www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -03 March, 2016 Page No. 16001-16003

Bluetooth Technology

Jagjeet Kaur[1], Ramandeep Kaur[2], Manpreet Kaur[3]

[1]Master of Computer Applications
jyotisembhi@gmail.com

[2] Master of Computer Applications
Ramanwarring@gmail.com

[3]Post Graduate Department of Computer Science and Applications,
GHG Khalsa College, Gurusar Sadhar (Distt. Ludhiana)
MK_Sidhu@yahoo.com

Abstract: Bluetooth technology unplugs our digital peripherals. In short, it is a wireless replacement for many of the cables we currently use to transmit voice and data signals. Bluetooth radio modules use Gaussian Frequency Shift Keying (GFSK) for modulation. Bluetooth employs an FHSS spreading technique, changing frequencies at a rate of 1600 times per second - 160 times the rate at which a wireless LAN changes frequencies. This paper focuses on the attacks and security issues in Bluetooth technology.

Keywords: Bluetooth technology features, Bluetooth network topology, Personal networking hardware and the protocol stack layers, the power modes, Bluetooth security, types of attacks.

Introduction

Bluetooth, the new technology named after the 10th Century Danish King Harold Bluetooth, is a hot topic among wireless developers. This article will provide an introduction to the technology.

The Bluetooth specification is an open specification that is governed by the Bluetooth Special Interest Group (SIG). The Bluetooth SIG is lead by its five founding companies and four new member companies who were added in late 1999. These nine companies form the Promoter Group of the Bluetooth SIG:

Founding Companies	**New Members**
Ericsson	3Com Corporation
IBM Corporation	Lucent Technologies
Intel Corporation	Microsoft Corporation
Nokia	Motorola Inc.
Toshiba Corporation	

More than 1200 additional companies are members of the Bluetooth SIG.

Bluetooth technology Features

It separates the frequency band into hops. This spread spectrum is used to hop from one channel to another, which adds a strong layer of security.

Signals can be transmitted through walls and briefcases, thus eliminating the need for line-of-sight. Devices do not need to be pointed at each other, as signals are Omni-directional.

BLUETOOTH is used in Phones and pagers and Headsets, Modems and LAN access devices , Notebook computers , Desktop and handheld computers, Printers and Fax machines, Keyboards and Joysticks.

The Bluetooth Network Topology: There are 3 types of connections in Bluetooth, as shown below:

The Piconet: Bluetooth devices can interact with one or more other Bluetooth devices in several different ways. The simplest scheme is when only two devices are involved. This is referred to as point-to-point. One of the devices acts as the master and the other as a slave. This ad-hoc network is referred to as a ***piconet***. A piconet is any such Bluetooth network with one master and one or more slaves. A diagram of a piconet is provided in Figure 1. In the case of multiple slaves, the communication topology is referred to as **point-to-multipoint**. In this case, the channel is shared among all the devices in the piconet. There can be up to seven active slaves in a piconet. Each of the active slaves has an assigned 3-bit Active Member address (AM_ADDR). There can be additional slaves which remain synchronized to the master, but do not have a Active Member address. These slaves are not active and are referred to as parked. For the case of both active and parked units, all channel access is regulated by the master. A parked device has an 8-bit Parked Member Address (PM_ADDR), thus limiting the number of parked members to 256. A parked device remains synchronized to the master clock and can very quickly become active and begin communicating in the piconet.

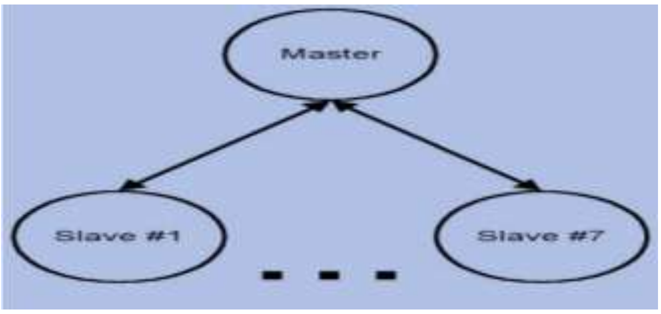

Figure 1: Piconet

The Scatternet: When two or more piconets are connected is called Scatternet.

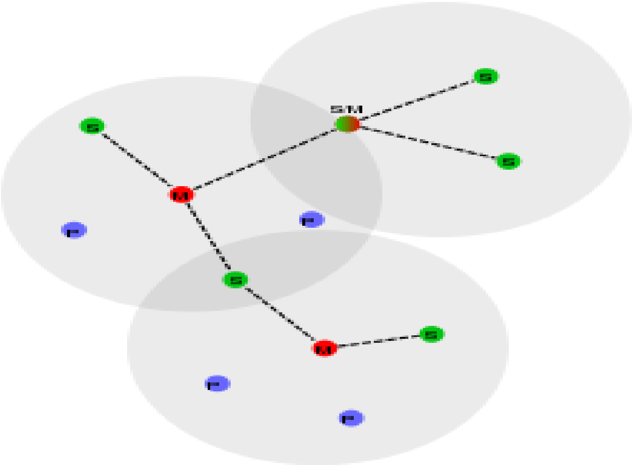

Figure 2: Scatternet

Because the two piconets are so close, they have overlapping coverage areas. A slaves in one piconet can participate in another piconet as either a master or slave. This is accomplished through time division multiplexing. In a scatternet, the two (or more) piconets are not synchronized in either time or frequency. Each of the piconets operates in its own frequency hopping channel while any devices in multiple piconets participate at the appropriate time via time division multiplexing.

Personal Networking Hardware And the Protocol Stack Layers: Bluetooth radio modules use Gaussian Frequency Shift Keying (GFSK) for modulation. The data is transmitted at a data rate of 1 Mb/second.

The Bluetooth Baseband Layer: The baseband layer performs functions like Bluetooth packet assembly, forward error correction (FEC), automatic repeat request (ARQ), data whitening, Bluetooth clock synchronization, and frequency hopping control.

The Bluetooth Link Manager Layer: The Link Manager forms the piconet by inquiring what other Bluetooth radios are in the area, establishing connection and maintaining the piconet. The Link Manager also handles security issues like authentication and encryption.

Radio: The Radio layer defines the requirements for a Bluetooth transceiver operating in the 2.4 GHz ISM band.

The Power Modes

Bluetooth provides for three low power modes to conserve battery life: sniff mode, hold mode, and park mode. While in the sniff mode, a device listens to the piconet at a reduced rate. The sniff interval is programmable, providing flexibility for different applications. In hold mode, only an internal timer is running, and data transfer restarts when units transition out of the hold mode. Park mode is used to handle more than seven clients - since only seven clients can be "active" at any time, one client can be "parked" and another one activated.

The advantage of "frequency-hopping"

Bluetooth has been designed to operate in noisy radio frequency environments, and uses a fast acknowledgement and frequency-hopping scheme to make the link robust, communication-wise. Bluetooth radio modules avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. Compared with other systems operating in the same frequency band, the Bluetooth radio typically hops faster and uses shorter packets. This is because short packages and fast hopping limit the impact of microwave ovens and other sources of disturbances. Use of Forward Error Correction (FEC) limits the impact of random noise on long-distance links.

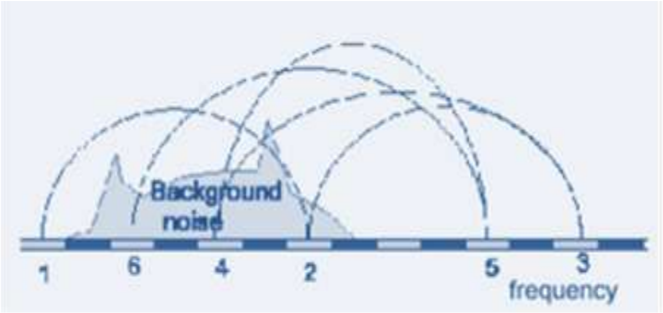

Figure 3: Frequency hopping

Bluetooth Security

Bluetooth defines three security modes. Security Mode 1 provides no security enforcement, meaning that the device is effectively taking no steps to protect itself. Security Mode 2 enforces security at the service level. In this mode, a particular application might be relatively safe but no additional device protection has been added. Security Mode 3 is the highest level of security, employing link level enforced security mechanisms. Security Mode 3 protects the device from certain intrusions.

Types of attacks

There are a variety of attacks that can be employed against Bluetooth devices, such as bluebugging, bluebumping, bluedumping, bluejacking, bluesmacking, bluesnarfing, bluespooofing [sic], bluestabbing, bluetoothing, and car whisperer. All take advantage of weaknesses in Bluetooth that allow an attacker unauthorized access to a victim's phone. Some of the common attacks on Bluetooth devices include:

Bluebugging: A powerful attack mechanism, bluebugging allows an attacker to take control of a victim's phone using the AT command parser. Bluebug allows an attacker to access a victim's phone in order to make phone calls, send short message service (SMS) messages, read SMS messages stored on the phone, read and write list entries, alter phone service parameters, connect to the Internet, set call forwarding, and more.

Bluejacking: The sending of unsolicited messages to open Bluetooth devices by sending a vCard with a message in the name field and exploiting the OBEX protocol.

Bluesmack: A Bluetooth analog of the Ping of Death denial of service attack. This is a buffer overflow attack using L2CAP echo messages.

Bluesnarf and Bluesnarf++ ; Attacks allowing for the theft of information from a Bluetooth device using the OBEX Push Profile. The attacker needs only find a phone that has Bluetooth in discoverable mode. Bluesnarf works by a connection to most of the Object Push Profile services and the attacker retrieves the file names of known files from the Infrared Mobile ommunications (IrMC) list instead of sending vCard information as expected. With these attacks the hacker can retrieve items such as the phonebook, calendar, and other personal information. With Bluesnarf++, the attacker has full read and write access to the file system of the phone. When an attacker is connected via the OBEX Push Profile, he/she has full access to the victim's phone without having to pair the two devices. The biggest risk with this function is that an attacker can delete crucial file system files, rendering the victim's device useless. In addition, the attacker can access any memory cards that are attached to the device.

Conclusion

Despite some of the problems, Bluetooth remains a very promising technology, with plenty of medium and long term applications. This technology is probably the only one which has a good chance to become widely available among PDAs and mobile devices. Bluetooth-equipped gadgets can connect to the LAN through the Access Protocols at once.50 kilobytes per second is about all you can expect from Bluetooth. So there we are: Bluetooth is simply the best.

References

[1] A Bluetooth Routing Protocol Using Evolving Fuzzy Neural Networks presented by Chenn-Jung Huang, Wei-Kuang Lai, Sheng-Yu Hsiao and Hao-Yu Liu.

[2] Hop Count Based Optimization of Bluetooth Scatternets presented by Csaba Kiss Kall_, Carla-Fabiana Chiasserini,Sewook Jung.

[3] Bluetooth Scatternets: An Enhanced Adaptive Scheduling Scheme presented by Simon Baatz, Matthias Frank, Carmen K¨uhl, Peter Martini, Christoph Scholz

[4] Bluetooth Scatternet with Infrastructure Support:Formation Algorithms given by Tatiana K. Madsen, Fjolnir Gudmundsson, Stefan Sverrisson, Hans P. Schwefel and Ramjee Prasad

[5] B. Miller and C. Bisdikian. *Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications*. Prentice-Hall, 2000.

[6] T. Salonidis, P. Bhagwat, L. Tassiulas, and R. Lamaire. Distributed topology construction of Bluetooth personal area networks. In *Proceedings of INFOCOM'2001*, 2001.

[7] T. Salonidis, P. Bhagwat, L. Tassiulas, Proximity awareness and fast connection establishment in bluetooth, in: First Annual Workshop on Mobile and Ad Hoc Networking and Computing, MobiHOC 2000, 2000, pp. 141–142.

[8] A. Aggarwal, M. Kapoor, L. Ramachandran, A. Sarkar, Clustering algorithms for wireless ad hoc networks, in: Proceedings of the 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Boston, MA, USA, 2000, pp. 54–63.

[9] https://gcn.com

[10] https://en.wikipedia.org

[11] https://creativeworld9.com

[12] https://ukessays.com