Available ONLINE www.vsrdjournals.com

VSRD International Journal of
Computer Science & Information Technology

ISSN No. 2231-2471

VSRD-IJCSIT, Vol. 1 (8), 2011, 567-572

RESEARCH ARTICLE

An Integrated Encryption Scheme Used in Bluetooth Communication Mechanism

[1]Gaurav Shrivastava*

ABSTRACT

To improve the security level of data Transmission in Bluetooth communication, A Integrated Encryption Scheme algorithm based on IDEA, RSA and MD5 is proposed. The currently hybrid encryption algorithm uses DES and RSA Algorithm, DES use for Encryption of Data and RSA use for Encryption of Key. Hybrid encryption algorithm employed by the Bluetooth to protect the confidentiality of data during transport between two or more devices [2]. In proposed Integrated Encryption Scheme algorithm mechanism makes a full use of advantage of IDEA Algorithm of Data Encryption because it's faster than RSA Algorithm for long plain text and RSA Algorithm distributed key safely and easily. Digital abstract Algorithm MD5 is adopted in this mechanism. This Mechanism realizes the confidentiality, Completeness, Authentication and Integrity.

Keywords: Authentication, IDEA, Integrity, MD5, RSA, Data Transmission.

1. INTRODUCTION

Bluetooth technology is an emerging wireless networking standard, which is based on chip that provides short-range wireless frequency hopping communication. Now, Bluetooth technology is mainly applied to the communication between mobile terminal devices, such as palm computers, mobile phones, laptops and so on, and also can successfully simplify the communication among above devices and the Internet, so that the data transmission between these modern communication equipments and Internet has become more quickly and efficiently, and widen the road for wireless communications. It has the characteristic of wireless, openness, and low-power and so on. However, the phenomenon of data-leaking frequently arise in using the Bluetooth technology for data transfer, since the emergence of Bluetooth, even if the Bluetooth takes the very robust security measures, there are still serious security risks.[2]

The encryption algorithm using in Bluetooth encryption process is the E0 stream cipher. However, this algorithm has some shortcomings, 128-bit E0 stream ciphers in some cases can be cracked by 0 (2^{64}) mode in

[1]Assistant Professor & Head, Department of Information Technology, Mathura-Devi Institute of Technology & Management, Indore, Madhya Pradesh, INDIA. *Correspondence: gaurav2086@gmail.com

some cases. So, for most applications that which need to give top priority to confidentiality, the data security is not enough if only use Bluetooth. Now I will introduce the Bluetooth mechanism, its disadvantages, and then propose a hybrid encryption algorithm to solve the current security risk in Bluetooth data transmission.

2. BLUETOOTH SECURITY MECHANISM

2.1. Bluetooth security mechanism

The Bluetooth specification defines three security modes:

- **Safe Mode 1 :** No safe mode, which has the lowest security level;
- **Safe Mode 2 :** Service-oriented security model, which start after the establishment of the channel;
- **Safe Mode 3:** Link-oriented security model, which install and initial before communication link is established.

Bluetooth system provides safety precautions in the application layer and link layer, the two sides achieve authentication and encryption in the same way. Link layer uses four entities to ensure the safety:

- 48-bit of the Bluetooth device address, which is global uniqueness decided by the IEEE;
- The authentication key for entity authentication is 128-bit;
- The secret key for data encryption is 8 ~ 128-bit;
- 128-bit random number trades once, changes once.

3. WEAKNESS OF BLUETOOTH SECURITY SYSTEM

3.1. The Weakness Of E0 Stream Cipher Algorithm

The main weakness of Stream cipher algorithm is that if a pseudo-random sequence make an error, it will make the whole cipher text mistake happen, it also bring about the cipher text cannot restore back to plaintext in decipherment.

3.2. Limited Resources Capacity Of Linear Feedback Shift Register LFSR

Encryption algorithm used in Bluetooth technology standard is somewhat fragile, and even if its E0 stream cipher uses 128-bit key, in some cases, the complexity of their decoding is only 0.

3.3. Low Credibility of PIN

Bluetooth technology uses non-standard 4-digit PIN code and another variable to generate the link key and encryption key. Actually, 4-digit PIN code is the only variable which is the real key generated, resulting only one key (a random number) transport in the air.

3.4. High Probability Of Non-Link Key Cheat

Along with the use of the link key takes new problems. Authentication and encryption set up on the basis of the link key.

3.5. Address Spoofing

Every Bluetooth device has a unique Bluetooth device address. However, its uniqueness raises new problems. Once the ID links with a certain fixed person, this person can be tracked and their activities can easily be recorded. In this case, the individual's privacy will be violated.

4. THE PROCESSES OF INTEGRATE ENCRYPTION SCHEME.

In The IDEA Algorithm is a symmetric, block-oriented cryptographic algorithm. It operates on 64-bit plaintext blocks and uses 128-bit keys, what makes it practically immune to brute force attacks. IDEA is build upon a basic function, which is iterated eight times. The first iteration operates on the input 64-bit plaintext block and the successive iterations operate on the 64-bit block from the previous iteration. After the last iteration, a final transform step produces the 64-bit cipher text block. [1]

Public key algorithm is also called asymmetric key algorithm. The basic thought of public key algorithm is that the key is divided into two parts. One is encryption key and the other is decryption key. Encryption key cannot be got from decryption key and vice versa. Because public key is open and private key keep secret, RSA algorithm overcomes difficult of key distribution. The principle of RSA algorithm is that: according to number theory, it is easy to finds two big prime number, but the factorization of the two prime numbers is hard. In this theory, every customer has two keys. They are encryption key $PK = (e, n)$ and decryption key $SK = (d, n)$. Customer opens public key. Each person who wants to transmit information can use the key. However, customer keeps private key to decrypt the information. Here, n is the product of two big prime number p and q (the bits of p and q which are decimal number extend 100). e and d satisfy certain relation. When e and n are known, d cannot be got. [1]

Message-Digest refers to hash transformation of message. MD5 algorithm gets the remainder (64 bits) of the primitive plaintext through mod 2^{64}. The result is added to the end of Message. The MD5 code includes the length information of the message. Some message whose range of bits from 1 to 512 is added into the place which is between message and remainder. After filling, the total length is several times of entire 512. Then the whole message is divided into some data blocks. Each of them includes 512 bits. The data block is further divided into four small data blocks which include 128 bits. The small data block is input into hash function to perform four round calculations. In the end, MD5 message abstract is got. [1]

Seeing form the efficiency of encryption and decryption of IDEA Algorithm is better than RSA Algorithm. IDEA Algorithm is suitable for encryption of large number of data. RSA Algorithm is based on difficult factoring, and its computing velocity is slower than IDEA, and it is only suitable for encrypting a small amount of data.

Seeing from key management, RSA algorithm is more superior to the IDEA algorithm. Because the RSA

algorithm can distribute encryption key openly, it is also very easy to update the encryption keys, and for the different communication objects, just keep the decryption keys secret; IDEA algorithm requires to distribute a secret key before communication, replacement of key is more difficulty, different communication objects, IDEA need to generate and keep a different key.

Based on the comparison of above IDEA algorithm and RSA algorithms, in order to give expression to the advantages of the two algorithms, and avoid their shortcomings at the same time, we can conceive a new encryption algorithm, that is, IDEA and RSA Integrated Encryption Scheme We will apply to Integrated Encryption Scheme Bluetooth technology; we can solve the current security risks of Bluetooth technology effectively.

In Integrated Encryption Scheme sender is A, the receiver is B. A's public key is A_P, and Secret key is A_S, B,s public key is B_P and Secret key is B_S.(We assuming that the two sides of communication know each RSA public key A_P and B_P).

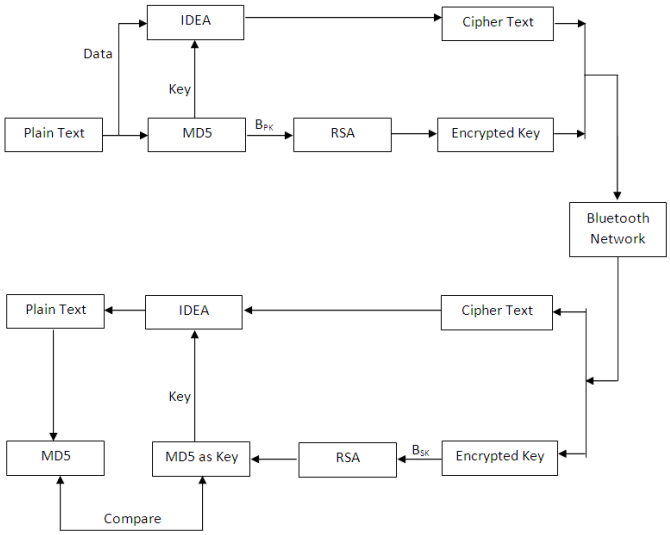

Fig 1: Integrate Encryption Scheme

4.1. Process of Encryption

The Encryption of Integrated Encryption Scheme as follows.

- The first, MD5 algorithm Calculate 128 Bit MD5.
- The second, IDEA algorithm encrypts the Original Message (M) with help of 128 Bit key generated by MD5 Algorithm, and then Produce a cipher text (C).
- The Third 128 Bit MD5 Encrypted by RSA Algorithm with receiver Public key B_{PK} and produce Cipher Text of Key (CK).
- Forth Combine a Cipher Text (C) and Cipher text of Key (CK), produces a Complex Message (CM).Complex Message (CM) is send to the Receiver B.

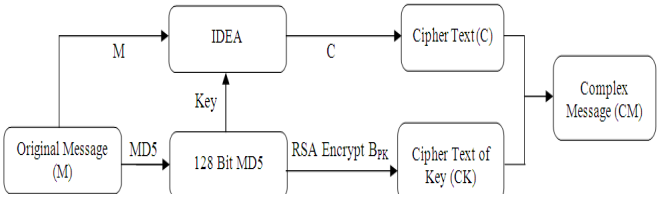

Fig 2: An Encryption Process of Integrate Encryption Scheme

4.2. Process of Decryption

The decryption of Integrated Encryption Scheme is as follows.

- The first, the receiver B received cipher text CM into two parts, one is cipher text of key CK from the RSA algorithm encryption, and the other is cipher text C from the IDEA algorithm encryption.
- The second, the receiver B decrypts cipher text CK by their own private key B_{SK}, and retrieve the key K which belongs IDEA algorithm, then decrypt the cipher text C to the original M by key K.

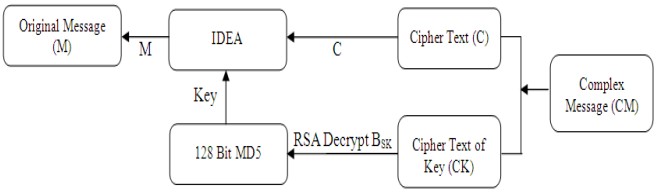

Fig 3: A Decryption Process of Integrate Encryption Scheme

4.3. Process of Compare MD5

- The first, Calculate MD5 of Original Message (M).
- The second, Cipher Text of Key (CK) decrypt by RSA Algorithm with help of Receiver Secrete Key B_{SK} and produce a key and it's also a MD5.
- The third compare Both MD5s.

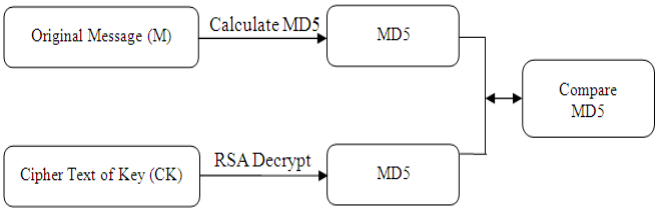

Fig 4 : Process of Compare MD5

5. ADVANTAGE OF INTEGRATE ENCRYPTION SCHEME

- Using MD5 Algorithm maintain a Integrity.

- Using RSA algorithm and the IDEA key for data transmission, so it is no need to transfer IDEA key secretly before communication;
- Management of RSA key is the same as RSA situation, only keep one decryption key secret;

6. CONCLUSION

Bluetooth technology is a new technology, which will change our transmission method. However, the Bluetooth technology has not fully considerate security issues in the standardization process. As communication networks, it uses wireless channel for the transmission medium. Compared to the fixed network Bluetooth network is more vulnerable to be attacked. For the applications that take data security as priori, achieving a high level of data security is essential. Currently, stream cipher E0 used in Bluetooth standard has many shortcomings, while the DES and RSA hybrid encryption algorithm is relatively more secure and easier to achieve, thus ensures data transmission between the Bluetooth device safety and real-time.

7. REFERENCES

[1] KUI-HE YANG, SHI-JIN NIU College of Information Hebei University of Science and Technology Shijiazhuang 050018, China *Data Safe Transmission Mechanism Based on Integrated Encryption Algorithm* Science and Technology Research program of Hebei province (042135117), 2009

[2] Wuling Ren College of Computer and Information Engineering Zhejiang Gongshang University *A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication* Second International Conference on Modeling, Simulation and Visualization Methods, 2010.

❑❑