

دانشکده مهندسی کامپیوتر

سمینار کارشناسی ارشد گرایش رایانش امن

عنوان:

|  |
| --- |
| ارائه رويكرد تطبیق‌پذير با تنوع ترافیكي شبكه‌هاي پهن‌باند براي شناسايي حملات منع‌خدمت توزيع‌شده  An Adaptive Approach with Variety Characteristic of High-Bandwidth Networks for Distributed Denial of Service Attacks Detection |
|  |

نگارش:

**روح‌الله جهان‌افروز**

**۴۰۰۲۱۰۷۵۵**

استاد راهنما:

**دکتر رسول جلیلی**

استاد ممتحن داخلی:

**دکتر امیرحسین جهانگیر**

**بهمن ۱۴۰۱**

چکیده**:**

**باتوجه به گسترش روز‌افزون شبکه‌های کامپیوتری و متداول‌شدن استفاده از آنها،‌ حجم تبادل اطلاعات نیز بالاتر رفته و امروزه نرخ‌گذر اطلاعات در بسیاری از تجهیزات شبکه به بیش از ۱۰۰ گیگابیت در ثانیه رسیده است. با توجه به گسترش شبکه‌ها پروتکل‌های مختلفی برای کاربردها و برنامه های مختلف ارایه شده است و علاوه بر آن بسیاری از برنامه‌های کاربردی امروزه با این که از پروتکل‌های استاندارد و مشهوری برای ارتباط با یکدیگر و تبادل اطلاعات در شبکه استفاده می‌کنند اما شیوه استفاده از این پروتکل‌ها در آنها متفاوت می‌باشد، به عنوان مثال برنامه‌های پیام‌رسان و مرورگر‌های وب از بسته‌های مبتنی بر پروتکل** HTTP **برای تبادل اطلاعات استفاده می‌کنند، با این تفاوت‌ که در برنامه‌های پیام‌رسان با ارسال تعداد معینی از بسته‌های** HTTP **در مقایسه با مرورگر‌های اینترنتی، نرخ متفاوتی از بسته‌ها را در پاسخ دریافت خواهیم کرد. لذا با ظهور برنامه‌های کاربردی مختلف شاهد بروز تنوع ترافیکی بر روی پروتکل‌های مختلف و رفتار‌های متفاوت در ترافیک شبکه هستیم. از طرفی حملات منع خدمت به‌عنوان یکی از متداول‌ترین و پرهزینه‌ترین حملات در سطح شبکه شناخته می‌شود که موجب بروز اختلال در ارائه خدمات سطح سازمانی و حتی ملی شده است.** یکی از اساسی‌ترین نیاز‌های امنیتی در سطح شبکه بحث دسترس‌پذیر بودن کامل شبکه می‌باشد**. حملات منع خدمت به‌عنوان تهدیدی جدی برای قابلیت دسترس‌پذیری این‌گونه شبکه‌ها شناخته می‌شود. لذا، مقابله با حملات منع خدمت در این شبکه‌ها، به یک بستر مهم تحقیقاتی در سال‌های اخیر تبدیل‌شده‌ است.**

**با افزایش نرخ ترافیک، چالش‌های امنیتی نظیر تشخیص حملات‌ منع ‌خدمت، که به دلیل سادگی در پیاده‌سازی و تاثیر بسیار‌مخرب یک تهدید جدی به حساب می‌آیند، افزایش پیداکرده‌است. سیستم‌های تشخیص‌ نفوذ در ترافیک‌هایی با نرخ‌گذردهی بالا به‌ خاطر لزوم استفاده از تعداد زیادی خط قوانین مبتنی بر امضا، نمی‌توانند ترافیک را پایش و حملات را در لحظه تشخیص دهند. بدین خاطر که با افزایش تعداد آدرس‌های مبدا، تعداد خطوط قوانین نیز افزایش خواهد یافت. در دهه‌های گذشته محققان روش‌های شناسایی بسیاری را برای حملات منع خدمت توزیع‌شده پیشنهاد کرده‌اند. عدم تطبیق پذیری و مقیاس‌پذیری برای استفاده در شبکه‌های پهن‌باند، از متداول‌ترین مشکلات این روش‌ها هستند. به لذا برای شناسایی صحیح حملات منع ‌خدمت در شبکه‌های پهن‌باند نیاز به یک رویکردی است که شامل دو ویژگی پردازش جامع به معنای پردازش تمامی بسته‌ها و تطبیق‌پذیری به معنای قابلیت تطبیق‌پذیری با تنوع ترافیکی باشد.**

**در این پژوهش ضمن بررسی کارهای مشابه صورت گرفته در این زمینه، قصد‌ داریم رویکردی تطبیق‌پذیر با تنوع ترافیکی موجود ‌در شبکه‌های پهن‌باند برای شناسایی حملات منع ‌خدمت توزیع‌شده معرفی نماییم علاوه بر آن دو‌ ویژگی پردازش جامع و سازگارپذیری برخوردار باشد. روش ما جریان‌ها را بر اساس اینکه برای کدام اپلیکیشن می‌باشند دسته بندی کرده و به کمک رفتار عادی ترافیک هر برنامه کاربردی، ترافیک‌ها متخاصم هر اپلیکیشن را تشخیص می‌دهد. به دلیل اینکه از الگوریتمها و داده ساختارهای مبتنی بر اسکچ استفاده می‌کنیم،سرعت بالا و استفاده بهینه از حافظه را تضمین می‌کنیم. همچنین در روش پیشنهادی از** DPDK **استفاده می‌کنیم که سرعت پردازش بسته‌ها را به طرز چشمگیری بهبود می‌بخشد. کارایی روش ارائه شده را نیز در مقایسه با برخی دیگر از راهکارهای ارایه شده در سالیان اخیر و با ‌درنظرگرفتن معیارهایی نظیر میزان استفاده از پردازشگر و حافظه، نرخ دورانداختن بسته‌ها، و میزان تاخیر در شناسایی حملات بررسی می‌کنیم.**

**کلیدواژه:** حملات منع خدمت توزیع‌شده، شبکه‌های پهن باند، تطبیق پذیری با تنوع ترافیکی، DPDK، سامانه‌های تشخیص نفوذ

**۱ سرآغاز**

امروزه با افزایش حجم تبادلات داده‌ای در بستر اینترنت، برقراریِ ارتباطی امن و پایدار در سطح شبکه به یکی از چالش‌های اساسی پیش روی هر سازمانی تبدیل شده است. با توجه به رشد روزافزون کاربران شبکه‌های کامپیوتری، حجم درخواست‌های آن‌ها بزرگ‌تر و پیچیده‌تر می‌شود. از طرف دیگر امروزه اینترنت به جزء جدایی‌ناپذیری در زندگی و تعاملات کاربران تبدیل شده و بحث دسترس‌پذیری[[1]](#endnote-2) آسان به خدمات بستر اینترنت بیش ‌از پیش مورد توجه قرار می‌گیرد، بدین معنا که ارائه‌دهندگان خدمات ارتباطی [[2]](#endnote-3)موظف هستند خدمات خود را به‌صورت شبانه‌روزی و بدون اختلال و وقفه در اختیار کارخواهان قرار دهند. درصورتی‌که این سازمان‌ها به هر دلیلی در ارائه خدمت دچار مشکل شوند و نتوانند به نحو مطلوب خدمت موردنظر خود را ارائه دهند با چالش‌های جدی از قبیل از بین رفتن اعتماد مشتریان، خسارات سنگین مالی و ازبین رفتن اعتبار سازمان مواجه می‌شوند .[1]

حملات منع خدمت[[3]](#endnote-4)، دسته‌ای از حملات در شبکه هستند که با هدف از بین بردن دسترس‌پذیری شبکه سعی در ممانعت از انجام یک خدمت در شبکه دارند. حملات منع خدمت پهنای باند یا ظرفیت لینک شبکه‌ را مصرف کرده یا باعث از کار افتادن و اختلال عملکرد در یک سرور یا هر دستگاه حیاتی دیگر در شبکه خواهند شد.گونه‌های مختلفی از این حملات وجود دارد که هرکدام به طریقی سعی می‌کنند دسترس‌پذیری شبکه را هدف قرار داده و یا با مصرف منابع خدمت‌دهنده، مانع از ارائه خدمت به‌صورت کامل و باکیفیت به کاربران قانونی شوند. حملات منع خدمت توزیع‌شده [[4]](#endnote-5)یک‌گونه مخرب‌تر از حملات منع خدمت هستند که در آن‌ها حمله‌کننده[[5]](#endnote-6) از طریق بات[[6]](#endnote-7)‌ها و سامانه‌[[7]](#endnote-8)هایی که تحت کنترل خود دارد حمله را انجام می‌دهند. بدین ترتیب علاوه بر حجم ترافیک سنگین‌ حملات و دشواری‌های ایجاد تمایز بین ترافیک قانونی شبکه و ترافیک حمله‌کننده(flash crowd)، پیدا کردن حمله‌کننده اصلی نیز به‌مراتب دشوارتر می‌شود. از طرفی با گسترش و فراگیری استفاده از اینترنت و انتشار ابزارهای مختلف برای اجرای این حملات و در نظر داشتن این نکته که با افزایش دستگاه های اینترنت اشیا و کمرنگ بودن و آسیپ پذیر بودن این دستگاه ها در برابر حملات و به تبع استفاده از این دستگاه ها به عنوان مجریان حملات منع خدمت توزیع شده، اجرای این حملات آسان‌تر و فراگیر‌تر شده است.

از طرفی امروزه با شبکه های پهن باند مواجه هستیم که در آن‌ها نرخ گذر اطلاعات به بیشترین حد ممکن رسیده و همچنین به دلیل ظهور پروتکل‌ها و اپلیکیشن‌های مختلف با حجم زیادی از داده‌ها و تنوع زیادی از پروتکلها مواجه هستیم. شناسایی و جلوگیری از حملات منع خدمت در این شبکه ها با چالش‌های جدی همراه می‌باشد. با‌‌ توجه به مخرب بودن این حملات پژوهش‌های فراوانی به‌منظور تشخیص و جلوگیری از وقوع آن‌ها انجام‌شده و روش‌های مختلفی در این زمینه ارائه‌شده است. با این‌حال، هم چنان این حملات یکی از تهدید‌های بزرگ در شبکه‌های پهن‌باند محسوب می‌شوند که راه حلی چندان مطلوبی برای آنها ارایه نشده است.

این گزارش در ۵ بخش تدوین‌شده است. در بخش ۲ مفاهیم پایه موردنیاز در این پژوهش‌ معرفی می‌شوند. ابتدا شبکه‌های پهن باند و ویژگی‌های آن بیان می‌شود. سپس انواع حملات منع خدمت، از نقطه‌نظرهای مختلف موردبررسی قرار می‌گیرند و در انتهای این بخش مفهوم دیتا استرینیمتگ و اسکچ‌ها توضیح داده می‌شود. در بخش ۳ به بررسی کار‌های پیشین انجام‌شده برای تشخیص حملات منع خدمت توزیع شده پرداخته می‌شود. در بخش ۴ روش پیشنهادی به‌منظور بهبود تشخیص حمله در شبکه‌های پهن باند بیان می‌شود و سرانجام در بخش ۵ نتیجه‌گیری، مراحل انجام پروژه و زمان‌بندی آن را بیان خواهد شد.

**۲ مفاهیم پایه**

2**.**1 **مقدمه**

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

2.1.1 **شبکه‌های پهن‌باند**

امروزه نرخ تبادل اطلاعات در شبکه‌های کامپیوتری بالا رفته و اصطلاحاً با شبکه‌های پهن‌باند مواجه هستیم. شبکه‌های پهن‌باند دارای سه ویژگی می‌باشند:

* سرعت بالا: داده‌ها و بسته‌ها با سرعت و فرکانس بالایی تولید می‌شوند.
* حجم بالا:‌ اطلاعات عبوری از شبکه و درحال تبادل بسیار حجیم می‌باشند. به عبارتی دیگر بسته‌هایی با پیلود‌ها و حجم زیادی از سرایند‌ها را خواهیم داشت.
* تنوع داشتن:علاوه بر ظهور پروتکل‌های مختلف که هر کدام برای کاربردی خاص می‌باشند، نحوه انتقال و دریافت بسته ها بین کلاینت-سرور و استفاده از این پروتکل‌ها بسته به وضعیت و کاربرد می‌تواند انواع مختلفی داشته باشد.

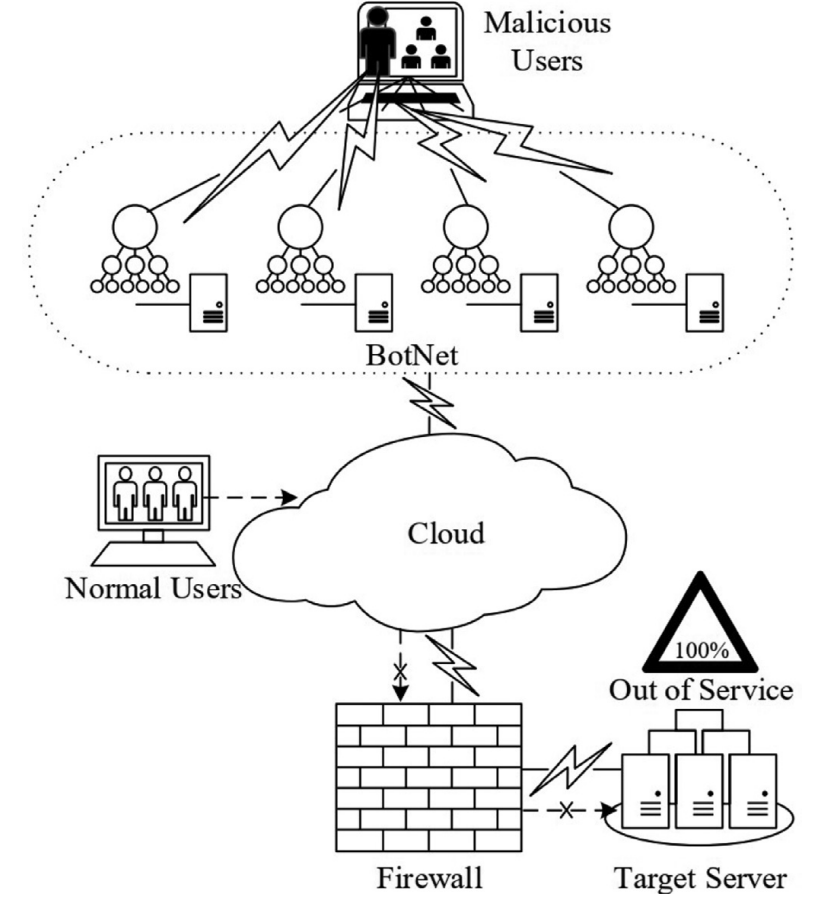
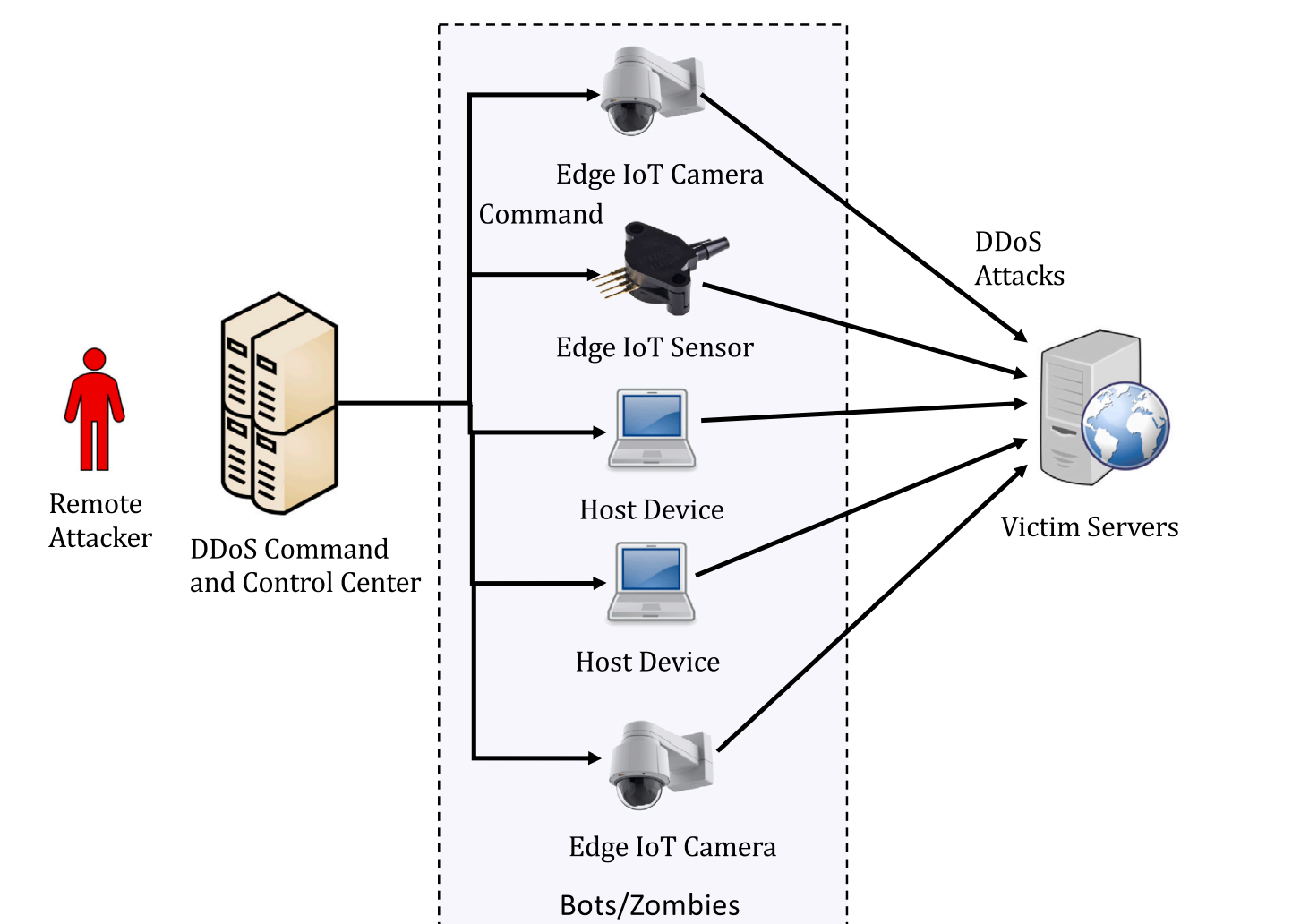
باتوجه‌ به ویژگی‌های ذکر شده،

2.2 **حملات منع خدمت و حملات منع خدمت توزیع شده**

به مجموعه حملاتی که با هدف ممانعت از انجام یک خدمت صورت می‌پذیرند، حملات منع خدمت گفته می‌شود. این حملات با انگیزه‌های مختلفی نظیر ایجاد اختلال یا ممانعت از ارائه یک خدمت، از بین بردن اعتبار و مقبولیت یک سازمان، آسیب زدن مالی و هدر دادن منابع یک سازمان، دستاوردهای سیاسی و ملی، انگیزه مالی و یا قدرت‌نمایی مهاجمین و مواردی از این دست می‌تواند صورت پذیرد.

هدف اصلی در حملات منع خدمت هدفشان تولید ازدحام و اختلال مصرف منابع پردازشی سیستم (پردازشگر سیستم) یا منابع شبکه (پهنای باند) می‌باشد.

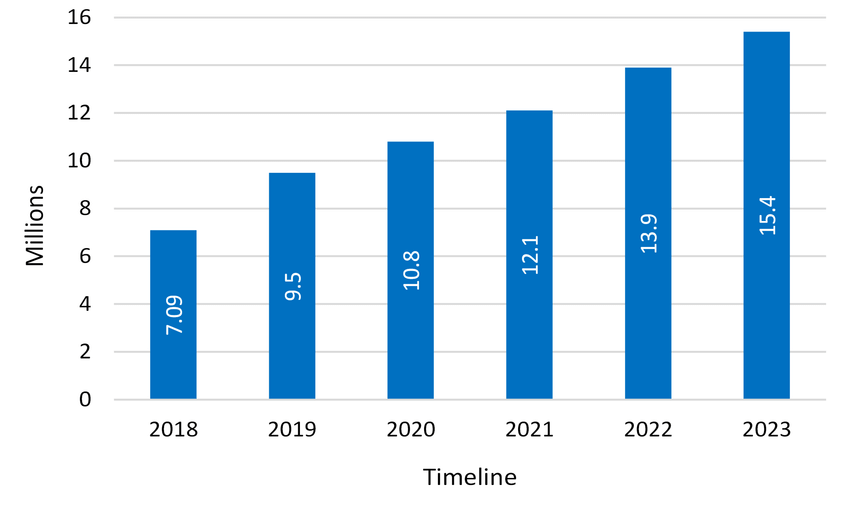
حملات منع خدمت توزیع شده گونه خطرناک‌تر از این حملات می‌باشند که در آن مزاحم ابتدا با اسکن آسیب پذیری های دستگاه های مختلف موجود در شبکه اینترنت شروع به به خطر انداختن ماشین های عامل متعددی می کند که ممکن در سطح جغرافیایی گسترده‌ای توزیع یافته باشند. هنگامی که یک نفوذگر با موفقیت برخی از آسیب پذیری های این سیستم‌ها را شناسایی کرد، می تواند این ماشین ها را با استفاده از یک برنامه مخرب مانند اسب تروجان به خطر بیاندازد. بدین صورت که با تکثیر فایل مخرب در چندین ماشین عامل، مزاحم توانایی کنترل بسیاری از دستگاه‌ها را دارد که می‌توانند به چندین هزار یا میلیون‌ها (که معمولاً به آنها ربات گفته می‌شود) برسند تا بدون اطلاع صاحب قانونی دستگاه، حملات منع‌ خدمت توزیع شده را آغاز کنند. کشف آسیب‌پذیری‌ها و فرآیند بهره‌برداری از عوامل معمولاً به‌طور خودکار انجام می‌شود، به عنوان مثال، با ارسال پیام‌های ایمیل با پیوست کد حمله. گروه‌هایی از ربات‌ها، که به عنوان بات‌نت شناخته می‌شوند، می‌توانند از راه دور از یک نفوذگر یعنی استاد ربات سفارش‌ها را دریافت کنند. ربات-مستر می تواند حملات DDoS در مقیاس بزرگ را انجام دهد تا یک سرویس یا شبکه قانونی را با ارسال یک فرمان کنترلی به عوامل بات نت برای ایجاد ترافیک بی فایده بدون توجه به یک سرویس یا شبکه قانونی انجام دهد. در نتیجه، در مدت زمان کوتاهی حجم زیادی از ترافیک را به سمت سرور و منابع آن هدایت می‌کنند که به طور قابل توجهی سرویس دهی آن یا رویکرد شبکه را برای پاسخگویی به کاربران قانونی با اختلال مواجه می کند. بدین صورت رهگیری مبدا حمله دشوارتر و همچنین ترافیک ایجاد شده در اثر حمله بزرگتر و مخرب‌تر می‌باشد.

در سال‌های اخیر، تعداد دستگاه‌های IoT که به نسبت تجهیزات شبکه سنتی آسیب پذیرتر هستند به سرعت در حال افزایش می‌باشد[[8]](#footnote-2). شبکه‌های بات تشکیل شده از این دستگاه‌های IoT مقیاس حملات DDoS را به میزان قابل توجهی گسترش می دهد. در سال 2016، Dyn ارائه‌دهنده سرویس DNS توسط دستگاه‌های IoT عظیم تحت کنترل Mirai Botnet مورد حمله قرار گرفت که درنهایت منجر به غیرقابل دسترس بودن منطقه وسیعی از خدمات(توییتر، اسپاتیفای، نتفلیکس، سی ان ان و...) در سواحل شرقی ایالات متحده شد. مشکل دیگر در دفاع در برابر حملات DDoS، بروز حملات تقویت بازتاب است. در سال 2018، GitHub با استفاده از آسیب‌پذیری پروتکل Memcached، با انعکاس چند برابر از 50000 بار و ترافیک پیک 1.35 ترابیت بر ثانیه، مورد حمله یک حمله DDoS تقویت بازتابی قرار گرفت. در فوریه 2020، ارایه دهندگان خدمات وب آمازون حمله ای با حجم پیک 2.3 ترابایت بر ثانیه را تجربه کرند. در ژوئیه 2021، شرکت ارایه دهنده خدمات تحویل محتوای Cloudflare در گزارشی به محافظت از یکی از مشتریان خود در برابر حمله DDoS نشات گرفته از یک شبکه بات نت در ابعاد جهانی Mirai با ترافیک پیک 17.2 میلیون درخواست در ثانیه، اشاره کرد. یاندکس، ارائه‌دهنده خدمات پیشگیری از DDoS روسیه گفت که در تاریخ 5 سپتامبر 2021 یک حمله DDoS خط لوله HTTP را که از تجهیزات شبکه Mikrotik وصله‌نشده سرچشمه می‌گرفت، مسدود کرده است.[Wikipedia]

طبق خلاصه سالانه حملات منع خدمت توزیع شده در Akamai در سال 2020، تعداد حملات DDoS در مقیاس بزرگ به طور قابل توجهی افزایش یافته است. در بزرگترین رویداد حمله DDoS، ترافیک حمله به 1.44 ترابیت در ثانیه رسیده است ولذا با چالش جدی مواجه هستیم.

در حال حاضر، بردارهای حمله جدید به طور مداوم در حال استخراج هستند. به عنوان مثال، در پایان ژوئیه 2020، FBI هشداری صادر کرد مبنی بر اینکه CoAP، WS-DDARMS و سایر پروتکل‌ها ممکن است برای انجام حملات DDoS مورد استفاده قرار گیرند. حملات DDoS بر اساس بردارهای حمله جدید ممکن است تغییرات زیادی در ویژگی های آماری مانند سرعت بسته ها و فاصله بسته های مورد استفاده در روش های سنتی داشته باشند، که باعث می شود روش های سنتی کمتر با حملات مختلف سازگار شوند.



https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

2.2.1 **رویه کلی حملات منع خدمت توزیع‌شده**

باوجوداینکه گونه‌های متفاوتی از حملات منع خدمت توزیع‌شده وجود دارد که هرکدام با روشی منحصربه‌فرد حمله را انجام می‌دهند، می‌توان در یک دید کلی و مجرد چهار مؤلفه اصلی برای انجام یک حمله منع خدمت توزیع‌شده در نظر گرفت. این چهار مؤلفه عبارت‌اند از: حمله‌کننده[[9]](#endnote-9) اصلی، کنترل‌کننده حمله، عامل‌[[10]](#endnote-10)ها و قربانی[[11]](#endnote-11). حمله‌کننده اصلی خود می‌تواند کنترل‌کننده حمله باشد و یا کنترل حمله را به یک سیستم آلوده‌شده توسط حمله‌کننده بسپارد. به‌طورکلی رویه حملات منع خدمت به این صورت است که تعدادی کامپیوتر که با روش‌های مختلف تحت کنترل حمله‌کننده قرار دارند بعد از صادر شدن دستور حمله، شروع به ارسال بسته به سمت سیستم قربانی می‌کنند[14].

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

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

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

2.2.3 **دسته‌بندی حملات منع خدمت توزیع‌شده**

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

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

حملات منع خدمت را می‌توان به سه دسته زیر تقسیم کرد:

* حملات حجیم: هدف مهاجم این است که پهنای باند قربانی (بیت بر ثانیه) را بیش از حد افزایش یابد. برخی از گونه‌های متداول آن UDP flood هدف آن اشباع پورت‌های تصادفی سرور مقصد با ارسال بسته‌های UDP می‌باشد و سرور مجبور می‌شود با ارسال بسته‌های ICMP پاسخ دهد و ICMP flood که قربانی با ارسال پیغام‌های بی وقفه ICMP echo request-ping بدون منتظر ماندن برای پاسخ روانه می‌کند، می‌باشند
* حملات پروتکل: با معیار پکت بر ثانیه اندازه گرفته می‌شود. از منابع سرور یا زیرساخت میانی مثل دیوارهای آتش و پکت فیلتر‌ها بهره می‌برد. Syn Flood یکی از این نوع حملات می‌باشد که از ویژگی دستدادن سه گانه TCP استفاده می‌کند و بسته‌های SYN بسیاری به سمت سرور ارسال می‌کند که می‌تواند آدرس آنها جعلی باشد، و هنگامی که سرور پاسخ Syn-Ack داد در قبالش ACK نمی‌فرستد و لذا آن استیت باز می‌ماند و باعث هدر رفت منابع می‌شود. نوع دیگر این حملات با استفاده از ساخت پکت‌های جعلی توسط مهاجم اجرا می‌شوند. حداکثر حجم بسته قابل قبول در لایه آی‌پی، ۶۵۵۳۵ می‌باشد اما حداکثر بسته قابل قبول در لایه لینک، ۱۵۰۰ بایت می‌باشد. لذا بسته رسیده از آی‌پی بایستی به بخش‌های کوچک تری قرگممت شود و در مقصد دوباره سرهم شوند. Ping of Death حمله‌ای است. که در آن بسته ای با حجم بیش از ۶۵۵۳۵ به گیرنده ارسال می‌شود و لذا باعث از کار افتادن او می‌شود.
* حملات برنامه کاربردی: هدفشان نابودی وب سرور با ارسال درخواستهایی با ضاهر معمولی و نا متخاصم متدوال (بسته بر ثانیه) می‌باشد. حملات کند و دستکاری شده، سیل‌آسای GET، حملات به سمت ویندوز،آپاچی و اوپن بی اس دی می‌باشد. Slowloris که در آن مهاجم تعداد کثیری کانکشن همزمان به سرور نگه می‌داردو این کار را با ارسال تنها بخشی از کویری درخواست انجام می‌دهد. تقویت NTP که در آن به کمک یک سرور NTP بسته‌های UDP کثیری به سمت قربانی ارسال می‌کند. سیل آسای hTTP که بسته‌هایی با متود bet/POST ارسال می‌کنداز حملات متداول این دسته هستند.
* حملات روز صفر: استفاده از آسیب پذیری‌هایی که تا به حال راهی برای برای رفع آنها ارایه نشده استو

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

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

1. حملات سیل‌آسا[[12]](#endnote-12): در این دسته از حملات مهاجم قصد دارد تا با ارسال بسته‌های زیاد در سطح شبکه سعی در اشباع کردن پهنای باند قربانی دارد تا قربانی را از دریافت خدمت در شبکه منع کند.

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

3. حملات سیل‌آسا مبتنی بر بازتاب[[13]](#endnote-13): این نوع حمله، حمله‌کننده قربانی را به جای خود معرفی می‌کند و درخواستی را به کارپذیر ارسال می‌کند و کارپذیر این درخواست را به صورت همه‌پخشی به تمامی میزبان‌های موجود ارسال می‌کند و پاسخ از جانب میزبان‌ها به قربانی ارسال می‌شود. پروتکل درخواست و پاسخ در این حمله مشابه هستند و حجم بسته ارسالی به قربانی به تعداد میزبان‌های موجود در شبکه بستگی دارد.

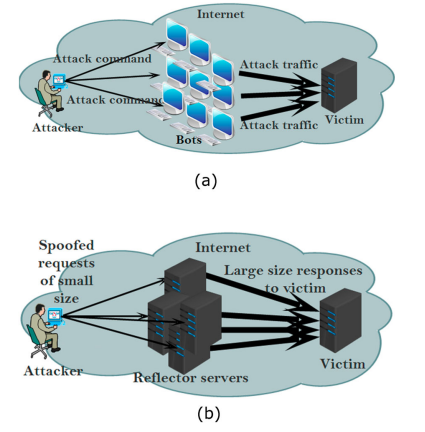
4. حملات سیل‌آسا مبتنی بر تقویت[[14]](#endnote-14): در این نوع حملات مهاجم با جعل آدرس قربانی و معرفی کردن قربانی به جای خود درخواستی با طول کوتاه و پاسخ بلند را از کارپذیرهای موجود درخواست می‌کند و این پاسخ توسط کارپذیر به قربانی ارسال می‌شود. در این حمله پروتکل درخواست و پاسخ متفاوت است و اندازه حمله به طول و تعداد پاسخ‌هایی که به سمت قربانی ارسال می‌شوند بستگی دارد.

* حملات موجود در لایه برنامه‌کاربردی: در این دسته از حملات، حمله‌کننده سعی دارد تا حمله را به کمک پروتکل‌های موجود در لایه کاربردی و با اتصالی مشابه اتصال کاربران قانونی انجام دهد. این حملات تلاش می‌کنند تا با مصرف منابع قربانی نظیر پردازنده، حافظه، دیسک سخت و مواردی از این قبیل در ارائه خدمت توسط قربانی اختلال ایجاد کنند و به مراتب پهنای باند کم‌تری نسبت به حملات لایه شبکه/انتقال مصرف می‌کنند. ازآنجایی‌که ترافیک حمله سعی دارد مشابه ترافیک کاربران قانونی باشد، ایجاد تمایز بین ترافیک حمله‌کننده و ترافیک معمولی از چالش‌های جدی در تشخیص این‌گونه حملات خواهد بود. این حملات به دو دسته‌ی حملات سیل‌آسا مبتنی بر تقویت/بازتاب و حملات سیل‌آسا اِچ‌.تی.‌تی.‌پی[[15]](#endnote-15) تقسیم می‌شوند.

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

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

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



2.3 **دیتا استریمینگ**

همانطور که در ویژگی‌های شبکه‌های پهن باند ذکر کردیم، نرخ بی وقفه تولید اطلاعات یکی از شاخصه‌های این شبکه‌ها می‌باشد. برای پردازش بسته‌ها در این حالت،‌ دو رویکرد متفاوت وجود دارد:

* Batch processing: در این رویکرد تمامی بسته‌ها در یک پنجره زمانی را ضبط کرده و سپس آن ها را در زمان‌های بعدی پردازش کرده. مشکل این روش این می‌باشد که به دلیل ذخیره اطلاعات در ابتدا و سپس ارسال آن به مراکز دیگر، دارای تاخیر ارسال و پردازش و هزینه بسیار زیادی (برای ذخیره سازی) می‌باشد.
* Stream processing: اکثر راهکارهای ارایه شده که در قسمت بعدی بررسی می‌کنیم، مبتنی بر این رویکرد می‌باشند. این الگوریتم ها دو محدودیت زیر را درنظر می‌گیرند: اول این که اطلاعات به صورت استریمی از داده ها ( بی وقفه و با سرعت بالا) در حال ارسال می‌باشند و دوم اینکه از نظر زمانی و حافظه با محدودیت روبرو هستیم. این خصیصه‌ها همان چالشهایی هستند که ما در شبکه‌های پهن باند با آن طرف هستیم. برای تشخیص حملات در این شبکه‌ها ما بایستی تمامی بسته‌ها را ضبط و پردازش کرده و این کار را باید با همان سرعت ورود اطلاعات و با کمترین میزان استفاده از حافظه انجام دهیم. الگوریتم‌های دیتا استریمینگ در بحث پردازش اطلاعات بسیار کاربردی هستند الگوریتم های مبتنی بر دیتااستریمینگ، ابتدا مسیله را به یکی از چندین روش مدل می‌کنند. یکی از این مدل‌های بسیار محبوب turnstile می‌باشد. در این مدل یک دیتا استریم ورودی به نام I درنظر می‌گیریم که شامل مجموعه‌ای از تاپل‌های دوتایی می‌باشد:

I= α1, α2, α3, α4,…

А αi={( a1, v1)| a1£{0,1,…,u-1}, v1ƐR}

[u]= key space

این تاپل‌ها، دوتایی‌هایی می‌باشند که شامل مقدار کلید و آپدیت می‌باشند. یک آرایه ای به نام A داریم که تعداد خان‌های آن برابر [u] و دارای مقادیر متناظر آپدیت هر کلید می‌باشد. هرگاه یک تاپل جدید( ax, vx) بیاد مقدار آپدیت آن با مقدار A[ax] جمع می‌شود:

A[ax] += vx

این پارامتر‌ها را بسته به مساله دیتااستریمی که داریم، می‌توانند متفاوت باشند. در بحث پردازش بسته‌‌های دریافتی شبکه، استریم همان جریان وردی، تاپل‌ها همان بسته‌ها می‌باشند که مثلن کلیدشان همان ۵ خصیصه و پدیت نیز سایز بسته باشد. و برای شناسایی حملات منع خدمت، ما بایستی آدرس‌هایی که بتسه های با حجم نامتعارف می‌فرستند را شناسایی کنیم.

و در بحث دیتا استریمینگ ما به دنبال چندین نوع جواب می‌توانیم باشیم، که پس از این که مسیله را مدل کردیم ، می‌توانیم الگوریتم‌هایی ارایه دهیم که بر مبنای آن مدل سعی در یافتن جواب‌ها دارند. چند نمونه از این مسایل در ذیل ارایه شده است:

* + Heavy hitterها:
  + Momentها:

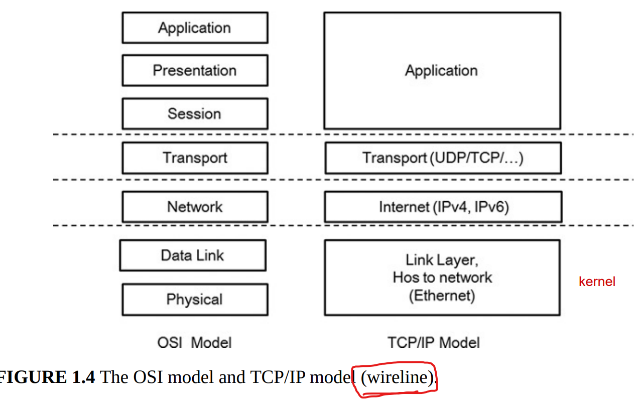
**اسکچ‌ها ( نمونه‌برداری)**

برای حل مسایل دیتا استریمینگ، راه های متفاوتی وجود دارد. یکی از راهکارها این می‌باشد که چون با حجم زیادی از اطلاعات روبرو هستیم، تنها بخشی از داده‌های ورودی را به عنوان نمونه انتخاب کرده و همان‌ها را پردازش کنیم(نمونه برداری). این رویکرد دقت پایینی خواهد داشت.پس ما لازم داریم که تمامی داده‌ها را بررسی کنیم. اما بررسی همه آنها نیز نیازمند حجم زیادی از منابع پردازشی و زمان می‌باشد.برای حل این مشکل، الگوریتم‌های به نام اسکچ ارایه شدند که از یک داده ساختار فشرده برای ذخیره سازی اطلاعات داده‌های ورودی استفاده می‌کنند. انواع مختلفی از این الگوریتم‌ها در پژوهش‌های مختلف ارایه شده است که هر کدام سعی در حل یکی از انواع خواسته‌های مسایل دیتااستریمینگ می‌باشند. در ذیل چند مورد از پر استفاده ترین آنها را بررسی خواهیم کرد:

* Count-Sketch: از یک جدول KxH تشکیل شده است که شامل K تا تابع هش می‌باشد. این ساختار را الگوریتم‌های اسکچ دیگر نیز استفاده می‌کنند. چون از توابع هش استفاده می‌کند لذا امکان تصادم وجود خواهد داشت و به همین دلیل تخمین میزند و به آنها داده ‌ساختارهای آماری احتمالاتی گویند. و یکی از ویژگی‌هایشان باید این باشد که نرخ خطای قابل قبولی و کرانداری ارایه دهند. از این الگوریتم در مسایل heavy hitter استفاده می‌شود.
* Count-Min Sketch
* Hetegronous
* Universal Sketch: اینها یک دسته جدید از اسکچ‌ها می‌باشند که سعی می‌کنند داده ساختاری ارایه دهند که برای حل تمامی انواع مسایل دیتااستریمینگ قابل استفاده باشد. در ذیل چند مورد از اینها را بررسی می‌کنیم:
  + Univmon

**DPDK و تفاوت با XDP**

هنگامی که یک بسته از طریق درگاه‌های یک سیستم دریافت می‌شود تا پردازش آن، مراحل مختلفی را طی خواهد کرد. بسته‌ها بر اساس کاربرد می‌توانند مراحل مختلفی را طی کنند از دریافت بسته تا پردازش بخش‌های مختلف ان و سپس ارسال آن در صورت نیاز بر مبنای معماری پشته TCP/IP می‌باشد که تمامی کرنل‌های سیستم‌عامل لینوکس از آن استفاده می‌کنند و همچنین بنا به کاربرد بایستی از لایه‌ها و دستگاه‌های مختلفی عبور داده شوند:

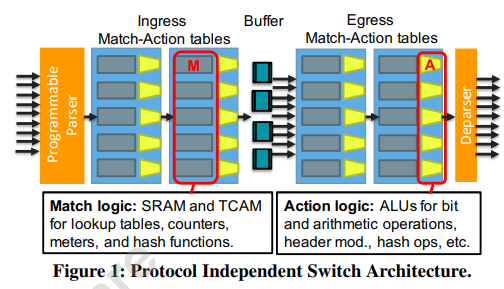
* بسته توسط کارت شبکه دریافت می‌شود (وقفه NIC)
* NIC از طریق DMA، بسته را در فضای حافظه در یک بافری قرار می‌دهد
* NIC یک سیگنال به پردازنده می‌دهد، و آن را برای پردازش بسته بیدار می‌کند(وقفه نرم افزاری)
* پردازنده اطلاعات مورد نیازش را خوانده و در صورت نیاز در بافر تعیین شده می‌نویسد.
* در صورت نیاز، بسته برای پردازش‌های بیشتر به استک پروتکلی کرنل برای انجام پردازش‌‌های پروتکلی مختلف (مثل بررسی آدرس‌ آی‌پی برای مقایسه آن با کنترل دسترسی تعریف شده) فرستاده می‌شود
* در نهایت اگر برنامه کاربردی در سطح کاربر باشد، پیلود بسته از فضای کرنل به فضای کاربر انتقال داده خواهد شد. در غیر اینصورت، بسته در همان فضای کرنل خواهد ماند

تمامی این مراحل بایستی در سطح کرنل انجام شده ولی پردازش بسته توسط کاربر در لایه اپلیکیشن صورت می‌گیرد. همانطور که مشاهده می‌شود این مراحل به دلیل وقفه‌هایی که انجام می‌شود، سربار زیادی خواهند داشت و در شبکه‌های پهن‌باند که با حجم زیادی از بسته‌ها مواجه هستیم، باعث اتلاف وقت زیادی خواهند شد.

DPDK یکی از راه های حل این مشکل می‌باشد، یک ابزار نرم افزاری می‌باشد که در سال ۲۰۰۹ توسط اینتل توسعه داده شد. اما بعدها به صورت یک پروژه متن باز درآمد. به طور خلاصه یک ابزار دورزدن کرنل در هنگام دریافت بسته در شبکه‌ می‌باشد که وقفه‌های مربوط به کرنل را حذف می‌کند و تمام عملیات را در سطح کاربر انجام میدهد و لذا عملیات دریافت و پردازش بسته را بسیار تسریع می‌بخشد. هدف این تکنولوژی استفاده از قابلیت پردازش چند هسته همان پردازنده‌های معمولی X86 برای بهبود سرعت پردازشی سرورها استفاده می‌کند. بدین صورت ما نرخ پردازشی نزدیک به هنگام استفاده از پردازنده‌های مخصوص سرور‌ها و یا بردهای مخصوص ASIC و FPGA با صرف هزینه‌ای بسیار کمتر خواهیم داشت. از چندین پردازنده برای بحث data-plane processing و از بقیه هسته‌ها برای امور کنترلی و سرویس‌های دیگر استفااده می‌کند. به صورت جزیی تر یعنی اینکه که چندین صف بر روی هر پورت تعریف می‌کند و هسته ها به صورت polling به این صفها الصاق می‌شوند. از این ابزار در کاربردهای مختلفی در جاهایی که حجم زیادی از ورودی/خروجی داریم از حیطه شبکه و امینت آن، پردازش و سوییچینگ ابرها، بهبود کارایی حافظه‌ها، NFVها،مخابرات و تلکام و..... استفاده می‌شود. البته به غیر از مورد اشاره شده که ویژگی اصلی این ابزار می‌باشد، امکانات مختلف دیگری مثل رمزگذاری و فشرده سازی .. به کمک رابطهای برنامه نویسی اش نیز ارایه می‌دهد.

XDP-eXpress Data Path

**سوییچ‌های برنامه‌پذیر:**

یکی از مشکلات روش‌های پیشین استفاده از یک کنترلر به عنوان مرکزی که تمام اطلاعات به آن فرستاده می‌شود و سپس در آنجا بر مبنای الگوریتم پیاده شده بر روی آن، تصمیم می‌گیرد که جلوی ترافیک را بگیرد یا نه. این روش تاخیر زیادی داشت و همچنین می‌تواند یک نقطه آسیب پذیر واحد برای مهاجمین فراهم کند. اما امروزه با معرفی سوییچ‌های برنامه پذیر، سوییچ‌های معمولی نیز با استفاده از برنامه‌هایی که بر روی آنها با استفاده از زبانهایی مثل p4 می‌نویسیم توانایی پردازش داده را تاحد زیادی خواهند داشت.

3 **کارهای ‌پیشین**

**با توجه به اهمیت موضوع حملات منع خدمت توزیع‌شده، در سال‌های گذشته پژوهش‌های بسیاری در این زمینه صورت گرفته است.** شبکه‌های نرم‌افزار محور و قابلیت‌هایی که این نوع شبکه‌ها ارائه می‌دهند به پژوهشگران حوزه تشخیص و مقابله با حملات منع خدمت کمک شایانی می‌کند تا با استفاده از ویژگی‌های موجود در این نوع شبکه‌ها، تشخیص و مقابله حملات منع خدمت را سریع‌تر و با دقت بالاتری انجام دهند. **به‌طورکلی پژوهش‌های انجام‌شده در حوزه حملات منع خدمت توزیع‌شده را می‌توان در سه دسته پیشگیری از وقوع حمله، تشخیص حمله و کاهش اثر حمله تقسیم‌بندی کرد. از آنجایی‌که تمرکز این گزارش بر مقالات حوزه تشخیص حملات منع خدمت توزیع‌شده می‌باشد،** در ادامه به معرفی چند روش پرکاربرد دسته تشخیص حملات منع خدمت توزیع‌شده در شبکه‌های کامپیوتری می‎‌پردازیم. باید توجه داشت که علاوه بر گروه‌بندی ارایه شده در ذیل، الگوریتم‌های تشخیص را می‌توان بر اساس اینکه‌ در کدام قسمت سعی به تشخیص متخاصم دارند نیز طبقه بندی کرد که شامل سه گروه می‌شوند:

* شناسایی در مبدا: نمی‌تواند همه حملات را تشخیص دهد
* شناسایی در مقصد(قربانی): نیاز به منابع بیشتری دارد و ممکن است با تاخیر هم همراه باشد
* شناسایی در مسیر‌های میانی(middlebox)

اما به دلیل کم اهمیت بودن، همین دسته بندی حمله‌ها از نظر الگوریتم پایه‌ای خود تقسیم می‌کنیم.

3.1**روش‌های مبتنی بر امضا**

آنتروپی[[16]](#endnote-16) معیاری است که برای اندازه‌گیری میزان تصادفی یک ویژگی در یک دوره زمانی معین استفاده می‌شود. روش‌های مبتنی بر آنتروپی به‌عنوان یک رویکرد مؤثر برای محاسبه تصادفی از یک مجموعه داده ایجادشده است. به‌طورکلی مقادیر بالای آنتروپی نشان‌دهنده توزیع پراکنده‌تر ویژگی در دادگان[[17]](#endnote-17) موجود است و مقادیر پایین آنتروپی نشان‌دهنده نامتوازن بودن یک توزیع است یعنی برخی مقادیر ویژگی موردنظر، فراوانی بیشتری نسبت به سایر مقادیر دارند. لذا، از این روش برای تشخیص ناهنجاری گسترده در سامانه‌های سنتی تشخیص نفوذ[[18]](#endnote-18) استفاده‌شده است. به‌منظور تشخیص حملات منع خدمت، آنتروپیِ جریان شبکه را می‌توان با استفاده از چندین ویژگی مانند جریان شبکه، آدرس آی.‌پی[[19]](#endnote-19) مبدأُ و مقصد بسته‌ها و یا تعداد بسته‌های موجود در یک جریان محاسبه کرد. سپس با یک حد آستانه[[20]](#endnote-20) از پیش تعریف‌شده، مقایسه کرد و در مورد نرمال یا غیرنرمال بودن جریان بررسی‌شده، تصمیم‌گیری کرد. یکی از مهم‌ترین مزیت‌های این روش داشتن سربار محاسباتی کم می‌باشد. با توجه به موفقیت الگوریتم‌های مبتنی بر آنتروپی در شبکه سنتی در تشخیص حملات منع خدمت توزیع‌شده، از این روش‌ها در تشخیص حملات در شبکه‌های نرم‌افزار محور نیز استفاده می‌شود[17].

Signature Based with XDP:flow-based signatures: سعی می‌کند امضاهای مهاجم را بدست آورد و تعداد حداقل بهینه خط قوانین از آنها را بسازد. مشکل آن عدم کارایی در شناسایی حملات متنوع می‌باشد.

3.**2 روش‌های مبتنی بر یادگیری ماشین (آنومالی – مدل)**

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

Jaqen: Universal Sketches and Data-Plane switches

این روش با استفاده از اسکچ‌های جهانی و پیاده سازی آنها بر روی سوییچ‌های برنامه پذیر و همچنین یک بخش کنترلر شمارنده‌ها به آن فرستاده می‌شود و تخمین و تشخیص می‌دهد استفاده می‌کند. همچنین به کمک همین کنترلر سوییچ‌های لایه داده را طوری کانفیگ می‌کند که امکان رفع مخاطره برای آنها فراهم باشد. با استفاده از زبان p4 این الگوریتم‌ها را بر روی سوییچ‌ها پیاده می‌کنیم و لذا وابسته به دستگاه و معماری خاصی نمی‌باشند. مشکل این روش این می‌باشد که پیلود بسته‌ها را بررسی نکرده و DPI ندارد.

RT-SAD: multi sketch tables and asymmetric based detection: ویژگی غیر متقارن بودن بین بسته‌های مختلف را به عنوان نشانی از وقوع حمله در نظر می‌گیرد. هدف اصلی آن ارایه راهکاری بهین از نظر میزان استفاده از حافظه می‌باشد. و حملات را در سمت کاربر مبدا تشخیص می‌دهد.

Smart Defenese: NN: از شبکه‌های عصبی عمیق در سمت لبه مشتری و شبکه‌های با الگوریتم‌های پیشرفته تر در سمت فراهم کننده اینترنت استفاده می‌کند. مشکل آن عدم سازگاری با تنوع ترافیک می‌باشد.

Bigflow: Trustworth Classifier : با درنظرگرفتن بسته‌‌ها به عنوان جریان، ویژگی‌های آن را استخراج می‌کند و سپس از روی آنها تشخیص می‌دهد. نرخ پاسخ پایینی دارد و نیاز به مداخله انسان برای کلاس‌بندی برخی جریان‌ها دارد.

4 **روش پیشنهادی**

در بخش قبل برخی روش‌های مبتنی بر امضا و یادگیری ماشین به منظور تشخیص حملات منع خدمت توزیع‌شده معرفی شدند. به عنوان نتیجه میتوان گفت روش‌های شناسایی و مقابله با حملات منع خدمت توزیع شده، ویژگی‌های ترافیک را از سه منظر بررسی می‌کنند (ترافیک را از سه منظر مشاهده می‌کنند) و سعی در مقابله دارند:

* بسته: یعنی جلوی یک بسته مثلاً HTTP‍‌ را می‌گیرند.
* جریان: یعنی جلوی یک جریان که مثلاً اندازه آن بیش از ۱۰۰ کیلوبایت باشد را می‌گیرند.
* رفتار کاربر: اگر رفتار ترافیک کاربری نامتعارف بود، جلوی آن را می‌گیرند. مثلاً در یک دقیقه، بیش از ۱۰ درخواست به منابع مختلف یک سایت ارسال کند.

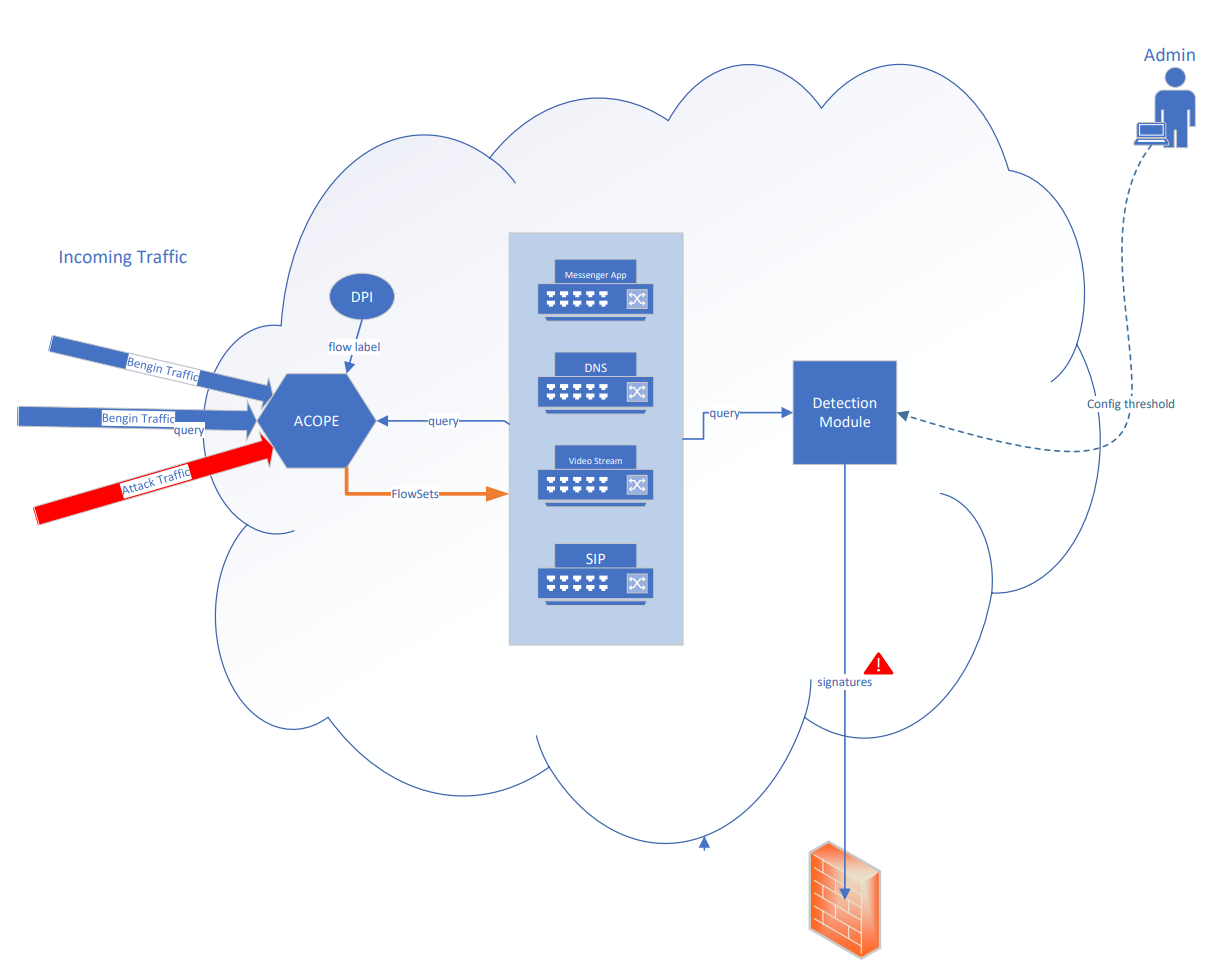
و در هر یک ازمنظرها طبق اطلاعاتی که به دست می‌اوردند، بر اساس روش‌هایی زیر، ترافیک نامتعارف را تشخیص می‌دهند:

* روشهای آماری
* روش‌های مبتنی بر مدل و تشخیص بی‌نظمی
* روش‌های مبتنی بر یادگیری ماشین که می‌توانند زیر مجموعه هر دو گروه بالا قرار گیرند

اما این روش‌ها (۳ روش اولی) مشکلشان این بود که با تنوع پروتکلی اپلیکیشن‌های مختلف، سازگار نبودند و باعث بروز خطا می‌شدند. در واقع ترافیک برای هر اپلیکیشن می‌تواند الگوی مختلفی داشته باشد و برای هر کاربردی نمی‌توان یک الگو، مرز و شناسه برای حالت متعارف آن تعریف نمود. برای حل این مشکل به شناسایی اپلیکیشن‌های مختلف می پردازند ،که از روش‌های مثل dpi یا یادگیری ماشین استفاده می‌شود و سپس با استفاده از اطلاعات آنها ترافیک را دسته بندی کرده و در هر کدام برای تشخیص الگو‌های نامتعارف، تنظیمات متفاوتی(مثل مقادیر آستانه متفاوت برای حجم بسته‌‌ها) به کار می‌برند.

اما در شبکه‌های پهن باند با مشکلی به نام تنوع ترافیکی بالا مواجه هستیم واز طرفی با توجه به استریمینگ ترافیک بایستی در کمترین زمان ممکن، کم هزینه‌ترین راهکار را ارایه دهیم. راهکارهای مبتنی بر یادگیری ماشین و استفاده از DPI، سربار محاسباتی زیاد دارند.

نکته ای که در پژوهش های پیشین نادیده گرفته می‌شد، مربوط به مولفه سوم شبکه‌های پهن باند یا همان تنوع ترافیکی می‌باشد. در روش‌های پیشین مولفه‌های اول و دوم یعنی اینکه داده‌ها با سرعت زیادی در حال تولید هستند و همچنین این داده شامل حجم زیادی از هدرها و پیلود می‌باشند را درنظر گرفته بودند. لذا روشی ارایه می‌دهیم تمامی این سه مورد را با تمرکز بیشتر بر روی ویژگی سوم به عنوان مسیله اصلی را هدف قرار می‌دهد. بدین منظور روشی که ارایه می‌دهیم از ویژگی‌ پردازش جامع[[21]](#endnote-21) برخوردار می‌باشد، یعنی تمامی بسته ها را یک و تنها یکبار بررسی می‌کند. و لذا بدین صورت روشی بسیار سریع و با دقت بالا و تطبیق پذیر با مشخصات ترافیکی[[22]](#endnote-22) ارایه می‌دهیم (علاوه بر معیارهای متداولی مثل سرعت-نرخ‌گذر بالا[[23]](#endnote-23) و تاخیر کم که خواسته همه روش‌های قبلی بوده است) که یک راه‌حلی نوین می‌باشد که در هیچ‌یک از پژوهش‌های پیشین تا به حال صورت نگرفته است.



شمای کلی از روش پیشنهادی

روال کاری ما بدین صورت خواهد بود با استفاده از روش ارایه شده در مقاله ACoPE به برچسپ زنی جریان‌ها و قراردادن جریان‌های شبیه به هم از نظر رفتار در یک گروه و این اطلاعات مربوطه را در داده ساختار‌های اسکچ‌ که بر روی سوییچ‌های برنامه پذیر می‌باشند و توسط ادمین شبکه کنترل می‌شوند، ذخیره می‌کنیم. این اطلاعات را برای هر اپلیکشن و پروتکل متناظر به صورت جدا ذخیره می‌کنیم. یک قسمت تشخیص داریم که با استفاده از این ویژگی‌‌های آماری و مشاهده رفتار متداول هر پروتکل ویا اپلیکیشن در زمانهای مختلف، این اطلاعات را با مقادیر آستانه‌ای که از آن طریق به دست آورده مقایسه می‌کند و نشان دهنده حداکثر بی‌نظمی قابل چشم‌پوشی در شبکه می‌باشد و در صورت مشاهده مغایرت آن جریان را به صورت یک حمله تشخیص داده و سعی می‌کند امضای معادل آن را تولید ‌کند و به عنوان خروجی به یک دیوار آتش ارسال کند . روش تشخیص ما می‌تواند به خوبی

5 **نتیجه‌گیری**

در این نوشتار به مرور مفاهیم اولیه مرتبط با حملات منع خدمت توزیع‌شده و انواع آن، شبکه‌های پهن‌باند و ویژگی‌های این شبکه وروش‌ها و الگوریتم‌های پردازش و معرفی مفاهیم و واژه‌های به کار رفته در پژوهش‌های مختلف به کار رفته شده است، مثل محاسبات دیتااستریمینگ پرداخت کردیم. سپس برخی پژوهش‌های انجام‌شده درزمینه‌ی تشخیص حملات منع خدمت در شبکه‌های پهن‌باند موردبررسی قرار گرفت و مشکلات پیاده‌سازی و عملکردی و چالش‌های حل نشده آنها بیان شد. در آخر روش پیشنهادی سریع با دقت بالا و بهینه از نظر میزان مصرف منابع و سازگار با تنوع ترافیکی براش شناسایی حملات منع خدمت توزیع‌شده در بستر شبکه ‌های پهن ‌باند به صورت مختصر شرح داده شد.

جدول ۱ : مراحل انجام و پیشبرد پروژه

|  |  |  |
| --- | --- | --- |
| فعالیت | میزان پیشرفت | تخمین زمان باقی‌مانده |
| ۱. مطالعه و بررسی مفاهیم | **۹۰٪** | **کمتر از ۱ هفته** |
| ۲. تحلیل و بررسی کارهای پیشین | **۷۰٪** | **۲ هفته** |
| ۳. ارائه و امکان‎سنجی روش پیشنهادی | **۱۰٪** | **۴ هفته** |
| ۴. پیاده‌سازی روش پیشنهادی | **۱۰٪** | **۴ هفته** |
| ۵. ارزیابی روش پیشنهادی | **۰٪** | **۳ هفته** |
| ۶. جمع‌بندی و تدوین پایان‌نامه | **۰٪** | **۶ هفته** |

**کتاب‌نامه**

1. Zecheng, Tianwei Zhang, and Ruby B. Lee. "Machine learning based DDoS attack detection from source side in cloud." 2017 IEEE 4th

**واژه‌نامه**

1. Availability [↑](#endnote-ref-2)
2. Internet Service Provider [↑](#endnote-ref-3)
3. Denial of Service [↑](#endnote-ref-4)
4. Distributed Denial of Service [↑](#endnote-ref-5)
5. Attacker [↑](#endnote-ref-6)
6. Bot [↑](#endnote-ref-7)
7. System [↑](#endnote-ref-8)
8. Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities [↑](#footnote-ref-2)
9. Attacker [↑](#endnote-ref-9)
10. Agent [↑](#endnote-ref-10)
11. Victim [↑](#endnote-ref-11)
12. Foading Attack [↑](#endnote-ref-12)
13. Reflection Attack [↑](#endnote-ref-13)
14. Amplification Attack [↑](#endnote-ref-14)
15. HTTP [↑](#endnote-ref-15)
16. Entropy [↑](#endnote-ref-16)
17. Dataset [↑](#endnote-ref-17)
18. Intrusion Detection System [↑](#endnote-ref-18)
19. IP Address [↑](#endnote-ref-19)
20. Trashhold [↑](#endnote-ref-20)
21. Compressive [↑](#endnote-ref-21)
22. Adaptive Learning [↑](#endnote-ref-22)
23. Linerate Processing [↑](#endnote-ref-23)