آینده‌پژوهی دفاعی، سال دوم، شماره ۶، پائیز ۱۳۹۶

تاریخ دریافت: ۱۳۹۷/۰۵/۲۸ تاریخ پذیرش: ۱۳۹۷/۰۷/۲۶

از صفحه ۷ تا صفحه ۲۹

ارائه یک مدل و روش حل بازی‌های امنیتی فازی و کاربرد آن در آینده‌پژوهی تهدیدات امنیتی

حمید بیگدلی*[۱]

جواد طیبی[۲]

چکیده

تهدیدات جهانی تروریسم، قاچاق مواد مخدر و سایر جرایم، نیاز به استقرار منابع امنیتی محدود برای به حداکثر رساندن اثربخشی آن‌ها را افزایش داده است. پیش‌بینی اقدامات آینده و بررسی تمام راهبردهای ممکن مهاجمان تأثیر زیادی در موفقیت نبرد دارد. نظریه بازی یکی از فنون آینده‌پژوهی محسوب می‌شود. در این مقاله به بررسی بازی‌های امنیتی در محیط فازی پرداخته شده است. بازی‌های امنیتی مدل رویارویی یک مدافع و چند نوع مهاجم را مورد بررسی قرار می‌دهد. هدف این مقاله، ارائه یک مدل و روشی برای محاسبه راهبرد بهینه مدافع در شرایط عدم قطعیت است. نحوه مدل‌سازی تهدیدات امنیتی مراکز حمل و نقل عمومی شرح داده شده است. برای حل مشکل عدم قطعیت مدافع برای رویارویی با نوع مهاجم ناشناخته از رویکرد بازی بیزی استفاده شده است و برای رفع مشکل عدم قطعیت ناشی از ابهام در فهم کارشناسان و قضاوت نادقیق آنها، نظریه فازی به کار گرفته شده است. پس از ارائه مدل، مسأله با استفاده از α – برش‌های اعداد فازی به صورت قطعی نوشته شده است. در نهایت به بررسی مدل به دست آمده و نقش آن در آینده‌پژوهی تهدیدات امنیتی پرداخته شده است، و اعتبار روش پیشنهادی برای یک نمونه کاربردی مورد بررسی قرار گرفته است.

واژه‌های کلیدی:

آینده پژوهی، بازی امنیتی، مدل‌سازی تهدید، مجموعه‌های فازی، امنیت مراکز حمل و نقل.

---

[۱]. پژوهشگر پژوهشکده عالی جنگ، دانشگاه فرماندهی و ستاد آجا

[۲]. استادیار گروه مهندسی صنایع، دانشگاه صنعتی بیرجند

* نویسنده مسئول: Email: hamidbigdeli92@gmail.com

مقدمه

امنیت یک نگرانی مهم برای بشر در همه عصرها و در سرتاسر نقاط جغرافیایی دنیا است. متأسفانه با پیشرفت علم و توسعه فناوری، تنوع تهدیدات تروریستی که در آینده رخ خواهد داد، رو به افزایش است. تروریسم و قاچاق مواد مخدر از جمله جرایمی هستند که در اقصی نقاط جهان مشاهده می‌شوند. از آنجا که منابع امنیتی محدود نمی‌تواند در همه جا و در هر زمانی حضور داشته باشد، این قبیل مهاجمان می‌توانند از این خلأهای امنیتی استفاده کنند. این موارد سبب می‌شود تا نیروهای امنیتی به دنبال راهبردی برای مقابله با این تهدیدات باشند. پیش‌بینی انواع مهاجمان، بررسی اقدامات آینده آن‌ها و مطالعه راهبرد مقابله با آن‌ها نقش بسیار مهمی در موفقیت هر چه بیشتر نیروهای امنیتی دارد. در حقیقت، آینده‌پژوهی تهدیدات امنیتی نقش بسزایی را در ایجاد امنیت و ثبات و پایداری نظام و آرامش مردم ایفا می‌کند.

نظریه بازی از فنون آینده‌پژوهی است و نقش مهمی در مطالعه موارد مذکور دارد. نظریه بازی شاخه‌ای از تحقیق در عملیات محسوب می‌شود که رفتار ریاضی حاکم بر یک موقعیت راهبردی را مورد بررسی قرار می‌دهد. محبوبیت نظریه بازی در میان رشته‌های مختلف، از جمله اقتصاد، زیست شناسی، علوم سیاسی، علوم رایانه، مهندسی برق، کسب و کار، حقوق و سیاست عمومی، در حال افزایش است. در عرصه امنیت که در آن نظریه بازی همیشه محبوب بوده است، اکنون افزایش چشم‌گیر استفاده از آن مشاهده می‌شود. بازی امنیتی دسته خاصی از بازی‌های استاکلبرگ[1] مهاجم- مدافع است. این بازی میان یک مدافع و مهاجم انجام می‌گیرد. در صورتی که بازی میان یک مدافع و چند نوع مهاجم صورت گیرد، آن را بازی امنیتی چند هدفی گوییم. در این نوع از بازی، عدم قطعیت وجود دارد؛ زیرا مدافع نمی‌داند با چه نوع مهاجمی مواجه خواهد شد.

در این مقاله، برای مدل‌سازی این تهدیدات امنیتی از بازی امنیتی استفاده می‌شود. در این مدل، مدافع در ابتدا راهبرد خود را اتخاذ می‌کند، سپس مهاجمان با مشاهده راهبرد مدافع، بهترین راهبرد خود را انتخاب می‌کنند. با توجه به اینکه مهاجمان راهبرد مدافع و خلأهای امنیتی را مشاهده می‌کنند، اتخاذ راهبرد برای مدافع بسیار سخت خواهد بود. مدافع می‌داند که پس از اتخاذ تصمیم، مهاجمان از این تصمیم اطلاع یافته و به دنبال راهی برای حمله با وارد کردن بیشترین خسارت و متحمل شدن کمترین هزینه می‌باشند. برای کمک به مدافع در

[1]. Stackelberg

انتخاب راهبرد، تصادفی‌سازی در بازی امنیتی پیشنهاد می‌شود. از طرفی در مدل‌سازی بازی از قضاوت کارشناسان خبره در اعمال عایدی‌های بازیکنان برای هر پیامد بازی استفاده می‌شود. با توجه به فهم مبهم کارشناسان و اطلاعات نادقیق آن‌ها، مدل بازی شامل عدم قطعیت خواهد بود که برای رفع این مشکل، استفاده از نظریه فازی پیشنهاد می‌شود. با توجه به اهمیت این موضوع، در این پژوهش، مدل‌سازی تهدیدات امنیتی در محیط عدم قطعیت مورد مطالعه قرار گرفته و سپس روشی برای محاسبه راهبرد بهینه مدافع ارائه می‌شود.

مبانی نظری و پیشینه پژوهش

پیشینه پژوهش

پس از انتشار کتاب نظریه بازی و رفتار اقتصادی توسط وان نیومن و مورگنسترن[1] (Neumann, 1944:1)، نظریه بازی به سرعت رشد یافت و کاربردهای وسیعی در علوم مختلف پیدا کرد. سرهنگ الیور هایوود[2] (Haywood, 1989:1) در مقاله خود اهمیت نظریه بازی را در تصمیم‌گیری فرماندهی نشان داد. او نبردهای مختلفی از جنگ جهانی دوم را از دید نظریه بازی بررسی کرد و نتیجه گرفت که تصمیم دکترین نظامی مشابه با جواب به دست آمده از نظریه بازی است. ارزیابی سرهنگ هایوود انجمن تحقیق در عملیات را تشویق کرد تا روش‌های نظریه بازی را بیشتر مورد بررسی قرار دهند و در تصمیم‌گیری‌های نظامی از این نظریه استفاده کنند. در دهه اخیر نظریه بازی به طور گسترده در مسائل نظامی و امنیتی مورد استفاده قرار گرفته است (برای اطلاعات بیشتر مرجع (Tambe, 2012:1) را ببینید). سناریوهای دزد و پلیس (Gatti, 2008:1)، امنیت شبکه‌های کامپیوتری (Lye & Wing, 2005:1)، سیستم دفاع موشکی ضدبالستیک (Brown et al, 2005:1) و تروریسم (Sandler & A.M, 2003:1) ازجمله این کاربردها هستند. در دهه اخیر اقدامات کاربردی در این زمینه در کشور آمریکا و در شهرهای لس‌آنجلس و نیویورک صورت گرفته است (Tambe, 2012:1).

نویسندگان در کارهای قبلی بازی‌های ماتریسی و دوماتریسی را در محیط فازی مورد بررسی قرار دادند و موقعیت آورانشه در جنگ جهانی دوم را به صورت یک بازی ماتریسی با عایدی‌های فازی مدل‌سازی کرده و نشان دادند که راهبردهای به دست آمده از روش پیشنهادی با تصمیم دکترین آمریکا مطابقت دارد (Bigdeli & Hassanpour, 2016:1;

---

1. Von Neumann & Morgenstern
2. Oliver Haywood

Bigdeli et al., 2016:1). همچنین بازی مذاکرات هسته‌ای بین دو کشور را به صورت یک بازی دوماتریسی چندهدفی مدل‌سازی کرده و یک روش برای محاسبه نقاط تعادل کارای ضعیف آن ارائه دادند (Bigdeli et al., 2018:1). همچنین بیگدلی و حسن‌پور (۲۰۱۶) به بررسی بازی‌های چندهدفی در محیط قطعی پرداختند و از روش برنامه‌ریزی آرمانی در محاسبه راهبرد بهینه مدافع استفاده کردند (Bigdeli & Hassanpour, 2016:1). بیگدلی و همکاران (۲۰۱۸) علاوه بر ارایه یک روش حل بازی‌های امنیتی چندهدفی با عایدی‌های فازی، کاربردی از این مدل را در ایجاد امنیت در ایستگاه‌های مترو ارائه دادند (Bigdeli et al., 2018:1). در آن مقاله با استفاده از عملگر تقریب نزدیکترین بازه اعداد فازی، مدل بازی امنیتی فازی به مدل بازه‌ای تبدیل شده و به کمک شرایط کاروش کان تاکر در مسائل بازه‌ای راهبرد بهینه مدافع محاسبه می‌شود. خیرخواه و همکاران (۲۰۱۶) به مدل‌سازی عدم تقارن اطلاعات در مسأله حمله به شبکه حمل و نقل مواد خطرناک پرداختند (kheirkhah et al, 2016:1). در این تحقیق تعارض موجود بین دو تصمیم‌گیرنده در حالتی که آن‌ها درک یکسانی از اطلاعات شبکه ندارند به صورت مسأله دوسطحی مدل‌سازی می‌شود و با استفاده از الگوریتم‌های فراابتکاری به حل آن پرداخته می‌شود.

مبانی نظری پژوهش

در این بخش مقدماتی از مفاهیم مجموعه‌های فازی و بازی‌های امنیتی که مورد نیاز بخش‌های آتی است، مرور می‌شود.

مفاهیم اولیه مجموعه‌های فازی

یک مجموعه فازی به صورت زیرمجموعه $\tilde{a}$ از مجموعه مرجع X با تابع عضویت $\mu_{\tilde{a}}: X \to [0,1]$ تعریف می‌شود که به هر عنصر $x \in X$ یک عدد حقیقی $\mu_{\tilde{a}}(x)$ از بازه $[0,1]$ تخصیص می‌دهد (Sakawa, 1993:1).

تبصره۱: بدیهی است که هر مجموعه‌ی معمولی مانند A را می‌توان مجموعه‌ای فازی در نظر گرفت که تابع عضویت آن، همان تابع نشانگر مجموعه A است.

تعریف۱. مجموعه فازی $\tilde{a}$ از مجموعه اعداد حقیقی را که تابع عضویت آن $\mu_{\tilde{a}}(x)$ در شرایط زیر صدق کند، یک عدد فازی گویند (Sakawa, 1993:31).

۱) $\mu_{\tilde{a}}: X \to \mathrm{R}$ یک تابع نیمه پیوسته باشد.

۲) در خارج از بازه‌ای مانند $[a,d]$، $\mu_{\tilde{a}}(x) = 0$.

۳) اعدادی حقیقی مانند b,c موجود باشند به طوری که $a \le b \le c \le d$ و

الف) $\mu_{\tilde{a}}(x)$ در $[a,b]$ صعودی باشد،

ب) $\mu_{\tilde{a}}(x)$ در $[c,d]$ نزولی باشد،

ج) در $[b,c]$، $\mu_{\tilde{a}}(x)=1$.

برای هر $\alpha \in [0,1]$، α- برش مجموعه فازی $\tilde{a}$ که با $\tilde{a}_\alpha$ نمایش داده می‌شود یک مجموعه معمولی است که به صورت $\tilde{a}_\alpha = \{x \mid \mu_{\tilde{a}}(x) \ge \alpha\}$ تعریف می‌شود و چنانچه $\alpha = 0$، $\tilde{a}_0$ به صورت $cl\{x \mid \mu_{\tilde{a}}(x) > 0\}$ تعریف می‌شود که cl به معنی بستار مجموعه است. تکیه‌گاه $\tilde{a}$ که با $Supp(\tilde{a})$ نمایش داده می‌شود، مجموعه‌ی تمام نقاط $x \in X$ است که $\mu_{\tilde{a}}(x) > 0$. هر α- برش عدد فازی $\tilde{a}$ یک بازه‌ی بسته به صورت $[a_\alpha^L, a_\alpha^R]$ است که در آن

$$a_\alpha^L = inf\{x \in \mathrm{R} \mid \mu_{\tilde{a}}(x) \ge \alpha\},\ a_\alpha^R = sup\{x \in \mathrm{R} \mid \mu_{\tilde{a}}(x) \ge \alpha\}.$$

عدد فازی مثلثی $\tilde{a} = (a^l, a^m, a^r)$، یک عدد فازی خاص است که تابع عضویت آن به صورت زیر می‌باشد:

$$\mu_{\tilde{a}}(x) = \begin{cases} \dfrac{(x-a^l)}{(a^m-a^l)} & a^l \le x \le a^m \\ \dfrac{(a^r-x)}{(a^r-a^m)} & a^m \le x \le a^r \\ 0 & OW \end{cases}$$

که در آن a^m نقطه میانی و a^l و a^r به ترتیب نقاط انتهایی چپ و راست $Supp(\tilde{a})$ می‌باشند. از رابطه‌ی فوق به سادگی نتیجه می‌شود که هر عدد فازی مثلثی را می‌توان مستقیماً از ۰- برش و ۱- برش آن به دست آورد. در واقع $[a_\alpha^L, a_\alpha^R] = \alpha\tilde{a}_1 + (1-\alpha)\tilde{a}_0$.

مفاهیم مقدماتی بازی‌های امنیتی

مطالب این زیربخش از مرجع (Tambe, 2012:1; Bigdeli et al, 2018:1) مرور می‌شود.

بازی‌های امنیتی در حالت کلی شامل دو بازیکن با عناوین مدافع و مهاجم هستند. مدافع ابتدا در مورد چگونگی تخصیص m منبع امنیتی برای پوشش یک مجموعه از اهداف T که $m < |T|$ تصمیم‌گیری می‌کند و مهاجم قبل از انتخاب هدف برای حمله، راهبرد مدافع را

نظاره می‌کند. راهبردهای محض مدافع را زیرمجموعه‌ای از اهداف T تعریف می‌کنیم به طوری که حداکثر m هدف از مجموعه T پوشش داده شده باشد. راهبرد محض مهاجم انتخاب یک هدف برای حمله است. به جز راهبرد محض راهبرد دیگری به نام راهبرد آمیخته وجود دارد. راهبرد آمیخته به بازیکنان اجازه می‌دهد تا یک توزیع احتمال روی راهبردهای محض در نظر بگیرند. با توجه به راهبرد آمیخته مدافع می‌توان میزان پوشش هر هدف را محاسبه کرد. راهبرد آمیخته مدافع را به صورت فشرده با بردار پوشش $c = c_t$ نمایش می‌دهیم که در آن c_t احتمال پوشش هدف t است. راهبرد آمیخته مهاجم را با بردار $a = a_t$ نمایش می‌دهیم که نشان دهنده احتمال حمله به هدف t است. فضای راهبردهای آمیخته مدافع و مهاجم را به ترتیب با C و A نمایش می‌دهیم. عایدی‌های هر بازیکن وابسته به میزان پوشش هدف مورد حمله قرار گرفته است. فرض کنید مهاجم به هدفی حمله کند که توسط مدافع با منابع امنیتی بسیار کمی مورد حفاظت قرار گرفته باشد، در این صورت عایدی مهاجم از عایدی مدافع بالاتر خواهد بود. در صورتی که هدف مورد حمله با منابع امنیتی بالایی توسط مدافع حفاظت شده باشد، عایدی بازیکن مدافع بالاتر از عایدی بازیکن مهاجم خواهد بود. با توجه به موارد مذکور بازی امنیتی همواره یک بازی مجموع صفر نیست. زیرا در حوزه‌های واقعی، مهاجمان و مدافعان اغلب دارای ترجیحات و معیارهای متفاوت هستند. قدرت بازیکنان در حفاظت از یک هدف و حمله به آن هدف در سناریوهای مختلف و از دیدگاه هر بازیکنی متفاوت است و ممکن است با انتخاب راهبردهای خود هر کدام به درصدی از موفقیت یا شکست برسند.

عایدی مدافع برای هدف مورد حمله پوشش داده شده با $U^{c,d}(t)$ و برای هدف مورد حمله پوشش داده نشده با $U^{u,d}(t)$ نمایش داده می‌شود. به طور مشابه عایدی‌های مهاجم با $U^{c,a}(t)$ و $U^{u,a}(t)$ نمایش داده می‌شود.

فرض کنید مدافع و مهاجم به ترتیب راهبردهای c و a را انتخاب کنند، در این صورت عایدی‌های مورد انتظار مدافع و مهاجم به صورت زیر تعریف می‌شوند:

$$U^d(c,a) = \sum_{t \in T} a_t U^d(c,t),$$

$$U^a(c,a) = \sum_{t \in T} a_t U^a(c,t),$$

که در آن

$$U^d(c,t) = c_k U^{c,d}(t) + (1-c_k) U^{a,d}(t),$$

و

$$U^a(c,t)=c_k U^{c,a}(t)+(1-c_k)U^{u,a}(t).$$

در مدل بازی امنیتی، مدافع ابتدا راهبرد خود را انتخاب می‌کند و سپس مهاجم با مشاهده راهبرد مدافع، بهترین پاسخ به راهبرد مدافع را انتخاب می‌کند. تابع پاسخ مهاجم را با $g:C\to A$ نمایش می‌دهیم که به ازای هر راهبرد آمیخته c مدافع، راهبرد پاسخ $g(c)$ مهاجم را برمی‌گرداند. جواب استاندارد برای این بازی‌ها مفهومی تحت عنوان تعادل استاکلبرگ قوی است. جفت راهبرد $c,g(c)$ تعادل استاکلبرگ قوی است، هرگاه در شرایط زیر صدق کند:

۱) مدافع بهترین پاسخ را می‌دهد: $U^d(c,g(c))\geq U^d(c',g(c')),\ \forall c'$

۲) مهاجم بهترین پاسخ را می‌دهد. یعنی $F^a(c)=\arg\max_a U^a(c,a)$ که در آن $F^a(c)$ بهترین پاسخ مهاجم در برخورد با راهبرد c مدافع است.

۳) مهاجم به صورت بهینه برای مدافع گره باز می‌کند. به این معنی که او استراتژی بهینه خود را طوری انتخاب می‌کند، که از نظر مدافع نیز مطلوب است. یعنی:

$$U^d(c,g(c))\geq U^d(c,a'),\quad a'\in F^a(c)$$

در این مقاله مسأله‌ای مورد بررسی قرار می‌گیرد که در آن مدافع با چند نوع مهاجم مواجه است که هر کدام از مهاجمان اهداف متفاوتی را دنبال می‌کنند. در حقیقت برای هر نوع مهاجم، ماتریس بازی جداگانه‌ای مشخص می‌شود. چون مدافع نمی‌داند با چه نوع مهاجمی روبرو خواهد شد لذا با یک مسأله بازی با اطلاعات ناکامل روبرو می‌شویم.

مدل سازی بازی امنیتی برای تهدیدات امنیتی مراکز حمل و نقل عمومی

بازی امنیتی مورد بحث در این مقاله، مدل تعارض بین یک مدافع و چند نوع مهاجم را مورد بررسی قرار می‌دهد. موارد مطرح شده برای ایجاد امنیت در مراکز عمومی و پر تردد شهری مناسب است. جزئیات مدل به صورت زیر و در چند زیربخش شامل مدل‌سازی تهدید در مراکز حمل و نقل، مدل‌سازی چالش‌های تخصیص منابع امنیتی و بیان راهبردها، اقدامات و عایدی‌های بازیکنان شرح داده می‌شود.

بررسی عوامل مدل‌سازی تهدید مراکز حمل و نقل

روزانه در مراکز حمل و نقل عمومی هزاران مسافر تردد می‌کنند. بنابراین این مراکز از اهداف تهاجمی تروریست‌ها برای سلب امنیت ملی هر کشور به شمار می‌آیند. در این مراکز تهدیدات

احتمالی متعددی وجود دارد. هدف، ارایه یک مدل در جهت محدود ساختن تهدیدات امنیتی است. برای این مهم نیاز است تا فعالیت‌ها و اهداف مهاجمان بررسی گردد. بررسی رفتار مهاجمان نشان می‌دهد که آن‌ها دو هدف کلی را دنبال می‌کنند: الف) جلوگیری از فعالیت‌های امنیتی در مکان مورد نظر ب) اعمال بیشینه خسارت با کمترین هزینه. برای این منظور، مهاجمان برنامه خود را در آن مکان طراحی خواهند کرد. به عنوان نمونه یک مرکز حمل و نقل عمومی با سه اقدام امنیتی مانند بازرسی مسافر، تفتیش کیف‌ها و گشت‌زنی در محیط را در نظر بگیرید. فرض کنید به علت ازدحام، زمان‌بر بودن و محدود بودن منابع امنیتی امکان اجرای هر سه فعالیت به صورت همزمان و در همه نقاط مرکز امکان پذیر نباشد. اگرچه بازرسی مسافر ممکن است بالاترین موفقیت را برای نیروهای امنیتی داشته باشد ولی در صورتی که تفتیش کیف‌ها و گشت‌زنی انجام نگیرد، مهاجمان از این خلأ استفاده می‌کنند، مانند استفاده از یک چمدان دارای بمب یا حمله از خلأ محیطی. لذا مدافع باید به صورت پیشگیرانه راهبردی اتخاذ کند که مهاجمان نتوانند از این روزنه‌های امنیتی بهره‌برداری کنند. برای این منظور، باید لیستی از تهدیدات در هر مکان تهیه شده و ترکیبات مختلف اقدامات امنیتی خاص پیش‌بینی شود. همچنین، در مدل مذکور اقدامات امنیتی طوری پیاده‌سازی شود که برای جلوگیری از هدف اعمال بیشینه خسارت با کمترین هزینه توسط مهاجم، هزینه‌ای به مهاجم اعمال شود. از آنجا که اکنون مهاجمان قادر به مشاهده راهبرد مدافع هستند، تصادفی‌سازی عامل کلیدی در موفقیت مدافع خواهد بود. زیرا انتخاب هر راهبرد مشخص مدافع توسط مهاجم قابل مشاهده خواهد بود و مهاجم به راحتی می‌تواند با بررسی خلأهای امنیتی به هدف خود برسد. ولی در صورتی که تصادفی‌سازی در انتخاب راهبردها صورت گیرد، تشخیص طرح دقیق مدافع برای مهاجمان بسیار سخت و اغلب ناممکن خواهد بود.

بررسی عوامل مدل‌سازی تخصیص منابع امنیتی مرکز حمل و نقل عمومی

در حوزه مرکز حمل و نقل عمومی سه چالش کلی برای مدافع می‌توان مدنظر قرار داد: الف) مدافع باید به بررسی اقدامات امنیتی ناهمگن برای اهداف احتمالی در ناحیه بپردازد، ب) با توجه به اقدامات متعدد امنیتی امکان دارد مدافع بیش از یک منبع را به یک منطقه اختصاص دهد؛ ج) مدافع باید در حال حاضر دشمنی را در نظر بگیرد که ممکن است حملات ناهمگن در منطقه انجام دهد. به عنوان مثال در مراکز حمل و نقل بخش‌های مختلفی مانند مکان‌های فروش بلیط، اتاق انتظار و مکان‌های حمل بار وجود دارد. مدافع ممکن است تعداد منابع امنیتی مختلفی را به هریک از این مکان‌ها اختصاص دهد. مدافع باید اقدامات امنیتی مختلفی

را اتخاذ کند. زیرا تهدیدات احتمالی متعددی در مراکز حمل و نقل عمومی مانند استفاده از سلاح‌های شیمیایی، تیراندازی و بمب‌گذاری وجود دارد. لذا سوال کلیدی آن است که مدافع چگونه باید منابع امنیتی را به اقدامات امنیتی خاص در نواحی مشخص و به عنوان پاسخی برای مهاجمان مختلف اختصاص دهد؟ برای پاسخ به این سوال، مدل بازی‌های امنیتی ارائه می‌شود. در مدل بازی امنیتی، مدافع باید از ترکیبی از راهبردها استفاده کند. در ادامه راهبردهای مدافع و مهاجم را شرح می‌دهیم.

بررسی راهبردهای مدافع

مدافع سعی دارد تا با استفاده از m منبع یکسان امنیتی از اهداف $T=\{1,2,\ldots,p\}$ محافظت کند که منابع به صورت پیوسته بین اهداف قابل توزیع است. راهبرد مدافع را می‌توان به صورت یک بردار پوشش $c=(c_1,\ldots,c_p)$ نشان داد که در آن به ازای $c_k, k=1,\ldots,p$ مقدار پوشش داده شده از هدف k است و احتمال موفقیت مدافع را در جلوگیری از هر حمله‌ای به هدف k نشان می‌دهد. در این مسأله فرض می‌شود که هزینه پوشش هر هدف با منابع در دسترس، یکسان است. تقسیم این منابع به صورت محض برای مدافع مناسب نخواهد بود، زیرا در این حالت ممکن است برخی اهداف پوشش داده نشده و مهاجمان از این نقطه ضعف برای حمله به این اهداف استفاده کنند. بنابراین مدافع راهبردهای آمیخته را در نظر می‌گیرد که در آن منابع به مجموعه بزرگتری از اهداف تخصیص می‌یابند. این در حالی است که مهاجمان قادرند این راهبردهای آمیخته را مشاهده کنند. فضای راهبرد مدافع به صورت زیر نمایش داده می‌شود:

$$C=\left\{c=(c_1,\ldots,c_p)\,|\,0\le c_k\le 1,\ \sum_{k=1}^{p}c_k\le m\right\}$$

بررسی راهبردهای مهاجم

راهبرد آمیخته برای مهاجم نوع i با بردار $a_i=(a_i^1,a_i^2,\ldots,a_i^p)$ نمایش داده می‌شود که در آن a_i^k احتمال حمله مهاجم نوع i به هدف k است. لذا فضای راهبرد مهاجم نوع i به صورت زیر نمایش داده می‌شود:

$$A_i=\left\{\ a_i=(a_i^1,a_i^2,\ldots,a_i^p)\,|\,a_i^k\ge 0,\ \sum_{k=1}^{p}a_i^k=1\right\}$$

مدل‌سازی دوسطحی فازی

در این بخش مدل بازی امنیتی را در محیط فازی شرح می‌دهیم. همان‌گونه که قبلاً بیان شد، عایدی‌های بازیکنان از هر خروجی بازی توسط کارشناسان خبره به دست می‌آید. البته می‌توان برای به دست آوردن این عایدی‌ها از روش‌های یادگیری ماشین نیز استفاده کرد. با توجه به اینکه فهم کارشناسان خبره از عایدی‌ها مبهم و نادقیق می‌باشد، استفاده از نظریه فازی برای مدل‌سازی مفاهیم مبهم در بازی ضروری است. در این مقاله برای نمایش ابهام در مقادیر عایدی بازیکنان از اعداد فازی استفاده می‌شود.

در صورتی که هدف k توسط مهاجم نوع i انتخاب شده باشد و از طرف مدافع پوشش داده شده باشد، مطلوبیت مدافع با $\tilde{U}_i^{c,d}(k)$ نمایش داده می‌شود. اگر k پوشش داده نشده باشد جریمه مدافع با $\tilde{U}_i^{u,d}(k)$ نمایش داده می‌شود. مطلوبیت مهاجم به طور مشابه با $\tilde{U}_i^{c,a}(k)$ و $\tilde{U}_i^{u,a}(k)$ نمایش داده می‌شود. در حقیقت در این مدل بازی برای هر هدف k، چهار عایدی وجود دارد که دو عایدی برای مدافع در دو حالت پوشش و عدم پوشش هدف، و دو عایدی برای مهاجم نوع i در این دو حالت وجود دارد.

با انتخاب راهبردهای c و a_i به ترتیب توسط مدافع و مهاجم نوع i، مطلوبیت‌های مورد انتظار برای دو بازیکن به ترتیب به صورت زیر تعریف می‌شود:

$$\tilde{U}_i^{d}(c,a_i)=\sum_{k=1}^{p} a_i^k \tilde{U}_i^{d}(c_k,k),$$

$$.\tilde{U}_i^{a}(c,a_i)=\sum_{k=1}^{p} a_i^k \tilde{U}_i^{a}(c_k,k),$$

که در آن

$$\tilde{U}_i^{d}(c_k,k)=c_k\tilde{U}_i^{c,d}(k)+(1-c_k)\tilde{U}_i^{u,d}(k),$$

$$.\tilde{U}_i^{a}(c_k,k)=c_k\tilde{U}_i^{c,a}(k)+(1-c_k)\tilde{U}_i^{u,a}(k).$$

به ترتیب عایدی دریافت شده مدافع و مهاجم نوع i هستند (در صورتی که به هدف k حمله شده باشد و به مقدار c_k پوشش داده شده باشد).

همان‌گونه که بیان شد، در این بازی ابتدا مدافع راهبرد خود را انتخاب می‌کند. در این بحث، راهبرد مدافع اتخاذ تصمیم در خصوص نحوه حضور منابع امنیتی در اهداف مورد نظر است. با توجه به توضیحات فوق، مدافع با آگاهی از اینکه پس از گرفتن تصمیم، مهاجم قادر به مشاهده راهبرد وی خواهد بود به دنبال تخصیص بهینه منابع امنیتی برای حفاظت از اهداف

مورد نظر است. هم‌چنین، مدافع می‌داند که مهاجم پس از مشاهده راهبرد، به دنبال بهترین پاسخ در برخورد با این تصمیم خواهد بود. مدافع در برخورد با مهاجم نوع i، با آگاهی از بهترین پاسخ او، به دنبال بیشینه‌سازی مطلوبیت خود (حفاظت هر چه بیشتر از اهداف) می‌باشد. در حقیقت مسأله زیر را خواهیم داشت:

$$\max_{c\in C} \tilde{U}_i^d\left(c,a_i\right)$$
$$\sum_{k=1}^{p} c_k \le m$$
$$0\le c_k \le 1 \qquad k=1,\ldots,m$$

که در آن a_i جواب مساله زیر است:

$$\max_{a_i\in A_i} \tilde{U}_i^d\left(c,a_i\right)$$
$$\sum_{k=1}^{p} a_i^k = 1$$
$$a_i^k \ge 0 \qquad k=1,\ldots,m$$

مسأله فوق یک مسأله برنامه‌ریزی دوسطحی با پارامترهای فازی است که در آن پارامترهای فازی با اعداد فازی نمایش داده می‌شوند. سطح اول مسأله مربوط به تصمیم‌گیری مدافع و سطح دوم مسأله نمایش تصمیم مهاجم نوع i است.

با نوشتن α- برش‌های اعداد فازی، مسأله برنامه‌ریزی دوسطحی بازه‌ای (به ازای $0\le\alpha\le 1$) زیر به دست می‌آید:

$$\max_{c\in C} \left[U_{i\alpha}^{dL}\left(c,a_i\right),U_{i\alpha}^{dR}\left(c,a_i\right)\right]$$
$$\sum_{k=1}^{p} c_k \le m$$
$$0\le c_k \le 1 \qquad k=1,\ldots,m$$

که در آن a_i جواب مساله زیر است:

$$\max_{a_i\in A_i} \left[U_{i\alpha}^{aL}\left(c,a_i\right),U_{i\alpha}^{aR}\left(c,a_i\right)\right]$$
$$\sum_{k=1}^{p} a_i^k = 1$$
$$a_i^k \ge 0 \qquad k=1,\ldots,m$$

برای حل مسأله فوق از روش کان تاکر استفاده می‌کنیم (Bigdeli, 2018:1). برای استفاده از این روش در مسأله دوسطحی بازه‌ای فوق به صورت شرح داده شده در ادامه عمل می‌کنیم.

با معلوم بودن سیاست بهینه c مدافع، مسأله بهینه‌سازی مهاجم نوع i که یک پاسخ بهینه در مقابل تصمیم c خواهد داد، به صورت یک مسأله برنامه‌ریزی ریاضی با تابع هدف بازه مقدار به ازای هر $0 \le \alpha \le 1$ نوشته می‌شود.

$$\max\left[U_{i\alpha}^{aL}(c,a_i), U_{i\alpha}^{aR}(c,a_i)\right]$$

$$\sum_{k=1}^{p} a_i^k = 1$$

$$a_i^k \ge 0, \quad k = 1,\ldots,p$$

شرایط کان تاکر برای این مسأله به صورت زیر نوشته می‌شود.

(c,a_i) جواب کارای LR مسأله فوق است اگر و تنها اگر $\mu_0^i, \mu_k^i, \lambda_i^L, \lambda_i^R$ وجود داشته باشند به طوری که

$$\lambda_i^L \frac{\partial U_{i\alpha}^{aL}(c,a_i)}{\partial a_i^k} + \lambda_i^R \frac{\partial U_{i\alpha}^{aR}(c,a_i)}{\partial a_i^k} - \mu_0^i + \mu_k^i = 0, \ k = 1,\ldots,p,$$

$$\mu_k^i a_i^k = 0 \qquad k = 1,\ldots,p,$$

$$\mu_k^i \ge 0, \ \lambda_i^L, \lambda_i^R \ge 0, \qquad k = 1,\ldots,p$$

که در آن

$$\frac{\partial U_{i\alpha}^{aL}(c,a_i)}{\partial a_i^k} = c_k U_{i\alpha}^{c,aL}(k) + (1-c_k) U_{i\alpha}^{u,aL}(k),$$

$$\frac{\partial U_{i\alpha}^{aR}(c,a_i)}{\partial a_i^k} = c_k U_{i\alpha}^{c,aR}(k) + (1-c_k) U_{i\alpha}^{u,aR}(k).$$

با توجه به شرایط بهینگی فوق برای مسأله برنامه‌ریزی بازه مقدار، برای راهبرد c مدافع، پاسخ بهینه a_i مهاجم نوع i در شرایط بهینگی فوق صدق می‌کند.

مدافع با هدف بیشینه‌سازی مطلوبیت خود (در مقابله با مهاجم نوع i) و با توجه به پاسخ بهینه مهاجم نوع i به ازای $0 \le \alpha \le 1$، با مساله زیر مواجه می‌شود:

$$\max\left[U_{i\alpha}^{dL}(c,a_i), U_{i\alpha}^{dR}(c,a_i)\right]$$

$$\sum_{k=1}^{p} c_k \le m$$

$$0 \le c_k \le 1 \qquad k = 1,\ldots,m$$
$$\sum_{k=1}^{p} a_i^k = 1$$
$$\lambda_i^L \frac{\partial U_{i\alpha}^{aL}(c,a_i)}{\partial a_i^k} + \lambda_i^R \frac{\partial U_{i\alpha}^{aR}(c,a_i)}{\partial a_i^k} - \mu_0^i + \mu_k^i = 0,\ k = 1,...,p,$$
$$\mu_k^i a_i^k = 0 \qquad k = 1,...,p,$$
$$\mu_k^i \ge 0,\ \lambda_i^L, \lambda_i^R \ge 0 \qquad k = 1,...,p$$
$$a_i^k \ge 0,\quad k = 1,\ldots,p$$

با فرض دیدگاه بدبینانه مدافع به مسأله و محدودیت کران بازه، مسأله به صورت زیر نوشته می‌شود:

$$\max\ U_{i\alpha}^{dL}(c,a_i)$$
$$U_{i\alpha}^{dL}(c,a_i) \le U_{i\alpha}^{dR}(c,a_i)$$
$$\sum_{k=1}^{p} c_k \le m$$
$$0 \le c_k \le 1 \qquad k = 1,\ldots,m$$

$$\sum_{k=1}^{p} a_i^k = 1$$
$$\lambda_i^L \frac{\partial U_{i\alpha}^{aL}(c,a_i)}{\partial a_i^k} + \lambda_i^R \frac{\partial U_{i\alpha}^{aR}(c,a_i)}{\partial a_i^k} - \mu_0^i + \mu_k^i = 0,\ k = 1,...,p,$$
$$\mu_k^i a_i^k = 0 \qquad k = 1,...,p,$$
$$\mu_k^i \ge 0,\ \lambda_i^L, \lambda_i^R \ge 0 \qquad k = 1,...,p$$
$$a_i^k \ge 0,\quad k = 1,\ldots,p$$

تاکنون مدل مسأله را برای یک نوع مهاجم به دست آورده‌ایم. اکنون قصد داریم نشان دهیم که چگونه می‌توان مسأله را برای n نوع مهاجم مختلف گسترش داد. در بازی بیزی مهاجم مجاز است تا از انواع مختلفی از $i = 1,\ldots,n$ باشد که هر یک ماتریس عایدی جداگانه‌ای دارند. برای این کار یک مقدار احتمال برخورد با هر نوع مهاجم را مدنظر قرار

می‌دهیم. با در نظر گرفتن P_i به عنوان احتمال برخورد مدافع با مهاجم نوع i، مدل بازی امنیتی بین یک مدافع و چند نوع مهاجم به صورت زیر بیان می‌شود:

$$\max \sum_{i=1}^{n} P_i U_{i\alpha}^{dL}(c, a_i)$$

$$U_{i\alpha}^{dL}(c, a_i) \le U_{i\alpha}^{dR}(c, a_i),\ i = 1, \ldots, n$$

$$\sum_{k=1}^{p} c_k \le m$$

$$0 \le c_k \le 1 \qquad k = 1, \ldots, m$$

$$\sum_{k=1}^{p} a_i^k = 1$$

$$\lambda_i^L \frac{\partial U_{i\alpha}^{aL}(c, a_i)}{\partial a_i^k} + \lambda_i^R \frac{\partial U_{i\alpha}^{aR}(c, a_i)}{\partial a_i^k} - \mu_0^i + \mu_k^i = 0,\ k = 1, \ldots, p, i = 1, \ldots, n$$

$$\mu_k^i a_i^k = 0 \qquad k = 1, \ldots, p, i = 1, \ldots, p,$$

$$\mu_k^i \ge 0,\ \lambda_i^L, \lambda_i^R \ge 0 \qquad k = 1, \ldots, p, i = 1, \ldots, n$$

$$a_i^k \ge 0,\quad k = 1, \ldots, p,\ i = 1, \ldots, n.$$

در مسأله فوق تابع هدف مدافع به صورت بیشینه‌سازی مطلوبیت مورد انتظار در برابر هر نوع مهاجم احتمالی است. در حقیقت بازی بیزی در مسأله فوق تجزیه شده است. زیرا این مسأله می‌تواند به طور مستقل برای هر نوع مهاجم حل شود. با حل این مسأله برنامه‌ریزی ریاضی، راهبرد بهینه مدافع به دست می‌آید (اثبات این مطلب مشابه اثبات ارائه شده در (Tambe, 2012:143) برای بازی‌های امنیتی در محیط قطعی است).

برای حل این مسأله به ازای هر α می‌توان از روش‌های مختلفی استفاده کرد و هم‌چنین می‌توان نرم‌افزارهایی مانند گمز، لینگو و ... را برای حل این مسأله به کار برد (Bazaraa & Jarvis, 1997:1). مدافع با مشاهده راهبردهای به دست آمده به ازای هر α راهبرد متناظر خود را انتخاب می‌کند. ولی برای انتخاب یک راهبرد مشخص و رضایت‌بخش باید مسأله را به ازای یک α معین حل کرد.

برای این کار دو روش پیشنهاد می‌دهیم. در روش اول، ابتدا مسأله را به ازای $\alpha = 0$ و $\alpha = 1$ حل می‌کنیم. اگر مدافع از مقادیر متناظر (سود) به دست آمده رضایت داشته باشد

راهبرد متناظر به دست آمده راهبرد رضایت‌بخش مدافع خواهد بود. در غیر این صورت با معرفی یک مقدار هدف مطلوب (با توجه به مقادیر مطلوبیت به دست آمده فعلی) توسط مدافع که نشان‌دهنده سود مورد نظر از این رقابت برای او می‌باشد، می‌توان از کمینه‌سازی اختلاف تابع هدف با آرمانش به صورت زیر استفاده کرد. فرض کنید $\hat{U}$ مقدار مطلوب معرفی شده توسط مدافع باشد. در این صورت مسأله زیر را داریم.

$$\max \left| \sum_{i=1}^{n} P_i U_{i\alpha}^{dL}(c, a_i) - \hat{U} \right|$$

$$U_{i\alpha}^{dL}(c, a_i) \le U_{i\alpha}^{dR}(c, a_i),\ i = 1, \ldots, n$$

$$\sum_{k=1}^{p} c_k \le m$$

$$0 \le c_k \le 1 \qquad k = 1, \ldots, m$$

$$\sum_{k=1}^{p} a_i^k = 1$$

$$\lambda_i^L \frac{\partial U_{i\alpha}^{aL}(c, a_i)}{\partial a_i^k} + \lambda_i^R \frac{\partial U_{i\alpha}^{aR}(c, a_i)}{\partial a_i^k} - \mu_0^i + \mu_k^i = 0,\ k = 1, \ldots, p, i = 1, \ldots, n$$

$$\mu_k^i a_i^k = 0 \qquad k = 1, \ldots, p, i = 1, \ldots, p,$$

$$\mu_k^i \ge 0,\ \lambda_i^L, \lambda_i^R \ge 0 \qquad k = 1, \ldots, p, i = 1, \ldots, n$$

$$a_i^k \ge 0,\quad k = 1, \ldots, p,\ i = 1, \ldots, n.$$

در روش دوم، α را به صورت یک متغیر مجهول در مسأله در نظر گرفته و با حل مسأله غیرخطی زیر مقدار α مطلوب نیز به دست می‌آید.

$$\max \sum_{i=1}^{n} P_i U_{i\alpha}^{dL}(c, a_i)$$

$$U_{i\alpha}^{dL}(c, a_i) \le U_{i\alpha}^{dR}(c, a_i),\ i = 1, \ldots, n$$

$$\sum_{k=1}^{p} c_k \le m$$

$$0 \le c_k \le 1 \qquad k = 1, \ldots, m$$

$$\sum_{k=1}^{p} a_i^k = 1$$

$$\lambda_i^L \frac{\partial U_{i\alpha}^{aL}(c,a_i)}{\partial a_i^k} + \lambda_i^R \frac{\partial U_{i\alpha}^{aR}(c,a_i)}{\partial a_i^k} - \mu_0^i + \mu_k^i = 0,\ k=1,...,p, i=1,...,n$$
$$\mu_k^i a_i^k = 0 \qquad k=1,...,p,\ i=1,...,p,$$
$$\mu_k^i \geq 0,\ \lambda_i^L, \lambda_i^R \geq 0 \qquad k=1,...,p,\ i=1,\ldots,n$$
$$a_i^k \geq 0,\quad k=1,\ldots,p,\ i=1,\ldots,n.$$
$$0 \leq \alpha \leq 1$$

بررسی مدل و نقش آن در آینده‌پژوهی تهدیدات امنیتی

همان‌گونه که ملاحظه شد در این مقاله به مطالعه مدل بازی‌های امنیتی در تهدیدات امنیتی مراکز حمل ونقل عمومی پرداختیم. در این مدل، مطابق با آنچه در دنیای واقعی رخ می‌دهد، ابتدا مدافع راهبرد خود را انتخاب می‌کند. یکی از بخش‌های مهم انتخاب این راهبرد شامل تعداد منابع امنیتی قرار داده شده در اهداف مورد نظر است. بدیهی است وجود منابع امنیتی در ناحیه مورد نظر سطح امنیت آن ناحیه را بالا می‌برد. معمولاً مهاجمان برای حمله، نواحی با منابع امنیتی پایین را انتخاب می‌کنند. در اینجا لازم است ذکر شود که ممکن است مدافع با انواع مهاجمان روبرو شود و لذا باید تصمیم اولیه خود را با در نظر گرفتن انواع مختلف مهاجمان مختلف اتخاذ کند. بنابراین در وهله اول مدافع باید لیست کاملی از تهدیدات ممکن را تهیه کند و مهاجمان مختلف را شناسایی کرده و طرح مقابله با هریک را مورد بررسی قرار دهد. هر مهاجم اهداف خاصی از حمله به این مراکز دارد. به عنوان مثال در مراکز عمومی مانند مترو، مدافع ممکن است با سه نوع مهاجم مواجه شود: مسافران بی‌بلیط، مجرمان و تروریست‌ها. در فرودگاه‌ها، مدافع ممکن است با مهاجمان مختلفی مانند تروریست‌ها، قاچاقچیان مواد مخدر، قاچاق اموال ملی و فرهنگی و غیره روبرو شود. هر یک از این مهاجمان اهداف مختلفی را دنبال می‌کنند و طرح مقابله مدافع نیز باید متناسب با نوع مهاجم متغیر باشد. در این مقاله این مسائل به صورت یک بازی امنیتی بین یک مدافع و چند نوع مهاجم مورد بررسی قرار گرفت. دو نوع عدم قطعیت در این مدل وجود دارد: الف) مدافع نمی‌داند با چه نوع مهاجمی روبرو خواهد شد. ب) عایدی بازیکنان به صورت نادقیق می‌باشد. برای رفع مشکل عدم قطعیت نوع اول از مقادیر احتمال اختصاص داده شده به هر نوع مهاجم استفاده شد و برای حل مشکل عدم قطعیت نوع دوم اعداد فازی به کار گرفته شد. سپس با توجه به اینکه در این مسأله مدافع ابتدا راهبرد خود را انتخاب می‌کند و هر نوع از مهاجمان پس از مشاهده راهبرد مدافع تصمیم خود را برای حمله اتخاذ می‌کنند، مسأله به صورت یک مساله

برنامه‌ریزی دوسطحی فازی مدل‌سازی شد. با حل این مسأله به دنبال پیدا کردن راهبرد بهینه مدافع هستیم. در حقیقت پرداختن به این مسایل بخش مهمی از آینده‌پژوهی دفاعی است، چرا که مدافع باید راهبردی را انتخاب کند که مهاجمان پس از مشاهده این راهبرد نتوانند بیشترین خسارت را وارد کنند. هر مرحله از مدل که شامل تهیه لیستی از تهدیدات و بررسی انواع مهاجمان، بررسی اقدامات آینده آن‌ها و در نهایت اتخاذ راهبرد بهینه است مراحل آینده‌پژوهی تهدیدات امنیتی به کمک بازی امنیتی صورت می‌گیرد.

یک نمونه کاربردی (امنیت مترو)

در این بخش یک مثال کاربردی از بازی‌های امنیتی فازی ارائه شده و برای حل آن از روش پیشنهاد شده در این مقاله استفاده شده است. این مثال برگرفته از مثال ارائه شده در پژوهش بیگدلی و حسن‌پور (۲۰۱۸) می‌باشد، با این تفاوت که در اینجا از اعداد فازی برای نمایش عایدی بازیکنان استفاده می‌شود (Bigdeli & Hassanpour, 2018:36).

مترو یکی از سامانه‌های مسافربری داخل شهری است و به لحاظ سرعت و راحتی روزانه مسافران زیادی از این وسیله برای رفت و آمد استفاده می‌کنند. خطوط مترو شامل چندین ایستگاه است و روزانه هزاران مسافر را جا به جا می‌کند. می‌توان در مترو حداقل سه نوع مهاجم با اهداف مشخص شناسایی کرد: مسافران بی‌بلیط، مجرمان و تروریست‌ها. تعداد قابل ملاحظه‌ای از اقدامات امنیتی ممکن است در مترو وجود داشته باشد (مانند استفاده از دوربین‌ها، گشت‌ها و بازرسی‌های تصادفی). بنابراین بهتر است به نحوه تخصیص نیروهای امنیتی محدود برای حفاظت از ایستگاه‌های مترو بپردازیم تا بیشترین امنیت در مترو برقرار شود. سه نوع مهاجم مختلف در این مسأله ترجیحات متفاوتی دارند و ممکن است پاسخ‌های متفاوتی نیز داشته باشند. به عنوان مثال مسافران بی‌بلیط معمولاً ایستگاه‌های شلوغ را انتخاب می‌کنند درحالی که معمولاً مجرمان ایستگاه‌های خلوت را برای رسیدن به هدفشان برمی‌گزینند. تروریست‌ها ممکن است برای رسیدن به اهداف سیاسی خود به ایستگاه‌هایی ضربه بزنند که از لحاظ اقتصادی و فرهنگی اهمیت داشته باشند. همچنین مسئولین امنیتی (مدافع) ممکن است راهبردهای متفاوتی برای جلوگیری از هر نوع تهاجم داشته باشند. ورود مسافران بی‌بلیط هزینه‌ای را برای مترو به دنبال دارد. مدافع با استقرار سیاست‌های امنیتی در برابر مسافران بی‌بلیط از هزینه‌ی از دست رفته جلوگیری خواهد کرد. میزان صدمه به اموال و جرایم خشونت‌آمیز توسط مجرمان نیز هزینه‌ی بالایی برای مترو خواهد داشت و باعث ایمنی پایین و درنتیجه کاهش مسافران خواهد شد. تجاوز، سرقت، قتل و ... از جمله‌ی این جرایم

است. تهدیدات تروریست‌ها ما را بر آن می‌دارد تا سیاست امنیتی خاصی برای مقابله در این خصوص اتخاذ کنیم چرا که در بیشتر حملات تروریستی در کشورهای مختلف، تروریست‌ها مترو را یکی از اهداف خود قرار داده‌اند. علیرغم احتمال نسبتاً کم حمله‌ی تروریستی، اقدامات امنیتی طراحی شده در این زمینه با توجه به تعداد قابل توجه افراد در معرض خطر همواره باید یک اولویت باشد. مسئولین امنیتی نیاز است تا تمام تهدیدات اعمال شده توسط انواع مهاجمان را به منظور ارائه راهبرد امنیتی موثر در نظر بگیرند. بنابراین دفاع در مقابل هر نوع مهاجم می‌تواند به عنوان یک هدف برای مدافع در نظر گرفته شود، در حالی که این اهداف کاملاً متضاد نیستند. به عنوان مثال اقدام در مقابل مسافران بی بلیط ممکن است از وقوع جرم نیز بکاهد. البته با تمرکز زیاد بر روی یک نوع مهاجم ممکن است مهاجمان دیگر نادیده گرفته شود. بنابراین نیاز است تا مسئولین امنیتی منابع محدود خود را در این ایستگاه‌ها طوری تخصیص دهند که سطح امنیت مترو بالاتر رود.

اکنون فرض کنید بازی امنیتی مذکور بین مسئولین امنیتی (مدافع) و سه نوع مهاجم (مسافران بی بلیط، مجرمان و تروریست‌ها) ($n=3$) با در نظر گرفتن دو ایستگاه مترو ($k=1,2$) و یک منبع امنیتی ($m=1$) به صورت جداول ۱، ۲ و ۳ زیر نمایش داده شود.

جدول۱. جدول عایدی بین مدافع و مهاجم نوع۱

	ایستگاه ۱		ایستگاه ۲	
	پوشش داده شده	پوشش داده نشده	پوشش داده شده	پوشش داده نشده
مدافع	$(3,5,6)$	$(-3,-2,-1)$	$(9,10,11)$	$(2,3,5)$
مهاجم نوع۱	$(-2,-1,0)$	$(2,4,5)$	$(-2,-1,0)$	$(9,10,11)$

جدول۲. جدول عایدی بین مدافع و مهاجم نوع۲

	ایستگاه ۱		ایستگاه ۲	
	پوشش داده شده	پوشش داده نشده	پوشش داده شده	پوشش داده نشده
مدافع	$(0,1,2)$	$(0,0,0)$	$(1,2,4)$	$(-3,-2,-1)$
مهاجم نوع۲	$(-2,-1,0)$	$(0,1,2)$	$(0,0,0)$	$(3,5,6)$

جدول۳. جدول عایدی بین مدافع و مهاجم نوع۳

	ایستگاه ۱		ایستگاه ۲	
	پوشش داده شده	پوشش داده نشده	پوشش داده شده	پوشش داده نشده
مدافع	$(1,2,4)$	$(-2,-1,0)$	$(2,3,5)$	$(-3,-2,-1)$
مهاجم نوع۳	$(-3,-2,-1)$	$(0,1,2)$	$(-5,-3,-2)$	$(2,4,5)$

هر جدول نمایش‌دهنده بازی امنیتی بین مدافع و نوع مهاجم مورد نظر است. سطرهای جداول نمایش‌دهنده بازیکنان (مدافع و مهاج نوع i) و ستون‌ها نمایش‌دهنده اهداف مورد نظر است. عایدی‌های بازیکنان در دو حالت پوشش دادن هدف و عدم پوشش هدف ارائه شده است. c_1 نشان‌دهنده میزان پوشش مدافع از ایستگاه ۱ است و احتمال موفقیت مدافع را در جلوگیری از هر حمله‌ای به این ایستگاه نشان می‌دهد و c_2 نشان‌دهنده میزان پوشش مدافع از ایستگاه ۲ است و احتمال موفقیت مدافع را در جلوگیری از هر حمله‌ای به این ایستگاه نشان می‌دهد. همان‌گونه که قبلاً بیان شد برای قرار دادن عایدی‌های بازی از نظرات خبرگان استفاده می‌شود. برای این کار، پرسشنامه مناسبی تهیه و در اختیار کارشناسان متخصص حوزه مربوطه قرار می‌گیرد. با استفاده از پاسخ‌های به دست آمده می‌توان مقادیر عایدی را مشخص کرد. هم‌چنین می‌توان از یادگیری ماشین در این زمینه استفاده کرد. در مثالی که در ادامه توضیح داده می‌شود عایدی‌های ماتریس‌ها به صورت ساختگی و البته منطقی وارد شده است. به دلیل فهم مبهم کارشناسان از عایدی‌ها، این مقادیر به صورت اعداد فازی مثلثی نمایش داده شده‌اند. برای استفاده از مدل برنامه‌ریزی پیشنهاد شده در تحقیق، با استفاده از α- برش‌های اعداد فازی مثلثی، عایدی‌ها به صورت بازه‌ای نوشته می‌شوند.

مدافع با بررسی‌های لازم و تشکیل جلسات با خبرگان و کارشناسان متخصص حوزه به دنبال یک برنامه راهبردی جهت ایجاد حداکثر امنیت موجود در ایستگاه‌های مترو است. او می‌خواهد با استفاده از منابع امنیتی محدودی که در اختیار دارد به بیشترین امنیت لازم برسد و می‌داند که پس از انتخاب راهبرد، مهاجم آن را مشاهده کرده و بهترین راهبرد را در مقابل آن انتخاب خواهد کرد. بنابراین با مدل‌سازی مسأله به صورت یک بازی امنیتی و با در نظر گرفتن موارد مذکور و طبق توضیحاتی که در متن مقاله ارائه شده است، مدافع به دنبال حل مسأله برنامه‌ریزی ریاضی زیر برای محاسبه راهبرد بهینه است:

$$max\ 1/3\{(\alpha+6)a_1^1c_1+(\alpha-3)a_1^1+7a_1^2c_2+(\alpha+2)a_1^2+\alpha a_2^1c_1+4a_2^2c_2+(\alpha-3)a_2^2 \\ +3a_3^1c_1+(\alpha-2)a_3^1+5a_3^2c_2+(\alpha-3)a_3^2\}$$

s.t

$$(\alpha+6)a_1^1c_1+(\alpha-3)a_1^1+7a_1^2c_2+(\alpha+2)a_1^2 \\ \le 7a_1^1c_1-(\alpha+1)a_1^1+(\alpha+7)a_1^2c_2+(5-2\alpha)a_1^2$$

$$\alpha a_2^1c_1+4a_2^2c_2+(\alpha-3)a_2^2 \le (2-\alpha)a_2^1c_1+(-\alpha+5)a_2^2c_2-(\alpha+1)a_2^2$$

$$(\alpha+3)a_3^1c_1+\alpha a_3^1+5a_3^2c_2+(\alpha-3)a_3^2 \le \\ (-\alpha+4)a_3^1c_1-\alpha a_3^1+(-\alpha+6)a_3^2c_2-(\alpha+1)a_3^2$$

$$\lambda_1^L\left(c_1(\alpha-2)+(1-c_1)(2\alpha+2)\right)+\lambda_1^R\left(c_1\alpha+(1-c_1)(-\alpha+5)\right)-\mu_1^0+\mu_1^1=0$$

$$\lambda_1^L\left(c_2(\alpha-2)+(1-c_2)(\alpha+9)\right)+\lambda_1^R\left(-c_2\alpha+(1-c_2)(-\alpha+11)\right)-\mu_1^0+\mu_1^2=0$$

$$\lambda_2^L\left(c_1(\alpha-2)+(1-c_1)\alpha\right)+\lambda_2^R\left(c_1\alpha+(1-c_1)(-\alpha+2)\right)-\mu_2^0+\mu_2^1=0$$

$$\lambda_2^L\left(c_2(0)+(1-c_2)(2\alpha+3)\right)+\lambda_2^R\left((1-c_2)(-\alpha+6)\right)-\mu_2^0+\mu_2^2=0$$

$$\lambda_3^L\left(c_1(\alpha-3)+(1-c_1)\alpha\right)+\lambda_3^R\left(c_1(-\alpha-1)+(1-c_1)(-\alpha+2)\right)-\mu_3^0+\mu_3^1=0$$

$$\lambda_3^L\left(c_2(2\alpha-5)+(1-c_2)(2\alpha+2)\right)+\lambda_3^R\left(c_2(-\alpha-2)+(1-c_2)(-\alpha+5)\right) \\ -\mu_3^0+\mu_3^2=0$$

$$\mu_1^1a_1^1=0$$

$$\mu_1^2a_1^2=0$$

$$\mu_2^1a_2^1=0$$

$$\mu_2^2a_2^2=0$$

$$\mu_3^1a_3^1=0$$

$$\mu_3^2a_3^2=0$$

$$0\le c_1\le 1$$

$$0\le c_2\le 1$$

$$c_1+c_2\le 1$$

$$a_1^1+a_1^2=1$$

$$a_2^1+a_2^2=1$$

$$a_3^1 + a_3^2 = 1$$
$$0 \le \alpha \le 1$$
$$a_1^1, a_1^2, a_2^1, a_2^2, a_3^1, a_3^2 \ge 0$$
$$\lambda_i^L, \lambda_i^R, \mu_1^i, \mu_2^i, \mu_3^i \ge 0,\ i = 1,2,3$$

با حل این مسأله به کمک نرم‌افزار لینگو $V\ 17.0.60$ راهبرد مدافع به صورت زیر به دست می‌آید:

$$c_1 = 0.14, c_2 = 0.86$$

که این به معنی حضور حدودا ۸۶ درصدی منابع امنیتی در ایستگاه ۲ است.

این نمونه در پژوهش بیگدلی (۲۰۱۸) به کمک تقریب نزدیکترین بازه اعداد فازی مورد بررسی قرار گرفت و راهبرد بهینه مدافع تمرکز ۷۱ درصدی منابع در ایستگاه ۲ را نشان می‌داد (Bigdeli, 2018:1).

نتیجه‌گیری و پیشنهادها

در این مقاله بازی امنیتی به عنوان یکی از فنون آینده‌پژوهی تهدیدات امنیتی در محیط عدم قطعیت مورد مطالعه قرار گرفت. مراکز حمل و نقل عمومی به عنوان یکی از اهداف مورد تهدید از سوی مهاجمان مختلف مورد بررسی قرار گرفت. نیروهای امنیتی برنامه‌های خاصی برای امنیت این مراکز در نظر می‌گیرند که پس از اجرا قابل مشاهده است. مهاجمان با مشاهده برنامه‌های امنیتی مدافع به دنبال شکاف‌های امنیتی هستند تا از این طریق به اهداف خود دست یابند. لذا مدافع در هنگام برنامه‌ریزی برای ایجاد امنیت باید این موارد را مدنظر قرار دهد. در این تحقیق تعارض میان یک مدافع و چند نوع مهاجم به صورت یک مدل بازی امنیتی فازی شرح داده شد. در این مدل دو نوع عدم قطعیت لحاظ شد که عدم قطعیت اول ناشی از ناشناخته بودن نوع مهاجم و اهداف و راهبردهای آن در حمله به اهداف و عدم قطعیت دوم ناشی از ابهام در اطلاعات حاصل از هر خروجی بازی است. برای رفع عدم قطعیت نوع اول از بازی بیزی و برای رفع عدم قطعیت نوع دوم از نظریه فازی استفاده شد. برای نمایش عایدی‌های فازی بازیکنان از اعداد فازی استفاده شد. سپس به کمک α-برش‌های اعداد فازی، این مدل به صورت قطعی نوشته شد. با در نظر گرفتن احتمال برخورد با انواع مهاجمان و با دیدگاه بدبینانه، مدل مسأله در برابر انواع مهاجمان به یک مسأله برنامه‌ریزی تک هدفی تبدیل شد که با حل این مسأله، راهبرد بهینه مدافع به دست می‌آید. از آنجا که در این مقاله از α-

برش‌های اعداد فازی در تبدیل مدل فازی به قطعی استفاده شد، این رویکرد ماهیت فازی مسأله را حفظ می‌کند. از ویژگی‌ها و قابلیت‌های مدل پیشنهاد شده می‌توان به موارد زیر اشاره کرد:

۱) بررسی راهبردهای دو طرف و خروجی حاصل از هر راهبرد

۲) در نظر گرفتن دو نوع عدم قطعیت در مدل: نوع مهاجم ناشناخته و ابهام در اطلاعات

۳) رفع مشکل عدم قطعیت مهاجم ناشناخته با استفاده از بازی بیزی

۴) رفع مشکل ابهام در اطلاعات با استفاده از نظریه فازی

۵) تصادفی‌سازی راهبردها

۶) تحلیل ریاضی مدل

۷) ارایه نقطه تعادل استاکلبرگ قوی بازی (که همواره موجود است): با استفاده از این نقطه مدافع می‌تواند با آگاهی از اینکه پس از انتخاب راهبرد، مهاجم قادر به مشاهده آن خواهد بود و بهترین راهبرد خود را در مقابل آن انتخاب خواهد کرد، میزان حضور نیروهای امنیتی خود را در اهداف مختلف تعیین کند.

پیشنهاد می‌شود با استفاده از مدل به دست آمده در این مقاله و توسعه مطالب و مدل مذکور، سامانه پشتیبان تصمیم امنیتی با هدف آینده‌پژوهی تهدیدات آینده امنیتی تهیه گردد. علاوه بر این، پیاده‌سازی مدل‌های مشابه و استفاده از آن‌ها در سامانه پشتیبان تصمیم بازی جنگ در آموزش نحوه تصمیم‌گیری و تصمیم‌سازی فرماندهان اهمیت بسزایی دارد.

منابع

- An, B. Tambe, M. Ordonez, F. & Shieh, E. (2011). *Refinement of Strong Stackelberg Equilibria in Security Games*, Association for the Advancement of Artificial Intelligence.
- Bazaraa M.S. & Jarvis J.J. (1997). *Linear Programming and Network Flows*, John Wiley & Sons, Inc: NewYork .
- Bigdeli, H. & Hassanpour, H. (2018). Modeling and solving multiobjective security game problem using multiobjective bilevel problem and its application in metro security system.
- Bigdeli, H. Hassanpour H. & Tayyebi, J. (2016). The optimistic and pessimistic solutions of single and multiobjective matrix games with fuzzy payoffs and analysis of some of military problems, *Defence Sci & Tech*, Acceptd, *(In Persian).*
- Bigdeli, H. Hassanpour, H. & Tayyebi, J. (2018). Constrained Bimatrix Games with Fuzzy Goals and its Application in Nuclear Negotiations.

- Bigdeli, H. Hassanpour, H., & Tayyebi, J. (2018). Multiobjective security game with fuzzy payoffs, *IJFS*.
- Bigdeli, H., Hassanpour, H. (2016). A satisfactory strategy of multiobjective two person matrix games with fuzzy payoffs, *Iranian Journal of Fuzzy Systems*, 13: 17-33.
- Brown, G., Carlyle, M., Kline, J. & Wood, K. (2005). A Two-Sided Optimization for Theater Ballistic Missile Defense, *In Operations Research*, 53: 263–275.
- Brown, M. An, B. Kiekintveld, C. Ordóñez, F. & Tambe, M. (2014). An extended study on multi-objective security games, *Auton Agent Multi-Agent Syst*, 28: 31–71.
- Gatti, N. (2008). Game Theoretical Insights in Strategic Patrolling: Model and Algorithm in Normal-Form, *in ECAI-08*, pp. 403–407.
- Haywood, O. G. (1989). Military Decision and Game Theory, Wiley, *Journal of the Operations Research Society of America*, 2 (4): 365-385.
- Kheirkhah, A. S. Navidi, H. R. Bidgoli, M. M. (2017). Modeling and Solving the Hazmat Routing Problem under Network Interdiction with Information Asymmetry, Journal of transportation engineering, 9 (1): 17-36.
- Lye, K. & Wing, J. M. (2005). Game Strategies in Network Security, *International Journal of Information Security*, 4 (1–2): 71–86.
- Neumann, J. V. & Morgenstern, O. (1944). *Theory of Games and Economic Behavior*, Wiley, New York.
- Owen, G. (1995). *Game Theory*, Academic Press, San Diego, Third Edition.
- Sakawa, M. & Nishizaki, I. (2009). *Cooperative and Noncooperative Multi-Level Programming*, Springer, New York and london.
- Sakawa, M. (1993). *Fuzzy sets and interactive multiobjective optimization*, Plenum press, New York and london.
- Sandler, T. & D. G. A. M. (2003). *Terrorism and Game Theory*, Simulation and Gaming, 34 (3): 319–337.
- Tambe, M. (2012). *Security and game theory*, algorithms, deployed systems, lessons learned, Cambridge university press.