ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

REVIEW ATICLE

Available Online at www.ijarcs.info

A Short Range Wireless Network: Bluetooth

Menal Dahiya
Assistant Professor, Dept. of Computer Science
Maharaja Surajmal Institute
Janakpuri, Delhi, India

Abstract: This paper discusses about the wireless networks, we are using now-a-days. The most widely used, standard of wireless network now-a-days is Bluetooth. Bluetooth is a standard which is open and used for short term range at a low cost, low power and low profile. The types of networks related to Bluetooth- Pico net and Scatter net. It also explains the four major components used in the Bluetooth Architecture. It specifies the range, benefits and security enforces in Bluetooth. The main three security services offered are Confidentiality, Integrity and Authenticity. It also explains the requirements to ensure the security.

Keywords: Authenticity; Bluetooth; Confidentiality; Integrity; Security; Wireless Network.

I. INTRODUCTION

Wireless technologies are very popular in our everyday business and personal lives. Personal digital assistants (PDA) allow users to access calendars, email, address and phone number lists, and the Internet. Few technologies even offer global positioning system (GPS) capabilities that can locate the location of any device anywhere in the world. Wireless networks serve as the transport mechanism among devices and the old wired networks. Wireless technologies will also offer even more features and functions in the next few years. The developing government agencies, businesses, and home users are using, or considering wireless technologies in their day-to-day life. Agencies should be aware of the security risks related to wireless technologies. Agencies need to develop strategies to handle risks as they integrate wireless technologies into their computing environments. Due to latest technologies in wireless LAN with WPA and 802.11i, enterprise deployments have finally started to use wireless access networks. Wireless LAN technologies are used in an enterprise deployment, For the past several years, Adoption of some 802.11i security features by the WiFi Alliance in the Wi-Fi Protected Access (WPA), as well as the standard of the 802.11i security has greatly improved the authentication, encryption and integrity security capabilities. This paper contains both a survey of security technologies and the threats to wireless mesh networks. The security technologies will cover current industry capabilities and 802.11s, and the overall security architecture.The popular standard now-a-days is Bluetooth. The Bluetooth is a computing and telecommunications industry specification that describes how mobile phones, computers should interconnect with each other, with home and business phones, and with computers using short-range wireless connections. Bluetooth provides three different classes of power management. Class 1 devices, the highest power devices, operate at 100 milliwatt (mW) and have an operating range of up to 100 meters (m). Class 2 devices operate at 2.5 mW and have an operating range of up to 10 m. Class 3, the lowest power devices, operates at 1 mW and have an operating range of from 1/10 meter to 10 meters. Section I describes about the Wireless Networks. Section II describes about a standard Bluetooth. Section III describes about Bluetooth architecture. Section IV describes about the security of Bluetooth.

II. WIRELESS NETWORKS

Wireless networks serve as the transport mechanism among devices and the old wired networks. There are many and diverse wireless networks, but are frequently categorized into three groups on the basis of their coverage range:- Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). WWAN covers wide coverage area technologies like 2G cellular, Cellular Digital Packet Data (CDPD) and Global System for Mobile Communications (GSM), and Mobitex [1]. WLAN, is wireless local area networks, which includes 802.11, HiperLAN, and several others. WPAN termed as wireless personal area network technologies like Bluetooth and IR. All of these technologies are “tether less”—they receive and transmit information using electromagnetic (EM) waves. Wavelengths are used by wireless technologies ranging from the radio frequency (RF) band up to and above the IR band [2]. A significant portion of the EM radiation spectrum is covered by the frequencies in the RF band which extends from 9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz (GHz),the highest allocated wireless communications frequency. EM energy moves into the IR and then into the visible spectrum, as beyond RF spectrum the frequency increases. Devices are allowed by wireless networks to move with changing degrees of freedom and they still maintain communication with each other. They also offer greater flexibility are offered by wireless networks than the cabled networks and the time and resources which are required to set up new networks are somewhat reduced and it allows the creation, modification or torn down of ad hoc networks easily. The most generally used Wireless Networks are the following: -

A. Wireless Local Area Networks (WLAN)

They are the groups of wireless networking nodes within a limited geographic area, such as an office building or campus, that are capable of radio communications [3]. WLANs are usually implemented as extensions to existing wired local area

networks to provide enhanced user mobility. WLANs are based on the IEEE 802.11 standard, which the IEEE first developed in 1997. This standard was designed to support medium-range, higher data rate applications, like Ethernet networks, and to address mobile and portable stations. The standard is designed for 1 to 2 Mbps wireless transmissions which is the original standard of WLAN. Iby 802.11a was developed in 1999 for high speed WLAN with 54 Mbps wireless transmissions and 5GHz band. The main standard of WLAN is 802.11b, which is in use now-a-days which gives the proper speed for today's applications.

B. Wireless Metropolitation Area Networks (WMAN)

This can provide connectivity to users located in multiple facilities generally within a few miles of each other. Many WMAN implementations provide wireless broadband access to customers in metropolitan areas. A WMAN covers a larger area than Wireless Local Area Network (WLAN) and smaller area than Wireless Wide Area Network (WWAN). It is owned by a single entity like Internet Service Provider (ISP) or Government Entity or Large Corporation and can be accessed by only authorized users or subscriber devices.

C. Wireless Personal Area Networks (WPAN)

WPAN is a wireless network, which needs a little or no infrastructure. It is operatable within a short range. A WPAN can connect few devices within a single room and does not connect devices using cables. WPAN includes print services are enabling a wireless keyboard or mouse to communicate with a computer as an example.

III. BLUETOOTH OVERVIEW

The popular standard now-a-days is Bluetooth. The Bluetooth is a computing and telecommunications industry specification that describes how mobile phones, computers should interconnect with each other, with home and business phones, and with computers using short-range wireless connections. Bluetooth network applications include wireless synchronization, e-mail/Internet/intranet access using local personal computer connections, hidden computing through automated applications and networking, and applications that can be used for such devices as hands-free headsets and car kits [4-5]. The Bluetooth standard specifies wireless operation in the 2.45 GHz radio band and supports data rates up to 720 kbps.5 It further supports up to three simultaneous voice channels and employs frequency-hopping scheme and power reduction to reduce interference with other devices operating in the same frequency band. The IEEE 802.15 organization has derived a wireless personal area networking technology based on Bluetooth specifications.

Bluetooth is an open standard for short-range communication. It is treated as a low-cost, low-power, and low-profile technology that provides a mechanism for creating small wireless networks on an ad hoc basis [6]. Bluetooth is considered a wireless PAN technology that offers fast and reliable transmission of both voice and data. Untethered Bluetooth devices will eliminate the need for cables and provide a bridge to existing networks. Bluetooth can be used to connect almost any device to any other device. An example is the connection between a PDA and a mobile phone. The goal of Bluetooth is to connect disparate devices (PDAs, cell phones, printers, faxes, etc.) together wirelessly in a small environment such as an office or home.

A. *Bluetooth is a Standard that will Ultimately*

- Eliminate wires and cables between both stationary and mobile devices
- Facilitate both data and voice communications
- Offer the possibility of ad hoc networks and deliver synchronized between personal devices.

Bluetooth is designed to operate in the ISM (industrial, scientific, medical applications) band that is available in most parts of the world. Bluetooth-enabled devices will automatically locate each other, but making connections with other devices and forming networks requires user action.

B. Bluetooth defines two types of networks

1. Piconet

- Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.
- Piconet can have up to eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters [7].
- There can be only one primary or master station in each piconet.
- The communication between the primary and the secondary can be one-to-one or one-to-many.
- All communication is between master and a slave. Salve-slave communication is not possible.

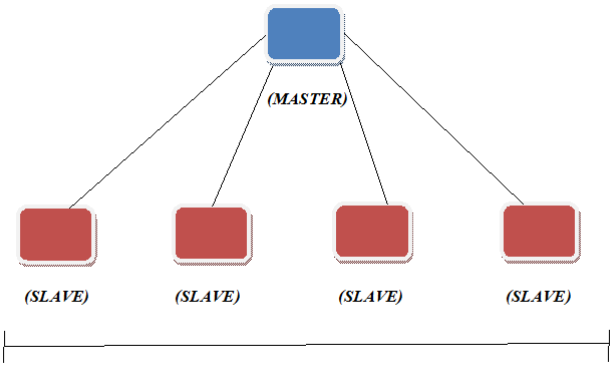

FIG 1-PICONET

Figure 1 shows the piconet which is having a master slave relationship between nodes.

2. Scatternet

- Scattemet is formed by combining various Pico nets.
- A slave in one piconet can act as a master or primary in other piconet.
- A station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.
- Thus a station can be a member of two piconets.
- A station cannot be a master in two Pico nets [8-9].

Figure 2 shows the Scatter net in which there are 2 Pico nets which are connected through bridge slave who receive a message from one Pico net and deliver that message to another Pico net connected to it.

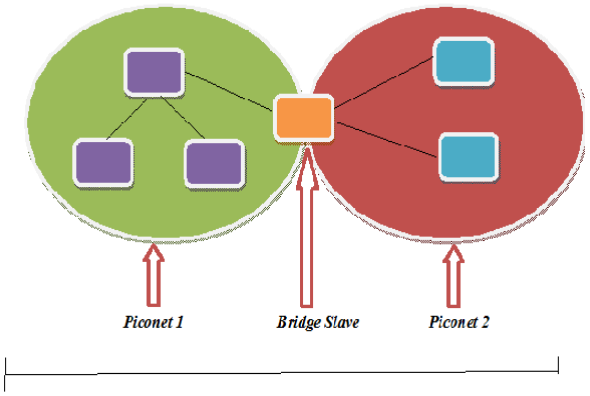

FIG 2- SCATTERNET

Bluetooth provides three different classes of power management. Class 1 devices, the highest power devices, operate at 100 milliwatt (mW) and have an operating range of up to 100 meters (m). Class 2 devices operate at 2.5 mW and have an operating range of up to 10 m. Class 3, the lowest power devices, operates at 1 mW and have an operating range of from 1/10 meter to 10 meters. Range depends on surroundings, radio performance and antennas.There are many factors affecting Bluetooth range, typically: -

- The output power of the transmitter.
- The sensitivity of the receiver.
- Physical obstacles in the transmission path.
- The antennas [10].

Bluetooth offers five primary benefits to users. This ad hoc method of untethered communication makes Bluetooth very attractive today and can result in increased efficiency and reduced costs. The efficiencies and cost savings are attractive for the home user and the enterprise business user. Benefits of Bluetooth include Cable replacement, Bluetooth technology replaces cables for a variety of interconnections. These include those of peripheral devices (i.e., mouse and keyboard computer connections), USB at 12 Mbps (USB 1.1) up to 480 Mbps (USB 2.0); printers and modems, usually at 4 Mbps; and wireless headsets and microphones that interface with PCs or mobile phones; Ease of file sharing, Bluetooth enables file sharing between Bluetooth-enabled devices. For example, participants of a meeting with Bluetooth-compatible laptops can share files with each other; Wireless synchronization, Bluetooth provides automatic wireless synchronization with other Bluetooth-enabled devices. For example, personal information contained in address books and date books can be synchronized between PDAs, laptops, mobile phones, and other devices; Automated wireless applications, Bluetooth supports automatic wireless application functions. Unlike synchronization, which typically occurs locally, automatic wireless application interface with the LAN and Internet. For example, an individual working offline on e-mails might be outside of their regular service area—on a flight, for instance. To e-mail the files queued in the inbox of the laptop, the individual, once back in a service area (i.e., having landed), would activate a mobile phone or any other device capable of connecting to a network. The laptop would then automatically initiate a network join by using the phone as a modem and automatically send the e-mails after the individual logs on Internet connectivity [11]. Bluetooth is supported by a variety of devices and applications. Some of these devices include mobile phones, PDAs, laptops, desktops, and fixed telephones. Internet connectivity is possible when these devices and technologies join together to use each other's capabilities. For example, a laptop, using a Bluetooth connection, can request a mobile phone to establish a dial-up connection; the laptop can then access the Internet through that connection [12].

IV. BLUETOOTH ARCHITECTURE

There are four major components of Architecture:

A. Radio Unit (Radio Transceiver)

Radio transceiver supports spectrum spreading and operates at a frequency between 2.402 GHz - 2.480 GHz ISM band.

B. Baseband Unit (Flash Memory & CPU)

Implements baseband protocols, and Link Manager (LM) routines.

C. Software Stack (Driver Software)

It is the software through which the driver are installed in the process of Bluetooth.

D. Application Software (User Interface)

Bluetooth give user interface also, hence this application software is for the user.

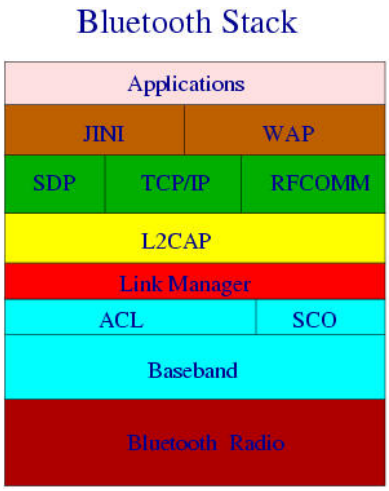

Figure 3 Architecture of Bluetooth.

V. SECURITY OF BLUETOOTH

To use a standard there is a major requirement to ensure the security of data using the standard. Bluetooth, plays an important role in security and Bluetooth SIG has put a lot of efforts to make Bluetooth secure to transmit critical information. We divide Bluetooth security in three modes:

Non-Secure, Service Level Enforced Security and Link level enforced security. Non-Secure mode does not provide any security measures between Bluetooth Devices. Service Level Enforced Security mode, provides an environment in which two Bluetooth devices can establish a non-secure Asynchronous Connection-Less (ACL) link. L2CAP (Logical Link Control and Adaptation Protocol) Connection-Oriented or Connection-Less channel request mode follows some security procedures that are authentication, authorization and optional encryption and the Bluetooth device initiates security procedures before the channel is established [13].

A. Security Services

Briefly, there are three basic security services defined by the Bluetooth specifications are as:

- *Authentication*- A goal of Bluetooth is the identity verification of communicating devices. This security service addresses the question "Do I know with whom I'm communicating?" This service provides an abort mechanism if a device cannot authenticate properly.

- *Confidentiality*- Confidentiality, or privacy, is another security goal of Bluetooth. The intent is to prevent information compromise caused by eavesdropping (passive attack). This service, in general, addresses the question "Are only authorized devices allowed to view my data?.

- *Integration*- A third goal of Bluetooth is a security service developed to prevent the information from alteration. This service addresses the question "Is the only sender can change the data?.

- *Encryption*- This process is used to secure the data by encoding the messages using one or two keys so that only authorized users can access the information [14].

B. Security Threats

Bluetooth offers several benefits and advantages. Organizations must not only address the security threats associated with Bluetooth before they implement the technologies; they must also assess the Capabilities of the devices they allow to participate in the Bluetooth networks. Specifically, organizations need to address Security concerns for Confidentiality, Data Integrity, and Network Availability.

- *Loss of Confidentiality*- Threats to confidentiality involve, when a Bluetooth device that is part of a piconet becomes compromised, it may still receive information that the malicious user should not access.

- *Loss of Integrity*- Integrity threats involving the alteration, addition, or deletion of information, which is then passed through the network without the user's or network administrator's knowledge. Information that is subject to corruption includes files on the network and data on user devices. For example, a infected user might employ an untrusted device, such as a PDA, to access the address book of another PDA or laptop.

- *Loss of Availability*- Bluetooth devices share bandwidth with microwave ovens, cordless phones, and other wireless networks and thus are vulnerable to interference. Malicious users can interfere with the flow of information, hence the loss of availability of resources occurs [15].

VI. CONCLUSION

The paper concludes that Bluetooth is the most widely used standards of Wireless Network which is used mostly by mobile devices to share files in the small range. Two structures of Bluetooth are Pico net and Scatter net. Bluetooth gives a lot of benefits and mostly are cable replacement, easily file sharing facility and non-requirement of Internet connection. Security of Bluetooth is maintained by using Symmetric Key Encryption to provide authentication, integrity, authenticity and confidentiality.

VII. REFERENCES

[1] Mohammad Mahmud Kabir, "Security & Privacy in WLAN - A Primer and Case Study," February 15, 2016, https://www.slideshare.net/mahmudkabir/security-privacy-in-wlan-a-primer-and-case-study.

[2] A. Gerkis, "A Survey of Wireless Mesh Networking Security Technology and Threats," Mesh Networking Security – GIAC Gold Pape, September 2006, https://www.sans.org/reading-room/whitepapers/networkdevs/survey-wireless-mesh-networking-security-technology-threats-1657.

[3] S. Gopala Krishnan, "A Survey of Wireless Network Security," International Journal of Computer Science and Mobile Computing, Volume.03, Issue.01, pp. 53-68, January-2014.

[4] Ghossoon M. Waleed. M. Faizal, R. B. Ahmad, M. F.B.A. Malek and M. A. Ghani, "Bluetooth Wireless Network Authentication Using Radio Frequency Communication Protocol," Journal of Computer Science, Volume.05, Issue.09, pp. 646-650, 2009, DOI: 10.3844/JCSSP.2009.646.650.

[5] Aafreen Singh and Shilpi, "Wireless Security," India Seminar on emerging trends in wireless communication-Vision 2020, pp. 7-14, https://www.scribd.com/document/13603859/wireless-security#.

[6] Tzu-Chang Yeh, Jian-Ren Peng, Sheng-Shih Wang, and Jun-Ping Hsu, "Securing Bluetooth Communications," International Journal of Network Security, Volume.14, Issue.04, pp. 229-235, July 2012.

[7] Devika Sindwani and et.al, "Bluetooth Technology," October 2016, https://www.slideshare.net/DevikaSindwani/bluetooth-technology-66777069.

[8] Entc Engineering, "Bluetooth Architecture and Layers of Bluetooth," http://www.entcengg.com/2016/12/bluetooth-architecture-layers-bluetooth.html.

[9] Dinesh Thakur, "Bluetooth - What is Bluetooth?," http://ecomputernotes.com/computernetworkingnotes/communication-networks/bluetooth.

[10] Mike Harwood, "CompTIA Network+ N10-004 Exam Cram, 3rd Edition," Pearson IT Certification, March 2009, ISBN: 978-0789737960.

[11] Manik Arora, "Mobile Security," https://www.scribd.com/presentation/29360549/Mobile-Security.

[12] Nitesh Rijal and Gopal Pd Shah, "Bluetooth Technology A Boon To Wireless Communication," http://niteshrijal.com.np/pub/bluetooth-technology.pdf.

[13] Colleen Rhodes, "Bluetooth Security," http://www.infosecwriters.com/Papers/CRhodes_Bluetooth.pdf.

[14] U.L.Muhammed Rijah, S.Mosharani, S.Amuthapriya, M.M.M Mufthas, Malikberdi Hezretov and Dhishan Dhammearatchi, "Bluetooth Security Analysis and Solution," International Journal of Scientific and Research Publications, Volume.06, Issue. 04, pp. 333-338, April 2016.

[15] Wi-Fi Notes, "Wireless Personal Area Networks-Bluetooth Networks," March 2015, http://wifinotes.com/wireless-personal-area-network.html.