#	نام مقاله	وضعیت خلاصه (دارد/ندارد/نیازبه بهبود)	شرح مختصر	ارتباط در معماری	تنوع ترافیکی
۱	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 بخش جمع آوری از آن استفاده کرد. به عنوان ماژول ACOPE استفاده می‌شود.	این که جریان‌های شبیه به هم را سعی می‌کند، دسته بندی کند و به صورت پویا نیز این کار را انجام می‌دهد، برای حل تنوع پروتکلی می‌توان استفاده کرد. برای شناسایی و برچسپ گذاری نیز از DPI استفاده می‌کند. ولی این که هرکدام از این جریان‌ها کدامشان آنومالی دارند بسته به آن اپلیکیشنی که استفاده می‌شوند، باید بررسی شود.
۲	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 ارتباطی ندارد	-
۳	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.	شبکه‌های نرم افزار محور به دلیل ساده تر کردن امور، برای مدیریت شبکه‌های پهن باند امروزی به کار گرفته می‌شوند. 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 می‌توان از ابزارهای مانیتورینگ و ارسال خطای معرفی شده و ابزار تولید فایل yaml استفاده کرد Promethus , Grafana➔ detection module : monitoring and sending alert	صحبتی نکرده است. تنها از یک معیار به عنوان مقدار آستانه استفاده می‌کند. که آنهم سازگارپذیر (پویا) نمی‌باشد.
۴	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.	۴شبیه به بخشی از طرح ما می‌باشد. شیوه کارکرد اسکچ‌ها و این که چگونه مقادیر را پیش بینی می‌کند و چگونه با استفاده از آنها و داده پنجره فعلی، حمله را تشخیص	از ویژگی نامتقارن بودن، استفاده می‌کند که برای همه اپلیکیشن‌ها کاربرد ندارد. البته این که چقدر اختلاف قابل قبول هست را نیز از ترافیک‌های قبلی به دست می‌آورد.

				Sketches, ← می‌دهد Detection Module	
۵	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. ارتباطی ندارد	-
۶	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 بخش جمع آوری اطلاعات توسط سوییچ‌های لایه داده و کویری‌هایی که ادمین می‌زند و حمله را از روی آنها تشخیص می‌دهد(راهکار ارتباطی شان) می‌تواند در بخش‌های مربوطه استفاده شود.	صحبتی نشده است. در مقاله ذکر شده است که محتوای پیلود بسته‌ها را بررسی نمی‌کند. حملات flood,amplification بر روی پروتکل‌های متداول را با استفاده از الگوریتم‌ها و اسکچ‌های مختلف تشخیص می‌دهد برای برخی حمله‌ها نیز گفته شده است با همان API ها می‌توان تشخیص داد.
۷	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 مثل captcha) 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 شبیه به جاکن	شبیه به مقاله Jaqen می‌باشد.
۸	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 می‌باشند و	ارتباطی ندارد. ارتباطی ندارد	

		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			
۹	A new DDoS attacks intrusion detection model based on deep learning for cybersecurity Computer & Security 2022	داده ورودی را پیش پردازش می‌کند(نرمالیزه کردن)، خصیصه‌های مهم را می‌یابد. مدل‌های مختلف شبکه عمیق را با هم مقایسه می‌کند.	دارد	بخش CNN می‌تواند استفاده شود این مدل هم مثل بالایی، سعی در شناسایی و به دست آوردن امضای متخاصم ها دارد به جای بخش AcoPE می‌تواند استفاده شود.	
۱۰	Towards Nearly-Zero-Error Sketching via Compressive Sensing USENIX 2021	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.	دارد اما کامل خلاصه نشده است و علاوه بر آن نامفهوم می‌باشد. باید یکبار دیگر خوانده شود	چون هدف ما شناسایی حملات منع خدمت توزیع شده با حجم زیاد می‌باشد(heavy hitter)، نیازی به اسکچ‌های دقیق‌تر شاید نباشد. با توجه به این‌که ما از چندین اسکچ استفاده خواهیم کرد، لذا این روش می‌تواند مفید باشد.	
۱۱	Signature-Based Traffic Classification and Mitigation for DDoS Attacks Using Programmable Network Data-Planes IEEE ACCESS 2021	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.	دارد	شبیه روش ما می‌باشد. تنها از اسکچ‌ها استفاده نکرده است در بخش Detection Module می‌تواند استفاده شود.	
۱۲	Sketch-based Change Detection: Methods, Evaluation, and Applications ACM 2003	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.	دارد	صرفاً جهت آشنایی معرفی مسایل دیتا استریم و اسکچ‌ها به عنوان راه حلی برای آنها. شبیه به روش ما و استفاده از اسکچ‌ها می‌باشد.	
۱۳	On High-Speed Flow-based Intrusion Detection using	ارایه روشی به نام FIXIDS که از امضاهای مبتنی بر IPFIX HTTP قوانینی تولید می‌کند که می‌تواند در کنار snort از آن استفاده کرد.	دارد	برای بخش فایروال که مبتنی بر امضا می‌باشد، می‌تواند استفاده شود	

	Snort compatible Signatures IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING 2020		پروتکل IPFIX استاندارد اصلی برای جمع‌آوری اطالعات بسته‌ها در قالب جریان برای پردازشهای بیشترمی‌باشد.(جایگزین عمومی برای netflow)	در بخش AcoPE و جمع آوری و دسته‌بندی اطلاعات می‌تواند استفاده شود	
۱۴	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. از الگوریتم تشخیص می توان برای شناسایی این‌گونه حملات استفاده کرد	
۱۵	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 به جای بخش AcoPE می‌تواند استفاده شود	
۱۶	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 اطلاعات را دقیق تر در المان‌هایی به نام باکت ذخیره می‌کند	مرتبط نیست اما می‌توان این روش را به جای اسکچ‌ها برای اندازه‌گیری آمار ترافیک به کار برد.	
۱۷	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.		

۱۸	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.	
۱۹	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	
۲۰	In Network Volumetric DDoS Victim Identification using Programmable Commodity Switches IEEE Transactions on Network & System Management 2021	دارد	اسکچی به نام bacon ارایه می‌دهد که از direct bitmap و Count-Min 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 سوییچ‌های واقعیی پیاده می‌کند. در مورد اینکه چگونه مقدار آستانه پیدا شود،به تفصیل بحثی نمی‌کند.	ارتباط دارد	
۲۱	Universal Online Sketch for Tracking Heavy Hitters and Estimating Moments of Data Streams IEEE INFOCOM 2020	دارد	اسکچی که ارایه می‌دهد علاوه بر heavz hitter ها moment هارا هم با دقت بالایی تخمین می‌زند. مزیت آن هم تعداد دفعات دسترسی به حافظه می‌باشد (در حین عملیات ورود بسته جدید و کویری زدن)	دارد	
۲۲	HeteroSketch: Coordinating Network-wide Monitoring in Heterogeneous and Dynamic Networks	کامل نیست. جزیات عملیات پروفایلینگ و تخصیص خلاصه نشده است.	هدف اصلی پیاده سازی اسکچ‌ها (الگوریتم‌های مانیتورینگ) به صورت بهینه برروی سوییچ‌های مختلف با درنظرگرفتن این نکات که الگوی ترافیک شبکه در حال تغییر است و عملیات دیگری بر روی سوییچ‌ها در حال انجام است و لذا منابع موجود سوییچ‌ها در حال تغییر است.	ارتباط مستقیم ندارد.	

				USENIX NSDI 2022	
	ارتباط دارد در شناسایی حملات منع خدمت volumetric می‌تواند استفاده شود	چالش اصلی استفاده بهینه از حافظه برای شناسایی top-k ها(heav hitter) به منظور پیاده سازی بر روی سوییچ‌های برنامه پذیر می‌باشد، بدین منظور الگوریتمی برای ضبط بسته‌ها ارایه می‌دهد. که برای هربسته دریافتی، تعداد عملیات write را کاهش دهد.	کامل نیست(۵۰٪)	Heavy Hitter Detection Entirely in Data-Plane ACM 2017	۲۳
				Bayesian Sketches for Volume Estimation in Data Streams ETH Zürich 2022	۲۴
				Elastic Sketch: Adaptive and Fast Network-wide Measurements ACM 2018	۲۵
				One Sketch to rule them All ACM 2016	۲۶
				Finding Frequent items in data streams 2004	۲۷
				An improved data stream summary: the count-min sketch and its applications 2005	۲۸
				High Speed Traffic Generation 2020 ETH Zürich	۲۹
	ارتباطی ندارد. چون به موضوع تنوع رفتار پروتکل‌ها توجهی نمی‌کند	۴ مشخصه‌ای که در هنگام حملات منع، با تغییر واضحی همگام هستند را به عنوان شناسه در نظر گرفته و بر اساس مقدار آستانه‌ای که آن را نیز برحسب واریانس و میانگین این مقادیر به دست می‌اورد، سعی در تشخیص حملات در هر بازه زمانی دارد	دارد	Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic Computer& Security 2019	۳۰
	سعی می‌کند رفتار ترافیک دسترسی کاربر را به دست بیارد، اما پویا نمی‌باشد	سعی می‌کند توزیع رفتار کاربر در هنگام تعامل با سایت‌ها را به دست بیاورد(بر اساس مشخصه‌های طول بسته‌ها و فاصله زمانی بین ورود	نیاز به مطالعه دقیق تر دارد. برخی	Identifying Application-Layer DDoS Attacks	۳۱

		بسته‌ها) و هرزمان که این توزیع با جهش همراه بود، به معنای وقوع یک حمله می‌باشد. RM را با RM های زیرین مقایسه می‌کنیم و هر کدام که درصد outlier هاش بیش از حد بود، به عنوان هاست متخاصم شناسایی می‌کند.	صفحات به درستی درک نشده است.	Based on Request Rhythm Matrices IEEE ACCESS 2019	
				EUCLID: A Fully InNetwork, P4-based Approach for Real-Time DDoS Attack Detection and Mitigation IEEE Transactions on Network and Service Management 2020	۳۲
	می‌تواند ارتباط داشته باشد.چون روشی برای تخمین آنتروپی			Data Streaming Algorithms for Estimating Entropy of Network Traffic ACM 2006	۳۳
				Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review Security and Communication Networks 2022	۳۴