فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال ششم، شماره یک، بهار 1401

روشی برای ارزیابی قابلیت اطمینان سیستم‌های سایبر - فیزیکی

حامد سپهرزاده[1]

تاریخ دریافت: 1401/02/18 **تاریخ پذیرش:** 1401/05/10

چکیده

سیستم‌های سایبر-فیزیکی ترکیبی از فضای سایبری و فرآیندهای فیزیکی هستند که در آن‌ها سیستم‌ها و فرآیندهای فیزیکی توسط بخش سایبری نظارت و مدیریت می‌شود. هدف از ورود بخش سایبر به دنیای فیزیکی افزایش انعطاف‌پذیری و بهبود کارایی سیستم‌هاست. امروزه این سیستم‌ها در زیرساخت‌های حیاتی نقش کلیدی دارند. این پیشرفت از طرف دیگر این سیستم‌ها را در معرض مخاطرات امنیتی جدّی قرار داده است که پیش از این وجود نداشته‌اند. بنابراین پرداختن به امنیت و قابلیت اطمینان این سیستم‌ها بسیار ضروری است. در این مقاله، روشی برای مدل‌سازی و ارزیابی قابلیت اطمینان سیستم‌های سایبر-فیزیکی در برابر حملات امنیتی ارائه شده است. در این روش رفتار مهاجم در نفوذ و حمله به سیستم به همراه رفتار سیستم با در نظر گرفتن اقدامات دفاعی مانند استفاده از مؤلفه‌های افزونه و راهبردهای تشخیص نفوذ مدل‌سازی شده است. ارزیابی کمّی قابلیت اطمینان با استفاده از سنجه‌های دسترس‌پذیری و میانگین زمان تا خرابی سیستم انجام شده است. نهایتاً در یک مثال، کاربردپذیری روش پیشنهادی نشان داده شده است.

واژگان کلیدی: سیستم‌های سایبر-فیزیکی، امنیت، قابلیت اطمینان، ارزیابی کمّی .

[1] گروه مهندسی کامپیوتر، دانشگاه فنی و حرفه‌ای، تهران، ایران (دانشکده شهید شمسی پور، استادیار) hsepehrzadeh@tvu.ac.ir

1. مقدمه

ورود فناوری اطلاعات و ارتباطات (ICT) در سیستم‌های صنعتی منجر به پیدایش صنعت 4,0[2] و سیستم‌های سایبر-فیزیکی[3] (CPS) می‌شود. [1]. در حقیقت، ماشین‌ها و دستگاه‌ها به‌عنوان یک جامعه مشارکتی در صنعت 4,0 به هم متصل شده‌اند و نقشی حیاتی در تولیدات صنعتی دارند. این امر باعث ترویج صنعت مبتنی بر سیستم‌های رایانه‌ای شده است که هدف آن اتخاذ تصمیمات غیرمتمرکز است. سیستم‌های سایبر-فیزیکی ترکیب فرآیند فیزیکی با پردازش، کنترل و نظارت توکار بر شبکه، با استفاده از حلقه‌های بازخوردی[4] است [1و 2]. در واقع سه جزء اصلی تعریف این سیستم‌ها، پردازش، ارتباط و کنترل است.

سه مؤلفه اصلی تشکیل دهنده سیستم‌های سایبر-فیزیکی حسگرها، کنترل‌کننده‌ها و محرّک‌ها هستند [3]. حسگرها وظیفه اندازه‌گیری برخی از پدیده‌های فیزیکی مانند فشار یا دما را بر عهده دارند. کنترل‌کننده‌ها مسئول انجام محاسبات بر اساس اطلاعات دریافتی از حسگرها و اعمال دستورهای کنترلی به محرّک‌ها هستند. محرّک ها هم دستورات دریافتی از کنترل‌کننده‌ها را بر سیستم فیزیکی اعمال می‌کنند [4].

سیستم‌های سایبر-فیزیکی در سیستم‌های حمل و نقل و توزیع، شبکه‌های برق هوشمند [5 و 6]، سیستم‌های مراقبت‌های بهداشتی [7 و 8 و 9]، تولید هوشمند [10 و 11]، صنایع شیمیایی و آبی [12] دیده می‌شوند. به دلیل حوزه‌های کاربردی حساس این سیستم‌ها، امنیت و قابلیت اطمینان[5] آن‌ها به یک حوزه فعّال پژوهشی تبدیل شده است.

داده‌ها و اطلاعات ارسال شده بین اجزای اصلی سیستم‌های سایبر-فیزیکی باید به صورت بی‌درنگ مبادله شوند [13]. داده‌های تهیه شده توسط حسگرها می‌توانند توسط کنترل‌کننده‌ها برای مدت زمان مشخصی مورد استفاده قرار گیرند، بنابراین دقت و تازگی داده‌ها بسیار مهم است. این زمان تأثیر بسزایی در عملکرد صحیح این سیستم‌ها دارد.

یک مهاجم ممکن است با انجام حملات جلوگیری از سرویس[6] (**DoS**) و حمله یکپارچگی[7] علیه خوانده‌های حسگر و سیگنال‌های کنترل، دسترس‌پذیری و صحّت عملکرد این دستگاه‌ها را هدف قرار دهد [14].

سیستم‌های سایبر-فیزیکی با توجه به ماهیتشان به طور کلّی به دو دسته خراب- ایمن[8] و خراب – عملیاتی[9] تقسیم‌بندی می شوند [15]. در د سته اول، سی ستم 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 د سته ه ستند. در دسته دوم، کارکرد پیوسته سیستم با ارائه حداقل سطح خدمت، 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.

این مقاله روشی را برای مدل‌سازی و ارزیابی قابلیت اطمینان سیستم‌های سایبر-فیزیکی در برابر حملات سایبری مخرّب ارائه می‌کند. روش ارائه شده مبتنی بر زنجیره‌های شبه مارکوف است. فرض شده است که این سیستم‌ها به منظور انجام اقدامات مدافعانه در برابر تهدیدات مهاجمان، به برخی تمهیدات مانند سیستم تشخیص نفوذ و مؤلفه‌های افزونه مجهز هستند. اهداف اصلی مقاله به شرح زیر است:

- ارائه یک روش مدل‌سازی برای در نظر گرفتن رفتار سیستم در شرایط عادی و تحت حملات امنیتی، با برخی اقدامات مدافعانه مانند مؤلفه‌های افزونه و سیستم‌های تشخیص نفوذ.
- بررسی تأثیر برخی پارامترهای مهم بر قابلیت اطمینان سیستم‌های سایبر-فیزیکی از جمله احتمال نفوذ، احتمال حمله،

[2] Industry 4.0
[3] Cyber-Physical Systems
[4] Feadback loops
[5] Reliability
[6] Denial of Service
[7] Integrity
[8] fail – safe
[9] fail – operational

احتمال تشخیص حمله، بازه زمانی تشخیص نفوذ، بازه زمانی حمله و نفوذ و ضریب افزونگی مؤلفه‌های سیستم.

• ارزیابی قابلیت اطمینان سیستم‌های سایبر-فیزیکی با بهره‌گیری از رویکرد مدل‌سازی ارائه‌شده بر اساس میزان دسترس‌پذیری سیستم و میانگین زمان تا خرابی.

• ارائه یک مثال به منظور نمایش کاربردی بودن روش پیشنهادی با بررسی سناریوهای مختلف حمله و پارامترهای با مقادیر مختلف.

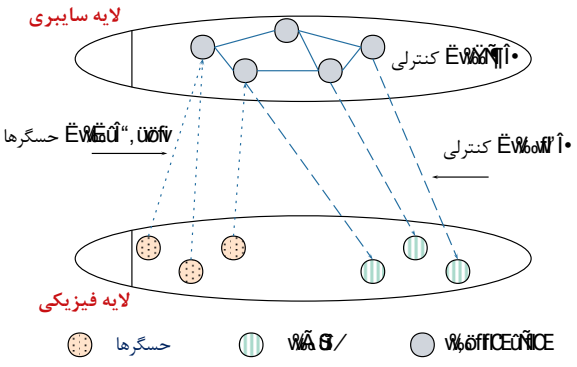
ساختار ادامه مقاله به شرح زیر است. بخش 2 برخی از کارهای مرتبط را برای مدل‌سازی و ارزیابی امنیت و قابلیت اطمینان سیستم‌های سایبر-فیزیکی ارائه می‌کند. بخش 3، مدل سیستم، توضیحات و اقدامات دفاعی در نظر گرفته شده را توصیف می‌کند. بخش 4، رویکردی برای مدل‌سازی و ارزیابی قابلیت اطمینان سیستم‌های سایبر-فیزیکی در برابر حملات امنیتی را پیشنهاد می‌کند. بخش 5، به ارائه یک مثال به منظور مشاهده کاربردپذیری روش پیشنهادی می‌پردازد و در نهایت بخش 6 نتایج مقاله را توصیف می‌کند.

2. مفاهیم پایه

2-1. سیستم‌های سایبر-فیزیکی

هر سیستم سایبر-فیزیکی از چندین حلقه کنترل ساده و پیچیده تشکیل شده است که در آن فرآیند فیزیکی توسط لایه سایبری کنترل و نظارت می‌شود [3]. شکل 1 انتزاعی از یک سیستم سایبر-فیزیکی را نشان می‌دهد.

سیستم‌های سایبر-فیزیکی در متون مختلف به عنوان سیستم‌های کنترل شبکه‌ای و یا سیستم‌های کنترل صنعتی هم شناخته می‌شوند [1 و 2]. 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 برنامه‌ریزی10 (**PLC**) هستند) ارسال می‌شوند. این کار معمولاً با نوشتن اطلاعات دریافت شده در بافرهای ورودی کنترل‌کننده‌ها انجام می‌شود [16]. کنترل‌کننده‌ها از آخرین مقدار ذخیره شده در بافرهای ورودی استفاده می‌کند و تصمیم کنترلی مناسب را بر آن اساس می‌گیرند.



شکل 1. انتزاعی از سیستم‌های سایبر-فیزیکی.

حالت فعلی یک سیستم سایبر-فیزیکی با استفاده از متغیرهای فرآیند[11] یا متغیرهای حالت[12] قابل توصیف است [15]. دو نوع از متغیرهای حالت مهم در این سیستم‌ها، متغیرهای اندازه‌گیری شده[13] و متغیرهای کنترلی[14] 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[15] منبع فیزیکی در لحظه گفته می‌شود. حسگرها این تصویرها را، به طور دوره‌ای یا بر اساس رخ دادن یک رویداد، به کنترل‌کننده‌ها ارسال می‌کنند [15]. مقدار عادی یک متغیر کنترلی نقطه تعیین شده[16] 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 محرّک ها ارسال می‌دارند. در نهایت، محرّک ها دستورات دریافت شده را به دستگاه‌های فیزیکی اعمال می‌کنند. این حلقه کنترلی به طور

10 Programmable Logic Controller
11 Process variable
12 State
13 measured variables
14 Control variable
15 Image
16 Set-point

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال ششم، شمارهٔ یک، بهار 1401

بی‌درنگ انجام می‌شود و تأخیر ناخواسته و عمدی نباید در آن ایجاد گردد [15 و 17].

در هر لحظه وضعیت سیستم به کنسول اپراتور در ایستگاه واسط انسان-ماشین[17] (**HMI**) ارسال می‌شود تا اپراتور سیستم در جریان وضعیت سیستم باشد [18]. اپراتور می‌تواند با توجه به شرایط در کنترل خودکار دخالت کرده و وضعیت یا کد کنترل‌کننده را تغییر دهد.

2-2. امنیت و قابلیت اطمینان سیستم‌های سایبر-فیزیکی

در سیستم‌های سایبر-فیزیکی، هدف اصلی اقدامات بهبود قابلیت اطمینان و امنیت، محافظت از کارکردها است. بنابراین، ما با معیارهایی مواجه هستیم که تأثیر حملات بر عملکرد کنترل سیستم را محاسبه می‌کند [19]. اهداف و پیامدهای حملات امنیتی با اثرات حملات بر سیستم‌های اطلاعاتی سنتی متفاوت است. حمله موفقیت آمیز به یک سیستم سایبر-فیزیکی ممکن است منجر به ایجاد خرابی یا اختلال فیزیکی، خطرات ایمنی، فرسودگی تجهیزات، آسیب بر تولید و آلودگی محیطی شود [20].

در سیستم‌های سایبر-فیزیکی نه تنها بهبود قابلیت اطمینان و امنیت بسیار پر هزینه است، بلکه حملات سایبری نیز هزینه‌های بالاتری را برای این سیستم‌ها به همراه دارد [21]. این موضوع به این دلیل است که مهاجمان راهبردهای خود را با راهبردهای تقویت امنیت و محافظت سیستم تطبیق می‌دهند [21]. هزینه‌های بالا برای تولید شبکه‌های سازمانی با امنیت و قابلیت اطمینان بالا و نرم‌افزارهای امن، سیستم‌های سایبر-فیزیکی را در معرض حملات سایبری خطرناک قرار داده است.

سیستم‌های سایبر-فیزیکی از سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری و مبتنی بر امضا برای تشخیص نفوذ مهاجم و رفتار غیرعادی فرآیند فیزیکی استفاده می‌کنند [22 و 23]. کیفیت آن‌ها با دو عامل احتمالات منفی کاذب و مثبت کاذب برآورد می شود. بررسی مستمر این سیستم‌ها برای شناسایی وجود هرگونه حمله در حسگرها، کنترل‌کننده‌ها و محرّک‌ها مورد نیاز است.

ارتباطات اصلی سیستم‌های سایبر-فیزیکی به تبادل داده میان حسگرها، میان حسگرها و کنترل‌کننده ها و میان کنترل‌کننده‌ها تقسیم‌بندی می شود. این سیستم‌ها از درجه‌ای از افزونگی برای این مؤلفه‌های حساس استفاده می‌کنند تا در مواقع ایجاد اختلال در یک مؤلفه، مؤلفه‌های افزونه جایگزین گردند [24].

3. پیشینه پژوهش

در این بخش، برخی از کارهای مرتبط در زمینه مطالعه قابلیت اطمینان و امنیت سیستم‌های سایبر-فیزیکی را مورد بررسی قرار می‌دهیم. لیو و همکاران [25] رویکردی برای مدل انتشار تهدید بین عناصر به عنوان یک بازی بیزی با راهبرد ترکیبی (حمله-دفاع) با اطلاعات ناقص ارائه کرده‌اند. آن‌ها همچنین یک الگوریتم تجزیه و تحلیل مسیر حمله برای سیستم‌های سایبر-فیزیکی ارائه کرده‌اند تا مسیرهای حمله احتمالی با تلفات ویژه را استخراج کنند. از نقاط ضعف این روش، عدم در نظر گرفتن اطلاعات مهمی مانند دانش و مهارت مهاجم در نمایه راهبرد مهاجم است که در مدل بازی سیستم‌های سایبر-فیزیکی باید در نظر گرفته شود تا تحلیل بهتری از امنیت ایجاد گردد.

نویسندگان در [26] روشی را برای ارزیابی مخاطره امنیتی سیستم‌های سایبر-فیزیکی با استفاده از یک بستر آزمایشی برای این سیستم‌ها با کنترل‌کننده‌های صنعتی دنیای واقعی و پروتکل‌های ارتباطی پیشنهاد کرده‌اند. نتایج آزمایش‌ها در این پژوهش نشان می‌دهد که همه حملات نمی‌توانند آسیب فیزیکی ایجاد کنند و توسعه آن زمان‌بر است و ممکن است بتوان در زمان موجود پیامد حمله را خنثی کرد. از جمله نقاط ضعف این روش در نظر نگرفتن ویژگی‌های مهاجم از جمله احتمال حمله و نفوذ است.

بارتو و همکاران [27] روی مخاطرات سایبری، ویژگی‌های آن‌ها و ابزارهای مدیریت مخاطره تمرکز کرده‌اند. علاوه بر این، آن‌ها تجزیه و تحلیل و مقایسه‌ای از مخاطرات سایبری را ارائه کرده‌اند. همچنین مقایسه‌ای بین مخاطرات سایبری سیستم‌های فناوری اطلاعات سنتی و سیستم‌های سایبر-فیزیکی انجام

[17] Human-Machine Interface

داده‌اند. مطالعات آن‌ها نشان داده است که این دو حوزه دارای ویژگی‌های متمایز برای مخاطرات سایبری هستند.

نویسندگان در [28] یک روش زمان طراحی برای تخمین کمّی و کیفی امنیت سیستم‌های سایبر-فیزیکی با استفاده از شبکه‌های پتری تصادفی[18] (**SPN**) ارائه کرده‌اند. این روش همچنین به انتخاب طراحی سیستم ایمن بهینه با تجزیه و تحلیل مدل‌های جایگزین مختلف کمک می‌کند.. در این روش تنها استفاده از سیستم تشخیص نفوذ به عنوان راه کار دفاعی در نظر گرفته شده است.

لالروپویا و همکاران [29] یک مدل بازی تصادفی با مجموع صفر برای ارزیابی امنیت سیستم‌های سایبر-فیزیکی پیشنهاد کرده‌اند. آن‌ها طول عمر سیستم‌های سایبر-فیزیکی مورد حمله را بر اساس زنجیره مارکوف زمان پیوسته[19] (**CTMC**) مطالعه کرده‌اند. فرض شده است که زمان اقامت سیستم در هر حالت از توزیع نمایی پیروی می‌کند. از جمله نقاط ضعف این روش، محدود بودن آن به توزیع نمایی با استفاده از زنجیره مارکوف پیوسته زمان است.

یانگ و همکاران [4] رویکردی برای مدل‌سازی و ارزیابی قابلیت اطمینان سیستم‌های سایبر-فیزیکی با در نظر گرفتن ارتباطات مبتنی بر مدل در دسترس بودن آنی[20] (**IA**) پیشنهاد کرده‌اند. نویسندگان از اصل فرآیند مارکوف برای مدل‌سازی امنیت و قابلیت اطمینان استفاده کرده‌اند. آن‌ها سه نوع حالت سیستم را در رویکرد مدل‌سازی خود در نظر گرفته‌اند که عبارتند از: حالات کار، تعمیر و تعمیر با تأخیر. از جمله نقاط ضعف این مقاله این است که تنها از سنجه دسترس‌پذیری به منظور ارزیابی قابلیت اطمینان استفاده کرده است.

پنگ و همکاران [30] یک مدل عملی برای سیستم‌های سایبر-فیزیکی وابسته به هم با استفاده از نظریه نفوذ شبکه ارائه کرده‌اند. آن‌ها عملکرد قابلیت اطمینان سیستم‌های سایبر-فیزیکی جفت شده را تحت انواع مختلف شبکه بررسی کرده‌اند. آن‌ها همچنین اثر شکست‌های آبشاری را مورد مطالعه قرار داده‌اند و نتایج تحلیلی بررسی آن‌ها انتشار شکست در این سیستم‌ها را نشان می‌دهند. در نهایت، قابلیت اطمینان مدل ارائه شده توسط شکست تصادفی با محاسبه اندازه عناصر عملکرد غول پیکر[21] در سیستم‌های سایبر-فیزیکی وابسته به هم تخمین زده شده است. تمرکز اصلی این مقاله بر روی شکست‌های تصادفی است که بر روی گره‌های مختلف سیستم‌ها اتفاق می‌افتد و نه حملات سایبری.

پریادرشینی و همکاران [31] چارچوب جدیدی را با در نظر گرفتن امنیت-حریم خصوصی برای سیستم‌های سایبر- فیزیکی پزشکی[22] (**MCPS**) ارائه کرده‌اند. چارچوب پیشنهادی آن‌ها مدل‌های متعددی را برای به تصویر کشیدن حوزه‌های مختلف امنیت در بر می‌گیرد. آن‌ها در نهایت یک ارزیابی کیفی از چارچوب ارائه کرده‌اند. این مدل صرفاً به دلیل مؤلفه‌های به کار گرفته شده، در سیستم‌های سایبر-فیزیکی پزشکی کاربرد دارد.

نویسندگان در [32] روشی را برای مدل‌سازی بقاپذیری شبکه در سیستم‌های سایبر-فیزیکی پیشنهاد کرده‌اند. آن‌ها یک مدل مهاجم-مدافع مبتنی بر بازی ارائه کرده‌اند تا رهیافت حمله-دفاع مناسبی را برای ارائه پاسخ مناسب به حوادث امنیت سایبری اتخاذ کنند. در واقع روش ارائه شده برای مدیریت بحران در سیستم‌های سایبر-فیزیکی قابل بکارگیری است.

در پژوهش اخیر، از نظریه بازی برای مدل‌سازی امنیت سیستم‌های سایبر-فیزیکی با پارامترهای خاص استفاده کردیم [33 و 34]. بازی‌های دونفره‌ای که تقابل بین مهاجم و سیستم را در مرحله نفوذ و اقدام به حمله مهاجم با هدف ایجاد خرابی فیزیکی مدل‌سازی می‌کند. همچنین، روشی را برای تخمین انتشار پیامد حملات امنیتی علیه سیستم‌های سایبر-فیزیکی پیشنهاد کردیم [20]. در این روش به اولویت‌بندی مؤلفه‌های حساس سیستم بر اساس پیامد حملات و میزان انتشار پیامد حملات پرداخته شده است.

همچنین در [35] روشی را به منظور مدل‌سازی و ارزیابی امنیت سیستم‌های سایبر-فیزیکی با استفاده از نظریه بازی‌های

[18] Stochastic Petri Nets

[19] Continious time Markov Chain

[20] Instantaneous availability

[21] Giant

[22] Medical CPS

بیزی با اطلاعات ناقص ارائه کردیم. بازی دو نفره‌ای که مهاجم و سیستم اطلاعات کاملی از یکدیگر ندارند و تصمیمات آن‌ها بر اساس اطلاعات ناکامل انجام می‌شود.

به طور خلاصه، پژوهش‌های ارائه شده دارای مشکلات و نقاط ضعفی زیر هستند:

- استفاده از توزیع خاص نمایی در مدل،
- عدم استفاده از نمایه[23] مهاجم در بعضی روش‌ها،
- استفاده از سیستم تشخیص نفوذ به عنوان تنهای راهکار دفاعی
- عدم بررسی استفاده از افزونگی که در سیستم‌های سایبر-فیزیکی برای کارکرد پیوسته سیستم بسیار حیاتی است،
- تمرکز بر روی خرابی‌های تصادفی
- مناسب بودن برای دسته خاصی از سیستم‌ها

در مقایسه با پژوهش‌های پیشین، در این مقاله، راهبرد دفاعی سیستم بجز سیستم تشخیص نفوذ، استفاده از مؤلفه‌های افزونه است که در پژوهش‌های ذکر شده در نظر گرفته نشده بود. در این روش فرض شده است سیستم به منظور ارتقای دسترس‌پذیری، از مؤلفه‌های افزونه برای حسگرها، کنترل‌کننده‌ها و محرّک ها استفاده می‌کند. همچنین به منظور کشف رفتار نادرست سیستم بر اثر حمله امنیتی، از سیستم تشخیص نفوذ در مؤلفه‌های حساس بهره می‌برد. در واقع، جنبه متمایز این روش نسبت به پژوهش‌های پیشین مدل‌سازی رفتار سیستم و مهاجم با وجود این اقدامات دفاعی ذکر شده و مطالعه پارامترهای حسّاس و مهم تأثیرگذار در قابلیت اطمینان و امنیت این سیستم‌ها از جمله، بازه زمانی تشخیص حمله، بازه زمانی حمله و نفوذ، احتمال حمله و کشف آن، و ضریب افرونگی است که نسبت به پژوهش‌های بیان شده متمایز است.

4. روش پیشنهادی

در این بخش به توصیف روش مدل‌سازی پیشنهادی، پارامترهای مدل، سنجه‌های در نظر گرفته شده و نحوه ارزیابی سنجه‌ها می‌پردازیم.

4-1. توصیف روش پیشنهادی

همانطور که ذکر شد، سیستم‌های سایبر-فیزیکی از مجموعه‌ای از حلقه‌های کنترلی ساده و پیچیده تشکیل می‌شوند. به علاوه مؤلفه‌های اصلی این سیستم حسگرها، کنترل‌کننده‌ها و محرّک ها هستند. همچنین همانطور که اشاره شد، ارتباطات اصلی سیستم‌های سایبر-فیزیکی هم به تبادل داده میان حسگرها، میان حسگرها و کنترل‌کننده‌ها و میان کنترل‌کننده‌ها تقسیم‌بندی می‌شود. فرض شده است که این سیستم‌ها از درجه‌ای از افزونگی برای این مؤلفه‌های حساس استفاده می‌کنند تا در مواقع ایجاد اختلال در یک مؤلفه، مؤلفه‌های افزونه جایگزین گردند. مدل ارائه شده بر اساس رویکردهای مدل‌سازی شبه مارکوف برای توصیف سیستم و رفتارهای مهاجم و همچنین برخی اقدامات متقابل در نظر گرفته شده است. توزیع زمان اقامت در حالت‌های مختلف سیستم با استفاده از مدل‌های شبه مارکوفی انعطاف‌پذیرتر خواهد بود و به توزیع نمایی محدود نمی‌شود، و این موضوع دلیل انتخاب مدل شبه مارکوفی به منظور مدل‌سازی در این مقاله است.

هر حالت در مدل پیشنهادی دارای نمایش (i, j, k) است که در آن i تعداد مؤلفه‌های حسگر سالم، j تعداد مؤلفه‌های کنترل‌کننده سالم و k تعداد مؤلفه‌های محرّک سالم است. حالت اولیه سیستم حالت عادی است که در آن همه مؤلفه‌ها به خوبی کار می‌کنند و مهاجم هنوز نتوانسته مؤلفه‌ای را مورد هدف قرار دهد. مهاجم سعی می‌کند با استفاده از مراحل برنامه‌ریزی شده و شناخت حاصل شده از سیستم، به سیستم نفوذ کند تا بتواند دسترسی لازم برای راه اندازی حمله به مؤلفه‌ها را بدست آورد. هدف او از این کار معمولاً ایجاد اختلال در رفتار سیستم یا ایجاد خرابی فیزیکی است.

مهاجم در ابتدا سعی می‌کند که با نفوذ به سیستم دسترسی لازم برای ایجاد اختلال فیزیکی در سیستم را بوجود آورد. از این رو، مهاجم ممکن است در نفوذ به سیستم موفق نباشد. در این صورت، سیستم در حالت عادی اولیه خود باقی می‌ماند. به علاوه، نفوذ نفوذگر نیز ممکن است توسط سیستم شناسایی گردد.

[23] Profile

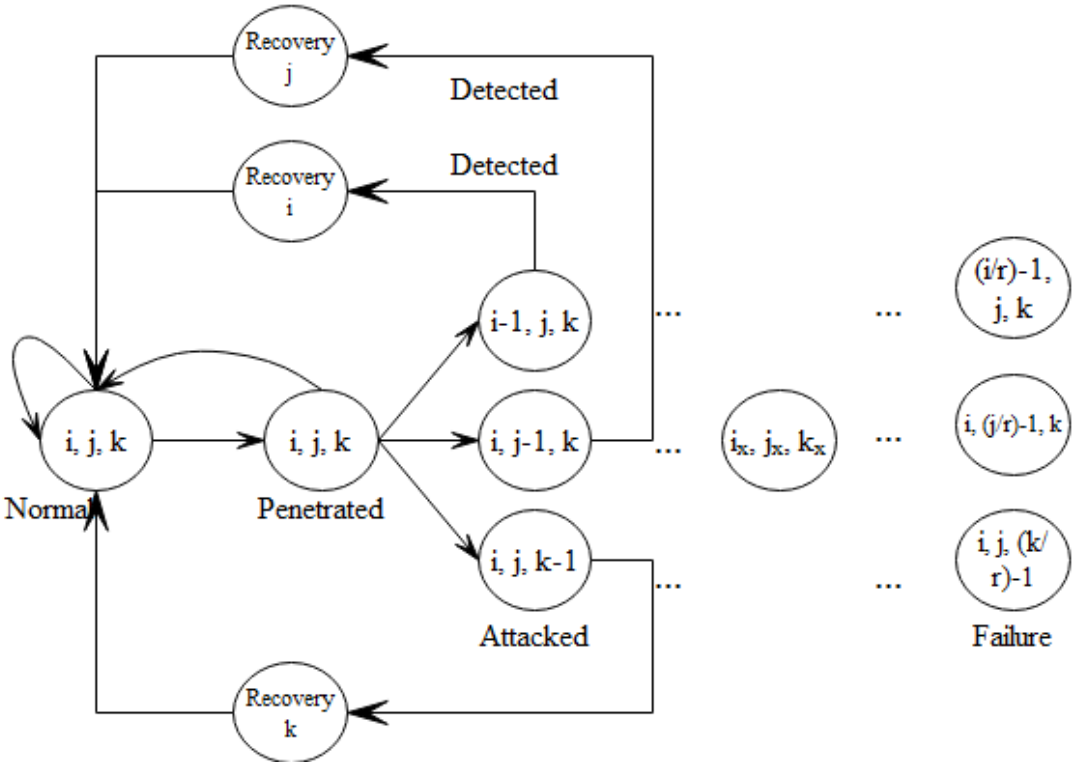
هنگامی که مهاجم به سیستم نفوذ می‌کند، چندین رویداد را می‌توان در نظر گرفت. اولین رویداد این است که مهاجم یک مؤلفه شامل یک حسگر، یک کنترل کننده یا یک محرّک را به خطر بیاندازد. هنگامی که یک مؤلفه توسط مهاجم در معرض حمله قرار می‌گیرد، تعداد مؤلفه‌های سالم از آن دسته کاهش می‌یابند. همچنین فرض شده است مهاجم در هر مرحله یک گره را تحت تأثیر قرار می‌دهد. به عنوان مثال، با به خطر انداختن یک مؤلفه حسگر، حالت بعدی (**i-1, j, k**) است. به طور مشابه، برای هدف قرار دادن یک کنترل کننده و یک محرّک به ترتیب خواهیم داشت: (**i, j-1, k**) و (**i, j, k-1**).

سیستم تشخیص نفوذ در بازه زمانی مشخصی مؤلفه‌های اصلی سیستم که حسگرها، کنترل‌کننده‌ها و محرّک ها هستند را از نظر وجود حملات مورد بررسی قرار می‌دهد. با انجام حمله موفق توسط مهاجم، ممکن است سیستم تشخیص نفوذ به درستی یک مؤلفه خراب شده را شناسایی کند. در این صورت، سیستم به یک زمان مشخص به منظور انجام بازیابی مؤلفه به حالت عادی اولیه نیاز دارد که این زمان از یک متغیر تصادفی با یک تابع توزیع عمومی پیروی می‌کند. همچنین فرض شده است در صورت کشف حمله به یک مؤلفه، آن مؤلفه بازیابی شده و به حالت سالم اولیه باز خواهد گشت.

آخرین رویداد خرابی سیستم است. پس از اینکه یک مؤلفه و تمام مؤلفه اضافی آن به خطر بیفتند، سیستم وارد حالت خرابی می‌شود. برای هر دسته مؤلفه، ضریب افزونگی (**x**) به عنوان یک پارامتر طراحی مهم استفاده می‌شود. حالت خرابی سیستم با در نظر گرفتن R_i به عنوان ضریب افزونگی حسگرها، R_j برای کنترل‌کننده‌ها و R_k برای محرّک‌ها، حالت‌های خرابی سیستم یکی از حالت‌های زیر خواهد بود:

$\left(\frac{i}{R_i}-1,j,k\right),\left(i,\frac{j}{R_j}-1,k\right),$ $\left(i,j,\frac{k}{R_k}-1\right)$	(1)

شکل 2، شمای کلّی از مدل پیشنهادی را نشان می‌دهد. همانطور که این شکل نشان می‌دهد، حالت اولیه سیستم حالت عادی (**Normal**) است. مهاجم پس از سوء استفاده از آسیب‌پذیری‌های سیستم به دسترسی دست پیدا می‌کند که بتواند اقدام به آغاز حمله به مولفه‌های حساس ذکر شده نماید که حالت نفوذ شده یا **(Penetrated)** نام دارد.



شکل 2. مدل شبه مارکوفی پیشنهادی.

پس از انجام حمله به یک مؤلفه از سه دسته مؤلفه حسگرها، کنترل‌کننده‌ها و یا محرّک ها، حالت سیستم یه یکی از سه حالت حمله شده (**Attacked**) که در شکل مشخص است وارد می‌شود. در صورت تشخیص حمله به یک مؤلفه حسگر، کنترل کننده و یا محرّک، به ترتیب سیستم از حالت جاری به حالت‌های ترمیم **(Recovery *i*, Recovery *j*, Recovery *k*)** وارد می‌شود.

نهایتاً حالت‌های (***i*/*r* -1, *j*, *k***)، (***i*, *j*/*r* -1, k**) و (***i*, *j*, *k*/*r* -1**) با فرض r به عنوان ضریب افزونگی، حالت‌هایی هستند که سیستم به ترتیب به دلیل خرابی مؤلفه‌های حسگر، کنترل‌کننده و محرّک قادر به ادامه کارکرد خود نخواهد بود و متوقف شده است (**Failure**).

شکل 3 همچنین وضعیت یک حالت میانی مدل پیشنهادی را به تصویر می‌کشد. همانطور که در این شکل مشخص است، حالت بعدی سیستم در یک حالت میانی یا وقوع یک حمله به یکی از مؤلفه‌ها خواهد بود و یا تشخیص حمله به یکی از مؤلفه‌هایی که مورد حمله واقع شده است.

2-4. پارامتردهی مدل پیشنهادی

جدول 1 لیست پارامترهای مدل و تعریف آن‌ها را ارائه کرده است.

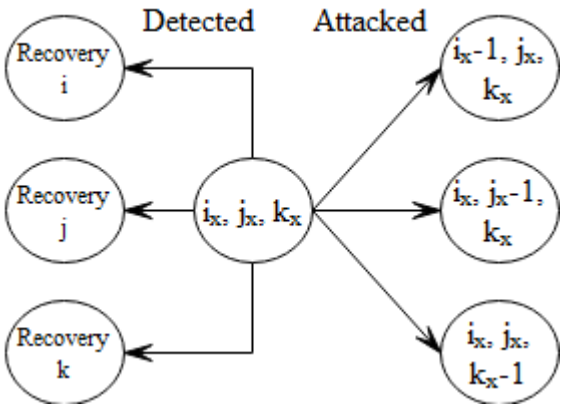
اکنون به توصیف فرآیند پارامتردهی مدل می‌پردازیم. فرض کنید λ_T نرخ گذار انتقال T در مدل ارائه شده باشد. با در نظر گرفتن پارامترهای تعریف شده می‌توان نرخ نفوذ مهاجمان به سیستم (λ_p) را به صورت زیر تخمین زد:

$$\lambda_p = Pp / Tp \qquad (2)$$

نرخ انجام حمله به مولفه i پس از نفوذ (λ_a) را می‌توان با استفاده از فرمول زیر بدست آورد:

$$\lambda_a = \frac{(g_i \times P_a)}{T_a} \qquad (3)$$

که در آن g_i تعداد مؤلفه‌های سالم از نوع i است.



شکل 3. یک حالت میانی در مدل پیشنهادی.

جدول 1. لیست پارامترهای مدل پیشنهادی

پارامتر	توصیف
P_i	احتمال نفوذ مهاجم به سیستم.
P_d	احتمال تشخیص حملات در مرحله نفوذ
T_p	بازه زمانی نفوذ مهاجم.
T_d	بازه زمانی کشف نفوذ نفوذ سیستم.
T_r	بازه زمانی بازیابی سیستم بعد از کشف حمله.
P_a	احتمال حمله به مؤلفه‌های حسگر، کنترل‌کننده و محرّک.
T_a	بازه زمانی حمله به یک حسگر، کنترل کننده یا محرّک.
R_i	ضریب افزونگی حسگرها، کنترل‌کننده‌ها و محرّک‌ها.

نرخ انتقال برای تشخیص مؤلفه‌های خراب‌شده (λ_d) را می‌توان به صورت زیر محاسبه کرد:

$$\lambda_d = \sum_i \frac{(b_i \times P_d)}{T_d} \qquad (4)$$

که در آن، b_i مؤلفه‌های خراب‌شده از نوع i است. در واقع فرض شده است که با کشف حمله بر روی هر یک از مؤلفه‌های سیستم، بعد از مدت زمان ترمیم سیستم به حالت نرمال اولیه باز خواهد گشت.

نرخ تشخیص نفوذ در مرحله نفوذ مهاجم ($\boldsymbol{\lambda_{dp}}$) را می‌توان به صورت زیر تخمین زد:

$$\boldsymbol{\lambda_{dp}} = \frac{\boldsymbol{1-Pp}}{\boldsymbol{Tp}} + \frac{\boldsymbol{Pdp}}{\boldsymbol{Tdp}} \quad (5)$$

در نهایت، نرخ انتقال خروج از حمله توسط مهاجم ($\boldsymbol{\lambda_w}$) را می‌توان به صورت زیر محاسبه کرد:

$$\boldsymbol{\lambda_w} = \frac{\boldsymbol{(1-P_a)}}{\boldsymbol{T_a}} \quad (6)$$

3-4. سنجه‌های کمّی

در این بخش در مورد سنجه‌های در نظر گرفته شده به منظور ارزیابی قابلیت اطمینان سیستم‌های سایبر-فیزیکی با بهره‌برداری از روش مدل‌سازی پیشنهاد شده بحث می‌کنیم. سنجه در نظر گرفته شده میانگین زمان تا خرابی سیستم ($MTTF$) با در نظر گفتن تعریف ذکر شده از خرابی سیستم است. این سنجه مقدار زمان مورد انتظار مهاجمان برای ورود آسیب یا ایجاد اختلال فیزیکی در یک فرآیند فیزیکی تعریف می‌شود [36]. به عبارت دیگر، این سنجه مقدار زمانی مورد انتظار است که سیستم قبل از رسیدن به حالت‌های جذب (شکست) در حالت‌های میانی قرار می‌گیرد. این سنجه را می‌توان با استفاده از فرمول زیر اندازه گیری کرد [37، 38]:

$$\boldsymbol{MTTF} = \sum_{\boldsymbol{i\in S}} \boldsymbol{V_i S_i} \quad (7)$$

که در آن V_i میانگین تعداد دفعاتی است که مدل قبل از رسیدن به یکی از حالت‌های جذب در حالت گذرا i می‌ماند و S_i میانگین زمان اقامت مدل در حالت i است. پارامترهای تعداد بازدید (V_i) را می‌توان با استفاده از معادله زیر محاسبه کرد [38، 39]:

$$\boldsymbol{V_i} = \boldsymbol{q_i} + \sum_{\boldsymbol{j\in M}} \boldsymbol{V_{ji}} \quad (8)$$

که در آن M مجموعه‌ای از حالت‌هایی است که از حالت i در مدل شبه مارکوف قابل دستیابی هستند، که در آن q_1 برابر با 1 است.

برای محاسبه میانگین زمان اقامت در حالت i، باید نرخ و احتمال انتقال خروجی از حالت i را تخمین بزنیم. میانگین زمان اقامت در حالت S_i می‌توان به صورت زیر تخمین زد [37، 38]:

$$\boldsymbol{S_i} = (\sum_{\boldsymbol{k\in M}} \boldsymbol{R_{ik}})^{-1} \quad (9)$$

که در آن R_{ij} نرخ گذار بین حالت i و حالت j است.

دسترس‌پذیری: دسترس‌پذیری احتمال در دسترس بودن سیستم در لحظه زمانی t برای ارائه سرویس درست است. برای تخمین این سنجه، نیاز است که رفتار سیستم در حالت پایدار مطالعه شود. به این معنا که همه حالت‌های مدل باید به صورت گذرا در نظر گرفته شوند. در نتیجه گذری از حالت خرابی به حالت عادی اولیه در نظر گرفته می‌شود. فرض می‌شود که T_f زمان مورد نیاز برای برگرداندن سیستم به حالت عادی اولیه باشد. بر این اساس، دسترس‌پذیری یک سیستم سایبر-فیزیکی به صورت زیر قابل محاسبه است:

$$\boldsymbol{A} = \boldsymbol{1-\pi_F} \quad (10)$$

که $\boldsymbol{\pi_F}$ احتمال بودن سیستم در حالت خرابی است.

از آنجا که مدل حاصل یک مدل شبه مارکوف است، احتمالات حالت پایدار آن بر حسب میانگین زمان اقامت و احتمالات حالت پایدار زنجیره مارکوف گسسته زمان نهفته آن به صورت زیر محاسبه می‌شود [37]:

$$\boldsymbol{\pi_i} = \frac{\boldsymbol{q_i h_i}}{\boldsymbol{\sum_j q_j h_j}} \quad (11)$$

که در آن احتمالات حالت پایدار زنجیره مارکوف گسسته زمان نهفته به صورت زیر محاسبه می‌شود [37]:

$$\boldsymbol{q} = \boldsymbol{q}.\boldsymbol{P} \quad (12)$$

که $\boldsymbol{P}$ ماتریس احتمال گذر است.

5. یک مثال

به عنوان مطالعه موردی، یک سیستم سایبر- فیزیکی فرضی را در نظر می‌گیرم که شامل دو مؤلفه حسگر با ضریب افزونگی

$R_i = 2$، دو کنترل کننده با ضریب افزونگی $R_j = 1$ و دو محرّک با ضریب افزونگی $R_k = 1$ است.

سناریوهای مختلفی برای حمله برای این سیستم قابل تصور است. شکل 4 مدل شبه مارکوفی اولین سناریوی حمله را نشان می‌دهد که در آن مهاجم مؤلفه‌های حسگر را هدف قرار می‌دهد. حالت امن اولیه (2، 2، 4) است. همانطور که قبلاً توضیح داده شد، سیستم زمانی وارد حالت خرابی می‌شود که تعداد قطعات با نوع جزء i کمتر از حداقل باشد (2، 2، 2): به ترتیب برای حسگرها، کنترل‌کننده‌ها و محرّک‌ها. بنابراین، حالت (2، 2، 1) حالت خرابی سیستم است.

سناریوی حمله دوم در شکل 5 نشان داده شده است. در این سناریو، مهاجم یک حسگر و سپس یک کنترل‌کننده را مورد هدف قرار می‌دهد. در این حالت، حالت (2، 1، 3) حالت خرابی است که در آن تعداد کنترل کننده کمتر از حداقل مورد نیاز برای قرار گرفتن سیستم در حالت فعّال است.

به عنوان سناریوی سوم و برای هدف ترکیب، وضعیتی را در نظر می‌گیریم که در آن ضریب افزونگی همه اجزا برابر با یک باشد. به منظور داشتن یک ترکیب منصفانه، فرض بر این است که مهاجم اجزای حسگر را در این سناریو هدف قرار می‌دهد. در این حالت، حالت (2، 2، 1) حالت خرابی سیستم خواهد بود.

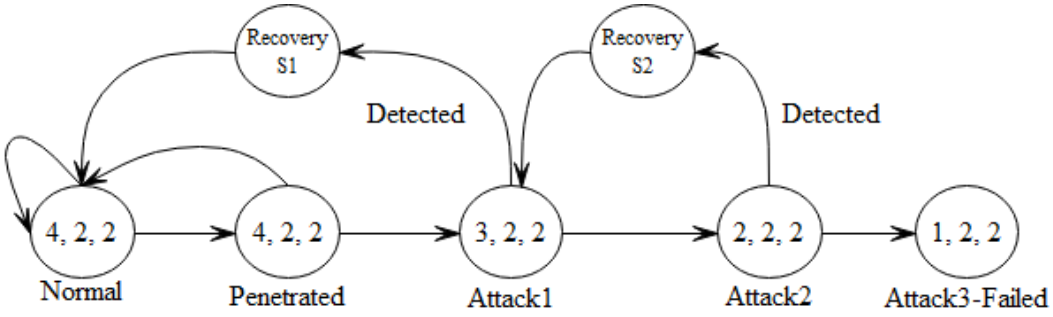
اولین سناریوی حمله به عنوان سناریوی اصلی در این مثال در نظر گرفته شده است. جدول 2 تمام پارامترهای تعریف شده مدل و مقادیر آن‌ها را فهرست می‌کند. هنگام مطالعه تأثیر یک پارامتر، مقادیر پیش فرض به پارامترهای دیگر اختصاص داده می‌شود. تمامی تحلیل‌های انجام شده در این مثال توسط با متلب شبیه‌سازی شده است.

بررسی اثر احتمال حمله: با در نظر گرفتن سه مقدار مختلف برای احتمال انجام حمله مهاجم به پارامتر احتمال حمله و ثابت بودن مقادیر سایر پارامترها، این بررسی صورت گرفته است. همانطور که در شکل 6 و 7 نشان داده شده است، با افزایش احتمال حمله، **MTTF** و میزان دسترس‌پذیری به طور قابل توجهی کاهش می‌یابند. این موضوع به این دلیل است که با افزایش احتمال حمله زمان اقامت سیستم در حالت نرمال کاهش می‌یابد و با احتمال بیشتری به حالت حمله شده وارد می‌شود.

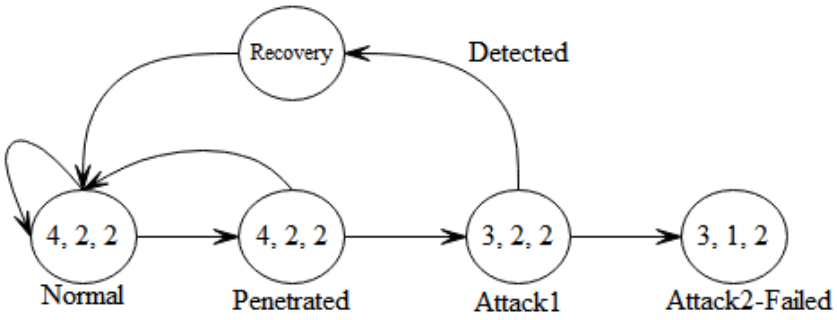
بررسی اثر احتمال تشخیص حمله: در این مطالعه، سه مقدار مختلف به پارامتر احتمال تشخیص حمله اختصاص داده شده است. همانطور که در شکل 8 و 9 نشان داده شده است، افزایش احتمال تشخیص حمله می‌تواند **MTTF** و دسترس‌پذیری سیستم را افزایش دهد. در واقع با افزایش احتمال تشخیص حمله، سیستم با احتمال بیشتری در حالت های میانی گذار و در حال کارکرد باقی می‌ماند.

بررسی اثر مدت زمان نفوذ: اکنون بررسی می‌کنیم که چگونه بازه زمانی نفوذ مهاجم می‌تواند بر **MTTF** و دسترس‌پذیری سیستم تأثیر بگذارد. برای انجام این بررسی، سه آزمایش با اختصاص سه مقدار مختلف به پارامترهای بازه زمانی نفوذ و ثابت بودن مقادیر سایر پارامترها انجام شده است. همانطور که در شکل 10 و 11 نشان داده شده است، افزایش بازه زمانی نفوذ منجر به افزایش **MTTF** و دسترس‌پذیری سیستم خواهد شد. در واقع با افزایش بازه زمانی نفوذ، سیستم مدت زمان بیشتری در حالت‌های میانی و در حال کارکرد باقی می‌ماند و در نتیجه **MTTF** و دسترس‌پذیری افزایش پیدا می‌کند.

بررسی اثر بازه زمانی حمله: شکل 12 و 13 به ترتیب اثر بازه زمانی حمله بعد از نفوذ مهاجم بر **MTTF** و دسترس‌پذیری سیستم را نشان می‌دهد. همانطور که انتظار می‌رود، افزایش بازه زمانی وقوع حمله می‌تواند **MTTF** و دسترس‌پذیری سیستم را افزایش دهد. در واقع با افزایش بازه زمانی حمله، سیستم مدت زمان بیشتری در حال کار باقی می‌ماند و در نتیجه **MTTF** و دسترس‌پذیری افزایش پیدا می‌کند.



شکل4. سناریو حمله اول در مثال.



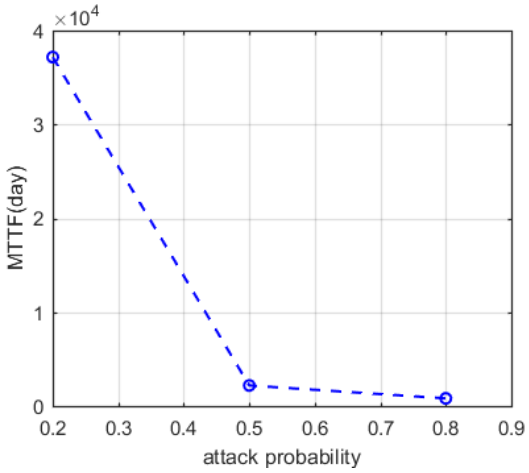
شکل 5. سناریو حمله دوم در مثال.

جدول 2. لیست پارامترهای مدل و مقادیر

پارامتر	مقدار پیشفرض	بازه مقادیر
P_i	0,3	[0,3 و 0,3]
P_d	0,8	[0,8 و 0,2]
T_p	0,9	[0,9 و 0,2]
T_d	30 روز	[40 و 10]
T_r	2 روز	[10 و 2]
P_a	0,5 روز	[10 و 0,5]
T_a	1 روز	[1 و 1]

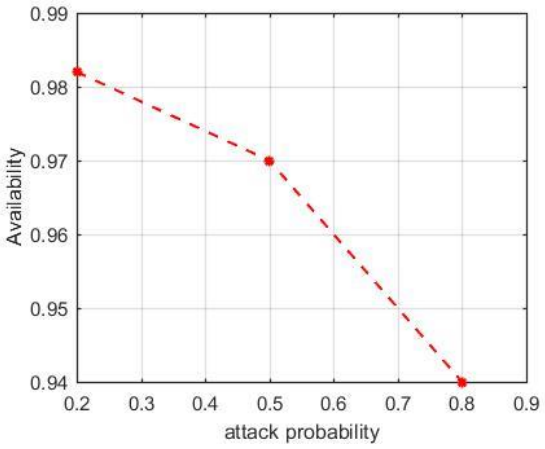
بررسی اثر بازه زمانی کشف حمله: شکل 14 و 15 به ترتیب اثر بازه زمانی کشف حمله بر **MTTF** و دسترس‌پذیری سیستم را نشان می‌دهند. با اختصاص سه مقدار مختلف به بازه زمانی کشف حمله و ثابت بودن مقادیر سایر پارامترها این آزمایش انجام شده است. همانطور که نتایج بررسی نشان می‌دهد، **MTTF** و دسترس‌پذیری سیستم با افزایش بازه زمانی کشف حمله کاهش می‌یابد. در واقع با افزایش بازه زمانی کشف حمله، امکان اینکه سیستم قبل از کشف حمله دچار اختلال و خرابی شود بیشتر خواهد بود.

بررسی اثر ضریب افزونگی: در این آزمایش شرایطی که سیستم از افزونگی استفاده کرده است را با شرایطی که بدون مؤلفه افزونه بوده است را مقایسه می‌کنیم. می‌خواهیم سناریوهای حمله اول و سوم را با هم مقایسه کنیم که در آن ضریب افزونگی برای گره حسگر به ترتیب دو و یک است.

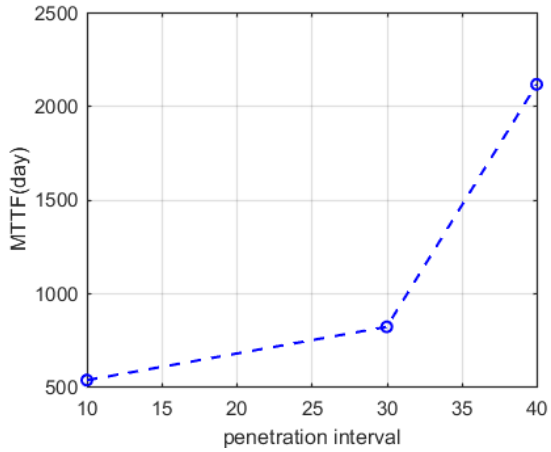


شکل 6. اثر احتمال حمله بر میانگین زمان تا خرابی.

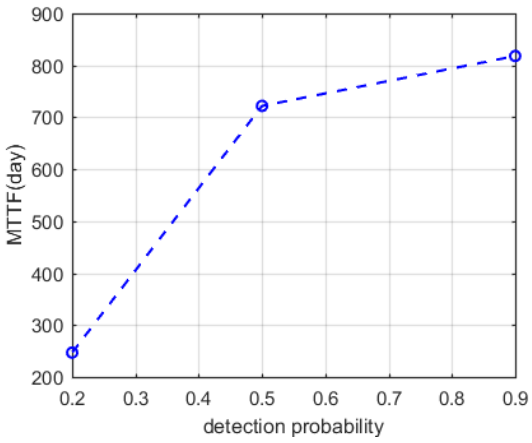
فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال ششم ، شمارهٔ یک، بهار1401



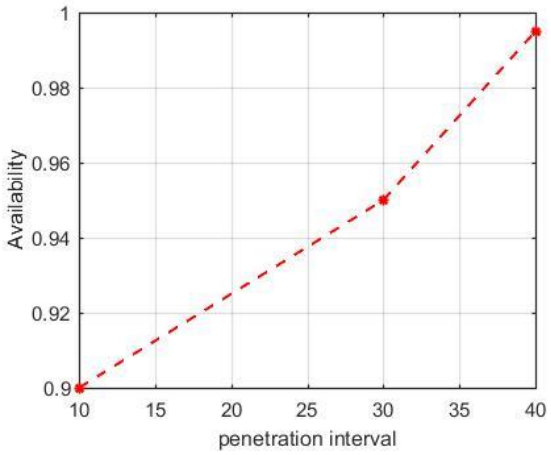
شکل 7. اثر احتمال حمله بر دسترس‌پذیری.



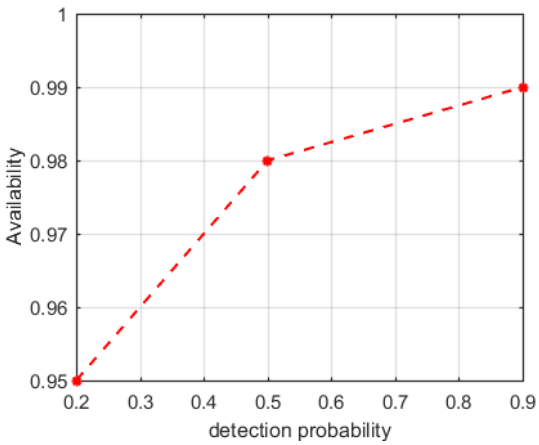
شکل 10. اثر بازه زمانی نفوذ بر میانگین زمان تا خرابی.



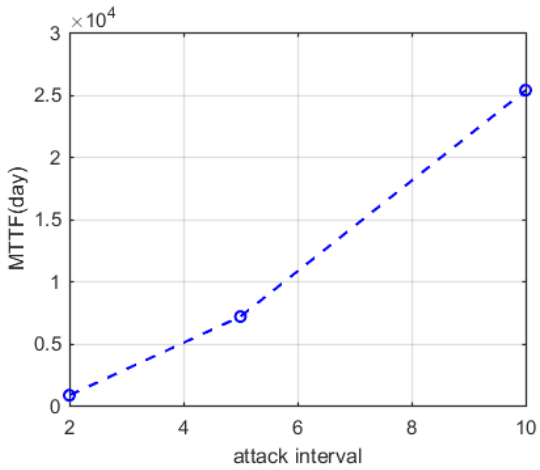
شکل8. اثر احتمال کشف بر میانگین زمان تا خرابی.



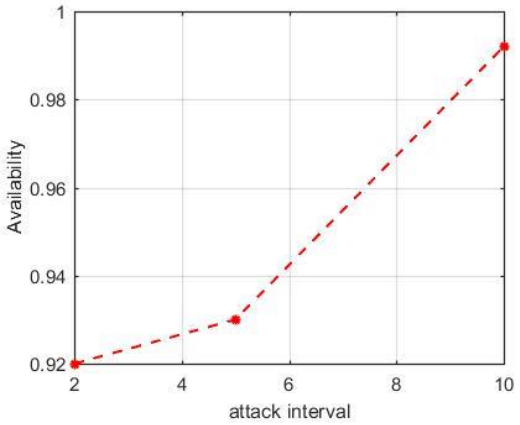
شکل 11. اثر بازه زمانی کشف حمله بر دسترس‌پذیری.



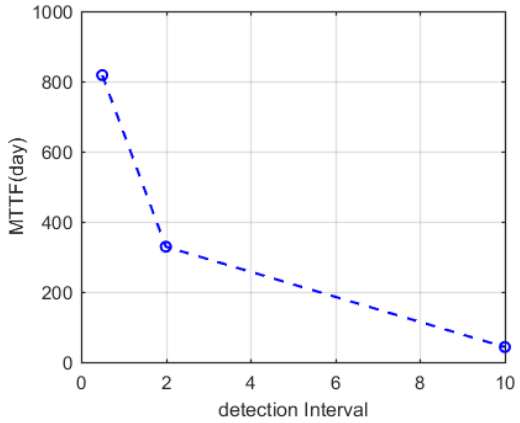
شکل 9. اثر احتمال کشف بر دسترس‌پذیری.



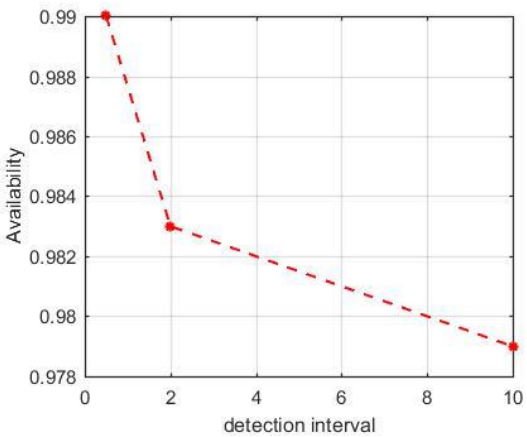
شکل 12. اثر بازه زمانی حمله بر میانگین زمان تا خرابی.



شکل 13. اثر احتمال حمله بر دسترس‌پذیری.

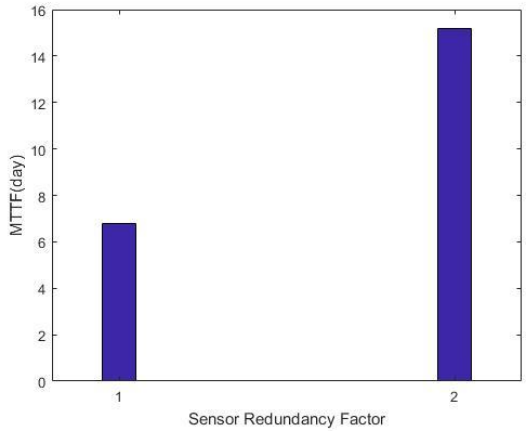


شکل 14. اثر بازه زمانی کشف بر میانگین زمان تا خرابی.

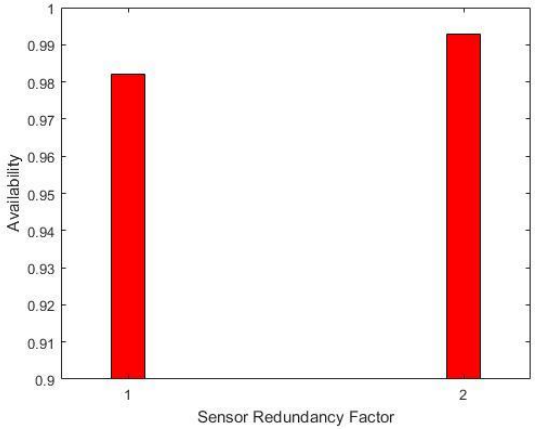


شکل 15. اثر بازه زمانی کشف حمله بر دسترس‌پذیری.

به منظور بررسی بهتر اثر افزونگی، مرحله نفوذ در این آزمایش نادیده گرفته شده است. همانطور که در شکل 16 و 17 قابل مشاهده است، **MTTF** و دسترس‌پذیری سیستم برای ضریب افزونگی حسگر برابر دو بسیار بیشتر از ضریب افزونگی حسگر برابر یک است.



شکل 16. اثر افزونگی بر میانگین زمان تا خرابی.



شکل 17. اثر افزونگی بر دسترس‌پذیری.

6. نتایج

در این مقاله روشی برای ارزیابی قابلیت اطمینان سیستم های سایبر-فیزیکی در برابر حملات سایبری ارائه شد. با استفاده از روش پیشنهادی، امکان مطالعه و بررسی تأثیر مؤلفه‌های افزونه حسگر، کنترل‌کننده و محرّک بر قابلیت اطمینان سیستم امکان‌پذیر خواهد بود. همچنین امکان بررسی اینکه استفاده از مؤلفه‌های افزونه در کدام گره‌های سیستم اولویت بالاتری دارد و میزان دسترس‌پذیری سیستم را افزایش می‌دهد امکان پذیر خواهد بود. همچنین، با استفاده از روش پیشنهادی به بررسی تأثیر برخی پارامترهای مهم بر قابلیت اطمینان سیستم‌های سایبر-فیزیکی از جمله احتمال نفوذ، احتمال حمله، احتمال تشخیص حمله، بازه زمانی تشخیص نفوذ، بازه زمانی حمله و نفوذ و ضریب افزونگی مؤلفه‌های سیستم پرداخته شد. نتایج بررسی‌ها نشان می‌دهند که استفاده از مؤلفه‌های افزونه، بازه زمانی کشف

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال ششم ، شمارهٔ یک، بهار 1401

حمله، بازه زمانی حمله و احتمال حمله و کشف آن تأثیر بسزایی در امنیت و قابلیت اطمینان سیستم‌های سایبر-فیزیکی دارند. یکی از مواردی که در استفاده از مؤلفه‌های افزونه باید در نظر گرفته شود ایجاد توازن بین کارآمدی و هزینه است. به عنوان کار آینده قصد داریم به این موضوع بپردازیم. همچنین به مدل‌سازی و ارزیابی امنیت سیستم‌های سایبر-فیزیکی با مدل کردن حملات جلوگیری از سرویس و یکپارچگی داده‌های حسگری و کنترلی خواهیم پرداخت.

7. مراجع

[1] Hu F. (2013), Cyber-Physical Systems: Integrated Computing and Engineering Design, CRC Press.

[2] Goyal D., Balamurugan S., Senthilnathan K., Annapoorani I., Israr M. (2022), Cyber-Physical Systems and Industry 4.0: Practical Applications and Security Management, Apple Academic Press.

[3] Pivoto, D. G., de Almeida, L. F., da Rosa Righi, R., Rodrigues, J. J., Lugli, A. B., & Alberti, A. M. (2021). Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. *Journal of manufacturing systems*, *58*, 176-192.

[4] Yang, Y., Wang, S., Wen, M., & Xu, W. (2021). Reliability modeling and evaluation of cyber-physical system (CPS) considering communication failures. *Journal of the Franklin Institute*, *358*(1), 1-16.

[5] Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, 107094.

[6] Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. *Computers & security*, *77*, 262-276.

[7] Priyadarshini, I., Kumar, R., Tuan, L. M., Son, L. H., Long, H. V., Sharma, R., & Rai, S. (2021). A new enhanced cyber security framework for medical cyber physical systems. *SICS Software-Intensive Cyber-Physical Systems*, *35*(3), 159-183.

[8] Monisha, K., & Rajasekhara Babu, M. (2019). A novel framework for healthcare monitoring system through cyber-physical system. In *Internet of things and personalized healthcare systems* (pp. 21-36). Springer, Singapore.

[9] Celdrán, A. H., Pérez, M. G., Clemente, F. J. G., & Pérez, G. M. (2018). Sustainable securing of medical cyber-physical systems for the healthcare of the future. *Sustainable Computing: Informatics and Systems*, *19*, 138-146.

[10] Ding, D., Han, Q. L., Xiang, Y., Ge, X., & Zhang, X. M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, *275*, 1674-1683.

[11] O'donovan, P., Gallagher, C., Bruton, K., & O'Sullivan, D. T. (2018). A fog computing industrial cyber-physical system for embedded low-latency machine learning Industry 4.0 applications. *Manufacturing letters*, *15*, 139-142.

[12] Mishra, V. K., Palleti, V. R., & Mathur, A. (2019). A modeling framework for critical infrastructure and its application in detecting cyber-attacks on a water distribution system. *International Journal of Critical Infrastructure Protection*, *26*, 100298.

[13] Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, *100*, 212-223.

[14] Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems*, *77*, 103201.

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

[16] Krotofil, M., & Larsen, J. (2014, August). Are you threatening my hazards?. In *International Workshop on Security* (pp. 17-32). Springer, Cham.

[17] Krotofil, M., Cardenas, A., Larsen, J., & Gollmann, D. (2014). Vulnerabilities of cyber-physical systems to stale data—Determining the optimal time to launch attacks. *International journal of critical infrastructure protection*, *7*(4), 213-232.

[18] Krotofil, M., & Cárdenas, A. A. (2013, October). Resilience of process control systems to cyber-physical attacks. In *Nordic Conference on Secure IT Systems* (pp. 166-182). Springer, Berlin, Heidelberg.

[19] Teixeira, A. M. (2021). Security Metrics for Control Systems. In *Safety, Security and Privacy for Cyber-Physical Systems* (pp. 99-121). Springer, Cham.

[20] Orojloo, H., & Azgomi, M. A. (2017). A method for evaluating the consequence propagation of security attacks in cyber–physical systems. *Future Generation Computer Systems*, *67*, 57-71.

[21] Barreto, C., Schwartz, G., & Cardenas, A. A. (2021). Cyber-Risk: Cyber-Physical Systems Versus Information Technology Systems. In *Safety, Security and*

cyber physical systems. *Mobile Networks and Applications*, *26*(4), 1532-1542.

[31] Ravishankar, M., Stephan, T., & Perumal, T. (2021). Time dependent network resource optimization in cyber–physical systems using game theory. *Computer Communications*, *176*, 1-12.

[32] Priyadarshini, I., Kumar, R., Tuan, L. M., Son, L. H., Long, H. V., Sharma, R., & Rai, S. (2021). A new enhanced cyber security framework for medical cyber physical systems. *SICS Software-Intensive Cyber-Physical Systems*, *35*(3), 159-183.

[33] Orojloo, H., & Azgomi, M. A. (2017). A game-theoretic approach to model and quantify the security of cyber-physical systems. *Computers in Industry*, *88*, 44-57.

[34] Orojloo, H., & Azgomi, M. A. (2018). A stochastic game model for evaluating the impacts of security attacks against cyber-physical systems. *Journal of Network and Systems Management*, *26*(4), 929-965.

[35] Sepehrzadeh (Orojloo) H. (2022). A method for assessing the security risk in cyber-physical systems with incomplete information using Bayesian game theory, Karafan Quarterly Research Journal, DOI:10.48301/KSSA.2022.320681.1909. in Persian.

[36] Sallhammar, K., Helvik, B. E., & Knapskog, S. J. (2006). On stochastic modeling for integrated security and dependability evaluation. *J. Networks*, *1*(5), 31-42.

[37] Madan, B. B., Goševa-Popstojanova, K., Vaidyanathan, K., & Trivedi, K. S. (2004). A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Performance Evaluation*, *56*(1-4), 167-186.

[38] Mendiratta, V. B. (2004). Trivedi, Kishor S. 2002. Probability and Statistics with Reliability, Queuing and Computer Science Applications. *Interfaces*, *34*(5), 407-409.

Privacy for Cyber-Physical Systems (pp. 319-345). Springer, Cham.

[22] Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, *46*(4), 1-29.

[23] Thakur, S., Chakraborty, A., De, R., Kumar, N., & Sarkar, R. (2021). Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model. *Computers & Electrical Engineering*, *91*, 107044.

[24] Krishnamurthy, P., & Khorrami, F. (2021). Resilient redundancy-based control of cyber–physical systems through adaptive randomized switching. *Systems & Control Letters*, *158*, 105066.

[25] Liu, X., Zhang, J., Zhu, P., Tan, Q., & Yin, W. (2021). Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game. *Computers & Security*, *102*, 102138.

[26] Tantawy, A., Abdelwahed, S., Erradi, A., & Shaban, K. (2020). Model-based risk assessment for cyber physical systems security. *Computers & Security*, *96*, 101864.

[27] Barreto, C., Schwartz, G., & Cardenas, A. A. (2021). Cyber-Risk: Cyber-Physical Systems Versus Information Technology Systems. In *Safety, Security and Privacy for Cyber-Physical Systems* (pp. 319-345). Springer, Cham.

[28] Tripathi, D., Singh, L. K., Tripathi, A. K., & Chaturvedi, A. (2021). Model based security verification of Cyber-Physical System based on Petrinet: A case study of Nuclear power plant. *Annals of Nuclear Energy*, *159*, 108306.

[29] Lalropuia, K. C., & Gupta, V. (2019). Modeling cyber-physical attacks based on stochastic game and Markov processes. *Reliability Engineering & System Safety*, *181*, 28-37.

[30] Peng, H., Kan, Z., Zhao, D., & Han, J. (2021). Security assessment for interdependent heterogeneous