

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 برنامه‌های مختلف ارایه شده است و علاوه بر آن بسیاری از برنامه‌‌های کاربردی[[1]](#endnote-2) امروزه با این که از پروتکل‌های استاندارد و متداولی برای ارتباط با یکدیگر و تبادل اطلاعات در شبکه استفاده می‌کنند با این‌حال شیوه استفاده از این پروتکل‌ها متفاوت می‌باشد، به عنوان مثال برنامه‌های پیام‌رسان و مرورگر‌های وب از بسته‌های مبتنی بر پروتکل** اچ.تی.تی.پی(اس)[[2]](#endnote-3) **برای تبادل اطلاعات استفاده می‌کنند، با این تفاوت‌ که در برنامه‌های پیام‌رسان با ارسال تعداد معینی از بسته‌های** اچ.تی.تی.پی(اس) **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 شبکه‌ها شناخته می‌شود.**

**در شبکه‌های پهن‌باند[[3]](#endnote-4) 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. همچنین در این شبکه‌ها با تنوع پروتکلی زیادی روبرو هستیم و سیستم‌های تشخیص‌ نفوذ در این شبکه ‌ها به تعداد زیادی خط قوانین مبتنی بر امضا، تیاز خواهند داشت و در نتیجه نمی‌توانند ترافیک را پایش و حملات را در لحظه تشخیص دهند. از این رو، مقابله با حملات منع خدمت در این شبکه‌ها، به یک بستر مهم تحقیقاتی در سال‌های اخیر تبدیل‌شده‌ است.در دهه‌های گذشته محققان روش‌های شناسایی بسیاری را برای حملات منع خدمت توزیع‌شده[[4]](#endnote-5) پیشنهاد کرده‌اند. عدم تطبیق‌پذیری و مقیاس‌پذیری برای استفاده در شبکه‌های پهن‌باند، از متداول‌ترین مشکلات این روش‌ها هستند. 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، که ویژگی پردازش جامع ترافیک را نیز شامل شود. روش ما جریان‌ها را بر اساس اینکه برای کدام کاربرد می‌باشند دسته‌بندی کرده و به کمک رفتار عادی ترافیک هر برنامه کاربردی، ترافیک‌ها متخاصم را تشخیص می‌دهد. به دلیل اینکه از الگوریتم‌ها و داده‌ساختارهای فشرده و سبک با قابلیت جستجوی سریع استفاده می‌شود، سرعت بالا و استفاده بهینه از حافظه تضمین می‌شود. همچنین در روش پیشنهادی از تکنولوژی‌های تسریع عملیات پردازش بسته که در سالیان اخیر بسیار مورد استقبال قرار گرفته‌است، استفاده می‌شود و می‌توان سرعت پردازش بسته‌ها را تسریع‌بخشد که منجر به پردازش جامع تمامی بسته‌های ترافیک شبکه خواهد شد. در انتها کارایی روش ارائه شده در مقایسه با برخی دیگر از راهکارهای موجود و با ‌درنظرگرفتن معیارهایی نظیر میزان استفاده از پردازشگر و حافظه، نرخ دورانداختن بسته‌ها، و میزان تاخیر در شناسایی حملات بررسی می‌شود.**

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

# 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[[5]](#endnote-6) آسان به خدمات بستر اینترنت بیش ‌از پیش مورد توجه قرار می‌گیرد، بدین معنا که ارائه‌دهندگان خدمات ارتباطی[[6]](#endnote-7) 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.

حملات منع خدمت[[7]](#endnote-8)، 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[[8]](#endnote-9) یک‌گونه مخرب‌تر از حملات منع خدمت هستند که در آن‌ها حمله‌کننده[[9]](#endnote-10) از طریق سیستم‌[[10]](#endnote-11)هایی که تحت کنترل خود دارد، حمله را انجام می‌دهد. بدین ترتیب علاوه بر حجم ترافیک سنگین‌ حملات و دشواری‌های قاپل شدن تمییز بین ترافیک بالا در عین حال قانونی شبکه[[11]](#endnote-12) و ترافیک حمله‌کننده، پیدا کردن فرد مهاجم 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 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.

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 برنامه‌های کاربردی 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 استریمینگ[[12]](#endnote-13) و اسکچ‌ها[[13]](#endnote-14) 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 بیان خواهد شد.

# مفاهیم پایه

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.

### شبکه‌های پهن‌باند

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

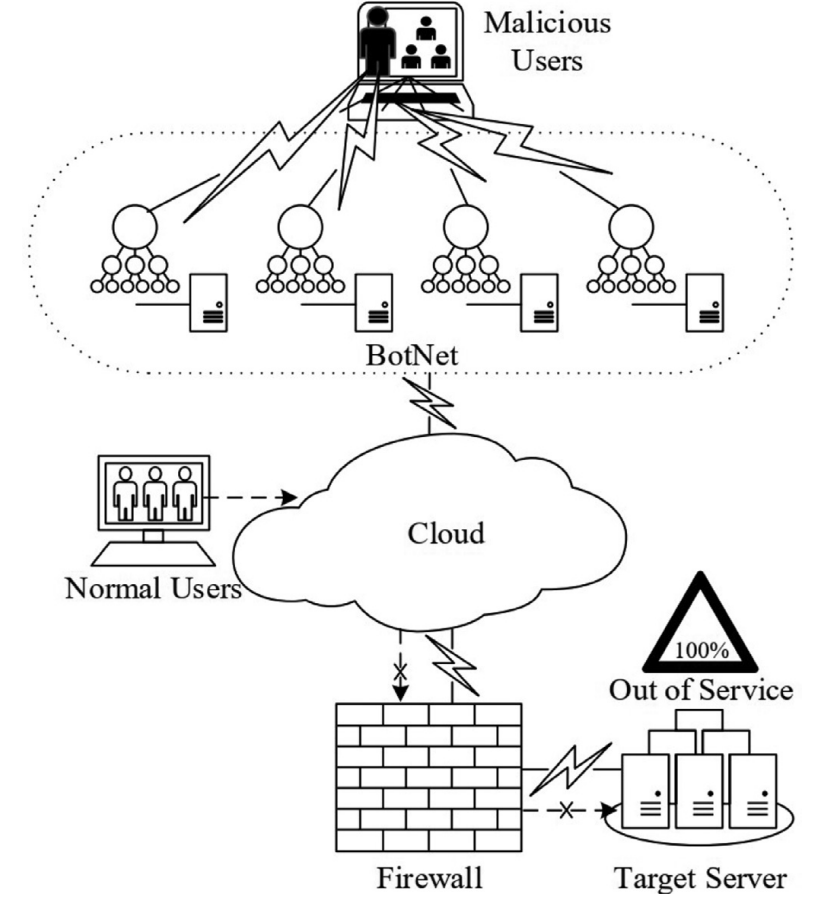
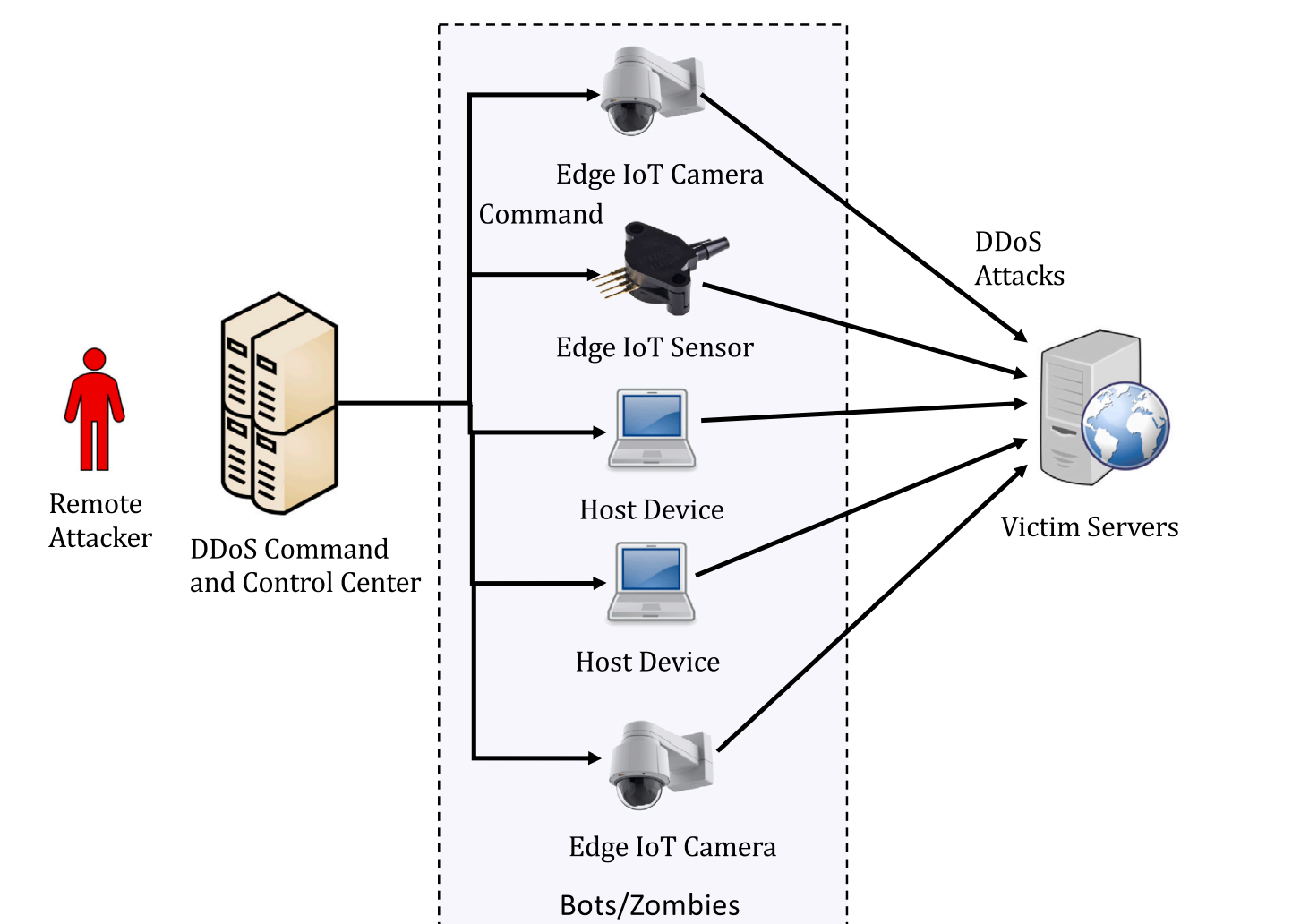
* سرعت بالا: داده‌ها و بسته‌ها با سرعت و فرکانس بالایی تولید می‌شوند.
* حجم بالا:‌ اطلاعات عبوری از شبکه و درحال تبادل بسیار حجیم می‌باشند. به عبارتی دیگر بسته‌هایی با پیلود‌ها و حجم زیادی از سرایند‌ها را خواهیم داشت.
* تنوع داشتن: علاوه بر ظهور پروتکل‌های مختلف که هر کدام برای کاربردی خاص می‌باشند، 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 برای شبکه‌های پهن‌باند، واضح است که مدیریت و کنترل ترافیک در این شبکه‌ها به یکی از چالش‌های اصلی در زمینه شبکه‌های کامپیوتری تبدیل شده است.

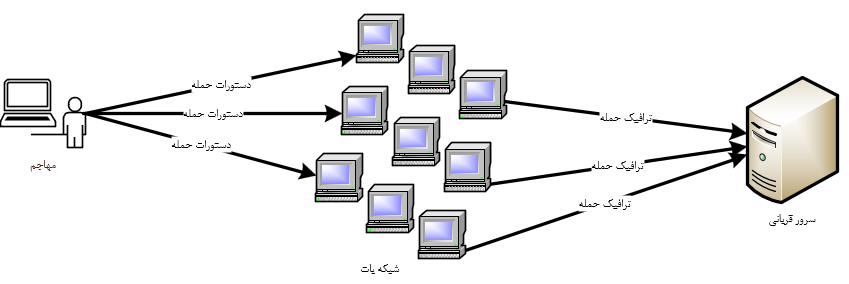
### حملات منع خدمت و حملات منع خدمت توزیع شده

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 تولید ازدحام و اختلال مصرف منابع پردازشی سیستم (پردازشگر سیستم) یا منابع شبکه (پهنای باند) می‌باشد.

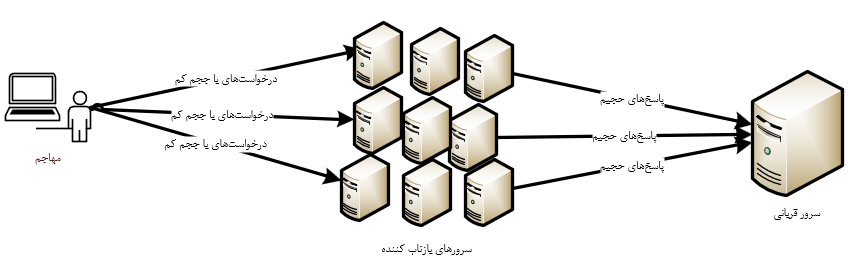
حملات منع خدمت توزیع شده گونه خطرناک‌تر از این حملات می‌باشند که در آن مزاحم ابتدا با اسکن[[14]](#endnote-15) آسیب پذیری‌های دستگاه‌های مختلف موجود در شبکه اینترنت شروع به خطر انداختن ماشین‌های عامل[[15]](#endnote-16) متعددی می‌کند که ممکن در سطح جغرافیایی گسترده‌ای توزیع یافته باشند. کشف آسیب‌پذیری‌ها و فرآیند بهره‌برداری از عوامل معمولاً به‌طور خودکار انجام می‌شود، به عنوان مثال، این کار را می‌توان با ارسال پیام‌های ایمیل با پیوست کد حمله انجام داد. هنگامی که یک نفوذگر با موفقیت برخی از آسیب پذیری‌های این سیستم‌ها را شناسایی کرد، می تواند این ماشین‌ها را با استفاده از یک برنامه مخرب مانند اسب تروجان[[16]](#endnote-17) به خطر بیاندازد. بدین صورت که با تکثیر فایل مخرب در چندین ماشین عامل، مزاحم توانایی کنترل بسیاری از دستگاه‌ها را دارد و بدون اطلاع صاحب قانونی دستگاه، می‌تواند حملات منع‌ خدمت توزیع شده را آغاز کند. تعداد این دستگاه‌ها می‌تواند به چندین هزار یا میلیون‌ها عدد دستگاه برسد. به این سیستم‌هایی که توسط فرد مهاجم یا هدایت کننده از راه دور گنترل می‌شوند، ربات گفته می‌ شود و این مجموعه ربات‌ها که به آنها شبکه‌ بات[[17]](#endnote-18) گفته می‌شود، دستورات را از شخص مهاجم دریافت ‌می‌کنند. مهاجم می تواند حملات منع خدمت توزیع‌شده در مقیاس بزرگ را انجام دهد تا یک سرویس یا شبکه قانونی را با ارسال یک فرمان کنترلی به دستگاه‌های شبکه بات نت برای ایجاد ترافیک زیاد بدون توجه به یک سرویس یا شبکه قانونی، با اختلال مواجه کند. در نتیجه، در مدت زمان کوتاهی حجم زیادی از ترافیک را به سمت سرور و منابع آن هدایت می‌کنند که سرویس دهی آن یا رویکرد شبکه را برای پاسخگویی به کاربران قانونی با اختلال مواجه می‌کند. در صورت بروز حملات منع خدمت توزیع‌شده، رهگیری مبدا حمله یعنی نقطه‌ای که حمله از آنجا شروع شده‌است، دشوارتر و همچنین ترافیک ایجاد شده در اثر حمله بزرگتر و مخرب‌تر می‌باشد.

در سال‌های اخیر، تعداد دستگاه‌های مبتنی بر اینترنت اشیا[[18]](#endnote-19) که به نسبت تجهیزات دیگر موجود در شبکه آسیب پذیرتر هستند، به سرعت در حال افزایش می‌باشد[[19]](#footnote-2). شبکه‌های بات تشکیل‌شده از این دستگاه‌های مبتنی بر اینترنت اشیا، مقیاس حملات منع خدمت توزیع شده را به میزان قابل توجهی گسترش می‌دهد. در سال ۲۰۱۶ میلادی، شرکت ارائه‌دهنده سرویس دامنه نام[[20]](#endnote-20) دی.وای.ان[[21]](#endnote-21)، توسط دستگاه‌های مبتنی بر اینترنت اشیا عظیم که توسط بدافزاری به نام میرای[[22]](#endnote-22) کنترل می‌شدند، مورد حمله قرار گرفت که درنهایت منجر به غیرقابل دسترس بودن منطقه وسیعی از خدمات (توییتر[[23]](#endnote-23)، اسپاتیفای[[24]](#endnote-24)، نتفلیکس[[25]](#endnote-25)، سی ان ان[[26]](#endnote-26) و...) برای کاربران در سواحل شرقی ایالات متحده شد. مشکل دیگر دفاع در برابر حملات منع خدمت توزیع شده، بروز حملات تقویت بازتاب[[27]](#endnote-27) است. در سال ۲۰۱۸، گیتهاب[[28]](#endnote-28) با استفاده از آسیب‌پذیری پروتکل ممکچ[[29]](#endnote-29)، با انعکاس چند برابر از ۵۰۰۰ بار و ترافیک پیک ۱.۳۵ ترابیت بر ثانیه، قربانی‌ یک حمله منع خدمت توزیع شده از نوع تقویت بازتابی قرار گرفت. در فوریه ۲۰۲۰، ارایه دهندگان خدمات وب آمازون[[30]](#endnote-30) حمله‌ای با حجم پیک ۲.۳ ترابایت بر ثانیه را تجربه کرند. در ژوئیه ۲۰۲۱، شرکت ارایه دهنده خدمات تحویل محتوای کلودفلر[[31]](#endnote-31) در گزارشی به محافظت از یکی از مشتریان خود در برابر حمله منع خدمت توزیع شده نشات گرفته از یک شبکه بات در ابعاد جهانی توسط بدافزار میرای با ترافیک پیک ۱۷.۲ میلیون درخواست در ثانیه، اشاره کرد. یاندکس[[32]](#endnote-32)، ارائه‌دهنده خدمات پیشگیری از حملات منع خدمت توزیع شده روسیه گفت که در تاریخ ۵ سپتامبر ۲۰۲۱ یک حمله منع خدمت توزیع شده پروتکل اچ.تی.تی.پی را که از تجهیزات شبکه میکروتک[[33]](#endnote-33) بروزنشده[[34]](#endnote-34) سرچشمه می‌گرفت، مسدود کرده است.



1حملات منع خدمت توزیع شده با استفاده از شبکه بات



2حملات منع خدمت توزیع شده از نوع تقویت بازتابی

طبق خلاصه سالانه آکامی[[35]](#endnote-35) برای سال ۲۰۲۰، تعداد حملات منع خدمت توزیع شده در مقیاس بزرگ به طور قابل توجهی افزایش یافته است. در بزرگترین حمله منع خدمت توزیع شده رخ داده تا به حال، ترافیک حمله به ۱.۴۴ ترابیت در ثانیه رسیده است. از طرفی در سالیان اخیر، این حملات با استفاده از پروتکل‌های جدیدتری ظاهر خود را تغییر می‌دهد. به عنوان مثال، در پایان ژوئیه ۲۰۲۰، پلیس فدرال آمریکا[[36]](#endnote-36) هشداری صادر کرد مبنی بر اینکه پروتکل برنامه‌های محدود شده[[37]](#endnote-37) و سایر پروتکل‌ها ممکن است برای انجام حملات منع خدمت توزیع شده مورد سو استفاده قرار گیرند. حملات منع خدمت توزیع شده بر اساس بردارهای حمله[[38]](#endnote-38) جدید ممکن است تغییرات زیادی در ویژگی های آماری مانند سرعت بسته ها و فاصله بسته های مورد استفاده در مقایسه‌ با روش های سنتی داشته باشند، که باعث می شود روش های سنتی مقابله در برابر این حملات مختلف کارایی لازم را نداشته باشند.

1گزارش و پیش‌بینی شرکت سیسکو از مجموع حملات منع خدمت توزیع شده

### 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[[39]](#endnote-39) اصلی، کنترل‌کننده حمله، عامل‌[[40]](#endnote-40)ها و قربانی[[41]](#endnote-41). 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.

### 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:

* شبکه: یکی از اصلی‌ترین اهداف حملات منع خدمت از بین بردن دسترس‌پذیری شبکه به‌منظور ممانعت از استفاده از یک خدمت ارائه‌شده 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 خدمات 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.

### 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.

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[[42]](#endnote-42): 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: دراکثر 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. به‌عنوان‌ مثال استفاده از ضعف در الگوریتم دست ‌تکانی سه مرحله‌ای پروتکل تی.سی.پی[[43]](#endnote-43).
  + 3. حملات سیل‌آسا مبتنی بر بازتاب[[44]](#endnote-44): 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[[45]](#endnote-45): 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[[46]](#endnote-46) 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.

### داده جريان[[47]](#endnote-47)

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:

* پردازش دسته‌ای[[48]](#endnote-48): در این رویکرد تمامی بسته‌ها در یک پنجره زمانی را ضبط کرده و سپس آن ها را در زمان‌های بعدی پردازش می‌کنیم. 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.
* پردازش جریانی[[49]](#endnote-49): اکثر راهکارهای ارایه شده که در قسمت بعدی بررسی می‌کنیم، مبتنی بر این رویکرد می‌باشند. این الگوریتم‌ها دو مشخصه زیر را درنظر می‌گیرند: اول این که اطلاعات به صورت جرياني از داده‌ها (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 پهن‌باند 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 [[50]](#endnote-50)و با کمترین میزان استفاده از حافظه انجام دهیم. الگوریتم‌های پردازش‌ جریانی در بحث پردازش اطلاعات مختلف بسیار کاربردی هستند. الگوریتم های مبتنی بر پردازش‌ جرياني، ابتدا مسئله را به یکی از چندین روش موجود مدل می‌کنند. یکی از این مدل‌های بسیار محبوب ترنستيل[[51]](#endnote-51) می‌باشد. در این مدل یک داده جريان ورودي به نام I درنظر می‌گیریم که شامل مجموعه‌ای از تاپل‌های دوتایی می‌باشد:

I= α1, α2, α3, α4,…

Ʌαi={( a1, v1)| a1Ɛ{0,1,…,u-1}, v1ƐR}

[u]= key space

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

A[ax] += vx

این پارامتر‌ها بسته به مساله داده‌ جرياني که داریم، می‌توانند متفاوت باشند. دربحث پردازش بسته‌‌های دریافتی شبکه، جريان همان جریان ورودی، تاپل‌ها همان بسته‌ها می‌باشند که به‌طور مثال کلیدشان همان ۵ خصیصه و به‌روز‌رسانی نیز می‌تواند اندازه بسته باشد. درنتیجه برای شناسایی حملات منع خدمت، ما بایستی آدرس‌هایی که بسته‌هایی با حجم نامتعارف ارسال می‌کنند، را شناسایی کنیم.

در مسائل داده جريان ما به دنبال چندین نوع جواب برای مسایل اندازه‌گیری مختلف می‌توانیم باشیم، که پس از این که مسئله را مدل کردیم، می‌توانیم الگوریتم‌هایی ارایه دهیم که بر مبنای آن مدل سعی در یافتن این جواب‌ها دارند. برای توضیح بهتر این انواع مسائل ابتدا توضیحات زیر را ارایه می‌دهیم.

جريان ورودی را توالي از بسته هايي به شكل تاپل‌ شامل شناسه جریان متناظر آن و سایز آن بسته در نظر می‌گیریم:

Ƒ= تعداد کل جریان‌های متمایز شناسه جریان=(srcIP, srcport, dstIP, dstport, protocol)

داده جريان ورودی = (f1,c1),…, (ft,ct),…

جواب‌هایی که به دنبال آنها هستیم عضو یک دسته‌ از مسائل زیر می‌باشند:

* سایز هر جریان[[52]](#endnote-52): به دنبال یافتن سایز جریان یا تعداد بسته های دریافت شده متعلق به جریان ƒ می‌باشیم که آن را با nƒ نشان می‌دهیم. سایز تمامی بسته های دریافتی نیز می‌باشد.
* لحظه جریان[[53]](#endnote-53): در لحظه دلخواهي، به دنبال یافتن وضعیت جريان با استفاده از تابع g در لحظه [[54]](#endnote-54)g می‌باشیم، که به صورت زیر می‌تواند تعریف شود:

, ƒ [1, Ƒ]

بسته به این که تابع به چه صورت تعریف شده باشد، وضعیت کلی ترافیک شبکه را می‌تواند به صورت عددی بیان کند.

* شاخص[[55]](#endnote-55): شاخص‌ها جریان‌‌هایی هستند که اندازه آنها بیشترین تاثیر در لحظه جریان Lg را تشکیل ‌می‌دهد. به عبارتی دیگر، یک جریان را شاخص می‌نامیم اگر:

که α مقدار آستانه از پیش تعریف شده بین صفر و یک می‌باشد.

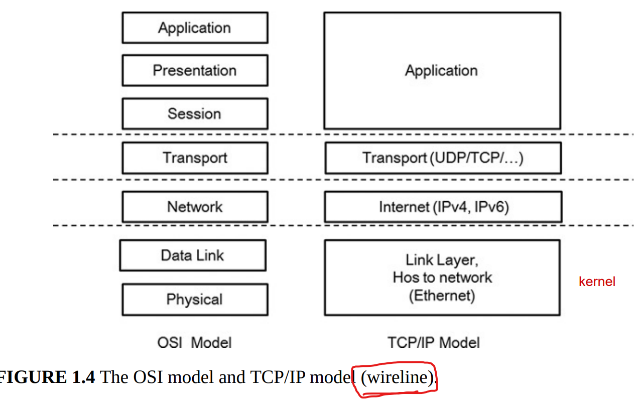
### انگاره[[56]](#endnote-56)

برای حل مسایل جريان داده، راهکارهای متفاوتی می‌توان به‌ کاربرد. 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. به اين روش اصطلاحاً نمونه برداری[[57]](#endnote-57) گفته می‌شود. نمونه ‌برداری 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 انگاره ارائه 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 مسایل داده جريان دارند. در ذیل به معرفی چند مورد از پر استفاده ترین آنها خواهیم پرداخت:

* انگاره شمارشي[[58]](#endnote-58): از یک جدول KxH تشکیل شده است که شامل K تا تابع درهم‌نگار[[59]](#endnote-59) مي‌‌باشد. این ساختار را الگوریتم‌های انگاره دیگر نیز استفاده می‌کنند. چون از توابع درهم‌نگار استفاده می‌کند لذا امکان تصادم[[60]](#endnote-60) وجود خواهد داشت و مقاديري كه برمي‌گردانند تخميني خواهند بود و درنتيجه به آنها داده ‌ساختارهای آماری احتمالاتی مي‌گویند اما یکی از ويژگی‌های آنها باید این باشد که نرخ خطای قابل قبول و کرانداری ارائه دهند. از این الگوریتم براي يافتن جواب مسائل شاخص استفاده می‌شود.
* انگاره شمارشي كمينه[[61]](#endnote-61): همانند انگاره بالايي مي‌باشد اما مرتبه فضایی را کاهش می‌دهد.
  + انگاره عمومي[[62]](#endnote-62): یک دسته جدیدي از انگاره‌ها با هدف ارائه داده ساختاری قابل استفاده برای حل تمامی انواع مسائل داده جريان مي‌باشند. يونيومان[[63]](#endnote-63) یکی از این الگوریتم‌ها می‌باشد.

پردازش سریع‌تر بسته‌‌ها

هنگامی که یک بسته از طریق درگاه‌های یک سیستم دریافت می‌شود تا پردازش آن، مراحل مختلفی را طی خواهد کرد. بنا به کاربرد، بسته‌ها از دستگاه‌های مختلفی عبور داده می‌شوند. برمبنای پشته پروتکل TCP/IP که تمامی کرنلهای سیستم عامل لینوکس از آن پشتیبانی می‌کنند بسته‌ها از دریافت تا پردازش بخش‌های مختلف ان و سپس ارسال آن در صورت نیاز، مراحل مختلفی را پشت سر خواهندگذاشت.

* 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 پشته پروتکلی کرنل برای انجام پردازش‌‌های پروتکلی مختلف (مثل بررسی آدرس‌ IP برای مقایسه آن با کنترل دسترسی تعریف شده) فرستاده می‌شود.
* در نهایت اگر برنامه کاربردی در سطح کاربر باشد، محتویات 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 استفاده می‌کند. به صورت جزیی تر 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.

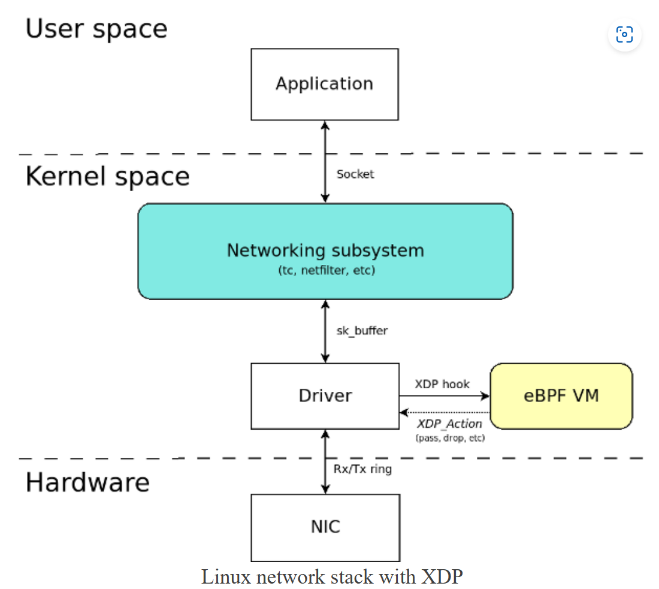
XDP-eXpress Data Path یکی از کامپوننت‌های جدید کرنل می‌باشد که پردازش بسته را به صورت بالایی بهبود می‌بخشد. روش‌های مثل DPDK کرنل را دور می‌زدند و تمام عملیات پردازش بسته در فضای کاربر صورت می‌گرفت. همچنین NIC را توسط یک درایور سطح کاربر بایست کنترل می‌نمود. پردازش شبکه در سطح کاربر با وجود مزایایش معایب زیر را دارد:

* چون که سیستم عامل یک لایه انتزاعی برای ارتباط با منابع سخت‌افزاری می‌باشد لذا برنامه‌‌های سطح کاربر برای تعامل با آنها بایستی درایور‌های مربوطه را خودشان بنویسند
* برنامه‌های سطح کاربر می‌بایست درصورت نیاز عملکرد‌هایی که توسط کرنل ایجاد می‌شد، پیاده سازی کنند.
* برنامه‌ها به صورت سندباکس اجرا می‌شوند که نحوه تعامل آنها با دیگر بخش‌های سیستم عامل را دشوار می‌کند.

به طور خلاصه XDP،برنامه‌‌های شبکه سطح کاربر(فیلتر،نگاشت،مسیریابی و...) را به جای انتقال به سطح کاربر، به ناحیه کرنل می‌برد. XDP به ما این امکان را می دهد که به محض ورود بسته به NIC و پیش از حرکت به سمت زیرسیستم شبکه هسته، برنامه خود را اجرا کنیم که منجر به افزایش قابل توجه سرعت پردازش بسته می شود.

BPF-Berkeley Packet Filter یک ماشین مجازی است که تنها مخصوص پردازش فیلترینگ می‌باشد. یکی از ابزارهایی که از BPF استفاده می‌کمد، tcpdump می‌باشد. عبارت فیلتر مربوطه توسط یک کامپایلر به بایت‌کد BPF تبدیل خواهد شد. از آنجایی که BPF یک ماشین مجازی می‌باشد، محیطی را به منظور اجرای برنامه‌ها در آن که علاوه بر بایت کد شامل یک مدل حافظه مبتنی بر بسته (دستورالعمل‌های بارگذاری به طور ضمنی بر روی بسته موردنظر انجام می‌شود)، ثبات‌ها (A و Xیعنی انباشتگر و ثبات اندیس)، یک حافظه موقت و یک شمارنده برنامه ضمنی می‌باشد را تعریف می‌کند. کرنل لینوکس از نسخه ۲.۵ به بعد از BPF پشتیبانی می‌کند. در کد آن تغییری به وجود نیامد تا اینکه در سال ۲۰۱۱، مفسر BPF را به یک JIT تغییر داد. این کار باعث شد که کرنل به جای تفسیر برنامه‌های BPF، قادر باشد که آن‌ها را به یک معماری هدف x86,ARM,MIPSو... تبدیل کند. این‌ منجر به معرفی eBPF در سال ۲۰۱۴ شد و BPF سنتی کنارگذاشته شد.ویژگی‌های جدید آن موارد زیر می‌باشد:

* بهره بردن از ویژگی‌های معماری ۶۴-بیتی مثل رجیستر‌ها و تعداد آن‌ها و opcode های بیشتر
* جداشدن از زیرسیستم شبکه و امکان استفاده در کاربرد‌های دیگر
* استفاده از مپ‌ها به عنوان راهی برای تبادل داده بین سطح کاربر و کرنل
* استفاده از توابع کمکی که در سطج گرنل اجرا می‌شوند. امکان صدازدن سیستم کال‌ها در برنامه‌های BPF نیزمی‌باشد
* امکان زنجیره سازی تعداد برنامه بیشتر BPF

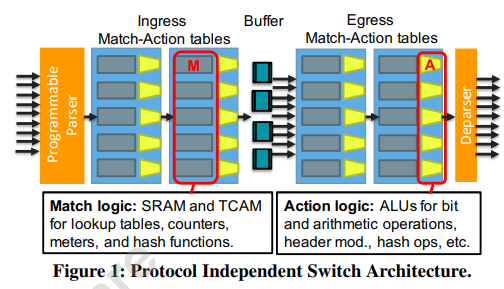
برخی از صف‌های NIC هنوز به هسته متصل هستند، در حالی که برخی دیگر به یک برنامه فضای کاربر متصل هستند که در مورد حذف شدن یا نشدن یک بسته تصمیم می‌گیرد. با این کار، میزان ترافیکی که به زیرسیستم شبکه هسته می رسد به میزان قابل توجهی کاهش می یابد. برای این کار بایستی یک نقطه بازرسی در پشته کرنل تعریف کرد که هرگاه بسته‌ای در NIC دریافت شد، آن را به فضای کاربر بفرستد که درآنجا تصمیم می‌گیرد که بسته را دراپ کند یا اجازه عبور از لایه‌های بالاتر پشته را بدهد. لذا نیاز به مکانیزمی بود که امکان اجرای کدهای سطح کاربر را در کرنل فراهم کند. به همین دلیل از eBPF استفاده شد.

هر اقدام در شبکه از یکسری عملیات پایه تشکیل شده است:

* دیوار‌آتش: خواندن ورودی، مقایسه با جدول قوانین، فوروارد یا دورانداختن بسته‌ها
* NAT: خواندن ورودی، دستکاری هدر بسته‌ها، فوروارد بسته‌ها
* تونلینگ: خواندن ورودی، ساخت یک قالب جدید برای بسته‌ها، فوروارد بسته

XDP بسته‌های دریافتی را به برنامه BPF هدایت می‌کند. که در آنجا می‌توان آن‌ها را ویرایش، فوروارد کرد. همچنین از توابع کمکی می‌توان برای انجام محاسبات و پردازش بسته‌ها بدون نیاز به سیستم کال استفاده کرد.

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.

3.1روش‌های مبتنی بر امضا

آنتروپی[[64]](#endnote-64) 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[[65]](#endnote-65) 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[[66]](#endnote-66) استفاده‌شده است. به‌منظور تشخیص حملات منع خدمت، آنتروپیِ جریان شبکه را می‌توان با استفاده از چندین ویژگی مانند جریان شبکه، آدرس آی.‌پی[[67]](#endnote-67) مبدأُ و مقصد بسته‌ها و یا تعداد بسته‌های موجود در یک جریان محاسبه کرد. سپس با یک حد آستانه[[68]](#endnote-68) 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.

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.

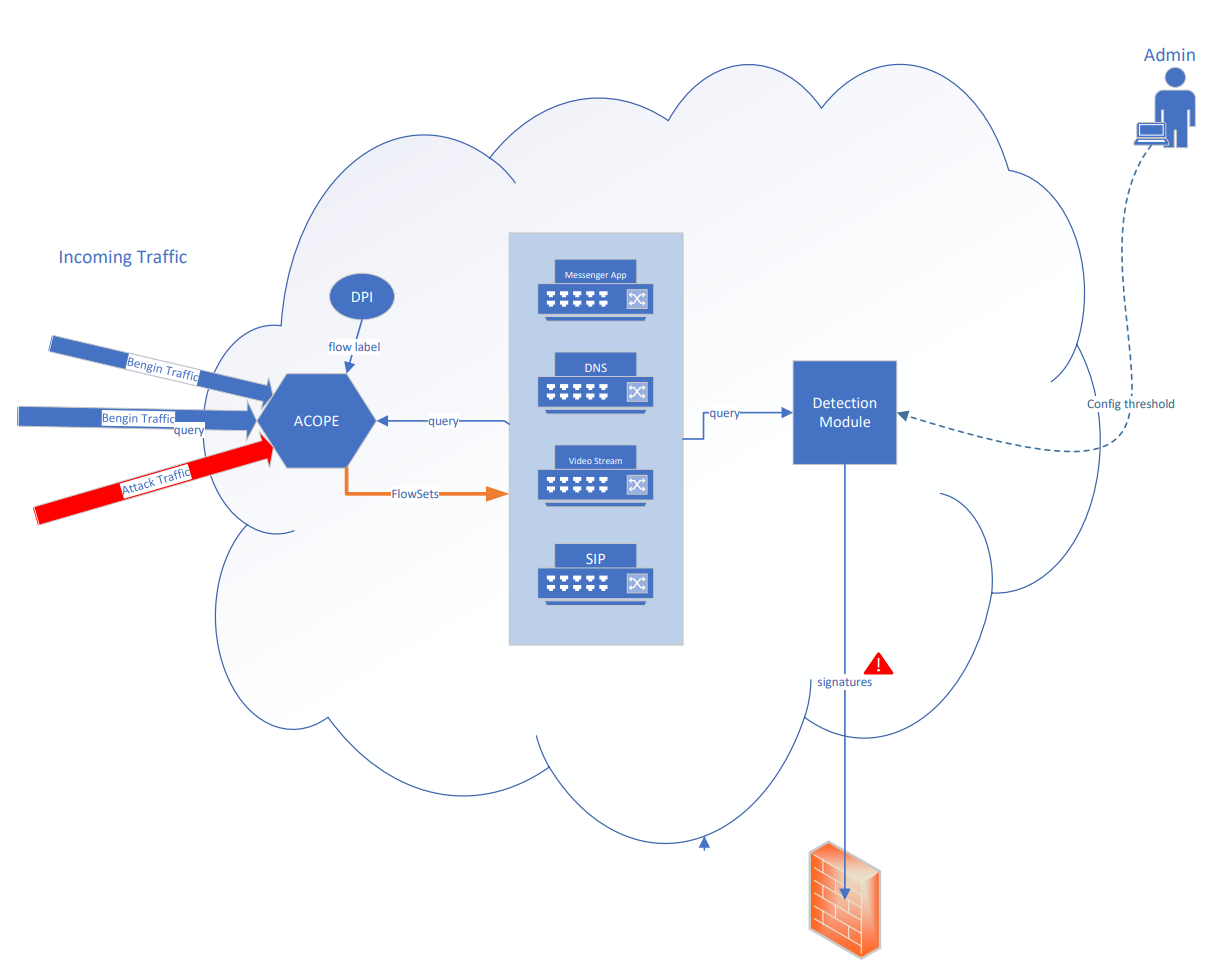
و در هر یک ازمنظرها طبق اطلاعاتی که به دست می‌اوردند، بر اساس روش‌هایی زیر، ترافیک نامتعارف را تشخیص می‌دهند:

* 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[[69]](#endnote-69) 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[[70]](#endnote-70) ارایه می‌دهیم (علاوه بر معیارهای متداولی مثل سرعت-نرخ‌گذر بالا[[71]](#endnote-71) 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. Application [↑](#endnote-ref-2)
2. HTTP/S [↑](#endnote-ref-3)
3. High-Bandwidth [↑](#endnote-ref-4)
4. Distributed Denial of Service attack [↑](#endnote-ref-5)
5. Availability [↑](#endnote-ref-6)
6. Internet Service Provider [↑](#endnote-ref-7)
7. Denial of Service [↑](#endnote-ref-8)
8. Distributed Denial of Service [↑](#endnote-ref-9)
9. Attacker [↑](#endnote-ref-10)
10. System [↑](#endnote-ref-11)
11. Flash coward [↑](#endnote-ref-12)
12. Data Streaming [↑](#endnote-ref-13)
13. Sketch [↑](#endnote-ref-14)
14. scan [↑](#endnote-ref-15)
15. Agent Machine [↑](#endnote-ref-16)
16. Trojan Horse malware [↑](#endnote-ref-17)
17. Botnet [↑](#endnote-ref-18)
18. Internet Of Things [↑](#endnote-ref-19)
19. Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities [↑](#footnote-ref-2)
20. Domain Name Service provider [↑](#endnote-ref-20)
21. DYN inc [↑](#endnote-ref-21)
22. Mirai malware [↑](#endnote-ref-22)
23. twitter [↑](#endnote-ref-23)
24. spotify [↑](#endnote-ref-24)
25. netflix [↑](#endnote-ref-25)
26. CNN [↑](#endnote-ref-26)
27. Amplification DDoS attack [↑](#endnote-ref-27)
28. github [↑](#endnote-ref-28)
29. memcached [↑](#endnote-ref-29)
30. Amazon Web Services [↑](#endnote-ref-30)
31. Cloudflare [↑](#endnote-ref-31)
32. Yandex [↑](#endnote-ref-32)
33. MikroTik [↑](#endnote-ref-33)
34. unpatched [↑](#endnote-ref-34)
35. Akamai technologies [↑](#endnote-ref-35)
36. FBI [↑](#endnote-ref-36)
37. Constrained Application Protocol(CAP) [↑](#endnote-ref-37)
38. Attack Vector [↑](#endnote-ref-38)
39. Attacker [↑](#endnote-ref-39)
40. Agent [↑](#endnote-ref-40)
41. Victim [↑](#endnote-ref-41)
42. flooding Attack [↑](#endnote-ref-42)
43. TCP 3-way handshake [↑](#endnote-ref-43)
44. Reflection Attack [↑](#endnote-ref-44)
45. Amplification Attack [↑](#endnote-ref-45)
46. HTTP [↑](#endnote-ref-46)
47. Data Stream [↑](#endnote-ref-47)
48. Batch processing [↑](#endnote-ref-48)
49. Stream processing [↑](#endnote-ref-49)
50. line rate [↑](#endnote-ref-50)
51. Turnstile model [↑](#endnote-ref-51)
52. Per flow size [↑](#endnote-ref-52)
53. Flow moment [↑](#endnote-ref-53)
54. Moment-g [↑](#endnote-ref-54)
55. Heavy hitter [↑](#endnote-ref-55)
56. sketch [↑](#endnote-ref-56)
57. sampling [↑](#endnote-ref-57)
58. Count-Sketch [↑](#endnote-ref-58)
59. Hash function [↑](#endnote-ref-59)
60. Hash collision [↑](#endnote-ref-60)
61. Count min sketch [↑](#endnote-ref-61)
62. Universal sketch [↑](#endnote-ref-62)
63. univmon [↑](#endnote-ref-63)
64. Entropy [↑](#endnote-ref-64)
65. Dataset [↑](#endnote-ref-65)
66. Intrusion Detection System [↑](#endnote-ref-66)
67. IP Address [↑](#endnote-ref-67)
68. Trashhold [↑](#endnote-ref-68)
69. Compressive [↑](#endnote-ref-69)
70. Adaptive Learning [↑](#endnote-ref-70)
71. Linerate Processing [↑](#endnote-ref-71)