نام مقاله	وضعیت خلاصه (دارد/ندارد/نیازبه بهبود)	شرح مختصر	ارتباط در معماری
ACoPE: Adaptive Semi Supervised learning approach for complex-policy enforcement in high-bandwidth networks Computer Networks 2019	دارد	ارایه راهکاری برای شناسایی رفتار متغیر شبکه. سعی می‌کند وضعیت شبکه را با استفاده از برچسب گذاری متافلو ها(جریان‌های مختلف شبیه به هم با برچسپ‌های متعدد) نشان دهد(یک جور طبقه‌بندی) و وضعیت متافلوها را نگه می‌دارد. به صورت لحظه‌ای وضعیت پایداری هر متافلو را بررسی می‌کند و در صورت پایدارنبودن آن را از لیست حذف می‌کند. و هرگاه جریانی جدید وارد شد با استفاده از DPI و ویژگی‌های هر متافلو، آن را به متافلو مربوطه اضافه می‌کند	چون جریان‌های نزدیک به هم را دسته بندی می‌کند، می‌توان در قسمت firewall، از آن برای سرعت بخشیدن استفاده کرد.
Analyzing Performance issues of open-source intrusion detection systems in highspeed network Journal of Information Security and Applications 2020	دارد	این دو سامانه را در ترافیکهای بالای ۱۰۰ گیگ با معیارهای بار مصرفی پردازشگر،حافظه و تعداد بسته‌های دریافتی بررسی می‌کند .سوریکاتا امکانات بیشتری از جمله قابلیت پشتیبانی از اسکریپت دارد.در ترافیک‌های تا ۶۰ گیگ دقت بالایی خواهند داشت. قابلیت چندنخی ورژن‌های جدیدتر و استفاده از DPDK، AF_Packet و الگوریتم‌های تطابق الگوی پیشنهادی می‌توان عملکرد را بهبود بخشید. با XDP در سوریکاتا در ترافیک ۱۰۰ گیگ ولی تنها یک خط قانون می‌توان اعمال کرد.	می‌توان به عنوان فایروال اولیه از snort یا Suricata استفاده کرد. البته بایستی چندین نمونه گذاشت و از load balancing استفاده کرد
An Efficient IDS Framework for DDoS Attacks in SDN Environment IEEE Access 2021	بخش الگوریتم تشخیص و مقابله و پیاده سازی دقیق خوانده نشده است. این که چی می‌باشند. در صورت نیاز یکبار خوانده شود.	استفاده از شبکه‌های نرم افزار محور به دلیل ساده تر کردن برای مدیریت شبکه‌های پهن باند امروزی به کار گرفته می‌شود. با کمک ابزار DPDK یک الگوریتم تشخیص ناهنجاری به صورت VNF ارایه می‌دهد. به دلیل متمرکز بودن این معماری، کنترلر هدف اصلی می‌باشد. این روش مقداری از کار را به سوییچ‌های لایه داده واگذار می‌کند. وقتی داده‌ها را جمع آوری کرد با استفاده از آن‌ها یک فایل کانفیگ می‌سازد.	ارتباطی ندارد
Real-Time Sketch-Based Adaptive DDoS Detection for ISP Network Security and Communication Networks 2021	شیوه کار و ارتباط بین اسکچ‌ها بررسی شود.ارتباط بین ماژولها نیز بررسی شود.	تنظیم خودکار پارامترهای مدل. ویژگی‌های آماری جریان‌ها را در اسکچ‌ها ذخیره می‌کند. به این دلیل بلادرنگ نامیده شده است که ترافیک را پنجره ای بررسی می‌کند و پارامترها را تنظیم می‌کند.	شبیه به بخشی از طرح ما می‌باشد.

Surgical DDoS Filtering With Fast LPM IEEE Access 2022	نامفهوم.نیاز به بازخوانی می‌باشد.	ارایه راهکار جستجو و تطبیق سریع برای کویریهایی که رو LPM ها زده می‌شود در سرعت‌های بالا با مصرف کم حافظه و پردازشگر	در بخش فایروال که قوانین را می‌نویسیم، میتواند برای تطبیق به کاررود.
A High-Performance Switch-Native Approach for Detecting and Mitigating Volumetric DDoS Attacks with Programmable Switches USENIX 2021	دارد	برای سوییچهای ISP . شناسایی و مقابله بر روی خود سوییچ ها نه scrubbing center صورت می‌گیرد. .برای ضبط اطلاعات آماری بسته‌ها از اسکچهای universal استفاده می‌کند. یک ادمین مرکزی هم داریم که این سوییچها را مدیریت می‌کند. تخصیص منابع بر اساس منابع سوییچهای موجود (سازگارپذیر) و هدایت ترافیک و انتخاب استراتژی دفاعی و نحوه ضبط بسته‌ها را می‌تواند کانفیگ کند	بخش detection module و ادمینی که رولهایی را براساس آنها استخراج می‌کند، شبیه به هم هستند. اما بخش mitigation جاکن این قوانین را روی سوییچ ها پیاده می‌کند و ترافیک را به سمت آنها هدایت می‌کند اما در روش ما رولهایمان را بر روی فایروالها پیاده می‌کنیم. البته از سوییچهای برنامه پذیر هم مثل روش جاکن می‌توان استفاده کرد
Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches Network & Distributed System Security Symposium 2020	دارد. بخش پیاده سازی و ارزیابی خلاصه نشده است	روش‌های mitigation را بر روی سوییچها پیاده می‌کند، به صورت بهینه آن‌ها را مدیریت می‌کند. الگوریتم‌های دفاعی را بروی سوییچها پیاده می‌کند. برخی مکانیزم‌های دفاعی (به غیر از block و limit مثلcaptcha) را به صورت نرم‌افزاری بر روی سرورها پیاده می‌کند. با استفاده از اسکچها اطلاعات آماری را جمع آوری می‌کند اما در جزییات آن توضیح داده نشده است. الگوریتم‌های تشخیص را بر روی سوییچ پیاده می‌کند. و ترافیک‌را بین آنها تقسیم می‌کند	شبیه روش ما
Smart Defense: A distributed deep defense against DDoS attacks with edge computing Computer Networks 2022	دارد	روشی مبتنی بر یادگیری عمیق تطبیق پذیر برای تشخیص و مقابله بی‌نظمی به صورت توزیع شده در لبه مبدا(مشتری) و همچنین با امکان تشخیص باتها به کمک اطلاعات فراهم شده توسط فراهم کننده و ارسال ترافیک‌های باقی مانده برای تشخیص و مقابله در لبه مقصد(فراهم کننده). بر روی روترهای برنامه پذیر پیاده می‌شوند.الگوریتم اجراشده در روترهای مبدا سبکتر	ارتباطی ندارد.

		می‌باشند و ترافیک‌ها برای بررسی بیشتر با یکدیگر جمع شده و در لبه فراهم کننده بررسی خواهند شد. مقادیر آستانه مدل‌ها نیز توسط ادمین ISP تعیین می‌شود	
A new DDoS attacks intrusion detection model based on deep learning for cybersecurity Computer & Security 2022	دارد	داده ورودی را پیش پردازش می‌کند(نرمالیزه کردن)، خصیصه‌های مهم را می‌یابد. مدل‌های مختلف شبکه عمیق را با هم مقایسه می‌کند.	بخش CNN می‌تواند استفاده شود
Towards Nearly-Zero-Error Sketching via Compressive Sensing USENIX 2021	دارد اما کامل خلاصه نشده است و علاوه بر آن نامفهوم می‌باشد. باید یکبار دیگر خوانده شود	طراحی اسکچی که اطلاعات تمامی جریان‌ها را(حتی کوچک‌ها) را نیز می‌تواند با دقت بالایی نگه دارد(خطای کم) با استفاده از الگوریتم compressive sensing. بر پایه اسکچ و با استفاده از این الگوریتم، گونه جدیدی از اسکچ‌ها ارایه می‌دهد.	چون هدف ما شناسایی حملات منع خدمت توزیع شده با حجم زیاد می‌باشد(heavy hitter)، نیازی به اسکچ‌های دقیق‌تر شاید نباشد.
Signature-Based Traffic Classification and Mitigation for DDoS Attacks Using Programmable Network Data-Planes IEEE ACCESS 2021	دارد	روشی که با استفاده از یادگیری ماشین نظارتی حداقل ویژگی های بسته‌های متخاصم را به عنوان امضای حملات تعیین می‌کند و قوانین فیلتر کمینه را تولید می‌کند و از XDP هم استفاده می‌کند. مدل های یادگیری ماشین را نیز از قبل آموزش داده ایم.	شبیه روش ما می‌باشد. تنها از اسکچ‌ها استفاده نکرده است
Sketch-based Change Detection: Methods, Evaluation, and Applications ACM 2003	دارد	معرفی اسکچ‌ها که اطلاعات آماری را نگه می‌دارند به عنوان روشی برای تشخیص بی نظمی با استفاده بهینه از حافظه. اسکچی از نوع ارایه جند بعدی معرفی می‌کند(مثل همون count-sketch). و سپس یک مدل پیش‌بینی سری زمانی از اطلاعات آن استفاده می‌کند تا مقدار موردانتظار هر جریان را به دست آورد و با مقایسه مقادیر واقعی با اینها می‌تواند بی‌نظمی را تشخیص دهد. در آخر به مقایسه اسکچ ارایه شده با روش نگهداری اطلاعات هر جریان می‌پردازد. و بهترین مدل پیش‌بینی سری زمانی را نیز انتخاب می‌کند.	صرفاً جهت آشنایی معرفی مسایل دیتا استریم و اسکچ‌ها به عنوان راه حلی برای آنها.

On High-Speed Flow-based Intrusion Detection using Snort compatible Signatures IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING 2020	دارد	ارایه روشی به نام FIXIDS که از امضاهای مبتنی بر IPFIX HTTP قوانینی تولید می‌کند که می‌تواند در کنار snort از آن استفاده کرد. پروتکل IPFIX استاندارد اصلی برای جمع‌آوری اطالعات بسته‌ها در قالب جریان برای پردازشهای بیشترمی‌باشد.(جایگزین عمومی برای netflow)	برای بخش فایروال که مبتنی بر امضا می‌باشد، می‌تواند استفاده شود
Low-rate DDoS attack detection method using data compression and behavior divergence measurement (LDDM) Computer Security 2021	دارد. اما نامفهوم می‌باشد.	الگوریتمی (با استفاده از الگوریتم‌های موجود در حوزه سیگنال) با استفاده از اسکچها ارایه می‌دهد که می‌تواند حملات منع‌خدمت با نرخ پایین و بی نظمی آنها را تشخیص دهد از واگرایی بین جداول اسکچ فعلی و قبلی(جداول اسکچ را مثل سیگنال در نظر می‌گیرد) استفاده می‌کند.(انرژی واگرایی سیگنال را محاسبه می‌کند)	در بخش sketch ها و الگوریتم‌ها نیز در بخش detection module به کار می‌روند.
BigFlow: Real-time and Reliable Anomaly based Intrusion Detection for High-Speed Networks Future Generation Computer Systems 2019	دارد	مدل نظارتی با رویکرد یادگیری افزایشی. نمونه‌هایی که classifier با اطمینان بالایی به عنوان مهاجم شناسایی نمی‌کند را به عنوان معیاری برای تغییر در شبکه در نظر می‌گیرد و با استفاده از آن نمونه‌ها بروزرسانی افزایشی مدل را انجام می‌دهد. اون رویداد را بعداً ادمین برچسب گذاری می‌کند. و این بروزرسانی افزایشی می‌تواند به کاهش زمان یادگیری و افزایش دقت بیانجامد. همچنین دیتاستی که استفاده می‌کند یک نوع جدید می‌باشد ضبط شده در طول یک سال می‌باشد.	روش ارایه شده برای بخش flow aggregator و CNN می‌تواند استفاده شود
DHS: Adaptive Memory Layout Organization of Sketch Slots for Fast and Accurate Data Stream Processing ACM 2021	دارد. بخش ارزیابی و تعیین کران خطای تخمین خلاصه نشده است.	این مقاله قصد دارد یک ساختار حافظه‌ای متغیر(بنا به نیاز هر جریان سایز آن افزایش می‌یابد) به منظور استفاده اسکچها ارایه دهد که به تسریع و افزایش دقت بازیابی بیانجامد. اما فرقش با اسکچها در این می‌باشد که	مرتبط نیست اما می‌توان این روش را به جای اسکچها برای اندازه‌گیری آمار ترافیک به کار برد.

		اطلاعات را دقیق تر در المان‌هایی به نام باکت ذخیره می‌کند	
Active learning to detect DDoS attack using ranked features Computer Communications 2019	دارد. اما بحث یادگیری فعال، SVM ها و Support Vector ها باید پیش زمینه داشت.	ارایه الگوریتمی برای استخراج ویژگی در شبکه‌های پهن‌باند با الگوهای ترافیکی متغیر که از رتبه بندی تجمعی موازی برای رتبه بندی ویژگی‌های دیتاست(این که کدوم مجموعه ویژگی ها را انتخاب کنیم و بر اساس اون تقسیم بندی کنیم) و یادگیری فعال نیمه نظارتی استفاده می‌کند. یک فرد خبره(ادمین) با بررسی بیشتر الگوهای نمونه‌های برچسب گذاری نشده، به آنها برچسب می‌زند و دایماً مجموعه آموزشی را بروز می‌کند.	
Multi-Level Elasticity for Data Stream Processing IEEE Transactions on Parallel and Distributed Systems 2018	دارد	محاسبات استریمی یکی از راه‌های پردازش بیگ دیتا می‌باشد. یک روش بهینه کشسان برای مدیریت منابع(کانتینرها) برای فریمورک پردازش استریمی Apache Storm ارایه می‌دهد. یکی از موارد بررسی اپلیکیشن ارایه شده، استفاده از آن برای تشخیص حملات DDoS می‌باشد.	ارتباطی ندارد.
The Hybrid Technique for DDoS Detection with Supervised Learning Algorithms Computer Networks 2019	برخی ابهامات در سمت سرور می‌باشد	استفاده از یادگیری افزایشی و تقسیم کار بین کلاینت و سرور با پیاده سازی الگوریتم‌های ML مختلف مثل:random forest,MLP,... classifier ها را با یک مجموعه ویژگی اولیه آموزش می‌دهیم ولی به مرور یک ویژگی به آن اضافه کرده تا جایی که دیگر عملکرد ماژول تغییری نکند. در سمت کلاینت با استخراج ویژگی‌ها و پس از بررسی دیورژانس اگر متخاصم نبود، آن را برای تحلیل به classifier می فرستد که اگر تشخیص حمله داد، دیورژانس را بروز می‌کند و اگر سالم بود به سرور می فرستد که در آنجا نیز می‌تواند بررسی بیشتر کند.	ارتباطی ندارد