تشخیص و کاهش اثر حملات DDOS در شبکه‌های نرم‌افزار محور با استفاده از تکنیک فاصله جفری

مژگان قصابی[۱]، دانشجوی کارشناسی ارشد؛ محمود دی‌پیر[۲]، استادیار

۱- دانشکده مهندسی برق و کامپیوتر – دانشگاه آزاد اسلامی واحد علوم تحقیقات - تهران - ایران - mozhgan.ghasabi@srbiau.ac.ir
۲- دانشکده رایانه و فناوری اطلاعات - دانشگاه علوم و فنون هوایی شهید ستاری - تهران - ایران - mdeypir@ssau.ac.ir

چکیده: شبکه‌های نرم‌افزار محور اخیراً کاربردهای گسترده‌ای در اینترنت به‌منظور استفاده بهینه از پهنای باند و مدیریت ترافیک پیدا کرده‌اند. در معماری این نوع شبکه‌ها، بخش کنترل از بخش داده جدا شده و به صورت متمرکز تحت عنوان خدمت دهنده کنترلر، سوئیچ‌های داده را مدیریت می‌کند. در این نوع شبکه‌ها، بخش کنترل نسبت به حملات منع خدمت آسیب‌پذیر بوده و مهاجم با تزریق مداوم بسته‌های درخواست جعلی، پردازش‌های سنگین را برای کنترلر تحمیل می‌کند که درنهایت به غیرقابل دسترس شدن کنترلر و عدم خدمت‌دهی شبکه به کاربران عادی منجر می‌گردد. به دلیل اثرگذاری بیشتر این حملات در شبکه‌های نرم‌افزار محور نسبت به شبکه‌های سنتی، حفاظت از این معماری در مقابل حملات منع خدمت بسیار حائز اهمیت است. ما در این مقاله به بررسی و شبیه‌سازی این حملات در معماری شبکه‌های نرم‌افزار محور پرداخته و با بهره‌گیری از امکانات منحصربه‌فرد این معماری، الگوریتم جدیدی برای تشخیص و کاهش اثر حملات منع خدمت توزیع شده ارائه داده‌ایم. در الگوریتم پیشنهادی از فرمول آماری فاصله جفری به‌منظور شناسایی حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور، استفاده شده است. ما برای ایجاد زیرساخت لازم برای شبکه نرم‌افزار محور آزمایشی و ارزیابی الگوریتم پیشنهادی از شبیه‌ساز مینی نت در محیط سیستم‌عامل لینوکس استفاده کرده‌ایم. آزمایش‌های انجام شده در این شبیه‌ساز، کارآیی روش پیشنهادی و برتری آن نسبت به روش‌های قبلی را نشان می‌دهند.

واژه‌های کلیدی: شبکه‌های نرم‌افزار محور، حملات منع خدمت توزیع شده، فاصله جفری، کاهش اثر حملات.

Detection and mitigation of DDOS attacks in Software Defined Networks using the Jeffrey distance

M. Ghasabi[1], MSc Student; M. Deypir[2], Assistant Proffessor

1- Department of Computer, Science and Research branch, Islamic Azad University, Tehran, Iran, Email: mozhgan.ghasabi@srbiau.ac.ir
2- Department of Science and Technology, University of Shahid Sattari, Tehran, Iran, Email: mdeypir@ssau.ac.ir

Abstract: Recently, software defined networks have wide applications on the Internet in order to optimize the use of bandwidth and better traffic management. In Software Defined Network (SDN), the control plane and data plane of the networks are decoupled. In this architecture, the control plane, centrally manages switches by an special server named controller. In SDN, the controller is so vulnerable to DDOS attacks. By injecting spoofed request packets continuously, attackers make a burdensome process which cause the controller to be unreachable and thus denial of services for legitimate users. Due to the augmented impact of these attacks on the software defiend networks rather than traditional networks, need for protection of such network against the attack is very much important. In this paper we will review and simulate DDOS attacks on SDN. We afterward propose a novel detection and mitigation algorithm which takes advantage of unique features of the SDN architecture. In this algorithm, for detecting DDOS attacks in SDN a statistical method based on Jeffrey distance is used. We created the necessary infrastructure for software-driven network and evaluated the proposed method using Mininet simiulator on the Linux operating system. Our experiments performed in the simulator, showed the efficiency of the proposed method and its superiority compared to previous approaches.

Keywords: Software defined networks, distributed denial of service, Jeffrey distance, attack mitigation.

تاریخ ارسال مقاله: ۱۳۹۵/۱۰/۰۵
تاریخ اصلاح مقاله: ۱۳۹۵/۱۱/۲۳ و ۱۳۹۶/۰۶/۱۶
تاریخ پذیرش مقاله: ۱۳۹۶/۰۷/۰۴
نام نویسنده مسئول: محمود دی‌پیر
نشانی نویسنده مسئول: ایران - تهران - ضلع جنوبی فرودگاه مهرآباد - دانشگاه علوم و فنون هوایی شهید ستاری - دانشکده رایانه و فناوری اطلاعات.

۱- مقدمه

بسیاری از اصول شبکه‌های رایانه‌ای، در دو دهه اخیر بدون تغییر باقی مانده‌اند. شبکه‌های کنونی از سوئیچ و مسیریاب‌های نسبتاً پیچیده ساخته شده‌اند. از آنجایی‌که این دستگاه‌ها توسط سازندگان مختلفی با سیستم‌عامل و رابط‌های اختصاصی ساخته شده‌اند، برای ساخت شبکه‌های ناهمگن نیاز به استخدام متخصصان مربوط به هر دستگاه با برندهای متفاوت خواهیم داشت. همچنین ساخت چنین شبکه‌هایی امکان اشتباهات پیکربندی و ناسازگاری بین نسخه‌های مختلف دستگاه‌های تولید شده توسط سازندگان متفاوت را افزایش می‌دهد. علاوه بر این، هر مسیریاب دید جزئی نسبت به کل شبکه داشته و به کمک سایر مسیریاب‌ها و تبادل ترافیک کنترلی بسته‌های شبکه را هدایت می‌کند.

معماری شبکه‌های نرم‌افزار محور[۱] (SDN) به‌منظور ایجاد تغییرات در معماری شبکه‌های سنتی و استفاده بهینه از منابع شبکه برای رسیدن به شبکه‌های هوشمند به وجود آمده است [۱]. این معماری در ارائه قابلیت اطمینان، کارآمدی، سادگی، انعطاف‌پذیری و قابلیت برنامه‌ریزی با هزینه کم موفقیت چشم‌گیری را نشان داده است[۲]. در این معماری ارسال داده‌ها و انجام پردازش‌ها به کمک پروتکلی به نام Open Flow از یکدیگر جدا شده‌اند. این جداسازی مزایایی از جمله کنترل متمرکز بر تصمیمات انتقال داده، به‌روزرسانی پویای قوانین انتقال داده، پیکربندی انعطاف‌پذیر و آسان‌تر شبکه، قابلیت برنامه‌ریزی کنترلر و زیرساخت‌های شبکه‌ای را به ارمغان می‌آورد[۳]. علی‌رغم مزایای ذکر شده، معماری شبکه‌های نرم‌افزار محور به دلیل ویژگی‌های ذاتی کنترلر متمرکز می تواند به‌طور بالقوه به‌عنوان هدفی برای مهاجمان تبدیل شود [۴].

با تکامل شبکه، حملات به شبکه نیز تکامل‌یافته است. یکی از تهدیدات فعلی هر شبکه‌ای، حملات منع خدمت توزیع شده[۲] (DDOS) است که با هدف ایجاد اختلال در یک شبکه یا غیرقابل دسترس سازی خدمات برای کاربران انجام می‌گیرد. در طی سال‌های پیش حملات منع خدمت توزیع شده به دلیل تغییر الگوی کاری مطابق با توسعه راه‌حل‌های مقابله‌ای توسط مهاجمان، به تهدیدی روزافزون در اینترنت تبدیل شده است[۵]. حملات منع خدمت توزیع شده به‌عنوان بزرگ‌ترین تهدید اقتصادی و سرمایه‌گذاری محسوب می‌شود[۶]، زیرا بر روی کارآیی شبکه، میزان تأخیر و نرخ دور ریختن بسته‌های مجاز تأثیر می گذارد. این حملات ممکن است تمام شبکه را فلج کرده یا عملکرد آن را متوقف کنند. اگرچه بر پیچیدگی‌های فنی و تکنیکی این حملات روزبه‌روز افزوده شده، اما مهاجمان برای راه‌اندازی این حملات نیاز به دانش و مهارت فنی بالا درباره سیستم قربانی و تکنیک‌های راه‌اندازی حملات ندارند. امروزه برخی ارائه‌دهندگان از جمله بوترز حملات منع خدمت توزیع شده را به‌عنوان یک سرویس در ازای مبلغی به مشتریان ارائه می‌دهند[۷].

حملات منع خدمت توزیع شده برای شبکه‌های مبتنی بر پروتکل Open Flow می‌تواند بسیار مخرب‌تر باشد، زیرا در این شبکه‌ها یک جریان مداوم بین کنترلر و سوئیچ‌ها برقرار است. ارتباط بین سوئیچ‌ها و کنترلر ممکن است مهاجمان را تحریک کند که این جریان را از مسیر اصلی خارج کرده و فعالیت معمول شبکه را مختل سازند. در حمله به یک شبکه نرم‌افزار محور، قدم اول شناسایی SDN بودن شبکه است. اغلب شبکه‌های سنتی، جداول انتقال پیش تنظیم شده‌ای دارند، بنابراین در این شبکه‌ها نیازی به زمان اضافی برای پردازش و ایجاد یک جریان برای بسته‌های ورودی جدید نیست. ولی در شبکه‌های نرم‌افزار محور، کنترلر بایستی یک زمان کوتاهی را برای جریان‌های ورودی بسته‌های جدید اختصاص دهد، بنابراین زمان بیشتری را برای پردازش اولین بسته در مقایسه با سایر بسته‌ها صرف می‌کند. بر اساس این دانش، مهاجم می‌تواند از زمان پاسخ به اولین بسته نسبت به سایر بسته‌ها به شناسایی شبکه‌های نرم‌افزار محور بپردازد. اگر اختلاف زمانی بیشتر از حدآستانه تعریف شده باشد؛ شبکه به‌عنوان شبکه نرم‌افزار محور شناخته می‌شود[۸].

بعد از شناسایی نوع معماری شبکه، مهاجم با تزریق حجم انبوهی از بسته‌های جعلی، موجب اشغال منابع محدود کنترلر شده و پردازش بسته‌ها در کنترلر به‌واسطه غیرقابل دسترس شدن کنترلر مختل می گردد. درنهایت کیفیت خدمات پایین آمده و کل جداول سرریز می‌شوند و بعد از آن سوئیچ‌ها قادر به خدمت رسانی به سایر بسته‌های جدید نخواهند بود، در نتیجه شبکه از کار می‌افتد. از آنجایی‌که کنترلر شبکه‌های نرم‌افزار محور نسبت به حملات منع خدمت توزیع شده آسیب‌پذیر هستند، بنابراین بایستی این حملات قبل از آسیب رسیدن به کنترلر شبکه تشخیص داده شوند. هدف اصلی ما در این مقاله تشخیص و کاهش اثر حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور است. برای رسیدن به این هدف، یک روش مؤثر و متناسب با ساختار و ویژگی‌های کنترلر شبکه‌های نرم‌افزار محور پیشنهاد شده است. در این روش برای نخستین بار از فرمول آماری فاصله جفری به‌منظور تشخیص حملات منع خدمت در شبکه‌های نرم‌افزار محور استفاده شده است.

در مقاله [۹] روش جداسازی مکان‌یاب[۳] به‌منظور مقابله با حملات منع خدمت توزیع شده پیشنهاد شده است. این روش امکان کنترل شبکه‌های بات توسط مهاجمان را دشوار می‌سازد. در مقاله [۱۰] تکنیک تشخیص حمله منع خدمت توزیع شده مبتنی بر IP آدرس مبدأ ارائه شده است. این روش به‌جای نظارت بر ترافیک، به آدرس‌هایIP مبدأ بسته‌های جدید نظارت می‌کند. در مقاله [۱۱] برای تشخیص حملات منع خدمت توزیع شده، روش مبتنی بر مدل‌سازی تغییرات میانگین و واریانس وضعیت‌های ترافیکی شبکه پیشنهاد شده است. در مقاله [۱۲] یک روش تشخیص مقایسه‌ای مبتنی بر ضریب همبستگی پیرسون ارائه شده است. این روش قادر به تشخیص تمایز بین ویژگی‌های بسته‌های ورودی ترافیک حمله از ترافیک عادی است. در مقاله [۱۳] یک سیستم تشخیص حمله منع خدمت توزیع شده بر اساس تحلیل همبستگی چند متغیره پیشنهاد شده است. در این روش از همبستگی هندسی ترافیک‌ها

برای شناسایی ویژگی‌های شبکه استفاده می‌شود. این سیستم با یادگیری الگوهای ترافیکی مجاز، قادر به تشخیص حمله است. در مقاله [۱۴] برای تشخیص حمله منع خدمت توزیع شده یک الگوریتم مبتنی بر پیش‌بینی ترافیک شبکه و تئوری بی‌نظمی[۴] ارائه شده است. در این روش پیش‌بینی ترافیک شبکه براساس اطلاعات به‌دست‌آمده از پیش‌پردازش ترافیک در یک محدوده زمانی با استفاده از مدل خطی AR انجام می‌شود. در گام بعدی با تحلیل خطاهای پیش‌بینی ترافیک توسط تئوری بی‌نظمی، ناهنجاری‌ها شناسایی شده، سپس با آموزش شبکه‌های عصبی حملات تشخیص داده می‌شوند.

در مقاله [۱۵] روش تحلیل تغییرات لیاپانوف مبتنی بر آنتروپی برای تشخیص حملات پیشنهاد شده است. در این روش پیش‌پردازش دنباله آنتروپی‌های IP آدرس‌های مبدأ و مقصد در واحدهای زمانی با استفاده از مدل خطی AR انجام می‌شود. سپس با تحلیل نرخ توان تفکیک بین این مقادیر، حدآستانه برای تشخیص حمله تعریف می‌گردد. در مقاله [۱۶] برای تشخیص حملات منع خدمت توزیع شده در شبکه‌های VOIP روش آماری فاصله هلینگر پیشنهاد شده است. در این مقاله به کمک یک سیستم تشخیص حمله که بین ترافیک شبکه در حالت حمله و حالت نرمال تمایز قائل می‌شود، تمامی جریان‌های ترافیک فعلی نسبت به یک الگوی خاصی سنجیده می‌شوند و حالت انحراف با اندازه‌گیری فاصله هلینگر بین دو زمان آموزشی و زمان تست به دست می‌آید.

در بررسی‌های مربوط به شبکه‌های نرم‌افزار محور برخی مقالات به بررسی اجزا و رابط‌های این معماری پرداختند و مشخصات شبکه‌های نرم‌افزار محور و قابلیت‌های کنترلی این ساختار و تکامل آن را مورد مطالعه قرار داده‌اند. پژوهش‌ها در زمینه امنیت مبتنی بر شبکه‌های نرم‌افزار محور در آغاز راه است که دلیل این امر می‌تواند جدید بودن این معماری باشد. حملات منع خدمت در برخی از تحقیقات اخیر مورد توجه قرار گرفته است. در مقاله [۱۷] تهدید اشباع منابع کنترلر و سرریز جداول جریان را مورد بررسی قرار دادند. در این مقاله روشی بر اساس تغییر و اصلاح ساختار سوئیچ‌ها برای مقابله با این تهدیدات ارائه شده است. در مقاله [۱۸] برای تشخیص حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور، تکنیک یادگیری ماشین نقشه‌های خودسازمانده[۵] (SOM) پیشنهاد شده است. در این روش، ماشین خودسازمانده رفتارهای شبکه را از طریق جمع‌آوری آمار جریان‌ها از سوئیچ‌های Open Flow آموزش می‌بینند. در مقاله [۱۹] برای مقابله با حملات منع خدمت، یک شبکه نرم‌افزار محور مبتنی بر دیوار آتش بر بالای کنترلر POX پیشنهاد شده است.

در مقاله [۲۰] به‌منظور تشخیص حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور، یک سیستم تشخیص نفوذ چندگانه[۶] را پیشنهاد دادند. در این روش توزیع جریان ترافیک در بین سیستم‌های با استفاده از الگوریتم خوشه‌بندی گروه جریان‌ها براساس اطلاعات مسیریابی و نرخ جریان داده‌ای انجام می‌گیرد. در مقاله[۲۱] برای دفاع علیه حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور، سیستم جابجایی هدف[۷] پیشنهاد شده است. در این روش برای مقابله با مشکل اشباع منابع کنترلر، حوضی از چندین کنترلر در نظر گرفته می شود و کنترلرها با توجه به چگالی جریان ترافیک‌ها، به‌صورت پویا جایگزین می‌شوند. در مقاله [۲۲] مکانیسم تشخیص حملات منع خدمت توزیع شده مبتنی بر تکنیک آماری آنتروپی در شبکه‌های نرم‌افزار محور ارائه شده است. در این روش آنتروپی بر اساس IP آدرس مقصد بسته‌های ورودی، محاسبه شده و با حدآستانه مقایسه می‌گردد. اگر مقدار آنتروپی در ۵ دوره متوالی از مقدار حدآستانه کمتر باشد؛ به‌عنوان حمله تفسیر می‌شود.

ادامه این مقاله به شرح زیر سازماندهی شده است. در بخش دوم ساختار معماری شبکه‌های نرم‌افزار محور و تأثیرات حملات منع خدمت توزیع شده بر روی این معماری بیان می‌گردد. در بخش سوم به بیان مسئله پرداخته می‌شود. در بخش چهارم راه‌حل پیشنهادی و چگونگی استفاده از تکنیک فاصله جفری در تشخیص حملات منع خدمت توزیع شده شرح داده می‌شود. بخش پنجم به ارزیابی روش پیشنهادی پرداخته و روش پیشنهادی با سایر روش‌های ارائه شده مقایسه می‌گردد. این مقاله در بخش ششم جمع‌بندی و نتیجه‌گیری می‌شود.

۲- شبکه‌های نرم‌افزار محور

پایه‌های معماری نوین شبکه‌های نرم‌افزار محور حاصل تلاش‌های دو استاد علوم کامپیوتر است. نیک مککون از استنفورد و اسکات شنکر از برکلی به همراه برخی از دانشجویان خود، این مفهوم را در سال ۲۰۰۲ تعریف کردند[۲۳]. پروژه آن‌ها اتان نام داشت و هدف آن افزایش امنیت شبکه با استفاده از یک سری پروتکل مبتنی بر جریان داده بود [۲۴].

معماری شبکه‌های نرم‌افزار محور بر اساس ایده جداسازی منطق نرم‌افزاری بستر کنترلی از بستر سخت‌افزاری انتقال داده‌ها شکل گرفته است. در شبکه‌های نرم‌افزار محور بخش کنترل[۸] و بخش داده[۹] از هم جدا شده است. سوئیچ‌ها، بسته‌های ورودی را مورد پردازش قرار نمی دهند، بلکه برای تطبیق بسته‌های ورودی به جدول جریان مراجعه می کنند و اگر تطبیقی بین رکوردهای جدول و فیلد بسته‌های ورودی نیافتند؛ بسته را به‌عنوان بسته جدید تلقی کرده و برای پردازش به سمت کنترلر ارسال خواهند کرد. بسته‌هایی که برای تعیین وضعیت از طرف سوئیچ‌ها به کنترلر ارسال می‌شوند بسته‌های packet-in نامیده می‌شوند. در واقع کنترلر یک سیستم‌عامل در شبکه‌های نرم‌افزار محور است که بسته‌های دریافتی را پردازش کرده و در مورد بسته‌ها طبق ماژول‌های موجود تصمیم‌گیری می‌کند[۲۵].

راهبری توسعه شبکه‌های نرم‌افزار محور و تدوین استانداردهای مربوطه بر عهده بنیاد شبکه‌های باز[۱۰] است که یک تشکل غیرانتفاعی است. از جمله مشهورترین استانداردهای تدوین شده توسط این بنیاد، پروتکل Open Flow است که چگونگی برقراری ارتباط بین بستر کنترلی و بستر ارتباطی تجهیزات مورد نیاز در شبکه‌های نرم‌افزار محور را تبیین می‌کند. این استاندارد در حقیقت اولین استانداردی است که خاص این

گونه شبکه‌ها تعریف شده است. در شبکه‌های نرم‌افزار محور ارتباط بین سوئیچ و کنترلر از طریق پروتکل Open Flow انجام می‌گیرد[۲۶]. کنترلر مغز و سیستم‌عامل شبکه‌های نرم‌افزار محور محسوب می‌شود که می تواند دارایی‌های شبکه را تغییر داده و قوانین جدیدی در سوئیچ‌ها وضع نماید. در این معماری کانال امن شاهراه ارتباطی بین کنترلر و سوئیچ‌های داده را تشکیل می‌دهد. اگر تعداد بسته‌های ورودی بیشتر از پهنای باند کانال امن باشد؛ کانال امن آسیب‌پذیر خواهد بود. هنگامی که کانال امن قطع شود؛ ساختار شبکه‌های نرم‌افزار محور از بین خواهد رفت، زیرا مکانیزمی برای تصمیم‌گیری وجود نخواهد داشت.

یکی از تهدیدات جدی برای شبکه‌های نرم‌افزار محور حملات منع خدمت توزیع شده است که به‌صورت مستقیم بر کنترلر این شبکه‌ها تأثیر می‌گذارد. هدف مهاجم در این نوع حمله غرق کردن کنترلر با بسته‌های packet-in است. اغلب حملات منع خدمت توزیع شده از آدرس مبدأ جعلی استفاده می‌کنند. این بسته‌ها به‌عنوان بسته ورودی جدید در سوئیچ‌ها تفسیر شده و برای پردازش و تعیین وضعیت به کنترلر ارسال خواهند شد. یکی دیگر از تأثیرات حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور، پر کردن جدول جریان سوئیچ‌ها است. در این حملات به دلیل حجم بالای ترافیک ورودی، جداول از جریان‌های جعلی پر می‌گردد.

۳- بیان مسئله

هر فناوری جدید، حملات و تهدیداتی را به همراه خواهد داشت. در شبکه‌های نرم‌افزار محور هم به دلیل تمرکز کنترل، حملات منع خدمت تهدیدی جدی محسوب می‌شوند. حمله منع خدمت حمله‌ای است که هدف آن از کار اندازی سیستم هدف با استفاده از هدر دادن منابع آن است [۲۷]. حمله منع خدمتی که مهاجم از سیستم‌های زیادی به‌طور هم‌زمان‌برای راه‌اندازی حملات علیه یک میزبان راه دور استفاده کند، به‌عنوان حمله منع خدمت توزیع شده تلقی می‌شود. مهاجمان برای پیشبرد حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور، ممکن است حجم زیادی از ترافیک با مشخصه‌های متغیر تصادفی با استفاده از مولدهای ترافیکی ایجاد کنند. چنین حملاتی با دو هدف اصلی ایجاد می‌شود. هدف اول اشباع جداول جریان سوئیچ‌ها با قوانین غیرمجاز است که این امر می‌تواند قابلیت سوئیچ‌ها را برای پذیرش قوانین جدید و همچنین هدایت ترافیک مختل سازد. هدف دوم مهاجمان از فرستادن چنین حجم انبوهی از جریان این است که سیل عظیم بسته‌ها، کنترلر را مشغول سازد تا از پاسخ به درخواست‌های مجاز از طرف سوئیچ‌ها بازماند[۲۸].

در اثر حمله مهاجم، کیفیت خدمات شبکه پایین آمده و درنهایت کل جداول سرریز شده و بعد از آن سوئیچ‌ها قادر به خدمت رسانی به سایر بسته‌های جدید نخواهند بود. به‌بیان‌دیگر؛ اگر پردازش بسته‌ها در کنترلر مختل شود، شبکه توان پردازشی و کنترلی نخواهد داشت و معماری شبکه‌های نرم‌افزار محور از کار خواهد افتاد، بنابراین حفاظت از کنترلر در معماری‌های شبکه‌های نرم‌افزار محور امری ضروری است. اگر تشخیص در مراحل اولیه حملات و قبل از آسیب رسیدن به کنترلر انجام گیرد؛ می‌توان اقدامات مقابله‌ای را در شبکه‌های نرم‌افزار محور اعمال کرد.

با وجود اینکه تاکنون روش‌های متنوعی برای مقابله با حملات در شبکه‌های سنتی ارائه شده است[۲۹]، اما طبق بررسی‌های ما در زمینه تشخیص و مقابله با حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور مطالعات کافی انجام نگرفته و روش‌های مقابله‌ای متناسب با این ساختار ارائه نشده است. در اکثر مطالعات انجام شده در این زمینه، شبکه‌های نرم‌افزار محور همانند شبکه‌های سنتی در نظر گرفته شده و روش‌های مقابله‌ای سنتی در این شبکه‌ها اعمال شده است. در شبکه‌های نرم‌افزار محور به دلیل محدودیت‌های منابع کنترلر، روش‌های سنتی مقابله‌ای از جمله دیوار آتش و سیستم‌های تشخیص نفوذ و... در این شبکه‌ها ایده مناسبی نیست. همچنین خصوصیات انعطاف‌پذیری بالا و مدیریت آسان شبکه‌های نرم‌افزار محور، ابزار قدرتمندی را برای تشخیص و مقابله با حملات منع خدمت توزیع شده فراهم آورده است، بنابراین استفاده از روش‌های مقابله‌ای سنتی موجب عدم بهره‌گیری درست از مزایای این معماری می‌گردد.

مسئله ما در اینجا ارائه روشی مؤثر به‌منظور تشخیص و مقابله با حملات منع خدمت در شبکه‌های نرم‌افزار محور است که ضمن سادگی با بهره‌گیری از مزایای منحصربه‌فرد این معماری، کارآیی بهتری در مقایسه با روش‌های قبلی داشته باشند. با توجه به این‌که شبکه‌های نرم‌افزار محور هنوز به بلوغ لازم نرسیده‌اند، ارائه روش‌های کارا در این زمینه و تجمیع این روش‌ها با معماری کنونی این نوع شبکه‌ها می‌تواند در حفظ امنیت آن‌ها مؤثر باشد. از طرف دیگر؛ زمینه را برای اعتماد بیشتر به این شبکه‌ها و به‌کارگیری فراگیرتر آن‌ها فراهم کند.

۴- راه‌حل پیشنهادی

کنترل متمرکز شبکه‌های نرم‌افزار محور، امکانات مناسبی را برای ارزیابی میزان بسته‌های ورودی جدید به شبکه را فراهم می‌کند. ما از این فرصت فراهم شده توسط کنترلر، برای جمع‌آوری آمار بسته‌های ورودی جدید استفاده می‌کنیم و با ارائه مکانیسمی مبتنی بر تکنیک فاصله جفری، حمله منع خدمت توزیع شده را تشخیص داده و اقدامات مقابله‌ای به‌منظور کاهش اثر این حملات را با بهره‌گیری از امکانات منحصربه‌فرد کنترلر شبکه‌های نرم‌افزار محور، اعمال خواهیم کرد.

۴-۱- تکنیک فاصله جفری برای تشخیص حملات

در نظریه اطلاعات و آمار، فاصله آماری برای تعیین کمیت فاصله بین دو موجودیت آماری به کار گرفته می‌شود که این موجودیت آماری ممکن است متغیر احتمالی یا توزیع احتمال یک نمونه باشد. در واقع اندازه‌گیری فاصله آماری، تفاوت بین متغیرهای تصادفی را بیان می‌کند [۳۰]. تکنیک فاصله جفری (JD) روش آماری است که برای محاسبه

فاصله بین دو توزیع احتمال در فضای متناهی به کار می‌رود. اگر دو مجموعه توزیع احتمال P و Q در فضای متناهی، مطابق رابطه ۱ دارای احتمالات p_i و q_i باشند:

$$P = \{p_1, p_2, \dots, p_n\} \text{ و } Q = \{q_1, q_2, \dots, q_n\} \quad (۱)$$

با توجه به مثبت بودن مقادیر احتمالات روابط زیر را داریم:

$$p_i \gg 0\,,\ \ q_i \gg 0 \ \rightarrow\ \sum_i^n q_i = 1,\ \ \sum_i^n p_i = 1 \quad (۲)$$

فاصله جفری طبق فرمول رابطه ۳ محاسبه می‌شود:

$$JD = \sum_{i=1}^{n}\left((p_i - q_i)(\ln p_i - \ln q_i)\right) \quad (۳)$$

اندازه فاصله جفری همیشه مقداری مثبت است. هرگاه دو مجموعه توزیع احتمال P و Q برابر باشند، مقدار JD صفر می‌شود. هرچه این دو توزیع احتمال اختلاف بیشتری داشته باشند؛ مقدار فاصله جفری نیز افزایش می‌یابد[۳۱].

ما در این مقاله قصد داریم با به‌کارگیری امکانات شبکه نرم‌افزار محور و با استفاده از تکنیک فاصله جفری، یک مکانیسم تشخیص و کاهش اثر حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور ارائه دهیم. حدآستانه ثابت برای مکانیسم تشخیصی راه‌حلی مناسب و عملی نیست. ما در راه‌حل پیشنهادی برای ایجاد حدآستانه تطبیقی[۳۲] از تکنیک EWMA[۱۱] در شبکه نرم‌افزار محور استفاده خواهیم کرد. حدآستانه تطبیقی برای تکنیک جفری طبق روابط زیر قابل محاسبه است:

$$J_{n+1} = (1-\alpha).J_n + \alpha.JD_n \quad (۴)$$

$$\sigma_n = |J_n - JD_n| \quad (۵)$$

$$S_{n+1} = (1-\beta).S_n + \beta.\sigma_n \quad (۶)$$

$$J_{n+1}^{thre} = \lambda.J_{n+1} + \mu.S_{n+1} \quad (۷)$$

اساس ایده حدآستانه تطبیقی، پیش‌بینی مقادیر بعدی بر اساس مقادیر فعلی است. در رابطه‌های بالا JD_n مقدار فعلی فاصله جفری و J_n و J_{n+1} به ترتیب برآورد میانگین فاصله‌های جفری فعلی و بعدی می باشند. σ_n میزان انحراف J_{n+1} از JD_n است. S_n و S_{n+1} نیز بیانگر میانگین انحراف فاصله جفری فعلی از فاصله جفری بعدی هستند. با استفاده از مقادیر J_{n+1} و S_{n+1} مقدار حدآستانه تطبیقی بر اساس فرمول رابطه ۷ محاسبه می‌شود. در روابط ذکر شده، همه پارامترهای λ ، μ ،α و β قابل تغییر هستند.

۴-۲- محاسبات آماری فاصله جفری در روش پیشنهادی

برای محاسبه فاصله جفری ابتدا به مدت زمان معینی (Δt) جریان عبوری وضعیت عادی شبکه را نمونه‌گیری می‌کنیم. این دوره زمانی را فاصله زمانی آموزشی می‌نامیم. سپس به نمونه‌گیری وضعیت حمله می پردازیم که این دوره زمانی را نیز فاصله زمانی تست نام‌گذاری می‌کنیم که طول این دوره، با طول دوره فاصله زمانی آموزش برابر خواهد بود. در این مقاله ما IP آدرس مقصد را به‌عنوان متغیر احتمالی در نظر می‌گیریم. با استفاده از آمارهای به‌دست‌آمده در بازه‌های زمانی مشخص شده، مجموعه توزیع احتمال در فاصله زمانی آموزشی (p_i ها) و توزیع احتمال در فاصله زمانی تست (q_i ها) از طریق رابطه ۸ محاسبه می‌شوند:

$$P_i = x_i/n \quad (۸)$$

در این رابطه x_i تعداد تکرار بسته‌هایی با IP آدرس مقصد یکسان است و n تعداد بسته‌های موجود در بازه زمانی مشخص شده است. بدین ترتیب با داشتن دو مجموعه توزیع احتمالات، مقدار فاصله جفری و حدآستانه تطبیقی طبق رابطه ۳ و ۷ برای هر بازه زمانی محاسبه می گردد. زمانی‌که اعضای هر دو مجموعه، توزیع احتمالات تقریباً یکسان داشته باشند؛ مقدار فاصله جفری نزدیک عدد صفر خواهد بود. زمانی‌که توزیع احتمالات اعضای دو مجموعه دارای نوسانات زیاد باشد؛ مقدار فاصله جفری نیز افزایش خواهد یافت.

۴-۳- تشخیص حملات منع خدمت توزیع شده

توانایی تعیین کمیت تصادفی فاصله جفری، این روش را برای تشخیص حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور مناسب می سازد. در مکانیسم پیشنهادی ما، برای تشخیص حملات منع خدمت توزیع شده، احتمالات تکرار بسته‌هایی با IP آدرس مقصد یکسان هر بازه زمانی، در کنترلر مورد بررسی قرار می‌گیرد. ما در این مقاله برای دستیابی به‌دقت تشخیص بالا و هزینه محاسباتی پایین، طول بازه زمانی را ۵ ثانیه در نظر می‌گیریم و جدولی را در کنترلر برای ثبت و ذخیره اطلاعات مربوط به IP آدرس مبدأ و مقصد بسته‌های انتقالی و زمان ورود بسته از سمت سوئیچ به کنترلر تعریف می‌کنیم. همچنین در این جدول یک شمارنده M برای شمارش تعداد تکرار مربوط به هر IP آدرس مقصد هر بسته انتقالی و یک شمارنده L برای شمارش تعداد بسته‌ها در هر بازه زمانی تعریف می‌شود. در این مکانیسم، بسته‌های ورودی به کنترلر در هر بازه زمانی ۵ ثانیه‌ای بر طبق IP آدرس مقصد، مورد تجزیه‌وتحلیل قرار می‌گیرند. با توجه به مقادیر شمارنده‌های M و L توزیع احتمالات هر بازه زمانی طبق فرمول رابطه ۸ محاسبه می‌شود. سپس طبق فرمول رابطه ۳ و رابطه ۷ فاصله جفری و حدآستانه تطبیقی محاسبه می‌گردد. درنهایت این مقادیر باهم مقایسه می‌شوند. اگر مقدار فاصله جفری از حدآستانه مربوطه بیشتر باشد به‌عنوان حمله تفسیر خواهد شد.

۴-۴- کاهش اثر حملات منع خدمت توزیع شده

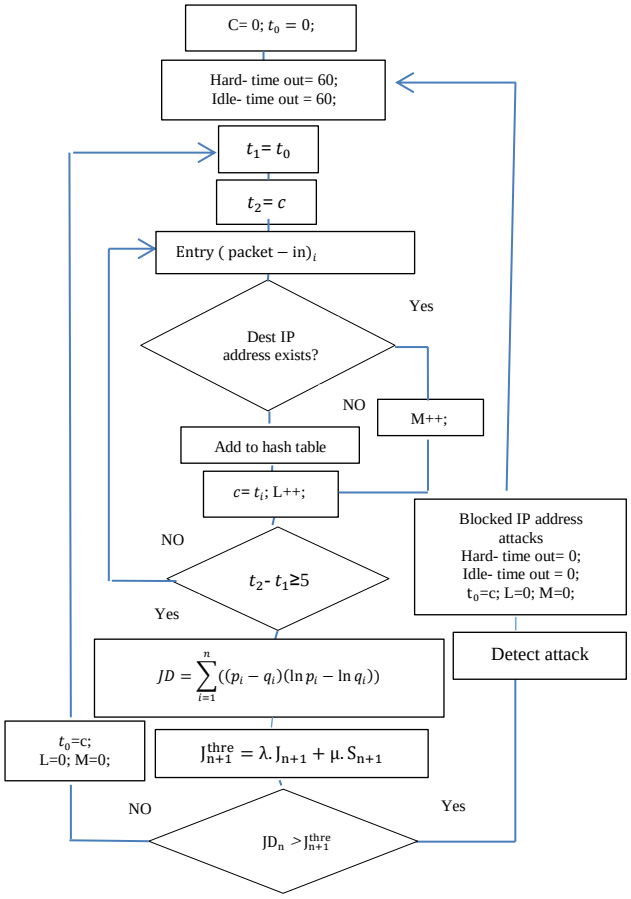
پس از تشخیص حمله بایستی اقدامات لازم جهت کاهش اثر حملات در شبکه اعمال گردد. کاهش اثر حملات منع خدمت توزیع شده، مجموعه‌ای از تکنیک‌ها برای حفاظت از شبکه مورد بررسی در برابر حملات منع خدمت توزیع شده است.

یکی از عملکردهای اختصاصی کنترلر در شبکه‌های نرم‌افزار محور، جمع‌آوری آمار از همه سوئیچ‌های مبتنی بر پروتکل Open Flow برای تشخیص جریان‌های غیرفعال است. مقدار idle - time out موجود در ماژول کنترلر، بیانگر مدت زمانی است که اگر طی این مدت، بسته یا ترافیکی که با جریان مربوطه مطابقت دا شته با شد، وارد نشود؛ جریان مذکور حذف می‌گردد. مقدار hard - time out نیز به کل مدت زمانی که یک جریان (حتی در صورت تداوم ار سال ترافیک از جریان مذکور) می‌تواند در جدول بماند، اطلاق می‌شود. پس از طی این مدت، جریان مذکور از جداول حذف می‌شود. در این روش پیشنهادی، با تنظیم مقادیر hard - time out و idle - time out می‌توان جریان‌های بسته‌های جعلی را کنترل نمود. در این مکانیسم پس از تشخیص حمله، برای جلوگیری از سرریز جداول و اشغال منابع کنترلر توسط بسته‌های حمله، اقدامات مقابله‌ای انجام می‌گیرد و با تغییر مقادیر time out بسته‌های حمله از جداول حذف شده و IP آدرس مبدأ مربوط به بسته‌های جعلی مسدود می‌شوند. به این ترتیب ما می‌توانیم تأثیرات حملات منع خدمت توزیع شده را در شبکه نرم‌افزار محور را کاهش دهیم.

۴-۵- جریان کاری روش پیشنهادی

مقادیر پیش فرض idle - time out وhard - time out در کنترلر Pox با ارقام ۶۰ و ۶۰ تنظیم شده است. در مکانیسم پیشنهادی همان‌طور که در شکل ۱ مشاهده می‌شود، مقادیر اولیه این ماژول‌ها را ۶۰ ثانیه و مقادیر متغیرهای زمانی c و t_0 با صفر مقداردهی اولیه می‌شوند. سپس IP آدرس مقصد اولین بسته ورودی مربوط به بازه زمانی ۵ ثانیه بررسی می‌شود. اگر مشخصات این بسته در جدول موجود بود، به تعداد شمارنده M مربوط به تعداد تکرار بسته‌هایی با IP آدرس مقصد بسته مورد نظر، یک واحد اضافه می‌گردد. در غیر این صورت، در جدول یک جریان جدیدی با مشخصات بسته مورد بررسی، ایجاد می‌شود. در مرحله بعدی به تعداد شمارنده L که مربوط به تعداد بسته‌های هر بازه زمانی است، یک واحد اضافه می‌گردد. همچنین زمان ورود بسته در متغیر زمانی c قرار داده می‌شود. در گام بعدی اندازه بازه زمانی برای تشخیص اتمام عملیات مربوط به یک بازه زمانی بررسی می‌شود. اگر اندازه بازه زمانی کمتر از ۵ ثانیه بود، بسته ورودی بعدی بررسی می‌شود. در صورت اتمام بازه زمانی عملیاتی، فاصله جفری و حدآستانه تطبیقی طبق توضیحات بخش ۴-۲ و ۴-۳ نسبت به اعضای متناظر مجموعه توزیع احتمالات دوره زمانی آموزشی محاسبه می‌گردد.

در این مرحله، مقادیر فاصله جفری و حدآستانه مقایسه می‌شوند. اگر مقدار فاصله جفری کمتر از حد آستانه باشد، بیانگر وضعیت عادی در بازه زمانی مورد نظر است. در این صورت مقدار متغیر c در متغیر t_0 قرار گرفته و مقدار شمارنده M و L نیز برای بررسی بازه زمانی بعدی صفر می‌گردد. سپس مراحل ذکر شده برای بازه زمانی ۵ ثانیه بعدی ادامه می‌یابد. اگر مقدار فاصله جفری از مقدار حد آستانه بیشتر باشد؛ بیانگر وقوع حمله در شبکه است. در این صورت IP آدرس‌های مبدأ مربوط به جریان بسته ورودی با IP آدرس مقصد مورد نظر، مسدود شده و مقادیر hard - time out و idle - time out برای حذف جریان‌های حمله از جداول سوئیچ‌ها با مقادیر صفر تنظیم می‌شوند. سپس مقدار متغیر c در متغیر t_0 قرار گرفته و مقادیر شمارنده‌های M و L نیز برای ادامه روند بررسی بازه‌های زمانی بعدی صفر می‌گردد.



شکل ۱- فلوچارت راه‌حل پیشنهادی با استفاده از تکنیک فاصله جفری

۵- ارزیابی و مقایسه

ما در این مقاله برای ارزیابی مکانیسم پیشنهادی، شبکه نرم‌افزار محور و حملات منع خدمت توزیع شده را در محیط مینی‌نت[۳۳] شبیه‌سازی کرده‌ایم. شبیه‌ساز مینی‌نت در واقع یک مقلد شبکه است که با استفاده از آن می‌توان یک توپولوژی متشکل از تعدادی میزبان مجازی، لینک مجازی و سوئیچ مجازی شبکه‌های نرم‌افزار محور را اجرا نمود. همچنین

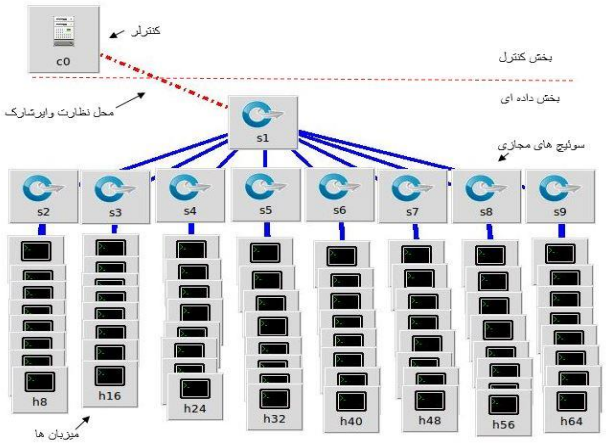
می‌توان سوئیچ‌های این شبکه را به یک کنترلر خارجی متصل کرد. این شبیه‌ساز برنامه‌ای است که می‌تواند شبکه مجازی را ایجاد کرده و هسته‌های واقعی، کدهای برنامه و سوئیچ‌های شبکه را بر روی یک ماشین (ماشین مجازی، ابر یا سیستم واقعی) به اجرا درآورد[۲۶]. ازآنجایی‌که در این شبیه‌سازی، توپولوژی مورد بررسی در مقیاس کوچک تست خواهد شد، ما یک کنترلر کم‌حجم و سبک را نیاز داریم. ما کنترلر POX را برای انجام این پروژه انتخاب نمودیم و این کنترلر را به همراه برخی نرم‌افزارهای مورد نیاز از جمله اسکاپی و وایرشارک به همراه محیط مینی‌نت نصب کرده‌ایم. در اینجا نرم‌افزار اسکاپی برای تولید ترافیک و وایرشارک برای پایش وضعیت ترافیکی مورد استفاده قرار گرفته‌اند.

هدف ما از این شبیه‌سازی ارزیابی مکانیسم ارائه شده است. برای این منظور ابتدا حملات منع خدمت توزیع شده در شبکه نرم‌افزار محور را شبیه‌سازی می‌کنیم. سپس برای آزمودن مکانیسم پیشنهادی، ترافیک‌های عادی و ترافیک‌های حمله با نرخ‌های مختلف را در یک توپولوژی فرضی بررسی کرده و با محاسبه مقادیر فاصله جفری در هر دو وضعیت، الگوریتم پیشنهادی را مورد تجزیه و تحلیل قرار می‌دهیم. درنهایت این مکانیسم را با سایر روش‌های ارائه شده مورد مقایسه قرار خواهیم داد.

۵-۱- شبیه‌سازی حملات DDOS در یک شبکه نرم‌افزار محور

برای راه‌اندازی شبکه نرم‌افزار محور و تولید ترافیک‌های حمله منع خدمت توزیع شده در محیط مینی‌نت، توپولوژی درختی متشکل از ۶۴ میزبان و ۹ سوئیچ را به همراه لینک‌های مجازی ایجاد می‌کنیم. سوئیچ‌های این شبکه به نحوی تنظیم می‌شوند که به یک کنترلر در حال اجرای خارجی با آدرس مشخص متصل باشند. ما در این توپولوژی برای ایجاد سوئیچ‌ها، از سوئیچ مجازی OVS[۱۲] که یک سوئیچ نرم‌افزاری با قابلیت اجرا بر روی سخت افزار و نرم‌افزار است، استفاده می‌کنیم. بعد از ایجاد توپولوژی، کنترلر POX را برای شناسایی آدرس‌های مک در لایه دو و انجام عمل سوئیچینگ، تنظیم و اجرا می‌کنیم. با اجرای کنترلر، سوئیچ‌ها به کنترلر متصل می‌شوند. توپولوژی ایجاد شده را در شکل ۲ می‌بینید. همان‌طور که در این شکل نشان داده شده است، کامپیوترهای میزبان به سوئیچ‌های مجازی بر اساس پروتکل Open Flow متصل شده‌اند و خود این سوئیچ‌ها نیز به یک سوئیچ سطح بالاتر متصل هستند. این مجموعه تشکیل دهنده بخش داده‌ای شبکه است. بخش داده‌ای شبکه از طریق سوئیچ‌ها به کنترلر POX که خارج از شبکه مجازی قرار دارد، متصل می‌شود و دستورات مربوطه را در صورت لزوم از آن دریافت می‌کند.

پس از ایجاد توپولوژی، با استفاده از برنامه اسکاپی دو نوع ترافیک حمله و ترافیک عادی را در شبکه تولید می‌کنیم. برای تعیین این‌که یک بسته اطلاعاتی در اینترنت یا سایر شبکه‌ها به چه برنامه‌ای در میزبان مقصد تعلق بگیرد، از شماره درگاه استفاده می‌شود.



شکل ۲- توپولوژی شبکه نرم‌افزار محور ایجاد شده در محیط مینی نت

در پروتکل‌های ارتباطی TCP این عدد در سرآیند بسته اطلاعاتی ارسالی قرار می‌گیرد و به میزبان مقصد ارسال می‌گردد. شماره درگاهی که برنامه کاربردی به‌وسیله آن، اطلاعات را ارسال می‌کند به‌عنوان شماره درگاه مبدأ و شماره درگاهی که برنامه کاربردی سیستم میزبان به‌وسیله آن اطلاعات را دریافت می‌کند به‌عنوان شماره درگاه مقصد نامیده می‌شوند. با توجه به این‌که در حالت پیش‌فرض Open Flow تنها سرآیند بسته‌ها به کنترلر ارسال می‌گردد، بسته‌های تولیدی در این شبیه‌سازی فاقد محتوی خواهند بود. مشخصات بسته‌های ترافیک تولیدی را در جدول ۱ می‌بینید.

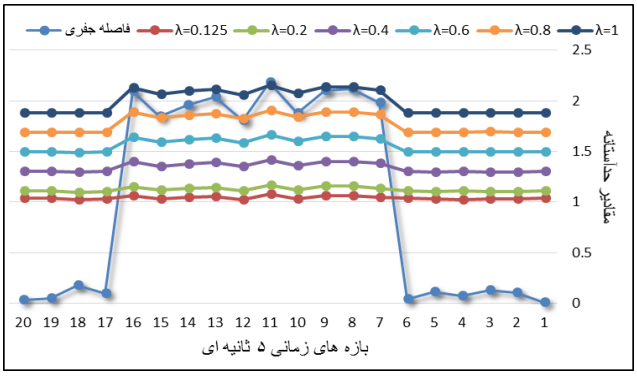
جدول ۱- مشخصات بسته‌های ترافیکی

نام پروتکل	شماره درگاه مبدأ	شماره درگاه مقصد	محتوی
TCP	۶۸	۶۶۳۳	فاقد محتوی

۵-۱-۱- بررسی تأثیر تغییرات پارامترهای حدآستانه تطبیقی

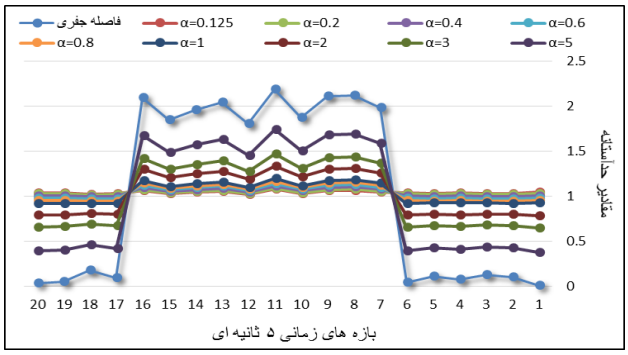
ما در این پژوهش، ابتدا تأثیرات پارامتر های λ، α و β را در مقدار حدآستانه تطبیقی مورد بررسی قرار می‌دهیم. برای این منظور این پارامترها را با اعداد مختلف مقداردهی کرده، سپس مقادیر حدآستانه را در حالات مختلف محاسبه می‌کنیم. شکل‌های ۳، ۴ و ۵ به ترتیب تأثیرات پارامترهای λ، α و β را در مقدار حدآستانه تطبیقی نشان می دهند. در این شکل‌ها محور افقی بیانگر بازه‌های زمانی ۵ ثانیه‌ای مورد بررسی و محور عمودی بیانگر مقادیر حدآستانه نسبت به وضعیت شبکه است. طبق شکل ۳ با افزایش مقدار پارامتر λ ، مقادیر حدآستانه افزایش یافته و حدآستانه به نمودار وضعیت حمله نزدیک‌تر می‌گردد. به‌بیان‌دیگر؛ با افزایش این پارامتر، حاشیه امن حالت حمله (فاصله حدآستانه تا حالت حمله) بسیار کمتر از حاشیه امن حالت نرمال (فاصله حدآستانه تا حالت عادی) خواهد بود. طبق نتایج به‌دست‌آمده، در مواقعی که شبکه در شرایط عادی قرار دارد بایستی حدآستانه با مقادیر $\lambda \geq 1$ محاسبه شود و در مواقعی که وضعیت غیرعادی در شبکه

رخ دهد بایستی مقادیر این پارامتر در محدوده بین ۱ > λ > ۰ لحاظ گردد.

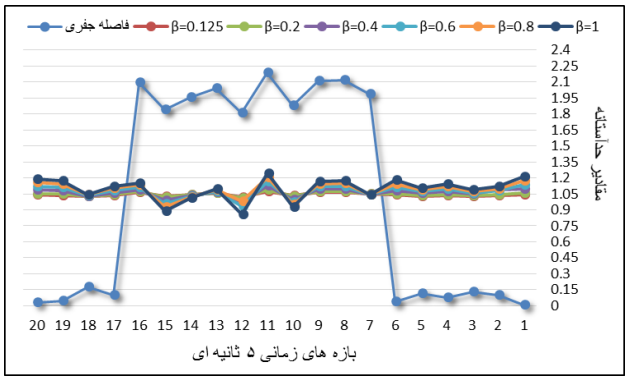


شکل ۳- تأثیرات پارامتر λ در مقدار حدآستانه تطبیقی

شکل ۴ تأثیر تغییرات پارامتر α را در حدآستانه تطبیقی نشان می‌دهد. طبق این شکل، با افزایش مقدار این پارامتر، حدآستانه به نمودار حالت حمله و حالت عادی نزدیک‌تر می‌شود. به‌بیان‌دیگر؛ با افزایش مقدار پارامتر α نسبت مقدار حاشیه امن حالت عادی به حاشیه امن حالت حمله کمتر می‌گردد. ما با استفاده از ویژگی این پارامتر، حدآستانه با حاشیه امن ایده‌آل را در روش پیشنهادی اعمال می‌کنیم. طبق شکل ۵ پارامتر β در میزان انحراف معیار فاصله حدآستانه تأثیرگذار است. میزان تغییرات انحراف معیار حدآستانه برای مقادیر مختلف در این شکل قابل مشاهده است.



شکل ۴- تأثیرات پارامتر α در مقدار حدآستانه تطبیقی



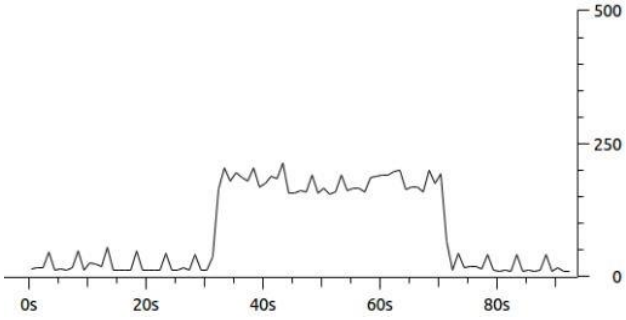
شکل ۵- تأثیرات پارامتر β در مقدار حدآستانه تطبیقی

۵-۲- بررسی روش پیشنهادی در نرخ حملات مختلف

در حملات منع خدمت توزیع شده تولید بسته‌های حمله، سریع‌تر از تولید بسته‌های ترافیک نرمال انجام می‌گیرد. ما برای پیاده‌سازی این ویژگی حملات، فاصله زمانی تولید بسته‌ها را در حالت نرمال به ۰/۱ ثانیه و فاصله زمانی تولید بسته‌های ترافیک حمله را به ترتیب ۰/۰۲۵، ۰/۰۵۰ و ۰/۰۷۵ ثانیه در برنامه اسکاپی تنظیم کردیم. طبق فرمول رابطه ۹ با اعمال این تنظیمات نرخ حملات ایجاد شده ۲۵، ۵۰ و ۷۵ درصد محاسبه می‌شود. در این رابطه T_A و T_N به ترتیب فاصله زمانی ارسال بسته‌ها در شرایط حمله و شرایط عادی است.

$$R = \frac{T_A}{T_N} \times 100 \qquad (۹)$$

ما برای بررسی حملات منع خدمت توزیع شده در شبکه نرم‌افزار محور، حملات را به مدت ۴۰ ثانیه ایجاد کرده و بسته‌های رصد شده توسط وایرشارک را مورد تجزیه و تحلیل قرار خواهیم داد. شکل ۶ گراف حاصل از شبیه‌سازی حمله‌ای با نرخ ۲۵ درصد را نشان می‌دهد که محور افقی بیانگر زمان و محور عمودی بیانگر تعداد بسته‌های رد و بدل شده بین سوئیچ‌ها و کنترلر می‌باشند. همان‌طور که در این شکل قابل مشاهده است، حمله از زمان ۳۰ تا ۷۰ ثانیه صورت گرفته و نرخ بسته‌های ورودی از ۴۰ بسته در ثانیه به ۲۴۵ بسته در ثانیه افزایش یافته است. در بخش بعدی مقادیر حدآستانه و فواصل جفری وضعیت عادی و حمله در حملاتی با نرخ‌های مختلف بررسی می‌گردد.

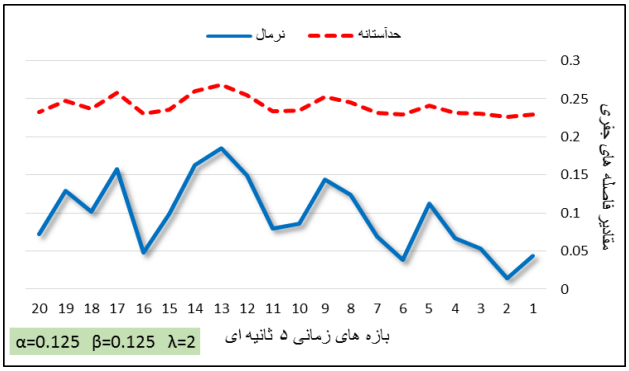


شکل ۶- گراف حاصل از شبیه‌سازی حمله با نرخ۲۵ درصد

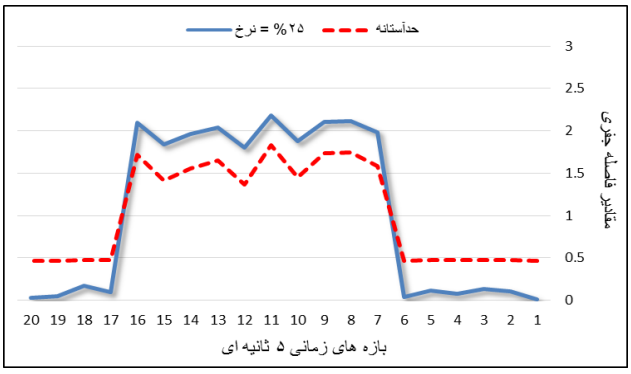
۵-۲-۱- تجزیه و تحلیل روش پیشنهادی

در روش پیشنهادی برای اندازه‌گیری شباهت میان جریان‌های ترافیکی در بازه‌های زمانی آموزشی و تست، توزیع احتمالات را به صورت توزیع نرمال فرض می‌کنیم. دو مجموعه توزیع احتمال شامل توزیع احتمالات دوره زمانی آموزشی و توزیع احتمالات دوره زمانی تست را در بازه‌های زمانی ۵ ثانیه‌ای به دست می‌آوریم. طبق فرمول رابطه ۳ و ۷ فاصله جفری و حدآستانه تطبیقی بین اعضای متناظر دو مجموعه محاسبه می‌گردد. ما در این پژوهش طبق بررسی‌های انجام شده در بخش قبلی، مقادیر پارامترهای λ، α و β را در شرایط غیرعادی شبکه به ترتیب با ۰/۱۲۵، ۵ و ۰/۶ مقداردهی می‌کنیم. شکل۷ تغییرات مقادیر فاصله جفری در وضعیت عادی شبکه را نشان می‌دهد. در این شکل محور افقی بیانگر بازه‌های زمانی مورد بررسی و محور عمودی بیانگر مقادیر

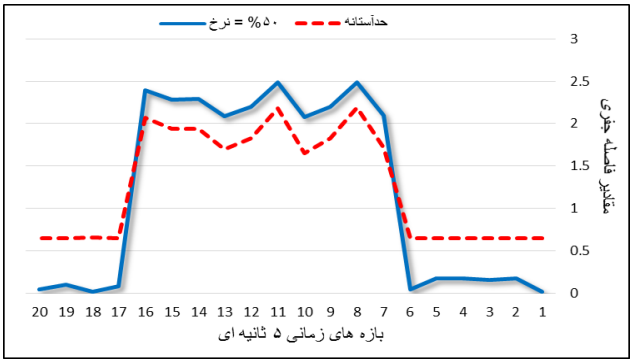
فاصله‌های جفری محاسبه شده است. هنگامی که شبکه در وضعیت عادی قرار دارد، میزان تغییرات فاصله جفری بسیار ناچیز و در حدود ۰/۱۷۱۵ است. در وضعیت عادی مقدار فاصله جفری کمتر از مقدار حدآستانه مربوط به بازه زمانی مورد نظر است. مطابق شکل‌های۸، ۹ و ۱۰ در بازه های زمانی ۳۰ تا ۷۰ ثانیه به دلیل وقوع حمله، توزیع احتمالات دچار نوسان شده و مقادیر فاصله جفری متناسب با میزان نرخ بسته‌های حمله دچار تغییر می‌شوند. میزان تغییرات مقادیر فاصله جفری در وضعیت حمله با نرخ‌های ۲۵، ۵۰ و ۷۵ درصد به ترتیب حدود ۲/۱۷۶۵، ۲/۴۷۲۳ و ۲/۸۱۹۲ است. این میزان تغییرات، در مقایسه با وضعیت نرمال افزایش چشم‌گیری را نشان می‌دهد. همان‌طور که در این شکل‌ها قابل مشاهده است در زمان وقوع حمله، مقادیر فاصله جفری از حدآستانه مربوطه فراتر می‌رود.



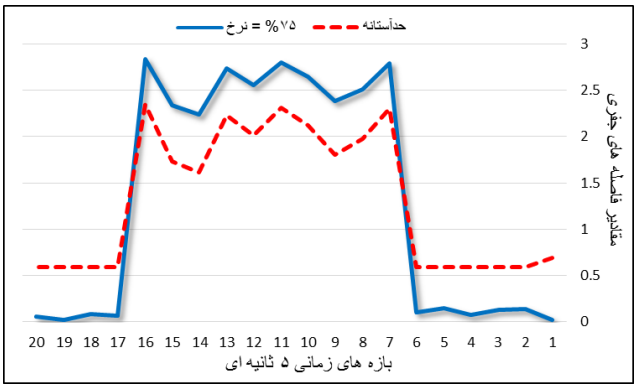
شکل ۷- میزان تغییرات فاصله جفری در وضعیت عادی شبکه



شکل ۸- میزان تغییرات فاصله جفری در وضعیت حمله با نرخ۲۵٪



شکل ۹- میزان تغییرات فاصله جفری در وضعیت حمله با نرخ ۵۰٪



شکل ۱۰- میزان تغییرات فاصله جفری در وضعیت حمله با نرخ ۷۵٪

نتایج حاصل از بررسی مقادیر فاصله جفری در وضعیت نرمال و وضعیت حملاتی با نرخ‌های مختلف در جدول ۲ نشان داده شده است. در این جدول همچنین میزان تغییرات حدآستانه نیز با توجه به متغیر بودن آن آمده است. طبق نتایج به‌دست‌آمده، اختلاف بین مقادیر کمترین فاصله جفری در ترافیک حملاتی با نرخ‌های ۲۵، ۵۰ و ۷۵ درصد و بیشترین فاصله جفری در ترافیک وضعیت نرمال به ترتیب ۱/۶۲۹۵، ۱/۹۰۳ و ۲/۰۸۸۵ محاسبه می‌شود. این مقادیر افزایش ۹۰/۲۷٪ ، ۹۱/۶۸٪ و ۹۳/۴۰۳٪ فاصله‌های جفری در ترافیک حمله را نشان می‌دهد. در نتیجه فاصله جفری وجود حمله را بسیار برجسته‌تر می‌کند.

طبق جدول ۲، اختلاف بین بیشترین مقدار حدآستانه و کمترین مقدار فاصله جفری در حالت حمله با نرخ‌های ۲۵، ۵۰ و ۷۵ درصد به ترتیب برابر ۰/۰۶۴۴، ۰/۱۱۴۴۳ و۰/۱۱۲۹ است که این مقادیر را حاشیه‌های امن حالت حمله می‌نامیم. میزان اختلاف بین کمترین مقدار حدآستانه و بیشترین فاصله جفری در وضعیت نرمال نیز به ترتیب برابر با ۰/۲۹۳۶، ۰/۴۷۲۱ و۰/۴۳۹۴ است که این مقادیر را حاشیه‌های امن حالت نرمال می‌نامیم. به‌بیان‌دیگر؛ در این حملات حاشیه امن حالت نرمال به ترتیب ۴/۵۵، ۴/۱۲۵ و۳/۸۹۱ برابر حاشیه امن حالت حمله مربوطه است. طبق نتایج به‌دست‌آمده، این مکانیسم پیشنهادی به دلیل دارا بودن حاشیه امن متناسب، قادر است حملات منع خدمت توزیع شده با هر نرخی را به‌درستی تشخیص داده و اقدامات مقابله‌ای را در شبکه‌های نرم‌افزار محور اعمال نماید.

جدول ۲- نتایج محاسبات انجام شده برای محاسبه فاصله جفری

معیار	وضعیت عادی (متوسط)	حمله با نرخ ۲۵٪	حمله با نرخ ۵۰٪	حمله با نرخ ۷۵٪
بیشترین مقدار فاصله جفری	۰/۱۷۰	۲/۱۸۵	۲/۴۹	۲/۸۳۵
کمترین مقدار فاصله جفری	۰/۰۱۳	۱/۸۰۵	۲/۰۷۵	۲/۲۳۶
بیشترین مقدار حدآستانه	۰/۵۲۰	۱/۸۶۹	۲/۱۹۰	۲/۳۴۸
کمترین مقدار حدآستانه	۰/۴۸۱	۰/۴۶۹	۰/۶۴۴	۰/۵۸۶

۵ -۳- مقایسه روش پیشنهادی با روش‌های قبلی

در این بخش به مقایسه الگوریتم پیشنهادی با سایر مکانیسم‌های ارائه شده می‌پردازیم. روش ارائه شده در مقاله [۱۴] به دلیل اینکه پیش‌بینی رفتار ترافیک شبکه براساس پیش‌پردازش ترافیک‌های نمونه‌برداری شده در زمان‌های خاصی انجام می‌گیرد، یک وضعیت استثنایی (خرابی لینک و...) در زمان نمونه‌برداری ممکن است منجر به پیش‌بینی نادرست ترافیکی گردد. این روش مراحل بسیار زیادی داشته و مرحله آموزش شبکه عصبی بسیار زمان‌بر است. در صورت تغییر رفتار شبکه نیاز به آموزش مجدد شبکه عصبی خواهد بود. ولی روش پیشنهادی ما قادر است تغییرات ترافیکی را براساس روابط آماری ساده با محاسبات کم تشخیص دهد. بر طبق بررسی‌های انجام شده، الگوریتم پیشنهادی ما برخلاف مکانیسم ارائه شده در مقاله[۱۷] نیاز به تغییرات ساختار سخت‌افزاری سوئیچ‌ها ندارد و با ایجاد تغییرات نرم‌افزاری جزئی در کنترلر قابل پیاده‌سازی است.

روش پیشنهادی مقاله[۱۸] برای یادگیری رفتار شبکه به ساعت‌ها آموزش نیاز دارد و بایستی ماتریس محاسباتی در کل دوره، محافظت شود. یکی دیگر از مشکلات این روش این است که این راه‌حل در کنار کنترلر برای تشخیص حملات استفاده می شد و از امکانات کنترلر بی بهره بود. در مقاله[۱۹] معماری شبکه نرم‌افزار محور همانند معماری شبکه‌های سنتی در نظر گرفته شده و از امکانات منحصربه‌فرد این معماری بی‌بهره بودند. راه‌حل ارائه شده در مقاله [۲۰] نیاز به نصب سیستم‌های تشخیص نفوذ چندگانه داشت تا بتوانند در کنار کنترلر اقدامات مقابله‌ای را انجام دهند. در این روش استقرار سیستم‌های چندگانه، منابع زیادی از کنترلر را اشغال می‌کنند. همچنین در این راه‌حل لزوم تداوم ارتباط بین سیستم‌ها می‌تواند به‌عنوان آسیب‌پذیری این مکانیسم در حملات مورد سوءاستفاده قرار گیرد. درصورتی‌که الگوریتم پیشنهادی ما با بهره‌گیری از امکانات کنترلر و در درون کنترلر انجام می‌گیرد و نیازی به نصب تجهیزات در بخش‌های مختلف شبکه ندارد.

راه‌حل ارائه شده در مقاله [۲۱] حافظه زیادی برای نگهداری اطلاعات موجود در چندین کنترلر نیاز دارد، زیرا هر کنترلر بایستی تمام اطلاعات مربوط به نقشه مسیرها را به‌صورت به‌روزرسانی شده در اختیار داشته باشد. در این روش تبادل مداوم اطلاعات بین کنترلرها با اشغال منابع کنترلرها و پهنای باند شبکه موجب افزایش تأخیر در ارسال بسته‌ها می‌گردد. در این روش مهاجم با ارسال حجم انبوهی از ترافیک‌های جعلی در درازمدت می‌تواند موجب اشباع منابع همه کنترلرهای در نظرگرفته شده شود. همچنین کانال‌های ارتباطی بین کنترلرها ممکن است به‌عنوان هدفی برای مهاجمان تبدیل شوند. درصورتی‌که روش پیشنهادی ما، بعد از تشخیص حمله با حذف بسته‌های مشکوک مانع اشباع کنترلر می‌شود و همچنین به منابع زیادی نیاز ندارد و تداخلی در روند ارسال بسته‌ها ایجاد نمی‌کند.

روش‌های پیشنهادی مقالات [۱۵، ۲۲] پیچیدگی محاسباتی بالایی دارند، بنابراین منابع زیادی از کنترلر را اشغال می‌کنند. همچنین این روش‌ها به دلیل ثابت بودن حدآستانه، توانایی تشخیص حمله‌ای با نرخ های مختلف را ندارد و در تشخیص حملاتی که ترافیک حمله به صورت یکنواخت بین میزبان‌ها توزیع شود، با مشکل مواجه خواهند بود. همچنین این روش‌ها فاقد مکانیسم کاهش اثر حمله است. ولی روش پیشنهادی ما، دارای حدآستانه تطبیقی است و این روش قادر است حتی این گونه حملات را نیز شناسایی کرده و اقدامات لازم جهت کاهش اثر حملات را در شبکه نرم‌افزار محور اعمال نماید.

ما در ادامه به ارزیابی دقیق تکنیک فاصله جفری مورد استفاده در روش پیشنهادی با سایر روش‌های آماری از جمله آنتروپی و فاصله سیبسون می‌پردازیم. برای این منظور روش ارائه شده در مقاله [۲۲] را بر روی داده‌های حاصل از شبیه سازی انجام شده، اعمال کرده و نتایج حاصل را مورد تجزیه و تحلیل قرار می‌دهیم. در مقاله [۲۲] برای تشخیص حمله، روش آماری آنتروپی پیشنهاد شده است. در این روش تعداد معینی از بسته ورودی به‌عنوان یک پنجره در نظر گرفته می‌شود. سپس تعداد بسته‌هایی با IP آدرس مقصد یکسان در هر پنجره مورد بررسی قرار می‌گیرد. در مقاله [۳۴] اندازه‌های مختلف پنجره، برای بهبود اندازه‌گیری آنتروپی تست شده است. جدول ۳ نتایج تست برای پنجره‌هایی با اندازه‌های مختلف را نشان می‌دهد. در این مقاله اظهار شده هنگامی‌که تست اعتبار بالاتر از ۱/۶۴ باشد فرضیه معتبر خواهد بود. تست اعتبار در واقع یک اعتبار سنجی برای فرضیه مورد نظر بین دو میانگین جامعه آماری (حالت حمله و حالت نرمال) است. این مقاله طبق نتایج به‌دست‌آمده پنجره‌های ۵۰ و ۱۰۰ را بهترین اندازه پنجره معرفی می‌کند.

جدول ۳- محاسبات آنتروپی در پنجره‌هایی با اندازه‌های مختلف[۳۴]

اندازه پنجره	آنتروپی نرمال	آنتروپی حمله	آزمون اعتبار
۵	۱/۳۶	۱/۹۸	۱/۲۹
۱۰	۱/۸۹	۲/۷۲	۱/۴۹
۵۰	۳/۱۱	۴/۲۲	۱/۷۰
۱۰۰	۳/۵۹	۴/۷۳	۱/۸۰
۵۰۰	۴/۵۴	۵/۵۱	۲/۴۰
۱۰۰۰	۴/۸۸	۵/۶۷	۲/۴۸
۵۰۰۰	۵/۵۰	۵/۹۲	۳/۲۵

مطابق جدول ۳، با توجه به این‌که آنتروپی مبتنی بر IP آدرس مبدأ محاسبه شده است، میزان آنتروپی حمله بالاتر از آنتروپی شرایط نرمال است، زیرا بسته‌های حمله IP آدرس مبدأ متفاوت و اغلب جعلی دارند. ولی در شرایط نرمال یک اتصال بین مبدأ و مقصد ایجاد می گردد، بنابراین عمدتاً IP آدرس مبدأ یکسانی خواهند داشت. در نتیجه

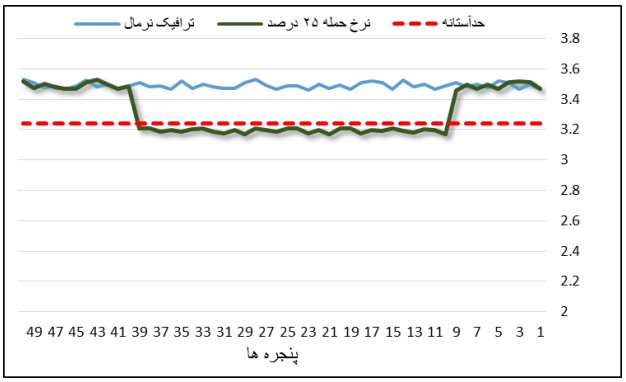
مقادیر آنتروپی محاسبه شده مبتنی بر IP آدرس مبدأ در شرایط حمله بالاتر از آنتروپی حالت نرمال خواهد بود.

در شبکه‌های نرم‌افزار محور تعداد سوئیچ‌ها و میزبان‌های متصل به کنترلر مشخص است. بسته‌ها از طریق گرفتن قوانین از کنترلر، یک جریانی را ایجاد می‌کنند. در این شبکه‌ها دارا بودن IP آدرس مبدأ متفاوت یک واقعیت شناخته شده است که هیچ کمکی برای تشخیص حملات منع خدمت توزیع شده نمی‌کند. در این شبکه‌ها با مشخص کردن اندازه پنجره، حداکثر آنتروپی IP آدرس مقصد مشخص می‌گردد، بنابراین در این پژوهش مقدار آنتروپی براساس IP آدرس مقصد محاسبه خواهد شد. در این روش، آنتروپی حالت حمله به دلیل تکرار IP آدرس مقصد حمله برخلاف مقاله [۳۴] کمتر از آنتروپی حالت نرمال می‌شود. ما در این پژوهش با توجه به تعداد ۶۴ میزبان موجود در توپولوژی مورد آزمایش، اندازه پنجره را ۵۰ در نظر گرفته و در ۵۰ پنجره متوالی مقادیر آنتروپی را برای حملاتی با نرخ ۲۵، ۵۰ و ۷۵ درصد بررسی کردیم. نتایج حاصل از بررسی مقادیر آنتروپی در شرایط حمله و شرایط عادی را در جدول ۴ می‌بینید.

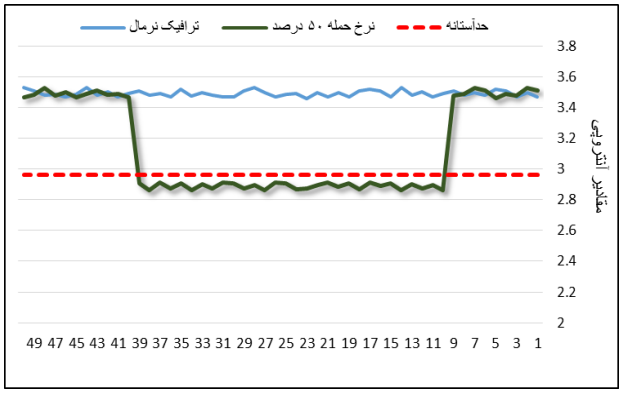
جدول ۴- نتایج حاصل از بررسی روش آنتروپی

	بیشترین مقدار آنتروپی	کمترین مقدار آنتروپی	حاشیه امن حمله/نرخ حملات
وضعیت نرمال	۳/۵۳	۳/۴۶	۰/۲۱ ۰/۵۴ ۰/۹۷
حمله با نرخ ٪۲۵	۳/۲۱	۳/۱۶	۰/۰۱
حمله با نرخ ٪۵۰	۲/۹۱	۲/۸۶	۰/۰۰۷
حمله با نرخ ٪۷۵	۲/۴۴	۲/۳۵	۰/۰۵

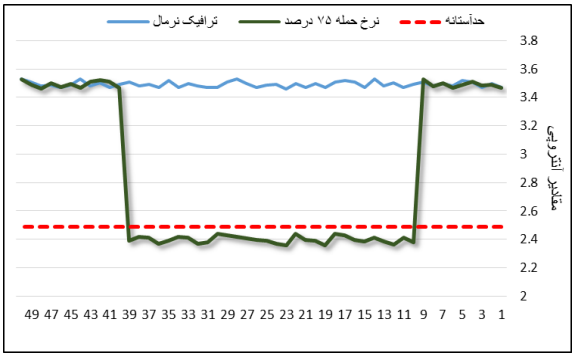
میزان تغییرات مقادیر آنتروپی در شرایط حمله با نرخ‌های ۲۵، ۵۰ و ۷۵ درصد در شکل‌های ۱۱، ۱۲ و ۱۳ نشان داده شده است. در این شکل‌ها محور افقی بیانگر پنجره‌های مورد بررسی و محور عمودی بیانگر مقادیر آنتروپی است. در شرایط عادی شبکه، میزان تغییرات آنتروپی بسیار ناچیز و در حدود ۰/۰۶۹ است. هنگامی که در شبکه حمله اتفاق میافتد، به دلیل افزایش تعداد بسته‌هایی با IP آدرس مقصد یکسان، مقادیر آنتروپی کاهش می‌یابد.



شکل ۱۱- میزان تغییرات آنتروپی در حمله با نرخ ٪۲۵

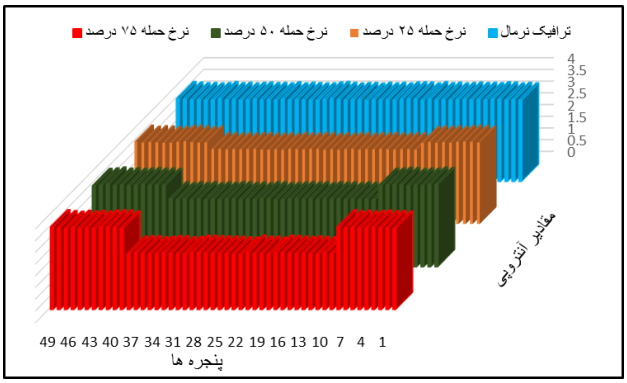


شکل ۱۲- میزان تغییرات آنتروپی در حمله با نرخ ٪۵۰

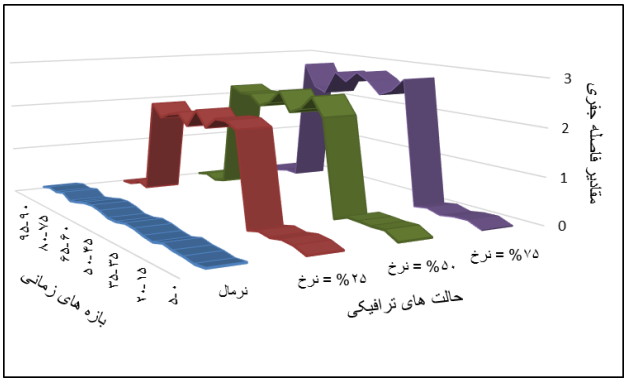


شکل ۱۳- میزان تغییرات آنتروپی در حمله با نرخ ٪۷۵

طبق نتایج به‌دست‌آمده، میزان افت مقادیر آنتروپی در حالات مختلف حمله، بسیار کمتر از میزان رشد مقادیر فاصله جفری در موارد مشابه است. شکل‌های ۱۴ و ۱۵ میزان افت آنتروپی و رشد فوا صل جفری را در نرخ حملات ۲۵، ۵۰ و ۷۵ درصد به‌خوبی نشان می‌دهند.



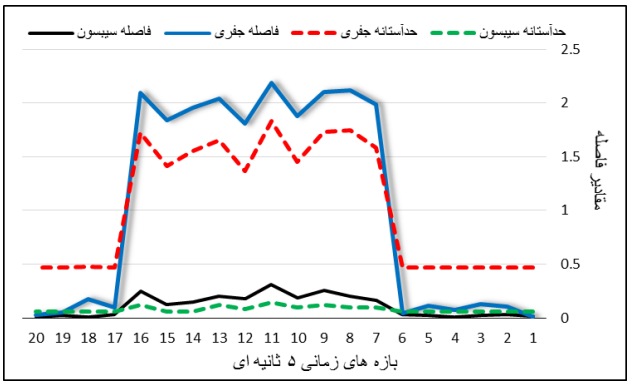
شکل ۱۴- میزان افت آنتروپی در نرخ‌های مختلف حملات



شکل ۱۵- میزان رشد مقادیر جفری در نرخ‌های مختلف حمله

طبق مشاهدات انجام شده اختلاف بین مقادیر آنتروپی بیشترین حالت حمله و کمترین حالت نرمال در حملات با نرخ‌های ۲۵، ۵۰ و ۷۵ درصد به ترتیب حدود ۰/۲۵، ۰/۵۵ و ۱/۰۲ است. در روش پیشنهادی ما اختلاف بین مقادیر بیشترین فاصله جفری در حالت نرمال و کمترین فاصله جفری در این حالت حمله به ترتیب برابر ۱/۶۲۹، ۱/۹۰۳ و ۲/۰۸۸ بود که این مقادیر ۶/۵۱، ۳/۴۶و ۲/۰۴۷ برابر مقادیر مشابه در روش آنتروپی است. بنابراین در روش جفری افزایش فاصله محدوده بین مقادیر وضعیت نرمال و حمله موجب افزایش دقت تشخیص حملات خواهد بود. در ادامه تکنیک فاصله جفری مورد استفاده در روش پیشنهادی را با روش آماری فاصله سیبسون مورد ارزیابی قرار می‌دهیم. شکل ۱۶ تغییرات مقادیر فاصله سیبسون و فاصله جفری در وضعیت حمله را نشان می‌دهد.

نتایج بررسی روش‌های آماری در جدول ۵ آمده است. طبق نتایج جدول ۵، در تکنیک فاصله جفری مورد استفاده در روش پیشنهادی، محدوده بین مقادیر در حالت نرمال و حالت حمله نسبت به سایر روش‌های آماری افزایش یافته است، بنابراین در این روش نرخ تشخیص غلط به دلیل نزدیکی محدوده مقادیر دو وضعیت کاهش می‌یابد. همچنین در روش آنتروپی حاشیه امن حالت حمله بسیار کمتر از حاشیه امن حالت نرمال است، بنابراین ممکن است برخی حملات با تغییرات آنتروپی جزئی قابل تشخیص نباشند. در نتیجه در روش آنتروپی احتمال خطای تشخیصی افزایش می‌یابد. ولی در روش فاصله جفری، هر دو وضعیت عادی و حمله، حاشیه امن مناسبی برخوردارند. بنابراین تکنیک فاصله جفری نسبت به دو روش آماری دیگر کارآیی بهتری در تشخیص حملات خواهد داشت.



شکل ۱۶- میزان تغییرات فاصله سیبسون و فاصله جفری

جدول ۵- مقایسه کارآیی روش‌های آماری

تکنیک‌های آماری	محدوده حالت نرمال و حمله	حاشیه امن نرمال	حاشیه امن حمله	نسبت حاشیه امن
آنتروپی	۰/۲۵	۰/۲۱	۰/۰۱	۲۱
فاصله سیبسون	۰/۰۹۲	۰/۰۹۸	۰/۰۲	۴/۹
فاصله جفری	۱/۶۲۹	۰/۲۹۳	۰/۰۶۴	۴/۵

۶- نتیجه‌گیری

پژوهش حاضر به‌منظور تشخیص و کاهش اثر حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور انجام گرفت. در این معماری به دلیل قابلیت کنترل متمرکز از طریق جداسازی بخش داده‌ای و بخش کنترل، مدیریت شبکه بسیار آسان‌تر شده است. کنترلر شبکه‌های نرم‌افزار محور به‌عنوان مغز این معماری است. کنترلر با داشتن نمای وسیعی از کل شبکه، امکانات مناسبی برای جمع‌آوری داده‌های آماری فراهم می‌کند. معماری شبکه‌های نرم‌افزار محور، به دلیل توانایی‌های کنترلر بستر ایده‌آلی را برای تشخیص و مقابله با حملات منع خدمت فراهم می‌نماید.

ما در این مقاله با بهره‌گیری از فرصت‌های ایجاد شده توسط کنترلر، راه‌حل مؤثر مبتنی بر روش آماری را برای تشخیص و کاهش اثر حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور ارائه دادیم. طبق دانش ما، این تکنیک در شبکه‌های نرم‌افزار محور استفاده نشده و این اولین راه‌حل در نوع خود در شبکه‌های نرم‌افزار محور است. با اعمال این تکنیک به‌عنوان روش تشخیصی، قادر به تشخیص حملات با نرخ‌های مختلف خواهیم بود. در این مکانیسم پیشنهادی، پس از تشخیص حملات با بهره‌گیری از امکانات کنترلر اقدامات مقابله‌ای اعمال می‌گردد.

مکانیسم پیشنهادی ما، برای جمع‌آوری آمار و محاسبات مورد نیاز، حافظه و منابع زیادی را مورد استفاده قرار نمی‌دهد و با اعمال تغییرات جزئی در کنترلر قابل پیاده‌سازی است. به‌عبارت‌دیگر؛ با این روش، کنترلر بدون نیاز به نصب تجهیزات، با وارد کردن دستورات و تغییرات جزئی توانایی تشخیص و کاهش اثر حملات را پیدا می‌کند.

در کارهای آتی می‌توان روش پیشنهادی ارائه شده در این مقاله را بهبود داده و در شبکه‌هایی با بیش از دو کنترلر مورد بررسی قرار داد. از آنجایی‌که روش پیشنهادی در مقاله ما، راه‌حل تشخیص و کاهش اثر بعد از وقوع حمله است، بنابراین می‌توان در بررسی‌های آینده بر روی چگونگی پیشگیری حملات منع خدمت توزیع شده در شبکه‌های نرم‌افزار محور متمرکز شد.

منابع

[1] S.Shin , G.Gu, "Attacking software-defined networks: A first feasibility study." Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, Hong Kong, China, August, 2013.

[2] S.Sezer, S.Scott-Hayward, P.K.Chouhan, B.Lake and D.Finnegan,"Are we ready for SDN? Implementation challenges for software-defined networks." IEEE Communications Magazine,vol.51,no.7, pp.36-43, Aug, 2013.

[3] N.McKeown, T.Anderson, H.Balakrishnan, G.Parulkar, L.Peterson, J.Rexford and J.Turner, "OpenFlow: enabling innovation in campus networks." ACM SIGCOMM Computer Communication Review,vol. 38,no.2, pp.69-74,Feb, 2008.

[4] P.Porras, S.Shin, V.Yegneswaran, M.Fong, M.Tyson, and G.Gu, "A security enforcement kernel for OpenFlow networks." In Proceedings of the first workshop on Hot topics in software defined networks ,pp. 121-126, ACM, Helsinki, Finland, August,2012.

[5] J.Mirkovic, P.Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review, vol.34,no.2,pp. 39-53, 2004.

[6] Y.Nayana, M.JustinGopinath and L.Girish, "DDoS Mitigation using Software Defined Network." International Journal of Engineering Trends and Technology (IJETT) , vol. 24 ,no. 5, June,2015.

[7] M.Karami, D.McCoy, "Understanding the emerging threat of ddos-as-a-service." In Presented as part of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats, Washington, D.C, 2013.

[8] N.N.Dao, J.Park, M.Park and S.Cho, "A feasible method to combat against DDoS attack in SDN network." In International Conference on Information Networking (ICOIN), pp. 309-311, IEEE, Cambodia, January, 2015.

[9] L.Hongbin, Y.Lin, H.Zhang and M. Zukerman, "Preventing DDoS attacks by identifier/locator separation." In IEEE network, vol.27, no.6, pp.60-65, Nov, 2013.

[10] T.Peng, C.Leckie, K.Ramamohanarao, "Proactively detecting distributed denial of service attacks using source IP address monitoring." In International Conference on Research in Networking ,Springer Berlin Heidelberg, pp. 771-782, May, 2014.

[11] T.Andrysiak, L. Saganowski, "DDoS Attacks Detection by Means of Statistical Models." In Proceedings of the 9th International Conference on Computer Recognition Systems CORES, Springer International Publishing, PP. 797-806, Nov, 2015.

[12] T. Thapngam, S. Yu, W. Zhou and S.K. Makki ," Distributed Denial of Service (DDoS) detection by traffic pattern analysis." In Peer-to-peer networking and applications, vol.7, no.4, Dec, 2014.

[13] Z.Tan, A. Jamdagni, P. Nanda and R.P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis." In IEEE transactions on parallel and distributed systems, vol. 25, no.2, pp.447-456, Feb, 2014.

[14] Y.Chen, X. Ma and X. Wu, "DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory." IEEE Communications Letters, vol.17, no.5, pp.1052-1054, May,2013.

[15] M.Xinlei, C. Yonghong, "DDoS detection method based on chaos analysis of network traffic entropy." IEEE Communications Letters, vol.18, no.1, pp.114-117, Jan,2014.

[16] H.Sengar, H.Wang, D.Wijesekera and S.Jajodia, "Detecting VoIP floods using the Hellinger distance." IEEE transactions on parallel and distributed systems, vol.19, no.6, pp.794-805,2008.

[17] R.Kandoi, M. Antikainen, "Denial-of-service attacks in OpenFlow SDN networks." In IFIP/IEEE International Symposium on Integrated Network Management (IM) , pp. 1322-1326, May, 2015.

[18] M.Ramadas, S.Ostermann and B.Tjaden, "Detecting anomalous network traffic with self-organizing maps." In International Workshop on Recent Advances in Intrusion Detection, , pp. 36-54, Springer Berlin Heidelberg, September ,2003.

[19] M.Suh, S.H.Park, B.Lee and S.Yang, "Building firewall over the software-defined network controller." In 16th International Conference on Advanced Communication Technology, pp. 744-748, IEEE, Ireland, Feb, 2014.

[20] H. Taejin, Y. Seunghyun, A.C. Risdianto,J.W. Kim and H. Lim, "Suspicious Flow Forwarding for Multiple Intrusion Detection Systems on Software-Defined Networks." In IEEE Network, vol.30, no.6, pp. 22-27, Nov, 2016.

[21] M.Duohe,X. Zhen and L. Dongdai "Defending blind DDoS attack on SDN based on moving target defense." In International Conference on Security and Privacy in Communication Systems, Springer International Publishing, pp. 463-480, Beijing, China, Sep, 2014.

[22] S.M.Mousavi, M.St-Hilaire, "Early detection of DDoS attacks against SDN controllers." In Computing, Networking and Communications (ICNC), pp. 77-81, International Conference on IEEE, California, USA, February,2015.

[23] S.Scott-Hayward, G.O'Callaghan and S.Sezer, "Sdn security: A survey." In Future Networks and Services (SDN4FNS), 2013 IEEE SDN , pp. 1-7, November,2013.

[24] M.Casado, M.Freedman, J.Pettit, J.Luo, N.McKeown and S.Shenker, "Ethane: taking control of the enterprise." In ACM SIGCOMM Computer Communication Review, Vol. 37, No. 4, pp. 1-12, ACM, August,2007.

[25] C.Buragohain, N.Medhi, "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers." In Signal Processing and Integrated Networks (SPIN), 2016 3rd International Conference, pp. 519-524, IEEE, NOIDA, India, February, 2016.

[26] S.Oshima, T.Nakashima and T.Sueyoshi, "Early DoS/DDoS detection method using short-term statistics." In Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference on IEEE, pp. 168-173, Krakow, Poland, February, 2010.

[27] محمد مؤمنی، مهدی آقا صرام، وحید شاکر، شهرام جمالی و مهدی نوشیار، «ارائه یک فیلتر جدید برای حذف نویزهای ضربه‌ای و ترکیب فیلتر پیشنهادی با الگوریتم PSO به‌منظور کشف و دفاع در برابر حملات

سیل آسای SYN» مجله مهندسی برق دانشگاه تبریز، جلد ۴۶، شماره ۱، صفحات ۳۱۱-۳۱۹، ۱۳۹۵ .

[28] I.Alsmadi, D.Xu, "Security of software defined networks: A survey." computers & security, vol.53,pp. 79-108,Feb, 2015.

[29] یاسر عظیمی، وحید هاشمی فرد و جمشید باقرزاده، «تشخیص توزیع شده و مشارکتی حمله کرم چاله در شبکه‌های حسگر بی سیم،» مجله مهندسی برق دانشگاه تبریز، جلد ۴۶، شماره ۴، صفحات ۲۰۶-۱۹۵، ۱۳۹۵.

[30] L.Le Cam, G.L.Yang, *Asymptotics in statistics: some basic concepts. Springer Science & Business Media*. 2012.

[31] G.McLachlan, *Discriminant analysis and statistical pattern recognition*. John Wiley & Sons, Vol. 544, Aug, 2004.

[32] J.F.Kurose, K.W.Ross, *Computer networking: a top-down approach*. Addison Wesley, 2007.

[33] B.Lantz, B.Heller and N.McKeown, "A network in a laptop: rapid prototyping for software-defined networks." In Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks ACM, p. 19, Monterey, CA, USA, October, 2010.

[34] S. Oshima, T. Nakashima and T. Sueyoshi "Early DoS/DDoS detection method using short-term statistics." In Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference on, pp. 168-173. IEEE, Krakow, Poland, Feb,2010.

زیرنویس‌ها

1- Software - defined Networks
2- Distributed denial of service attack
3- Identifier/Locator Separation
4- Chaos Theory
5- Self Organization Map
6- Multiple Intrusion Detection Systems
7- Moving Target System
8- Control plane
9- Data plane
10- Open Networking Foundation
11- Exponential Weighted Moving Average
12- Open virtual switch