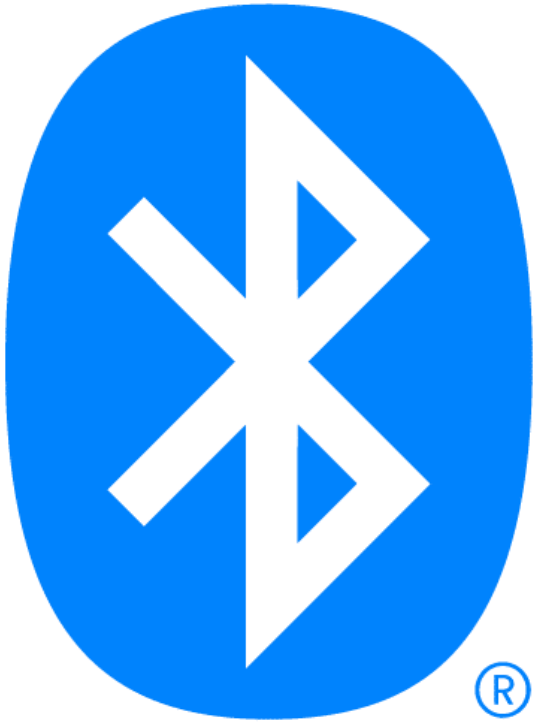
COEN 331 & COEN 233
(Wireless and Mobile Networks
& Computer Networks)
Winter 2020

Bluetooth



Kapil Varma
(1483983)
Guidance by: **Prof.Dr.Kevyan Moataghed**

Table of Contents

0. Audience.....5
1. Introduction.....6
2. Understanding Bluetooth.....8
    2.1 Communication Techniques.....8
    2.2 Bluetooth History.....10
    2.3 How does Bluetooth Work?.....14
    2.4 Bluetooth Applications.....17
    2.5 Bluetooth Versions.....19
3. Bluetooth Architecture and Hardware.....22
    3.1 Specification.....22
    3.2 Bluetooth Protocol Stack.....23
    3.3 Bluetooth Protocol Profiles.....32
4. Security.....35
    4.1 Bluetooth Security.....35
    4.2 Bluetooth Attacks.....39
    4.3 Bluetooth Attack Levels.....48
    4.4 Bluetooth Attack Prevention.....50
5. Conclusion.....52
6. Future Work.....53
7. Acronyms.....54
8. References.....56

Table of Figures

Figure 1: Bluetooth Network Topology.....14

Figure 2: Bluetooth Chip example.....15

Figure 3: Bluetooth Modes.....16

Figure 4: Bluetooth Applications.....18

Figure 5: Bluetooth Protocol Stack.....23

Figure 6: Interoperability with existing protocols and Applications.....27

Figure 7: Bluetooth Profiles.....32

Figure 8: Authentication Algorithm Working.....37

Figure 9: Categorization of Bluetooth Attacks.....39

Figure 10: Working of MAC Spoofing.....40

Figure 11: Working of PIN cracking attacks.....41

Figure 12: BlueSnarfing Attack.....43

Figure 13: Working of Man in the Middle Attack.....44

Table of Tables

Table 1. Comparison of Wireless Communication Technologies.....9
Table 2. Bluetooth History.....10
Table 3. Bluetooth Optional Features.....21
Table 4. Security Algorithms.....36
Table 5. Level of Threats.....48

O.

Audience

This report covers in-depth details of Bluetooth technology. It includes how Bluetooth came into working, its architecture, applications in the real world and most importantly the security. Power management is an important factor which determines the usage of Bluetooth in newer devices. Various version of Bluetooth has been discussed.

The reader is expected to have basic knowledge regarding communications mechanism and TCP/IP layers involved with them. A background of Computer Science/Information Technology/ Hardware engineer is desired but is not compulsory.

This report can be utilized by developers, system designers, technical author, students and hardware engineers.

1.

1. Introduction

Bluetooth is an always-on, short range radio technology that is present on a microchip. It is simply a wireless technology standard that is invented by Ericsson in 1994. The main usage of this technology is for exchanging data over short range using short – wavelength UHF radio waves. Bluetooth works by sending and receiving data over 2.4 GHz wireless link. As this communication works over short-range it not costly and works with low power consumption.

Every new technology nowadays consists of wireless capabilities, Bluetooth is large part of the wireless revolution. Bluetooth is being used a variety of products used by consumers on a daily basis. Some of these products are headphones, mobile phones, gaming devices. Bluetooth is perfectly suited for wirelessly transmitting small amounts of data and it serves as a perfect replacement for serial communication devices. Bluetooth is like a RF version of serial communications. Devices which are using Bluetooth communication need not be in visual lone of sight of each other however quasi optical wireless path must be viable. The IEEE standardized Bluetooth as IEE 802.15.1 but it does not maintain it anymore.

The Bluetooth specification give a protocol stack which is provided by a description of the hardware, software and an application framework for building interoperable applications called profile. This technology is provided free of licenses to the technology's adopter members. Bluetooth

Special Interest group (SIG) has large group of members (more than 30,000) who manage the qualification program and protect the trademarks. Any manufacturer who is going to make use of Bluetooth in its product needs to meet the standard which are given by SIG. A recent analysis shows that nearly 920 million units are shipped yearly which contain the Bluetooth integrated circuit.

This report will further talk about the specifics of Bluetooth which are as follows: Brief overview of the history of Bluetooth, Comparisons of different versions which were introduced over the years, The working and the architecture of hardware, Power Management mechanism, Techniques to handle security issues during the wireless transfer of data between two devices, Prevention of security attacks and Finally future works for the report.

2.

2. Understanding Bluetooth

2.1 Communication Techniques

Before diving deeper into Bluetooth, lets look at the various communication techniques which are alternatives to Bluetooth. Alternatives to Bluetooth exist that also for the exchange of data, audio and voice between two devices. Three alternatives to Bluetooth are list below.

Infrared Wireless

Hewlett-Packard developed this technology. This was the first technology which came under the PAN space called Infrared wireless. It was first introduced in early 1990s and is being used by some companies till date. Data can be transferred from laptops to printers and other short-range PANs. As compared to Bluetooth this technology works in a more limited range which is 10 feet. One of the other differences is that it requires a clear line of sight between the two devices communicating. One of the majorly used application of Infrared Wireless is microphones.

Ultra-Wideband

This wireless technology makes use of baseline pulses and sends data directly from the antenna of the device. These signals have advanced strength which makes it possible to pass through walls and other obstructions. It can be used to transfer large amounts of data at a speed greater than 100 megabits per second. Ultra-Wideband are being widely used by the government and the military.

Induction Wireless

This is another technology which uses magnetic induction as its core of data transmission technique. Magnetic Induction is one of the fields that comprise a radio signal and the other one is electric. The signal is delivered by a coiled transmitter to the other device. Advantages of Induction wireless is same as that of Bluetooth which I relatively cheaper way of data transfer with low power consumption. Induction wireless is more secure as compared to Bluetooth.

The table shown below compares some other wireless communications technologies on the basis of various parameters such as connection type, spectrum.

Feature & Function	Infrared	802.11 Wireless LANs	HomeRF	Bluetooth™
Connection Type	Infrared, narrow beam	Spread spectrum	Spread spectrum	Spread spectrum
Spectrum	Optical 850 nm	RF 2.4 GHz	RF 2.4 GHz	RF 2.4 GHz
Transmission Power	100mW	100mW	100mW	1mW
Data Rate	16Mbps	1Mbps, 2Mbps	1Mbps, 2Mbps	1Mbps
Range	1 meter	100 meters	Typical home	3 meters
Supported Devices	2		127	8
Voice Channels	1	VOIP	6	3
Addressing	32 bit physical ID	48 bit MAC	48 bit MAC	48 bit MAC

Table 1. Comparison of Wireless Communication Technologies

2.2 Bluetooth History

The Bluetooth Special Interest Group was formed by Ericson, IBM, Intel, Toshiba and Nokia in the year 1998 to provide a solution for communication over a short range. Before the standard was developed, Intel called its technology as Biz-RF, while Ericsson and Nokia used different terms. The name Bluetooth was borrowed from the 10th Century, second King of Denmark, King Harald Bluetooth. The idea behind it was that as the King was famous for uniting similarly Short-range wireless link is being made to unite the PC and cellular industries. The table shown below will briefly walk through the history of Bluetooth.

Year	Description
1998	SIG was formed with five companies and the technology was official named Bluetooth
1999	Bluetooth Specification Version 1.0 was released.
2000	First Mobile Phone with Bluetooth capacity appeared on the market.
2001	The first Printer with Bluetooth capabilities was invented. Also, Bluetooth was being integrated with electronic devices such as laptops and handsfree kits used in cars.
2002	IEEE approves the 802.15.1 specification to conform to Bluetooth Technology. Also, Bluetooth was integrated with digital cameras for capturing photos from a distance as well as sharing data from the camera to computers.
2003	Bluetooth Specification Version 1.2 was released. Music technology implemented Bluetooth in Mp3 devices. Also,

	certain Medical System made used of Wireless Tech for communication of data.
2004	Technology became much more widespread in 2004. Bluetooth Version 2.0 was released. Enhanced Data Rate Technology was added which boosted the data transfer to a maximum of 3 megabits per second (Mbit/s). Power Consumption also was seen to be nearly cut into half than the previous version.
2005	SIG membership hits 4000 companies. 5 million chipsets were being produced every week. Profile Testing Suite was Launched which could be used for testing and qualifications of tools.
2006	First Bluetooth sunglasses, Bluetooth watch, Bluetooth picture Frame. Bluetooth wireless was installed on 1 billion devices. Profile tuning suite testing becomes a mandatory part of the Bluetooth product qualification process. The SIG announced it will integrate Bluetooth technology with WiMedia Alliance version of UWB.
2007	Bluetooth version 2.1. This version included Secure Simple Pairing. This feature made the system pairing process simpler and more secure. Man in the middle attacks were made more difficult. First Bluetooth alarm-clock radio. First Bluetooth television. SIG membership hits 8000 companies.
2008	Profile Tuning Version 3.0 was released. It included automatic updates and improvements to report generation capabilities. SIG celebrated its 10th anniversary.
2009	Bluetooth 3.0 released with High speed data transfer. Data transfer speed reaching 24Mbut/s.

	SIG announced the adoption of Bluetooth Low Energy wireless technology.
2010	Bluetooth 4.0 released. It improved connectivity and range. It also included features such as Generic Attribute Profile (GATT) which is used to provide the profile of the device. Profile Tuning version 4.1 launched.
2011	Apple and Nordic Semiconductor join the SIG board of directors. Apple released first two computers with Bluetooth 4.0 technology. Microsoft windows 8 started supporting Bluetooth 4.0. The SIG adopted 29 new Bluetooth 4.0 profiles, services, protocols and prototyping specification, creating infrastructure for Bluetooth devices.
2012	Bluetooth technology was adapted in sports and fitness markets. New resources for app developers launched. The first Bluetooth low energy tablets were launched in the market.
2013	Bluetooth 4.1 was released with less changes in hardware, speed and range. New protocol introduced which enabled devices to connect indirectly through the cloud. It could now also coexist with LTE radios. Google announced support for Bluetooth low energy in android.
2014	Bluetooth 4.2 was introduced. It added features for IP connectivity, privacy and speed. Qualcomm joins the SIG board of Directors.
2015	Smart Mesh working group was founded. Also SIG shared its roadmap and upcoming enhancements for 2016. Two factor authentications was integrated.

2016	Bluetooth 5.0 released with new spec quadruples range and the speed is doubled also increases data broadcasting capacity by 800%.
2017	Bluetooth mesh networking capabilities were added to enable the usage of large-scale device networks. Google and Philips also joined the SIG board of directors. Launch studio was released to simplify the process of product qualification.
2018	Bluetooth celebrated 20 years of innovation. Major tech companies started supporting Bluetooth (Alibaba, Xiaomi).

Table 2. Bluetooth History

2.3 How does Bluetooth Work?

The protocol used by Bluetooth operates at 2.4GHz, similar to that of other wireless technologies such as ZigBee and Wi-Fi. Bluetooth model works on a master slave architecture. Bluetooth networks are also called as piconets. The master slave model basically means that one of the devices acts as the masters and control all the other devices connected to it. For Bluetooth a single master can have up to 7 slaves. One more thing to note is that each slave can only have one master. The master can request and send data to any of these slaves, slaves cannot communicate to other slaves. The below diagram shows how Bluetooth network is connected.

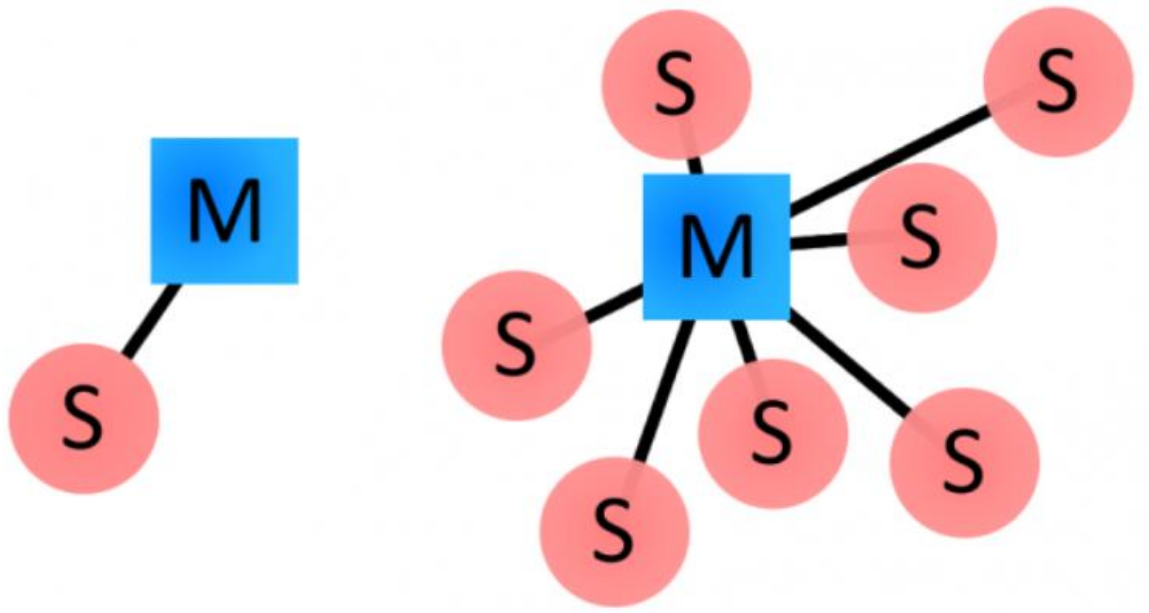


Figure 1. Bluetooth Network Topology

Multiple piconets can also be joined together to share information which is called as **scatter net**.

Bluetooth communication does not interfere with each other as there are 79 different frequencies which can be used. When two devices communicate a frequency is randomly chosen and if that's already being

used, they switch again. This technique is known as the **spread-spectrum frequency hopping**. Also, to minimize security risks these devices periodically change the channel they are communicating through. This technique also helps in decreasing the amount of interference.

Bluetooth Addresses and Names

A 48-bit unique Address is given to each Bluetooth device, this is in hexadecimal format. The manufacturer is identified by the most significant half. An example of such diagram is shown in the image below.

Figure 2. Bluetooth Chip example

Bluetooth devices can have user-friendly names which can be used to identify users. These are used in place of addresses usually.

Connection Process

The following steps are followed when two devices are connecting with each other.

- **Discovery**: If the two devices haven't already connected once before, on must run the discover Bluetooth devices around function. One of the devices will then send a connection request to the other with its address and the second device responds with its address.

- **Paging**: It is the process of forming a connection between the two devices. Before this process can be initiated it is important for the devices to know the address of each other.
- **Connection**: After the paging process, the devices are now connected. To save power the devices can be put to power saving mode when they are not actively transmitting. The devices can be in the following modes:
    - Active Mode: Actively transmitting mode
    - Sniff Mode: Power saving mode, sleep and listen for transmissions only.
    - Hold Mode: Hold is temporary mode where a master can command a slave device to hold.
    - Park Mode: This is deeper version of the sleep mode. A master can command the slave to sleep and be inactive until the master requires it to be active.

The process of pairing also involves an authentication process where the one of the devices displays a security code which the other device has to enter in its system. This process was followed on older legacy devices.

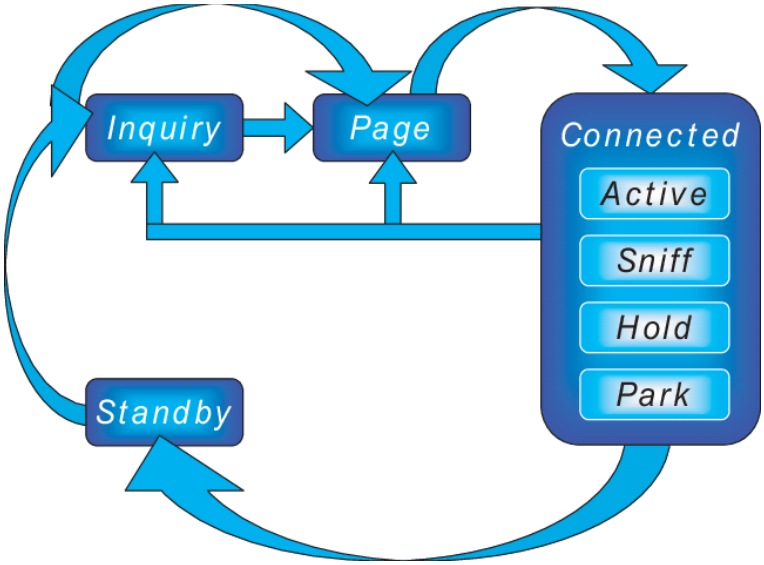


Figure 3. Bluetooth Modes

2.4 Bluetooth Applications

Bluetooth Usage Models

Basically, a usage model is a set of protocols that implement a particular Bluetooth based application. A large number of usage models are defined in the documents which talk about Bluetooth profiles. Every profile consists of certain features which these applications can make use of. Some of the highly used usage models are listed below.

File Transfer: This model supports transferring of documents, files, images, audio files, video files. It also gives the ability to browse a files on a remote device.

Internet Bridge: This model can be used for providing dial up connections and faxing capabilities (Operates over RFCOMM) when a PC is connected to a mobile phone or a modem wirelessly. Protocol stacks such as RFCOMM and PPP are used for data transfer.

LAN Access: Similar to accessing LAN of a Wi-Fi connection or an ethernet connection, Bluetooth network (Piconet) can be used to setup a Lan. One thing to note here is that the devices connected need to be closer to each other.

Synchronization: This model can be used to synchronize data between two devices. For example, when moving data from and older device to a newer device data such as contacts, messages, calendar can be synced. IrMC is and IrDA protocol that provides client/serve capability for transferring updated PIM information.

Three in one phone: This model was used in older phone systems where the wireless handset is connected to a base station as well as other

intercom can be connected to this base station which in turn can connected two callers using 3 phones.

Headset: Bluetooth helps in connecting a headset with a device to listen to audio. Many newer headsets now allow connection to multiple devise at the same time.

Cordless Desktop: Devices such as mouse, keyboard, speakers, printers, joysticks, cameras etc can be connected to personal computers.

Upcoming Devices: IBM is researching on devices which can use for data projections. Basically, these devices can project data which they receive using Bluetooth transmission from phones. This device when released would have many applications for example: Educational purposes, 3D holographic projections.

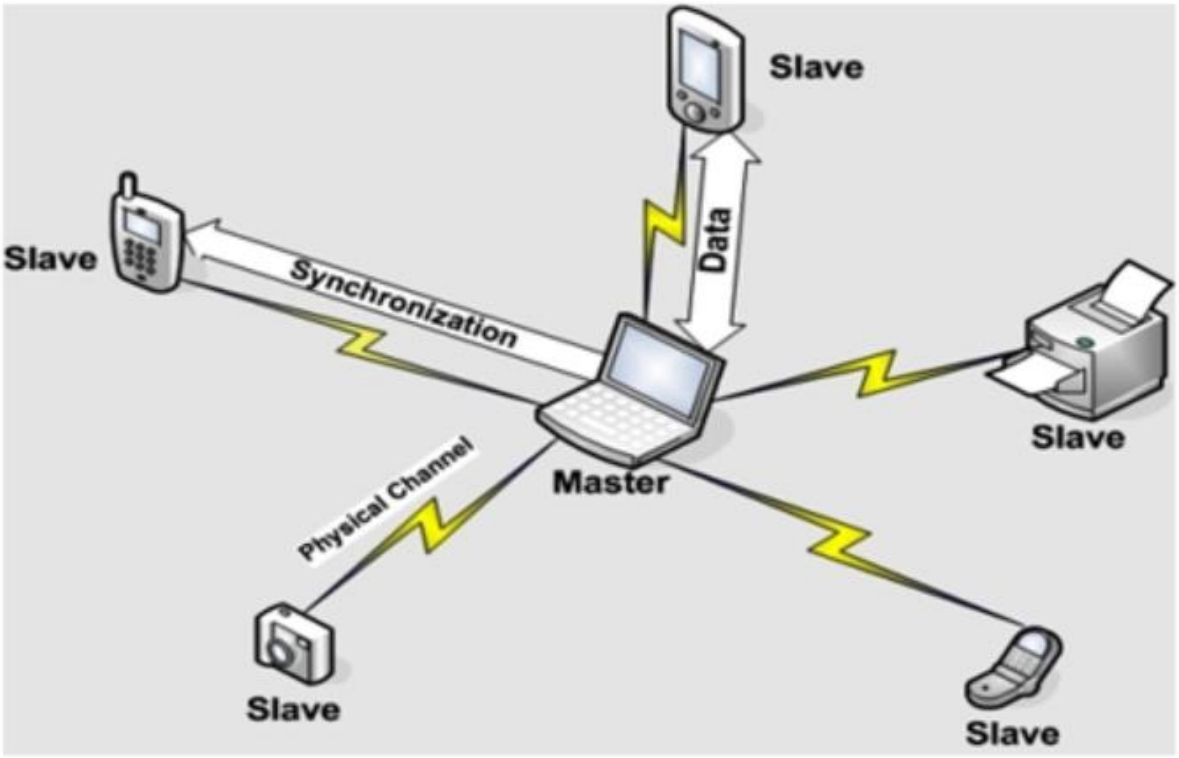


Figure 4. Bluetooth Applications

2.5 Bluetooth Versions

This section will provide with a brief description of various Bluetooth versions and their features.

Bluetooth 1.x

This version focused mainly on the transfer of data rather than newer functionality. This version was the beginning of Bluetooth and it had speeds of up to 1mbps also the pairing process between the two devices was very complicated. Because of these reasons this version was not really implement on devices which were being used by consumers.

Bluetooth 2.x

This version of Bluetooth was used on a large scale in the older mobile phones and technology as it provided faster data transfer rates. The data rates reached the peak which 3mbps. Also as compared to the version 1 the pairing process was made simpler. Bluetooth 2.0 made use of DQPSK and 8DPSK in place of Gaussian Frequency Shift Keying which used frequency modulation to send data. This was the main reason of increased data transfer speeds

Bluetooth 3.x

This version of Bluetooth further increased data transfer speeds using the optional High-Speed feature. The high-speed feature is basically the addition of 802.11 for up to 24 Mbps of data transfer. The connections became highly 802.11 for up to 24 Mbps of data transfer. The connections became highly reliable which then opened up the possibilities of using this technology in various other communication mediums. One of the drawbacks of the version 3.0 was that it consumed more power than the

other version. This could've been because of the its high-speed data transfer nature.

Bluetooth 4.x

One of the drawbacks that was seen in Bluetooth 3.0 was regarding power consumption. Bluetooth 4.0 introduced low energy feature (BLE). It was mainly bought so that devices such as sensors which are used for IoT devices could work on low power. When BLE is enabled it used the Bluetooth 2.0 data transmission technique which is called the Gaussian Frequency Shift Keying. Basically, smaller devices which did not require data transmission at all time could make use of this feature to be active for a longer time as and when required. Devices such as Wearable smartwatches, heart rate monitors, mobile phones and smart headphones.

Bluetooth 5.x

This is most recent version of Bluetooth which is being highly adapted in many electronic devices. It has made many improvements on the previously introduced BLE feature. Bluetooth 5.0 offers a variety of data transfer rates which are: 2Mbps, 1Mbps, 500kbps, 125kbps. To improve the range of Bluetooth 125kbps was added as increase in transmission range would require lowering of data rate. Bluetooth 5.0 can be used in medical sensors which occasionally transfer data over long ranges. Bluetooth 4.2 LE had half the bandwidth of Bluetooth 5.0. It increases the range over 4 times. Also, as previous Bluetooth networks had some problems when multiple devices are connected nearby, this version introduced a new feature to tackle the same. Slot Availability Masking can detect and prevent interference on neighbouring band which are being currently used. Many newer electronic devices can now cast music to multiple speakers at the same time from one device.

Optional Feature with Bluetooth

Bluetooth Versions	Optional Features				
	Basic Rate (BR)	**Enhanced Data Rate (EDR)**	**High Speed (HS)**	**Low Energy (LE)**	**Slot Availability Masking (SAM)**
Bluetooth 1.x	Yes	No	No	No	No
Bluetooth 2.x	Yes	Yes	No	No	No
Bluetooth 3.x	Yes	Yes	Yes	No	No
Bluetooth 4.x	Yes	Yes	Yes	Yes	No
Bluetooth 5.x	Yes	Yes	Yes	Yes	Yes

Table 3. Bluetooth Optional Features

3.

3. Bluetooth Architecture & H/W

3.1 Specification

The Bluetooth specification is basically used by manufacturers and creators who implement Bluetooth in their products. It describes how Bluetooth devices would group themselves for communication process. The specification includes radio frequency, link later and application layer definitions for the product developers of data, voice and content – centric applications. The documents contain details that help devices support wireless technology using which they can communicated with each other worldwide.

The specification document is mainly divided into two parts:

1. **Core Specification**: This defines the base of the technology.
2. **Profile Definitions**: This defines the usage of base technology towards a specific category application. For example: Audio transmission.

The specifications are very lengthy and as there are lot of topics that are covered, at the highest level the specification is split into two volumes. Where volume 1.2 is again split into multiple sub volumes. Volume 1 also describes the protocol stack and covers other topics such as testing and qualification.

In the next section Bluetooth Protocol Stack will be covered in detail.

3.2 Bluetooth Protocol Stack

Bluetooth is defined as a layer protocol architecture. Figure 4 shows how the protocol stack looks for Bluetooth. There are some protocols which are mandatory such as LMP, L2CAP and SDP. Basically, devices which tend to communicate with other Bluetooth devise can use these protocols for data transport.

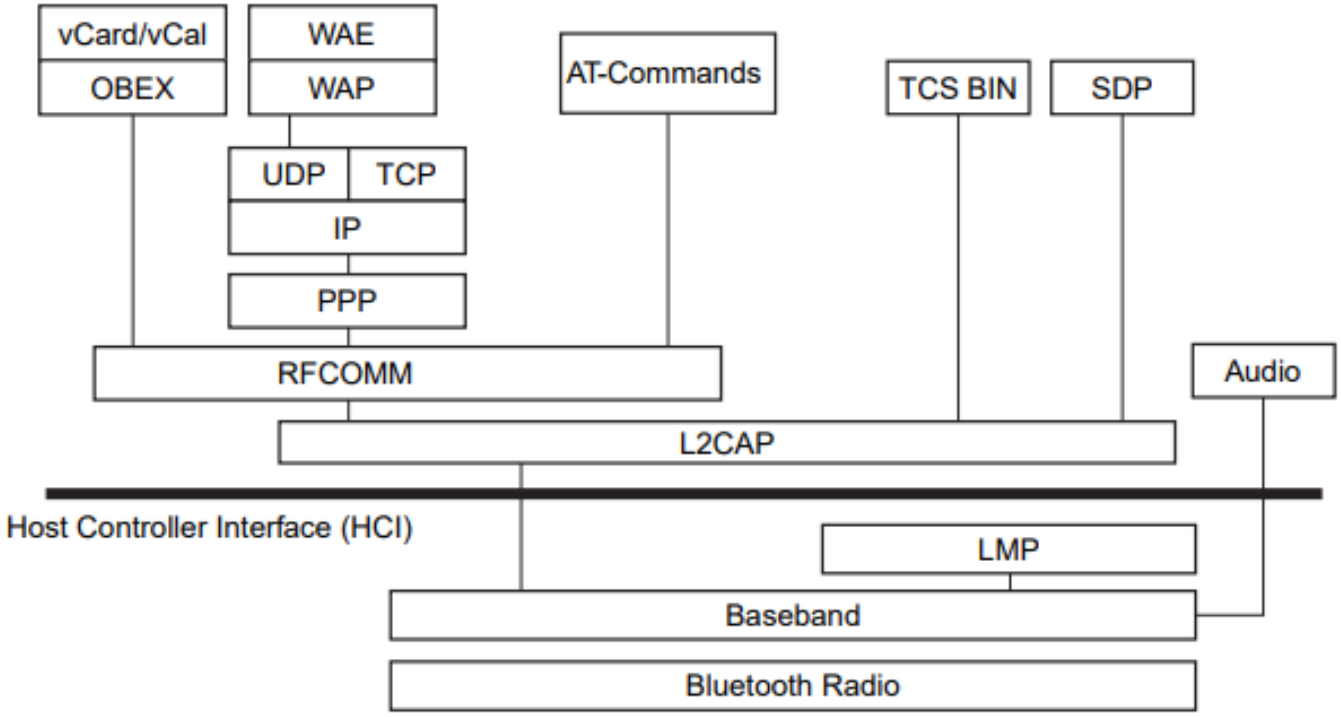


Figure 5. Bluetooth Protocol Stack

The Bluetooth specification divides the Bluetooth protocol stack into three logical groups.

1. The Transport Protocol Group
2. The Middleware Protocol Group
3. The Application Group

1. Transport Protocol Group

The protocols present in this group as designed to do the following functions:

These protocols allow devices to locate and connect to each other. The upper stack layers consist of profile specifications which focus on communication between two devices and how that is going to be built using the core technology. Different applications have various usages so for each application different traffic can be given distinct priorities. For example, for headphones carry audio and data traffic where audio traffic has higher priority. Communications are supported where transmission can be synchronous or asynchronous, this is specially for telephony grade voice communication. Management of the logical and the physical links is done so that the layers which are above it can easily be handled by the lower layers. The protocol which are contained in the Transport protocol group are listed below:

Logical Link Control and Adaptation Protocol Layer (L2CAP)

- This layer is present above the HCI layer. Its major function is to handle the communicating between the lower layers and upper layers of the protocol stack.
- It basically would keep a track of where the packets have arrived from and where the packets are needed to be sent. Because of this crucial feature it is a required layer in all the Bluetooth systems.
- One of the other features is that it also shields and hide the details of lower layers from the upper layers.
- It enables the upkeep of desired grade service in two peer devices.

- The lower layers are able to handle the packets easily as this layer will segment larger packets which travel from the upper layer to the lower layers into smaller packets. Smaller packets will have faster transmission.

Link Manager Layer (LML)

- The commands which are received from the Host Controller Interface from the upper stack are translated by this layer. The establishment and management of this link is also maintained by the LML.
- A part of power management is handled by the LML and it maintains fairness between multiple slaves in a piconet. The connection between each one of these devices are looked after by the LML. While maintaining the power management LML can request adjustments in the power level according to the requirements.
- In simple words the main idea of LML is to negotiate properties of Bluetooth between the communicating devices. Some of these properties can be support service for a reason, the allocation of bandwidth, verification of tokens transferred between the devices.
- After every pairing is completed between two or more devices this layer will then store the authentication key specific to the device which were connected.

Baseband and Radio Layers

- Before the transfer of data for transmission to and from the radio, baseband will format the data and then they will be transmitted.

- It basically controls the timing of the packets as well as the framing. The flow of these packets is again operated by the baseband.
- When two devices have to be connected the scanning of available devices in the nearby area is handled by the baseband.
- After the connection takes places then it will assign which devices act as the slave and which devices act as the master which is going to be commanding device.
- One of the crucial features of the baseband is controlling the synchronization and the transmission frequency hopping sequence of the Bluetooth device.
- Baseband also performs recognition of the packet types which are supported for synchronous and asynchronous traffic, with this management of the link between devices is performed.

Host Control Interface (HCI)

- HCI is basically an interface which is provided to control the user interaction is simpler way rather than providing the user with the minute details of the Bluetooth working.
- Having a single interface would help all the other upper layers such as applications, baseband, link manager etc to have a only one single standard way of communication which helps in maintaining consistency and also makes the flow of command simpler.
- The purpose of interoperability between the devices and the host module is served by the HCI.
- Using the commands provided by the HCI, the Bluetooth connection can enter various states which are provided. All the events which occur between these connected devices are informed to the upper layers through the HCI.

2. Middleware Protocol Group

The applications already present or the existing applications would need some way for them to communicate with other devices over Bluetooth technology. To fulfil this particular requirement this group contains layers which make it simpler for the existing application to communicate over Bluetooth. The protocol that are present in this group can be developed by the Third-party developers or specifically developed by the Simple Interest group. Third-party developers can developers can make use of this group to generate layers which work according to their products requirement.

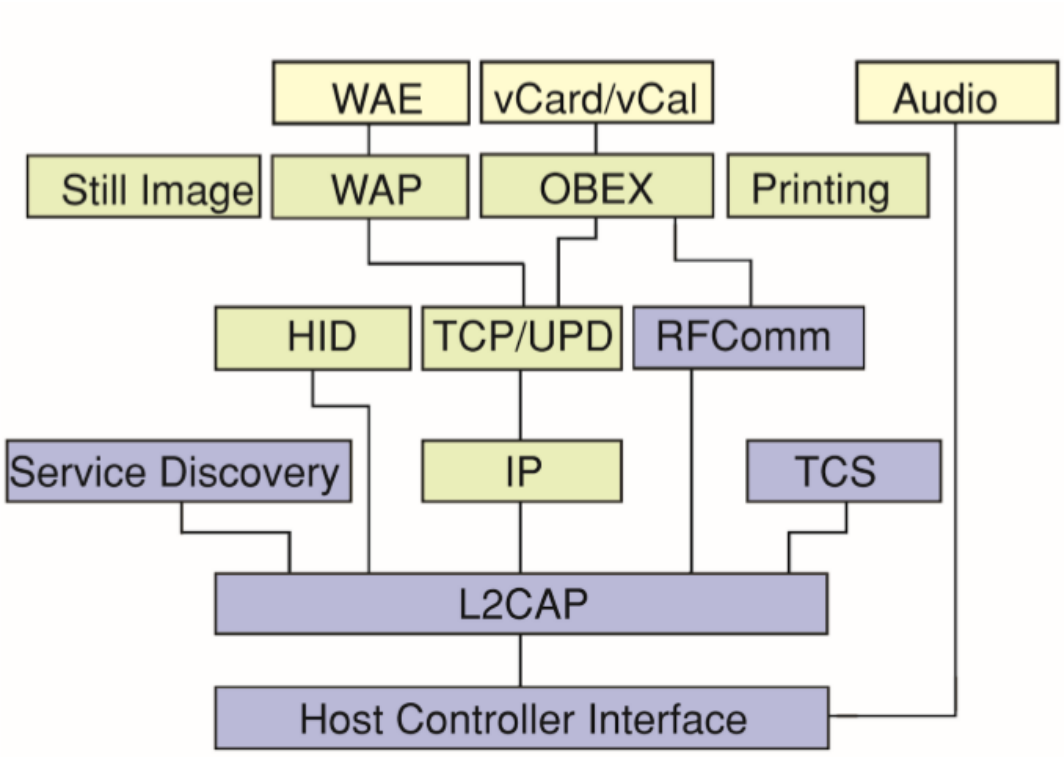


Figure 6. Interoperability with existing protocols and Applications

The layers which are present in this group are explained below:

RFCOMM Layer

- One of the most common way of communication interface is using serial ports. The RFCOMM layer provides an emulation of serial ports over L2CAP.
- It supports communication between the services of the upper layer using serial interfaces as transport mechanisms. One of the differentiating features it provides is that multiple devices can connect to a single device at the same time. This feature is used on a large scale by many newer versions of headphones released on the market.
- As RFCOMM will be used for the communication use of wire between these layers would be redundant hence this also eliminates the usage of cables.
- Some of the application which can utilize the serial port are dial up networking where Personal computers can be connected to the Internet using Dial up connection.

Service Discovery Protocol Layer (SDP)

- The services provided by a device would change when the device is moving. So, application need to know which services are currently available and function on the basis of that. SDP provides applications the capability to query the services and the characteristics which are being offered.
- SDP is built on top of L2CAP. It is different than many networks-based environments as in Bluetooth the devices are first found after scanning after which the services are queries which is different than

what happens in wires LAN connection. In Lan Connection we connect to a network and then find the available devices.

Infrared Data Association interoperability protocols (IrDA)

- Different types of data are needed to be communicated or transferred over the network. For example, files which are audio, video, graphic, documents etc.
- To make this possible the Simple Interest Group (SIG) has adopted certain Infrared Data association interoperability protocols which enables applications to exchange a wide variety of data.

Object Exchange Protocol (OBEX)

- OBEX is developed by the IrDA to exchange objects in a simple and spontaneous manner.
- OBEX is built on top of RFCOMM.
- OBEX is based on the client server architecture.
- It does not have to be dependent on the transport mechanism and transport 'Application programming Interface (API), but this only possible if it reaches a dependable transport base.
- To make browsing of contents of folder which are present on a remote device, OBEX would create a folder listing object which helps in traversing the contents of the folder.

Networking Layers

- The Bluetooth system is based on the architecture where multiple devices connect and form a network to exchange information. This topology is called peer to peer networking. For these devices to connect and transmit a standard packet would have to be created to encapsulate network layer protocols
- The AT commands are used by the Dial-up networking technology.
- Networks which are accessed by devices are in the most cases are IP networks which are based on standard protocols such as TCP, UDP, HTTP etc.
- It will be possible for a device to connected to an IP network using network access point. To connect an access point internet PPP can be used.
- The packets from various networking protocols are encapsulated by the Bluetooth network encapsulation protocol and will then be transported over L2CAP.

Telephone Control Specification Layer and Audio (TCS)

- This layer helps in the establishment of voice and data calls between Bluetooth devices by defining the call control signalling between the two devices. One more thing to note is that this layer is built on top of L2CAP.
- As it controls the signalling between the devices it supports functions such as management of a group and controlling of the call. It is mainly used to set up data calls.
- The protocol of Telephone Control specification layer and Audio layer are compatible with the specifications of ITU.

- The audio communication using Bluetooth can make use of two encoding schemes: 8-but logarithmic PCM or continuous variable slope delta modulation.
- Typically, the audio communication over Bluetooth is taken place at a rate of 64Kbps.

3. Application Group

- Application are simply software applications which use the Bluetooth technology for their communication purposes. They are built on top of all the above-mentioned protocol stack layers.
- These applications make use of Bluetooth links and refers to software that exists above protocol stack.
- Any kinds of APIs or any other application protocols are not defined by the Bluetooth Simple Interest Group.
- To establish a base point for the use of a protocol stack to accomplish a given usage case Bluetooth profiles can be used. We will go deeper into understanding Bluetooth profiles in the next section.

L2CAP, OBEX, SDP, RFCOMM are the layers of the Bluetooth protocol stack that represent the protocol which are addressed by Java APIs for Bluetooth wireless technology (JABWT). The Bluetooth SIG is defining newer protocol which will be built on top of the layers we discuss above. If we notice, L2CAP is supporting most of the newer protocols. Some of the newer protocols which are being integrated with the Bluetooth technology are: Video Distribution Transport Protocol (This will also support audio), Video Control Protocol (This will again also support audio), Hardcopy control channel and Hardcopy notification channel.

3.3 Bluetooth Protocol Profiles

Now to use the Bluetooth Protocol stacks towards the building of an application a certain set of steps are needed to be followed. To deal with different kinds of applications a variety of profiles have been established.

Some of the examples of such profiles are: A FAX machine can implement the FAX profile while at the same time a Headphone device can make use of the Headphone Profile. By following these set of steps, a manufacturer can accomplish the specific requirements of the Bluetooth device they are creating. The Diagram below shows the different types of profiles.

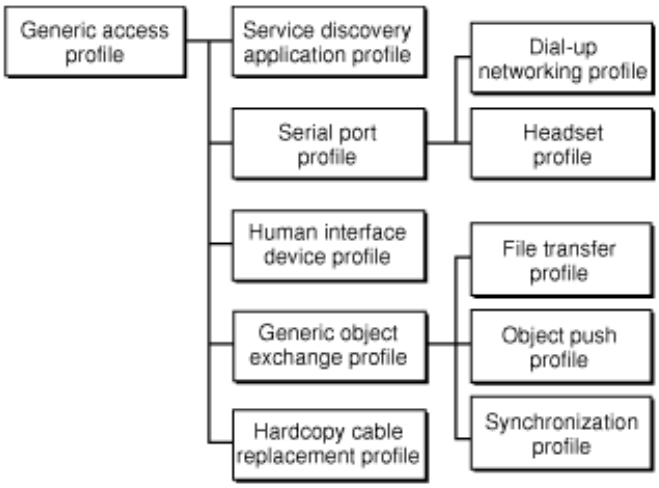


Figure 7. Bluetooth Profiles

It is possible that two profiles use a different set of protocol layers withing the stack and then also different set of features within the same protocol layer, therefore the dependency of the profiles on features and protocol layers will differ. Each Bluetooth profile contains information on the following main topics:

- Dependencies on other protocols
- Suggested user interface formats

- The parts of the Bluetooth protocol stack that are used by the profile.

The four basic profiles that are base for all other profiles are: Generic Access profile (GAP), the Serial Port Profile (SPP), the Service Discovery Application Profile (SDAP) and the Generic Object Exchange Profile (GOEP).

Generic Access Profile (GAP)

It defines a consistent means to create a baseband link between the two communicating devices. Some of the features of GAP are:

- The type of features which needs to implement in all Bluetooth devices
- The general process which is used to scan and connect two devices.
- A user – Interface for easier handling of the devices.

As all the other profiles are built on GAP this will enable different application to be able to communicate with each other as the standard is the same and the basic features are common. Also creating newer profiles is easier if a base is already created. So basically, GAP defines the general procedure between two devices which includes management of the link between the two, Configuration and setup for the connection and the process related to different levels of security measures.

Service Discovery Application Profile

This profile basically describes what process the application needs to follow to discover a remote device and connect to any available device in the surroundings. It also enables for services to be discovered on the Bluetooth devices it is connected to. For example, if the mobile device supports surround sound etc. Also, this profile helps in satisfying the rule which is given by GAP which says any Bluetooth device should be able to connect to any other Bluetooth device.

Serial Port Profile

This is simply the RS-232 serial – cable alternative for devices that use Bluetooth for communication. This also benefits legacy applications which enable them to work just like they would with a SPP port without any particular modifications. To provide with this emulation serial port profile uses the RFCOMM protocol. SPP directly maps the requirements from RFCOMM to support the required applications.

General Object Exchange Profile

All the client and server roles are defined by this profile. It also works as a base and helps other profiles using the OBEX protocol to map things according to a predefined standard. The general object exchange profile stipulates that the client should initiate all the transactions that take place, this is just like the process which is following with other OBEX transactions. But one of things to know while using this profile is that it does not define the how actually should applications define objects that are to be exchanged, so basically if any application does use this profile then it totally depends on the applications on how it will define the objects. Some of the fields are profile, object push, synchronization profiles and file transfer.

4.

4. Security

4.1 Bluetooth Security

Security has always played a major role in any kind of device. Although the Bluetooth SIG has put many types of efforts into making Bluetooth a secured technology still much of the security still depends on application to application because every device can utilize the different features provided by Bluetooth. Now some of the features are using different kinds of connection modes, these connections modes are shown below:

- **Private**
  The device cannot be found when in this mode, basically it won't be visible to other devices. It can be connected to another device only if the other device uses the Bluetooth address to connect. The Bluetooth address is unique and consists of 48-bits.
- **Public**
  In this state the device can be found by other devices as its discovery has been set to visible. After finding the other device it can be easily connected to.
- **Silent**
  Devices in this state will just monitor the traffic but will not accept any incoming connections at all.

Similar to the different modes provided for discoverability, there are mainly four different modes for security as shown below:

- **Non-secure**

  No kinds of security measures are taken this mode. This mode is very rarely used because even for transmissions which are smaller in size are usually covered by security measures.

- **Service-Level enforced security mode**

  The Bluetooth who are connected to each other can maintain a not secure Access Control List (ACL) which would help in determining which each device has access to. These security measures will only be only be started only after both the devices are connected. These connected devices can be on a L2CAP connection oriented or a L2CAP connection-less channel.

- **Link-Level enforced security mode**

  In this mode although the security measures are same as service level enforced security mode, but the difference is in the part of when these measures are taken. So here the security measures are taken when an ACL link is established and before any channel request is made.

- **Service-Level enforced security mode (SSP)**

  This mode provides measures similar to the mode 2 the only difference here is that Bluetooth devices which use secure simple pairing can use this mode. SSP is required by Bluetooth v2.1. Although legacy devices can use previous versions.

Security Mechanism	Legacy	Secure Simple Pairing	Secure Connections
Encryption	E0	E0	AES-CCM
Authentication	SAFER+	SAFER+	HMAC-SHA256
Key Generation	SAFER+	P-192 ECDH HMAC-SHA-256	P-256 ECDH HMAC-SHA-256

Table 4. Security Algorithms

There are various ways to handle the process of security in Bluetooth devices. There mainly 3 main steps which are included in this process. These steps are shown below:

- **Authentication**

  In this step the device which is trying to connect to a piconet or to other devices needs to provide its identity. The main gist of authenticating a device is to determine the client's authorization level. Authentication can be done when the sender will encrypt the Bluetooth device address of the receiver using the link key and random number which then it sends to the receiver and the connection will only be established if the two link keys are equal. The generated signal is the SRES. The working of Bluetooth authentication algorithm is shown in the figure below.

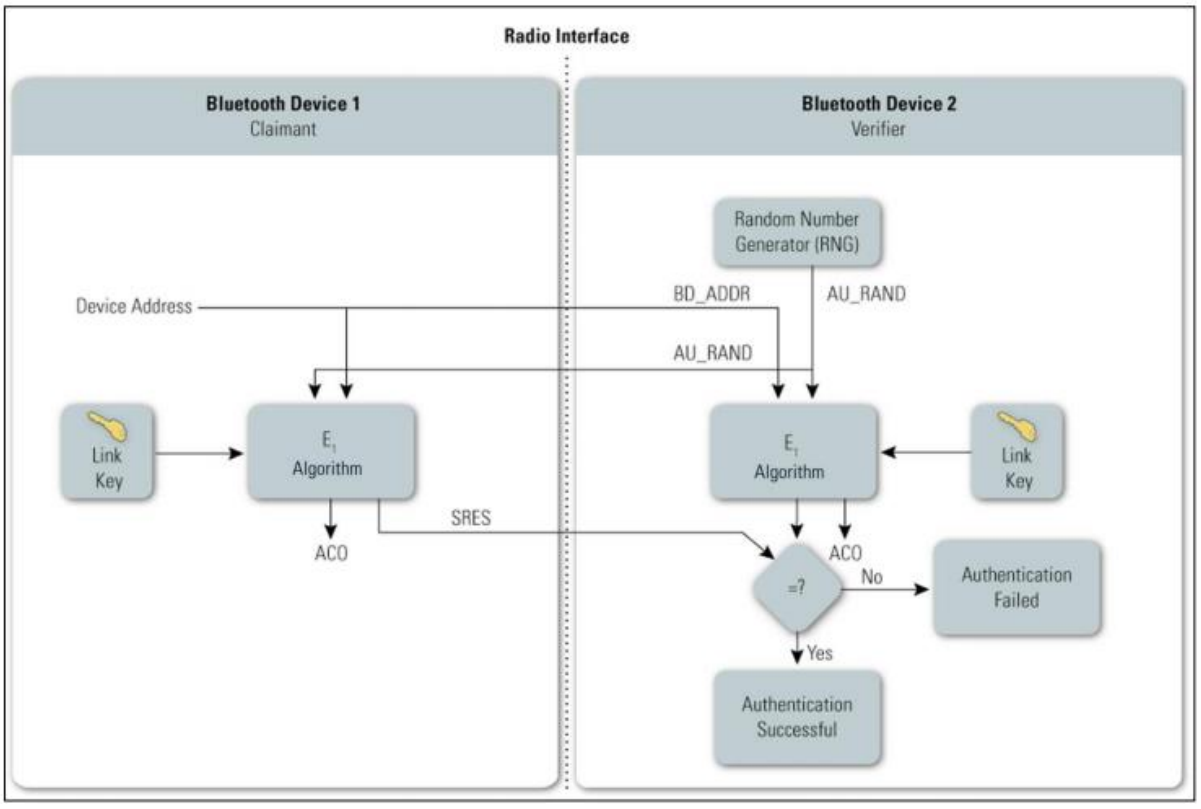


Figure 8. Authentication Algorithm Working

- **Authorization**

  Only devices which have been authenticated are allowed the access the services of the device they are trying to connect to. If the authentication fails, then authorization will not be provided. This layer is completely dependent on the Authentication. If the process used for authentication is not reliable then faulty devices will be authorized to access the services of the network.

- **Optional Encryption**

  To complicate the possibilities of attacker accessing the data optional encryption comes into the picture. If the data which is being transferred itself is encoded that would make eavesdropping a fail as the eavesdropper would not be able to decode its contents. The encryption key used can vary between 8 and 128 bits. The size of the encryption key is usually set by the manufacturer of the device itself. Enabling optional encryption would give two level of security – Connection using pin codes, Encryption of data being transferred.

4.2 Bluetooth Attacks

There are various kinds of attacks that are currently possible on devices which are using Bluetooth for transmission and different upcoming updates may have certain vulnerabilities which may create possibilities of carious other attacks. In General, the Bluetooth Attacks are categorized as shown the figure below.

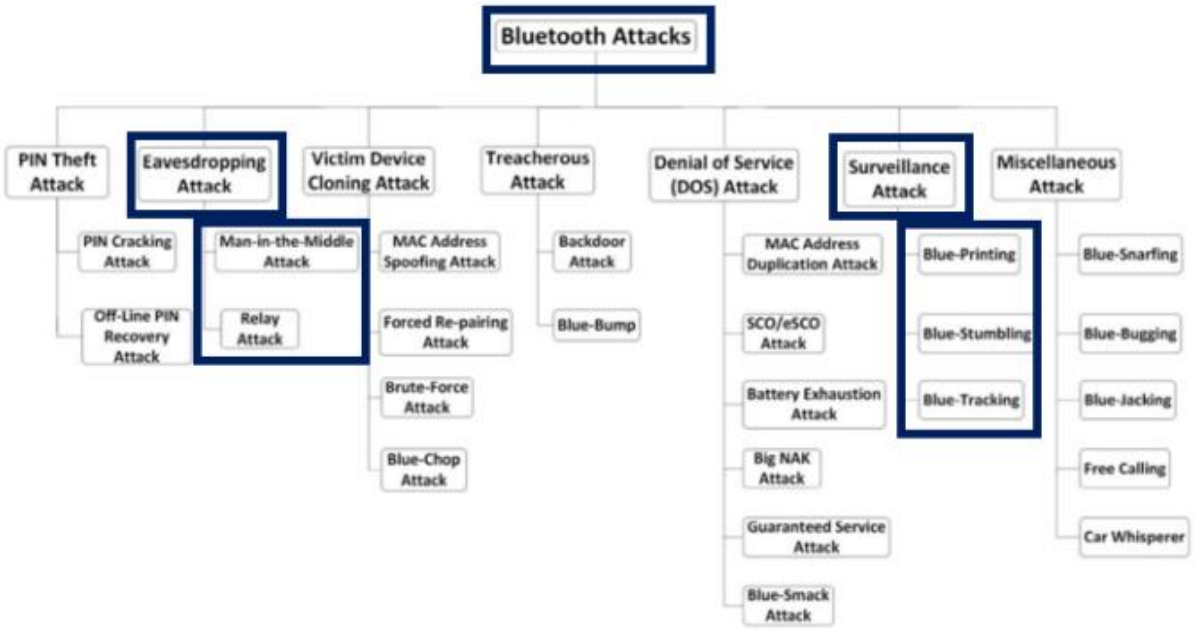


Figure 9. Categorization of Bluetooth Attacks

1. MAC Spoofing Attack

This type of attack is most frequently used to intercept Bluetooth connections. Attackers usually perform this attack during the generation of the link keys and when the piconets are being formed. If the attach is successful before the pairing takes places, then the attacker will have access to all the data that has been transmitted. Attackers can easily use hardware which are specialized for these attacks can capture and

manipulate data at the same time they get the option to terminate the ongoing connection. These issues can have adverse effects on many applications where Bluetooth is being used. SIG advices starting the pairing process in private mode or using long, random PIN numbers.

Figure 8 shows how MAC spoofing works.

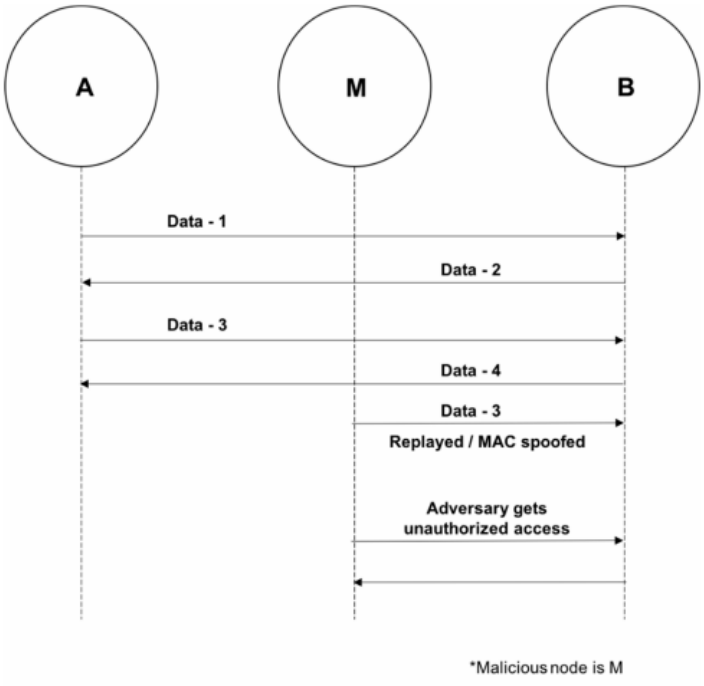


Figure 10. Working of MAC Spoofing

2. PIN Cracking Attacks

In these types of attacks, the attackers can use sniffers which are in simple words devices which analyse the protocol. Using these sniffers attackers can get access to the keys which are used during the pairing process. Although after getting access to the PIN, they would have to try different permutations and enter those into the algorithm to test. But after this process is carried out then they could hypothesize and test all the possibilities of the shared session link. If the right pin is acquired in the timely manner using the right equipment, then this process could be

carried out really easily. The solution for this attack would be to use a combination of private and public keys. The whole process can also be called as brute – force process. Figure 9. Shows the algorithm of this attack.

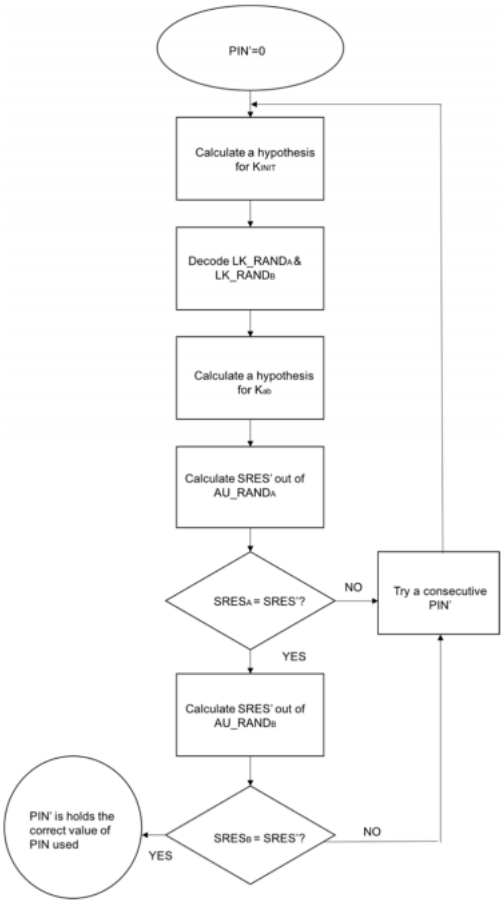


Figure 11. Working of PIN cracking attacks

3. Bluejacking Attack

Bluejacking is a kind of spam related attack. Basically, if any device is discoverable then other devices would be able to send requests to this device. Although the messages which are sent are unsolicited, but they can bother other people and repetitive messages can be annoying for the user. This attack was mainly used for promotional purposes. The best way to deal with such attacks is keeping your Bluetooth device in a non-discoverable mode so that no other device can send requests to it. This attack could open doors to various other types of attacks.

4. BlueBugging Attack

This is a very serious kind of attack where in an attacker would connect to the target device without the owner knowing about it. If the attacks also has access to the AT commands then it can be used for many purposes such as: Sending text messages to premium number (which basically gives the premium number money out of our mobile balance), attacker can also initiate phone calls, phone forwards which can cause harm to user in n number of ways. Getting the data from the gallery of the phone is another major crime that is possible.

5. BlueBump Attack

This attack takes the advantage during the time when the link keys handling is not strong. Basically, when the attack takes place a business card is sent by the attacker to the user. The user is forced to accept the card and then an authenticated connection is made. After the connection is made the user will be able to disconnect using the link key but the attacker could reconnect to this device later without authenticating again and by easily requesting new link key generation. (This is also feature used by earphones to automatically connect once they are started and previously paired)

6. BlueSnarfing Attack

This is a typical attack which is performed by experienced attackers. Here the attackers would hack the mobile device to steal all the available data on the device such as: Gallery images, Contacts, important files. The attack is performed on the OBEX protocol files. Also, once the attacker has access it can initiate Bluetooth connection and disconnect whenever required. Although previously when this attack was really common, companies like Nokia and Sony made improvements which made new

phones coming to the market less susceptible to these attacks. These attacks again can be minimized if the devices are kept in private mode. The working of this attack is show in Figure 10.

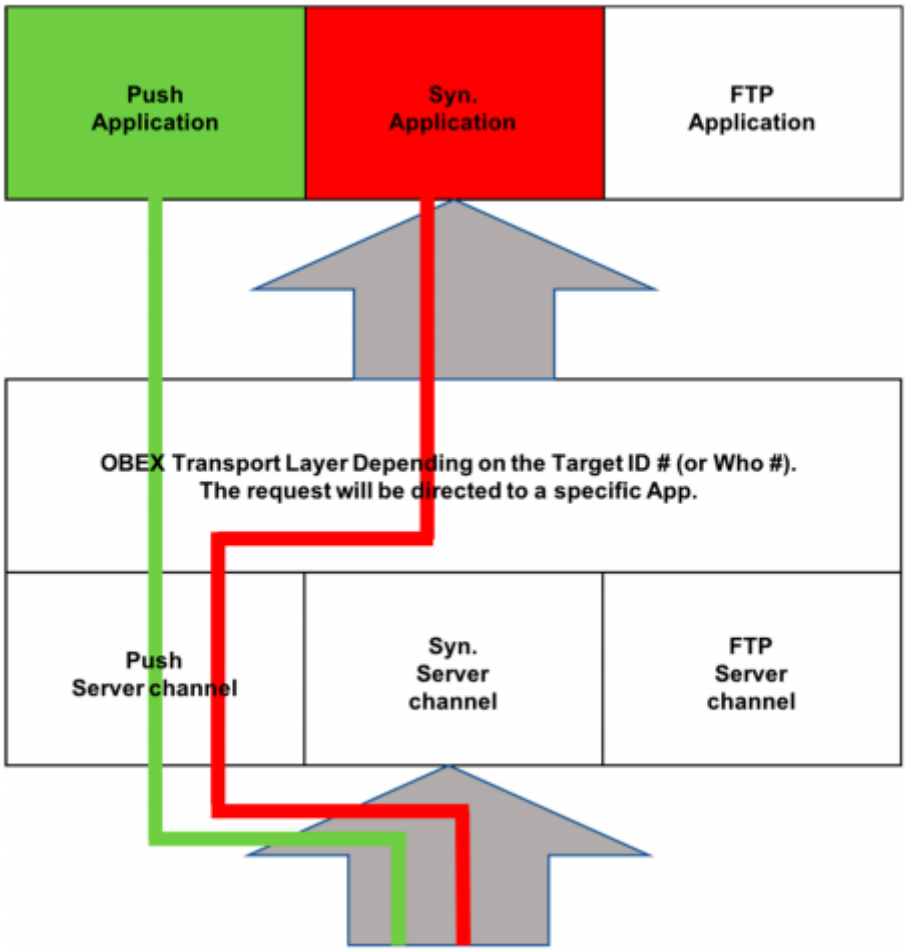


Figure 12. BlueSnarfing Attack

7. Man in the Middle Attack

These kinds of attacks occur when the pairing process between two devices is taking place. In this attack the middle person sends random messages to the two devices. This enables authentication without the shared secret keys. After the attack is conducted the two devices would think that they are connected to each other, but the reality is both the devices are connected to the attacker. The solution to this attack would be involvement of more piconet specific information into the pairing process.

Also, other than this, time stamps and nested mutual authentication can be used to determine if the responses received are from the actual device or if there is an attacker present in this transmission. Also, the use of private and public keys to identify the user can be implemented here. If the data which is being transmitted is encrypted before the transmission and only the receiver can decrypt the message using the private key already shared between the two devices would add another layer of protection. Figure 11 shows the working of Man-in-the-Middle Attack.

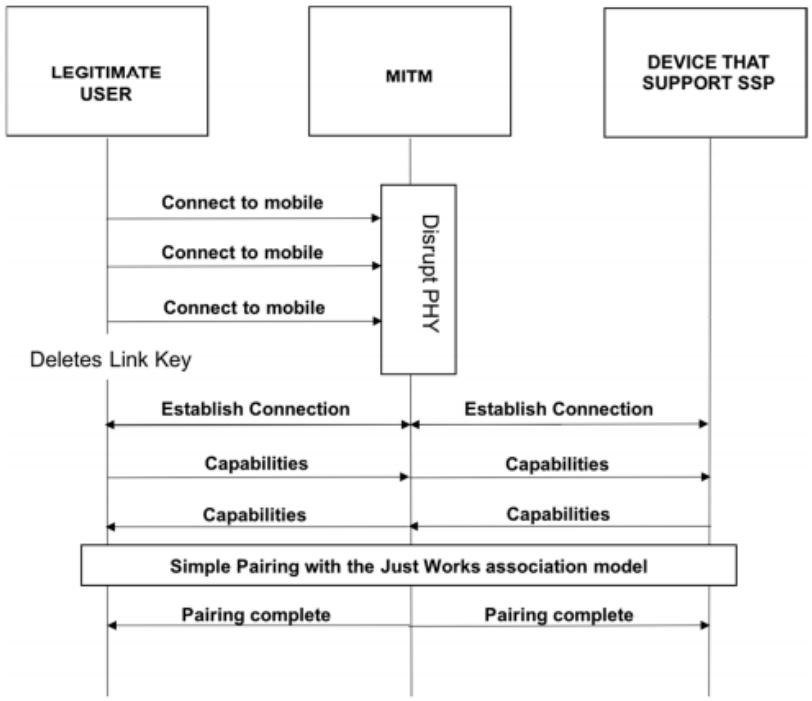


Figure 13. Working of Man in the Middle Attack

8. Denial of Service Attack

In the Denial of Service attacks the attacker would target the Physical layer of the protocol stack or the layers above the physical layer. The attack can be carried out by multiple attackers or even a single attacker. The way it works is that an attacker would overwhelm the server it is attacking with unlimited continuous requests which would make the servers respond late to legit request. This can cost applications and business a huge amount of loss. Restricting access to a network at a crucial time can also have adverse

effects. Some of the types of DDoS (Distributed Denial of Service) are BD_ADDR duplication, BlueSmack, BlueChop, L2CAP guaranteed service, battery exhaustion and Big NAK (Negative Acknowledgement). At the physical layer a jammer can jam the piconet entirely or capture the channel from the legitimate Piconet device.

9. Backdoor Attack

In this attack the intruder would have to previously be connected to the target device at least once for it to work. Also, the critical need for the attack to work is that the attacker needs to have BD_ADDR of the target device for it to connect again. After the registration process takes place, the attacker would be connected to the target device without the notice of the owner of the device and can get access to all of the data of the device. Not only the data but access to the location of the device as well as other services is possible. The attacker will be able to access all these resources without the notice of the user until the user actually checks in its device if it connected to another device. The device which is being targeted also needs to be vulnerable to this attack for it to work. BD_ADDR should be known as if the device is in a private or a hidden mode then the attacker can connect to it again using this address.

10. BluePrinting Attack

The main aim for carrying out this attack is to know if the Bluetooth Vulnerability that has come into picture is related to which devices so that the attacker can make use of this knowledge to only attack those specific devices. So, to know these details, after successful execution of this attack, the attacker would have information such as the manufacturer, model of the device and the firmware version that is currently affected. Using these statistics, the attacker can find out the range of the vulnerability. One of the tools which can be used for such attacks is BluePrint 0.1, this tool is

based on the BlueZ protocol and it runs on Linux. Again, just as that Backdoor attack in this attack also the BD_ADDR should be known.

11. Reflection Attack

This attack is also called as relay attacks. The simple gist of this attack is that once attacker has access to one of the devices it can impersonate it to talk to other devices and gain trust as well as valuable information. This attack takes place during the authentication between the two devices and the attacker does not need to know any secret information of the devices or the user to perform this attack. Considering these facts this attack can be categorized in the MITM attack again authentication category but not again encryption. The information needed to perform this attack is the BD_ADDRs of the target devices.

12. Brute-Force BD_ADDR Attack

In this attack the BD_ADDR combinations are tried to attack nearby devise or a target device. As the first 3 bytes are known publicly and can be set as fixed, only the last 3 bytes combinations are needed to be made. Although this process is fairly simple but takes a long amount of time to successfully derive the correct BD_ADDR. This attack is usually in highly populated areas to increase the chances of hitting the correct BD_ADDR.

12. Worm Attack

These kinds of attacks occur when a malicious file or a trojan sends itself to a Bluetooth device which then affects its working and privacy. There are mainly three kinds of worm attacks:

- **Cabir Worm**

  The Cabir worm is malicious software that transfers itself to available Bluetooth devices, but it only used to affect devices which were running on Symbian OS. Also, the user would have to accept

the file and install it for it to work. The worm is usually disguised into the form of applications which increase the probability of the user installing it. A similar kind of worm called the Mabir worm replicates itself similar to Cabir worm and spreads by using Multimedia messaging service messages and Bluetooth.

- **Skulls Worm**

  This worm poses as Macromedia Flash player and is used to attack on Symbian mobile phones with the Series 60 platform. It is a malicious Symbian installation trojan file (SIS). Similar to other worms the execution of this worm depends on the installation of it by the user. If it is installed, then it will be executed on the device otherwise it wont work. After infecting the current device, it then searches for other devices which are connected to this device and spreads to those devices as well.

- **Lasco Worm**

  This is a hybrid worm with a mixture of Bluetooth worm and the SIS worm it infects devices with a virus. It reaches the target device in the same way as the other worms do. One of the functions which differentiates it from the other worms is that it can insert itself into the other SI files in the target device. Symbian devices are the most prone to worms especially the ones which support series 60. Lasco worm is also called SymbOS or EPOC. As soon as the targeted use of the mobile device installing the veasco.sis file on the device, the worm will start infecting all the other devices connected to it previously or connected in that moment. And similar to this process it may start spready in a wider number of mobile devices and can cause further issues to the Bluetooth eco system.

4.3 Bluetooth Attack Level

Every Bluetooth attack has its own threat level. Not every threat is serious and everyone threat has to be dealt in different ways. According to different threat levels an efficient preventive algorithm to deal with the problem. The dangers associated and its threat level are shown in the table 4.

Category	Level of threats
Man-In-The Middle	Threat Level: High, these attacks can be easily carried out using security mode 1. Can gain access to personal data.
Surveillance	Threat Level: Low, these attacks are considered harmless. Techniques are used to monitor and collect information.
Obfuscation	Threat Level: Low, Techniques are used to hide attack and prevent detection.
Sniffing	Threat Level: Med, can be used to extract data from unencrypted data. If the packet is encrypted it makes the attack difficult to be executed.
Fuzzer	Threat Level: Med, can be injected inside a stack to affect the software/program. It only can lead to frustration and inconvenience.
Malware	Threat Level: High, can affect the whole system and spread to different connected Bluetooth devices as well. Thought the short range of Bluetooth can hinder the spread of malware.
Range Extension	Threat Level: Low, this attack is generally harmless on its own. Connectivity range is extended for attacks to be conducted.
Denial of Service	Threat Level: Med, Service can be blocked because of large number of faulty requests. Although Bluetooth won't be used for critical transaction and this attack would have less impact.

Unauthorized Direct Data Access	Threat Level: High, it is the most effective attack because of the impact of attacks which come under this category.

Table 5. Level of threats

4.4 Bluetooth Attack Prevention

The best way to avoid any kinds of attack is prevention. Prevention can be done by users' awareness and vigilance. Although if we see practically any kinds of attacks can be prevented if Bluetooth itself is off. If the Bluetooth has to be used, then users can use different model available to hide them from being discoverable. Installation of anti-virus software which are easily available from the play store (For devices running android) or the app store (for apple device) can help in preventing any attacks. One of the other things that the user can do is making sure that the application they are downloading are from trusted sources only, this also applies for documents or any kind of file being downloaded from the Internet.

Connection which have been previously made and not currently being used can have risk factors associated with them. It's a better option to remove paired devices after using them for Bluetooth transmission. Also keeping a check on the notification bar of devices clearly shows which devices are connected right and can again be helpful in finding out if any external devices are connected. Following a pairing guide using the standard methods can also be another method to avoid any kind of attacks to the system, also configuring the default settings on the device can help in minimizing password cracking based attacks. The process of pairing can also be made secure by using cookies which stored on devices.

The Federal Information Processing Standards (FIPS) published papers inform that there are mainly three kinds of security categories: Low, Medium and High. This is based on the fact that how much each attack would have an impact on the service. Organization can make use of the recommendations provided in the NIST SP 800-53 in general. But this should be used with the Bluetooth specification documents too.

The first way to deal with any kinds of Bluetooth attacks is to train and educate the users of the Bluetooth enables devices. Organization should document all the security policies related to their product which would take care of responsibilities of the users in different scenarios. The policies should also contain data regarding what kind of the data can be transmitted over the network and what are the data packets that will not be allowed. The scheme would have certain steps that are needed to follow to prevents attacks such as deciding on what kind of passwords are allowed etc.

We will look into a checklist now which provides multiple criteria which need to be taken care of. These are Bluetooth security check guidelines which can be used for maintaining security over Bluetooth networks.

- ✓ Development of an organization wide policy that addresses all Bluetooth technology.
- ✓ Need to ensure that the wireless device and the technologies involved are completely understood from the point of view of the architecture.
- ✓ The Bluetooth device should always be put in the lowest required power level so that the maximum discovery range for these devices have the smallest possible radius which decreases the probability of attacks that could occur.

- ✓ The users need to ensure that the capabilities which are not currently being used need to be disabled. It would minimize the exposure to potential malicious activities.
- ✓ Another way to deal with most of the attacks is to perform the pairing process in secure location and only with trusted devices. Performing the pairing process would decreases the chances of attacks taking place. If an attacker gets access to the transmitting frames during the pairing process, then getting access to the link key is quite trivial.
- ✓ Having multiple layers of authentication also helps in preventing attacks. The layers could be having biometric systems, two – factor authentication, smart card identification etc.
- ✓ The security modes 2 or 4 which are the BR/EDR level security modes should only be used by experienced users and in a controlled manner. As mode 2 and 4 allow link-level connection before any authentication takes place.
- ✓ Testing plays the most important role; regular testing of the software and the firmware needs to execute because as Bluetooth firmware evolves so does the types of attacks that are possible on the product.
- ✓ User should not accept transmission for unknown devices: these transmissions could be various types of formats but could also have worms in it. Establish connection only between trusted devices.
- ✓ The encryption keys that are used should be needed to be the size which is the maximum that are being allowed. The max that's allowed is 128 bits.
- ✓ The profiles which are not needed are not going to be used should disabled.
- ✓ Linked encryption should be invoked for all the Bluetooth connections.
- ✓ Broadcast transmissions should enable encryption mode 3.

5. Conclusion

In conclusion, this paper has discussed all the aspects for Bluetooth with the analysis of the possible attacks and the preventive measures that are needed to be taken in order to deal with evolving nature of Bluetooth. Bluetooth technology has been immensely adapted in various applications and the shorter range of the Bluetooth is what actually contributed to it becoming popular. Although a large number of devices are using Bluetooth for shorter communication not many organizations have focused on its security which needs to be worked on. A brief description of Bluetooth versions and how Bluetooth has evolved over the years has been discussed. The hardware perspective of Bluetooth has also been covered in this paper.

The mitigation techniques which have been discussed can surely help users in preventing any kinds of attacks to devices. If this technology is used in surgical process or transfer of medical data, then further steps are needed to be taken to maintain the privacy and the integrity of the data.

6. Future Work

In order to improve Bluetooth connection and increase the radius of the networks many improvements are being done by organizations regularly. With regular firmware updates also comes the responsibility to make sure there are no new backdoors or vulnerabilities created. Usage of a machine learning layer in the protocol stack can be worked on for creating Intrusion Detection Systems within the Bluetooth system itself. Hence security issues can be handled in a much better and efficient way with the probability of these attacks being decreases immensely.

Considering the discovery and inventions of many new products that are utilizing Bluetooth technology a survey on the future applications of the Bluetooth will be worked on in the future. Further investigation in the field on scatter nets is required also standard security measures need to be published which will helps organizations to maintain security for their devices.

7. Acronyms

AP Access Point

AFH Adaptive Frequency Hopping

DoS Denial of Service

GAP Generic Access Profile

GHz Gigahertz

MHz Megahertz

SMS Short Message Service

HCI Human Computer Interface

L2cap Logical Link Control and Adaptation Protocol

MAC Medium Access Control

Mbps Megabits per second

MITM Man in the Middle Attack

OS Operating System

SIG Simple Interest Group

SDP Service Discovery Protocol

PIN Personal Identification Number

GPS Global Positioning System

IoT Internet of Things

ICMP Internet Message Control Protocol

IP Internet Protocol

PC Personal Computer

WAP Wireless Application Protocol

OBEX Object Exchange

QOS Quality of Service

TDD Time Division Multiplexing

LAN Local Area Network

RFCOMM Radio Frequency Communication

MANET Mobile Area Network

TCP Transmission Control Protocol

OFDM Orthogonal Frequency Division Multiplexing

8. References

[1] Bluetooth Technology

https://www.electronicsforu.com/videos-slideshows/bluetooth-technology

[2] Bluetooth 101

https://hearinghealthmatters.org/waynesworld/2014/bluetooth-101-part-vi/

[3] Bluetooth Protocol Stack

https://www.ques10.com/p/2700/bluetooth-protocol-stack-1/?

[4] Science Direct: Bluetooth Protocol Stack

https://www.sciencedirect.com/topics/computer-science/bluetooth-protocol-stack

[5] Archived NIST Technical Series Publication

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf

[6] Angela M Lonzetta, Peter Cope, "Security Vulnerabilities in Bluetooth technology used in IoT

https://www.mdpi.com/2224-2708/7/3/28/pdf

[7] Nateq Be-Nazir, Mohammed Tarique, "Bluetooth Security Threats and Solutions: A Survey"

https://pdfs.semanticscholar.org/8872/521819c79505ac20e5da8dd14f8c41eb3f07.pdf

[8] Bluetooth Basics

https://learn.sparkfun.com/tutorials/bluetooth-basics/all

[9] The future of security

https://www.csoonline.com/article/3431705/are-you-being-tracked-through-a-bluetooth-security-vulnerability.html