ششمین همایش ملی
فناوریهای نوین در مهندسی برق، کامپیوتر و مکانیک ایران
The 6th National Conference on
New Technologies in Electrical, Computer and Mechanical Engineering of IRAN

نگاهی بر روش‌های دفاعی در مقابل حمله‌های توزیع‌شده بندآوری از خدمات در محیط شبکه‌های نرم‌افزار محور

امیرحسین جباری، احمدرضا منتظرالقائم

۱- دانشجوی کارشناسی ارشد مهندسی کامپیوتر، دانشگاه اصفهان
۲- استادیار گروه فناوری اطلاعات، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان

Email: jabbari@eng.ui.ac.ir
Email: a.montazerolghaem@comp.ui.ac.ir

چکیده

شبکه نرم‌افزارمحور (SDN[1]) فناوری مهمی است که علیرغم فراهم‌سازی ویژگی‌هایی همچون افزایش انعطاف، ساده‌سازی و کاهش هزینه برای شبکه‌هایی که از این فناوری استفاده می‌کنند، معایبی را به دلیل ماهیت مرکزی خود به‌دنبال دارد. امنیت، از مهم‌ترین چالش‌هایی است که اثر وجود یک ماهیت مرکزی در تامین آن، باید بررسی شود. در همین زمینه، بررسی حمله‌های توزیع‌شده بندآوری از خدمات (DDoS[2]) در محیط SDN اهمیت بیشتری پیدا می‌کند. در این پژوهش، چند سازوکار دفاعی که برای مقابله با این حملات در محیط شبکه‌های نرم‌افزار محور ارائه شده‌اند، بررسی شده و براساس تفاوت در نحوه عملکرد، طبقه‌بندی می‌شوند. این کار می‌تواند به شناسایی نقاط ضعف سازوکارهای دفاعی موجود و بهبود آن‌ها، و یا به ارائه یک سازوکار جدید، کمک کند.

کلمات کلیدی: حمله‌های بندآوری از خدمات، شبکه‌های نرم‌افزار محور، امنیت شبکه

۱. مقدمه

روند صعودی تعداد دستگاه‌های متصل به شبکه اینترنت، پیدایش فناوری‌های نوین مانند اینترنت اشیا (IoT[3]) و افزایش روزافزون خدمات ارائه شده در بستر شبکه، باعث افزایش پیچیدگی شبکه اینترنت شده است که این موضوع نیازها و چالش‌های جدیدی را به‌وجود می‌آورد. برای طراحی شبکه‌ها در آینده به نحوی که این چالش‌های جدید برطرف شوند، راه‌حل‌های مختلفی بیان شده‌اند که یکی از آن‌ها استفاده از شبکه‌های نرم‌افزارمحور (SDN) است. رویکرد اصلی در SDN، اعمال عملکردهای تصمیم‌گیری (در صفحه

[1] Software Defined Networking
[2] Distributed Denial of Service
[3] Internet of Things

کنترل[۴]) و انتقال (در صفحه داده[۵])، به‌صورت جداگانه است. در شبکه‌های سنتی، هر مسیریاب[۶] شبکه به کمک اعمال الگوریتم‌های مسیریابی، گرفتن تصمیم نهایی برای تعیین مقصد بسته‌ها[۷] را انجام می‌دهد. اما در SDN، فرایند تصمیم‌گیری در کنترلر[۸] انجام شده و سوییچ‌ها[۹] صرفا بسته‌ها را منتقل می‌کنند. به همین دلیل، امکان استفاده از سخت‌افزارهای ساده‌تر در سطح شبکه و قابلیت مدیریت مرکزی فراهم می‌شوند. این دو ویژگی، فوایدی مانند صرفه‌جویی در هزینه‌ها هنگام زیاد بودن تجهیزات شبکه، و انعطاف‌پذیری در انجام تغییراتی که برای اعمال آن‌ها، نیاز به انجام تغییرات در همه دستگاه‌های موجود در سطح شبکه است را نیز به دنبال دارند.
علیرغم این ویژگی‌های مثبت، برخی سوال‌ها در زمینه پایداری، مقیاس‌پذیری، تاخیر، و جانمایی کنترلر وجود خواهند داشت. در زمینه امنیت نیز، SDN با آسیب‌پذیری‌های جدیدی روبرو است. سرچشمه این آسیب‌پذیری‌ها به توانایی کنترل شبکه توسط نرم‌افزار و مرکزی بودن کنترل شبکه بازمی‌گردد. این دو خصوصیت می‌توانند باعث ایجاد چالش‌هایی از قبیل نحوه صحت‌سنجی برای دسترسی و امکان خرابی در تک نقطه‌ی مدیریتی (کنترلر) خواهند بود. مشکل اول، با اعمال سیاست‌های مجوز دسترسی و سازوکارهای احراز هویت قابل حل است، اما مورد دوم، با به خطر انداختن در دسترس بودن کنترلر، می‌تواند مورد سوء استفاده قرار گیرد. یکی از روش‌هایی که یک مهاجم با استفاده از آن، قادر خواهد بود تا در دسترس بودن کنترلر را به خطر بیاندازد، حمله‌های توزیع‌شده بندآوری از خدمات (DDoS) است.

۲. مفهوم DDoS و DoS

در حمله DoS[10]، سطح استفاده کاربران مجاز از منابع سیستم هدف، کاهش یافته و در نتیجه، در دسترس بودن سیستم دچار افت می‌شود. سازوکار بنیادین که در این روش به کار گرفته می‌شود، ارسال ترافیک عظیم و سیل‌آسا به سیستم هدف است. برخلاف حمله DoS که منشا ترافیک مخرب تنها یک منبع است، در حمله DDoS، مهاجم از چندین منبع برای ارسال ترافیک غیرمجاز استفاده می‌کند. حمله DDoS، بسیار مخرب‌تر از حمله DoS است. Mirai، نام بدافزاری است که می‌تواند پس از نصب روی دستگاه‌هایی که دارای سیستم عامل لینوکس هستند، از آن‌ها به عنوان یک بات[۱۱] برای اهداف مخرب استفاده کند. در حمله‌ای تحت عنوان Mirai IoT Botnet در سال ۲۰۱۶، چندین دستگاه هوشمند با آلوده شدن به این بدافزار، جزئی از شبکه گسترده‌ای از بات‌ها (که با نام Botnet شناخته می‌شود) شدند و به صفحه وب یک وبلاگ‌نویس در حوزه امنیت حمله کردند. به دلیل هزینه بالا برای دفاع دربرابر این حمله، ارائه‌دهنده خدمات محبور به قطع سرویس برای این شخص شد [۲].

[4] Control plane
[5] Data plane
[6] Router
[7] Packets
[8] Controller
[9] Switches
[10] Denial of Service
[11] Bot

در حمله‌های DDoS، ممکن است از روش‌های مختلفی استفاده شود که این روش‌ها قابل اعمال روی محیط SDN نیز هستند. از جمله این روش‌ها، می‌توان به NTP Amplification، UDP, ICMP, TCP SYN Flooding، و پینگ مرگ[12] اشاره کرد.

۳. آسیب پذیر بودن SDN در مقابل حمله DDoS

از جمله مواردی که می‌توانند باعث آسیب‌پذیری SDN در برابر حمله‌های DDoS شوند، می‌توان به موارد زیر اشاره کرد:

۳-۱. امکان از دسترس خارج شدن کل شبکه در صورت از کار افتادن کنترلر

در حالت کلی، وقتی بسته‌ای که سوییچ برای آدرس آی‌پی[13] مقصد آن، سطر متناظری در جدول جریان[14] خود نداشته باشد، به سوییچ برسد، سوییچ باید کنترلر را مطلع کرده تا کنترلر دستور لازم را که باید برای بسته مورد نظر اعمال شود، به سوییچ ارسال کند. اگر مهاجم از چندین آدرس آی‌پی حجم زیادی از بسته‌ها را ارسال کند، دسترسی کاربران عادی به کل شبکه می‌تواند به خطر بیافتد.

۳-۲. انتشار حمله‌ها در شبکه

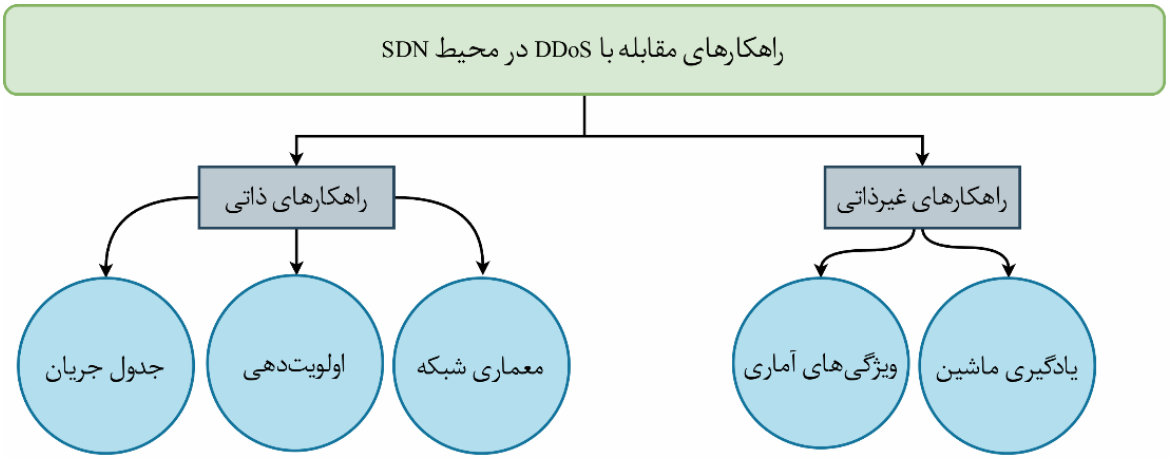
روند ساده پردازش بسته‌ها در هر سوییچ (در مقایسه با مسیریاب‌های معمول)، می‌تواند به انتشار حمله DDoS در محیط SDN کمک کند. در نتیجه، کنترلر می‌بایست با آثار ناشی از چنین رویدادی مقابله کند.

علاوه بر اهمیت موضوع تامین امنیت (در مواردی از قبیل حمله DDoS) برای شبکه‌های نرم‌افزارمحور، موضوعی تحت عنوان SDN برای امنیت نیز مطرح است که به کمک آن، می‌توان سازوکارهای دفاعی برای مواردی مانند حمله DDoS را فراهم کرد [۳].

مهاجم ممکن است با رویکردهای متفاوتی اقدام به حمله DDoS روی یک شبکه نرم‌افزارمحور کند. هدف اصلی تهاجم می‌تواند یکی از موارد زیر باشد:

- **لینک (های) منتهی به کنترلر:** مهاجم با تولید و ارسال ترافیک با آدرس آی‌پی جعل شده[15]، سوییچ (ها) را وادار به ارسال پکت‌هایی به کنترلر می‌کند. بنابراین لینک (های) منتهی به کنترلر ممکن است دچار تراکم شود.
- **منابع سیستمی کنترلر:** در این حالت، مهاجم‌ها به سوییچ‌های متمایزی که توسط یک کنترلر مدیریت می‌شوند، متصل هستند. به دلیل تقسیم بار مخرب، تشخیص حمله ذاتاً سخت‌تر است. این حمله تحت عنوان Blind DDoS Attack [۴] شناخته می‌شود.
- **حافظه سوییچ:** اگرچه اعمال طراحی‌های پیچیده برای جدول جریان سوییچ‌ها و استفاده بهینه از حافظه سوییچ ممکن است، در حالت کلی پر شدن جدول جریان می‌تواند برای سوییچ رخ دهد. اگر مهاجم باعث این اتفاق شود، سرویس‌دهی به ترافیک مجاز (از آدرس آی‌پی‌های جدید) قابل انجام نخواهد بود. همچنین، دسترسی به سوییچ هدف ممکن است با مسدودسازی لینک‌های منتهی به آن، به خطر افتد. این حمله با نام Crossfire Attack [۵] شناخته می‌شود.

---
[12] Ping of Death
[13] IP address
[14] Flow table
[15] Spoofed IP address



شکل ۱- طبقه‌بندی راهکارهای مورد بررسی

- **لینک (های) بین سوییچ‌ها:** با برقراری ارتباط دو یا چند مهاجم با یک‌دیگر، به‌صورتی که هر مهاجم به سوییچ‌های متمایز از هم متصل باشد، لینک (های) بین این سوییچ‌ها ممکن است دچار تراکم شود. این حمله با نام Coremelt Attack [۶] شناخته می‌شود.
- **کاربر عادی:** مهاجم‌ها می‌توانند تحت سوییچ متفاوتی با سوییچی که هدف به آن متصل است، باشند. در صورتی که تهاجم توسط کنترلر یا سوییچ‌ها تشخیص داده نشود، منابع سیستمی کاربر عادی (یا یک سرور) به خطر می‌افتد.

۵. طبقه‌بندی راه‌حل‌های مربوط به مقابله با DDoS

در زمینه مقابله با حملات DDoS، راه‌حل‌های مختلفی ارائه شده‌اند. انتخاب راه‌حل مناسب، باید با توجه با نیازهای موجود در هر شبکه و بررسی آن‌ها صورت گیرد.

۵-۱- ذاتی یا غیرذاتی بودن

اگر راه حل به خصوصیت‌های ذاتی محیط (SDN و اجزای آن) بستگی داشته باشد، از نوع ذاتی، و اگر به ویژگی‌های جریان‌های شبکه وابسته باشد، از نوع غیرذاتی طبقه‌بندی می‌شود.
شکل ۱، نمایی کلی از طبقه‌بندی راهکارهای بررسی شده براساس ذاتی یا غیرذاتی بودن راهکارها را نشان می‌دهد.

۵-۲- هوشمندی یا عدم هوشمندی سوییچ‌ها

برخی از راه‌حل‌های بررسی شده، به سوییچ‌ها میزانی از هوشمندی را اضافه می‌کنند. این کار به این دلیل صورت می‌گیرد که جریان‌های[16] شبکه تا حد ممکن در صفحه داده باقی بمانند. در صورتی که هوشمندسازی سوییچ‌ها بیش از حد انجام شود، باید به دور شدن از فلسفه بنیادین SDN (که به استفاده از سوییچ‌های ساده تاکید دارد) نیز توجه داشت.

[16] Flows

نوع راهکار	سوییچ‌های هوشمند	سوییچ‌های عادی
تشخیص	[۱۴]	[۱۶]
مقابله	—	[۵–۸, ۱۰, ۱۴]
تشخیص و مقابله	[۱۲, ۱۳]	[۱۰]

جدول ۱– مقایسه راهکارها براساس هوشمندی سوییچ‌ها و نوع راهکار

۵–۳– قابلیت تشخیص و مقابله

یک راه‌حل هنگامی دارای ویژگی تشخیص حمله DDoS است که بتواند بین حمله DDoS و Flash crowd تمایز قائل شود. عبارت Flash crowd، به جریان‌های ترافیکی مجاز اما با حجم بالا گفته می‌شود [۷]. همچنین قابلیت مقابله، به ارائه یک یا چند راهکار برای مقابله با ترافیک مخرب یا کاهش اثر آن اطلاق می‌شود.

در جدول ۱، طبقه‌بندی راهکارهای مورد بررسی براساس هوشمندی سوییچ‌هایی که در صفحه داده استفاده شده‌اند و نوع راهکار ارائه شده در هر پژوهش، مشاهده می‌شود.

۶. بررسی کلی ویژگی راهکارها

هر کدام از سازوکارهای ارائه شده در [۸] تا [۱۸]، به ارائه راهکارهایی در زمینه حمله‌های DDoS می‌پردازند که در این بخش، با نگاه کلی به روش‌های ارائه شده، جایگاه آن‌ها در طبقه‌بندی مورد نظر، بررسی می‌شود.

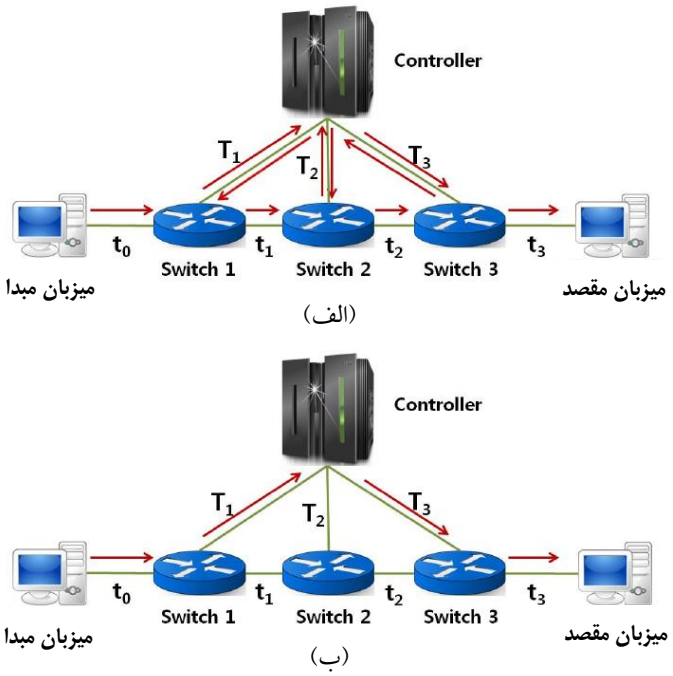
۱.۶. راهکارهای ذاتی

همان‌طور که گفته شد، این راهکارها به خصوصیت‌های ذاتی محیط SDN مرتبط هستند. مراجع [۸] تا [۱۳]، در این بخش قرار می‌گیرند.

۱.۱.۶. بر اساس ویرایش جدول جریان

جدول جریان هر سوییچ، اندازه محدودی دارد و به همین دلیل، مدیریت صحیح آن دارای اهمیت است. در صورت پر شدن جدول‌های جریان، کارایی شبکه به‌صورت جدی تهدید می‌شود. در شکل ۲، T_i و t_i بیان‌گر زمان تاخیر لینک‌های منتهی به کنترلر و سوییچ‌ها هستند. در این شکل، جدول جریان سوییچ‌ها فضای خالی ندارد و همچنین برای جریان ترافیکی که توسط میزبان مبدا برای میزبان مقصد ارسال شده است، سطر متناظری در جدول جریان سوییچ‌ها وجود ندارد. در شکل ۲–الف، کنترلر به درخواست‌هایی که از طرف هر سوییچ ممکن است ارسال شود، پاسخ داده و جدول جریان آن‌ها را به‌روزرسانی می‌کند. همچنین در شکل ۲–ب، جریان ارسالی از طرف خود کنترلر به میزبان مقصد فرستاده می‌شود. درصورتی که یک مهاجم با ارسال جریان‌های جعلی (که هدر[17] هر جریان با جریان بعدی تفاوت جزئی دارد) باعث پر شدن جدول‌های جریان شود، در حالت اول، سربار[18] زیادی برای به‌روزرسانی جدول‌های جریان در شبکه ایجاد می‌شود و در حالت دوم، کارایی و در دسترس بودن کنترلر تهدید خواهد شد.

[17] Header
[18] Overhead



شکل ۲- دو روش در نحوه رفتار با جریان‌های جدید [۸]

راهکار ارائه شده در [۸]، سیاست تعویض سطرهای جدول جریان، به جای استفاده از یک پارامتر، بر اساس چند پارامتر که مربوط به سطرهای جدول جریان است، عمل می‌کند. همچنین، کنترلر دارای یک ماژول بافر است که مدیریت و نگهداری موقت سطرهای جدول جریان را انجام می‌دهد.

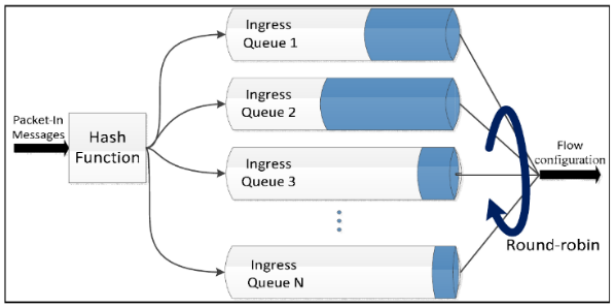
به طور مشابه، [۹] مکانیزمی را برای به روزرسانی سطرها در جدول سوییچ‌ها، ارائه می‌کند. موضوع اصلی این پژوهش مربوط به DDoS نیست اما مشابه با مرجع قبلی، می‌تواند برای مقابله با آن به کار گرفته شود.

۲.۱.۶. بر اساس اولویت دهی

این دسته از روش‌ها روی کنترلر پیاده‌سازی می‌شوند، و به محافظت از آن تاکید دارند. این کار، به کمک زمان‌بندی و اولویت‌دهی به فعالیت‌های محول شده به کنترلر از طرف سوییچ‌ها، انجام می‌شود. در [۱۰]، به مقیاس‌پذیری کنترلر و در [۱۱]، به ایزوله کردن کنترلر پرداخته شده است. هیچ کدام از این دو پژوهش، عملکرد تشخیصی را ارائه نمی‌کنند.

در [۱۰]، بسته‌های دریافتی از سوییچی که دچار ازدحام است، بر اساس سازوکاری که اولویت‌دهی براساس راندرابین مبتنی بر هش[19] نام‌گذاری شده است، عمل می‌کند. فرایند کلی در این سازوکار بر اساس تخصیص بسته‌های ورودی به کنترلر به تعدادی صف است (شکل ۳). به ازای هر بسته، مقدار هش براساس رابطه‌ی $H_{in} = [D_{in} + T_{in}] \% Q$، محاسبه می‌شود. در این رابطه، T_{in} و D_{in} به ترتیب زمان رسیدن بسته و حاصل جمع ده‌دهی هر ۴ قسمت از آدرس آی‌پی مقصد هستند و Q نیز نشان‌دهنده تعداد صف‌ها در کنترلر است. براساس مقدار محاسبه شده، هر بسته ورودی به صف خاصی تخصیص پیدا می‌کند و کنترلر نیز به‌کمک

[19] Hash-based round-robin scheduling



شکل ۳–صف‌بندی بسته‌های Packet-in در سازوکار اولویت‌دهی براساس راندرابین مبتنی بر هش [۱۰]

فرایند راندرابین، ارائه سرویس به صف‌ها را اولویت‌دهی می‌کند. در نهایت، کنترلر حتی در صورت وجود حجم ترافیک بالا، قادر به فراهم کردن دستورات برای سوییچ خواهد بود.

به‌طور مشابه و در [۱۱]، بخش غالب ترافیک مخرب در سوییچ مربوطه محدود می‌شود. به طور معمول اگر یک سوییچ دچار مشکل شود، کنترلر قادر به ارائه خدمات به سایر کاربران نخواهد بود. برای جلوگیری از این موضوع، برای هر سوییچ، صف‌های مختلفی در نظر گرفته می‌شود. بنابراین، شبکه به عنوان یک مجموعه واحد، به کار خود ادامه خواهد داد.

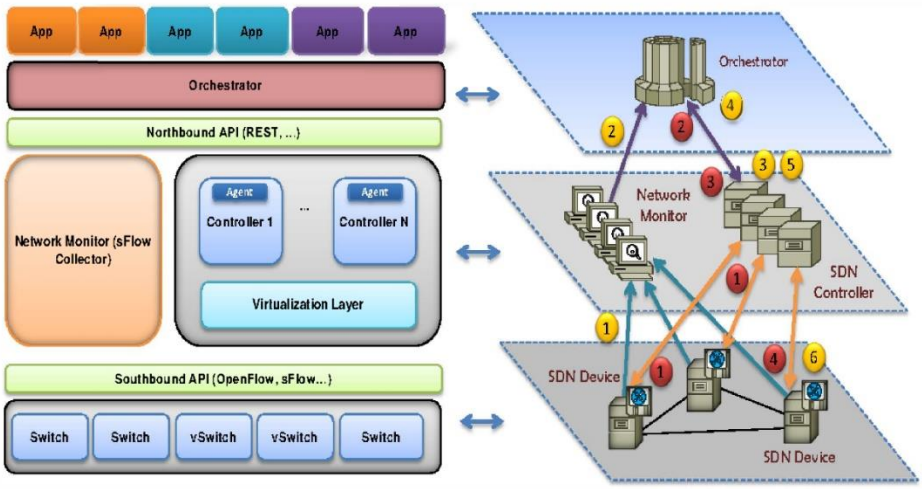
۳.۱.۶. بر اساس معماری شبکه

مفهوم کلی روش‌های ارائه شده در [۱۲] و [۱۳]، بر اساس سطوح عملکردی اجزای شبکه و وظایف آن‌ها است. در این دو روش، عملکردهای کنترلر در بخش‌های مانیتورینگ و کنترل از هم تفکیک می‌شوند و توسط واحدی به نام Master قابل مدیریت خواهند بود. از مزیت‌های این کار، فعال‌سازی هر بخش عملکردی بر اساس رزولوشن[۲۰] حمله‌ها است.

حمله‌هایی با رزولوشن پایین[۲۱]، بدون دسترسی به تمامی بسته‌هایی که در شبکه ردوبدل می‌شوند، قابل تشخیص هستند. برای نمونه، حمله‌های DDoS در این دسته قرار می‌گیرند. اما حمله‌های با رزولوشن بالا[۲۲]، بدون دسترسی به تمامی بسته‌هایی که در شبکه ردوبدل می‌شوند، قابل تشخیص نخواهند بود. یک نمونه از حمله‌ای با رزولوشن بالا، حمله‌ی جعل آرپ[۲۳] است.

در [۱۲]، معماری Orcsec پیشنهاد شده است. در این معماری، یک هماهنگ‌کننده[۲۴] وظیفه فعال‌سازی ماژول‌های مجزا (با نام‌های Network Monitor و SDN Controller) را بر اساس نوع حمله دارد. طبق روندی که در شکل ۴ مشاهده می‌شود، اعداد قرمز رنگ، مراحل طی شده برای تشخیص حمله‌ها با رزولوشن بالا، و اعداد زرد رنگ مراحل طی شده برای تشخیص حمله‌ها با رزولوشن پایین را نشان می‌دهند. برای حمله‌های با رزولوشن بالا، ابتدا ماژول‌های بخش Network Monitor با پایش رویدادهایی که در شبکه در روی می‌دهند، هماهنگ‌کننده را مطلع می‌کند (مراحل ۱ و ۲). سپس، با تعامل و تبادل اطلاعات میان هماهنگ‌کننده و ماژول‌های بخش SDN Controller، عمل مورد نیاز برای مقابله با حمله در سطح شبکه و سوییچ‌ها اعمال می‌شود (مراحل ۳ تا ۶). برای حمله‌های با رزولوشن پایین، هماهنگ‌کننده به ماژول‌های بخش SDN Controller دستور می‌دهد تا

[20] Resolution
[21] Low resolution
[22] High resolution
[23] ARP spoofing
[24] Coordinator



شکل ۴- معماری Orcsec و فرایند تشخیص حمله براساس رزولوشن آن [۱۲]

هدر بسته‌هایی که مربوط به نوع خاصی از ترافیک (برای مثال، ARP) هستند را به هماهنگ‌کننده ارسال کند (مراحل ۱ و ۲). سپس، با تعامل میان هماهنگ‌کننده و ماژول‌های بخش SDN Controller، عمل مورد نیاز برای مقابله با حمله در سطح شبکه اعمال می‌شود (مراحل ۳ و ۴). در این سازوکار هر دو عملکرد تشخیص و مقابله فراهم می‌شود اما روش مقابله، صرفا بر اساس محدودسازی نرخ ترافیک[۲۵] است.

معماری دیگری که در [۱۳] مطرح شده است، به توزیع‌شدگی کنترلر به عنوان عاملی برای دو هدف امنیت و توزیع بار تاکید دارد. همچنین، یک واگذارکننده[۲۶] و چندین کنترلر دیگر در سطح پایین‌تر از کنترلر اصلی قرار دارند تا وظایف محول شده از سمت واگذارکننده را اجرا کنند.

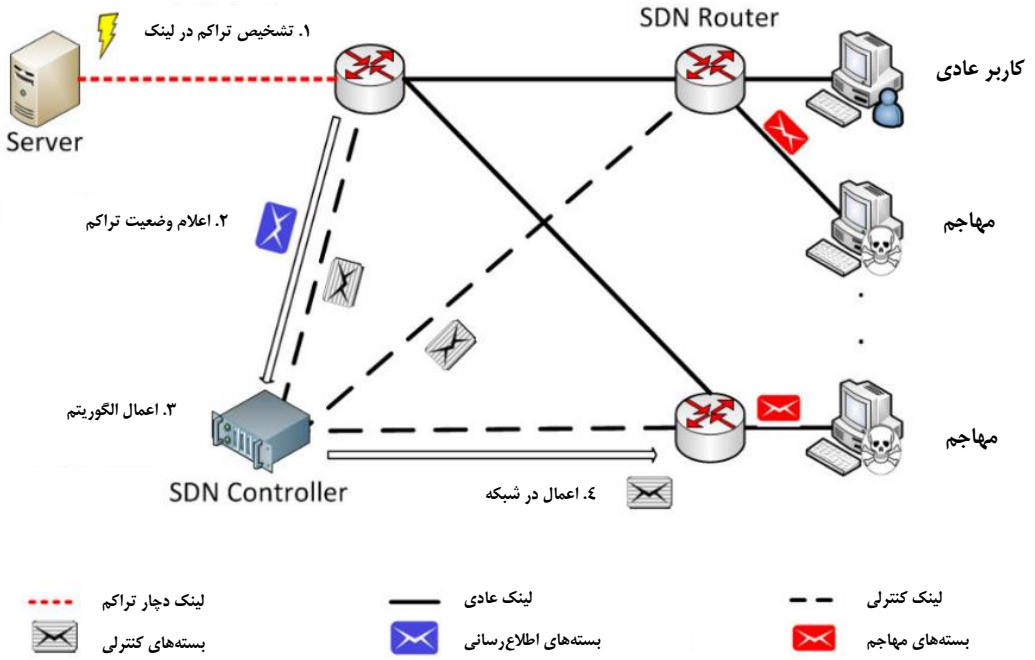
۲.۶. راهکارهای غیرذاتی

برخلاف راهکارهای ذاتی، این راهکارها به ویژگی‌های جریان‌ها در شبکه مربوط هستند و مراجع [۱۴] تا [۱۸] در این بخش قرار می‌گیرند.

۱.۲.۶. بر اساس روش‌های آماری

در روش‌هایی که مبتنی بر خصوصیات آماری جریان‌های شبکه هستند، به‌طور معمول باید هنگامی که ترافیک عادی در شبکه جریان دارد، تعدادی نمای پایه‌ای[۲۷] از وضعیت شبکه ایجاد شود. پس از آن و در زمان اعمال راهکار در شبکه، وضعیت کنونی ترافیک با نماهای پایه‌ای مقایسه شده و ترافیک مخرب تشخیص داده می‌شود .در [۱۴]، سازوکار دفاعی Flowfence معرفی شده است. در این سازوکار، سوییچ‌ها با پایش میزان استفاده از پهنای باند، ایجاد تراکم در لینک را تشخیص داده و سپس، کنترلر را مطلع

[25] Rate limiting
[26] Delegator
[27] Baseline profile



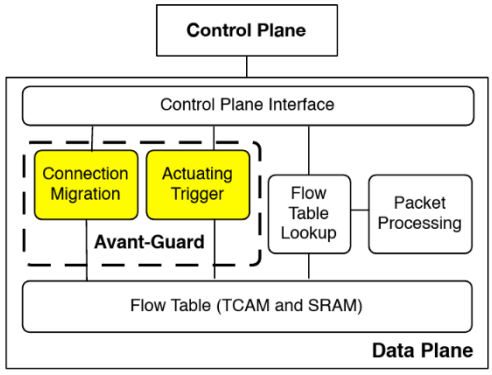
شکل ۵- تشخیص تراکم لینک در سازوکار Flowfence [ویرایش شده از ۱۴]

می‌کنند. کنترلر از هر سوییچ که به لینک دچار تراکم، جریانی را ارسال می‌کند، آمار مرتبط را درخواست کرده و بر همین اساس تصمیم به محدودسازی نرخ جریان‌های بدرفتار می‌گیرد (شکل ۵).

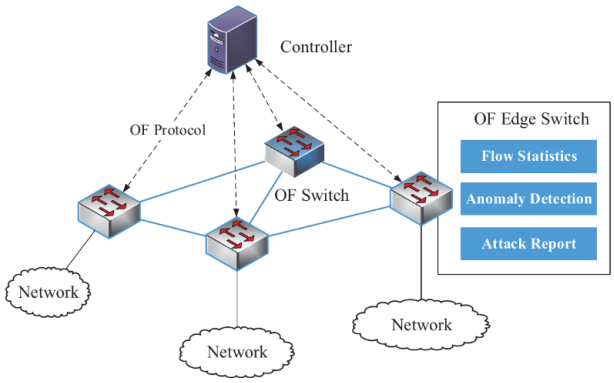
پژوهش انجام شده در [۱۵]، یک چارچوب[۲۸] که Avant Guard نام دارد را معرفی می‌کند و در برابر حملات DDoS از نوع TCP SYN Flood، هر دو عملکرد تشخیص و مقابله را فراهم می‌سازد. در خود سوییچ‌ها، دو نوع ماژول با نام‌های Conncection Migration (CM) و Actuating Triggers (ATs) معرفی شده‌اند (شکل ۶). ماژول CM، درخواست‌هایی که از نوع TCP SYN باشند را پراکسی[۲۹] کرده و براساس نتیجه طبقه‌بندی آن‌ها، ممکن است اجازه ارسال درخواست‌ها به هدف اصلی را بدهد. ماژول‌های AT، با تشخیص حجم بالای درخواست‌ها، یک رویداد از پیش تعیین شده در کنترلر را فعال می‌کنند تا کنترلر با افزودن سطرهای جدید به جدول جریان سوییچ‌ها، باعث کاهش زمان پاسخ شود. ایرادهای این راه‌حل در پیچیدگی زیاد سوییچ‌ها و محافظت از تنها یک نوع (TCP SYN Flooding) از حملات DDoS است.

در [۱۶]، از انتروپی استفاده می‌شود و راه‌حل پیشنهادی در سوییچ‌های لبه[۳۰] که مسئول انتقال ترافیک از میزبان‌ها به درون شبکه هستند و از پروتکل OpenFlow پشتیبانی می‌کنند، اجرا می‌گردد (شکل ۷). با محاسبه انتروپی برای هر آدرس آی‌پی مقصد، در صورتی که مقدار انتروپی کمتر از آستانه مشخصی باشد، حمله DDoS تشخیص داده می‌شود. دو مزیت این روش در امکان تشخیص هدف حمله، کاهش بار ناشی از تجمیع جریان‌ها در کنترلر، و کاهش سربار ترافیکی ناشی از ارتباط با کنترلر (در مقایسه با

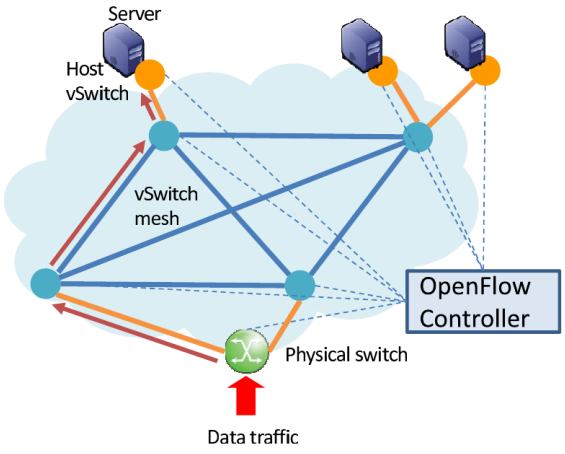
[28] Framework
[29] Proxy
[30] Edge Switches



شکل ۶- افزودن دو ماژول AT و CM در سطح سوییچ‌ها در چارچوب Avant Guard [۱۵]



شکل ۷- انجام هر سه روند آمارگیری، تشخیص و ارائه گزارش در سوییچ‌های لبه [۱۶]

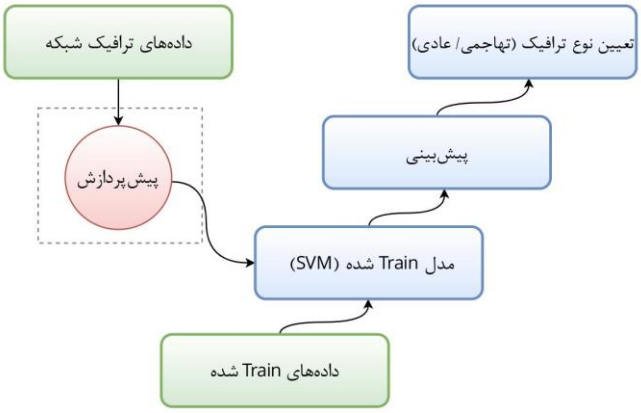


شکل ۸- شبکه همپوشان و سوییچ‌های مجازی در روش مقابله‌ی اسکاچ [۱۷]

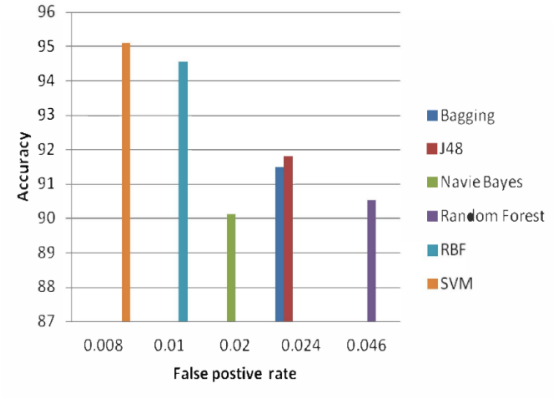
حالتی که تشخیص باید در کنترلر صورت گیرد) است. از معایب این روش، می‌توان به پیچیده شدن سوییچ‌ها و عدم امکان تفکیک بسته‌های مجاز از سایر بسته‌ها اشاره کرد.

در [۱۷]، ارتباط میان کنترلر و سوییچ‌ها به عنوان یک مشکل اصلی یاد شده و روش مقابله‌ی اسکاچ[۳۱] مطرح شده است. هنگامی که سوییچ اصلی دچار اضافه بار می‌شود، چندین سوییچ مجازی (vSwitch) که اجزای شبکه همپوشان[۳۲] اسکاچ را تشکیل می‌دهند، ایجاد شده و جریان‌های جدید به آن‌ها تونل[۳۳] می‌شوند (شکل ۸). در صورت عبور میزان بسته‌ها از مقداری معین، بسته‌ها دور انداخته[۳۴] می‌شوند و این موضوع، یکی از مشکلات این راهکار است.

[31] Scotch
[32] Overlay network
[33] Tunnel
[34] Drop



شکل ۹- روند کلی مورد استفاده در تشخیص حمله DDoS



شکل ۱۰- مقایسه دقت و نرخ مثبت کاذب برای الگوریتم‌های یادگیری ماشین در تشخیص حمله DDoS [۱۸]

۲.۲.۶. بر اساس یادگیری ماشین

مشابه با روش‌های آماری، در روش‌های یادگیری ماشین نیز به‌طور معمول باید مکانیزم دفاعی هدف در بازه‌ای که ترافیک عادی در شبکه جریان دارد، مورد آموزش[۳۵] قرار گیرد و سپس بسته‌های مخرب، به کمک الگوریتم‌های یادگیری ماشین، طبقه‌بندی شوند. سازوکار مطرح شده در [۱۸]، به کمک طبقه‌بندی[۳۶] براساس ماشین بردار پشتیبانی (SVM[37])، عملکرد تشخیص را فراهم می‌کند. شکل ۹، روند کلی استفاده از یک مدل ایجاد شده به کمک الگوریتم SVM و پیش‌بینی نوع ترافیک در این سازوکار را بیان می‌کند. در این سازوکار، با آزمودن کارایی الگوریتم‌های مختلف یادگیری ماشین و هدف حمله DDoS قرار گرفتن کنترلر، به این نتیجه رسیده‌اند که استفاده از SVM، علیرغم این‌که نسبت به سایر روش‌ها موجب صرف زمان بیشتری می‌شود، عملکرد بهتری خواهد داشت (شکل ۱۰).

۷. نتیجه‌گیری

در این پژوهش، چند سناریو از حمله‌های DDoS که ممکن است در محیط SDN رخ دهند، عنوان شدند. سپس، چند تکنیک برای دفاع دربرابر این حمله‌ها مطرح شد و طبقه‌بندی مقایسه‌ای آن‌ها ارائه گردید. در زمینه راه‌حل‌های مبتنی بر یادگیری ماشین، تحقیقات محدودتری وجود دارد.

برخی از راه‌حل‌ها به استفاده از سوییچ‌های هوشمند تأکید دارند که در این زمینه باید به مشکل پایبند بودن به چارچوب بنیادین SDN توجه کرد.

همچنین یک جدول مقایسه‌ای از راهکارهایی که مطرح شد، در جدول ۲ مشاهده می‌شود.

[35] Train
[36] Classification
[37] Support Vector Machine

شماره مرجع	عنوان کوتاه راهکار	استفاده از سوییچ‌های هوشمند	مقابله	تشخیص
۸	جایگزین کردن سطرهای جدول جریان	✗	✓	✗
۹	ارائه یک سازوکار برای به‌روزرسانی جداول سوییچ‌ها	✗	✓	✗
۱۰	اولویت‌دهی براساس راندرابین مبتنی بر هش	✗	✓	✗
۱۱	اولویت‌دهی با ایجاد صف در سوییچ‌ها	✗	✓	✗
۱۲	جداسازی عملکردها در کنترلر	✗	✓	✓
۱۳	جداسازی عملکردها در کنترلر	✓	✓	✗
۱۴	سازوکار Flowfence	✓	✓	✓
۱۵	آوانت گارد	✓	✓	✓
۱۶	تشخیص مبتنی بر انتروپی	✗	✗	✓
۱۷	روش مقابله اسکاچ	✗	✓	✗
۱۸	طبقه‌بندی براساس SVM	✗	✗	✓

جدول ۲- مقایسه کلی از سازوکارهای بررسی شده

۸. مراجع

1. *Kalkan, Kubra, et al. "Defense Mechanisms against DDoS Attacks in SDN Environment," 9, 2017, pp. 175–79.*
2. *https://techcrunch.com/2016/10/10/hackers-release-source-code-for-a-powerful-ddos-app-called-mirai/*
3. *Q. Yan et al., "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," IEEE Commun. Surveys Tutorials, vol. 18, no.1, 2016, pp. 602–22.*
4. *D. Ma, Z. Xu, and D. Lin, "Defending Blind DDoS Attack on SDN Based on Moving Target Defense," Proc. Int'l. Conf. Security and Privacy in Commun. Systems, Springer, 2014, pp. 463–80.*
5. *M. S. Kang, S. B. Lee, and V. D. Gligor, "The Crossfire Attack," Proc. 2013 IEEE Symp. Security and Privacy, 2013, pp. 127–41.*
6. *A. Studer and A. Perrig, "The Coremelt Attack," Proc. Euro.Symp. Research in Computer Security, Springer, 2009, pp. 37–52.*
7. *K. Li, W. Zhou, P. Li, J. Hai and J. Liu, "Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics," 2009 Third International Conference on Network and System Security, Gold Coast, QLD, Australia, 2009, pp. 9-17.*
8. *N. Tri, T. Hiep, and K. Kim, "Assessing the Impact of Resource Attack in Software Defined Network," Proc. 2015 Int'l. Conf. Info. Networking, 2015, pp. 420–25.*
9. *N. P. Katta, J. Rexford, and D. Walker, "Incremental Consistent Updates," Proc. 2nd ACM SIGCOMM Wksp. Hot Topics in Software Defined Networking, 2013, pp. 49–54.*
10. *S.-W. Hsu et al., "Design a Hash-Based Control Mechanism in vSwitch for Software-Defined Networking Environment," Proc. 2015 IEEE Int'l Conf. Cluster Computing, 2015, pp. 498–99.*
11. *S. Lim et al., "Controller Scheduling for Continued SDN Operation under DDoS Attacks," Electronics Letters, vol. 51, no. 16, 2015, pp. 1259–61.*
12. *A. Zaalouk et al., "OrchSec: An Orchestrator-Based Architecture for Enhancing Network-Security Using Network Monitoring and SDN Control Functions," Proc. IEEE Network Operations and Mgmt. Symp., 2014, pp. 1–9.*
13. *D. Chourishi et al., "Role-Based Multiple Controllers for Load Balancing And Security in SDN," Proc. 2015 IEEE Canada Int'l. Humanitarian Technology Conf., 2015, pp. 1–4.*

14. A. *F. M. Piedrahita et al., "Flowfence: A Denial of Service Defense System for Software Defined Networking," Proc. Global Info. Infrastructure Networking Symp., 2015, Oct.2015, pp. 1–6.*

15. *S. Shin et al., "Avant-Guard: Scalable and Vigilant Switch Flow Management in Software- Defined Networks," Proc.2013 ACM SIGSAC Conf. Computer Commun. Security, ACM, 2013, pp. 413–24.*

16. *R. Wang, Z. Jia, and L. Ju, "An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking," Proc. 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1. 2015,pp. 310–17.*

17. *A. Wang et al., "Scotch: Elastically Scaling up SDN Control Plane using vSwitch Based Overlay," Proc. 10th ACM Int'l. Conf. Emerging Networking Experiments and Technologies, 2014, pp. 403–14.*

18. *R. Kokila et al., "DDoS Detection and Analysis in SDN-Based Environment Using Support Vector Machine Classifier," Proc. 2014 IEEE Sixth Int'l. Conf. Advanced Computing, 2014, pp. 205–10*