Scientific Journal of Electronical & Cyber Defence
Vol. 11, No. 2, Summer 2023, Serial No. 42

A method for quantitative evaluation of security risk in cyber-physical systems

h. Sepehrzadeh*

* Assistant Professor, Department of Computer Engineering, Technical and Vocational University (TVU), Tehran, Iran

(Received: 20/08/2022, Accepted: 03/01/2023)

ABSTRACT

Cyber-physical systems were introduced with the introduction of the cyber sector into physical systems and the emergence of Industry 4.0. Although the main purpose of this combination has been to increase the efficiency, stability and manageability of physical systems, but this combination and integration has created very serious threats to physical systems. Successful attacks on these systems may lead to disruption or physical damage such as damage to equipment, products or even damage to humans. Therefore, the security of cyber-physical systems has become one of the important research topics. In this article, a method for quantitative assessment of security risk in cyber-physical systems is presented. This method divides the important and vital components affecting the security risks of cyber-physical systems into two categories: attacker profile and system profile, and quantitatively estimates the risk based on the index components of these two profile categories. These components include attack possibility, attack detection, attacker's knowledge of the target system, time to failure, system cost, system recovery and repair cost, and vulnerability rate. Finally, in order to demonstrate the applicability, the proposed method has been applied to a cyber-physical system and the security risk has been evaluated.

Keywords: Cyber-physical systems (CPSs), Security, Risk, Evaluation.

* Corresponding Author Email: Hsepehrzade@gmail.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال یازدهم، شماره ۲، تابستان ۱۴۰۲، ص۷۱-۸۰

علمی – پژوهشی

روشی برای ارزیابی کمّی مخاطره امنیتی در سامانه‌های سایبر – فیزیکی

حامد سپهرزاده

استادیار، گروه مهندسی کامپیوتر، دانشگاه فنی و حرفه‌ای، تهران، ایران

(دریافت: ۱۴۰۱/۰۵/۲۹، پذیرش: ۱۴۰۱/۱۰/۱۳)

چکیده

با ورود بخش سایبری به سامانه‌های فیزیکی و ظهور صنعت ۴,۰، سامانه‌های سایبر - فیزیکی معرفی شدند. اگر چه هدف اصلی این ترکیب افزایش کارایی و پایداری و مدیریت‌پذیری سامانه‌های فیزیکی بوده است، اما این ترکیب و یکپارچه‌سازی تهدیدات بسیار جدّی را برای سامانه‌های فیزیکی ایجاد کرده است. حملات موفق به این سامانه‌ها ممکن است منجر به اختلال یا خرابی فیزیکی مانند ایجاد آسیب به تجهیزات، تولیدات یا حتی آسیب به انسان‌ها گردد. ازاین‌رو امنیت سامانه‌های سایبر - فیزیکی به یکی از موضوعات مهم پژوهشی تبدیل شده است. در این مقاله، روشی برای ارزیابی کمّی مخاطره امنیتی در سامانه‌های سایبر - فیزیکی ارائه شده است. این روش، مؤلفه‌های مهم و حیاتی مؤثر در مخاطرات امنیتی سامانه‌های سایبر - فیزیکی را به دو دسته نمایه مهاجم و نمایه سیستم تقسیم‌بندی می‌کند و مخاطره را بر اساس مؤلفه‌های شاخص این دو دسته نمایه به صورت کمّی تخمین می‌زند. این مؤلفه‌ها شامل امکان حمله، کشف حمله، دانش مهاجم از سامانه مورد هدف، زمان تا خرابی، هزینه وارده به سامانه، هزینه بازیابی و ترمیم سامانه و نرخ آسیب‌پذیری هستند. نهایتاً به‌منظور نمایش کاربردپذیری، روش پیشنهادی بر یک سیستم سایبر - فیزیکی اعمال شده و مخاطره امنیتی ارزیابی شده است.

کلیدواژه‌ها: سامانه‌های سایبر - فیزیکی، امنیت، مخاطره، ارزیابی

۱- مقدمه

سامانه‌های سایبر - فیزیکی[1] از ترکیب مؤلفه‌های[2] فیزیکی با مؤلفه‌های سایبری تشکیل می‌شود. مؤلفه‌های فیزیکی شامل حسگرها[3] و محرّک‌ها[4] هستند که به ترتیب وظیفه اندازه‌گیری پدیده‌های فیزیکی و اعمال دستورات کنترلی به تجهیزات فیزیکی را برعهده دارند. همچنین مؤلفه‌های سایبری وظیفه رایانش و ارتباط را بر عهده دارند [۱]. این سامانه‌ها[5] در زیرساخت‌های مهم و حیاتی، شامل انرژی، حمل‌ونقل، صنایع و حوزه سلامت کاربرد دارند [۲].

هدف اصلی ترکیب مؤلفه‌های سایبری با مؤلفه‌های فیزیکی، دستیابی به کارایی، پایداری و قابلیت اطمینان بالاتر این سامانه‌ها بوده است، اما به هر شکل این ترکیب سامانه‌های فیزیکی را با تهدیدات جدی سایبری مواجه کرده است [۳]. روش‌های ارائه شده برای مطالعه امنیت سامانه‌های سایبری تنها به بخش سایبری و فیزیکی به طور مجزا می‌پردازند و عوامل مؤثر در ترکیب این دو بخش را در نظر نمی‌گیرند [۴].

در سامانه‌های سایبر - فیزیکی، حسگرها وظیفه اندازه‌گیری و تخمین بعضی از پدیده‌های فیزیکی مانند دما، فشار، سرعت و یا رطوبت را بر عهده دارند. پس از آن، حسگرها نتیجه مشاهدات را با نوشتن در میان‌گیرهای[6] ورودی به کنترل‌کننده‌های با منطق قابل برنامه‌ریزی[7] (PLC) ارسال می‌کنند [۵]. این مشاهدات با رخدادن یک رویداد یا به‌صورت دوره‌ای، توسط حسگرها به کنترل‌کننده‌ها ارسال می‌شود. کنترل‌کننده‌ها با استفاده از مقادیر دریافت شده در میان‌گیر، و بر اساس برنامه کنترلی که برای یک کارکرد خاص برنامه‌ریزی شده‌اند، تصمیم‌گیری می‌کنند و سیگنال کنترلی خود را به محرّک‌ها ارسال می‌کنند. در نهایت، دستورات کنترلی توسط محرّک‌ها به دستگاه‌های فیزیکی اعمال می‌شود. به این روند یک حلقه کنترلی گفته می‌شود [۵و۶]. شکل (۱) انتزاعی از این سامانه‌ها را نشان می‌دهد.

به مشاهدات حسگرها و سیگنال‌های کنترلی کنترل‌کننده‌ها متغیرهای حالت[8] گفته می‌شود [۶]. به مقدار یک متغیر حالت در هر لحظه تصویر[9] منبع گفته می‌شود و مقدار یک متغیر کنترلی نقطه تعیین شده[10] نام دارد. همچنین کنترل‌کننده‌ها با دریافت اندازه‌گیری انجام شده توسط حسگرها، اختلاف مابین مقدار دریافت شده و مقدار تعیین شده را برای متغیر حالت مورد نظر محاسبه می‌کنند و با دستورات کنترلی خود تلاش می‌کنند این

* رایانامه نویسنده مسئول: Hsepehrzade@gmail.com

[1] Cyber-Physical Systems
[2] Components
[3] Sensors
[4] Actuators
[5] Systems
[6] Buffers
[7] Programmable Logic Controller
[8] State
[9] Image
[10] Set-point

ناشر: دانشگاه جامع امام حسین (ع)

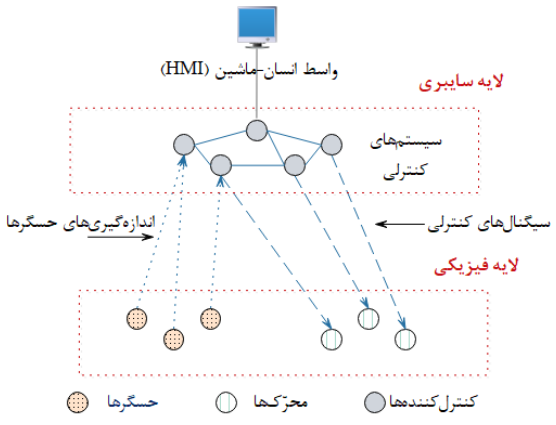
مقدار را به نقطه تعیین‌شده نزدیک نگه دارند.

در هر لحظه وضعیت سیستم به میز فرمان[1] کاربر گرداننده[2] در ایستگاه واسط انسان - ماشین[3] (HMI) ارسال می‌شود تا کاربر در جریان وضعیت سامانه باشد [۶]. این کاربر می‌تواند با توجه به شرایط در کنترل خودکار دخالت کرده و وضعیت یا کد کنترل‌کننده را تغییر دهد.

از جمله جنبه‌های متمایز در حمله به سامانه‌های سایبر - فیزیکی دانش و مهارت مهاجم است. بر اساس سیستم مورد هدف، مهاجم باید دانش دقیق در مورد کارکرد سیستم داشته باشد و بدون این دانش نتیجه حمله او به‌جز ایجاد اختلال بسیار جزئی نتیجه دیگری نخواهد داشت. علاوه بر این دانش مهاجم در مورد پردازش سیگنال، اصول کنترل، شرایط خرابی سیستم هدف، و نتایج حمله بسیار اهمیت دارد [۷و۸].

داده‌های ارسال شده توسط حسگرها بر اساس یک تأخیر کنترلی خاص توسط کنترل‌کننده‌ها استفاده می‌شود و بر روی محرّک‌ها اعمال می‌شوند. این زمان تأثیر بسزایی در عملکرد صحیح سامانه‌های سایبر - فیزیکی دارد و نباید تأخیرهای ناخواسته یا عمدی در آن ایجاد شود. داده‌های ارسال شده توسط حسگرها فقط برای یک دوره زمانی قابل‌استفاده هستند، بنابراین تازگی آن‌ها بسیار اهمّیت دارد [۹و۱۰]. همچنین از آنجایی که تصمیم کنترل بر اساس آن داده‌ها گرفته می‌شود، دقت آن‌ها بسیار مهم است [۹].

مطالعات تشخیص حمله سنّتی بر تشخیص خرابی حسگر و محرّک در فرایند فیزیکی تحت کنترل متمرکز است، بااین‌حال رویکردهای اخیر بر احتمال حملات عمدی مانند پارازیت کانال‌های ارتباطی، پخش مجدد، فریب، مخفیانه، انکار سرویس و تزریق داده‌های نادرست تمرکز دارند [۱۱].



شکل (۱). انتزاعی از سامانه‌های سایبر - فیزیکی

در سامانه‌های سایبر - فیزیکی نه‌تنها افزایش امنیت بسیار پرهزینه است، بلکه مشکلات امنیتی نیز هزینه بیشتری به این سامانه‌ها تحمیل می‌کند. این موضوع به این دلیل است که مهاجمان راهبردهای خود را با راهبردهای افزایش امنیت و محافظت سیستم تطبیق می‌دهند [۱۲]. هزینه‌های کلی برای تولید شبکه‌های شرکتی ایمن و نرم‌افزارهای امن، این سامانه‌ها را در معرض حملات بدخواهانه قرار داده است. هنگامی که یک آسیب‌پذیری[4] یافت شد و مورد سوء استفاده قرار گرفت، آن آسیب‌پذیری برای دستگاه‌های مشابه قابل سوء استفاده خواهد بود [۱۳].

به‌طورکلی آسیب‌پذیری‌های سامانه‌های سایبر - فیزیکی به سه دسته آسیب‌پذیری سکو[5]، شبکه و مدیریت تقسیم می‌شوند [۱۳]. آسیب‌پذیری‌های سکو عبارت‌اند از آسیب‌پذیری‌های پیکربندی، نرم‌افزار، سخت‌افزار و پایگاه داده. آسیب‌پذیری‌های شبکه به هدف قراردادن کانال‌های ارتباطی با انجام دست‌کاری بسته‌ها، پخش مجدد[6]، انکار سرویس[7] یا انکار سرویس توزیع شده، استراق سمع، جعل، بوکشی[8]، درهای پشتی[9] و حملات مرد میانی[10] اشاره دارد. آسیب‌پذیری‌های مدیریتی به فقدان دستورالعمل‌ها، رویه‌ها و سیاست‌های امنیتی مناسب اشاره دارد.

پیامد حملات به سامانه‌های سایبر - فیزیکی به دسته‌های زیر تقسیم‌بندی می‌شود [۱۴و۱۵]:

- آسیب به تجهیزات، شامل خرابی قطعات، افزایش استهلاک و کاهش طول عمر آن‌ها
- آسیب به تولیدات: شامل ازبین‌بردن تولیدات و تخریب
- هدف قراردادن ایمنی و جان انسان‌ها
- قطعی خدمت: از دسترس خارج‌شدن خدمت‌دهی سیستم
- مخاطرات محیطی و آلودگی: مانند آلودگی هوا

با توجه به موضوعات مطرح شده هدف اصلی مقاله به شرح زیر است:

۱) شناسایی و به‌کارگیری مؤلفه‌های مهم مطرح در ارزیابی مخاطره امنیتی در سامانه‌های سایبر - فیزیکی،

۲) ارائه روشی برای ارزیابی مخاطره امنیتی به‌صورت کمّی و کیفی برای سامانه‌های سایبر - فیزیکی،

۳) انجام مطالعه موردی به‌منظور نمایش کاربردپذیری روش پیشنهاد شده.

ادامه مقاله به این شرح است. در بخش ۲، به بررسی کارهای مرتبط و توضیح روش پیشنهادی خواهیم پرداخت. در بخش ۳،

[1] Console
[2] Operator
[3] Human-Machine Interface

[4] Vulnerability
[5] Platform
[6] Replay
[7] Denial of service (DoS)
[8] Snifing
[9] Back doors
[10] Man-in-the-Middle

یک مثال به‌عنوان یک مطالعه موردی ذکر خواهد شد و در بخش ۴ نتایج مقاله بیان خواهد شد.

۲- روش تحقیق

در این بخش ابتدا به بررسی کارهای مرتبط در حوزه ارزیابی امنیت و مخاطره امنیت در سامانه‌های سایبر - فیزیکی می‌پردازیم و نقاط ضعف و قوت آن‌ها را بیان می‌کنیم. سپس به توصیف روش پیشنهادی می‌پردازیم.

۲-۱- کارهای مرتبط

در حوزه ارزیابی امنیت و مخاطره امنیت کارهای متعددی انجام شده است. از جمله اوفوری و همکاران [۱۶] در پژوهش خود روشی برای مدل‌سازی و ارزیابی تهدید ارائه شده است. نویسندگان به بررسی امنیت زنجیره تأمین از زنجیره‌های ورودی و خروجی پرداخته‌اند. به همین منظور به حملات نفوذ و دست‌کاری از دیدگاه سازمانی متمرکز شده‌اند. کاستی روش ارائه شده در این مقاله این است که حساسیت منابع سایبر - فیزیکی و مؤلفه‌های زمانی مهم تأثیرگذار در مخاطره امنیتی را برای سامانه‌های سایبر - فیزیکی در نظر نگرفته‌اند و روش آن‌ها برای صنایع حیاتی قابل به‌کارگیری نیست.

اسچلگل و همکاران [۱۷] روشی را برای مدل‌سازی تهدید در سامانه‌های سایبر - فیزیکی با تمرکز بر الگوهایی که بر معماری این سامانه‌ها مربوط هستند ارائه کرده‌اند. همچنین به یکپارچه‌سازی تهدیدهایی که به شیوه‌های مشابه رفتار می‌کنند و با روش‌های مشابه کنترل می‌شوند پرداخته‌اند. مشابه روش قبل، کاستی این روش این است که حساسیت منابع سایبر - فیزیکی و مؤلفه‌های زمانی مهم تأثیرگذار در مخاطره امنیتی را برای سامانه‌های سایبر - فیزیکی در نظر نگرفته‌اند و روش آن‌ها برای صنایع حیاتی قابل به‌کارگیری نیست.

روسادو و همکاران [۱۸] الگویی برای ارزیابی مخاطره امنیتی برای سامانه‌های سایبر - فیزیکی ارائه شده است. این الگو از سه فهرست‌نامه[1] طبقه‌بندی شده (کنترل‌ها، دارایی‌ها و تهدیدها) تشکیل شده است. به‌عنوان مطالعه موردی، روش پیشنهادی بر یک بیمارستان هوشمند اعمال شده است. از جمله نقاط ضعف این روش عدم در نظر گرفتن مؤلفه‌های زمانی حمله و دانش موجود مهاجم از سیستم هدف است.

تنتاوی و همکاران [۱۹] در پژوهش خود یک رویکرد مبتنی بر مدل یکپارچه را برای ارزیابی مخاطره امنیتی سامانه‌های سایبر - فیزیکی با استفاده از یک بستر آزمایشی با کنترل‌کننده‌های صنعتی و پروتکل‌های ارتباطی واقعی توسعه داده و آزمایش کرده‌اند. بستر آزمایش یک رآکتور مخزن هم زده مداوم گرمازای شبیه‌سازی شده به‌صورت بی‌درنگ[2] را نظارت و کنترل می‌کند. در این روش مخاطره امنیتی سامانه‌های سایبر - فیزیکی بر اساس یک مؤلفه احتمال حمله، و سه مؤلفه پیامد هزینه ایمنی، هزینه مادی و هزینه محیطی تعریف شده است که به‌منظور استفاده برای سامانه‌های سایبر - فیزیکی کامل نیست. از طرف دیگر ایجاد این بستر آزمایشی هزینه نسبتاً بالایی را به سیستم تحمیل می‌کند.

ویو و همکاران [۲۰] به‌منظور ارزیابی مخاطره امنیت سایبری سامانه‌های سایبر - فیزیکی، یک مدل ارزیابی سلسله‌مراتبی کمّی شامل شدت حمله، احتمال موفقیت حمله و پیامد حمله پیشنهاد شده است که می‌تواند خطر ناشی از یک حمله مداوم در سطح میزبان و سطح سیستم را ارزیابی کند. در این پژوهش پارامترهای زمانی حمله و دانش مهاجم در نظر گرفته نشده است.

هوانگ و همکاران [۲۱] روشی برای ارزیابی مخاطره امنیتی سامانه‌های سایبر - فیزیکی صنعتی پیشنهاد شده است. روش ارائه شده با استفاده از یک شبکه بیزی برای مدل‌سازی فرایند انتشار حمله استفاده می‌کند و احتمال به‌خطرافتادن حسگرها و محرک‌ها را محاسبه می‌کند. این احتمالات به یک مدل سیستم ترکیبی تصادفی برای پیش‌بینی تکامل فرایند فیزیکی تحت کنترل وارد می‌شوند. سپس، مخاطره امنیتی با ارزیابی دردسترس‌بودن سیستم با مدل سیستم ترکیبی تصادفی کمّی‌سازی می‌شود. این روش جنبه‌های زمانی حملات سایبری با هدف اختلال فیزیکی را در نظر نگرفته است.

لیو و همکاران [۲۲]، یک مدل ارزیابی مخاطره سایبری به فیزیکی بر اساس شبکه بیزی (BN)[3] سلسله‌مراتبی پیشنهاد داده‌اند. امکان‌سنجی این مدل با ساخت دو سناریو رویداد نامطلوب بر روی یک سامانه سایبر - فیزیکی معمولی تأیید می‌شود. در این روش مخاطره امنیتی به هزینه خرید دارایی محدود شده است. با در نظر گرفتن سایر مؤلفه‌های مخاطره سایبری به فیزیکی مانند خسارت جانی و اقتصادی، زوال محیط‌زیست یا آسیب به شهرت، به‌عنوان کارهای آینده مطرح شده است.

خولیدی در پژوهش خود [۲۳] به موضوع نیاز به رویکردهای امنیتی پیشرفته برای پاسخگویی به حملات به سامانه‌ها سایبر - فیزیکی به‌صورت خودکار با وجود یا بدون وجود یک مدیر سیستم در حلقه کنترلی در هنگام صدور هشدار در مورد نفوذ

[1] Catalog

[2] Real time

[3] Bayesian network

احتمالی پرداخته است. برای این منظور، این مقاله چارچوب امنیتی با یک کنترل‌کننده با قابلیت پاسخ خودکار (ARC)[1] پیشنهاد کرده است. ARC از درخت همبستگی مخاطره سلسله‌مراتبی (HRCT)[2] استفاده می‌کند که مسیرهایی را که مهاجم می‌تواند برای رسیدن به اهداف معین طی کند، مدل‌سازی می‌کند و مخاطره مالی که دارایی‌های سامانه سایبر - فیزیکی در اثر حملات سایبری با آن مواجه است را اندازه‌گیری می‌کند. این پژوهش تنها مخاطرات مالی را در نظر گرفته است.

در کار پیشین [۲۴] روشی را برای ارزیابی مخاطره امنیت سامانه‌های سایبر - فیزیکی ارائه کردیم. تقابل بین سیستم و مهاجم به‌صورت یک بازی با اطلاعات ناقص مدل شد. در آن روش تمرکز اصلی بر روی پیش‌بینی رفتار مهاجم بود و پارامترهای مهمّ زمانی، مالی و سامانه‌ای را در نظر گرفته نشده بودند.

در پژوهشی دیگر [۱۵] روشی را برای ارزیابی انتشار پیامد حملات در سامانه‌های سایبر - فیزیکی پیشنهاد نمودیم. در این روش بررسی کردیم چگونه پیامد حمله اعمال شده به سیستم بر یک مؤلفه می‌تواند بر روی مؤلفه‌های دیگر متأثر باشد. تمرکز اصلی در این پژوهش حملات به داده‌های حسگر و دستورات کنترلی و ارسال شده به محرّک‌ها و بررسی انتشار پیامد این حملات بوده است و تأثیر سایر مؤلفه‌های مهم مانند مؤلفه‌های زمانی، مالی و دانش مهاجم مورد بررسی قرار نگرفته است.

به طور خلاصه، روش‌های موجود در مدل‌سازی و ارزیابی مخاطره امنیت برای سامانه‌های سایبر - فیزیکی نواقصی دارند. در واقع بعضی از مؤلفه‌های مهم این سامانه‌ها از جمله زمان خرابی سیستم، هزینه بازیابی از حمله موفق و دانش مهاجم از کارکرد سیستم در این روش‌ها در نظر گرفته نشده است. این مؤلفه‌ها مؤلفه‌هایی هستند که ارزیابی مخاطره امنیت سامانه‌های سایبر - فیزیکی بدون در نظر گرفتن آن‌ها کارآمدی و دقت بالایی نخواهد داشت. از طرفی، بعضاً روش‌های بیان شده خاص‌منظوره هستند و برای دسته مشخصی از سامانه‌های سایبر - فیزیکی قابل به‌کارگیری هستند؛ بنابراین به روش جدیدی برای ارزیابی مخاطره امنیت سامانه‌های سایبر - فیزیکی نیاز است که ویژگی‌های زیر را داشته باشد:

- مؤلفه‌های مهمّ این سامانه‌ها، از جمله احتمال حمله، احتمال کشف حمله، آسیب‌پذیری، زمان تا خرابی سیستم، زمان تا ترمیم از خرابی، هزینه وارد شده بر اثر حمله موفق و دانش مورد نیاز مهاجم برای حمله به این سامانه‌ها را در نظر بگیرد.
- برای طیف وسیعی از سامانه‌های سایبر - فیزیکی قابل استفاده باشد.
- مزیت سادگی به‌کارگیری و پیاده‌سازی را داشته باشد.

۲-۲- روش پیشنهادی

موضوع اصلی مطرح در این مقاله پیشنهاد روشی برای ارزیابی کمّی مخاطره امنیتی است که ویژگی‌های سامانه‌های سایبر - فیزیکی و مؤلفه‌های مهم در مخاطره امنیتی این سامانه‌ها را در نظر بگیرد و برای این سامانه‌ها کارآمد باشد. روش پیشنهادی بر اساس مؤلفه‌هایی تعریف می‌شود که در دو دسته کلّی نمایه مهاجم و نمایه سیستم جای می‌گیرند. بر این اساس مؤلفه‌های نمایه مهاجم به شرح زیرند:

- امکان حمله مهاجم به هدف مشخص.
- میزان دانش مهاجم برای انجام حمله مورد نظر.

همچنین مؤلفه‌های در نظر گرفته شده در نمایه سیستم عبارت‌اند از:

- امکان کشف حمله توسط سیستم
- مهلت زمان تا خرابی سیستم بعد از آغاز حمله
- هزینه ترمیم و بازیابی سیستم
- میزان خسارت محتمل در اثر حمله موفق
- نرخ آسیب‌پذیری سیستم

در ادامه به توصیف روش پیشنهادی می‌پردازیم. مخاطره به‌صورت حاصل‌ضرب امکان وقوع حمله با پیامد آن قابل ارزیابی است. در واقع مخاطره امنیتی به‌صورت زیر قابل تعریف است:

$$R = P_a \times E \qquad (۱)$$

که R مخاطره امنیتی، P_a امکان وقوع حمله و E پیامد آن حمله است.

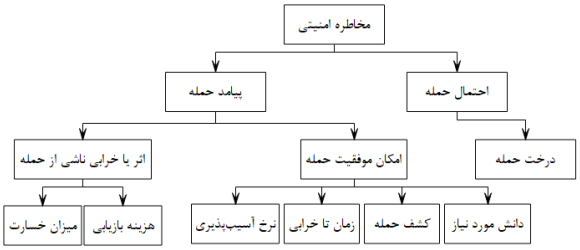
موضوع مهم این است که مؤلفه‌های این دو پارامتر در سامانه‌های سایبر - فیزیکی در مقایسه با سامانه‌های سایبری متفاوت است. شکل (۲) تصویر کلّی از مؤلفه‌های در نظر گرفته شده در روش و دسته‌بندی آن‌ها را نمایش می‌دهد.

ابتدا به مؤلفه امکان حمله می‌پردازیم. هر سیستم سایبر - فیزیکی دارای منابع با ارزشی است که ممکن است مورد حمله مهاجم قرار بگیرد. همان‌طور که ذکر شد هدف اصلی مهاجمان از حمله به سامانه‌های سایبر - فیزیکی ایجاد خرابی، ایجاد اختلال فیزیکی یا توقف کارکرد سیستم است. به این منظور، او ممکن

[1] Autonomous Response Controller
[2] Hierarchical Risk Correlation Tree

است منابع مختلفی از سیستم را هدف قرار دهد. برای رسیدن به هر هدف، سناریوهای حمله مختلفی وجود دارد. همچنین روش‌های مختلفی برای مدل‌سازی سناریوهای مختلف حملات و مسیرهای حمله وجود دارد. از جمله مهم‌ترین این روش‌ها، مدل‌سازی مسیرهای حمله با استفاده از درخت حمله است. با استفاده از درخت حمله، احتمال حمله انجام یک حمله مهاجم با یک هدف خاص در سیستم قابل تخمین خواهد بود.

مؤلفه دوم، پیامد حملات است. پیامد حملات خود از دو پارامتر دیگر منتج می‌شود: ۱) حملات محتمل تا چه اندازه موفقیت‌آمیز خواهند بود و منجر به ایجاد اختلال یا خرابی فیزیکی خواهند شد و ۲) نتیجه حمله چه خواهد بود، چه تأثیری بر کارکرد سیستم سایبر - فیزیکی خواهد داشت و چه آسیبی را به این سیستم وارد خواهد کرد. در واقع به‌منظور تخمین مؤلفه پیامد، با دو پارامتر امکان موفقیت حمله و میزان اثر حمله مواجه هستیم. پیامد حملات (E) در روش پیشنهادی از رابطه زیر قابل محاسبه است:



شکل (۲). مؤلفه‌های روش ارائه شده برای ارزیابی مخاطره امنیتی

$$E = S_a \times I \qquad (۲)$$

که S_a امکان موفقیت حمله و I میزان اثر حمله است.

موفقیت حمله مهاجم به پارامترهای مختلفی وابسته است. یک مهاجم تنها در صورتی در حمله به یک سیستم سایبر - فیزیکی موفق خواهد بود که از سطح دانش مناسبی در مورد سیستم مورد هدف برخوردار باشد. بدون این دانش، مهاجم نخواهد توانست تأثیر قابل توجهی بر عملکرد سیستم داشته باشد و اختلال یا آسیب فیزیکی بر آن وارد کند.

مورد دوم که در موفقیت حمله مهاجم تأثیرگذار است، کشف حملات توسط سیستم است. هر چه احتمال کشف حملات در کوتاه‌ترین زمان ممکن بالا باشد، احتمال موفقیت حمله و به نتیجه رسیدن آن کوتاه خواهد بود. بنابراین امکان موفقیت حمله با کشف حملات توسط سیستم نسبت معکوس دارد.

مورد سوم مؤثر در احتمال حمله موفق، مدت‌زمان اثر حمله یا میزان زمان تا خرابی است. هر چه مدت‌زمان تا خرابی سیستم بعد از شروع حمله کوتاه‌تر باشد، زمان مورد نیاز برای کشف و اقدام مناسب توسط سیستم کوتاه‌تر خواهد بود و در نتیجه احتمال موفقیت حمله بیشتر خواهد بود. در نتیجه، احتمال موفقیت حمله با زمان اثر حمله رابطه معکوس خواهد داشت.

مورد چهارم نرخ آسیب‌پذیری است. آسیب‌پذیری یک ضعف در دارایی‌ها و خدمات سیستم‌های سایبر - فیزیکی است که می‌تواند توسط عوامل تهدید برای انجام اقدامات مخرب مورد سوء استفاده قرار گیرد. آسیب‌پذیری که به‌صورت عمومی منتشر شده است نسبت به آسیب‌پذیری‌هایی که کشف نشده است امکان سوء استفاده بیشتری توسط مهاجمان دارد. آسیب‌پذیری‌های شناخته شده و مسائل امنیتی توسط نهادها و سازمان‌هایی مانند مراکز امنیت ملّی، و آژانس‌های امنیتی منتشر شده است [۲۵].

بر اساس پارامترهای تعریف شده، امکان موفقیت حمله مهاجم (S_a) از رابطه زیر به دست می‌آید:

$$S_a = \frac{V \times K}{D \times T} \qquad (۳)$$

که V نرخ آسیب‌پذیری سیستم، K دانش مهاجم از سیستم هدف، D امکان تشخیص حمله توسط سیستم و T زمان تا خرابی یا ورود آسیب به سیستم در اثر حمله است.

اکنون به بررسی مؤلفه اثر حمله می‌پردازیم. این مؤلفه نیز به پارامترهای مختلفی بستگی دارد. اولین پارامتر ارزش منابع سایبر - فیزیکی مورد هدف و میزان خسارتی است که حمله موفق به سیستم وارد می‌کند. هر چه ارزش منبع مورد هدف بیشتر باشد، خسارت و اثر حمله بیشتر خواهد بود. همچنین مهاجم انگیزه بیشتری برای حمله به آن منبع را خواهد داشت.

مورد دوم هزینه ترمیم و بازیابی سیستم در اثر وقوع خرابی است تا سیستم مجدداً به حالت عادی و کارکرد طبیعی خود بازگردد. یکی از مهم‌ترین پارامترهای هزینه، زمان بازگشت سیستم به حالت کارکردی و هزینه راه‌اندازی مجدد سیستم است. این هزینه می‌تواند خسارتی که بر اثر غیرفعال بودن سیستم وارد می‌شود را نیز شامل شود. هر چه زمان بازگشت سیستم به حالت عادی طولانی‌تر باشد، اثر حمله شدیدتر خواهد بود. بنابراین اثر حمله (I) از رابطه زیر قابل محاسبه است:

$$I = C_a + C_r \qquad (۴)$$

که C_a میزان خسارت ناشی از حمله به دارایی‌ها و منابع سیستم و C_r هزینه ترمیم و بازیابی سیستم به حالت کارکردی و عادی اولیه است.

۲-۳- ارزیابی و اعتبارسنجی مؤلفه‌ها

در این بخش به توضیح نحوه ارزیابی و اعتبارسنجی مؤلفه‌ها خواهیم پرداخت. لیست مؤلفه‌های استفاده شده در روش پیشنهادی به همراه توصیف نحوه مقداردهی آن‌ها در جدول (۱) آمده است. این مؤلفه‌ها با بررسی مطالعه‌های انجام شده در حوزه امنیت سامانه‌های سایبر - فیزیکی جمع‌بندی و به کار گرفته شده است (از جمله [۲]، [۸] و [۹]).

امکان حمله مهاجم به هدف مشخص: این مؤلفه با استفاده از شناسایی مسیرهای حمله و به کمک ساختار درخت و گراف حمله قابل برآورد است. در واقع باید مسیرهای مختلفی که مهاجم برای رسیدن به هدف خاص می‌تواند طی کند و احتمال انتخاب آن‌ها را برآورد نمود. هر چه مسیرهای موجود برای رسیدن به یک هدف خاص از پیچیدگی کمتری برخوردار باشد و مهاجم نیاز به دانش و مهارت کمتری برای رسیدن به هدف داشته باشد احتمال رسیدن به آن هدف مشخص بالاتر خواهد بود.

نرخ آسیب‌پذیری: همان‌طور که بیان شد، آسیب‌پذیری‌های شناخته شده و مسائل امنیتی توسط نهادها و سازمان‌هایی مانند مراکز امنیت ملّی، و آژانس‌های امنیتی منتشر شده است [۲۵]. این مؤلفه با توجه به وضعیت انتشار آسیب‌پذیری و تأثیر آن در سیستم مقداردهی می‌شود. هر چه آسیب‌پذیری از مهاجم پنهان باشد و مهاجم برای شناسایی آن نیاز به ابزار خاص داشته باشد، نرخ آسیب‌پذیری کمتر خواهد بود. در جدول (۱) نحوه ارزیابی این مؤلفه بیان شده است.

جدول (۱). ماتریس ارزیابی مؤلفه‌های معرفی شده در روش

مؤلفه	سطح حساسیت
امکان حمله مهاجم به هدف مشخص	○ ۵ خیلی بالا، احتمال بین ۰٫۸ تا ۱ ○ ۴ بالا، احتمال بین ۰٫۶ تا ۰٫۸ ○ ۳ متوسط، احتمال بین ۰٫۴ تا ۰٫۶ ○ ۲ کم، احتمال بین ۰٫۲ تا ۰٫۴ ○ ۱ خیلی کم، احتمال بین صفر تا ۰٫۲
نرخ آسیب‌پذیری	○ ۵: آسیب‌پذیری‌های منتشر شده و شناسایی شده با تأثیر خیلی بالا در سیستم ○ ۴: آسیب‌پذیری شناسایی شده با تأثیر بالا در سیستم ○ ۳: آسیب‌پذیری‌هایی شناسایی نشده و با تأثیر بالایی که برای شناسایی آن‌ها مهاجم نیاز به ابزار خاص دارد ○ ۲: آسیب‌پذیری‌هایی شناسایی نشده و با تأثیر محدودی که برای شناسایی آن‌ها مهاجم نیاز به ابزار خاص دارد. ○ ۱: آسیب‌پذیری‌هایی شناسایی نشده و با تأثیر بسیار جزئی که برای شناسایی آن‌ها مهاجم نیاز به ابزار خاص دارد.
میزان اثر (اختلال یا خرابی) حمله	○ ۵: وجود تهدید ایمنی و خرابی فیزیکی ○ ۴: امکان ایجاد خرابی فیزیکی ○ ۳: امکان ایجاد اختلال فیزیکی یا قطع کارکرد ○ ۲: ایجاد اختلال جزئی ○ ۱: عدم امکان ایجاد اختلال
میزان دانش مهاجم برای حمله مورد نظر	○ ۱: دانش خاص و مهارت بالا ○ ۰٫۸: مهارت بالا و دانش متوسط ○ ۰٫۵: مهارت بالا و دانش کم ○ ۰٫۲: مهارت و عدم نیاز به دانش خاص ○ ۰٫۱: مهارت جزئی
امکان کشف حمله	○ ۵: امکان کشف بالا از طریق سیستم کشف نفوذ ○ ۴: نیازمند مهارت برای کشف ○ ۳: نیازمند نظارت خاص برای کشف ○ ۲: نیازمند مهارت و نظارت خاص برای کشف ○ ۱: غیر قابل کشف
زمان تا خرابی سامانه بعد از آغاز حمله (بر اساس سیستم قابل برآورد است)	○ ۵: مناسب ○ ۴: نسبتاً مناسب ○ ۳: متوسط ○ ۲: کوتاه ○ ۱: بسیار کوتاه
هزینه ترمیم و بازیابی سیستم (بر اساس سیستم قابل برآورد است)	○ ۵: نیاز به توقف طولانی و بازیابی طولانی ○ ۴: نیاز به توقف متوسط و بازیابی طولانی ○ ۳: نیاز به توقف کوتاه و بازیابی متوسط ○ ۲: عدم نیاز به توقف و بازیابی متوسط ○ ۱: عدم نیاز به توقف و بازیابی سریع
میزان خسارت محتمل در اثر حمله موفق (بر اساس سیستم قابل برآورد است)	○ ۵: وجود تهدید ایمنی و خرابی فیزیکی ○ ۴: امکان ایجاد خرابی فیزیکی ○ ۳: امکان ایجاد اختلال فیزیکی یا قطع کارکرد ○ ۲: ایجاد اختلال جزئی ○ ۱: عدم امکان ایجاد اختلال

میزان اثر (اختلال یا خرابی) حمله: همان‌طور که بیان شد حملات به سیستم‌های سایبر - فیزیکی پیامدهای مختلفی می‌تواند داشته باشد. حمله‌های مهاجمان با توجه به شناخت آن‌ها از سامانه، هدف، دانش و مهارتش ممکن است پیامدهای متفاوتی داشته باشد. مهلک‌ترین حمله‌ها به این سیستم‌ها حمله‌هایی است که منجر به خرابی فیزیکی، ایمنی و به خطر افتادن جان انسان‌ها می‌شود. در درجه دوم حملاتی که پیامد آن‌ها بروز خرابی فیزیکی است مورد اهمیّت قرار می‌گیرند و در درجه سوم حملاتی که منجر به بروز اختلال کارکرد سامانه می‌شوند قرار می‌گیرند. در درجه چهارم حملاتی که به‌جز اختلال جزئی نتیجه‌ای برای مهاجم ندارند و نهایتاً در درجه پنجم حملاتی که ایجاد اختلال نمی‌کنند ارزیابی می‌شوند.

میزان دانش مهاجم برای حمله مورد نظر: این مؤلفه مشخص می‌کند که مهاجم برای انجام حمله خود به چه میزان دانش و مهارت نیاز دارد. به‌عنوان‌مثال، برنامه‌ریزی مجدد کنترل‌کننده

نیاز به دانش و مهارت بالایی از کارکرد سامانه مورد نظر دارد اما انجام حمله منع خدمت به واسط کاربر - ماشین به سطح بالایی از دانش نیاز ندارد.

امکان کشف حمله: اینکه یک حمله با هدف خاص از طریق سامانه تشخیص نفوذ قابل شناسایی است و یا اینکه به‌منظور تشخیص حمله نیاز به مهارت و نظارت خاص وجود دارد، این مؤلفه قابل ارزیابی است که نحوه ارزیابی آن در جدول (۱) بیان شده است.

زمان تا خرابی سامانه بعد از آغاز حمله: ارزیابی این مؤلفه با توجه به سامانه مورد هدف و نوع حمله انجام شده قابل برآورد است. هر چه مدت‌زمان بیشتری از آغاز حمله مهاجم و نمایان‌شدن آثار آن وجود داشته باشد، مهلت بیشتری برای تشخیص و جلوگیری از اثرات آن وجود دارد. بنابراین هر چه این مهلت بیشتر باشد مخاطره حمله کمتر خواهد بود و مقدار این مؤلفه بیشتر خواهد بود. برآورد این مؤلفه کاملاً به سامانه مورد نظر وابسته است. در بعضی از سامانه‌ها بیشینه مهلت زمان تا خرابی ممکن است در حد یک دقیقه باشد و در سامانه دیگر ممکن است به چندین ساعت مهلت نیاز باشد. بنابراین مقدار این مؤلفه کاملاً توسط متخصّصان امنیت سامانه قابل برآورد خواهد بود.

هزینه ترمیم و بازیابی سیستم: این مؤلفه میزان زمان توقف سامانه را نشان می‌دهد. هر چه این زمان بیشتر باشد، مقدار این مؤلفه هم بیشتر خواهد بود. مقداردهی این مؤلفه هم کاملاً نسبی است و به سامانه مورد مطالعه وابسته است و توسط متخصّصان امنیت آن سامانه قابل برآورد خواهد بود. به‌عنوان‌مثال در بعضی از سامانه‌های سایبر - فیزیکی توقف در حد چند دقیقه هم توقف طولانی محسوب می‌شود درحالی‌که در سیستم دیگر توقف ساعتی طولانی در نظر گرفته می‌شود.

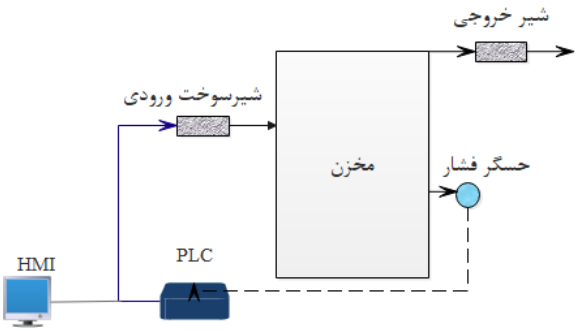
میزان خسارت محتمل در اثر حمله موفق: یک حمله با توجه به پیامدش می‌تواند به سامانه خسارت وارد نماید. حملاتی که پیامد نقض ایمنی و به‌خطرافتادن جان انسان‌ها را دارند در درجه اول و حملاتی که خسارت فیزیکی ایجاد می‌کنند در درجه دوم (ممکن است خرابی تجهیزات، تولیدات، آلودگی محیطی، توقف خط تولید و مانند آن داشته باشد)، از اهمیت بالاتری برخوردار هستند. این خسارت با توجه به نوع پیامد و هزینه تحمیل شده، توسط متخصصان امنیت سامانه بر اساس جدول (۱) قابل برآورد خواهد بود.

۳- مطالعه موردی

در این بخش به‌عنوان مطالعه موردی روش پیشنهادی را بر یک سیستم سایبر - فیزیکی اعمال می‌کنیم. همچنین مثالی از یک حمله واقعی را تحلیل می‌کنیم. سیستم مورد نظر شامل یک کنترل‌کننده یا PLC، حسگر فشار، واسط انسان - ماشین و شیر ورودی و خروجی است. درصورتی‌که فشار داخل مخزن از یک حد آستانه مشخص k بیشتر شود، انفجار رخ خواهد داد. شکل (۳) شمای سیستم سایبر - فیزیکی را نشان می‌دهد. حملات محتمل به این سیستم به‌صورت زیر در نظر گرفته شده‌اند:

- حمله تغییر کد PLC
- حمله جلوگیری از خدمت DOS به PLC
- حمله تغییر نقطه تعیین شده HMI
- حمله DOS به HMI

مقادیر مؤلفه‌های روش پیشنهادی برای حملات در نظر گرفته شده در جدول (۲) بیان شده است. مقدار مخاطره برای هر یک از حملات معرفی شده در ستون آخر نمایش داده شده است. بر اساس محاسبات صورت‌گرفته با استفاده از روش پیشنهادی، بالاترین سطح مخاطره بین این حملات مربوط به حمله تغییر کد PLC خواهد بود. بعد از آن تغییر نقطه تعیین شده به واسط انسان ماشین دومین سطح مخاطره را خواهد داشت. همچنین حملات جلوگیری از خدمت به PLC و HMI به ترتیب سطوح مخاطره بعدی را خواهند داشت.



شکل (۳). سیستم سایبر - فیزیکی مطالعه موردی

جدول (۲). مقادیر مؤلفه‌ها و مخاطره حملات برای مطالعه موردی

حمله	K	C_a	D	T_a	C_r	V	P_a	R
Code PLC	۰/۲	۵	۳	۴	۴	۴	۴	۲/۴
DOS PLC	۰/۸	۳	۴	۳	۳	۱	۲	۰/۸
Set Point HMI	۰/۳	۴	۳	۴	۴	۳	۴	۱/۸
DOS HMI	۰/۷	۳	۴	۳	۳	۱	۲	۰/۷

در ادامه به انجام آزمایشات بیشتر می‌پردازیم. در هر مرحله مقدار پیش‌فرض مؤلفه‌ها را با تغییر یک مؤلفه مورد مطالعه قرار می‌دهیم، تا اثر تغییر آن مؤلفه بر مخاطره امنیتی مشخص شود.

در آزمایش اول تأثیر دانش مهاجم بر مخاطره امنیتی مورد سنجش قرار گرفته است. همان‌طور که شکل (۴) نشان می‌دهد، با افزایش سطح دانش مهاجم از سیستم مخاطره امنیتی بالاتر می‌رود. علّت این موضوع این است که احتمال موفقیت مهاجم در حمله به سیستم و ایجاد خرابی و اختلال فیزیکی بیشتر خواهد شد.

در آزمایش دوم به بررسی تأثیر مقدار مؤلفه تشخیص حمله بر مخاطره امنیتی می‌پردازیم. همان‌طور که در شکل (۵) قابل مشاهده است، با افزایش امکان تشخیص حمله توسط سیستم، میزان مخاطره امنیت کاهش پیدا می‌کند. دلیل این موضوع آن است که با افزایش امکان تشخیص حمله، امکان موفقیت حمله کمتر شده و در نتیجه مخاطره امنیت کاهش خواهد یافت.

آزمایش سوم به بررسی تأثیر مؤلفه هزینه بازیابی سیستم بعد از وقوع حمله موفق می‌پردازد. نتیجه این آزمایش در شکل (۶) قابل مشاهده است. با افزایش هزینه بازیابی سیستم از حمله موفق، میزان مخاطره امنیت افزایش خواهد یافت. دلیل این موضوع آن است که با افزایش هزینه بازیابی، در واقع دارایی‌هایی که خسارت دیده‌اند و یا توقف صورت گرفته در تولید سیستم بیشتر خواهد بود.

در آزمایش چهارم که در شکل (۷) مشخص است، به بررسی مؤلفه زمان تا خرابی سیستم می‌پردازیم. هر چه بعد از آغاز حمله زمان تا خرابی سیستم کوتاه‌تر باشد، مخاطره امنیت بالاتر خواهد رفت. در واقع با افزایش زمان تا خرابی سیستم فرصت بیشتری برای تشخیص حمله و جلوگیری از بروز خسارت خواهد داشت و در نتیجه مخاطره امنیتی کاهش خواهد یافت.

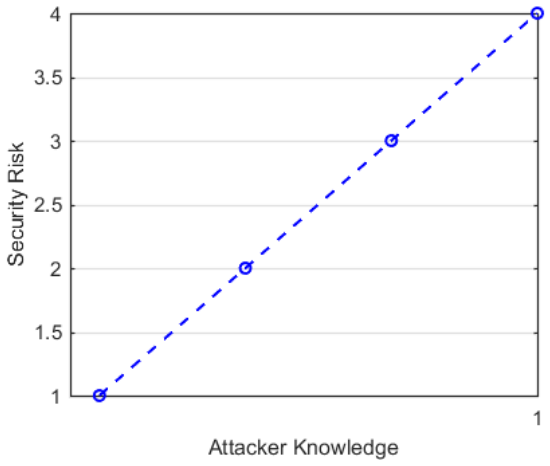
به‌عنوان یک مثال از یک حمله واقعی، حمله انجام شده به نیروگاه‌های هسته‌ای با هدف تغییر کد کنترل‌کننده را در نظر می‌گیریم [۲۶]. این کنترل‌کننده از نوع سیمنز[1] بود. برای این منظور مهاجمان از چهار آسیب‌پذیری صفر - روز[2] سیستم‌عامل ویندوز که امکان ارسال کدهای مخرب و سپس اجرای آن بر روی یک ماشین راه دور را فراهم می‌کرد بهره بردند [۲۷]. از آنجایی که این آسیب‌پذیری‌ها توسط مهاجمان شناسایی شده و منتشر نشده بود طبق جدول (۱) مقدار ۴ را به خود اختصاص می‌دهد. مهاجمان همچنین آگاهی کامل از نوع کنترل‌کننده و کدی که برنامه‌ریزی شده بود داشتند. به همین دلیل توانستند به موفقیت دست پیدا کنند و هزینه بالایی را به سیستم تحمیل کند (مقدار دانش ۱ و آسیب وارده به سیستم ۵ و هزینه بازیابی ۵).

در این حمله، کرم[3] طراحی شده با ارسال فرمان به درایو مبدل فرکانس سانتریفیوژ[4]، حداکثر فرکانس چرخش سانتریفیوژها را تغییر می‌داد. از طرفی کد تغییر داده شده از میز فرمان کاربر سامانه مخفی نگه داشته می‌شد و کد مجاز که قبلاً ذخیره شده بود در هر بار بررسی به کاربر نمایش داده می‌شد [۲۸]. به همین دلیل کشف نفوذ و حمله صورت گرفته بسیار مشکل و زمان‌بر بود (امکان کشف ۱). در این حمله، سرعت چرخش سانتریفیوژها در خارج از محدوده عملیاتی، بعد از مدت‌زمان کوتاهی و بعد از چند دقیقه، باعث کاهش عمر و در نهایت آسیب فیزیکی به سانتریفیوژها شد (زمان تا خرابی ۲).

با در نظر گرفتن سطح دانش مهاجم به‌صورت کامل و برابر ۱، امکان حمله ۵، امکان کشف حمله ۱ به دلیل عدم امکان کشف حمله، نرخ آسیب‌پذیری ۴، زمان تا خرابی ۲، هزینه بازیابی ۵، میزان آسیب وارده ۵، مخاطره امنیتی این حمله برابر ۱۰۰خواهد بود.

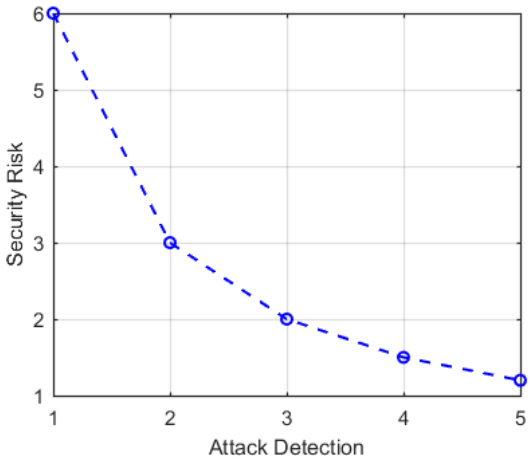
با رفع این آسیب‌پذیری، و تنزّل مقدار این مؤلفه به ۱، میزان مخاطره امنیتی این حمله برابر ۲۵ خواهد بود. همچنین با کاهش دانش مهاجم به مقدار ۰/۱ در مورد کد برنامه‌ریزی شده و حمله به سیستم، مقدار مخاطره امنیتی برابر ۱۰ خواهد بود.

نهایتاً با رفع آسیب‌پذیری سیستم و تعیین مقدار ۱ برای این مؤلفه، کاهش دانش مهاجم به‌صورت هم‌زمان (مقدار ۰/۱)، و توانایی کشف حمله توسط سیستم (مقدار ۵) و عدم تغییر مقدار سایر مؤلفه‌ها، مخاطره امنیتی برابر ۰/۵ خواهد بود.

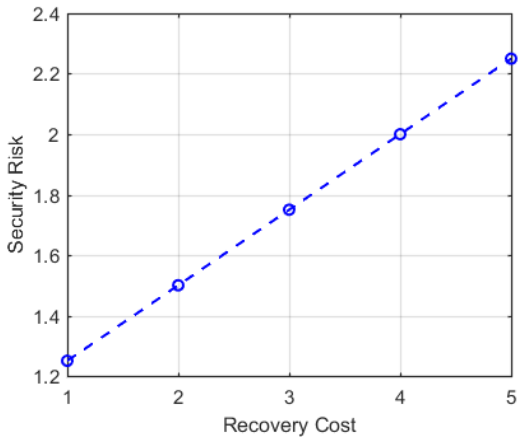


شکل (۴). تأثیر دانش مهاجم بر مخاطره امنیتی

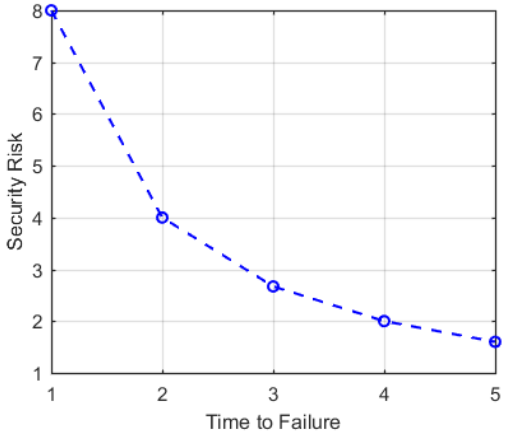
[1] Siemens
[2] Zero-day
[3] Worm
[4] Centrifuge frequency converter drives



شکل (۵). تأثیر کشف حمله بر مخاطره امنیتی



شکل (۶). تأثیر هزینه بازیابی بر مخاطره امنیتی



شکل (۷). تأثیر زمان تا خرابی بر مخاطره امنیتی

۴- نتیجه‌گیری

در این مقاله روشی برای ارزیابی کمّی مخاطره امنیتی در سامانه‌های سایبر - فیزیکی ارائه شده است. در این روش مؤلفه‌های بسیار مهمی که در مخاطره امنیت این سامانه‌ها تأثیرگذار هستند مدنظر قرار گرفته است. از جمله این مؤلفه‌ها می‌توان به دانش مهاجم، زمان تا خرابی سیستم، هزینه بازیابی بعد از وقوع حمله موفق، امکان حمله، امکان تشخیص حمله، خسارت وارده بر دارایی‌های سیستم اشاره کرد. نتایج آزمایشات انجام شده چگونگی تأثیر این مؤلفه‌ها بر مخاطره امنیت این سامانه‌ها را نشان داده است. به‌عنوان کار آینده قصد داریم با توسعه روش پیشنهادی به ارزیابی کیفی مخاطره نیز بپردازیم. همچنین از روش‌های تصمیم‌گیری چندمعیاره برای اولویت‌بندی مخاطرات امنیتی برای این سامانه‌ها بر اساس مؤلفه‌های مهم بپردازیم.

۵- مراجع

[1] F. Hu, Y. Lu, A.V. Vasilakos, Q. Hao, R. Ma, Y. Patil, ... & N.N. Xiong, "Robust cyber–physical systems: Concept, models, and implementation," FUTURE GENER COMP SY, vol. 56, pp. 449-475, 2016.

[2] J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends." MICROPROCESS MICROSY, vol. 77, p.103201, 2020.

[3] Y. Ashibani, Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions." COMPUT SECUR, vol. 68, pp.81-97, 2017

[4] X. Lyu, Y. Ding, S.H. Yang, "Safety and security risk assessment in cyber-physical systems." IET Cyber-Physical Systems: Theory & Applications, vol. 4, pp.221-232 2019.

[5] Bernardi, S., Gentile, U., Marrone, S., Merseguer, J., & Nardone, R. (2021). Security modelling and formal verification of survivability properties: Application to cyber–physical systems. *Journal of Systems and Software*, *171*, 110746.

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

[7] H. Orojloo, M. Abdollahi Azgomi, Predicting the behavior of attackers and the consequences of attacks against cyber-physical systems. *Security and Communication Networks*, vol. 9, pp. 6111-6136, 2016.

[8] H. Orojloo, M. Abdollahi Azgomi, "A stochastic game model for evaluating the impacts of security attacks against cyber-physical systems." Journal of Network and Systems Management, vol. 26, pp.929-965, 2018.

[9] M. Krotofil and et.al., "Vulnerabilities of cyber-physical systems to stale data-Determining the optimal time to launch attacks," *International Journal of Critical Infrastructure Protection*, vol. 7, pp. 213-232, 2014.

[10] B. Potteiger, A. Dubey, F. Cai, X. Koutsoukos, Z. Zhang, "Moving target defense for the security and resilience of mixed time and event triggered cyber–

physical systems security". COMPUT SECUR, vol. 96, p.101864, 2020.
[20] W. Wu, R. Kang, & Z. Li, "Risk assessment method for cyber security of cyber physical systems. In *2015 first international conference on reliability systems engineering (ICRSE)* (pp. 1-5). IEEE, 2015.
[21] K. Huang, C. Zhou, Y.C. Tian, S. Yang, Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems". IEEE T IND ELECTRON, vol. 65, pp. 8153-8162, 2018.
[22] X. Lyu, Y. Ding, S.H. Yang, "Bayesian network based C2P risk assessment for cyber-physical systems". IEEE Access, vol. 8, pp. 88506-88517, 2020.
[23] H. A. Kholidy, "Autonomous mitigation of cyber risks in the Cyber–Physical Systems". FUTURE GENER COMP SY, vol. 115, pp.171-187, 2021.
[24] H. Sepehrzadeh, "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, 2021.
[25] NCCIC, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ⟨https://us-cert.cisa.gov/ics⟩ (accessed 19 August 2022).
[26] M. Yampolskiy, P. Horváth, X.D. Koutsoukos, Y. Xue, and J. Sztipanovits, "A language for describing attacks on cyber-physical systems." *International Journal of Critical Infrastructure Protection*, vol. 8, pp.40-52, 2015.
[27] R. Alguliyev, Y. Imamverdiyev, L. and Sukhostat, "Cyber-physical systems and their security issues." COMPUT IND, 100, pp.212-223, 2018.
[28] M. Krotofil, J. and Larsen,. Are you threatening my hazards?. In *International Workshop on Security*. Springer, Cham, 2014, pp. 17-32.
physical systems." J SYST ARCHITECT", vol. 125, p.102420, 2022.
[11] A. Makkar, J. H. Park, "SecureCPS: Cognitive inspired framework for detection of cyber attacks in cyber–physical systems." INFORM PROCESS MANAG, vol. 59, p.102914, 2022.
[12] 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.
[13] C. Barreto, G. Schwartz, A.A. Cardenas, "Cyber-Risk: Cyber-Physical Systems Versus Information Technology Systems." In Safety, Security and Privacy for Cyber-Physical Systems (pp. 319-345). Springer, Cham.
[14] A. Humayed, J. Lin, F. Li, B. Luo, "Cyber-physical systems security—A survey". IEEE Internet of Things Journal, vol. 4, pp.1802-1831, 2017.
[15] H. Orojloo, M. Abdollahi Azgomi, "A method for evaluating the consequence propagation of security attacks in cyber–physical systems," Future Generation Computer Systems, vol. 67, pp. 57-71, 2017.
[16] A. Yeboah-Ofori, S. Islam, "Cyber Security Threat Modeling for Supply Chain Organizational Environments". Future Internet, vol. 11, 2019.
[17] R. Schlegel, S. Obermeier, and J. Schneider, Structured system threat modeling and mitigation analysis for industrial automation systems. In 2015 IEEE 13th International Conference on Industrial Informatics (INDIN) (pp. 197-203). IEEE, 2015.
[18] D.G. Rosado, A. Santos-Olmo, L.E., Sánchez, M.A. Serrano, et. all, "Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern". COMPUT IND, vol. 142, p.103715, 2022.
[19] A. Tantawy, S. Abdelwahed, A. Erradi, and K. Shaban, "Model-based risk assessment for cyber