구간 시변 지연이 존재하는 카오스 보안 통신시스템의 동기화

논 문
58-6-24

Synchronization of Chaotic Secure Communication Systems with Interval Time-varying Delays

권 오 민† · 박 주 현* · 이 상 문** · 박 명 진***
(Oh-Min Kwon · Ju-Hyun Park · Sang-Moon Lee · Myeong-Jin Park)

Abstract – In this paper, a method of designing a controller which ensures the synchronization between the transmission and the reception ends of chaotic secure communication systems with interval time-varying delays is proposed. To increase communication security, the transmitted message is encrypted with the techniques of N-shift cipher and public key. And to reduce the conservatism of the stabilization criterion for error dynamic system obtained from the transmitter and receiver, a new Lyapunov-functional and bounding technique are proposed. Through a numerical example, the effectiveness of the proposed method is shown in the chaotic secure communication system.

Key Words : Chaotic system, Interval time-varying delays, Secure communication, Lyapunov method, LMI

1. Introduction

During the recent decades, to increase the communication security, many efforts have been done to investigate the problem of data encryption and decryption. Since the dynamic behavior of chaotic system is highly sensitive to the initial values and parameter of a system, a considerable attention has been paid to the application of chaotic system to secure communication. For references, see [1]-[5] and references therein.

On the other hand, it is well recognized that many communication processes contain time-delays in transmission of information and time-delays often causes poor performance or even unstability [6]-[7], many efforts have been done to stability analysis of dynamic systems with either constant time-delays or time-varying delays [8]-[12]. Since delay-dependent stability and stabilization criteria, which give an information of maximum delay intervals for guaranteeing asymptotic stability, are generally less conservative than delay-independent ones when the size of time-delays are small, more attention has been paid to the delay-dependent stability and stabilization criteria than delay-independent ones. In D. Li *et al.* [5], the observer-based chaotic synchronization problem was investigated for a class of time-delay secure communication system. However, the proposed method is delay-independent and not applicable to the secure communication with fast time-varying delays, which means the time-derivative of time-delay is unknown.

Recently, delay-dependent stability or stabilization of system with interval time-varying delays has been a focused topic of theoretical and practical importance [13]-[14] in very recent years. The system with interval time-varying delays means that the lower bounds of time-delay which guarantees the stability of system is not restricted to be zero. A typical example of dynamic systems with interval time-varying delays is networked control system. However, to the best of author's knowledge, the problem of synchronization of the chaotic secure communication system with interval time-varying delays has not been investigated yet.

In this paper, we propose a new synchronization method of the chaotic system with interval time-varying delays. To reduce the conservatism of synchronization criteria, a new Lyapunov functional which fractions delay interval is proposed. Then, a sufficient condition of designing a controller L, which ensures the synchronization between the transmission and the reception ends of the chaotic secure communication system with interval time-varying delays is established in terms of Linear Matrix Inequalities(LMIs). To increase communication security, we adopt the encryption and decryption of the original to-be-transmitted message with the techniques of n-shift cipher and public key[4]. Through numerical example, it will be shown that the

† 교신저자, 정회원 : 충북대학교 전기공학과 조교수
E-mail : madwind@chungbuk.ac.kr
* 정 회 원 : 영남대학교 전기공학과 부교수
** 정 회 원 : 대구대학교 전자공학부 전임강사
*** 준 회 원 : 충북대학교 전기공학과 석사과정

접수일자 : 2009년 3월 6일
최종완료 : 2009년 4월 10일

proposed method is effective in synchronization of the transmission and reception ends of the system with interval time-varying delays of output state and recovering the original message at the reception end. Throughout this paper, ★ represents the elements below the main diagonal of a symmetric matrix. The notation $X>Y$, where X and Y are matrices of same dimensions, means that the matrix $X-Y$ is positive definite,I denotes the identity matrix whose dimensions can be determined from the context. R^n is the n-dimensional Euclidean space, $R^{m\times n}$ denotes the set of $m\times n$ real matrix. $diag\{\cdot\}$ means the diagonal matrix.

2. Problem Statements

Consider the following chaotic secure communication system with interval time-varying delays:

$$\begin{aligned} Transmitter: \dot{x}(t) &= Ax(t)+Bf(x(t))+Ls(t) \\ v(t) &= Cx(t-h(t))+s(t) \end{aligned} \qquad (1)$$

$$\begin{aligned} Receiver: \dot{y}(t) &= Ay(t)+Bf(y(t))+L(v(t)-w(t)) \\ w(t) &= Cy(t-h(t)) \end{aligned}$$

Here, $x(t)\in R^n$, $y(t)\in R^n$ are the state vectors, $v(t)\in R^p$ and $w(t)\in R^p$ are output states, $A\in R^{n\times n}$, $B\in R^{n\times n}$ and $C\in R^{1\times n}$ are known system matrices, $L\in R^n$ is the controller gain which will be designed, $h(t)$ represents time-varying delays which satisfies $0\le h_L\le h(t)\le h_U$, $\dot{h}(t)\le h_D$. $f(\cdot)$ is a nonlinear function which satisfies a sector condition with $f_j(\cdot),(j=1,2,\ldots,n)$ belonging to sectors $[k_j^-,k_j^+]$. That is,

$$(f_j(\xi)-k_j^-\xi)(f_j(\xi)-k_j^+\xi)\le 0, \forall\xi_j,\ j=1,2,\ldots,n. \qquad (2)$$

Let us define encryption key as $key_e(t)=\sum_{i=1}^{n}a_ix_i(t)$, decryption key as $key_d(t)=\sum_{i=1}^{n}a_iy_i(t)$ in which $a_i(i=1,\ldots,n)$ are constants, and $s(t)$ as the signal for applying the N-shift cipher in encryption and decryption [4] as follows:

$$\begin{aligned} s(t) &= E(s_o(t),key_e(t)) \\ &= \underbrace{f_1(\cdots f_1(f_1}_{N}(s_o(t),key_e(t)),key_e(t)),\ldots,key_e(t)), \end{aligned} \qquad (3)$$

where $s_0(t)\in R$ is the known orignal message signal, and $f_1(\cdot,\cdot)$ is the following nonlinear function:

$$f_1(x,k)=\begin{cases}(x+k)+2\tau, & -2\tau,\le(x+k)+2\tau,\le-\tau \\ (x+k), & -\tau\le(x+k)\le\tau \\ (x+k)-2\tau, & \tau\le(x+k)\le 2\tau\end{cases} \qquad (4)$$

where τ is chosen such that $s(t)$ and key signals lie within $(-\tau,\tau)$.

The recovered message $s_{or}(t)$ can be obtained by decryption function in the receiver [4] :

$$\begin{aligned} s_{or}(t) &= D(v(t)-w(t)) \\ &= f_1(\cdots f_1(f_1(s(t),-key_d(t)),-key_d(t)),\cdots-key_d(t)) \end{aligned} \qquad (5)$$

If the synchronization between transmitter and receiver is achieved, then $key_e(t)\approx key_d(t)$.

Define the synchronization error as $e(t)=x(t)-y(t)$. Then, from (1), the error dynamic system can be obtained as follows:

$$\dot{e}(t)=\dot{x}(t)-\dot{y}(t)=Ae(t)-LCe(t-h(t))+B\eta(e(t),y(t)) \qquad (6)$$

where

$\eta(e(t),y(t))=f(x(t))-f(y(t))=f(e(t)+y(t))-f(y(t))$. Suppose that

$$k_j^-\le\frac{n_j(e_j(t),y_j(t))}{e_j(t)}=\frac{f_j(e_j(t)+y_j(t))-f_j(y_j(t))}{(e_j(t)+y_j(t))-y_j(t)}\le k_j^+ \qquad (7)$$
$$\forall e_{j,}y_j(j=1,\ldots,n)$$

which implies

$$(n_j(e_j(t),y_j(t))-k_j^-)(n_j(e_j(t),y_j(t))-k_j^+)\le 0\forall e_{j,}y_j(j=1,\ldots,n). \qquad (8)$$

The objective of this paper is to develope a designing method of controller L such that the synchronization between the transmitter and receiver (1) is achieved and the original message signal $s_0(t)$ has been transmitted from the transmitter to the receiver and can be recovered at the receiver.

Before deriving the main result, we will utilize the following fact and lemma.

Fact 1. (Schur Complement) Given constant symmetric matrices $\Sigma_1,\Sigma_2,\Sigma_3$ where $\Sigma_1=\Sigma_1^T$ and $0<\Sigma_2=\Sigma_2^T$, then $\Sigma_1+\Sigma_3^T\Sigma_2^{-1}\Sigma_3<0$ if and only if

$$\begin{bmatrix}\Sigma_1 & \Sigma_3^T \\ \Sigma_3 & -\Sigma_2\end{bmatrix}<0,\text{or}\ \begin{bmatrix}-\Sigma_2 & \Sigma_3 \\ \Sigma_3^T & -\Sigma_1\end{bmatrix}<0. \qquad (9)$$

Fact 2. For any real vectors a, b and any matrix $Q>0$ with appropriate dimension, the following inequality

$$\pm 2a^Tb\le a^TQa+b^TQ^{-1}b \qquad (10)$$

is always satisfied.

To derive a less conservative stability criterion of the error dynamic system (6), let us introduce a integral inequality bounding lemma which will be used to take an upper bound of time derivative of Lyapunov functional.

Lemma 1.[15] For any constant matrix $M\in\boldsymbol{R}^{n\times n}$, $M=M^T>0$, scalar $\gamma>0$, vector function $x:[0,\ \gamma]\rightarrow\boldsymbol{R}^n$ such that the integrations concerned are well defined, then

$$\left(\int_0^\gamma x(s)ds\right)^T M\left(\int_0^\gamma x(s)ds\right)\le\int_0^\gamma x^T(s)Mx(s)ds. \qquad (11)$$

Lemma 2. For any scalar $h(t)>0$, and positive matrix Q, the following inequality holds:

$$\begin{aligned} &-\int_{t-h(t)}^{t}\dot{x}^TQ\dot{x}(s)ds\le \\ &+h(t)\zeta^T(t)\boldsymbol{X}Q^{-1}\boldsymbol{X}^T\zeta(t)+2\zeta^T(t)\boldsymbol{X}[x(t)-x(t-h(t))] \end{aligned} \qquad (12)$$

where

$$\begin{aligned} \zeta^T(t)=\Big[&e^T(t)\ e^T(t-h(t))\ e^T(t-h_L)\ e^T\left(t-\frac{h_U+h_L}{2}\right) \\ &e^T(t-h_U)\ \dot{e}^T(t)\ \eta^T(e(t),y(t))f(e(t))\Big] \end{aligned} \qquad (13)$$

and $\boldsymbol{X}$ is free variable matrix with appropriate dimension.

Proof. From Fact 2, the following inequality with Q>0 holds:

$$-\int_{t-h(t)}^{t} 2(\boldsymbol{X}^{\boldsymbol{T}}\zeta(t))^T\dot{x}(s)ds \le \tag{14}$$
$$\int_{t-h(t)}^{t}[\dot{x}^T(s)Q\dot{x}(s)+(\boldsymbol{X}^{\boldsymbol{T}}\zeta(t))^TQ^{-1}(\boldsymbol{X}\zeta(t))]ds$$

The inequality (14) can be written as

$$\begin{aligned}&\int_{t-h(t)}^{t}\zeta^T(t)\boldsymbol{X}Q^{-1}\boldsymbol{X}^{\boldsymbol{T}}\zeta(t)ds\\ &+2\zeta^T(t)\boldsymbol{X}\int_{t-h(t)}^{t}\dot{x}(s)ds+\int_{t-h(t)}^{t}\dot{x}^T(s)Q\dot{x}(s)ds\\ &=h(t)\zeta^T(t)\boldsymbol{X}Q^{-1}\boldsymbol{X}^{\boldsymbol{T}}\zeta(t)\\ &+2\zeta^T\boldsymbol{X}[x(t)-x(t-h(t)]+\int_{t-h(t)}^{t}\dot{x}^T(s)Q\dot{x}(s)ds\\ &\ge 0.\end{aligned} \tag{15}$$

Therefore, from (15), the inequality (12) can be obtained. This completes the proof of Lemma 1. ■

3. Main Results

For simplicity, let us define the following notations.

$$\Sigma=[\Sigma_{(i,j)}],(i,j=1,\ldots,8)$$
$$\Sigma_{(1,1)}=R_2+R_3-Q_3+\delta(P_1A+A^TP_1^T)-2K_1H_1K_2-2K_1H_2K_{2,}$$
$$\Sigma_{(1,2)}=-\delta YC,\ \Sigma_{(1,3)}=Q_{3,}\Sigma_{(1,4)}=0,\ \Sigma_{(1,5)}=0,$$
$$\Sigma_{(1,6)}=R_1-\delta P_1+A^TP_1^T,\ \Sigma_{(1,7)}=\delta P_1B+(K_1+K_2)H_{2,}$$
$$\Sigma_{(1,8)}=(K_1+K_2)H_1,\ \Sigma_{(2,2)}=-(1-h_D)R_2,\ \Sigma_{(2,3)}=0,\ \Sigma_{(2,4)}=0,$$
$$\Sigma_{(2,5)}=0,\ \Sigma_{(2,6)}=-C^TY^T,\ \Sigma_{(2,7)}=0,\ \Sigma_{(2,8)}=0,$$
$$\Sigma_{(3,3)}=-R_3+N_{11}-Q_3-\left(\frac{h_U-h_L}{2}\right)Q_4,\ \Sigma_{(3,4)}=N_{12}+\left(\frac{h_U-h_L}{2}\right)Q_4,$$
$$\Sigma_{(3,5)}=0,\ \Sigma_{(3,6)}=0,\ \Sigma_{(3,7)}=0,\ \Sigma_{(3,8)}=0,$$
$$\Sigma_{(4,4)}=N_{22}-N_{11}-(h_U-h_L)Q_4,\ \Sigma_{(4,5)}=-N_{12}+\left(\frac{h_U-h_L}{2}\right)Q_4,$$
$$\Sigma_{(4,6)}=0,\ \Sigma_{(4,7)}=0,\ \Sigma_{(4,8)}=0,\ \Sigma_{(5,5)}=N_{22}-\left(\frac{h_U-h_L}{2}\right)Q_4,$$
$$\Sigma_{(5,6)}=0,\ \Sigma_{(5,7)}=0,\ \Sigma_{(5,8)}=0,$$
$$\Sigma_{(6,6)}=\left(\frac{h_U-h_L}{2}\right)(Q_1+Q_2+Q_4)+h_L^2Q_3-P_1-P_1^T,$$
$$\Sigma_{(6,7)}=P_1B,\ \Sigma_{(6,8)}=\Lambda,\ \Sigma_{(7,7)}=-2H_2,\ \Sigma_{(7,8)}=0,\ \Sigma_{(8,8)}=-2H_1.$$
$$\mathbf{X}=\begin{bmatrix}0 & X_1^T & X_2^T & 0 & 0 & 0 & 0 & 0\end{bmatrix}^T,$$
$$\mathbf{Y}=\begin{bmatrix}0 & Y_1^T & 0 & Y_2^T & 0 & 0 & 0 & 0\end{bmatrix}^T,$$
$$\overline{\mathbf{X}}=\begin{bmatrix}0 & \overline{X}_1^T & 0 & \overline{X}_2^T & 0 & 0 & 0 & 0\end{bmatrix}^T,$$
$$\overline{\mathbf{Y}}=\begin{bmatrix}0 & \overline{Y}_1^T & 0 & 0 & \overline{Y}_2^T & 0 & 0 & 0\end{bmatrix}^T,$$
$$\Gamma=\begin{bmatrix}0 & -\mathbf{X}+\mathbf{Y} & \mathbf{X} & -\mathbf{Y} & 0 & 0 & 0 & 0\end{bmatrix},$$
$$\overline{\Gamma}=\begin{bmatrix}0 & -\overline{\mathbf{X}}+\overline{\mathbf{Y}} & 0 & \overline{\mathbf{X}} & -\overline{\mathbf{Y}} & 0 & 0 & 0\end{bmatrix},$$
$$\Pi_1=\begin{bmatrix}0&0&0&I&0&0&0&0\\0&0&0&0&I&0&0&0\end{bmatrix},$$
$$\Pi_2=\begin{bmatrix}0&0&I&0&0&0&0&0\\0&0&0&I&0&0&0&0\end{bmatrix},$$
$$\Xi_1=\Sigma+\Gamma+\Gamma^T+\left(\frac{h_U-h_L}{2}\right)^{-1}\Pi_1^T\begin{bmatrix}-Q_2 & Q_2\\ \star & -Q_2\end{bmatrix}\Pi_1,$$
$$\Xi_2=\Sigma+\overline{\Gamma}+\overline{\Gamma^T}+\left(\frac{h_U-h_L}{2}\right)^{-1}\Pi_2^T\begin{bmatrix}-Q_1 & Q_1\\ \star & -Q_1\end{bmatrix}\Pi_2, \tag{16}$$

Then, we have the following theorem.

Theorem 1. For given h_U, h_L satisfying $h_U>h_L>0$, and any constant h_D and δ, the chaotic secure communication system (1) is synchronized with controller gain $L=P_1^{-1}Y$ for $0\le h_L\le h(t)\le h_U$ and $\dot{h}(t)\le h_D$ if there exist positive matrices $R_i(i=1,\ldots,3)$, $Q_i(i=1,\ldots,4)$, $H_i(i=1,2)$, $\Lambda=diag\{\lambda_1,\cdots,\lambda_n\}$, $N=\begin{bmatrix}N_{11} & N_{12}\\ \star & N_{22}\end{bmatrix}$, and any matrices $X_i, Y_i, \overline{X}_i, \overline{Y}_i,(i=1,2)$ such that the following LMIs hold:

$$\begin{bmatrix}\Xi_1 & \left(\frac{h_U-h_L}{2}\right)\mathbf{Y}\\ \star & -\left(\frac{h_U-h_L}{2}\right)Q_1\end{bmatrix}<0, \tag{17}$$

$$\begin{bmatrix}\Xi_1 & \left(\frac{h_U-h_L}{2}\right)\mathbf{X}\\ \star & -\left(\frac{h_U-h_L}{2}\right)Q_1\end{bmatrix}<0, \tag{18}$$

$$\begin{bmatrix}\Xi_2 & \left(\frac{h_U-h_L}{2}\right)\overline{\mathbf{Y}}\\ \star & -\left(\frac{h_U-h_L}{2}\right)Q_2\end{bmatrix}<0, \tag{19}$$

$$\begin{bmatrix}\Xi_2 & \left(\frac{h_U-h_L}{2}\right)\overline{\mathbf{X}}\\ \star & -\left(\frac{h_U-h_L}{2}\right)Q_2\end{bmatrix}<0. \tag{20}$$

Proof.
Let us consider the following Lyapunov-Krasovskii's functional

$$V(t)=\sum_{i=1}^{3}V_i(t) \tag{21}$$

where

$$\begin{aligned}V_1(t)&=e^T(t)R_1e(t)+\int_{t-h(t)}^{t}e^T(s)R_2e(s)ds\\ &+2\sum_{i=1}^{n}\lambda_i\int_0^{e_i(t)}f_i(s)ds\\ V_2(t)&=\int_{t-h_L}^{t}e^T(t)R_3e(s)ds\\ &+\int_{t-\left(\frac{h_U+h_L}{2}\right)}^{t-h_L}\begin{bmatrix}e(s)\\ e\left(s-\left(\frac{h_U-h_L}{2}\right)\right)\end{bmatrix}^T\begin{bmatrix}N_{11} & N_{12}\\ \star & N_{22}\end{bmatrix}\\ &\times\begin{bmatrix}e(s)\\ e\left(s-\left(\frac{h_U-h_L}{2}\right)\right)\end{bmatrix}ds\\ V_3(t)&=\int_{t-\left(\frac{h_U+h_L}{2}\right)}^{t-h_L}\int_s^t\dot{e}^T(u)Q_1\dot{e}(u)duds\\ &+\int_{t-h_U}^{t-\left(\frac{h_U+h_L}{2}\right)}\int_s^t\dot{e}^T(u)Q_2\dot{e}(u)duds\\ &+h_L\int_{t-h_L}^{t}\int_s^t\dot{e}^T(u)Q_3\dot{e}(u)duds\\ &+\int_{t-h_U}^{t-h_L}\int_s^t\dot{e}^T(u)Q_4\dot{e}(u)duds\end{aligned}$$

The upper bounds of time-derivative V_1(t) can be obtained as

$$\begin{aligned}\dot{V}_1(t)&\le 2e^T(t)R_1\dot{e}(t)+e^T(t)R_2e(t)\\ &-(1-h_D)e^T(t-h(t))R_2e(t-h(t))+2f^T(e(t))\Lambda\dot{e}(t).\end{aligned} \tag{22}$$

By calculating the time-derivatives of $V_2(t)$ and $V_3(t)$, we have

$$\dot{V}_2(t)=e^T(t)R_3e(t)-e^T(t-h_L)R_3e(t-h_L)$$
$$+\begin{bmatrix} e(t-h_L) \\ e\left(t-\left(\frac{h_U+h_L}{2}\right)\right)\end{bmatrix}^T\begin{bmatrix} N_{11} & N_{12} \\ \star & N_{22}\end{bmatrix}\begin{bmatrix} e(t-h_L) \\ e\left(t-\left(\frac{h_U+h_L}{2}\right)\right)\end{bmatrix}$$
$$-\begin{bmatrix} e\left(t-\left(\frac{h_U+h_L}{2}\right)\right) \\ e(t-h_U)\end{bmatrix}^T\begin{bmatrix} N_{11} & N_{12} \\ \star & N_{22}\end{bmatrix}\begin{bmatrix} e\left(t-\left(\frac{h_U+h_L}{2}\right)\right) \\ e(t-h_U)\end{bmatrix} \quad (23)$$

$$\dot{V}_3(t)=\left(\frac{h_U-h_L}{2}\right)\dot{e}^T(t)Q_1\dot{e}(t)-\int_{t-\left(\frac{h_U+h_L}{2}\right)}^{t-h_L}\dot{e}^T(s)Q_1\dot{e}(s)ds$$
$$+\left(\frac{h_U-h_L}{2}\right)\dot{e}^T(t)Q_2\dot{e}(t)-\int_{t-h_U}^{t-\left(\frac{h_U+h_L}{2}\right)}\dot{e}^T(s)Q_2\dot{e}(s)ds$$
$$+h_L^2\dot{e}^T(t)Q_3\dot{e}(t)-h_L\int_{t-h_L}^{t}\dot{e}^T(s)Q_3\dot{e}(s)ds$$
$$+\left(\frac{h_U-h_L}{2}\right)\dot{e}^T(t)Q_4\dot{e}(t)-\int_{t-h_U}^{t-h_L}\dot{e}^T(s)Q_4\dot{e}(s)ds \quad (24)$$

Here, by utilizing Lemma 1, the upper bound of integral terms $-h_L\int_{t-h_L}^{t}\dot{e}^T(s)Q_3\dot{e}(s)ds$ and $-\int_{t-h_U}^{t-h_L}\dot{e}^T(s)Q_4\dot{e}(s)ds$ in $\dot{V}_3(t)$ can be obtained as

$$-h_L\int_{t-h_L}^{t}\dot{e}^T(s)Q_3\dot{e}(s)ds$$
$$\le\begin{bmatrix} e(t) \\ e(t-h_L)\end{bmatrix}^T\begin{bmatrix} -Q_3 & Q_3 \\ \star & -Q_3\end{bmatrix}\begin{bmatrix} e(t) \\ e(t-h_L)\end{bmatrix}. \quad (25)$$

$$-\int_{t-h_U}^{t-h_L}\dot{e}^T(s)Q_4\dot{e}(s)ds$$
$$=-\int_{t-\left(\frac{h_U+h_L}{2}\right)}^{t-h_L}\dot{e}^T(s)Q_4\dot{e}(s)ds-\int_{t-h_U}^{t-\left(\frac{h_U+h_L}{2}\right)}\dot{e}^T(s)Q_4\dot{e}(s)ds$$
$$\le\left(\frac{h_U-h_L}{2}\right)^{-1}\begin{bmatrix} e(t-h_L) \\ e\left(t-\left(\frac{h_U+h_L}{2}\right)\right)\end{bmatrix}^T\begin{bmatrix} -Q_4 & Q_4 \\ \star & -Q_4\end{bmatrix}$$
$$\times\begin{bmatrix} e(t-h_L) \\ e\left(t-\left(\frac{h_U+h_L}{2}\right)\right)\end{bmatrix}$$
$$+\left(\frac{h_U-h_L}{2}\right)^{-1}\begin{bmatrix} e\left(t-\left(\frac{h_U+h_L}{2}\right)\right) \\ e(t-h_U)\end{bmatrix}^T\begin{bmatrix} -Q_4 & Q_4 \\ \star & -Q_4\end{bmatrix}$$
$$\times\begin{bmatrix} e\left(t-\left(\frac{h_U+h_L}{2}\right)\right) \\ e(t-h_U)\end{bmatrix}. \quad (26)$$

Using Lemma 2, the upper bounds of other two integral terms $-\int_{t-\left(\frac{h_U+h_L}{2}\right)}^{t-h_L}\dot{e}^T(s)Q_1\dot{e}(s)ds$ and $-\int_{t-h_U}^{t-\left(\frac{h_U+h_L}{2}\right)}\dot{e}^T(s)Q_2\dot{e}(s)ds$ in $\dot{V}_3(t)$ can be estimated as follows respectively.

(i) Case 1: When $h_L\le h(t)\le\frac{h_U+h_L}{2}$, we have

$$-\int_{t-\left(\frac{h_U+h_L}{2}\right)}^{t-h_L}\dot{e}^T(s)Q_1\dot{e}(s)ds$$
$$=-\int_{t-h(t)}^{t-h_L}\dot{e}^T(s)Q_1\dot{e}(s)ds-\int_{t-\left(\frac{h_U+h_L}{2}\right)}^{t-h(t)}\dot{e}^T(s)Q_1\dot{e}(s)ds$$
$$\le(h(t)-h_L)\zeta^T(t)\mathbf{X}Q_1^{-1}\mathbf{X}^T\zeta(t)$$
$$+2\zeta^T(t)\mathbf{X}[e(t-h_L)-e(t-h(t))]$$
$$+\left(\left(\frac{h_U+h_L}{2}\right)-h(t)\right)\zeta^T(t)\mathbf{Y}Q_1^{-1}\mathbf{Y}^T\zeta(t)$$
$$+2\zeta^T(t)\mathbf{Y}\left[e(t-h(t))-e\left(t-\left(\frac{h_U+h_L}{2}\right)\right)\right], \quad (27)$$

$$-\int_{t-h_U}^{t-\left(\frac{h_U+h_L}{2}\right)}\dot{e}^T(s)Q_2\dot{e}(s)ds$$
$$\le\left(\frac{h_U-h_L}{2}\right)^{-1}\begin{bmatrix} e\left(t-\left(\frac{h_U+h_L}{2}\right)\right) \\ e(t-h_U)\end{bmatrix}^T\begin{bmatrix} -Q_2 & Q_2 \\ \star & -Q_2\end{bmatrix}$$
$$\times\begin{bmatrix} e\left(t-\left(\frac{h_U+h_L}{2}\right)\right) \\ e(t-h_U)\end{bmatrix}. \quad (28)$$

Note that $\zeta(t)$, $\boldsymbol{X}$, $\boldsymbol{Y}$, are defined in (16).

To obtain a less conservative results, we add the following zero equations with any matrix P_1 and scalar δ

$$0=2[e^T(t)(\delta P_1)+\dot{e}^T(t)P_1]$$
$$\times[-\dot{e}(t)+Ae(t)-LCe(t-h(t))+B\eta(e(t),y(t))]. \quad (29)$$

From (2) and (7), for any two positive matrices $H_1=diag\{h_{1i},\ldots,h_{1n}\}$, and $H_2=diag\{h_{2i},\ldots,h_{2n}\}$, the following inequalities hold

$$0\le-2\sum_{i=1}^{n}[h_{1i}((f_i(e_i(t))-k_i^-e_i(t))(f_i(e_i(t))-k_i^+e_i(t)))$$
$$+h_{2i}((\eta_i(e_i(t),y_i(t))-k_i^-e_i(t))(\eta_i(e_i(t),y_i(t))-k_i^+e_i(t)))]$$
$$=-2e^T(t)K_1H_1K_2e(t)+2e^T(K_1+K_2)H_1f(e(t))$$
$$-2f^T(e(t))H_1f(e(t))-2e^TK_1H_2K_2e(t)$$
$$+2e^T(t)(K_1+K_2)H_2\eta(e(t),y(t))$$
$$-2\eta^T(e(t),y(t))H_2\eta(e(t),y(t)) \quad (30)$$

where $K_1=diag\{k_1^-,\ldots,k_n^-\}$ and $K_2=diag\{k_1^+,\ldots,k_n^+\}$

Let $Y=P_1L$. From (21)-(30), and by applying S-procedure[16], the $\dot{V}(t)=\sum_{i=1}^{3}\dot{V}_i(t)$ has a new upper bound as

$$\dot{V}\le\zeta^T(t)\Omega_1\zeta(t) \quad (31)$$

where

$$\Omega_1=\Xi_1+(h(t)-h_L)XQ_1^{-1}X^T+\left(\left(\frac{h_U+h_L}{2}\right)-h(t)\right)YQ_1^{-1}Y^T$$

and Ξ_1 is defined in (16). Since

$$(h(t)-h_L)XQ_1^{-1}X^T+\left(\left(\frac{h_U+h_L}{2}\right)-h(t)\right)YQ_1^{-1}Y^T \quad (32)$$

is a convex combination of the matrices $XQ_1^{-1}X^T$ and $YQ_1^{-1}Y^T$ on $h(t)$, $\Omega_1<0$ with the condition $h_L\le h(t)\le\frac{h_U+h_L}{2}$ can be handled by two corresponding boundary LMIs:

$$\Omega_1=\Xi_1+\left(\frac{h_U-h_L}{2}\right)YQ_1^{-1}Y^T<0,(h(t)=h_L) \quad (33)$$

$$\Omega_1 = \Xi_1 + \left(\frac{h_U - h_L}{2}\right)\boldsymbol{X}Q_1^{-1}\boldsymbol{X}^T < 0, \left(h(t) = \frac{h_U + h_L}{2}\right). \quad (34)$$

Using Fact 1, (33) and (34) are equivalent to the LMIs (17) and (18), respectively.

(ii) Case 2: When $\frac{h_U+h_L}{2} \le h(t) \le h_U$, we have

$$-\int_{t-\left(\frac{h_U+h_L}{2}\right)}^{t-h_L} \dot{e}^T(s)Q_1\dot{e}(s)ds$$

$$\le \left(\frac{h_U-h_L}{2}\right)^{-1}\begin{bmatrix} e(t-h_L) \\ e\left(t-\left(\frac{h_U+h_L}{2}\right)\right)\end{bmatrix}^T \begin{bmatrix} -Q_1 & Q_1 \\ \star & -Q_1 \end{bmatrix}$$

$$\times \begin{bmatrix} e(t-h_L) \\ e\left(t-\left(\frac{h_U+h_L}{2}\right)\right)\end{bmatrix}, \quad (35)$$

$$-\int_{t-h_U}^{t-\left(\frac{h_U+h_L}{2}\right)} \dot{e}^T(s)Q_2\dot{e}(s)ds$$

$$= -\int_{t-h(t)}^{t-\left(\frac{h_U+h_L}{2}\right)} \dot{e}^T(s)Q_2\dot{e}(s)ds - \int_{t-h_U}^{t-h(t)} \dot{e}^T(s)Q_2\dot{e}(s)ds$$

$$\le \left(h(t)-\left(\frac{h_U+h_L}{2}\right)\right)\zeta^T(t)\overline{\mathbf{X}}Q_2^{-1}\overline{\mathbf{X}}^T\zeta(t)$$

$$+2\zeta^T(t)\overline{\mathbf{X}}\left[e\left(t-\left(\frac{h_U+h_L}{2}\right)\right)-e(t-h(t))\right]$$

$$+(h_U-h(t))\zeta^T(t)\overline{\mathbf{Y}}Q_2^{-1}\overline{\mathbf{Y}}^T\zeta(t)$$

$$+2\zeta^T(t)\overline{\mathbf{Y}}[e(t-h(t))-e(t-h_U)]. \quad (36)$$

From (21) - (26), (29)-(30), and (35)-(36) when $\frac{h_U+h_L}{2} \le h(t) \le h_U$, the $\dot{V}(t) = \sum_{i=1}^{3}\dot{V}_i(t)$ has a new upper bound as

$$\dot{V} \le \zeta^T(t)\Omega_2\zeta(t) \quad (37)$$

where

$$\Omega_2 = \Xi_2 + \left(h(t)-\left(\frac{h_U+h_L}{2}\right)\right)\overline{\boldsymbol{X}}Q_1^{-1}\overline{\boldsymbol{X}}^T + (h_U-h(t))\overline{\boldsymbol{Y}}Q_1^{-1}\overline{\boldsymbol{Y}}^T \quad (38)$$

and Ξ_2 is defined in (16). By using similar analysis of case 1, $\Omega_2 < 0$ with the condition $\frac{h_U+h_L}{2} \le h(t) \le h_U$ can be handled by two corresponding boundary LMIs:

$$\Omega_2 = \Xi_2 + \left(\frac{h_U-h_L}{2}\right)\overline{\boldsymbol{Y}}Q_1^{-1}\overline{\boldsymbol{Y}}^T < 0, \left(h(t) = \frac{h_U+h_L}{2}\right) \quad (39)$$

$$\Omega_2 = \Xi_2 + \left(\frac{h_U-h_L}{2}\right)\overline{\boldsymbol{X}}Q_1^{-1}\overline{\boldsymbol{X}}^T < 0, (h(t) = h_U). \quad (40)$$

Using Fact 1, (39) and (40) are equivalent to the LMIs (18) and (19), respectively. Therefore, if LMIs (17)-(20) are hold, then the error system is asymptotically stable, which means the chaotic secure communication system (1) with the controller gain $L = P_1^{-1}Y$ is synchronized between the transmitter and receiver. ■

Remark 1. In Eq. (15), the new Lyapunov functional which divided into two intervals $\left[h_L, \frac{h_U+h_L}{2}\right]$ and $\left[\frac{h_U+h_L}{2}, h_U\right]$ are proposed. Therefore, by taking different functional in two sub-intervals $\left[h_L, \frac{h_U+h_L}{2}\right]$ and $\left[\frac{h_U+h_L}{2}, h_U\right]$, the synchronization criterion in Theorem 1 utilizes more information on state variables. Also, by taking different free variables in sub-intervals, Theorem 1 may lead to provide larger delay bounds than the previous ones.

Remark 2. If we do not consider $\int_{t-h(t)}^{t} x^T(s)R_2x(s)ds$ in V_1 of Theorem 1 or set $h_D = 1$, then we can easily obtained a delay-dependent synchronization criterion of the error dynamic system (6) with no delay-derivative information. In other words, the synchronization criterion without $\int_{t-h(t)}^{t} x^T(s)R_2x(s)ds$ or $h_D = 1$ in Theorem 1 do not need the condition $\dot{h}(t) \le h_D$, which is not applicable to Theorem 2 in [5].

4. Numerical Examples

In this section, a simulation example is shown to support the validity and applicability of Theorem 1. Consider the chaotic secure communication system (1) with

$$A = \begin{bmatrix} -6.3 & -6.3 & 0 \\ -0.7 & -0.7 & -7 \\ 0 & 1 & 0 \end{bmatrix}, \ B = \begin{bmatrix} -6.3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \ C = [1 \ 0 \ 0],$$

$$s_o(t) = 0.15\sin(0.1\pi t), \ N = 2,$$

and $f(x) = m_2x + 0.5(m_1 - m_2)(|x+I_0| - |x-I_0|)$, where $m_1 = -1.143, m_2 = -0.714$, $I_0 = 3$. From the considered $f(x)$, we can obtain the following condition $-1.143 \le \frac{f(x)}{x} \le 0$. By applying Theorem 1 to the error dynamic system (6) with $h_L = 0.02$, $h_D = 1$ and $\delta = 3$ and parameters mentioned above, the maximum delay bounds h_U can be obtained as 0.15 and obtained controller gain is $L = [2.6228 \ \ -1.1662 \ -0.2267]^T$. This means that the transmitter and receiver with the obtained controller gain is synchronized for any $h(t)$ which belongs to the interval $[0.2, 0.15]$. Since $|s_o(t)| \le 0.15$, we can choose $\tau = 0.2$. Therefore, the parameters a_1, a_2, a_3 of key signal should be chosen to satisfy $|key_e(t)| \le 0.2$. Let us check the state response of transmitter with $x_0 = [0.15 \ -0.1 \ -0.14]^T$ as shown in Fig. 1. Then, by choosing $a_1 = 0$, $a_2 = 0.1$, $a_2 = 0.1$ and using the results of Fig. 1, the response of $key_e(t)$ can be obtained and shown in Fig. 2. From Fig. 2, we can confirm the obtained $key_e(t)$ is less than 0.2.

To confirm that the synchronization between the transmitter

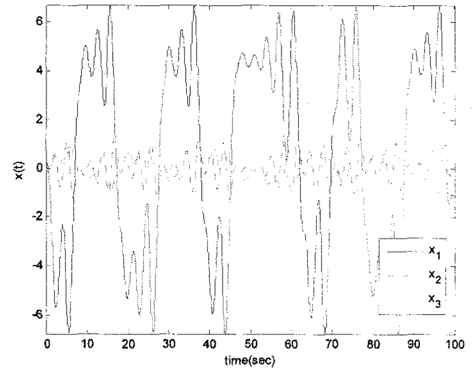


Fig. 1 State responses of the transmitter
그림 1 송신기의 상태 응답

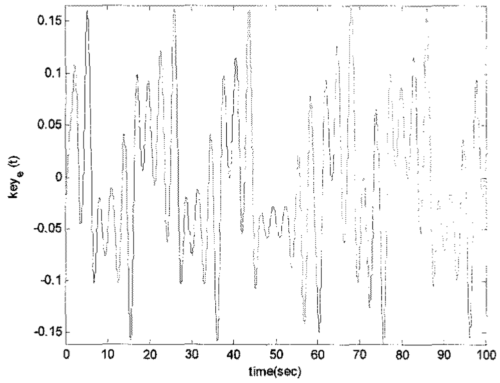


Fig. 2 Responses of key signals in the transmitter
그림 2 송신부의 암호키 신호 응답

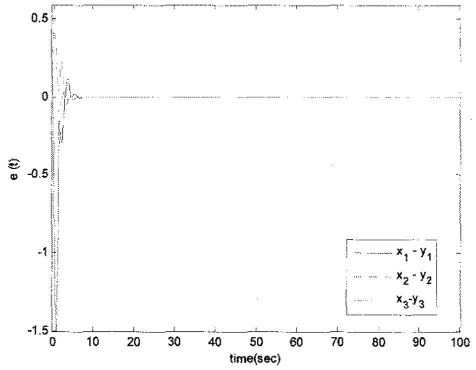


Fig. 3 Responses of error
그림 3 오차응답

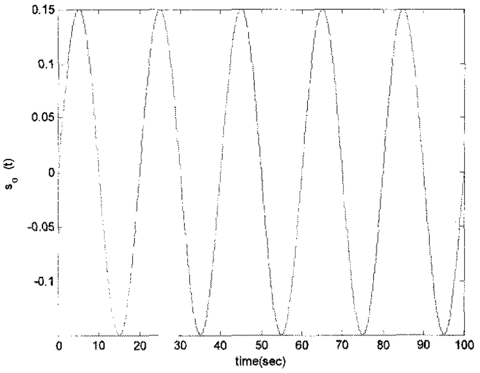


Fig. 4 Responses of the transmitted signal
그림 4 송신부에서 보낸 신호

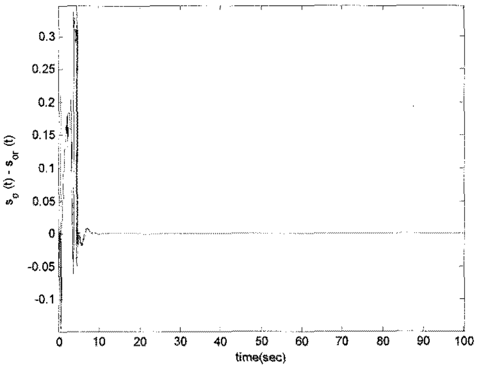


Fig. 5 Error response between the transmitted signal and the recovered signal
그림 5 송신부에서 보낸신호와 수신부에서 받은 신호의 오차 응답

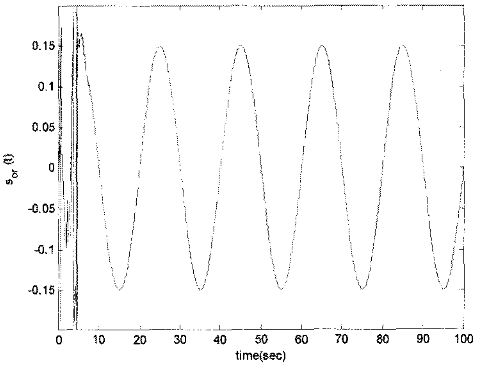


Fig. 6 Responses of the recovered signal
그림 6 수신부에서 복원된 신호

and receiver is achieved with the obtained controller gain $L=[2.6228 \ \ -1.1662 \ \ -0.2267]^T$, the error signal $e(t)$ is shown in Fig. 3 by setting $h(t)=0.02+0.13\sin^2(100t)$ and the initial condition as, $y_0=[0.1 \ \ 0.12 \ \ 0.11]^T$ which is different from the initial condition of the transmitter. From Fig. 3, the error signal goes to zero as time increases. Finally, let us check the recovery of the transmitted signal. From (5) and $key_d(t)=a_1y_1(t)+a_2y_2(t)+a_3y_3(t)$, the recovered $s_{or}(t)$ signal can be obtained. In Fig. 4, Fig, 5 and Fig. 6, the transmitted signal $s_o(t)$, the message error signal $s_0(t)-s_{or}(t)$, and the recovered signal $s_{or}(t)$ are shown, respectively. From these figures, we can confirm that the $s_{or}(t)$ goes to $s_o(t)$ as time increases.

5. Conclusions

In this paper, a new controller design method of the chaotic secure communication systems with interval time-varying delays is proposed. By utilizing LMI framework technique and based on Lyapunov method, a designing method of controller gain L is established. Furthermore, to increase the security of the communication system, the transmitted message is encrypted with the techniques of N-shift cipher and public key. In order to obtain a less conservative result, a new Lyapunov functional was proposed and an integral inequality lemma, which includes free variables, was utilized in obtaining an upper bound of the integral term. Through numerical example, the validity of the proposed method was confirmed. In the future, we will implement the chaotic circuit to examine the proposed synchronization criterion for the chaotic secure communication system.

Acknowledgement

This work was supported by the Korea Research Foundation Grant funded by the Korean Government (KRF-2008-331-D00315)

References

[1] M. Feki, "An adaptive chaos synchronization scheme applied to secure communication", Chaos Solitons & Fractals, vol.18, pp.141-148, 2003.

[2] Z. Li, D. Xu, "A secure communication scheme using projective chaos synchronization", Chaos Solitons & Fractals, vol.22, pp.477-481, 2004.

[3] C.C. Wang, J.P. Su, "A new adaptive variable structure control for chaotic synchronization and secure communication", Chaos Solitons & Fractals, vol.20, pp.967-977, 2004.

[4] T. Yang, C.W. Wu, L.O. Chua, "Crptography based on chaotic system", IEEE Transactions on Circuits and Systems -I: Fundamental Theory and Applications, vol.44, pp.469-472, 1997.

[5] D. Li, Z. Wang, J. Zhou, J. Fang, J. Ni, "A note on chaotic synchronization of time-delay secure communication systems", Chaos Solitons & Fractals, vol.38, pp.1217-1224, 2008.

[6] J. Hale, and S.M.V. Lunel, Introduction to Functional Differential Equatins, Springer-Verlag, New York, 1993.

[7] V.B. Kolmanovskii, and A. Myshkis, Applied Theory to Functional Differential Equations, Kluwer Academic Publishers, Boston, 1992.

[8] J.H. Park, S. Won, "Asymptotic stability of neutral systems with multiple delays", Journal of Optimization Theory and Applications. vol. 103, pp.187-200, 1999.

[9] O.M. Kwon, Ju H. Park, S.M. Lee, "On stability criteria for uncertain delay-differential systems of neutral type with time-varying delays", Applied Mathematics and Computations, vol.197, pp.864-873, 2008.

[10] J.-H. Kim, "Delay and its time-derivative dependent robust stability of time-delayed linear systems with uncertainty", IEEE Transactions on Automatic Control, vol.46, pp.789-792, 2001.

[11] J.-H. Kim, Y.-G. Yi, "Delay-dependent robust stability of uncertain time-delayed linear systems", Trans. KIEE, 55D, pp.147-156, 2006.

[12] O.M. Kwon, and J.H. Park, "An improved delay-dependent robust control for uncertain time-delay systems", IEEE Transactions on Automatic Control, vol. 49, No. 11, pp.1991-1995, 2004.

[13] V.L. Kharitonov, S.-I. Niculescu, "On the stability of linear systems with uncertain delay, IEEE Transactions on Automatic control, vol.48, pp.127-132, 2003.

[14] D. Yue, C. Pang, G.Y. Tang, "Guaranteed cost control of linear systems over networks with state and input quantisations", IEE Proceedings-Control Theory and Applications, vol.153, pp.658-664, 2006.

[15] K. Gu, An integral inequality in the stability problem of time-delay systems, Proceedings of 39th IEEE Conference on Decision and Control, Sydney, Australia, December, 2000.

[16] S. Boyd, L.E. Ghaoui, E. Feron, V. Balakrishnan, Linear Matrix Inequalities in Systems and Control Theory, Philadelphia, SIAM, 1994.

저자소개

권 오 민 (權 五 珉)

1974년 7월 13일생. 1997년 경북대학교 전자공학과 졸업(공학). 2004년 포항공과대학교 전기전자공학부 졸업(공박). 현재 충북대학교 전기공학과 조교수.

Tel : 043-261-2422

Fax : 043-263-2419

E-mail : madwind@chungbuk.ac.kr

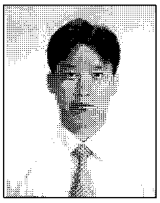
박 주 현 (朴 柱 炫)

1968년 1월 11일생. 1990년 경북대학교 전자공학과 졸업(공학). 1997년 포항공과대학교 전기전자공학부 졸업(공박). 현재 영남대학교 전기공학과 부교수

Tel : 053-810-2491

Fax : 053-810-4767

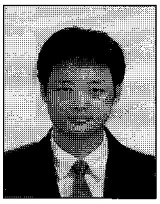
E-mail : jessie@ynu.ac.kr



이 상 문 (李 相 文)

1973년 6월 15일생. 1999년 경북대학교 전자공학과 졸업(공학). 2006년 포항공과대학교 전기전자공학부 졸업(공박). 현재 대구대학교 전자공학부 전임강사.

E-mail : moony@daegu.ac.kr



박 명 진 (朴 明 眞)

1982년 4월 7일생. 2009년 충북대학교 전기공학과 졸업(공학). 현재 충북대학교 전기공학과 석사과정

E-mail : netgauss@chungbuk.ac.kr