International Journal of Intelligent Information and Management Science
ISSN: 2307-0692, Volume 9, Issue 2, April, 2020

A Promote Encryption Algorithm based on DES Encryption and PRNG in Bluetooth Wireless Transmission

Tao Pan*, Haoran Yin
Internet Institute, Anhui University, Hefei, 230039, China

Abstract: Through the study of Bluetooth wireless transmission attack, based on DES algorithm to do a security defense upgrade, analysis of Bluetooth information security authentication and encryption algorithm principle, structure and algorithm, analysis of E_0 encryption weaknesses, but also based on DES algorithm how to secure Bluetooth encryption.

Keywords: Bluetooth wireless transmission; Security; DES; Encryption algorithm; PRNG

1. Introduction

Bluetooth is a typical transmission way in wireless sensor network, Bluetooth transmission is widely used in computers, mobile phones and other electronic equipment as well as some military equipment, and with the progress of wireless technology, wireless technology instead of traditional wired has become a trend, so how to do a good job in Bluetooth transmission data security protection is very necessary. Bluetooth transmission has the advantages of low power consumption, stable connection and simultaneous transmission of text and multimedia data, but the transmission rate and transmission range are limited, leading to limited security. The fast frequency hopping technology adopted by Bluetooth can only solve the related interference problems caused by the internal and external devices of the system, and cannot effectively detect and prohibit the access of illegal users. The encryption algorithm used in the Bluetooth encryption process is stream algorithm, but with the improvement of Bluetooth technology, many users need to transfer the data security, this encryption algorithm does not provide good security [1].

IEEE specifies that the Bluetooth address (BD-ADDR) is 48 bits, the authentication key used for identity authentication is 128 bits, and the encryption key used for data encryption is 8~128 bits. Currently, usually the wireless Bluetooth transmission is encryption by DES algorithm, but S - DES is too simple, can't meet with safety as the primary purpose of data transmission, and 3 - DES somewhat bloated, Bluetooth transmission rate and efficiency in limited circumstances, excessively encryption can let sell at a discount greatly transport experience, let users appear a series of problems in the process of transfer files, based on the DES algorithm, so how to design a safe, not easy to crack, and ensure the basic rate and efficiency of Bluetooth data transmission is very be necessary. This article describes how to use the N-DES algorithm and a special PRNG algorithm to enhance the security of wireless Bluetooth transmission while ensuring the basic transmission experience [2].

2. Bluetooth Transport and Security Mechanism

2.1. The encryption mechanism

Bluetooth security mechanism has five parts: pairing, binding, device authentication, encryption and message integrity. It adopts E_0, E_1, E_2 and E_3 algorithms. The user enters PIN code and generates the link key through E_2 algorithm. The key gets the encryption key through E_3 algorithm, generates the key stream through algorithm, and then outputs the ciphertext through plaintext encryption.

Matching the key is to establish, key is used in encrypt the connection, release key is for Shared key, is used to encrypt to reconnect and verify the signature and random address resolution, there are three stages of pairing, often use the first two stages, the third phase is optional, phase 1: matching feature exchange, phase 2 (LE legacy pairing): STK, LTK generated, phase three (LE Secure Connections): the key issue.

As shown in the figure below, the Initiator is the Initiator of the matching request, and the Responder is the Responder. In the first stage, authentication requirements and IO capabilities are exchanged to determine which of the following methods are used in the second stage:

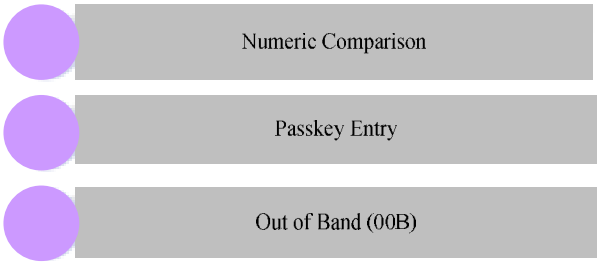

Figure 1. Pairing process

Numeric Comparison
Passkey Entry
Out of Band (OOB)
After pairing begins, if the Responder does not support pairing or cannot perform pairing, an error code is returned, pairing features are used to exchange IO capabilities, OOB authentication data availability, authentication requirements, key size requirements, and which key to publish.
LE legacy pairing USES and generates two keys:
Temporary Key (TK),128 bits, to generate STK
Short Term Key (STK), a 128-bit temporary Key used to encrypt paired connections
LE Secure Connections USES and generates a Key: Long Term Key (LTK) a 128-bit Key used to encrypt the paired Connections and subsequent Connections.

2.2. Authentication

Bluetooth authentication mechanism adopts competitive response mode. The applicant first sends his or her Bluetooth address to the verifier, who returns a random number. Both parties use the number, Bluetooth address and current link key as parameters to run algorithm E_1 and calculate their respective authentication code SRES. If the two are the same, the authentication passes; otherwise, the authentication fails [3].

2.3. Encryption Key Generation

The encryption key is calculated by E_3 algorithm:

$K_c = E_3(RAND, K, COF) = Hash(RAND, K, COF, 12)$.

[COF is the encryption offset. The Bluetooth device link control generates a new encryption key K_c each time the encryption module is activated] [4].

2.4. Encryption

The encryption adopts the stream encryption algorithm, and uses the linear feedback shift register group to generate pseudo-random sequences as the encryption key stream and the plaintext data stream are different or to achieve encryption, and the expression is

$X_{n+1} = aX_0 + c(\mathrm{mod}\, k)(n \geq 0)$

[a, c is constant, k is modulus, with some number X_0 bit seed number, can generate a series of random Numbers]

2.5. Safety System Analysis

Linear algorithm is used in the Bluetooth encryption process. It will be easy to crack brute force if the attacker adopts it, and the PIN code of most users is too simple, which greatly increases the cracking probability. Moreover, as algorithm is stream encryption, if a pseudo-random sequence is wrong, the ciphertext cannot be restored to plaintext. For now, DES algorithm seems to become the best solution, but S-DES cannot meet the safety-first data transmission.
In order to solve these potential security risks, the following will introduce how to use of N-DES algorithm and special PRNG to solve these problems, not only ensure data security, but also make the calculation appears less bloated.

3. Des and N-DES

3.1. Des and 3DES

The key length of DES algorithm is only 56 bits, which is relatively short, so the confidentiality of the algorithm has a low impact on the security of DES, and the key confidentiality is the key.
DES algorithm to choose plaintext attack resistance is insufficient, the attacker can target selection of some plaintext, so that the algorithm to choose the plaintext encryption to get ciphertext, and the attacker through the connection between plaintext and ciphertext to get some information of the algorithm, find out the law, convenient to crack the algorithm behind. If some processing and improvement are made to the key or related steps during the encryption process, the security of the algorithm will be enhanced.

3-DES is the encryption algorithm of DES transition to AES. It uses three 56-bit keys to encrypt data three times. Is a safer variant of DES. It takes DES as the basic module and designs the packet encryption algorithm by combining the grouping method. 3DES is safer than the original DES.

· $Encrytion: C = E_{k3}(D_{k2}(E_{k1}(P)))$

$Decryption: P = (D_{k1}(E_{k2}((D_{k3}(C)))$

3.2. Mersenne twister algorithm (MTA)

The Mersenne Twister is a pseudorandom number generator (PRNG). It is by far the most widely used general-purpose PRNG. Its name derives from the fact that its period length is chosen to be a Mersenne prime [5].

The commonly used version of Mersenne Twister, MT19937, which produces a sequence of 32-bit integers, has the following desirable properties:

·It is k-distributed to 32-bit accuracy for every $1 \le k \le 623$ [k-distributed: A pseudorandom sequence xi of w-bit integers of period P is said to be k-distributed to v-bit accuracy if the following holds. Let truncv(x) denote the number formed by the leading v bits of x, and consider P of the kv-bit vectors, then each of the 2kv possible combinations of bits occurs the same number of times in a period, except for the all-zero combination that occurs once less often.]

·It passes numerous tests for statistical randomness, including the Diehard tests.

For some common PRNG algorithms, when small samples are used to generate pseudo-random Numbers, 0 and 1 are not distributed evenly, and the following scenarios requiring PRNG algorithm are small samples, so MTA is safe and reliable to generate the required pseudo-random Numbers.

3.3. N-DES based on mta

Using DES algorithm is too simple, however, using 3 DES algorithm could make the Bluetooth transmission rate affected, in order to balance the two problems, we use the N - (N less than or equal to 6), the DES algorithm N values will be generated by the MTA, the seeds of the MTA will enter into a 32 bit binary number, take 1,2,4,8,16,32 bit to get six binary encodings, converting the six binary codes into decimal number G.

if $N \le 2$, then $N++$;

Note: N is rounded down.

Then, we'll encryption the plaintext into ciphertext by N-DES. The following will introduce a unique DES algorithm that is a little difference between S-DES.

1) Replacement

First, we should transform 64-bit binary notation into 56-bit K_1 through table PC-1. And then, we get 28-bit left and 28-bit right. And do it again and again for 8 times (not 16 times, because we want Bluetooth more efficient while it is also safe), the bit of C_{n-1} and D_{n-1} shift to left for one bit, so we get $C_0 - C_8$ $D_0 - D_8$, and $D_n D_n$ shifted by table PC-2, then we get $K_1 - K_8$

2) Iteration

Then, shift Binary plaintext through table IP get IP value, and divide IP value into Left and Right.

$L_n = R(n-1)$

$R_n = L(n-1) \oplus f(R_{n-1}, K_{n-1})$

The ciphertext of the IP value is expressed as:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

3) Function

4) Expansion Permutation

Through Expansion Permutation table E, we change into $E[R_n]$

$A = K_n \oplus E[R_{n-1}]$

5) S-Box Replacement

Cutting A into 4 groups, each group is 6-bit, and we only use $S_1 - S_4$ Box, then we get $S_1 - S_4$ value, and we should expand the bit of $S_1 S_2 S_3 S_4$, so we design a new Expansion Permutation E-1 in below.

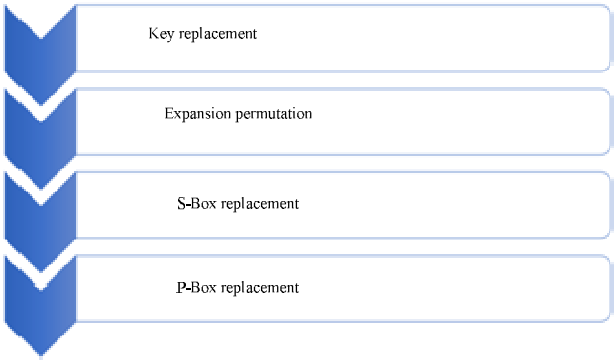

Figure 2. Flow chart

Table 1. Expansion permutation E-1

8	5	6	7	8	9
12	9	10	11	12	13
16	13	14	15	16	17

After shifting 16-bit into 24-bit, we will design another new Expansion Permutation E-2(in below) to shift 24-bit into 32-bit.

Table 1. Expansion permutation E-2

4	1	2	3	4	5
8	5	6	7	8	9
12	9	10	11	12	13
16	13	14	15	16	17
20	17	18	19	20	21
24	21	22	23	24	1

Then, through Permutation Function(P), we get P(B), then

$R_n = P(B) \oplus L_{n-1}$

$L_2 = R_1, L_3 = R_2$

We will get final $R_8 L_8 (64 - bit)$

6) Inverse Initial Permutation (IP^{-1})

We use this table to get IP^{-1} (Binary notation), and then shift it into Hexadecimal notation, it's the final ciphertext we want to get.

The final ciphertext is expressed as:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

4. Conclusion

DES has been considered to be the most suitable for Bluetooth wireless transmission of an encryption algorithm, and the n-des of this paper adopts a unique improved algorithm, optimize the time complexity and space complexity of encryption, optimize the security required for encryption, so that the encryption algorithm can be used in security-oriented occasions. The random number algorithm of MTA allows the 0 and 1 in a small sample to be distributed evenly, reducing the possibility of extreme cases and making the whole encryption algorithm more secure and scientific. Finally, we estimate that n-des is 30% faster than 3-des through some simulations, and at the same time, the security is improved by 50%, which is a big improvement for the security of Bluetooth technology.

References

[1] Liu Qihong, Yang Hao. A RFID encryption and decryption module based on DES algorithm. Science & Technology Information. 2019, (27), 13-15.

[2] Jia Jun. Analysis research and countermeasure of DES block encryption algorithm. Information & Communications. 2019, (6), 4-4.

[3] Wang Lei, Fan Huimin. A Wireless LAN encryption algorithm for short message transmission. Modern Electronics Technique. 2010, (04), 127-129.

[4] Feng Hua. Research on algorithm of information transmission encryption in social insurance network. China CIO News. 2013, 000(004), 147-148.

[5] Tang Pengzhi, Kang Wenyang, Zhang Peng, et al. An ultra-lightweight stream encryption scheme suitable for real-time encrypted transmission of WSN data. Journal of East China Jiaotong University. 2019, (4), 131-136.