Ramification of Low Energy Security Enhancement Aspects in Bluetooth

Mrs.Sandhya S
Research Scholar, VTU
Department of MCA, RVCE
Bangalore, India
sandhyas@rvce.edu.in

Dr.Sumithra Devi K A
Professor and Director,
Department of MCA, R V C E
Bangalore, India
sumithraka@gmail.com

Abstract— **The advent of Bluetooth technology has made wireless communication easier. Bluetooth as a technology has evolved a lot over the years. Security in any area is given more importance as it leads to better product and satisfied customers. Bluetooth security has evolved a lot with different versions of blue tooth. Keeping in mind the growing list of Bluetooth products in the market, there has been lot of improvements done in the version 4.0 of Bluetooth. The LE (Low Energy) operational mode which is new in version 4.0 has slightly different security features. In this paper, an overview of the Low Energy security aspects is presented. The different security modes, authentication, authorization procedures and data signing procedure are discussed in detail. The paper concludes by listing the ramifications of low energy enhancements in Bluetooth.**

Keywords- *Bluetooth Low Energy, Data Signing, Static Address and Private Address*

I. INTRODUCTION

Bluetooth is a wireless communication technology for short range communications. Blue tooth was designed for low power consumption and data transfer in moderate rate over short ranges. The system operates in the 2.4 GHz ISM Band. This frequency band is 2400 – 2483.5 MHz. The technology allows the formation of Adhoc networks called piconets between two or more wireless devices. The connected devices communicate on the same physical channel with a common clock and hopping sequence. A number of independent piconets may exist in close proximity. This will mean that each piconet will have a different master device and an independent timing and hopping sequence. A blue tooth device may participate in two or more piconets at the same time. This is achieved using a process called time-division multiplexing. A blue tooth device cannot be a master of more than one piconet. But it can be a slave in many independent piconets [1].

Bluetooth v4.0 has come up with a new technology for low energy devices to communicate. The key features of this technology include very low power consumption, ability to run on standard coin cell batteries and low cost [1]. Bluetooth LE employs two access schemes: Frequency division multiple access (FDMA) and Time division multiple access (TDMA). Forty physical channels separated by 2 MHz are used in FDMA. There are 37 channels and 3 advertising channels. The physical channel is divided into time units called as events [1].

The remainder of this paper is devoted to look at the features of Bluetooth Low Energy module and the security features of Low Energy module. Section 2 overviews the security modes in Bluetooth Low Energy. Section 3 overviews the privacy feature enhancements in v4.0 and the process of generating and resolving random addresses. Section 4 discusses the advantages of Bluetooth low energy. Section 5 reviews the ramifications of this technology for vendors and users.

II. BLUETOOTH LOW ENERGY SECURITY

The security requirements of a device, a service or a service request are expressed in terms of a security mode and a security level. Each service may have its own security requirement. A physical connection between two devices shall operate in only one security mode [1]. Bluetooth Low energy technology has two security modes (mode1 and mode2).

Security Mode 1: The security mode 1 has three security levels.

1. No security (No authentication and No encryption)
2. Unauthenticated pairing with encryption
3. Authenticated pairing with encryption

A connection operating in LE security mode 1 in a higher level will also satisfy the security requirements of one of the lower levels in the same security mode. For ex; a connection operating in mode 1 level 2 will also satisfy the requirements for mode 1 level 1. A connection operating in mode 1 level 3 will also satisfy the requirements for mode 1 level 1 or mode 1 level 2 [1].

Security Mode 2: The security mode 2 has two security levels.

1. Unauthenticated pairing with data signing
2. Authenticated pairing with data signing

This mode shall only be used for connection based data signing. Data signing will not be used for connections using security mode 1 level 2 or level 3 [1].

Data Signing: Data signing is used for transferring data which is authenticated between two devices that is using an unencrypted connection. This is typically used by services that

require fast connection setup and fast data transfer. This is used by service requests that specify LE security mode [1].

Due to the limited resources available, the encryption through Elliptic curves Diffie-Hellman is not used. So, protection against passive eaves dropping is not present in LE. LE uses AES-CCM [2] that is also used in Wireless LAN. The encryption is in the controller but the key generation is in the host. This facilitates the change of key generation algorithm without changing the hardware. Numeric comparison IO capability is not available in LE [3].

LE security uses the following keys for encryption, signing and generating and resolving random addresses [1]

1. Identity Resolving Key (IRK) is a 128 bit key which is used to generate and resolve random addresses.
2. Connection Signature Resolving Key (CSRK) is a 128 bit key which is used to sign data and verify signatures.
3. Long Term Key (LTK) is a 128 bit key which is used to generate session key for an encrypted connection
4. Encrypted Diversifier (EDV) is a 16 bit stored value which is used to identify LTK.
5. Random Number (Rand) is a 64 bit value which is used to identify LTK.

III. PRIVACY FEATURE

There have been lots of privacy issues with respect to Bluetooth as the device addresses were constant. In order to make it difficult for the attackers to track a device, v4.0 introduces a new privacy feature through which devices can hide their real address and use random address that changes after a period of time. Thus the privacy is guaranteed by not revealing the real address [3].

Random Device Address: The random device address may be a Static address type or a Private address type. The Private address may be of one of the following sub-types

1. Non resolvable private address
2. Resolvable private address

Static Address: A static address is a 48 bit randomly generated address. It should meet the following requirements

1. Two most significant bits should be 1
2. All the bits of the address should not be equal to 0
3. All the bits of the address should not be equal to 1

The device can optionally choose to initialize the static address to a new value after each power cycle [1].

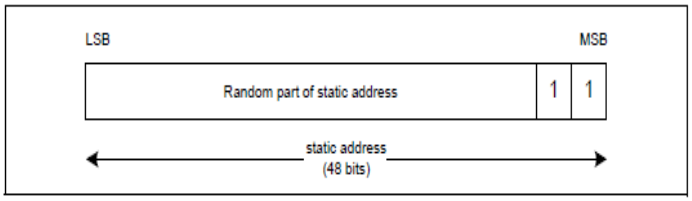

Fig 1. Format of Static Address

Non-resolvable Private Address: The original address of the device can never be identified in this method. The 48 bit address should meet the following requirements

1. Two most significant bits should be 0
2. All the bits of the address should not be equal to 0
3. All the bits of the address should not be equal to 1
4. The address shall not be equal to static address
5. The address shall not be equal to public address

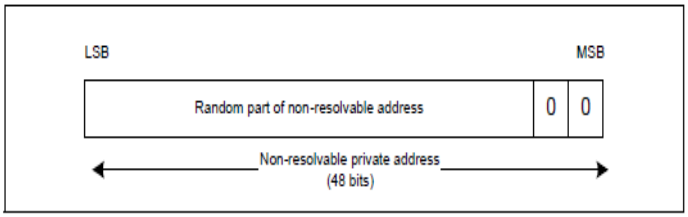

Fig 2. Format of Non-resolvable Private Address

Resolvable Private Address: The real address in this case can be derived from the random address and the link key of the connection. To generate a resolvable private address the host uses what is called a Identity Resolving Key (IRK). The resolvable private address is generated using IRK and a randomly generated 24 bit number [1]. The random number (prand) should meet the following requirements

1. The significant bit shall be equal to 0
2. The next significant bit shall be equal to 1
3. All the bits of the address should not be equal to 0
4. All the bits of the address should not be equal to 1

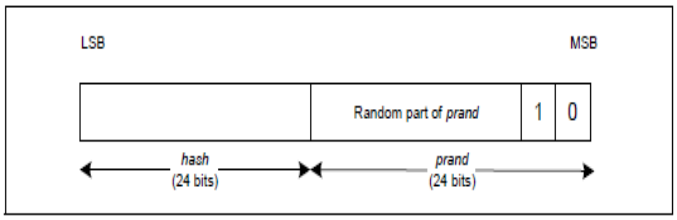

Fig 3. Format of Resolvable Private Address

Resolvable Private Address Resolution: In order to resolve the private addresses, the host should have the IRK for all the peer devices. The resolvable private address is divided into two parts; a 24 bit random part (prand) and another 24 bit hash part (hash). The least significant octet of the private address becomes the least significant octet of hash. The most

significant octet of the private address becomes the most significant octet of prand. A local hash value is then generated using the random address hash function with the IRK of the device and the prand part of the private address. The local hash value is then compared with the hash value generated from the private address. The identity of the device is known if the hash value matches [1].

IV. ADVANTAGES OF LOW ENERGY

There are other advantages of using Bluetooth LE apart from the very obvious which is the low energy consumption.

Reliability: This uses adaptive frequency hopping like classic Bluetooth and hence robust transmission is possible. Uses 40 two MHz wide channel as compared to classic Bluetooth which uses 79 one MHz channels.

Integration: Uses a simple start topology and fits very well with commonly used system architecture with a number of smaller devices connected to a master. The new advertising feature with LE enables the units to advertise frequently.

Range: LE has an approximately 3 dB better link budget compared to classic Bluetooth. A LE unit can offer a range of 200-300 meters though the actual range needed could be less than 100 meters.

Home Automation: Bluetooth LE can be used as a key in order to allow a mobile operator's panel to get access to the machine that is required to be monitored. This has wide spread usage in home automation solutions [4].

V. RAMIFICATIONS

Bluetooth low energy technology has been designed to use lowest possible power and provide Bluetooth connectivity. The Bluetooth low energy unit can be put to sleep mode when it is used for sending active files to a PC or mobile phone. Bluetooth low energy technology has a very efficient and discovery and connection setup, very short packets and client-server architecture [4]. This has led to a situation where wireless can be used in very simple and inexpensive devices like sensors. With low energy technology, the Bluetooth device market is set to explode with an approximate estimate of more than 10 billion devices for a variety of applications that may include phone accessories, smart energy, home automation, animal tagging and industrial automation devices. The average power consumption is about 1uA. This means, a small coin cell is enough for 5-10 years of operation [4].

A lot is at stake for vendors who manufacture Bluetooth devices to cater to this market which has increased 3 to 4 times after introduction of Bluetooth LE.

Bluetooth low energy technology meets all the requirements of a wireless solution for sensors and actuators. The highlights of the usage of LE for sensors and actuators are:

1. Cost effective and stand alone solutions
2. Robustness inherited from classic Bluetooth
3. Long range
4. Very low power consumption
5. Fast connectivity
6. Low maintenance cost
7. Low latency
8. Start topology which is very simple

VI. CONCLUSION

Bluetooth is a very remarkable technology for communicating the wireless way. The introduction of Low Energy technology has opened up a lot of opportunities for the vendors as well as the users. The privacy feature enhancement in LE will go a long way in ensuring device privacy. Your current Bluetooth phone can't communicate with LE devices but future ones will be able to since they'll include Bluetooth BR and LE (dual mode) in the same chip. When a Bluetooth LE peripheral wants to come onto a BR network, the host will downshift to LE mode and be able to communicate with it. This compatibility will have to wait for the next generation of consumer devices that incorporate dual mode Bluetooth chips. With all these benefits, Bluetooth Low Energy is all set to be a major player in the low power wireless word.

REFERENCES

[1] Bluetooth, S. I. G. (2010). Bluetooth Core Specification v4.0. 30 June 2010 Available online at https:// www. bluetooth.org /Technical /Specifications/adopted.htm

[2] http://en.wikipedia.org/wiki/CCMP

[3] Gustavo Padovan, University of Campinas. Bluetooth Security

[4] Rolf Nilsson, ConnectBlue. Bluetooth low energy technology – the optimal solution for wireless sensors and actuators.