A Robust Implementation of a Chaotic Cryptosystem for Streaming Communications in Wireless Sensor Networks

Pilar Mareca and Borja Bordel(✉)

Universidad Politécnica de Madrid, Madrid, Spain
mpmareca@fis.upm.es, bbordel@dit.upm.es

Abstract. Wireless sensor networks consist of tiny sensor nodes, which act as both data generators and network relays. These sensor nodes present limited processing capabilities, so hardware support is required for many tasks. Security, a key issue in sensor networks, is one of those tasks. However, current security solutions are always supported by complex software algorithms. Therefore, in this paper we propose a chaotic cryptosystem based on Chua's circuit, especially designed to encrypt streaming communications among sensor nodes. The proposed solution presents a robust design, which enables its implementation using hardware technologies. Moreover, an experimental validation is proposed proving that the maximum encryption error never goes up 12%.

Keywords: Cryptography · Chaos · Chaotic masking · Chua's circuit · Wireless sensor networks · Cyber security

1 Introduction

Wireless sensor networks (WSN) consist of spatially distributed autonomous tiny sensor nodes to monitor and recording physical or environmental conditions, which act as both data generators and network relays [1]. In general, deployments of WSN may present very different characteristics relative to each other. Furthermore, many times sensor nodes making up a unique WSN are a heterogeneous collection of devices with very different functionalities and capabilities. However, despite this fact, various aspects are common to every sensor node or WSN [2]: self-configurable, delay-tolerant, decentralized, etc. Among all them, one of the most important aspects is their reduced sized and its limited processing (and communication) capabilities [3]. As a consequence, traditional algorithms or network solutions are not directly applicable to WSN, as telecommunication networks (such as Internet or Frame Relay) incorporate additional infrastructures (such as the power supply) and devices with high capacities which cannot be considered in WSN.

One of the disciplines more affected by these limitations is security [4]. Firewalls, secure routing protocols or encryption technologies demand too many resources to be applied to WSN. As a solution, hardware-supported techniques are implemented [5]. Nevertheless, most existing proposals are focused on message transmission. There exist,

Á. Rocha et al. (eds.), *Recent Advances in Information Systems and Technologies*,
Advances in Intelligent Systems and Computing 570, DOI 10.1007/978-3-319-56538-5_10

however, applications where WSN must establish streaming communications among its nodes (such as border control or monitoring vital signals) which also require secure transmissions.

Therefore, the objective of this paper is to describe a hardware-based cryptosystem for streaming communications in WSN. The proposed system employs chaotic cryptography (specifically chaotic masking) in order to cipher the information signals before being transmitted through the wireless communications interface. The proposed system, moreover, presents a reduced size and a very low power consumption as it is based on Chua's circuit. Loading effects typical of this circuit are removed by means of a robust implementation of the electronic circuit.

The rest of the paper is organized as follows: Sect. 2 describes the state of the art on security solutions for WSN and chaotic cryptosystems; Sect. 3 includes the mathematical formalization of the proposed solution and its implementation as an electronic circuit; Sect. 4 presents an experimental validation in order to test the performance of the proposed solution; Sect. 5 contains the experimental results and Sect. 6 concludes the paper.

2 State of the Art

Security is one of the key problems in WSN [4]. Most works on this topic are focused on the development of secure routing protocols trying to avoid cyberattacks such as the sinkhole attack or the Sybil attack [6]. Works on generic security protocol (in order to support, for example, authentication) [7] and surveys about security issues and cyberattacks in WSN may also be found [8]. However, works on information encryption in WSN are quite common, and only some works about hardware-support might be found [5].

The main cause of this lack of works if that applying any encryption scheme requires extra bits, extra memory, extra battery power, etc. so encryption could increase delay, jitter and packet loss in WSN [9] (especially if streaming communications re considered). Then, novel technologies should be applied to WSN in order to, for example, guarantee a secure access to the physical layer (among other possibilities). One of these technologies may be chaotic cryptography.

Very complex schemes of chaotic cryptography have been defined [10, 11]. Discrete dynamics have been employed as pseudo-aleatory code [12], unidimensional maps have been integrated into spread spectrum techniques [13] and other solutions based on external keys have been described [14]. Additionally, digital and analog systems have been described [15]. However, all these proposals are based on complicated software algorithms. Thus, for WSN, most simple hardware-supported solutions are required. In this sense, Cuomo and Oppenheim [16] propose a couple of synchronized chaotic circuits as cryptosystem (based on Lorenz dynamics), capable of hiding the transmitted information. Moreover, Kokarev [17] has demonstrated the viability of chaotic masking solutions for other dynamics, such as the Chuas's circuit.

All the previously cited proposals, however, are always implemented using numerical programming and simulation environments. Thus, practical deployment problems

(such as the loading effects) are not addressed. Our proposal covers this gap as a robust hardware implementation (valid to be implemented in sensor nodes) is described.

3 A Robust Chaotic Cryptosystem

Various works have demonstrated that cryptographic techniques for protecting the transmitted information in WSN cannot be based on traditional digital schemes (which employ keys and complex algorithms) [9]. Instead, analog hardware-supported techniques are required. Specially, steganography seems to be one of the better alternatives. Steganography aims at hiding the existence of the data flows among the nodes by embedding information into other signals, so transmissions are not perceptible and hence, the medium looks just like usual. In this context, chaotic masking can be a steganography solution for streaming communications in WSN.

3.1 Mathematical Formalization

The basic scenario is showed on Fig. 1. Two sensor nodes are communicating through a wireless interface. Both nodes are provided with a chaotic circuit. Then, may authors [16, 17] have proved that both circuits can get synchronized if one of them (the transmitter) sends one of the generated chaotic signals to the other (the receptor). Thus, the chaotic signal creates a perturbation in the spectrum which may hide the information streaming, so intruders cannot capture the communication (as in steganography solutions). However, as both nodes can get synchronized, the receptor may recover the information using a subtractor.

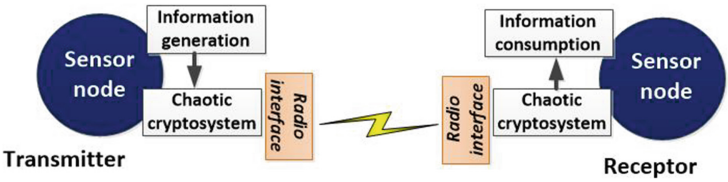

Fig. 1. Basic scenario

Almost every chaotic dynamic may be employed in masking systems. Nevertheless, considering the reduced size of the sensor nodes in the WSN, it is important to select a dynamic with a robust electronic implementation. Among the paradigm systems, Chua's dynamic (1) is which better meets those requirements. Many synchronization schemes for the Chua's dynamic are available.

$$\begin{aligned} \dot{x} &= \alpha\left(y - x - \left(m_1 x + \frac{1}{2}\left(m_0 - m_1\right)\left(|x+1| - |x-1|\right)\right)\right) \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y \end{aligned} \tag{1}$$

Adaptive control techniques [18], passive-active decompositions [19] and other synchronization techniques [20] have been used as base for the chaotic masking systems. However, the most simple, and robust, synchronization scheme was proposed by Pecora and Caroll [21]. Basically it consists of two identical chaotic systems acting one of them as transmitter and the other one as receptor. Then, at least one chaotic signal (called synchronization signal) is extracted from the transmitter and injected in the receptor from which the corresponding equations or subsystem (generating the injected signals) are removed. Specifically (see Fig. 2(a)), in the Chua's circuit the x variable is employed as a synchronization signal. With this selection the conditional Lyapunov's exponents are always negative [22], and the Vaidya's demonstration [23] proves the complete synchronization may occur.

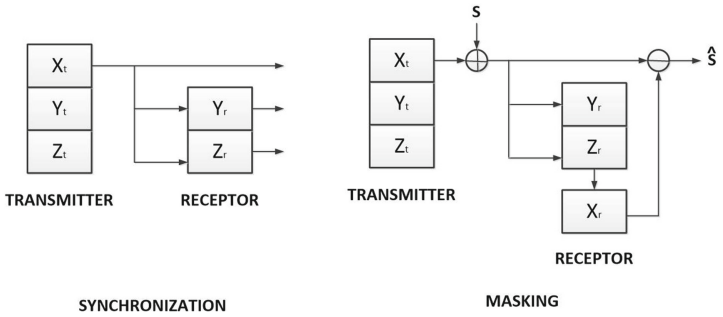

Fig. 2. Proposed schemes for Chua's circuit (a) synchronization (b) masking

In order to create a chaotic masking system using this synchronization scheme (called sometimes unidirectional transmitter-receptor decomposition), it is enough to include the removed equations or subsystems in the receptor, but isolated from the synchronization signal (see Fig. 2(b)). Thus, in the transmitter, the information streaming would be added to the synchronization signal, and the masked information would be recovered by the receptor using a subtractor. Mathematically, the masking scheme can be expressed considering two coupled Chua's dynamics (2).

$$\begin{gathered}\dot{x}_t = \alpha\left(y_t - x_t - f\left(x_t\right)\right) \\ \dot{y}_t = x_t - y_t + z_t \\ \dot{z}_t = -\beta y_t\end{gathered}$$

$$x_s = x_t + s \,(\text{masked information})$$

$$\begin{gathered}\dot{x}_r = \alpha\left(y_r - x_r - f\left(x_r\right)\right) \\ \dot{y}_r = x_s - y_r + z_r \\ \dot{z}_r = -\beta y_r\end{gathered} \tag{2}$$

$$\hat{s} = x_s - x_r \,(\text{recovered information})$$

$$f(x) = m_1 x + \frac{1}{2}(m_0 - m_1)(|x+1| - |x-1|)$$

Using numerical programming it is possible to evaluate the performance of the proposed scheme. In Fig. 3(a) it is showed the spectrum of the synchronization chaotic signal which must hide the information streaming. As can be seen, signals with bandwidths up to 25 kHz cannot be protected with this scheme. However, sensor nodes use to transmit low data rates, so this value is enough. Additionally, Fig. 3(b) and (c) shows a comparison between an analog and a digital information flow and the data flow recovered in the receptor using the proposed scheme. Of course, a radiofrequency chain may translate in frequency the spectrum to be transmitted using wireless communications.

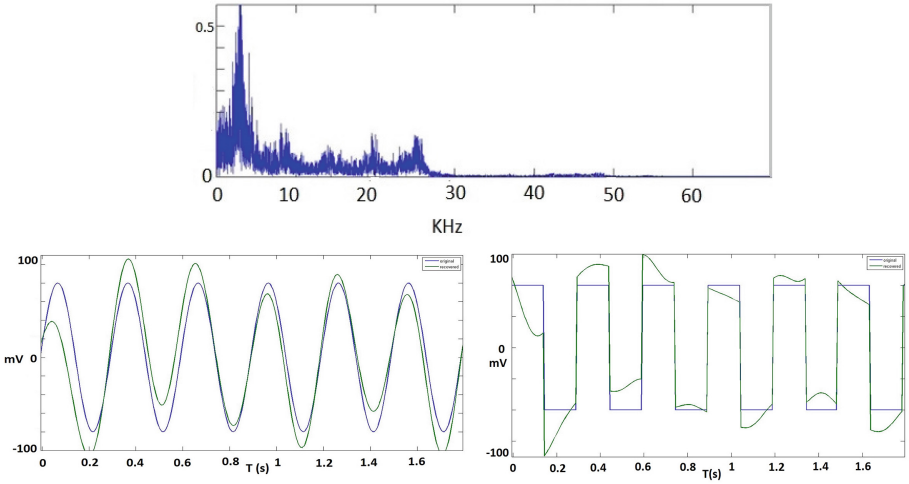

Fig. 3. Results of a numerical implementation of the chaotic masking scheme (a) original information and recovered information (b) spectrum of the masked signal

3.2 Electronic Implementation

In its origin, the Chua's circuit was designed as a real electronic circuit (see Fig. 4(a)), so the Chua's dynamics may be expressed as the evolution laws of this circuit (3). Thus, the proposed masking scheme could be directly implemented using standard electronic techniques (see Fig. 4(b)). The numerical solutions and the synchronization of Chua circuits, have a good behavior. However, electronic implementation of Chua circuit is very sensitive to the accuracy of its components [24]. Therefore, it is necessary to devote special attention to their implementation in simulated and real circuits [25, 26]. In particular, three problems have impeded until now the implementation of an electronic chaotic masking system based on Chua's circuit: the effects of the load, the required inductances and the high-frequency chaotic noise which tends to appear mixed with the recovered information. In this paper we propose a robust solution which addresses these problems.

$$\begin{aligned}\frac{dv_1}{dt} &= \frac{1}{C_1}\left(\frac{1}{R}(v_2 - v_1) - f(v_1)\right)\\ \frac{dv_2}{dt} &= \frac{1}{C_2}\left(i_3 + \frac{1}{R}(v_1 - v_2)\right)\\ \frac{di_3}{dt} &= -\frac{1}{L}v_2\end{aligned} \tag{3}$$

First, in order to avoid the effects of the load, voltage followers are included to extract and inject signals in or from the Chua's circuits. These new elements wean some part of the circuit to the others, so the effects of the load are minimized.

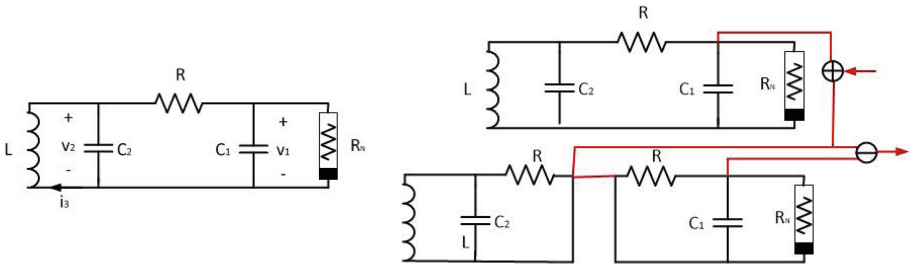

Fig. 4. Electronic implementation of (a) Chua's circuit (b) traditional masking system based on Chua's circuit

Second, the need of including various inductances in the system makes impossible to implement the circuit using high-integration techniques. Particularly, inductances require more space than other components in order to be implemented, so it is recommendable to employ alterative elements such as capacitors. In order to do that, the inductance in the traditional Chua's circuit (see Fig. 4(a)) is substituted by an inmitances converter [25].

Finally, in order to remove the high-frequency chaotic noise, a second-order Sallen-Key low-pass filter is included. Figure 5 shows the resulting robust implementation.

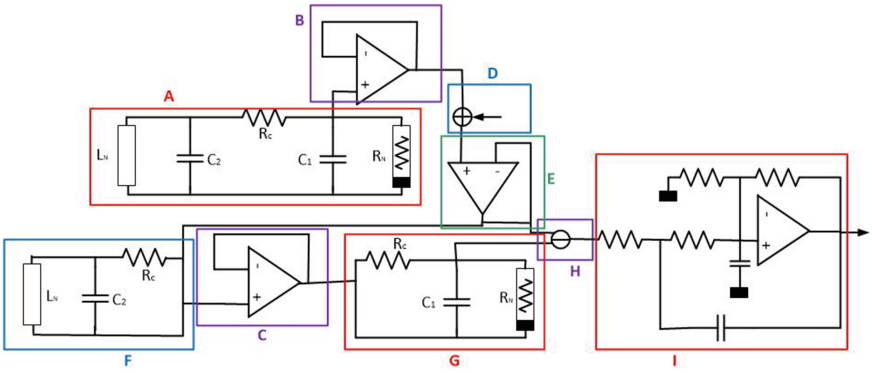

Fig. 5. Robust electronic implementation of the masking system based on Chua's circuit

Various modules are distinguished in the circuit:

- Module A: It is the Chua's circuit acting as transmitter. It generates the chaotic signal to mask the secured information. It includes the inmitances converter.
- Module B and module C: Voltage followers to wean some parts of the circuit and prevent the effect of the load.
- Module D: It is an operational amplifier acting as voltage adder, in order to incorporate the secure information to the chaotic signal
- Module E: It represents the transmission medium
- Module F: It includes the subsystem of the Chua's circuit which receives the synchronization signal. It includes the inmitances converter.
- Module G: It includes the subsystem of the Chua's circuit which it is not part of the Pecora and Caroll's synchronization scheme
- Module H: Two operational amplifiers as subtractor and inverting amplifier in order to recover the secure information.
- Module I: A second-order Sallen-Key low-pass filter in order to remove the chaotic noise.

4 Experimental Validation

In order to validate the proposed cryptosystem, an electronic circuit was implemented using two different techniques. First it was implemented in the PSPICE electronic circuit simulator, and, second, it was implemented using discrete electronic components (see Fig. 6(a)).

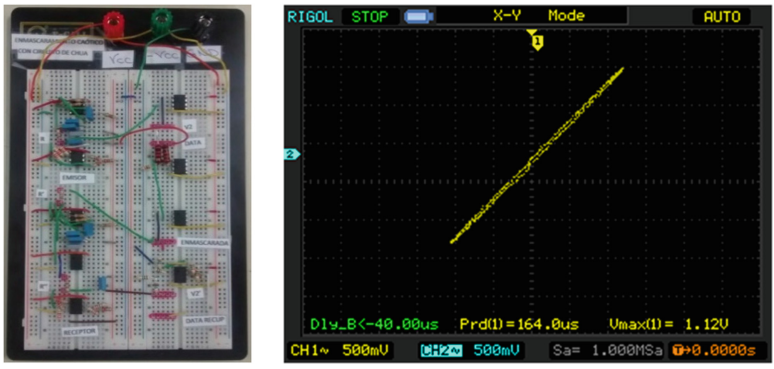

Fig. 6. (a) Electronic implementation of the masking system (b) synchronization curve

Nevertheless, chaotic cryptosystems are difficult to implement using generic commercial components, as they require very precise elements. Particularly, some works have proved that electronic components with tolerance below 3% are required in order to generate good-quality circuits. Thus, although early promising results were obtained using the electronic implementation (see Fig. 6(b)), in this first work we are focusing on a validation based on circuit simulation.

Considering an electronic circuit simulation of the proposed system, two different types of secure information were employed: a sinusoidal signal and a TTL signal. Detailed information is included on Table 1. Moreover, ten different values for the control parameter (in this case we employed the resistor R_c as control parameter, see Fig. 5) were considered. Thus, in total, twenty different simulations were performed.

Table 1. Simulation details for the experimental validation

Parameter	Sinusoidal signal	TTL signal
Amplitude	75 mV	75 mV
Frequency	2 kHz	2 kHz
Duty cycle	–	50%
Offset	0 V	0 V

Each simulation calculated the first three seconds of operation of the cryptosystem. Then, the medium value of the recovery error is also calculated (4) for each case.

$$[\varepsilon(t)] = \sum_{n=0}^{N_{max}} \frac{1}{N_{max}} |s[n] - \hat{s}[n]| \tag{4}$$

5 Results

Figure 7 shows the comparison between the covered signal and the original secure information in the case of considering $R_c = 1800\Omega$, for both, a TTL signal and a sinusoidal signal.

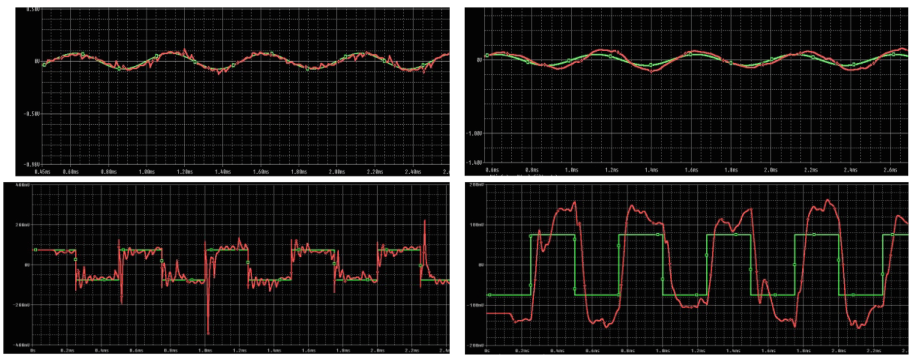

Fig. 7. Results obtained from the proposed solution

As seen above, the recovered signal presents good quality, although a high frequency parasite frequency is mixed with the recovered information. Using the appropriate filter this effect could be removed.

Table 2 shows the results for the medium recovery error. As can be seen, sinusoidal signal may be recovered with better quality than the TTL signal. However, the TTL signal recovery may be highly improved considering specialized digital circuits such as the Smith-trigger (employed to obtain pure TTL signals from TTL-like signals).

Table 2. Recovery error

Experiment	Recovery error (%)
Sinusoidal signal	2.7%
TTL signal	11.5%
Total	7.2%

6 Conclusions and Future Works

In this article we propose a chaotic electronic circuit implemented by means a Chua chaotic system to encrypt streaming communications among sensor nodes in WSN. The first result has been a good chaotic synchronization between the emitter and the receiver systems. We have reduced, also, the loading effects by introducing several voltage followers in the receiver system so obtaining a robust implementation of the electronic circuit. In addition, the circuit is characterized by a reduced size and a very low power consumption. We have implemented the cipher system by a electronic simulation in PSPICE code utilizing sine and TTL information signals. The recovery error was 3% for the sinusoidal signal and 7% for the TTL one. The work is addressed to protecting private communications that is essential in current devices using sensor networks. Future work is addressed to masking speech and sound signals with chaos by means of robust chaotic electronic circuits to protect private communications among sensor nodes.

Acknowledgments. One of us Borja Bordel has received funding from the Ministry of Education through the FPU program (grant number FPU15/03977) and from the Ministry of Economy and Competitiveness through SEMOLA project (TEC2015-68284-R). We are grateful for discussions with professor Vicente Alcober.

References

1. Akyildiz, I.F., Vuran, M.C.: Wireless Sensor Networks, vol. 4. Wiley, Hoboken (2010)
2. Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. Comput. Netw. **52**(12), 2292–2330 (2008)
3. Vieira, M.A.M., Coelho, C.N., da Silva, D.C., da Mata, J.M.: Survey on wireless sensor network devices. In: IEEE Conference Emerging Technologies and Factory Automation, vol. 1, pp. 537–544. IEEE (2003)
4. Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Commun. ACM **47**(6), 53–57 (2004)
5. Portilla, J., Otero, A., de la Torre, E., Riesgo, T., Stecklina, O., Peter, S., Langendörfer, P.: Adaptable security in wireless sensor networks by using reconfigurable ECC hardware coprocessors. Int. J. Distrib. Sensor Netw. **6**(1) (2010). doi:10.1155/2010/740823

6. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Netw. **1**(2), 293–315 (2003)
7. Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E.: SPINS: security protocols for sensor networks. Wireless Netw. **8**(5), 521–534 (2002)
8. Wang, Y., Attebury, G., Ramamurthy, B.: A survey of security issues in wireless sensor networks. IEEE Commun. Surv. Tutorials **8**(2) (2006). http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1087&context=csearticles
9. Pathan, A.S.K., Lee, H.W., Hong, C.S.: Security in wireless sensor networks: issues and challenges. In: 8th International Conference Advanced Communication Technology, vol. 2. IEEE (2006)
10. Vaidya, P.G., Angadi, S.: Decoding chaotic cryptography without access to the superkey. Chaos, Solitons Fractals **17**(2), 379–386 (2003)
11. Wong, K.W., Ho, S.W., Yung, C.K.: A chaotic cryptography scheme for generating short ciphertext. Phys. Lett. A **310**(1), 67–73 (2003)
12. Li, S., Li, Q., Li, W., Mou, X., Cai, Y.: Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 205–221. Springer, Heidelberg (2001). doi:10.1007/3-540-45325-3_19
13. Pareek, N.K., Patidar, V., Sud, K.K.: Cryptography using multiple one-dimensional chaotic maps. Commun. Nonlinear Sci. Numer. Simul. **10**(7), 715–723 (2005)
14. Pareek, N.K., Patidar, V., Sud, K.K.: Discrete chaotic cryptography using external key. Phys. Lett. A **309**(1), 75–82 (2003)
15. Amigó, J.M., Kocarev, L., Szczepanski, J.: Theory and practice of chaotic cryptography. Phys. Lett. A **366**(3), 211–216 (2007)
16. Cuomo, K.M., Oppenheim, A.V., Strogatz, S.H.: Synchronization of Lorenz-based chaotic circuits with applications to communications. IEEE Trans. Circuits Syst. II: Analog Digit. Signal Process. **40**(10), 626–633 (1993)
17. Kocarev, L., Halle, K., Eckert, K., Chua, L.: Experimental demonstration of secure communications via chaotic synchronization. Int. J. Bifurcat. Chaos **2**, 709–713 (1992)
18. Liao, T.L., Tsai, S.H.: Adaptive synchronization of chaotic systems and its application to secure communications. Chaos, Solitons Fractals **11**(9), 1387–1396 (2000)
19. Boccaletti, S., Kurths, J., Osipov, G., Valladares, D.L., Zhou, C.S.: The synchronization of chaotic systems. Phys. Rep. **366**(1), 1–101 (2002)
20. Bai, E.W., Lonngren, K.E.: Synchronization of two Lorenz systems using active control. Chaos, Solitons Fractals **8**(1), 51–58 (1997)
21. Carroll, T.L., Pecora, L.M.: Synchronizing chaotic circuits. IEEE Trans. Circuits Syst. **38**(4), 453–456 (1991)
22. Pecora, L.M., Carroll, T.L.: Synchronization in chaotic systems. Phys. Rev. Lett. **64**(8), 821 (1990)
23. He, R., Vaidya, P.G.: Analysis and synthesis of synchronous periodic and chaotic systems. Phys. Rev. A **46**(12), 7387 (1992)
24. Kyprianidis, I.M., Haralabidis, P., Stouboulos, I.N.: Dynamics and synchronization of a second-order nonlinear and nonautonomous electric circuit. In: 3rd World Multiconference on Circuits, Systems, Communications and Computers, CSCC 1999, pp. 3241–3247 (1999)
25. Alcober, V., Mareca, P., González,Y.G.: Una Optimización en la Sincronización y Enmascaramiento con el circuito de Chua. XXVIII Reunión Bienal de la Real Sociedad Española de Física. Simposio de Dinámica no-lineal. Sevilla, Spain (2001)
26. Murali, K., Lakshamanan, M., Chua, L.O.: Synchronizing Chaos in driven Chua's circuit. Int. J. Bifurcat. Chaos **05**(2), 563 (1995)