تاریخ دریافت مقاله: ۹۶/۰۵/۱۷
تاریخ پذیرش مقاله: ۹۶/۰۹/۱۲

بررسی حملات رد خدمت توزیع شده در شبکه‌های مبتنی بر نرم‌افزار

مژگان قصابی
دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات تهران، گروه کامپیوتر، تهران، ایران
پست الکترونیکی: mozhgan.ghasabi@srbiau.ac.ir

محمود دی‌پیر*
استادیار دانشکده رایانه و فناوری اطلاعات، دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران
پست الکترونیکی:mdeypir@ssau.ac.ir

چکیده

حملات رد خدمت توزیع شـده یکی از تهدیدات اصلی هر شـبکه‌ای می‌باشد. با توجه به افزایش دانش مهاجمان، شناسـایی و مسدودسـازی چنین حملاتی بسیار دشوار شـده اسـت. شـبکه‌های مبتنی بر نرم‌افزار یک معماری نوظهور برای شـبکه‌های ارتباطی اسـت. این معماری با جداسـازی عملکرد کنترل از بخش داده‌ای شبکه تا حدود زیادی مدیریت شـبکه را سـاده‌تر کرده است. شبکه‌های مبتنی بر نرم‌افزار برخی ویژگی‌های خاص از جمله کنترل متمرکز، برنامه‌پذیری، به‌روزرسانی پویای قوانین و تجزیه و تحلیل جریان‌های ترافیکی را دارا می‌باشند. این قابلیت‌ها این معماری را در شناسـایی آسـان و واکنش سـریع به حملات رد خدمت توزیع شـده توانمند می‌سازد. ما در این مقاله مطالعه جامعی را در زمینه معماری شبکه‌های مبتنی بر نرم‌افزار و مشخصات حملات رد خدمت توزیع شده در این معماری انجام داده‌ایم. ما روش‌های راه‌اندازی حملات رد خدمت توزیع شـده در شبکه‌های مبتنی بر نرم‌افزار را مطالعه کرده، سپس سازوکارهای دفاعی ارائه شده مبتنی بر معماری شـبکه‌های نرم‌افزار را بررسـی کردیم. نتایج مطالعات انجام شده نشان داد که این معماری فرصت‌های جدیدی را برای شکسـت حملات رد خدمت توزیع شده به ارمغان می‌آورد.

واژگان کلیدی: شـبکه‌های مبتنی بر نرم‌افزار، حملات رد خدمت توزیع شـده، سازوکارهای دفاعی، کنترل کننده متمرکز.

۱- مقدمه

شـبکه‌های مبتنی بر نرم‌افزار(SDN)[1] یک معماری نوید بخش برای شبکه‌های کامپیوتری است[۱]. در این معماری عملکرد کنترل از بخش سـوئیچ‌های شبکه جدا شده و در کنترل کننده، متمرکز شده است[۲]. جداسازی بخش کنترل از بخش انتقال داده‌ای، شـبکه‌های مبتنی بر نرم‌افزار را به یک معمـاری مطلوب برای طراحی و مدیریت شـبکه‌های بزرگ تبدیل کرده اسـت. در ایـن معماری بخش کنترل و بخـش انتقال از طریق کانال امن در ارتباط می‌باشـند[۳]. بـرای ایجاد ارتباط امن بین بخش داده و بخش کنترل نیاز بـه برخی پروتکل‌های خاص اسـت. به مجموعه قوانین و قراردادهایـی که بین فرسـتنده و گیرنده تنظیم می‌شـود تا بتوانند با همدیگر ارتباط داشـته باشـند، پروتکل گفته می‌شود. پروتکل OpenFlow یک استاندارد واسط ارتباطی

* نویسندهٔ مسئول

1- Software Defined Vetwork

است که در این معماری بین سطوح کنترل و انتقال تعریف می‌شود. این پروتکل سوییچ‌ها را در شبکه، مدیریت کرده و اجازه می‌دهد کنتـــرل کننده به‌عنوان موجودیت خارجی جریان بسته‌ها را از طریق شبکه اداره نماید[٤].

در ســـاختار معماری شـــبکه‌های مبتنی بـــر نرم‌افزار، دستگاه‌های شـــبکه از جمله سوئیچ‌ها و مسیریاب‌ها، فقط مســـئولیت ارسال بسته‌ها بر اســـاس قوانین بخش کنترل کننـــده متمرکز را برعهـــده دارند. در این شـــبکه‌ها بخش کنترل کننده به‌عنوان مغز این معماری، اطلاعات سوئیچ‌ها و مســـیریاب‌ها را پردازش کرده و برای پیکربندی شـــبکه تصمیـــم گیری می‌کنـــد و قوانین مربوط بـــه نحوه هدایت بسته‌ها را به دستگاه‌های موجود در مسیر ارسال می‌نماید. دستگاه‌های شبکه، دارای چندین جدول جریان می‌باشند که این جداول، اطلاعات و قوانین مربوط به ورودی‌ها را حفظ می‌کنند[٥].

در این شـــبکه‌ها به‌طور کلی در دو حالت پیش‌دستانه[٢] و حالت واکنشـــی[٣] قوانین در ســـوئیچ‌ها نصب می‌شوند. هنگام راه‌اندازی شـــبکه، کنترل کننده، سیاست‌های شبکه را بـــه قوانین جریان تجزیه کرده و آن‌ها را در ســـوئیچ‌ها نصـــب می‌کند که به این حالت نصب پیش‌دســـتانه قوانین گفته می‌شود. در حالت نصب قوانین واکنشی، کنترل کننده با پردازش درخواســـت‌ها، قوانین را در سوئیچ‌های شبکه نصب می‌کند [٢].

نصب قوانین پیش‌دستانه در این شبکه موجب می‌شود که کنترل کننده و سوئیچ‌های شبکه نسبت به حملات آسیب پذیر باشـــند. مهاجمان در شـــبکه‌های مبتنی بر نرم‌افزار می‌توانند با سوءاســـتفاده از ویژگی به‌روزرسانی پویای جداول، با ارســـال بسته‌های جعلی منابع شبکه را مشغول و موجب ســـرریز جداول گردند[٥]. ارســـال حجم انبوهی از بســـته‌های جعلی به سمت کنترل کننده توسط مهاجمان عواقـــب زیر را به دنبال خواهد داشـــت که منجر به کاهش عملکرد و در نهایت از کار افتادن شبکه می‌گردد[٢]:

- ابزار نرم‌افزاری سوئیچ‌ها دچار اضافه بار[٤] می‌شوند.
- کانال بین کنترل کننده و سوئیچ‌ها اشباع می‌گردد.
- منابع کنترل کننده اشباع می‌شوند.
- جـــداول جریان ســـخت‌افزاری ســـوئیچ‌ها ســـرریز می‌شوند.

سه اصل کلیدی امنیت هر شبکه‌ای عبارتند از[۶]:

- محرمانگـــی داده: ایـــن اطمینـــان را ایجـــاد می‌کند که اطلاعات خصوصی نباید در دسترس افراد غیر مجاز قرار گرفته یا فاش شود.
- جامعیت سیســـتم: این اطمینان را می‌دهد که سیستم عملیـــات مورد نظر خود را بدون نقص و عاری از تغییرات غیر مجاز عمدی انجام می‌دهد.
- دسترس پذیری: اطمینان می‌دهد که سیستم به درستی کار کرده و کاربران مجاز را از دسترسی به سرویس منع نمی‌کند.

بـــه فعالیـــت هوشـــمندانه بـــه منظـــور از بیـــن بردن ســـرویس‌های امنیتی و نقض سیاست امنیتی یک سیستم حمله گویند[٦]. یکی از تهدیدات جدی شـــبکه‌های مبتنی بر نرم‌افزار، حملات رد خدمت توزیع شده است که به صورت مستقیم بر کنترل کننده این شبکه‌ها تأثیر می‌گذارد. تهدید، خطری محتمل بوده که توســـط مهاجم با سوءاستفاده از آسیب پذیری‌ها موجب آســـیب به سیستم می‌شود. حمله رد خدمت نوعی تلاش برای نقض اصل دســـترس پذیری امنیتی سیستم می‌باشـــد که با پرکردن پهنای باند قربانی موجب مختل شدن دسترســـی کاربران مجاز به سرویس می‌گـــردد[٧]. حمله رد خدمتی که مهاجم از سیســـتم‌های زیـــادی به‌طور همزمان برای راه‌انـــدازی حملات علیه یک میزبـــان راه دور اســـتفاده کند، به‌عنـــوان حمله رد خدمت توزیع شده تلقی می‌شود.

محافظت از یک سیســـتم اطلاعاتی خودکار به منظور حفظ اصول امنیتی را دفـــاع گویند. هدف اصلی ما در این مقاله بررسی سازوکارهای دفاعی علیه حملات رد خدمت

2- proactive
3- reactive
4- overload

توزیع شـــده در شـــبکه‌های مبتنی بر نرم‌افزار است. برای رسیدن به این هدف، به بررسی ساختار معماری شبکه‌های مبتنی بر نرم‌افزار پرداخته و روش‌های راه‌اندازی حملات رد خدمت توزیع شده در این معماری را بررسی می‌کنیم. ســـپس با بیان ویژگی‌های معماری شـــبکه‌های مبتنی بر نرم‌افزار به بررسی سازوکارهای دفاعی ارائه شده مبتنی بر این معماری خواهیم پرداخت.

۲- معماری شبکه‌های مبتنی بر نرم‌افزار

شـــبکه مبتنی بر نرم‌افزار معماری نوظهوری است که بر اساس ایده جداســـازی منطق نرم‌افزاری بستر کنترلی از بستر ســـخت‌افزاری انتقال داده‌ها شکل گرفته است[۸]. جداسازی بخش داده‌ای از بخش کنترل شبکه، برنامه‌های کاربردی و کنترل شبکه را برنامه‌پذیر می‌کند[۹]. همچنین ماشـــین‌های مجازی و زیرساخت شبکه را قادر به تعریف و ارائه انواع سرویس‌ها و خدمات جدید می‌سازد و امکان ارتباط بـــا طیف جدیـــدی از برنامه‌های کاربـــردی برای انعطاف‌پذیری بیشـــتر شبکه و دسترســـی گسترده‌تر به داده‌های ردوبدل شـــده را فراهم می‌کند [۱۰]. مطابق شکل (۱) معماری شبکه‌های مبتنی بر نرم‌افزار را می‌توان به سه بخش لایه انتقال، لایه کنتـــرل و لایه برنامه‌های کاربردی طبقه‌بندی کرد.

۲-۱- لایه انتقال (زیرساخت)

لایه انتقال از تعداد زیادی سوئیچ‌های SDN تشکیل شده اســـت که از طریق رســـانه‌های بی‌سیم یا سیمی به صورت فیزیکی به همدیگر متصل شده‌اند. سوئیچ SDN یک دستگاه ساده است که مسئول انتقال بسته‌های شبکه می‌باشد. اغلب ســـوئیچ‌ها چندین جدول جریان دارند کـــه به صورت خط لوله‌ای[5] می‌باشـــند. جدول جریان هر سوئیچ شامل هزاران قانون برای تنظیمات انتقالات اســـت. شـــایان ذکر است که قوانین انتقال موجود در جداول جریان توسط خود سوئیچ‌ها تولید نمی‌شوند؛ بلکه توســـط کنترل کننده از لایه کنترل به ایـــن لایه اعمال می‌گردد. هر قانون موجود در جدول جریان ســـوئیچ از حوزه‌های فـــراداده[6]، کنش[7]، شمارشـــگر و الگو ســـاخته شده است. حوزه فراداده در صورت وجود بیش از یک جدول، به منظور انجام فرآیند تطبیق بسته‌ها امکان حمل اطلاعـــات از جدولی به جدول دیگـــر را فراهم می‌کند. حوزه الگو، مجموعه‌ای از مقادیر حوزه‌های سرآیند بسته‌ها است که الگوی جریان را تعریف می‌کنند.

در شبکه مبتنی بر نرم‌افزار هر بسته ورودی به سوئیچ با همه قوانین موجود در جداول جریان ســـوئیچ بررســـی می‌شود. اگر تطبیقی با قوانین موجود در جداول یافت شد؛ کنش مخصوص قانون مورد نظر اعمال شده و شمارشگر مربوطه به‌روزرســـانی می‌گردد[۱۱]. شمارشگرها هرگز ســـرریز ندارند و انـــواع مختلفی از جمله شمارشـــگر هر جریـــان ورودی، شمارشـــگر هر جدول، شمارشـــگر هر صف را شـــامل می‌شـــوند. کنتـــرل کننـــده از اطلاعات و آمار ایـــن شمارشـــگرها برای مـــوارد مختلف اســـتفاده می‌کند.

اگر بســـته ورودی، حوزه‌ای بـــرای مطابقت با قوانین موجود در جدول جریان نداشـــت؛ بســـته به‌عنوان بســـته نامعتبر و یا غیرقانونی شـــناخته شـــده و حذف می‌گردد. همچنین اگـــر تطبیقی بین بســـته ورودی و قوانین جدول جریان یافت نشد؛ بســـته به‌عنوان ورودی جدید به کنترل کننده ارسال خواهد شد. بســـته می‌تواند به صورت کامل به کنترل کننده ارسال شود و یا می‌تواند در سوئیچ ذخیره شده و فقط سرآیند آن به کنترل کننده ارسال گردد. هنگام ارسال بسته به کنترل کننده، بسته کپسوله شده و به‌عنوان پیام packet- in مشخص می‌گردد. کنترل کننده با توجه به طول بسته، اولویت‌ها و سایر فاکتورها، بسته‌ها را پردازش می‌کند. ســـپس اقدامات لازم را در مواجهه با این بســـته‌ها که می‌تواند انتقال، حـــذف، اضافه کردن در صف، اصلاح و تغییر حوزه باشد از طریق پیام packet-out به سوئیچ‌ها ارسال می‌کند[۱۲].

5- pipeline

6- metadata
7- action

۲-۲- لایه کنترل

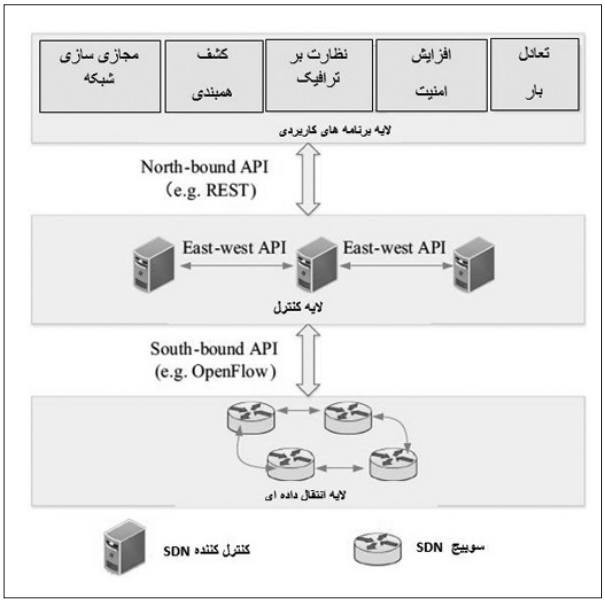
لایه کنترل، کل شبکه را مدیریت و کنترل می‌کند. کنترل کننده، یک گره شبکه است که ویژگی مدیریت و کنترل شبکه در آن پیاده‌سازی شده است و به‌طور کلی از دستگاه‌های فیزیکی با نرم‌افزارهای اختصاصی مجزا می‌باشد. در واقع کنترل کننـــده به‌عنوان مغز معماری شـــبکه‌های مبتنی بر نرم‌افزار می‌باشد که دید کلی از تمام همبندی‌های شبکه از جمله ســـوئیچ‌ها و پیوندها را دارد. پروتکل‌های مسیریابی مختلفی از جمله OSPF[۸], BGP[۹] در کنترل کننده شـــبکه‌های مبتنی بر نرم‌افزار اجرا می‌شوند تا همه انتقالات داده‌ای در لایه انتقال بر اساس دســـتورالعمل‌های مقرر شده توسط کنترل کننده انجام گیرد[۱۱].

لایه کنترل از طریق واســـط ارتباطی South-bound API با ســـوئیچ‌های لایه انتقال ارتباط برقـــرار می‌کند. امروزه اغلب معماری‌های شـــبکه‌های مبتنی بر نرم‌افزار با کنترل کننده‌هایی از جمله Nox، FloodLight [۱۳] و OpenDayLight پیاده‌سازی می‌شـــوند و به منظور بهبود مقیاس پذیری و دســـترس پذیری منابع از چندین کنترل کننده توزیع شده پشـــتیبانی می‌کنند. در ایـــن معماری‌ها هـــر کنترل کننده، مسئول بخشی از سوئیچ‌های لایه انتقال می‌باشد. به منظور حفظ انســـجام وضعیت شبکه و هماهنگی، هر کنترل کننده منحصر به فرد می‌تواند با سایر کنترل کننده‌های شبکه از طریق واسط ارتباطی East-West bound API ارتباط برقرار کند[۱٤].

۲-۳- لایه برنامه‌های کاربردی

لایـــه برنامه‌های کاربـــردی برای اپراتورهای شـــبکه امکان پاســـخ ســـریع به نیازهـــای کســـب و کار را فراهم می‌نمایـــد. نرم‌افزارهـــای کاربردی نوآورانه در قســـمت بالای کنتـــرل کننده قرار می‌گیرند تـــا نیازهای مختلف از جمله مجازی ســـازی [۱۵]، کشـــف همبندی [۱٦]، نظارت ترافیـــک[۱۷]، افزایـــش امنیـــت[۱۸]، تعـــادل بـــار [۱۹] را تأمین نماید.

8- Open Shortest Path First
9- Border Geteway Protocol

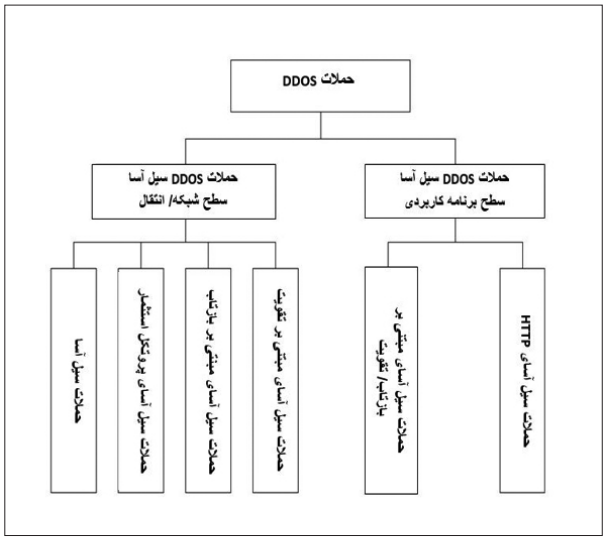


شکل ۱: معماری شبکه‌های مبتنی بر نرم‌افزار [۹]

لایـــه برنامـــه کاربـــردی از طریـــق واســـط ارتباطی north-bound API بـــا لایه کنترل ارتباط برقرار می‌کند. لایه کنترل، انتزاعی از منابع فیزیکی شبکه را برای لایه کاربردی فراهم می‌نماید. به بیان دیگر اپراتورهای شبکه می‌توانند به جای تغییر پیکربندی سوئیچ‌های فیزیکی از برنامه‌نویسی نرم‌افزاری مرکزی کنترل کننده‌های شـــبکه‌های مبتنی بر نرم‌افزار برای تغییر مسیر داده‌ای بسته‌ها استفاده کنند.

۳- حملات رد خدمت توزیع شده

حملات رد خدمت به منزلـــه یکی از تهدیدات اصلی در میان مسایل امنیتی دشوار در شبکه‌های فعلی و شبکه‌های آینده محسوب می‌شـــوند. این حملات در ابتدا به صورت دســـتی انجام می‌شد، ولی امروزه ابزارهای حملات بسیار پیچیده و خودکار برای همکاری با مهاجمان توســـعه داده شده است که همه مراحل حمله به صورت خودکار و بدون نیاز به دانش مهاجم راه‌اندازی می‌شوند [۲۰]. در واقع این حملات سوءاســـتفاده از اینترنت با هـــدف از کار انداختن خدمات وب می‌باشد [۲۱]. حملات رد خدمت توزیع شده در مقیاس بزرگ، یک حمله هماهنگ بر روی دســـترس‌پذیری ســـرویس سیســـتم قربانی و یا منابع شـــبکه‌ای می‌باشد



شکل ۲: طبقه‌بندی ساختارحملات رد خدمت توزیع شده[۲۳]

کــه به‌طور غیرمســتقیم از طریق تعداد زیــادی از عوامل کامپیوتری در معرض خطر در اینترنت راه‌اندازی می‌شود. مهاجــم با قــرار دادن کدهای مخرب یا ســایر تکنیک‌های رخنه‌گری، از نقطه ضعف کامپیوترها سوءاســتفاده کرده و این میزبان‌ها را تحت کنترل خود در می‌آورد [۲۲]. حمله رد خدمت توزیع شــده از دسترســی کاربــران قانونی به منابع ویژه شبکه جلوگیری می‌کند و با ارسال ترافیک کلان نامطلوب به سمت قربانی (ماشین/شبکه) با پرکردن ظرفیت اتصال پهنای باند و مختل کردن ســرویس موجب کاهش دســترس‌پذیری ســرویس‌های شــبکه به کاربران عادی می‌گردد. مطابق شکل(۲) حملات رد خدمت توزیع شده بر اساس ساختار به دو دسته حملات رد خدمت توزیع شده سطح شبکه/ انتقال[۱۰] و حملات رد خدمت توزیع شده سطح برنامه کاربردی[۱۱] طبقه‌بندی می‌شوند[۲۳].

۳-۱-حملات رد خدمت توزیع شــده سطح شبکه/ انتقال

در این حملات، مهاجمان از طریق اشــغال پهنای باند، ظرفیت پردازشی مسیریاب‌ها و منابع شبکه، موجب اختلال در اتصال کاربران قانونی می‌شوند[۲٤]. اغلب حملات سطح شبکه/ انتقال با اســتفاده از پروتکل‌های ICMP,UDP,TCP و DNS راه‌اندازی می‌شوند. این حملات به چهار دسته حملات سیل‌آسا[۱۲]، حملات سیل‌آسای پروتکل استثماری[۱۳]، حملات سیل‌آســای مبتنی بر بازتاب[۱٤] و حملات سیل‌آسای مبتنی بر تقویت[۱۵] تقسیم بندی می‌شوند[۲۳].

۳-۱-۱- حملات سیل‌آسا

در این حملات مهاجم از طریق اشغال پهنای باند شبکه قربانی، اتصال کاربران قانونی را مختل می‌سازد.

۳-۱-۲- حملات سیل‌آسای پروتکل استثمار

در ایــن حملات، مهاجمــان با سوءاســتفاده از برخی ویژگی‌های خاص یا اشــکالات[۱٦] اجرایی برخی پروتکل‌ها موجب مصرف بیش از حد منابع سیستم قربانی می‌گردند.

۳-۱-۳- حملات سیل‌آسای مبتنی بر بازتاب

در این نوع حملات، مهاجمان درخواست‌های جعلی را به ســمت قربانی ارســال می‌کنند. قربانی در پاسخ به این درخواست‌ها مجبور به ارسال پاسخ‌هایی عظیم می‌شود و به این ترتیب منابع قربانی اشغال می‌گردد.

۳-۱-۴- حملات سیل‌آسای مبتنی بر تقویت

مهاجمــان برای هر پیامی از ســرویس تولید پیام‌های بزرگ استفاده می‌کنند. به این ترتیب ترافیک جریان توسط مهاجمان تقویت شده و به سمت قربانی ارسال می گردد.

۳-۲- حمــلات رد خدمــت سیل‌آســای ســطح برنامه‌های کاربردی

این نوع حملات بر ایجاد اختلال در سرویس‌های کاربران قانونی از طریق اشــغال منابع کارسازها متمرکزند. حملات رد خدمت توزیع شده در سطح برنامه‌های کاربردی عموماً پهنای باند کمتری را مصرف می‌کنند. اثرات این حملات مشابه سرویس‌ها می‌باشد، زیرا آن‌ها مشخصات خاص برنامه‌های کاربردی از جمله,HTTP DNS و SIP را دارند. این حملات به دو دسته حملات سیل‌آسای مبتنی بر بازتاب/ تقویت[۱۷] و حملات سیل‌آسای HTTP[۱۸] دسته‌بندی می‌شوند[۲۳].

10- Network/transport-level DDOS attacks
11- Application- level DDOS flooding attacks

12- Flooding attacks
13 - Protocol explotation flooding attacks
14 -Reflection-based flooding attacks
15 - Amplification-based flooding attacks
16- bugs
17- reflection/amplification based flooding attacks
18- HTTP flooding attacks

۳-۲-۱- حملات سیل‌آسای مبتنی بر بازتاب/ تقویت

این حملات از فناوری‌های مشابه حملات سطح شبکه/ انتقال اســتفاده می‌کنند. به‌عنوان مثال حمله تقویت کننده DNS از دو فنــاوری بازتــاب و تقویت بهــره می‌گیرد. در این نوع حمله، مهاجمــان پرس‌وجوهای DNS کوچک را با نشانی‌های IP جعلی تولید می‌کنند. از آنجایی که پیام پاسخ DNS می‌تواند بسیار بزرگتر از پیام پرس وجو DNS باشد، به این ترتیب مهاجمان می‌توانند ترافیک بالای شــبکه‌ای را ایجاد نمایند. ارسال مستقیم این حجم بزرگ ترافیک شبکه به سمت قربانی می‌تواند موجب از کار انداختن شبکه گردد.

۳-۲-۲- حملات سیل‌آسای HTTP

در ایــن نوع حملات، مهاجمان با ارســال تعداد زیادی درخواست HTTP موجب از کار افتادن کارساز وب قربانی می‌گردند.

۴- انواع حملات رد خدمت توزیع شــده در معماری شبکه‌های مبتنی بر نرم‌افزار

معماری شــبکه‌های مبتنــی بر نرم‌افزار ممکن اســت به‌عنوان هدفی برای ایجاد حملات رد خدمت توزیع شــده قــرار گیرد. این معماری به صورت عمودی از ســه بخش لایه زیرســاخت، لایه کنترل و لایــه برنامه‌های کاربردی تشــکیل شده است. به‌طور بالقوه حملات رد خدمت توزیع شده می‌تواند در هر ســه لایه معماری مبتنی بر نرم‌افزار راه‌اندازی شود. همان‌طور که در شکل(۳) نشان داده شده اســت براساس اهداف احتمالی، می‌توان حملات رد خدمت توزیع شــده در معماری شــبکه‌های مبتنی بر نرم‌افزار را به سه دســته حملات رد خدمت توزیع شــده لایه برنامه کاربردی[19]، حملات رد خدمت توزیع شــده لایه کنترل[20] و حملات رد خدمت توزیع شــده لایه زیرساخت[21] طبقه‌بندی کرد[۲۵]. جدول(۱) شــرایط محقق شدن حملات رد خدمت توزیع شــده در شــبکه‌های مبتنی بر نرم‌افزار را به طور خلاصه بیان می‌کند.

19- Application Layer DDoS Attacks
20- Control Layer DDoS Attacks
21- Infrastructure Layer DDoS Attacks

٤-١- حملات رد خدمت توزیع شده لایه برنامه‌های کاربردی

برای راه‌اندازی این نــوع حملات از روش‌های حمله بر برنامه‌های کاربردی و حمله بر واسط ارتباطی north bound API اســتفاده می‌شود. از آنجایی‌که جداسازی[22] برنامه‌های کاربردی با منابع در معماری شبکه‌های مبتنی بر نرم‌افزار حل نشده است، حملات رد خدمت توزیع شده در برنامه‌های کاربردی می‌تواند بر سایر برنامه‌ها هم اثرگذار باشد.

٤-٢- حملات رد خدمت توزیع شده لایه کنترل

در شــبکه‌های مبتنی بر نرم‌افــزار، هنگامی که بخش داده‌ای با بسته ورودی جدیدی که با قوانین و جریان‌های موجود در جداول جریان مطابقتی نداشــته باشــد مواجه گــردد، بســته را به صورت کامل یا بخشــی از ســرآیند بســته را برای تعیین قوانین جدید به بخش کنترل ارسال می‌کنــد[۲٦]. بنابراین بســیاری از جریان‌های متناقض با قوانین می‌توانند منجر به حملات رد خدمت توزیع شده در بخش کنترل شــوند. کنترل کننده‌ها به‌طور بالقوه به‌عنوان یک نقطه پرخطر برای شکســت شــبکه مبتنی بر نرم‌افزار محســوب می‌شوند. این بخش همچنین برای مهاجمان یک هدف جذاب برای راه‌اندازی حملات رد خدمت توزیع شده می‌باشد. مهاجمان با استفاده از روش‌های حمله به کنترل کننده از طریق حمله به south bound API، north bound API، west bound API، و یا east bound API می‌توانند حملات رد خدمت توزیع شده در لایه کنترل را راه‌اندازی نمایند.

٤-٣- حملات رد خدمت توزیع شده لایه زیرساخت

مهاجمان برای راه‌اندازی این حملات از دو روش حمله به سوئیچ‌ها و حمله به واســط ارتباطی south bound API استفاده می‌کنند. هنگامی که سوئیچ، سرآیند بسته ورودی جدید را برای تعیین تکلیف به ســمت کنترل کننده ارسال می‌کند، خود بســته بایســتی در حافظه گره ذخیره شود. بنابرایــن مهاجــم می‌تواند به راحتــی جریان‌های جدید و ناشــناخته‌ای را راه‌اندازی نماید که موجب سربار اضافی

22- isolation

جدول ۱: حملات رد خدمت توزیع شده در شبکه‌های SDN

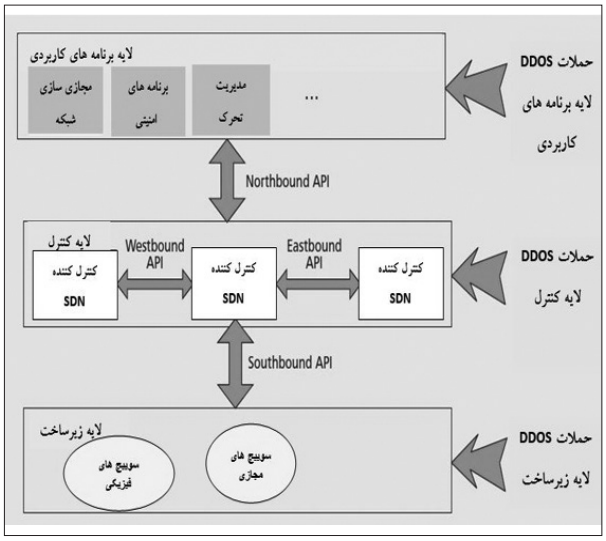
انواع حملات رد خدمت	پیاده‌سازی روش حمله
حمله به لایه برنامه کاربردی	حمله به برنامه‌های کاربردی-حمله به واسط ارتباطی north bound API
حمله به لایه کنترل	حمله به کنترل کننده از طریق حمله به واسط‌های ارتباطی north bound API-south bound API-west bound API-east bound API
حمله به لایه زیر ساخت	حمله به سوئیچ‌ها- حمله به واسط ارتباطی sourth bound API

حافظه سوئیچ‌ها گردد. در نتیجه حافظه گره به گلوگاه[۲۳] شبکه تبدیل می‌شود. همچنین تولید درخواست‌های جعلی موجب تولید قوانین بی فایده بسیاری می‌گردد که نیاز است همه این قوانین در بخش داده‌ای لایه زیرساخت نگه‌داری شوند. در نتیجه با توجه به محدودیت منابع، مشکلات زیادی را برای بخش داده‌ای برای نگهداری قوانین جریان‌های عادی شبکه به وجود می‌آورد[۲۶].

از آنجایی‌که حملات رد خدمت توزیع شده از نشانی‌های IP مبدأ ساختگی یا ترافیک‌های جعلی استفاده می‌کنند، یک سازوکار احراز هویت[۲۴] ساده می‌تواند موجب کاهش اثر جریان‌های جعلی گردد. اما اگر مهاجم کنترل کارسازی را که بسیاری از جزئیات اطلاعات کاربران را ذخیره کرده در اختیار بگیرد، می‌تواند با استفاده از درگاه‌های احراز هویت شده و نشانی‌های مک[۲۵] مبدأ، جریان‌های مجاز اما جعلی را به شبکه تزریق نماید[۲۷].

SSL یک پروتکل استاندارد و رایج امنیتی برپایه رمزگذاری است که در آن داده‌های رد و بدل شده بین سرویس دهنده و سرویس گیرنده توسط کلیدهای خصوصی و عمومی رمزنگاری شده و در سمت دیگر رمزگشایی می‌شود. TLS دوقلوی SSL است که توسط IEEE استاندارد شده است. مهاجمان با استفاده از آسیب پذیری‌های موجود در این پروتکل‌ها حملاتی

23- bottleneck-
24-authentication mechanisms
25- source Mac addresses



شکل ۳: حملات DDOS احتمالی در معماری SDN [۲۵]

مانند CRIME، BEAST، POODLE را راه‌اندازی می‌کنند. OpenFlow گزینه پشتیبانی از پروتکل TLS را در تبادلات بین سوئیچ و کنترل کننده فراهم می‌کند ولی استفاده از TLS/SSL ارتباطات امن را تضمین نمی‌کند. علاوه براین، مدل TLS/SSL برای ایجاد اطمینان و اعتماد بین کنترل کننده و سوئیچ‌ها کافی نمی باشد. پس از این‌که مهاجم دسترسی به بخش کنترل را افزایش داد، با متمرکز ساختن نیروهای کافی (از نظر تعداد سوئیچ‌های تحت کنترل) می‌تواند یک حمله رد خدمت توزیع شده را راه‌اندازی نماید[۲۵].

۵- مزایای معماری شبکه‌های مبتنی بر نرم‌افزار برای مقابله با حملات رد خدمت توزیع شده

ویژگی‌های معماری شبکه‌های مبتنی بر نرم‌افزار، مزایای متعددی را برای مقابله با حملات رد خدمت توزیع شده فراهم می‌آورد. برخی از این مزایا در ادامه شرح داده می‌شود.

- **جداسازی بخش کنترل از بخش داده‌ای**

در معماری شبکه‌های مبتنی بر نرم‌افزار، بخش داده‌ای از بخش کنترل جدا شده است. این جداسازی امکان انجام آزمایش‌های راه‌اندازی حملات رد خدمت توزیع شده و مقابله با آن‌ها را فراهم می‌سازد. توانایی بالای پیکربندی این معماری در میان شبکه‌های مجازی امکان اجرای آزمایش‌ها در یک محیط واقعی را ارائه می‌دهد. این ویژگی

تسهیلات بزرگی را برای ارائه ایده‌های جدید انتقالات و روش‌های کاهش اثر حملات رد خدمت توزیع شده فراهم می‌کند. در این محیط ایده‌های پیشرفته جدید می‌توانند از یک فاز آزمایشی به فاز اجرایی و عملیاتی منتقل شوند[۲۳].

- کنترل کننده متمرکز و دید کلی شبکه

در این معماری، کنترل کننده برای ایجاد سیاست‌های امنیتی ثابت و الگوی ترافیکی تحلیلی یا نظارتی در مقابل تهدیدات امنیتی بالقوه، دید کلی از همبندی شبکه‌ای را دارا می‌باشد. کنترل کننده متمرکز معماری شبکه‌های مبتنی بر نرم‌افزار، بر اساس اطلاعات به دست آمده از طریق درخواست میزبان‌های پایانی، امکان احراز هویت میزبان‌های قانونی در این معماری را می‌دهد[۲۳]. این ویژگی امکان اجرای پروتکل RADIUS[۲۶] در شبکه‌های مبتنی بر نرم‌افزار را فراهم می‌کند. این پروتکل استانداردی برای طراحی و پیاده‌سازی سرویس‌دهندگانی است که مسئولیت تأیید و مدیریت کاربران را برعهده خواهند گرفت. پروتکل RADIUS از یک معماری کارساز-کارخواه[۲۷] برای تأیید و ایجاد حساب استفاده می‌نماید. پروتکل فوق اطلاعات حساب، پیکربندی، تأیید و مجوزها را بین یک کارخواه RADIUS و یک کارساز RADIUS منتقل می‌کند[۲۸].

- **توانایی برنامه ریزی شبکه توسط برنامه‌های کاربردی خارجی:**

توانایی برنامه‌ریزی معماری شبکه‌های مبتنی بر نرم‌افزار از فرآیند هوشمند جمع‌آوری اطلاعات از سیستم‌های تشخیص نفوذ[۲۸] و سیستم‌های پیشگیری از نفوذ[۲۹] موجود پشتیبانی می‌کند. بسیاری از الگوریتم‌های هوشمند می‌توانند براساس حملات رد خدمت توزیع شده مختلف به صورت انعطاف پذیر استفاده شوند[۲۳].

- **تجزیه و تحلیل ترافیک مبتنی بر نرم‌افزار**

تجزیه و تحلیل ترافیک مبتنی بر نرم‌افزار، نوآوری‌های قابل توجهی را برای این معماری به ارمغان می‌آورد. به‌طوری‌که شبکه‌های مبتنی بر نرم‌افزار می‌تواند از انواع الگوریتم‌های هوشمند، پایگاه داده‌ها و سایر ابزارهای نرم‌افزاری استفاده نماید[۲۳].

- **به‌روزرسانی پویای قوانین انتقالات و جریان‌ها**

به‌روزرسانی پویای قوانین انتقالات به پاسخ سریع شبکه در مقابل حملات رد خدمت توزیع شده کمک می‌کند. براساس تجزیه و تحلیل ترافیک، سیاست‌های امنیتی جدید یا به‌روزرسانی شده می‌توانند بدون تأخیر در سراسر شبکه در قالب قوانین مسدودسازی جریان ترافیک حمله منتشر شوند[۲۹].

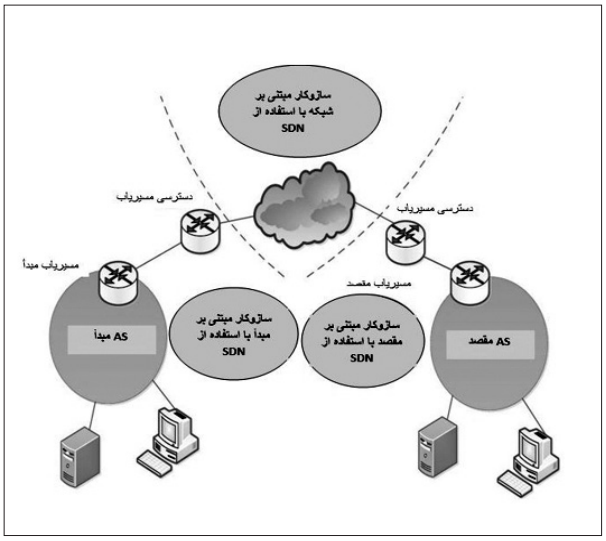
۵-۱- تأثیرات معماری شبکه‌های مبتنی بر نرم‌افزار در دفاع علیه حملات رد خدمت توزیع شده

پیاده‌سازی معماری شبکه‌های مبتنی بر نرم‌افزار تا حدود زیادی در دفاع علیه حملات رد خدمت توزیع شده در هر دو جهت تأثیر می‌گذارد. از یک سو، موجب پیشرفت منطق تشخیصی می‌شود و توانمندسازی عملیات متداول برای پیاده‌سازی را ساده‌تر می‌کند. از سوی دیگر، فرآیندهای نرم‌افزاری سیستم‌ها در مقایسه با فرآیندهای پردازشی مبتنی بر سخت افزار بسیار کندتر هستند. همچنین تأخیرات شبکه و هزینه‌های سربار ترافیکی در اثر ارتباطات بین برنامه‌های کنترل و بخش داده‌ای ایجاد می‌گردد. بنابراین معماری شبکه‌های مبتنی بر نرم‌افزار می‌تواند در مقابله با حملات رد خدمت کمک نماید، در عین حال می‌تواند به‌عنوان هدفی برای ایجاد سطح حمله جدید تبدیل شود[۲۹].

۶- سازوکارهای دفاعی حملات رد خدمت توزیع شده با استفاده از شبکه‌های مبتنی بر نرم‌افزار

مطابق شکل (٤) سازوکارهای دفاعی ارائه شده علیه حملات رد خدمت توزیع شده با استفاده از شبکه‌های مبتنی بر نرم‌افزار را می‌توان براساس محل استقرار در سه دسته سازوکارهای مبتنی بر مبدأ[۳۰]، سازوکارهای مبتنی بر

26- remote authentication dial in user service
27- client- server
28- intrusion detection systems
29- intrusion prevention systems
30- Source- based Mechanisms Using SDN



شکل ۴: طبقه‌بندی سازوکارهای دفاعی علیه حملات DDOS با استفاده از معماری SDN [۳۰]

شبکه[۳۱] و سازوکارهای مبتنی بر مقصد[۳۲] طبقه‌بندی کرد. جدول(۲) قابلیت‌های SDN مورد استفاده در این سازوکارها را را بیان می‌کند.

۶-۱- سازوکار مبتنی بر مبدأ با استفاده از شبکه‌های مبتنی بر نرم‌افزار

در این نوع سازوکار، از قابلیت‌های برنامه پذیر بودن، تجزیه و تحلیل ترافیک، به‌روزرسانی پویای قوانین شبکه و دید کلی از همبندی شبکه‌های مبتنی بر نرم‌افزار استفاده می‌شود. در این سازوکار کنترل کننده شبکه‌های مبتنی بر نرم‌افزار، ناهنجاری‌های ترافیکی را تشخیص داده و بسته‌های مخرب را فیلتر می‌کند. همچنین نشانی‌های IP مبدأ بسته‌های قانونی را نزدیک محل ورود معتبر می‌سازد.

جین و همکاران[۳۱] یک سیستم تشخیص بدافزار از طریق تجزیه و تحلیل بیدرنگ ترافیکی با استفاده از معماری شبکه‌های مبتنی بر نرم‌افزار را ارائه دادند. این سیستم فقط به جریان‌های ترافیکی که نشانی مبدأ آن‌ها در محدوده نشانی‌های IP مورد انتظار باشد، اجازه ورود به شبکه را می‌دهد. در این طرح، نقاط دسترسی که جزء نقاط اساسی در سوئیچ‌های OpenFlow هستند توسط کنترل کننده شبکه مبتنی بر نرم‌افزار، کنترل می‌شوند. نقاط دسترسی، ترافیک‌های متحرک را به کنترل کننده انتقال می‌دهد و جریان‌های ورودی به کنترل کننده را از طریق کانال امن دریافت و نصب می‌کند. این سیستم یک مدل تشخیص بدافزار در داخل کنترل کننده شبکه مبتنی بر نرم‌افزار است که می‌تواند اطلاعات ترافیکی را با استفاده از الگوریتم‌های تشخیصی استخراج نماید. برخی از الگوریتم‌های تشخیصی سازوکار مبتنی بر مبدأ عبارتند از: لیست سیاه IP [۳۳]، نرخ موفقیت ارتباطات[۳۴]، خفه کردن ارتباطات[۳۵] و تحلیل انباشتگی[۳۶].

- **لیست سیاه IP**

لیست سیاه IP نشانی‌های مخرب، یک راه ساده برای حفاظت از شبکه است که اطلاعات مورد نیاز را می‌تواند از منابع در دسترس موجود یا داده‌های تاریخی به دست آورد. بدین ترتیب از ورود هر جریان ترافیکی که شامل یک نشانی IP از لیست سیاه باشد، ممانعت می‌نماید[۳۰].

- **نرخ موفقیت ارتباطات**

نرخ موفقیت یک الگوریتم تشخیص بدافزار براساس نرخ موفقیت ارتباطات می‌باشد. طبق مشاهدات می‌توان بیان کرد که احتمال ارتباطات موفق برای یک میزبان عادی بسیار بیشتر از احتمال ارتباط موفق برای یک میزبان آلوده می‌باشد.

- **خفه کردن ارتباطات**

یک ماشین آلوده در سیستم سعی خواهد کرد هرچه سریعتر با ماشین‌های مختلف ارتباط برقرار کند. در حالی که ماشین‌های غیرآلوده رفتار متفاوتی دارند. در ماشین‌های غیرآلوده ارتباطات با نرخ پایین ساخته شده و به صورت محلی همبسته می‌شوند. الگوریتم خفه کردن ارتباطات می‌تواند نرخ ارتباطات میزبان‌های جدید را محدود سازد و کاربران آلوده را براساس مشاهدات در طی انتشار ویروس شناسایی نماید[۳۰].

- **تحلیل انباشتگی**

هنگامی که یک میزبان توسط بدافزار آلوده شود،

31- Network-based Mechanisms Using SDN
32- Destination-based Mechanisms Using SDN
33- IP Blacklist
34- Connection Success Ratio
35- Throttling Connection
36- Aggregation Analysis

ممکن اســت بســیاری از میزبان‌های موجود در شبکه را آلوده نماید. خصوصیات رفتاری مشــترک کاربران آلوده در شبکه آن‌ها را از سایر کاربران غیرآلوده متمایز می‌کند. تحلیل انباشتگی الگوریتمی اســت که براساس مشاهدات، میزبان‌های آلوده را به وسیله تشخیص انباشتگی از روی ارتباطات مشابه شناسایی می‌کند[۳۱].

۶-۲-سازوکار مبتنی بر شبکه با استفاده از شبکه‌های مبتنی بر نرم‌افزار

این ســازوکارها از قابلیت‌های کنتــرل کننده متمرکز، تجزیــه و تحلیل ترافیک و به‌روزرســانی پویــای قوانین شــبکه‌های مبتنی بر نرم‌افزار اســتفاده کرده و با نظارت بر ترافیک‌های شــبکه، حملات رد خدمت توزیع شــده را تشــخیص می‌دهند. ســپس اقدامات لازم جهت کاهش اثر حملات را اعمال می‌نمایند. اغلب این سازوکارها، به‌عنوان برنامه‌های شبکه‌های مبتنی بر نرم‌افزار طراحی می‌شوند. به‌طور کلی برنامه‌های شبکه‌های مبتنی بر نرم‌افزار شامل چهار واحد عملکرد زیر می‌باشند [۳۰]:

• کنترل جریان: مسئول درخواست دوره‌ای جریان‌های ورودی از همــه جــداول جریان ســوئیچ‌های موجود در بخش داده‌ای شبکه می‌باشند.

• استخراج ویژگی: این واحد تمامی جریان‌ها را دریافت کــرده و ویژگی‌هایــی را که برای تشــخیص حملات رد خدمت توزیع شده اهمیت دارند استخراج می‌کند. از جمله ویژگی‌های مهم می‌توان به میانگین بسته‌ها در هر جریان (Apf)[۳۷]، میانگیــن زمــان در هر جریان(Adf)[۳۸]، رشــد تک جریان(Gsf)[۳۹] اشاره نمود.

• تشخیص ناهنجاری: این واحد با اعمال برخی فناوری‌های تشــخیصی از جمله فناوری نقشه خودســازمانده(SOM)[۴۰] ناهنجاری موجود در شبکه را تشخیص می‌دهد.

• کاهش اثر حملات: این واحد اقدامات مقابله‌ای را برای کاهــش اثر حملات از جمله به‌روزرســانی قوانین انتقال، محدودیت نرخ انتقال و دورانداختن بســته‌ها در شــبکه اعمال می‌کند.

چــو و همــکاران در [۳۲] یک طرح جدیــد دفاعی علیه حمــلات رد خدمت توزیع شــده را ارائه دادند. این طرح بر روی کنترل کننده شــبکه مبتنی بر نرم‌افزار پیاده‌ســازی می‌شــد و با نظارت بر جریان‌های سوئیچ‌ها، حجم حملات رد خدمت توزیع شده را تشخیص داده و اقدامات مقابله‌ای را اعمال می‌نمود.

جیوتــس و همــکاران در [۳۳] یک ســازوکار دفاعی مقیاس پذیر در محیط شبکه‌های مبتنی بر نرم‌افزار را ارائه دادند. در این مقاله برای تشخیص و کاهش اثر ناهنجاری از ترکیب OpenFlow و SFlow اســتفاده شده بود. در واقع این طرح یک ســازوکار مدولار را ارائه می‌دهد که قابلیت نمونه گیری بسته‌ها را از SFlow به دست آورده و موجب کاهش ارتباطــات مورد نیاز بین ســوئیچ و کنترل کننده می‌گردد.

۶-۳- ســازوکار مبتنی بــر مقصد با اســتفاده از شبکه‌های مبتنی بر نرم‌افزار

این ســازوکارها، بیشــتر به عیب یابی و اشکال زدایی شــبکه با بهره‌گیــری از قابلیت‌های شــبکه‌های مبتنی بر نرم‌افــزار متمرکزنــد. از قابلیت‌های شــبکه‌های مبتنی بر نرم‌افزار اســتفاده شــده در این ســازوکارها می‌توان به دیــد کلی همبندی شــبکه و قابلیت به‌روزرســانی قوانین شــبکه اشاره کرد. در این ســازوکارها برای عیب یابی و اشــکال‌زدایی شــبکه از فناوری‌هایی ماننــد ردیابی IP و اســتفاده از تاریخچه بســته‌ها در محل نشــانی IP مقصد بسته‌ها استفاده می‌شود[۳۰].

ردیابی IP می‌تواند برای یافتن مبدأ و مســیرهای حمله مورد اســتفاده قرار گیرد. با این حال اجرای رویکردهای ردیابی IP در اینترنت بســیار دشــوار می‌باشد. هندیگل و همکاران در [۳٤] نشــان دادند که تاریخچه بســته‌ها، عیب یابی شــبکه را ســاده‌تر می‌کند. در این مقاله برای نمایش سودمندی تاریخچه بســته‌ها و امکان عملی ساختن آن‌ها

37- average of packets per flow
38- average of duration per flow
39- growth of single flows
40- Self Organizing Maps

جدول۲: سازوکارهای دفاعی علیه حملات رد خدمت توزیع شده با استفاده از شبکه‌های SDN

انواع سازوکار دفاعی	قابلیت SDN مورد استفاده در سازوکار دفاعی	مزایا/معایب
مبتنی بر مبدأ	برنامه پذیری-تجزیه و تحلیل ترافیک-به‌روزرسانی پویای قوانین-دیدکلی همبندی شبکه	تشخیص و توقف حملات با کمترین آسیب به ترافیک قانونی
مبتنی بر شبکه	کنترل کننده متمرکز- تجزیه و تحلیل ترافیک- به‌روزرسانی پویای قوانین	تشخیص پس از رسیدن حمله به قربانی صورت می‌گیرد - نیاز به بررسی برخط هشدارهای کاذب
مبتنی بر مقصد	دیدکلی همبندی- به‌روزرسانی پویای قوانین	ردیابی IP در اینترنت بسیار دشوار است.

یک بستر قابل گسترش با امکان ضبط بسته‌ها پیشنهاد شد. این بستر، برنامه‌ها را قادر به بازیابی تاریخچه‌های بسته‌های مورد نظر می‌سازد.

واندسام و همکاران در[۳۵] OFRewind را به‌عنوان ابزاری برای ثبت و اجرای ترافیک بخش کنترل کننده معماری شبکه‌های مبتنی بر نرم‌افزار معرفی کردند که امکان انعطاف‌پذیری، سازگاری، ثبت کنترل متمرکز شبکه و پخش هماهنگ ترافیک در دامنه کنترل کننده را فراهم می‌ساخت.

۷- نتیجه‌گیری

از شبکه‌های SDN به‌عنوان بزرگ‌ترین تحول چهار دهه شبکه‌های کامپیوتری یاد می‌شود. در سال‌های اخیر شبکه‌های مبتنی بر نرم‌افزار مورد توجه بسیاری از پژوهشگران واقع شده است و به احتمال زیاد در آینده نزدیک جایگزین شبکه‌های سنتی خواهد شد. این معماری مزایای زیادی را در مدیریت شبکه از نظر سادگی، برنامه پذیری و انعطاف‌پذیری به وجود می‌آورد. حملات رد خدمت توزیع شده به منزله یکی از تهدیدات اصلی در میان مسایل امنیتی شبکه‌ها می‌باشد. با توجه به توسعه ابزارهایی حملات پیچیده و خودکار، معماری شبکه‌های مبتنی بر نرم‌افزار نیز ممکن است به‌عنوان هدفی برای مهاجمان تبدیل شوند. با توجه به این شرایط بایستی قبل از پیاده‌سازی این نوع شبکه‌ها اقدامات و مطالعات لازم جهت امنیت این معماری از جمله سازوکارهای پیشگیری، تشخیصی و دفاعی متناسب با این ساختار انجام گیرد.

هدف از این مقاله فراهم کردن درک درستی از روش‌های حمله، ابزارها و روش‌های دفاعی در برابر این حملات می‌باشد. در این مقاله با بررسی ساختار معماری شبکه‌های مبتنی بر نرم‌افزار، روش‌های راه‌اندازی حملات رد خدمت توزیع شده در این معماری مورد بحث قرار گرفت. ما در این مقاله ویژگی‌های منحصر به فرد شبکه‌های مبتنی بر نرم‌افزار را در شکست حملات رد خدمت توزیع شده بیان کردیم. بررسی سازوکارهای دفاعی ارائه شده مبتنی بر شبکه‌های مبتنی بر نرم‌افزار نشان داد که شبکه‌های مبتنی بر نرم‌افزار ابزار امیدوارکننده‌ای برای شکست حملات رد خدمت توزیع شده می‌باشند. ویژگی‌های مثبت این معماری فرصت زیادی را برای تشخیص و مقابله علیه حملات رد خدمت توزیع شده به ارمغان می‌آورد.

با توجه به محبوبیت شبکه‌های مبتنی بر نرم‌افزار، در آینده نزدیک این معماری با سایر حوزه‌ها از جمله ارتباطات بی‌سیم، محاسبات ابری، اینترنت اشیاء تلفیق خواهد شد[۳۶]، بنابراین شناخت ساختاری و نقاط ضعف و قوت این معماری برای محققان بسیار حائز اهمیت می‌باشد. محققان می‌توانند با داشتن شناخت درستی از این ساختار بر روی امنیت این معماری در ترکیب با سایر حوزه‌ها متمرکز شوند.

مراجع

[1] McKeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, Shenker S, Turner J, "OpenFlow: enabling innovation in campus networks", ACM SIGCOMM Computer Communication Review, 31;38(2):69-74, Mar 2008.

[2] Zhang P, Wang H, Hu C, Lin C, "On Denial of Service Attacks in Software Defined Networks.", IEEE Network. 30(6):28-33, Nov 2016.

[3] Li CS, Liao W, "Software defined networks.", IEEE Communications Magazine, 1;51(2):113, Feb 2013.

[4] Braga R, Mota E, Passito A, "Lightweight DDoS flooding attack detection using NOX/OpenFlow.", InLocal Computer Networks (LCN), 2010 IEEE 35th Conference, IEEE, pp. 408-415, Oct 2010.

[5] Tri HT, Kim K, "Assessing the impact of resource attack in Software Defined Network.", InInformation Networking

[22] Criscuolo PJ, "Distributed denial of service, tribe flood network 2000 and stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC).", UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory; Feb 2000.
[23] Luo S, Wu J, Li J, Pei B, "A defense mechanism for distributed denial of service attack in software-defined networks." , InFrontier of Computer Science and Technology (FCST), 2015 Ninth International Conference, IEEE, pp. 325-329, Aug 2015.
[24] Mirkovic J, Reiher P, "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review, 34(2):39-53, Apr 2004.
[25] Yan Q, Yu FR, "Distributed denial of service attacks in software-defined networking with cloud computing.", IEEE Communications Magazine, 53(4):52-9, Apr 2015.
[26] Sezer S, Scott-Hayward S, Chouhan PK, Fraser B, Lake D, Finnegan J, Viljoen N, Miller M, Rao N, "Are we ready for SDN? Implementation challenges for software-defined networks.", IEEE Communications Magazine. 51(7):36-43, Jul 2013.
[27] Kreutz D, Ramos F, Verissimo P, "Towards secure and dependable software-defined networks.", InProceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, pp. 55-60 , Aug 2013.
[28] Szilagyi D, Sood A, Singh T, "RADIUS: A Remote Authentication Dial-In User Service.", InSight: RIVIER ACADEMIC JOURNAL;5(2):1-2, 2009.
[29] Wang B, Zheng Y, Lou W, Hou YT, "DDoS attack protection in the era of cloud computing and software-defined networking." Computer Networks, 22;81:308-19., Apr 2015.
[30] Yan Q, Yu FR, Gong Q, Li J, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey." , some research issues, and challenges. IEEE Communications Surveys & Tutorials.18(1):602-22, 2016.
[31] Jin R, Wang B, "Malware detection for mobile devices using software-defined networking." InResearch and Educational Experiment Workshop (GREE), 2013 Second GENI, pp. 81-88, IEEE, 2013.
[32] YuHunag C, MinChi T, YaoTing C, YuChieh C, YanRen C, "A novel design for future on-demand service and security." , InCommunication Technology (ICCT), 2010 12th IEEE International Conference, IEEE, pp. 385-388, Nov 2010.
[33] Giotis K, Argyropoulos C, Androulidakis G, Kalogeras D, Maglaris V, "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments.", Computer Networks, 62:122-36, 2014.
[34] Handigol N, Heller B, Jeyakumar V, Mazières D, McKeown N, "I Know What Your Packet Did Last Hop: Using Packet Histories to Troubleshoot Networks.", InNSDI, Vol. 14, pp. 71-85, 2014.
[35] Wundsam A, Levin D, Seetharaman S, Feldmann A, "OFRewind: Enabling Record and Replay Troubleshooting for Networks." , In-USENIX Annual Technical Conference, pp. 15-17, 2011.
[36] Bakhshi T, "State of the Art and recent research advances in software defined networking." Wireless Communications and Mobile Computing, 2017.
(ICOIN), 2015 International Conference, IEEE, pp. 420-425 Jan 2015.
[6] William Stallings, Lawrie Brown,"Computer Security Principles And Practice",vol 2, edition 3,Newyork, 2014.
[7] Peng T, Leckie C," Survey of network-based defense mechanisms countering the DoS and DDoS problems', Journal ACM Computing Surveys (CSUR), vol 39, no3, newyork, 2007.
[8] Dao NN, Park J, Park M, Cho S, "A feasible method to combat against DDoS attack in SDN network.", InInformation Networking (ICOIN), 2015 International Conference, pp. 309-311, Jan 2015.
[9] Hartman S, Wasserman M, Zhang D, "Software driven networks problem statement." Network Working Group Internet-Draft, Oct. 2013.
[10] Bates A, Butler K, Haeberlen A, Sherr M, Zhou W, "Let SDN be your eyes: Secure forensics in data center networks.", InProceedings of the NDSS workshop on security of emerging network technologies,SENT'14,Feb, 2014.
[11] Shu Z, Wan J, Li D, Lin J, Vasilakos AV, Imran M, "Security in software-defined networking: Threats and countermeasures.", Mobile Networks and Applications, 21(5):764-76, Oct 2016.
[12] Mousavi SM, St-Hilaire M, "Early detection of DDoS attacks against SDN controllers." InComputing, Networking and Communications (ICNC), 2015 International Conference, IEEE, pp. 77-81, Feb 2016.
[13] Gude N, Koponen T, Pettit J, Pfaff B, Casado M, McKeown N, Shenker S, "NOX: towards an operating system for networks.", ACM SIGCOMM Computer Communication Review;38(3):105-10, Jun 2008.
[14] Kreutz D, Ramos FM, Verissimo PE, Rothenberg CE, Azodolmolky S, Uhlig S, "Software-defined networking: A comprehensive survey.", Proceedings of the IEEE;103(1):14-76, Jan 2015.
[15] Bernardo DV, "Software-defined networking and network function virtualization security architecture. Internet Eng.", Task Force, Fremont, CA, USA.[Online]. Available: https:// tools. ietf. org/html/draftbernardo-sec-arch-sdnnvf-architecture-00. 2014.
[16] Yang M, Li Y, Jin D, Zeng L, Wu X, Vasilakos AV, "Software-defined and virtualized future mobile and wireless networks: A survey.", Mobile Networks and Applications;20(1):4-18, Feb 2016.
[17] Yuan W, Deng P, Taleb T, Wan J, Bi C, "An unlicensed taxi identification model based on big data analysis." IEEE Transactions on Intelligent Transportation Systems;17(6):1703-13, 2016.
[18] Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D, "Security of the internet of things: Perspectives and challenges.", Wireless Networks;20(8):2481-501, Nov 2014.
[19] Namal S, Ahmad I, Gurtov A, Ylianttila M, "SDN based inter-technology load balancing leveraged by flow admission control.", InFuture Networks and Services (SDN4FNS), IEEE, pp. 1-5, Nov 2013.
[20] Poongothai M, Sathyakala M, "Simulation and analysis of DDoS attacks.", InEmerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference,IEEE, pp. 78-85, 2012.
[21] Peng T, Leckie C, Ramamohanarao K, "Survey of network-based defense mechanisms countering the DoS and DDoS problems.", ACM Computing Surveys (CSUR);39(1):3, Apr 2007.