Software Engineering
4C03 Project Report

Bluetooth Technology

Name: Chun Yui Chan
Student No: 0055618
Date: March 29, 2005
Professor: Dr. K. Krishnan

Last Revision: March 25, 2004 (Security modifications, references added)

1. What is Bluetooth?

Bluetooth is one of the most efficient 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 everyday. Starting from communication between mobile phones and computers, Bluetooth has expanded to enable communication between such forms as headsets, printers and automobiles.

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.

1.1 How does Bluetooth Work?

Bluetooth establish connection using Radio waves signal, it broadcasts 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.

The control of communication aspect is more complicated and software plays an important role to control communication. Every main Bluetooth chip has an identity 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 Mandatory 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.

2. Security Architecture

Bluetooth security supports three security modes such as mode1 (non–secure), mode2 (Service-level), mode3 (Link-level security) and different security level for devices and service which are:

Devices:	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_ADDR) 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.

2.1 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 key 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.

2.2 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 if 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.

2.3 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.

3. Conclusion

Bluetooth technology has enabled wireless communication between various electronics and has been expanding everyday and more and more electronics come with the Bluetooth device. By using this newer hardware and smarter software algorithms to direct network data we can achieve more efficient, flexible wireless communications. However, the rapid development of Bluetooth, there has been a noticeable correlation burden on the existing security protocols, security systems always have their weakness, and there are still security issues that must be addressed and looked at in fine detail next time.

References

Lamm, Gregory, Gerlando Faluato, Jorge Estrada, Jag Gadiyaram. "Bluetooth Wireless Networks Security Features." Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. Online. Available. March 2002. http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW2A2(26).pdf

Bluetooth- An Overview. 2002. Johnson Consulting. 02 September 2002. <http://www.swedetrack.com/images/bluet04.htm>.

Bluetooth Security. Juha T. Vainio. 2000. Helsinki University of Technology. 25 May 2000. <http://www.niksula.cs.hut.fi/~jiitv/bluesec.html>.

Alzieu, Vincent. “Bluetooth: A Rundown.” Tom’s Hardware. 28 March 2003. <http://www.tomshardware.com/consumer/20030328/index.html>.