مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال سوم، شماره ۲، تابستان ۱۳۹۴، ص ۲۸- ۱۳

تجسم حملات سایبری چندمرحله‌ای مبتنی بر مدل انتقال باور و استنتاج فازی

علی‌جبار رشیدی[۱]، کوروش داداش تبار احمدی[۲]، فرید صمصامی خداداد[۳*]

۱- دانشیار، مرکز پژوهشی علوم و فناوری ادغام اطلاعات، دانشگاه صنعتی مالک‌اشتر
۲- دانشجوی دکتری، مرکز پژوهشی علوم و فناوری ادغام اطلاعات، دانشگاه صنعتی مالک‌اشتر
۳- استادیار، دانشکده مهندسی فناوری‌های نوین، دانشگاه تخصصی فناوری‌های نوین آمل
(دریافت: ۹۳/۱۲/۲۹؛ پذیرش: ۹۴/۰۶/۱۰)

چکیده

تحلیلگر امنیتی در یک سامانه آگاهی وضعیتی سایبری براساس میزان باورپذیری که از وضعیت آینده کسب می‌کند می‌تواند مناسب‌ترین تصمیم‌های دفاعی را اتخاذ کند. در این سامانه میزان باورپذیری یک وضعیت از تخمین وضعیتی و ادغام اطلاعات سطح بالا به‌دست می‌آید. در حال حاضر چالشی‌ترین موضوع در ادغام اطلاعات سطح بالا برای دست‌یابی به آگاهی از وضعیت آینده و ارزیابی تاثیر حملات سایبری مدل‌سازی تجسم حملات با چهار مولفه تجسم یعنی رفتار، فرصت، قابلیت و نیت است. عمده طرح‌ها و الگوریتم‌های قبلی در مدل‌سازی تجسم، برای ساده‌سازی در اجرای مدل چهار مولفه فوق را مستقل فرض کرده و عملا از تاثیر مولفه‌ها بر یکدیگر و قدرت ترکیب آنها در تجسم حملات سایبری چندمرحله‌ای صرف‌نظر کرده‌اند؛ اما در این مقاله طرح جدیدی براساس ترکیب فازی مولفه‌های تجسم و مدل انتقال باور ارائه شده است. با این طرح می‌توان اهداف بعدی یک حمله سایبری چندمرحله‌ای را به‌طور موثر تجسم نمود و تخمین مناسبی از باورپذیری آن ارائه داد. این طرح پیشنهادی در نهایت با استفاده از دادگان معتبر، براساس حملات با نویز بالا، حملات مخفی و حملات با تاثیر بالا و پایین مورد ارزیابی قرار گرفته است. نتایج شبیه‌سازی هم با توجه به سناریوهای تعریف‌شده نشان از افزایش میزان دقت با میانگین هفده درصدی در تجسم حملات سایبری چند مرحله‌ای دارد.

واژه‌های کلیدی: آگاهی وضعیتی، دفاع سایبری، انتقال باور، تجسم حملات سایبری

۱- مقدمه

با به‌کارگیری 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. برای ایجاد یک سامانه آگاهی وضعیتی سایبری نیز همان‌گونه که در شکل (۱) نشان داده‌شده است به سه زیرسامانه کلی درک[۱]، فهم[۲] و تجسم[۳] حملات سایبری نیاز است. زیرسامانه درک حملات سایبری، به استخراج نشانه‌ها و درک مفاهیم پرداخته و بدون وجود این زیرسامانه برای استخراج اطلاعات درست، احتمال شکل‌گیری، تصویری نادرست از فضای سایبری تحت فرماندهی و کنترل به‌شدت افزایش می‌یابد. با این زیرسامانه به این سؤال پاسخ داده خواهد شد که واقعیت‌های فعلی فضای سایبری چیست؟ زیرسامانه فهم به یک‌پارچه‌سازی تکه‌های مختلف اطلاعات و تعیین ارتباط میان آن‌ها می‌پردازد. با این زیرسامانه می‌توان دریافت که چه چیزی پیرامون فضای فرماندهی و کنترل سایبری رخ می‌دهد؟

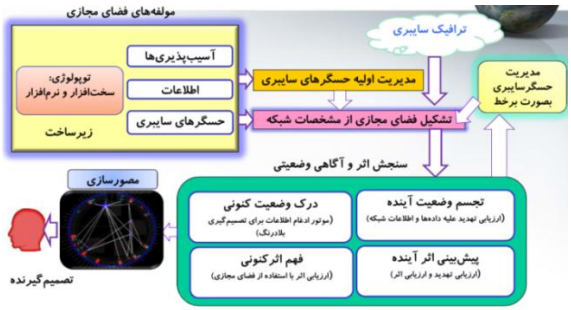
در زیرسامانه تجسم حملات سایبری که منجر به بالاترین سطح از آگاهی وضعیتی خواهد شد، به مسئله آینده‌نگری رویدادهای مربوط به هر وضعیت پرداخته خواهد شد. این توانایی در تجسم رویدادهای آتی بر اساس رویدادهای پویای جاری، موجب تصمیم‌گیری به‌موقع فرماندهان درصحنه نبرد سایبری خواهد شد [۱].

گرچه دو اصطلاح «تجسم» و «پیش‌بینی[۴]» در بسیاری از منابع تحقیقی یکسان فرض شده‌اند اما باید توجه داشت که تعریف تجسم با پیش‌بینی متفاوت است. ازلحاظ تئوری، پیش‌بینی حدس‌هایی است که مشخص می‌کند در آینده چه اتفاقی خواهد افتاد، درحالی‌که تجسم صرفاً چیزهایی که در آینده اتفاق خواهد افتاد را مشخص می‌کند [۲]. به بیان ساده‌تر، پیش‌بینی‌به حدس‌هایی گفته می‌شود که با احتمالات متفاوتی درآینده رخ خواهند داد یعنی پیش‌بینی، فرایند برآورد موقعیت‌های ناشناخته است. پیش‌بینی درواقع یک پیش‌گویی از رویدادهای آینده در اختیار می‌گذارد ولی تجسم، زیرمجموعه‌ای‌از مجموعه پیش‌بینی‌ها است که در آینده به احتمال‌زیاد اتفاق خواهند افتاد. این تمایز مهم است چون تعیین آینده‌ای دقیق، همیشه با توجه

* رایانامه نویسنده مسئول: samsami.farid@gmail.com

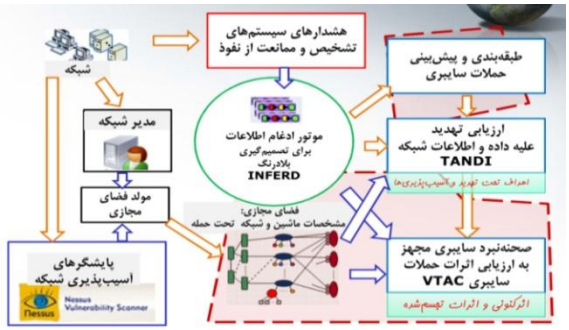
1- Perception
2- Comprehension
3- Projection
4- Prediction

به رخداد تصادفی یا دانش از دست‌رفته، مشخص نیست.



شکل (۱). سامانه آگاهی وضعیتی سایبری[۲]

تجسم به تحلیلگر اجازه می‌دهد تا به شرایط احتمالی آینده نگاه کند، پیش از آن‌که به آینده محتمل مراجعه کند و برای نتایج مختلف آماده شود. بنابراین با استفاده از تجسم صحنه نبرد سایبری و پیش‌بینی حملات سایبری، می‌توان الگوهای خاص هر حمله در سامانه را پیش‌بینی و آسیب‌پذیری‌های شبکه که برای مهاجمان جذاب هستند را تجزیه‌وتحلیل نمود. همچنین با استفاده از این سامانه می‌توان حملات سایبری چندمرحله‌ای و هماهنگ را ردگیری و تجسمی از وضعیت آینده این نوع حملات ارائه داد. همان‌گونه که در شکل (۲) آمده است با استفاده از سامانه صحنه نبرد سایبری مجهز شده به ارزیابی اثرات حملات سایبری می‌توان حملات را به اجرا گذاشت و با به تصویر کشیدن وضعیت فعلی صحنه نبرد سایبری و نمایش امتیازات اثرات تهدیدهای مختلف برای میزبان‌ها، سرویس‌ها، کاربران و کل شبکه، به تحلیلگران در امکان داشتن درک و نظارت بهتر بر وضعیت فعلی و آینده کمک نمود [۳].



شکل (۲). فرایند دستیابی به تجسم حملات سایبری[۱]

با توصیف مقدماتی بالا می‌توان گفت سامانه تجسم حملات به تجزیه‌وتحلیل هشدارهای همبسته شده، مربوط به حملات چندمرحله‌ای می‌پردازد و بر اساس آن اهداف بالقوه تحت خطر در یک شبکه را پیش‌بینی می‌کند. از چالش‌های مهم این سامانه استخراج مدلی برای چگونگی پیشرفت حرکتی حملات سایبری است. چراکه با توجه به پیچیدگی، عدم قطعیت و ماهیت توزیع‌پذیری شبکه‌ها و سامانه‌ها امکان اختلال در مدل‌سازی فوق وجود دارد. برای حل این مسئله در تجسم حملات سایبری از مؤلفه‌هایی چون نیت، قابلیت، فرصت و رفتار برای مدل‌سازی استفاده می‌شود. درحالی‌که کارهای قبلی برای مدل‌سازی، مؤلفه‌های مذکور را مستقل نموده‌اند؛ ما در این مقاله از ترکیب مؤلفه‌ها برای مدل‌سازی تجسم حملات سایبری استفاده می‌کنیم.

۲- کارهای مرتبط

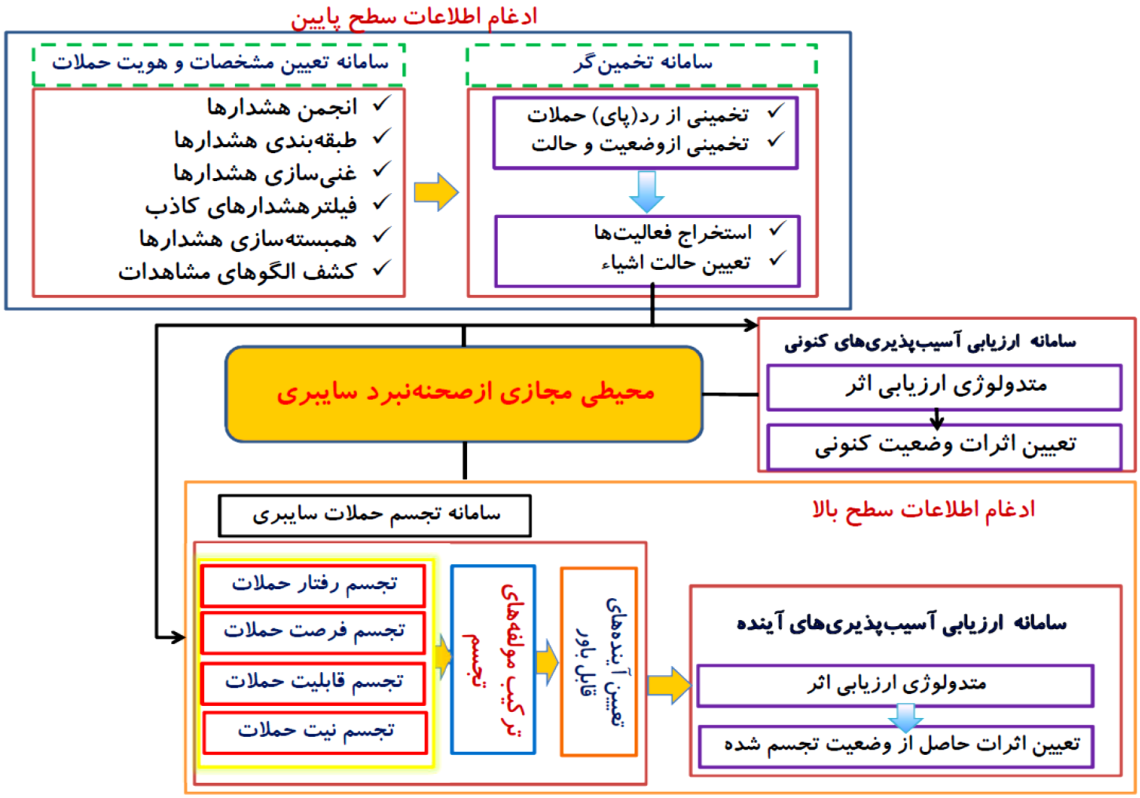
به‌طورکلی روش‌های مرسومی که در تجسم حملات استفاده می‌شود را می‌توان به چهار دسته تدوین الگوهایی برای تعیین سلسله اعمال دشمن (ازجمله گراف‌های حمله، الگوهای حمله)، فنون یادگیری ماشین و داده‌کاوی، تئوری بازی‌ها و زنجیره‌های مارکوف تقسیم‌بندی کرد. البته ممکن است از ترکیبی از این دسته‌ها نیز استفاده شود.

لی و همکاران [۴] در سال ۲۰۰۷ از الگوریتم همبسته‌ساز مبتنی بر آمار برای پیش‌بینی استراتژی‌های یک حمله جدید استفاده کرده‌اند. در این الگوریتم از همبسته‌سازی هشدار مکمل به نام‌های همبسته‌سازی مبتنی بر استنتاج بیزین و همبسته‌سازی مبتنی بر GCT استفاده شده بود. در این روش سناریوهای حمله با استفاده گراف‌های همبسته‌شده ایجاد می‌شوند. البته از این الگوریتم نمی‌توان برای تجسم حملات ترکیبی استفاده نمود چرا که با مثبت ناصحیح بالایی روبه‌رو است. وو و همکاران [۵] در سال ۲۰۱۲ برای پیش‌بینی حملات سایبری از شبکه بیزین استفاده نمودند. در این مدل علاوه بر آسیب‌پذیری‌ها در شبکه که به‌وسیله گراف حمله در نظر گرفته می‌شوند، سه عامل محیطی وضعیت شبکه، ارزش دارایی‌های شبکه و تاریخ حمله به شبکه نیز لحاظ شده است. بعد از ترکیب این عامل‌ها با گراف حمله، الگوریتم احتمالی بیزین میزان احتمال حمله هر گراف را تعیین می‌کند. لی و همکاران [۶] در سال ۲۰۰۴ از یک مدل تجسم حمله مبتنی بر شبکه بیزین به تعیین فعالیت‌های یک حمله پرداختند. در این روش‌ها پیچیدگی در توسعه و نگهداری مدل‌های مسیر حمله، چالش مهمی است چرا که روش‌های حمله، نیت‌ها و تنظیمات شبکه‌ای مرتباً تغییر می‌کنند. در بخش ارزیابی تأثیرات حملات سایبری، لیندگویست و جانسون[1] [۷] در سال ۱۹۹۷، به همراه گروه مهندسی کامپیوتر در دانشگاه فناوری چارلمز در سوئد، به تعیین ارتباط بین حمله و اثر حمله پرداختند. در این تحقیق، آن‌ها از طبقه‌بندی‌های فن حمله استفاده کردند که در اصل توسط نیومن و پارکر[2] [۸] معرفی‌شده بود. ویدالیس و جانز[3] [۹] برای

1- Lindqvist & Jonsson
2- Neuman & Parker
3- Vidalis & Jones

تعیین انواع حملاتی که یک مهاجم می‌تواند برای رسیدن به هدف انجام دهد، استفاده از نمودار درختی آسیب‌پذیری را پیشنهاد دادند. مدل آن‌ها به یک نمودار درختی جداگانه به‌ازای هر هدف نیاز دارد. فیلیپس و اسوایلر[1] [۱۰] برای مدل‌سازی آسیب‌پذیری‌ها به‌منظور تجزیه‌وتحلیل خطر، استفاده از شبکهٔ بیزین را پیشنهاد دادند و از «ارزیابی اثر» استفاده نموده‌اند. ویگنا و والر[2] و کروج و کمرر[3] [۱۱] از تجزیه و تحلیل اثر برای «تعیین اثرات حملات آشکارشده بر روی عملکرد شبکهٔ تحت نظارت و اجزایی که هدف فعالیت‌های مخرب قرارگرفته‌اند» استفاده می‌کنند. فونگ، پوراس و والدز[4] [۱۲] از یک الگوریتم همبسته‌سازی با رویکردی مبتنی بر مأموریت و اثر که از اولویت‌بندی و تراکم هشدارها برخوردار بود، استفاده نمودند آن‌ها با توجه به همبندی و مأموریت شبکه به رتبه‌بندی و ادغام هشدارهای ورودی بر اساس درجهٔ تهدیدی که شبکه را در معرض آن قرار می‌دهند، پرداختند. آرگور[5] با ایجاد یک محیط مجازی از صحنه نبرد سایبری به ارزیابی تأثیر و تجسم حملات سایبری پرداخت. در الگوریتم ارزیابی تأثیر فوق، از یک مدل فضای مجازی مبتنی بر گراف و ترکیب ارزیابی‌های تأثیر از آسیب ناشی از حملات استفاده شده است [۱۳]. چی‌ین و همکاران [۱۴] در سال ۲۰۱۲ چارچوبی را برای تجسم تهدیدات با استفاده از استخراج الگوهای خاص حمله ارائه نمودند. در این کار یک متدولوژی فرمال نیز برای تولید سناریوهای حمله ارائه شده است. هالسوپل و همکاران [۱۵] در سال ۲۰۰۶ نیز مدلی را برای پیش‌بینی حملات ارائه کردند. پیشنهاد این افراد برای ساده‌سازی در مدل‌سازی جدا کردن مدل‌سازی تنظیمات شبکه و روش‌های حمله‌ای سایبری است. در این کار نیز از گراف‌های حمله استفاده می‌شود. ارزیابی‌ها در هر یک به‌صورت جداگانه انجام‌شده و نتایج درنهایت با همدیگر ترکیب‌شده و هدف محتمل برای حمله آینده شناسایی می‌شود. روش‌های توسعه الگوهای سلسله اعمال دشمن که بر رفتارهای گذشته حمله‌کننده تمرکز دارند زمانی خوب کار می‌کنند که الگوها به‌درستی تعریف‌شده باشند و گاهی اوقات نیاز به یادگیری خودکار هم در این روش‌ها وجود دارد. دسته‌ای دیگر از روش‌ها بر استفاده از قواعد یادگیری ماشین و داده‌کاوی برای پیش‌بینی رفتارهای آینده تمرکز کرده‌اند. این روش‌ها مبتنی بر استخراج اطلاعات مفید و الگوها از مجموعه داده‌های زیاد بوده و دارای پیچیدگی محاسباتی بالایی نیز هستند. کیپریانو و همکاران [۱۶] در سال ۲۰۱۱ روش جدیدی را برای پیش‌بینی رفتارهای مهاجمین ارائه کردند. در این روش از قواعد یادگیری ماشین برای یادگیری رفتارهای گذشته مهاجمین استفاده‌شده که درنهایت از این اطلاعات برای تخمین رفتارهای آینده مهاجمین استفاده می‌کنند. ژی تانگ لی [۱۷] در سال ۲۰۰۷ از روش‌های داده‌کاوی برای تولید گراف‌های داده استفاده کردند. این الگوریتم برای هر دنباله حمله یک درجه پیش‌بینی محاسبه می‌کند. این درجه‌بندی‌ها درنهایت به پیش‌بینی محتمل‌ترین نتیجه آینده یاری می‌رساند. تئوری بازی‌ها نیز از روش‌هایی است که می‌تواند به پیش‌بینی رفتارهای آینده مهاجم یاری برساند. لیو و همکاران [۱۸] در سال ۲۰۰۵ یک مدل تئوری بازی مبتنی بر تشویق را برای استنتاج نیت، اهداف و استراتژی‌های مهاجم ارائه کرده‌اند. در این کار تحقیقاتی این نکته بیان‌شده است که انتخاب بهترین مدل بازی، به درجه دقت سیستم تشخیص نفوذ و درجه همبسته‌سازی گام‌های حمله وابسته است. در این کار یک متدولوژی برای مدل کردن تعاملات بین یک مهاجم DDoS و مدیر شبکه ارائه شده است. تانگ و همکاران [۱۹] در سال ۲۰۱۱ الگوریتمی را برای آگاهی وضعیتی تهدید نفوذکننده ارائه کرده‌اند. این الگویتم مبتنی بر تئوری بازی و ادغام اطلاعات است. در این مقاله از یک ساختار شبکه بیزین پویا و استنتاج دقیق برای کسب و ادغام اطلاعات رفتاری مربوط به نفوذگر استفاده می‌کنند. سرانجام پیش‌بینی رفتار آینده نفوذگر با استفاده از محاسبات موازنه پاسخ کوانتومی انجام می‌شود. درنهایت دسته چهارم روش‌ها بر استفاده از زنجیره‌های مارکوف تأکید دارند. گاوو و همکاران [۲۰] در سال ۲۰۰۳ از مدل‌های مارکوف مخفی برای پیش‌بینی حملات در لایه کاربرد استفاده کرده‌اند. مان و همکاران [۲۱] در سال ۲۰۱۰ از ARMA (که یک روش پیش‌بینی سری زمانی است) و مدل مارکوف برای پیش‌بینی وضعیت‌های امنیتی شبکه استفاده کردند. نتایج پیش‌بینی حاصل از دو مدل با مقادیر وزنی مناسبی باهم ترکیب می‌شوند تا پیش‌بینی دقیق‌تری به‌دست آید. یانگ[6] و همکاران در ۲۰۰۹ [۲۲] در حوزه حملات سایبری، روشی را برای ردگیری بلادرنگ و تجسم حملات آینده ارائه کردند. روش آن‌ها برای ردگیری و تجسم اعمال حملات سایبری، یک نوع مکانیسم پویش‌گرایانه[7] است. در [۲۳] فاوا[8] با استفاده از مدل مارکوف با طول متغیر[9] اقدام به استخراج الگوهای متوالی از ویژگی‌های مختلف و تجسم هشدارهای مرتبط با حملات چندمرحله‌ای نمود. هولسوپ در [۲۴] ضرورت تجسم آینده حملات سایبری را مطرح کرده و به معرفی کارایی ادغام اطلاعات سطح بالا پرداخته است. هولسوپ با ترکیب مستقل قابلیت و فرصت، نیت مهاجم را به‌دست آورده است.

1- Philips & Swiler
2- Vigna &Valeur
3- Kruege & Kemmerer
4- Fong & Porras & Valdes
5- B.Argauer
6- Yang
7- Proactive
8- Fava
9- Variable Length Markov Models



شکل (۳). معماری پیشنهادی برای تجسم حملات سایبری [یافته تحقیق]

۳- معماری پیشنهادی برای تجسم حملات سایبری

معماری آگاهی از وضعیت آینده و ارزیابی اثر شکل (۳) از سه بخش محیط مجازی از صحنه نبرد سایبری، ادغام اطلاعات سطح بالا و سطح پائین تشکیل‌شده و شامل چهار سامانه هویت سنج، تخمین‌گر، تجسم و ارزیابی میزان آسیب‌پذیری است. در معماری فوق رد حمله[1] بر اساس گروهی از مشاهدات همبسته‌شده در محیط تحت نظارت ایجاد می‌شود. که هسته اصلی شکل‌گیری آن موتور ادغام اطلاعات برای تصمیم‌گیری بلادرنگ در ادغام اطلاعات سطح پایین است. همچنین در این معماری سامانه تخمین‌گر وضعیت سیستم را در قالب مجموعه‌هایی از فعالیت‌ها و اشیاء مدل می‌کند و سامانه تجسم، آینده‌های محتمل را شناسایی می‌کند. سامانه ارزیابی نیز میزان آسیب‌پذیری را با استفاده از الگوریتم‌های ارزیابی اثر محاسبه و به بررسی اثرات ناشی از وقوع هرکدام از وضعیت‌های آینده می‌پردازد. خروجی این معماری برآوردی از وضعیت کنونی، اثرات وضعیت کنونی و اثرات وضعیت‌های قابل‌باور آینده است. اثرات آینده از محاسبه اثر وضعیت‌های محتمل آینده به‌دست می‌آید. آینده‌های قابل‌باور نیز توسط الگوریتم‌های ارزیابی اثر تحلیل می‌شوند که درنهایت خروجی این الگوریتم‌ها تعیین اثرات آینده است. یکی از وظایف این معماری محاسبه باورپذیری آینده‌ها بر اساس مدل مفهومی است که این مدل از روابط میان اشیاء و فعالیت‌ها در محیط مجازی از صحنه نبرد سایبری به‌دست می‌آید.

۳-۱- ادغام اطلاعات سطح پائین

در معماری پیشنهادی از ادغام اطلاعات سطح پایین برای تشخیص، تعیین و تخمین وضعیتی حملات سایبری استفاده خواهد شد. در این سطح ابزارهای حسگری مختلفی از سیستم تشخیص نفوذ قرار دارند که مسئول شناسایی اشیا محیط هستند. علاوه‌براین موجودیت‌ها (شامل اشیا و مفاهیم)، اشیاء (شامل مأموریت‌ها، میزبان‌ها و سرویس‌ها)، مفاهیم، رویدادها (هر چیزی که در یک‌زمان و مکان معین اتفاق می‌افتد)، گروه‌ها (تعدادی از چیزها که باهم در ارتباط‌اند) و فعالیت‌ها (هر چیزی که به آن عمل یا حرکت گفته می‌شود) در این سطح مشخص می‌شوند. در ادغام اطلاعات سطح پائین به دنبال فهم «ما» و هر آنچه برای ما مهم است، هستیم. ازجمله این موارد می‌توان به منابع ما (منظور قابلیت‌ها و ظرفیت‌ها)، هر آنچه برای ما مهم است و هر آنچه به‌عنوان آسیب‌پذیری‌های ما مطرح است، اشاره کرد. در حقیقت در این سطح به دنبال فهم از وضعیت جاری محیط هستیم تا بتوان با توجه به دانش کسب‌شده، میزان درجه اهمیت هر یک از فعالیت‌های داخل وضعیت را مشخص کرد. در

1- Attack track

این نوع ادغام اطلاعات که متشکل از مشاهدات همبسته شده، طبقه‌بندی‌شده، غنی‌شده و ادغام‌شده است، هدف ایجاد مدلی است که نشان‌دهنده وضعیت و برآوردی از وضعیت باشد. لازمه مدل کردن وضعیت نیز شناسایی عناصر تشکیل‌دهنده وضعیت است که در این کار از محیط، اشیاء موردعلاقه، فعالیت و حالت اشیاء برای مدل‌سازی استفاده شده است.

- محیط[1]: منظور از محیط تنها موجودیت‌ها و روابط ملموس نیست؛ بلکه شامل موجودیت‌های غیرقابل ملموس نظیر آسیب‌پذیری‌ها نیز است. در فضای سایبری برای مدل‌سازی محیط از محیط مجازی صحنه نبرد سایبری[2] [۲۵] استفاده می‌کنند.
- اشیا مورد علاقه[3]: عناصر و موجودیت‌هایی در محیط که حفاظت از آن برای تحلیل‌گر دارای اهمیت است؛ اشیاء مورد علاقه نامیده می‌شود.
- فعالیت[4]: اقداماتی که به‌منظور تأثیرگذاری بر روی محیط انجام می‌شود، تحت عنوان «فعالیت» شناخته می‌شوند.
- حالت اشیا[5]: با توجه به حوزه کاربرد، حالات اشیا در حوزه‌های مختلف با یکدیگر متفاوت‌اند. درواقع حالت اشیاء تابعی از سه مورد بالا است. در فضای سایبری این حالات ممکن است، معمولی، مورد حمله قرارگرفته، آشکارشده، به‌طور جزئی مورد سوء استفاده قرارگرفته و مورد سوء استفاده قرارگرفته، باشند.

۳-۲- محیط مجازی از صحنه نبرد سایبری

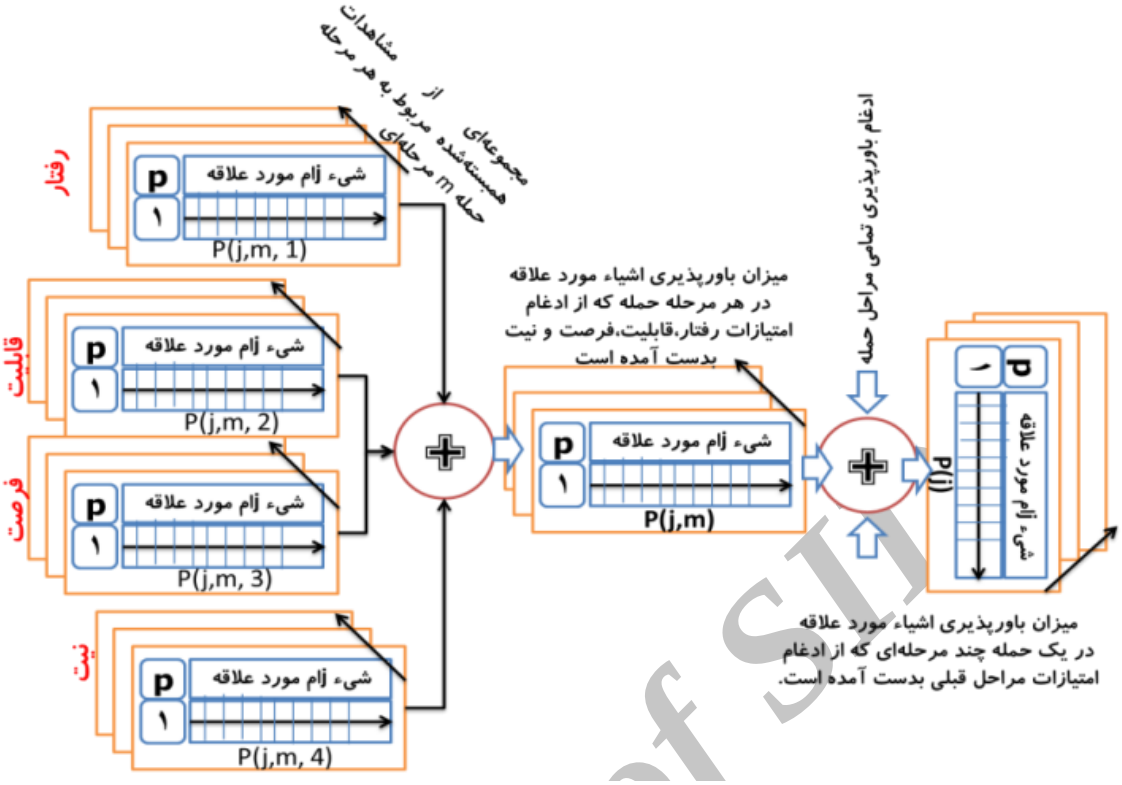
در محیط مجازی صحنه نبرد سایبری می‌توان به مدل‌سازی فضای سایبری برای اجرای مانورهای حملات سایبری پرداخت. صحنه نبرد سایبری نمایش عمومی از اطلاعات حساس در مورد آسیب‌پذیری‌ها، میزان در دسترس بودن اجزاء و میزان حساسیت محیط است و مسیرهای یک حمله در آن نشانگر سوءاستفاده‌های بالقوه از آسیب‌پذیری‌ها است. در این محیط مجازی موجودیت‌ها و روابط بین آن‌ها پردازش و مدل می‌شود. مدل فوق حاوی اطلاعات ضروری برای تشخیص رویدادهای سایبری در صحنه نبرد است و می‌توان آن را به‌عنوان مهم‌ترین و پیچیده‌ترین عامل تأثیرگذار در ادغام اطلاعات سطح بالا دانست.

۳-۳- ادغام اطلاعات سطح بالا

ادغام اطلاعات سطح بالا، به تجسم وضعیت جاری در آینده می‌پردازد. این سطح ادغام با توجه به «دانش ما» که از ادغام اطلاعات سطح پائین، حاصل‌شده کار خود را آغاز می‌کند و برخلاف سطح پائین، کسب «دانش از آن‌ها» مهم است. در این سطح درنهایت پیش‌بینی صرف انجام نخواهد شد بلکه تجسم مسئله اصلی است. به این دلیل که در پیش‌بینی فقط مجموعه حالاتی که بر اساس اطلاعات به‌دست‌آمده احتمال رخ دادن آن‌ها وجود دارد مشخص‌شده است. بنابراین از این مجموعه، حالاتی که با توجه به دانش قبلی، احتمال رخداد آن‌ها «بسیار بیشتر» است، جداشده و اتفاق افتادن آن‌ها تجسم می‌شود. واحد تجسم به تحلیل‌گر اجازه می‌دهد که بتواند از میان وضعیت‌های آینده ممکن، یک آینده باورپذیر را به‌ازای هر وضعیت ایجاد کند. در شکل (۳) می‌توان چارچوب کلی تجسم حملات را مشاهده کرد. مطابق این شکل برای تجسم وضعیت جاری (که از «دانش ما» استفاده می‌کند) به آینده، به «دانش از آن‌ها» نیاز است. این دانش، از تجسم مؤلفه‌های فرصت، قابلیت، نیت و رفتار قابل‌استخراج است. که منظور از تجسم فرصت[6] تجسم امکان فعالیت در محیط سایبری برای فرصت اجرای حمله توسط مهاجم است. همچنین منظور از تجسم قابلیت[7] تجسم آن چیزی است که یک مهاجم سایبری توانایی انجام آن را دارد. منظور از تجسم نیت[8] آن چیزی است که مهاجم برنامه‌ریزی می‌کند تا آن کار را انجام دهد و درنهایت منظور از تجسم رفتار[9]، مطالعه فعالیت‌های گذشته، به‌منظور یافتن الگوهای رفتاری است. بنابراین برای این‌که بتوان با یک تجسم از وضعیت جاری به آینده رسید می‌بایست هر یک از این مؤلفه‌ها، تجسم‌شده و وضعیت آینده با توجه به هر یک از این ویژگی‌ها ارزیابی شود. در شکل (۴) جزئیات بیشتری بر اساس ترکیب مؤلفه‌های تجسم مطابق با معماری توصیفی شکل (۳) به تصویر کشیده شده است که وظیفه اختصاص امتیاز باورپذیری توسط الگوریتم‌های موجود و ادغام این داده‌ها به‌منظور پیش‌بینی آینده را بر عهده دارد. همان‌طور که در شکل (۴) نشان داده‌شده، الگوریتم‌ها، موازی با یکدیگر عمل می‌کنند تا هرکدام یک امتیاز باورپذیری برای وضعیت‌های آینده محاسبه کنند.

این امتیازها برای هر وضعیت با استفاده از نظریه دمپستر شافر با یکدیگر ترکیب می‌شوند. امتیازهای محاسبه‌شده برای هر مرحله حمله بار دیگر باهم ترکیب می‌شوند تا فهرستی از آینده‌های قابل‌باور برای هر شیء در محیط تولید شود. واحد ارزیابی میزان آسیب‌پذیری در ادغام اطلاعات سطح بالا وظیفه تعیین تأثیر مجموعه‌ای از فعالیت‌ها بر موجودیت‌ها در شبکه را بر عهده دارد. در این مدل به هر موجودیت بر اساس الگوریتم ارزیابی خسارت امتیازی بین صفر و یک داده می‌شود.

1- environment
2- virtual terrain
3- object of interest
4- activity
5- state of objects
6- Opportunity
7- Capability
8- Intent
9- Behavior



شکل (۴). تجسم حملات سایبری چندمرحله‌ای مبتنی بر ترکیب مؤلفه‌های تجسم [یافته تحقیق]

برای مدل‌سازی تجسم حملات سایبری چندمرحله‌ای به مشاهدات هر مرحله از حمله، وضعیت محلی L را نسبت‌داده و قاعدتاً کل مراحل حمله، از مجموعه‌ی کلی $G = \{L_1, L_2, \ldots, L_M\}$ تشکیل خواهد شد که در آن M نشان‌دهنده تعداد مراحل حمله است. در معماری پیشنهادی می‌توان چندین حمله نامرتبط را که بر روی شبکه رخ می‌دهد در قالب یک وضعیت مجزا مدل کرد. نکته حائز اهمیت مدل‌سازی در ادغام اطلاعات سطح بالا آن است که الگوریتم‌های محاسبه باورپذیری باید اطلاعات را از این مدل استخراج کنند. علاوه‌براین مدل باید به‌گونه‌ای باشد که اشیاء موردعلاقه‌ی مشخصی را تعریف کند. اشیاء موردعلاقه (J) لیستی از اشیاء درون محیط هستند که به آن‌ها امتیاز باورپذیری تخصیص می‌یابد. اشیاء موردعلاقه در واقع جزئی از دارایی‌های ملموس و غیرملموس سازمان در محیط هستند که حفاظت از آن‌ها برای تحلیل‌گران حائز اهمیت است. رخدادهای آینده بر اساس نمره‌ی باورپذیری اختصاص داده‌شده به هر یک از اشیاء موردعلاقه ($j \in J$) در محیط مجازی صحنه نبرد سایبری پیش‌بینی می‌شوند. این امتیاز عددی در بازه [۰, ۱] بوده و یا مقدار نامشخص دارد. مقادیر نزدیک به صفر نشان‌دهنده احتمال وقوع کم‌تر و مقادیر نزدیک به ۱ نشان‌دهنده احتمال وقوع بیش‌تر در آینده است. امتیاز نامشخص بیان‌گر این مطلب است که هیچ اطلاعاتی در مورد موجودیت موردنظر وجود ندارد و به این دلیل امکان اختصاص امتیاز باورپذیری وجود ندارد و نه این‌که این وضعیت در آینده رخ نخواهد داد. درک تفاوت میان امتیاز ۰ و امتیاز نامشخص ضروری است. آینده قابل‌باور به‌صورت مجموعه‌ای از رخدادها که ناشی از وضعیت جاری می‌باشند، تعریف می‌شود. در تعریف ریاضی، آینده قابل‌باور یک وضعیت نظیر L به‌صورت $F = L\ U\ E$ تعریف می‌شود که در آن E مجموعه‌ای از رخدادهای آینده است. با محاسبه امتیاز باورپذیری نشانه‌هایی از وضعیت مستعدتر برای وقوع در آینده در اختیار تحلیل‌گران قرار می‌گیرد که به‌وسیله آن می‌توانند آمادگی لازم را در برابر وقوع رخدادها کسب کنند. در آگاهی وضعیتی سایبری امکان پیش‌بینی تمام آینده‌ها، ممکن نیست؛ از سوی دیگر پیش‌بینی تمام حالات آینده چندان مطلوب به نظر نمی‌رسد. در بحث تخمین وضعیت جاری سیستم نیز همواره خطا وجود دارد. این خطا ممکن است در محاسبه آینده‌های قابل‌باور تأثیر داشته باشد. دو مسئله مهم در مدل‌سازی تجسم باید مدنظر قرار گیرد. نخست آن‌که امتیاز باورپذیری نباید با احتمال اشتباه گرفته شود. منظور از باورپذیری آینده وجود نشانه‌هایی در وضعیت جاری سیستم است که احتمال وقوع آینده و رخ دادن عمل مربوطه را افزایش می‌دهد. همچنین برخلاف احتمال، امتیاز باورپذیری نیاز به محاسبه باورپذیری میان تمام اشیاء در محیط ندارد. مسئله مهم دوم این است که فرآیند محاسبه باورپذیری نباید با پیش‌بینی اشتباه گرفته شود، اگرچه هر چه امتیاز باورپذیری یک آینده بیش‌تر باشد، آن آینده با احتمال بالاتری رخ خواهد داد. تاکنون در مدل‌سازی تجسم از الگوریتم‌هایی به شکل موازی

استفاده‌شده است و از ارائه الگوریتمی که توانایی ارزیابی تمام وضعیت را داشته باشد؛ احتمالاً به‌دلیل پیچیدگی‌های زیادی در پیاده‌سازی و اجرا صرف‌نظر شده است. علاوه‌براین مدل‌سازی با فرض استقلال مؤلفه‌های تجسم و به‌صورت موازی سبب افزایش کارایی و به‌روزرسانی سیستم می‌شود. در این حالت هرکدام از مؤلفه‌های تجسم قابلیت، رفتار، فرصت و (نیت) برآوردی از وضعیت آینده را به همراه یک نمره تحت عنوان قابلیت اطمینان ارائه می‌کنند که درنهایت می‌توان تخمین‌های حاصله را بر اساس امتیاز قابلیت اطمینان وزن‌دهی و با استفاده از نظریه‌های مشتق شده از دمپستر شافر ترکیب نمود تا برآوردی از وضعیت نهایی یک شیء حاصل شود. در این مقاله ترکیب مؤثرتری بر اساس مدل انتقال باور و استنتاج فازی مدنظر قرارگرفته است.

۳-۳-۱- تجسم حملات سایبری مبتنی بر قابلیت

منظور از قابلیت، ادغام اقداماتی است که یک مهاجم سایبری توانایی انجام آن را دارد. قابلیت مهاجم‌ها به‌میزان سطح آموزشی و منابع فیزیکی که در اختیارشان است، بستگی دارد. اگر بخواهیم دسته‌بندی از این نوع مهاجم‌ها داشته باشیم می‌توان از مهاجمی که به‌عنوان یک کاربر عادی حوزه سایبری مطرح است و به‌سادگی اسکریپت‌های مربوط به نفوذ را دانلود می‌کند تا مهاجم پیشرفته‌ای که از دانش و آگاهی فوق‌العاده بالایی در زمینه آسیب‌رسانی به شبکه‌ها و سامانه‌های عامل برخوردار است، نام برد. یک مهاجم پیشرفته به‌مراتب حملات پیچیده‌تری نسبت به مهاجم عادی خواهد داشت که فقط اسکریپت‌های مربوط به نفوذ را به اجرا می‌گذارد. بنابراین نوع حمله می‌تواند نشان‌دهنده سطح توانمندی مهاجم باشد. اگر حمله پیچیده‌ای مشاهده شود، مهاجم سایبری به‌احتمال زیاد پیشرفته‌تر بوده است و بنابراین سطح بالاتری از تهدید می‌تواند همراه با آن حمله باشد. با این‌وجود، اگر یک حمله به متن یا سند عمومی رخ دهد، حمله‌کننده یک مهاجم مبتدی است، اگرچه هنوز این مهاجم نیز می‌تواند یک مهاجم پیشرفته تلقی شود. بنابراین پیچیدگی حمله می‌تواند نشان‌دهنده سطح توانمندی بالای مهاجم حوزه سایبری باشد. بنابراین تخمین قابلیت‌های مهاجم تنها به نوع حملات در دسترس وابسته نیست، بلکه به اجرای مؤثر آن حمله وابسته است. در فضای سایبر، مهاجم‌های حرفه‌ای قادر هستند تا از یک ماشین موجود در شبکه سوءاستفاده کنند، بدون آن‌که فعالیت آن‌ها شناسایی شود. درحالی‌که مهاجم‌های مبتدی غالباً از ابزارهای شناخته‌شده استفاده می‌کنند؛ بنابراین شناسایی فعالیت آن‌ها در شبکه نیز آسان‌تر است. بااین‌حال روش کاملی برای تخمین دقیق قابلیت‌های مهاجم وجود ندارد. در این مقاله برای ساده‌سازی مسئله اقدام به تخمین قابلیت‌های مهاجم بر اساس سرویس‌هایی شده که قبلاً مورد حمله واقع‌شده است. برای پی بردن به الگوریتم مطرح‌شده در [۲۶] ابتدا آسیب‌پذیری‌های مربوط به هر سرویس توسط پایگاه داده CVE استخراج می‌شود. فرض کنید که S زیرمجموعه‌ای از تمام سرویس‌های جاری در شبکه و S_a مجموعه‌ای از سرویس‌هایی باشند که هدف حمله a قرارگرفته‌اند. هدف در این مسئله یافتن سرویس‌هایی (S در شبکه است که با توجه به پیشرفت حملات جاری به‌احتمال‌زیاد مورد حمله قرار می‌گیرند؛ بنابراین برای هر سرویس در شبکه باید امتیاز باورپذیری را با توجه به رابطه زیر محاسبه نمود. فرض کنید X_{sa} یک متغیر برنولی باشد که نشان‌دهنده قابلیت مهاجم در اجرای حمله a به سرویس $s \in S$ باشد. امید ریاضی X_{sa} ($E[X_{sa}]$) از رابطه زیر محاسبه می‌شود.

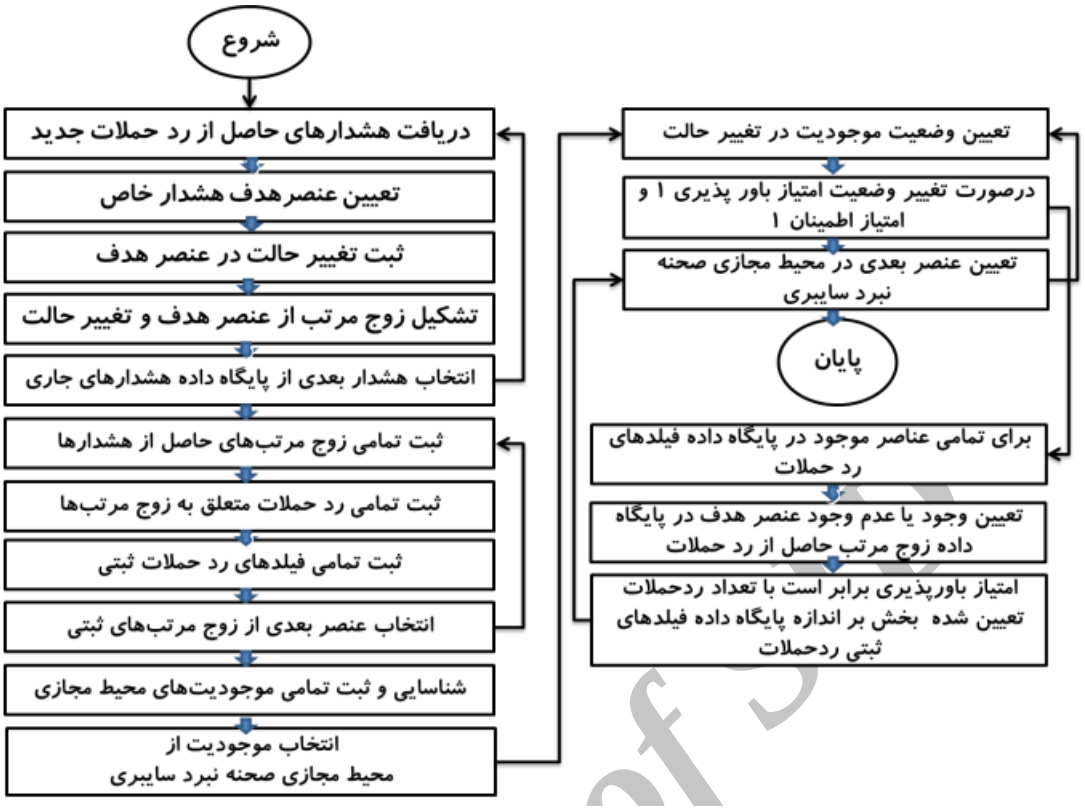
$$P[S|S_a] = \frac{E(S \cap S_a)}{E(S_a)} \quad (۱)$$

واضح است که برای $s \in S_a$، $E[X_{sa}]$ برابر ۱ خواهد بود. برای اضافه کردن پارامتر تأثیر به محاسبات فوق سرویس‌های موجود در شبکه را به چهار سرویس تقسیم می‌کنیم. سرویس‌هایی که (s_u) حمله به آن‌ها ناموفق بوده است؛ سرویس‌هایی (s_d) که کشف‌شده‌اند؛ سرویس‌هایی که s_p) کنترل آن‌ها به‌طور جزئی در اختیار مهاجم است و سرویس‌هایی که (s_c) کنترل آن‌ها به‌طور کامل در اختیار مهاجم است.

$$P[S|S_a] = \frac{E(S_u \cup S_d \cup S_p \cup S_c \cup S_a)}{E(S_a)} \quad (۲)$$

به‌ازای هر سرویس s و هر حمله a، مقدار امتیاز باورپذیری ($P[s|S_a]$) و امتیاز قابلیت اطمینان (r) محاسبه می‌شود.

با این توصیف در تجسم قابلیت برای هر میزبان در شبکه الگوریتم زیر اجرا می‌شود. این الگوریتم در شکل (۵) نشان داده‌شده است. همان‌طور که در شکل (۳) نیز مشخص است، این الگوریتم با دریافت هشدارهای رد حمله جاری ($T_{current}$) آغاز می‌گردد که این نیز نشان‌دهنده بلادرنگ بودن الگوریتم معرفی‌شده است. برای تمام این هشدارها عنصری که هدف هشدار بوده (V_A) و تغییر حالت آن عنصر (S_A) را به‌صورت یک مجموعه دوتایی ذخیره می‌گردد. سپس برای هر عنصر از محیط مجازی صحنه نبرد سایبری با مراجعه به تاریخچه رد حملات و استخراج رد حملاتی که عنصر موردنظر در آن وجود داشته نسبت تعداد رد حملاتی که این عنصر موردنظر در آن وجود داشته و تغییر حالت داده است را به تعداد رد حملاتی که عنصر موردنظر در آن عضویت دارد را به‌عنوان غیرحرفه‌ای قابلیت شیء موردنظر محاسبه می کند.



شکل (۵). الگوریتم تخمین قابلیت مهاجم [یافته تحقیق]

۳-۳-۲- تجسم حملات سایبری مبتنی بر فرصت

منظور از فرصت، زمان لازم مهاجم برای اجرای حملات در مرحله بعدی حمله است. در تعیین فرصت می‌توان از میزان آسیب‌پذیری سامانه‌ای که قرار است موردحمله قرار گیرد و اطلاعاتی که مهاجم در حال حاضر می‌تواند به آن‌ها دسترسی داشته باشد، استفاده کرد. فرض کنید یک مهاجم سایبری می‌داند چگونه سرویس‌هایی را بر روی یک سرور شناسایی کند تا از این طریق به قواعد و قوانین مدیریتی دسترسی پیدا کند. درحالی‌که مهاجم دارای توانمندی شناسایی آن خدمات است، نمی‌تواند آن خدمات را مورد سوء استفاده قرار دهد مگر این‌که دقیقاً بداند که آن اطلاعات بر روی سرور در حال اجرا است. اگر مهاجم تعیین کند که خدمات مدنظر بر روی سرور در حال اجرا هستند، بنابراین فرصت دسترسی به سرویس‌ها را پیدا خواهد نمود. حتی اگر مهاجم از چگونگی استفاده از یک سرویس خاصی آگاه نباشد، هنوز فرصت استفاده از آن سرویس را خواهد داشت، اما احتمال وقوع این امر اندک است به‌دلیل این‌که مهاجم از توانمندی و توانایی محدودی در این زمینه برخوردار است. بنابراین فرصت به پیشرفت یک مهاجم در شبکه بستگی دارد. در یک شبکه که سخت‌گیرانه پیکربندی‌شده است، برخی از کارگذارها و میزبان‌ها در پشت یک یا چند دیوار آتش مخفی‌شده‌اند. مهاجم ممکن است از ماشین‌هایی که آن‌ها را مورد بهره‌برداری قرار می‌دهد به‌عنوان پلی برای نفوذ به یک زیرشبکه دیگر استفاده کند. الگوریتم فرصت قواعد دیوار آتش را میان میزبانی که از آن بهره‌برداری شده و بقیه شبکه مورد تحلیل و بررسی قرار می‌دهد و سطحی از تهدید را به هر میزبان اعطا می‌کند. در تحقق تجسم فرصت فرض کنید پورت‌های بسته میان میزبان مورد بهره‌برداری قرارگرفته i و مورد بهره‌برداری قرار نگرفته j، به‌صورت C_{ij} نشان داده شود. همچنین S_{jk} مجموعه پورت‌های مربوط به سرویس k در میزبان j باشد. d_{jk} به‌عنوان عامل تنزیل برای سرویس‌هایی که هنوز کشف‌نشده یا موردحمله یا مورد بهره‌برداری قرار نگرفته، تعریف شود. این مقدار برای سرویس‌هایی که در حالت معمولی‌اند بین صفر و یک و در غیر این صورت d_{jk} برابر ۱ است. P_{jk} امتیاز اختصاص داده‌شده به سرویس k در میزبان j است.

در رابطه زیر p_{open}، p_{close} و $p_{partopen}$ همگی مقادیر میان صفر و یک دارند.

$$p_{jk} = \begin{cases} p_{open} & \text{for } C_{ij} \cap S_{jk} = \{\} \\ p_{close} & \text{for } C_{ij} \cap S_{jk} = \varnothing \\ p_{partopen} & \text{otherwise} \end{cases} \quad (۳)$$

پیچیدگی عمده ارزیابی فرصت ناشی از پیمایش صورت گرفته در مدل گراف مبنای شبکه که مدل عوارض مجازی نامیده می‌شود، به‌منظور تحلیل مسیر میان میزبان‌هایی که قبلاً توسط مهاجم مورد بهره‌برداری قرارگرفته‌اند و میزبان‌های در دسترسی که قبلاً توسط مهاجم مورد بهره‌برداری قرار نگرفته‌اند، است. به‌منظور کاهش این پیچیدگی، تمام میزبان‌هایی که قبلاً توسط مهاجم مورد بهره‌برداری قرارگرفته‌اند، به‌صورت گروهی و در قالب یک گره بانام CompSrc نشان داده می‌شوند. هنگامی‌که یک میزبان مورد بهره‌برداری مهاجم قرار می‌گیرد. گروه CompSrc به‌روزرسانی می‌شود. همچنین ما مجموعه میزبان‌های در دسترسی که قبلاً توسط مهاجم‌مورد بهره‌برداری قرار نگرفته‌اند که به‌صورت ExpTgt و مجموعه‌ی قواعد جمع‌آوری‌شده‌ی دیوار آتش رابین CompSrc و هر یک از مقصدها به‌صورت AggRules نشان می‌دهیم. پیچیدگی استفاده از جستجوی اول سطح در این الگوریتم برای به‌روزرسانی CompSrc، ExpTgt و AggRules هنگام اضافه شدن یک میزبان جدید (NewComp)، $O(n+m)$ است که در آن n برابر مجموع گره‌ها در CompSrc و ExpTgt است و m تعداد مسیرهای میان این دو است. در شکل ۶ الگوریتمی را مشاهده می‌کنید که خروجی آن مجموعه‌ای از میزبان‌ها است که از میزبان سوءاستفاده‌شده‌ی فعلی به آن دسترسی وجود دارد.

در الگوریتم شکل (۶) چهار دسته حالت جاری مبدأ حمله، حالت جاری مقصد حمله، پیکربندی قواعد دیوار آتش و سرویس‌های باز در مقصد مسیرهای ممکن در شبکه هستند. حالت جاری مبدأ و مقصد حمله، سطح دسترسی که مهاجم قبلاً به دست آورده را مشخص می‌کند. قواعد دیوار آتش نشان‌دهنده سطح محدودیت در طول مسیر است. سرویس‌های بازنشان می‌دهند که چه سرویس‌های در هدف قابل بهره‌برداری هستند. به هر عنصر موجود در یک دسته یک امتیاز تجسم بر اساس قابلیت مهاجم و یک امتیاز قابلیت اطمینان اعطا می‌شود. این مقادیر بر اساس پیکربندی شبکه مشخص می‌شوند.

در مسیر $p_{s,t}$ بین مبدأ s و مقصد t، امتیاز فرصت و قابلیت اطمینان که به‌صورت $o(p_{s,t})$ و $r(p_{s,t})$ نشان داده می‌شود، خروجی نرمالیزه شده چهارعنصر هستند که در مقیاس دو مقدار ثابت MaxProjScore و MaxReliability محاسبه می‌شوند. از رابطه (۴) محاسبه $o(p_s,t)$ استفاده می‌شود.

$$o(p_{s,t}) = \frac{\prod_{i\in\Omega(p_{s,t})} c_i}{\max_p(\prod_{i\in\Omega(p)} c_i)} \qquad (۴)$$

```
If HA is a newly compromised host then
     NHA = neighbor network components of HA
for all NHA
 exposed_rules of NHA = (exposed_rules of NHA)∪(firewall_rules of HA to NHA)
 parent of NHA = HA
end for
push neighbor network components of HA onto search_list
 for all elements in search_list
    N = removed last element of search_list
  if N has not been visited then
   if N is a Router then
   NN = neighbors of N
     for all NN
       exposed_rules of NH = (exposed_rules of NN) ∪((exposued_rules of N)∩
        parent of NN = N
     end for
     push all NN onto search_list
   else if N is a Host then
    add N to reachable_host_set
   end if
 end if
end for
end if
```

شکل (۶). شبه کد تخمین فرصت مهاجم با توجه به رد مشخص حمله، میزبان تحت حمله H و تمامی موجودیت‌های شبکه N

در رابطه‌ی (۴) c_i به مقادیر مشخص برای عنصر i مربوطه است. $\Omega(p)$ شامل چهار دسته عناصری است که مسیر p را توصیف می‌کنند.

۳-۳-۳- تجسم حملات سایبری مبتنی بر رفتار

در تجسم رفتار، هدف بررسی و داشتن الگوهای رفتاری است. درواقع در این سطح هدف استخراج الگوهایی با توجه به رفتارهای گذشته مهاجمین است. تجسم حملات سایبری مبتنی بر رفتار شامل سه مرحله تولید رد حمله، مدل‌سازی ترتیبی و پیش‌بینی است. بنابراین از مدل مارکوف با طول متغیر و درخت پسوندی می‌توان اقدام به تجسم رفتار نمود که از وضعیت فعلی درخت پسوندی توسط الگوریتم مدل مارکوف با طول متغیر به پیش‌بینی اقدامات آینده مبادرت می‌شود. مرتبه‌ی n اُم مدل مارکوف محتوا محدود بیانگر یک گام حمله جدید با n مشاهده قبلی در رد حمله است ($P^n\{x_{(t+1)} \mid x_{(t-n+1)},\ldots,x_t\}$). احتمال P^n با استفاده از وزن یال‌های فرزند درخت پسوندی با توجه به در نظر گرفتن مشاهدات قبلی محاسبه شده است. علاوه‌براین با برآورد قابلیت و فرصت برای تجسم حملات از تحلیل روند رفتاری مهاجم نیز می‌توان بهره گرفت. با این دلیل که میزان تکرار یک الگو نشان‌دهنده نوع حملات، سرویس‌های مورد حمله قرارگرفته، زیر شبکه‌هایی تحت کنترل مهاجم است که برای استخراج این الگوها از مدل مارکوف با طول متغیر استفاده می‌شود.

۴-۳-۳- تجسم حملات سایبری مبتنی بر نیت

منظور از نیت اقدامات و فعالیت‌های آتی یک مهاجم است که مهاجم با برنامه‌ریزی قبلی قصد انجام آن را دارد. تشخیص نیات مهاجمان سایبری بسیار مشکل است، مگر این‌که واقعاً یک عمل خاصی رخ داده باشد. وقتی مهاجمی گستردگی و تسلط خود را بر شبکه به‌دست آورد، نیاز دارد تا هدف خویش را پیگیری نماید. متأسفانه با توجه به آگاهی و دانش موجود در این حوزه هنوز هیچ مدل مرجع خاصی وجود ندارد که با استفاده از آن بتوان پیش‌بینی نمود که آیا مهاجم می‌تواند فایل حیاتی را تغییر دهد و یا این‌که به‌سادگی سامانه را رها خواهد ساخت. درهرصورت اگر مهاجم شناخته‌شده‌ای باشد که اغلب کارهای شرورانه‌ای را انجام می‌دهد، این احتمال وجود دارد که آن مهاجم دارای مقاصد و نیت‌های شرورانه‌ای است. با این‌وجود اگر هیچ‌گونه اقدام شرورانه‌ای را انجام نداده باشد، تقریباً تعیین مقاصد و نیات آن مهاجم غیرممکن است.

۵-۳-۳- ترکیب کلی مؤلفه‌های تجسم

در این مقاله چارچوبی برای تجسم حملات سایبری با استفاده از ترکیب چهار مؤلفه رفتار، نیت، فرصت و قابلیت ارائه شده است. در فرایند ترکیب این چهار مؤلفه، امتیاز باورپذیری توسط الگوریتم‌های باور سنج محلی در هر مرحله حمله از حملات چندمرحله‌ای تولیدشده و به‌عنوان ورودی وارد می‌شوند. همان‌طور که پیش‌ازاین نیز گفته شد، در اولین فاز ادغام امتیاز مشتق شده از الگوریتم‌های تخمین فرصت و قابلیت، رفتار و نیت برای هر مرحله حمله با یکدیگر ترکیب می‌شوند. توجه داشته باشید که اگر یکی از اشیاء موردعلاقه از قبل مورد بهره‌برداری مهاجم قرارگرفته باشد، دیگر به آن امتیاز باورپذیری تعلق نمی‌گیرد؛ بنابراین الگوریتم‌های باور سنج محلی به عناصر مجموعه $J^* \subseteq J$ امتیاز باورپذیری اختصاص می‌دهد؛ که J^* مجموعه‌ای از اشیاء است که مورد بهره‌برداری مهاجم قرار نگرفته‌اند. برای افزایش کارایی به هرکدام از عناصر موجود در J^* که فاقد امتیاز باورپذیری‌اند، مقدار نامشخص می‌دهیم؛ به‌عبارت‌دیگر، الگوریتم باور سنج هر مرحله حمله k در مرحله حمله L_l و شیء $j \subseteq J^*$ که j مقدار $p(j,l,k)$ را محاسبه می‌کند. هرکدام از الگوریتم‌های باور سنج در هر مرحله حمله یک امتیاز باورپذیری به هر شیء در هر وضعیت اختصاص می‌دهد. همان‌طور که در شکل (۴) نشان داده شد، دو مرحله ادغام وجود دارد. در مرحله اول امتیازهای اختصاص داده‌شده به هر شیء موردعلاقه توسط الگوریتم‌های فرصت و قابلیت، رفتار و نیت در هر مرحله از حملات سایبری با یکدیگر ادغام می‌شوند و خروجی آن $P(j,l)$ است. در مرحله دوم این امتیازها برای تمامی مراحل حمله با یکدیگر ادغام‌شده و برای هر حمله چندمرحله‌ای یک امتیاز اختصاص می‌یابد تا برای هر شیء موردعلاقه در محیط یک امتیاز باورپذیری $P(j)$ را محاسبه کنیم. ازآنجایی‌که هرکدام از الگوریتم‌های باور سنج محلی یک امتیاز قابلیت اطمینان محاسبه می‌کند، فرآیند ادغام می‌تواند از این خروجی به‌عنوان وزن استفاده کند. وزن اختصاص داده‌شده با امتیاز قابلیت اطمینان رابطه مستقیم دارد. در فرآیند ادغام به امتیاز دارای قابلیت اطمینان بالاتر وزن بیش‌تری اختصاص داده می‌شود. اگر امتیاز باورپذیری یک شیء نامشخص باشد، در فرآیند ادغام عاملی در محاسبه ندارد. علاوه بر این ممکن است نتایج این الگوریتم‌ها با یکدیگر تداخل داشته باشد. فرآیند ادغام انتخابی باید توانایی حل این مشکل را داشته باشد. درنهایت چندین نمره‌ی بالا (پایین) باید امتیاز ادغام‌شده را افزایش (کاهش) دهد.

نظریه ترکیب شواهد روشی برای ترکیب مشاهدات دارای عدم قطعیت است. ازآنجایی‌که خروجی الگوریتم‌های باورسنج در هر مرحله حمله شامل قابلیت اطمینان نیز می‌باشند، ما تصمیم گرفتیم از نظریه دمپستر شافر برای ادغام استفاده کنیم.

چهار نتیجه ممکن برای هر امتیاز ممکن است رخ دهد؛ نخست آن‌که خروجی باورپذیر و قابل‌اطمینان (PR) باشد؛ دوم این‌که خروجی نه قابل‌باور و نه قابل‌اطمینان (NU) باشد؛ سوم این‌که خروجی باورپذیر و غیر قابل‌اطمینان (PU) باشد و درنهایت این‌که خروجی غیرقابل‌باور و قابل‌اطمینان (NR) باشد؛ بنابراین چارچوب تشخیص به شکل زیر خواهد بود.

$$\theta = \{PR, NU, PU, NR\} \quad (۵)$$

تابع تخصیص جرم نیز به شکل زیر خواهد بود.

$$m(A) = \begin{cases} p\ (j,l,k)\ r\ (j,l,k) & \text{for A=\{PR\}} \\ p\ (j,l,k)\ [\ 1\ -\ r\ (j,l,k)\ ] & \text{for A=\{PU\}} \\ [\ 1\ -\ p\ (j,l,k)\ ]\ r\ (j,l,k) & \text{for A=\{NR\}} \\ [\ 1\ -\ p\ (j,l,k)\ ]\ [\ 1\ -\ r\ (j,l,k)\ ] & \text{for A=\{NU\}} \end{cases} \quad (۶)$$

برای محاسبه امتیاز باورپذیری و قابلیت اطمینان از روابط زیر استفاده می‌کنیم.

$$P(j,l) = Bel(\{PR, NU\}) \\ R(j,l) = Bel(\{PR, NR\} \quad (۷)$$

هم‌اکنون امتیازهای باورپذیری بر روی تابع تخصیص اولیه نگاشت می‌شوند و امتیاز باورپذیری P(j,l) برای هر شیء در هر مرحله حمله محاسبه می‌کنیم. در مرحله بعد این امتیازها برای هر شیء ادغام می‌شوند تا P(j) برای هر شیء در کل مراحل حمله محاسبه شود. همان‌طور که پیش‌ازاین نیز گفته شد، امتیاز نامشخص نشان‌دهنده عدم وجود اطلاعاتی در مورد شیء موردنظر است؛ بنابراین الگوریتم ادغام باید قابلیت نادیده گرفتن امتیاز ناشناخته را داشته باشد. بااین‌وجود اگر همه P(j,l,k) ها برای یک شیء ناشناخته باشد، P(j,l) = unknown خواهد بود.

در این مقاله ما اقدام به ترکیب فازی تجسم مدل مارکوف با طول متغیر برای قابلیت‌ها (چه سرویس‌هایی آشکارشده‌اند) و فرصت‌های مهاجم (چه زیر شبکه‌هایی مورد نفوذ قرارگرفته‌اند) می‌کنیم. با این فرض که تجسم قابلیت و فرصت منجر به تجسم رفتار مهاجم می‌شود. جدول (۱) تجسم بر اساس مدل مارکوف با طول متغیر برای سه خصوصیت tip و prt و dsc که به ترتیب بیان‌گر زیر شبکه، پروتکل، سرویس آشکارشده می‌باشند؛ است. روش مدل مارکوف با طول متغیر بر روی استخراج الگوها و تجسم بر پایه‌ی ویژگی‌های خاصی از هشدارهای سامانه‌های تشخیص نفوذ تمرکز می‌کند. بنابراین با استفاده از مدل مارکوف با طول متغیر و ایجاد درخت پسوندی برای هرکدام از مقادیر خصوصیت‌های tip، prt و dsc یک احتمال وقوع محاسبه خواهد شد.

تجسم با استفاده از مدل مارکوف با طول متغیر در شبکه تحت حمله نشان می‌دهد که مقادیر ۱۹۲,۱۶۸,۳.x، UDP، WEB-MISC http directory traversal دارای بالاترین امتیاز برای خصوصیات زیر شبکه، پوتکل و سرویس موردحمله واقع‌شده است. ترکیب مستقیم این داده‌ها چندان مؤثر به نظر نمی‌رسد؛ زیرا [1](پروتکل HTTP از UDP استفاده نمی‌کند ۲) زیر شبکه ۱۹۲,۱۶۸,۳x. شامل کارگذار وب نیست؛ بنابراین نیاز به یک ادغام هوشمندانه و قوی احساس می‌شود.

جدول (۱). تجسم مدل مارکوف با طول متغیر برای سه خصوصیت زیر شبکه، پروتکل و سرویس

خصوصیت	مقادیر ممکن	احتمال
زیر شبکه	۱۹۲,۱۶۸,۱.x	۰/۱۴۲۵
	۱۹۲,۱۶۸,۳.x	۰/۹۱۵۲
	۱۹۲,۱۶۸,۲۰.x	۰/۱۲۵۶
پروتکل	TCP	۰/۲۵۴۸
	UDP	۰/۵۵۸۹
سرویس موردحمله	SMTP sendmail 5.5.5 exploit	۰/۴۳۴۹
	WEB-MISC http directory traversal	۰/۵۵۱۳
	FTP adm scan	۰/۰۱۳۸

۳-۳-۵-۱- ترکیب قابلیت و فرصت بر اساس مدل انتقال باور

اولین رویکرد برای حل مشکل تجسم ترکیب الگوریتم‌های قابلیت و فرصت معرفی‌شده در [۲۶] است. در روش معرفی‌شده یک الگوریتم صوری با امکان ارتقاء ارائه شده است. توصیفات زیر، چگونگی ترکیب خروجی این دو الگوریتم را با استفاده از نظریه انتقال باور نشان می‌دهد. در این بخش از الگوریتم‌های تخمین استقرایی قابلیت و فرصت مهاجم استفاده‌شده است. برای ترکیب امتیازهای باورپذیری مشتق‌شده از الگوریتم‌های تخمین قابلیت و فرصت ما از نظریه‌های مشتق‌شده از دم دمپستر شافر استفاده می‌کنیم. روش‌های مختلف ترکیب باور مزایا و معایب مربوط به خود رادارند و هرکدام راه‌حلی برای یک مسئله است. ما در این گزارش مدل انتقال باور[1] را انتخاب می‌کنیم که روند نرمالیزه کردن تضاد را از نظریه شواهد دمپستر- شافر حذف می‌کند. در این ترکیب خروجی هرکدام از الگوریتم‌های تجسم، امتیاز باورپذیری و قابلیت اطمینان است که به‌صورت p_i و r_i نشان داده می‌شود که در آن i یکی از دو مقدار c و o را که به ترتیب نشان‌دهنده ارزیابی قابلیت و فرصت است را نشان می‌دهد. ما چارچوب تشخیص را به‌صورت زیر تعریف می‌کنیم:

$$\Phi = \{P, N\} \quad (۸)$$

که در آن، P نشان‌دهنده باورپذیر بودن حمله به مقصد و N نشان‌دهنده باورپذیر نبودن آن است. تابع تخصیص جرم برای هر ارزیابی به‌صورت زیر تعریف می‌شود.

$$m_i(\mathrm{A}) = \begin{cases} p_i r_i & A = \{P\} \\ (1-p_i) r_i & A = \{N\} \\ 1 - r_i & A = \{P, N\} \end{cases} \quad (۹)$$

$$m_f(\mathrm{A}) = m_c(\mathrm{A}) + m_0(\mathrm{A}) \\ = \sum_{B \cap C = A} m_c(B) m_0(C) \quad (۱۰)$$

1- Transferable belief model

با استفاده از قانون مدل انتقال باور نشان داده‌شده در بالا، نه‌تنها پیش‌بینی ادغام‌شده (m_f (A) بلکه میزان عدم قطعیت نیز مشخص می‌گردد. درصورتی‌که A = Ø باشد، این مقدار برابر حاصل جمع احتمال تمام زیرمجموعه‌های Φ می‌گردد. این بدین معنی است که m_f (Φ) نشان‌دهنده تضاد میان توابع جرم (ارزیابی) در حال ترکیب است. m_f (P,N) نشان‌دهنده‌ی عدم قطعیت در قابلیت اطمینان مشاهدات است. مجموع m_f (P,N) و m(Φ) نشان‌دهنده عدم اطمینان کل درنتیجه ادغام است. امتیاز تجسم بین بازه m_f (P) و m_f (P,N) + m_f (P) + m_f (Φ) قرار می‌گیرد. امتیاز تجسم (ادغام‌شده) و قابلیت اطمینان به‌صورت زیر به‌دست می‌آیند.

$$Projection = \frac{m_f(P)}{reliability} \qquad (۱۱)$$

$$reliability = 1 - (m_f(\emptyset) + m_f(P,N)) \qquad (۱۲)$$

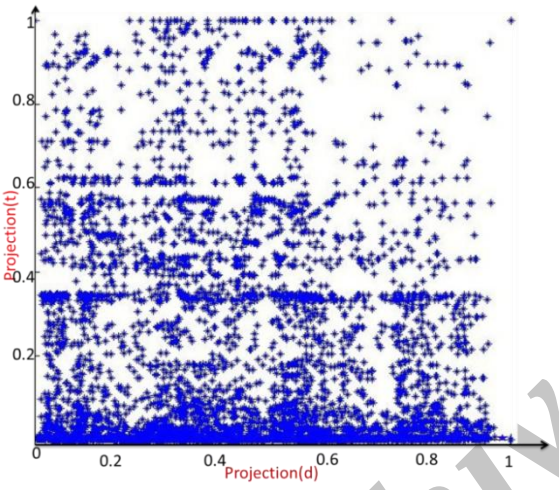
۳-۳-۵-۲. ترکیب قابلیت و فرصت مبتنی بر استنتاج فازی

برای هرکدام از پیش‌بینی‌های مدل مارکوف با طول متغیر یک امتیاز تجسم استخراج شود. دو امتیاز تجسم $Proj_t$ و $Proj_d$ بر اساس پیش‌بینی‌های مدل مارکوف با طول متغیر برای دو خصوصیت tip و dsc به هر میزبان شبکه اختصاص می‌یابد. $Proj_t(h)$ نشان می‌دهد بر اساس ترتیب زیرشبکه‌هایی که موردحمله واقع شده‌اند، به چه احتمالی میزبان h هدف بعدی حمله مهاجم است. $Proj_d(h)$ نیز بر اساس دنباله سرویس‌های آشکارشده، به میزبان h امتیازی اختصاص می‌دهد که نشان‌دهنده این احتمال است که میزبان h هدف بعدی حمله باشد. فرض کنید $P_t()$ و $P_d()$ به ترتیب احتمالات مشتق‌شده بر اساس مدل مارکوف با طول متغیر برای دو خصوصیت tip و dsc باشد. همچنین فرض کنید N(h) زیرشبکه‌ای که میزبان h در آن قرار دارد و E(h) مجموعه‌ای از آسیب‌پذیری‌های آشکارشده در میزبان h باشد. دراین‌صورت $Proj_t$ و $Proj_d$ با توجه به روابط زیر قابل محاسبه است.

$$Proj_t(h) = P_t\big(N(h)\big)$$
$$Proj_d(h) = P_t \sum_{i \in E(h)} P_d(i) \qquad (۱۳)$$

برای ترکیب $Proj_t(h)$ و $Proj_d(h)$ ما از سامانه‌های استنتاج فازی استفاده می‌کنیم که یکی از روش‌های قدرتمند برای ادغام داده محسوب می‌شوند و به تقلید از تحلیل‌های انسانی می‌پردازد. دو نوع سیستم استدلال فازی وجود دارد؛ ممدانی و سوگنو. ما در این گزارش از روش سوگنو استفاده می‌کنیم؛ زیرا پیوستگی سطح خروجی را تضمین می‌کند. این سامانه از دو جزء اصلی توابع عضویت جهت فازی کردن ورودی‌ها و قواعد استنتاج برای ترکیب، تشکیل‌شده است.

توابع عضویت می‌توانند از بررسی پراکندگی ورودی‌ها مشتق شوند. شکل (۷) نمودار پراکندگی $Proj_t$ را در مقابل $Proj_d$ برای تمام اهداف در طول آزمایش نشان می‌دهد. این نمودار نشان می‌دهد که $Proj_d$ بیش‌تر به‌صورت تراز میان صفر و یک است؛ درحالی‌که غلظت $Proj_t$ در بازه [۰ ,۰,۱] بیش‌تر است نتایج آزمایش‌های ما در بر روی دادگان متفاوت، نمودارهای پراکندگی یکسانی را از خود نشان دادند. این امر ناشی از این است که در بسیاری از نمونه‌ها تعداد زیادی از میزبان‌ها پشت دیوارهای آتش قرارگرفته‌اند. در این نمونه‌ها تخمین بر مبنای سرویس‌های آشکارشده، موجب تولید مجموعه‌هایی به‌اندازه کافی بزرگ با توزیع یکنواخت از خدمات می‌شود.



شکل (۷). نمودار پراکندگی $Proj_t$ در مقابل $Proj_d$

به‌منظور تفاوت قائل شدن میان غلظت ناحیه [۰,۰,۱] از توابع عضویت بیش‌تری برای $Proj_t$ استفاده شده است. در توابع عضویت مدنظر این مسئله از ۱۵ قاعده استنباط استفاده شده که $Proj_t$ و $Proj_d$ را با یکدیگر ترکیب می‌کند. تأکید بیش‌تر این قواعد بر روی $Proj_t$ است؛ زیرا تحلیل‌گران انسانی اعتبار بیش‌تری برای $Proj_t$ ا قائل هستند. جدول (۲) یک دید جدولی از این قواعد را نشان می‌دهد. عناصر موجود (a_{ij}) در جدول (۲) به‌منظور محاسبه تجسم، برمبنای متغیر پیشین (u_{ij}) که با عملگر AND در منطق فازی تعریف می‌شود؛ تجمیع می‌گردند.

$$Projection = \frac{\sum_{i=1}^{5}\sum_{j=1}^{3} u_{ij}.a_{ij}}{\sum_{i=1}^{5}\sum_{j=1}^{3} u_{ij}} \qquad (۱۴)$$

که در این رابطه، μ_i و μ_j به‌صورت i اُمین و j اُمین توابع عضویت $Proj_t$ و $Proj_d$ در نظر گرفته می‌شوند.

$$u_{ij} \triangleq u_i(Proj_t).u_j(Proj_d) \qquad (۱۵)$$

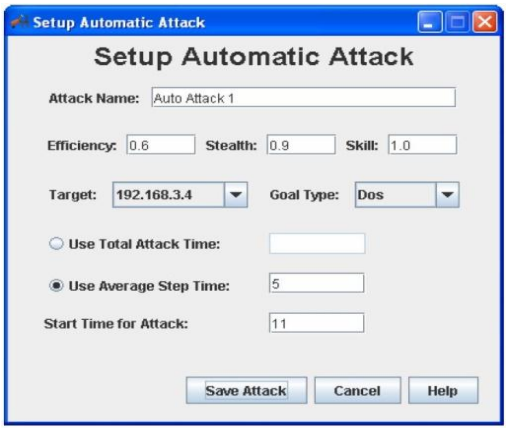
جدول (۲). قواعد استنتاج فازی: امتیاز تجسم به خروجی توابع عضویت داده می‌شود.

$Proj_d$	$Proj_t$ low 1	low 2	low 3	medium	high
low	۰/۰	۰/۲	۰/۴	۰/۶	۰/۸
medium	۰/۲	۰/۴	۰/۶	۰/۸	۱/۰
high	۰/۴	۰/۶	۰/۸	۰/۸	۱/۰

نتایج کلی می‌توانند با استفاده از نمودار سطح ورودی/ خروجی نشان داده شود؛ که سطح در ناحیه غلیظ IP exposure به‌منظور تمایز میان ورودی‌ها و کاهش مثبت اشتباه، یک‌روند صعودی با سرعت‌بالا دارند. تغییرات با در نظر گرفتن سرویس‌های آشکارشده، موجب توزیع یکنواختی که پیش این نیز گفته شد، می‌گردد.

۴- شبیه‌سازی الگوریتم پیشنهادی و نتایج آن

برای شبیه‌سازی معماری پیشنهادی از سناریوهای مختلف حمله استفاده شده است. این سناریوها از یکسری حملات از پیش معین ایجاد شده است. معمولاً در شبیه‌سازهای حملات سایبری، از واسط کاربری جهت انتخاب یک سری از پارامترهای حمله استفاده می‌شود. در شکل (۸)، واسط کاربری شبیه‌سازی مربوط به شبیه‌ساز نسخه هفت آرنا که برای ایجاد حملات از آن استفاده کرده‌ایم را مشاهده می‌کنید. این پارامترها سعی می‌کنند تا رفتار مهاجم را شبیه‌سازی کنند. دو پارامتر مهم که در بیش‌تر شبیه‌سازهای حملات سایبری وجود دارند، «سطح تأثیر» و «میزان مخفی بودن» حملات است. سطح تأثیر یک حمله نشان‌دهنده میزان انحراف مهاجم از کوتاه‌ترین مسیری است که مهاجم برای رسیدن میزبان هدف انتخاب می‌کند. یک حمله در حالتی مؤثرتر است که از کمترین «انحراف» برای رسیدن به مقصد استفاده شود. در جدول (۳ و ۴)، دو نمونه سناریوی حمله را به ترتیب با سطح تأثیر بالا و پایین مشاهده می‌کنید. 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. جدول (۵) یک سناریوی حمله با پارامتر مخفی را نشان می‌دهد.



جدول (۳). یک سناریوی حمله با سطح تأثیر بالا

مرحله	آدرس مهاجم	آدرس قربانی
۱	۹,۵,۲۳۱,۷۲	۱۹۲,۱۶۸,۱,۳
۲	۲۳۷,۲۲,۲۰۲,۱۴۰	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	۱۹۲,۱۶۸,۶,۱۱۱
۱۰	۱۹۲,۱۶۸,۶,۱۱۱	۱۹۲,۱۶۸,۷,۹

جدول (۴). یک سناریوی حمله با سطح تأثیر پایین

مرحله	آدرس مهاجم	آدرس قربانی
۱	۹,۵,۲۳۱,۷۲	۱۹۲,۱۶۸,۱,۳
۲	۲۳۷,۲۲,۲۰۲,۱۴۰	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

جدول (۵). یک سناریوی حمله با پارامتر مخفیانگی

مرحله	آدرس مهاجم	آدرس قربانی
۱	۹,۵,۲۳۱,۷۲	۱۹۲,۱۶۸,۱,۳
۲	۲۳۷,۲۲,۲۰۲,۱۴۰	۱۹۲,۱۶۸,۱,۴
۳	۱۹۲,۱۶۸,۱,۳	۱۹۲,۱۶۸,۲,۷
۴	۱۹۲,۱۶۸,۲,۹	۱۹۲,۱۶۸,۴,۲۰
۵	۱۹۲,۱۶۸,۴,۲۰	۱۹۲,۱۶۸,۶,۱۱۳
۶	۱۹۲,۱۶۸,۶,۱۱۳	۱۹۲,۱۶۸,۷,۹

با توجه به حملات شبیه‌سازی‌شده بر اساس سناریوهای تعریفی در جدول‌های (۳،۴ و ۵) عملکرد هرکدام از دو روش بدون‌ترکیب و با ترکیب قابلیت و فرصت برای حملات با پارامترهای متفاوت مورد ارزیابی قرار می‌گیرد. بر اساس دادگان

موجود، ما الگوریتم خود را برای بررسی میزان دقت در پیش‌بینی مقصد بعدی حمله اجرا کردیم. هدف اصلی سامانه‌های تجسم حملات سایبری ارائه یک فهرست رده‌بندی‌شده از اهداف تجسم‌شده، به‌جای این که دقیقاً هدف بعدی حمله را مشخص کنند، است. برای بررسی کارایی الگوریتم باید درصد احتمال به دست آمده برای میزبان مورد حمله واقع‌شده را یک مرحله قبل از حمله بررسی کنیم. نتایج در این مقاله به‌صورت بازه [lower, upper] بیان می‌شود که نشان‌دهنده بازه رتبه‌بندی‌شده از میزبان‌هایی است که همان امتیازی که هدف کسب کرده است را کسب کرده‌اند.

جدول (۶). میزان دقت تجسم با استفاده از ترکیب و بدون ترکیب مولفه‌های تجسم

نوع ترکیب	شبکه هدف		
	Low Eff	Medium Eff	High Eff
مدل انتقال باور	[54%,74%]	[55%,77%]	[59%,79%]
فازی	[81%,84%]	[84%,88%]	[85%,88%]
بدون ترکیب	[31%,54%]	[34%,58%]	[35%,48%]

جدول (۵) نشان‌دهنده میزان دقت تجسم با استفاده از ترکیب و بدون ترکیب مولفه‌های تجسم است. ضمنا با نتایج این بخش و آنچه در بخش پیشین بیان شد می‌توان گفت که :

- ترکیب فازی تجسم قابلیت و فرصت مهاجم برای حملات با تأثیر بالا بسیار مؤثر عمل می‌کند و در حملات با سطح تأثیر پایین جدول (۳)، که به مقصد ۱۹۲,۱۶۸,۷,۹ صورت می‌گیرد. کارایی تجسم صورت‌گرفته با روش ترکیب قابلیت و فرصت بر سامانه‌های استنتاج فازی در مراحل ۵ و ۹ و ۱۰ و ۱۳ و ۱۴ به‌شدت افت می‌کند. در مرحله ۵ مهاجم اقدام به حمله مجدد به میزبانی کرده است که قبلاً به آن نفوذ کرده است. در مرحله ۹، مهاجم پس از این که در مرحله قبل توانست به زیر-شبکه ۱۹۲,۱۶۸,۴.X نفوذ کند، مسیر حمله خود را تغییر داد و میزبان دیگری را در زیرشبکه ۱۹۲,۱۶۸,۲.X هدف قرارداد. در مراحل ۱۰ و ۱۳، مهاجم اقدام به نفوذ در زیرشبکه‌هایی کرده است (۱۹۲,۱۶۸,۳.X و ۱۹۲,۱۶۸,۵.X) که مقصد نهایی در آن زیرشبکه‌ها موجود نیست. در مرحله ۱۴، مهاجم از میزبانی به‌عنوان مقصد استفاده کرده است که در چند مراحل قبل کنترل آن را به‌دست آورده است. توجه داشته باشید آنچه در موارد فوق رخ می‌دهد (حمله به طیف زیادی از زیرشبکه‌ها)، موجب گم‌شدن الگوی حمله و درنتیجه کاهش بازدهی می‌گردد (روش ترکیب قابلیت و فرصت مبتنی بر سامانه‌های استنتاج فازی قادر نیست تا مقصد حقیقی حمله را تشخیص دهد). در ارزیابی روش مبتنی بر ترکیب فازی برای حملات مخفی از سناریوی حمله جدول (۵) استفاده‌شده است، و در این سناریوی حمله گام‌های مخفی میان گام ۲ و ۳، باعث ضعف روش ترکیب قابلیت و فرصت مبتنی بر سامانه‌های استنتاج فازی در شناسایی الگوی حملات و درنتیجه باعث کاهش دقت تجسم می‌شود؛ اما پس از مرحله ۳ مجدداً در مراحل ۴ و ۵، الگوی حملات شناسایی‌شده و برای مقصد نهایی دقت تجسم بیش‌تر می‌شود.

- ترکیب قابلیت و فرصت بر اساس مدل انتقال باور در برابر حملات با سطح تأثیر بالا در حالت معمولی دارای دقت بالایی است؛ اما این الگوریتم برای شبکه‌هایی، با تعداد زیاد میزبان‌ها و پیکربندی‌های یکسان مؤثر عمل نمی‌کند. درحالی‌که حملات با سطح تأثیر پایین موجب کاهش شدید عملکرد روش ترکیب قابلیت و فرصت بر سامانه‌های استنتاج فازی می‌گردد، در مورد روش ترکیب قابلیت و فرصت بر اساس مدل انتقال باور ماجرا متفاوت است. در این روش رتبه حمله میزبان‌های جدید به‌منظور گمراهی، موجب کاهش رتبه‌ی سایر میزبان‌ها نمی‌گردد؛ بنابراین از مزیت‌های روش ترکیب قابلیت و فرصت بر اساس مدل انتقال باور این است که تحت تأثیر این‌گونه حملات (سطح تأثیر پایین) قرار نمی‌گیرد و دچار انحراف نمی‌شود. عملکرد روش ترکیب قابلیت و فرصت بر اساس مدل انتقال باور در حملات مخفیانه شبیه به روش ترکیب قابلیت و فرصت بر سامانه‌های استنتاج فازی است.

۵- نتیجه‌گیری

در این مقاله معماری جدید برای تجسم حملات سایبری مبتنی بر آگاهی از وضعیت آینده و ارزیابی تأثیر معرفی گردید که به تجسم وضعیت‌های آینده یا همان آینده‌های قابل‌باور می‌پردازد. این آینده‌های قابل‌باور نیز در همین معماری مورد ارزیابی اثر قرار گرفته است. با اجرای موازی الگوریتم آگاهی از وضعیت آینده و ارزیابی تأثیر، برآوردی از وضعیت آینده صورت‌گرفته و یک نمره تحت عنوان قابلیت اطمینان ارائه شد. این تخمین‌ها بر اساس امتیاز قابلیت اطمینان وزن گرفته و با استفاده از نظریه‌های مشتق‌شده از دمپستر شافر ترکیب شده‌اند و برآوردی از وضعیت نهایی یک شیء را ارائه داده‌اند. در ادامه برای دست‌یابی به افزایش دقت تجسم در پیش‌بینی به موقع و دقیق اهداف احتمالی حمله به ترکیب مؤلفه‌هایی چون قابلیت، فرصت، رفتار و نیت پرداخته شد. به‌دلیل اهمیت ترکیب قابلیت و فرصت در نمایش نیت و رفتار مهاجم در این کار تحقیقی این دو مؤلفه باهم با دو روش فازی و مدل باور ترکیب شده‌اند. نتایج نشان داده است که ترکیب قابلیت و فرصت بر اساس مدل انتقال

باور در برابر حملات با سطح تأثیر بالا در حالت معمولی دارای دقت بالایی است و زمانی که شبکه، دیوار آتشی با قواعد سخت‌گیرانه و سرویس‌های کمکی محدودتری دارد، مؤثرتر است. این درحالی است که حملات با سطح تأثیر پایین موجب کاهش شدید عملکرد روش ترکیب قابلیت و فرصت بر سامانه‌های استنتاج فازی می‌گردد، در مورد روش ترکیب قابلیت و فرصت بر اساس مدل انتقال باور ماجرا متفاوت است. علاوه‌براین به این نتیجه رسیدیم که برای حملاتی که از الگوهای پایه منحرف می‌شوند، نظیر نویزها یا حملات مخفیانه روش ترکیب قابلیت و فرصت مبتنی بر استنتاج فازی می‌تواند از روش ترکیب قابلیت و فرصت بر اساس مدل انتقال باور استفاده کند و یا اگر این انحراف موقتی است مجدداً الگو را استخراج کند.

یکی از کارهای آینده بررسی کارایی این معماری و پارامترهای معرفی‌شده در الگوریتم‌های باورسنج در هر مرحله حمله با استفاده از دادگان‌های وسیع است. ارائه الگوریتم‌هایی برای ارزیابی اثر وضعیت‌های فعلی و آینده و ترکیب مؤثرتر الگوریتم‌های باورسنج می‌توانند از مسائل مطرح آینده باشند.

۶- مراجع

[1] K. Dadashtabar, A. J. Rashidi and H. Shirazi, " A new pattern for improvment of situation awareness beasd on information fusion," 6'th National conference in electronic warfare, 2014.(in persian)

[2] K. Dadashtabar, A. J. Rashidi, and H. Shirazi, "A new model for projection of multi stage cyber attack," 2'th National symposium in cyber defence, 2015. (in persian)

[3] K. Dadashtabar, A. J. Rashidi, and H. Shirazi, "a new architecture for impact projection of cyber attacks based on high level information fusion in cyber command and control," journal of electronical & cyber defence, vol. 2, no. 4, 2015, no. 8, (in persian)

[4] X. Qin and W. Lee, "Discovering novel attack strategies from INFOSEC alerts, in Data Warehousing and Data Mining Techniques for Cyber Security, Springer, pp. 109–157, 2007.

[5] J. Wu, L. Yin, and Y. Guo, "Cyber-attacks prediction model based on Bayesian network, presented at the Proceedings of the 2012 IEEE 18th International Conference on Parallel and Distributed Systems, pp. 730–731, 2012.

[6] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," in Proceedings of the IEEE Symposium on Security and Privacy, pp. 154–163, (Oakland, CA, USA), 1997.

[7] P. G. Neumann and D. B. Parker, "A summary of computer misuse techniques," in Proceedings of the 12th National Computer Security Conference, pp. 396–407, (Baltimore, Maryland, USA), 1989.

[8] S. Vidalis and A. Jones, "Using vulnerability trees for decision making in threat assessment," tech. rep. University of Glamorgan, School of Computing, Wales, UK, June 2003.

[9] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in Proceed-ings of the 1998 workshop for new security paradigms, pp. 71–79, (New York, NY, USA), 1998.

[10] F. Valeur, G. Vigna, C. Kruegel, and R. A. Kemmerer, "Comprehensive approach to intrusion detection alert correlation," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, pp. 146–169, 2004.

[11] P. Porras, M. Fong, and A. Valdes, "A mission impact based approach to infosec alarm correlation," in Recent Advances in Intrusion Detection, 5th International Symposium, RAID 2002. Proceedings (Lecture Notes in Computer Science Vo. 2516), pp. 95 – 114, (Zurich, Switzerland), 2002.

[12] J. A. Brian, "Virtual Terrain Assisted Impact Assessment for Cyber Attacks," Rochester, New York, July 2007.

[13] S. H. Chien and C. S. Ho, "A Novel Threat Prediction Framework for Network Security," in Advances in Information Technology and Industry Applications, Springer, pp. 1–9, 2012.

[14] J. Holsopple, S. J. Yang, and M. Sudit, "TANDI: threat assessment of network data and information, presented at the Defense and Security Symposium, p. 62420, 2006.

[15] C. Cipriano, A. Zand, A. Houmansadr, C. Kruegel, and G. Vigna, "Nexat: A history-based approach to predict attacker actions," presented at the Proceedings of the 27th Annual Computer Security Applications Conference, pp. 383–392, 2011.

[16] Z. Li, J. Lei, L. Wang, and D. Li, "A data mining approach to generating network attack graph for intrusion prediction, presented at the Fuzzy Systems and Knowledge Discovery, Fourth International Conference on FSKD 2007, vol. 4, pp. 307–311, 2007.

[17] P. Liu, W. Zang, and M. Yu, "Incentive based modeling and inference of attacker intent," objectives and strategies, ACM Trans. Inf. Syst. Secur. TISSEC, vol. 8, no. 1, pp. 78–118, 2005.

[18] K. Tang, M. Zhao, and M. Zhou, "Cyber Insider Threats Situation Awareness Using Game Theory and Information Fusion based User Behavior Predicting Algorithm, J. Inf. Comput. Sci. vol. 8, no. 3, pp. 529–545, 2011.

[19] F. Gao, J. Sun, and Z. Wei, "The prediction role of hidden markov model in intrusion detection," presented at the Electrical and Computer Engineering, IEEE CCECE 2003, vol. 2, pp. 893–896, 2003.

[20] D. Man, Y. Wang, Y. Wu, and W. Wang, "A combined prediction method for network security situation," International Conference on presented at the Computational Intelligence and Software Engineering (CiSE), pp. 1–4, 2010.

[21] S. J. Yang, A. Stotz, J. Holsopple, M. Sudit, and M. Kuhl, "High level information fusion for tracking and projection of multistage cyber-attacks, Inf. Fusion, vol. 10, no. 1, pp. 107–121, 2009.

[22] D. S. Fava, S. R. Byers, and S. J. Yang, "Projecting cyber attacks through variable-length markov models, Inf. Forensics Secur. IEEE Trans. On, vol. 3, no. 3, pp. 359–369, 2008.

[23] J. Holsopple, J. Yang, and M. Sudit, "TANDI: Threat assessment of network data and information," in Proceedings of SPIE, Defense and Security Symposium, vol. 6242, pp. 114–129, April 2006.

[24] D. Fava, J. Holsopple, S. J. Yang, and B. Argauer, "Terrain and behavior modeling for projecting multistage cyber attacks," 10th International Conference in Information Fusion, pp. 1–7, 2007.

[25] J. Holsopple and S. Yang, "FuSIA: Future situation and impact awareness," in Proceedings of 11th International Conference on Information Fusion, pp. 1–8, 2008.

Journal Of Electronical & Cyber Defence
Vol. 3, No. 2, 2015, Serial No. 10

Projection of Muli Stage Cyber Attack Based on Belief Model and Fuzzy Inference

A. J. Rashidi, K. Dadashtabar Ahmadi, F. Samsami Khodadad *
Amol new University of Technology
(Received: 20/03/2015, Accepted: 01/09/2015)

ABSTRACT

Determination of plausible future of ungoing cyber attacks enables the security analyst to make the best defense decisions based on achieved plausibility level. To achive the plausibility level of a situation, situational estimation and high level information fusion are used. In high level information fusion, for situation awareness of future and impact assessment of cyber attacks four componnets of projecting, behaviour, capability, opportunity and intent are used.

Almost all of the models used for projecting multi stage cyber attacks assuming the four components independent from each other to simplify the implementation. Thus, they ignored the impact of the components on each other and their combination ability in projecting multi stage cyber attacks.In this paper, we have presented a scheme based on belif model and fuzzy inference. Finally, the scheme has been evaluated using valid dataset, high stealth attacks and high impact and low impact attacks. The simulation results for the defined scenarios show accuracy increasy in projecting multi-stage cyber attacks.

Keywords: Situationa Awareness, Cyber Attack, Cyber Defense, Belief Model, Fuzzy Inference

* Corresponding Author Email: samsami.farid@gmail.com