مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال هشتم، شماره ۴، زمستان ۱۳۹۶؛ ص ۳۹۸-۳۸۷

ارائه مدلی برای ارزیابی حفاظت فیزیکی از تأسیسات حیاتی جهت پدافند غیرعامل در برابر تهدیدات فیزیکی و خرابکارانه

محمدحسین رنجبر[۱]، محمد مردانی شهربابک[۲*]، ابوالفضل پیرایش[۳]

۱- دانشجوی دکتری، دانشگاه شهید بهشتی ۲- دانشیار، دانشگاه جامع امام حسین (ع) ۳- استادیار، دانشگاه شهید بهشتی

(دریافت: ۹۵/۱۰/۰۵، پذیرش: ۹۵/۱۲/۰۲)

چکیده

یکی از مهم‌ترین روش‌های پدافند غیرعامل زیرساخت‌ها، حفاظت فیزیکی از تأسیسات حیاتی آن‌ها است. این حفاظت سبب می‌شود تا احتمال موفقیت آمیز بودن حمله فیزیکی و خرابکارانه کاهش یابد. در این مقاله مدلی کارآمد و اثربخش برای ارزیابی حفاظت فیزیکی تأسیسات حیاتی بر مبنای نقطه شناسایی بحرانی ارائه شده است. در این مدل نیازی به محاسبه احتمال موفقیت آمیز بودن حمله برای تمامی مسیرهای تهاجم به تأسیسات حیاتی مورد نظر نمی‌باشد. همچنین ویژگی‌ها و قابلیت‌های مهاجمین (خرابکاران) در محاسبه احتمال موفقیت آمیز بودن حمله به تأسیسات حیاتی در نظر گرفته شده است. برای محاسبات مدل و تعیین احتمال موفقیت آمیز بودن حمله به تأسیسات حیاتی از روش مونت‌کارلو استفاده شده است که سبب می‌شود تا نیازی به استفاده از روش‌های محاسباتی قطعی و پیچیده با احتمالات شرطی تو در تو نباشد. مدل ارائه شده توسط شبیه‌سازی با مدل‌های دیگر مقایسه شده است و نتایج مورد آزمون قرار گرفته است.

کلیدواژه‌ها: حفاظت فیزیکی، احتمال جلوگیری از حمله، احتمال موفقیت آمیز بودن حمله، تابع توزیع نرمال، روش مونت‌کارلو

Presenting a Model for Evaluation of the Physical Protection of Critical Installations for Passive Defense against Physical and Sabotage Threats

M. H. Ranjbar, M. Mardani*, A. Pirayesh
Imam Hossein University
(Received: 25/12/2016; Accepted: 20/02/2017)

Abstract

Physical protection of critical installations is one of the most important methods for passive defense of infrastructures. Physical protection reduces the success probability of a physical or sabotage attack. In this article, an efficient model is presented to evaluate the physical protection of critical installations based on critical detection point concept. In this model there is no need to calculate the success probability of the attack for all adversary paths of that critical installation. Furthermore, the abilities and capabilities of the saboteurs are also considered in calculating the success probability of an attack against the critical installation. Calculation of the model and determination of the success probability of attack against the critical installation is implemented by Monte-Carlo method which avoid the complex deterministic calculation methods with complex conditional probabilities. The simulation of presented model is compared with other models and the results are tested.

Keywords: Physical Protection, Attack Interruption Probability, Attack Success Probability, Normal Distribution Function, Monte-Carlo Method

*Corresponding Author E-mail: Mmardani@ihu.ac.ir

۱. مقدمه

کارکرد پیوسته و مطمئن زیرساخت‌های حیاتی نقش کلیدی در تأمین رفاه اجتماعی، بهره اقتصادی و امنیت ملی برای کشورها دارد. مسئله تأمین امنیت زیرساخت‌های حیاتی در سال‌های اخیر با توجه به افزایش فعالیت گروه‌های تروریستی، توجه زیادی را به خود معطوف کرده است [۶-۱]. کشورهای مختلف برنامه‌هایی برای دفاع از زیرساخت‌های اساسی خود در برابر تهدیدات آماده کرده‌اند که از جمله می‌توان به طرح ملی حفاظت از زیرساخت‌های ایالت متحده[1] و برنامه اتحادیه اروپا برای حفاظت از زیرساخت‌های بحرانی اشاره کرد. این برنامه‌ها شامل فازهای مختلف و معمولاً بلند مدتی برای مقابله با تهدیدات ناشی از حملات عامدانه و یا بلایای طبیعی علیه زیرساخت‌ها هستند. با وجود اینکه ممکن است تعاریف و اصطلاحات به‌کار رفته در این برنامه‌ها با هم متفاوت باشند، تمامی این برنامه‌ها شامل سه فاز اصلی آمادگی‌های قبل از وقوع بحران، اقدامات حین وقوع بحران و اقدامات پس از وقوع بحران ناشی از حمله یا بلایای طبیعی هستند.

به طور کلی در پدافند غیرعامل، آمادگی‌ها و اقدامات قبل از شروع بحران شامل سه مرحله پیش‌بینی، پیشگیری و هشدار است. مرحله پیش‌بینی بحران عبارت است شناسایی، رصد و تخمین تهدیدات علیه تأسیسات و زیرساخت‌ها که با توجه به ویژگی‌ها و مشخصات محیطی و محاطی این تأسیسات و تهدیداتی که علیه آن‌ها مطرح است، صورت می‌پذیرد. مرحله پیشگیری عبارت است از خنثی کردن تهدیدات از اولین مرحله شکل‌گیری تا مرحله قبل از وقوع بحران. به عنوان مثال فرض کنید حمله یک گروه تروریستی خارجی به عنوان یک تهدید علیه یک زیرساخت در داخل یک کشور شناسایی می‌شود. در این حالت اولین مرحله پیشگیری امن کردن مرزها جهت جلوگیری از ورود مهاجمین به داخل کشور است. با فرض عدم موفقیت اولین مراحل پیشگیری، حفاظت فیزیکی مناسب از تأسیسات مورد نظر به عنوان آخرین مرحله پیشگیری از وقوع بحران شناخته می‌شود. در نتیجه یکی از مهم‌ترین اقدامات جهت آمادگی قبل از وقوع بحران، حفاظت فیزیکی و یا مستحکم سازی تأسیسات است [۷]. حفاظت فیزیکی مناسب از تأسیسات سبب می‌شود که احتمال موفقیت آمیز بودن حمله به زیرساخت‌ها به میزان چشمگیری کاهش یابد. تمامی برنامه‌هایی که به پدافند زیرساخت‌ها می‌پردازند به حفاظت فیزیکی و نقش آن توجه ویژه دارند. مرحله هشدار نیز به منظور کسب آخرین آمادگی‌ها جهت مقابله با وقوع بحران انجام می‌پذیرد. مقابله با وقوع بحران با آمادگی کامل سبب کاهش خسارت ناشی از بحران می‌شود.

با توجه به محدود بودن منابع پدافند غیرعامل و همچنین تعدد اینگونه از تأسیسات، گام اول در تمامی برنامه‌های دفاع غیرعامل از زیرساخت‌ها، شناسایی تأسیسات حیاتی سامانه به منظور قرار گرفتن در اولویت مستحکم سازی است [۸ و ۹]. بدین منظور از روش‌هایی تحت عنوان ارزیابی آسیب‌پذیری و ارزیابی ریسک سامانه استفاده می‌شود [۱۲-۱۰]. در این روش‌ها، به منظور کمی سازی تحلیل‌ها نیاز است تا رابطه ریاضی میان حفاظت فیزیکی از تأسیسات حیاتی و احتمال موفقیت آمیز بودن حمله به آن‌ها تعیین گردد.

به عنوان مثال ازل و همکاران [۱۳] روشی برای ارزیابی آسیب‌پذیری زیرساخت آب و فاضلاب در برابر تهدیدات تروریستی با استفاده از نظریه ارزش چندگانه ارائه کرده‌اند. در این روش احتمال موفقیت آمیز بودن حمله به تأسیسات توسط توابع توزیع احتمال مثلثی مدل شده است که پارامترهای آن توسط متخصصان امنیتی تعیین می‌گردد. چن و همکاران [۱۴] احتمال موفقیت آمیز بودن حمله به تأسیسات سامانه قدرت را به صورت تابعی نزولی از میزان هزینه صورت گرفته برای حفاظت فیزیکی آن‌ها، ارائه کرده‌اند. متأسفانه تابع ارائه شده توسط آن‌ها کاملاً فرضی است و حاوی اطلاعات ارزشمندی نیست.

لانگفی و همکاران [۱۵] احتمال موفقیت آمیز بودن حمله به تأسیسات سامانه قدرت را به صورت تابعی دو متغیره $F(x,y)$ از میزان هزینه صورت گرفته برای حفاظت فیزیکی تأسیسات و منابع در دسترس مهاجمین، تعریف کرده‌اند. این تابع نیز همانند تابع ارائه شده در مرجع قبل، فرضی است.

در سالیان گذشته، مدل‌های نرم‌افزاری مختلفی برای ارزیابی حفاظت فیزیکی از تأسیسات حیاتی ارائه شده است که احتمال جلوگیری از حمله به تأسیسات را محاسبه می‌کنند [۱۶].

مدل‌های نرم‌افزاری EASI[2] و SAVI[3] از جمله مدل‌های نرم‌افزاری هستند که احتمال جلوگیری از حمله موفقیت آمیز را بر اساس تعیین نقطه شناسایی بحرانی سامانه حفاظت فیزیکی و احتمال تجمعی شناسایی، تخمین می‌زنند. یکی از معایب مدل‌های ارائه شده، لزوم محاسبه تمام مسیرهای تهاجم به صورت جداگانه است که برای تأسیساتی با مسیرهای تهاجم زیاد مشکل خواهد بود.

در سال‌های اخیر مدل‌های نرم‌افزاری دو بعدی و سه بعدی برای طراحی و ارزیابی سامانه حفاظت فیزیکی از تأسیسات بحرانی بر اساس همان مدل‌های EASI و SAVI ارائه شده است [۱۹-۱۷]. این مدل‌ها با افزایش درک شهودی از سامانه حفاظت

[1] National Infrastructure Protection Plan (Nipp)

[2] Estimate of Adversary Sequence Interruption

[3] Systematic Analysis of Vulnerability To Intrusion

فیزیکی، به طراحان کمک می‌کنند تا کارایی سامانه حفاظت فیزیکی را بالا ببرند. در این مدل‌ها حجم محاسبات به صورت تصاعدی با افزایش تعداد مش‌ها افزایش می‌یابد و نیاز است تا مش‌هایی غیر بهینه توسط روش‌های کاهش سناریو حذف گردند.

اغلب نرم‌افزارهای ارائه شده در این زمینه، توانایی‌ها و قابلیت‌های مهاجم (مهاجمین) را در ارزیابی سامانه حفاظت فیزیکی لحاظ نمی‌کنند. در این مقاله، مدلی کارآمد، اثربخش و ملموس برای ارزیابی حفاظت فیزیکی از تأسیسات حیاتی کشور بر اساس روش مونت‌کارلو[1] ارائه می‌شود.

ارائه مدل ریاضی برای ارزیابی حفاظت فیزیکی از تأسیسات سبب افزایش کارایی مراحل آمادگی قبل از وقوع بحران و اصلاح وضع موجود است که خود عاملی کنترل کننده در مقابل هوشمند است و کارایی سامانه حفاظت فیزیکی را تضمین می‌کند.

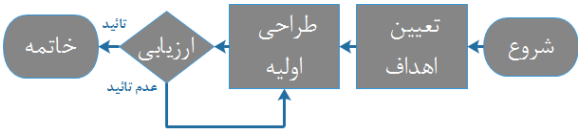
در این مدل با توجه به رفتار یک مهاجم هوشمند نیازی به محاسبه جداگانه مسیرهای تهاجم نیست و الگوریتم مسیرهای غیر بهینه تهاجم را حذف می‌نماید. همچنین سعی می‌شود قابلیت‌های مهاجمین به صورت تحلیلی در مدل لحاظ گردد.

در بخش دوم مبانی نظری و علمی حفاظت فیزیکی از تأسیسات بیان می‌گردد. در بخش سوم پس از تجزیه و تحلیل، مدلی ریاضی از رابطه حفاظت فیزیکی تأسیسات و موفقیت آمیز بودن حمله به آن‌ها ارائه می‌شود. در بخش چهارم مدل ارائه شده با استفاده از شبیه‌سازی مورد آزمون قرار می‌گیرد و درنهایت در بخش پنجم تحقیق، نتیجه‌گیری انجام خواهد گرفت.

۲. مبانی نظری و علمی تحقیق

۲-۱. حفاظت فیزیکی از تأسیسات حیاتی

حفاظت فیزیکی به تجهیزات و روش‌هایی اطلاق می‌گردد که برای حفاظت از تأسیسات در برابر دزدی، خرابکاری و حملات بدخواهانه به‌کار می‌روند. حفاظت فیزیکی مؤثر باید توسط الگویی روشمند پیاده‌سازی شود تا نتایج بهینه را در پی داشته باشد. پیاده‌سازی یک سامانه کارآمد حفاظت فیزیکی شامل گام‌های تعیین اهداف، طراحی اولیه، ارزیابی طرح و بازطراحی (در صورت لزوم) است که در شکل (۱) نشان داده شده است [۲۰].



شکل ۱. پیاده‌سازی یک سامانه کارآمد حفاظت فیزیکی

اهداف سامانه حفاظت فیزیکی به طور کلی ممانعت از اجرای موفقیت آمیز حمله مهاجم به تأسیسات مورد نظر است. این گام با شناخت ویژگی‌های تأسیسات مورد نظر، تعریف تهدیدات و شناسایی تهدیدات علیه تأسیسات مورد نظر محقق می‌شود.

طراحی اولیه سامانه حفاظت فیزیکی، استفاده بهینه از تجهیزات و روش‌ها به منظور تأخیر در ورود مهاجم، شناسایی ورود مهاجم و پاسخ به مهاجم است که در شکل (۲) نشان داده شده است [۲۱]. تأخیر به معنای تجهیزات و روش‌هایی است که در نفوذ فرد مهاجم به داخل تأسیسات، تأخیر ایجاد می‌کند. تأخیر توسط روش‌هایی مانند حصار، دیوار، سیم‌خاردار، قفل، استحکامات و غیره حاصل می‌شود.

شناسایی (آشکارسازی) به معنای فهمیدن و آگاه کردن نیروهای امنیتی از ورود مهاجم است. انواع حسگر و دوربین‌های مدار بسته جهت شناسایی ورود مهاجم به‌کار می‌روند.

پاسخ به معنای واکنش سریع نیروهای امنیتی جهت مقابله با مهاجمین و جلوگیری از اقدام موفقیت آمیز آنان است. برای تحقق این امر نیاز است که یک سامانه هشدار و همچنین نیروهای امنیتی آماده برای درگیر شدن با مهاجم (مهاجمین) وجود داشته باشد.

شکل ۲. طراحی سامانه حفاظت فیزیکی

به برآورد و آزمایش طرح پیاده شده به منظور سنجش میزان تحقق اهداف طرح، ارزیابی طرح اطلاق می‌گردد. این ارزیابی توسط روش‌های ارزیابی کیفی و کمی صورت می‌پذیرد. معمولاً تأسیساتی که بسیار با ارزش و حیاتی هستند، توسط روش‌های کمی و تأسیساتی با اولویت پایین‌تر با روش‌های کیفی ارزیابی می‌شوند. اگر نتایج ارزیابی نشان دهد که طراحی اولیه سامانه حفاظت فیزیکی اهداف را محقق نمی‌سازد، بازطراحی صورت

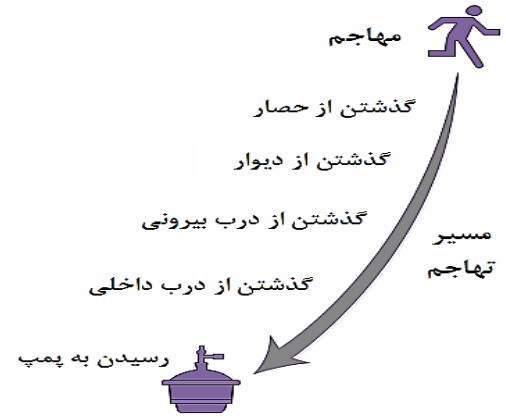
[1] Monte Carlo

می‌پذیرد. مباحث تعیین اهداف حفاظت فیزیکی و طراحی سامانه حفاظت فیزیکی در این مقاله نمی‌گنجد زیرا هدف این مقاله ارزیابی حفاظت فیزیکی موجود تأسیسات به منظور تعیین احتمال موفقیت آمیز بودن حمله به آن‌ها است.

۲-۲. ارزیابی حفاظت فیزیکی از تأسیسات حیاتی

برای ارزیابی سامانه‌های حفاظت فیزیکی از تأسیسات حیاتی، ابتدا باید مفهوم "مسیر تهاجم" تعریف شود. مسیر تهاجم روندی است که اگر مهاجم آن‌ها را طی کند، حمله موفقیت آمیزی به تأسیسات مورد نظر صورت پذیرفته است. به عنوان مثال، یک نمونه مسیر تهاجم برای نابود کردن یک پمپ بسیار حساس در تأسیسات آب و فاضلاب در شکل (۳) نشان داده شده است.

طی کردن مسیر تهاجم برای مهاجم با دشواری‌هایی همراه است. در واقع مهاجم برای رسیدن به هدف باید از لایه‌های مختلف حفاظتی عبور کند. هر کدام از این لایه‌ها که در شکل فوق نشان داده شده است، دارای عناصری برای ایجاد تأخیر در عبور مهاجم و یا شناسایی حضور مهاجم هستند. به عنوان مثال فرض کنید برای مسیر تهاجم نشان داده شده در شکل فوق، عناصر تأخیر و شناسایی لایه‌های حفاظتی در شکل (۴) نشان داده شده است.



شکل ۳. مسیر تهاجم برای نابود کردن یک پمپ حیاتی در تأسیسات آب و فاضلاب

معمولاً وجود عناصر تأخیر است که به لایه‌های حفاظتی در یک سامانه حفاظت فیزیکی معنا می‌بخشد. بنابراین در اغلب سامانه‌های حفاظت فیزیکی، هر لایه حفاظتی دارای عنصر تأخیر است ولی ممکن است دارای عنصر شناسایی باشد و یا نباشد (شکل (۴)).

شاخص کیفیت عملکرد عناصر تأخیر در یک سامانه حفاظت فیزیکی، مقدار زمانی است که این عناصر در نفوذ مهاجم تأخیر ایجاد می‌کنند. این زمان بر حسب دقیقه و یا ثانیه بیان می‌شود.

شاخص کیفیت عملکرد عناصر شناسایی سامانه حفاظت فیزیکی، قابلیت اطمینان این عناصر در شناسایی ورود مهاجم است که معمولاً با احتمال شناسایی وجود مهاجم بیان می‌گردد. همچنین شاخص عملکرد سامانه هشدار، قابلیت اطمینان سامانه هشدار در برقراری ارتباط و مطلع کردن نیروهای امنیتی از ورود مهاجم است.

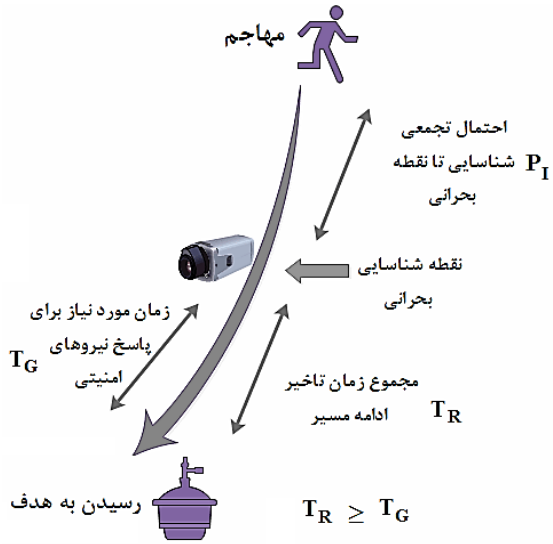
لایه	عناصر تاخیر	عناصر شناسایی
حصار	استحکامات حصار	سنسور حصار
درب دیوار	استحکامات دیوار	فاقد عنصر شناسایی
درب بیرونی	قفل و استحکامات درب	دوربین درب بیرونی
درب داخلی	قفل و استحکامات درب	دوربین درب داخلی
پمپ	استحکامات پمپ	فاقد عنصر شناسایی

شکل ۴. عناصر تأخیر و شناسایی لایه‌های حفاظتی مثال قبل

هدف مهاجم طی کردن کامل مسیر و انجام موفق عملیات به نحوی است که با کمترین احتمال ممانعت از سوی سامانه حفاظت فیزیکی مواجه شود. بدین منظور مهاجم (مهاجمین) ممکن است این راهبرد را انتخاب کنند که با حداکثر توان به تأسیسات مورد نظر حمله کنند و با نفوذ هر چه سریع‌تر به داخل مجموعه و بدون نگرانی از فعال شدن سامانه هشدار، قبل از رسیدن نیروهای امنیتی عملیات خود را انجام داده و از محل متواری شوند. در این حالت مهاجم سعی می‌کند تا زمان طی کردن مسیر را کمینه سازد.

راهبرد دیگری نیز وجود دارد که در آن مهاجم سعی می‌کند بدون توجه به زمان طی مسیر، احتمال شناسایی و فعال شدن سامانه هشدار را کمینه سازد و با موفقیت عملیات خود را انجام دهد. حالت اول معمولاً در عملیات‌های تروریستی و حالت دوم معمولاً در سرقت‌ها و خرابکاری‌های حرفه‌ای رخ می‌دهد. در حالت کلی راهبرد بهینه تهاجمی این است که مهاجم سعی کند تا قبل از اولین شناسایی یا اولین به صدا در آمدن آژیر هشدار، احتمال شناسایی و فعال شدن سامانه هشدار را کمینه سازد و بعد از به صدا در آمدن اولین آژیر، زمان طی کردن بقیه مسیر را کمینه سازد. در نتیجه سامانه حفاظت که از چندین لایه عناصر تأخیر و شناسایی تشکیل شده است باید به گونه‌ای باشد که در نقطه‌ای که به آن نقطه بحرانی شناسایی می‌گویند، زمان تأخیر ادامه مسیر مهاجم به اندازه‌ای باشد که نیروهای امنیتی قادر به

پاسخ و مقابله به مهاجمین باشند. این مفهوم در شکل (۵) نشان داده شده است.



شکل ۵. مفهوم نقطه شناسایی بحرانی

بنابراین منطقی است که سامانه حفاظت به گونه‌ای طراحی شود که تا حد ممکن تا قبل از نقطه بحرانی، عناصر شناسایی به خوبی عمل کنند و بعد از نقطه بحرانی عناصر تأخیر حداکثر تأخیر ممکن در مسیر حرکت مهاجم را ایجاد کنند.

اگر مهاجم از راهبرد بهینه تهاجمی که در بالا به آن اشاره شد پیروی نکند، تأثیرگذاری سامانه حفاظت فیزیکی بیشتر می‌شود. به عنوان مثال اگر مهاجم از همان ابتدا به سرعت عمل کند و به کم کردن احتمال شناسایی توجه نکند، همان ابتدای مسیر و قبل از رسیدن به نقطه بحرانی شناسایی می‌شود و سامانه هشدار نیروهای امنیتی را فعال می‌کند و در این حالت زمان برای پاسخگویی به مهاجم بیشتر می‌شود.

زمان تأخیر ادامه مسیر از نقطه بحرانی و احتمال تجمعی شناسایی از ابتدای مسیر تا نقطه بحرانی توسط روابط زیر محاسبه می‌شوند:

$$T_R = \sum_{i=k}^{m} T_i \qquad (۱)$$

$$P_I = (1 - \prod_{i=1}^{k} P_{NDi}) \qquad (۲)$$

که در آن، P_{NDi} احتمال عدم شناسایی مهاجم در نقطه i از مسیر است و k نقطه بحرانی شناسایی است.

فرض کنید در مثال قبل، زمان‌های تأخیر و احتمالات شناسایی عناصر تأخیر و شناسایی نشان داده شده در شکل (۴)، به صورت جدول (۱) است. همچنین فرض کنید زمان مورد نیاز برای پاسخ نیروهای امنیتی ۵ دقیقه است.

جدول ۱. زمان تأخیر و احتمال شناسایی در مثال مورد نظر

لایه	زمان تأخیر	احتمال شناسایی P_D و عدم شناسایی P_{ND}	
حصار	۱ دقیقه	۰/۴	۰/۶
دیوار	۳ دقیقه	۰	۱
در بیرونی	۲ دقیقه	۰/۸	۰/۲
در داخلی	۳ دقیقه	۰/۸	۰/۲
پمپ	۱ دقیقه	۰	۱

در این صورت درب بیرونی نقطه شناسایی بحرانی است. مهاجم برای گذشتن از درب بیرونی، درب داخلی و نابود کردن پمپ جمعاً به ۶ دقیقه زمان نیاز دارد که این زمان از زمان پاسخ نیروهای امنیتی بیشتر است (T_R=6 min).

فرض می‌شود که با زودتر رسیدن نیروهای امنیتی قطعاً از موفقیت مهاجم (مهاجمین) جلوگیری می‌شود. در نتیجه می‌توان ادعا کرد که احتمال شناسایی ورود مهاجم تا درب بیرونی برابر با احتمال جلوگیری از حمله موفقیت آمیز مهاجم است. احتمال تجمعی شناسایی ورود مهاجم تا نقطه بحرانی توسط رابطه (۲) محاسبه می‌شود. در اینجا این احتمال برابر با ۸۸ درصد است و به صورت زیر محاسبه می‌شود:

$$P_I = (1-(0.6\times1\times0.2)) = 0.88 \qquad (۳)$$

بنابراین در این مثال احتمال جلوگیری از حمله مهاجم برابر ۸۸ درصد و احتمال موفقیت آمیز بودن حمله برابر با ۱۲ درصد است. در همین مثال اگر زمان پاسخ نیروهای امنیتی به ۳ دقیقه کاهش یابد، نقطه شناسایی بحرانی درب داخلی می‌شود و احتمال جلوگیری از حمله مهاجم به ۹۷/۶ درصد افزایش پیدا می‌کند. روش نقطه شناسایی بحرانی و رابطه‌های (۱ و ۲)، پایه و اساس روش‌های ارزیابی سامانه حفاظت فیزیکی تأسیسات است [۱۶].

۳. تجزیه و تحلیل و ارائه مدل

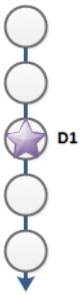
چندین مدل نرم‌افزاری برای ارزیابی کمی سامانه‌های حفاظت فیزیکی تأسیسات وجود دارد. بیشتر این مدل‌های نرم‌افزاری از یک فرمت مشابه که بر مبنای نقطه شناسایی بحرانی است، پیروی می‌کنند. برای نمونه یکی از این مدل‌های نرم‌افزاری که در آزمایشگاه ساندیا ایالات‌متحده نوشته شده است، مدل EASI است [۲۲]. در این مدل زمان پاسخ نیروهای امنیتی و زمان‌های تأخیر عناصر تأخیر سامانه حفاظت فیزیکی به صورت توابع توزیع احتمال نرمال (گوسی)، مدل می‌شوند و با توجه به توانایی عناصر شناسایی در تشخیص و آشکارسازی مهاجم، احتمال جلوگیری از حمله مهاجم برآورد می‌شود.

۳-۱. ارائه هسته اصلی مدل

مدل ارائه شده در این مقاله، بر مبنای روش مونت‌کارلو است [۲۳]. روش مونت‌کارلو روشی محاسباتی است که بر اساس تولید چند و چند باره متغیرهای حالت تصادفی و محاسبه جواب عددی مسئله با استفاده از این متغیرهای تصادفی، عمل می‌کند.

روش مونت‌کارلو در حل مسائلی که با عدم قطعیت زیادی مواجه هستند، به‌کار می‌رود [۲۴].

برای مدل‌سازی سامانه حفاظت فیزیکی، لایه‌هایی از سامانه که دارای عناصر تأخیر هستند را با دایره ○ نشان می‌دهیم و لایه‌هایی که دارای هر دو عنصر تأخیر و شناسایی هستند را با دایره و ستاره ✪ نشان می‌دهیم. ابتدا فرض کنید در مسیر مهاجم تنها یک عنصر شناسایی مانند حسگر یا دوربین وجود دارد. این حالت در شکل (۶) نشان داده شده است.



شکل ۶. مسیر تهاجم با یک نقطه شناسایی

زمان پاسخ نیروهای امنیتی و زمان‌های تأخیر عناصر تأخیر مسیر، یک عدد ثابت و مشخص نیستند و دارای عدم قطعیت می‌باشند. بنابراین این زمان‌ها باید به صورت تابع توزیع مناسب نشان داده شوند. یک توزیع احتمالی مناسب برای زمان‌های تأخیر، توزیع نرمال است که از دو پارامتر میانگین و انحراف معیار تشکیل شده است. به عنوان نمونه در جدول (۱) زمان تأخیر گذشتن از درب بیرونی می‌تواند به صورت تابع توزیع نرمال با میانگین ۳ دقیقه و انحراف معیار ۱ دقیقه بیان شود.

تعیین دقیق میانگین و انحراف معیار باید با استفاده از اطلاعات موجود از نفوذ در چنین سازه‌ای انجام پذیرد. در صورت عدم وجود اطلاعات در این باره، باید با استفاده از روشی موسوم به "تیم قرمز[1]"، این اطلاعات تهیه شود. تیم قرمز روشی است که در آن یک گروه عملیاتی در نقش مهاجمین به تأسیسات مد نظر حمله فرضی انجام می‌دهند تا اطلاعاتی از کارایی سامانه حفاظت به‌دست آید. همچنین شبیه‌سازی‌هایی نیز می‌تواند بدین منظور صورت پذیرد.

بعد از مشخص شدن پارامترهای توابع توزیع نرمال برای زمان‌های تأخیر عناصر تأخیر و زمان پاسخ نیروهای امنیتی، دو عدد تصادفی با توزیع نرمال تولید می‌شود. یکی از این اعداد تصادفی نشانگر زمان پاسخ نیروهای امنیتی است (T_G) و دیگری نشانگر زمان تأخیر باقیمانده از نقطه شناسایی تا هدف است (T_R). تولید اعداد تصادفی با توزیع نرمال در نرم‌افزار متلب با دستور Normrnd(μ,σ) انجام می‌پذیرد که μ میانگین و σ انحراف معیار است.

برای تعیین میانگین و انحراف معیار زمان تأخیر باقیمانده از نقطه شناسایی تا هدف بدین صورت عمل می‌شود که مطابق خاصیت جمع توابع توزیع نرمال، میانگین زمان‌های تأخیر عناصر تأخیر باقیمانده تا هدف با هم جمع می‌شوند و همچنین انحراف معیار آن‌ها نیز با هم جمع می‌شود [۲۵].

$$\mu_{T_R} = \mu_{T_k} + \mu_{T_{k+1}} + ... + \mu_{T_m}$$
$$\sigma_{T_R} = \sigma_{T_k} + \sigma_{T_{k+1}} + ... + \sigma_{T_m} \quad (۴)$$

دو عدد تصادفی تولید شده با هم مقایسه می‌شوند. اگر عدد تصادفی متناظر با T_R از عدد تصادفی تولید شده متناظر با T_G بیشتر باشد، احتمال جلوگیری از حمله مهاجم برابر با احتمال شناسایی عنصر شناسایی است و در غیر این صورت احتمال جلوگیری از حمله مهاجم برابر با صفر خواهد بود. رابطه زیر این مطلب را به صورت ریاضی نشان می‌دهد:

$$p_G = Normrnd(\mu_{T_G}, \sigma_{T_G})$$
$$p_R = Normrnd(\mu_{T_R}, \sigma_{T_R})$$
$$\begin{cases} \text{if} \quad p_R \geq p_G & P_I = P_{Dk} \\ else & P_I = 0 \end{cases} \quad (۵)$$

احتمال شناسایی عناصر شناسایی مانند حسگر و یا دوربین‌های مداربسته، بر اساس کاتالوگ مورد ادعای شرکت سازنده تعیین می‌شود. البته در این مورد نیز آزمایش‌ها و شبیه‌سازی‌هایی می‌تواند صورت پذیرد.

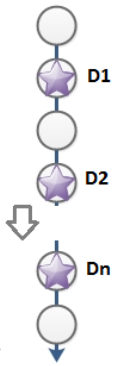
مطابق روش مونت‌کارلو، تولید این اعداد تصادفی چندین هزار بار مرتبه تکرار می‌شود و درنهایت میانگین P_I های به‌دست آمده به عنوان احتمال جلوگیری از حمله مهاجم برای این سامانه حفاظت پذیرفته می‌شود.

برای چنین سامانه حفاظت فیزیکی که متشکل از یک عنصر شناسایی است، احتمال موفقیت آمیز بودن حمله به سادگی توسط رابطه زیر به‌دست می‌آید:

$$P_S = 1 - P_I \quad (۶)$$

[1] Red Team

مدل را مقداری پیچیده‌تر می‌سازیم و فرض می‌شود که سامانه حفاظت فیزیکی، متشکل از n عنصر شناسایی باشد. این حالت در شکل (۷) نشان داده شده است.



شکل ۷. مسیر تهاجم با n نقطه شناسایی

در این حالت این‌گونه عمل می‌شود که همانند قبل یک عدد تصادفی برای T_G تولید می‌شود. همچنین به ازای هر n نقطه شناسایی، عددی تصادفی برای زمان باقیمانده از آن نقطه تا هدف تولید می‌شود.

$$\begin{aligned} p_G &= Normrnd\left(\mu_{T_G}, \sigma_{T_G}\right) \\ p_{R1} &= Normrnd\left(\mu_{T_{R1}}, \sigma_{T_{R1}}\right) \\ p_{R2} &= Normrnd\left(\mu_{T_{R2}}, \sigma_{T_{R2}}\right) \\ &\cdot \\ &\cdot \\ &\cdot \\ p_{Rn} &= Normrnd\left(\mu_{T_{Rn}}, \sigma_{T_{Rn}}\right) \end{aligned} \qquad (۷)$$

همانند قبل تمامی اعداد تصادفی تولید شده برای نقاط مختلف شناسایی مسیر، با عدد تصادفی تولید شده متناظر با T_G مقایسه می‌شوند و احتمال جلوگیری از حمله مهاجم برای آن نقطه شناسایی به‌دست می‌آید.

$$\begin{aligned} &\begin{cases} \text{if} \quad p_{R1} \geq p_G & P_{I1} = P_{D1} \\ else & P_{I1} = 0 \end{cases} \\ &\begin{cases} \text{if} \quad p_{R2} \geq p_G & P_{I2} = P_{D2} \\ else & P_{I2} = 0 \end{cases} \\ &\cdot \\ &\begin{cases} \text{if} \quad p_{Rn} \geq p_G & P_{In} = P_{Dn} \\ else & P_{In} = 0 \end{cases} \end{aligned} \qquad (۸)$$

این فرایند چند هزار بار تکرار است و میانگین P_{Ik}ها به عنوان احتمال جلوگیری از حمله برای آن نقطه شناسایی پذیرفته می‌شود.

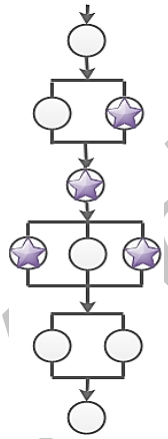
درنهایت احتمال جلوگیری از حمله مهاجم برای کل سامانه، توسط احتمالات شرطی به صورت زیر محاسبه می‌شود:

$$P_I = P_{I1} + \sum_{i=2}^{n}\left[\left(\prod_{j=1}^{i-1}(1-P_{Dj})\right)\times P_{Ii}\right] \qquad (۹)$$

برای سامانه‌ای با دو عنصر شناسایی رابطه فوق به صورت زیر است:

$$P_I = P_{I1} + (1-P_{D1})\times P_{I2} \qquad (۱۰)$$

نکته‌ای که در ادامه باید به آن اشاره کرد، این است که مهاجم معمولاً می‌تواند از چندین مسیر جداگانه خود را به هدف برساند. به عنوان مثال، مهاجم برای ورود به یک ساختمان گزینه‌های درب، دیوار، پنجره و سقف را می‌تواند انتخاب کند. بنابراین مسیر تهاجمی که در شکل (۳) نشان داده شده است یکی از مسیرهای تهاجم به پمپ حیاتی است و مسیرهای دیگری نیز ممکن است وجود داشته باشد. این مطلب در شکل (۸) نشان داده شده است.



شکل ۸. مسیرهای متفاوت برای رسیدن به یک سامانه فرضی

در مدل‌های نرم‌افزاری ارائه شده همانند EASI، احتمال جلوگیری از حمله مهاجم برای هر مسیر به صورت جداگانه باید محاسبه شود و بدترین حالت[1] (کمترین احتمال) به عنوان جواب نهایی برای ارزیابی سامانه حفاظت فیزیکی پذیرفته می‌شود.

همان‌طور که قبلاً عنوان شد، در یک حمله هوشمندانه، مهاجم در ابتدا سعی می‌کند احتمال شناخته شدن ورود را کاهش دهد و پس از شناخته شدن توسط اولین عنصر آشکارساز، سعی می‌کند تا زمان طی بقیه مسیر را کاهش دهد.

[1] Worst Case

در این مقاله برای مسیرهای مختلف مهاجم اینگونه عمل می‌شود که مهاجم در ابتدا مسیرهایی که احتمال شناسایی کمتری دارند را انتخاب و پس از اولین شناسایی، مسیرهایی که کمترین تأخیر را دارند، بر می‌گزینند. این رویکرد محاسباتی موجب می‌شود تا لازم نباشد تمامی مسیرها جداگانه مدل‌سازی و محاسبه شوند. در این حالت الگوریتم، مسیرهای غیر بهینه از دید مهاجم را حذف می‌نماید که سبب کاهش حجم و زمان محاسبات خواهد شد.

برای مدل‌سازی چنین حالتی، یک پرچم[1] باینری را به اولین شناسایی نسبت داده می‌شود. اگر این عدد باینری برابر با صفر باشد به معنی شناخته نشدن و اگر یک شود به معنی اولین شناسایی است. با شروع از آغاز مسیر، برای تمامی نقاط شناسایی لایه‌های مختلف، یک عدد تصادفی معمولی (توزیع یکنواخت) بین صفر و یک تولید می‌کنیم. فرض کنید احتمال شناسایی نقطه اول ۰/۹ باشد. اگر عدد تصادفی بین صفر تا ۰/۹ باشد به معنی این است که فرد مهاجم در آن نقطه، شناسایی می‌شود و پرچم باینری ۱ می‌گردد. اگر عدد تصادفی بین ۰/۹ و ۱ باشد، در این صورت مهاجم شناسایی نشده و پرچم باینری صفر است. تا زمانی که عدد باینری صفر باشد، مهاجم مسیرهای با احتمال شناسایی کمتر را بر می‌گزینند و به محض ۱ شدن عدد باینری، مهاجم مسیرهای با تأخیر کمتر را بر می‌گزینند.

$$\begin{aligned} &for\ i = 1:\mathrm{n} \\ &\text{if} \quad \mathrm{norm}(0,1) < P_{Di} \\ &flag = 1 \\ &else \\ &flag = 0 \end{aligned} \tag{۱۱}$$

مطابق روش مونت‌کارلو این روند چند هزار بار در الگوریتم تکرار می‌شود. یکی از مزیت‌های استفاده از روش مونت‌کارلو در این مدل در اینجاست که می‌توان شناخته شدن و یا نشدن مهاجم توسط عناصر شناسایی (صفر و یک شدن پرچم) را به صورت یک متغیر تصادفی تولید کرد و بقیه مسیر تهاجم را با آن متغیر تصادفی ادامه داد. در صورتی که برای استفاده از روش‌های احتمالی جبری (نه تصادفی) می‌بایست محاسبات را بر مبنای احتمالات شرطی تو در تو و پیچیده حل کرد که برای سامانه‌هایی با تعداد مسیر تهاجم زیاد عملاً غیر ممکن است.

۳-۲. در نظر گرفتن قابلیت‌های (مهاجم) مهاجمین

در اغلب قریب به اتفاق مدل‌های نرم افزاری ارائه شده، توانایی‌ها و قابلیت‌های مهاجم (مهاجمین) در نظر گرفته نمی‌شود. تعداد مهاجمین، نوع سلاح آن‌ها مهارت و تجهیزات آن‌ها، قابلیت‌های مهاجمین را شکل می‌دهد.

نقطه شناسایی بحرانی که اساس کار مدل‌های نرم‌افزاری است، با یک فرض بسیار مهم همراه است که "با زودتر رسیدن نیروهای امنیتی قطعاً از موفقیت مهاجم (مهاجمین) جلوگیری می‌شود".

این فرض در مواردی می‌تواند درست نباشد. در مواردی که تعداد مهاجمین از نیروهای امنیتی بیشتر است و یا تسلیحات مهاجمین از نیروهای امنیتی سنگین‌تر است، مهاجمین می‌توانند با شکست دادن نیروهای امنیتی به هدف خود نیز برسند و حمله موفقیتی آمیز به عنصر حیاتی مورد نظر داشته باشند.

همچنین توانایی مهاجمین بر پارامترهایی مانند زمان تأخیر عناصر تأخیر و احتمال شناسایی عناصر شناسایی تأثیر می‌گذارد.

بنابراین نیاز است تا توانایی‌ها و قابلیت‌های مهاجم در مدل در نظر گرفته شود.

بدین منظور نبرد تن به تن مهاجمین و نیروهای امنیتی این گونه مدل می‌شود که تعداد افراد نیروهای امنیتی و تعداد افراد مهاجمین و همچنین نوع سلاح هر دو گروه که می‌تواند سرد و یا گرم باشد، به عنوان ورودی مدل مشخص می‌شود. اگر گروهی دارای سلاح گرم باشد و گروه دیگری دارای سلاح سرد، قطعاً بدون توجه به تعداد افراد هر گروه، گروهی که دارای سلاح گرم است گروه دیگر را شکست می‌دهد.

از سوی دیگر، اگر سلاح هر دو گروه همسان باشد، گروهی که تعداد افراد بیشتری دارد برنده خواهد شد. در صورت برابر بودن تمامی شرایط، یک قرعه تصادفی نشانگر برنده خواهد بود که توسط روش مونت‌کارلو به راحتی انجام می‌شود.

درنهایت اگر نیروهای امنیتی برنده نبرد تن به تن باشند، رابطه (۵) به همان صورت باقی خواهد ماند. اگر مهاجمین برنده نبرد تن به تن باشند، با زودتر رسیدن نیروهای امنیتی نیز احتمال جلوگیری از حمله برابر صفر خواهد بود. بنابراین در حالت کلی می‌توان رابطه (۵) را به شکل رابطه (۱۲) بازنویسی کرد.

$$\begin{aligned} &p_G = Normrnd\left(\mu_{T_G}, \sigma_{T_G}\right) \\ &p_R = Normrnd\left(\mu_{T_R}, \sigma_{T_R}\right) \\ &\begin{cases} \text{if} \quad p_R \geq p_G \quad \& \, Guards\ \ Win & P_I = P_D \\ else & P_I = 0 \end{cases} \end{aligned} \tag{۱۲}$$

تعداد مهاجمین و تجهیزات آن‌ها می‌تواند بر زمان‌های تأخیر و احتمالات شناسایی نیز تأثیر بگذارد. افزایش تعداد مهاجمین معمولاً سبب کاهش زمان تأخیر عبور از لایه‌های حفاظتی و

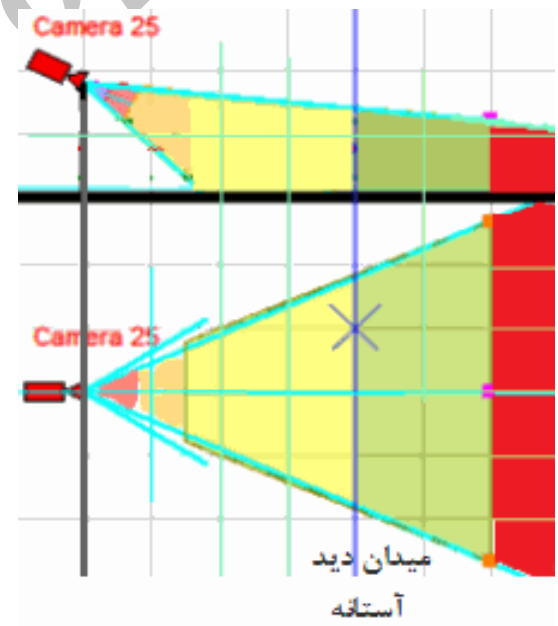
[1] Flag

افزایش احتمال شناخته شدن توسط عناصر شناسایی می‌شود. همچنین تجهیزات مهاجمین در نفوذ به لایه‌های حفاظتی، زمان تأخیر عبور از لایه‌های حفاظتی را تحت تأثیر قرار می‌دهد.

مدل‌سازی دقیق تأثیر قابلیت‌های مهاجمین بر روی پارامترهای تأخیر و شناسایی، پیچیده است. این مدل‌سازی به نوع فناوری استفاده شده در عناصر تأخیر و شناسایی نیز بسیار وابسته است و نیاز به شبیه‌سازی‌های دقیق دارد.

به عنوان نمونه، یک ابزار مناسب برای شبیه‌سازی عناصر شناسایی دوربین‌های مداربسته، نرم‌افزار VideoCAD 8.2 است [۲۶]. برای شبیه‌سازی و طراحی حفاظت فیزیکی با استفاده از دوربین‌های مداربسته، نیاز است تا مفاهیمی مانند فاصله کانونی دوربین، فرمت دوربین، میدان دید، میدان دید آستانه، توان تفکیک و ... تعریف شوند [۲۷].

طبق دستورالعمل‌های امنیتی، برای تشخیص وجود یک فرد باید حداقل ۱۰ درصد از پیکسل‌های تصویر دوربین توسط فرد با رنگی غیر از رنگ زمینه اشغال شود. در حالت کلی میدان دید افقی و عمودی یک دوربین در شکل (۹) نشان داده شده است.



شکل ۹. میدان دید یک دوربین مداربسته

در شکل فوق ناحیه‌ای که با رنگ زرد مشخص شده است (میدان دید آستانه)، ناحیه‌ای است که فرد در صورت قرارگیری در آن با احتمال بالایی شناسایی می‌شود. در نواحی بعد و قبل از ناحیه زرد، با توجه به اشغال کمتر از ۱۰ درصدی پیکسل‌های تصویر توسط فرد، احتمال شناسایی فرد کاهش می‌یابد. با توجه به محل استقرار دوربین مداربسته و مسیر حرکت مهاجم (مهاجمین)، می‌توان احتمال شناسایی مهاجم توسط دوربین را با استفاده از شبیه‌سازی و با توجه به تعداد پیکسل اشغال شده در تصویر، محاسبه کرد [۲۶].

افزایش تعداد مهاجمین سبب افزایش تعداد پیکسل اشغال شده آن‌ها در تصویر می‌شود که سبب افزایش احتمال شناسایی آن‌ها می‌گردد. مهاجمین هوشمند با دانستن عملکرد دوربین، سعی می‌کنند تا مساحت اشغال شده خود در تصویر را کاهش دهند. بنابراین مهاجمین در یک خط و پشت سر هم از مسیری که کمترین احتمال شناسایی را دارد، حرکت می‌کنند.

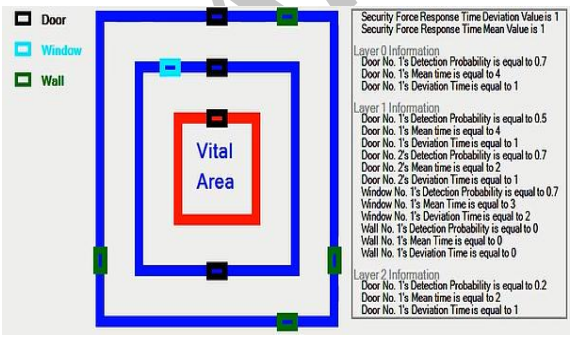
می‌توان از روش‌های مشابه برای شبیه‌سازی دیگر عناصر شناسایی مانند حسگرها استفاده کرد.

۳-۳. تبدیل مدل ارائه شده به نرم‌افزار دو بعدی

در این مقاله، به منظور افزایش درک شهودی از سامانه حفاظت فیزیکی، یک نرم‌افزار مستقل با امکان نمایش و ارزیابی سامانه حفاظت فیزیکی به صورت دو بعدی نوشته شده است. این نرم‌افزار توسط زبان برنامه‌ریزی C# نوشته شده و تحت فرمت exe و مستقل از نرم‌افزارهای دیگر قابل اجرا است.

با اجرای این نرم‌افزار، محیطی باز می‌گردد که از کاربر اطلاعاتی نظیر تعداد لایه‌های سامانه حفاظت فیزیکی، عناصر تأخیر و شناسایی لایه‌های سامانه حفاظت فیزیکی، تعداد افراد و تسلیحات نیروهای امنیتی و زمان پاسخ آن‌ها، تعداد افراد و تسلیحات نیروهای مهاجم و همچنین معماری سامانه‌ای که باید مورد حفاظت واقع شود را دریافت می‌کند.

پس از دریافت این اطلاعات، نرم‌افزار شکل دو بعدی سامانه حفاظت فیزیکی را رسم می‌کند و تعداد مسیرهای تهاجم به سامانه مشخص می‌کند (شکل (۱۰)).



شکل ۱۰. نمای دو بعدی سامانه حفاظت فیزیکی در نرم‌افزار

نرم‌افزار برای حل مسئله ابتدا سامانه حفاظت فیزیکی را توسط مش‌هایی با ابعاد نیم مترمربع، مش‌بندی می‌کند. سپس با استفاده از مشخصات سامانه حفاظت فیزیکی (فاصله لایه‌ها، زمان تأخیر عناصر و ...)، حرکت مهاجم و سرعت حرکت آن را مدل‌سازی می‌کند. مهاجم به صورت یک پیکسل از این

مش‌بندی، از نقطه شروع تهاجم تا نقطه رسیدن به هدف، حرکت می‌کند. در مدل‌سازی حرکت مهاجم، هوشمندی مهاجم در انتخاب مسیر بهینه و همچنین قابلیت‌های مهاجم در طی کردن مسیر در نظر گرفته می‌شود.

در نهایت نرم‌افزار با استفاده از مدل ارائه شده (روابط(۱۲-۷))، احتمال جلوگیری از حمله موفقیت آمیز برای بدترین مسیر تهاجم را با یک بار حل مسئله، محاسبه می‌کند و به عنوان خروجی تحویل می‌دهد.

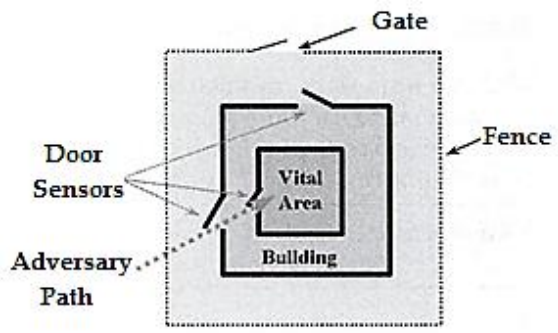
۴. آزمون مدل با استفاده از شبیه‌سازی

برای نشان دادن کارایی مدل ارائه شده، ابتدا آن را با نتایج به‌دست آمده توسط مدل EASI مقایسه می‌شود. در ادامه مدل ارائه شده با نتایج به‌دست آمده در مقاله سال ۲۰۱۶ مقایسه می‌گردد [۱۹].

۴-۱. مقایسه مدل ارائه شده با مدل EASI

در شکل (۱۱) یک سامانه حفاظت فیزیکی ساده نشان داده شده است [۱۶]. سامانه حفاظت فیزیکی نشان داده شده در این شکل شامل یک حصار است که دور تا دور ساختمانی کشیده شده است. این ساختمان دارای دو درب ورود و خروج است که هر دو به حسگرهایی با قابلیت شناسایی ورود مهاجم با احتمال ۹۰ درصد، مجهز هستند.

در داخل این ساختمان یک اتاق بسیار حیاتی وجود دارد که دارای یک درب با حسگری با قابلیت شناسایی ورود مهاجم با احتمال ۹۰ درصد است. یکی از مسیرهای تهاجم برای این سامانه در شکل (۱۱) مشخص شده است.



شکل ۱۱. یک نمونه سامانه حفاظت فیزیکی [۱۶]

در شکل زیر محیط نرم‌افزار EASI برای مسیر تهاجم مورد نظر، نشان داده شده است. زمان‌های تأخیر و احتمالات شناسایی در شکل (۱۲) نشان داده شده‌اند.

Estimate of Adversary Sequence Interruption

Probability of Guard Communication	Response Force Time (in Seconds)	
	Mean	Standard Deviation
0.95	300	90

Task	Description	P(Detection)	Delays (in Seconds): Mean:	Standard Deviation
1	Cut Fence	0	10	3
2	Run to Building	0	12	3.6
3	Open Door	0.9	90	27
4	Run to Vital Area	0	10	3
5	Open Door	0.9	90	27
6	Sabotage Target	0	120	36
7				
8				

Probability of Interruption: 0.476040779

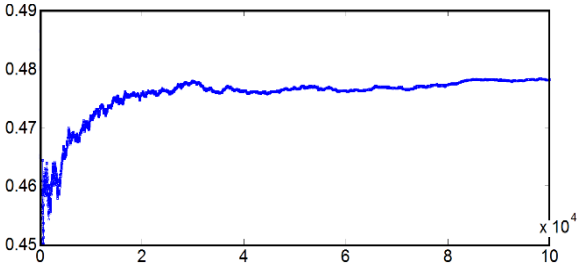
شکل ۱۲. محیط نرم‌افزار EASI برای مسیر تهاجم مورد نظر [۱۶]

در بالای صفحه نرم‌افزار EASI احتمال برقراری ارتباطات نیروهای امنیتی برابر با ۰/۹۵ تعیین شده است. این بدین معناست که آشکارسازی مهاجم توسط عناصر شناسایی توسط سامانه ارتباطی یا آژیری با قابلیت اطمینان ۰/۹۵ به نیروهای امنیتی اطلاع داده می‌شود. می‌توان قابلیت اطمینان سامانه ارتباطی را به راحتی در احتمال شناسایی حسگرها (دوربین‌ها) ضرب کرد و نتیجه را به عنوان احتمال شناسایی عناصر پذیرفت. در اینجا احتمال شناسایی عناصر، ۰/۸۵۵ می‌گردد. همان‌طور که در شکل (۱۲) نشان داده شده است، برای چنین سامانه‌ای احتمال جلوگیری از حمله برابر با ۰/۴۷۶ است. حال با استفاده از مدل ارائه شده در این مقاله (روابط (۹-۷)) و با یک صد هزار تکرار، مسیر تهاجم نشان داده شده در شکل (۱۱) به صورت زیر کدنویسی می‌گردد (شکل (۱۳)):

```
clear all;
i=1;
PI1tot=0;
PI1ave=0;
PI2tot=0;
PI2ave=0;
for i=1:100000;
pG=normrnd(300,90);
pR1=normrnd(310,93);
pR2=normrnd(210,63);
if pR1>pG
   PI1=.855;
else
      PI1=0;
end

if pR2>pG
   PI2=.855;
else
      PI2=0;
end
      PI1tot=PI1tot+PI1;
      PI1ave=(PI1tot)/(i);

      PI2tot=PI2tot+PI2;
      PI2ave=(PI2tot)/(i);

end
      PI=PI1ave+PI2ave*(.145);
```

شکل ۱۳. کد ارائه شده برای مسیر تهاجم شکل (۹)

بعد از اجرای کد ارائه شده توسط روش مونت‌کارلو، احتمال جلوگیری از حمله برابر با ۰/۴۷۸ به‌دست آمد که به جواب به‌دست آمده توسط روش EASI بسیار نزدیک است. همگرا شدن نهایی جواب در طی یک صد هزار تکرار، در شکل (۱۴) نشان داده شده است.

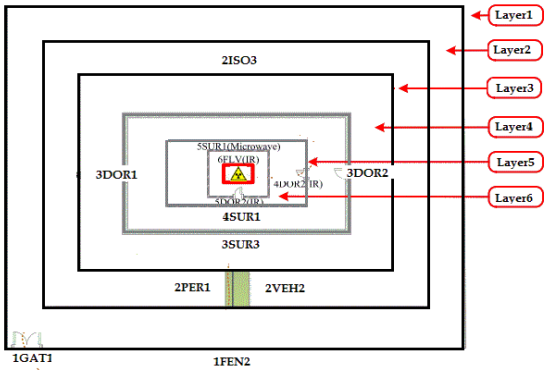


شکل ۱۴. همگرا شدن جواب در یک صد هزار تکرار

زمان محاسبات کد ارائه شده توسط یک رایانه معمولی حدود ۵ ثانیه به طول کشیده است.

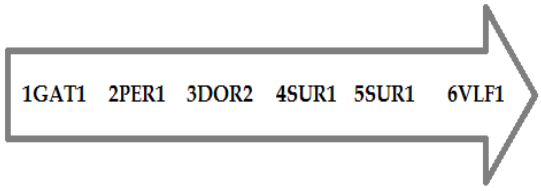
۴-۲. مقایسه مدل ارائه شده با گزارش‌های قبلی

در این قسمت نتیجه استفاده از مدل ارائه شده در این مقاله با نتیجه قبلاً گزارش شده [۱۹]، مقایسه می‌شود. در گزارش قبلی، حفاظت فیزیکی یک نیروگاه اتمی مدل شده است که لایه‌های مختلف آن در شکل (۱۵) نشان داده شده است.



شکل ۱۵. سامانه حفاظت فیزیکی یک نیروگاه اتمی

تعداد ۷۲ مسیر تهاجم برای نفوذ به این سامانه حفاظت فیزیکی وجود دارد. مدل ارائه شده در آن گزارش، احتمال جلوگیری از حمله را برای تمامی مسیرها محاسبه کرده است و در جدولی گزارش داده است. همچنین در این مقاله تنها زمان‌های تأخیر و احتمالات آشکارسازی عناصر شناسایی در نظر گرفته شده است و اطلاعاتی از تعداد مهاجمین و قابلیت‌های آن‌ها گزارش نشده است [۱۹]. برای این سامانه، بدترین مسیر تهاجم به صورت شکل (۱۶) گزارش شده است و احتمال جلوگیری از حمله برای این مسیر ۰/۹۲۳۴ محاسبه شده است.



شکل ۱۶. بدترین مسیر تهاجم برای نیروگاه اتمی فوق

سامانه حفاظت فیزیکی فوق توسط مدل ارائه شده در این مقاله (رابطه‌های (۱۱-۷))، مورد ارزیابی قرار گرفت و احتمال جلوگیری از حمله برای بدترین مسیر تهاجم برابر با ۰/۹۲۶ محاسبه شد.

۵. نتیجه‌گیری

در این مقاله ابتدا مفهوم ارزیابی حفاظت فیزیکی از تأسیسات حیاتی بر مبنای نقطه شناسایی بحرانی مورد بررسی قرار گرفت. سپس مدلی ریاضی برای ارزیابی حفاظت فیزیکی از تأسیسات حیاتی بر مبنای روش محاسباتی مونت‌کارلو ارائه شد. روش محاسباتی مونت‌کارلو این قابلیت را دارد تا متغیرهای سامانه را به صورت متغیرهای فرضی وارد مسئله کند و به حل مسئله بپردازد. این رویکرد محاسباتی سبب می‌شود تا نیاز به مدل‌سازی مسئله بر مبنای روش‌های قطعی و احتمالات شرطی پیچیده نباشد و مدل‌سازی مسئله ملموس گردد. در ادامه بر اساس رفتار مهاجم هوشمند، مدلی برای حذف مسیرهای غیر بهینه ارائه شده است تا نیازی به حل مسئله برای تک تک مسیرها نباشد. همچنین سعی شده است تا تعداد مهاجمین، تسلیحات و قابلیت‌های آن‌ها در مدل لحاظ گردد. به منظور ارائه درک شهودی از سامانه حفاظت فیزیکی، نرم‌افزاری مستقل با زبان برنامه‌نویسی C# نوشته شده است که سامانه حفاظت فیزیکی را به صورت دو بعدی مدل کرده و احتمال جلوگیری از حمله برای این سامانه را محاسبه می‌کند. درنهایت با استفاده از نتایج شبیه‌سازی و مقایسه مدل ارائه شده با مراجع دیگر، کارایی مدل ارائه شده مورد آزمون قرار گرفته است. ارتقا نرم‌افزار ارائه شده در مدل‌سازی سه بعدی سامانه حفاظت فیزیکی و همچنین مدل‌سازی عناصر تأخیر و شناسایی سامانه حفاظت فیزیکی با توجه به فناوری به‌کار رفته در آن‌ها، می‌تواند مبنای پژوهش‌های آینده قرار گیرد.

۶. مراجع

[1] Johansson, J. “Risk and Vulnerability Analysis of Interdependent Technical Infrastructures”; Ph.D. Thesis, Lund University, Dep. Measurement Technology and Industrial Electrical Eng. 2010.

[2] Ben-Haim, H.; Levitin, G. “Importance of Protections against Intentional Attacks”; Reliability Engineering and System Safety 2008, 93, 639-646.

[3] Yusta, J. M.; Correa, G. J.; Arantegui, R. L. “Methodologies and Applications for Critical Infrastructure Protection: State-of-the-art”; Energy Policy 2011, 10, 6100-6119.

[4] Haimes, Y. Y.; Longstaff, T. “The Role of Risk Analysis in the Protection of Critical Infrastructures against Terrorism”; Risk Anal. 2002, 22, 439-444.

[5] Zerriffi, H. “Electric Power Systems under Stress: An Evaluation of Centralized versus Distributed System Architectures”; Ph.D. Thesis, Carnegie Mellon University, Carnegie Institute of Technology, 2004.

[6] Apostolakis, G. E.; Lemon, D. M. “A Screening

Methodology for the Identification and Ranking of Infrastructure Vulnerabilities due to Terrorism"; Risk Anal. 2005, 25, 361-376.

[7] "Security Guidelines for the Electricity Sector: Physical Security"; North American Electric Reliability Corporation (NERC), 2007.

[8] Gent, M. R.; Costantini, L. P. "Reflections on Security"; IEEE Power & Energy Magazine 2003, 1, 1, 46-52.

[9] Ghaffarpour, R.; Pourmoosa, A. A. "Risk Assessment, Modeling, and Ranking for Power Network Facilities Regarding to Sabotage"; J. Advance Defense Sci. & Tech. 2015, 2, 127-144 (In Persian).

[10] Kaplan, S.; Garrick, B. L. "On the Quantitative Definition of Risk"; Risk Anal. 1989, 1, 11-27.

[11] Garrick, B. L.; Hall, L. E.; Kilger, M.; Mcdonald, L. C.; O'Toole, T.; Probst, P. S.; Parker, E. R.; Rosenthal, R. "Confronting the Risks of Terrorism: Making the Right Decisions"; Reliab. Eng. Syst. Safe. 2004, 86, 129-176.

[12] Ranjbar, M. H.; Pirayesh, A. "Providing a Method to Assess and Reduce the Risk of Power System against Terrorist Threats"; J. Advance Defense Sci. & Tech. 2016, 4, 327-337 (In Persian).

[13] Ezell, B. C. "Infrastructure Vulnerability Assessment Model (I-VAM)"; Risk Anal., 2007, 27, 571-583.

[14] Chen, G.; Dong, Z. Y.; Hil, D. L.; Xue, Y. S. "Exploring Reliable Strategies for Defending Power Systems against Targeted Attacks"; IEEE Trans. Power Syst. 2011, 26, 3, 1000-1009.

[15] Longfei, W.; Moghadsi, A. M.; Sundararajan, A.; Sarwat, A. "Defending Mechanisms for Protecting Power Systems against Intelligent Attacks"; System of Systems Engineering Conference (SoSE) 2015, 12-17.

[16] Garcia, M. L. "The Design and Evaluation of physical Protection Systems"; Butterworth Heinemann, 2007.

[17] Jang, S. S.; Kwan, S. W.; Yoo, H. S.; Kim, J. S.; Yoon, W. K. "Development of a Vulnerability Assessment Code for a Physical Protection System: Systematic Analysis of Physical Protection Effectiveness (SAPE)"; Nuclear Eng. Tech. 2009, 41, 747–752.

[18] Zou, B. W.; Yang, M.; Yoshikawa, H. "An Integrated Platform for Analysis and Design of Physical Protection Systems at Nuclear Power Plants," Proc. STSS/ISSNP, 2015.

[19] Zou, B. W.; Yang, M.; Yoshikawa, H. "Evaluation of Physical Protection Systems Using an Integrated Platform for Analysis and Design"; IEEE Trans. Syst. Man. Cybern. Syst. 2016, 99, 1-11.

[20] Burstein, H. "Introduction to Security"; Englewood Cliffs, NJ: Prentice Hall, 1994.

[21] Woo, T. H. "Analytic Study for Physical Protection System (PPS) in Nuclear Power Plants (NPPs)"; Nuclear Eng. Design 2013, 265, 932–937.

[22] Chapman, L.D.; Harlan, C. P. "EASI Estimate of Adversary Sequence Interruption on an IBM PC"; SAND Report 851105, 1985, l-63.

[23] Kalos, M. H.; Whitlock, P. A. "Monte Carlo Methods"; Wiley, 2008.

[24] Urteaga, I; Bugallo, M. F.; Djuric, P. M. "Sequential Monte Carlo Method under Model Uncertainty"; IEEE Statistical Signal Processing Workshop, 2016.

[25] Eisenberg, B.; Sullivan, R. "Why is the Sum of Independent Normal Random Variables Normal"; Math. Magazine, 2008, 81, 362-366.

[26] Utochkin, S. "The principles of CCTV design in VideoCAD"; http://www.cctvcad.com, 2016.

[27] Green, M. W. "The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies"; National Institute of Justice, 1999.