ISSN 2348-8565

Volume 9 Issue 1 | March 2021 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

A Review of Bluetooth Technology

Aptatim Pranshu
M.Tech Research Scholar
Computer Science and Engineering
Dr. A.P.J. Abdul Kalam University,
Indore (M. P.), India
Email: supercool.apratim@gmail.com

Lokendra Singh Songara
Assistant Professor
Department of Computer Science and Engineering
Dr. A.P.J. Abdul Kalam University,
Indore (M. P.), India
Email: lokendrasingh9229@gmail.com

Abstract*—Bluetooth is primarily utilized for communication between wireless Personal Area Network (PANs). It could be a broadly utilized and persuasive application for sending information from one device to another. It empowers clients to make ad hoc network for information exchange between a wide extend of gadgets. Bluetooth's current information transmission rate is 1 megabits per second utilizing FSK. Bluetooth signals are Omni-directional, so gadgets ought not to be pointed at each other. Our day by day gadgets like phone, wireless headset, smart home application, security framework, Bluetooth car packs etc. all utilize Bluetooth. However, as Bluetooth innovation gets to be more broadly utilized, security imperfections within the innovation are getting to be more visit, causing extreme harm to user's individual information. The matching gadgets play a basic part in anticipating such unauthorized get to from secure contact. This paper talks about that how Bluetooth technology work and also talks about effective security measures which can be included to avoid undesirable malevolent assaults and information lose whereas utilizing Bluetooth technology.*

Keywords:— *Bluetooth blending, application, Bluetooth core protocol, Bluetooth security, authentication, Bluetooth vulnerabilities, Bluetooth security attacks, Bluetooth security modes*

1. INTRODUCTION

Bluetooth is a wireless technology having exceptionally brief extend outlined enabling communication between the gadgets. It is designed by Ericsson in 1994. It named after the 10th Century Danish King Harold Bluetooth. It could be a short run radio connect outlined to put through portable or settled electronic devices. The compelling extend, to date, is thirty feet or ten meters. It could be a combination of computer program (software) and equipment innovation (hardware). The equipment innovation (hardware) part is riding on a radio chip. On the other hand, the computer program (software) most control and security conventions. By utilizing both equipment innovation (hardware) and computer program (software) Bluetooth has ended up a shrewd innovation for proficient and adaptable remote communication system. Now a days it's an important topic among all wireless developers.

Bluetooth gadgets are low-power and have a run of 10 meter remove from the gadget. Now a days Bluetooth innovation is the usage of the convention characterized by the IEEE 802.15 standard. The standard characterizes a wireless PAN (Personal Area Network) operable in a zone of the measure of a room or a lobby. It may be a convention of choice to associate two or more gadgets that are not in coordinate line of locate to each other. A security affiliation between two gadgets can be associated physically by

matching the client entered common PIN (Personal Identification Number) number to each of the gadgets. When two gadgets endeavor to associate, unique key is created based on the PIN number entered on both the gadgets.

The Bluetooth determination is an open detail that is governed by the Bluetooth Special Interest Group (SIG). The Bluetooth details give for three essential security administrations. [1]

- ***Authentication:*** Confirming the character of communicating gadgets based on their Bluetooth gadget address.
- ***Confidentiality:*** Ensuring data from eavesdropping by guaranteeing that as it were authorized gadgets can get to and see transmitted information.
- ***Authorization:*** This process permitting the control of assets by ensuring that a gadget is authorized to utilize a benefit some time recently allowing it to do so.

There are many security issue on Bluetooth technology. At whatever point a gadget tries to connect to put through to another gadget, a Bluetooth user has the ability to select in case they needs to associate or not. Unless higher security is covered, all transmission of important information over Bluetooth would be rash.

2. SOME BLUETOOTH APLICATION

The earliest application of Bluetooth that became popular was Remote control of and communication between a mobile phone and a hand-free headset. [2] Remote control of and communication between a mobile phone and a Bluetooth consistent car stereo system. Exchange of records, contact points of interest, calendar appointments, and updates between gadgets. Remote communication with PC input and output devices, the foremost common being the mouse, keyboard and Printer. Remote control of and communication with tablets and speakers such as iPad and Android gadgets. Remote communication for low transmission capacity applications where higher USB bandwidth isn't required and cable-free connection desired. Remote communication for exchange information records, recordings, and pictures and MP3 or MP4. Dial-up web get to on individual computers or PDAs using a data-capable portable phone as a remote modem. The caller can be connected to the airline's possess arrange association through the wireless local zone arrange (LAN) [2]. Within the short-range transmission of information from sensors gadgets to sensor hubs.

Figure 1: Bluetooth application [3]

Figure 2: Bluetooth application [4]

3. BLUETOOTH MODULE

The Bluetooth Module conveys openings for quick ad hoc associations and the plausibility of programmed, unconscious, connections between WPCOMs. The module may be a completely Bluetooth compliant gadget for data communication with a transmission control of up to +8dBm and recipient sensibility of down to -83dBm combined with low control utilization. The

Bluetooth Module may be a low power implanted Bluetooth v2.0+EDR module with a built-in high output radio wire.

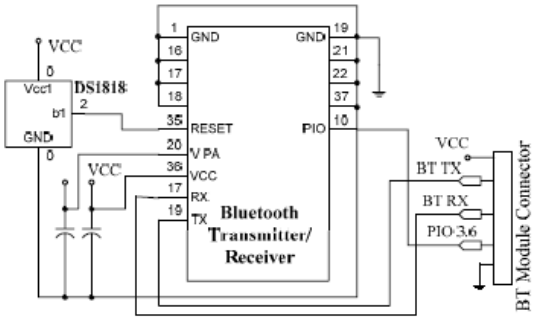

Figure 3: Bluetooth module circuit [5]

4. BLUETOOTH PROTOCOL STACKS

A protocol stack could be a combination of software or hardware implementation of the genuine protocol indicated within the standard. Bluetooth employments an assortment of protocol. Core protocols are characterized by Bluetooth SIG. Extra protocols have been embraced from other bodies. [6]

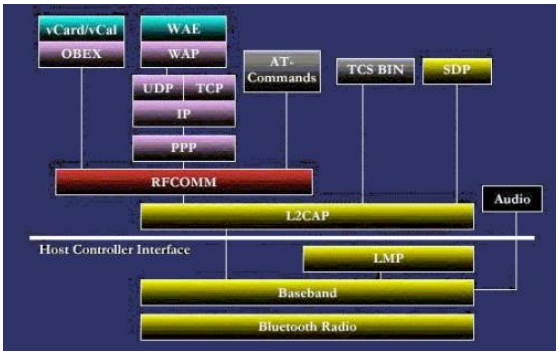

Figure 4: Bluetooth protocol stacks [7]

Bluetooth core protocol:

- ***Bluetooth radio:*** It defines counting recurrence, the air interface, modulation conspire, recurrence hopping and transmission control. [8]
- ***Baseband:*** This protocol defines packet frame format, addressing, timing and power control. [8]
- ***Link manager protocol (LMP):*** It establishes the connect setup between Bluetooth gadgets and oversees continuous joins, counting security viewpoints like verification and encryption, control and arrangement of baseband packet size. [8]
- ***Logical link control and adaptation protocol (L2CAP):*** This protocol adopts upper layer to the baseband layer. Gives both connection-oriented and connectionless services. [8]
- ***Service discovery protocol (SDP):*** SDP handles administrations, gadget information and questions for service Characteristics between two or more Bluetooth gadgets. [8]

Telephony protocol:

- ***TCS BIN:*** That protocol characterizes the call control signaling for the foundation of voice and data calls between Bluetooth gadgets. [6]

Cable replacement protocol:

- ***RFCOMM:*** It provides emulations of RS232 details over the L2CAP protocol. [9]

Adopted protocol:

- Point to Point Protocol (PPP)
- Internet Protocol (IP)
- User Datagram Protocol (UDP)
- Transmission Control Protocol (TCP)
- Wireless Application Protocol (WAP)
- Object Exchange (OBEX)

5. BLUETOOTH NETWORK CONNECTION

There are a variety of ways in which Bluetooth systems can be set up. Piconets and Scatternet are one of them. The fundamental unit of Bluetooth organizing may be a piconet. The terms piconet and scatternet are ordinarily connected to Bluetooth wireless innovation.

- ***Piconet***: It's a Bluetooth network that can have up to eight stations, one of which is called as master and the rest are called as slaves. The master hub is the essential station that oversees the little network. In figure 4, the laptop computer is called the master hub and the other gadgets are called as a slave.

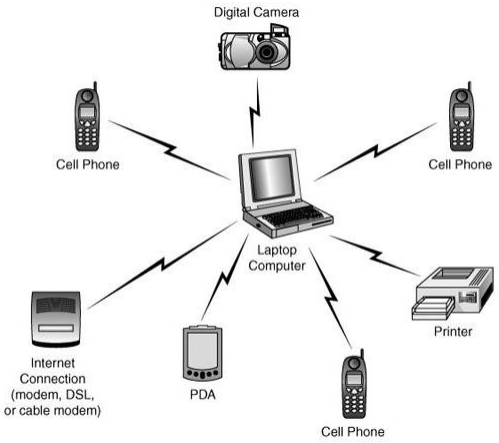

Figure 5: Piconet [10]

- Scatternet: It is a type of Bluetooth network that is formed by two or more piconets. There are three types of node in

Mode 3:

Before establishing a fully physical link a scatternet which is master node, slave node and bridge node. In scatternet there must be at least two piconots. In figure 5, the middle laptop computer is the bridge and also a master node between two piconet. Laptop computer may be a master in one piconet and a slave in another.

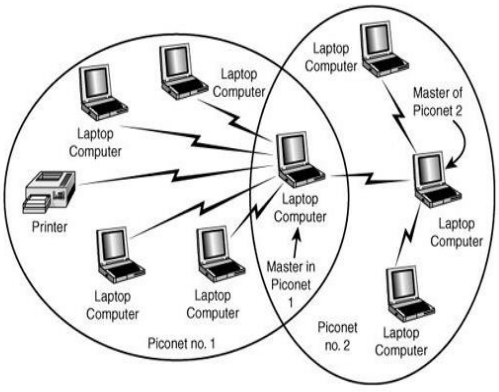

Figure 6: Scatternet [10]

6. BLUETOOTH SECURITY

Bluetooth security modes:

Bluetooth establishes a connection between devices that uses optional pre-shared key authentication and algorithms that are considered powerful when used properly. Bluetooth security is primarily based on the randomness and length of the passkey used during the initial communication. The settings for discoverability and connect-ability are also crucial in security strength. Depending on various versions of Bluetooth, there are 4 security modes. These modes are:-

Mode 1:

This mode is non-secure. The Bluetooth doesn't use any kind of mechanism to stop other Bluetooth-establishing connections. Any Bluetooth gadget can connect to it.

Mode 2:

Before creating a connection, a Bluetooth system does not initiate security procedures. This security mode is a service level enforced mode [11]. The central security manager keeps track of access control policies and communicates with other protocols and users. Security mode 2 is supported by all Bluetooth gadgets.

Bluetooth device generates security procedures.

This mode supports authentication and encryption. While two Bluetooth devices are interacting. When a user puts an identical PIN into both devices during the initialization process, two associated devices simultaneously derive connection keys, as per the Bluetooth specification. Devices automatically authenticate and encrypt the link after the initialization is complete. In Figure 1, the PIN entry, unit association, and main formulation are conceptually portrayed. The Bluetooth device pin codes vary between 1 to 16 bytes. For some application-digit PIN may be enough. But, longer code is always recommended.

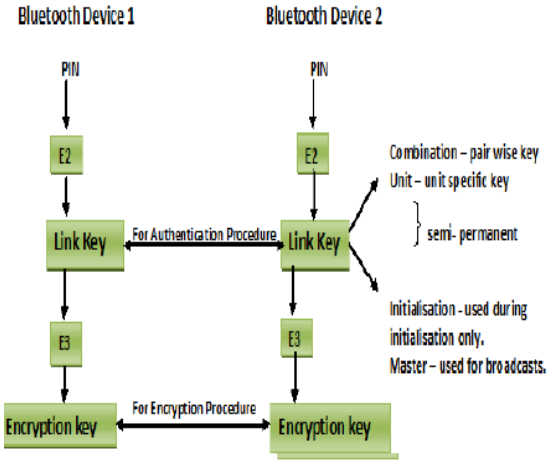

Figure 7: Bluetooth Generation key from PIN [12]

Mode 4:

Security mode 2 and 4 are similar. Like security 2 mode security 4 is also a service level enforced security mode. But this mode can be used only by Bluetooth devices that can use Secure Simple Pairing (SSP) [13] SSP uses Elliptic Curve Diffie Hellman (ECDH) for key exchange and key generation. In this mode, hashing is conducted with SHA-256, and encryption is done through AES CCM. [11]

Bluetooth security procedures:

In terms of security procedures, there are mainly 3 steps. These steps are:

- ***Authorization:*** Authorization is a process of accepting and denying access to a network resource.
- ***Authentication:*** It entails proving one Transceiver device's identity to another. The authentication procedure's aim is to figure out how much access the client has. The link keys are used to verify the authentication. To generate a signed answer authentication result, the sender encrypts the receiver's Bluetooth device address with the connection key and a random number (SRES). If the two link keys are identical, the SRES is sent to the recipient, and the connection is created.
- ***Optional Encryption:*** It's the process of encoding details sent between Bluetooth devices in such a way that eavesdroppers can't understand it. Encryption is a vital part of Bluetooth security. The encryption key size can range from 8 to 128 bits.

6. BLUETOOTH VULNERABILITIES

Despite having several benefits of Bluetooth there are some risks also and the risks are increasing. To prevent these threats Bluetooth security architecture has to be upgraded constantly. Bluetooth transmission can be jammed or intercepted like any other wireless communication system. Hackers or cybercriminals can deliberately mislead the recipient. Bluetooth security is now a great concern. Active researches are going on in both academia and industry. Security risks such as disclosure and privacy attacks usually expose confidential data and can therefore be pretty harmful. DoS attacks, on the other hand, usually harass Bluetooth network users and are considered less dangerous. Using powerful directional antennas in almost any kind of Bluetooth device will greatly increase its scanning, eavesdropping, and attacking range.

8. BLUETOOTH SECURITY ATTACKS

Amidst all of the defense mechanisms in place, using Bluetooth could lead to exploits and data loss from the device through the methods listed below:-

1. ***Bluejacking:*** An attacker basically sends spam messages to a Bluetooth-enabled device user. The attacker can send this message to the users within 30-foot radius.
2. ***Bluebugging:*** In this case, attackers access the user's device remotely. They can receive phone calls, can send text messages, and access data without the consent of the owner.
3. ***Blueover Attack:*** By using only software called Blueover or Blueover

II in a phone Blueover attack can steal data secretly. Blueover attack can be done only if the device is vulnerable to BlueBugging.

4. ***Denial of Service (DoS):*** Users may be denied access to a service by either making it inaccessible or severely restricting its availability to registered users. Attackers can block calls or switch off the Bluetooth of the user.
5. ***Car Whisperer:*** Car Whisperer is a software application that allows hackers to transmit and receive audio from a Bluetooth-enabled car stereo. [14]
6. ***Bluesmack Attack:*** This attack is comparable to a denial-of-service (DoS) attack. This attack is carried out on IP-based machines. Using L2CAP echo messages, this is a buffer overflow attack [15]
7. ***MAC spoofing:*** While Piconets are being generated, malicious attackers can perform MAC spoofing during the link key generation. Assuming, the attack is performed before successful pairing and encryption, attackers can easily intercept data meant for other devices. Long, random, and variable PIN codes are suggested [13]
8. ***BlueSnarfing:*** Without the owner's consent, attackers can access the data.
9. ***Cabir Worm:*** It's a sort of malicious software that searches for and sends itself to available Bluetooth devices using Bluetooth technology. The Cabir worm illustrates that writing mobile viruses that spread through Bluetooth is possible, which can enable other hackers to explore the possibility of writing Bluetooth viruses. The Mabir worm is a variation of the Cabir worm that simulates using Bluetooth and Multimedia Messaging Service messages (MMS) [16]
10. ***Fuzzing Attack:*** The attack happens when an adversary sends malformed data packets and non-standard data to a device's Bluetooth radio in an order to cause it to behave abnormally. When these attacks cause a device's response to be slowed or stopped, it indicates the protocol stack has a significant flaw. [17]
11. ***Backdoor Attack:*** The backdoor attack requires implementing a trust relationship through the pairing mechanism, but ensuring that it does not appear in the target's list of paired devices. When the connection is established the attackers have full control of the victim's device. The attacker remains stealth while accessing all the data.
12. ***Eavesdropping:*** It's all about wireless technology. Bluetooth encryption, like Wi-Fi encryption, is supposed to keep attackers from listening in on your information**.**

9. RISK MITIGATION AND COUNTERMEASURE

By applying countermeasures to prevent threats and vulnerabilities risk mitigation can be achieved. Organizations who are using Bluetooth should address document security policies. The policies should also include a proper password usage scheme. Organizations should include educational awareness-based knowledge to provide an adequate level of knowledge for those who will deal with Bluetooth-enabled devices. Some of the risk mitigation techniques and countermeasures are given below:-

- To achieve optimal standards default settings should be updated.
- PIN codes have to be random and long. Using long and random PIN codes makes it harder for the attackers to hack.
- Bluetooth devices have to be set to

the lowest power to secure transmission within a safe perimeter of the desired network.

- Devices should be discoverable only for a short period of time to pair with the desired devices. Devices that are discoverable and connectable all the time are prone to attack.
- On Bluetooth-enabled hosts that are often attacked by malware, antivirus software must be installed [12]
- To ensure that the policy is locally and widely applied, a centralized security policy management strategy should be used in accordance with an endpoint security product installed on the Bluetooth devices wherever possible. [15]
- Attackers can update or modify link keys if they are not stored properly [13]
- Bluetooth patches need to be fully tested before deploying and upgrades regularly.
- Users should not accept any kind of messages, photos, and files from unknown devices.

10. BLUETOOTH PREVENTION MEASURES

- Always keep physical control of your devices. Remove devices that have been missing or stolen from paired device lists.
- Avoid using the Bluetooth-enabled device to interact or transfer confidential or personal information, as it could be sniffed.
- When connecting your Bluetooth device to your PC, enable encryption. [14]
- To keep up with the latest viruses and Trojans, update your device antivirus on a regular basis.
- Security Mode 3 is strongly recommended for the highest level of security. Security mode 3 is enforced at the connection level to give the highest security.

11. CONCLUSION

This paper covers up different vital themes such as a few foundation data related to the Bluetooth system, its applications, how it works and different security issues included in Bluetooth. We talked about vulnerabilities in different versions of Bluetooth, as well as a bunch of new Bluetooth security attacks. Most of which arise from the pairing phase. Bluetooth risk mitigation and countermeasures were also researched in this paper. Bluetooth security experts need to research more and update their technologies frequently to stand against Bluetooth vulnerabilities.

REFERENCES:

[1] "Bluetooth Security," [Online]. Available: https://www.electronics-notes.com/articles/connectivity/bluetooth/security.php.

[2] S. S. B. K. Madhvi Verma, "*An Overview of Bluetooth Technology and its Communication",* vol. 3, 2015.

[3] Moumita, "Tutorialspoint," 2020. [Online]. Available: https://www.tutorialspoint.com/bluetooth-usage-and-applications.

[4] T. editor, "Applications of Bluetooth," 2017. [Online]. Available: https://www.polytechnichub.com/applications-of-bluetooth/.

[5] Y.-W. B. a. M.-B. L. Chia-Hung Lien, "Remote-Controllable Power Outlet System for Home Power Management," vol. 53, 2007.

[6] "Wikipedia," [Online]. Available:

https://en.wikipedia.org/wiki/List_of_Bluetooth_protocols.

[7] G. C. K. Dennis Browning, "Bluetooth Hacking: A Case Study," [Online]. Available: https://www.garykessler.net/library/bluetooth_hacking_browning_kessler.pdf.

[8] moumita, "tutorialspoint," 22 5 2020. [Online]. Available: https://www.tutorialspoint.com/the-bluetooth-protocol-stack.

[9] "Bluetooth Protocol stack/layers," RF wireless world, [Online]. Available: https://www.rfwireless-world.com/Tutorials/Bluetooth-protocol-stack.html#:~:text=between%20bluetooth%20devices.-Cable%20replacement%20protocol,specifications%20over%20bluetooth%20physical%20layer..

[10] "Flylib.com," [Online]. Available: https://flylib.com/books/en/4.152.1.144/1/.

[11] "Security Vulnerabilities in Bluetooth Technology as Used in IoT," *journal of sensor and Actuator Networks,* 2018.

[12] P. K. Mishra, "Bluetooth Security Threats," *International Journal of Computer Science & Engineering,* vol. 4, 2013.

[13] M. T. Nateq Be-Nazir Ibn Minar, "Bluetooth Security Threats and Solutions: A Survey" *International Journal of Distributed and Parallel Systems (IJDPS),* vol. 3, 2012.

[14] T. P. P. Panse, "A Survey on Security Threats and Vulnerability attacks on Bluetooth Communication," *(IJCSIT) International Journal of Computer Science and Information Technologies,* vol. 4(5), 2013.

[15] J. K. R. K. M. Kaur, "Bluetooth Technology," ijecs open access, vol. 5, 2016.

[16] C. Rhodes, "Bluetooth Security," East Carolina University.

[17] J. P. j. B. M. B. M. H. R. S. L. C. K. Scarfone, "Guide to BluetoothSecurity," in NIST Special Publication 800-121 Revision 2, 2017.