مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۴، زمستان ۱۳۹۶، ص ۲۷-۱۷

سنکرون‌سازی آشوب براساس معادلات دیفرانسیل و قضیه تقریب عمومی و کاربرد آن در مخابرات امن و رمزنگاری

محمد حسن مجیدی[1*] و سعید خراشادی‌زاده[2]

۱ و ۲- استادیار، دانشکده برق و کامپیوتر، دانشگاه بیرجند

(دریافت: ۹۵/۱۰/۲۰، پذیرش: ۹۶/۰۵/۰۱)

چکیده

در این مقاله، یک روش جدید به‌منظور سنکرون‌سازی آشوب با استفاده از کنترل غیرخطی ارائه شده است. در اکثر کنترل‌کننده‌های موجود فرض می‌شود مدل ریاضی سامانه‌های آشوبی فرستنده و گیرنده کاملاً یکسان هستند. با توجه به یکسان‌نبودن شرایط محیطی فرستنده و گیرنده و تاثیر درجه حرارت و سایر عوامل بر پارامترهای سامانه آشوبی از قبیل مقادیر مقاومت‌ها و سایر اجزا، یکسان درنظرگرفتن مدل‌های فرستنده و گیرنده معقول نیست. در این مقاله، روش جدیدی برای تخمین عدم قطعیت‌ها ارائه شده است که در آن عدم قطعیت‌ها با یک معادله دیفرانسیل خطی با ضرایب نامعلوم ثابت مدل‌سازی می‌شود. به عبارت دیگر، عدم قطعیت‌ها را می‌توان به‌صورت پاسخ این معادله دیفرانسیل نمایش داد. با توجه به این‌که این تابع (پاسخ معادله دیفرانسیل) شرایط قضیه تقریب عمومی را دارد، می‌توان هر تابع غیرخطی را با دقت دلخواه تخمین زد، اما با توجه به این‌که ضرایب معادله دیفرانسیل نامعلوم می‌باشند، پارامترهای این تابع نیز نامعلوم بوده و باید تخمین زده شوند. این‌کار با استفاده از قوانین تطبیق به‌دست‌آمده از تحلیل همگرایی خطای سنکرون‌سازی انجام می‌گردد. نتایج شبیه‌سازی بیانگر عملکرد مناسب تخمین‌گر ارائه شده بوده و در مقایسه با کنترل‌کننده فازی مد لغزشی، سرعت پاسخ کنترل‌کننده پیشنهادی بهتر می‌باشد. همچنین، کاربرد آن در مخابرات امن و رمزنگاری مورد بررسی قرار گرفته است.

واژه‌های کلیدی: سنکرون‌سازی آشوب، مخابرات امن، رمزنگاری، معادلات دیفرانسیل، قضیه تقریب عمومی

۱- مقدمه

مخابرات امن، کاربردهای نظامی بسیاری دارد و به همین دلیل در دهه‌های گذشته تحقیقات فراوانی پیرامون آن صورت گرفته است. منظور از مخابرات امن، ارسال امن اطلاعات بین فرستنده وگیرنده است، به طوری‌که سایر افراد به آن اطلاعات دسترسی نداشته باشند [۱]. با توجه به ویژگی‌های سامانه‌های آشوبی ازجمله تصادفی‌بودن، غیرقابل تناوبی‌بودن، حساسیت به شرایط اولیه و غیرقابل پیش‌بینی بودن، این سامانه‌ها نقش مهمی در مخابرات امن و رمزنگاری ایفا می‌کنند [۳-۲]. ایده استفاده از سامانه‌های آشوبی برای مخابرات امن به این صورت است که دو سامانه فرستنده (درایو) و گیرنده (پاسخ) توسط یک سیگنال درایو مشترک با یکدیگر کوپل شده‌اند که در صورت سنکرون‌بودن سیگنال‌های آشوبی فرستنده و گیرنده، سیگنال پیام با دقت خوبی آشکارسازی خواهد شد. روش‌های مخابرات امن آشوبی را می‌توان به انواع ماسک‌زدن آشوبی، مدولاسیون آشوبی و سوییچینگ آشوبی تقسیم‌بندی نمود. در روش اول، سیگنال پیام محرمانه فقط با سیگنال کریر آشوبی جمع می‌شود [۵-۴]. در روش دوم، نه نتها سیگنال پیام با سیگنال کریر آشوبی جمع می‌شود بلکه حالت‌های سامانه آشوبی توسط سیگنال پیام از طریق یک روند معکوس‌پذیر مدوله می‌گردند به‌نحوی‌که سیگنال آشوبی تولیدشده ذاتاً شامل اطلاعات سیگنال پیام است [۷-۶]. در روش سوم، نیازمند دو سامانه آشوبی برای تولید بیت‌های صفر و یک هستیم. سیگنال ارسالی توسط سوییچ بین این دو سامانه آشوبی براساس این‌که صفر یا یک سیگنال پیام منتقل می‌گردد انتخاب می‌شود [۹-۸]. همه این سامانه‌های مخابراتی امن آشوبی که اشاره شد برمبنای سنکرون‌سازی هستند. سنکرون‌سازی این سیگنال‌ها توسط کنترل‌کننده یا رویتگر[1] موجود در گیرنده انجام می‌شود [۴].

سنکرون‌سازی سامانه‌های آشوبی به منظور طراحی سامانه‌های مخابراتی امن، یکی از محبوب‌ترین حوزه‌های تحقیقاتی محسوب می‌شود و روش‌های بسیار زیادی ابداع شده است. در [۱۰]، از روش‌های کنترل بهینه برای همزمان‌سازی سامانه‌های آشوب استفاده شده است. با توجه به این‌که الگوریتم‌های کنترل بهینه برای

* رایانامه نویسنده مسئول: m.majidi@birjand.ac.ir

1- Observer

سامانه‌های خطی ارائه شده‌اند، سامانه‌های غیرخطی به فرم خطی نمایش داده شده‌اند. به عنوان نمونه‌ای از کنترل‌کننده‌های کلاسیک آشوب می‌توان به [۱۱] اشاره نمود که یک کنترل‌کننده PD برای سنکرون‌سازی سامانه آشوبی لور طراحی کرده است. در [۱۲] یک روش سیستماتیک برای سنکرون‌سازی دو سامانه آشوب لورنز براساس یک کنترل‌کننده مود لغزشی پیشنهاد شده است. به طور مشابه، در [۱۳] یک کنترل‌کننده مود لغزشی قوی برای تحقق-بخشیدن سنکرون‌سازی بین سه زوج متفاوت سامانه‌های آشوب (لورنز- شن، شن- لورنز، لین- لورنز) پیشنهاد شده است. سنکرون-سازی مقاوم سامانه‌های آشوبی با استفاده از کنترل مود لغزشی در [۱۴] ارائه شده است. روش‌هایی برای مقابله با عدم قطعیت پارامتری و ساختاری در سنکرون‌سازی مقاوم با استفاده از کنترل مود لغزشی در [۱۵] پیشنهاد شده است.

راه‌برد دیگر در سنکرون‌سازی سامانه‌های آشوبی، طراحی رویتگر حالت می‌باشد. چنان‌چه حالت‌های رویتگر با حالت‌های فرستنده سنکرون شود، می‌توان سیگنال پیام را با استفاده از رمزگشا در گیرنده به‌دست آورد. مزیت این راه‌برد نسبت به راه‌برد طراحی کنترلر آن است که فقط یکی از حالت‌های سامانه فرستنده باید ارسال شود. سایر حالت‌ها در گیرنده توسط رویتگر حالت تخمین زده می‌شوند. رویتگرهای بسیاری در این زمینه ارائه شده است [۲۲-۱۶]. ازجمله در [۱۶] یک رویتگر تطبیقی با استفاده از شبکه‌های عصبی طراحی شده است و سپس یک کنترل‌کننده مود لغزشی برای سنکرون‌سازی سامانه‌های آشوبی طراحی گردیده است. در [۱۸] فرض شده است سامانه‌های آشوبی فرستنده و گیرنده دو سامانه کاملاً مختلف هستند و سنکرون‌سازی آن‌ها با استفاده از طراحی رویتگر انجام شده است. در [۱۹] رویتگر غیرخطی با کاهش مرتبه طراحی شده است.

از سامانه‌های فازی و شبکه‌های عصبی به‌عنوان الگوریتم‌های هوشمند در سنکرون‌سازی سامانه‌های آشوبی بسیار استفاده شده است [۲۶-۲۳]. دو ویژگی مهم سامانه‌های عصبی- فازی که منجر به استفاده گسترده از آن‌ها در طراحی کنترل‌کننده شده است، عبارتند از: ویژگی تقریب عمومی و خطی‌بودن نسبت به پارامترها [۲۷]. سامانه‌های فازی با توابع تعلق گوسی و برخی شبکه‌های عصبی مانند MLP و RBFN شرایط قضیه تقریب عمومی را برآورده می‌کنند و می‌توانند برای تخمین توابع غیرخطی با دقت دلخواه به‌کار گرفته شوند [۳۱-۲۸]. همچنین، خروجی این سامانه‌ها نسبت به برخی از پارامترها خطی است که منجر به ساده‌ترشدن اثبات پایداری سامانه می‌شود. از دیگر نقاط قوت شبکه‌های عصبی و سامانه‌های فازی می‌توان به قابلیت یادگیری سریع، پردازش موازی و عدم نیاز به مدل ریاضی دقیق سامانه‌ها اشاره نمود.

اما باید توجه داشت سامانه‌های فازی و شبکه‌های عصبی در کنار مزایایی که دارند، طراحی تخمین‌گر را با چالش‌هایی نیز روبرو می‌کنند. گاهی اوقات طراحی یک کنترل‌کننده فازی خوب برای سامانه‌های پیچیده، نیازمند دانش افراد خبره می‌باشد تا بتوان قوانین فازی مناسبی سامانه تعریف کرد. علاوه‌بر این، سامانه‌های فازی و شبکه‌های عصبی پارامترهای تنظیم زیادی از قبیل تعداد قوانین فازی، نوع توابع تعلق، تعداد لایه‌های شبکه عصبی، نوع توابع فعال‌ساز شبکه عصبی، نرخ همگرایی پارامترهای آزاد، مرکز توابع تعلق فازی و ... دارند [۳۲]. تعیین مقدار مناسب این پارامترها به روش سعی و خطا انجام می‌شود که معمولاً وقت‌گیر است. ممکن است از الگوریتم‌های بهینه‌سازی مانند الگوریتم ژنتیک و پرندگان و غیره برای تعیین مقدار بهینه این پارامترها استفاده شود [۳۳]. اما در عمل، با اغتشاش خارجی مواجه هستیم که مقدار آن نامعلوم است و نمی‌تواند در بهینه‌سازی درنظر گرفته شود. البته برخی از این پارامترها را می‌توان با استفاده از قوانین تطبیق که از اثبات پایداری سامانه به‌دست می‌آیند، به طور خودکار تنظیم نمود، اما این ایده نیز پارامترهای دیگری ازجمله ضریب همگرایی پارامترهای تطبیقی و همچنین مقدار اولیه آن‌ها را به مسئله اضافه می‌کند.

روش‌های تخمین توابع غیرخطی محدود به سامانه‌های فازی و شبکه‌های عصبی نیست. در سال‌های اخیر، کاربردهایی از سری فوریه و چندجمله‌ای‌های لژاندر[1] به‌عنوان جایگزین سامانه‌های فازی و شبکه‌های‌عصبی در سامانه‌های کنترل ارائه شده است. این توابع نیز شرایط قضیه تقریب عمومی [۳۱] را برآورده می‌کنند و می‌توانند برای تخمین عدم‌قطعیت‌ها در سامانه‌های کنترل به کار گرفته شوند. مزیت سری فوریه و چندجمله‌ای‌های لژاندر نسبت به سامانه‌های فازی و شبکه‌های عصبی، کمتربودن تعداد پارامترهای تنظیم آن‌ها می‌باشد. در سری فوریه، ضرایب سری و دوره تناوب اساسی آن پارامترهای تنظیم بوده و در چندجمله‌ای‌های لژاندر ضرایب چندجمله‌ای پارامترهای آزاد تخمین‌گر می‌باشند. مشابه پارامترهای سامانه‌های فازی و شبکه‌های عصبی، می‌توان برای ضرایب سری فوریه و ضرایب چندجمله‌ای‌های لژاندر قوانین تطبیق طراحی نمود [۳۸-۳۴].

در این مقاله، نوع دیگری از تخمین‌گرهای تطبیقی مبتنی بر تقریب توابع ارائه می شود. فرض کنید یک معادله دیفرانسیل خطی با ضرایب نامعلوم وجود دارد که عدم قطعیت مدل‌های فرستنده وگیرنده تقریباً با پاسخ آن برابر باشد [۳۹]. می‌توان نشان داد که

[1] Legendre

این پاسخ، ویژگی‌های مطرح‌شده در قضیه تقریب عمومی را دارد. بنابراین، عدم‌قطعیت با پاسخ معادله دیفرانسیل مدل‌سازی شده و تخمین زده می‌شود. کنترل‌کننده از این تخمین برای بهبود خطای سنکرون‌سازی استفاده می‌کند. همچنین، برای جبران خطای مدل‌سازی معادلات دیفرانسیل، از الگوریتم‌های کنترل مقاوم، استفاده می شود.

ساختار مقاله پیش رو بدین صورت می‌باشد. در بخش ۲ ساختار سامانه‌های آشوبی فرستنده و گیرنده معرفی می‌گردد. تخمین‌گر پیشنهادی و قضیه تقریب عمومی در بخش ۳ ارائه می‌شود. در بخش ۴، به طراحی کنترل‌کننده پرداخته و معادلات آن بیان می‌شود. اثبات سنکرون‌سازی به کمک تئوری پایداری لیاپانوف در بخش ۵، انجام می‌شود. در بخش ۶، سامانه مخابراتی توضیح داده شده و کاربرد آن در مخابرات امن و رمزنگاری به همراه نتایج شبیه‌سازی ارائه می‌شود. در بخش پایانی نتیجه‌گیری بیان خواهد شد.

۲- سامانه‌های آشوبی فرستنده و گیرنده

فرض کنید سامانه آشوبی فرستنده، یک اسیلاتور لورنز به صورت زیر باشد:

$$\begin{aligned}\dot{x}_1 &= a_1(x_2 - x_1)\\ \dot{x}_2 &= b_1 x_1 - x_1 x_3 - x_2\\ \dot{x}_3 &= x_1 x_2 - c_1 x_3\end{aligned} \quad (۱)$$

همچنین فرض کنید سامانه آشوبی گیرنده، یک مدار آشوبی چن [۴۰] به صورت زیر باشد:

$$\begin{aligned}\dot{y}_1 &= a_2(y_2 - y_1) + u_1\\ \dot{y}_2 &= (b_2 - a_2)y_1 - y_1 y_3 + b_2 y_2 + u_2\\ \dot{y}_3 &= y_1 y_2 - c_2 y_3 + u_3\end{aligned} \quad (۲)$$

که در آن، u_1، u_2 و u_3 سیگنال‌های کنترل هستند. پارامترهای سامانه لورنز به صورت $a_1 = 10, b_1 = 28$ و $c_1 = 8/3$ و پارامترهای سامانه چن به صورت $a_2 = 35, b_2 = 28$ و $c_2 = 3$ تنظیم شده‌اند. بردار حالت فرستده به‌صورت $X = [x_1 \quad x_2 \quad x_3]^T$ تعریف می شود. بنابراین، (۱) به صورت زیر در می‌آید:

$$\begin{aligned}\dot{X} &= AX + f(X)\\ A &= \begin{bmatrix}-a_1 & a_1 & 0\\ b_1 & -1 & 0\\ 0 & 0 & -c_1\end{bmatrix}, f(X) = \begin{bmatrix}0\\ -x_1 x_3\\ x_1 x_2\end{bmatrix}\end{aligned} \quad (۳)$$

بردار حالت گیرنده به‌صورت $Y = [y_1 \quad y_2 \quad y_3]^T$ تعریف می‌شود. بنابراین، (۲) به صورت زیر در می‌آید:

$$\begin{aligned}\dot{Y} &= (A + \Delta A)Y + f(Y) + Bu\\ \Delta A &= \begin{bmatrix}-(a_2 - a_1) & (a_2 - a_1) & 0\\ b_2 - b_1 - a_2 & b_2 + 1 & 0\\ 0 & 0 & -(c_2 - c_1)\end{bmatrix},\\ u &= \begin{bmatrix}u_1\\ u_2\\ u_3\end{bmatrix}, f(Y) = \begin{bmatrix}0\\ -y_1 y_3\\ y_1 y_2\end{bmatrix}, B = I_3,\end{aligned} \quad (۴)$$

خطای سنکرون‌سازی به صورت $E = Y - X$ تعریف می‌شود. در این صورت، خواهیم داشت:

$$\dot{E} = AE + (\Delta A)Y + f(Y) - f(X) + Bu \quad (۵)$$

۳- معادلات دیفرانسیل و قضیه تقریب عمومی

فرض کنید می‌خواهیم تابع نامعلوم $\delta(t)$ را تخمین بزنیم. معادله دیفرانسیل خطی زیر را درنظر بگیرید:

$$\delta^{(p)} - \sum_{j=1}^{p} b_j \delta^{(p-j)} = 0 \quad (۶)$$

که در آن، p مرتبه معادله دیفرانسیل و b_j ضریب آن می‌باشد. به‌عبارت دیگر، فرض کرده‌ایم که یک معادله دیفرانسیل به فرم (۶) وجود دارد که $\delta(t)$ پاسخ آن است. با توجه با این‌که $\delta(t)$ را نامعلوم فرض کرده‌ایم، ضرایب b_j نیز نامعلوم هستند. می‌دانیم پاسخ این معادله را می‌توان به صورت زیر نوشت:

$$\delta(t) = \sum_{i=1}^{p} c_i e^{\lambda_i t} Cos\left(\omega_i t + \theta_i\right) \quad (۷)$$

که در آن، ضرایب نامعلوم c_i، λ_i، ω_i و θ_i به مقادیر b_j و ریشه‌های معادله مشخصه بستگی دارد. می‌توان نشان داد که این پاسخ شرایط قضیه استون- وایرشتراس[1] را برآورده میکند و می‌تواند به‌عنوان تخمین‌گر توابع غیرخطی استفاده شود.

قضیه استون- وایرشتراس [۲۹]

فرض کنید Ω مجموعه توابع پیوسته روی مجموعه محدب T باشد. اگر:

۱- مجموعه Ω نسبت به ضرب اسکالر، جمع و ضرب بسته باشد.

۲- مجموعه Ω نقاط T را جدا کند، یعنی

$$\forall t_1, t_2 \in T, t_1 \neq t_2, \exists \delta(t) \in \Omega: \delta(t_1) \neq \delta(t_2) \quad (۸)$$

۳- در مجموعه Ω در هیچ نقطه‌ای از T محو نشود، یعنی

$$\forall t \in T, \exists \delta(t) \in \Omega: \delta(t) \neq 0 \quad (۹)$$

1- Stone Weierstrass

آن‌گاه به‌ازای هر تابع حقیقی پیوسته $\delta(t)$ روی T و $\varepsilon > 0$ وجود دارد تابعی مانند f در Ω به‌طوری‌که:

$$\sup_{t\in T} |f(t)-\delta(t)| < \varepsilon \qquad (۱۰)$$

در نامساوی فوق، $\varepsilon > 0$ یک عدد دلخواه کوچک است که بیان‌گر خطای تقریب است. میتوان نشان داد توابعی به فرم $\sum_{i=1}^{p} c_i e^{\lambda_i t} Cos\left(\omega_i t + \theta_i\right)$ شرایط فوق را برآورده می‌کنند [۳۹].

۴- کنترل‌کننده پیشنهادی

قانون کنترل زیر را درنظر بگیرید:

$$u = -k^T E - \hat{F} - u_r \qquad (۱۱)$$

که در آن، k ماتریس بهره‌های کنترلی است که به روش جایابی قطب تعیین می‌شود به‌طوری‌که قطب‌های $A_c = A - Bk$ در محل‌های مطلوب قرار گیرند. همچنین $\hat{F}$ بیانگر تخمین بردار عدم قطعیت $F(t) = (\Delta A)Y + f(Y) - f(X)$ که در (۵) ظاهر شده است.

در قانون کنترل فوق، u_r برای جبران خطای مدل‌سازی عدم قطعیت با معادله دیفرانسیل درنظر گرفته شده است. برای سادگی فرض کنید معادله دیفرانسیل درنظر گرفته‌شده برای تخمین $F(t)$ از مرتبه $p = 2$ باشد. بنابراین، تابع $\hat{F}$ به فرم زیر می‌باشد:

$$\hat{F} = \varphi \hat{C} \qquad (۱۲)$$

به‌طوری‌که:

$$\begin{gathered} \varphi = \begin{bmatrix} \varphi_1 & 0 & 0 \\ 0 & \varphi_2 & 0 \\ 0 & 0 & \varphi_3 \end{bmatrix} \\ \varphi_i = \begin{bmatrix} e^{-\lambda_{1i} t} Cos(\omega t + \theta_{1i}) & e^{-\lambda_{2i} t} Cos(\omega t + \theta_{2i}) \end{bmatrix}^T \\ \hat{C} = \begin{bmatrix} \hat{C}_1^T & \hat{C}_2^T & \hat{C}_3^T \end{bmatrix}^T \\ \hat{C}_i = \begin{bmatrix} \hat{c}_{1i} & \hat{c}_{2i} \end{bmatrix} \end{gathered} \qquad (۱۳)$$

که در روابط فوق، $i = 1,2,3$ می‌باشد. ضرایب $\hat{C}_i$ نامعلوم بوده و توسط قانون تطبیق که در بخش بعد تخمین زده می‌شود. با جایگذاری قانون کنترل (۱۱) در معادله (۵) سامانه حلقه بسته زیر به‌دست می‌آید:

$$\dot{E} = AE + B(-kE - \hat{F} - u_r) + F(t) \qquad (۱۴)$$

که در آن، $F(t) = f(Y) - f(X) + (\Delta A)Y$ عدم قطعیت مجتمع می‌باشد. فرض کنید $F(t)$ توسط تخمین‌گر معرفی‌شده به‌صورت زیر تقریب زده شود:

$$F(t) = \varphi C^* + \Delta(t) \qquad (۱۵)$$

که در آن، C^* مقدار بهینه کران‌دار برای $\hat{C}$ بوده که منجر به خطای تقریب مینیمم (خطای مدل‌سازی) $\Delta(t)$ می‌شود. در واقع عبارت u_r در معادله (۱۷) برای جبران‌سازی خطای مدل‌سازی $\Delta(t)$ اضافه شده است. فرض می‌شود کران بالای $\Delta(t)$ به صورت $\|\Delta(t)\| \le \rho$ باشد که ρ مقدار ثابت معلوم می باشد. با توجه به معادلات (۱۲) و (۱۵) و با استفاده از تعریف $A_c = A - Bk$ معادله (۱۴) به صورت زیر بازنویسی می شود:

$$\dot{E} = A_c E + B(\varphi \tilde{C} - u_r + \Delta(t)) \qquad (۱۶)$$

که در آن، $\tilde{C} = C^* - \hat{C}$ می‌باشد. با توجه به این‌که C^* ثابت است، خواهیم داشت: $\dot{\tilde{C}} = -\dot{\hat{C}}$

۵- اثبات سنکرون‌سازی روش پیشنهادی

برای این‌که نشان دهیم سنکرون‌ساز پیشنهادی قادر است خطای سنکرون‌سازی را به صفر برساند، تابع لیاپانوف را به‌صورت زیر درنظر بگیرید:

$$V = \frac{1}{2} E^T P E + \frac{1}{2\gamma} \tilde{C}^T \tilde{C} \qquad (۱۷)$$

که در آن، P یک ماتریس مثبت معین متقارن است که در معادله زیر صدق می‌کند [۴۱]:

$$A_c^T P + P A_c = -Q \qquad (۱۸)$$

که در آن، Q یک ماتریس مثبت معین است که توسط طراح تعیین می‌شود و γ یک ثابت مثبت است. انتخاب تابع لیاپانوف با توجه به هدف مسئله انجام می‌شود. در این‌جا هدف آن است که خطای سنکرون‌سازی صفر شود و ضرایب $\hat{C}$ به سمت ضرایب واقعی C^* همگرا شوند. به عبارت دیگر، هدف آن است که بردارهای E و $\tilde{C}$ به صفر همگرا شوند. طبق قضیه پایداری لیاپانوف برای سامانه‌های غیرخطی، باید یک تابع مثبت معین مانند V از بردارهای E و $\tilde{C}$ درنظر بگیریم. این تابع باید به‌گونه‌ای باشد که تنها در مبدا صفر باشد. یعنی تنها اگر E و $\tilde{C}$ صفر باشند مقدار آن تابع نیز صفر شود. اگر بتوانیم نشان دهیم مشتق زمانی این تابع

منفی است آن‌گاه می‌توان نتیجه گرفت با گذشت زمان تابع V کاهش می‌یابد و چون مثبت است به صفر خواهد رسید. به عبارت دیگر، E و $\tilde{C}$ صفر خواهند شد. مشتق تابع لیاپانوف نسبت به زمان برابر است با:

$$\dot{V}=\frac{1}{2}(\dot{E}^T PE+E^T P\dot{E})-\frac{1}{\gamma}\tilde{C}^T\dot{\hat{C}} \qquad (۱۹)$$

با جایگذاری $\dot{E}$ از (۱۶) در (۱۹) خواهیم داشت:

$$\begin{aligned}\dot{V}=&\frac{1}{2}(E^T A_c{}^T+\tilde{C}^T\varphi^T-u_r{}^T+\Delta^T)PE\\&+\frac{1}{2}E^T P(A_c E+\varphi\tilde{C}-u_r+\Delta)-\frac{1}{\gamma}\tilde{C}^T\dot{\hat{C}}\end{aligned} \qquad (۲۰)$$

با توجه به این‌که V و $\dot{V}$ اسکالر هستند و ماتریس P متقارن است، می‌توان گفت:

$$\begin{aligned}&\tilde{C}^T\varphi^T PE=E^T P\varphi\tilde{C}\\&(\Delta^T-u_r{}^T)PE=E^T P(\Delta-u_r)\end{aligned}.$$

بنابراین، (۲۰) به صورت زیر ساده می‌شود:

$$\begin{aligned}\dot{V}=&\frac{1}{2}E^T(A_c{}^T P+PA_c)E+\tilde{C}^T\varphi^T PE\\&+E^T P(\Delta-u_r)-\frac{1}{\gamma}\tilde{C}^T\dot{\hat{C}}\end{aligned} \qquad (۲۱)$$

با استفاده از (۱۸) خواهیم داشت:

$$\begin{aligned}\dot{V}=&-\frac{1}{2}E^T QE+\tilde{C}^T\varphi^T PE\\&+E^T P(\Delta-u_r)-\frac{1}{\gamma}\tilde{C}^T\dot{\hat{C}}\end{aligned} \qquad (۲۲)$$

فرض کنید:

$$\dot{\hat{C}}=\gamma\varphi^T PE \qquad (۲۳)$$

بنابراین، (۲۲) می‌تواند به صورت زیر بازنویسی شود:

$$\dot{V}=-\frac{1}{2}E^T QE+E^T P(\Delta-u_r) \qquad (۲۴)$$

اگر u_r را طوری انتخاب کنیم که

$$E^T P(\Delta(t)-u_r)\le 0 \qquad (۲۵)$$

شرط $\dot{V}\le 0$ محقق خواهد شد. حال فرض کنید:

$$u_r=\rho sign(E^T P) \qquad (۲۶)$$

که در آن، $sign(.)$ تابع علامت می‌باشد. نشان می‌دهیم این تابع می‌تواند نامساوی (۲۵) را محقق کند. با جایگذاری (۲۶) در (۲۵) خواهیم داشت:

$$E^T P\Delta(t)-E^T P\rho sign(E^T P)\le 0 \qquad (۲۷)$$

می‌دانیم $E^T P\rho sign(E^T P)=\rho\left\|E^T P\right\|$. بنابراین، خواهیم داشت:

$$E^T P\Delta(t)-\rho\left\|E^T P\right\|\le 0 \qquad (۲۸)$$

به عبارت دیگر، باید نشان دهیم $E^T P\Delta(t)\le\rho\left\|E^T P\right\|$. اگر بتوانیم نشان دهیم $\left\|E^T P\Delta(t)\right\|\le\rho\left\|E^T P\right\|$ آن‌گاه مطمئناً نامساوی (۲۸) نیز برقرار خواهد بود. بنابراین، باید نشان دهیم نامساوی زیر صادق است:

$$\left\|E^T P\right\|\left\|\Delta(t)\right\|-\rho\left\|E^T P\right\|\le 0 \qquad (۲۹)$$

به عبارت دیگر، باید داشته باشیم

$$\left\|E^T P\right\|\left(\left\|\Delta(t)\right\|-\rho\right)\le 0 \qquad (۳۰)$$

با توجه به فرض $\left\|\Delta(t)\right\|\le\rho$ نامساوی فوق همواره برقرار خواهد بود و $\dot{V}$ منفی خواهد شد. درنتیجه، E، $\tilde{C}$ و $\hat{C}$ کران‌دار خواهند بود. بنابراین، می‌توان نتیجه گرفت که $\dot{E}$ در (۱۶) و قانون کنترل (۱۱) کران‌دار است. همچنین، منفی‌بودن $\dot{V}$ بیانگر آن است که:

$$V(\tilde{\theta}(t),E(t))\le V(\tilde{\theta}(0),E(0)) \qquad (۳۱)$$

برای اثبات صفرشدن خطای سنکرون‌سازی از لم باربالات استفاده می‌شود.

لم باربالات[۴۱]: اگر حد تابع $f(t)$ در $t\to\infty$ محدود باشد و $\dot{f}(t)$ پیوسته یکنواخت باشد ($\ddot{f}(t)$ کران‌دار باشد)، آن‌گاه در $t\to\infty$ خواهیم داشت: $\dot{f}(t)\to 0$

برای استفاده از لم باربالات، تابع زیر را تعریف می‌کنیم:

$$\Omega(t)=0.5E^T QE \qquad (۳۲)$$

روشن است که

$$\Omega(t)\le -\dot{V} \qquad (۳۳)$$

اگر از طرفین (۳۳) انتگرال بگیریم خواهیم داشت:

$$\int_0^t\Omega(\tau)d\tau\le V(\tilde{C}(0),E(0))-V(\tilde{C}(t),E(t)) \qquad (۳۴)$$

با توجه به این‌که $V(\tilde{C}(0),E(0))$ کران‌دار است و

$V(\tilde{C}(t),E(t))$ کاهشی و کران‌دار است، نتیجه زیر به‌دست می‌آید:

$$\lim_{t\to\infty}\int_0^t \Omega(\tau)d\tau \le \infty \qquad (۳۵)$$

با توجه به این‌که $\dot{E}$ کراندار است می‌توان گفت $\dot{\Omega}(t)=\dot{E}^T QE$ نیز کران‌دار است. اکنون، تابع $f(t)$ در لم باربالات را به صورت زیر درنظر بگیرید:

$$f(t)=\int_0^t \Omega(\tau)d\tau \qquad (۳۶)$$

با توجه به (۳۵) روشن است که حد $f(t)$ در بی‌نهایت کران‌دار است. همچنین، روشن است که:

$$\ddot{f}(t)=\dot{\Omega}(t)=\dot{E}^T QE \qquad (۳۷)$$

نیز کراندار است. زیرا نشان دادیم $\dot{E}$ و E کران‌دارند. بنابراین، شرایط لم باربالات برقرار است که نشان می‌دهد در $t\to\infty$ خواهیم داشت: $\dot{f}(t)=\Omega(t)\to 0$. با توجه به تعریف $\Omega(t)$ در (۳۲)، می‌توان نتیجه گرفت با گذشت زمان، خطای سنکرون‌سازی به صفر همگرا می‌شود.

۶- نتایج شبیه‌سازی

در این بخش روش پیشنهادی شبیه‌سازی گردیده و با کنترل‌کننده مود لغزشی مقایسه خواهد شد. همچنین، کاربرد روش پیشنهادی در مخابرات امن و رمزنگاری مورد بررسی قرار می‌گیرد.

۶-۱- شبیه‌سازی روش پیشنهادی

سامانه‌های آشوبی فرستنده و گیرنده را مطابق (۱) و (۲) درنظر بگیرید. مقادیر انتخابی برای ماتریس‌ها به نحوی است که سامانه‌های فوق شرایط آشوب را خواهند داشت [۴۲]. فرض کنید شرایط اولیه به‌صورت $X(0)=[10\ \ 10\ \ 10]^T$ و $Y(0)=[2\ \ 2\ \ 2]^T$ باشند [۴۲]. همچنین، فرض کنید بخواهیم با انتخاب k مقادیر ویژه سامانه حلقه بسته را در $[-40\ \ -62\ \ -64]$ قرار دهیم. با اجرای دستور:

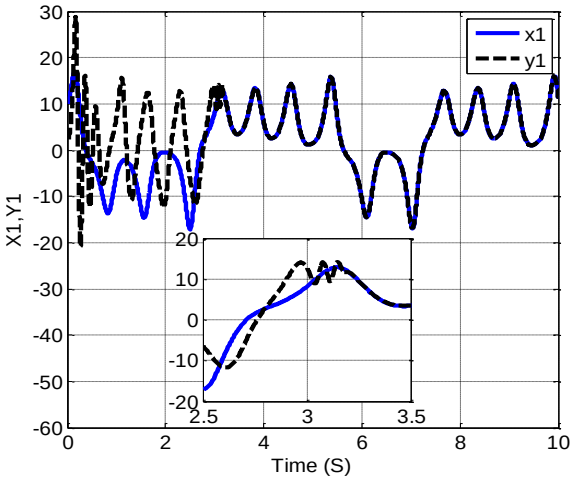
$$k=place(A,B,[-64\ \ -62\ \ -40]) \qquad (۳۸)$$

در Matlab خواهیم داشت:

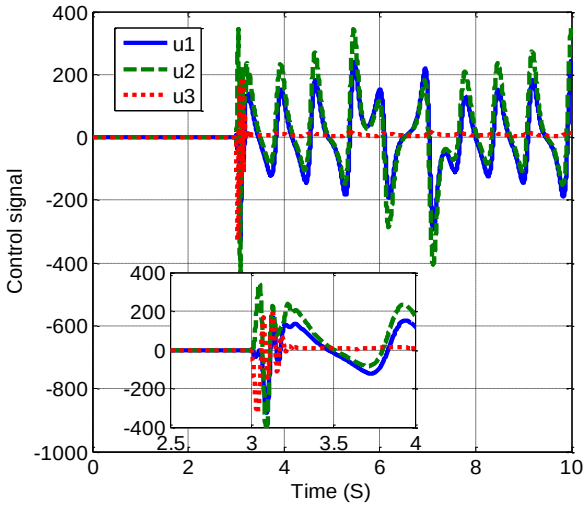
$$k=\begin{bmatrix}54 & 10 & 0\\ 28 & 61 & 0\\ 0 & 0 & 37.33\end{bmatrix} \qquad (۳۹)$$

اگر مقادیر ویژه به مبدا نزدیکتر شوند، عناصر ماتریس فوق کوچکتر می‌شوند که موجب افزایش خطا می‌شود.

عملکرد سنکرون‌سازی روش پیشنهادی در همزمان‌نمودن اولین متغیر حالت در شکل (۱) نشان داده شده است. تا قبل از اعمال کنترل‌کننده ($t=3S$)، سیگنال‌ها همزمان نیستند. اما بعد از اعمال سیگنال کنترل، متغیرهای حالت به سرعت همزمان می‌شوند. سیگنال‌های کنترل در شکل (۲) رسم شده‌اند. عملکرد تخمین‌گر پیشنهادی در تخمین عدم قطعیت در شکل (۳) نشان داده شده است.

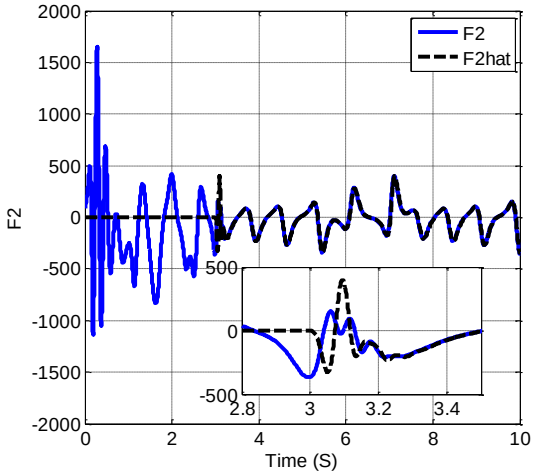


شکل (۱): عملکرد روش پیشنهادی در سنکرون‌کردن اولین متغیر حالت



شکل (۲): سیگنال‌های کنترل

عملکرد تخمین‌گر پیشنهادی در تخمین عدم قطعیت در شکل (۳) نشان داده شده است. بردار عدم قطعیت F، سه المان دارد که مقدار واقعی و تخمینی آن دومین عنصر آن در شکل (۳) رسم شده است. همان‌طورکه در این شکل مشاهده می‌شود، پس از اعمال کنترل‌کننده پیشنهادی، تخمین‌گر پس از گذشتن فقط ۰/۲ sec ، قادر به تخمین صحیح عدم‌قطعیت می‌باشد.

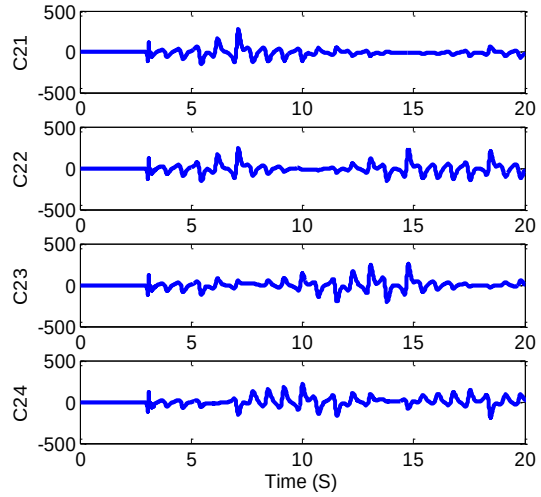


شکل (۳): عملکرد روش پیشنهادی در تقریب دومین درایه عدم قطعیت

مقدار اولیه بردار $\hat{C}$ صفر بوده است. همچنین فرض شده است کران بالای خطای مدل‌سازی عدم‌قطعیت، $\rho=1$ باشد. فرض کنید برای تخمین هر درایه بردار عدم قطعیت F از یک معادله دیفرانسیل مرتبه ۴ استفاده شود. مقادیر پارامترهای انتخاب شده برای تخمین‌گر به صورت زیر است:

$$\lambda=\begin{bmatrix}0 & -0.001 & -0.002 & -0.003\end{bmatrix}$$
$$\omega=\begin{bmatrix}0.1 & 0.2 & 0.3 & 0.4\end{bmatrix} \quad (۴۰)$$
$$\theta=\begin{bmatrix}0.4 & 0.1 & 0.2 & 0.3\end{bmatrix}$$

تغییراتی که قانون تطبیق به پارامترهای $\hat{C}_2$ اعمال می‌کند در شکل (۴) نشان داده شده است. همان‌طورکه مشاهده می‌شود این پارامترها کران‌دار می‌باشند.

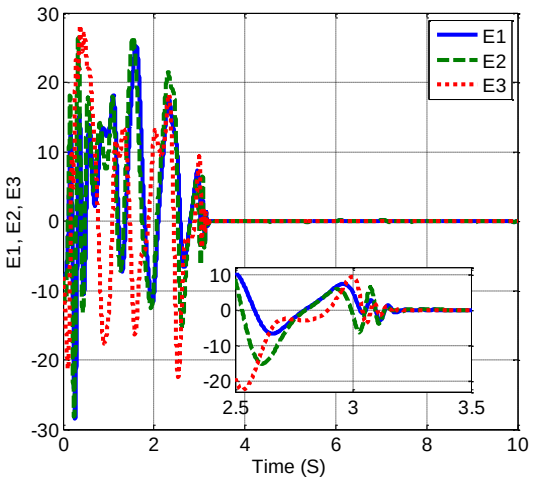


شکل (۴): چگونگی تغییرات درایه‌های بردار $\hat{C}_2$

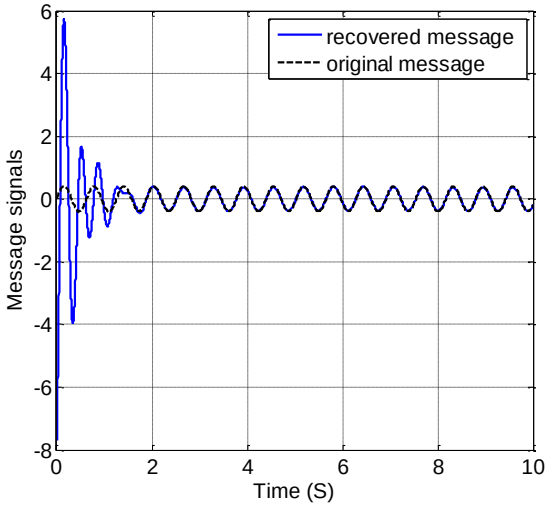
۶-۲- مقایسه با کنترل‌کننده مود لغزشی فازی

عملکرد کنترل کننده پیشنهادی را با یک کنترل‌کننده مود لغزشی فازی [۴۲] مقایسه می‌کنیم. تمام پارامترهای سامانه‌های آشوبی و شرایط اولیه آن‌ها با مقادیر ارائه شده در [۴۲] برابر می‌باشند. شکل (۷) در [۴۲] خطای سنکرون‌سازی این روش را نشان می‌دهد.

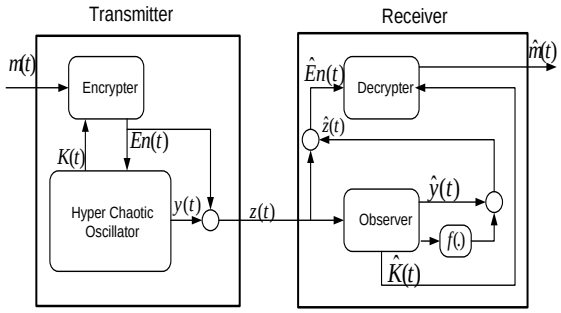
همان‌طور که در شکل (۷) مرجع [۴۲] مشاهده می‌شود، بعد از آن‌که کنترل‌کننده اعمال می‌شود، تقریبا ۳ sec طول خواهد کشید تا خطای سنکرون‌سازی صفر شود، اما همان‌طورکه در شکل (۵) مشاهده می‌شود، این زمان برای کنترل‌کننده پیشنهادی فقط ۰/۲ sec است که بیان‌گر مناسب‌تربودن سرعت پاسخ کنترل‌کننده پیشنهادی است. علاوه‌بر این، باید توجه داشت کنترل‌کننده‌های فازی معمولا به دانش افراد خبره برای تعیین قوانین فازی نیاز دارند [۴۳]، درحالی‌که تنظیم پارامترهای کنترل‌کننده پیشنهادی بسیار ساده‌تر است. شکل (۶)، نتایج شبیه‌سازی این رویتگر را نشان می‌دهد که در آن سیگنال‌های پیام اصلی و بازسازی شده ترسیم شده‌اند.



شکل (۵): خطای سنکرون‌سازی روش پیشنهادی



شکل (۶): بازیابی سیگنال پیام با استفاده از رویتگر پیشنهادی



شکل (۷): بلوک دیاگرام سامانه مخابراتی با استفاده از رویتگر و رمزنگار [۴۴]

۶-۳- کاربرد روش پیشنهادی در مخابرات امن

اکنون نحوه عملکرد کنترل‌کننده فوق در مخابرات امن مورد ارزیابی قرار می‌گیرد. در مخابرات امن، ارسال مستقیم همه متغیرهای حالت به فرستنده مجاز نیست. معمولاً فقط خروجی سامانه آشوب ارسال می‌گردد. در فرستنده، یک رویتگر حالت (تخمین‌گر) طراحی می‌شود. این تخمین‌گر با دریافت سیگنال ارسال‌شده، سایر متغیرهای حالت خود را با متغیرهای حالت فرستنده سنکرون می‌کند. سامانه فوق آشوبی زیر را درنظر بگیرید [۴۴]:

$$\dot{x} = Ax + B30(x_4 - 1)H(x_4 - 1) + Bd(t) + Bm(t)$$
$$A = \begin{bmatrix} 0.7 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & -3 \\ 0 & 0 & 3 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ -1 \end{bmatrix} \quad (۴۱)$$

که در آن، $m(t)$ سیگنال پیام است و H تابع پله واحد است ($H(u)=1\ if\ (u \geq 0);\ H(u)=0\ if\ (u<0)$) و $d(t)$ تغییرات ناخواسته‌ای است که در مدل فرستنده رخ می‌دهد. خروجی به صورت زیر تعریف می‌شود:

$$y(t) = 30(x_4 - 1)H(x_4 - 1) + Kx \quad (۴۲)$$

بردار سطری K طوری انتخاب می‌شود که مقادیر ویژه ماتریس $A-BK$ در موقعیت‌های دلخواه قرار گیرند. سیگنال ارسالی $z(t) = y(t) + m(t)$ خواهد بود. رویتگر زیر را درنظر بگیرید:

$$\dot{\hat{x}} = A\hat{x} + B(z - \hat{y}) + B(\hat{f} + u_r) \quad (۴۳)$$

که در آن $\hat{y} = K\hat{x}$ و $\hat{f} + u_r$ تخمین‌گر عدم قطعیت است که در این مقاله با استفاده از معادلات دیفرانسیل طراحی شده است. بردار خطای رویتگر را به صورت $e = x - \hat{x}$ تعریف کنید. با استفاده از (۴۳-۴۱) خواهیم داشت:

$$\dot{e} = A_c e + B(d - \hat{f} - u_r) \quad (۴۴)$$

که در آن، $A_c = A - BK$. مشابه (۱۳-۱۲) می‌توان نوشت:

$$\hat{f} = \varphi\hat{c}$$
$$\varphi = \begin{bmatrix} e^{-\lambda_1 t}Cos(\omega t + \theta_1) & e^{-\lambda_2 t}Cos(\omega t + \theta_2) \end{bmatrix} \quad (۴۵)$$
$$\hat{c} = \begin{bmatrix} \hat{c}_1 & \hat{c}_2 \end{bmatrix}^T$$

هم‌چنین، مشابه (۱۵) می‌توان نوشت:

$$d(t) = \varphi\hat{c} + \Delta(t) \quad (۴۶)$$

با جایگذاری (۴۶-۴۵) در (۴۴) خواهیم داشت:

$$\dot{e} = A_c e + B(\varphi\tilde{c} + \Delta - u_r) \quad (۴۷)$$

که مشابه (۱۶) می‌باشد. بنابراین، مانند آن‌چه در بخش ۵ تشریح شده است، سنکرون‌سازی رویتگر (۴۳) اثبات خواهد شد.

حال فرض کنید می‌خواهیم سیگنال پیام $m(t) = 0.4\sin(10t)$ را ارسال و دریافت کنیم. در این شبیه‌سازی فرض شده است $d(t) = 0.001\cos(t)$ باشد. بردار K را به صورت زیر تعریف کنید:

$$K = [-616.87 \quad -2237.9 \quad 116.1 \quad -10.7] \quad (۴۸)$$

سیگنال پیام بازسازی‌شده عبارت است از [۴۴]:

$$\hat{m}(t) = z(t) - \hat{z}(t)$$
$$\hat{z}(t) = 30(\hat{x}_4 - 1)H(\hat{x}_4 - 1) + \hat{y}(t) \quad (۴۹)$$

۶-۴- کاربرد روش پیشنهادی در رمزنگاری

معمولا، یکی از متغیرهای حالت (x_2) برای رمزنگاری پیام مورد استفاده قرار می‌گیرد. سپس پیام رمزشده ($En(t)$) با خروجی سامانه آشوب ($y(t)$) جمع شده و به گیرنده ارسال می‌شود. در فرستنده، یک رویتگر حالت (تخمین‌گر) طراحی میشود. این تخمین‌گر با دریافت سیگنال ارسال‌شده ($z(t)$)، سایر متغیرهای حالت خود را با متغیرهای حالت فرستنده سنکرون می‌کند [۴۶-۴۵]. در نتیجه، می‌توان یک تخمین مناسب از پیام رمزشده ($\hat{En}(t)$) به‌دست آورد. سپس، رمزگشا با استفاده از این سیگنال($\hat{En}(t)$) و سیگنال تخمینی متغیر حالتی‌که برای رمزنگاری استفاده شده است ($\hat{x}_2$)، سیگنال پیام را بازسازی می‌کند. بلوک دیاگرام این سامانه در شکل (۷) رسم شده است. مدل ریاضی به صورت زیر است [۴۴]:

$$\dot{x} = Ax + B30(x_4 - 1)H(x_4 - 1) + Bd(t) + B.En(t) \quad (۵۰)$$

برای رمزنگاری سیگنال پیام از رمزکننده شیفت‌دهنده n تایی استفاده شده است [۴۷]:

$$En(t) = f_1(...(f_1(f_1(m(t), K(t)), K(t)), ..., K(t)) \quad (۵۱)$$

که در آن، تابع غیرخطی $f_1(m(t), K(t))$ به‌صورت زیر تعریف

شده است:

$$f_1(m,K)=\begin{cases} m+K+2h & -2h\le m+K\le -h \\ m+K & -h\le m+K\le h \\ m+K-2h & h\le m+K\le 2h \end{cases} \quad (۵۲)$$

در این شبیه‌سازی، $n=30$ و $h=0.4$ انتخاب شده است و کلید $K(t)$ همان $x_2(t)$ می‌باشد. خروجی سامانه آشوبی همان خروجی تعریف شده در (۴۲) است. سیگنال ارسالی زیر را درنظر بگیرید:

$$z(t)=y(t)+En(t) \quad (۵۳)$$

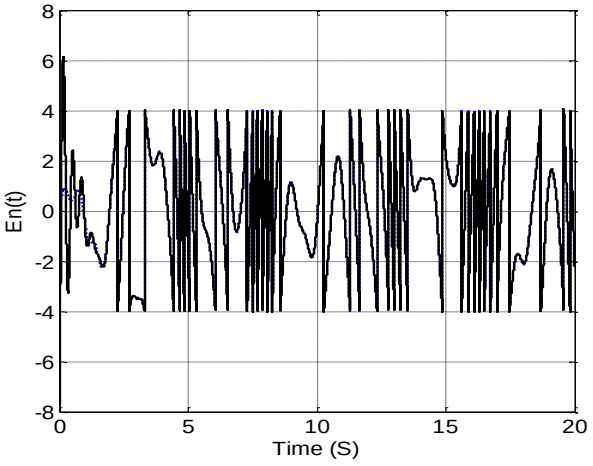
معادله رویتگر، همان رابطه (۴۳) خواهد بود. بردار K را به صورت (۴۸) درنظر بگیرید. مقدار تخمینی سیگنال پیام رمزشده برابر است با:

$$\begin{aligned} &\hat{En}(t)=z(t)-\hat{z}(t) \\ &\hat{z}(t)=30(\hat{x}_4-1)H(\hat{x}_4-1)+\hat{y}(t) \end{aligned} \quad (۵۴)$$

حال با استفاده از $\hat{En}(t)$ و $\hat{K}(t)=\hat{x}_2(t)$ باید سیگنال پیام را به صورت زیر رمزگشایی کنیم:

$$\hat{m}=f_1(...(f_1(f_1(\hat{En}(t),-\hat{K}(t)),-\hat{K}(t)),...,-\hat{K}(t)) \quad (۵۵)$$

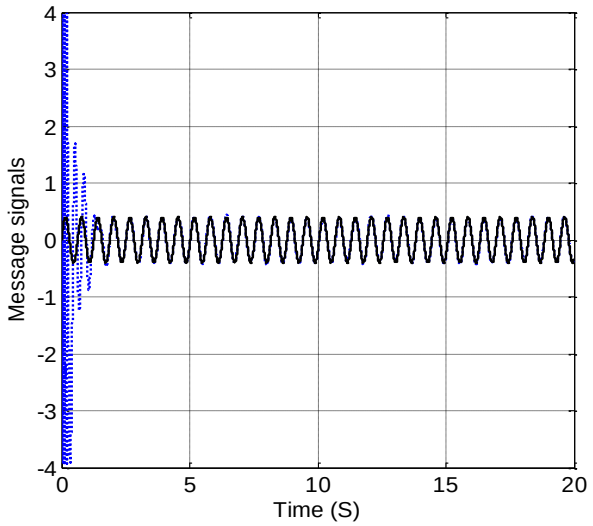
سیگنال پیام رمزشده و مقدار تخمین زده‌شده آن در شکل (۸) رسم شده‌اند. همان‌طورکه مشاهده می‌شود، رویتگر پیشنهادی عملکرد خوبی دارد و سیگنال پیام رمزشده را علی‌رغم تغییرات شدید آن می‌تواند به درستی تخمین بزند. سیگنال پیام اصلی و سیگنال پیام بازسازی‌شده در شکل (۹) رسم شده‌اند.



شکل (۸): پیام رمزشده $En(t)$ (خط پر) و مقدار تخمینی آن $\hat{En}(t)$ (نقطه چین)

۷- نتیجه گیری

در این مقاله یک روش جدید سنکرون‌سازی سامانه‌های آشوبی برمبنای قضیه تقریب عمومی و پاسخ معادلات دیفرانسیل ارائه گردید. برای این منظور، فرض شده است عدم قطعیت در یک معادله دیفرانسیل خطی با ضرایب ثابت نامعلوم صدق می‌کند. سپس نشان داده شد که پاسخ این معادله در شرایط قضیه عمومی صدق کرده و می‌تواند برای تخمین عدم قطعیت به‌کار گرفته شود. در کنترل‌کننده



شکل (۹): سیگنال پیام اصلی(خط پر) و سیگنال پیام بازسازی‌شده (نقطه چین)

پیشنهادی خطای مدل‌سازی نیز لحاظ شده است. برای تعیین پارامترهای تخمین‌گر پیشنهادی، با استفاده از قضیه پایداری لیاپانوف، قانون تطبیق طراحی گردید. همچنین، با استفاده از لم باربالات نشان داده شد که خطای سنکرون‌سازی به صفر همگرا میشود. در مقایسه با کنترل مود لغزشی فازی، کنترل‌کننده پیشنهادی سرعت به مراتب بهتری داشته و همچنین، تخمین‌گر پیشنهادی به‌خوبی می‌تواند عدم قطعیت را تخمین بزند. علاوه‌بر این، صحت عملکرد روش پیشنهادی در بازیابی سیگنال پیام در مخابرات امن و رمزنگاری مورد بررسی قرار گرفت.

۸- تشکر و قدردانی

این تحقیق در قالب طرح پژوهشی به شماره ابلاغیه ۱۷۷۶۶/د/۱۳۹۵ مورخ ۱۳۹۵/۹/۲۳ و با استفاده از اعتبارات

پژوهشی دانشگاه بیرجند انجام شده است که بدین‌وسیله تشکر و قدردانی می‌شود.

۹- مراجع

[1] L. Kocarev, G. Jakimoski, T. Stojanovski, and U. Parlitz, "From Chaotic Maps to Encryption Schemes." In Proceedings IEEE International Symposium Circuits and Systems, vol. 4, pp. 514-517, 1998.

[2] B. Fathi Vajargah, R. Asghari, and J. Vahidi, "Design and Analysis of a Novel Synchronous Stream Cipher Using Secure Pseudo Random Number Generator." Journal of Electronical & Cyber Defence, vol. 4, no. 1, pp. 59-68, 2016 (in Persian).

[3] A. Mirghadri, and A. Jolfaei, "A Novel Image Encryption Scheme Using Chaotic Maps." Passive Defence Sci. & Tech., vol. 2, no. 2, pp. 111-124, 2011 (in Persian).

[4] L. M. Pecora and T. L. Carroll, "Synchronization in Chaotic Systems," Phys. Rev. Lett., vol. 64, pp. 821-824, 1990.

[5] K. Y. Lian, P. Liu, and T.S. Chiang, "Adaptive Synchronization Design for Chaotic Systems via a Scalar Driving Signal." IEEE Trans. Circuits-I, vol .49, pp. 17-27, 2002.

[6] K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua, "Spread Spectrum Communication Through Modulation of Chaos", Int. J. Bifurcat Chaos, vol .3 , pp. 469-477, 1993.

[7] T. L. Liao, and N. S. Huang, "An Observer-Based Approach for Chaotic Synchronization with Application to Secure Communication", IEEE Trans. Circuits-I, vol .46, pp. 1144-1150, 1999.

[8] G. Kolumban, M. P. Kennedy, and L. O. Chua, "The Role of Synchronization in Digital Communication Using Chaos—Part I: Fundamentals of Digital Communications.", IEEE Trans. Circuits-I, vol .44, pp.927-936, 1997.

[9] K. Murali, H. Yu, V. Varadan, and H. Leung, "Secure Communication Using a Chaos Based Signal Encryption Scheme." IEEE Trans. Consum Electr, vol .47, pp. 709-714, 2001.

[10] J. M. V. Grzybowski, M. Rafikov and J. M. Balthazar, "Synchronization of the unified chaotic system and application in secure communication", Commun. Nonlinear Sci. Numer. Simul. vol. 14, pp. 2793-2806, 2009.

[11] C. Yin, S. M. Zhong, and W. F. Chen, "Design PD controller for master–slave synchronization of chaotic Lur'e systems with sector and slope restricted nonlinearities," Commun. Nonlinear Sci. Numer. Simul., vol. 16, pp. 1632–1639, 2011.

[12] J. S. Lin, and J. J. Yan, "Adaptive synchronization for two identical generalized Lorenz chaotic systems via a single controller." Nonlinear Anal. Real World Appl., vol. 10, pp. 1151–1159, 2009.

[13] M. Pourmahmood, S. Khanmohammadi, and G. Alizadeh, "Synchronization of two different uncertain chaotic systems with unknown parameters using a robust adaptive sliding mode controller." Commun. Nonlinear Sci. Numer. Simul. vol. 16, pp. 2853–2868, 2011.

[14] L. Li, Y. Liu, and Q. J. Yao, "Robust synchronization of chaotic systems using sliding mode and feedback control," Zhejiang Univ. - Sci. C, vol. 15, pp. 211-222, 2014.

[15] L. Xiao-run, Z. Liao-ying, and Z. Guang-zhou, "Sliding mode control for synchronization of chaotic systems with structure or parameters mismatching." J. Zheijang Univ.-Sci. A, vol. 6, pp. 571-576, 2005.

[16] W. Jing, T. Zhen-Yu, M. Xi-Kui, and G. Jin-Feng, "A novel adaptive observer-based control scheme for synchronization and suppression of a class of uncertain chaotic systems," Chinese Physics Letters, vol. 26, no. 5, pp. 050503, 2009.

[17] J. Yang, Y. Chen, and F. Zhu, "Associated observer-based synchronization for uncertain chaotic systems subject to channel noise and chaos-based secure communication," Neurocomputing, vol. 167, pp. 587-595, 2015.

[18] P. Bagheri, M. Shahrokhi, and H. Salarieh, "Adaptive observer-based synchronization of two non-identical chaotic systems with unknown parameters," J. Vib. Control, vol. 23, pp. 389-399, 2017.

[19] E. Cherrier, M. Boutayeb, and J. Ragot, "Observers-based synchronization and input recovery for a class of nonlinear chaotic models", IEEE Trans. Circ Syst – Part I, vol. 53, pp. 1977-1988, 2006.

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

[21] J. Yang, Y. Chen, and F. Zhu, "Singular reduced-order observer-based synchronization for uncertain chaotic systems subject to channel disturbance and chaos-based secure communication," Appl. Math. Comput., vol. 229, pp. 227–238, 2014.

[22] M. Chen, D. Zhou, and Y. Shang, "A sliding mode observer based secure communication scheme," Chaos Soliton Fract., vol. 25, pp. 573–578, 2005.

[23] C. F. Hsu, "Adaptive fuzzy wavelet neural controller design for chaos synchronization," Exp. Syst. Appl., vol. 38, pp. 10475–10483, 2011.

[24] C. S. Chen, "Quadratic optimal neural fuzzy control for synchronization of uncertain chaotic systems," Exp. Syst. Appl., vol. 36, pp. 11827–11835, 2009.

[25] T. C. Lin, F. Y. Huang, Z. Du, and Y. C. Lin, "Synchronization of fuzzy modeling chaotic time delay memristor-based Chua's circuits with application to secure communication," International Journal of Fuzzy Systems, vol. 17, no. 2, pp. 206-214, 2015.

[26] C. Mou, C. S. Jiang, J. Bin, and Q. X. Wu, "Sliding mode synchronization controller design with neural network for uncertain chaotic systems," Chaos Soliton Fract., vol. 39, pp. 1856–1863, 2009.

[27] S. Khorashadizadeh and M. M. Fateh, "Uncertainty estimation in robust tracking control of robot manipulators using the Fourier series expansion," Robotica, vol. 35, no. 2, pp. 310-336, 2015.

[28] L. X. Wang, "A Course in Fuzzy Systems and Control," Prentice-Hall, New York, 1997.

[29] M. Gupta, L. Jin, and N. Homma, "Static and dynamic neural networks: from fundamentals to advanced theory," John Wiley & Sons, 2004.

[30] M. M. Fateh, S. Azargoshasb, and S. Khorashadizadeh, "Model-free discrete control for robot manipulators using a fuzzy estimator," COMPEL: The International Journal for Computation and Mathematics in Electrical and Electronic Engineering, vol. 33, no. 3, pp. 1051-1067, 2014.

[31] M. M. Fateh, S. M. Ahmadi, and S. Khorashadizadeh, "Adaptive RBF network control for robot manipulators." Journal of AI and Data Mining, vol. 2, no. 2, pp. 159-166, 2014.

[32] S. Khorashadizadeh and M. M. Fateh, "Robust task-space control of robot manipulators using Legendre polynomials for uncertainty estimation," Nonlinear Dyn., vol. 79, no. 2, pp. 1151-1161, 2015.

[33] M. M. Fateh and S. Khorashadizadeh, "Optimal Robust voltage control of electrically driven robots," Nonlinear Dyn., vol. 70, no. 2, pp. 1445–1458, 2012.

[34] A. C. Huang, S. C. Wu, and W. F. Ting, "A FAT-based adaptive controller for robot manipulators without regressor matrix: theory and experiments," Robotica, vol. 24, no. 2, pp. 205-210, 2006.

[35] K. Chen-Yu and A. C. Huang, "A regressor-free adaptive controller for robot manipulators without Slotine and Li's modification," Robotica, vol. 31, no. 7, pp. 1051-1058, 2013.

[36] C. Ming-Chih and A. C. Huang, "Adaptive impedance controller design for flexible-joint electrically-driven robots without computation of the regressor matrix," Robotica, vol. 30, no. 1, pp. 133-144, 2012.

[37] M. B. Fard and S. Khorashadizadeh, "Model free robust impedance control of robot manipulators using fourier series expansion," In AI & Robotics (IRANOPEN), IEEE 2015, pp. 1-7, 2015.

[38] S. Khorashadizadeh and M. M. Fateh, "Adaptive Fourier series-based control of electrically driven robot manipulators," The 3rd International Conference on Control, Instrumentation and Automation (ICCIA), IEEE, pp. 213-218, 2013.

[39] A. Izadbakhsh, and S. Khorashadizadeh, "Robust task-space control of robot manipulators using differential equations for uncertainty estimation," Robotica, vol. 35, no. 9, pp. 1923-1938, 2017.

[40] J. Effa, B. Essimbi, and J. Ngundam, "Synchronization of improved chaotic Colpitts oscillators using nonlinear feedback control," Nonlinear Dyn., vol. 58, no. 1, pp. 39-47, 2009.

[41] J. J. Slotine and W. Li, "Applied nonlinear control," Englewood Cliffs, NJ: prentice-Hall, 1991.

[42] C. L. Kuo, "Design of a fuzzy sliding-mode synchronization controller for two different chaos systems," Computers and Mathematics with Applications, vol. 61, pp. 2090–2095, 2011.

[43] M. M. Fateh and S. Khorashadizadeh, "Robust control of electrically driven robots by adaptive fuzzy estimation of uncertainty," Nonlinear Dynamics, vol. 69, no. 3, pp. 1465-1477, 2012.

[44] G. Grassi, and S. Mascolo, "Synchronizing Hyperchaotic Systems by Observer Design," IEEE Trans. Circuits-II, vol. 46, no. 4, pp. 478-483, 1999.

[45] S. Khorashadizadeh and M. H. Majidi, "Chaos synchronization using the Fourier series expansion with application to secure communications," AEU-INT J ELECTRON C, vol. 82, pp. 37-44, 2017.

[46] S. Khorashadizadeh and M. H. Majidi, "Synchronization of two different chaotic systems using Legendre polynomials with application to secure communications," FRONT INFORM TECHEL, 2018. [doi="10.1631/FITEE.1601814"]

[47] T. Yang, C. W. Wu, and O. Chua, "Cryptography based on chaotic systems," IEEE Trans. Circuits-I, vol. 44, no. 5, pp. 469-471, 1997.

Journal of Electronical & Cyber Defence
Vol. 5, No. 4, 2017, Serial No. 20

Chaos Synchronization Using Differential Equations and the Universal Approximation Theorem with Application to Secure Communication and Cryptography

M. H. Majidi*, S. Khorashadizadeh

*University of Birjand

(Received: 20/10/2017, Accepted: 23/07/2017)

ABSTRACT

In this paper, a new method has been presented for chaos synchronization using a nonlinear controller. In most so-far presented approaches, it is assumed that the mathematical models of the transmitter and reciever are completely the same. Due to the non-identical environmental circumstances in the transmitter and receiver and the influence of temperature on the chaotic system parameters, this assumption is not true. In this paper, a novel approach, in which uncertainties are modeled by a linear diffential equation with unknown constant coefficients, has been presented for estimation of these uncertainties . Since this function satisfies the conditions of the universal approximation theorem, it can estimate nonlinear functions with arbitrary small approximation error. However, since the coefficients are unknown, the parameters of these functions are unknown and should be estimated using the adaptation laws derived from the synchronization analysis. Simulation results verify the effectiveness of the proposed estimator. In comparison with other controllers such as fuzzy sliding mode controllers, the proposed controller response is faster. Moreover, its application in secure communications and cryptography has been studied, as well.

Keywords: Chaos Synchronization, Secure Communication, Cryptography, Differential Equations, The Universal Approximation Theorem.

* Corresponding Author Email: m.majidi@birjand.ac.ir