

دانشکده مهندسی کامپیوتر

سمینار کارشناسی ارشد گرایش رایانش امن

عنوان:

|  |
| --- |
| تحلیل رفتاری ترافیک در شبکه نرم‌افزار محور به‌منظور تشخیص حمله منع خدمت توزیع‌شده |
| Traffic Behavior Analysis in Software Defined Network for DDoS Attack Detection |

نگارش:

**علیرضا کریمی**

**۹۷۲۱۳۲۹۶**

استاد راهنما:

**دکتر رسول جلیلی**

استاد ممتحن داخلی:

**دکتر جعفری**

**بهمن 1398**

چکیده**:**

**حملات منع خدمت به‌عنوان یکی از متداول‌ترین و پرهزینه‌ترین حملات در سطح شبکه شناخته می‌شود که موجب بروز اختلال در ارائه خدمات سطح سازمانی و حتی ملی شده است. امروزه، شبکه‌های نرم‌افزار‌ محور به‌عنوان یک رویکرد جدید در صنعت فناوری اطلاعات مورد توجه قرارگرفته است. در معماری این نوع شبکه‌ها، بخش کنترل از بخش داده جداشده و به‌صورت متمرکز تحت عنوان خدمت کنترل‌کننده، هدایت بسته‌ها توسط راه‌گزین‌ها در لایه داده را مدیریت می‌کند.** در حال حاضر شبکه‌های نرم‌افزار محور، توسط شرکت‌های پيشرو به‌صورت گسترده به کار گرفته‌شده و ازآنجایی‌که بر اساس پیش‌بینی‌ها این معماری به‌زودی جایگزین شبکه‌های فعلی خواهد شد و معماری شبکه‌های کنونی را تغيير خواهد داد، باید بتوان عملکرد‌های امنیتی در شبکه‌های نرم‌افزار محور را پیاده‌سازی کرده و جایگزین عملکردهای امنيتی در شبکه‌های فعلی شود. یکی از اساسی‌ترین نیاز‌های امنیتی در سطح شبکه بحث دسترس‌پذیر بودن کامل شبکه می‌باشد**. حملات منع خدمت به‌عنوان تهدیدی جدی برای قابلیت دسترس‌پذیری این‌گونه شبکه‌ها شناخته می‌شود. لذا، مقابله با حملات منع خدمت در این شبکه‌ها، به یک بستر مهم تحقیقاتی در سال‌های اخیر تبدیل‌شده‌ است. ویژگی‌‌های فراهم‌شده توسط شبکه‌های نرم‌افزار محور، به ما امکان بازپیکربندی ساده و پویا، جهت بهینه‌سازی هدایت جریان‌های شبکه و برقراری امنیت در این شبکه‌ها را می‌دهد. در این پژوهش، ضمن بررسی کار‌های مشابه صورت گرفته در این زمینه، با تحلیل رفتاری ترافیک در شبکه‌های نرم‌افزار محور به کمک ‌روش‌های مبتنی بر یادگیری ماشین، به دسته‌بندی ترافیک دریافتی پرداخته می‌شود. سپس یک روش بهبودیافته برای تشخیص حمله و کاهش اثرات ناشی از آن، متناسب با زیرساخت و ویژگی‌های شبکه‌های نرم‌افزار محور، ارائه خواهد شد و درنهایت روش پیشنهادی با روش‌های موجود ارزیابی و مقایسه خواهد شد.**

**کلیدواژه:** حملات منع خدمت، شبکه‌های نرم‌افزار محور، یادگیری ماشین

**1 سرآغاز**

امروزه با افزایش حجم تبادلات داده‌ای در بستر اینترنت، برقراریِ ارتباطی امن و پایدار در سطح شبکه به یکی از چالش‌های اساسی پیش روی هر سازمانی تبدیل شده است. با توجه به رشد روزافزون کاربران شبکه‌های کامپیوتری، حجم درخواست‌های آن‌ها بزرگ‌تر و پیچیده‌تر می‌شود. از طرف دیگر امروزه اینترنت به جزء جدایی‌ناپذیری در زندگی و تعاملات کاربران تبدیل شده و بحث دسترس‌پذیری[[1]](#endnote-1) آسان به خدمات بستر اینترنت بیش ‌از پیش مورد توجه قرار می‌گیرد، بدین معنا که ارائه‌دهندگان خدمات ارتباطی [[2]](#endnote-2)موظف هستند خدمات خود را به‌صورت شبانه‌روزی و بدون اختلال و وقفه در اختیار کارخواهان قرار دهند. درصورتی‌که این سازمان‌ها به هر دلیلی در ارائه خدمت دچار مشکل شوند و نتوانند به نحو مطلوب خدمت موردنظر خود را ارائه دهند با چالش‌های جدی از قبیل از بین رفتن اعتماد مشتریان، خسارات سنگین مالی و ازبین رفتن اعتبار سازمان مواجه می‌شوند .[1]

حملات منع خدمت[[3]](#endnote-3)، دسته‌ای از حملات در شبکه هستند که با هدف از بین بردن دسترس‌پذیری شبکه سعی در ممانعت از انجام یک خدمت در شبکه دارند. گونه‌های مختلفی از این حملات وجود دارد که هرکدام به طریقی سعی می‌کنند دسترس‌پذیری شبکه را هدف قرار داده و یا با مصرف منابع خدمت‌دهنده، مانع از ارائه خدمت به‌صورت کامل و باکیفیت به کاربران قانونی شوند. حملات منع خدمت توزیع‌شده [[4]](#endnote-4)یک‌گونه مخرب‌تر از حملات منع خدمت هستند که در آن‌ها حمله‌کننده[[5]](#endnote-5) از طریق بات[[6]](#endnote-6)‌ها و سامانه‌[[7]](#endnote-7)هایی که تحت کنترل خود دارد حمله را انجام می‌دهند. بدین ترتیب علاوه بر حجم ترافیک سنگین‌ حملات و دشواری‌های ایجاد تمایز بین ترافیک قانونی شبکه و ترافیک حمله‌کننده، پیدا کردن حمله‌کننده اصلی نیز به‌مراتب دشوارتر می‌شود[2]. با‌‌ توجه به مخرب بودن این حملات پژوهش‌های فراوانی به‌منظور تشخیص و جلوگیری از وقوع آن‌ها انجام‌شده و روش‌های مختلفی در این زمینه ارائه‌شده است. با این‌حال، هم چنان این حملات یکی از تهدید‌های بزرگ در شبکه‌های مختلف محسوب می‌شوند. بر اساس گزارش آزمایشگاه کسپرسکی[[8]](#endnote-8) در سال 2017 از هر سه کسب‌وکار جدید، حداقل یکی با حملات منع خدمت مواجه شده ‌است[3]. در گزارش منتشرشده توسط آزمایشگاه‌ مک‌‌آفی[[9]](#endnote-9) به‌طور واضح حملات منع خدمت توزیع‌شده را به‌عنوان سومین حمله از منظر بزرگی در لیست حملات امنیتی شبکه طبقه‌بندی می‌کند و معتقدند در آینده تنوع و پیچیدگی این حملات بیشتر می‌شود[3].

معماری شبکه‌های فعلی دارای محدودیت‌های بسیاری می‌باشند که همین محدودیت‌ها موجب کاهش نوآوری در فنّاوری شبکه شده است. لذا محققین حوزه شبکه به‌منظور ایجاد بستر‌های تحقیقاتی و افزایش نوآوری در شبکه‌های سنتی با تغییر در معماری آن‌ها، معماری‌های کاربردی

و جدیدتری ارائه داده‌اند. معماری شبکه‌های نرم‌افزار محور[[10]](#endnote-10) یکی از معماری‌های نوظهوری است که با هدف افزایش انعطاف‌پذیری در شبکه‌های فعلی و بهبود مدیریت در آن ارائه‌شده است. در این معماری با جدا شدن بخش کنترلی[[11]](#endnote-11) از بخش داده[[12]](#endnote-12)، مزایای زیادی از قبیل قابلیت برنامه‌ریزی نرم‌افزاری، ایجاد یک کنترل مرکزی روی همه مؤلفه‌‌[[13]](#endnote-13)های شبکه، به وجود آمدن یک دید جامع و انتزاعی و پیکربندی پویا ایجاد شده‌است. قابلیت‌های شبکه‌های نرم‌افزار محور به مدیران شبکه کمک می‌کند کنترل متمرکزی روی تمامی مؤلفه‌‌های شبکه داشته باشند و نظارت بهتری بر روی بسته‌های عبوری داشته باشد. به همین دلیل شبکه‌های نرم‌افزار محور می‌توانند فرآیند تشخیص و جلوگیری از حملات منع خدمت در سطح شبکه را ساده‌تر کنند[4].

این گزارش در ۵ بخش تدوین‌شده است. در بخش 2 مفاهیم پایه موردنیاز در این پژوهش‌ معرفی می‌شوند. ابتدا معماری شبکه‌های نرم‌افزار محور بیان می‌شود. سپس انواع حملات منع خدمت، از نقطه‌نظرهای مختلف موردبررسی قرار می‌گیرند و در انتهای این بخش مفهوم یادگیری ماشین و الگوریتم‌های موجود بر پایه یادگیری ماشین توضیح داده می‌شود. در بخش 3 به بررسی کار‌های پیشین انجام‌شده برای تشخیص حملات منع خدمت پرداخته می‌شود. در بخش 4 روش پیشنهادی به‌منظور بهبود تشخیص حمله در این معماری بیان می‌شود و سرانجام در بخش 5 نتیجه‌گیری، مراحل انجام پروژه و زمان‌بندی آن را بیان خواهد شد.

**2 مفاهیم پایه**

2**.**1 **مقدمه**

در این بخش به شرح مختصری از مفاهیم پایه مرتبط با این پژوهش‌خواهیم پرداخت. ابتدا شبکه‌های نرم‌افزار محور را معرفی می‌کنیم. سپس به معرفی حملات منع خدمت و حملات منع خدمت توزیع‌شده می‌پردازیم و در پایان این بخش مفهوم یادگیری ماشین را شرح می‌دهیم.

2.1.1 **شبکه‌های نرم‌افزار محور**

مؤلفه‌‌های مختلف شبکه هرکدام عناصری هستند که به‌منظور انجام یک عمل خاص در شبکه طراحی‌شده‌اند. به‌طورکلی تمامی‌ این مؤلفه‌‌ها از سه لایه اصلی سخت‌افزار، سیستم‌عامل و نرم‌افزار تشکیل‌شده‌اند. مجموعه این سه لایه در قالب یک بسته[[14]](#endnote-14) جامع در کنار یکدیگر عملکرد مورد هدف مؤلفه‌ را انجام می‌دهند. با تحولات صورت گرفته در رایانه‌های بزرگ اولیه[[15]](#endnote-15) و جداسازی لایه‌های مختلف تشکیل‌دهنده آن‌ها، عرصه‌های مختلف و فضای رقابتی متفاوتی ایجاد شد. رقابت ایجادشده بین شرکت‌های تولیدکننده و ارائه‌دهنده لایه‌ها، موجب شد تا سرعت رشد فنّاوری و نوآوری‌ها چند برابر شود و پیشرفت شگرفی در زمینه‌ی دستگاه‌های کامپیوتری و محاسباتی صورت پذیرد. تحولی که بسیاری از پژوهشگران حوزه شبکه معتقدند با الهام گرفتن از آن می‌توانند سرعت رشد نوآوری در شبکه‌ها را بیشتر و محدودیت‌های شبکه فعلی را کمتر و مدیریت شبکه را راحت‌تر کنند. معماری شبکه فعلی دارای محدودیت‌های بسیاری است[4]. در ادامه برخی از این محدودیت‌ها بیان می‌شوند:

* عدم پویایی بالا در شبکه‌ها: بدین معنا که هر شبکه تقریباً یک‌بار پیکربندی‌شده و بعد از آنکه شبکه طراحی و پیکربندی[[16]](#endnote-16) شد اِعمال تغییر هرچند جزئی در خط‌مشی‌های شبکه بسیار دشوار خواهد بود.
* امکان به وجود آمدن سیاست‌های متناقض در بین اجزای مختلف شبکه: به‌طور مثال با اضافه شدن یک ماشین مجازی[[17]](#endnote-17) جدید به شبکه، نیاز به پیکربندی مجدد در سراسر شبکه است. لذا پیکربندی و ایجاد انطباق در شبکه، بسیار زمان‌بر خواهد بود. با توجه به پیچیدگی شبکه‌های امروزی، رسیدن به یک مجموعه منسجم از سطوح دسترسی، امنیتی و کیفیت خدمات[[18]](#endnote-18) پیکربندی مجدد را بسیار دشوار می‌سازند.
* افزایش پیچیدگی و مدیریت دشوار شبکه: باگذشت زمان و بالا رفتن حجم درخواست‌ها، تنوع درخواست‌ها و افزایش کاربران، پیچیدگی بیشتر شده لذا مدیریت جامع و متمرکز روی مؤلفه‌‌های شبکه را بسیار دشوار کرده است.
* وابستگی طراحی شبکه به تولیدکننده مؤلفه مختلف شبکه: مؤلفه‌‌هایی که در عمل قرار است یک کار مشخص را انجام دهند ممکن است طراحی داخلی متفاوت از هم داشته باشند که سازگاری در شبکه را با چالش روبرو می‌کند.
* دشواری پیکربندی شبکه‌های بزرگ: در شبکه‌های فعلی مدیران شبکه مجبورند که به‌طور دستی و با داشتن دسترسی فیزیکی به هر مؤلفه‌ شبکه سياست‌های سطح بالا موردنیاز را به دستورات پيکربندی سطح پایين تبدیل کنند. بدین ترتیب برای هر بار پیکربندی هرکدام از مؤلفه‌ها باید در محلی که آن مؤلفه‌ وجود دارد حاضرشده و عمل پیکربندی را انجام دهند.
* عدم پویایی در پیکربندی شبکه: مدیران شبکه برای ایجاد هرگونه تغییر حتی جزئی در هم‌بندی مجبور خواهند بود شبکه را مجدد پیکربندی کنند.

وجود محدودیت در شبکه‌های سنتی در کنار پیشرفت فناوری‌های مرتبط با آن، افزایش حجم ترافیک و تعداد کاربران و همچنین ضرورت کاهش هزینه‌ها در کنار ارائه خدمات بهتر و باکیفیت‌تر، عوامل پیشرانه‌ای برای تحول و پیشرفت شبکه‌های فعلی هستند و موجب شکل‌گیری ساختار‌های جدید می‌شوند. از معماری شبکه‌های نرم‌افزار محور می‌توان به‌عنوان یکی از مهم‌ترین نتایج این تحولات شبکه نام برد. مفهوم شبکه‌های نرم‌افزار محور مفهومی است که به‌تدریج درحال‌توسعه و صنعتی‌ شدن است[4].

2.1.2 **تاریخچه پیدایش شبکه‌ نرم‌افزار محور**

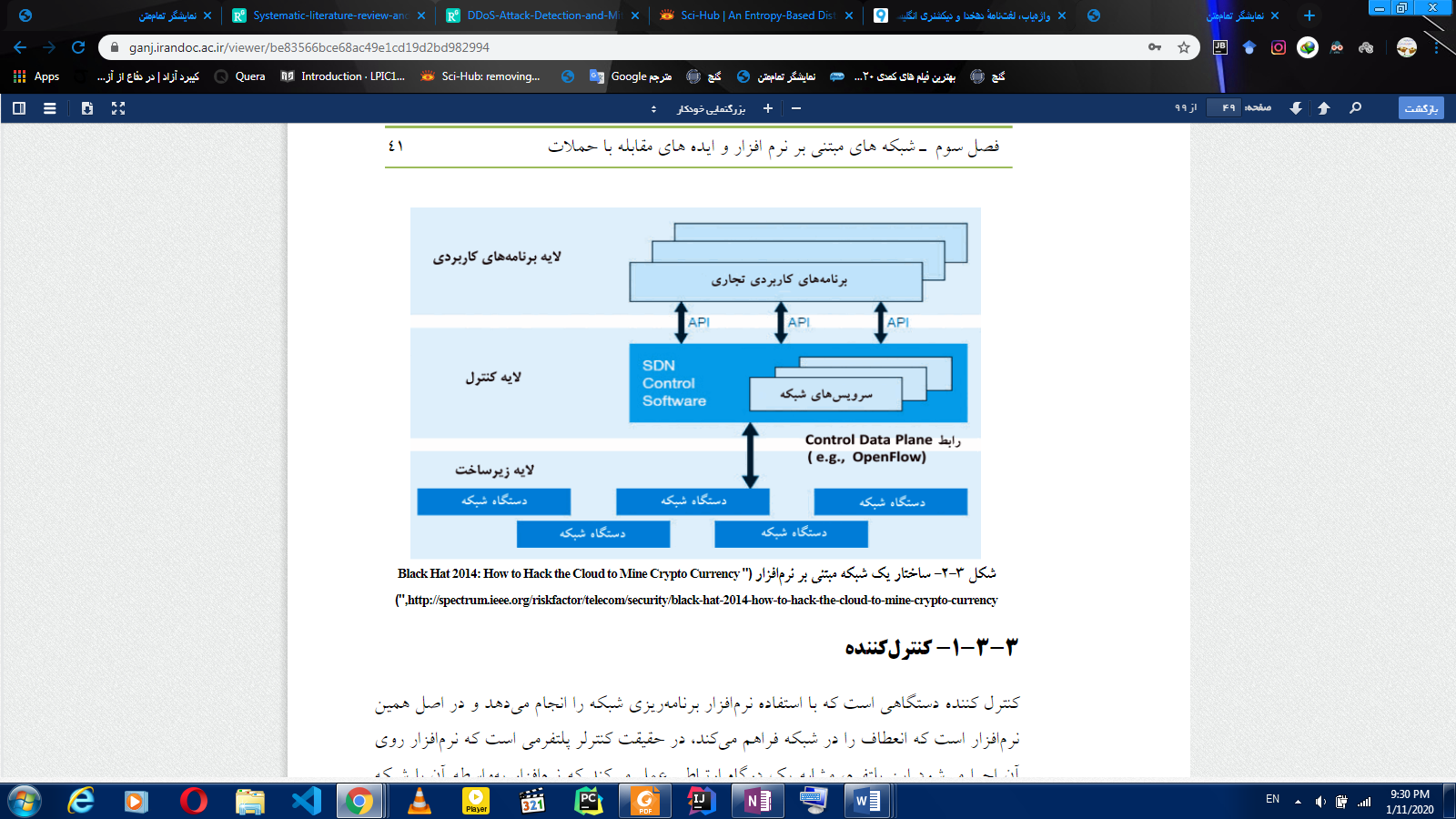
با رشد روزافزون و پیدایش شبکه‌های مختلف، مدیریت آن‌ها با چالش‌های فراوانی روبرو شد.. چراکه علی‌رغم تاثیرگذاری ایجاد زیرشبکه‌ها در تقسیم شدن حجم ترافیکی، لیکن درنهایت این زیرشبکه‌ها نیازمند به داشتن ارتباط با یکدیگر بودند. برای حل این مشکل پروتکل‌های مسیریابی[[19]](#endnote-19) ارائه شدند تا بر اساس سیاست‌های از قبل تعیین‌شده، مسیر مناسب تا مقصد انتخاب‌شده و بسته‌ها در بستر اینترنت ارسال شوند. با گذشت زمان و گسترده شدن شبکه، مشکل به شکل دیگری ظاهر شد. پروتکل‌های مسیریابی نیازمند دریافت اطلاعات مسیرها در فواصل زمانی خاص بودند تا بتوانند جداول مسیریاب خود را به‌روز کنند. این امر بار ترافیکی زیادی را بر شبکه تحمیل می‌کرد. درنهایت ایده بازنگری در معماری شبکه‌ها در سال 1998 در دانشگاه استنفورد[[20]](#endnote-20) و توسط مارتین کسادا مطرح شد. با توجه به نتایج ضعیف حاصل این ایده مسکوت ماند. در سال 2005 و با توجه به احساس نیاز شدید به طرح تحول بنیادی در شبکه‌ها، بنیاد ONF3 تشکیل شد و تحقیقات بر روی این نوع معماری دوباره انجام شد که درنهایت به ارائه معماری شبکه‌های نرم‌افزار محور منجر گردید. شبکه‌های نرم‌افزار محور معماری جدیدی در حوزه شبکه است که قصد دارد با جداسازی سخت‌افزار هدایت جریان‌ها از تصميمات کنترلی و افزودن قابلیت‌های ویژه به شبکه، مدیریت شبکه را راحت‌تر کند. در شبکه‌های نرم‌افزار محور هوش شبکه به‌صورت منطقی در کنترل‌کننده متمرکزشده است و سخت‌افزار شبکه تبدیل به یک وسيله ساده برای هدایت بسته می‌شود که از طریق واسط‌های برنامه‌نویسی قابل‌برنامه‌ریزی می‌باشد[7].

2.1.3 **قابلیت‌های ایجاد‌شده توسط شبکه نرم‌افزار محور**

ازجمله قابلیت‌های ایجادشده توسط شبکه‌های نرم‌افزار محور می‌توان به مدیریت آسان‌تر، تأمين کيفيت خدمت، افزایش امنيت و انعطاف‌پذیری شبکه، افزایش کنترل قانونمند شبکه، هوشمندی عملکرد شبکه و کنترل متمرکز تجهيزات توليدکننده‌های مختلف، عدم وابستگی به شرکت‌های فروشنده سخت‌افزار، سرعت در به‌روزرسانی تجهيزات شبکه و سرعت در ایجاد تغييرات در سیاست‌های شبکه اشاره کرد.

2.1.4 **معماری شبکه نرم‌افزار محور**

بعد از آشنایی مختصر با تاریخچه و همچنین انگیزه پیدایش شبکه‌های نرم‌افزار محور، در ادامه به بررسی دقیق‌تر معماری شبکه‌های نرم‌افزار محور خواهیم پرداخت. شبکه‌های نرم‌افزار محور باهدف ساده شدن مدیریت شبکه و هوشمندی شبکه‌ها به وجود آمدند. در معماری این شبکه‌ها قسمت کنترلی از قسمت سخت‌افزاری تجهیزات شبکه از هم تفکیک‌ شده‌اند و بخش کنترلی داده‌ها از راه‌گزین به لایه‌های نرم‌افزاری منتقل ‌شده است، که این امر باعث می‌شود تا قابليت برنامه‌پذیری، مقياس‌پذیری و انعطاف‌پذیری را از طریق توسعه نرم‌افزاری در شبکه فراهم شود. به‌طورکلی معماری شبکه‌های نرم‌افزار محور از سه لایه اصلی " لایه زیرساخت یا صفحه داده "، " لایه کنترل "، " لایه برنامه کاربردی" تشکیل ‌شده است که این لایه‌ها به کمک رابط‌های میانی با یکدیگر در ارتباط هستند. شکل 1 نمایی کلی از معماری شبکه‌های نرم‌افزار محور را نشان می‌دهد که بخش هوشمند شبکه به‌طور منطقی در کنترل‌کننده مرکزی شبکه قرار دارد. بنابراین شبکه از دید برنامه کاربردی به صورت یک راه‌گزین منطقی واحد به نظر خواهد رسيد[7,8].



شکل 1 نمای کلی از معماری شبکه نرم‌افزار محور

* لایه زیرساخت[[21]](#endnote-21) یا صفحه داده: پایینی‌ترین لایه معماری شامل همه مؤلفه‌‌های سخت‌افزاری مختلف نظیر راه‌گزین[[22]](#endnote-22)‌ها، مسیریاب[[23]](#endnote-23)‌ها و گره‌های نظیر آن در سطح شبکه است. ازآنجایی‌که در این معماری بخش کنترلی از بخش داده جداشده است، تمامی مؤلفه‌‌های موجود در این لایه تنها وظیفه جا‌به‌جایی بسته‌ها در سطح شبکه را بر اساس خط‌مشی‌های از قبل مشخص در جداول مسیریابی و یا خط‌مشی‌هایی که توسط لایه کنترلی مشخص می‌شود، بر عهده خواهند داشت.
* لایه کنترل: در معماری ارائه‌شده برای شبکه نرم‌افزار محور، بخش کنترلی جداشده از تمامی مؤلفه‌‌های شبکه به صورت متمرکز در لایه کنترل‌ قرار می‌گیرد. این لایه شامل یک کنترل‌کننده[[24]](#endnote-24) مرکزی است که درواقع همان واحد هوشمندی در این معماری می‌باشد و دستورات کنترلی را به واسطه پروتکل ارتباطی اُپن‌فلو[[25]](#endnote-25) به مؤلفه‌‌های سخت‌افزاری موجود در لایه زیرساخت منتقل می‌کند. همان‌طور که در شکل 1 مشخص است این لایه می‌تواند متشکل از چندین کنترل‌کننده مجزا باشد که به کمک واسط‌های شرقی و غربی با کنترل‌کننده‌های اطراف در ارتباط خواهند بود.
* لایه کاربرد: در این لایه مدیران شبکه با استفاده از واسط‌های برنامه‌نویسی مناسب، نیازهای خود را محقق می‌کنند. در این معماری، شبکه از طریق برنامه‌های کاربردی و به شکل نرم‌افزاری که روی کنترل‌کننده‌ها اجرا می‌شوند و در تعامل با دستگاه‌های لایه داده هستند برنامه‌ریزی می‌شود. این برنامه‌ها شامل مواردی چون کیفیت خدمت، کنترل دسترسی، مباحث مربوط به امنیت شبکه و مواردی ازاین‌دست می‌باشد.

2.1.5 **پروتکل اُپن‌فلو**

یک پروتکل ارتباطی است که امکان پيکربندی راه‌گزین‌ها و مسيریاب‌های شبکه را برای ما فراهم می‌کند. این پروتکل به‌عنوان رایج‌ترین پروتکل ارتباطی بين کنترل‌کننده و راه‌گزین در شبکه نرم‌افزار محور مطرح است. راه‌گزین‌هایی که از این پروتکل پشتيبانی می‌کنند، شامل یک یا چند جدول مسيریابی و یک جدول گروه هستند که عمليات یافتن درگاه[[26]](#endnote-26) خروجی برای بسته‌های ورودی و انتقال بسته‌ها را انجام می‌دهد. پروتکل برای ارتباط بين کنترل‌کننده و راه‌گزین یک واسط برنامه کاربردی تعریف می‌کند و به کمک آن ارتباط را برقرار می‌سازد. این پروتکل به کنترل‌کننده این قابلیت را می‌دهد تا بتواند از راه دور به مؤلفه‌‌های موجود در شبکه دسترسی داشته و خط‌مشی[[27]](#endnote-27)‌های موردنیاز را به آن‌ها ابلاغ کند. از جمله خط‌مشی‌های مذکور می‌توان به مواردی مانند اضافه کردن[[28]](#endnote-28)، حذف[[29]](#endnote-29) و یا به‌روزرسانی[[30]](#endnote-30) یک مسیر مشخص در شبکه و یا متوقف کردن موقت یا دائم ارسال بسته‌ها به یک راه‌گزین خاص اشاره کرد[8].

2.1.6 **هدایت بسته‌ها در معماری شبکه‌های نرم‌افزار محور**

راه‌گزین‌های موجود در معماری شبکه‌های نرم‌افزار محور، راه‌گزین‌های مخصوصی هستند که در کنار تمامی قابلیت‌هایی که در شبکه‌های سنتی دارند، دارای قابلیت ارتباط با کنترل‌کننده مرکزی از طریق پروتکل‌های اُپن‌فلو و یا پروتکل‌های ارتباطی مشابه هستند. عملیات هدایت بسته‌ها در این معماری، مشابه عملیات مسیریابی در شبکه‌های سنتی خواهد بود با این تفاوت که اگر بسته‌ای به راه‌گزین برسد و آدرس مقصد بسته در جدول مسیریابی راه‌گزین وجود نداشته باشد، به کمک پیام‌های ارتباطی اُپن‌فلو سرآیند بسته دریافتی را به کنترل‌کننده مرکزی شبکه ارسال می‌کند. کنترل‌کننده مرکزی در مورد اِعمال خط‌مشی بسته دریافت شده، تصمیم می‌گیرد و پاسخ را در قالب یک پیام اُپن‌فلو به راه‌گزین ارسال می‌کند. اگر آدرس مقصد در جدول مسیریابی موجود باشد و هیچ پیام منع‌کننده‌ای از جانب کنترل‌کننده مرکزی برای آن آدرس خاص وجود نداشته باشد، عمل هدایت[[31]](#endnote-31) بسته مشابه روش موجود در شبکه سنتی مبتنی به مقصد موردنظر، فرستاده می‌شود. تأثیر مثبت حضور کنترل‌کننده مرکزی در هدایت بسته‌ها در این معماری قابل ‌درک است. کنترل‌کننده به کمک دید جامعی که از بالا بر وضعیت فعلی شبکه و ترافیک عبوری دارد، می‌تواند از وقوع ازدحام[[32]](#endnote-32) در یک پیوند یا راه‌گزین خاص جلوگیری کند و مسیر‌های جایگزینی را بدون تأخیر قابل توجهی برای هدایت بسته‌ها تعیین کند[9]. اتفاقی که در شبکه‌های سنتی رخ نمی‌دهد و راه‌گزین‌ها از وضعیت کلی شبکه باخبر نیستند و عملیات یافتن مسیر جایگزین به صورت تصادفی انجام می‌شود. این ویژگی شبکه‌ نرم‌افزار محور در کنار قابلیت استفاده حداکثری از امکانات شبکه در راستای بهبود کیفیت خدمات، این امکان را به مدیران شبکه می‌دهد تا در لحظه و به صورت پویا قابلیت مشاهده وضعیت کلی شبکه را داشته باشند و در صورت تشخیص وقوع حملاتی نظیر منع خدمت توزیع‌شده عملیات مقابله با حملات را با سرعت بیشتر و قبل از اینکه به شبکه آسیب زیادی برسد آغاز کنند[11].

2.2 **حملات منع خدمت**

به مجموعه حملاتی که با هدف ممانعت از انجام یک خدمت صورت می‌پذیرند، حملات منع خدمت گفته می‌شود. این حملات با انگیزه‌های مختلفی نظیر ایجاد اختلال یا ممانعت از ارائه یک خدمت، از بین بردن اعتبار و مقبولیت یک سازمان، آسیب زدن مالی و هدر دادن منابع یک سازمان، دستاوردهای سیاسی و ملی، انگیزه مالی و یا قدرت‌نمایی مهاجمین و مواردی از این دست می‌تواند صورت پذیرد. حملات منع خدمت توزیع‌شده گونه بسیار خطرناک از حملات منع خدمت هستند که در آن مهاجم با استفاده از در اختیار گرفتن کنترل تعداد زیادی کامپیوتر آلوده‌شده که در نقاط مختلف در سطح اینترنت توزیع‌ شده‌اند اقدام به انجام حمله می‌کند. بدین ترتیب رهگیری مبدأ حمله دشوارتر و همچنین ترافیک ایجادشده در اثر حمله بزرگ‌تر و مخرب‌تر خواهد بود[12].

2.2.1 **رویه کلی حملات منع خدمت توزیع‌شده**

باوجوداینکه گونه‌های متفاوتی از حملات منع خدمت توزیع‌شده وجود دارد که هرکدام با روشی منحصربه‌فرد حمله را انجام می‌دهند، می‌توان در یک دید کلی و مجرد چهار مؤلفه اصلی برای انجام یک حمله منع خدمت توزیع‌شده در نظر گرفت. این چهار مؤلفه عبارت‌اند از: حمله‌کننده[[33]](#endnote-33) اصلی، کنترل‌کننده حمله، عامل‌[[34]](#endnote-34)ها و قربانی[[35]](#endnote-35). حمله‌کننده اصلی خود می‌تواند کنترل‌کننده حمله باشد و یا کنترل حمله را به یک سیستم آلوده‌شده توسط حمله‌کننده بسپارد. به‌طورکلی رویه حملات منع خدمت به این صورت است که تعدادی کامپیوتر که با روش‌های مختلف تحت کنترل حمله‌کننده قرار دارند بعد از صادر شدن دستور حمله، شروع به ارسال بسته به سمت سیستم قربانی می‌کنند[14].

2.2.2 **اهداف موردحمله حملات منع خدمت** **توزیع‌شده**

معمولا حملات منع خدمت توزیع‌شده با دسته‌ای از حملات شناخته می‌شوند که با ارسال زیاد بسته‌ و اشغال پهنای باند شبکه سعی در ممانعت از انجام یک خدمت دارند. اما دسته‌ی دیگری از حملات منع خدمت وجود دارند که منابع دیگر قربانی را مورد هدف قرار می‌دهند. موارد زیر بخش‌های متداولی هستند که این حملات معمولا آن‌ها را تحت تاثیر قرار می‌دهد[14].

* شبکه: یکی از اصلی‌ترین اهداف حملات منع خدمت از بین بردن دسترس‌پذیری شبکه به‌منظور ممانعت از استفاده از یک خدمت ارائه‌شده با ارائه خدمت یک توسط قربانی می‌باشد. شبکه‌ها با ارسال زیاد بسته‌ به صورت سیل‌آسا به سمت قربانی یا درخواست محتوای حجیم از قربانی، مشغول می‌شوند.
* زیرساخت: از دیگر اهداف حملات منع خدمت، حمله به زیرساخت شبکه موجود و از کار انداختن یا ایجاد اختلال در انجام فعالیت عناصر موجود در شبکه می‌باشد.
* منابع پردازشی: حمله‌کننده در این هدف قصد مشغول ساختن منابع پردازشی موجود در شبکه را دارد تا این منابع از ارائه خدمت به کاربران معمولی باز بمانند یا به کیفیت این خدمت خدشه وارد کنند.
* برنامه‌های کاربردی: مقصود از حمله به برنامه‌های کاربردی جلوگیری یا ایجاد اختلال در از ارائه یک خدمت خاص در سطح شبکه است.

2.2.3 **دسته‌بندی حملات منع خدمت توزیع‌شده**

حملات منع خدمت را از جنبه‌های مختلفی می‌توان دسته‌بندی کرد و حملات مختلف بر اساس اینکه چه معیاری برای دسته‌بندی مدنظر هست در یکی از دسته‌های موجود قرار می‌‌گیرند[16].

2.2.3.1 **انواع حملات منع خدمت از منظر پروتکل**

یکی از رایج‌ترین دسته‌بندی حملات منع خدمت، دسته‌بندی این حملات بر اساس لایه‌ا‌ی از شبکه است که حمله به کمک پروتکل‌های موجود در آن لایه آغازشده است. حملات منع خدمت می‌تواند از یکی از دو لایه شبکه/انتقال و لایه کاربرد آغاز شوند. آمار‌های منتشرشده اخیر حکایت از این موضوع دارد که با مرور زمان حجم حملات انجام‌شده از طریق پروتکل لایه شبکه/انتقال رو به کاهش و حملات مبتنی بر لایه کاربرد در حال افزایش است.

* حملات موجود در لایه شبکه/انتقال: این دسته از حملات از آسیب‌پذیری‌های موجود در لایه شبکه/انتقال و پروتکل‌های موجود در آن برای انجام حمله استفاده می‌کنند.ازنظر عملکردی و نوع پروتکل مورداستفاده این دسته از حملات را به چهار زیر دسته کلی می‌توان قسمت کرد:

1. حملات سیل‌آسا[[36]](#endnote-36): در این دسته از حملات مهاجم قصد دارد تا با ارسال بسته‌های زیاد در سطح شبکه سعی در اشباع کردن پهنای باند قربانی دارد تا قربانی را از دریافت خدمت در شبکه منع کند.

2. حملات سیل‌آسا بهره‌برداری از پروتکل: اکثر این حملات از آسیب‌پذیری و نقص در پیاده‌سازی موجود در یک پروتکل خاص و یا ویژگی‌هایی که مختص یک پروتکل مشخص هست برای شروع حمله استفاده می‌شود. به‌عنوان‌مثال استفاده از ضعف در الگوریتم دست ‌تکانی سه مرحله‌ای پروتکل تی.سی.پی.

3. حملات سیل‌آسا مبتنی بر بازتاب[[37]](#endnote-37): این نوع حمله، حمله‌کننده قربانی را به جای خود معرفی می‌کند و درخواستی را به کارپذیر ارسال می‌کند و کارپذیر این درخواست را به صورت همه‌پخشی به تمامی میزبان‌های موجود ارسال می‌کند و پاسخ از جانب میزبان‌ها به قربانی ارسال می‌شود. پروتکل درخواست و پاسخ در این حمله مشابه هستند و حجم بسته ارسالی به قربانی به تعداد میزبان‌های موجود در شبکه بستگی دارد.

4. حملات سیل‌آسا مبتنی بر تقویت[[38]](#endnote-38): در این نوع حملات مهاجم با جعل آدرس قربانی و معرفی کردن قربانی به جای خود درخواستی با طول کوتاه و پاسخ بلند را از کارپذیرهای موجود درخواست می‌کند و این پاسخ توسط کارپذیر به قربانی ارسال می‌شود. در این حمله پروتکل درخواست و پاسخ متفاوت است و اندازه حمله به طول و تعداد پاسخ‌هایی که به سمت قربانی ارسال می‌شوند بستگی دارد.

* حملات موجود در لایه برنامه‌کاربردی: در این دسته از حملات، حمله‌کننده سعی دارد تا حمله را به کمک پروتکل‌های موجود در لایه کاربردی و با اتصالی مشابه اتصال کاربران قانونی انجام دهد. این حملات تلاش می‌کنند تا با مصرف منابع قربانی نظیر پردازنده، حافظه، دیسک سخت و مواردی از این قبیل در ارائه خدمت توسط قربانی اختلال ایجاد کنند و به مراتب پهنای باند کم‌تری نسبت به حملات لایه شبکه/انتقال مصرف می‌کنند. ازآنجایی‌که ترافیک حمله سعی دارد مشابه ترافیک کاربران قانونی باشد، ایجاد تمایز بین ترافیک حمله‌کننده و ترافیک معمولی از چالش‌های جدی در تشخیص این‌گونه حملات خواهد بود. این حملات به دو دسته‌ی حملات سیل‌آسا مبتنی بر تقویت/بازتاب و حملات سیل‌آسا اِچ‌.تی.‌تی.‌پی[[39]](#endnote-39) تقسیم می‌شوند.

1. حملات سیل‌آسا مبتنی بر تقویت/بازتاب: ایده این حملات مشابه روش حملات در دسته قبل است و حمله‌کننده با تولید درخواست‌های کوتاه و ارسال پاسخ‌هایی با تعداد زیاد و همچنین بزرگ سعی در انجام حمله‌دارند.

2. حملات سیل‌آسا اِچ.‌تی.‌تی.‌پی: این حملات از پروتکل پرکاربرد اِچ‌.تی.‌تی.‌پی برای انجام حمله استفاده می‌کنند به کمک این پروتکل چهار حمله رایج صورت می‌پذیرد.

* + - حمله سیل‌آسای نشست: در این حمله به کمک شبکه‌های باتی که در اختیار حمله‌کننده قرار دارد حجم زیادی درخواست اِچ‌.تی‌.تی.‌پی معتبر به سمت قربانی ارسال می‌شود و با توجه به اینکه حجم درخواست‌های بسیار بیشتر از درخواست‌های کاربران قانونی است، قربانی را دچار مشکل می‌کند.
    - حمله سیل‌آسای درخواست: در این حمله، حمله‌کننده یک نشست قانونی ایجاد کرده و سپس شروع به حجم زیادی درخواست از سیستم قربانی می‌کند.
    - حمله غیرمتقارن: در این حملات حمله‌کننده در یک نشست چندین درخواست با بار کاری بالا را در قالب یک درخواست به سمت قربانی می‌فرستد و سعی در مشغول کردن قربانی دارد.
    - حمله درخواست/پاسخ آهسته: این حمله مشابه حالت قبلی است با این تفاوت که درخواست‌ها به‌مرور برای قربانی ارسال می‌شود تا منابع قربانی مشغول شوند.

2.3 **یادگیری ماشین**

در[6] تعریف یادگیری ماشین به این‌گونه بیان‌شده است: «یک برنامه کامپیوتری از یک تجربه آموزشی با نام E، یادگیری خواهد داشت اگر با در نظر گرفتن یک سری از وظایف به نام T و یک معیار اندازه‌گیری کارایی به نام P، با گذراندن تجربه E، کارایی آن در انجام وظایف T با توجه به معیار P بهبود داشته باشد «.

به طور کلی الگوریتم‌های یادگیری ماشین به سه دسته یادگیری با نظارت[[40]](#endnote-40)، یادگیری بدون نظارت[[41]](#endnote-41) و یادگیری تقویتی[[42]](#endnote-42) تقسیم می‌شوند.

2.3.1 یادگیری با نظارت

مجموعه آموزش در یادگیری با نظارت، به صورت زوج مرتب داده و خروجی متناظر با داده است که برچسب[[43]](#endnote-43) نامیده می‌شود. در این روش هدف یادگیری یک نگاشت از داده‌های ورودی X به خروجی Y با داشتن مجموعه آموزش است. داده‌های ورودی در واقع همان بردارهای ویژگی هستند و اگر دامنه مقادیر خروجی گسسته باشد، مسئله یادگیری ما دسته‌بندی[[44]](#endnote-44) نامیده می شود. مثال‌هایی از دسته‌بندی شامل دسته‌بندی تصویر، شناسایی دست خط، شناسایی چهره و پالایش هرزنامه می‌باشد. چنانچه دامنه مقادیر خروجی یک مجموعه پیوسته مثل مجموعه اعداد حقیقی باشد، مسئله یادگیری را رگرسیون[[45]](#endnote-45) می‌نامیم. از مثال‌های رگرسیون می‌توان به انواع پیش‌بینی‌ها مثل پیش‌بینی بورس و دمای هوای منطقه اشاره داشت.[17]

2.3.2 یادگیری بدون نظارت

هدف از این نوع یادگیری پیدا کردن یک الگوی قابل‌توجه در مجموعه داده‌ها است. در این نوع یادگیری مجموعه آموزش تنها از داده‌های بدون برچسب تشکیل می‌شود. سه کاربرد مهم یادگیری بدون نظارت در خوشه‌بندی[[46]](#endnote-46)، کاهش ابعاد داده و فشرده‌سازی است. در خوشه‌بندی سعی می‌شود تا بر اساس سنجه موردنظر، داده‌های مشابه در یک خوشه قرار داده شوند. از کاربردهای آن می‌توان به تشخیص ناهنجاری اشاره نمود. در کاهش بُعد سعی می‌کنند تا داده‌ها را به فضایی با ابعاد کوچک‌تر ببرند[17].

2.3.3 یادگیری تقویتی

به فرایند یادگیری به‌وسیله تعامل با محیط، یادگیری تقویتی می‌گویند. یک عامل در یادگیری تقویتی، از دستاورد عمل خویش آموزش می‌بیند. به‌عبارت‌دیگر، در این مدل، برخلاف یادگیری با نظارت، به یادگیرنده آموزش داده نمی‌شود که کدام عمل را انجام دهد. بلکه، یادگیرنده باید خودش با امتحان کردن کشف کند که کدام عمل بیشترین پاداش[[47]](#endnote-47) را دارد. در این یادگیری، یک عامل هدفمند در اثر تعامل با یک محیط غیرقطعی و انجام کنش[[48]](#endnote-48) روی آن، حالت مناسب از آن کنش و پاداش خود را دریافت می‌کند. آزمون ‌و خطا و پاداش با تأخیر، دو مورد از مهم‌ترین ویژگی‌های یادگیری تقویتی هستند. چهار عنصر کلیدی در یادگیری تقویتی شامل خط‌مشی، تابع پاداش، ارزش و مدل محیط است. تابع خط‌مشی یک نگاشت از حالت دریافتی از محیط به کنش اتخاذشده است. تابع پاداش هم یک نگاشت از زوج حالت-کنش به سیگنال تقویتی ایجاد می‌کند که نشان‌دهنده میزان خوب بودن کنش اتخاذشده است[17].

3 **کارهای ‌پیشین**

**با توجه به اهمیت موضوع حملات منع خدمت توزیع‌شده، در سال‌های گذشته پژوهش‌های بسیاری در این زمینه صورت گرفته است.** شبکه‌های نرم‌افزار محور و قابلیت‌هایی که این نوع شبکه‌ها ارائه می‌دهند به پژوهشگران حوزه تشخیص و مقابله با حملات منع خدمت کمک شایانی می‌کند تا با استفاده از ویژگی‌های موجود در این نوع شبکه‌ها، تشخیص و مقابله حملات منع خدمت را سریع‌تر و با دقت بالاتری انجام دهند. **به‌طورکلی پژوهش‌های انجام‌شده در حوزه حملات منع خدمت توزیع‌شده را می‌توان در سه دسته پیشگیری از وقوع حمله، تشخیص حمله و کاهش اثر حمله تقسیم‌بندی کرد. از آنجایی‌که تمرکز این گزارش بر مقالات حوزه تشخیص حملات منع خدمت توزیع‌شده می‌باشد،** در ادامه به معرفی چند روش پرکاربرد دسته تشخیص حملات منع خدمت توزیع‌شده در شبکه‌های نرم‌افزار محور می‎‌پردازیم[9].

3.1**روش‌های مبتنی بر محاسبه آنتروپی**

آنتروپی[[49]](#endnote-49) معیاری است که برای اندازه‌گیری میزان تصادفی یک ویژگی در یک دوره زمانی معین استفاده می‌شود. روش‌های مبتنی بر آنتروپی به‌عنوان یک رویکرد مؤثر برای محاسبه تصادفی از یک مجموعه داده ایجادشده است. به‌طورکلی مقادیر بالای آنتروپی نشان‌دهنده توزیع پراکنده‌تر ویژگی در دادگان[[50]](#endnote-50) موجود است و مقادیر پایین آنتروپی نشان‌دهنده نامتوازن بودن یک توزیع است یعنی برخی مقادیر ویژگی موردنظر، فراوانی بیشتری نسبت به سایر مقادیر دارند. لذا، از این روش برای تشخیص ناهنجاری گسترده در سامانه‌های سنتی تشخیص نفوذ[[51]](#endnote-51) استفاده‌شده است. به‌منظور تشخیص حملات منع خدمت، آنتروپیِ جریان شبکه را می‌توان با استفاده از چندین ویژگی مانند جریان شبکه، آدرس آی.‌پی[[52]](#endnote-52) مبدأُ و مقصد بسته‌ها و یا تعداد بسته‌های موجود در یک جریان محاسبه کرد. سپس با یک حد آستانه[[53]](#endnote-53) از پیش تعریف‌شده، مقایسه کرد و در مورد نرمال یا غیرنرمال بودن جریان بررسی‌شده، تصمیم‌گیری کرد. یکی از مهم‌ترین مزیت‌های این روش داشتن سربار محاسباتی کم می‌باشد. با توجه به موفقیت الگوریتم‌های مبتنی بر آنتروپی در شبکه سنتی در تشخیص حملات منع خدمت توزیع‌شده، از این روش‌ها در تشخیص حملات در شبکه‌های نرم‌افزار محور نیز استفاده می‌شود[17].

موسوی و همکاران [20]یک روش برای تشخيص زودهنگام حملات منع خدمت توزیع‌شده در برابر کنترل‌کننده‌ شبکه نرم‌افزار محور ارائه داده است. در مدل ارائه‌‌شده از آنتروپی به‌منظور محاسبه میزان تصادفی بودن بسته‌های‌ ورودی به شبکه استفاده می‌شود. هدف اصلی این روش تشخيص حمله در مراحل اوليه حمله می‌باشد. دو مؤلفه ضروری برای تشخيص حملات منع خدمت توزیع‌شده به‌وسیله آنتروپی، تنظيم پنجره زمانی و تنظيم حد آستانه مناسب است. به‌طوری‌که آنتروپی در طول پنجره زمانی برای اندازه‌گيری ميزان تصادفی بودن بسته‌های ورودی، محاسبه ‌می‌شود و برای تشخيص حمله به یک حد آستانه نياز داریم. درصورتی‌که آنتروپی محاسبه‌شده از حد آستانه عبور کرده باشد حمله تشخیص داده می‌شود. زمانی که حجم زیادی از بسته‌های حمله به سمت یک ميزبان یا مجموعه‌ای از ميزبان‌ها ارسال شوند، میزان تصادفی ارسال بسته‌ها دچار تغییر شده و بسته‌ها به یک مقصد مشخص هدایت می‌شوند. این امر موجب کاهش آنتروپی محاسبه‌شده می‌گردد. روال کلی روش بدین ترتیب است که در هر پنجره زمانی کنترل‌کننده آدرس آی‌.پی مقصد موجود در سرآیند بسته‌های ورودی را موردبررسی قرار می‌دهد، اگر آی‌.پی در جدول موجود در کنترل‌کننده جدید باشد، یک سطر حاوی آدرس آی.‌پی مقصد جدید به جدول اضافه می‌شود و درصورتی‌که از قبل یک نمونه از آدرس در جدول موجود باشد به شمارنده آن سطر یک واحد اضافه می‌شود. پس از گذشت یک پنجره زمانی، آنتروپی مربوط به آن پنجره محاسبه و سپس با میزان حد آستانه مقایسه می‌گردد. روش ارائه‌شده واکنشی در مقابل آدرس‌های آی‌.پی که در شبکه موجود نباشند نشان نمی‌دهد. لذا این روش توانایی تشخیص حملات منع خدمت توزیع‌شده‌‌ای که از جعل آی.‌پی استفاده می‌کنند را ندارد.

یک الگوریتم توزیع‌شده به‌منظور تشخیص ناهنجاری مبتنی بر آنتروپی توسط وانگ و همکاران[21] ارائه‌شده است. در روش ارائه‌شده برای هر لبه راه‌گزین‌های لایه زیرساخت در شبکه‌های نرم‌افزار محور، یک واحد تشخیص حمله سیل‌آسا منع خدمت توزیع‌شده در نظر گرفته‌شده است. بدین ترتیب وظیفه جمع‌آوری جریان و محاسبه آنتروپی که در روش‌های ارائه‌شده قبلی بر عهده کنترل‌کننده بود به این واحدها محول می‌شود و سربار محاسباتی کنترل‌کننده شبکه کاهش می‌یابد. در هر واحد بر اساس آدرس آی‌.پی مقصد، آنتروپی محاسبه‌شده و درصورتی‌که آنتروپی هرکدام از راه‌گزین‌های شبکه بیش‌ازحد آستانه تغییر کرده باشد، وقوع حمله سیل‌آسا احتمالی به کنترل‌کننده گزارش داده می‌شود. این روش با هدف کاهش سربار محاسباتی در کنترل‌کننده ایجادشده است و تنها حملاتی را می‌تواند تشخیص دهد که آنتروپی ترافیک عبوری از حد آستانه مشخص‌شده در هر راه‌گزین فراتر رود. با توجه به ویژگی توزیع‌شدگی در حملات منع‌ خدمت، لزوماً ترافیک حمله عبوری از یک راه‌گزین مشخص در شبکه نخواهد گذشت و حملات تنها در گره‌های آخر منتهی به قربانی، آن‌ هم در صورت بر هم خوردن آنتروپی به صورت محسوس، قابل‌شناسایی خواهند بود.

قرویریان و همکاران در [22]، به‌منظور کاهش زمان محاسباتی تشخیص حمله، ضمن حفظ دقت، یک قاعده محاسبه آنتروپی تحت عنوان آنتروپی سریع را به‌جای قاعده آنتروپی معمول ارائه دادند. روال کلی روش مشابه روش‌های قبلی است و برای این منظور ابتدا، آنتروپی سریع برای هر جریان در وقفه‌های زمانی مشخص محاسبه می‌شود. سپس با استفاده از حد آستانه‌ی تطبیق‌پذیر، احتمال وقوع یک حمله منع خدمت توزیع‌شده بررسی می‌شود. برای دستیابی به دقت بیشتر در کنار این روش، از یک روش محاسبه‌ی نرخ آغاز جریان هم استفاده‌شده است. پس از مشاهده‌ی نتایج این دو روش، درصورتی‌که این دو روش وقوع حمله را پیش‌بینی کنند، احتمال وقوع حمله وجود دارد. اگر در هیچ‌کدام از این دو روش وقوع حمله پیش‌بینی نشود احتمالا حمله رخ نداده است و اگر یکی از این دو روش وقوع حمله را تشخیص دهد این تصمیم در مرحله‌ی بعدی با بررسی آمارهای جریان راه‌گزین‌های شبکه توسط شبکه عصبی پِرسِپتِرون، انجام می‌گیرد. نتایج ارزیابی نشان می‌دهد که الگوریتم پیشنهادی توانسته است یک بهبود مهم در نرخ تشخیص و یک کاهش در نرخ اعلام خطا، نسبت به مرتبط‌ترین کارهای قبلی ایجاد نماید و میانگین زمان تشخیص الگوریتم را نیز در یک سطح قابل قبول نگه دارد.

3.**2 روش‌های مبتنی بر یادگیری ماشین**

امروزه استفاده از روش‌های یادگیری ماشین به‌عنوان یک روش کارآمد برای تأمین امنیت مورد استقبال پژوهشگران قرارگرفته است. در حوزه تشخیص حملات منع خدمت توزیع‌شده نیز از این روش استفاده می‌شود. گونه‌های مختلفی از الگوریتم‌های یادگیری نظیر استفاده از ماشین بردار پشتیبان، بیز ساده، نزدیک‌ترین همسایه، شبکه عصبی و شبکه‌های عصبی ژرف، نگاشت خودسازمان‌ده و مواردی از این قبیل به‌منظور انجام طبقه‌بندی جریان مورداستفاده قرار می‌گیرند. با توجه به مشکلات وجود داده برچسب‌دار مناسب، در شبکه واقعی برای آموزش مدل، روش‌های یادگیری تقویتی نیز در این بستر مورد توجه بسیار قرارگرفته است. به‌طورکلی مدل‌های یادگیری که برای تشخیص حمله منع خدمت توزیع‌شده از یادگیری ماشین استفاده می‌کنند از سه واحد اصلی جمع کننده جریان، استخراج‌کننده ویژگی و واحد طبقه‌بند تشکیل‌شده است. واحد جمع‌کننده جریان، وظیفه جمع‌آوری جریان‌های گذرنده از راه‌گزین‌های اُپن‌فلو در بستر شبکه را دارد. واحد استخراج ویژگی، ویژگی‌های موردنیاز مدل یادگیری را استخراج می‌کنند و به واحد طبقه‌بند ارسال می‌کنند. واحد طبقه‌بند بر اساس اطلاعات موجود در مورد حمله یا ترافیک عادی بودن جریان رسیده به مدل تصمیم می‌گیرد[16].

براگا و همکاران [23]به‌منظور تشخیص حملات منع خدمت یک معماری سه واحدی متشکل از واحد جمع‌کننده جریان، واحد استخراج ویژگی و واحد دسته‌بند ارائه داده است. بعد از جمع‌آوری جریان‌های گذرنده از راه‌گزین‌های اُپن‌فلو در بستر شبکه توسط واحد جمع‌کننده جریان، واحد استخراج ویژگی شش ویژگی موردنیاز برای تشخیص حمله منع خدمت این مدل را از هر نمونه جمع‌آوری‌شده استخراج می‌کند. واحد دسته‌بند که از قبل با تعداد کافی نمونه مشخص آموزش دیده است، با توجه به ویژگی‌های استخراج‌شده از هر نمونه، احتمال قانونی بودن و یا مشکوک بودن ترافیک عبوری را مشخص می‌کند. این دسته‌بندی می‌تواند با روش‌های آماری مختلف انجام شود که در این روش از نگاشت خودسازمان‌ده استفاده‌شده است تا فضای نمونه‌ای متغییر از شش بعدی را به دو بعد کاهش دهد و وضعیت جریان نمونه مشخص گردد. این روش با وجود کاهش سربار نسبت به روش‌های موجود در شبکه سنتی باز هم دارای سربار زیاد و تأخیر بالایی است.

کومار و همکاران در [24] روش دیگری بر اساس یادگيری عميق ارائه داده‌اند. در این روش یک سيستم شناسایی حمله به‌عنوان یک برنامه کاربردی در کنترل‌کننده مرکزی برای مدیریت حملات منع خدمت ارائه‌شده است و مشابه روش قبلی از سه واحد جمع‌آوری ترافيک، استخراج ویژگی و دسته‌بندی ترافيک تشکیل‌شده است. این روش با هدف کاهش مثبت کاذب موجود در روش‌های مشابه، سعی در وارسی کليه بسته‌های شبکه دارد. در این روش علی‌رغم دستیابی به بالاترین درصد دقت برای شناسایی حمله و بالاترین درصد دقت دسته‌بندی که ترافيک را به دو دسته حمله و عادی تقسيم می‌کند، روش مناسبی برای تشخیص حملات منع خدمت توزیع‌شده در شبکه‌های واقعی و بزرگ‌ نیست. چراکه در این روش تمامی بسته‌های شبکه مورد بررسی قرار می‌گیرند که در شبکه‌های با حجم بالای ترافیک کاربردی نخواهد بود.

برخلاف اغلب روش‌های موجود که حملات را در مقصد (قربانی) تشخیص دهند، راشد و همکاران [25]روشی برای تشخیص حملات منع خدمت در مبدأ حمله ارائه‌ داده‌اند. روش مذکور در بسترهایی مانند محیط ابر کاربرد دارد و با شناسایی شروع حمله، مانعی برای استفاده از امکانات ابر جهت حمله منع خدمت می‌شود. این روش سعی دارد تا هوشمندی موجود در روش‌‌های مبتنی بر یادگیری ماشین را با ویژگی‌هایی که شبکه‌های نرم‌افزار محور در اختیار قرار می‌دهد ترکیب کند و یک سامانه تشخیص حمله منع خدمت توزیع‌شده را ارائه دهد. در این روش یک مدل از قبل آموزش داده‌شده به معماری شبکه اضافه می‌شود. در این مقاله از دسته‌بند بیز ساده برای دسته‌بندی ترافیک عبوری استفاده می‌شود. ویژگی‌های موردنیاز مدل هوشمند توسط کنترل‌کننده از بسته‌ها استخراج شده و به مدل ارسال می‌شود. پس از پاسخ مدل هوشمند، درصورتی‌که ترافیک شبکه غیرعادی گزارش شود کنترل‌کننده باید اقدامات لازم جهت مقابله با حمله را انجام دهد. تا قبل از آن شبکه روال معمول خود را انجام می‌دهد و منتظر پاسخ مدل نمی‌ماند. از اصلی‌ترین نقاط ضعف در این روش، چالش‌های مربوط به سازگاری مدل هوشمند با معماری ابر است.

زی‌چنگ و همکاران [26] مدلی با الهام گرفتن از مدل ارائه‌شده در [25] به‌منظور تشخیص حملات منع خدمت توزیع‌شده در سمت حمله‌کننده ارائه دادند. مزیت استفاده از روش‌های تشخیص حمله در این سمت مشخص بودن آدرس حمله‌کننده است. این روش نُه الگوریتم یادگیریِ مختلف برای مدل هوشمند را در نظر گرفته و سپس نتایج حاصل از اجرای هر الگوریتم را با هم مقایسه کرده است. روش مذکور برای چهار نوع حمله متداول منع خدمت توزیع‌شده مورد آزمایش قرار گرفت و به دقت تشخیص 97% در بهترین الگوریتم یادگیری موجود در مدل هوشمند دست‌یافته‌اند.

3.3 **سایر روش‌‌های تشخیص**

در ادامه به برخی روش‌های متنوع دیگر درزمینه‌ی تشخیص حملات منع خدمت توزیع‌شده خواهیم پرداخت. در سال 2008 یک حمله جدید منع خدمت توزیع‌شده، به نام حمله سیلاب پیوند معرفی‌شده است. در این حمله پیوندهای موجود در شبکه مورد هدف قرار می‌گیرند. استفاده از جریان‌های کم‌سرعت قانونی در مقیاس بزرگ و تغییر تصادفی و مکرر مقصد ارسال جریان توسط حمله‌کننده دو ویژگی منحصربه‌فرد این حمله است که تشخیص این حمله را نسبت به سایر حملات دشوارتر می‌کند. استفاده از معماری شبکه نرم‌افزار محور باعث می‌شود این حملات در این شبکه‌ها توفیق چندانی به دست نیاورند و تنها ممکن است موجب اشغال منابع و پهنا باند پیوند شبکه شوند. چراکه با توجه به دید جامع و انتزاعی موجود در شبکه‌های نرم‌افزار محور، در صورت شلوغی بیش‌ازحد یک پیوند، مسیر جایگزین برای برخی بسته‌های عبوری از آن پیوند تعیین می‌شود.

یک روش تشخیص این‌گونه حملات در شبکه‌ نرم‌افزار محور توسط وانگ و همکاران [27] ارائه شد. این روش از قابلیت‌های شبکه نرم‌افزار محور برای نظارت بر شبکه استفاده می‌کند. واحد انتخاب پیوند هدف، واحد نظارت بر ازدحام پیوند، واحد انتخاب مسیر جایگزین و واحد مسدودکننده ترافیک مخرب، چهار واحد اصلی تشکیل‌دهنده معماری روش ارائه‌شده می‌باشند. ابتدا با استفاده از تحلیل جریان‌های شبکه، تعداد مسیر‌های مختلف عبورکننده از هر پیوند محاسبه می‌شود و پیوندهایی که احتمال ایجاد ازدحام در آن‌ها وجود دارد شناسایی می‌شوند. سپس واحد نظارت بر ازدحام در پیوندهای مشکوک فعال می‌شوند و با محاسبه نرخ ازدحام در هر پیوند، وضعیت ترافیک لحظه‌ای را به کنترل‌کننده شبکه گزارش می‌دهند. درصورتی‌که ازدحام در پیوندی تشخیص داده شود واحد انتخاب مسیر جایگزین، مسیر دیگری را برای جابه‌جایی بسته‌ها انتخاب می‌کند. به‌منظور جلوگیری و کاهش اثر حمله، واحد مسدودکننده سعی می‌کند تا با تشخیص و مسدود‌سازی مبدأ ترافیک حمله، مانع ازدحام بیشتر در شبکه شود.

دِراما و همکاران [28]از الگوی زمانی برای شناسایی و کاهش حمله منع خدمت توزیع‌شده در کنترل‌کننده استفاده کردند. در این مقاله یک واحد جدید به نام جمع‌کننده جریان به معماری شبکه اضافه می‌شود. در روش مذکور هرگاه بسته جدیدی به شبکه وارد شود به کنترل‌کننده ارسال می‌شود و کنترل‌کننده آن را به جمع‌کننده جریان، هدایت می‌کند. درصورتی‌که در یک بازه زمانی کوتاه، تعداد بسته‌های دریافتی جمع‌کننده جریان زیاد باشد این رفتار حمله تشخیص داده و وضعیت حمله به اطلاع کنترل‌کننده می‌رسد. برای جلوگیری از ازدحام در واحد کنترل‌کننده، یک قانون جدید برای ارسال تمامی بسته‌ها به سمت جمع‌کننده روی ‌تمامی مؤلفه‌ها اِعمال می‌شود. پس از کاهش نرخ دریافت بسته‌ها در بازه زمانی مشخص، جمع‌کننده جریان پایان حمله را به کنترل‌کننده ابلاغ می‌کند و سپس با تغییر قانون قبلی، شبکه به وضعیت عادی خود بازمی‌گردد. باوجوداینکه در روش مذکور کنترل‌کننده شبکه از حمله در امان می‌ماند اما در زمان وقوع حمله، هیچ بسته‌ای توسط کنترل‌کننده بررسی نمی‌‌شود و در عمل بسته‌های جدید دریافتی‌ دور انداخته می‌شوند. لذا در این روش در طول وقوع حمله بسته‌های جدید از جانب کاربران قانونی نیز به‌ناچار نادیده گرفته می‌شود.

4 **روش پیشنهادی**

در بخش قبل برخی روش‌های مبتنی بر آنتروپی و یادگیری ماشین به منظور تشخیص حملات منع خدمت توزیع‌شده معرفی شدند. روش‌های مبتنی بر آنتروپی بر اساس بی‌نظمی ایجادشده در ترافیک شبکه، فرآیند تشخیص حملات منع خدمت توزیع‌شده را در زمان سریع‌تری نسبت به سایر روش‌های ارائه‌شده انجام می‌دهند. با توجه به آسیب‌هایی که ممکن است حملات منع خدمت توزیع‌شده به قربانی وارد کنند، استفاده از روش‌هایی که حملات منع خدمت در مدت زمان کمتر تشخیص دهند، مورد توجه قرار می‌گیرند. این در حالی است که روش مبتنی بر آنتروپی با محدودیت‌هایی مواجه است. این روش‌ها، دسته‌ای ازحملات منع خدمت توزیع‌شده‌ که موجب ایجاد بی‌نظمی در توازن ترافیک شبکه می‌شوند را تشخیص می‌دهند و در صورتی‌که حمله منع خدمت توزیع‌شده‌ای موجب کاهش آنتروپی بسته‌های شبکه نشود توسط این روش قابل تشخیص نخواهد بود.

نمونه‌ای از‌ حملات منع خدمت توزیع‌شده، حملاتی تحت عنوان "حملات بدرفتاری" هستند. در این‌گونه حملات مهاجم ضمن ایجاد ترافیک حمله‌ به مقصد قربانی، به‌صورت آگاهانه و به‌منظور قانونی جلوه دادن رفتار خود، ترافیک‌هایی که عادی قلمداد می‌شود نیز ارسال می‌کند. این امر باعث می‌شود تا بی‌نظمی در ترافیک شبکه ایجاد نگردد. لذا استفاده از آنتروپی در تشخیص صحیح این‌گونه حملات کارایی مناسب نخواهد داشت.

به همین منظور قصد داریم با اضافه کردن واحدی به معماری شبکه نرم‌افزار محور، ضمن تشخیص سریع حملات منع خدمت محدودیت گفته‌شده برای روش مبتنی بر آنتروپی را برطرف نماییم. روال کاری واحد اضافه‌شده بدین‌گونه خواهد بود که در هر پنجره زمانی در صورت مشاهده بی‌نظمی بالاتر از حد آستانه از پیش تعیین‌شده، به کمک روش مبتنی بر آنتروپی حمله را تشخیص دهیم. این حد آستانه تعیین‌کننده حداکثر بی‌نظمی مورد چشم‌پوشی برای شبکه است. درصورتی‌که بی‌نظمی مشاهده نشود، ممکن است ترافیک شبکه عادی باشد و حمله‌ای رخ نداده باشد و یا اینکه حمله توسط روش آنتروپی تشخیص داده نشده است. لذا وضعیت ترافیک فعلی شبکه از یک کارپذیر خارجی پرسیده می‌شود. در صورتی‌که کارپذیر حجم ترافیک عبوری شبکه را غیرمعمول تشخیص دهد، جریان برای بررسی بیشتر به یک مدل دسته‌بندی مبتنی بر یادگیری ماشین در واحد اضافه شده، ارسال می‌شود. این مدل که از قبل توسط دادگان مناسب آموزش دیده است، جریان شبکه را به دو دسته عادی و حمله تقسیم می‌کند. درصورتی‌که ترافیک دریافتی یک ترافیک حمله تشخیص داده شود هشداری به واحد کنترل‌کننده، به منظور شروع فرایند جلوگیری و کاهش اثر حمله ارسال می‌شود. بدین‌ترتیب علاوه‌بر تشخیص زودهنگام حمله، مواردی که توسط روش‌های مبتنی بر آنتروپی قابل تشخیص نبودند (مانند حمله بدرفتاری)، به کمک روش یادگیری ماشین شناسایی می‌شوند.

5 **نتیجه‌گیری**

در این نوشتار به مرور مفاهیم اولیه مرتبط با حملات منع خدمت توزیع‌شده و انواع آن، شبکه‌های نرم‌افزار محور و ویژگی‌های این شبکه، روش‌های یادگیری ماشین پرداخته شد. سپس برخی پژوهش‌های انجام‌شده درزمینه‌ی تشخیص حملات منع خدمت موردبررسی قرار گرفت و دو حمله متفاوت که برخی سامانه‌های تشخیص حمله توانایی شناسایی آن‌ها را ندارند معرفی شد. در آخر روش پیشنهادی برای بهبود تشخیص سریع و دقیق حملات منع خدمت توزیع‌شده در بستر شبکه نرم‌افزار محور به صورت مختصر شرح داده شد.

جدول 1 : مراحل انجام و پیشبرد پروژه

|  |  |  |
| --- | --- | --- |
| فعالیت | میزان پیشرفت | تخمین زمان باقی‌مانده |
| 1. مطالعه و بررسی مفاهیم | **%80** | **3 هفته** |
| 2. تحلیل و بررسی کارهای پیشین | **%80** | **5 هفته** |
| 3. ارائه و امکان‎سنجی روش پیشنهادی | **%70** | **6 هفته** |
| 4. پیاده‌سازی روش پیشنهادی | **%10** | **2 ماه** |
| 5. ارزیابی روش پیشنهادی | **%0** | **1 ماه** |
| 6. جمع‌بندی و تدوین پایان‌نامه | **%20** | **1 ماه** |

**کتاب‌نامه**

1. Dong, Shi, Khushnood Abbas, and Raj Jain. "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments." IEEE Access 7 (2019).
2. D’Cruze, Hubert, et al. "A software-defined networking (SDN) approach to mitigating DDoS attacks." Information Technology-New Generations. Springer, Cham, (2018).
3. Meti, Nisharani, D. G. Narayan, and V. P. Baligar. "Detection of distributed denial of service attacks using machine learning algorithms in software defined networks." 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, (2017).
4. Somani, Gaurav, et al. "DDoS attacks in cloud computing: Issues, taxonomy, and future directions." Computer Communications 107 (2017).
5. Fajar, Andry Putra, and Tito Waluyo Purboyo. "A Survey Paper of Distributed Denial-of-Service Attack in Software Defined Networking (SDN)." International Journal of Applied Engineering Research 13.1 (2018)
6. Kamboj, Priyanka, et al. "Detection techniques of DDoS attacks: A survey." 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON). IEEE, (2017).
7. Rawat, Danda B., and Swetha R. Reddy. "Software defined networking architecture, security and energy efficiency: A survey." IEEE Communications Surveys & Tutorials 19.1 (2016).
8. Kreutz, Diego, et al. "Software-defined networking: A comprehensive survey." arXiv preprint arXiv:1406.0440 (2014).
9. Fernando, M. V., Paulo Esteves, and Christian Esteve. "Software-defined Networking: A Comprehensive Survey." PROCEEDINGS OF THE IEEE (2015).
10. Nunes, Bruno Astuto A., et al. "A survey of software-defined networking: Past, present, and future of programmable networks." IEEE Communications Surveys & Tutorials 16.3 (2014).
11. Mahjabin, Tasnuva, et al. "A survey of distributed denial-of-service attack, prevention, and mitigation techniques." International Journal of Distributed Sensor Networks 13.12 (2017).
12. Yan, Qiao, and F. Richard Yu. "Distributed denial of service attacks in software-defined networking with cloud computing." IEEE Communications Magazine 53.4 (2015).
13. Saharan, Shail, and Vishal Gupta. "Prevention and Mitigation of DNS based DDoS attacks in SDN Environment." 2019 11th International Conference on Communication Systems & Networks (COMSNETS). IEEE, 2019.‏
14. Bawany, Narmeen Zakaria, Jawwad A. Shamsi, and Khaled Salah. "DDoS attack detection and mitigation using SDN: methods, practices, and solutions." Arabian Journal for Science and Engineering 42.2 (2017).
15. Rai, Ankita, Prakash D Vyavahare, and Anjana Jain. "Distributed DoS Attack Detection and Mitigation in Software Defined Network (SDN)." Anjana, Distributed DoS Attack Detection and Mitigation in Software Defined Network (SDN) (2019).‏
16. Shakil, Muhammad, et al. "A novel dynamic framework to detect DDoS in SDN using metaheuristic clustering." Transactions on Emerging Telecommunications Technologies (2019).
17. R. S. Michalski, J. G. Carbonell, and T. M. Mitchell, machine Learning: An Artificial Intelligence Approach . Springer Science & Business Media (2013)
18. Myo Myint, Sinchai Kamolphiwong, and Thossaporn Kamolphiwong. "The Design of SDN Based Detection for Distributed Denial of Service (DDoS) Attack." 2017 21st International Computer Science and Engineering Conference (ICSEC). IEEE, (2017).‏‏
19. Wang, An, Wentao Chang, Songqing Chen, and Aziz Mohaisen. "A Data-Driven Study of DDoS Attacks and Their Dynamics." IEEE Transactions on Dependable and Secure Computing (2018).
20. Mousavi, Seyed Mohammad, and Marc St-Hilaire. "Early detection of ddos attacks against software defined network controllers." Journal of Network and Systems Management 26.3 (2018).
21. Rui Wang, Zhiping Jia, Lei Ju. "An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking‏. "2015 IEEE Trustcom BigDatSE ISPA (2015).
22. Gharvirian Fateme, and A. Bohlooli. "Neural network based protection of software defined network controller against distributed denial of service attacks." International Journal of Engineering-Transactions B: Applications 30.11 (2017).
23. Rodrigo Braga, Edjard Mota, Alexandre Passito. "Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow. " 35th Annual IEEE Conference on Local Computer Networks. (2012)
24. Niyaz Quamar, Weiqing Sun, and Ahmad Y. Javaid. "A deep learning based DDoS detection system in software-defined networking (SDN)." arXiv preprint arXiv:1611.07400 (2016).
25. ‏Mohammed, Saif Saad, et al. "A New Machine Learning-based Collaborative DDoS MitigationMechanism in Software-Defined Network." 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, (2018).
26. Zecheng, Tianwei Zhang, and Ruby B. Lee. "Machine learning based DDoS attack detection from source side in cloud." 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE, (2017).‏‏
27. Wang, Juan, et al. "Detecting and mitigating target link-flooding attacks using sdn." IEEE Transactions on Dependable and Secure Computing (2018).‏
28. I Gde Dharma N. et al. "Time-based DDoS Detection and Mitigation for SDN Controller. " 17th Asia-Pacific Network Operations and Management Symposium. (2015).

**واژه‌نامه**

1. Availability [↑](#endnote-ref-1)
2. Internet Service Provider [↑](#endnote-ref-2)
3. Denial of Service [↑](#endnote-ref-3)
4. Distributed Denial of Service [↑](#endnote-ref-4)
5. Attacker [↑](#endnote-ref-5)
6. Bot [↑](#endnote-ref-6)
7. System [↑](#endnote-ref-7)
8. Kaspersky [↑](#endnote-ref-8)
9. Macafee [↑](#endnote-ref-9)
10. Software Defined Networks [↑](#endnote-ref-10)
11. Control Plane [↑](#endnote-ref-11)
12. Data Plane [↑](#endnote-ref-12)
13. Component [↑](#endnote-ref-13)
14. Package [↑](#endnote-ref-14)
15. Mainframe [↑](#endnote-ref-15)
16. Config [↑](#endnote-ref-16)
17. Virtual Machine [↑](#endnote-ref-17)
18. Quality of Service [↑](#endnote-ref-18)
19. Routing Protocols [↑](#endnote-ref-19)
20. Stanford [↑](#endnote-ref-20)
21. Infrastructure Layer [↑](#endnote-ref-21)
22. Switch [↑](#endnote-ref-22)
23. Router [↑](#endnote-ref-23)
24. Controler [↑](#endnote-ref-24)
25. Open Flow [↑](#endnote-ref-25)
26. Port [↑](#endnote-ref-26)
27. Policy [↑](#endnote-ref-27)
28. Add [↑](#endnote-ref-28)
29. Delete [↑](#endnote-ref-29)
30. Update [↑](#endnote-ref-30)
31. Forward [↑](#endnote-ref-31)
32. Congestion [↑](#endnote-ref-32)
33. Attacker [↑](#endnote-ref-33)
34. Agent [↑](#endnote-ref-34)
35. Victim [↑](#endnote-ref-35)
36. Foading Attack [↑](#endnote-ref-36)
37. Reflection Attack [↑](#endnote-ref-37)
38. Amplification Attack [↑](#endnote-ref-38)
39. HTTP [↑](#endnote-ref-39)
40. Supervised Learning [↑](#endnote-ref-40)
41. Unsupervised Learning [↑](#endnote-ref-41)
42. Reinforcement Learning [↑](#endnote-ref-42)
43. Lable [↑](#endnote-ref-43)
44. Classification [↑](#endnote-ref-44)
45. Regression [↑](#endnote-ref-45)
46. Clustering [↑](#endnote-ref-46)
47. Reward [↑](#endnote-ref-47)
48. Action [↑](#endnote-ref-48)
49. Entropy [↑](#endnote-ref-49)
50. Dataset [↑](#endnote-ref-50)
51. Intrusion Detection System [↑](#endnote-ref-51)
52. IP Address [↑](#endnote-ref-52)
53. Trashhold [↑](#endnote-ref-53)