Electronic & Cyber Defense
Vol. 14, No.1, 2026 (Serial No. 35) .pp.21-34
ISSN: 2322-4347, E-ISSN: 2980-8979

Application of Game Theory for Optimal Strategy Selection in Cyber Attacks and Defense

M.S. Alamdari [1*]

[1] PhD in Mathematics and Head of the Mathematics Department, Supreme National Defense University, Tehran,. Iran (*Correspondence: *m.s.alamdari69@gmail.com*)

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 01 January 2026
Revised: 15 February 2026
Accepted: 27 February 2026
Available online: 09 April 2026

Keywords:
Game theory
Cyber defense
Cyber attack
Cyber security
Simulation

ABSTRACT

In today's world, the expansion of cyberspace and growing societal dependence on information systems have turned cyber threats into a serious challenge for national security. This paper presents a mathematical model based on game theory to analyze and simulate optimal strategies in cyber attacks and defenses. First, game theory is introduced as an analytical tool in cyberspace, and its significance in determining the best strategies for both attackers and defenders is examined. Next, a mathematical model is defined in which both parties aim to maximize their own payoff while minimizing damages caused by attacks through the selection of various strategies. Subsequently, several cyber scenarios—including DDoS attacks, phishing, and sophisticated malware—are investigated via MATLAB simulations, and the impact of varying levels of attack and defense is analyzed. The results demonstrate that optimal defensive strategies can significantly reduce the success rate of cyber attacks and enhance cybersecurity. Finally, the proposed model serves as an effective tool to assist cybersecurity policymakers in developing efficient strategies to counter cyber threats.

Cite this article: Alamdari, M.S. (2026). Application of Game Theory for Optimal Strategy Selection in Cyber Attacks and Defense. *Electronic and Cyber Defense*,14(1),21-34.2026.

DOI: https://dor.isc.ac/dor/20.1001.1.23224347.1405.14.1.2.4

Publisher: Imam Hossein University.

«پدافند الکترونیک و سایبری»
سال چهاردهم، شماره ۱، بهار ۱۴۰۵؛ ص ۳۴-۲۱
شاپا الکترونیکی: ۸۹۷۹-۲۹۸۰ شاپا چاپی: ۴۳۴۷-۲۳۲۲

به‌کارگیری نظریه بازی‌ها برای انتخاب راهبردهای بهینه در حملات و دفاع‌های سایبری

محمد سعید علمداری[۱]

[۱] دکتری ریاضی و دبیر گروه ریاضی ،دانشگاه عالی دفاع ملی، تهران، ایران .(نویسنده مسئول: *m.s.alamdari69@gmail.com*)

چکیده

در دنیای امروز، گسترش فضای سایبری و افزایش وابستگی جوامع به سیستم‌های اطلاعاتی، تهدیدات سایبری را به یک چالش جدی برای امنیت ملی کشورها تبدیل کرده است. در این مقاله، یک مدل ریاضی مبتنی بر نظریه بازی‌ها برای تحلیل و شبیه‌سازی راهبردهای بهینه در حملات و دفاع‌های سایبری ارائه شده است. ابتدا نظریه بازی‌ها به‌عنوان یک ابزار تحلیلی در فضای سایبری معرفی شده و اهمیت آن در تعیین بهترین راهبردها برای مهاجمان و مدافعان بررسی شده است. سپس، یک مدل ریاضی تعریف شده که در آن طرفین با انتخاب راهبردهای مختلف به دنبال بیشینه‌سازی سود خود و کاهش خسارات ناشی از حملات هستند. در ادامه، با استفاده از شبیه‌سازی در MATLAB ، چندین سناریوی سایبری شامل حملات DDoS، فیشینگ و بدافزارهای پیچیده مورد بررسی قرار گرفته و تأثیر سطوح مختلف حمله و دفاع تحلیل شده است. نتایج نشان می‌دهد که استراتژی‌های بهینه دفاعی می‌توانند میزان موفقیت حملات سایبری را کاهش داده و امنیت سایبری را بهبود بخشند. در نهایت، مدل پیشنهادی به‌عنوان ابزاری کارآمد به سیاست‌گذاران امنیت سایبری در تدوین راهبردهای کارآمد برای مقابله با تهدیدات سایبری کمک کند.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۴/۱۰/۱۱

بازنگری: ۱۴۰۴/۱۱/۲۶

پذیرش: ۱۴۰۴/۱۲/۰۸

ارائه آنلاین: ۱۴۰۵/۰۱/۲۰

کلید واژه ها:

نظریه بازی

دفاع سایبری

حمله سایبری

امنیت سایبری

شبیه‌سازی

استناد: علمداری، محمد سعید. (۱۴۰۵). به‌کارگیری نظریه بازی‌ها برای انتخاب راهبردهای بهینه در حملات و دفاع‌های سایبری. *پدافند الکترونیکی و سایبری*، ۱۴(۱)، ۳۴-۲۱. DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1405.14.1.2.4

ناشر: دانشگاه جامع امام حسین(ع).

۱. مقدمه

در دنیای امروز، پیشرفت‌های چشمگیر فناوری و گسترش سریع فضای سایبر، تأثیر عمیقی بر فضای فیزیکی گذاشته و موجب کاهش وابستگی به زمان و مکان شده است. فضای سایبر به‌عنوان یک محیط دیجیتال جهانی، به‌سرعت به بستری برای برقراری ارتباطات، تعاملات اقتصادی، اجتماعی و سیاسی تبدیل گردیده است. این روند منجر به وابستگی فزاینده جوامع به فضای سایبر و سیستم‌های اطلاعاتی شده، اما این وابستگی با خود تهدیدات و چالش‌های جدیدی در حوزه امنیت به همراه داشته است. به‌ویژه تهدیدات سایبری که به طور فزاینده‌ای به‌عنوان تهدیدی جدی برای امنیت اطلاعات و زیرساخت‌های حیاتی در سطح جهانی مطرح شده‌اند.

یکی از مهم‌ترین چالش‌ها در دنیای سایبر، سوءاستفاده از سیستم‌های اطلاعاتی برای مقاصد مختلف اقتصادی، اجتماعی، سیاسی یا ایدئولوژیک است. این نوع حملات نه‌تنها می‌تواند به خسارت‌های مالی و ازدست‌رفتن اطلاعات حساس منجر شود، بلکه تهدیدی جدی برای امنیت ملی و ثبات کشورهای مختلف به وجود می‌آورد. این وضعیت خطرناک ممکن است به ازدست‌رفتن جان انسان‌ها، آسیب به زیرساخت‌ها و تهدید امنیت ملی منتهی گردد. ازاین‌رو، ضروری است که این تهدیدات به طور دقیق تحلیل شده و راهبردهایی برای مقابله با آن‌ها تدوین گردد.

به‌ویژه باتوجه‌به اینکه حملات سایبری معمولاً علیه زیرساخت‌های حیاتی کشورها صورت می‌گیرد، شناسایی و به‌کارگیری راهبردهای مناسب و مؤثر در این زمینه امری ضروری است. یکی از روش‌های مهم برای شبیه‌سازی و تحلیل تهدیدات و راهبردهای دفاعی، استفاده از نظریه بازی‌هاست که می‌تواند به طور مؤثر در تحلیل راهبردهای حمله و دفاع در فضای سایبر کمک نماید [۱].

نظریه بازی‌ها به‌عنوان یکی از ابزارهای ریاضی در تجزیه‌وتحلیل راهبرد، به‌ویژه در زمینه امنیت سایبری و مدل‌سازی تهدیدات سایبری، اهمیت زیادی دارد. این نظریه به‌ویژه در شرایطی که دو طرف با اهداف مختلف (حمله‌کننده و مدافع) در حال تعامل هستند، بسیار کارآمد است.

در این زمینه، بازی‌ها می‌توانند تعاملات میان مهاجم و مدافع را مدل‌سازی کرده و راه‌حل‌هایی برای بهینه‌سازی راهبردهای طرفین ارائه دهند. به‌ویژه، بازی‌های راهبرد در تعیین بهترین راهبردها و پیش‌بینی نتایج در مقابل راهبردهای مختلف اهمیت دارند؛ بنابراین، مدل‌سازی با استفاده از نظریه بازی‌ها، ابزاری اساسی برای شبیه‌سازی سناریوهای سایبری و بررسی اقدامات مهاجم و مدافع به شمار می‌آید.

در زمینه‌های نظامی، گسترش استفاده از فناوری اطلاعات، به‌ویژه در بخش‌های دفاعی، چهره میدان جنگ را دگرگون ساخته است.

درگذشته، جنگ‌ها عمدتاً در محیط‌های فیزیکی و با حضور نیروهای انسانی انجام می‌شد، اما امروزه باتوجه‌به پیشرفت‌های فناوری، جنگ‌ها و تهدیدات سایبری، فضای جدیدی برای نبردهای آنلاین ایجاد کرده‌اند.

یکی از نمونه‌های بارز این نوع تهدیدات، بازی‌های راهبرد میان مهاجم و مدافع برای دسترسی به سیستم‌ها و رایانه‌ها از طریق اینترنت است. نظریه بازی‌ها به‌عنوان ابزاری برای شبیه‌سازی این نوع حملات و دفاع‌ها، می‌تواند به تحلیل و شبیه‌سازی راهبردهای مختلف کمک کند و به تحلیلگران این امکان را می‌دهد که به پیش‌بینی و انتخاب راهبردهای بهینه برای مقابله با حملات سایبری بپردازند.

در همین راستا، مطالعات زیادی نشان داده‌اند که استفاده از نظریه بازی‌ها می‌تواند به‌عنوان یک ابزار قدرتمند برای تحلیل و پیش‌بینی رفتار مهاجمان و مدافعان در فضای سایبر باشد [۲]. شناسایی الگو، شناسایی چهره و پردازش سیگنال به‌عنوان ابزارهای پیشرفته در تحلیل تهدیدات سایبری و امنیتی، در طراحی راهبردهای نظامی مدرن نقش حیاتی دارند و به‌عنوان یکی از پیشرفته‌ترین ابزارهای شناسایی افراد در مناطق جنگی یا هنگام شناسایی دشمن در عملیات نظامی به طراحان راهبردهای دفاعی کمک می‌کنند تا تصمیمات هوشمندانه‌تری در مواجهه با تهدیدات اتخاذ نمایند و از بروز خطرات امنیتی جلوگیری کنند [۳-۶].

در این مقاله، باتوجه‌به اهمیت بالای موضوعات مطرح‌شده، هدف اصلی آن تحلیل و مدل‌سازی ریاضی حمله و دفاع سایبری است. این مطالعه تلاش دارد تا با استفاده از مدل‌های ریاضی و نظریه بازی‌ها، سودها و ضررهای حاصل از حملات و دفاع‌های سایبری را شبیه‌سازی کرده و راهبردهای بهینه برای کشورهای مختلف را تعیین کند. به این منظور، در بخش دوم روش تحقیق ارائه خواهد شد. در بخش سوم مقاله، مفاهیم پایه‌ای نظریه بازی‌ها در فضای سایبر توضیح داده خواهد شد.

در بخش چهارم، سناریویی ارائه خواهد شد که در آن دو کشور Aو B به مدل‌سازی قابلیت‌های هجومی و دفاعی خود پرداخته و راهبردهای مختلف را ارزیابی می‌کنند و همچنین با استفاده از یک مدل ریاضی، ماتریس بازدهی محاسبه‌شده و راهبردهای بهینه برای هر دو کشور شناسایی خواهند شد.

سپس در بخش پنجم، برتری مدل ارائه شده در مقاله نسبت به سایر روش‌ها تشریح خواهد شد. در نهایت، نتیجه‌گیری و چند موضوع جهت پیشبرد مقاله بابت پژوهش‌های آینده پیشنهاد می‌شود. این تحقیق به طور ویژه به اهمیت استفاده

از نظریه بازی‌ها در تحلیل راهبردهای سایبری و شبیه‌سازی رفتار طرفین درگیر در یک حمله سایبری می‌پردازد.

۲. روش تحقیق

در این مقاله، به طور عمده هدف تحلیل و مدل‌سازی ریاضی با استفاده از نظریه بازی‌هاست تا راهبردهای بهینه برای مهاجم و مدافع در شرایط حملات سایبری شبیه‌سازی گردد. در این راستا، یک مدل بازی راهبرد دونفره به‌منظور بررسی تعاملات میان مهاجم و مدافع در فضای سایبری پیشنهاد شده است.

این مدل بر اساس اهداف و انگیزه‌های هر یک از طرفین (مهاجم و مدافع) و با درنظرگرفتن اثربخشی ضد حملات، طراحی شده است. مراحل تحقیق به شرح زیر است.

۱) مدل‌سازی بازی راهبرد: در ابتدا، یک مدل بازی راهبرد دو بازیکن (مهاجم و مدافع) تعریف می‌شود که در آن هر یک از طرفین باید راهبردهایی را انتخاب کنند که منجر به بیشترین منفعت برای خود و کمترین ضرر برای طرف مقابل شود. این مدل با استفاده از داده‌های واقعی و ارزیابی‌های مبتنی بر تجربه در زمینه حملات و دفاع‌های سایبری طراحی می‌گردد.

۲) استفاده از ماتریس‌های هزینه - فایده: برای تجزیه‌وتحلیل بهتر هزینه‌ها و فایده‌های انتخاب‌های راهبرد مختلف، از ماتریس‌های هزینه - فایده و ماتریس‌های احتمال استفاده می‌شود. این ماتریس‌ها اطلاعاتی در خصوص احتمال موفقیت هر راهبرد و هزینه‌های آن به دست می‌دهند و کمک می‌کنند تا طرفین بازی (مهاجم و مدافع) راهبردهای خود را بر اساس آن تنظیم نمایند. این روش همچنین به تحلیل سناریوهای "چه می‌شد اگر" می‌پردازد که به طرفین امکان می‌دهد اثرات تغییر راهبردها را پیش‌بینی کنند.

۳) تحلیل با استفاده از تعادل نش: پس از تعریف راهبردهای مختلف، از مفهوم تعادل نش برای پیداکردن نقاط بهینه استفاده می‌شود. در این مرحله، تعادل نش به‌عنوان یک نقطه راهبرد در نظر گرفته می‌شود که در آن هیچ‌یک از طرفین نمی‌توانند با تغییر راهبرد خود به منفعت بیشتری دست یابند. به‌عبارت‌دیگر، این مدل به تحلیل و شبیه‌سازی راهبردهایی می‌پردازد که در آن هر دو طرف بهینه‌ترین انتخاب‌ها را انجام می‌دهند.

۴) نتایج و پیشنهادها: پس از تحلیل راهبردهای مختلف و یافتن تعادل‌ها، با استفاده از مدل‌های ریاضی، راهبردهای بهینه تعیین می‌شوند. این راهبردها به طور خاص در مورد حملات سایبری و دفاع‌های مربوط به آن‌ها طراحی می‌شوند و به کمک آن‌ها، تصمیم‌گیری‌های مؤثری در مورد نحوه مقابله با تهدیدات سایبری صورت می‌گیرد.

در نهایت، این مدل‌ها می‌توانند برای بهبود امنیت در فضای سایبر و اتخاذ تصمیمات بهینه در شرایط بحرانی جنگ‌های سایبری مورد استفاده قرار گیرند.

۳. نظریه بازی و مفاهیم پایه مربوطه

هر رخدادی که شامل تقابل یا مبارزه باشد، می‌تواند به‌عنوان یک بازی تعریف شود [۷]. نظریه بازی‌ها به تحلیل این بازی‌ها پرداخته و مسائل تصمیم‌گیری را در شرایطی که چندین تصمیم‌گیرنده با یکدیگر تعامل دارند، بررسی می‌کند.

این نظریه به‌ویژه در شرایط خصمانه مفید است، جایی که دو یا چند عامل اهداف متضادی دارند [۸-۹]. به‌عنوان یک چارچوب در مدل‌سازی موقعیت‌هایی که در آن بیش از یک تصمیم‌گیرنده (بازیکن) وجود دارد، نظریه بازی‌ها در بسیاری از رشته‌ها استفاده می‌شود [۱۰]. نظریه بازی‌ها مسئله تصمیم‌گیری را به‌صورت یک بازی فرمول‌بندی می‌کند که در آن دو یا چند بازیکن تصمیماتی می‌گیرند که بر تصمیمات یکدیگر تأثیر می‌گذارد [11]. بازی به‌صورت مجموعه‌ای از راهبردها برای هر بازیکن تعریف می‌شود. فرض بر این است که بازیکنان منطقی هستند و هدف آنها حداکثرسازی بازدهی (سودمندی) حاصل از مشارکت در بازی است.

همه بازیکنان انتظار دارند سایر بازیکنان نیز منطقی عمل کنند. منطقی‌بودن به‌طورکلی به معنای داشتن اطلاعات کامل و دقیق درباره راهبردهای یکدیگر است. در شرایط اطلاعات ناقص که بازیکنان از راهبردهای حریف آگاه نیستند، می‌توان بازی‌هایی را به‌صورت بیزی مدل‌سازی کرد که بر اساس توزیع احتمالی اقدامات در مجموعه راهبردها طراحی می‌شود [۱۲].

سه نوع تابع بازدهی وجود دارد: بازی‌های مجموع صفر، مجموع ثابت و مجموع نا صفر. در بازی‌های مجموع صفر، سود یک بازیکن معادل زیان بازیکن دیگر است؛ هر آنچه یک بازیکن می‌برد، دیگری باید ببازد. در بازی‌های مجموع ثابت، تنها یک بازیکن در هر لحظه بازدهی غیرصفر خواهد داشت و در بازی‌های مجموع نا صفر هیچ محدودیتی برای ساختار نتایج اعمال نمی‌شود [۱۳]. فرضیه‌های بازی مجموع صفر در جنگ سایبری منطقی به نظر نمی‌رسند، زیرا بازیگران دولتی اهداف و اولویت‌های متفاوتی دارند [۱۴]. در این زمینه، مدل مجموع نا صفر به‌عنوان واقعی‌ترین مدل در جنگ اطلاعاتی پیشنهاد می‌شود [۱۵].

هدف بازی یافتن یک راه‌حل متعادل است؛ یعنی یافتن بهترین نتیجه یا بازدهی برای بازیکنان که تصمیمات سایر بازیکنان را در نظر می‌گیرد. در اصطلاح کلاسیک بهینه‌سازی، این راه‌حل محلی بهینه برای مسئله هر بازیکن است. یکی از

ساده‌ترین راه‌حل‌های بازی، راه‌حل مینی مکس[1] است که حداکثر زیان موردانتظار یک بازیکن را حداقل می‌کند.

تعادل نش زمانی حاصل می‌شود که یک راهبرد بهینه منحصربه‌فرد برای هر بازیکن وجود داشته باشد که با حرکت حریف تطابق داشته باشد [۱۶]. اگر احتمال انتخاب یک راهبرد برای یک سناریوی خاص برابر با یک باشد، آن راهبرد خالص نامیده می‌شود. اما در بیشتر موارد، حریفان اطلاعات کاملی ندارند یا در ماهیت بازی تردید دارند و راهبرد خالص مشخص نیست. در این حالت، از یک مدل تصادفی به نام راهبرد مختلط استفاده می‌شود که در آن احتمال‌های مرتبط با راهبردهای خاص تعریف می‌شوند.

بازی‌ها می‌توانند تعاملی یا غیرتعاملی باشند. بازی‌های تعاملی معمولاً زمانی مدل‌سازی می‌شوند که مکانیزم‌هایی برای اجرای مجموعه رفتارهای خاص (منابع) وجود داشته باشد. اگر راهبردهای تعاملی در جنگ سایبری امکان‌پذیر باشد، می‌توان بازی‌های غیرتعاملی را مدل‌سازی کرد. بر اساس نتایج حاصل از مدل‌های غیرتعاملی، می‌توان توصیه‌های سیاستی برای کاهش مشکلات جنگ سایبری ارائه کرد. بازی‌ها به دو نوع استاتیک یا پویا تقسیم می‌شوند.

در بازی‌های استاتیک، تصمیمات همه بازیکنان به طور هم‌زمان و بدون اطلاع از تصمیمات سایر بازیکنان گرفته می‌شود. بازی‌های پویا شامل مجموعه‌ای از بازی‌ها هستند که در آن راهبردها بر اساس انتخاب‌های قبلی بازیکنان بازبینی می‌شوند.

در زمینه جنگ سایبری، بازی‌های پویا می‌توانند زمانی وجود داشته باشند که تاکتیک‌های حمله شامل مراحل و آزمایش‌های متعدد باشند. همچنین، مکانیزم‌های دفاعی می‌توانند با شناسایی حملات قبلی برای محافظت از سیستم‌ها، رفتار آینده را تحت‌تأثیر قرار دهند [۱۷]. بااین‌حال، فرض استاتیک بودن بازی‌ها نیز معقول است؛ زیرا بسیاری از حملات سایبری بدون آگاهی از حمله رخ می‌دهند. در این مطالعه، از مدل استاتیک برای سناریو استفاده خواهد شد و از فرمول‌بندی ریاضی برای حل بازی‌های $2 \times n$ استفاده خواهد شد [۸].

۴. سناریوی حمله و دفاع سایبری بین دو کشور

الگوریتم‌هایی[2] که امکان اتخاذ تصمیمات امنیت سایبری را بر پایه اصولی مستحکم و مدل‌های بازی که منابع امنیتی را میان وظایف مختلف توزیع می‌کنند، فراهم می‌آورند، توسعه یافته‌اند [۱۸]. در این بخش، با طراحی سناریویی متفاوت از بازی، نخست باید ماتریس بازدهی محاسبه شود.

فرض کنید که دو کشور A و B، درگیر نبردی سایبری هستند. کشور A، با در اختیار داشتن دو سلاح سایبری، در پی وارد‌ساختن آسیب به اهداف کشور B است، مشروط بر آنکه A نقش مهاجم را بر عهده داشته و B به‌عنوان مدافع عمل کند. برای این منظور، چهار شبکه در دسترس قرار دارد که حملات از طریق آن‌ها انجام خواهد شد.

کشور A این امکان را دارد که هر دو سلاح سایبری خود را به‌سوی اهداف B چه از طریق شبکه‌های یکسان و چه از مسیرهای متفاوت ارسال کند.در مقابل، کشور Bنیز به چهار سیستم دفاع سایبری مجهز است که مأموریت آن‌ها محافظت از اهداف در برابر حملات کشور A خواهد بود. این سامانه‌های دفاعی قادرند سلاح‌های سایبری را شناسایی کرده و مانع از بهره‌برداری از شبکه‌ای شوند که در آن مستقر هستند.

درصورتی‌که یک سیستم دفاعی در شبکه‌ای مستقر شود که مورد حمله قرار می‌گیرد، تنها یکی از سلاح‌های سایبری که از آن شبکه بهره می‌برد، مسدود خواهد شد، و چنانچه دو سلاح سایبری از یک شبکه استفاده کنند، سامانه دفاعی حاضر در آن تنها قادر به مسدودکردن یکی از آن‌ها خواهد بود، درحالی‌که سلاح دیگر به هدف اصابت می‌کند. اما اگر در شبکه‌ای که مورد حمله قرار گرفته، دو سیستم دفاعی حضور داشته باشند، هر دو حمله دفع شده و هدف موردنظر محافظت خواهد شد.

تابع سود، بسته به راهبردهایی که هر یک از دو کشور A و B برمی‌گزینند، دستخوش تغییر می‌شود. هدف آن است که با درنظرگرفتن انتخاب‌های متنوع هر کشور، میزان موفقیت یا ناکامی حملات در فضای سایبری سنجیده شود. این موفقیت‌ها به‌صورت مقادیر عددی، نظیر ۰ و ۱، برای هر بازیکن مشخص خواهد شد.

تابع سود کشور A، میزان موفقیت حملات آن را نشان می‌دهد و با $g^A(I_A\ II_B)$ نمایش داده می‌شود. ازسوی‌دیگر، تابع سود کشور B، وابسته به عملکرد سیستم‌های دفاعی آن در شناسایی و مسدودسازی حملات کشور A است و با $g^B(I_A\ II_B)$ نشان داده می‌شود.

راهبردهای کشور A عبارت‌اند از:

I_1: حملات از طریق شبکه‌های مختلف انجام می‌شود.

I_2: حملات از طریق شبکه‌های یکسان صورت می‌گیرد.

راهبردهای کشور B عبارت‌اند از:

II_1: یک سیستم دفاعی در هر شبکه مستقر می‌شود.

II_2: دو سیستم دفاعی در دو شبکه مستقر شده و دو شبکه دیگر بدون دفاع باقی می‌مانند.

[1]. MiniMax
[2]. Algorithms

II_3: دو سیستم دفاعی در یک شبکه قرار گرفته، یک سیستم دفاعی در دو شبکه دیگر مستقر می‌شود و یک شبکه بدون دفاع باقی می‌ماند.

II_4: سه سیستم دفاعی در یک شبکه مستقر شده، یک سیستم دفاعی در شبکه‌ای دیگر قرار می‌گیرد و دو شبکه دیگر بدون دفاع خواهند بود.

II_5: چهار سیستم دفاعی در یک شبکه مستقر شده و سه شبکه دیگر بدون محافظت باقی می‌مانند.

۴-۱. حالت اول

ابتدا لازم است بازدهی محاسبه شود، یعنی g_{1j} که در آن $j = 1,2,3,4,5$ خواهد بود، در شرایطی که کشور A با راهبرد I_1حمله می‌کند.

گام اول: درصورتی‌که کشور Aاز راهبرد I_1استفاده کند، سلاح‌های سایبری از مسیرهای مختلف ارسال خواهد شد. ازآنجاکه در مجموع چهار شبکه وجود دارد، حمله با استفاده از این شبکه‌های مجزا صورت می‌گیرد و بر اساس (۱)، این حمله در شش روش مختلف انجام خواهد شد.

$$\binom{4}{2} = \frac{4!}{2!2!} = 6 \qquad (۱)$$

گام دوم: اگر کشور B با راهبرد II_2دفاع کند، ازآنجاکه یک سیستم دفاعی در هر شبکه مستقر خواهد شد، دو سلاح سایبری در هر یک از شش گزینه انتخابی کشور A مسدود می‌شوند؛ بنابراین، هدف محافظت خواهد شد. در این حالت بنا بر رابطه (۲)، سود کشور Aبرابر با صفر خواهد بود، چرا که تمامی حملات مسدود خواهند شد.

$$g_{11}^A = g^A(I_1\ II_1) = \frac{0}{6} + \frac{0}{6} + \frac{0}{6} + \frac{0}{6} + \frac{0}{6} + \frac{0}{6} = 0 \qquad (۲)$$

گام سوم: اگر کشورB با راهبرد II_3دفاع کند، دو سیستم دفاعی در یک شبکه مستقر خواهد شد، یک سیستم دفاعی در دو شبکه دیگر قرار خواهد گرفت و یک شبکه بدون دفاع باقی خواهد ماند. ازآنجاکه هر حمله سایبری از شبکه‌های مختلف انجام می‌شود، هدف در سه گزینه از شش گزینه انتخابی کشور A به هدف خواهد رسید و در سه گزینه دیگر هدف محافظت خواهد شد. در این حالت بنا بر رابطه (۳)، سود کشورA برابر با $\frac{1}{2}$ خواهد بود، چرا که در سه گزینه حملات به هدف اصابت کرده‌اند.

$$g_{13}^A = g^A(I_1\ I_3) = \frac{0}{6} + \frac{0}{6} + \frac{0}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2} \qquad (۳)$$

گام چهارم: اگر کشور Bبا راهبرد II_4دفاع کند، دو شبکه دیگر بدون دفاع باقی خواهند ماند؛ درحالی‌که یکی از این دو شبکه دارای سه سیستم دفاعی خواهد بود و دیگری یک سیستم دفاعی خواهد داشت. ازآنجاکه حملات سایبری از شبکه‌های مختلف انجام می‌شوند، هدف تنها در یکی از شش گزینه ممکن از کشور A محافظت خواهد شد و در هر یک از گزینه‌های دیگر هدف به دست خواهد آمد. در این حالت بنا بر رابطه (۴)، سود کشور Aبرابر با $\frac{5}{6}$ خواهد بود، چرا که در پنج گزینه حملات به هدف اصابت کرده‌اند.

$$g_{14}^A = g^A(I_1\ I_4) = \frac{0}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{5}{6} \qquad (۴)$$

گام پنجم: اگر کشور Bبا راهبرد II_5دفاع کند، چهار سیستم دفاعی در یک شبکه مستقر خواهند شد و سه شبکه دیگر بدون دفاع باقی خواهند ماند. ازآنجاکه هر حمله از شبکه‌های مختلف انجام می‌شود، در هر یک از شش گزینه کشور A، حمله به هدف خواهد رسید. در این حالت بنا بر رابطه (۵)، سود کشور A برابر با یک خواهد بود، زیرا در تمامی گزینه‌ها حملات به هدف اصابت کرده‌اند.

$$g_{15}^A = g^A(I_1\ I_5) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = 1 \qquad (۵)$$

۴-۲. حالت دوم

ابتدا بایستی بازدهی محاسبه شود، یعنی g_{2j}که در آن $j = 1,2,3,4,5$ خواهد بود، زمانی که کشور A با راهبرد I_2 حمله می‌کند.

گام اول: اگر کشور Aبا راهبرد I_2حمله کند، ازآنجاکه هر دو سلاح سایبری را از همان شبکه ارسال می‌کند و چهار شبکه وجود دارد، لذا کشور A قادر خواهد بود بر اساس (۶) حملات سایبری را در چهار روش مختلف انجام دهد.

$$\binom{4}{1} = \frac{4!}{3!1!} = 4 \qquad (۶)$$

گام دوم: اگر کشور B با راهبرد II_1 دفاع کند، هدف در هر چهار گزینه از حملات کشور A به دست می‌آید، زیرا یک سیستم دفاعی روی هر شبکه قرار دارد. بازدهی به‌صورت (۷) خواهد بود.

$$g_{21}^A = g^A(I_2\ II_1) = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1 \qquad (۷)$$

گام سوم: اگر کشور Bبا راهبرد II_2 دفاع کند، در دو گزینه از چهار گزینه حملات کشور A، هدف به دست خواهد آمد و در دو گزینه دیگر حملات مسدود خواهند شد. در این حالت بنا بر رابطه (۸) بازدهی کشور A برابر با $\frac{1}{2}$ خواهد بود، زیرا در دو گزینه حملات به هدف اصابت کرده‌اند.

$$g_{22}^A = g^A(I_2\ II_2) = \frac{0}{4} + \frac{0}{4} + \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \qquad (۸)$$

گام چهارم: اگر کشور Bبا راهبرد II_3دفاع کند، در سه گزینه از چهار گزینه حملات کشور A به هدف خواهد رسید و در یک گزینه حمله مسدود خواهد شد. در این حالت بنا بر رابطه (۹) بازدهی کشور A برابر با $\frac{3}{4}$ خواهد بود، زیرا در سه گزینه حملات به هدف اصابت کرده‌اند.

$$g_{23}^A = g^A(I_2\ II_3) = \frac{0}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4} \qquad (۹)$$

گام پنجم: اگر کشور B با راهبرد II_4 دفاع کند، در یک گزینه از چهار گزینه حملات کشور A مسدود خواهد شد و در سه گزینه دیگر، حداقل یک حمله به هدف خواهد رسید. در این حالت بنا بر رابطه (۱۰) بازدهی کشور A برابر با $\frac{3}{4}$ خواهد بود، زیرا در سه گزینه حملات به هدف اصابت کرده‌اند.

$$g_{24}^{A} = g^{A}(I_2\ II_4) = \frac{0}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4} = \frac{3}{4} \qquad (۱۰)$$

گام ششم: اگر کشور B با راهبرد II_5 دفاع کند، در یک گزینه از چهار گزینه حملات کشور A مسدود خواهد شد و حداقل یکی از گزینه‌های دیگر به هدف خواهد رسید. در این حالت بنا بر رابطه (۱۱) بازدهی کشور A برابر با $\frac{3}{4}$ خواهد بود، زیرا در یکی از گزینه‌ها حمله مسدود شده و در باقی گزینه‌ها حداقل یک حمله به هدف اصابت کرده است.

$$g_{25}^{A} = g^{A}(I_2\ II_5) = \frac{0}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4} = \frac{3}{4} \qquad (۱۱)$$

بنابراین، تمامی بازدهی‌های این سناریوی جنگ سایبری g_{ij} که در آن $i = 1,2$ و $j = 1,2,3,4,5$ محاسبه شده‌اند. در نتیجه، ماتریس بازدهی این بازی به شکل (۱۲) خواهد بود.

$$G = \begin{bmatrix} 0 & 5/6 & 1/2 & 5/6 & 1 \\ 1 & 1/2 & 3/4 & 3/4 & 3/4 \end{bmatrix}_{2\times5} \qquad (۱۲)$$

۴-۳. تحلیل ماتریس بازدهی

برای ساده‌سازی ماتریس بازدهی (۱۲)، این کاربین راهبردهای I_j با مقادیر مشابه انجام خواهد شد. ازآنجاکه $II_4 \geq II_5$ است، می‌توان راهبرد II_5 را حذف کرد و در نتیجه ماتریس بازدهی G_1 به شکل (۱۳) به دست خواهد آمد.

$$G_1 = \begin{bmatrix} 0 & 5/6 & 1/2 & 5/6 \\ 1 & 1/2 & 3/4 & 3/4 \end{bmatrix}_{2\times4} \qquad (۱۳)$$

ازآنجاکه $II_3 \geq II_4$ در ماتریس بازدهی G_1 است، اگر راهبرد II_4 حذف شود، در نتیجه ماتریس بازدهی G_2 به شکل (۱۴) به دست خواهد آمد و دیگر قابل ساده‌سازی نخواهد بود.

$$G_2 = \begin{bmatrix} 0 & 5/6 & 1/2 \\ 1 & 1/2 & 3/4 \end{bmatrix}_{2\times3} \qquad (۱۴)$$

حال بازدهی‌های φ برای راهبرد ترکیبی کشور A محاسبه می‌شود.

$$x = (x, 1-x) \in x_2\ ,\ x \in [0,1] \qquad (۱۵)$$

راهبرد (۱۵) و راهبرد خالص کشور B به نام II_j که $j = 1,2,3$ بایستی به‌صورت $\varphi_j(x) = g(x, II_j)$ محاسبه شود که در روابط (۱۶) تا (۱۸) به نمایش درآمده‌اند.

$$\varphi_1(x) = g(x, II_1) = 0.x + 1.(1-x) = 1-x \qquad (۱۶)$$

$$\varphi_2(x) = g(x, II_2) = \frac{5}{6}.x + \frac{1}{2}.(1-x) = \frac{1}{2}+\frac{1}{3}x \qquad (۱۷)$$

$$\varphi_3(x) = g(x, II_3) = \frac{1}{2}.x + \frac{3}{4}.(1-x) = \frac{3}{4}-\frac{1}{4}x \qquad (۱۸)$$

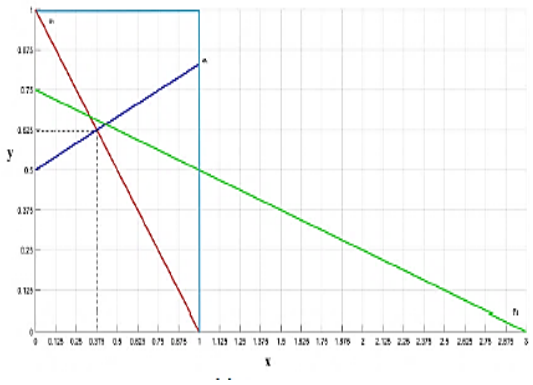
گام اول: توابع $\varphi_j(.): [0,1] \to \mathbb{R}$ که $j = 1,2,3$ هستند.

$$\varphi_1 = Y = 1-x \qquad (۱۹)$$

$$\varphi_2 = Y = \frac{1}{2}+\frac{1}{3}x \qquad (۲۰)$$

$$\varphi_3 = Y = \frac{3}{4}-\frac{1}{4}x \qquad (۲۱)$$

گراف توابع (۱۹) تا (۲۱) در شکل ۱ نمایش داده شده‌اند.



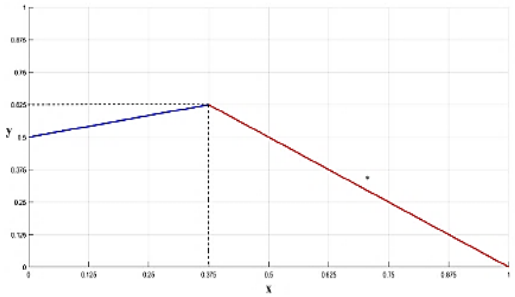
شکل (۱). نمودار توابع $\varphi_j(.)$

گام دوم: نمودار توابع $\psi(.): [0,1] \to \mathbb{R}$ رسم می‌شوند. این توابع به‌صورت $\psi(x) = min_{j=1,2,3}\ \varphi_j(x)$ بوده و به فرم (۲۲) و (۲۳) تعریف می‌شوند:

$$\psi(x) = \begin{cases} \varphi_2(x), & x \in \left[0, \frac{3}{8}\right] \\ \varphi_1(x), & x \in \left(\frac{3}{8}, 1\right] \end{cases} \qquad (۲۲)$$

$$\psi(x) = \begin{cases} \frac{1}{2}+\frac{1}{3}x, & x \leq \frac{3}{8} \\ 1-x, & x > \frac{3}{8} \end{cases} \qquad (۲۳)$$

نمودار تابع $\psi(x)$ به‌صورت یک خط شکسته است که در شکل (۲) نشان‌داده‌شده است.



شکل (2). نمودار تابع $\psi(x)$

گام سوم: با استفاده از نمودار تابع در شکل (۲)، بیشترین مقدار تابع $\psi(.): [0,1] \to \mathbb{R}$ محاسبه می‌شود؛ بنابراین، ابتدا مقدار بیشینه این تابع از روی نمودار استخراج می‌شود.

$$V = max_{x\in[0,1]}\psi(x) \quad (۲۴)$$

این مقدار برابر $y = \frac{5}{8}$ و به‌ازای $x = \frac{3}{8}$ برقرار است.

گام چهارم: بیشترین مقدار تابع $\psi(x)$ در بازه $[0,1]$ به دست می‌آید و لذا نقطه $X^* = (\frac{3}{8}, \frac{5}{8})$ راهبرد بهینه کشور A است.

گام پنجم: راهبردهای بهینه کشور B، با استفاده از شکل (۲) به‌صورت (۲۵) خواهد بود.

$$g(x^*, II_1) = g(x^*, II_2) = \frac{5}{8} \quad (۲۵)$$

بنابراین، راهبردهای II_1 و II_2 به‌عنوان راهبردهای لازم برای کشور B در نظر گرفته می‌شوند، درحالی‌که راهبرد II_3 به‌عنوان راهبرد غیرضروری محسوب می‌شوند. در این حالت، راهبرد ترکیبی بهینه کشور B به‌صورت (۲۶) خواهد بود.

$$Y^* = (y_*, 1-y_*, 0) \quad (۲۶)$$

همچنین، چون راهبرد بهینه کشور A در نقطه $X^* = (\frac{3}{8}, \frac{5}{8})$ به دست می‌آید. راهبردهای لازم کشور A برابر I_1 و I_2 خواهد بود. بنا بر $V = \frac{5}{8}, g(I_1, y^*) = \frac{5}{8}, g(I_2, y^*) = \frac{5}{8}$ داریم:

$$g(I_1, y^*) = 0.y_* + \frac{5}{6}(1-y_*) + \frac{1}{2}.0 = \frac{5}{6} - \frac{5}{6}y_* \quad (۲۷)$$

$$g(I_2, y^*) = 1.y_* + \frac{1}{2}(1-y_*) + \frac{3}{4}.0 = \frac{1}{2} + \frac{1}{2}y_* \quad (۲۸)$$

$$\frac{5}{6} - \frac{5}{6}y_* = \frac{5}{8} \quad (۲۹)$$

$$\frac{1}{2} + \frac{1}{2}y_* = \frac{5}{8} \quad (۳۰)$$

بر اساس معادلات (۲۷) تا (۳۰) مقدار $y_* = \frac{1}{4}$ بوده و پس از جای‌گذاری در رابطه (۲۶)، راهبرد ترکیبی به فرم (۳۱) است.

$$Y^* = (\frac{1}{4}, \frac{3}{4}, 0) \quad (۳۱)$$

به‌عنوان راهبرد بهینه کشور B در ماتریس بازدهی G_2 در نظر گرفته می‌شود؛ بنابراین، سه‌تایی (۳۲) به‌عنوان راه‌حل بازی در ماتریس بازدهی G_2 به دست می‌آید که همان راه‌حل ماتریس بازدهی G نیز خواهد بود.

$$(X^*, Y^*, V) = \left((\frac{3}{8}, \frac{5}{8}), (\frac{1}{4}, \frac{3}{4}, 0), \frac{5}{8}\right) \quad (۳۲)$$

۴-۴. نمونه کاربردی و مدل ریاضی پیشنهادی

در این بخش، یک نمونه کاربردی از مدل جنگ سایبری بین دو کشور Aو Bمورد بررسی قرار می‌گیرد. فرض شود که این دو کشور در یک محیط سایبری با یکدیگر در حال رقابت هستند و هدف هر یک از آن‌ها کسب بیشترین سود از طریق حملات سایبری و دفاع‌ها است. کشور Aبه مدت ۳۰۰ حمله با راهبرد I_1و ۵۰۰ حمله با راهبرد I_2 به اهداف کشور B حمله خواهد کرد. به‌عبارت‌دیگر، در ۳۰۰ حمله از ۸۰۰ حمله، سلاح‌های سایبری خود را از شبکه‌های مختلف به سمت اهداف کشور B ارسال خواهد کرد و در ۵۰۰ حمله از همان شبکه استفاده خواهد کرد. کشور Bنیز ۲۰۰ بار با راهبرد II_1و ۶۰۰ بار با راهبرد II_2 از خود دفاع خواهد کرد. به‌عبارت‌دیگر، کشور Bتلاش خواهد کرد تا حملات را با قراردادن یک سیستم دفاعی بر روی هر شبکه ۲۰۰ بار در برابر ۸۰۰ حمله متوقف کند و دو سیستم دفاعی را بر روی هر دو شبکه قرار دهد و دو شبکه دیگر را باز بگذارد. کشورهای مهاجم و راهبردها برای ۸۰۰ حمله در جدول ۱ نشان‌داده‌شده است.

جدول (۱). کشورهای مهاجم و راهبردها

راهبردها	I_1	I_2	II_1	II_2
کشور A	۳۰۰	۵۰۰	---	---
کشور B	---	---	۲۰۰	۶۰۰

بر اساس این جدول، زوج‌های احتمالی حمله و دفاع به شرح زیر خواهند بود:

حمله با راهبردI_1 و دفاع با راهبرد II_1

حمله با راهبرد I_1 و دفاع با راهبرد II_2

حمله با راهبرد I_2 و دفاع با راهبرد II_1

حمله با راهبرد I_2 و دفاع با راهبرد II_2

این ترکیب‌ها نشان‌دهنده تعاملات مختلف میان راهبردهای حمله کشور Aو دفاع کشور Bهستند که در هر یک از ۸۰۰ حمله به طور متفاوت اجرا خواهند شد و به فرم (۳۳) هستند.

$$\{(I_1, II_1), (I_1, II_2), (I_2, II_1), (I_2, II_2)\} \quad (۳۳)$$

حالت اول: زمانی که کشور A با ارسال سلاح‌های سایبری از شبکه‌های مختلف، ۳۰۰ مرتبه حمله می‌کند و کشور Bبا قراردادن یک سیستم دفاعی در هر شبکه، ۲۰۰ مرتبه از این حملات جلوگیری می‌کند. به‌عبارت‌دیگر، در این حالت، کشور Bبا استقرار یک سیستم دفاعی در هر یک از چهار شبکه، قادر خواهد بود تا ۲۰۰ حمله از مجموع ۳۰۰ حمله کشور Aرا مسدود کند و ۱۰۰ حمله باقی‌مانده به اهداف کشور Bخواهد رسید.

حالت دوم: زمانی که کشور A با ارسال سلاح‌های سایبری از شبکه‌های مختلف، ۳۰۰ مرتبه حمله می‌کند و کشور B با قراردادن دو سیستم دفاعی در دو شبکه و باز گذاشتن دو شبکه دیگر، ۶۰۰ مرتبه از این حملات جلوگیری می‌کند.

در این حالت، کشور B قادر خواهد بود تا از ۶۰۰ حمله کشور Aکه به طور هم‌زمان از دو شبکه مختلف ارسال می‌شود، دفاع کند. به‌این‌ترتیب، از مجموع ۳۰۰ حمله از

شبکه‌های مختلف، دو سوم از آن‌ها مسدود خواهد شد و یک‌سوم باقی‌مانده به اهداف کشور B خواهد رسید.

حالت سوم: زمانی که کشور A با ارسال سلاح‌های سایبری از همان شبکه‌ها ۵۰۰ مرتبه حمله می‌کند و کشور B با قراردادن یک سیستم دفاعی در هر شبکه، ۲۰۰ مرتبه از این حملات جلوگیری می‌کند. در این حالت، کشور B با استقرار یک سیستم دفاعی در هر یک از چهار شبکه، قادر خواهد بود تا ۲۰۰ حمله از مجموع ۵۰۰ حمله کشور A را مسدود کند؛ بنابراین، ۲۰۰ حمله از این تعداد به اهداف کشور B نخواهد رسید و ۳۰۰ حمله باقی‌مانده به هدف خواهد رسید.

حالت چهارم: زمانی که کشور A با ارسال سلاح‌های سایبری از همان شبکه‌ها، ۵۰۰ مرتبه حمله می‌کند، کشور B با قراردادن دو سیستم دفاعی در هر دو شبکه از این حملات، ۶۰۰ مرتبه جلوگیری می‌کند و دو شبکه دیگر را باز می‌گذارد.

در این حالت، کشور B قادر خواهد بود تا از ۶۰۰ حمله کشور A که به طور هم‌زمان از دو شبکه مختلف ارسال می‌شود، دفاع کند. به‌این‌ترتیب، از مجموع ۵۰۰ حمله از همان شبکه‌ها، دو سوم از آن‌ها مسدود خواهد شد و یک‌سوم باقی‌مانده به اهداف کشور B خواهد رسید.

در مجموع این موارد، کشور A در ۵۰۰ حمله موفق بود، درحالی‌که کشور B در ۳۰۰ حمله موفق به مسدودکردن حملات شد. به‌عبارت‌دیگر، از مجموع ۸۰۰ حمله، کشور A در ۵۰۰ مورد به هدف خود رسید و کشور B موفق شد ۳۰۰ مرتبه حملات را مسدود کند.

۵-۴. مدل ریاضی پیشنهادی برای رابطه سود و زیان

راهبرد ترکیبی کشور A به فرم (۱۶) و راهبرد ترکیبی B به فرم (۱۷) در نظر گرفته می‌شود. معادله‌ای که سود کشور A و زیان کشور B را بیان می‌کند از حاصل‌ضرب معادلات (۱۶) و (۱۷) به فرم (۳۴) به دست می‌آید که یک تابع بسته است.

$$F(x,y) = 6y^2 - 2x^2 + 4xy - 9y - 3 \qquad (۳۴)$$

در این حالت، $x,y \in [0,1]$ بوده و معادله (۳۴) رابطه سود و زیان را بیان می‌کند که در آن سود کشور A حداکثر و زیان کشور B حداقل است. اکنون، بررسی می‌شود که کدام یک از جفت‌های حمله و دفاع معادله (۳۳)، با مدل ریاضی (۳۴) بهینه خواهند بود. اگر مقادیر $\{F(1,1), F(1,2), F(2,1), F(2,2)\}$ محاسبه شوند، آنگاه $F = \{-5, -8, 8, 7\}$ به دست می‌آید که حداکثر مقدار F برابر با ۸ و متناظر با راهبرد ترکیبی (I_2, II_1) است و از طرفی حداقل مقدار F برابر با ۵- خواهد بود که متناظر با راهبرد ترکیبی (I_1, II_1) است؛ لذا راهبردهای بهینه این سناریو برابر $\{(I_1, II_1), \{(I_2, II_1)\}$ خواهند بود.

در ادامه به توسعه مدل ریاضی مبتنی بر نظریه بازی برای تحلیل حملات و دفاع‌های سایبری در سه سطح استراتژی غیرفعال، ضعیف یا قوی پرداخته می‌شود. این مدل به حل مسئله در مقیاس بزرگ شامل ۲۰ مهاجم و ۲۰ مدافع می‌پردازد که در محاسبات آن هزینه‌های حمله و دفاع لحاظ شده تا تحلیل تصمیم‌گیری واقع‌گرایانه‌تر گردد.

برای یافتن بهینه‌ترین راهبُردها، تعادل نش محاسبه و تحلیل نتایج از طریق نمودارهای MATLAB انجام می‌شود.

۵. تعمیم مدل ریاضی ارائه شده

مدل پیشنهادی از یک تابع هدف بهینه‌سازی شده استفاده می‌کند که تأثیر حملات و دفاع‌ها را بر سود نهایی مهاجم و مدافع تعیین می‌کند. این تابع در فرم توسعه بافته به‌صورت زیر تعریف می‌شود:

$$F_{\text{حمله}} = 6\sum Y^2 - 2\sum X^2 + 4\sum XY - 9\sum Y - C_{\text{حمله}} \qquad (۳۵)$$

$$F_{\text{دفاع}} = -C_{\text{دفاع}} - F_{\text{حمله}} \qquad (۳۶)$$

که در آن:

X استراتژی‌های مهاجمین و برداری از مقادیر ۰، ۱ یا ۲ است که به ترتیب استراتژی غیرفعال، حمله ضعیف، حمله قوی است.

Y استراتژی‌های مدافعین و برداری از مقادیر ۰، ۱ یا ۲ است که به ترتیب استراتژی غیرفعال، دفاع ضعیف، دفاع قوی است.

$C_{\text{حمله}}$ مجموع هزینه‌های استراتژی‌های مهاجمین است.

$C_{\text{دفاع}}$ مجموع هزینه‌های استراتژی‌های مدافعین است.

ضرایب ۶ و ۲- بیانگر وزن تأثیر حملات و دفاع‌ها بر سود نهایی است و ضریب ۴ نشان‌دهنده تأثیر تقابل استراتژی مهاجم و مدافع بر سود طرفین است.

مدل پیشنهادی از روش‌های زیر برای حل مسئله استفاده می‌کند:

هر مهاجم و مدافع به طور تصادفی یکی از سه استراتژی ممکن را انتخاب می‌کند. باتوجه‌به استراتژی انتخابی هر بازیکن، مجموع هزینه‌های حمله و دفاع محاسبه می‌شود و در نهایت با استفاده از نظریه بازی و تعادل نش، میزان سود هر بازیکن تعیین می‌شود و بهترین راهبُردها مشخص می‌گردند.

نتایج در قالب نمودارهای MATLAB تحلیل می‌شوند تا تأثیر راهبُردها بر سود و هزینه‌های نهایی مشخص گردد. مدل ارائه‌شده، تحلیل ریاضی از حملات و دفاع‌های سایبری را در مقیاس بزرگ ارائه می‌دهد که محاسبه تعادل نش و هزینه‌های حمله/دفاع باعث افزایش دقت و کاربردپذیری آن می‌شود. در ادامه برای استفاده از این مدل در تحلیل حملات سایبری واقعی و طراحی بهترین استراتژی‌های

دفاعی، چندین سناریوی عملیاتی تعریف و مدل پیشنهادی در هر یک از این سناریوها بررسی شده است.

سناریو اول) حمله DDoS و دفاع مبتنی بر فایروال: در این سناریو، یک سازمان در معرض حملات DDoS قرار دارد. مهاجمین قصد دارند با ارسال حجم بالای درخواست‌ها، سرورهای سازمان را از دسترس خارج کنند.

در مقابل، تیم امنیتی سازمان تلاش می‌کند با استفاده از فایروال‌ها و سیستم‌های کاهش ترافیک مخرب از این حملات جلوگیری کند. هر مهاجم می‌تواند یکی از سه سطح حمله را انتخاب کند.

$X = 0$: غیرفعال (بدون حمله)

$X = 1$: حمله ضعیف (ارسال درخواست‌های محدود)

$X = 2$: حمله قوی (ارسال تعداد بسیار زیاد درخواست‌ها)

در مقابل، هر مدافع یکی از سه سطح دفاع را انتخاب می‌کند:

$Y = 0$: غیرفعال (بدون فایروال یا دفاعی ضعیف)

$Y = 1$: حمله ضعیف (فایروال پایه با فیلتر محدود)

$Y = 2$: حمله قوی (سیستم تشخیص نفوذ IDS و مدیریت پیشرفته ترافیک)

فرض می‌شود که بیست مهاجم و بیست مدافع به‌صورت تصادفی استراتژی‌های خود را به شرح جدول (۲) انتخاب کرده‌اند و برای هر سطحی از حمله و دفاع، هزینه‌ای مطابق جدول (۳) در نظر گرفته می‌شود.

جدول (۲). استراتژی‌های بیست مهاجم و بیست مدافع

استراتژی‌های بیست مهاجم (X)									
۲	۱	۲	۰	۱	۲	۰	۱	۲	
۰	۱	۲	۱	۲	۲	۱	۰	۲	۱
استراتژی‌های بیست مدافع (Y)									
۱	۲	۱	۰	۲	۰	۲	۱	۲	۱
۰	۲	۱	۰	۲	۱	۲	۰	۲	۱

جدول (۳). هزینه حمله و دفاع سناریوی اول در سه سطح مختلف

سطح	هزینه حمله ($C_{\text{حمله}}$)	هزینه دفاع ($C_{\text{دفاع}}$)
۰ (غیرفعال)	۰	۰
۱ (ضعیف)	۵۰	۷۰
۲ (قوی)	۱۵۰	۲۰۰

مطابق جداول (۲) و (۳) هزینه حمله و دفاع برابر است با:

$$C_{\text{حمله}} = (4 \times 0) + (7 \times 50) + (9 \times 150) = 1700$$

$$C_{\text{دفاع}} = (5 \times 0) + (7 \times 70) + (8 \times 200) = 2090$$

طبق روابط (۳۵) و (۳۶) سود مهاجمین و مدافعین برابر است با:

$$F_{\text{حمله}} = 6\sum Y^2 - 2\sum X^2 + 4\sum XY - 9\sum Y - 1700 = -1631$$
$$F_{\text{دفاع}} = -C_{\text{دفاع}} - F_{\text{حمله}} = -2090 - (-1631) = -459$$

در نهایت، مدافعین موفق به دفع حملات شدند؛ اما هزینه دفاع بالابود. مهاجمین تلاش کردند با حملات قوی سرورها را از دسترس خارج کنند؛ اما به دلیل دفاع مناسب، موفق نشدند. مدل نشان می‌دهد که دفاع قوی می‌تواند حملات را دفع کند، اما در صورت کاهش هزینه‌های دفاع، امکان شکست وجود دارد لذا می‌توان با استفاده از تحلیل هوشمند، نقاطی را یافت که هزینه دفاع کاهش یابد بدون اینکه امنیت سازمان به خطر بیفتد.

سناریو دوم حمله فیشینگ و دفاع مبتنی بر آموزش کاربران: در این سناریو، بیست مهاجم تلاش می‌کنند با ارسال ایمیل‌های فیشینگ، کاربران یک سازمان را فریب داده و اطلاعات حساس آن‌ها را سرقت کنند. در مقابل، بیست مدافع (مسئولان امنیت سایبری سازمان) سعی دارند با آموزش کاربران و استفاده از فیلترهای هوشمند، احتمال موفقیت حملات را کاهش دهند. هدف این تحلیل، بررسی تأثیر سطح آموزش و مقابله با حملات فیشینگ با کمترین هزینه است. هر مهاجم می‌تواند یکی از سه سطح حمله را انتخاب کند.

$X = 0$: غیرفعال (بدون حمله)

$X = 1$: حمله فیشینگ ساده (ایمیل عمومی با لینک آلوده)

$X = 2$: حمله فیشینگ پیشرفته (ایمیل شخصی‌سازی‌شده، مهندسی اجتماعی، صفحات جعلی حرفه‌ای)

در مقابل، هر مدافع یکی از سه سطح دفاع را انتخاب می‌کند:

$Y = 0$: بدون آموزش و فیلتر (کاربران در برابر فیشینگ آسیب‌پذیرند)

$Y = 1$: آموزش پایه و فیلتر ساده (اطلاع‌رسانی اولیه، فیلترهای استاندارد ایمیل)

$Y = 2$: آموزش پیشرفته و فیلتر هوشمند (شبیه‌سازی حملات فیشینگ، استفاده از یادگیری ماشین برای شناسایی ایمیل‌های مشکوک)

جدول (۴). هزینه حمله و دفاع سناریوی دوم در سه سطح مختلف

سطح	هزینه حمله ($C_{\text{حمله}}$)	هزینه دفاع ($C_{\text{دفاع}}$)
۰ (بدون فعالیت)	۰	۰
۱ (حمله ساده / آموزش پایه)	۳۰	۵۰
۲ (حمله / آموزش پیشرفته)	۱۲۰	۱۵۰

مطابق جداول (2) و (4) هزینه حمله و دفاع برابر است با:

$$C_{\text{حمله}} = (4 \times 0) + (7 \times 30) + (9 \times 120) = 1290$$

$$C_{\text{دفاع}} = (5 \times 0) + (7 \times 50) + (8 \times 150) = 1550$$

طبق روابط (۳۵) و (۳۶) سود مهاجمین و مدافعین برابر است با:

$$F_{\text{حمله}} = 6\sum Y^2 - 2\sum X^2 + 4\sum XY - 9\sum Y - 1290 = -1221$$
$$F_{\text{دفاع}} = -C_{\text{دفاع}} - F_{\text{حمله}} = -1550 - (-1221) = -329$$

در نهایت، مدافعین موفق شدند حملات فیشینگ را با آموزش پیشرفته و فیلترهای هوشمند متوقف کنند. مهاجمین تلاش کردند با فیشینگ پیشرفته کاربران را فریب دهند، اما سازمان به دلیل آموزش کافی، موفق به مقابله شد. مدل نشان می‌دهد که سرمایه‌گذاری روی آموزش کاربران می‌تواند خطر حملات فیشینگ را کاهش دهد. اگر هزینه آموزش خیلی زیاد باشد، سازمان می‌تواند ترکیبی از آموزش پایه و فیلترهای هوشمند را انتخاب کند.

سناریو سوم بدافزارهای پیشرفته و دفاع با تحلیل رفتار شبکه: در این سناریو، ۲۰ مهاجم سعی دارند با استفاده از بدافزارهای ناشناخته و پیچیده، به سیستم‌های سازمان نفوذ کنند. در مقابل، ۲۰ مدافع تلاش می‌کنند با استفاده از تحلیل رفتار شبکه، هوش مصنوعی و سیستم‌های امنیتی پیشرفته از این حملات جلوگیری کنند. هدف این تحلیل، بررسی تأثیر فن‌های تحلیل رفتار شبکه در کاهش تأثیر حملات بدافزاری و بهینه‌سازی هزینه‌های دفاع است. هر مهاجم می‌تواند یکی از سه سطح حمله را انتخاب کند.

$X = 0$: غیرفعال (بدون حمله)

$X = 1$: بدافزار ساده (ویروس‌های معمولی و تروجان‌های قدیمی)

$X = 2$: بدافزار پیچیده (بدافزارهای پیشرفته و حملات صفر روزه)

در مقابل، هر مدافع یکی از سه سطح دفاع را انتخاب می‌کند:

$Y = 0$: بدون دفاع (مکانیزمی برای شناسایی بدافزار وجود ندارد)

$Y = 1$: آنتی‌ویروس و فایروال سنتی (روش‌های کلاسیک مبتنی بر فهرست سیاه)

$Y = 2$: تحلیل رفتار شبکه و هوش مصنوعی (تشخیص رفتارهای غیرعادی، یادگیری ماشین برای شناسایی تهدیدات جدید)

جدول (۵). هزینه حمله و دفاع سناریوی سوم در سه سطح مختلف

سطح	هزینه حمله ($C_{\text{حمله}}$)	هزینه دفاع ($C_{\text{دفاع}}$)
۰ (بدون فعالیت)	۰	۰
۱ (بدافزار ساده / آنتی‌ویروس سنتی)	۴۰	۸۰
۲ (بدافزار پیچیده / تحلیل رفتار شبکه)	۲۰۰	۳۰۰

مطابق جداول (۲) و (۵) هزینه حمله و دفاع برابر است با:

$$C_{\text{حمله}} = (4 \times 0) + (7 \times 40) + (9 \times 200) = 2080$$

$$C_{\text{دفاع}} = (5 \times 0) + (7 \times 80) + (8 \times 300) = 2960$$

طبق روابط (۳۵) و (۳۶) سود مهاجمین و مدافعین برابر است با:

$$F_{\text{حمله}} = 6\sum Y^2 - 2\sum X^2 + 4\sum XY - 9\sum Y - 2080 = -2011$$

$$F_{\text{دفاع}} = -C_{\text{دفاع}} - F_{\text{حمله}} = -2960 - (-2011) = -949$$

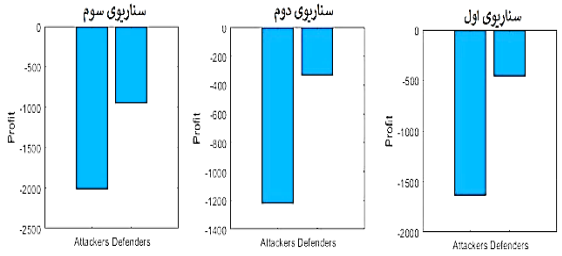
در نهایت، مدافعین موفق شدند حملات بدافزاری را با استفاده از تحلیل رفتار شبکه متوقف کنند. مهاجمین تلاش کردند با بدافزارهای پیچیده به سیستم نفوذ کنند، اما سازمان به دلیل استفاده از روش‌های پیشرفته، موفق به جلوگیری از حمله شد. مدل نشان می‌دهد که استفاده از یادگیری ماشین و تحلیل رفتار شبکه می‌تواند خطر نفوذ بدافزارها را به‌شدت کاهش دهد. اگر هزینه تحلیل رفتار شبکه خیلی بالا باشد، می‌توان ترکیبی از روش‌های سنتی و پیشرفته را به کار گرفت تا هزینه کاهش یابد.

۶. پیاده‌سازی مدل ارائه شده در MATLAB

در این بخش، مدل طراحی‌شده برای شبیه‌سازی تعاملات بین مهاجمین و مدافعین در حملات سایبری ارائه می‌شود و استراتژی‌های بیست مهاجم و بیست مدافع را در نظر گرفته و بر اساس نظریه بازی، استراتژی‌های بهینه، هزینه‌های حمله و دفاع، و سود هر طرف را محاسبه و در نهایت، نتایج مدل به‌صورت گرافیکی نمایش داده می‌شوند. ابتدا، تعداد مهاجمین و مدافعین و سپس هزینه‌های حمله و دفاع مشخص می‌گردد. در ادامه برای شبیه‌سازی سناریوی واقعی حمله و دفاع، هر بازیکن به‌صورت تصادفی یک استراتژی را انتخاب می‌کند و در نهایت مجموع هزینه‌هایی که مهاجمین و مدافعین پرداخت کرده‌اند محاسبه می‌شود. در نهایت تابع سود برای هر دو گروه با درنظرگرفتن میزان موفقیت حملات

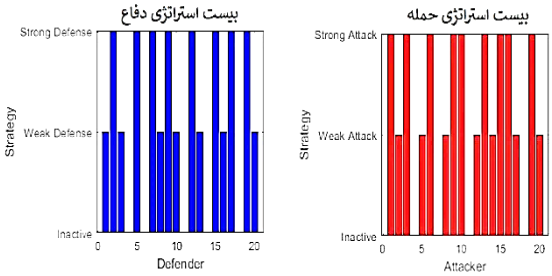
و هزینه‌های پرداخت‌شده تعریف می‌شود که در آن بر اساس فرمول (۳۵)، میزان موفقیت حملات مهاجمین به قدرت دفاعی مدافعین بستگی دارد (ضرایب ۶ و ۴) و هرچه حمله قوی‌تر باشد، تأثیر بیشتری دارد، اما هزینه آن نیز بیشتر است (ضریب ۲-) لذا افزایش تعداد مدافعین و سطح دفاع باعث کاهش سود مهاجمین می‌شود (ضرایب ۹-) و در نهایت طبق تعریف تعادل نش سود مدافعین برابر با منفی سود مهاجمین به‌اضافه هزینه‌های دفاع خواهد بود.

شکل (۲) به مقایسه سود مهاجمین و مدافعین در سه سناریو پرداخته است و نشان می‌دهد که مقدار سود مدافعین از مهاجمین بیشتر است؛ لذا دفاع مؤثر واقع شده است. مقدار منفی سود نشانگر هزینه‌های بالای حمله و دفاع است.



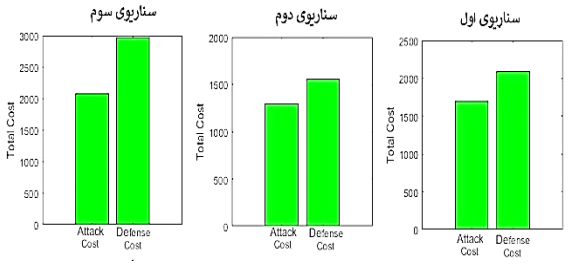
شکل (۲). نمودار مقایسه سود مهاجمین و مدافعین در سه سناریو

شکل (۳) بیست استراتژی انتخابی توسط مهاجمین و مدافعین را نشان می‌دهد. در استراتژی مهاجمین، اگر مقدار ۲ انتخاب شده باشد، یعنی حملات قوی‌تر و پیچیده‌تر است و در مقابل اگر مقدار ۰ انتخاب شده باشد، یعنی سیستم در حالت کم‌خطر است و حملات انجام نمی‌شوند. برای استراتژی مدافعین نیز اگر مقدار ۲ انتخاب شده باشد، یعنی سیستم امنیتی سازمان قوی است و در مقابل اگر مقدار ۰ انتخاب شده باشد، یعنی سیستم بدون محافظت است و ممکن است حملات موفق شوند. استراتژی‌های انتخابی برای مهاجمین و مدافعین در سه سناریو مشابه یکدیگر و مطابق جدول (۲) است.



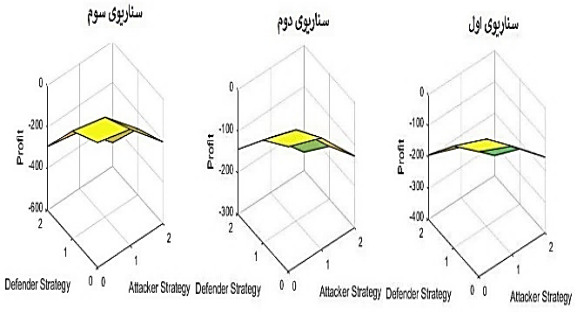
شکل (۳). نمودار توزیع استراتژی‌های مهاجمین و مدافعین

شکل (۴) به مقایسه هزینه‌های حمله و دفاع در سه سناریو پرداخته است و نشان می‌دهد که کدام طرف هزینه بیشتری پرداخت کرده است. اگر هزینه حمله بسیار بیشتر از هزینه دفاع باشد، مهاجمین منابع زیادی را صرف کرده‌اند و احتمال موفقیت پایین بوده است. اگر هزینه دفاع بسیار بیشتر از هزینه حمله باشد، سازمان ممکن است بیش از حد هزینه کند، درحالی‌که خطر حمله کم بوده است. درصورتی‌که هزینه حمله و دفاع برابر باشند، به این معنی است که هر دو طرف منابع خود را به شکل متعادلی خرج کرده‌اند.



شکل (۴). نمودار مقایسه هزینه‌های حمله و دفاع

شکل (۵) به تحلیل سود بر اساس استراتژی‌های حمله و دفاع در قالب نمودار سه‌بعدی پرداخته است و نشان می‌دهد که چگونه سود مهاجم و مدافع به استراتژی‌های انتخابی آن‌ها بستگی دارد. سطح‌های رنگی نشان می‌دهند که چه ترکیبی از حملات و دفاع‌ها بهترین یا بدترین سود را برای هر طرف ایجاد می‌کند. اگر رنگ زرد در بخش $X=2$ و $Y=0$ زیاد باشند، یعنی حملات قوی در صورت عدم دفاع، موفق خواهند شد و سازمان نیاز دارد که سطح دفاعی خود را افزایش دهد. اگر در بخش $X=2$ و $Y=2$ مقدار سود نزدیک به صفر باشد، یعنی دفاع قوی توانسته حملات قوی را خنثی کند.



شکل (۵). نمودار تحلیل سود بر اساس استراتژی‌های حمله و دفاع

۷. نتیجه‌گیری و پیشنهادها

در این مقاله، مدل‌سازی و تحلیل حملات و دفاع‌های سایبری با استفاده از نظریه بازی‌ها ارائه شد. هدف اصلی تحقیق، بررسی راهبردهای بهینه برای مهاجمان و مدافعان در فضای سایبری و تأثیر انتخاب‌های آن‌ها بر موفقیت یا شکست حملات بود. با استفاده از مدل‌های ریاضی و شبیه‌سازی در MATLAB، سناریوهای مختلفی از جمله حملات DDoS، فیشینگ و بدافزارهای پیچیده مورد بررسی قرار گرفت.

نتایج نشان داد که انتخاب راهبردهای دفاعی مناسب نقش مهمی در کاهش اثربخشی حملات دارد. استفاده از روش‌های

پیشرفته مانند تحلیل رفتار شبکه، یادگیری ماشین و سیستم‌های هوشمند شناسایی تهدیدات، می‌تواند میزان موفقیت حملات سایبری را به میزان قابل‌توجهی کاهش دهد. همچنین، محاسبه تعادل نش در مدل‌های ارائه‌شده، نشان داد که طرفین می‌توانند با اتخاذ راهبردهای بهینه، هزینه‌های حمله و دفاع را مدیریت کنند.

یافته‌های تحقیق تأکید دارند که رویکردهای سنتی امنیت سایبری دیگر به‌تنهایی کافی نیستند و لازم است ترکیبی از استراتژی‌های فعال و هوشمند برای مقابله با تهدیدات سایبری استفاده شود. مدل پیشنهادی این تحقیق می‌تواند به سیاست‌گذاران، متخصصان امنیت سایبری و تصمیم‌گیرندگان در سازمان‌ها کمک کند تا بر اساس تحلیل‌های دقیق، راهبردهای مؤثرتری برای دفاع سایبری طراحی کنند.

در پایان چند موضوع جهت پیشبرد مقاله بابت پژوهش‌های آینده پیشنهاد می‌شود که عبارت‌اند از:

۱) مدل‌سازی و تحلیل بازی‌های سایبری با بازیگران متنوع: جنگ‌های سایبری توسط بازیگران مختلف با اهداف و منابع متفاوت انجام می‌شوند، لذا مدل‌سازی بازی‌های پویا که رفتار بازیگران را با درنظرگرفتن عدم قطعیت‌ها، اطلاعات ناقص و رفتار انسانی شبیه‌سازی می‌کنند، می‌تواند راهکاری مؤثر برای پیش‌بینی و مدیریت تهدیدات باشد. این مدل‌ها می‌توانند تأثیر رفتارهای انسانی و تحلیل هزینه - فایده را نیز در خود جای دهند.

۲) تحلیل تأثیر فناوری‌های نوین بر راهبردهای امنیتی: با پیشرفت فناوری‌هایی مانند هوش مصنوعی[1] و اینترنت اشیا[2]، تحلیل نحوه تعامل این فناوری‌ها با حملات و واکنش‌های دفاعی در جنگ‌های سایبری می‌تواند به توسعه سیستم‌های دفاعی هوشمند و مقاوم کمک کند. همچنین، شبیه‌سازی حملات هماهنگ و پیچیده سایبری، همراه با واکنش‌های دفاعی در این سیستم‌ها، می‌تواند کارایی دفاع‌ها را بهبود بخشد.

۳) تحقیق بر تهدیدات جدید و تحلیل تأثیرات جغرافیایی: در دنیای جنگ‌های سایبری، تهدیداتی زیادی نظیر حملات آسیب‌پذیری روز صفر[3]، تهدیدات پایدار پیشرفته[4] وجود دارند. شبیه‌سازی این تهدیدات و ارزیابی واکنش‌های دفاعی می‌تواند به شناسایی بهترین راهبردهای امنیتی و سیاسی کمک کند.

۴) استفاده از یادگیری ماشین برای بهینه‌سازی سیستم‌های دفاعی: یادگیری ماشین می‌تواند به شناسایی الگوهای حملات و بهبود سیستم‌های دفاعی هوشمند کمک کند. در این راستا، اعتبارسنجی این سیستم‌های امنیتی در شرایط دنیای واقعی می‌تواند چالش‌های جدیدی ایجاد کند که نیازمند تحقیقات بیشتر برای اطمینان از عملکرد صحیح در محیط‌های عملی است.

۸. مراجع

[1] H. Eren, M. T. Gençoğlu, and S. Yenal, Strateji ve Güvenlik Alanında Temel ve Güncel Yaklaşımlar: Siber Savaş. Nobel Yayınları, 2020.

[2] A. Sokri, "Game theory and cyber defense," in Games in Management Science, pp. 335-352, Springer, 2019.

[3] M. S. Alamdari, M. Fatemi, and M. Shahrezaei, "Introducing an efficient method to identify the noise pattern of helicopters based on the area feature vector and weighted sparse representation classification," Electronic and Cyber Defense, vol. 12, no. 1, pp. 33-42, 2024, https://dorl.net/dor/20.1001.1.23224347.1403.12.1.4.2. (In Persian).

[4] M. S. Alamdari and M. Fatemi, "Applying weighted smoothed norm in sparse representation classification for face recognition," Electronic and Cyber Defense, vol. 11, no. 3, pp. 57-65, 2023, https://dorl.net/dor/20.1001.1.23224347.1402.11.3.6.1 (In Persian).

[5] M. Babaei, M. Motedayen, and M. Rezaee, "Semi-Blind Separation of Multiple Synchronous Wideband Frequency Hopping Signals Using a Band-Limited Receiver and Space-Time-Frequency Distributions," Electronic and Cyber Defense, vol. 11, no. 4, pp. 117-131, 2024, https://dorl.net/dor/20.1001.1.23224347.1402.11.4.10.7 (In Persian).

[6] A. Shojaeifard, H. Yazdani, and R. Nasiri, "Modular human face recognition method based on principal component analysis and Mahalanobis distance," Electronic and Cyber Defense, vol. 11, no. 4, pp. 93-98, 2024, https://dorl.net/dor/20.1001.1.23224347.1402.11.4.8.5. (in Persian).

[7] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S. S. Iyengar, "Game theory for cybersecurity and privacy," ACM Computing Surveys (CSUR), vol. 50, no. 2, p. 30, 2017.

[8] K. G. Guseinov, E. Akyar, and S. A. Düzce, Oyun Teorisi, Seçkin Yayınları, 2010.

[9] C. Kiekintveld, V. Lisy, and R. Pibil, "Game-theoretic foundations for the strategic use of honeypots in network security," in Cyber Warfare, pp. 81-101, Springer, 2015.

[10] M. J. Osborne, An Introduction to Game Theory, Oxford University Press, 2004.

[11] S. G. Sanjay and H. Yuan, "Cyber war games: Strategic jostling among traditional

[1]. Artificial Intelligence
[2]. Internet of Things
[3]. Zero-day
[4]. Advanced Persistent Threat

adversaries," Cyber Warfare, Advances in Information Security, vol. 56, 2015.

[12] J. Harsanyi, "Games with incomplete information played by Bayesian players, I-III, Part I, the basic model," Management Science, vol. 14, no. 3, pp. 159–182, 1967.

[13] R. Aumann and M. Maschler, Repeated Games with Incomplete Information, MIT Press, 1995.

[14] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari, "The role of game theory in information warfare," in 4th Information Survivability Workshop, Vancouver, Canada, 2002.

[15] J. Burke, "Robustness of optimal equilibrium among overlapping generations," Economic Theory, vol. 14, pp. 311–330, 1999.

[16] R. Gibbons, Game Theory for Applied Economists, Princeton University Press, 1992.

[17] M. Libicki, Defending Cyberspace, and Other Metaphors, National Defense University, 1997.

[18] F. Andrew, P. Emmanouil, M. Pasquale, H. Chris, and S. Fabrizio, "Game theory meets information security management," in IFIP International Information Security Conference SEC 2014: ICT Systems Security and Privacy Protection, pp. 15-29, 2014.