مجله کنترل
ISSN (print) 2008-8345
ISSN (online) 2538-3752
مقاله پژوهشی
جلد۱۸، شماره ۳، پاییز ۱۴۰۳، صفحه ۴۷-۳۷

کنترل ردیابی تحمل پذیر عیب ایمن برای کلاسی از سامانه‌های غیر خطی با عیوب چندگانه در حضور حملات انکار سرویس و تزریق

حمیدرضا باقی محمدآبادی[۱] ، فرزانه عبداللهی[۲] و حیدرعلی طالبی[۳]

[۱] دانشجوی دکتری، دانشکده مهندسی برق، گروه کنترل، دانشگاه امیرکبیر،تهران، ایران hamid.baghi@aut.ac.ir

[۲] دانشیار، دانشکدهٔ مهندسی برق، گروه کنترل، دانشگاه امیرکبیر، تهران، ایران f_abdollahi@aut.ac.ir

[۳] استاد، دانشکدهٔ مهندسی برق، گروه کنترل، دانشگاه امیرکبیر،تهران، ایران alit@aut.ac.ir

دریافت: ۱۴۰۲/۱۰/۱۶ ویرایش: ۱۴۰۳/۰۲/۰۷ پذیرش: ۱۴۰۳/۰۳/۲۷

چکیده: در این مقاله مسئله کنترل ردیابی تحمل پذیر عیب ایمن در طبقه ای از سامانه‌های غیرخطی نامعین که دچار حملات تزریق و حملات انکار سرویس (DoS) می‌شوند، بررسی شده است. با توجه به ماهیت حملات انکار سرویس و حملات تزریق ما یک رویکرد نوآورانه ارائه داده‌ایم که از یک مشاهده‌گر با بهره سوئیچ شونده جهت اطمینان از کنترل ردیابی و تاب آوری سایبری با تخمین حالت‌های غیر قابل دسترس با جبران اثر عیوب محرک و حسگر بطور همزمان بهره می‌برد. عدم قطعیت‌های ذاتی سامانه و عیوب محرک و حسگر و اغتشاشات سامانه از طریق یک رویکرد کنترل ردیابی تطبیقی حل می‌شوند. با یکپارچه‌سازی کنترل تطبیقی، یک سامانه منطق فازی (FLS) و روش‌های مبتنی بر مشاهده‌گر، روش پیشنهادی ما پارامترهای کنترلی و را به‌طور پویا تنظیم می‌کند تا با عدم قطعیت‌های سامانه سازگار باشد و تأثیر اغتشاشات، عیوب محرک و حسگر و حملات تزریق را کاهش دهد. رویکرد پیشنهادی ما همچنین پایداری سامانه و عملکرد ردیابی را تضمین می‌کند و عملکردی مناسبی را جهت کنترل سامانه در حضور حملات سایبری ارائه می‌دهد. نتایج شبیه سازی بر روی یک سامانه غیرخطی نمونه، اثربخشی روش پیشنهادی را نشان می‌دهد.

کلمات کلیدی: سامانه غیر خطی نامعین، حملات انکار سرویس، حملات تزریق، عیوب حسگر و محرک، کنترل ایمن، کنترل تحمل پذیر عیب.

Secure Fault-Tolerant Tracking Control for a Class of Nonlinear Uncertain Systems with Multiple Faults in the Presence of Denial-of-Service and Injection Attacks

Hamidreza Baghi Mohammad Abadi, Farzaneh Abdollahi and Heidar Ali Talebi

Abstract: This paper investigates the problem of secure fault-tolerant tracking control of a class of uncertain nonlinear systems suffering injection attacks and denial-of-service (DoS) attacks. Given the nature of DoS attacks and injection attacks, we have introduced a novel approach that utilizes a switching-type state observer for ensuring control over cyber tracking and resilience against constructed to simultaneously estimate unmeasured state and compensate the actuator and sensor faults. The inherent uncertainties of the system, along with actuator and sensor faults and system disturbances, are addressed through an adaptive tracking control approach. Through the integration of adaptive control, a Fuzzy Logic System (FLS), and observer-based techniques, our method dynamically adjusts control parameters to be compatible with system uncertainties and mitigates the impact of disturbances, actuator and sensor faults, and injection attacks. Our proposed approach ensures system stability and tracking performance, providing a suitable framework for controlling the

system in the presence of cyber-attacks. Simulation results on a non-linear example system demonstrate the effectiveness of the proposed method.

Keywords: Uncertain Nonlinear System; Denial-of-Service Attacks; Injection Attacks; Sensor and Actuator Faults; Secure Control; Fault-Tolerant Control.

۱- مقدمه

امروزه استفاده از سامانه‌های غیر خطی در بسیاری از صنایع، از جمله قدرت، هوافضا و حمل و نقل و... گسترش یافته است[۱-۴]. با پیشرفت تکنولوژی، افزایش پیچیدگی سامانه‌ها و پدیدار شدن تهدیدات سایبری مسائل مربوط به کنترل ایمن[۱] و تحمل پذیری عیب برای این سامانه‌ها اهمیت بیشتری یافته است [۴-۸].توسعه روزافزون سامانه‌های ابعاد وسیع، آسیب‌پذیری‌هایی را ایجاد کرده است که دشمنان می‌توانند از آنها سوءاستفاده کنند و تهدیدی برای عملکرد و ایمنی کلی آن ایجاد کنند. این امر به ویژه در زمینه سامانه‌های کنترل فرآیندهای پیچیده غیرخطی که در آنها عدم قطعیت‌ها و عیوب متعدد حضور دارند اجتناب‌ناپذیر است و ظهور حملات سایبری مانند انکار سرویس[۲]، حملات تزریق[۳] و بازپخش[۴] باعث افزایش پیچیدگی در کنترل این گونه از سامانه‌ها می‌شوند[۹-۱۰].

حضور عیوب چندگانه و حملات سایبری می تواند تهدید موثری برای عملکرد و ثبات سامانه های غیر خطی باشد [۱۱]. به منظور مقابله با این چالش‌ها، نیاز به توسعه روش‌ها و الگوریتم‌های نوین کنترل ردیابی ایمن تحمل پذیر عیب است که بتوانند در عین حفظ پایداری سامانه عملکرد سامانه را بهبود ببخشند[۱۲-۱۵].

در سالهای اخیر، تحقیقات قابل توجهی در مورد تاب آوری سامانه‌ها در حضور حملات DoS پدید آمده است. یکی از مسیرهای مورد بررسی توسط محققان استفاده از کنترل کننده‌های مبتنی بر ناظر بهره سوئیچ شونده[۵] می‌باشد[۱۶-۱۹]. در [۳۳] مسئله کنترل تحمل پذیر عیب مبتنی بر ناظر ورودی ناشناخته برای سامانه های سایبر-فیزیکی چندکاناله بررسی شده است. در [۳۴] ناظر سوئیچ شونده عصبی به همراه کنترل کننده ی بازگشت به عقب رویدادمحور جدیدی برای نوع خاصی از سیستم غیر خطی ارائه شده است. در [۱۶] نویسندگان برای کلاسی از سامانه‌های غیرخطی نامعین که تحت حملات DoS است، یک ناظر حالت تغییر یافته بهمراه یک طرح کنترل ایمن تطبیقی غیر متمرکز بهمراه الگوریتمی جهت تعیین زمان محاسبه بهره های ناظر از طریق حل نامساوی های ماتریسی خطی[۶] ارائه داده اند در واقع به دلیل وجود داشتن عبارت متغیر با زمان در LMIها الگوریتم زمان جدید محاسبه ی این LMIها را بر اساس عملکرد سامانه مشخص می کند. مسئله کنترل ردیابی فازی تطبیقی غیر متمرکز برای اینگونه ازسامانه‌ها که تحت عیب و حملات DoS اند در [۱۲] مورد بررسی قرار گرفته است. در [۱۱] نویسندگان مسئله کنترل ردیابی ایمن تطبیقی را برای کلاسی از سامانه های غیر خطی متصل شده ابعاد وسیع در حضور عیوب چند گانه و حمله DoS با استفاده از ناظر سوئیچ شونده توسعه داده اند که در آن معیار عملکرد الگوریتم بر خلاف [۱۶] از حالت تخمین زده شده به خطای ردیابی تغییر کرده است.

حملات تزریق به دلیل به خطر انداختن یکپارچگی اطلاعات چالش‌هایی را در طراحی و تجزیه و تحلیل سامانه‌های کنترل ایجاد کرده اند[۲۰-۲۲] در نتیجه، تلاش‌های تحقیقاتی به سمت رسیدگی به نگرانی‌های امنیتی مرتبط با سامانه‌های غیرخطی تحت حملات تزریق هدایت شده‌اند. فعالیت های تحقیقاتی مختلفی بر اهمیت روزافزون سامانه‌های ایمن در برابر حملات DoS و حملات تزریق در زمینه محیط‌های فیزیکی-سایبری مدرن تأکید می‌کنند[۲۳-۲۶]. در [۲۷] نویسندگان روشی را ارائه داده اند که بر خلاف روش‌های [۱۱،۱۶،۱۸و۳۲] محاسبه ی بهره ی ناظر سوییچ شونده از طریق حل LMIها به صورت غیربرخط می‌باشد و نویسندگان این روش را برای سامانه‌های ابعاد وسیع غیرخطی در حضور حملات سایبری DoS و تزریق توسعه داده اند اما تاثیر عیوب چندگانه در طراحی بررسی نشده است و همچنین تخمینی از عبارت های غیر خطی در ناظر طراحی شده انجام نگرفته است.

هدف این مقاله ارائه یک راه حل جدید و جامع جهت حل مسائل چند بعدی که شامل حضور همزمان عیوب چندگانه وحملات سایبری در سامانه است، می‌باشد. تمرکز ما بر روی توسعه یک استراتژی کنترل ردیابی بازخورد-خروجی تطبیقی فازی ایمنی است که جهت حفظ عملکرد کلی سامانه، حتی در مواجهه با عدم قطعیت‌ها، عیوب حسگر و محرک، و حملات سایبری مخرب به خوبی عمل کند. در این مقاله سعی شده است در عین حال مقابله با تمام مسائل ذکر شده از مشکل اصلی روش های برخط[۳۲] یعنی نیاز به حل چندباره LMIها جلوگیری شودکه موجب کاهش پیچیدگی های محاسباتی می شود و همچنین با معرفی ناظر جدیدی عملکرد ردیابی و تخمین حالت ها را نیز نسبت به روش های غیر برخط بهبود [۱۰و۲۷] دهد در واقع با بهبود عملکرد ناظر غیر برخط نیاز به استفاده از ناظر بر خط کاهش یافته است. از اهم آثار این مقاله می‌توان به موارد زیر اشاره کرد:

(۱) طراحی ناظر بهره سوئیچ شونده تطبیقی به همراه کنترل فازی بازگشت به عقب، این روش نه تنها پایداری سامانه را در حضور عدم

[1] Secure Control
[2] Denial of Service (DoS) Attack
[3] Injection Attack
[4] Replay Attack
[5] Switching Observer Gain
[6] Linear Matrix Inequality (LMI)

قطعیت‌ها و عیوب حسگر حفظ می کند، بلکه به طور موثر اثرات حملات DoS و حملات تزریق را بطور همزمان در سامانه کاهش می‌دهد.

(۲) یک رویکرد کنترل فازی تطبیقی ایمن جدید، که پارامترهای کنترل کننده را قادر می‌سازد به طور مستقل بر اساس شرایط سامانه بلادرنگ تنظیم شوند.

(۳) طراحی ناظر بگونه ای است که محاسبات LMI مورد نیاز بصورت غیر برخط صورت گیرد و در مقابل وقوع حملات سایبری و عیوب سامانه بطور همزمان عملکرد بهتری نسبت به روش های مشابه [۲۷] را داشته باشد.

ادامه مقاله به شرح زیر سازماندهی شده است:

بخش ۲ تعریف مسئله و مقدمات اولیه مربوطه را ارائه می‌دهد. طراحی ناظر در بخش ۳ بیان شده است. در بخش ۴ یک طرح کنترل تطبیقی همراه با اثبات پایداری کلی پیشنهاد شده است. یک مثال شبیه سازی در بخش ۵ برای نشان دادن اثربخشی طرح کنترل پیشنهادی ارائه شده است. در نهایت، مقاله در بخش ۶ جمع بندی و خلاصه می‌شود.

۲- تعریف مسئله

۲-۱- معرفی سامانه

سامانه غیرخطی ناشناخته زیر را در نظر بگیرید:

$$\begin{cases}\dot{x}_i = x_{i+1} + f_i(t,x) + d_i, i = 1,\dots,n-1\\ \dot{x}_n = u + f_n(t,x) + d_n\\ y = x_1\end{cases} \quad (۱)$$

که در آن $x = [x_1,\dots,x_n]^{\mathrm{T}} \in \mathbf{R}^n$ بردار حالت با مقدار اولیه $x(0) = x_0$ است.

$y \in \mathbf{R}$ و $u \in \mathbf{R}$ به ترتیب خروجی سامانه و ورودی کنترل هستند. $f_i: \mathbf{R}_+ \times \mathbf{R}^n \to \mathbf{R}, i = 1,\dots,n$، توابع غیر خطی ناشناخته ملایم و d_i اغتشاش خارجی می‌باشد [۲۸].

عیب محرک به صورت زیر در نظر گرفته می‌شود:

$$u = \alpha v + \bar{u} \quad (۲)$$

که در آن u ورودی محرک، v سیگنال کنترلی محاسبه شده و دو پارامتر عیب $\bar{u}$ و $\alpha \in [\underline{\alpha}, 1]$، که به ترتیب نشان دهنده عیب جمع شونده و ضربی محدود ناشناخته هستند. علاوه بر این، خروجی‌های سامانه، که نشان‌دهنده اندازه‌گیری‌های واقعی حسگرها هستند، توسط رابطه زیر توصیف می‌شود:

$$y = \beta x_1 \quad (۳)$$

که در آن β بیانگر پارامتر عیب حسگر است که نشان دهنده میزان کاهش اثربخشی حسگر می‌باشد.

فرض ۱ (شرط لیپشیتز): $\forall X_1, X_2$ ثابت‌های l_i^f وجود دارد بطوری که نامساوی زیر بر قرار است [۱۱]:

$$\|f_i(X_1) - f_i(X_2)\| \le l_i^f \|X_1 - X_2\|$$

۲-۲- حمله DoS

یک حمله DoS از منابع اختلال برای جلوگیری از انتقال داده‌ها استفاده می‌کند. در این مقاله مسئله حملات DoS متناوب در کانال‌های حسگرها مورد بررسی قرار می گیرد. $\{t_j\}_{j\in N}$، درزمان $t_0 \ge 0$ لحظه‌های حملات DoS را نشان می‌دهد. فاصله زمانی j امین حمله DoS با $T_j := \left[t_j, t_j + t_j^*\right)$ نشان داده می‌شود، و ارتباط در این بازه زمانی به طول $\tau_j \in \mathbb{R}^+$ ممنوع است. در نتیجه می‌توان نشان داد:

$$\Sigma(t^*,t) := \cup_{j\in N} T_j \cap [t^*,t],\quad \Pi(t^*,t) := [t^*,t]\backslash\Sigma(t^*,t) \quad (۴)$$

که در آن در بازه ی (t^*,t)، $\Sigma(t^*,t)$ و $\Pi(t^*,t)$ بیانگر زمانی است به ترتیب ارتباط ممنوع و مجاز است. در نهایت خروجی حسگر در حضور حملات DoS به صورت زیر در نظر گرفته می‌شود:

$$y^a(t) = \begin{cases}0, & \text{if} \quad t \in \Sigma(0,+\infty),\\ y(t), & \text{if} \quad t \in \Pi(0,+\infty),\end{cases}$$

تعداد وقوع حملات DoS در بازه $[t^*,t)$ با $n(t^*,t)$ نشان داده می‌شود. دو فرض زیر محدود بودن انرژی مهاجم در نتیجه متناوب بودن حملات DoS را مشخص می کند.

فرض ۲ (فرکانس DoS)- دو اسکالر مثبت n_1 و T_{n1} برای هر $t \ge t^* \ge 0$ وجود دارد، به طوری که نامساوی زیر برقرار است [۵].

$$m(t,t^*) \leqslant n_1 + \frac{t-t^*}{T_{n1}}, \quad (۵)$$

فرض ۳ (دوره DoS)- دو اسکالر مثبت n_2 و T_{n2} برای هر $t \ge t^* \ge 0$ وجود دارد، به طوری که نامساوی زیر برقرار است [۵].

$$\Sigma(t,t^*) \leqslant n_2 + \frac{t-t^*}{T_{n2}}, \quad (۶)$$

۲-۳- فرمول بندی حمله تزریق

حمله تزریق در کانال محرک به صورت زیر مدل شده است:

$$\bar{u}(t) = v(t) + \omega(t)v(t)$$

که در آن $\omega(t)$ یک بهره متغیر با زمان ناشناخته را نشان می‌دهد و $\omega(t)v(t)$ سیگنالی است که به کنترل کننده تزریق می‌شود. اگر $b(t) = 1 + \omega(t)$ تعریف شود، سپس می‌توانیم $u^*(t) = b(t)v(t)$ را تعریف کنیم. برای بهره متغیر با زمان $\omega(t)$ سیگنال حمله تزریقی، $-1 < \omega(t)$ را فرض می‌کنیم [۲۷]. علاوه بر این، دو ثابت مثبت $\bar{b}$ و $\underline{b}$ وجود دارد به طوری که برای بهره متغیر با زمان $b(t)$ همواره نامساوی زیر برآورده می‌شود[۲۷]:

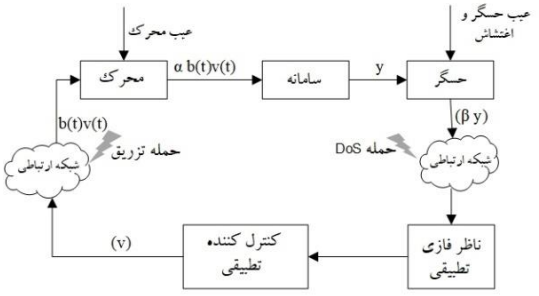
$$\underline{b} \le b(t) \le \bar{b}.$$

در نهایت اگر $\eta_i = \frac{x_i}{b(t)}, \dots, \eta_n = \frac{x_n}{b(t)}, i = 1,2,\dots,n-1$ تعریف شود می توان (۱) را بصورت زیر بازنویسی کرد:

$$\begin{cases}\dot{\eta}_i = \frac{\dot{x}_{i+1}}{b(t)} - \frac{\dot{b}(t)x_i}{b^2(t)} = \eta_{i+1} + f_i' + \frac{1}{b(t)}d_i(t),\\ \dot{\eta}_n = \frac{\dot{x}_n}{b(t)} - \frac{\dot{b}(t)x_n}{b^2(t)} = \alpha v + f_n' + \frac{1}{b(t)}d_n(t),\\ y = b(t)\beta x_1,\end{cases} \quad (۷)$$

که در آن $f_i' = \frac{1}{b(t)}f_i(\bar{x}_i) - \frac{\dot{b}(t)\eta_i}{b(t)}, f_n' = \frac{1}{b(t)}f_n(\bar{x}_n) - \frac{\dot{b}(t)\eta_n}{b(t)}$ است.

در نهایت در شکل ۱ طرح ساختار کلی سامانه در حضور عیوب حسگر و محرک با در نظر گرفتن حملات DoS و تزریق نشان داده شده است.



شکل ۱: طرح کلی ساختار سامانه

۴-۲- سامانه فازی (FLS)

FLS اغلب برای تقریب توابع غیر خطی ناشناخته استفاده می‌شود. بدین منظور ابتدا از یک فازی ساز تکین، یک موتور استنتاج کننده فازی و یک فازی زدای میانگین مرکز برای بدست آوردن سامانه فازی بصورت زیر استفاده می کنیم:

$$\varphi_l(x)=\frac{\prod_{i=1}^{n}\mu_{A_i^l}(x_i)}{\sum_{l=1}^{N}\prod_{i=1}^{n}\mu_{A_i^l}(x_i)} \quad (۸)$$

سپس اگر $\zeta=[\zeta_1,\zeta_2,\dots,\zeta^N]$ و $\varphi(x)=[\varphi_1(x),\varphi_2(x),\dots,\varphi_N(x)]^T$ باشد. با فرض اینکه (۸) برقرار است، عبارت $y(x)$ را می‌توان به شکل ماتریسی زیر بازنویسی کرد.

$$y(x)=\zeta^T\varphi(x) \quad (۹)$$

پیرو قضایای تقریب فراگیر سامانه‌های فازی [۲۹] برای یک عبارت دینامیکی غیرخطی ناشناخته مفروض $f(x)$ که بر روی یک مجموعه فشرده Ω تعریف شده است، می‌توان برای هر $q>0$ یک FLS پیدا کرد بطوری که برای آن نامساوی زیر برقرار باشد:

$$\sup_{x\in\Omega}|f(x)-\zeta^T\varphi(x)|\le q$$

در ادامه FLS برای تقریب f_i بصورت زیر استفاده می‌شود:

$$f_i(\hat{\bar{x}})=\zeta_i^T\varphi_i(\hat{\bar{x}})+\varepsilon_i^f(\hat{\bar{x}}), \quad (۱۰)$$

که در آن $\hat{\bar{x}}=[\hat{x}_1 \quad \hat{x}_2 \quad \dots \quad \hat{x}_i]^T$ است و در نهایت (۷) بصورت زیر بازنویسی می‌شود:

$$\begin{cases}\dot{\eta}_i=\eta_{i+1}+\zeta_i^T\varphi_i(\bar{x})+\mathcal{W}_i(t), i=1,\dots,n-1\\ \dot{\eta}_n(t)=\alpha v+\zeta_n^T\varphi_n(\bar{x})+\mathcal{W}_n(t)(t)\\ y(t)=b(t)\beta x_1\end{cases} \quad (۱۱)$$

که در آن $\mathcal{W}_i(t)=d_i'+\varepsilon_i^f+\Delta f_i$ و $\Delta f_i=f_i'(\bar{x}_i)-f_i'(\hat{\bar{x}}_i)$ است.

هدف طراحی یک کنترل ردیابی بازخورد خروجی انعطاف‌پذیر مبتنی بر ناظر تحت عیوب حسگر و محرک در حضور حملات DoS و تزریق است به گونه‌ای که تمامی سیگنال‌های خطای سامانه محدود شوند. ابتدا ناظر تطبیقی طراحی می‌شود که آنالیز اولیه آن برای دو حالت وقوع و عدم وقوع حملات DoS انجام می گیرد، پس از استخراج قوانین تطبیق طراحی کنترل کننده نیز بر اساس دو حالت وقوع و عدم وقوع حملات DoS انجام گرفته و در نهایت پایداری کلی بر این اساس بررسی می‌شود.

۳- طراحی ناظر تطبیقی

با توجه به کلاس سامانه های غیر خطی در نظر گرفته شده حالت‌های سامانه کاملاً قابل اندازه‌گیری نیستند و تنها دسترسی به خروجی سیستم وجود دارد و فرض می‌شود عیوب محرک و حسگر، همراه با اختلالات ناشناخته و حملات DoS و تزریق در سامانه وجود دارند. جهت مقابله با این چالش‌ها برای سامانه (۱۱)، یک ناظر به صورت زیر در طراحی می‌شود:

$$\begin{cases}\dot{\hat{\eta}}_i=\hat{\eta}_{i+1}+\hat{\zeta}_i^T\varphi_i(\hat{\bar{\eta}}_i)+k_ie^*-a^a{k_i}^0\hat{\eta}_1\\ \dot{\hat{\eta}}_n=\hat{\alpha}v+\hat{\zeta}_n^T\varphi_n(\hat{\bar{\eta}}_n)+k_ne^*-a^a{k_n}^0\hat{\eta}_1\\ y=\eta_1^*\end{cases} \quad (۱۲)$$

که درآن

$$\eta_1^*=\begin{cases}\hat{\eta}_1 & t\in\Sigma\\ \frac{1}{\hat{\beta}}y\triangleq\hat{s}y & t\in\Pi\end{cases},\ e^*=y^e-\hat{\eta}_1=\begin{cases}-\hat{\eta}_1 & t\in\Sigma\\ \hat{s}y-\hat{\eta}_1 & t\in\Pi\end{cases},\ a^a=\begin{cases}0 & t\in\Sigma\\ 1 & t\in\Pi\end{cases}$$

است و k_i پارامتر طراحی است.

اگر خطای تخمین بصورت $e=(e_1,e_2,\dots,e_n)^T=(\eta_1-\hat{\eta}_1,\dots,\eta_n-\hat{\eta}_n)^T$ تعریف شود. در نتیجه، با استفاده از (۱۱) و (۱۲) دینامیک خطا به صورت زیر ایجاد می شود:

$$\dot{e}=Ae+\Phi^T\tilde{Z}-K^0e_1-K^1a^ae^*+\triangle f+d^*+(\tilde{\alpha}v+\bar{u})\underline{I}_1, \quad (۱۳)$$

که در آن $a=1$ زمانی که $t\in\Pi$ است و $a=0$ زمانی که $t\in\Sigma$ و $\tilde{Z}=\left(\tilde{\zeta}_1^T,\dots,\tilde{\zeta}_n^T\right)^T, K^a=({k_1}^a,{k_2}^a,\dots,{k_n}^a)^T, \Phi^T=diag\{\varphi_1^T,\dots,\varphi_n^T,\}, \triangle f=(\triangle f_1,\triangle f_2,\dots,\triangle f_n)^T, d^*=\left(\varepsilon_1^f+d_1,\varepsilon_2^f+d_2,\dots,\varepsilon_n^f+d_n\right)^T, \underline{I}_1=(0,\dots,0,1)^T, \bar{I}_1=(1,0,\dots,0)^T, I_1=diag\{1,0,\dots,0\}, I_2=diag\{0,1,0,\dots,0\}, I_1^*=diag\{0,1,\dots,1\},$ و $A=\begin{pmatrix}0 & I\\ 0 & 0\end{pmatrix}$ است.

برای بررسی همگرایی ناظر، تحلیل پایداری به دو زمان فعال بودن حمله DoS (در Σ) و غیر فعال بودن حمله DoS (در Π) تقسیم می‌شود. بدین منظور یک تابع نامزد لیاپانوف بصورت زیر معرفی می کنیم:

$$V_0^a=\frac{1}{2}e^TMe+\frac{1}{2}\tilde{Z}^T(\Gamma)^{-1}\tilde{Z}+\frac{1}{3}|\tilde{\alpha}|^3+\frac{1}{3}|\tilde{s}|^3. \quad (۱۴)$$

۳-۱- فعال بودن حمله DoS

در این مرحله با فرض فعال بودن حمله DoS (در Σ)، مشتق (۱۴) نسبت به زمان بصورت زیر بدست می‌آید:

$$\dot{V}_0^0=e^TM^0[M^0A+\triangle f+\Phi^T\tilde{Z}-K^0e_1+d^*(t)+\tilde{\alpha}v+\bar{u}]-2\tilde{\Theta}^T\Gamma^{-1}\dot{\hat{\Theta}}-\tilde{\alpha}\dot{\hat{\alpha}}\text{sgn}(\tilde{\alpha})-\tilde{s}^2\dot{\hat{s}}\ \text{sgn}(\tilde{s}) \quad (۱۵)$$

با استفاده از نامساوی یانگ [۱۱] می‌توان نامساوی های زیر را بدست آورد:

$$\begin{aligned}&e^TM^0\Phi^T\tilde{Z}\le e^TI_1^*(M^0)^2I_1^*e+\tilde{Z}^T\tilde{Z}\\&+\eta_1^2\bar{I}_1^T(M^0)^2\bar{I}_1+e^*\bar{I}_1^TM^0\Phi^T\tilde{Z},\\&e^TM^0\triangle f\le\frac{1}{2}\varepsilon^T\left(\bar{l}+1\right)Me,\\&e^TM^0d^*\le e^T(M^0)^2e+(d^*)^Td^*,\\&e^TM^0(\tilde{\alpha}v+\bar{u})\underline{I}\le\frac{1}{2}e^TM^0\underline{I}_1\underline{I}_1^TM^0e+\tilde{\alpha}^2v^2+\bar{u}^2.\end{aligned} \quad (۱۶)$$

که در آن $\bar{l}=\max_i\left\{\left(l_i^f\right)^2\right\}, (d^*)^Td^*=\sum_{i=1}^{n}\left(\varepsilon_i^f+d_i\right)^2$ است.

با جایگذاری (۱۶) در (۱۵) نامساوی زیر حال حاصل می شود:

$$\dot{V}_0^1 \le \Big\{e^T\Big[(A-K^0C)^TM^0+(M^0)^2+ \quad (۱۷)$$
$$\frac{1}{2}M^0\underline{I}_1\underline{I}_1^TM^0+\frac{1}{2}\big(\bar{l}+1\big)M^0+I_1^*(M^0)^2I_1^*\Big]e+$$
$$\Big[-\tilde{Z}^T(\Gamma)^{-1}\hat{Z}+\tilde{Z}^T\tilde{Z}-\hat{\eta}_1\bar{I}_1^TM^0\Phi^T\tilde{Z}\Big]-\tilde{s}^2\hat{s}sgn(\tilde{s})-$$
$$\tilde{\alpha}^2\hat{\alpha}sgn(\tilde{\alpha})+\tilde{\alpha}^2v^2+\eta_1^2\bar{I}_1^T(M^0)^2\bar{I}_1+\frac{1}{2}(d^*)^Td^*+\bar{u}^2\Big\}$$

که در آن $C=(0,\dots,0,1)^T$ است. اکنون با توجه به (۱۷) می‌توانیم قوانین تطبیق را بصورت زیر معرفی کنیم:

$$\dot{\hat{Z}}=-e^*\Gamma\Phi M^a\bar{I}_1-\sigma\hat{Z},$$
$$\dot{\hat{\alpha}}=Proj_{[\underline{\alpha},1]}\{\mathcal{S}\}=\begin{cases}0, & \hat{\mathcal{A}}=\underline{\alpha}\text{ and }\mathcal{A}\le 0,\\ 0, & \hat{\mathcal{A}}=1\text{ and }\mathcal{A}\ge 0,\\ \mathcal{A}, & \text{Otherwise},\end{cases} \quad (۱۸)$$
$$\dot{\hat{s}}=Proj_{[\underline{s},\bar{s}]}\{\mathcal{S}\}=\begin{cases}0, & \hat{s}=\underline{s}\text{ and }\mathcal{S}\le 0,\\ 0, & \hat{s}=\bar{s}\text{ and }\mathcal{S}\ge 0,\\ \mathcal{S}, & \text{Otherwise},\end{cases}$$

که در آن $\mathcal{A}=-\frac{1}{2}(\lambda_\alpha)v^2-\lambda_1\hat{\alpha}$ و $\mathcal{S}=-\frac{1}{2}(\lambda_s)(\eta_1)^2-\lambda_2\hat{s}$ است و $\lambda_1,\lambda_2,\lambda_s,\lambda_\alpha>0$ پارامتر های طراحی اند.

تبصره ۱ –عملگر تصویر که با $Proj$ مشخص می‌شود، برای اطمینان از اینکه تخمین $\hat{\alpha}$ در بازه $[\underline{\alpha},1]$ و تخمین $\hat{s}$ در بازه $[\underline{s},\bar{s}]$ باقی می‌ماند، استفاده می‌شود. در نتیجه از آنجایی که $\dot{\hat{\alpha}}\le 0$، انتخاب $\hat{\alpha}(0)=1$ تضمین می‌کند که $\tilde{\alpha}\le 0$ همیشه برقرار است[۱۱].

مجدد با استفاده از نامساوی یانگ، نامساوی های زیر حاصل می شود:

$$-\tilde{Z}^T(\Gamma)^{-1}\hat{Z}+\tilde{Z}^T\tilde{Z}-\hat{\eta}_1\bar{I}^TM^0\Phi^T\tilde{Z}\le\frac{\sigma}{2}Z^T(\Gamma)^{-1}Z$$
$$+\Big(\frac{1}{\lambda_{\min}(\Gamma)^{-1}}-\frac{\sigma}{2}\Big)\tilde{Z}^T(\Gamma)^{-1}\tilde{Z},$$
$$-\tilde{\alpha}^2\hat{\alpha}\text{sgn}(\tilde{\alpha})+\tilde{\alpha}^2u^2\le\frac{1}{3}\lambda_1|\tilde{\alpha}|^3+\frac{1}{3}\lambda_1\alpha^3, \quad (۱۹)$$
$$-\tilde{s}^2\hat{s}\text{sgn}(\tilde{s})\le\frac{1}{3}(1-\lambda_2)|\tilde{s}|^3+\frac{1}{3}\lambda_2s^3$$
$$+\frac{1}{3}(\lambda_s(\hat{s}y)^2)^3.$$

و با جایگذاری (۱۹) در (۱۷) نامساوی زیر حاصل می شود:

$$\dot{V}_0^1\le\Big\{e^T\Big[(A-K^0C)^TM^0+(M^0)^2+ \quad (۲۰)$$
$$\frac{1}{2}M^0\underline{I}_1\underline{I}_1^TM^0+\frac{1}{2}\big(\bar{l}+1\big)M^0+I_1^*(M^0)^2I_1^*\Big]e-$$
$$\frac{1}{3}\lambda_1|\tilde{\alpha}|^3-\frac{1}{3}(1-\lambda_2)|\tilde{s}|^3+\Big(\frac{1}{\lambda_{min}(\Gamma)^{-1}}-\frac{\sigma}{2}\Big)\tilde{Z}^T(\Gamma)^{-1}\tilde{Z}+$$
$$\eta_1^2\bar{I}_1^T(M^0)^2\bar{I}_1+C_0^0\Big\},$$

که در آن $C_0^0=\frac{1}{3}\lambda_1\alpha^3+\frac{1}{3}\lambda_2s^3+\frac{\sigma}{2}Z^T(\Gamma)^{-1}Z+\frac{1}{2}(d^*)^Td^*+\bar{u}^2+\frac{1}{2}$ است.

آنالیز اولیه ناظر در زمان فعال بودن حمله DoS (در Σ) انجام گرفت و روابط تطبیقی برای تخمین عبارت های غیر خطی و ضرایب عیوب حسگر و عملگر بدست آمد با استفاده از این روابط تطبیقی مجدد مشتق زمانی V_0 در زمان غیر فعال بودن حمله DoS (در Π) بررسی می شود.

۲-۳- عدم فعال بودن حمله DoS

در این مرحله با توجه به اینکه $e^*=\hat{s}y-\hat{\eta}_1=b(t)\hat{s}\eta_1-\hat{\eta}_1$ $e_1+\omega(t)s\eta_1$ است f_i' در (۷) بصورت زیر اصلاح می‌شود:

$$f_i''=f_i'-\omega(t)s\eta_1 \quad (۲۱)$$

به طور مشابه، در اینجا نیز با استفاده FLS و (۱۸)، زمانی که حمله DoS غیر فعال است (در Π)، مشتق زمانی V_0 برابر است با:

$$\dot{V}_0^1\le\Big\{e^T\Big[(A-K^0C-K^1C)^TM^1+ \quad (۲۲)$$
$$\frac{1}{2}M^1K^1(K^1)^TM^1+(M^1)^2+\frac{1}{2}M^1\underline{I}_1\underline{I}_1^TM^1+\frac{1}{2}\big(\bar{l}+$$
$$1\big)M^1-M^1K^1\bar{I}_1^T+I_1^*(M^1)^2I_1^*\Big]e\Big[-\tilde{Z}^T(\Gamma)^{-1}\hat{Z}+\tilde{Z}^T\tilde{Z}-$$
$$\hat{\eta}_1\bar{I}_1^TM^1\Phi^T\tilde{Z}\Big]-\tilde{s}^2\hat{s}sgn(\tilde{s})-\tilde{\alpha}^2\hat{\alpha}sgn(\tilde{\alpha})+\tilde{\alpha}^2v^2+$$
$$\eta_1^2\bar{I}_1^T(M^1)^2\bar{I}_1+\frac{1}{2}\lambda_s(\hat{s}y)^2\tilde{s}^2+C_0^2\Big\}$$

که در آن $C_0^2=\frac{1}{2}(d^*)^Td^*+\bar{u}^2$ است.

با استفاده از نامساوی یانگ می توانیم نامساوی زیر را بدست آوریم:

$$-\tilde{s}^2\hat{s}\text{sgn}(\tilde{s})+\frac{1}{2}\lambda_s(\hat{s}y)^2\tilde{s}^2\le-\frac{1}{3}\lambda_2|\tilde{s}|^3+\frac{1}{3}\lambda_2s^3 \quad (۲۳)$$

در نهایت با در نظر گرفتن (۲۰) و (۲۳)، به نامساوی زیر می رسیم:

$$\dot{V}_0^1\le\Big\{e^T\Big[(A-K^0C-K^1C)^TM^1+ \quad (۲۴)$$
$$\frac{1}{2}M^1K^1(K^1)^TM^1+(M^1)^2+\frac{1}{2}M^1\underline{I}_1\underline{I}_1^TM^1-M^1K^1\bar{I}_1^T+$$
$$I_1^*(M^1)^2I_1^*+\frac{1}{2}\big(\bar{l}+1\big)M^1\Big]e+\Big(\frac{3}{2\lambda_{min}(\Gamma)^{-1}}-$$
$$\frac{\sigma}{2}\Big)\tilde{Z}^T(\Gamma)^{-1}\tilde{Z}-\frac{1}{3}\lambda_1|\tilde{\alpha}|^3-\frac{1}{3}\lambda_2|\tilde{s}|^3+\eta_1^2\bar{I}_1^T(M^1)^2\bar{I}_1+C_0^1\Big\}$$

که در آن $C_0^1=\frac{\sigma}{2}Z^T(\Gamma)^{-1}Z+\frac{1}{3}\lambda_1\alpha^3+\frac{1}{3}\lambda_2s^3+\frac{1}{2}(d^*)^Td^*+C_0^2$ است.

اکنون نامساوی (۲۰) برای زمان فعال بودن حمله و نامساوی (۲۴) برای زمان غیر فعال بودن حمله بدست آمده است. در ادامه جهت تکمیل آنالیز اولیه ناظر لازم است لم زیر معرفی و اثبات شود سپس کنترل کننده طراحی و در نهایت آنالیز نهایی پایداری انجام بگیرد.

لم ۱ –در بازه زمانی Π پایداری ناظر تطبیقی (۱۲) با ورودی $v(t)=0$ به همراه قوانین تطبیق (۲۱) تضمین می‌شود اگر مجموعه ای از ماتریس‌های قطعی مثبت M^0 و ماتریس‌های K^0 وجود داشته باشد که نامساوی زیر را برآورده کنند.

$$\frac{1}{2}M^0(A-K^0\bar{I}_1)+\frac{1}{2}(A-K^0\bar{I}_1)^TM^0+ \quad (۲۵)$$
$$\Big(\frac{\lambda_{max}(\Gamma)}{4\sigma}\Big)I_1^*(M^0)^2I_1^*<0$$

اثبات: با انتخاب تابع لیاپانوف $V=\Big\{\frac{1}{2}\hat{\eta}^TM^0\hat{\eta}+\frac{1}{2}\hat{Z}^T(\Gamma)^{-1}\hat{Z}$ و مشتق گیری آن نسبت به زمان بدست می‌آوریم:

$$\dot{V}=2\hat{\eta}^TM^0(A-K^0\bar{I}_1)\hat{\eta}+2\hat{\eta}^TM^0\Phi^T(\hat{\eta})\hat{Z}$$
$$+2\hat{Z}^T\Gamma^{-1}\big[-\Gamma\Phi(\hat{x})M^0I_1\hat{\eta}-\sigma\hat{Z}\big]s^3$$
$$=2\hat{\eta}^TM^0(A-K^0\bar{I}_1)\hat{\eta}$$
$$+\hat{\eta}^T\bar{I}_1M^0\Phi^T(\hat{\eta})\hat{Z}-2\sigma\hat{Z}^T\Gamma^{-1}\hat{Z}.$$

اکنون با استفاده از نامساوی یانگ داریم:

$$\dot{V}\le\hat{\eta}^T\Big[\frac{1}{2}M^0(A-K^0\bar{I}_1)+\frac{1}{2}(A-K^0\bar{I}_1)^TM^0+ \quad (۲۶)$$
$$\Big(\frac{\lambda_{max}(\Gamma_i)}{4\sigma_i}\Big)I_1^*(M^0)^2I_1^*\Big]\hat{\eta}.$$

بنابراین، شرط (۲۶) تضمین می‌کند که مشتق زمانی تابع لیاپانوف V قطعا منفی است، یعنی برای مقداری ثابت مثبت ϱ $\dot{V}\le-\varrho|\hat{\eta}|^2$ خواهد بود. این نشان می‌دهد که خطای تخمین $\hat{e}$ به طور مجانبی به صفر همگرا می‌شود که پایداری ناظر تطبیقی (۱۲) را با ورودی $v(t)=0$ تضمین می‌کند.

■

٤- طراحی کنترل کننده و آنالیز پایداری کلی

هدف ازطراحی کنترل کننده این است که خطای ردیابی در یک منطقه محدود در اطراف مبدا همگرا شود و در عین حال اطمینان حاصل

کنیم که سیگنال خروجی سامانه به طور دقیق یک تابع مرجع هموار y_r را ردیابی می‌کند. فرض بر این است که y_r و مشتقات آن در دسترس و محدود هستند.

$$\begin{aligned}&\dot{v}_i = -\frac{1}{\tau_i}v_i + \frac{1}{\tau_i}\alpha_{i-1}, v_i(0) = \alpha_{i-1}(0),\\ &z_1 = \eta_1 - y^r, z_i = \hat{\eta}_i - v_i,\\ &\xi_i = v_i - \alpha_{i-1}, i = 1,2,\dots,n,\end{aligned} \quad (۲۷)$$

در طراحی کنترل، α_i نشان دهنده سیگنال کنترل مجازی، v_i نشان دهنده سیگنال کنترل مجازی فیلتر شده است که با عبور α_i از یک فیلتر مرتبه اول بدست آمده است و τ_i پارامتر مثبت ثابت فیلتر مرتبه اول است. کنترل مجازی و ورودی کنترل با استفاده از عبارات زیر طراحی شده اند:

$$\begin{aligned}&\alpha_1 = -\hat{\zeta}_1^T\varphi_1(\hat{\eta}_1) + \dot{y}^r - p_1(\eta_1^* - y^r) - \widehat{w}_1^T\phi_1(\hat{\eta}_1),\\ &\alpha_i = -\hat{\zeta}_i^T\varphi_i(\hat{\eta}_i) - p_i z_i - k_i^v e_i^* + \dot{v}_i\\ &i = 2,\dots,n-1\\ &u = \frac{1}{\hat{\beta}}\left(-\hat{\zeta}_n^T\varphi_n(\hat{\eta}_n) - p_n z_n - k_n^a e^* + \dot{v}_n\right).\end{aligned} \quad (۲۸)$$

بدهی است در Σ، $\eta_1^* - y^r = -e_1 + z_1$ است در حالی که در Π، $\eta_1^* - y^r = \hat{s}y - \eta_1 + \eta_1 - y^r = -\tilde{s}y + z_1$ است. مشابه طراحی ناظر، روش طراحی کنترل به طور جداگانه برای دو بازه زمان Σ و Π تجزیه و تحلیل خواهد شد. اجازه دهید ابتدا بازه Σ را در نظر بگیریم.

مرحله ۱: در این مرحله یک تابع لیاپانوف را به صورت $V_1 = \frac{1}{2b(t)}z_1^2$ انتخاب می‌کنیم. از این رو داریم:

$$\dot{V}_1 = -\tilde{s}^2 z_1(z_2 + e_2 + \xi_2 + \alpha_1 + f' + \frac{d_1}{b(t)} + f^* - \dot{y}^r) - \frac{1}{\gamma_1}\tilde{w}_1^T\hat{w}_1. \quad (۲۹)$$

اگر $f' - \frac{f_1(\bar{\eta}_1)}{b(t)} - \frac{z_1 b(t)}{2b^2(t)}$ را تعریف کنیم، با استفاده از FLS برای تقریب تابع f^* بصورت زیر می توان استفاده کرد:

$$f^* = w_1^{*T}\phi_1(\bar{\eta}) + \zeta_1,$$

که در آن w_1^* بردار وزن دهی بهینه است، $\phi_1(\bar{\eta})$ تابع پایه فازی است، و ζ_1 خطای تقریبی برآورده کننده $|\zeta_1| \le \bar{\zeta}_1$ است. در نتیجه رابطه زیر حاصل می شود:

$$z_1\left(z_2 + e_2 + \xi_2 + \alpha_1 + \hat{\zeta}_1^T\varphi_1(\hat{\eta}_1) + \varepsilon_1^f + \Delta f_1 + d_1 - \dot{y}^r + \tilde{\zeta}_1^T\varphi_1(\hat{\eta}_1)\right) - \frac{1}{\gamma_1}\tilde{w}_1^T\hat{w}_1. \quad (۳۰)$$

با استفاده از نامساوی یانگ نامساوی های زیر بدست می آید:

$$z_1\left(z_2 + \xi_2 + \varepsilon_1^f + e_2\right) \le 4z_1^2 + \frac{1}{4}(z_2^2 + \xi_2^2 + e_2^2 + \varepsilon_1^2),$$

$$z_1\tilde{\zeta}_1^T\varphi_1(\hat{\eta}_1) \le z_1^2 + \frac{1}{2}\tilde{\zeta}_1^T\tilde{\zeta}_1,$$

$$z_1\frac{d_1(t)}{b(t)} \le z_1^2 + \frac{\|\bar{d}\|^2}{\|\underline{b}\|^2},$$

$$z_1\Delta f_1 \le z_1^2 + \frac{1}{2}\left(l_1^f\right)^2 e_1^2 - p_1 z_1\hat{x}_1 \le -p_1 z_1^2 + \frac{1}{2}\left(l_1^f\right)^2 e_1^2$$

$$p_1 e_1 z_1 \le \frac{e_1^2}{2} + \frac{p_1^2 z_1^2}{2}$$

سپس با جایگزینی نامساوی های بالا و (۳) و (۲۸) در (۳۰)، می‌توان به رابطه و در نهایت نامساوی زیر رسید:

$$\dot{V}_1 = \{z_1\left(z_2 + e_2 + \xi_2 + \varepsilon_1^f + \Delta f_1 + \omega_1 - p_1(-e_1 + z_1)\right) + z_1\tilde{\zeta}_1^T\varphi_1 - \frac{1}{\gamma_1}\tilde{w}_1^T\hat{w}_1\} \le [w_1^{*T}\phi_1(\bar{\eta}) + \widehat{w}_1^T\phi_1(\eta_1^*) + \tilde{w}_1^T\phi_1(\eta_1^*) - w_1^{*T}\phi_1(\eta_1^*)] + \left\{\left(7 - p_1 + \frac{1}{2}p_1^2\right)z_1^2 + \frac{1}{4}z_2^2 + \frac{1}{4}\xi_2^2 + \left(\frac{1}{2} + \frac{1}{2}\left(l_1^f\right)^2\right)\varepsilon_1^2 + \frac{1}{4}\varepsilon_2^2 + \frac{1}{4}\tilde{Z}^T\tilde{Z} + \frac{1}{4}\left(\varepsilon_1^f\right)^2 + \frac{\|\bar{d}\|^2}{\|\underline{b}\|^2}\right\}.$$

مجدد با استفاده از نامساوی یانگ نامساوی های زیر را بدست می آوریم:

$$z_1[w_1^{*T}\phi_1(\bar{\eta}) - w_1^{*T}\phi_1(\eta_1^*)] \le 2p_1 z_1^2 + \frac{l}{2p_1}w_1^{*T}w_1^*,$$

$$z_1\tilde{w}_1^T\phi_1(\hat{\eta}_1) - \hat{x}_1\tilde{w}_1^T\phi_1(\eta_1^*) \le \frac{1}{2}\varepsilon_1^2 + \frac{l}{2}\tilde{w}_1^T\tilde{w}_1.$$

حال، اگر یک قانون تطبیقی جدید را به صورت زیر در نظر بگیریم:

$$\dot{\widehat{w}}_1 = \gamma_1\eta_1^*\phi_1(\eta_1^*) - \sigma_1\widehat{w}_1. \quad (۳۲)$$

در نتیجه با جاگذاری ۳۲ در ۳۱ نامساوی زیر حاصل می‌شود:

$$\dot{V}_1 \le \left\{\left(7 + p_1 + \frac{1}{2}p_1^2\right)z_1^2 + \frac{1}{4}z_2^2 + \frac{1}{4}\xi_2^2 + \left(\frac{1}{2} + \frac{1}{2}\left(1 + \left(l_1^f\right)^2\right)\right)\varepsilon_1^2 + \frac{1}{4}\varepsilon_2^2 + \frac{1}{4}\tilde{Z}^T\tilde{Z} + \frac{1}{4}\left(\varepsilon_1^f\right)^2 + \frac{\|\bar{d}\|^2}{\|\underline{b}\|^2} + \left(\frac{l}{2} - \frac{\sigma_1}{2\gamma_1}\right)\tilde{w}_1^T\tilde{w}_1 + \left(\frac{\sigma_1}{2\gamma_1} + \frac{l}{p_1}\right)w_1^{*T}w_1^*\right\}. \quad (۳۳)$$

مرحله ۲: در این مرحله تابع لیاپانوف را به صورت $V_2 = \left\{\frac{1}{2}z_2^2 + \frac{1}{2}\xi_2^2\right\}$ انتخاب می‌کنیم. حال، با مشتق گرفتن از V_2 نسبت به زمان در امتداد دینامیک ناظر تطبیقی (۱۲) و استفاده از نامساوی یانگ و جایگزینی (۲۷) در آن، رابطه زیر را به دست می‌آوریم:

$$\dot{V}_2 = \left\{(-p_2 + 2)z_2^2 + \frac{1}{4}z_3^2 + \frac{1}{4}\xi_3^2 + \left(-\frac{1}{\tau_2}\xi_2 - \dot{\alpha}_1\right)\xi_2\right\} \quad (۳۴)$$

همانطور که در (۲۸) مشاهده می‌شود، α_1 تابعی است که قبلاً شناخته شده است. بنابراین، با توجه به یک مجموعه فشرده دقیق Ω، یک M_2 ثابت وجود دارد که $\frac{1}{2}|\dot{\alpha}_1|^2 \le M_2$ است. از این رو می‌توان نتیجه گرفت که نامساوی زیر برقرار است.

$$\dot{V}_2 \le \left\{(-p_2 + 2)z_2^2 + \frac{1}{4}z_3^2 + \frac{1}{4}\xi_3^2 + \left(-\frac{1}{\tau_2} + M_2\right)\xi_2^2 + \frac{1}{2}\right\}. \quad (۳۵)$$

مرحله i ام: مشابه قبل برای این مرحله نیز یک تابع لیاپانوف را به صورت $V_i = \left\{\frac{1}{2}z_i^2 + \frac{1}{2}\xi_i^2\right\}$ انتخاب می‌کنیم. مجدد با مشتق گرفتن V_i نسبت به زمان در امتداد دینامیک ناظر تطبیقی (۱۲) و جایگزینی (۲۷) در آن منجر به نامساوی زیر می‌شود:

$$\dot{V}_i \le \left\{(-p_i + 2)z_i^2 + \frac{1}{4}z_{i+1}^2 + \frac{1}{4}\xi_{i+1}^2 + \left(-\frac{1}{\tau_i} + M_i\right)\xi_i^2 + \frac{1}{2}\right\}. \quad (۳۶)$$

مرحله n ام: در این مرحله نیز یک تابع لیاپانوف را به صورت $V_n = \left\{\frac{1}{2}z_n^2 + \frac{1}{2}\xi_n^2\right\}$ انتخاب می‌کنیم، اگر V_n را در امتداد (۱۲) نسبت به زمان مشتق بگیریم و با استفاده از (۲۸) به طور همزمان، نامساوی زیر به دست می‌آید.

$$\dot{V}_n \le \left\{-p_n z_n^2 + \left(-\frac{1}{\tau_n} + M_n\right)\xi_n^2 + \frac{1}{2}\right\}. \quad (۳۷)$$

اکنون پس استخراج نامساوی های کنترل کننده لازم است تابع کلی لیاپانوف به صورت تعریف شود:

$$V = \frac{1}{2}\varepsilon^T M\varepsilon + \frac{1}{2}\tilde{Z}^T(\Gamma)^{-1}\tilde{Z} + \frac{1}{3}|\tilde{\alpha}|^3 + \frac{1}{3}|\tilde{s}|^3 + \sum_{i=0}^n V_i \quad (۳۸)$$

توجه شود که:

$$\eta_1^2\bar{I}_1^T M^2\bar{I}_1 = (z_1 + y^r)^2\bar{I}_1^T M^2\bar{I}_1 \le 2(z_1^2 + (y^r)^2)\bar{I}_1^T M^2\bar{I}_1.$$

اکنون در زمان فعال بودن حمله DoS یعنی بازه ی Σ ، $\dot{V}$ نهایی بصورت زیر مشخص می‌شود:

$$\dot{V} \le e^T \Big[(A-K^0C)^TM^0+(M^0)^2+ \quad (۳۹)$$
$$\tfrac{1}{2}M^0\underline{I}_1\underline{I}_1^TM^0+\tfrac{1}{2}\big(\bar{l}+1\big)M^0+\tfrac{1}{4}I_2+\Big(\tfrac{1}{2}+\tfrac{1}{2}\big(l_1^f\big)^2\Big)I_1+$$
$$I_1^*(M^0)^2I_1^*\Big]e+\Big(\tfrac{3}{2\lambda_{min}(\Gamma)^{-1}}-\tfrac{\sigma}{2}\Big)\tilde{Z}^T(\Gamma)^{-1}\tilde{Z}-\tfrac{1}{3}\lambda_1|\tilde{\alpha}|^3-$$
$$\tfrac{1}{3}(1-\lambda_2)|\tilde{s}|^3+\Big(\tfrac{l}{2}-\tfrac{\sigma_1}{2\gamma_1}\Big)\widetilde{w}_1^T\widetilde{w}_1+\textstyle\sum_{i=2}^{n}\Big(-\tfrac{1}{\tau_i}+M_i+$$
$$\tfrac{1}{4}\Big)\xi_i^2+\Big(7+p_1+\tfrac{1}{2}p_1^2+\bar{I}_1^T(M^0)^2\bar{I}_1\Big)z_1^2+\textstyle\sum_{i=2}^{n-1}\Big(-p_i+$$
$$\tfrac{9}{4}\Big)z_i^2+\Big(-p_n+\tfrac{1}{4}\Big)z_n^2+C_0\}$$

که در آن

$$C_0=C_0^1+\frac{n-1}{2}+(y^r)^2\bar{I}_1^T(M^0)^2\bar{I}_1+\frac{1}{2}\big(\varepsilon_1^f+d_1\big)^2+\frac{\|\bar{d}\|^2}{\|\underline{b}\|^2}+\Big(\frac{\sigma_1}{2\gamma_1}+\frac{l}{p_1}\Big)w_1^{*T}w_1^*$$

است. مشابه قبل در زمان غیر فعال بودن حمله DoS بازه ی Π، $\dot{V}$ نهایی بصورت زیر بدست می‌آید:

$$\dot{V} \le \Big\{e^T\Big[(A-K^0C-K^1C)^TM^1+ \quad (۴۰)$$
$$\tfrac{1}{2}M^1K^1(K^1)^TM^1+(M^1)^2+\tfrac{1}{2}M^1\underline{I}_1\underline{I}_1^TM^1-M^1K^1\bar{I}_1^T+$$
$$\tfrac{1}{4}I_2+I_1^*(M^1)^2I_1^*+\tfrac{1}{2}\big(\bar{l}+1\big)M^1\Big]e+\Big(\tfrac{3}{2\lambda_{min}(\Gamma)^{-1}}-$$
$$\tfrac{\sigma}{2}\Big)\tilde{Z}^T(\Gamma)^{-1}\tilde{Z}-\tfrac{1}{3}\lambda_1|\tilde{\alpha}|^3-\tfrac{1}{3}\lambda_2|\tilde{s}|^3-\tfrac{\sigma_1}{2\gamma_1}\widetilde{w}_1^T\widetilde{w}_1+$$
$$\textstyle\sum_{i=2}^{n}\Big(-\tfrac{1}{\tau_i}+M_i+\tfrac{1}{4}\Big)\xi_i^2+(7+p_1+\bar{I}_1^T(M^1)^2\bar{I}_1)z_1^2+$$
$$\textstyle\sum_{i=2}^{n-1}\Big(-p_i+\tfrac{9}{4}\Big)z_i^2+\Big(-p_n+\tfrac{1}{4}\Big)z_n^2+C_1\Big\}$$

که در آن

$$C_1=C_0^1+\frac{n-1}{2}+(y^r)^2\bar{I}_1^T(M^1)^2\bar{I}_1+\frac{1}{2}\big(\varepsilon_1^f+d_1\big)^2+\frac{1}{6}\Big(\Big(\frac{p_1^6}{l_2}\Big)(y)^6\Big)^3+\Big(\frac{\sigma_1}{2\gamma_1}+\frac{l}{p_1}\Big)w_1^{*T}w_1^*$$

است.

با توجه به هدف کنترل، کرانهای بالای $\frac{\delta}{2}$ و $-\frac{\gamma}{2}$ را به ترتیب برای ضرایب متغیرهای خطا در (۳۹) و (۴۰) در نظر می‌گیرد. علاوه بر این، ماتریس‌های مربوطه باید شرایط خاصی را داشته باشند که در زیر ذکر شده است:

$$(A-K^0C)^TM^0+(M^0)^2+\tfrac{1}{2}M^0\underline{I}_1\underline{I}_1^TM^0+ \quad (۴۱)$$
$$+\tfrac{1}{2}\big(\bar{l}+1\big)M^0+\tfrac{1}{2}I_2\Big(\tfrac{1}{2}+\tfrac{1}{2}\big(l_1^f\big)^2\Big)I_1+I_1^*(M^0)^2I_1^*\le\tfrac{\delta}{2}M^0$$
$$7+p_1+\tfrac{1}{2}p_1^2+\bar{I}_1^T(M^0)^2\bar{I}_1\le\tfrac{\delta}{2} \quad (۴۲)$$
$$(A-K^0C-K^1C)^TM^1+\tfrac{1}{2}M^1K^1(K^1)^TM^1+ \quad (۴۳)$$
$$(M^1)^2+\tfrac{1}{2}M^1\underline{I}_1\underline{I}_1^TM^1-M^1K^1\bar{I}_1^T+I_1^*(M^1)^2I_1^*+$$
$$\tfrac{1}{2}\big(\bar{l}+1\big)M^1+\tfrac{1}{4}I_2\le-\tfrac{\gamma}{2}M^1,$$
$$7+p_1+\bar{I}_1^T(M^1)^2\bar{I}_1\le-\tfrac{\gamma}{2} \quad (۴۴)$$
$$\begin{aligned}&\tfrac{3}{2\lambda_{\min}(\Gamma_i)^{-1}}-\tfrac{\sigma}{2}\le-\tfrac{\gamma}{2}\\&-\lambda_1\le-\gamma,\quad(1-\lambda_2)\le\delta\\&\Big(\tfrac{1}{1}-\lambda_2\Big)\le-\gamma,\\&-\tfrac{1}{\tau_i}+M+\tfrac{1}{4}\le-\tfrac{\gamma}{2},\\&-p_i+\tfrac{9}{4}\le-\tfrac{\gamma}{2},\quad-p_n+\tfrac{1}{4}\le-\tfrac{\gamma}{2}.\end{aligned} \quad (۴۵)$$

علاوه بر این، فرض می‌شود که یک ثابت Λ وجود دارد به طوری که نامساوی های زیر برقرار باشد:

$$M^0\le\Lambda M^1,\ \ M^1\le\Lambda M^0,\ \ \tfrac{\gamma-\lambda_*}{\delta+\gamma}>\tfrac{1}{T},\ \lambda_*>\tfrac{\ln\Lambda}{\tau_D}. \quad (۴۶)$$

قضیه ۱ – با فرض شرایط ۱–۳ برای سامانه شرح داده شده در (۱)، همراه با ورودی کنترل و ورودی مجازی در (۲۸)، ناظر در (۱۲) و قانون تطبیقی در (۲۱) و (۳۲) می‌توان ردیابی سیگنال‌های مرجع و همگرایی سیگنال‌های خطا به ناحیه ی کوچکی از مبدا را برای همه خروجی‌های سامانه با انتخاب ماتریس‌های مثبت- معین M^0 و M^1، ماتریس‌های K^0 و K^1 و پارامترهایی که شرایط (۴۱) تا (۴۶) را برآورده می‌کنند، تضمین کرد.

اثبات: تحت شرایط (۴۱–۴۵) می‌توان بدست آورد:

$$\dot{V}\le\vartheta(t)V+D, \quad (۴۷)$$

که در آن D یک ثابت است و $\vartheta(t)$ یک تابع سوئیچ شونده است که در بازه‌های زمانی مختلف تغییر می‌کند. به طور خاص، در بازه Π، $\vartheta(t)$ مقدار δ را می‌گیرد، در حالی که در بازه Σ، مقدار $-\gamma$ را می‌گیرد. در یک لحظه $t\in[t_i,t_{i+1})$، با استفاده از (۴۶) و (۴۷)، داریم:

$$\begin{aligned}V(t)&\le e^{\vartheta(t-t_i)}V(t_i^+)+D\int_{t_i}^{t}e^{\vartheta(t-\tau)}d\tau\\&\le\Lambda e^{\vartheta(t-t_i)}V(t_i^-)+D\int_{t_i}^{t}e^{\vartheta(t-\tau)}d\tau\end{aligned} \quad (۴۸)$$

توجه داشته باشید که $t_i^-\in[t_{i-1},t_i)$ و ما می‌توانیم نامساوی زیر را با اعمال همان رویه مورد استفاده برای (۴۸) بدست آوریم:

$$V(t_i^-)\le\Lambda e^{\vartheta(t_i^--t_{i-1})}V(t_{i-1}^-)+D\int_{t_{i-1}}^{t_i^-}e^{\vartheta(t_i^--\tau)}d\tau \quad (۴۹)$$

با انجام رویه مشابه در هر بازه $[t_k,t_{k+1}),k=0,1,\dots$ و با در نظر گرفتن فرض ۳ و (۴۶)، نامساوی زیر به دست می‌آید:

(۴۰)

$$\begin{aligned}&V(t)\\&\le\Lambda^{n(0,t)}e^{\vartheta(t-t_i)+\vartheta(t_i-t_{i-1})+\cdots+\vartheta(t_1-0)}V(0)\\&+D\int_0^{t_1}\Lambda^{n(t_1,t)}e^{\vartheta(t-t_i)+\vartheta(t_i-t_{i-1})+\cdots+\vartheta(t_1-\tau)}d\tau+\cdots\\&+D\int_{t_i}^{t}e^{\vartheta(t-\tau)}d\tau\\&\le\Lambda^{n(0,t)}e^{-[\gamma|\Sigma(0,t)|-\delta|\Pi(0,t)|]}V(0)\\&+D\int_0^{t_1}\Lambda^{n(\tau,t)}e^{-[\gamma|\Sigma(0,t)|-\delta|\Pi(0,t)|]}d\tau+\cdots\\&+D\int_{t_i}^{t}e^{-[\gamma|\Sigma(0,t)|-\delta|\Pi(0,t)|]}d\tau\\&=\Lambda^{n(0,t)}e^{-[\gamma|\Sigma(0,t)|-\delta|\Pi(0,t)|]}V(0)\\&+D\int_0^{t}\Lambda^{n(\tau,t)}e^{-[\gamma|\Sigma(0,t)|-\delta|\Pi(0,t)|]}d\tau\\&\le e^{-[\gamma|\Sigma(0,t)|-\delta|\Pi(0,t)|-n(0,t)ln\Lambda]}V(0)\\&+D\int_0^{t}e^{-[\gamma|\Sigma(0,t)|-\delta|\Pi(0,t)|-n(\tau,t)ln\Lambda]}d\tau\\&\le\Lambda^{\nu}\left(e^{-\epsilon t}V(0)+D\int_0^{t}e^{-\epsilon(t-\tau)}d\tau\right)\\&\le\Lambda^{\nu}\left(e^{-\epsilon t}V(0)+\frac{D}{\epsilon}\right).\end{aligned}$$

که در آن $\epsilon > 0$ یک ثابت است که تضمین کننده رابطه $(n(\tau-t)-\nu)\ln\mu + \epsilon(t-\tau) < \lambda_*(t-\tau)$ است. علاوه بر این، استخراج $\dot{V}(t) \le -\epsilon V(t) + D$ ساده است. این بدان معناست که اگر $\epsilon > \frac{D}{q}$، $V(t) \le q$ یک مجموعه ثابت است.

■

در نهایت برای به دست آوردن بهره‌های ناظر که شرایط مربوط به (۲۶)، (۴۱)، (۴۲)، (۴۳)، و (۴۴) را برآورده می‌کند، باید مجموعه ای از LMIها را حل کرد.

$$
\begin{bmatrix} \Psi_1 & * \\ q_1 M^0 I_1^* & -I \end{bmatrix} < 0
$$
$$
\begin{bmatrix} \Psi_2 & * & * & * \\ M^0 & -I & * & * \\ q_2 \underline{I}_1^T M^0 & 0 & -I & * \\ q_3 M^0 I_1^* & 0 & 0 & -I \end{bmatrix} < 0,
$$
$$
\begin{bmatrix} \Psi_3 & * \\ q_3 \bar{I}_1 M^0 & -I \end{bmatrix} < 0,
$$
$$
\begin{bmatrix} \Psi_4 & * & * & * & * \\ q_3 M^1 & -I & * & * & * \\ q_2 I_1^T M^1 & 0 & -I & * & * \\ q_2 (K^1)^T M^1 K^1 & 0 & 0 & -I & * \\ q_2 M^0 I_1^* & 0 & 0 & 0 & -I \end{bmatrix} < 0 \qquad (۵۱)
$$
$$
\begin{bmatrix} \Psi_5 & * \\ q_3 \bar{I}_1 M^1 & -I \end{bmatrix} < 0
$$

که در آن

$$
\Psi_1 = \frac{1}{2} He\{M^0(A - K^0 \bar{I}_1)\},
$$
$$
\Psi_2 = \frac{1}{2} He\{M^0(A - K^0 C)\} + \frac{1}{2}(\bar{l}+1)M^0 + \left(\frac{1}{2} + \frac{1}{2}\left(l_1^f\right)^2\right) I_1 + \frac{1}{2} I_1 + \frac{1}{4} I_2 - \frac{\delta}{2} M^0,
$$
$$
\Psi_3 = 7 + p_1 + \frac{1}{2} p_1^2 - \frac{\delta}{2},
$$
$$
\Psi_4 = \frac{1}{2} He\{M^1(A - K^0 C - K^1 C)\} + \frac{1}{2}(\bar{l}+1)M^1 I_1 + \frac{1}{2} I_2 + \frac{\gamma}{2} M^1,
$$
$$
\Psi_5 = 7 + p_1 + \bar{I}_1^T (M^1)^2 \bar{I}_1 + \frac{\gamma}{2}, \quad q_1 = \sqrt{\frac{\lambda_{\max}(\Gamma)}{4\sigma}}, \; q_2 = \sqrt{\frac{1}{2}}, \; q_3 = \sqrt{2}.
$$

است.

نکته ۱ – در مقایسه با [۱۱،۱۶]، در این مقاله نیازی به حل بی نهایت LMI وجود ندارد بلکه تنها یک مجموعه از LMIها نیاز به حل غیربرخط دارند، یعنی بهره ناظر نیازی به به روز رسانی برخط ندارد و بصورت غیربرخط تنها یکبار و مستقل از شرایط ایجاد شده در طول راه اندازی سامانه محاسبه می‌شود. از آنجایی که عبارت جبرانی $a^a {k_i}^0(-\hat{\eta}_1)$ به ناظر (۱۲) اضافه شده است، هیچ عبارت متغیر با زمانی در LMIها وجود ندارد در نتیجه محاسبه ی یکباره LMIها کافی است. این طراحی تا حد زیادی در توان و بار محاسباتی صرفه جویی می کند.

نکته ۲ – همانطور که در [۱۰،۳۰] بحث شده است، $\frac{1}{T} < 1$ حد بهینه شدت حمله قابل تحمل تحت مفروضات ۴-۵ است. سپس، افزایش γ یا کاهش δ می‌تواند شدت حمله DoS قابل تحمل را بهبود بخشد. با این حال، به دلیل محدودیت حل LMIها، انتخاب γ بسیار بزرگ یا δ بسیار کوچک امکان پذیر نیست. بنابراین، انتخاب پارامترها باید مناسب باشد. علاوه بر این، با افزایش p_i یا کاهش τ_i، عملکرد کنترل و شدت حمله قابل تحمل می‌تواند بهبود یابد، اما افزایش زیاد p_i یا τ_i بسیار کوچک می‌تواند منجر به افزایش تلاش و انرژی کنترلی شود. بنابراین، پارامترهای طراحی را می‌توان برای دستیابی به مصالحه بین شدت حمله DoS قابل تحمل، نرخ استفاده از منابع ارتباطی، عملکرد کنترل و انرژی کنترل انتخاب کرد.

۵- نتایج شبیه‌سازی

در این بخش، اثربخشی کنترل پیشنهادی را از طریق یک مثال عددی نشان می‌دهیم. یک سامانه غیرخطی نامشخص با کنترل مبتنی بر شبکه را مطابق با [۳۱] در نظر بگیرید:

$$
\begin{aligned} \dot{x}_1 &= x_2 + f_1(x_1) + d_1(x,t) \\ \dot{x}_2 &= u + f_2(x_2) + d_2(x,t) \\ y &= x_1 \end{aligned} \qquad (۵۶)
$$

که در آن $f_1(x_1) = 0.5\sin(0.5x_1)$، $f_2(x_2) = 0.5\sin(0.5x_1 + 0.5x_2)$ و $d_1(x,t) = 0.5\sin(2t)$، $d_2(x,t) = -0.5\cos(0.2t)$ است.

سیگنال مرجع $y_r(t) = \sin(t)$ است. عیب محرک در شروع شبیه سازی با از دست دادن نرخ اثربخشی کنترل $\alpha = 0.8$ و عیب بایاس $u^o(t) = e^{-2t}$ و عیب حسگر در شروع شبیه سازی $\beta = 0.75$ در ثانیه ۶ به $\beta = 0.5$ تغییر می‌کند. پارامترهای حمله $T_{n1} = 3.0$ و $T_{n2} = 5.0$ هستند. حملات تزریقی به صورت $\omega(t) = -0.5\sin(2t)\cos(t)$ داده می‌شود. پارامترهای طراحی شده را به صورت

$\delta = 10, \Lambda = 580, \gamma = 5$ انتخاب می‌کنیم. با محاسبه می‌توانیم به دست آوریم که $\lambda^* > \ln\Lambda/T_{n1} = 6.36301/3.0 = 2.1210$، $\lambda^* < \gamma - (\gamma+\delta)/T_{n2} = 2.5$ است. انتخاب توابع عضویت فازی به شرح زیر انجام می‌شود.

$$
\mu_i^f = \exp\left[-\frac{(x_1 + 2 - l)^2}{6}\right] \times \prod_{i=2}^{3} \exp\left[-\frac{(x_i - 20l)^2}{600}\right]
$$

با حل LMIهای (۵۱)، نتایج شبیه سازی ارائه شده در شکل‌های ۲ تا ۵ به دست می‌آید.

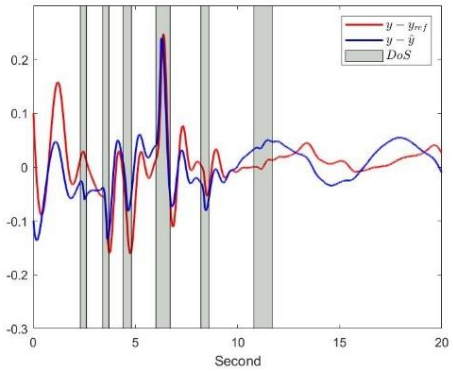
با توجه به شکل ۲ در طول حمله DoS، مدت زمان کوتاهی پس از توقف حمله عملکرد ردیابی سامانه بازیابی می شود ودر طول حمله سامانه به مرز ناپایداری نمی رسد. درنهایت خطای ردیابی و تخمین به یک منطقه کوچک در اطراف مبدا همگرا می‌شود. علاوه بر این، شایان ذکر است که همزمان با حمله DoS، حملات تزریقی عیوب حسگر و محرک نیز در سامانه رخ می‌دهد.

در شکل ۳ رفتار سیگنال کنترل در هنگام حملات و عیوب در سامانه به تصویر کشیده شده است.

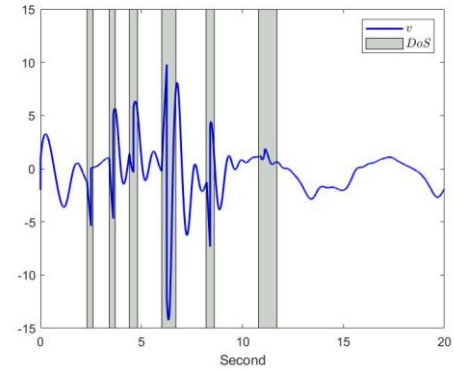
همچنین شکل ۴ نشان می‌دهد که پارامترهای عیوب محرک و حسگر به طور موثر شناسایی شده‌اند و مقادیر آنها در محدوده قابل قبولی قرار گرفته‌اند. تخمین پارامتر عیب حسگر و محرک به دلیل حمله DoS و تزریق و همچنین حضور اغتشاش ناشناخته دارای خطای جزئی است، با این حال نتایج در محدوده مناسبی قرار دارند و این خطای محدود تأثیری بر عملکرد ردیابی و تخمین کلی سامانه ندارد.

در شکل ۵ سیگنال تخمین حالت خروجی کنترل ایمن تحمل پذیر عیب (SFTC) پیشنهادی با کنترل تطبیقی توزیع شده (DAC) [۲۷] مقایسه شده است. مطابق با آن مشاهده می شود روش SFTC پیشنهادی

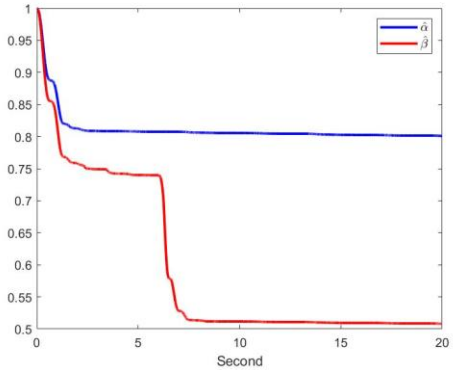
با توجه به تفاوت اصلی طراحی ناظر بالاخص در زمان عدم حضور حمله DoS با روش DAC از خطای ماندگار کمتری برخوردار است. با توجه به اینکه روش پیشنهادی در [۲۷] در حضور عیوب چندگانه عملکرد مناسبی ندارد جهت مقایسه بهتر در این بخش شبیه سازی عیب در نظر گرفته نشده است.



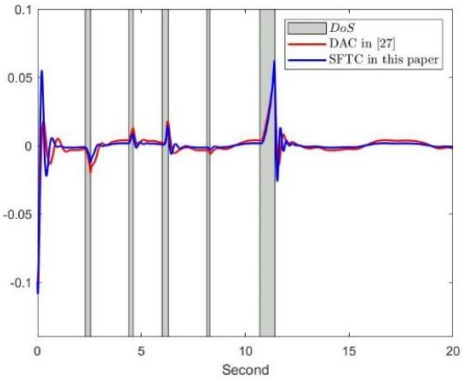
شکل ۱: سیگنال خطای ردیابی و تخمین خروجی سامانه در حضور حمله DoS و تزریق



شکل ۲: سیگنال کنترل سامانه در حضور حمله DoS و تزریق



شکل ۳: سیگنال تخمین پارامترهای عیب حسگر و محرک



شکل ۴: مقایسه خطای تخمین روش پیشنهادی با روش ارائه شده در [۲۷]

٦- نتیجه‌گیری

در این مقاله، رویکرد پیشنهادی "کنترل ردیابی خروجی-بازخورد تطبیقی تحمل پذیر عیب ایمن" یک راه حل انعطاف‌پذیر و موثر برای رسیدگی به چالش‌های پیچیده مرتبط با طبقه ای از سامانه‌های غیرخطی نامشخصکه در معرض عیوب حسگر و محرک و همچنین تهدیدات سایبری بالقوه منجمله DoS و تزریق می باشند، را نشان می‌دهد. رویکرد پیشنهادی ما با بهره‌گیری از یک ناظر بهره سوئیچ شونده، نه تنها کنترل ردیابی قوی را تضمین می‌کند، بلکه تاب آوری مناسبی را در برابر تهدیدات سایبری مهیا می‌کند. ادغام یک استراتژی کنترل ردیابی تطبیقی تحمل‌پذیر عیب تطبیقی با یک سیستم فازی و روش مبتنی بر ناظر سوئیچ شونده، امکان تنظیم پارامترهای دینامیکی را برای تطبیق با عدم قطعیت‌های سامانه و مقابله با اغتشاشات، عیوب و حملات سایبری همزمان را فراهم می‌کند. نتایج شبیه‌سازی بر روی یک سامانه غیرخطی نمونه، کارایی روش پیشنهادی را تأیید می‌کند و توانایی آن را برای حفظ پایداری سامانه، دستیابی به عملکرد ردیابی مطلوب و تاب آوری قوی در برابر حملات سایبری نشان می‌دهد. رویکرد ارائه شده نه تنها به چالش‌های مطرح شده می‌پردازد، بلکه زمینه را برای پیشرفت‌های بیشتر در توسعه استراتژی‌های کنترل تطبیقی و ایمن منعطف برای سامانه های متصل به هم و چند عامله را فراهم می‌کند.

مراجع

[1] B. Aboutalebian, H. A. Talebi, S. Etedali, and A. A. Suratgar, “Adaptive control of teleoperation system based on nonlinear disturbance observer,” European Journal of Control, vol. 53, pp. 109–116, May 2020, doi: https://doi.org/10.1016/j.ejcon.2019.10.002.

[2] L. Peng, X. Cao, C. Sun, Y. Cheng, and S. Jin, “Energy efficient jamming attack schedule against remote state estimation in wireless cyber-physical systems,” *Neurocomputing*, vol. 272, pp. 571–583, Jan. 2018, doi: https://doi.org/10.1016/j.neucom.2017.07.036.

Sciences, vol. 65, no. 6, May 2022, doi: https://doi.org/10.1007/s11432-021-3397-2.

[13] L. Zhang and G.-H. Yang, "Observer-Based Adaptive Decentralized Fault-Tolerant Control of Nonlinear Large-Scale Systems With Sensor and Actuator Faults," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 10, pp. 8019–8029, Oct. 2019, doi: https://doi.org/10.1109/tie.2018.2883267.

[14] L. Zhao and G.-H. Yang, "Adaptive fault-tolerant control for nonlinear multi-agent systems with DoS attacks," *Information sciences*, vol. 526, pp. 39–53, Jul. 2020, doi: https://doi.org/10.1016/j.ins.2020.03.083.

[15] L. Zhao, W.-W. Che, C. Deng, and Z.-G. Wu, "Adaptive Fault-Tolerant Control for Nonlinear MASs Under Actuator Faults and DoS Attacks," *IEEE transactions on systems, man, and cybernetics. Systems*, vol. 53, no. 9, pp. 5874–5884, Sep. 2023, doi: https://doi.org/10.1109/tsmc.2023.3276364.

[16] L. An and G.-H. Yang, "Decentralized Adaptive Fuzzy Secure Control for Nonlinear Uncertain Interconnected Systems Against Intermittent DoS Attacks," *IEEE Transactions on Cybernetics*, vol. 49, no. 3, pp. 827–838, Mar. 2019, doi: https://doi.org/10.1109/TCYB.2017.2787740.

[17] A.-Y. Lu and G.-H. Yang, "Input-to-State Stabilizing Control for Cyber-Physical Systems With Multiple Transmission Channels Under Denial of Service," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1813–1820, Jun. 2018, doi: https://doi.org/10.1109/tac.2017.2751999.

[18] Y. Cui, H. Sun, and L. Hou, "Decentralized event-triggered adaptive neural network control for nonstrict-feedback nonlinear interconnected systems with external disturbances against intermittent DoS attacks," vol. 517, pp. 133–147, Jan. 2023, doi: https://doi.org/10.1016/j.neucom.2022.10.056.

[19] D. Zhai, L. An, J. Dong, and Q. Zhang, "Switched Adaptive Fuzzy Tracking Control for a Class of Switched Nonlinear Systems Under Arbitrary Switching," *IEEE Transactions on Fuzzy Systems*, vol. 26, no. 2, pp. 585–597, Apr. 2018, doi: https://doi.org/10.1109/tfuzz.2017.2686378.

[20] M. Attar and W. Lucia, "An Active Detection Strategy Based on Dimensionality Reduction for False Data Injection Attacks in Cyber-Physical Systems," *IEEE Transactions on Control of Network Systems*, pp. 1–11, 2023, doi: https://doi.org/10.1109/tcns.2023.3244103.

[21] Arman Sargolzaei, K. Yazdani, Alireza Abbaspour, C. D. Crane, and W. E. Dixon, "Detection and Mitigation of False Data Injection Attacks in Networked Control Systems," *IEEE*

[3] Z. Zhang, G. Duan, and M. Hou, "Robust adaptive dynamic surface control of uncertain non-linear systems with output constraints," *IET Control Theory & Applications*, vol. 11, no. 1, pp. 110–121, Jan. 2017, doi: https://doi.org/10.1049/iet-cta.2016.0456.

[4] Q. Shen, B. Jiang, and V. Cocquempot, "Adaptive fault-tolerant backstepping control against actuator gain faults and its applications to an aircraft longitudinal motion dynamics," *International Journal of Robust and Nonlinear Control*, p. n/a-n/a, Apr. 2013, doi: https://doi.org/10.1002/rnc.3000.

[5] C. De Persis and P. Tesi, "Input-to-State Stabilizing Control Under Denial-of-Service," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015, doi: https://doi.org/10.1109/tac.2015.2416924.

[6] J. Huang, L. Zhao, and Q.-G. Wang, "Adaptive control of a class of strict feedback nonlinear systems under replay attacks," *ISA transactions*, vol. 107, pp. 134–142, Dec. 2020, doi: https://doi.org/10.1016/j.isatra.2020.08.001.

[7] L. Zhao and G.-H. Yang, "Adaptive fault-tolerant control for nonlinear multi-agent systems with DoS attacks," *Information sciences*, vol. 526, pp. 39–53, Jul. 2020, doi: https://doi.org/10.1016/j.ins.2020.03.083.

[8] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018, doi: https://doi.org/10.1016/j.neucom.2017.10.009.

[9] H. Yang and D. Ye, "Observer-Based Fixed-Time Secure Tracking Consensus for Networked High-Order Multiagent Systems Against DoS Attacks," *IEEE transactions on cybernetics*, vol. 52, no. 4, pp. 2018–2031, Apr. 2022, doi: https://doi.org/10.1109/tcyb.2020.3005354.

[10] Z. Zhang and H. Wang, "Resilient decentralized adaptive tracking control for nonlinear interconnected systems with unknown control directions against DoS attacks," *Applied mathematics and computation*, vol. 415, pp. 126717–126717, Feb. 2022, doi: https://doi.org/10.1016/j.amc.2021.126717.

[11] X. Jiang, X. Mu, and Z. Hu, "Decentralized Adaptive Fuzzy Tracking Control for a Class of Nonlinear Uncertain Interconnected Systems With Multiple Faults and Denial-of-Service Attack," vol. 29, no. 10, pp. 3130–3141, Oct. 2021, doi: https://doi.org/10.1109/tfuzz.2020.3013700.

[12] B. Guo, S. Dian, and T. Zhao, "Active event-driven reliable defense control for interconnected nonlinear systems under actuator faults and denial-of-service attacks," *Science China Information*

[31] X. Jin, B. Yan, J. Chi, X. Wu, and C. Deng, "Neural network-based output tracking control of high-order nonlinear systems with DoS attacks and perturbations," *Journal of the Franklin Institute*, vol. 360, no. 16, pp. 12221–12246, Nov. 2023, doi: https://doi.org/10.1016/j.jfranklin.2023.09.039.

[32]Yang, J. Ge, D. Yue, Q. Meng, and J. Wu, "Adaptive resilient control of a class of nonlinear systems based on event-triggered mechanism," *Neurocomputing*, vol. 403, pp. 304–313, Aug. 2020, doi: https://doi.org/10.1016/j.neucom.2020.04.061.

[33] X. Yang, T. Li, Y. Long, H. Yang, and C.L. Philip Chen, "Switched-type unknown input observer-based fault-tolerant control for cyber-physical systems in the presence of denial of service attack," *Information sciences*, vol. 647, pp. 119457–119457, Nov. 2023, doi: https://doi.org/10.1016/j.ins.2023.119457.

[34] H. Xie, G. Zong, D. Yang, Y. Guo, and X. Zhao, "Secure Control for Switched Nonlinear Systems With DoS Attacks: A Switching Event-Triggered Adaptive Output-Feedback Control Method," *IEEE transactions on systems, man, and cybernetics. Systems*, pp. 1–11, Jan. 2024, doi: https://doi.org/10.1109/tsmc.2024.3352557.

transactions on industrial informatics, vol. 16, no. 6, pp. 4281–4292, Jun. 2020, doi: https://doi.org/10.1109/tii.2019.2952067.

[22] M. Yang and J. Zhai, "Observer-based dynamic event-triggered secure control for nonlinear networked control systems with false data injection attacks," *Information Sciences*, vol. 644, pp. 119262–119262, Oct. 2023, doi: https://doi.org/10.1016/j.ins.2023.119262.

[23] Y. Raghuvamsi and K. Teeparthi, "Detection and reconstruction of measurements against false data injection and DoS attacks in distribution system state estimation: A deep learning approach," *Measurement*, vol. 210, p. 112565, Mar. 2023, doi: https://doi.org/10.1016/j.measurement.2023.112565.

[24] J. Shao, Z. Ye, D. Zhang, H. Yan, and J. Zhu, "Injection attack estimation of networked control systems subject to hidden DoS attack," *ISA transactions*, vol. 129, pp. 1–14, Oct. 2022, doi: https://doi.org/10.1016/j.isatra.2022.02.005.

[25] S. Hu, X. Ge, X. Chen, and D. Yue, "Resilient Load Frequency Control of Islanded AC Microgrids Under Concurrent False Data Injection and Denial-of-Service Attacks," vol. 14, no. 1, pp. 690–700, Jan. 2023, doi: https://doi.org/10.1109/tsg.2022.3190680.

[26] S. Wu, Y. Jiang, H. Luo, J. Zhang, S. Yin, and O. Kaynak, "An integrated data-driven scheme for the defense of typical cyber–physical attacks," *Reliability Engineering & System Safety*, vol. 220, p. 108257, Apr. 2022, doi: https://doi.org/10.1016/j.ress.2021.108257.

[27] Y. Cui, H. Sun, and L. Hou, "NN-based decentralized adaptive event-triggered control for nonlinear interconnected systems under intermittent DoS and injection attacks," *International journal of adaptive control and signal processing*, vol. 36, no. 9, pp. 2249–2268, Jun. 2022, doi: https://doi.org/10.1002/acs.3455.

[28] Hamed Rezaee and F. Abdollahi, "Adaptive Leaderless Consensus Control of Strict-Feedback Nonlinear Multiagent Systems With Unknown Control Directions," *IEEE transactions on systems, man, and cybernetics*, vol. 51, no. 10, pp. 6435–6444, Oct. 2021, doi: https://doi.org/10.1109/tsmc.2019.2962973.

[29] H. Ying, "Sufficient conditions on general fuzzy systems as function approximators," *Automatica*, vol. 30, no. 3, pp. 521–525, Mar. 1994, doi: https://doi.org/10.1016/0005-1098(94)90130-9.

[30] S. Feng and P. Tesi, "Resilient control under Denial-of-Service: Robust design," *Automatica*, vol. 79, pp. 42–51, May 2017, doi: https://doi.org/10.1016/j.automatica.2017.01.031.