

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 ارائه 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 که 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 توزيع‌‌شده[[3]](#endnote-4) 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[[4]](#endnote-5) بودن کامل شبکه می‌باشد**. حملات منع خدمت به‌عنوان تهدیدی جدی برای قابلیت دسترس‌پذیری شبکه‌ها شناخته می‌شود.**

**در شبکه‌های پهن‌باند[[5]](#endnote-6) 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 پیدا کرده ‌است. 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، نیاز خواهند داشت و در نتیجه توانايي پايش[[6]](#endnote-7) ترافيك به طور كامل و تشخيص حملات را نخواهند داشت. از این رو، مقابله با حملات منع خدمت در این شبکه‌ها، به یک بستر مهم تحقیقاتی در سال‌های اخیر تبدیل‌ شده‌ است. در دهه‌های گذشته محققان روش‌های شناسایی بسیاری را برای حملات منع خدمت توزیع‌شده 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[[7]](#endnote-8) به معنای پردازش تمامی بسته‌ها و تطبیق‌پذیری[[8]](#endnote-9) 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 برمبناي رفتار عادی ترافیک هر برنامه کاربردی، ترافیک‌هاي 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 بدين صورت می‌توان سرعت پردازش بسته‌ها را تسریع‌ بخشيد که منجر به پردازش جامع تمامی بسته‌های ترافیک عبوري شبکه خواهد شد. در انتها کارایی روش ارائه شده در مقایسه با برخی دیگر از راهکارهای موجود و با ‌در نظرگرفتن معیارهایی نظیر میزان استفاده از پردازشگر و حافظه، نرخ دور انداختن[[9]](#endnote-10) بسته‌ها، و میزان تاخیر در شناسایی حملات بررسی می‌شود.**

**کلیدواژه:** حملات منع خدمت توزیع‌شده، شبکه‌های پهن‌باند، تطبیق‌پذیری 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 اینترنت به جز جدایی‌ناپذیری در زندگی و تعاملات کاربران تبدیل شده و بحث دسترس‌پذیری آسان به خدمات بستر اینترنت بیش ‌از پیش مورد توجه قرار می‌گیرد، بدین معنا که ارائه‌دهندگان خدمات ارتباطی[[10]](#endnote-11) موظف هستند خدمات خود را به‌صورت شبانه‌روزی و بدون اختلال و وقفه در اختیار کارخواهان[[11]](#endnote-12) قرار دهند. درصورتی‌که این سازمان‌ها به هر دلیلی در ارائه خدمات خود دچار مشکل شوند و نتوانند به نحو مطلوب خدمات موردنظر 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[[12]](#endnote-13)، دسته‌ای از حملات در شبکه هستند که با هدف از بین بردن دسترس‌پذیری شبکه سعی در ممانعت از ارائه و انجام یک خدمت در شبکه دارند. حملات منع خدمت، پهنای باند یا ظرفیت لینک شبکه‌ را مصرف کرده و یا باعث از کار افتادن و اختلال عملکرد در یک کارپذیر[[13]](#endnote-14) 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 كارپذير، مانع از ارائه خدمت به‌صورت کامل و باکیفیت به کارخواهان و كاربران قانونی شوند. حملات منع خدمت توزیع‌ شده یک‌گونه مخرب‌تر از حملات منع خدمت هستند که در آن‌ها حمله‌کننده[[14]](#endnote-15) از طریق سیستم‌هایی که تحت کنترل خود مي‌آورد، حمله را انجام می‌دهد. بدین ترتیب علاوه بر حجم ترافیک سنگین‌ حملات و دشواری‌های تمییز قائل‌‌ شدن بین ترافیک بالا در عین حال قانونی شبکه[[15]](#endnote-16) و ترافیک حمله‌کننده، پیدا کردن فرد مهاجم اصلی نیز به‌مراتب دشوارتر می‌شود.

امروزه با شبکه‌هاي پهن‌باندي مواجه هستیم که منجر به بالا رفتن نرخ‌گذر اطلاعات به ميزان بيش از 100 گيگابيت در ثانيه در بسياري از تجهيزات شبكه شده ‌است. برای شناسایی مهاجمین در چنین شرایطی نیاز به راهکاری است که با سرعت بالایی بتواند تمامی بسته‌ها را بررسی کند. همچنین به دلیل ظهور پروتکل‌ها و برنامه‌های کاربردی مختلف با حجم زیادی از داده‌ها و تنوع زیادی از پروتکل‌ها مواجه هستیم. لذا چالش بعدی این می‌باشد که معیار تشخیص ما با توجه به کاربرد ترافیک بایستی متفاوت باشد. به همین دلایل، همچنان این حملات یکی از تهدید‌های بزرگ در شبکه‌های پهن‌باند محسوب می‌شوند که راه حل چندان مطلوبی برای آنها ارائه نشده است.

این گزارش در ۷ بخش تدوین‌ شده است. در بخش ۲ مفاهیم پایه مورد نیاز در این پژوهش‌ معرفی می‌شوند. ابتدا شبکه‌های پهن‌باند و ویژگی‌های آن‌ها بيان می‌شود. سپس انواع حملات منع خدمت، از نقطه ‌نظرهای مختلف مورد بررسی قرار می‌گیرند و در انتهای این بخش مفاهیم داده‌ جريان[[16]](#endnote-17) و انگاره‌‌ها[[17]](#endnote-18) توضیح داده می‌شود. در بخش ۳ به بررسی کار‌های پیشین انجام‌ شده برای تشخیص حملات منع خدمت توزیع شده پرداخته می‌شود. در بخش ۴ روش پیشنهادی به‌منظور بهبود تشخیص حمله در شبکه‌های پهن‌باند، 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 توزیع ‌شده می‌پردازیم و در پایان این بخش مفهوم داده‌ جريان و انگاره‌‌ها 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 زير می‌باشند[1]:

* سرعت بالا: داده‌ها و بسته‌ها با سرعت و فرکانس بالایی تولید می‌شوند. برای مثال در شبکه‌های نسل پنجم اینترنت همراه[[18]](#endnote-19)، هر کاربر از قابلیت تبادل اطلاعات با سرعت ۱۵ گیگابیت بر ثانیه برخوردار مي‌باشد.
* حجم بالا:‌ اطلاعات عبوری از شبکه و داده‌هاي در حال تبادل بسیار حجیم می‌باشند. به عبارتی دیگر بسته‌هایی با محتوا[[19]](#endnote-20) و حجم زیادی از سرایند‌ها[[20]](#endnote-21) را خواهیم داشت. به دلیل ظهور سرویس‌های مختلف و به دنبال آن پروتکل‌های مختلف و لزوم استفاده از الگوریتم‌های رمزنگاری، حجم زیادی از سرایند‌ها برای برقراری ارتباط الزامی می‌باشد. همچنین اطلاعاتی که کاربران در بستر اینترنت تبادل می‌کنند، می‌تواند طيف وسيعي از داده‌ها شامل فایل‌هایی حجیم و یا جرياني بي‌وقفه از بسته‌ها در هنگام مشاهده یک ویدئوي برخط يا در هنگام برگذاري يك كلاس مجازي باشد. در سال ۲۰۰۳، حجم کل داده‌های تولید شده در اینترنت حدود ۵ اگزابایت بود که این میزان در سال ۲۰۰۸ سه برابر شد و به ۱۴.۷ اگزابایت رسید. امروزه تقریباً ۵ اگزابایت داده در هر دو روز توسط کاربران تولید می شود.[2]
* تنوع داشتن: علاوه بر ظهور پروتکل‌های مختلف که هر کدام برای کاربردی خاص می‌باشند، نحوه انتقال و دریافت بسته‌ها بین كارخواه-كارپذير و استفاده از این پروتکل‌ها وابسته به وضعیت و کاربرد می‌تواند انواع مختلفی داشته باشد. براي مثال با اينكه بيشتر برنامه‌هاي مستقر بر بستر اينترنت، داده‌ها و تبادلات خود را در قالب بسته‌هاي اچ.تي.تي.پي لايه كاربرد انتقال مي‌دهند، اما محتويات اين بسته‌ها و نحوه تفسير‌ آنها براي برنامه‌هاي مختلف مي‌تواند متفاوت باشد.

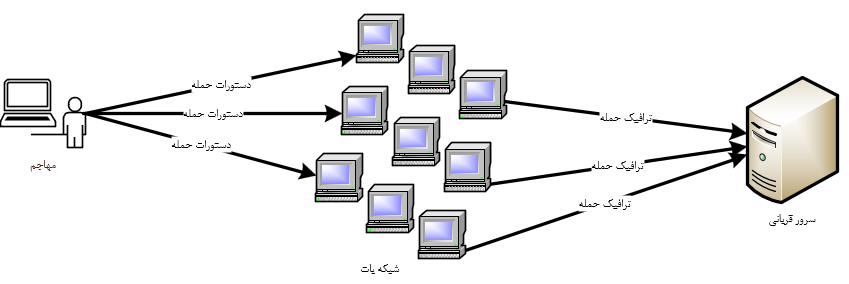
باتوجه به ویژگی‌های ذکر شده برای شبکه‌های پهن‌باند، واضح است که مدیریت و کنترل ترافیک در این شبکه‌ها به یکی از چالش‌های اصلی در زمینه شبکه‌های کامپیوتری تبدیل شده است.

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

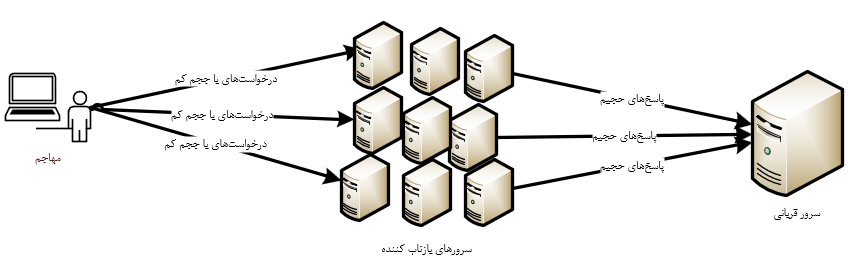
به مجموعه حملاتی که با هدف ممانعت از انجام یک خدمت صورت می‌پذیرند، حملات منع خدمت گفته می‌شود. این حملات با انگیزه‌های مختلفی نظیر ایجاد اختلال یا ممانعت از ارائه یک خدمت، از بین بردن اعتبار و مقبوليّت یک سازمان، آسیب زدن مالی و هدر دادن منابع یک سازمان، دستاوردهای سیاسی و ملّی، انگیزه مالی و یا قدرت‌نمایی مهاجمین و مواردی از این دست می‌تواند صورت پذیرد. هدف اصلی در حملات منع خدمت تولید ازدحام و اختلال در 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 فرد مزاحم ابتدا با پايش آسیب پذیری‌های دستگاه‌های مختلف موجود در شبکه اینترنت شروع به نفوذ به ماشین‌های عامل[[21]](#endnote-22) 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 آسیب‌پذیری‌های این سیستم‌ها را شناسایی کرد، می تواند این ماشین‌ها را با استفاده از یک برنامه مخرب مانند اسب تروجان[[22]](#endnote-23) 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 كنترل می‌شوند، ربات گفته می‌ شود و این مجموعه ربات‌ها که به آنها شبکه‌ بات[[23]](#endnote-24) گفته می‌شود، دستورات را از شخص مهاجم دریافت ‌می‌کنند. مهاجم می‌تواند حملات منع خدمت توزیع ‌شده در مقیاس بزرگ را انجام دهد تا یک سرویس یا شبکه قانونی را با ارسال یک فرمان کنترلی به دستگاه‌های شبکه بات برای ایجاد ترافیک زیاد بدون توجه به یک سرویس یا شبکه قانونی، با اختلال مواجه کند. در نتیجه، در مدّت زمان کوتاهی حجم زیادی از ترافیک را به سمت سرور و منابع آن هدایت می‌کنند که سرویس‌دهی آن یا رویکرد شبکه را برای پاسخگویی به کاربران قانونی با اختلال مواجه می‌کند. در صورت بروز حملات منع خدمت توزیع‌شده، رهگیری مبدأ حمله یعنی نقطه‌ای که حمله از آنجا شروع شده ‌است، دشوارتر و همچنین ترافیک ایجاد شده در اثر حمله بزرگتر و مخرّب‌تر می‌باشد.

در سال‌های اخیر، تعداد دستگاه‌های مبتنی بر اینترنت اشیا[[24]](#endnote-25) که به نسبت تجهیزات دیگر موجود در شبکه آسیب پذیرتر هستند، به سرعت در حال افزایش می‌باشد[3]. شبکه‌های بات تشکیل‌ شده 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[[25]](#endnote-26) دی.وای.ان[[26]](#endnote-27)، توسط شبكه‌اي از دستگاه‌های مبتنی بر اینترنت اشیا که توسط بدافزاری به نام میرای[[27]](#endnote-28) کنترل می‌شدند، مورد حمله قرار گرفت که در نهایت منجر به غیرقابل دسترس بودن منطقه وسیعی از خدمات (توییتر[[28]](#endnote-29)، اسپاتیفای[[29]](#endnote-30)، نتفلیکس[[30]](#endnote-31)، سی ان ان[[31]](#endnote-32) و...) برای کاربران در سواحل شرقی ایالات متحّده شد. مشکل دیگر دفاع در برابر حملات منع خدمت توزیع شده، بروز حملات تقویت بازتاب[[32]](#endnote-33) است. در سال ۲۰۱۸، گیتهاب[[33]](#endnote-34) با استفاده از آسیب‌پذیری پروتکل ممکچ[[34]](#endnote-35)، با انعکاس چند برابر بيش‌از 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[[35]](#endnote-36) حمله‌ای با حجم ترافيك پیک ۲.۳ ترابایت بر ثانیه را تجربه کردند. در ژوئیه ۲۰۲۱، شرکت ارائه‌‌دهنده خدمات تحویل محتوا[[36]](#endnote-37)ی کلودفلر[[37]](#endnote-38) در گزارشی به محافظت از یکی از مشتریان خود در برابر حمله منع خدمت توزیع شده نشأت گرفته‌ شده از یک شبکه بات در ابعاد جهانی توسط بدافزار میرای با ترافیک پیک ۱۷.۲ میلیون درخواست در ثانیه، اشاره کرد. یاندکس[[38]](#endnote-39)، 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[[39]](#endnote-40) بروزنشده[[40]](#endnote-41) سرچشمه می‌گرفت، مسدود کرده است.



1 حملات منع خدمت توزیع شده با استفاده از شبکه بات



2 حملات منع خدمت توزیع شده از نوع تقویت بازتابی

طبق خلاصه سالانه آکامی[[41]](#endnote-42) 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 می‌دهند. به عنوان مثال، در پایان ژوئیه ۲۰۲۰، پلیس فدرال آمریکا[[42]](#endnote-43) هشداری صادر کرد مبنی بر اینکه پروتکل برنامه‌های محدود شده[[43]](#endnote-44) و سایر پروتکل‌ها ممکن است برای انجام حملات منع خدمت توزیع شده مورد سوء استفاده قرار گیرند. حملات منع خدمت توزیع شده بر اساس بردارهای حمله[[44]](#endnote-45) جدید ممکن است تغییرات زیادی در ویژگی‌های آماری مانند سرعت بسته‌ها و فاصله بسته‌های مورد استفاده در مقایسه‌ با روش های سنتی داشته باشند، که اين امر باعث می‌شود روش‌های سنتی مقابله در برابر حملات مختلف کارایی لازم را نداشته باشند.[4]

1 گزارش و پیش‌بینی شرکت سیسکو[[45]](#endnote-46) از مجموع حملات منع خدمت توزیع شده[5]

### رویه کلی حملات منع خدمت توزیع‌ شده

با وجود اینکه انواع متفاوتی از حملات منع خدمت توزیع ‌شده وجود دارد که هرکدام با روشی منحصر به ‌فرد حمله را اجرا مي‌كنند، 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 اصلی، کنترل‌کننده حمله، عامل‌ها و قربانی. 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 توزیع‌ شده

اغلب حملات منع خدمت توزیع‌ شده 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 می‌دهند:

* 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 ارائه یک خدمت خاص در سطح شبکه است.

### دسته‌بندی حملات منع خدمت توزیع ‌شده

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 ازطريق پروتکل‌های موجود در آن لایه آغاز شده است[6]. 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 انجام ‌شده 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 مورد استفاده این دسته از حملات را به چهار زیر دسته کلی می‌توان قسمت کرد:
  + 1. حملات سیل‌آسا: در این دسته از حملات، مهاجم قصد اشباع پهناي باند قرباني با ارسال بسته‌های زیاد در سطح شبکه را 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[[46]](#endnote-47).
  + 3. حملات سیل‌آسا مبتنی بر بازتاب[[47]](#endnote-48): در 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: 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. از آنجایی ‌که 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 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[[48]](#endnote-49) 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

همانطور که در ویژگی‌های شبکه‌های پهن‌باند 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[[49]](#endnote-50): در این رویکرد تمامی بسته‌ها در یک پنجره زمانی را ضبط کرده و سپس آن‌ها را در زمان‌های بعدی پردازش می‌کنیم. مشکل این روش این می‌باشد که به دلیل ذخیره‌سازي اطلاعات در ابتدا و سپس ارسال آن به مراکز دیگر، دارای تأخیر در ارسال و پردازش و هزینه بسیار زیادی (برای ذخیره‌سازی) می‌باشد.
* پردازش جریانی[[50]](#endnote-51): اکثر راهکارهای ارائه 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[7]. 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[[51]](#endnote-52)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[[52]](#endnote-53) 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,…

Ɐꓰαi={( a1, v1)| a1Ɛ{0,1,…,u-1}, v1ƐR}

[u]= key space

تاپل‌ها، دوتایی‌هایی می‌باشند که شامل مقدار کلید و به‌روز‌رساني می‌باشند. آرایه‌ای 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 مسأله داده‌ جرياني که داریم، می‌توانند متفاوت باشند. دربحث پردازش بسته‌‌های دریافتی شبکه، جريان همان جریان ورودی و تاپل‌ها همان بسته‌ها می‌باشند که به‌طور مثال کلیدشان ۵ خصیصه (آدرس آي.پي[[53]](#endnote-54) مبدأ، آدرس مقصد، شماره پورت مبدأ، شماره پورت مقصد و پروتكل) 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.[8]

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

جريان ورودی را توالي از بسته‌هايي 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[9]:

* سایز هر جریان[[54]](#endnote-55): به دنبال یافتن سایز جریان یا تعداد بسته‌های دریافت شده متعلق به جریان ƒ می‌باشیم که آن را با nƒ نشان می‌دهیم. سایز تمامی بسته های دریافتی نیز می‌باشد.
* لحظه جریان[[55]](#endnote-56): در لحظه دلخواهي، به دنبال یافتن وضعیت جريان با استفاده از تابع g در لحظه [[56]](#endnote-57)g می‌باشیم، که به صورت زیر می‌تواند تعریف شود:

, ƒ [1, Ƒ]

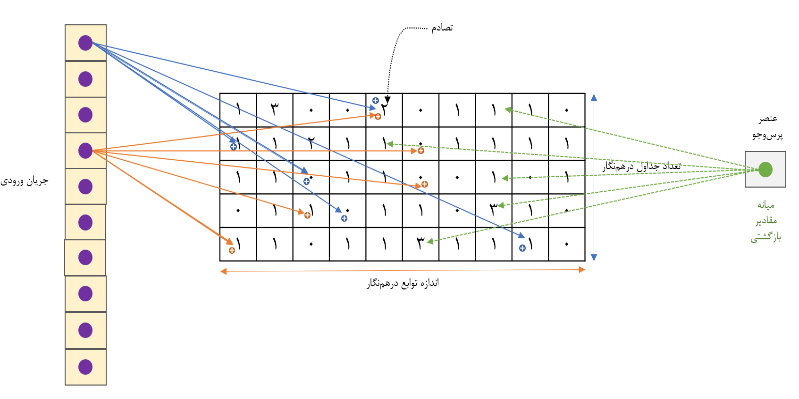
بسته به این که تابع به چه صورت تعریف شده باشد، وضعیت کلی ترافیک شبکه را می‌تواند به صورت عددی بیان کند.

* شاخص[[57]](#endnote-58): 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

برای حل مسائل جريان داده، راهکارهای متفاوتی می‌توان به‌ کار برد. 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[[58]](#endnote-59) گفته می‌شود.[10] نمونه‌‌برداری دقت پایینی خواهد داشت. لذا ما لازم داریم که تمامی داده‌ها را بررسی کنیم. اما بررسی همه بسته‌ها 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 ارائه شده است که هر کدام سعی در حل یکی از انواع مسائل داده جريان دارند. در ذیل به معرفی چند مورد از پر‌استفاده‌ترین آن‌ها خواهیم پرداخت:

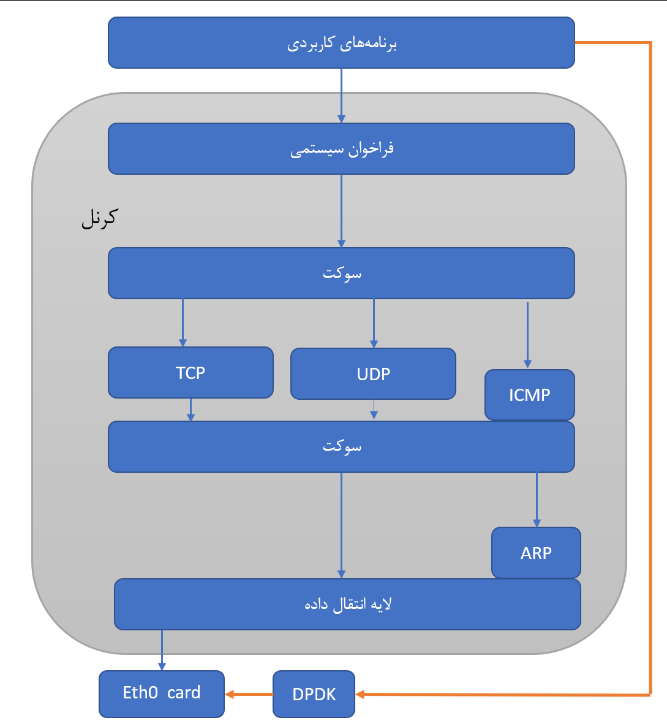
* انگاره شمارشي[[59]](#endnote-60): از یک جدول KxH تشکیل شده است که شامل K تا تابع درهم‌نگار[[60]](#endnote-61) مي‌‌باشد. H نیز اندازه توابع درهم‌نگار در یک سطر می‌باشد. این ساختار را الگوریتم‌های انگاره دیگر نیز استفاده می‌کنند. چون از توابع درهم‌نگار استفاده می‌کند لذا امکان تصادم[[61]](#endnote-62) وجود خواهد داشت‌ و مقاديري كه برمي‌گردانند تخميني خواهند بود و درنتيجه به آنها داده‌ساختارهای آماری احتمالاتی مي‌گویند. اما بايستي نرخ خطای قابل قبول و کرانداری ارائه دهند. از این الگوریتم براي يافتن جواب مسائل شاخص استفاده می‌شود.[11]

3 انگاره شمارشی

* انگاره شمارشي كمينه[[62]](#endnote-63): همانند انگاره شمارشي مي‌باشد اما سعي دارد مرتبه فضایی را کاهش دهد.[12]
* انگاره عمومي[[63]](#endnote-64): یک دسته جدیدي از انگاره‌ها با هدف ارائه داده‌ساختاری قابل استفاده برای حل تمامی انواع مسائل داده جريان مي‌باشند. يونيومان[[64]](#endnote-65) یکی از این الگوریتم‌ها می‌باشد.[13]

### پردازش سریع‌ بسته‌‌ها

هنگامی که یک بسته از طریق درگاه‌های یک سیستم دریافت می‌شود تا پردازش آن، مراحل مختلفی را طی خواهدکرد. بنا به کاربرد، بسته‌ها از دستگاه‌های مختلفی عبور داده می‌شوند. برمبنای پشته پروتکل تی‌.‌سی.پی‌/آی.پی[[65]](#endnote-66) که کرنل تمامی سیستم‌های عامل لینوکس از آن پشتیبانی می‌کنند، بسته‌ها از دریافت تا پردازش بخش‌های مختلف آن‌ها مراحل مختلفی را پشت ‌سر خواهند گذاشت و درنهایت در صورت نیاز بازارسال خواهند شد. در اینجا رویدادهای مهم در طی دریافت یک بسته توسط ماشین ذکر خواهد ‌شد.

* بسته توسط کارت شبکه[[66]](#endnote-67) ماشین ما دریافت می‌شود (وقفه کارت شبکه) .

4 مراحل ضبط و پردازش بسته

* کارت ‌شبکه از طریق دی.ام.ای[[67]](#endnote-68)، بسته را در فضای حافظه در یک بافری قرار می‌دهد.
* کارت ‌شبکه 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 مختلف (مثل بررسی آدرس‌ آی‌پی برای تطبیق با آدرس‌های متناظر لیست کنترل دسترسی) 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 کاربرد صورت می‌گیرد. 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.

دی‌.پی.دی‌.کی[[68]](#endnote-69) و ایکس.دی.پی[[69]](#endnote-70) از ابزار‌های موجود برای تسریع عملیات پردازش بسته می‌باشند. دی.پی.دی.کی ابزار نرم افزاری می‌باشد که در سال ۲۰۰۹ توسط اینتل[[70]](#endnote-71) توسعه داده شد. ولی بعدها به صورت یک پروژه متن باز[[71]](#endnote-72) درآمد. به طور خلاصه یک ابزار دورزدن کرنل[[72]](#endnote-73) در هنگام دریافت بسته در شبکه‌ می‌باشد که وقفه‌های مختلف مربوط به کرنل را حذف می‌کند و لذا تمام عملیات پردازش بسته را مي‌توان در سطح کاربر انجام داد و لذا عملیات دریافت و پردازش بسته را تا‌ حد خوبی می‌تواند تسریع ‌بخشد. هدف این تکنولوژی استفاده از قابلیت پردازش چندهسته‌ای پردازنده‌های معمولی ایکس۸۶[[73]](#endnote-74) برای بهبود سرعت پردازشی سرورها می‌باشد. بدین صورت ما نرخ پردازشی نزدیک به زمان استفاده از پردازنده‌های مخصوص سرور‌ها و یا مدار‌های مجتمع با کاربرد خاص[[74]](#endnote-75) و مدار مجتمع دیجیتال برنامه‌پذیر[[75]](#endnote-76) با صرف هزینه‌ای بسیار کمتر خواهیم داشت. از چندین پردازنده برای محاسبات مربوط به سطح داده و از بقیه هسته‌ها برای امور کنترلی و سرویس‌های دیگر استفاده می‌کند. به صورت جزئي‌تر چندین صف بر روی هر پورت تعریف می‌کند و هسته ها با حالت سرکشی[[76]](#endnote-77) به این صف‌ها الصاق می‌شوند. از این ابزار در کاربردهای مختلفی در مواقعی که حجم زیادی از ورودی/خروجی داریم از حیطه شبکه و امنيّت آن، پردازش و سوییچینگ در ابرها، بهبود کارایی حافظه‌ها، توابع مجازی شبکه[[77]](#endnote-78)، 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 فشرده‌سازی به کمک رابط‌های برنامه‌نویسی‌اش نیز ارائه می‌دهد.[14]

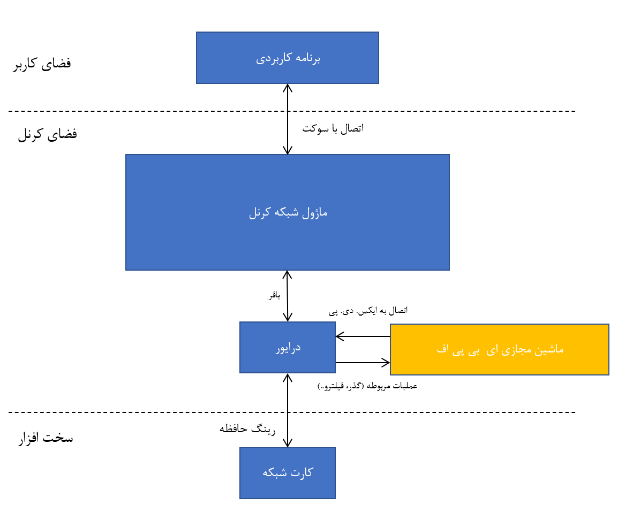
ایکس.دی.پی یکی از کامپوننت‌های جدید کرنل می‌باشد که پردازش بسته را به صورت بالایی بهبود می‌بخشد. روش‌های مثل دی.‌پی.دی. کی کرنل را دور مي‌زنند و تمام عملیات پردازش بسته در فضای کاربر صورت مي‌گرفت. همچنین کارت ‌شبکه را توسط یک درایور سطح کاربر مي‌بایست کنترل ‌نمود. پردازش شبکه در سطح کاربر با وجود مزاياي زيادش معایب زیر را نيز به همراه خواهد داشت:

* به دليل اينکه 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 را، پیاده‌سازی کنند.
* برنامه‌ها به صورت ایزوله اجرا می‌شوند که نحوه تعامل آنها با دیگر بخش‌های سیستم‌عامل را دشوار می‌کند.

به طور خلاصه ایکس. دی. پی، برنامه‌‌های شبکه سطح کاربر (فیلتر، نگاشت، مسیریابی و...) را به جای انتقال به سطح کاربر، به فضاي کرنل می‌برد. ایکس.دی.پی به ما این امکان را می دهد که به محض ورود بسته به کارت ‌شبکه و پیش از حرکت به سمت زیرسیستم شبکه‌ی هسته، برنامه خود را اجرا کنیم که منجر به افزایش قابل توجّه سرعت پردازش بسته می‌شود. اجرای برنامه در سطح کرنل با استفاده از بی. پی. اف[[78]](#endnote-79) میسر می‌شود.[15]

بی.پی.اف یک ماشین مجازی است که تنها مخصوص پردازش فیلترینگ می‌باشد. یکی از ابزارهایی که از بی.پی.اف استفاده می‌کند، تی‌سی‌پی‌دامپ[[79]](#endnote-80) می‌باشد. عبارت فیلتر مربوطه توسط یک کامپایلر به بایت‌کد[[80]](#endnote-81) بی.پی.اف تبدیل خواهد شد. از آنجایی که بی.پی.اف یک ماشین مجازی می‌باشد، محیطی را به منظور اجرای برنامه‌ها در آن که علاوه بر بایت‌کد شامل یک مدل حافظه مبتنی بر بسته (دستورالعمل‌های بارگذاری به طور ضمنی بر روی بسته موردنظر انجام می‌شود) ، ثبات‌ها[[81]](#endnote-82) (A و X یعنی انباشتگر[[82]](#endnote-83) و ثبات اندیس[[83]](#endnote-84)) ، یک حافظه موقت و یک شمارنده برنامه[[84]](#endnote-85) ضمنی نيز می‌باشد را، تعریف می‌کند. کرنل لینوکس از نسخه ۲.۵ به بعد از بی.پی.اف پشتیبانی می‌کند. در سال ۲۰۱۱، مفسر بی.پی.اف به یک کامپایلر درجا[[85]](#endnote-86) تغییر داده شد. این کار باعث شد که کرنل به جای تفسیر برنامه‌های بی.پی.اف، قادر باشد که آن‌ها را به یک معماری هدف میپس[[86]](#endnote-87)، ایکس‌۸۶، آرم[[87]](#endnote-88) و... تبدیل کند. این‌ امر به معرفی بی.پی.اف توزیع یافته[[88]](#endnote-89) در سال ۲۰۱۴ و کنار گذاشته ‌شدن بی.پی.اف سنتی منجر شد. ویژگی‌های جدید شامل موارد زیر می‌باشد:

* از ویژگی‌های معماری ۶۴-بیتی مثل رجیستر‌ها و تعداد آن‌ها و کد‌های عملیاتی[[89]](#endnote-90) بیشتر بهره مي‌برد.
* از زیرسیستم شبکه جدا شده است و امکان استفاده در کاربرد‌های دیگر میسّر می‌شود.
* مپ‌ها به عنوان راهی برای تبادل داده بین سطح کاربر و کرنل مورد استفاده قرار می‌گیرند.
* استفاده از توابع کمکی که در سطح کرنل اجرا می‌شوند. امکان صدازدن فراخوان سيستمي[[90]](#endnote-91) در برنامه‌های بی.پی.اف نیز وجود دارد.
* زنجیره سازی تعداد برنامه بیشتر بی.پی.اف نيز امكان‌پذير خواهد بود.[16]

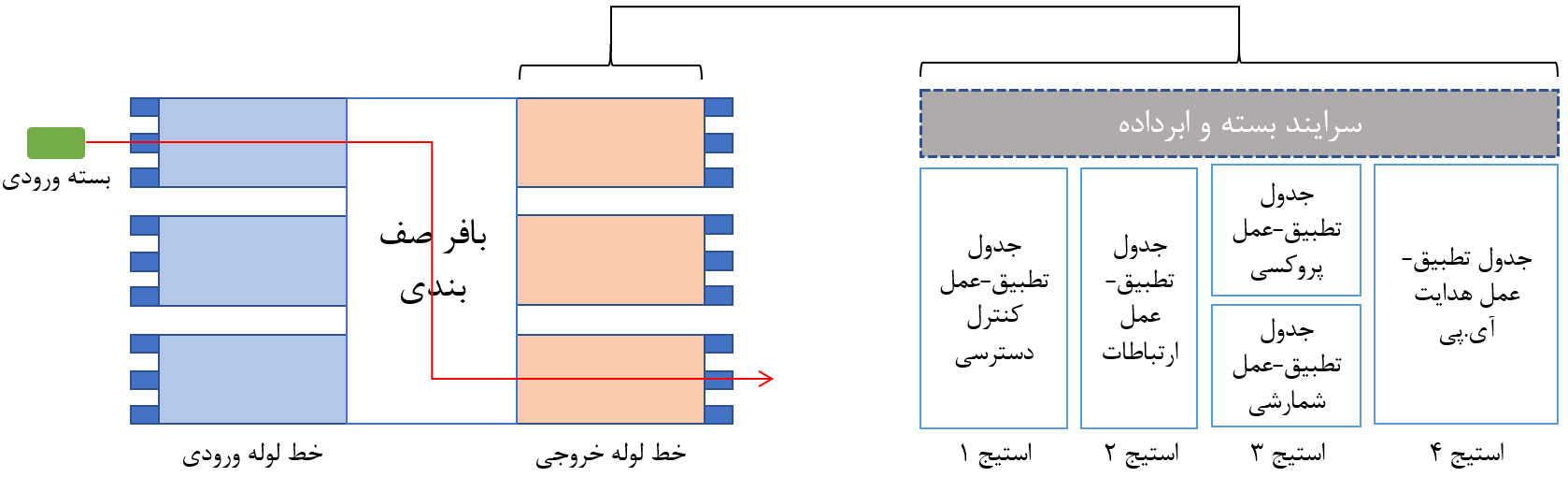
برخی از صف‌های کارت ‌شبکه هنوز به هسته متصل هستند، در حالی که برخی دیگر به یک برنامه فضای کاربر متصل هستند که در مورد حذف‌ شدن یا نشدن یک بسته تصمیم می‌گیرد. با این کار، میزان ترافیکی که به زیرسیستم شبکه هسته می‌رسد به میزان قابل توجهی کاهش می‌یابد. برای این کار بایستی یک نقطه بازرسی[[91]](#endnote-92) در پشته کرنل تعریف کرد که هرگاه بسته‌ای در کارت ‌شبکه دریافت شد، آن را به فضای کاربر بفرستد که درآنجا تصمیم می‌گیرد که بسته دور انداخته شود[[92]](#endnote-93) یا اجازه عبور از لایه‌های بالاتر پشته را صادر کند. لذا نیاز به مکانیزمی بود که امکان اجرای کدهای سطح کاربر را در کرنل فراهم کند. به همین دلیل از بی.پی.اف توزیع یافته استفاده شد.

5 ایکس دی پی بر روی کرنل

ایکس.دی.پی بسته‌های دریافتی را به برنامه بی.پی.اف هدایت می‌کند. در آنجا می‌توان بسته‌ها را ویرایش، هدايت[[93]](#endnote-94) کرد. همچنین از توابع کمکی می‌توان برای انجام محاسبات و پردازش بسته‌ها بدون نیاز به فراخوان سیستمی استفاده کرد. و همچنین با استفاده از داده‌ساختار‌های مپ امکان ذخیره داده‌ها به صورت دائمي را خواهيم داشت. در نهايت با استفاده از ویژگی‌های از پیش تعبیه‌شده در ایکس.دی.پی می‌توان عمل مورد نظر را بر روی بسته انجام داد.

### سوییچ‌های برنامه‌پذیر

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، یکی از مشکلات روش‌های پیشین بود. این روش با تأخیر زیادی همراه است و همچنین می‌تواند یک نقطه آسیب پذیر واحد برای مهاجمین فراهم کند. اما امروزه با معرفی سوییچ‌های برنامه پذیر[[94]](#endnote-95)، سوییچ‌های معمولی نیز با استفاده از برنامه‌هایی که بر روی آنها با استفاده از زبان‌هایی مثل p4 می‌نویسیم توانایی پردازش داده را تا حد زیادی خواهند داشت. یک سوییچ برنامه پذیر مبتنی بر مدار‌های مجتمع با کاربرد خاص، چندین خط لوله شامل درگاه‌های ورودی و خروجی را شامل می‌شود. و بسته‌ها استیج‌های مختلف در طول خط لوله را برای پردازش سپری می‌کنند. هر کدام از این استیج‌ها نیز منابع اختصاصی خود یعنی: ثبات‌ها برای ذخیره‌سازی، جداول تطبیق-عمل و واحد‌های منطق ریاضی به منظور پردازش را شامل می‌شوند. توسط زبان پی‌۴ امکان شخصی‌سازی جداول تطبیق-عمل به منظور انجام تغییر روی بسته‌ها میسر خواهد بود. در مجموع سوییچ‌های برنامه‌پذیر مبتنی بر مدار‌های مجتمع با کاربرد خاص دو برتری بهینه ‌بودن سرعت پردازشی به نسبت هزینه مصرفی و مصرف برق و انعطاف‌پذیری در برابر حملات جدید را در مقایسه با سخت‌افزار‌های دیگر ارائه مي‌دهند. [17]



6 معماري سوييچ برنامه‌پذير

# کارهای ‌پیشین

**به‌طورکلی پژوهش‌های انجام‌شده در حوزه حملات منع خدمت توزیع‌شده را می‌توان در سه دسته پیشگیری از وقوع حمله، تشخیص حمله و کاهش اثر حمله[[95]](#endnote-96) تقسیم‌بندی کرد. از آنجایی‌که تمرکز این گزارش بر مقالات موجود در حوزه تشخیص حملات منع خدمت توزیع‌شده می‌باشد،** در ادامه به بررسی چند روش اخيراً معرفی‌شده تشخیص حملات منع خدمت توزیع ‌شده در شبکه‌های کامپیوتری می‎‌پردازیم. علاوه بر شيوه‌ي دسته‌بندي راهكار‌هاي مختلف كه در ادامه استفاده مي‌كنيم، الگوریتم‌های تشخیص را می‌توان بر اساس اینکه‌ در کدام ناحیه از شبکه سعی به تشخیص عامل متخاصم دارند نیز طبقه بندی کرد، که شامل سه گروه می‌شوند:

* شناسایی در مبدأ: از توانایی تشخیص همه حملات برخوردار نمی‌باشند.
* شناسایی در مقصد(قربانی): نیاز به منابع بیشتری دارند و ممکن است با تأخیر هم همراه باشند.
* شناسایی در مسیر‌های میانی[[96]](#endnote-97).

### روش‌های مبتنی بر امضا

آنتروپی[[97]](#endnote-98) معیاری است که برای اندازه‌گیری میزان تصادفی بودن یک ویژگی در یک دوره زمانی معین استفاده می‌شود. روش‌های مبتنی بر آنتروپی به‌عنوان یک رویکرد مؤثر برای محاسبه تصادفی از یک مجموعه داده طراحي‌ شده‌اند. به‌طورکلی مقادیر بالای آنتروپی نشان‌دهنده توزیع پراکنده‌تر ویژگی در دادگان[[98]](#endnote-99) موجود است و مقادیر پایین آنتروپی نشان‌دهنده نامتوازن بودن یک توزیع است یعنی برخی مقادیر ویژگی موردنظر، فراوانی بیشتری نسبت به سایر مقادیر دارند. از این معيار برای تشخیص ناهنجاری گسترده در سامانه‌های سنتی تشخیص نفوذ[[99]](#endnote-100) استفاده ‌شده‌ است. به‌منظور تشخیص حملات منع خدمت، آنتروپیِ جریان شبکه را می‌توان با استفاده از چندین ویژگی مانند جریان شبکه، آدرس آی.‌پی مبدأُ و مقصد بسته‌ها و یا تعداد بسته‌های موجود در یک جریان محاسبه کرد. سپس با یک حد آستانه از پیش تعریف ‌شده، مقایسه مي‌كنيم و در مورد عادي یا غیرعادي بودن جریان بررسی‌شده، تصمیم‌گیری مي‌كنيم. یکی از مهم‌ترین مزیت‌های این روش داشتن سربار محاسباتی کم می‌باشد.

* تقسيم‌كننده و كاهنده ترافيك حملات منع ‌خدمت توزيع‌شده مبتني بر امضا با استفاده از سوييچ‌هاي برنامه‌پذير سطح‌ داده: در روش ارائه‌شده در سال 2021، ديموليانس و همكاران سعی می‌کنند امضاهای مهاجم را بدست آورند و تعداد حداقل بهینه خط قوانین از آنها را بسازند. مشکل روش عدم کارایی در شناسایی حملات متنوع می‌باشد. همچنين در مورد نحوه ياددهي مجدد مدل‌هاي طبقه‌بندي كننده توضيحي ارائه نمي‌دهد[18].
* روش تشخيص مبتني بر جريان در شبكه‌هاي با سرعت بالا براي شناسايي حملات با توليد امضاي سازگار با اسنورت[[100]](#endnote-101): در روش ارائه شده در سال 2020 توسط ارلاكر و همكاران، از دسته‌بندي جريان مبتني ‌بر آي‌.پي.فيكس[[101]](#endnote-102) استفاده مي‌كند، كه در اين‌صورت اطلاعات بيشتري علاوه بر اطلاعات آماري متداول مي‌تواند استخراج كند، همچنين با استفاده از برخي روش‌ها امكان بررسي محتواي داده‌اي نيز ميسر خواهد بود.[19]

### روش‌های مبتنی بر مدل‌سازي

اين دسته از روش‌ها با ضبط‌كردن و بررسي ترافيك عادي شبكه در يك بازه‌ زماني، رفتار عادي شبكه را شبيه سازي يا به اصطلاح مدل مي‌كنند و هرگونه رفتار مغاير با اين مدل يا اصطلاحاً آنومالي[[102]](#endnote-103) را به عنوان حمله در نظر مي‌گيرند. یادگیری ماشین به‌عنوان یکی از روش‌های کارآمد مبتنی بر مدل‌سازی می‌باشد، که امروزه به صورت گسترده‌ای مورد استقبال پژوهشگران قرارگرفته است. در حوزه تشخیص حملات منع خدمت توزیع‌شده نیز از این روش استفاده می‌شود. گونه‌های مختلفی از الگوریتم‌های یادگیری ماشين 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 مورد استفاده قرار می‌گیرند.

* رویکرد مبتنی بر سوییچ‌‌های برنامه‌پذیر برای شناسایی و مقابله با حملات منع خدمت توزیع‌شده: این روش به نام جاکن در سال ۲۰۲۱ توسط لیو و همکاران با استفاده از انگاره‌های عمومی و پیاده سازی آنها روی سوییچ‌های برنامه‌پذیر به منظور جمع‌‌آوری اطلاعات توسط همین دستگاه‌ها، ارائه شد. یک کنترل‌کننده مرکزی از این اطلاعات برای تشخیص حملات استفاده می‌کند. همچنین الکوریتم‌هایی به منظور رفع مخاطره برروی این سوییچ‌ها می‌توان پیاده کرد. به دلیل این که با استفاده از زبان پی‌[[103]](#endnote-104)۴، الگوریتم‌های تشخیص و رفع مخاطره را پیاده می‌کنیم، لذا این روش مبتنی بر معماری خاصی از سوییچ‌ها نمی‌باشد. عدم وارسي محتواي كامل بسته‌ها و استفاده از وارسي‌كننده عميق بسته[[104]](#endnote-105)، مشكل اصلي جاكن مي‌باشد. به همین دلیل به بحث تنوع پروتکلی و اینکه مقادير آستانه‌ برای برنامه‌های کاربردی مختلف می‌تواند متفاوت باشد، اشاره‌ای نکرده است.[20]
* روش بلادرنگ تطبيق‌پذير مبتني بر انگاره مخصوص شبكه‌هاي ارائه دهنده خدمات اينترنتي: آر. تي. ‌سد در سال 2021 توسط شي و همكاران پيشنهاد شد. از نامتواازن مقادير يك ويژگی‌ برای یک آدرس مقصد مشخص، قربانی‌ بودن آن را تشخیص می‌دهد. اما در مورد نحوه انتخاب این ویژگی‌ها برای برنامه‌های کاربردی مختلف و البته انجام این‌کار به صورت پویا صحبتی نمی‌کند. در مورد محل پیاده‌سازی این الگوریتم‌ها توضیحی نمی‌دهد. به دلیل استفاده از انگاره‌ها، آر.تي.‌سد از نظر مرتبه فضایی بسیار بهینه می‌باشد.[4]
* دفاع هوشمند: روشي به نام دفاع هوشمند در سال 2022 توسط ماينني و همكاران ارائه شد كه از شبکه‌های عصبی عمیق در سمت لبه مشتری و شبکه‌های عصبی عمیق با الگوریتم‌های پیشرفته‌تر در سمت فراهم کننده اینترنت برای شناسایی حملات استفاده می‌کند. اما مشکل این روش، عدم ارائه راهكاري بهينه به منظور آموزش مجدد شبكه‌ها در شبكه‌هاي پهن‌باند مي‌باشد. [21]
* روش بلادرنگ و قابل اعتماد مبتني بر آنومالي براي تشخيص رخنه در شبكه‌هاي با سرعت بالا: با درنظرگرفتن بسته‌‌ها به عنوان جریان، ویژگی‌های آن را استخراج می‌کند و سپس از روی آنها تشخیص می‌دهد. يك بخش اعتماد سازي دارد كه از ميزان قابل اعتماد بودن كلاس‌بندي ارائه شده توسط طبقه‌بندي كننده را بررسي مي‌كند و اگر از مقدار حداقلي پايين بود، به كمك يك شخص مدير آن را برچسب‌گذاري مي‌كند و سپس مدل طبقه‌بندي كننده را به صورت افزايشي به روز مي‌كند. به دليل مداخله انسان برای برچسب‌گذاري برخی جریان‌ها، در شبكه‌هاي پهن‌باند با تنوع پروتكلي بالا به مشكل خواهد خورد و سربار بالا و دقت پايين خواهد داشت.[22]

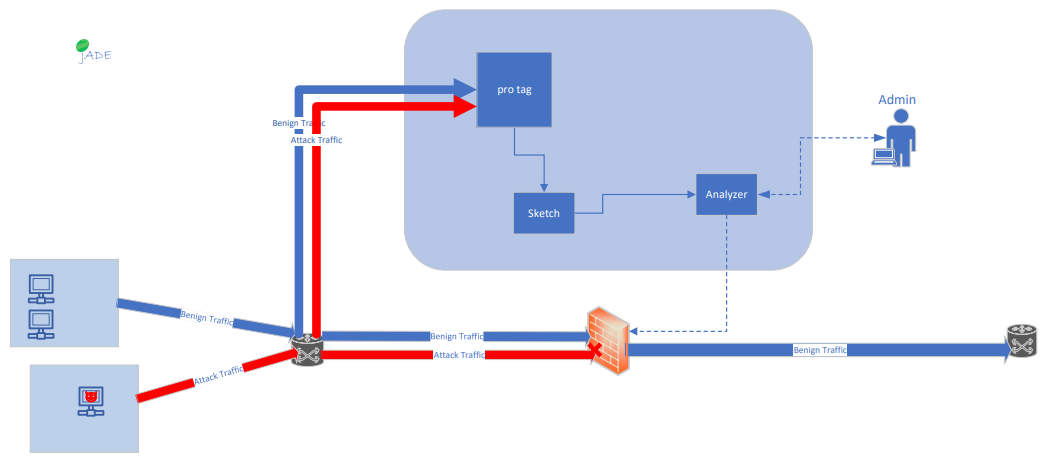
# روش پیشنهادی

در بخش قبل برخی روش‌های مبتنی بر امضا و مدل‌سازي 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 خاص مثلاً اچ.‌‌ تي.‌تي‌.پي‌ 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 جمع‌‌آوري مي‌كنند، ترافیک نامتعارف را با استفاده از رويكرد‌هاي مبتني بر محاسبات آماري يا با استفاده از رويكرد‌هاي مدل‌سازي و تشخيص آنومالي، مي‌توانند تشخيص دهند. اما عدم سازگاري با تنّوع پروتکلی برنامه‌هاي كاربردي مختلف، از مشكلات اين روش‌ها مي‌باشد و در هنگام تشخيص حملات دچار خطا مي‌شوند. 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 روش‌هايی مثل وارسي بسته عميق یا یادگیری ماشین استفاده می‌شود و سپس با استفاده از اطلاعات آنها ترافیک را دسته‌بندی کرده و در هر کدام برای تشخیص الگو‌های نامتعارف، تنظیمات متفاوتی(مثل مقادیر آستانه متفاوت برای حجم بسته‌‌ها) به کار می‌برند. اما در شبکه‌های پهن‌باند با مشکلی به نام تنوع ترافیکی بالا مواجه هستیم و از طرفی با توجه به نرخ‌ بالاي توليد ترافیک بایستی در کمترین زمان ممکن، کم ‌‌هزینه‌ترین راهکار را ارائه دهیم. راهکارهای مبتنی بر یادگیری ماشین و استفاده از وارسی‌کننده عمیق بسته، سربار محاسباتی زیاد دارند.

همانطور كه گفته شد، نکته‌ای که در پژوهش های پیشین نادیده گرفته می‌شد، مربوط به مولفه سوم شبکه‌های پهن‌باند 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 سرآيندها و محتوا می‌باشند را تنها درنظر گرفته بودند. لذا روشی كه ارائه می‌دهیم تمامی این سه مورد را با تمرکز بیشتر بر روی ویژگی سوم به عنوان مسئله اصلی را هدف قرار می‌دهد. بدین منظور روشی که ارائه می‌دهیم از ویژگی‌ پردازش جامع برخوردار می‌باشد، یعنی تمامی بسته‌ها را یک و تنها یکبار بررسی می‌کند. و بدین صورت روشی بسیار سریع و با دقت بالا و تطبیق‌پذیر با مشخصات ترافیکی ارائه می‌دهیم (علاوه بر معیارهای متداولی مثل سرعت-نرخ‌گذر بالا و تأخیر 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.



7 شمای کلی از روش پیشنهادی

روال کاری ما بدین صورت خواهد بود كه با استفاده از روش ارائه شده در مقاله آكوپي و همچنين استفاده از يك ماژول وارسی‌کننده عمیق بسته، جریان‌ها را برچسب‌گذاري مي‌كنيم و جریان‌های شبیه به هم از نظر رفتار را در یک گروه قرار مي‌دهيم و این اطلاعات را در داده‌ساختار‌های انگاره که بر روی سوییچ‌های برنامه‌پذیر می‌باشند و توسط مدیر شبکه کنترل می‌شوند، ذخیره می‌کنیم. این اطلاعات را برای هر برنامه‌ کاربردی 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 و یا برنامه‌ كاربردي در بازه‌های زمانی مختلف، این اطلاعات را با مقادیر آستانه‌ای که از قبل به دست آورده و نشان‌دهنده حداکثر بی‌نظمی قابل چشم‌پوشی در شبکه می‌باشد، مقایسه می‌کند و در صورت مشاهده مغایرت آن جریان را به عنوان یک حمله تشخیص داده و سعی می‌کند امضای معادل آن را تولید ‌کند و به عنوان خروجی به یک دیوار آتش ارسال کند.

# نتيجه‌گيري

در این نوشتار به مرور مفاهیم اولیه مرتبط با حملات منع خدمت توزیع ‌شده و انواع آن، شبکه‌های پهن‌باند و ویژگی‌های این شبکه، روش‌ها و الگوریتم‌های پردازش و معرفی مفاهیم و واژه‌های به کاررفته در اين‌ زمينه، مثل محاسبات و مسائل داده جريان پرداختيم. سپس برخی پژوهش‌های انجام‌شده درزمینه‌ی تشخیص حملات منع خدمت در شبکه‌های پهن‌باند مورد بررسی قرار گرفت و مشکلات پیاده‌سازی و عملکردی و چالش‌های حل‌نشده آنها بیان شد. در آخر روش پیشنهادی سریع با دقت بالا و بهینه از نظر میزان مصرف منابع و سازگار با تنوع ترافیکی به منظور شناسایی حملات منع خدمت توزیع‌شده در بستر شبکه‌‌های پهن‌باند به صورت مختصر توضيح‌ 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 |

# ۶. کتاب‌نامه

[1] M. Noferesti and R. Jalili, ‘ACoPE: An adaptive semi-supervised learning approach for complex-policy enforcement in high-bandwidth networks’, *Computer Networks*, vol. 166, p. 106943, Jan. 2020, doi: 10.1016/j.comnet.2019.106943.

[2] R. K. Deka, D. K. Bhattacharyya, and J. K. Kalita, ‘Active learning to detect DDoS attack using ranked features’, *Computer Communications*, vol. 145, pp. 203–222, Sep. 2019, doi: 10.1016/j.comcom.2019.06.010.

[3] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy, and A. A. Abd El-Latif, ‘Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities’, *Security and Communication Networks*, vol. 2021, pp. 1–13, Apr. 2021, doi: 10.1155/2021/5597679.

[4] H. Shi, G. Cheng, Y. Hu, F. Wang, and H. Ding, ‘RT-SAD: Real-Time Sketch-Based Adaptive DDoS Detection for ISP Network’, *Security and Communication Networks*, vol. 2021, pp. 1–10, Jul. 2021, doi: 10.1155/2021/9409473.

[5] K. Machap and H. Qiang, ‘Evaluating firewall tools and techniques in enhancing network security’, vol. 6, pp. 1–4, Jan. 2022.

[6] A. Cheema, M. Tariq, A. Hafiz, M. M. Khan, F. Ahmad, and M. Anwar, ‘Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review’, *Security and Communication Networks*, vol. 2022, pp. 1–15, May 2022, doi: 10.1155/2022/8379532.

[7] B. Zhao, X. Li, B. Tian, Z. Mei, and W. Wu, ‘DHS: Adaptive Memory Layout Organization of Sketch Slots for Fast and Accurate Data Stream Processing’, in *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*, Virtual Event Singapore, Aug. 2021, pp. 2285–2293. doi: 10.1145/3447548.3467353.

[8] B. Krishnamurthy, S. Sen, Y. Zhang, and Y. Chen, ‘Sketch-based change detection: methods, evaluation, and applications’, in *Proceedings of the 2003 ACM SIGCOMM conference on Internet measurement - IMC ’03*, Miami Beach, FL, USA, 2003, p. 234. doi: 10.1145/948205.948236.

[9] Q. Xiao, Z. Tang, and S. Chen, ‘Universal Online Sketch for Tracking Heavy Hitters and Estimating Moments of Data Streams’, in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, Toronto, ON, Canada, Jul. 2020, pp. 974–983. doi: 10.1109/INFOCOM41043.2020.9155454.

[10] V. Sivaraman, S. Narayana, O. Rottenstreich, S. Muthukrishnan, and J. Rexford, ‘Heavy-Hitter Detection Entirely in the Data Plane’, in *Proceedings of the Symposium on SDN Research*, Santa Clara CA USA, Apr. 2017, pp. 164–176. doi: 10.1145/3050220.3063772.

[11] M. Charikar, K. Chen, and M. Farach-Colton, ‘Finding Frequent Items in Data Streams’, in *Automata, Languages and Programming*, vol. 2380, P. Widmayer, S. Eidenbenz, F. Triguero, R. Morales, R. Conejo, and M. Hennessy, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 693–703. doi: 10.1007/3-540-45465-9\_59.

[12] G. Cormode and S. Muthukrishnan, ‘An improved data stream summary: the count-min sketch and its applications’, *Journal of Algorithms*, vol. 55, no. 1, pp. 58–75, Apr. 2005, doi: 10.1016/j.jalgor.2003.12.001.

[13] Z. Liu, A. Manousis, G. Vorsanger, V. Sekar, and V. Braverman, ‘One Sketch to Rule Them All: Rethinking Network Flow Monitoring with UnivMon’, in *Proceedings of the 2016 ACM SIGCOMM Conference*, Florianopolis Brazil, Aug. 2016, pp. 101–114. doi: 10.1145/2934872.2934906.

[14] H. Zhu, *Data Plane Development Kit (DPDK): A Software Optimization Guide to the User Space-based Network Applications*, 1st Edition. CRC Press, 2020.

[15] T. Høiland-Jørgensen *et al.*, ‘The eXpress data path: fast programmable packet processing in the operating system kernel’, in *Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies*, Heraklion Greece, Dec. 2018, pp. 54–66. doi: 10.1145/3281411.3281443.

[16] M. Fleming, ‘A thorough introduction to eBPF’, *LWN.net Linux Weekly News*, Dec. 02, 2017. https://lwn.net/Articles/740157/

[17] M. Zhang *et al.*, ‘Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches’, in *Proceedings 2020 Network and Distributed System Security Symposium*, San Diego, CA, 2020. doi: 10.14722/ndss.2020.24007.

[18] M. Dimolianis, A. Pavlidis, and V. Maglaris, ‘Signature-Based Traffic Classification and Mitigation for DDoS Attacks Using Programmable Network Data Planes’, *IEEE Access*, vol. 9, pp. 113061–113076, 2021, doi: 10.1109/ACCESS.2021.3104115.

[19] F. Erlacher and F. Dressler, ‘On High-Speed Flow-Based Intrusion Detection Using Snort-Compatible Signatures’, *IEEE Trans. Dependable and Secure Comput.*, vol. 19, no. 1, pp. 495–506, Jan. 2022, doi: 10.1109/TDSC.2020.2973992.

[20] Z. Liu *et al.*, ‘Jaqen: A ${$High-Performance$}$${$Switch-Native$}$ Approach for Detecting and Mitigating Volumetric ${$DDoS$}$ Attacks with Programmable Switches’, in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 3829–3846.

[21] S. Myneni, A. Chowdhary, D. Huang, and A. Alshamrani, ‘SmartDefense: A distributed deep defense against DDoS attacks with edge computing’, *Computer Networks*, vol. 209, p. 108874, May 2022, doi: 10.1016/j.comnet.2022.108874.

[22] E. Viegas, A. Santin, A. Bessani, and N. Neves, ‘BigFlow: Real-time and reliable anomaly-based intrusion detection for high-speed networks’, *Future Generation Computer Systems*, vol. 93, pp. 473–485, Apr. 2019, doi: 10.1016/j.future.2018.09.051.

# ۷. واژه‌نامه

1. Application [↑](#endnote-ref-2)
2. HTTP/S [↑](#endnote-ref-3)
3. Distributed Denial Of Service attack (DDOS) [↑](#endnote-ref-4)
4. Availability [↑](#endnote-ref-5)
5. High-Bandwidth [↑](#endnote-ref-6)
6. Monitor [↑](#endnote-ref-7)
7. Comprehensive Processing [↑](#endnote-ref-8)
8. Adaptive Learning [↑](#endnote-ref-9)
9. Drop Rate [↑](#endnote-ref-10)
10. Internet Service Provider [↑](#endnote-ref-11)
11. Client [↑](#endnote-ref-12)
12. Denial Of Service [↑](#endnote-ref-13)
13. Server [↑](#endnote-ref-14)
14. Attacker [↑](#endnote-ref-15)
15. Flash Coward [↑](#endnote-ref-16)
16. Data Streaming [↑](#endnote-ref-17)
17. Sketch [↑](#endnote-ref-18)
18. 5G [↑](#endnote-ref-19)
19. Payload [↑](#endnote-ref-20)
20. Header [↑](#endnote-ref-21)
21. Agent Machine [↑](#endnote-ref-22)
22. Trojan Horse Malware [↑](#endnote-ref-23)
23. Botnet [↑](#endnote-ref-24)
24. Internet Of Things (IOT) [↑](#endnote-ref-25)
25. Domain Name Service Provider [↑](#endnote-ref-26)
26. DYN inc. [↑](#endnote-ref-27)
27. Mirai Malware [↑](#endnote-ref-28)
28. Twitter [↑](#endnote-ref-29)
29. Spotify [↑](#endnote-ref-30)
30. Netflix [↑](#endnote-ref-31)
31. CNN [↑](#endnote-ref-32)
32. Amplification DDoS Attack [↑](#endnote-ref-33)
33. GitHub [↑](#endnote-ref-34)
34. Memcached Distributed Caching Memory System [↑](#endnote-ref-35)
35. Amazon Web Services [↑](#endnote-ref-36)
36. Content Delivery Network (CDN) [↑](#endnote-ref-37)
37. Cloudflare [↑](#endnote-ref-38)
38. Yandex [↑](#endnote-ref-39)
39. MikroTik [↑](#endnote-ref-40)
40. Unpatched [↑](#endnote-ref-41)
41. Akamai Technologies [↑](#endnote-ref-42)
42. FBI [↑](#endnote-ref-43)
43. Constrained Application Protocol(CAP) [↑](#endnote-ref-44)
44. Attack Vector [↑](#endnote-ref-45)
45. CISCO [↑](#endnote-ref-46)
46. TCP 3-Way Handshake [↑](#endnote-ref-47)
47. Reflection Attack [↑](#endnote-ref-48)
48. Session [↑](#endnote-ref-49)
49. Batch Processing [↑](#endnote-ref-50)
50. Stream Processing [↑](#endnote-ref-51)
51. Line Rate Processing [↑](#endnote-ref-52)
52. Turnstile Model [↑](#endnote-ref-53)
53. Internet Protocol (IP) [↑](#endnote-ref-54)
54. Per Flow Size [↑](#endnote-ref-55)
55. Flow Moment [↑](#endnote-ref-56)
56. Moment-g [↑](#endnote-ref-57)
57. Heavy Hitter [↑](#endnote-ref-58)
58. Sampling [↑](#endnote-ref-59)
59. Count-Sketch [↑](#endnote-ref-60)
60. Hash Function [↑](#endnote-ref-61)
61. Hash Collision [↑](#endnote-ref-62)
62. Count Min Sketch [↑](#endnote-ref-63)
63. Universal Sketch [↑](#endnote-ref-64)
64. Univmon [↑](#endnote-ref-65)
65. TCP/IP Stack [↑](#endnote-ref-66)
66. Network Interface Card (NIC) [↑](#endnote-ref-67)
67. Direct Memory Access (DMA) [↑](#endnote-ref-68)
68. Data Plane Development Kit(DPDK) [↑](#endnote-ref-69)
69. eXpress Data Path(XDP) [↑](#endnote-ref-70)
70. Intel [↑](#endnote-ref-71)
71. Open Source Project [↑](#endnote-ref-72)
72. Kernel Bypass [↑](#endnote-ref-73)
73. X86 Processor Architecture [↑](#endnote-ref-74)
74. Application Specific Integrated Circuit (ASIC) [↑](#endnote-ref-75)
75. Field Programmable Gate Array (FPGA) [↑](#endnote-ref-76)
76. Polling Mode [↑](#endnote-ref-77)
77. Network Function Virtualization(NFV) [↑](#endnote-ref-78)
78. Berkely Packet Filter (BPF) [↑](#endnote-ref-79)
79. Tcpdump [↑](#endnote-ref-80)
80. Bytecode [↑](#endnote-ref-81)
81. Register [↑](#endnote-ref-82)
82. Accumulator [↑](#endnote-ref-83)
83. Index Register [↑](#endnote-ref-84)
84. Program Counter [↑](#endnote-ref-85)
85. Just-In-Time Compiler (JIT) [↑](#endnote-ref-86)
86. MIPS Architecture [↑](#endnote-ref-87)
87. ARM Architecture [↑](#endnote-ref-88)
88. Extended BPF (EBPF) [↑](#endnote-ref-89)
89. Opcode [↑](#endnote-ref-90)
90. System Call [↑](#endnote-ref-91)
91. Checkpoint [↑](#endnote-ref-92)
92. Drop [↑](#endnote-ref-93)
93. Forward [↑](#endnote-ref-94)
94. Data-Plane Switch [↑](#endnote-ref-95)
95. Attack Mitigation [↑](#endnote-ref-96)
96. Middlebox [↑](#endnote-ref-97)
97. Entropy [↑](#endnote-ref-98)
98. Dataset [↑](#endnote-ref-99)
99. Intrusion Detection System [↑](#endnote-ref-100)
100. Snort Intrusion Detection System [↑](#endnote-ref-101)
101. IPFIX [↑](#endnote-ref-102)
102. Anomaly [↑](#endnote-ref-103)
103. P4 [↑](#endnote-ref-104)
104. Deep Packet Inspection(DPI) [↑](#endnote-ref-105)