© 2019 IJSRSET | Volume 6 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : 10.32628/IJSRSET196437

Analysis of E0, DES, RSA, AES and Hybrid Algorithm for Bluetooth Transmission

Shivam Vatshayan
Department of Computer Science and Engineering, Galgotias University, Uttar Pradesh, India

ABSTRACT

Bluetooth is a short range wireless technology standard for exchanging data over devices and It uses di erent types of Algorithms for its Data protection, easy secure transmission. This paper is analysis for E0, DES, RSA and AES cipher algorithms with concept of cryptog-raphy and machine learning. However, Hybrid Algorithm is convenient technique for encryption of transmission of data. Hybrid Algorithm is also discussed.

Keywords : E0 Algorithm RSA Algorithm AES Algorithm Cryp-tography Hybrid Algorithm.

I. INTRODUCTION

Wireless communication technology has advanced at a very fast pace during the last years, creating new applications and opportunities. In addition, the number of computing and telecommunications devices is increasing. Special attention has to be given in order to connect e ciently these devices. In the past, cable and infrared light connectivity methods were used.The cable solution is complicated since it requires special connectors, cables and space. This produces a lot of malfunctions and connectivity problems. The infrared solution requires line of sight. In order to solve these problems a new technology, named Bluetooth, has been developed. With this communication system, users are able to connect a wide range of computing and telecommunication devices easily and simply with out need for connecting cables.Unlike wireless LANs such as 802.11b, it was designed to be low power, operate over a short range, and support both data and voice services. It enables peer-to-peer communications among many types of handheld and mobile devices. Furthermore, it provides a conceptually simple communication model and lets these devices exchange information and work together to bene t the user.[1]

The key features of Bluetooth technology are robustness, low power, and low cost. Bluetooth was designed to be the basis of the Personal Area Network (PAN) { a way for devices within relatively close proximity to communicate wirelessly with one another. The range for Bluetooth transmissions varies from about 1 meter up to 100 meters starting from Bluetooth 1.0 to Bluetooth 4.2 and up to 400 meters using Bluetooth 5.0, depending on the power class of the device [3]. Data is transmitted between Bluetooth devices in packets across the physical channel that is subdivided into time units known as slots [2]. Thus, the most powerful (Class 1) can communicate over a distance of more than 300 feet, similar to a typical Wi-Fi network. The current Bluetooth 5.0 technology devices can communicate at distances of approximately 400 meters. Like 802.11b and g, Bluetooth transmits over the 2.4 GHz radio frequency. Its speed is limited to about 1-3 Mbps (far slower than Wi-Fi, but still roughly equivalent to a typical broadband Internet connection). The speed depends on the distance between the devices. It uses LMP

(Link Manager Protocol) to handle the connections between devices [2, 4]. Bluetooth mobile phones can be attacked by using social engineering techniques [5]. The lack of basic security awareness among phone users and general lack of understanding of Bluetooth technology is certainly an advantage for hackers.

To overcome the security limitations of Bluetooth, this works deals in usage of AES, DES and Triple DES encryption [6] for transferring data via Bluetooth.

II. RELATED WORK

2.1 Overview of Bluetooth Security

This section provides an overview of the security goals and mechanisms as pro-vided by the Bluetooth standard. We aim to illustrate the strengths and lim-itations of the current standard of Bluetooth security. Bluetooth devices that communicate with each other form a piconet. A piconet master is a device that initiates a connection and there can be up to seven slaves in the piconet. All com-munication has to go through the piconet master however. Slave devices (e.g. headset, mouse, keyboard) connect with master devices by a pairing process

2.2 Security Goals

There are ve basic security goals and principles speci ed by the Bluetooth stan-dard.

Authentication: One of the goals of Bluetooth is to be able to verify the iden-tity of communicating devices with a unique Bluetooth address. Bluetooth does not provide native user authentication.

Con dentiality: Another goal is to prevent the disclosure of information caused by eavesdropping by ensuring that only authorized devices can access and view transmitted data.

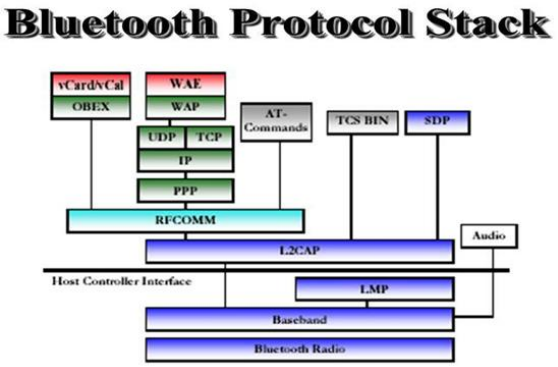
Authorization: The Bluetooth standard sets out to allow the control of re-sources by ensuring that a device is authorized to use a service rst.

Message Integrity: Messages sent between two Bluetooth devices should not be modi ed in transit.

Pairing/Bonding: The last goal of the Bluetooth standard is to create one or more shared secret keys between two devices and storing them for future use in subsequent communications.

2.3 Bletooth Protocol Stack

Security for Bluetooth is provided on the various wireless links, in other words, link authentication and encryption may be provided, but true end-to-end secu-rity is not possible without providing higher layer security solutions on top of Bluetooth. The complete Bluetooth protocol stack is shown in Figure.



The Bluetooth protocol stack comprises of Bluetooth speci c protocols such as LMP (Link Management Protocol), L2CAP (Logic Link Control and Adap-tation Protocol), and non-Bluetooth speci c protocols such as OBEX (Object Exchange), UDP (User Datagram) [2]. One of the major advantages of this Blue-tooth protocol stack is the re-use of the existing protocols for di erent purposes at the higher layers.

III. METHODS AND MATERIAL

Overview of E0, DES and RSA algorithm

3.1 EO Algorithm

The Bluetooth encryption system uses the stream cipher E0 to encrypt the payloads of the packets which is re-synchronized for every payload. The E0 stream cipher consists of the payload key generator, the key stream genera-tor and the encryption/decryption part. The input bits are combined by the payload key generator and are shifted to the four Linear Feedback Shift Registers (LSFR) of the key stream generator. The key stream bits are then generated which are used for encryption. The Exclusive-OR operation is then performed on the key stream bits and data stream bits to generate the ciphertext. Similarly the Exclusive-OR operation is performed on the ciphertext to get back the plaintext during the decryption process.But E0 Algorithm have Drawbacks such as easily attacked , Low credibility and address spoo ng

3.2 RSA Algorithm

RSA algorithm is an asymmetric key cryptographic algorithm; it was invented in 1977 by Ron Rivest, Adi Shamir and Len Adlemen. It uses the concept of two keys; the public and the private key; RSA algorithm converts the plaintext into a ciphertext by encrypting the message using the public key, which only the receiver can decrypt with the use of a private key. RSA algorithm's invention is base on the arithmetical concept that it is easy to nd and multiply large prime numbers but to factor their product is di cult. Both private key and public keys in RSA algorithm are based on prime numbers that are large (100 or more digits) [12] [13] . There are basically three steps in RSA algorithm; the selection and generation of the public and private keys, encryption and decryption process [12] [13] .

Algorithm:

1. Choose two large prime numbers P and Q.
2. Calculate N= P X Q.
3. Select the public key (i.e. the encryption key) E such that it is not a factor of (P-1) and (Q-1).
4. Select the private key (i.e. the decryption key) D such that the following equation is true: (D X E) mod (P-1) X (Q-1) =1
5. For encryption, calculate the cipher text CT from text PT as follows: CT = PTE mod N

3.3 DES Algorihtm

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 di erent key arrange-ment), the key can be any 56-bit value 253 (the key is usually 64-bit binary number, but every number that is a multiple of 8-bit used for parity are ig-nored). This algorithm uses two basic encryption techniques, make them chaos and spread, and composite them. Seeing from the e ciency 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.

3.4 AES

AES was introduced by NIST in 2001 to replace DES. The AES algorithm is a symmetric block cipher used to protect important documents by the US gov-ernment and implemented for data encryption all around the word [6] [7] [8]

AES algorithm comprises of three di erent ciphers blocks, which are; AES-128, AES-192 and AES-256 which can each encrypt or decrypt data in blocks of

128 bits utilizing 128 bits, 192 bits or 256 bits cryptographic keys. Basically for encryption and decryption process, AES goes through di erent rounds; it goes through 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [6] [7] [8] . A 128 bit data length is allowed in AES, which we can further split into four di erent basic functioning blocks; the blocks repre-sent as range of bytes and are organized as a 4 4 matrix called the state [6]

For encryption/decryption process in AES, AddRoundKey is the rst stage that starts the cipher, after which the output goes through additional nine main rounds before it eventually gets to the nal round. Four transformations are performed during each of these rounds, they are: 1) Sub-bytes, 2) Shiftrows, 3) Mix-columns, 4) Add round Key [6] . In the (10th) round, which is the nal, Mix-column transformation is not performed [9] [10] .

Encryption Mechanism in Bluetooth communication Drawbacks

Information security in the network has been a challenge, which demands urgent attention. Notably with the rapid development of computer technology, several issues arose to the surface of the Information Security eld such as User Authen-tication, data encryption, data integrity, and access control. Bluetooth is a radio communication standard short-range, which enables electronic devices to be con-nected as well as communicated wirelessly. Also, Bluetooth functions in the fre-quency band the 2.4 Hz. It uses FHSS (Frequency Hopping Spread Spectrum) be-cause it makes eavesdropping becomes tough. Frequency Hopping Spread Spec-trum, which is a radio transmission process where randomly, chosen frequencies hopping between 79 di erent frequencies at regular intervals in accordance with a pseudorandom sequence. Further, the transmission range is up to 10 meters, and data can be transmitted over asynchronous (ACL Asynchronous Connection Less) or synchronous channels (SCO, Synchronous Connection-Oriented). In ear-lier versions of Bluetooth, an E0 stream cipher algorithm is used for encryption process. However, this algorithm has proven to be vulnerable [11] , and many attacks in [12] [13] [14] preformed successfully on E0 stream cipher [15] . While in the latest versions (4.0 - 5.0 v), 128-bit AES for encryption is used. There-fore, this study devoted in order to further increase the security of encryption algorithm in Bluetooth.

Hybrid Algorithm

Due to the use of AES,DES and RSA algorithms, its operating e ciency depends on the speed and high e ciency of encryption and decryption by AES algorithm. Security of data transmission in Bluetooth Technology is improved by the secu-rity strength of the proposed hybrid encryption scheme. Data remains secured due to the special design and strength of all key lengths of the AES algorithm (128,192,256). Sidechannel attacks are the only known successful attacks against AES. Thus the security strength of data transfer using bluetooth technology is improved using AES encryption. Presently, RSA is the only popular algorithm used for public key cryptography. Its security mainly depends on the di culty of factoring large numbers in reasonable amount of time. 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.

The original message remains safe as long as the encryption key that is being used remains secret. Even if the data sent using the hybrid encryption algorithm is tracked, the complex message is organized in such a way that the tracker will not understand which part of the complex message contains the AES encrypted key and the ciphertext. Also, the private key of the receiver will not be known and hence the AES key cannot be decrypted ensuring the data in transit remains safe. So the

transmitted data remains secure due the security of hybrid encryption algorithm using AES and RSA.[14]

IV.CONCLUSION

Bluetooth is an inspiring innovative technology, which revolutionizes the way we communicate. However, the security mechanism of earlier versions Bluetooth technology has not been equipped with adequate level of security. Thus, it is more vulnerable to di erent attacks. Even though the current security mech-anism of the latest versions has been provided an acceptable level of security, however, a high level of security is Best.Bluetooth technology is widely used for transmission of data over short range distances up to 10 Metre range. Bluetooth being a wireless technology is more vulnerable to attacks as compared to other Transmission networks. So it is important to consider the security of data during transmission. E0 stream cipher algorithm which is currently used in Bluetooth for encryption has many shortcomings and can be easily attacked and approach-able. In focus of this paper, the proposed method as Hybrid Algorithm was feasible as well as successfully implemented, and it is utilized in live scenarios. In the context of the feasibility of our approach, because the high level of security provided the encryption key remains secret, the original message remains safe. In case of attack, the organization of the complex message is intricate, which confused the intruder in understanding which part of the complex message con-tains the cipher-text and encrypted key. Moreover, the private key of the receiver will not be known. Therefore, the process of transmission data remains secure due to the unique security combination as provided by our Hybrid algorithm. Indeed, the proposed method has improved the security of encryption algorithm in Bluetooth.

V. FUTURE WORK

In Future, we are planing to further develop new ideas concerning the Bluetooth transmission security. First, we plan to analyze the current encryption mecha-nism weakness, after which we will propose a proper solution with protocols. Second, we will propose a geographic pairing based protocol, which will o er resistance against several attacks and add another authentication factor to the pairing process in order to present a strong authentication approach during the Bluetooth pairing process. Security can also achieved by secured simple pairing by applying anti-intrusion mechanism and anti-attack customization. Positively, these contributions will supply an extra security layer to achieve a high level of security.[16]

VI. REFERENCES

[1]. Jagadeeshbabu, B et al. \DESIGN OF SAFER + ENCRYPTION ALGO-RITHM FOR BLUETOOTH TRANSMISSION." (2015).

[2]. Bluetooth Protocol Architecture. White Paper, Bluetooth. Downloadable from : (last visited: May 26, 2017) http://www.ece.eng.wayne.edu/ smahmud/BluetoothWeb/BT oothP rotocol.pdf

[3]. Bluetooth { What is Bluetooth? (last visited: May 26, 2017)

[4]. https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works.

[5]. Bluetooth Security Architecture. White Paper, Bluetooth. Downloadable from: (last visited: May 26, 2017) http://www.afn.org/ afn48922/downs/wireless/1c11600.pdf.

[6]. Bluetooth Security White Paper. Bluetooth SIG Security Expert Group.Downloadable from: (last visited: May 26, 2017) http://grouper.ieee.org/groups/1451/5/Comparison

[7]. Singh, G. (2013) A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. International Journal of

Computer Applications, 67, 33-38. https://doi.org/10.5120/11507-7224

[8]. Bhanot, R. and Hans, R. (2015) A Review and Comparative Analysis of Various Encryption Algorithms. International Journal of Security and Its Appli-cations, 9, 289-306. https://doi.org/10.14257/ijsia.2015.9.4.27

[9]. Shanta, J.V. (2012) Evaluating the Performance of Symmetric Key Algo-rithms: AES (Advanced Encryption Standard) and DES (Data Encryption Stan-dard). IJCEM International Journal of Computational Engineering Manage-ment, 15, 43-49.

[10]. Stallings, W. (2006) Cryptography and Network Security: Principles and Practices. Pearson Education, India.

[11]. Chowdhury, Z.J., Pishva, D. and Nishantha, G.G.D. (2010) AES and Con - dentiality from the Inside Out. The 12th International Conference on Advanced Communication Technology (ICACT), 2, 1587-1591.

[12]. Rege, K., Goenka, N., Bhutada, P. and Mane, S. (2013) Bluetooth Commu-nication Using Hybrid Encryption Algorithm Based on AES and RSA. Interna-tional Journal of Computer Applications, 71, 10-13.

[13]. Armknecht, F. and Krause, M. (2003) Algebraic Attacks on Combiners with Memory, in Advances. In: Boneh, D., Ed., Advances in Cryptology|CRYPTO 2003, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 162-175.

[14]. Hermelin, M. and Nyberg, K. (2000) Correlation Properties of the Bluetooth Combiner. In: Song, J., Ed., Information Security and Cryptology|ICISC'99, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 17-29.

[15]. Lu, Y. and Vaudenay, S. (2004) Faster Correlation Attack on Bluetooth Keystream Generator Eo. In: Franklin, M., Ed., Advances in Cryptology|CRYPTO

[16]. 2004, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 407-425.https://doi.org/10.1007/978-3-540-28628-825

[17]. Albahar; M:; Haataja; K:andT oivanen; P:(2016) TowardsEnhancingJustW orksM odelinBluetoothP airi

[18]. Albahar; M:; Olawumi; O:; Haataja; K:andT oivanen; P:(2018) NovelHybridEncryptionAlgorithmBased 176:doi : 10:4236=jis:2018:92012

Cite this article as :

Shivam Vatshayan, "Analysis of E0, DES, RSA, AES and Hybrid Algorithm for Bluetooth Transmission", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 4, pp. 361-366, July-August 2019.
Journal URL : http://ijsrset.com/IJSRSET196437