مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال ششم، شماره ۲، تابستان ۱۳۹۷، ص ۲۸-۲۱

مدل تصمیم‌گیری در یک درگیری سایبری مبتنی بر آسیب‌پذیری، با رویکرد نظریه بازی

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

۱- دانشجوی دکتری، دانشگاه جامع امام حسین (ع) ۲- دکتری هوش مصنوعی، دانشگاه صنعتی امیرکبیر، ۳- استادیار، دانشگاه جامع امام حسین (ع)
(دریافت: ۹۵/۱۲/۲۰، پذیرش: ۹۶/۰۶/۱۶)

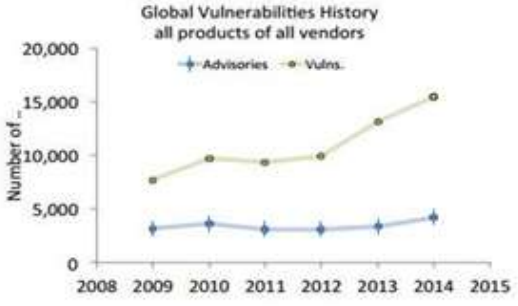
چکیده

در یک جنگ سایبری پیش‌بینی تصمیم‌های احتمالی دشمن برای هر یک از طرفین، یک مسئله حیاتی و بحرانی است. در این مقاله با استفاده از نظریه بازی و ساخت یک مدل تحلیلی، فرآیند تصمیم‌گیری دو حریف در فضای سایبری، هنگام کشف یک آسیب‌پذیری، مورد بررسی قرارگرفته است. در مقایسه باکارهای پیشین، مفروضات مسئله به شرایط واقعی نزدیک شده و احتمال تلافی طرف مقابل، نامتقارن بودن پاداش حمله و احتمال شکست حمله در تعریف بازی لحاظ شده است. به این منظور ساختار جدیدی برای درگیری احتمالی موردنظر طراحی‌شده که نسبت به کارهای پیشین شباهت بیشتری به ساختار درگیری سایبری در شرایط واقعی دارد. برای نمایش بازی از شکل توسعه‌یافته استفاده‌شده و تعادل نش برای آن محاسبه گردیده است. در انتها با تحلیل نتایج نشان داده‌شده که در شرایطی که توانایی طرفین در اجرای حمله سایبری به هم نزدیک باشد، هر دو طرف اقدام تهاجمی را انتخاب خواهند کرد و توانایی کشف آسیب‌پذیری تأثیر کمتری در انتخاب راهبرد دارد.

واژه‌های کلیدی: نظریه بازی، آسیب‌پذیری، راهبرد، توانایی حمله، دفاع سایبری

۱- مقدمه

در سال‌های اخیر استفاده از آسیب‌پذیری‌ها به ابزاری رایج در درگیری‌های سایبری تبدیل‌شده و روند جاری نشان‌دهنده رشد استفاده از آسیب‌پذیری‌ها است. از سوی دیگر هنوز هیچ روش قطعی برای تشخیص همه آسیب‌پذیری‌های نرم‌افزاری در یک سیستم وجود ندارد. رشد حملات مبتنی بر آسیب‌پذیری در سال‌های اخیر اهمیت چنین مطالعاتی را بیشتر می‌کند. بر اساس آمارهای موجود در سال ۲۰۱۳ میلادی ۹۶٪ از برنامه‌های کاربردی به‌طور میانگین دارای ۱۴ آسیب‌پذیری بوده‌اند [۱]. شکل (۱) روند افزایش آسیب‌پذیری در نرم‌افزارها را نشان می‌دهد:



شکل (۱): روند افزایش آسیب‌پذیری [۲]

در چنین شرایطی طرفین رقیب در فضای سایبری سعی خواهند کرد آسیب‌پذیری‌های موجود در سامانه‌ها را شناسایی کنند تا از آن‌ها برای تهاجم علیه حریف و یا ایمن‌سازی سیستم خود، استفاده کنند. 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 راهبرد تهاجمی یا دفاعی روی آورد. در این وضعیت مطالعه نحوه تعامل دو رقیب که هرکدام منابعی از آسیب‌پذیری در سیستم طرف مقابل در اختیاردارند و برآورد تصمیم آن‌ها در استفاده یا عدم استفاده از منابع به‌منظور انجام تهاجم و یا تقویت امنیت خود می‌تواند راهگشا باشد. قابلیت مدل کردن اعمال یک دشمن هوشمند و یک مدافع در پاسخ به او، یک بخش مهم و رو به گسترش از تحقیقات 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 بازی‌ها 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 [۳].

* رایانامه نویسنده مسئول: m.bagheri@ihu.ac.ir

کاربرد نظریه بازی برای امنیت سامانه‌های سایبری یک بخش فعال طی یک دهه گذشته بوده است.

کارهایی که اخیراً با استفاده از نظریه بازی در حوزه امنیت سایبری انجام‌شده با چالش‌هایی مثل اطلاعات ناقص برای بازیکن‌ها و عدم قطعیت همراه بوده است. در این کارها معمولاً یک‌طرف به‌عنوان مدافع و طرف مقابل به‌عنوان مهاجم در نظر گرفته‌شده و یک مدل مبتنی بر بازی مدافع-مهاجم شکل‌گرفته است درحالی‌که در یک درگیری سایبری واقعی ممکن است در شرایطی هر دو طرف تمایل به تهاجم داشته باشند. در این کار تلاش شده تا با توجه به این موارد مدلی ارائه شود که به شرایط واقعی نزدیک‌تر باشد. در ادامه ابتدا به برخی کارهای انجام‌شده در این حوزه اشاره خواهد شد. سپس در بخش ۳ مسئله و فرضیات آن بیان می‌شود. بخش ۴ به مدل‌سازی بازی، تشریح پارامترها و چگونگی یافتن نقطه تعادل بازی اختصاص‌یافته است. در بخش ۵ نتایج به‌دست‌آمده مورد ارزیابی و تحلیل قرارگرفته است و درنهایت بخش ۶ شامل پیشنهادهایی برای کارهای آینده است.

۲- پیشینه

اگرچه نظریه بازی ابتدا برای حل مسائل رقابتی در اقتصاد و سیاست بکار گرفته شد و توسعه یافت، اما در سال‌های اخیر مورد اقبال محققین در علوم تجربی و مهندسی قرارگرفته است. کاربردهای ابتدایی آن در حوزه امنیت سایبری به حدود سال ۲۰۰۵ بازمی‌گردد. جورموکا اولین بار چند مثال از بازی‌های استاتیک با اطلاعات کامل ارائه کرد که هر مثال نشان‌دهنده یک سناریو جنگ اطلاعات است [۴]. برای هر مثال نویسنده با تعریف بازی و مؤلفه‌های آن (ازجمله تابع پاداش) بهترین راهبرد بازیکنان را در یک شکل کمی پیدا کرد. در این مثال‌ها آن‌ها به‌طور ویژه به بررسی این سؤال پرداختند که آیا بیش از یک نقطه تعادل نش[1] وجود دارد؟ و اگر چنین است وقوع کدام‌یک از آن‌ها با توجه به راهبرد بازیکنان محتمل‌تر است. این مثال‌ها نشان می‌دهند که بازیکنان می‌توانند بر اساس سناریو از یک راهبرد متهورانه و یا یک راهبرد ترکیبی منفعت ببرند. کارین و همکارانش یک رویکرد محاسباتی از برآورد خطر کمی برای سرمایه‌گذاری راهبردهای مؤثر در امنیت شبکه ارائه کردند [۵]. لی یک مدل بازی برای امنیت شبکه کامپیوتری پیشنهاد داده که در آن یک شبکه سازمانی به‌صورت یک گراف با ۴ گره، شامل سرویس‌دهنده‌های وب و فایل و ایستگاه‌های کاری، تصور شده و وضعیت ترافیک برای همه پیوندها وجود دارد [۶]. این بازی دارای دو بازیکن (مهاجم و مدیر شبکه)، از نوع جمع عمومی و تصادفی است و نویسنده در آن بر روی سه سناریوی تغییر وب‌سایت[2]، منع سرویس و سرقت اطلاعات محرمانه، تمرکز نموده است.

در یک کار دیگر ژیائولین و همکارانش با در نظر گرفتن حالت‌های امنیتی اکنون و آینده یک بازی مارکوف برای برآورد خطر سیستم اطلاعات شبکه ارائه کردند [۷]. آن‌ها بیان کردند که تهدیدهایی که بر روی آسیب‌پذیری‌ها عمل می‌کنند می‌توانند خطر را تحریک کرده و آن را افزایش دهند، خطر با گسترش تهدید بزرگ و بزرگ‌تر می‌شود. از سوی دیگر خطر با اقدامات مدیر شبکه برای ترمیم آسیب‌پذیری کوچک و کوچک‌تر می‌شود. بنابراین آن‌ها یک بازی از تهدیدها و آسیب‌پذیری‌ها ترتیب دادند. اساساً آزمایش‌ها شامل یک بازی از اطلاعات کامل و سالم با دو بازیکن است. این تحقیق برای توضیح نحوه محاسبه راهبرد بهینه بازیکنان، با در نظر گرفتن یک شبکه کوچک شامل سه گره، یک مثال عددی ارائه کرد.

آلپکن و همکارانش تقابل بین مهاجمین بدخواه و سامانه تشخیص نفوذ را با استفاده از بازی تصادفی مارکوف مدل‌سازی کردند [۸]. آن‌ها عملیات سیستم حسگرهای سامانه تشخیص نفوذ را با استفاده از یک زنجیره مارکوف متناهی و در نظر گرفتن سه ساختار اطلاعاتی مختلف نشان داده‌اند: (الف) بازیکنان اطلاعات کاملی در مورد مشخصات حسگرها و دشمن دارند.(ب) مهاجم اطلاعاتی در مورد مشخصات حسگرها ندارد.(ج) هر بازیکن فقط اطلاعاتی در مورد ارزش داشته‌های خود و عمل‌های گذشته و حالت‌های قبلی دارد.

گاین و همکارانش به مسئله امنیت شبکه به‌عنوان ترتیبی از یک بازی با مجموع غیر صفر که توسط مدافع و مهاجم بازی می‌شود، نگاه کرده‌اند [۹]. این مدل بازی، "بازی جعلی"[3] نامیده شد. از روی محافظه‌کاری فرض شده که بازیکن‌ها نمی‌توانند مشاهده کاملی از اقدامات قبلی یکدیگر داشته باشند. در این تحقیق تأثیر خطای احتمالی سیستم حسگرها روی تعادل نش موردبررسی قرارگرفته و در این راه دو سناریو مدنظر قرارگرفته است: (۱) هر بازیکن از این خطاها مطلع می‌شود (۲) هیچ بازیکنی متوجه این خطاها نمی‌شود.

چن در مقاله دکتری خود یک مدل نظری بازی، برای پاسخ

1- Nash Equilibrium

2- Deface

3- Fictitious Play

به حمله اسکن کرم‌واره[1] اینترنتی ارائه کرد [۱۰]. در اینجا ایده اصلی آن است که مدافع می‌تواند با ایجاد یک برنامه کاربردی به نحوی عمل کند که هنگام شروع به کار در یک گروه توزیع‌شده در اینترنت سرعت انتشار کرم‌ها را حداقل کند. در سوی دیگر مهاجم می‌تواند از یک اسکن توزیعی بهینه به‌منظور حداکثر کردن آلودگی استفاده کند. مهاجم به دنبال راهی است که حداقل سرعت انتشار کرم را به حداکثر برساند درحالی‌که مدافع می‌خواهد حداکثر سرعت انتشار کرم را به حداقل برساند. با تعریف چارچوب، مسئله به‌صورت یک بازی مجموع صفر و یک مسئله حداقل-حداکثر[2] درمی‌آید. راه‌حل بهینه برای این مسئله آن است که مدافع باید با به‌کارگیری یک برنامه کل فضای آدرس‌های IP را به‌صورت یکنواخت پوشش دهد درحالی‌که بهترین راهبردی که مهاجم می‌تواند از آن سوءاستفاده کند راهبرد اسکن تصادفی است. این تحقیق یک چارچوب نظریه بازی برای طراحی محل میزبان‌های با ارزش بالا و آسیب‌پذیر، بر روی شبکه ارائه می‌کند. برای بهبود مدل انتشار کرم‌واره‌های اینترنتی یک کار دیگر نیز توسط نگارنده انجام‌شده است [۱۱].

مسئله حفاظت از یک سیستم با گره‌های متعدد در برابر حملات پنهانی توسط ژانگ و همکارانش موردبررسی قرارگرفته است [۱۲]. آن‌ها تعاملات بین مدافع و مهاجم را به‌صورت یک بازی با مجموع غیر صفر مدل کرده‌اند که در آن هر دو بازیکن منابع محدودی در اختیاردارند. ویژگی این کار این است که در آن‌یک مدل بازخورد نامتقارن در نظر گرفته‌شده به‌نحوی‌که حرکت‌های مدافع کاملاً قابل‌مشاهده است ولی حرکت‌های مهاجم پنهانی است. این تحقیق راهبرد بهینه را برای هر دو بازیکن تحلیل کرده و تعادل نش بازی را توصیف می‌کند.

در کاری که اخیراً توسط آقای شریفی و همکارانش ارائه شد، با استفاده از نظریه بازی اثر حملات سایبری بر بازار برق موردبررسی قرار گرفت [۱۳]. بر اساس سناریوی تعریف‌شده مهاجم سعی می‌کند با ارسال اطلاعات بد به واحدهای اندازه‌گیری بر روی فرآیند محاسبه قیمت برق تأثیر بگذارد. با تعریف مسئله به‌صورت بازی دونفره مجموع صفر، مدل ریاضی عملکرد مهاجم و مدافع برای یافتن بهترین راهبرد، پیشنهادشده است.

فریدمن و همکارانش فرآیند تصمیم‌گیری دو رقیب را در فضای سایبری و هنگام کشف یک آسیب‌پذیری در قالب یک بازی مدل کرده‌اند [۱۴]. طرفین در این مدل در صورت کشف یک آسیب‌پذیری می‌توانند آن را افشا کرده و به امنیت سیستم خود کمک کنند و یا آن را برای سوءاستفاده در آینده نزد خود مخفی نگه‌دارند. مدل آن‌ها شامل یک بازی مجموع صفر است که در آن پاداش طرفین متقارن است. در نظر نگرفتن واکنش رقیب و حتمی فرض کردن پیروزی در حمله، ازجمله شرایط محدودکننده مسئله در این کار است که تا حدودی آن را از فضای واقعی دور می‌کند.

عمده کارهای پیشین که از نظریه بازی در حوزه امنیت سایبری استفاده کرده‌اند، یک شبکه محدود با تجهیزات مشخص را در نظر گرفته‌اند. در همه کارها یک نقش ثابت به‌عنوان مهاجم یا مدافع در نظر گرفته‌شده که در طول بازی ثابت است و از اقدام متقابل حریف به‌عنوان یک پیامد چشم‌پوشی شده است.

۳- صورت‌مسئله

در این مسئله هدف آن است که در یک سطح راهبردی فرآیند تصمیم‌گیری طرفین در یک درگیری سایبری مدل‌سازی شود. این مدل کمک می‌کند تا بتوان روند اقدامات بعدی طرفین را تخمین زد و راهبرد بهینه را برای شرایط مختلف به آن‌ها پیشنهاد داد. 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، است.

دو حریف در فضای سایبری آسیب‌پذیری‌هایی را از یکدیگر در اختیاردارند. هنگام کشف یک آسیب‌پذیری جدید کاشف آن باید تصمیم بگیرد که از آن برای اقدام به حمله علیه رقیب استفاده کند یا برای امنیت بیشتر اطلاعات آن را منتشر نماید. رقیبی که موردحمله واقع می‌شود نیز باید در مورد اقدام متقابل تصمیم‌گیری کند. با استفاده از ابزارهای نظریه بازی و مفروضات زیر، مسئله موردبررسی قرار می‌گیرد:

- دو طرف بازی رفتاری مبتنی بر عقلانیت دارند. به‌عبارت‌دیگر، از بین عمل‌های قابل انتخاب، عملی را انتخاب می‌کنند که سود بیشتری دارد.
- بازیکن ۱ وابستگی بیشتری به زیرساخت‌های سایبری دارد و درصورتی‌که هدف حمله واقع شود دو برابر بازیکن ۲ خسارت خواهد دید. (این فرض ازآن‌جهت در نظر گرفته‌شده است که در دنیای واقعی موارد متعدد مشابهی به‌عنوان یک درگیری سایبری اتفاق افتاده است. مثلاً حمله

1- Worm
2- Min-Max

یک کشور با زیرساخت سایبری ضعیف به یک کشور با زیرساخت سایبری قوی مثل امریکا)

- در صورت حمله با استفاده از آسیب‌پذیری، احتمال اقدام متقابل طرف مقابل وجود دارد.
- در صورت اقدام به حمله، احتمال شکست نیز وجود دارد که در آن صورت پاداش منفی یا هزینه به مهاجم تحمیل خواهد شد.

با توجه به مفروضات فوق، شرایط محدودکننده در کارهای پیشین تقلیل یافته که باعث می‌شود صورت‌مسئله به فضای واقعی نزدیک‌تر شود. در نظر گرفتن احتمال انتخاب راهبرد تهاجم برای هر دو طرف و وجود پاداش نامتقارن برای بازیکن‌ها از ویژگی‌های این مسئله است که در کارهای قبلی به آن توجه نشده است.

۴- مدل‌سازی بازی

در فضای مسئله دو بازیکن با هم رقابت می‌کنند که به ترتیب بازیکن ۱ و بازیکن ۲ نامیده می‌شوند. هر بازیکن قادر است از بین دو عمل زیر راهبرد خود را تعیین کند:

A: اقدام به حمله علیه طرف مقابل. این حمله می‌تواند به‌عنوان یک حمله ابتدایی پس از یافتن یک آسیب‌پذیری باشد و یا به‌عنوان یک حمله تلافی‌جویانه پس از حمله طرف مقابل. سود ناشی از این حمله متناسب با نتیجه حمله (شکست یا پیروزی)، مرحله‌ای که حمله در آن انجام می‌شود و نوع هدف (بازیکن ۱ یا ۲) متفاوت خواهد بود.

D: بازیکن، آسیب‌پذیری نرم‌افزاری کشف‌شده را به تولیدکننده مربوطه اطلاع دهد تا بلافاصله آسیب‌پذیری اصلاح شود (از تأخیر زمانی لازم برای حل مشکل صرف‌نظر شده است) و یا آنکه در مقابل حمله حریف هیچ واکنشی نشان نداده و اقدام به حمله متقابل نمی‌کند. پاداش برای دفاع صفر است یعنی هیچ مزیت راهبردی یا خطری به ازای آن وجود ندارد.

۴-۱- پارامترها

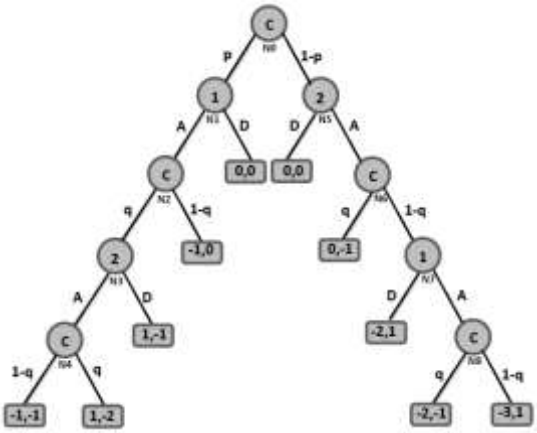
چند مشخصه کلیدی انتخاب‌شده است که مقادیر مختلف آن‌ها می‌تواند باعث تغییر در نتایج شود:

- p: با مقداری بین صفر تا یک نشان‌دهنده توان فنی بازیکن۱ در کشف یک آسیب‌پذیری است. این توان نسبت به بازیکن رقیب یعنی بازیکن۲ سنجیده می‌شود و 1-p میزان مهارت نسبی بازیکن ۲ در کشف آسیب‌پذیری است. مقدارهای کوچک p (p<0.5) نشان‌دهنده آن است که بازیکن ۱ مهارت کمتری در مقایسه با بازیکن ۲ دارد. درحالی‌که مقادیر بزرگ‌تر (p>0.5)، نشان‌دهنده این است که بازیکن ۱ دارای مهارت بیشتری است. اگر دو بازیکن مثل هم باشند، آنگاه: p=0.5. در واقع این پارامتر با یک نسبت احتمال نشان می‌دهد که کدام بازیکن قدرت بیشتری برای کسب آسیب‌پذیری دارد و با چه احتمالی زودتر آسیب‌پذیری موجود را کشف خواهد کرد.

- q: توانایی فنی بازیکن ۱ در اجرای یک تهاجم سایبری است که نسبت به بازیکن ۲ سنجیده می‌شود. این پارامتر نیز با مقادیر بین ۰ تا ۱ مقدارگذاری می‌شود و نشان‌دهنده میزان مهارت بازیکن ۱ نسبت به بازیکن ۲ برای موفقیت در یک تهاجم سایبری است. 1-q میزان مهارت بازیکن ۲ است. مقدارهای کوچک q (q<0.5) نشان‌دهنده آن است که بازیکن ۱ مهارت کمتری در مقایسه با بازیکن ۲ دارد. درحالی‌که مقادیر بزرگ‌تر (q>0.5) نشان‌دهنده مهارت بیشتر برای بازیکن ۱ است. اگر دو بازیکن مثل هم باشند آنگاه: q=0.5. مقدار q نشان می‌دهد کدام بازیکن شانس بیشتری برای موفقیت در حمله دارد.

گام‌های بازی در یک درخت در شکل (۲) 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 (A و D) مشخص‌شده است. خط بین گره شانس و فرزندانش با مقدار احتمال نشانه‌گذاری گردیده است. برگ‌های درخت که به‌صورت چهارگوش نشان داده‌شده‌اند شامل یک زوج عدد می‌باشند که اولی پاداش بازیکن ۱ و دومی پاداش بازیکن 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 دفاع (A یا D) را انتخاب کند. سرانجام وقتی به یک برگ می‌رسیم بازی تمام‌شده و بازیکنان به امتیازی که در آن برگ مشخص‌شده است، رسیده‌اند. این امتیازها بر اساس قواعد زیر به هر بازیکن نسبت داده می‌شود:

- برای حمله موفق، مهاجم پاداش ۱+ دریافت می‌کند.
- اگر حمله به بازیکن ۱ موفقیت‌آمیز باشد امتیاز منفی ۲- به او تحمیل خواهد شد. این مقدار برای بازیکن ۲ مقدار ۱- است (به دلیل فرض عدم تقارن که قبلاً به آن اشاره شد).
- مهاجم در یک حمله ناموفق امتیاز منفی ۱- را دریافت می‌کند.
- در صورت انتخاب راهبرد دفاعی امتیاز صفر دریافت خواهد شد.



شکل (۲): نمایش بازی در شکل توسعه‌یافته

بازی را می‌توان با توضیح نحوه نمایش آن توسط درخت، گام‌به‌گام پیش برد. با احتمال P بازیکن ۱ زودتر آسیب‌پذیری جدید را کشف می‌کند. در این صورت حرکت به گره N1 انجام می‌شود. در اینجا بازیکن ۱ باید بین عمل‌های A و D یکی را انتخاب کند. اگر او D را انتخاب کند هر دو بازیکن پاداش صفر را دریافت می‌کنند و بازی تمام می‌شود؛ اما اگر بازیکن ۱، حمله با استفاده از آسیب‌پذیری را انتخاب کند بازی به گره دوم شانس (N2) منتقل می‌شود. در اینجا بازیکن ۱ با احتمال 1-q ممکن است در حمله خود موفق نشود و با پاداش ۱- برای او، بازی به پایان برسد. بازیکن ۱ با احتمال q در حمله موفق خواهد شد و در این صورت بازیکن ۲ در گره N3 باید تصمیم بگیرد که چه عکس‌العملی در برابر این حمله نشان دهد. واکنش انفعالی یا دفاعی (D) پاداش ۱- را برای او و ۱ را برای بازیکن ۱ به همراه خواهد داشت؛ اما اگر بازیکن ۲ با یک راهبرد تهاجمی تصمیم به حمله سایبری متقابل بگیرد باید دید در گره شانس بعدی (N4) در این حمله موفق می‌شود یا نه؟ در صورت توفیق (با احتمال 1q-) نتیجه ۱- را به حریف تحمیل خواهد کرد و در صورت شکست پاداش ۲- به او خواهد رسید.

راهبرد تصمیم یک بازیکن برای حمله (A) یا دفاع (D) است. وقتی یک راهبرد انتخاب می‌شود، در تمام فرصت‌های تصمیم‌گیری یک بازیکن اعمال می‌شود. (در این مقاله راهبرد ترکیبی در نظر گرفته نشده است) یک زوج مرتب از راهبردهای (x,y) که $x \in \{A,D\}$ راهبرد بازیکن ۱ و $y \in \{A,D\}$ راهبرد بازیکن ۲، راهبرد- پروفایل نامیده می‌شود. سود بازیکن i برای راهبرد- پروفایل (x,y) که با $U_i(x,y)$ نشان داده می‌شود، پاداش مورد انتظار بازیکن i است وقتی بازیکن ۱ از راهبرد x و بازیکن ۲ از راهبرد y پیروی کند. برای محاسبه $U_1(A,D)$ جاییکه بازیکن ۱ تهاجمی و بازیکن ۲ تدافعی بازی می‌کند، به درخت شکل (۱) بازمی‌گردیم. بازی در N0 شروع می‌شود، با احتمال P به N1 می‌رویم جایی که بازیکن ۱، A بازی می‌کند. بازی به N2 هدایت می‌شود. بعد با احتمال 1-q به یک برگ با پاداش ۱- برای بازیکن ۱ می‌رسیم. با احتمال q به N3 می‌رویم که با برچسب بازیکن ۲ نشان‌گذاری شده است. بازیکن ۲، D بازی می‌کند که نتیجه آن پاداش ۱ برای بازیکن ۱ است.

در بازگشت به ریشه، با احتمال 1-p اولین حرکت بازی به سمت راست است که ما را به N5 می‌رساند. در ادامه بازیکن ۲، D بازی می‌کند و بازی با سود صفر برای بازیکن ۱ تمام می‌شود درنتیجه پاداش مورد انتظار برابر است با:

$$U_1(A,D) = p[(q) + (1-q)(-1)] + (1-P) \times 0$$
$$= 2pq - p$$

به‌صورت مشابه می‌توانیم پاداش مورد انتظار برای راهبرد پروفایل‌های هر دو بازیکن را محاسبه کنیم:

$$U_1(A,A) = 3pq^2 - q^2 - 4pq + 2p + 4q - 3 \quad (۱)$$

$$U_1(A,D) = 2pq - p \quad (۲)$$

$$U_1(D,A) = -2pq + 2p + 2q - 2 \quad (۳)$$

$$U_1(D,D) = 0 \quad (۴)$$

$$U_2(A,A) = -3pq^2 + 3pq + 2q^2 - p - 4q + 1 \quad (۵)$$

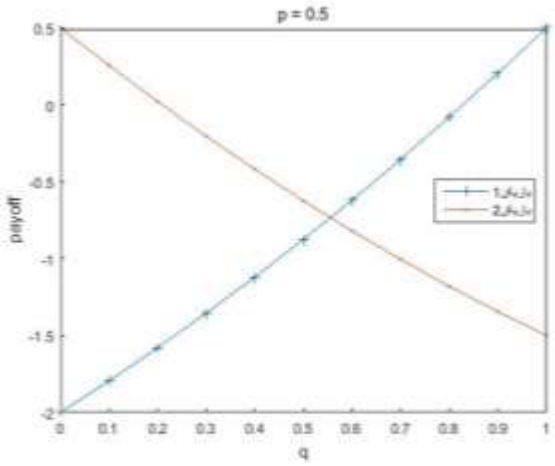
$$U_2(A,D) = -pq \quad (۶)$$

$$U_2(D,A) = 2pq - 2q - p + 1 \quad (۷)$$

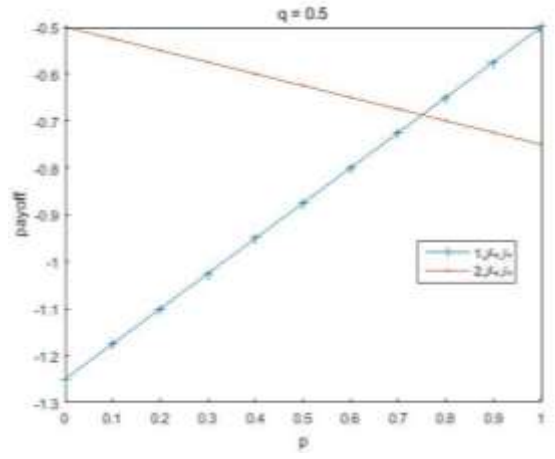
$$U_2(D,D) = 0 \quad (۸)$$

در نمودارهای ۳ و ۴ تأثیر توان نسبی کشف آسیب‌پذیری و قدرت تهاجم سایبری بر روی پاداش درزمانی که هر دو طرف

راهبرد تهاجمی را انتخاب کرده‌اند، بر اساس رابطه‌های (۱) و (۵)، نشان داده‌شده است. در شکل (۳) با فرض آن‌که طرفین مهارت یکسانی در کشف آسیب‌پذیری دارند (p=0.5)، تغییرات میزان پاداش به ازای توان تهاجم سایبری نسبت به حریف، رسم شده است. در شکل (۴) فرض بر این است که قدرت تهاجم سایبری در دو طرف برابر است (q=0.5) و تغییرات میزان پاداش بر اساس مهارت کشف آسیب‌پذیری به نمایش درآمده است.



شکل (۳): تغییرات تابع پاداش به ازای q



شکل (۴): تغییرات تابع پاداش به ازای p

همان‌طور که از شکل (۴) پیداست تلاش بازیکن ۲ برای به دست آوردن برتری در کشف آسیب‌پذیری، اثر کمی در پاداش او دارد اما در مورد بازیکن ۱ این تلاش می‌تواند پاداش او را به میزان بیشتری افزایش دهد. با مقایسه شکل‌های (۳) و (۴) می‌توان به این نتیجه رسید که برای بازیکن ۲ در چنین شرایطی بین سرمایه‌گذاری روی ارتقاء توان کشف آسیب‌پذیری و افزایش قدرت تهاجم، افزایش قدرت تهاجم اولویت بیشتری دارد زیرا اثر بیشتری بر روی پاداش او خواهد داشت.

۴-۲- یافتن تعادل

برای پیش‌بینی راهبرد انتخابی بازیکن‌ها باید نقطه تعادل بازی محاسبه شود. یک راهبرد- پروفایل یک تعادل نش نامیده می‌شود اگر هیچ بازیکنی نتواند با تغییر حرکت یک‌جانبه به بهره بیشتری دست یابد. برای آنکه راهبرد (A,A) یک تعادل نش باشد بازیکن ۱ باید ترجیح دهد که به سمت (D,A) منحرف نشود، درحالی‌که در همان زمان بازیکن ۲ باید ترجیح دهد که به سمت (A,D) منحرف نشود:

$$U_1(A,A) \geq U_1(D,A) \quad (۹)$$

$$U_2(A,A) \geq U_2(A,D) \quad (۱۰)$$

با جایگذاری مقدار تابع پاداش به رابطه‌های زیر می‌رسیم:

$$p \geq \frac{q^2-2q+1}{3q^2-2q} \quad (۱۱)$$

$$p \leq \frac{2q^2-4q+1}{3q^2-4q+1} \quad (۱۲)$$

برای آنکه راهبرد (D,A) تعادل نش باشد می‌بایست شرایط زیر برقرار باشد:

$$U_1(D,A) \geq U_1(A,A) \quad (۱۳)$$

$$U_2(D,A) \geq U_2(D,D) \quad (۱۴)$$

با جایگذاری مقدار تابع پاداش در رابطه (۱۴) رابطه (۱۵) حاصل می‌شود که فرضیات اولیه مسئله ($p\geq0$ و $q\geq0$) را نقض می‌کند. در نتیجه این راهبرد نمی‌تواند تعادل نش باشد.

$$-pq \geq 0 \quad (۱۵)$$

برای آنکه راهبرد (A,D) تعادل نش باشد می‌بایست شرایط زیر برقرار باشد:

$$U_1(A,D) \geq U_1(D,D) \quad (۱۶)$$

$$U_2(A,D) \geq U_2(A,A) \quad (۱۷)$$

با قرار دادن مقدار تابع پاداش در رابطه‌های (۱۶) و (۱۷)، رابطه‌های (۱۸) و (۱۹) حاصل می‌شود که نشان‌دهنده ناحیه‌ای از بازی است که در آن راهبرد (A,D) می‌تواند شرایط تعادل را فراهم کند.

$$q \geq 1/2 \quad (۱۸)$$

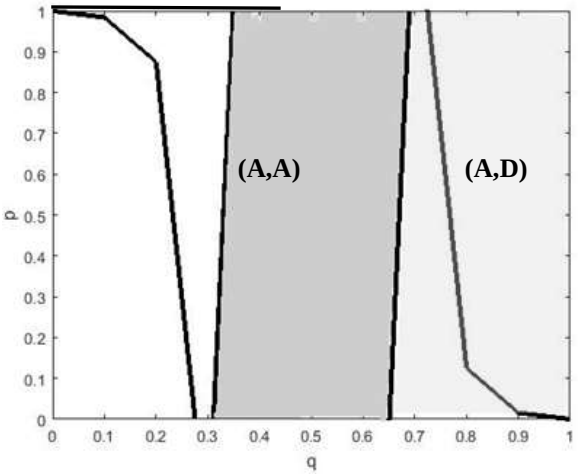
$$p \leq \frac{2q^2-4q+1}{3q^2-4q+1} \quad (۱۹)$$

برای آنکه راهبرد (D,D) تعادل نش باشد می‌بایست شرایط زیر برقرار باشد:

$$U_1(D,D) \geq U_1(A,D) \quad (۲۰)$$

$$U_2(D,D) \geq U_2(D,A) \quad (۲۱)$$

رابطه‌های بالا دو شرط زیر را محیا می‌سازد: $q \leq 1/2$ و $p \geq 1$؛ یعنی اگر کاملاً اطمینان شود که بازیکن ۱ ابتدا آسیب‌پذیری را کشف می‌کند و توان فنی او برای اجرای حمله کمتر از بازیکن ۲ باشد، آنگاه راهبرد- پروفایل (D,D) تعادل نش خواهد بود. نمودار شکل (۵) تعادل نش را برای مقادیر متفاوت p و q نشان می‌دهد.



شکل (۵): ناحیه تعادل

۵- تحلیل نتایج

بر اساس نتایج به‌دست‌آمده در شرایطی که توان فنی دو طرف در حمله سایبری به هم نزدیک باشد ($0.3 \leq q \leq 0.7$) فارغ از آنکه سطح مهارت نسبی آن‌ها در کشف آسیب‌پذیری به چه میزان باشد، هر دو طرف راهبرد تهاجمی را انتخاب خواهند کرد. با توجه به مفروضات مسئله توان فنی در اجرای یک حمله سایبری در مقایسه با مهارت نسبی یک رقیب برای کشف آسیب‌پذیری تأثیر بیشتری بر فرآیند تصمیم‌گیری طرفین در این درگیری سایبری خواهد داشت.

نکته جالب‌توجه دیگر آن است که بازیکن ۱ که با خطر خسارت بیشتر در حمله حریف روبرو است، در فضاهای گسترده‌تری از بازی راهبرد تهاجمی را انتخاب خواهد کرد و هیچ منطقه تعادلی در بازی وجود ندارد که او در مقابل راهبرد هجومی بازیکن ۲، به دفاع روی آورد.

وقتی توان نسبی اجرای تهاجم برای بازیکن ۱ نسبت به بازیکن ۲ از حد معینی فراتر رود ($q \geq 0.7$) آن‌گاه بازیکن ۲ ترجیح خواهد داد در مقابل راهبرد تهاجمی بازیکن ۱ سیاست دفاع را انتخاب کند.

نکته آخر آنکه در یک شرایط بسیار خاص که در آن توان فنی بازیکن ۱ برای انجام حمله سایبری کمتر از توان رقیب باشد و به‌طورقطع اطمینان شود که او ابتدا آسیب‌پذیری را کشف خواهد کرد یعنی شرایط حاصل از روابط (۲۰) و (۲۱) ($q \leq 1/2$ و $p \geq 1$) آنگاه راهبرد- پروفایل (D,D) فضای درگیری را به سمت تعادل خواهد برد یعنی هر دو طرف ترجیح خواهند داد که بر اساس یک سیاست دفاعی عمل کنند.

۶- نتیجه‌گیری و کارهای آینده

در این مقاله سعی شده است فرآیند تصمیم‌گیری طرفین یک درگیری سایبری با استفاده از نظریه بازی مدل شود. سپس با استفاده از این مدل نشان داده شده است که می‌توان اولویت‌های تصمیم‌گیری طرفین یک درگیری سایبری را هنگام روبرو شدن با چالش کشف یک آسیب‌پذیری، برای هر یک از طرفین و به ازای شرایط مختلف تعیین کرد. توجه به احتمال تلافی طرف مقابل و نیز نامتقارن بودن وابستگی طرفین به زیرساخت‌های سایبری مدل را به شرایط واقعی نزدیک‌تر کرده است. نتایج حاصل از مدل نشان داد در حالتی که توان تهاجمی طرفین نزدیک به هم باشد هر دو طرف تمایل به انتخاب راهبرد تهاجمی خواهند داشت و میزان مهارت آن‌ها در کشف آسیب‌پذیری تأثیر کمتری در این انتخاب دارد. میزان آسیب‌پذیری آن‌ها در برابر حملات سایبری نیز تأثیر چندانی در این انتخاب ندارد.

به‌عنوان ایده‌ای برای کارهای آینده می‌توان به بررسی نحوه تولید یک تابع پاداش بر اساس قابلیت‌های طرفین و نیز ویژگی‌های یک آسیب‌پذیری پرداخت. این کار باید به نحوی انجام شود که با تغییر شرایط میزان تابع پاداش نیز اصلاح شود. نخستین گام برای این کار شناسایی پارامترهایی است که بر روی مقدار پاداش تأثیرگذارند.

۷- مراجع

[1] cenzic, “Application Vulnerability Trends Report,” http://www.cenzic.com/, campbell, 2014.

[2] Secunia, “annual report on vulnerabilities exploited,” 2015. http://secunia.com/resources/vulnerability-review/introduction/

[3] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, “A Survey of Game Theory as Applied to Network Security,” in Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010.

[4] J. Jormakka and V. E. Molsa, "Modelling information warfare," in Journal of Information Warfare, vol. 4(2), 2005.

[5] L. Carin, G. Cybenko, and J. Hughes, "Quantitative evaluation of risk for investment efficient strategies in cybersecurity: The queries methodology," in IEEE Computer, 2008.

[6] K. Lye and J. Wing, "Game strategies in network security," in Proceedings of the Foundations of Computer Security, 2002.

[7] C. Xiaolin, T. Xiaobin, and Z. Yong, "A markov game theory-based risk assessment model for network," in International conference on computer science and software engineering, 2008.

[8] T. Alpcan and T. Baser, "An intrusion detection game with limited observations," in Proc. of the 12th Int. Symp. on Dynamic Games and Applications, 2006.

[9] C. Nguyen, T. Alpcan, and T. Baser, "Security games with incomplete information," in Proc. of IEEE Intl. Conf. on Communications(ICC), 2009.

[10] Z. Chen, "Modeling and defending against internet worm attacks," in Ph.D Dissertation at Georgia Institute Of Technology, 2007.

[11] M. Hasani and M. Forooghy, "The Study and Evaluation of the Effect of Peer-to-peer Network Users 'Behavior in Passive Worm Propagation," Padafand cyberi, 2014. (In Persian)

[12] M. Zhang, Z. Zheng, and N. Shroff, "A Game Theoretic Model for Defending Against Stealthy Attacks with," In Decision and Game Theory for Security, Springer, Berlin/Heidelberg, Germany, 2015.

[13] A. sharifi, M. Zadsar, and M. sheikholeslami, "Effects of cyber attacks on the electricity market using game theory," National Conference of Technology, Energy and Data on Electrical & Computer Engineering, Kermanshah, Iran, 2016. (In Persian)

[14] A. Friedman, T. Moore, and A. Procaccia, "The Dynamics of US Cybersecurity Policy Priorities," Center for Research on Computation & Society, Harvard University, 2010.

A Decision-Making Model in a Cyber Conflicts Acted Upon Vulnerability, Based on Game Theoretic Analysis

M. Forooghy, A. Akramizadeh, M. Bagheri*

*Imam Hossein University

(Received: 10/03/2017 , Accepted: 07/09/2017)

ABSTRACT

It is crucial to predict the other side possible actions in any conflict, especially in cyber security and cyberwars. In this paper, based on game theoretic analytical model, the decision-making process of two rivals during detection of vulnerability is discussed in cyberspace. Comparing the earlier approaches, the assumptions are made more realistic, such as possible retaliation of the opposed side, asymmetrical payoffs and risk of failure during usage of vulnerability and penetration. In order to achieve this goal, a new structure is proposed based on real conflicts in cyberwar. The proposed game is in extensive form with imperfect information in which the vulnerability is detected by chance for players. Based on Nash equilibrium concept, analytical approach proves that whenever players' ability for cyber-attack are close together, both sides will attend aggressive acts. The ability to detect vulnerabilities has less impact on strategy.

Keywords: Game Theory, Vulnerability, Strategy, Attack Ability, Cyber Defence

* Corresponding Author Email: m.bagheri@ihu.ac.ir