SIMPLE MODEL OF SYNCHRONIZED SYSTEM FOR THE CHAOTIC-MASKED COMMUNICATION

Jiří POSPÍŠIL,
Jaromír BRZOBOHATÝ,
Zdeněk KOLKA
Technical University of Brno
Purkyňova 118, 612 00 Brno
Czech Republic
pospisil@urel.fee.vutbr.cz

Abstract

In this paper the simplest form of the compound dynamical system is considered, i.e. the second-order subsystem homogeneously synchronized by the third-order autonomous subsystem where the synchronized block is identical to a part of the synchronizing block. Simplified design formulas are defined for the case of a stable synchronized subsystem and arbitrarily chosen dynamical behaviour of the whole system including any type of chaos. The resultant state equations and the corresponding integrator-based circuit models are shown. Their utilization in chaotic-masked signal communications is suggested.

Keywords

dynamical systems, state models, chaos, synchronization, chaotic-masked communication

1. Intorduction

Third-order piecewise-linear (PWL) dynamical systems belonging to Class C of vector fields in $\Re^3$ [1] represent the simplest autonomous systems which can also exhibit many types of chaotic behaviour. They can be described by the state equations in their general matrix form

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{b}h(\mathbf{w}^\mathsf{T}\mathbf{x}) \tag{1}$$

where $\mathbf{A} \in \Re^{3x3}$, $\mathbf{b} \in \Re^3$, $\mathbf{w} \in \Re^3$ and

$$h(\mathbf{w}^\mathsf{T}\mathbf{x}) = \tfrac{1}{2}\left(\left|\mathbf{w}^\mathsf{T}\mathbf{x}+1\right| - \left|\mathbf{w}^\mathsf{T}\mathbf{x}-1\right|\right) \tag{2}$$

is a continuous and odd-symmetric PWL function [1] partitioning $\Re^3$ by two parallel planes U_1: $\mathbf{w}^\mathsf{T}\mathbf{x} = +1$, U_{-1}: $\mathbf{w}^\mathsf{T}\mathbf{x} = -1$, into inner region $D_0: (-1 \le \mathbf{w}^\mathsf{T}\mathbf{x} \le +1)$ and two symmetrical outer regions D_{+1}: $(+1 \le \mathbf{w}^\mathsf{T}\mathbf{x})$, D_{-1}: $(-1 \le \mathbf{w}^\mathsf{T}\mathbf{x})$, as shown in Fig. 1.

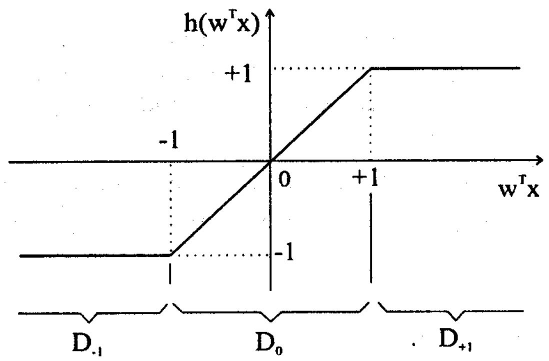

Fig. 1. Simple memoryless PWL feedback function

The dynamical behaviour of such systems is determined by two sets of eigenvalues representing two characteristic polynomials associated with the corresponding regions [1], i.e.

$$D_0: \quad \mathrm{P}(s) = \det(s\mathbf{1}-\mathbf{A}_0) = (s-\mu_1)(s-\mu_2)(s-\mu_3) = \\ = s^3 - p_1 s^2 + p_2 s - p_3 \,, \tag{3}$$

$$D_{+1}, D_{-1}: \mathrm{Q}(s) = \det(s\mathbf{1}-\mathbf{A}) = (s-\nu_1)(s-\nu_2)(s-\nu_3) = \\ = s^3 - q_1 s^2 + q_2 s - q_3 \tag{4}$$

where $\quad \mathbf{A}_0 = \mathbf{A} + \mathbf{b}\mathbf{w}^\mathsf{T}$. $\quad$ (5)

Many canonical state models of these systems having the same dynamical behaviour (including the so called Chua's circuit family) can be derived by using the linear topological conjugacy [2]. The basic case is represented by elementary canonical forms [3] having quite simple relations between their parameters and the corresponding equivalent eigenvalue parameters (p_k, q_k, $k=1,2,3$), i.e. the coefficients of the corresponding two characteristic polynomials in eqns (3), (4).

2. Synchronized Chaotic Systems

State models can also be utilized for systems generating synchronized chaotic signals. The simplest form of the corresponding compound system consists of the second-order subsystem homogeneously synchronized [4] by the third-order synchronizing autonomous subsystem described by general matrix form (1) where state matrix $\mathbf{A}$ and vectors $\mathbf{b}$, $\mathbf{w}$, $\mathbf{x}$ can be expressed as

$$\mathbf{A}=\begin{bmatrix} \multicolumn{2}{c}{\mathbf{A}'} & a_{13} \\ & & a_{23} \\ a_{31} & a_{32} & a_{33}\end{bmatrix}, \tag{6a}$$

and $$\mathbf{b}=\begin{bmatrix}\mathbf{b}'\\ b_3\end{bmatrix},\quad \mathbf{w}=\begin{bmatrix}\mathbf{w}'\\ w_3\end{bmatrix},\quad \mathbf{x}=\begin{bmatrix}\mathbf{x}'\\ x_3\end{bmatrix}. \tag{6b}$$

Submatrix $\mathbf{A}'$ and subvectors $\mathbf{b}'$, $\mathbf{w}'$, $\mathbf{x}'$ correspond to the second-order (x_1,x_2) synchronized subsystem also described by general matrix form

$$\dot{\mathbf{x}}'=\mathbf{A}'\mathbf{x}'+\mathbf{b}'h(\mathbf{w}'^{\mathrm{T}}\mathbf{x}') \tag{7}$$

where $\mathbf{A}'\in\Re^{2\mathrm{x}2}$, $\mathbf{b}'\in\Re^2$, $\mathbf{w}'\in\Re^2$. As follows from eqns (6a), (6b) and in accordance with [4] this subsystem is identical to a part of the synchronizing block (Fig. 2).

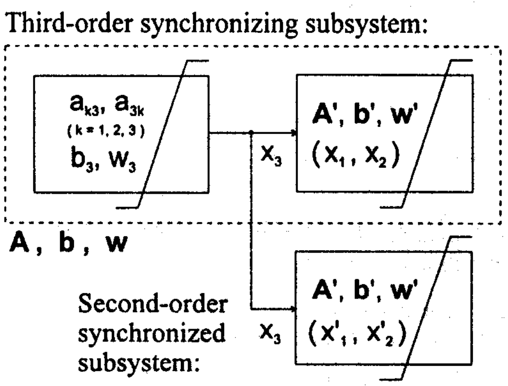

Fig. 2. Symbolic block diagram of the compound (x_1 -x_2) synchronized chaotic system

For a simplicity the synchronized subsystem can be considered in the first elementary canonical form [3]

$$\mathbf{A}'=\begin{bmatrix} q'_1 & -1\\ q'_2 & 0\end{bmatrix}, \tag{8a}$$

$$\mathbf{b}'=\begin{bmatrix} p'_1-q'_1\\ p'_2-q'_2\end{bmatrix},\quad \mathbf{w}'=\begin{bmatrix}1\\0\end{bmatrix},\quad \mathbf{x}'=\begin{bmatrix}x'_1\\ x'_2\end{bmatrix} \tag{8b}$$

where p'_i and q'_i $(i=1,2)$ represent the appropriate equivalent eigenvalue parameters associated with the individual regions (similarly as p_k, q_k, $k=1,2,3$ in eqns (3), (4) for the synchronizing subsystem), i.e.

$$D_0:\quad \mathrm{P}'(s)=\det(s\mathbf{1}-\mathbf{A}'_0)=(s-\mu'_1)(s-\mu'_2)= \\ = s^2-p'_1\,s+p'_2\,, \tag{9}$$

$$D_{+1},D_{-1}:\ \mathrm{Q}'(s)=\det(s\mathbf{1}-\mathbf{A}')=(s-\nu'_1)(s-\nu'_2)= \\ = s^2-q'_1\,s+q'_2 \tag{10}$$

where $$\mathbf{A}'_0=\mathbf{A}'+\mathbf{b}'\mathbf{w}'^{\mathrm{T}}\ . \tag{11}$$

The general design procedure of the compound system then starts from given (p_k, q_k), chosen (p'_i, q'_i) and results in calculating the remaining unknown parameters of the synchronizing subsystem. Expressing the conditions for these seven parameters, six nonlinear algebraic equations are generally obtained [5]. However, their exact solution is rather complicated therefore a few simplifying conditions have been used in further considerations.

3. Simplified State Model

For a simplification the synchronized subsystem can be considered **linear** and **unconditionally stable**, i.e.

$$p'_1=q'_1<0\,,\quad p'_2=q'_2>0\ . \tag{12}$$

Then, in accordance with eqn (8b), $\mathbf{b}'=\mathbf{0}$ and the corresponding nonlinear equations become linear. Parameter b_3 can be chosen quite arbitrarily (e.g. $b_3=1$) and the resultant design formulas have the following simple forms:

$$w_3=p_1-q_1\,,\quad a_{23}=q'_2(p_1-q_1)-(p_3-q_3)\,, \tag{13a,b}$$

$$a_{33}=q_1-q'_1\,,\quad a_{13}=q'_1(p_1-q_1)-(p_2-q_2)\,, \tag{14a,b}$$

$$a_{32}=\frac{a_{13}(q'_2\,a_{33}-q_3)-a_{23}(q'_1\,a_{33}-q_2+q'_2)}{a_{13}(q'_1\,a_{23}-q'_2\,a_{13})-a_{23}^2}\,, \tag{15}$$

$$a_{31}=\frac{(q'_1a_{33}-q_2+q'_2)(q'_1a_{23}-q'_2\,a_{13})-a_{23}(q'_2a_{33}-q_3)}{a_{13}(q'_1\,a_{23}-q'_2\,a_{13})-a_{23}^2} \tag{16}$$

Substituting (8a,b) into (6a,b), (7), and (1) the complete state equations of this simplified model are obtained, i.e. for synchronizing (i) and synchronized (ii) subsystems

(i) $$\dot{x}_1=q'_1\,x_1-x_2+a_{13}x_3\,, \tag{17a}$$

$$\dot{x}_2=q'_2\,x_1+a_{23}x_3\,, \tag{17b}$$

$$\dot{x}_3=a_{31}x_1+a_{32}x_2+a_{33}x_3+h(x_1+w_3x_3)\,, \tag{17c}$$

(ii) $$\dot{x}'_1=q'_1\,x'_1-x'_2+a_{13}x_3\,, \tag{18a}$$

$$\dot{x}'_2=q'_2\,x'_1+a_{23}x_3\ . \tag{18b}$$

In special cases these equations can be further simplified because some of their parameters can tend to zero by a suitable choice of the coefficients p'_i and q'_i, e.g. if $q_1<0$, it is possible to choose $p'_1=q'_1=q_1$, then $a_{33}=0$ and formulas (15), (16) have very simple forms.

The corresponding general integrator-based circuit model is shown in Fig. 3 where the PWL feedback block is included only in the synchronizing subsystem. Figure 4 shows results of numeric simulation for the double-scroll attractor. Perfect synchronization is established almost immediately due to suitable choice of the receiver parameters.

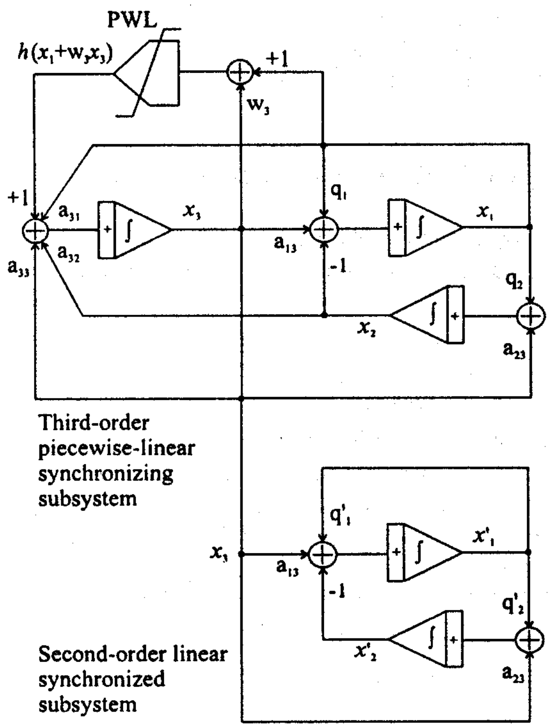

Fig. 3. Integrator based circuit model of the simple synchronized chaotic PWL dynamical system

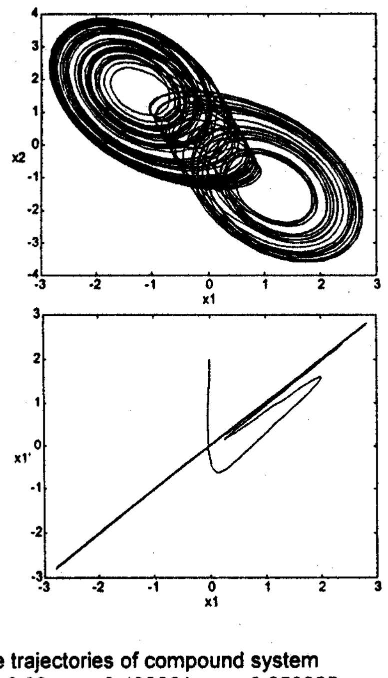

Fig. 4. State trajectories of compound system (p_1 = 0.09, p_2 = 0.432961, p_3 = 0.653325, q_1 = -1.168, q_2 = 0.846341, q_3 = -1.2948, p'_1 = q'_1 = -2, p'_2 = q'_2 = 1)

4. State Model of the Chaotic-Masked Signal Communication

The simplified state model of compound synchronized chaotic system developed can easily be utilized for the chaotic-masked communication. For this purpose the so called inverse approach [6] is convenient. Then the complete state eqns (17) and (18) are extended into the form:

(i) Synchronizing system (transmitter):

$$\dot{x}_1 = q'_1 x_1 - x_2 + a_{13}x_3 \ , \tag{19a}$$

$$\dot{x}_2 = q'_2 x_1 + a_{23}x_3 \ , \tag{19b}$$

$$\dot{x}_3 = a_{31}x_1 + a_{32}x_2 + a_{33}x_3 + h(x_1 + w_3x_3) + u(t) \ , \tag{19c}$$

(ii) Synchronized subsystem (receiver):

$$\dot{x}'_1 = q'_1 x'_1 - x'_2 + a_{13}x_3 \ , \tag{20a}$$

$$\dot{x}'_2 = q'_2 x'_1 + a_{23}x_3 \ , \tag{20b}$$

$$u(t) = -a_{31}x_1 - a_{32}x_2 - a_{33}x_3 - h(x_1 + w_3x_3) + \dot{x}_3 \tag{20c}$$

where $u(t)$ is the information signal transmitted. The corresponding circuit model is shown in Fig. 5.

The synchronization between transmitter (19) and receiver (20) can be achieved only if amplitude of transmitted driving signal is preserved. The signal can be amplified or attenuated during transmission through a real channel. A robust receiver must synchronize independently of amplitude of driving signal. The non-linear functions used to build such receiver must possess a scale-invariant property

$$h(ax) = ah(x) \tag{21a}$$

or

$$h(ax) = h(x) \tag{21b}$$

for $a > 0$. A class of non-linear functions that have property (21a) consist of piece-wise linear functions with the only breakpoint at 0. More suitable functions for modification of above described system belong to the class described by (21b). In [9] was shown that the middle region of function $h(x)$ in (1) can be omitted so that we obtain a new function $h(x) \to \mathrm{sgn}(x)$ fulfilling (21b). The new system has almost the same dynamics as the original one for the double-scroll attractors. The state equations of transmitter are in the form

$$\dot{x}_1 = q'_1 x_1 - x_2 + a_{13}x_3 \ , \tag{22a}$$

$$\dot{x}_2 = q'_2 x_1 + a_{23}x_3 \ , \tag{22b}$$

$$\dot{x}_3 = a_{31}x_1 + a_{32}x_2 + a_{33}x_3 + \mathrm{sgn}(x_1 + w_3x_3)(1 + u(t)) \ , \tag{22c}$$

and the receiver is described by

$$\dot{x}'_1 = q'_1 x'_1 - x'_2 + a_{13}x_3 \ , \qquad (23a)$$

$$\dot{x}'_2 = q'_2 x_1 + a_{23}x_3 \ , \qquad (23b)$$

$$u'(t) = \left(-a_{31}x'_1 - a_{32}x'_2 - a_{33}x_3 + \dot{x}_3\right)\mathrm{sgn}(x_1 + w_3x_3) - 1 \qquad (23c)$$

The information signal $u'(t)$ was recovered in (23c) using $\mathrm{sgn}(x)\,\mathrm{sgn}(x) \cong 1$ which is true for all x except of 0. The conception of using sgn function can be extended to other attractors as described in [9].

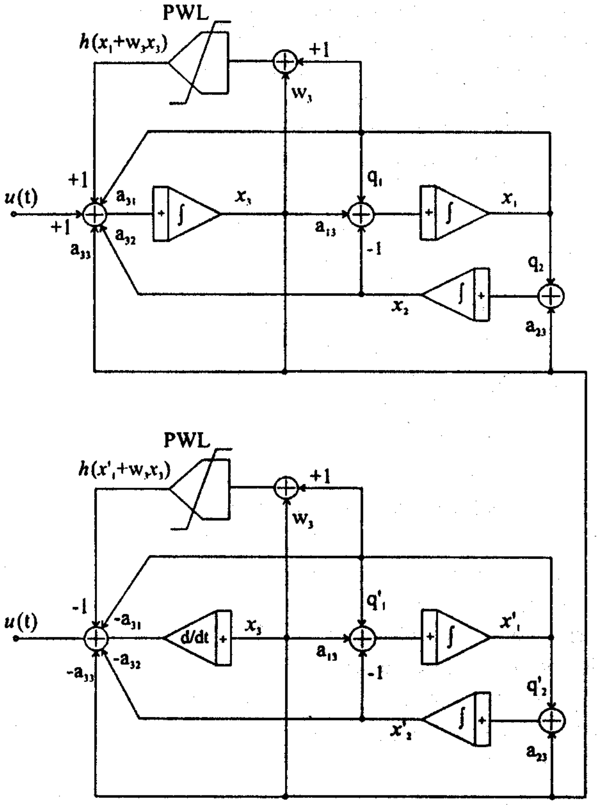

Fig. 5. Circuit model of the chaotic-masked communication system

5. Conclusion

The main advantages of the state model developed are:

(i) Its second-order part is always stable so that it can easily be synchronized,

(ii) Its synchronizing part can produce any type of the third-order chaotic behaviour,

(iii) Very simple design formulas given by the solution of linear equations.

Acknowledgement: This research has partially been supported by the Grant Agency of the Czech Republic - Grant No. 102/98/0130.

References

[1] L.O.Chua, G.N.Lin,"Canonical realization of Chua's circuit family", *IEEE Trans.CAS*, vol. 37, pp. 885-902, 1990.

[2] L.O.Chua, C.W.Wu, "On Linear Topological Conjugacy of Lur'e Systems," *IEEE Trans. CAS*, vol. 43, pp. 158-161, 1996.

[3] J.Pospíšil, J.Brzobohatý, "Elementary Canonical State Models of Chua's Circuit Family," *IEEE Trans.CAS.*, vol. 43, pp. 702-705, August 1996.

[4] L.M.Pecora, T.L.Carroll,"Synchronizing Chaotic Circuits," *IEEE Trans.CAS*, vol. 38, pp. 453-456, 1991.

[5] J.Pospíšil, J.Brzobohatý, "Optimum Design of Simple Synchronized Chaotic System", *Radioengineering 1998* (invited paper - will be published).

[6] U.Feldmann, M.Hasler, W.Schwarz, "Communication by Chaotic Signals: The inverse Approach," *Intern. Journal of Circuit Theory and Applic.*, 1996, Vol. 25, pp. 551-579.

[7] J.Kaderka,"Modelling of Third-Order Elementary Canonic- al State Models using Cellular Neural Networks," In: *Proc. ICECS'96*, Rhodos, vol. 1, pp. 295-298, Oct. 1996.

[8] S.Hanus, "Realization of the Third-Order Chaotic Systems Using Their Elementary Canonical State Models," In: *Proc. "Rádioelektronika'97"*, Bratislava, pp. 44-45, 1997.

[9] R.Brown, "Generalization of the Chua Equations," *IEEE Trans. CAS.*, vol. 40, No. 11, 1993, pp. 878-884.

About authors...

Jiří POSPÍŠIL was born in Brno, Czechoslovakia, in 1939. M.S. and Ph.D. (equivalent degrees): 1963 and 1973, respectively; DrSc. (Doctor of Technical Sciences): 1988, all in el. eng., Technical University of Brno, Czechoslovakia. 1964: Assist. Prof., Military Academy of Brno, Dept. of El. Eng.; 1970-1972: Visit. Prof., Military Technical College, Cairo, Egypt; since 1974: Tech. University of Brno, Dept. of Raioelectronics; 1980: Assoc. Prof.; 1989: Prof.; Research and pedagogical interest: Theory of Circuits, Network Theory, Piecewise-Linear Modelling, Nonlinear Dynamical Systems.

Jaromír BRZOBOHATÝ was born in Brno, Czechoslovakia, in 1935. M.S. and Ph.D. (equivalent degrees): 1960 and 1980, respectively, both in el. eng., Technical University of Brno, Czechoslovakia. 1960-1963: researcher in Metra Blansko; 1963: Assoc. Prof.; 1987: Prof.; Research and pedagogical interest: Theory of Circuits, Microelectronics, Piecewise-Linear Modelling, Nonlinear Dynamical Systems.

Zdeněk KOLKA was born in Brno, Czechoslovakia, in 1969. He received the M.S. (92) and Ph.D. (97) degrees in electrical engineering, both from the Faculty of Electrical Engineering and Computer Sciemce, Technical University of Brno. At present he is an Assistant Professor at the Department of Radioelectronics, Tech. Univ. of Brno. He is interested in PWL modelling, circuit simulation, and nonlinear dynamical systems.