ISSN No. 0976-5697

Volume 4, No. 2, Jan-Feb 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Privacy in Bluetooth using Cryptographic Technique

Rajapraveen.K.N*
M.tech (C.S.E)
Dept. CSE, SSET, SHIATS – Deemed University
Allahabad,India
rajapraveen.k.n@gmail.com

Dr.N.K.Prasanna Kumari
NIMH,
Nagpur, India
prasanna_rcp@yahoo.co.in

Abstract: Bluetooth is a wireless device, composed of hardware and software with interoperability requirements. Bluetooth specifies short range of communication between mobile's and computer devices. by using cryptographic technique the transfer of date should me made secure.

Keywords: Bluetooth security, Security in Bluetooth, Privacy in Bluetooth, Cryptographic protection in Bluetooth, Bluetooth security

I. INTRODUCTION

Bluetooth technology is considered as cheapest, reliable, and efficient in replacement of cables for connecting short range electronic devices. Bluetooth technology was come into focus in summer 1999 since then it has wide usage in various electronic devices. Bluetooth technology is mostly used in the fields of telecommunications, computing, automotive, music, and network industries. [1] Bluetooth is a combination of both hardware and software technologies**.** Hardware technology is riding on a radio chip. Software implements main control and security protocols. By using both hardware and software, Bluetooth has become a smart technology for flexible wireless communication technology. Bluetooth radio chip supports communication among a group of electronic devices. Once the hardware radio chips are installed into the electronic devices, wireless communication will be established among devices. Operating distance between two Bluetooth devices ranges from 10 and 100 meters. By using a directional antenna and an amplifier the range of Bluetooth can be extended up to a mile.

Using Fast Frequency Hopping Sequence a Bluetooth device hops from one channel to another channel up to 1600 times in one Second. Bluetooth also uses Adaptive Frequency Hopping technique, designed to cope with excessive packet losses due to packet collisions or external interferences. Each Bluetooth chip has a unique identity code. [2] The 'master-slave' concept is the core of a Bluetooth based network. The 'master' works as the moderator during the communication between itself and the slave as well as among the slaves themselves. In Bluetooth a trusted relationship between two devices called 'pairing' are formed by exchanging shared secret codes referred to as PINs. A 'master' device has the option of pairing with up to seven 'slave' devices establishing a network called a piconet. Two or more piconets together form a scatternet, which can be used to eliminate Bluetooth range restrictions. A scatternet is formed when the devices act as 'master' or 'slave' devices in multiple piconets at the same time.

II. BLUETOOTH PROTOCOL STACKS

Bluetooth protocol stack is a combination of both software and hardware for implementation of the actual protocols. It also explains how Bluetooth devices communicate with each other Bluetooth device based on the standard. The Bluetooth protocol stack is shown in fig 1.

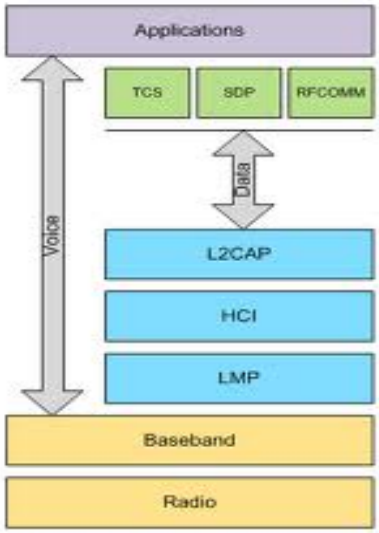

Figure 2: Bluetooth Protocol Stacks

Figure 1: Bluetooth protocol Stack

The protocols below the host controller interface (HCI) are built into the Bluetooth microchip and the protocols above the HCI are included in the host device's software package[7]. HCI ensures a secured communication between the host and the Bluetooth module. The radio layer transmits data in the form of bits by using a radio frequency. Base band layer performs the functions of frequency hopping for interference mitigation, medium access control and forming data packet. In addition, the baseband layer also controls link, channel, and error correction and flow control. It establishes two kinds of link depending on the application and operating environment[7]. A synchronous connection oriented (SCO) link is established to emulate circuit

switched connections for voice and data connection. While an asynchronous connection link (ACL) is defined for the data bursts. This link also supports broadcasting and data rate control by the master device.

The link manager (LM) acts as a liaison between the application and the link controller (LC) on the local device. It is also used for communication with the remote LM via protocol data units (PDU) and the link manager protocol (LMP). The audio protocol is used for a real time two way voice communication. The audio protocol is carefully located in such a way so that the overhead of upper layer protocols does not cause any delays for real-time two way voice connections. The logical link control and adaptation protocol (L2CAP) is a software module that normally resides in the host. It acts as a conduit for data on the asynchronous connection link (ACL) between the baseband and host applications.

The L2CAP is used to ensure both connection oriented and connection less services. Connection oriented service is used for communication between the master to one slave. Connection less service is used for communication between a master and multiple slaves. The L2CAP can initiate security procedures when a connection oriented or a connectionless connection request is made. The Object Exchange Protocol (OBEX) is used to exchange objects such as calendar notes, business cards and data files between devices based on a client-server model. The telephony control specification (TCS) defines the call control signaling for the establishment/release specific security protocols Bluetooth host security protocols Security protocols on Bluetooth hardware chip. Speech and data calls between Bluetooth devices. It also the service discovery protocol (SDP) discovers the services that are available in the RF proximity and determines the characteristic of these available services. SDP is an essential protocol that enables the Bluetooth devices to form an ad hoc network. RFCOMM is a transport protocol used to emulate the RS-232 serial ports. This protocol enables a Bluetooth device to connect with external devices like printers and scanners. The RFCOMM protocol relies on the baseband protocol stack to provide reliable in-sequence delivery of bit stream.

III. SECURITY ARCHITECTURE USING CRYPTOGRAPHIC TECHINIQUE (PUBLIC KEY ENCRYPTION)

Cryptography is the study of principle of encryption. By using cryptographic encryption technique [5], privacy protection in Bluetooth can be achieved. In this cryptographic technique public key encryption method plays an important role in providing privacy. Public key encryption[6]: it is also called two key encryption or Asymmetric encryption.

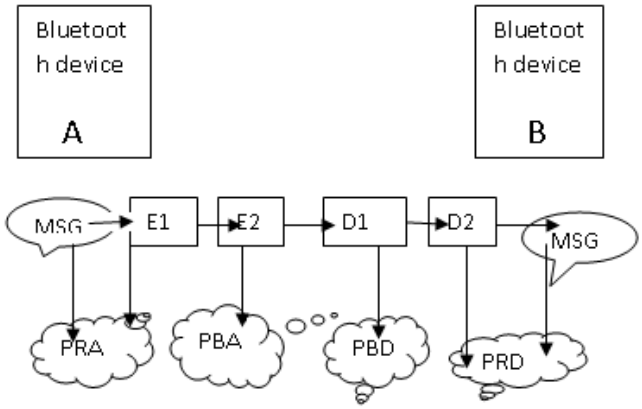

Figure 2: public key encryption between two Bluetooth devices

E1: Encryption of message with private key (PRA)
E2: Encryption of message with public key (PBA)
D1: Decryption of encrypted message using public key (PBD)
D2: Decryption of encrypted message using private key (PRA)

IV. ENCRYPTION PROCESS

The message sending from Bluetooth device 'A' to Bluetooth device "B", is encrypted by using private key encryption "PRA" and public key encryption "PBA", now the message is in encryption form when it reaches to Bluetooth device "B", the decryption process is just reverse to encryption method.[3] Message is decrypted in Bluetooth device by using public key "PBD" and "PRA" private key, the encrypted data sanded by Bluetooth device is successfully "A" is successfully decrypted by Bluetooth device "B" by using public key encryption technique in cryptography[4].

V. DISCUSSION

Bluetooth technology is very useful for all wireless systems. by using this wireless technology it is very much feasible for transfer of data with in short range of span, due to transfer of private data certain security protocols should be implemented, by using this cryptographic technique the private data is secure in transfer of date from one Bluetooth device to another Bluetooth device.

VI. CONCLUSION

This overview of this paper is some of the major attacks that are taking place in Bluetooth device that can be reduced by using cryptographic public key encryption technique. By using this method of encryption of data in Bluetooth, user can able to send his private information with privacy protection (safely).

VII. ACKNOWLEDGEMENT

I sincerely convey my thanks to my beloved Vice – chancellor & our founder, first Bishop YESHU DARBAR,

Rev. Fr. Prof.(Dr.) Rajendra B. Lal for his guidance ,support and help in each and every aspect , and I also convey my thanks to my mother and grandmother Mrs.Swarnalatha.N & M. Amulya Prema for their parental guidance.

VIII.REFERENCES

[1]. N. Ravindran, IT Applications for Health Care: Leverage processes for high quality set labs briefings (2008)

[2]. I. Howitt, IEEE Bluetooth Performance in the Presence of 802.11b WLAN. IEEE Transactions on Vehicular technology, vol. 51. 6, 2002 p. 1640-1651.

[3]. G. Julius Caesar, JF. Kennedy Security Engineering: A Guide to Building Dependable Distributed Systems p 73-114.

[4]. W. Diffie and M. E. Hellman New Directions in Cryptography *Invited Paper p 29-39.*

[5]. T. Duong and J. Rizzo Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET (2011) IEEE Symposium on Security and Privacy p 481-489.

[6]. T. Anan, K. Kuraki, and J. Takahashi Paper encryption technology Fujitsu Sci. Tech. (2010) Vol. 46. 1, p. 87-94.

[7]. Nateq Be-Nazir Ibn Minar and Mohammed Tarique,blue tooth security threats and solution :a survey; International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012

