A Study of Bluetooth Wireless Technology Using Recent Attacks

Article · May 2018

DOI: 10.23956/ijarcsse.v8i4.627

3 authors, including:

Rizwan Khan
ABES Institute of Technology
58 PUBLICATIONS **131** CITATIONS

SEE PROFILE

International Journals of Advanced Research in Computer Science and Software Engineering
ISSN: 2277-128X (Volume-8, Issue-4)

Research Article | **April 2018**

A Study of Bluetooth Wireless Technology Using Recent Attacks

Shivangi Gautam*
Scholar, Department of CSE, ABESIT, Ghaziabad, Uttar Pradesh, India
shivangigautam181@gmail.com

Ashutosh Pandey
Assistant Professor, Department of CSE, ABESIT, Ghaziabad, Uttar Pradesh, India
ashutosh.pandey@abesit.in

Rizwan Khan
Associate Professor, Department of CSE, ABESIT, Ghaziabad, Uttar Pradesh, India
rizwan.khan@abesit.in

Abstract— Bluetooth is a wireless technology that is used for the exchange of information over a network for short separations. It is a low controlled, short range application. It utilizes Bluetooth to convey to other Bluetooth-empowered gadgets because it is a communication protocol. Bluetooth resembles some other correspondence convention that you utilize each day, for example, HTTP, FTP, SMTP, or IMAP. Bluetooth is designed to connect with monitor and mouse without any connection with CPU. Different kinds of Bluetooth gadgets are headsets, Bluetooth prepared printer, in-auto Bluetooth framework, Bluetooth gps framework, Bluetooth console, Bluetooth prepared webcam and so on. Bluetooth advancement tends to an open entryway for the business to pass on remote arrangements that are unavoidable over an expansive scope of gadgets. The constraints and properties of Bluetooth scatter presents remarkable troubles in framing a system in which all devices communicate with each other directly. In this paper, detailed description of Bluetooth along with its working is given. Description also includes connection protocols of the Bluetooth, usage models, advantages and dis-advantages. Further, various applications of the Bluetooth wireless technology are portrayed.

Keywords— Applications, Piconets, Personal Area Network(PAN), Scatter-Nets, Ad-hoc Network.

I. INTRODUCTION

In the present situation, the wireless connectivity has become a dynamic zone of research as we have perceived an extensive number of government and industry initiatives, research efforts and standard activities that have targeted to enable wireless and mobile networking technologies. As a result, today we have a different arrangement of wireless access technologies[5].Bluetooth is an innovation which goes about as a medium to associate individuals with no geological confinements and time limitations, require less power, and can be utilized for short range. The Bluetooth innovation was at first concocted in 1994 by Ericsson, however is overseen by an affiliation or an institutionalization body Bluetooth Special Interest Group. Bluetooth is recently for small range, wireless communication which utilizes less power. In the starting, it was visualized just as a wire substitution. Its most frequently depicted application is that of a "cordless computer "comprising of several devices including a personal computer, mainly a laptop, keyboard, mouse, joystick, printer, scanner,etc., each outfitted with a Bluetooth card. There is not physical connection between these devices, and Bluetooth is to enable consistent transmission of data between all them, basically replacing what is accomplished today through a merger of links, and infrared connections. In every single conceivable case, Bluetooth has the limit with respect to being significantly something other than a substitution to wire, and arranged all the more energetically. Bluetooth holds the guarantee of becoming the innovation of choice in the near future.

A. Why The Name Bluetooth

The name Bluetooth in the technology came in the tenth century, after the ruler Harald Blatand . Things being what they are, the pervasive Bluetooth technology's name has nothing to do with being blue or tooth-like in appearance and has an inseparable tie to medieval Scandinavia. He had a nickname: Blatonn in Old Norse and the meaning of this name is Bluetooth. The presentation of Bluetooth as an innovation came as an upset, which enhanced the utility of cell phones, as well as made sharing of documents easier.

II. HOW BLUETOOTH TECHNOLOGY WORKS

The difference in Bluetooth is about 9milimeter x 9milimeter microchip, which provides us a remote connection which is of short range. A 10m area is provided to us by Bluetooth which assists in concurrent trade of both voice and non-voice data between the devices. With piconet we can associate up to 8 gadgets, and within the 10 meter bubble 10

piconets can exist. Every single piconet bolsters up to three synchronous voice gadgets that are full duplex.The overall information trade ought to be about 1 megabyte per second, however for full duplex transmission the veritable information trade ought to be about 432 Kilobyte per second, for unequal transmission it is 721 per 56 Kilobyte per second, and for tms 2000 transmission it is 384 Kilobyte per second. Bluetooth remote development is similar to a wire which is having up to 128-piece open per private key affirmation in case of security, and in light of a security, spilling figure up to 64 bit.

A. Transmission Types And Rates

The base band, which is a single channel per line convention, is a blend of circuit and bundle exchanging. To guarantee that parcels don't land out of request, openings (up to five) can be saved for synchronous bundles. As noted concurrent. We can bolster up to 3 synchronous (voice) information channels, or 1 synchronous and 1 offbeat information channel, on single channel. Every single synchronous channel can fortify 64 Kilobyte per second change standard, which is absolutely satisfactory for transmission of voice. An offbeat channel could be used to transmit 721 Kilobyte per second in single heading and 57.6 Kilobyte per second the other way. Furthermore, if the connection is symmetric, offbeat association can bolster 432.6 Kilobyte per second in the two headings.

B. Radio Frequency and Spectrum Hopping

The commotion in nature does not cause any damage in sending of the documents from Bluetooth. Quick affirmation and recurrence jumping, makes the associations powerful. The Bluetooth innovation is parcel based, and bounces to another recurrence after every bundle is gotten, which include security and also not helps in constraining impedance issues. The information rates including headers are 1Mbps. Refinement of full duplex transmission is done using time division multiplexing method. The Bluetooth radio chip has a capacity of 2.4 gigahertz. It isolates the recurrence band which is of 2 GHz into 79 jumps 1 MHz isolated, starting at 2.402 and stopping at 2.480 (however the information transmission is smaller in Spain, France and Japan). This spread range is used to jump starting with 1 channel then onto the next, pseudo-subjectively, which incorporates a layer of security that is strong. We can make up to 1600 consistent jumps. The standard recurrence run ranges from 10 cm to 10 m, and can be contacted no under 100 meters by expanding transmission control.

C. Data Transmission

Broadcasting of data can be done either synchronously or non-concurrently. The strategy that is utilized for voice is synchronous connection oriented(SCO), and the one for information is asynchronous connection-less(ACL). Within a single piconet, every ace slave can use other transmission mode, which can be changed at whatever point. Time Division Duplex (TDD) can be utilized by both ACL and SCO , and both help 16 sorts of parcels, out of them 4 are control bundles which are same in each kind. As we want information transmission to be smooth, SCO parcels are conveyed through held interims, it means, the bundles are transmitted in bunches without allowing interference from other transmissions. Transmission of SCO packets can be done without allowing the sending unit to survey them. We can perform both symmetric and asymmetric transmissions using ACL links. Ace unit controls the ability to exchange information, it decides the aggregate of the amount of time one slave unit can be used.

D. Network Management

In the network topology of Bluetooth, the associations are of two types: point-to-multipoint or point-to-point. In a piconet, one gadget can build up an association with another piconet to shape a scatter net. In the figure beneath, the graphs comprise of piconet A; that again consists of 4 units and piconet B, which comprises of 2 units.

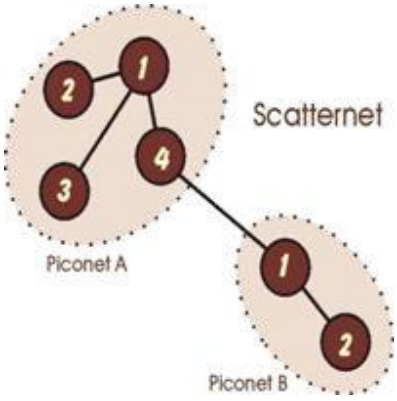

Fig.1 Scatternet

E. Error Correction And Security

The FEC strategies diminish the quantity of re-transmissions. The ARQ scheme requires that the checks being performed on header error and cyclic redundancy must be okay. If they are okay, an acknowledge is sent. If they aren't, the data is resent. We can provide security in three routes: through encryption, verification and pseudo-irregular recurrence band. Validation enables a client to control availability to just gadgets determined. Encryption utilizes key lengths of about 1, 40, and 64 bits. In any case, it isn't the most elevated amount accessible, and for those clients who require it, the proposition is to investigate isolate arrange exchange conventions and security programming.

III. CONNECTION PROTOCOL

Using the following techniques we can establish the Bluetooth connections:

A. *Standby*: The standby mode is the default stage. In this, the devices are not connected in a piconet. The standby mode of connection establishment, allows messages to be heard over 32 hop frequencies every 28 seconds (it is less in France, Spain and Japan).

B. *Page/Inquiry:* In the inquiry mode of connection establishment, the device issues an inquiry for identity of devices within range. A device wishing to establish a connection with another device, sends a page message or an inquiry message to the device nearby. If the address of the device is known, the master unit conveys on 16 hop frequencies, 16 identical page messages to the slave unit. The master re-transmits on the other 16 hop frequencies, if no response is received. Since the MAC address is obscure to the master unit, the request requires an extra response from the slave unit.

C. *Active:* It is one of the technique through which Bluetooth connections can be established. In this the transmission of data takes place.

D. *Hold:* The hold mode of connection establishment can be started whenever the master or slave wishes to start it. In the hold mode, no transmission of the data takes place. The motivation behind the hold mode is to save power or else the exchange of data takes place.

E. *Sniff:* The sniff mode of connection establishment is in relevance to the slave units, and it is also mainly for the power conservation. In this mode, there is no active role of the slave in the piconet. It is just a programmable setting.

F. *Park:* The park mode of connection establishment is the technique for Bluetooth connection establishment which involves diminished level of movement than the hold mode. During the establishment of connection using park mode, the slave is in sync to the piconet and therefore does not require full reactivation.

IV. USAGE MODEL

The Bluetooth usage indicate interfacing the gadgets together, it is centered around three general sequence: voice/information get to focuses, fringe interconnects Personal Area Network(PAN)

A. Voice/Data Access Points

It is the porting of a computing device to communication device through a safe and wireless connection. For example, consider a mobile computer having Bluetooth. It can be linked to a mobile that connects to internet to access e-mail with the help of Bluetooth. Now here the mobile phone acts as a personal access point. These access points have advantage over modems as they higher the information rate. A public space could connect to the private Bluetooth access point through LAN and then it could be guided over the dsl line using internet, allowing each access point to act as a private internet connection.

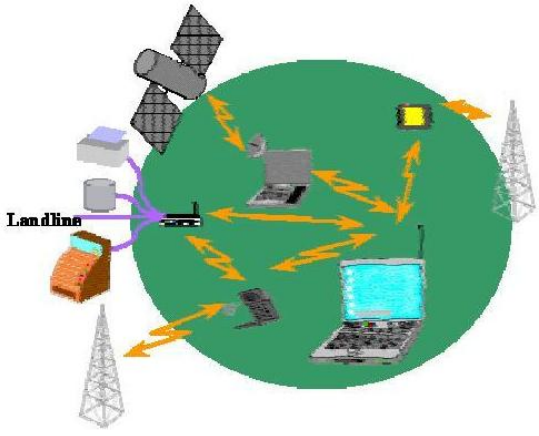

Fig.2. voice/data access points

B. Peripheral Interconnects

The peripheral interconnects model includes incorporating distinctive gadgets together. Envision joysticks, mouse and standard consoles that work over a wireless connection. Bluetooth interface is intertwined with the adaptable pc; along this line, the cost of the periphery contraption is less on the ground that a passageway point isn't required. Likewise, tremendous number of these gadgets can be used as a piece of different markets. For instance, a Bluetooth headset utilized as a bit of the work space could be identified with a Bluetooth and gets the chance to offers access to the multimedia parts as well as workplace phone of the versatile PC. In the event that there ought to be an event of versatile, the relative headset could be used to interface with the remote (which would now have the ability to stay in a coordinator case or tote). Bluetooth also provides a short-extended association in the domain of region security devices.

Fig. 3.Peripheral Interconnects

C. Personal Area Networking

The Personal Area Networking display is based on the breakdown of individual frameworks and impromptu arrangement. Imagine meeting some individual in an air terminal and rapidly and securely trading reports by working up a private piconet. Later on, when Bluetooth slows down, we could quickly download the electronic media for later access on the telephone.

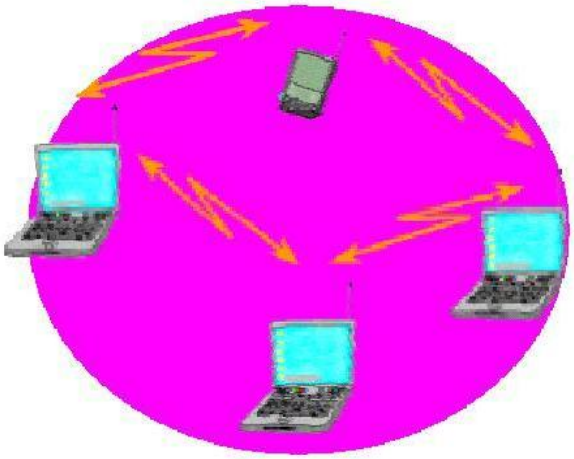

Fig 4 Personal Area Network

V. HACKER TOOLS

A hacking tool is a program intended to help with hacking, or a bit of programming which can be utilized for hacking purposes.

A. Bluesnarfing Attack

It is an attack which is done on wireless devices for the theft of information, for undue advantage, with the help of a Bluetooth connection.An attacker exploits the implementation of Bluetooth on mobile phones to access the private details or other information of the users such as user's calender,contacts, e-mail,texts etc. without leaving any clue of the attack. [1]

B. Blue-jacking

It is an attack which is done on the wireless devices to prevent the theft of information, for undue advantage with the help of a Bluetooth connection. An attacker exploits the implementation of Bluetooth on mobile phones to access the private details or other information of the users such as user's calendars, contacts, e-mails, texts etc. without leaving any clue of the attack. [1]

VI. ADVANTAGES AND DIS-ADVANTAGES

A. Advantages Of Bluetooth Technology

1) The Bluetooth technology has a simple setup.
2) The Bluetooth devices are very much compatible with other devices.
3) It requires less hardware.
4) It is a wireless technology and easy to use.

B. Disadvantages Of Bluetooth Technology

1) The transfer of data within the Bluetooth device is average in comparison to that with the Wi-Fi.
2) Scope of a Bluetooth Device is 15-30 feet relying on the device.
3) Security is the greatest weakness as transfer takes place through radio waves and a hacker can easily hack it.
4) Battery use is additionally an issue, it will make device out of power before it would have if Bluetooth was not powered on.

A house could be called a smart home if it has the ability to recognize when its residents arrive and automatically opens the door for them. This can be possible in the case of homes that are enabled with the Bluetooth devices. This Bluetooth device could also provide the modification in the temperature of the rooms. Along with all these, we can exchange the information between the person's PDA and electronic board of the home, and the calender of the family could be refreshed to reflect the activities that are scheduled.

VII. APPLICATIONS

A. Smart Home

A house could be called a smart home if it has the ability to recognize when its residents arrive and automatically opens the door for them. This can be possible in the case of homes that are enabled with the Bluetooth devices. This Bluetooth device could also provide the modification in the temperature of the rooms. Along with all these, we can exchange the information between the person's PDA and electronic board of the home, and the calender of the family could be refreshed to reflect the activities that are scheduled.

B. The Internet Bridge

The internet bridge can also be an application of the Bluetooth technology. This model could be thought of as a portable pc that allows us to surf the internet without identifying the individual's area, also it is independent of the fact that if the user is using a cellular device or the one connected through wire.

C. Automatic Check-In

Automatic check-in can be considered as an important application of Bluetooth technology. In the present scenario, the hotels test or are planning to test the various benefits that would authorize the visitors to check-in, unlock the doors of the technology. The mobile phones which have the inbuilt Bluetooth technology could be used to exhibit the ticket in the air crafts without having the prerequisite to go to the registration counters.

D. The Three-In- One Phone

A single handset can provide multiple functionality using Bluetooth Support. At home, the telephone can go about as a cordless device which is associated to the fixed line, while travelling, it could go about as a cell phone which is associated to the versatile system. The time two phones with built-in Bluetooth Technology comes in contact with each other having the same feature, they act a walkie-talkie.

E. Wireless communication can be easily implemented between computer and its peripheral devices like keyboard, mouse, printer [6]

VIII. CONCLUSION

The intent behind writing this paper was to provide brief introduction to the Bluetooth technology. We have described many of the junctures including connection protocol and usage model. The hacker tools are also described in the paper. Bluetooth is a standard used in links of radio of short scope, bound to substitute wired connections between electronic devices like cellular telephones, Personal Digital Assistants (PDA), computers, and many other devices. As the Bluetooth technology has become a popular technology for transferring the data, its security is also equally important. There can be various methods that can be used for the security.

REFERENCES

[1] International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012, BLUETOOTH SECURITY THREATS AND SO LUTIONS: A SURVEY, Nateq Be-Nazir Ibn Minar and Mohammed Tarique, Department of Electrical and Electronic Engineering, American International University, Bangladesh

[2] International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.3, August 2011, A Modern Study of Bluetooth Wireless Technology, Mrs. Pratibha Singh, Mr. Dipesh Sharma,Mr. Sonu Agrawal RIT, Raipur, Dept. of Computer science & Eng., RIT,Dept. of inf. Tech.,SSCET, durg, Dept. of Computer sci. & Eng. Raipur, (Chhattisgarh), India.

[3] https://en.wikipedia.org/wiki/Bluetooth

[4] Simranjit Singh Chadha, Mandeep Singh, Suraj Kumar Pardeshi, "Bluetooth for managing Pole Mounted Remote Terminal Unit", International Journal of Computer Science & Communication, Vol.4, No. 2, 2013

[5] Jaap Haartsen, Mahmoud Naghshinegh, Jon Inouye, Olaf J. Joeressen, Warren Allen, “bluetooth vision, goals and architecture”, Mobile Computing and communications Review, Volume 1, November 1997. [6] Rupali Ghodke, Sangeeta Jogade, Deepak Misaal, “Bluetooth Technology: An Overview”, Volume 3, 2018

