Journal Of Electronical & Cyber Defence
Vol. 2, No. 4, 2015, Serial No. 8

A new architecture for impact projection of cyber-attacks based on high level information fusion in cyber command and control

K. Dadashtabar Ahmadi[1*], A. J. Rashidi[2], M. Barari[3]

1- PhD Student, Malek Ashtar University of Technology

2- Associated professor, Malek Ashtar University of Technology

3- Assistant professor, Malek Ashtar University of Technology
(Received: 22/09/2013, Accepted: 11/05/2015)

ABSTRACT

Efficient and sustainable command and control networks have appropriate management and security policies and strong security components. In this kind of networks, even professional invaders for access to sensitive files or compromising entities such as host, user, service and network, require the implementation of multi-stage attacks. Therefore using multi-stage information fusion and impact projection of cyber-attacks, it is possible to prevent from interruption in network tasks and lose of important data at very early stages of them. In this paper, while providing a new architecture of the impact projection of cyber-attacks, with simulation of different patterns of this architecture in simulation environment specified for random processes, it will be shown how this architecture using high level information fusion led to improve cyber situational awareness. For simulation of random processes in the environment will be shown how this architecture using high level data integration led to the recovery of knowledge positions will be backed cyber.

Keywords: Information Fusion, situational Awareness, Cyber Defense, Impact projection.

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

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال دوم، شماره ۴، زمستان ۱۳۹۳، ص ۱۴-۱

ارائه یک معماری جدید برای تجسم اثرات حملات سایبری مبتنی‌بر ادغام اطلاعات سطح بالا در فرماندهی و کنترل سایبری

کوروش داداش‌تبار احمدی[1*]، علی‌جبار رشیدی[2]، مرتضی براری[3]
۱- دانشجوی دکتری، مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک‌اشتر
۲- دانشیار، مجتمع دانشگاهی برق و الکترونیک، دانشگاه صنعتی مالک‌اشتر
۳- استادیار، مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک‌اشتر
(دریافت: ۹۲/۰۶/۳۱؛ پذیرش: ۹٤/۲/۲۱)

چکیده

شبکه‌های فرماندهی و کنترل کارا و پایدار دارای مدیریت و سیاست‌های امنیتی مناسب بوده و از اجزاء امنیتی محکمی برخوردارند. در این نوع شبکه‌ها حتی مهاجمان حرفه‌ای نیز برای دستیابی به فایل‌های حساس یا به خطر انداختن موجودیت‌هایی چون میزبان، کاربر، سرویس و هسته شبکه نیازمند اجرای حملات هماهنگ و چندمرحله‌ای هستند. بنابراین با استفاده از ادغام اطلاعات و تجسم اثر حملات سایبری چندمرحله‌ای می‌توان در همان مراحل اولیه از ایجاد وقفه در عملیات شبکه و از دست دادن داده‌های مهم جلوگیری نمود. در این مقاله ضمن ارائه یک معماری جدید از تجسم اثرات حملات سایبری با شبیه‌سازی الگوهای مختلف این معماری در محیط شبیه‌سازی مختص فرایندهای تصادفی نشان داده خواهد شد که چگونه این معماری با استفاده از ادغام اطلاعات سطح بالا منجر به بهبودی آگاهی وضعیتی سایبری می‌شود.

واژه‌های کلیدی: دفاع سایبری، تجسم اثرات، ادغام اطلاعات، آگاهی وضعیتی

۱- مقدمه

در حال حاضر برای تشخیص و شناسایی حملات به‌صورت خودکار و گزارش به‌موقع رویدادهای ناشی از تهدیدات سایبری، از سامانه آشکارسازی مبتنی بر حالت، سامانه آشکارسازی ناهنجاری آماری، سامانه تحلیل ترافیک، سامانه تشخیص الگوهای رفتاری[1] و قالب الگوی شناخته‌شده استفاده می‌شود. این‌گونه سامانه‌ها دائما در حال جستجو و یافتن رفتارهای غیرعادی ناشی از حملات سایبری هستند و بر اساس تغییر رفتار در طول زمان و مقایسه آن با رفتارهای قبلی یک رویداد در سامانه عمل می‌کنند [۱]. با ادغام اطلاعات حاصل از عامل‌های توزیع‌شده ناهمگن در سامانه‌های تشخیص و شناسایی حملات سایبری، امکان توسعه سامانه مذکور با قابلیت اطمینان بالا برای شناسایی، ردگیری و ارزیابی وضعیت فضای سایبری، فراهم می‌شود [۲]. فناوری ادغام داده چندحسگری، چارچوب عملکردی مهمی را برای ایجاد آگاهی وضعیتی در نسل آینده سامانه‌های تشخیص و شناسایی حملات سایبری فراهم خواهد کرد [۳]. اِندسلی[2] آگاهی وضعیتی را در سه سطح درک[3]، فهم[4] و تجسم مطرح نموده است [۴]. درک نشانه‌ها، یک موضوع حیاتی است و بدون درک اولیه اطلاعات مهم، احتمال شکل‌گیری تصویر نادرست از یک موضوع به شدت افزایش می‌یابد. در این سطح به این سوال پاسخ داده می‌شود که واقعیت‌های فعلی چیست. آگاهی وضعیتی مفهومی، فراتر از درک یا توجه صرف به اطلاعات است، بلکه یکپارچه‌سازی تکه‌های مختلف اطلاعات؛ تعیین ارتباط میان آن‌ها و اهداف کاربر را نیز شامل می‌شود. این موضوع درست شبیه تفاوت میان سطح بالایی از درک مطلب نسبت به خواندن لغات تنها است. در مجموع سطح فهم، به این سوال پاسخ می‌دهد که چه‌چیزی اتفاق می‌افتد. در بالاترین سطح آگاهی وضعیتی که مبتنی‌بر بالاترین سطح درک از وضعیت است، توانایی آینده‌نگری رویدادهای مربوط به هر

* رایانامه نویسنده مسئول: Dadashtabar@mut.ac.ir

۱- تا رفتارهای غیرعادی در یک محیط شناسایی شود

2- Dr. Mica Endsley

3- Perception

4- Comprehension

وضعیت و کاربر مطرح خواهد بود. این توانایی امکان تصمیم گیری به‌موقع را برای تجسم رویدادهای پویای جاری به سمت رویدادهای آتی مورد انتظار، فراهم می‌سازد.

بر اساس ویژگی‌های حوزه سایبری، هدف آرمانی در این حوزه از فعالیت‌های دفاع سایبری، دست‌یابی به سامانه جدیدی برای تشخیص، شناسایی و تجسم حملات سایبری است.

عمده کارهای صورت‌گرفته در این زمینه، همبستگی و ادغام هشدارهای سامانه‌های تشخیص نفوذ بوده است [۵]. فلسفه کارهای پیشین براین نکته استوار بود که به‌جای نگهداری حجم انبوهی از هشدارها، با همبستگی و ادغام آن‌ها، آگاهی وضعیتی بهتری از حملات سایبری ایجاد خواهد شد. با این وجود هنوز هم سامانه‌های کنونی دفاع سایبری فاصله زیادی با اهداف اصلی دفاع سایبری، شناسایی حمله، کشف روابط بین حملات و پیش‌بینی اثرات حمله دارند. برای کاهش این فاصله می‌توان از ادغام اطلاعات در ارتقاء آگاهی وضعیتی و پیش‌بینی اثرات حملات سایبری در حجم انبوه داده‌های اخذشده از منابع مختلف، استفاده نمود [۱و۶]. با وجود تلاش‌های بسیار در بکارگیری و توسعه ادغام اطلاعات سطح بالا، این نوع ادغام نه‌تنها در حوزه سایبری بلکه در سایر حوزه ها نیز در مراحل ابتدایی تحقیق است* [۷]. با توجه به مطالب ذکرشده، در این مقاله قصد داریم با استفاده از معماری تجسم اثرات حملات سایبری مبتنی بر ادغام اطلاعات، بتوانیم آسیب‌پذیری‌های شبکه را که برای حمله‌کنندگان جذاب هستند تجزیه‌وتحلیل نماییم، تهدیدات را شناسایی و در نهایت، حملات سایبری چندمرحله‌ای و هماهنگ را ردگیری کرده و تجسمی از وضعیت آینده این نوع حملات ارائه دهیم.

۲- آگاهی وضعیتی سایبری و ادغام اطلاعات سطح بالا

سطوح آگاهی وضعیتی برای همه حوزه‌ها به یک صورت تعریف شده و ماهیت آگاهی وضعیتی و سازوکارهای مورد استفاده برای اکتساب آن نیز می‌تواند به‌صورت کلی تعریف گردد؛ ولی میزان نیاز به آن در هر حوزه بنا به نوع عملیات، اهمیت، حساسیت و عناصر تشکیل‌دهنده آگاهی وضعیتی با یکدیگر متفاوت است [۲۳]. رویکردهای حال حاضر در زمینه کسب آگاهی وضعیتی سایبری شامل تحلیل آسیب‌پذیری (با استفاده از گراف‌های حمله)، آشکارسازی نفوذ و همبستگی هشدارها، تجزیه و تحلیل روند حمله، تحلیل‌های علت و معلولی(پیمایش معکوس یک نفوذ)، ارزیابی خسارات (با استفاده از گراف‌های وابسته) و پاسخ به نفوذ است. با توصیف ارائه‌شده در این بخش می‌توان گفت، برای ایجاد یک دفاع سایبری کامل نیاز به آگاهی وضعیتی است که حداقل از هفت جنبه زیر تشکیل شود [۲۳ و ۶]:

- آگاهی از وضعیت کنونی: منظور از آگاهی وضعیت کنونی همان درک وضعیت است که شامل دو بخش تعیین[1] و شناسایی[2] است. منظور از تعیین، تعیین نوع حمله است که قاعدتا باید به سوالاتی چون، منبع حمله کجاست؟، مهاجم کیست؟ و هدف حمله چیست؟، پاسخگو باشد. منظور از شناسایی فقط شناسایی "یک حمله" رخ داده شده است. درک وضعیت، فراتر از آشکارسازی نفوذ است چرا که سامانه‌های مبتنی بر آشکارسازی نفوذ متشکل از حسگرهایی هستند که توانایی تعیین و شناسایی حمله را ندارند و فقط بخشی از رویدادهایی که ممکن است جزئی از یک حمله باشند را تشخیص می‌دهند؛ با این توصیف می‌توان گفت آشکارسازی نفوذ، عنصر اولیه درک وضعیت است.

- آگاهی از اثرات حمله: آگاهی از اثرات حمله همان تحلیل آسیب‌پذیری و ارزیابی اثر[3] است. تحلیل آسیب‌پذیری در این جنبه گسترده‌تر از ارزیابی اثر بوده و در این حالت است که تجسم اثر آینده حملات نیز محقق خواهد شد [۱۱].

- آگاهی از وضعیت آینده: در این جنبه، ردگیری وضعیت[4] یکی از مهم‌ترین مولفه‌ها است.

- آگاهی از رفتار متخاصم: مهم‌ترین مولفه این جنبه از آگاهی وضعیتی، درک نیات مهاجم است. این امر با کنترل و مراقبت رفتاری متخاصم و بررسی آن با وضعیتی که در آن است و وضعیتی که ایجاد خواهد شد، صورت می‌گیرد.

- آگاهی از چرایی و چگونگی وضعیت کنونی ایجادشده جنبه دیگری است که نیاز به تحلیل علت و معلولی دارد**.

- آگاهی از میزان کیفیت و اعتماد به اطلاعات جمع‌آوری شده، منجر به دانایی و هوشمندی تصمیمات خواهد شد.

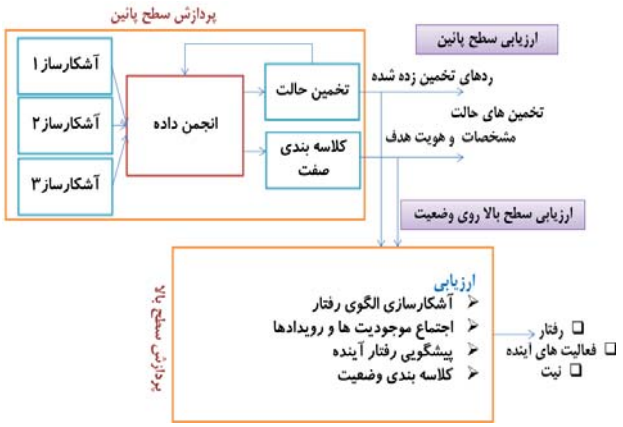
* ادغام اطلاعات سطح بالا برای پیش‌بینی حرکات دشمن در آینده، ارتقاء آگاهی از سطح تهدید و پیش‌بینی نیات حمله کننده سایبری [۱۵].

** نظیر پیمایش معکوس یک نفوذ

1- identification
2- recognition
3- impact assessment
4- Situation tracking

- ارزیابی آینده قابل باور: در این جنبه، از فناوری‌های متعددی برای تجسم اقدامات، فعالیت‌های مهاجم و تجسم مسیرهای محتمل مورد حمله استفاده می‌شود. درک نیت، فرصت و توانمندی مهاجم نیز از جمله محورهای کلیدی جنبه مذکور است.

با استفاده از آگاهی وضعیتی سایبری و ارزیابی وضعیت، روابط بین موجودیت‌ها کشف‌شده، رویدادهای مهم تعیین و فعالیت‌های اثرگذار، مشخص خواهند شد. همچنین برای ایجاد آگاهی وضعیتی، امکان استفاده از ارزیابی اثر امکان تخمینی از سطح تهدید فراهم و پیامدهای حاصل از تصمیمات خاص، پیش‌بینی و میزان آسیب‌پذیری دارائی‌ها تخمین زده خواهد شد [۷]. برای بهبود آگاهی وضعیتی سایبری در سامانه‌های دفاع سایبری، از ادغام اطلاعات استفاده می‌شود که در دسته‌بندی انجمن جهانی ادغام منابع[1]، ادغام اطلاعات به دو دسته ادغام اطلاعات سطح بالا[2] و سطح پائین[3] تقسیم شده است. در ادغام سطح پائین اطلاعات، موضوعاتی چون طبقه‌بندی، شناسایی و ردگیری هدف؛ جزء بخش‌های اصلی محسوب می‌شوند، این درحالی است که در ادغام سطح بالا اثر، وضعیت و پالایش فرایند ادغام، مهم‌ترین موضوعات هستند [۲۲]. ادغام سطح بالا با اطلاعات انتزاعی نمادین نظیر تهدید، نیت و اهداف روبرو است و با استفاده از کنترل، درک وضعیت و روابط حاکم بر محیط ادغام، رفتار، نیات و فعالیت‌های آتی یک رویداد استخراج



شکل (۱). مولفه‌های اصلی سامانه ادغام اطلاعات سطح پائین و بالا [۷]

1- http://www.isif.org
2- High-Level Information Fusion
3- Low-Level Information Fusion

می‌شود [۲۱] . تمایز بین دو دسته ادغام اطلاعات سطح بالا و پائین را می‌توان در شکل (۱) مشاهده نمود.

۳- تجسم اثرات حملات سایبری

با ایجاد آگاهی وضعیتی سایبری در قلب سامانه‌های فرماندهی و کنترل، این امکان فراهم خواهد شد تا بتوان درک نمود: الف) انواع روش‌های حمله چیست و رفتارهای حملات سایبری چگونه مدل می‌شود؟ ب) تا چه حد امکان تشخیص و پیش‌بینی حملات سایبری در همان مراحل اولیه حمله با دقت بالا وجود دارد؟ ج) از چه روش‌هایی برای ارزیابی سطح تهدید، علیه موجودیت‌های تحت خطر شبکه استفاده می‌شود؟ د) موجودیت‌های تحت خطر را براساس سطح تهدید، چگونه اولویت‌بندی می‌کنند؟

اصولا برای ایجاد و بهبود یک سامانه آگاهی وضعیتی سایبری، از سه مرحله اساسی نشان‌داده‌شده در شکل (۲) استفاده می‌شود. این انتظار از سامانه فوق وجود دارد که امکان تعیین، ردگیری و تجسم حملات سایبری چندمرحله‌ای را در همان مراحل اولیه با دقت بالا فراهم نماید؛ ضمن این‌که از دسترسی به داده حیاتی و سرقت اطلاعات با مدیریت به‌موقع و دقیق هشدارها جلوگیری می‌شود.

شکل (۲). فرایند طراحی در سه مرحله [یافته تحقیق]

مرحله اول، آشکارسازی فعالیت‌های بدخواهانه: هشدارها براساس پایش بسته‌های ترافیکی تولید شده و با تخمین و اجتماع هشدارهای ناشی از رفتارهای غیرمتعارف، مسئله شناسایی حملات حل می‌شود [۳۰].

مرحله دوم، همبستگی و ردگیری: در مرحله همبستگی هشدارها این احتمال وجود دارد که همبستگی نادقیق، همراه با افزونگی و بعضاً متعارض باشد، بنابراین نیاز است تا از ادغام اطلاعات

در سطح پائین استفاده شود. هدف اجتماع هشدارها، رهگیری و ردگیری حملات سایبری چندمرحله‌ای است. بنابراین نیاز است تا در این بخش، تخمینی از رد حملات و ارزیابی از اثرات حملات بر روی شبکه داشت [۳۰].

مرحله سوم، ارزیابی اثرات و تجسم تهدید: تجسم تهدید بر اساس آسیب‌پذیری و پیکربندی شبکه و رفتارهای مهاجم صورت می‌گیرد و هدف از این تجسم، پیش‌بینی اقدامات حملات درآینده است. این که کجای شبکه مورد حمله واقع خواهد شد؟ چه سوء استفاده‌ای از اجرای این حملات صورت‌می‌گیرد؟ و هدف از ارزیابی اثر، تخمین خسارات بر اساس حملات کنونی و آینده است. چالشی که تجسم تهدید در فضای سایبری با آن مواجه است این است که در فضای سایبری برخلاف فضای فیزیکی، نیت حمله‌کننده و قابلیت‌هایش ممکن است متضاد باشد و احیانا در یک مقیاس زمانی بسیار کوتاه تغییر کند. بنابراین ارائه مدلی برای تجسم و ارزیابی حملات سایبری بر اساس رفتارهای مهاجم و داده‌های تحت خطر شبکه ضروری است [۲۸]. با تجسم حملات سایبری مبتنی‌بر ادغام اطلاعات برای ارزیابی حملات سایبری می توان به سوالات فهرست‌شده زیر بهتر و شفاف‌تر پاسخ داد: الف) هم‌اکنون چه تعداد و در کجا حمله‌ای در حال انجام است؟ ب) چه دارائی‌هایی از شبکه تحت تهدید قرار دارند؟ ج) با چه دشمن و روش حمله ای مواجه هستیم؟ د) قصد و نیت مهاجم چیست؟ ه) اگر حمله‌ای موفقیت‌آمیز باشد، چه چیزی صدمه خواهد دید؟ و) با توجه به وضعیت کسب‌شده و پیش‌بینی‌شده آیا ساز و کار دفاعی مناسبی برای مقابله و خنثی‌سازی حملات وجود دارد؟

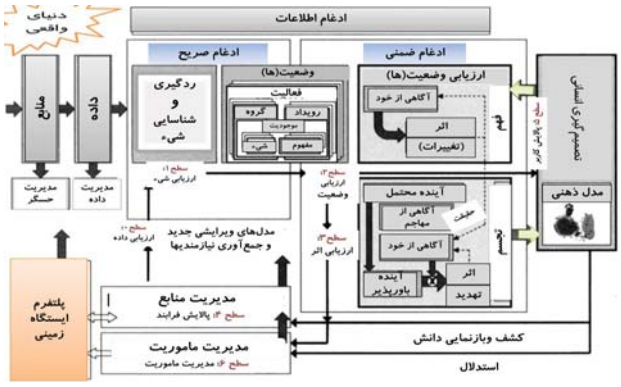
۴- مدل فرایندی ادغام اطلاعات در دفاع سایبری

به خاطر درک ناقص از فرایند ادغام داده و عدم استفاده درست از آن در دفاع سایبری، تاکنون موفقیت های چشم‌گیری در به‌کارگیری فرایند ادغام داده در فضای سایبری کسب نشده است. علاوه‌براین، به‌دلیل پیچیدگی بالای این حوزه نیاز است تا ادغام داده از منابع مختلف در سطح وسیعی صورت گیرد و الگوریتم‌های ترکیبی یا جدیدی از ادغام داده به‌کار گرفته شود که آگاهی لازمه از وضعیت را در سطوح مختلف ایجاد نماید و این آگاهی باید محتوی‌محور باشد. همچنین با توجه به این‌که سطوح مختلفی برای ادغام داده وجود دارد، الگوریتم‌های مختلفی نیز برای ادغام در سطوح مختلف استفاده می‌شود. بنابراین با استفاده از استنتاج های حاصل از ترکیب داده می‌توان به سوالات مختلف به‌صورت شفاف برای کسب آگاهی وضعیتی بهتر پاسخ مناسبی ارائه داد. علاوه براین؛

در این مرحله با درک صحیح ارتباط بین مولفه‌های پایه و سطوح ادغام داده در دفاع سایبری، و چگونگی ایجاد ابزارهای جدید دفاع سایبری مبتنی بر ادغام چند سطحی و پاسخ به سوالات در سطوح مختلف برای ایجاد آگاهی وضعیتی بهتر می توان مدلی مناسب به مانند آنچه در شکل (۳) نشان‌داده شده ارائه نمود. با در نظر گرفتن این نکته که ارزیابی وضعیتی، یک تابع ماشینی است و آگاهی وضعیتی، یک تابع شناختی محسوب می‌شود، برای طراحی یک سامانه آگاهی وضعیتی مناسب، در این تحقیق از مدل اندسلی در پردازش نیمه‌خودکار آگاهی وضعیتی استفاده شده است.

شکل (۳). ارتباط بین مولفه‌های پایه و سطوح ادغام [۲۷]

با بهره‌گیری از مولفه‌هایی چون ارزیابی وضعیتی، آگاهی وضعیتی و مدل ادغام گروه اطلاعاتی ادغام داده، یک مدل ارزیابی وضعیتی ادغام اطلاعات ترکیبی، مناسب حوزه سایبری حاصل خواهد شد [۲۳]. در شکل (۴) نمایی از این مدل به‌همراه فعالیت‌های مربوط به یک وضعیت که کاربر با آن درگیر است، نظیر استدلال(درک)، ارزیابی (فهم) و پیش‌بینی وضعیت آینده (تجسم) نشان داده شده است.



شکل (۴). مدل پیشنهادی برای ادغام اطلاعات در تشخیص، شناسایی و تجسم حملات سایبری [یافته تحقیق]

۴-۱- مدل پیشنهادی مبتنی بر ادغام اطلاعات سطح بالا

تاکنون تمرکز اکثر محققین بر روی سامانه‌های آشکارساز نفوذ و ادغام خروجی‌های این سامانه‌ها بوده تا بتوانند درک بهتری از فعالیت‌های مخرب در شبکه ایجاد کنند. این درحالی است که برای آگاهی کلی از وضعیت جاری شبکه و تجسم اقدامات آینده متخاصم، الگوی مناسبی استخراج نشده است. بنابراین، استخراج یک مدل رفتاری بر اساس مهارت‌ها و انگیزه‌های متفاوت هکرها برای نیل به چنین هدفی ضروری است [۲۰].

علاوه‌براین، اغلب ابزارهای تجاری برای ارزیابی و سنجش تهدیدات، از هشدارهای خاصی و یا هشدارهای رخداده بر روی ماشین‌های مشابه بهره می‌برند. بنابراین به رویکرد جدیدی نیاز است تا اثرات و تهدیدات ناشی از حملات سایبری گسترده‌شده بر روی چندین ماشین نیز مورد ارزیابی و سنجش قرار گیرد. برای حل چالش‌های فوق می‌توان از سطح سوم مدل ادغام ارائه‌شده در شکل (۴) استفاده نمود. در ادامه، چگونگی استفاده از این سطح برای ارزیابی اثرات و تهدیدات سایبری تشریح خواهد شد. همچنین در همین بخش با استفاده از الگوها یا همان مدل‌های تصادفی، مدل جدیدی برای سنجش تهدید و اثر حملات سایبری چندمرحله‌ای پیشنهاد خواهد شد. در مدل شکل (۴)، ادغام سطح ۳ با سه ویژگی توانمندی، فرصت و نیت یک‌حمله کننده سایبری سروکار دارد. در این سطح با ترکیب این سه ویژگی می‌توان آنچه را که یک حمله کننده سایبری طراحی و برنامه‌ریزی کرده تا کاری را انجام دهد پیش‌بینی نمود و تخمینی از اثری را که هر یک از اقدامات مهاجم ایجاد خواهد کرد، ارائه داد. در ادامه هر کدام از این سه ویژگی ادغام سطح ۳، تجزیه و تحلیل شده و این‌که چگونه آن‌ها می‌توانند در حملات سایبری به‌کار برده شوند، مورد بحث قرار می‌گیرد.

۴-۱-۱- توانمندی

منظور از توانمندی در سطح ۳، ادغام اقداماتی است که یک مهاجم سایبری توانایی انجام آن را دارد. توانمندی 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 به عنوان یک کاربر عادی حوزه سایبری مطرح است و به‌سادگی اسکریپت‌های مربوط به نفوذ را دانلود می‌کند تا مهاجم پیشرفته‌ای که از دانش و آگاهی فوق العاد 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 به احتمال زیاد پیشرفته‌تر بوده است و بنابراین سطح بالاتری از تهدید می‌تواند همراه با آن حمله باشد. با این وجود، 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 [۱۸].

۴-۱-۲- فرصت

منظور از فرصت، زمان لازم مهاجم برای اجرای حملات در مرحله بعدی حمله است. در تعیین فرصت می توان از میزان آسیب‌پذیری سامانه‌ای که قرار است مورد حمله قرار گیرد و اطلاعاتی که مهاجم در حال حاضر می‌تواند به آن‌ها دسترسی داشته باشد، استفاده کرد. فرض کنید یک مهاجم سایبری می‌داند چگونه خدماتی را بر روی یک سرور شناسایی کند تا از این طریق به قواعد و قوانین مدیریتی دسترسی پیدا کند. در حالی که مهاجم دارای توانمندی شناسایی آن خدمات است، نمی‌تواند آن خدمات را مورد سوءاستفاده قرار دهد مگر این‌که دقیقا 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 آن خدمات را پیدا خواهد نمود. اگر مهاجم از چگونگی استفاده از یک خدمات خاصی آگاه نباشد، پس فرصت استفاده از آن خدمات را هنوز خواهد داشت، اما احتمال وقوع این امر به دلیل اینکه مهاجم از توانمندی و توانایی محدودی در این زمینه برخوردار است اندک است [۱۲و۱۶].

۴-۱-۳- نیت

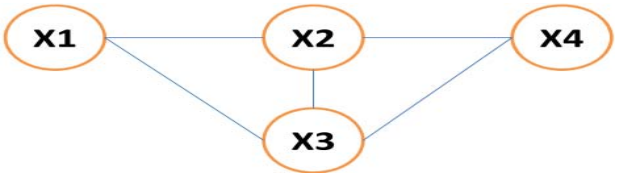
منظور از نیت؛ اقدامات و فعالیت‌های آتی یک مهاجم است و مهاجم با برنامه‌ریزی قبلی قصد انجام آن را دارد. در حوزه سایبری برخی از مهاجمین به‌عنوان مهاجم اخلاقی شناخته می‌شوند، چون آنها بدون اینکه دارای قصد و یا اهداف شرورانه و یا سوءنیت خاصی باشند به شبکه نفوذ می‌کنند. گرچه دیگر مهاجم‌ها وارد سامانه شده تا سرقت کنند، حذف کنند و یا اطلاعات خاصی را تحریف و تغییر دهند؛ با این توصیف تشخیص نیات مهاجمان حوزه سایبری بسیار مشکل است، مگر اینکه واقعا یک عمل شرورانه‌ای خاصی رخ داده باشد. وقتی مهاجمی گستردگی و تسلط خود را بر شبکه به‌دست

آورد، نیاز دارد تا هدف خویش را پیگیری نماید. متاسفانه 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 فایل‌های حیاتی را تغییر دهد و یا اینکه به سادگی سامانه را رها خواهد ساخت. در هر صورت اگر مهاجم شناخته‌شده‌ای باشد که اغلب کارهای شرورانه انجام می‌دهد، این احتمال وجود دارد که آن مهاجم دارای مقاصد و نیت‌های شرورانه‌ای است. با این وجود اگر هیچگونه اقدام شرورانه‌ای را انجام نداده باشد، تقریباً تعیین مقاصد و نیات آن مهاجم غیرممکن است [۹ و ۱۵].

۴-۱-۴- مدل‌سازی تصادفی در سنجش تهدید و اثرات حملات سایبری

بهره‌گیری از مدل‌سازی‌های تصادفی نظیر مدل‌های شبکه بیزین و مدل‌های مارکوف مخفی که در [۱۳] به تفصیل تشریح شده است، مبنای کار مدل‌سازی این بخش قرار گرفته است. درحالی‌که در [۱۳] تمرکز مدل‌سازی بر روی حملات تروریستی بوده است، ولی با گسترش و توسعه این ایده می‌توان از آن برای مدل سازی حملات سایبری نیز استفاده نمود. از شبکه‌های بیزین برای مدل‌سازی عدم قطعیت استفاده می‌شود. این مدل‌سازی بر این نکته تاکید دارد که اگر شواهد قبلی نشان‌دهنده آنچه باشد که می‌تواند در آینده اتفاق بیفتد، بنابراین می‌توان از آن برای پیش‌بینی آینده نیز استفاده کرد. حالت‌های اینگونه شبکه‌ها دارای احتمال معین و مشخص از وقوع و رخداد هستند. شبکه‌های بیزین با این حقیقت روبه‌رو هستند که احتمال وجود یک حالت از شبکه، به حالت‌ها و وضعیت‌های قبلی بستگی دارد. به عبارتی دیگر احتمال وجود آنها در حالت x، به مجموعه‌ای از حالت‌های قبلی y، p(x/y) بستگی دارد. شبکه های بیزین در حملات سایبری با تعریف یک مسیر عملکردی که در آن مهاجم توانایی نفوذ درشبکه را دارد، به کار گرفته می‌شوند [۱۹]. این مسیر عملکردی براساس انواع حملاتی که مهاجم می‌تواند انجام دهد و یا اطلاعات خاصی که نفوذگر در طول حمله خود به مخاطره می‌اندازد، تعریف می‌شود. فیلیپس و سویلر[1] در [۱۷] پیشنهاد می‌نمایند که این مسیر عملکردی می‌تواند بر اساس ساختار شبکه نظیر سرویس‌هایی که بر روی هر ماشین اجرا می‌شوند، پیکربندی شبکه، گروه‌های کاربری، پروفایل مهاجم و دیگر ویژگی‌های شبکه ایجاد شود. در طرح فوق هر یال مشخص کننده احتمال یک انتقال است، بنابراین محتمل‌ترین مسیر (و یا n تعداد مسیر احتمالی) می‌توانند با استفاده از الگوریتم‌های شناخته‌شده محاسبه شوند. از این روش می‌توان برای تخمین فرصت و نیت استفاده نمود. با استفاده از این نوع مدل‌سازی، پروفایل‌های مختلفی از مهاجم ایجاد خواهد شد که از آن می‌توان برای تخمین توانمندی یک مهاجم نیز استفاده کرد. با وجود اینکه این مسئله یک ایده بسیار جامع و فراگیر است، ممکن است برای استفاده از آن در شبکه‌های فرماندهی و کنترل، مشکلات جدیدی ایجاد شود. حتی اگر یک مسیر عملکردی برای شبکه پیچیده ایجاد شود، تعیین احتمالات، یک تکلیف یا وظیفه عادی و عامیانه محسوب نشده و این احتمالات توسط متخصصین موضوع اصلی باید به‌کارگرفته شوند، اما به‌دلیل پیچیدگی بالای آن، وقت‌گیر و نادقیق است. احتمالات فوق می‌توانند آموزش نیز داده شوند، اما با محدودیت داده‌ها و اطلاعات حمله سایبری مواجه هستند.

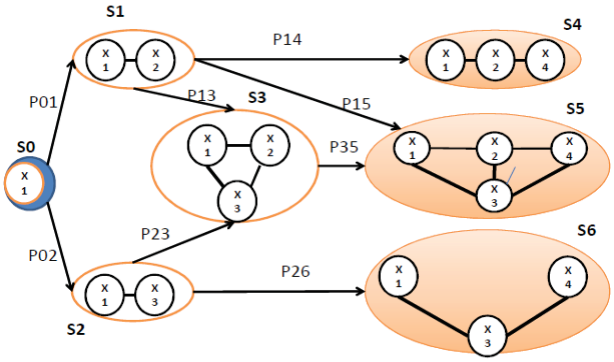
با توجه به این‌که حملات احتمالی سایبری به‌طور پیوسته رو به افزایش هستند، بنابراین ایجاد یک مسیر عملکردی بدون تغییر و ثابت عملا کارایی مدل را زیر سوال برده چراکه اطلاعات آموزشی تهیه‌شده برای پیش‌بینی آینده مفید واقع نخواهند شد. مؤلفان می‌پذیرند اگر سطوح تجمیع به‌صورت مناسبی انتخاب نگردند، (مثلاً سطح ماشین در برابر سطح شبکه فرعی)، این ایده ممکن است مقیاس‌پذیر نباشد. با این وجود، از ایده‌های این‌چنینی در جهت افزایش مقیاس‌پذیری استفاده شده تا با به‌کارگیری بلوک‌های ساختاری به‌طور خودکار، حداقل بخش‌هایی از مسیر عملکردی ایجاد شود. مدل مارکوف مخفی (HMM) از نوع مدل‌های رفتاری یک شبکه بیزین است که در آن، حالت کنونی فقط به حالت قبلی وابسته است و هر یال در یک (HMM) یا یک احتمال انتقالی مدل‌سازی می‌شود. چگونگی استفاده از این ایده از منبع [۲۶ و ۸] اخذ شده و در این مقاله به حوزه سایبری نگاشت شده است. شکل (۵)، یک مسیر بالقوه از حمله سایبری که در قالب الگوی حملات سایبری وجود دارد را نشان می‌دهد.



شکل (۵). یک مدل از حمله سایبری جاسازی شده در قالب الگوی حملات [یافته تحقیق]

در شکل(۶) نیز نشان داده خواهد شد که چگونه شکل مذکور به یک مدل مارکوف مخفی تبدیل شده است. به‌عنوان مثال، برای گذار از حالت S1 به حالت S3 با توجه به مسیر بالقوه حمله شکل (۵) فقط

1- Phillips and Swiler



شکل(۶). مدل‌سازی تصادفی با استفاده از مارکوف مخفی [یافته تحقیق]

امکان تخصیص احتمال p13 به‌خاطر تشکیل مسیر بین x2 و x1 و تخصیص احتمال p23 به‌خاطر تشکیل مسیر بین x3 و x1 وجود دارد.

زنجیره‌های مارکوف، از پراستفاده‌ترین فنون احتمالاتی در زمینه کشف نفوذ می‌باشند چرا که برحسب نرخ نفوذ و نرخ هشدارهای غلط، عملکرد بهتری را از خود نشان می‌دهند [۳۱]. دنیل فاوا در منبع [۳۲] از مدل‌های مارکوف برای مدل‌سازی ترتیبی تجسم حملات استفاده نموده است. او با استفاده از یک درخت پسوندی، مدل‌های مارکوفی با مرتبه مختلف را پیاده‌سازی کرده و سپس در یک مدل مارکوف با طول متغیر تلفیق نمود. فاوا از یک مدل مارکوف با طول متغیر که شامل چندین رد حمله مشاهده شده است، رفتار و مراحل آتی حملات احتمالی را استنتاج می‌نماید. بایرس[1] نیز در منبع [۳۳] یک سامانه بلادرنگ پیوسته یادگیرنده پیشنهاد داده است که قادر به تجسم ردهای حملات بوده و به دانش قبلی در خصوص ساختار شبکه نیازی ندارد. ما در این مقاله از یک مدل مبتنی بر حالت[2] به جای مدل مبتنی بر محتوی در زمینه تجسم حملات سایبری استفاده نموده‌ایم. اما در کار خود از یک الگوریتم به نام CSSR[3] که در منبع [۳۴] پیشنهاد شده است، بهره گرفتیم. الگوریتم CSSR، نسبت به روش‌های مرسوم از قبیل الگوریتم پیوند زیردرختی[4] ارائه‌شده توسط یانگ[5] و کرات فیلد[6] [۳۵] ، یا شیوه ادغام ساختاری پری و بایندر در منبع [۳۶] ترجیح داده شده است. دلیل این موضوع این است که روش‌های مرسوم، مدل‌های مارکوف را با داده سازگار می‌کند. ولی CSSR هیچ فرضی در خصوص ساختار فرایند تصادفی لحاظ نمی‌کند و واقعاً آن را از خود داده استنتاج می‌نماید. حالت‌های تصادفی استنتاج‌شده توسط سایر فنون نیز فاقد آن است. همچنین مجموع فرایندهایی که CSSR می‌تواند نمایش دهد نیز بیشتر از مجموعه فرایندهای قابل نمایش توسط مارکوف با طول متغیر است.

1- Byers
2- State-based
3- Causal-state Splitting Reconstruction
4- Subtree merging
5- Young
6- Crutchfeild

۴-۲- مدل پیشنهادی برای ارزیابی تهدیدات سایبری علیه داده‌ها و اطلاعات شبکه

با ادغام داده‌های اخذشده از بخش‌های مختلف و مقایسه آن با پایگاه داده می‌توان فهرستی از آسیب‌پذیری‌ها را استخراج کرد و با توجه به فهرست استخراجی موجودیت‌های آسیب‌پذیر و روش حمله سایبری، می‌توان تصویری از میزان و چگونگی آسیب‌پذیری ایجاد کرد. لذا تحلیل‌گر می‌تواند تصمیم بگیرد، تا اقدامات بیشتری را درصوت نیاز به‌کار گرفته و تصمیماتی را بر اساس اولویت داده‌های در خطر به اجرا در آورد [۱۰] . علاوه‌براین، اطلاعات استخراج‌شده از تمامی تخمین‌های مربوط به ردگیری حمله با هم ادغام شده تا موجودیت‌های تحت تهدید، شناسایی و براساس میزان تحت خطر بودن رتبه‌بندی شوند [۷] . ارائه مدل و استفاده از آن برای آشکارسازی موجودیت‌های تحت خطر شبکه از مهم‌ترین فعالیت‌های این بخش است.

۴-۲-۱- مدل ارزیابی تهدید علیه داده‌ها و اطلاعات شبکه

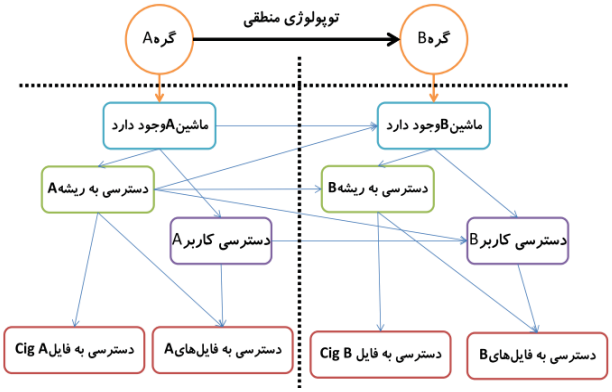
با توجه به موانع موجود در فنون تصادفی نظیر تغییرات پویای احتمالات، برای حل ابتدائی مسئله از یک رویکرد قطعی برای ارزیابی اثر و تهدیدات یک حمله سایبری استفاده شد. بنابراین هرگونه احتمالی که برای انتساب دادن به یک حالت انتقالی وجود دارد را نادیده گرفته و فرض بر این است که تمامی حالت‌های انتقالی از احتمال یکسانی برخوردارند. در ادامه تحقیق با استفاده از مدل‌های مبتنی بر حالت نظیر CSSR که مجموعه‌ای از حالت‌های مارکوفی مخفی را ایجاد می‌کنند و از لحاظ آماری قادر به تولید رفتار می‌باشند، برای حل مشکل تغییرات پویای احتمالات استفاده شد. همچنین در مدل پیشنهادی فرض شده است که با بدترین حالت توانمندی و نیت مهاجم روبرو هستیم و مهاجم، سایبری پیشرفته و بدطینت است. قابل ذکر است که مدل‌سازی و تخمین توانمندی مهاجم فراتر از دیدگاه این تحقیق است، چون به بررسی‌ها و مطالعات گسترده‌تری نیاز دارد. نیت مهاجم با توجه به این‌که غیرقابل پیش‌بینی است باید به‌طور دقیق مدل‌سازی شود [۱۰] . این مدل باید از ساختار خوبی برخوردار باشد تا بتواند در نهایت گسترش

و توسعه یافته تا احتمالاتی را که از نیت و توانمندی چندین مهاجم وجود دارد، یکپارچه سازد.

برای چارچوب پیشنهادی این بخش، نیاز به یکسری ورودی‌هایی چون سلسله‌مراتب دسترسی به اطلاعات، قالب الگوی حملات ممکن مستقل از اهداف، ساختار شبکه منطقی، نگاشت حملات و اولویت‌ها به گره‌های اطلاعاتی، نگاشت اهداف به گره‌های اطلاعاتی و تعیین وزن‌های هر گره است. سلسله‌مراتب دسترسی به اطلاعات، گراف جهت‌داری است که هریک از گره‌ها در آن نشان دهنده بخشی از اطلاعات است که یک مهاجم نیاز دارد تا اطلاعات بیشتری را به‌دست آورد؛ و یال‌ها در آن، میزان اطلاعاتی را که ممکن است در خطر باشند نشان می‌دهند. برای مثال، اگر یک یال از گره A به گره B تعریف شود، این نشان‌دهنده آن است که گره اطلاعاتی‌ای که A نشان می‌دهد می‌بایست به مخاطره بیفتد، قبل از اینکه اطلاعاتی را که به وسیله گره B نشان داده شود، در خطر قرار گیرد. هربخش از اطلاعات برای دسترسی به‌عنوان یک هدف ترسیم می‌شود؛ بنابراین از همین ساختار نیز می‌توان برای اجرای حملات در کسب اطلاعات استفاده نمود. در ساختار مذکور هر گره نشان‌دهنده اطلاعات حیاتی تحت خطر است.

اصولا اهداف با یک ساختار منطقی با هم در ارتباط بوده و ارتباط حملات نیز با استفاده از قالب الگوی حملات تعریف می‌شود. در مدل پیشنهادی، ساختار منطقی بر اساس رتبه در خطر بودن ماشین‌ها شکل می‌گیرد(شامل گراف‌های با چگالی بالا در داخل شبکه). قالب الگوی حملات، ارتباط ساده انواع حملات را در خود جای داده است تا از این طریق بتوان مجموعه‌ای از اقدامات بالقوه یک مهاجم را تعریف کرد. شکل (۷) سلسله مراتب دسترسی به اطلاعات و اینکه چگونه این سلسله‌مراتب با ساختار و قالب الگوی حملات ارتباط دارد را نشان می‌دهد. برای کاهش تعداد خطوط نشان‌داده‌شده، هر جعبه در سلسله‌مراتب، اطلاعاتی را نشان می‌دهد.

هر ماشین دارای حداقل سه سطح در سلسله مراتب دسترسی به اطلاعات است. اولین سطح نشان می‌دهد که آن مهاجم باید بداند که آن ماشین وجود دارد و برخی ویژگی‌های ماشین را نیز بشناسد. سطح دوم، سطح با اولویت را نشان می‌دهد. هر حساب کاربری می‌تواند برای گسترش دسترسی مورد استفاده قرار گیرد. سطح سوم، اطلاعات عملی ذخیره‌شده بر روی ماشین می‌باشد. قابل ذکر است که دسترسی به کاربر یا ریشه اصلی یک ماشین باعث می‌شود که دسترسی به ماشین مجاور و بعدی بر اساس ساختار منطقی، ممکن و مجاز گردد. این مسئله ممکن است در همه موارد و حالت‌ها



شکل (۷). سلسله‌مراتب دسترسی به اطلاعات [یافته تحقیق]

صحیح نباشد، اما یال‌ها می‌توانند همیشه در صورت لزوم اضافه یا حذف گردند.

از این مثال ساده فقط برای تشریح رابطه بین قالب الگوی حمله، سلسله‌مراتب دسترسی به اطلاعات و ساختار منطقی استفاده شده است. با این توصیف در مدل‌سازی ارزیابی اثر [۹و۱۱] اگر G تعداد کل حملاتی باشد که رخ داده‌اند، و A_i نشان‌دهنده نوع حمله از حمله iام باشد، و M_i نشان‌دهنده هدف حمله iام باشد، بنابراین A^* مجموعه حملاتی است که به وقوع پیوسته‌اند و براساس رابطه (۱) تعریف می‌شود:

$$\mathbf{A}^* = \bigcup_{i=1}^{G} A_i^* \qquad (۱)$$

به‌طور مشابه M^* مجموعه ماشین‌هایی است که مورد حمله واقع شده‌اند:

$$\mathbf{M}^* = \bigcup_{i=1}^{G} M_i^* \qquad (۲)$$

اگر $I(x), A(x)$ و $M(x)$ به‌ترتیب بیانگر حملات، اطلاعات و ماشین‌ها باشند که به مجموعه x بر اساس نگاشت‌های قبلی تعلق دارند، آنگاه تخمینی از مجموعه کنونی اطلاعات در خطر که توسط I^* بیان می‌شوند را می‌توان با رابطه (۳) محاسبه نمود.

$$\mathbf{I}^* = \bigcup_{i=1}^{G} \left(\mathbf{I}(A_i^*) \cap \mathbf{I}(M_i^*) \right) \qquad (۳)$$

ارزیابی تهدید: تهدید یک گره i به شکل t(i) بیان می‌گردد. ارزیابی اثر، تخمینی از تکه‌ها و بخش‌های اطلاعاتی را نشان می‌دهد که مهاجم به تازگی آن را به دست آورده است. بنابراین، تهدید هر قطعه یا بخشی از اطلاعات در I^* می‌تواند به‌صورت یک مورد خاص در نظر گرفته شود. مثلاً

$$t(I_i^*) = 1, 1 \le i \le |\mathbf{I}^*| \qquad (۴)$$

اکنون تخمین تهدید بخش‌های بعدی اطلاعاتی که ممکن است مورد سوءاستفاده قرار گیرند، مدنظر است. یادآوری می شود که سلسله مراتب اطلاعاتی به گونه‌ای تعریف می‌شوند که گره‌های اصلی می‌بایستی مورد سوءاستفاده قرار گیرند قبل از این‌که گره‌های فرزند مورد سوءاستفاده واقع شوند. بنابراین، تهدید فقط نیاز دارد که برای مجموعه I(I*) محاسبه شود. چهار مجموعه مختلف برای ارزیابی تهدید با استفاده از این الگوریتم وجود دارد.

$$\mathbf{S_1} = \mathbf{I}(\mathbf{M}^*) \quad (۵)$$

$$\mathbf{S_2} = \mathbf{I}(\mathbf{M}(\mathbf{M}^*)) \quad (۶)$$

$$\mathbf{S_3} = \mathbf{I}(\mathbf{A}^*) \quad (۷)$$

$$\mathbf{S_4} = \mathbf{I}(\mathbf{A}(\mathbf{A}^*)) \quad (۸)$$

S_1 مجموعه اطلاعاتی از تمامی ماشین‌هایی است که مورد حمله واقع شده‌اند. چون آن ماشین‌ها یک‌بار مورد حمله واقع شده‌اند، بنابراین در معرض خطر حمله مجدد نیز قرار دارند. S_2 مجموعه اطلاعات ماشین مجاور به آن ماشین‌هایی است که مورد حمله واقع شده‌اند. این ماشین‌ها در کمترین حالت و وضعیت خطر قرار دارند، چون مورد حمله واقع نشده‌اند، اما می‌توانند بعدها مورد حمله واقع شوند که به دلیل ساختار منطقی آنها می‌باشد. S_3 اطلاعاتی است که می‌تواند به وسیله مجموعه‌ای از حملاتی که اغلب رخ داده‌اند؛ مورد سوءاستفاده قرار گیرند. چون حمله اغلب رخ داه است، این نوع از حمله می‌تواند به احتمال زیادی دوباره رخ دهد. S_4 اطلاعاتی است که می‌توانست توسط مجموعه بعدی حملاتی که مهاجم توانسته انجام دهد، مورد سوءاستفاده قرار گیرد. یک حمله به احتمال زیاد بر روی یک ماشین در M* نسبت به ماشین در M(M*) رخ می دهد، بنابراین وزن بالاتری به S_1 در مقایسه با S_2 نسبت داده می‌شود. این موضوع برای S_3 و S_4 نیز به همین شکل است. وزن S_i، λ خواهد بود که λ به شکل رابطه (۹) تعریف می‌شود.

$$\sum_{k=1}^{4} \lambda_k = \beta, 0 \le \beta \le 1 \quad (۹)$$

که در اینجا β همان حداکثر میزان تهدید علیه گره‌ای که تحت خطر نیست، محسوب می‌شود. به منظور ارزیابی تهدید یک قطعه یا بخشی از اطلاعات، تابع شاخص زیر برای بیان این‌که آیا گره i در میان مجموعه s گنجانده شده است یا نه تعریف می‌شود:

$$m(i,\mathbf{S}) = \begin{cases} 0, i \notin \mathbf{S} \\ 1, i \in \mathbf{S} \end{cases} \quad (۱۰)$$

تهدید برای یک گره یعنی i، که در میان I (I*) گنجانده شده با رابطه (۱۱) تعریف می‌شود.

$$t(i) = \sum_{k=1}^{N} \lambda_k m(i, \mathbf{S_k}) \quad (۱۱)$$

به عبارت دیگر، تهدید گره‌ای، جمع وزن‌های متناسب با مجموعه‌هایی است که آن گره در آن گنجانده شده است. حداکثر مقدار عددی تابع، زمانی برآورد می‌شود که این گره در میان چهار مجموعه گنجانده شده است، بنابراین سطح تهدید β خواهد بود.

$$t(i) = 0, i \notin \left(\mathbf{I}^* \cup \mathbf{I}(\mathbf{I}^*)\right) \quad (۱۲)$$

روابط (۴، ۱۱ و ۱۲) می‌توانند با هم ترکیب شوند تا رابطه (۱۳) را برای تهدید هر گره در سلسله‌مراتب اطلاعاتی ایجاد نمایند.

$$t(i) = \max\left(m(i,\mathbf{I}^*), m(i,\mathbf{I}(\mathbf{I}^*)) \sum_{k=1}^{N} \lambda_k m(i, \mathbf{S_k}) \right) \quad (۱۳)$$

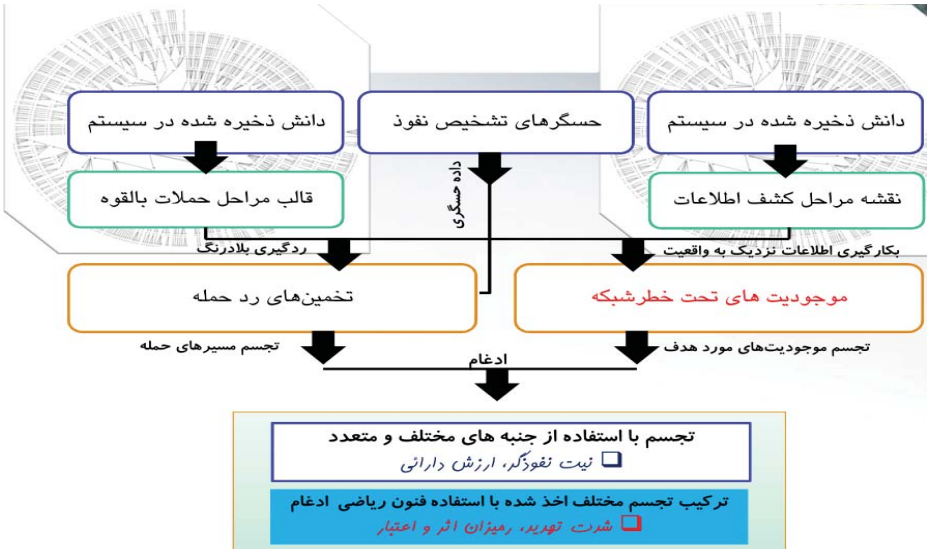
بر اساس دریافت شهودی، پارامتر normalized compromise score که با $\hat{t}_i^*(A)$ شان داده می‌شود، در واقع معادل است با مقدار تهدید نرمالیزه‌شده برای موجودیت ei ام e_i، یک گام قبل از آن‌که توسط حمله A مورد دسترسی قرار گیرد و برای آن می‌توان گفت [۲۴]:

$$\hat{t}_i^*(A) = \{ \frac{t_i(e_j^A)}{\max_{k \in I(I^*(e_j^A))} t_k(e_j^A)} \mid t_i(e_{j+1}^A) = 1, t_i(e_j^A) < 1 \}. \quad (۱۴)$$

توجه داشته باشید که مقدار تهدید نرمالیزه‌شده فقط برای موجودیت‌هایی تعریف می‌شود که مورد دسترس قرار گرفته باشند. همچنین حالتی که در آن $\max_{k \in I(I^*(e_j^A))} t_k(e_j^A) = 0$ (هیچ موجودیتی مورد تهدید قرار نگرفته است)، توسط سازوکار رهگیر حالت‌های غیرعادی در الگوریتم، فیلتر خواهند شد. با اتفاق افتادن رخدادهای تهاجمی در طی زمان، $\hat{t}_i^*(A)$ برای هر موجودیت و برای هر دنباله تهاجم تولیدشده، مورد رهگیری قرار خواهد گرفت.

۴-۳- معماری پیشنهادی تجسم اثرات حملات سایبری مبتنی بر ادغام اطلاعات سطح بالا

در این بخش با یکپارچه‌سازی مدل‌های ادغام اطلاعات پیشنهادی برای تصمیم‌گیری و مدل‌های پیشنهادی برای ارزیابی تهدید علیه اطلاعات و داده‌های شبکه، معماری مناسبی در شکل (۸) ارائه شد که قادر به ارزیابی وضعیت، تاثیر و تهدید حملات سایبری است. در این معماری یکی از مهم‌ترین مسائل این است که تجسم حاصل از رفتار حملات سایبری و تجسم حاصل از موجودیت‌های مورد هدف حمله‌کننده با استفاده از فنون ریاضی ادغام اطلاعات دمپستر- شافر، برای بهبود آگاهی وضعیتی سایبری ادغام شوند.



شکل (۸). معماری پیشنهادی برای تجسم اثرات حملات سایبری

۵- صحت‌سنجی و ارزیابی معماری پیشنهادی

روش‌های ایجاد امنیت سایبری به‌طور پیوسته در حال توسعه و گسترش هستند. بنابراین برای ارزیابی و آزمایش این روش‌ها نیز بسیاری از سازمان‌ها از شبکه‌های فیزیکی بهره می‌برند که این روش هم زمان‌بر بوده و هم هزینه بالایی را به سازمان‌ها تحمیل می‌کند [۲۵]. رویکرد جایگزین در این مقاله، استفاده از مدل‌سازی و شبیه‌سازی حملات سایبری برای آزمایش ابزارهای تحلیلی و آگاهی وضعیتی سایبری است [۱۴].

بنابراین با استفاده از بسته شبیه‌ساز تجاری ARENA مجموعه‌ای از هشدارهای سامانه‌های تشخیص نفوذ که برای آزمایش سامانه آگاهی وضعیتی سایبری مورد نیاز بوده تولید گردید و سناریوی لازم حملات نیز با استفاده از این بسته به اجرا گذاشته شد. همچنین قابل ذکر است که بسته نرم‌افزاری فوق همانگونه که در شکل (۹) نشان داده شده است این امکان را برای کاربر فراهم می‌سازد تا بتواند سناریوهای مختلف حمله، نرخ حمله، حملات با گام‌های متعدد، زمان‌بندی بین گام‌های حمله، زمان کل حمله، آدرس IP مهاجم، حملات هماهنگ و حملات کاذب را تعریف کند.

جدول (۱). انواع اقدامات مهاجم در یک حمله سایبری

مرحله	نوع اقدام مهاجم
۱	Recon Enumeration
۲	Intrusion User
۳	Goal Backdoor
۴	Recon Scanning
۵	Intrusion User
۶	Goal Denial of Service

یک سناریو از شبکه تحت حمله برای آزمایش طرح پیشنهادی که توسط این نرم‌افزار ایجاد شده است، در شکل(۱۰) نشان داده شده است. این شبکه کامپیوتری از وب سرور اصلی، دامنه‌های زیرشبکه اصلی، از یک ماشین خارجی و خطوط قرمز رنگ که همان سامانه‌های تشخیص نفوذ هستند، تشکیل شده است.

در آزمایش سامانه فرض بر این است که حمله‌سایبری از طریق اینترنت در ۶ مرحله صورت می‌گیرد. درجدول (۱)، این مراحل آمده است. میزان پیشرفت یک مهاجم به میزان توانمندی او و میزان

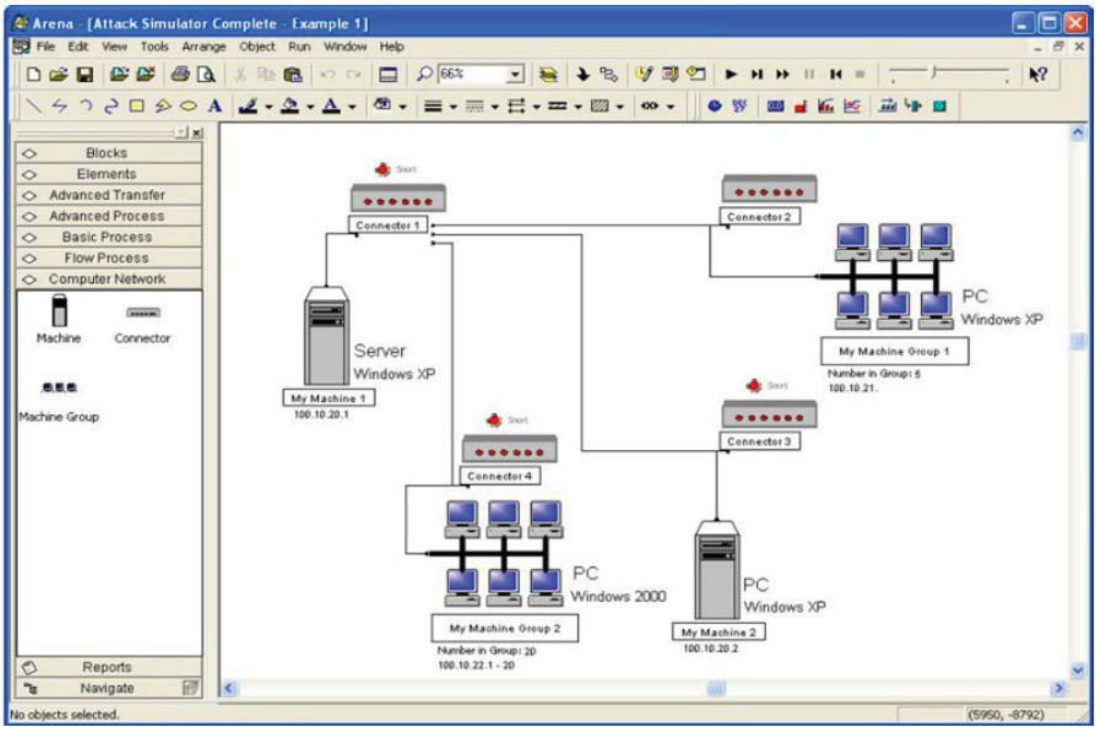
جدول (۲). پارامترهای تعریف یک حمله نوعی

حمله	آدرس هدف	نوع اقدام	بازدهی	پنهان‌کاری	مهارت	تاخیر	زمان هر گام
حمله (۱)	100.1.101. 1	Recon	۰/۸	۱/۰	۱/۰	۵	۳
حمله (۲)	100.10.219.41	Pilfering	۰/۹	۰/۸	۰/۹	۵	۴

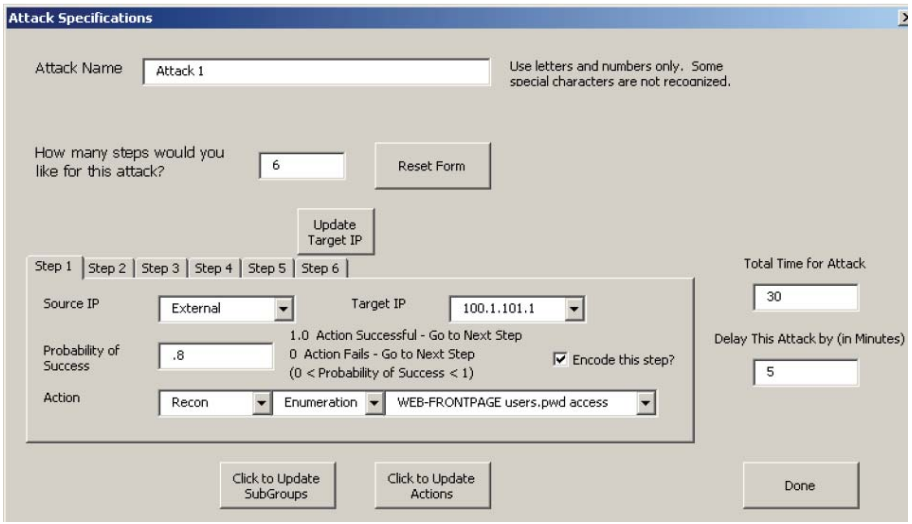
آسیب‌پذیری شبکه بستگی دارد. این موضوع در جدول (۲) نشان داده شده است. نتایج حاصل از ارزیابی اثر حملات سایبری بر اساس رتبه‌بندی موجودیت‌های تحت خطر شبکه در شکل‌های (۱۱، ۱۲، ۱۳، ۱۴) ارائه شده است.

این رتبه‌بندی‌ها براساس سناریوی حملات تعریف شده است، که یک‌بار شبکه تحت حمله واقعی قرارگرفته و اثرات این حمله بر موجودیت‌ها ارزیابی شد و یک‌بار نیز با استفاده از الگوریتم پیشنهادی تجسم اثرات بدست آمده است که نتایج، نشانگر نزدیک بودن تجسم اثرات و اثرات واقعی حمله بر روی کل شبکه می باشد. اثر بر میزبان، همان خسارت بالقوه‌ی وارد شده به میزبان با توجه به سرویس‌های میزبان و اهمیت آن سرویس‌ها برای میزبان است.

همان‌گونه که در شکل (۱۱) نشان داده شده است، اثر بر میزبان، به سرویس‌های در حال اجرا در آن و Exposureهای E (r, t) هر سرویس با توجه به اقدامات تهاجمی مشاهده‌شده در زمان t بستگی دارد. برای هر نمونه سرویس روی میزبان ، امتیازات Exposure، براساس CVSS محاسبه شده و به [۰و۱] نرمالیزه شده است.



شکل (۹). ایجاد یک شبکه تحت حملات سایبری برای آزمایش سامانه آگاهی وضعیتی سایبری



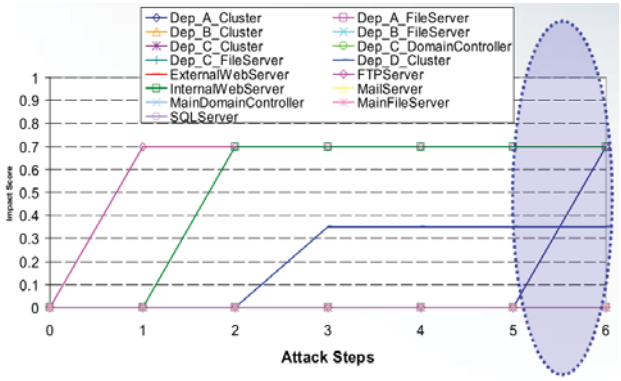
شکل (۱۰). شبیه‌سازی یک حمله در نرم‌افزار ARENA نسخه هفت

اثر حملات بر روی کاربر، اثر بالقوه‌ای است که بر هر کاربری که از میزبان‌های تحت حمله استفاده می‌کند، وارد می‌شود. در واقع همان‌گونه که در شکل (۱۲) آمده است، اثر بر کاربر نشان‌دهنده سطح اطمینانی است که یک کاربر می‌تواند از دستگاه استفاده کند.

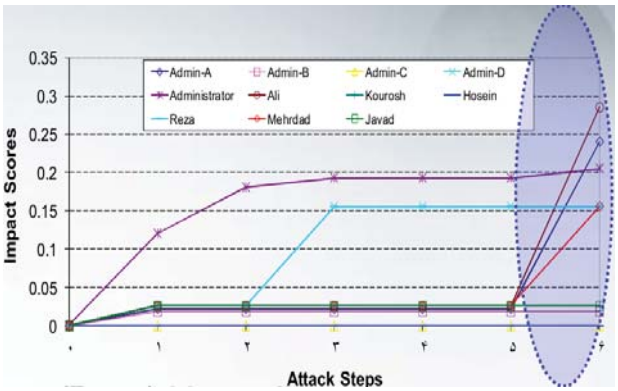
شکل (۱۳) نشان‌دهنده اثر بر سرویس است یعنی به چه اندازه یک سرویس خاص بطور بالقوه در کل شبکه تحت خطر است. برای محاسبه امتیاز اثر برای یک نوع سرویس، هرنمونه از سرویس فرضی که در حال اجرا بر روی میزبان‌های مختلف در شبکه است، بررسی شده است.

بنابراین ابتدا نمونه‌های مختلف سرویس مدنظر که در میزبان‌های مختلف در حال کار هستند را پیدا نموده سپس برای هریک از این نمونه‌های در حال اجرا روی میزبان‌های خاص با توجه به آسیب‌پذیری‌های هر کدام از آنها، امتیاز آسیب‌پذیری به‌دست آورده می‌شود و از آن امتیاز برای محاسبه میانگین امتیازات سرویس در حال اجرا بر روی میزبان‌های مختلف با توجه به اهمیت سرویس برای هر کدام از میزبان‌ها استفاده شده است.

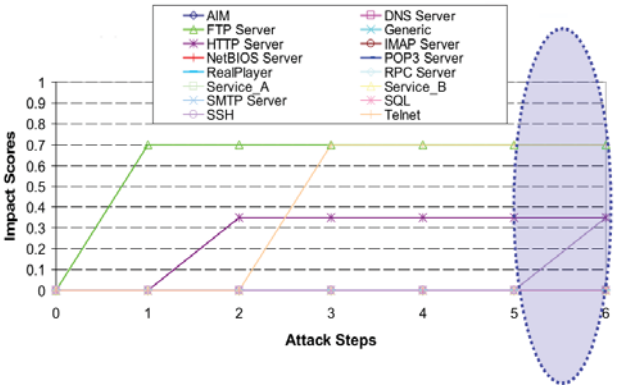
اثر بر شبکه که در شکل (۱۴) نشان داده شده است همان خسارت بالقوه روی یک زیرشبکه یا کل شبکه است. امتیاز اثر بر شبکه به تحلیلگر اجازه می‌دهد تا بر سلامت زیرشبکه یا کل شبکه نظارت کند. به‌طور خلاصه، امتیاز اثر بر شبکه از طریق محاسبه یک تجمیع از اثر بر سرویس،کاربر و میزبان در داخل زیرشبکه یا کل شبکه می‌باشد.



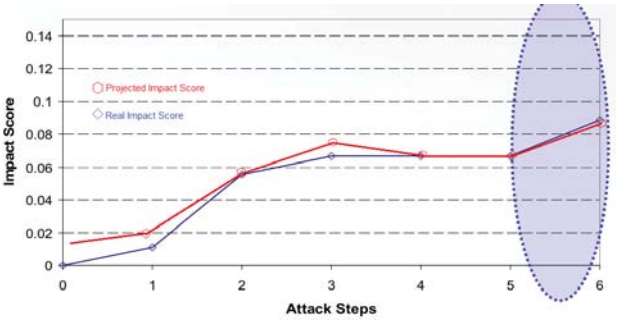
شکل (۱۱). تجسم اثر حملات سایبری برروی میزبان‌ها



شکل (۱۲). تجسم اثر حملات سایبری برروی کاربران



شکل (۱۳). تجسم اثر حملات سایبری برروی سرویس



شکل (۱۴). تجسم اثر حملات سایبری برروی کل شبکه

۶- نتیجه‌گیری

در طرح پیشنهادشده از ردگیری و همبستگی هشدارها و یک الگوی راهنمای مبتنی بر دسته‌بندی و مستقل از شبکه استفاده شده است. بنابراین، امکان تعیین ارتباط موثر هشدارها و نگاشت آن‌ها به مسیرهای حمله فراهم شده است. علاوه‌براین، تخمین مسیر، به گراف کشف مراحل دسترسی به اطلاعات خاص شبکه نگاشت شده تا امکان استدلال محتوایی و ارزیابی وضعیتی فراهم شود. تجسم‌های صورت‌گرفته از حمله‌های مستقل به شبکه و موجودیت‌های تحت

خطر شبکه براساس قانون ادغام دمپستر- شافر ترکیب شده‌اند تا تخمین‌هایی تلفیقی از اقدامات حمله آینده تامین شود. به‌علاوه به جهت حفظ یکپارچگی اطلاعات و عملیات حیاتی شبکه، طرح ارزیابی تهدید پیشنهادی، برای پیش‌بینی اقدامات آتی مهاجمان ارایه شده است. طرح مذکور با جدا کردن مدل‌سازهای مربوط به فرصت‌های پیش روی مهاجم (ساختار منطقی)، توانمندی‌های مهاجم (دنباله تهاجم) و هدف مهاجم (گراف اطلاعات) موجب کاهش پیچیدگی مدل‌سازی نیز شده است. طرح پیشنهادی پیاده‌سازی شده است و از طریق شبیه‌سازی با استفاده از دنباله‌های تهاجمی که به‌صورت تصادفی تولید شده‌اند، مورد آزمایش قرار گرفته است. نتایج بدست آمده حاکی از آن است که الگوریتم ارائه‌شده می تواند اثر حملات سایبری برروی کل شبکه را در گام‌های اولیه با میانگین اختلاف ۲۰٪ و در گام‌های نهایی تقریبا با میانگین اختلاف در حد ۱٪ به دقت مورد پیش‌بینی قرار دهد. بهره‌گیری از معماری پیشنهادی، تحلیل‌گر شبکه را قادر می‌سازد تا در مقابله با تهدیدات سایبری پیش‌بینی‌های بهتری را داشته باشد.

۷- مراجع

[1] G. Tadda, J. J. Salerno, D. Boulware, M. Hinman, S. Gorton, "Realizing situation awareness in a cyber-environment," Proceedings of SPIE, Defense and Security Symposium, vol. 6242, 2006.

[2] E. Blasch, I. Kadar, K. Hintz, J. Biermann, C. Chong, and S. Das, "Resource Management Coordination with Level 2/3 Fusion Issues and Challenges," IEEE Aerospace and Electronic Systems Magazine, vol. 23, no. 3, pp. 32-46, 2008.

[3] T. Bass, "Intrusion detection systems and multisensory data fusion," Communications of the ACM, vol. 43, no. 4, 2000.

[4] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," Human Factors Journal,vol. 37, no. 1, pp. 32–64, 1995.

[5] A. J. Rashidi, H. Shirazi and K. Dadashtabar, "Multi-Level Fusion to improve threat pattern recognition in cyber defense," Journal of mathematics and computer Science, 2014. (in Persian)

[6] W. Streilein, J. Truelove, C. R. Meiners and G. Eakman, "Cyber Situational Awareness through Operational Streaming Analysis," The 2011 Military Communications Conference - Track 3 - Cyber Security and Network Operations, pp.1152-1157, 2011.

[7] S. Vidalis and A. Jones, "Using vulnerability trees for decision making in threat assessment," University of Glamorgan, School of Computing, Tech. Rep. CS-03-2, 2003.

[8] J. Allanach, H. Tu, S. Singh, P. Willett, and K. Pattipati, "Detecting, tracking and counteracting terrorist networks via hidden markov models," in IEEE Aerospace Conference Proceedings, pp. 3246–3257, 2004.

[9] S. J. Yang, J. Holsopple, M. Sudit, "Evaluating threat assessment for multistage cyber-attacks," in: Proceedings of IEEE Military Communications Conference (MILCOM), Workshop on Situation Management (SIMA), 2006.

[10] J. Allanach, H. Tu, S. Singh, P. Willett, and K. Pattipati, "Modeling threats," IEEE Potentials, vol. 23, no. 3, pp. 18–21, 2004.

[11] Y. Liu and H. Man, "Network vulnerability assessment using Bayesian networks, " in: Proceedings of Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, vol. 5812, pp. 61–71, 2005.

[12] Insecure.com, Nmap (Network Mapper), "a free open source utility for network exploration or security auditing," http://insecure.org/nmap, 2007.

[13] M. Sudit, A. Stotz, and M. Holender, "Situational awareness of a coordinated cyber-attack," SPIE Defense & Security Symposium, Orlando, 2005.

[14] E. Blasch, P. Valin, and E. Bosse, "Measures of Effectiveness for High-Level Fusion," Int. Conf. on Info. Fusion, 2010.

[15] E. Blasch, J. Linas, D. Lambert, P. Valin, S. Das, C-Y. Chong, M. M. Kokar, and E. Shahbazian, "High Level Information Fusion Developments, Issues, and Grand Challenges – Fusion10 Panel Discussion," Int. Conf. on Info Fusion - Fusion10, 2010.

[16] D. A. Lambert, "A Blueprint for Higher Level Fusion Systems," Journal of Information Fusion, vol. 9, no. 1, pp. 6-24, 2009.

[17] C. Phillips and L. P. Swiler, "A graph-based system for network vulnerability analysis," in NSPW 98: Proceedings of the 1998 workshop on new security paradigms. New York, NY, USA: ACM Press, pp. 71–79, 1998.

[18] M. A. Solano, S. Ekwaro-Osire, and M. M. Tanik, "High-Level fusion for intelligence applications using Recombinant Cognition Synthesis," Information Fusion, vol. 13, no. 1, pp. 79-98, 2012.

[19] S. Maskell, "A Bayesian approach to fusing uncertainty imprecise and conflicting information," Information Fusion, vol. 9, pp. 259-277, 2008.

[20] J. Gomez-Romero and J. Garcia, "Strategies and Techniques for Use and Exploitation of Contextual In-

sis: Degree of Master of Science in Computer Engineering, Kate Gleason College of Engineering Rochester Institute of Technology, 2012.

[29] E. P. Blasch, D. A. Lambert, P. Valin, M. Kokar, J. Linas, S. Das, C. Chong and E. Shahbazian, "High Level Information Fusion (HLIF): Survey of Models, Issues and Grand Challenges," IEEE A&E SYSTEMS MAGAZINE, pp. 4-20, 2012.

[30] H. Chai and Y. Du,A, "Framework of Situation Awareness Based on Event Extraction and Correlation for Military Decision Support," Proceedings of 2012 IEEE International Conference on Mechatronics and Automation, August 5 - 8, Chengdu, China, pp. 192-196, 2012.

[31] N. Ye, X. Li, Q. Chen, S. M. Emran, and M. Xu, " Probabilistic techniques for intrusion detection based on computer audit data, " IEEE Transactions on Systems Man and Cybernetics,vol. 31, pp. 266–274, July 2001.

[32] D. S. Fava, "Characterization of cyber attacks through variable length markov models. Master's thesis," Rochester Insitute of Technology, 2007.

[33] S. R. Byers,"Real-time fusion and projection of network intrusion activity," Master's thesis, Rochester Institute of Technology, 2008.

[34] C. R. Shalizi and K. L. Klinkner, " Blind construction of optimal nonlinear recursive predictors for discrete sequences," In Proceedings of the 20th conference on Uncertainty in artificial intelligence, UAI '04, Arlington, Virginia, United States, pp. 504–511, 2004.

[35] J. P. Crutchfield and K. Young, "Inferring statistical complexity," Phys. Rev. Lett., vol. 63, pp. 105–108, July 1989.

formation for High-Level Fusion Architectures," Int. Conf. on Info. Fusion, 2010.

[21] E. Blasch, E. Bosse, and D. A. Lambert, "High-Level Information Fusion Management and Systems Design," Artech House, 2012.

[22] G. Toth, M. M. Kokar, K. Wallenius, K. B. Laskey, M. Sudit, M. Hultner, and O. Kessler, "Higher-level Information Fusion: Challenges to the Academic Community," Panel Discussion, Int. Conf. On Info. Fusion, 2008.

[23] J. Holsopple, S. J. Yang, and M. Sudit, "Threat assessment for networked data and information, " In Proceedings of SPIE, Defense and Security Symposium, vol. 6242, April 2006.

[24] L. E. Chase, "Integration of Cyber Situational Awareness into System Design," Thesis: Degree of Master of Science, Department of Electrical and Computer Engineering, Air University, Ohio, 2009.

[25] E. Blasch, J. J. Salerno, and G. Tadda, "Measuring the Worthiness of Situation Assessment, " IEEE Nat. Aerospace Electronics Conf., 2011.

[26] N. Ye, Y. Zhang, and C. M. Borror, "Robustness of the markov-chain model for cyber-attack detection," in IEEE Transactions on Reliability, vol. 53, no. 1, pp. 116–123, 2004.

[27] S. Schreiber-Ehle and W. Koch, "The JDL Model of Data Fusion Applied to Cyber-Defense, " a Review Paper, 2012 Workshop on Sensor Data Fusion: Trends, Solutions, Applications (SDF), pp. 116-119, 2012.

[28] V. Prasanth and K. R. Mudireddy, "Error Analysis of Sequence Modeling for Projecting Cyber Attacks," The-