Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) - May 2016
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Enhancing Performance, Features and Security Issues of Bluetooth

A. Parthibanr[#1], R. Anitha[*2]

[1]*Master of Computer Applications, S.A. Engineering college, Chennai-77.*
Parthi791791@gmail.com
[2]*Asst. Prof., Department of Computer Applications, S.A. Engineering College, Chennai-77.*
anithar@saec.ac.in

Abstract— Bluetooth is a Wireless LAN Technology which is designed to connect various devices of different functions such as telephones, computers, printers etc. The IEEE standardized Bluetooth as IEEE 802.11and is managed by SIG. A Bluetooth LAN is an Ad-hoc network, which is the network formed spontaneously in the devices, sometimes called GADGETS, to find each other and make a network called Piconet. This paper describes the performance, features and security issues of Bluetooth. Simple traffic shaping techniques are discussed to improve the performance. To implement new features, the check box are used. A hybrid encryption algorithm based on AES and RSA is planned to augment the protection of information broadcast in Bluetooth[1].Moreover, in the proposed Hybrid encryption algorithm provides a very convenient technique and efficient for the encryption of transmission data [1].

Keywords— SIG; Piconets; FHSS; RSA; AES.

1. Introduction

Bluetooth is a low cost, low power to connect devices in short range. A piconet have up to 8 stations (master & slave), one of which is called a primary, the rest are called secondary stations. All secondary stations are synchronizing their clocks and frequency hopping sequence with the primary. Piconets can be combined to form new network is called a scatternet. A secondary station in one piconet (master and slave) can be the primary in another piconet. This station can receive the messages from the primary in the first piconet (as a secondary). The Bluetooth has several layers such as L2cap layer, Radio layer, Baseband layer etc. The Radio Layer is roughly equivalent to the physical layers of the internet model. Bluetooth devices are low power and cost and have a range of 10m. Bluetooth uses a 2.4GHZ ISM band divided in to 79 channels of 1 MHZ each. To transform bits in to a signal Bluetooth uses a version FSK. (Frequency Shift Keying)Bluetooth uses 3 classes; class 2 is most commonly used in mobile phones. Bluetooth divides the data that need to transmit in to packets, and transmits each packet on one of the 79 designated Bluetooth channels (1MHZ each). Each and every channel has a bandwidth of 1 MHZ each that usually performs 800 hops per second, by Adaptive Frequency Hopping (AFH) enabled. Bluetooth low energy and low cost are using 2 MHz spacing, which accommodates 40 channels [4].

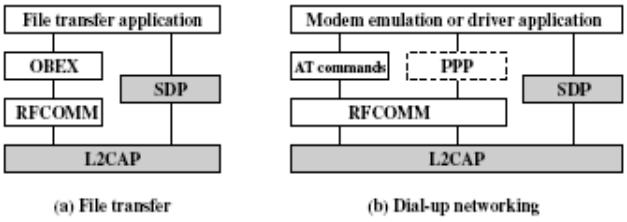


Fig.1: File transfer

Basic unit of Bluetooth networking is one Master and seven slave devices. Master determines channel and phase Device in one piconet might survive as head or slave in a different piconet tolerates numerous devices to share same area Made efficient use of bandwidth not implemented in COTS equipment. Baseband layer is roughly equivalent to the MAC sub layer that multiple accesses control in LAN. Bluetooth uses a form of TDMA (Time Division Multiple Access) that is called TDD-TDMA it is a kind of Half-duplex message in which the resulting and recipient propel and receive data. It is having two links known as SCO and ACL. The Synchronous Connection Oriented (SCO) links are useful at the time of avoiding delay in delivery of data. An Asynchronous Connectionless Link is used well data integrity is more important than avoiding delay in data delivery [6].

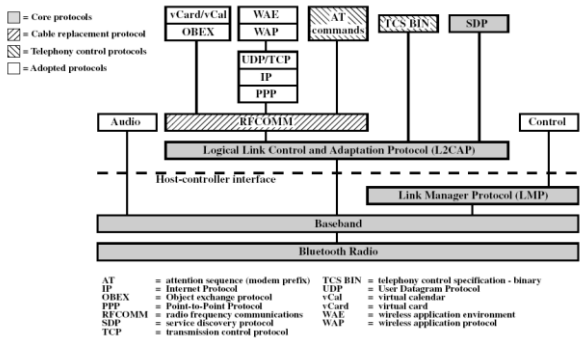


Fig 2: Bluetooth layers

Data transfer rate of Bluetooth is significantly low compared to other LAN like WI-FI. Bluetooth have no

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

advanced features like multiuser sharing like to share the same data more than one user at a same time. It has risk of unauthorized access of user data. Resists interference and multiple path effects Provides the multiple access among co-located devices in different piconet. Total bandwidth divided into 1 MHz to each channel FH occurs by jumping from one channel to another in pseudorandom FH sequence shared across entire Piconet access: Bluetooth devices uses time division duplex like half duplex communication (TDD) Access technique is TDMA FH-TDD-TDMA [4].

Bluetooth can provide a bit-rate equal to 1 Mb/s in later version that v4.2 24/s. The FHSS scheme was used at the physical level of the Bluetooth device; each master chooses a different FHSS sequence so that piconets can operate in the same place without interfering with each other. Frequency hopping frequencies range over 79 frequency channels in the ISM band, each of the channels being 1 Mega Hertz wide. The nominal hop well time is equal to 625 s. Sequences are created by developing several sub-sequences, each and every one was composed of 32 hops. The first sub-sequence is obtained by taking 32 hops at randomly over the first 64 MHz of the FH spectrum; then the successive 32 MHz are skipped, and the next sub-sequence is randomly selected among the following 16 MHz the procedure is repeated until the hopping sequence is completed. A TDD technique that is like a half duplex communication used to transmit and receive data in a piconet. Nowadays most of the people not using the Bluetooth because its data transfer rate is low compared to other LAN network like WI-FI. In today's mobile phones have the application called share it, xender etc., these are applications uses WI-FI LAN technology to share the between to two devices. This application gives higher data transfer compared to Bluetooth device [5].

So people using these types of applications to share the data not using Bluetooth because its performance is low. Using Bluetooth we can transfer the data with only one device at a time. If more than one user wants the same data the user share the data one by one not at the same time. By enhancing the data transfer rate and implementing new features and improving security features of Bluetooth its usage significantly goes high.

2. Transmit Power

The Bluetooth transmission power is very less than the other LAN networks that is WI-FI etc. Bluetooth has three classes class 1,2,3 and Class 2 is used in Bluetooth LAN the below table shows the power class maximum and nominal power and the power control.

3. Performance Analysis

Using simple traffic shaping techniques we can reduce the Interference from other devices [2]. To increase the speed and reliability of data transfer of Bluetooth By increasing the capacity of Bluetooth packets and design the Bluetooth to carry dual data packet at a time, devices transfer data up to 3 times faster than with previous versions.

Table 1: Transmit Power

Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1)]	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm to Pmax Optional: Pmin[2)] to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin[2)] to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin[2)] to Pmax

Table 3.1: Power classes

Note 1. Minimum output power at maximum power setting.

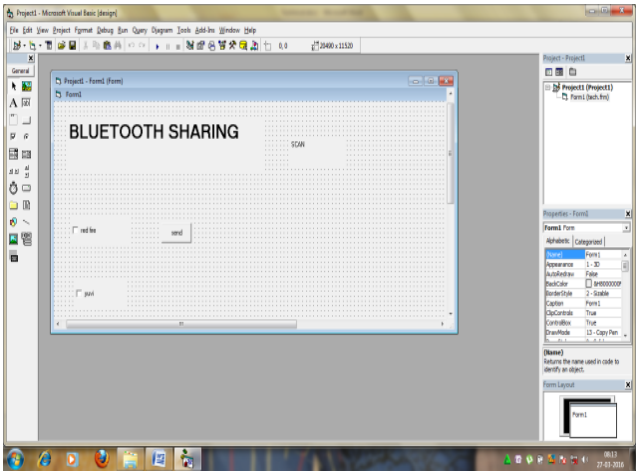
Note 2. The lower power limit Pmin<-30dBm is suggested but is not mandatory, and may be chosen according to application needs.

By rising data transport speed and twin packet capability decreases the occasion of transmission faults to crop up and lessen battery expenditure and that effects in most competent link. It is also having two physical links, which are Synchronous connection oriented and Asynchronous connection less. The links are useful to shun holdup in data release. By designing these links very effective and powerful data traffic is can be control and goes low.

4. Enhancing the Features

In this section, discuss about implementation of new feature in Bluetooth device. To select more than one user to share data in Bluetooth use the checkbox button and give coding as:

```
Private sub check1_ click ()
        If Check1.Value=1 Then
        Check1.Caption="Checked"
        Else
        Check1.Caption="Unchecked"
        End If
End Sub
```



ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

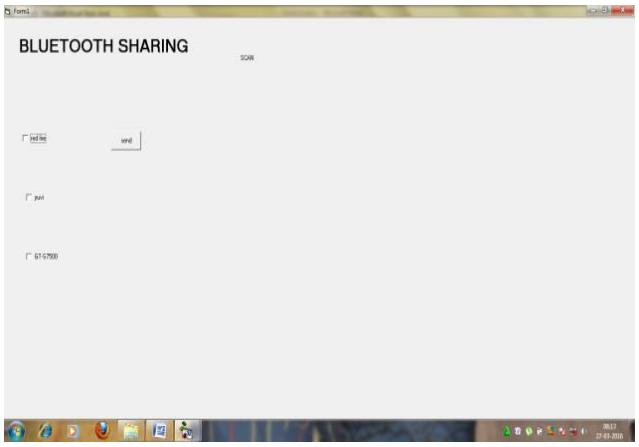


Fig. 3: Bluetooth sharing

To send data more than user we can choose this check box. It allows the user to choose two more options.

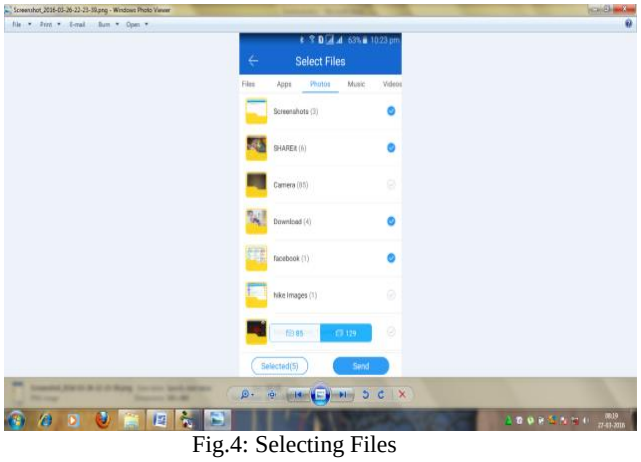


Fig.4: Selecting Files

5. Enhancing Security Issues

Security is essential one in data communication. Because some data are very confidential so that cannot be accessed by someone. Bluetooth transmit data in data packets. The basic security issues in Bluetooth were enhanced in latest versions. But the security issues in Bluetooth still there.

5.1 Process of Hybrid Encryption Algorithm

RSA was the first algorithm with public key which is used for data encryption and digital signatures [1]. It developed on the bases of factoring problems like complexity of factoring great numbers. RSA engages public keys and private keys. The public key may or may not recognize by everybody and it is used only for encrypting the messages. The information encrypted by the public key can merely be deciphered in a sensible quantity of time with the private key.

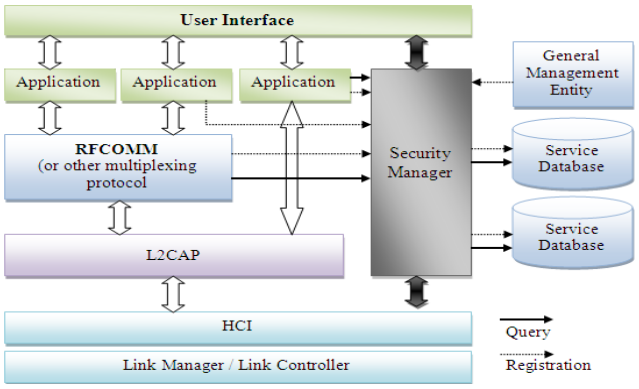


Fig.5: Security Architecture

The AES algorithm was developed based on permutation and replacement. Permutation is reorganization of data, and replacement substitute one component of data by a different.

5.2 Process of Encryption

It is different from Bluetooth stream cipher algorithm; cellular message encipher algorithm is completely safe. At first, AES algorithm encrypts Bluetooth data packet [1]. The 128 bit AES key is used to encrypt the data to get the cipher text C. The second, RSA algorithm encrypts the key of AES algorithm:

- The pubic key of the beneficiary is initially acquired from a server or a particular source.
- Then the 128-bit AES is encrypted using the public key of the receiver to form the cipher text key (CK). [1]
- Using cipher transcript C acquired from AES encryption of the novel communication and the cipher text key (CK) gained from RSA encryption the compound cipher text memo CM is produced and then broadcasted.

The whole amalgam encryption procedure is exposed in figure.

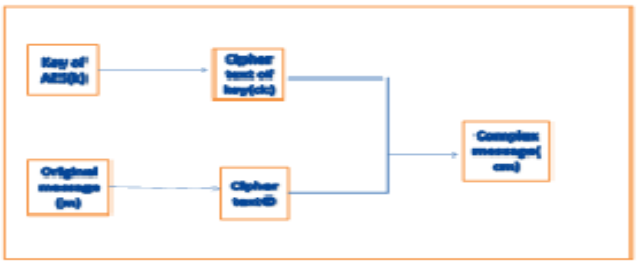


Fig.6: Hybrid encryption process

6. Result

By applying the simple traffic shaping techniques data traffic is significantly reduced and by increased capacity of the Bluetooth packets, devices transfer data up to 2.5 faster.

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

The new feature was proposed in this paper to share the data more than one user using check box. By using visual basic coding. This new feature is very useful for transmitting data for multi users at the same time. The Hybrid Encryption system was proposed for better security in Bluetooth. This encipher system assures that the user data was secured from unauthorized access [1].

7. Conclusion

In this paper, we presented a flexible model for the computation of interference between IEEE 802.11 WLANs and Bluetooth systems. Results showed that a high packet error probability is decreased. We applied simple traffic shaping techniques to the Bluetooth data flow and a significant reduction of the WLAN packet error probability was obtained. Bluetooth technology was mostly used for transferring of data over short range distances. Thus the new features help to share more than the user. Thus the proposed encipher algorithm, HE Algorithm using AES and RSA provides more secure and convenient technique for secure data trans-mission among Bluetooth devices.

8. Future Work

Bluetooth has a good future ahead because it met a basic needed of connection in close proximity, is the outcome of ideas of nine important communications and computer industry developers including companies like Apple, Ericsson, Lucent, IBM, Intel, Microsoft, Nokia, Toshiba etc. The development of the real group; more than 1800 manufacturers worldwide have joined the initiative worldwide. In future, we will put into practice several go forward features like connection of Bluetooth with a variety of operating systems.

References

[1] Bluetooth SIG http://www.bluetooth.com/bluetooth/
[2] Wikipedia http://en.wikipedia.org/wiki/Bluetooth
[3] IEEE 802.15.1 http://standards.ieee.org/getieee802/802.15.html
[4] Aswin Castro .B.U and Rajesh. M, "Bluetooth Enhancement in Data Transmission", Special Issue of Engineering and Scientific International Journal, Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College, May 2015, pp.5-8.