http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (19): 5107-5110, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.5107.5110

Improvements Algorithm of Des Cipher Key Based on Bluetooth Security Mechanism

[1]Yang Zhao-Hui, [2]Chen Hong-Juan and [3]Chi Yun-Fei
[1]School of Electrical and Control Engineering, Chang' an University
[2]PLA Third twenty-three Hospitals, Disinfection and Supply Room,
[3]School of Information Engineering, Chang' an University Xi'an, Shaanxi, China

Abstract: The encryption of existing norms which used by bluetooth can be cracked. A new Bluetooth security improvement program to enhance data security which provides by the existing Bluetooth standard. By analyzing Bluetooth information security mechanism, algorithm of each of its part and steps of achieving the algorithm are explored in detail and security of the existing Bluetooth regulations are evaluated. Targeted at its shortage, a new security mechanism is constructed using DES algorithm to meet the requirements of application of Bluetooth with higher security.

Key words: Bluetooth technology, encryption algorithm, DES algorithm, security mechanism, shift registers

INTRODUCTION

Bluetooth as a new short-range wireless communications technology has been widely used in various fields which provides low-cost, low power, short-range wireless communications, fixed and mobile communications constitute the environment in the personal network, so close in variety of information devices to seamlessly share resources. (Li *et al*., 2006; Dallas, 2002; Li *et al*., 2007).

As a short-range interconnect solutions Bluetooth communications technology, using wireless communications transmission which may lead to user data intercepted in transit by others. Hendler (1996). Bluetooth frequency hopping mechanism to provide security measures focus on solutions from other Bluetooth devices within the system caused by transmission interference but because of the wireless transmission of data, theft of data can easily shield themselves without the user found. Therefore, relying solely on frequency hopping technology, protection is not enough. (Joakim and Ben, 2000).Therefore, Bluetooth Security White Paper defines a set of security system and further to ensure the confidentiality of user data. Authentication mechanisms and encryption mechanism is the important part of the architecture, the encryption algorithm is the core of these two mechanisms. This study focuses on the Bluetooth security mechanism improved algorithm DES key. (Chatschik, 2001).

BLUETOOTH SECURITY MECHANISM

Bluetooth security mechanism adopted for communication of other cases in which the two sides in the same way to achieve authentication and encryption procedures. Link layer uses four entities to provide security: an open Bluetooth device address, length of 48bit; authentication key length of 128bit; encryption key length of 8 ~ 128bit; random number, length of 128bit

Encryption key length and encryption mode: Baseband Bluetooth devices need to define the standard maximum allowed length of the key bytes Lmax, $1 \leq Lmax \leq 16$. Before generating the encryption key, the unit must agree on the actual length of the key. Main unit will advise the value L (M) sug sent from the unit. If L (S) min≤L (M) min and support for the proposal from the unit value from the unit have given confirmation, L (M) min as the link encryption key length value. If you do not meet the above conditions, the main unit from the unit will send the new recommended value L (S) min <L (M) sug, the main unit the proposal evaluation. Repeat this procedure until an agreement or a party to abandon negotiations.

Encryption algorithm: Stream cipher encryption used encryption protocols. Encryption system Used Linear Feedback Shift Registers (LFSRs), system output of the register are combinate by a 16-state finite state machine, the state machine output may be key stream, or the initialization phase of the random initial value. Need to

Corresponding Author: Yang Zhao-hui, School of Electrical and Control Engineering, Chang' an University, Xi'an, Shaanxi 710064, China

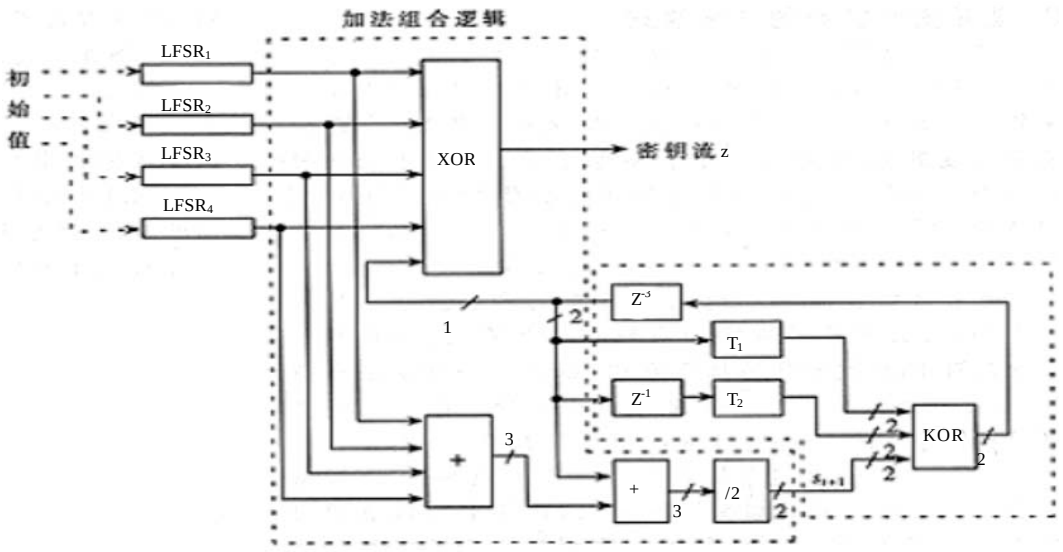

Fig. 1: Mechanism of the security algorithm

provide the encryption key encryption algorithm, 48bit Bluetooth address, the master clock and 128bit bit random number RAND, encryption algorithm shown in Fig. 1.

Of these, four LFSR (LFSR1, ..., LFSR4), bit length, respectively L1 = 25, L2 = 31, L3 = 33, L4 = 39, the feedback polynomial (tap polynomial, characteristic polynomial). Sum of the length of four registers is 128bit.

Moment that xit said LFSRit output state bit, four-tuple (x1t, ..., x4t) have Yt as follows:

$$Y_t = \sum_{i=1}^{4} x_t^i$$

where, Yt is an integer value of 0, 1, 2, 3 or 4. Adder output generated by the following equation:

$$z_t = x_t^1 \oplus x_t^2 \oplus x_t^3 \oplus x_t^4 \oplus C_t^0 \qquad \in \{0,1\}$$

$$S_{t+1} = \left(S_{t+1}^1, S_{t+1}^0\right) = \left[\frac{Y_t + C_t}{2}\right] \qquad \in \{0,1,2,3\}$$

$$C_{t+1} = \left(C_{t+1}^0, C_{t+1}^0\right) = S_{t+1} \oplus T_1[C_t] \oplus T_2[C_{t-1}]$$

where, T1 [.] And T2 [.] is the GF (4) on two different linear bijection.

Before working Key stream generator is required load the initial value into four LFSR (total 128bit) and determine the value of C0 and C-14bit, 132bit initial values □□ of these key stream generator using the specified input derived from the input, respectively for the key Kc, 48bit address and 26bit Bluetooth master unit clock CLK26-1. Encryption algorithm initialization process: (1) The effective encryption key was generated by128bit encryption key Kc, denoted K'c, so L (1 = L = 16) for the use of 8bit group said the number of effective key length, the K'c (x) = g2 (L) (x) (Kc (x) modg1 (L) (x)). (2) K'c, Bluetooth address, clock and 6bit constant 111001 move into LFSR. Encryption algorithm initialization is complete, the output from the adder combination keystream for encryption/decryption.

Certification: Bluetooth technology uses so-called inspection certification entities-response program. Through the "two-step" protocol, the applicant is aware of the secret key using the symmetric key to confirm. This means that a proper applicant/verifier pair, in the inspection - response program will share the same key Kc, confirmed by the applicant whether the authentication algorithm K1 certified random number AU_RANDA and returns the authentication result SERS, for inspection.

PROGRAMS TO IMPROVE THE BLUETOOTH SECUITY MECHANISM

There are two major problems in existing Bluetooth security mechanism. One is the use of key elements: The authentication and encryption process, because the key element has not changed, the third party to use this key to steal information. In some cases, 128-bit encryption key length of the E0 sequence can be crack by which is not

very sophisticated methods. Another is the Bluetooth unit to provide Personal Identification Number (PIN) of insecurity: Since most applications the PIN code is composed of four decimal digits, so a brute-force attack is easy to succeed.

In order to overcome these security solution to the problem, in addition to increasing the length of the PIN code, the key is to take a more robust encryption algorithm, such as the use of digital encryption standard instead of the sequence. DES encryption algorithm DES is a block encryption, the encryption process for a block of data. In the DES algorithm, the original information is divided into 64-bit fixed-length data blocks, then use 56-bit encryption key generated 64-bit encrypted information by the displacement method and the combination . Bluetooth encryption algorithm with a different sequence, you can mathematically prove that the block encryption algorithm is completely safe. DES block cipher is highly random and non-linear, the resulting ciphertext and the plaintext and key are related to each one. DES encryption key available to a very large number, used in every plaintext keys are generated from the keys the large number of randomly. DES algorithm has been widely used and considered very reliable. DES encryption algorithm using Bluetooth technology, Bluetooth can be applied to a high security applications to, for example, electronic financial transactions, ATM and so on.

DES IMPROVE ALGORITHM

DES algorithm: 1977, U.S. National Bureau of Standards published a Federal Data Encryption Standard DES. (Tumer and Demir, 2005). As the DES algorithm confidentiality and so far there is no practical way to decipher, so the DES has been widely used. DES is a block cipher system it will be clear by a group of 64 divided into several groups, the key length is 56 bits. The basic idea is to use a combination of transform and iterative, the plaintext into ciphertext group in each group. (Weston, 2000).

DES encryption process system: In the DES system, product transformation is the core of the encryption process, there are 16 times continuous operation, each time you can update a set of keys. Shift transformation B is A's inverse transform shift. Fig. 2 shows the system DES encryption process, the right side of the DES system diagram is the key generation process. Initial key is a string 64bit of random sequences. After repeated shift change, produced 16 groups of sub-keys (K1 ~ K16), each sub-key is used to transform a product. The so-called

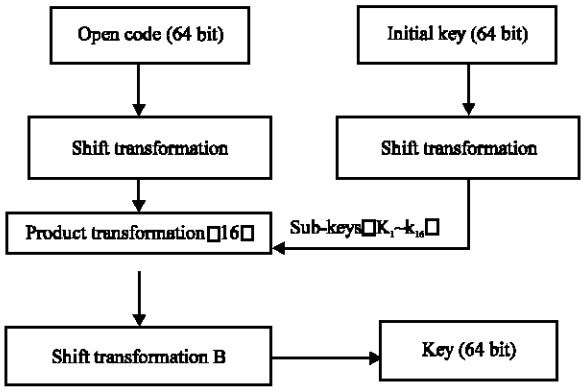

Fig. 2: Encryption process of DES system

initial rearrangement (IP) is disrupting the original arrangement of the input bit sequence within the group, re-arranged arrangement is fixed.

DES transformation operations steps of one product: (1) The 64bit input code was decomposed into two groups, each group is 32 bits respectively with Li-1 and Ri-1 representative. Which i represents the i-th product of transformation, i = 1 ~ 16. (2) input of the second product group which the right group of 32-bit transform into output grouping of 32-bit bit-left group that Li = Ri-1. (3) the right group of 32-bit input group turn into a bit after bit 48-bit code group by expanded operations . (4) the output 48-bit of extended transform add 48-bit sub-key Ki of 48-bit modulo 2 sum , the output of 48 bits divided into 8 groups of 6. (5) 6 bits for each dense sheet (S-box) instead, resulting in 4 bits. The two bit1,6 of which the first 6 bits is entered decided to close the table to select the number of rows and the remaining four decided to close the table's columns. (6) the eight dense table output was merged into 32 bit and then transform the product of this type with the left set of Ci-1 bitwise modulo 2 sum which can be obtained by changing the i-th product of the right 32-bit output Ri.

DES ALGORITHM FEATURES

DES algorithm has the following characteristics: DES key confidentiality depends only on the secrecy and the algorithm open.

At current levels it is impossible that we do not know the keys in a certain period of time to decipher (ie, parse out the key K or plaintext), at least to establish a 256 or 264 items of the table which is available resources can not be achieved.

The "avalanche effect", can not divide and break, a change will lead to a number of simultaneous changes.

CONCLUSION

For most of the need to give top priority to consider the application of confidentiality, the current Bluetooth standard provides data security is not enough. In some cases, bluetooth specification uses the existing 128-bit encryption key length of the sequence,which can be cracked. Also a new Bluetooth security improvement program need to propose ,which adopts strong DES encryption plus key institutions to build algorithms that can improve the current Bluetooth standard to provide data security.

REFERENCES

Chatschik, B., 2001. An overview of the bluetooth wireless technology. IEEE Commun. Magazin, 39: 86-94.

Dallas, S., 2002. DS1820 1-WireTM digital thermometer. Maxim Integrated Products. http://narong. ece. engr.tu.ac.th/microlab /doc/ ds1820.pdf

Hendler, J.A., 1996. Interlligent agents: Where AI meets information technology. In IEEE Expert, 11: 20-23.

Joakim, P. and S. Ben, 2000. Bluetooth security an overview. Inform. Security Technical Rep., 5: 32-43.

Li, J., B.Q. Feng and B. Li, 2006. Genetic algorithm based features reduction. Microelectronics Comput., 23: 151-154.

Li, S.W., Y.P. Wang, J.P. Fu, L.B. Han, Y.L. Song and D. Guo, 2007. Urban road intersection signal timing optimization simulation based on vehicle emissions. J. JiLin Univ., 6: 1202-1214.

Turner, M.B. and M.C. Demir, 2005. A genetic approach to data dimensionality reduction using a special initial population. Proceedings of the International Work Conference on the Interplay between Natural and Artificial Computation, June 15-18, 2005, Las Palmas, Canary Islands, Spain, pp: 310-316.

Weston, J., S. Mukherjee, O. Chapelle, M. Pontil, T. Poggio and V. Vapnik, 2000. Feature selection for SVMS. Adv. Neural Inform. Process. Syst., 13: 668-674.