A multiple data secure communication based on synchronization of chaotic systems with zero dynamics

Gang Zheng, Driss Boutat, Latifa Boutat-Baddas, Thierry Floquet, Jean-Pierre Barbot

A Multiple Data Secure Communication Based on Synchronization of Chaotic Systems with Zero Dynamics

G. Zheng, D. Boutat, L. Boutat-Baddas, T. Floquet and J.P. Barbot

***Abstract*— This paper gives a new scheme of data secure communication based on synchronization of chaotic systems with multi inputs multi outputs and zero dynamics. In addition, a sliding mode observer is proposed and a simple example and simulations are given in order to highlight the proposed method.**

I. INTRODUCTION

Since chaotic system is extremely sensitive to initial conditions and parameters variations, its application to secure communication has provoked a great deal of interest, especially after Carroll and Pecora's outstanding work on successfully synchronizing two chaotic systems [8].

Up to now, most chaos-based communication systems are based on chaos synchronization technique. Actually, this synchronization can be studied as an observer design problem, since the work of H. Nijmeijer and I. Mareels in [7].

In secure communication system, we need to estimate not only the state for chaos synchronization but also the input (confidential message), which can be considered as to design an unknown inputs observer with unknown inputs estimation. For the linear systems with unknown inputs and without input estimation, in [4], [5], the necessary and sufficient conditions for the existence of a classical observer are presented. Moreover, an algorithms of full order observers and conditions for their existence are stated in [2]. In the nonlinear case, at our knowledge, one of the first design of unknown inputs observer was given in [11] where authors relaxed the Usual Observability Matching condition. Roughly speaking the UOM condition means that all unknown inputs act on the first derivative of the output and also verify regularity properties. In [3] for the linear case and in [1] for nonlinear case a new observability matching condition are given, which relaxed again the previously mentioned conditions. Moreover, in the last reference the authors give conditions in order to recover the unknown inputs for systems without zero dynamics. This problem can be see as a Left Invertibility Problem [10].

In this paper, we propose to apply the results of [1] taking into account the stability of the zero dynamics into multi data secure communication scheme.

This paper is organized as follows: Notations and problem statement are presented in section 2. In section 3, a new scheme of transmitter based on the stability of zero dynamics is proposed. Moreover, A sliding mode observer design with unknown inputs estimation (receiver) is proposed in section 4. Finally, in order to highlight the well found of the proposed method, an example is given simulated and commented.

II. NOTATIONS AND PROBLEM STATEMENT

A multiple secure communication system can be represented in the following form:

$$\begin{cases} \dot{x} = f(x) + \sum_{i=1}^{m} g_i(x)\, u_i \\ y = [h_1(x), ..., h_p(x)]^T \end{cases} \tag{1}$$

where U is an open set of R^n, $x \in U$ is the state vector and $f : R^n \rightarrow R^n$ is analytic. $y \in R^p$ is the output vector and $u \in R^m$ represents the confidential information to be transmitted. The vector fields $f = [f_1, \ldots, f_n]^T, g_i = [g_{i1}, \ldots, g_{im}]^T$ and $h = [h_1, \ldots, h_p]^T$ are assumed to be sufficiently smooth on U, where $f_i, h_j \in R$ and $g_k \in R^n$, $i \in [1, n]$, $j \in [1, p]$, $k \in [1, m]$,. Without loss of generality, it is assumed that the distribution $span\{g_1, \ldots, g_m\}$ and the codistribution $span\{dh_1, \ldots, dh_p\}$ are nonsingular on U.

The relative degree r of system (1) is defined by $r = \{r_1, ..., r_p\}$, where $r_i = \min\{s$ such that $L_{g_k} L_f^{s-1} h_i \neq 0$ for $k = 1 : m\}$, $i = 1 : p$.

Under the case $r = \sum_{i=1}^{p} r_i = n$, a multiple secure communication system can be established easily. However, this method does not lead to an enough complexity of computation for decryption. Therefore in order to improve the security, the complexity of the scheme can be increased by choosing the outputs y and the input channel vectors $\{g_1, \ldots, g_m\}$ such that $r < n$. In [1], an algorithm to solve the observation problem for nonlinear systems with unknown inputs when $r < n$ has been proposed.

It is assumed that $p \geq m$, and that the system (1) has a relative degree $r = \{r_1, ..., r_p\}$. It should be noted that in this paper we do not consider the case of infinite relative degree. Let us define the following sets that will be used in the sequel:

G. Zheng is with INRIA Rhône-Alpes, 38330 Montbonnot Saint Ismier, France. gang.zheng@inria.fr

D.Boutat is with LVR, ENSI-Bourges, Université d'Orléans, 10, Bd. Lahitolle, 18020 Bourges Cedex, France. driss.boutat@ensi-bourges.fr

L. Boutat-Baddas is with UHP Nancy I, CRAN-UMR 7039-CNRS-INPL-UHP, IUT de Longwy, 54400 Cosnes-et-Romain, France. latifa.boutat-baddas@iut-longwy.uhp-nancy.fr

T. Floquet is with LAGIS UMR CNRS 8146, Ecole Centrale de Lille, BP 48, Cité Scientifique, 59651 Villeneuve-d'Ascq and Project ALIEN, INRIA-Futur, France. thierry.floquet@ec-lille.fr

J.P. Barbot is with Equipe Commande des Systèmes (ECS), ENSEA, 6 Av. du Ponceau, 95014 Cergy Cedex and Project ALIEN, INRIA-Futur, France. barbot@ensea.fr

- $\Omega = \{dh_1, ..., dL_f^{r_1-1}h_1, ..., dh_p, ..., dL_f^{r_p-1}h_p\}$ and $\mathcal{L}$ is the related distribution:
$$\mathcal{L} = span\{h_1, ..., L_f^{r_1-1}h_1, ..., h_p, ..., L_f^{r_p-1}h_p\}$$
where $r = \dim \Omega = \sum_{i=1}^{p} r_i$.
- G is the smallest involutive distribution that contains $\{g_1(x), ..., g_m(x)\}$. Note $k = dimG$, $m \leq k \leq n$.
- $G^{\perp}$ is the annihilator of G: $G^{\perp} = span\{\alpha_1, ..., \alpha_{n-k}\}$, where the α_i are one-forms such that for all $\lambda \in G$, $l_\lambda \alpha_i = 0$ for $i = 1 : n-k$, where $l_\lambda \alpha = \alpha(\lambda)$ is the inner product of the vector field λ and α.

Assume $r < n$. There exists a transformation $(\xi, \eta) = \phi(x)$ such that the system (1) can be locally transformed into the following normal form:

$$\begin{cases} \dot{\xi}_1^i = \xi_2^i \\ \vdots \\ \dot{\xi}_{r_i-1}^i = \xi_{r_i}^i \\ \dot{\xi}_{r_i}^i = L_f^{r_i} h_i(x) + \sum_{j=1}^{m} L_{g_j} L_f^{r_i-1} h_i(x) u_j \\ \dot{\eta} = Q(\xi, \eta, u) \\ y_i = \xi_1^i \end{cases} \tag{2}$$

where $\xi = \left[\begin{array}{ccc} \xi^1 & \cdots & \xi^p \end{array} \right]^T$ and

$$\xi^i = \left[\begin{array}{c} \xi_1^i \\ \vdots \\ \xi_{r_i}^i \end{array} \right] = \left[\begin{array}{c} h_i(x) \\ \vdots \\ L_f^{r_i-1} h_i(x) \end{array} \right], \text{ for } i \in [1, p].$$

If $r < n$ and if the distribution $span\{g_1, \ldots, g_m\}$ is not involutive, u can not be obtained using classical observation algorithm. [1] provided an algorithm, under sufficient conditions, to allow the recovery of both the state and the unknown inputs in finite time. The main idea of this algorithm is to find extra information through functions of the outputs and their time derivatives. Let us define:

$$V = \left[\begin{array}{ccc} L_f^{r_1} h_1(x) & \cdots & L_f^{r_p} h_p(x) \end{array} \right]^T + \Gamma(x) u \tag{3}$$

$$= \left[\begin{array}{ccc} y_1^{(r_1)} & \cdots & y_p^{(r_p)} \end{array} \right]^T \tag{4}$$

that can be known using the normal form (2).

Assume there exist $1 \times p$ vector functions

$$K(x) = [k_1(x), ..., k_p(x)] \in \mathcal{L}(x), with K(x) \neq 0$$

such that

$$K\Gamma = 0 \tag{5}$$

and define a fictitious output as follows:

$$\bar{y} = \bar{h}(x) = KV = \sum_{i=1}^{p} k_i(x) L_f^{r_i} h_i(x).$$

If $\bar{y} \notin \mathcal{L}(x)$, it can be considered as a suitable fictitious output in order to estimate more states[1]. Set $y = [y, \bar{y}]^T$. The system has a new relative degree with respect to this output and the algorithm iterates until the new relative degree with all new fictitious outputs is equal to n, and then it has been shown in [1] that both the state x and the unknown input u can be estimated in finite time. And a more general case: $r < n$ (even with all new fictitious outputs y), will be discussed in this paper. In the next section, several hypothesis will be given for system (2) in order to deduce a practical form with zero dynamics, which can be applied into multi data secure communication based on synchronization of chaotic system.

[1]It should be noticed that there may exist a submanifold of singularity $S = \{x \in U \text{ such that } \bar{h}(x) \in \mathcal{L}(x)\}$.

III. Zero Dynamics

Suppose that after s^{th} steps iteration, all new fictitious outputs construct the $\bar{\mathcal{L}}(x)$ as follows:

$$\begin{aligned} \bar{\mathcal{L}}(x) = \; & span\{h_1, ..., L_f^{r_1-1}h_1, ..., h_p, ..., L_f^{r_p-1}h_p, \\ & \bar{y}_{p+1}, ..., L_f^{r_{p+1}-1}\bar{y}_{p+1}, ...\bar{y}_{p+s}, ..., L_f^{r_{p+s}-1}\bar{y}_{p+s}\} \end{aligned} \tag{6}$$

and if $dim\bar{\mathcal{L}} = n$, then we can recover all the states and all the unknown inputs. However, for the last time iteration of this algorithm, if there is no new $\bar{y} \notin \bar{\mathcal{L}}$, or if there is a singularity, moreover if $dim\bar{\mathcal{L}} < n$, can we still recover all the states and all the unknown inputs? The answer is based on the Proposition 1.3 in Chapter 5 of [6]:

Proposition 1: [6]If $dimG = k = m$, which means that the distribution spanned by $\{g_1(x), ..., g_m(x)\}$ is involutive, then $dimG^{\perp} = n - m$. Moreover if $dim(G^{\perp} \cup \Omega) = n$, where

$$\Omega = \{dh_1, ..., dL_f^{r_1-1}h_1, ..., dh_m, ..., dL_f^{r_m-1}h_m\}$$

then there exists a diffeomorphism which can transform the original system into the following form with zero dynamics:

$$\begin{cases} \dot{\xi}_1^i = \xi_2^i \\ \vdots \\ \dot{\xi}_{r_i-1}^i = \xi_{r_i}^i \\ \dot{\xi}_{r_i}^i = a_i(\xi, \eta) + \sum_{j=1}^{m} b_j^i(\xi, \eta) u_j \\ \dot{\eta} = Q(\xi, \eta) \\ y_i = \xi_1^i \end{cases} \tag{7}$$

where $a_i(\xi, \eta) = L_f^{r_i} h_{i|\phi^{-1}(\xi,\eta)}$, and $b_j^i(\xi, \eta) = L_{g_j} L_f^{r_i-1} h_{i|\phi^{-1}(\xi,\eta)}$, for $i \in [1, p]$

Remark 1: For system (1), if $p = m = 1$, there is only one input g, which is obviously involutive. So in this case, it can be also transformed into the system (7).

Moreover, the following lemma is an extension of the above proposition for the case where the inputs are not involutive.

Lemma 1: Suppose that the last iteration of the algorithm gives $\bar{\mathcal{L}}(x)$ defined in (6) where $dim\bar{\mathcal{L}} = q < n$ and $rank\Gamma = m$. Define

$$\begin{aligned} \Omega = \; & \{dh_1, ..., dL_f^{r_1-1}h_1, ..., dh_m, ..., dL_f^{r_m-1}h_m, d\bar{y}_{p+1}, \\ & ..., dL_f^{r_{p+1}-1}\bar{y}_{p+1}, ..., d\bar{y}_{p+s}, ..., dL_f^{r_{p+s}-1}\bar{y}_{p+s}\} \end{aligned}$$

If

$$dim(G^{\perp} \cup \Omega) = n \tag{8}$$

then system (2) can be described into form (7), where $a_i(\xi,\eta) = L_f^{r_i} h_{i|\phi^{-1}(\xi,\eta)}$, and $b_j^i(\xi,\eta) = L_{g_j} L_f^{r_i-1} h_{i|\phi^{-1}(\xi,\eta)}$, for $i \in [1, p+s]$.

Proof: Suppose that

$$dim(G^{\perp} \cup \Omega) = n$$

with $dim\bar{\mathcal{L}} = q < n$ and $rank\Gamma = m$, it is possible to find $(n-q)$ functions from the set $\{\lambda_1, ..., \lambda_{n-k}\}$, without loss of generality, choosing $\{\lambda_1, ..., \lambda_{n-q}\}$, such that, the n differentials $\{dh_1, ..., dL_f^{r_1-1}h_1, ..., dh_p, ..., dL_f^{r_p-1}h_p,$
$d\bar{y}_{p+1}, ..., dL_f^{r_{p+1}-1}\bar{y}_{p+1}, ..., d\bar{y}_{p+s}, ..., dL_f^{r_{p+s}-1}\bar{y}_{p+s},$
$d\lambda_1, ..., d\lambda_{n-q}\}$ are linearly independent. Then there exists a diffeomorphism

$$\begin{aligned} \phi = \quad & \{h_1, ..., L_f^{r_1-1}h_1, ..., h_p, ..., L_f^{r_p-1}h_p, \\ & \bar{y}_{p+1}, ..., L_f^{r_{p+1}-1}\bar{y}_{p+1}, ..., \bar{y}_{p+s}, ..., \\ & L_f^{r_{p+s}-1}\bar{y}_{p+s}, \lambda_1, ..., \lambda_{n-q}\} \end{aligned} \tag{9}$$

which transforms system (2) into the form (7), whose zero dynamics part is given by

$$\dot{\eta} = Q(\xi,\eta)_{|\xi=0} \tag{10}$$

■

Remarks 1:

i) If $dim\bar{\mathcal{L}} = r < n$ and $dim(G^{\perp} \cup \Omega) < n$, then there does exist zero dynamics part in the transformed system, i.e., equation (10) becomes $\dot{\eta} = Q(\xi,\eta,u)$.

ii) If for all $i \in [1, p+s]$, $j \in [1, n-q]$, $\frac{\partial \dot{\xi}_{r_i}^i}{\partial \eta_1} = ... = \frac{\partial \dot{\xi}_{r_i}^i}{\partial \eta_{n-q}} = 0$, i.e., equation (10) becomes $\dot{\eta} = Q(\eta)$, then it is possible to recover the unknown input u.

iii) If for a certain $i \in [1, p+s]$, $j \in [1, n-q]$, we have $\frac{\partial \dot{\xi}_{r_i}^i}{\partial \eta_j} \neq 0$, then the unknown input u depends on the detectability of η.

For solving the problem stated above, we need the following hypothesis:

Hypothesis 1: The zero dynamics of system (7) is uniformly, at least exponentially detectable, i.e., there exists a strictly definitive positive Lyapunov function $V(\eta - \bar{\eta})$ which satisfies, for all $\eta, \bar{\eta}$ and ξ, the following relations:

$$\dot{V}(\eta - \bar{\eta}) = \frac{\partial V}{\partial(\eta - \bar{\eta})} [Q(\xi,\eta) - Q(\xi,\bar{\eta})] \leqslant -K_0 V$$

where K_0 is a positive constant. And moreover ϕ defined in (9) is a diffeomorphism on U.

Hypothesis 2: The system (1) is Bounded Input Bounded State (BIBS).

In the next section, for the proposed system (7), a sliding mode observer is designed in order to recover both state and unknown inputs.

IV. Observer design with unknown inputs estimation

Under the Hypothesis 1 and 2, we can observe both state and unknown inputs of system (7) using the following sliding mode observer

$$\begin{cases} \dot{\hat{\xi}}_1^i = \hat{\xi}_2^i + \lambda_1^i sign(\xi_1^i - \hat{\xi}_1^i) \\ \dot{\hat{\xi}}_2^i = \hat{\xi}_3^i + E_1^i \lambda_2^i sign(\tilde{\xi}_2^i - \hat{\xi}_2^i) \\ \vdots \\ \dot{\hat{\xi}}_{r_i-1}^i = \hat{\xi}_{r_i}^i + E_{r_i-2}^i \lambda_{r_i-1}^i sign(\tilde{\xi}_{r_i-1}^i - \hat{\xi}_{r_i-1}^i) \\ \dot{\hat{\xi}}_{r_i}^i = a_i(\tilde{\xi},\hat{\eta}) + E_{r_i-1}^i \lambda_{r_i}^i sign(\tilde{\xi}_{r_i-1}^i - \hat{\xi}_{r_i-1}^i) \\ \dot{\hat{\eta}} = Q(\tilde{\xi},\hat{\eta}) E_{n-q} \end{cases} \tag{11}$$

with the auxiliary states:

$$\tilde{\xi}_{t+1}^i = \hat{\xi}_{t+1}^i + E_t^i \lambda_{t+1}^i sign(\tilde{\xi}_{t+1}^i - \hat{\xi}_{t+1}^i) \tag{12}$$

where

$$\begin{aligned} E_t^i &= \begin{cases} 1 & \text{if } \tilde{\xi}_{t+1}^i = \hat{\xi}_{t+1}^i \text{ and } E_{t-1}^i = 1 \\ 0 & \text{otherwise} \end{cases} \\ E_{n-q} &= \begin{cases} 1 & \text{if all } E_t^i = 1 \\ 0 & \text{otherwise} \end{cases} \end{aligned} \tag{13}$$

for $i \in [1, q]$ (Noted: $\tilde{\xi}_1^i = \xi_1^i$).

Lemma 2: Thanks to the observer given in (11), for any initial condition, there exists λ_i^j and $t_r > 0$ such that $\forall t > t_r$, $\hat{\xi}(t) = \tilde{\xi}(t) = \xi(t)$ and $\lim_{t \to +\infty} |\eta(t) - \hat{\eta}(t)| = 0$.

Proof: Set $e_t^i = \xi_t^i - \hat{\xi}_t^i$, for $i \in [1, p+s]$, $t \in [1, r_i]$, $(\tilde{\xi}_1 = \xi_1)$.

Assume that after the first $(j-1)^{th}$ step, $j \in [2, p+s]$, we have obtained:

$$\tilde{\xi}_{j-1}^i = \hat{\xi}_{j-1}^i$$

and $E_{j-1}^i = 1$. Then we have

$$\tilde{\xi}_j^i = \hat{\xi}_j^i + \lambda_{j-1}^i sign(\tilde{\xi}_{j-1}^i - \hat{\xi}_{j-1}^i) = \xi_j^i.$$

So for the j^{th} step, the dynamic of observation error can be described in the following form:

$$\dot{e}_j^i = \xi_{j+1}^i - \hat{\xi}^i{}_{j+1} - E_{j-1}^i \lambda_j^i sign(\tilde{\xi}_j^i - \hat{\xi}_j^i)$$

We can choose the following Lyapunov function:

$$V_j^i = \frac{1}{2} \left(e_j^i\right)^2$$

Thanks to $E_{j-1}^i = 1$, and $\tilde{\xi}_j^i = \xi_j^i$, we have:

$$\dot{V}_j^i = e_j^i \left[\xi_{j+1}^i - \hat{\xi}_{j+1}^i - \lambda_j^i sign(e_j^i)\right]$$

So if $\lambda_j^i > \left|\xi_{j+1}^i - \hat{\xi}_{j+1}^i\right|_{\max}$ (i.e., $\exists k_j^i > 0$, such that $\lambda_j^i = k_j^i + \left|\xi_{j+1}^i - \hat{\xi}_{j+1}^i\right|_{\max}$), then

$$\dot{V}_j^i = -k|e| = -kV^{1/2}$$

which means there exists t_j^i, such that if $t > t_j^i > t_{j-1}^i$, $e_j^i = \dot{e}_j^i = 0$, and we obtain:

$$\xi_{j+1}^i - \hat{\xi}_{j+1}^i = \lambda_j^i sign(e_j^i) \tag{14}$$

According to the definitions of (12) and (13), we have:

$$\tilde{\xi}_{j+1}^i = \hat{\xi}_{j+1}^i$$

and $E_j^i = 1$.

Therefore, step by step we can recover all the components of vector ξ . But due to the unknown input u_i, we cannot recover η through $\dot{\xi}_r^i$. However, under the Hypothesis 1, we can reconstruct the remain states as follows.

Under the Hypothesis 2, as the state is bounded for all $t > 0$, then η is bounded. Moreover the estimation error of the zero dynamics ($e_{n-q} = \eta - \hat{\eta}$) is equal to:

$$\dot{e}_{n-q} = Q(\xi, \eta) - Q(\tilde{\xi}, \hat{\eta})$$

Thus from Hypothesis 1, we deduce that

$$\lim_{t\to\infty} |\eta(t) - \hat{\eta}(t)| = 0.$$

■

Proposition 2: Under Hypothesis 1 and 2, with $rank\Gamma = m$, thanks to the observer (11), for any given bounded initial condition, there exists $t_r > 0$ such that $\forall t > t_r$

$$\begin{aligned} &\hat{\xi}(t) = \tilde{\xi}(t) = \xi(t), \\ &\lim_{t\to+\infty} |\eta(t) - \hat{\eta}(t)| = 0 \quad \text{and} \\ &\lim_{t\to+\infty} |u(t) - \tilde{u}(t)| = 0 \end{aligned}$$

Proof:

Reconstruction of the unknown input u

As ξ and u are bounded, we can choose

$$\lambda_{k_i}^i > \left| a_i(\xi, \eta) - a_i(\tilde{\xi}, \hat{\eta}) + \sum_{j=1}^{m} b_j^i(\xi, \eta) u_j \right|_{\max},$$

such that $e_{r_i}^i$ converges to zero in finite time. Consequently we obtain $\xi = \tilde{\xi}$.

Set

$$\Gamma = \begin{bmatrix} b_1^1(\xi,\eta) & \cdots & b_m^1(\xi,\eta) \\ \vdots & \ddots & \vdots \\ b_1^{p+s}(\xi,\eta) & \cdots & b_m^{p+s}(\xi,\eta) \end{bmatrix}$$

As $rank\Gamma = m$, without loss of generality, we can assume that the first m rows are independent, i.e., $rankB(\xi, \eta) = m$, where $B(\xi,\eta) = \begin{bmatrix} b_1^1(\xi,\eta) & \cdots & b_m^1(\xi,\eta) \\ \vdots & \ddots & \vdots \\ b_1^m(\xi,\eta) & \cdots & b_m^m(\xi,\eta) \end{bmatrix}$. So we have $\dot{\tilde{\xi}}_r = A(\tilde{\xi}, \hat{\eta}) + B(\tilde{\xi}, \hat{\eta})u$, where $\dot{\tilde{\xi}}_r = \begin{bmatrix} \dot{\hat{\xi}}_{r_1}^1 \\ \vdots \\ \dot{\hat{\xi}}_{r_m}^m \end{bmatrix}$, $A(\tilde{\xi}, \hat{\eta}) = \begin{bmatrix} a_1(\tilde{\xi}, \hat{\eta}) \\ \vdots \\ a_m(\tilde{\xi}, \hat{\eta}) \end{bmatrix}$ and $u = \begin{bmatrix} u_1 \\ \vdots \\ u_m \end{bmatrix}$.

Once all the states ξ are observed and η is estimated exponentially, there exists $t_r > t_j^i$, for all $i \in [1, p+s]$, $j \in [1, r_i]$, when $t > t_r$, such that

$$e_A := A(\xi, \eta) - A(\tilde{\xi}, \hat{\eta})$$

then we can obtain

$$e_A + B\left(\tilde{\xi}, \hat{\eta}\right) u = E_{r-1} \lambda_r sign(\tilde{\xi}_r - \hat{\xi}_r) \tag{15}$$

where $E_{r-1} = diag\{E_{r_1-1}^1, E_{r_2-1}^2, ..., E_{r_m-1}^m\}$, $\lambda_r = diag\{\lambda_{r_1}^1, \lambda_{r_2}^2, ..., \lambda_{r_m}^m\}$ and $sign(\tilde{\xi}_r - \hat{\xi}_r) = \begin{bmatrix} sign(\tilde{\xi}_{r_1}^1 - \hat{\xi}_{r_1}^1) \\ \vdots \\ sign(\tilde{\xi}_{r_m}^m - \hat{\xi}_{r_m}^m) \end{bmatrix}$.

So if we assume:

$$\tilde{u} = B^{-1}(\tilde{\xi}, \hat{\eta}) E_{r-1} \lambda_r sign(\tilde{\xi}_r - \hat{\xi}_r) \tag{16}$$

for $t > t_r$, we have

$$\begin{aligned} u - \tilde{u} = &\left[B^{-1}(\xi,\eta) - B^{-1}(\xi,\hat{\eta})\right] E_{r-1} \lambda_r sign(\tilde{\xi}_r - \hat{\xi}_r) \\ &- B^{-1}(\xi,\eta) e_A \end{aligned}$$

and consequently, from the convergence of e_A and $(\eta - \hat{\eta})$ to zero, we have

$$\lim_{t\to\infty} |u - \tilde{u}| = 0$$

■

V. Example

In order to highlight the proposed method, we construct a simple multiple secure communication system based on the Qi's chaotic system in [9], which is described as follows:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2 x_3 x_4 \\ \dot{x}_2 = b(x_1 + x_2) - x_1 x_3 x_4 \\ \dot{x}_3 = -c x_3 + x_1 x_2 x_4 \\ \dot{x}_4 = -d x_4 + x_1 x_2 x_3 \end{cases} \tag{17}$$

where $x_i (i = 1:5)$ are the state variables, and a, b, c, d are all positive real constant parameters. Consider the following transmitter which is based on the chaotic system (17):

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2 x_3 x_4 + m_1 \\ \dot{x}_2 = b(x_1 + x_2) - x_1 x_3 x_4 \\ \dot{x}_3 = -c x_3 + x_1 x_2 x_4 + x_3 x_5 m_2 \\ \dot{x}_4 = -d x_4 + x_1 x_2 x_3 - x_4 x_5 m_2 \\ \dot{x}_5 = -10 x_5 + x_3 x_4 \end{cases} \tag{18}$$

where $g_1 = [\ 1 \quad 0 \quad 0 \quad 0 \quad 0\ ]^T$ and $g_2 = [\ 0 \quad 0 \quad x_3 x_5 \quad -x_4 x_5 \quad 0\ ]^T$. It is obvious that g_1

and g_2 are involutive. Assume that m_1 and m_2 are small, that $m_2 > 0$, and that the following condition is satisfied

$$m_2 + \frac{d-c}{x_5} > 0. \tag{19}$$

Suppose that the outputs are set as $y = \left[\begin{array}{cc} x_1 & x_2 \end{array} \right]^T$. The input channel vector fields g_1 and g_2 have been chosen such that the relative degree of the system is $r = 3$. So, following the lines of the algorithm proposed in [1], set $\pounds(x) = span\{h_1, h_2, L_f h_2\}$. Since

$$L_f h_2 = b(x_1 + x_2) - x_1 x_3 x_4 = x_3 x_4 mod\{x_1, x_2\}$$

one has $\pounds(x) = span\{x_1, x_2, x_3 x_4\}$. Then let us calculate

$$\Gamma = \left(\begin{array}{cc} L_{g_1} h_1 & L_{g_2} h_1 \\ L_{g_1} L_f h_2 & L_{g_2} L_f h_2 \end{array} \right) = \left(\begin{array}{cc} 1 & 0 \\ b - x_3 x_4 & 0 \end{array} \right).$$

One can choose $K = \left(\begin{array}{cc} b - x_3 x_4, & -1 \end{array} \right)$ such that $K\Gamma = (0, 0)$.

Then the following fictitious output can be defined:

$$\begin{array}{rcl} \bar{y} & = & K \left[\begin{array}{c} L_f h_1 \\ L_f^2 h_2 \end{array} \right] = (b - x_3 x_4)\, \dot{y}_1 - \ddot{y}_2 \\ & = & \left(x_3^2 + x_4^2\right) mod \pounds(x) \end{array}$$

because $\bar{y} \notin \pounds(x)$, and $\bar{y}$ can be selected as a new fictitious output. Then, let us set

$$y \triangleq \left[\begin{array}{ccc} x_1, & x_2, & x_3^2 + x_4^2 \end{array} \right]^T.$$

With this new output y, we have $\bar{\pounds}(x) = span\{x_1, x_2, x_3 x_4, \left(x_3^2 + x_4^2\right)\}$, where $dim \bar{\pounds}(x) = 4 < 5$. But due to the fact that $\{g_1, g_2\}$ is involutive, so according to Proposition 1, transmitter (18) can be transformed into the following form (7). Due to Proposition 2, we can recover both the state and the unknown messages in finite time. For this, let us design a sliding mode observer for system (18) as follows:

$$\left\{ \begin{array}{l} \dot{\hat{x}}_1 = a\,(x_2 - x_1) + x_2 \tilde{x}_3 \tilde{x}_4 + E_1 \lambda_1 sign(x_1 - \hat{x}_1) \\ \dot{\hat{x}}_2 = b(x_1 + x_2) + \lambda_2 sign(x_2 - \hat{x}_2) \\ \frac{d(\hat{x}_3 \hat{x}_4)}{dt} = -\,(c+d)\,\tilde{x}_3 \tilde{x}_4 \\ \qquad\quad + E_2 \lambda_3 sign(\tilde{x}_3 \tilde{x}_4 - \hat{x}_3 \hat{x}_4) \\ \frac{d\left(\hat{x}_3^2 + \hat{x}_4^2\right)}{dt} = -2c\tilde{x}_3^2 - 2d\tilde{x}_4^2 + 4x_1 x_2 \tilde{x}_3 \tilde{x}_4 \\ \qquad\quad + 2E_3 \lambda_4 sign\left(\left(\tilde{x}_3^2 + \tilde{x}_4^2\right) - \left(\hat{x}_3^2 + \hat{x}_4^2\right)\right) \\ \dot{\hat{x}}_5 = E_3\left(-10\hat{x}_5 + \tilde{x}_3 \tilde{x}_4\right) \end{array} \right. \tag{20}$$

with

$$\begin{array}{l} \lambda_i > 0,\ i = 1, ..., 4 \\ E_1 = \left\{ \begin{array}{ll} 1 & \text{if } x_2 = \hat{x}_2 \\ 0 & \text{otherwise} \end{array} \right. \\ E_2 = \left\{ \begin{array}{ll} 1 & \text{if } E_1 = 1 \text{ and } x_1 = \hat{x}_1 \\ 0 & \text{otherwise} \end{array} \right. \\ E_3 = \left\{ \begin{array}{ll} 1 & \text{if } E_2 = 1 \text{ and } \tilde{x}_3 \tilde{x}_4 = \hat{x}_3 \hat{x}_4 \\ 0 & \text{otherwise} \end{array} \right. \\ E_4 = \left\{ \begin{array}{ll} 1 & \text{if } E_3 = 1 \text{ and } \hat{x}_5 = x_5 \\ 0 & \text{otherwise} \end{array} \right. \end{array}$$

and with the auxiliary states:

$$\begin{array}{rcll} \tilde{x}_3 \tilde{x}_4 & = & -\dfrac{\lambda_2 sign(x_2 - \hat{x}_2)}{x_1} & (21) \\ \tilde{x}_3^2 + \tilde{x}_4^2 & = & \dfrac{E_2 \lambda_3 sign(\tilde{x}_3 \tilde{x}_4 - \hat{x}_3 \hat{x}_4)}{\hat{x}_5 x_1 x_2}. & (22) \end{array}$$

Obviously the submanifold of observability singularity S is equal to $S = \{x_1 = 0\} \cup \{x_1 x_2 = 0\}$.

Let us also define

$$\begin{array}{rcll} \tilde{m}_1 & = & E_2 \lambda_1 sign(x_1 - \hat{x}_1) & (23) \\ \tilde{m}_2 & = & \dfrac{E_5 \lambda_4 sign\left(\left(\tilde{x}_3^2 + \tilde{x}_4^2\right) - \left(\hat{x}_3^2 + \hat{x}_4^2\right)\right)}{\hat{x}_5\left(\tilde{x}_3^2 - \tilde{x}_4^2\right)}. & (24) \end{array}$$

where

$$E_5 = \left\{ \begin{array}{ll} 1 & \text{if } E_4 = 1 \text{ and } \tilde{x}_3^2 + \tilde{x}_4^2 = \hat{x}_3^2 + \hat{x}_4^2 \\ 0 & \text{otherwise} \end{array} \right.$$

The observation errors are defined by:

$$\begin{array}{l} e_1 = x_1 - \hat{x}_1 \\ e_2 = x_2 - \hat{x}_2 \\ e_{34} = x_3 x_4 - \hat{x}_3 \hat{x}_4 \\ e_{3^2+4^2} = \left(x_3^2 + x_4^2\right) - \left(\hat{x}_3^2 + \hat{x}_4^2\right) \\ e_5 = x_5 - \hat{x}_5 \end{array}$$

From system (18), it can be computed that:

$$\frac{d\,(x_3 x_4)}{dt} = -\,(c+d)\,x_3 x_4 + x_1 x_2\left(x_3^2 + x_4^2\right)$$

and

$$\begin{array}{rcl} \dfrac{d\left(x_3^2 + x_4^2\right)}{dt} & = & -2cx_3^2 + 4x_1 x_2 x_3 x_4 \\ & & -2dx_4^2 + 2\left(x_3^2 - x_4^2\right) m_2. \end{array} \tag{25}$$

Thus the dynamics of the observation error is given by

$$\left\{ \begin{array}{l} \dot{e}_1 = x_2\left(x_3 x_4 - \tilde{x}_3 \tilde{x}_4\right) + m_1 - E_1 \lambda_1 sign(e_1) \\ \dot{e}_2 = -x_1 x_3 x_4 - \lambda_2 sign(e_2) \\ \dot{e}_{34} = -\,(c+d)\left(x_3 x_4 - \tilde{x}_3 \tilde{x}_4\right) + x_1 x_2\left(x_3^2 + x_4^2\right) \\ \qquad\quad - E_2 \lambda_3 sign(\tilde{x}_3 \tilde{x}_4 - \hat{x}_3 \hat{x}_4) \\ \dot{e}_{3^2+4^2} = -2c\left(x_3^2 - \tilde{x}_3^2\right) - 2d\left(x_4^2 - \tilde{x}_4^2\right) \\ \qquad\quad + 4x_1 x_2\left(x_3 x_4 - \tilde{x}_3 \tilde{x}_4\right) + 2\left(x_3^2 - x_4^2\right) m_2 \\ \qquad\quad - 2E_3 \lambda_4 sign\left(\left(\tilde{x}_3^2 + \tilde{x}_4^2\right) - \left(\hat{x}_3^2 + \hat{x}_4^2\right)\right) \\ \dot{e}_5 = -10x_5 + x_3 x_4 - E_3\left(-10\hat{x}_5 + \tilde{x}_3 \tilde{x}_4\right) \end{array} \right.$$

The convergence of the sliding mode observer has been proved in the previous section. But for this example, it should note that the possibility to estimate m_2 requires the knowledge of $\tilde{x}_3^2$ and $\tilde{x}_4^2$, which can be computed in the following way after the successful estimations of $\hat{x}_5$, $\tilde{x}_3 \tilde{x}_4$ and $\left(\tilde{x}_3^2 + \tilde{x}_4^2\right)$.

The convergence of $\tilde{x}_3 \tilde{x}_4$ and $\left(\tilde{x}_3^2 + \tilde{x}_4^2\right)$ can be easily obtained. Moreover as x_5 is uniformly exponentially detectable, we can detect $\hat{x}_5$. Indeed, we choose $V(e_5) = \frac{e_5^2}{2}$, then $\dot{V}(e_5) = -10e_5^2 < 0$, which implies that the Hypothesis 1 is satisfied with $K_0 = 10$, and we obtain $\lim\limits_{t \to +\infty} |x_5 - \hat{x}_5| = 0$.

Then we can define: $\tilde{x}_3\tilde{x}_4 = A$ and $\tilde{x}_3^2 + \tilde{x}_4^2 = B$, obviously there are two groups of solutions:

$$S_1 : \begin{cases} \tilde{x}_{3_1}^2 = \frac{B+\sqrt{B^2-4A^2}}{2} \\ \tilde{x}_{4_1}^2 = \frac{B-\sqrt{B^2-4A^2}}{2} \end{cases}$$
and
$$S_2 : \begin{cases} \tilde{x}_{3_2}^2 = \frac{B-\sqrt{B^2-4A^2}}{2} \\ \tilde{x}_{4_2}^2 = \frac{B+\sqrt{B^2-4A^2}}{2} \end{cases} \quad (26)$$

Suppose that S_1 is the correct solution. From (25), the confidential message can be recovered correctly as follows:

$$-c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + \left(\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2\right)\hat{x}_5 m_{2_1} = -2x_1x_2\tilde{x}_3\tilde{x}_4 \triangleq C. \quad (27)$$

In this case, one has for S_2:

$$-c\tilde{x}_{3_2}^2 - d\tilde{x}_{4_2}^2 + \left(\tilde{x}_{3_2}^2 - \tilde{x}_{4_2}^2\right)\hat{x}_5 m_{2_2} = C. \quad (28)$$

Using equations (27) and (28), one has:

$$m_{2_2} = \frac{\left[\begin{array}{l} -c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + \left(\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2\right)\hat{x}_5 m_{2_1} \\ +c\tilde{x}_{3_2}^2 + d\tilde{x}_{4_2}^2 \end{array}\right]}{\left(\tilde{x}_{3_2}^2 - \tilde{x}_{4_2}^2\right)\hat{x}_5}$$

Note that $\tilde{x}_{3_1}^2 = \tilde{x}_{4_2}^2$ and $\tilde{x}_{3_2}^2 = \tilde{x}_{4_1}^2$. So this equation becomes

$$\begin{aligned} m_{2_2} &= \frac{\left[\begin{array}{l} -c\tilde{x}_{3_1}^2 - d\tilde{x}_{4_1}^2 + \left(\tilde{x}_{3_1}^2 - \tilde{x}_{4_1}^2\right)\hat{x}_5 m_{2_1} \\ +c\tilde{x}_{4_1}^2 + d\tilde{x}_{3_1}^2 \end{array}\right]}{\left(\tilde{x}_{4_1}^2 - \tilde{x}_{3_1}^2\right)\hat{x}_5} \\ &= \frac{c-d}{\hat{x}_5} - m_{2_1} \end{aligned}$$

If m_{2_1} is the correct solution, then $m_{2_2} < 0$ according to equation (19) and this excludes the solution m_{2_2}. Following this way, the correct solution corresponding to $\tilde{x}_3^2$ and $\tilde{x}_4^2$ can be found.

Since $\tilde{x}_3^2$ and $\tilde{x}_4^2$ have been estimated, one has:

$$\dot{e}_{3^2+4^2} = 2x_5(x_3^2 - x_4^2)m_2 - 2E_3\lambda_4 sign\left(e_{3^2+4^2}\right)$$

Thus, tuning $\lambda_4 > \left|x_5(x_3^2 - x_4^2)m_2\right|_{\max}$ ensures that

$$\lim_{t\to+\infty} \left|x_5(x_3^2 - x_4^2)m_2 - \lambda_4 sign\left(e_{3^2+4^2}\right)\right| = 0.$$

Then the relation (24) leads to the estimation of the second confidential message:

$$\begin{aligned} &\lim_{t\to+\infty} |\tilde{m}_2 - m_2| \\ = &\lim_{t\to+\infty} \left|\frac{E_4\lambda_4 sign\left(e_{3^2+4^2}\right)}{\hat{x}_5\left(\tilde{x}_3^2 - \tilde{x}_4^2\right)} - \frac{E_4\lambda_4 sign\left(e_{3^2+4^2}\right)}{x_5\left(\tilde{x}_3^2 - \tilde{x}_4^2\right)}\right| \\ = &\ 0. \end{aligned}$$

Figure 1 exhibits the states of the transmitter and those of the receiver. Figure 2 illustrates the original messages and their estimation. Figure 1 shows that the states of the receiver converge fast to those of the transmitter. It can be seen in Figure 2 that, once the state is estimated, the confidential messages are well reconstructed.

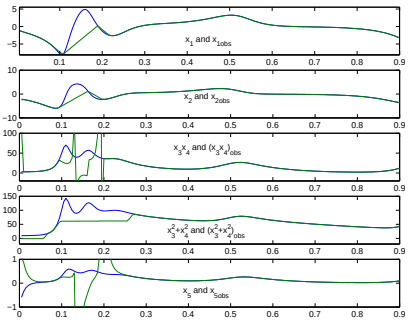

Fig. 1. States observation for transmitter and the receiver

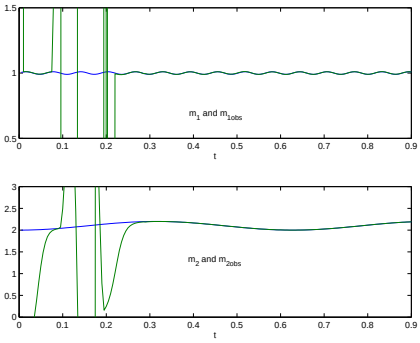

Fig. 2. Message observation for transmitter and the receiver

VI. Conclusion

The topic of this paper is to apply the the algorithm presented by [1] into multi data secure communication. Based on this algorithm, we propose a new scheme, under the condition on zero dynamics, to solve the Left Invertibility Problem. Moreover, an illustrated example based on one Qi's chaotic system is established in order to highlight the proposed method.

References

[1] Barbot J.P, Boutat D. and Floquet T. "A new observation algorithm for nonlinear system with unknown inputs". *IEEE CDC-ECC.*, seville, Dec 2005.

[2] Darouach M., Zasadzinski M. and Xu S.J., Full-order Observers for linear systems with unknown inputs. *IEEE Tans. on Auto. Contr.*, Vol. 39(3), pp 606-609, 1994.

[3] Floquet, T, Barbot, J.P., "A slidin mode approach of unknown input observers for linear systems". *IEEE CDC.*, pp 1724-1729, 2004.

[4] Hautus, M.L.J, Strong detectability and observers. *Linear algebra and its applications.*, vol. 50, pp 353-368.

[5] Hou, M. , Mülle, P.C., Disturbance decoupled observer design: A unified viewpoint. *IEEE Trans. on Auto. Contr.*, vol. 39(6), pp 632-635, 1994.

[6] Isidori A., *Nonlinear control systems.*, 3rd edition, Springer, Berlin, 1995.

[7] Nijmeijer H. and Mareels I. M. Y. An observer looks at synchronization. *IEEE Trans. on Circuits and Systems-1: Fundamental theory and Applications.*, vol. 44(10), pp 882-891, 1997.

[8] Pecora L. M. and Carroll T. L. Synchronization in chaotic systems. *Physical Review Letters.* vol. 64, pp 821-824, 1990.

[9] Qi G.Y., Du S.Z., Chen G.R. et al. On a four-dimensional chaotic system. *Chaos, Solitons and Fractals.*, vol. 23, pp 2005.

[10] Singh S.N., A modified algorithm for invertibility in nonlinear system, *IEEE Trans. on Auto. Contr.*, vol. 26(2), pp 595-598, 1981.

[11] Xiong. Y, Saif, M, Sliding mode observer for nonlinear uncertain systems. *IEEE Trans. on Auto. Contr.*, vol. 46, pp 2012-2017, 2001.