Kybernetika

Sergej Čelikovský

Observer form of the hyperbolic type generalized Lorenz system and its use for chaos synchronization

Kybernetika, Vol. 40 (2004), No. 6, [649]--664

Persistent URL: http://dml.cz/dmlcz/135624

KYBERNETIKA — VOLUME 40 (2004), NUMBER 6, PAGES 649 - 664

OBSERVER FORM OF THE HYPERBOLIC–TYPE GENERALIZED LORENZ SYSTEM AND ITS USE FOR CHAOS SYNCHRONIZATION

SERGEJ ČELIKOVSKÝ

This paper shows that a large class of chaotic systems, introduced in Čelikovský and Chen [7], as the *hyperbolic-type generalized Lorenz system*, can be systematically used to generate synchronized chaotic oscillations. While the generalized Lorenz system unifies the famous Lorenz system and Chen's system [10], the hyperbolic-type generalized Lorenz system is in some way complementary to it. Synchronization of two such systems is made through a scalar coupling signal based on nonlinear observer design using special change of coordinates to the so-called *observer canonical form* of the hyperbolic-type generalized Lorenz system. The properties of the suggested synchronization that make it attractive for the the secure encrypted communication application are discussed in detail. Theoretical results are supported by the computer simulations, showing viability of the suggested approach.

Keywords: nonlinear, chaotic, synchronization, observer

AMS Subject Classification: 93C10, 93D20

1. INTRODUCTION AND PROBLEM STATEMENT

Recently, the synchronization of chaotic systems became an important field of investigation with various applications, namely when using the chaotic systems for secure encryption of messages. Along this line of research, actually the broader problem of synchronization of nonlinear oscillations has already had a rich history and a great variety of applications (see [3] for a concise but informative summary). From theoretical point of view, narrower problem of chaos synchronization is related to the so-called chaos synthesis [4, 30] (or, equivalently, anticontrol of chaos [9]). The purpose of the chaos synthesis is to design chaos as a desired positive phenomenon to be used for various purposes. The ability to produce several identical copies of the desired chaotic behaviour is an essential part of it. Such an effort lead naturally in early 90's to the notion of the synchronization of chaotic systems [23]. Since that time, a numerous number of publications on this topic have appeared, see e. g. [1, 2, 3, 9, 13, 14, 18, 24, 25, 26, 28]. It is important to note here that the ideas from control theory find a natural practice in many of the mentioned papers. This

paper concentrates on the so-called full synchronization problem, i. e. when all state trajectories of the synchronized systems mutually asymptotically converge as time tends to infinity. For an alternative concept of partial synchronization, readers are referred to [24, 26] and the references cited therein.

The full synchronization problem is naturally close to the observer concept in systems theory [22]. Nevertheless, we would like to point out that one may view synchronization as a specific modification of a general observer design problem, since the system output may be freely selected by the designer, which however should have the smallest possible dimension, preferably using only one scalar signal.

The aim of this paper is to study a particular class of chaotic system, the so-called *hyperbolic-type generalized Lorenz system*, introduced and studied in [7], and to design the full synchronization of two identical copies of these systems via a scalar connection. While the generalized Lorenz system unifies the famous Lorenz system and Chen's system [10], the hyperbolic-type generalized Lorenz system is in some way complementary to it. The dependence of the above synchronization on various system parameters will be studied as well. It will be shown that while a small parameter mismatch causes a small synchronization error only, the larger mismatch causes crucial error that cannot be suppressed thanks to special features of the hyperbolic-type Lorenz system. This is important for the implementation purposes for secure encryption of messages as the system parameters may serve as the secure password.

Various secure encryption and decryption schemes may be used to hide the messages using synchronized chaotic oscillators. For an informative survey, including their critical evaluation from the point of view of the classical (i. e. discrete-valued, combinatorial) mathematical cryptography, see [11]. As an illustrative example, let us describe briefly the most simple of them: the so-called *chaotic masking*. This scheme consists in adding a chaotic signal to a secret message on the transmitter side, then transmitting encrypted signal and synchronizing output via public open channel and finally to decrypt the message on the receiver side by subtracting the same chaotic signal obtained via synchronizing the copy of the chaotic system on the receiver side by that synchronizing output. Parameters of the chaotic systems may serve as "password", since thanks to the previously mentioned properties of the synchronization, larger error in parameter(s) knowledge prevents copies of chaotic oscillators from being synchronized.

The paper is organized as follows. Both the generalized Lorenz system and the hyperbolic-type generalized Lorenz system will be introduced in the following section. Section 3 presents main results on synchronization. Throughout the paper, the results are demonstrated by computer simulations. Some conclusions and outlooks for further research are given in the final section.

2. HYPERBOLIC–TYPE GENERALIZED LORENZ SYSTEM

As already mentioned earlier, the hyperbolic-type generalized Lorenz system is a certain dual complement to the so-called generalized Lorenz system. To be more specific, let us introduce the latter class more in detail.

2.1. Generalized Lorenz system

The generalized Lorenz system is the class of systems unifying both classical Lorenz system and the Chen system [10, 19, 29]. It was introduced and studied in detail in [4, 5, 30], demonstarting, in particular, the rich chaotic behavior tunable via single scalar parameter. Moreover, recent result [6] provided the algorithm for synchronized chaos synthesis in two generalized Lorenz systems coupled via scalar connection. To keep the paper self-contained, let us briefly introduce some notations and basic facts.

To begin with, recall the following concept introduced in [30].

Definition 2.1. The nonlinear system of ordinary differential equations in $\mathbb{R}^3$ of the following form is called the *generalized Lorenz system*:

$$\dot{x} = \begin{bmatrix} A & 0 \\ 0 & \lambda_3 \end{bmatrix} x + x_1 \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} x, \tag{1}$$

where $x = [x_1 \;\; x_2 \;\; x_3]^\top$, $\lambda_3 \in \mathbb{R}$, and A is a (2×2) real matrix:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \tag{2}$$

with eigenvalues $\lambda_1, \lambda_2 \in \mathbb{R}$ such that

$$-\lambda_2 > \lambda_1 > -\lambda_3 > 0. \tag{3}$$

Moreover, the generalized Lorenz system is said to be *nontrivial* if it has at least one solution that goes neither to zero nor to infinity nor to a limit cycle.

Motivation for studying this generalized Lorenz system (or GLS) has been thoroughly discussed in [4, 5, 30]. In particular, it is now well understood the inequality condition (3) on the system eigenvalues, in view of Shilnikov's criterion. Since the eigenvalues requirement (3) is the only one, the generalized Lorenz system represents a quite general class of autonomous systems in $\mathbb{R}^3$. The interesting question thereafter is under what parameterization the generalized Lorenz system can be systematically classified in order to simplify its chaos synthesis. The following result has been obtained in [5].

Theorem 2.2. For the nontrivial generalized Lorenz system (1) – (3), there exists a nonsingular linear change of coordinates, $z = Tx$, which takes (1) into the following *generalized Lorenz canonical form*:

$$\dot{z} = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} z + cz \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & \tau & 0 \end{bmatrix} z, \tag{4}$$

where $z = [z_1, z_2, z_3]^\top$, $c = [1, -1, 0]$ and parameter $\tau \in (-1, \infty)$.

The above canonical form is very useful to study bifurcations and tune the chaos in the GLS. As a matter of fact, to tune the chaos, the eigenvalues $\lambda_{1,2,3}$ should only fulfill qualitative inequlity-type condition (3), while only a scalar parameter τ is responsible for subtle tuning of chaotic behaviours. For the detailed picture of GLS properties evolution as the parameter τ changes in its range $[-1, \infty)$ consult [5].

2.2. Hyperbolic-type generalized Lorenz system and its properties

Hyperbolic-type generalized Lorenz system is in a certain sense dual to the generalized Lorenz system. Tentative terminology "hyperbolic-type" reflects the fact that a certain matrix, which has in the case of classical Lorenz system eigenvalues $0, \pm j$, now has eigenvalues $0, \pm 1$. To be more specific, let us give the following

Definition 2.3. The nonlinear system of ordinary differential equations in $\mathbb{R}^3$ of the following form is called the *hyperbolic-type generalized Lorenz system*:

$$\dot{x} = \begin{bmatrix} A & 0 \\ 0 & \lambda_3 \end{bmatrix} x + x_1 \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} x, \tag{5}$$

where $x = [x_1 \;\; x_2 \;\; x_3]^\top$, $\lambda_3 \in \mathbb{R}$, and A is a (2×2) real matrix:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \tag{6}$$

with eigenvalues $\lambda_1, \lambda_2 \in \mathbb{R}$ such that

$$-\lambda_2 > \lambda_1 > -\lambda_3 > 0. \tag{7}$$

Moreover, the hyperbolic-type generalized Lorenz system is said to be nontrivial if it has at least one solution that goes neither to zero nor to infinity nor to a limit cycle.

Analogous comments as for the case of the generalized Lorenz system also apply here. In particular, the corresponding analogue of Theorem 2.2 is important and interesting, which will be derived below.

Despite the seemingly minor difference between the models (5) and (1), it will be seen from simulations and further analysis that the hyperbolic-type generalized Lorenz system presents different type of chaotic behaviour. Complementarity of both models becomes clear when obtaining canonical form for the hyperbolic-type generalized Lorenz system, given by the following theorem.

Theorem 2.4. System (4), with any $\tau \neq -1$, is state equivalent to the following system:

$$\dot{x} = \begin{bmatrix} A & 0 \\ 0 & \lambda_3 \end{bmatrix} x + x_1 \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -\operatorname{sign}(\tau + 1) \\ 0 & 1 & 0 \end{bmatrix} x, \tag{8}$$

where

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

$$\begin{aligned} a_{11} &= [\lambda_1 + (\lambda_2 - \lambda_1)(\tau+1)^{-1}], \\ a_{12} &= -[(\lambda_2 - \lambda_1)(\tau+1)^{-1}], \\ a_{21} &= [\lambda_1 - \lambda_2 + (\lambda_2 - \lambda_1)(\tau+1)^{-1}], \\ a_{22} &= [\lambda_2 - (\lambda_2 - \lambda_1)(\tau+1)^{-1}]. \end{aligned} \tag{9}$$

The corresponding change of coordinates is

$$\begin{aligned} x_1 &= \sqrt{|\tau+1|}\,[z_1 - z_2], \\ x_2 &= \sqrt{|\tau+1|}\,[z_1 + \tau z_2], \\ x_3 &= |\tau+1| z_3. \end{aligned} \tag{10}$$

Proof. Straightforward but laborious computations. □

Remark 2.5. By the previous theorem, the generalized Lorenz canonical form with $\tau > -1$ is equivalent to GLS while the generalized Lorenz canonical form with $\tau < -1$ to the hyperbolic-type GLS. The case $\tau = -1$ is equivalent neither to the generalized Lorenz system nor to the hyperbolic-type generalized Lorenz system. As a matter of fact, it constitutes a boundary between the hyperbolic and non-hyperbolic cases , which have qualitatively different structures in their nonlinear parts, so that they cannot be continuously changed from one to another. The case of $\tau = -1$ may also generate chaotic behavior, which has the similar character as for $\tau \neq -1$, as it will be seen in the next section. To summarize, the *canonical Lorenz form* is a more preferable description as it provides a good unification for many systems that seemingly appear to be very different.

The next proposition underlines even more the exquisite role of the case $\tau = -1$.

Proposition 2.6. Consider the generalized Lorenz canonical form for $\tau = -1$. Then, it is equivalent via the following linear state transformation and constant time scaling

$$x = (z_1 - z_2)\sqrt{\frac{\lambda_1 - \lambda_2}{(-\lambda_1\lambda_2)^{3/2}}} \tag{11}$$

$$y = (\lambda_1 z_1 - \lambda_2 z_2)\sqrt{\frac{\lambda_1 - \lambda_2}{(-\lambda_1\lambda_2)^{5/2}}} \tag{12}$$

$$z = z_3 \frac{\lambda_2 - \lambda_1}{\lambda_1\lambda_2} \tag{13}$$

$$\theta = t\sqrt{-\lambda_1\lambda_2} \tag{14}$$

to the Shimidzu–Morioka model (cf. (3) of [27])

$$\frac{\mathrm{d}x}{\mathrm{d}\theta} = y \tag{15}$$

$$\frac{\mathrm{d}y}{\mathrm{d}\theta} = x(1-z) - \lambda y \tag{16}$$

$$\frac{\mathrm{d}z}{\mathrm{d}\theta} = -\alpha z + x^2 \tag{17}$$

where

$$\lambda = -\frac{\lambda_1 + \lambda_2}{\sqrt{-\lambda_1 \lambda_2}}, \quad \alpha = \frac{\lambda_3}{\sqrt{-\lambda_1 \lambda_2}}. \tag{18}$$

Proof. Straightforward but laborious computations. □

Remark 2.7. It is possible to show that there exist possibly nontrivial hyperbolic type GLS (5) that are not equivalent to the form (4) with some $\tau \in \mathbb{R}$. In the sequel, (4) with $\tau \in \mathbb{R}$ and (7) will be referred to as the generalized Lorenz canonical form (GLCF). In other words, any nontrivial GLS is equivalent to GLCF with some $\tau > -1$ while nontrivial hyperbolic-type GLS is either equivalent to GLCF with some $\tau < -1$, or to a certain variation of the GLCF. The full atlas of all equivalent classes of the nontrivial hyperbolic type GLS is out of scope of this paper.

The GLCf class is illustrated by simulations in Figures 1–8.

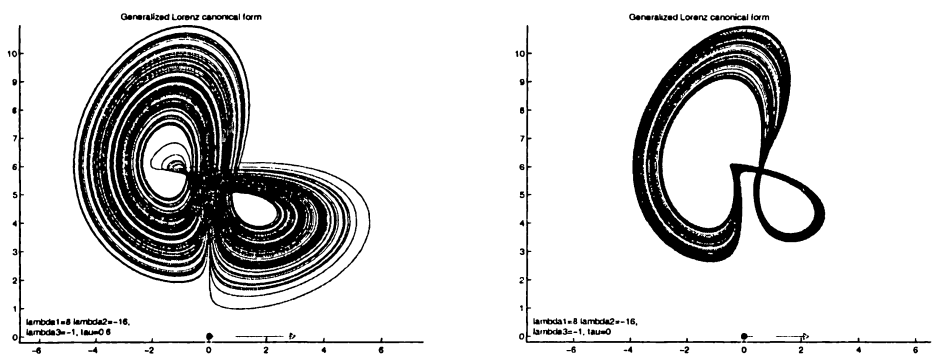

Fig. 1. The generalized Lorenz canonical form for the case of $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$. From the left to right: $\tau = 0.6$ and $\tau = 0$. The first attractor corresponds via linear change of coordinates to the classical Lorenz system. The second attractor presents "boundary" case between Chen's type and classical Lorenz systems.

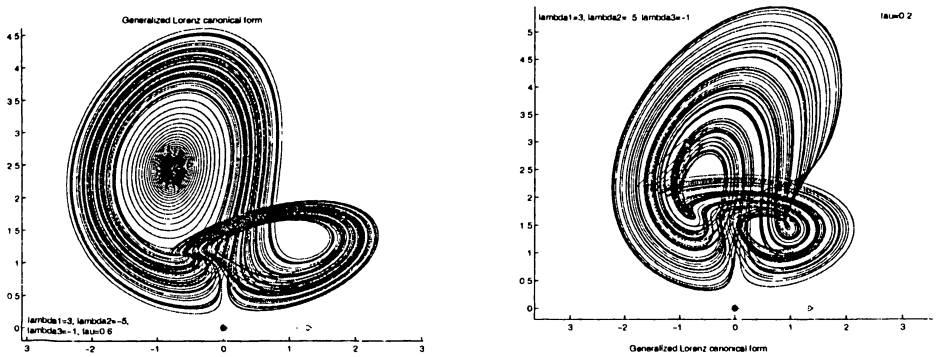

Fig. 2. The generalized Lorenz canonical form for the case of $\lambda_1 = 3$, $\lambda_2 = -5$, $\lambda_3 = -1$. From the left to right: $\tau = 0.6$ and $\tau = 0.2$. Both these cases are equivalent to the generalized Lorenz system and has similar topological structure of their attractors as the classical Lorenz system. Notice that the first one has also point attractors, so that chaotic attractor is not globally attractive.

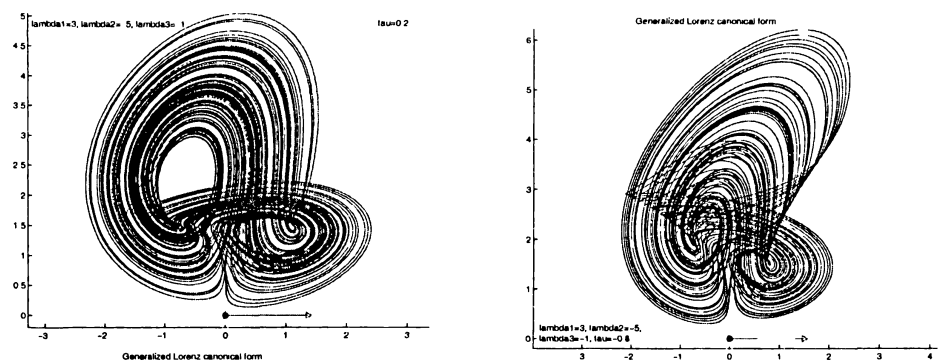

Fig. 3. The generalized Lorenz canonical form for the case of $\lambda_1 = 3$, $\lambda_2 = -5$, $\lambda_3 = -1$. From left to right: $\tau = -0.2$ and $\tau = -0.8$. Both these cases are equivalent to the generalized Lorenz system. The second attractor resembles the one of the Chen's system.

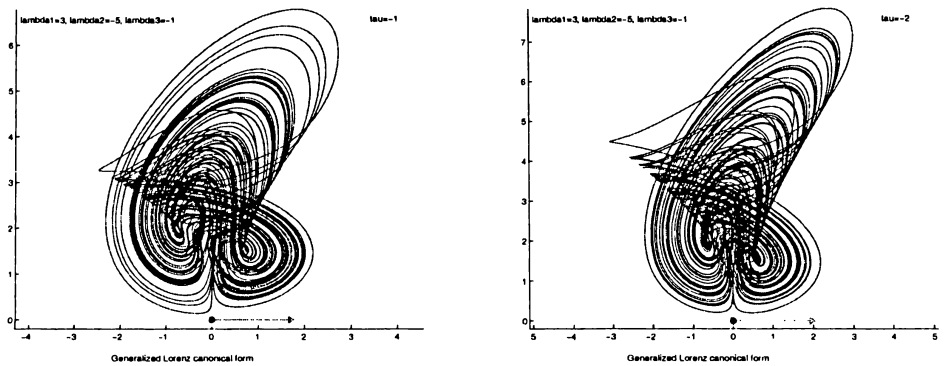

Fig. 4. The generalized Lorenz canonical form for the case of $\lambda_1 = 3$, $\lambda_2 = -5$, $\lambda_3 = -1$. From the left to right: $\tau = -1$ and $\tau = -2$. The case on the left is neither equivalent to the generalized Lorenz system nor to its hyperbolic counterpart. Actually, it is a well-known Shimizu–Morioka model. The case on the right is equivalent to the hyperbolic-type generalized Lorenz system.

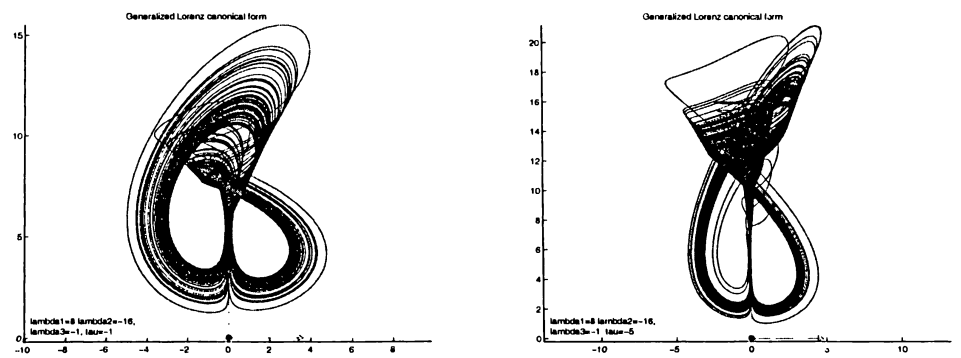

Fig. 5. The generalized Lorenz canonical form for the case of $\lambda_1 = 3$, $\lambda_2 = -5$, $\lambda_3 = -1$. From the left to the right: $\tau = -50$ and $\tau = -100$. This case equivalent to the hyperbolic-type generalized Lorenz system.

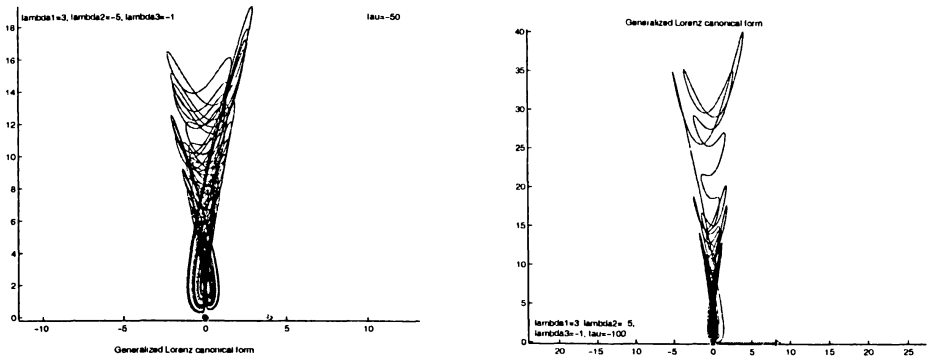

Fig. 6. The generalized Lorenz canonical form for the case of $\lambda_1 = 3$, $\lambda_2 = -5$, $\lambda_3 = -1$. From the left to the right: $\tau = -50$ and $\tau = -100$. This case is equivalent to the hyperbolic-type generalized Lorenz system.

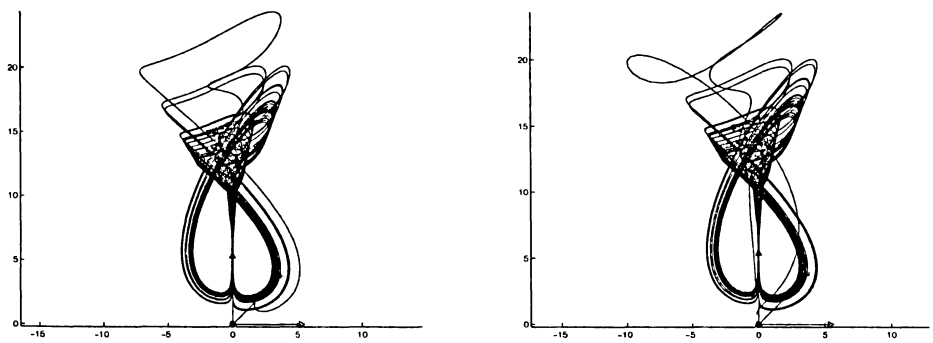

Fig. 7. The synchronization of the hyperbolic-type generalized Lorenz system for the case of $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$ and $\tau = -5$. Transmitter (left) and receiver (right) trajectories in the state space.

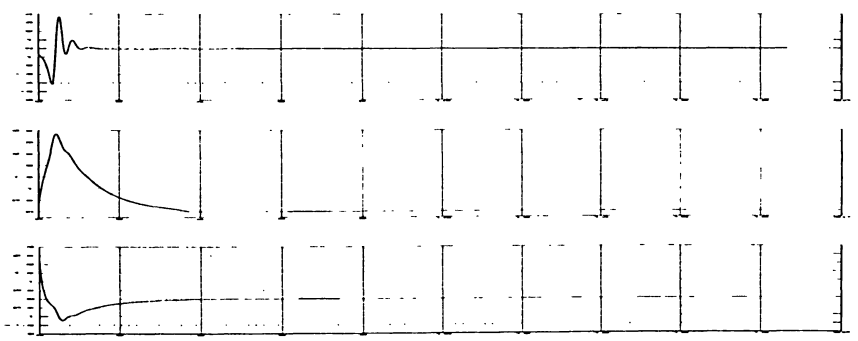

Fig. 8. The synchronization of the hyperbolic-type generalized Lorenz system for the case of $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$ and $\tau = -5$. From up to down: the time evolution of the first, second and third error components of the error dynamics.

3. SYNCHRONIZATION OF HYPERBOLIC-TYPE GENERALIZED LORENZ SYSTEMS

It has been demonstrated in [7] that the hyperbolic-type generalized Lorenz system provides rich possibilities for chaos synthesis as well. The further natural move would therefore be to synchronize copies of the same system from the class of hyperbolic-type systems. Synchronization of chaotic systems is necessary prerequisite of any use of chaotic generators, e. g. for secure encryption. Loosely speaking, synchronization enables to provide copies of the same chaotic oscillations. This is not trivial, due to the sensitive dependence on initial data. As a matter of fact, in practice, even two identical copies of chaotic system, starting at the same initial value, after some time would oscillate in a very different way.

3.1. Observer canonical form of the hyperbolic-type GLS

First, let us derive the so-called observer canonical form of the hyperbolic type generalized Lorenz system. Based on it, the global exponential observer from a suitable defined scalar output will be constructed later on and shown to be, actually, the copy of the system affected by its measured output. In such a way, two copies of the chaotic system will be coupled and synchronized via scalar connection.

Theorem 3.1. Both nontrivial GLS (1) and its canonical form (4) are state equivalent to the following form:

$$\frac{\mathrm{d}\eta}{\mathrm{d}t} = \begin{bmatrix} (\lambda_1+\lambda_2)\eta_1+\eta_2 \\ -\lambda_1\lambda_2\eta_1-(\lambda_1-\lambda_2)\eta_1\eta_3-(1/2)(\tau+1)\eta_1^3 \\ \lambda_3\eta_3+K_1(\tau)\eta_1^2 \end{bmatrix}, \qquad (19)$$

$$K_1(\tau) = \frac{\lambda_3(\tau+1)-2\tau\lambda_1-2\lambda_2}{2(\lambda_1-\lambda_2)},$$

where $\eta = [\eta_1, \eta_2, \eta_3]^\top$, which is referred to as the **observer canonical form**. The corresponding smooth coordinate change and its inverse are

$$\eta_1 = z_1 - z_2, \quad \eta_2 = \lambda_1 z_2 - \lambda_2 z_1, \quad \eta_3 = z_3 - \frac{\tau+1}{2(\lambda_1-\lambda_2)}(z_1-z_2)^2 \qquad (20)$$

$$z_1 = \frac{\lambda_1\eta_1+\eta_2}{\lambda_1-\lambda_2}, \quad z_2 = \frac{\lambda_2\eta_1+\eta_2}{\lambda_1-\lambda_2}, \quad z_3 = \eta_3 + \frac{(\tau+1)\eta_1^2}{2(\lambda_1-\lambda_2)}. \qquad (21)$$

Proof. Differentiating equalities (21) with respect to time and then substituting terms from (19) and (20) give (4) and the conclusion follows immediately.

Notice the key ingredient of the transformation here, i. e. the quadratic term in the last component of the transform. It is designed precisely to remove the cross term $z_2(z_1-z_2)$ and keeping only the term $K_1\eta_1^2 = K_1(z_1-z_2)^2$. The latter depends only on the component $\eta_1 = z_1 - z_2$, which will be crucial for synchronization design later on. □

The above observer canonical form for the hyperbolic-type GLS may seem to be more complicated then the previous one, nevertheless, it enjoys a nice structure where the nonlinearity in the third equation depends on the measured output candidate η_1 only. Therefore, thanks to $\lambda_3 < 0$, the variable η_3 is easily detectable via output injection linearization combined with a linear, Luenberger-type observer. Then, in the second equation the nonlinearities depend only on output candidate η_1 and on the just reconstructed variable η_3, so that one can repeat the previous idea. Such a loosely formulated idea will be presented rigorously in the next subsection.

3.2. Synchronization of the hyperbolic-type generalized Lorenz systems

The observer canonical form for the hyperbolic-type GLS suggests the simple observer, stemming basically form the well-known techniques on linearization via output injection [15, 16, 17]. As a matter of fact, we would need here a more special result and to keep the paper self-contained we prefer to prove our theorem directly. The interested reader may consult [8] and the references within there for the survey of the nonlinear observer techniques.

Our result is presented as the following theorem and treats also the aspect of the possible error in the output measurement, considering the measured quantity η_1^m that may, in general, differ from the value of the actual output η_1.

Theorem 3.2. Consider system (19) with the output η_1 and assume all its trajectories belong to a compact set for all times. Further, consider the following system having input η_1^m and state $\hat{\eta} = (\hat{\eta}_1, \hat{\eta}_2, \hat{\eta}_3)^\top$:

$$\begin{aligned}\frac{\mathrm{d}\hat{\eta}}{\mathrm{d}t} &= \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} \lambda_1 + \lambda_2 - l_1 \\ -\lambda_1\lambda_2 - l_2 \\ 0 \end{bmatrix} \eta_1^m \\ &+ \begin{bmatrix} 0 \\ -(\lambda_1 - \lambda_2)\eta_1^m\hat{\eta}_3 - (1/2)(\tau+1)(\eta_1^m)^3 \\ K_1(\tau)(\eta_1^m)^2 \end{bmatrix}, \end{aligned} \tag{22}$$

where $l_{1,2} < 0$. For all $\varepsilon \geq 0$, assume $|\eta_1(t) - \eta_1^m(t)| \leq \varepsilon$. Then, it holds exponentially in time that

$$\overline{\lim}_{t\to\infty} \|\eta(t) - \hat{\eta}(t)\| \leq C\varepsilon,$$

for a constant $C > 0$. In particular, for $\eta_1^m \equiv \eta_1$ system (22) is a global exponential observer for system (19) with the output η_1.

Proof. Let $e = (e_1, e_2, e_3)^\top = \eta - \hat{\eta}$. Then, subtracting (22) from (19) gives

$$\dot{e} = \begin{bmatrix} & F & & 0 \\ & & & (\lambda_2 - \lambda_1)\eta_1 \\ 0 & 0 & & \lambda_3 \end{bmatrix} e + \psi(\eta)(\eta_1 - \eta_1^m), \quad F = \begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix}, \tag{23}$$

where ψ is a smooth function. Select the gains l_1, l_2 in such a way that the matrix F is Hurwitz. Although the error dynamics (23) is a linear nonautonomous and

nonhomogeneous system depending on a particular observed trajectory[1], its matrix is block triangular with diagonal blocks being constant Hurwitz matrices and all other entries being bounded uniformly in time. Nonhomogeneity $\psi(\eta(t))(\eta_1(t) - \eta_1^m(t))$ is bounded uniformly in time, due to the assumptions of the theorem, by $\overline{C}\varepsilon$, where $\overline{C}$ is a suitable constant. This implies the conclusion in an obvious way. □

In the sequel, we will usually call, in accordance with a major part of the current literature listed in the bibliography, the system (19) as the transmitter while the system (22) as the receiver. Alternatively, the master-slave terminology may be encountered in some of the listed references.

Remark 3.3. Suppose that $\eta_1 \equiv \eta_1^m$ (i.e. $\varepsilon = 0$), in other words, the output candidate η_1 is available for the precise measurement. Then, due to the just formulated theorem, (22) is the global exponential observer from the output η_1. As a matter of fact, one can easily see that the right-hand side of the observer (22) can be represented as a copy of the system (19) (i.e. the system (19) with η replaced by $\hat{\eta}$) plus an additional term depending on $\hat{\eta}$ and η_1 only. The latter one may be interpreted as the scalar synchronizing connection between systems thereby providing synchronization scheme for several exemplars of the hyperbolic-type generalized Lorenz systems.

The following proposition analyzes the influence of mismatching the parameter τ. Here, τ_{sl} may be interpreted as a "false" value of mismatched parameter τ.

Proposition 3.4. Consider system (19) with chaotic behavior. The system (22), with $\eta_1 = \eta_1^m$ and $\tau = \tau_{sl}$, satisfies the following property: For $i = 1, 2, 3$ and for sufficiently small $|\tau - \tau_{sl}|$,

$$\overline{\lim}_{t\to\infty}|\hat{\eta}_i(t) - \eta_i(t)| \leq C_i^{up}(l_1, l_2)|\tau - \tau_{sl}|,$$

where $C_i^{up}(l_1, l_2) > 0$, $i = 1, 2$, are some parameters converging to zero if $l_1 \to -\infty, (l_2/l_1) \to -\infty$, while $C_3^{up}(l_1, l_2) > 0$ does not depend on $l_{1,2}$ at all. Moreover, for all values of $l_{1,2}$, it holds that

$$\frac{\mathrm{d}(\eta_3 - \hat{\eta}_3)}{\mathrm{d}t} = \lambda_3(\eta_3 - \hat{\eta}_3) + K_1(\tau - \tau_{sl})\eta_1^2, \tag{24}$$

where K_1 is given in (19).

Proof. Denoting $e = (e_1, e_2, e_3)^\top = \eta - \hat{\eta}$, we can easily obtain

$$\dot{e} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & (\lambda_2 - \lambda_1)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix} e + \begin{bmatrix} 0 \\ (-\tau + \tau_{sl})\eta_1^3/2 \\ K_1(\tau - \tau_{sl})\eta_1^2 \end{bmatrix},$$

so that (24) follows immediately. The remaining claims of the proposition easily follows from the proof of Proposition 4 of [8]. □

[1]This is the reason why one can not directly apply e.g. the results of [16].

Remark 3.5. A modification of Proposition 3.4 may be obtained in a straightforward way, to include some other system parameters as well. Another variant can also be obtained to take into account a biased output measurement. Resistance against an intruder not knowing τ precisely enough was obtained thanks to a special structure of the used observer, i. e. the third component is detectable but unobservable, which lead the third component of the error to be independent of the gains $l_{1,2}$.

Notice also that for $\eta_1 = 0$, there is a singularity preventing further transforming the observer canonical form (19) into the usual linear observability form where one could use, e. g. high gain robust observers design (see e. g. Proposition 4 of [8] and references within there for details) to cope with lack of password knowledge. In other words, the above singularity makes a reasonable precise knowledge of parameter τ crucial for the succesful synchronization thereby making this parameter an excellent candidate for the secure password.

To be more specific, the "password value" of τ may be discretized using the property that the influence of sufficiently small errors in value of τ can be removed during further signal processing while larger errors prevent from recovering the signal by an intruder. Moreover, the third component of the synchronization error evolves as the chaotic signal η_1 passes through a simple linear filter. This means that wrongly synchronized system creates a signal qualitatively similar to the correct one but no hint for the intruder is provided.

Still, one may immediately understand theoretical difficulties of proving the claim "there is no way how to synchronize the systems without reasonable precise knowledge of τ". Basically. we can just rule out some known schemes. Another scheme, that can be excluded is the adaptation scheme, again thanks to a special structure of the hyperbolic-type GLS. Namely, notice that the error dynamics are in a form where the unknown parameter enters the non-measurable dynamics (24), what prevents usual nonlinear adaptive techniques from being applied.

Summarizing, the discussed synchronization is therefore believed to be fairly safe against the potential intruder trying to cope with lack of knowledge of "password" τ via robust or adaptive techniques.

Numerous MATLAB-SIMULINK based simulations were performed to check the synchronization properties. Most of them use two relatively small gains $l_{1,2} = -1$ while the initial error between the transmitter and the receiver was set large. This is to demonstrate the nice global exponential convergence of the designed synchronization.

After the initial transition period, the synchronization error goes rapidly to zero. By selecting higher gains $l_{1,2}$, one can arbitrarily enhance the convergence rates of the first two components. The convergence of the third component, however, is given by the eigenvalue λ_3 therefore is unchanged. All these facts clearly correspond to the simple form of the error dynamics obtained during the proof of Theorem 3.2. As an illustrative sample, Figures 9 and 10 depict one typical simulation.

Simulations show the behavior of both the transmitter and the receiver in their z-coordinates. Here, the transmitter is the generalized canonical Lorenz system, while the receiver is its copy plus a certain synchronizing part using the scalar signal $z_1 - z_2$ as the only connection to the transmitter. The behavior of the receiver is

computed by solving its equation in the $\hat{\eta}$ coordinates and then mapping it via the corresponding diffeomorphism into $\hat{z}$.

4. CONCLUSIONS AND OUTLOOKS

The important issue of chaos synchronization for the secure communication has been thoroughly discussed in this paper, using the hyperbolic-type generalized Lorenz system family as the platform. The approach taken is based on the nonlinear observer theory, with both theoretical analysis and numerical simulation supports. The possibility of using system's parameters as "passwords" for secure communication has been thoroughly analyzed, both theoretically and numerically. It shows that without precise knowledge of the system parameters, one cannot remove synchronization error even by using a very high-gain observer design. This provides a promising methodology for chaos-synchronization-based secure communication, significantly improving most, if not all, existing schemes of this kind.

Further study of the security aspects of existing synchronization schemes is highly desirable. The heuristic observation made in this respect for the hyperbolic-type generalized Lorenz system studied in this paper is that system should be detectable, but not fully observable, resulting in a certain "fragile" (nonrobust) observers.

On the theoretical level, as a challenging outlook for further research one may consider setting out the proper definition(s) of the security concept using control theoretic terminology. For instance, one may ask the synchronization to be resistant against adaptive and/or robust techniques, giving the appropriate rigorous mathematical definitions and then trying to prove those properties for a particular synchronization scheme.

ACKNOWLEDGEMENT

This work was supported by the Grant Agency of the Czech Republic through the Research Grant No. 102/02/0709.

(Received August 20, 2003.)

REFERENCES

[1] H. N. Agiza and M. T. Yassen: Synchronization of Rössler and Chen chaotic dynamical systems using active control. Phys. Lett. A *278* (2000), 191–197.

[2] J. Alvarez-Ramirez, H. Puebla, and I. Cervantes: Stability of observer-based chaotic communications for a class of Lur'e systems. Internat. J. Bifur. Chaos *7* (2002), 1605–1618.

[3] I. I. Blekman, A. L. Fradkov, H. Nijmeijer, and A. Y. Pogromsky: On self-synchronization and controlled synchronization. Systems Control Lett. *31* (1997), 299–305.

[4] S. Čelikovský and A. Vaněček: Bilinear systems and chaos. Kybernetika *30* (1994), 403–424.

[5] S. Čelikovský and G. Chen: On a generalized Lorenz canonical form of chaotic systems. Internat. J. Bifur. Chaos *12* (2002), 1789–1812.

[6] S. Čelikovský and G. Chen: Synchronization of a class of chaotic systems via a nonlinear observer approach. In: Proc. 41st IEEE Conference on Decision and Control, Las Vegas 2002, pp. 3895–3900.
[7] S. Čelikovský and G. Chen: Hyperbolic-type generalized Lorenz system and its canonical form. In: Proc. 15th Triennial World Congress of IFAC, Barcelona 2002, CD ROM.
[8] S. Čelikovský, J. J. Ruiz-Léon, A. J. Sapiens, and J. A. Torres-Muñoz: Output feedback problems for a class of nonlinear systems. Kybernetika *39* (2003), 389–414.
[9] G. Chen and X. Dong: From Chaos to Order: Methodologies, Perspectives, and Applications. World Scientific, Singapore 1998.
[10] G. Chen and T. Ueta: Yet another chaotic attractor. Internat. J. Bifur. Chaos *9* (1999), 1465–1466.
[11] F. Dachselt and W. Schwartz: Chaos and cryptography. IEEE Trans. Circuits and Systems *48* (2001), 1498–1509.
[12] A. L. Fradkov, H. Nijmeijer, and A. Yu. Pogromsky: Adaptive observer based synhronization. In: Controlling Chaos and Bifurcations in Engineering Systems (G. Chen, ed.), CRC Press, Boca Raton 1999, pp. 417–435.
[13] G. Grassi and S. Mascolo: Synchronization of high-order oscillators by observer design with application to hyperchaos-based cryptography. Internat. J. Circuit Theory Appl. *27* (1999), 543- 553.
[14] M. Itoh and L. O. Chua: Reconstruction and synchronization of hyperchaotic circuits via one state variable. Internat. J. Bifur. Chaos *12* (2002), 2069–2085.
[15] A. J. Krener: Nonlinear stabilizability and detectability. In: Systems and Networks: Mathematical Theory and Applications, Vol. I (U. Helmke, R. Mennicken, and J. Sauer, eds.), Akademie Verlag, Berlin 1994, pp. 231–250.
[16] A. J. Krener and A. Isidori: Linearization by output injection and nonlinear observers. Systems Control Lett. *3* (1983), 47–52.
[17] A. J. Krener and W. Respondek: Nonlinear observers with linearizable error dynamics. SIAM J. Control Optim. *23* (1985), 197–216.
[18] J. Lian and P. Liu: Synchronization with message embedded for generalized Lorenz chaotic circuits and its error analysis. IEEE Trans. Circuits and Systems *47* (2000), 1418–1424.
[19] J. Lü, G. Chen, D. Cheng, and S. Čelikovský: Bridge the gap between the Lorenz system and the Chen system. Internat. J. Bifur. Chaos *12* (2002), 2917–2926.
[20] P. Marino and P. Tomei: Nonlinear Control Design: Geometric, Adaptive and Robust. Prentice–Hall, London 1991.
[21] H. Nijmeijer and A. J. van der Shaft: Nonlinear Dynamical Control Systems. Springer-Verlag, New York 1990.
[22] H. Nijmeijer: A dynamical control view on synchronization. Phys. D *154* (2001), 219–228.
[23] L. Pecora and T. Carrol: Synchronization in chaotic systems. Phys. Rev. Lett. *64* (1990), 821–824.
[24] A. Pogromsky, G. Santoboni, and H. Nijmeijer: Partial Synchronization: from symmetry towards stability. Phys. D *172* (2002), 65–87.
[25] G. Santoboni, A. Y. Pogromsky, and H. Nijmeijer: An observer for phase synchronization of chaos. Phys. Lett. A *291* (2001), 265–273.
[26] G. Santoboni, A. Y. Pogromsky, and H. Nijmeijer: Partial observer and partial synchronization. Internat. J. Bifur. Chaos *13* (2003), 453–458.
[27] A. L. Shilnikov, L. P. Shilnikov, and D. V. Turaev: Normal forms and Lorenz attractors. Internat. J. Bifur. Chaos *3* (1993), 1123–1139.
[28] E. Solak, Ö. Morgül, and U. Ersoy: Observer-based control of a class of chaotic systems. Phys. Lett. A *279* (2001), 47–55.

[29] T. Ueta and G. Chen: Bifurcation analysis of Chen's equation. Internat. J. Bifur. Chaos *10* (2000), 1917–1931.
[30] A. Vaněček and S. Čelikovský: Control Systems: From Linear Analysis to Synthesis of Chaos. Prentice–Hall, London 1996.
[31] X. Wang: Chen's attractor – a new chaotic attractor (in Chinese). Control Theory Appl. *16* (1999), 779.
[32] S. Wiggins: Global Bifurcation and Chaos: Analytical Methods. Springer–Verlag, New York 1988.
[33] G.-Q. Zhong and K.S. Tang: Circuit implementation and synchronization of Chen's attractor. Internat. J. Bifur. Chaos *12* (2002), 1423–1427.

Sergej Čelikovský, Faculty of Electrical Engineering, Czech Technical University in Prague, Technická 2, 166 36 Praha 6. Czech Republic.
e-mail: celikovs@control.felk.cvut.cz