BLUETOOTH

A SECURE MODE OF DATA TRANSMISSION

1. Mr. Kausar Ali
Sr. Lecturer-ECE
VIT-Jaipur

2. Akshata Saxena
B. tech. 4th year-ECE
VIT-Jaipur

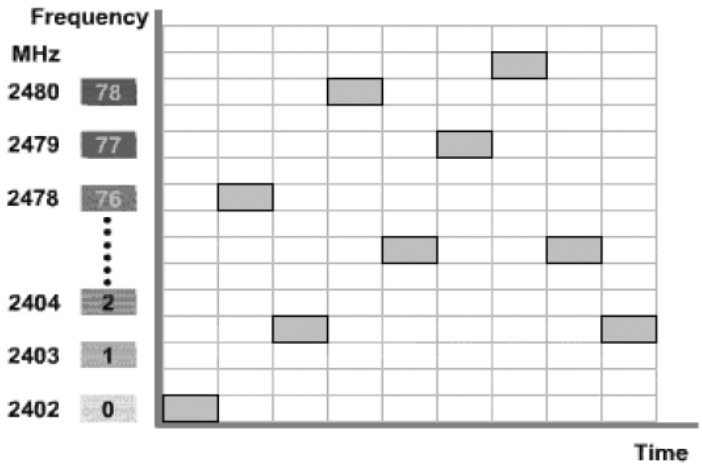
3. Meghna Mittal
B. tech. 4th year-ECE
VIT -Jaipur

INTRODUCTION

In today's scenario, the maximum utilisation of resources is required so we switched from wired communication to wireless communication and hence the invention of Bluetooth device took place. Bluetooth is a technology for wireless connections of short range devices and it operates in a unlicensed radio range of 2.402 - 2.480 GHz. Originally invented by Ericsson, it has been called after king Harald Bluetooth, a Danish Viking who lived during the 10th Century and unified Scandinavia. Later in 1998, IBM, Intel, Ericsson, Nokia, Toshiba formed the Bluetooth SIG, which serves as the governing body of the specification.

Bluetooth sets a high priority on small size, low power consumption, low cost, always on, short range, wireless technology for devices. Bluetooth devices can exchange data up to 723kbps.

wireless networking device. In order to avoid interference from these devices, Bluetooth uses a technology called frequency hopping spread spectrum(FHSS) spread spectrum frequency hopping changes transmission use and frequency up to 1600 times per second across 79 different frequencies with channel spacing of 1 MHz



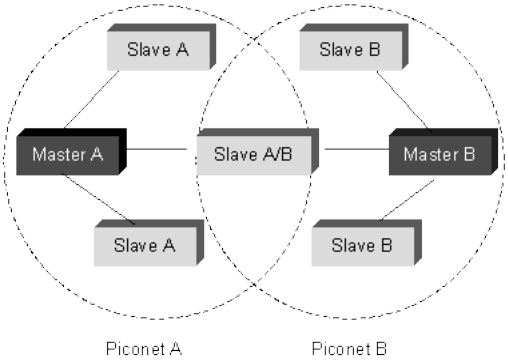
A sample FHSS distribution

BLUETOOTH TECHNOLOGY

Bluetooth is designed to operate in the unlicensed 2.4GHz industrial, scientific and medical application (ISM) frequency band.

This frequency is already used by some other device such as microwave ovens, baby monitors, cordless telephones and 802.11b/g

Bluetooth devices form ad hoc networks called piconet. In ad hoc network, devices are connect to each other rather than going through central access points so they don't have any centralized security control mechanism thus exposing important information on devices to other on Bluetooth networks .



An hoc networks of two or more Bluetooth devices is called a piconet. In these piconet, one of the Bluetooth devices acts as a master and the other are slaves. The master set the frequency –hopping behaviour of the piconets. It is also possible to connect up to 10 piconets to form so –called scatter nets.

2. CLASSES

There are three classes of Bluetooth devices, according to the power they use and the ranges they have .

TYPES	POWER	POWER LEVEL	OPERATING RANGE
CLASS 1 Devices	High	100mW (20 dbm)	Up to 100 meters
CLASS 2 Devices	Medium	2.5mW (4 dbm)	Up to 10 meters
CLASS 3 Devices	Low	1mW (0 dbm)	0.1 – 10 meters

3. SECURITY OVERVIEW

Bluetooth security is divided into two layers. They are-

Link layer

Application layer

3.1 LINK LAYER

A Bluetooth device address, BD _ADDER (48 bits):-unique for each device and identified by IEEE.

A secret authentication key, the link key (128 bits):- When a Bluetooth session (defined as the time interval for which the device is part of a piconet) is initiated, a series of additional keys is generated . one of these keys, referred to as the link key or .The process of authentication employs the encryption of random number by each devices to verify that each is sharing the same secret link key.

A secret encryption keys (8 – 128 bits):- IF encryption is required by the application, an encryption keys is further derived from the link keys , a ciphering offset number and a random number .while the authentication key is always 128 bits ,the encryption key may be shorter to accommodate government restrictions on encryption , which vary from country to country . A new encryption key is, however, is used during the entire session.

Random number (rand) 128 bits:- Every Bluetooth devices is equipped with a random number generator that can create as 128 bits random binary number on demand .

3.2 Application layer security

The Bluetooth General Access Profile defines three security modes:

Mode 1 is non-secure. Authentication is optional.

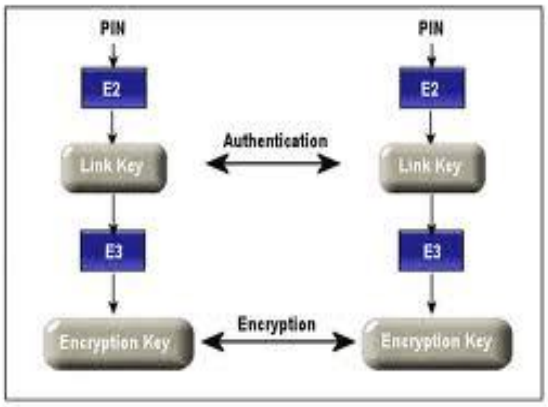
Mode 2 gives service-level enforced security. The service provided by the application decides whether or not authentication or encryption is required. The Bluetooth SIG has published the Bluetooth Security Architecture white paper5 that defines a suitable architecture for

implementing service-level enforced security on Bluetooth devices.

The white paper splits devices into different categories and trust levels, as well as suggesting three security levels for services. The utilization of a database is suggested for enabling the user to authorize devices to utilize only particular services. Because the implementation of security at this level does not affect interoperability, this white paper is advisory only, and is not part of the Bluetooth specification.

Mode 3 is link-level enforced security. Both devices must implement security procedures in order for a connection to be established.

In addition to the above modes, a device can be configured to not respond to paging, so that other devices cannot connect to it. Or it can be configured so that only devices that already know its address can connect to it. Such numerous and complex levels of security are necessary to accommodate the large.



4. Key management

The link key: - A link key is used in the authentication procedure and as one of the parameter to calculate encryption key.

The link keys are either semi-permanent or temporary a semi-permanent link key is stored in non volatile memory and may be used after the current session is terminated. The lifetime of a temporary link key is limited by the lifetime of current session.

Four types of link keys have been defined

The Unit key(KA)- if a device A has little memory, it can use a unit key for all the connection, this key can changed very rare.

The initialisation key (Kint) - the initialisation key used as link key in initialisation process. .The initialisations parameters are encryption using initialisation key are transferred. The key is derived from an random number an L –byte PIN code and a B-ADDR.

The combinational key (Kab)- the combination key is specific to a pair of device.

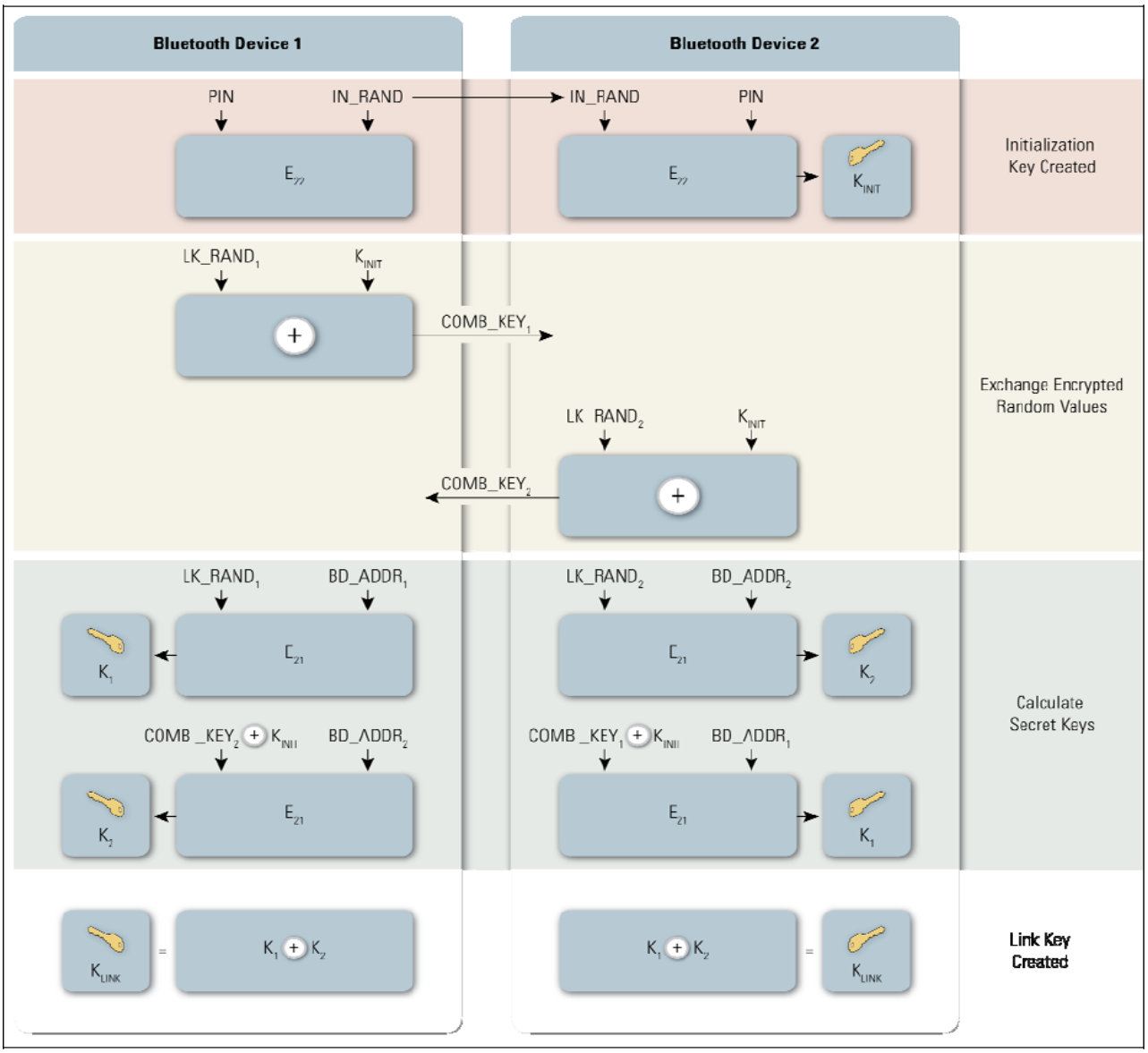
The temporary key (K)- if a master key is derived wants to send a broadcast message to more than two devices simultaneously, it replaces the original link key temporarily with the master key ad uses the master key as a link key .

The combinational key (KAB) and unit key (KA) are functionally indistinguishable. The difference in the way they are generated. The Combinational key is derived from information in both devices A and B.

The pin: - A pin may be a fixed number provide by the devices or it can be used may the user. If the pin NO number is available a default value of zero (0x00) is used. The pin code may be chosen to be any length from 1 to 16 bytes.

The Encryption Key:- the encryption key is derived from the current link key. Each time the key is activated, the key shall be change automatically. To be able to use a shorter key

without weakening the strength of authentication, the encryption key length can be separately configured.



CONCLUSION

It is estimated that before year 2002, Bluetooth will be a built-in feature in more than 100 million mobile phones and in several million other communication devices, ranging from headsets and portable PC's to desktop computers and notebooks. The first Bluetooth products will probably be basic cable replacement products. However, when the Bluetooth chips have entered the mass market and chips are found in a multitude of devices, several new markets will open for Bluetooth solutions. A few Software Development Kits (SDK) have now been introduced on the market. More competition on the SDK market and lower prices on Bluetooth chips will make manufacturers of electronic equipment easy to convince to insert Bluetooth support in their devices. The Bluetooth hardware dimensions and its uniform method for building applications will ensure a Bluetooth market with matching implementations regardless of brand and what country it is designed for.