ISSN:0975-9646

A Review on Security Mechanism of Bluetooth Communication

Trishna Panse, Vivek Kapoor

Department of Information Technology, Devi Ahilya Vishwavidyalaya
Institute of Engineering & Technology, Indore, India

Abstract— In this article we present a survey on security mechanism used in Bluetooth communication**.** Bluetooth is the personal area network (PAN).It is the kind of wireless Ad hoc network. Low cost, low power, low complexity and robustness are the basic features of Bluetooth. It works on Radio frequency. Bluetooth communication range is categorized as high, medium and low depending upon power level. High range of Bluetooth communication is up to 91 meter, medium range is up to 9 meter and low range is up to 1 meter. Authentication and Encryption are the key security features that are used at the link level in Bluetooth communication. A secret link key is used to achieve these security features which is shared between two Bluetooth devices.

***Keywords*— Bluetooth security; E0 key stream; encryption; authentication; keys**

I. INTRODUCTION

There are three methods used for connecting Bluetooth devices.

1. Voice/ Data Access Points: This model involves connecting a computing device to a communications device or a wireless link in order to share the communication connection with the non-peripheral device.

2. Peripheral Interconnect: In this method peripheral devices such as the keyboard, mouse and headsets can be connected to other types of devices.

3. Personal Area Networking (PAN): This model provides a method for connecting devices with each other in an ad hoc fashion which makes the transfer of data easy and fast.

Bluetooth Architecture and Protocols

The architecture of the Bluetooth technology is divided into several layers, varying in their functions and illustrated in Figure1.

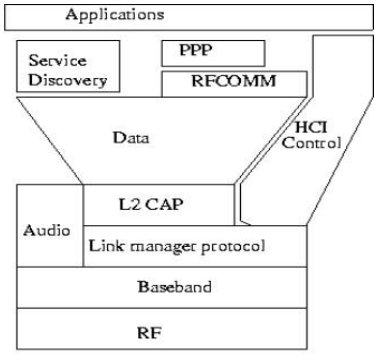

Fig. 1 Bluetooth architecture

1. 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.

2. 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.

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.

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.

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.

3. 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.

4. Logical Link Control and Adaptation Protocol (L 2CAP)

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.

5. 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.

6. Service Discovery Protocol (SDP)

The SDP protocol is used to discover services, providing the basis for all the usage models.

7. 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.

8. Application Layer

The application layer contains the user application. The applications interact with the RFCOMM protocol layer to establish an emulated serial connection. [1]

II. Bluetooth Security

Security for Bluetooth is provided on the radio paths, which means that link authentication and encryption may be provided, but true end-to-end security is not possible without providing security solutions for the higher layers of Bluetooth. Basically, Bluetooth addresses the three security services:

Confidentiality: The first goal of Bluetooth is confidentiality or privacy. This service prevents an eavesdropper from reading critical information. In general, with this security service only the authorized user can access the data.

Authentication: Providing identity verification of the communicating devices is the second goal of Bluetooth. Authentication allows the communicating devices able to recognize each other; hence communication aborts if the user is not authorized.

Authorization: The third goal of Bluetooth is to control access to the resources. This is achieved by determining the users who are authorized to use the resources.

Keys used in Bluetooth security

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. Consequently, all trusted devices are able to eavesdrop on any traffic based on this key. A trusted unit that has been modified or tampered with could also be able to impersonate the unit distributing the unit key. Thus, when using a unit key there is no protection against attacks from trusted devices.[3]

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 2

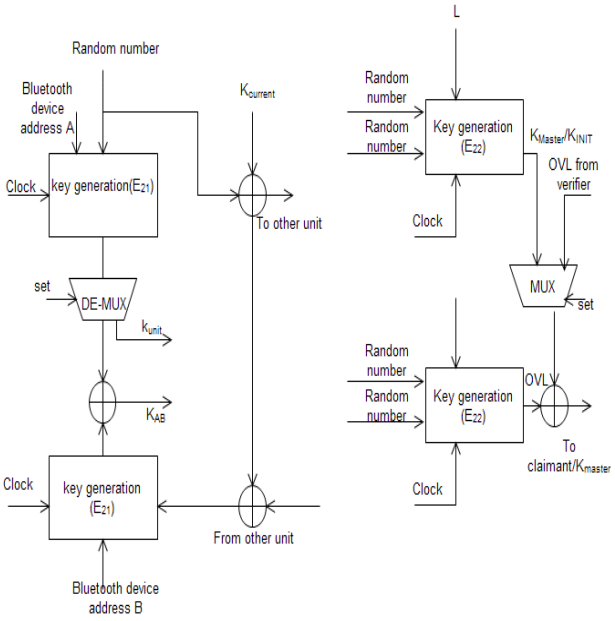

Fig 2: Link Key generation

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.[2]

III. Key Management

Prepare Your All security transactions between two or more parties are handled by the link key. The link key is a 128- bit random number. It is used in the authentication process and as a parameter when deriving the encryption key. The lifetime of a link key depends on whether it is a semi-permanent or a temporary key. A semi-permanent key can be used after the current session is over to authenticate Bluetooth units that share it. A temporary key lasts only until the current session is terminated and it cannot be reused. Temporary keys are commonly used in point-to- multipoint connections, where the same information is transmitted to several recipients. The length of the Personal Identification Number (PIN) code used in Bluetooth devices can vary between 1 and 16 octets. The regular 4-digit code is sufficient for some applications, but higher security applications may need longer codes. The PIN code of the device can be fixed, so that it needs to be entered only to the device wishing to connect. Another

possibility is that the PIN code must be entered to the both devices during the initialization.

IV. Encryption

The Bluetooth encryption system encrypts the payloads of the packets. This is done with a stream cipher E0, which is re-synchronized for every payload. The E0 stream cipher consists of the payload key generator, the key stream generator and the encryption/decryption part. The payload key generator combines the input bits in an appropriate order and shifts them to the four Linear Feedback Shift Registers (LFSR) of the key stream generator. The payload key generator combines the input bits in an appropriate order and shifts them to depending on whether a device uses a semi-permanent link key or a master key; there are several encryption modes available. If a unit key or a combination key is used, broadcast traffic is not encrypted. Individually addressed traffic can be either encrypted or not. If a master key is used, there are three possible modes. In encryption mode 1, nothing is encrypted. In encryption mode 2, broadcast traffic is not encrypted, but the individually addressed traffic is encrypted with the master key. And in encryption mode 3, all traffic is encrypted with the master key.[2]

As the encryption key size varies from 8 bits to 128 bits, the size of the encryption key used between two devices must be negotiated. In each device, there is a parameter defining the maximum allowed key length. In the key size negotiation, the master sends its suggestion for the encryption key size to the slave. The slave can either accept and acknowledge it, or send another suggestion. This is continued, until a consensus is reached or one of the devices aborts the negotiation. The abortion of the negotiation is done by the used application. In every application, there is a defined minimum acceptable key size, and if the requirement is not met by either of the participants, the application aborts the negotiation and the encryption cannot be used. This is necessary to avoid the situation where a malicious device forces the encryption to be low in order to do some harm.[4]

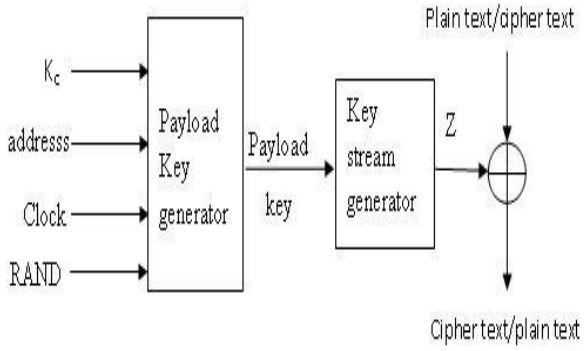

Fig 3: The Stream Cipher System E_0

V. Authentication

The Bluetooth authentication scheme uses a challenge-response strategy, 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. The claimant sends the response to the verifier, who then makes sure the responses match. The used application indicates who is to be authenticated. So the verifier may not necessarily be the master. Some of the applications require only one-way authentication, so that only one party is authenticated. This it not always the case, as there could be a mutual authentication, where both parties are authenticated in turn. If the authentication fails, there is a period of time that must pass until a new attempt at authentication can be made. The period of time doubles for each subsequent failed attempt from the same address, until the maximum waiting time is reached. The waiting time decreases exponentially to a minimum when no failed authentication attempts are made.[2]

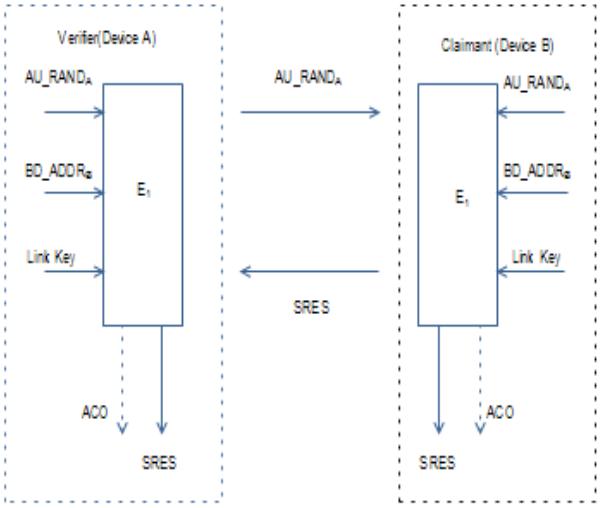

Fig 4: Challenge response for Bluetooth

VI. Security Modes of Bluetooth

Security Mode 1- This is the most insecure security mode in which the Bluetooth device does not initiate any security procedure, allowing other Bluetooth devices to initiate connections with it.

Security Mode 2- This mode enforces security after establishment of the link between the devices at the L2CAP level. This mode allows the setting up of

flexible security policies involving application layer controls running in parallel with the lower protocols.

Security Mode 3- This mode enforces security controls such as authentication and encryption at the Baseband level itself, before the connection is set up. The security manager usually enforces this onto the LMP. Bluetooth allows security levels to be defined for both devices and services. For devices there are two possible security levels. A remote device could either be a: 1. Trusted device-Such a device would have access to all services for which the trust relationship has been set. 2. Untrusted device-Such a device would have restricted access to services. Typically such devices would not share a permanent relationship with the other device.

VII. BLUETOOTH THREATS AND SECURITY TIPS

A. Bluesnarfing is a method of hacking into a Bluetooth enabled mobile phone and copying its entire contact book, calendar or anything else stored in the phone's memory.

B. Man in the Middle Attacks In a man in the middle attack, an attacker seeking (unauthorized) access to a Bluetooth device inserts himself "in between" two authorized devices Communications between the two devices then pass through the man in the middle, who intercepts and manipulates data packets.

First Bluetooth virus, Series 60 affected Jun 15 2004: Symantec warns of a worm for Series 60 mobile phones that transmits itself through Bluetooth. It's just a proof-of-concept (doesn't do any damage), but it's a scary concept.

C. Virus: METAL Gear.a for Series 60 Dec 21 2004: Another new security notice for Series 60 owners--avoid a file claiming to be the game Metal Gear Solid with the file name METAL Gear.sis.

SECURITY TIPS

- Enable Bluetooth only when you need it.
- Keep the device in non-discoverable (hidden) mode.
- Use long and difficult to guess PIN key when pairing the device.
- Reject all unexpected pairing requests.
- Update your mobile phone firmware to a latest version.
- Enable encryption when establishing BT connection to your PC.
- Update your mobile antivirus time to time to keep pace with the new emerging viruses and Trojans.

VIII. ACKNOWLEDGEMENT

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).

IX. REFERENCES

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

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

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

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