طراحی رویتگر امن با ورودی ناشناخته با استفاده از رمزنگاری

لادن صادقی خرمی[۱]، دانشجوی دکتری؛ سید علی اکبر صفوی[۲] ، استاد

۱- دانشکده مهندسی برق و کامپیوتر- دانشگاه شیراز- شیراز- ایران– sadeghikhorrami@gmail.com
۲- دانشکده مهندسی برق و کامپیوتر- دانشگاه شیراز- شیراز- ایران– safavi@shiraz.ac.ir

چکیده: در این مقاله، رویتگر امن با ورودی ناشناخته در سیستم کنترل مبتنی بر شبکه طراحی می‌شود. برای این هدف، تکنیک رمزنگاری پیلیر، که یک روش رمزنگاری نیمه همگن است، به کار گرفته می‌شود. محاسبات تخمین حالت بر حسب رمزنگاری انجام و در نهایت تخمین حالت‌ها به صورت رمز شده تولید خواهند شد. شرط محدود بودن خطای تخمین با در نظر گرفتن پردازشگر دیجیتال به دست می‌آید. این روش، امنیت تخمین حالت‌های سیستم را بالا می‌برد و در واقع از حملاتی که محرمانگی داده‌ها را از بین می‌برند، جلوگیری می‌کند. نتایج شبیه سازی انجام شده بر روی TE-PCS موفقیت روش پیشنهادی را نشان می‌دهد.

واژه‌های کلیدی: رویتگر با ورودی ناشناخته، امنیت سایبری، سیستم کنترل مبتنی بر شبکه.

Designing Secure Unknown Input Observer Using Encryption

L. Sadeghikhorrami[1], PhD student; A. A. Safavi[2], Professor

1- School of Electrical and Computer Engineering, University of Shiraz, Shiraz, Iran, Email: sadeghikhorrami@gmail.com
2- School of Electrical and Computer Engineering, University of Shiraz, Shiraz, Iran, Email: safavi@shiraz.ac.ir

Abstract: In this paper, a secure unknown input observer is designed in a networked control system environment. For this propose, the Paillier encryption, which is a semi- homomorphic encryption method, is employed. The algebraic calculations required for the estimation can be performed over the encrypted data and the encrypted states estimation are generated. The boundedness condition of estimation error is obtained by considering the digital processor. This method increases the security of system state estimates and effectively eliminates attacks that disrupt the confidentiality of the data. Simulation on the TE-PCS will be performed to illustrate the results.

Keywords: Unknown input observer, Cyber security, Network control system.

تاریخ ارسال مقاله: ۱۳۹۷/۰۴/۱۱
تاریخ اصلاح مقاله: ۱۳۹۷/۰۷/۲۹
تاریخ پذیرش مقاله: ۱۳۹۷/۱۰/۲۹
نام نویسنده مسئول: سید علی اکبر صفوی
نشانی نویسنده مسئول: - دانشکده مهندسی برق و کامپیوتر، دانشگاه شیراز، شیراز، ایران.

۱- مقدمه

امنیت سایبری سیستم کنترل مبتنی بر شبکه مرتبط با زیر ساخت‌های صنعتی چالش بزرگی است. تهدیدات سایبری می‌توانند بر محرمانه بودن، یکپارچگی و یا دسترسی داده‌ها بر اساس منابع موجود مهاجم تأثیر بگذارند. به عنوان مثال، در حمله استراق سمع[۱] یا حمله خرابکاری[۲]هدف، دستیابی به اطلاعات منتقل شده بین سنسورها، کنترل کننده‌ها و محرک‌ها است [۱].

روش‌های متعددی جهت امن کردن سیستم کنترل تحت شبکه در برابر تهدیدات سایبری در مقالات بررسی شده‌اند. چند مثال از این روش‌ها عبارت‌اند از طراحی سیستم تشخیص مبتنی بر مدل [۳,۲]، سیستم تشخیص با استفاده از روش‌های داده کاوی [۵,۴]، سیستم تشخیص مبتنی بر مدل فیزیکی و شبکه [۶] مدیریت ریسک [۷] و محافظت از سیگنال انتقالی از شبکه [۸] است. یک روش جهت حفظ محرمانگی سیگنال‌های منتقل شونده در سیستم کنترل تحت شبکه، رمز نگاری آن سیگنال‌ها است. استفاده از رمزنگاری، امنیت سیگنال‌های عبوری از شبکه (داده‌های سنسوری و سیگنال کنترلی) را افزایش می دهد و از حمله استراق سمع و یا شنود جلوگیری می‌کند. اطلاعات سنسوری قبل از ارسال از طریق شبکه ابتدا رمز شده، سپس بر روی شبکه منتقل شده و در سمت کنترلر، ابتدا رمزگشایی کرده، سپس سیگنال رمزگشایی شده وارد کنترلر می‌شود[۹]. در هین راستا تلاش‌های روزافزونی برای توسعه الگوریتم کنترلرها و رویتگرهای رمز شده در حال انجام است به گونه‌ای که بتوانند ورودی رمز شده را دریافت و خروجی رمز شده را تولید نمایند که مقالات [۱۴-۱۰] نمونمه هایی از آن‌ها است. اگر از کنترلر رمزنگاری شده برای حفظ محرمانگی سیگنال استفاده شود، نسبت به روش‌های قدیم همانند مرجع [۹]، دیگر نیازی به رمزگشایی سیگنال قبل از ورود به کنترلر نیست و سیگنال رمز شده مستقیماً به کنترلر رمزشده وارد می‌شود. در این روش داده‌های سنسوری قبل از ارسال به شبکه رمز شده و سپس به شبکه ارسال می‌شود. چون کنترلر به گونه‌ای طراحی شده است که بر روی سیگنال‌های رمز شده محاسبات کنترلی را انجام می‌دهد بنابراین نیازی به رمزگشایی سیگنال نمی‌باشد و سیگنال رمز شده مستقیماً به کنترلر وارد می‌شود. هم چنین سیگنال کنترلی نیز قبل از ارسال ابتدا رمز شده و سپس از طریق شبکه ارسال می‌شود. بنابراین، می‌بایست عملکرد کنترلر نیز بر اساس داده‌های رمز شده باشد و اگر نقص امنیتی در واحد کنترل رخ دهد، مهاجم قادر به بازسازی داده‌ها نباشد.

رمزنگاری در این کاربردها می‌تواند به دو روش رمزنگاری همگن کامل[۳] و نیمه همگن[۴] انجام شود. در رمزنگاری همگن همه عملیات ریاضی را می‌توان انجام داد. رمزنگاری نیمه همگن یک فرم ساده‌تر از رمزنگاری همگن است و تنها اجازه می‌دهد دسته عملیات خاصی بر روی داده‌ها انجام شود [۱۰]. این عملیات یا فقط جمع شونده و یا فقط ضرب شونده است. رمزکردن ساده‌ترین نوع کنترلر که کنترلر فیدیک حالت است با استفاده از دو روش متفاوت از مجموعه روش‌های رمزنگاری نیمه همگن در مقالات [۱۲,۱۰] بررسی شده‌اند. در مقاله [۱۱]، برای به دست آوردن یک کنترل کننده خطی امن از رمزنگاری همگن کامل استفاده کرده و پارامترهای رمزنگاری را از شرط پایداری سیستم حلقه بسته به دست آورده است. کنترل کننده پیش‌بین خطی رمزشده امن و خصوصی برای سیستم‌های با محدودیت خطی با استفاده از رمزنگاری نیمه همگن در [۱۳] و برای سیستم‌های بدون محدودیت در [۱۴] طراحی شده‌اند. روشی برای محلی سازی یک هدف موبایل بر اساس اندازه گیری‌های رمز شده سنسورها در مقاله [۱۵] تحلیل شده است. نویسنده [۱۶] به رمزنگاری رویتگر لوئنبرگر با استفاده از رمزنگاری نیمه همگن پرداخته است. مقاله [۱۷] رمزنگاری همگن از نوع جمع شونده برای توسعه فیلتر کالمن استفاده شده‌است ولی در این مقاله پایداری مورد بحث قرار نگرفته است.

مقالات [۱۰-۱۴] مربوط به کنترلر رمز شده می‌باشد. در مقابل، در این مقاله هدف، طراحی یک رویتگر امن رمزشده است. مقالات [۱۷,۱۶] به دنبال رویتگرهای امن هستند. در این مقاله نیز، رویتگر رمزشده جهت تضمین امنیت و حفظ محرمانگی با استفاده از رمزنگاری نیمه همگن بررسی می‌شود. هیچ‌یک از مقالات موجود رمزنگاری رویتگر با ورودی ناشناخته را بررسی نکرده‌اند. اما در این مقاله، رویتگر با ورودی ناشناخته رمز شده به وسیله تکنیک رمز نگاری نیمه همگن از نوع پیلیر[۵] [۱۸]، که از نظر محاسبات آسان‌تر از رمزنگاری همگن است، معرفی می‌شود. این تکنیک باعث می‌شود رویتگر پیشنهادی به هیچ کلید خصوصی رمز نگاری نیاز نداشته باشد. وجود رویتگر رمز شده سبب می‌شود رویتگر به نقص امنیتی و خصوصی در واحد محاسبات مقاوم باشد. در این مقاله امنیت تنها در برابر محرمانگی داده‌ها مدنظر قرار گرفته‌است. همچنین با در نظر گرفتن خطای کوانتیزه شدن و با استفاده از اثبات ثابت ماندن خطای تخمین در این وضعیت، مقادیر پارامترهای محاسبات رمزنگاری را به دست آورده است که نسبت به دو مقاله [۱۷,۱۵] که تخمین زننده رمز شده را طراحی کرده‌اند، برتری دارد. اگر رویتگر با ورودی ناشناخته رمزشده را برای طراحی سیستم تشخیص استفاده نمود، می‌توان سیستم را در مقابل حمله تزریق داده غلط علاوه بر حمله شنود، ایمن کرد.

با توجه به نکات ذکر شده، باید گفت که در این مقاله، ابتدا در بخش دوم مباحث مورد نیاز از محاسبات ممیز ثابت و سپس رمز نگاری نیمه همگن به صورت خلاصه بیان می‌شود. در بخش سوم الگوریتم رویتگر با ورودی ناشناخته رمز شده معرفی می‌شود. در بخش چهارم شبیه سازی با استفاده از رویتگر پیشنهادی بر روی TE-PCS با استفاده از برنامه پایتون نشان داده می‌شود. در نهایت، مقاله در بخش پنجم نتیجه‌گیری خواهد شد و کارهای آتی در این موضوع بیان می‌گردد.

۲- مباحث مورد نیاز

در این بخش دو مبحث اعداد اعشاری ممیز ثابت و تئوری رمزنگاری مرور می‌شوند.

۲-۱- محاسبات ممیز ثابت

در این مقاله، اعداد اعشاری ممیز ثابت در مبنای ۲ برای اعداد $n, m \in \mathbb{N}$ در نظر گرفته شده است، به طوری که $m \le n$ باشد:

$$\pm \underbrace{c_n c_{n-1} c_{n-2} \cdots c_{m+1}}_{\text{integer bits}} \cdot \underbrace{c_m c_{m-1} \cdots c_1}_{\text{fractional bits}}$$

که این مجموعه شامل تمام اعداد به صورت زیر است:

$$\mathbb{Q}(n,m) := \left\{ b \in \mathbb{Q} \mid b = -b_n 2^{n-m-1} + \sum_{i=1}^{n-1} 2^{i-m-1} b_i \ , b_i \in \{0,1\} \ \forall\, i \in \{1, \dots, n\} \right\}.$$

این مجموعه شامل تمامی اعداد اعشاری در بازه $[-2^{n-m-1}, 2^{n-m-1} - 2^{-m}]$ است. برای استفاده از این اعداد در پردازشگر دیجیتال می‌بایست این اعداد را به اعداد طبیعی انتقال دهیم. بنابراین از انتقال $f_{n,m}: \mathbb{Q}(n,m) \to \mathbb{Z}_{2^n}$ استفاده می‌شود، به طوری که $f_{n,m}(b) = 2^m\, b \bmod 2^n$ ، $b \in \mathbb{Q}(n,m)$ و $\mathbb{Z}_{2^n}$ بیانگر تمامی اعداد طبیعی کوچکتر از 2^n است. معکوس این انتقال برای $a \in \mathbb{Z}_{2^n}$، $f_{n,m}^{-1}(a) = (a - 2^n|_{a \ge 2^{n-1}})/\, 2^m$ است، به طوری که $|_p$ بیانگر

$$|_p = \begin{cases} 1 & if\ the\ statement\ p\ holds\ true, \\ 0 & otherwise \end{cases}$$

است. به کمک نتایج مقاله [۱۰] لم‌های زیر جهت کاربردهای آتی تعریف شده است. برای اثبات آن‌ها می‌توان به آن مقاله مراجعه کرد.

لم۲-۱- دو عبارت زیر که بیانگر هم ریخت[۶] بودن تابع انتقال است، برقرار هستند:

۱. $f_{n,m}^{-1}\left(f_{n,m}(b)\right) = b \ for\ all\ b \in \mathbb{Q}(n,m)$

۲. $f_{n,m}\left(f_{n,m}^{-1}(a)\right) = a \ for\ all\ a \in \mathbb{Z}_{2^n}$

لم ۲-۲- عملگرهای ابتدایی زیر برای تابع انتقال ذکر شده برقرار است:

۱. اگر $b, b' \in \mathbb{Q}(n,m)$ و $b + b' \in \mathbb{Q}(n,m)$ باشد، آنگاه $f_{n,m}(b + b') = \left(f_{n,m}(b) + f_{n,m}(b')\right) \bmod 2^n$.

۲. اگر $b \in \mathbb{Q}(\mathrm{n,m})$ و $-b \in \mathbb{Q}(\mathrm{n,m})$ باشد، آنگاه $f_{n,m}(-b) = 2^n - f_{n,m}(b)$.

۳. اگر $b, b' \in \mathbb{Q}(n,m)$ و $b - b' \in \mathbb{Q}(n,m)$ باشد، آنگاه $f_{n,m}(b - b') = \left(2^n + f_{n,m}(b) - f_{n,m}(b')\right) \bmod 2^n$.

۴. اگر $b, b' \in \mathbb{Q}(n,m)$ و $bb' \in \mathbb{Q}(n,m)$ باشد، آنگاه $f_{n,m}(bb') = \left(\left(f_{n,m}(b) - 2^n|_{b<0}\right)\left(f_{n,m}(b') - 2^n|_{b'<0}\right)/2^m\right) \bmod 2^n$.

به دلیل وابسته بودن عملگر ضرب به علامت، پروسه پیچیده‌تری در مقابل عملگر جمع دارد. از این رو لم زیر بیان می‌شود.

لم ۲-۳- خصوصیت‌های زیر برای $f(b), f(b') \in \mathbb{Z}_{2^n}$ برقرار است:

۱. $f_{n,0}(bb') = \left(f_{n,0}(b)\, f_{n,0}(b')\right) \bmod 2^n$

۲. اگر $2^m \mid f_{n,m}(b')$ و $f_{n,m}(b') < 2^{n-1}$ باشد، آنگاه $f_{n,m}(bb') = \left(\left(f_{n,m}(b)\right)\left(f_{n,m}(b')\right)/2^m\right) \bmod 2^n$

لم۲-۴- طبق مقاله [۱۰]، اگر $m \neq 0$ ، $b, b' \in \mathbb{Q}(n,m)$ و $bb' \in \mathbb{Q}(n,m)$ باشد، آنگاه عبارت زیر را خواهیم داشت:

$$f_{n+2m,0}(2^{2m} bb') = \left(\left(f_{n+2m,0}(2^m b)\right)\left(f_{n+2m,0}(2\text{^}mb')\right)\right).$$

۲-۲- رمز نگاری نیمه همگن

در این زیر بخش، تکنیک رمزنگاری پیلیر که یک نوع رمزنگاری نیمه همگن ساده است، معرفی می‌شود. این نوع رمزنگاری از نوع رمزنگاری جمع شونده است. در ادامه خاصیت‌های این نوع رمزنگاری بیان می‌شوند و علت جمع شونده بودن مشخص خواهد شد.

تابع‌های رمزنگاری و رمزگشایی بدین صورت است:

رمزنگاری:

فرض کنید N حاصل‌ضرب دو عدد بزرگ و اول p و q باشد که به صورت تصادفی و مستقل از یکدیگر انتخاب شده و خاصیت زیر را داشته باشد:

$$gcd^{\vee}\left(pq, (1-p), (1-q)\right) = 1$$

رمزنگاری پیام $t \in \mathbb{Z}_{\mathrm{N}}$ از رابطه زیر محاسبه می‌شود:

$$E(t;r) = (N+1)^t r^N \bmod N^2$$

به طوری که $r \in \mathbb{Z}_N^* := \{x \in \mathbb{Z}_N | gcd(x, N) = 1\}$ و به صورت تصادفی انتخاب شود. N کلید عمومی است و تمامی قسمت‌ها آن را می دانند و در رمزنگاری از آن استفاده می‌کنند.

رمزگشایی:

اگر $\lambda = lcm\text{^}(p-1, q-1)$ و $\mu = \lambda^{-1} \bmod N$ باشد جفت (λ, μ) کلید خصوصی است که تنها برای قسمت‌هایی که رمزگشایی در آن‌ها انجام می‌شود نیاز است. رمزگشایی پیام رمز شده $\mathrm{c} \in \mathbb{Z}_{\mathrm{N}^2}$ به صورت

$$D(c) = \left(\left(c^{\lambda} \bmod N^2\right) - 1\right)\frac{\mu}{N} \bmod N$$

است.

خاصیت مهم این نوع رمزنگاری، معکوس پذیری آن است:

$$D\left(E(t;r)\right) = t, \forall\, r \in \mathbb{Z}_{\mathrm{N}}^*, \forall\, t \in \mathbb{Z}_{\mathrm{N}}.$$

خاصیت‌های دیگر این نوع رمزنگاری در ادامه آمده است.

لم ۲-۵- خاصیت‌های رمزنگاری پیلیر بدین صورت است:

۱. اگر $r,r' \in \mathbb{Z}_N^*$ و $t,t' \in \mathbb{Z}_N$ به طوری که $t+t' \in \mathbb{Z}_N$ باشد، آنگاه خواهیم داشت:

$$E(t;r)E(t';r')\ mod\ N^2 = E(t+t';rr')$$

۲. اگر $r \in \mathbb{Z}_N^*$ و $t,t' \in \mathbb{Z}_N$ به طوری که $tt' \in \mathbb{Z}_N$ باشد، آنگاه خواهیم داشت:

$$E(t;r)^{t'}\ mod\ N^2 = E(tt';r)$$

۳. اگر $r,r' \in \mathbb{Z}_N^*$ و $t,t' \in \mathbb{Z}_N$ به طوری که $t+t' \in \mathbb{Z}_N$ باشد، آنگاه خواهیم داشت:

$$\frac{E(t;r)}{E(t';r')} mod\ N^2 = E(t-t';r/r')$$

اثبات دو قسمت اول در مقاله [۱۰] آمده است. اثبات قسمت سوم از لم ۲-۵ بدین صورت است:

$$\frac{E(t;r)}{E(t';r')}\ mod\ N^2$$
$$= \frac{(N+1)^t (r)^N}{(N+1)^{t'}(r')^N}\ mod\ N^2$$
$$= (N+1)^{t-t'}\left(\frac{r}{r'}\right)^N\ mod\ N^2$$
$$= E\left(t-t';\frac{r}{r'}\right), \forall\, r,r' \in \mathbb{Z}_N^*, \forall\, t,t' \in \mathbb{Z}_N.$$

در بخش بعد، از موارد گفته شده در این بخش استفاده می‌شود که رویتگر با ورودی ناشناخته را رمزنگاری نمود.

۳- طراحی رویتگر امن رمز شده

در این بخش رویتگر امن پیشنهادی، طبق بلوک دیاگرام شکل (۱) بیان می‌شود. هم‌چنین از رمزنگاری نیمه همگن بیان شده در بخش قبل برای رمزنگاری رویتگر با ورودی ناشناخته استفاده می‌شود. همان طور که در شکل (۱) دیده می‌شود، رویتگر دارای دو ورودی رمز شده می‌باشد و خروجی نیز به صورت رمز شده است. چون رویتگر کلید رمزگشایی را ندارد، تمام محاسبات در رویتگر بر اعداد رمز شده است. بنابراین حتی اگر امنیت رویتگر به خطر افتد، درستی اطلاعات از بین نمی‌رود. این مسئله در این بخش توضیح داده خواهد شد.

دینامیک سیستم زمان گسسته، همراه با ویژگی نامتغیر با زمان بودن به صورت زیر در نظر گرفته می‌شود:

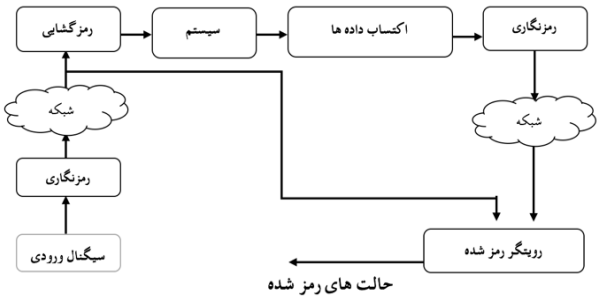
$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + Ed_k\ , x_0 = x(0) \\ y_k &= Cx_k, \end{aligned} \qquad (۱)$$

که در آن $x_k \in \mathbb{R}^{p_x}$ بیانگر حالت‌های سیستم، $y_k \in \mathbb{R}^{p_y}$ خروجی سیستم، $u_k \in \mathbb{R}^{p_u}$ ورودی سیستم، $d_k \in \mathbb{R}^{p_d}$ ورودی ناشناخته یا همان اغتشاش، $A \in \mathbb{R}^{p_x \times p_x}$، $B \in \mathbb{R}^{p_x \times p_u}$ و $E \in \mathbb{R}^{p_x \times p_d}$ و $C \in \mathbb{R}^{p_y \times p_x}$ است.

بنابراین رویتگر با ورودی ناشناخته استاندارد برای رویت حالت‌های سیستم (۱) به صورت زیر بیان می‌شود:

$$\begin{aligned} z_{k+1} &= Fz_k + TBu_k + Ky_k\ , z_0 = z(0) \\ \hat{x}_k &= z_k + Hy_k, \end{aligned} \qquad (۲)$$

که $\hat{x}_k \in \mathbb{R}^{p_x}$ حالت تخمین زده شده و $z_k \in \mathbb{R}^{p_x}$ حالت‌های رویتگر، $F \in \mathbb{R}^{p_x \times p_x}$ ، $T \in \mathbb{R}^{p_x \times p_x}$ ، $K \in \mathbb{R}^{p_x \times p_y}$ و $H \in \mathbb{R}^{p_x \times p_y}$ است.



شکل ۱: بلوک دیاگرام رویتگر رمز شده

فرضیه ۳-۱- فرض می‌کنیم سیستم (۱) پایدار و زوج (A,C) رویت پذیر است. بنابراین، $\lim_{k\to\infty}\|x_k - \hat{x}_k\| \to 0$.

فرضیه۳-۲- برای پیاده سازی رویتگر در کامپیوتر دیجیتال فرض شده‌است تمامی پارامترهای سیستم و سیگنال ورودی در مجموعه $\mathbb{Q}(n,m)$ باشد. هم چنین خروجی نیز بایستی در این مجموعه اعداد باشند.

تئوری ۳-۳- با فرض پایداری سیستم (۱) و $\bar{y}_k$ به عنوان خروجی کوانتیزه شده y_k، و در صورتی که

$\bar{y}_k \in [-M(x_0), M(x_0)]^{P_y}$,
$\bar{y}_k \in \mathbb{Q}(n_1, m_1)$

و نیز $n_1 \geq m_1 + 1 + \log_2(M(x_0))$، آنگاه ϵ ، به گونه‌ای وجود خواهد داشت که $\|y_k - \bar{y}_k\| < \epsilon$ باشد.

اثبات: فرض کنید $\|y_k - \bar{y}_k\| < \epsilon$ است، اگر m_1 طوری انتخاب شود که $\|y_k - \bar{y}_k\| < 2^{-m_1} < \epsilon$ باشد. بنابراین کافی است، n_1 در رابطه $2^{n_1 - m_1 - 1} > M(x_0)$ صدق کند.

چالش مسئله این است که با در نظر گرفتن خروجی کوانتیزه شده، تخمین حالت‌ها در این وضعیت در باند محدودی از حالت‌های سیستم باقی بمانند.

معادله‌های دینامیکی رویتگر با ورودی ناشناخته در این وضعیت چنین در نظر گرفته می‌شود

$$\begin{aligned} z_{k+1} &= Fz_k + TBu_k + K\bar{y}_k\ , x_0 = x(0) \\ \hat{x}_k &= z_k + H\bar{y}_k, \end{aligned} \qquad (۳)$$

اگر خطا $e_k = x_k - \hat{x}_k$ تعریف شود، خواهیم داشت:

$$\begin{aligned} e_{k+1} &= x_{k+1} - \hat{x}_{k+1} \\ &= Ax_k + Bu_k + Ed_k - Fz_k - TBu_k - P\bar{y}_k - H\bar{y}_{k+1} \end{aligned} \qquad (۴)$$

از طرفی می‌توان نوشت

$$\bar{y}_k = y_k - \Delta y_k\ , \Delta y_k < 2^{-m_1} \qquad (۵)$$

و اگر K را بدین صورت تجزیه کنیم:

$$K = K_1 + K_2 \qquad (۶)$$

با استفاده از معادله‌های (۵) و (۶) و بازنویسی معادله (۴) خواهیم داشت:

$$
\begin{aligned}
e_{k+1} = {} & (A - HCA - K_1C)e_k \\
& + [F - (A - HCA - K_1C)]z_k \\
& + [K_2 - (A - HCA - K_1C)H]y_k \\
& + [T - (I - HC)]Bu(t) \\
& + (HC - I)Ed(t) \\
& + P\,\Delta y_k + H\Delta y_{k+1}
\end{aligned} \qquad (۷)
$$

جهت تحقق شرایط مطلوب بر دینامیک خطا لازم است شرایط زیر را برآورده کنیم:

$$
\begin{aligned}
F &= (A - HCA - K_1C) \\
T &= (I - HC) \\
(HC - I)E &= 0 \\
K_2 &= FH
\end{aligned} \qquad (۸)
$$

در اینجا شرط لازم برای آنکه ماتریس H از رابطه $(HC - I)E = 0$ به دست آید، عبارت است از :

$$rank(CE) = rank(E)$$

با توجه به اینکه تعداد سطرهای مستقل خطی C، بیانگر تعداد خروجی و تعداد ستون‌های مستقل خطی E، تعداد اغتشاش را نشان می‌دهد و مرتبه حاصل ضرب این دو برابر با مینیمم تعداد خروجی و تعداد اغتشاش است. بنابراین اگر مرتبه حاصل ضرب برابر با مرتبه E باشد نشانگر این است که تعداد ورودی اغتشاش کمتر از تعداد خروجی است بنابراین می توان اثر اغتشاش را از خروجی حذف کرد. در واقع این عمل از نظر فیزیکی بیانگر این است تعداد اغتشاش نباید از تعداد خروجی بیشتر باشد.

بعد از یافتن ماتریس H، ماتریس K_1 به گونه‌ای به دست می‌آید که $A - HCA - K_1C < 0$ باشد. بنابراین ماتریس‌های F ، T و K_2 به دست می‌آیند.

در نهایت دینامیک خطا را بازنویسی می‌کنیم:

$$e_{k+1} = Fe_k + P\,\Delta y_k + H\Delta y_{k+1} \le Fe_k + 2^{-m_1}\alpha \qquad (۹)$$

به طوری که $W = P + H$ و $\alpha = \sum_{i,j}|W_{i,j}|$ است.

با توجه به کوانتیزه شدن خروجی، صفر شدن خطای بین تخمین حالت‌ها و حالت‌ها و یا پایداری خطای رویتگر امکان پذیر نیست. از این رو با استفاده از مرجع [۱۹] برای پایداری رویتگر از پایداری ورودی به حالت (ISS[۹]) با در نظر گرفتن 2^{-m_1} به عنوان ورودی خارجی استفاده شده است:

$$\|e_k\| \le \beta(\|e_0\|, k) + 2^{-m}\delta \qquad (۱۰)$$

برای کلاس $\mathcal{KL}$ تابع β و گین ثابت $\delta > 0$ می‌توان گفت که اگر $k \to \infty$ آنگاه $\beta(\|e_0\|, k) \to 0$ میل می‌کند، بنابراین خطای رویتگر با 2^{-m} کران دار است که این مقدار با انتخاب m به اندازه کافی بزرگ، به اندازه کافی کوچک می‌شود.

لم ۳-۴ [۲۰]- با در نظر گرفتن $\mathcal{X}, \mathcal{Y} \in \mathbb{R}^n$ و اگر $\mathcal{X}^\top$ ترانهاده $\mathcal{X}$ باشد، آنگاه به ازای هر $\varepsilon > 0$،

$$2|\mathcal{X}^\top\mathcal{Y}| \le \varepsilon\mathcal{X}^\top\mathcal{X} + \varepsilon^{-1}\mathcal{Y}^\top\mathcal{Y}$$

است. بنابراین، اثبات پایداری رویتگر در ادامه بیان می‌شود.

تئوری ۳-۵- سیستم (۱) به همراه رویتگر با دینامیک (۳) در نظر بگیرید. اگر ماتریس متقارن و مثبت معین S_1 و S_2 و P وجود داشته باشد به طوری که

$$\begin{bmatrix} -P & * \\ PA - PHCA - S_1C & -S_2 \end{bmatrix} < 0,$$
$$S_2 < P,$$

باشد، بنابراین K_1 و K_2 از رابطه

$$K_1 = P^{-1}S_1,$$
$$K_2 = (A - HCA - K_1C)H,$$

به گونه‌ای به دست می‌آیند که خطای تخمین $\lim_{k\to\infty}\|x_k - \hat{x}_k\|$ در باند محدود قرار گیرد.

اثبات: با در نظر گرفتن تابع لیاپانوف $V_k = e_k^\top Pe_k$ خواهیم داشت:

$$
\begin{aligned}
V_{k+1} - V_k \le {} & (Fe_k + 2^{-m_1}\alpha)^\top P(Fe_k + 2^{-m_1}\alpha) \\
& - e_k^\top Pe_k \\
= {} & e_k^\top(F^\top PF - P)e_k \\
& + 2^{-m_1+1}e_k^\top F^\top P\alpha + 2^{-2m_1}\alpha^2 P
\end{aligned} \qquad (۱۱)
$$

با استفاده از لم ۳-۴ خواهیم داشت:

$$2^{-m_1+1}e_k^\top F^\top P\alpha \le \varepsilon e_k^\top F^\top PFe_k + 2^{-2m_1}\alpha^2 P\varepsilon^{-1}$$

معادله (۱۱) را بازنویسی می‌کنیم:

$$
\begin{aligned}
V_{k+1} - V_k \le {} & e_k^\top(F^\top PF(1+\varepsilon) - P)e_k \\
& + 2^{-2m_1}\alpha^2 P(1+\varepsilon^{-1})
\end{aligned} \qquad (۱۲)
$$

با در نظر گرفتن $F^\top PF(1+\varepsilon) - P = -Q$ به طوری که ماتریس P و Q مثبت معین باشند و با استفاده از لم۳-۵ از مرجع [۱۹] اثبات انجام می‌شود. بنابراین باید متغیرهای مسئله را به گونه‌ای بیابیم که Q مثبت معین شود. برای این هدف، می‌بایست:

$$F^\top PF(1+\varepsilon) - P < 0 \qquad (۱۳)$$

با استفاده از قضیه مکمل شور[۱۰] معادله (۱۲) بازنویسی می‌شود:

$$\begin{bmatrix} -P & F^\top \\ F & -P^{-1}(1+\varepsilon)^{-1} \end{bmatrix} < 0 \qquad (۱۴)$$

از انتقال همانندی[۱۱] استفاده کرده:

$$
\begin{aligned}
\begin{bmatrix} I & 0 \\ 0 & P \end{bmatrix}\begin{bmatrix} -P & F^\top \\ F & -P^{-1}(1+\varepsilon)^{-1} \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & P \end{bmatrix} &= \begin{bmatrix} -P & * \\ PF & -P(1+\varepsilon)^{-1} \end{bmatrix} \\
&= \begin{bmatrix} -P & * \\ P(A - HCA - K_1C) & -P(1+\varepsilon)^{-1} \end{bmatrix} \\
&< 0
\end{aligned}
$$

اگر $PK_1 = S_1$ ، $(1+\varepsilon)^{-1} = 0.5$ در نظر گرفته شود:

$$\begin{bmatrix} -P & * \\ PA - PHCA - S_1C & -P \end{bmatrix} < 0$$
$$P = P^\top > 0 \qquad (۱۵)$$

معادله (۱۵) نامساوی ماتریسی خطی است و با حل آن‌ها K_1 و K_2 به دست می‌آیند.

در ادامه الگوریتم رویتگر با ورودی ناشناخته رمز شده، با توجه به مباحث ذکر شده در این بخش و بخش قبل، بیان می‌گردد.

الگوریتم ۱- الگوریتم رویتگر با ورودی ناشناخته رمز شده

ورودی

$A, B, C, F, S = TB, K, H, n_1, m_1$

خروجی

$\boldsymbol{Ex_k}$

 # داده‌های سنسور

$\boldsymbol{for\ \ i = 1, \dots, p_y}$

$\boldsymbol{\quad E\bar{y}_{k,i} = E(f_{n_1+2m_1,0}(2^{m_1}\bar{y}_{k,i}); r)}$

$\boldsymbol{end}$

$\bar{\mathbf{y}}_{k,i}$ بیانگر i امین المان از $\bar{\mathbf{y}}_k$ است.

$\boldsymbol{E\bar{y}_{k,i}}$ به رویتگر ارسال می‌شود.

 # سیگنال کنترلی

$\boldsymbol{for\ \ j = 1, \dots, p_u}$

$\boldsymbol{\quad Eu_{k,j} = E(f_{n_1+2m_1,0}(2^{m_1}u_{k,j}); r)}$

$\boldsymbol{end}$

ورودی رمز شده به رویتگر ارسال می‌شود.

 # رویتگر

ابتدا رمز مقادیر اولیه تخمین حالت‌ها محاسبه شود.

$\boldsymbol{for\ i = 1, \dots, p_x}$

$\boldsymbol{\quad Ez_{0,i} = E(z_{0,i}, r)}$

$\boldsymbol{end}$

سپس

$\boldsymbol{for\ k = 1, \dots}$

$\boldsymbol{\quad for\ i = 1, \dots, p_x}$

$\boldsymbol{\quad\quad Ez_{k,i} = 1}$

$\boldsymbol{\quad\quad for\ j = 1, \dots, p_x}$

$\boldsymbol{\quad\quad\quad fF_{i,j} = f_{n_1+2m_1,0}(2^{m_1}\mathrm{F_{i,j}})}$

$\boldsymbol{\quad\quad\quad l = (Ez_{k-1,j})^{fF_{i,j}} mod\ N^2}$

$\boldsymbol{\quad\quad\quad Ez_{k,i} = (Ez_{k,i} * l)\ mod\ N^2}$

$\boldsymbol{\quad\quad end}$

$\boldsymbol{\quad\quad for\ j = 1, \dots, p_u}$

$\boldsymbol{\quad\quad\quad fS_{i,j} = f_{n_1+2m_1,0}(2^{m_1}\mathrm{S_{i,j}})}$

$\boldsymbol{\quad\quad\quad l = (Eu_{k-1,j})^{fS_{i,j}} mod\ N^2}$

$\boldsymbol{\quad\quad\quad Ez_{k,i} = (Ez_{k,i} * l)\ mod\ N^2}$

$\boldsymbol{\quad\quad end}$

$\boldsymbol{\quad\quad for\ j = 1, \dots, p_y}$

$\boldsymbol{\quad\quad\quad fK_{i,j} = f_{n_1+2m_1,0}(2^{m_1}\mathrm{K_{i,j}})}$

$\boldsymbol{\quad\quad\quad l = (E\bar{y}_{k-1,j})^{fK_{i,j}} mod\ N^2}$

$\boldsymbol{\quad\quad\quad Ez_{k,i} = (Ez_{k,i} * l)\ mod\ N^2}$

$\boldsymbol{\quad\quad end}$

$\boldsymbol{\quad\quad Ex_{k,i} = Ez_{k,i}}$

$\boldsymbol{for\ j = 1, \dots, p_y}$

$\boldsymbol{\quad\quad fH_{i,j} = f_{n_1+2m_1,0}(2^{m_1}\mathrm{H_{i,j}})}$

$\boldsymbol{\quad\quad l = (E\bar{y}_{k-1,j})^{fH_{i,j}} mod\ N^2}$

$\boldsymbol{\quad\quad Ex_{k,i} = (Ex_{k,i} * l)\ mod\ N^2}$

$\boldsymbol{\quad end}$

$\boldsymbol{\quad end}$

$\boldsymbol{end}$

$\boldsymbol{Ex_{k,i}}$ به عنوان خروجی رویتگر ارسال می‌شود.

۴- شبیه سازی

پروسه کنترلی TE-PCS، یک شبیه سازی واقعی از یک پروسه شیمیایی است که به عنوان یک نمونه مطالعاتی در مقاله‌های کنترلی مورد بررسی قرار می‌گیرد. مدل این سیستم شیمیایی به همراه پروسه و حلقه‌های کنترلی PI آن توسط Ricker در [۲۱] و مدل خطی این پروسه در [۲۲] ارائه گردیده است:

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} h_{11} & 0 & 0 & h_{14} \\ h_{21} & 0 & h_{23} & 0 \\ 0 & h_{32} & 0 & 0 \\ 0 & 0 & 0 & h_{44} \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{bmatrix}$$

به طوری که:

$$h_{11} = \frac{1.7}{0.75s+1}, h_{21} = \frac{45(5.667s+1)}{2.5\,s^2+10.25\,s+1},$$
$$h_{23} = \frac{-15s-11.25}{2.5s^2+10.25s+1}, h_{32} = \frac{1.5}{10s+1}e^{-0.1s},$$
$$h_{14} = \frac{-3.4s}{0.1s^2+1.1s+1}, h_{44} = \frac{1}{s+1}$$

است. ماتریس طراحی رویتگر با حل نامساوی ماتریس خطی از تئوری ۳-۵ در برنامه نویسی متلب به دست آمده است:

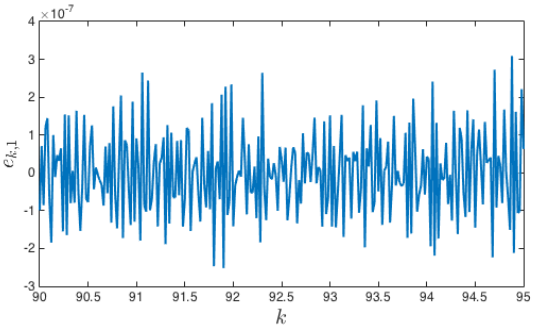
$$K = 10^3 * \begin{bmatrix} -2.4010 & -0.4784 & -1.7080 & -1.2225 \\ -0.6406 & -0.1277 & -0.4555 & -0.3261 \\ 2.4961 & 0.4952 & 1.7703 & 1.2964 \\ 0.0001 & 0.0222 & -0.0047 & -0.1704 \\ 0.0001 & 0.0000 & -0.0000 & -0.0000 \\ 0.0001 & 0.0000 & 0.0186 & -0.0263 \\ 0.0001 & -0.0002 & -0.4354 & -0.0011 \\ 0.0001 & -0.0002 & 0.0000 & 0.0018 \end{bmatrix}.$$

در ابتدا رویتگر با ورودی ناشناخته استاندارد که از خروجی کوانتیزه شده برای تخمین حالت‌ها استفاده می‌کند بررسی شده است. مشاهده می شود با انتخاب بزرگ مقادیر n_1, m_1 مقدار خطای بین تخمین حالت‌ها و حالت‌ها کوچک می‌شود. این خطا به عنوان نمونه برای اولین متغیر حالت در شکل ۲ نشان داده شده است. در واقع در این شبیه سازی، سیستم با خطای کوانتیزه شده و رویتگر استاندارد غیر رمز شده در نظر گرفته شده است.

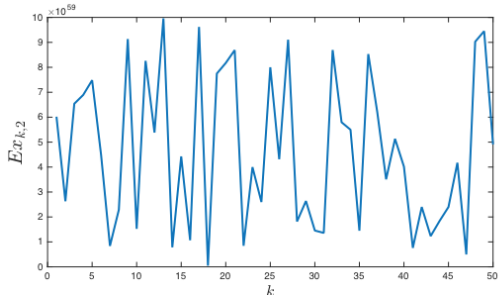
سپس، با استفاده از الگوریتم ۱، رویتگر با ورودی ناشناخته رمز شده طراحی شده است. با استفاده از این رویتگر، حالت‌های سیستم به صورت رمز شده، تخمین زده می‌شوند. سیستم انتخاب شده دارای هشت حالت است که در شکل ۳ دومین حالت تخمین زده شده که به صورت رمز است نشان داده شده است. سیگنال نشان داده شده در شکل ۳ را رمزگشایی کرده و سیگنال رمزگشایی شده که با $D(Ex_{k,2})$ مشخص شده‌است، در شکل ۴ دیده می‌شود. از شکل ۳ و ۴، متوجه می‌شویم که تخمین حالت از زمان حدود ده ثانیه به بعد تقریباً ثابت است در صورتی که سیگنال رمزگشایی شده در تمامی زمان‌ها تغییرات داشته است. علت این است که تغییرات تخمین حالت بعد از ثانیه دهم در حدود 10^{-5} است که این مقدار در شکل دیده نمی‌شود برای رمزنگاری عدد اعشاری را ابتدا به عدد صحیح برده و سپس رمز می‌کنیم. بنابراین اگر برای تبدیل اعشاری به صحیح در عدد بزرگتر از 10^6 ضرب کنیم مقدار

تغییرات دیده می‌شود. اما چون بعد از رمزگشایی دوباره عدد را به اعشار برمی‌گردانیم، عدد اصلی با عدد رمز شده و سپس رمزگشایی شده، برابر هستند.

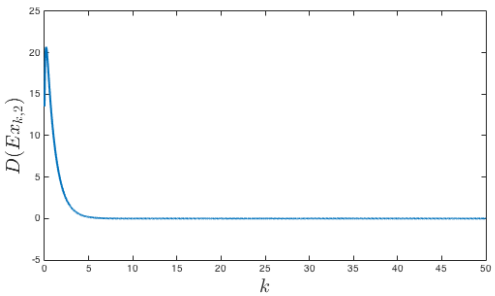
اختلاف سیگنال رمزگشایی این تخمین حالت رمز شده و خود حالت در شکل ۵ نشان داده شده است. در این شکل مشاهده می‌شود این اختلاف در باند محدودی نزدیک به صفر باقی مانده است و تخمین به خوبی انجام شده است. هم چنین برای نشان دادن این موضوع که رمزنگاری تخمین حالت را تغییر نمی‌دهد شبیه سازی دیگری انجام داده‌ایم. در این مورد تخمین حالت را یک بار از رویتگر با ورودی ناشناخته رمز شده طبق الگوریتم ۱ به دست آورده و سپس حالت‌ها را رمزگشایی کرده‌ایم و بار دیگر تخمین‌ها را با استفاده از رویتگر با ورودی ناشناخته استاندارد بدون رمز به دست آورده‌ایم. اختلاف تخمین دومین حالت از دو روش در شکل ۶ دیده می‌شود. این اختلاف در همه زمان‌ها برابر با صفر است و نشان می‌دهد رمزنگاری سیگنال را تغییر نمی‌دهد.



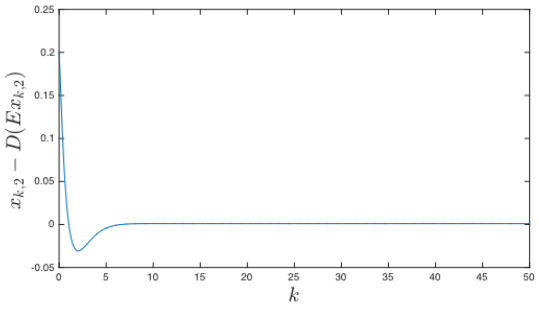
شکل ۲: خطای بین تخمین اولین حالت با رویتگر ورودی ناشناخته‌ای که با خروجی کوانتیزه شده کار می‌کند و حالت واقعی سیستم



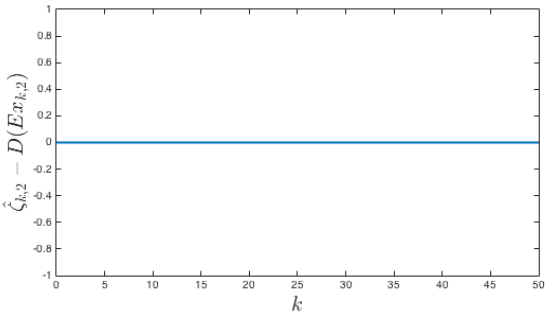
شکل ۳: تخمین دومین حالت رمز شده با استفاده از رویتگر با ورودی ناشناخته رمز شده



شکل۴: سیگنال رمزگشایی شده تخمین دومین حالت رمز شده با استفاده از رویتگر با ورودی ناشناخته رمز شده



شکل ۵: اختلاف سیگنال رمزگشایی شده تخمین دومین حالت رمز شده ($D(Ex_{k,2})$) با استفاده از رویتگر با ورودی ناشناخته رمز شده و دومین متغیر حالت ($x_{k,2}$)



شکل ۶: اختلاف سیگنال رمزگشایی شده تخمین دومین حالت رمز شده ($D(Ex_{k,2})$) با استفاده از رویتگر با ورودی ناشناخته رمز شده و تخمین دومین متغیر حالت با استفاده از رویتگر با ورودی ناشناخته استاندارد ($\hat{\xi}_{k,2}$)

۵- نتیجه گیری

در این مقاله، تکنیک جدیدی برای تخمین امن حالت‌های سیستم ارائه شد. این پیشنهاد جهت حفظ محرمانگی حالت‌های تخمین زده شده و هم چنین داده‌های که از طریق شبکه در سیستم کنترل مبتنی بر شبکه انتقال می‌یابند، بسیار مؤثر است. برای این هدف، از تکنیک رمزنگاری جهت رمز کردن رویتگر استفاده شد. هم چنین شرایطی برای محدود بودن خطای بین تخمین حالت‌ها و حالت‌های واقعی به دست آمد. در نهایت الگوریتم پیشنهادی بر روی TE-PCS شبیه سازی گردید و مؤثر بودن طراحی مربوطه نشان داده شد. در همین راستا، در مقالات بعدی می‌توان کنترلر مبتنی بر تخمین حالت طراحی کرد. همچنین می‌توان تاثیرات شبکه از جمله وجود تأخیر و اتلاف بسته را نیز به شرایط مسئله اضافه نمود.

مراجع

[1] Y. Mo and B. Sinopoli, “Secure control against replay attacks,” in Communication, Control, and Computing, 47th Annual Allerton Conference on. IEEE, pp. 911–918, 2009.

[۲] لادن صادقی خرمی و احمد افشار، «طراحی سیستم تشخیص و جداسازی حمله با استفاده از رویتگر با ورودی ناشناخته نامینیمم فاز برای سیستم کنترل مبتنی بر شبکه»، کنفرانس بین المللی مهندسی برق ایران، دوره ۲۴، صفحه ۲۰۱۹-۲۰۲۴، شیراز، ۱۳۹۶.

[3] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," IEEE Transactions on Control Systems Technology, vol. 22, no. 4, pp. 1396–1407, 2014.

[۴] مینا سلیم و محمد جواد خسروجردی، «طراحی تخمین گر عیب با استفاده از تکنیک H_∞ مبتنی بر داده»، مجله مهندسی برق دانشگاه تبریز، جلد ۴۶، شماره ۴، صفحه ۱۴۷-۱۵۸، ۱۳۹۵.

[۵] مرتضی خرم کشکولی و مریم دهقانی، «تشخیص، شناسایی و جداسازی عیب توربین گاز پالایشگاه دوم پارس جوبی با استفاده از روش‌های ترکیبی داده کاوی، kmeans، تحلیل مؤلفه‌های اصلی(PCA) و ماشین بردار پشتیبان (SVM)»، مجله مهندسی برق دانشگاه تبریز، جلد ۴۷، شماره ۲، صفحه ۵۰۱-۵۱۵، ۱۳۹۶.

[6] Khorrami, Ladan Sadeghi, and Ahmad Afshar. "Attack detection in active queue management within large-scale networks control system with information of network and physical system." Electrical Engineering (ICEE), 24th Iranian Conference on. IEEE, 2016.

[7] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure control systems: A quantitative risk management approach," IEEE Control Systems, vol. 35, no. 1, pp. 24–45, 2015.

[8] Amin, Saurabh, Alvaro A. Cárdenas, and S. Shankar Sastry. "Safe and secure networked control systems under denial-of-service attacks." International Workshop on Hybrid Systems: Computation and Control. Springer, Berlin, Heidelberg, 2009.

[9] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Achieving secure role-based access control on encrypted data in cloud storage." IEEE transactions on information forensics and security 8.12 , pp. 1947-1960, 2013.

[10] F. Farokhi, I. Shames, and N. Batterham, "Secure and private cloud-based control using semi-homomorphic encryption," IFAC-PapersOnLine, vol. 49, no. 22, pp. 163–168, 2016.

[11] J. Kim, C. Lee, H. Shim, J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Encrypting controller using fully homomorphic encryption for security of cyber-physical systems," IFAC-PapersOnLine, vol. 49, no. 22, pp. 175–180, 2016.

[12] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in Decision and Control (CDC), 2015 IEEE 54th Annual Conference on. IEEE, pp. 6836–6843, 2015.

[13] Darup, Moritz Schulze, et al. "Towards encrypted mpc for linear constrained systems." IEEE Control Systems Letters 2.2 , pp. 195-200, 2018.

[14] Alexandru, Andreea B., Manfred Morari, and George J. Pappas. "Cloud-based MPC with Encrypted Data." arXiv preprint arXiv:, pp. 1803.09891, 2018.

[15] A. Al-Anwar, Y. Shoukry, S. Chakraborty, P. Martin, P. Tabuada, and M. B. Srivastava, "Proloc: resilient localization with private observers using partial homomorphic encryption," in International Conference on Information Processing in Sensor Networks, pp. 41–52, 2017.

[16] M. Zamani, L. Sadeghikhorrami, A.A. Safavi, and F. Farokhi, "Private state estimation for cyber physical systems using semi homomorphic encryption," Proceedings of the 23nd International Symposium on Mathematical Theory of Networks and Systems, pp. 399–404, 2018.

[17] F. J. Gonzalez-Serrano, A. Amor-Martın, and J. Casamayon-Anton, "State estimation using an extended kalman filter with privacy- protected observed inputs," in IEEE International Workshop on In- formation Forensics and Security. IEEE, pp. 54–59, 2014.

[18] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 223– 238, 1999.

[19] Z.-P. Jiang and Y. Wang, "Input-to-state stability for discrete-time nonlinear systems," Automatica, vol. 37, no. 6, pp. 857 – 869, 2001.

[20] F. Zhang, Matrix theory: basic results and techniques. Springer Science & Business Media, 2011.

[21] L.Ricker, "Model predictive control of a continuous nonlinear two-phase reactor". Journal of Process Control, vol. 3, Nov, 1993.

[22] R.Chaboksawar, Y.Mo and B.Sinopoli, "Detecting integrity attacks on SCADA systems". Preprints of the 18th IFAC World Congress, Milano, Italy, 2011.

زیرنویس‌ها

[1] Eavesdropping attack
[2] sniffing attack
[3] Fully homomorphic encryption
[4] Semi homomorphic encryption
[5] Paillier
[6] Isomorph
[7] Greatest common divisor
[8] Least common multiple
[9] Input to state stability
[10] Schur complement
[11] Congruence transformation