International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

A Mobile Chatting Application Via Bluetooth Techniques

Prasath J, Dr. S. Sujatha

Master of Computer Application, University College of Engineering, Anna University, BIT Campus, Tiruchirapalli, Tamil Nadu, India

ABSTRACT

Wireless communication is often require in fields such as A MOBILE CHATTING APPLICATION VIA BLUETOOTH TECHNIQUES. Android operating system based smart phones are increasingly used now a days because of its simplicity and is open source to create application. The Bluetooth communication system has the low-power requirement making it suitable for wireless carrier. A hybrid encryption algorithm based on AES and RSA is proposed to enhance the security of data transmission in Bluetooth communication.

Keywords: Security, Hybrid Encryption Algorithm, Bluetooth, Data transmission, AES Algorithm, RSA Algorithm.

I. INTRODUCTION

1.1. BLUETOOTH

Bluetooth is a radio frequency standard used for short-range small-scale applications. Developed by the Bluetooth Special Interest Group, Bluetooth technology was designed to be highly compatible with various types of equipment and applications. It is low power consumption and ease of use makes it a very viable option for many short-range wireless applications.

1.2 BLUETOOTH SECURITY

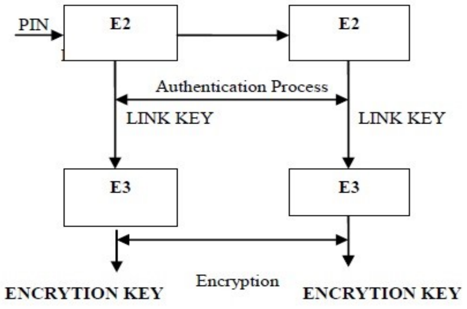
Encryption scrambles the data during transmission to prevent Eavesdropping and Maintain link privacy Bluetooth specification uses Secure and Fast Encryption Routine (SAFER) plus cipher to authenticate Bluetooth.

1.2.1 AES ALGORITHM

The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

1.2.2 RSA ALGORITHM

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography because one of them can be given to everyone. The other key must be kept private. It is because finding the factors of an integer is hard (the factoring problem).

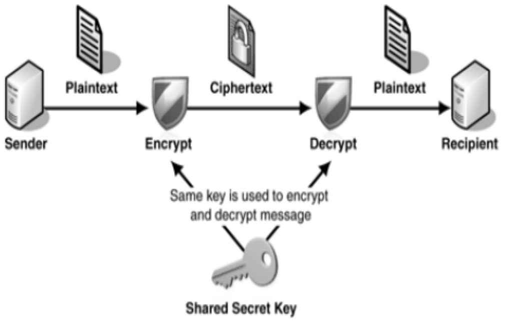


1.3. PROCESS OF HYBRID ENCRYPTION ALGORITHM

RSA is the first public key algorithm used for data encryption and digital signature algorithms. It is based on the difficulty of factoring large numbers, the factoring problem. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

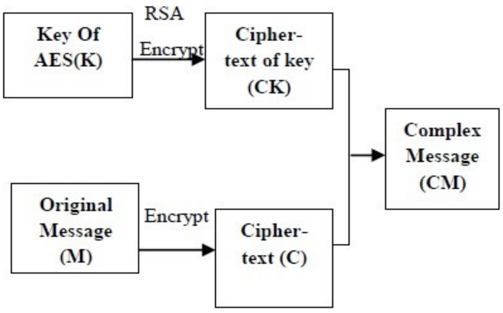
AES is faster than RSA for encryption and decryption of large messages while RSA is suitable for key management as it is based on the difficulty of factoring large numbers. RSA can distribute the encryption key openly and it always keeps the decryption keys secret.

Taking into account the advantages of both AES and RSA and avoiding their shortcomings, hybrid encryption algorithm based on AES and RSA has been proposed in which AES is used for encryption of message and RSA is used to encrypt the AES key. This hybrid encryption algorithm can be used in Bluetooth Technology to avoid the current risks.



1.4 Process of Encryption

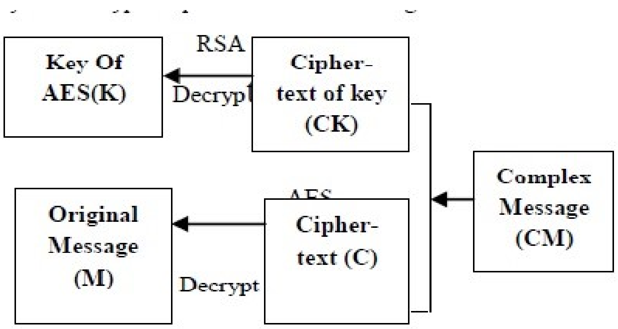
The encrypted message is send along with the encrypted AES key, private key and Big Integer n each separated by a semicolon and the order of which is known only to the sender and receiver. AES, being a block cipher divides the plaintext into number of blocks depending upon the key size for encryption.



The Hybrid Encryption Process

1.5. Process of Decryption

During the decryption of hybrid encryption algorithm, the receiver B first divides the complex message (CM) into two parts AES encrypted cipher text C and RSA encrypted AES session key CK. The receiver B uses its private key dB to decrypt the RSA encrypted AES session key CK to get the session key K. Using the AES key K it then decrypts the cipher text C to generate the original message M.



The Hybrid Decryption Process

II. LITERATURE SURVEY

2.1. WIRELESS COMMUNICATION

Wireless communications is a type of data communication that is performed and delivered wirelessly. This broad term incorporates all procedures and forms of connecting and communicating between two or more devices using a wireless signal through wireless communication technologies and devices.

The sending device can be a sender or an intermediate device with the ability to propagate wireless signals. The communication between two devices occurs when the destination or receiving intermediate device captures these signals, creating a wireless communication bridge between the sender and receiver device.

1. Satellite communication
1. Mobile communication
2. Wireless network communication
3. Infrared communication
4. Bluetooth communication

2.2. FPGA

The Field-programmable gate array (FPGA) system is capable of high speed parallel processing and build a Hierarchy design, which is powerful and fast enough to fulfil all the need of functionality, making it preferable over General purpose processor or micro-controller and has the added advantage of being reconfigurable for future Development. Also Benefits of FPGA Technology like high Performance, low Time to Market, low Cost, high Reliability, and Long-Term Maintenance. Real time applications FPGAs are perfectly suitable for applications in time critical Systems.

2.3. Android

Android is an operating system based on the Linux kernel, and designed primarily for touch Screen mobile devices such as smart phones and tablet computers. This open-source code allows the software to be freely modified and distributed by device manufacturers. Android provides high speed, low power consumption, flexibility and portability as compare to other.

The objective behind making this application was to bring the functionalities of a network service provider onto a mobile device. So while surveying as to on which platform or rather operating system the project has to be implemented ,we selected android for the following reasons:

1. Android is an open source platform
2. Supports multifunction
3. Provides rich tools to make interactive application
4. Downloading the software's required for making the application are absolutely free

2.4. Bluetooth

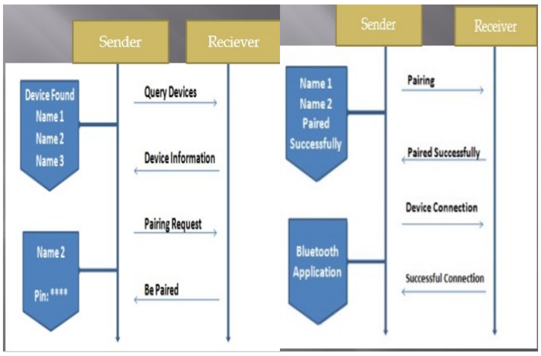
Bluetooth is one of the fast growing technology which offers short distance communication. Because of this there is high demand for both Bluetooth software and hardware. The main advantage of Bluetooth is low consumption which make suitable for mobile devices .It operates in the license-free 2.4 GHz band and supports data rates up to 600Kbps.

The Bluetooth 2.0 protocol has high speed margins, low power consumption, wide operational range, and freedom of transceivers position and simplicity.

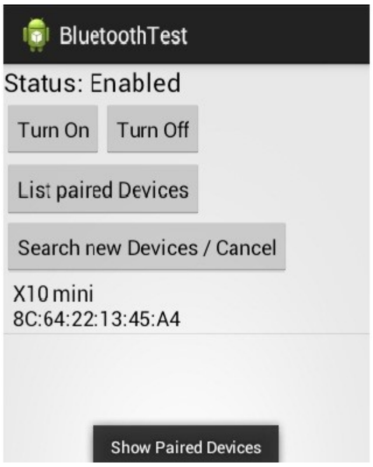
III. EXISTING SYSTEM

Request the necessary Bluetooth permissions. The existing system works with the sharing information sender to receiver

✓ Enable Bluetooth on your phone
✓ Get a list of paired devices
✓ Scan and display a list of nearby Bluetooth devices
✓ Establish a Bluetooth connection between two devices
✓ Send and receive data over a Bluetooth connection



Architecture diagram of the existing system



Status: Enabled

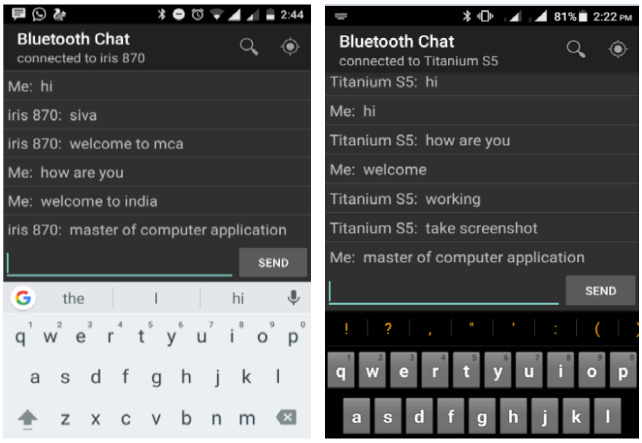
X10 mini
8C:64:22:13:45:A4

Overview of the Existing System

IV. PROPOSED SYSTEM

A Mobile Chatting Application for Bluetooth is not now for Bluetooth devices. The proposed system Communication no Signal any place anytime information sharing very easily for offline transaction. Then operates one Android Smartphone to Another. The all process co-operate with Bluetooth.

Persons can chat via Bluetooth Process for Offline. Easily sharing information between one to another offline process. Existing speed of Bluetooth is 600kbps and range of Bluetooth 10m, but now 15m increasing for Bluetooth range.



Bluetooth Chat
connected to iris 870
Me: hi
iris 870: siva
iris 870: welcome to mca
Me: how are you
Me: welcome to india
iris 870: master of computer application

Bluetooth Chat
connected to Titanium S5
Titanium S5: hi
Me: hi
Titanium S5: how are you
Me: welcome
Titanium S5: working
Titanium S5: take screenshot
Me: master of computer application

Overview of the proposed system

V. IMPLEMENTATION

The implementation of this application is done in the following manner.

- OS – Windows XP or above
- Hardware –Android Device & Computer Systems
- Software – Eclipse Juno, Android SDK, Android AVD
- Language – Java and XML
- Development Kit Used – ADT 21
- Designing – Android App
- The modules are
- Authentication module (Pair Key module (Sender, Receiver)
- Communication module (Range Increasing)
- Process of Hybrid Module (Encrypt, Decrypt)

The Authentication module is to device is on at the time pairing for particular device pair key given for same device. Only two device connecting with sharing information and communication.

Communication module is common on both the sender and the receiver. This is where both the devices chat and exchange information. Bluetooth chat are two way communication.

VI. CONCLUSION

Bluetooth technology is widely used for transmission of data over short-range distances. Bluetooth being a wireless technology is more susceptible to attacks as compared to other fixed networks. Therefore, it is important to consider the security of data during transmission. Bluetooth chatting is an innovative approach to the mobile world. This application shows use of Bluetooth in terms of chatting. Means persons can chat via Bluetooth Process for Offline. Starts the application and search the Bluetooth device, the other devices works to respond the other Bluetooth device. Bluetooth can offer fast and secure access to wireless connectivity all over the world. With potential like that, it is no wonder that Bluetooth is set to become the fastest adopted technology in history.

VII. FUTURE WORK

The implemented could be enhanced to handle multiple Device connected at the same period. In addition, other communication applications like Audio, video calls could be built on the top of this application to experience mobile face-to-face communication in any situation. In addition, the GSM service provider based identity of Bluetooth device (i.e. Device name) could be replaced with other customized identity in conjunction with other device specific identity.

Future Scope

1. Enhancing security by encryption.
2. Improving the range of Bluetooth.
3. Improving the speed of communication.
4. Extending the Frequency Band.

VIII. REFERENCES

[1]. Samer Hawayek, Claude Hargrove and Nabila A.BouSaba,"Real-Time Bluetooth Communication between an FPGA Based Embedded Sustem and an Android Phone,"in IEEE conference, Jacksonville,United States,2013,pp. 1-4.

[2]. Chalivendra G, Srinivasan R, and Murthy N. S, "FPGA based reconfigurable wireless sensor network protocol,"in International Conference on Electronic Design(ICED) 2008.

[3]. Fabrice Peyrard, "Real-time Bluetooth communication system for control of a mobile robot,"Can. J. Elect.Comput. Eng., Vol.33, No.2, Spring 2008.

[4]. Fang Yanan, Lu Xinghua, and Li Huaizu, "Real-time HealthInformation Acquisition and Alarm System Based on Bluetooth and GPRS Communication Technologies," pp.4717-4721,October 8-11,2006.

[5]. http://www.telehealth.philips.com/how_telehealth_works.html.