کنترل عملکردی پیش‌بین رمزگذاری شده برای سیستم کوادکوپتر با استفاده از تسهیم راز اعداد حقیقی

تاریخ دریافت: ۱۴۰۴/۰۸/۱۱
تاریخ پذیرش: ۱۴۰۴/۱۰/۱۴

میر ابوالفضل مختاری [۱]،
۱- دانشیار، دانشکده مهندسی و پرواز، دانشگاه افسری امام علی (ع)، تهران، s.abolfazl.mokhtari@aut.ac.ir

چکیده

در این مقاله، بر طراحی و پیاده‌سازی یک کنترل‌کننده پیش‌بین مدل رمزگذاری شده تمرکز کرده‌ایم. طرح رمزگذاری پیشنهادی می‌تواند محاسبات کنترلی را بر اساس ریاضیات رمزنگاری بدون نیاز به رمزگشایی میانی انجام دهد. در واقع، از یک طرح تسهیم راز به عنوان ابزار حفظ حریم خصوصی برای ایجاد یک محیط امن جهت محاسبه یک دسته از کنترل‌کننده‌های پیش‌بین به نام کنترل عملکردی پیش‌بین با توزیع داده‌ها در فضای ابری استفاده می‌شود.این کنترل‌کننده با حفظ سادگی و ویژگی‌های اساسی کنترل پیش‌بین، از رمزنگاری مبتنی بر تسهیم راز برای انجام عملیات مستقیم روی داده‌های رمزگذاری شده استفاده می‌کند و امنیت سایبری سیستم را به‌طور چشمگیری افزایش می‌دهد .کنترل‌کننده عملکردی پیش‌بین رمزگذاری شده پیشنهادی بر روی یک سیستم کوادکوپتر اعمال شده و کارایی آن توسط مجموعه‌ای از شبیه‌سازی‌های جامع ارزیابی می‌شود. نتایج شبیه‌سازی نشان می‌دهد که کنترل‌کننده رمزگذاری شده پیشنهادی ضمن حفظ کامل محرمانگی داده‌های حساس، عملکردی کاملاً مشابه با کنترل‌کننده غیررمزگذاری شده دارد و قادر است پایداری و عملکرد مطلوب سیستم کوادکوپتر را در شرایط عملیاتی مختلف تضمین نماید.

واژه‌های کلیدی: *کنترل رمزگذاری شده، کنترل عملکردی پیش‌بین، تسهیم راز ، کنترل امن، محاسبات توزیع شده، سیستم‌های کوادکوپتر، امنیت سایبری.*

Encrypted predictive functional control for quadcopter systems using real-number secret sharing

Mirabolfazl Mokhtari [1]

1- Associate Professor Faculty of Engineering and Flight, Imam Ali University, Tehran

Abstract

This paper focuses on the design and implementation of an encrypted model-based predictive controller. The proposed encryption scheme enables control computations to be performed directly on encrypted data using cryptographic mathematics, eliminating the need for intermediate decryption. Specifically, a secret sharing scheme is employed as a privacy-preserving tool to create a secure environment for computing a class of predictive controllers known as predictive functional control (PFC) with cloud-based data distribution. While retaining the simplicity and fundamental features of predictive control, the controller utilizes secret-sharing-based encryption to perform operations directly on encrypted data, significantly enhancing the cybersecurity of the system. The proposed encrypted predictive functional controller is applied to a quadcopter system, and its performance is evaluated through a series of comprehensive simulations. Simulation results show that the encrypted controller maintains performance nearly identical to that of the unencrypted controller while fully preserving the confidentiality of sensitive data. Moreover, it ensures stability and desired performance of the quadcopter system under various operational conditions.

Keywords*: Encrypted control, Predictive functional control, Secret sharing, Secure control, Distributed computation, Quadcopter systems, Cybersecurity.*

۱. مقدمه

تسهیم راز [1] (SS) به عنوان یک اصل رمزنگاری بنیادی در سیستم‌های محاسباتی امن مدرن ظهور کرده و نقش محوری در حفاظت از اطلاعات حساس در شبکه‌های توزیع‌شده ایفا می‌کند [۱]. پایه‌های مفهومی SS به طور مستقل توسط شامیر [۲] و بلکلی [۳] در سال ۱۹۷۹ با استفاده از چندجمله‌ای‌های درونیابی لاگرانژ و مفاهیم هندسی به ترتیب برای تقسیم رازها به سهم‌های متعدد پایدار شد. طرح‌های سنتی SS، از جمله طرح گسترده‌شده شامیر، عمدتاً بر محاسبات پیمانه‌ای روی میدان‌های متناهی متکی هستند که محدودیت‌های ذاتی مانند خطاهای گردکردن داده و سربار محاسباتی را به همراه دارد [۴]. این محدودیت‌ها به‌ویژه در کاربردهای سیستم کنترل که عملکرد بلادرنگ و دقت عددی از اهمیت بالایی برخوردار است، مشکل‌ساز می‌شوند [۵].

برای رفع این محدودیت‌ها، تحقیقات اخیر چارچوب‌های عددی جایگزین برای SS را بررسی کرده‌اند. تسهیم راز اعداد حقیقی [2] (RSS) به عنوان یک رویکرد امیدبخش که در حوزه‌های پیوسته عمل می‌کند، توجهات را به خود جلب کرده و به طور مؤثر خطاهای کوانتیزاسیون را حذف و کارایی محاسباتی را افزایش می‌دهد [۷,۶]. تجل و ویسنیوسکی [۸] یک طرح RSS جامع را پیشگامی کردند که از عملیات جمع، ضرب و حتی تقسیم امن بر روی داده‌های رمزگذاری شده پشتیبانی می‌کند و راه را برای کاربردهای کنترل حفظ حریم خصوصی هموار می‌سازد. کارهای بعدی این مفاهیم را برای پشتیبانی از عملیات پیچیده‌تر گسترش داده‌اند در حالی که تضمین‌های امنیتی اطلاعات-نظری را حفظ می‌کنند [۱۰,۹].

به موازات این پیشرفت‌های رمزنگاری، کنترل پیش‌بین مدل [3] (MPC) در طول دهه‌های اخیر انقلابی در اتوماسیون صنعتی و کنترل فرآیند ایجاد کرده است [۱۲,۱۱]. توانایی MPC در رسیدگی صریح به محدودیت‌ها در حالی که رفتار آینده سیستم را بهینه می‌سازد، آن را در کاربردهای متعدد نسبت به کنترل PID متعارف برتر ساخته است [۱۳]. در میان انواع MPC، کنترل عملکردی پیش‌بین (PFC) به دلیل کارایی محاسباتی و مدیریت سیستماتیک محدودیت‌ها از محبوبیت ویژه‌ای برخوردار شده است [۱۴]. PFC قابلیت‌های پیش‌بین ضروری MPC را حفظ می‌کند در حالی که پیاده‌سازی ساده‌ای ارائه می‌دهد که آن را برای کاربردهای بلادرنگ با منابع محاسباتی محدود مناسب می‌سازد [۱۶,۱۷,۱۸].

همگرایی رایانش ابری و سیستم‌های کنترل صنعتی هم فرصت‌ها و هم چالش‌هایی برای پیاده‌سازی‌های کنترل مدرن ایجاد کرده است [۱۹]. در حالی که کنترل مبتنی بر فضای ابری مقیاس‌پذیری و بهینه‌سازی منابع را ارائه می‌دهد، آسیب‌پذیری‌های امنیتی قابل توجهی از جمله نقض داده‌ها، حملات میانی و دسترسی غیرمجاز به اطلاعات حساس را معرفی می‌کند [۲۰,۱۵]. پیامدهای بالقوه این تهدیدات امنیتی از تخریب عملکرد تا خرابی‌های فاجعه‌بار سیستم، به‌ویژه در کاربردهای بحرانی از نظر ایمنی مانند وسایل نقلیه خودران، شبکه‌های برق و سیستم‌های هوافضا متغیر است [۲۱].

این چشم‌انداز امنیتی، ظهور کنترل رمزگذاری شده را به عنوان یک حوزه تحقیقاتی حیاتی کرده است [۲۸-۲۲]. سیستم‌های کنترل رمزگذاری

شـده از تکنیـک‌هـای رمزنگـاری بـرای انجـام محاسـبات کنتـرل مسـتقیماً بـر روی داده‌هـای رمزگذاری شده استفاده می‌کننـد و محرمـانگی را در سراسـر حلقـه کنتـرل تضـمین مـی‌کننـد. دو رویکـرد رمزنگـاری اولیـه بـر ایـن حـوزه مسـلط بوده‌اند: رمزگذاری هوموورفیـک[۴] (HE) و تسـهیم راز [۵]. در حالی که HE محاسـبه روی داده‌هـای رمزگـذاری شـده را بـا اسـتفاده از سـاختارهای ریاضی پیچیده امکـان‌پـذیر مـی‌سـازد [۲۹,۳۰]، اغلب از سربار محاسباتی قابل توجـه و پشـتیبانی محدود از عملیات پیچیده رنج می‌برد.

کنترل مبتنـی بـر تسـهیم راز بـه عنـوان یـک جایگزین قانع‌کننده، به‌ویژه برای پیاده‌سازی‌هـای توزیع‌شده مبتنی بر ابر ظهـور کـرده اسـت [۳۱]. مزیت بنیادی SS در توانایی آن بـرای توزیـع بـار محاسباتی در بـین چنـدین طـرف در حـالی کـه امنیت اطلاعات-نظـری را حفـظ مـی‌کنـد نهفتـه اسـت [۳۲]. مطالعـات اخیـر پیـاده‌سـازی‌هـای موفقیت‌آمیز SS را در معماری‌های کنترل مختلف نشـان داده‌انـد. کوگیسـو و فوجیتـا [۱۲] یـک چارچوب کنتـرل رمزگـذاری شـده بـا اسـتفاده از رمزگذاری کانولوشنی برای سیسـتم‌هـای فیـدبک خطی توسعه دادنـد، در حـالی کـه داروپ و یـاگر [۳۳] یک پیاده‌سازی کنترل مبتنی بر ابر ترکیبی تسهیم راز با پدهای یکبار مصرف ارائه دادنـد. ایـن رویکردهـا نتـایج امیدبخشـی در متعـادل‌سـازی الزامات امنیتی با عملـی بـودن محاسـباتی نشـان داده‌اند.

ادغام SS با اسـتراتژی‌هـای کنتـرل پیشـرفته مانند PFC نشان‌دهنده یک پیشـرفت طبیعـی بـه سمت سیستم‌هـای کنتـرل ابـری امـن و کارآمـد است. این ترکیب مزایای عددی RSS را با کـارایی محاسباتی PFC به کار می‌گیـرد و یـک چـارچوب قوی برای کنترل پیش‌بین حفظ حریم خصوصـی ایجاد می‌کنـد. کاربردهـای اخیـر در حـوزه‌هـایی ماننـد شـبکه‌هـای هوشـمند و IoT صـنعتی و سیستم‌های خودمختار قابلیت اجرای عملـی ایـن رویکرد را نشان داده‌اند.

با این حال، چندین چالش در تحقق پتانسـیل کامل سیسـتم‌هـای PFC رمزگـذاری شـده بـاقی می‌ماند. این چالش‌ها شامل مدیریت تعـادل بـین سطوح امنیتی و کارایی محاسباتی[۳۴]. رسیدگی به دینامیک‌های غیرخطی سیسـتم و اطمینـان از اسـتحکام در برابـر تهدیـدات سـایبری مختلـف می‌شود. علاوه بر این، اعمال ایـن تکنیـک‌هـا بـه سیسـتم‌هـای چنـدمتغیره پیچیـده ماننـد کوادکوپترهـا بـه دلیـل غیرخطـی بـودن ذاتـی و الزامات سـخت بلادرنـگ، چـالش‌هـای اضـافی را ایجاد می‌کند.

این مقاله بر اساس این پایه‌ها بـا توسـعه یـک چارچوب PFC رمزگذاری شـده جـامع مبتنـی بـر تسهیم راز اعداد حقیقی، که بـه‌طـور خـاص بـرای سیستم‌های کوادکوپتر طراحـی شـده اسـت، بنـا می‌شود. مشارکت ما بـه چـالش‌هـای کلیـدی در کنترل ابـری امـن اشـاره مـی‌کنـد در حـالی کـه استانداردهای عملکرد مورد نیاز بـرای کاربردهـای رباتیک هوایی را حفظ می‌کند. رویکرد پیشنهادی نشان می‌دهد که چگونه تکنیـک‌هـای رمزنگـاری مدرن می‌توانند به طـور مـؤثر بـا اسـتراتژی‌هـای کنترل پیشـرفته ترکیـب شـوند تـا سیسـتم‌هـای کنتـرل امـن، کارآمـد و عملـی بـرای کاربردهـای سایبری- فیزیکی نسل بعدی ایجاد کنند.

ساختار ادامه این مقاله به صورت زیر است: در بخش دوم، کنترل‌کننده‌های تسـهیم راز و کنتـرل عملکردی پیش‌بین تشریح مـی‌شـوند. سـپس در بخش سوم، کنترل‌کننده رمزگذاری شده طراحـی

می‌شود. بخش چهارم به ارائه نتایج شبیه‌سازی جهت نمایش کارایی روش پیشنهادی می‌پردازد و در نهایت، نتیجه‌گیری در بخش پنجم ارائه می‌گردد و در بخش ششم مراجع به کار گرفته شده در این مقاله آورده شده است.

۲. مبانی و پیش‌زمینه‌های نظری

در این بخش، مبانی نظری و اصول اولیه مرتبط با طرح تسهیم راز (SS) و کنترل‌کننده عملکردی پیش‌بین (PFC) به تفصیل مورد بررسی قرار می‌گیرد.

۱.۲. طرح تسهیم راز

تسهیم راز (SS) یک اصل رمزنگاری بنیادی برای حفظ حریم خصوصی در سیستم‌های توزیع‌شده است. اصل مرکزی آن تقسیم یک اطلاعات حساس، یعنی راز، به چندین قطعه به نام سهم است. این سهم‌ها میان مجموعه‌ای از شرکت‌کنندگان توزیع می‌شوند به طوری که هر سهم به تنهایی هیچ اطلاعاتی درباره راز اصلی فاش نمی‌کند. راز تنها زمانی می‌تواند بازسازی شود که تعداد کافی از سهم‌ها با هم ترکیب شوند، عددی که توسط یک آستانه تعریف می‌شود.

به طور رسمی، یک راز $s \in \mathbb{R}$ را در نظر بگیرید که باید میان یک مجموعه $p \in \mathcal{P}$ شرکت‌کننده به

اشتراک گذاشته شود. یک طرح تسهیم راز آستانه‌ای (k, p) به کار گرفته می‌شود، که در آن $k \in \mathbb{N}$ مقدار آستانه است و $k < p$. سهم‌های راز s به صورت $s[p] \in \mathbb{R}$ نشان داده می‌شوند. این طرح باید دو ویژگی کلیدی را دارا باشد:

- درستی: راز s می‌تواند از هر مجموعه‌ای از سهم های $\mathcal{T} \subseteq \mathcal{P}$ که در آن $|\mathcal{T}| \geq k+1$ باشد، بازسازی شود.
- محرمانگی: هر مجموعه‌ای از سهم‌های $\mathcal{T} \subseteq \mathcal{P}$ با $|\mathcal{T}| \leq k$ هیچ اطلاعاتی درباره s فاش نمی‌کند.

در ادامه، روش‌های تسهیم و بازسازی راز، بر اساس طرح شامیر به تفصیل شرح داده می‌شود.

۱) روش تسهیم راز:

برای تسهیم یک راز s، یک چندجمله‌ای تصادفی $q_s(x)$ با حداکثر درجه k ساخته می‌شود به طوری که $q_s(0) = s$. با استفاده از پایه لاگرانژ، چندجمله‌ای به صورت زیر تعریف می‌شود:

$$q_s(x) = sL_0 + \sum_{j=1}^{k} \frac{y_j}{x_j} x L_j(x) \qquad (۱)$$

که در آن x_j یک اندیس یکتا و غیرصفر اختصاص‌یافته به عضو-jام است، و y_j یک ضریب تصادفی است که از یک توزیع گاوسی با میانگین صفر و واریانس σ_y^2 انتخاب شده است. چندجمله‌ی پایه‌ی لاگرانژ $L_j(x)$ به صورت زیر تعریف می‌شود:

$$L_j(x) = \prod_{l=1, l\neq j}^{k} \frac{x - x_l}{x_j - x_l} \qquad (۲)$$

با توجه به اینکه $x_0 = 0$ و با توجه به خاصیت چندجمله‌ای‌های لاگرانژ که $L_j(x_i) = \delta_{i,j}$ (دلتای کرونکر) است، برقرار است که $q_s(0) = s$ سهم برای شرکت‌کننده -jام با جایگذاری اندیس او در چندجمله‌ای $s[p_j] = q_s(x_i)$ محاسبه می‌شود .

۲) بازسازی راز:

برای بازسازی راز از یک مجموعه $\mathcal{T}$ شامل حداقل $k+1$ سهم، چندجمله‌ای $q_r(x)$ از طریق نقاط $(x_j, s[p_j])$ برای تمام $p_j \in \mathcal{T}$ درون‌یابی می‌شود:

$$q_r(x) = \sum_{p \in \mathcal{T}} s[p] L_{p_j}(x) \qquad (۳)$$

که در آن $L_{p_j}(x)$ چندجمله‌ای پایه لاگرانژ

برای مجموعه $\mathcal{T}$ است. راز اصلی سپس با ارزیابی این چندجمله‌ای در نقطه صفر بازیابی می‌شود $\hat{s} = q_r(0)$. تضمین امنیتی اطمینان ایجاد می‌کند که با k سهم یا کمتر، $q_r(0)$ از راز واقعی s مستقل آماری است.

۳) عملیات محاسبات چندجانبه امن (MPC):

طرح‌های تسهیم راز را می‌توان برای فعال کردن محاسبات چندجانبه امن (MPC) گسترش داد که به شرکت‌کنندگان اجازه می‌دهد توابعی بر روی رازهای تسهیم شده بدون نیاز به بازسازی آن‌ها محاسبه کنند.

- جمع: جمع دو راز تسهیم شده s و a ساده است و به هیچ ارتباطی نیاز ندارد. هر طرف صرفاً مجموع سهم‌های محلی خود را محاسبه می‌کند:

$$\mathrm{add}(s[p], a[p]) = s[p] + a[p] \quad (۴)$$

سهم‌های حاصل مربوط به راز $s + a$ هستند.

- ضرب: ضرب دو راز تسهیم شده به صورت غیرتعاملی با یک طرح خطی ممکن نیست. از تکنیک سه‌تایی Beavers معمولاً برای دستیابی به این هدف استفاده می‌شود. این روش نیاز به یک سه‌تایی تصادفی همبسته از پیش توزیع شده $\{r_1[p], r_2[p], r_1r_2[p]\}_{p\in\rho}$ دارد، که در آن r_1 و r_2 رازهای تصادفی هستند. پروتکل ضرب برای سهم‌های $s[p]$ و $a[p]$به شرح زیر پیش می‌رود:

۱. طرفین به صورت محلی $\mathrm{d}[p] = \mathrm{s}[p] - \mathrm{r}_1[p]$ و $e[p] = \mathrm{s}[p] - \mathrm{r}_2[p]$ را محاسبه می‌کنند.

۲. این مقادیر به صورت عمومی بازسازی می‌شوند تا d و e افشا شوند:

$$d = \mathrm{recon}\left(\{s[p] - r_1[p]\}_{p\in T}\right)$$
$$e = \mathrm{recon}\left(\{a[p] - r_2[p]\}_{p\in T}\right) \quad (۵)$$

۳. سپس هر طرف به صورت محلی سهم خود از حاصل‌ضرب را به صورت $\mathrm{mult}(s[p], a[p]) = de + dr_2[p] + r_1[p]e + r_1r_2[p]$ محاسبه می‌کند که نتیجه یک تسهیم معتبر از حاصلضرب s و a است.

- معکوس ضربی: معکوس یک راز تسهیم شده s را می‌توان با استفاده از یک ضرب با یک مقدار تصادفی تسهیم شده r محاسبه کرد.

۱. طرفین حاصل‌ضرب $s[p]$ و $a[p]$ را با استفاده از پروتکل ضرب محاسبه می‌کنند:

$$sr = \mathrm{recon}\big(\mathrm{mult}(s[p], r[p])\big) \quad (۶)$$

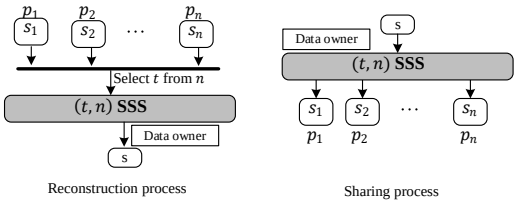
۲. اگر $sr \neq 0$ باشد، هر طرف به صورت محلی سهم خود از معکوس را به صورت زیر محاسبه می‌کند:

$$\mathrm{invers}(s) = s^{-1}[p] = (sr)^{-1}r[p] \quad (۷)$$

نتیجه یک تسهیم معتبر از s^{-1} است.

جایی که recon تابعی برای بازسازی مخفیانه است و r یک متغیر تصادفی است. ابتدا، ضرب بین سهم‌های طرف‌ها و متغیر تصادفی کمکی با استفاده از تابع recon بازسازی می‌شود، و سپس سهم‌های متناظر با معکوس متغیر مطلوب با استفاده از تابع invers ایجاد می‌شوند.

چندجمله‌ای‌های لاگرانژ برای تسهیم داده میان طرف‌ها استفاده می‌شوند، که در آن ضرایب چندجمله‌ای به صورت تصادفی تولید می‌شوند. این امر باعث حفظ حریم خصوصی می‌شود. با این حال، به دلیل استفاده از سه‌تایی‌های بیور در عمل ضرب، طرف‌ها نیاز دارند تا با یکدیگر ارتباط برقرار کرده تا داده‌های خود را برای محاسبه ضرایب ضرب به اشتراک بگذارند. در عملیات‌های دیگر، طرف‌ها محاسبات را تنها بر روی داده‌های تسهیم‌شده انجام می‌دهند.



شکل ۱. شماتیک توزیع و بازسازی داده در SS با طرح آستانه (t, n).

۲.۲. کنترل پیش‌بین عملکردی

کنترل پیش‌بین عملکردی (PFC) یک استراتژی کنترل پیش‌بین مبتنی بر مدل است که به دلیل سادگی محاسباتی و اثربخشی در تنظیم فرآیندهای با دینامیک کند، مانند آنچه معمولاً در صنایع شیمیایی، پتروشیمی و کنترل دما یافت می‌شود، مشهور است. برخلاف انواع پیچیده‌تر MPC که یک تابع هزینه را در یک افق بلندمدت بهینه می‌کنند، فلسفه اصلی PFC این است که خروجی پیش‌بینی شده فرآیند را در چند لحظه آینده از پیش انتخاب شده استراتژیک، که به عنوان نقاط تطبیق شناخته می‌شوند، با یک مسیر مرجع مطلوب منطبق کند. این رویکرد به طور قابل توجهی بار محاسباتی را کاهش می‌دهد و آن را برای برنامه‌های کاربردی که منابع محاسباتی محدود هستند یا نرخ نمونه‌برداری بالا مورد نیاز نیست، مناسب می‌سازد.

در یک کنترل‌گر PFC، از این نقاط تطبیق برای ارزیابی تابع هدف در طول افق پیش‌بینی استفاده می‌شود. بنابراین، تعیین سیگنال‌های کنترل به محاسبات کمتری در مقایسه با الگوریتم‌هایی که کل افق را در نظر می‌گیرند، نیاز دارد. در مطالعه حاضر، یک PFC دو نقطه‌ای پیاده‌سازی شده است که در آن از یک مدل CARIMA برای انجام پیش‌بینی‌های لازم استفاده می‌شود. یک مدل CARIMA توسط رابطه زیر داده می‌شود:

$$A'(z^{-1})y(t) = B'(z^{-1})u(t-1) + C'(z^{-1})\frac{w(t)}{\Delta} \quad (۸)$$

جایی که $\Delta = 1 - z^{-1}$ عملگر تفاضلی و $w(t)$ نشان‌دهنده نویز گوسی سفید است. استفاده از مدل CARIMA به طور ذاتی عمل انتگرال را فراهم می‌کند و خطای حالت ماندگار صفر را برای اغتشاشات ثابت تضمین می‌کند.

پیش‌بینی‌های خروجی $y_m(t+\mu_1)$ و $y_m(t+\mu_2)$ در دو نقطه تطبیق به شرح زیر محاسبه می‌شوند:

$$\begin{bmatrix} y_m(t+\mu_1) \\ y_m(t+\mu_2) \end{bmatrix} = \begin{bmatrix} g_{\mu_1} & g_{\mu_{1-m+1}} \\ g_{\mu_2} & g_{\mu_{2-m+1}} \end{bmatrix} \begin{bmatrix} \Delta u(t) \\ \Delta u(t+m-1) \end{bmatrix} + \begin{bmatrix} y_{\text{past}}(t+\mu_1) \\ y_{\text{past}}(t+\mu_2) \end{bmatrix} \quad (۹)$$

که در آن g_i، i-امین ضریب پاسخ پله واحد مدل است. عبارات $y_{\text{past}}(t+\mu_1)$ و $y_{\text{past}}(t+\mu_2)$ نشان‌دهنده پاسخ آزاد مدل هستند که بخشی از پیش‌بینی خروجی است که فقط به ورودی‌ها و خروجی‌های گذشته بستگی دارد، با این فرض که تمامی حرکت‌های کنترلی آینده صفر هستند. این مقادیر به صورت زیر محاسبه می‌شوند:

$$y_{\text{past}}(t+\mu_1) = \alpha_1^{\mu_1}u^-(t) + \beta_1^{\mu_1}y^-(t)$$
$$y_{\text{past}}(t+\mu_2) = \alpha_2^{\mu_2}u^-(t) + \beta_2^{\mu_2}y^-(t) \quad (۱۰)$$

که در آن $\alpha_1^{\mu_1}$ و $\alpha_2^{\mu_2}$ به ترتیب ردیف های μ_1 و μ_2 ماتریس $E_j(z^{-1})B$ و $\beta_2^{\mu_2}$ و $\beta_1^{\mu_1}$ ردیف های μ_1 و μ_2 ماتریس $F_j(z^{-1})$ هستند. چندجمله‌ای های $E_j(z^{-1})$ و $F_j(z^{-1})$ پاسخ معادله دیوفانتین زیر هستند:

$$E_j(z^{-1})\Delta A'(z^{-1}) + z^{-j}F_j(z^{-1}) = 1 \quad (۱۱)$$

بردارهای $u^-(t)$ و $y^-(t)$ به ترتیب شامل تاریخچه ورودی‌ها و خروجی‌های گذشته هستند و به صورت زیر تعریف می‌شوند:

$$u^-(t)=\begin{bmatrix}u(t-1)\\ \vdots\\ u(t-n_b)\end{bmatrix}-\begin{bmatrix}u(t-2)\\ \vdots\\ u(t-n_b-1)\end{bmatrix}$$
$$y^-(t)=\begin{bmatrix}y(t)\\ \vdots\\ y(t-n_a)\end{bmatrix} \quad (۱۲)$$

که در آن n_a و n_b به ترتیب مرتبه های صورت و مخرج تابع انتقال مدل هستند.

برای اجتناب از عمل کنترلی تهاجمی، مسیر آینده مطلوب سیستم، خود نقطه تنظیم نیست، بلکه یک مسیر هموار و نمایی از خروجی جاری به سمت نقطه تنظیم است. این خروجی مطلوب توسط یک فیلتر درجه اول روی نقطه تنظیم تعیین می‌شود:

$$\begin{aligned}y_d(t+\mu_1)&=\psi^{\mu_1}y(t)+(1-\psi^{\mu_1})y_{sp}(t)\\ y_d(t+\mu_2)&=\psi^{\mu_2}y(t)+(1-\psi^{\mu_2})y_{sp}(t)\end{aligned} \quad (۱۳)$$

که در آن ψ قطب فیلتر هموارسازی $(0\le\psi<1)$ و $y_{sp}(t)$ نشان‌دهنده نقطه تنظیم است. مقدار ψ نزدیک به ۱ منجر به پاسخ کندتر و محافظه‌کارانه‌تری می‌شود.

خروجی‌های پیش‌بینی شده فرآیند واقعی، نادقیقی‌های مدل و اغتشاشات اندازه‌گیری نشده را با گنجاندن یک برآورد اغتشاش در نظر می‌گیرند:

$$\begin{bmatrix}y_p(t+\mu_1)\\ y_p(t+\mu_2)\end{bmatrix}=\begin{bmatrix}y_m(t+\mu_1)+d(t)\\ y_m(t+\mu_2)+d(t)\end{bmatrix} \quad (۱۴)$$

که در آن $d(t)$ خطای مدل‌سازی است که در طول افق پیش‌بینی ثابت فرض می‌شود و می‌تواند به عنوان تفاوت بین خروجی فرآیند اندازه‌گیری شده جاری و خروجی مدل تعیین شود:

$$d(t)=\ y(t)-y_m(t) \quad (۱۵)$$

قانون کنترل اصلی PFC را می‌توان به سادگی با برابر قرار دادن خروجی‌های پیش‌بینی شده فرآیند $y_p(t+\mu_1)$ و $y_p(t+\mu_2)$ با خروجی‌های مطلوب $y_d(t+\mu_1)$ و $y_d(t+\mu_2)$ به دست آورد. این یک سیستم دو معادله با دو مجهول $\Delta u(t)$ و $\Delta u(t+m-1)$ به دست می‌دهد که می‌توان آن را مستقیماً حل کرد:

$$\begin{bmatrix}g_{\mu_1} & g_{\mu_{1-m+1}}\\ g_{\mu_2} & g_{\mu_{2-m+1}}\end{bmatrix}^{-1}\begin{bmatrix}y_d(t+\mu_1)-y_{\text{past}}(t+\mu_1)-d(t)\\ y_d(t+\mu_2)-y_{\text{past}}(t+\mu_2)-d(t)\end{bmatrix} \quad (۱۶)$$

به طور متناوب، برای بهبود مقاومت و جلوگیری از حرکت‌های کنترلی بیش از حد، سیگنال کنترل را می‌توان با کمینه کردن یک تابع هدف وزن‌دار که تعادل بین خطای ردیابی و تلاش کنترل را برقرار می‌کند، تعیین کرد:

$$\begin{aligned}J&=[e_{\mu_1}\quad e_{\mu_2}]\begin{bmatrix}e_{\mu_1}\\ e_{\mu_2}\end{bmatrix}\\ &+[\Delta u(t)\quad \Delta u(t+m-1)]R\begin{bmatrix}\Delta u(t)\\ \Delta u(t+m-1)\end{bmatrix}\end{aligned} \quad (۱۷)$$

که در آن $R=rI_{2\times2}$ یک ماتریس وزن‌دهی قطری است و خطاها به صورت زیر تعریف می‌شوند:

$$\begin{aligned}e_{\mu_1}&=y_d(t+\mu_1)-y_p(t+\mu_1)\\ e_{\mu_2}&=y_d(t+\mu_2)-y_p(t+\mu_2)\end{aligned} \quad (۱۸)$$

فاکتور وزن r یک پارامتر تنظیمی است که برای جریمه کردن تغییرات سیگنال کنترل استفاده می‌شود؛ r بزرگتر منجر به عمل‌های کنترلی نرم تر اما بالقوه کندتر می شود. کمینه کردن این تابع هدف درجه دوم منجر به یک جواب تحلیلی برای حرکت‌های کنترلی می‌شود:

$$\begin{bmatrix}\Delta u(t)\\ \Delta u(t+m-1)\end{bmatrix}=k_{\text{PFC}}\begin{bmatrix}y_d(t+\mu_1)-y_{\text{past}}(t+\mu_1)-d(t)\\ y_d(t+\mu_2)-y_{\text{past}}(t+\mu_2)-d(t)\end{bmatrix} \quad (۱۹)$$

که در آن k_{PFC} ماتریس بهره کنترل PFC است که به صورت زیر محاسبه می‌شود:

$$k_{\text{PFC}}=(A^TA+R)^{-1}A^T,\quad A=\begin{bmatrix}g_{\mu_1} & g_{\mu_{1-m+1}}\\ g_{\mu_2} & g_{\mu_{2-m+1}}\end{bmatrix} \quad (۲۰)$$

عناصر ماتریس A در اصل عناصر ردیف‌های μ_1 و μ_2 و ستون‌های ۱ و m ماتریس پویا

(ماتریس Toeplitz) مشتق شده از مدل پیش‌بینی CARIMA هستند. توجه به شرط علیت مهم است: برای $\mu_1 < m < \mu_2$ ، حرکت کنترلی $\Delta u(t+m-1)$ بر خروجی در نقطه تطبیق اول تأثیر نمی‌گذارد، بنابراین $g_{\mu_1-m+1}^{\mu_1} = 0$.

پس از محاسبه $\Delta u(t)$ از عنصر اول بردار در معادله (۱۷)، سیگنال کنترل نهایی که باید به فرآیند اعمال شود به صورت زیر محاسبه می‌شود:

$$u(t) = u(t-1) + \Delta u(t) \qquad (۲۱)$$

این فرم افزایشی کنترل‌گر، محافظت ذاتی در برابر وایندآپ (Anti-windup) فراهم می‌کند.

۳.۲. تنظیم کنترل کننده PFC

عملکرد یک سیستم کنترل پیش‌بین تابعی (PFC) به شدت به انتخاب مناسب پارامترهای کلیدی آن وابسته است. این پارامترها شامل μ_i برای $(i = 1,2)$ که نقاط هم‌پوشانی هستند؛ ψ که قطب فیلتر هموارساز مرتبه اول (که به آن قطب حلقه بسته یا فاکتور سرعت نیز می‌گویند) است؛ $R = rI_{2\times2}$ که ماتریس وزن دهی کنترل است؛ و T_s که زمان نمونه‌برداری است، می‌شوند. یک رویکرد سیستماتیک برای تنظیم این پارامترها برای دستیابی به تعادل مطلوب بین سرعت پاسخ، استحکام و تلاش کنترلی، حیاتی است.

۱. نقاط هم‌پوشانی (μ_1, μ_2)

نقاط هم‌پوشانی، لحظات آینده‌ای را تعریف می‌کنند که در آن‌ها خروجی پیش‌بینی شده مدل مجبور می‌شود با مسیر مرجع مطلوب مطابقت کند. انتخاب این نقاط مستقیماً با پاسخ گذرای مورد نظر سیستم حلقه بسته مرتبط است.

- $\boldsymbol{\mu_1 = t_r/T_s}$: اولین نقطه هم‌پوشانی، μ_1، برای کنترل زمان t_r (rise) انتخاب می‌شود. قرار دادن یک نقطه هم‌پوشانی در ابتدای افق پیش‌بینی، پاسخ اولیه سریع‌تری از کنترل کننده تشویق می‌کند.
- $\boldsymbol{\mu_2 = t_s/T_s}$: دومین نقطه هم‌پوشانی، μ_2، با زمان t_s (settling) مرتبط است. اعمال مطابقت در این نقطه اطمینان می‌دهد که خروجی فرآیند به‌صورت هموار و بدون بالازدگی یا نوسان قابل توجه به سوی نقطه تنظیم میل می‌کند.
- **ملاحظه عملی:** مقادیر μ_i باید اعداد صحیح باشند. بنابراین، زمان‌های محاسبه شده باید به نزدیک‌ترین مضرب از زمان نمونه‌برداری T_s گرد شوند. استفاده از یک نقطه هم‌پوشانی (μ_2) رایج است، اما استفاده از دو نقطه، شکل‌دهی مستقیم‌تری به پاسخ گذرا می‌دهد.

۲. قطب حلقه بسته $(\boldsymbol{\psi})$

پارامتر ψ، قطب مسیر مرجع مرتبه اول است که با $y_{ref}(k+p) = \text{setpoint} - \psi^p(\text{setpoint} - y(k))$ داده می شود. این پارامتر اساساً سرعت مورد نظر پاسخ حلقه بسته را تعیین می‌کند.

- **محدوده نظری:** برای پایداری، ψ باید بین ۰ و ۱ انتخاب شود. مقدار $\psi = 0$ معادل پاسخ dead-beat (رسیدن به نقطه تنظیم در یک نمونه) است، در حالی که مقادیر نزدیک به ۱ منجر به پاسخ‌های کندتر و تنبل می‌شوند.
- **تنظیم اولیه:** یک مقدار اولیه توصیه شده $\psi = \exp((-4T_s)/t_s)$ است که مربوط به یک سیستم مرتبه اول با ثابت زمانی $t_s/4$ می‌باشد. این مقدار نقطه شروع خوبی برای دستیابی به زمان مستقر مورد نظر فراهم می‌کند.

- **تنظیم دقیق:** مقدار اولیه باید به عنوان یک نقطه شروع در نظر گرفته شود. ψ را می‌توان با روش سعی و خطا به دقت تنظیم کرد:
  - **کاهش ψ:** برای سریع‌تر و تهاجمی‌تر کردن پاسخ حلقه بسته.
  - **افزایش ψ:** برای کندتر کردن پاسخ، که استحکام سیستم را بهبود می‌بخشد و تلاش کنترلی و حساسیت به نویز اندازه‌گیری را کاهش می‌دهد.

۳. وزن دهی کنترل (r)

فاکتور وزن دهی r در ماتریس $R = rI_{2\times2}$ تلاش کنترلی را در تابع هزینه جریمه می‌کند. این پارامتر نقشی حیاتی در متعادل کردن عملکرد در برابر فعالیت محرک (actuator) ایفا می‌کند.

- **اثر r:** انتخاب یک مقدار بزرگ برای r به شدت حرکت‌های کنترلی را جریمه می‌کند و منجر به یک کنترل کننده محافظه‌کار با عملکردی هموار اما بالقوه کند می شود. برعکس، یک r کوچک تأکید بیشتری بر عملکرد ردیابی دارد که می‌تواند منجر به پاسخی سریع‌تر، اما همچنین سیگنال‌های کنترلی تهاجمی‌تر و نوسانی شود.
- **راهنمای انتخاب:** یک قاعده سرعت مؤثر این است که r را مساوی مربع بهره حالت ماندگار فرآیند (K_{ss}) قرار دهیم، یعنی $r \approx K_{ss}^2$ این کار وزن دهی کنترل را نسبت به بهره فرآیند نرمالیزه می‌کند. از این خط پایه، اگر عمل کنترلی بیش از حد شدید است می‌توان r را افزایش داد و اگر پاسخ بسیار کند است می توان آن را کاهش داد.
- **زمان نمونه‌برداری (T_s)**
- زمان نمونه‌برداری یک پارامتر اساسی است که بر تمام جنبه‌های طراحی و عملکرد کنترل کننده تأثیر می‌گذارد.
- **مبادلات:** یک T_s بسیار کوچک، تقریب گسسته بهتری از سیستم پیوسته ارائه می‌دهد اما بار محاسباتی را افزایش می‌دهد و می‌تواند کنترل کننده را نسبت به نویز حساس کند. یک T_s بسیار بزرگ می‌تواند به دلیل از دست دادن اطلاعات بین نمونه‌ها، منجر به عملکرد ضعیف و عدم پایداری بالقوه شود.
- **قانون انتخاب:** یک روش معمول این است که زمان نمونه‌برداری را طوری انتخاب کنیم که ۴ تا ۱۰ نمونه در طول ثابت زمانی غالب فرآیند حلقه باز یا در طول زمان خیزش مورد نظر سیستم حلقه بسته وجود داشته باشد.

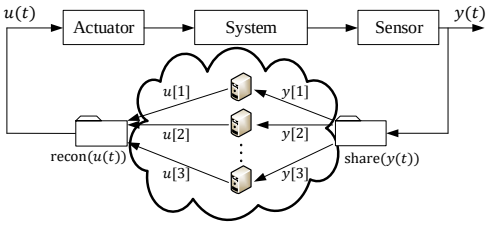
۳. کنترل کننده رمزنگاری شده

در این بخش، یک کنترل‌کننده PFC رمزشده طراحی می‌شود تا محرمانگی داده‌ها حفظ شده و از حملات سایبری جلوگیری شود. این هدف با به‌کارگیری طرح تسهیم راز (SS) در یک رویکرد رایانشی ابری توزیع‌شده محقق می‌گردد. در طرح پیشنهادی، متغیرهای $u^-(t),\ y^-(t),\ y_{\text{past}}(t),\ e(t),\ \Delta u(t),\ u(t)$ و k_{PFC} با استفاده از طرح تسهیم راز بین طرفین به اشتراک گذاشته می‌شوند. این متغیرها به‌صورت برخط به‌روزرسانی می‌شوند، به جز k_{PFC} که به‌صورت برون‌خط محاسبه می‌شود.

در این طرح، خروجی سیستم حلقه بسته، $y(t)$، بین p طرف به صورت $p \in \mathcal{P}$, $y[1],\dots,y[p]$ توزیع می‌شود. هیچ یک از این طرفین از

سهم‌های طرف دیگر آگاه نیستند. طرفین محاسبات را بر روی داده‌های تسهیم شده در فضای ابری انجام می‌دهند و $p \in \mathcal{P}$, $u[1],\dots,u[p]$ تعیین می‌شوند. سپس، سیگنال کنترل $u(t)$ از طریق بازسازی استخراج می‌گردد. ساختار کنترل‌کننده پیشنهادی در شکل ۲ نشان داده شده است.

برای به‌دست آوردن سیگنال خروجی در هر تکرار، نیاز به به‌روزرسانی سیگنال کنترل داریم. برای انجام این کار، $u^-(t)$ باید بین p طرف به صورت $u^-[p], p \in \mathcal{P}$ است توزیع شود. از آنجا که $u^-(t)$ یک ماتریس است، برای محاسبه $u^-[p]$، لازم است هر عنصر از ماتریس $u^-(t)$ بین p طرف توزیع گردد. با توجه به اینکه طرفین ما مجهز به حافظه هستند، آن‌ها می‌توانند هر سهم از عناصر $u^-(t)$ را ذخیره نمایند. به طور مشابه، عناصر ماتریس $y^-(t)$ بین p طرف توزیع می‌شوند تا $y^-[p]$ به صورت زیر به دست آید:



شکل ۲. نمودار پیاده‌سازی SS روی کنترلر.

$$y_t^-[p] = \begin{bmatrix} y_t[p] \\ \vdots \\ y_{t-n_a}[p] \end{bmatrix}, p \in \mathcal{P} \quad (۲۲)$$

برای محاسبه خصوصی $y_{\text{past}}(t+\mu_i) = y_{\text{past},1}(t+\mu_i) + y_{\text{past},2}(t+\mu_i)$ در سرورهای ابری، باید سهم‌های متناظر هر طرف، یعنی $y_{\text{past},1}^{\mu_i}[p]$ و $y_{\text{past},2}^{\mu_i}[p]$ را با هم جمع کنیم. توجه داشته باشید که $y_{\text{past},1}^{\mu_i}[p]$ به معنای سهم رمزشده $y_{\text{past},1}(t+\mu_i)$ متعلق به سرور p-ام در فضای ابری در زمان $t+\mu_i$ است.

برای انجام ضرب $y_{\text{past},1}(t+\mu_i) = \alpha_i^{\mu_i} u^-(t)$ به صورت سهم‌هایی در فضای ابری، ابتدا $\alpha_i^{\mu_i}$ را به طور جداگانه بین p طرف توزیع کرده و سپس از سه‌تایی‌های Beavers استفاده می‌کنیم. برای این کار، $r_1[p]$ و $r_2[p]$ که سهم‌های مربوط به سه‌تایی هستند، به صورت تصادفی تولید می‌شوند. سپس با اجرای روال ضرب مطابق با روابط (۵)، می‌توان $y_{\text{past},1}^{\mu_i}[p]$ را توسط تابع mult به صورت زیر محاسبه نمود:

$$y_{\text{past},1}^{\mu_i}[p] = \text{mult}(\alpha_i^{\mu_i}[p], u^-[p]), p \in \mathcal{P}, i = 1,2 \quad (۲۳)$$

به طور مشابه، مقادیر $y_{\text{past},2}(t+\mu_i) = \beta_i^{\mu_i} y^-(t)$ برای $p \in \mathcal{P}$ و $i = 1,2$ به صورت زیر محاسبه می‌شوند:

$$y_{\text{past},2}^{\mu_i}[p] = \text{mult}(\beta_i^{\mu_i}[p], y_t^-[p]), p \in \mathcal{P}, i = 1,2 \quad (۲۴)$$

در نتیجه، می‌توان محاسبه کرد:

$$y_{\text{past}}^{\mu_i}[p] = y_{\text{past},1}^{\mu_i}[p] + y_{\text{past},2}^{\mu_i}[p], p \in \mathcal{P}, i = 1,2 \quad (۲۵)$$

مقدار $k_{\text{PFC}} = (A^T A + R)^{-1} A^T$ به صورت برون‌خط محاسبه می‌شود. برای این کار، $A[p]$, $A^T[p]$ و $R[p]$ تعیین می‌شوند. سپس، معکوس $(A^T A + R) = (A^T A + R)^{-1}[p] = ((A^T A + R)r)^{-1} r[p]$ با استفاده از تابع invers محاسبه می‌گردد. در نهایت داریم:

$$k_{\text{PFC}}[p] = \text{mult}(\text{invers}(A^T A + R), A^T[p]) \quad (۲۶)$$

در محاسبه $\Delta u(t) = k_{\text{PFC}}[v_{\mu_1} v_{\mu_2}]^T[p]$، مقادیر $v_{\mu_1}[p]$ و $v_{\mu_2}[p]$ برابر هستند با:

$$v_{\mu_i}[p] = y_d^{\mu_i}[p] - y_{\text{past}}^{\mu_i}[p] - d[p], p \in \mathcal{P}, i = 1,2 \quad (۲۷)$$

در رابطه بالا، مقدار $d[p]$ بیانگر تفاوت بین خروجی فرآیند و خروجی مدل است که بین طرفین به تسهیم گذاشته شده است. برای محاسبه $\Delta u(t)$، هر عنصر از ماتریس خطا به صورت جداگانه در فضای ابری بین p طرف به تسهیم گذاشته می‌شود و سپس داریم:

$$\Delta u_t[p] = \text{mult}(k_{\text{PFC}}[p], [v_{\mu_1}[p]^T, v_{\mu_2}[p]^T]^T) \quad (۲۸)$$

در نهایت، $u(t)$ در فضای ابری به صورت زیر به تسهیم گذاشته می‌شود:

$$u^t[p] = u^{t-1}[p] + \Delta u^t[p], p \in \mathcal{P} \qquad (۲۹)$$

این طرح از n واحد محاسباتی استفاده می‌کند که محاسبات را بر روی سهم‌های داده انجام داده و مقادیر را در هر تکرار به روز می‌کنند. طرفین محاسباتی، هیچ داده اصلی‌ای را فرا نمی‌گیرند یا پردازش نمی‌کنند و خروجی که تولید می‌کنند تنها به صورت سهم‌هایی از داده است.

الگوریتم ۱ پیاده‌سازی یک کنترل‌کننده PFC دو نقطه‌ای مبتنی بر طرح تسهیم راز پیشنهادی را خلاصه می‌کند.

Algorithm 1. PFC controller based on the SS scheme.

Inputs: Process output measurements $y(t)$, Previous control inputs $u(t-1)$
Outputs: Computed control action $u(t)$

for each sampling instant t **do**
  Distribute $u^-{}_t[p] = \text{share}(u^-(t))$ among parties $p \in \mathcal{P}$
  Distribute $y^-{}_t[p] = \text{share}(y^-(t))$ among parties $p \in \mathcal{P}$
➢ *Compute predicted system states*
  for $i = 1$ *to* 2 **do**
    state_comp1$[p] = \text{mult}(\alpha_1^{\mu_i}[p], u^-[p])$,
    state_comp2$[p] = \text{mult}(\beta_1^{\mu_i}[p], y_t^-[p])$,
    reference$[p] =$ add(state_comp1$[p]$, state_comp2$[p]$)
➢ *Generate reference trajectory*
    traj_weight$[p] = \text{share}(\psi_i)$,
  for $k = 1$ to μ_i do
    $\psi_i[p] = \text{mult}(\text{traj\_weight}[p], \psi_i[p])$
  ref_comp1$[p] = \text{mult}(\psi_i[p], y_d^t[p])$,
  ref_comp2$[p] = \text{mult}(\text{add}(1, -\psi_i[p]), y_{sp}^t[p])$
    reference$[p] =$ add(ref_comp1$[p]$, ref_comp2$[p]$)
➢ *Calculate tracking error*
    error_signal$[p] =$ $add(y_d^{\mu_i}[p], -\text{reference}[p])$)
    adjusted$_{\text{error}[p]} =$ add(error_signal$[p], -d^t[p]$))
    $\Delta u^t[p] =$ mult($k_{\text{PFC}}[p]$, [adjusted$_{\text{error}_1[p][p]^T}$, adjusted_err
➢ *Update control signal*
  $u^t[p] = \text{add}(u^{t-1}[p], \Delta u^t[p])$, $p \in \mathcal{P}$
end

نکته ۱: الگوریتم ۱ یک کنترل‌کننده PFC امن را پیاده‌سازی می‌کند. ماهیت حفظ حریم خصوصی در این الگوریتم ناشی از این واقعیت است که طرفین کلیه محاسبات مربوط به کنترل‌کننده را بر اساس داده‌های تسهیم شده انجام می‌دهند. در دسترس بودن کمتر از مقدار آستانه‌ای از داده‌های اشتراکی، کسب اطلاعات درباره داده‌های اصلی را غیرممکن می‌سازد.

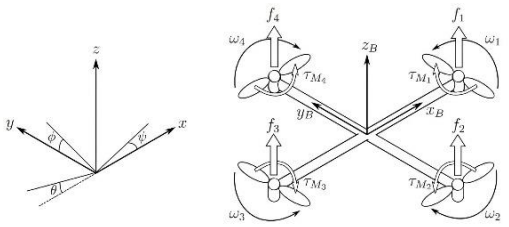
نکته ۲: برای بازسازی سیگنال کنترل، تنها به مجموعه‌ای از سهم‌های $T \subseteq P$ نیاز داریم، که در آن تعداد اعضا $T \geq k+1$ است. برای بازسازی، داشتن تمامی سهم‌های مجموعه p ضروری نیست.

نکته ۳: کنترل‌کننده‌های PFC تک‌نقطه‌ای و دو نقطه‌ای در نقاط تطبیق ورودی و خروجی و همچنین تعداد پارامترهای مورد استفاده در طراحی آنها تفاوت دارند. PFC دو نقطه‌ای می‌تواند کارایی بیشتری از نظر قابلیت پیش‌بینی ارائه دهد. الگوریتم ۱ برای یک PFC دو نقطه‌ای نوشته شده است. برای پیاده‌سازی یک PFC تک‌نقطه‌ای، استفاده تنها از μ_1 در الگوریتم ۱ کافی است.

۴. شبیه سازی

در این بخش، کنترل‌کننده PFC رمزگذاری شده پیشنهادی برای یک سیستم کوادکوپتر طراحی شده است. دینامیک کوادکوپتر با بردار حالت زیر در نظر گرفته می‌شود:

$$x = [\phi, \theta, \psi, p, q, r, z, v_x, v_y, v_z]^T \qquad (۳۰)$$



شکل ۳. بدنه‌ی کوادکوپتر.

در مدل دینامیکی کوادکوپتر، بردار حالت سیستم شامل ده متغیر به شرح زیر می‌باشد: زوایای اویلری ϕ (رول)، θ (پیچ) و ψ (یو) جهت توصیف وضعیت زاویه‌ای، نرخ‌های زاویه‌ای p ، q و r در چارچوب بدنه برای بیان سرعت چرخش حول محورهای مربوطه، متغیر z که بیانگر ارتفاع عمودی کوادکوپتر است، و در نهایت مؤلفه های سرعت خطی v_x ، v_y و v_z در راستای محورهای مختصات.

سیستم حول نقطه تعادل شناور $x_e = 0_{10\times1}$ با ورودی کنترلی $u_e = [mg/4, mg/4, mg/4, mg/4]^T$ خطی‌سازی شده است. مدل خطی‌شده به صورت $\begin{cases}\delta\dot{x} = A\delta x + B_u\delta u \\ \delta y = C\delta x\end{cases}$ است،که در آن داریم:

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$B_u = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ l/I_{xx} & 0 & -l/I_{xx} & 0 \\ 0 & l/I_{yy} & 0 & -l/I_{yy} \\ 0 & 0 & l/I_{zz} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/m & 1/m & 1/m & 1/m \end{bmatrix}$$

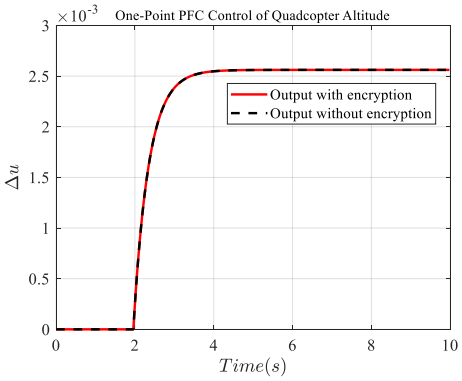
پارامترهای دینامیکی سیستم کوادکوپتر مورد استفاده در این شبیه‌سازی عبارتند از: جرم کوادکوپتر ۱ کیلوگرم، طول بازوهای آن ۰/۲۵ متر، ممان‌های اینرسی آن حول محورهای x ، y و zبه ترتیب ۰/۰۱، ۰/۰۱ و ۰/۰۲ کیلوگرم بر متر مربع، و شتاب گرانش ۹/۸۱ متر بر مجذور ثانیه می‌باشد.

مدل خطی‌شده با زمان نمونه‌برداری $T_s = 0.02$ s گسسته‌سازی شده است. کنترل‌کننده PFC از ۱۳ سرور محاسباتی در ابر با اندیس‌های $\mathcal{P} = [0.5,1,1.5,2,2.5,3,3.5,4,4.5,5,5.5,6,6.5]$ استفاده می‌کند. متغیرهای تصادفی از توزیع گاوسی با میانگین صفر و واریانس $\sigma^2 = 1000$ انتخاب شده‌اند.

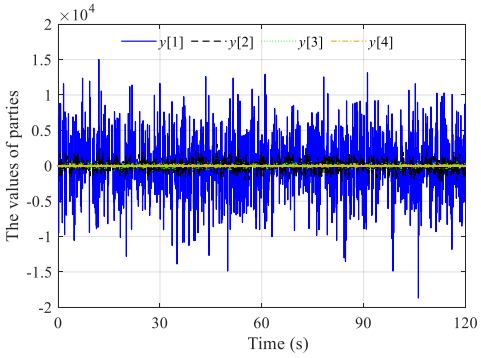
۱.۴. کنترل کننده PFC تک نقطه:

پارامترهای کنترل‌کننده PFC تک‌نقطه‌ای برای کنترل ارتفاع به‌صورت زیر تنظیم شده‌اند: نقطه تطابق در $\mu_1 = ۱۵$ گام پیش‌بین، وزن کنترل‌کننده $R = ۰/۱$، قطب فیلتر هموارساز $\psi = ۰/۹۵$ و بهره کنترل کننده $k_{\mathrm{PFC}} = ۰/۵$ در نظر گرفته شده است. از آنجا که هر سرور محاسباتی تنها به سهم مربوط به خود از سیگنال خروجی دسترسی دارد و قادر به استنباط هیچ اطلاعاتی از مقدار اصلی داده نیست، حریم خصوصی داده‌های خروجی در کنترل‌کننده پیشنهادی حفظ خواهد شد. برای اثبات این امر، سهم‌های چهار سرور مختلف برای سیگنال خروجی رمزگذاری‌شده y در شکل ۴ نشان داده شده است.

همان‌طور که مشاهده می‌شود، مقدار دریافتی هر سرور تفاوت قابل‌توجهی با سیگنال اصلی دارد. علاوه بر این، سهم‌ها به‌صورت تصادفی بین سرورهای مختلف در طول شبیه‌سازی توزیع شده‌اند. بنابراین، بدون همکاری و تبانی، سرورهای منفرد به داده‌های محرمانه سیستم دسترسی نخواهند داشت.



شکل ٤. پاسخ‌های PFC تک نقطه‌ای رمزگذاری شده/رمزگذاری نشده.



شکل ۵. سهم سیگنال خروجی y که توسط ٤ سرور محاسباتی اول دریافت می‌شود.

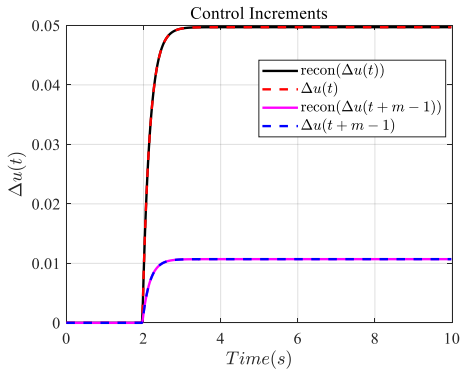
۲.۴. کنترل کننده PFC دو نقطه:

در این بخش، یک کنترل‌کننده PFC دو نقطه‌ای رمزگذاری شده با استفاده از پارامترهای مشابه طرح تسهیم راز طراحی شده است. پارامترهای کنترل‌کننده به صورت زیر انتخاب شده‌اند:

$$k_{PFC} = \begin{bmatrix} 0.0185 & 0.0421 \\ -0.0052 & 0.0287 \end{bmatrix}, R = 0.1I_{2\times 2} \quad (۳۱)$$

$$\mu_1 = 15, \quad \mu_2 = 30, m = 10, \psi_1 = 0.9, \quad \psi_2 = 0.95 \quad (۳۲)$$

ماتریس بهره PFC، k_{PFC} به صورت آفلاین و بر اساس ضرایب پاسخ پله سیستم و نقاط تطابق انتخاب شده محاسبه می شود. ماتریس وزن دهی R اقدام کنترلی را جریمه می‌کند، در حالی که قطب‌های فیلتر هموارساز ψ_1 و ψ_2 مسیر مطلوب را برای ردیابی نقطه تنظیم تعیین می کنند. افق کنترلی $m = 10$ اطمینان می دهد که افزایش کنترل آتی $\Delta u(t+m-1)$ به درستی در بهینه‌سازی لحاظ شود.



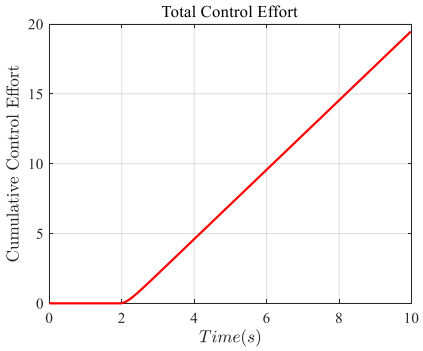
شکل ۶. پاسخ‌های PFC دو نقطه‌ای رمزگذاری شده/رمزگذاری نشده.

عملکرد کنترل‌کننده رمزگذاری شده با نمونه بدون رمز آن در شکل ۶ مقایسه شده است. همان‌طور که در نتایج شبیه‌سازی نشان داده شده است، کنترل‌کننده PFC دو نقطه‌ای رمزگذاری شده ضمن حفظ حریم خصوصی داده‌ها از طریق طرح تسهیم راز، عملکرد ردیابی ممتازی را حفظ می‌کند. این کنترل‌کننده تغییرات مرجع ارتفاع را با کم‌ترین فراجهش و زمان نشست سریع به طور مؤثر مدیریت می‌کند. رابطه اساسی بین عملکرد کنترلی و مصرف انرژی در کنترل‌کننده PFC دو نقطه‌ای را نشان می‌دهد. این نمودار کارایی کنترل‌کننده را از دو منظر کلیدی بررسی می‌کند: از یک سو توزیع آماری سیگنال‌های کنترلی که بیانگر میزان پرخاشگری کنترل‌کننده است و از سوی دیگر تجمع انرژی مصرفی در طول زمان که هزینه دستیابی به عملکرد مطلوب را کمّی می‌سازد.

الگوی به دست آمده نشان می‌دهد که کنترل‌کننده رمزگذاری شده با وجود محاسبات توزیع شده در فضای ابری، چگونه بهینه‌ترین مسیر بین دقت ردیابی و مصرف انرژی را طی

می‌کند. این تحلیل به وضوح نشان می‌دهد که طرح تسهیم راز اگرچه موجب افزایش جزئی در نوسانات کنترلی می‌شود، اما در مجموع کارایی سیستم را در سطح قابل قبولی حفظ می‌کند.

همان‌طور که در شکل‌های ۴ و ۶ نشان داده شده است، خروجی‌های رمزگذاری شده و بدون رمز کنترل‌کننده‌های PFC تک‌نقطه‌ای و دونقطه‌ای با دقت قابل توجهی با یکدیگر مطابقت دارند.



شکل ۷: تحلیل تلاش کنترلی در کنترل‌کننده PFC دو نقطه‌ای رمزگذاری‌شده.

دقت را می‌توان با استفاده از خطای مربع ریشه(RSE) بین نتایج رمزگذاری شده و بدون رمز y و $\hat{y}$ ارزیابی کرد که به صورت زیر محاسبه می‌شود:

$$\mathrm{RSE} = \sqrt{\sum_{i=1}^{N} \left(y(i) - \hat{y}(i)\right)^2} \qquad (۳۳)$$

که در آن N نشان‌دهنده تعداد کل تکرارهای شبیه‌سازی است. مقادیر به‌طور استثنایی پایین RSE، در حدود 10^{-5} برای PFC تک‌نقطه‌ای و 10^{-4} برای PFC دونقطه‌ای، پایداری عددی طرح تسهیم راز را نشان می‌دهد. این اختلاف ناچیز تأیید می‌کند که فرآیند رمزگذاری، خطاهای محاسباتی قابل چشم‌پوشی را معرفی می‌کند در حالی که به طور مؤثر محرمانگی داده را حفظ می‌نماید. مقدار کمی بالاتر RSE در پیاده‌سازی PFC دونقطه‌ای را می‌توان به تعداد عملیات ریاضی رمزگذاری شده بیشتر، به ویژه محاسبات ضرب ماتریسی و معکوس اضافی مورد نیاز برای فرمولاسیون دو نقطه‌ای نسبت داد. علیرغم این افزایش جزئی، هر دو پیاده‌سازی عملکرد کنترلی عالی را حفظ می‌کنند و PFC دونقطه‌ای به دلیل قابلیت پیش‌بینی یافته از طریق نقاط تطابق متعدد، قابلیت ردیابی برتری را ارائه می‌دهد. همترازی پیوسته بین خروجی‌های رمزگذاری شده و بدون رمز در هر دو نوع کنترل‌کننده، امکان‌پذیری عملی پیاده‌سازی سیستم‌های کنترل حفظ حریم خصوصی در محیط‌های ابری را بدون به خطر انداختن کیفیت کنترل تأیید می‌کند.

جدول ۱. مقایسه PFC های یک نقطه‌ای و دو نقطه‌ای از نظر خطای رمزگذاری.

PFC Controller	RSE
one-point	0.4404×10^{-5}
two-point	0.7509×10^{-4}

۵. جمع‌بندی و نتیجه گیری

در این مقاله، یک طرح تسهیم راز (SS) بر روی کنترل‌کننده پیش‌بین تابعی (PFC) پیاده‌سازی شده است. این پیاده‌سازی، یک کنترل‌کننده حفظ‌کننده حریم خصوصی در فضای ابری فراهم می‌کند. با توزیع داده‌های مشترک بین طرف‌های مختلف، محاسبات توزیع شده و می‌توانند به صورت موازی توسط طرف‌ها انجام شوند. کنترل‌کننده رمزگذاری شده عملکردی بسیار مشابه با کنترل‌کننده بدون رمز نشان می‌دهد. از نظر خطای رمزگذاری، PFC تک‌نقطه‌ای رمزگذاری شده بهتر از PFC دونقطه‌ای رمزگذاری شده عمل می‌کند، زیرا در مورد اخیر تعداد عملیات ریاضی رمزگذاری شده بیشتری انجام می‌شود که منجر به خطای رمزگذاری بیشتری

می‌شود. با این حال، به طور کلی، PFC دونقطه‌ای از نظر عملکرد کنترلی بهتر از PFC تک‌نقطه‌ای است زیرا قابلیت پیش‌بینی بهتری دارد. طرح پیشنهادی مبتنی برتسهیم راز اعداد حقیقی (RSS)از پیچیدگی محاسباتی کمتری نسبت به روش‌های رمزنگاری هوموروفیک برخوردار است. در این معماری، بار پردازشی بین چندین سرور توزیع شده و محاسبات به صورت موازی انجام می‌گیرد. همچنین، استفاده از کنترل پیش‌بین عملکردی (PFC) که ذاتاً نیاز محاسباتی کمتری دارد، به کاهش سربار کلی کمک می‌کند. در شبیه‌سازی انجام‌شده با زمان نمونه‌برداری $T_s = 0.02\,\mathrm{s}$ و ۱۳ سرور ابری، سیستم قادر به حفظ پایداری و عملکرد مطلوب بوده و خطای محاسباتی ناشی از رمزنگاری در حد 10^{-5} تا 10^{-4} گزارش شده است. این نتایج نشان می‌دهند که طرح پیشنهادی علیرغم افزودن لایه امنیتی، از نظر محاسباتی کارآمد و قابل اجرا در محیط‌های بلادرنگ است.

۶. محدودیت‌ها

اگرچه نتایج شبیه‌سازی عملکرد مطلوب و حفظ حریم‌خصوصی کنترل‌کننده‌ی رمزگذاری‌شده را تأیید می‌کنند، این پژوهش تحت فرض وجود یک کانال ارتباطی ایده‌آل و بدون تأخیر بین نهادها (پهپاد و سرورهای ابری) انجام شده است. در محیط‌های عملیاتی، اجرای پروتکل‌های تسهیم راز نیازمند تبادلات پیام و محاسبات توزیع‌شده است که می‌تواند سربار زمانی و تأخیر ارتباطاتی قابل‌توجهی را به حلقه‌ی کنترل تحمیل کند. این تأخیرها در صورت عدم مدیریت، ممکن است بر پایداری و کارایی سیستم تأثیر بگذارند. بنابراین، در نظر گرفتن اثرات تأخیر شبکه و ارائه‌ی راهکارهای جبران‌ساز (مانند استفاده از پیش‌بینی‌کننده‌های حالت یا مکانیسم‌های کنترل رویداد-محور برای بهینه‌سازی ترافیک داده) به عنوان یک گام ضروری بعدی برای تبدیل این طرح به یک راه‌حل عملی‌شده مطرح می‌شود. همچنین، ارزیابی عملکرد طرح پیشنهادی بر روی یک بستر آزمایشی سخت‌افزاری یا شبیه‌ساز شبکه‌ای واقع‌گرا جهت اندازه‌گیری دقیق سربار و مقاوم‌سازی آن در برابر نویز و از دست‌دادن بسته‌های داده، از دیگر محورهای پژوهشی آتی خواهد بود.

۷. فهرست علائم

نماد	توضیح
$\boldsymbol{s}$	راز اصلی
$\boldsymbol{k}$	آستانه بازسازی راز
$\boldsymbol{p}$	تعداد طرف‌ها یا سرورها
$\boldsymbol{T}$	زیرمجموعه‌ای از طرف‌ها با حداقل $\boldsymbol{k+1}$ عضو
$q_s(x)$	چندجمله‌ای درجه $\boldsymbol{k}$ برای اشتراک‌گذاری راز $\boldsymbol{s}$
$L_j(x)$	چندجمله‌ای پایه‌ی لاگرانژ
$s[p]$	سهم $\boldsymbol{p}$ام از راز $\boldsymbol{s}$
σ^2	واریانس توزیع گاوسی برای ضرایب تصادفی
$y(t)$	خروجی سیستم در زمان $\boldsymbol{t}$
$u(t)$	سیگنال کنترل در زمان $\boldsymbol{t}$
$\Delta u(t)$	تغییرات سیگنال کنترل
μ_1, μ_2	نقاط تطابق(Coincidence Points)
m	افق کنترلی(Control Horizon)
g_i	ضریب پاسخ پله واحد در گام $\boldsymbol{i}$
$y_d(t)$	خروجی مطلوب(Reference)
$y_{sp}(t)$	نقطه تنظیم(Setpoint)
ψ	قطب فیلتر هموارساز$(\boldsymbol{0 \le \psi < 1})$
$d(t)$	خطای مدل‌سازی/اغتشاش
R	ماتریس وزن‌دهی کنترل
r	فاکتور وزن‌دهی کنترل (اسکالر)
k_{PFC}	ماتریس بهره کنترل‌کننده PFC
T_s	زمان نمونه‌برداری
ϕ, θ, ψ	زوایای اویلر (رول، پیچ، یاو)
p, q, r	نرخ‌های زاویه‌ای در چارچوب بدنه
v_x, v_y, v_z	مؤلفه‌های سرعت خطی
I_{xx}, I_{yy}, I_{zz}	ممان‌های اینرسی حول محورهای $\boldsymbol{x, y, z}$
RSE	خطای مربعات ریشه

۸. مآخذ

[1] K. Tjell and R. Wisniewski, “Privacy in distributed computations based on real number secret sharing,” Journal of the Franklin Institute, vol. 359, no. 16, pp. 8752–8771, November 2022.

[2] C. Shamir, A. Shamir, A. Surendar, B. Binyamin, D. O. Bokov, D. Toghraie, and M. Omidi, “How to share a secret,” Journal of Thermal Science, vol. 22, no. 11, pp. 612–613, September 1979.

[3] M. J. Atallah and W. Du, "Secure multi-party computational geometry," *Workshop on Algorithms and Data Structures*, pp. 165–179, 2001.

[4] R. Cramer, I. Damgård, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.

[5] Z. Brakerski, “Fully homomorphic encryption without modulus switching from classical GapSVP,” in *Proc. Annu. Cryptol. Conf.*, 2012, pp. 868–886.

[6] A. C. C. Yao, “How to generate and exchange secrets,” *Journal of Thermal Science*, vol. 31, no. 5, pp. 1663-1681, September 2022.

[7] M. S. Darup and T. Jager, “Encrypted cloud-based control using secret sharing with one-time pads,” in Proceedings of the 58th IEEE Conference on Decision and Control, 2019, pp. 7215–7221.

[8] C. Mohtadi, D. W. Clarke, and P. S. Tuffs, “Generalized predictive control—Part I. The basic algorithm,” *Automatica*, vol. 23, no. 2, pp. 137–148, 1987.

[9] D. Bogdanov, S. Laur, and J. Willemson, “Sharemind: A framework for fast privacy-preserving computations,” *European Symposium on Research in Computer Security*, Berlin, Heidelberg, pp. 192–206, 2008.

[10] T. Nishide and K. Ohta, “Multiparty computation for interval, equality, and comparison without bit-decomposition protocol,” *International Workshop on Public Key Cryptography*, Berlin, Heidelberg, pp. 343–360, 2007.

[11] C. E. F. Camacho and C. Bordons, “Model Predictive Control,” London, U.K.: Springer, 2007.

[12] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," *Journal of Decision and Control*, vol. 54, no. 1, pp. 6836–6843, December 2015.

[13] J. A. Rossiter and M. S. Aftab, “Recent developments in tuning methods for predictive functional control,” *Processes*, vol. 10, no. 7, p. 1398, 2022.

[14] Z. Zhang, L. Xie, S. Lu, J. A. Rossiter, and H. Su, “A low-cost pole-placement MPC algorithm for controlling complex dynamic systems,” *Journal of Process Control*, vol. 111, pp. 106–116, March 2022.

[15] M. S. Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, “Encrypted control for networked systems: An illustrative introduction and current

challenges," IEEE Control Systems Magazine, vol. 41, no. 3, pp. 58–78, June 2021.
[16] S. J. Qin and T. A. Badgwell, "A survey of industrial model predictive control technology," *Control Engineering Practice*, vol. 11, no. 7, pp. 733–764, Jul. 2003.
[17] D. W. Clarke, C. Mohtadi, and P. S. Tuffs, "Generalized predictive control—Part I. The basic algorithm," *Automatica*, vol. 23, no. 2, pp. 137–148, March 1987.
[18] J. A. Rossiter, *Model-Based Predictive Control: A Practical Approach*. Boca Raton, FL, USA: CRC Press, 2003.
[19] R. A. Gupta and M. Y. Chow, "Networked control system: Overview and research trends," IEEE Transactions on Industrial Electronics, vol. 57, no. 7, pp. 2527–2535, July 2010.
[20] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Hong Kong, 2011, pp. 355–366.
[21] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 24–45, February 2015.
[22] C. Murguia and J. Ruths, "On model-based detectors for linear time-invariant stochastic systems under sensor attacks," *IET Control Theory & Applications*, vol. 13, no. 8, pp. 1051–1061, May 2019.
[23] C. M. S. Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, "Encrypted control for networked systems: An illustrative introduction and current challenges," IEEE Control Systems Magazine, vol. 41, no. 3, pp. 58–78, 2021.
[24] K. Tjell and R. Wisniewski, "Privacy in distributed computations based on real number secret sharing," *arXiv preprin* arXiv:2107.00911, 2021.
[25] Y. A. Kadakia, F. Abdullah, A. Alnajdi, and P. D. Christofides, "Encrypted distributed model predictive control of nonlinear processes," *Control Eng. Pract.*, vol. 145, p. 105874, 2024.
[26] J. Blevins and J. Ueda, "Encrypted model reference adaptive control with false data injection attack resilience via somewhat homomorphic encryption-based overflow trap," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, pp. 1–14, 2025.
[27] A. Khodaverdian, G. Wu, Z. Wu, and P. D. Christofides, "Encrypted machine learning-based model predictive control architectures for nonlinear systems," *Computers & Chemical Engineering*, vol. 196, p. 109166, December 2025.
[28] C. Sui, J. Wang, W. Liu, J. Pan, L. Wang, Y. Zhao, and L. Kong, "Optimizing encrypted control algorithms for real-time secure control," Journal of the Franklin Institute, vol. 361, no. 5, p. 106677, March 2024.
[29] C. Gentry, "Fully homomorphic encryption using ideal lattices," Proc. ACM STOC, Bethesda, MD, USA, pp. 169–178, 2009.
[30] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," Proceedings of the 3rd ACM Cloud Computing Security Workshop, Chicago, IL, USA, pp. 113–124, October 2011.
[31] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," IEEE Transactions on Automatic Control, vol. 52, no. 9, pp. 1680–1685, September 2007
[32] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Journal of Thermal Science*, vol. 31, no. 5, pp. 1663–1681, September 2022.
[33] M. Schulze Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, "Encrypted cooperative control based on structured feedback," *IEEE Transactions on Automatic Control*, vol. 66, no. 1, pp. 1–13, January 2021.
[34] Y. Mo and B. Sinopoli, "Secure control against replay attacks," *Proc. IEEE Conf. Decision Control*, Shanghai, China, pp. 597–602, 2009

۷. پی نوشت‌ها

1 Secret Shair (SS)
2 Real Secret Sharing (RSS)
3 Model Predictive Control (MPC)
4 Homomorphic Encryption (HE)