

بررسی چالش‌های امنیتی و چگونگی مقابله با آنها در شبکه‌های نرم‌افزارمحور

محمود دی‌پیر^{۱*} و مژگان قصابی^۲

^۱ استادیار، دانشکده رایانه و فناوری اطلاعات، دانشگاه هوایی شهید ستاری، تهران، ایران

mdeypir@ssau.ac.ir

^۲ دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، گروه کامپیوتر، تهران، ایران

mozghan.ghasabi@srbiau.ac.ir

چکیده

در سال‌های اخیر، شبکه‌های نرم‌افزارمحور به‌منظور انعطاف و برنامه‌پذیری بیشتر در شبکه‌های رایانه‌ای مطرح شده و به‌سرعت در شبکه‌های زیرساختی و مراکز داده به کار گرفته شده‌اند. استفاده از این گونه شبکه‌ها مزایایی چون مقیاس‌پذیری، کاهش ترافیک کنترلی، استفاده بهینه از پهنای باند، مهندسی ترافیک بهتر و غیره را دارد؛ که همگی این مزایا ریشه در قابلیت برنامه‌پذیری این شبکه‌ها دارند. در کنار این مزایا، چالش‌های امنیتی نیز وجود دارند که اغلب از همین قابلیت‌ها سرچشمه می‌گیرند. وجود این چالش‌ها، اطمینان‌پذیری شبکه‌های نرم‌افزارمحور را در مقابل شبکه‌های سنتی کاهش می‌دهند؛ بنابراین شبکه‌های نرم‌افزارمحور در صورتی که بر اساس یک معماری امن طراحی نشوند در مقابل حملات سایبری شناخته‌شده‌ای چون حمله منع خدمت توزیع‌شده، جعل و سرقت داده‌ها بسیار آسیب‌پذیر خواهند بود؛ اما به‌منظور مقابله با این چالش‌ها، راهکارهایی ارایه شده است. در این مقاله چالش‌های امنیتی شبکه‌های نرم‌افزارمحور را به‌صورت ساختاری بررسی کرده و راهکارهای ارایه‌شده برای آنها را توصیف خواهیم کرد. علاوه‌براین، کاربردهای امنیتی این نوع شبکه‌ها مانند ایجاد و جداسازی ترافیک شبکه‌های مجازی، کنترل دسترسی بر روی جریان‌های داده و مسیریابی امن را بررسی کرده و درنهایت چگونگی شبیه‌سازی حملات به‌منظور انجام آزمایش‌های امنیتی را به کمک شبیه‌ساز این گونه شبکه‌ها، بررسی می‌کنیم.

واژگان کلیدی: شبکه‌های نرم‌افزارمحور، امنیت، حملات سایبری، حملات منع خدمت.

۱- مقدمه

چگونگی مقابله با این حملات به‌وسیله ارایه راهکارهای مختلف می‌پردازیم. همچنین در مورد چگونگی طراحی یک شبکه نرم‌افزارمحور امن که در مقابل حملات و آسیب‌پذیری‌ها مقاوم باشد، بحث می‌کنیم. درنهایت برخی از کاربردهای امنیتی شبکه‌های نرم‌افزارمحور را برمی‌شمایم و چگونگی شبیه‌سازی حملات و بررسی تأثیرات حملات امنیتی را توصیف خواهیم کرد.

۲- شبکه‌های نرم‌افزارمحور

معماری بسیاری از شبکه‌های سنتی، سلسله‌مراتبی است که با استفاده از گره‌هایی از سوییچ‌های اترنت در یک ساختار

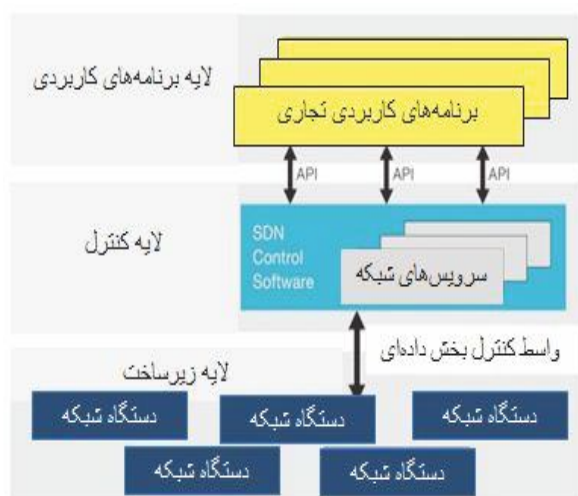
استفاده از شبکه‌های نرم‌افزار^۱محور سبب انعطاف‌پذیری و برنامه‌پذیر شدن^۲ شبکه می‌شود. با استفاده از این گونه شبکه‌ها می‌توان همه جوانب شبکه را از تنظیمات سطح پایین گرفته تا ایجاد تسهیلات مدیریت شبکه، مدیریت ترافیک و خطایابی را به‌صورت نرم‌افزاری و بهینه انجام داد. این نوع شبکه‌ها روش‌های جدیدی برای حل مسایل قدیمی شبکه مانند مسیریابی^[۱] و کنترل ازدحام را ارایه می‌دهند. همچنین اجازه استفاده از روش‌هایی چون کنترل دسترسی و مقابله با حملات سایبری را فراهم می‌سازند. در این مقاله، ابتدا تهدیدهایی را که می‌توانند از آسیب‌پذیری‌های شبکه‌های نرم‌افزارمحور استفاده کنند، برشمرد، سپس به

¹Software defined networks

²Programmability

* نویسنده عهده‌دار مکاتبات

بستر بین جریان‌های مختلف، به اشتراک گذاشته می‌شود. این ویژگی سبب افزایش بهره‌وری از منابع شبکه برای مدیریت ارتباطات متعدد به‌ویژه در مراکز داده کنونی می‌شود [۴]. با در نظر گرفتن نیازمندی‌های دیگر همچون قابلیت برنامه‌ریزی شبکه مطابق خواسته‌های کاربران، امکان دسترسی به داده‌های توزیع‌شده، مدیریت جامع و یکپارچه و افزایش میزان گسترش‌پذیری شبکه، لزوم اصلاح ساختار شبکه‌های سنتی و ارائه یک معماری جدید، به‌طور کامل مشهود است.



(شکل-۱): معماری شبکه SDN [۵]

با توجه به این مقدمات، معماری SDN بر اساس ایده جداسازی منطق نرم‌افزاری بستر کنترلی از بستر سخت‌افزاری انتقال داده‌ها شکل گرفته است. در شبکه‌های نرم‌افزارمحور سوییچ‌ها بسته‌های ورودی را مورد پردازش قرار نمی‌دهند؛ بلکه برای تطبیق بسته‌های ورودی به جداول جریان مراجعه می‌کنند و اگر تطبیقی بین رکوردهای جدول و بسته ورودی نیافتند، بسته را برای پردازش به بررسی‌کننده ارسال خواهند کرد. در واقع بررسی‌کننده، یک سیستم عامل در شبکه‌های SDN است که بسته‌های دریافتی را پردازش کرده و در مورد بسته‌ها طبق قوانین موجود تصمیم‌گیری می‌کند؛ به عبارت دیگر در این شبکه‌ها ارسال و پردازش‌ها از یکدیگر جدا شده‌اند. همان‌گونه که در شکل (۱) نیز قابل مشاهده است؛ کنترل‌کننده اصلی سامانه به صورت یک واحد متمرکز از بستر انتقال داده، جدا شده و نرم‌افزارها در لایه بالایی و بستر ارتباطی شبکه در لایه زیرین قرار گرفته‌اند و

درختی شکل می‌گیرد. این معماری بر پایه ارتباطات مدل کارخواه/کارگزار^۱ شکل گرفته است؛ اما چنین معماری ایستایی، برای ارتباطات پویا و نیازهای شرکت‌ها در زمینه مراکز داده و رسانه‌های کارگزار، کافی نیست [۲]. مواجهه با نیازهای کنونی بازار با استفاده از معماری‌های متداول شبکه تقریباً غیرممکن است. شرکت‌های فناوری اطلاعات، برای رویارویی با مسائلی نظیر رکود یا کاهش بودجه از ابزارهای مدیریتی در سطح ماشین و پردازش‌های دستی بهره می‌گیرند. شرکت‌های کارگزار مخابراتی نیز با چالش‌های مشابهی روبه‌رو هستند؛ چرا که تقاضا برای دسترسی به پهنای باند شبکه‌های پویا رو به افزایش چشم‌گیری است؛ در عین حال، با افزایش هزینه‌های مربوط به تجهیزات مرکزی و کاهش درآمد، سود این شرکت‌ها به خطر می‌افتد. معماری شبکه‌های موجود، به گونه‌ای طراحی نشده‌اند که نیازهای کنونی شرکت‌ها، کارگزارهای مخابراتی و کاربران را برطرف کنند؛ به عبارت دیگر، طراحان شبکه با محدودیت‌هایی مانند: پیچیدگی، سیاست‌های متناقض، فقدان مقیاس‌پذیری و وابستگی به سخت‌افزار، وجود نداشتن هماهنگی بین نیازهای بازار و قابلیت‌های شبکه مواجه هستند که این عوامل صنعت IT را به سوی نقطه انحرافی می‌کشاند. برای جلوگیری از چنین رخدادی، صنعت شبکه مجبور به بازنگری این ساختارهای سنتی شده است. بر همین اساس و با پیشگامی بنیاد شبکه‌های باز^۲، سعی شده است که با مطرح کردن مفهوم شبکه‌های نرم‌افزارمحور، معماری جدیدی برای شبکه‌ها ارائه شود که بتواند حد قابل قبولی از این نیازها را در نسل جدید سامانه‌های مبتنی بر شبکه پوشش دهد [۳].

اگر بخواهیم به‌طور دقیق‌تر دلیل اصلی احساس نیاز به SDN را بررسی کنیم، بایستی گفت که انگیزه اصلی در این تغییرات، تحقق ویژگی مجازی‌سازی شبکه بوده است. بر اساس این ویژگی، تعدادی شبکه مجازی متمایز با سازوکارهای نشانی‌دهی و هدایت بسته متفاوت، می‌توانند یک بستر ارتباط فیزیکی یکسان را به اشتراک گذاشته و از آن استفاده کنند. یکی از کارآمدترین روش‌های نیل به این هدف، استفاده از قابلیت‌های نرم‌افزار است؛ به گونه‌ای که نرم‌افزارهای مختلف با منطق‌های خاص خود، هر یک هدایت بسته‌های یک جریان متناظر را در کنار سایر جریان‌های ارتباطی در بستر فیزیکی بر عهده می‌گیرند؛ در واقع این

² Open Networking Foundation

¹ Client/server

معماری SDN در عرصه شبکه، تغییرات بنیادی ایجاد کرده که در جامعه حوزه شبکه جنب و جوش زیادی را به راه انداخته است. ظهور شبکه‌های نرم‌افزارمحور، کسب و کار و حاشیه سود فروش سخت‌افزاری بسیاری از شرکت‌های بزرگ را تحت تأثیر قرار داده است. در سال‌های ۲۰۰۷ تا ۲۰۱۰ مدیران شرکت‌های بزرگ، مزایا و قابلیت‌های شبکه‌های نرم‌افزارمحور و پروتکل Open Flow را انکار می‌کردند و حذف مسیریاب‌ها و سویچ‌ها را غیرممکن می‌دانستند. با تشکیل بنیاد ONF و عضویت شش شرکت بزرگ صنعت شبکه در این بنیاد و فعالیت شرکت‌های نوپا در عرصه SDN، کم‌کم شرکت‌های بزرگ، شبکه‌های نرم‌افزارمحور را به‌عنوان یک تهدید جدی شناختند و برای پیشگامی در این معماری نوظهور اقداماتی را انجام دادند. در ادامه رویکردهای شرکت سیسکو و شرکت ماکروسافت در زمینه شبکه‌های نرم‌افزارمحور بیان می‌شود.

۳-۱- رویکرد شرکت سیسکو در زمینه SDN

شرکت سیسکو در سال ۲۰۱۱ تغییرات زیادی را در رویکرد خود اعمال و همچنین به عضویت بنیاد ONF پیوست. این شرکت شروع به راه‌اندازهای شبکه نرم‌افزار محور، مراکز داده مجازی، شبکه‌های مجازی و... کرد. درواقع سیسکو به‌جای ارائه محصولات بیشتر، به فکر ارائه راهکار و معماری برای کل شبکه‌های نرم‌افزارمحور بود و موجب ایجاد یکپارچگی شد. سیسکو در سال ۲۰۱۲ معماری و راهکار مختص شبکه‌های نرم‌افزارمحور را با نام ONE معرفی کرد. در این معماری علاوه بر Open Flow از پروتکل Open Stack نیز استفاده می‌شود. شرکت سیسکو در سال ۲۰۱۳ سخت‌افزارهای مختص شبکه نرم‌افزارمحور مانند سویچ‌های مجازی، سری جدید سویچ‌های قدرتمند^۳ و بسترهای جدید مراکز داده^۴ را معرفی کرد که همگی مبتنی بر معماری ONE با قابلیت‌های نرم‌افزاری و برنامه‌پذیری بودند. شکل (۲) نمونه‌ای از سویچ‌های جدید Catalyst 6800 را نشان می‌دهد.



(شکل-۲): سویچ Catalyst 6800 سیسکو

^۳ Catalyst 6800

^۴ Nexus7700, Insiem

لایه کنترل ارتباط مابین برنامه‌های کاربردی بخش بالا و دستگاه‌های قسمت پایین معماری را فراهم می‌کند. درواقع لایه کنترل، بررسی‌کننده شبکه است. بررسی‌کننده نمای متمرکز شبکه را حفظ می‌کند و از طریق رابط‌های باز به برنامه‌های کاربردی اجازه کنترل اصول زیربنایی شبکه را می‌دهد. در این معماری جزییات لایه پایینی از دید نرم‌افزارهای لایه بالاتر، پنهان شده است [۵]. این ویژگی سبب می‌شود که سازمان‌های بزرگ و توسعه‌دهندگان زیرساخت شبکه ضمن افزایش قابلیت گسترش‌پذیری و انعطاف‌پذیری شبکه، بتوانند با برنامه‌ریزی، ساختار شبکه را مطابق با نیازمندی‌ها اصلاح و به‌روزرسانی کنند.

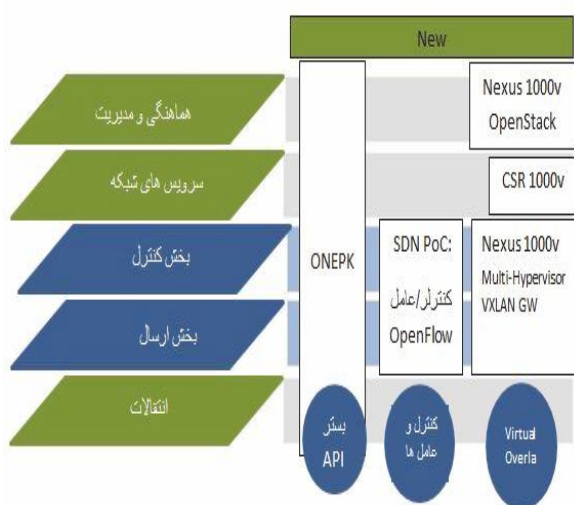
راهبری توسعه SDN‌ها و تدوین استانداردهای مربوطه بر عهده بنیاد شبکه‌های باز^۱ است که یک شکل غیرانتفاعی است. از جمله مشهورترین استانداردهای تدوین‌شده توسط این بنیاد، پروتکل Open Flow است که چگونگی برقراری ارتباط بین بستر کنترلی و بستر ارتباطی تجهیزات مورد نیاز در SDN را تبیین می‌کند. این استاندارد درحقیقت نخستین استاندارد است که خاص این‌گونه شبکه‌ها تعریف شده و ضمن ارایه کارایی مطلوب، توانسته سازندگان متفاوت را قادر به ارایه محصولات هماهنگ کند. مزایای این پروتکل عبارتند از: الف) مدیریت متمرکز و همگون ادوات با نشان‌های تجاری متفاوت ب) مخفی‌سازی جزییات بستر فیزیکی ارتباط از دید مدیریت شبکه ج) افزایش سرعت توسعه سرویس‌های شبکه بدون نیاز به پیکربندی جداگانه ادوات شبکه و یا تأمین تجهیزات جدید با قابلیت‌های به‌روزشده د) امکان برنامه‌ریزی کل مجموعه شبکه با استفاده از محیط‌های توسعه نرم‌افزار شناخته‌شده به‌منظور تأمین نیازهای خاص هر شبکه ه) قابلیت اطمینان و امنیت بیشتر شبکه به دلیل مدیریت متمرکز و هماهنگ که احتمال بروز رخنه‌های امنیتی و خطاهای پیکربندی را کاهش می‌دهد. و) امکان کنترل شبکه در سطوح مختلف راهبری، کاربری و... ی) افزایش کیفیت سرویس‌دهی از دید کاربران نهایی به واسطه تمرکز و یکپارچگی اطلاعات مربوط به هر ارتباط [۵].

۳- رویکرد شرکت‌های بزرگ درخصوص شبکه‌های نرم‌افزارمحور

^۱ Open Networking Foundation

^۲ Open Network Environment

عامل و تجهیزات شبکه است. شکل (۴) نمایی از این ابزار را در راهکار ONE نشان می‌دهد. بسیاری از شرکت‌هایی که محصولاتی را برای شبکه‌های نرم‌افزارمحور توسعه دادند، فقط به ارایه یک بررسی‌کننده مرکزی یا پیاده‌سازی یک شبکه هم‌پوشان^۳ اکتفا کردند؛ ولی شرکت سیسکو معماری کاملی براساس شبکه‌های نرم‌افزارمحور برای مشتریان خود ارایه کرده است تا با استفاده از آن و ابزارهای سخت‌افزاری و نرم‌افزاری ارایه‌شده توسط خود سیسکو از جمله سویچ 1000v بتوانند شبکه SDN خود را بسازند [۷].



(شکل-۴): ONEPK چارچوبی برای برنامه‌نویسی شبکه‌های

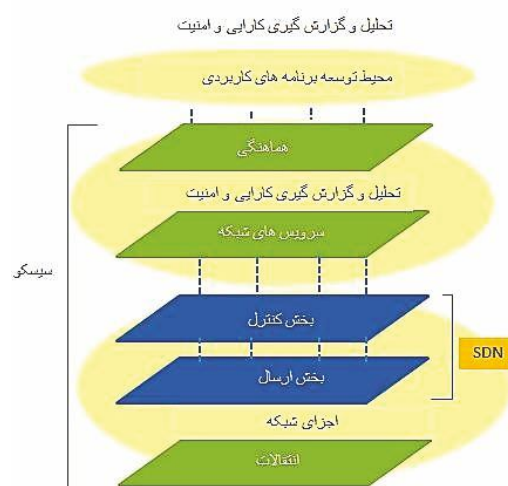
[۷] SDN

۲-۳- رویکرد شرکت مایکروسافت در زمینه SDN

سال‌های پیش، نقش شرکت مایکروسافت در مراکز داده و شبکه‌های گسترده، تولید ویندوز بود که سود بسیار ناچیزی نسبت به شرکت‌های تولیدکننده سخت‌افزار داشت. با ظهور شبکه‌های نرم‌افزارمحور فرصت مناسبی برای شرکت مایکروسافت ایجاد شد. مایکروسافت یکی از شش شرکت مؤسس بنیاد ONF است که نتایج همراهی با این بنیاد در ویندوز ۲۰۱۲ و بستر مجازی‌سازی اختصاصی مایکروسافت و ابزارهای مدیریت ماشین مجازی (VMM) نمود پیدا کرد. طبق اظهارات مایکروسافت، راهکارها و ابزارهایی که این شرکت فراهم آورده، یک بستر باز و عمومی قابل توسعه و منعطف برای ساخت هر نوع شبکه مبتنی بر شبکه‌های

³ Overlay

معماری ONE یک چارچوب^۱ برای هوشمندسازی شبکه‌ها است. این چارچوب انواع رویکردهای شبکه نرم‌افزارمحور مانند واسط‌های برنامه‌نویسی و بررسی‌کننده‌ها را در اختیار کاربر قرار می‌دهد تا با استفاده از آن‌ها امکانات و قابلیت‌های بیشتری از جمله قابلیت‌های زیرساختی، سادگی عملیات و داشتن چشم‌انداز وسیع‌تر نسبت به شبکه را ایجاد کند و همچنین به مدیران شبکه اجازه می‌دهد استانداردهای صنعتی، پروتکل‌ها و ملزومات شبکه خود را بر اساس نیاز و مدل سازمان خود انتخاب و پیاده‌سازی کنند و به‌مرور زمان نیز با استفاده از بازخوردها و نظرات مشتریان و کاربران اقدام به سفارشی‌سازی و بازسازی شبکه کنند [۶]. معماری ONE را در شکل (۳) می‌بینید.



(شکل-۳): معماری ONE سیسکو مبتنی بر شبکه‌های

نرم‌افزارمحور [۷]

ONEPK^۲ جعبه‌ابزاری ارایه‌شده توسط شرکت سیسکو برای به‌کارگیری چارچوب ONE و SDN است که می‌تواند حرکت به سوی شبکه‌های نرم‌افزارمحور را سرعت بخشد. با استفاده از این جعبه‌ابزار می‌توان نوآوری، برنامه‌پذیری مسیرپای‌ها و سویچ‌ها، و خودکارسازی را روی بستر شبکه به‌وجود آورد. این ابزار درواقع بستر اختصاصی سیسکو برای برنامه‌نویسی شبکه‌های نرم‌افزارمحور است که این محیط توسعه از زبان‌های برنامه‌نویسی جاوا، پایتون و C پشتیبانی می‌کند. زیرساخت این بستر روی انواع سیستم عامل‌های سیسکو قرار گرفته که در واقع رابط مابین سیستم

¹ Framework

² ONE Platform Kit

نیاز خود را روی ویندوز سرور ۲۰۱۲ نصب و پیکربندی کنند [۱۰].

۴- چالش‌های امنیتی در شبکه‌های نرم‌افزارمحور

شبکه‌های نرم‌افزارمحور برای حل مسایل سنتی شبکه‌ها نظیر کنترل ازدحام، مهندسی ترافیک و مسیریابی و توازن بار راهکارهای نرم‌افزاری و خلاقانه‌ای ارائه می‌دهند [۱] و در عین حال امکان اعمال سیاست‌های شبکه‌ای پیچیده‌ای مانند کنترل دسترسی، تشخیص و مقابله با نفوذ و قابلیت اطمینان را فراهم می‌کنند. به‌عنوان مثال در شبکه ایتین^۳ [۱۱] معماری شبکه‌های نرم‌افزارمحور به مدیران اجازه می‌دهد تا سیاست‌های کنترل دسترسی ریزدانه‌ای را در سطح شبکه به کار گیرند. به‌عنوان مثال در [۱۲] یک هسته‌ی اعمال امنیت در کنترلرهای شبکه‌های نرم‌افزارمحور به‌منظور اولویت‌بندی مسایل امنیتی ارائه شده است. با توسعه این ایده در [۱۳] چارچوبی به‌منظور توسعه و نصب برنامه‌های امنیتی در شبکه‌های نرم‌افزارمحور معرفی شده است. از آنجایی‌که بسیاری از سوییچ‌های شبکه امروزه از پروتکل Open Flow [۱۴] پشتیبانی می‌کنند؛ این فناوری در بسیاری از شبکه‌های صنعتی به کار گرفته شده است. بنابراین، امنیت این نوع شبکه‌ها به یک نگرانی جدی در صنعت تبدیل شده است [۱۵]، [۱۶]. علت اصلی این نگرانی به مزایای شبکه‌های نرم‌افزاری مربوط می‌شود. به عبارت دیگر قابلیت برنامه‌ریزی شبکه و تمرکز منطقی کنترل هم مزیت هستند و هم می‌توانند چالش امنیتی ایجاد کنند. درواقع این قابلیت‌ها راه را برای تهدیدهای جدید که درقبل وجود نداشت و یا بهره‌برداری از آنها مشکل بود، باز می‌کنند. شبکه‌های سنتی یک محافظت طبیعی و ذاتی در مقابل آسیب‌پذیری‌های معمول سیستم‌های IT دارند. این محافظت طبیعی ریشه در ماهیت بسته‌ها و دستگاه‌های انحصاری، طراحی ایستا، ناهمگونی نرم‌افزارها و توزیع‌شدگی کنترل دارد که سبب دفاع در مقابل تهدیدها معمول می‌شود. برای مثال یک حمله یا تهدید که از آسیب‌پذیری یک دستگاه خاص مربوط به یک تولیدکننده استفاده می‌کند، به‌احتمال فقط به بخش خاصی از شبکه که دارای آن دستگاه است، می‌تواند ضرر برساند. تنوع دستگاه‌ها و ادوات شبکه به‌نسبت شبکه‌های معمولی در شبکه‌های نرم‌افزارمحور کمتر است، زیرا دستگاه‌های مورد

نرم‌افزارمحور را فراهم می‌کند که با استفاده از این ابزارها می‌توان یک شبکه نرم‌افزارمحور کامل را ایجاد کرد.

Hyper-V مهم‌ترین ابزار مایکروسافت برای شبکه‌های نرم‌افزارمحور است. این بستر مجازی‌سازی، اجازه می‌دهد انواع شبکه‌های مجازی، ماشین‌های مجازی را روی یک شبکه فیزیکی تعریف، پیکربندی و سیاست‌های شبکه‌های نرم‌افزارمحور را روی آن‌ها اعمال کرد. این ابزار با ساختن شبکه‌های مجازی چندمستأجره^۱ روی یک شبکه فیزیکی مشترک، امکان انعطاف‌پذیری بیشتر شبکه را فراهم می‌کند. Hyper-V روی هر میزبان می‌تواند سیاست‌های شبکه‌های نرم‌افزارمحور را به‌صورت پویا به هر شبکه مستأجر اختصاص دهد تا ترافیک شبکه براساس این سیاست‌ها به سوی مقصد هدایت شود. [۸]

VMM^۲ ابزار دیگر مایکروسافت برای به‌کارگیری شبکه‌های نرم‌افزارمحور است. این ابزار کلید اصلی پیکربندی خودکار شبکه‌های نرم‌افزارمحور بر روی Hyper-V است. با استفاده از VMM می‌توان شبکه‌های مجازی چندمستأجره را بدون نیاز به پیکربندی شبکه فیزیکی، تعریف کرد. کاربران با استفاده از VMM می‌توانند سوییچ‌های مجازی مختلفی مطابق نیازها و مشخصات شبکه مجازی روی هر یک از میزبان‌های Hyper-V تعریف کنند و برای هر سوییچ مجازی چندین ماشین مجازی مرتبط با آن را بسازند. این ابزار با نظارت بارکاری^۳ ماشین‌های مجازی و تغییر سیاست‌های مبتنی بر شبکه‌های نرم‌افزارمحور بر روی میزبان‌ها، بالاترین کارایی و مقیاس‌پذیری را در شبکه‌های مجازی و مراکز داده به‌وجود می‌آورد [۹].

ویندوز سرور ۲۰۱۲ جزء دیگری از راهکار SDN مایکروسافت است که این شرکت با ارائه ویندوز سرور ۲۰۱۲ بستر لازم برای ایجاد شبکه‌های نرم‌افزارمحور را کامل کرد. این سیستم عامل ارتباط بین بخش‌های Hyper-V و VMM را با سیستم مرکزی برقرار می‌کند و توسعه SDN را توسط سازمان‌ها و شرکت‌ها امکان‌پذیر می‌سازد. در ویندوز ۲۰۱۲ می‌توان سوییچ‌های مجازی قابل توسعه با بالاترین هماهنگی و یکپارچگی با شبکه‌های فیزیکی را ایجاد کرد. سازمان‌ها در استفاده از این سیستم عامل محدودیتی ندارند و می‌توانند افزونه‌های برنامه‌نویسی مورد

^۳ workload

^۴ Ethane

^۱ Multi-tenant Virtual Network

^۲ Virtual Machine Manager

استفاده در شبکه‌های نرم‌افزارمحور هر چند از تولیدکنندگان مختلف باشند، از استاندارد و ساختار یکسانی بر مبنای پروتکل Open Flow استفاده می‌کنند. به عبارت دیگر، میزان ریسک در پیاده‌سازی‌های پروتکل و نرم‌افزار کنترلی سازگار، افزایش می‌یابد. به عنوان مثال حمله‌ای مانند استاکس نت^۱ [۱۷] به عنوان یک کرم هدفمند که تنها ساختار شبکه‌ای خاص را هدف قرار می‌دهد، می‌تواند در شبکه‌های نرم‌افزارمحور صدها دستگاه را با تغییر برنامه کنترلی از کار بیندازد و نتایج بسیار بدی را در این نوع شبکه قابل تنظیم و قابل برنامه‌ریزی به بار آورد. بسیار محتمل است که چنین حملات هدفمندی که تهدیدهای پایدار پیشرفته [۱۸] نامیده می‌شوند برای مقابله با شبکه‌های نرم‌افزارمحور توسعه داده شوند. بنابراین، اگرچه شبکه‌های نرم‌افزارمحور تحولی شگرف در معماری شبکه‌ها به وجود آورده است، اما سطح تهدید^۲ را به شکل خطرناکی افزایش می‌دهند. ما باید با حفظ مزایای این نوع شبکه‌ها درصدد دفع خطرات سایبری آن بایسیم. البته مقابله با این تهدیدها بایستی هم با ارایه راهکارهای امنیتی و تنظیمات مناسب و هم به صورت ساختاری در طراحی آنها در نظر گرفته شود که این دو مکمل هم هستند. شبکه‌های نرم‌افزارمحور دو ویژگی زیر را دارند که در صورتی که مدیران شبکه آمادگی لازم برای مقابله با آنها را ایجاد نکرده باشند، می‌توانند شبکه را به محلی ناامن برای نفوذ کاربران خرابکار^۳ تبدیل کند: ویژگی نخست، توانایی کنترل شبکه به وسیله نرم‌افزار است که نرم‌افزار همیشه منبع اشکالات و آسیب‌پذیری‌هاست. ویژگی دوم، تمرکز هوش و توانایی شبکه در بررسی‌کننده است؛ یعنی هر شخصی با دسترسی و تسلط به کارگزارهایی که محل قرارگیری بررسی‌کننده هستند، ممکن است کل شبکه را به دست گیرد. در ادامه برخی از حملات که ممکن است شبکه‌های نرم‌افزارمحور را تهدید کند، معرفی می‌کنیم.

۴-۱- حملات منع خدمت در شبکه‌های

نرم‌افزارمحور

حمله منع خدمت جزء جدی‌ترین تهدیدهاست چون بر روی کارایی شبکه، افزایش تأخیر و دور ریختن بسته‌های مشروع تأثیر می‌گذارند. این حملات ممکن است تمام شبکه را فلج یا عملکرد آن را متوقف کنند. برای شبکه‌های بر مبنای Open Flow حملات منع خدمت می‌تواند بسیار مخرب‌تر باشد؛ زیرا

در این شبکه‌ها یک جریان مداوم بین بررسی‌کننده و سویچ‌ها وجود دارد. ارتباط مداوم بین سویچ و بررسی‌کننده ممکن است مهاجمان را تحریک کند تا جریان بین بررسی‌کننده و سویچ را خارج کرده و فعالیت معمول شبکه را مختل سازند. برخی از حملات منع خدمت موجب تغییر حجم ترافیک می‌شود. تمایز اصلی در حملات منع خدمت اندازه وسیع ترافیک است. روش‌های شناسایی اندازه وسیع ترافیک، معمول‌ترین روش‌ها برای شناسایی این حملات است. برای پیشبرد حملات منع خدمت در شبکه‌های نرم‌افزارمحور، مهاجمان ممکن است حجم زیادی از ترافیک با مشخصه‌های تصادفی متغیر با استفاده از مولدهای ترافیکی ایجاد کنند تا هر جریان که از منظر سویچ‌ها جدید است بسته‌های آن جریان برای تصمیم‌گیری، به سمت بررسی‌کننده فرستاده شود. چنین حملاتی می‌تواند دو هدف زیر را داشته باشد. هدف نخست اشباع جداول سویچ‌ها با قوانین غیر مشروع است که این امر می‌تواند قابلیت سویچ‌ها را برای پذیرش قوانین جدید مختل سازد. هدف دوم مهاجمان از فرستادن چنین حجم انبوه جریان این است که سیل عظیم جریان‌ها، کنترل را مشغول سازد تا از پاسخ به جریان‌های مشروع و سویچ‌ها بازمانده و از کار بیفتد. روش‌های رمزنگاری قوی و قابل اعتماد می‌تواند در ایمن‌سازی ارتباطات انحصاری بین بررسی‌کننده و سویچ‌ها یاری‌رسان باشد [۱۳]. با این حال این روش نیز نمی‌تواند از حملات منع خدمت که از طرف میزبان‌هایی که ترافیک را به شبکه‌های Open Flow هدایت می‌کنند، جلوگیری کند. اگرچه برخی مطالعات بیان داشته‌اند که شبکه‌های Open Flow نسبت به شبکه‌های سنتی با حملات منع خدمت مشکلات بیشتری داشته‌اند، اما در [۱۹] نشان دادند که شبکه‌های نرم‌افزارمحور می‌تواند راه بهتری برای کنترل RTBH^۴ فراهم کند. مولی و همکارانش در [۲۰] یک سازوکار چند دفاعی را در برابر حملات منع خدمت ارایه دادند که ارایه محتوای شبکه از طریق کنترلر SDN کنترل می‌شود. دایو و همکارانش نیز در [۲۱] یک فناوری فیلترکردن IP براساس منبع را برای مقابله با این حملات در SDN ارایه کردند.

۴-۲- حمله جعل هویت در شبکه‌های

نرم‌افزارمحور

³ Malicious users

⁴ Remote Triggered Black Hole

¹ Stuxnet

² Threat surface

همچنین می‌توانند جدول جریان یا قوانین حفاظ^۶ را تزریق کرده تا موجب رد کردن میزبان‌های قانونی یا موجب ورود میزبان‌های غیرقانونی شوند. همچنین مهاجمان ممکن است سعی در دست‌کاری اطلاعات توپولوژی را داشته باشند که متعاقباً منجر به ربوده شدن بخشی از ترافیک شوند. در SDN جلوگیری از حملات دست‌کاری به دلیل ماهیت ساختاری بسیار حایز اهمیت است [۲۴]. SDN برای جلوگیری از دست‌کاری غیرعمدی می‌تواند بسیار کارآمد باشد. زیرا در این شبکه، بسته‌ها می‌توانند پیش از رفتن به مسیر مقصد به منظور تعیین صحت ویژگی مشخصه‌ها مورد بررسی قرار گیرند. به عبارتی در این شبکه‌ها دست‌کاری با استفاده از بازرسی توزیعی و نظارت در نقاط مختلف شبکه کاهش اثر داده می‌شود. برای مقابله با دست‌کاری بررسی‌کننده بایستی به طور مرتب روش‌های رمزنگاری را بررسی کرده و اتصالات را از نظر مشروعیت مورد ارزیابی قرار داد.

۴-۴- ارتقای امتیاز^۸ در شبکه‌های نرم‌افزارمحور

هنگام ورود به سامانه، مهاجمان سعی می‌کنند تا امتیازات دسترسی خود را افزایش داده تا به منابع و کاربردهایی که به مجوز ویژه مورد نیاز است، دسترسی پیدا کنند. شناسایی حملات ارتقای امتیاز نیاز به یک فرایند بازرسی هوشمند و توانمند دارد. از آنجاکه امتیازها در ماژول‌های کنترل دسترسی یا ماژول‌های کنترل مجوز گماشته می‌شوند، حملات تشدید اغلب این ماژول‌ها را هدف قرار داده و سعی می‌کنند تا اطلاعات آنها را دست‌کاری کنند. علاوه بر این، بسیاری از حملات فعلی، تهاجم خود را توسط حمله به یک کاربرد مشروع و مصالحه آن شروع می‌کند و سامانه‌هایی با سطوح مجوزهای محدود و ساده که تنها شامل دو یا سه سطح مجوز باشند نسبت به این حمله بیشتر آسیب پذیرتر خواهند بود.

۵- دسته‌بندی تهدیدها در شبکه‌های نرم‌افزارمحور

در این بخش، هفت بردار تهدید^۹ ممکن را که در شبکه‌های نرم‌افزارمحور شناسایی شده‌اند با توجه به شکل (۵) توصیف

جعل هویت^۱ به فرایندی اطلاق می‌شود که در آن اطلاعات شبکه به صورت عمدی تغییر شکل داده شده تا هویت واقعی شناسه ترافیک و یا مهاجم پنهان شود. برای مثال، کاربران ممکن است از نشانی IPهای جعلی برای دستیابی به منابع شبکه استفاده کنند. جعل هویت اغلب بخشی از یک حمله بزرگ‌تر است و نشانی‌های جعلی ممکن است بخشی از یک شبکه بات^۲ یا شبکه زامبی به منظور اجرای حملات منع خدمت توزیع شده باشد [۲۲]. در حال حاضر تهدید جعل هویت در شبکه‌های نرم‌افزارمحور بیش‌تر شامل جعل پروتکل تجزیه و تحلیل نشانی^۳ (ARP) و جعل IP است.

۴-۲-۱- جعل پروتکل تجزیه و تحلیل نشانی

جعل ARP شامل اتصال نشانی MAC یک مهاجم به یک نشانی IP مشروع است. حمله جعل ARP می‌تواند موجب ربوده شدن ترافیک از دریافت‌کننده هدف شود که به دنبال آن یک کاربر یا میزبان قانونی در شبکه از کار می‌افتد. در شبکه‌های Open Flow امکان مسمومیت ARP بین بررسی‌کننده و سوئیچ‌ها وجود خواهد داشت [۲۳].

۴-۲-۲- جعل IP

جعل IP به طور معمول به عنوان دریچه‌ای برای دیگر حملات از جمله دست‌کاری^۴ یا تقویت DNS^۵ به کارگرفته می‌شود. DNS در واقع یک فهرست راهنما^۶ است که نشانی IP را به نام دامنه مربوط می‌سازد. به منظور تغییر مسیر ترافیک به سمت پایگاه‌های وب غیرمشروع، یک مهاجم می‌تواند فهرست راهنما DNS را دست‌کاری کند. چیزی که به طور معمول در تمامی حملات جعل حضور دارد این است که همه آنها سعی در تغییر مسیر ترافیک به سمت میزبان‌های غیرمشروع دارند. آنها همچنین می‌توانند به عنوان تلاشی برای دستیابی به حملات فرد در میانه تلقی شوند.

۴-۳- حمله دست‌کاری در شبکه‌های نرم‌افزارمحور

دست‌کاری شامل تغییرات غیرمجاز و یا تخریب اطلاعات شبکه همانند توپولوژی جریان‌ها در جدول جریان، سیاست‌ها و فهرست‌های دسترسی است. برای مثال یک مهاجم ممکن است سعی در تزریق قوانین جریان را داشته باشد که منجر به ناهنجاری در رفتار شبکه خواهد شد. آنها

⁶ directory

⁷ firewall

⁸ Elevation of privilege

⁹ threat vector

¹ Spoofing

² Botnet

³ Address Resolution Protocol

⁴ Tampering

⁵ Domain Name System

تجهیزات شبکه می تواند برای مقابله با این نوع تهدیدات مفید باشند.

بردار تهدید سوم، حملات به ارتباطات لایه کنترل شبکه های نرم افزارمحور است که می تواند به منظور ایجاد حمله منع خدمت یا سرقت داده انجام شود. در شبکه های نرم افزارمحور از ارتباط امن بر مبنای TLS/SSL به منظور ارتباط کنترلی امن بین سویچ ها و بررسی کننده استفاده می شود؛ اما همان طور که در دنیای امنیت شناخته شده است، این نوع اتصال تضمین کننده ارتباط امن بین بررسی کننده و دستگاه های شبکه نیست و سبب ممانعت از سرقت اطلاعات نمی شود. پژوهش های متعددی ضعف ارتباطات بر مبنای پروتکل های TLS/SSL و همچنین نقطه قوت آن یعنی زیرساخت کلید همگانی^۴ (PKI) را گزارش کرده اند [۲۷].

توان امنیتی این ارتباطات به اندازه ضعیف ترین جزء آن است که این جزء می تواند یک مجوز امضا شده، یک مرجع صدور گواهی^۵ CA مورد حمله قرار گرفته و یا یک برنامه یا کتابخانه برنامه نویسی آسیب پذیر باشد. برای مثال پیاده سازی های زیادی از SSL آسیب پذیر به حمله فرد در میانه^۵ در سامانه های حساس در سطح دنیا در حال استفاده است [۲۸]. علاوه بر این مدل TLS/SSL برای برقراری و اطمینان از اعتماد بین بررسی کننده و سویچ، کافی نیست. زمانی که یک مهاجم، دسترسی به لایه کنترلی را داشته باشد، توان لازم را به منظور اجرای حملات منع خدمت توزیع شده به واسطه سویچ های تحت نظر بررسی کننده خواهد داشت. این خلأ اعتماد حتی می تواند سبب ایجاد یک سیاه چاله مجازی به منظور جذب و نشت داده ها به وجود آورد. استفاده از اعتماد چندگانه به نحوی که هر زیردامنه یا هر بررسی کننده یک مرجع صدور گواهی مربوط به خود را داشته باشد، یکی از راه حل های احتمالی است. راه حل دیگر، امن سازی ارتباطات با رمزنگاری آستانه ای در سطح بررسی کننده های تکرار شده است [۲۹]؛ به طوری که یک سویچ به منظور دریافت یک پیام معتبر نیازمند دریافت n بخش اشتراکی از جانب بررسی کننده است.

خواهیم کرد [۲۵]. در این شکل بخش های آسیب پذیر یک شبکه نرم افزارمحور با توجه به بردارهای تهدید مربوطه شماره گذاری شده اند. البته هدف از بیان این مشکلات، این نیست که بگوییم شبکه های نرم افزارمحور ذاتاً ناامن تر از شبکه های فعلی هستند. نکته مهم این است که شبکه های نرم افزارمحور تهدیدهایی با ماهیت متفاوت دارند که نیازمند ارزیابی راهکارهای متفاوتی نیز هستند. در صورتی که یک شبکه نرم افزارمحور به خوبی طراحی و نصب شود، نه تنها از نظر توانایی های عملیاتی بلکه از نظر دوام در مقابل تهدیدهای سایبری، یک پیشرفت قابل توجه محسوب می شود.

بردار تهدید اول در رابطه با جریان ترافیک جعلی و ساختگی است که می تواند به منظور حمله به سویچ ها یا بررسی کننده ها به کار رود. این تهدید می تواند غیر عمدی و به وسیله یک دستگاه خراب و یا به صورت عمدی توسط یک کاربر خراب کار انجام شود. مهاجم می تواند با استفاده از عناصر مختلف شبکه مانند سویچ ها، کارگزارها یا رایانه های شخصی یک حمله منع خدمت^۱ را علیه سویچ های دیگر و یا بررسی کننده انجام دهد. با یک سازوکار احراز هویت ساده می توان از این مشکل جلوگیری کرد، اما در صورتی که مهاجم کنترل کارگزاری که اطلاعات کاربران را در اختیار دارد به دست آورد، می تواند با استفاده از نشانی سخت افزاری مبدأ اتصالات و پورت های احراز هویت شده، جریان مجاز اما جعلی را به شبکه تزریق کند. استفاده از یک سامانه تشخیص نفوذ^۲ با قابلیت تشخیص ترافیک غیر نرمال، یکی از راه حل های مقابله با این تهدید است. این راه حل می تواند با کنترل و پایش رفتار سویچ ها تکمیل شود. به عنوان مثال می توان حد بالایی برای نرخ درخواست های کنترلی سویچ ها در نظر گرفت.

بردار تهدیدی دوم، حملات با استفاده از آسیب پذیری های سویچ است. این حملات در یک سویچ می تواند با کند کردن حرکت بسته ها در شبکه موجب حذف آنها یا رونوشت کردن یا منحرف کردن ترافیک بسته ها به منظور سرقت داده ها یا حتی تزریق ترافیک و درخواست های جعلی به منظور overload کردن بررسی کننده شبکه و سویچ های مجاور به کار رود. راه حل نرم افزاری مانند مدیریت اعتماد برای اجزای نرم افزاری [۲۶] و سازوکارهایی به منظور نظارت و تشخیص رفتارهای غیر نرمال

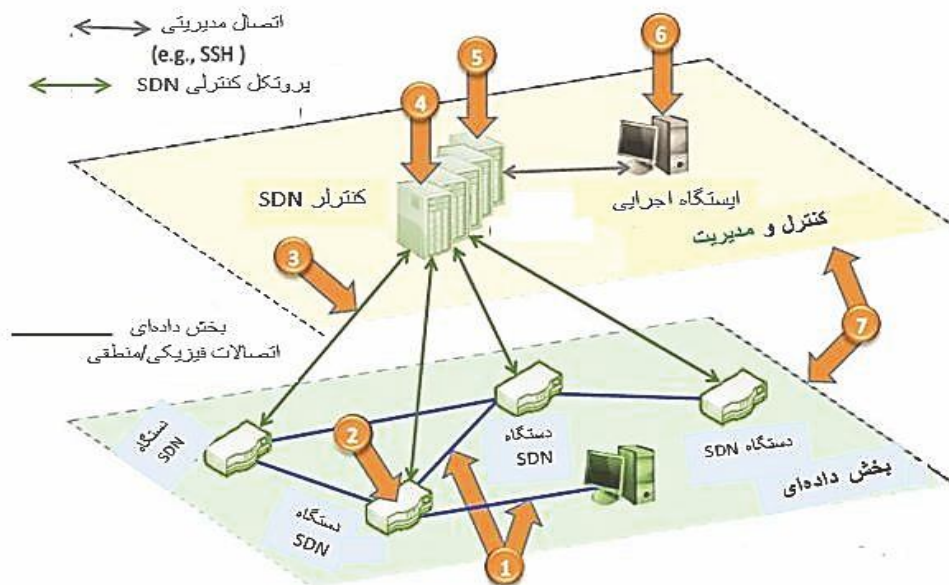
⁴ Certification Authority

⁵ man-in- the- middle- attacks

¹ Denial Of Service attack(DOS)

² Intrusion Detection System(IDS)

³ Public key infrastructure



(شکل-۵): نقشه بردارهای حملات در شبکه‌های نرم‌افزار محور [۲۵]

بردار تهدید ششم همانند شبکه‌های سنتی، حملات به آسیب پذیری‌های پایانه‌های مدیریتی^۲ است. این تهدید در شبکه‌های نرم‌افزارمحور، برای دسترسی به بررسی‌کننده انجام می‌شود. تفاوت در اینجا است که در شبکه‌های نرم‌افزارمحور، این حمله اثرات بسیار مخربی دارد؛ زیرا به جای یک یا چند پایانه اجرایی، کل شبکه با احاطه بر بررسی‌کننده می‌تواند در اختیار مهاجم قرار گیرد. همچنین مهاجم می‌تواند کل شبکه را دوباره از طریق بررسی‌کننده برنامه‌ریزی کند. راه حل‌های ممکن در اینجا استفاده از پروتکل‌هایی است که نیاز به واریسی اعتبار دوطرفه دارند. همچنین استفاده از سازوکارهایی برای بازیابی، سبب می‌شود که پس از راه اندازی مجدد، سیستم به حالت درست و قابل اطمینانی بازگردانده شود.

بردار تهدید هفتم، فقدان منابع قابل اعتماد برای تشخیص مقابله و بازیابی امن است. به‌منظور شناسایی حقایق در مورد یک رخداد امنیتی، نیازمند اطلاعات قابل اعتماد از همه اجزا و دامنه‌های شبکه هستیم و علاوه بر این، داده‌ها در صورتی مفید خواهند بود که از اعتماد به آن‌ها از نظر صحت و مجازبودن بتوان اطمینان حاصل کرد. مقابله و حل مشکل، نیازمند اطلاعات لحظه‌ای، مطمئن و قابل اعتمادی است که بازیابی سریع و درست عناصر شبکه‌ای را به یک حالت درست تضمین می‌کند. راه حل از طریق آزمایش و نظارت سازوکارهای معمول در لایه‌های داده و

بردار تهدید چهارم، شامل حملات به آسیب‌پذیری‌های بررسی‌کننده است که به احتمال جدی‌ترین نوع تهدید به شبکه‌های نرم‌افزار محور است. یک بررسی‌کننده مخرب می‌تواند تمام شبکه را تحت تأثیر قرار دهد. استفاده از سامانه تشخیص نفوذ ممکن است به تنهایی کافی نباشد؛ زیرا روش‌های تشخیص نفوذ بر اساس الگو عمل می‌کنند و پیداکردن الگوی واقعی منجر به واکنشی خاص می‌شود و همچنین مشخص کردن یک الگو به عنوان مخرب کار دشواری است. راه حل‌های ممکن استفاده از تکرار بررسی‌کننده‌ها به منظور تشخیص و حذف رفتار غیرنرمال، بهره‌گیری از گوناگونی^۱ در کنترلرها، پروتکل‌ها، زبان‌های برنامه‌نویسی و...، بازیابی دوره‌ای سامانه به منظور بردن آن به یک وضعیت شفاف و قابل اعتماد و همچنین امن‌سازی عناصر داخلی کنترلر مانند کلیدهای رمزنگاری هستند. علاوه بر این‌ها سیاست‌های امنیتی و قوانینی که برای برنامه‌سازی شبکه استفاده می‌شود، می‌توانند مؤثر باشند.

بردار تهدید پنجم، نیز همانند بردار تهدید سوم فقدان سازوکارها به منظور اعتماد بین بررسی‌کننده و برنامه‌های مدیریتی است. البته تفاوت آنها در این است که نوع تأیید تجهیزات با تأیید برنامه‌ها متفاوت است. راه حل آن وجود سازوکارهایی به منظور تضمین قابلیت اعتماد برنامه‌های مدیریتی در زمان حیات آن‌هاست.

² Administrative stations

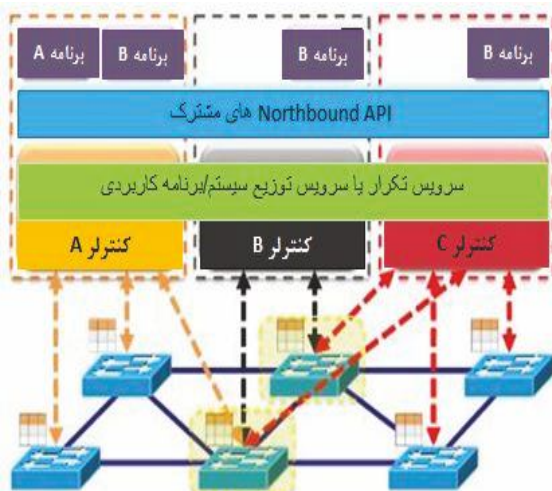
¹ Diversity

شوند. در این شکل، برنامه B نیز سه بار تکرار شده است. این روش ترکیبی، تحمل پذیری سخت افزار و نرم افزار را در مقابل حوادث و خراب کاری ها بیشتر می کند. به کمک تکرار می توان عیوب^۵ را پوشاند و برنامه یا بررسی کننده مشکل دار و یا مخرب را عایق^۶ کرد. در صورت از هم گسسته شدن شبکه، برنامه B می تواند به منظور برنامه ریزی کل سوییچ های شبکه به کار رود؛ ولی برنامه A که تکرار نشده است، قادر به اجرا نخواهد بود.

(جدول ۱): بردارهای تهدید شبکه های نرم افزار محور در مقابل

تهدیدهای عمومی شبکه ها [۲۵]

تهدیدات	مخصوص SDN	نتیجه در شبکه نرم افزار محور
بردار اول	خیر	میتواند راهی برای حملات منع خدمت باشد.
بردار دوم	خیر	تأثیر بالقوه ای آن افزایش یافته است.
بردار سوم	بله	ارتباطات با کنترل کننده متمرکز منطقی میتواند مورد سوء استفاده قرار گیرد.
بردار چهارم	بله	کنترل غیر مجاز کنترل کننده ممکن است کل شبکه را به خطر بیندازد.
بردار پنجم	بله	برنامه های مخرب میتوانند توسعه یافته و در کنترلر مستقر شوند.
بردار ششم	خیر	تأثیر بالقوه ای آن افزایش یافته است.
بردار هفتم	خیر	اطمینان از بازیابی سریع و تشخیص زود هنگام رخداد خطا بسیار مهم است.



(شکل ۶): معماری شبکه نرم افزار محور امن [۲۵]

کنترل است؛ اما برای اینکه مؤثر واقع شوند می بایست داده های مربوطه پاک نشدنی^۱ باشند و همچنین تضمین شود که غیرقابل تغییر و امن هستند. همچنین رخداد نماهای^۲ ثبت وقایع باید به صورت راه دور و در محیطی امن ذخیره شوند.

جدول (۱) هفت بردار تهدید توصیف شده بالا را جمع بندی کرده و همچنین وضعیت خاص بودن این حملات برای شبکه های نرم افزار محور را نشان می دهد. طبق این جدول، تهدیدهای شماره ۳ تا ۵ در شبکه های سنتی ظاهر نمی شوند و خاص شبکه های نرم افزار محور هستند. این تهدیدها ناشی از جداسازی لایه کنترل و لایه داده و نتیجه معرفی موجودیتی جدید در این شبکه ها یعنی "کنترلر منطقی متمرکز" هستند. تأثیر این حملات در شبکه های نرم افزار محور بیشتر بوده و به شکلی متفاوت بروز می کنند؛ بنابراین نیاز است که به نحو متفاوتی با آنها برخورد و مقابله شود. بررسی هفت بردار تهدید؛ نشان می دهد که گستره حملات^۳ در شبکه های نرم افزار محور نسبت به شبکه های سنتی بیشتر است و روش های مقابله ای متفاوتی را می طلبد. با توجه به این تهدیدهای می بایست امنیت و قابلیت اطمینان جزء نخستین مراحل طراحی این گونه شبکه ها باشد.

در بخش بعدی در مورد بستر بررسی امن و قابل اعتماد برای شبکه های نرم افزار محور به منظور مقابله با این تهدیدات می پردازیم.

۵-۱- بستر بررسی کننده امن و قابل اعتماد

برای شبکه های نرم افزار محور

در این بخش راه حل های مقابله ای لازم را برای بردارهای تهدید ۱ تا ۷ ارایه می کنیم. این راه حل ها در طراحی یک شبکه نرم افزار محور می بایست لحاظ شوند. شکل (۶) یک شکل ساده شده را از چنین طراحی نشان می دهد. در ادامه روش هایی به منظور مقابله با بردارهای تهدید شناسایی شده در شبکه های نرم افزار محور ارایه شده است.

تکرار^۴ یکی از فنون مهم بهبود قابلیت اعتماد سامانه های شبکه ای توزیع شده است [۳۰]. همان طور که در شکل ۶ دیده می شود، بررسی کننده با سه نمونه A، B و C تکرار شده است. همچنین برنامه های سطح شبکه نیز می توانند تکرار

⁴ Replication⁵ Fault⁶ Isolated¹ Indelible² Log³ Attack Surface

گوناگونی^۱ روش دیگری به‌منظور افزایش استحکام سامانه‌های امن است [۳۱]، [۳۲]. تکرار و گوناگونی بررسی‌کننده‌ها، یک انتخاب خوب برای افزایش امنیت است. اصل پشت سر این سازوکار، اجتناب از عیوب یکسان است که می‌توانند شامل اشکالات نرم‌افزاری^۲ یا انواع آسیب‌پذیری‌ها باشند. برای مثال می‌دانیم که سیستم‌عامل‌های موجود از خانواده‌های متفاوت، تعداد بسیار کمی آسیب‌پذیری مشترک دارند [۳۲] یعنی گوناگونی سیستم‌عامل‌ها تأثیر حملات روی آسیب‌پذیری‌های مشترک را کم می‌کند. در شبکه‌های نرم‌افزارمحور، یک برنامه‌مدیریتی می‌تواند روی کنترلرهای مختلف اجرا شود که این کار با تعریف یک واسط برنامه‌نویسی استاندارد و مشترک و یک تجرید مناسب در بخش بالایی شبکه نرم‌افزارمحور که محل اجرای برنامه‌های شبکه‌ای است، قابل انجام خواهد بود.

سازوکارهای خوددرمان‌کننده^۳، در شرایط مورد حمله قرارگرفتن طولانی؛ بازیابی پویا و واکنشی^۴ می‌تواند سامانه را به حالت درست برگردانده و اجزای آسیب دیده را جایگزین کند. جایگزینی بایستی با نسخه جدید و گوناگونی اجزا صورت گیرد که این مسئله توان دفاع را در مقابل حملاتی که آسیب‌پذیری‌های مشخصی هدف قرار می‌دهند، افزایش می‌دهد.

تخصیص پویای تجهیزات^۵، یکی دیگر از راه‌کارهای امن‌سازی شبکه‌های نرم‌افزارمحور است. اگر یک سویچ فقط به یک بررسی‌کننده نسبت داده شود، لایه کنترل آن تحمل‌پذیری لازم در مقابل عیوب و حملات را نخواهد داشت. زمانی که بررسی‌کننده مربوطه خراب شود، عملیات کنترلی سویچ از کار می‌افتد. بنابراین نیاز است که این سویچ به‌صورت پویا و امن به چند بررسی‌کننده متصل باشد. البته می‌بایست قابلیت‌هایی چون رمزنگاری آستانه‌ای به‌منظور تشخیص بررسی‌کننده خراب‌کار و همچنین احراز هویت بررسی‌کننده‌ها را برای جلوگیری از حمله فرد در میانه، در این راه‌کار لحاظ کرد. سویچی که به بررسی‌کننده‌های مختلفی می‌تواند وصل شود، به‌صورت خودکار در مقابل عیوب و حملات تحمل‌پذیر است. از جمله مزایای جانبی این قابلیت می‌توان به افزایش بازدهی (توازن بار به‌وسیله چند

بررسی‌کننده) و کاهش تأخیر (پاسخ‌گویی سریع چند بررسی‌کننده نسبت به بررسی‌کننده واحد) اشاره کرد [۳۳]. به‌منظور داشتن قابلیت اتصال به چند بررسی‌کننده و داشتن قابلیت‌های امنیتی مربوطه، نیاز است که قابلیت برنامه‌ریزی در سمت لایه داده (سویچ‌ها) با به‌کارگیری پردازنده مناسب، افزایش یابد.

اعتماد بین تجهیزات و بررسی‌کننده در امنیت شبکه‌های نرم‌افزارمحور بسیار مهم است. برقراری اعتماد بین دستگاه‌ها و بررسی‌کننده، یک نیازمندی مهم برای قابلیت اعتماد در لایه کنترلی است. اگرچه سویچ‌ها باید این اجازه را داشته باشند که به‌صورت پویا به کنترلرها متصل شوند، اما باید یک ارتباط قابل اعتماد وجود داشته باشد. یک راه حل در اینجا استفاده از فهرست سفید دستگاه‌های قابل اعتماد و مجاز در سمت بررسی‌کننده است؛ اما این راه‌کار انعطاف‌پذیری مطلوب را در شبکه‌های نرم‌افزارمحور ندارد. راه حل دیگر، اعتماد به همه سویچ‌هاست تا زمانی که غیر قابل اعتماد بودن آنها محرز شود. یک رفتار غیر نرمال یا مخرب از هر طرف ارتباط می‌تواند به‌وسیله سویچ یا بررسی‌کننده با استفاده از الگوریتم‌های تشخیص ناهنجاری یا تشخیص خرابی، شناسایی و گزارش شود. زمانی که میزان اعتماد سویچ یا بررسی‌کننده از یک حد آستانه‌ای مشخص و قابل قبول کمتر شود، سویچ به‌صورت خودکار، توسط همه دستگاه‌ها و بررسی‌کننده‌های دیگر، قرنطینه می‌شود.

اعتماد بین برنامه‌ها و نرم‌افزار بررسی‌کننده یکی دیگر از راه‌کارهای امنیتی است. با گذشت زمان مؤلفه‌های نرم‌افزار، قدیمی شده و اشکالاتی در آنها پدیدار می‌شود و یا مورد حمله قرار می‌گیرند. بنابراین یک مدل اعتماد پویا مانند آنچه در [۲۶] ارائه شده نیاز است. در این نوع مدل‌ها براساس ویژگی‌های مشاهده‌شده طرف مقابل مانند دسترس‌پذیری، قابلیت اتکا^۶، یک‌پارچگی، امنیت، قابلیت نگهداری و قابلیت اطمینان، میزان اعتماد مشاهده و اندازه‌گیری می‌شود. این مدل، اعتماد بین موجودیت‌های سامانه را تعریف و نظارت می‌کند.

دامنه‌های امنیتی مجزا^۷ روشی بسیار معمول است که در سامانه‌های مختلف استفاده می‌شود. برای مثال، در سیستم‌عامل‌ها برنامه‌های سطح کاربر اجازه دسترسی به

^۵ Dynamic device association

^۶ Reliability

^۷ Isolated security domains

^۱ Diversity

^۲ Software bugs

^۳ Self-healing

^۴ Proactive and reactive recovery

۶- توسعه نرم افزارهای امنیتی

برای مقابله با چالش‌های امنیتی علاوه بر داشتن یک معماری امنیتی مناسب و راه کارهای فهرست شده در جدول ۲، می‌بایست از قابلیت برنامه ریزی این شبکه‌ها نیز استفاده کرد. همان‌طور که در شکل (۷) دیده می‌شود، در بالاترین لایه یک شبکه نرم افزارمحور، با استفاده از توابعی که کنترلرها فراهم می‌کنند؛ می‌توان نرم افزارهایی را برای انجام کارهایی چون مدیریت ترافیک، توازن بار، مقابله با خرابی پیوند، نظارت امنیتی و غیره توسعه داد. همان‌طور که در قبل نیز گفته شد، ترافیک ناشناخته‌ای که به سویچ‌ها می‌رسد، برای تعیین تکلیف به بررسی کننده ارسال می‌شود. بسیاری از حمله‌ها در همین ترافیک ناشناخته پنهان هستند. بنابراین می‌توان نرم افزارهایی را هم برای مقابله با چالش‌های امنیتی، توسعه داده و بر روی بررسی کننده اجرا کرد تا مقابله با حملات شناخته شده و همچنین حملات جدید را بر عهده گیرند. شکل (۷) محل قرارگیری این برنامه‌های امنیتی را در کنار سایر اجزای یک شبکه نرم افزارمحور، نشان می‌دهد. همان‌طور که در بالاترین لایه این شکل دیده می‌شود، محیط حفاظ، کنترل دسترسی جریان، سامانه تشخیص نفوذ (IDS) در کنار سایر نرم افزارها با استفاده از توابع برنامه نویسی در بررسی کننده‌ها، به کار گرفته می‌شوند.

(جدول ۲-): راه حل‌هایی برای بردارهای تهدید [۲۵]

بردارهای تهدید	راه حل / سازوکار
۱،۴،۵،۷	تکرار
۳،۴،۶	گوناگونی
۲،۴،۶	خود درمانی
۳،۴	تخصیص پویای سویچ
۱،۲،۳	اعتماد بین کنترلر و دستگاه‌ها
۴،۵	اعتماد بین کنترلر و برنامه‌ها
۴،۵	دامنه‌های امنیتی
۴،۵،۷	مؤلفه های امن
۲،۴،۶	ترمیم و بروز رسانی سریع و امن

بخش‌های سطح هسته را ندارند. کرومیوم یک مثال خوبی برای طراحی دامنه‌های امنیتی مجزا است که بسیار کارآمد عمل می‌کند [۳۴]. کرومیوم از جعبه‌های شنی^۱ برای جداسازی موتور رندر از هسته مرورگر استفاده می‌کند. بنابراین در بسیاری از حمله‌ها که موتور رندر را تحت تأثیر قرار می‌دهند، هسته سیستم مصون خواهد ماند. دامنه‌ها یا محدوده‌های امنیتی در بستر کنترلی یک شبکه نرم افزارمحور می‌توانند به وسیله روش‌هایی چون استفاده از جعبه شنی و مجازی سازی ایجاد شوند. در این روش‌ها اجازه انجام عملیات و ارتباطات حداقلی بین دامنه‌های امنیتی داده می‌شود.

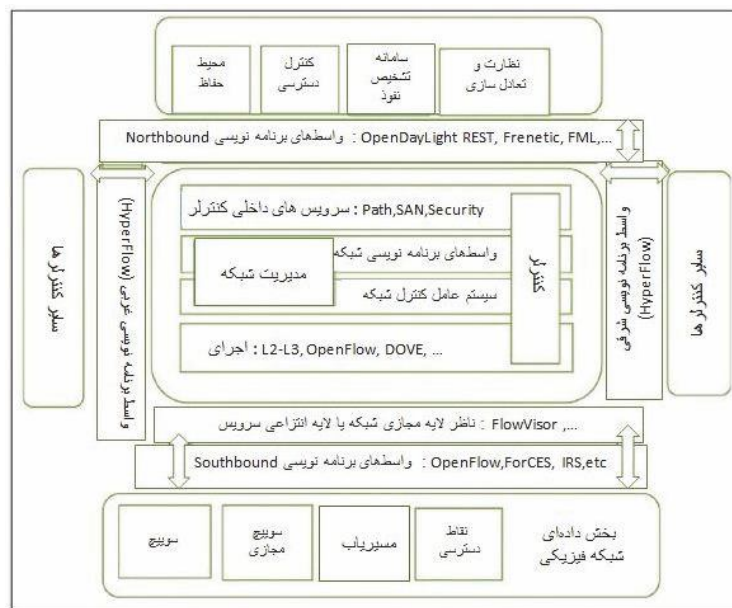
مؤلفه های امن^۲ یکی از بلوک‌های ساختاری لازم برای طراحی یک سامانه امن و قابل اعتماد را فراهم می‌کنند. این مؤلفه‌ها باید طوری باشند که در صورت تهاجم به سیستم، داده‌های حساس مانند کلیدهای رمزنگاری از دست نروند.

ترمیم و به روز رسانی پویا و امن نرم افزار، راه کار امنیتی دیگری است. از آنجایی که هیچ نرم افزاری بدون اشکال یا آسیب پذیری نیست، ترمیم و به روز رسانی برای کاهش اندازه پنجره آسیب پذیری (کاهش زمان وجود آسیب پذیری) لازم است. بنابراین بستر کنترلی باید سازوکارهایی به منظور اطمینان از روش‌های امن و منعطف به روز رسانی را فراهم آورد. راه حل‌هایی مانند آنچه در [۳۵] ارایه شده است، می‌تواند برای نیل به این هدف سودمند باشد. در جدول ۲ تهدیدهایی که به کمک هر راه حل و سازوکار، قابل مقابله هستند، مشخص شده‌اند [۲۵].

راه حل‌های ارایه شده در جدول ۲ سازوکارهای پایه‌ای لازم را به منظور طراحی و پیاده سازی یک بستر کنترلی امن و قابل اعتماد برای شبکه‌های نرم افزارمحور فراهم می‌آورند. این بستر امن می‌تواند از سازوکارهای سنتی مانند محیط حفاظ، سامانه تشخیص نفوذ و سایر ابزارها نیز استفاده کند [۳۶]. ابزارهای سنتی تأمین امنیت، در شبکه‌های نرم افزارمحور را می‌توان به صورت نرم افزاری پیاده سازی کرد و در قالب برنامه‌های تحت شبکه سازماندهی کرد.

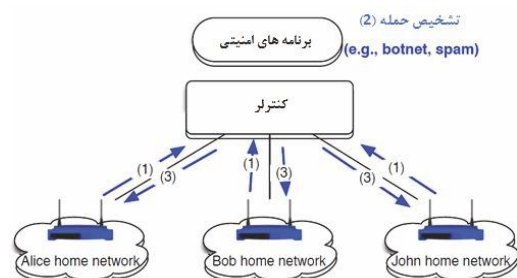
² Secure components

¹ Sandbox



(شکل-۷): معماری یک شبکه نرم‌افزارمحور به همراه برنامه‌های امنیتی [۲۳]

که توسط یک برنامه امنیتی، ترافیک شبکه را نظارت کرده و پس از تشخیص حمله، قوانین لازم برای مقابله با حمله را به جدول سوییچ اضافه کند.



(شکل-۸): به کارگیری شبکه‌های نرم‌افزارمحور برای مقابله با حملات در شبکه‌های خانگی

حفظ امنیت شبکه‌های ابری به دلیل وجود حملات از داخل ابر و همچنین پیکربندی پویای این گونه شبکه‌ها بسیار مشکل است. به کمک شبکه‌های نرم‌افزارمحور الگوریتم‌های جدیدی می‌توان توسعه داد که با استفاده از یک دستگاه نظارت کننده در درون ابر، امنیت آن را تا حدود زیادی برقرار کرد [۴۰]. در این الگوریتم مسیریابی نه تنها کوتاه‌ترین فاصله بین مبدأ و مقصد به دست می‌آید، بلکه کوتاه‌ترین فاصله این مسیر تا دستگاه نظارت کننده حملات نیز محاسبه می‌شود. برای مثال در شکل ۹ کوتاه‌ترین فاصله بین گره‌های S و E به دست آمده و سپس با استفاده از انعطاف‌پذیری شبکه‌های نرم‌افزارمحور، ترافیک در مسیریاب R6 رونوشت و به سمت مسیریاب R4

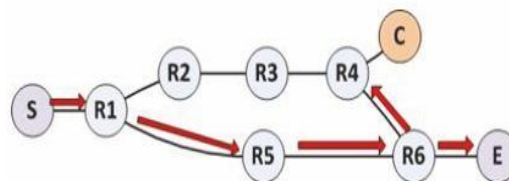
۷- امنیت به کمک شبکه‌های نرم‌افزارمحور

اگرچه شبکه‌های نرم‌افزارمحور با برخی چالش‌های امنیتی روبه‌رو هستند، اما خود این شبکه‌ها می‌توانند برای برقراری امنیت به کار روند. یکی از کاربردهای شبکه‌های نرم‌افزارمحور استفاده از آنها به منظور کنترل دسترسی جریان‌های داده است [۳۷]. این کنترل دسترسی در سطح ماشین‌های مجازی انجام می‌گیرد؛ به نحوی که قبل از ارسال داده از یک ماشین مجازی، یک بسته بررسی فرستاده، به وی پاسخ لازم را می‌دهد. بر اساس نوع پاسخ دریافتی، فرستنده بر حسب دسترسی خود می‌تواند عملیاتی را انجام دهد. جداسازی ترافیک شبکه‌های منطقی مختلف بر روی یک شبکه فیزیکی واحد، یکی دیگر از کاربردهای امنیتی شبکه‌های نرم‌افزارمحور است [۳۸] که محدودیت‌های شبکه‌های مجازی VLAN را ندارد. در این کاربرد، شبکه‌های مجازی اگرچه بر روی یک یا چند شبکه فیزیکی، قرار دارند؛ ولی از ترافیک ارسالی یکدیگر مطلع نمی‌شوند که در محرمانه‌نگه داشتن اطلاعات بسیار مؤثر می‌تواند باشد. حفظ امنیت دستگاه‌های مربوط به شبکه‌های خانگی^۱ توسط شبکه‌های نرم‌افزارمحور به‌صورتی کارا قابل انجام است [۳۹]. همان‌طور که در شکل ۸ مشاهده می‌شود، یک سوییچ شبکه نرم‌افزارمحور را می‌توان در یک نقطه دسترسی^۲ به‌صورت توکار به کار گرفت به‌نحوی

^۲ Access Point

^۱ Home networks

هدایت می‌شود. این مسیر یاب به یک دستگاه نظارت‌کننده امنیتی شبکه با نام C متصل است.



(شکل-۹): الگوریتم مسیریابی کوتاه‌ترین مسیرها [۴۰]

در اینجا کم‌ترین فاصل مسیری شناسایی شده تا مسیریاب متصل به دستگاه نظارت‌کننده، توسط الگوریتم مسیریابی به دست می‌آید. به این ترتیب حملات درونی شبکه‌های ابری توسط دستگاه نظارت‌کننده، قابل تشخیص خواهند بود. برای توسعه برنامه‌های امنیتی مختلف مانند محیط حفاظ نرم‌افزاری و تشخیص حملات منع خدمت و... در شبکه‌های نرم‌افزارمحور دانش زیادی لازم است. به منظور ساده‌سازی برنامه‌نویسی امنیتی در شبکه‌های نرم‌افزارمحور، بستری به نام Fresco توسعه داده شده است [۱۳]. این بستر یک محیط توسعه با امکان اشتراک پیام‌ها و منابع شبکه بین برنامه‌ها را به وجود می‌آورد. علاوه بر این امکاناتی را به منظور ایجاد برنامه‌های کنترل دسترسی جریان در شبکه‌های نرم‌افزارمحور فراهم می‌کند. همچنین در این محیط توسعه توابع پایه‌ای کنترل دسترسی جریان مانند مسدودسازی، ممانعت کردن، اجازه دادن، تغییر مسیر دادن و قرنطینه کردن جریان‌های شبکه‌ای، فراهم شده است.

کاربردی^۲ می‌تواند در راستای توسعه، آموزش و پژوهش استفاده شود. این شبیه‌ساز محیطی را فراهم می‌کند که به کمک آن می‌توان توپولوژی دلخواه یک شبکه نرم‌افزارمحور را به صورت گرافیکی شبیه‌سازی کرد و کل شبکه را در یک رایانه واحد در اختیار داشت. علاوه بر این، می‌توان کلیه قابلیت‌ها و تنظیمات انجام‌شده بر روی شبکه نرم‌افزارمحور شبیه‌سازی شده را بدون هیچ تغییری در یک شبکه واقعی به کار گرفت.

حمله منع خدمت توزیع‌شده، یکی از مرسوم‌ترین حملات بوده که همان‌طور که در قبل گفته شد، تشخیص و مقابله با آن در شبکه‌های نرم‌افزارمحور اهمیت خاصی دارد. ما به منظور آزمایش امنیتی شبکه‌های نرم‌افزارمحور از شبیه‌ساز مینی نت استفاده خواهیم کرد و تأثیرات حمله منع خدمت توزیع‌شده را بر روی این شبکه مورد بررسی قرار می‌دهیم. به منظور بررسی تأثیرات حمله منع خدمت توزیع‌شده در شبکه‌های نرم‌افزارمحور، توپولوژی با ۱۳ سوئیچ و ۸۴ میزبان در مینی نت ایجاد کرده و از بررسی‌کننده Ryu که کامل‌ترین بررسی‌کننده برای شبکه‌های نرم‌افزارمحور است [۴۲] استفاده می‌کنیم. به کمک ابزار Scapy از یک نود خارج از شبکه نرم‌افزارمحور ترافیک مصنوعی را با نشانی‌های مبدأ جعلی تولید کرده و به گره‌های هدف شبکه نرم‌افزارمحور ارسال می‌کنیم. مشخصات بسته‌های ترافیک تولیدی را در جدول ۳ می‌بینید.

(جدول-۳): مشخصات بسته‌های ترافیک حمله [۴۳]

نوع حمله	محتوی	شماره پورت مبدأ	نام پروتکل
منع خدمت توزیع شده	فاقد محتوی	۸۰	UDP

با توجه به این که درآمد بسته‌های ورودی وضعیت حمله با جداول موجود در سوئیچ‌ها مطابقتی ندارند، به عنوان بسته‌های جدید شناخته شده و برای تعیین تکلیف به بررسی‌کننده ارسال می‌شوند و به این ترتیب حجم زیادی از ترافیک به بررسی‌کننده روانه می‌شود.

به منظور نظارت بر ترافیک شبکه بین سوئیچ‌ها و بررسی‌کننده از ابزار Wireshark استفاده می‌کنیم. این نرم‌افزار یک تحلیل‌گر بسته در شبکه است و بسته‌هایی را که در شبکه رد و بدل

۸- شبیه‌سازی حمله منع خدمت توزیع شده

در شبکه‌های نرم‌افزارمحور

آزمایش نرم‌افزارها و راه‌کارهای جدید امنیتی در شبکه‌های نرم‌افزارمحور واقعی، زمان‌بر و پرهزینه هستند؛ بنابراین می‌توان از شبیه‌سازهای شبکه نرم‌افزارمحور برای آزمایش و بررسی‌های موردنظر استفاده کرد. شبیه‌ساز مینی نت^۱ به منظور آزمایش شبکه‌های نرم‌افزارمحور توسعه داده شده است [۴۱]. شبیه‌ساز مینی نت برنامه‌ای است که می‌تواند شبکه‌ای مجازی را ایجاد کرده و هسته‌های واقعی، کدهای برنامه و سوئیچ‌های شبکه را بر روی یک ماشین (ماشین مجازی، ابر یا سامانه واقعی) به اجرا درآورد. این نرم‌افزار به دلیل امکان تعامل‌پذیری توسط واسطه‌های برنامه‌نویسی

² application programming interface (API)

¹ Mininet

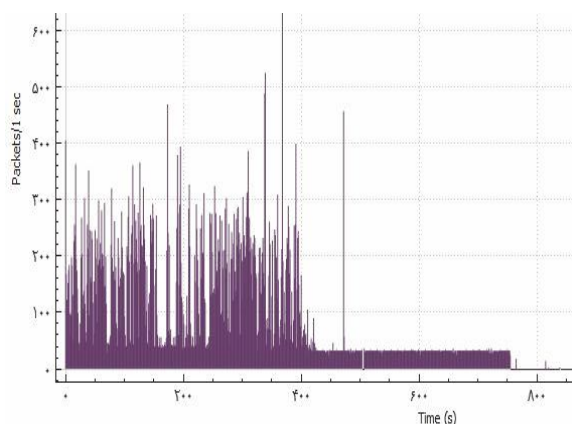
۹- جمع‌بندی

ما در این مقاله ضمن معرفی شبکه‌های نرم‌افزارمحور و مزایای آنها، چالش‌های امنیتی آنها را به‌صورت ساختاری معرفی کردیم و راه کارهای ارائه شده برای این چالش‌ها را مرور کردیم. این راه کارها را می‌توان به‌صورت عمده به دو گروه راه کارهایی بر اساس معماری امنیتی و راه کارهای نرم‌افزاری دسته‌بندی کرد. از طرف دیگر نمونه‌هایی از کاربردهای امنیتی شبکه‌های نرم‌افزارمحور را برشمردیم. باید به این نکته دقت شود که شبکه‌های نرم‌افزارمحور اگرچه در عمل در دنیا به کار گرفته شده است، اما پروتکل‌ها و ابزارهای مربوط به این شبکه‌ها در حال تغییر و تحول هستند. بنابراین هم‌زمان باید مسایل امنیتی مربوط به تغییرات پروتکل‌های آن را نیز در کنار تکامل قابلیت‌های عملیاتی، مدنظر قرار داد.

۱۰- منابع

- [1] Caesar, M., Caldwell, D., Feamster, N., Rexford, J., Shaikh, A., & van der Merwe, J. (2005, May). Design and implementation of a routing control platform. In *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2* (pp. 15-28). USENIX Association.
- [2] Hakiri, A., Gokhale, A., Berthou, P., Schmidt, D. C., & Gayraud, T. (2014). Software-defined networking: Challenges and research opportunities for future internet. *Computer Networks*, 75, 453-471.
- [3] Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1), 14-76.
- [4] Chowdhury, N. M, and Raouf Boutaba, "Network virtualization: state of the art and research challenges" *Communications Magazine*, IEEE 47, (2009), no.7, 20-26.
- [5] Fundation, Open Networking. "Software-defined networking: The new norm for networks" ONF White Paper (2012), url: <https://www.opennetworking.org>
- [6] http://blogs.cisco.com/data_center/cisco-open-network-environment-explained, Access Date: October 2016.
- [7] http://www.theregister.co.uk/2012/06/14/cisco_one_sdn_openflow_openstack, Access Date: October 2016.
- [8] [https://technet.microsoft.com/enus/library/mt169373\(v=ws.11\).aspx](https://technet.microsoft.com/enus/library/mt169373(v=ws.11).aspx) (Access Date: October 2016).

می‌شوند، با دام انداختن آنها مورد پردازش قرار می‌دهد. یکی از قابلیت‌های خوب شبیه‌ساز مینی‌نت این است که به‌طور دقیق مانند یک شبکه واقعی به نظر می‌رسد، به‌طوری که Wireshark این تفاوت را متوجه نمی‌شود و با دادن نشانی‌های درونی شبکه شبیه‌سازی شده می‌توان ترافیک هر پیوند دلخواهی از شبکه را نظارت کرد. گراف حاصل از پایش ترافیک بررسی کننده توسط این ابزار را در شکل ۱۰ می‌بینید.



(شکل-۱۰): گراف حاصل از شبیه‌سازی حمله منع خدمت توزیع شده

همان‌طور که در گراف شکل ۱۰ مشاهده می‌شود، در طول حمله منع خدمت توزیع شده راه‌اندازی شده در شبکه، بسته‌های زیادی به سمت بررسی کننده ارسال شده است. به‌طور تقریبی در ثانیه ۳۹۱ عملکرد بررسی کننده به دلیل کمبود منابع، مختل شده و به‌طور تقریبی در ثانیه ۷۴۸ بررسی کننده به‌طور کامل از کار افتاده است. در طول شبیه‌سازی میزان مصرف CPU و حافظه و پهنای باند نیز بررسی شده است که نتایج را در جدول ۴ مشاهده می‌کنید. طبق نتایج حاصل از این بررسی، مهاجم با تزریق مداوم بسته‌های جعلی، پردازش سنگینی را برای کنترلر ایجاد می‌کند که این امر موجب اشغال پهنای باند در کانال سوئیچ- بررسی کننده می‌شود. با توجه به منابع محدود بررسی کننده قادر به پاسخ‌گویی ترافیک عادی شبکه نخواهد بود و در نتیجه از دسترس خارج می‌شود [۴۴].

(جدول-۴): نتایج بررسی میزان مصرف CPU و حافظه

وضعیت شبکه	مصرف CPU	پهنای باند	مصرف حافظه
وضعیت عادی	۳۱٪	۱,۳ G	۸۱ Mb
وضعیت حمله	۱۰۰٪	۰,۳ G	۳۰۸ Mb

- [22] Yao, G., Bi, J., & Xiao, P. (2011, October). Source address validation solution with OpenFlow/NOX architecture. In *2011 19th IEEE International Conference on Network Protocols* (pp. 7-12). IEEE.
- [23] Alsmadi, I., & Xu, D. (2015). Security of software defined networks: A survey. *computers & security*, 53, 79-108.
- [24] Othman, O. M., & Okamura, K. (2013). Securing distributed control of software defined networks. *International Journal of Computer Science and Network Security (IJCSNS)*, 13(9), 5.
- [25] Kreutz, D., Ramos, F., & Verissimo, P. (2013, August). Towards secure and dependable software-defined networks. In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking* (pp. 55-60). ACM.
- [26] Yan, Z., & Prehofer, C. (2011). Autonomic trust management for a component-based software system. *IEEE Transactions on Dependable and Secure Computing*, 8(6), 810-823.
- [27] Holz, R., Riedmaier, T., Kammenhuber, N., & Carle, G. (2012, September). X. 509 Forensics: Detecting and Localising the SSL/TLS Men-in-the-middle. In *European Symposium on Research in Computer Security* (pp. 217-234). Springer Berlin Heidelberg.
- [28] Georgiev, M., Iyengar, S., Jana, S., Anubhai, R., Boneh, D., & Shmatikov, V. (2012, October). The most dangerous code in the world: validating SSL certificates in non-browser software. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 38-49). ACM.
- [29] Y. G. Desmedt, "Threshold cryptography", In: *European Transactions on Telecommunications* 5.4 (1994).
- [30] Andrew S. Tanenbaum, "Modern Operating Systems", Pearson; 4 edition, 2014.
- [31] S. Neti, A. Somayaji, and M. E. Locasto, "Software diversity: Security, Entropy and Game Theory", In: 7th USENIX HotSec, 2012.
- [32] M. Garcia et al, "Analysis of operating system diversity for intrusion tolerance", In: *Software Practice and Experience* (2013).
- [33] B. Heller, R. Sherwood, and N. McKeown, "The controller placement problem", In: *HotSDN*. ACM, 2012.
- [34] A. Barth et al, "The Security Architecture of the Chromium Browser", Tech. rep. Stanford University, (2008).
- [35] J. H. Perkins et al, "Automatically patching errors in deployed software", In: *ACM SIGOPS SOSP*, 2009.
- [9] [https://technet.microsoft.com/enus/library/gg610610\(v=sc.12\).aspx](https://technet.microsoft.com/enus/library/gg610610(v=sc.12).aspx) (Access Date: October 2016).
- [10] <https://www.microsoft.com/en/servercloud/products/windows-server-2012-r2/> (Access Date: October 2016).
- [11] Casado, M., Freedman, M. J., Pettit, J., Luo, J., Gude, N., McKeown, N., & Shenker, S. (2009). Rethinking enterprise network control. *IEEE/ACM Transactions on Networking (ToN)*, 17(4), 1270-1283.
- [12] Porras, P., Shin, S., Yegneswaran, V., Fong, M., Tyson, M., & Gu, G. (2012, August). A security enforcement kernel for OpenFlow networks. In *Proceedings of the first workshop on Hot topics in software defined networks* (pp. 121-126). ACM.
- [13] Shin, S., Porras, P. A., Yegneswaran, V., Fong, M. W., Gu, G., & Tyson, M. (2013, February). FRESKO: Modular Composable Security Services for Software-Defined Networks. In *NDSS*.
- [14] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., ... & Turner, J. (2008). OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2), 69-74.
- [15] S. Sorensen, "Security implications of software-defined networks", (2012), url: <http://goo.gl/BiXH2>.
- [16] S. M. Kerner, "Is SDN Secure?" (2013), url: <http://goo.gl/IPn2V>.
- [17] D. Kushner, "The Real Story of Stuxnet", (2013). url: <http://goo.gl/HIEHQ>.
- [18] Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network security*, 2011(8), 16-19.
- [19] Yuzawa Tamihiro, "OpenFlow 1.0 actual use case: RTBH of DDoS traffic while keeping the target", (2013). Online, <http://packetpushers.net/open-flow-1-0-actual-use-case-rtbh-ofddos-traffic-while-keeping-the-target-online>.
- [20] Mowla, N. I., Doh, I., & Chae, K. (2014, July). Multi-defense Mechanism against DDoS in SDN Based CDNi. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2014 Eighth International Conference on* (pp. 447-451). IEEE.
- [21] Dao, N. N., Park, J., Park, M., & Cho, S. (2015, January). A feasible method to combat against DDoS attack in SDN network. In *2015 International Conference on Information Networking (ICOIN)* (pp. 309-311). IEEE.

امنیت فضای سایبر است و دارای مقالات متعددی در مجلات و کنفرانس‌های معتبر ملی و بین‌المللی است. نامبرده در پروژه‌های پژوهشی و صنعتی متعددی مشارکت داشته است.



مژگان قصابی مدرک کارشناسی را در رشته فناوری اطلاعات با کسب رتبه نخست از دانشگاه زنجان اخذ کرده و اکنون دانشجوی دوره کارشناسی ارشد رشته فناوری اطلاعات گرایش شبکه‌های رایانه‌ای در دانشگاه علوم تحقیقات تهران می‌باشد که در دوره کارشناسی ارشد نیز در دو نیمسال تحصیلی، رتبه نخست را کسب کرده است. از جمله زمینه‌های پژوهشی مورد علاقه وی می‌توان به امنیت شبکه‌های نرم‌افزارمحور، محاسبات فراگیر، محاسبات ابری و سیستم‌های خبره اشاره کرد.

- [36] N. Foster et al, "Frenetic: a network programming language", In: SIGPLAN Not, 2011.
- [37] Lucian Popa, Minlan Yu, Steven Y. Ko, Sylvia Ratnasamy, "CloudPolice: taking access control out of the network", Ion Stoica HotNET, 2010.
- [38] A. Blenk, A. Basta, M. Reisslein, & W. Kellerer. Survey on Network Virtualization Hypervisors for Software Defined Networking. arXiv preprint arXiv:1506.07275, 2015.
- [39] S. Sundaresan, S. Burnett, N. Feamster, & W. De Donato. BISmark: A testbed for deploying measurements and applications in broadband access networks. In 2014 USENIX Annual Technical Conference (USENIX ATC 14). (2014), pp. 383-394.
- [40] Seungwon Shin, Guofei Gu, "CloudWatcher: Network Security Monitoring Using Openflow In Dynamic Cloud Networks" 20th IEEE International Conference on Network Protocols, 2012.
- [41] Lantz, Bob, Brandon Heller, and Nick McKeown, "A network in a laptop: rapid prototyping for software-defined networks", In Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, ACM, (2010), p-19.
- [42] R. Khondoker, A. Zaalouk, R. Marx, & K. Bayarou. Feature-based comparison and selection of Software Defined Networking (SDN) controllers. In Computer Applications and Information Systems (WCCAIS), 2014 World Congress on. (2014), pp. 1-7.
- [43] Seyed Mohammad Mousavi and Marc St Hilaire, "Early Detection of DDoS Attacks against SDN Controllers", International Conference on Computing, Networking and Communications, Communications and Information Security Symposium, (2015) pp. 10-15
- [44] Zhang, J., Qin, Z., Ou, L., Jiang, P., Liu, J., & Liu, A. X. (2010, October). An advanced entropy-based DDOS detection scheme. In *2010 International Conference on Information, Networking and Automation (ICINA)* (Vol. 2, pp. V2-67). IEEE.



محمود دی‌پیر مدرک دکترای خود را در رشته کامپیوتر-سامانه‌های نرم‌افزاری و مدرک کارشناسی ارشد خود را در رشته کامپیوتر-نرم‌افزار هر دو از دانشگاه شیراز دریافت کرده است. مقطع کارشناسی خود را نیز در همین رشته از دانشگاه هوایی شهید ستاری دریافت کرده است. ایشان هم‌اکنون عضو هیئت علمی دانشکده رایانه و فناوری اطلاعات دانشگاه هوایی شهید ستاری است. زمینه‌های پژوهشی وی شامل داده‌کاوی و

