مجموعه مقالات پانزدهمین کنفرانس بین‌المللی انجمن رمز ایران
دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی، تهران، ۶-۷ شهریور ۱۳۹۷
(مقاله مدعو)

ارزیابی امنیت سیستم‌های سایبر-فیزیکی

حامد اروجلو

دکتری مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران،
orojloo@iust.ac.ir

چکیده

سیستم‌های سایبر-فیزیکی فناوری‌های ارتباطی و رایانشی با فرآیندهای فیزیکی هستند. در واقع در این سیستم‌ها، سیستم‌های فیزیکی توسط بخش سایبری نظارت و کنترل می‌شود. ترکیب سیستم‌های فیزیکی با دنیای سایبری اگرچه موجب افزایش کارآمدی و قابلیت اطمینان آن‌ها شده است، اما به هر حال آن‌ها را با مسائل امنیتی جدی روبرو کرده است. مهاجمان می‌توانند از آسیب‌پذیری-های سایبری سوء استفاده نموده و به سیستم‌های فیزیکی آسیب بزنند. در این مقاله به بررسی ویژگی‌های متفاوت امنیت سیستم‌های سایبری با سیستم‌های سایبر-فیزیکی پرداخته شده است. همچنین روشی برای ارزیابی پیامد حملات به سیستم‌ها ارائه شده است. اینکه با انجام هر یک از حملات، چه بخش‌ها و پارامترهایی از سیستم تحت تأثیر قرار خواهند گرفت و میزان این تأثیر به چه میزان خواهد بود، اهمیت بالایی دارد. با استفاده از روش ارائه شده می‌توان اثری که حمله به هر پارامتر بر سایر پارامترها دارد و اثر سایر پارامترها بر پارامتر کنترلی مورد نظر را ارزیابی نمود. به طور خلاصه، نتیجه این روش این است که می‌توان مؤلفه‌های کنترلی از نظر میزان تأثیرگذاری بر سایر مؤلفه‌ها بر اثر حمله و میزان حساسیت آن‌ها در برابر حملات (میزان تأثیرپذیری) رتبه‌بندی نمود.

کلمات کلیدی

سیستم‌های سایبر-فیزیکی، امنیت، ارزیابی کمّی.

۱- مقدمه

با ترکیب فناوری‌های ارتباطی و رایانشی با فرآیندهای فیزیکی، سیستم‌های سایبر-فیزیکی (CPS) ایجاد شده‌اند [1]. سیستم‌های سایبر-فیزیکی، سیستم‌هایی مبتنی بر کامپیوتر هستند که فرآیندهای فیزیکی را کنترل و نظارت می‌کنند [2]. این اجماع به منظور رسیدن به کارآمدی، قابلیت اطمینان و استحکام بیشتر سیستم‌های فیزیکی به کار رفته در کاربردهای مختلف است. به دلیل کاربرد این سیستم‌ها در زیرساخت‌های حیاتی مانند شبکه برق، شبکه توزیع گاز و آب، صنایع، خودروهای پیشرفته و پزشکی، امنیت این سیستم‌ها بسیار اهمیت پیدا می‌کند.

ارتباط تنگاتنگ فرآیندهای فیزیکی با فناوری‌های ارتباطات و اطلاعات در این سیستم‌ها، نگرانی‌های امنیتی جدیدی را مطرح می‌کند که با روش‌های موجود قابل برطرف کردن نیستند. با فرض اینکه روش‌های جدیدی نیز با توجه به ساختار و شرایط خاص این‌گونه سیستم‌ها برای حفظ امنیت آن‌ها ایجاد شوند، نمی‌توان انتظار داشت که فنون امنیتی ارائه شده برای حفظ تمام و کمال امنیت یک سیستم سایبر-فیزیکی کافی باشند؛ چون رفتار و تفکر مهاجمان این سیستم‌ها عاملی پویاست که با وجود تمام پیش‌بینی‌ها و در نظر گرفتن تمام احتمالات ممکن، امکان بروز نمونه جدید و دیده نشده‌ای از آن وجود دارد.

مدل‌سازی و ارزیابی امنیت، یکی از روش‌های مطالعه امنیت سیستم هاست. تاکنون روش‌های متعددی در این زمینه ارائه شده‌اند. به طور کلی می‌توان روش‌های ارائه شده برای تحلیل و مدل‌سازی امنیت سیستم‌های سایبر-فیزیکی را به سه دسته کلّی تقسیم کرد:

- روش‌های مبتنی بر امنیت اطلاعات، که بر رمزگذاری و امنیت داده‌ها تمرکز دارد [3] و [4].
- روش‌های مبتنی بر نظریه کنترل امن، که مورد حمله قرار گرفتن پویایی فیزیکی سیستم‌های کنترلی با حملات سایبری را مورد مطالعه قرار می-دهند [5]، [6]، [7] و [8].

- روش‌های سطح بالا، که به مدل‌سازی حملات و اقدامات متقابل در برابر آن‌ها می‌پردازند [9]، [10]، [11] و [12].

در این مقاله ابتدا به بررسی و تعریف سیستم‌های سایبر–فیزیکی می‌پردازیم. سپس امنیت این سیستم‌ها را با سیستم‌های سایبری مقایسه می‌کنیم و انواع حملاتی که در برابر این سیستم‌ها قابل انجام است و پیامد حملات به این سیستم‌ها را مورد بررسی قرار می‌دهیم. در نهایت هم روشی را برای ارزیابی اثر حملات بر امنیت سیستم‌های سایبر–فیزیکی ارائه می‌کنیم.

ادامه این مقاله به این شکل تدوین شده است. در بخش ۲ به تعریف سیستم‌های سایبر–فیزیکی، معماری، انواع و مثالی از این سیستم‌ها پرداخته شده است. در بخش ۳ امنیت این سیستم‌ها، انواع حملات و پیامد آن‌ها به این سیستم‌ها مورد بررسی قرار گرفته است. در بخش ۴ روشی برای ارزیابی اثر حملات بر آن‌ها ارائه شده است و در بخش ۵ مطالعه موردی برای روش پیشنهاد شده ارائه شده است. نهایتا در بخش ۶ نتایج مقاله ارائه شده است.

۲- سیستم‌های سایبر–فیزیکی

در این بخش به تعریف سیستم‌های سایبر–فیزیکی، بررسی معماری، انواع، و ارائه مثالی از این سیستم‌ها می‌پردازیم.

۲-۱- تعریف سیستم‌های سایبر–فیزیکی

سیستم‌های سایبر–فیزیکی ترکیب و یکپارچه‌سازی سیستم‌های رایانشی و ارتباطی (به عنوان بخش سایبری) با فرآیندهای فیزیکی هستند [2]. در این سیستم‌ها، فرآیندهای فیزیکی توسط بخش سایبری نظارت و کنترل می‌شوند. سیستم‌های سایبر–فیزیکی در متون مختلف به عنوان سیستم‌های کنترل شبکه‌ای و یا سیستم‌های کنترل صنعتی هم شناخته می‌شوند. این سیستم‌ها در زیرساخت‌های حیاتی مانند شبکه برق هوشمند، خطوط توزیع آب، گاز و سوخت، اتومبیل‌های پیشرفته، صنایع شیمیایی، صنایع هوایی، حمل و نقل، سلامت و پزشکی قابل مشاهده هستند.

انتزاعی از یک سیستم سایبر–فیزیکی در شکل (۱) به تصویر کشیده شده است. در این سیستم‌ها مجموعه‌ای از حسگرها پدیده‌های فیزیکی مانند سرعت، دما، رطوبت و فشار را اندازه‌گیری می‌کنند. سپس، مشاهدات به کنترل‌کننده‌ها (که معمولاً کنترل‌کننده‌های با منطق قابل برنامه‌ریزی (PLC) هستند) ارسال می‌شود. این کار معمولاً با نوشتن اطلاعات دریافت شده در بافرهای ورودی کنترل‌کننده‌ها انجام می‌شود [2]. کنترل‌کننده‌ها از آخرین مقدار ذخیره شده در بافرهای ورودی استفاده می‌کند و تصمیم کنترلی مناسب را بر آن اساس می‌گیرند.

حالت فعلی یک سیستم سایبر–فیزیکی با استفاده از متغیرهای فرآیند یا متغیرهای حالت قابل توصیف است [13]. دو نوع از متغیرهای حالت مهم در این سیستم‌ها، متغیرهای اندازه‌گیری شده و متغیرهای کنترلی هستند که به ترتیب نشان‌دهنده اندازه‌گیری حسگرها و سیگنال‌های کنترلی کنترل‌کننده‌ها هستند. برای مثال وضعیت دما، فشار و سرعت نمونه‌هایی از این متغیرهای حالت هستند. به مقادیر این متغیرهای حالت، تصویر منبع فیزیکی در لحظه گفته می‌شود. حسگرها این تصویرها را، به طور دوره‌ای یا بر اساس رخ دادن یک رویداد، به کنترل‌کننده‌ها ارسال می‌کنند [13]. مقدار عادی یک متغیر کنترلی نقطه تعیین شده نام دارد. کنترل‌کننده‌ها با دریافت داده‌های حسگرها، تفاوت بین مقدار دریافت شده و مقدار تعیین شده را برای متغیر حالت مورد نظر محاسبه می‌کنند و سعی می‌کنند این مقدار را به نقطه تعیین شده نزدیک نگه دارند. به همین منظور، پس از محاسبه این اختلاف، با توجه به کدی که طبق آن برای انجام یک وظیفه مشخص برنامه‌ریزی شده‌اند تصمیم‌گیری کرده و فرمانی را به محرّک‌ها ارسال می‌دارند. در نهایت، محرّک‌ها دستورات دریافت شده را به دستگاه‌های فیزیکی اعمال می‌کنند. این حلقه کنترلی به طور بی‌درنگ انجام می‌شود و تأخیر ناخواسته‌ای و عمدی نباید در آن ایجاد گردد [13] و [14].

در هر لحظه وضعیت سیستم به کنسول اپراتور در ایستگاه واسط انسان–ماشین (HMI) ارسال می‌شود تا اپراتور سیستم در جریان وضعیت سیستم باشد [15]. اپراتور می‌تواند با توجه به شرایط در کنترل خودکار دخالت کرده و وضعیت یا کد کنترل‌کننده را تغییر دهد.

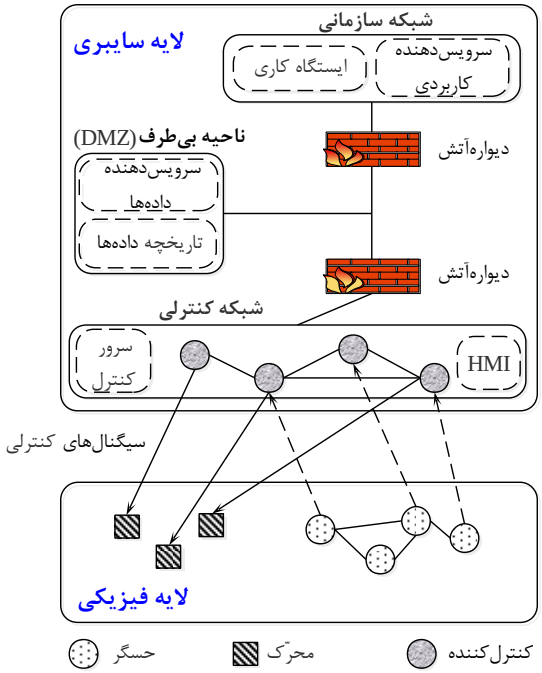
فرض کنید $y_i(t)$ مقدار اندازه‌گیری شده توسط حسگر i در زمان t باشد، $u_i(t)$ خروجی کنترل‌کننده i در زمان t و $x_i(t)$ مقدار حالت i در زمان t باشد. همچنین $A = (a_{ij})_{n*n}$ وابستگی فیزیکی حالت i به حالت j را نشان دهد، $B = (b_{ij})_{n*m}$ = ماتریس ورودی برای حالت i از ورودی کنترل j و $C = (c_{ij})_{p*n}$ ماتریس خروجی باشد. بر اساس نمادهای تعریف شده، رفتار پویای سیستم به صورت زیر تعریف می‌شود:

$$x(t+1) = Ax(t) + Bu(t),$$
$$y(t) = Cx(t) \qquad (۱)$$

۲-۲- معماری سیستم‌های سایبر–فیزیکی

معماری سیستم‌های سایبر–فیزیکی از دو لایه تشکیل می‌شود [16]:

- لایه سایبری که شامل شبکه کنترلی، شبکه سازمانی و ناحیه بی‌طرف (DMZ) است.
- لایه فیزیکی که شامل حسگرها، محرک‌ها و دستگاه‌های فیزیکی هستند.



شکل (۱) : انتزاعی از یک سیستم سایبر–فیزیکی

معماری اغلب سیستم‌های سایبر–فیزیکی به صورت شکل (۱) است. هنگام ارائه معماری این سیستم‌ها، معمولاً توصیه می‌شود شبکه کنترلی از شبکه سازمانی جدا گردد [17]. ماهیت ترافیک شبکه در این دو لایه متفاوت است. در شبکه سازمانی دسترسی به اینترنت، FTP، ایمیل و ورود راه دور معمولاً مجاز است اما این دسترسی‌ها در شبکه کنترلی مجاز نیست. با داشتن این دو لایه مجزا، مشکلات امنیتی و کارایی در شبکه سازمانی بر شبکه کنترلی تأثیر محدودتری خواهد داشت.

به هر حال، نیاز است بین این دو شبکه ارتباط برقرار گردد. سرویس-دهنده‌هایی در ناحیه بی‌طرف قرار می‌گیرند که لازم است از شبکه سازمانی مورد دسترسی قرار گیرند. ناحیه بی‌طرف قسمت مجزا از شبکه است که مستقیماً به دیواره‌آتش متصل می‌شود [17] و [18]. ارتباطات در این شبکه مابین شبکه سازمانی و ناحیه بی‌طرف و شبکه کنترلی و ناحیه بی‌طرف با ایجاد یک شبکه خصوصی مجازی (VPN) بین هر دو شبکه برقرار می‌شود.

شبکه کنترلی مستقیماً به اینترنت متصل نمی‌شود و همه ارتباطات بین شبکه‌ها باید از ناحیه بی‌طرف بگذرد. کاربران برای اتصال به شبکه سازمانی باید از سازوکارهای احراز هویت قوی مانند احراز هویت چندعاملی مبتنی بر نشانه و شبکه خصوصی مجازی عبور کنند. وقتی کاربر احراز هویت شد برای اتصال به شبکه کنترلی هم باید برای بار دوم در دیواره‌آتش شبکه کنترلی، با استفاده از سازوکار قوی احراز هویت شود.

در شبکه کنترلی حسگرها، محرّک‌ها، واسط انسان–ماشین و کنترل-کننده‌ها قرار می‌گیرند و در شبکه سازمانی ایستگاه‌های کاری، چاپگرها و سرویس‌دهنده‌های کاربردی و مانند آن قرار می‌گیرند.

لایه سایبری معمولاً از پروتکل‌های DNP3 [19]، 61850 [20] و Modbus [21] برای ارتباط با دستگاه‌های لایه فیزیکی استفاده می‌کنند. مرسوم‌ترین راه محافظت از این پروتکل‌ها، استفاده از شبکه خصوصی مجازی است. همه جریان داده‌ها، بین شبکه‌های سازمانی و شبکه کنترلی تنها از طریق تونل شبکه خصوصی مجازی مجاز خواهد بود.

ارتباطات مابین حسگرها و کنترل‌کننده‌ها در سیستم‌های سایبر–فیزیکی معمولاً به سه دسته تقسیم می‌شوند [22]: (۱) ارتباطات حسگر به حسگر، برای جمع‌آوری داده‌های دریافت شده، (۲) ارتباطات حسگر به کنترل‌کننده برای ایجاد تصمیمات کنترلی مناسب و (۳) کنترل‌کننده به کنترل‌کننده برای اخذ تصمیم کنترلی مناسب.

۲-۳- انواع سیستم‌های سایبر–فیزیکی

سیستم‌های سایبر–فیزیکی با توجه به ماهیتشان به طور کلّی به دو دسته خراب– ایمن و خراب – عملیاتی تقسیم‌بندی می‌شوند [13]. در دسته اول، سیستم با رخ دادن یک خرابی می‌تواند حالت ایمن را شناسایی کند و به آن وارد شود. در اغلب موارد این سیستم‌ها به حالت تعلیق در خواهند آمد تا مشکل برطرف شود. کارخانه‌های شیمیایی و سیستم سیگنال‌دهی خط آهن قطار مثال‌هایی از این دسته هستند. در دسته دوم، کارکرد پیوسته سیستم با ارائه حداقل سطح سرویس، ضروری است. یعنی سیستم باید تا حد ممکن برای جلوگیری از یک حادثه عملیاتی باقی بماند. سیستم‌های کنترل پرواز هواپیما در این دسته قرار می‌گیرند.

۲-۴- مثالی از یک سیستم سایبر–فیزیکی

تقریباً همه مؤلفه‌های مکانیکی در یک ماشین پیشرفته با واحدهای الکترونیکی (ECU) کنترل می‌شوند [16]. ECUها کامپیوترهای کوچکی هستند که همه کارکرد بخش‌های مکانیکی ماشین را کنترل می‌کنند. خودروهای پیشرفته بیشتر از ۵۰ واحد کنترل الکترونیکی ECU دارند که از طریق شبکه به هم متصل شده‌اند.

ایمنی این وسیله نقلیه به ارتباط بی‌درنگ بین ECUهای مختلف وابسته است. برای مثال انتقال، سیستم قفل، ترمز، مدیریت موتور. این ECUها با استفاده از شبکه‌ای به نام گذرگاه CAN به هم متصل شده‌اند و از طریق این شبکه با هم ارتباط برقرار می‌کنند. این بسته‌ها به همه مؤلفه‌های متصل به گذرگاه همه‌پخشی می‌شوند. و هر مؤلفه تصمیم می‌گیرد آیا آن بسته به آن تعلق دارد یا خیر. برای مثال ECU انتقال هنگام تغییر دنده در گیربکس به ECU موتور سیگنال می‌دهد که توان موتور باید برای لحظه‌ای کاهش یابد تا تغییر لازم در گیربکس نرم‌تر انجام شود.

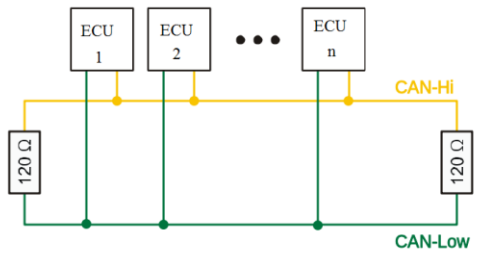
یک گذرگاه CAN از دو خط تشکیل شده است: خط بالای گذرگاه و خط پایین گذرگاه. سیگنال‌های دو خط دنباله یکسانی از داده‌ها را دارند اما دامنه آن‌ها متضاد است. اگر یک پالس در خط بالا از ۲٫۵ ولت به ۳٫۷۵ ولت برود، پالس متناظر آن در خط پایین از ۲٫۵ به ۱٫۲۵ می‌رود. با ارسال داده‌ها به این شکل ایمنی در برابر نویز بیشتر خواهد بود و احتمال تخریب داده‌ها کم خواهد شد. شکل (۲) تصویری از یک شبکه CAN را نشان می‌دهد.

همه ECUها دستگاه‌های توکاری هستند که از طریق شبکه گذرگاه CAN به هم شبکه شده‌اند. هر کدام تعدادی حسگر و محرک دارند که به آن‌ها متصل شده‌اند. بعضی از ECUها به طور دوره‌ای داده‌ها (مانند نتایج حسگر) را پخش می‌کنند، در حالی‌که اقدام ECUهای دیگر ممکن است به ECUهای همسایه وابسته باشد.

بسته‌های CAN حاوی شناسه و داده‌ها هستند. در قسمت داده‌ها، جمع کنترلی وجود دارد. شناسه به عنوان فیلد اولویت استفاده می‌شود. هر چه مقدار کوچکتر باشد اولویت بالاتری دارد. همچنین شناسه‌ها به ECUها کمک می‌کنند تا تشخیص دهند که باید آن را پردازش کنند یا خیر.

برای دو دهه اخیر، معمول‌ترین راه برای دسترسی خارجی به این شبکه اشکال‌یاب روی برد بوده است که از صندلی راننده قابل دسترس است. یعنی برای دسترسی به آن دسترسی فیزیکی به ماشین لازم است.

تولیدات جدید خودروهای پیشرفته امکان دسترسی راه دور به شبکه داخلی خودرو را از طریق اتصالات تلفن همراه فراهم می‌کند. این امکان برای به‌روز کردن نرم‌افزار و سرویس‌های ماشین استفاده می‌شود. همچنین سرویس‌هایی مانند Ecall را فراهم می‌کند. که با استفاده از آن خودرو به طور خودکار هنگام یک اتفاق جدی سرویس‌های نجات را فراخوانی می‌کند.



شکل (۲) : شمایی از یک شبکه CAN [16]

۳- امنیت سیستم‌های سایبر-فیزیکی

در این بخش، موضوعات امنیتی مطرح در مورد سیستم‌های سایبر-فیزیکی را مورد بررسی قرار می‌دهیم.

- **نیاز به تمرکز در سطح کنترل:** برای شکست واقعی سیستم یا بروز آسیب‌های فیزیکی، مهاجمین ناگزیرند که بر روی کنترل سیستم متمرکز شوند [14]. بدون انجام این کار پیامد حملات بسیار ناچیز خواهد بود.
- **نیاز آگاهی مهاجم از اثر حملات:** اگر حمله‌ای بدون اطلاع از اثرات آن بر روی فرآیند فیزیکی انجام شود، با احتمال بالا تنها مزاحمت کوچکی را برای سیستم به بار می‌آورد به جای اینکه موجب شکست واقعی سیستم شود [14] و [24].
- **دانش جنبشی مهاجم:** اجرای بسیاری از حملات در برابر سیستم‌های سایبر-فیزیکی نیازمند سطح مناسبی از دانش در مورد شرایط خرابی تجهیزات سیستم، اصول کنترل، رفتار فرآیند، پردازش سیگنال و مانند آن است [14]. دانشی که برای حمله و نفوذ به سیستم‌های سایبری مورد نیاز نخواهد بود.
- **اهمیت ویژگی‌های محیط فیزیکی:** پارامترهای محیط فیزیکی مانند سرعت شیرها و زمان‌بندی کنترل‌کننده‌ها بر روی کشف حمله و موفقیت مهاجم اثر می‌گذارد [25].
- **کشف حملات:** فرآیند کشف حملات امنیتی در سیستم‌های سایبر-فیزیکی به دو دسته کلی تقسیم می‌شود. بخش اول کشف حملات در فرآیند نفوذ است یعنی هنگامی که مهاجم سعی می‌کند به سطح دسترسی مورد نظر برای انجام اقداماتش (ایجاد خرابی فیزیکی) دست پیدا کند. این بخش می‌تواند هم ماهیت فیزیکی و هم سایبری داشته باشد. بخش دوم هم کشف حملات از روی رفتار فیزیکی بی‌نظم و نادرست سیستم است [26]. بسیاری از حملات پیچیده سعی می‌کنند این رفتار را از اپراتورهای سیستم مخفی نمایند تا پیامد حملات شدیدتر باشد [27].
- **رمزگذاری و احراز هویت پیام:** در حالی‌که رمزگذاری ترافیک کنترلی اغلب به دلیل انجام فعالیت‌های اشکال‌زدایی و محافظت از عملیات کنترل بی‌درنگ قابل انجام نیست، استفاده از مکانسیم‌های احرازهویت و جامعیت برای جلوگیری از حملات جاسوسی، تغییر داده‌ها و تکرار، ضروری است. اگرچه کدهای احرازهویت پیام به مهاجم اجازه دستکاری جریان داده‌ها (برای مثال از طریق تزریق بسته یا تغییر داده) را نمی‌دهند، به هر حال، مهاجم می‌تواند با بهره‌گیری از اصول کنترلی مشخص، به نتایجی شبیه به آنچه می‌توانست با دستکاری جریان داده‌ها دست پیدا کند، برسد [14] و [28].
- **شناخت شرایط خرابی سیستم:** در سیستم‌های سایبر-فیزیکی نفوذ به سیستم به معنای شکست سیستم نیست [14]. مهاجم بدون اطلاعات کافی در مورد کارکرد سیستم در سطح کنترل و شرایط خرابی‌اش نمی‌تواند اثرات زیان‌باری به بار آورد. بعضی از حملات تنها زمانی برای مهاجم نتیجه بخش خواهند بود که وقتی سیستم در یک حالت خاص قرار دارد به سیستم اعمال شوند.
- **هدف اقدامات بهبود امنیت در سیستم‌های سایبر-فیزیکی:** حملات به سیستم‌های سایبر-فیزیکی معنای مشابهی با حملات به سیستم‌های سایبری دارند. امّا موضوع قابل توجه این است که اهداف و پیامد حملات در سیستم‌های سایبر-فیزیکی، با سیستم‌های سایبری متفاوت است. اهداف فعالیت‌هایی که به منظور ارتقای امنیت در حوزه سایبری انجام می‌شوند با سیستم‌های سایبر-فیزیکی متفاوت است. در حوزه سایبری تمرکز اصلی از یک طرف بر روی در دسترس بودن سرویس‌ها، و از طرف دیگر محافظت از اطلاعات منتقل شده و ذخیره شده است. اما هدف اصلی اقدامات بهبود امنیت در سیستم‌های سایبر-فیزیکی محافظت از کارکردهاست [15].
- **بی‌درنگی کنترل:** داده‌های ارسال شده توسط حسگرها، بر مبنای یک تأخیر کنترلی مشخص توسط کنترل‌کننده مورد استفاده قرار می‌گیرد و به محرّک‌ها اعمال می‌شود. این زمان در کارکرد صحیح سیستم‌های سایبر-فیزیکی تأثیر بسزایی دارد و تأخیر ناخواسته یا عمدی نباید در آن ایجاد شود. داده‌های ارسال شده توسط حسگرها تنها برای مدت زمانی قابل استفاده هستند بنابراین تازگی آنها اهمیت دارد [13]. همچنین چون تصمیم کنترلی بر اساس آن داده‌ها گرفته می‌شود، صحت آن‌ها هم بسیار مهم است.

۳-۱- انواع حمله‌ها به سیستم‌های سایبر-فیزیکی

در این بخش به بررسی انواع حملات به سیستم‌های سایبر-فیزیکی می‌پردازیم.

سیستم‌های سایبر-فیزیکی تحت حمله به صورت زیر مدل می‌شوند [29]:

$$\begin{aligned} E\dot{x} &= Ax + Bu, \\ y &= Cx + Du \end{aligned} \qquad (۲)$$

به طوری‌که $x : \Re -> \Re^n$ و $y : \Re -> \Re^p$ نگاشت‌هایی هستند که سیر تکامل حالت‌های سیستم و اندازه‌گیری‌های آن را نشان می‌دهند و $A, E \in \Re^{n\times n}$ ، $B \in \Re^{n\times m}$ و $C \in \Re^{p\times n}$ ماتریس‌های ثابت $D \in \Re^{p\times m}$ هستند. در این رابطه ماتریس E می‌تواند تکین باشد و حالت غیرتکین این ماتریس (E = I)، حالت خاصی از آن است. ورودی‌های Bu و Du سیگنال‌های ناشناخته‌ای هستند که به ترتیب اختلال‌های ایجاد شده بر حالت یا سیگنال‌های محرّک‌ها و اندازه‌گیری سیستم را نشان می‌دهند.

ماتریس‌های ورودی به شکل $B[I\ 0]$ و $D[0\ I]$ هستند و به صورت ماتریس‌های یکه و صفر در ابعاد مناسب تقسیم‌بندی می‌شوند. همچنین برای u هم خواهیم داشت: $u = \begin{bmatrix} u_x \\ u_y \end{bmatrix}$.

این اختلال‌ها تأثیر حملات بر سیستم‌های سایبر-فیزیکی را نشان می‌دهند. بنابراین حمله به طور کلی به صورت $(Bu, Du) = (u_x, u_y)$ تعریف می‌شود که به حمله حالت $(Bu, 0)$ که بر پویایی سیستم تأثیر می‌گذارد و یا به عنوان حمله $(0, Du)$ که تنها اندازه‌گیری‌ها را هدف قرار می‌دهد دسته‌بندی می‌شود. سیگنال حمله $u : \Re \rightarrow \Re^{n+p}$ به راهبرد حمله بستگی دارد. با فرض اینکه $k \in \{1,..., n+p\}$ متغیر حمله وجود داشته باشد، حملات به صورت $k \subseteq \{1,..., n+p\}$ قابل تعریف هستند. بنابراین بردار حمله به صورت (B_k, D_k) تعریف می‌شود به طوری‌که B_k و D_k

زیرماتریس‌هایی از ماتریس‌های B و D با k ستون هستند. بنابراین $B_u = B_k u_k$ و $D_u = D_k u_k$، به طوری‌که u_k زیربرداری از u است.

با فرض اینکه $d_i^a(t)$ بیانگر حمله مهاجم به اندازه‌گیری انجام شده توسط حسگر i در زمان t و $b_i^a(t)$ نشان‌دهنده حمله مهاجم به سیگنال کنترلی i در زمان t و درنهایت $a_i(t)$ نشان‌دهنده اختلال اعمال شده توسط مهاجم در سیگنال حسگر یا کنترل‌کننده i باشد، حملات زیر به سیستم‌های سایبر–فیزیکی قابل انجام است:

- **حمله جامعیت**

حملات جامعیت را به چهار دسته تقسیم می‌کنیم. اولین دسته حملات مقیاس هستند که به طور صوری به صورت زیر تعریف می‌شود:

$$d_i^a(t) = a_i(t).y_i(t) \quad (۳)$$

حملات جامعیت افزایشی به صورت زیر قابل تعریف هستند:

$$d_i^a(t) = a_i(t) + y_i(t) \quad (۴)$$

معمولاً مقدار سیگنال‌های کنترل‌کننده و حسگر، بازه ممکن مشخصی دارند و اگر مقدار سیگنال در بازه مورد نظر نباشد به راحتی قابل کشف است. در حقیقت برای حسگر i خواهیم داشت:

$$y_i(t) \in [y_i^{\min}, y_i^{\max}] \quad (۵)$$

همچنین برای کنترل‌کننده i خواهیم داشت:

$$u_i(t) \in [u_i^{\min}, u_i^{\max}] \quad (۶)$$

در صورتی که مقدار سیگنال تولید شده توسط حسگر i در بازه مورد نظر نباشد به صورت زیر در نظر گرفته می‌شود:

$$d_i^a(t) = y_i^{\min}, if . d_i^a(t) < y_i^{\min} \quad (۷)$$

همچنین

$$d_i^a(t) = y_i^{\max}, if . d_i^a(t) < y_i^{\max} \quad (۸)$$

تعاریف مشابهی برای سیگنال کنترل‌کننده قابل ارائه است.

در ادامه دو نمونه از حمله‌های جامعیت که به سیستم‌های سایبر–فیزیکی قابل اعمال است را تعریف می‌کنیم.

- **حمله نهان**

در حمله نهان [5] مهاجم با دستکاری فیزیکی و یا با دسترسی به کانال ارتباط، داده‌های حسگر را تغییر می‌دهد. نکته این است که این حمله تنها رابطه اندازه‌گیری‌های حسگر را هدف قرار می‌دهد. در نتیجه بردار حمله به صورت $(0,\ Du)$ و پویایی سیستم بر اثر این حمله به صورت زیر تعریف می‌شود:

$$\begin{aligned} E\dot{x} &= Ax, \\ y &= Cx + Du \end{aligned} \quad (۹)$$

- **حمله تکرار**

در حمله تکرار [6] مهاجم سه عمل اصلی را انجام می‌دهد: ابتدا خروجی سیستم متناظر با یک وضعیت کارکرد ذخیره می‌شود. سپس داده‌های حسگر تغییر داده می‌شود تا اندازه‌گیری‌های ذخیره شده متناظر با آن وضعیت کارکردی را تکرار کند. سوم اینکه یک سیگنال کنترلی تزریق می‌شود تا کارکرد سیستم را دچار اختلال کند. در واقع در این حمله مهاجم اندازه‌گیری‌ها را طوری تنظیم مجدد می‌کند تا بیان‌گر یک شرایط کارکردی قبلاً ذخیره شده باشد و حمله حالت را از پویایی سیستم پنهان نماید.

پویایی سیستم تحت این حمله به صورت زیر تعریف می‌شود:

$$\begin{aligned} E\dot{x} &= Ax + Bu, \\ y &= C\tilde{x} \end{aligned} \quad (۱۰)$$

به طوری‌که $C\tilde{x}$ اندازه‌گیری‌های ذخیره شده سیستم بدون حمله است. در این حمله $\tilde{x}$ در رابطه زیر صدق می‌کند.

$$E\dot{\tilde{x}} = A\tilde{x} \quad (۱۱)$$

- **حمله منع سرویس**

کنترل‌کننده از آخرین مقادیر خوانده شده توسط حسگرها که در بافرهای ورودی ذخیره شده‌اند استفاده می‌کند [7]. اگر داده‌های حسگر به روز نشوند، کنترل‌کننده از آخرین مقدار ذخیره شده در بافرهای ورودی استفاده می‌کند و تصمیمش را بر آن اساس می‌گیرد. در این صورت، مهاجم کنترل‌کننده را در مورد حالت جاری فرآیند فریب داده است. به عنوان مثال ممکن است نیاز باشد شیری بسته شود در حالی‌که دستور کنترلی آن را باز نگه دارد و یا اینکه موتوری نیاز باشد که خاموش شود و روشن بماند.

بنابراین حمله منع سرویس (DoS) به حسگر i به صورت زیر قابل تعریف است:

$$b_i^a(t) = y_i(t_e) \quad (۱۲)$$

که t_e نشان‌دهنده زمان آغاز حمله DoS است. همچنین برای حمله DoS به کنترل‌کننده i خواهیم داشت:

$$d_i^a(t) = u_i(t_e) \quad (۱۳)$$

۳-۲- پیامد حمله‌ها به سیستم‌های سایبر–فیزیکی

پیامدهای حملات به سیستم‌های سایبر–فیزیکی می‌توانند به پنج دسته کلّی تقسیم‌بندی شوند. مسلماً دسته‌های مختلف به هم مرتبط هستند و بروز یک آسیب می‌تواند منجر به بروز آسیب در گروه دیگر شود. به عنوان مثال، با آسیب دیدن تجهیزات، تولید هم ممکن است متوقف گردد. به هر حال، برای بیشینه کردن اثرات حمله و کمینه کردن هزینه‌ها، دانش کافی در مورد هدف حمله بسیار ضروری است.

- آسیب رساندن به تجهیزات: ممکن است هدف حملات آسیب رساندن به تجهیزات مانند خط لوله‌ها و شیرها باشد. این آسیب خود به دو دسته تقسیم می‌شود [28]:
- فرسوده کردن تجهیزات، که زمان حیات تجهیزات را کاهش می‌دهد.
- نقض کردن محدودیت‌های ایمنی: مانند افزایش فشار داخل یک مخزن تا رسیدن به حد انفجار.
- آسیب رساندن به تولیدات، که خود به دو دسته قابل تقسیم است [28]:
- هدف قرار دادن کیفیت تولید و نرخ تولید: حمله مهاجم ممکن است تولیدات را بی‌استفاده کند.

- هدف قرار دادن هزینه عملیاتی: مثلاً حمله مهاجم ممکن است مصرف انرژی برق را افزایش دهد.
- هدف قرار دادن اقدامات نگهداری: حمله یک مهاجم ممکن است با افزایش تراکم نگهداری، بر روی فرآیند تولید اثر بگذارد. منظور از نگهداری فرآیند رفع عیب تولیدات است. برای مثال عملکرد سریع یک شیر ممکن است ایجاد خلأ نماید. خلأ نهایتاً باعث فرسودگی شیر خواهد شود.
- نقض ایمنی: یک حمله ممکن است موجب به خطر افتادن ایمنی انسان‌ها و کارکنان شود.
- اثرات و آلودگی‌های محیطی: یک حمله ممکن است موجب آلوده شدن هوا، آب و مانند آن شود.

۴- روشی برای ارزیابی پیامد حمله‌ها به سیستم‌های سایبر-فیزیکی

بعد از مدل‌سازی رفتار سیستم و مهاجم، باید برآورد شود که پیامد هر یک از حملات به سیستم‌های سایبر-فیزیکی و مؤلفه‌های کنترلی آن چه خواهد بود. بر این اساس می‌توان میزان حساسیت مؤلفه‌های کنترلی به حملات امنیتی را تخمین زد نمود. در واقع ارزیابی میزان تأثیرگذاری مؤلفه‌ها بر روی یکدیگر، میزان تأثیرپذیری یک مؤلفه از سایر مؤلفه‌ها و میزان اثرات مستقیم و غیرمستقیم حملات بر مؤلفه‌های سیستم می‌تواند اطلاعات مناسبی برای بهبود راهبردهای دفاعی در اختیار قرار دهد.

به منظور پرداختن به این موضوع، روشی برای ارزیابی انتشار پیامد حملات امنیتی به سیستم‌های سایبر-فیزیکی ارائه شده است. برای این کار پارامترهای کنترلی به دو دسته پارامترهای سبب و اثر تقسیم شده‌اند. به این معنا که پارامترهای گروه سبب بر پارامترهای گروه اثر تأثیر می‌گذارند. پارامترهای کنترلی مانند سیگنال‌های حسگر و کنترل‌کننده به عنوان پارامترهای گروه سبب در نظر گرفته می‌شوند. در پارامترهای گروه اثر، بجز پارامترهای کنترلی، پارامترهای دیگری نظیر هزینه‌های عملیاتی هم می‌توانند در نظر گرفته شوند.

با استفاده از روش ارائه شده، می‌توان اثری که حمله به هر پارامتر بر سایر پارامترها دارد و اثر سایر پارامترها بر پارامتر کنترلی مورد نظر را ارزیابی نمود. به طور خلاصه نتیجه این روش این است که می‌توان مؤلفه‌های کنترلی از نظر میزان تأثیرگذاری بر سایر مؤلفه‌ها بر اثر حمله و میزان حساسیت آن‌ها در برابر حملات (میزان تأثیرپذیری) رتبه‌بندی نمود.

همان‌طور که ذکر شد، امنیت سیستم‌های سایبر-فیزیکی به دلیل ارتباط با دنیای فیزیکی حساسیت بالایی دارد. پیامد حملات به این سیستم‌ها ممکن است بسیار پرهزینه و خطرناک باشد و آثار فیزیکی به دنبال داشته باشد و یا زندگی افراد را تهدید کند. بنابراین یکی از موضوعات مهم در امنیت سیستم‌های سایبر-فیزیکی بررسی اثر و پیامد حملات است.

در این بخش روشی برای ارزیابی انتشار پیامد حملات امنیتی به سیستم‌های سایبر-فیزیکی ارائه خواهیم کرد. ورودی روش ارائه شده مؤلفه‌های کنترلی سیستم مانند داده‌های حسگرها و سیگنال‌های کنترلی هستند. در این روش، این مؤلفه‌های کنترلی را هدف اصلی حملات در نظر می‌گیریم و رفتار سیستم را در شرایط عادی با رفتار سیستم تحت حمله مقایسه می‌کنیم. در این روش بررسی می‌کنیم چگونه حمله به یک مؤلفه کنترلی یا دسته از مؤلفه‌ها می‌تواند پارامترهای دیگر را تحت تأثیر قرار دهد و این اثرگذاری تا چه میزان خواهد بود.

پارامترهای کنترلی به دو دسته پارامترهای سبب و اثر تقسیم شده‌اند. به این معنا که پارامترهای گروه سبب بر پارامترهای گروه اثر تأثیر می‌گذارند. پارامترهای کنترلی مانند سیگنال‌های حسگر و کنترل‌کننده به عنوان پارامترهای گروه سبب در نظر گرفته می‌شوند. در پارامترهای گروه اثر، بجز پارامترهای کنترلی، می‌تواند پارامترهای دیگری نظیر هزینه‌های عملیاتی در نظر گرفته شود.

با استفاده از روش ارائه شده می‌توان اثر هر پارامتر بر سایر پارامترها و اثر سایر پارامترها بر پارامتر کنترلی مورد نظر را ارزیابی نمود.

اکنون به توصیف رسمی روش ارائه شده می‌پردازیم. فرض می‌کنیم $T = \{0, 1, 2, \ldots, n\}$ مجموعه لحظات زمانی گسسته، $C = \{c_1, c_2, \ldots, c_m\}$ مجموعه پارامترهای گروه سبب و $E = \{e_1, e_2, \ldots, e_k\}$ مجموعه پارامترهای گروه اثر باشد. در این صورت، مراحل روش ارائه شده به صورت زیر است:

مرحله ۱: ایجاد ماتریس تأثیر مستقیم اولیه، بر اساس رفتار نرمال سیستم بدون وجود حمله ($M_n^t = [n_j]_{1\times k}$) و همچنین با وجود حمله ($M_a^t = [a_{ij}]_{m\times k}$). در واقع ماتریس M_n^t مقدار نرمال پارامترهای کنترلی را در لحظه زمان t نشان می‌دهد. در واقع سطرهای این ماتریس پارامترهای سبب و ستون‌ها پارامترهای اثر هستند که ممکن است یکسان باشند یا نباشند. همچنین ماتریس M_a^t اثر مستقیم بین هر دو پارامتر کنترلی در لحظه زمانی t را نشان می‌دهد. سطرهای این ماتریس نشان‌دهنده حملات انجام شده به متغیرهای کنترلی سبب و ستون‌ها هم نشان‌دهنده پارامترهای اثر هستند. در صورتی که پارامترهای اثر و سبب یکسان باشند خواهیم داشت: $n = m = p$.

مرحله ۲: ایجاد ماتریس انحراف اولیه ($M_d^t = [d_{ij}]_{m\times k}$). درایه‌های این ماتریس که از رابطه زیر به دست می‌آیند نشان‌دهنده انحراف پارامترهای کنترلی سیستم از مقدار نرمال هستند:

$$M_d^t = [d_{ij}]_{m\times k} = \left| n_j^t - a_{ij}^t \right| / n_j^t \qquad (۱۴)$$

مرحله ۳: ایجاد ماتریس اثر نرمال‌شده. ماتریس اثر نرمال شده با استفاده از رابطه زیر به دست می‌آید:

$$M^t = w.M_d^t \qquad (۱۵)$$

به طوری‌که:

$$w = 1/(\max_{1\le i\le m} \sum_{j=1}^{k} d_{ij}) \qquad (۱۶)$$

مرحله ۴: ایجاد ماتریس پیامد نهایی R. با فرض برابر بودن پارامترهای سبب و اثر، ماتریس اثر کلی از رابطه زیر قابل محاسبه است:

$$R^t = M^t (1 - M^t)^{-1} \qquad (۱۷)$$

نکته آنکه پس از مرحله نرمال‌سازی، هر درایه ماتریس در این رابطه صدق می‌کنند:

$$0 \le m_{ij} < 1,$$
$$0 \le \sum_i m_{ij} \le 1 and 0 < \sum_j m_{ij} \le 1 \quad (۱۸)$$

در این صورت، حداقل جمع یک سطر یا یک ستون ماتریس برابر یک خواهد بود. همچنین خواهیم داشت:

$$\lim_{h\to\infty} M^h = [0]_{p\times p} \quad (۱۹)$$

در نتیجه ماتریس پیامد نهایی به صورت زیر قابل محاسبه است:

$$R = M(I-M)^h(I-M)^{-1} \quad (۲۰)$$

هنگامی که $\lim_{h\to\infty} M^h = [0]_{p\times p}$ خواهیم داشت: $R = M(I-M)^{-1}$.

بعد از محاسبه ماتریس پیامد نهایی، مقادیر جدید را می‌توان به گراف وابستگی ایجاد شده انتساب داد. این مقادیر نشان‌دهنده اثرات کلّی هر پارامتر (مستقیم و غیرمستقیم) بر دیگر پارامترهاست.

مرحله۵: ارزیابی. در این مرحله دو بردار جدید تعریف می‌شوند. بردار اول ($V_r^t = [r_j^t]_{m\times 1}$) نشان‌دهنده میزان اثراتی است که حمله به یک پارامتر بر روی سایر پارامترها می‌گذارد و بردار دوم ($V_c^t = [c_i^t]_{1\times k}$) نشان‌دهنده میزان اثری است که یک پارامتر از انجام حمله به سایر پارامترها خواهد داشت.

بر این اساس دو سنجه جدید قابل تعریف هستند. سنجه (u_i^t) که و سنجه (l_i^t) که این دو سنجه به صورت زیر قابل تعریف هستند:

$$u_i^t = r_i^t + c_i^t \text{ و } l_i^t = r_i^t - c_i^t \quad (۲۱)$$

مرحله۶: رتبه‌بندی پارامترها بر اساس میزان اثرات آن‌ها در سیستم.

در صورتی که پارامترهای سبب و اثر یکی باشند، با استفاده از مقادیر u_i و l_i می‌توانیم میزان اثرات مستقیم و غیرمستقیم حملات به پارامترهای کنترلی مورد نظر را ارزیابی کنیم. در صورتی که این پارامترهای متفاوت باشند، رتبه‌بندی بر اساس بردارهای V_r و V_c که در مرحله قبل بدست آمدند انجام می‌شود. در این حالت تنها اثرات مستقیم قابل اندازه‌گیری است و اثرات غیرمستقیم قابل مطالعه نیستند.

شایان ذکر است که مراحل ذکر شده از لحظه زمانی t_0 تا t_n تکرار می‌شوند و در هر لحظه از زمان، رتبه‌بندی ذکر شده انجام می‌شود. فاصله بین این لحظه‌های زمانی برای سیستم‌های مختلف متفاوت است و باید توسط متخصصان امنیت سیستم انجام شود.

با استفاده از روش ذکر شده و رتبه‌بندی انجام شده، پارامترهای کنترلی که حساسیت امنیتی بالایی دارند قابل شناسایی هستند و اقدامات دفاعی متناسب با آن قابل به کارگیری است.

۵- مطالعه موردی

در این بخش به بررسی یک سیستم صنعتی شیمیایی [30] می‌پردازیم. معماری این واحد صنعتی در شکل (۳) نشان داده شده است. شبکه‌های کنترلی، سازمانی و ناحیه بی‌طرف آن مطابق با معماری ارائه شده برای سیستم‌های سایبر-فیزیکی در این شکل مشخص است.

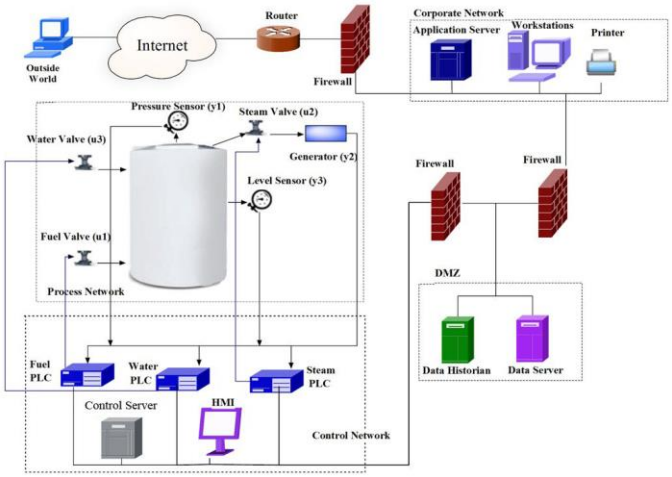
این سیستم دارای سه شیر است: شیر ورودی آب (u_3) ، شیر جریان (u_2) و شیر سوخت (u_1). همچنین اندازه‌گیری پدیده‌های فیزیکی در این سیستم توسط سه حسگر انجام می‌شود: حسگر فشار داخل مخزن (x_1)، حسگر سطح آب (x_2) و حسگر انرژی الکتریکی تولید شده (x_3). همچنین در رفتار حالت پایدار سیستم، موقعیت شیرها به این صورت تعریف شده است: $u_1 = 0.34$, $u_2 = 0.69$, $u_3 = 0.433$.

علاوه بر این، سرعت تغییر وضعیت شیرها که به صورت زیر تعریف شده‌اند:

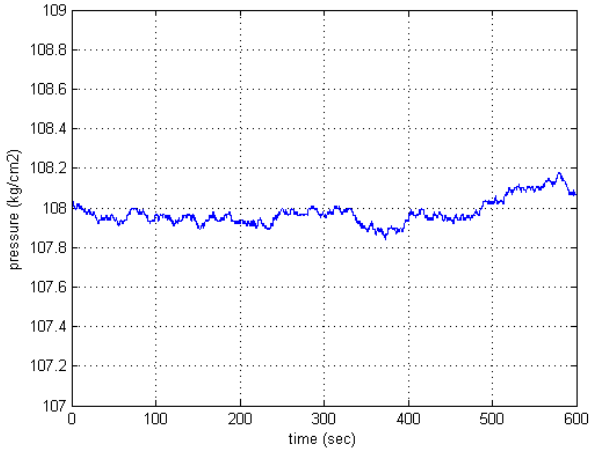
$$0.007 \le \dot{u}_1 \le 0.007/\text{sec},$$
$$-1.0 \le \dot{u}_2 \le 1.0/\text{sec}, \quad (۲۲)$$
$$-0.05 \le \dot{u}_3 \le 0.05/\text{sec}$$

این سیستم از سه کنترل‌کننده برای کنترل کارکرد فرآیند فیزیکی تحت کنترل استفاده می‌کند: کنترل‌کننده جریان (c_1)، کنترل‌کننده ورودی آب (c_2) و کنترل‌کننده سوخت (c_3). هر سه کنترل‌کننده دارای تأخیر انجام کار برابر با 100میلی ثانیه هستند. بنابراین داریم: $TS_i = 100\text{ms}$, $i=1, 2, 3$.

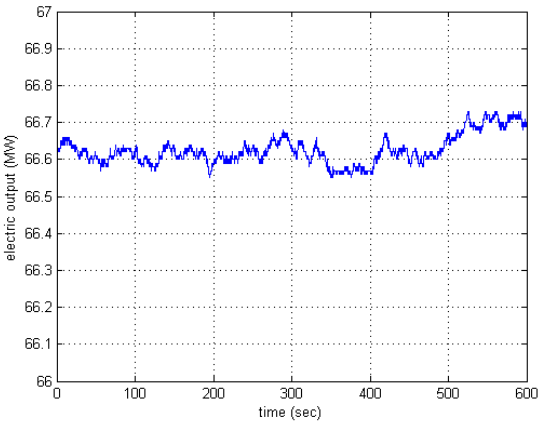
برای این سیستم یک محدودیت ایمنی وجود دارد. اگر فشار داخل مخزن به 250kg/cm^2 برسد، انفجار رخ خواهد داد که این موضوع در تابع نگهبان مدل امنیت در نظر گرفته می‌شود.



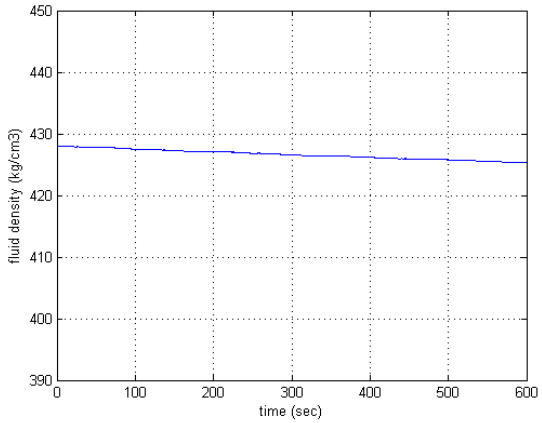
شکل (۳) : سیستم سایبر-فیزیکی مورد مطالعه [30]



شکل (۴) : فشار داخل مخزن به همراه نویز



شکل (۵) : انرژی الکتریکی خروجی به همراه نویز



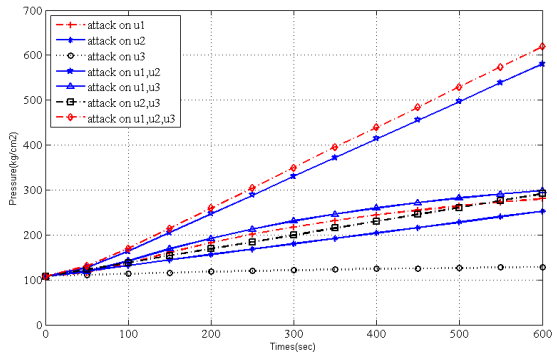
شکل (۶) : غلظت جریان به همراه نویز

مجموعه متغیرهای سیستم به این صورت است: $X=\{x_1, x_2, x_3, y_1, y_2, y_3, u_1, u_2, u_3, e_r, s_q\}$. که در آن y_3 نشان‌دهنده سطح آب است و e_r و s_q به ترتیب کیفیت جریان و نرخ تبخیر را نشان می‌دهند.

فرض شده است که مهاجم برای رسیدن به هدفش سعی به تغییر سیگنال‌های کنترلی صادر شده توسط کنترل‌کننده‌ها به شیرها می‌نماید. به همین منظور او سعی می‌کند شیر سوخت را با تزریق سیگنال نادرست به طور کامل باز کند و شیرهای ورودی آب و جریان را به طور کامل ببندد.

وضعیت فشار داخل مخزن (شکل (۴))، انرژی الکتریکی تولید شده (شکل (۵)) و غلظت جریان (شکل (۶)) را با وجود نویز گوسی با انحراف معیار ۰٫۰۵ و میانگین ۰ و بدون وجود حمله نشان می‌دهد. این میزان نویز به داده‌های حسگر و سیگنال‌های کنترلی اعمال شده است تا سیستم نتواند به حالت پایدار بازگشت نماید.

فرض می‌کنیم مهاجم حمله‌های تکی یا ترکیبی را در جهت نقض جامعیت سیگنال‌های کنترلی انجام می‌دهد. شکل (۷) میزان فشار داخل مخزن بر اثر هر یک از حمله‌های انجام شده را نشان می‌دهد. ابتدا حمله به سیگنال کنترلی u_1 مربوط به شیر سوخت را در نظر می‌گیریم. فرض می‌کنیم بسته‌های ارسال شده توسط مهاجم با در نظر گرفتن محدودیت سرعت شیرها اثرگذار خواهند بود. در مورد این حمله، مهاجم شیر سوخت را کامل باز می‌کند و فشار داخل مخزن بعد از ۴۲۴٫۶ ثانیه به مقدار 250kg/cm2 می‌رسد. حمله بعدی حمله به سیگنال مربوط به شیر جریان یعنی u_2 است. در اینجا



شکل (۷) : فشار داخل مخزن بر اثر حمله‌های مختلف

هدف مهاجم بسته نگه داشتن شیر جریان است. در مورد این حمله فشار داخل مخزن بعد از ۵۹۰ ثانیه به مقدار نامطلوب می‌رسد. حمله سوم حمله به سیگنال مربوط به شیر آب یعنی u_3 است. مهاجم برای آنکه با حمله به این سیگنال کنترلی به هدف مورد نظرش برسد، باید شیر ورودی آب را در حالت بسته نگه دارد. در مورد این حمله فشار داخل مخزن به این مقدار نامطلوب نمی‌رسد.

اکنون حمله‌های ترکیبی را در نظر می‌گیریم. ابتدا فرض می‌کنیم حمله به سیگنال‌های کنترلی u_1 و u_2 انجام شود. در این حمله مهاجم سعی می‌کند شیر سوخت را باز و شیر جریان را بسته نگه دارد. همان‌طور که در شکل (۷) نشان داده شده است، بر اثر این حمله بعد از ۲۰۳٫۹ ثانیه فشار داخل مخزن به حد نامطلوب می‌رسد. حمله بعدی حمله ترکیبی به سیگنال‌های u_1 و u_3 است. بر اثر این حمله هم بعد از ۳۶۲٫۷ ثانیه فشار داخل مخزن به حد نامطلوب می‌رسد. مورد بعدی حمله ترکیبی به u_2 و u_3 است. بر اثر این حمله، فشار داخل مخزن بعد از ۴۶۵٫۱ ثانیه به مقدار 250kg/cm^2 می‌رسد. حمله آخر حمله ترکیبی بر سه سیگنال کنترلی u_1 و u_2 و u_3 است. همان‌طور که در شکل (۷) مشخص است، بر اثر این حمله فشار داخل مخزن بعد از ۱۸۹٫۶ ثانیه به حد مورد انتظار مهاجم خواهد رسید.

مطالعه پارامترهای گروه سبب به صورت زیر در نظر گرفته می‌شود:

- سیگنال‌های کنترلی وضعیت شیر سوخت
- سیگنال‌های کنترلی وضعیت شیر جریان
- سیگنال‌های کنترلی وضعیت شیر ورودی آب

پارامترهای گروه اثر هم به صورت زیر در نظر گرفته می‌شوند:

- فشار داخل مخزن
- انرژی الکتریکی تولید شده
- غلظت جریان

فرض شده است مهاجم می‌تواند حملاتی به یک پارامتر کنترلی یا ترکیبی از پارامترهای کنترلی ترتیب دهد. ابتدا رفتار عادی سیستم بدون خطا مورد مطالعه قرار می‌گیرد. سپس رفتار سیستم تحت حمله بررسی می‌شود و با رفتار نرمال مقایسه می‌گردد. در نهایت نتایج زیر از این روش بدست خواهد آمد:

- اولویت‌بندی حمله‌های انجام شده بر اساس میزان تأثیر آن‌ها بر پارامترهای اثر در نظر گرفته شده
- اولویت‌بندی و رتبه‌بندی پارامترهای اثر بر اساس میزان تأثیرپذیریشان از حملات انجام شده

با توجه به روش کشف ذکر شده، مقدار پارامترهای کشف مورد نظر برای سیگنال‌های کنترلی و حسگری به صورت جدول (۱) بدست آمده‌اند.

حمله‌های جامعیت انجام شده به مؤلفه‌های کنترلی سیستم به صورت زیر قابل تعریف است:

$$u_1 = u_1 * 1.05,\ u_2 = u_2 * 1.05,\ \text{and}\ u_3 = u_3 * 0.95$$

اکنون به توضیح کامل مراحل روش پیشنهادی می‌پردازیم. رفتار سیستم در هر ۵۰ ثانیه مورد بررسی قرار گرفته است. این مقدار برای سیستم‌های مختلف متفاوت خواهد بود و باید توسط متخصص سیستم و با توجه به میزان حساسیت سیستم به اختلال انتخاب شود.

مرحله ۱: در این مرحله، وضعیت سیستم در حالت عادی اولیه و با نویز مورد بررسی قرار می‌گیرد. شکل‌های (۴)، (۵) و (۶) میزان فشار داخل مخزن، انرژی الکتریکی تولید شده و غلظت جریان را در حالت عادی و با نویز نشان می‌دهد. در گام بعدی مقدار پارامترها بعد از انجام حمله به سیستم حاصل می‌شوند. شکل‌های (۸)، (۹) و (۱۰) میزان تأثیر حملات بر این پارامترها را در هر لحظه زمانی نشان می‌دهد.

مرحله ۲: در این مرحله با توجه به داده‌های بدست آمده از مرحله قبل (M_n و M_a)، میزان انحراف (M_d) پارامترهای اثر محاسبه می‌شود.

مرحله ۳: در این مرحله داده‌های اثر بدست آمده در مرحله ۲ نرمال‌سازی می‌شوند.

مرحله ۴: از آنجا که پارامترهای سبب و اثر یکسان نیستند، از این مرحله صرف نظر می‌شود.

مرحله ۵: در این مرحله اثر کلی حمله‌ها بر پارامترهای کنترلی محاسبه می‌شوند تا بردارهای V_r و V_c محاسبه می‌شوند. نتایج کمّی نهایی شکل (۱۱) و شکل (۱۲) نشان داده شده‌اند. شکل (۱۱) حملات را بر اساس پیامد آن‌ها رتبه‌بندی کرده است و شکل (۱۲) پارامترهای کنترلی را بر اساس میزان تأثیرپذیریشان رتبه‌بندی نموده است.

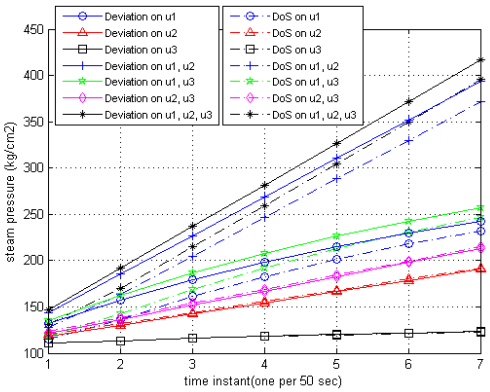
مرحله ۶: با توجه به متفاوت بودن پارامترهای سبب و اثر، رتبه‌بندی نهایی بر اساس دو بردار بدست آمده در مرحله قبل انجام می‌شود.

با توجه به تحلیل انجام شده و مقادیر کمّی حاصل شده، نتایج زیر از این مطالعه حاصل شده‌اند:

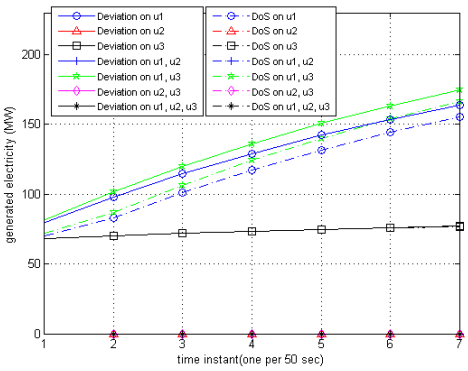
- سیگنال‌های کنترلی جریان و سوخت حساس‌ترین سیگنال‌های کنترلی هستند.
- به منظور هدف قرار دادن پارامترهای اثر مختلف (به عنوان مثال فشار داخل مخزن یا جریان الکتریکی تولید شده) نیاز است پارامترهای کنترلی مختلفی هدف قرار داده شوند.

جدول (۱) : مقدار پارامترهای کشف حمله در سیستم مورد نظر

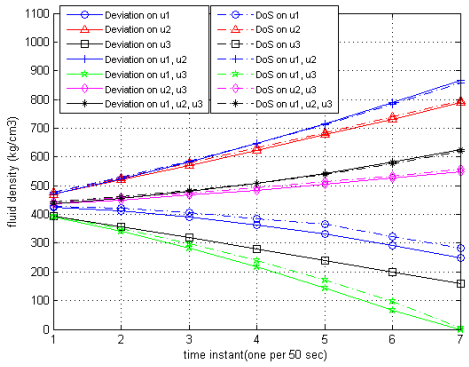
مولفه کنترلی	b_i	τ_i
u_1	0.3	600
u_2	0.2	600
u_3	0.2	1000
x_1	0.1	1500
x_2	0.3	1000
x_3	1.5	2000



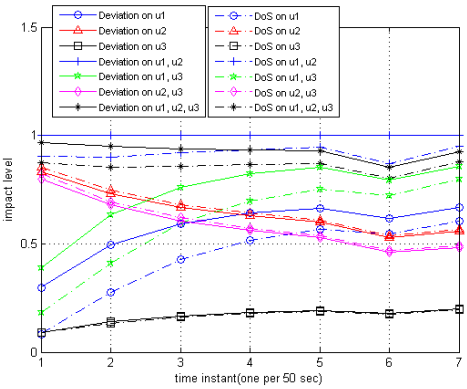
شکل (۸) : تاثیر حمله بر فشار داخل مخزن در زمان‌های مختلف



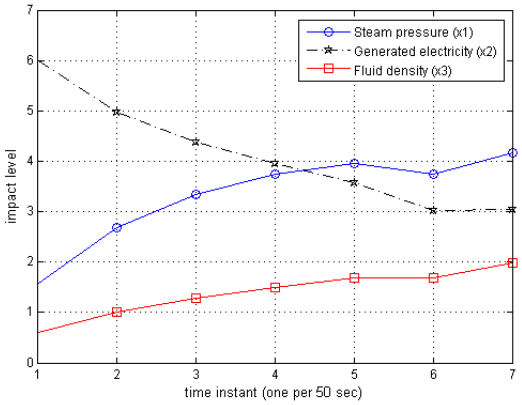
شکل (۹) : تاثیر حمله بر الکتریسیته در زمان‌های مختلف



شکل (۱۰) : تاثیر حمله بر غلظت جریان در زمان‌های مختلف



شکل (۱۱) : میزان اثرگذاری حملات بر پارامترهای کنترلی



شکل (۱۲) : میزان تاثیرپذیری پارامترهای کنترلی از حملات

- با توجه به نتایج حملات، حمله‌های ترکیبی به u_1، u_2، u_3خطرناک‌ترین نوع حمله به این سیستم است. همچنین حمله به سیگنال کنترلی u_3 کمترین اثر را بر پارامترهای سیستم داشته است.
- همان‌طور که شکل (۱۱) نشان می‌دهد، میزان پیامد حملات در لحظه‌های زمانی مختلف ممکن است تغییر کند.
- حساس‌ترین پارامترهای سیستم فشار داخل مخزن و میزان الکتریسیته تولید شده است.
- همچنین میزان حساسیت پارامترهای اثر با گذشت زمان تغییر می‌کند (شکل (۱۲)).

۶- نتیجه

این مقاله به بررسی امنیت سیستم‌های سایبر-فیزیکی و جنبه‌های متفاوت امنیت در این سیستم‌ها نسبت به سیستم‌های سایبری پرداخته است. همچنین روشی برای ارزیابی پیامد حملات به این سیستم‌ها ارائه شده است. نتایج مطالعات نشان می‌دهد، به منظور ایجاد اختلال فیزیکی، مهاجمین ناگزیرند که بر روی کنترل سیستم متمرکز شوند، از اثر حملات خود باخبر باشند و شرایط خرابی تجهیزات سیستم، اصول کنترل، رفتار فرآیند، پردازش سیگنال و کارکرد فرآیند فیزیکی تحت کنترل را به طور دقیق بشناسند [20]. بدون این دانش حمله ایجاد شده علیه سیستم با احتمال بسیار زیاد منجر به اختلال ناچیز خواهد شد، به جای اینکه منجر به خسارت فیزیکی جدّی شود [20] و [21]. به عنوان مثال، هکرهای آمریکایی با سوءاستفاده از آسیب‌پذیری‌های یک خودروی جیپ توانستند از راه دور به شبکه داخلی آن دسترسی پیدا کنند و کارکردهایی مانند سیستم تهویه، برف پاک‌کن، موتور و ترمزها را تحت اختیار خود قرار دهند [22]. اگر حمله‌ای بدون تمرکز بر سطح کنترل سیستم و بدون اطلاع از اثرات آن بر روی فرآیند فیزیکی انجام شود، با احتمال بالا تنها مزاحمت کوچکی را برای سیستم به بار می‌آورد به جای اینکه موجب خرابی واقعی سیستم شود [23] و [24].

سپاسگزاری

با سپس و تقدیم احترام به استاد گرانقدر دوره دکتری اینجانب، جناب آقای دکتر محمد عبداللّهی ازگمی که همواره راهنما و مشاور بنده بودند.

مراجع

[1] H. Fei and et.al., "Robust Cyber–Physical Systems: Concept, models, and implementation," *Future Generation Computer Systems*, vol. 56, pp. 449-475, 2016.

[2] M. Krotofil and et.al., "Are You Threatening My Hazards?," in *9th International Workshop on Security (IWSEC'14)*, Hirosaki, Japan, August 2014, pp.17-32.

[3] R. Akella and e. al., "Analysis of Information Flow Security in Cyber–Physical Systems," *International Journal of Critical Infrastructure Protection*, pp. 157-173, 2010.

[4] M. Burmester and e. al., "Modeling Security in Cyber–Physical Systems," *International Journal of Critical Infrastructure Protection*, vol. 2012, pp. 118-126.

[5] F. Pasqualetti, "Secure Control Systems: A Control-Theoretic Approach to Cyber-Physical Security," PhD.Thesis, University Of California, 2012.

[6] A. Teixeira and et.al., "Revealing Stealthy Attacks in Control Systems," in *proceeding of Fiftieth Annual Allerton Conference Allerton House, UIUC, IEEE Press*, Illinois, USA, 2012, pp. 1806-1813.

[7] A. Hoehn and et.al., "Detection of replay attacks in cyber-physical systems," in *American Automatic Control Council (AACC)*, 2016, pp. 290-295.

[8] C. Kwon and et.al., "Security Analysis for Cyber-Physical Systems against Stealthy Deception Attacks," in *American Control Conference (ACC)*, 2013, pp. 3344-3349.

[9] H. Orojloo and M. Abdollahi Azgomi, "A Game-Theoretic Approach to Model and Quantify the Security of Cyber-Physical Systems", *Computer in Industry*, Vol. 88, Elsevier, 2017, pp. 44-57.

[10] H. Orojloo and M. Abdollahi Azgomi, "A method for evaluating the consequence propagation of security attacks in cyber-physical systems," *Future Generation Computer Systems (FGCS)*, Vol. 67, Elsevier, Feb. 2017, pp. 57-71.

[11] H. Orojloo and M. Abdollahi Azgomi, "A Stochastic Game Model for Evaluating the Impacts of Security Attacks Against Cyber-Physical Systems." *Journal of Network and Systems Management*: 1-37. https://link.springer.com/article/10.1007/s10922-018-9449-0.

[12] H. Orojloo and M. Abdollahi Azgomi, " Predicting the Behavior of Attackers and the Consequences of Attacks against Cyber-Physical Systems," Security and Communication Networks, Wiley, vol. 9, pp.6111-6136.

[13] H. Kopetz, Real-Time Systems: Design Principles for Distributed Embedded Applications, 2d. ed., Real-Time Systems Series, 2011.

[14] M. Krotofil and et.al., "The Process Matters: Ensuring Data Veracity in Cyber-physical Systems," in *10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '15)*, Singapore, April 2015, pp. 133-144.

[15] M. Krotofil and et.al., "Resilience of process control systems to cyber-physical attacks," in *Nordic Conference on Secure IT Systems, Springer Berlin Heidelberg*, October 2013, pp. 166-182.

[16] A. Hahn and et.al., "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 11, pp. 39-50, 2015.

[17] k. Stouffer and et.al., "Guide to Industrial Control Systems (ICS) Security," Recommendations of the National Institute of Standards and Technology, 2011.
[18] R. Hills, "Common VPN security flaws," White Paper, NTA Monitor, Rochester,www.nta-monitor.com/posts/2005/01/VPN-Flaws- Whitepaper.pdf, 2005.
[19] M. Majdalawieh, "Security Framework for DNP3 and SCADA," VDM Verlag, 2008.
[20] "Commission, International Electrotechnical," Technical Specification IEC TS 61850, Geneva, Switzerland, 2003.
[21] "Modbus-IDA, Modbus Application Protocol Specification V.1.1b, Hopkinton," Massachusetts. Available onlline: www.modbus.org/docs/Modbus_Application_Protocol_ V1_1b.pdf, 2006.
[22] H. Li and et.al., "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1097-1107, 2012.
[23] C. Miller and et.al., "Adventures in automotive networks and control units," *DEF CON*, vol. 21, pp. 260-264, 2013.
[24] M. Krotofil and et.al., "CPS: Driving cyber-physical systems to unsafe operating conditions by timing DoS attacks on sensor signals," in *30th Annual Computer Security Applications Conference*, 2014, pp. 146-155.
[25] B. Genge and et.al., "Impact of network infrastructure parameters to the effectiveness of cyber attacks against industrial control systems," *International Journal of Computers Communications & Control*, vol. 7, no. 4, pp. 674-687, 2014.
[26] C. Ten and et.al., "Anomaly detection for cybersecurity of the substations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 865-873, 2011.
[27] M. Krotofil and et.al., "Resilience of process control systems to cyber-physical attacks," in *Nordic Conference on Secure IT Systems, Springer Berlin Heidelberg*, October 2013, pp. 166-182.
[28] Krotofil and et.al., "The Process Matters: Ensuring Data Veracity in Cyber-physical Systems," in *10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '15)*, Singapore, April 2015, pp. 133-144.
[29] A. A. Cardenas and et.al., "Attacks against process control systems: risk assessment, detection, and response," in *6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11)*, Hong Kong, March 2011, pp. 355-366.
[30] T. Wen and et.al., "Analysis and control of a nonlinear boiler-turbine unit," *Journal of Process Control*, vol. 15, no. 8, pp. 883-891, 2005.