فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال دوم، شماره چهار، زمستان ۱۳۹۷

یک مدل مبتنی بر نظریه بازی برای تصمیم‌گیری راهبردی در جنگ سایبری

محمود فروغی[۱]*، علی اکرمی‌زاده[۲]، مسعود باقری[۳]

تاریخ دریافت: ۱۳۹۷/۰٤/۱۳ تاریخ پذیرش: ۱۳۹۷/۱۲/۲۵

چکیده

در این مقاله با استفاده از نظریه بازی و ساخت یک مدل تحلیلی فرآیند تصمیم‌گیری در یک درگیری سایبری موردبررسی قرارگرفته است. بازیکن‌ها طرفین درگیری هستند که آسیب‌پذیری‌هایی را روی سامانه‌های یکدیگر شناسایی کرده و قصد دارند در یک موقعیت مناسب از آن برای تهاجم علیه رقیب استفاده کنند. آن‌ها می‌خواهند بدانند تصمیم عاقلانه برای رسیدن به سود بیشتر در جریان این تقابل چیست؟ در مقایسه با کارهای پیشین، مفروضات مسئله به شرایط واقعی نزدیک شده و احتمال تلافی طرف مقابل و احتمال شکست حمله، در تعریف بازی لحاظ شده است. برای نمایش بازی از فرم توسعه‌یافته استفاده شده و تعادل نش برای آن محاسبه گردیده است. با تحلیل نتایج در حالت استراتژی مختلط نشان داده شده که نظریه بازی می‌تواند ضمن برآورد تصمیم طرفین، به هر یک از آن‌ها پیشنهادهایی در مورد انتخاب استراتژی ارائه دهد.

واژگان کلیدی: آسیب‌پذیری، بازیکن، تابع پاداش، راهبرد بهینه

[۱]* دانشگاه دریایی امام خامنه‌ای(مدظله)، استادیار گروه فناوری اطلاعات، نویسنده مسئول mforooghy@mail.ihu.ac.ir

[۲] دکتری هوش مصنوعی، استادیار مدعو دانشگاه تهران

[۳] دانشگاه جامع امام حسین (ع)، استادیار گروه مهندسی کامپیوتر

[Downloaded from ic4i-journal.ir on 2026-11-18]

۱. کلیات

۱,۱. بیان مسئله

بازیگران عرصه جنگ‌های سایبری در سال‌های اخیر نشان داده‌اند که می‌توانند تصمیماتی اتخاذ کنند که موجودیت یک فرد، سازمان و حتی یک دولت و کشور را با خطر مواجه کند. بر این اساس یک مسیر مهم تحقیقات، مدل‌سازی فرآیندهای تصمیم‌گیری در این حوزه است. هر یک از طرفین در این عرصه ممکن است بر اساس شناختی که از شرایط موجود و میزان توانائی‌های خود و رقیب دارد به یک استراتژی تهاجمی یا دفاعی روی آورد. در این وضعیت مطالعه نحوه تعامل دو رقیب که هرکدام منابعی از آسیب‌پذیری در سیستم طرف مقابل در اختیار دارند و برآورد تصمیم آن‌ها در استفاده یا عدم استفاده از منابع به‌منظور انجام تهاجم و یا تقویت امنیت خود می‌تواند راهگشا باشد. از سوی دیگر استفاده از آسیب‌پذیری‌ها به ابزاری رایج در حملات سایبری تبدیل شده و روند جاری نشان‌دهنده رشد استفاده از آسیب‌پذیری‌ها در این حملات است [۱].

یک رویکرد نسبت به این امر شامل مدل‌سازی سناریوهای تصمیم‌گیری، با استفاده از نظریه بازی‌ها است. ازآنجاکه در این فضای رقابتی، کنش‌های هر یک از طرفین بر روی میزان بهره ناشی از رفتار طرف مقابل مؤثر است و طرفین به دنبال کسب بهترین نتایج از عملکردشان هستند، به‌خوبی می‌توان آن را در قالب یک بازی مدل کرد و با استفاده از مبانی علمی موجود در نظریه بازی برای حل آن تلاش نمود. نظریه بازی به‌عنوان ابزار ریاضی می‌تواند در ارائه یک چارچوب کمی برای حل مسئله فوق کمک کند. ضعف راه‌حل‌های سنتی این است که آن‌ها فاقد یک چارچوب تصمیم‌گیری کمی هستند [۲]. کاربرد رویکردهای نظریه بازی در مورد امنیت سایبری، اخیراً برای به دست آوردن ماهیت جنگ اطلاعات موردتوجه قرارگرفته است.

مسئله در اینجا مدل‌سازی فرآیند تصمیم‌گیری برای طرفین یک درگیری سایبری است. در فضای رقابت سایبری، دو طرف آسیب‌پذیری‌هایی را از سامانه‌های طرف مقابل در اختیار دارند. به ازای شرایط ممکن است یکی از آن‌ها تصمیم بگیرد که طی یک تهاجم سایبری از آسیب‌پذیری طرف مقابل برعلیه او بهره‌برداری کند. چالشی که برای تصمیم‌گیری پیش روی او قرار دارد و نحوه انتخاب وی، می‌تواند زنجیره‌ای از اتفاقات بعدی را رقم بزند که پیش‌بینی ماحصل آن همواره به‌عنوان یک مسئله مهم در علوم تصمیم‌گیری است: آیا با توجه به شرایط خود و طرف مقابل از آسیب‌پذیری برای حمله به رقیب استفاده کند و یا از اقدام به حمله منصرف شود. رقیبی که موردحمله واقع می‌شود نیز باید در مورد اقدام متقابل تصمیم‌گیری کند. شرایطی که در اینجا در نظر گرفته می‌شود شامل مواردی مثل قدرت سایبری حریف در مقایسه با طرف مقابل، احتمال حمله تلافی‌جویانه او، پاداش‌ها و هزینه‌های حمله و شکست، می‌باشد. با استفاده از ابزارهای نظریه بازی می‌توان مسئله را موردبررسی قرارداد.

۱,۲. اهمیت و ضرورت موضوع تحقیق

یک بازیگر در عرصه نبرد سایبری نیازمند آن است که تصمیم‌های درستی را بر اساس یک راهبرد تعیین‌شده اتخاذ نماید. یک تصمیم غلط در این عرصه می‌تواند یک فرد، سازمان و حتی یک کشور را با چالش جدی روبرو کند. از سوی دیگر کنش‌ها و واکنش‌های رقیب در بهره ناشی از این تصمیم‌ها مؤثر است، بنابراین برای انتخاب یک راهبرد مناسب می‌بایست بتوان پاداش‌ها و هزینه‌های یک اقدام را از قبل ارزیابی کرد و با مقایسه آن‌ها به راهبرد بهینه دست‌یافت.

۱,۳. هدف تحقیق

هدف اصلی از انجام این تحقیق ارائه یک چارچوب کمی برای توسعه مدل رفتاری و تجزیه‌وتحلیل رفتار طرفین یک درگیری سایبری است تا بتوان بر اساس آن شرایط مناسب برای استفاده بهینه از یک آسیب‌پذیری موجود در سیستم هدف را تخمین زد. نتایج حاصل از این تحلیل می‌تواند به تصمیم‌گیری مؤثر در فرآیند درگیری سایبری کمک کند. به‌علاوه این تحلیل‌ها باعث می‌شود تا بازیگران بتوانند قبل از وقوع درگیری سایبری جوانب مختلف آن را سنجیده و به یک آمادگی ذهنی در مورد آن دست یابند.

[Downloaded from ic4i-journal.ir on 2026-11-18]

۱,٤. پیشینه تحقیق

در سال‌های اخیر استفاده از نظریه بازی به‌منظور مدل‌سازی در حوزه امنیت سایبری در هر دو جنبهٔ مسائل فنی و مسائل تصمیم‌گیری راهبردی موردتوجه محققین بوده است. بیشتر کارهای انجام‌شده در حوزه امنیت سایبری با استفاده از نظریه بازی در سال‌های اخیر در سطح تاکتیک و تکنیک بوده‌اند و تنها تعداد معدودی کار در سطح استراتژیک انجام‌شده است [۳] [٤]. از دیدگاه نظریه بازی عمده کارهای انجام‌شده در ارتباط با امنیت سایبری در گروه بازی‌های غیرهمکارانه قرار می‌گیرند. در همین کارها نیز محدودیت‌هایی مثل در نظر نگرفتن احتمال شکست حمله و یا احتمال تلافی طرف مقابل وجود داشته است. در ادامه برخی کارهای اخیر در این حوزه بررسی خواهد شد.

فریدمن [٤] و همکارانش یک مدل نظریه بازی برای تصمیم‌گیری استراتژیک هنگام کشف یک آسیب‌پذیری ارائه کرده‌اند. سؤال اصلی در پژوهش آن‌ها این است که یک سازمان امنیت سایبری هنگام شناخت آسیب‌پذیری‌های ناشناختهٔ نرم‌افزاری چه باید بکند؟ آیا بهتر است اطلاعات مربوط به آسیب‌پذیری را به تولیدکننده مرتبط ارائه کرده و به بهبود امنیت عمومی کمک کند و یا با احتیاط بیشتر آسیب‌پذیری را همچنان مخفی نگه دارد تا در آینده بتوان از آن برای یک حمله روز صفر علیه دشمن استفاده کرد. آن‌ها با به دست آوردن تعادل نش، نشان دادند که وقتی توانایی طرفین برای کشف ناهنجاری به هم نزدیک باشد هر دو طرف استراتژی مخفی نگه‌داشتن آسیب‌پذیری کشف‌شده را انتخاب خواهند کرد، اما اگر در توانایی دو طرف اختلاف چشمگیری وجود داشته باشد پیش‌بینی مدل آن‌ها آن است که یکی از بازیکن‌ها سیاست افشای آسیب‌پذیری را در پیش خواهد گرفت. یک مشکل این کار آن است که آن‌ها استراتژی ترکیبی را در مدل در نظر نگرفته و مسئله را صرفاً با فرض استراتژی خالص حل کرده‌اند.

اکسلرود و ایلیف [۵] با الهام از نظریه بازی یک مدل ریاضی ارائه کرده‌اند که از دیدگاه یک مهاجم مسئله زمان مناسب برای سوءاستفاده از یک آسیب‌پذیری را تحلیل می‌کند. آسیب‌پذیری در اینجا به‌عنوان منبعی برای عملیات جاسوسی یا اختلال یا خرابکاری فرض می‌شود و با تعریف ویژگی‌هایی مثل پایداری و پوشیدگی و نیز تعریف پاداش یا بهره ناشی از حمله برای مهاجم، تلاش شده تا تأثیر این عوامل بر زمان‌بندی بهینه برای تهاجم با استفاده از مدل تحلیل شود. هرچند کار آن‌ها به درک استراتژیک از فضای درگیری سایبری کمک می‌کند اما در آن صرفاً از دیدگاه مهاجم به مسئله توجه شده و پارامترهایی مثل هزینه‌های تهاجم و احتمال شکست مهاجم نیز در نظر گرفته نشده است.

هوآ و باپنا [۷] تأثیر تروریسم سایبری بر اقتصاد را موردمطالعه قراردادند. آن‌ها با تأکید بر تفاوت بین هکرهای معمولی و تروریست‌های سایبری یک مدل نظریه بازی ارائه کرده‌اند تا به‌وسیله آن سرمایه‌گذاری بهینه روی سامانه‌های امنیت اطلاعات را، از طریق تحلیل ریسک و پیش‌بینی رفتار تروریست‌ها، بیابند. آن‌ها با در نظر گرفتن اثر سرمایه‌گذاری امنیتی بر سطح بازدارندگی، روی توسعه مدلی از نظریه بازی تمرکز کرده‌اند که رفتار هکرها و تروریست‌های سایبری را از دیدگاه سرمایه‌گذاری سازمانی توضیح می‌دهد. یک بازی ساده استاتیک با دو بازیکن مهاجم و هدف تعریف‌شده است که در آن اقدامات مهاجم شامل حمله یا عدم حمله و انتخاب‌های هدف شامل حفظ سطح سرمایه‌گذاری فعلی و یا افزایش آن است. برای رسیدن به سرمایه‌گذاری بهینه آن‌ها به کاهش خسارت در هدف و به حداقل رساندن پاداش مهاجم توجه کرده‌اند. با به دست آوردن تعادل نش نتایج شبیه‌سازی‌های آن‌ها نشان می‌دهد که در چه مواردی افزایش سرمایه‌گذاری مقرون‌به‌صرفه است.

کار مشابه دیگر آن‌ها در این زمینه، [۷] تأثیر تهدیدهای اینترنتی را بر سرمایه‌گذاری در سامانه‌های اطلاعاتی با استفاده از رویکرد نظریه بازی بررسی می‌کند. آن‌ها یک بازی مجموع کلی ۲×۲ استاتیک را پیشنهاد می‌کنند تا تأثیر تهدید ناشی از یک عنصر داخلی و یک مهاجم خارجی را با هم مقایسه کنند. نتایج شبیه‌سازی نشان می‌دهد که میزان سرمایه‌گذاری مطلوب موردنیاز برای محافظت از زیرساخت‌ها در برابر تهاجم خودی،

[Downloaded from ic4i-journal.ir on 2026-11-18]

نسبت به محافظت از سامانه‌ها در برابر تهدیدات سایبری هکرهای خارجی، بالاتر است.

بن سوسان و همکارانش [۸] جنبه‌های اقتصادی فعالیت بات‌نت را مطالعه کرده و راهکارهای دفاعی را برای مقابله با دزدان بات‌نت ارائه می‌دهند. در این مطالعه، بات‌نت‌ها به‌عنوان تعدادی از کامپیوترهای متصل‌به‌هم و آلوده به نرم‌افزارهای مخرب تعریف می‌شوند که اجازه می‌دهند تا سارقین بدون اطلاع مالک، سامانه‌های آلوده بات‌نت را از راه دور به کنترل خود درآورند. فعالیت‌های بات‌نت‌ها اغلب با انگیزه اقتصادی انجام می‌شوند، مانند سودی که دزدان سامانه‌ها از فعالیت غیرقانونی خود به دست می‌آورند. در مدل ارائه‌شده هدف مهاجم حداکثر کردن سود از طریق افزایش نفوذ در شبکه است، البته او برای این هدف باید هزینه بیشتری نیز صرف کند. در مقابل مدافع سعی می‌کند تعداد دستگاه‌های آلوده را کاهش دهد. افزایش تعداد دستگاه‌های آلوده به معنای افزایش هزینه دفاع است. برای حل این مشکل، بن سوسان و همکارانش یک رویکرد نظریه بازی ارائه کرده‌اند که می‌تواند استراتژی بهینه را برای مقابله با دزدهای بات‌نت انتخاب کند. در این مطالعه، میزان کامپیوترهایی که آلوده‌شده‌اند بر اساس یک مدل اپیدمی اصلاح می‌شوند. درنهایت آن‌ها نشان دادند که در نواحی مشخصی ازنظر سطح حمله و دفاع و تعداد دستگاه‌های آلوده، این تقابل می‌تواند با تعادل همراه باشد.

شلینکر و همکارانش [۹] یک بازی برای فریب مهاجم شبکه تعریف کرده‌اند. در این سناریو مهاجم برای جمع‌آوری اطلاعات، شبکه هدف را اسکن می‌کند و مدافع در مقابل تلاش می‌کند او را فریب دهد. دو نوع مهاجم در این بازی در گرفته شده است: مهاجم قدرتمندی که از استراتژی فریب مدافع آگاهی دارد و مهاجم ساده‌ای که از این استراتژی آگاه نیست. آن‌ها نشان داده‌اند که محاسبات مربوط به استراتژی بهینه فریب برای هر دو نوع مهاجم دارای پیچیدگی‌هایی است. تمرکز عمده آن‌ها در این کار بر روی ارائه الگوریتمی برای غلبه بر این پیچیدگی‌های محاسباتی بوده است. درنهایت آن‌ها با تجزیه‌وتحلیل تجربی سعی کرده‌اند اثربخشی راه‌حل خود را اثبات کنند.

ساکدویو و همکارانش [۱۰] مشکل حمله تداخل امواج در شبکه بی‌سیم را موردبررسی قرار داده‌اند. در این مطالعه، حمله پارازیتی به‌عنوان یک بازی غیر همکارانه مدل‌سازی می‌شود که توسط دو نوع بازیکن، یکی به‌عنوان فرستنده ویکی پارازیت دهنده انجام می‌شود. در این مسئله، فرستنده‌ها با کاربران معمولی مرتبط هستند و می‌خواهند عملکرد خود را بهینه کنند. در مقابل، پارازیت‌دهندگان با مهاجمان ارتباط دارند که هدفشان کاهش عملکرد فرستنده‌ها است. تمرکز این کار عمدتاً بر آسیب‌پذیری سیستم نسبت به حملات منع خدمات در لایه کنترل دسترسی رسانه می‌باشد. استفاده از نظریه بازی، بهبود درک تأثیر حملات منع خدمات را بر عملکرد سیستم در شبکه‌های بی‌سیم، نشان داده است.

ژید چن [۱۱] بر اساس تئوری بازی تکاملی، یک مدل دفاعی پیشگیرانه را برای حفاظت از شبکه‌های حسگر بی‌سیم در برابر مهاجمان پیشنهاد می‌دهد. این مطالعه سناریوی خاصی را در نظر می‌گیرد که مهاجمان سعی می‌کنند منابع را از دیگر گره‌ها غارت کنند تا طول عمر خود را با مصرف کمتر انرژی افزایش دهند. مدل پیشنهادی اجازه می‌دهد تا گره‌های حسگر بی‌سیم به‌صورت پویا استراتژی‌های دفاعی خود را بر اساس استراتژی‌های مختلف مهاجمان تنظیم کنند. نتایج شبیه‌سازی نشان می‌دهد که مدل پیشنهادی عملکرد شبکه‌های حسگر بی‌سیم را بهبود می‌بخشد و موجب صرفه‌جویی در مصرف انرژی می‌شود.

ژانگ و همکارانش [۱۲] مسئله چگونگی محافظت از سامانه‌ای شامل چند گره در برابر حملات مخفیانه را موردبررسی قرار می‌دهند. فرض بر آن است که هم مدافع و هم مهاجم منابع محدودی در اختیار دارند. مدل بازی ارائه‌شده از نوع ترتیبی است که در آن ابتدا مدافع استراتژی خود را اعلام می‌کند. حرکت مدافع کاملاً آشکار و قابل‌مشاهده است. سپس مهاجم در پاسخ حرکت خود را صورت پنهان انجام می‌دهد. تقابل بین مهاجم و مدافع به‌عنوان یک بازی دو نفره و مجموع غیر صفر مدل‌سازی شده است. این مطالعه ضمن یافتن تعادل نش استراتژی بهینه برای هر دو بازیکن را تحلیل می‌کند.

[Downloaded from ic4i-journal.ir on 2026-11-18]

در کاری که اخیراً توسط ادوارد و همکارانش [۱۳] ارائه‌شده یک مدل نظریه بازی پیشنهاد می‌شود که می‌تواند برای مدل‌سازی تصمیم‌گیری قربانی یک تهاجم سایبری مورداستفاده قرار گیرد. در سناریوی تعریف‌شده قربانی تهاجم در صورت شناسایی عامل حمله با یک چالش تصمیم‌گیری مواجه می‌شود. او می‌بایست با توجه به شرایط خودش و مهاجم تصمیم بگیرد که در برابر حمله سکوت کرده و هویت مهاجم را به‌صورت رسمی اعلام نکند و یا آن‌که با اعلام رسمی هویت مهاجم در صحنه عمومی از خود واکنش اعتراضی نشان دهد. این بازی "بازی سرزنش" نامیده شده و تحلیل‌های انجام‌شده نشان می‌دهد که در شرایطی قربانی حتی با وجود شناسایی مهاجم، ترجیح می‌دهد حمله و مهاجم آن پنهان مانده و در صحنه عمومی واکنش اعتراضی صورت نگیرد.

کارهایی که تاکنون در حوزه امنیت سایبری با استفاده از نظریه بازی انجام‌شده است دارای محدودیت‌های مختلفی هستند که برخی از این محدودیت‌ها به شرح زیر است:

- در طول بازی برای هر طرف نقش ثابت مهاجم یا مدافع در نظر گرفته‌شده است.
- در صورت اقدام به حمله احتمال تلافی طرف مقابل در نظر گرفته نشده است.
- در صورت اقدام به حمله احتمال شکست در نظر گرفته نشده است.
- بیشتر کارهای انجام‌شده در سطح تاکتیکی و تکنیکی بوده و تعداد بسیار معدودی کار در سطح استراتژیک برای تصمیم‌گیری در صحنه جنگ سایبری انجام شده است.

۱,۵. سؤالات تحقیق

سؤال اصلی تحقیق را می‌توان به این صورت بیان کرد که: برای حریفی که منبعی از آسیب‌پذیری‌های سیستم رقیب را در اختیار دارد، استراتژی بهینه در نحوه استفاده از این منبع کدام است؟ به‌عبارت‌دیگر او در چه شرایطی از این منبع استفاده کند تا به بیشترین نتایج موردنظر دست یابد؟

سؤالات فرعی تحقیق عبارت‌اند از:

- از بین مدل‌های کلاسیک موجود در نظریه بازی کدام‌یک انطباق بیشتری با شرایط مسئله دارد؟
- آیا لازم است برای حل مسئله یک مدل جدید در نظریه بازی ارائه کرد؟
- تابع پاداش مناسب برای این بازی و پارامترهای مؤثر در آن را چگونه می‌توان محاسبه کرد؟
- آیا به کمک تعریف تعادل نش می‌توان برای این بازی منطقه تعادل را به دست آورد؟

۱,۶. سازمان‌دهی تحقیق

این مقاله در پنج بخش تنظیم شده است که فصل اول شامل بیان مسئله، ضرورت و اهمیت، اهداف، پیشینه، و پرسش‌های تحقیق است. در بخش دوم مدل پیشنهادی و پارامترهای مربوط به آن تشریح می‌شود. در ادامه و در بخش سوم نحوه محاسبه تعادل نش برای بازی تشریح شده و سپس با مشخص شدن تعادل سعی شده راهبردهای مختلف انتخابی توسط بازیکن‌ها بررسی شود.

در بخش چهارم مدل را در حالت راهبرد مختلط اجرا کرده و نتایج موردبررسی قرارگرفته است. در بخش پنج نتیجه‌گیری و پیشنهادهایی برای کارهای آینده ارائه شده است.

۲. مدل پیشنهادی

در فضای مسئله دو بازیکن با هم رقابت می‌کنند که به ترتیب بازیکن۱ و بازیکن۲ نامیده می‌شوند. در این فضا فرضیات لازم برای حل مسئله عبارت‌اند از:

- دو طرف بازی رفتاری مبتنی بر عقلانیت دارند؛ به‌عبارت‌دیگر، از بین عمل‌های قابل انتخاب، عملی را انتخاب می‌کنند که سود بیشتری دارد.
- در صورت حمله با استفاده از آسیب‌پذیری، احتمال اقدام متقابل طرف مقابل وجود دارد؛ یعنی هدفی که موردتهاجم قرار می‌گیرد ممکن است تصمیم بگیرد در پاسخ به حمله‌ای که به او شده است، به یک حمله تلافی‌جویانه دست بزند. در کارهای دیگر به این نکته به‌عنوان یک پیامد برای مهاجم اول توجه نشده است.

[Downloaded from ic4i-journal.ir on 2026-11-18]

- در صورت اقدام به حمله، احتمال شکست نیز وجود دارد که در آن صورت پاداش منفی یا هزینه به مهاجم تحمیل خواهد شد.

بازیکن۱ بازیکنی است که در موضع حمله ابتدایی قرار دارد. او می‌تواند بین حمله یا عدم حمله یکی را انتخاب کند. احتمال آن‌که او اقدام به حمله کند با **PA1** نشان داده می‌شود. برخی عوامل مؤثر در میزان این احتمال در جدول (۱) آمده است.

منظور از سطح مخاصمه در این جدول آن است که با افزایش یا کاهش تنش بین دو رقیب ممکن است انگیزه آن‌ها برای اقدام به تهاجم افزایش یا کاهش یابد؛ مثلاً تنش در روابط میان دو کشور باعث می‌شود تا آن‌ها انگیزه بیشتری برای تهاجم سایبری علیه یکدیگر داشته باشند. میزان سود ناشی از یک حمله نیز می‌تواند بر انگیزه مهاجم تأثیر بگذارد. ویژگی آسیب‌پذیری نیز از عوامل تأثیرگذار در تصمیم برای حمله است؛ مثلاً این‌که اگر فعلاً از آسیب‌پذیری موجود استفاده نشود تا چه مدت دیگر از دید رقیب پنهان مانده و در سیستم او باقی می‌ماند و یا در صورت استفاده از یک آسیب‌پذیری آیا امکان دارد آن آسیب‌پذیری همچنان پنهان مانده و برای دفعات بعد قابل‌استفاده باشد.

اگر در همان ابتدا تصمیم بازیکن۱ ترک حمله باشد بازی با یک امتیاز مساوی برای طرفین به پایان می‌رسد. در صورت اقدام به حمله شانس بازیکن۱ برای پیروزی **PS1** است. پارامترهای مؤثر در تعیین این شانس نیز در جدول (۱) آمده است.

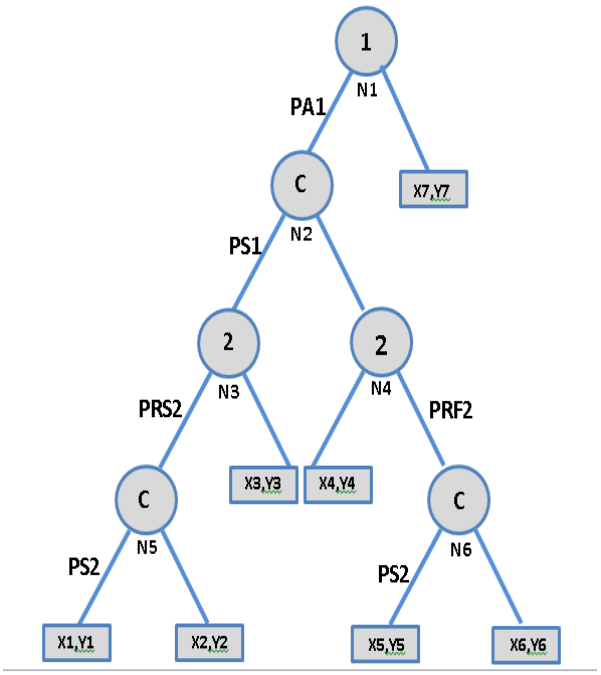
بازیکن۲ بازیکنی است که هدف حمله ابتدایی قرارگرفته و باید در مورد واکنش مناسب تصمیم‌گیری کند. تصمیم‌های ممکن او به ترتیب عبارت‌اند از تلافی یا عدم تلافی چه در صورت پیروزی چه در صورت شکست حمله اولیه بازیکن۱. در صورت تصمیم به حمله متقابل، احتمال پیروزی بازیکن۲ مقدار **PS2** خواهد بود؛ اما احتمال تلافی توسط بازیکن۲، یسته به توفیق یا شکست حمله ابتدایی بازیکن۱، به ترتیب **PRS2** و **PRF2** است.

با توجه به آن‌که بازی، یک بازی چندمرحله‌ای و ترتیبی است برای نمایش آن از فرم توسعه‌یافته استفاده‌شده است. این شیوه نمایش در مقایسه با روش دیگر (فرم نرمال یا استراتژیک) کاملاً منطبق بر ویژگی‌ها و شرایط مسئله است. گام‌های بازی در یک درخت در شکل ۱ نشان داده‌شده است. هر گره داخلی به‌صورت گرافیکی با یک دایره همراه با شماره بازیکن و یا برچسب **c** (برای گره شانس) نمایش داده می‌شود. خط ارتباطی بین یک گره بازیکن و فرزندانش با برچسب دو عمل ممکن برای او (احتمال حمله اولیه برای بازیکن۱ و احتمال تلافی برای بازیکن۲) مشخص‌شده است. خط بین گره شانس و فرزندانش با مقدار احتمال موفقیت در حمله نشانه‌گذاری گردیده است. برگ‌های درخت که به‌صورت چهارگوش نشان داده‌شده‌اند شامل یک زوج عدد می‌باشند که اولی پاداش بازیکن۱ و دومی پاداش باریکن ۲ است. بازی از ریشه درخت شروع می‌شود و جریان می‌یابد. اگر گره جاری گره شانس باشد، انتقال به‌طور اتفاقی به یکی از زیرشاخه‌های آن صورت می‌گیرد که در آن احتمال رسیدن به یک فرزند، مقدار درج‌شده روی خط اتصال است. متناوباً اگر گره جاری به‌عنوان یک بازیگر برچسب خورده باشد (۱ یا ۲) بازیگر باید حمله یا عدم حمله را انتخاب کند. سرانجام وقتی به یک برگ می‌رسیم بازی تمام شده و بازیکنان به امتیازی که در آن برگ مشخص شده است، رسیده‌اند.

جدول ۱- مجموعه متغیرهای احتمالی تعریف‌شده برای مدل

نام	شرح	عوامل مؤثر
PA1	احتمال حمله بازیکن۱	سطح مخاصمه یا انگیزه مهاجم، ویژگی آسیب‌پذیری
PS1	احتمال موفقیت حمله بازیکن۱	توان تهاجم ۱، میزان پوشش دفاعی در ۲
PRS2	احتمال تلافی ۲ بعد از حمله موفق ۱	سطح مخاصمه یا انگیزه مهاجم، ویژگی آسیب‌پذیری، شناسایی مهاجم
PRF2	احتمال تلافی ۲ بعد از حمله ناموفق ۱	سطح مخاصمه یا انگیزه مهاجم، ویژگی آسیب‌پذیری، شناسایی مهاجم
PS2	احتمال موفقیت حمله بازیکن۲	توان تهاجم ۲، میزان پوشش دفاعی در ۱

[Downloaded from ic4i-journal.ir on 2026-11-18]



شکل ۱-نمایش بازی در فرم توسعه‌یافته

بازی را می‌توان با توضیح نحوه نمایش آن توسط درخت، گام‌به‌گام پیش برد. در گره **N1** بازیکن۱ در موضع تصمیم‌گیری برای حمله قرار دارد. با احتمال **PA1** او اقدام به حمله می‌کند و در این صورت جریان بازی به گره **N2** منتقل خواهد شد. ولی اگر او از حمله منصرف شود (با احتمال **PA1**-۱) درنتیجه بازی با امتیازهای **X7** و **Y7** به ترتیب برای خودش و بازیکن۲ به پایان می‌رسد.

اگر تصمیم بازیکن۱ حمله ابتدایی باشد باید دید در گره شانس **N2** احتمال موفقیت او چقدر است. با احتمال **PS1** حمله او موفقیت‌آمیز است در این صورت باید دید در گره **N3** بازیکن۲ چه تصمیمی خواهد گرفت. با احتمال (**PRS2**-۱) او ترجیح می‌دهد حمله را تلافی نکند، بنابراین با امتیازهای **X3** و **Y3** برای دو بازیکن بازی تمام خواهد شد؛ اما اگر او تصمیم به حمله تلافی‌جویانه بگیرد (با احتمال **PRS2**) در گره **N5** این حمله می‌تواند با پیروزی (با احتمال **PS2**) و یا شکست (با احتمال **PS2**-۱) همراه باشد که در هر حالت بازی با پاداش‌های مشخص برای هر در بازیکن به پایان خواهد رسید.

اگر حمله ابتدایی بازیکن۱ با شکست همراه باشد جریان بازی از گره **N2** به گره **N4** منتقل خواهد شد (با احتمال **PS1**-۱) و در آنجا بازیکن۲ باید در مورد تلافی حمله تصمیم بگیرد. بدیهی است احتمال تلافی در برابر یک مهاجم ناکام با احتمال تلافی در مقابل یک مهاجم موفق متفاوت خواهد بود، به همین دلیل احتمال تلافی در این وضعیت با **PRF2** نشان داده شده است. بر اساس تصمیم بازیکن۲ و احتمال موفقیت او مسیر بازی مطابق ساختار تعریف‌شده تا رسیدن به گره‌های پایانی ادامه خواهد یافت.

بر اساس ساختار بازی و پارامترهای تعریف‌شده می‌توان تابع پاداش را در حالت کلی برای هر یک از دو بازیکن به دست آورد. رابطه (۱) تابع پاداش بازیکن۱ و رابطه (۲) تابع پاداش بازیکن۲ را نشان می‌دهد.

$$P1 = (PA1.PS1.PRS2.PS2).X1 + (PA1.PS1.PRS2.(1-PS2)).X2 + (PA1.PS1.(1-PRS2)).X3 + (PA1.(1-PS1).(1-PRF2)).X4 + (PA1.(1-PS1).PRF2.PS2).X5 + (PA1.(1-PS1).PRF2.(1-PS2)).X6 + (1-PA1).X7 \quad (۱)$$

$$P2 = (PA1.PS1.PRS2.PS2).Y1 + (PA1.PS1.PRS2.(1-PS2)).Y2 + (PA1.PS1.(1-PRS2)).Y3 + (PA1.(1-PS1).(1-PRF2)).Y4 + (PA1.(1-PS1).PRF2.PS2).Y5 + (PA1.(1-PS1).PRF2.(1-PS2)).Y6 + (1-PA1).Y7 \quad (۲)$$

مقدار پاداش کسب‌شده توسط هر یک از طرفین که شامل مقدارهای **X** و **Y** به ازای شرایط مختلف می‌شود در جدول (۲) آمده است. با دقت در پاداش‌های هریک از طرفین مشاهده می‌شود که پاداش یک بازیکن قرینه پاداش طرف مقابل است. بنابراین می‌توان بازی را یک بازی مجموع صفر در نظر گرفت که در آن برای اجتناب از منفی شدن، مقدار همه پاداش‌ها با عدد مثبت ۳ جمع شده‌اند.

[Downloaded from ic4i-journal.ir on 2026-11-18]

جدول (۲)- پاداش بازیکن‌ها به ازای شرایط متفاوت بازی

عمل بازیکن۱	عمل بازیکن۲	پاداش بازیکن۱		پاداش بازیکن۲	
حمله موفق	تلافی ناموفق	X2	6	Y2	0
حمله موفق	بدون تلافی	X3	5	Y3	1
حمله موفق	تلافی موفق	X1	4	Y1	2
حمله ناموفق	بدون تلافی	X4	2	Y4	4
حمله ناموفق	تلافی ناموفق	X6	1	Y6	5
حمله ناموفق	تلافی موفق	X5	0	Y5	6
صرف‌نظر از حمله	-	X7	3	Y7	3

۳. یافتن تعادل

برای پیش‌بینی استراتژی انتخابی بازیکن‌ها می‌بایست نقطه تعادل بازی محاسبه شود. یک استراتژی پروفایل یک تعادل نش نامیده می‌شود اگر هیچ بازیکنی نتواند با تغییر حرکت یک‌جانبه به بهره بیشتری دست یابد. برای یافتن تعادل ناحیه‌های مختلفی که متناسب با انتخاب استراتژی توسط بازیکن‌ها وجود دارد را در نظر گرفته و وجود تعادل نش را برای هر ناحیه بررسی می‌کنیم.

اولین ناحیه، ناحیه‌ای از بازی است که در آن بازیکن۱ استراتژی حمله را انتخاب می‌کند و بازیکن۲ در هر حالتی استراتژی تلافی را برمی‌گزیند. بر این اساس همه مقادیر پارامترهای احتمالی در انتخاب استراتژی برابر یک خواهد بود: (**PA1=1, PRS2=1, PRF2=1**)

برای این‌که این ناحیه تعادل نش باشد می‌بایست هم‌زمان دو شرط برقرار باشد:

- درصورتی‌که بازیکن۲ حرکت خود را تغییر ندهد، اقدام به حمله برای بازیکن۱ پاداش بیشتری به همراه داشته باشد.
- اگر انتخاب بازیکن۱ همچنان اقدام به حمله باشد، استراتژی " تلافی درهرصورت" نسبت به هر یک از سه استراتژی ممکن دیگر برای بازیکن۲ پاداش بیشتری را نتیجه دهد. این شرایط در روابط (۳) تا (٦) بیان شده است.

$$P1(\text{attack}) > P1(\text{no attack}) \quad (۳)$$

$$P2(\text{response}) > P2(\text{no response}) \quad (٤)$$

$$P2(\text{response}) > P2(\text{response if attack success}) \quad (٥)$$

$$P2(\text{response}) > P2(\text{response if attack no success}) \quad (٦)$$

بر اساس مدل بازی و میزان پاداش در جدول (۲)، پاداش بازیکن۱ اگر حمله نکند برابر با مقدار ۳ خواهد بود، بنابراین برای سمت چپ رابطه (۳) داریم: **P1(no attack)= ۳**. اما برای محاسبه **P1(attack)** در رابطه (۳) با توجه به آن‌که استراتژی بازیکن۱ حمله و استراتژی بازیکن۲ تلافی درهرصورت (پیروزی یا شکست حمله اولیه بازیکن۱) است مقدار متغیرهای **PA1**، **PRS2** و **PRF2** را برابر یک قرار داده و مقادیر **X** و **Y** نیز از جدول (۲) جایگذاری می‌شود. درنتیجه رابطه (۳) به‌صورت زیر قابل بازنویسی است:

$$PA1=0 \rightarrow P1(\text{no attack}) = 3$$

$$PA1=1, PRS2=1, PRF2=1$$

$$P1(\text{attack}) = PS1*PS2+5*PS1-PS2+1$$

$$P1(\text{attack}) > P1(\text{no attack})$$

$$PS1*PS2+5*PS1-PS2+1 > 3$$

$$PS2 < \frac{2-5*PS1}{PS1-1} \quad (۷)$$

با حل نامعادله فوق برحسب **PS2** رابطه (۷) به دست می‌آید که یکی از دو شرط لازم برای وجود تعادل در این استراتژی پروفایل است. برای به دست آوردن شرط دوم ابتدا رابطه (٤) را در نظر می‌گیریم و با مقدار گذاری **PA1**، **PRS2**، **PRF2**، **X** و **Y** در آن و حل نامعادله حاصل، رابطه (۸) به دست می‌آید:

$$PA1=1, PRS2=1, PRF2=1$$

$$P2(\text{response}) = PS1*PS2+PS2-5*PS1+5$$

$$PA1=1, PRS2=0, PRF2=0$$

$$P2(\text{no response}) = 4-3*PS1$$

$$P2(\text{response}) > P2(\text{no response})$$

[Downloaded from ic4i-journal.ir on 2026-11-18]

PS1*PS2+PS2-5*PS1+5 > 4-3*PS1

$$PS2 > \frac{2*PS1-1}{1+PS1} \qquad (۸)$$

به ترتیب فوق برای رابطه (۵) نیز به‌صورت زیر عمل می‌شود تا رابطه (۹) نتیجه شود:

PA1=1, PRS2=1, PRF2=1

P2(response) = PS1*PS2+PS2-5*PS1+5

PA1=1, PRS2=1, PRF2=0

P2(response if attack success) = 2*PS1*PS2 – 4*PS1+4

P2(response) > P2(response if attack success)

PS1*PS2+PS2-5*PS1+5 > 2*PS1*PS2 – 4*PS1 + 4

PS2 > 1/2 (۹)

و درنهایت آخرین شرط در رابطه (٦) بیان شده است که با قرار دادن مقدار متغیرها در آن رابطه (۱۰) به دست خواهد آمد:

PA1=1, PRS2=1, PRF2=1

P2(response) = PS1*PS2+PS2-5*PS1+5

PA1=1, PRS2=0, PRF2=1

P2(response if attack no success) = PS2-PS1*PS2-4PS1+5

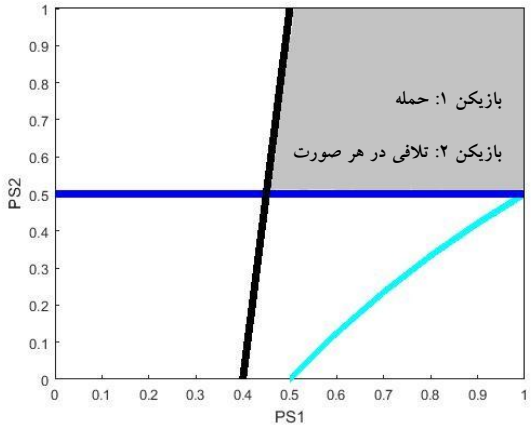
P2(response) > P2(response if attack no success)

PS1*PS2+PS2-5*PS1+5 > PS2-PS1*PS2-4PS1+5

PS2 > -1 (۱۰)

در نمودار شکل (۲) ناحیه مشترک بین روابط (۷) تا (۱۰) یعنی منطقه‌ای که همه شرایط لازم در آن برقرار می‌باشد نشان داده‌شده است، بنابراین در حالتی که استراتژی بازیکن۱ "حمله" و استراتژی بازیکن۲ "تلافی درهرصورت" باشد، این ناحیه می‌تواند ناحیه تعادل بازی باشد.

همان‌طور که در شکل مشاهده می‌شود وقتی شانس موفقیت برای بازیکن۱ بیش از ٤۰٪ است او ترجیح خواهد داد که حمله کند. در این شرایط اگر شانس موفقیت در حمله متقابل برای بازیکن۲ بیش از ۵۰٪ باشد برای او بهترین گزینه "تلافی درهرصورت" خواهد بود. در چنین شرایطی پیش‌بینی مدل ما این است که هر دو بازیکن رویکردی تهاجمی را انتخاب خواهند کرد.



شکل (۲) -تعادل نش در استراتژی (حمله، تلافی درهرصورت)

یک حالت دیگر برای استراتژی‌های انتخابی بازیکن‌ها آن است که بازیکن۱ حمله را انتخاب کند و در مقابل بازیکن۲ تنها در صورت پیروزی بازیکن۱ تصمیم به تلافی بگیرد. در این حالت مقدار پارامترهای احتمالی برابر است با: (**PA1=1, PRS2=1, PRF2=0**). مشابه حالت قبل، برای آن‌که این ناحیه از بازی تعادل نش باشد می‌بایست هم‌زمان شرایط زیر برقرار باشد:

P1(attack) > P1(no attack) (۱۱)

P2(response if attack success) > P2(response) (۱۲)

P2(response if attack success) > P2(no response) (۱۳)

P2(response if attack success) > P2(response if attack no success) (۱٤)

با جایگذاری مقدار متغیرهای **PA1**، **PRS2**، **PRF2**، **X** و **Y** در تابع پاداش بازیکن۱ و بازیکن۲ و سپس مقدار حاصل در روابط (۱۱) تا (۱٤) خواهیم داشت:

$$PS2 < \frac{4 * PS1 - 1}{2 * PS1} \qquad (۱۵)$$

PS2 > -1 (۱٦)

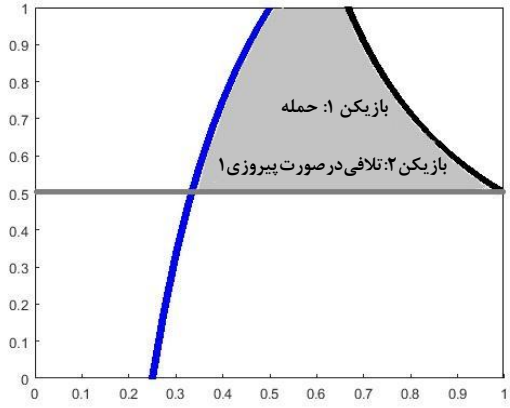
PS2 > 1/2 (۱۷)

$$\boldsymbol{PS2 < \frac{1}{3PS1 - 1}} \qquad (۱۸)$$

در نمودار شکل (۳) ناحیه مشترک بین روابط (۱۵) تا (۱۸) نشان داده‌شده که در آن همه شرایط برای وجود تعادل نش برقرار است، بنابراین در حالتی که استراتژی بازیکن۱ حمله، و

[Downloaded from ic4i-journal.ir on 2026-11-18]

استراتژی بازیکن۲ "تلافی فقط در صورت پیروزی حمله بازیکن۱" است، این ناحیه می‌تواند ناحیه تعادل بازی باشد.



شکل(۳) -تعادل‌نش در استراتژی(حمله، تلافی در صورت پیروزی ۱)

شکل (۳) نشان می‌دهد که وقتی استراتژی بازیکن۲ "تلافی در صورت پیروزی حمله بازیکن۱" باشد، بازیکن۱ با شانس توفیق کمتر هم (نسبت به استراتژی "تلافی درهرصورت" بازیکن۲) برای حمله انگیزه خواهد داشت. زیرا اگر حمله‌اش با شکست مواجه شود خطر تلافی او را تهدید نخواهد کرد. این شرایط تا زمانی که شانس موفقیت بازیکن۱ در حدود متوسط قرار دارد، طرفین را ارضاء می‌کند. بنابراین هیچ‌یک از آن‌ها رویه خود را تغییر نخواهد داد. اما وقتی شانس موفقیت بازیکن۱ از این حدود فراتر می‌رود و بازیکن۲ هم دارای شانس خوبی برای پیروزی در حمله متقابل می‌شود (گوشه بالا و سمت راست شکل ۳) آنگاه بازیکن۲ تصمیم خواهد گرفت که استراتژی خود را به "تلافی درهرصورت" تغییر دهد. این نتیجه را می‌توان با بررسی شکل‌های (۲) و (۳) به دست آورد.

با همین روال می‌توان بقیه مناطق را ازنظر وجود تعادل نش موردبررسی قرار داد و شرایط آن را به دست آورد. جدول (۳) وجود تعادل نش به ازای استراتژی‌های مختلف دو بازیکن را نشان می‌دهد. در ردیف ۳ این جدول به ازای استراتژی‌های انتخابی تعادل نش ندارد زیرا بین شرایط ذکرشده هیچ منطقه مشترکی وجود ندارد و در ردیف ٤ نیز علت عدم وجود تعادل آن است که یکی اعمال یکی از شرایط چهارگانه فرضیات مسئله را نقض می‌کند (**PS2<-1**).

٤. تحلیل مدل در حالت استراتژی مختلط

یک استراتژی مختلط انتصاب یک احتمال به هر استراتژی خالص است. این استراتژی به یک بازیکن اجازه می‌دهد به‌صورت تصادفی یک استراتژی خالص را برگزیند. چون احتمال‌ها پیوسته هستند استراتژی‌های مختلط نامتناهی برای یک بازیکن وجود دارد، حتی اگر مجموعه استراتژی‌های آن متناهی باشد.

جدول (۳)- نواحی مختلف بازی (استراتژی‌های ممکن) و بررسی تعادل نش برای آن‌ها

ردیف	استراتژی بازیکن۱	استراتژی بازیکن۲	شروط لازم برای تعادل نش		تعادل نش
۱	حمله PA1=1	تلافی درهرصورت PRS2=1 PRF2=1	$PS2 < \frac{2-5*PS1}{1-PS1}$ PS2 > 1/2	$PS2 > \frac{2*PS1-1}{1+PS1}$ PS2 > -1	دارد
۲	حمله PA1=1	تلافی در صورت پیروزی حمله ۱ PRS2=1 PRF2=0	$PS2 < \frac{4*PS1-1}{2*PS1}$ PS2 > -1	PS2 > 1/2 $PS2 < \frac{1}{3PS1-1}$	دارد
۳	حمله PA1=1	تلافی در صورت شکست حمله ۱ PRS2=0 PRF2=1	$PS2 < \frac{2-4*PS1}{PS1-1}$ PS2 > 1/2	PS2 > -1 $PS2 > \frac{1}{3PS1-1}$	ندارد
۴	حمله PA1=1	عدم تلافی درهرصورت PRS2=0 PRF2=0	$PS1 > -1$ PS2 < 1/2	$PS2 > \frac{2*PS1-1}{1+PS1}$ PS2<-1	ندارد

[Downloaded from ic4i-journal.ir on 2026-11-18]

برای در نظر گرفتن استراتژی مختلط در این مدل مقدارهای متفاوتی در بازهٔ مجاز صفر تا یک به متغیرهای احتمالی **PA1**، **PRS2** و **PRF2** نسبت داده می‌شود و سپس خروجی‌های مدل محاسبه و تحلیل می‌شود. به‌عنوان‌مثال فرض کنید بازیکن۱ قبل از تصمیم‌گیری برای اقدام به حمله شرایط را بررسی کرده و برآوردهای زیر را به دست آورده است:

- شانس او برای پیروزی در حمله ٦٠٪ است. (**PS1=0.6**)
- در صورت پیروزی او ٨٠٪ احتمال دارد بازیکن۲ تلافی کند. (**PRS2=0.8**)
- در صورت شکست او ٦٠٪ احتمال دارد بازیکن۲ تلافی کند. (**PRF2=0.6**)
- شانس پیروزی بازیکن۲ در حمله تلافی‌جویانه ٦٠٪ است. (**PS2=0.6**)

اکنون بازیکن۱ باید تصمیم بگیرد که آیا اقدام به حمله در این شرایط به نفع او هست یا نه؟ ارائه اطلاعات فوق به مدل در دو حالت حمله (**PA1=1**) و عدم حمله (**PA1=0**) نشان می‌دهد که انجام حمله سود بیشتری را نصیب بازیکن۱ خواهد کرد. بنا براین به او پیشنهاد می‌شود که حمله را آغاز کند.

جدول (٤) روند تابع پاداش بازیکن۱ را به ازای تصمیم برای حمله یا رها کردن آن، با توجه به شرایط خودی و حریف نشان می‌دهد. بدیهی است هر جا روند تابع پاداش صعودی است اقدام به حمله پیشنهاد می‌شود و در بقیه موارد توصیه می‌شود همان‌طور که در جدول نشان داده شده است، وقتی احتمال پیروزی بازیکن۱ (**PS1**) از ٦٠٪ عبور می‌کند اقدام به حمله باعث افزایش پاداش خواهد شد، درنتیجه در این شرایط باید منتظر حمله بازیکن۱ بود.

جدول (٥) میزان تغییرات تابع پاداش بازیکن۱ را به ازای افزایش احتمال پاسخ بازیکن۲ در برابر حمله موفق بازیکن۱ نشان می‌دهد. ازآنجاکه تابع پاداش بازیکن۲ قرینه تابع پاداش بازیکن۱ است (بازی مجموع صفر) بنابراین می‌توان مقدار تابع پاداش بازیکن۲ را از مقدار تابع پاداش بازیکن۱ به دست آورد.که حمله صورت نگیرد.

همان‌طور که در جدول نشان داده شده است، وقتی احتمال پیروزی بازیکن۱ (**PS1**) از ٦٠٪ عبور می‌کند اقدام به حمله باعث افزایش پاداش خواهد شد، درنتیجه در این شرایط باید منتظر حمله بازیکن۱ بود.

جدول (۴) – روند تابع پاداش بازیکن۱ به ازای تغییرات PA1

ردیف	PA1	PS1	PRS2	PRF2	PS2	PAYOFF1	روند تابع پاداش ۱
1	0-1	.2	.4	.3	.8	3-2.1	↓
2	0-1	.2	.4	.3	.4	3-2.3	↓
3	0-1	.2	.4	.3	.2	3-2.35	↓
4	0-1	.2	.8	.3	.2	3-2.4	↓
5	0-1	.2	.8	.6	.2	3-2.1	↓
6	0-1	.2	.8	.6	.6	3-1.8	↓
7	0-1	.4	.8	.6	.6	3-2.55	↓
8	0-1	.55	.9	.6	.8	3-2.86	↓
9	0-1	.6	.8	.6	.6	3-3.3	↑
10	0-1	.8	.8	.6	.6	3-4.1	↑
11	0-1	.8	.4	.6	.6	3-4.15	↑
12	0-1	.8	.4	.6	.8	3-4	↑
13	0-1	.8	.9	.6	.8	3-3.75	↑

[Downloaded from ic4i-journal.ir on 2026-11-18]

جدول (۵)- روند تابع پاداش بازیکن۱ به ازای تغییرات PRS2

ردیف	PS1	PRS2	PRF2	PS2	PAYOFF1	روند تابع پاداش ۱
1	.3	0-1	.2	.4	2.7-2.76	↑
2	.3	0-1	.6	.4	2.31-2.37	↑
3	.3	0-1	.6	.5	2.25-2.25	→
4	.3	0-1	.8	.55	2.032-2.002	↓
5	.6	0-1	.2	.55	3.675-3.615	↓
6	.6	0-1	.2	.7	3.67-3.42	↓
7	.8	0-1	.2	.7	4.34-4.01	↓
8	.8	0-1	.2	.45	4.34-4.42	↑
9	.2	0-1	.2	.45	2.368-2.387	↑
10	.2	0-1	.8	.45	1.672-1.692	↑

جدول (۵) میزان تغییرات تابع پاداش بازیکن۱ را به ازای افزایش احتمال پاسخ بازیکن۲ در برابر حمله موفق بازیکن۱ نشان می‌دهد. ازآنجاکه تابع پاداش بازیکن۲ قرینه تابع پاداش بازیکن۱ است (بازی مجموع صفر) بنابراین می‌توان مقدار تابع پاداش بازیکن۲ را از مقدار تابع پاداش بازیکن۱ به دست آورد.

نکته جالب‌توجه در جدول (۵) آن است که در ردیف‌های ۱ و ۲ و ۸ تا ۱۰ اگر بازیکن۲ احتمال تلافی خود را در برابر بازیکن۱ افزایش دهد درواقع باعث افزایش مقدار تابع پاداش رقیب خواهد شد. درنتیجه در چنین شرایطی بهتر است استراتژی او عدم تلافی در برابر حمله بازیکن۱ باشد. در بقیه موارد افزایش احتمال تلافی، پاداش بازیکن۱ را کاهش خواهد داد که این روند مورد انتظار است.

جدول (٦) بیانگر آن است که در تمامی شرایط افزایش احتمال تلافی در برابر حمله منتهی به شکست بازیکن۱ باعث افزایش پاداش بازیکن۲ خواهد شد؛ بنابراین توصیه دائمی به بازیکن۲ آن است که در برابر حملات شکست‌خورده بازیکن۱ استراتژی تلافی را انتخاب کند.

جدول‌های (۷) و (۸) اثر افزایش احتمال پیروزی در حمله را بر رو پاداش بازیکنان نمایش می‌دهد. همان‌طور که کاملاً قابل پیش‌بینی است افزایش احتمال پیروزی به‌طور مستقیم باعث افزایش تابع پاداش خواهد شد. بر این اساس توصیه همیشگی به دو بازیکن این خواهد بود که توانایی خود را در تهاجم سایبری افزایش دهند.

۵. نتیجه‌گیری

مدل ارائه‌شده در این کار تلاش می‌کند تا بر چالش تصمیم‌گیری طرفین در یک درگیری سایبری غلبه کند. برای تصمیم‌گیری می‌بایست شرایط مؤثر مورد ارزیابی قرار گیرد. در این مدل پارامترهایی برای ارزیابی شرایط ارائه گردید که هرچند برای تعیین دقیق مقدار آن‌ها چالش‌هایی وجود دارد ولی با تخمین این پارامترها می‌توان از آن‌ها به‌عنوان ورودی‌های مدل استفاده کرد.

جدول (۶)- روند تابع پاداش بازیکن۱ به ازای تغییرات PRF2

ردیف	PS1	PRS2	PRF2	PS2	PAYOFF1	روند تابع پاداش ۱
1	.2	.8	0-1	.45	2.6-1.45	↓
2	.2	.2	0-1	.45	2.6-1.45	↓
3	.2	.2	0-1	.2	2.6-1.7	↓
4	.4	.2	0-1	.2	3.25-2.55	↓
5	.6	.2	0-1	.2	3.87-3.4	↓
6	.8	.2	0-1	.2	4.5-4.25	↓
7	.8	.2	0-1	.8	4.3-3.95	↓
8	.8	.2	0-1	.1	4.52-4.32	↓
9	.8	.8	0-1	.1	4.91-4.69	↓

[Downloaded from ic4i-journal.ir on 2026-11-18]

جدول (۷)- روند تابع پاداش بازیکن۱ به ازای تغییرات PS1

ردیف	PS1	PRS2	PRF2	PAYOFF1	روند پاداش ۱
1	0-1	.7	.4	1.4-4.8	↑
2	0-1	.7	.4	1.4-4.5	↑
3	0-1	.7	.8	.5-4.5	↑
4	0-1	.9	.8	.5-4.5	↑
5	0-1	.9	.8	1-5.5	↑

جدول (۸)- روند تابع پاداش بازیکن۱ به ازای تغییرات PS2

ردیف	PS1	PRS2	PRF2	PS2	PAYOFF1	روند پاداش ۱
1	.2	.9	.8	0-1	2.1-1.1	↓
2	.4	.9	.8	0-1	3.1-1.9	↓
3	.4	.6	.8	0-1	2.95-2	↓
4	.4	.6	.4	0-1	3.2-2.5	↓
5	.8	.6	.4	0-1	4.8-3.8	↓

نتایج حاصل از مدل نشان داد که از آن می‌توان برای تخمین تصمیم طرفین استفاده کرد. علاوه بر این در مثال‌های ارائه‌شده نشان داده شد که این مدل به‌عنوان یک ابزار مبتنی بر نظریه بازی، می‌تواند به ازای شرایط متفاوت استراتژی مناسب را به هر یک از بازیکن‌ها ارائه دهد.

هرچند برخی نتایج حاصل از مدل با انتظارات و پیش‌فرض‌های اولیه تطبیق دارد، اما در مواردی نتایج کاملاً جالب‌توجه و غیرمنتظره است. مثل زمان‌هایی که تصمیم برای تلافی در مقابل حمله حریف باعث افزایش پاداش او می‌شود. وجود متغیرهای **x** و **y** این امکان را فراهم می‌کند که در مورد بازیکنان و سناریوهای حمله متفاوت بتوان با محاسبه هزینه و سود ناشی از حمله مقدارهای مختلفی برای پاداش بازیکن‌ها در نظر گرفت.

یک مسئله مهم در این کار نحوه برآورد متغیرهای احتمالی است. هرچند در اینجا به عوامل مؤثر بر هر یک از این متغیرها اشاره شده است اما در ادامه لازم است تحقیقات بیشتری برای نحوه برآورد توان تهاجم سایبری و سایر متغیرهای احتمالی انجام شود.

مراجع

[۱] **Symantec“ ,ISTR, Internet Security Threat Report ”, 2018.**

[۲] **Sankardas Roy, "A Survey of Game Theory as Applied to Network Security," in *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 2010.**

[۳] **M. H. K. S. a. J. H. Kathryn Merrick“ ,* A Survey of Game Theoretic Approaches to Modelling Decision-Making in Information Warfare Scenarios ”,*Future Internet* ,۸ جلد ,p. 34, 2016.**

[٤] **T. M. a. A. D. P. Allan Friedman“ ,The Dynamics of US Cybersecurity Policy Priorities ”,Center for Research on Computation & Society,Harvard University, 2010.**

[٥] **Robert Axelrod“ ,The Timing of Cyber Conflict ”, PNAS (Proceedings of the National Academy of Sciences of the United States of America.2014 ,(**

[٦] **J. Hua و S. Bapna“ ,The economic impact of cyber terrorism ”,*The Journal of Strategic Information System* ,۲۲ جلد ,pp. 175-186, 2013.**

[۷] **J. Hua و S. Bapna“ ,Who CanWe Trust?: The Economic Impact of Insider Threats ”,*J. Glob. Inf. Technol. Manag* ,١٦ جلد ,pp. 47-67, 2013.**

[۸] **A. Bensoussan, M. Kantarcioglu و S. Hoe“ ,A game-**

[Downloaded from ic4i-journal.ir on 2026-11-18]

theoretical approach for finding optimal strategies in a botnet defense model ",***Decision and Game Theory for Security; Springer*** ,pp. 135-148, 2010**.

[۹] **O. T. H. X. Aaron Schlenker" ,Deceiving Cyber Adversaries: A Game Theoretic Approach** در ۱۷ **"**,***th International Conference on Autonomous Agents and Multiagent Systems*** ,Stockholm,, 2018**.

[۱۰] **Y. Sagduyu, R. Berry** و **A. Ephremides" ,Jamming games in wireless networks with incomplete information "**,***IEEE Commun. Mag*** ،٤٩ جلد ,pp. 112-118, 2011**.

[۱۱] **Z. Chen, C. Qiao, Y. Qiu, L. Xu** و **W. Wu" ,Dynamics stability in wireless sensor networks active defense model "**,***Journal of Computer and System Sciences*** جلد ,**
،۸۰pp. 1434-1548, 2014**.

[۱۲] **M. Zhang, Z. Zheng** و **N. Shroff" ,A Game Theoretic Model for Defending Against Stealthy Attacks with Limited Resources "**,***Decision and Game Theory for Security; Springer*** ,pp. 93-112, 2015**.

[۱۳] **.۱A. F. S. F. a. R. A. Benjamin Edwardsa" ,Strategic aspects of cyberattack, attribution, and blame "**,***PNAS (National Academy of Sciences of the United State of America*** ،١٤ جلد ,pp. 2825-2830, 2017**.

[Downloaded from ic4i-journal.ir on 2026-11-18]