width of the band can contrast in various nations. This is the recurrence of band of the logical and medicinal commercial ventures 2.45 GHz (ISM*).
The extents of the transmission capacity in The United States and Europe are between 2.400 to 2.483,5 MHz furthermore, it covers a portion of France and Spain. The scopes of the data transmission in Japan are between 2.471 to 2.497 MHzSo, the framework can be utilized worldwide because of that the transmitters of radio spreads 2.400 and 2.500 MHz and it is conceivable to choose the proper recurrence. This ISM* is opened for any arrangement of radio and should deal with the impedances of screens for infant, the controls for entryways of carports, the remote phones and the microwave stoves (the source with higher obstruction).

ISM: The mechanical, exploratory and medicinal (ISM) radio groups were initially saved universally for the utilization of RF electromagnetic fields for modern, experimental also, restorative purposes other than interchanges. When all is said in done, correspondences gear must acknowledge any obstruction produced by ISM hardware.

### B. *Power*

The types of gear of transmission are qualified in 3 bunches as indicated by the level of force of discharge, as should be obvious beneath. The beneficiary hardware must have a sensibility of no less than 70 dBm, and the rate of allowable slip-up must be a minor or equivalent to 0,1 %. Gadget Power Class Most extreme Permitted Power mW(dBm)

### C. *Range (rough)*

Class 1 100 mW (20 dBm) ~100 meters

Class 2 2.5 mW (4 dBm) ~10 meters

Class 3 1 mW (0 dBm) ~1 meter

The chip will be fused in compact gadgets and controlled by batteries, that is, the reason it must has an exceptionally constrained utilization of force (up to 97 % less than a cellular phone).

If the Bluetooth gadgets don't trade data, "hold up" method is built to spare vitality. The force of transmission that is utilized as detail is of 1 mW for an extent of 10 m, 100 mW for an extent of up to 100 m.

### D. *Scope*

The associations have a most extreme scope of 10 meters, however utilizing enhancers it is conceivable to come up to 100 meters, however making some bending meddles. Possibly it doesn't look excessively, however it is important to recall that these gadgets were made by the aim of utilizing them as a part of shut situations and little separations.

### E. *Conventions*

Diverse applications can work under various arrangements of conventions; by the by, every one of them have a connection of data and a physical top basic Bluetooth. The figure beneath demonstrates the arrangement of conventions:

We are not going to examine in subtle element every one of the conventions since it would take as well long and this is in fact excessively complex for the point of this

work. At any rate, I included this notice about the Bluetooth conventions since I found a ton of data about that point.

### *F. Obstructions*

If we investigate impedances with different gadgets, it is important to have care with the individuals who work in the same band. For instance, the same as there is disallowed the utilization of cellular phones in the planes, it is conceivable to disallow the utilization of any another gadget that fuses a Bluetooth chip, since it can meddle with the components of route. However, this can be an issue since it has been intended to keep up a consistent correspondence, even in development, and inside portfolios, and it can be working even incidentally for the client.

## VI. BLUETOOTH SECURITY

Bluetooth specifications define four security modes [7]:

According to NIST,

- Security Mode 1: Non-secure.
- Security Mode 2: Only security manager has access to particular services and devices.
- Security Mode 3: Bluetooth device establishes security mechanisms before the physical link is completely established. These devices approve authentication and encryption for all connections to and from the device.
- Security Mode 4: It is similar to Security Mode 2. Here, security procedures are initiated after the link setup. Security requirements for services must be categorized as one of the following:
    i. Authenticated link key required
    ii. Unauthenticated link key required
    iii. Or no security required

### *A. Confidentiality [8]*

In addition to the Security Modes, Bluetooth allows a separate confidentiality service to prevent eavesdropping efforts on the payloads of the packets interchanged between Bluetooth devices. Only two out of three encryption modes actually provide confidentiality.

The modes are as follows:

- Encryption Mode 1—No encryption at all.
- Encryption Mode 2— In this mode, only the Broadcast traffic is not encrypted. Traffic which is individually addressed is encrypted using encryption keys based on individual link keys
- Encryption Mode 3—Entire traffic is encrypted using an encryption key based on the master link key.

### *B. How Bluetooth security works?*

Bluetooth security prevents unwanted devices from gaining access to the data that is transmitted between devices. Bluetooth's security system builds upon three procedures: Pairing, Authentication and Encryption. [10]

Pairing: When two devices connect for the first time, they need to go through a setup process called pairing. During this procedure, both the devices goes through a handshake process in which a shared secret key is created. This key is never transmitted over the air and can't be accessed by a third party. Once this process is complete, the secret key is saved and used for authentication purpose and generates encryption key when the devices communicate with each other. But the pairing process cannot be initiated over the air. For this physical access to devices is needed.

Authentication: The intention of authentication is to verify that the other device actually belongs to the paired and trusted devices. Using the secret key and some rules, one device creates a challenge for the other device it wants to authenticate. If the device that is being challenged is paired it will have all the important information to determine the right response to the stated challenge.

Encryption: The main aim of encryption is to make the data transmission between two entities illegible for everybody except the true receiver. Sender encrypts the data using an encryption algorithm. Data will be decrypted by the receiving module to its actual format based on the same algorithm. Only the paired entities know the information that is necessary to perform encryption and decryption. The encryption information is never transmitted over the air. It is submerged in the units which make it very hard for an eavesdropper to make out anything from data even with access to it. [10]

### *C. Trust Levels, Service Levels, and Authorization*

Bluetooth allows two levels of trust and three levels of service security [8][9]

Trust Levels of Bluetooth

- Trusted device: It has a permanent relationship with another device and has complete access to all services.
- Untrusted device: It does not have an established and secure relationship with another Bluetooth device, therefore, it doesn't have full access to all the services. It receives restricted access to services.

Levels of service security -

- Service Level 1:It requires authentication and authorization. Only trusted devices can gain automatic access while untrusted devices require manual authorization.
- Service Level 2: It requires authentication only. Authorization is not compulsory. Devices can gain

access to an application only after an authentication process.

- Service Level 3: It is open to all devices, means no authentication needed. Automatic access is granted.

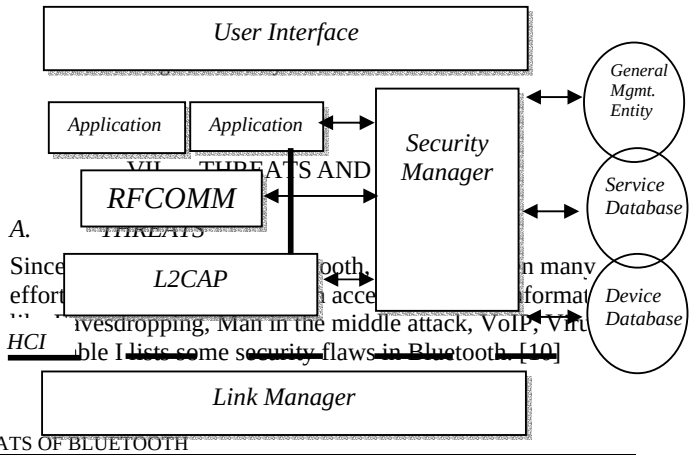
### D. *Security Architecture*

Security Manager is the key component in Bluetooth Architecture. He keeps all the information related to security of devices. It's his duty to decide whether to accept or reject a connection request based upon security requirements like authentication, encryption etc. He initiates the pairing and PIN query process. The Security manager requires all the information related to devices and services before taking a decision whether to allow access or deny it and if so, then to what services. [19]

Following are the few steps followed by security manager in granting or denying access to a remote device to connect:

1) Remote device requests for access to the service.
2) Connection request by remote device comes to L2CAP (logical link control and adaptation protocol)
3) L2CAP sends request to security manager to grant access
4) Both device and service databases are queried by security manager.
5) If the remote device is a trusted one, then security manager may or may not ask for authentication or authorization.
6) But if the device is untrusted, then the security manager may either end the connection or ask for authorization. Authentication will happen when link keys are exchanged. The security manager can call an application protocol to apply application level security such as a username or a password for authentication of device. It all depends upon on the security policy governing access.
7) The Security manager then needs to determine whether the service access requires link encryption or not. If yes, then keys will be negotiated and exchanged at the logical link control and adaptation protocol level. Then the connection will further continue to be setup. *[9] [20]*

The security architecture above is a very flexible. This framework tells that when a user must be involved (for e.g., during providing a PIN) and what does the underlying Bluetooth protocol layers needs to follow. With a centralizedsecurity manager, this approach provides ease in implementation of policies. [21]




## VII. THREATS AND

### A. *THREATS*

Since ooth, n many effort acce format ivesdropping, Man in the middle attack, VoIP, Viru ble I lists some security flaws in Bluetooth. [10]

TABLE I. SOME THREATS OF BLUETOOTH

| SECURITY | WHAT IS IT? | HOW IS IT HANDLED? | LEVEL OF SECURITY |
|---|---|---|---|
| Man in the middle attack | The attacker gains access to the link key used by the two devices. The attacker can create a new connection with each of the devices, impersonating to be the other device. The two devices still assume that they are talking to each other, but they are communicating with the attacker. The attacker can alter the data transmitted between them or connect later to those devices. | An excellent way to prevent this attack is make sure that pairing takes place in private environment. | VERY HIGH SECURITY - It is very hard to execute this kind of attack in actual practices. No real-life cases have been reported yet. |
| Eavesdropping | A third party gains unwanted access to the Bluetooth connection and listens to all the communication between them. | Voice can be encrypted into digital data and then decrypted. | HIGH SECURITY- Instrument that observes a Bluetooth connection is quite expensive. Even with the correct instrument, the eavesdropper can be present when the pairing takes place. |
| Virus | A virus or malware can be transmitted to the Bluetooth system over the air. | Few Bluetooth systems provides great security and doesn't provide an environment where virus can run. | VERY HIGH SECURITY- Viruses have been made by engineers as a proof of concept of security flaws. Presently there are no known Bluetooth viruses that can be dangerous or harmful. |
| VoIP | Someone can gain access to a LAN via a Bluetooth unit supporting VoIP. | Bluetooth security is managed in the similar way for VoIP as for other voice | HIGH SECURITY- Few products only offer voice data to be transmitted from the Bluetooth headset to the connection |

| | | | |
|---|---|---|---|
| | | communication. | point. So it's not possible to gain access to data in a LAN via few products. |
| Free Calling | A third-party attempt to pair a headset with a Bluetooth unit to make phone calls for free. | Authentication and Pairing are used to make sure that a device cannot be paired without granting physical access. | HIGH SECURITY- The invader would have to gain physical access to the mobile phone to pair his device. The invader would be able to make calls even after pairing only when being in close proximity to the target. |

Some Other Threats

- Denial of service attacks(DoS): These attacks can be conducted against the Bluetooth radio, battery power or communications channels. This results in unwanted access to the Bluetooth device by other devices or resources. [6] Mobile networks are always unsafe to Denial of Service (DoS) attacks. They comprise of mobile devices which are mostly battery powered. Bluetooth is no special case. An intruder can send unwanted or fake messages to a mobile device. When this device receives a message, it executes some kind of computations, a procedure will start absorbing battery power [14]. After some time, all the battery power will be consumed. This depletion of the battery power is known as sleep deprivation attack [13]. The Bluetooth system which is providing some kind of service is flooded by malicious requests from an attacker, which results in crashing of the system and consumption of battery power. [12][18]

"Blue" Threats [11]

- Bluesnarfing – In some phones, it is possible to create a connection to a Bluetooth device without the knowledge of user and gain unwanted access to personal data stored like phonebook, calendars, photos and even device (International Mobile Equipment Identity) IMEI number. IMEI number uniquely identifies the phone and can be used for illegal "Phone Cloning". This happens when user has set his phone to discoverable mode. There are different tools available now which can even bypass the safety net. [12] [17] The Bluesnarf attack can be combined with a backdoor attack. Thus, not only the personal data of the mobile phone can be accessed, but other services also such as gaining access to the Internet, sending messages etc. are available to the attacker without the knowledge of user. [16] [15]

- Bluejacking - Two Bluetooth devices send their name to each other on being paired. By default, name of a device is typically set to its brand name (for e.g., "SAMSUNG-S6-EDGE"). However, the user can later change this default name into an arbitrary string (up to 248 characters) and then this (user defined) name will be shown on other devices. This name is basically used to further enable the pairing process. First, a list of all the discoverable devices in the neighbourhood is displayed on device. Then the user selects name of the device with whom it wants to pair its device. The Bluejacking attack tries to manipulate this name to send advertisements to other Bluetooth devices. Malicious sender's name is the advertisement itself. This can become an irritating problem for some users. [15]

- Bluebugging – Without the knowledge of user, an attacker can use the commands of user's device due to a security errors. In BlueBugging , the attacker attempts to unauthorized gain access to a Bluetooth enabled device and manipulates the victim device to compromise on its security. Attackers can make use of this technique to track the target device and access his personal information or make calls or send SMS from his device or do some other illegal activities.

### *B. MEASURES*

Bluetooth Technology has many security risks. There are few ways by which we can secure ourselves. Following provides a checklist with few guidelines and recommendations for secure Bluetooth connections [22]:

- It might be possible that the device we are connected to be sniffed, therefore, avoid communicating or transmitting critical and personal information.

- Users should never enter passkey if an unexpected prompt comes. Don't accept any kind of attachment or file received on your phone if you were not expecting. If your device receives a pair request and you didn't initiate, then deny it and make sure your 'discoverable' mode is either "off" or "hidden". Users must not allow any kind of transmissions like messages, images etc. from any unknown or suspicious devices.

- The Bluetooth device must be set to non-discoverable mode if a pairing is not important. This can help to reduce the chances of Bluetooth devices responding to prompts by unknown Bluetooth devices. If the pairing is done, "Discoverable" mode must be turned off. [2]

- If possible conduct the pairing in a private place to prevent the attackers from interfering the communication.

- The attacker won't be able to decrypt the payload if he hasn't determined the encryption keys and link keys. If the device is put into "non-discoverable" mode, then unit key will be difficult to obtain. The unit key can be used for fraud or spoofing purposes. [5]

- If the pairing is just for one-time communication and sharing of data, then stored link keys on Bluetooth device must be deleted after that.

- Exercising application layer security and a public key infrastructure provides extra security benefits and limits the Bluetooth devices which have access to certain services and provides authentication or authorization. For example, password could be requested from the user for authentication of the user. This could help to reduce risk against lost or theft, man-in-the-middle attacks, eavesdropping etc.

- Users must be made aware of their security-related duties related Bluetooth use.

- A list detailing all the precautionary measures must be provided to users. For eg: protecting Bluetooth devices from theft.

- To ensure that all the transmissions remain within secured area of organization, all the Bluetooth devices must be set to the lowest necessary and sufficient power level.

- Random and long PIN codes must be chosen. Avoid PINs like all zeroes. The PIN needs to be saved by an attacker. Protecting and choosing the correct PIN reduces the chances of eavesdropping.

- If a Bluetooth device is misplaced or stolen, users should instantly remove that missing device with which it was earlier paired.

- Install an antivirus software on Bluetooth-enabled hosts which can be commonly targeted by malware.

- Deploy fully tested software patches and upgrades on regularly basis.

## VIII. CONCLUSION

This paper discusses how one can utilize Bluetooth Technology amazingly. It can do much more than just replacing the cables between devices. Bluetooth is a standard utilized as a part of connections of radio of short degree, bound to supplant wired associations between electronic gadgets like cell phones, Personal Digital Associates (PDA), PCs, and numerous different gadgets. Each year we need to include new peripherals to our PCs and the need to supplant the wired associations is more essential consistently. That is the reason the Bluetooth innovation is going proceed extending with the backing of the business of Computer science and of Information transfers, which somehow ensures the achievement. It also discusses various security issues involved in this technology. Different vulnerabilities, threats and measures a user can take to protect himself are discussed. The latest improvements and innovations to Bluetooth will be studied for future work.

## REFERENCES

[1] [Online] Bluetooth Wireless Technology Basics, http://www.cs.odu.edu/~cs752/papers/bluetooth-001.pdf

[2] vikethozotsira, Gypsy Nandi, "Bluetooth Technology: Security Issues and Its Prevention", Int.J.Computer Technology &Applications,Vol 5 (5),1833-1837

[3] Nateq Be-Nazir Ibn Minar, Mohammed Tarique, "Bluetooth Security Threats and Solutions: A Survey", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012

[4] [Online] Bluetooth Network Connection &Pairing,http://www.radio-electronics.com/info/wireless/bluetooth/networks-networking-connections-pairing.php

[5] [Online] Service Discovery, https://www.bluetooth.com/specifications/assigned-numbers/service-discovery

[6] Tu C. Niem, "Bluetooth And Its Inherent Security Issues", SANS GIAC Security Essentials Certification (GSEC) v1.4b 11/04/2002

[7] [Online] Security of Bluetooth Systems and Devices, http://csrc.nist.gov/publications/nistbul/august-2012_itl-bulletin.pdf

[8] John Padgette, Karen Scarfone, Lily Chen, "Guide to Bluetooth Security", NIST Special Publication 800-121 Revision 1

[9] Nikhil Anand. "An Overview of Bluetooth Security", Global Information Assurance Certification Paper

[10] [Online] Bluetooth Security,www.jabra.com/~/media/Documentation/.../WP_Bluetooth_50004_V01_1204.ashx

[11] [Online] Bluetooth security, http://www.ece.umd.edu/class/ents650/bluetoothsecurity.pdf

[12] Dave Singelée, Bart Preneel, "Review of the Bluetooth Security Architecture", Information Security Bulletin, March 2006 Volume 11

[13] C. Candolin, Security Issues for Wearable Computing and Bluetooth Technology, 2000 http://www.tml.hut.fi/~candolin/ Publications/BT/

[14] A. Hodjat and I. Verbauwhede, The Energy Cost of Secrets in Ad–Hoc Net works. In Proceedings of the IEEE Workshop on Wireless Communications and Networking (CAS '02), 2002

[15] [Online] Bluejackinghttp://www.bluejackq.com/

[16] A. Laurie and B. Laurie,Serious Flaws in Bluetooth Security Lead to Disclosure of Personal Data http://bluestumbler.org

[17] Sarbanes-Oxley Compliance Journal. 2005. Detecting Bluetooth Security Vulnerabilities. Retrieved July 1, 2006 from http://www.sox.com/News/detail.cfm?Articleid= 217

[18] Harry O'Sullivan, "Security Vulnerabilities of Bluetooth Low Energy Technology (BLE)", Tufts University

[19] C. S. R. Prabhu, A. PrathapReddi, bluetooth technology: and its applications with java and j2me, phi Learning Pvt. Ltd., 01-Jan-2004

[20] Vinayak P. Musale, S. S. Apte, "Security Risks in Bluetooth Devices", International Journal of Computer Applications (0975 – 8887) Volume 51– No.1, August 2012

[21] Thomas Muller, "Bluetooth Security Architecture",

[22] Praveen Kumar Mishra, "Bluetooth Security Threats", International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 4 No. 02 Feb 2013

AUTHORS PROFILE

Bhawna Singla is a student of Masters of Computer Applications, Ansal University, Gurgaon, Haryana, India.

Vijaya Lakshmi Singh is the Assisatnt Professor in School of Engineering And Technology, Ansal University, Gurgaon, Haryana, India. She has 6 years of teaching experience. Her area of interest include ad hoc networ and cloud computing.