طراحی سامانه هوش امنیتی برای مرکز عملیات امنیت با رویکرد عامل‌بنیان

ابراهیم نظری فرخی[1]

عباس طلوعی اشلقی[2]

چکیده:

استفاده از روش‌های سنتی همچون نظارت و نصب آنتی ویروس‌ها هرچند مفید بوده اما پاسخگوی تهدیدها نیست. مرکز عملیات امنیت، قلب امنیتی و نظارتی شبکه بوده و تمام رویدادهای شبکه را جمع آوری، بررسی، طبقه‌بندی و در صورت نیاز تصمیماتی اخذ می‌نماید. با توجه به پیچیدگی تهدیدات و سرعت تغییرات محیطی و رشد شتابان تکنولوژی، مساله اصلی پژوهش حاضر طراحی سامانه هوش امنیتی برای مرکز عملیات امنیتِ شبکه، جهت تشخیص ناهنجاری بین انواع داده‌های امنیتی و به صورت بهنگام در سازمان است. هدف اصلی پژوهش، طراحی سامانه هوش امنیتی برای مرکز عملیات امنیت شبکه می‌باشد. نوع پژوهش کاربردی است. روش پژوهش در مرحله اول به علت شناخت ابعاد مدل، اکتشافی است. به علت شبیه‌سازی در مرحله نهایی، روش پژوهش در این مرحله، تجربی است. جامعه آماری پژوهش، شامل ۱۵ نفر از صاحب نظران در حوزه پژوهش مورد مطالعه می‌باشد. دیتاست شامل ۱۰۰۰۰ رکورد مرتبط با مرکز عملیات امنیت شبکه می‌باشد. بر اساس مدل رابینسون، آزمون انجام شد و در نهایت سامانه مورد تایید خبرگان قرار گرفت.

کلمات کلیدی: **مرکز عملیات امنیت؛ مدل؛ هوش امنیتی؛ عامل‌بنیان؛ شبیه‌سازی**.

[1]. دانشجوی پسادکتری، واحد علوم و تحقیقات تهران، دانشگاه آزاد اسلامی، تهران، ایران e60_itmgtn@yahoo.com

[2]. استاد مدیریت صنعتی، واحد علوم و تحقیقات تهران، دانشگاه آزاد اسلامی، تهران، ایران،، نویسنده مسئول toloei@gmail.com

جستارگشایی

هوش امنیتی به جمع‌آوری، به‌هنجارسازی، همبسته‌سازی و تحلیل بزرگ داده‌های امنیتی یک سازمان به منظور خودکار نمودن فرآیندهای کاهش سطح مخاطرات گفته می‌شود؛ به عبارتی، تبدیل میلیون بسته اطلاعات به یک اقدام عملی آنی گفته می شود (کیان‌پور، ۱۳۹۵: ۱۰). برخی از ویژگی‌های هوش امنیتی شامل: کاهش تهدیدات و مخاطرات در سازمان ها، تسهیل تصمیم‌گیری امنیتی، خودکار نمودن فرآیندهای امنیتی و کاهش سطح عدم انطباق می‌باشد (پورابراهیمی و همکاران، ۱۳۹٦: ۳۲). سازمان‌ها در صدد گسترش حیطه مدیریت امنیت اطلاعات و کاهش تهدیدات و مخاطرات خود از لایه قدیمی چون فایروال و شبکه داخلی به بررسی داده‌ها هستند. گاهی اوقات سازمان‌ها، زمان و منابع قابل توجهی را برای اجرای کنترل‌های امنیتی اختصاص می‌دهند که به طور کامل با تهدیداتی که شرکت در حال تلاش برای کاهش آنهاست، بی ربط می‌باشد. این عدم تطابق درک نامناسبی از فناوری امنیت و تهدیدها نشان می‌دهد. مرکز عملیات امنیت به عنوان مغز هوشیار يك مجموعه عمل مي‌كند و اطلاعات را جمع آوري كرده، از غربال هشدارها مي‌گذراند، ريسک‌ها را اولويت‌بندي كرده و از حملات قبل از آنكه بتوانند اجرا شوند و آسيب برسانند جلوگيري مي‌كند (قربانی و محمدی، ۱۳۹۶: ۷).

مولفه‌های معماری مرکز عملیات امنیت شامل: تولید رویدادها، جمع آوری و همسان سازی رویدادها، ذخیره سازی رویدادها، تحلیل و آنالیز وعکس‌العمل می‌باشد (Nathans and David, 2015: 12). در معماری هوش امنیتی، داده‌های مرتبط با ارزیابی آسیب‌پذیری، دیواره آتش، سیستم تشخیص نفوذ، مسیریاب‌ها، سوئیچ‌ها، سیستم عامل و نرم‌افزارها به عنوان ورودی سامانه در نظر گرفته می‌شود. در ادامه نرمال‌سازی و جداسازی داده‌ها انجام می‌شود. در گام بعدی، دسته‌بندی و همبسته‌سازی داده‌ها شکل گرفته و سپس با توجه به بستر مورد نظر، کشف تهدید، تقلب و پیش‌بینی ریسک یا مخاطره صورت می گیرد. هوش امنیتی به سازمان‌ها کمک می کند تا وضعیت امنیت در گذشته و موجود را بهتر مشاهده کنند تا بتوانند وضعیت امنیت خودشان را خوب تحلیل نمایند. عامل‌ها، واحدهای اصلی مدل‌سازی عامل‌بنیان را تشکیل می دهند. دو جنبه مهمی که در تعریف عامل ها مطرح می شوند متعلقات عامل و نوع رفتار آنهاست (امینی و همکاران، ۱۳۹٦: ۲۱). شبیه‌سازی عامل‌بنیان ویژگی‌های از قبیل موارد زیر را داراست:

نمایشی واقع‌گرایانه از یک پدیده

در نظر گرفتن همزمان چندین متغیر

استفاده داده‌ها از منابع مختلف و ناهمگون

بررسی پدیده‌های خرد و کلان به صورت همزمان و توامان

پیش‌بینی در طول زمان

ایجاد چارچوبی برای اجرای سناریوهای مختلف

نمایش و پیش‌بینی بوجود آمدن پدیده‌های نوظهور

قابلیت انعطاف‌پذیری (کم و زیاد کردن اجزای مساله) و گسترش راحت

امکان تغییر داده‌های اولیه، اجرا و دستکاری مدل توسط سایر محققان (آذرفر و همکاران، ۱۳۹۵: ۳٤).

نت لوگو یک محیط مدل‌سازی قابل برنامه ریزی برای شبیه سازی پدیده های طبیعی و اجتماعی است. این نرم افزار توسط یوری ولنسکی در سال ۱۹۹۹ نوشته شده و از آن زمان تا به حال مرتب در حال تکوین و بهینه سازی بوده است. نت لوگو برای مدل‌سازی سیستم‌های پیچیده که در طول زمان رشد و توسعه می یابند، بسیار مناسب است. مدل‌سازان می توانند شیوه های رفتار هزاران عامل را به طور مستقل تعیین کنند. این توانایی امکان کشف ارتباط را بین رفتار هر فرد و الگوهای به وجود آمده در سطح کلان را که از تعامل افراد بسیار زیادی پدیدار می شود را فراهم می کند (Wilensky and Rand, 2015: 9).

در حالت کلی ساختار یک مدل عامل‌بنیان، شامل سه مولفه زیر است:

الف- مجموعه عامل‌ها، ویژگی‌ها و رفتارهای آنها

ب- مجموعه روابط و نحوه تراکنش میان عامل‌ها

ج- محیطي که عامل‌ها در آن قرار دارند و با آن در تعامل هستند (نیکی اسکویی، ۱۳۹۶: ۱۶).

برای طراحی سامانه هوش امنیتی برای مرکز عملیات امنیت، بایستی نخست، مولفه‌ها و شاخص‌های تاثیرگذار بر تامین امنیت مرکز عملیات امنیت شبکه را به طور مستمر رصد و شناسایی نمود. هرچند که شناسایی مولفه‌ها و شاخص‌های اثرگذار به خودی خود، دارای اهمیت هستند، ولی این به تنهایی کافی نیست. حال، پرسش اصلی این است که با توجه به پیچیدگی تهدیدات، سرعت تغییرات محیطی و رشد شتابان تکنولوژی، سامانه هوش امنیتی برای مرکز عملیات امنیتِ شبکه، جهت تشخیص ناهنجاری بین انواع داده‌های امنیتی و به صورت بهنگام در سازمان چگونه است؟ برای پرداختن به مساله پژوهش سئوال‌هایی در خصوص شاخص‌های تاثیرگذار بر مرکز عملیات امنیت و نحوه جمع‌آوری داده و نحوه تحلیل داده‌ها مطرح گردیده است. مهمترین شاخص های تاثیرگذار امنیتی بر مرکز عملیات امنیت کدامند؟ نحوه جمع آوری داده برای تامین نیازهای اطلاعاتی سامانه چگونه است؟ چه نوع معماری اطلاعاتی برای تحلیل در سامانه، مناسب است؟ تحلیل داده‌ها بر اساس بکارگیری تابع همبسته‌سازی در سامانه چگونه است؟ تحلیل داده‌ها بدون استفاده از تابع همبسته‌سازی چگونه است؟ هوش امنیتی شامل گردآوری، تحلیل و همبسته‌سازی انواع داده‌ها در قالب یک دیتاست است که در نهایت مقایسه تحلیل داده‌ها بر اساس استفاده/بدون استفاده از تابع همبسته‌سازی انجام می گیرد تا بسته‌های سالم از بسته‌های آلوده تشخیص داده شوند. در سامانه، عامل‌های تعریف شده شامل: تعداد بسته‌ها[3]، فرستنده[4]، گیرنده[5]، احتمال ایجاد نویز[6]، احتمال ایجاد بسته‌های آلوده[7]، تابع همبستگی[8] و مسیریاب[9].

برای تشخیص میزان نفوذ در شبکه، وضعیت هر بسته که وارد شبکه می‌شود، بررسی شده است. این وضعیت‌ها شامل: بسته اشتباه ارسال شده، بسته ارسال نشده، بسته‌های بد (خاطی)، بسته‌های نویزدار، بسته‌ای که کاملا به مقصد رسیده است. عامل مسیریاب، برای تشخیص آدرس‌های مربوط[10] به هر بسته در شبکه به کار گرفته شده است. اگر بسته‌ای در شبکه به صورت اشتباه ارسال و یا اینکه اصلا ارسال نشود، عاملِ مسیریاب وظیفه تشخیص این دسته از بسته‌ها را بر عهده دارد و دقیقا مشخص می کند که هر بسته توسط چه کسی و برای چه مقصدی در شبکه ارسال شده است. عامل همبسته‌سازی در شبکه وظیفه دارد تا بسته‌های بد و بسته‌هایی که در شبکه، نویز می گیرند را تشخیص دهد.

نوع پژوهش، کاربردی است. روش پژوهش در مرحله اول به علت شناخت ابعاد مدل، اکتشافی، در مرحله دوم، مطالعه تطبیقی مدل‌های منتخب، در مرحله سوم، تحلیلی است. در نهایت سامانه‌ایی ارائه شده و اعتبارسنجی آن از طریق آزمون‌های مربوطه صورت گرفته که روش پژوهش در این مرحله، تجربی خواهد بود. جامعه آماری این پژوهش به علت استفاده از داده‌های خام و تحلیل شده مرکز عملیات امنیت، شامل ۱۵ نفر از صاحب نظران در حوزه پژوهش مورد مطالعه مي‌باشد. برای احصاء عامل‌های هوشمند اثرگذار بر سامانه از نظرات کارشناسان و اساتید رشته مدیریت فناوری اطلاعات و فناوری اطلاعات و متخصصان و کارکنانِ حوزه امنیت فناوری اطلاعات و مرکز عملیات امنیت، بهره‌گیری شد. ضمنا برای آزمون مدل شبیه‌سازی شده از دیتاست شامل ۱۰۰۰۰ رکورد مرتبط با مرکز عملیات امنیت شبکه استفاده شد. روش گردآوري اطلاعات در این پژوهش، استفاده از دیتاست‌های خاص است. همچنین از روش‌هاي فیش‌برداری، پرسش‌نامه و مصاحبه با خبرگان برای احصاء و تعریف عامل‌های اثرگذار بر سامانه، استفاده شد.

---

[3] Number of Packets
[4] Sender
[5] Destination
[6] possibility-of-Noise
[7] possibility-of-bad-packet
[8] Correlation Function
[9] Router
[10] IP address

مفاهیم و مبانی نظری

سیستم‌های هوش امنیتی براي انجام تحلیل‌هاي موردي و پاسخ به پرسش‌هاي مرتبط با عملیات مداوم بخش‌های مختلف مرکز عملیات امنیت، برآورد تهدیدات و ... مورد استفاده قرار مي‌گیرند. اگر بخواهیم هوش امنیتی را با روش‌های سنتی امنیت، مقایسه نمائیم، می‌توان به نکات زیر اشاره نمود: (پورابراهیمی و همکاران، ۱۳۹۶: ۱۴)

جدول شماره ۱

روش‌های سنتی امنیت	هوش امنیتی
اسکن نرم افزارها	همبسته‌سازی اطلاعات
اسکن شبکه	یکپارچگی اطلاعات
نظارت بر سیستم مدیریت پایگاه داده	همبسته‌سازی تکنولوژی
نظارت بر دسترسی‌ها	یکپارچگی تکنولوژی
خروجی در قالب ارائه گزارش	خروجی در قالب گزارش و استعلام از سامانه هوش امنیتی
تصمیم غیرهوشمند	تصمیم و اقدام هوشمند

در صورت عدم استفاده از معماری هوش امنیتی در مراکز عملیات امنیت، نظارت بهنگام بر هر دو بعد زمان واقعی رویداد و داده‌هایی که از نگاه شرکت، قبلا پنهان بوده، صورت نخواهد گرفت و شرکت هشدار لازم در مورد تهدیدات و مخاطرات را در زمانی که به آن نیاز دارد، دریافت نمی‌نماید. در صورت عدم به کارگیری این مدل در مرکز عملیات امنیت شرکت، نه تنها به ارتباط بین داده‌ها پرداخته نمی‌شود؛ بلکه تشخیص ناهنجاری و ارائه گزارش به منظور تشخیص فوری تهدید و مخاطره، پرداخته نمی‌شود. مدل‌سازی عامل‌بنیان به عنوان یکی از تکنیک‌های شبیه‌سازی سیستم‌های سازگار پیچیده در کنار تکنیک‌های سیستم پویا و گسسته پیشامد قرار می‌گیرد. تأکید بر مدل‌سازی رفتار عامل های غیرهمگن و بروز رفتارهای برآیندی دو قابلیت مهمی است که مدل‌های عامل‌بنیان را از رویکردهای شبیه‌سازی پیش آمد گسسته و سیستم‌های پویا مجزا می‌کند (امینی و همکاران، ۱۳۹۶: ۲۷). اهمیت پژوهش از آن جهت است که با بهره گیری از نظر خبرگان، سامانه هوش امنیتی که لایه ورودی آن مبتنی بر داده‌های دنیای واقعی است، طراحی می‌شود و سپس در لایه میانی، پردازش و تحلیل داده‌های لایه ورودی صورت گرفته و در نهایت، سامانه بر اساس رویکرد عامل‌بنیان، طراحی خواهد شد. هوش امنیتی، امکان و توانایی بهبود کیفیت نظارت و کنترل بر داده‌های شبکه را فراهم نموده و می‌توانند برنامه‌ریزی و تصمیم‌گیری در این حوزه را نیز تسهیل نماید. با استفاده از فناوری هوش امنیتی و تحلیل داده‌های سازمان برای استخراج حداکثر ارزش افزوده مقدار زیادی از اطلاعات، در صدد تامین نیازمندی های سیستم مدیریت امنیت اطلاعات هستیم. با این روش سازمان می تواند فرصت‌ها را به حداکثر و تهدیدات و مخاطرات مرکز عملیات امنیت شرکت را به حداقل برساند. با طراحی سامانه امنیت مراکز امنیت، شرکت‌ها و سازمان‌ها، قادر خواهند بود تا به پشتیبانی حیاتی در تصمیم گیری خود با خودکار فرآیندهای تحلیل داده‌ها دست یابند (ملک‌زاده و سلطانی، ۱۳۹۳: ۲۵). سامانه مذکور با به کارگیری ابزارهای به روز فناوری اطلاعات از قبیل: رویکرد عامل‌بنیان، به روزترین الگوریتم‌ها و مدل‌های معماری اطلاعات، انواع داده را جمع‌آوری و تحلیل نموده تا ضمن جمع‌آوری و شناسایی به موقع داده‌ها و تحلیل مناسب، مرکز عملیات امنیت، این فرصت برای برنامه‌ریزان و تصمیم‌سازان و تصمیم گیرندگان، فراهم گردد تا نسبت به رفع آسیب‌پذیری‌های موجود، بر اساس تحلیل و ارائه گزارش سیستم و اتخاذ تصمیم متناسب با هر هشدار، اقدام نمایند.

امینی و همکاران در سال ۱۳۹۶، با انجام پژوهشی، با استفاده از روش مبتنی بر عامل و نرم‌افزار نت لوگو مدلی برای محاسبه تقاضای کل بخش‌های مختلف اقتصادی ارائه نموده‌اند. در این مدل هر یک از بخش‌های اقتصادی به عنوان یک عامل فرض که الگوریتم رفتاری مشخصی داشته و با یکدیگر تعامل می‌کنند. مدل‌سازی پژوهش می‌تواند به عنوان جایگزین ارزان، سریع و با دقت مناسب برای تصمیم‌گیری‌های مدیریتی در زمینه‌های مختلف اقتصادی و زیست محیطی استفاده شود.

نیکویی اسکویی و همکاران در سال ۱۳۹۶، هدف خود را تعیین استراتژی بهینه ایران در تجارت بین‌المللی گاز طبیعی با استفاده از رویکرد مدل‌سازی عامل بنیان عنوان کرده‌اند. به واسطه شبیه‌سازی رفتار کشورهای واردکننده و عرضه‌کننده و همچنین مدنظر قراردادن پیچیدگی‌های خاص بازار بین‌المللی گاز که ناشی از ریسک سرمایه‌گذاری، زیرساخت‌های انتقال و همچنین مکانیزم‌های قیمت‌گذاری مربوط به این حامل انرژی است، می تواند تصویر واقع‌بینانه‌تری از شرایط بازار و نحوه تعامل بازیگران ارائه نماید. در نهایت یک مدل برای مکانیزم انتخاب کشورهای عرضه‌کننده و واردکننده در نرم افزار Any logic کدنویسی و پیاده سازی شده است.

مودی و مردمی در سال ۱۳۹۶، در پژوهشی به طراحی مرکز فرهنگی فناوری‌های معماری با استفاده از مدل‌سازی عامل‌بنیان پرداخته‌اند. هدف این مطالعه، بررسی کاربردهای مدل‌سازی عامل‌محور در معماری و شهرسازی است. برای ساخت این مدل، از فرآیندهای موجود در طبیعت الهام‌برداری شده است که در آن حرکت مبتنی بر تصمیمات محلی، جهت‌یابی است که منجر به ظهور شبکه‌های با پیچیدگی و سازگاری سطح بالا می‌شود.

صالح و براآنی در سال ۱۳۹۶، طی پژوهشی، پایگاه دانش مرکز عملیات امنیت را مورد بررسی قرار داده‌اند. نتیجه نشان می‌دهد که با جامع در نظر گرفتن قوانین سیستم‌های امنیتی و اضافه کردن فیلد محتوا به راهکار ارائه شده، ناظر قوانین شبکه و تغییرات روی آن، می‌توان به این خواسته رسید و گزارشات نادرست ارائه شده کاهش یافته و می‌توان قوانین سیستم‌های مختلف را با هم بررسی کرد. با کم‌شدن گزارشات، کار برای مدیر شبکه به منظور بررسی صحت ناسازگاری‌ها، کاهش می‌یابد و باعث ساده‌تر شدن کار مدیر شبکه و در نتیجه کاهش خطای انسانی می‌شود.

غلامی و همکاران طی پژوهشی در سال ۱۳۹۶، به طراحی سیستم خبره فازی ارزیابی امنیت سایبری در مبادلات الکترونیکی کسب وکارها پرداخته‌اند. هدف از این پژوهش، طراحی سیستم هوشمند مبتنی بر دانش خبرگان به منظور ارزیابی کم هزینه و دقیق امنیت سایبری در مبادلات الکترونیکی کسب و کارها بوده است. نتایج نشان می‌دهد خطای سیستم خبره فازی در مقایسه با روش اجرای پرسشنامه بسیار ناچیز و قابل اغماض بوده و می‌تواند جهت ارزیابی مورد استفاده قرار گیرد.

قربانی و محمدی در سال ۱۳۹۶، طی پژوهشی به بررسی عملکرد مرکز عملیات امنیت و ارائه الگوي مناسب براي بکارگیري در ایران پرداختند. در این پژوهش، ابتدا خدمات مرکز عملیات امنیت بیان شده و سپس معماري آن تشریح گردیده است. نهایتا الگوي پیشنهادي به منظور بکارگیري مراکز عملیات امنیت، ارائه گردیده است. بر اساس این الگو می توان بر اساس شرایط جغرافیایی، سیاسی، اجتماعی بخش‌بندي‌هاي مختلفی را ترسیم نمود و سپس مدیریت هر حوزه را به یک مرکز عملیات امنیت سطح بالاتر که وظیفه آن هماهنگی و راهبري مرکز عملیات امنیت‌هاي محلی است، واگذار نمود.

آذرفر و همکاران در سال ۱۳۹۵ نسبت به ارائه مدل پایه عامل بنیان، به شبیه‌سازی تغییرات جمعیتی ایران پرداختند. از روش عامل بنیان برای شبیه‌سازی و تحلیل سناریوها استفاده شده و توابع و سناریوهای متفاوتی در شبیه‌سازی مورد تحلیل قرار گرفته‌اند. نتایج نشان داد که ایران در حال حاضر با فرصت پنجره جمعیتی مواجه است و در آینده، پیری جمعیت را به طور حتم تجربه می کند، لذا لازم است تا دولت‌مردان برنامه‌ریزی‌های بلندمدت و کوتاه مدت برای رویارویی با این دو پدیده در این دو برهه زمانی داشته باشند.

قلعه‌بان تکمه‌داش و همکاران در سال ۱۳۹۴ طی پژوهشی، چارچوب مدل‌های عامل‌بنیان در شبیه‌سازی رفتار ذی‌نفعان برای مدیریت منابع آب را ارائه نمودند. در این پژوهش، اساس مدل‌سازی عامل‌بنیان تبیین می‌شود، ابزارهای مورد استفاده در این زمینه معرفی و کاربرد آن در زمینه‌ی مدیریت منابع آب نمایش داده شده است. تلفیق این‌گونه مدل‌های شبیه‌سازی با مدل‌های شبیه‌سازی منابع آب، به تولید و بالابردن اطمینان پذیری مدل‌های جامع پشتیبانی تصمیم گیری مدیریت منابع آب کمک می کند.

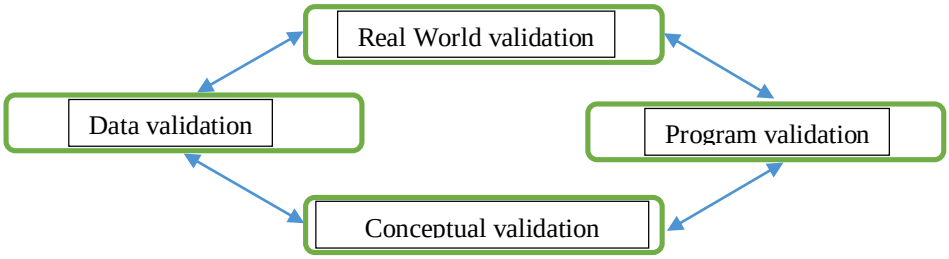
جلینی و همکاران در سال ۱۳۹۴ طی پژوهشی با استفاده از نظریه بازی تکاملی و مدل‌سازی عامل‌بنیان به تحلیل رفتار اعضای اوپک پرداختند. از نظریه بازی تکاملی و مدل‌سازی عامل‌بنیان به صورت متوالی به عنوان وسیله ای برای پرداختن به مشکلات بین زمان (بین دوره‌ای) که نمایش دهنده ویژگی‌های تکاملی هستند، استفاده شده است. در مقاله، یک مدل نظریه بازی تکاملی متقارن برای بررسی رفتار عوامل اوپک استفاده شده و این مدل نشان می دهد که آنها آموختند تا کنترل منابع خود را به دست بگیرند.

دیمرتزیس در سال ۲۰۱۹ طی پژوهشی به مطالعه مرکز عملیات امنیت شناختی نسل بعد پرداختند. مرکز عملیات امنیت[11] یک واحد فنی مرکزی پاسخگو برای مانیتور، تحلیل، ارزیابی و دفاع برای وضعیت در حال پیشرفت یک سازمان است. این پژوهش یک راهبرد امنیتی فعال و متنوعِ متکی بر خلاقیت که شامل تحلیل داده، پردازش و حمایت از تصمیم‌گیری برای مواجهه با خطرات سایبری است را پیشنهاد نموده که بر رویه‌های کاملا خودکارِ پیشرفته متکی است. در نهایت چارچوبِ معماری دفاع فارنزیک جریان شبکه برای ارتقاء امنیت سایبری در برابر حملات مهاجمان پیشنهاد شده است.

خلیلی و همکاران در سال ۱۳۹۶ پژوهشی با عنوان مانیتور و بهبود خدمات امنیتی مدیریت شده در مرکز عملیات امنیت انجام دادند. در این سامانه سه ماژول برای نظارت بر فعالیت‌های تحلیل‌گران، ارزیابی عملکرد تحلیل و سناریوهای شبیه‌سازی عملکرد طراحی شده است. سامانه طراحی شده به وسیله ماژول خدمات پشتیبان تقویت شده است تا بازخوردی در مورد ناهنجاری‌ها یا مباحث غیرنرمال اطلاعاتی برای تحلیل‌گران امنیت فراهم نماید. نتایج شبیه‌سازی از اثربخشی ماژول‌ها در سیستم طراحی شده در بهبود عملکرد SOC منتشر شده است.

تجزیه و تحلیل یافته‌ها:

در این بخش تحلیل توصیفی و تبیینی به شرح زیر ارائه شده است. آزمون مدل بر اساس مدل رابینسون انجام شد. مطابق شکل شماره یک، چهار بعد اصلی در خصوص آزمون نرم‌افزار مورد بررسی قرار گرفت که در ادامه، مدل طراحی شده در این پژوهش بر اساس شکل شماره یک آزمون گردید.



شکل شماره ۱. آزمون مدل

مرحله اول: اعتبارسنجی داده[12]

۱. شناخت داده

شناخت داده‌ها شامل انتخاب داده‌ها برای کسب مناسب‌ترین داده‌های مورد نیاز است. این مرحله، قبل از مرحله پیش‌پردازش صورت می‌گیرد؛ این مرحله از آزمون مدل، شامل اطمینان از داده‌هاست که پاک‌سازی داده‌ها صورت گرفته باشد تا از کیفیت داده‌ها اطمینان حاصل شود. در این مرحله، فرآیند حذف و اصلاح داده‌های نامطمئن صورت می‌گیرد.

۲. سازگاری

سازگاری شامل مهیا نمودن داده‌ها برای عملیاتی است که پس از این روی آن انجام می‌شود. از آن جایی که سامانه طراحی شده از قالب‌های فایل مرتبط با داده‌های مرکز عملیات امنیت پشتیبانی می‌کند، از مخزن داده‌ها (دیتاست)، فایل مربوطه جهت ورود به نرم‌افزار فراخوانی می‌شود.

۳. نوع داده

در این مدل، شش محدوده ایجاد شده و در مجموع، دو مقصد داریم. راه‌کاری که در این مرحله از آزمون مدل برای اجرا و ممیزی بسته‌ها در نظر گرفته شد، شامل موارد زیر است:

الف- شش ارسال کننده دیتا به درون شبکه

ب- شش دریافت کننده بسته‌ها

---

[11] SOC

[12] Data validation

ج- مقصد ۱ (destination1) نشان می‌دهد که چه مقداری از بسته‌ها کاملا به مقصد اصلی رسیده‌اند.
د- مقصد ۲ (destination2) نشان می‌دهد که چه مقداری از بسته‌ها کاملا به مقصد اصلی رسیده‌اند.

۴. تحلیل مولفه‌های اصلی

منطق اعتبارسنجی داده‌ها دراین مرحله از آزمون، مشابه روش تحلیل مولفه‌های اصلی[۱۳] می‌باشد. به این صورت که مولفه‌های متنیِ مشخصی از مجموع داده‌های مورد استفاده جهت پردازش در نرم‌افزار، انتخاب می‌شود که این خود به فرآیند ارزیابی داده، کمک نمود. در واقع در این مرحله از آزمون مدل، داده‌های مربوط به بسته‌ها وارد سیستم شده تا بر اساس پردازش صورت گرفته توسط تابع همبسته‌سازی، داده‌های ناسازگار و غیرمرتبط در شبکه تشخیص داده شود.

۵. دقت

دقت معیار مناسبی برای نشان‌دادن میزان تشخیص سامانه در ممیزی بسته‌های ورودی به شبکه هست. نویزها توسط همبسته‌سازی از بسته‌ها جدا می‌شوند که این در محیط زرد رنگ مشخص شده است. در قسمت نمودار state بسته‌های آلوده در دو حالت بسته‌های بد و نویز شناسایی می‌شوند که میزان دقت سامانه طی مقایسه در سناریوهای مختلفی مورد بررسی قرار گرفته است.

۶. **اعتبارسنجی ساختاری** (استفاده از شش محیط با رنگ‌های متفاوت)

در سمت راست محیط سامانه، شش لایه طراحی شده است که به منظور تحلیل حساسیت مدل، مقادیر آن‌ها، قابل تغییر است. این لایه‌ها شامل: لایه تعداد بسته‌ها، لایه نمایش دیتای محیط طراحی، لایه احتمال ایجاد نویز در شبکه، لایه احتمال ایجاد بسته‌های خاطی در شبکه، لایه توان تابع همبسته‌سازی حین اجرای شبیه‌سازی، لایه مسیریاب برای توان و عملکرد مسیریاب در مدل شبیه‌سازی.

مرحله دوم: اعتبارسنجی مفهومی[۱۴]

مدل طراحی شده مورد قضاوت و تایید خبرگان قرار گرفت. برای تشخیص بسته‌های آلوده در سامانه‌ی طراحی شده، بررسی عامل‌هایی همچون: تعداد بسته‌ها، فرستنده و گیرنده، احتمال ایجاد نویز، احتمال ایجاد بسته‌های آلوده، تابع همبسته‌سازی و مسیریاب، کفایت می‌نماید. لذا، مدل نهایی پژوهش با استفاده از نرم‌افزار نت‌لوگو، طراحی و شبیه‌سازی گردید.

اعتبارسنجی برنامه[۱۵]

این بخش از آزمون با مراحل اعتبارسنجی داده و اعتبارسنجی مفهومی، ارتباط مستقیم و دوسویه‌ای دارد. به این معنا که اگر داده‌ها در مرحله ورود به درستی شناسایی، انتخاب و پاک‌سازی نشوند، باعث بُروز خطا در محاسبات الگوریتم‌های برنامه خواهد شد.

الف- تایید منطقِ برنامه: مدل طراحی شده در حالت مفهومی با خبرگان مطرح و روش‌ها و الگوریتم پیاده‌سازی شده، مورد تایید خبرگان قرار گرفت که این خود نیز به اعتبار سامانه، افزوده است.

ب- خطایابی: در اعتبارسنجی سامانه، نخست از خطایابی برنامه جهت بررسی کدهای برنامه، استفاده شد که هیچ‌گونه خطایی وجود نداشت.

ج- اجرای الگوریتم: برای آزمون الگوریتم‌های نوشته شده، از دو رویکرد جعبه سفید۱٦ و جعبه سیاه۱۷ استفاده و از اجرای درست الگوریتم، اطمینان حاصل گردید. در رویکرد جعبه سفید، تمامی آیکون‌ها، دکمه‌ها و فرامین به درستی اجرا شدند. در رویکرد جعبه سیاه، سیستم به عنوان یک جعبه سیاه در نظر گرفته شد و تمامی محاسبات ریاضی و ساختارهای زبان برنامه‌نویسی و حلقه‌های استفاده شده در الگوریتم‌ها، بررسی و تایید گردید.

---

[13] Principle Component Analysis (PCA)
[14] Conceptual Validation
[15] Program validation
[16] White-Box
[17] Black-Box

د- بررسی معیارهای صحت و دقت الگوریتم: برای تخمین میزان اطمینان درباره صحت و دقت الگوریتم، از عامل‌های تعریف شده، بهره گرفته شد که نتایج، درستی عملکرد الگوریتم استفاده شده در مدل شبیه‌سازی را اثبات نمود.

اعتبارسنجی در دنیای واقعی[18]

یکی از مشکلات مدل‌سازی، مواجهه شدن مدل در عمل و با دنیای واقعی است. به عبارتی دیگر، مدل طراحی شده زمانی معتبر است که در یک نمای واقعی، جواب بدهد. برای این منظور در مدل شبیه‌سازی شده در این پژوهش، سناریوهایی متفاوتی در نظر گرفته شد تا از اعتبار مدل در دنیای واقعی جهت بررسی شباهت تشخیص بسته‌ها، اطمینان حاصل نمود:

در این مدل، مسیریاب[19]، وظیفه دارد IP آدرس‌ها را چک کند تا تشخیص دهد بسته ارسالی از چه کسی ارسال و در نهایت به چه کسی می‌رسد. گاهی ممکن است مسیریاب وظیفه خود را به درستی در شبکه انجام ندهد.

در حالت اجرای مدل، اگر مقدار تابع همبسته‌سازی را ۵۰ و مقدار مسیریاب ۱۰۰ و بقیه لایه‌ها روی عدد ۱ تنظیم شوند، نویز و بسته‌های بد در شبکه وجود دارند، یعنی تابع همبسته‌سازی در حال انجام وظیفه تعیین شده است.

حال اگر مقدار تابع کرولیت روی عدد ۵۰ قرار بگیرد به این معناست که کرولیت ۱۰۰% اتفاق نمی‌افتد پس ۵۰% نویز و بسته‌های بد تشخیص داده نمی‌شوند و در واقع ۵۰% بسته‌ها به سمت تحویل‌گیرنده‌ها(Receiver) می‌رود.

در قسمت‌های destination1 و destination2 بسته‌های به رنگ بنفش وجود دارند که این بسته‌های آلوده هستند؛ یعنی تابع کرولیت این بسته‌ها را درست تشخیص نداده و نویزها و بسته‌های بد به مقصد رسیده است.

در قسمت پایین محیط سامانه، چهار نمودار تعریف شده است.

نمودار Sender: نشان‌دهنده این است که چه تعداد بسته و به چه مقداری از هر ارسال‌کننده به داخل شبکه فرستاده شده است. نمودار Destination: در مدل طراحی شده ۶ تحویل‌گیرنده وجود دارد. محور افقی، زمان و محور عمودی نشان‌دهنده تعداد بسته‌هایی است که به مقصد رسیده‌اند. اختلاف محور عمودی نمودار Sender و محور عمودی Destination، نشان‌دهنده اختلاف بسته‌های سالم از بسته‌های آلوده اعم از بسته‌های بد و نویز است. نمودار State : در این نمودار تعداد نویز و بسته‌های بدی که آلوده هستند، مشاهده می‌شود که این موارد به مسیریاب، سوئیچ و هاب در شبکه می‌رسند و نویز می‌گیرند که در این مدل با رنگ زرد و قرمز مشخص می‌شوند. نمودار کاملا صعودی است؛ چون بسته‌ها فقط ارسال می‌شوند و برگشت داده نمی‌شوند. نمودار Correlate: در ابتدا این تابع، مقدار صفر را نشان می‌دهد و این به معنای Validate بودن تابع کرولیت است. اگر در حالت اجرا، تابع کرولیت را کمتر کنیم، نمودار کرولیت مقداری شیب می‌گیرد. با اجرای مدل در نرم‌افزار نت‌لوگو، وقتی بسته‌ها به آدرس اشتباهی ارسال می‌شوند و یا اصلا ارسال نمی‌شوند در قسمت Not complete می‌نشینند. مقدار متغیر مسیریاب در حالت‌های مختلفی قابل تغییر هست تا از این طریق، تحلیل حساسیت مدل انجام شود. به منظور تحلیل حساسیت مدل، بایستی مقادیر هریک از لایه‌ها، کم و یا زیاد شد تا خروجی مدل مشخص و سپس تحلیل مرتبط با هر لایه و در نهایت اعتبار مدل طراحی شده، مشخص گردد. در این پژوهش سه سناریو با هم مقایسه شد.

سناریوی الف- تابع همبسته‌سازی در مدل وجود ندارد، مقدار مسیریاب ۰، ۵۰ و ۱۰۰ می‌باشد. تعداد بسته‌ها در این حالت ۱۰۰ در نظر گرفته شده است.

سناریوی ب- تابع همبسته‌سازی در مدل وجود دارد، مقدار مسیریاب ۵۰، ۷۵ و ۱۰۰ می‌باشد. تعداد بسته‌ها در این حالت ۱۰۰ در نظر گرفته شده است.

سناریوی ج- تابع همبسته‌سازی در مدل دو حالت ۰ و ۱۰۰ و مقدار مسیریاب نیز ۰ و ۱۰۰ می‌باشد. تعداد بسته‌ها در این حالت دو مقدار متفاوت ۵۰۰۰ و ۱۰۰۰۰ در نظر گرفته شده است.

الف- سناریوی اول: اگر تابع همبسته‌سازی، در مدل شبیه‌سازی وجود نداشته باشد ولی مقدار عامل مسیریاب در سه حالت ۰، ۵۰ و ۱۰۰ مورد سنجش قرار گرفته است. تعداد بسته‌ها است.

---

[18] Real-World Validation

[19] Router

جدول شماره ۲

Correlate	0	0	0
Router	0	50	100

ب– سناریوی دوم: تابع همبسته‌سازی، در مدل شبیه‌سازی وجود دارد و مقدار آن به ترتیب: ۵۰، ۷۵ و ۱۰۰ در نظر گرفته شد. مقدار عامل مسیریاب نیز در سه حالت ۰، ۵۰ و ۱۰۰ مورد سنجش قرار گرفته است. تعداد بسته‌ها ۱۰۰ است.

جدول شماره ۳

Correlate	50	75	100	100
Router	0	50	100	0

ج– سناریوی سوم: فرض بر این است که تابع همبسته‌سازی در مدل دو حالت ۰ و ۱۰۰ است و مقدار مسیریاب نیز ۰ و ۱۰۰ می‌باشد. همچنین تعداد بسته‌ها در این حالت دو مقدار متفاوت ۵۰۰۰ و ۱۰۰۰۰ است.

جدول شماره ۴

Correlate	0	100
Router	0	100

اجرای سناریوی اول در سه حالت: اگر تابع همبسته‌سازی، در مدل شبیه‌سازی وجود نداشته باشد.

برای اجرای مدل در حالت سناریوی اول، از لایه، مقدار تابع همبسته‌سازی، ۰ در نظر گرفته شد. خروجی این حالت در جدول زیر آمده است. مقدار مسیریاب در حالت اول از سناریوی الف، ۰ فرض شده است.

نتیجه‌گیری:

در این پژوهش بر اساس تحلیل داده مرکز عملیات امنیت شبکه از طریق تابع همبسته‌سازی، زمینه هشدار مخاطرات فراهم گردید که این با نتیاج پژوهش دیمرتزیس در سال ۲۰۱۹ همراستا است. بکارگیری مدل‌های عامل‌بنیان برای مسائل فرهنگی، اجتماعی از قبیل مدل‌سازی جمعیت، مدیریت مصرف آب توسط امینی و همکاران، ۱۳۹۶ و نیکویی اسکویی و همکاران در سال ۱۳۹۶ انجام شده بود که این با نتایج این پژوهش که از روش عامل‌بنیان بهره گرفته است، همراستا بود. در ادامه پاسخ به سئوال‌های پژوهش و بررسي فرضیه‌ها و نیز نتایج مستقیم حاصل از اجراي پژوهش و حاصل از مطالعات حوزه ادبیات بیان شده است. در این پژوهش با استفاده از اکتشاف عامل‌های تاثیرگذار در تشخیص نفوذ در مرکز عملیات امنیت شبکه، زمینه تحلیل داده‌ها در قالب بسته‌های ورودی شش‌گانه فراهم گردید. عامل‌های تعداد بسته‌ها، فرستنده، گیرنده، احتمال ایجاد نویز، احتمال ایجاد بسته‌های بد (خاطی)، تابع همبسته‌سازی و مسیریاب به عنوان مهمترین شاخص‌های تاثیرگذار در سامانه طراحی‌شده در این پژوهش، تعریف شده است. تحلیل و آنالیز شامل نمایش تحلیل داده‌ها در دو حالت بدون استفاده از تابع همبسته‌سازی و با استفاده از تابع همبسته‌سازی است. در این پژوهش سه سناریو در نظر گرفته شد. سناریویی که تابع همبسته‌سازی، در مدل شبیه‌سازی وجود داشته باشد که مقدار تابع همبسته‌سازی برای این سناریو به ترتیب: ۵۰، ۷۵ و ۱۰۰ در نظر گرفته شد. مقدار عامل مسیریاب نیز در سه حالت ۰، ۵۰ و ۱۰۰ مورد سنجش قرار گرفته است.

جدول شماره ۵

Correlate	50	75	100	100
Router	0	50	100	0

تحلیل داده‌ها بدون استفاده از تابع همبسته‌سازی در سامانه، چگونه خواهد بود؟ تابع همبسته‌سازی، در مدل شبیه‌سازی وجود ندارد و عامل مسیریاب در سه حالت ۰، ۵۰ و ۱۰۰ مورد سنجش قرار گرفته است.

جدول شماره ۶

Correlate	0	0	0
Router	0	50	100

مقایسه سناریوهای قبلی با افزایش تعداد بسته‌ها از ۱۰۰ به ۵۰۰۰:

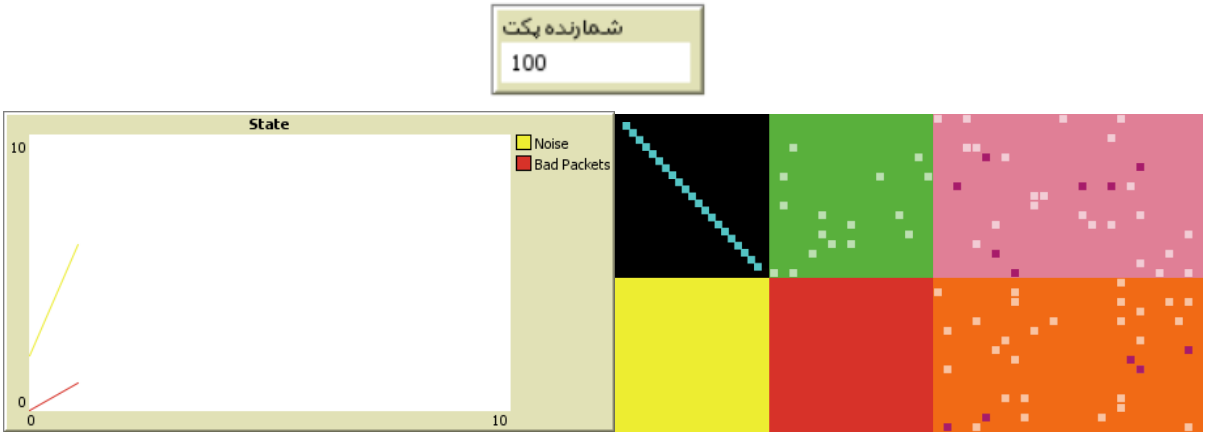
فرض بر این است که تابع همبسته‌سازی در مدل دو حالت ۰ و ۱۰۰ است و مقدار مسیریاب نیز ۰ و ۱۰۰ می‌باشد. تعداد بسته‌ها در این حالت دو مقدار متفاوت ۵۰۰۰ و ۱۰۰۰۰ است.

جدول شماره ۷

Correlate	0	100
Router	0	100

نتایج حاصل از اجرای پژوهش:

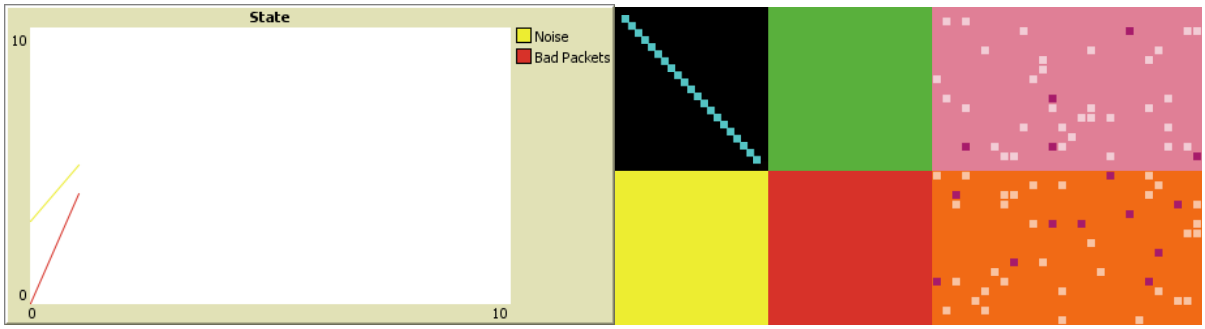
الف- نتایج شامل عدم استفاده از تابع همبسته‌سازی آمده است. مقدار عامل تابع همبسته‌سازی ۰ و عامل مسیریاب ۰ با تعداد بسته ۱۰۰



شکل شماره ۲ نتیجه حاصل از عدم استفاده از تابع همبسته‌سازی

طبق شکل شماره دو، بسته‌های آلوده اعم از: بسته‌های بد و نویزها به مقصد رسیده و در قسمت‌های بنفش و نارنجی، بسته‌های پررنگی به تعداد بیشتری مشاهده می‌شود. در این حالت ۱۰۰ بسته بررسی شده است، اگر تعداد بسته‌ها بیشتر شود، میزان تشخیص بسته‌های بد و نویزها در قسمت‌های نارنجی و بنفش بیشتر نمایان خواهد شد. در محیط سبزرنگ هم بسته‌هایی که اشتباه ارسال شده‌اند، مشخص شده است، چون مقدار عامل مسیریاب ۰ در نظر گرفته شده است، نمودار تابع همبسته‌سازی هم حالت صعودی به خود گرفته است.

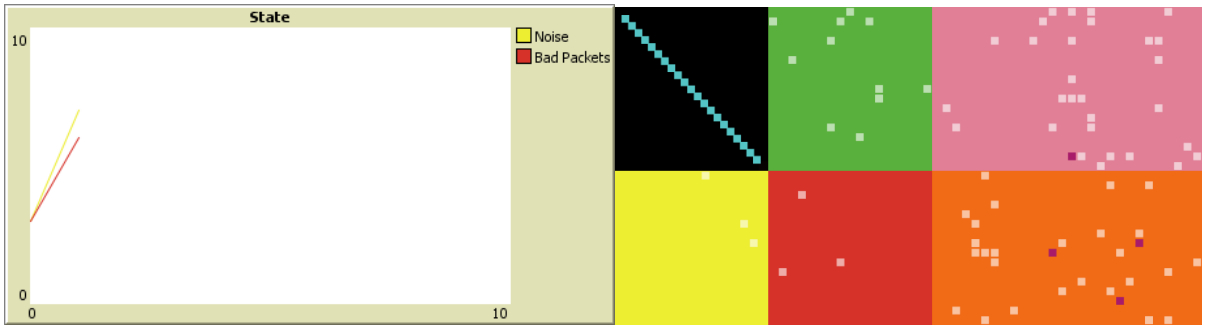
نتیجه سناریو با مقدار عامل تابع همبسته‌سازی ۰ و عامل مسیریاب ۱۰۰



شکل شماره ۳ نتیجه با حاصل تابع همبسته‌سازی صفر

طبق شکل شماره سه، بسته‌های آلوده اعم از: بسته‌های بد و نویزها به مقصد رسیده‌اند و در قسمت‌های بنفش و نارنجی، بسته‌های پررنگی، مشاهده می‌شود. تفاوت این مرحله با مرحله قبل که مقدار عامل مسیریاب از ۵۰ به ۱۰۰ افزایش پیدا کرده است، که تعداد بسته‌هایی که اشتباه ارسال شده‌اند به صفر رسیده است.

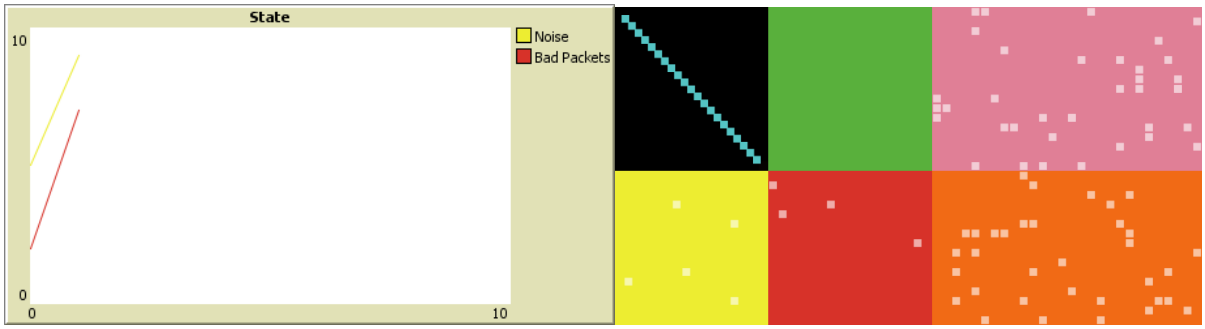
ب- نتایج بکارگیری تابع همبسته‌سازی ارائه شده است. نتیجه سناریو با مقدار عامل تابع همبسته‌سازی ۵۰ و عامل مسیریاب ۰



شکل شماره ۴ نتیجه با حاصل تابع همبسته‌سازی پنجاه

طبق شکل شماره چهار، تعداد بسته‌های آلوده اعم از: بسته‌های بد و نویزهایی که به مقصد رسیده، کاهش یافته و در قسمت‌های بنفش و نارنجی، بسته‌های پررنگی به تعداد خیلی کمتر از حالت سناریویی که مقدار عامل همبسته‌سازی ۰ و مسیریاب ۵۰ بود، مشاهده می‌شود. با افزایش مقدار عامل تابع همبسته‌سازی، تشخیص بسته‌های آلوده اعم از بسته‌های بد و بسته‌هایی که نویز گرفته‌اند (محیط قرمز و زرد رنگ)، افزایش داشته و مدل از طریق تشخیص و پیش‌گیری از رسیدن آن‌ها به مقصد، موفق عمل نموده است. با کاهش عامل مسیریاب از ۵۰ به ۰، میزان بسته‌هایی که اشتباه ارسال شده‌اند نیز افزایش داشته است.

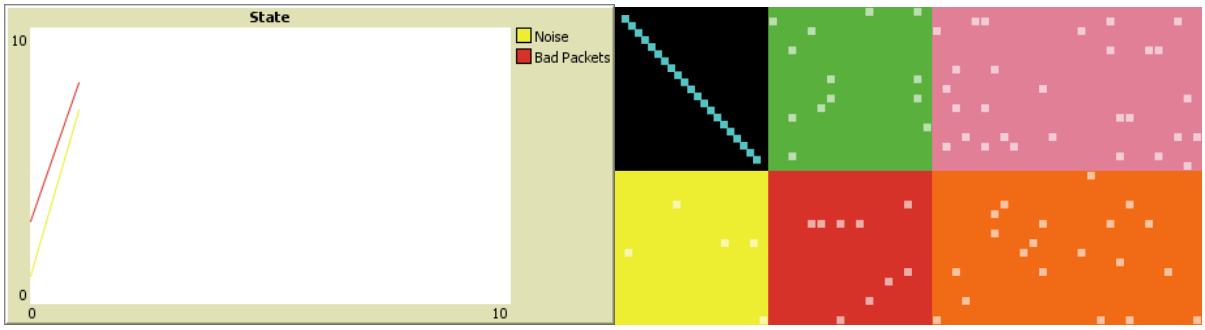
نتیجه سناریو با مقدار عامل تابع همبسته‌سازی ۱۰۰ و عامل مسیریاب ۱۰۰



شکل شماره ۵ نتیجه با حاصل تابع همبسته‌سازی یکصد

طبق شکل شماره پنج، سامانه در تشخیص بسته‌های آلوده اعم از: بسته‌های بد و نویزها موفق عمل نموده و هیچ بسته پررنگی در قسمت مقصد (محیط نارنجی و بنفش) مشاهده نمی‌شود. این یعنی بسته‌هایی که به مقصد رسیده‌اند، کاملا سالم هستند. از طرفی تعداد بسته‌هایی که به اشتباه ارسال شده‌اند به درستی تفکیک شده و در قسمت سبزرنگ (Not Complete) دیده نمی‌شود در عوض تعداد بسته‌هایی بد و نویزدار، بیشتر شده و مدل از رسیدن آن‌ها به مقصد پیش‌گیری نموده است که این در محیط زرد رنگ (Noise) دیده می‌شود.

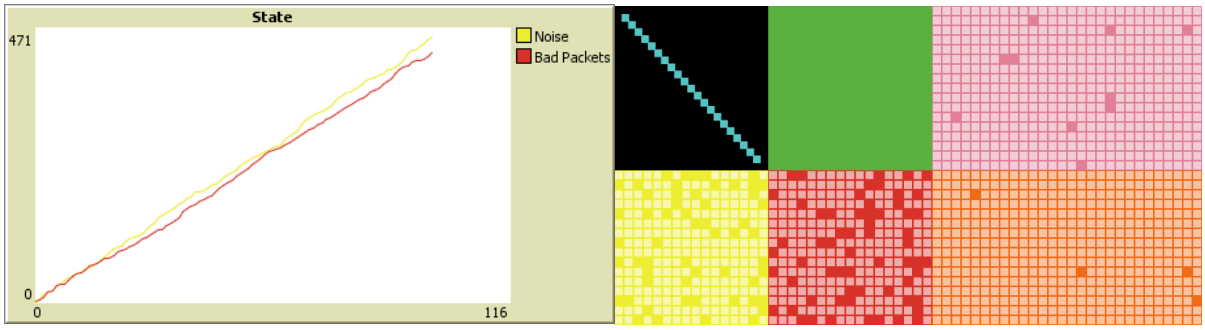
نتیجه سناریو با مقدار عامل تابع همبسته‌سازی ۱۰۰ و عامل مسیریاب ۰



شکل شماره ۶ نتیجه با حاصل تابع همبسته‌سازی یکصد

طبق شکل شماره شش، سامانه در تشخیص بسته‌های آلوده اعم از: بسته‌های بد و نویزها موفق عمل نموده و هیچ بسته پررنگی در شکل شماره شش مشاهده نمی‌شود. این یعنی بسته‌هایی که به مقصد رسیده‌اند، کاملا سالم هستند. با کاهش مقدار عامل مسیریاب به ۰، تعداد بسته‌هایی که اشتباه ارسال شده‌اند (محیط سبز رنگ)، افزایش محسوسی نموده است.

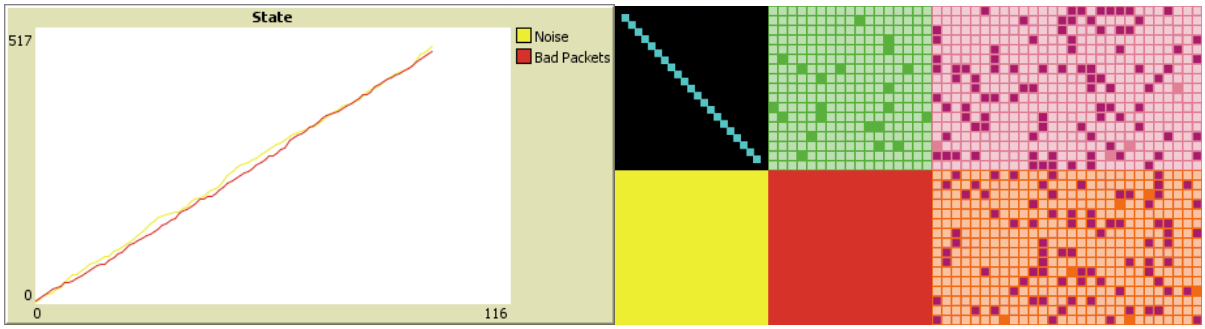
نتیجه سناریو با مقدار عامل تابع همبسته‌سازی ۱۰۰ و عامل مسیریاب ۱۰۰ با تعداد بسته ۵۰۰۰



شکل شماره ۷ نتیجه با حاصل تابع همبسته‌سازی یکصد

طبق شکل شماره هفت، سامانه در تشخیص و پیش‌گیری از رسیدن بسته‌های آلوده اعم از: بسته‌های بد و نویزها به مقصد موفق عمل نموده و هیچ بسته پررنگی در شکل شماره هفت مشاهده نمی‌شود؛ این یعنی بسته‌هایی که به مقصد رسیده‌اند، کاملا سالم هستند. با افزایش مقدار مسیریاب در بالاترین حد ممکن (۱۰۰)، تعداد بسته‌هایی که اشتباه ارسال شده‌اند (محیط سبز رنگ)، کمترین مقدار ممکن (۰) بوده است. همچنین سامانه در تشخیص بسته‌های آلوده اعم از بسته‌های بد و بسته‌های نویز دار موفق عمل نموده است.

نتیجه سناریو با مقدار عامل تابع همبسته‌سازی ۰ و عامل مسیریاب ۰ با تعداد بسته ۵۰۰۰



شکل شماره ۸ نتیجه با حاصل تابع همبسته‌سازی صفر

طبق شکل شماره هشت، سامانه در تشخیص بسته‌های آلوده اعم از: بسته‌های بد و نویزها موفق عمل نکرده است (تعداد بسته‌های پررنگی که در قسمت بنفش و نارنجی مشاهده می‌شود). این یعنی بسته‌های آلوده‌ای که به مقصد رسیده‌اند، بسیار افزایش داشته است. با کاهش مقدار مسیریاب به کمترین حد ممکن (۰)، تعداد بسته‌هایی که اشتباه ارسال شده‌اند (محیط سبز رنگ)، بیشتر شده است. سامانه هیچ بسته‌های آلوده اعم از بسته‌های بد و بسته‌های نویز دار را تشخیص نداده که این بخاطر ۰ بودن مقدار عامل مسیریاب در مدل است.

نتایج حاصل از مقایسه سناریوهای طراحی شده برای سامانه:

الف- مقایسه همبسته‌سازی و مسیریاب با عدد ۰ و تعداد بسته ۱۰۰ و ۵۰۰۰

جدول شماره ۸

مقایسه عوامل	Correlate	Router	Packet Number	Bad packet/Noise	Not Complete	State Diagram	Correlation Diagram
۱	۰	۰	۱۰۰	بسته‌های بد و نویزدار به مقصد رسیده‌اند	افزایش ارسال بسته‌های اشتباه	بسته‌های نویزدار بیشتر از بسته‌های بد است	حالت صعودی نمودار
۲	۰	۰	۵۰۰۰	بسته‌های بد و نویزدار به مقصد رسیده‌اند	افزایش ارسال بسته‌های اشتباه	نویز و بسته-های بد منطبق بر هم هستند	نمودار حالت نزولی گرفته و به مقدار ثابتی رسیده است.

ب- مقایسه همبسته‌سازی و مسیریاب با عدد ۱۰۰ و تعداد بسته ۱۰۰ و ۵۰۰۰

جدول شماره ۹

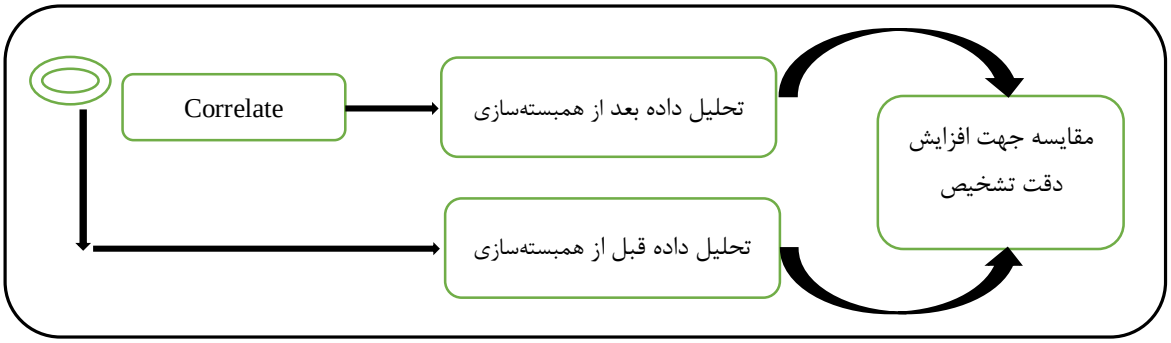
مقایسه عوامل	Correlate	Router	Packet Number	Bad packet/Noise	Not Complete	State Diagram	Correlation Diagram
۱	۱۰۰	۱۰۰	۱۰۰	بسته‌های نویزدار افزایش داشته است.	افزایش ارسال بسته‌های اشتباه	بسته‌های بد و نویزدار به موازی هم حالت صعودی گرفته‌اند	حالت ثابت صفر روی محور زمان
۲	۱۰۰	۱۰۰	۵۰۰۰	مقدار ۰	بسته‌های اشتباه وجود ندارد	نویز و بسته-های بد منطبق بر هم هستند	حالت ثابت صفر در محور زمان

پ- مقایسه همبسته‌سازی و مسیریاب با عدد ۱۰۰ و تعداد بسته ۱۰۰

جدول شماره ۱۰

مقایسه عوامل	Correlate	Router	Packet Number	Bad packet/Noise	Not Complete	State Diagram	Correlation Diagram
۱	۰	۱۰۰	۱۰۰	بسته‌های آلوده (بد و نویزدار) به مقصد رسیده‌اند	مقدار بسته‌های اشتباه صفر است	بسته‌های بد و نویزدار حالت صعودی گرفته-اند	حالت ثابت صفر روی محور زمان
۲	۱۰۰	۰	۱۰۰	مقدار ۰	افزایش بسته-های اشتباه	نویز و بسته-های بد موازی با هم حالت صعودی دارند	حالت ثابت صفر روی محور زمان

با توجه به نتایج شبیه‌سازی در این پژوهش، وجود عامل همبسته‌سازی در مدل باعث می‌شود تا بسته‌های آلوده اعم از بسته‌های بد(خاطی) و بسته‌های نویزدار، به عنوان بسته آلوده تشخیص داده شده و به مقصد نرسند. با توجه به نتایج این پژوهش، وجود عامل مسیریاب در مدل باعث شده که بسته‌های ارسال شده در شبکه، درست به مقصد رسیده و در مسیر، اشتباه ارسال نشوند. مدل مفهومی پژوهش نشان داد که وجود عامل‌های همبسته‌سازی و مسیریاب در مدل ضروری بوده و از این طریق، بسته‌های آلوده به درستی تشخیص داده شده و از رسیدن این بسته‌ها به مقصد توسط سامانه، پیش‌گیری خواهد شد.



شکل شماره ۹ مدل پژوهش

بر اساس مدل رابینسون، آزمون مدل انجام و در نهایت، سامانه مورد تایید قرار گرفت. اساس طراحی سامانه هوش امنیتی مرکز عملیات امنیت شبکه، شامل جدول زیر است:

جدول شماره ۱۱

نوع اجرا	زبان پشتیبانی	روش	بررسی نتیجه	آنلاین/ آفلاین
تحت شبکه	جاوا	عامل‌بنیان	الف–تشخیص بسته‌های آلوده اعم از بسته‌های خاطی و بسته‌های نویزدار در شبکه بر اساس بکارگیری تابع همبسته‌سازی/ بدون تابع همبسته‌سازی ب– تشخیص بسته‌هایی که در شبکه اشتباه ارسال می‌شوند	آفلاین

نتیجه آن که وجود عامل‌های همبستگی و مسیریاب در مدل ضروری بوده و از این طریق، بسته‌های آلوده به درستی تشخیص داده شده و از رسیدن این دسته از بسته‌ها به مقصد، پیش‌گیری خواهد شد. پیشنهاد می‌شود در طراحی سامانه، هر دو حالت آنلاین و آفلاین مد نظر قرار گرفته و از سایر نرم‌افزارهای مدل‌سازی، استفاده و نتایج با این پژوهش مقایسه شود.

منابع:

۱. آذرفر، امیر، آذر، عادل، گودرزی، غلامرضا (۱۳۹۵). شبیه‌سازی تغییرات جمعیتی ایران، ارائه مدل پایه عامل‌بنیان.

۲. امینی، الهام، خدیور، آمنه، موسوی، میرحسین، ژو، مینگ (۱۳۹۶)، طراحی یک مدل عامل‌بنیان برای بازتولید تقاضای کل بخش‌های مختلف اقتصادی در اثر تغییرات تقاضای نهایی، کارشناسی ارشد، دانشگاه الزهرا (س).

۳. پورابراهیمی، علیرضا، قنبری، فائزه، نظری فرخی، ابراهیم، سلیمانی، فاطمه (۱۳۹۶). سند راهبردی پدافند غیرعامل وزارت ارتباطات و فناوری اطلاعات.

۴. جلینی، سحر، خاکستری، مرضیه، عاملی، احمد (۱۳۹٤)، تحلیل رفتار اعضای اوپک (نظریه بازی تکاملی – مدل‌سازی عامل بنیان)، کارشناسی ارشد، دانشگاه خوارزمی.

۵. صالح، رضا، نوری، فرهاد، نوروزی، احسان (۱۳۹۱). ساختار پایگاه دانش، مستند پروژه مرکز عملیات امنیت، شرکت پیام‌پرداز، شهرک علمی و تحقیقاتی دانشگاه صنعتی اصفهان.

۶. قربانی، ولی‌ا...، محمدی، علی (۱۳۹۶). بررسی عملکرد مرکز عملیات امنیت و ارائه الگوي مناسب براي بکارگیري در ایران، همایش ملی دفاع و امنیت، دانشگاه عالی دفاعی ملی.

۷. قلعه‌بان تکمه‌داش، میلاد، طاهری تیزرو، عبدالله، زارع ابیانه، حمید (۱۳۹٤). «چارچوب مدل‌های عامل‌بنیان در شبیه‌سازی رفتار ذی‌نفعان برای مدیریت منابع آب»، نشریه آب و توسعه پایدار، سال دوم، شماره ۱، شهریور ، صفحات ۸۷-۹۷.

۸. کیان‌پور، علیرضا (۱۳۹۵). هوش امنیتی، دومین همایش بین‌المللی بانکداری الکترونیک و نظام‌های پرداخت.

۹. ملک‌زاده، غلامرضا، سلطانی، فرشته (۱۳۹۳). «سیستم‌های هوشمند کسب و کار و تحول‌گرایی مدیران در شرکت‌های کوچک و متوسط»، فصلنامه رشد فناوری، سال یازدهم، شماره ۴۱.

۱۰. مودی، آرمین، مردمی، کریم (۱۳۹۶)، طراحی مرکز فرهنگی فناوری‌های معماری با استفاده از مدل‌سازی عامل محور، کارشناسی ارشد، دانشگاه بین‌المللی امام رضا(ع).

۱۱. نیکی اسکویی، کامران، بهبودی، داود، اصغرپور، حسین (۱۳۹۶)، تدوین استراتژی بهینه ایران در تجارت بین‌المللي گاز: رویکرد مدل‌سازی عامل‌بنیان، کارشناسی ارشد، دانشگاه تبریز.

1. Konstantinos Demertzis, Nikos Tziritas, Panayiotis Kikiras, Salvador Llopis Sanchez and Lazaros Iliadis (2019). The Next Generation Cognitive Security Operations Center: Adaptive Analytic Lambda Architecture for Efficient Defense against Adversarial Attacks, big data and cognitive computing.
2. Nathans, David (2015). Designing and Building Security Operations Center 1st Edition.
3. Wilensky, U., & Rand, W. (2015). An introduction to agent-based modeling. Agent analyst.