تاریخ دریافت: ۱۳۹۹/۱۰/۲۳
تاریخ پذیرش: ۱۳۹۹/۱۲/۲۴

از صفحه ۱۲۸ تا صفحه ۱۵۴

تخصیص بهینه منابع در جنگ سایبری با رویکرد نظریه بازی در محیط غیرقطعی

اسماعیل افراشته[۱]، اکبر زارع چاوشی[۲]

چکیده

افزایش اعتماد به فناوری اطلاعات و ارتباطات، تعریف امنیت و ماهیت جنگ را به طرز چشمگیری تغییر داده است. بسیاری از زیرساخت‌های مهم مانند بانک‌ها، فرودگاه‌ها، سیستم‌های اطلاعاتی، مراکز تحقیقاتی، نیروگاه‌ها، بیمارستان‌ها، مراکز مخابراتی، خطوط انتقال نفت و غیره به‌طور بالقوه در برابر حملات سایبری آسیب پذیر هستند. نظریه بازی مجموعه‌ای غنی از ابزارهای ریاضی را برای مدل‌سازی و تحلیل تعاملات استراتژیک بین مهاجمان و مدافعان در فضای جنگ سایبری فراهم کرده است که می‌توان از آن به عنوان یک مبنای تئوریکی پایه‌ای و دقیق در امر تصمیم‌گیری در شرایط پیچیده جنگی برای انتخاب راهبرد بهینه استفاده کرد. در این مقاله مسئله چالش برانگیز تخصیص بهینه منابع با اطلاعات نادقیق در جنگ سایبری با روش نظریه بازی به صورت یک مدل برنامه‌ریزی صحیح-آمیخته درجه دو غیرقطعی فرمول‌بندی شده و با دو معیار محدودیت درجه باور و ارزش در معرض ریسک شرطی بررسی می‌گردد.

واژه‌های کلیدی: نظریه بازی، حمله سایبری، دفاع سایبری، برنامه‌ریزی غیرقطعی

[۱] پژوهشگر، مرکز شبیه سازی ریاضی، پژوهشکده آماد و فناوری‌های دفاعی و پدافند غیر عامل، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران afrashteh66@yahoo.com

[۲] عضو هیئت علمی، مرکز شبیه سازی ریاضی، پژوهشکده آماد و فناوری‌های دفاعی و پدافند غیر عامل، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران

Optimal resource allocation in cyber warfare with a game theory approach in uncertain environment

Afrashteh E.[۱], Zare Chavoshi A.[۲]

ABSTRACT

Increasing confidence in information and communication technology has dramatically changed the definition of security and the nature of war. Many important infrastructures, such as banks, airports, information systems, research centers, power plants, hospitals, telecommunication centers, oil pipelines, etc., are potentially vulnerable to cyberattacks. Game theory has provided a rich set of mathematical tools for modeling and analyzing strategic interactions between attackers and defenders in cyber warfare, which can be used as a fundamental and accurate theoretical basis for deciding in the most challenging war situations to select the optimal strategy. In this paper, the challenging propblem of optimal resource allocation in cyber warfare with uncertain information in cyber warfare is formulated by game theory as a uncertain mixed-integer quadratic programming model and it is investigated with limited belief degree and conditional value at risk criterions.

KEYWORDS: Game Theory, Cyber Attack, Cyber Defense, Uncertain Programing

[1] Researcher, Supreme National Defense University, Tehran, Iran
2 Faculty Member, Supreme National Defense University, Tehran, Iran

۱- مقدمه

فناوری اطلاعات و ارتباطات فرماندهان نظامی را قادر ساخته در زمان مناسب از اطلاعات صحیح برخوردار باشند و تغییرات بسیاری در ماهیت جنگ به وجود آورده است. فضای مجازی به فضای جنگ جدیدی تبدیل شده است که در آن سلاح ها عبارتند از مهندسی اجتماعی، ویروس‌های به روز شده، اسب‌های تروجان، کرم‌ها، حمله منع سرویس[1] و تهدیدات مداوم پیشرفته [۱] ،[۲]. حملات سایبری ممکن است مستقیماً به یک اثر کشنده منجر نشوند، بلکه می‌توانند باعث سوءاستفاده، نقص عملکرد یا از بین رفتن تجهیزات شوند [۳]، [۴].

در فضای سایبر، سلاح‌ها بر مبنای نقاط ضعف سیستم دفاعی هدف طراحی می شوند. هرگونه ضعف در رویه‌های امنیتی سیستم‌ها، طرح‌ها، کنترل‌های داخلی یا سیستم‌های اجرایی می‌تواند توسط یک منبع تهدید مورد سوء استفاده قرار گیرد [۵]. ماهیت پویای آسیب‌پذیری‌ها حاکی از آن است که آنها به مرور زمان در حال تغییر هستند. تشخیص آسیب پذیری‌ها توسط مدافع باعث بی‌اثر شدن سلاح مهاجم و تقویت سیستم دفاعی در برابر حملات مهاجم می‌شود.

بسیاری از محققان از جمله روی[2] و همکاران [۶]، کی‌کینتولد[3] و همکاران [۷] و تامب[4] [۸] از نظریه بازی برای مدل‌سازی تعاملات استراتژیک بین مهاجمان و مدافعان در فضای مجازی استفاده کرده‌اند. نظریه بازی در موضوعات بی شماری از جمله تخصیص منابع، امنیت شبکه و مدل‌های همکاری استفاده شده است. مسئله تخصیص منابع که معمولاً به عنوان بازی تخصیص از آن یاد می‌شود، یک بازی معمولی در حوزه سایبر است [۹]. در این بازی مدافع و مهاجم تصمیم می‌گیرند که منابع مربوطه را به کجاها اختصاص دهند. منابع مدافع ممکن است زیرساخت‌های امنیتی مانند فایروال‌ها، آنتی‌ویروس‌ها و غیره

[1] Denial of Service
[2] Roy
[3] Kiekintveld
[4] Tambe

باشد. به عنوان مثال، یکی از اهداف اصلی مدیر یک شبکه تخصیص بهینه منابع این است که خطر حمله و همچنین هزینه غیرضروری مرتبط به حداقل رسانیده شود [۱۰]. همینطور مهاجم نیز ممکن است منابع محدودی در اختیار داشته باشد یا اینکه هر یک از عملیات تهاجمی می‌تواند خطر پیگیری و مجازات را نیز در پی داشته باشد.

مسئله تصمیم‌گیری برای تخصیص بهینه منابع در جنگ سایبری امری بسیار پیچیده است و استفاده از مدل‌های نظریه بازی برای تحلیل راهبردهای پیش رو مفید به نظر می‌رسد. اما با توجه به نامشخص و غیر دقیق بودن اطلاعات موقعیت‌ها، هزینه‌ها، دستاوردها، میزان صدمات وارده در راهبردهای حمله و دفاع جنگ سایبری لازم است که از مدل‌های غیرقطعی نظریه بازی برای فرمول‌بندی جنگ‌های سایبری استفاده شود. در واقع به علت عدم وجود نمونه به اندازه کافی و عدم اطلاعات کافی از هزینه‌ها و دستاوردهای راهبردهای حمله و دفاع می‌توان از درجات باور کارشناسان برای توصیف این داده‌های غیرقطعی استفاده کرد. در این مقاله هدف ما بررسی مسئله تخصیص در جنگ سایبری با رویکرد نظریه بازی در محیط غیرقطعی است.

این مقاله در پنج بخش سازماندهی شده است. پس از بخش مقدمه، بخش بعدی مروری مختصر از ادبیات تحقیقی در زمینه نظریه عدم قطعیت و تخصیص منابع با رویکرد نظریه بازی ارائه می‌دهد. سپس مفاهیم مقدماتی نظریه عدم قطعیت مطرح شده و یک مدل بازی برای مسئله تخصیص منابع در جنگ سایبری و در محیط قطعی بیان می‌شود. در ادامه مدل تخصیص غیرقطعی با محدودیت درجه باور و مدل تخصیص غیرقطعی با ارزش در معرض ریسک شرطی ارائه می‌گردد. همچنین برای هر مدل یک مطالعه موردی برای نشان دادن رویکرد پیشنهادی ارائه می‌گردد. در نهایت نتیجه‌گیری و پیشنهادات برای مطالعات آتی بیان می‌شود.

۲- پیشینه پژوهش

توسعه الگوریتم‌های تخصیص منابع در حوزه‌های امنیت فیزیکی در دهه گذشته یکی از موضوعاتی است که مورد توجه محققان زیادی قرار گرفته است که از این جمله می‌توان به [۶]، [۸]، [۱۱] و [۱۲] اشاره کرد. به‌عنوان نمونه، نویسندگان در منابع [۷]، [۱۳]، [۱۴] برای اختصاص منابع امنیتی محدود به پست‌های بازرسی تصادفی در فرودگاه بین المللی لس‌آنجلس از بازی‌های تخصیص استفاده کردند. حملاتی که در دنیای سایبر انجام می‌شوند بسیار پیچیده‌تر از حملاتی هستند که در دنیای فیزیکی انجام می‌شوند. حملات دیجیتالی غالباً برای حواس انسان غیرقابل تصور بوده، محدود به جغرافیا و مرزهای سیاسی نبوده و بسیار پویا و پراکنده هستند [۱۱]. بولیم[1] و همکاران [۱۵] پاسخ به نفوذ در سیستم‌های کنترل دسترسی را به عنوان یک مسئله تخصیص منابع مورد بررسی قرار دادند. نویسندگان تعامل بین یک مهاجم و یک سیستم تشخیص نفوذ توزیع شده را به عنوان یک بازی مجموع ناصفر غیرهمکارانه مدل کردند. آنها الگوریتمی برای تخصیص بهینه زمان مدیر سیستم که به عنوان یک منبع کمیاب در نظر گرفته شده است، ارائه کردند. وانک[2] و همکاران [۱۸] یک بازی را مورد بررسی قرار دادند که در آن مهاجم با ارسال بسته‌های مخرب از چندین ورودی شبکه به دنبال آسیب رساندن به حریف است. این مدافع به دنبال تخصیص بهینه منابع موجود جهت به حداکثر رساندن احتمال شناسایی بسته‌های مخرب تحت محدودیت‌های تأخیر شبکه است. نویسندگان این مسئله را به عنوان یک بازی امنیتی مبتنی بر شبکه با منابع متعددی از قابلیت‌های ناهمگن شکل داده و یک مدل برنامه‌ریزی ریاضی برای آن پیشنهاد کردند. فیلدر[3] و همکاران [۱۶] تعامل بین یک مهاجم همه کاره و تیمی از مدیران سیستم را تحلیل کردند. نویسندگان از یک مدل نظریه بازی برای تخصیص بهینه منابع امنیت سایبری مانند زمان سرپرستان در کارهای

[1] Bloem
[2] Vanek
[3] Fielder

مختلف استفاده کردند. آنها در این بازی ایستای دو نفره و همکارانه دریافتند که راهبرد مدافع مستقل از راهبرد مهاجم، بهینه است.
همچنین از نظریه بازی برای تعیین تخصیص بهینه کل بودجه دفاعی بر روی اجزای مختلف سیستم به منظور به حداقل رساندن احتمال موفقیت یک حمله احتمالی یا به حداکثر رساندن هزینه مورد انتظار آن استفاده می‌شود. برای مثال آزیز و بیار[1] [۱۷] از یک بازی استفاده کردند که در آن مدافع سعی می‌کند با صرف هر چه بیشتر بودجه، از حمله مهاجمان جلوگیری کند. نویسندگان با استفاده از نظریه بازی راهبردهای حمله و دفاع بهینه را مشخص کردند. وان دیجک[2] و همکاران [۱۸] یک بازی پویای دونفره تحت عنوان فلیپیت[3]، را ارائه کردند که در آن مدافع و مهاجم برای کنترل یک منبع مبارزه می کنند. بسته به مسئله تحت مطالعه، منبع ممکن است یک رمز عبور یا یک زیرساخت کلی باشد. باورز[4] و همکاران [۱۹] کاربرد فلیپت را در طیف گسترده‌ای از مسائل امنیتی در دنیای واقعی از جمله سیاستهای تنظیم مجدد گذرواژه و محاسبات ابری نشان دادند. نویسندگان نتیجه گرفتند که این مدل در دنیایی که هیچ سیستمی در آن ایمن نیست، کاربردهای بی‌شماری دارد و فرضیه‌های طراحان سیستم امنیتی ممکن است دیگر مورد تایید نباشند.

در بسیاری از مسائل دنیای واقعی، به ویژه در مدل‌سازی و شبیه سازی جنگ‌ها، پارامترها و اطلاعات مدل‌های تحت مطالعه نادقیق و غیرقطعی هستند و برای توصیف این داده‌ها می‌توان از درجات باور کارشناسان استفاده کرد. در سال ۲۰۰۷، لیو[5] نظریه عدم قطعیت را برای برخورد با درجات باور معرفی کرد [۲۰] و در سال ۲۰۰۹، آن را بر پایه چهار اصل نرمال بودن، اصل دوگانگی، اصل زیرجمعی و اصل حاصلضربی اندازه غیرقطعی تکمیل کرد [۲۱]. سپس پنگ[6] و

[1] Azaiez and Bier
[2] Van Dijk
[3] Flipit
[4] Bowers
[5] Liu
[6] Peng

ایوامورا[1] شرایط لازم و کافی برای توزیع غیرقطعی را اثبات کردند [۲۲]. بعلاوه، لیو مفهوم توزیع غیرقطعی معکوس را ارائه کرد و شرایط لازم و کافی برای آن را ارائه کرد [۲۳] و [۲۴]. همچنین قضیه برگردانی اندازه [۲۴]، مفهوم استقلال متغیرهای غیرقطعی [۲۱]، قانون عملگری برای محاسبه توزیع غیرقطعی و توزیع غیرقطعی معکوس توابع یکنوای اکید از متغیرهای غیرقطعی مستقل [۲۴]، مفهوم عملگر مقدار مورد انتظار [۲۰] و خطی بودن آن توسط لیو ارائه شدند. لیو و ها[2] یک فرمول کاربردی برای محاسبه مقادیر مورد انتظار توابع یکنوای اکید از متغیرهای غیرقطعی مستقل به دست آوردند [۲۵]. برای مدل‌بندی مسائل بهینه‌سازی با داده‌های غیرقطعی، برنامه‌ریزی غیرقطعی توسط لیو در سال ۲۰۰۹ ارائه شد [۲۶]. در زمینه مدل‌های بازی با داده‌های غیرقطعی از نوع فازی تحقیقات ارزنده‌ای انجام شده و خوانندگان علاقمند برای مطالعات بیشتر می‌توانند به [۲۷]، [۲۸]، [۲۹] و [۳۰] مراجعه کنند.

در صحنه واقعی نبردهای سایبری تصمیم‌گیری‌ها بر مبنای راهبردها، دستاوردها، هزینه‌ها و اطلاعات غیرقطعی و نامشخص اتخاذ می‌شوند و به دلیل عدم وجود داده و اطلاعات کافی می‌توان از درجات باور کارشناسان برای توصیف داده‌های غیرقطعی استفاده کرد. در این پژوهش با استفاده نظریه بازی‌ها و نظریه عدم قطعیت منسوب به لیو که مبتنی بر درجه باور است به مدل‌سازی مساله تخصیص منابع در جنگ‌های سایبری می‌پردازیم.

۳- مفاهیم اولیه نظریه عدم قطعیت

در این بخش برخی از مفاهیم اساسی نظریه عدم قطعیت که در بخش‌های بعدی مورد نیاز است، بیان می‌گردد. تصمیمات واقعی معمولا در محیطی غیر قطعی اتخاذ می‌گردد. منظور از نامشخصی حادثه‌ای است که نتیجه آن در آینده برای ما مشخص می‌شود. برای مثال، قبل از پرتاب تاس نمی‌توان به‌طور دقیق پیش‌بینی کرد که چه عددی ظاهر می‌شود. بنابراین پرتاب تاس نمونه‌ای از

[1] Iwamura
[2] Ha

حوادث نامشخص است. برای مدل‌بندی نامشخصی می‌توان از نظریه‌های احتمال، مجموعه فازی و یا عدم قطعیت منسوب به لیو استفاده کرد. نظریه احتمال برای مدل‌بندی فراوانی، نظریه مجموعه فازی برای مدل‌بندی نظر کارشناسان (با استفاده از اطلاعات موجود) و نظریه عدم قطعیت لیو برای مدل‌بندی درجات باور به کار می‌روند. در واقع در صورت عدم وجود نمونه به اندازه کافی و عدم اطلاعات کافی می‌توان از درجه باور کارشناسان برای توصیف داده‌های غیرقطعی استفاده کرد. تعاریف، مفاهیم و قضایای این بخش که در بخش‌های بعدی مورد استفاده قرار خواهد گرفت، از مرجع [۳۱] برگرفته شده است. برای جزئیات بیشتر در زمینه مفاهیم پایه‌ای ریاضی مطرح شده در این بخش به کتاب‌های [۳۲]، [۳۳] و [۳۴] رجوع شود.

تعریف۱. فرض کنید Γ یک مجموعه ناتهی و L یک σ- جبر روی Γ باشد. در این صورت (Γ,L)یک فضای اندازه‌پذیر و هر عضو L یک مجموعه اندازه‌پذیر نامیده می‌شود. در نظریه عدم قطعیت هر مجموعه اندازه‌پذیر را یک پیشامد گویند.

برای ارائه یک تعریف روشن از اندازه غیرقطعی لازم است که به هر پیشامد Λ یک عدد نامنفی $M(\Lambda)$ نسبت داده شود که بیانگر احتمال وقوع آن پیشامد است.

تعریف۲. تابع ξ از فضای اندازه‌پذیر (Γ,L) به مجموعه اعداد حقیقی اندازه‌پذیر گفته می‌شود اگر برای هر مجموعه بورل B از اعداد حقیقی رابطه زیر برقرار باشد:

$$\xi^{-1}(\mathrm{B})=\{\gamma\in\Gamma:\xi(\gamma)\in B\}\in L$$

یعنی نقش معکوس مجموعه B متعلق به σ -جبر L باشد.

تعریف۳. فرض کنید (Γ,L) یک فضای اندازه‌پذیر باشد. تابع $\mathrm{M}:L\to[0,1]$ اندازه غیرقطعی نامیده می‌شود هرگاه سه اصل زیر برای آن برقرار باشد:

۱. اصل نرمال بودن: برای مجموعه مرجع Γ، $\mathrm{M}(\Gamma)=1$.

۲. اصل دوگانگی: برای هر پیشامد Λ، $\mathrm{M}(\Lambda)+\mathrm{M}(\Lambda^c)=1$.

۳. اصل زیرجمعی: برای هر دنباله شمارا از پیشامدهای Λ_1، Λ_2، ... نامساوی زیر برقرار باشد.

$$\mathrm{M}\left\{\bigcup_{i=1}^{\infty}\Lambda_i\right\}\leq\sum_{i=1}^{\infty}M\{\Lambda_i\}.$$

تعریف۴. فرض کنید Γ یک مجموعه ناتهی، L یک σ- جبر روی Γ و M یک اندازه غیرقطعی باشد. در این صورت سه تایی (Γ, L, M) یک فضای غیرقطعی نامیده می‌شود.

تعریف۵. متغیر غیرقطعی τ یک تابع اندازه‌پذیر از فضای غیرقطعی (Γ, L, M) به مجموعه اعداد حقیقی است به طوری که برای هر مجموعه بورل B از اعداد حقیقی مجموعه

$$\{\tau\in B\}=\{\gamma\in\Gamma:\tau(\gamma)\in B\}$$

یک پیشامد باشد.

اگر τ یک متغیر غیر قطعی باشد، آنگاه توزیع غیرقطعی آن به ازای هر عدد حقیقی x به صورت زیر تعریف می‌شود:

$$\Upsilon(\mathrm{x})=\mathrm{M}\{\tau\leq\mathrm{x}\}.$$

از جمله متغیرهای غیرقطعی پرکاربرد متغیرهای غیرقطعی خطی و زیگزاگ را می‌توان نام برد. متغیر غیرقطعی τ خطی نامیده می‌شود هرگاه توزیع غیرقطعی آن به صورت زیر باشد:

$$\Upsilon(\mathrm{x})=\begin{cases}0, & x\leq a,\\ (x-a)/(b-a), & a\leq x\leq b,\\ 1, & x\geq b,\end{cases}$$

و به صورت $l(a,b)$ نشان داده می‌شود که در آن $a,b\in$، و $a<b$.

تعریف۶. توزیع غیر قطعی $\Upsilon(x)$ منظم گفته می‌شود هرگاه یک تابع پیوسته نسبت به x بوده و در مجموعه $\{x\,|0<\Upsilon(x)<1\}$ اکیداً صعودی باشد و

$$\lim_{x\to-\infty}\Upsilon(x)=0,\quad \lim_{x\to+\infty}\Upsilon(x)=1.$$

تعریف۷. اگر τ یک متغیر غیرقطعی با توزیع غیرقطعی منظم $\Upsilon(x)$ باشد، آنگاه تابع معکوس $\Upsilon^{-1}(\alpha)$ توزیع غیرقطعی معکوس τ نامیده می‌شود.

به عنوان مثال توزیع غیرقطعی معکوس متغیرغیرقطعی خطی $l(a,b)$ به صورت زیر است:

$$\Upsilon^{-1}(\alpha)=(1-\alpha)a+\alpha b.$$

تعریف۸. متغیرهای غیرقطعی ξ_1، ξ_2، ...، ξ_n مستقل نامیده می‌شوند هرگاه برای مجموعه‌های بورل دلخواه B_1، B_2، ...، B_n از اعداد حقیقی رابطه زیر برقرار باشد:

$$M\left\{\prod_{i=1}^{n}(\xi_i\in B_i)\right\}=\min_{i=1,\ldots,n}M\{\xi_i\in B_i\}.$$

قضیه زیر قاعده‌ای برای تابع توزیع معکوس ترکیب متغیرهای غیرقطعی مستقل ارائه می‌کند.

قضیه۱ (لیو [۳۱] صفحه ۵۵). فرض کنید ξ_1، ξ_2، ...، ξ_n متغیرهای غیرقطعی مستقل، به ترتیب با توزیع‌های غیرقطعی منظم Υ_1، Υ_2، ...، Υ_n باشند. اگر $f(\xi_1,\xi_2,\ldots,\xi_n)$ نسبت به ξ_1، ξ_2، ...، ξ_k اکیداً صعودی و نسبت به ξ_{k+1}، ξ_{k+2}، ...، ξ_n اکیدا نزولی باشد، آنگاه توزیع غیرخطی معکوس $\xi=f(\xi_1,\xi_2,\ldots,\xi_n)$ به صورت زیر است:

$$\Upsilon^{-1}(\alpha)=f\left(\Upsilon_1^{-1}(\alpha),\Upsilon_2^{-1}(\alpha),\ldots,\Upsilon_k^{-1}(\alpha),\Upsilon_{k+1}^{-1}(1-\alpha),\ldots,\Upsilon_n^{-1}(1-\alpha)\right).$$

تصمیمات واقعی در زندگی معمولا در شرایط عدم اطمینان یا ریسک گرفته می‌شود. ریسک را می‌توان سود یا زیان غیرقطعی سرمایه‌گذاری شده تعریف کرد. آنالیز ریسک غیرقطعی ابزاری برای اندازه‌گیری ریسک با استفاده از نظریه عدم قطعیت منسوب به لیو است. یکی از روش‌های اندازه‌گیری ریسک ارزش در

معرض ریسک شرطی[1] در محیط غیرقطعی است که در ادامه تعریف آن بر اساس منابع [۳۵] و [۳۶] ارائه می‌شود.

یک سیستم معمولا شامل عوامل غیرقطعی ξ_1، ξ_2، ...، ξ_n می‌باشد که ممکن است به عنوان تقاضا، نرخ تولید، هزینه و سود در نظر گرفته شود. به طور کلی برخی ضررهای معین بستگی به این عوامل دارد که آن را می‌توان به صورت یک تابع ضرر تعریف کرد.

تعریف۹. عوامل غیرقطعی ξ_1، ξ_2، ...، ξ_n موجود در یک سیستم را در نظر بگیرید. در صورت وجود برخی ضررهای معین، تابع f تابع ضرر نامیده می‌شود هرگاه

$$f\left(\xi_1, \xi_2, ..., \xi_n\right) > 0.$$

تعریف۱۰. فرض کنید سیستم شامل عوامل غیرقطعی ξ_1، ξ_2، ...، ξ_n و تابع ضرر f باشد. به ازای هر سطح اطمینان ریسک $\alpha \in [0,1]$، ارزش در معرض ریسک شرطی (CVaR) به صورت زیر تعریف می‌شود:

$$\mathrm{CVaR}_\alpha = \frac{1}{\alpha}\int_0^\alpha \sup\{x : \mathrm{M}\{f\left(\xi_1, ..., \xi_n\right) \geq x\} \geq \beta\} d\beta.$$

قضیه۲ ([۳۵] صفحه ۹). فرض کنید سیستم شامل متغیرهای غیرقطعی مستقل ξ_1، ξ_2، ...، ξ_n، به ترتیب، با توزیع‌های غیرقطعی منظم Υ_1 ، Υ_2 ، ...، Υ_n باشند. اگر تابع ضرر $f\left(\xi_1, \xi_2, ..., \xi_n\right)$ نسبت به ξ_1، ξ_2، ...، ξ_k اکیداً صعودی و نسبت به ξ_{k+1}، ξ_{k+2}، ...، ξ_n اکیدا نزولی باشد، آنگاه

$$\mathrm{CVaR}_\alpha =$$
$$\frac{1}{\alpha}\int_0^\alpha f\left(\Upsilon_1^{-1}(1-\beta), \Upsilon_2^{-1}(1-\beta), ..., \Upsilon_k^{-1}(1-\beta), \Upsilon_{k+1}^{-1}(\beta), ..., \Upsilon_n^{-1}(\beta)\right) d\beta.$$

[1] Conditional Valu-at-Risk (CVaR)

۴- تخصیص منابع در جنگ سایبری

در ادامه به ذکر تحقیقات تامب[1] [۸]، پاروچری[2] و همکاران [۳۷] در زمینه امنیت فیزیکی سایبری پرداخته و یک سیستم امنیت سایبری را به صورت یک مدل بازی فرمول‌بندی می‌کنیم. در این مدل فرض می‌شود که $T=\{t_1,t_2,...,t_n\}$ مجموعه n هدف حساس است که در معرض خطر قرار دارند و $S=\{s_1,s_2,...,s_n\}$ منابع در دسترسی هستند که به‌واسطه آنها می‌توان اهداف مورد نظر را تحت پوشش قرار داد. به عنوان مثال در دنیای سایبر سیستم‌های متصل به اینترنت را می‌توان به عنوان اهداف در معرض خطر و زیرساخت‌های امنیتی مانند دیوارهای آتش[3] را می‌توان به عنوان منابع در نظر گرفت.

فرض کنید بردارهای $\langle a(t)\rangle$ و $\langle p(t)\rangle$ به ترتیب بیانگر راهبرد ترکیبی مهاجم و مدافع باشند بطوریکه $a(t)$ و $p(t)$ به ترتیب نشان‌دهنده احتمال حاشیه‌ای حمله به هدف t و احتمال حاشیه‌ای محافظت از هدف t هستند. در حالت کلی راهبردهای ترکیبی مدافع و مهاجم با بردار $\langle a(t),p(t)\rangle$ نشان‌داده می‌شود. بعلاوه، فرض کنید $r_d(t)$ بیانگر دستاورد مدافع در صورت پوشش دادن هدف t و $c_d(t)$ نشان‌دهنده زیان تحمیل شده در صورت پوشش ندادن هدف t باشند. همچنین، فرض کنید $r_a(t)$ نشانگر دستاورد مهاجم از حمله به هدف t در صورت پوشش داده نشدن آن و $c_a(t)$ نشان‌دهنده زیان تحمیل شده مهاجم در صورت پوشش داده شدن هدف t باشد. در صورتی که بازیکنان بر اساس بردار راهبرد $\langle a(t),p(t)\rangle$ بازی کنند، عایدی مورد انتظار بازیکن مدافع با رابطه

$$U_d(a,p)=\sum_{t\in T}a(t)\big(p(t)r_d(t)-(1-p(t))c_d(t)\big)$$

[1] Tambe
[2] Paruchuri
[3] firewall

و عایدی مورد انتظار بازیکن مهاجم با رابطه

$$U_a(a,p)=\sum_{t\in T} a(t)\big((1-p(t))r_a(t)-p(t)c_a(t)\big)$$

تعیین می‌شود. برای حالتی که بازیکنان به طور همزمان حرکت کنند، نویسندگان در [۱۲] تعادل نش بازی را بدست آوردند. اگر بازی دنباله‌ای باشد که مدافع در ابتدا حرکت کند و به یک راهبرد متعهد شود و مهاجم واکنش نشان دهد، راه حل استاندارد در این تعامل سلسله مراتبی (رهبر-پیرو)، تعادل استاکلبرگ نامیده می‌شود که در [۳۸] و [۱۶] بررسی شده است.

بازی‌های استاکلبرگ به این فرض تکیه دارند که رهبر از عایدی‌های خود و عایدی‌های پیروان خبر دارد. پیروان نه تنها باید عایدی خود را بدانند بلکه باید از راهبردی را که رهبر به آن متعهد شده است نیز مطلع باشند. در اکثر مسائل امنیت سایبری در دنیای واقعی، این فرضیات همیشه درست نیستند. برای حل این مشکل سکری[1] [۳۹] با استفاده از شبیه‌سازی تصادفی، یک مدل برنامه‌ریزی صحیح-آمیخته درجه دوم برای بازی در محیط قطعی به صورت

CRAM:
$$\max \sum_{t\in T} a(t)\big(p(t)r_d(t)-(1-p(t))c_d(t)\big)$$

$$\sum_{t\in T} p(t)\le m \qquad (1)$$

$$\sum_{t\in T} a(t)=1 \qquad (2)$$

$$u-U_a(t,p)\ge 0, \quad \forall t\in T,$$

$$u-U_a(t,p)\le (1-a(t))\Omega, \quad \forall t\in T,$$

$$p(t)\in\{0,1\}, \quad \forall t\in T, \qquad (3)$$

$$a(t)\ge 0, \quad \forall t\in T, \qquad (4)$$

$$u\in R, \qquad (5)$$

ارائه کردکه در آن

[1] Sokri

$$U_a(t,p(t)) = (1-p(t))r_a(t) - p(t)c_a(t)$$

و Ω عددی بسیار بزرگ است. اما با توجه به اینکه در مسائل امنیت سایبری بازیکنان به طور کلی قادر به ارزیابی دقیق عایدی خود و عایدی حریفان خود نیستند، ما در این مقاله بازی استاکلبرگ رهبر-پیرو فوق با پارامترهای غیرقطعی را با دو رویکرد مدل غیرقطعی با محدودیت درجه باور و مدل غیر قطعی با ارزش در معرض ریسک شرطی فرمول‌بندی کرده و برای آنها روش حل ارائه می‌کنیم.

۵- مدل تخصیص غیرقطعی با محدودیت درجه باور

در این بخش فرض می‌کنیم که پارامترهای $c_a(t)$، $r_a(t)$، $c_d(t)$ و $r_d(t)$ در مدل CRAM داده‌هایی غیرقطعی به ترتیب با توزیع غیرقطعی مستقل Υ_{ca}، Υ_{ra}، Υ_{cd} و Υ_{rd} باشند. با توجه به اینکه مقدار مینیمم تابع هدف غیرقطعی را نمی‌توان بطور مستقیم حساب کرد، ما مقدار مورد انتظار آن یعنی

$$\mathrm{E}\left(\sum_{t\in T} a(t)\left(p(t)r_d(t) - (1-p(t))c_d(t)\right)\right)$$

را بیشینه می‌کنیم. بعلاوه قیدهای غیر قطعی نیز بیانگر یک مجموعه شدنی قطعی نیستند، اما طبیعی است که این قیدها در سطوح اطمینان مختلف α_1، α_2، ...، α_p که $\alpha_j \in [0,1]$ فضای شدنی قطعی را توصیف می‌کنند. بنابراین مجموعه‌ای از قیدهای

$$M\{u - U_a(t,p(t)) \geq 0\} \geq \alpha_j, \qquad \forall t \in T,$$
$$M\{u - U_a(t,p(t)) \leq (1-a(t))\Omega\} \geq \alpha_j, \qquad \forall t \in T,$$

را به ازای سطوح اطمینان مختلف α_j خواهیم داشت. برای گرفتن تصمیمی با حداکثر ارزش مورد انتظار، با استفاده از روش برنامه‌ریزی غیرقطعی لیو [۲۴] می‌توان بر نامه‌ریزی قطعی زیر را در سطوح اطمینان مختلف α_j مختلف حل کرد.

$$\max\ E\left(\sum_{t\in T} a(t)\left(p(t)r_d(t)-(1-p(t))c_d(t)\right)\right)$$
$$M\left\{u-U_a(t,p(t))\geq 0\right\}\geq \alpha_j,\qquad \forall t\in T,$$
$$M\left\{u-U_a(t,p(t))\leq (1-a(t))\Omega\right\}\geq \alpha_j,\qquad \forall t\in T,$$
$$(1)-(4).$$

بنابراین، بردار $\langle p(t),a(t),u\rangle$ یک جواب شدنی برای مدل غیر قطعی فوق است هرگاه

$$M\left\{u-U_a(t,p(t))\geq 0\right\}\geq \alpha_j,\qquad \forall t\in T,\ j=1,...,p,$$
$$M\left\{u-U_a(t,p(t))\leq (1-a(t))\Omega\right\}\geq \alpha_j,\qquad \forall t\in T,\ j=1,...,p.$$

همچنین جواب شدنی $\langle p^*(t),a^*(t),u^*\rangle$ یک جواب بهینه برای مدل غیر قطعی فوق است هرگاه

$$\mathrm{E}\left(\sum_{t\in T} a^*(t)\left(p^*(t)r_d(t)-(1-p^*(t))c_d(t)\right)\right)$$
$$\geq \mathrm{E}\left(\sum_{t\in T} a^*(t)\left(p^*(t)r_d(t)-(1-p^*(t))c_d(t)\right)\right).$$

قضیه۳ (لیو[۳۱] صفحه ۶۹). فرض کنید تابع هدف $\mathrm{f}(\xi_1,\xi_2,...,\xi_n)$ نسبت به ξ_1، ξ_2، ...، ξ_k اکیداً صعودی و نسبت به ξ_{k+1}، ξ_{k+2}، ...، ξ_n اکیدا نزولی باشد. اگر ξ_1، ξ_2، ...، ξ_n متغیرهای غیرقطعی مستقل با توزیع‌های غیرقطعی منظم به ترتیب Υ_1، Υ_2، ...، Υ_n باشند. آنگاه تابع هدف مورد انتظار $\mathrm{E}\left(\mathrm{f}(\xi_1,\xi_2,...,\xi_n)\right)$ برابر است با

$$\int_0^1 f\left(x,\Upsilon_1^{-1}(\alpha),\Upsilon_2^{-1}(\alpha),...,\Upsilon_k^{-1}(\alpha),\Upsilon_{k+1}^{-1}(1-\alpha),...,\Upsilon_n^{-1}(1-\alpha)\right)d\alpha.$$

قضیه۴ (لیو [۳۱] صفحه ۵۹). فرض کنید تابع محدودیت $g(\xi_1,\xi_2,...,\xi_n)$ نسبت به ξ_1، ξ_2، ...، ξ_k اکیداً صعودی و نسبت به ξ_{k+1}، ξ_{k+2}، ...، ξ_n اکیدا نزولی باشد. اگر ξ_1، ξ_2، ...، ξ_n متغیرهای غیرقطعی مستقل با توزیع‌های غیرقطعی منظم Υ_1، Υ_2، ...، Υ_n باشند. آنگاه محدودیت درجه باور

$$\mathrm{M}\left\{g\left(\xi_1,\xi_2,...,\xi_n\right)\le 0\right\}\ge\alpha$$

برقرار است اگر و تنها اگر

$$g\left(x,\Upsilon_1^{-1}(\alpha),\Upsilon_2^{-1}(\alpha),...,\Upsilon_k^{-1}(\alpha),\Upsilon_{k+1}^{-1}(1-\alpha),...,\Upsilon_n^{-1}(1-\alpha)\right)\le 0.$$

با توجه به اینکه تابع

$$U_d(a,p,r_d,c_d)=\sum_{t\in T}p(t)r_d(t)-(1-p(t))c_d(t)$$

نسبت به r_d اکیداً صعودی و نسبت به c_d اکیداً نزولی است و همچنین تابع

$$U_a(t,p(t),r_a(t),c_a(t))=(1-p(t))r_a(t)-p(t)c_a(t)$$

نسبت به r_a اکیداً صعودی و نسبت به c_a اکیداً نزولی است، بر اساس قضایای ۳ و ۴ مدل غیر قطعی فوق برای یک سطح اطمینان از قبل تعیین شده α_j با مدل قطعی زیر معادل است:

$$\begin{aligned}&\max\int_0^1 U_d\left(a,p,\Upsilon_{rd}^{-1}(\alpha),\Upsilon_{cd}^{-1}(1-\alpha)\right)d\alpha\\&u-U_a\left(t,p(t),\Upsilon_{ra}^{-1}(\alpha_j),\Upsilon_{ca}^{-1}(1-\alpha_j)\right)\ge 0,\quad \forall t\in T,\\&u-U_a\left(t,p(t),\Upsilon_{ra}^{-1}(\alpha_j),\Upsilon_{ca}^{-1}(1-\alpha_j)\right)\le(1-a(t))\Omega,\quad \forall t\in T,\\&(1)-(4).\end{aligned}$$

فرض کنید پارامترهای غیر قطعی $r_d(t)$، $c_d(t)$، $c_a(t)$و $r_a(t)$ به ترتیب دارای توزیع غیرقطعی خطی $\Upsilon_{rd}(t)=l(\mu_{rd}(t),\nu_{rd}(t))$، $\Upsilon_{cd}(t)=l(\mu_{cd}(t),\nu_{cd}(t))$، $\Upsilon_{ra}(t)=l(\mu_{ra}(t),\nu_{ra}(t))$ و $\Upsilon_{ca}(t)=l(\mu_{ca}(t),\nu_{ca}(t))$ باشند. در این صورت دستگاه فوق به مدل UCRAMزیر تبدیل می‌شود:

$$\text{UCRAM:}\quad \max \sum_{t\in T} a(t)p(t)\left((\alpha-\frac{\alpha^2}{2})\mu_{rd}(t)+\frac{\alpha^2}{2}\nu_{rd}(t)\right)$$
$$-\sum_{t\in T} a(t)(1-p(t))\left(\frac{\alpha^2}{2}\mu_{cd}(t)+(\alpha-\frac{\alpha^2}{2})\nu_{cd}(t)\right)$$
$$u+(1-p_t)\left(\alpha\mu_{ra}(t)+(1-\alpha)\nu_{ra}(t)\right)$$
$$-p(t)\left((1-\alpha)\mu_{ca}(t)+\alpha\nu_{ca}(t)\right)\geq 0, \qquad \forall t\in T,$$
$$u+(1-p(t))\left(\alpha\mu_{ca}(t)+(1-\alpha)\nu_{ca}(t)\right)$$
$$-p(t)\left((1-\alpha)\mu_{ra}(t)+\alpha\nu_{ra}(t)\right)\leq (1-a(t))\Omega, \qquad \forall t\in T,$$
$$(1)-(4).$$

حال، برای مدل غیرقطعی ارائه شده یک مثال عددی ارائه می‌کنیم.

مثال۱: امروزه در اغلب تسلیحات نظامی از وسایل الکترونیکی استفاده می‌شود. به عنوان نمونه می‌توان از بکارگیری رادارها برای آشکارسازی و مکانیابی سکوها و مراکز حساس دشمن و استفاده از ادوات الکترونیکی برای هدایت موشکها نام برد. در مقابل نیز از تجهیزات الکترونیکی برای فریب رادارها و ایجاد اختلال در سیگنال‌های دریافتی آنها استفاده می‌شود. اما تامین تجهیزات الکترونیکی اختلال راداری برای پوشش دادن تمامی مراکز حساس و حیاتی نظامی و غیرنظامی کشور با توجه به هزینه بالای آنها مکان پذیر نیست. در این زمینه یک موقعیت نبرد سایبری را در نظر می‌گیریم که در آن ۶ مرکز حساس نظامی وجود دارند که بصورت بالقوه می‌توانند مورد هدف حملات موشکی دشمن قرار بگیرند و ۲ منبع اختلال راداری وجود دارند و با هر منبع تنها می‌توان یکی از اهداف را پوشش داد. برای هر هدف دو نوع عایدی وجود دارد: عایدی مدافع و عایدی مهاجم. هر عایدی هم تابعی از پاداش و هزینه است. زمانی که هدفی مورد حمله واقع می‌شود، اگر مدافع آن را پوشش داده باشد پاداشی دریافت کرده و در صورت پوشش ندادن آن متحمل زیان خواهد شد. همچنین اگر هدفی توسط مدافع پوشش داده شود، با حمله مهاجم به آن هدف، مهاجم فریب

خورده و متحمل هزینه خواهد شد. ولی اگر هدف توسط مدافع پوشش داده نشود، مهاجم از حمله به آن سود خواهد برد. فرض می‌کنیم که ورودی‌های مسئله که شامل هزینه و سود مهاجم از هر هدف است پارامترهایی غیرقطعی با توزیع‌های خطی مطابق با جدول ۱ باشند. با اجرای مدل UCRAM برای سطوح اطمینان مختلف $\alpha = 0.1, 0.3, 0.5, 0.7, 0.9$ راهبردهای بهینه حمله و دفاع برای مهاجم و مدافع در جدول ۲ آورده شده است.

داده‌های ورودی مثال ۱ جدول ۱.

مهاجم		مدافع		
هزینه $l(\mu_{ca}(t), v_{ca}(t))$	سود $l(\mu_{ra}(t), v_{ra}(t))$	هزینه $l(\mu_{cd}(t), v_{cd}(t))$	سود $l(\mu_{rd}(t), v_{rd}(t))$	هدف
$l(12,25)$	$l(9,18)$	$l(6,14)$	$l(1,17)$	۱
$l(5,13)$	$l(6,18)$	$l(5,15)$	$l(8,28)$	۲
$l(5,13)$	$l(22,36)$	$l(10,27)$	$l(16,28)$	۳
$l(32,42)$	$l(2,15)$	$l(15,35)$	$l(5,20)$	۴
$l(13,27)$	$l(2,12)$	$l(3,12)$	$l(19,23)$	5
$l(9,26)$	$l(12,15)$	$l(16,36)$	$l(6,15)$	6

برای سطوح اطمینان مختلف UCRAM نتایج حاصل از اجرای مدل جدول ۲.

α	دستاورد مدافع U_d	راهبرد بهینه مهاجم $(a(1),...,a(6))$	راهبردهای بهینه مدافع $(p(1),...,p(6))$
0.1	0.16	$(0,1,0,0,0,0)$	$(0,1,0,0,1,0)$
0.3	0.84	$(0,1,0,0,0,0)$	$(1,1,0,0,0,0)$
0.5	2.00	$(0,1,0,0,0,0)$	$(0,1,0,0,1,0)$
0.7	3.15	$(0,0,0,0,1,0)$	$(0,0,0,0,1,0)$
0.9	6.57	$(0,0,1,0,0,0)$	$(0,1,1,0,0,0)$

۶- مدل تخصیص منابع غیرقطعی با هدف ارزش در معرض ریسک شرطی

در این قسمت حالت غیرقطعی مدل CRAM را به شکل دیگری بررسی می‌کنیم. با در نظر گرفتن ارزش در معرض ریسک شرطی تابع هدف مدل غیرقطعی CRAM به ازای سطوح اطمینان ریسک $\alpha \in [0,1]$ و امید ریاضی (مقدار مورد انتظار) محدودیت‌های غیرقطعی مساله یک مدل جدید با هدف ماکسیمم‌سازی ارزش در معرض ریسک شرطی و برحسب محدودیتهای مقادیر مورد انتظار به صورت

$$\max CV_{\alpha}R_{\alpha}\left(\sum_{t\in T} a_t\left(p(t)r_d(t)-(1-p(t))c_d(t)\right)\right),$$
$$E\{u-U_a(t,p)\}\geq 0, \qquad \forall t\in T,$$
$$E\{u-U_a(t,p)\}\leq \mathrm{E}\{(1-a_t)\Omega\}, \qquad \forall t\in T,$$
$$(1)-(4).$$

بدست می‌آوریم. توجه داشته باشید که در این مدل تنها پارامترهای تابع هدف در سطح اطمینان α در نظر گرفته شده در حالی که در مدل UCRAM همه پارامترهای وردی مساله در سطح اطمینان α در نظر گرفته شده است. بر اساس قضایای 2 و3 مدل فوق را می‌توان به صورت مدل CVRCRAM زیر بازنویسی کرد:

$$\text{CVRCRAM}: \max \sum_{t\in T} a(t)p(t)\left((\frac{\alpha}{2})\mu_{rd}(t)+(1-\frac{\alpha}{2})\nu_{rd}(t)\right)$$
$$-\sum_{t\in T} a(t)(1-p(t))\left((1-\frac{\alpha}{2})\mu_{cd}(t)+(\frac{\alpha}{2})\nu_{cd}(t)\right),$$
$$u-p(t)\left(\frac{\mu_{ra}(t)}{2}+\nu_{ra}(t)\right)$$
$$+(1-p(t))\left(\mu_{ca}(t)+\frac{\nu_{ca}(t)}{2}\right)\geq 0, \qquad \forall t\in T,$$
$$u-p(t)\left(\frac{\mu_{ra}(t)}{2}+\nu_{ra}(t)\right)$$
$$+(1-p(t))\left(\mu_{ca}(t)+\frac{\nu_{ca}(t)}{2}\right)-(1-a(t))\Omega\leq 0, \qquad \forall t\in T,$$
$$(1)-(4).$$

حال برای مدل غیرقطعی ارزش در معرض ریسک شرطی CVRCRAM یک مثال عددی ارائه می‌کنیم.

مثال۲ : یک جنگ سایبری با اطلاعات مثال ۱، با ۴ هدف و ۳ منبع را در نظر بگیرید. نتایج حاصل از اجرای مدل غیرقطعی ارزش در معرض ریسک شرطی CVRCRAM را برای سطوح اطمینان مختلف به صورت جدول ۳ می‌باشد.

برای سطوح اطمینان مختلف CVRCRAM نتایج حاصل از اجرای مدل جدول ۳.

α	$CV_\alpha R_\alpha$	راهبرد بهینه مهاجم $(a(1),...,a(6))$	راهبرد بهینه مدافع $(p(1),...,p(6))$
0.1	34.40	$(0,1,1,1,0,1)$	$(0,0,1,1,0,0)$
0.3	29.20	$(0,1,1,1,0,1)$	$(0,0,1,1,0,0)$
0.5	28.00	$(1,1,1,0,0,1)$	$(1,0,1,0,0,0)$
0.7	23.20	$(1,1,1,0,0,1)$	$(1,0,1,0,0,0)$
0.9	18.40	$(1,1,1,0,0,1)$	$(1,0,1,0,0,0)$

۷- بحث و نتیجه‌گیری

در این مقاله مسئله تخصیص بهینه منابع که مسئله‌ای حیاتی در جنگ‌های سایبری است مورد بررسی قرار گرفت و با استفاده از نظریه بازی به صورت یک مدل بازی استاکلبرگ فرمول‌بندی شد. با توجه به اینکه در مسائل امنیت سایبری بازیکنان به طور کلی قادر به ارزیابی دقیق هزینه‌ها، دستاوردها و صدمات خود و دشمن نیستند، مدل بازی تحت مطالعه در محیط غیرقطعی بررسی شده و با دو رویکرد مدل غیرقطعی با محدودیت درجه باور و مدل غیر قطعی با ارزش در معرض ریسک شرطی فرمول‌بندی مجدد شده و برای آنها روش حل ارائه گردید. همچنین رویکردهای پیشنهاد شده روی یک مثال عددی پیاده‌سازی شد.

در پایان پیشنهاد میشود که از رویکردهای بهینه سازی غیرقطعی ارائه شده در این مقاله در توسعه مدل‌های بهینه‌سازی در سایر حوزهای بازی جنگ و جنگ سایبری استفاده شود. بعلاوه توسعه مدل‌های بازی با اضافه کردن قواعدی مانند تکرار بازی، وجود مهاجمین متعدد، امکان تشکیل ائتلاف و....، متناسب با سناریوهای نبرد در دنیای واقعی برای شبیه‌سازی نبرد سایبری پیشنهاد می‌گردد.

مراجع

[۱] M. Bernier, S. Leblanc, B. Morton, E. Filiol, and R. Erra, "Metrics framework of cyber operations on command and control," in Proceedings of the 11th European Conference on Information Warfare and Security, 2012: Laval, France. Academic Publishing International Ltd, pp. 53-62.

[۲] R. Aslanoğlu and S. Tekir, "Recent cyberwar spectrum and its analysis," 2012.

[۳] C. Czosseck and K. Podins, "A vulnerability-based model of cyber weapons and its implications for cyber conflict," International Journal of Cyber Warfare and Terrorism (IJCWT), vol. 2, no. 1, pp. 14-26, 2012.

[٤] K. Ziolkowski, "Computer network operations and the law of armed conflict," Mil. L. & L. War Rev., vol. 49, p. 47, 2010.

[٥] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," Nist special publication, vol. 800, no. 30, pp. 800-30, 2002.

[٦] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in 2010 43rd Hawaii International Conference on System Sciences, 2010: IEEE, pp. 1-10.

[۷] C. Kiekintveld, V. Lisý, and R. Píbil, "Game-theoretic foundations for the strategic use of honeypots in network security," in Cyber warfare: Springer, 2015, pp. 81-101.

[۸] M. Tambe, Security and game theory: algorithms, deployed systems, lessons learned. Cambridge university press, 2011.

[۹] V. M. Bier, L. A. Cox, and M. N. Azaiez, "Why both game theory and reliability theory are important in defending infrastructure against intelligent attacks," in Game theoretic risk analysis of security threats: Springer, 2009, pp. 1-11.

[۱۰] J. Acquaviva, M. Mahon, B. Einfalt, and T. LaPorta, "Optimal Cyber-Defense Strategies for Advanced Persistent Threats: A Game Theoretical Analysis," in 2 ۱۱۷IEEE 36th Symposium on Reliable Distributed Systems (SRDS), 2017: IEEE, pp. 204-213.

[۱۱] F. Moisan and C. Gonzalez, "Security under uncertainty: adaptive attackers are more challenging to human defenders than random attackers," Frontiers in psychology, vol. 8, p. 982, 2017.

[۱۲] S. Conti, "Algorithms for finding leader-follower equilibrium with multiple followers," 2014.

[۱۳] M. Jain et al., "Software assistants for randomized patrol planning for the lax airport police and the federal air marshal service," Interfaces, vol. 40, no. 4, pp. 267-290, 2010.

[۱٤] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordóñez, and M. Tambe, "Computing optimal randomized resource allocations for massive security games," in Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1, 2009, pp. 689-696.

[۱٥] M. Bloem, T. Alpcan, and T. Basar, "Intrusion response as a resource allocation problem," in Proceedings of the 45th IEEE Conference on Decision and Control, 2006: IEEE, pp. 6283-6288.

[۱٦] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Game theory meets information security management," in IFIP International Information Security Conference, 2014: Springer, pp. 15-29.

[۱۷] M. N. Azaiez and V. M. Bier, "Optimal resource allocation for security in reliability systems," European Journal of Operational Research, vol. 181, no. 2, pp. 773-786, 2007.

[۱۸] M. Van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "FlipIt: The game of “stealthy takeover”," Journal of Cryptology, vol. 26, no. 4, pp. 655-713, 2013.

[۱۹] K. D. Bowers et al., "Defending against the unknown enemy: Applying FlipIt to system security," in International Conference on Decision and Game Theory for Security, 2012: Springer, pp. 248-263.

[۲۰] B. Liu, "Uncertainty theory," in Uncertainty theory: Springer, 2007, pp. 205-234.

[۲۱] B. Liu, "Some research problems in uncertainty theory," Journal of Uncertain systems, vol. 3, no. 1, pp. 3-10, 2009.

[۲۲] Z. Peng and K. Iwamura, "A sufficient and necessary condition of uncertainty distribution," Journal of Interdisciplinary Mathematics, vol. 13, no. 3, pp. 277-285, 2010.

[۲۳] B. Liu, "Toward uncertain finance theory," Journal of Uncertainty Analysis and Applications, vol. 1, no. 1, p. 1, 2013.

[۲۴] B. Liu, Uncertainty theory: A branch of mathematics for modeling human uncertainty. Berlin: Springer-Verlag, 2010.

[۲۵] Y. Liu and M. Ha, "Expected value of function of uncertain variables," Journal of uncertain Systems, vol. 4, no. 3, pp. 181-186, 201.۰

[۲۶] B. Liu and B. Liu, Theory and practice of uncertain programming. Springer, 2009.

[۲۷] H. Bigdeli, H. Hassanpour, and J. Tayyebi, "Multiobjective security game with fuzzy payoffs," Iranian Journal of Fuzzy Systems, vol. 16, no. 1, pp. 89-101, 2019.

[۲۸] H. Bigdeli and H. Hassanpour, "A satisfactory strategy of multiobjective two person matrix games with fuzzy payoffs," Iranian Journal of Fuzzy Systems, vol. 13, no. 4, pp. 17-33, 2016.

[۲۹] H. Bigdeli, H. Hassanpour, and J. Tayyebi, "Optimistic and Pessimistic Solutions of Single and Multi-Objective Matrix Games with Fuzzy Payoffs and Analysis of Some Military Cases."

[۳۰] H. Bigdeli, H. Hassanpour, and J. Tayyebi, "Constrained bimatrix games with fuzzy goals and its application in nuclear negotiations," Iranian Journal of Numerical Analysis and Optimization, vol. 8, no. 1, pp. 81-110, 2018.

[۳۱] B. Liu, Uncertainty theory 4ed. Springer-Verlag Berlin Heidelberg, 2015.

[۳۲] W. Arveson, An invitation to C*-algebras. Springer Science & Business Media, ۲۱۱۲.

[۳۳] R. M. Dudley, Real analysis and probability. CRC Press, 2018.

[۳٤] H. L. Royden and P. Fitzpatrick, Real analysis. Macmillan New York, 1988.

[۳٥] J. Peng, "Risk metrics of loss function for uncertain system," Fuzzy Optimization and Decision Making, vol. 12, no. 1, pp. 53-64, 2013.

[۳٦] B. Liu, "Uncertain risk analysis and uncertain reliability analysis," Journal of Uncertain Systems, vol. 4, no. 3, pp. 163-170, 2010.

[۳۷] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus, "Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games," in Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems-Volume 2, 2008: International Foundation for Autonomous Agents and Multiagent Systems, pp. 895-902.

[۳۸] A. Sinha, T. H. Nguyen, D. Kar, M. Brown, M. Tambe, and A. X. Jiang, "From physical security to cybersecurity," Journal of Cybersecurity, vol. 1, no. 1, pp. 19-35, 2015.

[۳۹] A. Sokri, "Optimal resource allocation in cyber-security: A game theoretic approach," Procedia computer science, vol. 134, pp. 283-288, 2018.