مجله علمی پژوهشی «پدافند الکترونیکی و سایبری»
سال ششم، شماره ۴، زمستان ۱۳۹۷؛ ص ۱۲-۱

تجسم حملات سایبری با تخمین خسارت و ترکیب قابلیت و فرصت مهاجم بر اساس مدل انتقال باور

علی‌جبار رشیدی[1*]، مجید جعفری[2]، کوروش داداش‌تبار احمدی[3]

۱- دانشیار، ۲- دانشجوی کارشناسی ارشد، ۳- استادیار، دانشگاه صنعتی مالک اشتر

(دریافت: ۱۳۹۶/۰۶/۰۵ ، پذیرش: ۱۳۹۷/۰۳/۰۶)

چکیده

در حال حاضر ابزارهای مختلفی برای ثبت رویدادها و هشدارهای موجود در شبکه‌ها وجود دارد. بااین‌وجود، نیاز به سامانه‌ای که بتوان به کمک آن اطلاعات جمع‌آوری‌شده از تمام این منابع را به‌درستی کنار یکدیگر قرار داد و از ترکیب این اطلاعات تصمیم‌های درست اتخاذ نمود، کاملاً محسوس است. اگر قبل از حمله‌ی مهاجمین بتوان آن را پیش‌بینی نمود و اثرات آن را تخمین زد، راهبرد دفاعی مشخص‌تری انتخاب خواهد شد و می‌توان به میزان قابل‌توجهی خسارات را کاهش داد. تجسم حملات سایبری، پیش‌بینی حملات بر اساس یک چارچوب کاری مشخص است. برای این کار می‌توان از روش‌های مختلف ریاضی بهره جست. یکی از این روش‌ها، مدل انتقال باور است. در این پژوهش با استفاده از مدل انتقال باور از دادگان موجود در سطح بالا که همگی رد حمله هستند بهره گرفته‌ایم و با ترکیب قابلیت و فرصت مهاجم که از مؤلفه‌های تجسم حملات سایبری هستند، وضعیت آتی حملات را پیش‌بینی نموده‌ایم. الگوریتم پیشنهادی این پژوهش نسبت به الگوریتم قبلی ارائه‌شده در مرکز ادغام اطلاعات دانشگاه صنعتی مالک اشتر، به‌طور متوسط ۷٪ بهبود داشته است.

واژه‌های کلیدی: تجسم حملات سایبری، آگاهی وضعیتی، تخمین خسارت، قابلیت، فرصت، مدل انتقال باور

۱- مقدمه

با به کارگیری سامانه آگاهی وضعیتی در فرماندهی و کنترل سایبری امکان شناسایی حملات، کشف روابط بین حملات، ردگیری حملات، ارزیابی وضعیتی فضای سایبری و پیش‌بینی اثرات حمله در حجم انبوه داده‌های اخذشده از منابع مختلف فراهم خواهد شد [۱].

در [۲] آگاهی وضعیتی در یک مفهوم کلی این گونه توصیف شده است: "یافتن درک زمانی و مکانی از عناصر موجود در یک محیط، یافتن فهم از روابط میان آن‌ها و مفهومی که این روابط دارد، تجسم وضعیت این عناصر و روابط میان آن‌ها در آینده". همان‌طور که از اسم آن مشخص است آگاهی وضعیتی سایبری به معنای آگاهی یافتن از وضعیت موجود در فضای سایبری یک سازمان است. این فرآیند یک فرآیند دائمی و همواره در حال انجام است و به‌منظور پیش‌بینی حملات و تخمین اثر آن‌ها بر دارایی‌ها و مأموریت‌های سازمان انجام می‌شود. بنا بر تعریف در [۲]، برای رسیدن به آگاهی وضعیتی در فضای سایبری، ابتدا داده‌ها و هشدارهای حسگرهای مختلف مثل سامانه‌های تشخیص نفوذ[1]، دیواره‌های آتش[2]، سامانه‌های پیش‌گیری از نفوذ[3]، مدیریت رویدادها و اطلاعات امنیتی[4]، مرکز عملیات امنیت[5] و غیره در مرحله اول این فرآیند؛ یعنی مرحله درک[6]، جمع‌آوری می‌گردد. سپس اطلاعات جمع‌آوری‌شده، در مرحله دوم فرآیند؛ یعنی مرحله فهم[7]، به اپراتور انسانی یا ماشین تحویل می‌شود. در این مرحله، با کنار هم قرار دادن این اطلاعات و دانشی که از مهاجم وجود دارد (آن را دانش از ایشان[8] می‌نامیم)، وضعیت جاری تخمین زده می‌شود. در انتها، در مرحله تجسم[9] که موضوع این پژوهش است با وضعیت جاری و رویدادهای موجود به همراه دانش از ایشان و دانشی که از توانایی‌ها، دارایی‌ها و مأموریت خود داریم (آن را دانش ما[10] می‌نامیم)، سعی می‌کنیم تا حملات آتی را پیش‌بینی نماییم و اثرات هر یک را بر دارایی‌ها و مأموریت

*رایانامه نویسنده پاسخگو: rashidi@mut.ac.ir

1- Intrusion Detection System (IDS)
2- Firewall
3- Intrusion Prevention System (IPS)
4- Security Information Events Management System (SIEM)
5- Security Operations Center (SOC)
6- Perception
7- Comprehension
8- Knowledge of them
9- Projection
10- Knowledge of us

سازمان تخمین بزنیم. بدین ترتیب می‌توانیم دانش درستی را در اختیار افراد تصمیم‌ساز قرار دهیم تا بتوانند برای تهدید موجود تصمیم درستی اتخاذ کنند. همان‌طور که گفته شد این فرآیند دائمی است، بنابراین، همواره اطلاعات به‌دست‌آمده در مرحله تجسم به مراحل پیشین بازگشت داده می‌شود و اطلاعات در این مراحل به‌روز می‌گردد.

در بخش ۲، مفاهیم اولیه مثل مدل فرآیندی آگاهی وضعتی و مؤلفه‌های تجسم حملات سایبری توضیح داده می‌شود. سپس در بخش ۳، الگوریتم پیشنهادی خود را برای تجسم حملات سایبری شرح خواهیم داد. در بخش ۴، نتایج آزمایش‌های خود را در قالب چند آزماش مختلف بیان خواهیم نمود و در مورد هر یک بحث خواهیم کرد. در آخر، در بخش ۵، یافته‌های خود را در این زمینه جمع‌بندی و پیشنهادهای خود را ارائه خواهیم نمود.

۲- پیش‌زمینه و مفاهیم اولیه

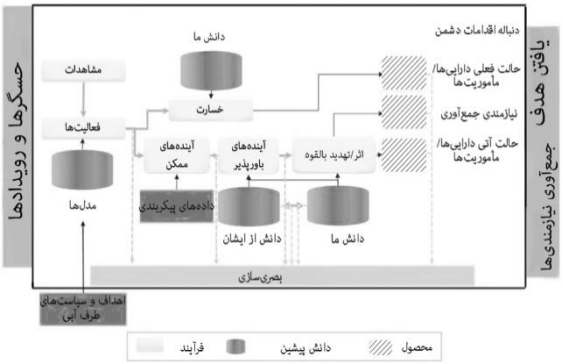
۲-۱- فرآیند تجسم حملات سایبری

فرآیند تجسم حملات سایبری در قالب مدل فرآیندی آگاهی وضعیتی در شکل (۱) تعریف شده است. مشاهدات[1]، ورودی فرآیند است و می‌توان آن را به‌نوعی متناظر با نتیجه سطح اول مدل اصلی آگاهی وضعیتی یعنی سطح درک دانست که در مورد فعالیت‌ها، اطلاعاتی کلی را در اختیار قرار می‌دهد. این فعالیت‌ها که آن را فعالیت‌های موردعلاقه[2] می‌نامیم، فعالیت‌های در حال گذار در سیستم است که در ارزیابی از وضعیت و ایجاد آگاهی وضعیتی برای تصمیم‌ساز مهم است؛ چراکه به‌نوعی مرتبط با سیاست‌ها، اهداف و مأموریت‌های سازمان است. مجموعه‌ای از این فعالیت‌ها در واحد زمان را وضعیت جاری می‌نامیم.

بنا بر آنچه گفته شد، درواقع، ارزیابی وضعیتی تحلیل این فعالیت‌ها و مفهوم آن‌ها یا همان ایجاد وضعیت جاری است. برای این‌که وضعیت جاری ایجاد شود، پس از این که مشاهدات وارد فرآیند و دسته‌بندی شد، یکی از سه حالت زیر رخ می‌دهد:

۱) با یکی از گام‌ها دریکی از فعالیت‌های موجود در ارتباط است، بنابراین، جزء آن گام از فعالیت شناسایی‌شده قرار می‌گیرد.
۲) با هیچ‌یک از فعالیت‌های موجود در ارتباط نیست، بنابراین، اولین مشاهده از یک فعالیت جدید خواهد بود، که مشاهدات آتی با این فعالیت مقایسه می‌گردد.
۳) با هیچ‌یک از فعالیت‌های موجود در ارتباط نیست، ولی می‌تواند به‌عنوان محرک عمل کند و موجب حذف یا ادغام فعالیت‌ها یا گام‌هایی از آن‌ها شود.

همان‌طور که در ادامه آمده است، زمانی که در مرحله تجسم قرار داریم، وضعیت آتی را در نظر می‌گیریم. بنابراین، ارزیابی اثرات وضعیت جاری را می‌توانم ارزیابی خسارت[3] در نظر بگیریم. برای ارزیابی خسارت باید فعالیت‌ها را بررسی کنیم تا در صورت وجود فعالیتی که احتمال دارد خسارتی در آینده به ما تحمیل کند، آن را شناسایی کنیم. این همان چیزی است که از آن به‌عنوان تجسم نام می‌بریم؛ یعنی ارزیابی اثر و تهدید و خساراتی که خواهد داشت. برای این‌که تجسم انجام شود، باید ابتدا فعالیت‌ها شناخته‌شده باشند؛ یعنی مرحله درک انجام شده باشد. سپس باید بدانیم که هر فعالیت چه معنی و مفهومی دارد و تأثیر وجود آن بر ما چیست؛ یعنی باید به فهم وضعیت رسیده باشیم. اطلاعات موردنیاز برای انجام این کار بخشی از دانش ما است که درواقع مجموعه‌ای از دانش در مورد خودمان مثل سیاست‌ها، اهداف و مأموریت‌های سازمان، توانایی کارکنان و سامانه‌های موجود سازمان و غیره است.



شکل (۱): مدل فرآیندی آگاهی وضعیتی [۳]

این‌که دشمن تاکنون چه اقداماتی را انجام داده است یا قرار است در آینده انجام دهد نیز بسیار حائز اهمیت است، که ممکن است یک تصمیم‌ساز نیاز به دانستن آن داشته باشد. این مهم به معنی دخول به حلقه OODA[4] در سمت دشمن است؛ یعنی این‌که تصمیم‌ساز متوجه شود، دشمن چگونه مراحل این حلقه (مشاهده، جهت‌گیری، تصمیم و اقدام) را طی کرده است تا گزینه‌های بیشتری را برای اتخاذ یک تصمیم درست در اختیار داشته باشد. این فرآیند در شکل (۱) با هاشور مشخص شده است و تحت عنوان دنباله اقدامات دشمن[5] آمده است. برای انجام این

1- Observables
2- Activities of Interest (AOI)

3- Damage Assessment
4- Observe, Orient, Decide, Act (OODA)
5- Enemy Course of Ations (eCoA)

فرآیند باید تمامی فعالیت‌های موردعلاقه را در نظر گرفت و بر اساس دانش پیشین آن‌ها را روبه‌جلو تجسم نمود. فعالیت‌ها بر اساس زمان تجسم نمی‌شود، بلکه بر اساس گام بعدی خود تجسم می‌شود. در حال حاضر مشخص نیست که آینده‌های آتی تجسم‌یافته باورپذیر هستند یا خیر. برای این‌که باورپذیری آن‌ها مشخص شود، نیاز به دانشی اضافه تحت عنوان دانش از ایشان داریم که مجموعه دانشی از رفتار گذشته مهاجم، قابلیت‌ها، فرصت‌ها و نیت و اهداف غایی او است. بنابراین، برای آینده‌های ممکن[1] هر یک از فعالیت‌های موردعلاقه، میزان باورپذیری آن‌ها تخمین زده می‌شود. اما آینده‌های باورپذیر به‌تنهایی برای تصمیم‌ساز معنی و مفهومی ندارد، بنابراین، دوباره از دانش ما استفاده می‌کنیم تا تهدیدات بالقوه و اثراتی که بر اهداف سازمان خواهد داشت را شناسایی کنیم. همچنین از دانش ما برای تعیین چیزهایی که باید در آینده جمع‌آوری شود که از آن به‌عنوان نیازمندی جمع‌آوری[2] یاد می‌کنیم، نیز استفاده می‌شود. برای این کار، پس‌ازاین که آینده‌های مورد انتظار تخمین زده شد، رویدادهای تفکیک‌شده کلیدی[3] مشخص می‌شود. سپس با استفاده از این مجموعه از رویداد می‌توان نیازمندی‌هایی که باید جمع‌آوری شود را تعیین نمود. هدف از جمع‌آوری این نیازها، بالا بردن دقت در تخمین میزان باورپذیری آینده‌های دورتر است [۳].

۲-۱-۱- مؤلفه‌های تجسم حملات سایبری

برای انجام مرحله تجسم می‌توان دو مؤلفه کلی دانش از ایشان و دانش ما را در نظر گرفت. درواقع با ادغام عناصر این دو مؤلفه کلی است که فرآیند تجسم حملات سایبری انجام می‌شود.

۲-۱-۱-۱- دانش از ایشان

منظور از دانش از ایشان، اطلاعاتی است که از مهاجم در اختیار داریم. این اطلاعات در ۴ دسته کلی رفتار گذشته، قابلیت، فرصت و نیت قرار می‌گیرد.

- **رفتار گذشته**

یکی از عناصر مهم در تحلیل حملات مهاجم ضبط الگوهای رفتاری گذشته، درنتیجه روتین‌ها ، عادات ، استفاده از کیت‌های ابزاری، تحلیل عقاید و باورهای انسانی و غیره است. راه‌کارهای مختلفی برای ضبط رفتار مهاجم وجود دارد. یکی از این روش‌ها بهره‌گیری از فنون داده‌کاوی است. این فنون عموماً برای فرآیند برون‌خطی[4] ساخته و پرداخته شده است و در حوزه‌هایی که نیازمند عملکرد آنی است و کارکرد نزدیک به زمان واقعی را می‌طلبد، دچار محدودیت است. راه‌کاری دیگر توسعه مجموعه‌ای از دنباله اقدامات دشمن برای انطباق دادن و همبسته‌سازی مشاهدات است. علی‌رغم این‌که این راه‌کار در حوزه مسائلی که در آن دنباله اقدامات دشمن به‌خوبی تعریف شده و نسبتاً پایدار است، مثمر ثمر واقع می‌شود، ممکن است در حوزه‌های مسائلی مثل فضای سایبری که در آن دنباله اقدامات سریع رشد و نمو پیدا می‌کند و نمی‌توان برای آن حدومرزی متصور شد، نیاز به یادگیری‌های خودکار مضاف و خوشه‌بندی رفتارها باشد.

در [۴] یک سیستم استنتاج فازی تقریباً نزدیک به زمان واقعی در زمان‌هایی که مهاجم سریعاً رفتارهای متفاوت و ناشناخته متفاوتی را از خود بروز می‌دهد، توسعه داده شده است. در این روش، نتایج پیش‌گویانه از یک مدل مارکوف با طول متغیر باهم ترکیب می‌شود. این سیستم، F-VLMM نام دارد که الگوهای متوالی مشهود در فعالیت‌های مشاهده‌شده مهاجم را ضبط و با ترکیب ویژگی‌های مختلف که با استفاده از منطق فازی تخمین زده شده است، اقدامات احتمالی بعدی او را پیش‌بینی می‌نماید. در این روش با استفاده از مدل مارکوف با طول متغیر، مدل درخت پسوندی[5] پیش‌بینی می‌شود. این پیش‌بینی برای تمام ویژگی‌ها انجام می‌شود. نتیجه این پیش‌بینی‌ها برای هر ویژگی مختلف با استفاده از منطق فازی ترکیب می‌گردد تا منعکس‌کننده تحلیل‌های انسانی باشد [۳].

- **فرصت**

ارزیابی فرصت یک درک حیاتی از مهاجم را فراهم می‌سازد. تحلیل آسیب‌پذیری‌های خودی که می‌تواند برای مهاجم افشا گردد، به‌شدت در ارزیابی فرصت تأثیر دارد. تحلیل‌های انسانی سنتی فرصت مهاجم را بر اساس تجربه و دانش ما تخمین می‌زند. گاهی اوقات نیز، همانند الگوریتم پیشنهادی در این پژوهش، فرصت به همراه قابلیت مهاجم با یکدیگر ارزیابی می‌شوند، تا مشخص گردد کدام‌یک از فرصت‌ها می‌تواند در عمل توسط مهاجم بهره‌جویی شود. در همین حال که حوزه مسئله پیچیده‌تر می‌گردد و رفتار و قابلیت‌های طرف مخالف بیشتر غیرقابل پیش‌بینی می‌نماید، نیاز به یک راه‌کار ارزیابی فرصت خودکار، سامانمند، و توانمند محسوس‌تر خواهد بود.

یک محیط مجازی[6] از صحنه نبرد سایبری را در نظر بگیرید که یک محیط عملیاتی متشکل از دسترسی‌ها، آسیب‌پذیری‌ها و وابستگی‌های داخلی بین طرفین به هر شکل فیزیکی، فرهنگی و یا سایبری را مدل می‌کند. به‌عنوان‌مثال این محیط مجازی می‌تواند یک مدل بر اساس گراف، یا مدل هستان‌شناسی[7] باشد.

1- Possible futures
2- Collection Requirement
3- Key differentiating events
4- Off-line
5- Suffix tree
6- Virtual terrain
7- Ontology

با کنار هم قرار دادن مشاهدات مربوط به فعالیت هر طرف در این محیط مجازی، به‌صورت نظری می‌توان پیشرفت هر فعالیت را قیاس کرد، و در ادامه آینده‌های باورپذیر فرضی را بر اساس میزان سختی برای بسط دادن آن به رویدادهای آتی، تفکیک ساخت. در واقعیت، ساخت و تنظیم پویای چنین محیط مجازی با دقت بالا ممکن است بسته به حوزه مسائل امکان‌پذیر نباشد.

مرجع [۵] مدلی را بر اساس گراف پیشنهاد می‌کند که وابستگی‌های بین جبهه‌های مختلف در فضای سایبری را بازنمایی می‌نماید و برای ارزیابی اثر در [۶] و ارزیابی فرصت در [۷] مثمر ثمر واقع شده است. مثالی دیگر محیط مجازی که می‌تواند به‌صورت بالقوه برای ارزیابی فرصت استفاده گردد، مدل محیط انسانی[1] است [۹-۸]. یک چالش بحث‌برانگیز در مورد ارزیابی فرصت، توسعه یک محیط مجازی توانمند است که بتوان آن را به حوزه‌های مختلف بسط داد.

در مورد ارزیابی فرصت در حملات سایبری می‌توان گفت، مشاهدات ممکن است در محیط مجازی کنار هم قرار داده شود [۱۰] و با تفکیک کردن از طریق بررسی قوانین دیواره آتش، آسیب‌پذیری در سرویس‌های شبکه و حالت دستگاه‌های هدف و به مخاطره افتاده[2] بتوان مسیرها را قیاس نمود [۲]. در فرآیند جستجو برای فرصت‌ها و یا دستگاه‌های هدف آسیب‌پذیر، یک چالش محاسباتی، پیمایش گراف مدل محیط مجازی است. یک الگوریتم جستجوی ابتدا-عرض[3] با بازده بالا برای ترکیب و انطباق گره‌های موردحمله و قوانین مربوطه توسعه داده شده است تا الگوریتم قدرت اجرای تقریباً بلادرنگ در حملات سایبری را داشته باشد. اصلی‌ترین مزیت استفاده از ارزیابی فرصت به‌صورت خودکار کاهش فضای جستجو از تمام آینده‌های محتمل به آینده‌های باورپذیر است. مطالعات شبیه‌سازی‌شده یک کاهش ۵۰٪ تا ۹۰٪ فضای جستجو را نشان می‌دهد. این مقدار از تفاوت در عملکرد، به‌علت وجود سناریوهایی خاص است که در آن بعضی از حملات، در مراحل ابتدایی حمله، آینده‌های احتمالی کمی را متصور می‌شود اما درعین‌حال تمایز این آینده‌ها دشوار است، این در حالی است که در دیگر حملات ممکن است شاهد آینده‌های بسیاری باشیم که به‌راحتی قابل‌تمایز از یکدیگر هستند [۳].

- **قابلیت**

درحالی‌که ارزیابی فرصت به‌صورت سامانمند آسیب‌پذیری‌های افشاشده را استنتاج می‌نماید، نتایج آن باید در ادامه با ارجاع متقابل به قابلیت‌های مهاجم برای دسترسی به هر دارایی[4] از سازمان که برای انجام یک یا چند مأموریت سازمان ضروری است، تحلیل گردد. ترکیب قابلیت و فرصت امری است حیاتی، چراکه هر یک از آن‌ها به‌طور مجزا برای پیش‌بینی اقدامات مهاجم اطلاعات کمی محسوب می‌شود .

ارزیابی قابلیت به شیوه سنتی به‌شدت به آرایش نظامی مهاجم (مانند نیروی انسانی، ادوات تسلیحاتی و غیره) بستگی دارد. زمانی که به‌سختی بتوان مهاجم را شناسایی کرد و یا اطلاعات کمی از آن در اختیار باشد، آرایش‌دهی نظامی آماری انطباقی، همتایی متوالی و خوشه‌بندی ممکن است مورد استفاده قرار گیرد. در تحلیل حملات سایبری، حملاتی که قابلیت مشابهی دارند از طریق بررسی سرویس‌هایی از شبکه که مورد حمله قرار گرفته‌اند، و شدت حملات، شناسایی می‌شود. یک الگوریتم آرایش دهی آماری بر اساس سرویس‌های مورد حمله در [۷] توسعه داده شده است. ویژگی‌های سایبری چندگانه برای تعیین شباهت میان حملاتی استفاده شده است که از الگوریتم بزرگ‌ترین زیررشته مشترک استفاده می‌نماید [۱۱]. علاوه بر این، خوشه‌بندی سلسله‌مراتبی تقسیم‌کننده[5]، که در شناسایی روابط برای تحلیل شبکه اجتماعی مثمر ثمر واقع شده است، برای گروه‌بندی انواع مختلف مانورهای حمله در یک شبکه رایانه‌ای به کار بسته شده است.

لزوماً شناسایی دقیق قابلیت مهاجم که نیازمند دانش خبره است، هدف تحلیل قابلیت به‌صورت خودکار نیست. هدف رده‌بندی قابلیت‌های مختلف مهاجم است. نتایج نشان می‌دهد که با ارزیابی قابلیت‌های رده‌بندی‌شده، به مقادیر مختلف اثربخشی دست پیدا خواهیم کرد. تفاوت در عملکرد این روش وابسته به این است که تا چه حد فضای ویژگی‌های انواع مختلف مهاجمین را به‌درستی تمیز داده است [۳].

- **نیت و اهداف غایی**

مطابق [۱۲]، می‌توان به‌عنوان قصد و عزم کاری معین و یا یک حالت ذهنی که در آن کاری صورت می‌گیرد، نیت را نگاه کرد. مقصود از نیت هر چیزی مثل نشانه، برنامه، عمد، قصد، هدف و غایت را در برمی‌گیرد.

همان‌طور که در [۱۲] موردتوجه قرارگرفته است، نیت یک مفهوم غیرملموس است که نمی‌توان آن را مستقیماً با حسگرها مشاهده نمود، و باید با مشاهده دیگر جنبه‌ها از علوم گوناگون به دنبال شاخصه‌هایی از نیت گشت و آن را تفسیر نمود. این امر، نیازمند یک مدل از نیت است که در حد لزوم دقیق و با جزئیات باشد، و از عوامل متعددی که نیت را ناشی می‌شوند، درک درستی بدهد. تلاش‌های گذشته در جهت تعریف یک مدل برای

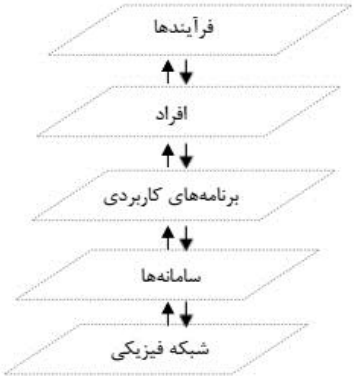
1- Human terrain
2- Compromised
3- Breadth first
4- Asset
5- Divisive Hierarchical Clustering (DHC)

نیت یک دیدگاه نظامی در مورد نیت فرمانده، یک چارچوب عقیده- علاقه- نیت، مدل‌های نیت بر اساس برنامه‌ریزی، نیت صریح و ضمنی و همین‌طور خبرگان چیره بر موضوع[1] را شامل می‌شود. صرف داشتن علاقه اجازه به اجرای نیت را نمی‌دهد، بلکه یک فرد باید فرصت لازم برای اجرای اقدامات خود در شرایط بحرانی مدنظر خود را داشته باشد. فرصت‌ها امکان انجام نیت یک فرد با قابلیت‌های کافی را میسر می‌سازد [۱۴-۱۳]. یک فرصت درواقع، حضور یک محیط عملیاتی است که در آن اهداف بالقوه یک عمل حاضر و مستعد مفعول واقع‌شدن هستند [۱۳].

علاوه‌بر این‌ها، برآورد نیت طرف مخالف تقریباً چالش برانگیزترین وظیفه در بیشتر حوزه‌های مسئله است، و بستگی بسیاری به خبرگان چیره بر موضوع که بخشی از دانش ایشان محسوب می‌گردند، دارد. رهیافت‌های ترکیب باور می‌تواند برای کمک در ادغام ایده‌های خبرگان چیره بر موضوع به کار بسته شود. علاوه‌بر این، ممکن است نیت در بدترین حالت برآورد شود [۱۵]. علی‌الخصوص، اگر دانش پیشین کمی در مورد مهاجمی خاص در دست باشد. به‌عنوان مثال افراد یاغی در یک قلمرو نامشخص و یا هکرهای اینترنتی، ممکن است فرض شود که اهدافی که قصد حمله به آن‌ها شده است، حیاتی‌ترین دارایی‌ها و یا مهم‌ترین اطلاعات مربوط به یک یا چند مأموریت است. این برآورد نیت بر اساس مأموریت و بدترین حالت را می‌توان از طریق پیگیری اقدامات مهاجم، تأیید کرد [۱۶].

۲-۱-۱-۲- دانش ما

در ساده‌ترین مفهوم، دانش ما اطلاعاتی است که محیط‌ها، دارایی‌ها و مأموریت‌های خودی را تشریح می‌کند و برای سطح بالاتری از تحلیل مفید است. در حوزه سایبری، این اطلاعات می‌تواند به همراه احتمالات دیگری چون نتایج ارزیابی‌های آسیب‌پذیری، گزارش‌های کتبی یا هشدارهایی از سوی مدیریت شبکه یا مدیریت امنیت اطلاعات، گزارش‌های مربوط به پیکربندی دستگاه‌ها، نقشه‌های همبندی[2] شبکه، خدماتی که یک دستگاه ارائه می‌کند، و در این اواخر اطلاعاتی در مورد چگونگی استفاده از دستگاه‌های خاص شبکه برای پشتیبانی از انجام مأموریت‌ها (و یا فرآیندهای کسب‌وکار) باشد. این‌ها همان اطلاعاتی هستند که برای انجام ارزیابی خسارت مطابق آنچه در مدل فرآیندی آگاهی وضعیتی بیان شد، و همین‌طور برای انجام ارزیابی اثر و یا تهدید لازم است. برخی محققین در این زمینه، تحلیل چگونگی عملکرد دستگاه خسارت‌دیده در وظایف انجام‌شده فعلی را، تنها اطلاعات لازم برای ارزیابی خسارت می‌دانند. دانستن این‌که یک دستگاه در برابر یک حمله که قبلاً اتفاق افتاده است، آسیب‌پذیر می‌باشد اطلاعات خوبی محسوب می‌گردد، اما برای ارزیابی اثر یا خسارت فعلی واردشده به دستگاه مفید نخواهد بود. اطلاعات بسیار زیادی می‌تواند برای تحلیل ارزیابی اثر یا تهدید آینده‌های باورپذیر مورداستفاده قرار گیرد.



شکل (۲): سطوح انتزاعی در نگاشت مأموریت [۱۶]

بزرگ‌ترین چالش فنی موجود مربوط به این اطلاعات، نگهداری[3] و در جریان نگه‌داشتن[4] آن‌ها است. دانستن این‌که ترتیب اثر به یک فرآیند کسب و کار، هفته‌ها و یا حتی ساعت‌ها بعد از فعالیت مخرب صورت گرفته است خیلی مفید نخواهد بود، علی‌الخصوص زمانی که به تصمیم‌گیری، عمل و ادامه دادن به فرآیند، نیاز فوری باشد. که این شرایط در فضای کسب و کار و در محیط شبکه وجود دارد.

بخش بسیار عظیمی از اطلاعات مذکور می‌تواند با تأیید درجات موفقیت و با استفاده از فناوری‌های خودکار، جمع‌آوری گردد. اما به علت محدودیت بار شبکه، سختی در فنون خودکار و پیچیدگی‌های داده‌ای، اطلاعات همیشه به‌روز نخواهد بود. اغلب اوقات کمبود هر نوع فن خودکار برای ضبط اطلاعات را می‌توان حس کرد. به‌منظور انجام تحلیل‌های در عمق و فراهم کردن کامل‌ترین سطح آگاهی برای یک تصمیم‌ساز، این موضوع مورد اهمیت قرار می‌گیرد که این داده‌ها آماده، دقیق و به‌روز باشد. علاوه بر این، یک معضل پیچیده دیگر نیز وجود دارد و آن زمانی است که یک دستگاه منفرد برای انجام تعداد زیادی وظیفه مورداستفاده قرار گیرد، خصوصاً زمانی که این وظایف در طول زمان تغییر می‌کند و یا ممکن است با دوره تناوب خاصی انجام شود. همان‌طور که یک دستگاه منفرد می‌تواند برای انجام چندین هدف ازپیش‌تعیین‌شده مورداستفاده قرار گیرد، یک خدمت منفرد نیز ممکن است به مجموعه‌ای از دستگاه‌ها نیاز داشته باشد. تمام

1- Subject Matter Experts (SMEs)
2- Topology
3- Maintenance
4- Currency

این‌ها به پیچیدگی آمادگی داده، دقت و به‌روز بودن آن‌ها می‌افزاید.

شکل (۲)، یک مجموعه از آغاز کارها در این حوزه و مجموعه کلی داده‌هایی که برای تحلیل مفید هستند را شناسایی می‌کند. لایه‌های نشان داده شده در این شکل، مدل‌های شبکه، مدل‌های سیستم، برنامه‌های کاربردی، کاربران و مدل‌های فرآیندهای کسب‌وکار را تشریح می‌کند و ارتباط بین لایه‌ها، وابستگی‌ها را نشان می‌دهد [۱۷]. یک مدل هستان‌شناسی که این لایه‌ها و ارتباط بین آن‌ها را تشریح می‌سازد در [۶] توسعه داده شده است. سایر کارها روی مدل‌ها و ارتباطات در [۱۱-۱۰] توصیف شده‌اند. در حال حاضر نیز استفاده از این مدل‌ها با در نظر گرفتن ماهیت بسیار پویای حوزه‌های عملیاتی مفید خواهد بود. باید به ضبط داده در روگرفت‌های لحظه‌ای[1] که به‌سرعت منقضی می‌شوند و از اطلاعات به‌صورت شناختی[2] یا با به‌روزرسانی انباره‌های داده حفظ و نگهداری می‌کنند، توجه داشت. حالت آرمانی این است که جمع‌آوری داده، به‌روزرسانی مدل‌ها و انجام جمع‌آوری با حصول اطمینان از به‌هنگام بودن و دقیق بودن و نداشتن سربار روی شبکه، به‌صورت خودکار انجام شود.

۳- روش تحقیق

همان‌طور که پیش‌تر گفته شد، در این پژوهش تجسم حملات سایبری را به کمک ادغام مؤلفه‌های فرصت و قابلیت مهاجم انجام خواهیم داد. روش کلی، الگوریتم ارائه‌شده در [۱] و استفاده از چارچوب FuSIA[3] ارائه‌شده در [۷] است. برای این‌که الگوریتم اثربخشی بیشتری داشته باشد و تجسم به واقعیت نزدیک‌تر باشد، تغییراتی در الگوریتم پیشنهادی در [۱] صورت گرفته است که در ادامه در مورد آن صحبت خواهیم کرد.

۳-۱- الگوریتم تخمین قابلیت

در این پژوهش همانند [۱] و [۷] با شناسایی سرویس‌هایی از شبکه که مهاجم قادر به حمله به آن‌ها بوده است، قابلیت مهاجم را تخمین می‌زنیم. برای این‌کار باید آسیب‌پذیری‌های هر سرویس را مورد بررسی قرار دهیم. آسیب‌پذیری مربوط به هر سرویس با مراجعه به پایگاه داده CVE تعیین شده است. فرض کنیم S، مجموعه تمام سرویس‌های موجود در شبکه و $S_a \subseteq S$ مجموعه سرویس‌هایی باشد که در حمله a مورد تهاجم قرار گرفته است. مشکل اصلی، تخمین امکان وجود داشتن سرویس $s \notin S_a$ که در حملات بعدی، مشخص شده است که جز قابلیت‌های مهاجم در حمله a بوده است ($s \in a$)؛ یعنی $S_a \subseteq a$ است.

در حالت کلی، برای هر $s \in a$، یا s متعلق به مجموعه $a \cap S_a$ است یا متعلق به مجموعه $a \cap \overline{S_a}$. بنابراین، چارچوب تشخیص[4] $\Omega_1 = \{a, \overline{S_a} - a\}$ خواهد بود و رابطه (۱) برقرار خواهد بود:

$$\begin{aligned} Bel(s \in a) &= m(s \in (a \cap S_a)) \\ &+ m\left(s \in \left(a \cap \overline{S_a}\right)\right) \\ &= m_{S_a}(s) + m_{\overline{S_a}}(s) \end{aligned} \quad (۱)$$

که در آن، $\overline{S_a}$ مجموعه سرویس‌هایی است که در S_a وجود ندارد. برای این‌که بتوانیم به تخمین دقیق‌تری دست پیدا کنیم از مدل انتقال باور به‌جای احتمال بهره جسته‌ایم. با رده‌بندی قابلیت مهاجم می‌توانیم اثربخشی هر حمله را بهتر مشخص کنیم. بنابراین هر سرویس $s \in S$ یکی از ۴ حالت زیر را در هر حمله خواهد داشت:

- s_u برای زمانی که به s حمله شده باشد اما این حمله موفقیتی را در بر نداشته باشد.
- s_d برای زمانی که s اسکن و درنتیجه کشف شده باشد.
- s_p برای زمانی که درنتیجه حمله، کنترل s تا حدی به دست مهاجم افتاده باشد.
- s_c برای زمانی که درنتیجه حمله، کنترل s به‌طور کامل به دست مهاجم افتاده باشد.

درنتیجه رابطه (۱) به رابطه (۲) تبدیل خواهد شد:

$$\begin{aligned} Bel(s) = m_{S_a}(s_u) &+ m_{S_a}(s_d) + m_{S_a}(s_p) + m_{S_a}(s_c) \\ &+ m_{\overline{S_a}}(s_u) + m_{\overline{S_a}}(s_d) + m_{\overline{S_a}}(s_p) \\ &+ m_{\overline{S_a}}(s_c) \end{aligned} \quad (۲)$$

این رابطه، کران پایین تخمین را حساب می‌کند. کران بالای تخمین از رابطه (۳) به دست می‌آید

$$\begin{aligned} &\Omega_2 = \{s | s \in S\} \\ &Pl(s) = Bel(\Omega_2) - Bel(\overline{s}) \end{aligned} \quad (۳)$$

که در آن، منظور از $\overline{s}$ مجموعه مکمل سرویس s است.

امتیاز تجسم[5]، امکان حمله به هر سرور یا خوشه‌ای از ماشین‌های میزبان موجود در شبکه را تخمین می‌زند. این امتیاز با استفاده از امتیاز خسارت[6] که در ادامه نحوه محاسبه آن را شرح خواهیم داد، محاسبه می‌شود. همچنین با کمک $Bel(s)$ و $Pl(s)$ امتیاز اطمینان[7] را محاسبه می‌کنیم که همان‌طور که از نام آن پیدا است، میزان اطمینان به تخمین محاسبه‌شده را اندازه‌گیری می‌کند. امتیاز اطمینان برای تخمین قابلیت با فاصله کران بالای تخمین (Pl) و کران پایین آن (Bel) رابطه مستقیم دارد؛ هرچه

1- Snapshots
2- Cognitive
3- Future Situation and Impact Assessment (FuSIA)

4- Frame of discernment
5- Projection score
6- Damage score
7- Reliability score

این فاصله کمتر باشد، میزان اطمینان به این تخمین بیشتر است.

در این روش، برای این‌که تخمین قابلیت واقعی‌تر انجام شود، به‌جای استفاده از توزیع احتمال یکنواخت که در [۱] انجام شده است، از قانون شرطی‌سازی دمپستر و شفر[1] استفاده کرده‌ایم. برای انجام این کار، به‌ازای هر یک از حملات که حداقل یکی از عناصر S_a در آن وجود دارد و در سرویس s با یکدیگر مشترک هستند، امتیاز خسارت را تخمین زده و آن‌ها را با یکدیگر ترکیب نموده‌ایم.

درادامه، باتوجه به توضیحات فوق الگوریت مورد استفاده را بیان خواهیم نمود.

فرض کنیم H مجموعه تمام میزبان‌های موجود در شبکه باشد. در این صورت برای هر $h \in H$ الگوریتم آمده در شکل (۳) را خواهیم داشت:

```
Given a, S, S_a, H
A = the set of attacks with at least one element of S_a
for all s ∈ S do
    if s ∈ S_a then
        s.score = 1.0
        s.reliablity = 1.0
    else
        for all a_i ∈ A do
            m(a_i) = d_s(a_i)

        m(s) = Σ_{B∩C=s, B,C∈A} m(B)m(C)
        s.score = m(s)
        s.reliability = 1 − (Pl(s) − Bel(s))
    end if
end for
for all h ∈ H do
    S(h) = set of services provided by machine h
    h.score = max_{s∈S(h)}(s.score)
    h.reliability = max_{s∈S(h)}(s.reliability)
end for
```

شکل (۳): الگوریتم تخمین قابلیت [یافته تحقیق]

منظور از d_s امتیاز خسارت است که در ادامه نحوه تخمین آن شرح داده خواهد شد.

۳-۲- الگوریتم تخمین خسارت

برای تخمین خسارت به سرویس‌ها، آن‌ها را بر اساس چند فضای حالت دسته‌بندی می‌کنیم و به هر یک از این حالت‌ها در فضای حالت خود یک امتیاز تخصص می‌دهیم. حالات مختلف در یک فضای حالت با یکدیگر دوبه‌دو ناسازگار هستند؛ یعنی یک سرویس در هر لحظه و در هر فضای حالت تنها یک حالت می‌تواند داشته باشد. درنهایت برای این‌که خسارت وارده به هر سرویس در یک حمله را تخمین بزنیم، امتیاز این سرویس در هر فضای حالت را با استفاده از مدل انتقال باور ترکیب می‌نماییم.

در هر فضای حالت، امتیاز خسارت را با $d_{i,j(t)}$ که نشان‌دهنده امتیاز خسارت تخمین‌یافته برای سرویس i در فضای حالت j در زمان t است. در این پژوهش دو فضای حالت برای سرویس‌های موجود در شبکه، در نظر گرفته‌ایم: ۱) فضای حالت مهاجم، و ۲) فضای حالت عملیاتی که به ترتیب در جدول (۱) و جدول (۲) شرح داده شده است.

حالت‌های موجود در فضای حالت مهاجم، درواقع حالت‌های بالقوه یک سرویس از دیدگاه مهاجم هستند. این حالت‌ها همان حالت‌هایی است که یک سرویس هنگام حمله ممکن است داشته باشد. اما حالت‌های موجود در فضای عملیاتی، حالت سرویس موردنظر ازنظر عملکرد در شبکه خودی را نشان می‌دهد که یا کاملاً عملیاتی است و می‌توان بدون هیچ مشکلی از این سرویس استفاده کرد، یا نیاز به تعمیر و نگهداری دارد[2]، یا در حال تحلیل رفتن و افول کردن است[3]، و یا دیگر نمی‌توان از آن استفاده کرد و عملکردی برای شبکه ندارد[4].

همان‌طور که گفته شد، به هر یک از این حالت‌ها در فضای حالت خود امتیازی داده‌ایم. توجه شود که محاسبه این امتیازها اصولاً بر اساس دانش ما خصوصاً همبندی شبکه و دانش پیشین است. در این پژوهش ما یک توزیع خطی را برای فضای حالت مهاجم و یک توزیع غیرخطی را برای فضای حالت عملیاتی بر اساس هستان‌شناسی شبکه مورداستفاده، در نظر گرفته‌ایم.

همان‌طور که پیش‌تر اشاره شد، از مدل انتقال باور برای ترکیب امتیاز خسارت هر سرویس از هر فضای حالت، استفاده کرده‌ایم. چارچوب تشخیص در این مسئله $\{D, N\}$ خواهد بود. به‌طوری‌که، D بیانگر این باور است که سرویس موردنظر در انجام وظایف خود ناتوان است؛ یعنی $D = d_{i,j}(t)$ و N بیانگر این است که سرویس موردنظر توانایی انجام وظایف خود را دارد؛ یعنی $N = 1 - d_{i,j}(t)$.

جدول (۱): فضای حالت مهاجم و امتیاز خسارت حالت‌های آن

حالت	امتیاز خسارت ($d_{i(t)}$)
Normal	۰/۰۰
Attempted	۰/۲۵
Discovered	۰/۵۰
Partially Compromised	۰/۷۵
Compromised	۱/۰۰

1- Dempster-Shafer rule of conditioning

2- Maintenance
3- Degraded
4- Non-operational

جدول (۲): فضای حالت عملیاتی و امتیاز خسارت حالت‌های آن

حالت	امتیاز خسارت ($d_{i(t)}$)
Operational	۰/۰۰
Maintenance	۰/۳۰
Degraded	۰/۷۰
Non-operational	۱/۰۰

ماهیت روش‌های مبتنی بر نظریه شواهد دمپستر و شفر مثل مدل انتقال باور به‌گونه‌ای است که ترکیب امتیازات پایین ممکن است یک امتیاز پایین‌تر باشد؛ که این مورد برای محاسبه اثر یا خسارت در یک حمله سایبری نامطلوب است. همچنین، ترکیب امتیازات بالا، نیز ممکن است حتی امتیاز بالاتری را نتیجه دهد؛ که این مورد برای محاسبه اثر یا خسارت مطلوب است، و بنابراین در روش خود آن را لحاظ کرده‌ایم.

رابطه (۴) راهکار پیشنهادی ما برای ترکیب امتیاز خسارت از فضاهای حالت مختلف را نشان می‌دهد.

$$d_i(t) = \begin{cases} max_{j\in J}(d_{i,j}(t)), & \forall i,j;\ d_{i,j}(t) < \\ \bigoplus_{j\in J, d_{i,j}(t)\geq 0.5}(d_{i,j}(t)), & \exists d_{i,j}(t) \geq 0.5 \end{cases} \quad (۴)$$

که در آن، منظور از $\oplus$ قانون ترکیب[1] دمپستر و شفر است.

در راه‌کار پیشنهادی، زمانی که تمام امتیازات پایین باشد، بیشترین امتیاز مدنظر قرار گرفته می‌شود تا نتیجه نهایی ترکیب حداقل به‌اندازه بدترین حالت ممکن باشد، نه کمتر از آن. چنانچه حداقل یکی از امتیازات بالای ۰/۵ باشد، از مدل انتقال باور برای ترکیب امتیازات بالا استفاده می‌کنیم تا مطمئن باشیم که امتیاز ترکیبی از هر امتیاز دیگری بالاتر است.

۳-۳- الگوریتم تخمین فرصت

برای تخمین فرصت، از روش ارائه‌شده در [۱] و چارچوب FuSIA در [۷] باکمی تغییر بهره گرفته‌ایم. در این روش از باورهای رتبه‌بندی شده[2] مشابه روشی که برای تخمین خسارت انجام داده‌ایم، استفاده شده است. در [۱] همچنین الگوریتمی برای به‌روزرسانی اشیا موردعلاقه، ارائه شده است که ماشین‌های تحت کنترل کامل مهاجم، ماشین‌های هدف مورد انتظار که از طریق ماشین‌های تحت کنترل می‌توان به آن‌ها دسترسی پیدا کرد، و قوانین دیواره آتش میان آن‌ها و دیگر ماشین‌های موجود در شبکه که در تخمین فرصت نقش مهمی دارد، در آن محاسبه شده است.

همانند تخمین خسارت، برای این‌که ترکیب امتیازات پایین تجسم فرصت و اطمینان آن، پایین‌تر از بدترین امتیاز نباشد، رابطه موجود در [۱۷] برای تخمین فرصت را به رابطه (۵) تغییر داده‌ایم:

$$o(Ps,t) = \begin{cases} max(c_i), & \forall i \in \Omega(\mathrm{p});\ c_i < 0.5 \\ \frac{\prod_{i\in\Omega(p_{s,t})} c_i}{\max(\prod_{i\in\Omega(\mathrm{p})} c_i)}.MaxProjScr, & \exists c_i \geq 0.5 \end{cases} \quad (۵)$$

t تحت کنترل مهاجم و مقصد s مسیر بین مبدأ $P_{s,t}$ که در آن امتیاز تجسم فرصت حاصل ترکیب از امتیاز $o(Ps,t)$در شبکه و ۴ عنصر حالت مبدأ، حالت مقصد، قوانین دیواره آتش و باز بودن سرویس‌ها از مسیر است که در [۱] تعریف شده است. همچنین یک مقدار ثابت و نشان‌دهنده بیشترین امتیاز $MaxProjScr$ است. همین رابطه را می‌توان برای 0.9تجسم فرصت و برابر با امتیاز اطمینان فرصت نیز در نظر گرفت که در (۶) آمده است:

$$r(Ps,t) = \begin{cases} max(c_i), & \forall i \in \Omega(\mathrm{p});\ c_i < 0.5 \\ \frac{\prod_{i\in\Omega(p_{s,t})} c_i}{\max(\prod_{i\in\Omega(\mathrm{p})} c_i)}.MaxRelScr, & \exists c_i \geq 0.5 \end{cases} \quad (۶)$$

که در آن، $r(Ps,t)$ امتیاز اطمینان فرصت حاصل ترکیب است. همچنین $MaxRelScr$ یک مقدار ثابت و نشان‌دهنده بیشترین امتیاز اطمینان فرصت است که آن‌هم برابر با ۰/۹ است.

۳-۴- ترکیب قابلیت و فرصت با استفاده از مدل انتقال باور

در اصل، استفاده از مدل انتقال باور به‌جای استفاده از خود نظریه شواهد دمپستر و شفر، این است که مدل انتقال باور نیازی به فرآیند نرمال‌سازی تناقضات[3] ندارد. و این پیچیدگی الگوریتم ازنظر زمانی را کاهش می‌دهد. و درنتیجه عملکرد روش، قوی‌تر خواهد بود.

چارچوب تشخیص $\Psi = \{P, N\}$ برای این مسئله را در نظر بگیرید که در آن، P بیانگر این است که هدف A باورپذیر است، و N به معنی باورناپذیر بودن هدف A است. در این صورت تابع جرم مورد استفاده برای ارزیابی مطابق رابطه (۷) خواهد بود:

$$\mathrm{m_i(A)} = \begin{cases} \mathrm{p_i r_i}, & \mathrm{A} = \{\mathrm{P}\} \\ (1-\mathrm{p_i})\mathrm{r_i}, & \mathrm{A} = \{\mathrm{N}\} \\ 1-\mathrm{r_i}, & \mathrm{A} = \{\mathrm{P,N}\} \end{cases} \quad (۷)$$

که در آن، p و r به ترتیب امتیاز تجسم و اطمینان است، و i می‌تواند مقادیر c یا o را به ترتیب برای قابلیت و فرصت بگیرد.

1- Demspter-Shafer rule of combination
2- Ranked belief
3- Conflict Normalization Process

بنابراین، بر اساس قانون شرطی‌سازی دمپستر و شفر رابطه (۸) را برای ادغام قابلیت و فرصت خواهیم داشت:

$$m_f(A) = m_c(A) \oplus m_o(A) = \sum_{B \cap C = A} m_c(B) m_o(C) \quad (۸)$$

با استفاده از رابطه (۸)، علاوه بر تجسم ادغام‌شده $m_f(A)$ می‌توان عدم قطعیت موجود را نیز به‌دست آورد. توجه شود که به‌ازای $A = \emptyset$، رابطه (۷) تمام مجموعه‌های ناسازگار در Ψ را با یکدیگر جمع می‌کند. این بدان معنی است که $m_f(\emptyset)$ بیانگر تعداد تضاد موجود میان توابع جرم یا همان ارزیابی‌های انجام‌شده است که با یکدیگر ترکیب می‌شود. $m_f(P,N)$ نشان‌دهنده عدم قطعیت کل در نتیجه ادغام شده است، و امتیاز تجسم بین $m_f(P)$ و $m_f(P) + m_f(\emptyset) + m_f(P,N)$ خواهد بود. با این‌که هر عددی در این بازه می‌تواند مورد قبول باشد، برای این‌که بتوانیم گام‌های دیگر تجسم را بر اساس این گام انجام دهیم، نیازمند یک مقدار ثابت برای امتیاز تجسم هستیم. این مقدار با استفاده از رابطه (۹) به دست می‌آید:

$$reliability = 1 - (m_f(\emptyset) + m_f(P,N))$$
$$projection = \frac{m_f(P)}{reliability} \quad (۹)$$

۴- نتایج و بحث

برای این‌که بتوانیم کارایی الگوریتم خود را با الگوریتم ترکیب قابلیت و فرصت ارائه‌شده در [۱] مقایسه کنیم، از همان دادگان استفاده‌شده در [۱] بهره جسته‌ایم. بدیهی است که شبکه شبیه‌سازی‌شده نیز همانند [۱] است. بنابراین، نتایج خود را در دو سناریو حمله متفاوت با نتایج الگوریتم پیشنهادی در [۱] مقایسه خواهیم نمود. اولین سناریو، یک حمله ده مرحله‌ای با سطح تأثیر بالا[1] و دومین سناریو، یک حمله چهارده مرحله‌ای با سطح تأثیر پایین[2] است. سطح تأثیر یک حمله نشان‌دهنده میزان انحراف مهاجم از کوتاه‌ترین مسیری است که برای رسیدن به میزبان هدف انتخاب می‌کند. یک حمله در حالتی مؤثرتر است که از کمترین انحراف برای رسیدن به مقصد استفاده شود [۱]. در جدول‌های (۳) و (۴) دو نمونه سناریوی حمله به ترتیب با سطح تأثیر بالا و پایین آمده است.

همان‌طور که در جدول‌های (۳) و (۴) می‌بینید، برای پیاده‌سازی این دو سناریو، حملات متفاوتی انجام شده است. همچنین از سرویس‌های مختلف و قوانین متعدد دیواره‌های آتش بین میزبان‌های شبکه استفاده شده است.

جدول (۳): یک سناریو حمله با سطح تأثیر بالا

مرحله	آدرس مهاجم	آدرس قربانی
۱	۹,۵,۲۳۱,۷۲	۱۹۲,۱۶۸,۱,۳
۲	۲۲۷,۲۲,۲۰۲,۱۴	۱۹۲,۱۶۸,۱,۳
۳	۱۷۸,۸۷,۴۶,۹۱	۱۹۲,۱۶۸,۱,۳
۴	۱۹۲,۱۶۸,۱,۳	۱۹۲,۱۶۸,۲,۶
۵	۱۹۲,۱۶۸,۱,۳	۱۹۲,۱۶۸,۲,۸
۶	۱۹۲,۱۶۸,۱,۳	۱۹۲,۱۶۸,۲,۹
۷	۱۹۲,۱۶۸,۱,۳	۱۹۲,۱۶۸,۲,۱۸
۸	۱۹۲,۱۶۸,۲,۱۸	۱۹۲,۱۶۸,۴,۲۲
۹	۱۹۲,۱۶۸,۴,۲۲	۱۹۲,۱۶۸,۶,۱۱
۱۰	۱۹۲,۱۶۸,۶,۱۱۱	۱۹۲,۱۶۸,۷,۹

جدول (۴): یک سناریو حمله با سطح تأثیر پایین

مرحله	آدرس مهاجم	آدرس قربانی
۱	۹,۵,۲۱,۷۲	۱۹۲,۱۶۸,۱,۳
۲	۲۲۷,۲۲,۲۰۲,۱۴	۱۹۲,۱۶۸,۱,۳
۳	۱۷۸,۸۷,۴۶,۹۱	۱۹۲,۱۶۸,۱,۳
۴	۱۹۲,۱۶۸,۱,۳	۱۹۲,۱۶۸,۲,۶
۵	۱۹۲,۱۶۸,۱,۳	۱۹۲,۱۶۸,۲,۶
۶	۱۹۲,۱۶۸,۱,۳	۱۹۲,۱۶۸,۲,۹
۷	۱۹۲,۱۶۸,۲,۹	۱۹۲,۱۶۸,۴,۳۵
۸	۱۹۲,۱۶۸,۲,۹	۱۹۲,۱۶۸,۴,۱۶
۹	۱۹۲,۱۶۸,۲,۹	۱۹۲,۱۶۸,۲,۲
۱۰	۱۹۲,۱۶۸,۲,۲	۱۹۲,۱۶۸,۵,۵
۱۱	۱۹۲,۱۶۸,۲,۲	۱۹۲,۱۶۸,۴,۴۰
۱۲	۱۹۲,۱۶۸,۴,۴۰	۱۹۲,۱۶۸,۶,۵
۱۳	۱۹۲,۱۶۸,۲,۲	۱۹۲,۱۶۸,۳,۱۷
۱۴	۱۹۲,۱۶۸,۶,۵	۱۹۲,۱۶۸,۷,۹

۴-۱- مقایسه الگوریتم پیشنهادی با روش قبلی در [۱]

الگوریتم ارائه‌شده برای تعیین هدف بعدی موردحمله آزمایش شده است. منظور از تجسم پیش‌بینی اتفاقات آینده به معنی واقعی کلمه نیست، بلکه منظور از پیش‌بینی، ایجاد یک فهرست رتبه‌بندی شده برای تحلیلگر است تا بداند هر دارایی موجود در

1- High-efficient attack
2- Low-efficient attack

سازمان، به چه اندازه امکان دارد مورد حمله قرار گیرد تا با توجه به مأموریت‌های سازمان یا به‌طورکلی دانش ما بتواند، بهترین تحلیل را در اختیار تصمیم‌سازان قرار دهد، و به‌نوعی هدف، پیش‌بینی به‌صورت سامانمند و فهرست‌وار است. بنابراین، برای بررسی کارایی الگوریتم باید درصد احتمال به‌دست‌آمده را یک مرحله قبل از حمله بررسی کنیم [۱]. بدیهی است که نمی‌توان یک امتیاز مشخص و دقیق برای تجسم به‌دست آورد، بنابراین، در این پژوهش نیز همانند تمام پژوهش‌های مشابه در این حوزه از بازه‌ای که یک کران بالا[1] و یک کران پایین[2] دارد برای نشان دادن محدوده رتبه تخصیص‌داده شده به اهدافی که امتیاز یکسانی باهدف موردحمله دارند، استفاده کرده‌ایم. نتایج الگوریتم ترکیب قابلیت و فرصت ارائه‌شده در [۱] و الگوریتم استفاده‌شده در این پژوهش در جدول (۵) آمده است.

جدول (۵): مقایسه عملکرد الگوریتم موجود در [۱] و الگوریتم یافته تحقیق

روش ترکیب	سناریو انتخابی		
	حمله با سطح تأثیر پایین	حمله با سطح تأثیر متوسط	حمله با سطح تأثیر بالا
الگوریتم استفاده‌شده در [۱]	[۵۴٪ , ۷۴٪]	[۵۵٪ , ۷۷٪]	[۵۹٪ , ۷۹٪]
الگوریتم یافته تحقیق	[۶۳٪ , ۷۹٪]	[۶۱٪ , ۸۳٪]	[۶۵٪ , ۸۰٪]

همان‌طور که مشاهده می‌کنید، عملکرد متوسط الگوریتم یافته تحقیق بهتر از الگوریتم ترکیب در [۱] است. چراکه الگوریتم یافته تحقیق علاوه بر این‌که کران بالا و کران پایین را افزایش داده است، فاصله میان آن‌ها را نیز کاهش داده است که موجب افزایش میزان اطمینان به آن می‌شود که این امر دو دلیل دارد:

اول این‌که، خسارت وارده به هر سرویس با قابلیت مهاجم برای کنترل آن نسبتی مستقیم دارد، و روش یافته تحقیق به این نسبت وزن بیشتری در محاسبه تخمین امتیاز قابلیت می‌دهد. دلیل این مدعا این است که بعضی سرویس‌های از یک نوع، روی ماشین‌های مختلف به شکل متفاوتی پیکربندی شده‌اند. این مسئله در حمله با سطح تأثیر پایین که گام‌های بیشتری نسبت به حمله با سطح تأثیر بالا دارد، و درنتیجه افزونگی پیکربندی آن بیشتر است، نمود بیشتری پیدا می‌کند. توجه شود که بازه به‌دست‌آمده برای هر تجسم، محدوده رتبه‌بندی برای اهدافی است که به آن‌ها حمله شده است و همگی ماشین‌های میزبان هستند. در حقیقت، رتبه اختصاص‌یافته به ارزیابی قابلیت برای انواع سرویس‌ها در الگوریتم استفاده‌شده در [۱] که مبتنی بر توزیع نرمال و محدوده اطمینان حاصل از خطای استاندارد نمونه‌برداری است، عملکرد خوب این الگوریتم در تخمین قابلیت تنها را نشان می‌دهد. به‌طورکلی الگوریتم استفاده‌شده در [۱] برای تخمین قابلیت به ازای تمام داده‌های موجود دادگان به‌طور میانگین محدوده رتبه‌بندی [۷۷٪ , ۸۳٪] را کسب کرده است که نشان می‌دهد این روش نگاشت تخمین قابلیت سرویس‌ها به تخمین قابلیت ماشین‌های هدف را به‌خوبی انجام نمی‌دهد. این در حالی است که چون روش یافته تحقیق از مدل انتقال باور برای تخمین امتیاز قابلیت و تخمین امتیاز خسارت برای هر سرویس استفاده می‌کند، و از امتیاز خسارت برای تعیین امتیاز قابلیت استفاده کرده است، نگاشت تخمین امتیاز قابلیت سرویس‌ها به تخمین امتیاز ماشین‌های هدف را بهتر انجام می‌دهد.

دومین دلیل این است که با پیشرفت حمله، کران بالای تخمین فرصت در هر دو روش بالا می‌ماند، اما در الگوریتم استفاده‌شده در [۱] کران پایین آن مرتباً کاهش پیدا می‌کند. دلیل این امر این است که با در نظر گرفتن n تعداد کل ماشین‌های موجود در شبکه، m تعداد ماشین‌هایی که در کنترل مهاجم قرار دارند، و k تعداد ماشین‌های هدفی که می‌توان از ماشین‌های به کنترل درآمده به آن دسترسی پیدا کرد، چنانچه تمام این اهداف بالقوه به یک میزان رتبه‌بندی شده باشد، محدوده رتبه‌بندی ارزیابی امتیاز فرصت بین $100\% \times {(n-m-k)}/{(n-m)}$ و ۱۰۰٪ خواهد بود. بدیهی است که با پیشرفت هرچه بیشتر حمله، اهداف بیشتری در کنترل مهاجم قرار می‌گیرد؛ یعنی m افزایش پیدا می‌کند، و همچنین اهداف بالقوه بیشتری برای او مشخص خواهند شد؛ یعنی k افزایش پیدا می‌کند، که منتج به کران پایین کمتری می‌شود. این در حالی است که در الگوریتم تخمین فرصت یافته تحقیق، قانونی را اضافه کرده‌ایم که چنانچه تمام امتیاز فرصت پیش‌آمده در مسیر بین مبدأ تحت کنترل مهاجم و مقصد بالقوه آن پایین باشد، بیشترین میزان آن را انتخاب می‌کنیم تا حاصل ترکیب آن‌ها حداقل برابر با بدترین حالت باشد.

در هر دو روش، در حمله با اثربخشی متوسط، فاصله کران بالای رتبه‌بندی تا کران پایین آن نسبت به دو حمله با اثربخشی پایین بیشتر است. دلیل آن را می‌توان پیچیدگی در تعیین مراحل حمله با اثربخشی متوسط دانست که در حال حاضر یک میانگین ساده بین اثربخشی پایین و اثربخشی بالا است. این در حالی است که تعداد مراحل حمله با اثربخشی متوسط می‌توانست میانگین وزنی حملات با اثربخشی پایین و بالا بر اساس تعداد آن‌ها یا حتی ترکیبی بر اساس مدل انتقال باور میان آن‌ها باشد.

1- Upper bound
2- Lower bound

۴-۲- شبیه‌سازی حمله با پارامتر مخفیانگی

علاوه بر سناریوهای مقایسه شده در بالا، یک سناریوی حمله با پارامتر مخفیانگی[1] نیز پیاده‌سازی شده است. مخفی بودن یک حمله نشان‌دهنده این موضوع است که مهاجم در مسیر رسیدن به قربانی ممکن است از چند میزبان میانی نیز استفاده کرده باشد، اما فعالیت‌های منجر به بهره‌برداری از این میزبان‌ها کشف نشده‌اند [۱]. به علت عدم وجود نتایج پیاده‌سازی این سناریو در [۱] نمی‌توان مقایسه‌ای در خصوص آن انجام داد، اما نتایج شبیه‌سازی آن با الگوریتم پیشنهادی در این پژوهش را آورده‌ایم. این سناریو در جدول‌های (۶) و (۷) شرح داده شده است:

جدول (۶): یک سناریو حمله با پارامتر مخفیانگی (آدرس‌ها)

مرحله	آدرس مهاجم	آدرس قربانی	سرویس/پروتکل
۱	۹,۵,۲۳۱,۷۲	۱۹۲,۱۶۸,۱,۳	tcp/۲۳
۲	۲۲۷,۲۲,۲۰۲,۱۴	۱۹۲,۱۶۸,۱,۴	icmp/۴۵۶
۳	۱۹۲,۱۶۸,۱,۳	۱۹۲,۱۶۸,۲,۷	tcp/۲۲
۴	۱۹۲,۱۶۸,۲,۹	۱۹۲,۱۶۸,۴,۲۰	tcp/۲۲
۵	۱۹۲,۱۶۸,۴,۲۰	۱۹۲,۱۶۸,۶,۱۱۳	tcp/۲۱
۶	۱۹۲,۱۶۸,۶,۱۱۳	۱۹۲,۱۶۸,۷,۹	tcp/۸۰

جدول (۷): یک سناریو حمله با پارامتر مخفیانگی (جزئیات حمله)

مرحله	توضیحات حمله	اثر در فضای حالت مهاجم	اثر در فضای حالت عملیاتی
۱	TELNET BSD telnet exploit response	Attempted	Operational
۲	ICMP PING Microsoft Windows	Discovered	Operational
۳	SCAN SSH Version map attempt	Discovered	Maintenance
۴	SCAN SSH Version map attempt	Discovered	Maintenance
۵	WEB-MISC /home/ftp access	Partially Compromised	Degraded
۶	WEB-IIS .asa HTTP header buffer overflow	Compromised	Non-operational

همان‌طور که مشاهده می‌کنید، پس از مرحله دوم در این سناریو، حمله یا حملاتی صورت گرفته است که منجر به کنترل میزبان با آدرس ۱۹۲,۱۶۸,۱,۳ شده است اما در این رد حمله ثبت نشده است. در واقع آن‌ها مراحلی مخفی هستند. این مسئله پس از مرحله سه و در مورد آدرس ۱۹۲,۱۶۸,۲,۹ که در مرحله چهار با آن حمله صورت گرفته است، نیز دیده می‌شود. اما پس از مرحله چهار دیگر هیچ مرحله‌ای مخفی نیست.

نتایج الگوریتم پیشنهادی برای این سناریو حمله در جدول (۸) آمده است

جدول (۸): عملکرد الگوریتم پیشنهادی در سناریوی حمله با پارامتر مخفیانگی

نوع امتیاز	مؤلفه‌های تجسم		
	قابلیت	فرصت	ترکیب قابلیت با استفاده از تخمین خسارت و فرصت
امتیاز تجسم	۰/۸۳	۰/۷۶	-
امتیاز اطمینان	۰/۹۱	۰/۸۷	-
محدوده رتبه‌بندی	-	-	[۷۳٪ , ٪۹۲]

همان‌طور که مشاهده می‌کنید، در نتایج به‌دست‌آمده برای حمله با پارامتر مخفیانگی نیز صحت ادعای قبلی اثبات شده است، و فاصله کران بالا و کران پایین در امتیاز رتبه‌بندی کلی الگوریتم پیشنهادی در این سناریو، نیز فاصله قابل‌اطمینانی است. به علت این‌که از تخمین خسارت در تخمین قابلیت استفاده کرده‌ایم، امتیاز اطمینان به این مؤلفه، میزان بالایی است. همچنین همان‌طور که ارائه شد، در حالتی که امتیاز تجسم و اطمینان فرصت کمتر از ۰/۵ باشد، بیشترین مقدار را محاسبه می‌کنیم، و به همین علت تجسم مؤلفه فرصت نیز امتیازهای قابل قبولی کسب کرده است.

پیش‌بینی می‌شود چنانچه مراحل این حمله بیشتر شود، حتی اگر تعداد مراحل بیشتری مخفی گردد، بازهم این الگوریتم عملکرد قابل قبولی ارائه می‌دهد، چراکه اساس مدل انتقال باور بر پایه عدم قطعیت است. به همین علت است که در حمله با سطح تأثیر پایین و در حمله با پارامتر مخفیانگی الگوریتم پیشنهادی عملکرد قابل قبولی دارد. این در حالی است که در [۱۶]، نشان داده شده است که استفاده از ترکیب فازی با استفاده از مدل مارکوف با طول متغیر، در حمله با سطح تأثیر بالا، عملکرد بهتری دارد و مؤثرتر عمل می‌کند.

۵- نتیجه‌گیری

در این پژوهش، از مدل انتقال باور برای ترکیب دو مؤلفه قابلیت و فرصت مهاجم برای انجام تجسم حملات سایبری استفاده

1- Stealthy attack

گردید، و ملاحظه شد که چگونه می‌توان با بهره‌گیری بیشتر از مدل انتقال باور در مراحل مختلف ادغام، نتایج دقیق‌تری را به دست آورد. مزیت استفاده از مدل انتقال باور در تخمین مؤلفه‌های تجسم این است که تحت تأثیر الگوی حمله قرار نمی‌گیرد، و درنتیجه برای حملاتی که مهاجم با افزایش مراحل حمله یا انجام حملات الکی[1] اصطلاحاً قصد رد گم کردن را دارد (حملات نامتعارف) انتخاب بسیار خوبی است. این در حالی است که در حملاتی که الگوی حمله مشخص‌تر است (حملات متعارف) استفاده از روش‌هایی مثل ترکیب فازی بر اساس مدل مارکوف با طول متغیر یا مدل مارکوف مخفی، نتایج بهتری را رقم می‌زند. بنابراین می‌توان از ترکیب روش ادغام فازی در حملات متعارف و روش ترکیب مؤلفه‌های تجسم بر اساس مدل انتقال باور هنگامی‌که حملات مخفی باشد یا به هر دلیلی دچار انحراف شده باشد برای تجسم نمودن حملات سایبری بهره جست. در این پژوهش الگوریتم پیشنهادی خود را با الگوریتم قبلی ارائه‌شده در مرکز ادغام اطلاعات دانشگاه صنعتی مالک اشتر مقایسه نمودیم. نتیجه این مقایسه، به‌طور متوسط ۷٪ بهبود در عملکرد را نشان می‌دهد.

یکی از کارهای آینده استفاده از باورهای رتبه‌بندی شده در تخمین فرصت است (مشابه روش تخمین خسارت در الگوریتم پیشنهادی). با استفاده از این راه‌کار و افزایش فضای حالت‌ها برای فرصت مثل فضای حالت مبدأ، فضای حالت هدف مورد دسترسی، فضای حالت قوانین دیواره‌های آتش و فضای حالت باز بودن یا بسته بودن سرویس‌ها، می‌توان تخمین دقیق‌تری از فرصت مهاجم صورت داد. همچنین با استفاده از مدل انتقال باور در تعیین حمله با سطح تأثیر متوسط، می‌توان تخمین دقیق‌تری در این نوع حمله داشت.

۶- منابع

[1] A. J. Rashidi, K. Dadashtabar Ahmadi, and F. Samsami Khodad, “Projection of Muli Stage Cyber Attack Based on Transferable Belief Model and Fuzzy Inference,” Journal of Electronical & Cyber Defence, vol. 3, no. 2, Serial No. 10, 2015 (In Persian).

[2] M. R. Endsley, “Design and Evaluation for Situation Awareness Enhancement,” Proceedings of the 32nd Annual Meeting of the Human Factors Society, pp. 97–101, 1998.

[3] J. J. Salerno, M. Sudit, S. J. Yang, G. P. Tadda, I. Kadar, and J. Holsopple, “Issues and Challenges in Higher Level Fusion: Threat/Impact Assessment and Intent Modeling (A Panel Summary),” IEEE Information Fusion (FUSION)13th Conference, July 2010.

[4] D. Fava, S. R. Byers, and S. J. Yang, “Projecting Cyber Attacks through Variable Length Markov Models,” IEEE Transactions on Information Forensics and Security, vol. 3, Issue 3, September 2008.

[5] J. Holsopple, M. Nusinov, D. Liu, H. Du, S. J. Yang, and M. Sudit, “Enhancing Situation Awareness via Automated Situation Assessment,” IEEE Communication Magazine, March 2010.

[6] A. D’Amico, L. Buchanan, and J. Goodall, “Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships between Cyber Assets, Missions, and Users,” fifth International Conference on Information Warfare and Security, 8-9 Apr. 2010.

[7] J. Holsopple and S. J. Yang, “FuSIA: Future Situation and Impact Awareness,” inProceedings of the 11th ISIF/IEEE InternationalConference on Information Fusion, Cologne, Germany, July1-3, 2008.

[8] J. Kipp, L. Grau, K. Prinslow, and D. Smith, “The Human Terrain System: A CORDS for the 21st Century,” Military Review, September 2006.

[9] R. J. Gonzalez, “Human Terrain, Past, Present, and Future Applications,” Anthropology Today, vol. 24, no 1, February 2008.

[10] J. Holsopple, B. Argauer, and S. J. Yang, “Virtual terrain: a common representation of acomputer network,” in Proceedings of SPIE Security and Defense Symposium, Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security Conference, Orlando, FL, March 16-20, 2008.

[11] A. E. Khalili, B. Michalk, L. Gilbert, and L. Alford, “Situational Awareness and mission Risk in computer networks,” Proceedings of SPIE Security and Defense Symposium, Cyber Security, Situation Management, and Impact Assessment II Conference (7709A), Orlando FL, 5-9 April 2010.

[12] E. Bosse, J. Roy, and S. Wark, “Concepts, Models, and Tools for Information Fusion,” Artech House, Inc, ISBN-13: 978-1- 59693-081-0, p. 4, 2007.

[13] A. Steinberg, C. Bowman, and F. White, “Revisions to the JDL Data Fusion Model,” presented at the Joint NATO/IRIS Conference, Quebec, October 1998.

[14] J. Salerno, M. Hinman, and D. Boulware, “A Situation Awareness Model Applied to Multiple Domains,” Proceedings of the Defense and Security Conference, Orlando FL, March 2005.

[15] S. J. Yang, S. Byers, J. Holsopple, B. Argauer, and D. Fava, “Intrusion Activity Projection for Cyber Situational Awareness,” in Proceedings of IEEE International Conferences on Intelligence and Security Informatics, Taipei, Taiwan, June 17-20, 2008.

[16] H. Du, D. F. Liu, J. Holsopple, and S. J Yang, “Toward Ensemble Characterization and Projection of Multistage Cyber Attacks,” IEEE ICCCN, Zürich, Switzerland, August 2-5, pp. 1-8, 2010.

[17] M. R. Grimaila, R. F. Mills, and L. W. Fortson, “An Automated Information Asset Tracking Methodology to Enable Timely Cyber Incident Mission Impact Assessment,” 13th International Command and Control Research and Technology Symposia (ICCRTS 2008), Seattle, WA, 17-19 Jun, 2008.

Projection of Cyber Attacks using Damage Estimation and Combination of Attacker's Capability and Opportunity based on Transferable Belief Model

A. J. Rashidi*, M. Jafari, K. Dadashtabr Ahmadi

Malek-Ashtar University of Technology
(Received: 27/08/2017, Accepted: 27/05/2018)

ABSTRACT

Nowadays there are so many tools available for capturing the events and alerts within networks. The need for a system that could aggregate the information generated by these tools and combine them to make better decisions is strongly acknowledged. If we could predict cyber attacks and estimate their effects before they actually occur, we would be able to apply a better defense strategy and reduce the damage to our critical assets. The projection of cyber attacks is to predict them based on a certain framework using mathematical methods. One of these methods is the Transferable Belief Model (TBM). In this paper, we used the TBM to combine capability and opportunity of attackers - which are cyber attacks' projection components- to project the future situation of attacks. We have also tested our results against our customized high-level attack tracks dataset. The result of comparison between our algorithm and the previously presented algorithm at the Information Fusion Centre of Malek-Ahstar University of Technology shows an average improvement of 7%.

Keywords: Cyber Attacks Projection, Situation Awareness, Damage Estimation, Capability, Opportunity, Transferable Belief Model

*Corresponding Author Email: rashidi@mut.ac.ir