

نام مقاله	وضعیت خلاصه ) دارد/ندارد/نیاز به بهبود)	شرح مختصر	ارتباط در معماری
ACoPE: Adaptive Semi Supervised learning approach for complex-policy enforcement in high-bandwidth networks <i>Computer Networks</i> 2019	دارد	ارایه راهکاری برای شناسایی رفتار متغیر شبکه. سعی می کند وضعیت شبکه را با استفاده از برچسب گذاری متافلو ها) جریان های مختلف شبیه به هم با برچسب های متعدد( نشان دهد(یک جور طبقه بندی) و وضعیت متافلوها را نگه می دارد. به صورت لحظه ای وضعیت پایداری هر متافلو را بررسی می کند و در صورت پایداری نبودن آن را از لیست حذف می کند. و هرگاه جریانی جدید وارد شد با استفاده از DPI و ویژگی های هر متافلو، آن را به متافلو مربوطه اضافه می کند	چون جریان های نزدیک به هم را دسته بندی می کند، می توان در قسمت firewall، از آن برای سرعت بخشیدن استفاده کرد.
Analyzing Performance issues of open-source intrusion detection systems in highspeed network <i>Journal of Information Security and Applications</i> 2020	دارد	این دو سامانه را در ترافیک های بالای ۱۰۰ گیگ با معیارهای بار مصرفی پردازشگر، حافظه و تعداد بسته های دریافتی بررسی می کند. سوریکاتا امکانات بیشتری از جمله قابلیت پشتیبانی از اسکرپت دارد. در ترافیک های تا ۶۰ گیگ دقت بالایی خواهند داشت. قابلیت چندنخی ورژن های جدیدتر و استفاده از DPDK، AF_Packet و الگوریتم های تطابق الگوی پیشنهادی می توان عملکرد را بهبود بخشید. با XDP در سوریکاتا در ترافیک ۱۰۰ گیگ ولی تنها یک خط قانون می توان اعمال کرد.	می توان 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 <i>IEEE Access</i> 2021	بخش الگوریتم تشخیص و مقابله و پیاده سازی دقیق خوانده نشده است. این که چی می باشند. در صورت نیاز یکبار خوانده شود.	استفاده از شبکه های نرم افزار محور به دلیل ساده تر کردن برای مدیریت شبکه های پهن باند امروزی به کار گرفته می شود. با کمک ابزار DPDK یک الگوریتم تشخیص ناهنجاری به صورت VNF ارایه می دهد. به دلیل متمرکز بودن این معماری، کنترلر هدف اصلی می باشد. این روش مقداری از کار را به سویچ های لایه داده واگذار می کند. وقتی داده ها را جمع آوری کرد با استفاده از آن ها یک فایل کانفیگ می سازد.	ارتباطی ندارد
Real-Time Sketch-Based Adaptive DDoS Detection for ISP Network <i>Security and Communication Networks</i> 2021	شیوه کار و ارتباط بین اسکچ ها بررسی شود. ارتباط بین ماژولها نیز بررسی شود.	تنظیم خودکار پارامترهای مدل. ویژگی های آماری جریان ها را در اسکچ ها ذخیره می کند. به این دلیل بلادرنگ نامیده شده است که ترافیک را پنجره ای بررسی می کند و پارامترها را تنظیم می کند.	شبیه به بخشی از طرح ما می باشد.

در بخش فایروال که قوانین را می نویسیم، میتواند برای تطبیق به کار رود.	ارایه راهکار جستجو و تطبیق سریع برای کویریهای که رو LPM ها زده می شود در سرعت های بالا با مصرف کم حافظه و پردازشگر	نامفهوم. نیاز به بازخوانی می باشد.	Surgical DDoS Filtering With Fast LPM IEEE Access 2022
بخش detection module و ادمینی که رولهایی را براساس آنها استخراج می کند، شبیه به هم هستند. اما بخش mitigation جاکن این قوانین را روی سویچ ها پیاده می کند و ترافیک را به سمت آنها هدایت می کند اما در روش ما رولهایمان را بر روی فایروالها پیاده می کنیم. البته از سویچ های برنامه پذیر هم مثل روش جاکن می توان استفاده کرد	برای سویچ های ISP . شناسایی و مقابله بر روی خود سویچ ها نه scrubbing center صورت می گیرد. برای ضبط اطلاعات آماری بسته ها از اسکیچ های universal استفاده می کند. یک ادمین مرکزی هم داریم که این سویچ ها را مدیریت می کند. تخصیص منابع بر اساس منابع سویچ های موجود (سازگارپذیر) و هدایت ترافیک و انتخاب استراتژی دفاعی و نحوه ضبط بسته ها را می تواند کانفیگ کند	دارد	A High-Performance Switch-Native Approach for Detecting and Mitigating Volumetric DDoS Attacks with Programmable Switches USENIX 2021
شبیه روش ما	روش های mitigation را بر روی سویچ ها پیاده می کند، به صورت بهینه آنها را مدیریت می کند. الگوریتم های دفاعی را بروی سویچ ها پیاده می کند. برخی مکانیزم های دفاعی ( به غیر از block و limit مثل captcha ) را به صورت نرم افزاری بر روی سرورها پیاده می کند. با استفاده از اسکیچ ها اطلاعات آماری را جمع آوری می کند اما در جزئیات آن توضیح داده نشده است. الگوریتم های تشخیص را بر روی سویچ پیاده می کند. و ترافیک را بین آنها تقسیم می کند	دارد. بخش پیاده سازی و ارزیابی خلاصه نشده است	Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches Network & Distributed System Security Symposium 2020
ارتباطی ندارد.	روشی مبتنی بر یادگیری عمیق تطبیق پذیر برای تشخیص و مقابله بی نظمی به صورت توزیع شده در لبه مبدا(مشرتی) و همچنین با امکان تشخیص باتها به کمک اطلاعات فراهم شده توسط فراهم کننده و ارسال ترافیک های باقی مانده برای تشخیص و مقابله در لبه مقصد(فراهم کننده). بر روی روترهای برنامه پذیر پیاده می شوند. الگوریتم اجرا شده در روترهای مبدا سبکتر	دارد	Smart Defense: A distributed deep defense against DDoS attacks with edge computing Computer Networks 2022

	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		
بخش CNN می‌تواند استفاده شود	داده ورودی را پیش پردازش می‌کند (نرمالیزه کردن)، خصیصه‌های مهم را می‌یابد. مدل‌های مختلف شبکه عمیق را با هم مقایسه می‌کند.	دارد	A new DDoS attacks intrusion detection model based on deep learning for cybersecurity Computer & Security 2022
چون هدف ما شناسایی حملات منع خدمت توزیع شده با حجم زیاد می‌باشد (heavy hitter)، نیازی به اسکچ‌های دقیق‌تر شاید نباشد.	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 ارائه می‌دهد.	دارد اما کامل خلاصه نشده است و علاوه بر آن نامفهوم می‌باشد. باید یکبار دیگر خوانده شود	Towards Nearly-Zero-Error Sketching via Compressive Sensing USENIX 2021
شبیه روش ما می‌باشد. تنها از اسکچ‌ها استفاده نکرده است	روشی که با استفاده از یادگیری ماشین نظارتی حداقل ویژگی‌های بسته‌های متخصص را به عنوان امضای حملات تعیین می‌کند و قوانین فیلتر کمینه را تولید می‌کند و از XDP هم استفاده می‌کند. مدل‌های یادگیری ماشین را نیز از قبل آموزش داده ایم.	دارد	Signature-Based Traffic Classification and Mitigation for DDoS Attacks Using Programmable Network Data-Planes IEEE ACCESS 2021
صرفاً جهت آشنایی معرفی مسایل دیتا استریم و اسکچ‌ها به عنوان راه حلی برای آنها.	معرفی اسکچ‌ها که اطلاعات آماری را نگه می‌دارند به عنوان روشی برای تشخیص بی‌نظمی 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 مورد انتظار 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.	دارد	Sketch-based Change Detection: Methods, Evaluation, and Applications ACM 2003

<p>برای بخش فایروال که مبتنی بر امضا می‌باشد، می‌تواند استفاده شود</p>	<p>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 اطلاعات بسته‌ها در قالب جریان برای پردازشهای بیشتر می‌باشد. (جایگزین عمومی برای netflow)</p>	<p>دارد</p>	<p>On High-Speed Flow-based Intrusion Detection using Snort compatible Signatures IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING 2020</p>
<p>در بخش sketch ها و الگوریتم‌ها نیز در بخش detection module به کار می‌روند.</p>	<p>الگوریتمی ( با استفاده از الگوریتم‌های موجود در حوزه سیگنال) با استفاده از اسکچ‌ها ارایه می‌دهد که می‌تواند حملات منع خدمت 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)</p>	<p>دارد. اما نامفهوم می‌باشد.</p>	<p>Low-rate DDoS attack detection method using data compression and behavior divergence measurement (LDDM) Computer Security 2021</p>
<p>روش ارایه شده برای بخش flow aggregator و CNN می‌تواند استفاده شود</p>	<p>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 برجسب 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.</p>	<p>دارد</p>	<p>BigFlow: Real-time and Reliable Anomaly based Intrusion Detection for High-Speed Networks Future Generation Computer Systems 2019</p>
<p>مرتبط نیست اما می‌توان این روش را به جای اسکچ‌ها برای اندازه‌گیری آمار ترافیک به کار برد.</p>	<p>این مقاله قصد دارد یک ساختار حافظه‌ای متغیر (بنا به نیاز هر جریان سباز آن افزایش می‌یابد) به منظور استفاده اسکچ‌ها ارایه دهد که به تسریع و افزایش دقت بازیابی بیانجامد. اما فرقی با اسکچ‌ها در این می‌باشد که</p>	<p>دارد. بخش ارزیابی و تعیین کران خطای تخمین خلاصه نشده است.</p>	<p>DHS: Adaptive Memory Layout Organization of Sketch Slots for Fast and Accurate Data Stream Processing ACM 2021</p>

	اطلاعات را دقیق تر در المان‌هایی به نام باکت ذخیره می‌کند		
	ارایه الگوریتمی برای استخراج ویژگی در شبکه‌های پهن‌بند با الگوهای ترافیکی متغیر که از رتبه بندی تجمعی موازی برای رتبه بندی ویژگی‌های دیتاست (این که کدوم مجموعه ویژگی‌ها 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 برجسب گذاری نشده، به آنها برجسب می‌زند و دائماً مجموعه آموزشی را بروز می‌کند.	دارد. اما بحث یادگیری فعال، SVM ها و Support Vector ها باید پیش زمینه داشت.	Active learning to detect DDoS attack using ranked features Computer Communications 2019
ارتباطی ندارد.	محاسبات استریمی یکی از راه‌های پردازش بیگ دیتا می‌باشد. یک روش بهینه کشسان برای مدیریت منابع (کانتینرها) برای فریمورک Apache Storm پردازش استریمی ارایه می‌دهد. یکی از موارد بررسی اپلیکیشن ارایه شده، استفاده از آن برای تشخیص حملات DDoS می‌باشد.	دارد	Multi-Level Elasticity for Data Stream Processing IEEE Transactions on Parallel and Distributed Systems 2018
ارتباطی ندارد	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 می‌فرستد که اگر تشخیص حمله داد، دیورژانس را بروز می‌کند و اگر سالم بود به سرور می‌فرستد که در آنجا نیز می‌تواند بررسی بیشتر کند.	برخی ابهامات در سمت سرور می‌باشد	The Hybrid Technique for DDoS Detection with Supervised Learning Algorithms Computer Networks 2019
ارتباط دارد	اسکچی به نام bacon ارایه می‌دهد که از direct bitmap و Count-Min	دارد	In Network Volumetric DDoS Victim Identification using

	<p>Sketch استفاده می‌کند و جریانات منحصر به فرد به یک مقصد را شناسایی می‌کند و بر اساس مقدار آستانه می‌باشد. لذا قربانی را می‌تواند شناسایی کند و به صورت عملی بر روی سویچ‌های واقعی پیاده می‌کند. در مورد اینکه چگونه مقدار آستانه پیدا شود، به تفصیل بحثی نمی‌کند.</p>		<p>Programmable Commodity Switches IEEE Transactions on Network &amp; System Management 2021</p>
دارد	<p>اسکچی که ارایه می‌دهد علاوه بر heavz hitter ها moment ها را هم با دقت بالایی تخمین می‌زند. مزیت آن هم تعداد دفعات دسترسی به حافظه می‌باشد (در حین عملیات ورود بسته جدید و کویری زدن)</p>	دارد	<p>Universal Online Sketch for Tracking Heavy Hitters and Estimating Moments of Data Streams IEEE INFOCOM 2020</p>
ارتباط مستقیم ندارد.	<p>هدف اصلی پیاده سازی اسکچ‌ها (الگوریتم‌های مانیتورینگ) به صورت بهینه بر روی سویچ‌های مختلف با در نظر گرفتن این نکات که الگوی ترافیک شبکه در حال تغییر است و عملیات دیگری بر روی سویچ‌ها در حال انجام است و لذا منابع موجود سویچ‌ها در حال تغییر است.</p>	<p>کامل نیست. جزئیات عملیات پروفایلینگ و تخصیص خلاصه نشده است.</p>	<p>HeteroSketch: Coordinating Network-wide Monitoring in Heterogeneous and Dynamic Networks USENIX NSDI 2022</p>
ارتباط دارد در شناسایی حملات منع خدمت volumetric می‌تواند استفاده شود	<p>چالش اصلی استفاده بهینه از حافظه برای شناسایی top-k ها (heav hitter) به منظور پیاده سازی بر روی سویچ‌های برنامه پذیر می‌باشد، بدین منظور الگوریتمی برای ضبط بسته‌ها ارایه می‌دهد. که برای هر بسته دریافتی، تعداد عملیات write را کاهش دهد.</p>	<p>کامل نیست (۵۰٪)</p>	<p>Heavy Hitter Detection Entirely in Data-Plane ACM 2017</p>