نشریه علمی «پدافند الکترونیکی و سایبری»
سال هفتم، شماره ۱، بهار ۱۳۹۸؛ ص ۳۸-۲۵

مدل بازدارندگی در فضای سایبر مبتنی بر گراف حمله باورهای بیزی با استفاده از ترجیحات مخاطره آفرینی

علی ملائی[۱]، مهرداد کارگری[۲*]، مجید شیخ‌محمدی[۳]، علی اکرمی‌زاده[۴]

۱- دانشجوی دکتری، دانشگاه عالی دفاع ملی، ۲ و ۳- استادیار مهندسی صنایع و سیستم‌ها، دانشگاه تربیت مدرس،
۴- استادیار مدعو، دانشگاه تهران.

(دریافت: ۹۶/۰۹/۱۶، پذیرش: ۹۷/۰۷/۲۱)

چکیده

امروزه رشد سریع وابستگی زندگی بشری به فضای سایبر توجه بیشتر دشمنان هر جامعه را به تهدیدات در این فضا برانگیخته است. حملات سایبری مختلفی که درگذشته در کشورهایی همچون استونی، گرجستان و جمهوری اسلامی ایران رخ‌داده است این هشدار را خواهد داد که آینده فضای سایبر عاری از هرگونه تهدید و حمله سایبری نخواهد بود. همیشه بازدارندگی یک موضوع بسیار مهم برای همه کشورها بوده است. در این پژوهشِ توسعه‌ای و کاربردی مدل راهبردی بازدارندگی در فضای سایبر مبتنی بر نظریه بازی‌ها ارائه خواهد شد. نظریه بازی‌ها در مدل‌سازی و تحلیل سازوکار بازدارندگی در فضای سایبر ما را یاری خواهد کرد و استنتاج‌های توصیفی و ریاضی برای تجزیه‌وتحلیل مدل به کار گرفته خواهد شد. در این پژوهش مدل راهبردی بازدارندگی در فضای سایبر در چهار مرحله شناخت وضع موجود، شناخت وضع مطلوب، تحلیل فاصله و برنامه اقدام بر اساس بازی علامت‌دهی با اطلاعات ناقص ارائه خواهد شد. در نهایت بعد از تشریح هر یک از اجزاء مدل و ارتباط آنها با یکدیگر، نشان داده شده است که مقدار تعادل بازی می‌تواند نشان‌دهنده وضعیت بازیگران در سه وضعیت منازعه، توازن و ضعف متقابل باشند و تنها در دو وضعیت توازن و ضعف متقابل بازدارندگی وجود خواهد داشت.

کلید واژه‌ها : بازدارندگی، فضای سایبر، بازی علامت‌دهی، گراف‌های حمله، تابع بهره مخاطره آفرینی

۱- مقدمه

رشد هر چه بیشتر فضای سایبر و وابستگی‌های زندگی بشری به این حوزه باعث شده است تا تهدیدات به زیرساخت‌های ملی سایبری نیز مورد توجه دشمنان هر جامعه‌ای قرار گیرد. حملات سایبری که در کشورهایی چون استونی، گرجستان و همچنین در ایران در گذشته رخ داده است به ما هشدار خواهد داد، آینده فضای سایبر عاری از حملات و تهدیدات دفاعی و امنیتی نخواهد بود. بازاندگی یکی از موضوعات اساسی در حوزه دفاعی-امنیتی هر کشور می‌باشد. در سند راهبردی پدافند سایبری جمهوری اسلامی ایران [۱] نیز بازدارندگی در ماموریت، چشم‌انداز، اهداف کلان و راهبردهای آن مورد تاکید قرارگرفته است.

نظریه بازدارندگی کلاسیک محصولی جانبی در دوران جنگ سرد می‌باشد و توسعه آن بیشتر تحت تاثیر روابط خصمانه ایالات متحده آمریکا و اتحاد جماهیر شوروی و سلاح های اتمی بوده است. بازدارندگی یک پدیده جهانی است که در همه ابعاد فرهنگی، فناوری در همه سال‌ها به‌کار گرفته می‌شود [۲]. در بازدارندگی هدف کاهش مخاطره حمله سایبری به سطح قابل پذیرش، با هزینه‌ای قابل پذیرش می‌باشد [۳].

در ابعاد کلانِ مدل تحقیق، پنج بعد اصلی سیاسی، اقتصادی، حقوقی، اجتماعی و فناوری برای تهدیدات و ارزش‌های تهدیدکننده و بازدارنده در نظر گرفته شده است. در این تحقیق تهدیدات و دارائی‌هایی مدنظر هستند که از نگاه تهدیدکننده و بازدارنده، تاثیرپذیری یا تاثیرگذاری در فضای سایبر داشته باشند.

طبیعتا امنیت در فضای سایبر یکی از مولفه‌های اصلی امنیت ملی کشور می‌باشد. از این رو تقویت و توسعه ادبیات راهبردی بازدارندگی در امنیت و دفاع سایبری به منظور بهره‌برداری سازمان‌های مسئول در پیاده‌سازی و اجرای سیاست‌های کلی فضای سایبر یکی از موضوعات پر اهمیت و اساسی می‌باشد. نبود یک زبان و شیوه مناسب برای محاسبه روابط متغیرهای بازدارندگی در فضای سایبر، درک طرفین را از محیط و اتخاذ تصمیمِ مناسب را با مشکل مواجه خواهد ساخت و پیامدها را غیرقابل پیش‌بینی می‌سازد و دقت تصمیم‌گیری‌ها را پائین می‌آورد. بنابراین، ممکن است طرفین را به یک جنگ سایبری

*رایانامه نویسنده پاسخگو: m_kargari@modares.ac.ir

سوق دهد، از این رو نبود مدل‌های دانشی برای شفاف‌سازیِ مسائل پیش‌رو می‌تواند صدمات و خسارت‌هایِ جبران‌ناپذیری را به همراه داشته باشد. این مدل می‌بایست تبیین بهتری از شناخت و برآورد اعتبار تهدیدات ارائه نماید، مخاطرات هر تهدید را شناسائی کند و راهبردهای بهینه امنیتی و دفاعی سایبری را برای بازدارندگی پیشنهاد نماید تا راهبرد و تهدید متناسب و تاثیرگذار در پاسخ به دشمن فراهم گردد.

وجود یک مدل بازدارندگی در فضای سایبر به ما کمک خواهد کرد تا درک بهتری از متغیرهای محیط منازعه داشته باشیم. این فهم مشترک سطح عقلانیت را بالا خواهد برد و در نتیجه آن احتمال حمله سایبری را کاهش خواهد داد. در این تحقیق فرض ما بر این است که نظریه بازی‌هامی‌تواند ارزیابی بهتری از متغیرهای دخیل در بازدارندگی را ارائه دهد و راه‌کارهایی را نتیجه دهد که ریسک‌پذیری تهدیدکننده را کاهش داده و او را متقاعد سازد تا از اجرای اقدام خصمانه خود منصرف شود.

در ادامه در بخش دوم، ادبیات تحقیق ارائه می‌شود. در بخش سوم مدل مفهومی بازدارندگی در فضای سایبر معرفی می‌شود. در بخش چهارم تجزیه و تحلیل مدل با استفاده از یک سناریوی وضعیتی مورد بررسی قرار می‌گیرد. در نهایت در بخش‌های پنجم و ششم نتیجه‌گیری و کارهای آینده ارائه شده است.

۲- ادبیات تحقیق

۲-۱- بازدارندگی

بازدارندگی به زبان ساده متقاعد ساختن یک حریف است بطوریکه او بداند هزینه‌های مخاطره‌ی اجرای اقدامات خصمانه خیلی بیشتر از مزایای حاصل از آن است [۴]. در مقاله [۵]. نویسنده اشاره دارد که آگاهی می‌تواند عاملی جلوگیری کننده از تهدید باشد همچنین مولفه‌هایی چون وجود تسلیحات آفندی باعث اعتبار بخشی خواهد شد و نیاز به پیمان‌های بین‌المللی در حوزه سایبر و حضور غیرنظامیان در خط مقدم جنگ سایبری بر موفقیت بازدارندگی تاثیرگذار است. نویسنده در پایان می‌نویسد: به بیانی دیگر در دنیای دیجیتالی‌شده کنونی ملتی قادر خواهد بود پیروز کارزار باشد که بتواند توانمندی‌های بالقوه خود را در جهت صحیح و با سیاستی زیرکانه به کار ببرد که بتواند با ایجاد اعتبار و قدرت کافی، خود را از گزند حملات مخرب سایبری مصون بدارد.در مقاله [۶] نویسنده معتقد است بر اساس نظریه رئالیسم ساختاری، کشورها در حوزه‌های مختلف از جمله سایبر، به تقویت قدرت تهاجمی خود ادامه خواهند داد تا بتوانند امنیت خود را ارتقا بخشند. بر این اساس، فضای سایبر به سمت نا امنی روزافزون حرکت خواهند کرد. مشخصات فضای سایبر تفاوت زیادی با فضای سنتی دارد و ضروری است تغییراتی متناسب با این موضوع در بازدارندگی اعمال شود تا بتواند در محیط جدید قابلیت کاربرد پیدا کند. از مهم ترین تغییرات مورد نیاز، می‌توان به لزوم استفاده از چهار سازوکار تلافی، انکار، گرفتارسازی و هنجار اشاره نمود.

در مقاله [۷]، قابلیت‌های بازدارندگی در سطح راهبردی و فنی مورد توجه قرار گرفته است. برخی معماری‌های راه‌کار پیشنهاد شده است و سرانجام نتیجه تحقیق در قالب یک معماری مفهومی برای بازدارندگی سایبری ارائه شده است. در تحقیق [۸]، پتانسیل حملات سایبری را که به شدت خسارات سنگینی به امنیت ملی کشور وارد می‌کند مورد کاوش قرار می‌دهد و حملات سایبری را به عنوان یک عمل جنگی تعیین می‌کند. همچنین در روشی توصیفی و تحلیلی ارائه شده است که حملات سایبری در شرایطی خاص می‌توانند به عنوان عملی در جنگ به‌کار گرفته شوند. تعریف هنجارهای بین‌المللی در فضای سایبر به بازدارندگی می‌تواند کمک کند. بازدارندگی برای دلسرد کردن تجاوزگر به‌کار می‌رود و بازدارندگی پیشنهادهایی را برای محافظت از منافع ملی ارائه می‌کند. این تحقیق تلاش می‌کند تا هنجارهای موجود بین‌المللی را برای فضای سایبر به‌کار بگیرد و همچنین چگونگی به‌کارگیری مفاهیم سنتی بازدارندگی را در فضای سایبر مورد بررسی قرار می‌دهد. بازدارندگی پیشنهادهایی را برای محافظت از منافع ملی آمریکا مطرح می‌نماید. به طور کلی بازدارندگی یک حالت ذهنی است، به نوعی مفهومی است، از نفوذ بر دیگر کشورها، برای عدم اجرای گزینه‌هایی که برخلاف منافع کشور مورد نفوذ می‌باشد.

در مقاله [۹]، به صورت تحلیلی و توصیفی اساس بازدارندگی راهبردی (بازدارندگی مرسوم، بازدارندگی هسته‌ای و بازدارندگی درخور یا مناسب) مورد بررسی قرار گرفته است. تهدیدهای رو به رشد در فضای سایبر بررسی شده‌اند و خصوصیات بازدارندگی سایبری نیز تعیین شده‌اند و بازدارندگی انکار، بازدارندگی تنبیه، تکنیک‌ها، و تعیین حدآستانه و توسعه سیاست‌های ملی مورد تحلیل و بررسی قرارگرفته است. در تحقیق [۱۰]، مدافع برای بازداری مهاجم از حملات تروریستی تکرارشونده، یک دارائی را تحت کنترل خود قرار می‌دهد و تأثیرات پویائی و نیز اجزا اساسی بازی‌های ضدتروریستی، شامل هزینه‌های دفاعی، هزینه‌های حمله و ارزشیابی سرمایه را مورد مطالعه قرار می‌دهد.

نظریه بازدارندگی بعضی از اقدامات متقابل و محرک‌ها را برای پیشگیری پیشنهاد می‌کند. بازدارندگی سایبری می‌تواند به عنوان توانمندی سازمان‌ها و موسسات برای انکار، محافظت و

اقدام متقابل علیه حملات سایبری تعریف شود [۱۱]. بازدارندگی سایبری گزینه‌های بیشتر و قابل انعطاف‌تری به نسبت روش‌های توسعه‌یافته در عصر هسته‌ای جنگ سرد در اختیار می‌گذارد. حتی بیش از اقدام تلافی‌جویانه سنتی، بازدارندگی سایبری گزینه‌هایی همچون اتخاذ اقدام قانونی، ایجاد پوشش در شبکه، مقاوم‌سازی و وابستگی متقابل را شامل می‌شود و همچنین راه‌های جدیدی را برای مشاهده و بکارگیری متدولوژی‌های پذیرفته‌شده همچون عدم آسیب‌پذیری را ارائه می‌کند [۱۲]. هدف بازدارندگی جلوگیری از اقدامات خصمانه بوسیله تضمین این امر در ذهن یک متخاصم است که تفهیم کند مخاطره عملش از مزایای آن بیشتر است، بطوریکه متخاصم عدم اقدام را ترجیح دهد [۱۲]. بازدارندگی اساساً روی تهدید یک مهاجم بالقوه با پاسخ تنبیهی به منظور بازداری از وقوع حمله تمرکز دارد. هرچند به دلیل ویژگی‌های خاص فضای سایبر، یک سیاست بازدارندگی کلی مبتنی بر تهدید اقدام تلافی‌جویانه، ممکن است برای بازدارندگی مناسب نباشد و در برخی شرایط ممکن است غیرسازنده[1] باشد. بنابراین چهار عامل اساسی شامل: ۱- جریمه (ایده آشنایی که هزینه‌های حمله را از طریق تنبیه افزایش می‌دهد)، ۲- خنثی‌سازی (ایده‌ای که از طریق مقاوم‌سازی و یا قابلیت‌های بازیابی، حملات را بی‌فایده و خنثی می‌سازد)، ۳- وابستگی (ایده‌ای از وابستگی داخلی به‌طوری‌که نفوذ را تعدیل و مدیریت می‌کند) و ۴- عدم سازندگی (ایده‌ای که یک عکس‌العمل تضمین‌شده می‌تواند از رفتار خصمانه ممانعت نماید) [۱۳]. جنبه‌های مختلفی از بازدارندگی وجود دارد، اما بازدارندگی عموماً به وسیله تهدید از دو عنصر ۱- تنبیه مهاجم به‌وسیله تحمیل کردن هزینه‌های غیرقابل‌پذیرش و ۲- جلوگیری از مهاجم از موفقیت در حمله‌اش صورت می‌پذیرد[۱۴]. بازدارندگی سایبری همانند دیگر بازدارندگی‌ها وقتی موفق خواهد شد که دشمن تصمیم به اقدام خصمانه نمی‌گیرد. این تصمیم از دو ارزیابی جداگانه پیروی می‌کند، هزینه‌های تخاصم بیشتر از مزایای آن باشد و مزایای خودداری در فضای سایبر بیشتر از هزینه‌ها باشد [۱۵].

بازدارنده در صورتی موفق خواهد شد که تهدید در سطحی باشد که هزینه‌های دشمن در صورت اجرائی کردن عمل خصمانه بیشتر از مزایای آن باشد [۹]. در مقاله [۸]. ایده اصلی بازدارندگی از نگاه وزارت دفاع "نفوذ قاطعانه بر محاسبات تصمیم‌گیری متخاصم به منظور جلوگیری از عمل خصومت‌آمیز علیه منافع حیاتی ایالات‌متحده" گفته شده است. کشور بازدارنده تصمیم می‌گیرد تا اقدامی انجام نشود زیرا آنها فهمیده‌اند یا درک کرده‌اند که انجام چنین عملی پیامدهای غیرقابل تحملی را به همراه خواهد داشت. ایده تأثیر بر تصمیمات کشورها فرض می‌کند که کشورها بازیگران عاقلی هستند، مایل‌اند تا هزینه‌های درک شده از یک عمل علیه منافع درک شده را اندازه‌گیری کنند و یک برنامه عمل انتخاب کنند به صورتی‌که این برنامه منطقاً مبتنی بر نرخ هزینه و فایده قابل استدلال می‌باشد.

بازدارندگی یک رابطه روان‌شناختی می‌باشد، هدف آن شکل‌دهی به ادراک‌های حریف، انتظارات و درنهایت تصمیمات آن درباره شروع حمله می‌باشد. بنابراین، بازدارندگی یک حریف نیاز دارد، کسی که در حال فکر کردن است یا تصور می‌کند به راحتی می‌تواند حمله کند [۱۶]. الزامات کلیدی و اساسی برای حصول قابلیت‌های مؤثر برای ایجاد راهبرد بازدارندگی مؤثر آمریکا از دیدگاه نویسندگان [۱۷]، شامل موارد زیر می‌شود: ۱- یک سیاست تدوین‌شده‌ی رسمی، محکم و شفاف مقاصد ما را برای بازداری حملات سایبری مشخص خواهد کرد، ۲- یک سامانه آگاهی موقعیتی کلان سراسری که طیف کاملی از تهدیدات سایبری و شرایطی که این تهدیدات بوجود می‌آیند را رصد کند، ۳- سیستم فرماندهی و کنترلی که مجوزهای لازم را برای پاسخ‌های چند منطقه‌ای و وطنی به تهدیدات سایبری فراهم سازد، ۴- دفاع سایبری مؤثر که نیروهای نظامی وطن آمریکا را به همراه اولویت‌هایی برای دفاع از زیرساخت‌های اساسی فراهم می‌سازد، ۵- طیف وسیعی از قابلیت‌های آفندی متقابل شامل حملات و دیگر ابزارها برای اثبات قدرت ایالات‌متحده به منظور تضمین بازدارندگی قبل، حین و بعد از بحران‌ها، ۶- هماهنگی یکپارچه بین سازمان‌های داخلی و همکاری با متحدان و شرکا در اروپا، آسیا و دیگر قاره‌ها که به خوبی توسعه‌یافته باشد، و ۷- روش‌های بازدارندگی سایبری، معیارها و تجاربی که می‌تواند به فرآیند برنامه‌ریزی کمک کند.

۲-۲- بازدارندگی و نظریه بازی‌ها

در تحقیق [۱۸]، با عنوان «یک چارچوب علامت‌دهی برای بازدارندگی تجاوز سایبری» به صورت توصیفی بدون حل مدل، اجزا چارچوب در سطح فنی تشریح شده است. بدون فرموله سازی از حل مسئله و یا چگونگی حل تعادل بازی، دسته‌بندی علامت‌ها در بازی بازدارندگی انجام‌شده است و دسته‌بندی عمل‌های مدافع و دشمن از نگاه محقق در تحقیق ارائه شده است. در [۱۹]، تحقیقی با عنوان مدل نظریه بازی‌ها از منازعه راهبردی در فضای سایبر، در قالب سؤال چگونه می‌توان ارزش وارد شدن در منازعه سایبری را به‌وسیله نظریه بازی‌ها مدل‌سازی کرد؟، منازعه سایبری را به‌عنوان یک بازی دونفره با جمع صفر در زمان گسسته که هر بازیکن یک سوءاستفاده بر طبق یک

1- Counter productive

فرآیند تصادفی کشف می‌کند، در نظر گرفته شده است. مدل‌سازی ریاضی بازی، با بازی جمع صفر با اطلاعات کامل و بررسی بازی مارکوف انجام شده است. به طور ضمنی به بازدارندگی اشاره شده است و چارچوبی برای تحلیل منازعه سایبری آورده شده است و نیز نشان داده است که در منازعه سایبری زمان انتظار اهمیت زیادی دارد و باید به طور مناسب در مورد زمان حمله تصمیم‌گیری شود. در [۲۰]. مدلی ارائه شده است تا بتواند اندازه‌گیری نماید اینکه مهاجم تا چه حد از حمله منصرف شده است و چه حدی از کاهش مخاطره در نتیجه اجرای بازدارندگی صورت گرفته است و هزینه‌ها و تأثیرات در اجرای بازدارندگی چه هستند. در مقاله[۲۱]، یک مدل از بازی‌های علامت‌دهی تطبیقی[1] برای شناسائی مخاطرات قابل کنترل ناشی از تهدیدات داخلی[2] در سازمان توسعه داده شده است. در این مطالعه سیستم‌های مبتنی بر عامل در بازی های تکاملی نیز مورد توجه بوده است. اگر رفتارهایی از کارمندان که باعث آسیب‌پذیری بیشتر سازمان شود، انجام شود، دقیقا وضعیتی است که می‌بایست مدیر[3] به دنبال بازدارندگی باشد. در مقاله [۴]،تاثیرات مخاطره بر رفتار تعادلی و تاثیر آن روی مفهوم بازدارندگی در برابر مدل‌های ریسک-خنثی مطالعه شده است. بازیگران در حالت‌های ریسک‌گریز[4] و ریسک‌پذیر[5] فرض شده‌اند. در مدل ارائه‌شده در دو حالت تک مرحله‌ای و ترتیبی بازی مدافع-مهاجم، مدافع محدوده پیوسته از سطوح سرمایه گذاری دفاعی را در اختیار دارد که می‌تواند به صورت راهبردی در جهت بازداری مهاجم انتخاب شود. در مقاله [۲۲]، مدلی برای بازداری تنبیهیِ حملات تطهیر[6] در تمهیدات مبتنی اشتهار[7] در شبکه‌های ادهاک ارائه شده است. نودهایی که به صورت خودخواهانه عمل می‌کنند بدرفتار هستند و کارایی شبکه را پائین می‌آورند بنابراین، به‌واسطه حذف مزایایی که به‌واسطه انجام حمله تطهیر برای مهاجم حاصل می‌شود از این حمله بازداری می‌شود. نودهایی که همکاری بیشتری داشته‌اند رتبه‌بندی می‌شوند و اشتهار آنها افزایش پیدا می‌کند. استفاده از نظریه بازیها از کارهای آینده این پژوهش عنوان شده است. در مقاله [۱۰]، مدل بازی دو مرحله‌ای جهت زمانبندی و بازدارندگی حملات تروریستی که در یک دوره زمانی تکرار می‌شود نشان داده شده است. در ساختار بازی برای هر دو بازیگر همه پارامترها به صورت دانش مشترک فرض شده است. در این مدل متغیری برای حداقل سطح سرمایه گذاری دفاعی که برای بازدارندگی مفید است معرفی می‌شود و تعادل نش کامل زیربازی[8] مورد استفاده قرارگرفته است. در مقاله [۲۳] بازی امنیت سایبری با سه بازیگر مهاجم، مدافع و کاربر درنظر گرفته شده است و توافق هماهنگی[9] بین مدافع و راهبردهای دفاعی کاربر، سازوکار مدل برای بازداری مهاجم معرفی شده است.

در بخش ۲-۱، مروری بر مفهوم بازدارندگی در ادبیات تحقیق انجام شد و در بخش ۲-۲، کارهای انجام شده در بهره‌گیری از نظریه بازی‌ها در تبیین بازدارندگی در فضای سایبر مورد بررسی قرار گرفت. در نهایت بعد از مرور ادبیات این بخش درباره تعریفی از بازدارندگی می‌توان عنوان کرد بازدارندگی در فضای سایبر، یک مفهوم مجرد و ذهنی است و زمانی محقق خواهد شد که اگر تهدیدکننده در محاسبات هزینه-فایده مخاطره آفرینی خود علیه بازدارنده، خطر اجرای راهبردهایش را بیشتر از عدم اجرای آن ببیند آنگاه با توجه به اصل عقلانیت در فرض مسئله، تهدیدکننده متقاعد خواهد شد تا از اجرایی کردن راهبردهایش صرف‌نظر کند.

۲-۳- اندازه‌گیری مخاطره

سطح مخاطره یک تهدید به‌طور مستقیم بر بهره بازیگران در بازی بازدارندگی تاثیرگذار است. در مقاله [۴]، تأثیر ترجیحات مخاطره‌ای بازیگران را روی رفتار تعادلی آنها و تأثیرش روی ایده بازدارندگی مطالعه می‌کند. پرسش اساسی این مقاله بررسی این موضوع است که چگونه مخاطره ترجیحات روی راهبردهای تعادلی بازیگران در بازی ترتیبی دفاع-حمله تأثیرمی‌گذارد و چه چیزی را بر ایده بازدارندگی تحمیل می‌کند. در مدل ارائه شده در پژوهش [۲۴]، از یک سو مهاجم با توجه به اجرای اقدامات متقابل سعی می‌کند تا بهره خودش را بوسیله کاهش مخاطرات و هزینه‌های سرمایه‌گذاری افزایش دهد و از سویی دیگر مدافع سعی می‌کند تا بازگشت خودش را بوسیله کمینه‌سازی خسارات و با توجه به سازوکارهای دفاعی هزینه‌های سرمایه‌گذاری، بیشینه سازد. مهاجم همیشه برای کاهش مخاطره کشف شدن، تلاش می‌کند، همچنین مدافع از سویی دیگر سعی می‌کند تا مخاطره مورد حمله قرار گرفتن را کاهش دهد. در مقاله [۲۵]، اندازه‌گیری مخاطره ابری از سه جز شرکت‌کنندگان، مجموعه اقدامات و تابع بهره تشکیل شده است. خسارت، بازیابی، تنبیه و هزینه‌هایی همچون منابع و زمان فاکتورهای مخاطره هستند که تابع بهره را در قابی از تابع هزینه و فایده شکل داده است. در مقاله [۲۶]، سه ویژگی از نودهای برگ شامل هزینه حمله

1- Compliance
2- Insider threats
3- principal
4- Risk averse
5- Risk seeking
6- whitewashing
7- reputation
8- Subgame perfect Nash equilibrium
9- Coordination

(کسری از هزینه- فایده)، تفاوت‌های فنی و احتمال کشف شدن را در نظر گرفته است و استانداردهای سطوح رتبه‌بندی در یک جدول تعیین شده‌اند.

برای اندازه‌گیری بهتر مخاطرات حریم خصوصی مکان در VANET[1]، مدلی بر پایه جنبه‌های مختلف امکان موفقیت، هزینه حمله، تفاوت‌های فنی و مخاطره‌ی کشف‌شده توسعه داده شده است [۲۴]. در مقاله [۲۷]، در مدل بازی از پارامترهای مخاطره در تابع بهره بازی برای اندازه‌گیری مخاطرات در محاسبات ابری استفاده کرده است. محققین در این پژوهش با در نظر گرفتن احتمال وقوع یک رویداد مخاطره‌آمیز، تأثیر آن رویداد و تخمین سطح مخاطره فاکتورهای مخاطره را گروه‌بندی کرده‌اند. در مقاله [۲۸]، احتمال تهدید، شدت آسیب‌پذیری و پیامد حادثه در اندازه‌گیری مخاطره دارائی‌های اطلاعاتی مورد استفاده قرارگرفته است.

با توجه تحقیقات انجام گرفته مشاهده می شود در محیط تنازع مدافع-مهاجم متغیرهای تهدید، میزان خسارات، هزینه و دریافتی‌های حاصل از حمله به طور مستقیم بر محاسبات مخاطره تاثیرگذار هستند و از منظری دیگر مبتنی بر رویکرد نظریه بازی‌ها تابع بهره بازی را شکل خواهند داد، از این رو بازدارنده و تهدیدکننده نیاز دارند تا شناخت دقیقی را از محیط بازی خویش حاصل نمایند. در بخش ۳-۲-۲ به جزئیات تعریف تابع بهره بر اساس مخاطرات خواهیم پرداخت.

۲-۴- گراف حمله

با توجه به جمع بندی بخش ۲-۳ در رابطه با نیاز محیط منازعه سایبری به تحلیل مخاطرات بازی، بازیگران نیاز دارند تا با توجه به پیچیدگی و تنوع محیطی، تبیین بهتری در جهت شناخت وضعیت محیط و اندازه‌گیری مخاطرات حاصل نمایند. گراف‌های حمله مدل‌های ریاضی هستند که باتوجه به ساختار شبکه‌ای فضای سایبر برای توصیف محیط، سرمایه‌ها و دارائی‌های سایبری و ارتباط‌دهی آسیب‌پذیری آنها با تهدیدات، مورد توجه بسیاری از محققین بوده است. گراف حمله در مقاله [۲۹]، چارچوبی برای پیشگیری از نفوذ مبتنی بر گراف حمله ارائه شده است. چهار پارامتر مربوط به طول مسیر، تنوع آسیب‌پذیری‌های موجود در یک مسیر، میزان سادگی قابل بهره‌برداری بودن یک مسیر و نیز میزان تأثیر منفی اجرای آن مسیر حمله بر روی پارامترهای امنیتی (محرمانگی، دسترس‌پذیری و یکپارچگی) شبکه استفاده شده است. برای تعیین مقادیر آثار بهره‌برداری از یک آسیب‌پذیری از پایگاه داده CVSS[2] استفاده شده است. در تحقیق [۳۰] برای مدیریت مخاطرات امنیتی از شبکه‌های تصمیم بیزی استفاده شده است. در تحلیل ریسک با استفاده از گراف حمله بیزی قبل از تولید شبکه تصمیم بیزی می‌بایست ابتدا گراف حمله بیزی مربوط به شبکه مورد بررسی تولید شود. در مقاله [۲۴]، از ساختار درخت حمله برای کشف راهبردهای حمله برای تصمیم‌گیری اقدام متقابل و تعیین احتمال حصول اهداف تهاجم مورد استفاده قرارگرفته است.

در این تحقیق با توجه به این‌که در بازی بازدارندگی در فضای سایبر به ساختارهایی نیاز داریم تا وضعیت موجود بازیگران را از جهت سناریوهای موجود تهدید و همچنین سناریوهای اقدام متقابل شناسائی نمائیم بنابراین از ساختار گراف حمله برای این منظور استفاده خواهیم کرد. در بخش ۳-۲-۱، تعریف گراف‌های حمله مورد استفاده در این تحقیق ارائه شده است.

در پایان بخش ۲، در جمع‌بندی می‌توان عنوان کرد در پژوهش های گذشته بیشتر به صورت ضمنی و توصیفی مبحث بازدارندگی در دستور کار محققین بوده است یا برخی از متغیرهای بازی در نظر گرفته نشده است که برای پوشش برخی از این کاستی ها و نزدیک شدن مدل پیشنهادی به شرایط واقعی تلاش شده است در قالب نوآوری‌های پژوهش و توسعه و بهبود مدل‌های پیشین مدلی از بازدارندگی در فضای سایبر را با تمرکز بر: ۱- مدل راهبردی، ۲- بهبود پارامترهای مدل بازی (تابع بهره مخاطره محور، علامت‌ها و راهبردهای بازیگران)، ۳- ارائه گام‌های شناخت وضع موجود، شناخت وضع مطلوب، تحلیل فاصله، برنامه اقدام، ۴- احصا سناریوهای حمله مبتنی بر گراف حمله برای توصیف حالت‌ها[3] در مدل بازی علامت‌دهی، ۴- تعیین شرایط تحقق بازدارندگی، ۵- عدم محدودیت در استفاده از راهبردهای بازدارندگی از جمله تنبیهی، انکاری و همبستگی، بهره‌گیری از راهبردهای غیرسایبری (مانند اقدام حقوقی) و ۶- معرفی وضعیت‌های منازعه، توازن و ضعف متقابل را ارائه دهیم.

۳- مدل بازدارندگی در فضای سایبر(مدل پیشنهادی)

بازیگران در بازدارندگی در بهره‌برداری از منافعشان دارای تعارض می‌باشند بنابراین، نوعی از بازی مبتنی بر تعاریف نظریه بازی‌ها می‌تواند در روابط آن‌ها تعریف شود. هدف از بازدارندگی

1- Vehicular Ad Hoc Network

2- Common vulnerability scoring system
3- types

جلوگیری از وقوع جنگ می‌باشد بنابراین، وقتی بازدارندگی موفق است که هیچ‌گونه اقدام خصمانه‌ای صورت نپذیرد. مدل بازی بازدارنده- تهدیدکننده در این پژوهش با دو بازیکن در نظر گرفته‌شده است. در مرحله اول تهدیدکننده با هدف قراردادن سرمایه‌های بازدارنده سناریوهای تهدیدی را به صورت بالقوه در نظر گرفته است. تهدیدکننده یکی از سناریوهای حمله را برای اعمال انتخاب کرده است. در این فرآیند تهدیدکننده علامت‌هایی را ارسال یا از خود بروز خواهند داد. این علامت‌ها مبتنی‌بر ساختار بازی علامت‌دهی راهبردهای تهدیدکننده را شکل می‌دهند. سناریوهای تهدید تعداد آن‌ها مشخص است اما وقوع آن‌ها برای بازدارنده محتمل است. مجموعه راهبردهای تهدیدکننده شامل علامت‌های رفتار هنجار[1] N و رفتار ناهنجار[2] NN است و راهبردهای بازدارنده مجموعه‌ای از سناریوهای اقدام متقابل است که بر علیه تهدیدکننده در نظر گرفته است. مدل بازی بازدارندگی در فضای سایبر را با توجه به این‌که بازدارنده در مورد نوع یا حالت تهدیدکننده (سناریوهای تهدید) اطلاعات کافی ندارد به‌عنوان یک بازی علامت‌دهی با اطلاعات ناقص در نظر گرفته می‌شود. متغیرهای این مدل در جدول (۱) معرفی‌شده‌اند و در شکل (۱) مدل مفهومی بازدارندگی در فضای سایبر در چهار مرحله به تصویر کشیده شده است. در ادامه به شرح هر یک از این وضعیت‌ها خواهیم پرداخت.

جدول (۱): تعاریف متغیرهای مورد استفاده در فرموله‌سازی مدل

تعریف متغیر	علائم متغیرها
بازیگر تهدیدکننده (۱)	T
بازیگر بازدارنده (۲)	D
ارزش دارائی سایبری	W
هزینه بهره‌برداری از آسیب‌پذیری	c
درصد خسارت به ازای هر آسیب‌پذیری	IM
احتمال بهره‌برداری آسیب‌پذیری در یک نود	POE[3]
میزان مخاطره آفرینی	RCF[4]
تابع بهره هر سناریو	U
باور بازدارنده درباره حالت(نوع) تهدیدکننده	μ
یک سناریوی حمله یا یک مسیر در گراف حمله	π
راهبرد بازیگر	σ
هزینه اجرای راهبرد یا سناریو	C
عایدی ارزشمند حاصل از اجرای یک سناریو برای بازیگر	E
خسارت وارده در نتیجه اجرای سناریوی متقابل توسط بازیگر حریف	I

1-Normative
2- Non-Normative
3-Probabilty of exploiting
4-Risk creating function

در این پژوهش مدل بازدارندگی در فضای سایبر را چهار گام شناخت وضع موجود، شناخت وضع مطلوب، تحلیل فاصله و برنامه اقدام معرفی می کنیم. در بخش‌های بعد به معرفی هریک از این گام‌ها خواهیم پرداخت.

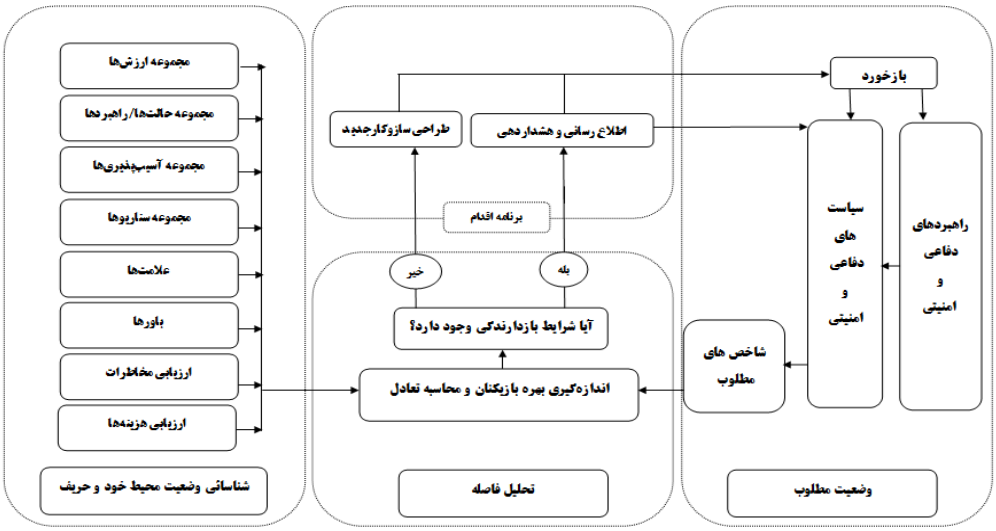
۳-۱- وضع مطلوب یا شرایط بازدارندگی

وضع مطلوب زمانی است که در آن بازدارندگی خواهیم داشت. تعادل حاصل از بازی نوعی پیش‌بینی از بازی را ارائه خواهد کرد اما آنچه تعادل بازی نشان می‌دهد ممکن است ضرورتا بازدارنده نباشد بنابراین، زمانی بازدارندگی فراهم می‌شود که بهره‌ای در اجرای راهبردهای بازیگران وجود نداشته باشد این وضعیت را وضع مطلوب می‌نامیم. در این شرایط تهدیدکننده انگیزه حمله نخواهد داشت و بهره مثبتی از اجرای راهبرد یا سناریوی حمله خود حاصل نخواهد کرد.

دریافتی حاصل از اجرای تهدید، هزینه‌ها و خسارات احتمالی متغیرهایی هستند که در بهره بازیگران تاثیرگذار هستند بنابراین با توجه به فرض عقلانیت اگر بازیگری اجرای راهبرد خود را سودمند ببیند آنرا عملی خواهد کرد و از آنجایی که حالت‌های تهدیدکننده از تهدیدات علیه بازدارنده تشکیل شده است بنابراین، در صورت سودمندی اجرای راهبرد برای تهدیدکننده دیگر بازدارندگی نخواهیم داشت. بنابراین، در مواقعی که تعادل بازی متشکل از بهره‌های کوچکتر مساوی صفر باشد بازدارندگی خواهیم داشت.

در وضع مطلوب یا چشم انداز وضعیت بهینه محیط سایبری بازیگران، از پیش در اهداف، قوانین، راهبردها و سیاست‌های کلان بازیگران ترسیم می‌شود. اینکه کدام دارائی‌ها بایستی امنیت آنها تامین شوند و کدام یک از آنها ارزشمند هستند؟، چه راهبردهایی برای تهاجم یا اقدام متقابل دارای مجوز است؟ و چه سطحی از مخاطرات می‌تواند قابل پذیرش باشد؟ این موارد در وضع مطلوب ترسیم می‌شود.

از آنجائی که در محیط‌های واقعی یک سیستم با توجه به عدم قطعیت‌های موجود ممکن است دقت صددرصد را حاصل نکند بنابراین، در هر دوره از اقدام و اجرای راهبردها نیاز است تا بازخوردهای لازم اعمال شود و شرایط مدنظر مطابق با تجارب یا نتایج شبیه‌سازی مناسب‌سازی شود. در شکل (۱) گام وضع مطلوب به‌عنوان اولین گام در تحلیل بازدارندگی محیط سایبری بازیگران نمایش داده شده است.



شکل (۱): این شکل مدل مفهومی بازدارندگی در فضای سایبر با چهار گام وضع مطلوب، تحلیل فاصله و شناسایی وضعیت محیط خود و حریف (وضع موجود) و برنامه اقدام را نشان می‌دهند.

۳-۲- شناسایی وضع موجود محیط بازی

در گام شناخت وضع موجود با اندازه‌گیری متغیرهای بازی مدل‌سازی اولیه بازی انجام می‌شود. هر سرمایه از بازیگران ممکن است یک یا چند آسیب‌پذیری داشته باشد. آسیب‌پذیری با احتمال مشخصی می‌تواند توسط تهدیدکننده مورد بهره‌برداری قرار گیرد. برای به تصویر کشیدن ارتباط بین آسیب‌پذیری‌ها و ابزارهای سوءاستفاده‌گر از گراف حمله استفاده خواهیم کرد. هر بازیکن باید گراف حمله خود و حریف را برای محاسبات تعادل حاصل نماید. در سمت تهدیدکننده مسیرهایی که از نودهای ابتدائی شروع و به برگ‌ها ختم می‌شوند برابر مفهومی به نام نوع[1] در بازی علامت‌دهی هستند و در سوی بازدارنده این مسیرها متناظر با اقدامات تلافی‌جویانه به عنوان راهبردهای بازدارنده در نظر گرفته می‌شوند.

علامت‌ها به عنوان راهبردهای تهدیدکننده، حاوی اطلاعات هستند این علامت‌ها می‌تواند از طریق دسته‌بندی کننده‌های سیستمی یا به‌صورت خبره‌محور تولید شود. سامانه‌های آنتی‌ویروس[2]، کشف نفوذ[3]، آگاهی موقعیتی[4]، سرویس‌دهنده‌های رویداد نگار[5]، مرکز عملیات امنیت[6]، دیواره‌های آتش[7] و ... از سامانه‌های مهمی هستند که به همراه تحلیل و رصدهای انسانی نقش مهمی در تولید علامت دارند. در این پژوهش علامت‌ها پس از بررسی تحرکات و رفتارهای تهدیدکننده به‌واسطه احصاء ویژگی‌های مشخص از داده‌های جمع‌آوری‌شده، ترافیک شبکه، خبرها، اعلام مواضع و ... با تکیه بر تحلیل انسانی و یادگیری ماشین در دو دسته‌بندی هنجار(N) و ناهنجار(NN) تهیه می‌شوند. درنهایت یک علامت شرایطی است که در قضیه بیزین با استفاده از آن می‌توان احتمال پسین یا اعتبار تهدید را محاسبه کرد.

۳-۲-۱- گراف‌های حمله

در این تحقیق بهره‌گیری از نظریه گراف حمله، نقش مهمی در استخراج سناریوهای تهدید دارد. بنابراین، گراف حمله متناسب با نیاز این تحقیق در ادامه تعریف می‌شود.

تعریف (۱): $Gr = (V, E)$ را گراف جهت‌دار بدون سیکل در نظر بگیرید در این گراف $V = \{v_{m,n}, \dots, v_{M,N}\}$ مجموعه رئوسی هستند که آسیب‌پذیری سرمایه‌های سایبری را نشان می‌دهند. اندیس‌های m و n به ترتیب نشان‌دهنده یک دارائی مشخص و آسیب‌پذیری خاص آن دارائی است. مقادیر M به‌ازای هر دارائی، بسته به تعداد آسیب‌پذیری‌های آن متغیر است.

$Er= \{e_1, \dots, e_k\}$ مجموعه‌ای از یال‌های جهت‌دار گراف است که نشان‌دهنده امکان بهره‌برداری یک آسیب‌پذیری توسط سوءاستفاده‌گرها است. به‌طوری که می‌گوییم یک $v_{i,j}$ می‌تواند با احتمال مشخص به‌وسیله سوءاستفاده‌گر e_k توسط بازیکن مورداستفاده قرار گیرد. این بهره‌برداری در طول یک مسیر باعث می‌شود تا بازیکن به گره بعدی گام بردارد و درنهایت به هدف موردنظر دست یابد. گراف حمله در حالت ایده‌آل می‌تواند کلیه آسیب‌پذیری‌های دارائی‌های حریف را در بر بگیرد. در شکل (۲) ساختار گراف حمله نمایش داده شده است.

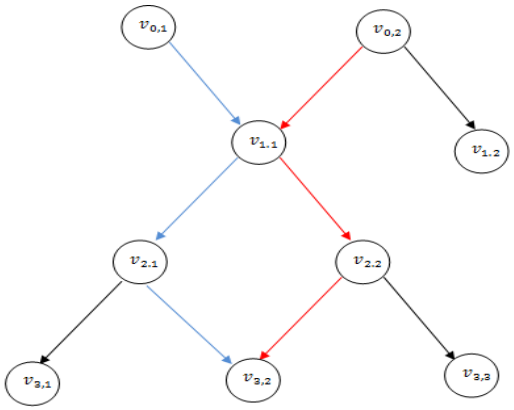
1- Type
2- Anti-virus
3- Situation awareness
4- Situation awareness
5- Log Server
6- Security operation center
7- Firewall

تعریف (۲) : هر مسیر، در مجموعه $\pi = \{\pi_1, \dots, \pi_l\}$ در گراف Gr از نودهای اولیه تا هدف یک سناریوی حمله را ایجاد می‌کند.

تعریف (۳) : تخمین احتمال بهره‌برداری آسیب‌پذیری برای هر نود به‌وسیله پارامترهای پایه و موقت مرتبط با سامانه امتیازدهی آسیب‌پذیری مشترک (CVSS[1]) از رابطه (۱) محاسبه خواهد شد [۳۱].

$$\text{Temporal probability (tp)} = (2 * AV * AC * AU) * (E * RL * RC) \quad (۱)$$

در این رابطه AV[2] بردار دسترسی، AC[3] پیچیدگی دسترسی، AU[4] نمونه‌های اعتبارسنجی، E[5] ابزارهای بهره‌برداری، RL[6] وضعیت ترمیم و RC[7] محرمانگی گزارش را نشان خواهد داد.



شکل (۲): نمونه‌ای از گراف حمله بدون دور. نودها در هر سطح آسیب‌پذیری‌های یک سرمایه سایبری را نشان می‌دهند. وجود یک یال جهت‌دار امکان بهره‌برداری از آسیب‌پذیری را نشان می‌دهد.

اگر سوءاستفاده‌گری حالت شبکه را از یک $s_i \in V$ به $s_j \in V$ تغییر دهد و $s_i \in Parent[s_j]$ باشد آنرا e_i می‌نامیم. توزیع احتمال شرطی s_j یا احتمال پیشین بهره‌برداری سناریو[8] برابر $pr(s_j|parent[s_j])$ است که به‌وسیله رابطه (۲) محاسبه می‌شود. با توجه به این‌که ارتباط بین یال‌های ورودی به نود s_j از نوع AND می‌باشد بنابراین، از قاعده ضرب استفاده شده است.

$$POE = pr(s_j|parent[s_j]) = \begin{cases} 0, & \exists s_i \in parent[s_j], s_i = 0; \\ pr\left(\bigcap_{s_i=1} e_i\right) = \prod_{s_i=1} tp(e_i), & otherwise. \end{cases} \quad (۲)$$

در هر نود از مسیر، متغیرهای ارزش دارائی (w)[9]، درصد خسارت[10] به سرمایه سایبری زمانی که سوءاستفاده‌گر عملیاتی می‌شود (im)، و احتمال پیشین بهره‌برداری[11] (tp) می‌بایست اندازه‌گیری شوند. از این مقادیر برای محاسبه مقدار مخاطره‌ای که برای هر نود ایجاد می‌شود (RCF) از طریق رابطه (۳) استفاده می‌شود.

$$RCF = (w*im*tp) \quad (۳)$$

در هر نود از مسیرهای حمله یا سناریوهای حمله علاوه بر مقدار متغیر RCF، هزینه‌ای که سوءاستفاده‌گر[12] برای بهره‌برداری صرف می‌کند (c) و مقادیر منافع دریافتی حاصل از اجرای سوءاستفاده‌گر در هر نود (En) نیز بایستی اندازه‌گیری شود. حاصل جمع مقادیر c، En و RCF به‌ازای نودهای هر سناریوی π، به ترتیب منافع دریافتی (E)، هزینه‌ی اجرا (C) و مخاطره ایجادشده به‌وسیله آن سناریو (I) را نشان می‌دهد. از پارامترهای E، C و I در اندازه‌گیری بهره بازیگران در بخش بعد استفاده خواهیم کرد.

۳-۲-۲- تابع بهره

با توجه به تعریف بازدارندگی نیاز به تابعی داریم تا مخاطراتی که بازیگران به یکدیگر تحمیل می‌کنند و متحمل می‌شوند را محاسبه کنیم. دو بازیگر تهدیدکننده و بازدارنده از سازوکار مخاطره‌آفرینی برای تسلط و منصرف‌کردن یکدیگر استفاده می‌کنند. بنابراین بهره بازیگران را در مدل بازدارندگی مبتنی بر مخاطره‌آفرینی (رابطه (۳)) در یک مسیر حمله (سناریوی حمله) با استفاده از رابطه (۵) محاسبه می‌کنیم. از آنجائی که بازدارنده علامت‌هایی را از سمت تهدیدکننده دریافت می‌کند نیاز دارد تا باورهای خود را از اعمال تهدیدات (سناریوهای حمله) محاسبه و به‌روزرسانی نماید.

از آنجائی که تهدیدکننده دارای حداقل دو حالت[13] در بازی است و بازدارنده فقط یک حالت دارد بنابراین، با توجه به این فرض محاسبه باورها برای تهدیدکننده ضرورتی ندارد. با توجه به سازوکار علامت‌دهی، مدل بازی علامت‌دهی، پایه مدل بازدارندگی را شکل خواهد داد و شبکه باور بیزی باورهای بازدارنده را بروز رسانی خواهد کرد. برای محاسبه باور بازدارنده، مبتنی بر قضیه بیزین از رابطه (۴) استفاده خواهیم کرد.

$$\mu(\pi_i|\sigma_j) = \frac{\mu(\boldsymbol{\sigma}_j|\pi_i)\mu(\pi_i)}{\sum_i \mu(\boldsymbol{\sigma}_j|\pi_i)\mu(\pi_i)} \quad (۴)$$

1- common vulnerability scoring system
2- Access vector (AV)
3- Access complexity (AC)
4- authentication instances (AU)
5- Exploitable (E) tools
6- remediation status
7- report confidence
8- prior probability of exploiting scenario

9- Worth value
10- Impact factor
11- posterior probability
12- Cost of exploiting
13- Type

در این رابطه π_i به‌ازای i=1,2 برای تهدیدکننده حالت بازیکن و نیز سناریوهای حمله را نشان می‌دهد و $\boldsymbol{\sigma}_j$ به‌ازای j=1,2 نشان‌دهنده راهبردها یا علامت‌های تهدیدکننده می‌باشد. احتمال $\mu(\boldsymbol{\sigma}_j|\pi_i)$ با استفاده از تاریخچه رویدادها و حوادث ثبت شده در سامانه‌های رصد و پایش سایبری محاسبه می‌شود.

در نهایت برای محاسبه بهره بازیگران از رابطه (۵) استفاده خواهیم کرد.

$$U(\mathrm{E},\mathrm{C},\mathrm{RCF},\mu) = \mu(\pi|\sigma)(E_\pi - C_\pi - C_\sigma - I_{\hat{\pi}}) \qquad (۵)$$

در این رابطه پارمترهایE_π و C_π به ترتیب مقدار منافع دریافتی و هزینه اجرای سناریوی π را نشان می‌دهد. C_σ نشان‌دهنده هزینه علامت‌دهی برای تهدیدکننده است و $I_{\hat{\pi}}$ نشان‌دهنده میزان خسارت وارده از طرف سناریوی متقابل حریف می‌باشد. مقدار باور در رابطه (۵)، برای محاسبه بهره تهدیدکننده برابر یک، و مقدار C_σ، برای محاسبه بهره بازدارنده برابر صفر می‌باشد.

با توجه به این که تهدیدکننده علامت‌هایی را قبل از اجرای سناریوی مدنظرش بروز می‌دهد، این علامت‌ها را در چارچوب بازی علامت‌دهی، راهبرد تهدیدکننده و سناریوهای حمله بر علیه بازدارنده را حالت‌های وی در نظر می‌گیریم. اما در سمت بازدارنده سناریوهای حمله بر علیه تهدیدکننده راهبردهای او را در چارچوب بازی علامت‌دهی شکل خواهد داد.

۳-۳- تحلیل فاصله از وضع موجود به وضعیت بازدارندگی

بعد از شناسائی وضع موجود و اندازه‌گیری متغیرهای مورد نیاز آن، تعادل بازی محاسبه می‌شود. نقطه تعادل بازی گرایش بازیگران را در صحنه آتی محیط بازی نشان می‌دهد.

براساس مقادیر بهره‌ای که تعادل بازی به خود می گیرد سه وضعیت: ۱- منازعه، ۲- توازن و ۳- ضرر متقابل حاصل می‌شود. در گام آخر در صورتی که بازدارنده در وضعیتی قرار گیرد که بازدارندگی تامین شود (وضعیت‌های ۲ و ۳) می‌تواند نسبت به اعلان و هشداردهی لازم اقدام کند و در صورتی که بازدارندگی تامین نشود (وضعیت ۱) می‌بایست برای طراحی سازوکار جدید تدابیر لازم در نظر گرفته شود.

۳-۴- برنامه اقدام

برنامه اقدام شامل دو فعالیت هشدار-اطلاع رسانی و طراحی سازوکار می باشد. برنامه اقدام بعد از تحلیل فاصله در دستور کار بازدارنده قرار می‌گیرد تا در صورتی که بر اثر خروجی گام تحلیل فاصله، یعنی تعادل بازی، با وضع مطلوب تطبیق داشت، بازدارنده نسبت به هشدار و اطلاع رسانی لازم اقدام می‌نماید و در صورتی که تعادل بازدارنده نباشد آن‌گاه متناسب با پیش‌بینی زمان حمله طراحی سازوکار جدیدی را می‌بایست در دستور کار خود قرار دهد.

۴- تجزیه و تحلیل تعادل بازی

محدودیت‌های دسترسی به دادگان در محیط‌هایی که بازدارندگی در آن‌ها رخ داده است و وجود متغیرهای مختلفی مانند، تعداد بازیگران، تعدد حالت‌های تهدیدکننده، تعدد اقدامات بازدارنده و ... باعث خواهد شد تا مدل در اندازه‌های مختلف متصور باشد بنابراین، ناگزیر هستیم تا بررسی کارائی مدل را با شرایط اولیه از پیش تعیین‌شده مورد ارزیابی قراردهیم. اثبات روابط ریاضی تعادل بازی و حل یک نمونه عددی روش‌هایی هستند که به کمک آن سعی داریم تا کارائی مدل را نشان دهیم.

تعادل بازی، جهت‌گیری و گرایش بازیگران را به نقطه‌ای خاص نشان می‌دهد که بازیگران انگیزه تخطی از آن را ندارند. بنابراین بازدارنده در بررسی وضعیت فعلی خود به دنبال محاسبه تعادل بازی است. برای تجزیه و تحلیل نحوه محاسبه تعادل بازی در مدل بازی بازدارندگی در فضای سایبر برای هر بازیگر دو سناریو در نظر گرفته شده است. در سمت تهدیدکننده سناریوهای خرابکاری در کنترل‌کننده های صنعتی در نیروگاه برق هسته‌ای (M) و تغییرچهره سایت‌های رسمی کشور حریف (F) را در نظر می گیریم و در سمت بازدارنده سناریوهای اقدام متقابلِ افشاء اسناد (R) و حملات منع سرویس برای فلج‌سازی سرویس‌دهنده‌های تراکنش بانکی (D) را خواهیم داشت. در شکل‌های (۵-۲) گراف حمله هر سناریو نمایش داده شده است.

محاسبه تعادل در بازی‌های علامت‌دهی نیازمند سه شرط اساسی ۱- محاسبه باور، ۲- انتخاب عمل با توجه باورها و علامت‌ها به گونه‌ای که بهره انتظاری بیشینه شود و ۳- بروز رسانی باورها با استفاده از قاعده بیزین می باشد. با توجه به اینکه در محاسبه بهره بازی در رابطه (۵)، محاسبه باور نقش مهمی دارد و از طریق قاعده بیزین (رابطه ۴) این باور بروز رسانی می شود بنابراین شرط اول و سوم محاسبه تعادل تامین می شود.

انتخاب راهبردهای تعادلی منفک N در این بازی بستگی به هزینه علامت‌دهی دارد بنابراین، اگر هزینه‌های علامت‌دهی C_N و C_{NN} برابر نباشد، تعادل‌های منفک را خواهیم داشت و اینکه کدام یک از تعادل های منفک را خواهیم داشت به بزرگتر یا کوچکتر بودن این هزینه‌ها نسبت به یکدیگر وابسته است.

هزینه‌های علامت‌دهی در انتخاب راهبردهای تعادلی

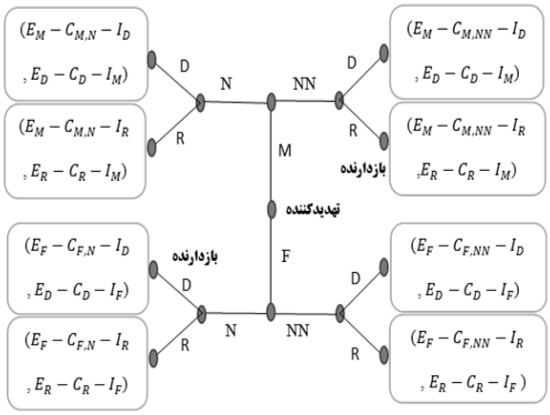
یک‌کاسه نیز تاثیرگذار هستند به‌طوری که اگر $C_{NN} > C_N$ آن‌گاه احتمال وجود تعادل یک کاسه (N,N) وجود دارد و اگر $C_{NN} < C_N$ باشد آن‌گاه احتمال وجود تعادل یک‌کاسه (NN,NN) وجود دارد. در مدل پیشنهادی با توجه به روابط نشان داده شده در شکل (۳) و جداول (۲) و (۳)، تعادل راهبرد غالب وجود دارد و بنابراین، می‌توان از طریق حذف پیاپی راهبردهای مغلوب به تعادل بازی رسید. حذف راهبردهای مغلوب باعث خواهد شد تا بهره انتظاری بازیکنان بیشینه شود بنابراین، با توجه به وجود تعادل راهبردهای غالب بازیکنان به صورت مختلط عمل نخواهند کرد.

جدول (۲): در ستون‌ها دو راهبرد N و NN به‌ازای سناریوهای F و M تهدیدکننده و در سطرها دو راهبرد D و R بازدارنده در نظر گرفته شده است. در هر سلول براساس راهبردهای بازیگران تابع بهره تهدیدکننده در بالا و تابع بهره بازدارنده در پائین نمایش داده شده است.

	F		M	
	N	NN	N	NN
D	$(E_F - C_{F,N} - I_D)$ $,\mu(F\|N)\,(E_D - C_D - I_F)$	$(E_F - C_{F,NN} - I_D)$ $,\mu(F\|NN)\,(E_D - C_D - I_F)$	$(E_M - C_{M,N} - I_D)$ $,\mu(M\|N)\,(E_D - C_D - I_M)$	$(E_M - C_{M,NN} - I_D)$ $,\mu(M\|NN)\ (E_D - C_D - I_M)$
R	$(E_F - C_{F,N} - I_R$ $,\mu(F\|N)\ (E_R - C_R - I_F)$	$(E_F - C_{F,NN} - I_R$ $,\mu(F\|NN)\,(E_R - C_R - I_F)$	$(E_M - C_{M,N} - I_R$ $,\mu(M\|N)\,(E_R - C_R - I_M)$	$(E_M - C_{M,NN} - I_R$ $,\mu(M\|NN)\,(E_R - C_R - I_M)$

جدول (۳): در این جدول برای ساده‌سازی تجزیه و تحلیل مقادیر باورهای $\mu(F|N)$، $\mu(F|NN)$، $\mu(M|N)$ و $\mu(M|NN)$ به‌ترتیب با علائم α، β، γ و λ و تفاضل‌های $E_D - C_D$ و $E_R - C_R$ به‌ترتیب با علائم Y و X معادل‌سازی شده است.

	F		M	
	N	NN	N	NN
D	$E_F - C_{F,N} - I_D$ $\alpha(Y - I_F)$	$E_F - C_{F,NN} - I_D$ $\beta\,(Y - I_F)$	$E_M - C_{M,N} - I_D$ $\gamma\,(Y - I_M)$	$E_M - C_{M,NN} - I_D$ $\lambda\,(Y - I_M)$
R	$E_F - C_{F,N} - I_R$ $\alpha\ (X - I_F)$	$E_F - C_{F,NN} - I_R$ $\beta\,(X - I_F)$	$E_M - C_{M,N} - I_R$ $\gamma\,(X - I_M)$	$E_M - C_{M,NN} - I_R$ $\lambda\,(X - I_M)$



شکل (۳): نمای توسعه‌یافته بازی بازدارندگی در فضای سایبر با دو سناریوی تهدید M و F برای تهدیدکننده و دو سناریوی D و R برای بازدارنده. تهدیدکننده دارای دو راهبرد NN و Nدر قالب علامت می‌باشد.

۴-۱- تجزیه و تحلیل راهبردهای تهدیدکننده

همان‌طور که در روابط بهره بازیکن تهدیدکننده مشاهده می‌شود مقادیر I_D و I_R در سطرهای جدول یکسان بوده بنابراین، با فرض اینکه $I_R > I_D$ باشد و از طرفی با وابستگی مقادیر تابع بهره در هر سناریوی تهدید به هزینه علامت‌دهی، اگر $C_{NN} > C_N$ باشد آن‌گاه می توان نتیجه گرفت در حالت F ، راهبرد N، راهبرد غالب خواهد بود. به همین ترتیب در حالت M با فرض $I_R > I_D$ و $C_{NN} > C_N$ راهبرد N غالب می‌باشد. در نهایت در مقایسه بهره بین دو حالت U(M,N) و U(F,N) غلبه بهره یک راهبرد به راهبرد دیگر به متغیر E بستگی دارد بنابراین، اگر $E_M < E_F$ آن‌گاه برای تهدیدکننده راهبرد N از سناریوی F راهبرد غالب می‌باشد.

۴-۲- تجزیه و تحلیل راهبردهای بازدارنده

در این بخش برای سادگی تحلیل، مقادیر باورهای $\mu(F|N)$، $\mu(F|NN)$، $\mu(M|N)$ و $\mu(M|NN)$ را به ترتیب معادل α، β، γ و λ فرض می‌کنیم و تفاضل‌های $E_D - C_D$ و $E_R - C_R$ را به ترتیب برابر Y و X فرض می کنیم. در نتیجه برابر جدول (۳) مقادیر تابع بهره را برای بازیکن بازدارنده خواهیم داشت. همانطور که در روابط مشاهده می شود باورها در هر سطر با ستون متناظر آن و همچنین مقادیر I در هر سناریوی (حالت) تهدیدکننده یکسان است بنابراین غلبه یک راهبرد به راهبرد دیگر (به ازای هر حالت تهدیدکننده) به مقادیر متغیرهای X و Y بستگی دارد حال با فرض $Y>X$ و $I_M < I_F$ همیشه راهبرد R مغلوب راهبرد D خواهد بود.

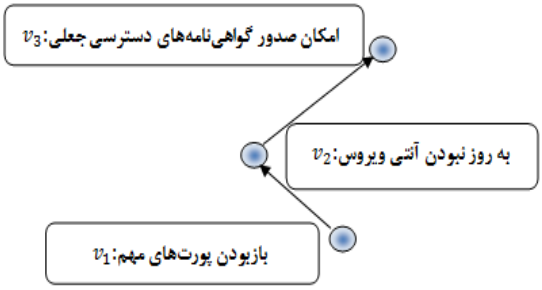
۴-۳- مثال عددی

در این بخش، در قالب سناریوهای وضعیتی فرضی، سعی داریم تا کارائی مدل را نشان دهیم. در این مثال برای هر سناریو سه دارائی در نظر گرفته شده است. هر بازیگر برای بهره‌برداری از نود هدف بایستی از نودهای اول و دوم عبور کند. بنابراین هر نود نشان‌دهنده‌ی یک آسیب‌پذیری برای هر دارائی می‌باشد و مهاجم برای اجرای کدها و برنامه‌های سوءاستفاده‌گر خود بایستی مسیری از نود ابتدایی v_1 تا v_3 را طی نماید. برای هر سناریو برابر تابع بهره‌ی مدل بازی، پارامترهای، احتمال پیشین بهره‌بردای از آسیب پذیری(POE) برابر رابطه (۲)، درصد خسارت وارده(im)، ارزش دارائی (w)، عواید و دریافتی حاصل از اجرای سناریو E (برابر حاصل جمع دریافتی ها در هر نود در صورت بهره‌برداری از آسیب‌پذیری)، هزینه‌ی اجرای سناریو(c) (برابر حاصل جمع اجرای سوء استفاده‌گر در هر نود) و خسارت (I) (برابر رابطه (۳)) در صورت اجرای سناریو محاسبه می‌شود. در مواردی که با ارزش‌های غیرمادی (مانند حسن شهرت) یا ترکیبی از ارزش‌های مادی و معنوی مواجه هستیم یا مواقعی که سطوح ارزش‌گذاری برای بازیگران متفاوت است نیاز است تا مقادیر پارامترهای تابع بهره در یک طیف زبان‌شناختی مانند طیف لیکرت نرمال‌سازی شود. در این مثال از سطح بندی خیلی‌کم=۰، کم=۱، متوسط=۲، زیاد=۳ و خیلی‌زیاد=۴ استفاده خواهیم کرد.

در شکل‌های (۴،۵،۶ و ۷) مسیرهای حمله معادل یک سناریوی حمله فرضی نمایش داده شده است. این مسیرهای حمله (سناریوهای M و F) در شکل (۴) و (۵) گراف حمله علیه بازدارنده را تشکیل خواهند داد و مسیرهای حمله (سناریوهای D و R) در شکل‌های (۶-۷) گراف حمله علیه تهدیدکننده را تشکیل خواهند داد. در جدول‌های (۷-۴) مقادیر متغیرهای مورد نیاز بر اساس روابط (۳) و (۵) نشان داده شده است و بعد از محاسبه این مقادیر در جدول (۸) مقادیر مدل نرمالِ بازی نشان داده شده است. در ستون اول جدول‌های (۷-۴) نام هر یک از نودهای گراف حمله آمده است. اندیس اول شماره دارائی را نشان می‌دهد و از آنجائی که هر نود یک آسیب‌پذیری دارد اندیس دوم یکسان است. در ستون E عایدی که بازیگر در صورت بهره برداری از آن آسیب‌پذیری در دارائی مربوطه حاصل می کند، نمایش داده شده است. این مقادیر در یک بازه صفر تا ۴ در نظر گرفته شده است تا یک طیف کیفی برای سطح‌بندی و نرمال‌سازی ایجاد نماید. صفر نشان‌دهنده‌ی *خیلی‌کم*(V.L)، یک معادل *کم*(L)، دو معادل *متوسط* (M)، سه معادل *زیاد* (H) و چهار معادل *خیلی‌زیاد (V.H)* است. این تبدیل مقادیر به یک طیف کیفی به ما کمک خواهد کرد تا نوعی از یکسان سازی واحدهای اندازه‌گیری را داشته باشیم.

جدول (۴): مقادیر متغیرهای روابط ۳ و ۴ برای سناریوی تهدید M

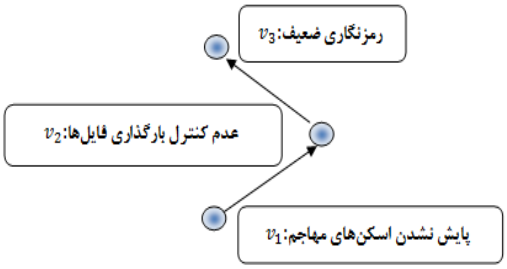
v	E	c	I	w	im	P
$v_{1,1}$	M	L	۰/۳۴۲	L	۰/۵۸	۰/۵۹
$v_{2,1}$	H	M	۰/۶۳۴	M	۳ ۰/۳	۰/۹۶
$v_{3,1}$	V.L	M	۱/۱۲۲	H	۰/۶۸	۰/۵۵



شکل (۴): سناریوی تهدید M (خرابکاری در کنترل‌کننده‌های صنعتی)

جدول (۵): مقادیر متغیرهای روابط ۳ و ۴ برای سناریوی F

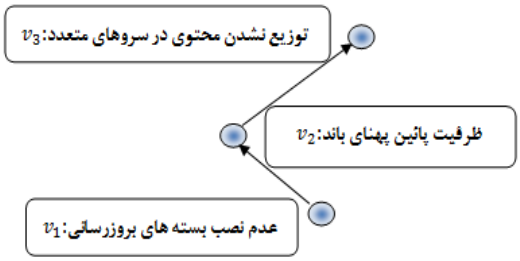
v	E	c	I	w	im	P
$v_{1,1}$	V.L	M	۲/۹۸۸	V.H	۰/۹	۰/۸۳
$v_{2,1}$	L	M	۳/۳۸۵	V.H	۰/۹۱	۰/۹۳
$v_{3,1}$	L	M	۰/۸۵۸	V.H	۰/۳۲	۰/۶۷



شکل (۵): سناریوی تهدید F (تغییرچهره سایت‌های رسمی بازیگر)

جدول (۶): مقادیر متغیرهای روابط ۳ و ۴ برای سناریوی D

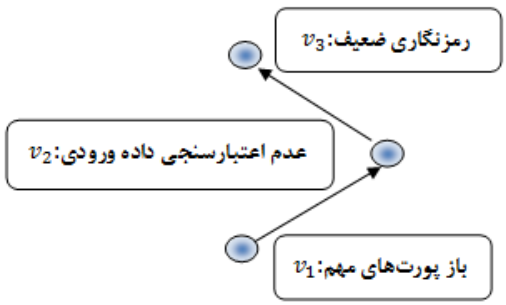
v	E	c	I	w	im	P
$v_{1,1}$	L	V.L	۰/۵۱	L	۰/۸۵	۰/۶
$v_{2,1}$	M	M	۰/۰۴۲	H	۰/۷	۰/۰۲
$v_{3,1}$	M	M	۰/۰۳۶	L	۰/۰۷	۰/۵۲



شکل (۶): سناریوی اقدام متقابل D (حملات منع سرویس)

جدول (۷): مقادیر متغیرهای روابط ۳ و ۴ برای سناریوی R

v	E	c	I	w	im	P
$v_{1,1}$	V.L	M	۰/۲۰۶	L	۰/۲۴	۰/۸۶
$v_{2,1}$	V.L	V.L	۱/۷۰۹	V.H	۰/۴۸	۰/۸۹
$v_{3,1}$	V.L	M	۰/۱۷۲	V.H	۰/۴۳	۰/۱



شکل (۷): سناریوی اقدام متقابل R (افشاء اسناد)

در ستون سوم جدول‌های (۷-۴) مقداری که بازیگر برای بهره‌برداری از نود بایستی هزینه کند (C) در یک طیف کیفی نشان داده شده است.

در ستون چهارم جدول‌های (۷-۴) مقداری که نود قربانی در ازای بهره‌برداری از آسیب‌پذیری خسارت می بیینند (I) نشان داده شده است. این مقدار نشان دهنده میزان مخاطره برای هر نود است. مقدار این ستون در هر سطر از حاصل ضرب ستون‌های پنجم تا هفتم حاصل می‌شود.

در ستون پنجم جدول‌های (۷-۴) مقدار ارزش دارائی بازیگر در یک طیف کیفی نشان داده شده است. در مواقعی که ارزشمندی دارائی هر بازیگر، بسته به شرایط محیطی می‌تواند متفاوت باشد یا دارائی‌های غیرهمجنس وجود داشته باشد و نتوانیم به صورت پولی ارزشگذاری کنیم، کیفی‌سازی ارزش‌ها کمک می‌کند تا واحدهای اندازه‌گیری یکسانی داشته باشیم.

در ستون ششم جدول‌های (۷-۴) درصد خسارت وارده نمایش داده شده است. این مقدار نشان می‌هد چه درصدی از ارزش دارائی در زمان اجرای سوءاستفاده‌گر از دست خواهد رفت و در ستون آخر جدول‌های (۷-۴) احتمال پیشین بهره‌بردای از آسیب‌پذیری برای هر نود نشان داده شده است.

با توجه به‌وجود تعادل با راهبردهای غالب می‌توان از طریق حذف تکراری راهبردهای مغلوب تعادل بازی را حاصل کرد. بنابراین برای بازدارنده راهبرد مغلوب D حذف خواهد شد و برای تهدیدکننده راهبرد NN در سناریوی M راهبرد غالب می باشد و مابقی حذف خواهند شد.

بنابراین، در این مثال تهدیدکننده با ارسال علامت ناهنجار NN با سناریوی M و بازدارنده با سناریوی D عمل خواهد کرد. در این نقطه تعادل، بازیگران مقادیر بهره (۰/۶۳- ,۰/۵۸-) را خواهند داشت. در صورتی که، بازیگران در وضعیت توازن با بهره (۰,۰) یا ضعف متقابل با بهره (u_t, u_d) به‌طوری‌که بهره بازدارنده $u_d < 0$ و بهره تهدیدکننده $u_t < 0$ باشد آن‌گاه بازدارندگی خواهیم داشت. با توجه به این‌که در نقطه تعادل، بازیگران بهره منفی دارند بنابراین، در این بازی بازیگران وارد یک منازعه سایبری نخواهند شد و بازدارندگی خواهیم داشت.

در این مثال هرچند سناریوهایی که در نظر گرفته شده‌اند ماهیت سایبری دارند اما بازیگران می‌توانند سناریوها و راهبردهایی در دیگر ابعاد مانند حقوقی، اقتصادی و ... را در دستور کار خود قرار دهند. به‌عنوان مثال، بازدارنده می‌تواند در

مقابل پیش‌بینی که از حملات تهدیدکننده دارد اقدام به برخورد حقوقی یا تحریم‌های اقتصادی را در دستور کار خود قرار دهد. همانند سناریوی سایبری برای چنین سناریوهایی هم می‌بایست پارمترهای ECI نیز اندازه‌گیری شود.

جدول (۸): در هر سلول جدول، در راست-بالا مقدار بهره تهدیدکننده و در سمت چپ-پائین مقدار بهره بازدارنده نمایش داده شده است. مقادیر باورهای بازدارنده $\mu(F|N) = 0.557$، $\mu(F|NN) = 0.427$، $\mu(M|N) = 0.537$ و $\mu(M|NN) = 0.572$ فرض شده است.

	F		M	
	N	NN	N	NN
D	-۵/۶ -۳/۵	-۴/۵۸ -۲/۷	-۱/۵۸ -۰/۶	-۰/۵۸ -۰/۶۳
R	-۷/۰۸ -۶/۳	-۶/۰۸ -۴/۸	-۳/۰۸ -۳/۲۸	-۲/۰۸ -۳/۵

۵- نتیجه‌گیری

اقدامات بازدارنده می‌تواند در حالت کلی در چهار دسته‌بندی اقدامات (۱) انکاری، (۲) تنبیهی، (۳) وابستگی متقابل و (۴) تشویقی مورد توجه قرار گیرد. در این پژوهش مدل راهبردی بازدارندگی در فضای سایبر را در نمایی مفهومی به همراه مسئله اصلی آن یعنی بررسی نقطه تعادل در بازی مورد مطالعه قراردادیم. بازی تهدیدکننده-بازدارنده مبتنی بر علامت‌دهی، با اطلاعات ناقص و بهره‌گیری از تابع ترجیح مخاطره آفرینی هسته اصلی مرحله تحلیل وضع موجود را تشکیل می‌دهد. همان‌طور که در ارائه مدل مطرح شد یکی از متغیرهای اصلی مدل بررسی وضعیت تهدیدات مدنظر تهدیدکننده است که در این تحقیق با ترکیب گراف‌های حمله با مدل بازی می‌توانیم سناریوهای حمله را در قالب حالات بازیگر تهدیدکننده احصا نمائیم. گراف‌های حمله در سمت بازدارنده نیز برای تدوین راهبردهای بازدارنده (سناریوهای اقدام متقابل) می‌تواند مورد استفاده قرار گیرد.

با توجه به مدل ارائه‌شده در پژوهش و وضعیت بازیگران در بازی بازدارندگی، وجود یک برگ برنده برای داشتن قدرت سایبری، یا راهبرد بازدارنده متمایز که بتواند مخاطره لازم را برای تهدیدکننده ایجاد نماید و همچنین اعلام اطلاعات این راهبرد در سطح ضرورت و به‌طور مناسب، به تهدیدکننده می‌تواند موفقیت بازدارندگی را تا حد زیادی تقویت نماید. شناختی که در تهدیدکننده درنتیجه تبادل اطلاعات و اعلان هشدارها از سوی بازدارنده به پشتوانه اقدامات معتبر بازدارنده صورت می‌گیرد نشان می‌دهد که اساساً اطلاعات به‌خودی‌خود می‌تواند نه به‌صورت قطعی بلکه در سطح عقلانیت مشخصی از بازیگران، بازدارنده باشد. یک بازیکن بازدارنده در صورتی‌که فاقد برگ برنده است می‌بایست با فریبِ تهدیدکننده زمان لازم را برای طراحی سازوکار جدید[1] یا یک بازی جدید فراهم نماید.

۶- کارهای آینده

در شرایط مختلف بازی با بیش از دو بازیکن، تکرار بازی، بازی‌های مبتنی‌بر یادگیری و علامت‌های متنوع، نیاز است تا در تحقیقات آینده مدل بازدارندگی توسعه داده شود. از جمله دیگر حوزه‌های مطالعاتی، که می‌تواند در آینده مورد توجه محققین قرار گیرد طراحی مدل، برای طراحی سازوکار بازدارندگی است، این مدل در وضعیت‌هایی که نتایج پیش‌بینی بازدارنده نخواهد بود لازم و ضروری است.

۷- منابع

1. C. D. Organization and P. D. Organization, “Cyber defense strategy ducument of iran,” Papsa (monthly journal), no. 1, May 22, 2014.
2. F. C. Zagare and D. M. Kilgour, “Perfect deterrence,” Cambridge University Press, vol. 72, 2000.
3. M. C. Libicki, “Cyberdeterrence and cyberwar,” Rand Corporation, 2009.
4. V. M. Payappalli, J. Zhuang, and V. R. R. Jose, “Deterrence and Risk Preferences in Sequential Attacker–Defender Games with Continuous Efforts,” Risk Analysis, 2017.
5. H. Vahidpoor, “The need for cyber defensive and offensive capabilities as deterrence factors,” in The 6th Congress of the Iranian Geopolitical Association Passive Defense, Mashhad, 2013.

1-Mechanisim design

political and international approaches, year. 8 , no.4, pp. 121-147, 2018.

7. T. Mowbray, "Solution architecture for cyber deterrence," 2010.
8. S. W. Beidleman, "Defining and deterring cyber war," DTIC Document, 2009.
9. R. J. Moore, "Prospects for cyber deterrence," DTIC Document, 2008.
10. K. Hausken and J. Zhuang, "The timing and deterrence of terrorist attacks due to exogenous dynamics," Journal of the Operational Research Society, vol. 63, no. 6, pp. 726-735, 2012.
11. J. S. Liles and J. Davidson, "Modern Cyber Deterrence Theory: Norms," Assumptions and Implications, 2013.
12. E. T. Jensen, "Cyber Deterrence," 2012.
13. K. Taipale, "Cyber-deterrence, Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization," IGI Global, 2010.
14. J. P. Kesan and C. M. Hayes, "Mitigative counterstriking: Self-defense and deterrence in cyberspace," Harv. JL & Tech., vol. 25, p. 429, 2011.
15. W. Goodman, "Cyber deterrence: Tougher in theory than in practice?," DTIC Document, 2010.
16. P. M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy, 2010.
17. R. L. Kugler, "Deterrence of cyber attacks," Cyberpower and national security, p. 320, 2009.
18. M. Rice, J. Butts, and S. Shenoi, "A signaling framework to deter aggression in cyberspace," International Journal of Critical Infrastructure Protection, vol. 4, no. 2, pp. 57-65, 2011.
19. H. Schramm, et al., "A game theoretic model of strategic conflict in cyberspace," In Proceedings of the 7th International Conference on Information Warfare and Security, Academic Conferences Limited, 2012.
20. E. F. Taquechel and T. G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," 2012.
21. W. Casey, et al., "Compliance signaling games: toward modeling the deterrence of insider threats,"
6. A. Dehghani, "Cyber Deterrence in global modern security: Russia's and China's threats against the critical US infrastructure," Journal of Quarterly Computational and Mathematical Organization Theory, pp. 1-32, 2016.
22. S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks," in Wireless Days (WD), 2010 IFIP, IEEE, 2010.
23. J. Cui, H. Rosoff, and R. S. John, "Deterrence of Cyber Attackers in a Three-Player Behavioral Game," in International Conference on Decision and Game Theory for Security, Springer, 2017.
24. S. Garg and G. S. Aujla, "An attack tree based comprehensive framework for the risk and security assessment of VANET using the concepts of game theory and fuzzy logic," Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 2, pp. 247-252, 2014.
25. Y. Sun, Z. Li, and W. Chaoxia, "Cloud computing risk assessment method based on game theory," in Cyberspace Technology (CCT 2015), Third International Conference on, IET, 2015.
26. R. Jiang, J. Luo, and X. Wang, "An attack tree based risk assessment for location privacy in wireless sensor networks," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on, IEEE, 2012.
27. E. Furuncu and I. Sogukpinar, "Scalable risk assessment method for cloud computing using game theory (CCRAM)," Computer Standards & Interfaces, vol. 38, pp. 44-50, 2015.
28. S. A. Cheharsoghi, et al., "Applicable of Artificial Neural Network in information security risk assessment," Cyber and electronic defense journal of imam hossein university, pp. 23-33, 2013.
29. K. Marjan, A. Hasan, and A. Ahmad, "Providing a framework for preventing network intrusion as low cost," 20th iranian conferance on electronical engineering, 2012.
30. K. Masoud, et al., "Cost-benefit analysis of security risks using decision-making bayesian networks," 20th yearly national conferance of computer society of iran, 2015.
31. M. Khosravi-Farmad, et al., "Network security risk mitigation using Bayesian decision networks," in Computer and Knowledge Engineering (ICCKE), 2014 4th International eConference on, IEEE, 2014.

Deterrence Model in Cyberspace Based on Bayesian Belief Attack Graph by using Risk Creating Payoff Function

A. Molaei, M. Kargari*, M. SheikhMohammady, A. Akramizadeh

*Supreme National Defense University

(Received: 07/12/2017 , Accepted: 13/10/2018)

ABSTRACT

Today, the rapid growth of dependence of human life on the cyberspace has raised the attention of the enemies of every society to the threats in this space. Several cyberattacks that have taken place in countries such as Estonia, Georgia and the Islamic Republic of Iran in the past, warn that the future of cyberspace will not be free of threats and attacks. Deterrence has always been a very important issue for all countries. In this practical and developmental research, we present Strategical Deterrence model in cyberspace. The game theory will help us model and analyze the deterrent model and descriptive and mathematical inferences will be used to analyze the model. Finally, in this paper, a strategical model for deterrence in cyberspace will be presented in four stages: the current, optimal, gap analysis and warning stages based on the signaling game with incomplete information. Finally after describing each components of the model and their relationship with each other, it has been shown that the amount of equilibrium can indicate the status of the players in the three situation of conflict, balance and mutual weakness, and only in two situation of balance and mutual weakness, the deterrence will exist.

Keywords: Deterrence, Cyberspace, Signaling Game, Attack Graph, Risk Creating Payoff Function

* Corresponding Author Email: m_kargari@modares.ac.ir