آینده‌پژوهی دفاعی، سال پنجم، شماره ۱۶، بهار ۱۳۹۹

تاریخ دریافت: ۱۳۹۸/۱۱/۲۰ تاریخ پذیرش: ۱۳۹۹/۰۲/۲۷

از صفحه ۸۹ تا صفحه ۱۰۸

# برنامه‌ریزی الفبایی برای حل بازی امنیتی با عایدی‌های فازی و محاسبه راهبرد فریب بهینه

سمانه اسماعیلی[۱]

حسن حسن‌پور[*۲]

حمید بیگدلی[۳]

**چکیده**

برقراری امنیت و ایجاد آرامش در بخش‌های مختلف جامعه از مهمترین مسائل امروز بشر است. به ویژه با توجه به گسترش ارتباطات، افزایش پروازهای بین‌المللی و توسعه حمل‌ونقل، نیاز به تأمین امنیت بیش از پیش احساس می‌شود. دست‌یافتن به این مهم، نیازمند پیش‌بینی و پیشگیری از آشوب یا حمله‌های احتمالی به مراکز مختلف، با استفاده از فنون علمی است. از طرفی در برقراری امنیت، محدودیت منابع امنیتی اعم از نیروی انسانی و امکانات نظامی باید مورد توجه قرار گیرد. چالش دیگری که نیروهای امنیتی با آن روبه‌رو هستند، این است که مهاجمان قبل از انجام هر حمله‌ای، الگوی چینش نیروهای امنیتی را مشاهده می‌کنند. لذا نیروهای مدافع باید در اتخاذ تصمیم خود اولویت‌های مهاجم را نیز مدنظر قراردهند. نظریه بازی رویکردی ریاضی برای به‌کارگیری منابع محدود امنیتی برای به حداکثر رساندن کارآیی آن‌ها فراهم می‌کند. در این مقاله با استفاده از تحلیل نظریه بازی، یک مدل ریاضی برای تخصیص بهینه‌ی نیرو ارائه شده است. طبیعی است که هر بازیکن از میزان اهمیت اهداف برای دیگری، اطلاع دقیق نداشته باشد. در این مدل به منظور بیان عدم قطعیت بازیکنان از میزان اهمیت اهداف، عایدی آن‌ها اعداد فازی مثلثی درنظر گرفته شده است سپس با استفاده از ترتیبی روی اعداد فازی مثلثی، از برنامه‌ریزی الفبایی برای حل مسئله استفاده شده است. در بخش نهایی مقاله به حل مسئله‌ی بازی امنیتی با منابع فریبنده در محیط فازی پرداخته شده که در آن مدافع می‌تواند با درنظر گرفتن میزان بودجه موجود، به منظور کاهش بهره‌وری مهاجم، از منابع غیرواقعی نیز استفاده کند.

**واژه‌های کلیدی:**

***بازی استاکلبرگ، بازی امنیتی، تخصیص بهینه نیرو، منابع فریبنده، نظریه فازی.***

---

[۱]. دانشجوی دکتری، دانشگاه بیرجند

[۲]. استادیار، دانشگاه بیرجند

[۳]. استادیار، پژوهشکده عالی جنگ دانشگاه فرماندهی و ستاد آجا

[*] نویسنده مسئول: Email: hhassanpour@birjand.ac.ir

**مقدمه**

امنیت، یک نگرانی اساسی در سراسر جهان است که در زمینه‌های متنوع از قبیل محافظت از بنادر، فرودگاه‌ها، شبکه‌های حمل و نقل و سایر زیرساخت‌های مهم ملی، محدود کردن جریان غیرقانونی مواد مخدر، سلاح و پول، سرکوب جرم و جنایت شهری، و همچنین در حفاظت از حیات‌وحش دریایی و جنگلی مطرح می‌شود. برقراری امنیت و ایجاد آرامش از مهمترین دغدغه‌های گردانندگان کشورهاست. افزایش انواع جرایم، حملات تروریستی، قاچاق و سایر تهدایدات امنیتی نیاز امروز کشورها به ایجاد امنیت برای برقراری آرامش را افزایش می‌دهد. کشورها باید برای تامین امنیت در مکان‌های عمومی، پروازها، حمل‌ونقل دریایی و ... از بالاترین استاندارد در این زمینه برخوردار باشند. تنها از سال ۱۹۸۰ بیش از پنج هزارکشته بر اثر حملات تروریستی به هواپیماها انجام شده است. حدود ۲۰۰ کشته در حملات به خود فرودگاه‌ها رخ داده است(Tambe, 2011 :27). نمونه‌ای دیگر، در حملات نوامبر ۲۰۰۸ در بمبئی هندوستان (یک رشته حملات همزمان مسلحانه در ۲۶ نوامبر ۲۰۰۸) موجب کشته شدن بیش از ۱۹۵ نفر شد. همچنین امروزه بیش ۹۰ درصد تجارت جهانی و حدود ۶۵ درصد کل نفت جهان از طریق دریا منتقل می‌شود. این میزان بالا، گویای اهمیت مسئله امنیت دریایی کشورهاست که به دلیل تهدیداتی مانند تروریسم و قاچاق‌کالا و مواد مخدر با خطرات جدی برای کشورها روبرو است. در زمینه امنیت دریایی در ایران، خلیج‌فارس به دلیل موقعیت استراتژیک و به خصوص تنگه هرمز نیازمند گشت‌زنی‌های نیروهای امنیتی در اشکال مختلف گشت‌زنی با قایق، پهپاد و ... است. بر اساس آنچه گفته شد تخصیص نیرو برای برقراری امنیت، به مسئله‌ی مهمی در دنیای امروز تبدیل شده است. با این وجود اغلب برای تحقق این هدف منابع امنیتی محدودی وجود دارد؛ از جمله تخصیص منابع کمیابی مانند بمب‌یاب‌ها، وسایل نقلیه و دوربین‌های امنیتی، یا پرسنل محدود نیروی پلیس برای انجام گشت و محدودیت در ایجاد ایستگاه‌های بازرسی. سوال کلیدی این است که چگونه تخصیص این منابع محدود امنیتی را برای محافظت در برابر طیف وسیعی از تهدیدات بالقوه بهینه کنیم. با توجه به محدودیت منابع، منابع امنیتی باید به صورت انتخابی مستقر شوند. از طرفی مهاجمان می‌توانند تا حدودی نیروهای دفاعی (امنیتی) را تحت نظر بگیرند و از الگوی استقرار نیروهای امنیتی بهره برداری کنند. مهاجمان می‌توانند با نظارت مداوم، اطلاعات را در مورد اقدامات امنیتی-دفاعی برای حملات موثرتر جمع‌آوری کنند. در این صورت تخصیص منابع قابل پیش‌بینی ممکن است توسط مهاجمان مورد بهره‌برداری قرار گرفته و از این رو باعث کاهش بهره‌وری منابع امنیتی شود. بنابراین

یافتن روش‌های بهینه‌سازی تخصیص نیرو در این زمینه نیازمند تحقیقات علمی است. منابع محدود امنیتی باید با درنظرگرفتن تفاوت در اولویت‌های اهداف نیازمند پوشش امنیتی، پاسخ مخالفان به وضعیت امنیتی و عدم اطمینان بالقوه نسبت به انواع قابلیت‌ها، و دانش و اولویت‌های مهاجمان هوشمند مستقر شوند. نظریه بازی‌ها می‌تواند با درنظرگرفتن اهمیت اهداف مختلف و پاسخ مهاجم به هر راهبرد خاص برای حمایت از زیرساخت‌ها و اهداف نیازمند محافظت، روشی برای تخصیص منابع امنیتی محدود برای حفاظت از اهداف فراهم کند. امروزه تخصیص منابع مسئله‌ی مهمی از مسائل امنیتی به عنوان شاخه‌ای از نظریه بازی‌هاست. بازی‌های امنیتی با توجه به نوع و تعداد مهاجمان و مدافعان در حل مسائل مختلف امنیتی کاربرد دارد. تخصیص بهینه نیروهای انتظامی در اماکن مختلف یک شهر یا مکان‌های نیازمند محافظت، سیستم دفاع موشکی، تصمیم‌گیری در نبردهای نظامی، گشت‌زنی نیروهای امنیتی، امنیت شبکه‌های کامپیوتری و ... از جمله این کاربردهاست.

موضوع دیگری که در یک بازی امنیتی می‌تواند مورد توجه قرار گیرد، این است که اقدامات فریبکارانه مدافع می‌تواند بر باور مهاجم در مورد راهبرد مدافع و بهترین پاسخ مهاجم تأثیر بگذارد. اخیرا روش‌های فریبنده نیز برای دفاع از سیستم‌های اطلاعاتی به کار می‌رود. منابع فریبنده در سیستم دفاعی، با گمراه کردن مهاجم احتمال شناسایی دقیقش را کاهش می‌دهد. کوهن[1] و کویک[2] (2004) بحث جامعی در زمینه فریب به منظور افزایش امنیت سیستم اطلاعاتی ارائه داده و نتیجه می‌گیرند که «فریب» عاملی مثبت برای مدافع و منفی برای مهاجم محسوب می‌شود. لذا مدافع می‌تواند از منابع فریبنده که هزینه‌ی کمتری نیز نسبت به منابع واقعی دارند، استفاده کند. به عنوان مثال پلیس به عنوان مدافع می‌تواند از دوربین‌های مخفی در جاده‌ها برای شناسایی اتومبیل‌هایی با سرعت غیرمجاز به عنوان محافظ مخفی و یا استفاده از دوربین‌های جعلی که هزینه بسیار کمتری دارند استفاده کند. همچنین در بسیاری از موارد اگر مهاجم نتواند تشخیص دهدکه منبع مورد استفاده مدافع واقعی است یا جعلی، ترجیح می‌دهد حمله نکند. لذا مدافعان می‌توانند برای افزایش اثربخشی سیستم دفاعی خود از منابع فریبنده نیز استفاده کنند.

در سال‌های اخیر اقداماتی کاربردی در زمینه حل مسائل بازی امنیتی صورت گرفته است. با توجه به نادقیق بودن اطلاعات بازیکنان، حل مسئله در محیط غیرقطعی نیازی ضروری به نظر می‌رسد. در این مقاله، یک مدل بازی امنیتی را معرفی می‌کنیم که در آن عایدی‌های بازیکنان

---

1. Cohen
2. Koike

به صورت غیرقطعی بیان شده‌اند و برای بیان عدم قطعیت، از اعداد فازی مثلثی استفاده شده است. در بخش انتهایی این پژوهش، مسئله‌ی بازی امنیتی با داده‌های فازی مورد بحث قرارگرفته که در آن مدافع می‌تواند از محافظت فریبنده نیز استفاده کند.

## مبانی نظری و پیشینه‌های پژوهش

### مفاهیم اولیه مجموعه‌های فازی

در این زیربخش، برخی از تعاریف مربوط به اعداد فازی مثلثی ارائه می‌شود.

**تعریف۱.** یک عدد فازی $\tilde{A}$ با تابع عضویت $\mu_{\tilde{A}}: \mathbb{R} \to [0,1]$ به صورت زیر، یک عدد فازی مثلثی نامیده شده و با $\tilde{A} = (a^1, a^2, a^3)$ نشان داده می‌شود.

$$\mu_{\tilde{A}}(x) = \begin{cases} x - a^1/a^2 - a^1 & a^1 \le x \le a^2 \\ a^3 - x/a^3 - a^2 & a^2 \le x \le a^3 \\ \text{در غیر این صورت} \quad 0 & \end{cases}$$

$a^2$ و $a^3$ به ترتیب ابتدا و انتهای تکیه‌گاه عدد فازی $\tilde{A}$ بوده و $a^2$ هسته (نقطه‌ای با درجه عضویت یک) آن است.

جمع دو عدد فازی مثلثی $\tilde{A} = (a^1, a^2, a^3)$ و $\tilde{B} = (b^1, b^2, b^3)$ و ضرب اسکالر در عدد فازی مثلثی با استفاده از اصل گسترش (Sakawa, 1993) به صورت زیر به دست می‌آیند:

$$\tilde{A} + \tilde{B} = (a^1 + b^1, a^2 + b^2, a^3 + b^3)$$

$$k\tilde{A} = \begin{cases} (ka^1, ka^2, ka^3) & k \ge 0 \\ (ka^3, ka^2, ka^1) & k \le 0. \end{cases}$$

برای مقایسه دوعدد فازی، از ترتیبی که توسط عزتی و همکاران پیشنهاد شده استفاده می‌کنیم.(Ezzati et al., 2013:1)

**تعریف۲.** فرض کنید $\tilde{A} = (a^1, a^2, a^3)$ و $\tilde{B} = (b^1, b^2, b^3)$ دو عدد فازی مثلثی دلخواه باشند. گوییم $\tilde{A}$ از $\tilde{B}$ کوچکتر است و می‌نویسیم $\tilde{A} \prec \tilde{B}$ هرگاه:

۱) $a^2 < b^2$ یا

۲) $a^2 = b^2$ و $(a^3 - a^1) > (b^3 - b^1)$ یا

۳) $a^2 = b^2$، $(a^3 - a^1) = (b^3 - b^1)$ و $(a^3 + a^1) < (b^3 + b^1)$.

**تبصره۱.** $\tilde{A} = \tilde{B}$ اگر و تنها اگر $a^2 = b^2$ و $a^3 - a^1 = b^3 - b^1$ و $a^3 + a^1 = b^3 + b^1$ (Ezzati et al., 2013:1).

**تبصره۲.** $\tilde{A} \preccurlyeq \tilde{B}$ اگر وتنها اگر $\tilde{A} \prec \tilde{B}$ یا $\tilde{A} = \tilde{B}$ (Ezzati et al., 2013:1).

به راحتی می‌توان نشان داد که ترتیب پیشنهاد شده، یک ترتیب کلی است.

**بازی‌های امنیتی**

در این پژوهش از یک قالب بازی استاکلبرگ برای مدل‌سازی تقابل بین نیروهای امنیتی و مهاجمین و محاسبه راهبردهای نیروهای امنیتی استفاده شده است. در چارچوب بازی استاکلبرگ یک بازیکن (بازیکنانی) به عنوان رهبر و بقیه به عنوان پیرو عمل می‌کنند. در این بازی فرض بر این است که رهبر همیشه متعهد است. به بیان دیگر رهبر بعد از اتخاذ انتخاب اولیه‌اش اجازه ندارد تصمیم خود را تغییر دهد و باید به حرکت خود پایبند باشد. بازی امنیتی مطابق با بازی استاکلبرگ است. مدافع (نیروی امنیتی) نقش رهبر و مهاجم نقش پیرو را ایفا می‌کنند. مدافع ابتدا با تعهد به یک راهبرد گشت‌زنی یا بازرسی عمل می‌کند و مهاجم پس از مشاهده انتخاب مدافع، تصمیم می‌گیرد که به کدام هدف حمله کند. در این بازی امنیتی که مورد مطالعه این نوشته است، مجموعه اهداف $T = \{1,2, \dots, n\}$ توسط مهاجم مورد تهدید است. مدافع سعی دارد با استفاده از $m$ منبع امنیتی یکسان از این اهداف محافظت کند. مدافع و مهاجم بازیکنان این بازی بوده و هر کدام برای به دست آوردن سود بیشتر راهبردهایی برای انتخاب دارند.

**تعریف۳.** فرض کنید $U_1(x,y)$ و $U_2(x,y)$ به ترتیب عایدی‌های بازیکنان رهبر و پیرو و $x$ و $y$ راهبردهای اتخاذ شده‌ی این بازیکنان باشند. جفت راهبرد $(x^*,y^*)$ را جواب تعادل بازی استاکلبرگ گوییم هرگاه جواب مسئله‌ی زیر باشد:

$$U_1(x^*,y^*) = \max_x U_1(x,R(x)).$$

که در آن $R(x)$ نشان دهنده‌ی بهترین پاسخ بازیکن پیرو به راهبرد $x$ بازیکن رهبر است.

به عبارتی برای به دست آوردن تعادل استاکلبرگ، ابتدا بیشینه مقادیر $U_2(x,y)$ به ازای راهبردهای مختلف رهبر به دست آمده و سپس مجموعه‌ی راهبردهای رهبر روی بهترین پاسخ‌های پیرو بهینه می‌شود.

راهبردهای محض مدافع را زیرمجموعه‌ای از اهداف تعریف می‌کنیم، به طوری که حداکثر $m$ هدف مورد محافظت قرار گیرند. راهبرد آمیخته مدافع برداری مانند $C = (c_1, c_2, \dots, c_n)$ است که در آن به ازای $t = 1,2, \dots, n$، $c_t$ میزان پوشش هدف $t$ام را نشان می‌دهد. با توجه به محدودیت منابع، بردار راهبرد مدافع به صورت زیر تعریف می‌شود:

$$\forall t \in T \quad 0 \le c_t \le 1 \ , \ \sum_{t \in T} c_t \le m.$$

راهبرد محض مهاجم انتخاب یک هدف برای حمله است. به عبارتی هر راهبرد مهاجم، برداری مانند $A = (a_1, a_2, \dots, a_n)$ است که

$$\forall t \in T \quad a_t \in \{0,1\}\,, \ \sum_{t\in T} a_t = 1.$$

فرض بر این است که مهاجم دقیقا به یک هدف حمله خواهد کرد. پس برای وی راهبرد آمیخته تعریف نمی‌گردد.

عایدی مدافع و مهاجم در دو حالت وجود پوشش حفاظتی و عدم وجود پوشش برای هر هدف $t$ داده شده است که به ترتیب با $U_d^c(t)$ و $U_d^u(t)$ برای مدافع و $U_a^c(t)$ و $U_a^u(t)$ برای مهاجم نمایش داده می‌شود. همچنین عایدی مدافع از هر پوشش $c_t$ به ازای هدف $t$ با $U_d(t,c_t)$ نمایش داده شده و به صورت زیر محاسبه می‌شود:

$$U_d(t,c_t) = \ c_t U_d^c(t) + (1-c_t)U_d^u(t).$$

بدیهی است چنانچه هدفی توسط یکی از منابع مدافع محافظت (پوشش داده) شود، عایدی مدافع افزایش و عایدی مهاجم کاهش یابد. عایدی مدافع و مهاجم به ازای یک جفت راهبرد $(C,A)$ به ترتیب به صورت زیر محاسبه می‌شود:

$$U_d(C,A) = \sum_{t\in T} a_t\, U_d(t,c) = \sum_{t\in T} a_t \left(c_t U_d^c(t) + (1-c_t)U_d^u(t)\right), \quad (1)$$

$$U_a(C,A) = \sum_{t\in T} a_t\, U_a(t,c) = \sum_{t\in T} a_t \left(c_t U_a^c(t) + (1-c_t)U_a^u(t)\right). \quad (2)$$

**پیشینه پژوهش**

اخیراً علاقه زیادی به پژوهش در مورد نظریه بازی برای امنیت در فرودگاه‌ها، بنادر، حمل‌ونقل و سایر زیرساخت‌ها وجود داشته است (Pita et al., 2008; Pita et al., 2009; Jain et al., 2010). در دهه‌ی اخیر نظریه بازی در بخش‌های مختلف نظامی، امنیت شبکه‌های کامپیوتری (Lye & Wing, 2005:1)، سیستم دفاع موشکی ضدبالستیک (Brown et al, 2005:1)، تروریسم (Sandler & A.M, 2003:1) و گشت‌زنی نیروهای محافظ حیات وحش و ... مورد استفاده قرار گرفته است. بیگدلی و حسن پور (۲۰۱۶) به بررسی بازی‌های چندهدفی در محیط قطعی پرداختند و از برنامه‌ریزی آرمانی برای 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 ).

بخش عمده‌ای از پژوهش‌های موجود روی بازی‌هایی با یک نوع مدافع متمرکز شده که در آن ابتدا مدافع منابع لازم را برای محافظت از مجموعه‌ای از اهداف اختصاص می‌دهد و سپس یک مهاجم پس از مشاهده تخصیص، با حمله به یک هدف سودآور، پاسخ بهینه می‌دهد. این

پژوهش‌ها از بازی استاکلبرگ برای مدل‌سازی تقابل بین نیروهای امنیتی و مهاجمین (تروریست‌ها، سارقان، شکارچیان، قاچاقچیان و غیره) و محاسبه راهبردهای نیروهای امنیتی استفاده کرده‌اند. بازی‌های امنیتی استاکلبرگ چهارچوبی را برای بهینه‌سازی تخصیص منابع دفاعی در برابر مهاجمان ارائه می‌دهند. بازی‌های استاکلبرگ این واقعیت را مدل می‌کنند که یک مهاجم هوشمند می‌تواند راهبرد مدافع را رصد و از آن بهره‌برداری کند. تحقیقات زیادی در مورد این موضوع وجود دارد که کاربردهای موفقی داشته است (Tambe, 2011:1 & An, 2017:1). در ادامه به چند نمونه از این کاربردها اشاره می‌کنیم.

مأموریت گارد ساحلی ایالات متحده شامل تامین امنیت دریایی سواحل، بنادر و آبراه‌های داخلی ایالات متحده است؛ یک حوزه امنیتی که به دلیل تهدیداتی مانند تروریسم و قاچاق مواد مخدر با خطراتی روبرو است. گارد ساحلی ایالات متحده با توجه به بندر خاص و تنوع زیرساخت‌های حیاتی که ممکن است یک دشمن در داخل بندر به آن حمله کند، گشتی را برای محافظت از این زیرساخت‌ها انجام می‌دهد. منابع امنیتی محدود بوده و گشت‌ها نمی‌توانند در همه‌ی مکان‌ها تمام مدت حضور یابند. در تخصیص منابع گشت‌زنی با قایق، مدل PROTECT[1] برای تقویت امنیت دریایی طراحی شده و از آوریل ۲۰۱۱ در بندر بوستون مورد استفاده قرار گرفته است(Tambe et al, 2013:2). این سیستم از چهارچوب بازی استاکلبرگ استفاده می‌کند. PROTECT در حال حاضر در بنادر بوستون، نیویورک، لس‌آنجلس، لانگ‌بیچ و چند بندر دیگر مستقر شده است (An et al., 2013). تامبه و همکاران (2008) ایجاد پاسگاه در مسیرهای منتهی به فرودگاه و گشت‌زنی با سگ در فرودگاه لس‌آنجلس را با استفاده از نظریه بازی‌ها بهینه‌سازی کردند. فرودگاه بین المللی لس‌آنجلس بزرگترین فرودگاه مقصد در ایالات متحده است و سالانه به ۶۰ تا ۷۰ میلیون مسافر خدمت‌رسانی می‌کند. پلیس فرودگاه از اقدامات متنوعی برای محافظت از فرودگاه شامل پاسگاه‌های وسایل نقلیه و واحدهای پلیس گشت‌زنی با سگ استفاده می‌کند. برای تخصیص بهینه این منابع امنیتی به منظور بهبود اثربخشی آن‌ها سیستم دستیار نظارت تصادفی در مسیرها (ARMOR[2]) برای دو مورد از اقدامات امنیتی در این فرودگاه (تخصیص مکان پاسگاه‌ها و گشت‌زنی با سگ) طراحی شد. این سیستم، تخصیص منابع امنیتی را با استفاده از بازی‌های استاکلبرگ بیزی بهینه می‌کند(Paruchuri, et al, 2008). همچنین سرویس فدرال مارشال هوایی ایالات متحده برای

[1]. Port Resilience Operational / Tactical Enforcement to Combat Terrorism
[2]. Assistant for Randomized Monitoring over Routes

جلوگیری از تجاوز احتمالی و جلوگیری از حمله، مارشال‌های هوایی[۱] را به پروازهای مبدأ و مقصد از ایالات متحده اختصاص می‌دهد. تعداد محدودی سرویس فدرال مارشال هوایی باید روزانه برای پوشش هزاران پرواز تجاری برنامه‌ریزی شود. در این زمینه جین[۲] و همکاران (2010) سیستم زمان‌بندی تصادفی هوشمند (IRIS[۳]) را برای برنامه‌های مارشال‌های هوایی در پروازهای بین‌المللی با استفاده از بازی‌های استاکلبرگ، طراحی کرده و از اکتبر ۲۰۰۹ توسط سرویس فدرال مارشال هوایی ایالات متحده مستقر شده است. در این سیستم، اهداف مجموعه‌ای از پروازها است و مهاجم به‌طور بالقوه می‌تواند حمله به یکی از این پروازها را انتخاب کند. در نمونه‌های دیگر، کیکینتولد[۴] و همکاران (۲۰۰۹) یک رده‌ی کلی از بازی‌های امنیتی را بر اساس تخصیص منابع دفاعی به اهداف یا زیرمجموعه‌ای از اهداف تعریف کردند. این مدل که بعدا توسط یین[۵] و همکارانش گسترش یافت (2010) اجازه می‌دهد مهاجم منابع متعدد داشته باشد، به این معنی که مهاجم به طور همزمان می‌تواند به اهداف مختلف حمله کند. کانیتزر[۶] و سندهولم[۷] (۲۰۰۶) روشی را برای انجام راهبردهای تصادفی بهینه در بازی‌های امنیتی ارائه کردند. ترجو[۸] و همکاران (2015) روشی برای محاسبه تعادل نش در حالت یک مدافع و چندین مهاجم به کار گرفتند. در زمینه‌های امنیتی محافظت از حیات‌وحش در پژوهش فنگ و همکاران (۲۰۱۶)، تعاملات تکراری بین محیط‌بانان و شکارچیان در مناطق حفاظت‌شده به محیط‌بانان اجازه می‌دهد که علایم شکار را در طول زمان جمع‌آوری کنند. با استفاده از این داده‌ها محیط‌بانان می‌توانند استراتژی گشت‌زنی را برنامه‌ریزی کنند (Fang et al., 2016:1).

برآورد ناقص مهاجم می‌تواند فرصت‌ها و احتمالاً تهدیداتی برای یک مدافع ایجاد کند. پژوهش‌های گذشته به طور معمول فرض می‌کنند که مهاجم از راهبرد اتخاذ شده‌ی مدافع آگاهی کاملی دارد و بر همین اساس واکنش نشان خواهد داد. با توجه به اینکه نظارت هزینه‌بر و پرخطر است، این فرض ساده انگارانه است. با توجه به نادقیق بودن اطلاعات بازیکنان در

---

۱. نیروهای امنیتی مخفی در هواپیما که هنگام بروز حوادث غیرقابل پیش‌بینی وارد عمل می‌شوند.

2. Jain
3. Intelligent Randomization In Scheduling
4. Kiekintveld
5. Yin
6. Conitzer
7. Sandholm
8. Trejo

دنیای واقعی، عدم قطعیت در مورد عایدی هر بازیکن از انتخاب یک راهبرد، امری طبیعی است. همچنین با وجود سناریوهای موجود برای فریب، این مسئله در محیط غیرقطعی بررسی نشده است. در این تحقیق نخست یک مسئله‌ی بازی امنیتی با عایدی‌های فازی مورد بررسی قرار گرفته و یک مدل ریاضی برای حل آن ارائه شده است. سپس یک نوع بازی امنیتی با منابع فریبنده معرفی گردیده و بر اساس مدل مذکور راهبرد فریب بهینه در این بازی‌ها به دست آمده است.

**ارائه مدل ریاضی برای حل مسئله بازی امنیتی با عایدی‌های فازی**

در مسئله‌ی بازی امنیتی مدافع راهبردی را اتخاذ کرده و سپس مهاجم با توجه به راهبرد مدافع بهترین پاسخ خود را ارائه می‌کند. مهاجم می‌کوشد عایدی خود را با انتخاب راهبردی که بهترین پاسخ به راهبرد مدافع است، به حداکثر برساند. لذا مدافع قبل از اینکه راهبرد خود را انتخاب کند، باید از اولویت‌های مهاجم آگاه باشد و در محدودیت‌های خود بیشینه عایدی مهاجم را درنظر بگیرد. این مسئله به صورت مسئله‌ی برنامه‌ریزی فازی دوسطحی آمیخته $(P_1)$ فرمول‌بندی می‌شود که در آن ابتدا در سطح پایین عایدی مهاجم به عنوان پیرو، بیشینه شده و سپس در سطح بالا عایدی مدافع به عنوان رهبر بازی، بیشینه می‌شود.

$$(P_1): \quad \max_{C} \quad \widetilde{U}_d\,(C, A)$$
$$s.t \quad \sum_{t\in T} c_t \le m,$$
$$0 \le\ c_t \le 1,$$

که در آن $A$ جواب بهینه مسئله‌ی زیر است:

$$\max_{A} \quad \widetilde{U}_a\,(C, A)$$
$$s.t \quad \sum_{t\in T} a_t = 1,$$
$$a_t \in \{0,1\}.$$

در این مسئله فرض می‌کنیم که پارامترها در توابع هدف هر دو سطح (عایدی‌های بازیکنان) اعداد فازی مثلثی هستند.

با توجه به روابط (۱) و (۲) حل مسئله‌ی $(P_1)$ معادل با حل مسئله‌ی زیر خواهد بود:

$$(P_2): \quad \max_{C} \sum_{t\in T} a_t(c_t\widetilde{U}_d^c(t) + (1-c_t)\widetilde{U}_d^u(t))$$
$$s.t \quad \sum_{t\in T} c_t \le m,$$
$$0 \le\ c_t \le 1$$

که در آن $A$ جواب بهینه مسئله زیر است:

$$max_A \sum_{t\in T} a_t \left(c_t \widetilde{U}_a^c(t) + (1-c_t)\widetilde{U}_a^u(t)\right)$$
$$s.t \sum_{t\in T} a_t = 1,$$
$$a_t \in \{0,1\}.$$

تعریف می‌کنیم

$\tilde{k} = \sum_{t\in T} a_t \left(c_t \widetilde{U}_a^c(t) + (1-c_t)\widetilde{U}_a^u(t)\right)$. و $\tilde{d} = \sum_{t\in T} a_t(c_t \widetilde{U}_a^c(t) + (1-c_t)\widetilde{U}_a^u(t))$

در قضیه زیر مسئله‌ای یک سطحی ارائه می‌شود که از حل آن جواب مسئله‌ی دوسطحی $(P_2)$ به دست می‌آید.

**قضیه۱.** حل مسئله‌ی زیر یک جواب مسئله‌ی $(P_2)$ را به دست می‌دهد.

$$(P_3): \quad max \quad \tilde{d}$$
$$s.t \sum_{t\in T} c_t \le m, \qquad (3)$$
$$0 \le c_t \le 1, \qquad (4)$$
$$\sum_{t\in T} a_t = 1, \qquad (5)$$
$$a_t \in \{0,1\}, \qquad (6)$$
$$\tilde{d} \le (1-a_t)\widetilde{M} + \widetilde{U}_d(t,c) \quad \forall t \in T, \qquad (7)$$
$$\tilde{k} \le (1-a_t)\widetilde{M} + \widetilde{U}_a(t,c) \quad \forall t \in T, \qquad (8)$$
$$\widetilde{U}_a(t,c) \le \tilde{k} \quad \forall t \in T, \qquad (9)$$

که در آن $\widetilde{M} = (M^1, M^2, M^3)$ یک عدد فازی مثلثی با مولفه‌های بسیار بزرگ است.

**اثبات**. ابتدا نشان می‌دهیم که جواب‌های شدنی مسئله‌ی $(P_3)$ برای سطح پایین مسئله‌ی $(P_2)$ بهینه هستند. اولا واضح است که هر بردار شدنی مانند$(C, A)$ برای مسئله‌ی $(P_3)$ برای مسئله‌ی سطح پایین $(P_2)$ نیز شدنی است. قیود (۹) نشان می‌دهند که $\tilde{k}$ از ماکزیمم عایدی مهاجم به ازای هر بردار شدنی $(C, A)$ کمتر نیست. محدودیت‌های (۸) نشان می‌دهند که $\tilde{k}$ از عایدی هدفی که مورد حمله قرار می‌گیرد بیشتر نیست (این قیود برای اهدافی که مورد حمله قرار نگیرند، زاید هستند). لذا از این دو دسته محدودیت نتیجه می‌شود که هدفی با بیشترین عایدی برای مهاجم مورد حمله قرار خواهد گرفت. از آنجا که تنها یک هدف مورد حمله قرار می‌گیرد، نتیجه می‌شود که جواب‌های شدنی مسئله‌ی $(P_3)$ از بین جواب‌های بهینه سطح پایین $(P_2)$ انتخاب می‌شوند.

به طور مشابه تابع هدف و قیود (۷) نتیجه می‌دهند که در جواب بهینه مسئله‌ی $(P_3)$ بردار $(C, A)$ با بیشترین عایدی برای مدافع انتخاب می‌شود. لذا جواب به دست آمده از مسئله‌ی $(P_3)$ یک جواب بهینه‌ی مسئله‌ی $(P_2)$ را نتیجه می‌دهد.

تابع هدف مسئله‌ی $(P_3)$ فازی است. در ادامه با توجه به نوع ترتیب تعریف شده روی اعداد فازی مثلثی (تعریف۲)، از برنامه‌ریزی الفبایی[1] برای بیشینه‌سازی تابع هدف استفاده می‌شود. این روش اهداف را به ترتیب بهینه می‌کند، به طوری که هر هدف روی جواب‌های بهینه مرحله‌ی قبل، بهینه می‌شوند. در این روش، بهینه‌سازی تا به اتمام رسیدن اهداف ادامه پیدا می‌کند یا در مرحله‌ای با این نتیجه که مسئله جواب بهینه‌ی متناهی ندارد یا جواب بهینه منحصربفرد است متوقف می‌شود (Ehrgott, 2005:128).

فرض کنید $\tilde{d} = (d^1, d^2, d^3)$ و $\tilde{k} = (k^1, k^2, k^3)$. اکنون با حل مسئله‌ی بیشینه‌سازی الفبایی زیر یک جواب فازی مثلثی برای مسئله‌ی $(P_3)$ خواهیم داشت.

$$(P_4): \quad lexmax\ (d^2, d^1 - d^3, d^1 + d^3)$$

$$s.t \quad \sum_{t\in T} c_t \le m, \tag{10}$$

$$0 \le c_t \le 1, \tag{11}$$

$$\sum_{t\in T} a_t = 1, \tag{12}$$

$$a_t \in \{0,1\}, \tag{13}$$

$$d^2 - U_d^2(t,c) \le (1-a_t)M \qquad \forall t \in T, \tag{14}$$

$$\left(U_d^3(t,C) - u_d^1(t,C)\right) - (d^3 - d^1) \le (1-a_t)M + \left(U_d^2(t,C) - d^2\right)M \ \forall\, t \in T, \tag{15}$$

$$d^3 + d^1 - \left(U_d^3(t,C) + U_d^1(t,C)\right) \le (1-a_t)M + \left(U_d^2(t,C) - d^2\right)M + (U_d^3(t,C) - U_d^1(t,C) - (d^3 - d^1)M \ \forall\, t \in T, \tag{16}$$

$$0 \le k^2 - U_a^2(t,C) \le (1-a_t)M \quad \forall t \in T, \tag{17}$$

$$\left(U_a^3(t,C) - U_a^1(t,C)\right) - (k^3 - k^1) \ge (1-a_t)M + (U_a^2(t,C) - k^2)M \ \forall\, t \in T, \tag{18}$$

$$k^3 + k^1 - \left(U_a^3(t,C) + U_a^1(t,C)\right) \ge (1-a_t)M + (U_a^2(t,C) - k^2)M + (U_a^3(t,C) - U_a^1(t,C) - (k^3 - k^1)M \ \forall\, t \in T, \tag{19}$$

$$d^1 \le d^2 \le d^3\ , k^1 \le k^2 \le k^3, \tag{20}$$

که در آن $M$ عدد مثبت بسیار بزرگی است. از آنجا که $M^1$، $M^2$ و $M^3$ اعداد مثبت بسیار بزرگی هستند، بی آن که خللی به مسئله وارد شود، قرار داده‌ایم $M^1 = M^2 = M^3 = M$.

[1]. Lexicographic maximization (lexmax)

**قضیه ۲.** جواب بهینه‌ی مسئله‌ی برنامه‌ریزی آمیخته‌ی $(P_4)$ یک جواب تعادل استاکلبرگ است.

اثبات. فرض کنید $(C,A)$ جواب بهینه مسئله‌ی $(P_4)$ باشد. اولا از قیود مسئله‌ی $(P_4)$ بدیهی است هر جواب این مسئله، یک نمایه راهبرد بازی است. همچنین قیود (17) نشان می‌دهند که $\tilde{k}=(k^1,k^2,k^3)$ از عایدی مهاجم به‌ازای هر بردار حمله‌ای کمتر نیست. همچنین قیود (۱۷)-(۱۹) اجازه نمی‌دهند $\tilde{k}$ از عایدی هدفی که مورد حمله قرار می‌گیرد، کمتر باشد. بنابراین چنانچه راهبرد مدافع $C$ باشد، این قیود به مهاجم اجازه نخواهند داد که به هدف دیگری که بیشینه عایدی را برایش ندارد حمله کند. لذا قیود مسئله، مهاجم را محدود به انتخاب بهترین پاسخ‌های خود می‌کند. اکنون فرض کنید بازی مدافع $\acute{C}\neq C$ و بازی مهاجم $\acute{A}$ باشد. $(\acute{C},\acute{A})$ یک جواب شدنی برای مسئله‌ی $(P_4)$ است و چون $(C,A)$ جواب بهینه این مسئله است و با توجه به قیود (۱۴)-(۱۶) مسئله‌ی $(P_4)$، با انتخاب نمایه راهبرد $(\acute{C},\acute{A})$ عایدی بیشتری نصیب مدافع نخواهد شد. لذا جواب بهینه بهترین پاسخ مدافع است، زمانی که مهاجم بهترین پاسخ خود را بازی می‌کند.

**مثال۱.** بازی امنیتی با چهار هدف $T=\{1,2,3,4\}$، سه منبع امنیتی و ماتریس‌های عایدی زیر را درنظر بگیرید:

**جدول (۱) ماتریس عایدی مدافع و مهاجم در مثال۱**

| بازیکنان / اهداف | عایدی مهاجم | | عایدی مدافع | |
|---|---|---|---|---|
| | بدون پوشش هدف | با پوشش هدف | بدون پوشش هدف | با پوشش هدف |
| ۱ | (۳, ٤ ,٦) | (-۳,-۲ ,۰) | (-٤,-۳,-۲) | (۹ ,۱۰ ,۱۱) |
| ۲ | (۳ ,۳ ,٤) | (-۲,-۲,-۲) | (-۳,-۲,-۲) | (۹ ,۱۰ ,۱۱) |
| ۳ | (٥ ,٥ ,۸) | (-۲,-۱ ,۰) | (-۲,-۱ ,۰) | (٥ ,۷ ,۸) |
| ٤ | (٥ ,٥ ,۸) | (-۱ ,۰ ,۰) | (-۱,-۱ ,۰) | (٤ ,٥ ,٦) |

مسئله‌ی بهینه‌سازی الفبایی $(P_4)$ با داده‌های جدول (۱) به صورت زیر است:

$$\text{lexmax}\ (d^2, d^1 - d^3, d^1 + d^3)$$
$$\text{s.t} \quad \sum_{t\in T} c_t \le 3$$
$$0 \le c_t \le 1$$
$$\sum_{t\in T} a_t = 1$$
$$a_t \in \{0,1\}$$
$$d^2 - \big(10\, c_1 - 3(1-c_1)\big) \le (1-a_1)M$$
$$d^2 - \big(10\, c_2 - 2(1-c_2)\big) \le (1-a_2)M$$
$$d^2 - \big(7\, c_3 - (1-c_3)\big) \le (1-a_3)M$$

$$d^2 - \left(5\ c_4 - (1 - c_4)\right) \le (1 - a_4)M$$
$$\left(3\ c_1 + (1 - c_1)\right) - (d^3 - d^1) \le (1 - a_1)M - \left(d^2 - \left(10\ c_1 - 3(1 - c_1)\right)\right)M$$
$$\left(3\ c_2 + (1 - c_2)\right) - (d^3 - d^1) \le (1 - a_2)M - \left(d^2 - \left(10\ c_2 - 2(1 - c_2)\right)\right)M$$
$$\left(3\ c_3 + 2(1 - c_3)\right) - (d^3 - d^1) \le (1 - a_3)M - \left(d^2 - \left(7\ c_3 - (1 - c_3)\right)\right)M$$
$$\left(2\ c_3 + (1 - c_4)\right) - (d^3 - d^1) \le (1 - a_4)M - \left(d^2 - \left(5\ c_4 - (1 - c_4)\right)\right)M$$
$$d^3 + d^1 - \left(21\ c_1 - 6(1 - c_1)\right) \le (1 - a_1)M - \left(d^2 - \left(10\ c_1 - 3(1 - c_1)\right)\right)M + \left((3\ c_1 + 2(1 - c_1) - (d^3 - d^1)\right)M$$
$$d^3 + d^1 - \left(20\ c_2 - 5(1 - c_2)\right) \le (1 - a_2)M - \left(d^2 - \left(10\ c_2 - 2(1 - c_2)\right)\right)M + \left((3\ c_2 + (1 - c_2) - (d^3 - d^1)\right)M$$
$$d^3 + d^1 - \left(13\ c_3 - 2(1 - c_3)\right) \le (1 - a_3)M - \left(d^2 - \left(7\ c_3 - (1 - c_3)\right)\right)M + \left((3\ c_3 + 2(1 - c_3) - (d^3 - d^1)\right)M$$
$$d^3 + d^1 - \left(10\ c_4 - (1 - c_3)\right) \le (1 - a_4)M - \left(d^2 - \left(5\ c_3 - (1 - c_4)\right)\right)M + \left((2c_4 + (1 - c_4) - (d^3 - d^1)\right)M$$
$$0 \le k^2 - \left(-2\ c_1 + (1 - c_1)\right) \le (1 - a_1)M$$
$$0 \le k^2 - \left(-2c_2 + 3(1 - c_2)\right) \le (1 - a_2)M$$
$$0 \le k^2 - \left(-\ c_3 + 5(1 - c_3)\right) \le (1 - a_3)M$$
$$0 \le k^2 - 7(1 - c_4) \le (1 - a_4)M$$
$$\left(3\ c_1 + 3(1 - c_1)\right) - (k^3 - k^1) \le (1 - a_1)M - \left(k^2 - \left(-2\ c_1 + (1 - c_1)\right)\right)M$$
$$\left(\ c_2 + (1 - c_2)\right) - (k^3 - k^1) \le (1 - a_2)M - \left(k^2 - \left(-2c_2 + 3(1 - c_2)\right)\right)M$$
$$\left(3\ c_3 + 3(1 - c_3)\right) - (k^3 - k^1) \le (1 - a_3)M - \left(k^2 - \left(-\ c_3 + 5(1 - c_3)\right)\right)M$$
$$\left(\ c_3 + 2(1 - c_4)\right) - (k^3 - k^1) \le (1 - a_4)M - \left(k^2 - 7(1 - c_4)\right)M$$
$$k^3 + k^1 - \left(-3\ c_1 + 9(1 - c_1)\right) \le (1 - a_1)M - \left(k^2 - \left(-2\ c_1 + (1 - c_1)\right)\right)M + \left((3\ c_1 + 3(1 - c_1) - (k^3 - k^1)\right)M$$
$$k^3 + k^1 - \left(-3c_2 + 7(1 - c_2)\right) \le (1 - a_2)M - \left(k^2 - \left(-2c_2 + 3(1 - c_2)\right)\right)M + \left((\ c_2 + (1 - c_2) - (k^3 - k^1)\right)M$$
$$k^3 + k^1 - \left(-\ c_3 + 14(1 - c_3)\right) \le (1 - a_3)M - \left(k^2 - \left(-\ c_3 + 5(1 - c_3)\right)\right)M + \left((3\ c_3 + 3(1 - c_3) - (k^3 - k^1)\right)M$$
$$k^3 + k^1 - \left(-\ c_4 + 13(1 - c_3)\right) \le (1 - a_4)M - \left(k^2 - 7\left((1 - c_4)\right)\right)M + \left((c_4 + 2(1 - c_4) - (k^3 - k^1)\right)M$$
$$0 \le k^1 \le k^2 \le k^3, 0 \le d^1 \le d^2 \le d^3.$$

با حل مسئله‌ی فوق به کمک نرم‌افزار لینگو، بردار حمله مهاجم و راهبرد آمیخته مدافع به صورت زیر به دست می‌آیند:

$$A = (0{,}1{,}0{,}0), C = (0.55{,}0.60{,}0.83{,}1).$$

که نشان می‌دهد هدف چهارم باید به صورت کامل پوشش داده شده و به ترتیب ۰,۵۵، ۰,۶۰ و ۰,۸۳ باقیمانده‌ی منابع به اهداف اول، دوم و سوم اختصاص یابد. این نتیجه که باید حداکثر پوشش امنیتی برای هدف چهارم درنظر گرفته شود، با نگاهی به جدول عایدی‌ها نیز منطقی به نظر می‌رسد. زیرا مهاجم با حمله به هدف چهارم بیشترین عایدی را در هر دو حالت (وجود پوشش یا عدم پوشش هدف چهارم) به دست می‌آورد، لذا منطقی است که به این هدف حمله شود و لذا نسبت به سایر اهداف باید پوشش بیشتری برای آن درنظر گرفت. در نهایت با توجه به بردار تخصیص به دست آمده، مهاجم حمله به هدف دوم را ترجیح خواهد داد. همچنین جواب بهینه‌ی مسئله‌ی فوق نشان می‌دهد به ازای نمایه‌ی راهبرد $(C, A)$ حداکثر عایدی مدافع و مهاجم به ترتیب به صورت اعداد فازی $\tilde{d} = (3.9,5.1,6.9)$ و $\tilde{k} = (0,0,1)$ (یعنی تقریبا ۵,۱ و تقریبا صفر) به دست می‌آیند.

**حل بازی امنیتی با محافظت فریبنده**

در برخی از مسائل دنیای واقعی، مدافع می‌تواند برای کاهش بهره‌وری مهاجم در جمع‌آوری اطلاعات یا کاهش هزینه‌های خود، از منابع غیرواقعی استفاده کند. به عنوان مثال استفاده از حسگرها در مکان‌های مختلف یا دوربین‌های مخفی در جاده‌ها برای شناسایی اتومبیل‌هایی با سرعت غیرمجاز یا استفاده از دوربین‌های جعلی برای فریب رانندگان متخلف از جمله منابع غیرواقعی هستند. فرض کنید مدافع برای حفاظت اهداف، از سه نوع پوشش واقعی، جعلی[1] و مخفی[2] استفاده کند. در این بازی راهبرد محض مدافع $i \in \{R, F, Se, N\}$ است که نشان‌دهنده‌ی انتخاب یک نوع منبع واقعی (R)، جعلی (F)، مخفی (Se) و یا فاقد پوشش‌گذاشتن هدف (N) است. راهبرد آمیخته‌ی مدافع، احتمالات استفاده از راهبردهای محض است. به عبارتی یک راهبرد آمیخته مدافع انتخاب پوشش $c_{t,i}$ برای هدف $t \in T$ است که در آن $i \in \{R, F, Se\}$. اگر محافظت جعلی موفق شود، مهاجم هدف را محافظت شده و اگر شکست بخورد مهاجم آن را فاقد پوشش مشاهده می‌کند. فرض کنید محافظت جعلی با احتمال $r_F$ موفق شود. همچنین اگر حفاظت مخفی موفق شود مهاجم هدف را بدون محافظت و اگر شکست بخورد هدف را محافظت شده مشاهده می‌کند. فرض کنید هر محافظت مخفی با احتمال $r_{Se}$ شکست می‌خورد. بعد از مشاهدات زیاد، مهاجم بردار پوشش $e$ را مشاهده می‌کند که در آن $e_t$ احتمال این است که مهاجم هدف $t$ را محافظت شده ببیند. به عبارتی اگر مدافع

[1]. Fake resource
[2]. Secret resource

برای هدف $t$راهبرد $C = (c_{t,R}, c_{t,F}, c_{t,Se})$ را اتخاذ کند، مهاجم آن را به شکل بردار $e$ مشاهده می‌کند که در آن

$$\forall t \in T \qquad e_t = c_{t,R} + r_F c_{t,F} + r_{Se} c_{t,Se}.$$

به عنوان مثال اگر مدافع از حسگر به عنوان منبع مخفی استفاده نماید، مهاجم پس از مشاهدات زیاد با احتمال ۷۰ درصد تشخیص می‌دهد که هدف مورد نظر مجهز به حسگر است. چنانچه $c_{t,Se}$ میزان پوشش حفاظتی مخفی در هدف $t$ باشد و از منابع واقعی یا جعلی در این هدف استفاده نشده باشد، مهاجم میزان محافظت این هدف را $e_t = 0.7c_{t,Se}$ مشاهده می‌کند.

به ازای یک نمایه راهبرد سه تایی $(C, e, A)$ ، عایدی مورد انتظار مدافع و مهاجم به ترتیب به صورت زیر تعریف می‌شود:

$$\widetilde{U}_d(C, A) = \sum_{t \in T} a_t \, \widetilde{U}_d(C, t),$$
$$\widetilde{U}_a(e, A) = \sum_{t \in T} a_t \, \widetilde{U}_a(e, t),$$

که در آن

$$\widetilde{U}_d(C, t) = \big(c_{t,R} + c_{t,Se}\big)\widetilde{U}_d^c(t) + \big(1 - c_{t,R} - c_{t,Se}\big)\widetilde{U}_d^u(t),$$
$$\widetilde{U}_a(e, t) = e_t \widetilde{U}_a^c(t) + (1 - e_t)\widetilde{U}_a^u(t).$$

بودجه مدافع برای خرید منابع جعلی و مخفی را $B$ و هزینه‌ی لازم برای خرید هر منبع جعلی و مخفی را به ترتیب $B_F$ و $B_{Se}$ درنظر می‌گیریم. لذا محدودیت‌های زیر را در مسئله خواهیم داشت:

$$B_F \sum_{t \in T} c_{t,F} + \tilde{B}_{Se} \sum_{t \in T} c_{t,Se} \le B \qquad (21)$$

بر اساس توضیحات فوق، محاسبات فازی و با استفاده از قضیه ۲، برای حل یک بازی امنیتی با منابع فریبنده، می‌توان راهبرد دفاعی بهینه را با حل مسئله‌ی بهینه‌سازی الفبایی زیر به دست آورد:

$$(P_5): \ lexmax \quad (d^2, d^1 - d^3, d^1 + d^3)$$
$$s.t \quad (10) - (14),$$
$$B_F \sum_{t \in T} c_{t,F} + B_{Se} \sum_{t \in T} c_{t,Se} \le B, \qquad (22)$$
$$c_t^i \in [0,1] \qquad \forall t \in T, i \in \{R, F, Se\}, \qquad (23)$$
$$c_{t,R} + c_{t,F} + c_{t,Se} \le 1 \qquad \forall t \in T, \qquad (24)$$
$$e_t = c_{t,R} + r_F c_{t,F} + r_{Se} c_{t,Se} \qquad \forall t \in T, \qquad (25)$$
$$0 \le k^2 - U_a^2(t, e) \le (1 - a_t)M \quad \forall t \in T, \qquad (26)$$

$$\left(U_a^3(t,e)-U_a^1(t,e)\right)-(k^3-k^1)\geq (1-a_t)M +(U_a^2(t,e)-k^2)M \quad \forall\, t\in T, \qquad (27)$$

$$k^3+k^1-\left(U_a^3(t,e)+U_a^1(t,e)\right)\geq (1-a_t)M+(U_a^2(t,e)-k^2)M +(U_a^3(t,e)-U_a^1(t,e)-(k^3-k^1)M \quad \forall\, t\in T, \qquad (28)$$

$$d^1\leq d^2\leq d^3\,, k^1\leq k^2\leq k^3. \qquad (29)$$

**مثال۲.** بازی امنیتی با چهار هدف، یک منبع واقعی و ماتریس‌های عایدی زیر را در نظر بگیرید.

**جدول (۲) ماتریس عایدی مدافع و مهاجم مثال۲**

| بازیکنان / اهداف | عایدی مهاجم | | عایدی مدافع | |
|---|---|---|---|---|
| | با پوشش هدف | بدون پوشش هدف | با پوشش هدف | بدون پوشش هدف |
| ۱ | (۰ ,-۳ ,-۳) | (۶ ,۲ ,۱) | (۱۲ ,۱۰ ,۹) | (-۲ ,-۳ ,-۴) |
| ۲ | (-۱ ,-۲ ,-۲) | (۴ ,۳ ,۳) | (۱۱ ,۱۰ ,۸) | (-۲ ,-۲ ,-۳) |
| ۳ | (-۱ ,-۱ ,-۱) | (۸ ,۵ ,۵) | (۷ ,۷ ,۶) | (۰ ,-۱ ,-۲) |
| ٤ | (-۱ ,-۳ ,-۴) | (۸ ,۵ ,۵) | (۶ ,۵ ,۴) | (۰ ,-۱ ,-۱) |

فرض کنید بودجه‌ی موجود $B=100$ و هزینه‌ی مورد نیاز برای خرید هر منبع مخفی و جعلی به ترتیب $B_{Se}=30$ ، $B_F=50$ و احتمال اینکه مهاجم منابع فریبنده‌ی مخفی وجعلی را شناسایی کند به ترتیب $r_{se}=0.4$ و $1-r_F=0.3$ باشد. مسئله‌ی $(P_5)$ به ازای داده‌های فوق به کمک نرم افزار لینگو حل شده و نتایج حاصل در مورد میزان استفاده از منابع واقعی، جعلی و مخفی برای هریک از اهداف در جدول (۳) آورده شده است.

**جدول (۳) میزان محافظت‌های محاسبه شده برای هر**

| اهداف / محافظت‌ها | ۱ | ۲ | ۳ | ۴ |
|---|---|---|---|---|
| واقعی | ۰/۲۷ | ۰/۲۹ | ۰/۱۹ | ۰/۲۵ |
| جعلی | ۰ | ۰ | ۰/۵۳ | ۰/۲۴ |
| مخفی | ۰ | ۰/۱۱ | ۰ | ۰ |

با حل مسئله‌ی $(P_5)$ منابع امنیتی واقعی موجود، منابع جعلی و منابع مخفی به ترتیب به صورت $c_R=(0.27,0.29,0.19,0.25)$، $c_F=(0,0,0.53,0.24)$ و $c_{Se}=(0,0.11,0,0)$ به اهداف اختصاص داده می‌شود. همچنین بردار مشاهدات مهاجم نیز به صورت $e=(0.27,0.33,0.56,0.42)$ به دست می‌آید. هدف ۱ فاقد منبع امنیتی فریبنده است لذا بدیهی

است $e_1 = c_1$. با توجه به جدول عایدی مهاجم، میزان پوشش به دست آمده از مدل برای هر هدف، با ترتیب احتمال حمله مهاجم به اهداف منطقی است. از جدول عایدی بنظر می‌رسد مهاجم ترجیح می‌دهد به ترتیب به اهداف ۳، ۴، ۲ و ۱ حمله کند. با توجه به عایدی‌های مهاجم، حمله به هدف ۳ نسبت به هدف ۴ ارجح بنظر می‌رسد. لذا هدف ۳ نیازمند پوشش بیشتری است. در پاسخ به دست آمده از مدل، میزان پوشش منابع واقعی هدف ۳ کمتر از هدف ۴ است. کمبود نیرو در این هدف با استفاده از منابع مخفی جبران شده است. در نهایت با این چیدمان بهینه نیروهای امنیتی، راهبرد بهینه مهاجم $A = (0,1,0,0)$ و به ازای نمایه‌ی راهبرد $(C, e, A)$ حداکثر عایدی مدافع و مهاجم به ترتیب به صورت عدد فازی $\tilde{d} = (1.5,1.5,2.74)$ و $\tilde{k} = (0.65,1.65,1.65)$ (یعنی تقریبا ۱,۵ و تقریبا ۱,۶۵) به دست می‌آیند.

در مسئله‌ی $(P_5)$، چنانچه اطلاعات بودجه به صورت اعداد فازی مثلثی $\tilde{B}_F = (B_F^1, B_F^2, B_F^3)$، $\tilde{B}_{Se} = (B_{Se}^1, B_{Se}^2, B_{Se}^3)$ و $B = (B^1, B^2, B^3)$ بیان شده باشد، قیود زیر جایگزین قید (۲۲) می‌شوند:

$$B_F^2 \sum_{t\in T} c_{t,F} + B_{Se}^2 \sum_{t\in T} c_{t,Se} \le B^2,$$

$$(B_F^3 - B_F^1) \sum_{t\in T} c_t^F + \left(B_{Se}^3 - B_{Se}^1\right) \sum_{t\in T} c_{t,Se} \le B^3 - B^1 + \left(B^2 - B_F^2 \sum_{t\in T} c_{t,F} - B_{Se}^2 \sum_{t\in T} c_t^{Se}\right) \mathrm{M},$$

$$(B_F^3 + B_F^1) \sum_{t\in T} c_{t,F} + \left(B_{Se}^3 + B_{Se}^1\right) \sum_{t\in T} c_{t,Se} \ge B^3 + B^1 + \left(B^2 - B_F^2 \sum_{t\in T} c_{t,F} - B_{Se}^2 \sum_{t\in T} c_{t,Se}\right) \mathrm{M} + \left(B^3 - B^1 - (B_F^3 - B_F^1) \sum_{t\in T} c_{t,F} - (B_{Se}^3 - B_{Se}^1) \sum_{t\in T} c_{t,Se}\right) M.$$

## نتیجه‌گیری و پیشنهادها

بهینه‌سازی تخصیص نیروها مسئله‌ی مهمی است که در شرایط جنگی برای نقاط مورد حمله دشمن و در هر شرایطی (اعم از جنگی یا غیرجنگی) برای مراکز حساس و زیرساخت‌ها مورد توجه است. مهاجم با انگیزه نیروهای دفاعی را تحت‌نظر گرفته و از الگوی چینش نیروها بهره‌برداری می‌کند. نیروهای مدافع باید بتوانند عکس‌العمل مهاجم در برابر راهبردهای مختلف

مدافع را با بالاترین احتمالات پیش‌بینی کنند. از طرفی محدودیت منابع مشکل مهمی در بسیاری از حوزه‌های امنیتی است. نظریه‌ی بازی می‌تواند به عنوان یک ابزار ارزشمند برای تجزیه و تحلیل این مسائل و به‌خصوص برای تعیین راهبرد بهینه در شرایط تضاد منافع استفاده شود. بازی‌های امنیتی با توجه به نوع و تعداد مهاجمان و مدافعان در حل مسائل مختلف امنیتی کاربرد دارند. در این تحقیق یک مدل ریاضی برای تخصیص بهینه‌ی نیروهای دفاعی-امنیتی در محیط فازی ارائه گردید. برای این منظور، با درنظرگرفتن محدودیت منابع و بر اساس تحلیل نظریه بازی‌ها این مدل پیشنهادی تشریح گردید. همچنین از آنجا که اطلاعات نیروهای امنیتی از میزان اهمیت اهداف برای مهاجم و همچنین اطلاعات مهاجم از الگوی چینش نیروهای امنیتی دقیق نیست، برای بیان این اطلاعات از اعداد فازی مثلثی استفاده شده است.

نیروهای دفاعی می‌توانند به منظور کاهش بهره‌وری مهاجم از منابع مخفی یا برای کاهش هزینه‌های خود از منابع جعلی استفاده کنند. اما مدافع برای استفاده از منابع فریبنده بودجه محدودی در اختیار دارد. همچنین استفاده از این منابع می‌توانند با احتمال خاصی با شکست مواجه شود. با درنظرگرفتن این احتمال و محدودیت بودجه، یک مدل ریاضی برای بهینه‌سازی تخصیص این منابع فریبنده معرفی شد. در مدل پیشنهادی، میزان بودجه، اهمیت اهداف برای مهاجم و مدافع و راهبردهای ممکن آن‌ها درنظرگرفته شده و سپس تخصیص نیروها بهینه شد.

در این پژوهش بازی امنیتی مورد مطالعه قرار گرفته است که یک نوع مهاجم قصد حمله به اهداف را دارد. در ادامه بازی امنیتی با منابع فریبنده با احتمال حمله چند مهاجم به اهداف، در محیط قطعی/فازی می‌تواند مورد بررسی قرار گیرد. همچنین در این پژوهش راهبردهای دو بازیکن، میزان پوشش حفاظتی مدافع و بردار حمله مهاجم، قطعی درنظرگرفته شده است. از مدل پیشنهادی می‌توان برای مطالعه موردی مکان‌یابی جهت استقرار سامانه‌های پدافند موشکی، گشت‌زنی نیروهای امنیتی در مناطق مختلف نیز استفاده کرد.

## منابع

≠ بیگدلی، حمید. و طیبی، جواد. (۱۳۹۷). روش برنامه‌ریزی ریاضی برای حل و مدل‌سازی سناریوهای نبرد در سامانه پشتیبان تصمیم بازی جنگ تاکتیکی و عملیاتی، *فصلنامه آینده‌پژوهی دفاعی*، ۳ (۹): ۵۶-۳۵.

≠ شادرام، وحید.، بیگدلی، حمید. و همت، حمید. (۱۳۹۸). مدل‌سازی و حل مسأله تعارض دولت– تروریست با استفاده از بازی دیفرانسیلی، *فصلنامه آینده پژوهی دفاعی*، ۴ (۱۳): ۸۶-۶۱.

≠ An, B. (2017, August). Game Theoretic Analysis of Security and Sustainability. In IJCAI (pp. 5111-5115).

≠ An, B., Ordóñez, F., Tambe, M., Shieh, E., Yang, R., Baldwin, C., ... & Meyer, G. (2013). A deployed quantal response-based patrol planning system for the US Coast Guard. *Interfaces*, *43*(5), 400-420.

≠ Bigdeli, H., & Hassanpour, H. (2018). An approach to solve multi-objective linear production planning games with fuzzy parameters. *Yugoslav Journal of Operations Research*, *28*(2), 237-248.

≠ Bigdeli, H., Hassanpour, H., & Tayyebi, J. (2017). Optimistic and Pessimistic Solutions of Single and Multi-Objective Matrix Games with Fuzzy Payoffs and Analysis of Some Military Cases.

≠ Brown, G., Carlyle, M., Diehl, D., Kline, J., & Wood, K. (2005). A two-sided optimization for theater ballistic missile defense. *Operations research*, 53(5), 745-763.

≠ Cohen, F., & Koike, D. (2004, June). Misleading attackers with deception. In *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004.* (pp. 30-37). IEEE.

≠ Conitzer, V., & Sandholm, T. (2006, June). Computing the optimal strategy to commit to. In *Proceedings of the 7th ACM conference on Electronic commerce* (pp. 82-90).

≠ Ehrgott, M. (2005). *Multicriteria optimization* (Vol. 491). Springer Science & Business Media.

≠ Ezzati, R., Khorram, E., & Enayati, R. (2015). A new algorithm to solve fully fuzzy linear programming problems using the MOLP problem. *Applied mathematical modelling*, 39(12), 3183-3193.

≠ Fang, F., Nguyen, T. H., Pickles, R., Lam, W. Y., Clements, G. R., An, B., ... & Lemieux, A. (2016, February). Deploying PAWS: Field Optimization of the Protection Assistant for Wildlife Security. In *AAAI* (Vol. 16, pp. 3966-3973).

≠ Jain, M., Kardes, E., Kiekintveld, C., Ordónez, F., & Tambe, M. (2010, July). Security games with arbitrary schedules: A branch and price approach. In *AAAI*.

≠ Kiekintveld, C., Jain, M., Tsai, J., Pita, J., Ordóñez, F., & Tambe, M. (2009, May). Computing optimal randomized resource allocations for massive security games. In *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1* (pp. 689-696).

≠ Lye, K. W., & Wing, J. M. (2005). Game strategies in network security. *International Journal of Information Security*, *4*(1-2), 71-86.

≠ Paruchuri, P., Kraus, S., Pearce, J. P., Marecki, J., Tambe, M., & Ordonez, F. (2008). Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games.

≠ Pita, J., Jain, M., Marecki, J., Ordóñez, F., Portway, C., Tambe, M., ... & Kraus, S. (2008, May). Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport. In *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track* (pp. 125-132).

≠ Pita, J., Jain, M., Ordónez, F., Portway, C., Tambe, M., Western, C., ... & Kraus, S. (2009). Using game theory for Los Angeles airport security. *AI magazine*, *30*(1), 43-43.

≠ Sakawa, M. (2013). *Fuzzy sets and interactive multiobjective optimization*. Springer science & business media.

≠ Sandler, T. & D. G. A. M. (2003). *Terrorism and Game Theory, Simulation and Gaming*, 34 (3): 319–337.

≠ Tambe, M. (2011). Security and game theory: algorithms, deployed systems, lessons learned. Cambridge University Press.

≠ Tambe, M., Jiang, A. X., An, B., & Jain, M. (2014, March). Computational game theory for security: Progress and challenges. In *AAAI spring symposium on applied computational game theory*.

≠ Trejo, K. K., Clempner, J. B., & Poznyak, A. S. (2015). A Stackelberg security game with random strategies based on the extraproximal theoretic approach. *Engineering Applications of Artificial Intelligence*, *37*, 145-153.

≠ Yin, Z., Korzhyk, D., Kiekintveld, C., Conitzer, V., & Tambe, M. (2010, May). Stackelberg vs. Nash in security games: Interchangeability, equivalence, and uniqueness. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: volume 1-Volume 1* (pp. 1139-1146).