



دانشگاه صنعتی شریف  
دانشکده‌ی مهندسی کامپیوتر

سمینار کارشناسی ارشد  
گرایش رایانش امن

عنوان:

ارائه‌ی رویکرد تطبیق‌پذیر با تنوع ترافیکی شبکه‌های پهن‌بند برای شناسایی حملات منع خدمت توزیع‌شده  
An Adaptive Approach with Variety Characteristic of High-Bandwidth Networks for  
Distributed Denial of Service Attacks Detection

نگارش:

روح‌الله جهان‌افروز

استاد راهنما:

دکتر رسول جلیلی

استاد ممتحن:

دکتر امیرحسین جهانگیر

بهمن ۱۴۰۱

## چکیده

بسیاری از برنامه‌های کاربردی<sup>۱</sup> امروزی از پروتکل‌های یکسان و مشترکی برای تبادل اطلاعات استفاده می‌کنند. برنامه‌های پیام‌رسان و مرورگرهای وب از بسته‌های مبتنی بر پروتکل اچ.تی.تی.پی/اس<sup>۲</sup> 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. در شبکه‌های پهن‌بند<sup>۳</sup> با افزایش نرخ ترافیک و وجود تنوع پروتکلی زیاد، چالش‌های امنیتی نظیر تشخیص حملات منع خدمت<sup>۴</sup>، که به دلیل سادگی در پیاده‌سازی و تاثیر بسیار مخرب یک تهدید جدی به حساب می‌آیند، افزایش پیدا کرده است. در دهه‌های گذشته محققان روش‌های شناسایی بسیاری را برای حملات منع خدمت توزیع شده<sup>۵</sup> پیشنهاد کرده‌اند. عدم تطبیق‌پذیری و مقیاس‌پذیری برای استفاده در شبکه‌های پهن‌بند، از متداول‌ترین مشکلات این روش‌ها هستند. لذا برای شناسایی صحیح حملات منع خدمت در شبکه‌های پهن‌بند نیاز به یک رویکردی است که شامل دو ویژگی پردازش جامع<sup>۶</sup> به معنای پردازش تمامی بسته‌ها و تطبیق‌پذیری<sup>۷</sup> 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 پهن‌بند برای شناسایی حملات منع خدمت توزیع شده معرفی نماییم که ویژگی پردازش جامع ترافیک را نیز شامل شود. روش پیشنهادی جریان‌ها را بر اساس اینکه برای کدام کاربرد می‌باشند، دسته‌بندی کرده و بر مبنای رفتار عادی ترافیک هر برنامه کاربردی، ترافیک‌های متخاصم را تشخیص می‌دهد. به دلیل اینکه از الگوریتم‌ها و داده ساختارهای فشرده و سبک با قابلیت جستجوی سریع استفاده می‌شود، سرعت بالا و استفاده بهینه از حافظه تضمین می‌شود. همچنین در روش پیشنهادی از ابزارهای تسریع عملیات پردازش بسته که در سالیان اخیر بسیار مورد استقبال قرار گرفته است، استفاده می‌شود و بدین صورت می‌توان سرعت پردازش بسته‌ها را تسریع بخشید که منجر به پردازش جامع تمامی بسته‌های ترافیک عبوری شبکه خواهد شد. در انتها کارایی روش ارائه شده در مقایسه با برخی دیگر از راهکارهای موجود و با در نظر گرفتن معیارهایی نظیر میزان استفاده از پردازشگر و حافظه، نرخ دور انداختن بسته‌ها<sup>۸</sup>، و میزان تأخیر در شناسایی حملات بررسی می‌شود.

کلیدواژه‌ها: حملات منع خدمت توزیع شده، شبکه‌های پهن‌بند، تطبیق‌پذیری با تنوع ترافیکی، سامانه‌های تشخیص نفوذ

## ۱ مقدمه

امروزه با افزایش حجم تبادلات داده‌ای در بستر اینترنت، برقراری 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 عنصر جدایی‌ناپذیری در زندگی و تعاملات کاربران تبدیل شده و بحث دسترسی‌پذیری آسان به خدمات بستر اینترنت بیش از پیش مورد توجه قرار می‌گیرد؛ بدین معنا که ارائه‌دهندگان خدمات ارتباطی<sup>۹</sup> موظف هستند خدمات<sup>۱۰</sup> خود را به صورت شبانه‌روزی و بدون اختلال و وقفه در اختیار کارخواهان<sup>۱۱</sup> قرار دهند. در صورتی که 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 از بین رفتن اعتبار سازمان مواجه می‌شوند.

حملات منع خدمت، دسته‌ای از حملات در شبکه هستند که با هدف از بین بردن دسترسی‌پذیری شبکه سعی در ممانعت از ارائه و انجام یک خدمت<sup>۱۲</sup> 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 کاربر<sup>۱۳</sup> یا هر دستگاه حیاتی دیگر در شبکه خواهند شد. گونه‌های مختلفی از این حملات وجود دارد که هر کدام به طریقی سعی می‌کنند دسترسی‌پذیری شبکه را هدف قرار داده و یا با مصرف منابع کاربردی، مانع از ارائه خدمت به صورت کامل و با کیفیت به کارخواهان و کاربران قانونی شوند. حملات منع خدمت توزیع شده یک گونه مخرب‌تر از حملات منع خدمت هستند که در آن‌ها حمله‌کننده<sup>۱۴</sup> از طریق سیستم‌هایی که تحت کنترل خود می‌آورد، حمله را انجام می‌دهد. بدین ترتیب علاوه بر حجم ترافیک سنگین حملات و دشواری‌های تمییز قائل شدن بین حجم ترافیک بالا در عین حال قانونی شبکه<sup>۱۵</sup> و ترافیک حمله‌کننده، پیدا کردن فرد مهاجم اصلی نیز به مراتب دشوارتر می‌شود.

از سویی دیگر امروزه با شبکه‌های پهن‌بندی مواجه هستیم که منجر به بالا رفتن نرخ گذر اطلاعات به میزان بیش از ۱۰۰ گیگابیت در ثانیه در بسیاری از تجهیزات شبکه شده‌اند. 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 تطبیق معیار تشخیص حملات با توجه به کاربرد ترافیک می‌باشد. با توجه به دلایل مطرح شده، همچنان حملات منع خدمت (توزیع شده) یکی از تهدیدهای بزرگ در شبکه‌های پهن‌بند محسوب می‌شوند.

این گزارش در پنج بخش تدوین شده است. در بخش ۲ مفاهیم پایه مورد نیاز در این پژوهش معرفی می‌شوند. ابتدا شبکه‌های پهن‌بند و ویژگی‌های آن‌ها بیان می‌شود. سپس انواع حملات منع خدمت، از نقطه نظرهای مختلف مورد بررسی قرار می‌گیرند و انتهای این بخش به توضیح مفاهیم داده جریان<sup>۱۶</sup> و انگاره<sup>۱۷</sup>، راهکارهای افزایش سرعت پردازش بسته‌ها، و معرفی راه‌گزین<sup>۱۸</sup>‌های برنامه‌پذیر اختصاص می‌یابد. بخش ۳ به بررسی کارهای پیشین انجام شده برای تشخیص حملات منع خدمت توزیع شده می‌پردازد. در بخش ۴ راهکار پیشنهادی به منظور بهبود تشخیص حمله در شبکه‌های پهن‌بند، بیان می‌شود و سرانجام در بخش ۵ نتیجه‌گیری، مراحل انجام پروژه، و زمان‌بندی آن بیان خواهد شد.

## ۲ مفاهیم پایه

در این بخش به شرح مختصری از مفاهیم پایه مرتبط با این پژوهش پرداخته خواهد شد. ابتدا شبکه‌های پهن‌بند را معرفی می‌کنیم. سپس به معرفی حملات منع خدمت و حملات منع خدمت توزیع شده می‌پردازیم و در پایان این بخش مفهوم داده جریان و انگاره‌ها شرح داده می‌شود.

### ۱-۲ شبکه‌های پهن‌بند

امروزه نرخ تبادل اطلاعات در شبکه‌های کامپیوتری بالا رفته و مفهومی به عنوان شبکه‌های پهن‌بند مطرح می‌باشد. شبکه‌های پهن‌بند دارای سه ویژگی زیر می‌باشند [۱]:

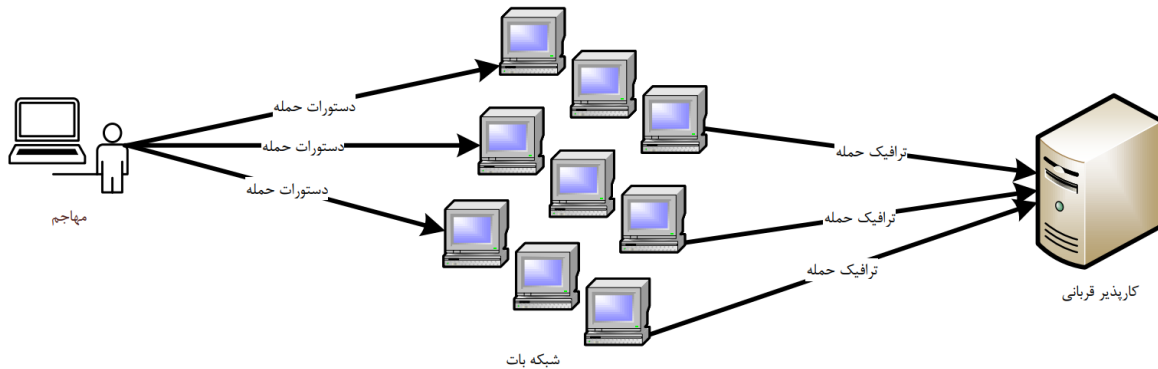
- سرعت بالا: داده‌ها و بسته‌ها با سرعت و نرخ بالایی تولید می‌شوند. برای مثال در شبکه‌های نسل پنجم اینترنت همراه<sup>۱۹</sup>، هر کاربر از قابلیت تبادل اطلاعات با سرعت ۱۵ گیگابیت بر ثانیه برخوردار می‌باشد.
- حجم بالا: اطلاعات عبوری از شبکه و داده‌های در حال تبادل باعث تولید حجم زیادی از فراداده<sup>۲۰</sup> می‌شوند. به عبارتی دیگر بسته‌هایی با محتوا<sup>۲۱</sup> و حجم زیادی از سرایندها<sup>۲۲</sup> را خواهیم داشت. به دلیل ظهور کاربردهای مختلف و به دنبال آن پروتکل‌های مختلف و لزوم استفاده از الگوریتم‌های رمزنگاری، حجم زیادی از سرایندها برای برقراری ارتباط الزامی می‌باشد که نگهداشت فراداده‌های تولید شده آن‌ها هزینه زیادی را شامل می‌شود. همچنین اطلاعاتی که کاربران در بستر اینترنت تبادل می‌کنند، می‌تواند طیف وسیعی از داده‌ها شامل فایل‌هایی حجیم و یا جریانی بی‌وقفه از بسته‌ها در هنگام مشاهده یک ویدئوی برخط یا در هنگام برگذاری یک کلاس مجازی باشد. در سال ۲۰۰۳، حجم کل داده‌های تولید شده در اینترنت حدود پنج اگزابایت بود که این میزان در سال ۲۰۰۸ سه برابر شد و به ۱۴۰۷ اگزابایت رسید. در سال ۲۰۱۹، ترافیک تولیدی کاربران به میزان پنج اگزابایت داده در هر دو روز می‌رسید [۲].
- تنوع بالا: علاوه بر ظهور پروتکل‌های مختلف که هر کدام برای کاربردی خاص می‌باشند، نحوه انتقال و دریافت بسته‌ها بین کارخواه-کارپذیر و استفاده از این پروتکل‌ها وابسته به وضعیت و نوع کاربرد می‌تواند متنوع باشد. برای مثال با اینکه بیشتر برنامه‌های مستقر بر بستر اینترنت، داده‌ها و تبادلات خود را در قالب بسته‌های اچ.تی.تی.پی/اس لایه کاربرد انتقال می‌دهند، اما محتویات این بسته‌ها و نحوه تفسیر آنها برای برنامه‌های مختلف می‌تواند متفاوت باشد.

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

## ۲-۲ حملات منع خدمت (توزیع شده)

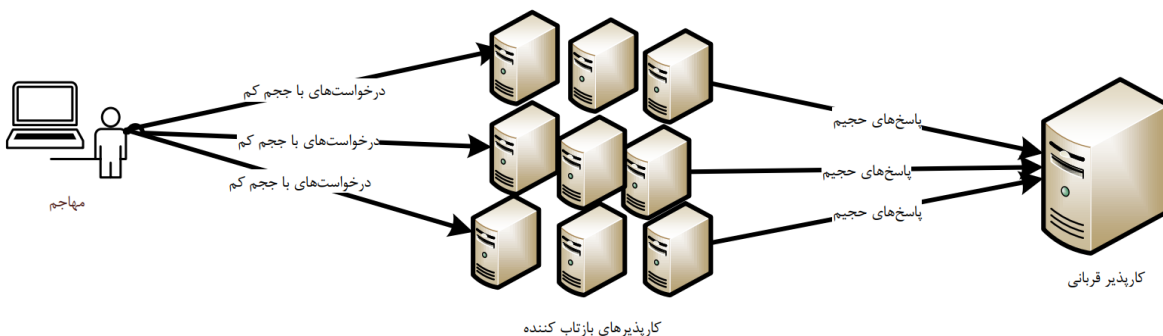
به مجموعه حملاتی که با هدف ممانعت از انجام یک خدمت صورت می‌پذیرند، حملات منع خدمت گفته می‌شود. این حملات با انگیزه‌های مختلفی نظیر ایجاد اختلال یا ممانعت از ارائه یک خدمت، از بین بردن اعتبار و مقبولیت یک سازمان، آسیب زدن به اموال و هدر دادن دارایی‌ها و منابع سازمان، دستاوردهای سیاسی و ملی، انگیزه مالی، و یا قدرت‌نمایی مهاجمین و مواردی از این دست می‌تواند صورت پذیرد. هدف اصلی در حملات منع خدمت، تولید ازدحام و اختلال در مصرف منابع پردازشی سیستم (پردازشگر سیستم) یا منابع شبکه (پهنای باند) می‌باشد.

حملات منع خدمت توزیع شده گونه خطرناک‌تر از حملات منع خدمت می‌باشند که در آن فرد مهاجم ابتدا با پایش آسیب پذیری‌های دستگاه‌های مختلف موجود در شبکه اینترنت، شروع به نفوذ به ماشین‌های عامل<sup>۲۳</sup> متعددی می‌کند و سعی می‌کند این دستگاه‌ها را تحت کنترل خود درآورد. به این سیستم‌هایی که توسط فرد مهاجم از راه دور کنترل می‌شوند، ربات گفته می‌شود و این مجموعه ربات‌ها که به آنها شبکه بات<sup>۲۴</sup> گفته می‌شود، دستورات را از شخص مهاجم دریافت می‌کنند (شکل ۱). مهاجم می‌تواند در مدت زمان کوتاهی حجم زیادی از ترافیک را به سمت کارپذیر و منابع آن هدایت کند که خدمت‌دهی آن یا رویکرد شبکه را برای پاسخگویی به کاربران قانونی با اختلال مواجه می‌کند. در صورت بروز حملات منع خدمت توزیع شده، رهگیری مبدأ حمله یعنی نقطه‌ای که حمله از آنجا شروع شده است، به نسبت حملات منع خدمت معمولی، دشوارتر و همچنین ترافیک ایجاد شده در اثر حمله بزرگتر و مخرب‌تر می‌باشد.



شکل ۱: حملات منع خدمت توزیع شده با استفاده از شبکه بات [۴]

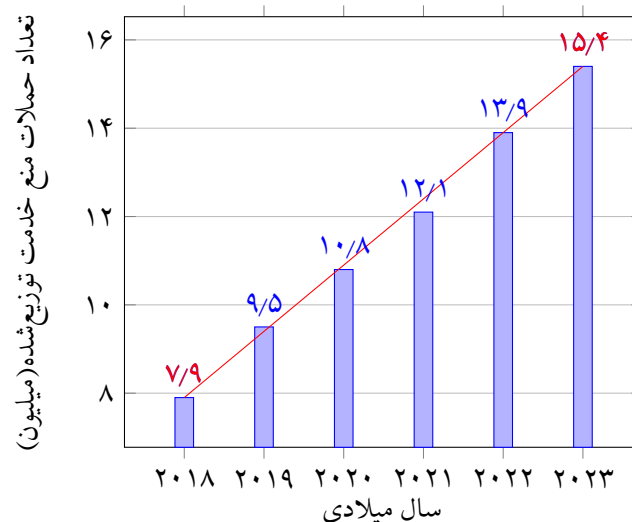
مشکل دیگر دفاع در برابر حملات منع خدمت توزیع شده، بروز حملات تقویت بازتاب<sup>۲۵</sup> می‌باشد (شکل ۲). در سال ۲۰۱۸، گیت‌هاب<sup>۲۶</sup> با استفاده از آسیب‌پذیری پروتکل ممکج<sup>۲۷</sup>، با انعکاس چند برابر بیش از ۵۰۰۰ بار و اوج ترافیک<sup>۲۸</sup> ۱.۳۵ ترابایت بر ثانیه، قربانی یک حمله منع خدمت توزیع شده از نوع تقویت بازتابی قرار گرفت.



شکل ۲: حملات منع خدمت توزیع شده از نوع تقویت بازتابی [۴]

در فوریه ۲۰۲۰، ارائه دهندگان خدمات وب آمازون<sup>۲۹</sup> حمله‌ای با حجم ترافیک پیک ۲.۳ ترابایت بر ثانیه را تجربه کردند. در ژوئیه ۲۰۲۱، شرکت ارائه‌دهنده خدمات تحویل محتوا<sup>۳۰</sup> کلودفلر<sup>۳۱</sup> در گزارشی به محافظت از یکی از مشتریان خود در برابر حمله منع خدمت توزیع شده نشئت گرفته شده از یک شبکه بات در ابعاد جهانی توسط بدافزار میرای<sup>۳۲</sup> با

ترافیک پیک ۱۷.۲ میلیون درخواست در ثانیه، اشاره کرد. یاندکس<sup>۳۳</sup>، ارائه‌دهنده خدمات پیشگیری از حملات منع خدمت توزیع‌شده روسیه گفت که در تاریخ پنج سپتامبر ۲۰۲۱ یک حمله منع خدمت توزیع‌شده پروتکل اچ.تی.تی.پی را که از تجهیزات شبکه میکروتک<sup>۳۴</sup> بروزنشده<sup>۳۵</sup> سرچشمه می‌گرفت، مسدود کرده است. طبق پیش‌بینی شرکت سیسکو<sup>۳۶</sup>، تعداد حملات منع خدمت توزیع‌شده به حدود ۱۶ میلیون در سال ۲۰۲۳ میلادی خواهد رسید (شکل ۳). در بزرگترین حمله منع خدمت توزیع‌شده رخ داده تا به امروز، ترافیک حمله به ۱.۴۴ ترابیت در ثانیه می‌رسید. 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<sup>۳۷</sup> هشدار صادر کرد مبنی بر اینکه پروتکل برنامه‌های محدود شده<sup>۳۸</sup> و سایر پروتکل‌ها ممکن است برای انجام حملات منع خدمت توزیع‌شده مورد سوءاستفاده قرار گیرند. حملات منع خدمت توزیع‌شده بر اساس بردارهای حمله<sup>۳۹</sup> جدید ممکن است تغییرات زیادی در ویژگی‌های آماری مانند سرعت بسته‌ها و فاصله‌ی بسته‌های مورد استفاده در مقایسه با روش‌های سنتی داشته باشند، که این امر باعث می‌شود روش‌های سنتی مقابله در برابر حملات مختلف کارایی لازم را نداشته باشند [۳].



شکل ۳: گزارش و پیش‌بینی سیسکو از مجموع حملات منع خدمت توزیع‌شده [۵]

## ۳-۲ داده جریان

همانطور که در ویژگی‌های شبکه‌های پهن‌بند ذکر شد، نرخ بالای تولید اطلاعات یکی از شاخصه‌های این شبکه‌ها می‌باشد. برای پردازش بسته‌ها در این حالت، دو رویکرد متفاوت وجود دارد:

- پردازش دسته‌ای<sup>۴۰</sup>: در این رویکرد تمامی بسته‌ها در یک پنجره زمانی را ضبط می‌شوند و سپس در زمان‌های بعدی پردازش می‌شوند. از مشکلات پردازش دسته‌ای می‌توان به تأخیر در ارسال و پردازش و نیز هزینه بسیار زیاد (برای ذخیره‌سازی) به دلیل ذخیره‌سازی اطلاعات در ابتدای کار و سپس ارسال آن به مراکز دیگر، اشاره کرد.
- پردازش جریانی<sup>۴۱</sup>: اکثر راهکارهای ارائه شده که در قسمت بعد بررسی می‌شوند، مبتنی بر این رویکرد می‌باشند. این الگوریتم‌ها دو مشخصه زیر را در نظر می‌گیرند: اول این که اطلاعات به صورت جریانی از داده‌ها (بی‌وقفه و با سرعت بالا) در حال ارسال می‌باشند و دوم اینکه از نظر زمانی و حافظه محدودیت وجود دارد [۶]. این خصیصه‌ها همان چالش‌هایی هستند که برای پردازش ترافیک در شبکه‌های پهن‌بند مطرح می‌شوند. برای تشخیص حملات در این شبکه‌ها باید تمامی بسته‌ها را ضبط و پردازش کرده و این کار باید با همان سرعت ورود اطلاعات<sup>۴۲</sup> و با کمترین میزان استفاده از حافظه انجام شود. الگوریتم‌های پردازش جریانی در بحث پردازش اطلاعات مختلف بسیار کاربردی هستند. الگوریتم‌های مبتنی بر پردازش جریانی، ابتدا مسئله را به یکی از چندین روش موجود مدل می‌کنند.

یکی از این مدل‌های بسیار متداول و کاربردی ترنستیل<sup>۴۳</sup> می‌باشد. در این مدل یک داده جریان ورودی به نام  $I$  در نظر گرفته می‌شود که شامل مجموعه‌ای از تاپل‌های دوتایی می‌باشد:

$$I = \alpha_1, \alpha_2, \alpha_3, \dots \quad \alpha_i = \{(a_i, v_i) \mid a_i \in \{0, 1, \dots, u-1\}, v_i \in R\}$$

$[u]$  = فضای کلید

تاپل‌ها، دوتایی‌هایی هستند که شامل مقدار کلید و به‌روزرسانی می‌باشند. آرایه‌ای به نام  $A$  وجود دارد که تعداد خانه‌های آن برابر  $[u]$  و دارای مقادیر متناظر به‌روزرسانی برای هر کلید می‌باشد. هرگاه یک تاپل جدید  $(a_x, v_x)$  دریافت شود مقدار به‌روزرسانی آن با مقدار  $A[a_x]$  جمع می‌شود:

$$A[a_x] + = v_x$$

این پارامترها وابسته به مسئله داده جریانی که مطرح می‌شود، می‌توانند متفاوت باشند. در بحث پردازش بسته‌های دریافتی شبکه، جریان همان جریان ورودی و تاپل‌ها همان بسته‌ها می‌باشند که برای مثال کلیدشان پنج خصیصه‌ی آدرس آی.پی. مبدأ، آدرس آی.پی. مقصد، شماره درگاه مبدأ، شماره درگاه مقصد و پروتکل و به‌روزرسانی نیز می‌تواند اندازه بسته باشد. در نتیجه برای شناسایی حملات منع خدمت، باید آدرس‌هایی که بسته‌هایی با حجم نامتعارف ارسال می‌کنند را، شناسایی کرد [۷]. در مسائل داده جریان، چندین نوع پاسخ برای مسائل اندازه‌گیری مختلف مطرح می‌باشد و پس از مدل‌سازی مسئله، الگوریتم‌هایی استفاده می‌شود که بر مبنای مدل سعی در یافتن این پاسخ‌ها دارند. برای تحلیل بهتر این نوع مسائل، ابتدا مفاهیم اولیه باید توضیح داده شود. جریان ورودی، توالی‌ای از بسته‌هایی به شکل تاپل شامل شناسه جریان متناظر و اندازه آن بسته در نظر گرفته می‌شود:

$F$  = تعداد کل جریان‌های متمایز

(پروتکل، شماره درگاه مقصد، آدرس آی.پی. مقصد، شماره درگاه مبدأ، آدرس آی.پی. مبدأ) = شناسه جریان  $[u]$

$(f_1, c_1), \dots, (f_t, c_t), \dots$  = داده جریان ورودی

پاسخ‌های مسائل یکی از انواع زیر می‌باشند [۸]:

- سایز هر جریان<sup>۴۶</sup>: خواسته این مسائل، یافتن سایز جریان یا تعداد بسته‌های دریافت شده متعلق به جریان می‌باشد که با  $n_f$  نشان داده می‌شود. سایز تمامی بسته‌های دریافتی نیز  $n_f = \sum_{1 \leq i \leq F} n_i$  می‌باشد.
- لحظه جریان<sup>۴۷</sup>: در لحظه دلخواهی، وضعیت جریان با استفاده از تابع  $g$  در لحظه  $g$ <sup>۴۸</sup> مطلوب است، که به صورت زیر می‌تواند تعریف شود:

$$L_g = \sum_{1 \leq f \leq F} g(n_f), f \in [1, F] \quad (1)$$

تابع ۱ وابسته به اینکه به چه صورت تعریف شده باشد، می‌تواند وضعیت کلی از ترافیک شبکه را به صورت عددی بیان کند.

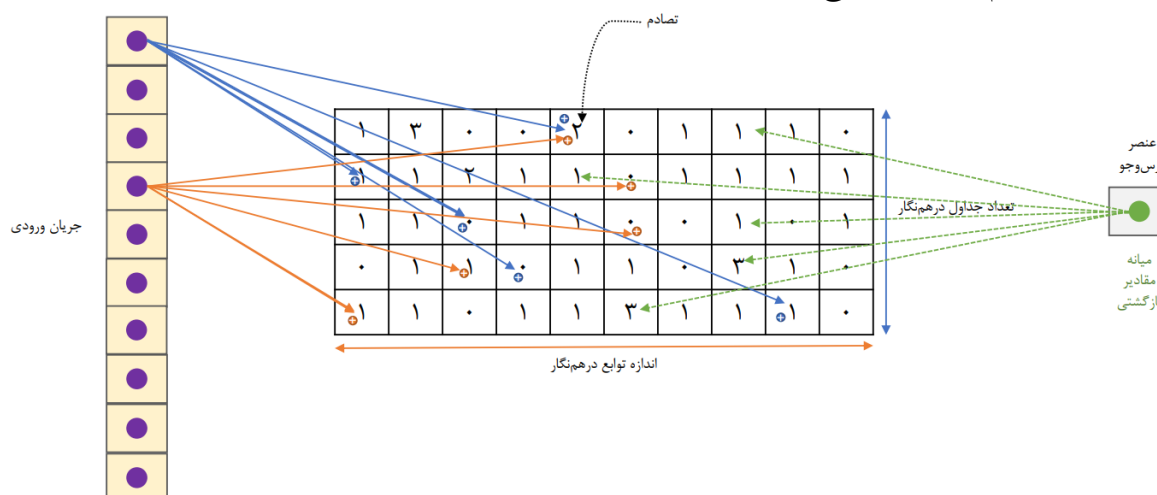
- شاخص<sup>۴۹</sup>: شاخص‌ها جریان‌هایی هستند که اندازه آنها بر لحظه جریان  $L_g$  بیشترین تاثیر را می‌گذارد. به عبارتی دیگر:

$$H_g = \{f \mid g(n_f) \geq \alpha L_g\}$$

که  $\alpha$  مقدار آستانه از پیش تعریف شده بین صفر و یک می‌باشد.

برای حل مسائل داده جریان، راهکارهای متفاوتی را می‌توان استفاده کرد. یکی از راهکارها بدین صورت می‌باشد که به دلیل اینکه با حجم زیادی از اطلاعات روبرو هستیم، تنها بخشی از داده‌های ورودی به عنوان نمونه انتخاب شوند و عملیات پردازش تنها روی آن‌ها صورت گیرد. این روش نمونه برداری<sup>۵۰</sup> نامیده می‌شود [۹]. نمونه برداری دقت پایینی خواهد داشت. به منظور بالا بردن دقت، پردازش تمامی بسته‌ها الزامی می‌باشد. اما بررسی همه بسته‌ها نیز نیازمند حجم زیادی از منابع پردازشی و زمان می‌باشد. برای حل این مشکل، الگوریتم‌هایی به نام انگاره ارائه شده‌اند که از یک داده ساختار فشرده برای ذخیره‌سازی 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 جریان دارند. در ذیل چند مورد از پراستفاده‌ترین آن‌ها معرفی خواهند شد:

- انگاره شمارشی<sup>۵۱</sup>: از یک جدول  $K \times H$  تشکیل شده است که شامل  $K$  تابع درهم‌نگار<sup>۵۲</sup> می‌باشد (شکل ۴).  $H$  نیز اندازه توابع درهم‌نگار در یک سطر می‌باشد. این ساختار را الگوریتم‌های انگاره دیگر نیز استفاده می‌کنند. چون از توابع درهم‌نگار استفاده می‌شود لذا امکان تصادم<sup>۵۳</sup> وجود خواهد داشت. مقادیر بازگشتی تقریبی خواهند بود و در نتیجه به آنها داده ساختارهای آماری احتمالاتی می‌گویند. اما بایستی نرخ خطای قابل قبول و کرانداری ارائه دهند. از این الگوریتم برای یافتن پاسخ مسائل شاخص استفاده می‌شود [۱۰].



شکل ۴: انگاره شمارشی [۱۱]

- انگاره شمارشی کمینه<sup>۵۴</sup>: همانند انگاره شمارشی می‌باشد اما سعی دارد مرتبه فضایی را کاهش دهد [۱۲].
- انگاره عمومی<sup>۵۵</sup>: یک دسته جدیدی از انگاره‌ها با هدف ارائه داده ساختاری قابل استفاده برای حل تمامی انواع مسائل داده جریان می‌باشند. یونیومان<sup>۵۶</sup> یکی از این الگوریتم‌ها می‌باشد [۱۳].

## ۵-۲ پردازش سریع بسته‌ها

هنگامی که یک بسته از طریق واسطه‌های شبکه یک سیستم دریافت می‌شود تا پردازش آن، مراحل مختلفی را طی خواهد کرد. بنا به کاربرد، بسته‌ها از دستگاه‌های مختلفی عبور داده می‌شوند. بر مبنای پشته پروتکل تی.سی.پی/آی.پی<sup>۵۷</sup> که هسته<sup>۵۸</sup> تمامی توزیع‌های مختلف سیستم عامل لینوکس از آن پشتیبانی می‌کنند، بسته‌ها از دریافت تا پردازش بخش‌های مختلف آن‌ها مراحل مختلفی را پشت سر خواهند گذاشت و در نهایت در صورت نیاز بازرسال خواهند شد. رویدادهای مهم در هنگام دریافت یک بسته توسط ماشین بدین شرح می‌باشد:

۱. بسته توسط کارت شبکه<sup>۵۹</sup> ماشین دریافت می‌شود (وقفه کارت شبکه).

۲. کارت شبکه از طریق دی.ام.ای<sup>۶۰</sup>، بسته را در فضای حافظه در یک بافر قرار می‌دهد.

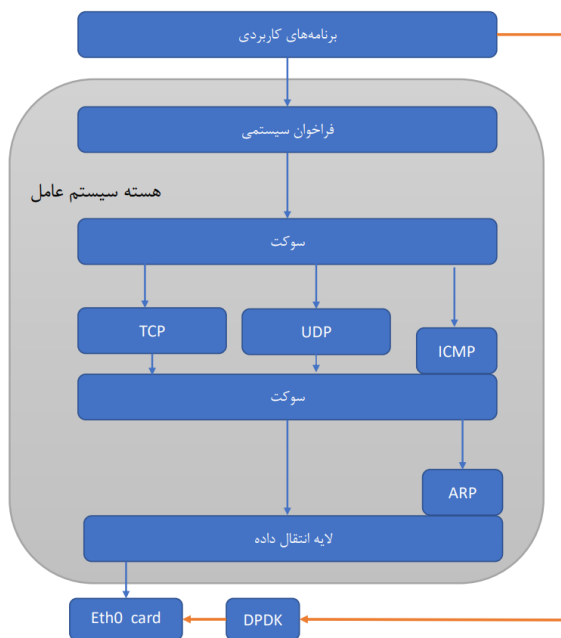
۳. کارت شبکه سیگنالی به پردازنده ارسال می‌کند و آن را برای پردازش بسته بیدار می‌کند (وقفه نرم افزاری).

۴. پردازنده اطلاعات مورد نیازش را خوانده و در صورت نیاز در فضای بافر تعیین شده می‌نویسد.

۵. در صورت نیاز، بسته برای پردازش‌های بیشتر به پشته پروتکلی هسته برای انجام پردازش‌های مختلف (مثل بررسی آدرس آی.پی برای تطبیق با آدرس‌های متناظر لیست کنترل دسترسی) فرستاده می‌شود.

۶. در نهایت اگر برنامه کاربردی در سطح کاربر باشد، محتویات بسته از فضای هسته به فضای کاربر انتقال داده خواهد شد. در غیر اینصورت، بسته در همان فضای هسته خواهد ماند.

تمامی این مراحل بایستی در سطح هسته انجام شده ولی پردازش بسته توسط کاربر در لایه کاربرد صورت می‌گیرد. این مراحل به دلیل وقفه‌هایی که انجام می‌شود، سرشار زیادی خواهند داشت و در شبکه‌های پهن‌بند که با حجم زیادی از بسته‌ها مواجه هستیم، باعث اتلاف وقت زیادی خواهند شد.



دی.پی.دی.کی<sup>۶۱</sup> و ایکس.دی.پی<sup>۶۲</sup> از ابزارهای موجود برای تسریع عملیات پردازش بسته می‌باشند. دی.پی.دی.کی ابزار نرم افزاری می‌باشد که در سال ۲۰۰۹ توسط اینتل<sup>۶۳</sup> توسعه داده شد. ولی بعدها به صورت یک پروژه متن‌باز<sup>۶۴</sup> درآمد. به طور خلاصه یک ابزار دورزدن هسته در هنگام دریافت بسته در شبکه می‌باشد که وقفه‌های مختلف مربوط به هسته را حذف می‌کند و لذا تمام عملیات پردازش بسته را می‌توان در سطح کاربر انجام داد و در نهایت عملیات دریافت و پردازش بسته را تا حد خوبی می‌تواند تسریع بخشد. هدف این فناوری استفاده از قابلیت پردازش چند هسته‌ای پردازنده‌های معمولی ایکس۸۶<sup>۶۵</sup> برای بهبود سرعت پردازشی کاربرها می‌باشد. بدین صورت ما نرخ پردازشی برابر هنگام استفاده از پردازنده‌های مخصوص کاربرها و یا مدارهای مجتمع با کاربرد خاص<sup>۶۶</sup> و مدار مجتمع دیجیتال برنامه‌پذیر<sup>۶۷</sup>، با صرف هزینه‌ای بسیار کمتر، خواهیم داشت. از چندین پردازنده برای محاسبات

شکل ۵: مراحل ضبط و پردازش بسته [۱۳]

مربوط به سطح داده و از بقیه هسته‌ها برای امور کنترلی و خدمات دیگر استفاده می‌کند. به صورت جزئی‌تر، چندین صف بر روی هر واسط شبکه تعریف می‌کند و هسته‌ها با حالت سرکشی<sup>۶۸</sup> به این صف‌ها الصاق می‌شوند. از این ابزار در کاربردهای مختلفی در مواقعی که حجم زیادی از ورودی/خروجی مطرح می‌باشد از حیطه شبکه و امنیت آن، پردازش و راه‌گزینی در ابرها، بهبود کارایی حافظه‌ها، توابع مجازی شبکه<sup>۶۹</sup>، مخابرات، و تلکام استفاده می‌شود. البته به غیر از مورد اشاره شده که ویژگی اصلی این ابزار می‌باشد، امکانات مختلف دیگری مانند رمزگذاری و فشرده‌سازی به کمک رابط‌های برنامه‌نویسی‌اش نیز ارائه می‌دهد [۱۴].

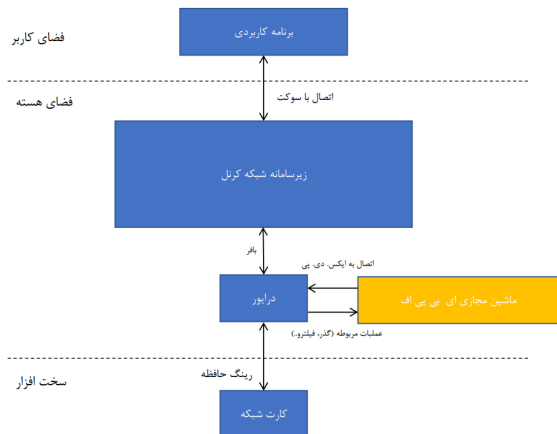
ایکس.دی.پی.یکی از مؤلفه‌های جدید هسته می‌باشد که پردازش بسته را به صورت خوبی بهبود می‌بخشد. روش‌هایی مثل دی.پی.دی.کی هسته را دور می‌زنند و تمام عملیات پردازش بسته در فضای کاربر صورت می‌گیرد (شکل ۵). همچنین کارت شبکه را باید توسط یک گرداننده<sup>۷۰</sup> سطح کاربر کنترل نمود. پردازش شبکه در سطح کاربر با وجود مزایای زیاد، معایب زیر را نیز به همراه خواهد داشت:



- به دلیل اینکه سیستم عامل یک لایه انتزاعی برای ارتباط با منابع سخت‌افزاری می‌باشد، لذا برنامه‌های سطح کاربر برای تعامل با آنها بایستی گرداننده‌های مربوطه را خودشان توسعه دهند
- برنامه‌های سطح کاربر می‌بایست در صورت نیاز، عملکردهایی که توسط هسته ایجاد می‌شد را پیاده‌سازی کنند.
- برنامه‌ها به صورت ایزوله اجرا می‌شوند که نحوه تعامل آنها با دیگر بخش‌های سیستم عامل را دشوار می‌کند.

به طور خلاصه ایکس.دی.پی، برنامه‌های شبکه سطح کاربر (پالایش، نگاشت، مسیریابی و ...) را به جای انتقال به سطح کاربر، به فضای هسته می‌برد. ایکس.دی.پی امکان اجرای برنامه به محض ورود بسته به کارت شبکه و پیش از حرکت به سمت زیرسیستم شبکه‌ی هسته را فراهم می‌کند که منجر به افزایش قابل توجه سرعت پردازش بسته می‌شود. اجرای برنامه در سطح هسته با استفاده از بی.پی.اف<sup>۷۱</sup> میسر می‌شود [۱۵] (شکل ۶).

بی.پی.اف یک ماشین مجازی است که تنها مخصوص پردازش پالایش ترافیک می‌باشد. یکی از ابزارهایی که از بی.پی.اف استفاده می‌کند، تی.سی.پی دامپ<sup>۷۲</sup> می‌باشد. عبارت پالایش مربوطه توسط یک کامپایلر به بایت‌کد<sup>۷۳</sup> 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<sup>۷۴</sup> (انباشتگر<sup>۷۵</sup> و ثبات اندیس<sup>۷۶</sup>)، یک حافظه موقت، و یک شمارنده برنامه ضمنی<sup>۷۷</sup> نیز می‌باشد، تعریف می‌کند. هسته لینوکس از نسخه ۵.۲ به بعد از بی.پی.اف پشتیبانی می‌کند. در سال ۲۰۱۱، مفسر بی.پی.اف به یک کامپایلر درجا<sup>۷۸</sup> تغییر داده شد. این کار باعث شد که هسته به جای تفسیر برنامه‌های بی.پی.اف، قادر باشد که آن‌ها را به معماری هدف‌های مختلف مانند ایکس۸۶، میپس<sup>۷۹</sup>، و آرم<sup>۸۰</sup> تبدیل کند. این امر به معرفی بی.پی.اف توزیع یافته<sup>۸۱</sup> در سال ۲۰۱۴ و کنار گذاشته شدن بی.پی.اف سنتی منجر شد.



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<sup>۸۲</sup> در پشته هسته تعریف کرد که هرگاه بسته‌ای در کارت شبکه دریافت شد، آن را به فضای کاربر بفرستد و در آنجا تصمیم می‌گیرد که بسته دور انداخته شود یا اجازه عبور به لایه‌های بالاتر پشته را صادر کند. لذا نیاز به مکانیزمی بود که امکان اجرای کدهای سطح کاربر را در هسته فراهم کند. به همین دلیل از بی.پی.اف توزیع یافته استفاده شد.

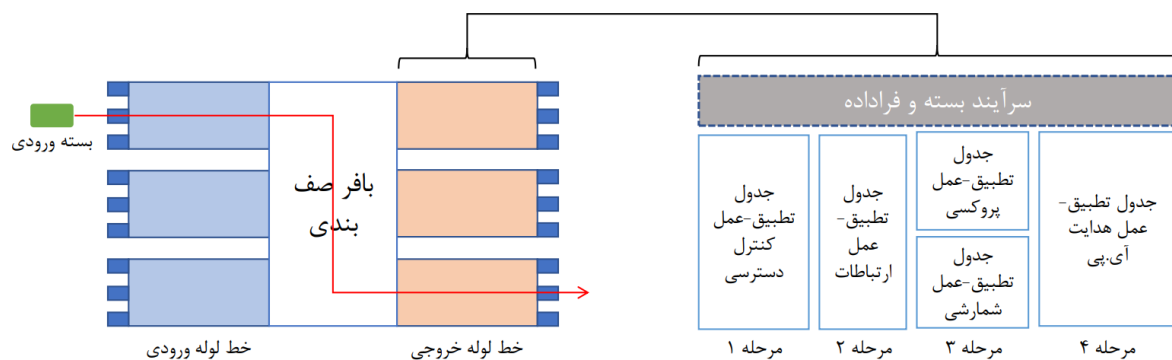
شکل ۶: ایکس.دی.پی بر روی هسته سیستم عامل [۱۵]

ایکس.دی.پی بسته‌های دریافتی را به برنامه بی.پی.اف هدایت می‌کند. در آنجا می‌توان بسته‌ها را ویرایش و یا هدایت<sup>۸۳</sup> کرد. از توابع کمکی می‌توان برای انجام محاسبات و پردازش بسته‌ها بدون نیاز به فراخوان سیستمی استفاده کرد. همچنین با استفاده از داده ساختارهای نگاشت امکان ذخیره داده‌ها به صورت دائمی را خواهیم داشت. در نهایت با استفاده از ویژگی‌های از پیش تعبیه‌شده در ایکس.دی.پی می‌توان عمل مورد نظر را بر روی بسته انجام داد [۱۶].

## ۲-۶ راه‌گزین‌های برنامه‌پذیر

استفاده از یک کنترل‌کننده به عنوان مرکزی که تمامی اطلاعات به آنجا 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 برخی روش‌های تشخیص پیشین

بود. این روش با تأخیر زیادی همراه است و همچنین می‌تواند یک نقطه آسیب‌پذیر واحد برای مهاجمین فراهم کند. اما امروزه با معرفی راه‌گزین‌های برنامه‌پذیر<sup>۸۴</sup>، با استفاده از برنامه‌هایی که بر روی آنها با استفاده از زبان‌هایی مثل پی.پی.۸۵۴ توسعه داده می‌شوند، توانایی پردازش داده را تا حد زیادی خواهند داشت. یک راه‌گزین برنامه‌پذیر مبتنی بر مدارهای مجتمع با کاربرد خاص، چندین خط لوله شامل واسط‌های ورودی و خروجی را شامل می‌شود و بسته‌ها مراحل مختلفی را در طول خط لوله برای پردازش سپری می‌کنند. هر کدام از این مراحل نیز منابع اختصاصی خود را یعنی: ثبات‌ها برای ذخیره‌سازی، جداول تطبیق-عمل، و واحدهای منطق ریاضی به منظور پردازش شامل می‌شوند (شکل ۷). توسط زبان پی.پی.۴ امکان شخصی‌سازی جداول تطبیق-عمل به منظور انجام تغییر روی بسته‌ها میسر خواهد بود. در مجموع راه‌گزین‌های برنامه‌پذیر مبتنی بر مدارهای مجتمع با کاربرد خاص در مقایسه با سخت‌افزارهای دیگر، از دو مزیت بهینه بودن سرعت پردازشی به نسبت هزینه و برق مصرفی و انعطاف‌پذیری در برابر حملات جدید برخوردار می‌باشند [۱۷].



شکل ۷: معماری راه‌گزین برنامه‌پذیر [۱۷]

### ۳ کارهای پیشین

به طور کلی پژوهش‌های انجام‌شده در حوزه حملات منع خدمت توزیع‌شده را می‌توان در سه دسته پیشگیری از وقوع حمله، تشخیص حمله، و کاهش اثر حمله<sup>۸۶</sup> تقسیم‌بندی کرد. از آنجایی که تمرکز این گزارش بر پژوهش‌های موجود در حوزه تشخیص حملات منع خدمت توزیع‌شده می‌باشد، در ادامه به بررسی چند روش اخیراً معرفی‌شده تشخیص حملات منع خدمت توزیع‌شده در شبکه‌های کامپیوتری می‌پردازیم. علاوه بر شیوه‌ی دسته‌بندی‌ای که در ادامه استفاده می‌کنیم، الگوریتم‌های تشخیص را می‌توان بر اساس اینکه در کدام ناحیه از شبکه سعی به تشخیص مهاجم دارند نیز طبقه‌بندی کرد، که شامل سه گروه می‌شوند:

- شناسایی در مبدأ: از توانایی تشخیص همه حملات برخوردار نمی‌باشند.
- شناسایی در مقصد (قربانی): نیاز به منابع زیادی دارند و ممکن است با تأخیر هم همراه باشند.
- شناسایی در مسیرهای میانی<sup>۸۷</sup>.

#### ۳-۱ روش‌های مبتنی بر امضا

طبقه‌بندی و فیلترکردن ترافیک شبکه با استفاده از امضا، معمولاً در سیستم‌های تشخیص نفوذ<sup>۸۸</sup> استفاده می‌شود. در این روش مقادیر فیلدهای مختلف بسته‌های عبوری با یک سری از امضاها (الگوها) ی بسته‌های مهاجم مقایسه می‌شوند. اگرچه این روش الگوهای حمله‌ی مشاهده‌شده‌ی قبلی را با سرعت بالایی شناسایی می‌کند، اما قادر به شناسایی حملات با الگوهای جدیدتر نمی‌باشد.

- تقسیم‌کننده و کاهنده ترافیک حملات منع خدمت توزیع شده مبتنی بر امضا با استفاده از راه‌گزین‌های برنامه‌پذیر سطح داده: در روش ارائه شده در سال ۲۰۲۱، دیمولیانس و همکاران سعی می‌کنند امضاها را مهاجم را بدست آورند و تعداد حداقل بهینه خط قوانین به منظور مقابله با آنها را تولید کنند [۱۸]. مشکل روش، عدم کارایی در شناسایی حملات متنوع می‌باشد. همچنین در مورد نحوه یاددهی مجدد مدل‌های طبقه‌بندی‌کننده توضیحی ارائه نمی‌دهد.
- روش تشخیص مبتنی بر جریان در شبکه‌های با سرعت بالا برای شناسایی حملات با تولید امضای سازگار با اسنورت<sup>۸۹</sup>: در روش ارائه شده در سال ۲۰۲۰ توسط ارلاکر و همکاران، از دسته‌بندی جریان مبتنی بر آی.پی. فیکس<sup>۹۰</sup> استفاده می‌شود، که اطلاعات بیشتری علاوه بر اطلاعات آماری متداول می‌تواند استخراج کند. همچنین با استفاده از برخی روش‌ها امکان بررسی محتوای داده‌ای نیز میسر خواهد بود [۱۹]. مشکل این روش عدم کارایی در شناسایی حملات مختلف می‌باشد.

### ۲-۳ روش‌های مبتنی بر ناهنجاری<sup>۹۱</sup>

این دسته از روش‌ها با ضبط کردن و بررسی ترافیک عادی شبکه در یک بازه زمانی، رفتار عادی شبکه را شبیه‌سازی می‌کنند و هرگونه رفتار مغایر با این مدل را به عنوان ناهنجاری و بروز حمله در نظر می‌گیرند. یادگیری ماشین به عنوان یکی از روش‌های کارآمد مبتنی بر ناهنجاری می‌باشد، که امروزه به صورت گسترده‌ای مورد استقبال پژوهشگران قرار گرفته است. در حوزه تشخیص حملات منع خدمت توزیع شده نیز از این روش استفاده می‌شود. گونه‌های مختلفی از الگوریتم‌های یادگیری ماشین نظیر استفاده از ماشین بردار پشتیبان، بیز ساده، نزدیک‌ترین همسایه، شبکه عصبی و شبکه‌های عصبی ژرف، و نگاشت خودسازمان‌ده به منظور انجام طبقه‌بندی جریان ترافیک در شبکه و تشخیص ناهنجاری در آن مورد استفاده قرار می‌گیرند.

- رویکرد تشخیص ناهنجاری به کمک راه‌گزین‌های برنامه‌پذیر برای شناسایی و مقابله با حملات منع خدمت توزیع شده: این روش به نام جاکن در سال ۲۰۲۱ توسط لیو و همکاران با استفاده از انگاره‌های عمومی و پیاده‌سازی آنها بر روی راه‌گزین‌های برنامه‌پذیر به منظور جمع‌آوری اطلاعات توسط همین دستگاه‌ها، ارائه شد. یک کنترل‌کننده مرکزی از این اطلاعات برای تشخیص حملات استفاده می‌کند. همچنین الگوریتم‌هایی به منظور رفع مخاطره بر روی این راه‌گزین‌ها می‌توان پیاده کرد. به دلیل این که با استفاده از زبان پی ۴ الگوریتم‌های تشخیص و رفع مخاطره پیاده می‌شود، این روش مبتنی بر معماری خاصی از راه‌گزین‌ها نمی‌باشد [۲۰]. عدم واریس محتوای کامل بسته‌ها و عدم استفاده از واریس‌کننده عمیق بسته<sup>۹۲</sup>، مشکل اصلی جاکن می‌باشد. به همین دلیل به بحث تنوع پروتکلی و اینکه مقادیر آستانه برای برنامه‌های کاربردی مختلف می‌تواند متفاوت باشد، اشاره‌ای نکرده است.

- روش بلادرنگ تطبیق‌پذیر مبتنی بر انگاره مخصوص شبکه‌های ارائه‌دهنده خدمات اینترنتی: آر.تی. سد<sup>۹۳</sup> در سال ۲۰۲۱ توسط شی و همکاران پیشنهاد شد. از نامتوازن بودن مقادیر یک ویژگی برای یک آدرس مقصد مشخص، قربانی بودن آن را تشخیص می‌دهد [۴]. به دلیل استفاده از انگاره‌ها، آر.تی. سد از نظر مرتبه فضایی بسیار بهینه می‌باشد. اما در مورد نحوه انتخاب این ویژگی‌ها برای برنامه‌های کاربردی مختلف به صورت پویا صحبتی نمی‌کند.

- روش توزیع شده مقابله با حملات منع خدمت توزیع شده به کمک شبکه‌های عصبی: روشی به نام دفاع هوشمند در سال ۲۰۲۲ توسط مایینی و همکاران ارائه شد که از شبکه‌های عصبی عمیق در سمت لبه مشتری و شبکه‌های عصبی عمیق با الگوریتم‌های پیشرفته‌تر در سمت فراهم‌کننده اینترنت برای شناسایی حملات استفاده می‌کند [۱۹]. اما مشکل این روش، عدم ارائه راهکاری بهینه به منظور آموزش مجدد شبکه‌ها در شبکه‌های پهن‌بند می‌باشد.

- روش بلادرنگ مبتنی بر ناهنجاری برای تشخیص رخنه در شبکه‌های با سرعت بالا: روشی توسط ویگاس و همکاران در سال ۲۰۱۹ ارائه شد که با در نظر گرفتن بسته‌ها به عنوان جریان، ویژگی‌های آنها را استخراج می‌کند و سپس از روی آنها حمله را تشخیص می‌دهد. یک بخش اعتمادسازی دارد که میزان قابل اعتماد بودن گروه‌بندی ارائه شده توسط طبقه‌بندی‌کننده را بررسی می‌کند و اگر از مقدار حداقلی پایین بود، به کمک یک شخص مدیر آن را برچسب‌گذاری

می‌کند و سپس مدل طبقه‌بندی‌کننده را به صورت افزایشی به‌روز می‌کند [۲۰]. به دلیل مداخله‌ی انسان برای برچسب‌گذاری برخی جریان‌ها، در شبکه‌های پهن‌بند با مشکل مواجه می‌شود و سربار بالا و دقت پایینی خواهد داشت.

## ۴ راهکار پیشنهادی

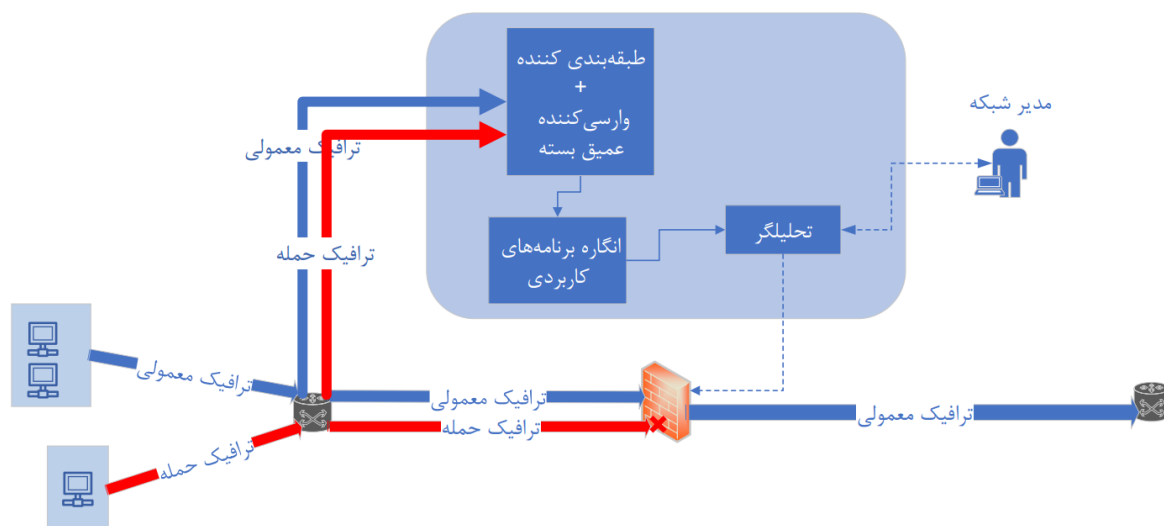
در بخش قبل برخی روش‌های مبتنی بر امضا و مدل‌سازی به منظور تشخیص حملات منع خدمت توزیع‌شده معرفی شدند. به عنوان نتیجه می‌توان گفت، روش‌های شناسایی و مقابله با حملات منع خدمت توزیع‌شده، ویژگی‌های ترافیک را از سه منظر بررسی می‌کند (ترافیک را از سه منظر مشاهده می‌کند) و سعی در مقابله دارند:

- بسته: با استفاده از ویژگی‌ها در سطح بسته (برای مثال یک بسته اچ. تی. پی با اندازه خاص) حملات را تشخیص می‌دهند.
- جریان: در صورت مشاهده ویژگی‌های نامتعارف برای یک جریان (برای مثال داشتن اندازه‌ای بیش از ۱۰۰ کیلوبایت) حملات را تشخیص می‌دهند.
- کاربر: با استفاده از نامتعارف بودن رفتار ترافیک کاربری سعی می‌کنند حملات را تشخیص دهند. به طور مثال کاربری که در مدت زمان مشخصی، بیش از ۱۰ درخواست به منابع مختلف یک سایت ارسال کند.

در هر یک از منظرها طبق اطلاعاتی که جمع‌آوری می‌کنند، ترافیک نامتعارف را با استفاده از رویکردهای مبتنی بر امضا یا با استفاده از رویکردهای مدل‌سازی و تشخیص ناهنجاری، می‌توانند حملات را تشخیص دهند. اما عدم سازگاری با تنوع پروتکلی برنامه‌های کاربردی مختلف، از مشکلات آن‌ها می‌باشد و در هنگام تشخیص حملات دچار خطا می‌شوند. در واقع ترافیک برای هر کاربرد می‌تواند الگوی مختلفی داشته باشد و برای همه کاربردها نمی‌توان یک الگو، مرز و شناسه برای حالت متعارف آن تعریف نمود. برای حل این مشکل به شناسایی کاربردهای مختلف می‌پردازند که از روش‌هایی مانند واریسی عمیق بسته یا یادگیری ماشین استفاده می‌شود و سپس با استفاده از نتایج آنها ترافیک را دسته‌بندی کرده و در هر کدام برای تشخیص الگوهای نامتعارف، تنظیمات متفاوتی (مانند مقادیر آستانه متفاوت برای حجم بسته‌ها) به کار می‌برند. اما در شبکه‌های پهن‌بند با مشکلی به نام تنوع ترافیکی بالا مواجه هستیم و از طرفی با توجه به نرخ بالای تولید ترافیک بایستی در کمترین زمان ممکن، کم هزینه‌ترین راهکار را استفاده کنیم. راهکارهای مبتنی بر یادگیری ماشین و استفاده از واریسی‌کننده عمیق بسته، سربار محاسباتی زیاد دارند.

همانطور که گفته شد، نکته‌ای که در پژوهش‌های پیشین نادیده گرفته می‌شد، مربوط به مؤلفه سوم شبکه‌های پهن‌بند یا تنوع بالای ترافیک می‌باشد. در روش‌های پیشین مؤلفه‌های اول و دوم یعنی اینکه داده‌ها با سرعت زیادی در حال تولید هستند و با حجم زیادی از سرآیندها و محتوا روبرو هستیم را تنها در نظر گرفته بودند. لذا روشی که ارائه می‌دهیم تمامی این سه مورد را با تمرکز بیشتر بر روی ویژگی سوم به عنوان مسئله اصلی، هدف قرار می‌دهد. روش ارائه شده، از ویژگی پردازش جامع برخوردار می‌باشد، یعنی تمامی بسته‌ها را یک و تنها یکبار بررسی می‌کند. بدین صورت روشی بسیار سریع و با دقت بالا و تطبیق‌پذیر با مشخصات ترافیکی شبکه‌های پهن‌بند می‌باشد (علاوه بر معیارهای متداولی مثل سرعت-نرخ‌گذر بالا و تأخیر کم که خواسته همه روش‌های قبلی بوده است) که راه‌حل نوینی نیز به شمار می‌رود.

روش پیشنهادی ما بدین صورت خواهد بود که با استفاده از راهکارهای ارائه شده در پژوهش‌های پیشین و همچنین استفاده از یک زیرسامانه واریسی‌کننده عمیق بسته، جریان‌ها را برچسب‌گذاری می‌کنیم و جریان‌های شبیه به هم از نظر رفتار را در یک گروه قرار می‌دهیم. این اطلاعات در داده ساختارهای انگاره که بر روی راهگزين‌های برنامه‌پذیر می‌باشند و توسط مدیر شبکه کنترل می‌شوند، برای هر برنامه کاربردی و پروتکل متناظر به صورت جدا ذخیره می‌شود. یک قسمت تحلیلگر وجود دارد که با استفاده از این ویژگی‌های آماری و مشاهده رفتار متداول هر پروتکل و یا برنامه کاربردی در بازه‌های زمانی



شکل ۸: معماری کلی از روش پیشنهادی

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 خط‌مشی امنیتی معادل آن را تولید کند و به عنوان خروجی به یک دیوار آتش ارسال کند (شکل ۸). برای بهبود سرعت پردازش بسته‌ها و حذف وقفه‌های زمانبر نیز از ابزارهای مخصوص پردازش سریع بسته‌ها (مانند دی.پی.کی و ایکس.دی.پی) استفاده می‌شود. همچنین کارایی روش ارائه شده در مقایسه با دیگر راهکارها و با در نظر گرفتن معیارهایی نظیر میزان استفاده از پردازشگر و حافظه، نرخ دورانداختن بسته‌ها، و میزان تاخیر در شناسایی حملات در مواجهه با ترافیک‌های حجیم و ترافیک‌های تولیدی از انواع مختلف حملات منع خدمت، بررسی خواهد شد.

## ۵ نتیجه‌گیری و گزارش روند پیشرفت پروژه

در این نوشتار به معرفی شبکه‌های پهن‌بند و ویژگی‌های این شبکه‌ها، حملات منع خدمت توزیع‌شده، روش‌ها و الگوریتم‌های پردازش داده جریان، و معرفی مفاهیم و واژه‌های به کاررفته در این زمینه پرداخته شد. سپس برخی پژوهش‌های انجام‌شده در زمینه تشخیص حملات منع خدمت توزیع‌شده در شبکه‌های پهن‌بند مورد بررسی قرار گرفت و مشکلات پیاده‌سازی و عملکردی و چالش‌های حل‌نشده آنها بیان شد. در پایان 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 پهن‌بند به صورت مختصر توضیح داده شد. در جدول ۱ زمان‌بندی لازم برای بخش‌های مختلف این پژوهش آورده شده است.

جدول ۱: مراحل انجام و پیشبرد پروژه

ردیف	عنوان مراحل پروژه	درصد پیشرفت	پیش‌بینی زمان مورد نیاز
۱	مطالعه و بررسی مفاهیم	۹۰٪	۱ هفته
۲	تحلیل و بررسی کارهای پیشین	۷۰٪	۳ هفته
۳	ارائه و امکان‌سنجی روش پیشنهادی	۱۰٪	۶ هفته
۴	پیاده‌سازی روش پیشنهادی	۱۰٪	۸ هفته
۵	ارزیابی روش پیشنهادی	۰٪	۶ هفته
۶	جمع‌بندی و تدوین پایان‌نامه	۰٪	۶ هفته

- [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.
- [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, Sept. 2019.
- [3] 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, July 2021.
- [4] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommunication Systems*, vol.73, pp.3–25, Jan. 2020.
- [5] "Cisco Annual Internet Report (2018–2023) White Paper," tech. rep., Mar. 2020.
- [6] 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), pp.2285–2293, ACM, Aug. 2021.
- [7] 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), p.234, ACM Press, 2003.
- [8] 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), pp.974–983, IEEE, July 2020.
- [9] 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), pp.164–176, ACM, Apr. 2017.
- [10] M. Charikar, K. Chen, and M. Farach-Colton, "Finding Frequent Items in Data Streams," in *Automata, Languages and Programming* (G. Goos, J. Hartmanis, J. van Leeuwen, P. Widmayer, S. Eidenbenz, F. Triguero, R. Morales, R. Conejo, and M. Hennessy, eds. ), vol.2380, pp.693–703, Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. Series Title: Lecture Notes in Computer Science.
- [11] S. Muthukrishnan, "Data Streams: Algorithms and Applications," *Foundations and Trends® in Theoretical Computer Science*, vol.1, no.2, pp.117–236, 2005.
- [12] G. Cormode and S. Muthukrishnan, "An improved data stream summary: the count-min sketch and its applications," *Journal of Algorithms*, vol.55, pp.58–75, Apr. 2005.
- [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), pp.101–114, ACM, Aug. 2016.
- [14] H. Zhu. *Data Plane Development Kit (DPDK): A Software Optimization Guide to the User Space-based Network Applications*. CRC Press, 1st edition ed. , 2020.

- [15] T. Høiland-Jørgensen, J. D. Brouer, D. Borkmann, J. Fastabend, T. Herbert, D. Ahern, and D. Miller, “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), pp.54–66, ACM, Dec. 2018.
- [16] M. Fleming, “A thorough introduction to eBPF,” Dec. 2017.
- [17] M. Zhang, G. Li, S. Wang, C. Liu, A. Chen, H. Hu, G. Gu, Q. Li, M. Xu, and J. Wu, “Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches,” in *Proceedings 2020 Network and Distributed System Security Symposium*, (San Diego, CA), Internet Society, 2020.
- [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.
- [19] F. Erlacher and F. Dressler, “On High-Speed Flow-Based Intrusion Detection Using Snort-Compatible Signatures,” *IEEE Transactions on Dependable and Secure Computing*, vol.19, pp.495–506, Jan. 2022.
- [20] Z. Liu, H. Namkung, G. Nikolaidis, J. Lee, C. Kim, X. Jin, V. Braverman, M. Yu, and V. Sekar, “Jaquen: A High-Performance Switch-Native Approach for Detecting and Mitigating Volumetric DDoS Attacks with Programmable Switches,” in *30th USENIX Security Symposium (USENIX Security 21)*, pp.3829–3846, 2021.
- [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.
- [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.

## پانویس‌ها

Switch <sup>۱۸</sup>	Application <sup>۱</sup>
5G <sup>۱۹</sup>	HTTP/S <sup>۲</sup>
Metadata <sup>۲۰</sup>	High-Bandwidth Networks <sup>۳</sup>
Payload <sup>۲۱</sup>	Denial Of Service (DoS) <sup>۴</sup>
Header <sup>۲۲</sup>	Distributed Denial Of Service (DDoS) <sup>۵</sup>
Agent Machine <sup>۲۳</sup>	Comprehensive Processing <sup>۶</sup>
Botnet <sup>۲۴</sup>	Adaptive Learning <sup>۷</sup>
Amplification DDoS Attack <sup>۲۵</sup>	Packet Drop Rate <sup>۸</sup>
Github <sup>۲۶</sup>	Internet Service Provide (ISP) <sup>۹</sup>
Memcached Distributed Caching Memory System <sup>۲۷</sup>	Application <sup>۱۰</sup>
Traffic Peak <sup>۲۸</sup>	Client <sup>۱۱</sup>
Amazon Web Services <sup>۲۹</sup>	Service <sup>۱۲</sup>
Content Delivery Network(CDN) <sup>۳۰</sup>	Server <sup>۱۳</sup>
Cloudflare <sup>۳۱</sup>	Attacker <sup>۱۴</sup>
Mirai Malware <sup>۳۲</sup>	Flash Coward <sup>۱۵</sup>
Yandex <sup>۳۳</sup>	Data Stream <sup>۱۶</sup>
MikroTik <sup>۳۴</sup>	Sketch <sup>۱۷</sup>

X86 Process Architecture<sup>୧୦</sup>  
 Application Specific Integrated Circuit(ASIC)<sup>୧୧</sup>  
 Field Programmable Gate Array(FPGA)<sup>୧୨</sup>  
 Polling Mode<sup>୧୩</sup>  
 Network Function Virtualization<sup>୧୪</sup>  
 Driver<sup>୧୫</sup>  
 Berkely Packet Filter<sup>୧୬</sup>  
 Tcpdump<sup>୧୭</sup>  
 Byte Code<sup>୧୮</sup>  
 Register<sup>୧୯</sup>  
 Accumulator<sup>୨୦</sup>  
 Index Register<sup>୨୧</sup>  
 Program Counter<sup>୨୨</sup>  
 Just In Time Compiler(JIT)<sup>୨୩</sup>  
 MIPS Architecture<sup>୨୪</sup>  
 ARM Architecture<sup>୨୫</sup>  
 Extended BPF<sup>୨୬</sup>  
 Checkpoint<sup>୨୭</sup>  
 Forward<sup>୨୮</sup>  
 Data-Plane Programmable Switch<sup>୨୯</sup>  
 P4<sup>୩୦</sup>  
 Attack Mitigation<sup>୩୧</sup>  
 Middlebox<sup>୩୨</sup>  
 Network Intrusion Detection<sup>୩୩</sup>  
 Snort Intrusion Detection<sup>୩୪</sup>  
 IPFIX<sup>୩୫</sup>  
 Anomaly<sup>୩୬</sup>  
 Deep Packet Inspection(DPI)<sup>୩୭</sup>  
 RT-SAD<sup>୩୮</sup>

Unpatched<sup>୩୯</sup>  
 Cisco<sup>୪୦</sup>  
 FBI<sup>୪୧</sup>  
 Constrained Application Protocol<sup>୪୨</sup>  
 Attack Vector<sup>୪୩</sup>  
 Batch Processing<sup>୪୪</sup>  
 Stream Processing<sup>୪୫</sup>  
 Line Rate Processing<sup>୪୬</sup>  
 Turnstile Model<sup>୪୭</sup>  
 Internet Protocol(IP)<sup>୪୮</sup>  
 Port<sup>୪୯</sup>  
 Per Flow Size<sup>୫୦</sup>  
 Flow Moment<sup>୫୧</sup>  
 Moment-g<sup>୫୨</sup>  
 Heavy Hitter<sup>୫୩</sup>  
 Sampling<sup>୫୪</sup>  
 Count Sketch<sup>୫୫</sup>  
 Hash Function<sup>୫୬</sup>  
 Hash Collision<sup>୫୭</sup>  
 Count-Min Sketch<sup>୫୮</sup>  
 Universal Sketch<sup>୫୯</sup>  
 Univmon Sketch<sup>୬୦</sup>  
 TCP/IP Stack<sup>୬୧</sup>  
 Kernel<sup>୬୨</sup>  
 Network Interface Card<sup>୬୩</sup>  
 Direct Memory Access(DMA)<sup>୬୪</sup>  
 Data Plane Development Kit(DPDK)<sup>୬୫</sup>  
 eXpress Data Path(XDP)<sup>୬୬</sup>  
 Intel<sup>୬୭</sup>  
 Open Source Project<sup>୬୮</sup>