A brief survey and some discussions on chaos-based communication schemes

K. Busawon, P. Canyelles-Pericas, R. Binns, I. Elliot and Z. Ghassemlooy

(Invited Paper)

***Abstract*—Reaserch on chaos-based communication, or simply chaotic communication, has been ongoing since the early nineties. It was argued that chaotic communication has the potential of addressing the security issue that is omnipresent in standard communication systems, yet this technology has not taken over traditional methods of communication. In this paper, we give a brief survey on the existing methods for designing chaos-based communication schemes. We also provide a discussion as to why there is still some reluctance in applying this technology in practice. Finally, we propose some solutions to address this issue. In more detail, we propose a framework for the development of the fifth generation of chaotic cryptosystems based on bridging chaotic and traditional modulation methods. Then, we discuss the shape that this generation of chaotic cryptosystems could take and explain the challenges in designing and implementing them.**

***Index Terms*—Chaos-based communication, parameter modulation, inclusion methods, cryptosystem**

I. Introduction

The problem of designing a secure communication system using synchronization between chaotic systems has been the subject of intensive research over the last few decades. In effect, research on this topic started since the 1990's, when it was discovered that deterministic chaos can be controlled and that two chaotic oscillators can be indeed synchronized (see eg. [1],[2],[4],[5]); even though they exhibit extreme sensitivity with respect to their initial conditions and parameters. In [3], a comprehensive survey is carried out and classified according to the research evolutions on this topic; thus leading to four generations of research development in that area. In what follows, some of the ideas from [3] are borrowed and detailed. The first generation of chaotic communication schemes was developed in 1993 and is known as chaotic shift keying as shown in Figure 1, and as additive chaos masking/modulation as displayed in Figure 2.

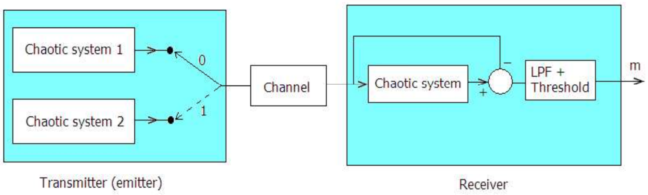

Figure 1. Chaotic shift keying

K. Busawon, P. Canyelles-Pericas, R. Binns, I. Elliot and Z. Ghassemlooy are with Northumbria University, Department of Mathematics, Physics and Electrical Engineering, Newcastle upon Tyne, NE1 8ST, UK. krishna.busawon@northumbria.ac.uk

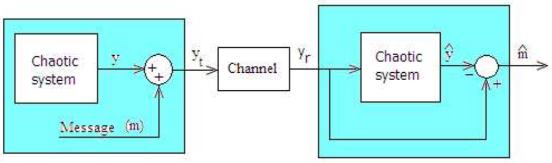

Figure 2. Additive chaos masking

In the chaotic shift keying methods, the two chaotic systems have same structure but different parameters so that their attractors are statistically similar. This scheme was designed to transmit digital messages. In this method, the message signal is used to switch the transmitted signal between the two statistically alike chaotic attractors, which are respectively used to encode bit 0 and bit 1 of the message signal. At the receiver end, the received signal is used to drive a chaotic system, which is identical to any of the two chaotic systems in the transmitter. The message is recovered by low-pass filtering and by thresholding the error signal. This scheme is very robust to noise and parameter mismatch. However, it has a low degree of security if the chaotic attractors are too far away in the bifurcation space and the switching becomes obvious. However, there may still exist many possibilities of improving this technique, as well as for application in other areas.

The additive chaos masking scheme is shown in Figure 2. It consists of two identical chaotic systems in both the transmitter and the receiver. The chaotic mask denoted by $y(t)$ is one of the state variables of the chaotic system in the transmitter. The message signal $m(t)$, which is typically 20dB to 30dB weaker than $y(t)$, is added into the chaotic mask signal giving the transmitted signal $y_t(t)$. Since the chaotic signal $y(t)$ is very complex and $m(t)$ is much smaller than $y(t)$, one would generally expect that the message signal $m(t)$ cannot be separated from $y_t(t)$ without knowing the exact $y(t)$. Given $m(t)$ is weak enough, the synchronization between the transmitter and the receiver can be maintained if the latter is sufficiently robust. The main drawbacks of this scheme are that it is very sensitive to channel noise and parameter mismatch between the chaotic systems in the transmitter and the receiver. Furthermore, this scheme has a very low degree of security as demonstrated in [6].

The second generation of chaotic communication schemes used two different ways to modulate message signals into chaotic carriers. The first method is called chaotic parameter modulation whereby, as its name implies, used the message to modulate system's parameters as shown in Figure 3.

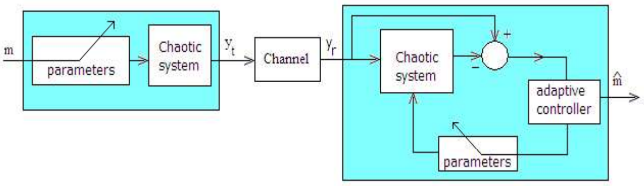

Figure 3. Parameter modulation

Here, the message, $m(t)$, is used to modulate some sensitive parameters of the chaotic system in the transmitter such that its trajectories keep changing in different chaotic attractors. Since the bifurcation space of a chaotic system is very complex, it is very difficult to figure out the way by which the parameters change even through the intruder might possess some partial knowledge of the structure of the chaotic system in the transmitter. At the receiver end, an adaptive controller is used to adaptively tune the parameters of the chaotic system such that the synchronization error converges to zero. Since the chaotic system keeps changing its attractors, the waveform of the transmitted signal is much more complex than a normal chaotic signal with one fixed attractor.

The second method proposed in the second generation is the inclusion technique and sometimes also referred to as the chaotic non-autonomous modulation, depicted in Figure 4.

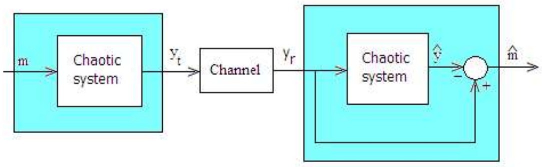

Figure 4. Inclusion method

Here the message is embedded in one of the states of the system rather than in the parameters. So doing, the message signal perturbs the system's chaotic attractor directly in the phase space. Unlike in chaotic parameter modulation where the transmitter is switched among different trajectories in various chaotic attractors, the transmitter in chaotic inclusion is switched among different trajectories of the same chaotic attractor. Theoretically, chaotic inclusion method is an error-free scheme. As a result, the second generation improved the degree of security to some degree but was still found unsatisfactory (see eg. [9]). In addition, there are some further inconveniences associated to chaotic inclusion such as the left invertibility constraint, which tends to be computationally expensive and difficult to design. One can also argue that the first and second generation were developed as a field of their own, that is without taking into account standard communication protocols or encryption procedures.

In contrast, the third generation of chaotic communication schemes uses a combination of the classical cryptographic techniques and chaotic synchronization in order to enhance the degree of security. That is borrowing concepts from standard cryptography but applied to the chaotic communication context. This type of scheme is referred to as a chaotic cryptosystem as depicted in Figure 5. So far, because of this combination, this generation has the highest security than all the existing chaotic secure communication systems.

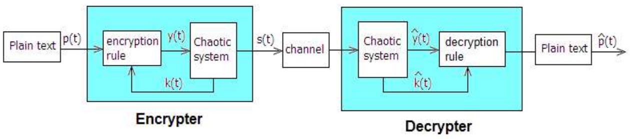

Figure 5. Chaotic cryptosystem

In the chaotic cryptosystem the plain text signal $p(t)$ is encrypted by a encryption rule with a key signal, $k(t)$, which is generated by the chaotic system in the transmitter. The scrambled signal is used to drive the chaotic system such that the chaotic dynamics are continuously modified in a very complex way. Then another state variable of the chaotic system in the transmitter is transmitted to through public channel which can be accessed by the intruder. Since the intruder cannot get access to the chaotic hardware key, it is very difficult to find $p(t)$ out from $s(t)$. At the receiver, the received signal $r(t) = s(t) + n(t)$, where $n(t)$ is the channel noise, is used to synchronize both chaotic systems in transmitter and receiver. After the chaotic synchronization has been achieved, the signal $k(t)$ and $y(t)$ can be recovered at the receiver with some noise as denoted by $\hat{k}(t)$ and $\hat{y}(t)$. By feeding $\hat{k}(t)$ and $\hat{y}(t)$ into the decryption rule, the plain text signal can be recovered with some noise as $\hat{p}(t)$.

Since the publication of several chaotic cryptanalysis results in low-dimensional chaos-based secure communication systems (see eg. [6]), there were concerns that such communication schemes may not be secure enough. To overcome this objection, one approach is to exploit hyperchaos-based secure communication systems, but such systems may introduce more difficulties to synchronization as the dynamics are far more complex. Note that a hyperchaotic system has at least two positive Lyapunov exponents.

The fourth generation of chaotic cryptosystems uses impulsive synchronization to decipher a message. The scheme is similar to that of the chaotic cryptosystem except that the driven system is described by an impulsive differential equation. It is also important to note that the chaotic system at the receiver end is sometimes replaced with a control theory observer in order to improve the synchronization error.

The question is, therefore, what is structure of the fifth generation of chaotic cryptosystem and the challenges related to designing such cryptosystems. In this paper, we shall discuss the shape that the fifth generation of chaotic cryptosystems will take and explain the difficulties in designing and implementing such cryptosystems.

II. Some preliminaries in traditional communication systems

To make this paper self-contained and to clarify the subsequent discussions, we shall recall the main ideas behind traditional communication systems; namely the modulation techniques employed for message transmission. Note that the main aim of traditional communication engineering was to transmit information between two distant points. As such, security was not considered. This need came afterwards once effective communication was established, which explains its implementation in upper communication layers. In the chaotic communication context, one of the main claims is the possibility of implementing security directly in the physical layer.

Traditional analog communication systems indeed employ four main methods of modulation technique: modulation by multiplication (MM), amplitude modulation (AM), frequency modulation (FM) and phase modulation (PM).

In what follows, we shall denote by $m(t)$ the message to be transmitted and by $c(t) = A_c \cos(2\pi f_c t)$ the carrier signal. We shall also assume that the message $m(t)$ is sinusoidal; that is, $m(t) = A_m \cos(2\pi f_m t)$ or $m(t) = A_m \sin(2\pi f_m t)$ with the frequency f_m being very low when compared to $2f_c$.

A. Modulation by multiplication

The modulation by multiplication, as its name implies, consist in the multiplication of the message signal with the carrier signal leading to a transmitted signal of the form:

$$\begin{aligned} y(t) &= km(t)A_c \cos(2\pi f_c t) \\ &= m_0 A_c \cos(2\pi f_m t)\cos(2\pi f_c t) \end{aligned} \tag{1}$$

where $m_0 = kA_m$ is the modulation index. Then,

$$\begin{aligned} y(t) &= m_0 A_c \cos(2\pi f_m t)\cos(2\pi f_c t) \\ &= \frac{m_0 A_c}{2}\left(\cos(2\pi\left(f_c + f_m\right)t) + \cos(2\pi\left(f_c - f_m\right)t)\right) \end{aligned}$$

To recover the message the transmitted signal can either be multiplied by itself or by a local carrier. Then, by low-pass filtering the original message can be recovered due to the fact that $f_m \ll 2f_c$.

B. AM Modulation

The main shortcoming of the modulation by multiplication is that it requires the overall reconstitution of the carrier at the receiver side. To overcome this, the carrier signal is added to the transmitted signal; that is

$$\begin{aligned} y(t) &= A_c\left(\cos(2\pi f_c t) + m_0 \cos(2\pi f_m t)\cos(2\pi f_c t)\right) \\ &= A_c \cos(2\pi f_c t)\left[1 + m_0 \cos(2\pi f_m t)\right] \end{aligned} \tag{2}$$

The message is recovered here by using a diode demodulator circuit.

C. Phase Modulation and Frequency modulation

Here the transmitted signal is of the form

$$y(t) = A_c \cos(2\pi f_c t + \varphi(t))$$

where the phase $\varphi(t)$ is directly proportional to the message; that is

$$\varphi(t) = km(t)$$

or

$$\frac{d\varphi(t)}{dt} = km(t)$$

In other words, we will obtain a transmitted message

$$y(t) = A_c \cos(2\pi f_c t + m_0 \sin(2\pi f_m t)) \tag{3}$$

The message recovery is done via a phase lock loop circuit.

III. Challenges in designing the fifth generation of cryptosystems

The fifth cryptosystem generation is more likely to address the issue of speed of transmission, cyber security and ease of implementation without a complete overhaul of existing infrastructure. With regards to speed of transmission, wireless transmission and chaos-based communication via wireless and, for instance, visible light communication, is likely to be a hot topic to address. The threat posed by cyber attacks has recently resurfaced based on various recent events. One way to address this problem is adding security at every layer of the communication system. Some preliminary works on that topic has been done in [12] whereby a chaotic encryption is made right at the physical layer using established IEEE standards.

The issue of ease of implementation without a complete overhaul of existing infrastructure is crucial. When one assess the applicability of chaotic communication after two and half decades of research work on the topic, one can realise that such technology has not gained much popularity in the industrial context. Chaotic communication is seen as a new approach with a complete new paradigm that requires engineers with high mathematical knowledge to implement them. In addition, it also requires a complete overhaul of the existing communication system in order to secure its implementation. It would therefore be recommendable to find a way to chaoticize the existing (FM/AM) communication systems rather than implementing a complete new transmission system. By doing so, chaotic communications can complement existing communication engineering technology instead of aiming its complete replacement.

One idea is to decompose a chaotic system into a harmonic oscillator together with a nonlinear feedback (see eg. [11]). Then, standard AM/FM modulation can still be applied to the system. The nonlinear feedback serves both as a key and a method to render the transmitted signal chaotic as shown in Figure 6. This approach can potentially bridge both disciplines.

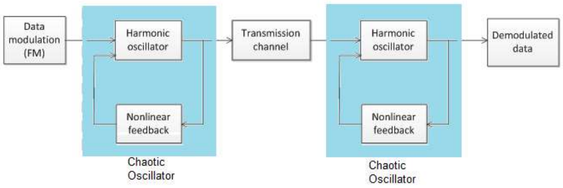

Figure 6. Chaotic modulation

Another method using the same line of reasoning would be to render the modulation index of existing modulation by multiplication (MM) and FM/AM based communication system to chaotic. In what follows, this technique is explained for the MM. Figure 7 depicts the chaotic multiplicative modulation scheme

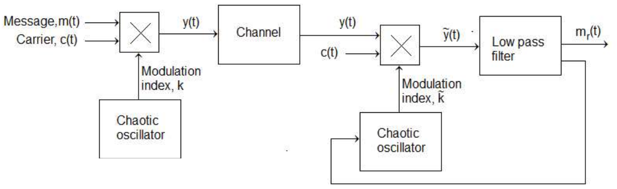

Figure 7. Chaotic multiplicative modulation

In this figure, $y(t)$ is the transmitted signal obtained by the multiplication of the message, $m(t)$, with the carrier signal, $c(t)$, and the modulation index, k, as described by equation 1 in the previous section. At the receiver end, to recover the message, the transmitted signal is multiplied by a local carrier. Then, the original message is recovered by using a low pass filter. For simulation purposes, we have chosen a sinusoidal message whose frequency is several times lower than the carrier frequency. The chaotic oscillator implemented is the Duffing model given by:

$$\ddot{x} + \delta\dot{x} + \alpha x + \beta x^3 = \gamma \cos(\omega t) \tag{4}$$

where $\alpha = 1$, $\beta = 1$,$\delta = 0.02$,$\gamma = 2$ and $\omega = 0.5$ to provide chaotic dynamics.

Figure 8 depicts the original message, $m(t)$ and the recovered message $m_r(t)$. It can be seen that the message is relatively well recovered after some time delay.

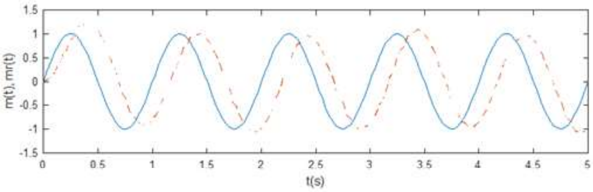

Figure 8 Original m(t) and recovered message mr(t) (dotted lines)

The above methods can be applied for all the aforementioned standard communication schemes; that is, AM, FM and PM.

The fifth generation of chaotic communication system should also address the issue of message recovery or demodulation, which remains the bottleneck for such technology. In this respect, much research has to be carried out on the problem of left inversion for several classes of nonlinear systems. This because is because demodulation is mainly a left inversion problem whereby one has to deduce the input (message) based on the measured output (received signal). Some works addressing this issue can be found in [14].

Finally, to test the security of the proposed systems coherent cryptanalytic methods (i.e., attacks) have to be derived.

IV. Concluding remarks

It is important to realise that the complexity of chaos does not necessarily mean that a chaos-based cryptosystem is secure. A proper way to evaluate the security of a cryptosystem is to evaluate all possible and known cryptanalytic methods for the target cryptosystem. A comprehensive survey of the employed methods of attacks are shown in [13]. The most common ones include parameter estimation, return maps analysis, direct extraction of plaintext and power-spectral analysis. These techniques have been used to demonstrate that none of the above aforementioned methods are secure. As a result, new countermeasures against known attacks are being developed. These include using more complex chaotic systems, such as hyperchaoticity, and more complicated synchronization modes, such as impulsive synchronisation as mentioned previously. In addition to these, combining heterogeneous chaos-based cryptosystems whereby a combination different types of chaos-based cryptosystems is employed with the hope that the security of the resulting system may be higher than the security of each constituent. Unfortunately, this simple combination has been proved to be ineffective. So, more complicated approaches of combination should be further investigated. As most traditional chaos-based secure communication systems and many new-generation ones are known to be insecure, novel ideas need to be created to improve security. One possible way would be to combine the ideas and the technology from traditional communications together with those developed in chaotic communication in order to solidify the latter. Chaotic communication should therefore complement existing digital communication. After all, the theory of traditional communication system is far more richer than that of chaos-based communication.

In this survey we have briefly reviewed the different generations of chaotic communications since their emergence during the nineties. We have shown that during the early days chaos communications where developed as a field of their own, built upon chaos synchronization phenomena and far away from standard communication practices. Later generations took the engineering communication framework progressively into account, especially with regards to cryptographic techniques. Nonetheless, much work needs to be done to fully bridge harmonic data transmission with chaotic communication. If chaos communication is to make a real impact to standard communication engineering, it needs to be compatible existing technology with its modulation and demodulation methods. As such, we have presented two approaches that go in this direction to aid the development of the fifth generation.

References

[1] E. Ott, C. Grebogi, and J.A. Yorke, "Controlling chaos". Physical Review Letters, 64(11), 1196-1199, 1990.

[2] C.W. Wu, T. Yang, and L.O. Chua, "On adaptive synchronization and control of nonlinear dynamical systems". Int. J. of Bifurcation and Chaos, 6(3), 455-471, 1996.

[3] Tao yang, "A survey of chaotic secure communication systems", International Journal of Computational Cognition, Vol. 2, no. 2, pp. 81–130, 2004.

[4] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett., 64, pp. 821-824, 1990.

[5] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," Phy. Rev. Lett., 71, pp. 65-68, 1993.

[6] K.M. Short, Steps toward unmasking secure communications. Int. J. of Bifurcations and Chaos, 4(4), 959-977, 1994.

[7] T. Yang and L. O. Chua, "Secure communication via chaotic parameter modulation," IEEE Trans. on Circ. Sys., I, 43, pp. 817-819, 1996.

[8] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," Int. J. of Bifur. Chaos, 3, pp. 1619- 1627, 1994.

[9] T. Yang and L.B. Yang and C.M. Yang, “Breaking chaotic secure communication using a spectrogram”, Physics Letters A, Vol.247, No.1-2:105-111, OCT 5, 1998.

[10] B. Schneier, Applied Cryptography – Protocols, algorithms, and souce code in C 2nd ed. New York: John Wiley & Sons, Inc., 1996.

[11] P. Canyelles-Pericas, X. Dai, R. Binns and K. Busawon, "Decomposing chaos into a harmonic oscillator with nonlinear feedback using pole placement methods", IEEE Conference in Decision and Control, Melbourne 2017.

[12] T. T. Son, H. Le-Minh, N. Aslam, P. Canyelles-Pericas, K. Busawon, D. Q. Hien, Chaos-based Physical Layer Security for IEEE 802.15.7 Visible Light Communication, submitted to Int. J. of Birfucation and Chaos, 2018.

[13] G. Alvarez and S. Li, “Some basic cryptographic requirements forchaos-based cryptosystems,” Int. J. Bifurcation and Chaos, vol. 16, no. 8, pp. 2129–2151, 2006.

[14] D Boutat, JP Barbot and M Darouach, "On the inversion of a class of nonlinear systems", Systems & Control Letters, 2015.