راهبردهای بهینه‌ی دفاع از سامانه‌های حسّاس با وجود اهداف مجازی و رویکرد قابلیت اطمینان

مهدی رحیمدل میبدی- دانشجوی دکتری مهندسی صنایع، دانشگاه پیام نور تهران.
امیرحسین امیری*- دانشیار، گروه مهندسی صنایع، دانشکده فنی و مهندسی، دانشگاه شاهد؛Email:amiri@shahed.ac.ir
مهدی کرباسیان- دانشیار، گروه مهندسی صنایع، دانشگاه صنعتی مالک اشتر.
تاریخ دریافت: ۹۴/۳/۱۷
تاریخ پذیرش: ۹۴/۷/۱۵
ویراستار فارسی مقاله: سروش جنابی

چکیده

امروزه دفاع از مناطق و منابع حسّاس، یکی از سیاست‌های کلان بقای دولت‌ها محسوب می‌شود و برای رسیدن به این هدف، به‌کارگیری راهبردهای آگاهانه و مفید لازم و ضروری است. در این تحقیق، نمونه‌سازی برای بهینه‌یابی سرمایه‌گذاری حفاظت از سامانه‌های حساس در نظر گرفته شده است که در این سامانه‌ها، مدافع با توجه به محدودیت‌های بودجه و فضای مورد نیاز برای تجهیزات دفاع، به دنبال حداقل‌سازی خسارت وارده از سوی مهاجم است در حالی که هدف مهاجم تخریب حداکثری اهداف حساس با توجه به محدودیت‌های بودجه و وزن تجهیزات تهاجمی است. در این حالت، مدافع برای فریب دادن مهاجم همچنین کاهش خسارت وارده به سامانه‌های حساس، تعدادی اهداف مجازی (مصنوعی) ایجاد می‌کند و مهاجم در پی شناسایی نکردن قطعی این اهداف مجازی، برای تشخیص آنها به‌صورت احتمالی عمل می‌کند. به‌طور کلّی در این تحقیق، با توجه به احتمالات موجود در حمله‌ی موفق، قدرت تشخیص مهاجم در شناسایی اهداف مجازی، ساختار قابلیت اطمینان سامانه و رویکرد نظریه بازی‌ها در پیدا کردن نقطه‌ی تعادل، یک نمونه‌ی برنامه‌ریزی غیرخطی برای تعیین میزان سرمایه‌گذاری دفاع از تمامی زیرسامانه‌ها ارائه شده است. در نهایت، نمونه‌ی ارائه شده‌ی تحقیق برای یک نمونه‌ی کاربردی استفاده می‌شود و نتایج نهایی آن، مورد تجزیه و تحلیل قرار می‌گیرد.

واژه‌های کلیدی: *سامانه‌های حساس، قابلیت اطمینان، دفاع، اهداف مجازی، نظریه بازی‌ها.*

Optimal Strategies for Defense of Sensitive Systems with False Targets and Reliability Approach

Mahdi Rahimde Meybodi[1], **Amirhossein Amiri**[2*], **Mahdi Karbasian**[3]

Abstract

Nowadays, protecting sensitive resources is one of the most important issues by government politics. So, it is essential that government, in order to achieve this target, utilizes beneficial strategies. In this paper, investment optimization for the protection of sensitive systems has been investigated. Defender minimizes the expected damage with respect to budget and area restrictions of defense equipment. However, the attacker maximizes the expected damage of sensitive targets with respect to cost and weight restrictions of attack equipment. Besides, defender deploys false elements to reduce the probability of system and real target vulnerability. False and real elements cannot be distinguished by the attacker. But the attacker has some probability of successfully detecting false targets. The aim of this study is to determine the optimal strategies for defense of sensitive targets considering probability of a successful attack, attacker capability in detecting false targets, reliability block diagram and game theory approach. Finally, the presented model is illustrated for the case study and final findings are analyzed.

Key words: *Sensitive systems, Reliability, Defense, False targets, Game theory.*

1 PhD Student of Industrial Engineering, Payam noor University, Tehran, Iran.
2 Associate Professor, Industrial Engineering Department, Faculty of Engineering, Shahed University, Tehran, Iran; Email: amiri@shahed.ac.ir
3 Associate Professor, Industrial Engineering Department, Malek ashtar University of Technology, Tehran, Iran

مقدمه

امروزه به‌کارگیری ابزارهای متداول نمونه‌سازی در سامانه‌های دفاع و حمله، علاوه بر تبیین صریح صورت مسئله، منجر به کشف راه‌حل‌های سازنده می‌شوند. زیرساخت‌های حساس و مهم هر کشور، دارایی‌هایی هستند که با توجه به نقش حیاتی آنها در ثبات، آرامش و امنیت زندگی اجتماعی مردم، نیاز مبرم به حفظ و نگهداری دارند که از نمونه این زیرساختارها، می‌توان مراکز نظامی، جاده‌ها، منابع انرژی، سامانه‌های مخابراتی، منابع آبی، مراکز تجاری، مدارس و بیمارستان‌ها را نام برد. دولت‌ها به عنوان یک مدافع، باید در مقابل حملات احتمالی دشمنان به مناطق حسّاس، اقدامات حفاظتی را به عمل آورند و خسارت مورد انتظار زیرساختارها را تا حد امکان، کمینه کنند. به عبارت دیگر، مدافع باید قابلیت اطمینان عملکرد زیرساختارها را که اجرای اهداف به‌صورت پایدار است، افزایش دهد. در مقابل، هدف مهاجم بیشینه کردن خسارت اهداف مورد تهاجم است.

مدافع برای نگهداری زیرساختارهای خود، باید متناسب با ماهیت اهداف سامانه‌ها، سرمایه‌گذاری‌های مربوط به اقدامات حفاظتی را انجام دهد. برخی زیرساختارها سریعاً ساخته می‌شوند در حالی که ساخت برخی دیگر سالیان سال طول می‌کشد. بنابراین، برای تخصیص بودجه و امکانات برای حفاظت از زیرساختارها باید به ارزش اهداف، محدودیت بودجه، ساختارهای سیاسی، نظامی و تاریخی نیز توجه کرد. همچنین از منظر اطمینان‌پذیری، ساختار چیدمان این سامانه‌ها با توجه به نوع عملکرد آنها می‌تواند به‌صورت‌های گوناگونی مانند سری، موازی ، مختلط و پیچیده باشد.

تاکنون تحقیقات زیادی برای تعیین راهبردهای بهینه دفاع و حمله انجام شده است. ژوآنگ و بیر، تخصیص منابع مدافع برای محافظت از حوادث طبیعی و حملات مهاجم را نمونه‌سازی کردند [۱]. جوردن و لوب، تخصیص منابع سرمایه‌گذاری و امنیت سایبری را نمونه‌سازی و تجزیه و تحلیل کردند[۲]. پترسون و اپوستولاکیس، معیارهای اساسی رتبه‌بندی اجزای سامانه‌های پیچیده (در مناطق جغرافیایی مختلف) برای تعیین مکان‌های بحرانی در معرض خطر حمله را ارائه کردند[۳]. ژیو و روکو با رویکرد شبیه‌سازی، ایمنی شبکه‌های پیچیده در معرض خطر مهاجم را ارزیابی کردند [۴]. همچنین از دیدگاه راهبردهای علوم و اقتصاد سیاسی، تحقیقات زیادی انجام شده است که نمونه آن، تحقیق ارائه شده‌ی سندلر و سیکویرا است [۵].

بسیاری از محققان، از مفاهیم و کاربردهای نظریه بازی‌ها برای تعیین راهبردهای بهینه دفاع و حمله استفاده کرده‌اند. نظریه بازی‌ها یک تکنیک ریاضی به منظور تجزیه و تحلیل مسائلی است که دربرگیرنده‌ی موقعیت‌های در تعارض هستند. در هر بازی، بازیکنان به‌دنبال انتخاب بهترین راهبرد برای خود در مقابل راهبردهای ممکن برای رقیب هستند که این روند در انتها به یک نقطه‌ی تعادل ختم می‌شود [۶،۷،۸]. گایکما، نمونه‌های نظریه بازی‌ها برای بازیگران هوشمند را از منظر قابلیت اطمینان، مورد تجزیه و تحلیل قرار داده است [۹]. کانتورسکا و همکاران با توجه به کاربرد نظریه بازی‌ها، چگونگی بهبود قابلیت اطمینان شبکه‌های حمل و نقل را از طریق مسیرهای چندگانه و راهبردهای مختلف دفاعی، نمونه‌سازی کردند [۱۰]. در نمونه ارائه شده‌ی ژین یانگ و همکاران، پس از تعیین تمامی راهبردهای دو طرف بازی و معیارهای سنجش آنها، هر یک از راهبردها با متغیرهای کلامی و با توجه به اصول نظریه دمپستر- شیفر مورد سنجش قرار می‌گیرند و پس از محاسبه ماتریس نهایی تصمیم‌گیری و استفاده از نظریه بازی‌ها، نقطه‌ی تعادل در صورت وجود، تعیین می‌شود [۱۱]. بیر و همکاران با هدف کاهش احتمال حمله موفقیت‌آمیز، محافظت از سامانه‌هایی را نمونه‌سازی کردند که ساختار قابلیت اطمینان آنها به‌صورت ساده کاملاً موازی یا سری باشد و با توجه به آگاهی مهاجم از اهداف مورد نظر، نمونه مربوط را در دو حالت بدون محدودیت و با محدودیت بودجه، مورد تجزیه و تحلیل قرار دادند [۱۲]. یانگ و همکاران، سرمایه‌گذاری بهینه امنیت اطلاعات با توجه به انواع مختلف حمله‌ها را نمونه‌سازی کردند [۱۳]. لوتین خسارت مورد انتظار به مدافع را با توجه به روش‌های توزیع حمله مهاجم و روش‌های جداسازی و گروه‌بندی مواضع مدافع، تعیین کرد [۱۴]. لوتین و هاسکن، تأثیر تک حمله یا حمله دوگانه به یک سامانه با n جزء موازی و یکسان را نمونه‌سازی کردند که در آن، مهاجم منابع خود را بین دو حمله تقسیم و سعی می‌کند در حمله‌ی دوم به تمامی مواضع تخریب نشده حمله ور شود [۱۵]. همچنین این محققان با در نظر گرفتن تابع احتمال میزان خسارت واردشده به سامانه، در چند حالت (با وجود محافظت از تمام یا زیرمجموعه‌ای از زیرسامانه‌ها) میزان کاهش این احتمال را ارزیابی کرده‌اند [۱۶]. هاسکن و لوتین با هدف حداقل سازی حد اکثر خسارت مورد انتظار از منظر مدافع، یک سامانه سری- موازی در نظر گرفتند که هریک از اجزای آن، دارای میزان ظرفیت متفاوتی است و برای حل نمونه، از الگوریتم ژنتیک استفاده کردند [۱۷]. در تحقیق دیگری از این محققان، با درنظرگرفتن یک سامانه سری که در آن، مدافع اهداف مجازی تولید می‌کند و مهاجم قادر به تشخیص غیرواقعی بودن آنها نیست، تعداد بهینه اهداف مجازی با توجه به هدف کاهش احتمال حمله موفقیت‌آمیز، تعیین می‌شود [۱۸]. در نمونه مورد تحقیق هاسکن، دو سامانه‌ی سری- موازی و موازی- سری در نظر گرفته شده است و راهبردهای بهینه‌ی دفاع و حمله با توجه به کاربردهای نظریه بازی‌ها، احتمال حمله موفقیت، ارزش زیرسامانه‌ها و محدویت بودجه تعیین می‌شود [۱۹]. این محقق برای بهبود نمونه‌ی ارائه‌شده‌ی خود، با توجه به نقاط هدف سامانه‌ها که دارای ساختارهایی مانند سری، موازی و پیچیده هستند، یک نمونه بر اساس نظریه بازی‌ها ارائه کرده است که در آن مدافع، در پی حداقل سازی خسارت وارده و مهاجم در پی حداکثر کردن آن است. برای این کار یک تابع خسارت که برابر با احتمال حمله‌ی موفق به اهداف است، تعریف می شود که وابسته به میزان سرمایه‌گذاری دفاع و حمله همچنین وابسته به مشخصه‌ی دیگری است که شدت اهمیت آن اهداف هستند. در این نمونه، میزان سرمایه‌گذاری بهینه‌ی دفاع و حمله با توجه به

آگاهی کامل مهاجم از اهداف مدافع تعیین می‌شود[۲۰]. همچنین در تحقیق انجام شده از سوی لوتین و همکاران، دفاع بهینه از اجزای یکسان، ولی با محافظ گروهی از آنها نمونه‌سازی شده است که در این تحقیق، مهاجم برای حمله به اجزا باید ابتدا محافظ گروهی آنها را تخریب کند [۲۱].

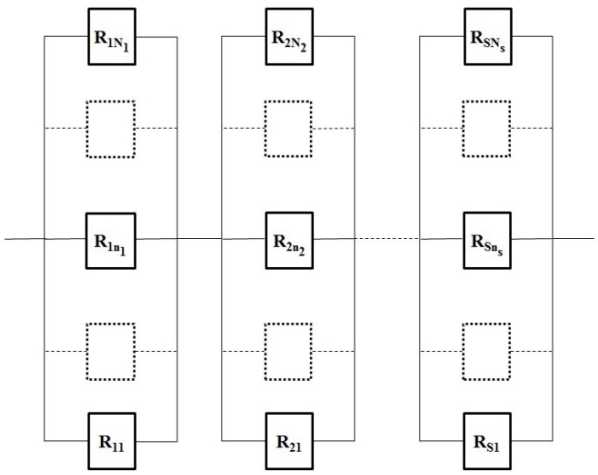
مقاله حاضر به استناد تحقیقات سابق در زمینه‌ی موضوع تحقیق و با توجه به نواقص و کمبودهای موجود در آنها، یک نمونه‌ی کاربردی و واقعی‌تر برای تخصیص سرمایه‌گذاری دفاع از سامانه‌های حساس ارائه می‌کند که هریک از این سامانه‌ها، چند زیرسامانه دارند و با توجه به عملکرد این زیرسامانه‌ها، دارای ساختار موازی از جنبه‌ی قابلیت اطمینان است،اما تمامی سامانه‌های حساس مورد نظر، ساختار سری با یکدیگر دارند. در مجموع، مسئله مورد مطالعه ساختاری سری- موازی دارد که تخصیص سرمایه‌گذاری برای دفاع از تمامی اجزای آن، مورد نظر است. در این سامانه‌ها، مدافع به دنبال حداقل‌سازی خسارت وارده از سوی مهاجم است در صورتی‌که هدف مهاجم، تخریب حداکثری اهداف (سامانه‌های) حساس است.

مهم‌ترین موضوع‌های که در این تحقیق معرفی شده است، استفاده از اهداف مجازی برای فریب‌دادن مهاجم همچنین کاهش خسارت وارده به سامانه‌های حساس است، اما مهاجم در پی شناسایی قطعی این اهداف مجازی، در تشخیص آنها به‌صورت احتمالی عمل می‌کند. یکی دیگر از نوآوری‌های این تحقیق، استفاده از ضریب برتری تجهیزات دفاع به حمله، در تعریف تابع احتمال موفقیت حمله است که منجر به واقعی‌تر شدن نمونه پیشنهادی می‌شود. همچنین در تحقیقات گذشته، فقط محدودیت هزینه برای نمونه‌سازی در نظر گرفته شده است درصورتی‌که نمونه‌ی ارائه شده این تحقیق، محدودیت‌های بودجه و فضای مورد نیاز برای تجهیزات دفاع و هزینه و وزن تجهیزات حمله را در نظر می‌گیرد. به‌طور کلی، در این تحقیق با توجه به احتمالات موجود در حمله موفق، قدرت تشخیص مهاجم در شناسایی اهداف مجازی، ساختار قابلیت اطمینان سامانه و رویکرد نظریه بازی‌ها در پیداکردن نقطه‌ی تعادل، میزان سرمایه‌گذاری بهینه برای دفاع از تمامی زیرسامانه‌ها، مورد محاسبه قرار می‌گیرد.

تعریف مسئله

در سامانه‌های دفاع و حمله، هدف اصلی مدافع، افزایش قابلیت اطمینان عملکرد سامانه و زیرمجموعه‌های مربوطه به آن است. در مقابل، هدف مهاجم حداکثرسازی خسارت به سامانه و زیرمجموعه‌های آن است. فرض کنید که در مسئله مورد نظر، s سامانه حساس وجود دارد که هر سامانه شامل n_i هدف واقعی با ساختار عملکردی موازی باشد. بنابراین، برای عملکرد سامانه iام، باید حداقل یک زیرسامانه به‌طور مطلوب فعالیت کند.

مدافع برای فریب‌دادن مهاجم، در هر سامانه تعدادی هدف مجازی (غیر واقعی) ایجاد می‌کند تا با این کار بتواند با فرض محدودیت بودجه مهاجم برای سرمایه‌گذاری حمله به زیرسامانه‌ها، احتمال حمله‌ی موفقیت‌آمیز به اهداف واقعی را کاهش دهد. بنابراین، هر سامانه شامل h_i هدف مجازی و در مجموع N_i زیرسامانه‌ی واقعی و مجازی است. مدافع برای حفاظت از زیرسامانه‌ها، سرمایه‌گذاری‌های متفاوت f_{ij} را با هزینه واحد c_{ij} انجام می‌دهد و مهاجم نیز به‌طور مشابه برای حمله به هریک از زیرسامانه‌ها، F_{ij} را با هزینه واحد C_{ij} سرمایه‌گذاری می کند که ij، نشان‌دهنده‌ی هدف jام از زیرسامانه i ام است. همچنین از نظر مدافع، ارزش هر هدف ij برابر با v_{ij} و ارزش کل سامانه برابر با v است و به‌طور مشابه برای مهاجم، هر هدف ij، ارزشی برابر با V_{ij} و کل سامانه، ارزشی برابر با V دارد. تصویر ۱ ساختار قابلیت اطمینان مسئله مورد نظر را نشان می‌دهد.



تصویر۱: ساختار قابلیت اطمینان سامانه سری – موازی

قابلیت اطمینان هر هدف بستگی به میزان سرمایه‌گذاری برای محافظت اهداف از طرف مدافع و میزان سرمایه‌گذاری برای حمله‌کردن از طرف مهاجم دارد و در نتیجه، تعیین‌کننده ی موفقیت حمله و دفاع است.

پایایی سامانه با اهداف مجازی

فرض کنید که یک سامانه شامل N_i زیرسامانه باشد و باید برای عملکرد صحیح آن، حداقل یک زیرسامانه، عملکرد مطلوب داشته باشند. بنابراین، خرابی تمامی زیرسامانه‌ها، موجب خرابی کل سامانه می‌شود . احتمال خرابی سامانه (F_p) با استفاده از رابطه ۱ قابل محاسبه است [۲۲].

رابطه ۱:

$$F_p = \prod_{i=1}^{N_i}(1 - R_i).$$

که در آن، R_i برابر با قابلیت اطمینان زیرسامانه iام است. این روش محاسباتی زمانی مورد استفاده قرار می‌گیرد که تمامی زیرسامانه‌ها، واقعی باشند.

در صورتی‌که تعدادی از زیرسامانه‌ها، مجازی و غیرواقعی باشند و واقعی بودن آنها را بتوان به‌صورت احتمالی تشخیص داد، می‌توان با استفاده از رابطه (۲)، احتمال خرابی کل سامانه را محاسبه کرد.

رابطه ۲:

$$F_p = \prod_{i-1}^{N_i}(1 - \tau_i R_i).$$

τ_i احتمال تشخیص واقعی‌بودن زیرسامانه i ام است که اگر این احتمال برای تمامی زیرسامانه‌ها برابر با یک باشد، روش محاسباتی معادل رابطه ۱ خواهد بود.

با توجه به تعریف مسئله‌ی تحقیق، مدافع برای هریک از سامانه‌های حساس، تعدادی زیرسامانه مجازی در نظر گرفته است، اما مهاجم به علت ناآگاهی، واقعی بودن این زیرسامانه‌ها را به‌صورت احتمالی تشخیص می‌دهد. بنابراین، اگر سامانه مورد نظر (i) شامل n_i زیرسامانه واقعی و $h_i=N_i-n_i$ زیرسامانه مجازی باشد، قابلیت اطمینان مسئله‌ی سری- موازی موردنظر (R_{sp}) از نظر مدافع، به‌صورت رابطه(۳) محاسبه می‌شود.

رابطه ۳:

$$R_{sp}=\prod_{i=1}^{s}(1-(\prod_{j=1}^{n_i}(1-R_{ij})).$$

همچنین از منظر مهاجم، اگر در سامانه iام، احتمال تشخیص واقعی‌بودن زیرسامانه j برابر با τ_{ij} باشد، احتمال خرابی کل سامانه‌ی مورد نظر (F_{sp}) به‌صورت رابطه (۴) است.

رابطه ۴:

$$F_{sp}=1-\prod_{i=1}^{s}(1-\prod_{j=1}^{N_i}(1-\tau_{ij}R_{ij})).$$

تابع احتمال موفقیت حمله

یک روش ساده برای تعریف احتمال یک حمله موفق روی هدف ij (زیرسامانه j از سامانه i ام) استفاده از نسبت ارائه شده توسط آقای تالوک [۲۳] است که به‌صورت رابطه ۵ بیان می‌شود.

رابطه ۵:

$$p_{ij}=\frac{F_{ij}^{m_{ij}}}{f_{ij}^{m_{ij}}+F_{ij}^{m_{ij}}}\ .$$

که در آن m_{ij} میزان شدت رقابت بر سر هدف ij و یک مشخصه رقابت با توجه به نوع هدف ij است. برای اهدافی که قابل دفاع یا پیش‌بینی هستند، مقدار کم شدت (m_{ij}) وجود دارد که در این گونه موارد، نه مدافع و نه مهاجم نمی‌توانند به برتری کامل دست یابند. برای اهدافی که اجزای آن به‌صورت متمرکز هستند، قابلیت کمی برای پیش‌بینی دارند یا به سادگی مورد حمله قرار می‌گیرند، مقدار شدت بسیار بالا می‌شود که در این گونه موارد، ممکن است هر دو طرف (مدافع و مهاجم) به برتری کامل دست یابند. با وجود اقدامات دفاعی(حفاظتی) نامحدود و اقدامات تهاجمی محدود، هدف ۱۰۰٪ قابل اطمینان است و $p_{ij}=0$. به‌طور معکوس با وجود اقدامات تهاجمی نامحدود و اقدامات تدافعی محدود، هدف ۰٪ قابل اطمینان است و $p_{ij}=1$ است.

در این تحقیق، برای تعیین تابع احتمال موفقیت، علاوه بر فاکتورهای شدت رقابت و میزان سرمایه‌گذاری‌های مدافع و مهاجم، از عامل تأثیرگذار برتری تکنولوژیکی تجهیزات دفاع و حمله نیز استفاده شده که در دستیابی به احتمالات واقع‌گرایانه‌تر، بسیار مفید است. فرض کنید که میزان اهمیت سطح تکنولوژیکی تجهیزات دفاع و حمله برای هدف ij، که با استناد به تصمیم‌گیری گروهی خبرگان است، به ترتیب برابر با w_{ij} و W_{ij} تعیین شده باشد، ضریب α_{ij} به عنوان میزان برتری تجهیزات دفاع به حمله هدف ij تعریف می‌شود که با استفاده از رابطه ۲ محاسبه می‌شود.

رابطه ۶:

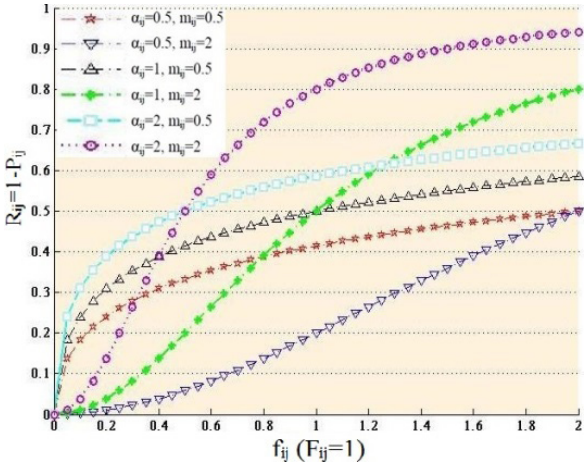
$$\alpha_{ij}=\frac{w_{ij}}{W_{ij}}\ .$$

به ازای هریک از اهداف (ij)، با توجه به احتمال موفقیت حمله (رابطه ۵) و در نظر گرفتن ضریب برتری تجهیزات دفاع نسبت به تجهیزات حمله (α_{ij})، می‌توان تابع احتمال شکست حمله (R_{ij}) را به‌صورت رابطه ۷ تعریف کرد.

رابطه۷:

$$R_{ij}=\frac{(\alpha_{ij}f_{ij})^{m_{ij}}}{(\alpha_{ij}f_{ij})^{m_{ij}}+F_{ij}^{m_{ij}}}\ .$$

تصویر ۲ روند تغییرات احتمال عدم موفقیت حمله (R_{ij}) نسبت به f_{ij} را نشان می‌دهد.



تصویر ۲: میزان تغییرات احتمال شکست حمله نسبت به میزان سرمایه‌گذاری

با در نظر گرفتن مقدار ثابت ۱ = f_{ij} ، در صورتی‌که ضریب شدت (m_{ij}) و ضریب برتری تجهیزات دفاع نسبت به تجهیزات حمله (α_{ij}) کوچک‌تر از یک باشند، مهاجم با سرمایه‌گذاری کمتری می‌تواند به موفقیت بیشتری دست یابد. بر عکس، در صورتی‌که m_{ij} و α_{ij} بزرگتر از یک باشند، افزایش سرمایه‌گذاری موجب رسیدن به قابلیت اطمینان بالاتر و بیشتر از آن تناسب می‌شود. به عبارت دیگر، در این حالت، مهاجم با سرمایه‌گذاری زیادتر نیز نمی‌تواند به موفقیت بیشتری دست یابد.

نمونه‌سازی راهبردهای بهینه دفاع از سامانه‌های حسّاس

با درنظرگرفتن تابع احتمال خطر (p_{ij})، مدافع در پی کاهش این احتمال و در نتیجه، افزایش قابلیت اطمینان ($1-p_{ij}$) است. همچنین در صورت وجود محدودیت‌های بودجه و فضا، مطلوبیت مدافع، کمینه کردن دو هدف دیگر یعنی هزینه و حجم فضای کل نیز هست. بنابراین، می‌توان سه تابع هدف به‌صورت زیر برای مطلوبیت مورد نظر مدافع در نظر گرفت:

رابطه ۸:

$$Max:\ u_1=\sum_{i=1}^{s}\sum_{j=1}^{N_i}R_{ij}v_{ij}+R_{sp}v\ .$$

رابطه ۹:

$$Min:\ u_2=\sum_{i=1}^{s}\sum_{j=1}^{N_i}c_{ij}f_{ij}\ .$$

رابطه ۱۰: $Min:\ u_3 = \sum_{i=1}^{s}\sum_{j=1}^{N_i} b_{ij} f_{ij}$.

R_{sp}، قابلیت اطمینان کل سامانه (سری- موازی) و b_{ij} حجم مورد نیاز برای هر واحد سرمایه‌گذاری دفاع از هدف j ام از زیرسامانه i ام است. بنابراین، نمونه‌ی برنامه‌ریزی خطی مناسب برای بهینه‌سازی مطلوبیت مدافع با در نظر گرفتن محدودیت‌های مربوط به‌صورت روابط ۱۱ تا ۱۳ خواهد بود.

رابطه ۱۱:

$$Max: u = \sum_{i=1}^{s}\sum_{j=1}^{N_i} \frac{(\alpha_{ij} f_{ij})^{m_{ij}}}{(\alpha_{ij} f_{ij})^{m_{ij}} + F_{ij}^{m_{ij}}} v_{ij} + v \prod_{i=1}^{s}\left(1 - \left(\prod_{j=1}^{n_i} \frac{F_{ij}^{m_{ij}}}{(\alpha_{ij} f_{ij})^{m_{ij}} + F_{ij}^{m_{ij}}}\right)\right) - \sum_{i=1}^{s}\sum_{j=1}^{N_i} c_{ij} f_{ij} - \sum_{i=1}^{s}\sum_{j=1}^{N_i} b_{ij} f_{ij} \quad .$$

s.t. :

رابطه ۱۲: $\sum_{i=1}^{s}\sum_{j=1}^{N_i} c_{ij} f_{ij} \le c_{max}$.

رابطه ۱۳: $\sum_{i=1}^{s}\sum_{j=1}^{N_i} b_{ij} f_{ij} \le b_{max} \quad , \quad f_{ij} \ge 0$

از سوی دیگر، مهاجم متمایل به افزایش احتمال خطر (p_{ij}) است. همچنین در صورت وجود محدودیت‌های بودجه و وزن، مطلوبیت مهاجم، کمینه کردن دو هدف دیگر یعنی هزینه و وزن کل تجهیزات نیز هست. بنابراین به‌طور مشابه، نمونه‌ی برنامه‌ریزی خطی مناسب برای بهینه‌سازی مطلوبیت مهاجم با در نظر گرفتن محدودیت‌های مربوط به‌صورت روابط ۱۴ تا ۱۶ خواهد بود.

رابطه ۱۴:

$$Max: U = \sum_{i=1}^{s}\sum_{j=1}^{N_i} \frac{F_{ij}^{m_{ij}}}{(\alpha_{ij} f_{ij})^{m_{ij}} + F_{ij}^{m_{ij}}} \tau_{ij} V_{ij} + V\left(1\prod_{i=1}^{s}\left(1 - \prod_{j=1}^{N_i}\left(\frac{F_{ij}^{m_{ij}} + (1-\tau_{ij})(\alpha_{ij} f_{ij})^{m_{ij}}}{(\alpha_{ij} f_{ij})^{m_{ij}} + F_{ij}^{m_{ij}}}\right)\right)\right) - \sum_{i=1}^{s}\sum_{j=1}^{N_i} C_{ij} F_{ij} - \sum_{i=1}^{s}\sum_{j=1}^{N_i} O_{ij} F_{ij} .$$

s.t. :

رابطه ۱۵: $\sum_{i=1}^{s}\sum_{j=1}^{N_i} \tau_{ij} C_{ij} F_{ij} \le C_{max}$.

رابطه ۱۶: $\sum_{i=1}^{s}\sum_{j=1}^{N_i} \tau_{ij} O_{ij} F_{ij} \le O_{max} , \quad F_{ij} \ge 0$

c_{max} و b_{max} به ترتیب، بیشینه‌ی هزینه و بیشینه‌ی حجم مورد نظر مدافع است. همچنین O_{ij} وزن مورد نیاز برای هر واحد سرمایه‌گذاری حمله به هدف j ام از زیرسامانه i ام، C_{max} بیشینه‌ی هزینه مورد نظر مهاجم و O_{max} بیشینه‌ی وزن تجهیزات حمله است.

برای به‌دست‌آوردن راه‌حل از مفاهیم بنیادی نقطه‌ی تعادل نش در نظریه بازی‌ها استفاده می شود که در آن، هیچ‌یک از طرفین بازی به‌صورت یک‌طرفه عمل نمی‌کنند، بلکه با توجه به منطقی‌بودن بازیکنان، مناسب‌ترین پاسخ تعیین می‌شود [۲۴،۲۵].

بنابراین، برای تعیین نقطه‌ی تعادل هر هدف، باید مسئله‌ی برنامه‌ریزی غیرخطی با روابط ۱۷ تا ۲۳ حل شود که در آن، از تعمیم شرایط کوهن- تاکر استفاده شده است [۲۶،۲۷،۲۸]. بهترین حالت تابع هدف، صفربودن آن است؛ زیرا این تابع به ازای هر راه‌حل عملی، غیرمنفی می‌شود.

رابطه ۱۷:

$$Min: \lambda_{1,1}\left(c_{max} - \sum_{i=1}^{s}\sum_{j=1}^{N_i} c_{ij} f_{ij}\right) + \lambda_{1,2}\left(b_{max} - \sum_{i=1}^{s}\sum_{j=1}^{N_i} b_{ij} f_{ij}\right) + \lambda_{2,1}\left(C_{max} - \sum_{i=1}^{s}\sum_{j=1}^{N_i} \tau_{ij} C_{ij} F_{ij}\right) + \lambda_{2,2}\left(O_{max} - \sum_{i=1}^{s}\sum_{j=1}^{N_i} \tau_{ij} O_{ij} F_{ij}\right)$$

رابطه ۱۸:

$$v_{kl} \frac{m_{kl} (\alpha_{kl} F_{kl})^{m_{kl}} f_{kl}^{(m_{kl}-1)}}{((\alpha_{kl} f_{kl})^{m_{kl}} + F_{kl}^{m_{kl}})^2} + v \frac{m_{kL} (\alpha_{kL} F_{kL})^{m_{kL}} f_{kL}^{(m_{kL}-1)}}{((\alpha_{kL} f_{kL})^{m_{kL}} + F_{kL}^{m_{kL}})^2} Q_a Q_b - (1+\lambda_{1,1}) c_{kl} - (1+\lambda_{1,2}) b_{kl} = 0$$

$$k = 1,\ldots,s \ , \ L = 1,\ldots n_i \ , \ l = 1,\ldots, N_i .$$

رابطه ۱۹:

$$\tau_{kl}\left(\tau_{kl}\left(v_{kl} \frac{m_{kl} (\alpha_{kl} f_{kl})^{m_{kl}} F_{kl}^{(m_{kl}-1)}}{((\alpha_{kl} f_{kl})^{m_{kl}} + F_{kl}^{m_{kl}})^2} + V \frac{m_{kl} (\alpha_{kl} f_{kl})^{m_{kl}} F_{kl}^{(m_{kl}-1)}}{((\alpha_{kl} f_{kl})^{m_{kl}} + F_{kl}^{m_{kl}})^2} Q_c Q_d\right) - (1+\lambda_{2,1}) C_{kl} - (1+\lambda_{2,2}) O_{kl}\right) = 0 \ ,$$

$$k = 1,\ldots,s \quad , \ l = 1,\ldots, N_i .$$

رابطه ۲۰: $\sum_{i=1}^{s}\sum_{j=1}^{N_i} c_{ij} f_{ij} \le c_{max}$.

رابطه ۲۱: $\sum_{i=1}^{s}\sum_{j=1}^{N_i} b_{ij} f_{ij} \le b_{max}$.

رابطه ۲۲: $\sum_{i=1}^{s}\sum_{j=1}^{N_i} \tau_{ij} C_{ij} F_{ij} \le C_{max}$.

رابطه ۲۳: $\sum_{i=1}^{s}\sum_{j=1}^{N_i} \tau_{ij} O_{ij} F_{ij} \le O_{max}$.

$$i = 1,\ldots,s \ , \ j = 1,\ldots,Ni \quad \lambda_{1,1}, \lambda_{1,2}, \lambda_{2,1}, \lambda_{2,2} \ge 0$$

$$Q_a = \prod_{\substack{i=k \\ j \ne L}}^{n_i} \frac{F_{ij}^{m_{ij}}}{(\alpha_{ij} f_{ij})^{m_{ij}} + F_{ij}^{m_{ij}}} \quad ,$$

$$Q_b = \prod_{\substack{i=1 \\ i \ne k}}^{s} \left(1 - \prod_{j=1}^{n_i} \frac{F_{ij}^{m_{ij}}}{(\alpha_{ij} f_{ij})^{m_{ij}} + F_{ij}^{m_{ij}}}\right) .$$

$$Q_c = \prod_{\substack{i=k \\ j \ne l}}^{N_i} \frac{F_{ij}^{m_{ij}} + (1-\tau_{kl})(\alpha_{ij} f_{ij})^{m_{ij}}}{(\alpha_{ij} f_{ij})^{m_{ij}} + F_{ij}^{m_{ij}}} ,$$

$$Q_d = \prod_{\substack{i=1 \\ i \ne k}}^{s} \left(1 - \prod_{j=1}^{N_i} \frac{F_{ij}^{m_{ij}} + (1-\tau_{kl})(\alpha_{ij} f_{ij})^{m_{ij}}}{(\alpha_{ij} f_{ij})^{m_{ij}} + F_{ij}^{m_{ij}}}\right)$$

جدول ۱ :اطلاعات اولیه مطالعه موردی

ij	۱۱	۱۲	۱۳	۱۴	۲۱	۲۲	۲۳	۲۴	۳۱	۳۲
c_{ij}	۰/۹	۰/۹	۰/۹	۰/۲	۱/۱	۱/۱	۰/۲	۰/۲	۱	۱
b_{ij}	۰/۴	۰/۴	۰/۴	۰/۴	۰/۴	۰/۴	۰/۴	۰/۴	۰/۴	۰/۴
C_{ij}	۰/۸	۰/۸	۰/۸	۰/۸	۱	۱	۱	۱	۱/۳	۱/۳
O_{ij}	۰/۲۵	۰/۲۵	۰/۲۵	۰/۲۵	۰/۲۵	۰/۲۵	۰/۲۵	۰/۲۵	۰/۲۵	۰/۲۵
v_{ij}	۱۰	۸	۱۱	۲	۱۲	۱۲	۲	۲	۱۱	۱۲
V_{ij}	۱۰	۷	۱۰	۴	۱۲	۱۲	۳	۴	۱۱	۱۲
a_{ij}	۰/۷	۰/۷	۰/۷	۰/۷	۰/۷	۰/۷	۰/۷	۰/۷	۰/۷	۰/۷
m_{ij}	۱/۳	۲	۱/۳	۱	۲	۱/۵	۱	۱	۲	۱/۳
τ_{ij}	۱	۰/۸	۰/۹	۰/۶	۱	۱	۰/۲	۰/۸	۱	۱
	$v=V=۱۰۰,\ c_{max}=۴۰,\ C_{max}=۲۵,\ b_{max}=۱۵,\ O_{max}=۱۰$									

نتیجه‌ی نهایی برنامه‌ریزی غیرخطی مذکور، نقطه‌ی تعادل را نشان می‌دهد و تعیین‌کننده‌ی میزان سرمایه‌گذاری بهینه دفاع برای هریک از زیرسامانه‌های حسّاس است.

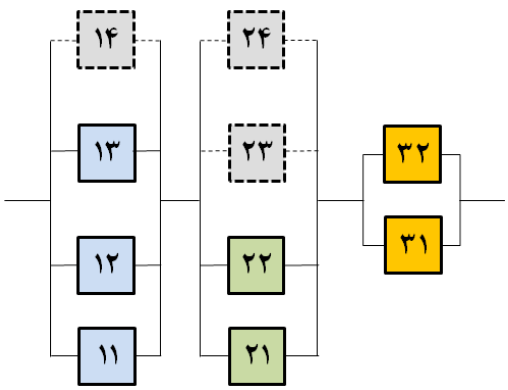
برای حل مسئله در ابعاد کوچک، می‌توان از نرم‌افزارهای کاربردی در این زمینه مانند Lingo و Gams استفاده کرد. ولی در صورت بزرگ شدن ابعاد مسئله، باید با استفاده از روش‌های فراابتکاری، الگوریتم بهینه‌یابی مسئله را طراحی و اجرا کرد [۲۹].

در صورتی‌که مسئله‌ی برنامه‌ریزی غیرخطی مذکور، بیش از یک نقطه‌ی تعادل داشته باشد، با توجه به راهبردها و نوع نگرش طرفین بازی (مدافع و مهاجم)، می‌توان نقطه‌ی تعادل ارجح را تعیین کرد. اگر بنا به فرض، بازی‌کننده اول، مدافع باشد، می‌توان راهبردهای زیر را برای تعیین نقطه‌ی تعادل ارجح، در نظر گرفت:

- درصورتی‌که مجموع کل هزینه یا مجموع کل حجم تجهیزات برای مدافع، معیار تصمیم‌گیری باشد، از تمامی نقاط تعادل به‌دست‌آمده، نقطه‌ی تعادل ارجح، نقطه‌ای است که پایین‌ترین مقدار هزینه یا حجم (و یا ترکیب آنها) را داشته باشد.
- درصورتی‌که معیار تصمیم‌گیری مدافع، قابلیت اطمینان کل سامانه باشد، نقطه‌ی تعادل ارجح، نقطه‌ای است که به‌کارگیری آن، بیشترین مقدار قابلیت اطمینان دفاع از کل سامانه را با توجه به روابط مربوط، ایجاد کند.
- اگر برای مدافع، معیار تصمیم‌گیری مشخصی وجود نداشته باشد، می‌توان با توجه به احتمالات پیش‌بینی‌شده مدافع در انتخاب هریک از نقاط تعادل توسط مهاجم و ارزیابی‌های مربوطه، نقطه‌ی تعادل ارجح را تعیین کرد [۳۰].

مطالعه‌ی موردی

در این قسمت، برای نشان‌دادن چگونگی استفاده از نمونه‌ی پیشنهادی و تحلیل نتایج مربوط، یک مثال کاربردی ارائه می‌شود. منابع حیاتی و ضروری برای یک منطقه‌ی مسکونی، سامانه‌های تأمین آب، برق و گاز هستند که باید منابع مذکور برای تأمین آسایش ساکنان آن منطقه، به‌صورت پیوسته و مداوم پاسخگوی نیازهای اساسی باشند. از طرف دیگر، یکی از اهداف مهاجم فرضی منطقه‌ی مذکور ایجاد ناامنی از طریق اختلال در عملکرد سامانه‌های مذکور یا انهدام کامل آنهاست. بنابراین، باید راهبردهای بهینه دفاع از این منابع حسّاس در برابر حملات مهاجم فرضی، برنامه‌ریزی شود. یکی از راهبردهای مطلوب در این زمینه، بهینه‌یابی سرمایه‌گذاری دفاع از کل سامانه، متشکل از سه سامانه حساس تأمین‌کننده‌ی آب، برق و گاز منطقه است. فرض کنید که در مسئله مورد نظر به ترتیب، ۳، ۲ و ۲ زیرسامانه تأمین‌کننده‌ی آب، برق و گاز وجود داشته باشد که ساختار عملکردی آنها به‌صورت سری-موازی باشد. همچنین تعداد اهداف مجازی برای سامانه‌های مذکور به ترتیب برابر با ۱، ۲ و صفر در نظر گرفته شده است. تصویر۳ ساختار قابلیت اطمینان این سامانه را نشان می‌دهد.



تصویر۳: ساختار قابلیت اطمینان مطالعه موردی

در تصویر۳ اهداف مجازی با خطوط نقطه‌چین مشخص شده‌اند و به‌طور مثال، ۳۲ نشان‌دهنده‌ی زیرسامانه دوم از سامانه سوم (نیروگاه گاز) است.

سایر اطلاعات مورد نیاز برای نمونه‌سازی این مسئله در جدول ۱ نشان داده شده است.

جدول۲: مقادیر بهینه سرمایه‌گذاری دفاع و حمله برای مطالعه موردی

متغیرهای حمله		متغیرهای دفاع	
۲/۱۱۰۹	F_{11}	۰/۶۸۵۷	f_{11}
۱/۱۹۹۶	F_{12}	۰/۴۱۷۹	f_{12}
۲/۲۶۹۲	F_{13}	۰/۷۹۵۹	f_{13}
۱/۵۶۹	F_{14}	۰/۲۶۳۲	f_{14}
۱/۷۳۵۶	F_{21}	۰/۶۶۶۰	f_{21}
۲/۲۶۹۳	F_{22}	۰/۸۷۱۵	f_{22}
۰/۹۹۱۵	F_{23}	۰/۳۲۷۹	f_{23}
۱/۵۳۹	F_{24}	۰/۲۹۲۸	f_{24}
۱/۶۹۸۳	F_{31}	۰/۶۷۷۱	f_{31}
۲/۴۲۱۷	F_{32}	۰/۹۶۳۷	f_{32}

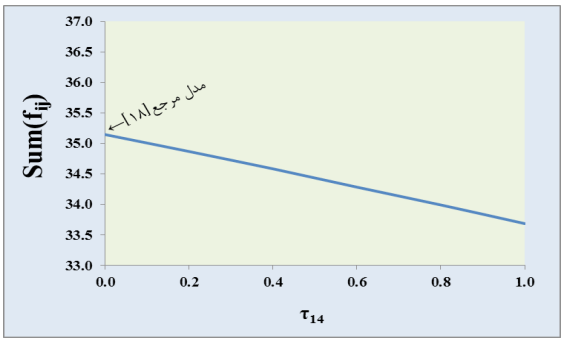
به استناد نمونه برنامه‌ریزی غیرخطی روش پیشنهادی و استفاده از آن با توجه به داده‌های جدول ۱، نتایج نهایی مسئله که نقاط تعادل سرمایه‌گذاری دفاع و حمله برای هریک از زیرسامانه‌ها است، به‌صورت جدول ۲ تعیین می‌شود.

نتایج حاصل از برنامه‌ریزی غیرخطی پیشنهادی برای مطالعه‌ی موردی، منطقی خواهد بود؛ زیرا در زیرسامانه ۱۴ که در واقع مجازی است، از نظر مهاجم با احتمال بالایی (۶۰ درصد) واقعی است، بنابراین، مهاجم برای حمله به این زیرسامانه حتماً برنامه‌ریزی می‌کند. اما مدافع با توجه به ارزش کم این زیرسامانه و همچنین مجازی بودن آن، سرمایه‌گذاری بسیار اندکی برای دفاع از این زیرسامانه می‌کند. همین موضوع برای زیرسامانه‌های ۲۳ و ۲۴ نیز منطقی است. همچنین مهاجم با توجه به تشخیص احتمالی واقعی‌بودن نسبتاً بالا برای اهداف ۱۴ و ۲۴، سرمایه‌گذاری نسبتاً زیادی را برای حمله به این اهداف مجازی پیش‌بینی می‌کند که در حقیقت بیهوده است.

تحلیل حساسیت نمونه‌ی پیشنهادی

نمونه پیشنهادی تحقیق را می‌توان در زمینه‌های مختلف تجزیه و تحلیل کرد. در این تحقیق، حساسیت نمونه پیشنهادی نسبت به تغییرات احتمال تشخیص صحیح اهداف مجازی از نظر مهاجم، تعداد اهداف مجازی، ضرایب برتری تجهیزات دفاع به حمله همچنین تغییرات ضرایب شدت اهداف مجازی، مورد تجزیه و تحلیل قرار گرفته است.

برای تحلیل حساسیت نمونه‌ی پیشنهادی نسبت به تغییرات احتمال تشخیص صحیح مهاجم از مجازی بودن اهداف، برای مثال، حالتی در نظر گرفته می‌شود که در آن، تمامی اهداف واقعی و مجازی به‌صورت صحیح از طرف مهاجم، تشخیص داده می‌شوند. برای این حالت، با حل‌کردن نمونه‌ی برنامه‌ریزی غیرخطی پیشنهادی، مجموع سرمایه‌گذاری‌های دفاع مورد محاسبه قرار می‌گیرد. ذکر این نکته لازم است که این حالت و با در نظرگرفتن ضریب برتری یکسان تجهیزات دفاع به حمله، مشابه نمونه‌ی پیشنهادی آقای هاسکن است [۱۸]. در مرحله بعد، تنها یکی از اهداف مجازی، انتخاب می‌شود و با تغییر دادن میزان



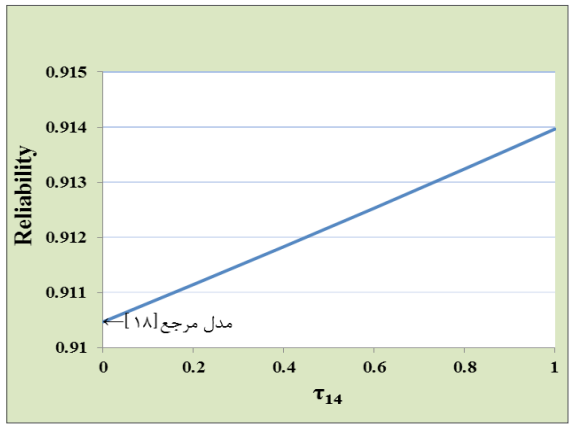
تصویر۴: روند تغییرات مجموع سرمایه‌گذاری‌های دفاع نسبت به τ_{14}

تشخیص مجازی بودن آن (از طرف مهاجم) و حل‌کردن نمونه‌ی برنامه‌ریزی غیرخطی مربوط به آن، مجموع سرمایه‌گذاری‌های دفاع و حمله محاسبه می‌شود. در این تحقیق، هدف مجازی ۱۴ مورد تجزیه و تحلیل قرار گرفته و نتایج نهایی آن، مطابق تصویر (۴) است.

تصویر ۴ نشان می‌دهد که اگر مهاجم در تشخیص مجازی بودن هدف ۱۴ به‌طور کامل اشتباه کند، یعنی این هدف را کاملاً واقعی تشخیص دهد ($\tau_{14}=1$)، مجموع سرمایه‌گذاری برای دفاع از تمامی زیرسامانه‌ها به کمترین حالت می‌رسد. وقوع این حالت‌ها منطقی است؛ زیرا مهاجم با اطمینان کامل از واقعی بودن زیرسامانه ۱۴، برای حمله به آن، برنامه‌ریزی و سرمایه‌گذاری می کند، در صورتی‌که مدافع با آگاهی از این موضوع (سرمایه‌گذاری کمتر مهاجم برای حمله به سایر زیرسامانه‌ها با توجه به محدودیت‌های مهاجم)، برای دفاع از سایر زیرسامانه‌ها به مجموع سرمایه‌گذاری کمتری نیاز دارد. با کاهش تشخیص احتمال واقعی بودن زیرسامانه مذکور که در واقع افزایش احتمال مجازی بودن آن را به دنبال دارد، مجموع سرمایه‌گذاری مدافع برای دفاع از کل زیرسامانه‌ها، افزایش می‌یابد. با توجه به نمودار تصویر ۴، درصورتی‌که مجازی بودن زیرسامانه ۱۴ به‌طور کامل از طرف مهاجم تشخیص داده شود، برای حمله به این زیرسامانه هیچ‌گونه سرمایه‌گذاری انجام نمی‌شود و مهاجم، سرمایه‌ی محدود خود را برای حمله به سایر زیرسامانه‌ها، برنامه‌ریزی می‌کند و این‌کار باعث می‌شود که مدافع، برای دفاع از سایر زیرسامانه‌ها سرمایه‌گذاری بیشتری انجام دهد.

با در نظر گرفتن تغییرات احتمال تشخیص صحیح مهاجم از مجازی‌بودن اهداف، می‌توان تغییرات قابلیت اطمینان سامانه‌ی مورد نظر را تحلیل کرد. مانند قبل برای نمونه، حالتی در نظر گرفته می‌شود که در آن، تمامی اهداف واقعی و مجازی به‌صورت صحیح از طرف مهاجم تشخیص داده می‌شوند و تغییرات احتمال تشخیص یکی از زیرسامانه‌های مجازی مورد تجزیه و تحلیل قرار می‌گیرد. تصویر ۵ روند تغییرات قابلیت اطمینان کل سامانه مورد نظر را متناسب با تغییرات احتمال تشخیص واقعی‌بودن هدف مجازی ۱۴ نشان می‌دهد.

همان‌گونه که در تصویر (۵) مشاهده می‌شود، با افزایش احتمال واقعی بودن هدف مجازی ۱۴ از طرف مهاجم(τ_{14})، قابلیت اطمینان کل سامانه افزایش می‌یابد. کمترین عدد قابلیت اطمینان، برای نمونه‌ی مشابه، نمونه‌ی آقای هاسکن [۱۸] است

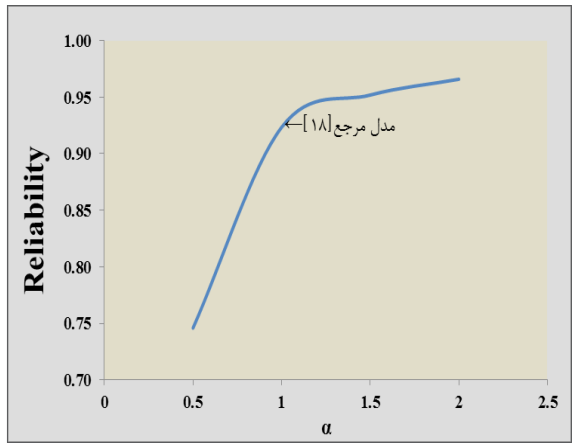


تصویر۵ :روند تغییرات قابلیت اطمینان کل سامانه نسبت به τ_{14}

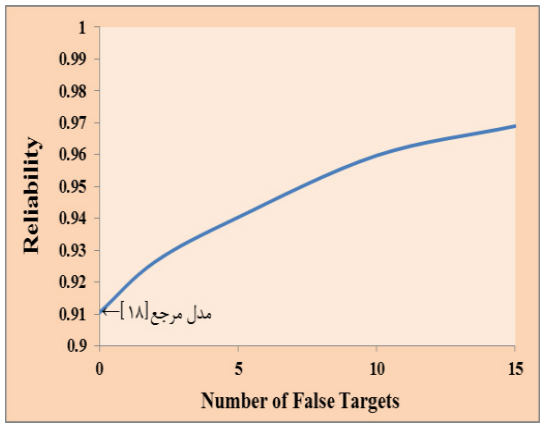
که در آن، تمام اهداف مجازی به‌طور کامل و صحیح، توسط مهاجم تشخیص داده شوند. بنابراین، وجود اهداف مجازی در بالابردن قابلیت اطمینان دفاع از کل سامانه، تأثیر مثبت و قابل توجهی دارد. به‌طور مشابه می‌توان تغییرات مجموع سرمایه‌گذاری دفاع و همچنین قابلیت اطمینان دفاع از کل سامانه را متناسب با تغییرات احتمال تشخیص مجازی بودن سایر اهداف مجازی (شامل زیرسامانه‌های ۲۳ و ۲۴)، تحلیل کرد و به نتایج مشابه فوق دست یافت.

برای تحلیل حساسیت نمونه‌ی پیشنهادی نسبت به تغییرات تعداد اهداف مجازی، مانند مرحله‌ی قبل، ابتدا مسئله در حالتی که هدف مجازی وجود ندارد، (مانند نمونه مرجع [۱۸]) ارزیابی می‌شود. سپس تعداد اهداف مجازی یکی از سامانه‌ها به‌صورت متوالی افزایش می‌یابد و در هر مرحله، نمونه پیشنهادی ارزیابی می‌شود. در مطالعه موردی این تحقیق، سامانه ۲ انتخاب شده است و تغییرات قابلیت اطمینان کل سامانه‌ی مورد نظر در تصویر ۶ نشان داده شده است. بنابراین، با افزایش تعداد اهداف مجازی، قابلیت اطمینان کل سامانه به‌صورت صعودی افزایش می‌یابد.

یکی دیگر از عواملی که می‌توان با تغییرات آن، نمونه‌ی پیشنهادی تحقیق را تجزیه و تحلیل کرد، ضریب برتری تجهیزات دفاع به حمله (α) است. برای تحلیل حساسیت نمونه‌ی پیشنهادی تحقیق نسبت به تغییرات این ضریب، در مطالعه‌ی



تصویر۷: تغییرات قابلیت اطمینان کل سامانه نسبت به ضریب α

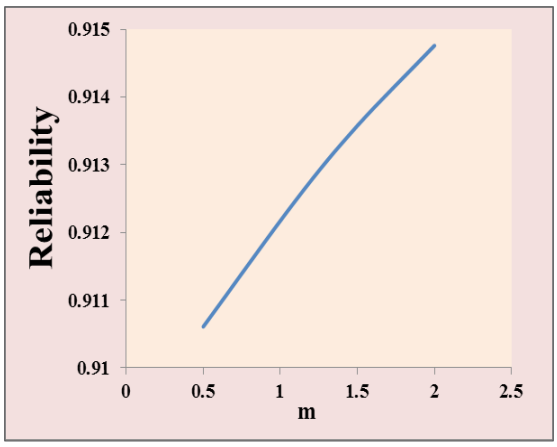


تصویر ۶: تغییرات قابلیت اطمینان کل سامانه نسبت به افزایش تعداد اهداف مجازی

موردی مذکور ابتدا تمامی ضرایب α برابر با یک در نظر گرفته می‌شود (مشابه نمونه مرجع [۱۸]) و نمونه‌ی برنامه‌ریزی غیرخطی مربوط ارزیابی می‌شود. سپس با تغییرات افزایشی و کاهشی ضرایب برتری تجهیزات دفاع به حمله و ارزیابی‌های نمونه‌ی پیشنهادی تحقیق، میزان سرمایه‌گذاری‌های دفاع و حمله مربوط به هرکدام از اهداف تعیین می‌شوند. سپس با توجه به رابطه ۳، قابلیت اطمینان کل سامانه محاسبه می شود. تصویر ۷ تغییرات قابلیت اطمینان کل سامانه نسبت به تغییرات ضریب α را نشان می‌دهد.

بنابراین، برای بالابردن قابلیت اطمینان کل سامانه، باید برتری تجهیزات دفاع به حمله افزایش یابد.

در نهایت، برای تحلیل حساسیت نمونه‌ی پیشنهادی نسبت به تغییرات ضریب شدت (m)، ابتدا یکی از اهداف مجازی انتخاب می‌شود و نمونه‌ی پیشنهادی تحقیق با در نظر گرفتن یک عدد احتمال تشخیص ثابت برای آن هدف و با تغییر دادن متوالی ضریب شدت آن هدف مجازی، مورد ارزیابی قرار می‌گیرد. برای مطالعه‌ی موردی این تحقیق، هدف مجازی ۱۴ با احتمال تشخیص ۰/۵ انتخاب و تغییرات قابلیت اطمینان کل سامانه با توجه به تغییرات ضریب شدت این هدف، در تصویر۸ نشان داده شده است.



تصویر۸: تغییرات قابلیت اطمینان کل سامانه نسبت به ضریب m

بنابراین، افزایش ضریب شدت اهداف مجازی در بالا بردن عدد قابلیت اطمینان کل سامانه تأثیر مثبت دارد.

نتیجه‌گیری و پیشنهادها

یکی از مهم‌ترین دغدغه‌های دولت‌ها، تعیین راهبردهای مطلوب و کارآمد برای دفاع از سامانه‌های حساس و حیاتی کشور است. این تحقیق با نگاه اطمینان‌پذیری و رویکرد نظریه بازی‌ها، یک نمونه‌ی برنامه‌ریزی غیرخطی برای تعیین راهبردهای بهینه دفاع و حمله ارائه کرد که در مسئله مورد نظر، مطلوبیت مدافع، افزایش قابلیت اطمینان کل سامانه و هریک از زیرسامانه‌ها و کاهش هزینه و فضای مورد نیاز تجهیزات دفاع در نظر گرفته شد. در مقابل، مطلوبیت مهاجم، افزایش موفقیت در حمله به سامانه‌های حسّاس و کاهش هزینه و وزن تجهیزات حمله منظور شد. در نمونه‌سازی مسئله‌ی مورد تحقیق، تابع احتمال شکست حمله با توجه به شاخص‌هایی مانند میزان سرمایه‌گذاری دفاع و حمله، شدت رقابت و همچنین ضریب برتری تجهیزات دفاع به حمله، تعریف شد. همچنین در مسئله‌ی مورد تحقیق، وجود اهداف مجازی مدافع برای فریب دادن مهاجم همچنین کاهش خسارت وارده به سامانه‌های حساس در نظر گرفته شد که در آن، مهاجم در پی شناسایی نکردن قطعی این اهداف مجازی، در تشخیص آنها به‌صورت احتمالی عمل می کند. در نهایت، نمونه ارائه شده‌ی تحقیق، برای یک نمونه کاربردی مورد استفاده قرار گرفت و نتایج نهایی مربوط به آنکه تعیین میزان سرمایه‌گذاری بهینه دفاع و حمله برای هریک از زیرسامانه‌هاست، محاسبه و تجزیه و تحلیل شد.

تحلیل حساسیت نمونه‌ی ارائه شده تحقیق، نشان‌دهنده‌ی این نتایج منطقی بود که با افزایش احتمال واقعی بودن اهداف مجازی از طرف مهاجم، قابلیت اطمینان کل سامانه‌ی مورد نظر افزایش می‌یابد و در مقابل، باعث کاهش مجموع سرمایه‌گذاری دفاع از زیرسامانه‌ها می‌شود. بنابراین، وجود اهداف مجازی در بهبود قابلیت اطمینان دفاع از کل سامانه همچنین بهبود میزان سرمایه‌گذاری دفاع از زیرسامانه‌ها، تأثیر مثبت و قابل توجهی دارد. همچنین با ارزیابی و تجزیه و تحلیل نمونه پیشنهادی تحقیق نسبت به تغییرات تعداد اهداف مجازی، ضریب برتری تجهیزات دفاع به حمله و ضریب شدت اهداف مجازی، نتیجه‌گیری شد که افزایش عوامل مذکور در بالا بردن قابلیت اطمینان کل سامانه مورد نظر تأثیر مثبت دارد.

برای انجام مطالعات بیشتر در زمینه موضوع تحقیق نیز می‌توان به ارائه‌ی الگوریتم‌های مفید و فراابتکاری برای بهینه‌یابی نتایج مورد نظر در مسائل پیچیده و بزرگ پرداخت. همچنین برای تحقیقات آتی، ارائه‌ی نمونه برای مکان‌یابی مراکز و مناطق حسّاس با هدف افزایش قابلیت اطمینان دفاع از اهداف پیشنهاد می‌شود. در نهایت، پیاده‌سازی نمونه‌ی این تحقیق و تحلیل نتایج برای موارد کاربردی واقعی مانند مراکز نظامی، جاده‌ها، منابع انرژی، سامانه‌های مخابراتی، مراکز تجاری، مدارس و بیمارستان‌ها می‌تواند به عنوان یک موضوع جذاب، مورد توجه محققان قرار گیرد.

منابع

1. Zhuang J, Bier VM. (2007). Balancing terrorism and natural disasters-defensive strategy with endogenous attacker effort. Operations Research, Vol. 55, 976–999.
2. Gordon LA, Loeb M. (2002). The economics of information security investment. ACM Transactions on Information and System Security, Vol. 5, 438–457.
3. Patterson SA, Apostolakis GE. (2007). Identification of critical locations across multiple infrastructures for terrorist actions. Reliability Engineering and System Safety, Vol. 92, 1183–1203.
4. Zio E, Rocco CM. (2008). Security assessment in complex networks exposed to terrorist hazard: A simulation approach. International Journal of Critical Infrastructures, vol.4, 80–95.
5. Sandler T, Siqueira K. (2009). Games and terrorism: recent developments. Simulation and Gaming, Vol. 40, 164–192.
6. Fudenberg D, Tirole J. (1991). Game theory. Cambridge, MA: MIT Press.
7. Elnaz B, János F, Dries V. (2013). Perfect equilibrium in games with compact action spaces. Games and Economic Behavior, Vol. 82, 490–502.
8. Ye D. (2013). On the complexity of deciding degeneracy in a bimatrix game with sparse payoff matrix. Theoretical Computer Science, Vol. 472, 104–109.
9. Guikema SD. (2009). Game theory models of intelligent actors in reliability analysis: a state of the art review, In: Bier VM, Azaiez MN, editors. Game theoretic risk analysis of security threats. New York: Springer, 13–31.
10. Kanturska U, Schmocker JD, Fonzone A, Bell MGH. (2009). Improving reliability through multi-path routing and link defiance: an application of game theory to transport, In: Bier VM, Azaiez MN, editors. Game theoretic risk analysis of security threats. New York: Springer, 199–227.
11. Xinyang D, Xi Z, Xiaoyan Su, Felix T.S, Yong H, Rehan S,Yong D. (2014). "An evidential game theory framework in multi Criteria decision making process." Applied Mathematics and Computation, Vol. 244, 783–793.
12. Vicki M, Aniruddha N, Vinod A. (2005). Protection of simple series and parallel systems with components of

different values. Reliability Engineering and System Safety, Vol. 87, 315–323.

13. Yong W, Gengzhong F, Nengmin W, Huigang L. (2015). Game of information security investment: Impact of attack types and network vulnerability. Expert Systems with Applications, Vol. 42, 6132–6146.

14. Levitin G. (2007). Optimal defense strategy against intentional attacks. IEEE Transactional Reliability, Vol. 56, 148–57.

15. .Levitin G, Hausken K. (2009). Parallel systems under two sequential attacks. Reliability Engineering and System Safety, Vol. 94, 763-772.

16 . Levitin G, Hausken K. (2010). Separation in homogeneous systems with independent identical elements. European Journal of Operational Research, Vol. 203, 625–634.

17 . Hausken K, Levitin G. (2009). Minmax defense strategy for complex multi state systems. Reliability Engineering and System Safety, Vol. 94, 577– 587.

18. Hausken K, Levitin G. (2009). Protection vs. false targets in series systems. Reliability Engineering and System Safety, Vol. 94, 973–981.

19. Hausken K. (2008). Strategic defense and attack for reliability systems. Reliability Engineering and System Safety, Vol. 181, 1740–1750.

20. Hausken K. (2010). Defense and attack of complex and dependent systems. Reliability Engineering and System Safety, Vol. 95, 29-42.

21. Levitin G, Hausken K, Yuanshun D. (2014). Optimal defense with variable number of overarching and individual protections. Reliability Engineering and System Safety, Vol. 123, 81–90.

22. Birolini A. (2007). Reliability Engineering: Theory and Practice, Fifth edition. Springer, Berlin Heidelberg, New York.

23- Tullock G. (1980). Efficient rent-seeking. In: Buchanan JM, Tollison RD, Tullock G, editors. Toward a theory of the rent-seeking society. College Station: Texas A&M University Press, 97–112.

24. Fontanini A, Ferreira PAV. (2014). A game-theoretic approach for the web services scheduling problem. Expert Systems with Applications, Vol. 41, 4743–4751.

25. Goldberg P, Arnoud P. (2014). On the communication complexity of approximate Nash equilibria. Games and Economic Behavior, Vol. 85, 19–31.

26. Surabhi S, Sinha SB. (2002). KKT transformation approach for multi-objective multi-level linear programming problems. European Journal of Operational Research, Vol. 143, 19–31.

27. Roghanian E, Aryanezhad MB, Sadjadi SJ. (2008). Integrating goal programming, Kuhn–Tucker conditions, and penalty function approaches to solve linear bi-level programming problems. Applied Mathematics and Computation, Vol. 195, 585–590.

28. Zhongping W, Lijun M, Guangmin W. (2014). Estimation of distribution algorithm for a class of nonlinear bilevel programming problems. Information Sciences, Vol. 256, 184–196.

29. Abdullah K, Sadan K, Lawrence VS. (2015). A game-theoretic genetic algorithm for the reliable server assignment problem under attacks. Computers & Industrial Engineering, Vol. 85, 73–85.

۳۰. اصغرپور، محمدجواد (۱۳۸۹). تصمیم‌گیری گروهی و نظریه بازی‌ها با نگرش تحقیق در عملیات. تهران، انتشارات دانشگاه تهران.