ISSN No. 0976-5697

Volume 3, No. 1, Jan-Feb 2012

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review paper on Architechture and Security system of Bluetooth Transmission

Mrs. Trishna Panse*
Department of Information Technology
Institute of Engineering & Technology, DAVV
Indore, India
trishna_shri@rediffmail.com

Prof. Vivek Kapoor
Department of Information Technology
Institute of Engineering & Technology, DAVV
Indore, India
vkapoor13@yahoo.com

Abstract: In this paper we will attempt to provide understanding of what Bluetooth is and how security mechanism work in existing Bluetooth communication. Bluetooth is a method for data communication that uses short-range radio links to replace cables between computers and their connected units. A Bluetooth technology consist of radio technology, a protocol stack and interoperability profiles. The basic features of Bluetooth are robustness, low complexity, Adhoc in nature and low cost. It is the most popular technique among the generation to fast transfer of data. Different communication ranges are available in this technique such as low (upto 1 meter), medium (upto 9 meter) and high (upto 91 meter). Bluetooth security uses authentication, authorization & encryption to attain security in communication.

Keywords: Bluetooth security; E0 stream cipher; Bluetooth Architecture; Security challenges in Bluetooth;

I. INTRODUCTION

a. *Bluetooth Architecture and Protocols:*

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology was designed primarily to support simple wireless networking of personal consumer devices and peripherals, including cell phones, PDAs, and wireless headsets.[1]

The architecture of the Bluetooth is divided into several layers, varying in their functions and illustrated in Fig. 1.

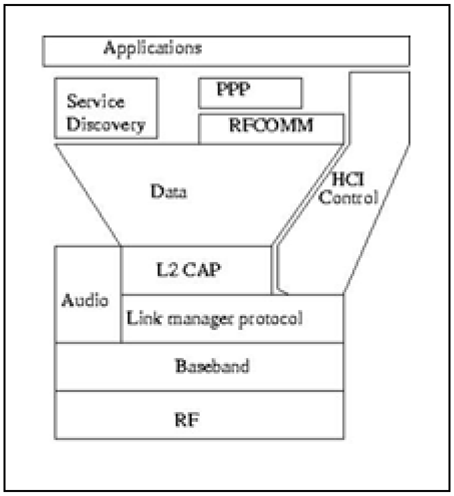

Figure. 1: Bluetooth architecture

A. *Radio Frequency (RF) Layers:*

The radio layer is the physical wireless connection. In order to reduce collisions with other devices using the ISM range, the radio uses frequency mapping to separate the range into 79MHz bands, starting at 2.402GHz and stopping at 2.480Hz and uses this spread spectrum to hop from one channel to another, up to 1600 times per second.

B. *Base band layer:*

The base band allows the physical connection between devices. It is responsible for controlling and sending data packets over the radio link. When a Bluetooth device connects to another Bluetooth device, they form a small network called a piconet. A piconet is a small network of Bluetooth devices, where every device in the network can be in one of the following states.

a. ***Master***: The Bluetooth device that initiates communication. The master sets the time and broadcasts its clock to all slaves providing the hopping pattern, in which they hop frequency at the same time.
b. ***Slaves***: The state given to all devices that are connected to another. The device can be an active slave if it actively transmits or receives data from the master, or a passive slave if it is not currently sending or receiving any information. The passive slaves check if there is a connection request from the master by enabling their RF receivers periodically.
c. ***Standby***: All devices that are not connected to a master (i.e. not slave) are called standby devices. When searching for other devices, a device enters the inquiry state. When a device starts creating a Bluetooth link, it enters the page state. Also a device can go to a low power mode to save power.

C. *Link 2 Manager Protocol (LMP):*

The LMP protocol uses the links set up between devices by the base band to establish logical connection responsibilities of the LMP. It also includes security aspects and device authentication.

D. *Logical Link Control and Adaptation Protocol (L2CAP):*

The L2CAP is responsible for receiving applicative data from the upper layers and translates it to the Bluetooth format so that it can be transmitted to the higher layer protocol over the base band.

E. Radio Frequency Communication Protocol (RFCOMM):

The RFCOMM is used to emulate serial connections over the base band layer to provide transport capabilities for upper level services and avoiding direct interface of the application layer with L2CAP.

F. Service Discovery Protocol (SDP):

The SDP protocol is used to discover services, providing the basis for all the usage models. SDP allows Bluetooth a device to ask other devices for its services, so it can know the characteristics of the services. Accordingly suitable connections can be established between two or more devices.

G. Telephony Control and Signaling layer (TCS):

The TCS protocol defines the call control signaling for the establishment of speech and data calls between Bluetooth devices. TCS signaling messages are carried over L2CAP.

H. Application Layer:

The application layer contains the user application. The applications interact with the RFCOMM protocol layer to establish an emulated serial connection. [2]

II. BLUETOOTH SECURITY

a. ***Encryption***: The encryption algorithm using in Bluetooth encryption process is the E0 stream cipher. However, this algorithm has some shortcomings; 128-bit E0 stream ciphers in some cases can be cracked. So, for most applications that which need to give top priority to confidentiality and integrity, the data security is not enough if only use Bluetooth. The Fig. 2 shows the E0 stream cipher system. [3]

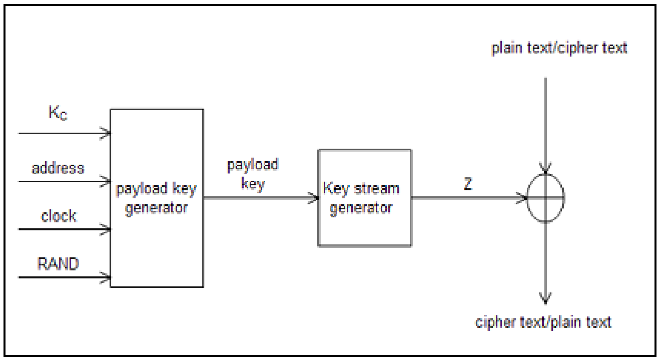

Figure. 2: Stream Cipher system E0

b. ***Authentication***: The Bluetooth authentication scheme uses a challenge-response strategy as shown in Fig. 3, where a 2-move protocol is used to check whether the other party knows the secret key. The protocol uses symmetric keys, so a successful authentication is based on the fact that both participants share the same key. The Authenticated Ciphering Offset (ACO) is computed and stored in both devices and is used for cipher key generation later on. The verifier sends the claimant a random number to be authenticated. Then, both participants use the authentication function E1 with the random number, the claimants Bluetooth Device Address and the current link key to get a response. [3]

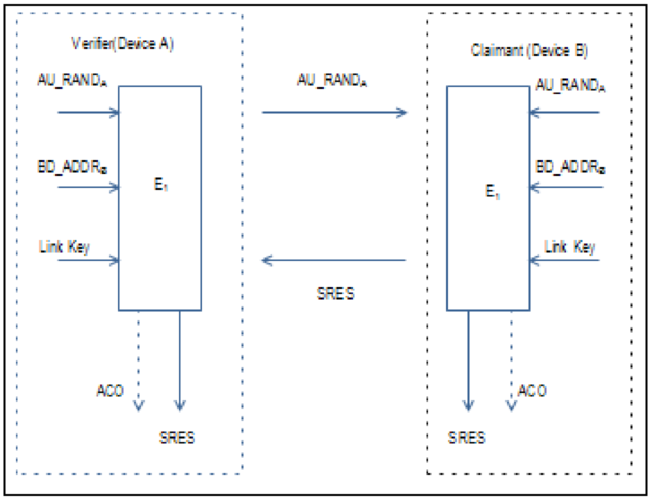

Figure. 3: Challenge – Response for Bluetooth

A. Keys used in Bluetooth security:

a. ***Unit Keys:*** The authentication and encryption mechanisms based on unit keys are the same as those based on combination keys. However, a unit that uses a unit key is only able to use one key for all its secure connections. Hence, it has to share this key with all other units that it trusts. Using a unit key there is no protection against attacks from trusted devices. [4]

b. ***Combination Keys:*** The combination key is generated during the initialization process if the devices have decided to use one. Both devices generate it at the same time. First, both of the units generate a random number. With the key generating algorithm E21, both devices generate a key, combining the random number and their Bluetooth device addresses. After that, the devices exchange securely their random numbers and calculate the combination key (K_{ab}) to be used between them as shown in Fig 4.

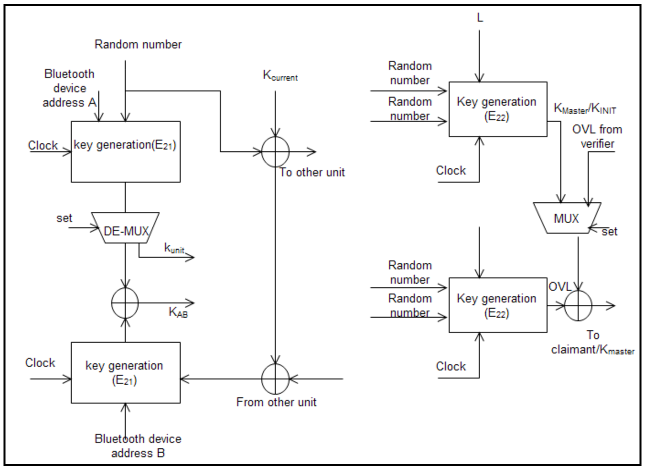

Figure. 4: Link Key Generation function unit

c. ***Encryption keys:*** The encryption key is generated from the current link key, a 96-bit Ciphering Offset Number (COF) and a 128-bit random number. The COF is based on the Authenticated Ciphering Offset (ACO), which is generated during the authentication process. When the Link Manager (LM) activates the encryption, the encryption key is generated. It is automatically changed every time the Bluetooth device enters the encryption mode. [5]

III. CHALLENGES IN BLUETOOTH SECURITY SYSTEM

a. ***Low credibility of PIN:*** Bluetooth technology uses non-standard 4-digit PIN code and another variable to generate the link key and encryption key. Actually, 4-digit PIN code is the only variable which is the real key generated, resulting only one key (a random number) transport in the air.

b. ***High probability of non-link key cheat:*** Along with the use of the link key takes new problems. Authentication and encryption set up on the basis of the link key. All the other Information used in this connection usually is public.

c. ***Address Spoofing:*** Every Bluetooth device has a unique Bluetooth device address. However, its uniqueness raises new problems. Once the ID links with a certain fixed person, this person can be tracked and their activities can easily be recorded. In this case, the individual's privacy will be violated.

d. ***The weakness of E0 stream cipher algorithm:*** the main weakness of stream cipher algorithm is that if a pseudo-random sequence make an error, it will make the whole cipher text mistake happen, it also bring about the cipher text cannot restore back to plaintext in decipherment.[7]

IV. RELATED RESEARCH WORK

A. Li Juan, Chen Bin, Li Kun in 2009[6] proposed a solution against weaknesses in current Bluetooth security system. This paper uses DES algorithm.

B. Wuling Ren, Zhiqian Miao in 2010[7] proposed a solution to the shortcomings in existing Bluetooth security system. In this paper they discuss the hybrid mechanism using DES and RSA algorithm.

C. Markus Jakobsson and Susanne Wetzel [8] discussed the security weakness in Bluetooth and suggest counter – measures.

V. CONCLUSION

We have presented an overview of the existing security mechanism in the Bluetooth communication. Also discuss the encryption and decryption techniques. Currently used Security mechanisms have some problems. There is a need to enhance the existing security system used in Bluetooth data transmission. In Bluetooth security improvement area lots of research work has to be carried out which is discussed in this paper.

VI. ACKNOWLEDGMENT

The authors thank editor-in-chief and anonymous reviewers for their comments and suggestions. The work is supported by the Science & Technology Research Program of Zhejiang Province, China (No.2009C03016-4, 2008C01060-2).

VII. REFERENCES

[1] Karen Scarfone John Padgette,Guide to Bluetooth Security, National Institute of Standards and Technology, U.S. Department of Commerce.

[2] Silan Liu,Bluetooth Technology, Bluetooth Technology layers.htm#_Toc41989838.

[3] Antnan ,Bluetooth Security, Communication Security Department,Ruhr University,Bochum.

[4] Christian Gehrmann, Bluetooth™ Security White Paper, Bluetooth SIG Security Expert Group.

[5] Paraskevas Kitsos, Nicolas Sklavos,Kyriakos Papadomanolakis, and Odysseas Koufopavlou, Hardware Implementation of Bluetooth Security,*University of Patras, Greece.*

[6] Li Juan, Chen Bin, Li Kun,Electronic Engineering College, Naval University of Engineering Wuhan, China, Study on the Improvement of Encryption Algorithm of Bluetooth, 2009 International Conference on Networking and Digital Society.

[7] Wuling Ren, Zhiqian Miao, College of Computer and Information Engineering, Zhejiang Gongshang University, *A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication* Second International Conference on Modeling, Simulation and Visualization Methods, 2010.

[8] Markus Jakobsson and Susanne Wetzel, Lucent Technologies – Bell Labs, Information Sciences Research Center, Murray Hills, NJ 07974 USA, Security Weaknesses in Bluetooth.