فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال ششم، شماره 1، بهار 1401

ارائه مدل گسترده برای آگاهی وضعیتی در دفاع سایبری فعال

علی جبار رشیدی[1]، حامد رادی نیا[2]*

تاریخ دریافت: 1401/03/18 **تاریخ پذیرش**: 1401/05/15

چکیده

امروزه حملات پیشرفته‌ی سایبری، خطرهای جدی را برای اقتصاد و امنیت ملی کشورها پدید آورده‌اند. متاسفانه غالبا مهاجمین و بدافزارهای رایانه‌ای یک قدم از سیستم‌های امنیتی جلوتر می‌باشند. از این رو باید به جای انتظار برای مواجهه با تهدیدات و هجمه‌های احتمالی، یعنی همان روش‌های پیشین دفاع سایبری، به دنبال راه‌حلی قوی‌تر و هوشمندانه‌تر برای از میان بردن آن خطر احتمالی باشیم. اینجاست که نظریه "دفاع سایبری فعال" مطرح می‌شود که بخش اساسی آن آگاهی وضعیتی سایبری می‌باشد. طی چند سال اخیر متخصصان و پژوهشگران همواره به دنبال یک آگاهی وضعیتی فعالانه، موثر و هوشمند برای دستیابی به یک دفاع مطلوب در مقابل حملات پیچیده امروزی بوده‌اند. با ظهور دفاع سایبری فعال و اثبات اثربخشی و بازدارندگی بالای آن در بهبود دفاع سایبری، دستیابی به یک مدل مطلوب آگاهی وضعیتی بر مبنای مفاهیم و رویکردهای این نوع دفاع، از اصلی ترین موضوعات تحقیقاتی در این مسئله می‌باشد.

در این مقاله با ارائه یک مدل پیشنهادی گسترده و جامع آگاهی وضعیتی سایبری به همراه زیربخش‌های آن بر مبنای راهبردها و تکنیک‌های دفاع سایبری فعال در مقایسه با سایر مدل‌ها، تغییر اساسی در بهبود دفاع سایبری خصوصا در زیرساخت‌های حیاتی و حساس ایجاد خواهد شد. برخی از این راهبردها و تکنیک‌ها شامل راهبرد هک متقابل، مقابله با حملات صفر روزه، آگاهی وضعیتی اشتراکی و غیره می‌باشند. ارائه یک تعریف جدید از مؤلفه قدرت مدافع و افزایش ضرایب آن با بهره‌گیری از شاخصه‌های مدل پیشنهادی و همچنین بررسی نتایج ارزیابی بر اساس نظریه بازی‌ها نشان می‌دهد، مدل گسترده پیشنهادی کارایی بهتری در مقابله با حملات مهاجمین داشته است.

واژگان کلیدی: دفاع سایبری، دفاع سایبری فعال، آگاهی وضعیتی، هک متقابل، بازدارندگی، حملات صفر روزه

[1] دانشیار و عضو هیئت علمی مجتمع برق و کامپیوتر دانشگاه صنعتی مالک اشتر تهران rashidi@mut.ac.ir (نویسنده مسئول)

[2] کارشناسی ارشد مهندسی کامپیوتر گرایش رایانش امن دانشگاه صنعتی مالک اشتر تهران h.radinia@gmail.com

1. مقدمه

امروزه حملات سایبری[1] دارای پیچیده‌گی‌های زیادی هستند و نفوذگران[2] باهوش‌تر از گذشته با شناسایی دقیق شبکه مورد نظر و طی کردن یکسری از دستورالعمل‌های از پیش تعیین شده حملات خود را آغاز می‌نمایند[7]. دولت‌ها در سراسر جهان، به منظور حفاظت از زیرساخت‌های اطلاعاتی حساس، راهبردها و قابلیت‌های امنیتی یا برنامه‌های پاسخ به حادثه ملی را درون چشم انداز تهدید جدید در عصر سایبری قرار می‌دهند[18].

مَشی کلی و متداولی که نفوذگرانی حرفه‌ای برای حمله به شبکه استفاده می‌کنند به خوبی قابل فهم می‌باشد[7]. جمع‌آوری اطلاعات، شناسایی هدف، برنامه ریزی اولیه و توسعه آن، شناسایی شبکه، دنبال نمودن برنامه و آماده‌سازی، حمله و ارزیابی خسارات از این دست می‌باشند. این فرآیند در زمان اجرا دارای نقاط تصمیم گیری کنترل شده (مانند نقطه برگشت یا پایان عملیات) است. موفقیت در تاثیرگذاری بر تصمیم گیری‌های نفوذگر در این نقاط کلیدی می‌تواند نتیجه خوبی برای مدافع داشته باشد. به مجموعه اقدامات بازدارنده، رفع کننده، دفع کننده و بازیابی کننده به منظور پیشگیری، حفظ، حمایت از ارزش‌ها، منافع و دارایی‌های ملی در مقابل تهدیدات و حملات سایبری انجام می‌گیرد، دفاع سایبری می‌گویند[3]. البته این تعریف حاوی معیارهای پیش‌کنشگرانه[3] مربوط به دفاع سایبری فعال[4] نیز می‌باشد. تعریف دفاع سایبری قبل از ورود مفهوم دفاع سایبری فعال به عرصه سایبر، به دسته‌ای از اقدامات که به منظور مقابله با آسیب‌های ناشی از رویدادهای سایبری یا بازگردانی کارکرد سیستم‌ها و شبکه‌ها به حداکثر عملکرد ممکن در زمان به وقوع پیوستن یک رویداد به کار می‌روند، گفته می‌شد، که همان تعریف دفاع سایبری غیرفعال[5] می‌باشد. اکثرا دفاع سایبری فعال را در مقابل دفاع سایبری غیر فعال قرار می‌دهند و استفاده از پادآوندها[6]، ضدبدافزارها[7] و فن‌آوری‌های تشخیص بدافزار[8] را دفاع سایبری غیرفعال می‌دانند. اساسا غیرفعال دانستن بقیه رویکردهای دفاعی نادرست است و باید آن را ناشی از نبود تعریف روشن برای آن‌ها دانست. دفاع سایبری فعال تنها عبارتی نیست که نیاز به یک تعریف درست دارد بلکه برای دسته‌ای از اقدامات که به منظور مقابله با آسیب‌های ناشی از رویدادهای سایبری یا بازگردانی کارکرد سیستم‌ها و شبکه‌ها به حداکثر عملکرد ممکن در زمان به وقوع پیوستن یک رویداد به کار می‌روند نیز یک تعریف کامل و درست نیاز است. بدین منظور به جای استفاده از عبارت نادرست دفاع سایبری غیرفعال باید از یک دسته بندی دقیق‌تر برای این اقدامات یعنی مفهوم دفاع سایبری مستحکم[9] و دفاع سایبری تاب‌آور[10] استفاده شود. دو مفهوم دفاع سایبری مستحکم و دفاع سایبری تاب‌آور به نوعی زیرمجموعه مفهوم دفاع سایبری پیشین بوده است.

یکی از بهترین تعاریف موجود برای دفاع سایبری فعال توسط رابرت دوار[3] در سال 2014 ارائه شده است. او دفاع سایبری فعال را یک الگوی امنیتی دارای دو مؤلفه زیر بیان می‌کند.

- شناسایی و مقابله برخط با تهدیدات در شبکه‌های مدافعین
- ظرفیت اتخاذ اقدام متقابل تهاجمی و خشن در شبکه خارجی

بنابراین اینگونه دفاع سایبری فعال را تعریف نموده است: "رویکردی به منظور دستیابی به امنیت سایبری[11] مبتنی بر بکارگیری تدابیری برای کشف، شناسایی، تجزیه و تحلیل و مقابله با تهدیدات به صورت برخط از داخل و خارج شبکه‌ها و سیستم‌های ارتباطی، ترکیب شده با توانایی و ابتکار در انجام اقدامات پیش‌کنشگرانه یا تهاجمی در قبال تهدیدات و موجودیت آن‌ها شامل اقداماتی در شبکه‌های خانگی حمله‌کنندگان[3]."

اطلاعات جزء مهم‌ترین بخش‌های دفاع سایبری فعال بوده و جمع‌آوری اطلاعات به هر طریق و روش ممکن جزء اصلی ترین

[1] Cyber Attacks
[2] Hackers
[3] Proactive Measures
[4] Active Cyber Defense (ACD)
[5] Passive Cyber Defense
[6] Firewall
[7] Antivirus
[8] Intrusion detection system
[9] Fortified Cyber Defense (FCD)
[10] Resilient Cyber Defense (RCD)
[11] Cyber Security

رکن این نوع دفاع می‌باشد. این جمع آوری اطلاعات از مهاجم به حدی اهمیت دارد که حتی روش حمله متقابل هم در این نوع دفاع سایبری به عنوان یک عامل بازدارنده قوی و ایجاد کننده آگاهی وضعیتی، مورد بررسی و پیاده‌سازی قرار می‌گیرد. نفوذگر باید در مرحله تجسس و پویش شبکه شکست داده شود و مغلوب گردد، نه در زمانی که حمله را انجام داده است. زیرا حین شناسایی شبکه، نفوذگران به علت نداشتن اطلاعات کافی در مدت زمان طولانی تری در معرض خطر هستند. بدین ترتیب نفوذگران در این زمان بیشتر مستعد آسیب دیدن می‌باشند. دفاع فعال سایبری برای محقق نمودن این منظور از روش‌ها و تکنیک‌های منحصربه فرد مختلفی استفاده می‌کند، که هدف همه آن‌ها جمع آوری اطلاعات و ایجاد یک آگاهی وضعیتی از شبکه خودی، خود مهاجم، روش‌ها، تکنیک‌ها و ابزارهای مورد استفاده او می‌باشد[7].

طبق گفته اندسلی[4]، آگاهی وضعیتی به طور ساده این است که بدانید در اطراف شما چه می‌گذرد. تعریفی که وی به این صورت گسترش داده است. "مشاهده عناصر در محیط در یک حجم از زمان و مکان، درک و فهم معنای آن‌ها و پیش بینی وضعیت آن‌ها در آینده نزدیک".

ذکر این نکته ضروریست که کشورهای پیشتاز در عرصه سایبری یک به یک در حال گذار از دفاع سایبری غیر فعال به دفاع سایبری فعال هستند، و برای رسیدن به هدف خود برنامه‌های چند ساله طراحی نموده‌اند. در این بین کشور جمهوری اسلامی ایران با تهدیدهای زیادی در این عرصه روبرو است و باید همگام با دیگر کشورهای قدرتمند جهانی، حرکت خود به سمت دفاع سایبری فعال را آغاز نماید. بدین منظور باید با شناخت جنبه‌های مختلف آن و ارائه یک مدل گسترده از مهم ترین بخش این دفاع یعنی آگاهی وضعیتی، بهترین تعریف و مدل را ارائه دهد.

ما در این مقاله با ارائه یک مدل پیشنهادی گسترده و جامع آگاهی وضعیتی سایبری به همراه زیربخش‌های آن بر مبنای راهبردها و تکنیک‌های دفاع سایبری فعال، تغییر اساسی در بهبود دفاع سایبری خصوصا در زیرساخت‌های حیاتی و حساس ایجاد می‌کنیم. برخی از این راهبردها و تکنیک‌ها شامل راهبرد اقدام فعال (هک متقابل[1])[5و24]، مقابله با حملات صفر روزه[2]، آگاهی وضعیتی اشتراکی[3] و غیره می‌باشند. ارائه یک تعریف جدید از مؤلفه قدرت مدافع و افزایش ضرایب آن با بهره‌گیری از شاخصه‌های مدل پیشنهادی و همچنین بررسی نتایج ارزیابی بر اساس نظریه بازی‌ها نشان می‌دهد، مدل گسترده پیشنهادی کارایی بهتری در مقابله با حملات مهاجمین داشته است.

در بخش‌های بعدی مقاله به دفاع سایبری فعال، آگاهی وضعیتی سایبری و پیشینه آن‌ها پرداخته می‌شود. سپس مدل پیشنهادی با زیرشاخه‌های آن ارائه شده و در بخش بعدی توسط نظریه بازی‌ها مورد ارزیابی قرار می‌گیرد. در انتها نیز نتیجه‌گیری ذکر می‌گردد.

2. کلیات

2-1. دفاع سایبری فعال

رویکردهای دفاعی پیشین دیگر جوابگوی حملات پیچیده و هوشمند مهاجمان نیستند و همیشه چندین گام از آن‌ها عقب‌تر می‌باشند[6]. به همین علت متخصصان و کارشناسان حوزه سایبری چند سالی است که نظریه یک رویکرد جامع، هوشمند، خودکار و بلادرنگ را مطرح نمودند. این نظریه "دفاع سایبری فعال" نام گرفته است که مهم ترین بخش آن آگاهی وضعیتی می‌باشد. دفاع سایبری فعال مبتنی بر استفاده از ابزارهایی است که نه تنها حوادث سایبری را در هنگام وقوع شناسایی و متوقف می‌کند، بلکه اقدامات تهاجمی را برای به حداقل رساندن قابلیت‌های مهاجمان انجام می‌دهد. علاوه بر این می‌تواند از طریق انواع راه‌های فنی مانند استقرار طعمه یا هک کردن شبکه مهاجم اقداماتی را جهت خنثی سازی فعالیت‌های صورت گرفته انجام دهد[1]. با توجه به تمامی تعریف‌های موجود برای دفاع سایبری فعال و بررسی و تحلیل‌های انجام گرفته در خصوص این نوع دفاع، تعریف ما به صورت زیر ارائه می‌گردد:

یک توانایی هماهنگ، خودکار و برخط به منظور کشف، شناسایی و مقابله با تهدیدات قبل از وقوع خسارت با استفاده از یک آگاهی وضعیتی قدرتمند و اشتراک گذاری اطلاعات تهدید[4] بوده که از

[1] Hack-back
[2] Zero-day Attack
[3] Shared Situational Awareness
[4] Threat Intelligence

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال ششم ، شمارهٔ یک، بهار 1401

تمامی ظرفیت‌های دفاع‌های پیشین(پیشگیرانه و تاب‌آور و بازسازی کننده) در کنار تکنیک‌های منحصربه فرد دفاع سایبری فعال شامل توانایی و ابتکار در انجام اقدامات پیش‌کنشگرانه یا تهاجمی با تکیه بر اصل مدیریت خطرپذیری سیستم و محیط، بهره می‌گیرد.

همان‌طور که در شکل(1) مشخص است، چرخه دفاع سایبری فعال ماموریت یک چرخه فعال دفاع سایبری ادامه دار و بدون توقف را مفهوم‌سازی نموده که شامل چهار فاز (مرحله) می‌باشد:

- شناسایی دارایی‌ها و نظارت بر امنیت شبکه
- واکنش به حوادث
- تهدید و دست کاری محیط
- بهره برداری از اطلاعات تهدید

شکل(1): چرخه دفاع سایبری فعال[8]

چرخه دفاع سایبری فعال یک چرخه ادامه دار و بدون حالت پایان می‌باشد. اگرچه همانند یک چرخه‌ای از رخدادهای متوالی معرفی شده است ولی در عمل فازهای چرخه دفاع سایبری فعال، فرآیندهای ادامه داری را نشان می‌دهد که به طور همزمان اتفاق افتاده و به هم وابسته می‌باشند.در واقع شناسایی دارایی‌ها و نظارت برامنیت شبکه یک آگاهی وضعیتی[1] قدرتمند از طریق شناخت محیط یک سازمان، شامل یک محاسبه دقیق از تجهیزات شبکه، یک فهم عمیق از معماری شبکه و یک نظارت موثر بر فعالیت‌های شبکه، ایجاد می‌نماید. بهره برداری از اطلاعات تهدید، شناسایی و استفاده از اطلاعات تهدید مناسب برای محیط کاری یک سازمان، دارایی‌های شبکه و معماری آن می‌باشد. واکنش به حوادث، اقدامی است که به منظور مقابله با یک تهدید شناسایی شده در شبکه یک سازمان انجام می‌گیرد. تهدید و دستکاری محیط مشخص می‌نماید چطور یک سازمان انتخاب می‌کند که از طریق تعامل با تهدید، اطلاعات بیشتری از آن بدست آورد یا از طریق دستکاری محیط با تهدید مقابله نماید. این شامل اقداماتی از قبیل تجزیه و تحلیل ایستا و پویای بدافزارها و ایجاد تغییرات فیزیکی یا منطقی در معماری شبکه باشد.

آمریکا و انگلستان به عنوان دو قدرت سایبری مدل‌های دفاع سایبری فعال بومی را طراحی نموده و توسعه داده‌اند. مرکز دارپای[2] ایالات متحده آمریکا در سال 2015 راهبرد دفاع سایبری فعال را با ارائه مدل شارکسیر[3] پیاده سازی نمود[9]، که می‌تواند در مقابل حملات صفر روزه نیز مقاومت نماید. مرکز ملی امنیت سایبری[4] انگلستان نیز در سال 2016[10]، راهبرد پنج ساله‌ای برای تحقق و پیاده سازی دفاع سایبری فعال در کشور خود ارائه داده است. همه این‌ها نشان دهنده اهمیت دفاع سایبری فعال و لزوم حرکت جمهوری اسلامی ایران به سمت پیاده‌سازی مدل‌های بومی این نوع دفاع می‌باشد.

2-2. تکنیک‌های اختصاصی ACD[5]

از گزینه‌های دفاعی نسبتاً متداول و کم‌خطر دفاع سایبری فعال می‌توان از به اشتراک گذاری اطلاعات[6] و استفاده از تله عسل یا تارپیت[7] نام برد. یک متخصص امنیت رایانه که از یک تله عسل در شبکه خود استفاده می‌کند، می‌تواند با فرض اینکه این سیستم مهاجم را فریب می‌دهد، تکنیک‌های حمله مهاجم را مشاهده کرده و از این مشاهدات برای اطلاع دفاع در شبکه واقعی مدافع استفاده نماید. همچنین تارپیت سرویسی در یک سیستم رایانه‌ای یا سرور است که عمداً اتصالات ورودی را به تاخیر می‌اندازد و به شناسایی کرم‌های مخرب کمک می‌نماید.

[1] Situational Awareness (SA)
[2] The Defense Advanced Research Projects Agency
[3] sharkseer
[4] National Cyber Security Centre (NCSC)
[5] Active Cyber Defense
[6] Information sharing
[7] Honeypot or Tarpits

تکنیک انکار و فریب سایبری[1] یکی دیگر از روش‌های دفاعی کم خطر است که می‌تواند برای مشاهده رفتار مهاجم، طراحی سایر تکنیک‌های دفاعی فعال و بهبود قابلیت پاسخ به حوادث مورد استفاده قرار گیرد. این تکنیک توانایی پنهان سازی اطلاعات واقعی و آشکارسازی اطلاعات غلط را داشته تا درک متجاوز از اطلاعات موجود در یک سیستم رایانه‌ای، آسیب پذیری‌های آن سیستم و دفاع‌های مستقر در شبکه را مختل کند. فرآیند شکار مهاجمان در شبکه، بیرون کردن مهاجمین در صورت دور زدن اقدامات غیرفعال دفاعی و ورود به شبکه مدافع می‌باشد. شکار مهاجمین[2] به همان اندازه که به منظور از بین بردن تهدیدها بوده، شناسایی روش‌ها و واکنش‌های قابل اجرای آنان را نیز در نظر می‌گیرد و به افشای آن‌ها نیز می‌پردازد. تکنیک‌هایی مانند دیده‌بان شبکه[3] با مشاهده کل رویدادهای شبکه و جابه جایی آدرس شبکه[4] به منظور ارسال ترافیک مشکوک به سرورهای از پیش تعیین شده جهت ارزیابی می‌توانند اطلاعاتی در مورد حملات احتمالی بدست آورند[5و7]. همچنین استفاده از کرم‌های سفید[5]، به عنوان نوعی نرم افزارهای بی‌خطر شبیه ویروس‌ها که وظیفه جستجو و نابود ساختن نرم افزارهای مخرب، تشخیص تجاوز و همچنین ایفای نقش در شیوه‌های بازیابی را دارند، یکی دیگر از تکنیک‌های موثر این نوع دفاع هستند[3].

برخی از تکنیک‌ها دفاع فعال، فعالیت‌هایی هستند که مخاطره بیشتری را شامل می‌شوند، زیرا عموماً شامل عملیات خارج از شبکه شخص بوده و در صورت استفاده بدون دقت لازم، می‌تواند منجر به آسیب‌های جانبی جزئی یا نگرانی‌های مربوط به حریم خصوصی شوند. این فعالیت‌ها شامل استفاده از بیکن‌ها[6] و جمع آوری اطلاعات در وب عمیق[7] و وب تاریک[8] است. بیکن‌ها قطعاتی از کد هستند که در پرونده‌هایی که حاوی اطلاعات حساس هستند جاسازی شده‌اند. آن‌ها را می‌توان به دو طریق اصلی عملیاتی کرد. اولاً بیکن‌هایی با مخاطره پایین که به سادگی اگر یک موجودیت غیرمجاز بخواهد فایلی را از شبکه خانگی حذف کند، به صاحب آن هشدار می‌دهند و به عنوان یک زنگ هشدار داخلی عمل می‌کند. دوم، بیکن‌هایی تهاجمی‌تر برای بازگرداندن اطلاعات قربانی از میان آدرس‌های اینترنتی و پیکربندی شبکه سیستم‌های رایانه‌ای که یک سند سرقت شده از طریق آن‌ها هدایت می‌شود، طراحی شده‌اند.

مدافعان شبکه به طور فزاینده‌ای متوجه این امر خواهند شد که اطلاعاتی که از طریق شبکه تاریک عبور می‌کند توانایی این را دارد که برای اطلاع از راهبردهای دفاعی و هشدار مقامات امنیتی، به اطلاعات در مورد یک آسیب پذیری کمک کننده باشد. در این قلمرو از اینترنت که در آن وب سایت‌ها از سرورهای قابل ردیابی جدا شده‌اند، ناشناس بودن کاربران رایج است و اطلاعات آنان بین شبکه‌های معتبر و گروه‌های امن هدایت می‌شود. این شبکه در تجارت مجرمانه اطلاعات سرقت شده و خدمات بدافزارها رایج بوده و از این رو امکانات اطلاعاتی مناسبی برای مدافعان شبکه فراهم می‌نماید. به عنوان مثال، تیم امنیتی یک بانک می‌تواند در بازارهای غیرقانونی جستجو کرده و اطلاعات شخصی یا مالی برای فروش را با اطلاعاتی که بانک در مورد مشتریان و حساب‌های آن‌ها حفظ می‌کند مقایسه کند. اگر تیم امنیتی این مورد مهم را کشف کند، به احتمال زیاد یک نفوذگر شبکه آن‌ها را نقض کرده و بدون ایجاد زنگ هشدار، داده‌های حساس را با موفقیت سرقت کرده است. مدافعان، که اکنون از وجود آسیب پذیری شبکه آگاه شده‌اند، می‌توانند به دنبال تقویت شکاف در معماری امنیتی خود باشند و پیش از به خطر انداختن اطلاعات بیشتر، نفوذگران را از سیستم و شبکه خود دور کنند. از دیگر اقدامات دفاع فعال که بیشتر تهاجمی و خطرناک هستند، شامل باج افزارهای کلاه سفید[9]و ماموریت نجات[10]، اغلب مورد توصیه برای اطلاعاتی هستند که قبلاً از شبکه شخصی سرقت شده است. در حالی که استفاده مخرب از باج افزار در سال‌های گذشته به یکی از نگران‌کننده‌ترین موضوعات امنیت سایبری تبدیل شده است، کارشناسان امنیتی امکان استفاده از ابزارهای مشابه برای

[1] Denial and Deception
[2] Hunting
[3] Network Telescope
[4] Network Address Hopping
[5] White Worm
[6] Beacons
[7] Deep Web
[8] Dark Web
[9] White-Hat Ransomware
[10] Rescue Mission

رمزگذاری داده‌های سرقت شده که در حال انتقال در شبکه سوم هستند را در نظر گرفته‌اند. به این ترتیب، آن‌ها می‌توانند به شخص سوم اطلاع دهند که نفوذگران شبکه آن‌ها را به خطر انداخته و از آن برای انتقال داده‌های سرقت شده استفاده می‌کنند. باج افزار کلاه سفید به مدیران شبکه اطلاع می‌دهد و می‌تواند اطلاعات سرقت شده را بازیابی کرده و سپس باج افزار را از رایانه‌های طرف سوم حذف کند. ماموریت نجات نیز مجموعه اقداماتی است که به موجب آن به سیستم و شبکه مهاجم نفوذ شده و فایل‌های دزدیده شده در معرض خطر برگردانده شود[5,21و24].

2-3. آگاهی وضعیتی سایبری

آگاهی وضعیتی به عنوان حالتی از آگاهی نسبت به شرایطی که در اطراف ما وجود دارد، به ویژه شرایطی که مربوط به ما بوده و ما به آن‌ها علاقه مند هستیم، تعریف می‌شود[11]. مدل اندسلی به عنوان یک مدل مرجع در آگاهی وضعیتی سایبری بوده و سایر مدل‌های آگاهی وضعیتی بر پایه آن توسعه داده شده‌اند. آگاهی وضعیتی توسط اندسلی به صورت زیر تعریف شده است: «آگاهی وضعیتی، درک یک عناصر محیط در یک زمان و مکان مشخص، شناخت معنای آن‌ها، و پردازش وضعیت آن‌ها در آینده نزدیک است[4]. یک مدل آگاهی وضعیتی سایبری کامل باید روی پیشگیری، یعنی پیاده‌سازی یک سیستم هشدار زودهنگام که می‌تواند حوادث ملی را پیشگیری و شناسایی کند، تمرکز نماید[12].

بر مبنای تعریف آگاهی وضعیتی ارائه شده توسط اندسلی، تشکیل آگاهی وضعیتی شامل سه سطح است.

سطح 1: مشاهده عناصرها در محیط، اولین قدم در دستیابی به آگاهی وضعیتی است. این سطح، مشاهده وضعیت، ویژگی‌ها، و دینامیک[1]های عناصر مرتبط در محیط را پوشش می‌دهد.

سطح 2: فهم وضعیت کنونی بر مبنای خروجی سطح(1) انجام می‌شود. این سطح شامل شناخت اهمیت عناصر مرتبط است.

سطح 3: تجسم وضعیت‌های آتی، قابلیت پیش‌بینی کنش‌های آینده عناصر در محیط را پوشش می‌دهد. این موضوع با اطلاعات وضعیت و دینامیک عناصر و فهم وضعیت انجام می‌شود[13].

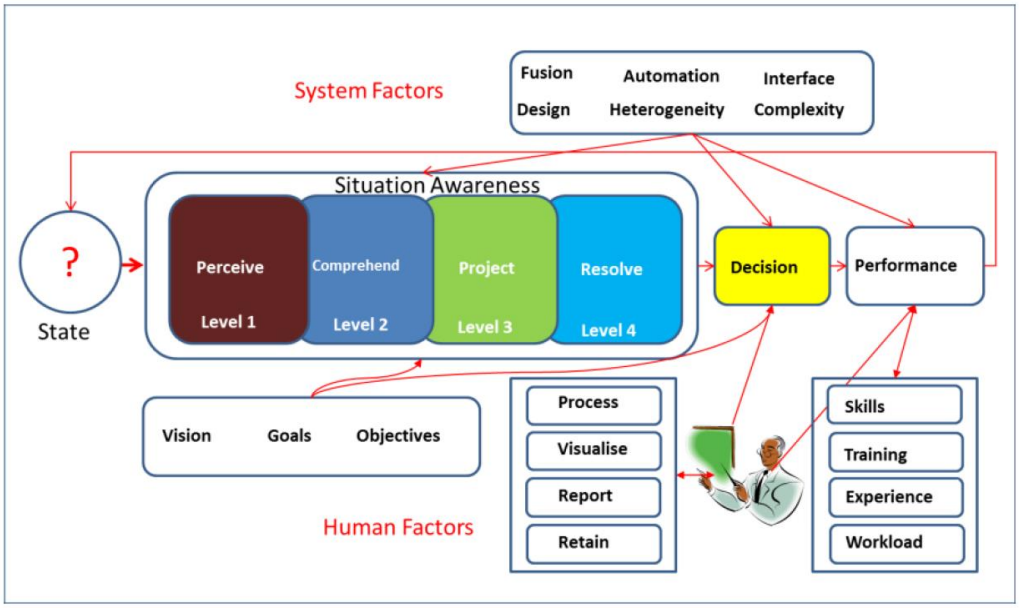
همان‌طور که در شکل(2) مشخص است فوی و مک گینس[14] از مدل آگاهی وضعیتی اندسلی استفاده نموده و مرحله پیشنهاد را به عنوان مؤلفه چهارم اضافه کرده‌اند. که بعدها توسط اونووبیکو[15] پالایش و ارائه شده است.

این اصطلاحات (مشاهده، درک، پیش بینی و پیشنهاد[2]) و ارتباط آن‌ها با فضای سایبر بررسی شده است. مشاهده با جمع آوری شواهد از وضعیت‌های سایبری سروکار دارد، درک مربوط به فهم دقیق وضعیت بوده که ممکن است از تجزیه و تحلیل مجموعه‌ای از شواهد جمع آوری شده یا از وضعیت فعلی فضای سایبر حاصل شود، همچنین شامل درک دقیق سطح تهدید است. شناسایی انواع حمله و خطرات مرتبط یا وابسته به یکدیگر از دیگر وظایف این مرحله می‌باشد. مرحله تجسم با اقدامات پیش بینی کننده به منظور پیش بینی حوادث، شرایط یا وضعیت‌های آینده با استفاده از اطلاعات وضعیت فعلی و درک چگونگی تشدید شرایط فعلی سروکار دارد. سرانجام، مرحله پیشنهاد با کنترل‌هایی برای ترمیم، بازیابی، اصلاح و پاسخ به وضعیت‌های سایبری شناخته می‌شود.

مرحله تصمیم گیری ورودی‌های چند بعدی را به منظور توصیه مجموعه‌ای از اقدامات انجام می‌دهند. برای این امر از فاکتورهای سیستم[3] استفاده می‌کنند و شواهد نتیجه تجزیه و تحلیل داده‌های اطلاعات تهدید را با در نظر گرفتن چشم انداز، اهداف و اهداف کسب و کار در نظر می‌گیرند. بعلاوه، مرحله تصمیم از گزارش‌های ارائه شده توسط کارشناسان یا متصدیان برای تصمیم گیری در مورد مناسب‌ترین اقدام جهت رسیدگی به وضعیت یا شرایط استفاده می‌کند. در مدل اندسلی تصمیمات به شدت تحت تاثیر آگاهی وضعیتی قرار می‌گیرند، زیرا آگاهی وضعیتی، داده ورودی غالب در تصمیم گیری است. تصمیمات از فاکتورهای متنوع، مانند فاکتورهای فردی(تجربه یا قابلیت‌ها) یا از فاکتورهای وظیفه و محیطی(حجم کاری، فشارها یا پیچیدگی‌ها) تاثیر

[1] dynamics
[2] Resolve
[3] System Factors

می‌گیرد. در این مدل می‌توان ارتباط بین آگاهی وضعیتی و عملکرد کنش‌ها را پیش‌بینی کرد[4]. آگاهی وضعیتی مناسب، احتمال عملکرد خوب و کنش‌های دقیق را افزایش می‌دهد، اما نمی‌تواند آن را تضمین کند.



شکل(2): مدل مرجع آگاهی وضعیتی[16]

همچنین بازخورد، وضعیت محیط یا سیستم تحت تاثیر تصمیمات و عملکرد کنش‌های انتخابی را پوشش می‌دهد.

در مدل آگاهی وضعیتی، زمان یک نقش مهم ایفا می‌کند. آگاهی وضعیتی یک ساختار دینامیک متاثر از محیط بیرونی و فاکتورهای متعدد است و در مدل، به عنوان ورودی عمل می‌کند. آگاهی وضعیتی سایبری موثر مستلزم این است که آگاهی وضعیتی سایبری ایجاد شده توسط سیستم، هوشمندی بهتری در خصوص وضعیت شبکه به تحلیلگرها ارائه کند[17].

در بررسی مدل‌های آگاهی وضعیتی پیشین موجود مشخص گردید، نقطه ضعف مشترک همه آنان در بهره‌گیری حداکثری از مفاهیم و چهارچوب دفاع سایبری فعال و تکنیک‌های آن (راهبرد اقدام فعال)، بوده است. در همه مدل‌های آگاهی وضعیتی قبلی پیشنهادات برای تصمیم گیری نهایی به متصدی امنیتی سپرده شده که این موضوع چابکی و برخط بودن اقدامات سیستم را با مشکل مواجه می‌نماید. دخالت عامل انسانی در اتخاذ همه تصمیمات با مخاطره بالا یا پایین موجب می‌گردد، آگاهی وضعیتی ایجاد شده نتواند در زمان مقرر به تهدیدات پاسخ دهد. در تمامی این مدل‌ها به موضوع سرعت و دقت در تصمیم گیری به طور جدی پرداخته نشده و به نظر تمامی این مدل‌ها برای چهارچوب دفاع‌های سایبری پیشین طراحی شده‌اند. نبود یک بخش مدیریت مخاطره به منظور اتخاذ برخی از اقدامات عملیاتی توسط خود سیستم آگاهی وضعیتی برای افزایش مؤلفه فعالانه و خودکار بودن، یکی دیگر از ضعف‌های این مدل‌ها می‌باشد. این موضوع لزوم ارائه یک مدل گسترده شامل تمامی زیرشاخه‌ها و بخش‌های عملکردی براساس چهارچوب دفاع سایبری فعال و در برگیرنده راهبرد و تکنیک‌های این نوع دفاع را به خوبی نشان می‌دهد.

2-4. کارهای مرتبط

با وجود بازه گسترده کاربرد آگاهی وضعیتی، اغلب مدل‌های دستیابی به **SA**[1] یک شباهت دارند: آن‌ها مبتنی بر تعریف کلی و رایج‌ترین مدل **SA** یعنی اندسلی[4] هستند. بنابراین، اجزای توصیف شده توسط اندسلی با ترکیب تمامی مدل‌های مناسب موجود، به عنوان پایه‌ای برای ایجاد یک فرآیند جدید برای دستیابی و اعمال **SA** عمل می‌کنند.

[1] Situational Awareness

تمامی مدل‌های موجود در فرآیند دستیابی به آگاهی وضعیتی سه مرحله (مشاهده، درک و پیش بینی) را پوشش می‌دهند. (به عنوان مثال مرحله مشاهده و درک در مدل اندسلی یا مرحله مشاهده و جهت‌گیری در حلقه اوودا[1]). البته مدل‌های اندسلی و اوودا[26] بر خلاف مدل‌های دیگر بر اساس مهارت‌های شناختی متصدی[2]های انسانی عمل می‌نمایند و سایر مدل‌ها از فرآیندهایی که توسط ماشین‌ها انجام شده بهره می‌گیرند. در خصوص فرآیندهای کاربردی **SA** که شامل (پیش‌بینی و پیشنهاد، اقدام و بازخورد) بوده مدل‌ها وضعیت متفاوتی از خود به نمایش می‌گذارند. مدل‌های اندسلی، اوودا، اوانکیچ[17] و پاهی[12] مرحله پیشنهاد را به صورت جامع‌تر توصیف می‌کنند و مدل‌های ادغام اطلاعات استینبرگ[25]، مدل مرجع تادا و سالیرنو[22] و همچنین مدل اوکولیکا[23] با فراهم نمودن اطلاعات بهتر و دقیق فرآیند پیشنهاد و تصمیم گیری را ارتقا می‌دهند. برای مثال مدل اوودا مراحل مورد نیاز برای پیشنهاد را به صورت مفصل توصیف می‌کند، در حالی که مدل اوانکیچ ویژگی‌های فنی مورد نیاز برای پیشنهاد با پیش‌بینی سناریوهای احتمالی را فراهم می‌نماید. به طور ایده آل، فرآیند دستیابی به **SA** شامل یک چرخه بازخورد بین محیط و تصمیم‌گیر است. برای مثال متصدی می‌تواند فرآیندهای دستیابی به **SA** و یا حتی نتایج آن‌ها را تایید یا اصلاح کند.

از جنبه متصدی، هدف از تحلیل، ارزیابی چگونگی رسیدن به **SA** توسط انسان‌ها یا ماشین‌ها (مانند برنامه‌ها) در مدل‌های **SA** است. مدل‌های اول، مانند اندسلی و حلقه اوودا، روی جنبه انسانی در شرایط بحرانی تمرکز می‌کنند. آن‌ها **SA** را به عنوان یک دانش شناختی توصیف نموده، که می‌توان با تجربه آن را غنی کرد. در این مدل‌ها، متصدی یک انسان، مانند یک خلبان یا یک سرباز است. حسگرهای فنی و داده‌های آن‌ها مشاهده انسانی را تکمیل می‌کنند. به عنوان نمونه رویکرد مدل ادغام داده نیاز به فرآیندهای اطلاعاتی انسانی و ماشینی در دستیابی به **SA** و کاربرد آن را بیان می‌کند. همه مدل‌های آگاهی وضعیتی بیان شده تلاش می‌کنند تا فرآیندهای دستیابی به **SA** شناختی را با ترکیب راه حل‌های فنی بهبود دهند. مدل‌های دیگر، مانند آگاهی وضعیتی سایبری موثر اوانکیچ و مدل مرجع آگاهی وضعیتی، رویکرد متفاوتی دارند. آن‌ها در فرآیندهای ایجاد **SA**، از متصدی انسانی در نقش تاییدکننده یا بهبود دهنده استفاده می‌کنند، در حالی که فرآیندهای دستیابی به **SA** کاملا خودکار است[12]. در این بین مدل دفاع فعال سادک[3][2] تمام ویژگی‌ها را دارا بوده و به صورت یک چرخه فعال مفاهیم فعالانه و خودکارسازی اقدامات را به صورت مفهومی نشان می‌دهد.

نقطه ضعف مشترک همه مدل‌های آگاهی وضعیتی در بهره‌گیری حداکثری از مفاهیم و چهارچوب دفاع سایبری فعال و تکنیک‌های آن، بوده است. در همه مدل‌های آگاهی وضعیتی مذکور پیشنهادات برای تصمیم گیری نهایی به متصدی امنیتی سپرده شده که این موضوع چابکی و برخط بودن اقدامات سیستم را با مشکل مواجه می‌نماید. دخالت عامل انسانی در اتخاذ همه تصمیمات با مخاطره بالا یا پایین موجب می‌گردد آگاهی وضعیتی ایجاد شده نتواند در زمان مقرر به تهدیدات پاسخ دهد. در تمامی این مدل‌ها به موضوع سرعت و دقت در تصمیم گیری به طور جدی پرداخته نشده و به نظر تمامی این مدل‌ها برای چهارچوب دفاع‌های سایبری پیشین طراحی شده‌اند. نبود یک بخش مدیریت مخاطره به منظور اتخاذ برخی از اقدامات عملیاتی توسط خود سیستم آگاهی وضعیتی برای افزایش مؤلفه فعالانه و خودکار بودن، یکی دیگر از ضعف‌های این مدل‌ها می‌باشد.

مدل مفهومی سادک تنها مدلی بوده که بر مبنای چهارچوب دفاع سایبری فعال طراحی شده و اقدامات فعالانه و خودکار در آن دیده شده است. تکمیل این مدل نیاز به طراحی یک مدل گسترده‌تر با مشخص نمودن همه زیرشاخه‌ها و بخش‌ها را داشته که مدل پیشنهادی تمامی این ابعاد را در بر می‌گیرد.

3. مدل پیشنهادی

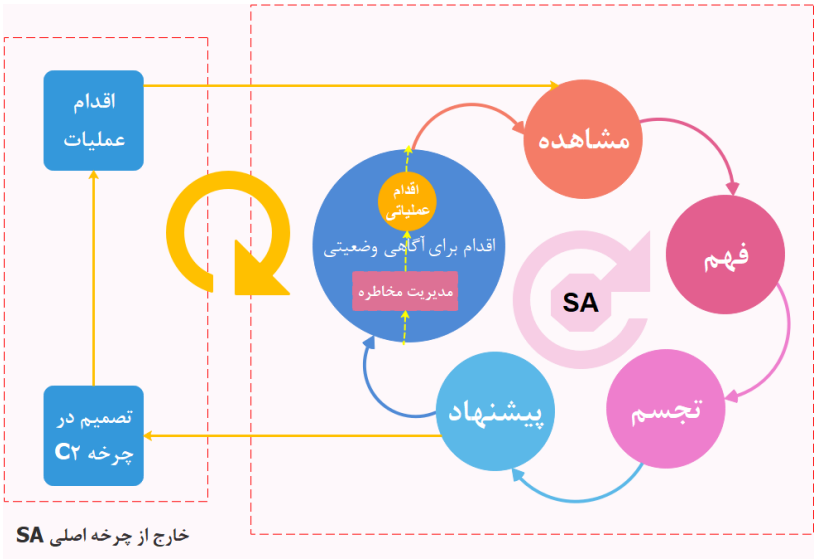
ساختار مدل پیشنهادی ما بر پایه مدل سادک بوده و از پنج مرحله اصلی مشاهده، فهم، تجسم و پیش بینی، پیشنهاد و تصمیم و اقدام تشکیل شده است. در تمامی این مراحل مفاهیم و تکنیک‌های **ACD** ظهور و بروز داشته و این بخش‌ها به صورت فعالانه و

[1] ooda

[2] operator

[3] Situational Awareness Decision Action (SADAC)

خودکار عمل می‌کنند. در مدل پیشنهادی زیرشاخه‌های هر بخش اصلی طراحی شده و اقدامات منحصر به فرد آگاهی وضعیتی با تکیه بر چهارچوب و تکنیک‌های دفاع سایبری فعال آورده شده است. همان‌طور که در مدل مفهومی برگرفته از مدل سادک شکل(3) مشخص می‌باشد، نکته مهم در مدل پیشنهادی با تکیه بر چهارچوب دفاع سایبری فعال تصمیم خودکار بر اساس بخش مدیریت مخاطره[1] سیستم، توسط هوش مصنوعی آموزش داده شده[2] می‌باشد. در عمل سناریوهای پیشنهادی با پیش بینی وضعیت سیستم در آینده توسط مغز سیستم بررسی شده و تصمیم لازم و مقتضی جهت اقدام برای آگاهی وضعیتی اتخاذ می‌گردد. به تبع آن بخش زیادی از اقدامات عملیاتی نیز می‌تواند به صورت خودکار و در داخل چرخه آگاهی وضعیتی صورت می‌پذیرد.



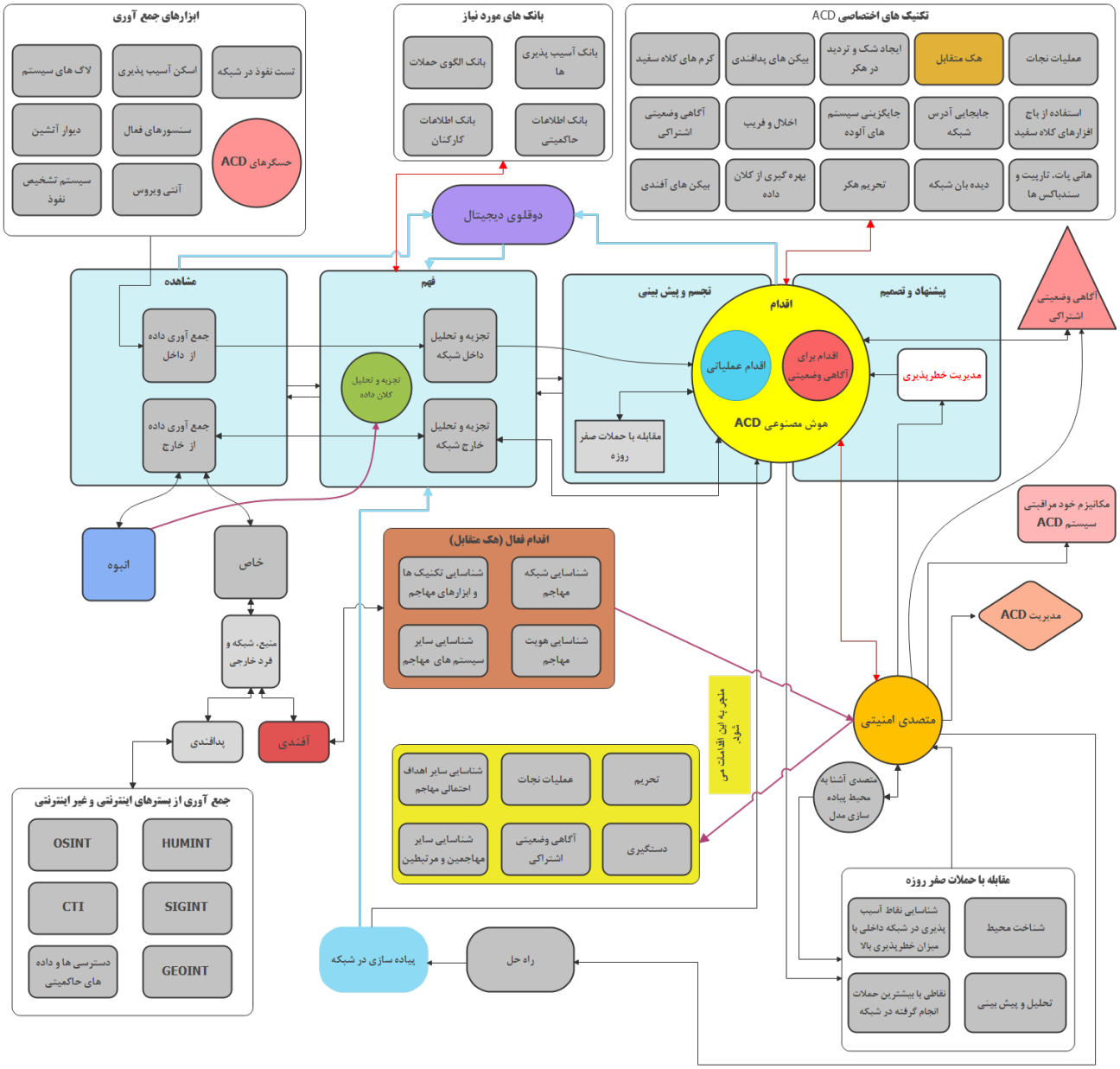
شکل(3): مدل مفهومی دفاع فعال برگرفته از مدل سادک[2]

در مدل پیشنهادی اقدامات برای آگاهی وضعیتی و اقدامات عملیاتی با خطر بالا (تعریف شده توسط متصدی امنیتی سیستم) برای تصمیم گیری به متصدی امنیتی ارسال می‌شود. از آنجا که پیش بینی، تصمیم و اجرا توسط خود سیستم انجام می‌گیرد، سرعت عمل و دقت اقدامات به حد زیادی افزایش می‌یابد. در این مدل بخش ویژه‌ای نیز به مقابله با حملات صفر روزه اختصاص داده شده است. با توجه به بررسی مدل‌های آگاهی وضعیتی و نقاط قوت و ضعف آن‌ها و نواقص مدل‌های قبلی در بهره‌گیری حداکثری از مفاهیم و چهارچوب دفاع سایبری فعال و تکنیک‌های آن، انتظار می‌رود مدل پیشنهادی ما این کمبود را جبران نموده و با بهره‌گیری از تمامی ظرفیت‌های دفاع سایبری فعال یک مدل مطلوب و ایده آل به منظور پیاده سازی در زیرساخت‌های متنوع باشد.

در مدل پیشنهادی شکل(4) سعی شده تمامی جوانب یک مدل آگاهی وضعیتی در دفاع سایبری فعال در نظر گرفته شده و مدل پیشنهادی بتواند در محیط‌ها و زیرساخت‌های حساس بیشترین بازدهی را داشته باشد. این مدل شامل پنج بخش اصلی مشاهده، فهم، تجسم و پیش‌بینی، پیشنهاد و تصمیم و مرحله اقدام می‌باشد. هوش مصنوعی **ACD** به عنوان مغز متفکر این مدل تصمیم‌های لازم را به صورت خودکار گرفته و فقط در صورت لزوم اتخاذ تصمیمات با خطر بالا، موارد برای تصمیم نهایی به متصدی امنیتی سیستم ارسال می‌گردد. بخش مدیریت مخاطره (خطرپذیری) سیستم در این مدل یک بخش اساسی بوده که متصدی امنیتی با سفارشی سازی این بخش با توجه به شرایط محیط و شبکه، حدّ، نوع و شدت تصمیمات خودکار توسط **ACD** را مشخص می‌نماید. در مدل پیشنهادی متصدی کم ترین درگیری را نسبت به سایر مدل‌های آگاهی وضعیتی دارد که این مورد باعث پویایی شده و در بهبود عملکرد این مدل در زیرساخت‌های حساس و مراکز حیاتی کشور نقش بسزایی دارد.

[1] Risk

[2] Trained artificial intelligence



شکل(4): مدل پیشنهادی گسترده آگاهی وضعیتی در دفاع سایبری فعال

3-1. مرحله مشاهده

مرحله مشاهده در این مدل جزء مهم ترین مراحل بوده و علاوه بر مشاهده لاگ‌های متفاوت و ورودی‌های حساس مانند هشدار از حسگرها و ابزارهای موجود در شبکه، مشاهده رفتار اجزای موجود در شبکه و احیانا رفتارهای مشکوک و مضر نیز بر عهده این بخش می‌باشد.

عملکرد خوب این بخش می‌تواند از حمله نفوذگر به سیستم قبل از هر گونه اقدام جلوگیری نماید.

در این مرحله دو نوع جمع آوری مدنظر بوده که شامل جمع‌آوری از داخل و جمع‌آوری از خارج می‌باشد. در بخش جمع‌آوری از داخل، ورودی‌های متعددی وجود داشته که می‌توان به لاگ‌های سیستم، پادآوند، سیستم تشخیص نفوذ، ضد ویروس، حسگرهای فعال، اسکن آسیب پذیری و تست نفوذ در شبکه و همچنین حسگرهای **ACD** (تکنیک‌های اختصاصی **ACD**) اشاره نمود. همچنین در بخش جمع آوری از خارج دو بخش انبوه و خاص وجود دارد. بخش انبوه مربوط به جمع آوری کلان داده‌ها از

اینترنت، وب تاریک و وب عمیق بر اساس مؤلفه‌های پیشنهادی متصدی امنیتی می‌باشد.

متصدی امنیتی با توجه به بودجه و زیرساخت مورد نیاز به منظور جمع آوری، نگهداری و تجزیه و تحلیل کلان داده براساس اهداف سازمانی و نیازسنجی انجام گرفته، تصمیم به استفاده از این امکان گرفته و یا با محدودسازی مؤلفه‌های جمع‌آوری به صورت خاص و کاملا سفارشی از این بخش استفاده می‌نماید.

هنگامی که مغز متفکر سیستم درخواست جمع آوری داده از یک منبع، شبکه یا فرد خاص خارج از شبکه را داشته و یا نیازمند تکمیل برخی از داده‌های داخل شبکه و بروزرسانی بانک‌های در اختیار (بانک الگوی حملات، بانک آسیب پذیری‌ها و...) باشد، از طریق بخش خاص موجود در مدل اقدام می‌گردد. در این بخش دو اقدام از نوع پدافندی و آفندی (تهاجمی) تعریف شده که اقدامات پدافندی بدون مخاطره با استفاده از تکنیک‌های جمع‌آوری اطلاعات آشکار از منابع اینترنتی و غیر اینترنتی شامل (اطلاعات انسانی[1]، اطلاعات سیگنالی[2]، اطلاعات جغرافیایی[3]) و همچنین منابع متصل به بانک‌های حاکمیتی به کار گرفته می‌شوند. اقدامات آفندی بر روی شبکه خانگی و خود مهاجم طراحی و اجرا شده که بر اساس تخمین مخاطرات احتمالی و سطح مدیریت مخاطره تعیین شده توسط متصدی امنیتی با تکنیک‌های منحصر به فرد **ACD** پیاده‌سازی می‌گردد.

با توجه به مخاطرات احتمالی این نوع جمع آوری اقدامات با متصدی امنیتی هماهنگ می‌شود. استفاده از تکنیک‌های **ACD** در جمع آوری اطلاعات و در ادامه اقدامات فعال مانند هک متقابل برای نفوذگران مشکلات زیر را ایجاد نموده که خود نوعی بازدارندگی برای محیط و سیستم ما ایجاد می‌کند[7].

- غیرقابل پیش بینی بودن
- تردید و بلاتکلیفی نفوذگر
- افزایش هزینه منابع مصرفی نفوذگر
- افزایش مخاطره برای نفوذگر

اقدامات دفاع فعال مانند حمله متقابل شامل شناسایی شبکه مهاجم، شناسایی تکنیک‌ها و ابزارهای مهاجم، شناسایی سایر سیستم‌ها و تجهیزات مهاجم و شناسایی هویت مهاجم می‌گردد. بخشی از این اطلاعات به منظور پیشگیری از حملات بعدی به **ACD** ارسال شده و بخشی دیگر جهت اقداماتی از قبیل شناسایی سایر اهداف احتمالی مهاجم، شناسایی سایر مهاجمین و مرتبطین، عملیات نجات، تحریم، دستگیری و اشتراک اطلاعات به متصدی امنیتی سیستم جهت تصمیم گیری پیشنهاد می‌گردد. به دلیل حساسیت بالای اقدامات این بخش اشتراک اطلاعات فقط با مجوز متصدی امنیتی صورت می‌گیرد.

2-3. مرحله فهم

این مرحله از سه بخش تجزیه و تحلیل داخل و خارج شبکه و یک بخش خاص تجزیه و تحلیل کلان داده تشکیل شده که در بخش تجزیه و تحلیل داده‌های داخل شبکه، باتوجه به شناخت سیستم از داده‌های ورودی از شبکه داخل و استاندارد بودن بخش قابل توجهی از این داده‌ها، تجزیه و تحلیل لازم صورت گرفته و به منظور پیش بینی، تصمیم و اقدام نهایی به **ACD** ارسال می‌شود. این تجزیه و تحلیل شامل استاندارد سازی داده‌ها و مقایسه داده‌های پیشین و جدید به منظور ایجاد فهم بهتری از وضعیت کنونی سیستم و بروزرسانی بانک‌های موجود به صورت برخط می‌باشد.

بخش تجزیه و تحلیل خارج شبکه داده‌های حاصل از جمع آوری از خارج به صورت خاص را که مستقیما توسط سیستم **ACD** درخواست می‌شود، بررسی و تحلیل نموده و برای پیش بینی و اتخاذ تصمیمات مناسب به **ACD** ارسال می‌نماید. در صورتی که داده جمع آوری شده به منظور بروزرسانی بخشی از بانک‌ها بوده باشد مستقیما به آن بخش ارسال می‌گردد.

در این مرحله دو بخش تجزیه و تحلیل داخل و خارج شبکه به دلیل عملکرد متفاوت از هم مجزا شده‌اند که برخی از دلایل این جدا سازی به شرح زیر می‌باشد.

- تجزیه و تحلیل از خارج بنا به درخواست **ACD** است.
- اولویت منابع سیستم با تجزیه و تحلیل از داخل شبکه می‌باشد که به دلیل اهمیت این بخش است.

[1] Human Intelligence (HUMINT)

[2] Signals intelligence (SIGINT)

[3] Geospatial intelligence (GEOINT)

- داده‌های جمع آوری شده از خارج تنوع بالایی داشته که موجب پیچیدگی بررسی و تحلیل بوده و منابع سیستم را بیشتر درگیر می‌نماید.
- عملکرد بخش تجزیه و تحلیل از خارج نباید بر روی تجزیه و تحلیل از داخل اثر منفی داشته باشد.

داده‌های ورودی از جمع آوری انبوه از خارج به بخش تجزیه و تحلیل کلان داده ارسال شده تا براساس مؤلفه‌های از پیش تعیین شده توسط متصدی امنیتی بررسی و تحلیل شده و در ادامه به **ACD** ارسال شود. این بخش نیز به دلیل مصرف منابع زیاد و اختصاصی بودن آن از سایر بخش‌ها جدا شده تا داده کاوی لازم بر روی این کلان داده در صورت نیاز سیستم و صلاحدید متصدی امنیت انجام گیرد.

3-3. مرحله تجسم و پیش بینی

این مرحله وظیفه دریافت داده‌های حاصل از تجزیه و تحلیل، پیش بینی حوادث، وضعیت‌ها و یا حالت‌های آتی سیستم را با استفاده از حالت کنونی آن و فهم اینکه چطور وضعیت کنونی ممکن است تشدید گردد، برعهده دارد. علاوه بر این به پیش بینی آینده نزدیک سیستم بر اساس وضعیت فعلی آن می‌پردازد. این مرحله تصویر کلی از وضعیت آینده سیستم را بر اساس داده‌های جدید و تجزیه و تحلیل شده به‌روز می‌نماید. پیش‌بینی حملات مهاجمین و شناسایی نقاط حساس و آسیب پذیر سیستم از دیگر وظایف آن می‌باشد.

3-4. مرحله پیشنهاد و تصمیم

این مرحله با دریافت داده‌های حاصل از تجسم و پیش بینی، وظیفه تهیه گزینه‌های مختلف برای پاسخگویی به وضعیت کنونی سیستم و ارائه به تصمیم گیرنده، بر اساس مدیریت مخاطره تعبیه شده را بر عهده دارد. این گزینه‌ها به منظور اصلاح، بازیابی و برطرف نمودن وضعیت‌های پیش آمده و یا پاسخ به رخدادهای آینده پیش‌بینی شده پیشنهاد گردیده و جهت اقدام به مرحله بعد ارسال می‌شود.

3-5. مرحله اقدام

در این مرحله هوش مصنوعی **ACD** به عنوان مغز متفکر این مدل وظیفه اقدام برای آگاهی وضعیتی با بهره‌گیری از گزینه‌های مختلف تهیه شده برای پاسخگویی به وضعیت کنونی سیستم در مرحله قبل، انتخاب گزینه و واکنش مناسب به حالت‌های سیستم را بر عهده دارد. همچنین اجرایی نمودن خودکار اقدامات عملیاتی پیش بینی شده بر اساس مدیریت مخاطره تعبیه شده در سیستم شکل(4) نیز از دیگر وظایف پیش بینی شده برای این مدل می‌باشد. باتوجه به موارد مطروحه در این مدل مرحله اقدام از دو زیر مرحله اقدام برای آگاهی وضعیتی و اقدام عملیاتی تشکیل شده است.

تکنیک‌های اختصاصی **ACD** که در مراحل مختلف این مدل به کار گرفته می‌شود، مکمل روش‌ها و تکنیک‌های دفاع‌های پیشین مانند **RCD** و **FCD** بوده و پیاده‌سازی این مدل به معنای حذف این روش‌ها و تکنیک‌ها نمی‌باشد. این امر به خودی خود یکی از ویژگی‌های منحصربه فرد **ACD** بوده که در سایر مدل‌های قبلی دیده نمی‌شود. استفاده از کرم‌های سفید، بیکن‌های پدافندی و آفندی، عملیات اخلال و فریب، بهره‌گیری از کلان داده، آگاهی وضعیتی اشتراکی بین اجزای **ACD** به منظور اتصال همه ابزارهای **ACD** به یکدیگر، اطلاع از فعالیت فعلی و ایجاد هماهنگی بین آن‌ها، جایگزینی سیستم‌های آلوده، دیده‌بان شبکه، عملیات نجات، استفاده از باج افزارهای کلاه سفید، تحریم نفوذگر و هک متقابل برخی از تکنیک‌های اختصاصی **ACD** می‌باشند. عملیات اخلال و فریب با ایجاد شک و تردید در نفوذگر با مخلوط نمودن داده‌های درست و غلط، استفاده از تله عسل، تارپیت و سندباکس-ها[1] (محیطی امن برای اجرای برنامه‌ها) و تکنیک بسیار موثر جابجایی آدرس شبکه انجام می‌گیرد. به نظر می‌رسد این تکنیک‌ها در صورت تلفیق و یکپارچه شدن می‌توانند به هم کمک کنند و به نوعی پشتیبان هم نیز باشند. برای مثال کارایی روزافزون فناوری‌های شناسایی، طول عمر مفید تله عسل را در مقابل نفوذگرانی حرفه‌ای کم می‌نماید.

اینجاست که جابجایی آدرس شبکه می‌تواند با تغییرات مداوم هویت تله عسل این مساله را جبران نماید. این می‌تواند اثر

[1] Sandbox

بازدارندگی را افزایش دهد و باعث کاهش هزینه‌هایی که به واسطه تولید و مدیریت تله عسل خیلی باکیفیت و پیچیده انجام می‌شود، گردد.

3-6. آگاهی وضعیتی اشتراکی

یکی از موارد راهبردی که نقش مهمی در دفاع سایبری فعال داشته و نبود آن در اکثر مدل‌های موجود مشاهده می‌گردد، آگاهی وضعیتی اشتراکی، یعنی به اشتراک گذاری اطلاعات تهدید با سایر سازمان‌های همکار و استفاده کننده این مدل می‌باشد. با توجه به اینکه آگاهی وضعیتی اشتراکی در مدل دفاع سایبری فعال ایالات متحده امریکا (شارکسیر) علاوه بر اتصال به مراکز حکومتی، نظامی و سازمان‌های همکار داخلی، به کشورهای دوست آن (اغلب کشورهای اروپایی) نیز متصل شده و این اشتراک اطلاعات تهدید بین آنان وجود دارد. با نگاه به افق بالاتر راه اندازی این مدل پیشنهادی و به تبع آن آگاهی وضعیتی اشتراکی در کشور ایران می‌تواند این اطلاعات را با کشورهای دوست به اشتراک بگذارد. بدین ترتیب با حمله به یکی از سازمان‌ها، کشورها و استفاده کنندگان از این مدل، اطلاعات حمله و تهدید به سایرین اطلاع رسانی شده و بانک‌های موجود شامل بانک الگوی حملات و بانک آسیب‌پذیری‌ها تکمیل می‌گردد. همچنین اقدامات بعدی از قبیل دستگیری و تحریم مهاجم یا مهاجمین و مرتبطین آنان می‌تواند به واقعیت نزدیکتر شود.

3-7. مدیریت دفاع سایبری فعال

در این قسمت تمامی اقدامات مورد نیاز برای بروزرسانی مغز **ACD** و ابزارهای آن مدیریت می‌شود. آموزش[1] هوش مصنوعی **ACD** و بروزرسانی ابزارها(برای مثال، اگر یک حسگر نیاز به بروزرسانی داشته باشد) و تکنیک‌های آن که توسط متصدی امنیت سایبری سیستم آماده سازی شده از طریق بخش مدیریت **ACD** پیاده سازی می‌شود. متصدی امنیتی سیستم از طریق این بخش با **ACD** ارتباط دارد.

همان‌طور که بسیاری از سیستم‌های امنیتی و ضد امنیتی دارای سیستم خود مراقبتی و دفاع از خود می‌باشند، این مدل نیز از این بخش مهم و کاربردی بهره گرفته است.

3-8. بانک‌های‌مورد نیاز سیستم

در این مدل به منظور شناسایی هر چه بهتر حملات و آسیب پذیری‌های سیستم، نیاز به تقاطع گیری داده‌های جمع آوری شده با بانک‌های پیش بینی شده می‌باشد. این بانک‌ها شامل بانک آسیب پذیری‌ها، بانک الگوی حملات، بانک‌های حاکمیتی و بانک اطلاعات کارکنان محیط پیاده سازی سیستم بوده که بروز رسانی بخش بزرگی از این بانک‌ها توسط خود سیستم انجام گرفته و بخشی نیز توسط متصدی امنیتی بروز رسانی می‌گردد. توضیح هرکدام از بانک‌ها به شرح زیر است:

بانک آسیب پذیری[2]: بانک آسیب پذیری بستری[3] است که با هدف جمع آوری، نگهداری و انتشار اطلاعات مربوط به آسیب پذیری‌های امنیتی رایانه کشف شده است. پایگاه داده معمولاً آسیب پذیری شناسایی شده را توصیف می‌کند. همچنین تأثیر احتمالی آن بر سیستم‌های آسیب دیده و هرگونه راه حل یا بروز رسانی را برای کاهش این مشکل ارزیابی می‌کند. **VDB** یک شناسه منحصر به فرد برای هر آسیب پذیری فهرست بندی شده مانند شماره (به عنوان مثال **123456**) یا نام الفبایی (برای نمونه **VDB-2020-12345**) اختصاص می‌دهد.

بانک الگوی حملات[4]: فراهم نمودن یک فرهنگ لغت[5] جامع از الگوی حملات شناخته شده که توسط دشمنان به منظور بهره کشی از نقاط ضعف شناخته شده در سیستم به کار گرفته می‌شود. با استفاده از بانک الگوی حملات می‌توان با شناسایی حملات شناخته شده حین وقوع، از به ثمر نشستن آن‌ها و ایجاد خسارت در سیستم جلوگیری نمود.

بانک‌های حاکمیتی: هر نوع بانک حاکمیتی که به آگاهی وضعیتی سیستم کمک نموده و به شناسایی نفوذگران منجر گردد. این

[1] Train
[2] Vulnerability Database (VDB)
[3] Platform
[4] Attack pattern
[5] Dictionary

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال ششم، شمارهٔ یک، بهار 1401

بانک‌ها می‌تواند شامل لاگ تمامی آی پی‌های کشوری، اطلاعات هویتی افراد، لیست نفوذگرانی فعال و غیره باشند.

بانک اطلاعات کارکنان: بانکی از اطلاعات هویتی، قابلیت‌ها و توانمندی‌های کارکنان و میزان دسترسی‌های آن‌ها به سیستم زیرساختی که مدل پیشنهادی آگاهی وضعیتی در آن راه‌اندازی می‌گردد. با توجه به اینکه حملات به سیستم می‌تواند از شبکه داخلی توسط هر یک از کارکنان انجام گیرد وجود بانک اطلاعاتی از این افراد می‌تواند به آگاهی وضعیتی و شناسایی مبدا حملات کمک نماید.

وجود این بانک‌ها در مجموع می‌تواند به یک آگاهی وضعیتی قدرتمند تبدیل شده و بسیاری از حملات قبل از ایجاد تاثیر منفی در سیستم شناسایی شود. این همان رویکرد دفاع فعال می‌باشد.

3-9. دوقلوهای دیجیتالی[1]

یک دوقلوی دیجیتال یک نمایش مجازی از سیستم بوده که به عنوان همتای دیجیتال در زمان واقعی یک شی یا روند فیزیکی عمل می‌کند[19]. همان‌طور که در مدل ارائه شده دیده می‌شود فناوری دوقلوهای دیجیتالی در تمامی مراحل این مدل می‌تواند ایفای نقش نماید. این فناوری تمامی حالت‌های شبکه داخلی و سیستم را به صورت برخط شبیه سازی نموده تا اقدامات کنترلی و خصوصا اسکن‌های عمیق در شبکه، تست نفوذهای پی در پی و هر اقدامی که عملکرد سیستم را با مشکل و کندی مواجه می‌کند در این بخش صورت گرفته و نتایج به بخش‌های مربوطه ارسال شود. این سیستم مجازی به **ACD** کمک می‌کند تا پیش بینی و به تبع آن تصمیم‌های خود را قبل از پیاده سازی در سیستم اصلی، در این همتای دیجیتال اجرا نموده و در صورت بازخورد مناسب عملیاتی نماید. همچنین این سیستم در راستای ارتقای امنیت مدل پیشنهادی و انجام عملیات اخلال و فریب نیز می‌تواند با **ACD** همراهی نموده و بسیار موثر باشد.

3-10. مقابله با حملات صفر روزه

یکی از ویژگی‌های مهم دفاع سایبری فعال و تکنیک‌های استفاده شده در آن موفقیت این نوع دفاع در دفع حملات ناشناخته یا همان صفر روزه می‌باشد[8]. اما این نوع حملات همواره خطاهایی را نیز برای سیستم به وجود می‌آورد. پیاده سازی این مدل در زیرساخت‌های حساس از قبیل زیرساخت برق کشور، انرژی اتمی و غیره، جای هیچگونه خطایی را برنمی‌تابد و لازم است تا این خطاها به صفر برسد. هر نوع خطا و حمله موفق به این زیرساخت‌ها می‌تواند منجر به فاجعه انسانی و به خطر افتادن امنیت ملی کشور گردد. بدین منظور در مدل پیشنهادی بخشی به نام مقابله با حملات صفر روزه پیش بینی شده که نحوه عملکرد آن به شرح زیر می‌باشد.

در زمان پیاده سازی این مدل بر روی یک زیرساخت حساس لازم است متصدی آشنا به محیط پیاده سازی مدل، نقاط آسیب پذیر در شبکه داخلی با میزان خطرپذیری بالا(برای مثال نقطه‌ای که در صورت حمله به آن و گرفتن دسترسی مهاجم می‌تواند بیشترین ضربه را به زیرساخت وارد نماید.)، را به سیستم اعلام نموده و شناخت کاملی از محیط به این بخش ارائه نماید. هوش مصنوعی **ACD** نیز با دریافت اطلاعات از بخش‌های دیگر، نقاطی با بیشترین حملات انجام گرفته در شبکه را ارزیابی نموده و به صورت سیستمی نقاط مهم و قابل دسترسی توسط مهاجم را پیش بینی نموده و آخرین وضعیت را به این بخش اعلام نماید. کلیه اطلاعات، مستندات، تحلیل و پیش‌بینی‌های انجام گرفته به متصدی امور امنیتی داده شده تا اقدامات موثر و مکانیزم‌های امنیتی لازم را در نقاط شناسایی شده پیاده سازی و بروزرسانی نماید. متصدی امنیتی سیستم با اجرایی نمودن راه‌حل‌های بدست آمده مکانیزم امنیتی جدید را به **ACD** معرفی نموده و داده‌های آن را نیز همواره جهت تجزیه و تحلیل به بخش درک ارسال می‌نماید. در بخش بعدی به ارزیابی مدل پیشنهادی بر اساس نظریه بازی‌ها می‌پردازیم.

4. نظریه بازی‌ها

جمعیتی از گره‌ها را در نظر بگیرید که می‌توانند رایانه‌ها را در یک سیستم سایبری نمایش دهند. در هر برهه از زمان، یک گره توسط مدافع B اشغال می‌شود (یعنی گره امن است)، یا توسط مهاجم R اشغال می‌شود (یعنی گره به خطر می‌افتد). با $i_B(t)$

[1] Digital Twins

نسبت گره‌هایی را که در زمان t توسط مدافع اشغال شده‌اند، و با $i_R(t)$ نسبت گره‌هایی را که در زمان t توسط مهاجم اشغال شده‌اند، نشان می‌دهیم. و این یعنی برای هر $t \geq 0$ داریم:

$$i_B(t) + i_R(t) = 1 \quad (1)$$

در تعامل بین حمله سایبری و دفاع سایبری فعال، مدافع و مهاجم می‌توانند گره‌ها را به شیوه مشابه "بگیرند". همچنین، می‌توان α_B را قدرت مدافع انتزاعی B در گرفتن گره‌های اشغال شده توسط مهاجم با استفاده از دفاع سایبری فعال و α_R را قدرت مهاجم انتزاعی R در به خطر انداختن گره‌های تحت اشغال مدافع با استفاده از حملات سایبری (مشابه بدافزار) در نظر گرفت. همچنین، فرض‌های همگن زیر را می‌توان درنظر گرفت:

- هر گره امن در "گرفتن" گره‌های اشغال شده توسط مهاجم قدرت یکسانی دارد.
- هر گره به خطر افتاده قدرت یکسانی در به خطر انداختن گره‌های اشغال شده توسط مدافع دارد.

پس می‌توان مدل دینامیک سیستم را چنین نوشت[20]:

$$\begin{cases} \frac{d}{dt}(i_B(t)) = \alpha_B i_B(t) i_R(t) - \alpha_R i_R(t) i_B(t) \\ \frac{d}{dt}(i_R(t)) = \alpha_R i_R(t) i_B(t) - \alpha_B i_B(t) i_R(t) \end{cases} \quad (2)$$

جایی که در آن برای همه $t \geq 0$ خواهیم داشت:

$i_B(t) + i_R(t) = 1$ ، $i_B(t) \geq 0$ و $i_R(t) \geq 0$. با توجه به تقارن معادلات، می‌توان نوشت:

$$\frac{d}{dt}(i_B(t)) = \alpha_B i_B(t)(1 - i_B(t)) - \alpha_R i_B(t)(1 - i_B(t)) \quad (3)$$

صورت ساده شده معادله بالا به شکل زیر است:

$$\frac{d}{dt}(i_B) = i_B(1 - i_B)(\alpha_B - \alpha_R) \quad (4)$$

حال اگر فرض کنیم مهاجم و مدافع هیچ یک، راهبردی نباشند (به عنوان مثال، هزینه انجام یک واکنش را در نظر نمی‌گیرند)، معادله دینامیک سیستم را می‌توان به شرح زیر مشخص کرد:

- اگر مهاجم قدرتمندتر از مدافع باشد $(\alpha_R \geq \alpha_B)$، مهاجم کل شبکه را به روش معادله لجستیک اشغال می‌کند (یعنی وقتی که i_R کوچک باشد، i_R به آرامی افزایش می‌یابد؛ وقتی i_R حدود یک حد آستانه باشد، i_R به طور تصاعدی افزایش می‌یابد؛ وقتی i_R بزرگ باشد، i_R به آرامی افزایش می‌یابد).
- اگر مدافع قدرتمندتر از مهاجم باشد $(\alpha_B \geq \alpha_R)$، مدافع نیز شبکه را به همان روال فوق اشغال می‌کند.
- اگر مهاجم و مدافع به یک اندازه قدرتمند باشند $(\alpha_R = \alpha_B)$، حالت سیستم در تعادل است. به عبارت دیگر برای همه $t \geq 0$ خواهیم داشت: $i_B(t) = i_B(0)$ و $i_R(t) = i_R(0) = 1 - i_B(t)$.

مدل فوق، مهاجمان غیر راهبردی و مدافعان غیر راهبردی را در خود جای می‌دهد و نقطه آغازین مطالعه ما در زمینه دفاع سایبری فعال است.

یک راهکار مناسب برای مواردی که قدرت مهاجم بیش از مدافع تشخیص داده شود، قطع شبکه و از دسترس خارج نمودن فضای سایبری برای مهاجم بوده که در مدل پیشنهادی به عنوان یکی از تکنیک‌های ACD آمده است. این امر بسته به زمان تشخیص قدرت مهاجم، می‌تواند کارا و یا غیرکارآمد باشد. برای مدلسازی بیان بالا به اصلاح معادله(4) به شکل بیانی از تصاحب گره‌های سیستم توسط مهاجم نیاز است. پس خواهیم داشت:

$$\frac{d}{dt}(i_R) = i_B(1 - i_B)(\alpha_R - \alpha_B) \quad (5)$$

پس با مقایسه رابطه بالا و رابطه(4) می‌توان نوشت:

$$\frac{d}{dt}(i_R) = -\frac{d}{dt}(i_B) \quad (6)$$

و در ادامه با تعریف رابطه زیر، به مدلسازی قطع شبکه و خارج از دسترسی نمودن فضای سایبری برای مهاجم می‌پردازیم:

$$if \ \frac{i_R}{\frac{d}{dt}(i_R)} \geq 0.1 \rightarrow \frac{d}{dt}(i_B) = 0 \quad (7)$$

که در آن داریم:

$$\frac{i_R}{\frac{d}{dt}(i_R)} = \frac{(1 - i_B)}{i_B(1 - i_B)(\alpha_R - \alpha_B)} = \frac{1}{i_B(\alpha_R - \alpha_B)} \quad (8)$$

پس شکل نهایی رابطه(7) برابر خواهد بود:

$$if \ \frac{1}{i_B(\alpha_R - \alpha_B)} \geq 0.1 \rightarrow \frac{d}{dt}(i_B) = 0 \quad (9)$$

همان‌طور که در معادله بالا مشخص است، یک حد (0.1) برای قطع شبکه دسترسی مهاجم درنظر گرفته شده است. این حد با توجه به میزان قدرت مهاجم ($\frac{d}{dt}(i_R)$) که بیانگر سرعت گسترش تسلط آن بر سیستم است، می‌تواند درصد بالا و یا پایینی از گره‌های مهم سیستم را اشغال کند (i_R). این امر به شدت وابسته به سرعت عمل سیستم در تشخیص میزان قدرت مهاجم خواهد بود؛ و اگر در زمان کوتاهی این امر تشخیص داده شود، حمله مهاجم بی اثر شده و سیستم به قابلیت دفاع مناسبی دست خواهد یافت. در مدل پیشنهادی با توجه به بهره‌گیری از راهبرد دفاع فعال و تکنیک‌های دفاع سایبری فعال نظیر هک متقابل و یا اقدامات اخلال و فریب (استفاده از تله عسل و تارپیت‌ها) و غیره، و همچنین خودکار بودن بخش قابل توجهی از اقدامات، زمان تشخیص قدرت مهاجم نسبت به سایر مدل‌های موجود بیشتر بوده که در ادامه توضیح بیشتری در این خصوص ارائه می‌گردد. تا این مرحله از کار، ضریب قدرت مدافع به شکل یک پارامتر ثابت فرض شده است؛ این درحالی است که تنها زمانی می‌توان چنین فرض کرد که مؤلفه قدرت مدافع در حین وقوع حمله تغییری نکند و صرفا به پیش بینی مدافع از شرایط حمله متکی باشد. اما در مدل پیشنهادی ما، قدرت مدافع با تصمیم‌هایی که در طول عملیات حمله خواهد گرفت متناسب است. علاوه بر این، مفهوم در حلقه بودن مدل پیشنهادی و سیستم آگاهی وضعیتی دفاع سایبری فعال بیانگر بازبینی و جمع‌آوری اطلاعات از مهاجم است؛ این امر به افزایش قدرت عمل و تصمیم گیری در مدافع منجر خواهد شد. به همین دلیل، مؤلفه قدرت مدافع را چنین تعریف می‌کنیم:

$$\alpha_B = ax + b \qquad (10)$$

که در آن، b بخش غیرفعال مؤلفه قدرت مدافع است. این بخش به شرایط سیستم و پیش‌بینی‌های انجام شده از حملات پیش رو وابسته است. متغیر x وضعیتی از مهاجم است که در طول حمله مشاهده می‌گردد. بدین معنی که با مشاهده رفتارهای مهاجم می‌توان راهبرد دفاع را اصلاح نموده و بهبود داد. و در نهایت، a مؤلفه‌ای بر حسب تمامی راهبردهایی است که در طول حمله می‌توان از آن‌ها بهره گرفت. به منظور پیاده‌سازی رابطه(10) در معادله کلی سیستم، متغیر x را می‌توان بر حسب سرعت تصرف گره‌ها توسط مهاجم مدلسازی کرد. پس داریم:

$$\alpha_B = a\frac{d}{dt}(i_R) + b \qquad (11)$$

حال با جایگذاری رابطه(11) در رابطه(4) داریم:

$$\frac{d}{dt}(i_B) = i_B(1-i_B)(a\frac{d}{dt}(i_R) + b - \alpha_R) \qquad (12)$$

و با اعمال (6) داریم:

$$\frac{d}{dt}(i_B) = i_B(1-i_B)(-a\frac{d}{dt}(i_B) + b - \alpha_R) \qquad (13)$$

پس خواهیم داشت:

$$\frac{d}{dt}(i_B) = \frac{i_B(1-i_B)(b-\alpha_R)}{1 + ai_B(1-i_B)} \qquad (14)$$

همان‌طور که در رابطه بالا مشخص است:

- هرچه مقدار پارامتر b بیشتر باشد، اثر قدرت مهاجم (α_R) کمتر خواهد شد. معنی ضمنی این بیان چنین است: هرچه آمادگی برای وقوع حمله بالاتر باشد، آسیب ناشی از حمله کمتر خواهد بود.
- هرچه پارامتر a بیشتر باشد، سرعت اشغال گره‌ها توسط مهاجم (در صورتی که قدرت مهاجم بیشتر باشد) کمتر می‌شود. معنی ضمنی این بیان چنین است: هرچه راهبردهای بکارگرفته شده حین وقوع حمله قوی‌تر باشد، تاب آوری در برابر حمله نیز بیشتر است.

روابط و معادلات دیفرانسیل بالا جهت مدلسازی ریاضی روشی که با نام آگاهی وضعیتی در دفاع سایبری فعال شناخته می‌شود. در این معادلات موارد زیر در نظر گرفته شده است:

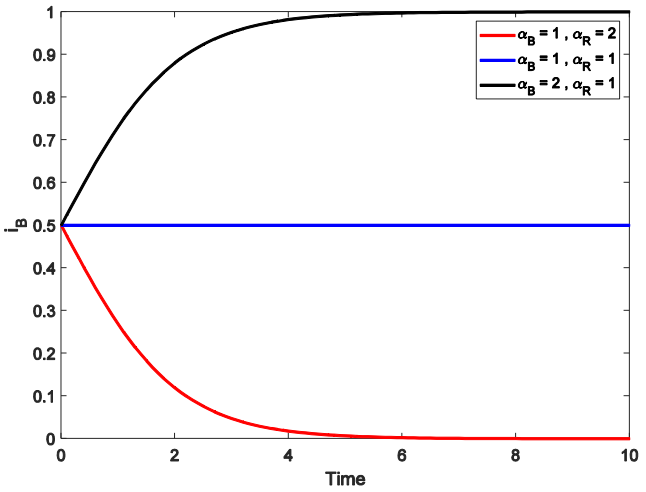
حلقه بسته بودن سیستم: در این سیستم همواره بازخورد رفتار سیستم مورد مطالعه قرار گرفته و تصمیمات دفاعی اصلاح می‌شود. این بخش در معادله(10) با تعریف متغیر x دیده شده است. در مدل پیشنهادی این مؤلفه موجب می‌گردد خروجی اقدامات انجام گرفته مورد ارزیابی دوباره سیستم قرار گرفته و دقت در تصمیم گیری خودکار سیستم بالا رود. به نوعی سیستم

به خودی خود با گرفتن بازخورد از عملکرد و نتیجه تصمیمات خود ارتقا پیدا می‌کند.

مدیریت مخاطره سیستم: در این سیستم، با توجه به نوع و قدرت حمله انجام شده و با وجود سیستم مدیریت مخاطره، به طور خودکار تصمیماتی اتخاذ و اقدام می‌گردد که هدف اصلی آن‌ها قطع دسترسی مهاجم به شبکه و در ادامه شناسایی تکنیک‌ها، ابزارها و هویت وی می‌باشد. این موضوع موجب افزایش سرعت تصمیم گیری و شناخت بهنگام قدرت مهاجم می‌گردد. باید توجه شود که این امر به معنای قطع کلی شبکه و عدم پاسخ دهی به کاربران نبوده و در موارد اضطرار تنها بخش مورد حمله واقع شده از دسترسی خارج خواهد شد. مدلسازی این بخش در رابطه(9) به خوبی قابل مشاهده است.

4-1. شبیه سازی و ارزیابی نهایی

نتیجه شبیه سازی مدل فوق در نرم افزار MATLAB به شرح زیر است: محور عمودی i_B نسبت گره‌های اشغال شده توسط مدافع می‌باشد.

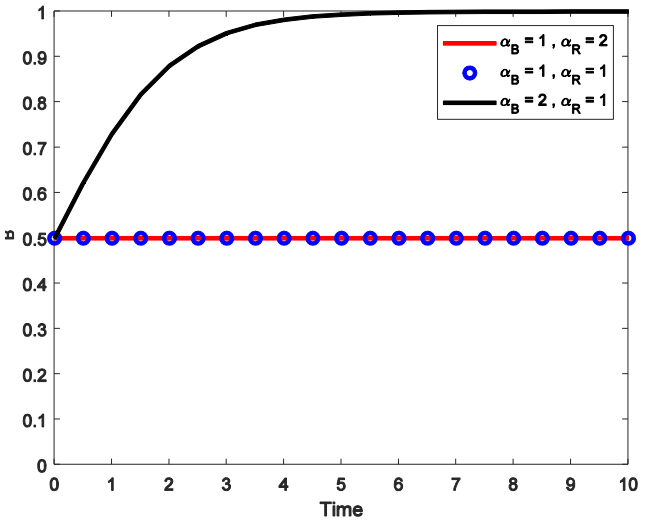


شکل(5): پاسخ مدل دینامیکی آگاهی وضعیتی دفاع سایبری فعال برای حالات مختلف قدرت مدافع و مهاجم

همان‌طور که مشخص است:

- اگر مهاجم قدرتمندتر از مدافع باشد $(\alpha_R \geq \alpha_B)$، مهاجم کل شبکه را به روش معادله لجستیک اشغال می‌کند (یعنی وقتی که i_R کوچک باشد، i_R به آرامی افزایش می‌یابد؛ وقتی i_R حدود یک حد آستانه باشد، i_R به طور تصاعدی افزایش می‌یابد؛ وقتی i_R بزرگ باشد، i_R به آرامی افزایش می‌یابد).
- اگر مدافع قدرتمندتر از مهاجم باشد $(\alpha_B \geq \alpha_R)$، مدافع نیز شبکه را به همان روال فوق اشغال می‌کند. اینجا اهمیت پارامتر b به خوبی مشخص شده است.
- اگر مهاجم و مدافع به یک اندازه قدرتمند باشند $(\alpha_R = \alpha_B)$، حالت سیستم در تعادل است. به عبارت دیگر برای همه $t \geq 0$ خواهیم داشت: $i_B(t) = i_B(0)$ و $i_R(t) = i_R(0) = 1 - i_B(t)$.

یک راهکار مناسب برای مواردی که قدرت مهاجم بیش از مدافع تشخیص داده شود، قطع شبکه و خارج از دسترس نمودن فضای سایبری برای مهاجم است. این امر بسته به زمان تشخیص قدرت مهاجم، می‌تواند کارا و یا غیرکارآمد باشد. طبق رابطه(9) که در قسمت پیشین بررسی شد خواهیم داشت:



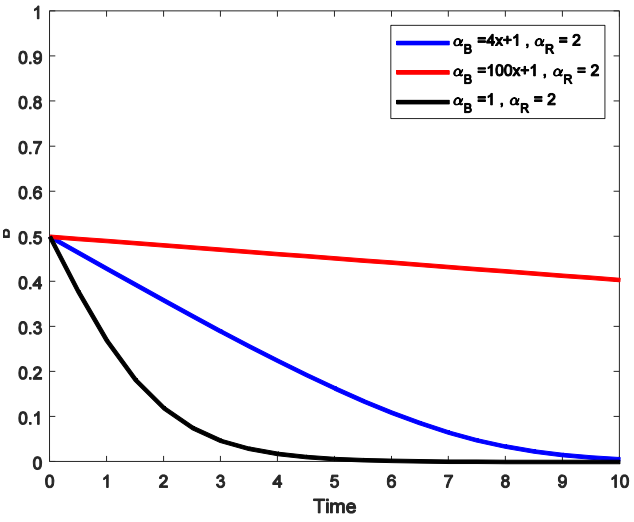
شکل(6): پاسخ مدل دینامیکی آگاهی وضعیتی دفاع سایبری فعال در صورت استفاده از تکنیک از دسترس خارج کردن شبکه

همان‌طور که مشخص است، در حالتی که قدرت مهاجم بیش از مدافع است، سیستم با تشخیص به موقع این امر به قطع شبکه دسترسی مهاجم مبادرت نموده و مانع از تصرف سیستم سایبری توسط آن شده است. این امر به خوبی نشان دهنده کارایی و صحت عملکرد این بخش از مدل خواهد بود.

در ادامه به شبیه سازی مدل دینامیکی آگاهی وضعیتی دفاع سایبری فعال در حالتی می‌پردازیم که سیستم به صورت حلقه بسته و با فیدبک از قدرت حمله کننده عمل نموده و پارامتر a به

فصلنامهٔ علمی - پژوهشی فرماندهی و کنترل، سال ششم ، شمارهٔ یک، بهار1401

عنوان راهبردهای اتخاذ شده حین حمله به آن اضافه شده است. نمودار پاسخ مدل دینامیکی آگاهی وضعیتی دفاع سایبری فعال در حالت پیاده‌سازی این نوع سیستم با در نظر گرفتن 3 مقدار متفاوت $(0, 4, 100)$ برای متغیر a چنین است:



شکل(7): پاسخ مدل دینامیکی آگاهی وضعیتی دفاع سایبری فعال در حالت پیاده سازی سیستم با اضافه شدن پارامتر a

همان‌طور که از شکل(7) مشخص است، در حالتی که قدرت مهاجم از مدافع در حالت استاتیک بیشتر باشد، هرچه راهبرد مدافع بهتر باشد (a بزرگتر باشد)، سرعت از دست دادن گره‌های سیستم پایین تر خواهد بود. این امر بیانگر اهمیت اخذ راهبرد مناسب جهت مواجهه با حمله است. این راهبرد در حملاتی از جنس ناشناخته اهمیت بالاتری پیدا خواهد کرد. با تمام این تفاسیر، نکته مهم این است که قدرت مدافع در این بخش، نهایتا به یک دفاع خوب با کاهش سرعت از دست دادن گره‌ها منجرخواهد شد. در حالی که قدرت تعریف شده تحت این پارامتر (a) بر بازیابی گره‌های از دست رفته اثری ندارد.

این امر اهمیت آمادگی حمله یعنی همان راهبردهای دفاعی پارامتر b را به خوبی نشان می‌دهد. بدین معنا که هرچقدر هم راهبردهای قویتری در سیستم وجود داشته باشد، در صورتی که آمادگی اولیه کافی وجود نداشته باشد، عمل دفاع ناقص خواهد بود. با این وجود، کاهش سرعت از دست دادن گره‌های سیستم به کمک مدافع می‌آید و فرصتی را فراهم می‌سازد تا بخش‌های مهم سیستم را قفل نموده و از دسترسی مهاجم دور نگاه دارد.

4-2. اقدام فعال

اثر اقدام فعال مانند (هک متقابل) را در دو بخش می‌توان بررسی نمود: 1- پارامتر بازدارندگی 2- پارامتر بازپس‌گیری

پارامتر بازدارندگی: اقدام فعال به دلیل ماهیت استاتیک خود بر قدرت مدافع در بخش b اثر گذار است؛ و آن را تقویت می‌کند. بدین معنا که بسیاری از مهاجمین را پیش از حمله از انجام چنین عملی بازخواهد داشت. همچنین در صورتی که مهاجم در مرحله شناسایی زیرساخت مدافع بوده باشد، راهبرد اقدام فعال (مانند هک متقابل) عملا با نفوذ به شبکه خانگی مهاجم ابتکار عمل را از وی گرفته و عملا مهاجم قبل از گرفتن حتی یک گره، تمام گره‌های خودش نیز اشغال می‌گردد که این موضوع اهمیت مؤلفه b را نشان می‌دهد.

پارامتر بازپس‌گیری: اقدام فعال بر کل قدرت مدافع اثرگذار بوده و تمامی رابطه(10) را متاثر خواهد کرد. بدین معنا که اقدام فعال خود یک راهبرد حین حمله نیز محسوب می‌شود و می‌تواند بر افزایش پارامتر a موثر باشد. باید توجه داشت که گره‌های سیستم در هنگام وقوع حمله با گره‌های سیستم در حالت عادی متفاوت است. به عنوان مثال، در هنگام حمله، رایانه حمله کننده نیز با رایانه‌های مورد حمله واقع شده در یک شبکه کار می‌کنند؛ و معادله(4) بیانگر تمامی گره‌های دخیل در شبکه بوده و تفاوتی بین گره‌های مهاجم و مدافع قائل نیست. در این حالت، با گرفتن رایانه حمله کننده توسط مدافع (هک متقابل) یکی از تکنیک‌های اقدام فعال در عمل تمامی شبکه توسط مدافع تصرف می‌شود. این امر بیانگر قدرت بالای این راهبرد در تحت تاثیر قراردادن پارامتر a و b به عنوان یک راهبرد دفاعی حین و قبل از حمله است. ذکر این نکته ضروریست که مؤلفه a یک حمله پیشین در مؤلفه b یک مؤلفه پسین نیز تاثیر گذار بوده و موجب بالا رفتن قدرت مدافع قبل از حمله می‌گردد. برای مثال هنگامی که حین حمله مهاجم یک هک متقابل صورت پذیرد در عمل موجب افزایش این مؤلفه شده و از تصاحب گره‌های بیشتر توسط مهاجم جلوگیری می‌نماید. با توجه به شناسایی مهاجم، ابزارها و تکنیک‌های آن در هک متقابل صورت گرفته، راهبردهای دفاعی قبل از حملات سایبری آتی کامل‌تر شده و مؤلفه b افزایش

می‌یابد. در عمل در حمله بعدی مهاجم بدون گرفتن یک گره شکست داده می‌شود.

4-3. مقایسه با سایر مدل‌ها

با توجه به اضافه شدن پارامترهای a و b به قدرت مدافع α_B و در ادامه بهبود این پارامترها توسط راهکارها و تکنیک‌های منحصر به فرد اتخاذ شده در مدل پیشنهادی، (قبل و حین حمله)، این مدل نسبت به سایر مدل‌های موجود از عملکرد دفاعی بهتری برخوردار بوده و دفاع را بهبود داده است.

برخی از مهم ترین شاخصه‌های مدل پیشنهادی نسبت به سایر مدل‌های موجود که با اضافه نمودن پارامترهای a و b و در ادامه بهبود آن‌ها، موجب برتری مدل پیشنهادی نسبت به سایر مدل‌ها شده‌اند به شرح زیر می‌باشند:

برخی از این راهبردها موجب افزایش مقدار پارامترهای a، b و یا به صورت همزمان در هر دو پارامتر شده و موجب افزایش قدرت مدافع می‌شوند.

- در مدل پیشنهادی مرحله اقدام شامل دو زیرشاخه اقدام برای آگاهی وضعیتی و اقدام عملیاتی طراحی شده است. بدین صورت بخشی از اقدامات (با توجه به بخش مدیریت مخاطره سیستم که توسط متصدی امنیتی سیستم پیاده سازی شده) به صورت خودکار انجام گرفته و نیازی به دخالت نیروی انسانی (متصدی امنیتی سیستم) نمی‌باشد. این مؤلفه موجب بالا رفتن سرعت تصمیم گیری در تصمیمات با مخاطره پایین می‌گردد.
- بخش راهبردی اقدام فعال مانند (هک متقابل) در این مدل موجب بازدارنگی شده و بخشی از مهاجمین را از حمله به زیرساخت مورد نظر منصرف می‌نماید. همچنین موجب می‌گردد، آگاهی وضعیتی نه فقط از داخل شبکه مدافع بلکه از شبکه مهاجم نیز حاصل شود، که این امر به خودی خود به جمع آوری داده‌های ارزشمند (شناخت بهتر از قدرت مهاجم)، آگاهی وضعیتی بهتر، دقت در تصمیم گیری و اتخاذ تصمیم درست کمک زیادی می‌نماید. همان‌طور که گفته شد با اتخاذ این راهبرد عملا با گرفتن رایانه حمله کننده توسط مدافع تمامی شبکه توسط مدافع تصرف می‌شود.
- مجزا نمودن بخش جمع آوری از داخل و خارج شبکه در مرحله مشاهده و همچنین مجزا نمودن بخش تجزیه و تحلیل داده از داخل و خارج و کلان داده در مرحله درک در بالابردن عملکرد و سرعت سیستم در پردازش داده‌ها و پویایی سیستم و به تبع آن افزایش سرعت سیستم موثر می‌باشد. علاوه بر این، امکان پیاده سازی مدل در مقیاس کوچک و بزرگ (با توجه به توان سخت‌افزاری زیرساخت) را فراهم می‌سازد.
- استفاده از بخش دوقلوی دیجیتال با انتقال برخی از اقدامات آگاهی وضعیتی به سیستم مجازی همسان موجب می‌گردد بار پردازشی بر روی زیرساخت پیاده شده کاهش یافته و در عملکرد سیستم اصلی اخلال وارد نشود. این موضوع به افزایش سرعت و دقت سیستم منجر می‌گردد.
- آگاهی وضعیتی اشتراکی یعنی اشتراک گذاری اطلاعات تهدید با سایر سازمان‌های همکار و استفاده‌کننده این مدل که موجب می‌گردد اطلاعات حمله و تهدید به سایرین اطلاع رسانی شده و بانک‌های موجود شامل بانک الگوی حملات و بانک آسیب‌پذیری‌ها تکمیل گردد. این امر به شناسایی مهاجم قبل از هرگونه اقدام کمک قابل توجهی نموده و سرعت تصمیم گیری را بالا می‌برد.
- بخش خود مراقبتی سیستم که موجب می‌گردد بخش‌های مختلف آگاهی وضعیتی تحت تاثیر عوامل بیرونی قرار نگرفته و به نوعی دستکاری نشوند. این موضوع منجر به حفاظت از مؤلفه دقت در تصمیمات می‌شود
- بخش راهبردی مقابله با حملات صفر روزه به منظور مقابله با حملات ناشناخته به طوری که اگر تمهیدات مدل پیشنهادی به منظور دفع این نوع حملات ناموفق بوده و یا تاخیر داشته باشد بتوان با این روش از وقوع این نوع حملات و یا تاثیرگذاری جدی آن‌ها خصوصا در زیرساخت‌های حیاتی جلوگیری نمود.

مجموعه همه موارد فوق الذکر و برخی دیگر از تکنیک‌های استفاده شده ACD در مدل پیشنهادی موجب بالا بردن دو مؤلفه سرعت و دقت در سیستم و به تبع آن بهبود دفاع می‌شود. همان‌طور که در شکل(7) مشخص است برای مدل پیشنهادی با

مقدار فرضی a=100 بر اساس شاخصه‌های برتری گفته شده، نسبت به مقادیر فرضی پایین تر a در سایر مدل‌های قبلی موجود a=0 و a=4، عملکرد بهتری در مقابله با مهاجم صورت گرفته که این امر به سبب به کارگیری راهبردهای خاص مدل پیشنهادی نسبت به سایر مدل‌های قبلی موجود بوده است.

5. نتیجه‌گیری

در سال‌های اخیر دفاع سایبری فعال و مهم ترین بخش آن یعنی آگاهی وضعیتی سایبری به عنوان یک راهبرد جدید دفاعی در حوزه سایبر، بین متخصصان و دانشمندان جهانی مورد بحث و بررسی قرار گرفته است و با توجه به اثربخشی و بازدارندگی این نوع دفاع، کشورهای بزرگ دنیا راهبردهای دفاعی خود را بر مبنای آن تبیین می‌کنند. هر کشور بر اساس زیرساخت‌های داخلی و ساختار خود، تعریف و رویکردی متفاوت از دفاع سایبری فعال و بخش‌های مهم آن دارد. در این بین، کشور ایران به منظور مواجه با تهدیدات و حملات پیچیده روزافزون (خصوصا از نوع حملات صفر روزه) باید به این سمت حرکت نموده و راهبردهای دفاعی خود را به روز نماید.

در این مقاله یک مدل گسترده آگاهی وضعیتی سایبری بر مبنای تکنیک‌ها و رویکردهای دفاع سایبری فعال ارائه شده است که در آن به جنبه‌های مختلف این مسئله شامل، ایجاد یک توانایی هماهنگ، خودکار و برخط به منظور کشف، شناسایی و مقابله با تهدیدات قبل از وقوع خسارت با استفاده از یک آگاهی وضعیتی قدرتمند و اشتراک گذاری اطلاعات تهدید، استفاده از تمامی ظرفیت‌های دفاع‌های پیشین در کنار تکنیک‌های منحصربه فرد دفاع سایبری فعال شامل توانایی و ابتکار در انجام اقدامات پیش کنشگرانه یا تهاجمی با تکیه بر اصل مدیریت خطرپذیری سیستم و محیط، پرداخته شده است. مدل پیشنهادی با بهره‌گیری از برخی راهبردها مانند اقدام فعال(هک متقابل)، آگاهی وضعیتی اشتراکی، مقابله با حملات صفرروزه موجب ایجاد بازدارندگی و اثربخشی مطلوب در مقابل تهدیدات سایبری می‌شود. استفاده از بخش دوقلوی دیجیتال، تفکیک مرحله اقدام به دو زیرشاخه اقدام برای آگاهی وضعیتی و اقدام عملیاتی، بهره گیری از هوش مصنوعی ACD جهت اتخاذ تصمیمات بلادرنگ و خودکار (با توجه به بخش مدیریت مخاطره سیستم) از جمله مهم ترین ویژگی‌های مدل پیشنهادی در بالا بردن سرعت و دقت عملکرد دفاعی می‌باشد.

نتایج شبیه‌سازی و ارزیابی مدل پیشنهادی بر اساس نظریه بازی‌ها نیز مشخص می‌نماید ما با ارائه یک تعریف جدید از مولفه قدرت مدافع و بالا بردن ضرایب آن براساس ویژگی‌های مدل گسترده پیشنهادی، دفاع را بهبود داده و موفق عمل نموده‌ایم.

ارایه یک مدل ریاضی جامع که در برگیرنده تمامی جوانب و بخش‌های عملکردی مدل آگاهی وضعیتی در دفاع سایبری فعال باشد، به همراه یک بستر نرم‌افزاری برای شبیه سازی و همچنین پیاده‌سازی و ارزیابی این مدل در یک محیط عملیاتی، می‌توانند **به** عنوان پیشنهاداتی برای کارهای آینده مورد بررسی قرار گیرند.

6. مراجع

[1] تبار احمدی، داداش و بابویی، محمود، (1400). ارائه مدلی برای دفاع سایبری فعال به منظور کاربرد در فناوری فریب سایبری. پدافند الکترونیکی و سایبری، 9(4)، 140-125.

[2] رشیدی، علی جبار، (1399). آگاهی وضعیتی سایبری. گزارش فنی، دانشگاه صنعتی مالک اشتر.

[3] R. S. Dewar, "The “triptych of cyber security”: A classifi cation of active cyber defence," in *2014 6th International Conference On Cyber Conflict (CyCon 2014)*, pp. 7-21: IEEE, 2014.

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

[5] D. C. Blair, M. Chertoff, F. J. Cilluffo, and N. O'Connor, "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," *Project Report, The George Washington University*, 2016.

[6] M. J. Herring and K. D. Willett, "Active cyber defense: a vision for real-time cyber defense," *Journal of Information Warfare*, vol. 13, no. 2, pp. 46-55, 2014.

[7] K. A. Repik, "Defeating adversary network intelligence efforts with active cyber defense techniques," 2008.

[8] Mandt, Erick J. "On integrating cyber intelligence analysis and active cyber defense operations." PhD diss., Utica College, 2015.

[9]Active Cyber Defense System. Available: https://www.iad.gov/iad/programs/iad-initiatives/active-cyber-defense.cfm. 2017.

[10] Levy, Ian, S. Maddy, and Mission Analytics. "Active Cyber Defence-The Second Year." 2019.

[11] C. Onwubiko and T. J. Owens, "Situational Awareness in Computer Network Defense: Principles, Methods and," 2011.

[12] T. Pahi, M. Leitner, and F. Skopik, "Analysis and assessment of situational awareness models for national cyber security centers," in *International Conference on Information Systems Security and Privacy*, vol. 2, pp. 334-345: SCITEPRESS, 2017.

[13] RASHİDİ, Ali, Kourosh AHMADİ, and Mostafa HEİDARPOUR. "Cyber Situational Awareness using Intelligent Information Fusion Engine (IIFE)." Fen Bilimleri Dergisi (CFD) 36, no. 3 2015.

[14] B. McGuinness and L. Foy, "A subjective measure of SA: the Crew Awareness Rating Scale (CARS)," in *Proceedings of the first human performance, situation awareness, and automation conference, Savannah, Georgia*, vol. 16, pp. 286-291, 2000.

[15] C. Onwubiko, *Situational Awareness in Computer Network Defense: Principles, Methods and Applications: Principles, Methods and Applications*. IGI Global, 2012.

[16] C. Onwubiko, "Understanding Cyber Situation Awareness," *Int. J. Cyber Situational Aware.*, vol. 1, no. 1, pp. 11-30, 2016.

[17] N. Evancich, Z. Lu, J. Li, Y. Cheng, J. Tuttle, and P. Xie, "Network-wide awareness," in *Cyber Defense and Situational Awareness*: Springer, pp. 63-91, 2014.

[18] U. Franke and J. Brynielsson, "Cyber situational awareness–a systematic review of the literature," *Computers & security*, vol. 46, pp. 18-31, 2014.

[19] Eckhart, Matthias, Andreas Ekelhart, and Edgar Weippl. "Enhancing cyber situational awareness for cyber-physical systems through digital twins." In 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1222-1225. IEEE, 2019.

[20] Lu, Wenlian, Shouhuai Xu, and Xinlei Yi. "Optimizing active cyber defense." In *International Conference on Decision and Game Theory for Security*, pp. 206-225. Springer, Cham, 2013.

[21] Heckman, Kristin E., Frank J. Stech, Roshan K. Thomas, Ben Schmoker, and Alexander W. Tsow. "Cyber denial, deception and counter deception." Advances in Information Security 64 2015.

[22] Tadda, George P., and John S. Salerno. "Overview of cyber situation awareness." In Cyber situational awareness, pp. 15-35. Springer, Boston, MA, 2010.

[23] Okolica, James, J. Todd McDonald, Gilbert L. Peterson, Robert F. Mills, and Michael W. Haas. "Developing systems for cyber situational awareness." In 2nd Cyberspace Research Workshop, vol. 46. 2009.

[24] Broeders, Dennis. "Private active cyber defense and (international) cyber security—pushing the line?." Journal of Cybersecurity 7, no. 1 2021.

[25] A. Steinberg, C. Bowman, and F. White, "Revisions to the JDL Model: Joint NATO," in IRIS Conference Proceedings, Quebec, October, 1998.

[26] B. Brehmer, "The dynamic OODA loop: A new basis for designing C2 support," in Proceedings of the Second International Conference on Military Technology, Stockholm Obtober, 2005, vol. 25, p. 2005.