مقاله پژوهشی

ارائه یک روش جهت تشخیص و تقلیل حملات انکار سرویس در اینترنت اشیا از طریق شبکه‌های نرم‌افزارمحور

فاطمه مطیع شیرازی و سید اکبر مصطفوی

چکیده: اینترنت اشیا (IoT) شبکه‌ای از اشیاست که بر بستر آن اشیا می‌توانند با سایر اشیا ارتباط برقرار کنند. اینترنت در حال حاضر به‌طور مداوم به علت مشکلات فنی، قانونی و انسانی تحت حملات متعددی قرار می‌گیرد. یکی از مهم‌ترین این حملات، حمله منع سرویس (DoS) است که در آن سرویس‌های عادی شبکه از دسترس خارج می‌شوند و دسترسی اشیا و کاربران به سرور و سایر منابع ناممکن می‌شود. راهکارهای امنیتی موجود نتوانسته که به‌طور مؤثر از حملات وقفه در خدمات اینترنت اشیا جلوگیری کند. شبکه نرم‌افزارمحور (SDN) یک معماری جدید در شبکه است که اساس کار آن، جداسازی بخش کنترلی و داده‌ای شبکه از یکدیگر می‌باشد. قابلیت برنامه‌ریزی و مدیریت شبکه توسط SDN را می‌توان در خدمات IoT به کار برد، زیرا دستگاه‌هایی وجود دارند که تنها به‌صورت دوره‌ای و در زمان‌های مشخص اقدام به ارسال داده‌ها می‌کنند. SDN در صورت استقرار مناسب در مرکز داده می‌تواند به تقلیل یا جلوگیری از سیل داده‌های ناشی از IoT کمک کند. در این مقاله، راهکاری برای تشخیص حملات DDoS در اینترنت اشیا بر پایه SDN و سپس الگوریتمی جهت کاهش حمله DDoS ارائه می‌شود. روش پیشنهادی بر اساس معیار آنتروپی است که یکی از مفاهیم بسیار مهم در تئوری اطلاعات و میزان شروع جریان و مطالعه مشخصات جریان می‌باشد. در این روش با استفاده از دو مؤلفه جدید روی کنترل‌کننده برای دریافت بسته‌های ورودی و درنظرگرفتن پنجره زمانی و محاسبه آنتروپی و نرخ جریان، حمله احتمالی در شبکه تشخیص داده شده و در صورت نیاز، آمارهای جریان از سوئیچ‌ها دریافت می‌گردد و سپس حمله به‌صورت قطعی در شبکه تشخیص داده می‌شود. روش پیشنهادی در مقایسه با روش‌های موجود، ۱۲ درصد از نظر زمان تشخیص حمله و ۲۶ درصد از نظر مثبت/ منفی کاذب بهبود داشته است.

کلیدواژه: **شبکه‌های نرم‌افزارمحور، اینترنت اشیا، حمله انکار سرویس توزیع‌شده، آنتروپی.**

۱- مقدمه

اینترنت اشیا (IoT)[1] سیستمی از دستگاه‌های محاسباتی، ماشین‌های مکانیکی و دیجیتال، اشیا، حیوانات یا افراد است که با شناساگرهای یکتایی مشخص شده‌اند و توانایی انتقال داده در شبکه را بدون نیاز به تعاملات انسان با انسان یا انسان با کامپیوتر دارند. همچنین این فناوری به‌ویژه هنگامی که صحبت از استانداردهای مختلف، امنیت و سازگاری با سایر سامانه‌ها می‌شود، می‌تواند مفاهیم جدید و ویژه‌ای پیدا کند. معماری اینترنت اشیا با چندین میلیون و شاید میلیاردها شیء سر و کار دارد؛ به‌طوری که این اشیا با یکدیگر در تعامل هستند. همه این تعاملات باید به نحوی محافظت شود؛ از جمله حفاظت از اطلاعات و تأمین خدمات و نیز محدودکردن تعداد رخدادهای امنیتی که بر کل این فناوری تأثیر می‌گذارد. تهدیدات مختلفی مانند تهدیدات فیزیکی، محرومیت از خدمات، ساخت هویت جعلی و غیره در اینترنت اشیا وجود دارد. با توجه به اینکه منابع اشیا در این تکنولوژی اغلب محدود است، لذا این شبکه‌ها نسبت به حمله‌های امنیتی بسیار آسیب‌پذیر هستند. یکی از مهم‌ترین حملات در اینترنت اشیا، حمله انکار سرویس (DoS)[2] است. حملات انکار سرویس به‌واسطه هدف قرار دادن پهنای باند شبکه و یا اتصالات آن به‌منظور جلوگیری از ارائه سرویس عادی مورد استفاده قرار می‌گیرند. این حملات برای دستیابی به اهداف خود، جریانی از بسته‌ها را به سمت گره قربانی ارسال می‌کنند که به دلیل بالارفتن حجم پردازش در آن گره، سیستم دچار وقفه شده و یا ارائه سرویس با اختلال مواجه می‌شود. این اختلال سرویس حتی می‌تواند منجر به قطعی کامل و از دسترس خارج شدن سرویس نیز شود. نوع دیگری از این حملات تحت عنوان حملات انکار سرویس توزیع‌شده (DDoS)[3] وجود دارد. در این روش، حمله از یک نقطه آغاز نمی‌شود بلکه مهاجم به‌صورت توزیع‌شده عمل کرده و حملات از چندین گره صورت می‌گیرد تا اثربخشی بیشتری داشته باشد. به‌عبارت دیگر بهتر بتواند اختلال در سرویس ایجاد کند و از طرفی شناسایی حمله‌کننده نیز سخت‌تر شود. طبیعتاً در این شرایط، شناسایی و مقابله با این حملات نیز پیچیده‌تر شده و هزینه‌بر خواهد بود. هر دوی این حملات در حال حاضر به‌خوبی برای اینترنت فعلی قابل درک است و راه حل‌هایی برای آنها ارائه شده است [۱].

۱-۱ ضرورت و اهمیت تحقیق

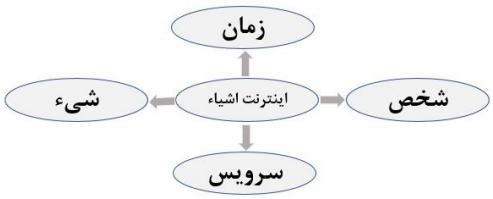
امنیت، مهم‌ترین چالش پیش رو در اینترنت اشیاست. هدف حمله DoS به‌جای ازکارانداختن کل سیستم، مختل‌نمودن آن از طریق محدودکردن دسترسی به گره‌ها یا سرویس‌ها می‌باشد. از طرفی اینترنت اشیا نیز مستعد ابتلا به چنین حملاتی است؛ لذا تکنیک‌های خاص و راه حل‌هایی برای حصول اطمینان از مقابله با چنین حملاتی جهت محافظت از اینترنت اشیا مورد نیاز است. شبکه نرم‌افزارمحور (SDN)[4]، رویکرد جدید شبکه است که هدف آن، مدیریت شبکه از طریق جداکردن صفحه کنترل

این مقاله در تاریخ ۲۸ خرداد ماه ۱۴۰۱ دریافت و در تاریخ ۱۴ دی ماه ۱۴۰۱ بازنگری شد.

فاطمه مطیع شیرازی، دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران، (email: fatemehmotieshirazi@yahoo.com).

سید اکبر مصطفوی (نویسنده مسئول)، دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران، (email: a.mostafavi@yazd.ac.ir).

1. Internet of Things
2. Denial of Service
3. Distributed Denial of Service
4. Software Defined Network



شکل ۱: طرح مفهومی اینترنت اشیا.

و داده می‌باشد. SDN یک پارادایم شبکه هوشمند است که فرصت‌های فراوانی را برای مدیریت و ایمنی IoT باز می‌کند. معماری SDN، الگوهای ارتباطی شبکه IoT را تغییر می‌دهد که منجر به رویکرد جدیدی برای آشکارساختن شبکه امنیتی IoT می‌شود. کنترل متمرکز بر لایه داده و لایه کنترل، نه‌تنها مدیریت بسته‌های داده را ساده‌تر می‌کند، بلکه امنیت را افزایش می‌دهد. چون مقدار داده‌های موجود در این سیستم‌ها بسیار زیاد است، مدیریت ترافیک مناسب و تعادل بار کمک خواهد کرد که برخی از اثرات اضافی را به علت ایجاد جریان داده ساده‌تر کند. ادغام SDN با IoT می‌تواند راه را برای مکانیسم‌های امنیتی و کنترل دسترسی بهتری باز کند و راهی برای تشخیص و تقلیل حملات DoS در IoT باشد [۲].

۱-۲ نوآوری در تحقیق

این تحقیق مشتمل بر حملات DDoS اینترنت اشیا از طریق شبکه‌های SDN است. روش پیشنهادشده برای حفاظت از سوئیچ‌های SDN و کنترلرها در برابر تأثیرات مخرب حملات DDoS در اینترنت اشیا با افزودن سازوکار تشخیصی سبک در کنترلر به‌دست آمده است. دستاوردهای اصلی این تحقیق به‌صورت زیر است:

- طراحی الگوریتم تشخیص DDoS در اینترنت اشیا با استفاده از شبکه‌های SDN
- روش‌های تشخیص مختلف از جمله انواع آنتروپی آدرس‌های IP مقصد، میزان شروع جریان و مطالعه ویژگی‌های جریان
- روش تقلیل حمله مبتنی بر کوتاه‌نمودن تایمر اتلاف جریان در زمان حمله برای کمک به حفظ سوئیچ‌ها

۱-۳ ساختار مقاله

ساختار مقاله به صورت زیر سازماندهی شده است: بخش ۲ برخی اطلاعات اساسی در مورد اینترنت اشیا، معماری و انواع حملات در اینترنت اشیا را ارائه می‌کند. همچنین در آن، ویژگی‌های امنیتی IoT و موارد مربوط به آن با نگاهی بر حملات DDoS و موضوعات مربوط به SDN مورد بحث قرار گرفته است. بخش ۳ به شرح تشخیص حملات DDoS و الگوریتم حذف آن می‌پردازد و پیاده‌سازی مرحله‌به‌مرحله این الگوریتم نیز تشریح شده است. در بخش ۴ ارائه نتایج شبیه‌سازی و تحلیل تفصیلی آمده و نهایتاً نتیجه‌گیری و کارهای آینده در بخش پنجم بیان می‌گردد.

۲- مبانی نظری و پیشینه تحقیق

در این بخش ابتدا به مطالعه خصوصیات اینترنت اشیا، معماری آن، حملات مختلف در اینترنت اشیا، شبکه‌های نرم‌افزاری تعریف‌شده و خصوصیات این شبکه‌ها و نقش کنترل‌کننده و پروتکل OpenFlow در اینترنت اشیا می‌پردازیم. سپس کارهای انجام‌شده در زمینه شناسایی حملات منع سرویس توزیع‌شده در شبکه‌های سنتی و شبکه‌های SDN و به‌طور کلی امنیت در این شبکه‌ها را بررسی می‌کنیم. همین طور خصوصیات و مزایای این شبکه‌ها که می‌توانند در شناسایی حملات به ما کمک کند را بیان می‌کنیم و در نهایت به مقایسه روش‌های پیشین خواهیم پرداخت.

۲-۱ اینترنت اشیا

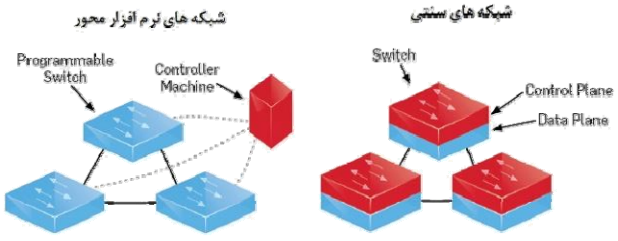
با به‌کارگیری فرستنده و گیرنده‌های با برد کوتاه در زنجیره وسیعی از ابزارها و اقلام هوشمند امروزی، شکل جدیدی از ارتباطات بین افراد و اشیا و اشیا با اشیا شکل گرفته است. در همین راستا و در سال ۱۹۹۸ در بحث شبکه‌ها و ارتباطات بی‌سیم، پارادایم جدیدی به نام اینترنت اشیا توسط کوین اشتون مطرح شد. در واقع، اینترنت اشیا شبکه‌ای جهت اتصال اشیای مختلف از طریق اینترنت به یکدیگر است که کاربردهای متعددی در زمینه سلامت، شهر هوشمند، کشاورزی و صنعت دارد. بنابراین اینترنت اشیا بعد جدیدی را به دنیای اطلاعات و ارتباطات خواهد افزود. اینترنت اشیا فناوری مدرنی است که در آن برای هر موجودیت (انسان، حیوان و یا به‌طور کلی اشیا)، قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت فراهم گردد. در حال حاضر، صنایع گوناگون، مراکز استانداردسازی و منابع تحقیقاتی در حال فعالیت روی توسعه راه حل‌هایی برای فراهم‌کردن نیازمندی‌های فناوری اینترنت اشیا هستند. اینترنت اشیا با نام‌های مختلفی همچون اینترنت همه‌چیز[1](IoE) یا سیاره هوشمندتر[2](SP) نیز شناخته می‌شود. اینترنت اشیا به افراد و اشیا اجازه می‌دهد که در هر زمان با هر شیء، هر شخص و هر سرویس ارتباط برقرار کنند.

۲-۲ انواع حملات در اینترنت اشیا

انواع مختلفی در اینترنت اشیا وجود دارد که هر یک از آنها از مکانیزم خاصی استفاده می‌کنند. عمده حملات در اینترنت اشیا به شرح زیر است:

- حملات فیزیکی: این نوع حملات اشاره به عملکرد سخت‌افزاری دارند و تجهیزات فیزیکی را مورد حمله قرار می‌دهد؛ مانند حمله به میکروکنترلرها.
- حملات رمزگشایی: همان طور که از نام آنها پیداست، این حمله سعی در شکستن رمزها دارد؛ مانند یافتن کلید رمزنگاری برای به‌دست‌آوردن متن اولیه.
- حملات نرم‌افزاری: یکی از اصلی‌ترین حملات در اینترنت اشیا، حملات نرم‌افزاری است. نمونه‌ای از این حملات را که رایج‌ترین آنها نیز است می‌توان برنامه‌های تروجان، ویروس‌ها و کرم‌ها دانست. همچنین کدهای مخرب در این دسته قرار می‌گیرند.
- حملات شبکه‌ای: در دنیای ارتباطات، خصوصاً ارتباطات بی‌سیم که شامل انواع شبکه‌ها از جمله شبکه اینترنت اشیا می‌شود این حمله بسیار کاربردی است. حملاتی مانند استراق سمع، تجزیه و تحلیل ترافیک ورودی و عبوری گره‌ها، حملات انکار سرویس و تخریب یا تغییر در بسته‌ها از جمله این حملات هستند. از آنجایی که تمرکز اصلی ما در این مقاله نیز بر روی حملات انکار سرویس است، این حملات را در ادامه با جزئیات بیشتری مورد بررسی قرار داده‌ایم [۱]. حمله منع سرویس در اینترنت اشیا از متداول‌ترین حمله‌ها در شبکه است و در شبکه اینترنت اشیا نیز صورت می‌گیرد. هدف این حمله، ازکارانداختن سرویس/گره و در نتیجه آن از دسترس خارج کردن

1. Internet of Everything
2. Smarter Planet



(الف) (ب)

شکل ۲: مقایسه شبکه‌های سنتی و SDN.

شبکه است. مهاجم با استفاده از مکانیزم‌هایی مثل افزودن اطلاعات و یا تغییراتی در لایه‌های مختلف شبکه باعث این کار می‌شود.دامنه این حملات بسیار گسترده بوده و شامل گره‌های متعددی می‌شود. از طرفی تشخیص این نوع حملات بسیار مشکل است، چرا که باید الگوریتم مورد نظر ترافیک عادی را از ترافیک حمله متمایز کند. از طرفی زمانی که حمله صورت می‌گیرد، شبکه از کار افتاده و داده‌ها از دسترس خارج می‌شوند. به‌طور کلی در حمله انکار سرویس، الگوهای حمله‌ای مختلفی مانند حمله Sybil، حمله تعلیق پیام، حمله جعل، حمل تغییر و حمله بازپخش مورد استفاده قرار می‌گیرد. همچنین دو نوع کلی از حملات انکار سرویس وجود دارند: ۱) حملات سیل‌آسا و ۲) حملات تخریبی. در حملات سیل‌آسا زمانی که گره، ترافیک بیش از حد آستانه خود را دریافت می‌کند، برای پردازش آنها نیاز به زمان بیشتری دارد و از آنجایی که نمی‌تواند در زمان مورد نیاز، پردازش‌های لازم را انجام دهد، باعث کندشدن آن شده و عملاً از سرویس‌دهی خارج می‌شود. در حمله انکار سرویس توزیع‌شده، اطلاعات بیش از حد تعریف‌شده (حد آستانه) به گره ارسال می‌گردد. در این شرایط منابع گره که شامل پردازنده، حافظه و ... می‌باشد به‌دلیل حجم بالای پردازش از شرایط عادی خارج شده و در نتیجه نمی‌تواند سرویس‌های لازم را به سرویس‌گیرندگان دهد و از دسترس خارج می‌شود. تفاوت این حمله با حمله قبلی در آن است که در این حمله در یک زمان و با یک دوره زمانی خاص به‌صورت مداوم از طریق گره‌های حمله‌کننده مختلف که ممکن است خواسته یا ناخواسته درگیر این مسئله شده باشند، به یک گره قربانی مشخص حمله صورت می‌گیرد. این حمله که قدرت تخریب بیشتری نسبت به حمله قبلی دارد، باعث ازکارافتادن گره سرویس‌دهنده می‌شود [۳].

۲-۳ شبکه‌های نرم‌افزارمحور

شبکه‌های نرم‌افزارمحور برای ساده‌شدن مدیریت شبکه و هوشمندی شبکه‌ها به وجود آمده‌اند و در این شبکه‌ها قسمت کنترلی و قسمت سخت‌افزاری تجهیزات شبکه از هم تفکیک شده‌اند و بخش کنترل داده‌ها از روی سوئیچ به لایه‌های نرم‌افزاری منتقل شده که قابلیت برنامه‌پذیری، مقیاس‌پذیری و انعطاف‌پذیری را از طریق توسعه نرم‌افزاری برای ما فراهم می‌کند. شبکه‌های نرم‌افزاری از سه قسمت اصلی تشکیل گردیده‌اند: برنامه‌های کاربردی، صفحه کنترل و صفحه داده که لایه زیرساخت هم نامیده می‌شود [۲].

همان گونه که در شکل ۲- الف نشان داده شده است، عملیات گره شبکه در یک شبکه معمولی متشکل از تعامل بین داده و صفحات کنترلر است. مسئولیت صفحه کنترل، محاسبه مسیرهای بین شبکه و انتقال آنها به صفحه داده برای ارسال داده است. بنابراین بعد از جریان ایجادشده در اکثر موارد، هر گونه تغییرات مختصر مستلزم تغییر پیکربندی در هر یک از دستگاه‌ها خواهد بود. در تعداد زیادی از شبکه‌ها این بدان معنا است که اپراتورهای شبکه به زمان زیادی برای پیکربندی مجدد دستگاه‌ها به‌صورت روتین با سازگاری با تقاضاهای متغیر ترافیک و شرایط شبکه نیاز دارند. مفهوم اصلی SDN در مفهوم جدایی صفحات داده و کنترل نهفته است که در شکل ۲- ب نشان داده شده است. OpenFlow نوعی پروتکل SDN استانداردشده است که برای پشتیبانی از ارتباطات بین کنترلر و گره‌های شبکه استفاده می‌شود [۳].

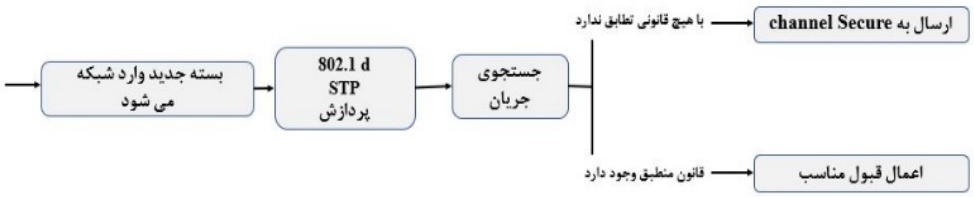
از آنجا که کنترلرها دید کاملی نسبت به تمام شبکه دارند، می‌توانند تغییرات متناسب با شرایط ترافیک را مدیریت کنند. این رویکرد به‌صورت چشم‌گیری موجب تسهیل پیاده‌سازی برخی از توابع شبکه می‌شود. همان گونه که در شکل ۳ نشان داده شده است، هنگامی که بسته اول به سوئیچ می‌رسد، جدول جریان به بررسی قوانین جریان انطباقی می‌پردازد. اگر تطبیقی یافت شود، اقدامات جریان از طریق آن تعیین و اجرا و آمار جریان به‌روزرسانی خواهد شد؛ در غیر این صورت، هدر بسته از طریق یک کانال امن به‌سوی کنترلر ارسال خواهد شد. کنترلر به پردازش بسته بر حسب الگوریتم تعریف‌شده در کنترلر پرداخته و اقدامات انجام‌شده از سوی سوئیچ‌ها را در راستای انتخاب مسیر بین منبع و مقصد تعیین می‌کند. قانون جریان جدید در مسیری که قرار است در جداول جریان آنها نصب شود، فرستاده خواهد شد. سوئیچ شروع به اقدامات مناسب روی بسته‌های داده جریان و بر اساس قانون جریان جدید می‌نماید. اگر هیچ ورودی جریان تطبیقی در کنترلر یافت نشود، از آن صرف‌نظر خواهد شد [۴].

۲-۴ مزایای استفاده از SDN در IoT

امروزه شاید بعضی، تمایل چندانی به پرداخت هزینه برای استفاده از چنین راهکاری نداشته باشند، اما همگی توافق دارند که SDN راهکاری کلیدی برای حل مشکلات IoT است. در واقع نمی‌توان عنوان کرد که IoT به SDN وابسته است، ولی SDN می‌تواند فواید زیادی برای IoT داشته باشد. با این حال به‌کارگیری SDN، اقدامی ضروری از طرف ارائه‌دهندگان خدمات برای استفاده از فرصت‌های IoT می‌باشد. مدیریت پویای ترافیک نیز امکان نظارت و هماهنگ‌کردن تغییرات پهنای باند را به‌صورت خودکار برای اپراتورها فراهم می‌کند. چنین چیزی به‌خصوص برای ارائه‌دهندگان خدمات IoT در سطح جهانی که خود را برای افزایش تصاعدی تعداد دستگاه‌ها و داده‌های IoT آماده می‌کنند، بسیار ایده‌آل است. به‌صورت کلی، SDN در صورت استقرار مناسب در مرکز داده می‌تواند به‌خوبی از پس سیل داده‌هایی که از IoT ناشی می‌شود برآید. امکانات SDN مثل خودکارسازی، تأمین منابع، قابلیت برنامه‌ریزی و هماهنگی می‌تواند ارزش زیادی را در یک محیط مبتنی بر IoT ایجاد کند [۵]. هنگام استفاده از SDN در خدمات و برنامه‌های کاربردی IoT باید امنیت را در تمام بخش‌ها بهبود بخشید، زیرا هر دستگاه یا برنامه کاربردی می‌تواند الزامات امنیتی خاص خود را داشته باشد و سطح متفاوتی از امنیت را طلب کند.

۲-۵ مطالعات پیشین

مقالات متعددی، بحث تشخیص حملات DDoS در اینترنت اشیا را با استفاده از شبکه‌های SDN مورد بررسی قرار داده‌اند. در سال ۲۰۱۶، لو و وانگ از ترکیب OpenFlow و sFlow برای طراحی مکانیسمی برای شناسایی و کاهش اثر ناهنجاری (حملات DDoS) در شبکه SDN استفاده کرده‌اند. در این روش، نمونه‌برداری داده‌ها با استفاده از sFlow و



شکل ۳: پردازش جریان در پروتکل OpenFlow.

جدول ۱: مقایسه روش‌های پیشین.

روش	توضیح
در [۶] از sFlow برای نمونه‌برداری جریان و از الگوریتم تشخیص بر پایه آنتروپی استفاده شده است.	از ترکیب OpenFLow و sFlow استفاده شده و نمونه‌برداری جریان با استفاده از sFlow انجام می‌شود و با استفاده از الگوریتم‌های بر مبنای آنتروپی، اقدام به شناسایی حمله می‌کند. بار کاری کنترل‌کننده و زمان پاسخگویی را افزایش می‌دهد و مقدار مثبت اشتباه بالایی دارد.
در [۷] از آنتروپی استفاده شده است.	ابتدا اطلاعات جریان جمع‌آوری می‌شود و سپس تعداد IPهای فعال در پنجره زمانی به دست می‌آید. این روش میزان مثبت/منفی کاذب زیادی دارد.
در [۸] تحلیل ترافیک و به‌روزرسانی پویای قوانین استفاده شده است.	معماری جدید شبکه‌های محتوامحور، قابلیت واکنش در برابر حملات DDoS به‌وسیله استفاده از OpenFLow را دارند. اما در این روش سربار پردازشی و تأخیر زیادی دارد.
در [۱۰] از آنتروپی و آمار جدول جریان استفاده شده است.	این متد روی سوئیچ لبه شبکه پیاده‌سازی شده و از محاسبه آنتروپی روی IP مقصد به‌عنوان مکانیزم شناسایی استفاده می‌کند؛ دقت خوبی دارد ولی میزان مثبت اشتباه، زیاد است.
در روش پیشنهادی از بسته‌های Packet-in و جمع‌آوری آمار جدول جریان استفاده شده است.	در این روش با استفاده از دریافت بسته‌های Packet-in و درنظرگرفتن پنجره زمانی و محاسبه آنتروپی و نرخ جریان، حمله احتمالی در شبکه تشخیص داده می‌شود.

شناسایی ناهنجاری با استفاده از الگوریتم‌های بر مبنای آنتروپی انجام شده و با استفاده از OpenFlow در سطح شبکه اقدام به کاهش اثر حمله روی شبکه گردیده است [۶].

موسوی در ۲۰۱۷، روشی برای تشخیص زودهنگام حملات DDoS در برابر کنترل‌کننده‌های SDN ارائه کرده است [۷]. در مدل ارائه‌شده، تصادفی‌بودن بسته‌های ورودی به‌وسیله آنتروپی اندازه‌گیری شده و هدف اصلی این مقاله، تشخیص حمله در مراحل اولیه است. دلیل اصلی استفاده از آنتروپی برای تشخیص DDoS توانایی در اندازه‌گیری تصادفی‌بودن بسته‌های ورودی است که به شبکه می‌آیند. هرچه تصادفی‌بودن بیشتر باشد، آنتروپی نیز بیشتر است و بالعکس. در ارزیابی‌ها این روش موفق گردیده که در ۲۵۰ بسته اولیه بتواند حمله را شناسایی کند ولی اشاره‌ای به مقدار مثبت اشتباه نشده است.

کاروالیو و همکاران در سال ۲۰۱۹، راه حلی برای کاهش حملات DDoS با استفاده از OpenFlow ارائه کرده‌اند. OpenFlow آمارهای جریان را نگهداری می‌کند که این آمارها می‌توانند برای شناسایی تغییرات ناگهانی در ترافیک که ممکن است علامت یک حمله DDoS باشند، استفاده شود [۸].

بختیاری در سال ۲۰۲۰، روشی را پیشنهاد کرده که می‌تواند رفتار شبکه‌های نرم‌افزارمحور را به‌منظور تشخیص حمله منع سرویس توزیع‌شده مدل‌سازی کند. در این مقاله با توجه به ساختار SDN و تحلیل ترافیک، یک مدل آماری ذوزنقه‌ای برای تخمین رفتار شبکه در حالت نرمال معرفی شده است. سپس با استفاده از روش رگرسیون خطی و تخمین EWMA، حد آستانه تشخیص حمله به‌صورت پویا در بازه‌های زمانی مشخص، تخمین زده شده است. بر اساس این مدل، حد آستانه‌ای برای تعداد خطاهای جدول سوئیچ تعریف می‌گردد که این حد آستانه بر اساس روش EWMA محاسبه می‌شود. نتایج ارزیابی نشان داده‌اند که مدل پیشنهادی قادر است حملاتی را که توسط روش‌های مبتنی بر آنتروپی و PCA قابل تشخیص نیستند تشخیص دهد [۹].

گالیانو در سال ۲۰۲۰، یک مکانیزم شناسایی حمله منع سرویس توزیع‌شده را بر اساس آنتروپی ارائه کرده است. این مکانیزم روی سوئیچ لبه شبکه ارائه شده که قادر به شناسایی حملات سیل‌آسا می‌باشد و بار جمع‌آوری ترافیک توسط کنترلر را کاهش داده است. الگوریتم ارائه‌شده به‌صورت دوره‌ای اجرا می‌شود و از کنترل‌کننده فلودلایت استفاده می‌کند [۱۰]. در جدول ۱ روش‌های مطرح موجود مورد مقایسه قرار گرفته و مزایا و معایب هر روش قید شده است.

۳- روش پیشنهادی

این الگوریتم تشخیص بر اساس سه مفهوم اصلی از جمله تنوع آنتروپی آدرس IP مقصد، میزان جریان اولیه و مطالعه ویژگی‌های جریان طراحی شده است. آنتروپی یا شاخص شانون- وینر در سال ۱۹۸۴ [۱۱] ارائه شده و یکی از مفاهیم بسیار مهم در تئوری اطلاعات است. آنتروپی، معیار عدم قطعیت یا پیشامد تصادفی مربوط به متغیر تصادفی است که در این مورد، آدرس مقصد است. با استفاده از آنتروپی خصوصیات و آمارهایی که از جدول جریان سوئیچ‌ها دریافت می‌کنیم، اقدام به شناسایی حملات منع سرویس توزیع‌شده می‌نماییم. میزان پیشامد تصادفی بالاتر به آنتروپی بالاتر می‌انجامد. هنگامی که تمام ترافیک به سوی مقاصد معینی ارسال شود، مقدار آنتروپی در میزان کمینه خود قرار دارد. از سوی دیگر، مقدار آنتروپی در بیشینه مقدار خود است، زمانی که ترافیک به‌طور برابر در تمام مقاصد احتمالی توزیع‌شده باشد [۱۲]. الگوریتم تشخیص مبتنی بر آنتروپی در جایی مشابه مورد ذکرشده در [۷] استفاده می‌شود. الگوریتم از پنجره‌ای استفاده می‌کند که با تعداد n بسته‌ها اندازه‌گیری می‌شوند که در آن n اندازه پنجره است. به ازای هر پنجره، بسته‌ها در گروه‌های مبتنی بر آدرس IP مقصد دسته‌بندی می‌شوند. تمام بسته‌های هر گروه از آدرس مقصد یکسان برخوردار هستند اما ممکن است آدرس‌های منبع متفاوتی داشته باشند. آدرس IP مقصد به‌عنوان معیار ویژگی و توالی آدرس IP مقصد مجزا در این پنجره به‌عنوان معیار پیشامد تصادفی در نظر گرفته شده است. فرض کنید که m تعداد آدرس‌های IP مقصد کل مربوط به این بسته‌های n باشد. معیار آنتروپی که با H نمایش داده می‌شود از

رابطه زیر محاسبه می‌شود که توالی نسبی آدرس IP مقصد، یعنی Ipi احتمال رویداد iام در دنباله رویدادها است [۷]

$$F_i = \frac{n_i}{n} \quad (۱)$$

$$H = -\sum_{i=۱}^{m} F_i \log_۲ F_i \quad (۲)$$

$$۰ \le F_i \le ۱ \rightarrow H \ge ۰ \quad (۳)$$

در حالت نرمال شبکه، انتظار داریم که گسترش ترافیک به بسیاری از میزبان‌ها صورت پذیرد. در طول حمله DDoS، تعداد بسته‌های مقصد برای میزبان معین یا مجموعه کوچکی از میزبان‌ها به‌طور ناگهانی، افزایش و آنتروپی کاهش می‌یابد. کاهش در مقدار آنتروپی، هشداری برای شبکه و توجه به حملات احتمالی است.

در شبکه‌های SDN، برخورداری از روش تشخیص سریع و شناسایی حملات در مراحل اولیه ضرورت دارد. شبکه‌های SDN در مقابل حملات DDoS آسیب‌پذیری بیشتری نسبت به شبکه‌های سنتی دارند. اگر زمان تشخیص بسیار طولانی شود، مهاجم می‌تواند سوئیچ‌ها یا کنترلرها را تخریب کند و بنابراین تشخیص اولیه تا حد زیادی اهمیت دارد. برای تشخیص در مراحل اولیه، پنجره نباید زیاد بزرگ باشد و از سوی دیگر، پنجره کوچک هم موجب افزودن سربار محاسباتی می‌شود. همان گونه که توسط اوشیما و همکاران [۱۳] در این تحقیق پیشنهادشده، از اندازه پنجره پنجاه برای ایجاد توازن بین این دو مقوله استفاده می‌کنیم. ماژول اضافه‌شده به کنترلر pox برای محاسبات آنتروپی است و به ازای هر پنجاه بسته‌ای که به کنترلر می‌رسد، توالی نسبی محاسبه می‌شود. آنتروپی محاسبه‌شده با مقدار آستانه محاسبه می‌گردد. اگر آنتروپی محاسبه‌شده کمتر از آستانه باشد، به ازای هر پنج محاسبه آنتروپی، یک حمله مشکوک وجود دارد و تحلیل بیشتری برای تشخیص واقعیت آن لازم است [۱۳].

اگرچه آنتروپی، روش تشخیص موفقی محسوب می‌شود اما استفاده از آن نمی‌تواند سناریوهای حمله زیادی را تشخیص دهد. برای نمونه، زمان‌های اوج با افزایش ناگهانی ترافیک مجاز در میزبان مقصد شبکه مشخص مانند سرور وب یا ایمیل افزایش می‌یابد و روش تشخیص مبتنی بر آنتروپی می‌تواند به‌صورت پیوسته، هشدار مثبت کاذب را گزارش کند. از سوی دیگر، هنگامی که مهاجم حمله را در میان قربانی‌های زیاد توزیع می‌کند، آنتروپی نمی‌تواند کاهش چشم‌گیر را نشان دهد و بنابراین به گزارش منفی کاذب منجر می‌شود. برای غلبه بر محدودیت‌های ذکرشده تشخیص از طریق آنتروپی، روش تشخیص پیشنهادی در این پروژه با الگوریتم‌های تشخیصی دیگر همراه می‌شود. مفهوم دیگری که برای شناسایی حملات منع سرویس توزیع‌شده استفاده کرده‌ایم بر اساس این واقعیت است که نرخ جریان ورودی به‌طور ناگهانی هنگام حمله در شبکه افزایش می‌یابد. از آنجا که نرخ جریان ورودی در شبکه‌های SDN به دلیل دارابودن کنترل‌کننده مرکزی به راحتی امکان‌پذیر است، در اینجا به عنوان دومین عامل برای آزمایش ترافیک شبکه از آن استفاده می‌کنیم

$$FlowRate = \frac{Window\ Size}{Window\ Time} \quad (۴)$$

که در این رابطه *FlowRate* نرخ جریان، *Window Size* اندازه پنجره و *Window Time* طول مدت پنجره است. چنانچه نرخ اولیه جریان محاسبه‌شده بالاتر از آستانه باشد، احتمال بروز حمله وجود دارد و بررسی بیشتری باید انجام شود. اگر نرخ محاسبه‌شده کمتر از آستانه باشد، حالت ایمن تلقی می‌شود. هنگام استفاده از نرخ اولیه به‌عنوان روش تشخیص باید به خاطر داشته باشیم که مقدار بالایی از نرخ اولیه برای گزارش حمله ممکن است که موجب احتمال بالای مثبت کاذب شود [۱۴]. بنابراین در الگوریتم پیشنهادی، پایش نرخ جریان اولیه صرفاً به‌عنوان میانگین تشخیص نشانه حمله و نه تأیید آن مورد استفاده قرار می‌گیرد. اگر حمله‌ای مشکوک باشد، آمار جریان از جداول جریان سوئیچ‌های مشکوک به حضور در مسیر حمله تحلیل می‌شود تا رخداد حمله تأیید شود. همان طور که می‌دانید، تعیین دقیق حد آستانه برای الگوریتم‌های تشخیص ناهنجاری در شبکه بسیار حیاتی است و در صحت تشخیص و میزان مثبت اشتباه و منفی اشتباه در شبکه نقش اساسی دارد. در الگوریتم پیشنهادی آستانه اولیه در سطحی ثابت‌شده که میزان ترافیک شبکه قابل است و در چنین حالتی شبکه قادر به عملیات ایمن خواهد بود. اگر مطالعه بیشتر آمار جریان، وجود حمله را نشان نداد، میزان آستانه باید برای نرخ محاسبه‌شده فعلی به‌روزرسانی شود تا از گزارش حمله مثبت کاذب در سیستم اجتناب شود. مطالعه جداول جریان به‌عنوان سازوکاری برای اطمینان نهایی از بروز حمله بعد از تردید نسبت به حمله بر اساس تحلیل آنتروپی و نرخ اولیه جریان خواهد بود. هنگامی که تمام جریان‌های جدول جریان بررسی شدند، نرخ حمله یعنی Attack rate برای نشان‌دادن احتمال اینکه سوئیچ ممکن است تحت حمله قرار گرفته باشد، محاسبه می‌شود. این نرخ حمله با تقسیم تعداد جریان‌هایی که دو مورد از شرایط حمله را داشته باشند بر تعداد کل جریان‌های جدول جریان به‌دست می‌آید

$$Attack\ Rate = \frac{Two\ cases\ of\ attack\ conditions}{Total\ number\ of\ flow\ table} \quad (۵)$$

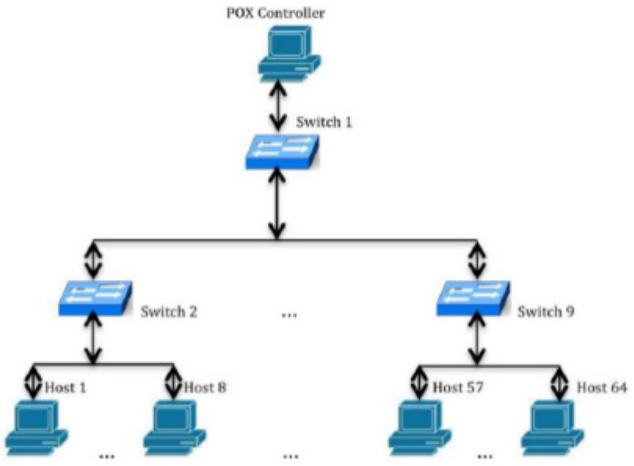
در نهایت می‌توان گفت حمله رخ داده است اگر

$$Attack\ Rate > Threshold\ Rate \quad (۶)$$

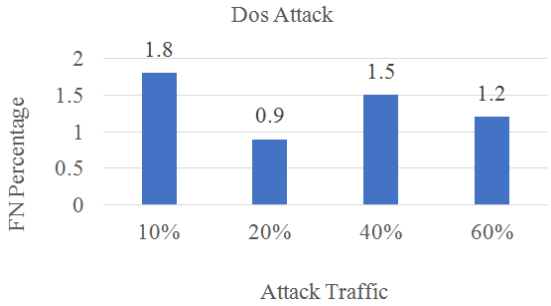
در الگوریتم پیشنهادی برای تقلیل حملات انکار سرویس توزیع‌شده، تایمر جعلی جریان از مقدار پیش‌فرض به کاهشی تغییر می‌کند تا از تخریب سوئیچ‌ها جلوگیری کند. مقادیر کاهش‌یافته کمتر از مقادیر پیش‌فرض هستند و در نتیجه، جریان‌های جعلی کوتاه به سرعت از بین می‌روند و از جدول جریان سوئیچ حذف می‌شوند.

٤- شبیه‌سازی و نتایج

شبیه‌سازی و تست روش پیشنهادی برای تشخیص حمله DDoS در لپ‌تاپ ASUS K۴۵۱-Corei۷ ،CPU ۱٫۸۰ گیگاهرتز و RAM ۸ گیگابایت انجام شده است. این الگوریتم با زبان Python و بر اساس کنترلر pox در محیط شبکه مجازی Mininet [۱۵] پیاده‌سازی گردیده است. از Scapy scripts برای تولید ترافیک حمله و مجاز در میزبان‌های شبکه در طول شبیه‌سازی استفاده شده است. Scapy یک برنامه قدرتمند دستکاری بسته تعاملی است که قادر به جعل یا برداشتن کد بسته‌های تعداد زیادی از پروتکل‌ها و ارسال آنها به شبکه، شبیه‌سازی حملات، قراردادن بسته‌ها در سیستم‌های کامپیوتری، تطبیق درخواست‌ها و پاسخ‌ها و موارد دیگر است. Scapy را می‌توان در دو حالت مختلف به‌صورت تعاملی از طریق پنجره پایانه و به لحاظ برنامه‌ای از طریق نسخه Python اجرا کرد. پارامترهای دیگری در Scapy وجود دارند که از جمله آنها نوع بسته‌ها، تعداد بسته‌هایی که باید فرستاده شوند، بار اضافی بسته و فواصل زمانی ترافیک است [۱۶]. ساختار شبکه برای شبیه‌سازی فعلی، شبکه از نوع درخت با ارتفاع ۲ و گنجایش خروجی ۸ است که ۶۴ میزبان در آن جای می‌گیرند (شکل ۴). ساختار درخت بر اساس اینکه ساختار شبکه به‌طور گسترده در کدام مراکز داده استفاده می‌شوند، انتخاب گردیده است.



شکل ۴: توپولوژی شبکه.



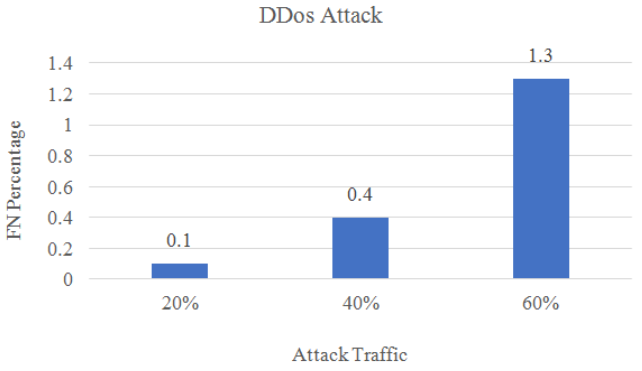
شکل ۵: گزارش رفتار FN در حمله به یک قربانی.

سوئیچ‌های مورد استفاده در شبکه همان سوئیچ‌های مجازی باز یا OVS هستند.

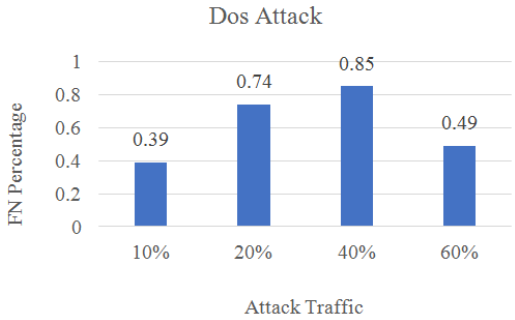
در پیاده‌سازی از چهار نرخ جریان مختلف استفاده کردیم که از رابطه زیر به دست می‌آیند

$$Attack\ Traffic\ Ratio = \frac{Attack\ Traffic\ Rate}{Total\ Traffic\ Rate} \qquad (۷)$$

که در این رابطه *Attack Traffic Ratio* نسبت نرخ ترافیک حمله، *Attack Traffic Rate* نرخ ترافیک حمله و *Total Traffic Rate* نرخ کل ترافیک می‌باشد [۱۷]. در ارزیابی‌ها زمان تشخیص حمله و زمان هشدار حمله احتمالی از لحظه آغاز حمله برای تعیین سرعت شناسایی حمله توسط الگوریتم، میزان مثبت اشتباه و منفی اشتباه برای تست دقت الگوریتم و میزان مصرف CPU و میزان تغییرات آنتروپی و تأثیر تغییر ترافیک روی آنتروپی در هر سناریو برای ارزیابی میزان کارایی ثبت شده و مورد بررسی قرار گرفته و نتایج با جزئیات در ادامه آورده شده‌اند. در ارزیابی‌ها نشان دادیم که فارغ از نوع ترافیک به دلیل استفاده از آنتروپی روی آدرس مقصد و میزان شروع جریان و مطالعه مشخصات جریان، الگوریتم توانایی تشخیص کلیه حملات را دارد و همچنین با افزایش نرخ ترافیک حمله، میزان دقت در تشخیص بالاتر می‌رود و زمان تشخیص نیز کاهش می‌یابد. همچنین در این الگوریتم به دلیل عدم استفاده از محاسبات پیچیده، سربار محاسباتی قابل چشم‌پوشی و سربار پردازشی در حد قابل قبولی می‌باشد و با استفاده از منابع سخت‌افزاری قوی‌تر قابل مدیریت‌کردن است. در مراحل شناسایی، زمان شناسایی احتمال حمله و زمان شناسایی حمله قطعی ثبت می‌شود و همچنین میزبانی که بیشترین ترافیک را به خود اختصاص می‌دهد به عنوان قربانی، شناسایی و اعلام می‌گردد و همچنین تأخیر در شناسایی برای هر سناریو محاسبه شده است.



شکل ۶: گزارش رفتار FN در حمله به چند قربانی.



شکل ۷: گزارش رفتار FP در حمله به یک قربانی.

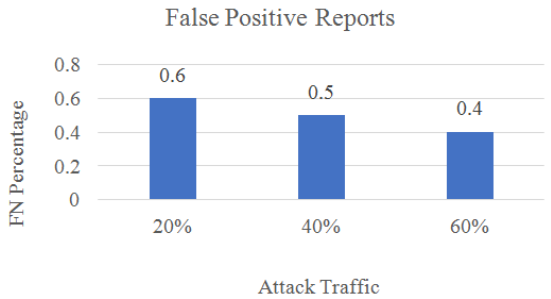
الگوریتم پیشنهادی در این تحقیق، هشت روش تشخیص را نشان می‌دهد که مستلزم داشتن منابع حداقلی شبکه و در عین حال ارائه نرخ تشخیص بسیار بالاست. این روش تشخیص، تحت رفتارهای مختلف شبکه و با حداقل تأخیر تشخیص عملکرد خوبی داشته است. این روش پیشنهادی برای تشخیص حملات است و این روش قادر به تشخیص مهاجمان در هر حمله به یک یا چند قربانی می‌باشد و از دقت بالایی برخوردار است.

شکل ۵ گزارش میانگین منفی کاذب را در حمله به یک قربانی در چهار نرخ متفاوت نشان می‌دهد. اگرچه بیشترین نرخ حمله FN متعلق به پایین‌ترین نرخ حمله بوده است، اما همان گونه که مشاهده می‌شود نرخ FN از رفتار خطی تبعیت نمی‌کند.

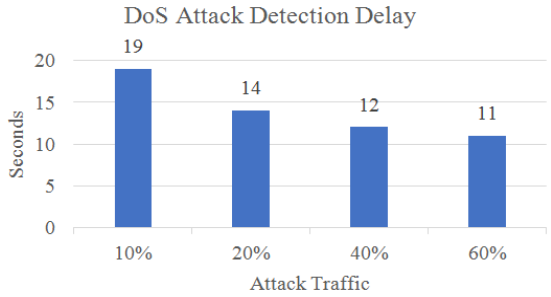
شکل ۶ گزارش میانگین منفی کاذب را در حمله به چند قربانی نشان می‌دهد. همان گونه که مشاهده می‌شود به‌محض افزایش نرخ حمله، فرصت گزارش منفی کاذب بیشتر می‌شود. دلیل این امر آن است که در آزمایش‌های ترافیک حمله، تعداد قربانی‌های حمله افزایش می‌یابد و در نتیجه تعداد سوئیچ‌های گزارش‌شده به‌عنوان تحت حمله نیز زیاد می‌شود و از آنجا که ترافیک حمله در چندین قربانی توزیع می‌شود، همه سوئیچ‌ها حجم بالایی از جریان حمله را دریافت نمی‌کنند و تعداد گزارش‌های منفی کاذب شروع به افزایش می‌کند. اما با این حال روش پیشنهادی نشان می‌دهد که درصد گزارش مثبت کاذب حاکی از رفتار نسبتاً پایدار با کاهش جزئی در افزایش ترافیک حمله مواجه است.

شکل ۷ میانگین گزارش‌های FP در نرخ‌های حمله مختلف را نشان می‌دهد. در سه نرخ اول حمله، گزارش‌های FP با نرخ ترافیک افزایش می‌یابند، اما به‌محض رشد ترافیک بیشتر در شبکه، گزارش‌های FP شروع به کاهش تا مقدار کمینه می‌کند. نتایج نشان می‌دهند که این الگوریتم، نرخ FP بسیار پایینی را در تمام طیف‌های حمله نشان می‌دهد.

همان طور که دیدیم در این حمله نه‌تنها احتمال خطای گزارش کاذب (هم منفی و هم مثبت) کم است، بلکه میزان گزارش‌های کاذب به‌آسانی



شکل ۸: گزارش رفتار FP در حمله به چند قربانی.



شکل ۹: تأخیر در تشخیص حمله در حمله به یک قربانی.

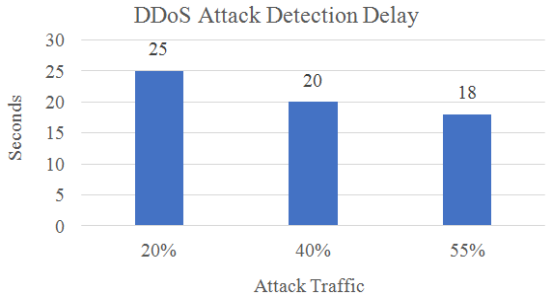
می‌تواند با تغییرات کوچک در الگوریتم کاهش یابد. در نتایج به‌دست‌آمده از شبیه‌سازی‌ها می‌توان مشاهده کرد مادامی که کنترلرها و سوئیچ‌ها مورد حمله قرار نگیرند، گزارش FP یا FN بیشتر از دو بار تکرار نخواهد شد و با توجه به شدت حمله، زمان شناسایی حمله در نرخ بالاتر، کاهش قابل ملاحظه‌ای می‌یابد. همچنین کاهش آنتروپی نیز روی IP مقصد قابل مشاهده است و با توجه به زمان شناسایی و تأثیر معیارهای در نظر گرفته شده، به نظر می‌رسد که این پژوهش در رسیدن به هدف خود موفق عمل کرده است. این بدان معناست که الگو در تمامی شبیه‌سازی‌ها اجرا گردیده و از طریق این نظریه نشان داده شده که گزارش FN یا FP به‌طور مستمر حداکثر دو بار تکرار شده و خطا از طریق نتایج به‌دست‌آمده در حداکثر دور سوم اصلاح شده و این یک گزارش FP است که در حالت قبل از حمله برقرار بوده است.

شکل ۸ گزارش میانگین مثبت کاذب را در حمله به چند قربانی نشان می‌دهد. درصد گزارش مثبت کاذب حاکی از رفتار نسبتاً پایدار با کاهش جزئی در افزایش ترافیک حمله است.

از اهداف این مقاله، ارائه راه حلی برای شناسایی حملات در مراحل اولیه یا به عبارت دیگر حداقل زمان تشخیص است. شکل ۹ میانگین زمان تشخیص حمله را در بار ترافیک هر حمله نشان می‌دهد. همان گونه که مشاهده می‌کنید با افزایش بار حمله، میانگین زمان تشخیص حمله شروع به کاهش می‌کند. این بدان دلیل است که بار ترافیک بالاتر می‌رود و پنجره نمونه‌برداری بسته به سرعت جمع‌آوری شده و بنابراین حمله سریع‌تر شناسایی می‌شود.

شکل ۱۰ میانگین زمان تشخیص حمله تحت نرخ‌های مختلف ترافیک حمله را نشان می‌دهد. همان گونه که در شکل می‌بینیم به دلیل اینکه در روش پیشنهادی، ترافیک و طول مدت پنجره نمونه‌برداری بسته کوتاه‌تر است، با افزایش در نرخ حمله زمان تشخیص شروع به افت می‌کند و در نتیجه حمله سریع‌تر تشخیص داده می‌شود.

همان گونه که در حمله به چندین قربانی مشاهده می‌شود، روش آنتروپی به اندازه حمله به یک قربانی کارآمد نیست. در واقع، فرصت حمله به چندین قربانی از طریق تغییرات نرخ جریان اولیه بیشتر از تغییرات



شکل ۱۰: تأخیر در تشخیص حمله در حمله به چند قربانی.

آنتروپی است. نتایج نشان می‌دهند که روش تغییر آنتروپی نمی‌تواند به‌عنوان روش تشخیص استاندارد برای حمله به چندین قربانی استفاده شود و در حمله چند قربانی، محاسبه نرخ جریان و مطالعه جریان کارآمدتر خواهد بود.

۵- مقایسه روش پیشنهادی و پژوهش‌های پیشین

همان طور که در پژوهش‌های پیشین بیان کردیم، آنتروپی در متدهای مختلفی در شبکه‌های سنتی برای شناسایی ناهنجاری در شبکه استفاده گردیده و اگر بخواهیم که از روش‌های تشخیص در شبکه‌های SDN مواردی را بیان کنیم و با روش پیشنهادی مقایسه کنیم، موارد زیر مورد توجه هستند.

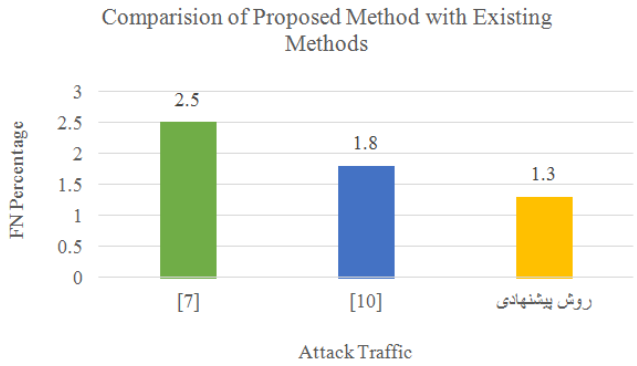
در این پژوهش مشابه با [۷]، پنجره زمانی برابر با ۵۰ بسته در نظر گرفته شده و آنتروپی محاسبه گردیده و ما نیز از این واقعیت که محاسبات برای پنجره زمانی کوچک بسیار سربار محاسباتی کمتری دارد، استفاده کرده‌ایم. ولی قابل ذکر است که استفاده از آنتروپی به‌تنهایی در شرایط اوج ترافیک شبکه و شرایطی که تعداد بیش از یک قربانی در شبکه داشته باشیم برای شناسایی ایجاد محدودیت می‌کند. لذا در این شرایط احتمال "مثبت کاذب" و "منفی کاذب" بالا می‌رود و نیازمند معیارهای دیگری برای اطمینان از وجود حمله در شبکه هستیم.

در [۱۸] یک مکانیزم شناسایی حمله منع سرویس توزیع‌شده بر اساس آنتروپی ارائه شده که با وجود تفاوت‌ها، شبیه‌ترین کار به روش پیشنهادی این پروژه می‌باشد. این مکانیزم روی سوئیچ لبه شبکه ارائه گردیده که قادر به شناسایی حملات سیل‌آسا می‌باشد و بار جمع‌آوری ترافیک توسط کنترلر را کاهش داده است. این الگوریتم محاسبات کمی دارد و به سادگی روی SDN پیاده‌سازی می‌شود. تفاوت‌های این مطالعه با روش پیشنهادی در مقدار حد آستانه، پنجره زمانی و محل اجرای الگوریتم می‌باشد. ما در ادامه، دو مقاله [۷] و [۱۰] را شبیه‌سازی و با مقاله پیشنهادی خود مقایسه کرده‌ایم.

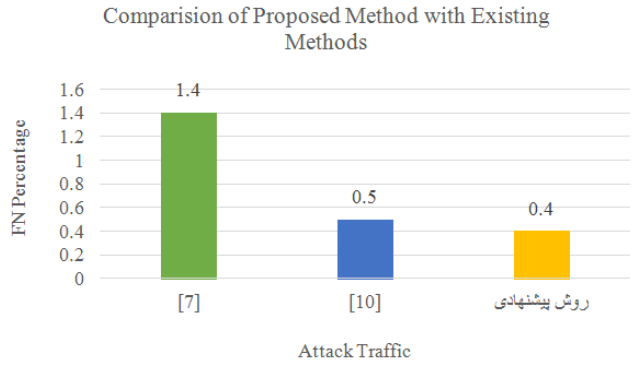
شکل ۱۱ گزارش‌های مربوط به منفی کاذب را در روش پیشنهادی و روش‌های موجود در الگوی ترافیک حمله به یک قربانی نشان می‌دهد. همان طور که مشخص است، روش پیشنهادی بعد از اجرای چندین سناریو تعداد منفی کاذب کمتری را گزارش می‌کند.

شکل ۱۲ گزارش‌های مربوط به مثبت کاذب را در روش پیشنهادی و روش‌های موجود در الگوی ترافیک حمله به چند قربانی نشان می‌دهد. همان طور که مشخص است، روش پیشنهادی بعد از اجرای چندین سناریو تعداد مثبت کاذب کمتری را گزارش می‌کند.

شکل ۱۳ میانگین زمان تشخیص حمله را در روش پیشنهادی و روش‌های موجود نشان می‌دهد. روش پیشنهادی در مقایسه با روش‌های موجود از کاهش زمان تشخیص قابل توجهی برخوردار است.



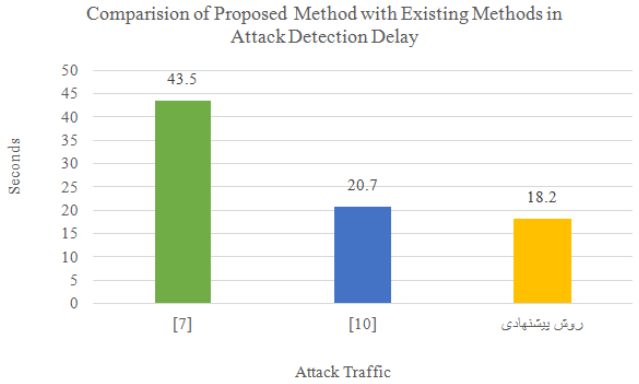
شکل ۱۱: مقایسه رفتار گزارش‌های منفی کاذب در حمله به چندین قربانی در روش پیشنهادی و روش‌های موجود.



شکل ۱۲: مقایسه رفتار گزارش‌های مثبت کاذب در حمله به چندین قربانی در روش پیشنهادی و روش‌های موجود.

۶- نتیجه‌گیری

اینترنت اشیا یکی از فناوری‌های نوین در عصر کنونی می‌باشد که در آن بسیاری از وسایل و اشیای پیرامون ما جهت کاربردهای گوناگون به شبکه اینترنت متصل می‌شوند. رشد نمایی وسایل و اشیای متصل به شبکه، ضرورت توسعه برنامه‌های کاربردی و سرویس‌های اینترنت اشیا را بیش از پیش کرده است. با این حال، زیرساخت شبکه کنونی شامل محدودیت‌هایی است و توسعه اینترنت اشیا مستلزم داشتن زیرساخت‌های مخصوص به خود می‌باشد. اساس کار شبکه‌های نرم‌افزارمحور، جداسازی بخش کنترلی شبکه از داده‌ای آن است که قابلیت برنامه‌ریزی و کنترل متمرکز را برای زیرساخت شبکه فراهم می‌آورد. امکانات SDN مثل خودکارسازی، تأمین منابع، قابلیت برنامه‌ریزی و هماهنگی می‌تواند ارزش زیادی را در یک محیط مبتنی بر IoT ایجاد کند و از حملاتی چون DoS جلوگیری نماید. قابلیت کنترل متمرکز در SDN سبب می‌شود که کنترلر، دید جامعی از شبکه داشته باشد و در صورتی که در شبکه، حمله DoS رخ دهد از طریق دید سراسری زودتر تشخیص داده و همچنین تصمیمات بهتری گیرد. انعطاف‌پذیری ارائه‌شده توسط SDN نیز می‌تواند به‌طور مؤثر جهت اتصال اشیا در شبکه‌های ناهمگن مورد استفاده قرار بگیرد. در پژوهش حاضر، روش جدیدی را با استفاده از معیار آنتروپی و خصوصیات جریان ترافیک ورودی پیشنهاد کردیم و جزئیات مراحل و محاسبات را بیان نمودیم. این سیستم، مقیاس‌پذیری و انعطاف‌پذیری کاملی را در برابر توپولوژی شبکه دارد و قابل توسعه برای کنترل‌کننده‌های دیگر نیز است. همچنین نشان دادیم که شبکه‌های نرم‌افزاری تعریف‌شده، قابلیت بسیار بالایی را برای اجرا و توسعه برنامه‌های امنیتی دارا هستند. در دنیای واقعی می‌توان الگوریتم پیشنهادی را در سیستم‌هایی که مجهز به تکنولوژی SDN باشند، پیاده‌سازی کرد. به عنوان مثال، زمانی که تعداد



شکل ۱۳: مقایسه تأخیر در تشخیص حمله در روش پیشنهادی و روش‌های موجود.

زیادی از دستگاه‌های IoT داشته باشیم و حمله DoS رخ دهد، می‌توان الگوریتم پیشنهادی را اجرا کرد تا از وقوع حمله جلوگیری کنیم. از آنجا که استفاده از آمارهای جریان، سربار کنترل‌کننده را به میزان زیادی افزایش می‌دهد، در اینجا این آمار برخلاف اغلب روش‌های شناسایی موجود به‌صورت دوره‌ای جمع‌آوری نمی‌شود و فقط در صورت نیاز از سوئیچ‌ها درخواست می‌شود. به دلیل عدم استفاده از محاسبات پیچیده و پنجره زمانی کوچک، زمان تشخیص حمله به میزان قابل قبولی رسیده که خود، عاملی برای کاهش مقدار مثبت اشتباه و منفی اشتباه و در نتیجه افزایش دقت شده است.

مراجع

[1] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. on Computational Intelligence and Security,* pp. 663-667, Emeishan, China, 14-15 Dec. 2013.

[2] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, "IoT survey: an SDN and fog computing perspective," *Computer Networks*, vol. 143, pp. 221-246, Oct. 2018.

[3] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: a survey," *IEEE SDN for Future Networks and Services, SDN4FNS,* 7 pp., Trento, Italy, 11-13 Nov. 2013.

[4] J. Ren, H. Guo, C. Xu, and Y. Zhang, "Serving at the edge: a scalable IoT architecture based on transparent computing," *IEEE Network*, vol. 31, no. 5, pp. 96-105, 2017.

[5] K. S. Sahoo, B. Sahoo, and A. Panda, "A secured SDN framework for IoT," in *Proc. Int Conf. on Man and Machine Interfacing MAMI'15,* 4 pp., Bhubaneswar, India, 17-19 Dec. 2015.

[6] Y. Lu and M. Wang, "An easy defense mechanism against botnet-based DDoS flooding attack originated in SDN environment using sFlow," in *Proc. of the 11th Int. Conf. on Future Internet Technologies-CFI'16*, pp. 14-20, Nanjing, China, 15-17 Jun. 2016.

[7] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against software defined network controllers," *J. of Network and Systems Management*, vol. 26, no. 3, pp. 573-591, Jul. 2018.

[8] R. Neres Carvalho, J. Luiz Bordim, and E. Adilio Pelinson Alchieri, "Entropy-based DoS attack identification in SDN," in *Proc. IEEE Int. Parallel and Distributed Processing Symp. Workshops, IPDPSW'19,* pp. 627-634, Rio de Janeiro, Brazil, 20-24 May 2019.

[9] R. B. Shohani and S. A. Mostafavi, "Introducing a new linear regression based method for early DDoS attack detection in SDN," in *Proc. 6th Int. Conf. on Web Research, ICWR'10,* pp. 126-132, Tehran, Iran, 23-24 Apr. 2020.

[10] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdes, and F. Luna-Valero, "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: an experimental approach," *Sensors*, vol. 20, no. 3, Article ID: 816, 18 pp., Feb. 2020.

[11] L. Li, J. Zhou, and N. Xiao, "DDoS attack detection algorithms based on entropy computing," In: Qing, S., Imai, H., Wang, G. (eds) *Information and Communications Security. ICICS 2007.* Lecture Notes in Computer Science, vol 4861. Springer, Berlin, pp. 452-466, 2007.

[12] R. Wang, Z. Jia, and L. Ju, "An entropy-based distributed DDoS detection mechanism in software-defined networking," in *Proc. IEEE Trustcom/BigDataSE/ISPA,* pp. 310-317, Helsinki, Finland, 20-22 Aug. 2015.

[13] S. Oshima, T. Nakashima, and T. Sueyoshi, "Early DoS/DDoS detection method using short-term statistics," in *Proc. Int Conf. on Complex, Intelligent and Software Intensive Systems,* pp. 168-173, Krakow, Poland, 15-18 Feb. 2010.

[14] K. Muthamil Sudar and P. Deepalakshmi, "A two level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4.5 technique," *J. of High Speed Networks*, vol. 26, no. 1, pp. 55-76, Mar. 2020.

[15] R. L. S. de Oliveira, C. M. Schweitzer, A. A. Shinoda, and L. R. Prete, "Using mininet for emulation and prototyping software-defined networks," in *Proc. IEEE Colombian Conf. on Communications and Computing, COLCOM'14,* 6 pp., Bogota, Colombia, 4-6 Jun. 2014.

[16] C. S. Wright, *Searching for Exploits, SCAPY Fuzzing*, 11 pp., 31 Mar. 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3153525,

[17] M. A. Al-Adaileh, M. Anbar, Y. W. Chong, and A. Al-Ani, "Proposed statistical-based approach for detecting distribute denial of service against the controller of software defined network (SADDCS)," in *Proc. MATEC Web of Conf.*, vol. 218, Article ID: 02012, 8 pp., 26 Oct2018.

[18] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602-622, Firstquarter 2016.

فاطمه مطیع شیرازی مدرک کارشناسی خود را در سال ۱۳۹۶ از دانشگاه صنعتی شیراز در رشته مهندسی فناوری اطلاعات و مدرک کارشناسی ارشد خود را از دانشگاه یزد در سال ۱۴۰۰ در رشته مهندسی کامپیوتر– شبکه های کامپیوتری دریافت کرده است. زمینه‌های تحقیقاتی او شامل شبکه‌های نرم افزارمحور، اینترنت اشیا و امنیت شبکه و تشخیص حملات امنیتی روی شبکه های کامپیوتری است.

سید اکبر مصطفوی در سال ۱۳۸۷ مدرک کارشناسی خود را در رشته مهندسی فناوری اطلاعات از دانشگاه صنعتی شریف و به ترتیب در سال های ۱۳۸۹ و ۱۳۹۴ مدارک کارشناسی ارشد و دکتری خود را در رشته مهندسی فناوری اطلاعات از دانشگاه صنعتی امیرکبیر دریافت نمود. وی از سال ۱۳۹۴ تا کنون استادیار دانشکده مهندسی کامپیوتر دانشگاه یزد است. زمینه های تحقیقاتی مورد علاقه ایشان متنوع بوده و شامل موضوعات نو در حوزه طراحی شبکه های کامپیوتری، سیستم‌های توزیع شده و شبکه‌های بی‌سیم است.