Review

حملهٔ توزیع‌شدهٔ منع سرویس (DDoS) در شبکه‌های نرم‌افزارمحور (SDN): مروری بر مجموعه‌داده‌های باز، بردارهای حمله و راهبردهای کاهش‌دهی

Winston Hill1 · Yaa Takyiwaa Acquaah1 · Janelle Mason1 · Daniel Limbrick1 · Stephanie Teixeira-Poit 1 · Carla Coates1· Kaushik Roy1

Received: 25 June 2024 / Accepted: 26 August 2024
Published online: 31 August 2024
© The Author(s) 2024 OPEN

چکیده

حملات توزیع‌شدهٔ منع سرویس (DDoS) تهدیدی جدی برای شبکه‌های نرم‌افزارمحور (SDN) بوده و اغلب توسط عاملان مخرب به کار گرفته می‌شوند SDN .به‌عنوان یک الگوی برجستهٔ شبکه ظهور کرده است و با جدا کردن صفحهٔ کنترل و داده، امکان کنترل و برنامه‌پذیری بیشتری بر شبکه فراهم می‌کند. در مقایسه با شبکه‌های سنتی، SDNراه‌حل‌هایی پویا، چابک، مقرون‌به‌صرفه و قابل مدیریت ارائه می‌دهد. با این حال، یک ضعف قابل‌توجه SDN این است که کنترل‌کنندهٔ مرکزی به یک سطح حملهٔ آسیب‌پذیر تبدیل می‌شود و آن را در برابر تصرف کامل شبکه از طریق حملات DDoS آسیب‌پذیر می‌سازد. نوآوری این مقاله گردآوری منابعی است که برای کاهش حملات DDoS در محیط‌های SDN مورد استفاده قرار خواهند گرفت. این مقاله بر بررسی مجموعه‌داده‌های باز شامل حملات DDoS و همچنین بررسی تکنیک‌ها و چارچوب‌های تشخیص و کاهش حمله تمرکز دارد. با تحلیل راهبردهای مختلف تشخیص و مقابله، مدیران شبکه و متخصصان امنیت می‌توانند تصمیمات آگاهانه‌تری برای افزایش استحکام و تاب‌آوری محیط‌های SDN در برابر تهدیدات تکامل‌یابندهٔ DDoS اتخاذ کنند.

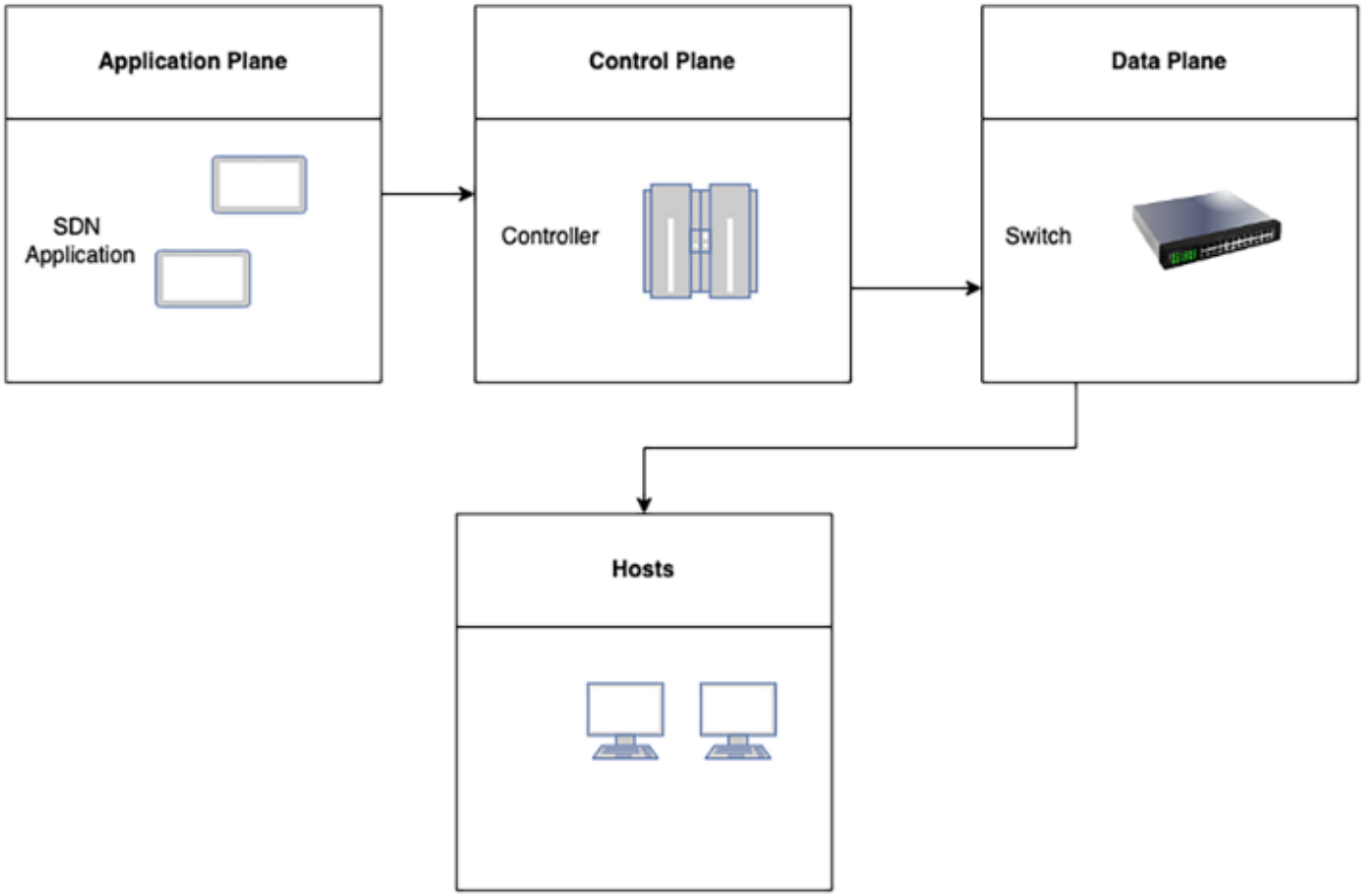
واژه‌های کلیدی: شبکهٔ نرم‌افزارمحور، حملات توزیع‌شدهٔ منع سرویس، مجموعه‌داده‌های باز

۱ .مقدمه

شبکه‌های توزیع‌شدهٔ سنتی به سامانه‌های به‌هم‌پیوسته‌ای اشاره دارند که در آن منابع محاسباتی، داده‌ها و وظایف به‌جای متمرکز بودن در یک مکان واحد، در میان چندین گره توزیع شده‌اند. این شبکه‌ها طی دهه‌ها نقش بنیادی در تسهیل ارتباطات، اشتراک‌گذاری منابع و همکاری در محیط‌های مختلف محاسباتی ایفا کرده‌اند. در شبکه‌های توزیع‌شدهٔ سنتی، هر گره به‌طور مستقل عمل می‌کند و از طریق پروتکل‌های تعریف‌شده با سایر گره‌ها ارتباط برقرار می‌کند، که این امر امکان تصمیم‌گیری غیرمتمرکز و عملکرد تحمل‌پذیر در برابر خطا را فراهم می‌سازد. نمونه‌هایی از شبکه‌های توزیع‌شدهٔ سنتی شامل معماری‌های کاربر–سرویس‌دهنده، شبکه‌های همتابه‌همتا (P2P) و سامانه‌های فایل توزیع‌شده هستند که نقش‌های مهمی در کاربردهایی مانند میزبانی وب، تحویل محتوا و محاسبات توزیع‌شده داشته‌اند. در شبکه‌های توزیع‌شدهٔ سنتی، صفحهٔ داده و صفحهٔ کنترل با استفاده از دستگاه‌های سخت‌افزاری مانند روترها و سوئیچ‌ها پیاده‌سازی می‌شوند. اپراتورهای شبکه، سیاست‌های ترافیکی را برای هر دستگاه پیکربندی می‌کنند که شامل کیفیت خدمات، مسیریابی و سوئیچینگ است. با این حال، شبکهٔ نرم‌افزارمحور (SDN) با معرفی رویکردی انعطاف‌پذیرتر و قابل مدیریت‌تر، قصد دارد محدودیت‌های شبکه‌سازی سنتی را برطرف کند SDN .صفحهٔ کنترل و صفحهٔ داده را از هم جدا می‌کند و این امر امکان تنظیم‌پذیری بیشتر و سهولت مدیریت را فراهم می‌سازد. جداسازی صفحات مختلف در شکل ۱ نشان داده شده است . SDNمزایایی همچون کنترل متمرکز از طریق یک دستگاه راه دور به نام کنترل‌کننده. این جداسازیِ صفحهٔ کنترل و صفحهٔ داده، مدیریت کارآمد سامانهٔ شبکه را ارتقا می‌دهد و به‌روزرسانی‌ها و تغییرات را ساده‌تر کرده و احتمال خطاهای انسانی را کاهش می‌دهد SDN .همچنین قابلیت بی‌نیازی از فروشنده را ارائه می‌دهد و به مدیران IT اجازه می‌دهد از دستگاه‌های مختلف شبکه استفاده کنند و بدون محدودیت زیرساخت را ارتقا دهند. کنترل‌کنندهٔ SDN دیدی جامع از کل شبکه فراهم می‌کند و دیدپذیری و کنترل را افزایش می‌دهد. در حالی‌که SDN با ایجاد امکان برنامه‌پذیری، فناوری شبکه‌سازی را متحول کرده است، آسیب‌پذیری‌های جدیدی نیز معرفی شده‌اند. در شکل ۱ سطح حمله نشان داده شده است و نقطهٔ ورود انواع حملات را نمایش می‌دهد. یکی از چالش‌برانگیزترین حملات در شبکه‌هایSDN ، حملهٔ توزیع‌شدهٔ منع سرویس (DDoS) است DDoS . حافظهٔ کنترل‌کننده و سوئیچ‌ها را هدف قرار می‌دهد و باعث غیرفعال شدن پهنای‌باند شبکه و منابع سرور شده و عملیات عادی کاربران را مختل می‌کند. حملات DDoS بسیار مخرب و هماهنگ هستند و از چندین ماشین به‌خطر افتاده برای انجام هم‌زمان حملات منع سرویس علیه یک هدف استفاده می‌کنند. این امر موجب تخلیهٔ منابع و فروپاشی سامانه شده و خدمات هدف را برای کاربران قانونی غیرقابل دسترس می‌سازد.

مهاجمان از حملات DDoS برای اهداف مختلفی استفاده می‌کنند، از جمله منافع سیاسی یا مالی، ایجاد اختلالات کوچک یا حتی اختلالات گسترده. چنین حملاتی می‌توانند منجر به از دست دادن سودهای تجاری و اعتماد کاربران به خدمات آسیب‌دیده شوند. یک حملهٔ DDoS یورشی هماهنگ علیه دسترس‌پذیری خدمات ارائه‌شده توسط یک سامانه یا شبکهٔ هدف است که از طریق شبکه‌ای از سامانه‌های محاسباتی به‌خطر افتاده اجرا می‌شود. هدف حمله «قربانی اصلی» نامیده می‌شود، در حالی‌که سامانه‌های به‌خطر افتاده‌ای که برای اجرای حمله به کار می‌روند «قربانیان ثانویه» نام دارند [1]. با استفاده از قربانیان ثانویه، مهاجمان می‌توانند حملاتی بسیار بزرگ‌تر و مختل‌کننده‌تر انجام دهند و در عین حال ناشناس باقی بمانند، زیرا حمله توسط سامانه‌های به‌خطر افتاده اجرا می‌شود. این امر ردیابی حمله را برای تحلیلگران شبکه بسیار دشوارتر می‌سازد.

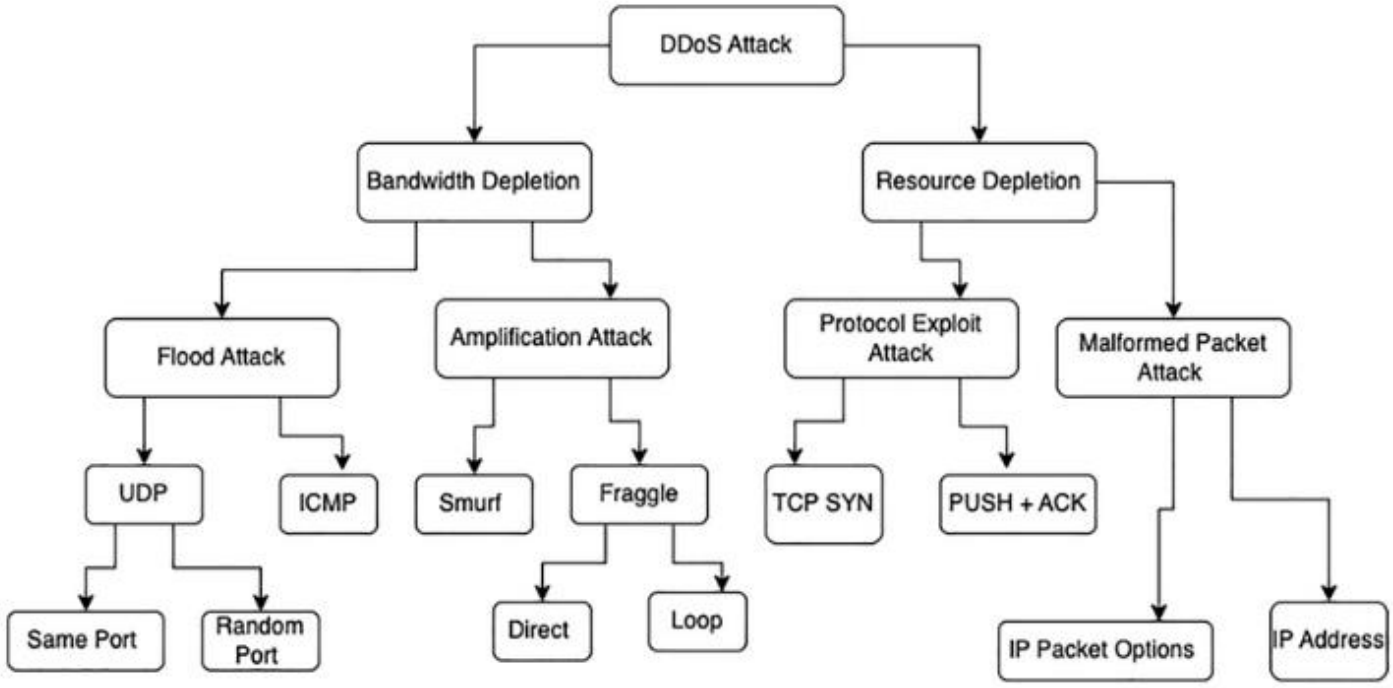
حملات DDoS به‌دلیل معماری منحصربه‌فرد شبکه‌های SDN که صفحهٔ کنترل را از صفحهٔ داده جدا می‌کند، تأثیر عمیقی بر آن‌ها دارند [1]. در SDN، کنترل‌کنندهٔ متمرکز مؤلفه‌ای حیاتی است که مسئول مدیریت کل شبکه است. این متمرکز بودن، کنترل‌کننده را به هدفی اصلی برای حملات DDoSتبدیل می‌کند. اگر مهاجم بتواند کنترل‌کننده را با حجم بالایی از درخواست‌ها غرق کند، می‌تواند منابع محاسباتی آن را تخلیه کرده و منجر به اختلالات جدی شبکه، حذف بسته‌ها و تأخیر در ترافیک قانونی شود. علاوه بر این، حملات DDoS می‌توانند از سازوکار تنظیم جریان در SDNسوءاستفاده کرده و با ایجاد تعداد زیادی درخواست جریان یکتا، موجب پر شدن جدول جریان در سوئیچ‌ها شوند. این سوئیچ‌ها که ظرفیت محدودی دارند، ممکن است شروع به حذف بسته‌ها یا کاهش کارایی کنند. آسیب‌پذیری دیگری نیز درAPI های شمالی و جنوبی وجود دارد که اگر به‌درستی ایمن‌سازی نشوند، می‌توانند برای ایجاد اختلال در ارتباط میان کنترل‌کننده و دستگاه‌های شبکه هدف قرار گیرند.



شکل ۱ معماری[1] SDN

شکل ۲ (در منبع [2]) رده‌بندی حملات DDoS را نشان می‌دهد که می‌توان آن‌ها را به‌طور کلی به دو دستهٔ اصلی تقسیم کرد: حملات تخلیهٔ پهنای‌باند و حملات تخلیهٔ منابع. حملات تخلیهٔ پهنای‌باند با هدف سیل‌آسا کردن شبکهٔ قربانی با ترافیک ناخواسته انجام می‌شوند و اجازه نمی‌دهند ترافیک قانونی به مقصد برسد. از سوی دیگر، حملات تخلیهٔ منابع برای مصرف کامل منابع سامانهٔ قربانی طراحی می‌شوند و باعث می‌گردند که سامانه نتواند درخواست‌های قانونی خدمات را پردازش کند. حملات تخلیهٔ پهنای‌باند را می‌توان به حملات سیل‌آسا (Flood) و حملات تقویتی (Amplification)دسته‌بندی کرد. در حملات سیل‌آسا، حجم زیادی از ترافیک توسط دستگاه‌های به‌خطر افتاده (زامبی‌ها) به سامانهٔ قربانی

ارسال می‌شود و موجب ازدحام پهنای‌باند شبکه می‌گردد. این ازدحام می‌تواند باعث کندی، ازکارافتادگی یا اشباع پهنای‌باند قربانی شده و دسترسی کاربران قانونی را مختل کند. حملات سیل‌آسا می‌توانند با استفاده از بسته‌های UDP (پروتکل دیتاگرام کاربر) و ICMP (پروتکل پیام کنترلی اینترنت) انجام شوند. در حملهٔUDP Flood ، تعداد زیادی بستهٔ UDP به پورت‌های تصادفی یا مشخص‌شده در سامانهٔ قربانی ارسال می‌شود. سامانهٔ قربانی تلاش می‌کند داده‌های ورودی را پردازش کرده و مشخص کند کدام برنامه‌ها آن را درخواست کرده‌اند. اگر هیچ برنامه‌ای روی پورت هدف اجرا نشود، سامانهٔ قربانی یک بستهٔ ICMP با پیام «پورت مقصد در دسترس نیست» به فرستنده بازمی‌گرداند. در حملهٔICMP Flood ، دستگاه‌های به‌خطر افتاده حجم زیادی بستهٔ ICMP_ECHO_REPLY («پینگ») به سامانهٔ قربانی ارسال می‌کنند. این بسته‌ها قربانی را مجبور به پاسخ‌دادن می‌کنند و ترافیک ترکیبی موجب ازدحام و اشباع پهنای‌باند قربانی می‌شود. حملات تقویتی (Amplification) شامل ارسال پیام توسط مهاجم یا دستگاه‌های به‌خطر افتاده به یک آدرس IP پخشی (Broadcast) است که موجب می‌شود همهٔ سامانه‌های درون زیرشبکه به سامانهٔ قربانی پاسخ دهند. بیشتر روترها از قابلیت پخش IP پشتیبانی می‌کنند؛ وقتی یک آدرس پخشی به عنوان مقصد تعیین شود، روتر بسته را تکثیر کرده و به تمام IPهای موجود در دامنهٔ پخش ارسال می‌کند. این سازوکار ترافیک حمله را تقویت و بازتاب می‌دهد و موجب اشباع پهنای‌باند قربانی می‌شود. حملهٔ Smurf نوعی حملهٔ تقویتی است که در آن مهاجم بسته‌هایی را به یک تقویت‌کنندهٔ شبکه (سامانه‌ای که پخش آدرس را پشتیبانی می‌کند) ارسال می‌کند، در حالی‌که آدرس بازگشتی جعل شده و روی IP قربانی تنظیم شده است. به‌طور مشابه، در حملهٔDDoS Fraggle ، مهاجم بسته‌های UDP ECHO را به یک تقویت‌کنندهٔ شبکه ارسال می‌کند. یک گونهٔ دیگر از حملهٔ Fraggle شامل ارسال بسته‌های UDP ECHO به پورتی است که تولید کاراکتر را پشتیبانی می‌کندchargen ، پورت ۱۹ در سیستم‌های یونیکس در حالی‌که آدرس بازگشتی جعل شده و روی سرویس Echoقربانی (پورت ۷) تنظیم شده است، که یک حلقهٔ بی‌نهایت ایجاد می‌کند. بستهٔ UDP Fraggle مولد کاراکتر سامانه‌های موجود در آدرس پخشی را هدف قرار می‌دهد. این سامانه‌ها کاراکتری تولید کرده و برای سرویس Echo قربانی می‌فرستند، و سرویس Echo نیز بستهٔ Echo را به مولد کاراکتر برمی‌گرداند و این چرخه بی‌پایان ادامه می‌یابد. حملات تخلیهٔ منابع در DDoS شامل ارسال بسته‌هایی است که از ارتباطات پروتکل‌های شبکه سوءاستفاده می‌کنند یا به‌صورت نادرست ساخته شده‌اند و منابع شبکه را اشغال کرده و هیچ منبعی برای کاربران قانونی باقی نمی‌گذارند.



شکل ۲ رده‌بندی حملات[2] DDoS

حملات بهره‌برداری از پروتکل‌ها: دو نمونه شامل سوءاستفاده از پروتکل (Transfer Control Protocol Synchronize) TCP SYN و پروتکل PUSH + ACKهستند. در یک حملهٔDDoS TCP SYN ، مهاجم به دستگاه‌های به‌خطر افتاده دستور می‌دهد درخواست‌های جعلی TCP SYN را به سرور قربانی ارسال کنند و منابع پردازشی سرور را مشغول کرده و مانع پاسخ‌گویی آن به درخواست‌های قانونی شوند. در یک حملهٔ PUSH + ACK، عاملان حمله بسته‌های TCP را با بیت‌های PUSH و ACK که روی ۱ تنظیم شده‌اند ارسال می‌کنند. این تریگرها در سربرگ بستهٔ TCP به سامانهٔ قربانی دستور می‌دهند تمام داده‌های موجود در بافر TCP را (صرف‌نظر از اینکه بافر پر باشد یا نه) تخلیه کرده و پس از تکمیل، یک تأییدیه ارسال کند.

حملهٔ بستهٔ معیوب زمانی رخ می‌دهد که مهاجم به دستگاه‌های به‌خطر افتاده دستور می‌دهد بسته‌های IP نادرست‌ساخت را به سامانهٔ قربانی ارسال کنند تا آن را از کار بیندازند. حداقل دو نوع حملهٔ بستهٔ معیوب وجود دارد. در حملهٔ آدرسIP ، بسته شامل آدرس‌های IP مشابه برای مبدأ و مقصد است که می‌تواند سیستم‌عامل قربانی را سردرگم کرده و موجب ازکارافتادگی آن شود. در حملهٔ گزینه‌های بستهٔIP ، بستهٔ معیوب ممکن است فیلدهای اختیاری درون بستهٔ IP را تصادفی‌سازی کرده و همهٔ بیت‌های کیفیت خدمات را روی ۱ تنظیم کند که سامانهٔ قربانی را مجبور می‌کند زمان پردازشی بیشتری برای تحلیل این ترافیک صرف کند. پژوهشگران چارچوب‌ها و تکنیک‌های تشخیص و مقابله برای رسیدگی به حملات DDoSتوسعه داده‌اند. پیشرفت سریع مدل‌های یادگیری ماشین نقش مهمی در افزایش دقت تشخیص و مقابله با حملات داشته است. مجموعه‌داده‌های باز، مجموعه‌هایی از داده‌های عمومی در دسترس هستند که آزادانه برای استفاده، بازتوزیع و اصلاح بدون هیچ محدودیتی قابل‌دسترسی می‌باشند. این مجموعه‌داده‌ها موضوعات گسترده‌ای را پوشش می‌دهند و اغلب توسط نهادهای دولتی، مؤسسات پژوهشی، سازمان‌های غیرانتفاعی و مشارکت‌کنندگان فردی ارائه می‌شوند. مجموعه‌داده‌های باز نقش مهمی در ترویج شفافیت، نوآوری و همکاری ایفا می‌کنند و منابع ارزشمندی برای پژوهش، تحلیل، توسعهٔ کاربرد و آموزش فراهم می‌سازند. این مجموعه‌ها به‌عنوان بلوک‌های سازندهٔ بنیادین برای مواجهه با چالش‌های اجتماعی، پیشبرد دانش علمی و ایجاد پیشرفت‌های فناورانه در حوزه‌های گوناگون به کار می‌روند. با استفاده از مجموعه‌داده‌های باز، پژوهشگران مدل‌ها را ارزیابی و تنظیم می‌کنند و از معیارهای ارزیابی عملکرد مانند دقت(precision) ، فراخوان (recall) و نرخ F-measure برای سنجش کارایی مدل‌ها بهره می‌گیرند. اهداف این پژوهش شامل مجموعه‌داده‌های باز مربوط به حملاتDDoS ، انجام یک مرور تطبیقی بر DDoS در SDN و بررسی تکنیک‌ها و چارچوب‌های تشخیص و مقابله با حملات توزیع‌شده در خدمات مختلف است. این بررسی چارچوب‌ها و روش‌های رایج، دیدگاه‌های ارزشمندی دربارهٔ مزایا و محدودیت‌های رویکردهای موجود در اختیار پژوهشگران و متخصصان قرار می‌دهد و امکان توسعهٔ راهبردهای دفاعی مقاوم‌تر و آینده‌نگر را فراهم می‌سازد. علاوه بر این، تحلیل مجموعه‌داده‌های موجود، پژوهشگران و متخصصان را نسبت به داده‌های در دسترس خود آگاه‌تر کرده و توان بالقوهٔ آن را برای بهره‌گیری در تحقیقات‌شان افزایش می‌دهد. این مطالعه به بررسی مجموعه‌داده‌های باز شامل نمونه‌های حملات DDoS می‌پردازد که در پژوهش‌های مختلف استفاده شده‌اند. برای مثال، وانگ و وانگ [3] یک تکنیک مقابلهٔ ردیابی برای SDN ارائه کردند و برای توسعه و اعتبارسنجی روش خود به مجموعه‌داده‌های InSDN [4] و CICIDS2017 [5] متکی بودند. این مرور روش‌ها و چارچوب‌های گوناگون طراحی‌شده برای تشخیص و پیشگیری از حملات، به‌ویژه حملاتDDoS ، را بررسی می‌کند. از میان چارچوب‌های برجسته بررسی‌شده در این پژوهش، Pro-Defenseاست که توسط Bawany و همکاران [6] توسعه یافته و بر کاربرد آن در شهرهای هوشمند تمرکز دارد Pro-Defense .رویکردی ماژولار اتخاذ می‌کند و اجزای گوناگون را برای افزایش کارایی آن ادغام می‌نماید. نقاط اصلی مشارکت این پژوهش، ارائهٔ مجموعهٔ به‌روز از تکنیک‌ها و چارچوب‌های مقابله با حملات DDoS در محیط‌های SDN و نیز مروری جامع بر مجموعه‌داده‌های باز مربوط به این حملات و تکنیک‌ها و چارچوب‌های تشخیص و مقابله است. افزون بر این، این پژوهش مجموعه‌داده‌های در دسترس شامل نمونه‌های حملات DDoS را برجسته می‌سازد. دوم اینکه با ارائهٔ مروری جامع بر تکنیک‌ها و چارچوب‌های موجود برای تشخیص و مقابله، این مقاله نقطهٔ شروع بسیار خوبی برای پژوهشگران فراهم می‌کند. همچنین نسخهٔ به‌روزرسانی‌شده و گسترده‌تری از مجموعه‌داده‌های موجود نسبت به آنچه در Gebremariam و همکاران [7] ذکر شده ارائه می‌دهد. در نتیجه، این کار پژوهشگران را با مجموعه‌داده‌های به‌روز مجهز می‌کند تا دقت و مرتبط‌بودن آزمایش‌هایشان افزایش یابد. جمع‌آوری و سازمان‌دهی اطلاعات ضروری در این مقاله، روند پیشرفت پژوهشگران را تسهیل می‌کند، زیرا منبعی یکپارچه و کاربرپسند ارائه می‌دهد. با گردآوری و قالب‌بندی مناسب داده‌های لازم، پژوهشگران می‌توانند به‌راحتی به اطلاعات دسترسی یافته و از آن بهره بگیرند و در نهایت تحقیقات خود را در حوزهٔ تشخیص و مقابله با حملات پیش ببرند.

باقی‌ماندهٔ این مقاله به‌صورت زیر سازمان‌دهی شده است. بخش دوم به کارهای مرتبط با DDoS در SDN می‌پردازد. بخش سوم مروری دقیق بر مجموعه‌داده‌های باز ارائه می‌دهد که منبعی در دسترس بوده و بینش‌های ارزشمندی دربارهٔ حملات DDoS در SDN فراهم می‌کنند. بخش چهارم بر تکنیک‌ها و چارچوب‌های مقابله طراحی‌شده برای خنثی‌سازی حملات DDoS در SDN تمرکز دارد. بخش پنجم به بحث و تحلیل انتقادی یافته‌ها، پیامدها و مسیرهای بالقوهٔ تحقیقات آینده می‌پردازد. در نهایت، بخش ششم مشارکت‌های پژوهش ما را خلاصه کرده و توصیه‌هایی برای کارهای آینده ارائه می‌دهد.

۲. مرور ادبیات

پژوهشگران مجموعه‌ای از تکنیک‌ها و داده‌ست‌ها را برای رسیدگی به چالش‌های مختلف امنیتی بررسی کرده‌اند. برخی بر استفاده از یک داده‌ست مشترک با تکنیک‌های متفاوت یادگیری ماشین تمرکز کرده‌اند، در حالی‌که دیگران داده‌ست‌های مختلف را از سال‌های گوناگون بررسی کرده‌اند. این بخش این رویکردها را به‌تفصیل بررسی می‌کند و موضوعاتی مانند امنیت در شبکه‌های اینترنت اشیاء مدیریت‌شده توسطSDN ، تکنیک‌های تشخیص و کاهش حملات Denial-of-Service (DoS) و Distributed Denial-of-Service (DDoS) با استفاده ازSDN ، به‌کارگیری یادگیری عمیق و یادگیری ماشین برای تشخیص و کاهشDDoS ، سیستم‌های تشخیص نفوذ (IDS) با استفاده ازXGBoost ، و بهره‌گیری از هوش مصنوعی

و یادگیری ماشین برای امنیت SDN به‌طور کلی را پوشش می‌دهد. علاوه‌براین، این بخش آسیب‌پذیری‌های امنیتی در شبکه‌های خودروبی ایمن‌شده با SDN را نیز بررسی می‌کند.

۲/۱ شبکه‌های اینترنت اشیاء مدیریت‌شده توسطSDN

ساریکا و همکاران [1] یک رویکرد خودکار و هوشمند برای تشخیص و کاهش نفوذ در SDN پیشنهاد کردند که هدف آن ارائهٔ امنیت قابل توضیح در شبکهٔ اینترنت اشیاء عصر 5 Gبود. رویکرد آن‌ها از استخراج خودکار ویژگی‌های جریان و یک دسته‌بندی‌کنندهٔ جنگل تصادفی با دقت بالا برای طبقه‌بندی جریان شبکه در لایهٔ کاربرد SDN استفاده کرد. این دسته‌بندی‌کننده قادر بود انواع مختلفی از حملات را تشخیص دهد و با نصب قواعد جریان جدید با اولویت بالا در صفحهٔ داده، اقدامات اصلاحی انجام دهد. علاوه‌براین، نویسندگان یک داده‌ست ویژهٔ SDN را معرفی کردند که یک محیط IoT واقعی را مدل‌سازی می‌کرد و شامل داده‌های جریان برای حملات رایج شبکه و ترافیک عادی بود. نتایج دقت تشخیص نفوذ و همچنین نتایج عملکرد سیستم با و بدون مکانیزم امنیتی پیشنهادی گزارش شد [1] اگرچه پژوهشگران یک مکانیزم امنیتی نویدبخش ارائه دادند، اما باید توجه داشت که سیستم تشخیص آن‌ها عمدتاً در زمینهٔ حملات DoS و DDoS ارزیابی شده بود. در نتیجه، داده‌ست استفاده‌شده ممکن است نمایندهٔ کافی برای انواع دیگر حملات مانند fuzzing و پویش پورت نباشد. همچنین، در آزمایش‌ها تنها یک میزبان مخرب برای تولید حملات استفاده شد که با سناریوهای واقعی، که در آن تهدیدها از منابع متعدد منشأ می‌گیرند، تفاوت دارد. با وجود این محدودیت‌های جزئی، مقاله به‌خوبی نوشته شده و داده‌ها را به‌صورت واضح و قابل‌فهم ارائه می‌کند.

ساریکا و همکاران [8] یک داده‌ست بدون عنوان برای تشخیص نفوذ در شبکه‌های IoT مدیریت‌شده توسط SDN تولید کردند. این داده‌ست‌ها شامل شبکه‌های IoT ایستا و پویا هستند و به‌ترتیب شامل 27.9 میلیون و 30.2 میلیون رکورد داده‌اند. داده‌ست‌ها شامل انواع مختلفی از حملات سایبری هستند، از جملهDoS ، DDoS، پویش پورت، OS fingerprintingوfuzzing ، و همچنین ترافیک سالم. کنترلر Open Network Operating System (ONOS)به‌عنوان کنترلر در این مطالعه استفاده شد، در حالی که ابزار hping3 برای ساخت بسته‌های TCP/IP جهت حملات DoS وDDoS ، ابزار Nmap برای پویش پورت وOS fingerprinting ، و Boofuzz برای fuzzing استفاده شدند. هر داده‌ست شامل 33 ویژگی است. تفاوت اصلی میان ویژگی‌ها تعداد دستگاه‌های IoT در شبکه است؛ به‌طوری‌که یکی از داده‌ست‌ها دارای پنج دستگاه IoT و دیگری دارای ۱۰ دستگاه IoT است. ترافیک سالم نیز از طریق تحلیل داده‌ست IoT bot به‌صورت خودتولیدی ایجاد شد، اما یک چالش قابل‌توجه، نبود نرم‌افزار متن‌باز برای این منظور بود.

کورونیوتیس و همکاران یک داده‌ست جدید با نام Bot-IoT معرفی کردند که شامل ترافیک معمول IoT و انواع مختلف ترافیک حمله رایج در بات‌نت‌ها بود [9]. داده‌ها با ویژگی‌هایی مربوط به جریان حمله، دسته‌بندی و زیردسته‌بندی برچسب‌گذاری شدند. معیارهای آماری مانند ضریب همبستگی و آنتروپی برای تعیین ۱۰ ویژگی برتر استفاده شد. برای ارزیابی کیفیت داده‌ست، پژوهشگران مدل‌هایSVM ، شبکه عصبی بازگشتی (RNN)، و شبکه عصبی بازگشتی حافظه کوتاه‌مدت (LSTM-RNN) را آموزش دادند. چهار معیار—دقت، دقت پیش‌بینی، بازخوانی و نرخ خطای مثبت کاذب—برای سنجش کیفیت داده‌ست استفاده شد. نتایج نشان داد داده‌ست کامل هنگام آموزش با SVM بالاترین دقت و بازخوانی را به‌دست آورد، در حالی‌که داده‌ست ۱۰ ویژگی برتر بالاترین دقت پیش‌بینی و کمترین خطای مثبت کاذب را هنگام آموزش با SVM ارائه داد. با وجود اینکه این مطالعه بنیان ارزشمندی برای درک ترافیک حمله به دستگاه‌های IoT ایجاد کرد، محدودیت‌هایی نیز داشت. یک محدودیت کلیدی استفاده از تنها ٪۵ داده‌ست تولیدشده برای آزمایش بود، که عمدتاً به‌دلیل چالش مدیریت ۷۲ میلیون رکورد بود. پژوهشگران به‌جای آن ۳ میلیون رکورد را برای مجموعه‌های آموزش و آزمایش انتخاب کردند که ممکن است خطاهای آماری مانند مثبت‌های کاذب ایجاد کند. علاوه‌براین، گرچه روش‌های جمع‌آوری و پردازش داده برای یادگیری ماشین شرح داده شده بود، تکرار آن دشوار بود، تا حدی به‌دلیل منحنی یادگیری ابزارهایی مانند argus. همچنین برخی ابزارها که در ابتدا متن‌باز بودند، به مدل تجاری تغییر وضعیت داده بودند، مانندostinato ، که می‌تواند مانعی برای تکرارپذیری ایجاد کند. پژوهشگران یک چارچوب تشخیص حملات DDoS مبتنی بر شمارنده با نام C-DADبرای شناسایی حملات DDoS ایجاد کردند [10]. این چارچوب با کنترلر SDNWISEادغام شده و از شبیه‌ساز Coojaبرای ایجاد یک محیط شبکه اینترنت اشیای نرم‌افزارمحور (SD-IoT) استفاده می‌کند SDNWISE. یک راهکار دو بخشی برای شبکه‌های حسگر بی‌سیم است که هم یک چارچوب نرم‌افزاری مبتنی بر مفهوم شبکه‌های حسگر بی‌سیم نرم‌افزارمحور (SD-WSN) و هم یک نمونه سخت‌افزاری واقعی برای تست و پیاده‌سازی نرم‌افزار ارائه می‌دهد. با تحلیل ترافیکIoT ، چارچوب C-DAD می‌تواند حملات DDoS را با دقت بالا شناسایی کند. پژوهشگران سه آزمایش مختلف برای نشان دادن اثربخشی این چارچوب در شناسایی حملات انجام دادند. با وجود عملکرد قابل‌قبول چارچوب، یک محدودیت مهم آن این است که کنترلر IoT تنها در یک شبکه در محیط ناهمگون آزمایش شده و عملکرد آن در چندین شبکه IoT با شرایط متنوع بررسی نشده است. یین و همکاران [11] یک الگوریتم و چارچوب برای شناسایی و کاهش حملات DDoS در محیط SD-IoT ایجاد کردند. این چارچوب شامل مجموعه‌ای از کنترلرهایSDN ، سوییچ‌های SD-IoT همراه با دروازه‌های IoT و دستگاه‌های IoT است. الگوریتم با استفاده از شباهت کسینوسی بردارهای نرخ packet-in سوییچ مرزی را با یکدیگر مقایسه می‌کند. پژوهشگران این چارچوب و الگوریتم را در یک محیط شبیه‌سازی SDN مبتنی بر Mininetآزمایش کردند که در آن Floodlightنقش کنترلر را بر عهده داشت [11]

پژوهشگران در توسعه یک سیستم دفاعی پیش‌دستانه که بتواند حملات DDoS را در زمان واقعی شناسایی و خنثی کند، با چالش‌هایی روبه‌رو بودند. علاوه‌براین، آن‌ها توازن بار پویا را در مجموعه کنترلرها پیاده‌سازی نکردند. توازن بار، مکانیزمی است که برای توزیع یکنواخت ترافیک شبکه یا بار کاری میان چندین کنترلر یا منبع طراحی می‌شود، و باعث بهبود استفاده از منابع و افزایش کارایی شبکه می‌گردد. در نهایت، شبیه‌سازی‌ها نشان دادند الگوریتم پیشنهادی می‌تواند منبع حمله DDoS را که از یک دستگاه IoT آغاز شده است، با دقت بالا شناسایی کند. این شناسایی سریع باعث تسریع فرآیند کاهش حمله شده و امنیت شبکه‌های IoT را که اغلب دارای قدرت پردازشی و حافظه محدود هستند، افزایش می‌دهد.

در جدول ۱، مروری بر اطلاعات داده‌ست، مزایا و معایب پژوهش‌های مربوط به شبکه‌های اینترنت اشیاء مدیریت‌شده توسط SDN ارائه شده است.

۲/۲ تشخیص و مقابله با حملات DoS و DDoS با استفاده ازSDN

گالئانو-براخونس و همکاران [13] یک رویکرد Statefulمبتنی بر SDN برای شناسایی و کاهش حملات DoS و DDoS در شبکه‌های IoT توسعه دادند. آن‌ها از قابلیت OpenStateبرای ایجاد ویژگی‌های Stateful روی یک سوییچ مجازی Open vSwitch استفاده کردند. آزمایش‌ها در سه سناریو انجام شد:

- سناریوی اول :تحلیل مصرف پهنای باند در هنگام حمله DoS و فرایند مقابله، همراه با بررسی مقادیر آنتروپی. این سناریو به‌عنوان خط پایه عمل می‌کرد و از یک تست‌بد SDN شامل کنترلر Ryuو Mininetاستفاده شد.
- سناریوهای دوم و سوم :استفاده از داده‌های Bot-IoT [12]برای ارزیابی فرایند تشخیص و مقابله با حملات DoS و DDoS در محیط IoT.

با وجود نتایج ارائه‌شده، مطالعه چند محدودیت داشت:

1. تنها حملات DDoS مبتنی بر UDP بررسی شدند، که دید محدودی از عملکرد روش در برابر سایر بردارهای حمله ارائه می‌کند.
2. در اندازه‌های پنجره بزرگ، برخی سوییچ‌ها نسبت به کنترلر بی‌پاسخ می‌شدند که می‌تواند قابلیت اجرایی سیستم را کاهش دهد.
3. فرایند تشخیص می‌توانست با افزودن روش‌های آماری بیشتر یا مدل‌های یادگیری ماشین بهبود یابد.

یک رویکرد تشخیص دومرحله‌ای در [14] ارائه شد تا امکان شناسایی زودهنگام حملات DDoS فراهم شود. این رویکرد شامل دو الگوریتم است که برای هر کاربر یک مقدار اعتماد (Trust Value) تعیین می‌کنند.

الگوریتم دو مرحله دارد:

- مرحله اول :استخراج فیلدهای هدر بسته‌های ورودی
- مرحله دوم :محاسبه مقدار اعتماد بر اساس اطلاعات استخراج‌شده

این مقدار اعتماد نقش اصلی در شناسایی مهاجمان احتمالی دارد. آزمایش با ابزارهایMininet ، Wireshark، Scapyو کنترلر POX انجام شد. با اینکه روش ارائه‌شده قوی است، یک چالش مهم باقی می‌ماند:

- تعیین آستانه مناسب برای تشخیص. آستانه کم ← هشدار کاذب زیاد؛ آستانه زیاد ← تشخیص پایین.
- حساسیت سیستم نیز وابسته به سطح اعتماد تعیین‌شده است که ممکن است فرایند تشخیص را پیچیده کند.

آسیس و همکاران [15] یک سیستم دفاعی برای شبکه‌های SDN پیشنهاد کردند که قادر است حملات DDoS روی کنترلر و سرورهای خارجی را با بازرسی ترافیک در بازه‌های یک‌ثانیه‌ای شناسایی و کاهش دهد. مدل تشخیص آن‌ها از شبکه عصبی کانولوشنی (CNN) استفاده می‌کند و با سه روش دیگر مقایسه شد: رگرسیون لجستیک(LR) ، MLPو.Dense-MLP

روش‌ها در دو سناریو ارزیابی شدند:

- سناریوی اول: داده شبیه‌سازی‌شده SDN با Mininet وFloodlight
- سناریوی دوم: استفاده از داده‌ست عمومی [16] CICDDoS2019 که شامل بیش از ۱۲ نوع حمله DDoS است

نتایج نشان داد روش:CNN

- بالاترین دقت، بیشترین Precision وF-measure
- کمترین نرخ مثبت کاذب
- را به دست آورده است.

جدول ۱: خلاصه‌ای از اطلاعات مجموعه‌داده‌ها، مزایا و معایب شبکه‌های اینترنت اشیاء مدیریت‌شده توسطSDN

ساریکا و همکاران [1]، مجموعه‌دادهٔ[8] SDN

مزیت :طبقه‌بند قادر بود انواع مختلفی از حملات را شناسایی کند و با نصب قوانین جریان جدید با اولویت بالا در صفحهٔ داده، اقدامات اصلاحی انجام دهد.

عیب :مجموعه‌دادهٔ استفاده‌شده ممکن است انواع دیگر حملات را به‌طور کافی پوشش ندهد. آزمایش‌ها تنها شامل یک میزبان مخرب بودند که حمله را ایجاد می‌کرد، که با سناریوهای واقعی که در آن تهدیدها از منابع متعدد سرچشمه می‌گیرند، متفاوت است.

ساریکا و همکاران [8]، مجموعه‌دادهٔ[8] SDN

مزیت :مجموعه‌داده‌ها شامل شبکه‌های IoT ایستا و پویا هستند.

عیب :یک چالش قابل‌توجه، عدم دسترسی به نرم‌افزار متن‌باز برای این منظور بود.

کورونیوتیس و همکاران [9] [12] Bot-IoT

مزیت :پژوهش روش‌های جمع‌آوری و پردازش داده برای یادگیری ماشین را به‌تفصیل توضیح داده است.

عیب :تکرار فرایند دشوار بود.

بهیو و همکاران [10]، بدون مجموعه‌داده

مزیت :چارچوب به‌طور مؤثر عمل می‌کند.

عیب :عملکرد آن در چندین شبکهٔ IoT در محیط‌های ناهمگون نشان داده نشده است.

یین و همکاران [11]، بدون مجموعه‌داده

مزیت :این شناسایی سریع، امکان کاهش حمله را سریع‌تر فراهم کرده و امنیت شبکه‌های آسیب‌پذیر IoT را بهبود می‌دهد.
عیب :این شبکه‌ها اغلب به دلیل توان پردازشی و حافظهٔ محدود دستگاه‌های پایانی با محدودیت مواجه‌اند.

روش‌های MLP و D-MLP در شاخص Recall عملکرد بهتری داشتند. پژوهشگران همچنین یک ماژول کاهش حمله معرفی کرده و یک رویکرد نظریهٔ بازی را به‌عنوان نمونهٔ نحوهٔ عملکرد آن ارائه کردند. روش مبتنی بر نظریهٔ بازی، نرخ دورریزی بسته‌ها را در سیاست به‌کاررفته در کنترلر مرکزی SDN افزایش می‌دهد و مشخص شد که در بازیابی عملکرد عادی SDN موفق بوده است. با وجود موفقیت ماژول تشخیص، این تحقیق محدودیت‌هایی نیز دارد. یکی از محدودیت‌های اصلی استفاده از تعداد کمی میزبان در مرحلهٔ آزمایش بود؛ افزایش تعداد میزبان‌ها می‌تواند تشخیص

حملات DDoS را دشوارتر و پنهان‌تر کند. محدودیت دیگر، استفادهٔ نسبتاً محدود از تکنیک‌های یادگیری ماشین در ماژول تشخیص است که می‌توانست برای افزایش کارایی، گسترده‌تر شود.

کیانی و همکاران [17] الگوریتمی برای شناسایی ناهنجاری‌ها در SDN ارائه کردند. یکی از الگوریتم‌ها بر تشخیص ناهماهنگی‌های متمرکز در جدول جریان تمرکز داشت و دیگری برای شناسایی ناهماهنگی‌های توزیع‌شده در میان چندین سوییچ شبکه طراحی شده بود. عملکرد این الگوریتم‌ها با استفاده از Mininet و کنترلر Ryu ارزیابی شد و مشخص شد که در شناسایی ناهنجاری‌ها مؤثر هستند. تنها محدودیت مشاهده‌شده این بود که فرایند تشخیص در مسیرهای طولانی‌تر زمان بیشتری نیاز داشت. یکی از نکاتی که پژوهشگران به آن اشاره کردند این است که افزایش تعداد قوانین در جدول جریان باعث ارسال مسیرهای طولانی‌تر به الگوریتم می‌شود، که در نتیجه زمان تشخیص ناهنجاری را افزایش می‌دهد. با این حال، الگوریتم توانست همهٔ ناهنجاری‌ها را در محیط آزمایش شامل ۳۰ سوییچ و ۱۰۰ میزبان با موفقیت شناسایی کند.

روشی برای کاهش حملات traceback در شبکه‌های SDN توسط وانگ و همکاران [3] توسعه یافت Traceback .به فرایند شناسایی منبع ترافیک یا فعالیت‌های مخرب در شبکه اشاره دارد و شامل ردیابی مسیر بسته‌ها از مقصد به مبدأ است. نویسندگان از ۱۰ ویژگی برای ردیابی منبع حملهٔ DDoS اجراشده با hping3 استفاده کردند. علاوه بر این، یک مدل یادگیری عمیق ترکیبی به نام CNN-ELM که شبکهٔ عصبی کانولوشنی (CNN)و ماشین یادگیری اکستریم (ELM) را ترکیب می‌کند، برای تشخیص دقیق ناهنجاری پیشنهاد شد. این مدل با استفاده از مجموعه‌داده‌های CICIDS-2017 [5]و InSDN [4] آزمایش شد. مجموعه‌دادهٔ CICIDS-2017 دقت 98.92٪ و مجموعه‌دادهٔ InSDN دقت 99.91٪ را نشان داد. یکی از معایب قابل‌توجه این روش، وابستگی آن به یادگیری نظارت‌شده است که به دادهٔ برچسب‌خورده فراوان نیاز دارد. پژوهشگران قصد دارند در آینده این چالش را با به‌کارگیری شبکه‌های عصبی گرافی برطرف کنند.

یک سازوکار امنیتی توسط نویسندگان SDIoT-DDoS-DA برای شناسایی و کاهش حملات DDoS در شبکه‌های SDN پیشنهاد شد [18]. این سیستم با استفاده از چارچوب SDN-Wise و کنترلر ONOS پیاده‌سازی شد. برای ایجاد ترافیک DDoS از ابزار Trinoo استفاده شد و عملکرد سیستم روی مجموعه‌داده‌ای شامل 1054 درخواست آزمایش شد Trinoo .ابزاری مشهور است که در بسیاری از حملات گذشته علیه وب‌سایت‌های بزرگ استفاده شده و ترافیک DDoS را با ارسال سیل‌آسای بسته‌های UDP تولید می‌کند، در حالی که ارتباط بین مهاجم و برنامهٔ کنترل مرکزی با TCP برقرار می‌شود. یکی از محدودیت‌های مهم این مطالعه، کوچک بودن اندازهٔ آزمایش (تنها 1054 درخواست) بود که می‌تواند بر دقت نتایج تأثیر بگذارد. نتایج شبیه‌سازی نشان داد سیستم تشخیص، 876 درخواست را به‌عنوان «دسترسی غیرقانونی» طبقه‌بندی کرده است. در این مجموعه‌داده، 11 درخواست به‌اشتباه به‌عنوان مثبت کاذب شناسایی شدند. ماژول تشخیص همچنین 178 درخواست را درست به‌عنوان «دسترسی مشروع» طبقه‌بندی کرد، اما 32 منفی کاذب نیز تولید نمود که نشان‌دهندهٔ نیاز به بهبود بیشتر بخش تشخیص است.

بوانی و همکاران [6] یک چارچوب ماژولار به نام ProDefenceبرای تشخیص و مقابله با حملات DDoS در یک شبکه گسترده، از جمله یک شهر هوشمند مبتنی بر زیرساختSDN ، توسعه دادند. این چارچوب شامل چندین مؤلفه است، مانند جمع‌آورنده جریان ترافیک، موتور سیاست‌گذاری، تشخیص‌دهنده حمله و موتور مقابله ProDefence .این مزیت را دارد که معیارهای سفارشی برای تشخیص حملات DDoS ارائه می‌دهد و در عین حال از توازن بار پشتیبانی می‌کند و با استفاده از یک پلتفرم کنترلر توزیع‌شده، خطر خرابی کنترلر را کاهش می‌دهد . ProDefenceدر محیط‌هایی با کنترلرهای ناسازگار با چالش‌هایی روبه‌رو است. اتکای سیستم به Node.js برای یکپارچگی ممکن است هنگام استقرار سریع قوانین شبکه مشکل ایجاد کند. علاوه بر این، اگرچه ProDefence ادعا می‌کند با هر زبان برنامه‌نویسی سازگار است، این انعطاف‌پذیری نیازمند بررسی بیشتری است تا از عملکرد سازگار آن در محیط‌های اسکریپت‌نویسی مختلف اطمینان حاصل شود.

پژوهشگران OpCloudSecرا طراحی کردند، یک سیستم حمله و واکنش که مبتنی بر تشخیص ناهنجاری است [19]. این سیستم از یک شبکه باور عمیق (DBN) برای ساخت مدل پیشگیری از حمله استفاده می‌کند. برای آزمایش، از دیتاست UNB ISCX [20]استفاده شد. مدل حمله، دقت بیشتری نسبت به طبقه‌بندهایSVM ، نقشه خودسازمان‌ده (SOM) و NB نشان داد. این مطالعه توانایی سیستم را در ارتقای امنیت، در عین ایجاد حداقل اختلال در شبکه، توصیف می‌کند. با این حال، از آنجا که دیتاست UNB ISCX در یک محیط SDN تولید نشده است، ممکن است همان سطح دقتی را که یک دیتاست اختصاصی SDN برای اعتبارسنجی سیستم فراهم می‌کند، ارائه ندهد. آزمایش‌های بیشتر با یک دیتاست ویژه SDN لازم است.

سینگ و همکاران [21]حدود ۷۰ مقاله برجسته را بررسی کردند. آنها دریافتند که حدود ۴۷٪ از مطالعات از روش‌های مبتنی بر نظریه اطلاعات، حدود ۴۲٪ از روش‌های مبتنی بر یادگیری ماشین و تقریباً ۲۰٪ از روش‌های مبتنی بر شبکه‌های عصبی مصنوعی برای تشخیص حملات DDoS در SDN استفاده کرده‌اند. کنترلر همچنان هدف اصلی مهاجمان است، زیرا حیاتی‌ترین مؤلفه شبکه فعال‌شده توسط SDN محسوب می‌شود. چندین چالش پژوهشی همچنان وجود دارد، از جمله پذیرش معماریSDN ، عدم وجود کنترلرهای سطح تولید، مشکلات مقیاس‌پذیری، نگرانی‌های

امنیتی درباره سوییچ‌های SDN و لینک‌های ارتباطی، و وابستگی به یک کنترلر مرکزی. این چالش‌ها پیاده‌سازی یک SDN ایمن را دشوار کرده و آن را به یک مسئله باز تبدیل می‌کنند.

سینگ و همکاران [22] طبقه‌بندی‌ای از آسیب‌پذیری‌های امنیتی موجود در معماری SDN ارائه می‌دهند که می‌تواند توسط حملات DDoS مبتنی بر جریان‌های جدید مورد سوءاستفاده قرار گیرد. آن‌ها تحلیلی از جدیدترین پیشرفت‌ها در پژوهش‌های شناسایی و مقابله با DDoS ارائه کرده‌اند که با هدف رفع این آسیب‌پذیری‌های امنیتی انجام شده است. همچنین، آن‌ها چالش‌های پژوهشی مرتبط با امنیت SDN را بررسی می‌کنند که می‌تواند برای جامعه پژوهشی و دانشگاهیان در تحقیقات آینده ارزشمند باشد. این مرور، طبقه‌بندی‌ای از مسائل امنیتی موجود در معماری SDN مرتبط با حملات DDoS مبتنی بر جریان‌های جدید ارائه می‌دهد. با تمرکز بر مشکلات امنیتی ذاتی، آن‌ها یک رده‌بندی از آسیب‌پذیری‌های اصلی طراحی در معماری SDN ایجاد کردند که به مهاجمان اجازه می‌دهد حملات مبتنی بر جریان‌های جدید را آغاز کنند. این طبقه‌بندی یک دیدگاه سلسله‌مراتبی روشن از آسیب‌پذیری‌های بالقوه‌ای که می‌توان در معماری SDN از آن‌ها بهره‌برداری کرد، ارائه می‌دهد. این چارچوب به جامعه تحقیقاتی کمک می‌کند تا با درک ابعاد، وابستگی‌ها و تأثیرات مشکلات حملاتDDoS ، راهکارهای مؤثر دفاعی را شناسایی کنند. علاوه بر این، آن‌ها یک مرور جامع از راهکارهای دفاعی DDoS ارائه می‌دهند که شامل جدیدترین پیشرفت‌ها و تکنیک‌های مورد استفاده در محیط SDN است. پژوهشگران دلایلی برای روش‌های شناسایی DDoS مطرح می‌کنند تا بینشی درباره استراتژی‌های نوینی که طی سال‌های اخیر توسعه یافته‌اند، ارائه دهند و نشان دهند که چگونه الگوهای حملات DDoS تکامل یافته‌اند. در نهایت، آن‌ها چند پرسش چالش‌برانگیز پژوهشی مرتبط با امنیت SDN را که همچنان بدون پاسخ باقی مانده‌اند، بررسی می‌کنند.

جدول 2 نمای کلی‌ای از اطلاعات دیتاست‌ها، مزایا و معایب مرتبط با *شناسایی و مقابله DoS و DDoS با استفاده از SDN* ارائه می‌دهد.

2.3 روش‌های یادگیری عمیق و یادگیری ماشین برای شناسایی و مقابله باDDoS

در یک چارچوب پیشنهادی در [23]، از شبکه LSTM برای شناسایی حملات DDoS در سمت منبع شبکه استفاده شده است. این چارچوب با هدف رسیدگی به کاهش عملکرد ناشی از الگوهای غیرقابل پیش‌بینی ترافیک شبکه طراحی شده و با اعمال آستانه‌های تطبیقی مبتنی بر LSTM برای هر شبکه در سمت منبع عمل می‌کند. علاوه بر این، چارچوب یک شبکه همکاری شامل چندین نقطه تشخیص ایجاد می‌کند تا بازخوردهایی مانند الگوهای ترافیک محلی، نرخ‌های شناسایی و زمان‌سنج‌ها را از هر نقطه جمع‌آوری کند. برای ارزیابی عملکرد این چارچوب، از ترافیک واقعی درخواست‌های DNS جمع‌آوری‌شده از DNS-STAT: Hedgehog متعلق به ICANN استفاده شد [23]

یک محدودیت این مطالعه، امکان بهبود روش تشخیص سمت منبع از طریق استفاده از dynamic seasonality embeddingاست؛ رویکردی که با تحلیل و سازگاری با الگوها و روندهای در حال تغییر داده‌ها می‌تواند دقت تشخیص را افزایش دهد. علاوه بر این، فرآیند تشخیص می‌تواند با انتخاب هوشمندانه‌تر دستگاه‌هایی که در سیستم همکاری می‌کنند، بهبود یابد. راوی و همکاران [24] رویکرد LEDEMرا برای شناسایی حملات DDoSبا استفاده از یک الگوریتم نیمه‌نظارتی یادگیری ماشین پیشنهاد کردند. این رویکرد با استفاده از دیتاست [20] UNB-ISCX و یکtestbed ، همچنین توپولوژی شبیه‌سازی‌شده در Mininet ارزیابی شد و با راهکارهای موجود مقایسه شد. نتایج نشان داد که LEDEM نرخ دقت تشخیص حملات DDoS را تا 96.28٪ افزایش داده است. یک محدودیت قابل توجه در این پژوهش، اتکا به یک تکنیک واحد یادگیری ماشین یعنی ELM نیمه‌نظارتی است. این انتخاب به دلیل احتمال بروز false positive در هر دو روش نظارتی و بدون‌نظارت چالش‌برانگیز بود. پیدا کردن یک رویکرد جایگزین که هم مدل فعلی را حفظ کند و هم بهبودهای واضحی ارائه دهد، مسئله‌ای دشوار است. سانتوس و همکاران [25]: در این مطالعه، الگوریتم‌های یادگیری ماشین شامل MLP، SVM، درخت تصمیم، و جنگل تصادفی برای شناسایی سه دسته حمله DDoS پیشنهاد شدند: حملات جدول جریان(flow-table) حملات پهنای‌باندوحملات علیه کنترلرواین حملات با استفاده از ابزار Scapy و فهرستی شامل بیش از 20,000 آدرس IP به‌عنوان مهاجم تولید شدند و میزبان‌های متصل به شبکه SDN هدف قرار گرفتند، که در شبیه‌ساز Mininet VN با کنترلر POXاجرا شده بود. نتایج آزمایشی نشان داد که الگوریتم درخت تصمیم به‌طور کلی بهترین عملکرد را به دلیل زمان پردازش کم داشت، اگرچه جنگل تصادفی بالاترین دقت مطلق را کسب کرد.

جدول ۲: خلاصه‌ی اطلاعات دیتاست‌ها، مزایا و معایب مرتبط با شناسایی و مقابله DoS و DDoS با استفاده ازSDN

Galeano-Brajonesو همکاران 13, 12 Bot-IoT

- اطلاعات مجموعه‌دادهBot-IoT :
- مزایا :از قابلیت *Open State Extension*برای ایجاد ویژگی‌های stateful بر روی یک *Open vSwitch*استفاده کردند.

- معایب :از حملات UDP DDoS در آزمایش استفاده شد که دید محدودی از کارآمدی روش در مقابله با انواع مختلف DDoS ارائه می‌دهد.

Salemو همکاران [14] – بدون مجموعه‌داده

- اطلاعات مجموعه‌داده :ندارد
- مزایا :این روش برخلاف روش‌هایی است که بر یک مقدار آستانه ثابت و همواره متغیر تکیه می‌کنند.
- معایب :ایجاد تعادل در سیستم تعیین آستانه چالش‌برانگیز است.

Assisو همکاران15 CICDDoS2019 – 16

- اطلاعات مجموعه‌دادهCICDDoS2019 :
- مزایا :روش CNN بالاترین دقت و صحت را به دست آورد.
- معایب :تعداد محدود میزبان‌ها در مرحله آزمایش ماژول.

Kianiو همکاران [17] – بدون مجموعه‌داده

- اطلاعات مجموعه‌داده :ندارد
- مزایا :الگوریتم در تشخیص همه ناهنجاری‌ها در یک محیط آزمایشی شامل ۳۰ سوئیچ و ۱۰۰ میزبان عملکرد مؤثری نشان داد.
- معایب :افزایش تعداد قوانین در جدول جریان موجب افزایش طول مسیرها می‌شود.

Wangو همکاران 3 InSDN – 4 ، [5] CICIDS2017

- اطلاعات مجموعه‌داده InSDN :وCICIDS2017
- مزایا :مجموعه‌داده CICIDS2017 دقت 98.92٪ و مجموعه‌داده InSDN دقت بالاتر 99.91٪ را نشان داد.
- معایب :وابستگی به یادگیری نظارت‌شده.

Waniو همکاران [18] – بدون مجموعه‌داده

- اطلاعات مجموعه‌داده :ندارد
- مزایا :ماژول تشخیص توانست 178 فرمان را به‌عنوان درخواست‌های دسترسی مشروع طبقه‌بندی کند.
- معایب :سیستم برخی درخواست‌های مخرب را به‌اشتباه به‌عنوان benign (بی‌ضرر) تشخیص داد.

Bawanyو همکاران [6] – بدون مجموعه‌داده

- اطلاعات مجموعه‌داده :ندارد
- مزایا ProDefence :امکان تعریف معیارهای سفارشی برای تشخیص حملات DDoS را فراهم می‌کند.
- معایب :ادعای سازگاری با هر زبان برنامه‌نویسی نیازمند بررسی بیشتر است.

Sharmaو همکاران 19 UNB ISCX – 20

- اطلاعات مجموعه‌دادهUNB ISCX :
- مزایا :مدل حمله دقت بیشتری نسبت بهSVM ، SOMو NB نشان داد.
- معایب :این مجموعه‌داده در یک محیط آزمایشی SDN تولید نشده است.

Singhو همکاران [21] – بدون مجموعه‌داده

- اطلاعات مجموعه‌داده :ندارد

- مزایا :بررسی حدود 70 مقاله برجسته پژوهشی.
- معایب :نبود کنترلرهای سطح تولید.(Production-level controller)

Singhو همکاران [22] – بدون مجموعه‌داده

- اطلاعات مجموعه‌داده :ندارد
- مزایا :طبقه‌بندی پیشنهادی دیدی سلسله‌مراتبی و شفاف از آسیب‌پذیری‌هایی ارائه می‌دهد که ممکن است در معماری SDN مورد سوءاستفاده قرار گیرند.
- معایب :الگوهای حمله DDoS به‌مرور تکامل یافته‌اند و مقابله با آنها دشوار شده است.

Nadeem، محمد وقاص و همکاران 26

این مقاله چندین روش مهم انتخاب ویژگی را برای یادگیری ماشین در زمینه تشخیص حملات DDoS ارزیابی می‌کند. انتخاب ویژگی‌های بهینه تأثیر قابل‌توجهی بر دقت طبقه‌بندی تکنیک‌های یادگیری ماشین و عملکرد کنترلر SDN دارد. پژوهشگران یک تحلیل مقایسه‌ای از روش‌های انتخاب ویژگی و طبقه‌بندهای یادگیری ماشین برای تشخیص حملات SDN ارائه می‌کنند. نتایج آزمایش‌ها نشان می‌دهد که طبقه‌بند *Random Forest (RF)*، هنگامی که روی ویژگی‌های انتخاب‌شده با روش *Recursive Feature Elimination (RFE)* آموزش داده شود، به دقت بسیار بالای 99.97٪ دست می‌یابد. مجموعه‌داده NSL-KDD [27] برای آموزش و آزمون طبقه‌بندهای یادگیری ماشین در تشخیص حملات DDoS استفاده شد. سه روش فیلتر *Information Gain (IG)*—، *Correlation Coefficient (CC)* و *Chi-Square*— برای انتخاب ویژگی‌های بهینه به‌کار رفتند. علاوه‌براین، سه روش wrapper—*Forward Feature Selection (FFS)* ، *Backward Feature Elimination (BFE)* و *RFE*— برای رتبه‌بندی ویژگی‌های بهینه استفاده شدند. الگوریتم انتخاب ویژگی *Lasso* نیز برای حذف کم‌اهمیت‌ترین ویژگی‌ها و تولید یک مجموعه ویژگی کاهش‌یافته به‌کار رفت. طبقه‌بندهایی مانند SVM ، KNN، NB، RF و DT نیز ارزیابی شدند. استخراج و انتخاب ویژگی‌های بهینه برای تشخیص دقیق حملات در مدل‌های یادگیری ماشین حیاتی است. نتایج آزمایش‌ها نشان می‌دهد که طبقه‌بند RF آموزش‌دیده با ویژگی‌های رتبه‌بندی‌شده توسط RFE عملکرد بسیار مناسبی در تشخیص حملات به کنترلر SDN دارد. با این‌حال، با افزایش مقیاس ترافیک شبکه، مصرف منابع کنترلر SDN افزایش یافته و دقت تشخیص کاهش می‌یابد. همچنین استفاده از ویژگی‌های نامربوط یا بیش‌ازحد، بار کاری کنترلر را افزایش داده و ممکن است کارایی آن را تحت تأثیر قرار دهد.

Dehkordi و همکاران 28 این مقاله یک روش جدید برای تشخیص حملات DDoS در SDN ارائه می‌کند که شامل سه بخش اصلی است: بخش گردآورنده(collector) ، بخش مبتنی بر آنتروپی، و بخش طبقه‌بندی. نتایج آزمایش با استفاده از مجموعه‌داده UNB-ISCX [20] و دیگر مجموعه‌داده‌ها نشان می‌دهد که این روش از نظر دقت عملکرد بهتری نسبت به روش‌های موجود دارد.

ارزیابی‌ها نشان داد که بخش‌های مبتنی بر آنتروپی با آستانه‌های ثابت، در مجموعه‌داده‌های مختلف نتایج رضایت‌بخشی ارائه نمی‌دهند. استفاده از آستانه‌های پویا نتایج بهتری ارائه کرد، اما نرخ مثبت کاذب (FPR) بالایی ایجاد می‌کند. برای رفع این مشکل، انواع الگوریتم‌های طبقه‌بندی به‌کار گرفته شدند که نتایج دقیق‌تری تولید کردند. اهمیت این روش در دقت بالاتر آن نسبت به روش‌های مشابه است. با این‌حال، از آنجا که مدل ارائه‌شده بر یافتن راه‌حل پس از وقوع حمله تمرکز دارد، ارزیابی روش‌های پیشگیری از حملات DDoS در شبکه‌های SDN همچنان نیازمند بررسی بیشتر است. در این مطالعه از کنترلر Floodlight و Mininet 2.2.1 برای شبیه‌سازی شبکه استفاده شد. الگوریتم‌های طبقه‌بندی *RandomTree*، *Logistic Regression*، *J48*، *BayesNet* و *REPTree* همراه با روش K-fold با مقدار K=10 برای تشخیص حملات کم‌حجم استفاده شدند Perez-Diaz .، خِسوس آرتورو و همکاران 29 در این مقاله یک معماری ماژولار و انعطاف‌پذیر برای شناسایی و مقابله با حملات DDoS کم‌نرخ (LR-DDoS) در محیط SDN ارائه شده است. سیستم تشخیص نفوذ (IDS) با استفاده از شش مدل یادگیری ماشین *J48*—، *Random Tree*، *REP Tree*، *Random Forest*، *MLP* و *SVM*— آموزش دید و عملکرد آنها با استفاده از مجموعه‌داده CIC DoS [5] ارزیابی شد. یافته‌ها نرخ تشخیص 95٪ را نشان می‌دهند، باوجود اینکه تشخیص حملات LR-DDoS ذاتاً دشوار است. آن‌ها کنترلر ONOS را بر روی یک ماشین مجازی Mininet مستقر کردند تا شرایط شبکه‌های واقعی را شبیه‌سازی کنند. ابزار SlowHTTPTest برای اجرای حملات LR-DDoS از سمت مهاجمان به سرور وب مجازی استفاده شد و نتایج به‌گونه‌ای طراحی شد که به‌راحتی به محیط واقعی قابل انتقال باشد. سیستم جلوگیری از نفوذ (IPS) توانست تمامی حملات شناسایی‌شده توسط IDS را با موفقیت کاهش دهد. معماری امنیتی ماژولار و انعطاف‌پذیر طراحی‌شده امکان جایگزینی هر ماژول بدون تأثیرگذاری بر سایر بخش‌ها را فراهم می‌کند . IDS جریان‌ها را با استفاده از مدل‌های مختلف یادگیری ماشین که می‌توانند با زبان‌ها و چارچوب‌های متفاوت توسعه یابند، شناسایی می‌کند. ارزیابی شش الگوریتم یادگیری ماشین با استفاده از مجموعه‌داده CIC DoS (2017) دقت 95٪ را نشان داد. با استفاده از دو توپولوژی متفاوت، آن‌ها نشان دادند که تمامی حملات شناسایی‌شده توسط IDS به‌طور موفقیت‌آمیز کاهش داده شدند.

۲/۴ سامانه تشخیص نفوذ (IDS) با استفاده از الگوریتمXGBoost

نویسندگان در پژوهش [30] یک سامانه تشخیص نفوذ (IDS) برای شبکه‌های بین‌خودرویی VANETطراحی کردند و از مجموعه‌داده ToN-IoT [31]استفاده نمودند. برای بهبود کارایی و سرعت مدل، از تکنیک Chi-square (Chi²)برای انتخاب ویژگی استفاده شد که تعداد ویژگی‌ها را از ۱۰۸ به ۲۰ کاهش داد. تکنیک Chi² ابزاری ارزشمند در یادگیری ماشین برای انتخاب مرتبط‌ترین ویژگی‌ها از یک مجموعه‌داده است. این روش آماری با محاسبه نمره‌ای مبتنی بر میزان وابستگی هر ویژگی به متغیر هدف (برچسب‌های کلاس) عمل می‌کند. از این طریق می‌توان ویژگی‌هایی را که تأثیر اندکی بر پیش‌بینی خروجی دارند شناسایی و حذف کرد. با تمرکز بر ویژگی‌های مهم‌تر، تکنیک Chi² باعث افزایش کارایی و دقت مدل‌های یادگیری ماشین می‌شود. برای مقابله با بیش‌برازش (Overfitting) و سوگیری نسبت به کلاس اکثریت، از روش SMOTEاستفاده شد. این روش با ایجاد نمونه‌های مصنوعی از کلاس اقلیت، مشکل عدم‌توازن داده را برطرف کرده و عملکرد مدل را بهبود می‌بخشد.

جدول ۳: خلاصهٔ اطلاعات مجموعه‌داده، مزایا و معایبِ روش‌های یادگیری عمیق و یادگیری ماشین برای تشخیص و مقابله

یئوم و همکاران [23] — بدون مجموعه‌داده — ترافیک واقعی درخواست‌های DNS جمع‌آوری‌شده ازDNS-STAT: Hedgehog ، تحت مدیریت ICANN — امکان بهبود در روش تشخیص حمله از سمت منبع

راوی و همکاران 24 — [20] UNB ISCX — [نتایج نشان داد روش LEDEM دقت تشخیص حملات DDoS را تا ٪۹۶,۲۸ افزایش داده است — احتمال بروز مثبت‌های کاذب در روش‌های نظارت‌شده و بدون‌نظارت

سانتوس و همکاران [25] — بدون مجموعه‌داده — الگوریتم Random Forest بالاترین دقت را به‌دست آورد — الگوریتم Decision Tree به‌دلیل زمان پردازش پایین، بهترین عملکرد کلی را داشت

ندیم و همکاران 26 — [27] NSL-KDD — [طبقه‌بند RF آموزش‌دیده با ویژگی‌های انتخاب‌شده توسط RFE نتایج بسیار دقیقی در تشخیص حملات روی کنترلر SDN ارائه داد — مصرف منابع کنترلر SDN افزایش می‌یابد و دقت با افزایش ترافیک کاهش پیدا می‌کند دهکردی و همکاران 28 — [20] UNB ISCX — [به‌کارگیری الگوریتم‌های مختلف طبقه‌بندی نتایج دقیق‌تری ایجاد کرد — نتایج بهتر با آستانه‌های پویا حاصل شد، اما با نرخ بالای مثبت کاذب(FPR)

پرز–دیاز و همکاران 29 — [5] CICIDS2017 —همهٔ حملاتی که توسط IDS شناسایی شدند با موفقیت مهار شدند — دشواری ذاتی در تشخیص حملات کم‌نرخ(LR-DDoS)

مشکل عدم توازن داده‌ها مطرح است. برای ارزیابی عملکرد مدل یادگیری ماشین، از معیارهای مختلفی مانند دقت(Accuracy) ، دقت مثبت (Precision)، فراخوانی(Recall) ، امتیازF1 ، نرخ مثبت کاذب (FPR) و ماتریس سردرگمی استفاده شد. الگوریتم XGBoostبالاترین عملکرد را در میان الگوریتم‌های آزمایش‌شده نشان داد. این مقاله یک توضیح جامع از فرایند پردازش داده برای پیاده‌سازی تکنیک‌های یادگیری ماشین ارائه می‌دهد. استفاده از مجموعه‌داده Ton-IoTنیازمند تلاش‌های پیش‌پردازشی گسترده بود. در آینده می‌توان از یک مجموعه‌داده جایگزین برای آزمایش سیستم استفاده کرد که می‌تواند مفید باشد.

در مرجع [32]، نویسندگان یک سامانهٔ تشخیص نفوذ (IDS) طراحی کردند که حملات را سریع شناسایی کرده و تصمیم‌گیری می‌کند. این سیستم از شبکهٔ عصبی مصنوعی (ANN) استفاده کرده و با مجموعه‌داده [33] UNSW-15برای ارزیابی کارایی آن تست شد. نتایج ارزیابی نشان داد روش پیشنهادی نرخ دقت ٪84 برای شناسایی تهدیدات و نرخ مثبت کاذب ٪8 دارد. قرار است IDS در یک کنترل‌کنندهٔ IoT ادغام شود تا میان داده‌های سالم و مخرب تمایز قائل شده و داده‌های مخرب را سریع حذف کند. در تحلیل مقایسه‌ای این سیستم، دو مجموعه‌دادهٔ متفاوت استفاده شد. یک آزمایش ایده‌آل باید از یک مجموعه‌داده یکسان برای تمام سیستم‌ها استفاده کند تا مقایسه منصفانه باشد. لازم به ذکر است که مجموعه‌داده [27] NSL-KDDاز جنبه‌های مختلف با UNSW-15 متفاوت است، از جمله اندازهٔ کوچک‌تر، تعداد کمتر نمونه‌های حمله، تعداد شبکه‌های کمتر، و تکرار بیشتر در داده‌ها Cruz .و همکاران [34] روشی برای ایجاد یک مدل سبک‌وزن با سربار کم ارائه دادند که دقت 93.6٪ را به دست آورد. این مطالعه از XGBoost به‌عنوان مدل یادگیری ماشین استفاده کرده و آن را بر روی مجموعه‌داده [35] IoT-23با تمرکز بر حملات تکرارسازی (Replication Attacks) آزمایش کرد. حملهٔ تکرارسازی نوعی اقدام فریبکارانه است که در آن مهاجم با تقلید ترافیک مشروع تلاش می‌کند به سیستم دسترسی غیرمجاز پیدا کند. مدل مورد استفاده در این روش می‌تواند در یک راهکار میان‌افزار IoT برای مسدود کردن دسترسی دستگاه‌های مشکوک ادغام شود. یکی از بهبودهای احتمالی در این تحقیق می‌تواند ارزیابی قابلیت سازگاری مدل و عملکرد سیستم بر اساس مجموعه‌داده‌های مختلف باشد. علاوه بر این، مفید است که الگوریتم XGBoost با سایر تکنیک‌های یادگیری ماشین مانند جنگل تصادفی (Random Forest)یا مدل‌هایی که خود را در طول آموزش با داده‌ها تطبیق می‌دهند مقایسه شود.

جدول 4 نمای کلی از اطلاعات مجموعه‌داده، مزایا و معایب IDS مبتنی بر الگوریتم XGBoost را ارائه می‌دهد.

2.5 رویکردهای هوش مصنوعی و یادگیری ماشین درSDN

Gebremariamدر پژوهش خود بینش‌های ارزشمندی دربارهٔ استفاده از هوش مصنوعی/یادگیری ماشین (AI/ML) در شبکه‌های SDNو مجازی‌سازی کارکردهای شبکه (NFV) ارائه می‌دهد و پیشرفت‌های مهم این حوزه و همچنین چالش‌های آینده را در [7] شناسایی می‌کند. او معتقد است که ادغام AI/ML می‌تواند به ایجاد شبکه‌هایی منجر شود که خودپیکربندی، خودتطبیق‌پذیر و خودمدیریت‌شونده باشند. با این حال، محدودیت منابع شبکه و نبود مجموعه‌داده‌های در دسترس همچنان از موانع مهم تحقیقات در این حوزه هستند. این تحقیق چندین مفهوم برجسته معرفی می‌کند. عملیات ابری نیازمند الگوریتم‌های کارآمد و پردازش لبه (Edge Computing) است تا وظایف پیچیده را با حداقل‌سازی مصرف انرژی مراکز داده انجام دهد. علاوه بر این، ذخیره‌سازی راهبردی داده‌ها در سراسر شبکه در برابر خرابی‌ها و حملات از داده محافظت کرده و یکپارچگی و تاب‌آوری آن را تضمین می‌کند Zhoe .یک چارچوب ایجاد کرد که تولید، استقرار و تنظیم دفاع پیش‌گیرانه برای IoT را خودکار می‌کند [36]. این تیم از انعطاف‌پذیری معماری SDN برای استقرار کارآمد سازوکارهای دفاعی استفاده کرد. این چارچوب مبتنی بر تکنیک‌های دفاع هدف متحرک (MTD) و فریب سایبری است. این رویکرد قصد دارد مهاجمان را گمراه کرده و اختلالات سیستم را کاهش دهد. تیم در محیط آزمایش از کنترلر Ryuو شبیه‌ساز Mininetبرای ایجاد زیرساخت SDN استفاده کرد. این چارچوب دو ضعف کلیدی دارد: آسیب‌پذیری در برابر حملات اتمام منابع؛ مهاجمانی با منابع زیاد می‌توانند سیستم را با انبوهی از درخواست‌ها از کار بیندازند. ناتوانی در تشخیص کاربران مشروع از افراد داخلی (Insiders)؛ این محدودیت باعث می‌شود چارچوب تنها در برابر تهدیدات خارجی مؤثر بوده و در برابر حملات داخلی آسیب‌پذیر باشد Sahoo . و همکاران [37] یک روش برای تشخیص و کاهش حملات DDoS ارائه کردند که از ترکیب مدل‌های یادگیری ماشین SVM، تحلیل مؤلفه‌های اصلی هسته‌ای (KPCA) و الگوریتم ژنتیک (GA) استفاده می‌کند. در این روش SVM :نقش طبقه‌بندی‌کننده را دارد، KPCAویژگی‌ها را استخراج می‌کند، GAپارامترهای SVM را بهینه می‌کند. همچنین یک تابع هسته‌ای اصلاح‌شده به نام N-RBFبرای کاهش تفاوت‌های ویژگی (نویز) استفاده شد. برای ارزیابی مدل، نویسندگان از دو مجموعه‌داده، شامل [27] NSL-KDDو یک SDN testbedبا کنترلر POX استفاده کردند. این بستر آزمایشی با Mininetایجاد شد. این راهکار چند محدودیت دارد: این سیستم در تشخیص بسته‌های ICMPمشکل دارد، زیرا این بسته‌ها در کلاس *"smurf"*طبقه‌بندی می‌شوند و تمایز میان ترافیک سالم و حمله سخت می‌شود. نگرانی‌های مقیاس‌پذیری وجود دارد؛ زیرا محیط آزمایشی تنها شامل یک کنترلر بود. هرچند عملکرد آن در این شرایط قابل قبول بود، اما کارایی آن در محیطی با چندین کنترلر نامشخص است Tan .و همکاران چارچوبی برای شناسایی و جلوگیری از حملات DDoS توسعه دادند [38]. این چارچوب از یک مکانیزم تحریک (Trigger Mechanism) در صفحه داده برای تشخیص چنین حملاتی استفاده کرده و از الگوریتم یادگیری ماشین مبتنی بر KNNو K-Meansبهره می‌برد.

جدول ۴. خلاصه‌ای از اطلاعات مجموعه‌داده، مزایا و معایب سامانهٔ تشخیص نفوذ (IDS) با استفاده از الگوریتمXGBoost

Gadو همکاران 30 مجموعه‌داده[31] ToN-IoT :

مزیت :الگوریتم XGBoost بهترین عملکرد را در میان الگوریتم‌های آزمایش‌شده نشان داد.

عیب :استفاده از مجموعه‌دادهٔ ToN-IoT به فرایند پیش‌پردازش قابل‌توجهی نیاز داشت.

Hanifو همکاران 32 مجموعه‌داده[27] NSL-KDD :

مزیت :روش پیشنهادی دارای دقت ۸۴٪ است.

عیب :برای مقایسهٔ منصفانه، لازم است تمام سیستم‌ها از یک مجموعه‌دادهٔ یکسان استفاده کنند.

Cruzو همکاران 34مجموعه‌داده[35] IoT-23 :

مزیت :مدل مورد استفاده می‌تواند در یک میان‌افزار IoT برای مسدودسازی دسترسی دستگاه‌های مشکوک ادغام شود.

عیب :مقایسه‌ای میان الگوریتم XGBoost و سایر تکنیک‌های یادگیری ماشین انجام نشده است.

در این چارچوب، از کنترلر SDN برای شناسایی جریان‌های مشکوک استفاده می‌شود. کارایی این چارچوب با استفاده از مجموعه‌داده NSL-KDD [27]و همچنین یک محیط SDN ساخته‌شده با Mininet و کنترلر ONOS ارزیابی شده است. پژوهشگران با چالش‌هایی مربوط به توان پردازشی کنترلر مواجه شدند، به‌ویژه هنگامی که بار شبکه برای مدیریت ترافیک گسترده افزایش پیدا کرد. قابلیت تشخیص DDoS در این چارچوب تحت بارهای سنگین شبکه کاهش می‌یابد. با افزایش حجم داده‌ها، به‌خصوص در زمان اوج ترافیک، کنترلر دچار اضافه‌بار می‌شود. این فشار باعث کاهش توانایی کنترلر در تشخیص مؤثر حملات DDoS شده و در نتیجه آسیب‌پذیری شبکه افزایش یافته و ممکن است کیفیت ارائه خدمات در زمان‌های پرترافیک کاهش یابد. چارچوب دیگری توسط Revathiو همکاران [39] ارائه شد که از یک ماشین بردار پشتیبان مبتنی بر حافظه مقیاس‌پذیر گسسته (DSM-SVM) برای پیش‌بینی و کاهش حملات DDoS در SDN استفاده می‌کند. برای ارزیابی الگوریتم، مجموعه‌داده [40] KDD99 و یک بستر آزمایشی SDN شامل Mininet و کنترلر RYU مورد استفاده قرار گرفت. براساس پژوهش انجام‌شده، نگرانی‌هایی درباره نسبت تقسیم داده‌های آموزشی و آزمایشی وجود دارد. یک نسبت تقسیم متعادل نقش مهمی در تعمیم‌پذیری مناسب الگوریتم ایفا می‌کند. این موضوع توانایی چارچوب را در تشخیص و کاهش حملات افزایش می‌دهد. مطالعه همچنین کاربرد سیستم در خدمات آنلاین را بررسی کرده و اثربخشی آن را در جلوگیری و کاهش حملات نشان می‌دهد؛ که این موضوع به افزایش امنیت و قابلیت اطمینان در محیط‌های خدمات آنلاین می‌انجامد Fajar . روش‌های مختلف کاهش حملات DDoS که از منابع مختلف منشأ می‌گیرند را بررسی کرده است [41]. مسائل امنیتی مرتبط با SDN نیز مورد بررسی قرار گرفت. باوجود تلاش‌های مداوم جامعه امنیتی برای توسعه مکانیزم‌های مقابله با حملاتDDoS ، تکنیک‌های موجود با محدودیت‌هایی مواجه هستند. برای رفع این نقص‌ها و تقویت امنیت کلیSDN ، نویسندگان پیشنهاد می‌کنند از قابلیت‌های منحصربه‌فرد شبکه نرم‌افزارمحور برای ایجاد یک راهبرد دفاعی قوی‌تر استفاده شود Elsayed .و همکاران 4یک مجموعه‌داده عمومی جدید به نام InSDN [4] معرفی کردند که شامل 343,939 نمونه از ترافیک عادی و مخرب است. داده‌های عادی 68,424 نمونه و داده‌های مربوط به حملات 275,515 نمونه را تشکیل می‌دهند. این مجموعه‌داده همچنین دارای 83 ویژگی است. مجموعه‌داده شامل دسته‌های مختلف حملات مانندDoS ، DDoS، حملات وب، بات‌نت، حدس رمزعبور، پروب‌ها و سوءاستفاده‌ها است. نویسندگان کارایی مجموعه‌داده را با استفاده از معیارهایی مانند دقت، بازخوانی، نمره F و زمان آموزش ارزیابی کردند. هنگامی که چهار مجموعه‌داده عمومی مقایسه شدند، الگوریتم AdaBoost بهترین عملکرد را نشان داد. برای ارزیابی کیفیت مجموعه‌داده، هشت الگوریتم یادگیری نظارت‌شده از جمله درخت تصمیم(DT) ، جنگل تصادفیAdaBoost ,(RF) ، KNN، بیز ساده (NB)، SVMبا هسته خطی، SVMبا هسته RBF ، و MLP استفاده شد AdaBoost .بالاترین امتیاز را کسب کرد و پس از آن DT و RF قرار گرفتند. این مقاله محدودیت‌های مهمی را نیز بیان کرده است. از جمله مهم‌ترین محدودیت‌ها، عدم توازن چشمگیر کلاس‌ها در مجموعه‌داده است که ممکن است منجر به افزایش نرخ هشدار کاذب و کاهش دقت ارزیابی شود. علاوه بر این، آزمایش‌ها تنها از یک کنترلر ONOS استفاده کردند که نمی‌تواند تنوع کنترلرهای SDN و مکانیسم‌های امنیتی مختلف را پوشش دهد. همچنین به دلیل محدودیت‌های سخت‌افزاری، تنها یک کنترلر در شبکه مورد استفاده قرار گرفت، که توانایی بازنمایی معماری‌های بزرگ سازمانی با چند کنترلر، چند سوییچ و چند گره را محدود می‌کند.

Tanو همکاران[42]سازوکارهای تشخیص و دفاع در برابر حملات DDoS در SDN را با استفاده از قابلیت‌های SDN و الگوریتم‌های یادگیری ماشین تحلیل کردند. رویکرد آن‌ها شامل یک روش هدفمند برای تشخیص و دفاع در برابر حملات DDoS است که به‌طور خاص کنترلر SDN را هدف قرار می‌دهند. نتایج آزمایش‌ها نشان می‌دهد که روش پیشنهادی تشخیص عملکرد مثبتی دارد. علاوه بر این، سازوکار شروع تشخیص (Trigger Mechanism)قادر است جریان‌های غیرعادی را به‌طور مؤثر شناسایی کند، در حالی که منابع کنترلر نیز حفظ می‌شوند. این استراتژی دفاعی نیز حملات DDoS را به‌طور مؤثر کاهش می‌دهد. بااین‌حال، تحت ترافیک وسیع‌تر شبکه، بار کنترلر افزایش یافته و کارایی تشخیص کاهش پیدا می‌کند. در این مطالعه از کنترلر ONOS و Mininet برای شبیه‌سازی محیط شبکه استفاده شد. ابزار Scapy برای ایجاد آدرس‌های IP مقصد تصادفی جهت شبیه‌سازی حملات DDoS روی صفحه کنترل استفاده شد. برای تشخیص حملاتDDoS ، از یک الگوریتم ترکیبی K-Means و KNN استفاده شد. همچنین برای ارزیابی عملکرد روش، مجموعه‌داده NSL-KDD [27] به کار گرفته شد. در نهایت، محققان الگوریتم‌هایK-Means ، KNN، و نسخه ترکیبی آن دو را با نتایج DPTCM-KNN و KD-Tree مقایسه کردند.

Aliو همکاران [43]

هدف این مرور نظام‌مند، شناسایی، ارزیابی و بررسی تلاش‌های اخیر در زمینه‌ی راهکارهای تشخیص حملات DDoS مبتنی بر یادگیری ماشین (ML)و یادگیری عمیق (DL) در شبکه‌های SDN است. برای این منظور، یک مرور نظام‌مند از مقالات منتشرشده که از روش‌های ML/DL برای شناسایی حملات DDoS در شبکه‌های SDN بین سال‌های 2018 تا اوایل نوامبر 2022 استفاده کرده‌اند، انجام شد. این جستجوی جامع شامل چندین کتابخانه دیجیتال از جمله IEEE ، ACM، Springerو دیگر منابع، به‌همراه Google Scholar بود. پژوهشگران مطالعات مرتبط را تحلیل کرده و نتایج را در پنج بخش اصلی دسته‌بندی کردند: انواع روش‌های تشخیص حملات DDoS در رویکردهایML/DL روش‌شناسی‌ها، نقاط قوت و ضعف رویکردهای موجودمجموعه‌داده‌ها و انواع حملات استفاده‌شده در تحقیقات پیشین راهبردهای پیش‌پردازش، مقادیر ابرپارامترها، تنظیمات آزمایش و معیارهای ارزیابی مقایسه عملکرد مدل‌هابسیاری از مطالعات، نرخ دقت بالاتر از 99٪ را گزارش کرده‌اند. بااین‌حال، از آنجاکه اکثر این تحقیقات از تحلیل آفلاین داده استفاده کرده‌اند، ممکن است عملکرد واقعی مدل‌ها در محیط‌های عملیاتی یا تولیدی متفاوت باشد. همچنین استفاده از مجموعه‌داده‌ها و روش‌های ارزیابی متفاوت در مقالات موجود، مقایسه مستقیم نتایج آن‌ها را دشوار می‌کند .

این مقاله قابلیت‌ها و اثربخشی مدل‌های یادگیری عمیق، به‌ویژه LSTM و شبکه‌های عصبی کانولوشنی(CNN) ، را در تشخیص و مقابله با حملات DDoSبررسی می‌کند. تمرکز این پژوهش بر حملات TCP ، UDPو ICMP Flood علیه کنترلر SDN است. عملکرد این مدل‌ها بر اساس معیارهایی مانند دقت، بازخوانی و نرخ منفیِ درست ارزیابی و با مدل‌های سنتی یادگیری ماشین مقایسه شد. همچنین مدت زمان لازم برای تشخیص و مقابله با حملات مورد بررسی قرار گرفت. نتایج نشان داد که الگوریتم RNN LSTM یک مدل مناسب و کارآمد برای تشخیص و کاهش حملات DDoS در کنترلر SDN است. این مدل به دقت 89.63٪ دست یافت که بهتر از مدل‌های خطی مانندSVM 86.85% وNaive Bayes % 82.61 بود. اگرچه الگوریتم KNN به دقت بالاتری99.4 ٪دست یافت، اما مدل پیشنهادی با ارائه یک تعادل خوب میان دقت و بازخوانی، گزینهٔ مناسبی برای دسته‌بندی حملات DDoS محسوب می‌شود. پژوهشگران همچنین مشاهده کردند که نسبت تقسیم داده‌های آموزشی و آزمایشی تأثیر قابل توجهی بر عملکرد مدل‌های یادگیری عمیق دارد. نسبت 70/30بهترین عملکرد را نسبت به نسبت‌های 20/80 و 40/60 ارائه کرد. برای تولید ترافیک، از ابزار hping3 استفاده شد که ترافیک عادیTCP ، UDPو ICMP را میان دو نقطه شبکه شبیه‌سازی می‌کرد. مجموعه‌داده شامل 10,031نمونه بود که 4,270نمونه 43٪ ترافیک مخرب و 5,761نمونه 57٪ترافیک عادی بودند. این داده‌ها برای ساخت مدل‌های طبقه‌بندی دودویی با الگوریتم‌های مختلف ML مانندKNN ، رگرسیون لجستیک، Linear SVC، SVC، درخت تصمیم، جنگل تصادفی، گرادیان بوستینگ و انواع طبقه‌بندهای Naive Bayes (گاوسی، برنولی و چندجمله‌ای)، و همچنین دو مدل اصلی یعنی RNN LSTM و CNN استفاده شدند.

2.6 حملات در شبکه‌های خودرویی با استفاده از SDN و موارد بیشتر

Yuو همکاران 45یک پلتفرم برای شناسایی و کاهش حملات DDoS در شبکه‌های خودرویی مبتنی بر SDN توسعه دادند. این پلتفرم از یک تکنیک تشخیص مبتنی بر جدول جریان (Flow Table Detection) استفاده می‌کند. برای ارزیابی اثربخشی این پلتفرم، آن را بر روی مجموعه‌داده‌های DARPA 1999 [46]، DARPA 2000 [47]و CAIDA DDoS 2007 [48] آزمایش کردند. همچنین یک بستر آزمایشی SDN مبتنی بر Mininet ایجاد شد که از کنترلر Floodlightاستفاده می‌کرد. این پژوهش به مسئلهٔ بار اضافی وارد بر کنترلر SDN در اثر تعداد زیاد پیام‌های PACKET_IN می‌پردازد. روش پیشنهادی با بهره‌گیری از PACKET_INبه‌عنوان محرک پاسخ سریع‌تر، این مشکل را کاهش داد. علاوه بر این، این مطالعه از پروتکل‌هایTCP ، UDPو ICMP در سناریوهای حمله DDoS استفاده کرد. همچنین یک روش انتخاب ویژگی مبتنی بر ضریب همبستگی برای افزایش کارایی تحلیل به کار گرفته شد .Maity و همکاران یک سیستم تشخیص DDoS مبتنی بر مدل‌سازی احتمالاتی توسعه دادند که از توزیع پرچم‌های TCP در کنترلر SDN به جای سرعت ترافیک استفاده می‌کند تا نرخ خطای منفی کاهش یابد. این سیستم با استفاده از مجموعه‌داده DARPA 2009 [49]ارزیابی شد و در یک محیط SDN با کمک Mininet و کنترلر Floodlight آزمایش گردید. پژوهشگران با محدودیت‌هایی مواجه شدند، از جمله نبود تنوع کافی در انواع ترافیک شبکه که برای آزمایش جامع سیستم لازم بود. همچنین، مقاومت سیستم در برابر حملات DDoSکمتر از حد انتظار بود. آنان ابراز داشتند که قصد دارند در آینده این سیستم را به سمت پیاده‌سازی بلادرنگ در محیط‌های توزیع‌شده هدایت کنند. جدول 6 مروری بر اطلاعات مجموعه‌داده‌ها، مزایا و معایب مربوط به حملات در شبکه‌های خودرویی مبتنی بر SDN و موارد بیشتر ارائه می‌دهد. جدول 7 نمایی کلی از مطالعات پیشین شامل روش‌ها، مجموعه‌داده‌ها و نکات کلیدی ارائه می‌کند .

3.جموعه‌داده‌ها

مجموعه‌داده‌های باز یا قابل‌دسترس عمومی برای پیشرفت پژوهش در زمینهٔ تشخیص و کاهش حملات در SDN اهمیت فراوانی دارند. این مجموعه‌داده‌ها به‌عنوان یک پایهٔ مشترک عمل کرده، امکان ادامهٔ تحقیقات و تکرارپذیری نتایج را فراهم می‌کنند. دسترس‌پذیری مجموعه‌داده‌های باز به محققان اجازه می‌دهد تا یک استاندارد مشترک برای ارزیابی کاربردها و سناریوهای مختلف ایجاد کنند. در میان مجموعه‌داده‌های موجود، آن‌هایی که به‌طور خاص بر حملات DDoS تمرکز دارند برای پیشرفت تحقیقات بسیار ارزشمند هستند.

DARPA98 [46] مجموعه‌داده DARPA 98 الگوهای رایج ترافیک را در یک وب‌سایت دولتی با صدها کاربر و هزاران میزبان شبیه‌سازی می‌کند. هنگام ایجاد این مجموعه‌داده، بیش از 300 نمونه از 38 نوع حملهٔ خودکار متفاوت تولید شده بود.

جدول ۵ خلاصه‌ای از اطلاعات مجموعه‌داده‌ها، مزایا و معایب رویکردهای هوش مصنوعی و یادگیری ماشین درSDN

Gebremariam و همکاران 7بدون مجموعه‌داده

✓ذخیره‌سازی راهبردی داده‌ها در سراسر شبکه از خرابی‌ها و حملات جلوگیری می‌کند و یکپارچگی و تاب‌آوری داده‌ها را تضمین می‌کند.
✗منابع محدود شبکه و نبود مجموعه‌داده‌های آماده و در دسترس.

Zhouو همکاران 36 بدون مجموعه‌داده

✓این روش با هدف گمراه‌کردن مهاجمان و کاهش اختلالات سیستم طراحی شده است.
✗مستعد حملات تخلیه منابع.(Resource exhaustion)

Sahooو همکاران 37
NSL-KDD [27]
SVM ✓به‌عنوان دسته‌بند عمل می‌کند، درحالی‌که KPCA استخراج ویژگی‌ها را انجام می‌دهد و GA نیز SVM را بهینه می‌کند.
✗در محیط‌هایی با چند کنترلر، عدم قطعیت‌هایی ایجاد می‌شود.

Tanو همکاران 38
NSL-KDD [27]
✓کارایی این چارچوب با استفاده از مجموعه‌داده NSL-KDD و یک محیط SDN مبتنی بر Mininet ارزیابی شده است.
✗کنترلر توانایی خود را در تشخیص مؤثر حملات DDoS از دست می‌دهد.

Revathiو همکاران 39
KDD99 [40]
✓مطالعه همچنین به کاربرد این سیستم در خدمات آنلاین پرداخته و کارایی آن را در جلوگیری و کاهش حملات نشان می‌دهد.
✗نگرانی‌هایی درباره نسبت تقسیم داده‌های آموزش و آزمون وجود دارد.

Fajarو همکاران 41
بدون مجموعه‌داده
✓نویسندگان پیشنهاد بهره‌گیری از قابلیت‌های منحصربه‌فرد SDN را برای یک راهبرد دفاعی قدرتمندتر مطرح می‌کنند.
✗هیچ مورد منفی گزارش نشده است.

Elsayedو همکاران 4
InSDN [4]
✓دسته‌بند AdaBoost بالاترین عملکرد را داشته و پس از آن DT و RF در رتبه‌های بعدی قرار دارند.
✗این مجموعه‌داده تنها از یک کنترلر استفاده کرده است.

Tanو همکاران 42
NSL-KDD [27]
✓آزمایش‌ها نشان می‌دهند روش‌های پیشنهادی تشخیص نتایج مثبتی ارائه می‌دهند.
✗در ترافیک شبکه در مقیاس بزرگ، بار کنترلر افزایش یافته و کارایی تشخیص DDoS کاهش می‌یابد.

Aliو همکاران 43
بدون مجموعه‌داده
✓بسیاری از مطالعات دقت بالای ٪۹۹ را گزارش کرده‌اند.
✗این مطالعات از تحلیل آفلاین استفاده کرده‌اند؛ بنابراین عملکرد در محیط واقعی ممکن است متفاوت باشد.

Gadzeو همکاران 44

بدون مجموعه‌داده
✓نسبت تقسیم ۷۰/۳۰ بهترین عملکرد را نسبت به ۸۰/۲۰ و ۶۰/۴۰ ارائه داده است.
✗نبود مجموعه‌داده باعث دشوار شدن تکرارپذیری نتایج می‌شود.

Discover

ترجمهٔ فارسی جدول ۶: خلاصه اطلاعات مجموعه‌داده، مزایا و معایب حملات در شبکه‌های خودرویی مبتنی بر SDN و سایر موارد

Yu et al. [45]
CAIDA DDoS 2007 [48], DARPA 99 [47], DARPA 2000 [50]
مزیت :این روش با بهره‌گیری از مکانیسم *PACKET_IN trigger* توانست این مشکل را به‌طور موفقیت‌آمیزی کاهش دهد و زمان واکنش را تسریع کند.
عیب :هیچ‌کدام گزارش نشده است.

Maity et al. [49]
DARPA 2009 [51]
مزیت :هیچ‌کدام گزارش نشده است.
عیب :مقاومت سیستم در برابر حملات DDoS کمتر از حد انتظار بود.

دارپا 98:[46] (DARPA98)
در این مجموعه‌داده، الگوهای ترافیکی معمولی مربوط به یک وب‌سایت دولتی که صدها کاربر در میان هزاران میزبان از آن استفاده می‌کنند، شبیه‌سازی شده است. طی فرآیند ایجاد این مجموعه‌داده، بیش از ۳۰۰ نمونه از ۳۸ نوع حملهٔ خودکار مختلف علیه میزبان‌های مبتنی بر UNIXاجرا شد. آزمایشگاه لینکلن MIT این مجموعه‌داده را طی ۷ هفته و با حجم ۴ گیگابایت دادهٔ باینری تولید کرد. این مجموعه، سناریویی شبیه یک شبکهٔ کوچک نیروی هوایی متصل به اینترنت را بازسازی می‌کند و به‌عنوان یک مرجع مهم برای ارزیابی سامانه‌های تشخیص نفوذ (IDS)مورد استفاده قرار می‌گیرد [9]

دارپا 99:[47] (DARPA99)
این ارزیابی جامع، که منجر به تولید مجموعه‌دادهٔ DARPA 99 شد، هشت مرکز پژوهشی را در تحلیل توانایی تشخیص و نرخ هشدار اشتباه سامانه‌های تشخیص نفوذ درگیر کرد. ارزیابی در یک محیط شبکه‌ای کنترل‌شده انجام شد که شامل میزبان‌هایی بود که در معرض حملات قرار می‌گرفتند و ترافیک مصنوعی ایجادشده توسط مولدهای پیشرفته‌ای را دریافت می‌کردند که رفتاری مشابه ترافیک زندهٔ یک پایگاه کوچک نیروی هوایی داشتند. شبیه‌سازی ترافیک، رفتار صدها کاربر و هزاران میزبان را تقلید می‌کرد.
در طی ۳ هفته دادهٔ آموزش و ۲ هفته دادهٔ آزمون، بیش از ۲۰۰ نمونه از ۵۸ نوع حملهٔ متفاوت علیه میزبان‌های UNIX و Windows NT اجرا شد. حاصل این فرایند، مجموعه‌دادهٔ ارزشمند DARPA 99 برای تحقیقات امنیت سایبری بود.

دارپا 2000:[50] (DARPA2000) در سال ۱۹۹۹، آزمایشگاه لینکلن مجموعه‌دادهٔ DARPA 2000 را معرفی کرد که شامل ۵ هفته ترافیک شبیه‌سازی‌شدهٔ شبکه‌ای است. این مجموعه شامل دو سناریوی حمله است LLDoS 1.0 :و .LLDoS 2.0.2
هر دو سناریو از میزبان‌های حمله‌کننده و قربانی یکسان استفاده می‌کنند و شامل انواع حملات:

- DoS
- User-to-Root (U2R)
- Remote-to-Local (R2L)
- Probe

هستند.
حملات در پنج مرحله انجام می‌شوند:

۱.اسکن میزبان،۲. ارسال بسته‌های پرسش آسیب‌پذیری،۳. سوءاستفاده و افزایش سطح دسترسی،۴. نصب نرم‌افزار DDoS روی میزبان قربانی،۵. اجرای حملهٔ DDoS روی هدف.

دارپا 2009:[51] (DARPA2009)

این مجموعه‌داده با استفاده از ترافیک مصنوعی شبیه‌سازی شد تا تعاملات میان یک زیرشبکهٔ /16 (دامنهٔ 16/172.28.0.0) و اینترنت را بازنمایی کند. داده‌ها طی ۱۰ روز، از ۳ تا ۱۲ نوامبر ۲۰۰۹ جمع‌آوری شدند. این مجموعه شامل ترافیک مصنوعیHTTP ، SMTPو DNS است و دارای

طیف وسیعی از رویدادهای امنیتی و انواع حملات، از جمله حملات مختلف DDoS و انواع کرم‌ها (worms) با الگوهای گسترش متفاوت است. این مجموعه شامل ۷۰۰۰ فایل pcap بوده و حجم کل آن تقریباً ۶/۵ ترابایت است.

[40] KDD99:

برای تهیهٔ یک زیرمجموعه از داده‌های DARPA 1998 ، یک شبکهٔ LAN نیروی هوایی آمریکا شبیه‌سازی شد و انواع مختلف حملات روی آن اجرا شد. این فرایند از ۹ هفته دادهٔ TCP dump جمع‌آوری‌شده در MIT Lincoln Lab استفاده کرد. نتیجهٔ آن، مجموعه‌دادهٔ KDDCup است که شامل تقریباً ۴/۹ میلیون نمونه با ۴۱ ویژگی است. این نمونه‌ها به دو دستهٔ «عادی» و «دارای نفوذ» تقسیم می‌شوند. دادهٔ آموزشی: شامل 24 برچسب (۱ رفتار عادی + ۲۳ نوع حمله) دادهٔ آزمون: شامل ۱۴ نوع حملهٔ جدید اضافه شده

حملات در چهار گروه طبقه‌بندی می‌شوند Probe-R2L-DoS- U2R

[27] NSL-KDD:

این مجموعه پس از حذف داده‌های تکراری و افزونه‌های موجود در KDDCup ایجاد شد. داده‌ها شامل:

- 125,973 رکورد برای آموزش
- 22,544 رکورد برای آزمون

در این مجموعه، از میان ۳۷ حمله:

- ۲۷ حمله در دادهٔ آزمون
- ۲۳ حمله در دادهٔ آموزش

قرار گرفته‌اند. این مجموعه مانند KDDCup ، ۴۱ ویژگی و ۵ کلاس (۱ کلاس عادی + ۴ کلاس حمله) دارد و توزیع بهتری نسبت به KDD99 ارائه می‌کند.

[52] DECON-8:

نسخهٔ DEFCON-8 شامل حملات مبتنی بر اسکن پورت و سرریز بافر است. نسخهٔ دیگر این مجموعه شامل حملات مبتنی بر FTP ، بسته‌های مخرب، اسکن پورت و حملات sweep است. با این حال، این مجموعه‌داده محدودیت دارد؛ زیرا ترافیک موجود در مسابقات «Capture the Flag (CTF)» با ترافیک واقعی شبکه تفاوت زیادی دارد و همین موضوع ارزیابی سامانه‌های IDS را تحت تأثیر قرار می‌دهد.

جدول ۷. خلاصهٔ کارهای پیشین بر اساس روش‌ها، مجموعه‌داده‌های به‌کاررفته و نکات برجسته

Sarica و همکاران 1
روش طبقه‌بندی‌کننده Random Forest
مجموعه‌داده [8] SDN Dataset :
رویکرد آن‌ها بر استخراج خودکار ویژگی‌های جریان و طبقه‌بندی بسیار دقیق جریان‌های شبکه با استفاده از طبقه‌بندی‌کنندهٔ Random Forest در لایهٔ کاربردی SDN متکی بود. این روش برای تشخیص انواع مختلف حملات و انجام اقدامات اصلاحی از طریق نصب قوانین جریان جدید با اولویت بالا در سطح داده به کار گرفته شد.

Galeano-Brajones و همکاران 13
روش الگوریتم مبتنی بر آنتروپی
مجموعه‌داده [12] Bot-IoT :
سه سناریو ارائه شد:

1. نمایش مصرف پهنای باند و مقادیر آنتروپی در طول یک حمله DoS و فرایند کاهش آن با استفاده از کنترلر Ryu و بستر آزمایشی Mininet.
2. دو سناریوی بعدی از مجموعه‌داده Bot-IoT برای ارزیابی فرایند تشخیص و کاهش حملات DoS در محیط IoT استفاده کردند.

3. سناریوی پایانی بر تشخیص و کاهش حملات DDoS در محیط IoT تمرکز داشت.

Wangو همکاران 3

روش :مدل ترکیبی CNN-ELM وExtreme Learning Machine
مجموعه‌داده[4] InSDN :، [5] CICIDS2017
پژوهشگران یک روش کاهش حمله (traceback) برای شبکه‌های SDN ارائه کردند. آن‌ها با استفاده از ده ویژگی توانستند مسیر منبع حمله را شناسایی کنند. همچنین یک مدل یادگیری عمیق ترکیبی CNN-ELM (شبکهٔ عصبی کانولوشنی + ماشین یادگیری سریع) پیشنهاد شد.

Sharmaو همکاران 19
روش :شبکه باور عمیق(Deep Belief Network)
مجموعه‌داده[20] UNB ISCX :
پژوهشگران یک سیستم تشخیص و واکنش به حمله مبتنی بر ناهنجاری به نام OpCloudSec ایجاد کردند. این سیستم از DBN برای ایجاد مدل پیشگیری از حملات استفاده می‌کند.

Salemو همکاران 14
روش :الگوریتم دو مرحله‌ای
مجموعه‌داده :بدون مجموعه‌داده
آن‌ها یک روش تشخیص دوبخشی با دو الگوریتم ارائه کردند تا تشخیص زودهنگام حملات DDoS امکان‌پذیر شود. این روش به هر کاربر یک مقدار اعتماد اختصاص می‌دهد و همراه با ارسال درخواست‌ها به کنترلر، تعداد درخواست‌ها ثبت و مستند می‌شود.

de Assisو همکاران 15
روشCNN :
مجموعه‌داده[16] CICDDoS2019 :
پژوهشگران یک سیستم دفاعی برای شبکه‌های SDN پیشنهاد دادند که ترافیک را در بازه‌های یک‌ثانیه‌ای بررسی می‌کند. سیستم، حملات DDoSبه کنترلر و سرور خارجی را تشخیص و کاهش می‌دهد. همچنین ماژول کاهش و یک نمونه رویکرد مبتنی بر نظریه بازی توضیح داده شد.

Raviو همکاران 24
روشLEDEM :
مجموعه‌داده[20] UNB ISCX :
آن‌ها رویکرد جدیدی به نام LEDEM (تشخیص و کاهش مبتنی بر یادگیری) ارائه کردند که از یک الگوریتم نیمه‌نظارتی برای تشخیص حملات DDoSاستفاده می‌کند.

Gadو همکاران 30
روشXGBoost :
مجموعه‌داده[31] ToN-IoT :
یک IDS برای VANET با استفاده از مجموعه‌داده ToN-IoT ساخته شد. برای بهبود سرعت و کارایی مدل، از روش انتخاب ویژگی Chi2 استفاده شد که ویژگی‌ها را به ۲۰ مورد کاهش داد.

Hanifو همکاران 32
روش :شبکه عصبی مصنوعی(ANN)
مجموعه‌داده[27] NSL-KDD :
پژوهشگران یک IDS توسعه دادند که قادر به تشخیص حملات و اتخاذ تصمیم سریع است. این سیستم در کنترلر IoT ادغام می‌شود تا داده ورودی را به سالم یا مخرب طبقه‌بندی کند و داده مخرب را بلافاصله حذف کند.

Waniو همکاران 8
روشSDIoT-DDoS-DA :

مجموعه‌داده :بدون مجموعه‌داده
یک سازوکار امنیتی برای تشخیص و کاهش حملات DDoS در شبکه‌های SDN با نام SDIoT-DDoS-DA پیشنهاد شد.

Sahooو همکاران 37
روشSVM :، KPCAوGA
مجموعه‌داده[27] NSL-KDD :
یک روش برای تشخیص و کاهش حملات DDoS ارائه شد که از ترکیبSVM ، تحلیل مؤلفه‌های اصلی هسته‌ای(KPCA) ، و الگوریتم ژنتیک (GA)استفاده می‌کند.

در ادامه Table 7

Yu et al. [45]
تکنیک تشخیص جدول جریان
مجموعه‌داده‌ها[48] CAIDA DDoS 2007 :، [47] DARPA 99، [50] DARPA 2000
پژوهشگران یک پلتفرم برای شناسایی و مقابله با حملات DDoS در شبکه‌های خودرویی مبتنی بر SDN ایجاد کردند. این پلتفرم از یک تکنیک تشخیص جدول جریان استفاده می‌کرد.

Maity et al. [49]
یک مدل احتمالاتی
مجموعه‌داده[51] DARPA 2009 :

یک تیم پژوهشی یک سیستم تشخیص DDoS مبتنی بر مدل‌سازی احتمالات طراحی کرد. این مدل به‌جای تکیه بر سرعت ترافیک، از توزیع پرچم‌های TCP در کنترلر برای کاهش نرخ منفی کاذب استفاده می‌کند.

LSTM Yeom et al. [23]مجموعه‌داده :بدون مجموعه‌داده

پژوهشگران یک چارچوب تشخیص حملات DDoS مبتنی بر LSTM پیشنهاد کردند که در سمت منبع عمل می‌کند. برای کاهش افت عملکرد ناشی از رفتار نامنظم ترافیک شبکه، این چارچوب از آستانه‌های تطبیقی مبتنی بر LSTM برای هر منبع شبکه استفاده می‌کند.

UNIBS [53]

تِرِیس‌های بستهٔ UNIBS طی سه روز کاری پیاپی از روتر لبهٔ شبکهٔ دانشگاه برسیا در ایتالیا جمع‌آوری شدند. این مجموعه‌داده شامل ترافیکی است که از ۲۰ ایستگاه کاری که همه آن‌ها سرویس GT (Ground Truth) را اجرا می‌کردند، استخراج شده است. داده‌ها با استفاده از tcpdump از روتر دانشکده — یک سیستم لینوکسی دو پردازندهٔ — Xeon که شبکه محلی را از طریق یک لینک اختصاصی ۱۰۰ مگابیت بر ثانیه به اینترنت متصل می‌کرد، جمع‌آوری شد. این مجموعه‌داده شامل ۲۷ گیگابایت داده و حدود ۷۹,۰۰۰ جریان است؛ عمدتاً ترافیک TCP ٪۹۹ و UDP. ترافیک ثبت‌شده شامل وب (HTTP) و(HTTPS ، ایمیل(POP3 ، IMAP4، SMTPو نسخه‌های SSL آنها، اسکایپ، برنامه‌های همتابه‌همتا مانند BitTorrentوeDonkey ، و سایر پروتکل‌ها مانندFTP ، SSHو MSN است.

CAIDA DDoS 2007 [48]

این مجموعه‌داده شامل تِرِیس‌های ترافیکی است که در جریان حملات DDoS در سال ۲۰۰۷ ضبط شده‌اند. این حملات با ارسال حجم عظیمی از بسته‌ها، باعث اختلال در ترافیک طبیعی شبکه و جلوگیری از رسیدن درخواست‌های مشروع به مقصد می‌شوند. یکی از ضعف‌های این مجموعه‌داده، تنوع پایین حملات است. همچنین دادهٔ جمع‌آوری‌شده شامل ویژگی‌های جامع از کل شبکه نیست و این موضوع، تشخیص دقیق ترافیک عادی و غیرعادی را دشوار می‌کند.

LBNL [54]

این مجموعه‌داده شامل ترافیک ناشناس‌شده و فقط داده‌های سریرگ بسته‌ها است. داده‌ها در آزمایشگاه ملی لورنس برکلِی از دو روتر لبه جمع‌آوری شده‌اند و شامل ترافیک ورودی، خروجی و مسیریابی واقعی می‌شوند. این مجموعه‌داده دارای برچسب نیست و هیچ ویژگی اضافی نیز ایجاد نشده است. ترافیک داخلی و خارجی عمدتاً شامل وب، ایمیل و سرویس‌های نام‌دامنه است، در حالی‌که میزبان‌های داخلی از سرویس‌های ویندوز، سرویس‌های فایل شبکه و پشتیبان‌گیری نیز استفاده می‌کنند. ترافیک مخرب عمدتاً شامل درخواست‌های TCP SYN ناموفق است که نشان‌دهندهٔ اسکن پورت به مقصد میزبان‌های LBNL است. برخی اسکن‌های خروجی نیز وجود دارد. بیشتر ترافیک UDP (ورودی و خروجی) شامل اتصال‌های موفق است که میزبان‌ها به جریان‌های UDP دریافتی پاسخ می‌دهند.

TUIDS [55]

این مجموعه‌داده توسط اساتید دانشگاه تزپور هند تولید شده و شامل سناریوهای DoS ، Probing، Scan، U2Rو DDoS در یک محیط آزمایشگاهی است. شبکهٔ تست شامل ۲۵۰ میزبان، ۱۵ سوییچ لایه ۲، هشت سوییچ لایه ۳، سه کنترلر بی‌سیم و چهار روتر در پنج شبکهٔ مختلف است. داده‌های سطح جریان فقط شامل ویژگی‌های تولیدشده توسط فرآیند جمع‌آوری جریان هستند و هیچ ویژگی اضافه‌ای ساخته نشده است.

InSDN [4]

مجموعه‌دادهٔ InSDN برای ارزیابی واقع‌گرایانهٔ سامانه‌های تشخیص نفوذ طراحی شده است. این مجموعه شامل انواع حملات به‌روز، از جمله DoS، DDoS، brute force، بدافزار، probe، exploitو حملات وب است. همچنین ترافیک معمول برنامه‌هایHTTPS ، HTTP، DNS، ایمیل، FTPو SSH را دارد. این مجموعه ترکیبی از حملات داخلی و خارجی در SDN است و برای استخراج بیش از ۸۰ ویژگی آماری از CICFlowMeterاستفاده می‌کند. در مجموع 343,939 رکورد از ترافیک نرمال و مخرب دارد که آن را مشابه شرایط واقعی می‌کند.

UNB ISCX [20]

این مجموعه‌داده در مؤسسه امنیت سایبری کانادا تولید شده است. این مجموعه از پروفایل‌ها برای تعریف تکنیک‌های حمله و توزیع ترافیک استفاده می‌کند. تِرِیس‌های واقعی برای ایجاد پروفایل‌های دقیق و ارزیابی سامانه‌های تشخیص نفوذ تحلیل شده‌اند. داده‌ها با استفاده از یک بستر آزمایشی واقعی و حملات چندمرحله‌ای گردآوری شده‌اند. دو پروفایل α (بر اساس حملات مشخص) و β (بر اساس ترافیک فیلترشده) برای تولید ترافیک بلادرنگ در پروتکل‌هایی مانندHTTP ، SMTP، SSH، IMAP، POP3و FTP استفاده شده‌اند. سناریوهای مختلف حملات چندمرحله‌ای نیز برای تولید ترافیک مخرب گنجانده شده است.

UNSW-NB15 [33]

این مجموعه‌داده در UNSW کانبرا با استفاده از IXIA PerfectStorm تولید شده است و ترکیبی از ترافیک عادی و مخرب است. نتیجهٔ آن یک مجموعه‌دادهٔ ۱۰۰ گیگابایتی در قالب فایل‌های PCAP است که شامل ۴۹ ویژگی جدید و مجموعاً 2,540,044 رکورد در چهار فایل CSV است. این مجموعه‌داده برای تولید و اعتبارسنجی سیستم‌های تشخیص نفوذ طراحی شده و در یک محیط مصنوعی شبیه‌سازی حملات ایجاد شده است.

Bot-IoT [12]

این مجموعه‌داده ترکیبی از ترافیک معمول IoT و شبکه و همچنین انواع مختلف ترافیک مخرب است که معمولاً توسط بات‌نت‌ها استفاده می‌شود. این مجموعه در یک بستر آزمایشی واقعی ایجاد شده و شامل ویژگی‌های برچسب‌گذاری‌شده برای جریان‌های حمله، دسته‌بندی حملات و زیردسته‌های آنها برای طبقه‌بندی چندکلاسه است. ویژگی‌های اضافی برای افزایش قدرت پیش‌بینی طبقه‌بندها ایجاد شده‌اند. با تحلیل آماری، یک زیرمجموعه شامل ۱۰ ویژگی برتر نیز استخراج شده است. این مجموعه‌داده که در سال ۲۰۱۸ ساخته شده، شامل ۴۶ ویژگی و شش نوع حمله است: اسکن سرویس، اثرانگاری سیستم‌عامل، DoS، DDoS، کی‌لاگر و سرقت داده. با این حال، مجموعه‌داده نامتوازن است؛ برای مثال تنها 118 رکورد سرقت داده و 1469 رکورد کی‌لاگر دارد — مقادیری که برای بسیاری از الگوریتم‌های یادگیری ماشین کافی نیستند. نقطه قوت مهم این مجموعه‌داده حضور ترافیک IoT است که در بیشتر مجموعه‌داده‌های تشخیص نفوذ وجود ندارد. با وجود غنای ویژگی‌ها، تعداد نمونه‌ها برای برخی حملات و ترافیک عادی کم است.

CICIDS2017 [5]

مجموعه‌دادهٔ CICIDS2017 شامل رفتارهای سالم (benign) و جزئیات انواع بدافزارها و حملات نوظهور مانندBrute Force FTP ، Brute Force SSH، DoS، Heartbleed، Web Attack، Infiltration، Botnetو DDoS است .(Sharafaldin et al. 2018) این مجموعه‌داده با دقت بالا و بر اساس برچسب‌هایی مانند زمان، آدرس‌های IP مبدأ و مقصد، پورت‌های مبدأ و مقصد، پروتکل‌ها و نوع حمله مشخص‌سازی شده است. برای تولید این مجموعه‌داده، یک توپولوژی شبکه جامع شامل مودم‌ها، فایروال‌ها، سوئیچ‌ها، روترها و گره‌هایی با سیستم‌عامل‌های مختلف (Windows 10، Windows 8، Windows 7، Windows XP، macOSو لینوکس (ایجاد شد. در مجموع، این مجموعه‌داده شامل 80 ویژگی جریان شبکه (network flow) استخراج‌شده از ترافیک ثبت‌شده است.

CICDDoS2019 [16]

مجموعه‌دادهٔ CICDDoS2019 به‌طور عمومی در دسترس پژوهشگران و متخصصان امنیت قرار دارد تا بتوانند سیستم‌های تشخیص نفوذ (IDS) را در برابر تهدیدات در حال تکامل DDoS ارزیابی کنند. این مجموعه‌داده شامل جدیدترین و رایج‌ترین انواع حملات DDoS همراه با ترافیک سالم است تا شرایط شبکهٔ واقعی را شبیه‌سازی کند. برای ایجاد مجموعه‌ای غنی از ویژگی‌ها، CICFlowMeterبرای استخراج بیش از 80 ویژگی آماری از ترافیک شبکه استفاده شده است. این مجموعه‌داده دارای بیش از 343,939رکورد از ترافیک عادی و مخرب است و امکان آموزش جامع مدل‌های IDS را فراهم می‌کند.

IoT-23 [35]

مجموعه‌دادهٔ IoT-23 برای پژوهشگران امنیت سایبری که روی حفاظت از اینترنت اشیا کار می‌کنند بسیار ارزشمند است. این مجموعه‌داده به‌طور عمیق روی بدافزارهای مرتبط با دستگاه‌های IoT تمرکز دارد IoT-23. مجموعه‌ای از ترافیک واقعی دستگاه‌های آلوده و سالم را ارائه می‌دهد و امکان توسعهٔ الگوریتم‌های یادگیری ماشین برای تشخیص فعالیت‌های مخرب را فراهم می‌کند. در این مجموعه‌داده 20 نمونهٔ مختلف بدافزار وجود دارد و داده‌ها با دقت بالا برچسب‌گذاری شده‌اند که کار آموزش مدل‌ها را ساده می‌کند. این مجموعه‌داده رایگان و قابل دسترس است.

ToN-IoT [31]

مجموعه‌دادهٔ ToN-IoT که در آزمایشگاه‌های IoT دانشگاه UNSW کانبرا تولید شده، دیدگاهی جامع دربارهٔ امنیت IIoT ارائه می‌دهد. این مجموعه شامل داده‌های متنوع (heterogeneous data) مانند: داده‌های تله‌متری دستگاه‌های متصل،لاگ‌های سیستم‌های لینوکس و ویندوز،و ترافیک شبکه. این مجموعه‌داده در قالب CSV ارائه شده و شامل برچسب‌های نرمال و حمله است. حتی نوع حمله نیز مشخص شده و شامل مواردی مانند باج‌افزار، حملاتbrute-force ، اسکن‌ها، انواعDoS ، تزریق داده، بک‌دور، XSSو MITM است. این داده‌ها امکان توسعهٔ مدل‌های مبتنی بر هوش مصنوعی برای حفاظت از محیط‌های IIoT را فراهم می‌کند.

SDN Dataset [8]

این مجموعه‌داده شامل دو بخش است که هر کدام یک نوع شبکه IoT را مدل‌سازی می‌کنند: شبکهٔ ایستا (Static) با 27.9 میلیون رکوردوشبکهٔ پویا (Dynamic) با 30.2 میلیون رکورد هر دو شامل حملات سایبری و ترافیک سالم بوده و 33 ویژگی دارند. پنج نوع حمله در این مجموعه وجود داردDoS :، DDoS، اسکن پورت، OS fingerprintingو.fuzzing شبکه با Mininet شبیه‌سازی و با کنترلر ONOS مدیریت شد. شبکه ایستا شامل 5 دستگاه IoT و شبکه پویا شامل 10 دستگاه بود که برخی در طول ضبط داده خاموش می‌شدند تا سناریوهای مختلف شبکه شبیه‌سازی شود. استفاده از مجموعه‌داده‌های باز امکان بازتولید مدل‌ها و دستیابی به نتایج سازگار در مطالعات مختلف را فراهم می‌کند. این کار شفافیت را افزایش داده و پیشبرد تحقیقات را تسهیل می‌کند .جدول 8 مروری بر مجموعه‌داده‌های باز قابل‌دسترسی ارائه می‌دهد که به‌عنوان پایه‌های اساسی پژوهش در زمینهٔ تشخیص و کاهش حملات عمل می‌کنند.

۴ .راهکارهای کاهش و شناسایی حملات توزیع‌شده منع سرویس(DDoS)

حملات DDoS همچنان چالش‌های قابل‌توجهی برای شبکه‌هایی که با SDN پیاده‌سازی شده‌اند ایجاد می‌کنند. پژوهشگران پیشرفت‌های مهمی در توسعهٔ روش‌های مختلف برای کاهش و شناسایی این حملات داشته‌اند. اطلاعات ارائه‌شده در این بخش مروری بر پژوهش‌های اخیر دارد که بر راهکارهای مؤثر در کاهش و تشخیص حملات تمرکز می‌کنند. شایان ذکر است که این تکنیک‌ها به‌طور مداوم در حال تحول‌اند، زیرا حملات DDoSروزبه‌روز پیچیده‌تر می‌شوند.

جدول ۸: مرور کلی مجموعه‌داده‌های باز

مجموعه‌داده	مقالهٔ پژوهشی استفاده‌کننده از مجموعه‌داده
Dataset	Research paper using dataset
DARPA 98 [46]	As mentioned in [9]
DARPA 99 [47]	[45]
DARPA 2000 [50]	[45]
DARPA 2009 [51]	[49]
KDD99 [40]	[4] and [39]
NSL-KDD [27]	[4, 32, 37] and [38]
DEFCON-8 [52]	As mentioned in [9]
UNIBS [53]	As mentioned in [9]
CAIDA DDoS 2007 [48]	[45]
LBNL [54]	As mentioned in [9]
TUIDS [55]	As mentioned in [9]
InSDN [4]	[4] and [3]
UNB ISCX [20]	[19] and [24]
UNSW-NB15 [33]	[32]
Bot-Iot [12]	[9] and [13]
CICIDS2017 [5]	[4] and [3]
CICDDoS 2019 [16]	[15]
IoT-23 [35]	[34]
ToN-IoT [31]	[30]
SDN Dataset [8]	[1]

۴,۱ شبکه‌های اینترنت اشیا مدیریت‌شده باSDN

ساریکا و همکاران 1 :راهبرد آن‌ها بر استخراج خودکار ویژگی‌های جریان و طبقه‌بندی دقیق جریان‌های شبکه با استفاده از دسته‌بند جنگل تصادفی در لایهٔ کاربرد SDN استوار است. این روش به آن‌ها اجازه داد طیف گسترده‌ای از حملات را شناسایی کرده و اقدامات اصلاحی را با ایجاد قوانین جدید جریان با اولویت بالا در لایهٔ داده آغاز کنند.

۴,۲ شناسایی و کاهش حملات DoS و DDoS با استفاده ازSDN

گالیانو-براخونس و همکاران 13 :

سه سناریو ارائه شد: سناریوی اول میزان مصرف پهنای باند در طول حملهٔ DoS و روند کاهش آن را همراه با مقدار آنتروپی اندازه‌گیری می‌کند. این سناریو از کنترلر Ryu و Mininet استفاده می‌کند. دو سناریوی بعدی از مجموعه‌دادهٔ Bot-IoT برای ارزیابی تشخیص و کاهش حملات DoS در یک محیط IoT استفاده می‌کنند. سناریوی نهایی بر تشخیص و کاهش حملات DDoS در محیط IoT تمرکز دارد.

وانگ و همکاران 3 :پژوهشگران یک روش رهگیری منبع حمله برای شبکه‌های SDN با استفاده از ده ویژگی جهت ردیابی منبع حمله توسعه دادند و مدل ترکیبی یادگیری عمیق CNN-ELM (شبکهٔ عصبی پیچشی و ماشین یادگیری شدید) را معرفی کردند.

شارما و همکاران 19 :پژوهشگران یک سیستم حمله و پاسخ به نام OpCloudSec طراحی کردند که برای ساخت مدل جلوگیری از حمله از شبکه باور عمیق استفاده می‌کند.

سالم و همکاران 14 :پژوهشگران یک رویکرد دو مرحله‌ای مبتنی بر الگوریتم‌ها برای شناسایی اولیهٔ حملات DDoS ارائه دادند. این رویکرد به هر کاربر در سیستم یک مقدار اعتماد اختصاص می‌دهد و درخواست‌های تعاملی آن‌ها با کنترلر را ثبت می‌کند.

دی آسیس و همکاران 15 :پژوهشگران یک سیستم دفاعی بررسی ترافیک با بازه‌های یک‌ثانیه‌ای برای شبکه‌های SDN معرفی کردند که قادر به شناسایی و کاهش حملات DDoS بر روی کنترلر و یک سرور خارجی است. آن‌ها ماژول کاهش را توضیح دادند و یک مثال عملی مبتنی بر نظریه بازی ارائه کردند.

وانی [18]: پژوهشگران مکانیزم امنیتی SDIoT-DDoS-DA را برای شناسایی و کاهش حملات DDoS در شبکه‌های SDN پیشنهاد کردند.

۴,۳ تکنیک‌های شناسایی و کاهش حملات DDoS با استفاده از یادگیری عمیق و یادگیری ماشین

راوی و همکاران 24 :پژوهشگران رویکرد جدیدی به نام LEDEM را برای شناسایی حملات DDoS با استفاده از الگوریتم یادگیری ماشین نیمه‌نظارتی معرفی کردند.

۴,۴ سامانه‌های تشخیص نفوذ (IDS) با استفاده از الگوریتمXGBoost

گاد و همکاران 30 :پژوهشگران یک IDS برای VANET با استفاده از مجموعه‌دادهٔ ToN-IoT توسعه دادند و با به‌کارگیری روش انتخاب ویژگی کای‌دو(Chi-2) ، تعداد ویژگی‌ها را از ۱۰۸ به ۲۰ کاهش داده و کارایی مدل را بهبود بخشیدند.

حنیف و همکاران] 32 :[پژوهشگران یک IDS برای شناسایی سریع حملات و تصمیم‌گیری فوری طراحی کردند. این سیستم در یک کنترلر IoT ادغام شد تا داده‌های ورودی را ارزیابی کرده و داده‌های مخرب را بلافاصله حذف کند.

۴,۵ رویکردهای هوش مصنوعی و یادگیری ماشین درSDN

ساهو و همکاران 37 :پژوهشگران روشی برای شناسایی و کاهش حملات DDoS با استفاده از یک مدل یادگیری ماشین ترکیبی شاملSVM ، KPCA و GA طراحی کردند.

۴,۶ حملات در شبکه‌های خودرویی با استفاده از SDN و موارد دیگر

یو و همکاران 45 :پژوهشگران یک پلتفرم برای شناسایی و مقابله با حملات DDoS در شبکه‌های خودرویی مبتنی بر SDN ایجاد کردند که از یک تکنیک تشخیص جدول جریان استفاده می‌کند.

مایتی و همکاران 49 :پژوهشگران یک سیستم تشخیص DDoS مبتنی بر مدل احتمالاتی ارائه کردند که به‌جای سرعت ترافیک، از توزیع پرچم‌های TCPدر کنترلر برای کاهش نرخ منفی کاذب بهره می‌برد. پژوهشگران تاکنون روش‌های متنوعی برای شناسایی و کاهش حملات ارائه کرده‌اند و از طیف گسترده‌ای از مدل‌های یادگیری ماشین یا ترکیب چند مدل برای افزایش دقت استفاده کرده‌اند. بخش زیر نیز چارچوب‌هایی برای شناسایی و کاهش حملات ارائه می‌کند. تمرکز اصلی این چارچوب‌ها بر حوزهٔ شناسایی و کاهش حملات DDoS است.

۴,۷ تکنیک‌های شناسایی و کاهش حملات DDoS با استفاده از یادگیری عمیق و یادگیری ماشین

یئوم و همکاران 23 :پژوهشگران یک چارچوب شناسایی DDoS مبتنی بر LSTM ارائه کردند که از سمت منبع عمل کرده و با استفاده از آستانه‌های تطبیقی مبتنی بر LSTM برای هر شبکه در سمت منبع، مشکلات عملکردی ناشی از رفتار نامنظم ترافیک را کاهش می‌دهد.

۴,۸ شناسایی و کاهش حملات DoS و DDoS با استفاده ازSDN

باوانی و همکاران 6 :پژوهشگران ProDefence را ایجاد کردند؛ یک چارچوب ماژولار برای شناسایی و مقابله با حملات DDoS در شبکه هوشمند مقیاس‌بالای مبتنی بر .SDN این چارچوب شامل اجزایی مانند جمع‌آوری‌کننده جریان ترافیک، موتور سیاست‌گذاری، تشخیص‌دهنده حمله، و موتور کاهش حمله است.

۴,۹ رویکردهای هوش مصنوعی و یادگیری ماشین درSDN

ژو و همکاران 36 :پژوهشگران یک چارچوب برای تولید، استقرار و تنظیم خودکار اقدامات دفاعی پیش‌دستانه در IoT طراحی کردند. این چارچوب بر تکنیک‌های MTD و فریب سایبری تکیه دارد تا مهاجمان را سردرگم کرده و اختلالات را به حداقل برساند.

تان و همکاران 38 :برای تشخیص DDoS از یک مکانیزم محرک (trigger) در لایهٔ داده همراه با الگوریتم یادگیری ماشین مبتنی بر کنترلر و استفاده از KNN و K-Means برای شناسایی جریان‌های مشکوک بهره گرفته شد.

رواتی و همکاران 39 :پژوهشگران چارچوبی مبتنی بر DSM-SVM برای پیش‌بینی و مقابله با حملات DDoS در SDN ایجاد کردند.

۴,۱۰ شبکه‌های اینترنت اشیا مدیریت‌شده باSDN

بهایو و همکاران 10 :پژوهشگران یک چارچوب تشخیص حمله DDoS با استفاده از C-DAD تشخیص حمله DDoS مبتنی بر شمارنده توسعه دادند.

یین و همکاران 11 :پژوهشگران یک چارچوب و الگوریتم برای شناسایی و کاهش حملات DDoS در محیط SD-IoT طراحی کردند. این الگوریتم از شباهت کسینوسی برای مقایسهٔ بردارهای نرخ Packet-in در سوئیچ مرزی استفاده می‌کند.

5 .بحث

این مرور، به کاربردهای نوینِ تکنیک‌ها و چارچوب‌های یادگیری ماشینی در زمینهٔ حملات DDoS در SDN می‌پردازد. این مطالعه بر ماهیت پویای این حوزه تأکید کرده و اهمیت استفاده از جدیدترین پژوهش‌ها برای ایجاد معیارهای تازه و پیشبرد پیشرفت‌ها را برجسته می‌کند. با وجود تمرکز قابل توجه پژوهش‌ها بر به‌کارگیری یادگیری ماشینی در امنیتSDN ، یکی از چالش‌های اصلی، کمبود مجموعه‌داده‌های عمومی است. این مجموعه‌داده‌ها برای پیشبرد تحقیقات در این حوزه ضروری هستند [7]. مقایسه‌ها نشان می‌دهد که تعداد محدودی مجموعه‌دادهٔ باز مختص SDNشناسایی شده است. این مسئله احتمالاً به دلیل کمبود چنین مجموعه‌داده‌هایی در زمان انجام مرور بوده است. هرچند مجموعه‌داده‌های موجود شامل حملات مرتبط هستند، اما اغلب فاقد محیط‌های تست‌بد مطلوب بوده‌اند. علاوه بر این، پژوهشگران بررسی‌هایی دربارهٔ تکنیک‌های مقابله با DDoS و چالش‌های امنیتی در SDN انجام داده‌اند [41]. اگرچه برخی از مقالات بررسی‌شده قدیمی‌تر هستند، اما درک جامعی از انواع مختلف حملات DDoS در SDN ارائه می‌دهند. مرور حاضر، با معرفی تکنیک‌های اضافی در زمینهٔ تشخیص و کاهش حملات، دانش موجود را گسترش می‌دهد. بررسی ادبیات نشان می‌دهد برخی مجموعه‌داده‌های باز در مطالعهٔ [41] تحلیل نشده‌اند. دلایل مختلفی برای این موضوع وجود دارد. نخست، ممکن است این مجموعه‌داده‌ها قدیمی باشند و حملات یا پیکربندی‌های مرتبط با پژوهش‌های جدید را شامل نشوند. همچنین برخی مجموعه‌داده‌های قدیمی ممکن است از نظر حجم برای استفاده در تکنیک‌های مدرن یادگیری ماشینی مناسب نباشند. با این وجود، درک استانداردهای گذشته همچنان ارزشمند است. با پیشرفت مداوم یادگیری ماشینی و فناوری‌هایSDN ، انتظار می‌رود مجموعه‌داده‌های به‌روزتر و مرتبط‌تری در دسترس قرار گیرند تا زمینه را برای تحقیقات دقیق‌تر و ارزیابی بهتر روش‌های تشخیص و کاهش حملات فراهم کنند. در ادامهٔ مسیر، لازم است میان بهره‌گیری از بینش‌های پژوهش‌های قدیمی و استفاده از مجموعه‌داده‌ها و روش‌های نوین، تعادلی منطقی برقرار شود تا با چشم‌انداز روبه‌تغییر حملات DDoS در محیط‌های SDN سازگار باشد.

6 .نتیجه‌گیری و کارهای آینده

در جمع‌بندی، این مقاله مروری جامع بر مجموعه‌داده‌های باز شامل حملاتDDoS ، و همچنین تکنیک‌ها و چارچوب‌های تشخیص و کاهش حملات ارائه می‌دهد. در دسترس بودن این مجموعه‌داده‌های باز برای ایجاد بستری استاندارد که پژوهشگران بتوانند در آن مشارکت کنند، حیاتی است. میزان اثربخشی و دقت پژوهش‌ها در زمینهٔ تشخیص و کاهش حملات، از طریق استفاده از این مجموعه‌داده‌های باز نشان داده می‌شود. مقاله با ارائهٔ مطالعات موردی عملی، نمونه‌های واقعی از به‌کارگیری این داده‌ها در توسعه و اعتبارسنجی تکنیک‌های مقابله را نشان می‌دهد و شکاف میان فهم نظری و کاربرد عملی را کاهش می‌دهد. همچنین، مقاله بر استفاده از مجموعه‌داده‌های SDN برای به‌کارگیری تکنیک‌ها و چارچوب‌های جدیدتر تأکید دارد. علاوه بر این، مقاله یافته‌های خود را با دو مطالعهٔ مروری دیگر که به وضعیت مجموعه‌داده‌های باز و روش‌های تشخیص و کاهش حملات می‌پردازند مقایسه کرده است. این مقایسه، دید عمیق‌تری نسبت به چشم‌انداز پژوهش‌ها فراهم می‌کند. همچنین لازم است تلاش‌هایی برای ایجاد مجموعه‌داده‌های معیار و جامع صورت گیرد؛ مجموعه‌داده‌هایی که طیف گسترده‌ای از سناریوهای حمله، توپولوژی‌های شبکه و پیکربندی‌های SDN را شامل شوند. توسعهٔ معیارهای استاندارد ارزیابی نیز به مقایسه‌پذیری و تکرارپذیری نتایج در مطالعات مختلف کمک شایانی خواهد کرد. همکاری‌های گسترده میان دانشگاه، صنعت، و نهادهای امنیت سایبری می‌تواند نقش مهمی در رفع کمبود مجموعه‌داده‌های باز ایفا کند. برای تحقیقات آینده، برنامه‌هایی جهت ایجاد یک مجموعه‌دادهٔ SDN با تمرکز ویژه بر حملات DDoS وجود دارد. این مجموعه‌داده با استفاده از یک تست‌بد SDN ایجاد و ارزیابی خواهد شد و نتایج آن با مجموعه‌داده‌های دیگرِ شامل حملات DDoS مقایسه می‌شود. این اقدام می‌تواند به پیشبرد تحقیقات در زمینهٔ SDN و افزایش کارایی روش‌های تشخیص و کاهش حملات کمک کند.

قدردانی(Acknowledgements)

این پژوهش بر مبنای کاری انجام شده است که با حمایت ONR شماره جایزه N00014-22-1-2724 :تأمین شده است. دیدگاه‌ها و نتایج مطرح‌شده در اینجا متعلق به نویسندگان است و نباید لزوماً به‌عنوان بازتاب سیاست‌ها یا تأییدهای رسمی دولت ایالات متحده، چه به‌صورت صریح و چه ضمنی، تعبیر شوند.

مشارکت نویسندگان(Author contributions)

WHمتن اصلی دست‌نوشته را تهیه کرده است و تمامی نویسندگان آن را بازبینی کرده‌اند.

JM ، SP، CC، YA، KRمشارکت‌های قابل توجهی در ایده‌پردازی یا طراحی کار؛ یا گردآوری، تحلیل، یا تفسیر داده‌ها؛ یا ایجاد نرم‌افزار جدید مورد استفاده در این پژوهش داشته‌اندWH .، YA، JM، KR، DLپیش‌نویس کار را تهیه کرده یا آن را از نظر محتوای علمی مهم، به‌طور انتقادی بازنگری کرده‌اند KR .و WH نسخهٔ نهایی برای انتشار را تأیید کرده‌اند و موافقت دارند که مسئولیت تمام جنبه‌های کار را بر عهده بگیرند تا اطمینان حاصل شود که هرگونه پرسش دربارهٔ صحت یا یکپارچگی هر بخش از کار، به‌درستی بررسی و حل‌وفصل می‌شود.

تأمین مالی(Funding) برای این مطالعه هیچ بودجه‌ای دریافت نشده است.

دسترس‌پذیری داده‌ها و مواد(Availability of data and materials)

داده‌های استفاده‌شده در این پژوهش در مخازن عمومی در دسترس هستند. اطلاعات دقیق در بخش تحلیل نتایج ارائه شده است.

بیانیه‌ها(Declarations)

منافع متعارض(Competing interests) نویسندگان اعلام می‌کنند که هیچ تضاد منافع ندارند .

دسترسی آزاد(Open Access)

این مقاله تحت مجوز *Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International*منتشر شده است. این مجوز هرگونه استفادهٔ غیرتجاری، اشتراک‌گذاری، توزیع و تکثیر در هر رسانه یا قالبی را مجاز می‌داند، به شرطی که: اعتبار مناسب به نویسندگان اصلی و منبع داده شود،پیوندی به مجوز Creative Commons ارائه شود،و اگر تغییری در محتوای دارای مجوز داده شده باشد، اعلام شود. تحت این مجوز، شما اجازه ندارید نسخه‌های اصلاح‌شدهٔ این مقاله یا بخش‌هایی از آن را منتشر یا به اشتراک بگذارید. تصاویر یا سایر مواد متعلق به اشخاص ثالث موجود در مقاله، تحت مجوز Creative Commons مقاله قرار دارند مگر اینکه در خط اعتباری (credit line)خلاف آن ذکر شده باشد. اگر بخشی از مواد موجود در مقاله تحت مجوز Creative Commons نباشد و استفادهٔ شما مجاز نباشد یا فراتر از حدود استفادهٔ قانونی قرار گیرد، لازم است مستقیماً از صاحب حق نشر اجازه بگیرید. برای مشاهدهٔ نسخهٔ این مجوز، به وب‌سایت مربوطه مراجعه کنید http://creativecommons.org/licenses/by-nc-nd/4.0/ .

منابع

.1Sarica AK, Angin P. Explainable security in SDN-based IoT networks. Sensors. 2020;20(24):7326. https://doi.org/10.3390/s20247326.

.2Stephen MS. Distributed denial of service: taxonomies of attacks, tools and countermeasures. Electrical Engineering Princeton University;

.2004

.3Wang J, Wang L. SDN-defend: a lightweight online attack detection and mitigation system for DDoS attacks in SDN. Sensors.

.8287:(21)22;2022https://doi.org/10.3390/s22218287.

.4Elsayed MS, Le-Khac N-A, Jurcut AD. InSDN: a novel SDN intrusion dataset. IEEE Access. 2020;8:165263–84. https://doi.org/10.1109/ACCESS.

.2020.3022633

.5CIC-IDS2017. University of New Brunswick est.1785. (n.d.-a). https://www.unb.ca/cic/datasets/ids-2017.html.

.6Bawany NZ, Shamsi JA, Salah K. DDoS attack detection and mitigation using SDN: methods, practices, and solutions. Arab J Sci Eng.

.41–42:425;2017

.7Gebremariam AA, Usman M, Qaraqe M. Applications of artificial intelligence and machine learning in the area of SDN and NFV: a survey.

In: 2019 16th International multi-conference on systems, signals & devices (SSD), Istanbul, Turkey; 2019, pp. 545–549. https://doi.org/10.

/1109SSD.2019.8893244.

.8Sarica AK, Angin P. A novel SDN dataset for intrusion detection in IoT networks. In: 2020 16th International conference on network and

service management (CNSM); 2020, pp. 1–5. https://doi.org/10.23919/CNSM50824.2020.9269042.

.9Koroniotis N, Moustafa N, Sitnikova E, Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network

forensic analytics: Bot-IoT Dataset; 2018.

.10Bhayo J, Hameed S, Shah SA. An efficient counter-based DDoS attack detection framework leveraging software defined IoT (SD-IoT). IEEE

Access. 2020;8:221612–31.

.11Yin D, Zhang L, Yang K. A DDoS attack detection and mitigation with software-defined Internet of Things framework. IEEE Access.

.705–6:24694;2018

.12The Bot-IOT dataset. The Bot-IoT Dataset | UNSW Research. (n.d.). https://research.unsw.edu.au/projects/bot-iot- dataset.

.13Galeano-Brajones J, Carmona-Murillo J, Valenzuela-Valdés JF, Luna-Valero F. Detection and mitigation of DoS and DDoS attacks in IoT-

based stateful SDN: an experimental approach. Sensors. 2020;20(3):816.

.14Salem FM, Youssef H, Ali I, Haggag A. A variable-trust threshold-based approach for DDoS attack mitigation in software-defined networks.

PLoS ONE. 2022;17(8):e0273681.

.15de Assis MV, Carvalho LF, Rodrigues JJ, Lloret J, Proença ML Jr. Near real-time security system applied to SDN environments in IoT networks

using convolutional neural network. Comput Electr Eng. 2020;86:106738.

.16CIC-DDoS2019. University of New Brunswick est.1785. (n.d.-a). https://www.unb.ca/cic/datasets/ddos-2019.html.

.17Kiani R, Bohlooli A. Distributed rule anomaly detection in SDN-based IoT. In: 2021 5th International conference on Internet of Things and

applications (IoT). IEEE; 2021, pp. 1–6.

.18Wani A, Revathi S. DDoS detection and alleviation in IoT using SDN (SDIoT-DDoS-DA). J Inst Eng (India) Ser B. 2020;101(2):117–28. https//:

doi.org/10.1007/s40031-020-00442-z.

.19Sharma PK, Singh S, Park JH. OpCloudSec: open cloud software-defined wireless network security for the Internet of Things. Comput

Commun. 2018;122:1–8.

.20UNB ISCX. University of New Brunswick est.1785. (n.d.-b). https://www.unb.ca/cic/datasets/ids.html.

.21Singh J, Behal S. Detection and mitigation of DDoS attacks in SDN: a comprehensive review, research challenges and future directions.

Comput Sci Rev. 2020;37:100279.

.22Singh MP, Bhandari A. New-flow based DDoS attacks in SDN: taxonomy, rationales, and research challenges. Comput Commun.

.27–154:509;2020

.23Yeom S, Choi C, Kim K. LSTM-based collaborative source-side DDoS attack detection. IEEE Access. 2022;10:44033–45.

.24Ravi N, Shalinie SM. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. IEEE Internet Things J.

.70–3559:(4)7;2020

.25Santos R, et al. Machine learning algorithms to detect DDoS attacks in SDN. Concurr Comput Pract Exp. 2020;32(16):e5402. https://doi.

org/10.1002/cpe.5402.

.26Nadeem MW et al. DDoS detection in SDN using machine learning techniques. Comput Mater Continua. 71(1) (2022). https://cdn.techs

cience.cn/ueditor/files/cmc/TSP_CMC-71-1/TSP_CMC_21669/TSP_CMC_21669.pdf.

.27NSL-KDD Dataset. University of New Brunswick est.1785. (n.d.). https://www.unb.ca/cic/datasets/nsl.html.

.28Banitalebi Dehkordi A, Soltanaghaei MR, Boroujeni FZ. The DDoS attacks detection through machine learning and statistical methods in

SDN. J Supercomput. 2021;77(3):2383–415.

.29Perez-Diaz JA, et al. A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. IEEE

Access. 2020;8:155859–72.

.30Gad AR, Nashat AA, Barkat TM. Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset.

IEEE Access. 2021;9:142206–17.

.31The Ton_IoT datasets. The TON_IoT Datasets | UNSW Research. (n.d.). https://research.unsw.edu.au/projects/toniot- datasets.

.32Hanif S, Ilyas T, Zeeshan M. Intrusion detection in IoT using artificial neural networks on UNSW-15 dataset. In: 2019 IEEE 16th international

conference on smart cities: improving quality of life using ICT & IoT and AI (HONET-ICT). IEEE; 2019, pp. 152–156.

.33The UNSW-NB15 Dataset | UNSW Research—UNSW sites. (n.d.). https://research.unsw.edu.au/projects/unsw-nb15- dataset.

.34da Cruz MA, Abbade LR, Lorenz P, Mafra SB, Rodrigues JJ. Detecting compromised IoT devices through XGBoost. IEEE Trans Intell Transp

Syst. 2022;24:15392–9.

.35IOT-23 dataset: A labeled dataset of malware and benign IOT traffic. Stratosphere IPS. (n.d.). https://www.stratosphereips.org/datas

ets-iot23.

.36Zhou Y, Cheng G, Yu S. An SDN-enabled proactive defense framework for DDoS mitigation in IoT networks. IEEE Trans Inf Forensics Secur.

.80–16:5366;2021

.37Sahoo KS, Tripathy BK, Naik K, Ramasubbareddy S, Balusamy B, Khari M, Burgos D. An evolutionary SVM model for DDoS attack detection

in software-defined networks. IEEE Access. 2020;8:132502–13.

.38Tan L, Pan Y, Wu J, Zhou J, Jiang H, Deng Y. A new framework for DDoS attack detection and defense in SDN environment. IEEE Access.

.19–8:161908;2020

.39Revathi M, Ramalingam VV, Amutha B. A machine learning based detection and mitigation of the DDOS attack by using SDN controller

framework. Wirel Pers Commun. 2021;127:2417–41.

.40KDD Cup 1999 Dataset. KDD Cup 1999 Data. (n.d.). http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

.41Fajar AP, Purboyo TW. A survey paper of distributed denial-of-service attack in software defined networking (SDN). Int J Appl Eng Res.

.82–476:(1)13;2018

.42Tan L, et al. A new framework for DDoS attack detection and defense in SDN environment. IEEE Access. 2020;8:161908–19.

.43Ali TE, Chong Y-W, Manickam S. Machine learning techniques to detect a DDoS attack in SDN: a systematic review. Appl Sci. 2023;13(5):3183.

.44Gadze JD, et al. An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers.

Technologies. 2021;9(1):14.

.45Yu Y, Guo L, Liu Y, Zheng J, Zong YUE. An efficient SDN-based DDoS attack detection and rapid response platform in vehicular networks.

IEEE Access. 2018;6:44570–9.

1998 .46DARPA Intrusion Detection Evaluation Dataset. MIT Lincoln Laboratory. (n.d.-a). https://www.ll.mit.edu/r-d/datasets/1998-darpa-

intrusion-detection-evaluation-dataset.

1999 .47DARPA Intrusion Detection Evaluation Dataset. MIT Lincoln Laboratory. (n.d.-b). https://www.ll.mit.edu/r- d/datasets/1999-darpa-

intrusion-detection-evaluation-dataset.

.48Center of applied internet data analysis. https://www.caida.org/data/

.49Maity P, Saxena S, Srivastava S, Sahoo KS, Pradhan AK, Kumar N. An effective probabilistic technique for DDoS detection in OpenFlow

controller. IEEE Syst J. 2021;16(1):1345–54.

2000 .50DARPA intrusion detection scenario specific datasets. MIT Lincoln Laboratory. (n.d.-c). https://www.ll.mit.edu/r- d/datasets/2000-

darpa-intrusion-detection-scenario-specific-datasets.

.51DARPA_2009. The ant lab: Analysis of network traffic. (n.d.). https://ant.isi.edu/datasets/readmes/DARPA_2009_DDoS_attack-2009.1105.

README.txt.

.52Defcon, “The Shmoo Group,” http://cctf.shmoo.com/, 2011.

.53UNIBS, University of Brescia Dataset (2009). http://www.ing.unibs.it/ntw/tools/traces./

.54Lawrence Berkley National Laboratory (LBNL), ICSI, LBNL/ICSI enterprise tracing project (2005). http://www.icir.org/enterprise-tracing./

.55Bhuyan MH, Bhattacharyya DK, Kalita JK. Towards generating real-life datasets for network intrusion detection. Int J Netw Secur.

.701–17:683;2015

یادداشت ناشر

اسپرینگر نیچر نسبت به ادعاهای قضایی مطرح‌شده در نقشه‌های منتشرشده و وابستگی‌های سازمانی، بی‌طرف باقی می‌ماند.