IOSR Journal of Engineering (IOSRJEN)
ISSN: 2250-3021 Volume 2, Issue 7(July 2012), PP 72-77
www.iosrjen.org

Performance Analysis of Triple DES-Tiger-RSA Vs DES-RSA algorithms for Bluetooth Security Systems

Sudhir Nagwanshi[1], Akhilesh A.Waoo[2], P. S. Patheja[3], Sanjay Sharma[4]
1(Student, CSE Department, BIST/ RGPV Bhopal, India)
2(Astt. Prof., CSE Department, BIST/ RGPV Bhopal, India)
3(HOD, CSE Department, BIST/ RGPV Bhopal, India)
4(Prof., CSE Department, MANIT Bhopal, India)

ABSTRACT : - *In this paper, comparison of the Hybrid Encryption algorithm (3DES-Tiger-RSA) and Old Hybrid Method (DES-RSA, by Wuling Ren & Zhiqian Miao)[1] for Bluetooth Security system is done. Performance of the above security algorithm is evaluated based on the efficiency of the algorithm. The efficiency is calculated on the basis of performance obtained by both the algorithm's which was captured entirely in JDK Net beans Environment. In order to check the efficiency of the algorithm, the data is encrypted with both the algorithm and the time and space complexity are compared with each other. The output is seen to be obtained without any incorrectness which justifies the level of security. On comparison, the new Hybrid Encryption technique proves to be better for implementation in Bluetooth Devices then the Old Encryption algorithm [2].*

Keywords: - *Secure and Fast Encryption Routine, Triple DES, Tiger, RSA, Encryption and Decryption.*

I. INTRODUCTION

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc or peer-to-peer (P2P) networks.[2] Bluetooth technology has been integrated into many types of business and consumer devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets.[2] This allows users to form ad hoc networks between a wide variety of devices to transfer voice and data.[2] This document provides an overview of Bluetooth technology and discusses related security concerns. There have been several versions of Bluetooth, with the most recent being 2.0 + Enhanced Data Rate (EDR) (November 2004) and 2.1 + EDR (July 2007). While 2.0 + EDR provided faster transmission speeds than previous versions (up to 3 M bits/second), 2.1 + EDR provides a significant security improvement for link key generation and management in the form of Secure Simple Pairing (SSP).[2] There are several security algorithms available to ensure the security in wireless network devices. Some of the major methods are AES, DES, Triple DES, IDEA, BLOWFISH, SAFER+[2] , RC2 to RC5 and Hybrid DES-RSA. Although DES-RSA is one of the best secure algorithm but, it seems to have some vulnerabilities. Our objective is to compare the integrated 3DES-Tiger-RSA algorithm and DES-RSA algorithm for the Bluetooth security systems. In our algorithm we have used Triple DES in which multiple stages of permutation and substitution are performed, Tiger use a hash function and RSA use public and private key encryption and decryption methods which results in a more complex algorithm, which increases the difficulty of cryptanalysis. This shows that the integrated 3DES-Tiger-RSA algorithm proves to be a better one for the implementation in Bluetooth devices than DESRSA.[1,2]
In this paper, section 2 deals with Bluetooth security. The DES-RSA algorithm is explained in section 4. Section 5 describes the TDES-Tiger-RSA algorithm.

II. BLUETOOTH SECURITY

This section provides Bluetooth specifications to illustrate their limitations and provide a foundation for some of the security recommendations A high-level example of the scope of the security for the Bluetooth radio path is depicted in Figure 3. In this example, Bluetooth security is provided only between the mobile phone and the laptop computer, while IEEE 802.11 security protects the wireless local area network link between the laptop and the IEEE 802.11 AP. However, the communications on the wired network are not protected by Bluetooth or IEEE 802.11 security capabilities. End-to-end security is not possible without using higher-layer security solutions in addition to the security features included in the Bluetooth specification and IEEE 802.11 standards.[8,10]

The following are the three basic security services specified in the Bluetooth standard:

- Authentication: verifying the identity of communicating devices. User authentication is not provided natively by Bluetooth.[10]
- Confidentiality: preventing information compromise caused by eavesdropping by ensuring that only authorized devices can access and view data.[11]
- Authorization: allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so. The three security services offered by Bluetooth and details about the modes of security are described below. Bluetooth does not address other security services such as audit and non-repudiation; if such services are needed, they must be provided through additional means.[8,10,11]

III. THE DES-RSA ALGORITHM

According to the work done by Wuling Ren & Zhiqian Miao they have used the following model for securing Bluetooth communication.[1] RSA algorithm is the first relatively complete public key algorithm. It can be used for data encryption, also can be used for digital signature algorithms. RSA cryptosystem is based on the difficulty of integer factorization in the group Zn, and its security establishes in the assumption that constructed by almost all the important mathematicians, it is still a theorem that does not permit, which is lack of proof, but Mathematicians believe it is existent. DES is a group cipher algorithm, which encrypts data by a group of 64-bit. A group of 64-bit plaintext is entered from one beginning of the algorithm; 64-bit cipher text is exported from the other side. DES is a symmetric algorithm, encryption and decryption use the same algorithm (e the different key arrangement), the key can be any 56-bit value (the key is usually 64- bit binary number, but every number that is a multiple of 8-bit used for parity are ignored).[1]

This algorithm uses two basic encryption techniques, make them chaos and spread, and composite them. Seeing from the efficiency of encryption and decryption, DES algorithm is better than the RSA algorithm. The speeds of DES encryption is up to several M per second, it is suitable for encrypting large number of message; RSA algorithm is based on the difficulty of factoring, and its computing velocity is slower than DES', and it is only suitable for encrypting a small amount of data, The RSA encryption algorithm used in the. NET, it encrypts data at most 117 bytes of once. Seeing from key management, RSA algorithm is more superior than the DES 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; DES algorithm requires to distribute a secret key before communication, replacement of key is more difficulty, different communication objects, DES need to generate and keep a different key. Based on the comparison of above DES 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, DES and RSA hybrid encryption algorithm. We will apply hybrid encryption algorithm to Bluetooth technology, we can solve the current security risks of Bluetooth technology effectively. The entire hybrid encryption process is as follows: Let the sender is A, the receiver is B, B's public key is eB, B's private key is dB, K is DES encryption session key (assuming that the two sides of communication know each RSA public key).[9,12]

A. Process of encryption

During the process of sending encrypted information, the random number generator uses 64-bit DES session key only once, it encrypt the plaintext to produce cipher text. On the other hand, the sender get debit's public key from public key management centre, and then using RSA to encrypt session key. Finally, the combination of the session key from RSA encryption and the cipher text from DES encryption are sent out. DES encryption scheme is that encrypt the plaintext bit-by- bit or byte-by-byte, then form key stream, and the intermediate processing results are saved in the process. Key stream has the characteristics of self synchronization, if the key text which is sent encounters errors and data lost, it will only affect a small section of the final text (64-bit). It is different from Bluetooth stream cipher algorithm, cellular message encryption algorithm is completely safe in mathematically prove.[1]

- Bluetooth packet plaintext M is divided into 64-bit plaintext Mi(i=1,2,…,n)).
- Crypts Mi for 16 cycles by 64-bit key K ,and Mi will turn into a 64-bit cipher text Ci (i = 1,2, ... n), then all the Ci (i = 1,2 , ... n) are combined into cipher text C. The second, RSA algorithm encrypts the key of DES algorithm:
- Obtain RSA public key of receiver B from the key server, or other sources Make DES 64-bit session key K for RSA encryption by public key eB that obtains from recipient, then a session key encrypted information CK is formed
- Composite Cipher text message C from the use of DES encryption, and session key CK from RSA encryption, we can get the hybrid CM for transmission. All above steps shows the whole mixed-encryption process.

B. Process of Decryption

The decryption of hybrid encryption algorithm is as follows.

- The receiver B divide received cipher text CM into two parts; one is cipher text CK from the RSA algorithm encryption. The other is cipher text C from the DES algorithm encryption.
- The receiver B decrypt cipher text CK by their own private key dB, receive the key K which belongs DES algorithm, then decrypt the cipher text C to the original M by key K. is a decryption of hybrid encryption algorithm.[1]

IV. 3DES-TIGER-RSA ALGORITHM

The Triple DES 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. 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. Tiger refers to hash transformation of message. Tiger algorithm gets the 64 bits of the primitive plaintext through mod 264. The result is added to the end of Message. The Tiger 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, Tiger message abstract is got.

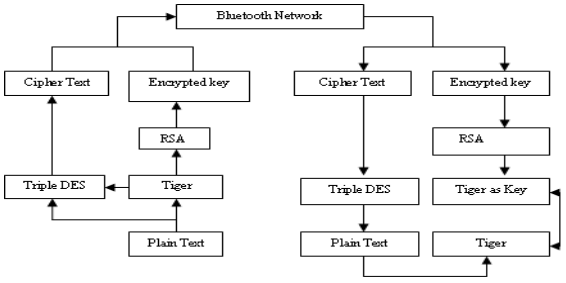


Fig 1: Process of Hybrid Encryption Scheme

A. Process of Encryption

The Encryption of Integrated Encryption Scheme as follows.

- Tiger algorithm Calculate 128 Bit Tiger value.
- Triple DES algorithm encrypts the Original Message (M) with help of 128 Bit key generated by Tiger Algorithm, and then produce a cipher text (C).
- 128 Bit Tiger Encrypted by RSA Algorithm with receiver Public key BPK and produce Cipher Text of Key (CK).
- 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.

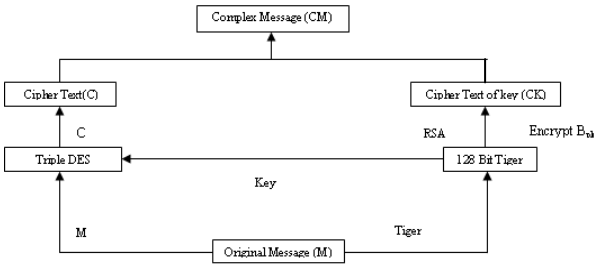


Fig 2: Process of Encryption

B. Process of Decryption

The decryption of Integrated Encryption Scheme is as follows.

- 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 Triple DES algorithm encryption.
- The Receiver B decrypts cipher text CK by its own private key BSK, and retrieves the key K which belongs Triple-DES algorithm, then decrypt the cipher text C to the original M by key K.

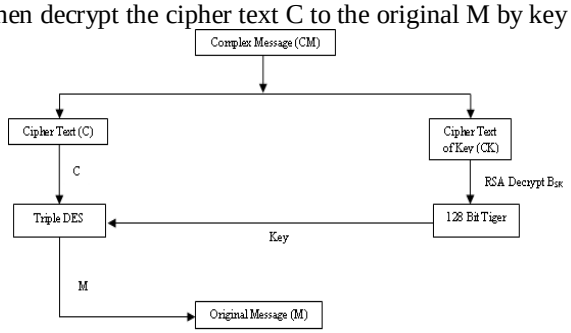


Fig 3: Process of Decryption

V. RESULTS ANALYSIS BETWEEN NEW AND OLD METHOD

The table 1 shows the result related to the Time to send a file from one Bluetooth device to another Device, Time to Discover, Time used in Encryption, Time used in Decryption and Average Time. For the New "3DES-Tiger-RSA". In this table we have performed the operation be sending 3 different size of data packets of 20kb, 40kb and 60 kb. And for comparing our results we have performed the same operations with the same data packet on the old "DES-RSA" encryption method, whose values are mentioned in table 2.

Table 1: Result for 3DES-Tiger-RSA

Packet Size	20 kb	40 kb	60 kb
Time to Discover	12576.4 ms	12975.6 ms	12044.0 ms
Time to encrypt	54612.3 ms	88362.3 ms	112242.5 ms
Time to send packet	117.2 ms	280.1 ms	436.0 ms
Time to Decrypt	3145.1 ms	7484.2 ms	8896.7 ms
Average Time	2436852.0 ms	4572802.3 ms	5723589.7 ms

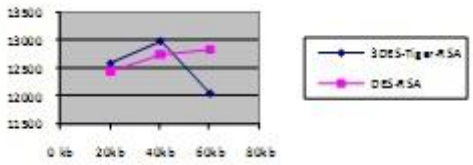
These results have been obtained by performing both the operations on Java Net beans environment using the encryption and decryption algorithm.

Table 2: Result for DES-RSA

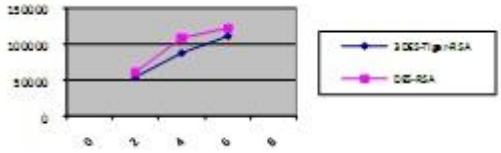
Packet Size	20 kb	40 kb	60 kb
Time to Discover	12431.1 ms	12759.3 ms	12842.3 ms
Time to encrypt	61342.1 ms	109415.3 ms	123754.0 ms
Time to send packet	131.1 ms	390.2 ms	640.8 ms
Time to Decrypt	5175.1 ms	6852.3 ms	10892.3 ms

Now I am comparing every parameter of the old method with new method by plotting its value on it values on graphs.

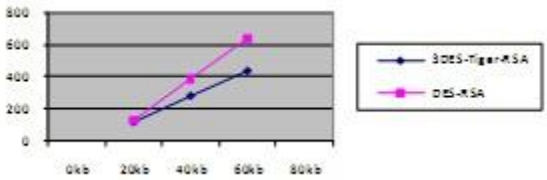
The graphs is plotted between the size of Data Packet and Time in microseconds, in which the size of data packet is taken on X axis, and the time is taken on Y axis.



The first graph is for the parameter Time to discover the ranged Bluetooth devices. From the above result it is clear that the Time required in Discovering the Device is almost equal for both the Methods. There is a slit difference at every time when we try to search the other Device from the primary Device, this is because of the wireless environment and a little bit of noise is added to the data for checking its efficiency.

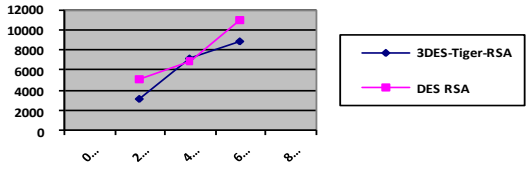


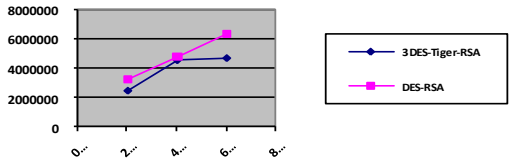
The second parameter is about the time taken by the old and new method for encrypting the file which is to be send from one device to another, and from the result table it is clear that the time for encryption in the new method is lesser than the old method. As we can see that new method takes lesser time the old method for encrypting the Data packet. So it shows the newer method is better than the old method.



The third parameter which is about the Time required sending a Data packet from one device to another, in this we have tried for Different size of data packets which are of 20 kb,40 kb and 60 kb, and the result shows that the new method is much better than the old method, But there is a limitation also in the new method as we have performed the experiment on various sizes of data packet and it seems that the as we increases the size of data packet the new method proves to be less effective than the old method.

Forth parameter is on decryption time and this also proves that the new method is better than the old one.





The last parameter is about the average time usage during the whole process, Average time taken in new method is less than the old method. This proves that the whole process for encrypting the data for Bluetooth communication in new method is better than the old method.

The limitation of the new improver algorithm is Memory Used in New method is higher than the old method. This is because of the algorithms which we have used is providing a very high security. As we have used "3DES-Tiger-RSA" a bundle of three algorithms which is providing very high security as compared to the previous hybrid algorithm which is "DES-RSA". So from these results we can conclude that we have reduced the time complexity and enhanced the security level for the Data Transmission.

VI. CONCLUSION

Our research work focus on some aspects which are Bluetooth security weaknesses were studied and a Bluetooth security environment for implementing Bluetooth security attacks in practice was built, moreover different types of attacks against Bluetooth security were investigated and the feasibility of some of them were demonstrated and Countermeasures against each type of attacks were also proposed. Finally a novel system for detecting and preventing intrusions in Bluetooth networks was described, and a further classification of Bluetooth-enabled ad-hoc networks depending on a risk analysis within each classified group was presented.

ACKNOWLEDGEMENTS

To all the authors that is listed below in list of reference and to those who are anonymous included in the writing papers thanks to all.

REFERENCES

[1] A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication, Wuling Ren, Zhiqian Miao, College of Computer and Information Engineering Zhejiang Gongshang University.
[2] G Performance Analysis of SAFER+ and Triple DES security algorithms for Bluetooth SecuritySystems ,Dr.R.Neelaveni,D.Sharmila
[3] Bluetooth Hacking: A Case Study, Dennis Browning, Gary C. Kessler
[4] Zheng Hu. Network and Information Security [M]. Peking: Tsinghua University Pres, 2006.
[5] Man Young Rhee. Network Security Encryption Principle, algorithm and Protocol[M]. Peking: Tsinghua University Pres, 2007.
[6] Suri, P. R.; Rani, S. Bluetooth security Need to increase the efficiency in pairing [J]. IEEE/ Southeastcon, 2008.
[7] Fengying Wang. Dynamic Key 3DES Algorithm of Discrete System Based on Multi-dimension Chaos [J]. Microelectronics and Computer, 2005, 7: 25-28.
[8] Falk A. The IETF, the IRTF and the networking research Community.Computer Communication Review, v35, n5, Oct. 2005:6970.
[9] Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs, Amit Dhir
[10] Cryptanalysis of Bluetooth Keystream Generator Two-level E0, Yi Lu? and Serge Vaudenay
[11] On the Existence of low-degree Equations for Algebraic Attacks, Frederik Armknecht?
[12] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher Revised 19 May 2008 William C. Barker
[13] Tiger: A Fast New Hash Function, Ross Anderson, Eli Biham
[14] Serpent: A New Block Cipher Proposal, Eli Biham, Ross Anderson and Lars Knudsen
[15] Cracking the Bluetooth PIN, Yaniv Shaked and Avishai Wool
[16] Yaniv Shaked, Avishai Wool. Cracking t he Bluetooth P[C]. 3rd USEN IX/ ACM Conf. Mobile Systems, Application and Services (MobiSys). Seattle, WA, June 2005:39250.. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34-39, Jan. 1959.
[17] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767-782, May 2001.
[18] J.J.Martinez Castillo & K.Aviles Rodriguez: "Using Hybrid Wireless NOMOHi Devices in Green Rural Telecommunications Networks," World Telecommunications Congress(WTC), 2012 , vol., no., pp.1-6, 5-6 March 2012
[19] M.La Polla,F.Martinelli & D.Sgandurra: "A Survey on Security for Mobile Devices," Communications Surveys & Tutorials, IEEE , vol.PP, no.99, pp.1-26, 0 doi:10.1109/SURV.2012.013012.00028
[20] S.Sandhya, K.A.S.Devi: "Analysis of Bluetooth threats and v4.0 security features," Computing, Communication and Applications(ICCCA),2012 International Conference on, vol., no.,pp.1-4,22- 24Feb.2012 doi:10.1109/ICCCA.2012.6179149
[21] R.Bouhenguel, I.Mahgoub & M.Ilyas: "Bluetooth Security in Wearable Computing Applications," High Capacity Optical Networks and Enabling Technologies, 2008. HONET 2008. International Symposium on, vol., no., pp.182-186, 18-20 Nov.2008 doi:10.1109/HONET.2008.4810232
[22] F.R.M.Rashidi, M.H.Ariff & M.Z.Ibrahim: "Car monitoring using Bluetooth security system," Electrical, Control and Computer Engineering (INECCE), 2011 International Conference on , vol., no., pp.424-428, 21-22 June 2011 doi: 10.1109/INECCE.2011.5953919
[23] M.Tan & K.A.Masagca: "An Investigation of Bluetooth Security Threats," Information Science and Applications (ICISA), 2011 International Conference on, vol., no., pp.1-7, 26-29 April 2011 doi: 10.1109/ICISA.2011.5772388