AN OVERVIEW OF BLUETOOTH TECHNOLOGY

BY

OJO, Folorunso Fidelis

Department of Computer Science

Federal College of Education, Abeokuta

Tel: 08065797801

AND

AMUDA, Tajudeen Gbenga
Department of Biological Sciences
Tai Solarin University of Education, Ijagun, Ijebu-Ode
Tel: 08135656868

ABSTRACT

A Bluetooth adhoc network can be formed by interconnecting piconets into scatter nets. The constraints and properties of Bluetooth scatter net present special challenges in forming an ad hoc network efficiently. This research work was brought together, to give an overview of the state of the art. Simply stated, Bluetooth is a wireless communication protocol. Since it's a communication protocol, you can use Bluetooth to communicate to other Bluetooth-enabled devices. In these sense, Bluetooth is like any other communication protocol that we use every day, such as HTTP, FTP, SMTP, or IMAP. Bluetooth has client server architecture; the one that initiates the connection is the client, and the one who receive the connection is the server. Bluetooth is a great protocol for wireless communication because it's capable of transmitting data at nearly IMB'S while consuming 1/100th of the power of WI-FI. Then we review the state of – the art approaches with respect to Bluetooth scatter net formation and contrast them.

KEY: *Bluetooth,Communication, Protocol, Server, Architecture, Client, Wireless*

INTRODUCTION

The development of the “short-link” radio technology, later name Bluetooth, was initiated in 1989 by Nils Rydbeck, CTO at Ericsson Mobile in Lund, Sweden and by Johan Ullman, The purpose was to develop wireless headsets, according to two inventions by Johan Ullman, SE 8902098-6, issued 1989-06-12 and SE 9202239, issued 1992-07-24. Nils Rybeck tasked Tord Wingren with specifying and Jaap Haartsen and Sven Mattisson with developing. Both were working for Ericsson in Lund. The specification is based on frequency-hopping spread spectrum technology. Andreas, (2007)

WHAT IS BLUETOOTH?

Bluetooth is one of the most efficiently short distance wireless communication devices in our daily lives. With its stability and convenience in communication, this has allowed Bluetooth technology to become a valuable asset for both computers and electronic communication. It was first developed by a group called Bluetooth Special Interest Group (SIG) which formed by elite companies such as Ericsson, Nokia, Intel, IBM and Toshiba in May 1998. Bluetooth technology was officially approved in the summer of 1999. Since then the creation of Bluetooth wireless communication is widely used in various electronics and has been expanding every day. Starting from communication between mobile phones and computers, Bluetooth has expanded to enable communication between such forms as headsets, printers and automobiles Alzieu, Vincent (2003).

Bluetooth is a combination of hardware and software technology, running on a hardware radio chip and utilizing software to provide the main control and security protocols. By using this newer hardware and smarter software algorithms to direct network data we can achieve more efficient, flexible and secure wireless communications. The future is geared towards wireless communication as the cables seen on desktops are slowly becoming obsolete. The movement towards Bluetooth is rapidly rising and the low cost and efficiency is a clear indication of the unlimited possibilities of Bluetooth. Lamm, Gregory, Gerlando Faluato, Jorge Estrada, Jag Gadiyaram (2002).

Bluetooth is a networking technology aimed at low-powered, short range applications. It was initially developed by Ericsson, but it is governed as an open specification by the Bluetooth Special Interest Group. Bluetooth is a recently proposed standard for short range, low power wireless communication. Initially, it is being envisioned simply as a wire replacement technology. Its most commonly described application is that of a “cordless computer

consisting of several devices including a personal computer, possibly a laptop, keyboard, mouse, joystick, printer, scanner etc., each equipped with a Bluetooth card. There are no cable connections between these devices and Bluetooth is to enable seamless communication between all them, essentially replacing what is today achieved through a combination of serial and parallel cables, and infrared links Miller B and Bisdikian C. (2000).

However, Bluetooth has the potential for being much more than a wire replacement technology and the Bluetooth standard was indeed drafted with such a more ambitious goal in mind. Bluetooth holds the promise of becoming the technology of choice for adhoc networks of the future. This is in part because its low power consumption and potential low cost make it an attractive solution for the typical mobile devices used in adhoc networks. Bluetooth is a specification for Wireless Personal Area. It is a way to connect and exchange information and data between mobile phones, laptops, digital cameras and video games. The communication is wireless and has the range of up to 10 meters. Imagine the situation, you go to your office, you connect your notebook to the LAN port, you switch it on, it goes through the entire process of booting up and then transfer the data to your desktop computer this around process takes around 10-15 minutes, depending upon the speed of your notebook. Bluetooth will also enables to transfer files, photos and songs from the mobile to other device. The Bluetooth comes in with a wireless headsets and it comes in free with the mobile phone or computer, the wireless headset also useful for people who like to be on the go or while driving the car, as they are hands free Scarfone, K. & Padgette, J. (September 2008).

IMPLEMENTATION OF BLUETOOTH TECHNOLOGY

Bluetooth operates at frequencies between 2402 and 2480 MHz, or 2400 and 2483.5 MHz including guard bands 2 MHz wide at the bottom end and 3.5 MHz wide at the top. This is in the globally unlicensed (but not unregulated) industrial, scientific and medical (ISM) 2.4 MHz short-range radio frequency band. Bluetooth uses a radio technology called frequency-hopping spread spectrum. Bluetooth divides transmitted data into packets, and transmits each packet on one of 79 designated Bluetooth channels. Each channel has a bandwidth of 1 MHz. It usually performs 800 hops per second, with Adaptive Frequency-Hopping (AFH) enabled. Bluetooth Low Energy uses 2 MHz spacing which accommodates 40 channels.

Originally, Gaussian frequency-shift keying (GFSK) modulation was the only modulation scheme available. Since the introduction of Bluetooth 2.0+EDR, $\pi/4$-DQPSK (differential quadrature phase shift keying) and 8DPSK modulation may also be used between compatible

devices. Devices functioning with GFSK are said to be operating in basic rate (BR) mode where an instanteous bit rate of 1 Mbit/s is possible. The term Enhanced Data Rate (EDR) is used to describe $\pi/4$ DPSK and 8DPSK schemes, each giving 2 and 3 Mbit/s respectively. The combination of these (BR and EDR) modes in Bluetooth radio technology is classified as a "BR/EDR radio".

Bluetooth is a packet-based protocol with a master/slave architecture. One master may communicate with up to seven slaves in a piconet. All devices share the master's clock. Packet exchange is based on the basic clock, defined by the master, which ticks at 312.5 μs intervals. Two clock ticks make up a slot of 625 μs and two slots make up a slot pair of 1250 μs. in the simple case of single-slot packets, the master transmits in odd slots. Packets may be 1, 3 or 5 slots long, but in all cases the master's transmission begins in even slots and the slave's in odd slots.

COMMUNICATION AND CONNECTION

A master BR/EDR Bluetooth device can communicate with a maximum of seven devices in a piconet (an ad-hoc computer network using Bluetooth technology), though not all devices reach this maximum. The devices can switch roles, agreement, and the slave can become the master (for example, a headset initiating a connection to a phone necessarily begin as master – as an initiator of the connection - but may subsequently operate as the slave).

The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatter net, in which certain devices simultaneously play the master role in one piconet and the slave role in another.

At any given time, data can be transferred between the master and one other device (except for the little-used broadcast mode). The master chooses which slave device to address; typically, it switches rapidly from one device to another in a round-robin fashion. Since it the master that chooses which slave to address, whereas a slave is (in theory) supposed to listen in each receive slot, being a master is a lighter burden than being a slave. Being a master of seven slaves is possible; being a slave of more than one master is possible. The specification is vague as to required behavior in scatter nets.

HOW BLUETOOTH WORKS

Bluetooth establish connection using Radio waves signal, it broadcast its signal at Radio frequency of 2.45 Gigahertz. The picture to the immediate right is the Bluetooth radio chip that provides the communication between devices. Once the hardware radio chip is installed on two electronic devices, wireless communication can be established hopping channels up to 1600 times per second. Because Bluetooth is using Radio waves to achieve communication, the main chip operates with frequency hopping and thus does not need a clear path between two devices Newton (2007).

The control of communication aspect is more complicated and software plays an important role to control communication. Every main Bluetooth chip has an identify coding and different types of links. Both of these characteristics of the chip allow two different devices to communicate. Two devices must have the same type of linkage in order to establish communication.

The concept behind a Bluetooth communication is the use of masters and slaves. The master works as the moderator between communication between itself and the slave as well as between the slaves themselves. The Bluetooth network can link up to eight devices with this use of masters and slaves. This type of network is referred to as a piconet. As a connection needs to be made between two slaves, then one slave will “act” as a master and communicate to the other slave while still maintaining connection to the original master.

The software will first send a page from the master to the slaves and the slaves will listen for its device access code. If there is a match, then a connection is established. Once this connection is established, then a NULL packet is sent from the master to the slave and the master must wait for the slave to respond. At this point, the Link Manager Protocol (LMP) takes over. The LMP is comprised of Madatory Protocol Data Units and these are transferred between devices through a single packet. When a connection is requested, the requesting device must send LMP host connection req. the requested device can respond with either LMP accepted or LMP not accepted. Once the linkage is complete, LMP setup complete is sent and packets are transmitted.

BLUETOOTH PROFILE

To use Bluetooth wireless technology, a device must be able to interpret certain Bluetooth profiles, which are definitions of possible applications and specify general behaviors that Bluetooth-enabled devices use to communicate with other Bluetooth devices. These profiles

include settings to parameterize and to control the communication from the start. Adherence to profiles saves the time for transmitting the parameters anew before the bi-directional link becomes effective. There are a wide range of Bluetooth profiles that describe many different types of applications or use cases for devices Juha T. and Vainio (2000).

LIST OF APPLICATIONS

- Wireless control and communication between a mobile phone and a handset. This was one of the earliest applications to become popular. Kurawar, Arwa; Koul, Ayushi; Patil, Viki Tukaram (August 2014).
- Wireless control of and communication between a mobile phone and a Bluetooth compatible car stereo system.
- Wireless control of and communication with IOS and Android device phones, tablets and portable wireless speakers.
- Wireless Bluetooth headset and Intercom. Idiomatically, a headset is sometimes called " a Bluetooth".
- Wireless streaming of audio to headphones with or without communication capabilities.
- Wireless streaming of data collected by Bluetooth-enabled fitness devices to phone or PC.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communication with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of files, contact details, calendar appointments and reminders between devices with OBEX.
- Replacement of previous wired RS-232 serial communications in test equipment, GPS receivers, medical equipment, bar codes scanners, and traffic control devices.
- For controls where infrared was often used.
- For low bandwidth applications where higher US bandwidth is not required and cable free connection desired.
- Sending small advertisements from Bluetooth-enabled advertising hoardings to other discoverable Bluetooth devices Kurawar, Arwa; Koul, Ayushi; Patil, Viki Tukaram (August 2014).

SECURITY ARCHITECHTURE

Bluetooth security supports three security modes such as model (non-secure), mode 2 (Service-level), mode 3 (Link-level security) and different security level for devices and services which are:

Devices: Johnson (2002)

1. Trusted-unrestricted access
2. Not trusted-restricted access

Services:

1. Require authentication and authorization
2. Authentication only
3. Open to all devices

Also every Bluetooth chip has four security identifiers which make up at the link level and these identifiers are:

1. Bluetooth Device Address (BD-AAR) which is a 48-bit address and this is a unique address for in every Bluetooth chip.
2. Authentication Key which is a 128-bit random number and it is used for authentication purpose.
3. Encryption Key which is an 8 to 128-bit length key and it is used for encryption purposes.
4. Random Number which is a 128-bit random number and it is used for security purposes, it will change often, K. & Padgette, J. (September 2008).

KEY MANAGEMENT

When two or more Bluetooth devices establish together, the first link between each two devices must be established by the link key. This link key is a 128-bit random number and it is also encryption key. It is depending on the type of application, this link can be one of the following:

Unit Key	E21 (Unit and combination keys generation).	Generated while initialization of link occurs. Stored in memory. Used when one device wishes to use the other's unit key.
Combination Key	E21 (Unit and combination keys generation)	Generated by both devices. Devices exchange their random numbers and calculate

		combination key.
The Personal Identification Number is part of the E21 algorithm which is the algorithm that first establishes a connection between two devices (initialization key).		
Master Key	E22 (Initialization and master keys generation).	Generated by the master device. Temporarily used by devices, then purged.

Alzieu, Vincent (2003)

ENCRYPTION

The encryption is an essential part of Bluetooth security. The encryption key can vary between 8 and 128 bits. The user does not have access to change the size of the encryption as the key size must be specified by the manufacturer according to the countries regulations. A random number must be sent from one device to the other is any two Bluetooth devices wish to start the communication. The receiving device must also have knowledge of the PIN from the sending devices. With these two sets of information, a link key is generated (as above) on both devices. The sender would then have to enter in their PIN on receiver device manually or by a key exchange mechanism Juha T. Vainio (2000).

AUTHENTICATION

Bluetooth authentication is to ensure that the information sent to a device or party is coming from an authorized device. The way of authentication is to verify if the link keys are equal the sender must generate another random number and encrypts the Bluetooth Device Address (of the receiver) using the link key and the random number to produce a signed response authentication result (SRES). The sender sends the new random number and encrypts it to also produce a SRES. At last, a connection is established if those two random numbers are equal.

RECOMMENDATIONS

i) A mature implementation of the technology would have students using their mobile devices actively during their studies on campus and other places.

ii) A wide spread implementation would ensure a wide usage and encompassing strategies to make better use of the potential of the transient technology that works in and out of the campus everyday but which few organization rarely make effective use of.

REFERENCES

Alzieu, Vincent (2003) Bluetooth: A Rundown" Tom's Hardware. 28 March 2003

Andreas Becker (16 August 2007) "Bluetooth Security & Hacks" (PDF). Ruhr-Universitat Bochum. Retrieved 10 October 2007.

Bluetooth – An Overview 2002. Johnson Consulting. 02 September 2002.

Bluetooth Security Juha T. Vainio 2000. Helsinki University of Technology 25 May 2000

Juha T. Vainio (2000). "Bluetooth Security" (PDF). Helsinki University of Technology. Retrieved 1 January 2009.

Kurawar, Arwa; Koul, Ayushi; Patil, Viki Tukaram (August 2014). "Survey of Bluetooth and Applications". International Journal of Advanced Research in Computer Engineering & Technology. 3: 2832-2837. ISSN 2278-1323

Lamm, Gregory, gerlando Faluato, Jorge Estrada, Jag Gadiyaram (2002) "Bluetooth Wireless Networks Security Features". Proceedings of the 2001 IEEE Workshop on Information Assuarnce and Security. Online Available. March 2002.

Miller B and Bisdikian C. (2000) Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications.

Mroz, Mandy (2018-05-21). "Bluetooth hearing aids: Hearing aids with Bluetooth technology use today's wireless technology to help you easily stay connected to IOS and Android phones, televisions, tablets and other favorite audio devices". Healthy Hearing

Newton, Harold (2007) newton's telecom dictionary. New York: Flatiron publishing

Stallings, William (2005) Wireless communication & networks. Upper Saddle River, NJ: Pearson Prentice Hall

Scarfone, K & Padgette, J. (September 2008) "Guide to Bluetooth Security "(PDF). National Institute of Standards and Technology. Retrieved July 2013.

.

Yaniv Shaked; Avishai Wool (2 May 2005) "Cracking the Bluetooth PIN". School of Electrical Engineering Systems, Tel Aviv University. Retrieved 1 February 2007.

http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted-Abstracted/paperW2A2(26).pdf

http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted-Abstracts/paperW2A2(26).pdf