# A Data-encrypted Transportation Framework Based on Composite Discrete Chaotic System

Hongqian Chen, Yi Chen , Li Liu
A School of Computer & Information Engineering
Beijing Technology and Business University
Beijing, 100048, China
chenhongqian1@163.com

***Abstract*-To improve the security of data in distributed simulation system, propose a data-encrypted transportation framework. The framework encrypts the simulation data via the composite chaotic system in simulation. It can obtain the data security in data transportation based on the composite discrete chaotic system. The framework can be accomplished via the federator-based structure, which add an encrypt federator for each simulation group. The encryption algorithm can achieve the self-synchronization because of the feature of the chaotic system. The chaotic system can produce continuous acyclic encrypt key for each simulation data. This framework has been proved feasible and effective.**

***Keywords-Data Security, Chaotic System, Distributed Simulation, Data-Encryption, HLA***

## I. INTRODUCTION

The distributed simulation system [1] is becoming more and more powerful. The High-Level Architecture (HLA) defines an approach to integrate separate autonomous simulators into a single distributed simulation system. Data exchange and other services in the HLA framework are realized by the Runtime Infrastructure (RTI) [2]. The RTI provides services of data transferring to support simulations and to carry out federate-to-federate interactions. In commonly case, the data are transferring directly using RTI services. Each of federator in the federation can access the transferring data via RTI services [2].

With the increase in the scale and complexity of simulations, the data security in the processing of simulation is one of the most important topics in distributed system. Encryption is the popular method to achieve the security purpose currently [3].

There are two type of encryption algorithm who named Block Cipher and Stream Cipher [4]. The Block Cipher divides the data into block with unified length, and encrypts them individually. The encryption for each data block is independent of each other. It has the advantages such as fast processing and storage-saving. But it just provides inferior security. Stream Cipher can produce difference cipher text even from the same plain text. But it has the complex processing in generate, transfer and store for encryption key [5]. Most of Stream Cipher algorithm is also secretive. The public algorithm includes A5, SEAL, RC4, PIKE and etc.

Chaos is one form of nonlinear dynamic system [6, 7]. It is pseudo-random phenomena between certainty and randomness. It has some interesting features as following. A) It is extremely sensitive to initial condition and parameters. The feature can lead unpredictable result from a long-term sense. B) It has topological transitivity, which means high randomness. C) The nonlinear system where chaos located is a certain system, which states the system has strong certainty and regularity. The features of chaos are match closely to the requirement in cryptology. The chaos system can simplify the procedure of building stream encryption key in. The encryption key produced from chaos system has excellent ability.

The fitting encryption method in simulation should achieve the following features: A) The encrypt algorithm is suitable with various block size data. The federator could produce uncertain data size block in simulation. The half-baked or incorrect data could lead to enigmatical simulated result. B) The algorithm is efficient to avoid affect the simulation processing. The real time interaction is required generally among federators in simulation. C) The algorithm has special encryption key mechanism to prevent being decoded during the simulation. The simulation often cost a long period of time. The encryption scheme need update its setting to provide more strength security.

In this paper, we focus on introducing the composite discrete chaotic system [9] into the data-encrypted transportation procedure. And we propose a framework to improve the security for the high level architecture (HLA). The framework which can achieve encrypted transportation of simulation data in distributed simulation. The framework can be accomplished via two structures. One is module-based structure, which add an encrypt module for every federator. The other is federator-based structure, which add an encrypt federator for each simulation group. The security of the simulator is obtained via logic and flexible federation construction.

The framework proposed in the paper has the following feature comparing to the traditional one. A) This framework can achieve the access-controlling by authority for members. The encryption function can integrate into the federators as a module. B) The chaos system automatic reproduces the stream encrypt key along with advancing of simulation, while the traditional encryption scheme need to the management and distribution of encrypt key. C) The chaos-based encryption algorithm works on the continuous real

Published by Atlantis Press, Paris, France.

numbers set, while the traditional algorithm works on the discrete integer number set.

The remainder of this paper is organized as follows: In Section 2, an overview of the HLA architecture, the encryption and related work is given. Section 3 describes in detail this distributed simulation framework design and technical issues arising from this approach. Section 4 presents the analysis of the simulation framework. Finally, Section 5 summarizes the framework.

## II. THE DATA-ENCRYPTED TRANSPORTATION FRAMEWORK

According to the requirement in the encryption in distributed simulation system, we introduce the composite discrete chaotic system into the high level architecture (HLA) standard. The encryption function can be achieved by two forms which named separately encrypt module-based and encrypt federator-based structure. The encrypt federator is named "Encryptor" in the paper.

### A. Encryption Federator-based Framework

The encryption federator-based framework divides the whole simulation system into several groups. It is suppose that the data is secure within each group in the framework. The encryption function is accomplished by a federator which independent of original federators. The structure of the federator-based framework is described as Figure 1.

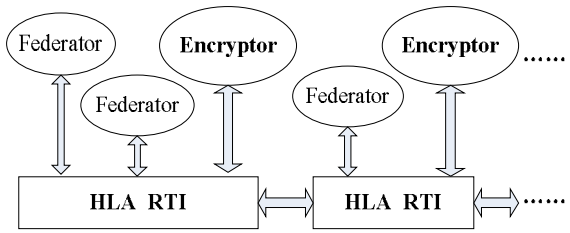


Figure 1. The Structure of Encryption Federator-based Framework

The messages data among federators are encrypted by the encryption federator before transfer the destination. The data are transferred to the actual destination federator by the encryption federator. At the same situation, the receiving data are decrypted by the federator firstly.

This framework has some advantages such as modifying the federator and the OMT files less than the frontier one. But the framework redesigns the logical relation among federators. The step of transferring data increases from one step to two, which could affect the performance of simulation system. The security of system could be cut down because of more transferring path.

### B. The Data-encrypted Algorithm

According to the requirement in the encryption in distributed simulation system, this paper proposes the data encrypted method based on the composite discrete chaotic system. The chaotic system generates the chaos sequence which can be transformed into binary value. The binary value sequence was combined into chaos encryption key. This key can be used as direct operator or in traditional encryption algorithm as encryption key. And the key also can be updated for each data block via chaotic iteration.

The composite discrete chaotic system has two chaotic iteration equations. The system can select automatically one equation according to the plain text stream. The chaos-based algorithm can achieve the aim of one-time pad encryption because of the updating chaos key.

### C. Composite Discrete Chaotic-based Encryption

The iteration in the composite discrete chaotic system [9,10] depends on both the frontier iteration result and the plain data. The feature takes up a new method which has more randomness.

There are two iteration equations $f_0(x)$ and $f_1(x)$ in one composite discrete chaotic system. It selects one equation $f_0(x)$ or $f_1(x)$ to execute depends on the plain data and the frontier iteration result in each step of iteration.

The executing of composite discrete chaotic iteration $n$ depends on the plain data mn-1 and the frontier iteration xn-1. In the other word, the Ciphers data can not be decrypted if have not the frontier part of the data. The feature can take more security when transport.

The iteration formula of the composite discrete chaotic can be described as Equ.1.

$$x_{n+1} = \begin{cases} f_0(x_n), & m = 0 \\ f_1(x_n), & m = 1 \end{cases} \tag{1}$$

In Equ.5, m is the current bit of plain data, $f_0(x)$ is the corresponding iteration equation for the current bit 0, while $f_1(x)$ is corresponding to the current bit 1. They can show respectively as Equ.2.

$$f_0(x) = \begin{cases} 1-\sqrt{1-2x}, & 0 \le x < \frac{1}{2} \\ \sqrt{2x-1}, & \frac{1}{2} \le x < 1 \end{cases}$$
$$f_1(x) = \begin{cases} \sqrt{1-2x}, & 0 \le x < \frac{1}{2} \\ 1-\sqrt{2x-1}, & \frac{1}{2} \le x < 1 \end{cases} \tag{2}$$

The summation of the two equations $f_0(x)$ and $f_1(x)$ is always equal to 1. The equation $f_0(x)$ is selected when the current bit in the plain text is zero (0). While the equation $f_1(x)$ is selected when the current bit in the plain text is one (1). The next binary bit in the sequence of composite discrete chaotic system is produced by the selected equation. The encrypted text is obtained by the XOR operation between the chaotic sequence and the plain text.

Published by Atlantis Press, Paris, France.

### D. Synchronization in Composite Discrete Chaotic-based System

The decryption is the inverse processing relative to the encryption processing. The decryption needs the self-synchronization according to the encrypted text.

The decryption firstly constructs a reversible transformation $H$ and its inverse transformation $v$, which can be expressed with Equ.3.

$$\begin{aligned} H: \quad & y(k) = \sqrt[3]{\tfrac{1}{3}x(k)} \\ v: \quad & x(k) = 3y^3(k) \end{aligned} \tag{3}$$

The function $q$ is set as the following Equ.4.

$$\begin{aligned} & q(x_m(k), y(k)) = 1/8 \cdot e(k) \\ & = 1/8 \cdot (x(k) - v(y(k))) \\ & = 1/8 \cdot (x(k) - 3y^3(k)) \end{aligned} \tag{4}$$

The iteration equation $e(k+1)$ can be obtained approximately by the follow Equ.5.

$$e(k+1) = (\frac{1}{8})^{k+1} e(0) \tag{5}$$

The iteration system can be concluded that it will be gradually stabilized. The response system can be expressed by Equ.6.

$$\begin{aligned} & Y(k+1) = g(y(k), x_m(k)) \\ & = H(f_m(x_k) - q(x_m(k), y(k))) \end{aligned} \tag{6}$$

And the two chaotic system expressed by the Equ.1 and the system expressed by the Equ.8 are the systems with generalized chaos synchronization. The encryption and decryption algorithm can be summarized by the following Equ.7.

$$\begin{aligned} & f_m(x(k)) - q(x_m(k), y(k)) \\ & = f_q(x(k)) - \frac{1}{8}(x(k) - 3y^3(k)) \\ & Y(k+1) \\ & = H(f_m(x(k)) - q(x_m(k), y(k))) \\ & = \sqrt[3]{\frac{1}{3}(f_q(x(k)) - \frac{1}{8}(x(k) - 3y^3(k)))} \end{aligned} \tag{7}$$

$x(k)$ is the encrypting sequence produced by the chaotic system, while the $v(Y(k))$ is the decryption sequence, which is the inverse operation of the equation $Y(k+1)$.

## III. Application and Analysis

This paper proposed a frameworks for distributed simulation including the function of encrypted transportation. The framework is implemented based on HLA/RTI system, which had been widely applied in distributed simulation. The framework are constructed with the ordinary federator and the encryption federator.

We realize a small distributed simulation system base on the framework proposed in this paper. There are three simulation federators in the system. The system encrypts the simulation data using the chaos key. The experimental environment includes Intel Core2 3.0GHz CPU， 1GB RAM，Windows XP Sp2 OS.

The result demonstrates that the framework can qualified the encryption requirement in the distributed simulation system. The simulation data can be accurately encrypted and decrypted at sender and receiver respectively. The time cost of chaos encryption and decryption is less than 300ns. It affects little to simulation performance.

## IV. Summaries

This paper proposes a distributed simulation framework with data-encrypted transportation function. The framework obtains more security in data transportation via encrypting the plain data based on the composite discrete chaotic system. The framework has some advantages as following. The encryption Scheme is designed according to the feature of the data security in the system. The chaotic system-based algorithm can generate the encryption key which has the same length with the plain data. So it can suit for encrypting any length simulation data. The encryption algorithm can achieve self-synchronization due to the transformation and the inverse transformation in the composite discrete chaotic system. The chaotic system can produce continuous acyclic encrypt key for every federator during the whole of simulation. It can provide higher security than symmetrical encryption system.

This framework has been proved utility and feasible. The future works include researching the chaos-based encryption algorithm on the graphic hardware.

## V. Acknowledgment

This work was supported by the Fund for Young Teachers and the Fund for the Beijing Key Construction Subjects. We are grateful to our schoolmates and colleagues for their help of proofreading this paper.

## References

[1] Richard M. Fujimoto, Parallel simulation: parallel and distributed simulation systems. Proceedings of the 33nd conference on Winter simulation, Arlington, Virginia, (2001) 147 - 157

[2] Dahmann, J.S., Morse, K.L., Sci. Applications Int. Corp., High Level Architecture for simulation, Proceedings. 2nd International Workshop on Montreal, Distributed Interactive Simulation and Real-Time Applications, , Que., Canada, (1998) 32-40

[3] Szabo, C.; Teo, Y.M.; An Approach for Validation of Semantic Composability in Simulation Models, Principles of Advanced and Distributed Simulation, 2009. PADS '09. ACM/IEEE/SCS 23rd Workshop, 2009: pp 3-10.

[4] Ewald, R. Himmelspach, J. Uhrmacher, A.M. An Algorithm Selection Approach for Simulation Systems, Principles of Advanced and Distributed Simulation, 2008. PADS '08. 22nd Workshop Page(s): 91 - 98

[5] Bellare, M., Boldyreva, A., Micali, S.: Public-key encryption in a multi-user setting: Security proofs and improvements. In: EUROCRYPT'00. Volume 1807 of LNCS. (2000) 259–274

[6] Gleick, James, Chaos making a new science, Book, ISBN: 9781400925018, New York: Viking Penguin Inc., 1987

[7] Goce Jakimoski, Ljupco Kocarev, Chaos and cryptography: Block encryption ciphers based on chaotic maps, IEEE Transactions on Circuits and Systems-I:Fundamental Theory and Applications, 2001(2)

[8] Wei Song, Jun Meng, Research on Logistic Mapping and Synchronization, Preceeding of Sixth World Congress on Intelligent Control and Automation, (WCICA2006), vol.3, 987-991

[9] LI Hong-Da, FENG Deng-Guo, Composite Nonlinare Discrete Chaotic Dynamical Systems and Keyed Hash Functions, Chinese Journal of Computers, (2003) 460 – 464

Published by Atlantis Press, Paris, France.