نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال چهاردهم، شماره ۲، تابستان ۱۴۰۲؛ ص ۹۹-۸۹

علمی - پژوهشی

یک مدل سه سطحی نظریه بازی‌ها برای مدل‌سازی مدافع و مهاجمین با درنظرگرفتن راهبرد فریب بین آن‌ها

حامد دهقان[۱]، حمید بیگدلی[۲*]

۱- دکترای تخصصی، دانشگاه تربیت مدرس ۲- استادیار، دانشگاه فرماندهی و ستاد آجا

(دریافت: ۱۴۰۲/۰۲/۳۰، بازنگری: ۱۴۰۲/۰۴/۲۲، پذیرش: ۱۴۰۲/۰۵/۰۷، انتشار: ۱۴۰۲/۰۶/۱۷)
DOR: 20.1001.1.26762935.1402.14.2.3.5

چکیده

امنیت اساسی‌ترین نیاز هر جامعه‌ای است که بر بخش‌های مختلف آن اثرگذار است. همچنین، به علت تهدیدات امنیتی روبه‌افزایش و محدود بودن منابع در دسترس برای مقابله، ضروری است که منابع امنیتی در حالت بهینه استقرار یابند. همچنین به علت کمبود منابع، استفاده از منابع فریبنده توسط مهاجم و مدافع مورداستفاده قرار می‌گیرد. نظریه بازی‌ها یک رویکرد متداول برای درک انگیزه‌ها، راهبردها و درنتیجه تخصیص منابع محدود مهاجم و مدافع است. در این مقاله یک بازی امنیتی استکلبرگ سه سطحی بین یک مدافع و دو مهاجم و در شرایطی که مدافع و مهاجم سعی در فریب یکدیگر دارند، مدل‌سازی می‌شود. مزیت این پژوهش نسبت به کارهای قبلی مدل‌سازی فریب مهاجم و مدافع و همچنین درنظرگرفتن محدودیت‌های مالی و محدودیت‌های مربوط به حمله و دفاع در یک مدل سه سطحی است. مطلوبیت مدافع و مهاجمین به همراه محدودیت‌های آن‌ها مدل‌سازی می‌شود. مدل با استفاده از روش کاروش - کان - تاکر به یک مدل تک‌سطحی تبدیل می‌شود و سپس حل می‌شود و کاربرد آن‌ها در تصمیم‌گیری دفاعی شرح داده می‌شود. نتایج به‌دست‌آمده نشان می‌دهد که با استفاده از مدل پیشنهادی، منابع محدود امنیتی به‌صورت بهینه تخصیص داده می‌شود که به بهبود شرایط امنیتی و مقابله بهینه با تهدیدات امنیتی می‌انجامد.

کلیدواژه‌ها: بازی امنیتی استکلبرگ، تخصیص بهینه منابع، نظریه بازی‌ها، منابع فریبنده، مدل سه سطحی

A Three-level Game Theory Model for Modeling the Defender and Attackers Considering the Deception Strategy Between Them

H.Dehghan, H. Bigdeli*

AJA University of Command and Staff

(Received: 2023/05/20, Revised: 2023/07/13, Accepted: 2023/07/29, Published: 2023/09/08)

Abstract

Security is the most basic need of any society that affects different parts of it. Also, due to increasing security threats and limited resources to deal with them, it is necessary for security resources to be deployed in an optimal state. Furthermore, because of resources limitation, the use of deceptive resources is used by the attacker and the defender. Game theory is a common way to understand the concepts, strategies and consequently the allocation of limited resources of the attacker and defender. In this paper, a three-level Stackelberg security game between a defender and two attackers is modeled in a situation where the defender and the attacker try to deceive each other. The advantage of this research compared to the previous papers is to model the attacker and defender deception as well as considering the financial limitations and limitations related to attack and defense in a three-level model. The utility of the defender and the attackers is modeled along with their limitations. The model is converted into a single-level model using the Karush-Kuhn-Tucker method and solved, describing its application in defense decision-making. The obtained results show that by using the proposed model, limited security resources are optimally allocated, which leads to the improvement of security conditions and dealing optimally with security threats.

Keywords: Stackelberg Security Game, Optimal Allocation of Resources, Game Theory, Deceptive Resources, Three-Level Model.

[۱]*Corresponding Author E-mail: h.bigdeli@casu.ac.ir

۱. مقدمه

جهانی‌شدن تهدیدات امنیت داخلی، مانند تروریسم بین‌المللی، قاچاق اسلحه یا مواد مخدر، یا سرقت‌های بزرگ به یکی از چالش‌های اصلی نیروهای امنیتی در قرن بیست و یکم تبدیل‌شده است. در تمام این چالش‌ها، منابع امنیتی محدودی وجود دارد که مانع از پوشش کامل امنیتی در هر زمان می‌شود [۱]. درنتیجه، منابع امنیتی محدود باید هوشمندانه و بهینه با درنظرگرفتن تفاوت در اولویت‌های اهدافی که نیاز به پوشش امنیتی دارند، پاسخ‌های دشمنان به وضعیت امنیتی و همچنین عدم‌اطمینان‌های احتمالی در مورد انواع، قابلیت‌ها، دانش و اولویت‌های دشمنان مورداستفاده قرار گیرند.

افزایش تهدیدات جهانی مستلزم اتخاذ تدابیر کافی برای حفظ سطح مورد انتظار امنیت است. درواقع، روش‌های مدرن و مبتنی بر علمی برای مبارزه با جرائم سازمان‌یافته و تهدیدات تروریستی در سال‌های اخیر پیشنهاد و توسعه‌یافته است. یکی از حوزه‌های تحقیقاتی مرتبط با سرعت درحال‌توسعه، بازی‌های امنیتی است که شامل مدل‌سازی مسائل امنیتی تاکتیکی در قالب یک بازی بین نیروهای امنیتی (سرویس مخفی، پلیس و غیره) و مهاجمان سازمان‌یافته (تروریست‌ها، گروه‌های نظامی و غیره) است [۲]. بازی‌های استکلبرگ[1] بازی‌های غیرمتقارن هستند که در آن‌یک بازیکن یا گروه مشخصی از بازیکنان این امتیاز را دارند که قبل از سایر بازیکنان تصمیم بگیرند. آن‌ها ابتدا بازی می‌کنند و بقیه بازیکنان از رهبر(ها) پیروی می‌کنند و بر اساس اقدامات رهبر تصمیم می‌گیرند. اخیراً مدل بازی استکلبرگ در سیستم‌هایی که مسائل امنیتی در آن‌ها وجود داشته و معیار تصمیم‌گیری حیاتی بوده است، موردتوجه قرار گرفته است. به‌عنوان‌مثال، بازی استکلبرگ مهاجم - مدافع یعنی بازی راهبردی که در آن راهبرد بازیکن نسبت به اقدامات رقیب واکنش نشان می‌دهد، در طراحی، الگوریتم‌هایی استفاده می‌شود که به تخصیص منابع امنیتی محدود کمک می‌کنند. در این مدل، مدافع راهبرد خود را اتخاذ می‌کند، سپس مهاجمان با مشاهده راهبرد مدافع، راهبردی که حداکثر مطلوبیت را داشته باشد، انتخاب می‌کنند [۳].

نظریه بازی[2] یک روش رایج برای توسعه الگوریتم‌های دفاعی به‌منظور مدل‌سازی مسائل امنیتی است. به‌عنوان‌مثال، بازی‌های استکلبرگ در طراحی الگوریتم‌هایی که به تخصیص منابع امنیتی محدود کمک می‌کنند، رایج هستند. در این مدل، هر بازیکن اهداف و ملاحظات خاص خود را در چارچوب یک سناریو دارد. انتخاب‌هایی که هر بازیکن انجام می‌دهد باید نه‌تنها پاداش و جریمه‌های بالقوه خود، بلکه پاداش و جریمه‌های احتمالی بازیکنان دیگر را نیز در نظر بگیرد [۴].

بازی‌های امنیتی[3] به طور معمول شامل دو سمت بازی با عناوین مهاجم و مدافع است. در ابتدا، مدافع درباره نحوه تخصیص منابع امنیتی در دسترس خود برای محافظت و پوشش مکان‌های نیازمند محافظت تصمیم‌گیری می‌نماید. سپس، مهاجم قبل از اتخاذ تصمیم حمله به اهداف می‌تواند راهبرد انتخاب‌شده مدافع را مشاهده نماید. مدافع و مهاجم راهبردهای را انتخاب می‌کنند که منجر به حداکثرسازی تابع هدفشان شود.

راهبرد محض در بازی امنیتی انتخاب یکی از اهداف به‌منظور دفاع یا حمل ه است. راهبرد آمیخته[4] یا ترکیبی از چند راهبرد محض تشکیل‌شده است. به‌عبارت‌دیگر، هر سمت بازی می‌تواند یک توزیع احتمال بر روی راهبردهای محض در نظر بگیرد. راهبرد ترکیبی برای یک مدافع، انتخاب میزان پوشش برای هریک از اهداف است. همچنین، راهبرد محض برای یک مهاجم انتخاب یکی از اهداف برای حمله است. در این پژوهش با تصادفی‌سازی راهبردهای مهاجمین، راهبرد ترکیبی نیز برای مهاجمین در نظر گرفته می‌شود. به‌عبارت‌دیگر، مهاجم میزان حمله به هریک از اهداف را تعیین می‌کند.

همچنین باید توجه داشت که تعداد و پیچیدگی حملات سایبری در سال‌های گذشته به طور پیوسته در حال افزایش بوده است. دشمنان، سیستم‌های ارتباطات و اطلاعات، سازمان‌های دولتی، نظامی و صنعتی و همچنین زیرساخت‌های حیاتی را هدف قرار می‌دهند و مایل‌اند مقدار زیادی پول، زمان و تخصص را برای رسیدن به اهداف خود صرف کنند. توانایی راه‌حل‌های امنیتی فعلی برای مقابله با چنین مهاجمانی آشکارا مورد تردید قرار گرفته است، تکنیک‌های فریب برای نظارت بر شبکه‌های سازمانی و شناسایی آماده‌سازی حمله و بهره‌برداری بعدی ارزشمند هستند. در چنین سناریوهایی، مدافع از اطلاعات ناقص برای فریب مهاجم استفاده می‌کند، در این مقاله این وضعیت با نظریه بازی‌ها مدل‌سازی می‌شود و رفتار بهینه‌سازی را هم برای مهاجمین و هم برای مدافع استخراج می‌شود.

نظریه بازی ابزاری کلیدی برای بهبود تصمیم‌گیری در مسائل امنیتی پیچیده است. استفاده از این ابزار در این حوزه از سال ۲۰۰۶ و با طراحی مدل استکلبرگ امنیتی محقق شد. در این مدل با استفاده از تخصیص منابع امنیتی به هشت پایانه لس‌آنجلس در فرودگاه بین‌المللی، امکان حل مسائل امنیتی با پیچیدگی بسیار زیاد را فراهم کرد [۵].

[1] Stackelberg
[2] Game Theory
[3] Security Games
[4] Mixed strategy

از آن زمان به بعد، تحقیقاتی که به تجزیه‌وتحلیل و حل بازی‌های امنیتی پرداخته‌اند، رشد قابل‌توجهی داشته‌اند که باانگیزه ایجاد مدل‌های کاربردی در حوزه‌های مختلف طراحی‌شده‌اند. با گسترش تحقیقات در حوزه بازی‌های امنیتی، این بازی‌ها قابل‌دسته‌بندی به چند بخش می‌باشند. بازی‌های امنیتی را می‌توان به دودسته تک بازی و بازی تکرارشونده تقسیم‌بندی نمود. همچنین، از حیث کاربرد، بازی‌های امنیتی را می‌توان به چهار دسته بازی‌های امنیتی زیرساخت، بازی‌های امنیتی سبز، بازی‌های امنیتی فرصت‌طلبانه جرم و جنایت و بازی‌های امنیتی سایبری تقسیم-بندی نمود [۶]. چندین مقاله پیچیدگی محاسباتی بازی‌های امنیتی را در حالات خاص بررسی کرده‌اند. کورزیک و همکاران [۷] حالات امنیتی را در نظر گرفته است که در آن هر منبع امنیتی را می‌توان برای محافظت از زیرمجموعه‌ای از اهداف اختصاص داد. لچفورد و کانیتزر [۸] بازی‌های امنیتی را روی نمودارها در نظر گرفته است که در آن اهداف گره‌ها هستند و منابع امنیتی در طول مسیرها گشت‌زنی می‌کنند. این مقاله بازی‌های امنیتی را از منظر نظری بررسی می‌کند و دیدگاهی واحد از مدل‌های مختلف بازی امنیتی ارائه می‌دهد. زو [۹] در مقاله خود بازی‌های امنیتی را از منظر نظری بررسی می‌کند و دیدگاهی واحد از مدل‌های مختلف بازی امنیتی ارائه می‌دهد. به طور خاص، هر بازی امنیتی را می‌توان با یک سیستمی مشخص کرد که از راهبردهای خالص مدافع تشکیل‌شده است. هان و همکاران [۱۰] یک رویکرد نظریه بازی را برای مقایسه سه سیاست تخصیص ماشین مجازی رایج، ازنظر امنیت (توانایی دفاع در برابر حملات هم‌زمان)، تعادل حجم کار و مصرف انرژی، طراحی کردند.

بیگدلی و حسن‌پور [۱۱] بازی‌های ماتریسی و دو ماتریسی را در محیط فازی مورد بررسی قراردادند و یک موقعیت جنگی در جنگ جهانی دوم را به‌صورت یک بازی ماتریسی با عایدی‌های فازی مدل‌سازی کرده و نشان دادند که راهبردهای به‌دست‌آمده از روش پیشنهادی با تصمیم رهنامه آمریکا مشابه است. همچنین بیگدلی و حسن‌پور [۱۲] در پژوهشی دیگر مذاکرات هسته‌ای بین دو کشور را به‌صورت یک بازی دو ماتریسی چند هدفی مدل‌سازی شده و یک روش برای محاسبه نقاط تعادل کارای ضعیف آن ارائه داده شده است. علاوه بر این، تودشکی و زهرایی [۱۳] به مدل‌سازی یک بازی امنیتی در شرایط عدم‌قطعیت پرداختند. آن‌ها برای مقابله با مسئله عدم‌قطعیت مطلوبیت‌ها را به‌صورت بازه‌ای در نظر گرفتند و با استفاده از نظریه بازی، تصمیم‌گیری و تصمیم‌سازی دفاعی را مدل‌سازی نمودند. بیگدلی و همکاران [۱۴] یک روش حل بازی‌های امنیتی چندهدفی با عایدی‌های فازی، کاربردی از این مدل را در ایجاد امنیت در ایستگاه‌های مترو ارائه دادند. در این مقاله با استفاده از عملگر تقریب نزدیک‌ترین بازه اعداد فازی، مدل بازی امنیتی فازی به مدل بازه‌ای تبدیل‌شده و به کمک شرایط کاروش‌کان‌تاکر در مسائل بازه‌ای راهبرد بهینه مدافع محاسبه می‌شود. خیرخواه و همکاران [۱۵] به مدل‌سازی عدم تقارن اطلاعات در مسئله حمله به شبکه حمل‌ونقل مواد خطرناک پرداختند. در این تحقیق تعارض موجود بین دو تصمیم‌گیرنده در حالتی که آن‌ها درک یکسانی از اطلاعات شبکه ندارند به‌صورت مسئله دوسطحی مدل‌سازی می‌شود و با استفاده از الگوریتم‌های فراابتکاری به حل آن پرداخته می‌شود.

گان و همکاران [۱۶] بازی‌های امنیتی با مدافعان ناهماهنگ را مدل‌سازی کردند که به طور مشترک از مجموعه‌ای از اهداف محافظت می‌کنند، اما ممکن است ارزش‌گذاری‌های متفاوتی برای این اهداف داشته باشند. هر مدافعی منابع خود را برنامه‌ریزی می‌کند و ابزار خود را بهینه می‌کند. در این پژوهش مدل استاندارد (تک مدافع) بازی‌های امنیتی استکلبرگ تعمیم داده می‌شود و یک مفهوم تعادلی تدوین می‌شود که ماهیت تعامل راهبرد بین بازیکنان را نشان می‌دهد. نگوین و زو [۱۷] یک مدل فریب تکرارشونده حمله‌کننده در یک بازی امنیتی طراحی کردند. نتایج مدل نشان می‌دهد که در صورت اجرای فریب تکرارشونده پتانسیل بالایی برای سود مهاجم وجود دارد. اسماعیلی و همکاران [۱۸] با استفاده از یک مدل استکلبرگ به حل مسئله بازی امنیتی با منابع فریبنده در محیط فازی پرداختند که در آن مدافع می‌تواند با درنظرگرفتن میزان بودجه موجود، به‌منظور کاهش بهره‌وری مهاجم، از منابع غیرواقعی و مخفی نیز استفاده کند. بیگدلی و طیبی [۱۹] یک بازی مدافع و مهاجم با نتایج مبهم شهودی طراحی کردند. سپس، مدل به حالت تک‌سطحی تبدیل می‌شود. درنهایت اعتبار و کاربرد روش با یک مثال عملی نشان‌داده‌شده است. نگوین و زو [۲۰] یک مدل برای انجام فریب توسط مدافع طراحی کردند. آن‌ها راهبرد فریب بهینه را در حالت‌های مختلف پاسخ مهاجمین از قبیل حالت‌هایی که مهاجمین از فریب مدافع آگاه یا ناآگاه هستند، مدل‌سازی کردند.

مزیت و نوآوری این پژوهش، چنان‌که در جدول (۱) نشان‌داده‌شده است، طراحی یک مدل سه سطحی با درنظرگرفتن فریب توسط مهاجمین و مدافعین است. تا آنجایی که محققین این مقاله می‌دانند تاکنون یک مدل سه سطحی در شرایط امنیتی طراحی نشده است. دیگر تمایز این کار با پژوهش‌های دیگر مدل‌سازی روش فریب مهاجمین و مدافع است. همچنین، محدودیت‌های مالی و غیرمالی مربوط به دفاع و حمله که در این پژوهش استفاده‌شده است به واقعی‌تر شدن مدل کمک می‌کند که در پژوهش‌های دیگر به این میزان استفاده‌نشده است.

در ادامه تحقیق در بخش دوم روش تحقیق مورد بررسی قرار می‌گیرد و مدل‌سازی صورت می‌پذیرد. سپس، در بخش سوم، نتایج مدل موردبحث و بررسی قرار می‌گیرد و درنهایت در بخش چهارم نتیجه‌گیری می‌شود. شکل (۱) مراحل کار در روش‌شناسی را نشان می‌دهد.

جدول ۱. نوآوری و تفاوت این پژوهش با پیشینه موضوع پژوهش

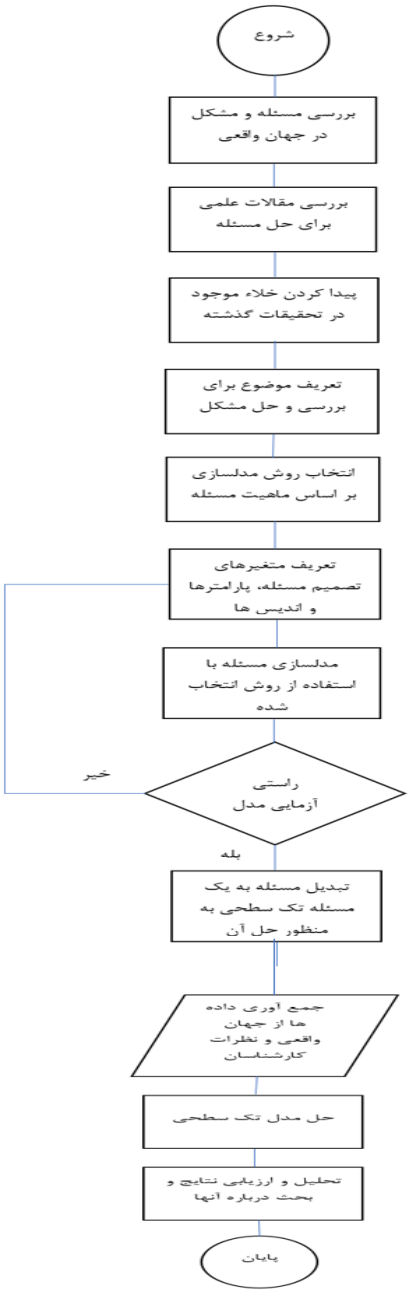
مقاله	تعداد سطح مدل	ابزار مدل‌سازی	درنظرگرفتن فریب		درنظرگرفتن محدودیت‌های مالی		درنظرگرفتن محدودیت‌های مربوط به حمله و دفاع
			مدافع	مهاجم	مدافع	مهاجم	
[۱۳]	دو	نظریه بازی‌ها					
[۱۴]	دو	نظریه بازی‌ها					✓
[۱۵]	دو	نظریه بازی‌ها			✓		✓
[۱۷]	تک	نظریه بازی‌ها و بازی تکرارشونده	✓				
[۱۸]	دو	نظریه بازی‌ها	✓		✓		
[۲۰]	تک	نظریه بازی‌ها	✓				
این پژوهش	سه	نظریه بازی‌ها	✓	✓	✓	✓	✓

۲. روش تحقیق

در این پژوهش یک مدل سه سطحی نظریه بازی طراحی می‌شود که از توابع بازیگران مسئله و محدودیت‌هایشان تشکیل‌شده است. با استفاده از روش کاروش - کان - تاکر[1]، مدل به یک ساختار تک‌سطحی تبدیل می‌شود. از نرم‌افزار بهینه‌سازی گمز برای مدل‌سازی و حل مدل تک‌سطحی استفاده می‌شود.

در مدل امنیتی استکلبرگ، یک مدافع باتوجه‌به محدودیت منابعی که دارد، باید از مجموعه‌ای از اهداف دفاع کند، درحالی‌که مهاجمین می‌توانند راهبرد و چینش مدافع را مشاهده و سپس تصمیم بگیرند. یک اقدام یا راهبرد خالص برای مدافع نشان‌دهنده به‌کارگیری مجموعه‌ای از منابع برای دفاع از اهداف است. راهبرد محض برای مدافع و مهاجم به ترتیب انتخاب یک مکان برای دفاع یا حمله است. راهبرد آمیخته برای مدافع و مهاجم یک توزیع احتمال بر روی راهبردهای خالص است. راهبرد محض برای یک مهاجم حمله به یک هدف است. راهبرد ترکیبی مهاجم فرض می‌کند که مهاجم می‌تواند حملات واقعی یا جعلی داشته باشد؛ بنابراین، در هر هدف، مجموعه‌ای از مطلوبیت‌ها در صورت حمله موفقیت‌آمیز یا جعلی و همچنین نحوه دفاع برای مدافع و مهاجم تعریف می‌شود. منابع امنیتی محدود نمی‌تواند پوشش امنیتی کامل را فراهم کند و به مهاجمان این فرصت را می‌دهد تا نحوه استقرار را کشف کرده و به نقاط ضعف حمله کنند؛ بنابراین، یک رویکرد رایج، تصادفی‌سازی برنامه‌های امنیتی برای جلوگیری از قابلیت پیش‌بینی است.

هر دو مدافع و مهاجمین راهبرد آمیخته را می‌توانند در نظر بگیرند. راهبرد آمیخته این اجازه را به بازیکنان می‌دهد تا یک توزیع احتمال روی راهبردهای محض در نظر بگیرند. عایدی هر بازیکن بستگی به نوع حمله مهاجم و میزان پوشش هدف است. درصورتی‌که مهاجم با تعداد زیادی از منابع خود به هدفی حمله کند و آن هدف بدون پوشش یا با پوشش کمی تحت حفاظت



شکل ۱. مراحل طی شده در این پژوهش

[1] Karush-Kuhn-Tucker

باشد، عایدی به‌دست‌آمده مهاجم بیشتر از مدافع خواهد بود و درصورتی‌که مهاجم حمله واقعی انجام ندهد؛ یعنی با مقدار کمی از منابع خود به هدفی حمله کند که پوشش بالایی دارد عایدی مدافع از مهاجم بیشتر خواهد بود.

در این پژوهش، دو مهاجم در نظر گرفته‌شده است که مدافع سعی دارد از سه مکانی که وظیفه حفاظت از آن‌ها را به عهده دارد، در برابر حمله این دو مهاجم محافظت نماید. به‌منظور کاهش هزینه‌های مدافع و کاهش کارایی مهاجمین، مدافع می‌تواند از منابع غیرواقعی استفاده کند. در دو حالت مهاجمین هدف را محافظت‌شده توسط مدافع می‌بینند. چنانچه هدف با منبع واقعی پوشش داده شود و یا هدف تحت محافظت غیرواقعی باشد و مهاجمین هدف را با احتمال P_F محافظت‌شده ببینند و در صورت شکست، مهاجمین آن را فاقد پوشش مشاهده می‌کنند. مهاجمین نیز می‌توانند به دو صورت جعلی و واقعی به اهداف حمله کنند. چنانچه یک مهاجم با بخش قابل‌توجهی از منابع خود اقدام به حمله کند آن حمله واقعی در نظر گرفته می‌شود و چنانچه با بخش کمی از منابع خود حمله کند، آن حمله جعلی در نظر گرفته می‌شود. احتمال اینکه مدافع حمله جعلی مهاجم را واقعی مشاهده کند R_i است. بنابراین، این احتمال وجود دارد که مدافع، حمله جعلی مهاجم را واقعی در نظر بگیرد و بر اساس آن تصمیم‌گیری می‌نماید که کاربرد روش فریب را نشان می‌دهد.

در این مدل سه سطحی مدافع ابتدا رهبر است و تصمیم اول را اتخاذ می‌کند. به این معنا که منابع خود را در سه هدفی که وظیفه حفاظت از آن‌ها را دارد، چینش و تخصیص می‌دهد. سپس، مهاجمین نیز بعد دیدن آرایش دفاعی با همکاری یکدیگر اقدام به حمله می‌کنند. مهاجم اول با دیدن چینش منابع امنیتی در مورد حمله به اهداف و همچنین میزان استفاده از منابع خود تصمیم‌گیری می‌کند و در مرحله سوم، مهاجم دوم با دیدن چینش مدافع و حمله یا حمله‌های مهاجم اول، تصمیم حمله به اهداف را اتخاذ می‌کند.

نمایه‌ها، متغیرهای تصمیم و پارامترهای مدل به ترتیب در جدول (۲)، جدول (۳) و جدول (۴) نمایش‌داده‌شده است:

جدول ۲. نمایه‌ها

تعداد مکان‌ها یا پادگان‌هایی که مدافع می‌خواهد مورد محافظت قرار دهد.	$j = 1, \dots, c$
تعداد حمله‌کنندگان	i=1,2
نوع پوشش و محافظت هدف	$k \in \{R, NR\}$
نوع حمله: واقعی یا برگه	$A \in \{R, F\}$

جدول ۳. متغیرهای تصمیم

مقدار پوشش داده شده از هدف است و احتمال موفقیت مدافع را در جلوگیری از حمله‌ای به هدف نشان می‌دهد؛ بنابراین مقدار هر دوبین صفر و یک است. به معنای دیگر نوع پوشش j است	$e_{jk} = (e_{jR}, e_{jNR})$
میزان حمله واقعی و جعلی مهاجم i به هدف j. مقدار هرکدام بین صفر و یک است.	$a_{iw}^{j} = \{a_{iR}^{j}, a_{iF}^{j}\}$

جدول ۴. پارامترهای مدل

منبع‌های یکسان امنیتی که از اهداف محافظت می‌کنند	N
مطلوبیت مدافع در مواجهه با حمله‌کننده‌های متفاوت	$U_{A1,A2}^{d}$
احتمال اینکه مهاجم i هدف j را محافظت‌شده ببیند	L_j^i
احتمال اینکه مدافع، حمله جعلی مهاجم i را واقعی ببیند	$R_i = .7$
احتمال موفقیت محافظت غیرواقعی	$P_F = 0.7$
مطلوبیت مهاجم i از حمله به مکان j در حالت حمله واقعی و مکان هم پوشش داده شده. مقدار این مطلوبیت در جدول باید مشخص شود	$U_{a_i}^{e,RR}(j)$
مطلوبیت مهاجم i از حمله به مکان j در حالت حمله جعلی و مکان هم پوشش داده شده. مقدار این مطلوبیت در جدول باید مشخص شود	$U_{a_i}^{e,RR}(j)$
مطلوبیت مدافع از حمله مهاجم i به مکان j در حالت حمله جعلی و مکان هم پوشش داده نشده. مقدار این مطلوبیت در جدول باید مشخص شود	$U_{d}^{ue,FR}(j)$
مطلوبیت مدافع i از حمله به مکان j در حالت حمله واقعی و مکان هم پوشش داده شده. مقدار این مطلوبیت در جدول باید مشخص شود	$U_{d}^{e,RR}(j)$

در بازی استکلبرگ امنیتی ابتدا مدافع اقدام اول را انجام می‌دهد و راهبرد خود را انتخاب می‌کند. راهبرد مدافع تصمیم درباره نحوه استقرار و حضور منابع امنیتی در اهداف موردنظر است. مدافع بااطلاع از اینکه پس از گرفتن تصمیم، مهاجمین می‌تواند راهبرد وی را مشاهده کند به دنبال تخصیص بهینه منابع امنیتی

برای حفاظت از اهداف است. مدافع نیز اطلاع دارد که مهاجمین پس از دیدن راهبرد مدافع، راهبردی را انتخاب می‌کند که منجر به حداکثر شدن مجموع مطلوبیتشان می‌شود. مسئله استکلبرگ از رابطه (۱) تا (۱۹) نشان داده می‌شود:

$$Max\ U^d(e,a) \quad (۱)$$

$$\sum_{j=1}^{c}(e_{jR} + e_{jNR}) \le N \quad (۲)$$

$$0 \le (e_{jR} + e_{jNR}) \le 1 \qquad j = 1,\dots,c \quad (۳)$$

$$\sum_{j=1}^{c} e_{jR} > \sum_{j=1}^{c} e_{jNR} \quad (۴)$$

$$\sum_{j=1}^{c}(b_{jR} * e_{jR} + b_{jNR} * e_{jNR}) \le B \quad (۵)$$

$$Max\ U_1^a(L,a) \quad (۶)$$

$$\sum_{j=1}^{c} a_{1R}^j + a_{1F}^j = 1 \quad (۷)$$

$$a_{1R}^j \ge 0 \qquad j = 1,\dots,c \quad (۸)$$

$$a_{1F}^j \ge 0 \qquad j = 1,\dots,c \quad (۹)$$

$$\sum_{j=1}^{c} a_{1R}^j > \sum_{j=1}^{c} a_{1F}^j \quad (۱۰)$$

$$a_{1R}^j * a_{1F}^j = 0 \qquad j = 1,\dots,c \quad (۱۱)$$

$$\sum_{j=1}^{c}(C_{jR} * a_{1R}^j + C_{jNR} * a_{1F}^j) \le C_1 \quad (۱۲)$$

$$Max\ U_2^a(L,a) \quad (۱۳)$$

$$\sum_{j=1}^{c} a_{2R}^j + a_{2F}^j = 1 \quad (۱۴)$$

$$a_{2R}^j \ge 0 \qquad j = 1,\dots,c \quad (۱۵)$$

$$a_{2F}^j \ge 0 \qquad j = 1,\dots,c \quad (۱۶)$$

$$\sum_{j=1}^{c} a_{2R}^j > \sum_{j=1}^{c} a_{2F}^j \quad (۱۷)$$

$$a_{2R}^j * a_{2F}^j = 0 \qquad j = 1,\dots,c \quad (۱۸)$$

$$\sum_{j=1}^{c}(C_{jR} * a_{2R}^j + C_{jNR} * a_{2F}^j) \le C_2 \quad (۱۹)$$

مدل از سه سطح تشکیل شده است که در سطح اول، مدافع تصمیم می‌گیرد و در سطح دوم و سوم به ترتیب مهاجم اول و دوم تصمیم‌گیری می‌کنند. تابع هدف مدافع مطلوبیت مدافع را در مواجهه با حمله مهاجمان حداکثر می‌کند. محدودیت اول مدافع، محدودیت منابع در دسترس مدافع را برای حفاظت از اهداف نشان می‌دهد. محدودیت دوم مدافع نشان می‌دهد که مدافع منابع خود را بیشتر صرف پوشش واقعی می‌کند تا پوشش غیرواقعی. محدودیت سوم مدافع نیز محدودیت‌های مالی مدافع را نشان می‌دهد و بیان می‌کند که هزینه استفاده از منابع واقعی و غیرواقعی نمی‌تواند از بودجه بیشتر باشد. بعد از اینکه مدافع تصمیم خود را گرفت، مهاجم اول برای حداکثرکردن تابع هدف خود، راهبرد خود را مشخص می‌کند. محدودیت اول مهاجم اول بیان می‌کند که حمله این مهاجم می‌تواند حمله واقعی و یا ترکیبی از حمله واقعی و جعلی باشد. محدودیت دوم و سوم مقدار حمله واقعی و غیرواقعی مهاجم اول را بزرگ‌تر مساوی صفر قرار می‌دهد. محدودیت بعدی اشاره به این مطلب دارد که مقدار حمله واقعی مهاجم باید از مقدار حمله غیرواقعی بیشتر باشد. محدودیت بعدی بیان می‌کند که هر هدف، یا مورد حمله واقعی مهاجم اول قرار می‌گیرد یا مورد حمله جعلی آن مهاجم و امکان اینکه مهاجم هم حمله جعلی به یک هدف داشته باشد و هم حمله واقعی وجود ندارد. محدودیت بعدی به محدود بودن منابع مالی مهاجم اول اشاره دارد که جمع هزینه‌های حمله واقعی و غیرواقعی از بودجه اختصاص‌یافته نمی‌تواند بیشتر باشد. در سطح سوم مهاجم دوم وجود دارد که بعد از مشاهده تصمیم مدافع و مهاجم اول اقدام به تصمیم‌گیری برای حمله می‌کند. محدودیت‌های مهاجم دوم نیز به‌مانند مهاجم اول است. مسئله بالا یک مسئله بهینه‌سازی سه سطحی است که در آن سطح اول مسئله مربوط به تصمیم‌گیری مدافع و سطح دوم مسئله مربوط به تصمیم مهاجم اول و سطح سوم مربوط به مهاجم دوم است.

تابع هدف مدافع باهدف حداکثر امنیت طراحی‌شده است. تابع هدف مهاجمین نیز به دنبال حداکثرکردن مطلوبیت خود از طریق انتخاب راهبردی است که بیشترین منفعت را داشته باشد. چنانچه هدف j مورد حمله واقعی مهاجم اول و دوم واقع شود و آن هدف توسط مدافع پوشش داده شده باشد مطلوبیت مدافع و مهاجم i به ترتیب با $U_{a_i}^{e,RR}(j)$ و $U_d^{e,RR}(j)$ نشان داده می‌شود. درواقع، برای هر هدف هشت مطلوبیت وجود دارد که بستگی به این دارد که هدف پوشش داده‌شده یا نشده و حمله مهاجم اول و دوم از نوع واقعی است یا جعلی. نوع پوشش هدف توسط مدافع می‌تواند از دو نوع واقعی یا غیرواقعی باشد که جمع این پوشش‌ها کل پوشش یک هدف توسط مدافع در مقابل حمله i را نشان می‌دهد. L_j نیز احتمال اینکه هدف j پوشش داده‌شده دیده شود، نشان می‌دهد. معادله (۲۰) بیان می‌کند که وقتی هدف پوشش داده‌شده دیده می‌شود که یا تحت پوشش واقعی باشد یا تحت پوشش غیرواقعی که در این حالت با احتمال P_F هدف پوشش داده‌شده دیده می‌شود.

$$L_j = e_{jR} + P_F e_{jNR} \quad (۲۰)$$

تابع هدف مدافع و مهاجمین به ترتیب رابطه (۲۱) و رابطه (۲۲) است:

$$U^d(e,a) = \sum_{j=1}^{c} a_{iw}^j \, U_d^{e,RR}(j) \quad (۲۱)$$

$$U_i^a(e,a_i) = \sum_{j=1}^{c} a_{iw}^j \, U_{a_i}^{e,RR}(j) \quad (۲۲)$$

صورت کامل این دو معادله به ترتیب رابطه (۲۳) و رابطه (۲۴) است:

$$\begin{aligned} U^d(e,a) = \sum_{j=1}^{c} & a_{1R}^j * a_{2R}^j * ((e_{jR} * U_d^{e,RR}(j)) \\ & + ((1-e_{jR}) * U_d^{Ue,RR}(j))) \\ & + \sum_{j=1}^{c} a_{1R}^j * a_{2F}^j * (R_2) \\ & * ((e_{jR} * U_d^{e,RR}(j)) \\ & + ((1-e_{jR}) * U_d^{Ue,RR}(j))) \\ & + \sum_{j=1}^{c} a_{1F}^j * a_{2R}^j * (R_1) \\ & * ((e_{jR} * U_d^{e,RR}(j)) \\ & + ((1-e_{jR}) * U_d^{Ue,RR}(j))) \\ & + \sum_{j=1}^{c} a_{1F}^j * a_{2F}^j * (R_1) \\ & * (R_2) * ((e_{jR} * U_d^{e,RR}(j)) \\ & + ((1-e_{jR}) * U_d^{Ue,RR}(j))) \\ & + \sum_{j=1}^{c} a_{1R}^j * a_{2F}^j * (1-R_2) \\ & * ((e_{jR} * U_d^{e,RF}(j)) \\ & + ((1-e_{jR}) * U_d^{Ue,RF}(j))) \\ & + \sum_{j=1}^{c} a_{1F}^j * a_{2R}^j * (1-R_1) \\ & * ((e_{jR} * U_d^{e,FR}(j)) \\ & + ((1-e_{jR}) * U_d^{Ue,FR}(j))) \\ & + \sum_{j=1}^{c} a_{1F}^j * a_{2F}^j * (1-R_1) \\ & * (1-R_2) * ((e_{jR} \\ & * U_d^{e,FF}(j)) + ((1-e_{jR}) \\ & * U_d^{Ue,FF}(j))) \end{aligned} \quad (۲۳)$$

$$\begin{aligned} U_i^a(L,a) = \sum_{j=1}^{c} & a_{1R}^j * a_{2R}^j * ((L_j * U_{a_i}^{e,RR}(j)) \\ & + ((1-L_j) * U_{a_i}^{Ue,RR}(j))) \\ & + \sum_{j=1}^{c} a_{1R}^j * a_{2F}^j * ((L_j \\ & * U_{a_i}^{e,RF}(j)) + ((1-L_j) \\ & * U_{a_i}^{Ue,RF}(j))) \\ & + \sum_{j=1}^{c} a_{1F}^j * a_{2R}^j * ((L_j \\ & * U_{a_i}^{e,FR}(j)) + ((1-L_j) \\ & * U_{a_i}^{Ue,FR}(j))) \\ & + \sum_{j=1}^{c} a_{1F}^j * a_{2F}^j * ((L_j \\ & * U_{a_i}^{e,FF}(j)) + ((1-L_j) \\ & * U_{a_i}^{Ue,FF}(j))) \end{aligned} \quad (۲۴)$$

برای حل مدل نیاز به این است که مدل به حالت یک‌سطحی تبدیل شود. با نوشتن شرایط کاروش - کان - تاکر برای مسئله استکلبرگ و کنار هم قراردادن مجموعه معادلات، مدل به یک مسئله تک‌سطحی تبدیل می‌شود که در رابطه (۲۵) تا رابطه (۴۲) مشاهده می‌شود.

$$Max\ U^d(e,a) \quad (۲۵)$$

$$\sum_{j=1}^{c} (e_{jR} + e_{jNR}) \le N \quad (۲۶)$$

$$0 \le (e_{jR} + e_{jNR}) \le 1 \qquad j = 1, \dots, c \quad (۲۷)$$

$$\sum_{j=1}^{c} e_{jR} > \sum_{j=1}^{c} e_{jNR} \quad (۲۸)$$

$$\sum_{j=1}^{c} (b_{jR} * e_{jR} + b_{jNR} * e_{jNR}) \le B \quad (۲۹)$$

$$\begin{aligned} & \left[\sum_{i=1}^{2} \sum_{j=1}^{c} L_j U_{a_i}^{e,RR}(j) \right. \\ & + (1-L_j) U_{a_i}^{Ue,RR}(j), \sum_{i=1}^{2} \sum_{j=1}^{c} L_j U_{a_i}^{e,RF}(j) + (1 \\ & \left. - L_j^i) U_{a_i}^{Ue,RF}(j) \right] \\ & = \sum_{i=1}^{2} \alpha_i [c,c] + \sum_{i=1}^{2} \gamma_i [-c,c] \\ & + \sum_{i=1}^{2} \sum_{j=1}^{c} \mu_i^j [a_{iF}^j, a_{iR}^j] + \beta_1 \left[\sum_{j=1}^{c} C_{jR}, \sum_{j=1}^{c} C_{jNR} \right] \\ & + \beta_2 \left[\sum_{j=1}^{c} C_{jR}, \sum_{j=1}^{c} C_{jNR} \right] \end{aligned} \quad (۳۰)$$

$$\alpha_i \left(\sum_{j=1}^{c} (a_{iR}^j + a_{iF}^j) - 1 \right) = 0 \qquad i = 1,2 \quad (۳۱)$$

$$\gamma_i\left(\sum_{j=1}^{c}-a_{iR}^{j}+\sum_{j=1}^{c}a_{iF}^{j}\right)=0 \qquad i=1,2 \tag{۳۲}$$

$$\mu_i^j\left(a_{iR}^{j}*a_{iF}^{j}\right)=0 \qquad i=1,2 \quad j=1,\dots,c \tag{۳۳}$$

$$\beta_1\left(\sum_{j=1}^{c}(C_{jR}*a_{1R}^{j}+C_{jNR}*a_{1F}^{j})-C_1\right)=0 \tag{۳۴}$$

$$\beta_2\left(\sum_{j=1}^{c}(C_{jR}*a_{2R}^{j}+C_{jNR}*a_{2F}^{j})-C_2\right)=0 \tag{۳۵}$$

$$\sum_{j=1}^{c}(C_{jR}*a_{1R}^{j}+C_{jNR}*a_{1F}^{j})\le C_1 \tag{۳۶}$$

$$\beta_2\left(\sum_{j=1}^{c}(C_{jR}*a_{2R}^{j}+C_{jNR}*a_{2F}^{j})-C_2\right)=0 \tag{۳۷}$$

$$\sum_{j=1}^{c}\left(a_{iR}^{j}+a_{iF}^{j}\right)=1 \qquad i=1,2 \tag{۳۸}$$

$$\sum_{j=1}^{c}-a_{iR}^{j}+\sum_{j=1}^{c}a_{iF}^{j}<0 \qquad i=1,2 \tag{۳۹}$$

$$a_{iR}^{j}*a_{iF}^{j}=0 \qquad i=1,2 \quad j=1,\dots,c \tag{۴۰}$$

$$\sum_{j=1}^{c}(C_{jR}*a_{1R}^{j}+C_{jNR}*a_{1F}^{j})\le C_1 \tag{۴۱}$$

$$\sum_{j=1}^{c}(C_{jR}*a_{2R}^{j}+C_{jNR}*a_{2F}^{j})\le C_2 \tag{۴۲}$$

α_i آزاد در علامت

$\gamma_i,\mu_i^j,\beta_1,\beta_2\ge 0$

۳. نتایج و بحث

مدل طراحی‌شده در جهان واقعی در انتخاب راهبرد مناسب مسائل امنیتی مثل محافظت از اهداف مهمی از قبیل پالایشگاه‌ها، پادگان‌ها و بندرها کاربرد قابل‌توجه دارد. در مدل پیشنهادی مهاجمین به اهدافی حمله می‌کنند و مدافع با درنظرگرفتن محدودیت منابع دفاعی سعی بر مقابله با حملات و حداکثرکردن تابع هدف خود را دارد. مهاجمین نیز در حملات خود در تلاش برای ازبین‌بردن و یا متوقف کردن فعالیت آن‌ها برای مدتی هستند. مهم‌ترین عملیات فریب در تاریخ جهان، عملیات فریبی است که در نبرد نرماندی علیه آلمان در جنگ جهانی دوم رخ داد. این فریب زمانی رخ داد که متفقین می‌خواستند به ساحل نرماندی حمله کنند. متفقین با استفاده از این تاکتیک، در جبهه‌های مختلف تعداد زیادی عملیات انحرافی انجام دادند. به دلیل این عملیات فریب گسترده، آلمان نمی‌دانست که حملهٔ واقعی از کجا صورت می‌گیرد.

در این مقاله سه هدف در نظر گرفته می‌شود که ازنظر مهاجمین این اهداف نسبت به بقیه اهداف می‌تواند حساس‌تر باشد. هدف سوم از اهمیت بیشتری به نسبت اهداف دیگر برخوردار است؛ بنابراین، در صورت عدم پوشش، ضرر بیشتری به مدافع می‌رسد. همچنین، در صورت حمله واقعی مهاجمین آسیب بیشتری به مدافع می‌رسد. مهاجم دوم نیز درصورتی‌که به هدفی حمله کند که پیش‌تر مهاجم اول حمله واقعی کرده است، مطلوبیت بیشتری را کسب خواهد کرد.

جدول (۵) مقدار مطلوبیت مدافع و مهاجمین را تحت شرایط مختلف نشان می‌دهد. برای به‌دست‌آوردن مطلوبیت بازیکنان از نظرات خبرگان استفاده شد. عدد اول مطلوبیت مدافع و اعداد دوم و سوم به ترتیب مطلوبیت مهاجم اول و دوم است.

جدول ۵. مطلوبیت بین مدافع و مهاجم اول و دوم

	ایستگاه ۱		ایستگاه ۲		ایستگاه ۳	
	پوشش مدافع	عدم پوشش مدافع	پوشش مدافع	عدم پوشش مدافع	پوشش مدافع	عدم پوشش مدافع
حمله واقعی مهاجم ۱ و حمله واقعی مهاجم ۲	(5,7,9)	(-5,12,15)	(3,5,7)	(-3,9,12)	(7,10,12)	(-7,14,17)
حمله واقعی مهاجم ۱ و حمله جعلی مهاجم ۲	(7,6,7)	(-3,11,12)	(5,5,5)	(-2,8,10)	(9,9,9)	(-5,14,14)
حمله جعلی مهاجم ۱ و حمله واقعی مهاجم ۲	(6,5,8)	(-4,8,13)	(4,4,6)	(-2.5,7,11)	(8,8,10)	(-5.5,12,15.5)
حمله جعلی مهاجم ۱ و حمله جعلی مهاجم ۲	(9,4.5,5)	(-2,4,4)	(7,3,4.5)	(-1, 5,7)	(11,7,8)	(-4,10,12)

به‌عنوان موضوعی از اقتصاد، مفهوم مطلوبیت برای مدل‌سازی ارزش استفاده می‌شود. این اصطلاح به‌عنوان معیاری از رضایت یا ترجیحات معرفی می‌شود. به‌عبارت‌دیگر، تنها هزینه‌ها و منافع پولی مطرح نیست و همه هزینه‌ها و منافع غیرپولی را نیز در

برمی‌گیرد. این اصطلاح در اقتصاد نوکلاسیک به‌صورت یک تابع مطلوبیت معرفی شد که نشان‌دهنده ترجیحات ترتیبی بازیکن بر مجموعه انتخاب‌هایش است. اما لزوماً دارای تفسیر اصلی نیست؛ بنابراین، مقایسه اعداد با یکدیگر و برتری یک انتخاب بر انتخاب دیگر به‌خاطر مطلوبیت بیشتر اهمیت می‌یابد.

مدافع سعی دارد که با بررسی‌های لازم و وجود محدودیت‌های بودجه‌ای، راهبردی را اتخاذ کند که منابع محدود در اختیارش به‌گونه‌ای اختصاص یابند که منجر به حداکثر امنیت شود. مدافع اطلاع دارد که پس از انتخاب راهبرد خود، مهاجم قادر به مشاهده این راهبرد خواهد بود و درنتیجه، مهاجم نیز راهبردی را انتخاب خواهد کرد بهترین پاسخ در برابر راهبرد مدافع باشد. در مدل پیشنهادی، تلاش مدافع و مهاجم در فریب بازیکن مقابل در تشخیص راهبرد اتخاذشده است. مدافع این امکان را دارد که برای کاهش کارایی مهاجمین از منابع مخفی یا به‌منظور کاهش هزینه‌های خود از منابع غیرواقعی استفاده کند. هرچند استفاده از منابع غیرواقعی باعث کاهش هزینه‌های مدافع می‌شود، اما در صورت استفاده از این منابع با احتمالی امکان شکست وجود دارد. مهاجمین نیز می‌توانند به دو صورت واقعی یا جعلی نیز به هدف‌ها حمله کنند که منجر به مطلوبیت متفاوت برای خود و مدافع می‌شوند. استفاده از روش فریب علاوه بر سردرگم کردن بازیگر مقابل، در کنترل هزینه‌ها هم مثمرثمر است.

مسئله به‌صورت یک مسئله بهینه‌سازی تک‌سطحی غیرخطی تبدیل‌شده است. برای حل مسائل غیرخطی روش‌های متنوعی وجود دارد که مهم‌ترین آن‌ها عبارت‌اند از: بهینه‌سازی نسبت طلایی(Golden Section) ، الگوریتم گرادیان نزولی (Gradient Descent)، الگوریتم نیوتن، الگوریتم مجموعه فعال(Active-set) و الگوریتم بهینه‌سازی مربعی(Quadratic Optimization) . در این پژوهش، برای حل مسئله از روش نسبت طلایی استفاده می‌شود که الگوریتم آن در ادامه می‌آید:

Step 1. Determine initial interval [a1, b1] and give the precisions

Compute λ_1, μ_1 as follows:

$$\begin{cases}\lambda_1 = a_1 + 0.382(b_1 - a_1)\\ \mu_1 = a_1 + 0.618(b_1 - a_1)\end{cases}$$

Evaluate $f(\lambda_1)$ & $f(\mu_1)$

Set k=1

Step 2. If $f(\lambda_1) > f(\mu_1)$ go to step 3

o.w. go to step 4

step 3. If $b_k - \lambda_k < \delta$ stop and output μ_k

o.w. set a_{k+1}=a_k

b_{k+1}=b_k

λ_{k+1}=μ_k

$f(\lambda_{k+1}) = f(\lambda_k)$

μ_{k+1}=$a_{k+1} + 0.618(b_{k+1} - a_{k+1})$

evaluate $f(\mu_{k+1})$ and go step 5

step 4. If $\mu_k - a_k \le \delta$ stop and output μ_k

o.w. set a_{k+1}=a_k

b_{k+1}=b_k

λ_{k+1}=μ_k

$f(\lambda_{k+1}) = f(\lambda_k)$

λ_{k+1}=$a_{k+1} + 0.382(b_{k+1} - a_{k+1})$

evaluate $f(\lambda_{k+1})$ and go step 5

step 5. Set k=k+1 and go to step 2.

جدول (۶) نتایج حاصله از مدل را نشان می‌دهند. مهاجم اول اقدام به حمله جعلی به هدف شماره یک می‌نماید. اگرچه حمله واقعی کارایی و آسیب‌رسانی بیشتری را برای مدافع به همراه دارد. اما حمله‌های غیرواقعی نیاز به هزینه کمتری دارند. مهاجم اول به اهداف شماره دو و سه به ترتیب حمله غیرواقعی و واقعی انجام می‌دهد. مهاجم دوم نیز به اهداف دو و سه به ترتیب حمله غیرواقعی و واقعی می‌کند. حملات بدین صورت بیشترین مطلوبیت را برای مهاجمین به ارمغان می‌آورد. مدافع نیز با آگاهی از این مطلب سعی در پوشش اهداف به کمک منابع مختلف خود دارد.

جدول (۷) نحوه تخصیص و پوشش اهداف را به کمک منابع امنیتی نشان می‌دهد. مدافع در برابر حمله مهاجمین به هدف سوم از پوشش واقعی استفاده می‌کند تا این هدف را که ازنظر امنیتی اهمیت بالایی دارد مورد محافظت قرار دهد. به علت هزینه بالای استفاده از منبع واقعی و کمبود منابع از منابع غیرواقعی نیز استفاده می‌شود. برای پوشش اهداف یک و دو از منابع غیرواقعی استفاده‌شده است که میزان پوشش به ترتیب برابر است با ۰/۳۷ و ۰/۴۱ مشاهده می‌شود که محدودیت‌های مالی بازیگران استفاده از منابع امنیتی غیرواقعی را برای مدافع و استفاده از حمله‌های غیرواقعی را برای مهاجمین افزایش داده است.

جدول ۶. مقدار حملات و پوشش اهداف

مقدار	متغیر
۰/۱۲	a_{1F}^1
۰/۱۶	a_{1F}^2
۰/۷۲	a_{1R}^3
۰/۲۲	a_{2F}^2
۰/۷۸	a_{2R}^3

جدول ۷. مقدار پوشش اهداف

مقدار	متغیر
۰/۳۷	e_{1F}
۰/۴۱	e_{2F}
۰/۸۲	e_{3R}

۴. نتیجه‌گیری

امنیت یک نگرانی حیاتی در سراسر جهان است که در مشکلاتی مانند حفاظت از بندرها، فرودگاه‌ها، حمل‌ونقل عمومی، و دیگر زیرساخت‌های مهم ملی در برابر تروریست‌ها، در حفاظت از حیات‌وحش و جنگل‌های ما در برابر شکارچیان و قاچاقچیان، و در محدودکردن محدودیت‌ها ظاهر می‌شود. جریان غیرقانونی سلاح، مواد مخدر و پول در سراسر مرزهای بین‌المللی. در تمام این

مشکلات، ما منابع امنیتی محدودی داریم که مانع از پوشش امنیتی همه اهداف در هر زمان می‌شود. در عوض، منابع امنیتی باید هوشمندانه با درنظرگرفتن تفاوت در اهمیت اهداف، پاسخ مهاجمان به وضعیت امنیتی و عدم‌اطمینان احتمالی در مورد انواع، قابلیت‌ها، دانش و اولویت‌های مهاجمان مورداستفاده قرار گیرند.

تهدیدات جهانی تروریسم، قاچاق مواد مخدر و سایر جرم‌ها منجر به افزایش قابل‌توجه تحقیقات در نظریه بازی برای مسائل امنیتی شده است. نظریه بازی یک رویکرد ریاضی مناسب برای استقرار منابع امنیتی محدود برای به حداکثر رساندن اثربخشی آن‌ها ارائه می‌دهد. این روش یک مدل ریاضی برای تصمیم‌گیری‌های امنیتی فراهم می‌کند. چارچوب‌های تحلیلی حاصل منجر به تخصیص بهتر منابع محدود و پاسخ‌های آگاهانه‌تر به مشکلات امنیتی در سیستم‌ها و سازمان‌های پیچیده می‌شود. مدل پیشنهادی برای ارتقا امنیت در طیف گسترده‌ای از سیستم‌های فیزیکی سایبری و زیرساخت‌های حیاتی مانند سیستم‌های قدرت الکتریکی، خدمات مالی، حمل‌ونقل، مراکز داده و شبکه‌های ارتباطی قابل‌استفاده است.

در این پژوهش یک مدل نظریه بازی متشکل از یک مدافع و دو مهاجم تحت شرایط فریب مدل‌سازی شد. مدافع به‌عنوان رهبر ابتدا تصمیمات دفاعی خود را اتخاذ می‌کند و سپس مهاجمین که تلاش دارند درمجموع بیشترین آسیب را وارد کنند، اقدام به تصمیم‌گیری می‌کنند. مزیت و تفاوت مدل نسبت به پژوهش‌های قبلی مدل‌سازی فریب مدافع و مهاجم با درنظرگرفتن محدودیت‌های مالی و محدودیت‌های منطقی مربوط به دفاع و حمله در یک مدل سه سطحی است. نتایج مدل نشان می‌دهد که مدافع می‌تواند با استفاده از مدل طراحی‌شده تابع هدف خود را بهینه بسازد. همچنین برای کاهش هزینه‌ها، مدافع از منابع غیرواقعی نیز استفاده می‌کند. نتایج مدل بهترین چینش منابع مدافع در برابر حملات مهاجمین است. باتوجه‌به ساختار بازی، مدافع در ابتدا این ترکیب چینش را در برابر حمله مهاجمین قرار می‌دهد و انتظار می‌رود که مهاجمین نیز به‌منظور حداکثر ساختن مطلوبیت خود اقدام به حمله نمایند. استفاده از فریب، کارایی بازیگر مقابل را کاهش می‌دهد و تابع هدف بازیکنان نسبت به حالتی که شرایط اطلاعات کامل بین بازیکنان برقرار است، وضعیت بدتری دارد.

برای تحقیقات آتی می‌توان استفاده از مدل‌های چندهدفه را مدنظر قرارداد. همچنین، افزایش تعداد مهاجمین و اهداف که علاوه بر نزدیکی به واقعیت، برای حل مدل نیاز به توسعه روش‌های حل است، مدنظر قرارداد. مدل‌سازی در شرایط اطلاعات ناکامل از مطلوبیت بازیگران و در حالتی که بازیگران سیگنال دریافت می‌کنند نیز می‌تواند موضوع جذابی برای تحقیقات آتی باشد.

۵. مرجع‌ها

[1] Garrec, T. “Continuous Patrolling and Hiding Games”; Eur. J. Oper. Res. 2019, 277, 42-51. https://doi.org/10.1016/j.ejor.2019.02.026

[2] Kar, D.; Nguyen, T.H.; Fang, F.; Brown, M.; Sinha, A.; Tambe, M.; Jiang, A.X. “Trends and Applications in Stackelberg Security Games”; Handbook of dynamic game theory, 2017. 1-47.

[3] Yuan, Y.; Sun, F.; Liu, H. “Resilient Control of Cyber-physical Systems against Intelligent Attacker: a Hierarchal Stackelberg Game Approach”; Int. J. Syst. Sci. 2016, 47, 2067-2077. https://doi.org/10.1080/00207721.2014.973467

[4] Hunt, K.; Agarwal, P.; Zhuang, J. “Technology Adoption for Airport Security: Modeling Public Disclosure and Secrecy in an Attacker-Defender Game”; Reliab. Eng. Syst. Safe 2021, 107355. https://doi.org/10.1016/j.ress.2020.107355

[5] Sinha, A.; Fang, F.; An, B.; Kiekintveld, C; Tambe, M. “Stackelberg Security Games: Looking Beyond a Decade of Success”; Int. Joint Conf. Artificial Intelligence 2018, 1-13. https://doi.org/10.24963/ijcai.2018/775

[6] An, B.; Tambe, M.; and Sinha, A., “Stackelberg security games (ssg) basics and application overview”; Improving Homeland Security Decisions. 2017. 2. 485.

[7] Korzhyk, D.; Conitzer, V.; Parr, R. “Complexity of Computing Optimal Stackelberg Strategies in Security Resource Allocation Games”; Twenty-Fourth AAAI Conf. Artificial Intelligence. 2010. 805-810.

[8] Letchford, J.; Conitzer, V. “Solving security games on graphs via marginal probabilities”; Twenty-Seventh AAAI Conf. Artificial Intelligence. 2013. 591-597. https://doi.org/10.1609/aaai.v27i1.8688

[9] Xu, H.; “The mysteries of security games: Equilibrium computation becomes combinatorial algorithm design”; Conf. Economics and Computation. 2016. 497-514.

[10] Han, Y.; Alpcan, T.; Chan, J.; Leckie, C. “Security Games for Virtual Machine Allocation in Cloud Computing”; 4th Int. Conf. Decision and Game Theory for Security. 2013. 99-118.

[11] Bigdeli, H.; Hassanpour H.; Tayyebi, J. “The Optimistic And Pessimistic Solutions of Single and Multiobjective Matrix Games with Fuzzy Payoffs and Analysis of Some of Military Problems”; J. Adv. Defense Sci. & Technol. 2016, 8, 133-45 (In Persian).

[12] Bigdeli, H.; Hassanpour, H; Tayyebi, J. “Constrained Bimatrix Games with Fuzzy Goals and Its Application in Nuclear Negotiations”; J. Numerical Anal. Optim. 2018, 8, 81-110. https://doi.org/10.1142/S0218488523500459

[13] Toudashki, M.; Zahraee, S.; “Solving Multiobjective Security Games with Interval Payoffs”; J. Wargaming 2020, 2, 71-90. https://doi.org/10.22034/ijwg.2020.106194

[14] Bigdeli, H.; Hassanpour, H. “Modeling and Solving Multiobjective Security Game Problem Using Multiobjective Bilevel Problem and Its Application in Metro Security System”; J. Elect. Cyber Def. 2017, 31-38 (In Persian). https://doi.org/10.22034/ijwg.2020.106194

[15] Kheirkhah, A. S.; Navidi, H. R.; Bidgoli, M. M. “Modeling and Solving the Hazmat Routing Problem under Network Interdiction with Information Asymmetry”; J. Trans. Eng. 2017, 9, 17-36. https://dor.net/20.1001.1.20086598.1396.9.1.1.7

[16] Gan, J; Elkind, E; Wooldridge, M. “Stackelberg Security Games With Multiple Uncoordinated Defenders”; 17th Int. Conf. Autonomous Agents and Multiagent Systems. 2018. 703-711. https://dlnext.acm.org/doi/abs/10.5555/3237383.3237487

[17] Nguyen, T.; Xu, H. "Imitative Attacker Deception in Stackelberg Security Games"; IJCAI. 2019, 528-534. https://doi.org/10.24963/ijcai.2019/75

[18] Esmaieli, S.; Hassanpour, H; Bigdeli, H. "Lexicographic Programming for Solving Security Game with Fuzzy Payoffs and Computing Optimal Deception Strategy"; Defensive Future Study Researches J. 2020, 5, 89-108. https://doi.org/10.22034/dfsr.2020.39783

[19] Bigdeli, H.; Tayyebi, J. "A Defender-Attacker Game with Intuitionistic Fuzzy Payoffs"; 14th Int. Conf. Iranian Operations Research Society 1400, 60-74.

[20] Nguyen, T.; Xu, H. "When Can the Defender Effectively Deceive Attackers in Security Games?"; Thirty-Sixth AAAI. Conf. Artificial Intelligence 2022. 9405-9412.