فصلنامه علمی-ترویجی پدافند غیرعامل
سال هشتم، شماره ٤، زمستان ١٣٩٦، (پیاپی ٣٢): صص ٩٣-٧٩

راه‌حلی برای کاهش بار ترافیکی حملات سایبری در سامانه‌های امنیتی و دفاعی با استفاده از توزیع‌شدگی تعاملی

مصطفی عباسی*[1]، سامان کشوری [2]، محمدرضا حسنی آهنگر [3]

تاریخ دریافت: ۱۳۹۶/۰۱/۲۸، تاریخ پذیرش: ۱۳۹۶/۰۴/۱۹

چکیده

با گسترش روزافزون فضای مجازی و ضریب نفوذ آن در سازمان‌ها، حملات سایبری به‌خصوص حملات منع خدمت به‌وسیله بدافزارها و نفوذگران افزایش یافته است. با توجه به محدودیت‌هایی که نمی‌توان شرایط یک حمله سایبری را به‌صورت واقعی در سازمان‌ها ایجاد کرد، استفاده از شبیه‌سازی، علاوه‌بر ارائه وضعیت سامانه‌ها در زمان حمله، امکان ایجاد تنوع در نوع و اندازه حملات و بررسی میزان کاهش بار ترافیکی را نیز فراهم می‌آورد؛ با توجه به ویژگی‌ها و قابلیت‌های مدل‌سازی و شبیه‌سازی مبتنی بر عامل، در این مقاله مدل مفهومی و زیرساخت لازم جهت بررسی سناریوهای مختلف حمله و دفاع سایبری توزیع‌شده تعاملی و غیرتعاملی و ارزیابی کارایی آن‌ها، بررسی، طراحی و پیاده‌سازی شده است. نتایج حاصل از تحقیق و شبیه‌سازی نشان می‌دهد که دفاع توزیع‌شده تعاملی نسبت به حالت غیرتعاملی کارایی بهتری داشته و میزان بار ترافیک در زمان حمله را براساس معیارهای ارزیابی، به‌طور میانگین ۱۵ ٪ کاهش می‌دهد. این کاهش بار به دلیل تعامل عوامل دفاعی با یکدیگر و به‌روزرسانی دانش آن‌ها در زمان حمله بوده است که افزایش توان سامانه‌های پدافندی و دفاعی سایبری هنگام وقوع حمله را در پی دارد. لذا پیشنهاد می‌گردد که سامانه‌های امنیتی و دفاعی سایبری به‌صورت توزیع‌شده تعاملی در سطح شبکه به‌کارگیری شود.

کلیدواژه‌ها: شبیه‌سازی، مبتنی بر عامل، حمله سایبری ترکیبی، منع خدمت، امنیت سایبری، دفاع توزیع‌شده.

۱- دانشجوی دکتری، دانشگاه جامع امام حسین(ع)، (moabbasi@ihu.ac.ir) نویسنده مسئول
۲- دانشجوی کارشناسی ارشد، گروه کامپیوتر، دانشگاه جامع امام حسین(ع)
۳- دانشیار، گروه کامپیوتر، دانشگاه جامع امام حسین(ع)

۱- مقدمه

با توجه به افزایش حملات سایبری به‌خصوص حملات منع خدمت، نیاز به بررسی راه‌حل‌ها و روش‌هایی جهت حذف یا کاهش بار ترافیکی واردشده به زیرساخت‌های سایبری است. یکی از روش‌های آزمون و ارزیابی سامانه‌ها در شرایط مختلف و راه‌حل‌های ارائه‌شده، مدل‌سازی و شبیه‌سازی هست. شبیه‌سازی مدلی از عملیات یک دستگاه، فرایند یا سامانه واقعی در طول زمان است. با شبیه‌سازی می‌توان یک تاریخچه مصنوعی از رفتار سامانه بدون اخلال در عملکرد سامانه واقعی تولید نمود. شبیه‌سازی و مدل‌سازی مبتنی بر عامل[1] روشی است که در سامانه‌های پیچیده با مؤلفه‌ها و عامل‌های مختلف، کاربرد دارد و یک جهش در حوزه شبیه‌سازی محسوب می‌شود [۲-۱]. حملات سایبری به‌خصوص حملات منع خدمت[2]، مشکلات متعددی برای سازمان‌ها در پی دارد؛ اطمینان از نحوه عملکرد سامانه‌های مختلف کامپیوتری، بدون ایجاد وقفه در عملکرد آن‌ها، از طریق شبیه‌سازی امکان‌پذیر است [۳]. هدف اصلی حملات منع خدمت توزیعی از بین‌بردن قابلیت دسترس‌پذیری برنامه‌ها، شبکه و خدمات اینترنتی برای کاربران است. در این نوع حمله، حجم زیادی پیام و داده به ماشین یا سایت مقصد با هدف ایجاد تداخل در عملیات آن ارسال می‌شود که نتیجه آن معلق‌کردن ماشین یا سایت مقصد به دلیل استفاده بیش‌ازحد از منابع آن مانند پردازنده، حافظه و پهنای باند است [۳]. حمله اسمارف[3] یکی از انواع حملات منع خدمت سیل‌آسا روی شبکه است [۴]. این نوع حمله به پیکربندی نامناسب تجهیزات شبکه متکی است که در آن امکان ارسال بسته به همه کامپیوترهای میزبان روی یک شبکه خاص با آدرس‌های همه پخشی وجود دارد. در چنین حمله‌ای، مهاجمان با یک شناسه جعلی یک تقاضای پینگ[4] به یک یا چندین سرور همه پخشی ارسال کرده و آدرس شناسه ماشین هدف (قربانی) را به‌عنوان گیرنده پیغام تنظیم می‌کنند. سرور همه‌پخشی این تقاضا را برای تمام زیربخش‌های شبکه ارسال نموده و ماشین‌های شبکه پاسخ بسته را به سرور همه‌پخشی می‌فرستند. سرور همه‌پخشی پاسخ‌های دریافتی را به ماشین هدف هدایت یا ارسال می‌کند؛ بدین‌صورت زمانی‌که ماشین حمله‌کننده تقاضایی را به چندین سرور روی شبکه‌های متفاوت همه‌پخشی می‌نماید؛ پاسخ‌های تمامی کامپیوترهای شبکه‌های مختلف به ماشین هدف ارسال‌شده و آن را از کار می‌اندازند؛ بنابراین پهنای باند شبکه به‌سرعت اشغال‌شده و از انتقال بسته‌های مجاز به مقصدشان جلوگیری به عمل خواهد آمد [۴].

سامانه‌های امنیتی، دفاعی و کاربری یک شبکه کامپیوتری را می‌توان در قالب عامل‌های مختلفی نظیر مهاجم، مدافع و بی‌طرف در نظر گرفت تا هرکدام بخشی از عامل‌های مدل‌سازی و شبیه‌سازی مبتنی بر عامل تحقیق را پوشش دهند [۵]. عامل را می‌توان موجودیتی خودمختار[5] تعریف کرد که دارای حافظه بوده و می‌تواند با درک از محیط اطراف خود، تجربه و دانش خود را افزایش دهد تا متناسب با شرایط محیطی تصمیم‌گیری نموده و در برابر درخواست‌های سایر عامل‌ها، از خود رفتار نشان دهد [۶].

در این تحقیق، سامانه‌های تشخیص و جلوگیری از نفوذ[6] در لبه ورودی و درون شبکه، آنتی‌ویروس‌های نصب‌شده در رایانه‌ها و قابلیت‌های دفاعی تعبیه‌شده تجهیزات به‌عنوان عوامل دفاعی در نظر گرفته شده است. رایانه‌های داخلی اجیرشده[7]، شبکه‌ها و رایانه‌های اجیرشده خارج از شبکه به‌عنوان عوامل هجومی، کاربران، رایانه‌های قانونی بیرونی و داخلی نیز به‌عنوان عوامل بی‌طرف در نظر گرفته شده‌اند؛ بنابراین برای سازمان‌های مختلف مهم است که با شبیه‌سازی زیرساخت ارتباطی، عوامل دفاعی و پدافندی موجود خود، شناخت کافی از آسیب‌پذیری در برابر حملات سایبری و میزان بار ترافیک اعمال‌شده به آن‌ها را داشته باشند. با انجام این کار نقاط آسیب‌پذیر براساس استانداردها شناسایی‌شده و می‌توان ضمن ترمیم آن‌ها، میزان بار ترافیک حمله را تا حد مشخصی کاهش داد. بنابراین در این مقاله، در بخش ۲ ابتدا پیش‌زمینه تحقیق شامل تشریح روش شبیه‌سازی و مدل‌سازی مبتنی بر عامل، حمله سایبری ترکیبی منع خدمت و ویژگی‌های آن عنوان گردیده و در بخش ۳ روش و پارامترها و نحوه مدل‌سازی مبتنی بر عامل حمله و دفاع سایبری توزیع‌شده متناسب با سناریوها، تشریح شده است. نتایج مدل‌سازی و شبیه‌سازی و ارزیابی آن در بخش ۴ ارائه‌شده و در پایان نتیجه‌گیری تحقیق عنوان می‌شود.

۲- پیش‌زمینه تحقیق

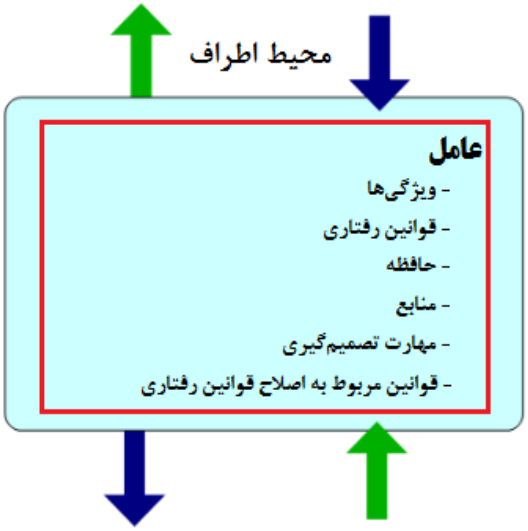
در این مقاله برای کاهش بار ترافیکی حملات سایبری در سامانه‌های امنیتی و دفاعی، حمله منع خدمت توزیع‌شده از داخل و بیرون به شبکه، با استفاده از توزیع‌شدگی تعاملی شبیه‌سازی شده است.

1 -Agent Based Modeling and Simulation
2 -Denial of Service attack
3 -Smurf
4 -ping
5 -Autonomy
6 -Intrusion prevention system
7 -Zombie

بسته‌های تولیدشده در شبکه با توزیع‌های مختلفی به اجزای شبکه رسیده و پردازش می‌شوند. سامانه دفاعی این شبکه نیز به‌صورت توزیع‌شده عمل می‌کند. در ادامه این مفاهیم شرح داده می‌شود.

۲-۱- شبیه‌سازی و مدل‌سازی مبتنی بر عامل

عامل‌ها قابلیت هم‌گروه‌شدن جهت اجرای مناسب و موفقیت‌آمیز کارها را دارند. مطابق شکل (۱) یک عامل علاوه بر خودمختاری، دارای حافظه، رفتار و منابع نیز است:



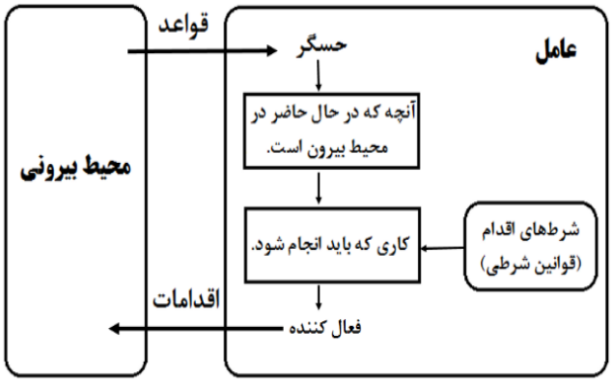
شکل (۱): یک عامل و ویژگی‌های آن [۲]

برخی از ویژگی‌ها و قابلیت‌های کلیدی یک عامل به شرح زیر است:

- رفتار[1]: عامل براساس شرایط محیطی می‌تواند رفتارهای خود را تغییر داده و رفتارهای متفاوتی نشان دهد.
- ادراک[2]: عامل می‌تواند مطابق با اطلاعات استخراج‌شده از محیط و پیش‌بینی آینده، داده‌ها و اطلاعات خود را تغییر دهد.
- همکاری[3]: با توجه به ویژگی‌های یک عامل، به‌خصوص خودمختاری آن، دانش و اطلاعات خود را با سایر عامل‌های هم‌پیمان[4] به اشتراک گذاشته و در موفقیت گروهی نقش به‌سزایی دارد.
- واکنش هوشمند[5]: عامل می‌تواند خودش را با تغییرات محیط وفق داده و در مقابل درخواست سایر عامل‌ها و محیط رفتارهای هوشمندانه نشان دهد [۲].

1- Behavior
2- Perception
3- Cooperation
4- Associated Agent
5- Intelligent

در شکل (۲) نمودار تعامل یک عامل با محیط اطراف آن به نمایش درآمده است؛ یک عامل با بهره‌گیری از حسگرهای خود، شناختی از محیط اطراف کسب می‌نماید و سپس براساس مجموعه قوانین و دانش درونی خود تصمیم می‌گیرد که در مقابل محیط پیرامونی چه اقدامی انجام دهد [۷].



شکل (۲): فرایند تعامل یک عامل با محیط اطراف خود و نحوه تصمیم‌گیری [۷]

بنابراین در یک مدل‌سازی و شبیه‌سازی مبتنی بر عامل، باید عامل‌های مهاجم و مدافع، محیط تعامل[6] و توپولوژی تعامل[7]- که شامل قوانین و پروتکل‌های تعاملی عامل‌ها هستند- تعریف شود. به‌عنوان نمونه برای شبیه‌سازی پروتکل تعامل در زیرساخت ارتباطی شبکه، مفاهیم و ویژگی‌های پروتکل ارتباطی TCP/IP به‌عنوان الگو و اجزاء مختلف شبکه به‌عنوان عامل‌ها در نظر گرفته می‌شود.

۲-۲- حمله سایبری منع خدمت

حمله منع خدمت، تلاش برای خارج‌کردن سامانه و منابع شبکه از دسترس کاربران مجاز است. اگرچه منظور از حمله منع خدمت و انگیزه انجام آن گاهی متفاوت است، اما به‌طورکلی شامل تلاش برای قطع موقت یا دائمی و تعلیق خدمات یک میزبان متصل به شبکه است. طراحان حمله منع خدمت، معمولاً سایت‌ها یا خدمات میزبانی وب سرور با ویژگی‌های مناسب مانند بانک‌ها، کارت‌های اعتباری و سایر خدمات را هدف قرار می‌دهند. یکی از روش‌های معمول حمله، اشباع ماشین‌های هدف با افزایش بار ترافیک از طریق درخواست‌های خارجی و داخلی است. به‌طوری‌که به ترافیک قانونی پاسخ نداده یا با سرعت کم پاسخ‌ها داده شوند یا حتی منابع از دسترس خارج شوند. در ادامه برخی از علائم حملات منع خدمت ارائه می‌گردد:

- کارایی کند و غیرمعمول شبکه

6- Interaction Environment
7- Interaction Topology

- در دسترس نبودن یک وب‌سایت خاص
- ناتوانی در دسترسی به یک وب‌سایت
- افزایش چشمگیر تعداد هرزنامه‌های دریافتی
- قطع اتصال به اینترنت

راه‌کارهای مختلفی برای اجرای حملات منع خدمت وجود دارد که خدمات دهنده‌ها را در حالت سقوط[1] قرار می‌دهند یا آن‌ها را با بسته‌های سیل‌آسا غرق می‌کنند. در ادامه پنج روش اصلی که با بهره‌برداری و هدف قراردادن آن‌ها، حملات منع خدمت انجام می‌گیرد، شرح داده می‌شوند:

- مصرف منابع محاسباتی مانند پهنای باند، حافظه، فضای دیسک و زمان پردازش
- ایجاد تداخل در اطلاعات پیکربندی مانند اطلاعات مسیریابی
- ایجاد تداخل در اطلاعات وضعیت مانند بازنشاندن ناخواسته نشست‌های TCP
- ایجاد تداخل در تجهیزات فیزیکی شبکه
- قطع ارتباط بین کاربران مجاز و قربانی به جهت جلوگیری از ارتباط

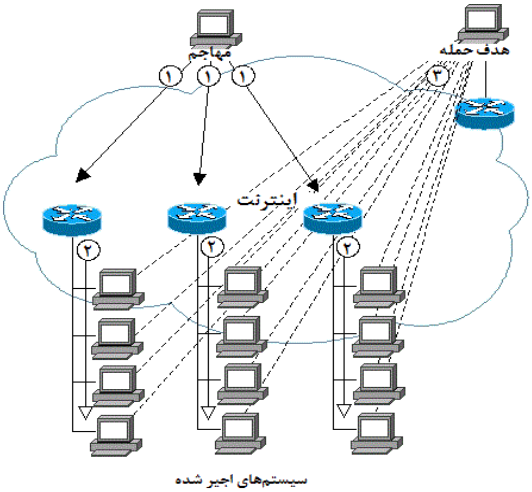
بنابراین یک مهاجم برای اجرای سناریوی حمله منع خدمات، یکی از راه‌کارهای فوق را انتخاب و متناسب با شرایط هدف، برنامه-ریزی و طراحی سناریو نموده و نقشه حمله را اجرا می‌نماید [۴-۳].

۲-۳- حمله سایبری منع خدمت اسمارف[2]

این حمله ممکن است از بیرون و داخل شبکه به قربانی صورت پذیرد. با توجه به این‌که در شبیه‌سازی این مقاله هر دو نوع حمله انجام می‌شود در ادامه به تفکیک آن‌ها را تشریح می‌کنیم.

۲-۳-۱- حمله اسمارف از بیرون شبکه به یک قربانی در درون شبکه

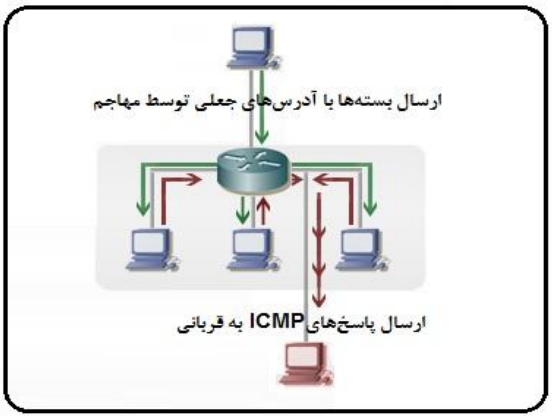
در این نوع حمله مطابق شکل (۳) ابتدا مهاجم یک آسیب‌پذیری در تنظیمات تجهیزات شبکه داخلی شناسایی نموده، سپس بسته‌های جعلی با آدرس مبدأ کامپیوتر هدف (قربانی) به تجهیزات لبه شبکه‌های هدف ارسال می‌نماید، تجهیزات شبکه درخواست مربوطه را به‌صورت پخشی برای کامپیوترهای شبکه خود ارسال کرده و در ادامه، تمامی سامانه‌های شبکه‌های هدف پاسخ درخواست جعلی را به آدرس سامانه قربانی ارسال می‌کنند که نتیجه آن منع خدمت‌دهی سامانه قربانی می‌شود.



شکل (۳): مدل مفهومی از حمله اسمارف از بیرون شبکه به قربانی در درون شبکه

۲-۳-۲- حمله اسمارف از درون شبکه به یک قربانی

مطابق شکل (۴) مهاجم بسته‌های درخواست انعکاس ICMP[3] با آدرس IP مبدأ جعلی که آدرس IP هدف مورد حمله است را درون شبکه پخش می‌کند. تمامی میزبانان شبکه هرکدام یک نسخه از درخواست انعکاس ICMP را دریافت می‌کنند و یک پاسخ انعکاس ICMP را به سیستمی که به‌عنوان مبدأ تلقی می‌کنند، می‌فرستند [۸].



شکل (۴): مدل مفهومی از حمله اسمارف از درون شبکه به قربانی در شبکه [۸]

زمانی که میزبان‌های زیادی در شبکه محلی هستند یا مهاجم از بسته‌های با حجم بزرگ استفاده نماید، تأثیر حمله به‌صورت عمده‌ای افزایش می‌یابد.

1 -Crash
2 -Smurf
3 - ICMP Echo Request

۲-۳-۳- انواع توزیع در شبیه‌سازی

در مدل‌سازی و شبیه‌سازی متناسب با نرخ تولید بسته، ارسال و پردازش درخواست‌ها بین زیربخش‌های مختلف شبکه داخلی و بیرونی و حملات، متناسب با شرایط شبیه‌سازی و سامانه‌های واقعی از توزیع احتمالاتی مختلف مطابق با جدول) استفاده شده است [۹].

جدول (۱): توزیع احتمالاتی استفاده‌شده در شبیه‌سازی

ردیف	نام توزیع	پارامترها	رابطه
۱	نمایی[1]	میانگین	$f(x;\lambda)=\begin{cases}\lambda e^{-\lambda x} & , x\geq 0,\\ 0 & , x<0.\end{cases}$
۲	نرمال[2]	میانگین و انحراف معیار	$f(x)\frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$
۳	مثلثی[3]	حداقل، میانه و حداکثر	$\begin{cases}\frac{(x-a)^2}{(b-a)(c-a)} & \text{for } a\leq x\leq c\\ 1-\frac{(b-x)^2}{(b-a)(b-c)} & \text{for } c\leq x\leq b\end{cases}$
۴	ثابت	عدد ثابت	مقدار ثابت

۲-۳-۴- معیارهای ارزیابی

معیارهای ارزیابی کارایی اجزا مختلف شبیه‌سازی بر اساس رابطه‌های بیان‌شده در ادامه، محاسبه می‌گردد [۱۰].

- میانگین زمان انتظار در صف برای n درخواست مورد نیاز برای پردازش:

$$W_Q=\frac{1}{n}\sum_{i=1}^{n}(D_i) \quad (۱)$$

- میانگین زمان صرف شده در سامانه برای پردازش درخواست‌ها:

$$W=W_Q+E[S] \quad (۲)$$

که در آن، E[S] میانگین زمان پردازش درخواست توسط سرویس‌دهنده است.

- میانگین تعداد درخواست‌های در صف پردازش:

$$L_Q=\frac{1}{T(n)}\int_0^{T(n)}Q(t) \quad (۳)$$

که در آن، Q(t) منحنی تغییرات درخواست‌های منتظر پردازش در واحد زمان است و میانگین زمانی سطح زیرمنحنی Q(t) میانگین تعداد مشتریان در صف را مشخص می‌کند.

- **بهره‌وری سرویس‌دهنده:**

کسری از زمان که سرویس‌دهنده مشغول پردازش درخواست‌ها بوده است:

$$\rho=\frac{1}{T(n)}\int_0^{T(n)}B(t) \quad (۴)$$

که در آن، B(t) منحنی نشان‌دهنده مشغول‌بودن سرویس‌دهنده در واحد زمان است و میانگین زمانی سطح زیرمنحنی B(t) بهره‌وری سرویس‌دهنده را مشخص می‌کند.

- **میانگین تعداد مشتریان در سامانه**

$$L=L_Q+\rho \quad (۵)$$

لذا مطابق با رابطه‌های بیان‌شده وضعیت‌های سامانه‌ها در شرایط مختلف شبیه‌سازی پردازش و ارائه می‌گردد تا میزان مقاومت سامانه در برابر حملات مورد ارزیابی قرار گیرد و در صورت لزوم به‌صورت مناسب‌تر تنظیم و یا به‌روزرسانی گردد [۱۰].

۳- کارهای مرتبط

با توجه به مباحث مطرح‌شده در مقاله، برخی از مجموعه پژوهش‌های صورت گرفته مرتبط با موضوعات تحقیق شامل حملات منع خدمت ترکیبی، حملات سیل‌آسا و راه‌کارهای مقابله و مدل‌سازی و شبیه‌سازی مبتنی بر عامل، ارائه می‌گردد.

در پژوهش سلیمی و دهقانی [۱۱] با معرفی بات‌نت و مفاهیم مرتبط با آن، روش‌های فرماندهی و کنترل بات‌نت[4] مطرح‌شده و باهم مقایسه شده‌اند؛ همچنین مهم‌ترین حملات و عملیات مخرب بات‌نت‌ها مطرح شده است، سپس تعدادی از حملات سایبری بررسی شده و با توجه به مطالب تحقیق، درباره شباهت آن‌ها به حملات بات‌نت، مباحثی ارائه شده است.

در مقاله خواجویی نژاد و همکارانش [۱۲] نحوه ایجاد حمله سیل‌آسای درخواست تماس در شبکه VOIP[5] و تأثیرات این حمله روی سرور SIP[6] بررسی شده است. طبق نتایج این آزمایش با افزایش نرخ حمله، میزان مصرف پردازنده سرور افزایش می‌یابد. افزایش مصرف پردازنده خود منجر به افزایش تعداد بسته‌های تکراری ارسالی و کاهش موفقیت در برقراری نشست می‌گردد؛ همچنین در ادامه راه‌کاری جدید برای تشخیص حمله ارائه‌شده که با جایگزینی فاصله

1- Exponential
2- Normal
3-Triangular

4 - Botnet
5 - Voice over Internet Protocol
6 - Session Initiation Protocol

جفری[1] به‌جای فاصله هلینگر[2] تشخیص حمله سریع‌تر انجام می‌گیرد.

در پژوهش دیگری، سامانه تشخیص نفوذی برای مقابله با حمله منع سرویس در شبکه‌های بی‌سیم اقتضایی ارائه شده است. این سامانه پس از تشخیص حمله با اتخاذ تدابیری، اثر حمله را به حداقل رسانده و عملکرد شبکه را در حد قابل قبولی نگه می‌دارد. مزیت این سامانه تشخیص نفوذ، مقابله سریع یا عاجل آن با گره‌های حمله‌کننده و خنثی‌کردن حمله آن‌ها است. سامانه تشخیص نفوذ پیشنهادی، منجر به تغییر پروتکل مسیریابی نمی‌گردد، بلکه به‌عنوان یک واسط بین ترافیک شبکه و پروتکل مسیریابی قرار می‌گیرد. عملکرد سامانه پیشنهادی با استفاده از نرم‌افزار OPNET شبیه‌سازی و تحلیل شده است [۱۳].

در مقاله صالح‌پور [۱۴] حملات ناشی از فریم‌های EAP[3] در استاندارد IEEE802.11i بررسی شده و روش مناسبی برای مقابله با حملات منع خدمت ناشی از این فریم‌ها حملات ارائه شده است. در تحقیق دیگری پروتکل دست‌دهی ۴ مرحله‌ای امن و کارآمد برای مقابله با حمله DoS در شبکه هوشمند انرژی پیشنهاد شده است [۱۵]. در این تحقیق دو طرح تبادل برپایه توابع یک‌سویه و عدم وابستگی بین مراحل پروتکل پیشنهاد شده است که مقاومت شبکه در برابر حمله منع خدمت به‌صورت کامل بهبود می‌دهد. در عین حال این پروتکل، با محاسبه پیچیدگی مخابراتی و حافظه از نظر سربار تحمیل‌شده به شبکه نیز بهینه است. این پژوهش ضمن توسعه مدل حمله DoS، امنیت طرح پیشنهادی خود را با شبیه‌سازی گسترده به‌وسیله Avispa ارزیابی و اثبات کرده است.

در مقاله جمالی و شاکر [۱۶] یک الگوریتم زمان‌بندی در مقابل حملات سیل‌آسا SYN ارائه شده است. این الگوریتم نیمی از اتصالات با طولانی‌ترین مدت‌زمان را هنگامی‌که اتصالات باز به حد بالایی رسیده، دفع می‌کند. نتایج شبیه‌سازی این مقاله نشان می‌دهد که روش دفاعی ارائه‌شده منجر به بهبود عملکرد سیستمی که مورد هجوم قرارگرفته می‌شود و درخواست‌ها و اشتراک‌های منابع سیستم با افت کارایی کمتری همراه است. در تحقیق دیگری مدیریت ترافیک امنی برای محیط خوشه‌ای برای کنترل حمله منع خدمت توزیع‌شده ارائه شده است [۱۷]. این مقاله یک انتقال امن داده در محیط خوشه را ارائه می‌دهد که ترافیک‌های مختلف جهت کنترل حمله منع خدمت توزیع‌شده در محیط خوشه را باهم مقایسه کرده است.

در مقاله گو و همکارانش [۱۸] حمله توزیع‌شده منع خدمت در زیرساخت‌های اندازه‌گیری پیشرفته مدل‌سازی شده است. در این مقاله مدل‌های مختلف نصب و راه‌اندازی نرم‌افزارهای مخرب و حمله سیل‌آسا به دستگاه‌های AMI[4] معرفی‌شده و اثرات آن مورد بررسی قرار گرفته‌اند. برخی از سناریوهای خاص حمله با استفاده از ابزار NS3 شبیه‌سازی شده و درباره روش‌های امنیتی آن نیز بحث شده است. در مقاله دیگری حمله منع خدمت توزیع‌شده در شبکه‌های بی‌سیم مدل‌سازی و امکان راه‌اندازی حملات توزیع‌شده در شبکه‌های ad hoc بی‌سیم بحث شده است [۱۹]. با توجه به پویایی و سفارشی‌بودن طراحی و اجرای حملات منع خدمت توزیعی برای هر سایت، در مقاله فتحیان و همکارانش [۲۰]، یک سازوکار پویا با قابلیت سفارشی‌سازی برای تشخیص روبات‌های وب مخرب مشارکت‌کننده در حملات، با استفاده از تحلیل رفتار مرورگری آن‌ها ارائه شده است.

مدل‌سازی و شبیه‌سازی عامل محور در تحقیقاتی که در آن‌ها راه‌کارهایی جهت مقابله با حملات سایبری ارائه‌شده کاربرد دارد. در مقاله بن و همکارانش [۲۱] تأثیر شبیه‌سازی عامل محور در پیشرفت اهداف سایبری با رویکرد تجزیه تحلیل و توسعه پدافند سایبری بررسی شده است. در پژوهشی روش شبیه‌سازی زنده و مدل‌سازی جهت شبیه‌سازی رفتار مورد انتظار، به‌خصوص در حملات سایبری در تصمیم‌گیری ارائه شده است [۲۲]. در تحقیق دیگری [۲۳] یک سامانه نمونه برای ارزیابی ریسک شبکه جهت استفاده مدیران شبکه به‌صورت عامل محور شبیه‌سازی شده است. برای شبیه‌سازی و ارزیابی حالات مختلف مهاجم، مدافع با توجه به سخت‌افزارهای مجاز و غیرمجاز درنظر گرفته شده است. در مقاله دیگری دورزدن امنیت توسط کاربران به‌صورت مبتنی بر عامل بیان شده است [۲۴]. در این مقاله یک نمونه خاص از مشکلات امنیتی بررسی و روش‌های کاربر محور جهت تقویت امنیت سامانه پرداخته‌شده، ضمناً قابلیت استفاده از آن‌ها نیز افزایش یافته است.

مدل‌سازی مبتنی بر عامل در زمینه‌های مختلف کاربرد دارد. به‌عنوان مثال، در تحقیق اصغرپور و صادقی [۲۵] مدل‌سازی عامل محور اعتماد در ساختارهای مختلف شبکه‌های اجتماعی ارائه شده است. در پژوهش دیگری رویکردی مبتنی بر عامل برای برنامه

1- Jeffrey Distance (JD)
2- Hellinger Distance (HD)
3- Extensible Authentication Protocol
4- Advanced Metering Infrastructure (AMI)

زمان‌بندی تعاونی‌ها بیان شده است [۲۶]. در تحقیق وکیلی فرد و همکارانش [۲۷] رویکرد مبتنی بر عامل و کاربردهای آن در بازارهای مالی، نرم‌افزارهای مهم درخصوص ایجاد بازارهای مالی مصنوعی و چگونگی به‌کارگیری مدل‌های مبتنی بر عامل در مالی کلاسیک و رفتاری بحث شده است. براساس نتایج این تحقیق رویکرد مدل‌سازی مبتنی بر عامل در کنار الگوی مالی کلاسیک و رفتاری باعث افزایش دقت و کارآمدی در مطالعات مربوط به بازارهای مالی شده است. ریچارد و همکارانش [۲۸] توسعه یک چارچوب مدل‌سازی برای کار تیمی مهندسی شبیه‌سازی شده است.

۴- شبیه‌سازی و ارزیابی راه‌حل

با توجه به مفاهیم بیان‌شده در بخش پیش‌زمینه تحقیق، برای شبیه‌سازی راه‌حل کاهش بار ترافیکی حملات سایبری در سامانه‌های امنیتی و دفاعی با استفاده از توزیع‌شدگی، زیرشبکه‌ها، کامپیوترهای موجود در زیرشبکه‌ها و بستر ارتباطی به‌عنوان محیط تعاملی عامل‌ها درنظر گرفته می‌شود؛ سامانه تشخیص و جلوگیری از نفوذ داخلی جهت شناسایی حملات داخلی، سامانه تشخیص نفوذ نصب شده در لبه‌های شبکه داخلی برای شناسایی و جلوگیری از حملات خارجی و ویروس‌یاب‌های نصب‌شده بر سرورها و کامپیوترهای مشتری -که هرکدام درصدی از نفوذها و حمله‌های منع خدمت را شناسایی و دفع می‌نمایند- به‌عنوان عامل‌های دفاعی و پدافندی شناخته می‌شوند. کامپیوترهای شبکه خارجی و محلی که توسط مهاجمان اجیرشده و در زمان‌های مختلف -که نقش حمله‌کننده را ایفا می‌کنند- به‌عنوان عامل‌های تهاجمی معرفی می‌شوند. در این شبیه‌سازی عامل‌های هجومی و دفاعی در محیط تعاملی با همدیگر رقابت می‌کنند؛ زمانی که منابع (شامل پهنای باند، حافظه و پردازش سرورها، سامانه‌های جلوگیری از نفوذ و تجهیزات شبکه) محدود شد به‌طوری‌که پاسخگوی درخواست کاربران قانونی نیست، زیرساخت شبکه دچار حمله سایبری منع خدمت شده است.

در این تحقیق به دلیل نیاز به بهره‌برداری از ابزاری برای مدل‌سازی و شبیه‌سازی قابلیت‌ها و مفاهیم مبتنی بر عامل از نرم‌افزار ارنا[1] استفاده شده است. نرم‌افزار ارنا قابلیت‌های مناسبی جهت شبیه‌سازی‌های گسسته رخداد و شیءگرا دارد. با کمک این قابلیت‌ها می‌توان ضمن ایجاد عامل‌ها و پروتکل ارتباطی موردنیاز، از انواع توزیع‌های مختلف آماری برای ایجاد رویدادها، پردازش دستورات و سایر نیازمندهای یک شبیه‌سازی مبتنی بر عامل و گسسته رخداد استفاده نمود [۲۹].

۴-۱- تشریح هدف و سناریوی حمله

در این شبیه‌سازی فرض بر شناخت مهاجمان از زیرساخت و توپولوژی شبکه داخلی است؛ لذا تصمیم به طراحی حمله سایبری علیه زیرساخت‌ها و سروهای شبکه می‌نمایند. با توجه به وجود نقطه ضعف امنیتی در تنظیمات سوییچ‌های شبکه و همچنین آسیب‌پذیری روز صفر[2] در سیستم عامل‌ها، تصمیم به اجرای حمله اسمارف با استفاده از سامانه‌های داخلی شبکه می‌نمایند؛ جهت اطمینان از تأثیرگذاری حمله از مجموعه رایانه‌های اجیرشده خود در بیرون از شبکه نیز استفاده می‌نمایند. آن‌ها با توجه به آشنایی با تنظیمات شبکه، سرعت، پهنای باند و دیگر اجزای شبکه، سناریوی حمله را طراحی می‌کنند. در این حمله، آن‌ها موفق به خروج اجزای مختلف شبکه از سرویس‌دهی به مدت معینی می‌شوند؛ بنابراین مهاجمان با استفاده از ظرفیت شبکه داخلی به دلیل ضعف تنظیمات در تجهیزات شبکه و بهره‌برداری از ظرفیت اشغال منابع توسط کاربران قانونی داخلی و خارجی و همچنین سامانه‌های اجیرشده خارجی، حمله منع خدمت اسمارف خود را طراحی و اجرا کرده تا فعالیت‌های سرویس‌دهنده‌های مختلف شبکه مختل نمایند. پارامترها، نتایج شبیه‌سازی و ارزیابی این حمله در اجزای مختلف در ادامه تشریح شده است.

۴-۲- طراحی اجزاء هدف

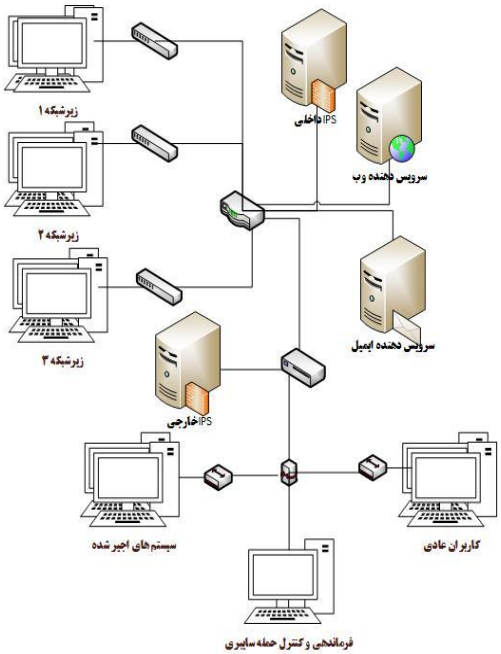
در این قسمت ویژگی‌ها و قابلیت‌های مورد نیاز عامل‌ها و محیط تعاملی بین آن‌ها، تعریف و طراحی شده است، سپس تنظیمات اجزاء مختلف شبکه متناسب با پارامترهای سناریوها، انجام می‌پذیرد.

۴-۲-۱- مدل کلی و تشریح آن

در این مدل، حمله ترکیبی شامل حمله از بیرون و درون شبکه به قربانی مورد نظر شبیه‌سازی می‌گردد که عامل‌های هجومی و دفاعی و بی‌طرف طراحی و پیاده‌سازی می‌گردد. لذا در شکل (۵) نمای کلی و مفهومی زیرساخت‌های شبکه هدف شامل زیرشبکه‌ها، سیستم‌های تشخیص نفوذ و سرویس‌دهنده‌ها، کاربران داخلی و اجیرشده و نحوه جای‌گذاری آن‌ها ارائه‌شده تا براساس آن‌ها میزان کارایی دفاع توزیع‌شده تعاملی و غیرتعاملی بررسی گردد.

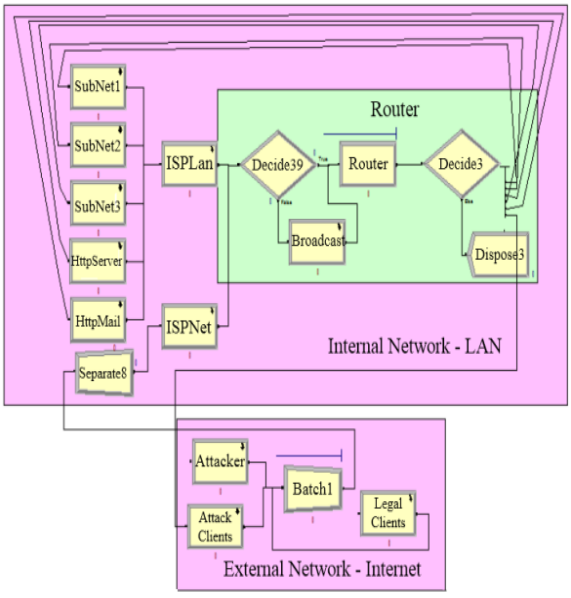
1- Arena

2- Zero-day vulnerabilities



شکل (۵): طرح کلی زیرساخت شبکه سازمان هدف و جایگذاری اجزاء

در شکل (۶) طرح کلی پیاده‌سازی‌شده این مدل در نرم‌افزار ارنا نشان داده شده که شامل شبکه داخلی (زیرشبکه‌ها، سرویس‌دهنده وب، سرویس‌دهنده ایمیل، سامانه جلوگیری از نفوذ) و شبکه خارجی (سامانه فرماندهی و کنترل حملات سایبری، سامانه جلوگیری از نفوذ خارجی، کاربران قانونی خارج از شبکه، رایانه‌های اجیرشده خارجی) است.



شکل (۶): طرح کلی شبیه‌سازی حمله سایبری ترکیبی با نرم‌افزار ارنا

۴-۲-۲- محیط تعامل عامل‌ها

محیط تعامل و ارتباطی عامل‌ها زیرساخت ارتباطی شبکه‌ای مبتنی بر شبیه‌سازی پروتکل TCP/IP بوده که فرماندهی و کنترل عامل‌ها از آن طریق صورت می‌گیرد و ضمن رعایت ویژگی خودمختاری عامل‌ها، در راستای اهداف تعیین‌شده از سمت مدیر نیز اقدام می‌کنند. در این شبیه‌سازی به‌منظور تشخیص و جلوگیری از نفوذ، سامانه‌ای تعاملات داخلی کاربران و سامانه دیگری نظارت بر تعاملات خارجی شبکه را نظارت می‌کنند. در طراحی اجزا، نحوه و میزان درصد بهره‌برداری از منابع جهت پاسخ به درخواست‌های مختلف به ازای هر بسته اهمیت دارد؛ در صورت متناسب‌نبودن تنظیمات و توزیع منابع، در حداقل زمان ممکن سامانه سقوط خواهد کرد.

۴-۲-۳- طراحی و پیاده‌سازی اجزای شبکه خارجی

طرح کلی شبکه خارجی مجموعه‌ای از کاربران قانونی با قابلیت دسترسی از راه دور، سرور فرماندهی و کنترل عملیات حمله سایبری و رایانه‌های اجیرشده توسط مهاجم است؛ که در بخشی از شکل (۵) نشان داده شده است. هرکدام از این بخش‌ها از زیرسامانه‌هایی تشکیل‌شده که با استفاده از امکانات نرم‌افزار و ویژگی‌های عامل طراحی شده است. هر حمله سایبری نیاز به سامانه فرماندهی و کنترلی دارد، در این شبیه‌سازی براساس تجربه و مصاحبه با خبرگان چنین فرض شده که احتمال حمله سایبری به سرویس‌دهنده وب ۵۵ ٪، سرویس‌دهنده ایمیل ۳۰ ٪ و حمله به سایر بخش‌ها ۱۵ ٪ است. فرمانده عملیات سایبری متناسب با شرایط و با توزیع احتمال مشخص، قربانی را تعیین و سپس با تنظیم نرخ بسته‌های ارسالی از رایانه‌های اجیرشده و تغییر اندازه بسته‌های ارسالی، حمله را به سمت قربانی هدایت می‌نماید. در این مدل تنظیمات مربوط به بسته‌ها با توجه به دستورات فرماندهی و کنترل حمله و تعامل عامل‌ها با یکدیگر صورت می‌گیرد تا بسته‌ها متناسب با الگوریتم‌های مسیریابی و ویژگی‌های پروتکل Tcp/Ip به نحو مطلوبی به سمت مقصد هدایت شوند.

۴-۲-۴- طراحی و پیاده‌سازی اجزای شبکه داخلی

در بخشی از شکل (۵) اجزای مختلف شبکه داخلی که متشکل از رایانه‌های کاربران، زیرشبکه با تعداد مشخصی کاربر متناسب با بخش‌های سازمان، سامانه جلوگیری از نفوذ و مسیریاب اصلی و ارتباطات آن‌ها نشان داده شده است؛ در ادامه نحوه طراحی و پیاده‌سازی این بخش‌ها شرح داده شده است.

۴-۲-۵- طراحی و پیاده‌سازی زیر شبکه‌ها

در این زیربخش متناسب با تعاملات عادی شبکه و تعداد رایانه‌های

هر زیرشبکه، بسته تولید می‌شود. بسته‌های دریافتی از خارج از شبکه متناسب با توزیع احتمالاتی مثلثی پردازش و پاسخ داده می‌شود. در زیربخش‌های مختلف شبکه، مدت‌زمانی صرف تنظیم بسته‌ها شامل مسیریابی بسته در زیر شبکه، تغییر آدرس‌های فرستنده و گیرنده، بررسی طول عمر بسته‌ها[1]، حذف بسته‌های سرگردان، بررسی و حذف بسته‌های حملات با توجه به وجود آنتی‌ویروس در سامانه‌های کاربران شبکه است؛ مجموعه این زمان‌ها در قالب توزیع احتمالاتی نرمال محاسبه می‌شود، براساس این تنظیمات، توزیع احتمالاتی و همچنین منابع موجود در زیرشبکه‌ها توان دسترس‌پذیری، توان عملیاتی زیرشبکه و رایانه‌ها ارزیابی می‌گردد.

۴-۲-۶- طراحی و پیاده‌سازی سامانه جلوگیری از نفوذ

در سامانه جلوگیری از نفوذ، بسته‌های دریافتی براساس توزیع احتمالاتی پردازش می‌شوند. براساس مجموعه ویژگی‌ها و الگوی حملات تعریف‌شده، برخی از بسته‌های حمله شناسایی و از زیرساخت شبکه حذف می‌شوند. از آن‌جا که سامانه‌های دفاعی و امنیتی نمی‌توانند به‌طور کامل حملات را شناسایی و از آن‌ها جلوگیری کنند، براساس توزیع احتمال ثابت این اقدام صورت می‌گیرد؛ البته متناسب با سناریوهای مختلف این درصدها قابل تغییر هستند. با توجه به منابع محدود این واحد پردازشی (شامل پردازنده، حافظه اصلی و پهنای باند) در صورت بروز حمله و ازدیاد ترافیک و حجم بسته‌های حمله ممکن است سامانه سقوط نماید که این باعث کاهش پایداری و امنیت شبکه به‌صورت زنجیروار می‌گردد.

۴-۲-۷- طراحی و پیاده‌سازی سرویس‌دهنده وب و ایمیل

در سرویس‌دهنده وب و ایمیل، درخواست‌های مختلف مربوط به کاربران داخلی و خارجی دریافت می‌شود. براساس یک توزیع احتمال مثلثی پردازش و پس از مدتی پاسخ ارسال می‌شود. سامانه‌های دفاعی و امنیتی وب سرور بسته‌های سرگردان و آن‌هایی که به‌عنوان حمله شناسایی کرده، با درصد احتمال مشخصی حذف می‌نماید. لازم به ذکر است که نحوه پردازش و پاسخ‌گویی درخواست‌ها براساس پروتکل ارتباطی شبکه Tcp/ip است که در صورت بروز حمله و ازدیاد ترافیک و حجم درخواست‌ها به دلیل محدودبودن منابع سرویس‌دهنده احتمال سقوط سرویس‌دهنده‌ها وجود دارد.

۴-۲-۸- طراحی و پیاده‌سازی مسیریاب مرکزی

بیشترین پردازش بسته‌ها در مسیریاب مرکزی بوده که بسته‌های مختلف شبکه داخلی و خارجی را پردازش کرده و ضمن مسیریابی بسته‌ها، بسته‌های سرگردان و آن‌هایی که با الگوهای حملات سایبری شباهت دارد را حذف می‌نماید. درصورت افزایش بسته‌ها در مسیریاب، با توجه به محدودیت منابع جهت پردازش، صف تشکیل می‌شود که موجب اختلال در مسیریاب می‌شود. در این صورت مسیریاب توانایی سرویس‌دهی در زمان مشخص به سایر بخش‌ها را نداشته و کل شبکه مختل می‌شود. جهت تولید بسته‌های جعلی (ICMP) در حمله اسمارف، از قابلیت‌های نرم‌افزاری برای تکثیر بسته‌ها استفاده می‌شود تا بتوان به تعداد رایانه‌های زیرشبکه بسته ایجاد نمود. با این روش حجم زیادی از منابع اجزای مختلف شبکه مصرف می‌گردد که موجب ایجاد ترافیک بسته در زیرساخت‌ها می‌شود.

۴-۲-۹- طراحی و پیاده‌سازی مفهوم تعامل عامل‌ها در حمله

در این شبیه‌سازی عامل‌های هجومی براساس اعلان عمومی زمان حمله و هدف، از طریق مدیر و سامانه فرماندهی و کنترل حمله سایبری، حمله به سمت هدف را آغاز می‌نمایند و سعی دارند تا متناسب با نوع حمله هدف را از ارائه سرویس‌دهی عمومی و در دسترس‌بودن خارج نمایند؛ همچنین پس از شروع حمله و شناسایی الگوی اولیه حمله توسط سامانه‌های تشخیص، براساس یک اعلان عمومی حمله از طرف یکی از عوامل تشخیص حمله و تأیید مدیر سامانه امنیتی، سایر مؤلفه‌ای دفاعی از بروز حمله مطلع شده‌اند و با به‌روزرسانی پایگاه دانش خود، دقت شناسایی و تشخیص را افزایش می‌دهند.

در این تحقیق، سامانه‌های کاربران، سرویس‌دهنده وب و ایمیل به‌عنوان عوامل بی‌طرف در نظر گرفته شده‌اند؛ اما درصورتی‌که مهاجم بتواند به سامانه‌های کاربران دسترسی غیرمجاز پیدا کند، آن‌ها به عامل هجومی تغییر وضعیت می‌دهند. رایانه‌های اجیرشده داخلی و خارجی که در دسترس مهاجم هستند به‌عنوان عامل هجومی شناخته می‌شوند. کنترل این سامانه‌ها در اختیار سامانه فرماندهی و کنترل مهاجم است.

۴-۳- پارامترها و معیارهای ارزیابی شبیه‌سازی حمله سایبری

از آن‌جا که میزان تأثیرگذاری حمله سایبری به ویژگی بخش‌های مختلف شبکه و پارامترهای آن ارتباط مستقیم دارد، می‌توان متناسب با شرایط سناریوها و زیرساخت‌های تعریف‌شده، پارامترهای مشخصی تعیین و براساس آن‌ها، نتایج شبیه‌سازی را بررسی نمود. لذا پارامترهای زیر براساس نظر متخصصان احصاء شده تا کارایی دفاع توزیع‌شده مبتنی بر عامل بررسی و ارزیابی گردد.

1- time-to-live or packet lifetime

۴-۳-۱-پارامترهای شبیه‌سازی

در این بخش پارامترهای اجزای مختلف شبیه‌سازی، شامل میزان تولید نرخ بسته‌ها در زیرشبکه‌ها، کاربران خارجی شبکه، قربانیان اجیر شده و همچنین میزان پاسخ و پردازش اجزای سامانه تشخیص نفوذ داخلی و خارجی، پردازش در سرویس‌دهنده‌های وب و ایمیل، مسیریاب مرکزی مطابق با جداول‌های (۴-۲) ارائه شده است.

جدول (۲): اجزای مختلف شبکه

مؤلفه‌ها	مقدار/تعداد
زیر شبکه با تعداد ۱۰۰ مشتری	۳ عدد
تعداد رایانه‌های کل شبکه	۳۰۰ رایانه
تعداد رایانه‌ها و کاربران خارجی	۱۰۰۰ عدد
تعداد قربانیان اجیرشده	۵۰۰ عدد
سامانه‌های تشخیص نفوذ	۲ عدد
سرویس‌دهنده‌های وب و ایمیل	۲ عدد
مسیریاب اصلی شبکه	۱ عدد

جدول (۳): نرخ تولید بسته و پاسخ‌ها در اجزاء مختلف شبکه

ردیف	شرح فعالیت	مؤلفه‌ها	توزیع احتمالاتی	تعداد در ثانیه
۱	نرخ تولید بسته/درخواست	کاربران قانونی خارجی	نمایی	۰/۰۰۸
		رایانه‌های قربانی اجیرشده خارجی	نمایی	۰/۰۰۴
		زیر شبکه داخلی در زمان حمله	نمایی	۰/۰۰۳۵
		زیر شبکه‌های داخلی	نمایی	۰/۰۰۸
۲	زمان پردازش (درخواست و پاسخ)	سرویس‌دهنده وب	مثلثی	۰/۰۱
		ایمیل	مثلثی	۰/۰۵
۳	زمان پردازش درخواست	IPS داخلی	مثلثی	۰/۰۰۱
		IPS خارجی	مثلثی	۰/۰۰۸
		مسیریاب شبکه داخلی	مثلثی	۰/۰۰۰۵

جدول (۴): وضعیت تعاملات و درخواست‌های مختلف شبکه داخلی و خارجی

ردیف	وضعیت توزیع	مؤلفه‌ها	مقدار/تعداد به درصد
۱	درخواست‌ها در شبکه داخلی	سرویس‌دهنده وب	۵۵
		سرویس‌دهنده ایمیل	۳۰
		سایر زیر شبکه‌ها و اجزاء	۱۵
۲	درخواست‌ها در کاربران خارجی	سرویس‌دهنده وب	۶۵
		سرویس‌دهنده ایمیل	۳۵
۳	حمله به زیرساخت‌ها	سرویس‌دهنده وب	۴۰
		سرویس‌دهنده ایمیل	۳۰
		سایر زیرساخت‌ها	۳۰

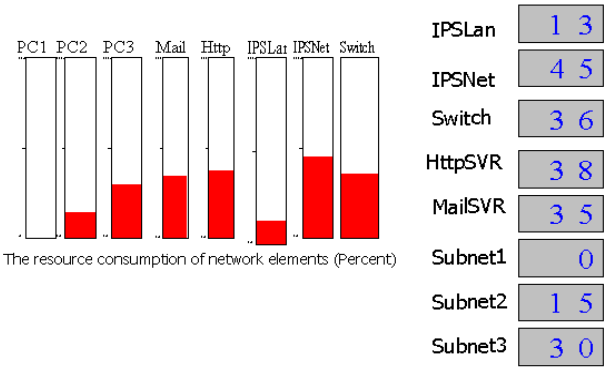
متناسب با نوع حمله، تعداد زیرشبکه و منابع مختلف اجزاء می‌توان مقادیر را متناسب‌سازی و معادل‌سازی کرد و نتایج مورد نظر را از شبیه‌سازی به دست آورد. در جدول (۵) لیست منابع اجزای مختلف شبکه شامل حافظه اصلی، پهنای باند، سرعت پردازنده ارائه شده است. اجزای شبکه شامل سرویس‌دهنده‌های ایمیل و وب، سوییچ مرکزی شبکه، سامانه تشخیص‌دهنده شبکه خارجی و داخلی هستند که متناسب با نوع شبکه‌ها و اجزای آن و میزان مصرف به ازای هر درخواست قابل تنظیم بوده تا براساس آن بتوان اجزای شبکه را به بهینه‌ترین وضعیت تنظیم نمود. با این کار می‌توان هر نوع حمله با هر مقیاسی را نیز اجرا کرد تا نتایج این حملات بر بخش‌های مختلف شبکه مشخص شود.

جدول (۵): لیست منابع اجزای مختلف شبکه، مقدار و نوع آن‌ها

ردیف	اجزاء شبکه	نام و مقدار منبع		
		پهنای باند	حافظه	توان پردازش
۱	سرویس‌دهنده وب	۴۰	۴۰	۴۰
۲	ایمیل سرور	۳۰	۳۰	۳۰
۳	مسیریاب مرکزی	۵۰	۵۰	۵۰

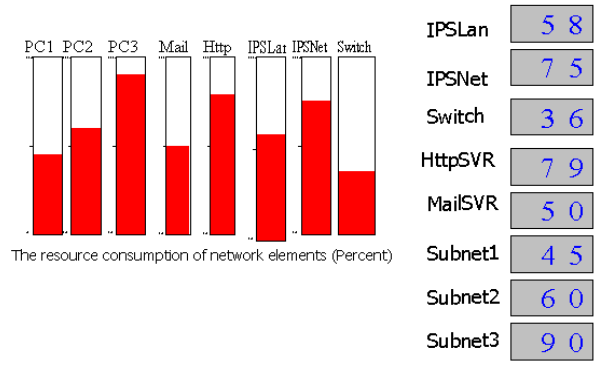
۴-۴- اجرای سناریوهای حمله

در زمان شروع شبیه‌سازی و تا قبل از حمله وضعیت مصرف منابع در زیرساخت‌های مختلف شبکه عادی بوده و درخواست کاربران در زمان‌های پیش‌بینی‌شده پردازش و پاسخ داده می‌شود که این شرایط در شکل (۷) نمایش داده شده است.



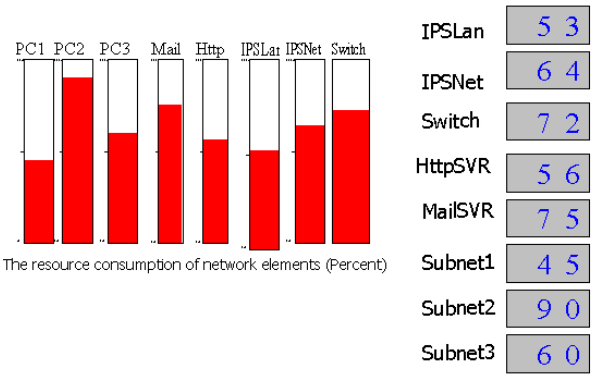
شکل (۷): وضعیت بسته‌های دریافتی در سرویس‌دهنده‌های وب، ایمیل، IPS ها و مسیریاب در اوایل شبیه‌سازی

به‌عنوان نمونه، میزان مصرف منابع در سامانه تشخیص نفوذ شبکه و سرویس‌دهنده وب به ترتیب ۴۵ ٪ و ۳۸ ٪ است. برای شناسایی‌نشدن حمله سایبری، مهاجم ممکن است هدف خود را مطابق با احتمالات بیان‌شده در جدول (۴) تغییر دهد تا بار ترافیکی تولیدشده در اجزای مختلف توزیع شود؛ به دلیل ازدحام و عدم توانایی پردازش به‌موقع بسته‌ها توسط تجهیزات میانی شبکه، بسته‌ها با تأخیر به مقصد منتقل می‌شود، لذا مطابق با شکل (۸) و وضعیت منابع مصرف‌شده، می‌توان استدلال کرد که در این لحظه، هدف حمله سایبری، زیرشبکه ۳ و سرویس‌دهنده وب است که این حمله باعث ایجاد ترافیک بر روی سامانه‌های تشخیص نفوذ شده است.



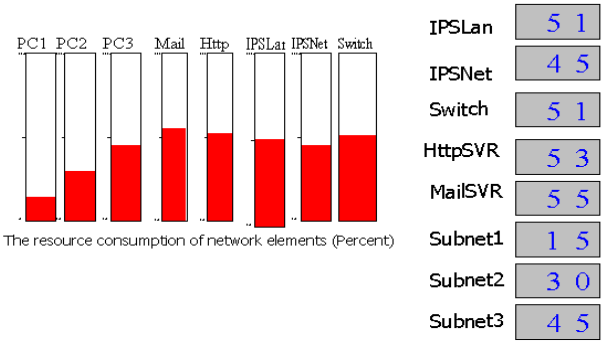
شکل (۸): وضعیت منابع در زمان حمله سایبری به زیرشبکه ۳ و سرویس‌دهنده وب

با توجه به توضیحات بیان‌شده، مطابق با شکل (۹) هدف حمله سایبری زیر شبکه ۲ و سرویس‌دهنده ایمیل است. بار ترافیکی ناشی از حملات قبلی و این حمله همچنان در تجهیزات میانی شبکه بخصوص سوییچ مرکزی و سامانه‌های تشخیص نفوذ مشاهده می‌شود.



شکل (۹): وضعیت منابع در زمان حمله سایبری به زیر شبکه ۲ و سرویس‌دهنده ایمیل

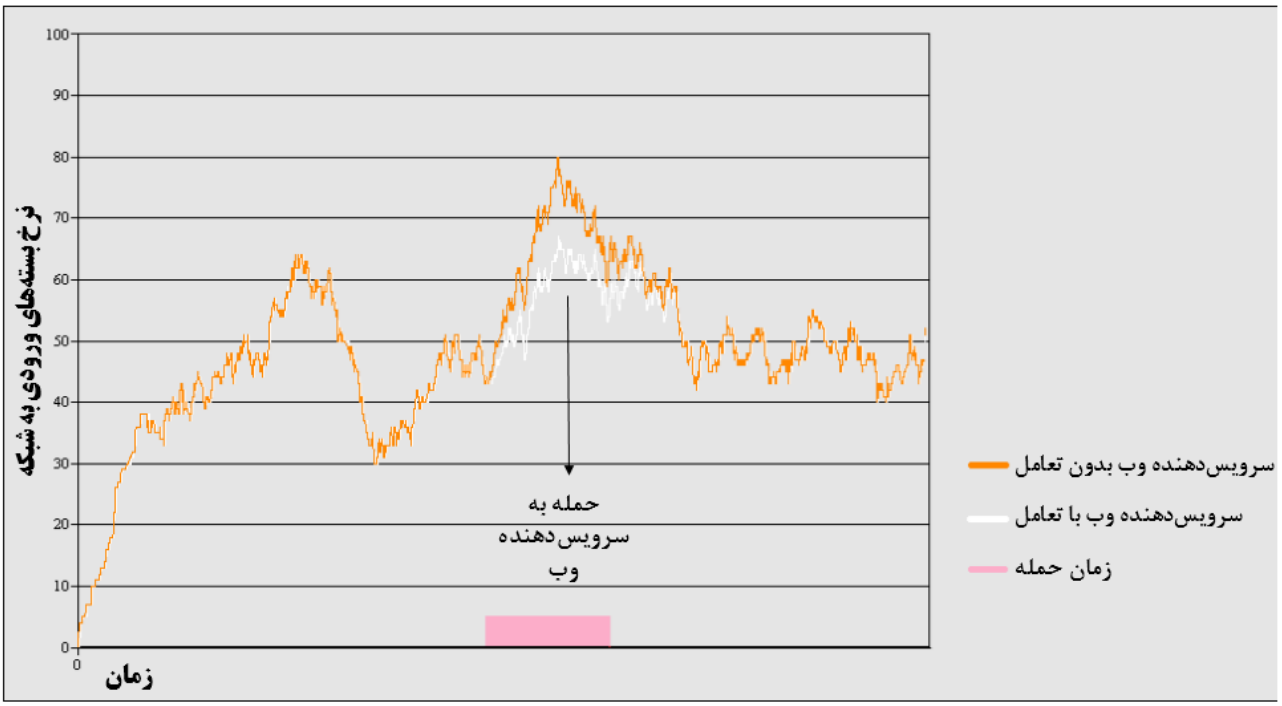
شکل (۱۰) وضعیت منابع تجهیزات پس از حمله سایبری به زیرساخت‌ها را نشان می‌دهد که براساس آن وضعیت مصرف منابع همه تجهیزات و سرویس‌دهنده‌ها متعادل بوده و به درخواست‌ها را در حد زمانی معقول پاسخگو هستند. همان‌طورکه نشان داده شد، با شروع حملات سایبری از درون و بیرون به زیرساخت‌های شبکه و با مدیریت، فرماندهی و کنترل مهاجم، منابع قربانیان در شبکه به‌طور سریع مصرف شده و آن‌ها قادر به پاسخگویی درخواست‌های مجاز نیستند. لذا با شبیه‌سازی زیرساخت‌های شبکه، بدون اخلال و تأخیر در شبکه واقعی، می‌توان وضعیت تجهیزات و تنظیمات آن‌ها را در برابر حملات سایبری ارزیابی و تعیین نمود.



شکل (۱۰): وضعیت بسته‌های دریافتی در سرویس‌دهنده‌های وب، ایمیل، IPS ها و مسیریاب پس از کنترل و دفع حمله سایبری توسط سامانه‌های دفاعی

اجرای شبیه‌سازی به دو مدل انجام‌شده که در یکی عامل‌های دفاعی با یکدیگر در تعامل بوده و در دیگری تعاملی وجود ندارد. در حالتی که عوامل دفاعی با یکدیگر در تعامل هستند، IPS خارجی هنگام مشاهده افزایش تعداد بسته‌های خارجی و IPS داخلی نیز هنگام مشاهده افزایش تعداد بسته‌های داخلی به سایر اجزای دفاعی هشدار می‌دهند که احتمال حمله افزایش یافته یا حمله به وجود آمده است. هنگام رسیدن هشدار به اجزای دفاعی همچون آنتی‌ویروس‌ها، این اجزا با به‌روزرسانی پایگاه دانش خود، سامانه‌های دفاعی را در برابر بسته‌های بعدی افزایش می‌دهند.

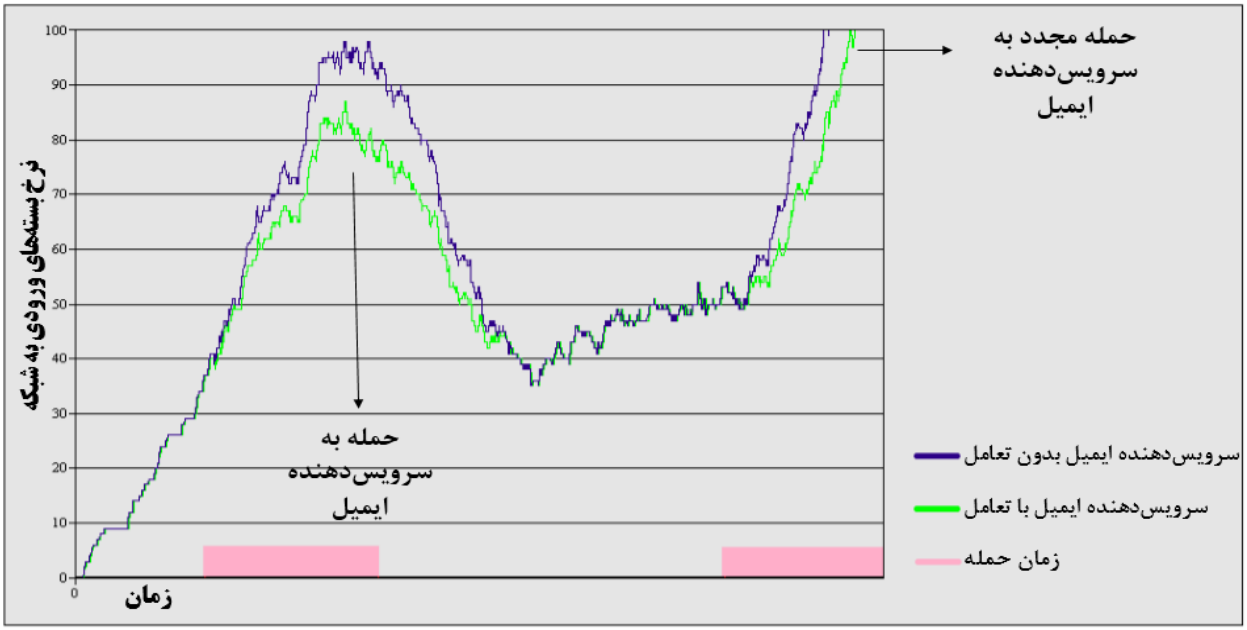
طبق سناریوهای تعریف‌شده در این شبیه‌سازی حمله به سرویس‌دهنده ایمیل و وب موجود در شبکه صورت می‌گیرد. حمله از طرف رایانه‌های اجیرشده خارج از شبکه به‌صورت منع خدمت توزیع‌شده و از طرف اجیرشدگان داخل شبکه به‌صورت اسمارف انجام می‌شود. اشکال (۱۲-۱۱) به ترتیب نتایج حمله به سرویس‌دهنده ایمیل و وب را در مدل شبکه تعاملی و غیرتعاملی نمایش می‌دهد که ترافیک شبکه درحالتی که عامل‌های دفاعی باهم تعامل دارند.



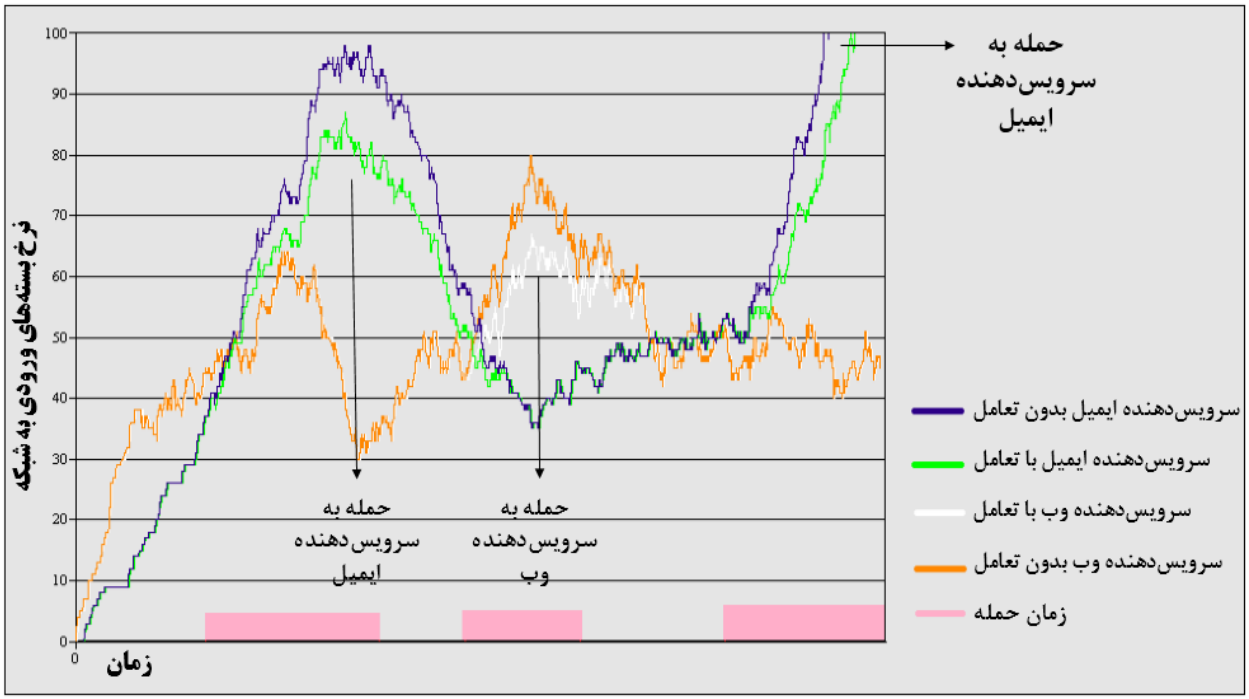
شکل (۱۱): ازدحام بسته‌های شبکه در حمله انجام‌شده به سرویس‌دهنده ایمیل

نسبت به حالت غیرتعاملی به‌طور میانگین ۱۵ ٪ کاهش یافته است. در ادامه شبیه‌سازی با پایان حمله به سرویس‌دهنده‌ها شبکه به حالت عادی خود برگشته تا این‌که پس از مدتی با نظارت سامانه فرماندهی و کنترل حمله سایبری مجدداً حمله‌ای به سرویس‌دهنده‌ها شروع می‌شود و هرچه نرخ ارسال بسته‌ها بیشتر باشد در زمان کمتری سرویس‌دهنده‌ها از کار می‌افتند. حمله‌های انجام‌شده به شبکه در طول زمان شبیه‌سازی در شکل (۱۳) مشاهده می‌شود؛ همان‌طور که نمایش داده‌شده، شبکه ابتدا در حالت عادی قرار دارد تا این‌که از سمت سامانه فرماندهی کنترل حمله سایبری، زمان شروع و هدف حمله به‌تناسب جدول احتمالاتی بیان‌شده تعیین شود.

همان‌گونه که در شکل (۱۳) مشخص است، در این حمله ترکیبی، در شبکه‌ای که عامل‌ها در آن با یکدیگر تعامل دارند، به دلیل به‌روزرسانی پایگاه دانش الگوهای حمله در سامانه‌های دفاعی در حداقل زمان پس از شروع حمله، ترافیک حمله در نقاط مختلف شبکه بررسی و حذف خواهند شد. میزان کاهش ترافیک حمله در شبکه تعاملی به اهداف مختلف به دلیل تعامل عامل‌ها و توزیع احتمالاتی تعریف‌شده، متناسب با ویژگی‌ها و تنظیمات زیرساخت‌های هدف متغیر است.



شکل (۱۲): ازدحام بسته‌های شبکه در حمله انجام‌شده به سرویس‌دهنده وب



شکل (۱۳): نتایج شبیه‌سازی کل حملات انجام‌شده توسط سامانه فرماندهی کنترل حمله

۴-۵- تحلیل و ارزیابی نتایج

نتایج حاصل از مدل‌سازی و شبیه‌سازی برمبنای مقادیر پارامترها و تنظیمات مفروض زیرساخت‌های شبکه و معیارهای ارزیابی کارایی، نشان می‌دهد که در حالت تعامل عامل‌های دفاعی توزیع‌شده، نرخ ترافیک حمله به نحو محسوسی و زنجیروار در المان‌های مختلف کاهش می‌یابد و علت این کاهش، شناخت عامل‌ها از وضعیت حمله و ویژگی‌های آن است؛ بنابراین در دو مرحله حمله به سرویس‌دهنده ایمیل، بار ترافیک درخواست‌ها، نسبت به حالت غیرتعاملی عامل، به‌طور میانگین ۱۵ ٪ کاهش‌یافته است که این میزان کاهش با توجه به فرضیات توزیع‌های احتمالاتی تولید و توزیع درخواست‌ها، نرخ شناسایی حملات جدید و سایر ویژگی‌های زیرساخت شبکه است. همچنین در یک مرحله حمله به سرویس‌دهنده وب، برمبنای شرایط ذکرشده در زیرساخت شبکه و سرویس‌دهنده ایمیل، نتایج نیز مجدداً تکرار شده است؛ بنابراین در شرایط یکسان حمله به زیرساخت‌ها، کارایی عامل‌های دفاعی تعاملی نسبت به عامل‌های غیرتعاملی مطلوب‌تر بوده، درصورتی‌که سامانه‌های امنیتی و دفاعی در بستر شبکه به‌صورت توزیع‌شده و تعاملی قرار گیرند، به دلیل تعامل و به‌روزرسانی الگوهای حمله در حداقل زمان ممکن در عامل‌ها، ترافیک حمله اعمال‌شده به شبکه سریع‌تر توسط عامل‌های دفاعی شناسایی و حذف می‌شوند. با افزایش سرعت در شناسایی و تعامل عامل‌ها، میزان پایداری شبکه و سرویس‌دهنده‌ها بیشتر خواهد می‌شود.

۵- نتیجه‌گیری

در این مقاله از مفاهیم مدل‌سازی و شبیه‌سازی مبتنی بر عامل و حملات سایبری منع خدمت توزیع‌شده به‌منظور بررسی راه‌حل ارائه‌شده جهت کاهش بار ترافیکی حملات سایبری در سامانه‌های امنیتی و دفاعی استفاده شده است؛ برای این منظور، از نرم‌افزار شبیه‌سازی ارنا، برای مدل‌سازی عامل‌های هجومی، دفاعی و بی‌طرف مطابق با سناریوهای مشخص و پروتکل ارتباطی عامل‌ها استفاده شده است. در دفاع توزیع‌شده تعاملی به دلیل تعامل بین عامل‌ها، پس از شناسایی حمله و الگوی حمله با اعلان عمومی، دانش سایر عامل‌ها نسبت به حمله صورت‌گرفته به‌روزرسانی شده و ترافیک حمله واردشده به شبکه، سریع‌تر شناسایی و حذف می‌گردد. نتایج حاصل از این مدل‌سازی و شبیه‌سازی نشان می‌دهد که متناسب با شرایط و سناریوهای حمله تعریف‌شده به سرویس‌دهنده‌ها، دفاع مبتنی بر عامل توزیع‌شده کارایی مناسب‌تری نسبت به حالت بدون تعامل دارد و این میزان بهبود با توجه به شرایط مفروض در سناریوها، به‌طور میانگین ۱۵ ٪ بوده که باعث کارآمدترشدن سامانه‌های دفاعی در زمان حمله می‌شود. لذا با توجه به نتایج، پیشنهاد می‌گردد جهت کارآمدنمودن سامانه‌های دفاعی و امنیتی، از ویژگی و قابلیت‌های دفاع مبتنی بر عامل توزیع‌شده، استفاده گردد.

۶- مراجع

1. C. M. Macal and M. J. North, "Tutorial on agent-based modeling and simulation," in Proceedings of the 37th conference on Winter simulation, pp. 2-15, 2005.
2. C. M. Macal and M. J. North, "Agent-based modeling and simulation," in Winter simulation conference, pp. 86-98, 2009.
3. J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, vol. 34, pp. 39-53, 2004.
4. S. Kumar, "Smurf-based distributed denial of service (ddos) attack amplification in internet," in Internet Monitoring and Protection. ICIMP. Second International Conference on, pp. 25-25, 2007.
5. I. Kotenko and A. Ulanov, "Simulation of internet DDoS attacks and defense," in International Conference on Information Security, pp. 327-342, 2006.
6. I. Kotenko, A. Konovalov, and A. Shorov, "Simulation of Botnets: Agent-based approach," in Intelligent Distributed Computing IV, pp. 247-255, Springer, 2010.
7. P. R. Norvig and S. A. Intelligence, "A modern approach," Prentice Hall, 2002.
8. F. Sajjad, "Denial of Service–The Smurf Attack," School of Computer Science University of Windsor, vol. 401, 2009.
9. W. L. Martinez and A. R. Martinez, "Computational statistics handbook with MATLAB," vol. 22: CRC press, 2007.
10. U. N. Bhat, "An introduction to queueing theory: modeling and analysis in applications," Birkhäuser, 2015.
11. T. Salimi and M. Dehghani, "Botnet and Its Attacks," Passive defense quarterly, vol. 4, no. 2, Summer 2014. (in persian)
12. A. Khajejoei, H. R. Oskoei, and S. R. Chogan, "Study the impacts of INVITE flooding attack in VOIP and offering a new approach to detect attack," Electronics indostries quarterly, vol. 6, no. 2, 2015. (in persian)
13. M. Saleh Esfehani and M. Aboali, "An IDS for Detection of Active Attacks against Routing inMobile Ad Hoc Networks," Journal of Passive Defence Science and Technology, Issue 1, vol. 1, 2010. (in persian)
14. A. Salehpour, "A New Method Against DoS Attacks of EAP Frames in IEEE802.11i," Majlesi Journal of Electrical Engineering, Issue 4, vol. 8, 2009.
15. M. H. Ansari, V. Tabatab Vakily, and M. Gohareie, "Secure and Efficient 4-way Handshake in Smart Grid to DoS Attacks Mitigation," Journal of electronical & cyber defenc, vol. 4, no. 1, 2016. (in persian)
16. Sh. Jamali and Gh. Shaker, "Defense against SYN Flooding Attacks: A Scheduling Approach," Journal of Information Systems and Telecommunication, vol. 2, no 1, pp. 55-62, 2014.
17. K. Govinda and E. Sathiyamoorthy, "Secure Traffic Management in Cluster Environment to Handle DDOS Attack," World Applied Sciences Journal, vol. 32, Issue 9, pp. 1828-1834, 2014.
18. Y. Guo, C. W. Ten, S. Hu, and W. W. Weaver, "Modeling distributed denial of service attack in advanced metering

infrastructure," Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power & Energy Society, 2015.

19. Q. Huang, H. Kobayashi, and B. Liu, "Modeling of distributed denial of service attacks in wireless networks," PACRIM. 2003 IEEE Pacific Rim Conference on, 2003.
20. M. Fathian, M. Abdollahi Azgomi, and H. Dehghani, "Modeling Browsing Behavior Analysis for Malicious Robot Detection in Distributed Denial of Service Attacks, Journal Of Electronical & Cyber Defense," vol. 4, no. 2, 2016. (In Persian)
21. B. W. Priest, E. Vuksani, N. Wagner, and et al., "Agent-based simulation in support of moving target cyber defense technology development and evaluation," Proceeding CNS '15 Proceedings of the 18th Symposium on Communications & Networking, San Diego, CA, USA, pp. 16-23, 2015.
22. E. Cayirci and R. Ghergherehchi, "Modeling cyber attacks and their effects on decision process," Proceeding WSC '11 Proceedings of the Winter Simulation Conference, pp. 2632-2641, 2011.
23. N. Wagner, R. Lippmann, M. Winterrose, and et al., "Agent-based simulation for assessing network security risk due to unauthorized hardware," Proceeding ADS '15 Proceedings of the Symposium on Agent-Directed Simulation, Society for Computer Simulation International San Diego, CA, USA, pp. 18-26, 2015.
24. V. Kothari, J. Blythe, S. Smith, and R. Koppel, "Agent-based modeling of user circumvention of security," Proceeding ACySE '14 Proceedings of the 1st International Workshop on Agents and Cyber Security, no. 5, ACM New York, NY, USA, 2014.
25. A. Asgharpoor masuleh and A. Sadeghi, "Agent-based modeling of trust in the different structures of social networks," Iranian Journal of Sociology, vol. 15, no. 2, 2014. (In Persian)
26. J. Behnamian, "Agent-based approach for cooperative scheduling," Journal of Industrial and Systems Engineering, vol. 9, Issue 4, 2016.
27. H. Vakili fard, M. Khoshnood, H. Foroughnejad, and M. Osoolian, "Agent-based modeling in financial markets," Journal of Knowledge and investment, vol. 3, 2014. (In Persian)
28. R. M. Crowder, M. A. Robinson, H. P. N. Hughes, and Y. W. Sim, "The Development of an Agent-Based Modeling Framework for Simulating Engineering Team Work," IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans, vol. 42, Issue: 6, pp. 1425-1439, 2012.
29. M. D. Rossetti, "Simulation modeling and Arena," John Wiley & Sons, 2015.

A Solution to Reduce the Traffic Load of Cyber Attacks in Security and Defense Systems Using Interactive Distribution

M. Abbasi*, S. Keshvari, M. R. Hasani Ahangar

Abstract

With the increase in using cyber space in organizations, cyber-attacks specially DDOS attacks by malware and intruders have increased. According to limits that do not allow the terms of a cyber attack to be created in organizations, in addition to providing information about systems at the time of the attack, using simulation provides the possibility of a wide variety of attacks with different sizes. Agent-based modeling and simulation is a method for simulating systems comprised of different agents. In this article, in addition to describing the concepts and features of the agent-based modeling and simulation and DDOS attack, the necessary conditions to examine the various scenarios of distributed interactive and non-interactive cyber attack and defense and evaluation of its performance is provided. The results show that the Defense Distributed Interactive has a better performance than non-interactive mode and the load at the time of the attack is reduced to an average of 15 percent. This reduction of traffic load is due to interaction of defence agents with each other that subsequently increases the defense capability of agents when the attack occurs.

Key Words: *Simulation, Agent Based, Cyber Attack, DDOS, Cyber Security, Defense Distributed*

* Imam Hussein Comprehensive University, (moabbasi@ihu.ac.ir) - Writer-in-Charge