Improve the Fault-tolerance of Spatiotemporal Chaotic Stream Cryptosystem by Coupled-drivers Model

Jing Guo, Jian Yuan, Jian Wang, Xiuming Shan, Yong Ren

Electronic Engineering, Tsinghua University
Beijing, China
Email: guo-j04@mails.tsinghua.edu.cn, jyuan@tsinghua.edu.cn, jian-wang@tsinghua.edu.cn,
shanxm@tsinghua.edu.cn, reny@tsinghua.edu.cn

Abstract– A coupled-drivers model was present to improve the fault-tolerance of spatiotemporal chaotic stream cryptosystem. In this model, the driver signals were generated by two coupled chaotic systems, with error detection and correction at the receiver. This model is applicable to all kinds of spatiotemporal chaotic systems base on driver-response synchronization scheme. Theoretical analysis and simulations were given to show the improvement of system's tolerance under channel noise and active attacks. In conclusion, the model present by this article could significantly improve the system's fault-tolerance without loss on security.

Key words– spatiotemporal chaos, stream cryptosystem, error propagation, coupled-drivers

1. Introduction

In the past decade, there has been tremendous research in spatiotemporal chaotic cryptosystems[1]-[3]. To ensure the legitimate receivers decrypt correctly and efficiently, driven synchronization scheme, which divides the whole system into driver subsystem and response subsystem, synchronizes the spatiotemporal chaotic systems at transmitter and receiver with as little as possible driving information. As a result, the system is lack of detection capacity against channel noise and active attacks. The errors, which are omitted by channel coding layer, propagate in spatiotemporal chaotic system, and could be discovered only after decryption.

Moving instability of the coupled chaotic system is the basis of security, while causes error propagation at the same time. According to reference [4], propagation in coupled chaotic system is related to the system's commoving Lyapurov indexes. Reference [5] gave the relations between them under homogeneous assumption. Reference [6] made improvement to the self-synchronized system, which suggested to reasonably increasing the driver information to avoid errors in decryption. If properly improved, the system's robustness, security, as well as encryption (decryption) speed would be enhanced simultaneously.

In this article, we changed the traditional driven synchronization scheme and propose a novel spatiotemporal chaotic stream cryptosystem based on coupled-drivers model. The essential thinking is to detect and correct errors in the driver subsystem with the help of error propagation law of the coupled chaotic system, before them spreading into the response subsystem. There are two main changes put forward, including coupled-chaos structure in the driver subsystem and error detection and correction between driver and response subsystems. We will give detailed description in the following sections.

2. Coupled-drivers Model

2.1. Coupled-chaos Structure in the Driver Subsystem

Generally, spatiotemporal chaotic system is described by the model of equation (1).

$$\begin{aligned} y_0(n) &= x(n) = f(x(n-1)) \\ y_i(n) &= (1-\hat{\varepsilon})h(y_i(n-1)) + \\ &\hat{\varepsilon}\cdot h(y_{i-1}(n-1)), i=1,2,\cdots,I \end{aligned} \tag{1}$$

Here, $x(n)$ is the driver subsystem, $y_i(n), i=1,2,\cdots,I$ is the response subsystem, $f(\cdot)$ and $h(\cdot)$ are chaotic mappings, and $\hat{\varepsilon}\in(0,1)$ is the coupling strength of response subsystem. Keys of encryption and decryption are generated by the above model.

Different from the traditional system, the coupled-drivers model introduces a coupled-chaos structured driver subsystem, as shown in equation (2-1) and (2-2), while the response subsystem is similar with the traditional one.

$$\begin{aligned} x_{1,2}(n) &= (1-\varepsilon)f_{1,2}(x_{1,2}(n-1)) + \\ &\varepsilon f_{2,1}(x_{2,1}(n-1)) \end{aligned} \tag{2-1}$$

$$\begin{aligned} x''_{1,2}(n) &= (1-\varepsilon)f_{1,2}(x''_{1,2}(n-1)) + \\ &\varepsilon f_{2,1}(x'_{2,1}(n-1)) \end{aligned} \tag{2-2}$$

Both of $\{x_1(n)\}$ and $\{x_2(n)\}$ are sent into the channel, and only $\{x_2(n)\}$ and $\{x''_2(n)\}$ are used to drive the response subsystem at the transmitter and receiver. Under ideal circumstances, $\{x_{1,2}(n)\}=\{x'_{1,2}(n)\}$, where $\{x'_{1,2}(n)\}$ stands for the received signals, so that the synchronization of $\{x''_{2,1}(n)\}$ and $\{x_{2,1}(n)\}$ also achieves. However, errors in $\{x'_1(n)\}$ and $\{x'_2(n)\}$ caused by channel noise or active attacks may destroy the above synchronization. So we have to detect errors with the help of $\{x'_{1,2}(n)\}$ and $\{x''_{1,2}(n)\}$.

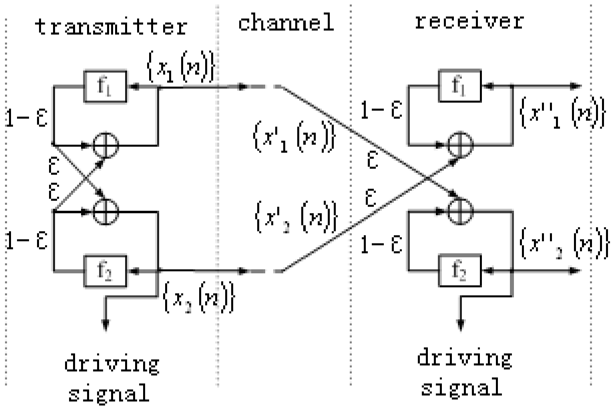

Fig. 1 Coupled-drivers model

2.2. Detection and Correction of Errors

As mentioned in reference [7], error propagation range is related to several system parameters, such as coupled strength and precision. Under that consideration, we set four integers, namely L_1, L_2, L_3 and L_4, to optimize the effects of detection and correction. In the following sections, we take $L_1 = 2\, or\ 3$, $L_2 = L_3$, $L_1 < L_4 < 2 \cdot L_2$.

We check the elements of $\{x'_1(n)\}$ and $\{x'_2(n)\}$ by ascending sort of n at the receiver. Take $\{x'_1(n)\}$ as example, the detection consists of the following steps.

- Step 1 of Detection

If $\exists k \in [0, L_1 - 1]$,
so that $x'_1(n-k) \neq x''_1(n-k)$,
then $x'_1(n) \in E_1$.

- Step 2 of Detection

If $\exists k_1, k_2 \in [0, L_2 - 1]$and $\exists k_1 + k_2 + 1 \le L_2$,
so that $x'_1(n - k_1 - 1) = x''_1(n - k_1 - 1)$,
$x'_1(n+k) \neq x''_1(n+k), k = n - k_1, \cdots, n + k_2$
and $x'_1(n + k_2 + 1) = x'_1(n + k_2 + 1)$,
then $x'_1(n+k) \in E_2, k = n - k_1, \cdots, n + k_2$.

- Step 3 of Detection

If $x'_1(n) \neq x''_1(n)$, $\forall k \in [1, L_3]$,
so that $x'_2(n+k) \neq x''_2(n+k)$,
then $x'_1(n) \in E_3$.

Check elements in $\{x'_1(n)\}$ and $\{x'_2(n)\}$ with the above steps, then we obtain three sets, namely E_1, E_2 and E_3. Let $E = E_1 \cap (E_2 \cup E_3)$, and treat the elements of E as wrong symbols.

If $x'_2(n) \in E$, then we attempt to correct it by the following steps.

- Step 1 of Correction

If $x'_1(n-1) \notin E$ and $x'_2(n-k) = x''_2(n-k)$ with every $k \in [0, L_1 - 1]$, then we consider $x''_2(n)$ as correct, and replace $x'_2(n)$ with it. If the above conditions couldn't be satisfied, then

- Step 2 of Correction

If $\exists \hat{n} \in [n - L_4, n - 1]$, so that for every $k \in [0, L_1 - 1]$, it shows that $x'_{1,2}(\hat{n} - k) = x''_{1,2}(\hat{n} - k)$, then define the maximal $\hat{n}$ as $\hat{n}_{\max}$. Replace $x'_{1,2}(\hat{n}_{\max})$ with $x''_{1,2}(\hat{n}_{\max})$, and calculate $x''_2(n)$ iteratively by equation (1). We consider $x''_2(n)$ as correct, and replace $x'_2(n)$ with it. If the above conditions couldn't be satisfied, then

- Step 3 of Correction

Report the error and require the transmitter to resend.

3. Properties of the Coupled-drivers Model

3.1. Robustness against Channel Noise

With the help of coupled-drivers model, most of the errors in the received driving signal are prevented from entering the response subsystem. In this section, we'll analyze the failure probability of detection.

As mentioned in section 2.2, elements of set E are treated as wrong symbols. It should be noted that the actual set, which consists of all driving symbols affected by the channel noise, should not be exactly the same as E. The probability of an wrong driving symbol, which is not belong to E, is considered as the error rate out of the coupled-drivers model. The out-symbol-error-rate is related to the definition of E_1, E_2 and E_3.

According to the first step of detection, if $\exists k \in [0, L_1 - 1]$, so that $x'_1(n-k) \neq x''_1(n-k)$, we'll treat $x'_1(n)$ as an element of E_1. However, a correct driving symbol could also lead to a similar situation. Simulations were carried out to find the upper limit of that probability. Suppose that a symbol consists of M bits, figure 2 shows the simulation results under an AWGN channel. The horizontal axis stands for the channel bit error rate, namely P_e, while the vertical axis stands for the out-symbol-error-rate of the coupled-drivers model. Other parameters are: $f(a) = 1 - 2a^2$, $\varepsilon = 0.8$. As can be seen from figure 2, the OSER (out-symbol-error-rate) is tremendously reduced compared to the channel symbol error rate, which is $1 - (1 - P_e)^M$.

As to the other steps of detection, the situation is similar. Figure 3 shows the relation between OSER and

SNR (signal-noise-ratio). In this simulation, $\{x'_1(n)\}$ and $\{x'_2(n)\}$ were transmitted in independent AWGN channels, and other parameters are: $M = 8$, $\varepsilon = 0.8$, $L_2 = L_3 = 12$, $L_4 = 20$. As can be seen from figure 3, the out-symbol-error-rate could be distinctly reduced by proper parameters.

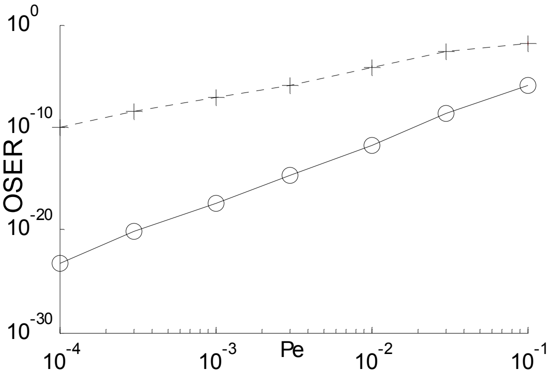

Fig. 2 The OSER of the first detection step (plus + for $M = 8$, circle o for $M = 32$), plotted vs the error bit rate in the noisy transmission channel noise.

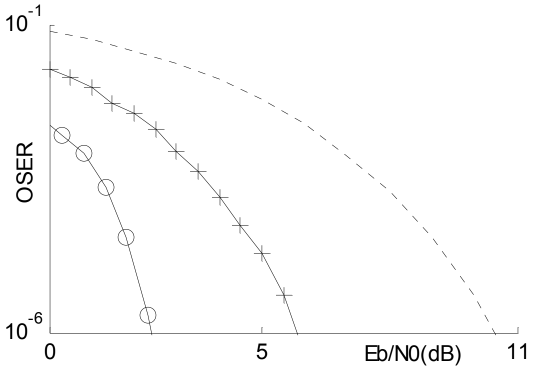

Fig. 3 The OSER of the first detection step (plus + for $L_1 = 2$, circle o for $L_1 = 3$ and dashed line for the traditional cryptosystem without coupled-drivers model), plotted vs SNR.

3.2. Security

3.2.1. Cryptanalysis

As we know, the keys of encryption and decryption are generated by the response subsystem, so the key generating structure won't be influenced by the improvement. As mentioned in reference [8], the properties of the keys are related to the driving signal. So, the task now is to compare the security of the cryptosystem based on coupled-drivers model and the traditional driver subsystem. We have evaluated the security by trying various cryptanalysis methods based on key-sensitivity analysis and statistical-property analysis with the knowledge of system structure and plaintext, and find that no any tested method, which is ineffective to the original cryptosystem, can be effective than the brute force attack to the modified one. So we claim that the coupled-drivers model doesn't reduce security of the cryptosystem.

3.2.2. Active Attack

In the traditional spatiotemporal chaotic stream cryptosystem, the driving signal is sent into the channel together with the ciphertext. It's worse to be modified in the driver signal, for a cryptosystem base on driver-response synchronization scheme, than in the ciphertext. Because a false driver symbol could lead to error propagation in the response subsystem at the receiver, which is likely to cause large numbers of wrong decrypted symbols, while a false ciphertext symbol just cause one. To make matters worse, the modification by the attacker could only be discovered by semantic analysis after decryption. So the traditional cryptosystem is vulnerable to attacks in the driver signal.

As to the improved cryptosystem, because of the detection in the coupled-drivers model, it's convenient to discover the changes of driver signal before decryption. We have evaluated the security of the improved system under various active attacks, such as insertion, deletion and modification, and found that the coupled-drivers model is useful against these attacks.

In the case of modification attack, the attacker couldn't escape from detection, unless he calculates a new driver sequence, which is different from the working one and doesn't satisfy the three conditions of detection in section 2.2. This is an extremely hard work, taking account of the instability of chaotic systems. Considering modification to a group of successive driver symbols, figure 4 shows the probabilities of failure detection to different modified symbol numbers. The horizontal axis stands for the number of modified symbols, while the vertical axis stands for the probability of failure detection. It's obvious that the coupled-drivers model detected the vast majority of modification attack.

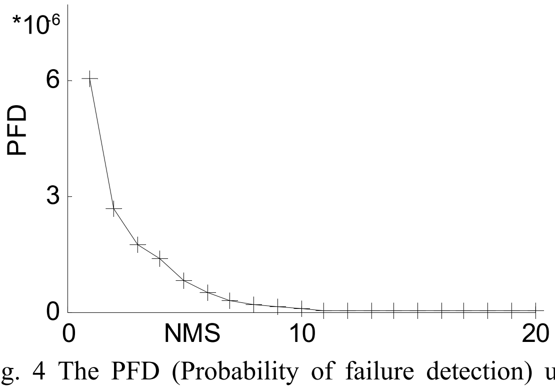

Fig. 4 The PFD (Probability of failure detection) under modification attacks, plotted vs the NMS (Number of Modified Symbols).

Similar simulations have been taken for insertion attacks and deletion attacks, and the probability of failure detection is even less. Consequently, we claim that the modified cryptosystem base on coupled-drivers model is more secure than the original one.

3.3. Encryption (decryption) speed

The coupled-drivers model proposed by this article, which is based on the driver-response synchronization scheme, only modifies the driver subsystem. Usually, the parameter I in equation (1), which is the space size of spatiotemporal chaotic system, is considerably large (which is suggested to be larger than 10 in practice). The structure of coupled-drivers model is similar with the response subsystem, so it can be seen that the space size of the modified spatiotemporal chaotic system is $I+1$. From this point of view, the encryption (decryption) speed doesn't reduce too much. Another crucial factor is the process of detection and correction, as mentioned in section 2.2. In the software implementation, status information is put into the memory in each iteration. Therefore, the time complexity is just $O(n)$, where n is the iteration number of the spatiotemporal chaotic system. Specifically the modified system ($I=20$) can encrypt 895 Mbit and 331 Mbit per second with 2 GHz and 512MHz CPU computers, respectively, while the traditional one ($I=20$) produces 932 Mbit and 357 Mbit ciphers for the same computers. Based on the above discussion of two aspects, the encryption (decryption) speed of the modified cryptosystem is close to the traditional one, and is acceptable in practice.

4. Conclusions

In conclusion, we have suggested a novel driver subsystem, namely coupled-drivers model, for spatiotemporal chaotic stream cryptosystems based on driver-response synchronization scheme. This model makes use of the law of error propagation in coupled chaotic systems, and detects and corrects errors in the received driver signal. We have carried out simulations to prove the detection capacity of the model. The results show that, the improved cryptosystem is robust in AWGN channel. In addition, more analysis and simulations show that, the cryptosystem based on coupled-drivers model is more secure than the original one under cryptanalysis and active attacks. The encryption (decryption) speed of the improve cryptosystem is also acceptable in practice. The coupled-drivers model is an improvement to the traditional driver subsystem, so is applicable to all kinds of spatiotemporal chaotic stream cryptosystems based on driver-response synchronization scheme.

References

[1] L. Kocarev, “Chaos-based cryptography: A brief overview “, *Circuits and Systems Magazine, IEEE*, vol. 1, pp. 6-21, 2001.

[2] W. P. Ye, Q. L. Dai, S. H. Wang, et al. “Experimental realization of a highly secure chaos communication under strong channel noise”, *Physics Letters A*, vol. 330, pp. 75-84, 2004.

[3] S. H. Wang, J. Y. Kuang, J. H. Li, et al. “Chaos-based secure communications in a large community”, *Physical Review E*, vol. 66, pp. 065202 (1-4), 2002.

[4] E. Klein, R. Mislovaty, I. Kanter, et al. “Public-channel cryptography using chaos synchronization”, *Physical Review E*, vol. 72, pp. 016214 (1-4), 2005.

[5] K. Kaneko. “Propagation of disturbance, co-moving Lyapunov exponent and path summation”, *Physics Letters A*, vol. 170, pp. 210-216, 1992.

[6] H. P. Lv, G. Hu. “Propagation of desynchronous disturbances in synchronized chaotic one-way coupled map lattices”. *Physical Review E*, vol. 69, pp. 036212 (1-4), 2004.

[7] J. Guo, J. Yuan, J. Wang. “Spatiotemporal chaotic stream cryptosystem based on coupled-drivers model”, *J. Tsinghua Univ. (Sci. & Tech.)*, vol. 49, No. 8, 2009.

[8] Y. X. Xia, X. M. Shan, Y. Ren. “Influence of the Driving Sequence to Synchronized Spatiotemporal Chaos”, *NOLTA*, 2002.