International Journal of Research in Advent Technology, Vol.7, No.3, March 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

An overview of Bluetooth Technology and Security

Rajinder Singh
Department of Computer Science and Applications PUSSGRC Hoshiarpur (Pb.)
Email: rajinderid@gmail.com

Abstract- Bluetooth is a short range wireless technology used for wireless communication. It allows devices to communicate with each other without needing cables or wires. Bluetooth technology devices are of low power, low cost and low complexity. With the help of Bluetooth a number of different kinds of devices can be connected. This technology follows client server architecture. It operates in 2.4GHz ISM bands. In this paper an overview of this technology and its security concern is given.

Keywords-Piconet;Scatternet;Bluejacking;

1. INTRODUCTION

Wireless communication means exchanging information between sender and receiver without using wires. In this case data is exchanged between sender and receiver with the help of radio waves. Bluetooth technology is a short range wireless technology that supports communication between portable devices including cell phones, wireless speakers, printers and computers [1]. This technology uses the short range radio signals which replace cables and wires. It is used to build Personal area network. It is managed by a group called Bluetooth Special Interest Group (SIG). Initial members were ERICSSION, IBM, NOKIA Intel and Toshiba. Currently there are more than 30000 members in this group [2]. This technology has not only replaced the wires, but it has made a tremendous impact on the market also.

Main features of this technology are low power and it support point to point as well as point to multipoint connections. Bluetooth signals can pass through walls. It operates in 2.4 GHz band and it avoids interference by hopping to a new frequency [3].

2. MAIN FEATURES OF BLUETOOTH

Less Hardware: It eliminates the need of different wires and cables which are required to connect two different devices, e.g. mouse, keyboards and printers etc.

Compatibility: Bluetooth devices are capable of exchanging the information regardless of the manufacturer of the devices.

Reliability: Bluetooth uses three techniques to ensure protocol reliability, FH-CDMA, Error Correction and RSSI.

Speed: High quality voice and data can be transferred with speed. Data can be transferred under noisy environments and its voice transmission is audible even under noisy conditions.

Power: Bluetooth devices changes there power levels dynamically [3].

Internet connectivity: Bluetooth enabled device can share internet facility with other Bluetooth enabled devices [4].

Security:

Main built in features which provide the security of the data are i) Authentication Process ii) Encryption of Data iii) FHSS [3].

3. WORKING OF BLUETOOTH TECHNOLOGY

Bluetooth is also helpful to create Personal Area Network. Bluetooth enabled devices use two types of topology called piconets and scatternets. A piconet contains maximum of 8 Bluetooth enabled devices. One device is acting a master and up to 7 slaves. A master starts communication with other devices. It governs the communication and traffic among the slave devices. A slave device responds to master device. Master device sets the frequency hopping pattern and slave devices are required to follow that pattern. Slave devices are required to synchronize the time with the master

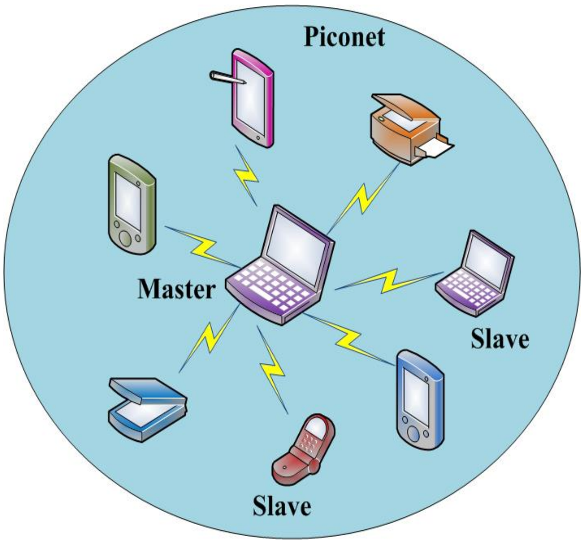


Figure 1 Piconet

device. A slave can transfer data in the time slot following master's time slot. Frequency hopping sequence is also defined by the master device. The master device sets frequency hopping sequence and sends a radio signal to the slave device asking for response. The slaves synchronize their hop frequency and clock with the master device. Each piconet uses different frequency pattern to avoid the interference from the other nearby piconet. In case of scatternet topology two or more piconets are connected by a common Bluetooth enabled device [5].

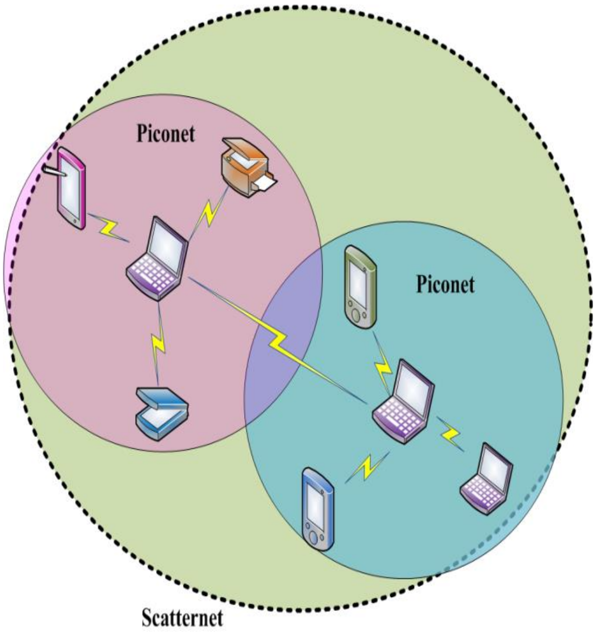


Figure 2 Scatternet

4. BLUETOOTH PROTOCOL STACK

In this technology following protocol stacks are used.
1) Core Protocols
Core protocols deals with link layer and networking. Radio protocol used to mange modulation techniques, frequency bands and frequency hopping specifications. Baseband protocol is concerned with address scheme and packet format. Link protocols are concerned with creating and maintain link. L2CAP protocol deals with handling upper layer packets.
Service discovery protocol handles service related queries.
2) Cable Replacements Protocols
RFCOMM is used for cable replacement protocol. It is used for providing serial communication between Bluetooth enabled devices.
3) Telephony Control Protocols
It is used for providing call control functionality.
4) Adopted Protocol

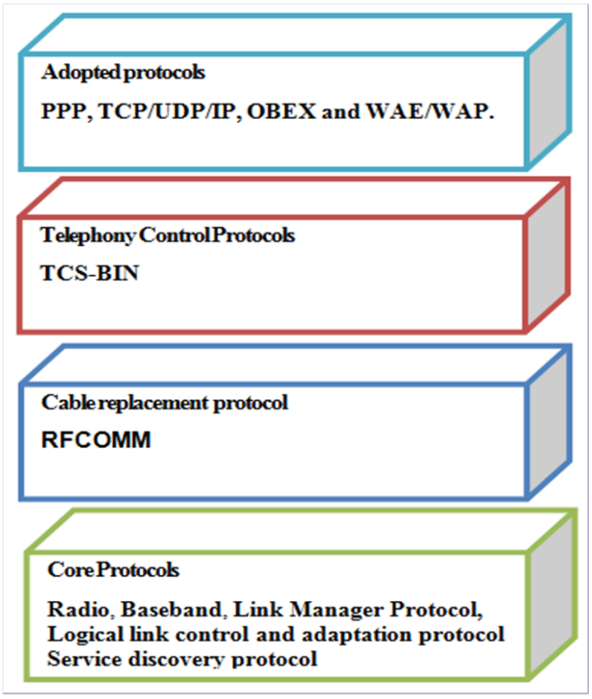

Adopted protocols
PPP, TCP/UDP/IP, OBEX and WAE/WAP.
Telephony Control Protocols
TCS-BIN
Cable replacement protocol
RFCOMM
Core Protocols
Radio, Baseband, Link Manager Protocol,
Logical link control and adaptation protocol
Service discovery protocol

Figure 3 Bluetooth Protocol Stack

These are used for supporting higher layer applications. These are also used for providing interoperability [6].

5. SECURITY

Bluetooth technology is safer as compared to Wi-Fi but it is still prone to cyber attacks. Some of the common Bluetooth threats are given below.

Bluebugging
In this attack, attackers take control of a mobile cell.
Attacker can do call forwarding, can listen conversation or can send messages.
Bluejacking
Sending inappropriate messages or advertisements, images or sound is called Bluejacking. This attack is harmless but it creates confusion among the users.

Bluesnarfing
It is the theft of information from a Bluetooth device when attacker has gained the unauthorized access to it. Attacker can steal messages, contacts and passwords [7].

Blueborne
This attack is done by exploiting stack buffer overflow. Attacker can hijack Bluetooth connections [8].

Security of the Bluetooth device is very important. Nowadays hackers are gaining access to increasing number of devices. So the security of the Bluetooth device becomes very important.

Bluetooth claims that Bluetooth technology provide better security as compared to WLAN/ IrDA. All these features are built in protocol stack. Applications can also be implement their own security requirements. Bluetooth technology follows following different security mode for a Bluetooth device.

Security Mode 1
First operating mode is non secure mode. In this case authentication and encryption schemes are not followed by the device. So this device can be hacked. Since in this module no security mechanism is used, so other Bluetooth enabled devices can establish connection with the device.

Security Mode 2
In this case centralized manager control the access of specific services and device. Control manager maintains the policies for accessing a device. This module has authentication and encryption mechanism at LMP layer.

Security Mode 3
In this case security procedures are initiated first. Once this procedure is setup only then link is established with the Bluetooth device. Authentication and encryption schemes are used for all connections. These schemes use separate secret link key for pairing [9].

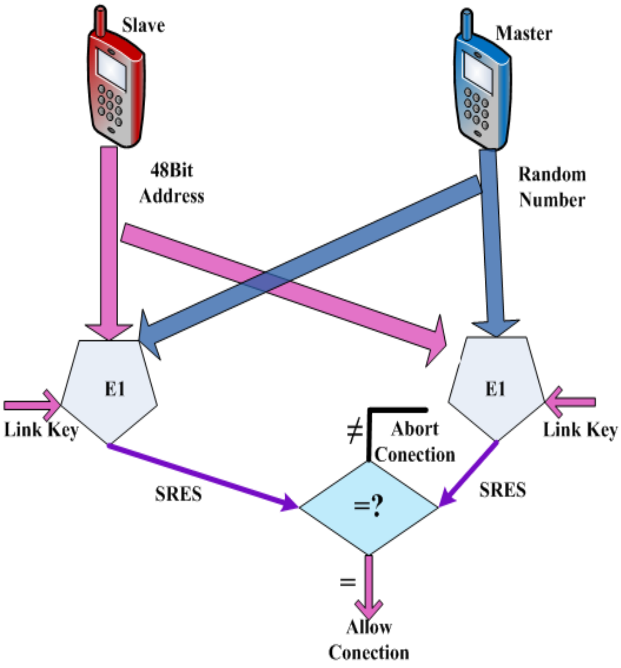
Main security procedures for the Bluetooth are
1) Initialization 2) authentication 3) encryption

During initialization phase Bluetooth Link Key is generated. This process starts when two devices starts communicating. Both these devices generate link keys when the same pin is entered in both of them. When this process is complete then authentication and encryption procedure is done automatically without intervention of the user.

Main steps of the authentication are:

1. First communicating device transmit its 48-bit address to the second device.
2. Second device send a random number (128-bit number) called random challenge.
3. Both devices then generate authentication response called SRES using E1 algorithm.
4. Device 1 sends SRES to device 2 where it is compared. If SRES are equal then connection is established else it is rejected [10].

Figure 4 Authentication Process



Encryption
For providing confidentiality Bluetooth devices use encryption algorithms. Encryption key is generated from random number, ciphering offset and from the current link key [11].

6. CONCLUSION

Bluetooth technology is a good option to replace the wired connections. With the help of this technology a number of devices can communicate. This technology is also very helpful for creating personal area network. This technology is moderately secure; therefore it is vulnerable to attacks. Therefore it is important for the users to understand this technology and risk associated with this technology. These risks can be mitigated if the users follow proper configuration guidelines and security policies.

REFERENCES

[1] Wang, Hongfeng. "Overview of Bluetooth technology." Univ. Pennsylvania, Philadelphia, PA, Tech. Rep (2001): 10
[2] https://en.wikipedia.org/wiki/Bluetooth
[3] Prabhu, C. S. R., and A. Prathap Reddi. Bluetooth Technology: And Its Applications With Java And J2Me. PHI Learning Pvt. Ltd., 2004.
[4] https://www.ukessays.com/essays/computer-science/the-characteristics-of-bluetooth-technology-computer-science-essay.php
[5] https://www.elprocus.com/how-does-bluetooth-work/

[6] http://www.rfwireless-world.com/Tutorials/Bluetooth-protocol-stack.html

[7] http://www.rfwireless-world.com/Tutorials/Bluetooth-security.html

[8] Lonzetta, Angela, et al. "Security vulnerabilities in Bluetooth technology as used in IoT." Journal of Sensor and Actuator Networks 7.3 (2018): 28.

[9] https://www.electronics-notes.com/articles/connectivity/bluetooth/security.php

[10] http://www.rfwireless-world.com/Tutorials/Bluetooth-security.html

[11] Padgette, John, Karen Scarfone, and Lily Chen. "Guide to bluetooth security." NIST Special Publication 800.121 (2012): 25.