نشریه علمی «پدافند الکترونیکی و سایبری»
سال هفتم، شماره ۱، بهار ۱۳۹۸؛ ص ۹۴-۷۷

آگاهی وضعیتی حملات منع خدمت توزیع‌شده بر اساس پیش‌بینی (تجسم آینده نزدیک) صحنه نبرد مبتنی بر نظریه شواهد دمپستر- شافر و بیزین

حمید اکبری[1*]، سید مصطفی صفوی همامی[2]، رضوان خاندانی[3]

۱- دانشجوی دکتری، دانشگاه جامع امام حسین (ع)، ۲- دانشیار، دانشگاه صنعتی امیرکبیر، ۳- دانش‌آموخته دانشگاه خوارزمی

(دریافت: ۹۶/۱۱/۱۳، پذیرش: ۹۷/۰۳/۰۶)

چکیده

صحنه نبرد سایبری در حملات منع خدمت‌رسانی توزیع‌شده دارای دو بازیگر مهاجم و مدافع (قربانی) است که مهاجم با گسیل بسته‌های پی‌درپی و تغییر روش‌های خود درصدد قطع یا کاهش خدمت‌رسانی قربانی است و قربانی با انجام انواع تمهیدات امنیتی درصدد دفاع بوده و اصرار بر خدمت‌رسانی به ذینفعان خود دارد. ارزیابی این صحنه از منظر یک ناظر می‌تواند دارای ابهام باشد به‌طوریکه قادر باشد ادامه این صحنه را پیش‌بینی نمایید. در این پژوهش انواع وضعیت‌های مهاجم و مدافع و سپس معیارهای خبرگی در قالب مهارت، قابلیت تداوم حمله یا دفاع، تسریع در عکس‌العمل نشان دادن حمله یا دفاع و درنهایت قابلیت دسترس‌پذیری خدمات تبیین شده است. در ادامه با استفاده از یک مجموعه داده ۳۰۰۳ تایی که حاوی دنباله وضعیت‌های یک مهاجم و مدافع است، معیارهای فوق اندازه‌گیری شده و نتایج این تحقیق نشان داد که نیمی از داده‌ها دارای طول زمانی کوتاه حمله هستند که این بیانگر بهره‌مندی از اصل غافل‌گیری است و یا اینکه قربانی‌ها برای دفاع در برابر حمله، هیچ‌گونه آمادگی ندارند. همچنین همبستگی معیارها نسبت به یکدیگر نشان داد که هر چه زمان حمله طولانی باشد خسارت مدافع بیشتر می‌گردد و محاسبات به نفع مهاجم رقم می‌خورد. همچنین امکانات و تجهیزات در سرعت عمل مهاجم تأثیر مثبتی ندارد و بلکه قدری هم تأثیر منفی دارد و این بدان معناست که مهارت مهاجم نسبت تجهیزات او اثرگذارتر است. در ادامه به‌منظور تجسم صحنه نبرد در پیش‌بینی وضعیت طرفین تجسم‌های قابلیت چهارگانه تبیین گردید و سپس با استفاده از نظریه شواهد دمپستر- شافر، تجسم‌های فوق، ادغام‌شده تا بتوانند پیش‌بینی وضعیت اثر حمله بر قربانی را تخمین بزنند. همچنین در ادامه، تجسم قابلیت روش و تمهید با استفاده از قوانین بیزین تبیین گردید تا بتواند وضعیت آتی روش مهاجم و تمهید امنیتی مدافع را پیش‌بینی کند. با اجرای پنج سناریو در چهار گام زمانی، نشان داده شد که تخمین‌های حاصل‌شده با بیش از ۶۵ درصد قابل‌باور هستند.

کلید واژه‌ها: حملات منع خدمت توزیع‌شده، باتنت، آگاهی وضعیت، خبرگی، نظریه دمپستر- شافر، تجسم آینده

۱- مقدمه

توسعه فناوری اطلاعات موجب تغییرات اساسی درروند زندگی جوامع بشری شده است به‌طوری‌که بسیاری از زیرساخت‌های اساسی ملی و بین‌المللی در فضای سایبری شکل‌گرفته است. به طبع این تحولات، فضای منازعات نیز تغییریافته و صحنه نبرد را متحول کرده است. امروزه حملات سایبری نقش اثرگذاری داشته و یکی از مهم‌ترین تهدیدات مخرب محسوب می‌شود. صحنه نبرد سایبری متشکل از عناصر مهاجم سایبری، مدافع سایبری و بهره‌برداران در فضای سایبری است.

درصحنه جنگ‌های سایبری حمله‌کننده تلاش خواهد کرد تا از وضعیت قربانی و اثر حمله خود مطلع شود تا بتواند تصمیمات مناسبی بگیرد. اما در این راستا مشکلات بسیاری وجود دارد، به‌عنوان‌مثال ممکن است قربانی تمهیداتی بیندیشد و به‌کار گیرد [۱] که حمله‌کننده را در مورد تأثیر حمله گمراه کند. در این بخش در نظر است صحنه نبرد حمله منع خدمت با در نظر گرفتن وضعیت‌های مهاجم و مدافع به‌صورت یکپارچه تبیین و موردبررسی قرار گیرند. این صحنه باید حاوی قابلیت، فرصت، نیت و رفتار طرفین باشد و بتوان تجسمی از صحنه نبرد را به‌دست آورد. به‌منظور ارزیابی این صحنه نبرد باید این فضا به‌خوبی ترسیم شود، ازاین‌رو، در این نوشتار درصدد هستیم تا چنین صحنه‌ای را مهندسی و ابعاد نهفته آن را روشن کرده و مورد تجزیه‌وتحلیل قرار دهیم. بدیهی است که نتیجه چنین ارزیابی موجب آگاهی وضعیتی مطلوب گردد.

این نوشتار در نه بخش تنظیم‌شده است که در ابتدا تعاریف و مفاهیم و سپس به تبیین آگاهی از وضعیت حملات منع خدمت پرداخته می‌شود و در ادامه عملکرد طرفین را در قالب آمادگی رزم (خبرگی) با معرفی معیارهای مهارت، زمان پاسخ یا عکس‌العمل، تداوم عملیات بیان می‌گردد و سپس مدل و شبیه‌سازی طرح پیشنهادی به‌وسیله تجسم قابلیت با استفاده از دادگان ۳۰۰۳ تایی و در ادامه ارزیابی و نتیجه‌گیری انجام می‌گیرد.

*رایانامه نویسنده پاسخگو: kphakbari@ihu.ac.ir

۲- تعاریف و مفاهیم

نظر به این‌که در ادامه این نوشتار از عباراتی همچون آگاهی وضعیتی، حملات منع خدمت توزیع‌شده، شبکه بات استفاده می‌شود، ازاین‌رو، لازم است در این خصوص منظور نویسنده اجمالاً بیان شود.

۲-۱- حملات منع خدمات

حمله منع خدمت، تلاش برای از کار انداختن سیستم کاربر یا سازمان است. در حمله منع خدمت، مهاجم تلاش می‌کند تا سامانه‌ای را از حالت پایدار خارج کند و یا سرعت سیستم را به‌شدت کاهش دهد و کاربران نتوانند از منابع آن استفاده کنند. هدف از این حمله این نیست که به سیستم یا داده‌های هدف دسترسی پیدا کند، بلکه هدف این است که اجازه خدمت‌دهی کاربران قانونی را بگیرد [۲]. در این حملات، تعداد زیادی بسته از طریق صدها یا هزاران ماشین برای از کار انداختن منابع قربانی (سیستم پردازنده، حافظه و پهنای باند شبکه) ارسال می‌شود. برای ارزیابی تأثیرات این نوع حملات، از معیارهایی همچون محاسبه هزینه خسارت، افت کیفیت خدمات، بازدهی تراکنش، تأخیر در خدمت و غیره استفاده می‌شود.

۲-۲- آگاهی وضعیتی

فهم و درک این‌که چه چیزی اتفاق افتاده و یا در حال رخ دادن است و یا اینکه ممکن است در آینده نزدیک اتفاق بیفتد را آگاهی وضعیتی گویند، به‌طوری‌که این درک، از فهم عناصری (موضوع موردتوجه) از محیط حاصل می‌شود که به یکدیگر مربوط می‌شوند. مباحثی همچون نحوه کسب آگاهی و استنتاج آن و عوامل تأثیرگذار در درک (بهتر یا بدتر) انسانی یا ماشینی، موردنظر پژوهشگران این حوزه است. در تمامی حوزه‌های عملیاتی (نظامی یا غیرنظامی) تلاش می‌شود تا وضعیت‌ها معین گردد، سپس با استفاده از قرائن و شواهد (و سایر روش‌های استنتاجی) تشخیص داده می‌شود که کدام وضعیت در حال رخ دادن است یا در آینده‌ای نزدیک ممکن است اتفاق بیفتد. در یک صحنه منازعه ممکن است هر دو طرف در نقش مدافع یا مهاجم ظاهر گردند که معمولاً درصحنه جنگ متقارن بدین گونه است. در برخی صحنه‌های دیگر ممکن است یک‌طرف مدافع و طرف دیگر مهاجم باشد. اغلب درصحنه نبرد سایبری بدین گونه است. زیرا ماهیت مهاجم مخفی بوده و نیز مدافع یک خدمات‌دهنده است که ابزارهای لازم را برای مقابله در اختیار ندارد و فقط می‌تواند از خود دفاع کند و حتی اگر هم در اختیار داشته باشد، به علت گمنامی مهاجم نمی‌تواند با او مقابله کند. بنابراین، درصحنه سایبری می‌توان وضعیت‌های مربوط به مدافع و مهاجم را به‌صورت نامتقارن تبیین کرد.

۲-۳- آگاهی وضعیتی حملات منع خدمات

در حملات منع خدمات اهمیت درک شرایط کنونی، برای هر دو طرف مهاجم و قربانی اهمیت دارد. چراکه بتوانند شرایط فعلی را ارزیابی کرده و برای آینده نزدیک تصمیم‌گیری کنند. برای مدافعی که از حمله باخبر شده است، مهم است با سرعت عمل به تمهیدات از پیش تعیین‌شده بپردازد و همچنین مهم است که بداند مهاجم چه نقشه‌ای دارد و در لحظه یا قدم بعدی از چه روشی[1] استفاده خواهد کرد. به‌همین ترتیب برای مهاجم نیز مهم است که بتواند برنامه‌های فعلی و همچنین تمهیدات بعدی مدافع را برای ادامه حمله، تشخیص دهد.

۲-۴- انواع وضعیت‌ها

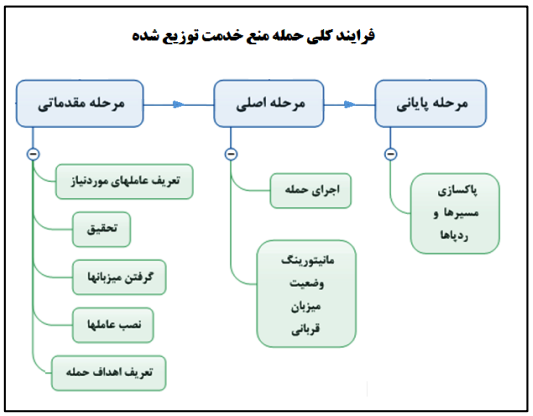
در این مرحله در نظر داریم انواع وضعیت‌های متصور طرفین را تبیین و سپس با استفاده اتوماتای کردن آن‌ها، شرایط را برای ترکیب مهیا می‌کنیم.

۲-۴-۱- وضعیت‌های مهاجم

فرآیند حملات منع خدمت توزیع‌شده معمولاً در سه مرحله صورت می‌گیرد. در گام اول (مرحله مقدماتی) با توجه به هدف تعیین‌شده لازم است تعداد زیادی ماشین‌های قوی تحت اختیار مهاجم قرار گیرد. ازاین‌رو لازم است با استفاده از یک یا چند آسیب‌پذیری مبادرت به آلوده کردن میزبان‌های (ماشین‌ها) مستعد کرد تا همگی تحت فرمان مهاجم قرار گیرند (مدیریت این کار توسط شبکه بات صورت می‌گیرد). در گام دوم (مرحله اصلی)، حمله اصلی بر روی قربانی انجام می‌گیرد. مهاجم در این مرحله با استفاده از انواع روش‌ها، درصدد تحت‌فشار قرار دادن هر چه بیشتر خدمات قربانی است تا به نتایج مطلوب خود برسد. ازاین‌رو مهاجم نیازمند است برای بهبود اقدامات بعدی خود، تأثیرات حمله بر قربانی را مشاهده نماید. بنابراین مهاجم با استفاده از بات‌های دیده‌بان می‌تواند مبادرت به پایش وضعیت قربانی کند. در آخرین گام (مرحله پایانی) مهاجم لازم است برای ردیابی نشدن، مبادرت به پاک‌سازی کلیه اثرات حمله نماید. به‌عنوان‌مثال تمام لاگ‌های بر روی سرورهای بات مستر و فرماندهی و کنترل را از بین ببرد تا کار ردیابی عقیم بماند. در شکل (۱) فرآیند کلی حمله منع خدمات نشان داده‌شده است. مهاجم دارای امکاناتی است که با استفاده از آن‌ها مبادرت به حمله می‌کند. این امکانات شامل سکوهای عملیاتی، ابزارهای نفوذگری، توانمندی‌های شخص (یا اشخاص) مهاجم، در اختیار داشتن آسیب‌پذیری‌های روز صفر و غیره است. با توجه به چنین امکاناتی می‌توان برای مهاجم انواع وضعیت‌ها را تعریف نمود. وضعیت‌هایی که بیان‌کننده توانایی مهاجم متناسب با شرایط و زمان است. به‌عنوان‌مثال در حملات

1- Method

منع خدمت، امکانات مهاجم شامل وجود شبکه بات، تعداد بات‌های تحت اختیار، داشتن انواع روش‌ها و آسیب‌پذیری‌های روز صفر و غیره است.



شکل (۱): فرایند کلی حمله منع خدمت

این امکانات در واحد زمان بیانگر شرایط و وضعیت حاکم بر صحنه نبرد از طرف مهاجم است. به عبارتی فرآیندهای کاری و قابلیت‌های مهاجم، می‌توانند به‌عنوان وضعیت‌های او تعریف گردد. در این پژوهش مبنای وضعیت مهاجم بر پایه حمله قرار داده شده است یعنی مرحله مقدماتی به عدم آمادگی حمله، مرحله اصلی به انجام حمله و مرحله پایانی به توقف حمله معنا شده است که در ادامه در قالب چهار وضعیت کلی بیان می‌گردد.

- **شبکه بات برای حمله آماده نیست (در حال بازسازی است):** در این وضعیت شبکه بات در حال شناسایی بات‌های زنده، به دام انداختن بات‌های جدید (نیروهای تازه‌نفس)، به دام انداختن بات‌های فراری (به دام انداختن این باتها ساده‌تر می‌باشد) است. به عبارتی شبکه بات توان لازم را برای حمله ندارد و یا هنوز هماهنگی و چیدمان بین بات و شبکه فرماندهی و کنترل صورت نگرفته است که همگی این حالات بیانگر این وضعیت می‌باشند. این وضعیت نشان‌دهنده این است که مهاجم در مرحله مقدماتی قرار دارد.
- **شبکه بات برای حمله آماده است (عبور از مرحله مقدماتی):** در این وضعیت همه‌چیز برای یک حمله مهیا است.
- **شبکه بات در حال حمله است:** در این وضعیت شبکه بات حمله را آغاز کرده است و حمله با توان قبلی ادامه می‌یابد و نیز توان حمله با زیادشدن تعداد باتها افزایش می‌یابد همچنین تغییری درروش حمله شبکه بات ایجادشده و درنهایت توان حمله کاهش می‌یابد که همگی این حالات بیانگر این وضعیت می‌باشند (مرحله اصلی).
- **شبکه بات حمله را متوقف کرده است:** در این وضعیت شبکه بات به‌طور موقت حمله را متوقف کرده است و درنهایت وضعیت توقف کامل، صورت می‌گیرد (مرحله پایانی).

۲-۴-۲- وضعیت‌های مدافع

ماشین‌های خدمات‌دهنده (قربانی)، موظف به ارائه خدمت باکیفیت قابل‌قبول به کاربران مجاز می‌باشند. ازاین‌رو باید تلاش کنند تا ضمن خدمات‌رسانی مطلوب در برابر حملات از خود مقاومت نشان داده و اثرات حمله را کاهش یا خنثی نمایند. بنابراین، لازم است (صاحبان) خدمات‌دهندگان همواره نسبت به تأمین منابع موردنیاز خدمات خود و نیز مسائل امنیتی اعم از تجهیزات دفاعی (دیواره آتش، فیلترینگ، سیستم تشخیص نفوذ[1]، سیستم تشخیص حملات منع خدمات و هانی پات[2] و غیره) و متخصصین امنیت و غیره مبادرت نمایند. بدیهی است که به‌کارگیری این تمهیدات دفاعی بتواند اثرات حمله را کاهش یا خنثی نماید. در خصوص روش‌های دفاعی می‌توان به روش پیشگیرانه، واکنشی و پیش‌کنشانه اشاره کرد که ممکن است ملزومات هر یک متفاوت باشد. مراحل دفاعی در برابر حملات منع خدمات را می‌توان به سه‌گام تقسیم کرد. در گام اول نیاز است وجود حمله تشخیص داده شود. در گام دوم باید از ورود ترافیک حمله به سامانه جلوگیری کرد و در گام سوم به دنبال ردیابی مهاجم (به‌منظور شکایت، دریافت غرامت، مقابله به‌مثل و ...) باشد. نظر به این‌که ترافیک کاربران عادی با ترافیک حمله تلفیق‌شده است، اجرای مراحل فوق را مشکل می‌کند و یا اجرای غلط آن موجب خسارت می‌شود (یعنی اگر تمهید امنیتی مناسب نباشد ممکن است از عبور ترافیک کاربران مجاز جلوگیری شود). با توجه به امکانات مدافع می‌توان انواع وضعیت‌ها را تعریف نمود. وضعیت‌هایی که بیان‌کننده توانایی مدافع متناسب با شرایط و زمان است. به‌عنوان مثال در مقابله با حملات منع خدمات، امکانات مدافع شامل وجود فیلترینگ، دیواره آتش، تشخیص حمله منع خدمات، افزایش منابع (پهنای باند، حافظه و پردازش) و ... است. این امکانات در واحد زمان بیانگر شرایط و وضعیت حاکم بر صحنه نبرد از طرف مدافع است. به عبارتی فرآیندهای کاری و قابلیت‌های مدافع، می‌تواند به‌عنوان وضعیت‌های او تعریف گردد. همچنین تمامی این امکانات بایستی بر روی وضعیت کیفیت خدمت‌رسانی مدافع اثر مطلوب بگذارد. وضعیت‌های به‌وجود آمده برای یک خدمات‌دهنده که در مقام یک قربانی ممکن است مورد حمله قرار بگیرد، به شرح زیر خواهد بود [۳]:

1- Intrusion detection system
2- Honey pot

- وضعیت خدمت‌رسانی خوب
- وضعیت خدمت‌رسانی قابل‌قبول (حیثیتی)
- وضعیت خدمت‌رسانی مختل (وخیم)
- درنهایت وضعیت قطع خدمت‌رسانی

۳- کارهای مرتبط

رشیدی و همکاران [۴] برای تجسم حملات چندمرحله‌ای، از روش درخت پسوندی توسعه‌یافته و مدل مارکوف با طول متغیر برای پیش‌بینی رفتارهای نوظهور استفاده کرده است. در مقاله [۵] ارنه ولزل و همکاران سرورهای فرماندهی و کنترل ۱۴ شبکه بات DIRTJUMPER و YODDS را مورد پایش قرار داده و توانسته‌اند اهداف موردحمله منع خدمت توزیع‌شده را روی شبکه فوق ضبط کنند. سپس آن‌ها با استفاده از انواع اندازه‌گیری‌ها از قبیل زمان پاسخ TCP و تحلیل محتوای HTTP توانستند دسترس‌پذیری قربانی‌ها را ارزیابی کنند. آن‌ها نشان دادند که بیش از ۶۵٪ قربانی‌ها توسط حملات منع خدمت توزیع‌شده، به‌شدت آسیب‌پذیر هستند و حملات کم‌تری به شکست منجر می‌شوند. همچنین آقای پنگ و همکاران [۶] برای ارزیابی تأثیر حمله منع خدمت، شاخص‌هایی همچون مصارف پهنای باند، پردازش، حافظه، تأخیر زمان پاسخ، گم‌شدن بسته، زمان (موردنیاز) بازیابی، روش‌های حمله (مصرف منابع، از کار انداختن خدمت و از کار انداختن سسیستم) را در قالب یک ماتریس در آورده و تأثیر ۱۰ نوع حمله شبیه‌سازی‌شده را با استفاده از خوشه‌بندی ترکیبی خاکستری مورد ارزیابی قراردادند و توانستند حملات ده‌گانه را به چهار دسته ضعیف، معمولی، خوب و خیلی خوب تقسیم نمایند. اشکال این روش آن است که نمی‌توان شاخص‌های فوق را (به‌جز تأخیر زمان) بدون همکاری از ماشین قربانی به‌دست آورد. در مرجع [۷] کریستین برای اندازه‌گیری انتشار بات نت‌ها (میزان مخاطره آن‌ها)، معیارهایی را معرفی کرده و آن‌ها را با مدل پیشنهادی خود تبدیل به یک رابطه ریاضی نموده است. او ۱۷ نوع شبکه‌بات متداول دنیا را با استفاده از مدل خود مورد سنجش و مقایسه قرار داده است. معیارهای پیشنهادی شامل تعداد بات‌های شبکه، شیوه آلوده‌سازی، پنهان ماندن، میزان فعالیت، انعطاف‌پذیری، ارزشمندی اهداف موردحمله و خسارات مالی است که ملاک ارزیابی ایشان است. در مرجع [۸]، گوبتا و همکاران یک طرح جدید برای تخمین قدرت حمله منع خدمت ارائه کردند، به‌طوری‌که توانستند بین قدرت حمله و میزان انحراف آنتروپی (مشاهده‌شده)، رابطه‌ای پیداکرده و مدل خود را به‌صورت یک رگرسیون چندجمله‌ای ارائه دهند، همچنین برای ارزیابی مدل، از انواع اندازه‌گیری عملکردهای آماری استفاده کردند و نیز با استفاده از شبیه‌ساز شبکه NS2، حملات منع خدمت توزیع‌شده را با انواع قدرت‌های حمله راه‌اندازی کردند. نتایج شبیه‌سازی نشان داد که می‌توانند قدرت کارآمدی حمله منع خدمت توزیع‌شده را تخمین بزنند. در مقاله پیش‌بینی حملات منع خدمات [۹]، نویسنده مبادرت به جمع‌آوری انواع معیارهای تأثیرگذار و پیامدها بر این نوع حملات داشته است، معیارهای همچون محاسبه هزینه خسارت، افت کیفیت خدمات، بازدهی تراکنش، تأخیر در خدمات و ... به چشم می‌خورد و نیز به نحوه ارزیابی و ابزارهای اندازه‌گیری آن اشاره شده است. در مقاله [۱۰]، نویسنده ابتکاری به خرج داده و مقیاسی همچون سنجه «ریشتر» در اندازه‌گیری زلزله، واحد مقیاس «میداس» را برای تخمین شدت تأثیر حملات منع خدمات از منظر اپراتورهای شبکه ابداع کرده است. به عبارتی تلاش کرده تا معیاری برای اندازه‌گیری خسارات متصور از حملات فوق، در فعالیت‌های یک شرکت خدمات دهنده خدمات اینترنت[1] ارائه دهد تا آن‌ها بتوانند راهبردهای گوناگون را برای کاهش خسارات (مالی) به‌کارگیرند. هزینه خسارات ناشی از حمله، اعم از جریمه، خطر سود آینده، هزینه‌های برقراری لینک نسبت به سود سالانه در نظر گرفته شده است. در مقاله [۱۱] معیارهای در خصوص نحوه محاسبه میزان خسارات ناشی از حملات منع خدمات ارائه شده است. ازجمله خسارت در سود، خسارت در هزینه، خسارت بازسازی و نوسازی، خسارت در برابر تعهدات است که این خسارت ناشی از عدم تعهد به مشتریان است و این‌زمانی محقق می‌شود که به مشتری خدمات مطلوبش داده نشود. با توجه به سه وضعیت موجود، انتظار می‌رود وقتی خسارت در سود خدمات دهنده ناشی می‌شود، کمتر از خسارت در هزینه و بازسازی باشد. به عبارتی بیانگر این مسئله است که عدم تعهد به مشتریان با این ترتیب بیشتر می‌شود و خسارت ناشی از آن بیشتر می‌گردد. یکی از معیارهای مورد ارزیابی، مربوط به کاهش کیفیت خدمات است که موردتوجه مهاجمان حملات منع خدمات است. راهنمای استانداردهای موجود برای پاسخ زمانی ایده‌آل صفحات وب عبارت‌اند از [۱۲]: یک‌دهم ثانیه، زمان ایده آل پاسخ کاربر که هیچ‌گونه تأخیری را حس نمی‌کند. یک ثانیه، حداکثر زمان قابل قبول است که زمان دانلود بیش از یک ثانیه کاربر را خسته می‌کند. ده ثانیه، زمان غیرقابل قبول که کاربر خسته شده و دوست دارد سایت را ترک کند. این اعداد برای طراحی ظرفیت سرور کاربرد زیادی دارند. در مقاله [۱۳] طرحی بر اساس ترکیب فازی مؤلفه‌های تجسم و مدل انتقال باور ارائه‌شده است. این طرح اهداف بعدی یک حمله سایبری چند مرحله‌ای را تجسم نموده و تخمین مناسبی از باورپذیری را ارائه داده است. این تجسم‌ها در قالب قابلیت[2]، فرصت[3]، نیت[4] و رفتار[5] مهاجم در نظر گرفته و با استفاده از مدل انتقال باور هر چهار تجسم را مورد تلفیق قرار داده

1- Internet service provider (ISP)
2- Capability
3- Opportunity
4- Intent
5- Behavior

است. در طرح فوق با استفاده از دادگان معتبر، بر اساس حملات با نویز بالا، حملات مخفی و حملات با تأثیر بالا و پایین مورد ارزیابی قرارگرفته است و نتایج شبیه‌سازی هم به‌صورت سناریوهایی تعریف‌شده است که نشان از افزایش میزان دقت با میانگین هفده‌درصدی در تجسم حملات سایبری چند مرحله‌ای دارد. اکبری در [۳] وضعیت خدمت‌رسانی سرورهای قربانی در مواجه با حملات منع خدمات توزیع‌شده را به چهار دسته وضعیت خدمت‌رسانی خوب، وضعیت خدمت‌رسانی قابل‌قبول (حیثیتی)، وضعیت خدمت‌رسانی مختل یا وخیم و وضعیت قطع خدمت‌رسانی تقسیم نموده است. در [۱۴] هایتائو در رساله خود به مدل‌سازی و استنتاج احتمالاتی برای دنباله‌ها (روندها)ی حملات شبکه‌ای مبهم، پرداخته است. ایشان دنباله‌های حملات را از مجموعه داده حاوی هشدارهای سیستم تشخیص نفوذ مورداستفاده قرار داده و با استفاده از طرح پیشنهادی خود به مقایسه دسته‌بندی انواع دنباله‌ها می‌پردازد. وی دنباله‌های مشاهده‌شده را به چهار نوع حمله و همچنین دنباله‌ها را به لحاظ پیچیدگی، به سه دسته تقسیم کرده است. دسته اول اقدامات حمله اصلی بدون مبهم‌سازی (پاک[1])، دسته دوم اقدامات حمله مبهم (مختل شده[2]) و دسته سوم حملات با الگوریتم استنتاجی[3] است. ایشان نتایج را برمبنای طول دنباله‌ها مورد ارزیابی قرار داده است.

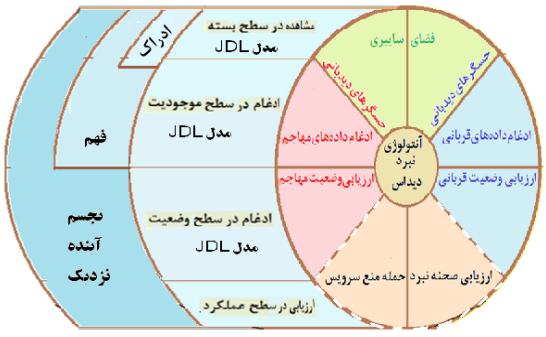
وی در تخمین خود به این نتیجه رسیده است که هراندازه سطح مبهم سازی دنباله حمله بیشتر باشد، دقت مورد انتظار دسته‌بندی، کاهش میابد و همچنین هراندازه طول دنباله‌ها بیشتر باشد، دقت دسته‌بندها بیشتر می‌گردد.

در پایان این بخش یادآوری می‌گردد که کارهای مرتبط ارائه‌شده، به‌طور مستقیم راجع به تحقیق پیشنهادی مطلبی را عنوان نکرده‌اند، بلکه هر یک به بخشی از فعالیت‌های مرتبط با این پایان‌نامه مربوط می‌شوند.. همچنین در حوزه سایبری، مقالات آگاهی وضعیتی از منظر دفاع سایبری مطالبی را ارائه کردند و نگارنده در خصوص آفند سایبری نتوانست منبعی را بیابد و این نشانه مبنی‌بر این مسئله است که اولاً در حوزه آفندی ملاحظاتی وجود دارد و دوم این‌که در حوزه نظامی کسی تمایل به انتشار این‌گونه مطالب ندارد و سوم آن‌که عموم این منابع مرتبط، به دانشگاه‌های نظامی دنیا تعلق دارد و سایر دانشگاه‌ها در این خصوص کاری انجام نداده‌اند. ازاین‌رو، نگارنده تلاش کرده است در حوزه آفند سایبری (منع خدمات)، ارائه الگوی مدل آگاهی وضعیتی مناسبی را پیشنهاد دهد.

۴- چارچوب پیشنهادی آگاهی از وضعیت صحنه نبرد

حسگرها در فضای سایبری مبادرت به دیده‌بانی و رصد میزبان‌های خدمات دهنده (قربانی) و شبکه بات مهاجم می‌کنند. در این میان وجود یک هستان‌شناسی کارآمد، تمامی بخش‌ها را پشتیبانی کرده و سؤال «چه‌کارهایی باید کرد؟» را پاسخ‌گو است.

در حالت کلی می‌توان ارزیابی وضعیت صحنه نبرد حمله منع خدمات را به‌صورت شکل (۲) متصور شد که سمت راست مربوط به قربانی و سمت چپ مربوط به مهاجم است. مدل پیشنهادی با مدل پنج لایه[4] JDL [۱۵] و مدل سه لایه آگاهی وضعیتی اندسلی[5] [۱۶] دارای هم‌پوشانی است با این تفاوت که این مدل توسط یک هستان‌شناسی نبرد منع خدمات پشتیبانی می‌گردد. هریک از طرفین درگیری بعد از انجام یک حمله، پیگیری خواهند کرد تا از وضعیت طرف مقابل آگاهی یابند و بدانند اثر حمله و دفاع آن‌ها به چه میزان بوده است. درصحنه جنگ‌های سایبری نیز به همین صورت است و حمله‌کننده تلاش خواهد کرد تا از وضعیت قربانی و اثر حمله خود مطلع شود تا بتواند تصمیمات مناسبی بگیرد. اما در این راستا مشکلات بسیاری وجود دارد، به‌عنوان مثال ممکن است قربانی تمهیداتی بیندیشد و به‌کار گیرد [۱] که حمله‌کننده را در مورد تأثیر حمله گمراه کند. در این بخش در نظر است صحنه نبرد حمله منع خدمت با در نظر گرفتن وضعیت‌های مهاجم و مدافع به‌صورت یکپارچه تبیین و موردبررسی قرار گیرند (قسمت مشخص‌شده با خط‌چین در شکل). بنابراین، در ادامه، بار دیگر وضعیت‌ها با در نظر گرفتن شرایط طرفین تبیین می‌گردند.



شکل (۲): شمای کلی طرح پیشنهادی ارزیابی صحنه نبرد حمله منع خدمات.

۴-۱- آگاهی از وضعیت مهاجم

در این مرحله وضعیت‌های مهاجم با ترکیب تعدد شبکه بات شامل افزایش، کاهش و روش حمله، تشکیل می‌گردد، به‌طوری‌که شرایط

1- Clean
2- Noise
3- InfAlg

4- Joint Direction Literary
5- Endsley

فوق ۹ رابطه مختلف ذیل را به‌وجود آورده که در جدول (۱) برای هر یک نماد و شماره‌گذاری مشخصی در نظر گرفته شده است.

جدول (۱): نماد و شماره‌گذاری نُه وضعیت مختلف مهاجم

آغاز حمله با توان مشخص با روش جدید	= SA 1:با روش جدید and	X =< تعداد بات فعلی	∀
ادامه حمله با توان قبلی با روش قبلی	= SA 2:با روش قبلی and	تعداد بات قبلی = تعداد بات فعلی	∀
ادامه حمله با توان قبلی با روش جدید	= SA 3:با روش جدید and	تعداد بات قبلی = تعداد بات فعلی	∀
ادامه حمله با افزایش بات با روش قبلی	= SA 4:با روش قبلی and	تعداد بات قبلی < تعداد بات فعلی	∀
ادامه حمله با افزایش بات با روش جدید	= SA 5:با روش جدید and	تعداد بات قبلی < تعداد بات فعلی	∀
ادامه حمله با کاهش بات با روش قبلی	= SA 6:با روش قبلی and	تعداد بات قبل > تعداد بات فعلی	∀
ادامه حمله با کاهش بات با روش جدید	= SA 7:با روش جدید and	تعداد بات قبل > تعداد بات فعلی	∀
توقف موقت حمله	= SA 8:با روش قبلی and	Y =< تعداد بات فعلی	∀
توقف کامل حمله	= SA 9:با روش قبلی and	۰ = تعداد بات فعلی	∀

مهاجم بنابر شرایط پیشرویش و وضعیت مدافع می‌تواند وضعیت خود را تغییر دهد. تغییر روش به‌منظور طرح جدید حمله تلقی می‌شود و افزایش بات به‌منظور اعمال اشباع ترافیک صورت می‌گیرد و کاهش شبکه‌بات نیز به‌منظور صرفه‌جویی صورت می‌گیرد. بنابراین، در مدل ما، این تغییر وضعیت‌ها با مفروضات ذیل مقررشده است.

مفروضات حرکت گذرها

۱. بعد از حمله، امکان بازگشت به وضعیت شروع وجود ندارد.
۲. امکان بازگشت از توقف دائم وجود ندارد. یعنی عملیات با شکست یک‌طرف به پایین رسیده است.
۳. برای رسیدن به توقف دائم (SA9)، لازم است از وضعیت توقف موقت (SA8)، گذر شود.
۴. از کلیه وضعیت‌ها (به‌جز SA9 و SA1) می‌توان به‌وضعیت توقف موقت گذر کرد.
۵. همواره حمله از وضعیت شروع یا SA1 آغاز می‌شود و وضعیت بعدی آن ادامه حمله قبلی است.
۶. از وضعیت‌های ادامه حمله قبلی (SA2 یا SA3) می‌توان به وضعیت‌های ادامه حمله با کاهش یا افزایش بات گذر کرد.
۷. از وضعیت‌های افزایش بات (SA4 و SA5) نمی‌توان به وضعیت‌های کاهش بات و توقف‌ها، گذر کرد و نیز از وضعیت‌های کاهش بات (SA6 وSA7) نمی‌توان به وضعیت‌های افزایش بات گذر کرد. (یعنی به‌طور مستقیم امکان گذر از افزایش یا کاهش شبکه بات به یکدیگر معنا ندارد)

۴-۲- آگاهی از وضعیت مدافع

همچنین وضعیت‌های مدافع از ترکیب پاسخ‌های تأخیر زمانی ماشین قربانی و به‌کارگیری تمهیدات امنیتی، تشکیل شده است که در شرایط مختلف هشت رابطه ذیل را به‌وجود آورده که برای هر یک نماد و شماره‌گذاری مشخصی در جدول (۲) در نظر گرفته شده است. مدافع بنابر شرایط پیشرویش می‌تواند وضعیت خود را تغییر دهد. تغییر تمهید امنیتی به‌منظور طرح جدید دفاعی تلقی می‌شود. بنابراین، در مدل ما، این تغییر وضعیت‌ها با مفروضات ذیل مقررشده است.

مفروضات حرکت گذرها

۱. همواره دفاع از وضعیت توقف، آغاز نمی‌شود.
۲. برای رسیدن به توقف دائم (SD8)، لازم است از وضعیت توقف موقت (SD7) گذر کند.
۳. امکان بازگشت از توقف دائم وجود ندارد. یعنی عملیات با شکست یک‌طرف به پایین رسیده است.
۴. از وضعیت خدمات خوب می‌توان به وضعیت قابل‌قبول یا بالعکس گذر کرد.
۵. از وضعیت‌های خدمات قابل‌قبول (SD3 یا SD4) می‌توان به وضعیت‌های مختل و بالعکس گذر کرد.
۶. از وضعیت‌های مختل (SA5 و SA6) می‌توان به وضعیت توقف موقت و بالعکس گذر کرد.

جدول (۲): نماد و شماره‌گذاری هشت وضعیت مختلف مدافع

سرویس خوب بدون تمهید	= SD 1 :بدون تمهید امنیتی[1]	and	∀a <= D.T < b
سرویس خوب با تغییر تمهید	= SD 2 :با تمهید امنیتی[2]	and	∀a <= D.T < b
سرویس قابل‌قبول بدون تمهید	= SD 3 :بدون تمهید امنیتی	and	∀b <= D.T < c
سرویس قابل‌قبول با تغییر تمهید	= SD 4 :با تمهید امنیتی	and	∀b <= D.T < c
سرویس وخیم بدون تمهید	= SD 5 :بدون تمهید امنیتی	and	∀c <= D.T < d
سرویس وخیم با تغییر تمهید	= SD 6 :با تمهید امنیتی	and	∀c <= D.T < d
قطع موقت سرویس	= SD 7 :بدون تمهید امنیتی	and	∀d <= D.T
قطع کامل سرویس	= SD 8 :بدون تمهید امنیتی	and	∀d <= D.T

این مجموعه حالت‌ها را می‌توان در قالب مدل مارکوف در نظر گرفت که دارای ۷۲ گره (حالت) است و یال‌های آن شامل گذرهای محتملی است که می‌تواند رخ دهد. لذا از منظر یک ناظر می‌توان ترکیبی از هر دو وضعیت مهاجم و مدافع را یکجا تصور کرد و مجموعه‌ای از حالت‌ها را با نماد State به‌وجود آورد. همچنین تغییر وضعیت‌ها با استفاده از یال‌ها در نظر گرفته‌شده است که می‌توان مجموعه یال‌ها را با نماد Step نشان داد.

$$State = \{s \; ; \; s \in [SA_i \, , SD_{j\_*}]\}$$

1- Security Method of Previous (SecMPre)
2- Security Method of New (SecMNew)

$$Step = \{(s,t) ; s,t \in State , s \longrightarrow t \}$$

مجموعه حالت‌ها را می‌توان به‌صورت یک ماتریس دوبعدی در نظر گرفت که وضعیت‌های مدافع و مهاجم به ترتیب در سطرها و ستون‌ها قرار دارند، همان‌گونه که در جدول (۳) نشان داده‌شده است. این ماتریس دارای ۷۲ عضو است که شروع حمله می‌تواند یکی از وضعیت‌های ستون SA_1 باشد. شایان‌ذکر است که به‌جز وضعیت‌های ۵۵ و ۶۴ بقیه وضعیت‌ها می‌توانند منطقی باشند.

جدول (۳): ماتریس ترکیبی وضعیت‌های مهاجم و مدافع

	SA_1	SA_2	SA_3	SA_4	SA_5	SA_6	SA_7	SA_8	SA_9
SD_1	۱	۲	۳	۴	۵	۶	۷	۸	۹
SD_2	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸
SD_3	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷
SD_4	۲۸	۲۹	۳۰	۳۱	۳۲	۳۳	۳۴	۳۵	۳۶
SD_5	۳۷	۳۸	۳۹	۴۰	۴۱	۴۲	۴۳	۴۴	۴۵
SD_6	۴۶	۴۷	۴۸	۴۹	۵۰	۵۱	۵۲	۵۳	۵۴
SD_7	۵۵	۵۶	۵۷	۵۸	۵۹	۶۰	۶۱	۶۲	۶۳
SD_8	۶۴	۶۵	۶۶	۶۷	۶۸	۶۹	۷۰	۷۱	۷۲

در این پژوهش پیش‌فرض دنباله‌های حمله از وضعیت یک شروع می‌شوند. بنابراین می‌توان وضعیت طرفین را به‌صورت صفحات ماتریس با رویداد گسسته زمان همانند شکل (۳) در نظر گرفت.

شکل (۳): وضعیت ترکیبی مهاجم و مدافع درصحنه نبرد

۴-۳- معیارهای ارزیابی صحنه نبرد

در این مرحله اگر فرض شود (SA_1 , SD_1) حمله‌ای توسط مهاجم رخ دهد و مدافع شروع به دفاع کند، وضعیت‌ها متناسب با شرایط طرفین به وجود می‌آید و این کش‌وقوس‌ها موجب تغییر وضعیت‌ها در ماتریس می‌گردد تا اینکه بعد از طی مدت‌زمانی یکی از طرفین مغلوب شود و عملیات خدمت‌رسانی یا عملیات حمله متوقف شود.

حال اگر فرض شود قبل از اتمام مخاصمه، عملکرد طرفین مورد ارزیابی قرار گیرد، می‌توان قابلیت آمادگی رزم (مهاجم و مدافع) اعم از مهارت، سرعت پاسخ (عکس‌العمل)، تداوم عملیات و امکانات مورداستفاده را مدنظر قرارداد که ما در این پژوهش آن را خبرگی طرفین در نظر می‌گیریم. همچنین عملکرد دسترس‌پذیری به خدمات هم می‌تواند جداگانه در مورد مدافع در نظر گرفت.

معیارهای (قابلیت) مهارت و امکانات دو متغیر مستقل هستند که، دستاورد و نتیجه آن‌ها سرعت پاسخ و تداوم عملیات را حاصل می‌کند و درنهایت پیامد سرعت پاسخ و تداوم عملیات موجب تأثیر در معیار دسترس‌پذیری به خدمات می‌گردد.

$$\left(P^1.T^2\right) \Longrightarrow \left(C^3.RS^4\right) \Longrightarrow Ava$$

در ادامه هریک از معیارها جداگانه توضیح داده می‌شود.

مهارت: در لغت‌نامه دهخدا مهارت به معنی زیرکی و رسایی در کار و استادی و زبردستی است، ما به‌کارگیری توانایی‌ها و تجربیات کارا، که سرعت عمل و دقت لازم را درصحنه نبرد در پی داشته باشد را مهارت گوییم.

مهارت مهاجم: به‌کارگیری توانایی‌ها و تجربیات کارا (تکنیک‌ها مانند تغییر روش‌ها و تاکتیک‌ها مانند افزایش یا کاهش بات) که وضعیت خدمت‌رسانی مدافع را تنزل دهد. به‌طوری‌که مهاجم ماهر باید قادر باشد اقدامات مدافع را درست درک کند و اقدام صحیح متقابل انجام دهد.

$$PA^5_{general} = \{(s,t) \in Step ; ([SA_i , SD_{k\_*}] , [SA_j, SD_{k+1\_*}]) \}$$
$$(i=1,\ldots,8 ; j=1,\ldots,7 ; k=1,\ldots,4)$$

کلیه یال‌هایی که صرف‌نظر از وضعیت مهاجم، منجر به تنزل وضعیت مدافع شود.

$$PA_{sequence} = \{(m,n)_{sequence} ; (m,n) \in PA_{general} \}$$

کلیه (تکراری یا غیرتکراری) از یک دنباله صحنه نبرد که در مجموعه $PA_{general}$ باشند را مجموعه $PA_{sequence}$ می‌نامیم که تعداد اعضای این مجموعه را PA_{total} در نظر می‌گیریم. بنابراین، PA_{total} میزان مهارت مهاجم را بیان می‌کند.

$$PA_{total} = count(PA_{sequence})$$
$$(PA_{total}/SeqLen, SeqLen)$$

مهارت مدافع: به‌کارگیری توانایی‌ها و تجربیات کارا (تمهیدات دفاعی و امنیتی) که وضعیت خود را بهبود دهد. به‌طوری‌که مدافع ماهر باید قادر باشد اقدامات مهاجم را درست درک کند و با تمهیدات صحیح، آن‌ها را ناکارآمد سازد.

$$PD^6_{general} = \{ (s,t) \in Step ; ([SA_i , SD_{k\_*}] , [SA_j , SD_{k-1\_*}])$$
$$or ([SA_i , SD_{1\_*}] , [SA_j , SD_{1\_*}]) \}$$
$$(i=1,\ldots,8 ; j=1,\ldots,9 ; k=2,\ldots,4)$$

کلیه یال‌هایی که منجر به بهبود وضعیت مدافع می‌شود یا یال‌هایی که مدافع را در وضعیت خوب نگه می‌دارد.

$$PD_{sequence} = \{(m,n)_{sequence} ; (m,n) \in PD_{general} \}$$

کلیه یال‌های (تکراری یا غیرتکراری) از یک دنباله صحنه نبرد که در مجموعه $PD_{general}$ باشند را مجموعه $PD_{sequence}$ می‌نامیم که

1- Professional
2- Tools
3- Continue
4- Response Speed
5- Professional Attack
6- Professional Defense

تعداد اعضای این مجموعه را PD_{total} در نظر می‌گیریم. بنابراین، PD_{total} میزان مهارت مدافع را بیان می‌کند.

$PD_{total} = count(PD_{sequence})$

$(PD_{total}/SeqLen, SeqLen)$

زمان پاسخ: زمانی که طول می‌کشد تا طرفین اقدام تهاجمی یا تدافعی را درست درک کند و اقدام کارسازی در مقابل آن انجام دهد.

متوسط زمان پاسخ مهاجم: مدت‌زمانی که طول می‌کشد که مهاجم بتواند اقدامات مدافع اعم از انواع تمهیدات امنیتی دفاعی را درست درک کند و با فن[1]ها و تدبیر[2]های کارساز اثر دفاع را کاهش دهد و موجب تنزل خدمات‌دهی مدافع شود.

$RSA_l^3 = SeqNum(\text{first event } ([SA_i , SD_{k\_*}] , [SA_j , SD_{k+1\_*}]))- SeqNum(\text{first event } ([SA_i , SD_{k\_*}] , [SA_j, SD_{k-1\_*}]))$

$RSA_{Total} = \{(\sum_{l=1}^{SeqLen} RSA_l)/Count(RSA_l), SeqLen\}$

تعداد گام‌هایی که طول می‌کشد تا مهاجم، اولین اقدام را در مقابل اولین اقدام مؤثر (مهارت) مدافع از خود عکس‌العمل نشان داده تا وضعیت مدافع تنزل یابد.

بنابراین میانگین تعداد این گام‌ها را در طول مدت حمله به‌عنوان متوسط زمان پاسخ مهاجم در نظر گرفته می‌شود.

متوسط زمان پاسخ مدافع: مدت‌زمانی که طول می‌کشد که مدافع بتواند اقدامات مهاجم اعم از نوع حمله، توان حمله را درست درک کند و با تمهیدات کارساز اثر حمله را کاهش دهد و موجب بهبودی یا بدتر نشدن وضعیت فعلی شود.

$RSD^4 = SeqNum(\text{first event } ([SA_i, SD_{k\_*}], [SA_j, SD_{k-1\_*}])) - SeqNum(\text{first event}([SA_i, SD_{k\_*}], [SA_j , SD_{k+1\_*}]))$

$RSD_{Toatal} = \{(\sum_{l=1}^{SeqLen} RSD_l)/Count(RSD_l), SeqLen\}$

تعداد گام‌هایی که طول می‌کشد تا مدافع، اولین اقدام را در مقابل اولین اقدام مؤثر (مهارت) مهاجم از خود عکس‌العمل نشان داده تا وضعیت مدافع بهبود یابد.

بنابراین، میانگین تعداد این گام‌ها را در طول مدت دفاع به‌عنوان متوسط زمان پاسخ مدافع در نظر گرفته می‌شود.

تداوم: میل به استمرار (افزایش مدت‌زمان) در حمله یا دفاع تا رسیدن به هدف. واحد اندازه‌گیری این معیار می‌تواند به شکل زوج مرتب (زمان یا گام‌های صرف شده، نسبت فراوانی تداوم حمله به‌کل زمان) باشد.

تداوم در حمله: تمایل مهاجم به افزایش زمان حمله درحالی‌که وضعیت مدافع در شرایط نامطلوب است.

$CA^5_{general} = \{(s,t) \in Step ; ([SA_i, SD_{k>2\_*}] , [SA_j, SD_{k>2\_*}])\}$ $(i=1,...,8 ; j=1,...,7)$

کلیه یال‌هایی که وضعیت مدافع را به حالت وخیم، قطع موقت و قطع دائم انتقال می‌دهد.

$CA_{sequence} = \{(m,n)_{sequence} ; (m,n) \in CA_{general} \}$

کلیه یال‌های (تکراری یا غیرتکراری) از یک دنباله صحنه نبرد که در مجموعه $CA_{general}$ باشند را مجموعه $CA_{sequence}$ می‌نامیم که تعداد اعضای این مجموعه را CA_{total} در نظر می‌گیریم. بنابراین CA_{total} اندازه تداوم حمله را بیان می‌کند.

$CA_{total} = count(CA_{sequence})$

$(CA_{total}/SeqLen, SeqLen)$

تمایل ادامه حمله در واحد زمانی زیاد به‌شرط آن‌که وضعیت خدمات‌دهی مدافع را در وضعیت نامطلوب نگه دارد یا آن را از کار بیندازد.

تداوم در دفاع: تمایل مدافع به افزایش زمان دفاع و ارائه خدمات مطلوب درحالی‌که اقدامات مهاجم ناکارآمد باشد و موجب پشیمانی گردد.

$CD^6_{general} = \{(s,t) \in Step ; ([SA_i , SD_{k<=2\_*}] , [SA_j, SD_{k<=2\_*}])\}$ $(i=1,...,8 ; j=1,...,7)$

کلیه یال‌هایی که وضعیت مدافع را به حالت خدمات خوب یا قابل‌قبول انتقال می‌دهد.

$CD_{sequence} = \{(m,n)_{sequence} ; (m,n) \in CD_{general} \}$

کلیه یال‌های (تکراری یا غیرتکراری) از یک دنباله صحنه نبرد که در مجموعه $CD_{general}$ باشند را مجموعه $CD_{sequence}$ می‌نامیم که تعداد اعضای این مجموعه را CD_{total} در نظر می‌گیریم. بنابراین CD_{total} اندازه تداوم دفاع را بیان می‌کند.

$CD_{total} = count(CD_{sequence})$

$(CD_{total}/SeqLen, SeqLen)$

امکانات، تجهیزات و ابزار: مجموعه توانمندی‌های سخت‌افزاری و نرم‌افزاری مهاجم (شبکه بات، روش‌ها و غیره) یا مدافع (فایروال، سیستم تشخیص حمله و غیره) که موجب قدرتمندی وی می‌گردد.

1 Technique
2 Tactic
3 Response Speed Attack
4- Response Speed Attack

5- Continue Attack
6- Continue Defense

امکانات، تجهیزات و ابزار مهاجم: به‌منظور سنجش این معیار به دارایی‌هایی به کار گرفته‌شده‌ی مهاجم رجوع می‌کنیم که میزان حداکثر بات رؤیت شده و تعداد روش‌های غیرتکراری استفاده‌شده می‌توانند بیانگر میزان قدرتمندی مهاجم باشند. به عبارتی برای بیان امکانات، تجهیزات و ابزار مهاجم از زوج مرتب (میزان حداکثر بات, تعداد روش‌های غیرتکراری) استفاده می‌کنیم.

برای تعداد روش‌های رؤیت شده داریم:

$MethA^{1}_{general} = \{(s,t) \in Step ; ([SA_i , SD_{x\_*}] , [SA_j, SD_{y\_*}]) \} (i=1,...,8 ; j=1,3,5,7 ; x,y=1,...,5)$

کلیه یال‌هایی که وضعیت مهاجم را (صرف‌نظر از وضعیت مدافع)، به وضعیت‌های تغییر روش جدید می‌برد.

$MethA_{sequence} = \{(m,n)_{sequence} ; (m,n) \in MethA_{general} \}$

کلیه یال‌های (تکراری یا غیرتکراری) از یک دنباله صحنه نبرد که در مجموعه $MethA_{general}$ باشند را مجموعه $MethA_{sequence}$ می‌نامیم که تعداد اعضای این مجموعه را $MethA_{total}$ در نظر می‌گیریم. بنابراین، $MethA_{total}$ تعداد روش‌های رؤیت شده را بیان می‌کند.

$MethA_{total} = count(MethA_{sequence}/SeqLen)$

برای بیان میزان حداکثر بات رؤیت شده داریم:

$IncBot^{2}_{general} = \{(s,t) \in Step ; ([SA_i , SD_{x\_*}] , [SA_j, SD_{y\_*}]) \} (i=1,...,8 ; j=4,5 ; x,y=1,...,5)$

$IncBot_{sequence} = \{(m,n)_{sequence} ; (m,n) \in IncBot_{general} \}$

$IncBot_{total} = count(IncBot_{sequence})$

$DecBot^{3}_{general} = \{(s,t) \in Step ; ([SA_i , SD_{x\_*}] , [SA_j, SD_{y\_*}]) \} (i=1,...,8 ; j=6,7 ; x,y=1,...,5)$

$DecBot_{sequence} = \{(m,n)_{sequence} ; (m,n) \in DecBot_{general} \}$

$DecBot_{total} = count(DecBot_{sequence})$

کلیه یال‌هایی که وضعیت مهاجم را (صرف‌نظر از وضعیت مدافع)، به وضعیت توقف موقت می‌برد.

$StopBot_{total} = count(StopBot_{sequence})$

کلیه یال‌هایی که وضعیت مهاجم را (صرف‌نظر از وضعیت مدافع)، به وضعیت ادامه حمله بدون افزایش یا کاهش بات می‌برد.

$UCBot_{total}^{4} = count(UCBot_{sequence})$

$NumBot_{sequence} = iniBot + (IncBot_{total} - DecBot_{total}) * \frac{m}{iniBot}$

$$MaxBot = \begin{cases} NumBot_{sequence} & NumBot_{sequence} > iniBot \\ iniBot & NumBot_{sequence} > iniBot \end{cases}$$

$TA^{5} = (MethA_{total} , MaxBot)$

$TA_{Total} = MethA_{total} + \log(MaxBot)$

امکانات، تجهیزات و ابزار مدافع: به‌منظور سنجش این معیار به دارایی‌هایی به‌کار گرفته‌شده مدافع رجوع می‌کنیم که تعداد تمهیدات غیرتکراری استفاده‌شده، می‌تواند بیان‌گر میزان قدرتمندی مدافع باشد.

$TD^{6}_{general} = \{(s,t) \in Step ; ([SA_i , SD_{x\_*}] , [SA_j, SD_{y\_1}]) \} (i,j=1,...,8 ; x=1,2,3,4 ; y=1,2,3)$

کلیه یال‌هایی که وضعیت مدافع را (صرف‌نظر از وضعیت مهاجم)، به وضعیت‌های تغییر تمهید می‌برد.

$TD_{sequence} = \{(m,n)_{sequence} ; (m,n) \in TD_{general} \}$

کلیه یال‌های (تکراری یا غیرتکراری) از یک دنباله صحنه نبرد که در مجموعه $TD_{general}$ باشند را مجموعه $TD_{sequence}$ می‌نامیم که تعداد اعضای این مجموعه را TD_{total} در نظر می‌گیریم. بنابراین، TD_{total} تعداد تمهیدهای رؤیت شده را بیان می‌کند.

$TD_{total} = count(TD_{sequence})/SeqLen$

دسترس‌پذیری[7] به خدمات: میزان دسترس‌پذیری به خدمات (در طول دنباله حمله) با میزان کیفیت خدمات تقریب زده می‌شود به‌طوری‌که فرض می‌گردد هرقدر کیفیت خدمات کاهش یابد موجب کاهش دسترس‌پذیری شود. بنابراین، میانگین ضرایب اثر وضعیت‌های مدافع، بیان‌گر میزان دسترس‌پذیری به خدمات است.

$State = \{s ; s \in [SA_i , SD_{j\_*}]\}$

$$Ava_i = \begin{cases} 1 & S_i \in SD_1 \\ 0.9 & S_i \in SD_2 \\ 0.4 & S_i \in SD_3 \\ 0.05 & S_i \in SD_4 \\ 0 & S_i \in SD_5 \end{cases}$$

$$AvaTotal = \frac{\sum_{i=1}^{SeqLen} Ava_i}{SeqLen}$$

پیروزی طرفین: پیروزی زمانی مفهوم پیدا می‌کند که طرفین، اهداف خود را تحقق دهند. هدف مدافع ارائه خدمات در حد مطلوب و قابل‌قبول و هدف مهاجم از کار انداختن و یا کاهش خدمت‌رسانی مدافع است. به عبارتی اگر مهاجم بتواند در طول مدت حمله، خدمت‌رسانی مدافع را به وضعیت‌های مختل (وخیم)، قطع موقت و درنهایت به قطع دائم ببرد، پیروز میدان است و در غیر این صورت مدافع برنده صحنه است.

$$Win = \begin{cases} attacker & Ava = 0 \\ defender & Ava > 0.7 \end{cases}$$

درصورتی‌که مهاجم نتواند خدمات مدافع را قطع کند، پیروز میدان به میزان کاهش خدمت‌رسانی (که خسارت‌بار باشد) بستگی

1- Methods Attack
2- Increase Bot
3- Decrease Bot
4- Unchanged Bot
5- Tools Attack

6- Tools Defense
7- Availability

دارد. به فرض اینکه تراکنش مالی (بانک) نیازمند دسترس‌پذیری بیش از ۴۰٪ باشد، می‌توان حد آستانه پیروزی طرفین را همین میزان در نظر گرفت.

$$\text{Win} = \begin{cases} \text{attacker} & ; \quad \text{Ava} \le 0.4 \\ \text{defender} & ; \quad \text{Ava} > 0.4 \end{cases}$$

محاسبه درجه پیروزی:

تعریف اثر: اقدامات مهاجم و مدافع موجب اثرگذاری در خدمات‌دهی مدافع می‌گردد. این خدمات‌دهی را می‌توان در دو کلاس اثر تعریف کرد.

اثر کلاس بهبود (A): فراوانی یال‌هایی که به وضعیت‌های خوب و قابل‌قبول وارد می‌شوند.

$$\text{Imp}_G = \text{count}\ \{ (s,t) \in \text{Step} ; ([SA_i , SD_k] , [SA_j , SD_{k<=4}]) \} \quad (i=1,\dots,8 ; j=1,\dots,9 ; k=1,2,3,4)$$

اثر کلاس فشار (B): فراوانی یال‌هایی که به وضعیت‌های وخیم، توقف موقت و توقف کامل وارد می‌شوند.

$$\text{Imp}_B = \text{count}\ \{ (s,t) \in \text{Step} ; ([SA_i , SD_k] , [SA_j , SD_{k>4}]) \} \quad (i=1,\dots,8 ; j=1,\dots,9 ; k=5,6,7,8)$$

به‌منظور سنجش درجه پیروزی طرف برنده، لازم است نسبت فراوانی کلاس‌ها به طول دنباله اندازه‌گیری شود. به عبارتی اگر مهاجم پیروز میدان باشد، درجه پیروزی آن نسبت فراوانی اثر کلاس B به طول دنباله است و برعکس.

$$DegWin = \begin{cases} \dfrac{\text{Imp}_B}{\text{SeqLen}} & ; \ Win = attacker \\ \dfrac{\text{Imp}_G}{\text{SeqLen}} & ; \ Win = defender \end{cases}$$

در ادامه به‌منظور ارزیابی صحنه نبرد، مبادرت به تبیین تجسم آینده از صحنه نبرد می‌شود. هم‌اکنون شرایط برای ارزیابی صحنه نبرد فراهم‌شده است که در ادامه با مدل‌سازی، شبیه‌سازی و ارزیابی، این کار تکمیل می‌گردد.

۵- مدل آگاهی وضعیتی مبتنی‌بر فرایند مارکوف

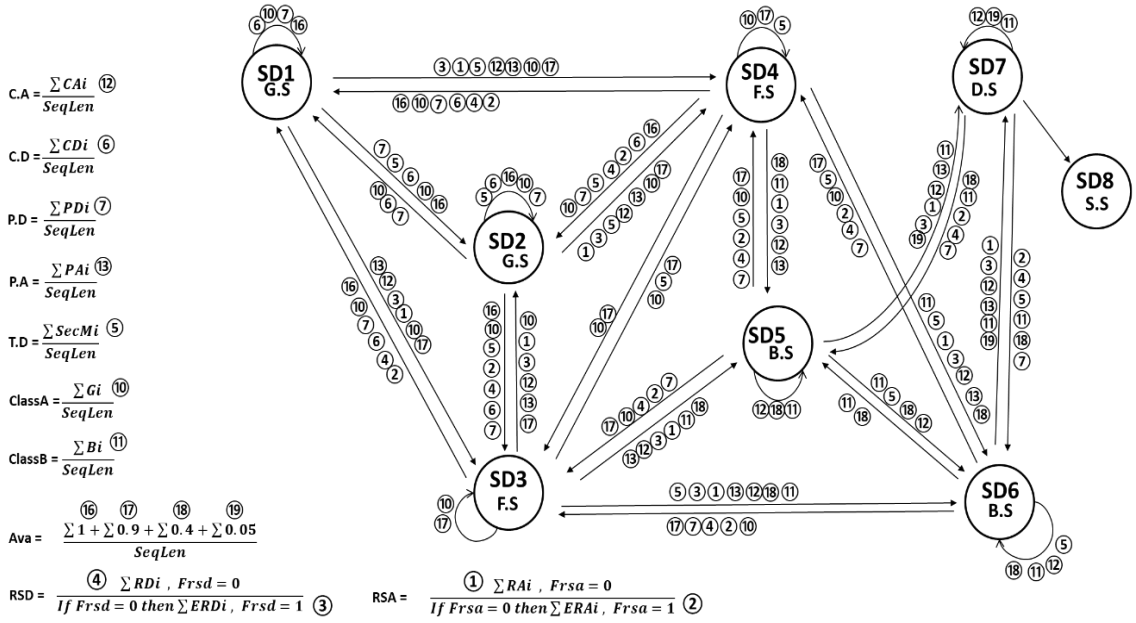
همان‌گونه که در مدل پیشنهادی بیان شد با ورودی وضعیت‌ها به مدل، یال‌های گذر وضعیت‌ها به حرکت درمی‌آیند و میزان آمادگی طرفین با به‌کارگیری امکانات خود صحنه نبرد را شکل می‌دهند.

بنابراین ما مدل آگاهی وضعیتی صحنه نبرد را مبتنی بر فرایند مارکوف طراحی کرده‌ایم که بتواند امکانات، مهارت، عکس‌العمل و تداوم در حمله و دفاع، محاسبات نماید.

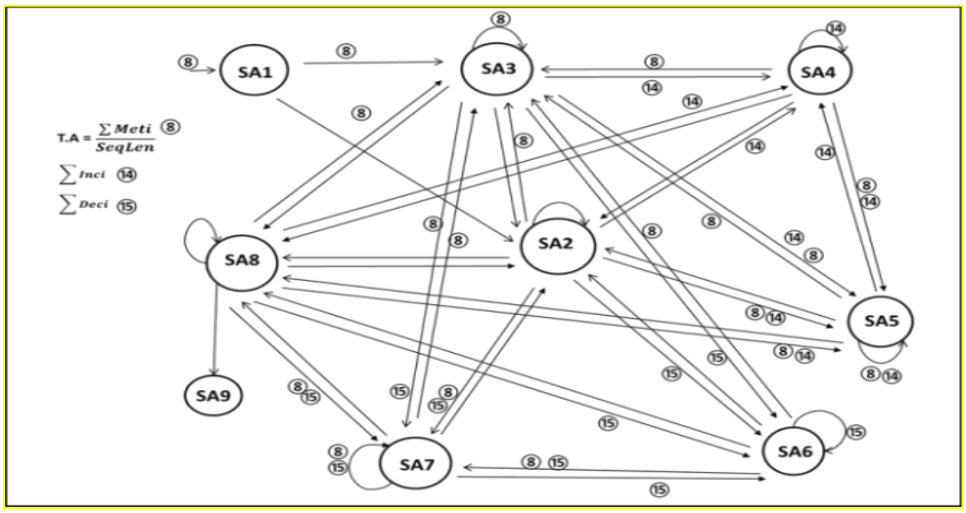
در شکل (۴) این مدل در وضعیت مدافع نشان داده‌شده است. بدیهی است برخی از ویژگی‌های مهاجم نیز در این مدل مورد سنجش قرار می‌گیرد.

تمام روابط این ویژگی‌ها (در بخش قبل) در کنار شکل (۴) قابل‌ملاحظه است که هرکدام با شماره ویژه‌ای نشانه‌گذاری شده است. لذا درگذر یال‌ها هر یک از روابطی که نیاز است محاسبه شود با شماره ویژه علامت‌گذاری شده است. بنابراین، با اعمال ورودی (وضعیت مهاجم و مدافع) به این مدل، وضعیت مدافع از وضعیت قبلی به وضعیت بعدی تغییر کرده و روابط مربوط به آن یال موردمحاسبه قرار می‌گیرد.

بدیهی است با این مدل می‌توان گام‌به‌گام تمام ویژگی‌های صحنه نبرد را مورد محاسبه و ارزیابی قرار داد. همچنین بخش دیگر مدل مربوط به آگاهی وضعیتی صحنه نبرد مبتنی بر مهاجم است که در شکل (۵)، فرایند این مدل مبتنی فرایند مارکوف در وضعیت مهاجم نشان داده شده است.



شکل (۴): مدل آگاهی وضعیتی صحنه نبرد در وضعیت مدافع مبتنی بر فرایند مارکوف

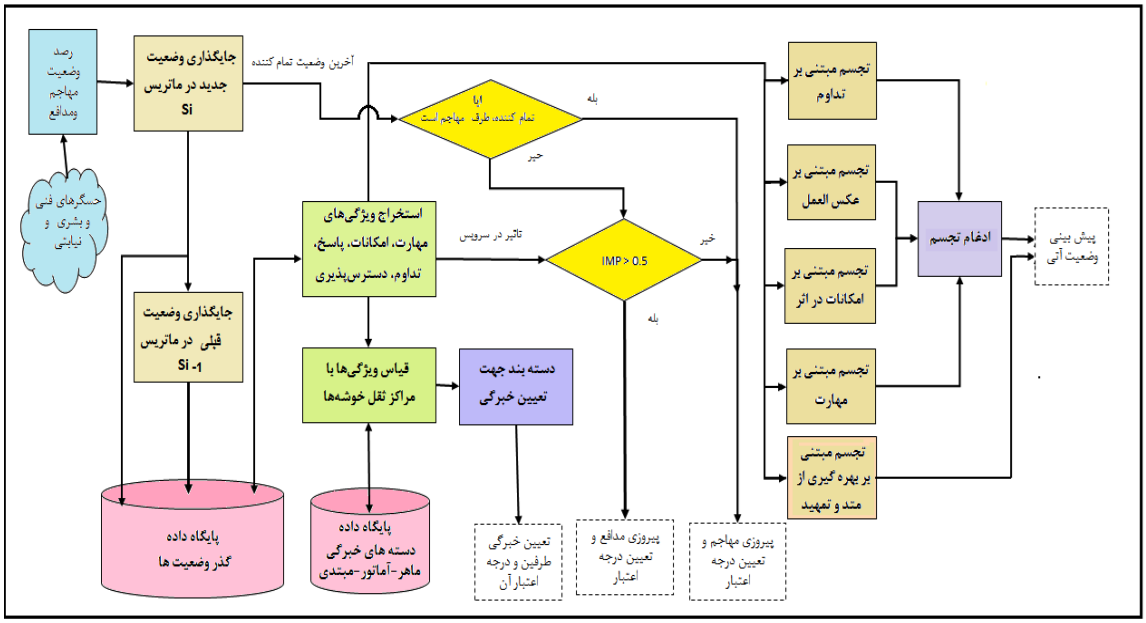


شکل (۵): مدل آگاهی وضعیتی صحنه نبرد در وضعیت مهاجم مبتنی بر فرایند مارکوف

همان‌گونه که در شکل (۵) ملاحظه می‌گردد این فرایند ویژگی مربوط به قابلیت مهاجم را موردمحاسبه قرار می‌دهد و شماره‌های نشانه‌گذاری شده مربوط به افزایش، کاهش و روش‌های به‌کار گرفته شده است. در فصل بعدی برای آزمایش‌ها، در شبیه‌سازی از همین مدل‌ها بهره گرفته خواهد شد.

۶- مدل‌سازی طرح تجسم صحنه نبرد

در این بخش در نظر است طرح تجسم صحنه نبرد (از آینده نزدیک) با استفاده از قابلیت‌های خبرگی، تخمین‌زده و آخرین مرحله آگاهی وضعیتی تکمیل شود که مدل نهایی در قالب شکل (۶) نشان داده شده است. در گام اول وضعیت‌های مدافع توسط حسگرهای فنی و بشری [۳ و ۱۷] و وضعیت‌های مهاجم توسط حسگرهای نیابتی [۱۸] در واحد زمان احصا می‌گردد. در گام دوم وضعیت‌های فوق در قالب ماتریس ترکیب وضعیت تشکیل می‌شود و باگذشت زمان وضعیت‌ها در ماتریس به حرکت درآمده و شرایط محاسبه معیارهای چهارگانه طرفین مهیا می‌شود. در گام سوم ویژگی‌های خبرگی طرفین با تغییر وضعیت‌ها در گره و یال‌ها استخراج می‌شود و در گام چهارم فرد پیروز و درجه پیروزی نتیجه می‌شود. در گام پنجم تجسم‌های قابلیت چهارگانه مورد سنجش (پیش‌بینی) قرار می‌گیرد و سپس با استفاده از نظریه شواهد دمپستر- شافر، تخمین‌های فوق ادغام‌شده و پیش‌بینی وضعیت اثر حمله بر قربانی حاصل شود و در گام ششم دو وضعیت روش مهاجم، تمهید امنیتی مدافع پیش‌بینی می‌شود.



شکل (۶): مدل تجسم (پیش‌بینی) صحنه نبرد منع خدمات مبتنی‌بر قابلیت‌های مهاجم و مدافع.

لذا هریک از تجسم‌ها بر اساس معیار و تخمین کلاس به شرح ذیل تبیین می‌گردد:

الف- تجسم قابلیت امکانات بر، اثر

این معیار درصدد است تعیین کند که امکانات مهاجم و مدافع چقدر توانسته است در ثبات یا عدم ثبات خدمات قربانی اثرگذار باشد. ازاین‌رو، می‌توان برای کلاس اول، تأثیر امکانات مدافع (تمهیدات امنیتی) را بر میزان ثبات موجود محاسبه نمود و نیز کلاس دوم را تأثیر امکانات مهاجم (روش‌ها و تعداد بات‌ها) را بر میزان بی‌ثباتی موجود در نظر گرفت.

$$\text{proj}_{IT^1}(\text{Imp}_G) = \frac{\text{Imp}_A}{\text{TD}_{total}} \quad (۱)$$

$$\text{proj}_{IT}(\text{Imp}_B) = \frac{\text{Imp}_B}{\text{TA}_{Total}} \quad (۲)$$

ب- تجسم قابلیت مهارت بر، اثر

این معیار درصدد است تعیین کند که مهارت مهاجم و مدافع چقدر توانسته است در ثبات یا عدم ثبات خدمات قربانی اثرگذار باشد. ازاین‌رو، می‌توان برای کلاس اول، تأثیر مهارت مدافع را بر میزان ثبات موجود محاسبه نمود و نیز کلاس دوم را تأثیر مهارت مهاجم را بر میزان بی‌ثباتی موجود در نظر گرفت.

$$\text{proj}_{IP^2}(\text{Imp}_G) = \text{Imp}_G * \text{PD}_{total} \quad (۳)$$

$$\text{proj}_{IP}(\text{Imp}_B) = \text{Imp}_B * \text{PA}_{total} \quad (۴)$$

ج- تجسم قابلیت تداوم بر، اثر

این معیار درصدد است تعیین کند که تداوم مهاجم و مدافع چقدر توانسته است در ثبات یا عدم ثبات خدمات قربانی اثرگذار شود. ازاین‌رو، می‌توان برای کلاس اول تأثیر تداوم مدافع را بر میزان ثبات موجود محاسبه نمود و نیز کلاس دوم را تأثیر تداوم مهاجم را بر میزان بی‌ثباتی موجود در نظر گرفت.

$$\text{proj}_{IC^3}(\text{Imp}_G) = \text{Imp}_G * \text{CD}_{total} \quad (۵)$$

$$proj_{IC}(\text{Imp}_B) = \text{Imp}_B * \text{CA}_{total} \quad (۶)$$

د- تجسم قابلیت عکس‌العمل بر، اثر

این معیار درصدد است تعیین کند که عکس‌العمل مهاجم و مدافع چقدر توانسته است در ثبات یا عدم ثبات خدمات قربانی اثرگذار شود. ازاین‌رو می‌توان برای کلاس اول تأثیر عکس‌العمل مدافع را بر میزان ثبات موجود محاسبه نمود و نیز کلاس دوم را تأثیر عکس‌العمل مهاجم را بر میزان بی‌ثباتی موجود در نظر گرفت.

$$\text{proj}_{IR^4}(\text{Imp}_G) = \frac{\text{Imp}_G}{\text{RSD}_{Total}} \quad (۷)$$

$$\text{proj}_{IR}(\text{Imp}_B) = \frac{\text{Imp}_B}{\text{RSA}_{Total}} \quad (۸)$$

در این مرحله با کمک نظریه دمپستر- شافر تجسم‌های فوق مطابق روابط (۸-۱) را تلفیق نموده و تخمینی از پیش‌بینی صحنه نبرد را به‌دست می‌آوریم که مراحل آن را می‌توان در جدول‌های (۳) و (۴) ملاحظه نمود.

جدول (۳): تطبیق تجسم‌های اثر در رتبه‌بندی دو وضعیت بهبود و فشار بر خدمات آتی با چهار شاهد.

Class	proj_{IT}	proj_{IP}	proj_{IC}	proj_{IR}
کلاس بهبود (A)	$\frac{\text{Imp}_G}{\text{TD}_{total}}$	$\text{Imp}_G * \text{PD}_{total}$	$\text{Imp}_G * \text{CD}_{total}$	$\frac{\text{Imp}_G}{\text{RSD}_{Total}}$
کلاس فشار (B)	$\frac{\text{Imp}_B}{\text{TA}_{Total}}$	$\text{Imp}_B * \text{PA}_{total}$	$\text{Imp}_B * \text{CA}_{total}$	$\frac{\text{Imp}_B}{\text{RSA}_{Total}}$

جدول (۴): مرحله ادغام تجسم‌های اثر با استفاده از نظریه دمپستر- شافر

کلاس بهبود (A)

$$\text{m(A)} = \frac{1}{1-\text{K}} * [\sum_{\cap S_i = A} \mathbf{M}_{proj_{IT}}(S_i) * \mathbf{M}_{proj_{IP}}(S_i) * \mathbf{M}_{proj_{IC}}(S_i) * \mathbf{M}_{proj_{IR}}(S_i) + \theta_i * m_i(A)] \quad (۹)$$

کلاس فشار (B)

$$\text{m(B)} = \frac{1}{1-\text{K}} * [\sum_{\cap S_i = B} \mathbf{M}_{proj_{IT}}(S_i) * \mathbf{M}_{proj_{IP}}(S_i) * \mathbf{M}_{proj_{IC}}(S_i) * \mathbf{M}_{proj_{IR}}(S_i) + \theta_i * m_i(B)] \quad (۱۰)$$

ه- تجسم قابلیت روش و تمهید

در این مرحله مدنظر است بعد از تعیین (تخمین) تجسم اثر بر خدمات مدافع، تجسم قابلیت به‌کارگیری روش توسط مهاجم و تمهید امنیتی توسط مدافع تخمین زده شود. لذا استفاده از قوانین بیزین می‌تواند در این مرحله کارساز باشد که رابطه‌های (۱۱) و (۱۲) آورده شده است. در رابطه (۱۱) احتمال به‌کارگیری روش جدید و رابطه (۱۲- الف) احتمال به‌کارگیری با روش قبلی توسط مهاجم قابل تخمین زدن است (جهت سادگی محاسبه از رابطه (۱۲- ب) استفاده می‌شود).

$$\begin{aligned}\text{P(MethA}_{total}) &= \text{P(MethA}_{total} | \text{IncBot}_{total}) * \text{P(IncBot}_{total}) \\ &+ \text{P(MethA}_{total} | \text{DecBot}_{total}) * \text{P(DecBot}_{total}) \\ &+ \text{P(MethA}_{total} | \text{UCBot}_{total}) * \text{P(UCBot}_{total}) \\ &+ \text{P(MethA}_{total} | \text{StopBot}_{total}) * \text{P(StopBot}_{total})\end{aligned} \quad (۱۱)$$

$$\begin{aligned}\text{P(Met}_{old}^5) &= \text{P(Met}_{old} | \text{IncBot}_{total}) * \text{P(IncBot}_{total}) \\ &+ \text{P(Met}_{old} | \text{DecBot}_{total}) * \text{P(DecBot}_{total}) \\ &+ \text{P(Met}_{old} | \text{UCBot}_{total}) * \text{P(UCBot}_{total}) \\ &+ \text{P(Met}_{old} | \text{StopBot}_{total}) * \text{P(StopBot}_{total})\end{aligned} \quad (۱۲\text{- الف})$$

1- Impact of Tools
2- Impact of Professional
3- Impact of Continue
4- Impact of Response
5- Previous Method

$$P(Met_{old}) = 1 - P(Met_{new}) \quad (۱۲\text{-ب})$$

همچنین قوانین فوق را می‌توان برای تخمین به‌کارگیری تمهید امنیتی جدید یا عدم به‌کارگیری آن مورداستفاده قرارداد که مطابق رابطه‌های (۱۳) و (۱۴) است.

$$P(SecM_{New}) = \quad (۱۳)$$
$$P(SecM_{New} \mid IMP_B) * P(IMP_B) + P(SecM_{New} \mid IMP_A) * P(IMP_A)$$

$$P(SecM_{Pre}) = \quad (۱۴\text{-الف})$$
$$P(SecM_{Pre} \mid IMP_B) * P(IMP_B) + P(SecM_{Pre} \mid IMP_A) * P(IMP_A)$$

$$P(SecM_{Pre}) = 1 - P(SecM_{New}) \quad (۱۴\text{-ب})$$

جهت سادگی محاسبه به‌جای رابطه (۱۴-الف)، از رابطه (۱۴-ب) استفاده می‌شود. همان‌گونه که پیشتر در جدول (۱) بخش ۴-۲، بیان شد، $SecM_{New}$ اشاره به تمهیدات امنیتی جدید و همچنین $SecM_{Pre}$ اشاره به تمهیدات امنیتی قبلی دارد. در بخش شبیه‌سازی از روابط فوق جهت مدل‌سازی تجسم وضعیت بهره‌مند خواهیم شد.

۶-۱- صحت سنجی[1] مدل

در این مرحله در نظر داریم صحت مدل را مورد تجزیه‌وتحلیل قرار دهیم و از طرفی با فقدان مجموعه داده‌های واقعی مواجه هستیم و در بسیاری از کارهای مرتبط، برای درست یابی مدل‌ها از شبیه‌سازی بهره می‌گیرند که ما هم برای ارزیابی مدل خود از همین روش استفاده می‌کنیم. برنامه شبیه‌سازی با استفاده از متلب و مبتنی بر رویداد گسسته[2] پیاده‌سازی کرده‌ایم. لذا فرایند ارزیابی تجسم، مورد شبیه‌سازی قرار می‌گیرد و مجموعه داده موردنیاز را با استفاده یک تولیدکننده دنباله (که بر اساس قواعد صحنه نبرد و مطابق پیوست الف) تهیه می‌کنیم. ما سپس نتایج شبیه‌سازی را با استدلال‌های منطقی که حاکم بر صحنه نبرد است مورد مقایسه قرار می‌دهیم. لذا در مرحله اول با استفاده از تولیدکننده دنباله به‌صورت تصادفی از ۳۰۰۰ دنباله متفاوت بهره‌مند می‌شویم.

۶-۲- معیار ارزیابی

در این پژوهش، یکی از معیارهای ارزیابی ما بهره‌مندی از ضریب همبستگی پیرسون است. ضریب همبستگی که از ۱- تا ۱+ متغیر است که بیان‌گر ارتباط دو عامل با یکدیگر است. اگر مقدار آن به ۱+ نزدیک باشد بیانگر این است که این دو عامل، ارتباط مستقیم و کاملی با یکدیگر دارند و اگر مقدار آن به ۱- نزدیک باشد بیانگر این است که این دو عامل، ارتباط معکوس و کاملی با یکدیگر دارند. اگر مقدار آن صفر باشد بیانگر نداشتن ارتباط بین دو عامل است. در این پژوهش از ضریب همبستگی پیرسون جهت ارزیابی ارتباط معیارهای احصا شده با یکدیگر استفاده می‌گردد.

$$r = \frac{cov(X,Y)}{\sigma X \sigma Y}$$

مقایسه و همگرایی نتایج تحلیل‌های واقعی با تحلیل‌های شبیه‌سازی‌شده مدل پیشنهادی و نیز انتظارات منطقی که مورد تأیید خبرگان این حوزه است، به‌عنوان معیار ارزیابی مورد استفاده قرار می‌گیرد.

۷- شبیه‌سازی و ارزیابی

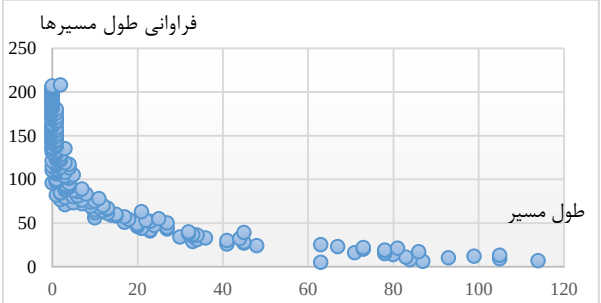
در این بخش مدنظر است مدل پیشنهادی مورد شبیه‌سازی و پیاده‌سازی قرار گیرد، لذا با استفاده از یک مجموعه داده ۳۰۰۳ تایی که حاوی دنباله وضعیت‌های ترکیبی مطابق با جدول (۱)، است، معیارهای ارزیابی درصحنه نبرد برای هر یک از طرفین محاسبه گردد. با استفاده از شبیه‌ساز متلب، کلیه روابط مربوط به معیارها مورد پیاده‌سازی قرارگرفته و با اعمال مجموعه داده فوق، معیارهای ارزیابی برای کلیه دنباله‌های صحنه نبرد موردمحاسبه قرار گرفت. لذا لازم است در ابتدا قدری راجع دنباله‌ها مختصری توضیح دهیم.

اگر در هر مقطع زمانی، وضعیت مهاجم و مدافع را یکی از ۵۶ وضعیت ترکیبی ماتریس (بدون سطر و ستون توقف)، در نظر بگیریم و این کار به‌طور مدام ادامه پیدا کند تا این‌که به یکی از وضعیت‌های واقع در سطر و ستون توقف برسد، یک دنباله مرتب را تشکیل می‌دهد که آن را به فرم $X=< X1, X2, \ldots, Xn >$ در نظر می‌گیریم، که در آن متغیر تصادفی $Xk \in State$ ، نشان‌دهنده $K = \{1,2, \ldots, N\}$ اُمین وضعیت در دنباله است. ازلحاظ نظری X به‌صورت یک بردار با مجموعه‌ای از خصوصیات تعریف می‌شود و N را طول مسیر پیمایش دنباله در نظر می‌گیریم. ما در بخش شبیه‌سازی، با توجه به مفروضات پایگاه داده گذر یال‌ها و مفروضات بخش‌های (۴-۱) و (۴-۲) مبادرت به تولید دنباله می‌کنیم.

۷-۱- دستاوردهای حاصل از روابط آماری معیارها

نتایج حاصل از شبیه‌سازی در ابعاد گوناگون به نقل از محاسبات آماری، ظهور و بروز پیدا کرد که مطابق اشکال و جداول این بخش ارائه می‌گردد. شکل (۷) نمودار فراوانی طول مسیرهای مجموعه داده‌ها را نشان می‌دهد. همان‌طور که ملاحظه می‌شود ۴۶٪ از داده‌ها دارای طول دنباله کمتر از ۲۰ گام می‌باشند.

1- Validation
2- Discrete-Event Simulation

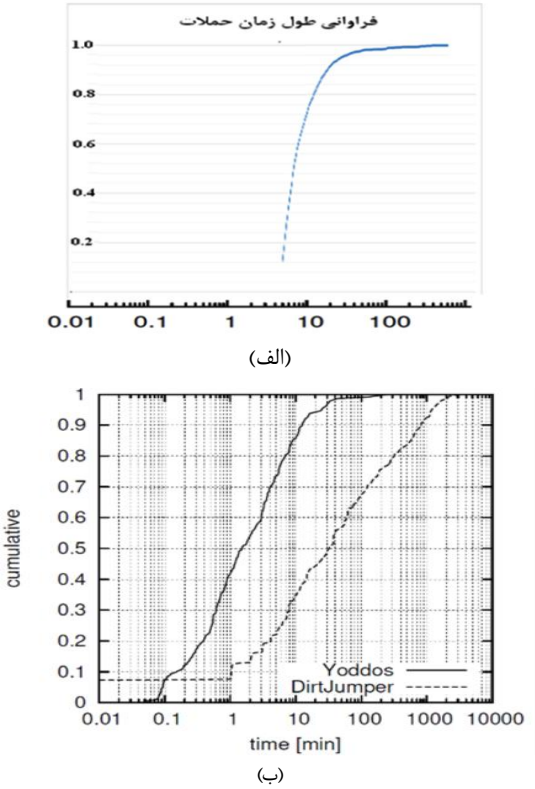


شکل (۷): نمودار فراوانی طول مسیرهای در مجموعه داده ۳۰۰۳.

اگر طول مسیر حمله را در بعد زمان در نظر بگیریم، می‌توان گفت نیمی از حملات در مدت‌زمان کوتاهی به اتمام رسیده‌اند و این بدان معناست که مهاجم یا مدافع توانسته‌اند بااقتدار بر مدافع فائق یابند و یا حریف دفاع او نشوند و یا این‌که با اصل غافلگیری [۱۷] قربانی را شکست دهد. بسیار جالب است که نتایج فوق با نتایج واقعی هم‌خوانی دارد، به‌طوری‌که در [۱۸] با تحلیل ترافیک هفت‌ماهه دو خانواده شبکه بات Yoddos و Dirtjumper نشان داد که نیمی از حملات Dirtjumper در کمتر از ۳۰ دقیقه به طول انجامیده است. لذا نمودارهای فراوانی طول مدت‌زمان حملات در شکل‌های (۸- الف و ب) به ترتیب برای مجموعه داده ۳۰۰۳ تایی و حملات واقعی نشان داده‌شده است.

همچنین میزان همبستگی معیارهای تداوم و زمان پاسخ به تجهیزات و مهارت مدافع و مهاجم اندازه‌گیری گردید که در جدول (۵) نشان داده‌شده است. مطابق جدول فوق تداوم دفاع و زمان پاسخ با میزان تجهیزات (و امکانات) مدافع، به ترتیب با ۰/۹۳ و ۰/۵- همبستگی، رابطه خوبی دارد. همچنین همبستگی فوق بامهارت مدافع، به ترتیب با ۰/۵ و ۰/۷- رابطه نسبتاً خوبی دارد. این بدان معناست که روابط تبیین شده معیارها در مجموعه داده ۳۰۰۳ تایی صدق می‌کند.

ولیکن معیارهای تداوم و زمان پاسخ هجوم با میزان تجهیزات مهاجم به ترتیب با ۰/۳ و ۰/۱۷ همبستگی، رابطه نه‌چندان خوبی را نشان می‌دهد، بخصوص اینکه زمان پاسخ مثبت ۰/۱۷ بیان‌گر این است که لزوماً امکانات و تجهیزات در سرعت عمل مهاجم تأثیر مثبتی ندارد و بلکه قدری هم تأثیر منفی دارد و این بدان معناست که مهارت مهاجم نسبت تجهیزات او اثرگذارتر است. نظر به این‌که انتظار می‌رود نتیجه میزان آمادگی رزم (خبرگی) در معیار دسترس‌پذیری تأثیرگذار باشد، ازاین‌رو، میزان همبستگی کلیه معیارهای آمادگی رزم (خبرگی) طرفین صحنه نبرد با معیار دسترس‌پذیری مورد سنجش قرار گرفت که نتایج در جدول (۶) نشان داده شده است.



(الف)

(ب)

شکل (۸): الف- نمودار فراوانی طول حملات در مجموعه داده ۳۰۰۳ تایی، ب- نمودار فراوانی طول حملات شبکه بات [۱۹].

جدول (۵): همبستگی معیارهای تداوم و زمان پاسخ به تجهیزات و مهارت.

	مدافع		مهاجم	
	مهارت	تجهیزات	مهارت	تجهیزات
تداوم	+۰/۵	+۰/۹۳	+۰/۳۲	+۰/۳
زمان پاسخ	-۰/۷	-۰/۵	-۰/۳۷	+۰/۱۷

جدول (۶): همبستگی معیارها با دسترس‌پذیری

Correlation	RSD	PD	CD	TD
Ava	-۰/۳۳	۰/۵۵	۰/۹۴	۰/۲۰
Correlation	RSA	PA	CA	TA
Ava	۰/۰۸	-۰/۴	-۰/۹۲	-۰/۱۵

همان‌گونه که ملاحظه می‌شود، ضریب همبستگی قابلیت دسترس‌پذیری و تداوم حمله (۹۲٪-) بیانگر یک رابطه معکوس و کاملی است. یعنی با افزایش تداوم حمله، قابلیت دسترس‌پذیری کاهش می‌یابد. همچنین ضریب همبستگی قابلیت دسترس‌پذیری و تداوم دفاع (۹۴٪) بیانگر وجود رابطه مستقیم و کاملی است. یعنی با افزایش تداوم دفاع، قابلیت دسترس‌پذیری نیز افزایش می‌یابد. همچنین ضریب همبستگی قابلیت دسترس‌پذیری و ابزار و امکانات مدافع (۰/۰۲) و مهاجم (۰/۱۵-) بیانگر عدم رابطه بین این معیارها است و به نظر می‌رسد تأثیر

متقابل ابزارهای طرفین بر یکدیگر موجب این عدم رابطه باشد. در مورد معیار مهارت نیز مشاهده می‌شود که رابطه مستقیم و ناکاملی بین قابلیت دسترس‌پذیری و مهارت مدافع و نیز رابطه معکوس و ناکاملی بین قابلیت دسترس‌پذیری و مهارت مهاجم وجود دارد.

۷-۲- تخمین وضعیت در پنج سناریو

در این مرحله در نظر داریم شبیه‌سازی تخمین وضعیت بر اساس تجسم اثر هر یک از عوامل قابلیت (خبرگی) را انجام داده و سپس با استفاده از روابط دمپستر- شافر توسعه‌یافته، مرحله ادغام آن‌ها به انجام رسانیم. لذا لازم است در ابتدا ضریب اهمیت هریک از شواهد (تجسم اثر قابلیت) را تعیین نماییم. ازاین‌رو با استفاده از مجموعه داده ۳۰۰۳ تایی، تأثیر عوامل فوق را بر کاهش خدمت‌رسانی قربانی اندازه‌گیری کرده و سپس با استفاده از روش تحلیل سلسله مراتبی مبادرت به تعیین ضریب اهمیت هر یک از عوامل قابلیت می‌کنیم که نتایج حاصل از آن را می‌توان در جدول (۷) ملاحظه نمود.

جدول (۷): تعیین ضرایب شواهد بر اساس فراوانی‌های مجموعه داده ۳۰۰۳ با استفاده از روش AHP

	میانگین طرفین
تداوم	۰/۱۸
پاسخ زمانی	۰/۳۰
مهارت	۰/۲۱
امکانات	۰/۹۴

	ضرایب شواهد	تداوم	پاسخ زمانی	مهارت	امکانات	A.H.P
تداوم	۰/۶۱	۵/۲	۱/۱۷	۰/۱۷	۱/۰۰	امکانات
پاسخ زمانی	۰/۶۶	۳/۱۳	۰/۷	۱/۰۰	۰/۶	مهارت
مهارت	۰/۶۱	۴/۴۸	۱/۰۰	۰/۲۰	۰/۸۶	پاسخ زمانی
امکانات	۰/۷۲	۱/۰۰	۴/۶۰	۰/۹۱	۰/۱۹	تداوم

در سمت راست این جدول میانگین ضریب همبستگی هر یک از معیارها در مجموعه داده محاسبه‌شده است. در سمت چپ، جدول AHP قرار دارد که در سطرها و ستون‌های آن معیارهای چهارگانه قرارگرفته است. مقادیر این جدول، از محاسبه نسبت دو به دوی میانگین فراوانی هر یک از معیارها حاصل‌شده است. در ادامه با استفاده از میانگین هندسی (فرجه ۴)، مقدار ضرایب را به دست می‌آوریم و همین ضرایب را می‌توان در روابط دمپستر-شافر به‌عنوان ضریب اهمیت شواهد بکار برد. حال با استفاده از مجموعه داده ۳۰۰۳ تعدادی دنباله حمله را مطابق جدول (۸) انتخاب کرده و به‌عنوان سناریو، مورد راستی آزمایی قرار داده‌ایم که نتایج تخمین تجسم وضعیت مطابق جدول (۹) حاصل شده است.

جدول (۸): سناریوهای مورد آزمایش

مراحل	سناریو یک	سناریو دو	سناریو سه	سناریو چهار	سناریو پنج
	۵۹۲	۴۳۲	۲۵۲۵	۶۷۱	۱۶۳۶
۱	۱	۱	۱	۱	۱
۲	۱۱	۱۱	۱۱	۱۱	۳۰
۳	۲۶	۱۲	۳	۳۲	۴۲
۴	۱۱	۱۳	۱۳	۸	۳۸
۵	۸	۱۳	۲	۳۲	۴۳
۶	۲۲	۳۵	۷	۳۲	۳۳
۷	۱۳	۱۴	۱۲	۲	۲۵
۸	۲۱	۲۶	۱۷	۱۶	۷
۹	۱۱	۲۹	۲	۱۲	۲۹
۱۰	۷	۴۲	۳۲	۳۰	۳
۱۱	۱۵	۲۹	۵	۳۵	۱۳
۱۲	۶	۱۲	۲۳	۳۰	۲۰
۱۳	۲۵	۲۲	۸	۱۲	۲۹
۱۴	۲	۱۳	۳۱	۱۴	۷
۱۵	۲۳	۳۱	۴۸	۱۷	۱۱
۱۶	۳۱	۲۶	۴۸	۱۶	۲۴
۱۷	۲۱	۵۳	۴۳	۱۷	۳۴
۱۸	۲۶	۵۶	۲۹	۲۶	۱۶
۱۹	۳۶	۵۷	۲۰	۴۵	۱۷
۲۰		۶۵	۲	۰	۱۱
۲۱			۱۵		۱۴
۲۲			۱۲		۵
۲۳			۲۱		۵
۲۴			۳۴		۳۱
۲۵			۱۲		۳۵
۲۶			۲		۳۸
۲۷			۲۱		۲۱
۲۸			۱۲		۱۱
۲۹			۶		۸
۳۰			۱۱		۱۵
۳۱			۲۴		۱۱
۳۲			۱۵		۱۶
۳۳			۳۵		۲۴
۳۴			۱۳		۳۸
۳۵			۲۹		۴۴
۳۶			۵		۴۲
۳۷			۲		۲۵
۳۸			۲۴		۸
۳۹			۵۳		۹
۴۰			۵۱		
۴۱			۲۶		
۴۲			۵۳		
۴۳			۲۰		
۴۴			۲۲		
۴۵			۴۱		
۴۶			۵۶		
۴۷			۵۸		
۴۸			۵۶		
۴۹			۶۹		

جدول (۹): نتایج تخمین تجسم وضعیت در تعیین اثر بعدی

نتایج		سناریو ۱		سناریو ۲		سناریو ۳		سناریو ۴		سناریو ۵	
اهمیت	شواهد	A	B	A	B	A	B	A	B	A	B
۰/۱۲	I.C	۰/۶۱	۰/۳۹	۰/۳۳	۰/۶۷	۰/۴۶	۰/۵۴	۰/۵۶	۰/۴۴	۰/۳۵	۰/۶۵
۱/۰۰	I.R	۰/۵۴	۰/۴۶	۰/۲۶	۰/۷۴	۰/۴۷	۰/۵۳	۰/۴۳	۰/۵۷	۰/۳۴	۰/۶۶
۰/۷	I.P	۰/۵۶	۰/۴۴	۰/۳۸	۰/۶۳	۰/۵	۰/۵	۰/۴۷	۰/۵۳	۰/۴۰	۰/۶۰
۰/۶۶	I.T	۰/۴۸	۰/۵۲	۰/۲۴	۰/۷۶	۰/۴۱	۰/۵۹	۰/۴۶	۰/۵۴	۰/۳۷	۰/۶۳
باور		۰/۵۷	۰/۴۰	۰/۱۵	۰/۸۴	۰/۴۰	۰/۵۷	۰/۴۷	۰/۵۷	۰/۲۴	۰/۷۳
مقبولیت		۰/۶۰	۰/۴۳	۰/۱۸	۰/۸۷	۰/۴۳	۰/۶۰	۰/۴۷	۰/۵۷	۰/۲۷	۰/۷۷

در بخش انتهایی هر یک از سناریوهای جدول (۹)، میزان تخمین برای هر یک از کلاس‌های A, B با مقادیر میزان باور و مقبولیت محاسبه و درج شده است. در سناریو اول تخمین ۰/۵۶۷ بیانگر این مطلب است که گام بعدی با حداکثر احتمال مقبولیت ۰/۶۰۳به وضعیت بهبود A سیر خواهد کرد و به همین ترتیب در سناریوهای دوم و سوم ۰/۸۶۷ و ۰/۶۰۴ به وضعیت تحت‌فشار B خواهد رفت. در جدول (۱۰) نتایج تخمین تجسم وضعیت در تعیین به‌کارگیری امکانات روش مهاجم و تمهید امنیتی مدافع در دو دسته جدید و قبلی نشان داده شده است.

جدول (۱۰): نتایج تخمین تجسم وضعیت در تعیین به‌کارگیری امکانات روش مهاجم و تمهید امنیتی مدافع

نتایج احتمالاتی	سناریو ۱		سناریو ۲		سناریو ۳		سناریو ۴		سناریو ۵	
	جدید	قبلی	جدید	قبلی	جدید	قبلی	جدید	قبلی	جدید	قبلی
متد	۰/۳۸	۰/۶۳	۰/۳۶	۰/۶۴	۰/۳۹	۰/۶۱	۰/۶۷	۰/۳۳	۰/۳۹	۰/۶۱
تمهید	۰/۵۴	۰/۵	۰/۷۹	۰/۲۱	۰/۵	۰/۵	۰/۸۷	۰/۱۳	۰/۴۷	۰/۵۳

۷-۳- تخمین وضعیت در ۲۰ سناریو متوالی

در این مرحله تخمین وضعیت در پنج سناریو با چهار گام متوالی مورد محاسبه قرارگرفته است که دقت نتایج آن مطابق جدول (۱۱) نشان داده شده است. ستون‌ها از راست به چپ به ترتیب شماره سناریو، چهار وضعیت متوالی از هر سناریو[1]، گام‌های سناریو[2]، صحت (T) یا عدم صحت (F) تخمین در تعیین نوع گروه اثر A یا B، تعیین نوع روش و نوع تمهید مطابق وضعیت از پیش تعیین شده است.

ستون دقت، بیانگر درصد صحت و یا عدم صحت سه ستون قبلی است. ستون‌های بعدی نیز مقادیر تخمین را برای نوع گروه اثر A، تعیین نوع روش و نوع تمهید می‌دهند.

در ستون و سطر دقت میزان دقت تخمین در هر مرحله و در هر گام از سناریوها موردمحاسبه قرارگرفته است که از ۰/۴ تا ۰/۸۵ را نشان می‌دهد که میانگین آن برابر دقت ۰/۶۵ است.

۸- نتیجه‌گیری

صحنه نبرد سایبری در حملات منع خدمت‌رسانی توزیع‌شده دارای دو بازیگر مهاجم و مدافع (قربانی) است که مهاجم با گسیل بسته‌های پی‌درپی و تغییر روش‌های خود درصدد قطع یا کاهش خدمت‌رسانی قربانی است و قربانی با انجام انواع تمهیدات امنیتی درصدد دفاع بوده و اصرار بر خدمت‌رسانی به ذینفعان خود دارد. ارزیابی این صحنه از منظر یک ناظر می‌تواند دارای ابهام باشد.

جدول (۱۱): نتایج دقت تخمین تجسم با پنج سناریوی در چهار گام متوالی

سناریوها	Seq.v	Seq.n	گروه	روش	تمهید	دقت	A.G	N.Met	N.Sec
سناریو۱	۲۳<[۲]	T1	T	F	T	۰/۶۶	۵۷	۳۸	۵۰
	۳۱	T2	T	T	F	۰/۶۶	۶۵	۳۳	۴۷
	۲۱	T3	T	F	T	۰/۶۶	۷۴	۲۹	۴۳
	۲۶	T4	T	T	T	۱	۶۹	۲۳	۳۸
سناریو۲	۲۲<[۱۲]	T1	F	T	F	۰/۳۳	۱۵	۳۶	۷۹
	۱۳	T2	F	T	T	۰/۶۶	۲۰	۳۱	۷۷
	۳۱	T3	F	T	T	۰/۶۶	۱۳	۲۵	۷۵
	۲۶	T4	F	T	F	۰/۳۳	۱۶	۲۷	۸۲
سناریو۳	۲۰<[۵۳]	T1	F	F	T	۰/۳۳	۴۰	۳۹	۵۰
	۲۲	T2	F	F	T	۰/۳۳	۴۲	۳۷	۵۱
	۴۱	T3	T	T	T	۱	۴۴	۳۸	۵۲
	۵۶	T4	T	F	T	۰/۶۶	۴۶	۳۹	۵۴
سناریو۴	۱۴<[۱۲]	T1	F	T	T	۰/۶۶	۴۴	۶۷	۸۷
	۱۷	T2	F	T	T	۰/۶۶	۴۲	۶۵	۸۴
	۱۶	T3	F	T	T	۰/۶۶	۴۰	۶۳	۸۰
	۱۷	T4	F	T	T	۰/۶۶	۴۲	۶۰	۸۳
سناریو۵	۴۴<[۳۸]	T1	T	T	T	۱	۲۴	۴۰	۴۷
	۴۲	T2	T	T	T	۱	۲۲	۴۲	۴۵
	۲۵	T3	F	F	T	۰/۳۳	۲۴	۴۴	۴۳
	۸	T4	F	T	T	۰/۶۶	۲۰	۴۲	۴۵
دقت			۰/۴	۰/۷	۰/۸۵	۰/۶۵	۲۲	۴۰	۴۳

در این پژوهش انواع وضعیت‌های مهاجم و مدافع و تجسم قابلیت تبیین گردید و در ادامه با استفاده از یک مجموعه داده ۳۰۰۳ تایی که حاوی دنباله وضعیت‌های یک مهاجم و مدافع بود مبادرت به اندازه‌گیری معیارهای قابلیت گردید که نتایج معناداری را به همراه داشت. در این تحقیق نشان داده شده که نیمی از داده‌ها دارای طول زمانی کمی هستند که این بدان معناست که مهاجم یا مدافع توانسته‌اند بااقتدار برطرف مقابل فائق آیند و یا این‌که مهاجم با بهره‌مندی از اصل غافل‌گیری، مدافع را شکست داده است و یا این‌که قربانی‌ها برای دفاع در برابر حمله هیچ‌گونه آمادگی نداشته‌اند. همچنین نشان داده شد، افزایش یا کاهش طول زمان نبرد ارتباط معناداری با میزان قابلیت (خبرگی) طرفین دارد و نیز همبستگی معیارها نسبت به یکدیگر نشان داده شد که هر چه زمان حمله طولانی باشد خسارت مدافع بیشتر می‌گردد و محاسبات به نفع مهاجم رقم می‌خورد و نیز امکانات و تجهیزات در سرعت عمل مهاجم تأثیر مثبتی ندارد و بلکه قدری هم تأثیر منفی دارد و این بدان معناست که مهارت مهاجم در مقایسه با تجهیزات او اثرگذارتر است. در ادامه به‌منظور تجسم صحنه نبرد در پیش‌بینی وضعیت طرفین، از اثر چهار معیار قابلیت (خبرگی) بر وضعیت قربانی بهره

1- Seq.v
2- Seq.n

گرفته شد و درنهایت با استفاده از نظریه شواهد دمپستر- شافر و قانون بیزین عملیات تلفیق صورت گرفت و با اجرای پنج سناریو در چهار گام زمانی، نشان داده شد که تخمین‌های حاصل‌شده با بیش از ۶۵٪ قابل‌باور است. بنابراین، نوآوری طرح شامل موارد ذیل است:

- مدل ارائه‌شده، برآورد مناسبی از آگاهی وضعیت صحنه نبرد حمله منع خدمات در شرایط عدم قطعیت را حاصل می‌کند.
- معیارهای قابلیت (خبرگی)، فرد پیروز و درجه موفقیت مبتنی بر قابلیت طرفین در حملات منع خدمات توزیع‌شده، تبیین گردید که قابل‌اندازه‌گیری است.
- امکان پیش‌بینی وضعیت‌های آتی مبتنی بر قابلیت طرفین میسر است و می‌توان قابلیت اطمینان تخمین وضعیت را با دقت بیش از ۶۵٪ حاصل کرد.

برای ادامه کار و تحقیقات بعدی پیشنهاد می‌گردد با به‌کارگیری قابلیت‌های دیگر و با استفاده از روش‌های مارکوف، نظریه بازی‌ها و شبکه‌های عصبی موجب کاهش ابهامات شد و دقت و قابلیت اطمینان تخمین وضعیت را بهبود بخشید.

۹- منابع

[1] M. H. Hamza Kalai and M. R. M. J. shaman, “IP optimization ant colony algorithm for tracking denial of service attacks,” Journal of electronic and cyber defense, vol. 1, vol. 4, 2014. (In Persian), Ihu.ac.ir

[2] K. Kumar, M. Sachdeva, and K. Arora, “Impact Analysis of Recent DDoS Attacks,” International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397, vol. 3 no. 2, Feb. 2011.

[3] H. Akbari, et al, “A Framework For The Status Estimation In Distributed Denial-of-Service Attacks By Data Fusion of Human-And-Technical Sensors Based on Fuzzy Logic,” Journal of Electronical & Cyber Defence vol. 5, no. 3, 2017, Serial No. 19 (In Persian).

[4] A. J. Rashidi, et al, “A New Framework for Projection of Cyber-Attacks Based on Information Fusion,” Journal of Passive defense Quarterly,Vol. 6, No. 2, 2015, (In Persian).

[5] C. Rossow and H. Bos. Arne Welzel, “On Measuring the Impact of DDoS Botnets,” EuroSec’14, Amsterdam, Netherlands, April 2014.

[6] Z. Peng, W. Zhao, and J. Long, “Grey synthetic clustering method for DoS attack effectiveness evaluation,” International Conference on Modeling Decisions for Artificial Intelligence, pp. 139-149, Springer Berlin Heidelberg, July 2011.

[7] C. Nordlohne, “Measuring Botnet Prevalence: Malice Value,” in University of Applied Sciences Gelsenkirchen, Germany, January 7, 2015.

[8] P. A. A. M. B. B. Gupta, “Estimating Strength of Ddos Attack Using Various Regression Models,” in springer, 2011.

[9] C. Bannwart, “Predicting the Impact of Denial of Service Attacks,” Master Thesis MA-2012-03, 2012.

[10] R. Vasudevan, et al, “MIDAS: An Impact Scale for DDoS attacks,” Proceedings of the 2007 15th IEEE Workshop on Local and Metropolitan Area Networks, 2007.

[11] T. Dubendorfer, A. Wagner, and B. Plattner, “An economic damage model for large-scale Internet attacks,” In 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 223–228, IEEE Comput. Soc., 2004.

[12] http://cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/w/World_Wide_Web.htm

[13] K. Dadashtabar, et al, “Projection of Multi stage cyber Attack Based on Belief Model and fuzzy inference,” journal of Electronical & cyber Defense, vol. 3, no. 2, serial no.10, 2015 (In Persian).

[14] Du, Haitao, “Probabilistic Modeling and Inference for Obfuscated Network Attack Sequences,” Thesis, Rochester Institute of Technology, 2014. Accessed from http://scholarworks.rit.edu/theses.

[15] F. S. Yuan Yuan, “Data Fusion-based Resilient Control System under DoS Attacks: A Game Theoretic Approach,” International Journal of Control Automation and Systems, vol. 13, no. 3, June 2015.

[16] M. R. Endsley, “Final Reflections: Situation Awareness Models and Measures,” Journal of Cognitive Engineering and Decision Making, March 2015.

[17] H. Akbari and S. M. Safavi, “Determine of the victim machine situation by data fusion of cyber sensors at packet level,” Journal of Command and Control, vol. 1, no. 2, pp. 39-64, winter 2017 (In Persian).

[18] H. Akbari and S. M. Safavi, “Estimate botnet using vicarious servers in distributed denial of service attacks,” Journal of Electronical & Cyber Defence pp. 95-109, vol. 5, no. 4, Serial No. 20, 2018 (In Persian).

[19] A. Welzel, C. Rossow, and H. Bos, “On Measuring the Impact of DDoS Botnets,” VU University Amsterdam, 2014. available: http://dx.doi.org/10.1145/2592791.2592794

پیوست

تولیدکننده دنباله مبتنی بر مفروضات مدل

```
// sequence generator
#include <iostream>
#include <string>
int main()
{
 int i=0 ,x=1 , y=1, z=1;
                                        // ارائه حاوی گذر یال‌ها است شامل ۷۲*۴۹
int array[73][49]=  {
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
```

```
{25,40,41,49,50,22,23,31,32,26,35,38,39,47,48,20,21,29,30,44,53,
56,57,58,59,62,,,,,,,,,,,,,,,,,,,,,},
{25,42,43,51,52,24,25,33,34,26,35,44,53,60,61,20,21,29,30,38,39,
47,48,56,57,62,,,,,,,,,,,,,,,,,,,,,},
{25,42,43,51,52,24,25,33,34,26,35,44,53,60,61,20,21,29,30,38,39,
47,48,56,57,62,,,,,,,,,,,,,,,,,,,,,},
{40,44,53,22,23,31,32,26,35,27,36,38,39,47,48,40,41,49,50,20,21,
29,30,45,54,56,57,58,59,62,63,24,25,33,34,42,43,51,52,60,61,,,,,,,
},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{10,20,21,29,30,38,39,47,48,56,57,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{35,38,39,47,48,22,23,31,32,26,35,20,21,29,30,40,41,49,50,44,53,
56,57,58,59,62,24,25,33,34,42,43,51,52,60,61,,,,,,,,,,,,},
{35,38,39,47,48,22,23,31,32,26,35,20,21,29,30,40,41,49,50,44,53,
56,57,58,59,62,24,25,33,34,42,43,51,52,60,61,,,,,,,,,,,,},
{25,40,41,49,50,22,23,31,32,26,35,38,39,47,48,20,21,29,30,44,53,
56,57,58,59,62,,,,,,,,,,,,,,,,,,,,,},
{25,40,41,49,50,22,23,31,32,26,35,38,39,47,48,20,21,29,30,44,53,
56,57,58,59,62,,,,,,,,,,,,,,,,,,,,,},
{25,42,43,51,52,24,25,33,34,26,35,44,53,60,61,20,21,29,30,38,39,
47,48,56,57,62,,,,,,,,,,,,,,,,,,,,,},
{25,42,43,51,52,24,25,33,34,26,35,44,53,60,61,20,21,29,30,38,39,
47,48,56,57,62,,,,,,,,,,,,,,,,,,,,,},
{40,44,53,22,23,31,32,26,35,27,36,38,39,47,48,40,41,49,50,20,21,
29,30,45,54,56,57,58,59,62,63,24,25,33,34,42,43,51,52,60,61,,,,,,,
},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{8,38,39,47,48,56,57,65,66,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{28,56,57,40,41,49,50,44,53,38,39,47,48,58,59,62,65,66,67,68,71,
60,61,69,70,42,43,51,52,,,,,,,,,,,,,,,,,,},
{28,56,57,40,41,49,50,44,53,38,39,47,48,58,59,62,65,66,67,68,71,
60,61,69,70,42,43,51,52,,,,,,,,,,,,,,,,,,},
{20,58,59,40,41,49,50,44,53,56,57,38,39,47,48,62,65,66,67,68,71,
,,,,,,,,,,,,,,,,,,,,,,,,,},
{20,58,59,40,41,49,50,44,53,56,57,38,39,47,48,62,65,66,67,68,71,
,,,,,,,,,,,,,,,,,,,,,,,,,},
{20,60,61,42,43,51,52,44,53,62,69,70,38,39,47,48,56,57,65,66,71,
,,,,,,,,,,,,,,,,,,,,,,,,,},
{20,60,61,42,43,51,52,44,53,62,69,70,38,39,47,48,56,57,65,66,71,
,,,,,,,,,,,,,,,,,,,,,,,,,},
{32,62,40,41,49,50,44,53,45,54,56,57,58,59,38,39,47,48,63,65,66,
67,68,71,72,42,45,51,52,60,61,69,70,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
} ;
 for (i=0 ; i<  ; i++)
  {
  std::cout << x ;
  while (x)
   {
      y= array[x][0] ;
      z= rand() % y +1 ;
      x = array[x][z] ;
      std::cout <<  "," << x ;
   }   // while
   std::cout << "\n"  ;
   x=1 ;
  }  // for
 //   {main
```

```
{8,2,3,11,12,20,21,29,30,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{28,2,3,11,12,4,5,13,14,8,17,20,21,29,30,22,23,31,32,26,35,6,7,15
,16,24,25,33,34,,,,,,,,,,,,,,,,,,},
{28,2,3,11,12,4,5,13,14,8,17,20,21,29,30,22,23,31,32,26,35,6,7,15
,16,24,25,33,34,,,,,,,,,,,,,,,,,,},
{20,4,5,13,14,2,3,11,12,8,17,20,21,29,30,22,23,31,32,26,35,,,,,,,,,,
,,,,,,,,,,,,,,,,},
{20,4,5,13,14,2,3,11,12,8,17,20,21,29,30,22,23,31,32,26,35,,,,,,,,,,
,,,,,,,,,,,,,,,,},
{20,6,7,15,16,24,25,33,34,2,3,11,12,20,21,29,30,8,17,26,35,,,,,,,,,,
,,,,,,,,,,,,,,,,},
{20,6,7,15,16,24,25,33,34,2,3,11,12,20,21,29,30,8,17,26,35,,,,,,,,,,
,,,,,,,,,,,,,,,,},
{28,8,17,4,5,13,14,2,3,11,12,9,8,20,21,29,30,22,23,31,32,26,35,27
,36,6,7,15,16,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{8,2,3,11,12,20,21,29,30,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{28,2,3,11,12,4,5,13,14,8,17,20,21,29,30,22,23,31,32,26,35,6,7,15
,16,24,25,33,34,,,,,,,,,,,,,,,,,,},
{28,2,3,11,12,4,5,13,14,8,17,20,21,29,30,22,23,31,32,26,35,6,7,15
,16,24,25,33,34,,,,,,,,,,,,,,,,,,},
{20,4,5,13,14,2,3,11,12,8,17,20,21,29,30,22,23,31,32,26,35,,,,,,,,,,
,,,,,,,,,,,,,,,,},
{20,4,5,13,14,2,3,11,12,8,17,20,21,29,30,22,23,31,32,26,35,,,,,,,,,,
,,,,,,,,,,,,,,,,},
{20,6,7,15,16,24,25,33,34,2,3,11,12,20,21,29,30,8,17,26,35,,,,,,,,,,
,,,,,,,,,,,,,,,,},
{20,6,7,15,16,24,25,33,34,2,3,11,12,20,21,29,30,8,17,26,35,,,,,,,,,,
,,,,,,,,,,,,,,,,},
{28,8,17,4,5,13,14,2,3,11,12,9,8,20,21,29,30,22,23,31,32,26,35,27
,36,6,7,15,16,,,,,,,,,,,,,,,,,,},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{12,2,3,11,12,20,21,29,30,38,39,47,48,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{42,20,21,29,30,4,5,13,14,8,17,2,3,11,12,22,23,31,32,26,35,38,39,
47,48,40,41,49,50,44,53,6,7,15,16,24,25,33,34,42,43,51,52,,,,,,},
{42,20,21,29,30,4,5,13,14,8,17,2,3,11,12,22,23,31,32,26,35,38,39,
47,48,40,41,49,50,44,53,6,7,15,16,24,25,33,34,42,43,51,52,,,,,,},
{30,22,23,31,32,4,5,13,14,8,17,20,21,29,30,2,3,11,12,26,35,38,39,
47,48,40,41,49,50,44,53,,,,,,,,,,,,,,,,},
{30,22,23,31,32,4,5,13,14,8,17,20,21,29,30,2,3,11,12,26,35,38,39,
47,48,40,41,49,50,44,53,,,,,,,,,,,,,,,,},
{30,24,25,33,34,6,7,15,16,8,17,26,35,42,43,51,52,2,3,11,12,20,21,
29,30,38,39,47,48,44,53,,,,,,,,,,,,,,,,},
{30,24,25,33,34,6,7,15,16,8,17,26,35,42,43,51,52,2,3,11,12,20,21,
29,30,38,39,47,48,44,53,,,,,,,,,,,,,,,,},
{48,26,35,4,5,13,14,8,17,9,18,20,21,29,30,22,23,31,32,2,3,11,12,2
7,36,38,39,47,48,40,41,49,50,44,53,45,54,6,7,15,16,42,43,51,52,2
4,25,33,34},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{12,2,3,11,12,20,21,29,30,38,39,47,48,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{42,20,21,29,30,4,5,13,14,8,17,2,3,11,12,22,23,31,32,26,35,38,39,
47,48,40,41,49,50,44,53,6,7,15,16,24,25,33,34,42,43,51,52,,,,,,},
{42,20,21,29,30,4,5,13,14,8,17,2,3,11,12,22,23,31,32,26,35,38,39,
47,48,40,41,49,50,44,53,6,7,15,16,24,25,33,34,42,43,51,52,,,,,,},
{30,22,23,31,32,4,5,13,14,8,17,20,21,29,30,2,3,11,12,26,35,38,39,
47,48,40,41,49,50,44,53,,,,,,,,,,,,,,,,},
{30,22,23,31,32,4,5,13,14,8,17,20,21,29,30,2,3,11,12,26,35,38,39,
47,48,40,41,49,50,44,53,,,,,,,,,,,,,,,,},
{30,24,25,33,34,6,7,15,16,8,17,26,35,42,43,51,52,2,3,11,12,20,21,
29,30,38,39,47,48,44,53,,,,,,,,,,,,,,,,},
{30,24,25,33,34,6,7,15,16,8,17,26,35,42,43,51,52,2,3,11,12,20,21,
29,30,38,39,47,48,44,53,,,,,,,,,,,,,,,,},
{48,26,35,4,5,13,14,8,17,9,18,20,21,29,30,22,23,31,32,2,3,11,12,2
7,36,38,39,47,48,40,41,49,50,44,53,45,54,6,7,15,16,42,43,51,52,2
4,25,33,34},
{1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{10,20,21,29,30,38,39,47,48,56,57,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,},
{35,38,39,47,48,22,23,31,32,26,35,20,21,29,30,40,41,49,50,44,53,
56,57,58,59,62,24,25,33,34,42,43,51,52,60,61,,,,,,,,,,,,},
{35,38,39,47,48,22,23,31,32,26,35,20,21,29,30,40,41,49,50,44,53,
56,57,58,59,62,24,25,33,34,42,43,51,52,60,61,,,,,,,,,,,,},
{25,40,41,49,50,22,23,31,32,26,35,38,39,47,48,20,21,29,30,44,53,
56,57,58,59,62,,,,,,,,,,,,,,,,,,,,,},
```

Journal of Electronical & Cyber Defence
Vol. 7, No. 1, 2019, Serial No. 25

The Distributed Denial of Service Attacks Situation Awareness Based on The Prediction of Battle Scene Using Dempster-Shefer Evidences Theories and Bayesian Rules

H. Akbari*, S. M. Safavi, R. Khandani

*Imam Hossein University
(Received: 02/02/2018, Accepted: 27/05/2018)

ABSTRACT

The cyber battle scene has two main actors: attacker and defender. Attacker will reduce or interrupt the services that defender provides by continuously sending huge packets and defender will insist on continuing the services by apply various kinds of security methods. Evaluating this scene from the perspective of an observers can be ambiguous and the scene cannot be predictable. In this research, we have defined different kinds of attacker and defender situations and expertise criteria including: capabilities, response time, tools, capability of continued defense and/or attack operations, and ultimately accessibility of defender's services. We used a dataset include 3003 sequence of attacker or defender situations for measuring the above-mentioned criteria. The results show that half of the scene sequences have a short time, which means that the attacker takes advantage of surprising, the victims not being prepared for the attack. The correlation criteria show that prolonged time length of attack is to the benefit of attacker and the defender's loss is increased. Also, the equipment does not have a positive effect on the response time of the attacker. This means that for the attacker skill is more effective than equipment. Then, in order to predict the situation of battle scene four criteria of impact capacity were combined using the Evidences Dempster-Shefer Theory to predict the victim status and finally, we estimated future methods of attacker and defense strategies of defender by using the Dempster-Shefer Evidences Theory and Bayesian rules and showed using five scenarios in four stages that the reliability of our estimation is more than 65%.

Keywords: Distributed Denial of Service, Botnet, Situation Awareness, Expert, Dempster-Shefer Evidences Theory, Projection of Future

* Corresponding Author Email: kphakbari@ihu.ac.ir