International Journal of Control and Automation
Vol.7, No.2 (2014), pp.159-166
http://dx.doi.org/10.14257/ijca.2014.7.2.15

Research on the Technique of End-hopping Based Upon Clock-controlled Nonlinear Sequence

Xie Hui[1*], Li Jing[1] and Zhoh Yi-lei[2]

[1]*Dept. of Information Security, Naval Univ. of Engineering, Wuhan, China*
[2]*The 6th detachment, Xing-hai Garden, East-fortune Lake, Ningbo, China*

Abstract

According to the Pseudo-random numbers for the end-hopping technique, an end-hopping communication model combined with Stream Cipher is established, then the key problems of the model are discussed. The model shows the communication based on the clocked nonlinear sequence use random hopping port, which could prevent hackers from seizing the hopping rules of port, and it is an effective way to secure the information. The work analyzes the security of the model , verifies the feasibility of the communications technology in theory, and the performance of the program is simulated.

Keywords: *Stream Cipher; end-hopping; security*

1. Introduction

The technique of end-hopping (EH) is learned from the frequency-hopping (FH) which is mature in the field of wireless communication. The communication could effectively guard against information attack by constantly changing the port which the connection is established on. EH is accepted with anti-jamming, anti-intercepted advantages, and the key technology is pseudo-random synchronization transition of the communication port between the two sides.

Nowadays, the research about EH all over the word, is usually carried out on the basis of the port table agreed on or the address pool created [1-3]: document [1] proposed the concept of EH, document [2] established an active defense model in which the protective function of EH is realized, and the adaptive strategy for EH system is studied in document [3]. The port table or the address pool determined artificially in traditional EH technology is limited in quantity, which is the hidden danger for being intercepted and crack. In this paper stream ciphers were added to original EH system to make the pseudo-random port hopping.

An applied port sequence should have the characteristics of uniform distribution, wide transition interval, good Hamming correlation, random performance and large linear complexity. Sequences that easily realized in FH present are mainly concentrated in m/M-sequence, LCC-sequence, Bent-sequence, *etc.* And NLFSR (Nonlinear Feedback Shift Register) is adapted to the EH [4]. However, all the sequences mentioned are vulnerable to the fast correlation attacks and algebraic attacks for the lack of complexity and confidentiality. Thus, the LFSR-based nonlinear combination generators and nonlinear filter generator is

* *XIE Hui: a vice professor. she does much research on network confrontation and published many excellent papers. Email:1165324303@qq.com*

ISSN: 2005-4297 IJCA
Copyright ⓒ 2014 SERSC

gradually phased out. In contrast, there is increased emphasis on the irregular clocked LFSR (clocked nonlinear sequence). The clock-controlled nonlinear sequence is generally accepted for its good performance and is more mature in traditional cryptography. It is a better pseudo-random number generator method for its great period and linear complexity which could increase the difficulty of intercepting by prediction or the difficulty of tracking interference. The clock-controlled nonlinear sequence is adapted to EH communication in this paper. Pseudo-random number generator based on clock-controlled nonlinear sequence provides the port numbers that needed. It shows that the improved EH technology could effectively prevent the port hopping program from controlling by enemies and the security of the hidden communication is further enhanced.

2. Built-port Communication Model based on the Sequence of Jump Clocked Nonlinear

The prototype EH system that existed has been improved. The clock-controlled linear sequence of pseudo-random number generator which is the important part is added.

2.1 Clock-controlled nonlinear sequence generation mechanism

The clock-controlled sequence is controlled by the level of the clock pulses to the output sequence, which is the principle. The basic model of clocked-controlled sequence generator is that one LFSR determine the shift clock pulses of another LFSR (Figure 1). If LFSR1 output 1, then the shift clock pulses pass through the AND gate, which makes the LFSR2 carry one shift to generate the next one. And the shift clock pulses will not impact the LFSR2 when LFSR1 output 0, which make LFSR2 output the previous number repeatedly.

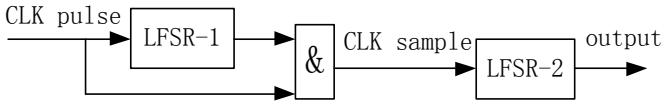

Figure 1. the model of clocked-controlled sequence

Although the clocked-controlled sequence generator greatly enhance the linear complexity, the data is not good enough to meet the requirement of uniform distribution of random numbers. Therefore, it can not be used as a pseudo-random number generator directly. Then the basic clock-controlled sequence is transformed to be added with the m-sequence whose autocorrelation function is constant [5], as shown in Figure 2. The LFSR1 output 16-bit data in parallel, whose lowest bit a1 will AND with the clock signal CLK, which will be input into LFSR2 as the signal that control the clock, then the low 16-bit LFSR2 data will XOR with the 16-bit LFSR1 data that output in parallel. Compared with the multi-stage LFSR in the case of the same number of stages, the output data of this pseudo-random number generator has higher linear complexity, it is evenly distributed and has good autocorrelation characteristics. The design of generator hardware circuit is very simple, which is easy to achieve, and the cycle of the pseudo-random generator is short that 16-bit data is output in parallel in one clock cycle, the generator has great application prospects with these advantages.

 Copyright ⓒ 2014 SERSC

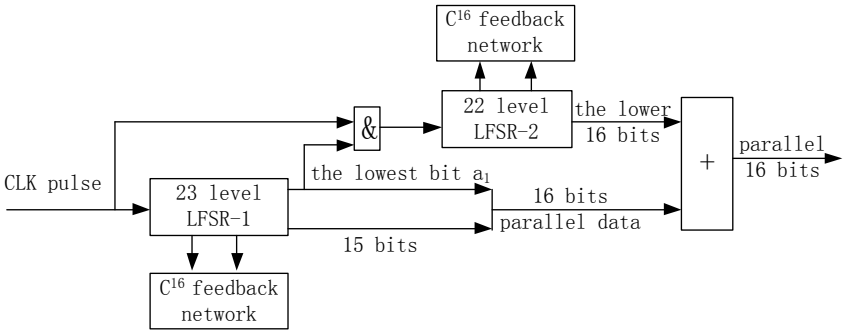

Figure 2. the design diagram of complex pseudo-random number generator based on clock-controlled nonlinear sequence

2.2 The model of EH based on clock-controlled nonlinear sequence

A communication system composed of four modules is constructed in this paper: key-distribution, port-management, data-processing, and collaborative control center, as is shown in Figure 3. The key-distribution module completes the calculation of the shared key in the initial stage of communication and generates the seed key. Port-management module is used to select the appropriate ones from the pseudo-random sequence to create a port table and manage the ports during the communication. The data-processing module is responsible for the encryption and decryption of the information, the data transmission and reception, etc. The collaborative control module is the core of the system, which coordinates the orderly operation of each module, the internal task switching, and expands the external defense.

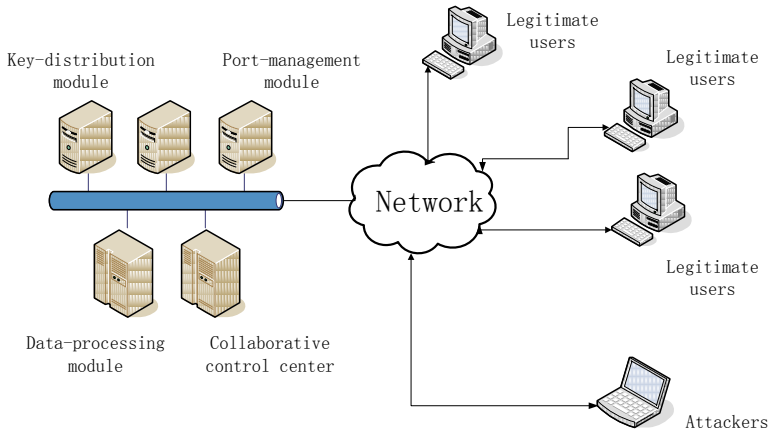

Fig.3 the model of EH based on clock-controlled nonlinear sequence

The end-to-end communication between the two sides is based on the TCP / IP protocol. In the initialization phase of the security communication, the transmitting side sends a data transfer request to the receiving side on the default port, the key distribution server program (recipient) receives and parses the request of the client (the sender). The server replies native randomly generated key computational materials, and the shared key is calculated, and the key will be used as a seed to generate a pseudo-random sequence the next step, then the transition port table can be created. Subsequently, the two sides communicate on the specified port according to the table.

Copyright ⓒ 2014 SERSC

3. Key Technology and Anti-attack Analysis

In the prototype system given above, there are some key issues existed in the design and implementation aspects and these key issues will be discussed next.

3.1 Key Distribution

The program using the Diffie-Hellman algorithm for key distribution, to ensure that the seed key is absolutely safe and reliable. Diffie-Hellman algorithms rely on mathematical calculations to secure communications in an insecure network environment. The key the algorithm generates, on the other hand, can also be used for data encryption and decryption which can reduce the key management safety hazards, as well as the communication load and cost. The security of the Diffie-Hellman algorithm stems from the difficulty of computing discrete logarithm in a finite field.

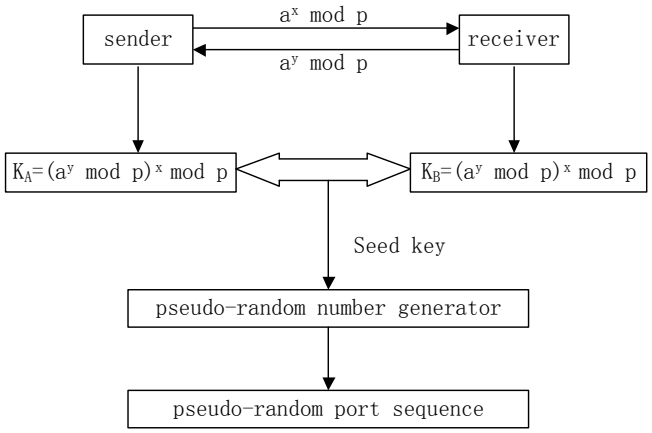

Figure 4. The Key distribution process

As shown above, P, and a is a large public prime number, the sender and receiver select the random number x and y, K_A and K_B are calculated while K_A equals K_B, which will be used as seed key.

3.2 The selection of EH ports

The module will continue to generate a pseudo-random binary string, when the seed key was put into the port-management module. However, this binary string could not be used directly as the port sequence. Considering to the TCP / IP communication port range 0-65536, the binary string is divided in 16 bits units, each divided value represents the port number. The 0-1023 port numbers, which have been assigned to some fixed special applications should be avoided. the following method was used for processing 0-1023 number: square and modulo, the modulo value will be used directly when greater than 1023, or else discarded and continue to deal with the next number; Some numbers within a specified small range could be weeded out from the pseudo-random sequence, which will not affect the characteristics of the sequence.

 Copyright ⓒ 2014 SERSC

3.3 Synchronization mechanism

There are some researches on synchronization problems, such as strict time synchronization [1], time-stamp synchronization mechanism (the UDP spokesman service synchronization) [2], the ACK packet synchronization mechanism [6] and distributed synchronization mechanism [7], modified time-stamp synchronization is taken in this program. In the modified manner, the port information of do not need to be transferred or encrypted, calculated by complex hopping algorithm, comparing with the original way. The system unified the clock with reference to the control center, and the control center got a certain number with its own timestamp as the parameters according to the interval of transition. The number will be sent to the users who query the port-table, then the service was started and information will be fed back to the control center who later send update timestamp instructions to the UDP spokesman server.

The mechanism is simple and easy to achieve, at the same time, the communicating parties could judge the network status and determine the transition time slot according to the timestamp-option which could give the current RTT (round-trip time). To ensure reliable transmission of information, it is clear that transition time interval must be greater than RTT. Otherwise, the message could not be effectively recognized.

3.4 Socket connection migration

The socket connection migration is another key issue of EH technology, the current data transfer did not end when the transition of ports occurred. The UDP protocol is connectionless-oriented, which does not save the information of the communicating parties, therefore, the data migration is easy to implement. The TCP protocol is connection-oriented, and the TCP connection each time with the state was needed to save, therefore, the TCPCP technology [8] related to TCP connection migration was used in this program. The previous connected socket migrates from the foreground to the background, and the connection will not be interrupted during the whole process, which is the principle of TCPCP technical. The other end of the host protocol stack does not need to make any changes, it does not require any non-standard function library support, not either the support of the middle layer, and so, for the other end of the connection, the TCP connection migration process is completely transparent.

3.5 Anti-attack

The security of EH based on clocked-controlled nonlinear sequence is analyzed below: Firstly, the consistent pseudo random port number generated through a safe and secure key distribution, could fundamentally eliminate the security risks of the port table passed link, which will make the attack against a specific port number difficult to form, and prevent the middleman attacks, replay attacks; Secondly, the pseudo-random hopping could reduce the possibility of data packets intercepted by continuous attacks, and increase the difficulty of the packet fragment reorganization decipher. Again, encrypted transmission of data, effectively prevent the stealing attack; The same time, compared to traditional port encrypted transmission mode, the technique avoids the cumbersome port information encryption and decryption and transfer steps to reduce the overhead of network transmission, the transmission efficiency multiplied.

Suppose the number of available addresses is a, available ports is n, the data encryption algorithm is m, and the average transition time interval is t, the attack packet transmission rate is v, and the average packet length is l. Then it can be deduced, that the Dos attacks in a

Copyright ⓒ 2014 SERSC

transition time slot on a fixed port i is $X_i = K_1 \frac{v/l}{an}$ in the ideal case of non-interference. The probability for the attacker who successfully intercepted and decoded information is $P_i = K_2 \frac{1}{an(m+1)}$. Suppose the unavailable threshold condition is that the average attack for continuous-time T is $T(T >> t_A)$ greater than the X_T. Then the unavailable probability of time slot t_h P_i' and availability of steady state P_{Avail} could be expressed as follow [2]:

$$P_i' = P_i(X > X_T) = P_i(K_1 \frac{v/l}{an} > X_T) \tag{1}$$

$$P_{Avail}' = 1 - \sum P_i'^j \ (j \ \ from \ \ T/X_T \ \ to \ \ \infty) \tag{2}$$

Assume that the background noise is uniform and data quantity is N, effective message data is S, and the complete message is divided into u parts, then the probability for the complete message's interception and decode, recombination is

$$P_s = (1/(P^1_{[N/S]+1} m))^u = (1/([N/S]+1)m)^u \tag{3}$$

Obviously, the probability decreases exponentially, and it is visible that the technology can greatly increase the attack time and flow consideration.

4. Performance Simulation of the Program

The new technology that proposed in this paper is simulated and demonstrated in the Matlab platform. During the experiment, the hopping slot is 1 seconds.

From Figure 5 it can be seen, although the packets loss rate of the new technology has slight oscillation but is stable on the whole, and it is increased corresponded while the attack strength gradually increased. The packets loss rate is smaller while compared with the conventional communication technology, it is because the ports hidden could effectively prevent the attacks.

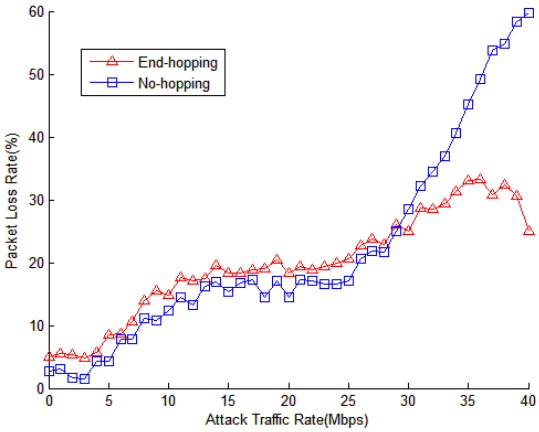

Figure 5. The packet loss rate under different attack

Copyright ⓒ 2014 SERSC

From Figure 6 it can be seen that the average network Throughput is slightly higher than the traditional network communication, this is because the EH technology with anti-jamming capability receive data-packets on different ports, which can alleviate the pressure of receiving and processing on fixed port, effectively decentralize the network traffic.

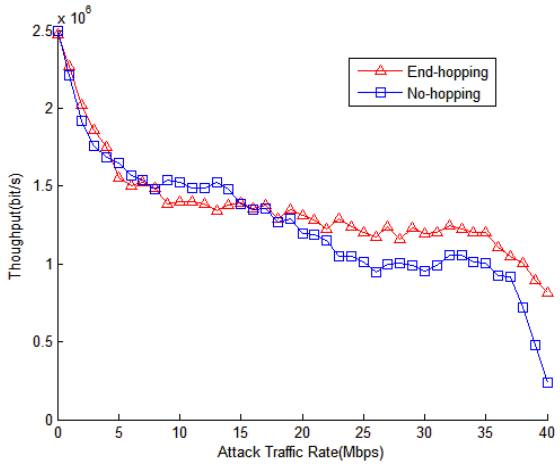

Figure 6. the throughout under different attack

From Figure 7 it can be seen there is a certain degree of end-to-end delay increases, apparently because of multiple TCP connections and release process result in the communication efficiency be affected.

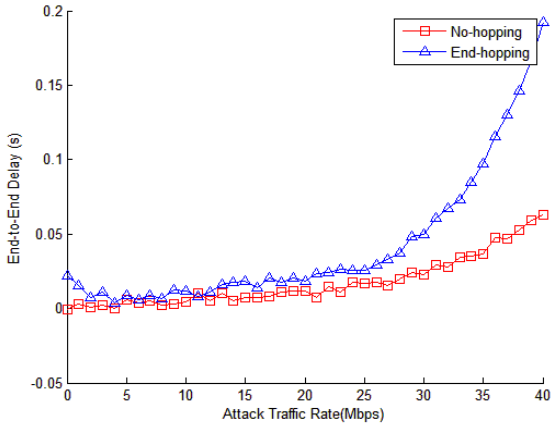

Figure 7. The end-to-end deply under different attack

5. Conclusion

In this paper, a security enhancements technology is proposed, EH combined with the clocked-controlled nonlinear sequence, which solved some security issues that currently exist in EH. The basic principles of the technology, the system model, the implementation process is studied, and the key distribution, synchronization mechanisms, socket migration, the key issues of this technology are discussed and the performance of the program is simulated. This

Copyright ⓒ 2014 SERSC

security enhancement technology is still in the phase of simulation studies, and is needed to demonstrate authentic. In addition, in the complex network environment applications there may be some problems, such as, how to optimize the settings on the transition time or the encryption algorithm, as well as how to achieve the transition on UDP, all these aspects are needed to be further studied.

References

[1] H. Lee and V. Thing, "Port hopping for resilient networks", Conf 60th IEEE Vehicular Technology, **(2004)**, pp. 3291-3295.
[2] S. Le-yi, J. Chun-fu and L. V. Shu-wang, "Research on end hopping for active network confrontation", Journal on Communications, vol. 29, no. 2, **(2008)**, pp. 106-110.
[3] Z. Chun-lei, J. Chun-fu, W. Chen and L. Kai, "Research on adaptive strategy for end-hopping system", Journal on Communications, vol. 32, no. 11, **(2011)**, pp. 51-57.
[4] C. Jian, "Design and implementation of Port-Hopping technology based on nonlinear shift register", Ocean University of China, **(2009)**.
[5] Q. Xue-li, C. Ming and L. Wei, "RFID pseudorandom number generator based on clock-controlled non-linear sequence", Journal of Computer Applications, vol. 29, no. 11, **(2009)**.
[6] H. Badishiy, A. Herzberg, I. Keidar, *et al.*, "Keeping denial-of-service attackers in the dark", Int Symp Distributed Computing (DISC), Springer-Verlag, **(2005)**, pp. 18-31.
[7] K. Lin, C. F. Jia and C. Weng, "Distributed timestamp synchronization for end hopping", China Communications, vol. 8, no. 4, **(2011)**, pp. 164-169.
[8] X. Qun-feng and S. Jie, "Elaborates of TCPCP----the technology of TCP connetion migration on Linux", Science and Technology Consulting Herald, **(2007)**.
[9] L. Kai, "Design and Implementation of End-Hopping System", NANKAI University, **(2010)**.
[10] M. Wei-ju and F. Deng-guo, "On a clock-controlled keystream generator and its cryptographic properties", Journal on Communications, vol. 28, no. 7, **(2007)**, pp. 42-47.
[11] L. Kai, J. Chunfu and S. Leyi, "Improvement of distributed timestamp synchronization", Journal on Communications, vol. 33, no. 10, **(2012)**, pp. 110-116.
[12] L. Kai and J. Chunfu, "A Punching Scheme for Crossing NAT in End Hopping", Wuhan University Journal of Natural Sciences, vol 17, no. 6, **(2012)**, pp. 539-543.

 Copyright ⓒ 2014 SERSC