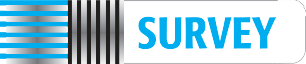


دریافت شده ۵ ژانویه ۲۰۲۴، پذیرفته شده ۲۴ ژانویه ۲۰۲۴، تاریخ از انتشار ۳۱ ژانویه ۲۰۲۴، تاریخ از فعلی نسخه ۷ فوریه ۲۰۲۴.

*دیجیتال شیء شناسه ‎۱۰.۱۱۰۹/دسترسی.۲۰۲۴.۳۳۶۰۸۶۸‎*

**

تکنیک‌های یادگیری ماشین و یادگیری عمیق برای تشخیص ناهنجاری انکار سرویس توزیع‌شده

راه‌حل‌های تحقیقاتی فعلی

نورا شفا موسی [](https://orcid.org/0000-0001-7343-4000)۱،۲ ، ندا مسعود میرزا [](https://orcid.org/0000-0002-4410-7657)۳ ، صیدا حفصه رفیق [](https://orcid.org/0000-0002-2445-3798)۱ ،

امیرا ماهات عبدالله [](https://orcid.org/0000-0001-9896-5676)۱ ، و تانگاول مورگان [](https://orcid.org/0000-0002-2510-8857)۴ ، (ارشد عضو، IEEE)

۱ دانشکده اطلاعات فناوری، یونایتد امارات متحده عربی دانشگاه، آل عین، ابو دبی، یونایتد امارات متحده عربی

۲ کالج از مهندسی، آل عین دانشگاه، آل عین، ابو دبی، یونایتد عرب امارات

۳ کالج از مهندسی، یونایتد عرب امارات دانشگاه، آل عین، ابو دبی، یونایتد عرب امارات

۴ گروه سیستم‌های اطلاعاتی و امنیت، دانشکده فناوری اطلاعات، دانشگاه امارات متحده عربی، العین، ابوظبی، امارات متحده عربی امارات

متناظر نویسنده: تانگاول موروگان [(thangavelm@uaeu.ac.ae)](mailto:(thangavelm@uaeu.ac.ae)

این کار بود پشتیبانی شده در بخشی توسط ‎‏ ... یونایتد عرب امارات دانشگاه تحت تحقیق استارتاپ پیشنهاد گرانت G00004612/12T048.

 **چکیده** این بررسی پیشرفته، چشم‌انداز انکار توزیع‌شده‌ی ... را به‌طور جامع بررسی می‌کند. خدمات (عدم سرویس توزیع‌شده) ناهنجاری تشخیص در نرم‌افزار تعریف شده شبکه‌ها (SDN) از طریق ‎‏ ... لنز از دستگاه پیشرفته یادگیری (میلی لیتر) و عمیق یادگیری (دی ال) تکنیک‌ها. کاربرد دامنه از این کار است متمرکز بر آدرس‌دهی ‎‏ ... ذاتی امنیت آسیب‌پذیری‌ها از شبکه SDN محیط‌ها و در حال توسعه یک خودکار سیستم برای تشخیص و کاهش دهنده شبکه حملات. مشکل متمرکز روی در این بررسی است ‎‏ ... نیاز برای دفاع مؤثر مکانیسم‌ها و تشخیص روش‌شناسی‌ها به آدرس اینها آسیب پذیری ها. متعارف روش‌های اندازه‌گیری شبکه در زمینه SDNها محدود هستند و تکنیک‌های پیشنهادی ML و DL با ارائه تشخیص و کاهش حملات DDoS دقیق‌تر و کارآمدتر، بر این محدودیت‌ها غلبه می‌کنند. هدف این کار، ارائه مروری جامع بر کارهای مرتبط در زمینه تشخیص ناهنجاری SDN با پیشرفت‌های اخیر است که از طریق تکنیک‌های ML و DL به دو گروه طبقه‌بندی می‌شوند. سیستم‌های پیشنهادی از تکنیک‌های متنوعی، از جمله یادگیری نظارت‌شده (SL)، یادگیری بدون نظارت (UL)، یادگیری گروهی (EL) و راه‌حل‌های DL، برای پردازش جریان‌های IP، نمایش ترافیک شبکه، و حملات را شناسایی می‌کند. خروجی شامل سیاست‌های کاهش اثرات آموخته‌شده توسط تکنیک‌های ML/DL است و سیستم‌های پیشنهادی به عنوان دروازه‌بان‌های پیچیده عمل می‌کنند و سیاست‌های کاهش اثرات خودکار را برای کاهش میزان آسیب ناشی از این حملات اعمال می‌کنند. نتایج به‌دست‌آمده از معیارهای ارزیابی، از جمله دقت، دقت، و به یاد آوردن، تایید ‎‏ ... علامت گذاری شده اثربخشی از ‎‏ ... پیشنهادی سیستم‌ها در تشخیص و کاهش مختلف انواع از حملات، از جمله توزیع‌شده انکار از خدمات (عدم سرویس توزیع‌شده) حملات. سهم بنیادی سیستم‌های پیشنهادی در اثربخشی آنها برای تشخیص و دفاع در برابر حملات DDoS آشکار است. درون ‎‏ ... شبکه SDN محیط زیست. با این حال، ‎‏ ... بررسی اذعان می‌کند قطعی ذاتی محدودیت‌ها و فشار دادن نیاز برای بیشتر اعتبارسنجی درون دنیای واقعی سناریوها به ارزیابی کردن ‎‏ ... پیشنهادی روش‌ها عملی بودن و اثربخشی. در خلاصه، این سیستماتیک بررسی پیشنهادات ارزشمند دیدگاه‌ها روی ‎‏ ... حاضر وضعیت تشخیص انسداد سرویس توزیع‌شده در شبکه‌های نرم‌افزاری تعریف‌شده با استفاده از روش‌های یادگیری ماشینی و یادگیری عمیق، برجسته کردن نقاط قوت و محدودیت‌های سیستم‌های پیشنهادی مختلف و شناسایی زمینه‌های تحقیق و توسعه آینده.

 **اصطلاحات شاخص** تشخیص ناهنجاری، یادگیری عمیق (DL)، انکار سرویس توزیع‌شده (DDoS)، یادگیری ماشین (ML)، شبکه تعریف‌شده توسط نرم‌افزار (SDN).

[](https://orcid.org/0000-0001-8691-0141) وابسته ویرایشگر هماهنگ کننده ‎‏ ... بررسی از این نسخه خطی و تایسون بروکس آن را برای انتشار تأیید کرد .

1. **مقدمه**

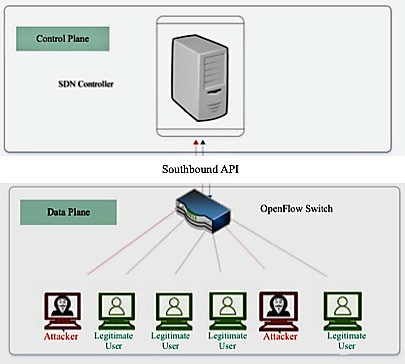
ظهور شبکه‌های نرم‌افزاری تعریف‌شده (SDN) انقلابی در فناوری اطلاعات ایجاد کرده است. ‎‏ ... راه شبکه‌ها هستند مدیریت شده و عمل شده.

۱۷۹۸۲

© ۲۰۲۴ نویسندگان. این کار است دارای مجوز تحت الف خلاق عوام انتساب مجوز ۴.۰

برای برای اطلاعات بیشتر، به https://creativecommons.org/licenses/by/4.0/ مراجعه کنید . جلد ۱۲، ۲۰۲۴

SDNها زیرساخت شبکه‌ای انعطاف‌پذیر و قابل برنامه‌ریزی ارائه می‌دهند. که قادر می‌سازد شبکه مدیران به مدیریت و کنترل ترافیک شبکه به طور کارآمدتری انجام می‌شود. با این حال، این انعطاف‌پذیری می‌آید در الف هزینه، به عنوان SDN ها هستند ذاتاً در برابر انواع مختلف حملات آسیب‌پذیر هستند؛ از جمله حملات (DDoS) (شکل را ببینید) [۱](#_bookmark2) ). کاربرد دامنه از این تحقیق است متمرکز بر پرداختن به آسیب‌پذیری‌های امنیتی ذاتی محیط‌های SDN و توسعه یک سیستم خودکار برای تشخیص و کاهش دهنده شبکه حملات [[25] .](#_bookmark41) سیستم پیشنهادی با استقرار یک ماژول تشخیص و یک ماژول کاهش، که هر دو برای یکپارچه‌سازی در کنترل‌کننده ادغام شده‌اند، عمل می‌کند. منطقی ارتباطات. سیستم بلعیدن داده‌های ترافیک شبکه به عنوان ورودی، و متعاقباً آن را در معرض یک فرآیند چند مرحله‌ای شامل تشخیص ناهنجاری و کاهش ردیابی قرار می‌دهد. نتایج به دست آمده از ‎‏ ... ارزیابی معیارها دقت تشخیص بالا و کاهش کارآمد حمله DDoS را نشان می‌دهند.



**شکل ۱.** حملات انسداد سرویس (DDOS) حمله در اس دی ان.

بیان مسئله این تحقیق، نیاز به اثربخشی است. دفاعی مکانیسم‌ها و تشخیص روش‌هایی برای رسیدگی به این آسیب‌پذیری‌ها. طبق گزارش سیسکو [[51] ،](#_bookmark67) فراوانی و شدت نقض‌های امنیت سایبری هستند روی ‎‏ ... برخاستن، علامت گذاری شده توسط الف مداوم افزایش تعداد نقض‌ها و حجم رکوردهای افشا شده در هر حادثه. علاوه بر این، پیش‌بینی حملات انکار سرویس توزیع‌شده (DDoS) نگران‌کننده است و انتظارات به دو برابر از ۷.۹ میلیون حوادث در ۲۰۱۸ به رقم سرسام‌آور ۱۵.۴ میلیون نفر تا سال ۲۰۲۳.

اهمیت از این مشکل نمی‌تواند باش اغراق‌آمیز است، زیرا حملات DDoS می‌توانند خسارات قابل توجهی به زیرساخت‌های شبکه وارد کنند و منجر به از کارافتادگی، از دست رفتن داده‌ها و آسیب به اعتبار شوند. علاوه بر این، پیچیدگی روزافزون زیرساخت‌های شبکه و مهارت روزافزون مهاجمان، تشخیص و کاهش این حملات را به طور فزاینده‌ای چالش‌برانگیز می‌کند [[25] ،](#_bookmark41) [[27] ،](#_bookmark43) [[29] .](#_bookmark45)

راه‌حل‌های پیشرفته‌ای که در این مطالعه بیان شده‌اند شامل طیف وسیعی از یادگیری نظارت‌شده (SL)، یادگیری بدون نظارت (Unsupervised Learning) و ... هستند. (UL) گروه یادگیری (ای ال) و دی ال راه حل ها.

این روش‌ها نقش محوری در تحلیل جریان‌های IP، توصیف ترافیک شبکه و تشخیص حملات بالقوه دارند. پایان نتیجه شامل می‌شود یاد گرفت کاهش استراتژی‌ها. پیش‌بینی شده سیستم‌ها تابع به عنوان پیشرفته دروازه‌بانان، با استفاده از اقدامات کاهش خودکار برای کوچک‌سازی تأثیر خسارات احتمالی ناشی از حملات DDOS را ارزیابی کنید [[1] ،](#_bookmark17) [[6] ،](#_bookmark22) [[30] .](#_bookmark46)

تحقیق است لازم به آدرس ‎‏ ... محدودیت‌ها بررسی راه‌حل‌های موجود و توسعه روش‌های مؤثرتر و کارآمدتر تشخیص و کاهش حملات DoS در SDNها. هدف سیستم‌های پیشنهادی ارائه رویکردی جامع‌تر و دقیق‌تر برای تشخیص و کاهش حملات DoS است که در نتیجه امنیت شبکه را افزایش داده و خطر از کارافتادگی و از دست رفتن داده‌ها را کاهش می‌دهد.

فراگیر مشارکت‌ها از این تحقیق هستند در ارائه یک مکانیسم دفاعی جامع متناسب با SDN، که در مقابله با حملات DDoS مهارت دارد، منعکس شده است . چشم‌انداز تحقیقات آینده ممکن است بر کاوش الگوریتم‌های یادگیری ماشین پیشرفته‌تر، در کنار ادغام سیستم پیشنهادی با سایر مکانیسم‌های امنیتی موجود برای افزایش بیشتر امنیت شبکه متمرکز باشد.

در نهایت، این تحقیق بینش‌های ارزشمندی در مورد ‎‏ ... فعلی ایالت از داس تشخیص در SDN ها با استفاده از تکنیک‌های یادگیری ماشینی و یادگیری عمیق، نقاط قوت و محدودیت‌های سیستم‌های پیشنهادی مختلف را برجسته کرده و زمینه‌های تحقیق و توسعه آینده را شناسایی می‌کند. سیستم‌های پیشنهادی اثربخشی در تشخیص و کاهش دهنده مختلف انواع از حملات، از جمله حملات انسداد سرویس (DDOS) حملات، تأکید می‌کند ‎‏ ... اهمیت توسعه روش‌های تشخیص و کاهش مؤثرتر و کارآمدتر برای حملات DoS در SDNها.

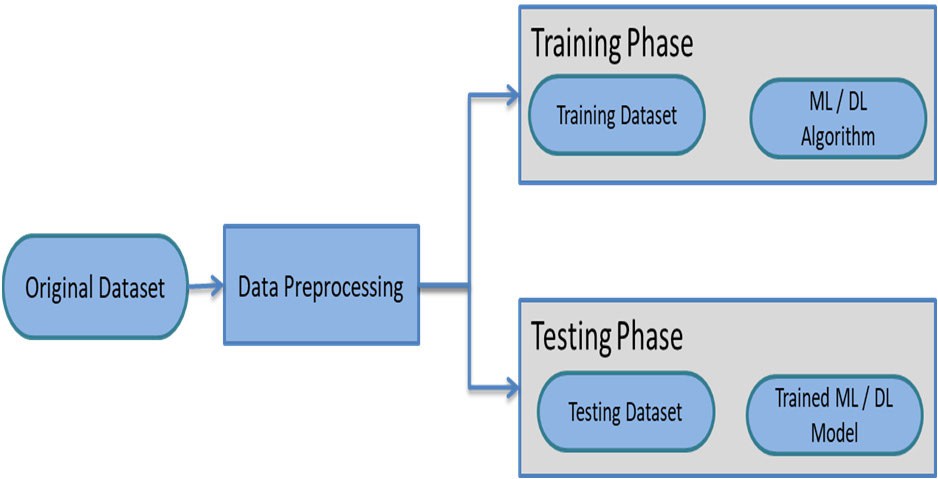
اکتشافات کلیدی را روشن خواهیم کرد و مشارکت‌ها از تحقیق در انکار از تشخیص سرویس در شبکه نرم‌افزار محور، با بررسی دقیق کاربرد یادگیری ماشین (ML) و یادگیری عمیق (دی ال) تکنیک‌ها. این تلاش جستجو می‌کند به فراهم کردن جامع​ درک کردن از این بحرانی وجه از شبکه امنیت، که بر اهمیت حیاتی این فناوری‌ها در حفاظت از شبکه‌های مدرن تأکید دارد.

1. **تحقیق روش‌شناسی**

در انجام بررسی ادبیات موضوع برای بررسی ادبیات موضوع با عنوان مروری بر تشخیص انکار سرویس در نرم‌افزار تعریف‌شده شبکه با استفاده از میلی لیتر و دی ال تکنیک‌ها، الف از روش تحقیق سیستماتیک و جامع استفاده شد. تحقیق مقالات انتخاب فرآیند هدف قرار داده شده به شناسایی، فیلتر و تحلیل کردن مقالات مربوط به ‎‏ ... مشخص شده کلمات کلیدی و مضامین (شکل [2 را ببینید](#_bookmark9) ).

* 1. *تحقیق مقالات انتخاب فرآیند*

مرحله اولیه شامل جستجوی پایگاه داده با استفاده از کلید- کلماتی مانند «انکار سرویس توزیع‌شده»، «DDoS»، «تشخیص ناهنجاری»، «شبکه تعریف‌شده توسط نرم‌افزار» و «SDN» منجر به شناسایی ۱۱۳۰ مقاله بالقوه مرتبط شد. متعاقباً، مقالاتی که قبل از سال ۲۰۲۰ منتشر شده‌اند (221) بودند مستثنی شده، باریک شدن ‎‏ ... تمرکز به ۹۰۹ مقالات منتشر شده از ژانویه ۲۰۲۰ تا دسامبر ۲۰۲۳.



**شکل ۲.** روش‌شناسی عمومی تشخیص ناهنجاری DDoS در SDN با استفاده از ام ال/دی ال.

به پالایش ‎‏ ... انتخاب در ادامه، غیر ماشینی یادگیری و غیر عمیق یادگیری مقالات (622) بودند مستثنی شده، ترک ۲۸۷ مقالات درون ‎‏ ... دامنه از مصنوعی هوش (هوش مصنوعی). الف دقیق عنوان/چکیده نقد و بررسی فرآیند رهبری کرد به محرومیت از ۱۷۵ مقالات، و ‎‏ ... باقی مانده ۱۱۲ مقالات تایید شدند به باش منتشر شده در داوری‌شده توسط همتا کنفرانس‌ها و

مجلات

سپس مقالات مروری و پیمایشی (82) حذف شدند و در نتیجه مجموعه‌ای از 30 مقاله کاملاً بررسی شده باقی ماند. علاوه بر این ، ۲۰ مقالات بودند شامل از طریق بازگشتی جستجوهای مرجع . نهایی انتخاب برای عمیق تحلیل شامل ۵۰ مقاله بود (شکل [۳ را ببینید](#_bookmark10) ).

* 1. *آمار و طبقه‌بندی از نظرسنجی*

انتخاب شده مقالات بودند دسته‌بندی‌شده به دو اصلی مباحث: انکار از خدمات تشخیص در نرم‌افزار تعریف شده شبکه با استفاده از دستگاه تکنیک‌های یادگیری (۲۵ مقاله) و انکار​ خدمات تشخیص در نرم‌افزار تعریف شده شبکه با استفاده از دیپ یادگیری تکنیک‌ها (25 مقالات)، جمع کل ۵۰ مقالات. توزیع از انتخاب شده مقالات به ازای هر سال آشکار شد یک تمرکز روی اخیر تحقیق، با ۲۴ مقالات از ۲۰۲۳، ۱۱ از سال ۲۰۲۲ و ۷ مورد از سال ۲۰۲۱. خلاصه‌ای از ناشر نشان می‌دهد که IEEE، ام دی پی آی، الزویر، وایلی، تیلور و فرانسیس، اسپرینگر، و هنداوی مشارکت به ‎‏ ... انتخاب شده مقالات،

جمع کل ۵۰. (یا: ۵۰.)

این سخت‌گیرانه روش‌شناسی تضمین می‌کند ‎‏ ... ادبیات عمق، ارتباط و پایبندی این بررسی به تمرکز ویژه بر تشخیص انکار سرویس در شبکه‌های نرم‌افزار محور با استفاده از تکنیک‌های یادگیری ماشین و یادگیری عمیق (شکل را ببینید) [۴](#_bookmark13) ). اختصارات در این کاغذ هستند سازمان یافته و در (جدول [1](#_bookmark11) ) ارائه شده است.

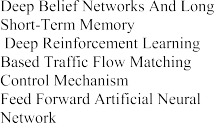
1. **I. تشخیص ناهنجاری شبکه با استفاده از یادگیری ماشین تکنیک‌ها**

شبکه‌های مدرن هستند و نیازمند رویکردهای نوآورانه برای پاسخگویی به موقع و دقیق می‌باشند. تشخیص. بخش کاوش می‌کند به الف انبوه از الگوریتم‌های یادگیری ماشین که اثبات شده کارایی به عنوان الف نوشدارو در این توجه (ببینید) شکل [۵](#_bookmark14) )، همراه با الف خلاصه میز هدف گیری به ارائه یک جامع نمای کلی از ‎‏ ... فعلی روندها در این دامنه (به جدول [2 مراجعه کنید](#_bookmark12) ).

**شکل ۳.** خلاصه از تحقیق روش‌شناسی.

لیو و ال. [[1]](#_bookmark17) کاوش می‌کند به ‎‏ ... قلمرو از تشخیص حملات انکار سرویس توزیع‌شده (DDoS) در شبکه‌های نرم‌افزاری تعریف‌شده (SDN) از طریق کاربرد تکنیک‌های یادگیری ماشین (ML). افزایش وابستگی به فناوری SDN و تهدید رو به رشد حملات DDoS، زمینه‌ساز مسئله تحقیقاتی مورد نظر است. پرداختن به عدم کفایت از سنتی شبکه مدل‌ها در جلسه امنیت خواسته‌ها از SDN ها و ساختمان بر زودتر مبتنی بر مهندسی ویژگی روش‌ها برای حملات انسداد سرویس (DDOS) تشخیص در SDN ها، این مطالعه به دنبال راه‌حل‌های مؤثر برای مسئله تحقیقاتی شناسایی‌شده است. اهداف این مطالعه شامل انجام مهندسی ویژگی روی مجموعه داده‌ها برای استخراج ویژگی بهینه است. زیرمجموعه، آموزش و آزمایش متنوع میلی لیتر طبقه‌بندی‌کننده‌ها با این زیرمجموعه، و استقرار طبقه‌بندی‌کننده بهینه در کنترل‌کننده SDN برای حملات انسداد سرویس (DDOS) تشخیص. مشارکت‌ها دروغ در ارائه یک رویکرد اصلاح‌شده که با تحقیقات موجود اعتبارسنجی شده است. با استفاده از مجموعه داده CSE-CIC-IDS2018 [[51] ،](#_bookmark67) سیستم پیشنهادی درگیر مهندسی ویژگی می‌شود، الگوریتم‌های طبقه‌بندی یادگیری ماشین را اعمال می‌کند و در کنترل‌کننده SDN مستقر می‌شود و یک زیرمجموعه ویژگی و طبقه‌بندی‌کننده بهینه ارائه می‌دهد. برای حملات انسداد سرویس (DDOS) تشخیص. آزمایش‌ها بودند انجام شده، نتایج تحلیل شده، و مقایسه‌ها ساخته شده با مشابه کار می‌کند،

**جدول ۱.** فهرست از اختصارات





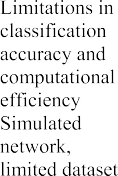
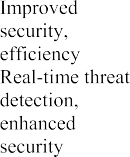
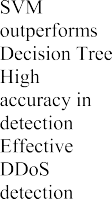
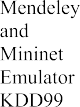
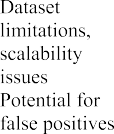
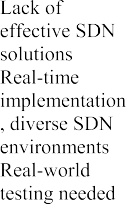
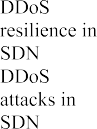


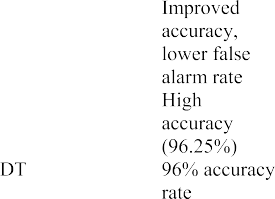
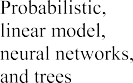
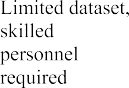
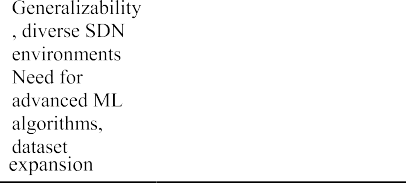


با استفاده از معیارهایی مانند دقت، صحت، فراخوانی، امتیاز F1 و مقادیر AUC. تأکید بر معیارهای امنیتی مربوط به مبتنی بر یادگیری ماشینی حملات انسداد سرویس (DDOS) حمله تشخیص در SDN ها. مطالعه نشان داده شده برتر عملکرد معیارها، از جمله دقت، صحت، فراخوانی، امتیاز F1 و مقادیر AUC، که اثربخشی روش پیشنهادی را در تشخیص DDoS در SDNها نشان می‌دهد. دستاوردهای این مطالعه شامل تدوین یک روش موثر تشخیص DDoS در SDNها است که از طریق مهندسی ویژگی و یادگیری ماشین حاصل می‌شود. این رویکرد جدید، دیدگاه و راه‌حل جدیدی را برای SDN ارائه می‌دهد. امنیت. آینده تلاش ها ممکن است شامل کردن یکپارچه‌سازی روش پیشنهادی را با سایر فناوری‌های امنیت شبکه برای یک راه‌حل جامع مقایسه کنید. علاوه بر این، تحقیقات می‌تواند بررسی کند روش‌ها به افزایش ‎‏ ... روش‌ها استحکام در برابر خصومت حملات. مطالعه محدودیت‌ها شامل شدن الف تمرکز محدود بر تشخیص DDoS در SDNها، که به طور بالقوه جنبه‌های امنیتی گسترده‌تر شبکه را نادیده می‌گیرد. یافته‌ها همچنین ممکن است توسط مجموعه داده‌های خاص و تنظیمات آزمایشی به کار رفته محدود شوند .

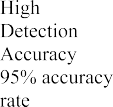
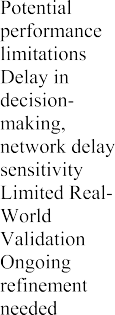
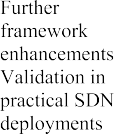
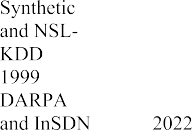
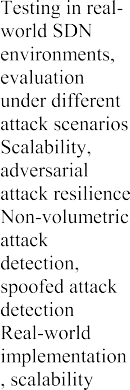
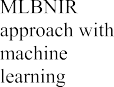
حماد و همکاران [[2]](#_bookmark18) یک استراتژی جدید برای تقویت بازیابی نفوذ شبکه در SDN از طریق ادغام یادگیری ماشین معرفی می‌کند. زمینه تحقیق شامل امنیت شبکه است، به طور خاص بر تشخیص حملات DDoS در SDN با استفاده از الگوریتم‌های یادگیری ماشین تمرکز دارد. آدرس‌دهی ‎‏ ... سریع بهبودی از شبکه نفوذهای جریان در تنظیمات شبکه معاصر، به ویژه در داخل ‎‏ ... SDN چارچوب، باقی مانده است الف چالش به دلیل به پیچیده طبیعت و رشد از شبکه ترافیک. فعلی

راه حل ها هستند مقید توسط اینها پیچیدگی‌ها هدف تحقیق است به به طور مؤثر مقابله این چالش توسط پیشنهاد دادن نوآورانه روش که به صورت پویا انتخاب می‌کند پشتیبان گیری مسیرهایی مبتنی بر الگوهای ترافیکی در حال تکامل و با استفاده از یادگیری ماشینی الگوریتم‌ها برای حملات انسداد سرویس (DDOS) حمله تشخیص. سیستم پیشنهادی فرآیندها شبکه ترافیک داده‌ها با دستگاه الگوریتم‌های یادگیری برای تشخیص حمله DDoS. با استفاده از یک رویکرد جدید به نام MLBNIR، این سیستم به صورت استراتژیک مسیرهای پشتیبان را بر اساس الگوهای ترافیکی انتخاب می‌کند و از الگوریتم‌های یادگیری ماشین برای تشخیص DDoS استفاده می‌کند. این سیستم ... تولید می‌کند. الف جامع گزارش جزئیات ‎‏ ... نوع و شدت از شناسایی شده حملات. تجربی راه اندازی استفاده می‌کند ‎‏ ... مجموعه داده InSDN، شامل کردن واقعی SDN محیط زیست شبکه داده‌های ترافیک. معیارهای عملکرد شامل دقت، صحت، فراخوانی و امتیاز F1 می‌شوند، در حالی که معیارهای امنیتی شامل نرخ مثبت کاذب، نرخ منفی کاذب و نرخ تشخیص هستند. نتایج نشان می‌دهند ‎‏ ... سیستم برتری بیش از موجود راه‌حل‌هایی در زمینه دقت، صحت، فراخوانی و امتیاز F1، همراه با دستیابی به کم نادرست مثبت و نادرست منفی نرخ‌ها، همراه با نرخ تشخیص بالا. سیستم پیشنهادی به نرخ تشخیص حمله DDoS چشمگیر ۹۸.۵٪ دست می‌یابد، همراه با توسط الف کم نادرست مثبت نرخ از ۰.۵٪ و الف حداقل نرخ منفی کاذب ۱٪. ارزیابی از طریق ماتریس درهم‌ریختگی، دقت سیستم را برجسته می‌کند و به درستی شناسایی می‌کند. ۱۹۷ حمله از ۲۰۰ حمله DDoS. این تحقیق رویکرد جدید MLBNIR را معرفی می‌کند و از الگوریتم‌های یادگیری ماشین برای تشخیص حمله DDoS در SDN استفاده می‌کند و از روش‌های موجود پیشی می‌گیرد. راه حل ها در کلید عملکرد معیارها آینده کار

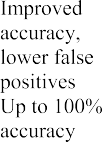
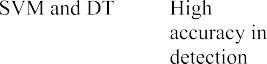




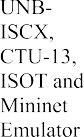
**جدول ۲.** قبلی تحقیق خلاصه از دستگاه یادگیری راه حل ها

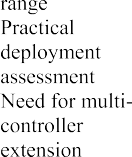
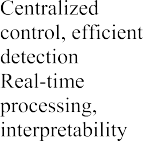




**جدول ۲.** *(ادامه دارد.)* قبلی تحقیق خلاصه از دستگاه یادگیری راه حل ها





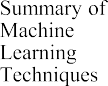
شامل می‌شود دنیای واقعی آزمایش و عملکرد ارزیابی تحت شرایط متنوع حمله سناریوها محدودیت‌ها شامل شدن اتکا روی یک مجموعه داده منفرد و با فرض توپولوژی شبکه استاتیک.

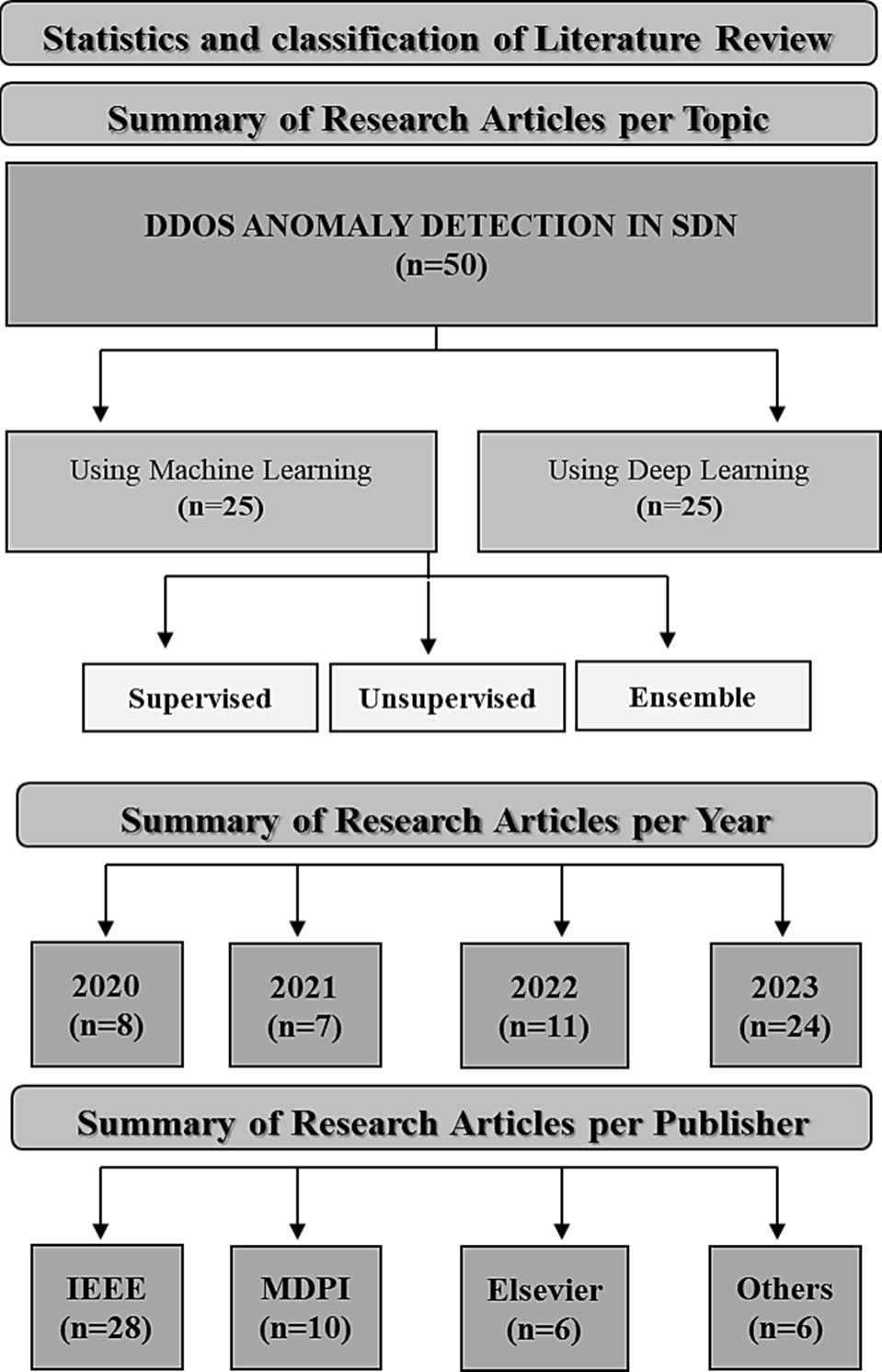


رامپراسات و همکارانش [[3]](#_bookmark19) حوزه مقابله با حملات DDoS در SDN را از طریق به‌کارگیری تکنیک‌های یادگیری ماشین بررسی می‌کنند [.](#_bookmark19) پیشنهادی سیستم تلاش ها به با بررسی دقیق ترافیک شبکه و با استفاده از الگوریتم‌های یادگیری ماشین برای شناسایی الگوهای مخرب، حملات DDoS را شناسایی و خنثی کنید. این مقاله اثربخشی سیستم پیشنهادی را از طریق نتایج تجربی که مهارت آن را در تشخیص و کاهش DDoS نشان می‌دهد، اثبات می‌کند. پرداختن به افزایش فرکانس و شدت حملات DDoS در شبکه‌های SDN، نقطه کانونی این مقاله را تشکیل می‌دهد. راه‌حل‌های موجود، از اقدامات امنیتی شبکه سنتی گرفته تا اقدامات امنیتی معاصر رویکردها مانند مبتنی بر SDN ترافیک مهندسی و تشخیص DDoS مبتنی بر یادگیری ماشین، محدودیت‌هایی در مورد دقت، مقیاس‌پذیری و سازگاری با حملات نوظهور نشان می‌دهند. الگوها تحقیق عینی اهداف به معرفی یک سیستم پیشگام برای تشخیص و کاهش حملات DDoS در SDN با استفاده از تکنیک‌های یادگیری ماشین. مقالات شامل شرح مفصلی از سیستم پیشنهادی، ارزیابی تجربی عملکرد آن و بحثی در مورد محدودیت‌ها و راه‌های بالقوه برای تحقیقات آینده است. سیستم پیشنهادی با بررسی دقیق ترافیک شبکه با الگوریتم‌های یادگیری ماشین عمل می‌کند. نکته سنج الگوها نشانگر از بدخواه ترافیک مرتبط با حملات DDoS. داده‌های ورودی، که از سوئیچ‌های SDN گرفته شده‌اند، تحت پیش‌پردازش قرار می‌گیرند تا ویژگی‌های مربوطه استخراج شوند. مانند بسته اندازه، منبع و مقصد آی پی آدرس‌ها، و پروتکل نوع. میلی لیتر مدل‌ها چنین به عنوان ماشین بردار پشتیبان و آر اف

سپس از طبقه‌بندی‌کننده‌ها برای تمایز ترافیک عادی از مخرب استفاده می‌شود. سیستم، قوانینی را برای مسدود کردن یا هدایت ترافیک مخرب ارائه می‌دهد. شبیه‌سازی حملات DDoS بر روی یک شبکه SDN شامل استفاده از کنترلر Floodlight و شبیه‌ساز Mininet به عنوان تنظیمات آزمایشی بود. Mininet، یک شبیه‌ساز شبکه قوی، شبکه‌های مجازی معتبری را بر روی یک دستگاه واحد با هسته، سوئیچ و ... واقعی می‌سازد. و کاربرد کد اجزا. آن همه کاره تقلید دهانه‌ها مجازی ماشین آلات، ابر تنظیمات، و بومی سیستم‌ها، تجزیه و تحلیل‌ها و آزمایش‌های دقیق شبکه را برای محققان و متخصصان توانمند می‌سازد.

معیارهای ارزیابی شامل دقت، صحت، فراخوانی و امتیاز F1 در کنار معیارهای امنیتی مانند نرخ مثبت کاذب بودند. نادرست منفی نرخ، و تشخیص نرخ. نتایج را به نمایش گذاشت پیشنهادی سیستم ستودنی دقت و نرخ تشخیص، میانگین گیری در ۹۸.۵٪ و ۹۹.۲٪، به ترتیب. کم نرخ‌های مثبت کاذب و منفی کاذب، دقت سیستم را برجسته کرد. و به یاد آوردن گروه روش‌ها چنین به عنوان انباشته کردن و کیسه کشی بیشتر تقویت‌شده سیستم عملکرد. مشارکت‌ها شامل معرفی یک سیستم پیشگام مبتنی بر یادگیری ماشین برای حملات DDoS است. تشخیص و کاهش در SDN، همراه توسط یک امر تجربی ارزیابی برجسته سازی بالا دقت و نرخ تشخیص ، در کنار نرخ پایین مثبت کاذب و منفی کاذب. تلاش‌های آینده ممکن است بر افزایش مقیاس‌پذیری و سازگاری و ادغام سیستم با سایر سیستم‌های مبتنی بر SDN متمرکز شود. امنیت اقدامات. محدودیت‌ها شامل شدن ‎‏ ... وابستگی سیستم به داده‌های آموزشی قابل توجه برای افزایش دقت، آسیب‌پذیری در برابر مثبت‌ها و منفی‌های کاذب در سناریوهای خاص، و آسیب‌پذیری بالقوه در برابر حملات خصمانه که از نقاط ضعف مدل یادگیری ماشین سوءاستفاده می‌کنند.



**شکل ۴.** آمار و طبقه بندی از نظرسنجی

وانگ و همکاران [[4] در](#_bookmark20) تحقیقات خود بر حوزه شناسایی تمرکز دارند حملات انسداد سرویس (DDOS) حملات درون نرم‌افزار تعریف شده شبکه‌ها (SDN) با استفاده از ام ال. پیشنهادی سیستم عصاره‌ها داده‌ها از SDN​ کنترل کننده و استخدام می‌کند میلی لیتر الگوریتم‌ها برای حملات انسداد سرویس (DDOS) تشخیص حمله، با ارزیابی عملکرد و معیارهای امنیتی برای سنجش اثربخشی سیستم. نگرانی اصلی که در این مطالعه به آن پرداخته شده است، تشخیص حملات DDoS در SDN است. ارائه رمان حریم خصوصی و امنیت چالش‌ها. اجاره فعلی راه حل های درمانی شامل شدن هر دو متعارف شبکه اقدامات امنیتی و استراتژی‌های مبتنی بر یادگیری ماشین. با این حال، رویکردهای سنتی ثابت کردن بی‌اثر علیه مدرن حملات انسداد سرویس (DDOS) حملات، و میلی لیتر راه حل ها اغلب ایجاب کردن با کیفیت بالا مجموعه داده‌ها. هدف این تحقیق، معرفی یک مدل یادگیری ماشین سبک وزن تعبیه شده در SDN برای تشخیص DDoS با استفاده از داده‌ها و ویژگی‌های در دسترس است. سیستم پیشنهادی، درخواست‌های بسته را در بازه‌های زمانی از کنترل‌کننده SDN رصد می‌کند و نوسانات جریان را برای شناسایی حملات DDoS که کنترل‌کننده SDN را هدف قرار می‌دهند، بررسی می‌کند. با استفاده از کنترل متمرکز SDN، تمام فرآیندهای یادگیری ماشین - از آماده‌سازی داده‌ها گرفته تا ... به حملات انسداد سرویس (DDOS) تشخیص - می‌تواند باش اعدام شده به طور یکپارچه درون یک کنترلر واحد. ورودی شامل داده‌هایی از کنترلر SDN است، ‎‏ ... فرآیند استخدام می‌کند میلی لیتر الگوریتم‌ها، و ‎‏ ...

**شکل ۵.** خلاصه از دستگاه یادگیری تکنیک‌ها.

خروجی دلالت می‌کند ‎‏ ... موفق تشخیص از حملات انسداد سرویس (DDOS) حملات. تجربی پیکربندی شامل می‌شود هر دو تأسیس شد مجموعه داده‌ها و داده‌های خودتولید شده برای ارزیابی عملکرد سیستم پیشنهادی و امنیت معیارها ارزیابی معیارها شامل دقت، صحت، بازخوانی و معیار F می‌شود، در حالی که معیارهای امنیتی شامل محرمانگی، یکپارچگی و در دسترس بودن می‌شوند. نتایج، ظرفیت سیستم را برای تشخیص حملات DDoS به تنهایی با استفاده از یک ویژگی واحد، با دقت متفاوت، نشان می‌دهد. مشروط روی ‎‏ ... آموزش تنظیم شده. پیشنهادی سیستم به دست می‌آید الف زمان واقعی تشخیص دقت در شبکه SDN تجاوز کردن ۹۰٪. مشارکت‌ها شامل معرفی یک شبکه نرم‌افزاری سبک وزن جاسازی‌شده می‌شود. میلی لیتر مدل برای حملات انسداد سرویس (DDOS) تشخیص، با تأکید بر استفاده از داده‌ها و ویژگی‌هایی که به راحتی در دسترس هستند. تحقیقات آینده چشم اندازها شامل کردن موشکافی کردن جعل شده حملات انسداد سرویس (DDOS) حملات با ترافیک واقعی SDN با استفاده از یادگیری ماشین و دستیابی به اهداف واقعی تشخیص زمان. محدودیت‌های این سیستم شامل مناسب بودن منحصراً برای حملات DDoS سیل‌آسا، عدم توانایی در تشخیص حملات غیر حجمی و تمرکز انحصاری بر حملات علیه صفحه کنترل است.

سانتوس و همکاران [[5]](#_bookmark21) به بررسی کاربرد و حوزه فناوری SDN می‌پردازد و در عین حال به چالش‌های ناشی از حملات DDoS می‌پردازد. این مقاله از استفاده از چهار الگوریتم یادگیری ماشین مجزا برای طبقه‌بندی پشتیبانی می‌کند. حملات DDoS را در یک محیط شبیه‌سازی شده با SDN بررسی می‌کند و نتایج امیدوارکننده‌ای به همراه دارد. نگرانی اصلی که در این مقاله به آن پرداخته شده است، گسترش حملات DDoS در محیط‌های SDN است. به ویژه آسیب پذیری ‎‏ ... کنترل‌کننده متمرکز ، که در صورت به خطر افتادن، می‌تواند کل شبکه را مختل کند. راه‌حل‌های مرسوم شامل روش‌های تشخیص مبتنی بر امضا و مبتنی بر ناهنجاری هستند، با این حال این روش‌ها محدودیت‌هایی را نشان می‌دهند. در اثربخشی و کارایی. این کاغذ

هدف تحقیق، حمایت از ادغام الگوریتم‌های یادگیری ماشین برای تشخیص حملات DDoS در ... محیط‌های SDN، ارائه تجزیه و تحلیل مقایسه‌ای از اثربخشی و کارایی آنها در مقایسه با راه‌حل‌های موجود. پیشنهاد شده سیستم توابع توسط خوردن ترافیک داده‌ها از محیط SDN، که آن را در معرض پردازش از طریق چهار دستگاه قرار می‌دهد یادگیری الگوریتم‌ها (MLP، ماشین بردار پشتیبان، دی تی، و آر اف)، و ایجاد طبقه‌بندی ترافیک به عنوان عادی یا نشان‌دهنده‌ی حمله‌ی DDoS. متغیرهای ورودی شامل آدرس‌های IP، پروتکل‌ها، بسته اندازه‌ها، و درخواست مقادیر از یک «مشتری». تنظیمات آزمایشی شامل شبیه‌سازی بود حملات انسداد سرویس (DDOS) حملات و عادی ترافیک درون الف شبکه مجازی Mininet، با استفاده از یک کنترلر POX. معیارهای ارزیابی شامل دقت و زمان پردازش و امنیت بودند. معیارها شامل درست مثبت نرخ، نادرست مثبت نرخ، درست منفی نرخ، و نادرست منفی نرخ. یافته‌ها نشان داد که الگوریتم‌های یادگیری ماشین از راه‌حل‌های موجود پیشی گرفته‌اند در اصطلاحات از دقت و پردازش زمان. الگوریتم MLP بالاترین دقت را با 99.9٪ نشان داد، در حالی که الگوریتم جنگل تصادفی با زمان پردازش ۰.۰۰۰۲ ثانیه سریع‌ترین زمان پردازش را به خود اختصاص داد. در مورد تشخیص DDoS در SDN از طریق ML، هر چهار الگوریتم در محیط شبیه‌سازی شده کارایی خود را نشان دادند. الگوریتم MLP با ۹۹.۹٪ بالاترین دقت را به دست آورد و پس از آن با اختلاف کمی قرار گرفت. الگوریتم SVM با دقت ۹۹.۸٪. الگوریتم‌های درخت تصمیم و جنگل تصادفی دقت بالایی را نشان دادند به ترتیب ۹۹.۷٪ و ۹۹.۶٪. نکته قابل توجه این است که همه الگوریتم‌ها نرخ مثبت کاذب را زیر ۰.۱٪ حفظ کردند که نشان‌دهنده حداقل نرخ طبقه‌بندی اشتباه ترافیک عادی به عنوان حملات DDoS است. مشارکت‌ها از این کاغذ شامل شدن ‎‏ ... حمایت و پیاده‌سازی الگوریتم‌های یادگیری ماشین برای حملات DDoS تشخیص در شبکه SDN محیط‌ها، به نمایش گذاشتن دقت برتر و پردازش زمان مقایسه شده به موجود تلاش‌های آینده شامل آزمایش در دنیای واقعی و پرداختن به پتانسیل‌ها است . پیاده‌سازی چالش‌ها. محدودیت‌ها شامل شدن استفاده از ترافیک تولید شده مصنوعی و ضرورت تحقیقات بیشتر در مورد مقیاس‌پذیری سیستم پیشنهادی.

تان و همکاران [[6]](#_bookmark22) به حوزه تشخیص و دفاع در برابر حملات DDoS در SDN می‌پردازد. این کار با پرداختن به مسئله تحقیقاتی ضرورت شناسایی و مکانیسم‌های دفاعی دقیق و کارآمد DDoS در محیط‌های SDN، چارچوب جدیدی را معرفی می‌کند که شامل موارد زیر است: الف ماشه مکانیسم برای حملات انسداد سرویس (DDOS) حمله تشخیص، یک دستگاه یادگیری الگوریتم تحلیل کردن جریان ویژگی‌ها، و یک کنترل‌کننده برای اجرای اقدامات دفاعی. در زمینه SDN، مسئله تحقیق بر ضرورت حیاتی مکانیسم‌های دقیق و کارآمد برای شناسایی و دفاع در برابر حملات DDoS تأکید می‌کند. روش‌های سنتی تشخیص DDoS معمولاً با چالش‌هایی مربوط به دقت و کارایی در محیط‌های SDN مواجه می‌شوند. اهداف کلی تحقیق شامل معرفی یک چارچوب پیشگام برای تشخیص و دفاع از حمله DDoS در SDN است. مشارکت‌های خاص شامل ایجاد یک مکانیسم محرک برای تشخیص حمله DDoS، پیاده‌سازی یک الگوریتم یادگیری ماشین برای تجزیه و تحلیل ویژگی‌های جریان و توسعه ... یک کنترل کننده برای

اجرای اقدامات دفاعی. سیستم پیشنهادی، این فرآیند را با شناسایی جریان‌های غیرعادی درون شبکه از طریق یک مکانیسم ماشه در صفحه داده آغاز می‌کند. متعاقباً، یک الگوریتم یادگیری ماشین، که ریشه در K- Means دارد، و کی ان ان روش‌شناسی‌ها، تحلیل می‌کند ‎‏ ... تشخیص داده شد ترافیک برای تشخیص حمله DDoS. خروجی حاصل به کنترل‌کننده اطلاع می‌دهد، هدایت کردن آن در پیاده‌سازی مناسب اقدامات دفاعی. آزمایش‌های جامع، اساس تنظیمات آزمایشی را تشکیل دادند و اثربخشی و کارایی روش‌های پیشنهادی را ارزیابی کردند. معیارهای عملکرد، شامل دقت و کارایی، در کنار معیارهای امنیتی مربوط به تشخیص حمله DDoS و دفاع در SDN با استفاده از یادگیری ماشین، مورد بررسی قرار گرفته و با دقت ارائه شدند. نتایج حاصل از آزمایش‌ها زیرخط دار ‎‏ ... اثربخشی و کارایی از​ پیشنهادی روش‌ها در هر دو تشخیص و دفاع کردن علیه DDoS حملات درون شبکه SDN محیط‌ها، اعمال نفوذ یادگیری ماشین . تجزیه و تحلیل دقیق عملکرد و امنیت خاص معیارها مرتبط به حملات انسداد سرویس (DDOS) تشخیص و دفاع از طریق داده‌های جدول‌بندی شده و نمایش‌های گرافیکی توضیح داده شدند. سهم قابل توجه این کار شامل فرمول‌بندی از الف پیشگامانه چارچوب برای حملات انسداد سرویس (DDOS) تشخیص حمله و دفاع درون شبکه SDN محیط‌ها، بهره برداری از دستگاه یادگیری برای تشدید شده دقت و کارایی. تلاش‌های آینده ممکن است بر اصلاح بیشتر چارچوب پیشنهادی و پرداختن به هرگونه محدودیت شناسایی‌شده در طول مرحله آزمایش متمرکز شود. محدودیت‌های این مطالعه شامل محدودیت‌ها یا چالش‌های بالقوه‌ای است که در طول ارزیابی تجربی با آن‌ها مواجه شده‌ایم، همراه با حوزه‌های شناسایی‌شده برای بهبود بالقوه در چارچوب پیشنهادی.

Shakil و همکارانش [[7] در](#_bookmark23) حوزه SDN با تمرکز ویژه بر تشخیص و کاهش خطرات قرار دارد. حملات انسداد سرویس (DDOS) حملات. تأکید دروغ می‌گوید در کاردستی الف پویا چارچوب با استفاده از فراابتکاری خوشه‌بندی برای حملات انسداد سرویس (DDOS) تشخیص در اس دی ان. تحقیق چنگ زدن‌ها با توجه به آسیب‌پذیری SDNها در برابر حملات DDoS، که عمدتاً ناشی از جداسازی صفحه کنترل از ... است. صفحه داده. اگرچه راه‌حل‌های موجود الگوریتم‌های امنیتی را برای تقویت شبکه‌ها پیشنهاد می‌دهند، اما در محافظت مؤثر از SDNها در برابر حملات DDoS کمبود دارند. تحقیق اصلی عینی است ‎‏ ... فرمولاسیون از الف پیشگام چارچوب پویا با استفاده از خوشه‌بندی فراابتکاری برای تشخیص DDoS در اس دی ان. مشارکت‌ها شامل شدن ‎‏ ... معرفی WOA-DD و ارزیابی استحکام آن در مقایسه با راه‌حل‌های موجود. سیستم پیشنهادی به صورت زیر عمل می‌کند : توسط دریافت شبکه ترافیک داده‌ها به عنوان ورودی، تحت الشعاع قرار دادن آن به پردازش از طریق ‎‏ ... WOA-DD الگوریتم ریشه در خوشه‌بندی فراابتکاری دارد و خروجی را به شکل زیر تولید می‌کند از خوشه بندی شده حمله درخواست‌ها سیستم هسته هدف، خوشه‌بندی ماهرانه درخواست‌های حمله، تشخیص مؤثر و کاهش دهنده حملات انسداد سرویس (DDOS) حملات در اس دی ان. راه‌اندازی آزمایشی شامل پیاده‌سازی الگوریتم WOA-DD در یک محیط SDN شبیه‌سازی شده بود. معیارهای عملکرد شامل دقت تشخیص، نرخ مثبت کاذب، نرخ منفی کاذب بودند. نرخ، و محاسباتی سربار امنیت معیارهای پذیرفته شده تاب‌آوری به حملات انسداد سرویس (DDOS) حملات، سازگاری به پویا

ترافیک، و پایداری تحت متنوع شرایط. نتایج مورد تأکید ‎‏ ... WOA-DD الگوریتم استحکام، پایداری و کارایی در برابر حملات DDoS در SDN. به ویژه در داخل ‎‏ ... قلمرو از حملات انسداد سرویس (DDOS) تشخیص با استفاده از دستگاه یادگیری ، الگوریتم به نمایش گذاشته شده نویدبخش عملکرد توسط تشخیص دقیق و خوشه‌بندی حمله درخواست‌ها، بدین وسیله به طور ماهرانه ای کاهش می یابد حملات انسداد سرویس (DDOS) حملات در اس دی ان. مشارکت‌ها کپسوله کردن توسعه و ارزیابی از ‎‏ ... WOA-DD الگوریتمی برای تشخیص DDoS در SDN، که استحکام و پایداری آن را نشان می‌دهد. تلاش‌های آینده مستلزم اصلاح و بهینه‌سازی است. ‎‏ ... الگوریتم، جفت شده با آن عملی پیاده‌سازی در محیط‌های SDN دنیای واقعی. محدودیت‌های این مطالعه شامل اتکا به محیط‌های شبیه‌سازی شده و ضرورت اعتبارسنجی در استقرارهای عملی SDN است.

سنگودوین و همکاران [[8]](#_bookmark24) به حوزه تشخیص و دسته‌بندی حملات انسداد سرویس (DDOS) سیل حملات روی SDN ها از طریق استفاده از دستگاه یادگیری تکنیک‌ها. کانونی مشکل تحقیق بر حساسیت SDNها به حملات سیل DDoS متمرکز است و مکانیسم‌های تشخیص و طبقه‌بندی مؤثری را برای مقابله با این تهدیدات ضروری می‌سازد. راه‌حل‌های موجود شامل روش‌های مرسوم تشخیص حمله سیل DDoS، رویکردهای مبتنی بر SDN و روش‌های مبتنی بر یادگیری ماشین در SDNها هستند. هدف این مطالعه ارائه یک سیستم مبتنی بر یادگیری ماشین است که برای تشخیص و طبقه‌بندی حملات سیل DDoS به SDNها طراحی شده است. سهم آن در مفهوم‌سازی این سیستم و ارزیابی اثربخشی آن از طریق تجزیه و تحلیل تجربی نهفته است. سیستم پیشنهادی با دریافت داده‌های ترافیک شبکه، قرار دادن آن در معرض الگوریتم‌های یادگیری ماشین برای شناسایی و طبقه‌بندی حملات سیل DDoS و ارائه نتایج به عنوان نتایج تشخیص و طبقه‌بندی حمله عمل می‌کند. تنظیمات تجربی شامل شبیه‌سازی سناریوهای حمله سیل DDoS بر روی یک معماری SDN با استفاده از معیارهای متنوعی مانند تشخیص دقت، نادرست مثبت نرخ، پردازش زمان، تشخیص حمله نرخ، حمله طبقه بندی دقت، و تاب‌آوری برای گریز تکنیک‌ها به ارزیابی کردن ‎‏ ... پیشنهادی دستگاه سیستم تشخیص مبتنی بر یادگیری. نتایج مربوط به تشخیص DDoS در SDN با استفاده از یادگیری ماشین، معیارهایی مانند دقت تشخیص، نرخ مثبت کاذب، دقت طبقه‌بندی حمله و سازگاری سیستم با الگوهای حمله در حال تکامل را در بر می‌گرفت. مشارکت‌ها شامل شدن ‎‏ ... گزاره و ارزیابی الف دستگاه یادگیری محور سیستم متناسب سازی شده برای ‎‏ ... تشخیص و طبقه‌بندی حملات سیل‌آسای DDoS در SDNها آینده تلاش ها ممکن است چرخش اطراف ارتقاء دهنده ‎‏ ... مقیاس‌پذیری و استحکام سیستم ، همراه با ادغام قابلیت‌های تطبیقی در زمان واقعی. محدودیت‌های این مطالعه شامل موارد زیر است پتانسیل محدودیت‌ها گره خورده به خاص مجموعه داده‌ها و ضرورت اعتبارسنجی بیشتر در محیط‌های شبکه متنوع.

پرز-دیاز و ال. [[9]](#_bookmark25) کاوش می‌کند به ‎‏ ... قلمرو از تشخیص و کاهش حملات DDoS با نرخ پایین در محیط‌های SDN، با استفاده از تکنیک‌های یادگیری ماشین. موضوع اصلی تحقیق، آسیب‌پذیری سیستم‌های متمرکز، به ویژه پلتفرم‌های محاسبات ابری، در برابر حملات DDoS با نرخ پایین را بررسی می‌کند. در حالی که سنتی نفوذ تشخیص و پیشگیری

سیستم‌هایی وجود دارند، اثربخشی آنها در شناسایی DDoS با نرخ پایین حملات است سوال برانگیز. تحقیق عینی هدف، تدوین یک معماری امنیتی ماژولار و سازگار با هدف شناسایی و کاهش حملات DDoS با نرخ پایین در محیط‌های SDN است. سیستم پیشنهادی از ... استفاده می‌کند. یک ماژول IDS که برای تشخیص جریان‌ها با استفاده از مدل‌های یادگیری ماشین از پیش آموزش‌دیده طراحی شده است. داده‌های جریان شبکه به عنوان داده‌های سیستم عمل می‌کنند. ورودی، پردازش شده توسط ‎‏ ... شناسه‌ها از طریق دستگاه الگوریتم‌های یادگیری، که خروجی آنها متعاقباً جریان‌های مخرب را شناسایی می‌کند تخفیف یافته توسط ‎‏ ... آی پی اس ماژول راه‌اندازی آزمایشی مستلزم استقرار معماری در یک محیط مجازی بود اعمال نفوذ ‎‏ ... اونوس کنترل کننده، ارزیابی کردن شش الگوریتم یادگیری ماشین مجزا. معیارهای عملکرد، شامل دقت، صحت، فراخوانی و امتیاز F1، همراه با معیارهای امنیتی مانند نرخ تشخیص و نرخ مثبت کاذب در نظر گرفته شدند. نتایج حاصل از ارزیابی الگوریتم‌های یادگیری ماشین، نرخ دقت چشمگیری را گزارش کردند. ۹۵٪. معماری با موفقیت تشخیص داده شد و متنوع کاهش یافته نرخ پایین حملات انسداد سرویس (DDOS) حملات، اثبات کننده آن اثربخشی در یک دنیای واقعی تولید محیط زیست. مشارکت‌ها شامل طراحی و پیاده‌سازی معماری امنیتی همه‌کاره برای تشخیص و کاهش حملات DDoS با نرخ پایین در محیط‌های SDN، با استفاده از تکنیک‌های یادگیری ماشین. آینده کار شامل می‌شود بیشتر سیستم بهینه‌سازی و کاوش الگوریتم‌های یادگیری ماشینی اضافی. محدودیت‌ها شامل نیاز مداوم به اصلاح و سازگاری با استراتژی‌های در حال تکامل حمله DDoS است.

ریبیرو و ال. [[10] ،](#_bookmark26) معرفی می‌کند الف جامع چارچوب طراحی شده به تشخیص و مقابله کردن حملات انسداد سرویس (DDOS) حملات درون SDN از طریق استفاده از الگوریتم‌های یادگیری ماشین. تمرکز این مطالعه بر محافظت از سیستم‌های مبتنی بر اینترنت در برابر مضر تأثیر از حملات انسداد سرویس (DDOS) حملات. پیشنهادی سیستم تصویب می کند یک خودکار جریان طبقه بندی روش مبتنی بر روی الگوریتم‌های یادگیری ماشین به شناسایی و کاهش دادن حملات انسداد سرویس (DDOS) حملات درون شبکه‌های SDN . این تحقیق به بررسی وقوع فزاینده اختلالات سرویس ناشی از حملات DDoS و پیامدهای فنی و اقتصادی ناشی از آنها. راه‌حل‌های موجود شامل اقدامات امنیتی سنتی مانند فایروال‌ها و سیستم‌های تشخیص نفوذ، همراه با تکنیک‌های پیشرفته‌ای مانند دفاع هدف متحرک و رویکردهای مبتنی بر یادگیری ماشین هستند. با این حال، این راه‌حل‌ها از نظر اثربخشی و مقیاس‌پذیری محدودیت‌هایی را نشان می‌دهند. هدف اصلی از این کاغذ است به حاضر الف جامع نگر چارچوب برای تشخیص و کاهش حملات DDoS در شبکه‌های SDN، با استفاده از میلی لیتر الگوریتم‌ها. مشارکت‌ها مستلزم الف شرح دقیق چارچوب پیشنهادی، عملکرد و امنیت متریک ارزیابی، و الف مقایسه‌ای تحلیل در برابر راه‌حل‌های موجود. این سیستم با پیاده‌سازی عمل می‌کند یک روش طبقه‌بندی خودکار جریان مبتنی بر الگوریتم‌های یادگیری ماشین. داده‌های ترافیک شبکه، که توسط حسگرهای مستقر در شبکه SDN جمع‌آوری می‌شوند، به عنوان ورودی عمل می‌کنند. این حسگرها استفاده کردن میلی لیتر الگوریتم‌ها به طبقه بندی کردن شبکه ترافیک به جریان‌های عادی و مخرب. متعاقباً، جریان‌های مخرب به یک هانی‌پات هدایت می‌شوند، در حالی که جریان‌های عادی از آنجا عبور می‌کنند. شبکه. فرآیند طبقه‌بندی جریان شامل یادگیری ماشینی مختلفی است الگوریتم‌ها، از جمله احتمالاتی، خطی مدل،

شبکه‌های عصبی و درخت‌ها. آموزش دیده بر روی مجموعه داده ترافیک شبکه، اینها الگوریتم‌ها تشخیص دادن الگوها در عادی و بدخواه جریان می‌یابد. سیستم خروجی شامل می‌شود الف فهرست از بدخواه میزبان‌ها، که به‌روزرسانی‌ها ‎‏ ... امنیت سیاست‌ها از ‎‏ ... شبکه SDN کنترل کننده. تجربی راه اندازی درگیر شبیه‌سازی متنوع حمله سناریوها روی یک شبکه SDN به کارگیری شبکه ‎‏ ... پیشنهادی چارچوب. ارزیابی معیارهای گنجانده شده تشخیص نرخ، نادرست مثبت نرخ، و پاسخ زمان. امنیت معیارها احاطه شده محرمانگی، صداقت، و در دسترس بودن. شبیه‌سازی نتایج نشان داده شده ‎‏ ... کارایی ‎‏ ... پیشنهادی معماری در تشخیص و کاهش حملات DDoS در عرض تقریباً ۳ ثانیه. نرخ تشخیص از ۹۹.۹٪، الف نادرست مثبت نرخ زیر ۰.۱٪، و یک پاسخ زمان درون ۳ ثانیه‌ها بودند مشاهده شده - خوب درون قابل قبول محدوده برای زمان واقعی حملات انسداد سرویس (DDOS) حمله تشخیص و کاهش. معیارهای امنیتی نشان داد که معماری پیشنهادی حفظ می‌کند الف بالا سطح از امنیت علیه حملات DDoS. محرمانگی، صداقت، و در دسترس بودن از شبکه باقی ماند دست نخورده حتی تحت شدید حمله سناریوها. مشارکت‌ها از این کاغذ شامل شدن الف معماری جامع با استفاده از میلی لیتر الگوریتم‌ها برای ‎‏ ... تشخیص و کاهش از حملات انسداد سرویس (DDOS) حملات در شبکه SDN شبکه‌ها. چارچوب پیشنهادی، دفاع قوی در برابر حملات DDoS را نشان می‌دهد و ... ‎‏ ... محرمانگی، صداقت، و در دسترس بودن ‎‏ ... شبکه. آینده تلاش ها شامل شدن یکپارچه‌سازی پیشنهادی معماری با اضافی امنیت اقدامات مانند فایروال ها و نفوذ تشخیص سیستم‌ها. محدودیت‌ها شامل موارد زیر است ‎‏ ... اتکا روی شبیه‌سازی شده حمله سناریوها، که ممکن است کاملاً منعکس کننده شرایط دنیای واقعی نباشد. به طور خلاصه، معماری پیشنهادی یک راه حل کارآمد و مقیاس پذیر برای تشخیص و کاهش حملات DDoS در شبکه های SDN ارائه می دهد. با استفاده از میلی لیتر الگوریتم‌ها. ارزیابی نتایج آن را برجسته کنید اثربخشی در نگهداری الف بالا سطح از امنیت ضمن حفظ محرمانگی، یکپارچگی و دسترس‌پذیری شبکه. سبار و ال. [[11]](#_bookmark27) کنسانتره روی استخدام یادگیری ماشینی تکنیک‌ها به تقویت کردن ‎‏ ... تاب‌آوری از عرضه مبتنی بر SDN زنجیره ای شبکه‌ها علیه حملات انسداد سرویس (DDOS) حملات. شامل SDN، یادگیری ماشین، امنیت شبکه و شبکه‌های زنجیره تأمین، ‎‏ ... فناوری دامنه تحت ملاحظه کم امتیاز ‎‏ ... چندوجهی طبیعت از ‎‏ ... مطالعه کردن. تحقیقات مورد بررسی دوراهی می‌چرخد اطراف ‎‏ ... عدم کفایت از راهکارهای موجود در تقویت تاب‌آوری زنجیره تأمین مبتنی بر SDN شبکه‌ها علیه حملات انسداد سرویس (DDOS) حملات. سنتی مکانیسم‌های دفاعی ممکن است ثابت کردن ناکافی داده شده ‎‏ ... مقیاس، پیچیدگی و پویایی در حال تکامل حملات DDoS. علاوه بر این، روش‌های سنتی محدودیت‌هایی در مورد قابلیت مشاهده و نادرست نکات مثبت. تحقیق اهداف هدف به معرفی یک دستگاه یادگیری محور پارادایم برای افزایش دهنده تاب‌آوری از مبتنی بر SDN عرضه زنجیره ای شبکه‌ها در برابر حملات DDoS، با بهره‌گیری از قابلیت‌های ذاتی SDN برای محافظت در برابر چنین تهدیدهایی. سیستم پیشنهادی مهار می‌کند دستگاه یادگیری تکنیک‌ها، به طور خاص تحت نظارت طبقه بندی الگوریتم‌ها، به پیش بینی کردن ترافیک شبکه و تشخیص دادن پتانسیل حملات درون مبتنی بر SDN زنجیره تامین شبکه‌ها. ورودی داده‌ها شامل می‌شود شبکه ترافیک داده‌ها منبع‌یابی شده‌اند از چندگانه امتیازها درون ‎‏ ... شبکه SDN معماری.

چارچوب رویه‌ای مستلزم آموزش یک طبقه‌بندی‌کننده برای تشخیص الگوهای مشخصه رفتار عادی شبکه و حملات DDoS است. خروجی سیستم شامل طبقه‌بندی ترافیک ورودی شبکه، تمایز بین موجودیت‌های عادی و بالقوه مخرب است و در نتیجه شناسایی و کاهش حملات احتمالی DDoS را تسهیل می‌کند. راه‌اندازی آزمایشی شامل اجزای سخت‌افزاری و نرم‌افزاری مستقر، از جمله SDN است. کنترل کننده، شبیه‌سازی توپولوژی، و ابزارها ابزاری در مولد عادی و حمله ترافیک. عملکرد معیارهایی مانند دقت، صحت، فراخوانی و امتیاز F1، در کنار معیارهای امنیتی مانند نرخ تشخیص، نرخ مثبت کاذب و زمان پاسخ، مورد بررسی دقیق قرار می‌گیرند. نتایج مربوط به تشخیص DDoS در SDN با استفاده از یادگیری ماشین، دقت قابل تحسینی را در تشخیص حملات DDoS و اثربخشی آن نشان می‌دهد. کاهش استراتژی‌ها. مشارکت‌ها از این این مطالعه شامل پیشنهاد یک طرح نوآورانه مبتنی بر یادگیری ماشین است. رویکرد به تقویت کردن ‎‏ ... تاب‌آوری از مبتنی بر SDN شبکه‌های زنجیره تأمین در برابر حملات DDoS. تلاش‌های آینده ممکن است مستلزم اصلاح بیشتر مدل‌های یادگیری ماشین و گسترش آنها باشد ‎‏ ... محدوده به شامل شدن دیگر حمله انواع، و بررسی اقدامات یکپارچه برای افزایش امنیت. محدودیت‌ها اذعان کرد شامل شدن اتکا روی برچسب گذاری شده داده‌های آموزشی و ویژگی‌های ذاتی حملات. این خلاصه جامع با هدف خلاصه‌سازی جنبه‌های کلیدی کار آکادمیک ارائه شده است.

راج و همکاران [[12]](#_bookmark28) به حوزه تشخیص و کاهش آسیب می‌پردازد حملات انسداد سرویس (DDOS) حملات SDN از طریق ‎‏ ... استفاده از تکنیک‌های یادگیری ماشین. نقطه کانونی این مطالعه، تهدید فزاینده ناشی از حملات DDoS در محیط‌های SDN است که توسعه استراتژی‌های مؤثر تشخیص و کاهش آن را ضروری می‌سازد. روش‌های سنتی تشخیص DDoS مورد بررسی قرار گرفته و محدودیت‌های آنها در زمینه SDN آشکار شده و بر ضرورت رویکردهای پیشرفته مبتنی بر یادگیری ماشین تأکید می‌شود. تحقیق تلاش ها به معرفی کردن یک مدل کارآمد برای تشخیص DDoS در SDN با استفاده از تکنیک‌های یادگیری ماشین، و متعاقباً، به رفتار الف مقایسه‌ای تحلیل در برابر روش‌های تشخیص موجود. مشارکت‌ها شامل تدوین یک رویکرد جدید مبتنی بر یادگیری ماشین برای تشخیص DDoS، همراه با ارزیابی جامع عملکرد آن است. سیستم پیشنهادی شامل دریافت داده‌ها از مختص SDN مجموعه داده‌ها، پیاده‌سازی ویژگی انتخاب، و قرار دادن داده‌ها در معرض طبقه‌بندی‌کننده‌های مختلف یادگیری ماشین مانند XGBoost، SVM، LR، KNN و DT. خروجی سیستم طبقه‌بندی ترافیک به عنوان DDoS یا مشروع، و متعاقباً اقدامات امنیتی اجرا شده توسط کنترل‌کننده SDN. تجربی پیکربندی استخدام می‌کند یک مجموعه داده‌های SDN تولید شده از طریق Mininet، شامل داده‌های بی‌خطر و مخرب ترافیک. کلید ویژگی‌ها شامل شدن بایت‌های tx، بایت‌های rx، تاریخ و زمان، به همراه یک ویژگی کلاس که نشان‌دهنده‌ی DDoS یا ترافیک بی‌خطر است. ارزیابی‌های نتیجه شامل مقایسه‌ی دقت بین طبقه‌بندی‌کننده‌های مختلف یادگیری ماشین، شامل معیارهای عملکردی مانند دقت، فراخوانی، دقت و امتیاز F1. معیارهای امنیتی شامل تشخیص و پیشگیری از حملات DDoS در محیط‌های SDN می‌شود. یافته‌ها مرتبط با تشخیص DDoS در SDN با استفاده از ML

نورافکن ‎‏ ... اثربخشی از ‎‏ ... پیشنهادی مدل در دقیقاً قابل تشخیص و تسکین دهنده حملات انسداد سرویس (DDOS) حملات، به عنوان روشن شد در ارائه شده میزها و نمودارها این تحقیق مشارکت می‌کند با تدبیر کردن یک پیشرفته مبتنی بر یادگیری ماشینی مدل برای حملات انسداد سرویس (DDOS) تشخیص در SDN، تکمیل شده توسط الف دقیق مقایسه‌ای ارزیابی از آن عملکرد. آینده تلاش ها ممکن است شامل کردن پالایش پیشنهادی​ مدل، گسترش آن کاربردپذیری به متنوع انواع حمله ، و کاوش زمان واقعی پیاده‌سازی در متنوع محیط‌های SDN . محدودیت‌ها شامل ویژگی محیط‌های به کار رفته می‌شود. SDN مجموعه داده‌ها، پتانسیل مقیاس‌پذیری نگرانی‌ها، و امر ضروری برای بیشتر اعتبارسنجی در سراسر متنوع SDN تنظیمات. سودار و ال. [[13]](#_bookmark29) کاوش‌های [الکترونیکی](#_bookmark29) ‎‏ ... قلمرو از حملات انسداد سرویس (DDOS) تشخیص درون SDN توسط استخدام میلی لیتر تکنیک‌ها. سیستم پیشنهادی استفاده می‌کند ماشین بردار پشتیبان و دی تی الگوریتم‌ها به تشخیص دادن ترافیک مخرب از عادی ترافیک. دقت، به یاد آوردن، دقت، و معیار F هستند شاغل به عنوان عملکرد معیارها، در حالی که معیارهای امنیتی تمرکز روی ‎‏ ... سیستم توانایی به تشخیص حملات روز صفر و حجم ترافیک قابل توجهی را مدیریت می‌کند. مجموعه داده KDD99 اساس تنظیمات تجربی برای آموزش و آزمایش مدل را تشکیل می‌دهد. این مقاله به بررسی آسیب‌پذیری SDN در برابر حملات DDoS می‌پردازد و بر کاستی‌های سیستم‌های تشخیص نفوذ مرسوم و روش‌های مبتنی بر امضا تأکید می‌کند . مطالعه عینی است به معرفی کردن الف ام ال- رانده شده مکانیسم برای شناسایی بدخواه فعالیت‌ها درون SDN، با الف خاص تأکید روی ‎‏ ... توانایی به حملات جدید و بارهای ترافیکی بزرگ را مدیریت کند. سیستم پیشنهادی شامل موارد زیر است ویژگی استخراج از ترافیک جریان داده‌ها از ورودی‌های جدول جریان گرفته شده است. مجموعه داده‌ها به بخش‌های آموزشی تقسیم می‌شوند. و آزمایش زیرمجموعه‌ها، و ماشین بردار پشتیبان و تصمیم الگوریتم‌های درختی بیا به بازی کردن برای طبقه بندی ترافیک به عنوان عادی یا بدخواه. تصمیم درخت خدمت می‌کند به تمایز قائل شدن بین متمایز ترافیک انواع، هدایت کردن ‎‏ ... شناسایی از عادی و بدخواه ترافیک. طبقه‌بندی‌کننده خروجی‌ها ماشه هشدارها به کنترل‌کننده‌ها، ترغیب کردن ‎‏ ... حذف از خاص جریان‌ها از میز در ‎‏ ... رویداد از یک حمله کردن. کی دی دی ۹۹ مجموعه داده‌ها شاغل است برای آموزش و آزمایش. دقت، یادآوری، دقت، و معیار F تشکیل دهنده ‎‏ ... عملکرد معیارها SVM دقت و فراخوانی ۸۰٪ را نشان می‌دهد، با تغییرات جزئی در تصمیم درخت دقت و به یاد آوردن نتایج نشان دادن برتر عملکرد از ماشین بردار پشتیبان بیش از تصمیم درخت در ‎‏ ... شبیه‌سازی شده محیط زیست. امنیت معیارها در بر گرفتن ظرفیت به تشخیص روز صفر حملات و مدیریت کردن ترافیک بالا حجم‌ها مشارکت‌ها شامل شدن ‎‏ ... پیشنهاد از یک برنامه‌ی مبتنی بر یادگیری ماشینی مکانیسم برای شناسایی بدخواه فعالیت‌ها در SDN، به نمایش گذاشتن ‎‏ ... اثربخشی از ماشین بردار پشتیبان و درخت تصمیم الگوریتم‌ها در حملات انسداد سرویس (DDOS) حمله تشخیص. آینده‌نگر کار شامل می‌شود پالایش سیستم دقت و انجام دادن دنیای واقعی آزمایش، با محدودیت‌ها متمرکز اطراف ‎‏ ... نیاز برای

گسترده آموزش داده‌ها و پتانسیل نادرست نکات مثبت.

کاویتا و همکاران [[14]](#_bookmark30) به حوزه امنیت شبکه، به ویژه در SDN، می‌پردازد و از تکنیک‌های یادگیری ماشین برای شناسایی حملات DDoS استفاده می‌کند. سیستم پیشنهادی از الگوریتم‌های یادگیری ماشین برای بررسی دقیق ترافیک شبکه استفاده می‌کند، نکته سنج پتانسیل حملات انسداد سرویس (DDOS) تهدیدها مطالعه از مجموعه داده KDD Cup 99 برای آموزش و آزمایش مدل‌های یادگیری ماشین استفاده می‌کند ، ارزیابی کردن ‎‏ ... سیستم عملکرد با استفاده از معیارها

مانند دقت و فراخوانی. معیارهای امنیتی، از جمله نرخ‌های مثبت کاذب و منفی کاذب نیز مورد بررسی قرار می‌گیرند. نتایج زیرخط دار ‎‏ ... سیستم اثربخشی در شبکه SDN حملات انسداد سرویس (DDOS) تشخیص حمله ، با ‎‏ ... تصمیم درخت مدل به نمایش گذاشتن عملکرد برتر در بین الگوریتم‌های یادگیری ماشین. مسیرهای تحقیقاتی آینده شامل کاوش الگوریتم‌های یادگیری عمیق و ارزیابی شبکه‌های دنیای واقعی است. افزایش حجم و پیچیدگی داده‌های شبکه، یک خطر امنیتی قابل توجه را ایجاد می‌کند که مستلزم... یک تأکید روی شبکه امنیت. شبکه SDN به عنوان راه حلی برای پیکربندی شبکه‌های انعطاف‌پذیر پدیدار می‌شود ؛ با این حال، معماری آن چالش‌های امنیتی جدیدی را معرفی می‌کند. IDS ایستاده است به عنوان محوری امنیت ابزارها، شناسایی پتانسیل تهدیدات شبکه. روش‌های سنتی IDS در تشخیص حملات ناشی از حجم بالای داده‌ها، انواع مختلف داده‌ها و سرعت بالای داده‌ها دچار مشکل می‌شوند. الگوریتم‌های یادگیری ماشین نویدبخش افزایش دقت و کارایی IDS، به ویژه برای تشخیص حمله DDoS هستند. موجود راه حل ها گنجاندن کلاسیک میلی لیتر مدل‌هایی مانند KNN، LR و DT برای تحلیل ترافیک شبکه. هدف تحقیق، ارائه یک سیستم با استفاده از یادگیری ماشین برای تشخیص حمله DDoS در محیط‌های SDN و ارزیابی اثربخشی آن است. این سیستم داده‌های ترافیک شبکه را با ... پردازش می‌کند. الگوریتم‌های یادگیری ماشین برای تشخیص حملات احتمالی DDoS. ورودی داده‌ها تحت پیش‌پردازش، از جمله انتخاب ویژگی، نرمال‌سازی و پیش‌پردازش داده‌ها، قرار می‌گیرند تا مدل یادگیری ماشینی بهبود یابد. عملکرد. شاغل میلی لیتر مدل‌ها شامل شدن KNN، LR و درخت‌های تصمیم‌گیری. خروجی سیستم پیش‌بینی می‌کند که آیا ترافیک شبکه بی‌خطر است یا نشان‌دهنده‌ی یک حمله‌ی DDoS بالقوه. راه‌اندازی آزمایشی مستلزم استفاده از مجموعه داده‌های KDD Cup 99 برای آموزش و آزمایش مدل ML است. معیارهای عملکرد مانند دقت، فراخوانی، نرخ مثبت کاذب و نرخ منفی کاذب، اثربخشی سیستم را اندازه‌گیری می‌کنند. نتایج، موارد زیر را برجسته می‌کنند: تصمیم درخت مدل برتری در دقت و یادآوری. این سیستم به نرخ پایین مثبت کاذب و منفی کاذب دست می‌یابد که مهارت آن را در تشخیص حمله DDoS تأیید می‌کند. مصور میزها و نمودارها روشن کردن ‎‏ ... یافته‌ها معیارهای امنیتی، فراگیر نادرست مثبت و نادرست منفی نرخ‌ها، تضمین ‎‏ ... سیستم اعتصابات الف تعادل، اجتناب کردن بیش از حد هشدارهای کاذب یا حملات بالقوه از دست رفته. نتایج مربوط به تشخیص DDoS در شبکه SDN با استفاده از میلی لیتر زیرخط دار سیستم اثربخشی. مدل DT به دقت ۹۸.۵٪ و میزان فراخوانی ۹۷.۵٪ دست می‌یابد که گواهی بر به آن مهارت در پرچم گذاری پتانسیل حملات. سیستم پیشنهادی، پتانسیل الگوریتم‌های یادگیری ماشین را در افزایش دقت IDS برای تشخیص حمله DDoS در محیط‌های SDN برجسته می‌کند. مشارکت‌ها شامل پیشنهاد یک الگوریتم یادگیری ماشین با استفاده از سیستم برای حملات انسداد سرویس (DDOS) تشخیص و ارزیابی اثربخشی آن. کاوش‌های آینده شامل الگوریتم‌های یادگیری عمیق و ارزیابی‌های شبکه در دنیای واقعی است. محدودیت‌های سیستم شامل اتکا به مجموعه داده‌های KDD Cup 99 است که به طور بالقوه نماینده کاملی از ترافیک شبکه در دنیای واقعی نیست.

الحمامی و ال. [[15]](#_bookmark31) بررسی می‌کند ‎‏ ... دامنه از تشخیص حملات DDoS در SDN از طریق استفاده از الگوریتم‌های یادگیری ماشین. این مطالعه به مسئله حیاتی افزایش تشخیص حمله DDoS در محیط‌های SDN می‌پردازد که ناشی از تقاضای روزافزون برای خدمات آنلاین و ماهیت در حال تکامل است. از حملات انسداد سرویس (DDOS) حملات. فعلی راه حل ها، تکیه کردن روی

اقدامات امنیتی سنتی و پروتکل‌های شبکه، به دلیل استفاده مهاجمان از چندین پروتکل، با چالش‌هایی روبرو هستند که تشخیص DDoS را پیچیده می‌کند. هدف اصلی، طراحی سیستمی است که از الگوریتم‌های یادگیری ماشین، به ویژه XGBoost، LR، SVM و KNN، برای تشخیص حملات DDoS در SDN استفاده کند. پیشنهادی سیستم مشارکت می‌کند به تقویت کننده امنیت شبکه با محافظت از کنترل‌کننده‌های SDN در برابر حملات DDoS. سیستم عمل می‌کند توسط استخدام میلی لیتر طبقه‌بندی‌کننده‌ها برای بررسی دقیق یک مجموعه داده شبیه‌سازی شده که شرایط حمله DDoS در دنیای واقعی را تکرار می‌کند. ورودی شامل داده‌های ترافیک شبکه است و این فرآیند شامل آموزش طبقه‌بندی‌کننده‌های ML است که منجر به شناسایی حملات DDoS می‌شود که کنترل‌کننده‌های SDN را هدف قرار می‌دهند. تجربی راه اندازی شبیه‌سازی شده یک شبکه SDN شبکه با استفاده از شبیه‌ساز Mininet که توسط یک کنترل‌کننده OpenDaylight مدیریت می‌شود، سناریوهای حمله خوش‌خیم و DDoS را در بر می‌گیرد. معیارهای عملکرد شامل دقت، صحت، فراخوانی، امتیاز F1 و زمان پردازش بود. معیارهای امنیتی، اثربخشی مدل‌های ML را در تشخیص حملات DDoS ارزیابی کردند. XGBoost، LR، SVM و KNN در تشخیص ... کارایی نشان دادند. حملات علیه شبکه SDN کنترل کننده ها، با ایکس‌جی‌باووست و LR به ویژه از نظر کارایی محاسباتی قابل توجه است. با این حال، ‎‏ ... توجه طبقه بندی کننده به نمایش گذاشته شده محدودیت‌ها در دقت طبقه‌بندی مطالعه مشارکت می‌کند توسط ارزیابی کردن میلی لیتر الگوریتم‌های تشخیص حمله DDoS در SDN، با برجسته کردن XGBoost و LR به عنوان گزینه‌های مؤثر برای تشخیص تهدید در زمان واقعی. تلاش‌های آینده شامل پیاده‌سازی تکنیک‌های بهینه‌سازی برای بهبود طبقه‌بندی‌کننده‌ها برای تشخیص حمله DDoS در SDN خواهد بود. محدودیت‌ها شامل نیاز مبرم به بهبود بیشتر در دقت طبقه‌بندی و کارایی محاسباتی است.

کیا و همکاران [[16]](#_bookmark32) به آسیب‌پذیری کنترل‌کننده‌های SDN در برابر حملات DDoS می‌پردازد و یک سیستم مبتنی بر یادگیری ماشین را معرفی می‌کند که برای شناسایی و دسته‌بندی ترافیک به صورت عادی یا مخرب در شبکه‌های SDN طراحی شده است. تمرکز این مقاله بر حوزه امنیت شبکه در شبکه‌های SDN است. نگرانی اصلی که در این مقاله به آن پرداخته شده است مربوط می‌شود به ‎‏ ... در حال نمایان شدن تهدید از حملات انسداد سرویس (DDOS) حملات روی شبکه‌های SDN ، ایجاب کننده ‎‏ ... توسعه از یک کارآمد تشخیص​ و طبقه بندی سیستم. موجود راه حل ها شامل آنتروپی مبتنی بر و دستگاه یادگیری محور روش‌شناسی‌ها. هدف تحقیق، معرفی یک رویکرد مبتنی بر یادگیری ماشین است. سیستم ماهر در به طور دقیق شناسایی و طبقه‌بندی حملات DDoS در شبکه‌های SDN. سیستمی که در این مقاله پیشنهاد شده است، اطلاعات وضعیت جریان جمع‌آوری‌شده را تجزیه و تحلیل می‌کند. از شبکه SDN و با استفاده از استخراج ویژگی، تشخیص می‌دهد بین عادی و بدخواه ترافیک. دو الگوریتم‌های یادگیری ماشین، یعنی SVM خطی و SVM چندجمله‌ای، هستند مورد استفاده قرار گرفت برای ترافیک طبقه بندی. ورودی به سیستم شامل اطلاعات وضعیت جریان است که تولید می‌کند یک خروجی که دلالت می‌کند ‎‏ ... طبقه بندی از ترافیک به صورت عادی یا مخرب. پیکربندی آزمایشی شامل ایجاد یک شبکه SDN شبیه‌سازی شده با استفاده از Mininet بود. رابط کاربری گرافیکی با نه جریان باز مجازی سوئیچ‌ها و ۶۴ میزبان. مجموعه داده‌های آزمایشی شامل ۶۵۰ نمونه از ترافیک بی‌خطر و مخرب تولید شده از طریق بسته scapy بود. نسل ابزار. عملکرد معیارها فراگیر

دقت، نرخ هشدار اشتباه، نرخ تشخیص و دقت برای ارزیابی سیستم استفاده شد. معیارهای امنیتی شامل اثربخشی سیستم در تشخیص و کاهش حملات DDoS بود. حملات. نتایج نشان داده شده ‎‏ ... برتری سیستم پیشنهادی، به ویژه روش SVM چندجمله‌ای، بیش از ‎‏ ... موجود خطی ماشین بردار پشتیبان رویکرد در از نظر دقت و نرخ هشدار اشتباه. سیستم به دقتی دست یافت از ۹۸.۴۶٪، الف نادرست زنگ هشدار نرخ از ۱.۵۴٪، الف نرخ تشخیص ۹۸.۴۶٪ و دقت ۹۸.۴۶٪. علاوه بر این، ‎‏ ... سیستم به نمایش گذاشته شده مؤثر تشخیص و کاهش حملات DDoS. این مقاله با ارائه یک سیستم مبتنی بر یادگیری ماشین که برای تشخیص و طبقه‌بندی حملات DDoS در شبکه‌های SDN طراحی شده است، و با نتایج تجربی قانع‌کننده پشتیبانی می‌شود، به این امر کمک می‌کند. کار آینده شامل آزمایش سیستم بر روی شبکه‌های گسترده‌تر و پیچیده‌تر، در کنار بررسی یادگیری ماشین جایگزین است. الگوریتم‌ها. محدودیت‌ها شامل شدن ‎‏ ... اتکا روی یک شبکه شبیه‌سازی شده و یک مجموعه داده محدود. به طور خلاصه، این مقاله یک سیستم مبتنی بر یادگیری ماشین را معرفی می‌کند که برای تشخیص و طبقه‌بندی حملات DDoS در SDN طراحی شده است. شبکه‌ها. اهرم سازی جریان وضعیت اطلاعات و با استفاده از دو الگوریتم یادگیری ماشین، این سیستم پیشرفت‌های قابل توجهی در دقت و نرخ هشدارهای کاذب نشان می‌دهد. به موجود روش‌ها. تجربی پیامدها زیر خط کشیدن سیستم مهارت در به طور موثر تشخیص و کاهش حملات DDoS.

سکار و همکاران [[17]](#_bookmark33) به حوزه تشخیص و خنثی کردن حملات DDoS در حوزه SDN می‌پردازد. چشم‌انداز فناوری مورد بررسی شامل کاربرد است. از تکنیک‌های یادگیری ماشین، به ویژه درخت‌های تصمیم‌گیری، Cat Boost و Extra Tree، برای تقویت امنیت شبکه در محیط‌های SDN. مشکل اصلی تحت بررسی در این تحقیق، آسیب‌پذیری SDN در برابر حملات DDoS مطرح شده است که باعث تلاش برای تشخیص و کاهش قوی این حملات شده است. روش‌شناسی‌ها در حالی که متعارف شبکه اقدامات امنیتی وجود داشته باشد، آنها کفایت در مدیریت ‎‏ ... پویا و ماهیت پیچیده حملات DDoS در SDN مورد سوال قرار گرفته است. این مطالعه تلاش ها به تدبیر و ارزیابی کردن دستگاه استراتژی‌های مبتنی بر یادگیری برای تشخیص و پیشگیری از حملات DDoS در SDN. سیستم پیش‌بینی‌شده با استفاده از داده‌های شبکه عمل می‌کند. ترافیک داده‌ها، در معرض قرار دادن آن به پردازش از طریق یادگیری ماشینی الگوریتم‌ها مانند تصمیم درختان، گربه تقویت، و درخت اضافی، و خروجی مبلمان در قالب پیش‌بینی‌هایی در مورد پتانسیل حملات انسداد سرویس (DDOS) حملات. سیستم رابط‌ها با یک مجموعه داده‌ها شامل ویژگی‌ها چنین به عنوان پروتو، پرچم‌ها، صدر، بابا، ورزش، ایالت، دسته بندی، و زیررده. ورودی داده‌ها تحت پیش‌پردازش قرار می‌گیرد ، آموزش، و آزمایش از طریق دستگاه مدل‌های یادگیری و نتایج برای پیش‌بینی وقوع به کار گرفته می‌شوند از حملات انسداد سرویس (DDOS) حملات. تجربی راه اندازی مستلزم استفاده از مجموعه داده Kaggle، پیش‌پردازش داده‌ها و آموزش مدل‌های یادگیری ماشین با استفاده از طبقه‌بندی‌کننده‌های DT، Cat Boost و Extra Tree است. معیارهای عملکرد اولیه شامل دقت است که در آن درخت‌های تصمیم به اوج خود می‌رسند. دقت از ۹۶.۲۵٪. امنیت معیارها سنجش تشخیص الگوهای ترافیکی غیرعادی و افزایش تقاضا برای خاص مقاصد بودند همچنین مورد بررسی دقیق قرار داد.

یافته‌ها پیشنهاد دادن ‎‏ ... وعده از ‎‏ ... دستگاه رویکرد یادگیری محور ، به طور قابل توجه ‎‏ ... دی تی مدل، در به طور ماهرانه‌ای شناسایی حملات DDoS در اس دی ان. دی تی مدل نشان داده شده الف نرخ دقت قابل تحسین ۹۶.۲۵٪، که از الگوریتم‌های یادگیری ماشین جایگزین ارزیابی‌شده پیشی می‌گیرد. این تحقیق به موارد زیر کمک می‌کند: این حوزه با ایجاد وب‌سایتی که به پیش‌بینی حملات DDoS از طریق روش‌های یادگیری ماشینی می‌پردازد، همراه شده است. با یک ارزیابی از تصمیم درختان، گربه طبقه‌بندی‌کننده‌های Boost و Extra Tree برای تشخیص DDoS در SDN. آینده‌نگر کار مستلزم بیشتر هونینگ از دستگاه مدل‌های یادگیری و ‎‏ ... شمول از تکمیلی امنیت معیارها. محدودیت‌ها شامل ویژگی‌های خاص مجموعه داده‌های مورد استفاده می‌شوند. و ‎‏ ... تعمیم پذیری از یافته‌ها به متنوع محیط‌های SDN

کوراکولا و همکاران [[18]](#_bookmark34) با استفاده از روش‌های یادگیری ماشینی، به حوزه تشخیص حملات DDoS در SDN می‌پردازد. سیستم پیشنهادی به دنبال افزایش دقت و اثربخشی در تشخیص و مقابله با حملات DDoS در محیط‌های SDN است. مسئله اصلی مورد بررسی در این مطالعه، آسیب‌پذیری SDN در برابر حملات DDoS است که با کاستی‌های روش‌های فعلی در تشخیص و کاهش مؤثر این تهدیدات، تشدید می‌شود. راه‌حل‌های رایج شامل روش‌های سنتی و مبتنی بر یادگیری ماشینی هستند، با این حال نمایشگاه فرعی دقت، تشدید شده پیچیدگی، و تقاضا برای تخصص تخصصی. هدف تحقیق ایجاد یک مکانیزم قابل اعتماد و کارآمد برای شناسایی دقیق و مقابله با تأثیرات حملات DDoS بر روی SDN است. سیستم پیش‌بینی شده با استفاده از ingesting عمل می‌کند. شبکه ترافیک داده‌ها، در معرض قرار دادن آن به پردازش از طریق دستگاه یادگیری الگوریتم‌ها، و مولد خروجی‌ها نشان دهنده تشخیص و کاهش حمله DDoS است. این سیستم از یک مجموعه داده تهیه شده از Kaggle استفاده می‌کند که شامل ۴۱ ویژگی ترافیک است. دستگاه یادگیری الگوریتم از انتخاب درخت تصمیم است که نتایج دقت برتر (96٪) را در مقایسه با تکنیک‌های جایگزین یادگیری ماشین نشان می‌دهد. تنظیمات آزمایشی شامل استفاده از مجموعه داده CICDDoS2019 بود. با دقت ساخته شده به اصلاح کردن کمبودها در مجموعه داده‌های موجود. معیارهای عملکرد اصلی شامل دقت، صحت و فراخوانی بودند، در حالی که معیارهای امنیتی شامل نرخ مثبت کاذب، نرخ منفی کاذب و نرخ تشخیص بودند. نتایج نشان داد که سیستم پیشنهادی با استفاده از الگوریتم DT از روش‌های موجود در این حوزه عملکرد بهتری دارد. از حملات انسداد سرویس (DDOS) حمله تشخیص و کاهش درون SDN. سیستم پیشنهادی به نرخ دقت ۹۶٪ دست یافت که از روش‌های موجود پیشی گرفت. نرخ مثبت کاذب ۰.۰۴، نرخ منفی کاذب ۰.۰۸ و نرخ تشخیص در ۰.۹۲. این یافته‌ها اثربخشی روش پیشنهادی را برجسته می‌کنند. سیستم در تشخیص و کاهش دهنده حملات انسداد سرویس (DDOS) حملات روی SDN از طریق میلی لیتر روش‌شناسی‌ها مشارکت‌ها از این این کار، فرمول‌بندی یک روش قابل اعتماد و کارآمد برای تشخیص و کاهش حملات DDoS در SDN را با استفاده از روش‌های یادگیری ماشینی خلاصه می‌کند. تلاش‌های آینده ممکن است شامل بهبود عملکرد سیستم از طریق ادغام الگوریتم‌های پیشرفته یادگیری ماشین و گسترش مجموعه داده‌ها باشد. محدودیت‌ها شامل مجموعه داده‌های محدود و تخصص لازم برای عملکرد سیستم است.

طاهرو و ال. [[19]](#_bookmark35) کاوش می‌کند به ‎‏ ... قلمرو از به کارگیری تکنیک‌های یادگیری ماشین برای شناسایی و مقابله با حملات DDoS در SDN. این مقاله چالش‌های امنیتی پیش روی معماری SDN به دلیل تفکیک صفحه کنترل و صفحه داده را برجسته می‌کند. معمای تحقیق حول محور ... می‌چرخد. اطراف ‎‏ ... دقیق تشخیص و مؤثر کاهش حملات DDoS در SDN، با تأکید بر لزوم افزایش دقت و کاهش نرخ‌های مثبت کاذب. روش‌های فعلی شامل استراتژی‌های مبتنی بر آنتروپی، تحلیل الگوی ترافیک و الگوریتم‌های مبتنی بر یادگیری ماشینی هستند. هدف این تحقیق، به‌کارگیری تکنیک‌های یادگیری ماشینی تحت نظارت و بهره‌برداری از ... ذاتی ... است. ویژگی‌ها از جریان باز ترافیک به تشخیص دادن حملات DDoS که لایه کنترل را هدف قرار می‌دهند. سیستم پیشنهادی از الگوریتم‌های یادگیری ماشین تحت نظارت مانند Naive Bayes، KNN، و ماشین بردار پشتیبان به فرموله کردن الف طبقه بندی مدل. آموزش و آزمایش رخ دادن روی ‎‏ ... CIC-2019 مجموعه داده‌ها، کجا ترافیک Openflow به عنوان ورودی عمل می‌کند و خروجی به صورت طبقه‌بندی ترافیک به دسته‌های عادی یا غیرعادی نمایان می‌شود. رویه ای توالی مستلزم آموزش میلی لیتر الگوریتم‌های روی مجموعه داده‌ها و به‌کارگیری مدل آموزش‌دیده برای طبقه‌بندی ترافیک در زمان واقعی. پیکربندی آزمایشی مستلزم موارد زیر است: ‎‏ ... استفاده از ‎‏ ... مینی‌نت شبیه ساز در کنار کنترلر Floodlight. معیارهای عملکرد شامل دقت، صحت، فراخوانی و امتیاز F1 می‌شوند، در حالی که معیارهای امنیتی شامل نرخ مثبت کاذب، نرخ منفی کاذب و نرخ تشخیص هستند. نتایج نشان می‌دهد که سیستم پیشنهادی به دقت بالا همراه با حداقل نرخ مثبت کاذب دست یافته است. حملات DDoS با دقت و فراخوانی قابل توجهی شناسایی می‌شوند و یافته‌ها به صورت بصری از طریق جداول و نمودارها ارائه می‌شوند. سیستم پیشنهادی به موارد زیر دست می‌یابد: یک چشمگیر دقت از ۹۹.۹٪ با الف ناچیز نرخ مثبت کاذب ۰.۱٪. دقت در تشخیص حملات DDoS به ۹۹.۸٪ می‌رسد، همراه با نرخ بازیابی ۹۹.۹٪. این سیستم نمایشگاه‌ها الف مقاوم تشخیص نرخ از ۹۹.۹٪. این این مقاله با معرفی سیستمی که در شناسایی و کاهش تهدیدات مهارت دارد، سهم قابل توجهی در حوزه امنیت SDN ایفا می‌کند. حملات انسداد سرویس (DDOS) حملات با قابل توجه دقت و حداقل نرخ مثبت کاذب. تلاش‌های آینده شامل قرار دادن موارد زیر است: سیستم به بزرگتر مجموعه داده‌ها و کاوش ‎‏ ... پتانسیل الگوریتم‌های یادگیری ماشین بدون نظارت. محدودیت‌ها شامل پیش‌نیاز داده‌های آموزشی گسترده و پتانسیل منفی‌های کاذب می‌شود. به طور خلاصه، این مقاله بینش‌های ارزشمندی ارائه می‌دهد. به استخدام میلی لیتر تکنیک‌ها برای ‎‏ ... شناسایی و کاهش حملات DDoS در SDN. مهارت سیستم پیشنهادی در دستیابی به دقت بالا و نرخ پایین مثبت کاذب، آن را به عنوان یک راه حل امیدوارکننده برای تقویت امنیت SDN قرار می‌دهد.

ساناپالا و همکاران [[20]](#_bookmark36) یک سیستم نوآورانه مبتنی بر یادگیری ماشینی را معرفی می‌کند. استراتژی برای ‎‏ ... تشخیص و کاهش حملات DDoS در چارچوب SDN. سیستم پیش‌بینی‌شده از طبقه‌بندی‌کننده‌های SVM و DT برای نظارت فعال و بررسی دقیق ترافیک شبکه در زمان واقعی، به طور ماهرانه‌ای استفاده می‌کند. شناسایی و خنثی کننده پتانسیل حملات با الف به طور قابل توجه بالا سطح از دقت. کانونی نقطه از این مقاله حول محور امنیت شبکه می‌چرخد و به طور خاص به آن می‌پردازد. حملات انسداد سرویس (DDOS) حمله تشخیص و کاهش در شبکه SDN

از طریق به‌کارگیری تکنیک‌های یادگیری ماشین. نگرانی اصلی که در این مقاله به آن پرداخته شده است، افزایش فرکانس و پیچیدگی حملات DDoS است که تهدیدی قابل توجه برای دسترسی به خدمات اینترنتی محسوب می‌شود. روش‌های تشخیص مرسوم، از جمله رویکردهای مبتنی بر امضا، هستند کاهش یابنده در اثربخشی علیه حملات در حال تکامل . علیرغم وجود راهکارهایی مانند فایروال‌ها، سیستم‌های تشخیص نفوذ و شبکه‌های تحویل محتوا، اثربخشی آنها در برابر حملات DDoS همچنان متناقض است. هدف تحقیق، طراحی سیستمی است که به طور ماهرانه ... را تشخیص دهد. حملات انسداد سرویس (DDOS) حملات توسط اعمال نفوذ تصمیم درختان و الگوریتم‌های SVM، تأکید بر بدون درز ادغام به سیستم‌های امنیتی شبکه رایج. سیستم پیشنهادی با استفاده از SVM، ترافیک شبکه را به صورت بلادرنگ نظارت و ارزیابی می‌کند. و دی تی طبقه بندی کننده ها شبکه ترافیک داده‌ها، که شامل فعالیت‌های مشروع و مخرب می‌شود، به عنوان ورودی عمل می‌کند. این فرآیند شامل آموزش طبقه‌بندی‌کننده‌ها بر روی یک مجموعه داده قابل توجه، پیاده‌سازی اعتبارسنجی متقابل برای تقسیم مجموعه آموزشی و آزمایشی ۷۰/۳۰ است. خروجی سیستم شامل تشخیص دقیق و کاهش حملات DDoS، با تأکید بر افزایش دقت و به حداقل رساندن خطاهای احتمالی است. نکات مثبت. تجربی پیکربندی شامل مجموعه‌ای از داده‌ها است که شامل ترافیک شبکه مشروع و مخرب است. آزمایش پیامدها تأیید کردن ‎‏ ... اثربخشی از ‎‏ ... روش پیشنهادی، تشخیص و کاهش حملات DDoS را با سطح دقت قابل توجهی نشان می‌دهد و در عین حال، موارد مثبت کاذب را نیز کاهش می‌دهد. معیارهای ارزیابی شامل دقت، صحت، فراخوانی و امتیاز F1 هستند، در حالی که معیارهای امنیتی، محرمانگی، یکپارچگی و در دسترس بودن را در نظر می‌گیرند. یافته‌های مربوط به تشخیص DDoS در SDN از طریق ML، عملکرد برتر رویکرد پیشنهادی را در مقایسه با تکنیک‌های موجود برجسته می‌کند. سهم قابل توجه این مقاله شامل یک روش مبتنی بر یادگیری ماشین است که الگوریتم‌های SVM و DT را برای DDoS متحد می‌کند. تشخیص در اس دی ان. پیشنهادی سیستم به عنوان یک مکانیسم دفاعی عملی در برابر حملات DDoS ظاهر می‌شود و ادغام یکپارچه‌ای را در سیستم‌های امنیتی شبکه معاصر نشان می‌دهد. تلاش‌های آینده ممکن است روش‌های پیچیده‌تری را برای شناسایی و کاهش حملات DDoS، صرف نظر از نیاز به انتخاب دقیق ویژگی‌ها، بررسی کنند. و پتانسیل داده‌ها بیش‌برازش به عنوان ذاتی محدودیت‌ها. در اصل، این مقاله مسیری امیدوارکننده برای تشخیص و کاهش حملات DDoS در SDN، با استفاده از تکنیک‌های یادگیری ماشین برای ارائه یک بهبود مقیاس‌پذیر و کارآمد برای چشم‌انداز امنیتی شبکه‌های مبتنی بر SDN.

فنگ و همکاران [[21]](#_bookmark37) با تمرکز بر حوزه SDN، به کاوش در این حوزه می‌پردازد. در مورد ادغام یادگیری ماشین برای تشخیص حملات DDoS. هدف اصلی، مقابله با پیچیدگی‌های امنیتی ذاتی در SDN با ارائه یک مدل ترکیبی است. استخدام کی ان ان و ماشین بردار پشتیبان الگوریتم‌ها برای حمله شدید تشخیص. تحقیق چنگ زدن‌ها با ‎‏ ... آسیب‌پذیری SDN در برابر حملات DDoS، که عمدتاً از صفحه کنترل متمرکز آن ناشی می‌شود و به طور بالقوه منجر به ناتوانی شبکه می‌شود. راه‌حل‌های فعلی شامل SVM، KNN و آر اف الگوریتم‌ها برای حملات انسداد سرویس (DDOS) حمله شناسایی درون

اس دی ان. مطالعه تلاش می‌کند به مشارکت توسط طرفداری کردن الف ترکیبی SVM-KNN رویکرد، هدف گیری به بالا بردن تشخیص دقت، کاهش موارد مثبت کاذب و ساده‌سازی فواصل تشخیص. سیستم پیشنهادی از اطلاعات سرآیند بسته به عنوان ورودی خود استفاده می‌کند و از استخراج ویژگی و SVM- KNN بهره می‌برد. الگوریتم برای آموزش و طبقه بندی. رویه مستلزم آن است ‎‏ ... مدت زمان از محوری ترافیک ویژگی‌ها، مدل آموزش، و طبقه‌بندی ترافیک شبکه به دسته‌های عادی یا حمله DDoS. این سیستم نتایج تشخیص حمله DDoS را با دقت افزایش یافته و نرخ‌های مثبت کاذب کاهش یافته ارائه می‌دهد. راه‌اندازی آزمایشی شامل تجزیه و تحلیل مقایسه‌ای SVM- KNN پیشنهادی بود. مدل علیه موجود ماشین بردار پشتیبان، کی ان ان، و آر اف الگوریتم‌ها. معیارهای ارزیابی شامل دقت، نرخ هشدار اشتباه، و زمان‌های تشخیص، در کنار معیارهای امنیتی مربوط تشخیص حمله DDoS در SDN از طریق یادگیری ماشین. یافته‌ها به نمایش گذاشته شده ‎‏ ... برتری از ‎‏ ... مدل SVM- KNN نسبت به الگوریتم‌های موجود، دقت بهبود یافته، نرخ مثبت کاذب پایین‌تر و زمان تشخیص نسبتاً کمتری را در مقایسه با مدل‌های SVM و KNN نشان می‌دهد. تحقیق باعث می‌شود قابل توجه مشارکت‌ها توسط معرفی یک هیبریدی ماشین بردار پشتیبان (SVM)-KNN مدل برای حملات انسداد سرویس (DDOS) حمله تشخیص در SDN، به نمایش گذاشتن مرتفع عملکرد معیارها مانند دقت و کاهش نرخ مثبت کاذب. تلاش‌های آینده ممکن است شامل کردن بیشتر پالایش ‎‏ ... مدل و آزمایش کردن آن در معتبر شبکه SDN محیط‌ها. پتانسیل محدودیت‌ها می‌تواند تقاضا برای داده‌های آموزشی گسترده و چالش‌های مقیاس‌پذیری در سناریوهای شبکه گسترده را در بر بگیرد.

بالا و همکاران [[22]](#_bookmark38) به حوزه تشخیص می‌پردازد حملات DDoS در چارچوب SDN از طریق پیاده‌سازی یک رویکرد مبتنی بر یادگیری ماشین. پرداختن به آسیب‌پذیری SDN در برابر تهدیدات امنیتی، به‌ویژه حملات DDoS، دغدغه اصلی این مطالعه است و بر ... تأکید دارد. بحرانی پیامدها برای ‎‏ ... آینده از اینترنت فناوری. راهکارهای فعلی، مانند فایروال‌ها، سیستم‌های تشخیص نفوذ، و شبکه نظارت ابزارها، هستند مورد بررسی قرار گرفت در چارچوب SDN. با این حال، معماری منحصر به فرد SDN ژست‌ها چالش‌ها برای اینها سنتی امنیت اقدامات، ایجاب می‌کند نوآورانه رویکردها. تحقیق اهداف شامل ارزیابی طبقه‌بندی‌کننده‌های مختلف یادگیری ماشین برای تشخیص و تحلیل کردن حملات انسداد سرویس (DDOS) حملات در یک SDN محیط زیست. مطالعه​ مشارکت می‌کند توسط انجام دادن الف مقایسه‌ای تحلیل عملکرد برای شناسایی موثرترین تکنیک‌ها برای تشخیص DDoS. سیستم پیشنهادی با جمع‌آوری و پیش‌پردازش داده‌ها از یک مجموعه داده تعیین‌شده و تبدیل آن به یک قالب تمیز و ساختاریافته آغاز می‌شود. انتخاب ویژگی اجرا می‌شود. مبتنی بر روی مجموعه داده‌ها ویژگی اهمیت، و تقسیم‌بندی بعدی به مجموعه‌های آموزشی و آزمایشی به شرح زیر است. یادگیری ماشین الگوریتم‌ها، از جمله ماشین بردار پشتیبان، دی تی، ال آر، آر اف، و KNN، هستند شاغل به تشخیص دادن حملات انسداد سرویس (DDOS) حملات. میلی لیتر این مدل برای ادغام در کنترل‌کننده SDN جهت نظارت مداوم بر ترافیک شبکه و تشخیص DDoS طراحی شده است. تجربی راه اندازی ارزیابی می‌کند دستگاه یادگیری طبقه‌بندی‌کننده‌هایی مانند SVM، RF، DT، LR و KNN برای شناسایی و تحلیل حملات DDoS در یک محیط SDN. نتایج شامل موارد زیر است عملکرد معیارها مانند دقت، دقت،

یادآوری، امتیاز F1 و سطح زیر منحنی ROC (ROC-AUC). امنیت معیارها ممکن است شامل شدن نادرست مثبت نرخ، نرخ منفی کاذب و نرخ تشخیص. یافته‌ها نشان می‌دهد که برخی طبقه‌بندی‌کننده‌ها دستیابی به بالا به ۱۰۰٪ دقت، و ‎‏ ... عملکرد است اعتبارسنجی شده با استفاده از ‎‏ ... ROC-AUC منحنی. این این مطالعه با ارزیابی طبقه‌بندی‌کننده‌های یادگیری ماشین برای تشخیص DDoS در SDN و تعیین مؤثرترین تکنیک‌ها، مشارکت می‌کند. برای این هدف. آینده کار ممکن است شامل کردن اصلاح بیشتر مدل‌های یادگیری ماشین و ادغام یکپارچه آنها به کنترل‌کننده‌های SDN. محدودیت‌ها، از جمله ویژگی‌های خاص دامنه ، مورد تأیید قرار گرفته‌اند که بر کاربردپذیری مدل در زمینه‌های متنوع تأثیر می‌گذارند.

الاشهب و ال. [[23]](#_bookmark39) معرفی می‌کند الف پیشرفته رویکرد برای تشخیص حملات انکار سرویس توزیع‌شده (LDDoS) با نرخ پایین در SDN با استفاده از یک مدل یادگیری ماشین آنلاین پیشرفته. این مدل یک بهینه‌ساز گرادیان نزولی تصادفی و یک طبقه‌بندی‌کننده ماشین تقویت‌کننده قابل توضیح (EBM) را ادغام می‌کند و امکان پردازش بلادرنگ ترافیک شبکه را فراهم می‌کند. سیستم در یک محیط شبیه‌سازی‌شده SDN ارزیابی شد. با استفاده از مینی‌نت و ‎‏ ... ریو کنترل کننده، دقت قابل توجهی را نشان می‌دهد و از روش‌های موجود در تشخیص حمله LDDoS پیشی می‌گیرد. این مطالعه بر کاربرد تشخیص حملات LDDoS در شبکه‌های مبتنی بر SDN، با استفاده از فناوری‌های پیشرفته یادگیری ماشین و یادگیری عمیق، تمرکز دارد. پرداختن به مسئله مهم LDDoS حملات در مبتنی بر SDN شبکه‌ها، ‎‏ ... کاغذ به ناکارآمدی روش‌های تشخیص مرسوم، به‌ویژه در شناسایی حملات با نرخ ترافیک پایین که اغلب نادیده گرفته می‌شوند، اذعان می‌کند. استاندارد رویکردها. تحقیق هدف است به معرفی یک مدل یادگیری ماشین آنلاین که قادر به پردازش مقادیر قابل توجهی از داده‌های ترافیک شبکه به صورت بلادرنگ و در عین حال به‌روزرسانی پویا پارامترهای مدل باشد. روش‌های موجود، چنین به عنوان ماشین بردار پشتیبان، تشخیص درخت، ساده‌لوح بیز و ماشین فاکتورگیری برای تشخیص LDDoS مورد استفاده قرار گرفته‌اند. اما ‎‏ ... کاغذ طرح کلی آنها محدودیت‌ها. در حالی که برخی از رویکردها از مدل‌های ترکیبی مانند CNN-LSTM استفاده می‌کنند، اما چالش‌ها همچنان پابرجا هستند، از جمله مجموعه داده‌های قدیمی، نیازهای منابع فشرده و ناکارآمدی بالقوه در سناریوهای عملی. پیشنهادی سیستم پیشگامان یک آنلاین مدل یادگیری ماشینی که از نزول گرادیان تصادفی و مدل مبتنی بر انرژی (EBM) برای تشخیص مؤثر حملات LDDoS در شبکه‌های مبتنی بر SDN استفاده می‌کند. این مدل که به صورت بلادرنگ عمل می‌کند، پارامترها را از طریق SGD به صورت تدریجی به‌روزرسانی می‌کند و ... تفسیرپذیری از طریق ای بی ام، ارائه بینش‌ها به مشارکت‌ها و تعاملات ویژگی‌ها که بر پیش‌بینی‌ها تأثیر می‌گذارند. ارزیابی درون یک شبیه‌سازی‌شده با SDN محیط زیست، استفاده از مجموعه داده‌هایی مانند CICIDS 2017، CICDDoS2019، MQTT و یک مجموعه داده سفارشی، برتری مدل پیشنهادی را نشان می‌دهد. معیارهای عملکرد، از جمله دقت، صحت، فراخوانی، امتیاز F1، و AUC، همراه با امنیت معیارهایی مانند نرخ مثبت واقعی (TPR)، نرخ مثبت کاذب (FPR)، نرخ منفی واقعی (TNR) و نرخ منفی کاذب (FNR) قابلیت‌های استثنایی مدل را برجسته می‌کنند. نکته قابل توجه این است که مدل به دست آمده یک دقت از ۹۹٪، الف دقت از ۹۹٪، الف به یاد بیاورید از ۹۹٪، یک امتیاز F1 از ۹۹٪، و یک AUC از ۹۹٪. تجربی​ راه اندازی شاغل مینی‌نت و ‎‏ ... ریو کنترل کننده

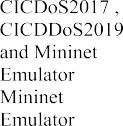
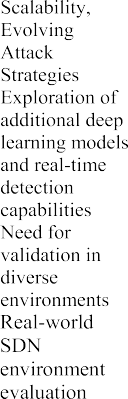
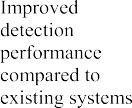
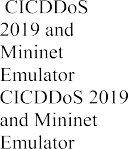
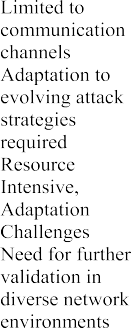
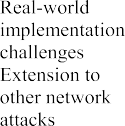
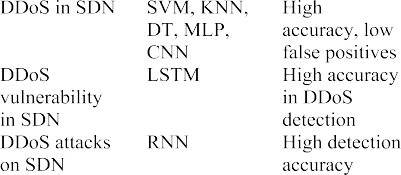
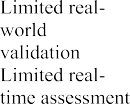
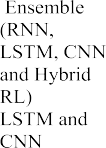
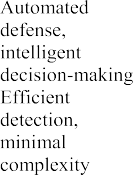
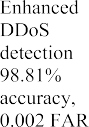
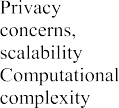
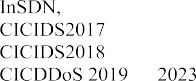
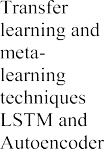
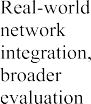
برای شبیه‌سازی یک شبکه مبتنی بر SDN، با مجموعه داده‌هایی مانند CICIDS ۲۰۱۷، CICDDoS2019، ام کیو تی تی، و الف سفارشی مجموعه داده برای اهداف آموزشی و ارزیابی. مدل یادگیری ماشین آنلاین پیشنهادی، با ادغام نزول گرادیان تصادفی و EBM، به عنوان یک راه حل پیشگامانه برای تشخیص حمله LDDoS در شبکه‌های مبتنی بر SDN ظاهر می‌شود. این مدل برجسته است. عملکرد در الف شبیه‌سازی شده محیط زیست بر کاربرد عملی بالقوه آن تأکید می‌کند. مشارکت‌ها شامل توسعه یک مدل آنلاین برای تشخیص LDDoS، همراه با شفافیت و قابلیت تفسیر ارائه شده است. توسط ای بی ام. آینده تلاش ها شامل کردن دنیای واقعی آزمایش، ارزیابی سناریوهای حمله گسترده‌تر، و کاوش الگوریتم‌های یادگیری ماشین آنلاین جایگزین. محدودیت‌های اذعان شده شامل آزمایش محیط شبیه‌سازی شده و ارزیابی انحصاری در مورد حملات LDDoS است.

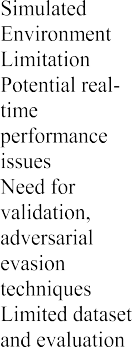
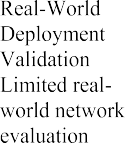
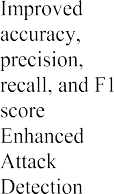
الموهگری و همکاران [[24]](#_bookmark40) به حوزه امنیتی SDNها در رابطه با تهدید حملات DDoS می‌پردازد. این مطالعه بر استفاده از الگوریتم‌های یادگیری ماشین تأکید دارد. برای تقویت قابلیت‌های تشخیص حمله DDoS در SDNها. ‎‏ ... بحرانی مسئله از SDN کنترل کننده آسیب‌پذیری در برابر حملات DDoS؛ این تحقیق خطرات امنیتی بالقوه برای زیرساخت شبکه گسترده‌تر را برجسته می‌کند. در حالی که موجود است راه حل ها شامل شدن سنتی مبتنی بر قاعده روش‌ها و ناهنجاری تشخیص، آنها اثربخشی متزلزل می‌شود علیه حملات DDoS پیچیده و در حال تکامل. هدف اصلی این تحقیق ارزیابی اثربخشی الگوریتم‌های یادگیری ماشین - به طور خاص، ایکس‌جی‌بوست، آر اف، و دی تی در تشخیص حملات DDoS در SDNها. این مطالعه در پی پیشبرد توسعه سیستم‌های تشخیص DDoS قوی و دقیق است. متناسب سازی شده برای SDN محیط‌ها. پیشنهادی سیستم، داده‌های جریان ترافیک SDN را از طریق الگوریتم‌های انتخاب ویژگی و یادگیری ماشین (XGBoost، RF و DT) پردازش می‌کند. نتیجه شامل دسته‌بندی ترافیک شبکه به حالت عادی است. و حملات انسداد سرویس (DDOS) حمله طبقه بندی ها مبتنی بر روی ‎‏ ... مدل‌های آموزش دیده بهره گیری ‎‏ ... CICDDoS2019 مجموعه داده‌ها، ‎‏ ... عملکرد اندازه‌گیری‌شده با آزمایش با استفاده از معیارهایی مانند دقت، یادآوری، دقت، و امتیاز F1. امنیت معیارها، از جمله نرخ تشخیص ، نرخ مثبت کاذب و نرخ منفی کاذب نیز در نظر گرفته شدند. این مطالعه دقت و نرخ بازیابی قابل توجهی را برای تشخیص حمله DDoS از طریق مدل‌های یادگیری ماشین پیشنهادی نشان داد. به طور خاص، XGBoost بالاترین دقت را با 99.94٪ نشان داد و به بازیابی، دقت و امتیاز F1 کاملی دست یافت. سهم این مطالعه شامل موارد زیر است : به نمایش گذاشتن ‎‏ ... اثربخشی از دستگاه یادگیری الگوریتم‌ها، به ویژه ایکس‌جی‌بوست، در دقیق حملات انسداد سرویس (DDOS) حمله تشخیص درون SDN ها. آینده تلاش ها باید تمرکز روی دنیای واقعی ارزیابی سناریوها و توسعه مدل‌های تطبیقی و خودآموز برای تشخیص DDoS در زمان واقعی. محدودیت‌ها شامل لزوم ارزیابی بیشتر در محیط‌های شبکه عملی است. این بررسی جامع دانشگاهی، بینش‌های ارزشمندی در مورد کاربرد یادگیری ماشین برای تشخیص DDoS در SDNها، کپسوله‌سازی مشارکت‌ها، مسیرها و ... ارائه می‌دهد. برای آینده تحقیق، و به رسمیت شناخته شده محدودیت‌ها در روش‌شناسی پیشنهادی.

دهکردی و همکاران [[25]](#_bookmark41) در معرفی یک رویکرد جدید کاوش کنید برای تشخیص حملات انسداد سرویس (DDOS) حملات درون شبکه SDN توسط

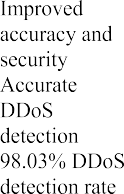


**جدول ۳.** قبلی تحقیق خلاصه از عمیق یادگیری راه حل ها



**جدول ۳.** *(ادامه دارد.)* قبلی تحقیق خلاصه از عمیق یادگیری راه حل ها



استخدام الف ترکیب از دستگاه یادگیری و تکنیک‌های آماری. دامنه فناوری شامل امنیت شبکه، SDN معماری، و ‎‏ ... پیاده‌سازی از الگوریتم‌های مختلف یادگیری ماشین. این مطالعه به محدودیت‌های آشکار در روش‌های تشخیص DDoS موجود در SDN پاسخ می‌دهد. توسط پیشنهاد دادن یک پیشرفته روش‌شناسی که از نظر دقت، از رویکردهای مرسوم پیشی می‌گیرد. دغدغه اصلی از این مطالعه است ‎‏ ... ضروری نیاز برای بیشتر مکانیسم‌های مؤثر تشخیص DDoS در SDN برای مقابله با تهدید فزاینده ناشی از حملات DDoS. تشخیص DDoS سنتی روش‌ها، اگرچه تأسیس شده، ممکن است نه تراز کردن خوب با ‎‏ ... پویا و انعطاف‌پذیر طبیعت از SDN اهداف تحقیق به صورت معرفی روشی جدید که قادر به شناسایی حملات DDoS با حجم بالا و کم در SDN است، با بهره‌گیری از هم‌افزایی تکنیک‌های آماری و یادگیری ماشینی، تشریح شده است. سهم قابل توجه این مطالعه در ارائه یک رویکرد نوآورانه برای تشخیص DDoS در SDN و ارزیابی عملکرد آن نهفته است. علیه موجود روش‌ها. پیشنهادی سیستم آغاز می‌شود با ‎‏ ... مجموعه از شبکه ترافیک داده‌ها، و به دنبال آن یک تحلیل مبتنی بر آنتروپی که برای آشکار کردن الگوهای غیرعادی نشان‌دهنده حملات احتمالی DDoS طراحی شده است. یک فرآیند طبقه‌بندی بعدی، حملات شناسایی شده را به طور دقیق برچسب‌گذاری می‌کند. سیستم داده‌های ترافیک شبکه را به عنوان ورودی دریافت می‌کند، اجرا می‌کند مبتنی بر آنتروپی تحلیل و طبقه بندی، در نهایت، شناسایی حملات DDoS با دقت بالا را فراهم می‌کند. مرحله آزمایش شامل اعمال روش پیشنهادی بود به مجموعه داده‌ها چنین به عنوان UNB-ISCX، سی‌تی‌یو-۱۳، و ISOT. معیارهای عملکرد، شامل دقت، صحت، فراخوانی و امتیاز F1، در کنار معیارهای امنیتی مانند ... در نظر گرفته شدند. به عنوان اف پی آر و اف ان آر. پیامدها نشان داده شده که

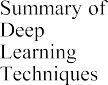


روش پیشنهادی از نظر دقت در تشخیص حملات DDoS در SDN از راه‌حل‌های موجود پیشی گرفت. محوری مشارکت‌ها شامل شدن ‎‏ ... توسعه یک روش پیشرفته برای تشخیص DDoS در SDN، که دقت بالاتری را در مقایسه با روش‌های مرسوم نشان می‌دهد. آینده‌نگر تحقیق راه‌ها ممکن است شامل شدن بیشتر تنظیم دقیق ‎‏ ... پیشنهادی روش و آن کاربرد در دنیای واقعی محیط‌های SDN . این مطالعه به محدودیت‌ها، به ویژه تمرکز آن بر تشخیص حملات DDoS توسط یک کنترل‌کننده واحد، اذعان دارد. در SDN، که نشان‌دهنده فرصت‌هایی برای بهبود و گسترش کاربردپذیری این روش در شبکه‌هایی با چندین کنترل‌کننده است.

1. **تشخیص ناهنجاری شبکه با استفاده از یادگیری عمیق تکنیک‌ها**

شبکه‌های مدرن هستند و نیازمند رویکردهای نوآورانه برای تشخیص به موقع و دقیق می‌باشند. این بخش به بررسی انبوهی از الگوریتم‌های DL می‌پردازد. که اثبات شده کارایی به عنوان الف نوشدارو در این توجه (ببینید) شکل [۶](#_bookmark16) )، همراه با الف خلاصه میز هدف گیری به ارائه یک جامع نمای کلی از ‎‏ ... فعلی روندها در این دامنه (به جدول [3 مراجعه کنید)](#_bookmark15) ).

لازاریس و ال. [[26]](#_bookmark42) معرفی می‌کند الف رمان سیستم برای تشخیص حملات انکار سرویس توزیع‌شده (DDoS) در شبکه‌های نرم‌افزار محور (SDN) از طریق کاربرد یادگیری عمیق (DL). هدف این سیستم غلبه بر چالش‌های مرتبط با حملات DDoS در SDN با مهار ... دی ال ها قابلیت‌ها برای تشخیص و کاهش. این مقاله به بررسی امنیت شبکه و حوزه SDN می‌پردازد و بر اهمیت پرداختن به تهدیدات DDoS تأکید می‌کند. اولیه تمرکز از این کاغذ است ‎‏ ... شناسایی و



**شکل ۶.** خلاصه از عمیق یادگیری تکنیک‌ها.

کاهش از حملات انسداد سرویس (DDOS) حملات درون SDN، اذعان عمده امنیت تهدید آنها ژست گرفتن. در حالی که شبکه SDN پیشنهادات الف اگرچه پلتفرم مدیریت شبکه انعطاف‌پذیر و مقیاس‌پذیر است، اما ماهیت پویای آن، وظیفه تشخیص و کاهش مؤثر حملات DDoS را پیچیده می‌کند. راه‌حل‌های موجود، مانند تشخیص مبتنی بر جریان، مبتنی بر امضا و مبتنی بر ناهنجاری، محدودیت‌هایی دارند. در اصطلاحات از دقت، مقیاس‌پذیری، و سازگاری . مرکزی هدف از این کاغذ است به پیشنهاد دادن الف مبتنی بر DL سیستمی برای تشخیص DDoS در SDN که از محدودیت‌ها فراتر می‌رود از راه‌حل‌های موجود. مشارکت‌ها شامل طراحی و پیاده‌سازی این سیستم مبتنی بر DL و ارزیابی تجربی عملکرد آن است. سیستم مبتنی بر DL شامل سه جزء کلیدی است: جمع‌آوری داده‌ها، استخراج ویژگی، و مبتنی بر DL طبقه بندی. شبکه ترافیک داده‌های سوئیچ‌های SDN به عنوان ورودی عمل می‌کنند و برای استخراج ویژگی‌های مربوطه مانند اندازه بسته، نرخ بسته و مدت زمان جریان، پیش‌پردازش می‌شوند. سپس این ویژگی‌ها به یک سیستم مبتنی بر DL وارد می‌شوند. طبقه بندی کننده، آموزش دیده به به طور موثر شناسایی حملات انسداد سرویس (DDOS) حملات. تنظیمات آزمایشی شامل یک شبکه SDN شبیه‌سازی شده است که در معرض حملات مختلف DDoS قرار گرفته است. معیارهای عملکرد عبارتند از: تشخیص دقت، نادرست مثبت نرخ، و زمان تشخیص، با معیارهای امنیتی که نرخ تشخیص حمله، حمله را پوشش می‌دهند کاهش نرخ، و حمله تأثیر. نتایج اثربخشی سیستم را در تشخیص و کاهش بلادرنگ، با دستیابی به دقت بالا و نرخ مثبت کاذب پایین در انواع مختلف حمله DDoS نشان دهید . مشارکت‌های این مقاله شامل موارد زیر است: ‎‏ ... پیاده‌سازی از الف مبتنی بر DL سیستم برای تشخیص DDoS در SDN و ارزیابی تجربی آن، اثربخشی در کاهش حملات را با دقت بالا نشان می‌دهد. کارهای آینده مستلزم ادغام در دنیای واقعی و ارزیابی عملکرد تحت شرایط مختلف شبکه است. محدودیت‌ها شامل موارد زیر است: ‎‏ ... استفاده از الف شبیه‌سازی شده شبکه محیط زیست و دامنه ارزیابی تجربی.

چوانگ و ال. [[27]](#_bookmark43) کاوش می‌کند به ‎‏ ... قلمرو از SDN، با تمرکز بر اعمال نفوذ انتقال یادگیری رویکردها به افزایش نفوذ تشخیص. تکنولوژیکی منظره شامل می‌شود استفاده از روش‌های یادگیری عمیق در معماری SDN به آدرس امنیت چالش‌ها ذاتی در مدیریت متمرکز شبکه. مسئله اصلی که در این تحقیق به آن پرداخته شده است است ‎‏ ... ضروری نیاز به تقویت کردن نفوذ قابلیت‌های تشخیص در محیط‌های SDN، به ویژه در شناسایی حملات DDoS. در حالی که راه‌حل‌های موجود شامل مدل‌های طبقه‌بندی سنتی، تکنیک‌های یادگیری عمیق و سیستم‌های دفاعی SDN با استفاده از تحلیل جریان هستند، چالش‌های مداوم، از جمله داده‌های آموزشی ناکافی، نابرابری در توزیع داده‌ها و ظرفیت‌های محاسباتی متفاوت، همچنان پابرجا هستند . هدف اصلی این تحقیق، اعمال یادگیری انتقالی است. روش‌شناسی‌ها به افزایش ‎‏ ... اثربخشی از تشخیص نفوذ سیستم‌ها درون شبکه SDN تنظیمات. مشارکت‌ها شامل معرفی یک رویکرد یادگیری انتقالی برای غلبه بر محدودیت‌های مرتبط با سیستم‌های تشخیص نفوذ رایج است که در نهایت طبقه‌بندی خودکار ترافیک غیرطبیعی را به انواع حمله متمایز بهبود می‌بخشد. سیستم پیشنهادی از یادگیری انتقالی برای جذب دانش از ... استفاده می‌کند. متفرق منبع دامنه‌ها، پالایش ‎‏ ... عملکرد مدل‌های طبقه‌بندی مرسوم در دامنه هدف. داده‌های ترافیک شبکه به عنوان ورودی عمل می‌کنند و تحت یادگیری انتقالی قرار می‌گیرند. فرآیند به تقویت کردن ‎‏ ... نفوذ تشخیص مدل. سیستم خروجی آشکار می کند به عنوان یک ارتقا یافته نفوذ سیستم تشخیص ماهر در دسته‌بندی ترافیک غیرطبیعی به حملات متنوع انواع. تجربی پیکربندی‌ها درگیر ‎‏ ... استفاده از عموم قابل دسترسی شبکه SDN مجموعه داده‌ها، به دست آمده از ‎‏ ... نویسندگان اصلی وب‌سایت‌ها عملکرد معیارها، از جمله دقت، صحت، فراخوانی و امتیاز F1 در کنار معیارهای امنیتی مانند نرخ تشخیص، نرخ مثبت کاذب و نرخ منفی کاذب در نظر گرفته شدند. نتایج آزمایش تأکید می‌کند اثربخشی رویکرد یادگیری انتقالی پیشنهادی در تقویت حملات انسداد سرویس (DDOS) تشخیص درون اس دی ان. مدل دقت، صحت و یادآوری بالاتری در شناسایی DDoS نشان داد. حملات چه زمانی مقایسه شده به متعارف مدل‌های طبقه‌بندی. نکته‌ی اصلی این مطالعه ارائه‌ی یک مدل یادگیری انتقالی است. رویکرد به بالا بردن نفوذ تشخیص درون مناظر SDN ، با الف خاص تمرکز روی مبارزه کردن حملات انسداد سرویس (DDOS) حملات. کار بعدی ممکن است شامل ارزیابی‌های گسترده در محیط‌های مختلف SDN و گنجاندن امنیت اضافی باشد. معیارها محدودیت‌ها زیرخط دار ‎‏ ... ضرورت برای ارزیابی کامل رویکرد پیشنهادی در دنیای واقعی شبکه SDN پیاده‌سازی‌ها این جامع کار آکادمیک، دیدگاهی جامع ارائه می‌دهد که حوزه‌های کاربردی را در بر می‌گیرد، تحقیق چالش‌ها، موجود راه حل ها، اهداف، روش‌شناسی، بینش‌های تجربی و ملاحظات آینده‌نگر .

السید و همکاران [[28]](#_bookmark44) با استفاده از یک روش انتخاب ویژگی، به حوزه تشخیص ناهنجاری مبتنی بر جریان می‌پردازد. برای مبارزه با حملات DDoS در SDNها. این مطالعه به بررسی حوزه کاربرد و فناوری به‌کارگیری تکنیک‌های یادگیری عمیق برای تشخیص حمله DDoS در محیط‌های SDN می‌پردازد. آزمایش دقیق بر روی مجموعه داده‌های مبتنی بر جریان معیار، یعنی InSDN، CICIDS2017، و CICIDS2018،

اثربخشی سیستم را در کاهش پیچیدگی مدل نشان می‌دهد. بدون سازشکارانه دقت. کانونی نکته‌ی اصلی این مقاله، شناسایی حملات DDoS در محیط‌های SDN است که به نگرانی‌های امنیتی فزاینده‌ی ناشی از ظهور فناوری SDN می‌پردازد. راه‌حل‌های موجود به سمت استفاده از تکنیک‌های یادگیری ماشین و یادگیری عمیق گرایش دارند. برای ناهنجاری تشخیص سیستم‌ها. با این حال، ‎‏ ... اثربخشی اینها مدل‌ها است به طور پیچیده گره خورده به ‎‏ ... کیفیت از ‎‏ ... مجموعه داده‌های آموزشی. این مقاله به دنبال کاهش افزونگی یا بی‌ربط بودن ویژگی‌ها بدون به خطر انداختن دقت طبقه‌بندی حیاتی برای تشخیص DDoS است. با استفاده از دو انتخاب ویژگی روش‌ها، یعنی اطلاعات سود (اینگرید) و آر اف، سیستم پیشنهادی، مرتبط‌ترین ویژگی‌های حمله DDoS را شناسایی می‌کند. درون هر کدام مجموعه داده‌ها. قلب از ‎‏ ... سیستم در یک فرآیند IDS مبتنی بر یادگیری عمیق نهفته است که بر اساس DDoSnet ساخته شده است. مدل و یکپارچه‌سازی ویژگی انتخاب رویکردها. عملیاتی روی مبتنی بر جریان مجموعه داده‌ها، ‎‏ ... سیستم استخدام می‌کند انتخاب ویژگی روش‌ها به اشاره کردن ‎‏ ... بیشترین مربوطه حملات انسداد سرویس (DDOS) ویژگی‌های حمله. این ویژگی‌های انتخاب‌شده سپس به مبنایی برای آموزش یک فرآیند IDS مبتنی بر یادگیری عمیق تبدیل می‌شوند و قابلیت‌های مدل DDoSnet قبلی را گسترش می‌دهند. خروجی نهایی سیستم، شناسایی حملات DDoS در محیط‌های SDN است. چارچوب آزمایشی مستلزم موارد زیر است: در معرض قرار دادن ‎‏ ... پیشنهادی سیستم به سخت‌گیرانه آزمایش روی سه معیار مبتنی بر جریان مجموعه داده‌ها – InSDN، CICIDS2017، و CICIDS2018. عملکرد معیارها، از جمله دقت، صحت، فراخوانی، امتیاز F1 و AUC، همراه با معیارهای امنیتی مانند نرخ تشخیص، نرخ مثبت کاذب و نرخ منفی کاذب، مورد بررسی دقیق قرار می‌گیرند. خوشبختانه، نتایج، مهارت سیستم در کاهش پیچیدگی مدل بدون به خطر انداختن دقت را تأیید می‌کند و تشخیص بالایی را نشان می‌دهد. نرخ‌ها، و بهینه سازی ‎‏ ... مدل‌سازی زمان. رویکرد یادگیری عمیق، عملکرد کنترلر را بدون افت قابل توجه حفظ می‌کند. مشارکت‌های این مقاله چندوجهی هستند و یک رویکرد تشخیص ناهنجاری مبتنی بر جریان قوی را با یک روش انتخاب ویژگی متناسب با کاهش حمله DDoS در SDNها معرفی می‌کنند. با استفاده از تکنیک‌های یادگیری عمیق، سیستم پیشنهادی نه تنها به نرخ تشخیص و کارایی بالایی دست می‌یابد، بلکه پایه‌ای برای کاوش‌های آینده در کاربردهای امنیتی گسترده‌تر ایجاد می‌کند. درون شبکه SDN محیط‌ها. همانطور که راه‌ها برای نویسندگان برای کارهای آینده پیشنهاد می‌کنند که آزمایش‌ها به مجموعه داده‌های اضافی گسترش یابد و کاربرد وسیع‌تر تکنیک‌های یادگیری عمیق در سناریوهای مختلف امنیتی SDN بررسی شود. ‎‏ ... مطالعه محدودیت‌ها، از جمله ‎‏ ... دامنه مجموعه داده‌ها و عدم مقایسه با روش‌های انتخاب ویژگی جایگزین، نکات ظریفی را به یافته‌ها اضافه می‌کند.

چن و ال. [[29]](#_bookmark45) کاوش می‌کند به ‎‏ ... کاربرد و حوزه فناوری مربوط به تشخیص و دفاع در برابر حملات DDoS در محیط‌های SDN، با استفاده از یادگیری عمیق پیشرفته تکنیک‌ها. مطالعه آدرس‌ها ‎‏ ... ذاتی آسیب پذیری از شبکه SDN محیط‌ها به حملات انسداد سرویس (DDOS) حملات، با تأکید بر ضروری برای مقاوم تشخیص و دفاع اگرچه روش‌های سنتی وجود دارند، اما ممکن است در مقابله با ماهیت پویای حملات DDoS در محیط‌های SDN ناکارآمد باشند. اولیه هدف است به معرفی کردن یک نوآورانه

شبکه باور عمیق تخاصمی (DBN) - حافظه کوتاه مدت بلند مدت (LSTM) چارچوب برای حملات انسداد سرویس (DDOS) حمله تشخیص و دفاع در اس دی ان. قابل توجه، ‎‏ ... مشارکت‌ها شامل کردن پیشگام​ الف عمیق مبتنی بر یادگیری رویکرد به تقویت کردن شبکه SDN کنترل‌کننده‌ها در برابر تهدیدات DDoS. سیستم پیشنهادی شامل چهار ماژول است: داده‌ها مجموعه، داده‌ها پردازش، خصمانه یادگیری عمیق ناهنجاری تشخیص، و غیرطبیعی دفاع. این شامل جمع‌آوری داده‌ها از سوئیچ‌های فیزیکی و مجازی، تبدیل غیر عددی ویژگی‌ها به عددی فرم، و استقرار یک خصمانه DBN-LSTM چارچوب برای حمله DDoS شناسایی و کاهش. سیستم خروجی هدف آن محافظت از کنترل‌کننده‌های SDN با شناسایی و خنثی کردن حملات DDoS است. در این آزمایش، از یک مجموعه داده با ... استفاده شد. بیش از ۸۰ ویژگی‌ها، فراگیر ۵۰۰۰۶۲۴۹ حملات انسداد سرویس (DDOS) حملات و ۵۶۸۶۳ نمونه نرمال. معیارهای ارزیابی، از جمله دقت، دقت، به یاد بیاورید، و اف۱ امتیاز، بودند در نظر گرفته شده، همراه با امنیت معیارها سنجش ‎‏ ... سیستم توانایی تشخیص حملات DDoS خصمانه و اثربخشی استراتژی‌های دفاعی غیرطبیعی. نتایج، دقت قابل توجه ۹۶.۵۵٪ را در تشخیص حملات DDoS نشان داد که از روش‌های یادگیری عمیق جایگزین پیشی می‌گیرد. علاوه بر این، این سیستم حساسیت کمتری به حملات خصمانه نشان داد که بر اثربخشی آن در تشخیص و دفاع در برابر حملات DDoS در محیط‌های SDN تأکید دارد. سهم این مطالعه شامل آغاز یک ... عمیق مبتنی بر یادگیری استراتژی برای حملات انسداد سرویس (DDOS) تشخیص و دفاع در شبکه SDN محیط‌ها. آینده تلاش ها ممکن است شامل پالایش باشد ‎‏ ... پیشنهادی سیستم و آدرس‌دهی محدودیت‌ها مانند مقیاس‌پذیری و استقرار بلادرنگ. در دسترس نبودن مجموعه داده‌ها به دلیل نگرانی‌های مربوط به حریم خصوصی، به عنوان یک محدودیت مطرح است که به طور بالقوه بر تکرارپذیری نتایج تأثیر می‌گذارد. تحقیقات بیشتر به ‎‏ ... مقیاس‌پذیری و زمان واقعی عملکرد از سیستم پیشنهادی تضمین شده است.

فان و ال. [[30]](#_bookmark46) معرفی می‌کند الف پیشگامانه سیستم تشخیص ناهنجاری مبتنی بر هوش مصنوعی/یادگیری ماشین ، به نام DEEP GUARD، برای شبکه‌های مبتنی بر SDN طراحی شده است. سیستم پیشنهادی با بهره‌گیری از یادگیری تقویتی عمیق، به طور ماهرانه‌ای استراتژی‌های تطبیق جریان ترافیک را یاد می‌گیرد و به طور پیشگیرانه از صفحه داده SDN در برابر خطرات اضافه بار محافظت می‌کند. این مقاله ادعاهای خود را اثبات می‌کند. با تجربی شواهد به نمایش گذاشتن ‎‏ ... اثربخشی سیستم، به ویژه در تشخیص حملات انکار سرویس توزیع‌شده (عدم سرویس توزیع‌شده) حملات. کاغذ کاوش می‌کند به ‎‏ ... حوزه تشخیص ناهنجاری در شبکه‌های مبتنی بر SDN، کپسوله‌سازی فناوری‌هایی مانند یادگیری تقویتی عمیق، ترافیک جریان نظارت، و شبکه SDN سوئیچ ها شناسایی محدودیت‌های مکانیسم‌های کنترل و مدیریت جریان ترافیک موجود در سوئیچ‌های SDN، مسئله تحقیق را تشکیل می‌دهد. با وجود راه‌حل‌های موجود مانند فشرده‌سازی و تجمیع قوانین جریان، فقدان نظارت دقیق بر جریان ترافیک همچنان ادامه دارد. هدف تحقیق بر تدوین یک مکانیسم نوآورانه برای نظارت دقیق بر جریان ترافیک، به طور خاص برای شناسایی کارآمد حملات سایبری در شبکه‌های مبتنی بر SDN، متمرکز است. DEEP GUARD شامل دو جزء جدایی‌ناپذیر است: یک مکانیسم کنترل تطبیق جریان ترافیک که از تقویت عمیق استفاده می‌کند. یادگیری و یک ناهنجاری تشخیص مکانیسم

با استفاده از الگوریتم‌های هوش مصنوعی/یادگیری ماشین. اولی استراتژی‌های پیچیده تطبیق جریان ترافیک را یاد می‌گیرد، در حالی که دومی ناهنجاری‌ها را تشخیص می‌دهد درون ‎‏ ... ترافیک جریان می‌یابد. سیستم می‌گیرد داده‌های آماری از سوئیچ‌های SDN به عنوان ورودی، که منجر به تشخیص حمله سایبری می‌شود به عنوان خروجی. انجام شده درون ‎‏ ... ماکسی نت شبیه‌ساز برای شبیه‌سازی یک شبکه مبتنی بر SDN، تنظیمات آزمایشی معیارهای عملکرد مانند دقت، صحت، فراخوانی، و امتیاز F1. امنیت معیارها احاطه شده نرخ تشخیص، نرخ مثبت کاذب و نرخ منفی کاذب. نتایج نشان‌دهنده برتری سیستم در نظارت بر جریان ترافیک و آن مهارت در محافظ SDN سوئیچ‌ها از عملکرد حمل و نقل تخریب قابل توجه، ‎‏ ... حملات انسداد سرویس (DDOS) تشخیص عملکرد از ‎‏ ... پیشنهادی سیستم است به طور برجسته برجسته شده است. مشارکت‌های این مقاله شامل تدوین یک مکانیسم پیشگام نظارت بر جریان ترافیک ریزدانه است که برای تشخیص کارآمد حملات سایبری در شبکه‌های مبتنی بر SDN طراحی شده است. این مقاله با پشتیبانی از نتایج تجربی که اثربخشی تشخیص حمله DDoS را نشان می‌دهد، خواستار کارهای آینده برای گسترش قابلیت‌های سیستم برای مقابله با حملات سایبری مختلف است. و ارزیابی کردن عملکرد در دنیای واقعی سناریوها. محدودیت‌ها شامل نیاز به داده‌های آموزشی گسترده و پیچیدگی محاسباتی مرتبط با الگوریتم یادگیری تقویتی عمیق است.

شاجی و همکاران [[31]](#_bookmark47) معرفی Deep-Discovery IDS، پیشرفته‌ترین شناسه‌ها که استخدام می‌کند شبکه عصبی مصنوعی (ANN) فناوری به شناسایی تهدیدات امنیتی در اس دی ان. این تحقیق پیشگامان الف رمان رویکردی برای تشخیص حملات DDoS به صفحه داده SDN، با استفاده از یک مدل طبقه‌بندی MLP. با دقت چشمگیر ۹۸.۸۱٪ و الف حداقل نادرست زنگ هشدار نرخ از ۰.۰۰۲، این این مدل، یک راه‌حل امیدوارکننده برای پرداختن به چالش‌های امنیتی در SDN است. چارچوب پیشنهادی Deep-Discovery IDS برای تشخیص تهدیدات امنیتی در SDN، با تمرکز ویژه بر شناسایی حملات DDoS که صفحه داده را هدف قرار می‌دهند، طراحی شده است. این مقاله به ضرورت IDS کارآمد و قوی برای شناسایی تهدیدات امنیتی در SDN، به ویژه حملات DDoS، می‌پردازد. راه‌حل‌های موجود از ... رنج می‌برند. محدودیت‌ها مرتبط به دقت، محاسباتی سربار و شفافیت. هدف IDS مبتنی بر کشف عمیق، غلبه بر این معایب است. ارائه یک قابل اعتماد و شفاف رویکرد برای تشخیص حملات انسداد سرویس (DDOS) حملات در اس دی ان. فعلی رویکردهای تشخیص DDoS در SDN شامل روش‌های مبتنی بر قانون، تکنیک‌های آماری و روش‌های مبتنی بر یادگیری ماشین است. روش‌های مبتنی بر قانون با چالش‌های مقیاس‌پذیری و سازگاری مواجه هستند. روش‌های آماری محدودیت‌هایی در دقت و ... نشان می‌دهند. محاسباتی سربار در حالی که دستگاه روش‌های مبتنی بر یادگیری نویدبخش هستند، اما نگرانی‌هایی در مورد شفافیت و تکرارپذیری مانع آنها می‌شود. هدف این مقاله معرفی یک رویکرد جدید برای تشخیص DDoS در SDN با استفاده از مدل طبقه‌بندی MLP، ارزیابی عملکرد مدل پیشنهادی از طریق مختلف معیارها، و مقایسه آن در مقابل راه‌حل‌های موجود. چارچوب IDS مبتنی بر کشف عمیق از سه مؤلفه اصلی تشکیل شده است: جمع‌آوری و پیش‌پردازش داده‌ها، ویژگی استخراج، و طبقه بندی. ترافیک شبکه داده‌ها از ‎‏ ... شبکه SDN داده‌ها هواپیما است جمع‌آوری‌شده و پیش‌پردازش‌شده​ به از بین بردن سر و صدا و بی‌ربط اطلاعات. مؤلفه اصلی تحلیل (پی سی ای) است شاغل برای ویژگی استخراج-

برای کاهش ابعاد داده‌ها. مدل طبقه‌بندی MLP، طبقه‌بندی دودویی ترافیک شبکه را به دسته‌های غیرعادی و عادی انجام می‌دهد. تنظیمات آزمایشی شامل موارد زیر است: الف شبیه‌سازی شده شبکه SDN محیط زیست با استفاده از مینی‌نت و ریو کنترل کننده. NSL-KDD مجموعه داده‌ها است استفاده شده برای آموزش و آزمایش مدل طبقه‌بندی MLP. معیارهای عملکرد شامل دقت، صحت، فراخوانی، امتیاز F1 و مساحت زیر منحنی مشخصه عملیاتی گیرنده (ROC) (AUC) می‌شود. معیارهای امنیتی شامل نرخ هشدار کاذب، منفی کاذب نرخ، و تشخیص نرخ (دکتر) نتایج نشان می‌دهد که مدل MLP پیشنهادی به دقت قابل توجهی دست می‌یابد. ۹۸.۸۱٪ و حداقل نرخ هشدار کاذب ۰.۰۰۲. دقت، فراخوانی و امتیاز F1 برای کلاس غیرعادی ۰.۹۹ است. ۰.۹۸، و ۰.۹۸، به ترتیب. AUC، در ۰.۹۹، نشان دهنده قدرت تمایز بالای مدل است. معیارهای امنیتی نشان می‌دهند کم نادرست زنگ هشدار نرخ و بالا دکتر، برجسته کردن مدل اثربخشی در تشخیص حملات انسداد سرویس (DDOS) حملات در SDN. این مقاله شامل معرفی چارچوب IDS مبتنی بر کشف عمیق برای تشخیص DDoS در SDN با استفاده از یک مدل طبقه‌بندی MLP، ارزیابی جامع با استفاده از متنوع معیارها، و الف مقایسه‌ای تحلیل با موجود راه حل ها. آینده کار ممکن است گسترش دادن ‎‏ ... مدل برای تشخیص دیگر امنیت تهدیدها در شبکه SDN و افزایش شفافیت و تفسیرپذیری محدودیت‌ها شامل شدن ‎‏ ... استفاده از الف محیط شبیه‌سازی شده و دامنه محدود مجموعه داده‌ها.

یونگایسلا-نائولا و ال. [[32]](#_bookmark48) تمرکزها روی دفاع کردن در برابر حملات DDoS با سرعت پایین از طریق یک چارچوب مبتنی بر SDN که DL و RL را برای تشخیص و کاهش خودکار ادغام می‌کند، مقابله می‌کند. این مطالعه به آسیب‌پذیری فزاینده شبکه‌ها در برابر حملات DDoS پیچیده و با توان عملیاتی بالاتر می‌پردازد که ناشی از تغییر قابل توجه و پیش‌بینی نشده در استفاده از اینترنت است. موجود شبکه امنیت راه حل ها هستند تلقی شده ناکافی در رسیدگی ‎‏ ... افزایش ناگهانی در حمله حجم، ترغیب کردن ‎‏ ... ضرورت مکانیسم‌های دفاعی خودکار. راه‌حل‌های مختلفی ارائه شده است پیشنهادی برای حملات انسداد سرویس (DDOS) حملات، پوشا دستگاه مدل‌های یادگیری ماشین (ML) و یادگیری ماشینی (DL) برای تشخیص، در کنار استراتژی‌های کاهش خطر، از رویکردهای کاهش ترافیک گرفته تا رویکردهایی که از یادگیری ماشینی (RL) استفاده می‌کنند. هدف این تحقیق ارائه یک چارچوب خودکار مبتنی بر SDN است که یادگیری ماشینی، یادگیری ماشینی و هدف متحرک (Moving Target) را با هم ادغام می‌کند. دفاع (MTD)، و شبکه عملکرد مجازی‌سازی (NFV) برای مقابله با حملات DDoS با سرعت پایین. مشارکت‌ها شامل ارزیابی عملکرد در لحظه در یک شبکه شبیه‌سازی شده است. و ‎‏ ... تأمین از منبع کد برای الف نمونه اولیه چارچوب پیشنهادی. سیستم پیشنهادی از یک چارچوب مبتنی بر SDN با استفاده از یادگیری ماشینی (DL) و یادگیری ماشینی (RL) برای تشخیص و کاهش خودکار حملات DDoS با سرعت پایین استفاده می‌کند. داده‌های ترافیک شبکه به عنوان ورودی عمل می‌کنند و با استفاده از یادگیری ماشینی (DL) پردازش می‌شوند. برای حمله تشخیص و آر ال برای کاهش، در نتیجه در یک سیستم مدیریت شبکه بهینه شده با قابلیت‌های تصمیم‌گیری هوشمند. این راه‌اندازی آزمایشی از ابزارهای متن‌باز مانند ONOS، Containernet، وب سرور آپاچی و Docker در یک شبکه شبیه‌سازی شده استفاده می‌کند. معیارها شامل توان عملیاتی، تأخیر و استفاده از منابع، همراه با معیارهای امنیتی مانند نرخ تشخیص حمله، مثبت کاذب هستند. نرخ، و شبکه عملکرد در طول حملات. پیامدها ویترین ‎‏ ... اثربخشی از ‎‏ ... چارچوب در

قابلیت‌های تصمیم‌گیری هوشمند را معرفی می‌کند . این سیستم سازگاری با شرایط مختلف شبکه را نشان می‌دهد. از جمله مشارکت‌ها می‌توان به اثربخشی چارچوب در برابر حملات DDoS با سرعت پایین، بهبود عملکرد شبکه از طریق MTD با کمک NFV و تصمیم‌گیری هوشمند از مکانیسم RL اشاره کرد. کار مداوم بر اصلاح بیشتر تمرکز دارد، در حالی که محدودیت‌ها بر نیاز به آزمایش و اعتبارسنجی بیشتر در دنیای واقعی تأکید دارند.

حیدر و همکاران [[33]](#_bookmark49) بر تشخیص حملات DDoS در SDN از طریق کاربرد تکنیک‌های DL تمرکز دارد. این مطالعه به بررسی ... ‎‏ ... تشدید شونده تهدید از پیشرفته حملات انسداد سرویس (DDOS) حملات در شبکه SDN محیط‌ها، ژست گرفتن چالش‌ها به سنتی سیستم‌های تشخیص نفوذ. سیستم‌های تشخیص نفوذ (IDS) عمدتاً از رویکردهای مبتنی بر امضا و مبتنی بر ناهنجاری استفاده می‌کنند. IDS مبتنی بر ناهنجاری، به ویژه با استفاده از یادگیری عمیق، نویدبخش پیشی گرفتن از سیستم‌های مبتنی بر امضا و مبتنی بر قانون است. روش‌ها برای شناسایی ناشناخته نفوذها این تحقیق یک چارچوب گروهی عمیق CNN برای کارایی ارائه می‌دهد. حملات انسداد سرویس (DDOS) حمله تشخیص در SDN، هدف گیری به بر محدودیت‌های موجود در رویکردهای IDS موجود غلبه کرده و دقت و کارایی تشخیص DDoS را افزایش می‌دهد. این سیستم از یک چارچوب گروهی Deep CNN برای تشخیص DDoS استفاده می‌کند و از داده‌های ترافیک شبکه به عنوان ورودی استفاده می‌کند. فرآیند یادگیری عمیق شامل شبکه‌های عصبی کانولوشن، طبقه‌بندی و ... است. شبکه ترافیک به عنوان عادی یا بدخواه بر اساس الگوهای حمله DDoS. ارزیابی شامل عملکرد استاندارد است معیارها، از جمله تشخیص دقت، دقت، فراخوانی، معیار F1 و منحنی ROC. آموزش و زمان آزمایش، همراه با مصرف حافظه سیستم، نیز ارزیابی می‌شوند. معیارهای عملکرد شامل دقت، صحت، یادآوری و معیار F1 می‌شوند، در حالی که معیارهای امنیتی بر تشخیص و طبقه‌بندی حملات DDoS در محیط‌های SDN با استفاده از یادگیری عمیق تمرکز دارند. نتایج نشان می‌دهد که اثربخشی از ‎‏ ... عمیق سی‌ان‌ان گروه چارچوب در تشخیص و طبقه‌بندی دقیق حملات DDoS. نمایش‌های بصری از طریق گیجی ماتریس‌ها و ROC نمودارها نشان می‌دهند ‎‏ ... سیستم عملکرد. تحقیق مشارکت توسط در حال توسعه یک کارآمد عمیق سی‌ان‌ان گروه چارچوبی برای تشخیص DDoS در SDN، با پرداختن به محدودیت‌های IDS، و افزایش دقت. تلاش‌های آینده ممکن است شامل اصلاح باشد ‎‏ ... چارچوب، کاوش زمان واقعی پیاده‌سازی و تضمین مقیاس‌پذیری برای محیط‌های SDN در مقیاس بزرگ. محدودیت‌ها شامل لزوم اعتبارسنجی بیشتر در محیط‌های SDN متنوع و سازگاری با الگوهای حمله DDoS در حال تکامل است.

موسی و همکاران [[34]](#_bookmark50) به آسیب‌پذیری‌های امنیتی SDN می‌پردازد. با الف تمرکز روی مقابله حملات انسداد سرویس (DDOS) حملات. راه‌حل پیشنهادی ، یک مدل یادگیری عمیق را معرفی می‌کند که برای شناسایی ... طراحی شده است. و جلوگیری از حملات انسداد سرویس (DDOS) حملات درون SDN ها، به طور خاص امنیت سایبری را در مراکز داده چند مستاجری هدف قرار می‌دهد. نگرانی اصلی این مطالعه، آسیب‌پذیری SDNها است. به حملات DDoS، که می‌تواند دسترسی مشروع کاربر را مختل کند به منابع مورد انتظار. روش‌های تشخیص DDoS موجود هستند اشاره کرد برای آنها پتانسیل مثبت کاذب نتایج پیشین

راه‌حل‌ها، که عمدتاً تکنیک‌های مبتنی بر یادگیری ماشین هستند ، به نمایش گذاشته شده وعده اما مبارزه به سازگار شدن به ‎‏ ... طبیعت در حال تکامل از حملات انسداد سرویس (DDOS) حملات. تحقیق عینی است به ارائه مروری جامع بر مطالعات انجام شده در این حوزه، با تأکید بر ... ‎‏ ... نقاط قوت و نقاط ضعف از مختلف رویکردها. سیستم پیشنهادی یک مدل یادگیری عمیق مبتنی بر یک شبکه ترکیبی خودرمزگذار و ایست بازرسی را معرفی می‌کند. ورودی داده‌ها شامل می‌شود شبکه ترافیک داده‌ها جمع‌آوری شده توسط ‎‏ ... SDN، با ‎‏ ... آموزش فرآیند هدف قرار داده شده در تمایز قائل شدن بین ترافیک عادی و حمله. خروجی مدل شامل موارد زیر است طبقه بندی ترافیک به عادی و حمله این آزمایش شامل آموزش و اعتبارسنجی مدل با استفاده از مجموعه داده NSL-KDD بود. دستیابی به نرخ موفقیت از ۹۹.۹۹٪ در آموزش و ۹۹.۹۲۳٪ در اعتبارسنجی، مدل دقت ۱۰۰٪ و به طور قابل توجهی پایین را نشان داد مثبت کاذب نرخ‌ها مقایسه شده به جایگزین رویکردها. معیارهای عملکرد شامل دقت، فراخوانی و امتیاز F1، در حالی که معیارهای امنیتی شامل نرخ تشخیص، نرخ مثبت کاذب و زمان تشخیص حمله بودند. از نظر تشخیص DDoS در SDN با استفاده از یادگیری عمیق، مدل پیشنهادی به دست آمده الف ۱۰۰٪ موفقیت نرخ در شناسایی حملات DDoS منفرد در تمام مجموعه داده‌ها. این تحقیق کمک می‌کند یک مدل یادگیری عمیق جدید که برای تشخیص DDoS در SDNها طراحی شده است، و به دلیل نرخ موفقیت بالا و حداقل موارد مثبت کاذب قابل توجه است. آینده تلاش ها شامل کردن ارزیابی ‎‏ ... مدل به عنوان یک زمان واقعی طبقه بندی کننده در یک شبکه SDN محیط زیست تحت زنده DDoS و شرایط ترافیک عادی. محدودیت‌های این مطالعه عبارتند از اتکا روی الف مجرد مجموعه داده‌ها برای آموزش و اعتبارسنجی، که به طور بالقوه نمایش تمام حملات DDoS قابل تصور را محدود می‌کند.

وانگ و همکاران [[35]](#_bookmark51) به حوزه شبکه می‌پردازد امنیت، به طور خاص تمرکز کردن روی ‎‏ ... شناسایی و کاهش حملات DDoS در SDN. این تحقیق تلاش می‌کند تا آسیب‌پذیری SDN در برابر حملات DDoS را برطرف کند، تأکید بر ‎‏ ... ضرورت برای یک ماهر سیستم تشخیص و کاهش برای محافظت از دارایی‌های شبکه. اگرچه راه‌حل‌های موجود شامل روش‌های سنتی تشخیص DDoS و مکانیسم‌های دفاعی مبتنی بر SDN هستند، اما اغلب با مشکلات دقت و کارایی دست و پنجه نرم می‌کنند. هدف اصلی معرفی SDN-Defend، یک راهکار آنلاین سبک است. حمله تشخیص و کاهش سیستم، مهارت در تشخیص و کاهش حملات DDoS در SDN. مشارکت‌ها شامل کردن فرموله کردن یک نوآورانه مکانیزم دفاعی، تشخیص نفوذ مبتنی بر یادگیری عمیق را با یک مکانیزم ردیابی IP که ریشه در معماری SDN دارد، ادغام می‌کند. SDN-Defend داده‌های ترافیک شبکه را با استفاده از یک روش تشخیص نفوذ CNN-ELM پردازش می‌کند و از کنترل و مدیریت متمرکز SDN برای ردیابی مؤثر منبع و پاکسازی ترافیک غیرطبیعی بهره می‌برد. این سیستم به طور مؤثر حملات DDoS را در مبدا آنها محدود می‌کند. آزمایش‌های شبیه‌سازی که بر روی پلتفرم Mininet انجام شد، تشخیص را اندازه‌گیری کردند. دقت، کارایی، و آی پی ردیابی برگشتی اثربخشی. مدل پیشنهادی CNN-ELM دقت بالایی را نشان داد و در مجموعه داده CICIDS-2017 به 98.92٪ و در مجموعه داده InSDN به 99.91٪ دست یافت. روش ردیابی IP مبتنی بر SDN به طور ماهرانه‌ای شناسایی شده حمله منابع و تخفیف یافته حملات انسداد سرویس (DDOS) حملات.

این مقاله به SDN-Defend، یک سیستم دفاعی ماهر مبتنی بر SDN برای تشخیص و کاهش حملات DDoS، می‌پردازد. تلاش‌های آینده شامل بررسی روش‌های یادگیری بدون نظارت برای تشخیص ناهنجاری و اصلاح الگوریتم‌های تشخیص و استراتژی‌های کاهش ترافیک غیرعادی است. این مطالعه تأکید می‌کند ‎‏ ... ضرورت برای بیشتر دنیای واقعی آزمایش و اعتبارسنجی سیستم پیشنهادی.

علی و همکاران [[36]](#_bookmark52) به کاوش در قلمرو تکنیک‌های یادگیری ماشینی و یادگیری عمیق می‌پردازد. به تشخیص و کاهش دادن حملات انسداد سرویس (DDOS) حملات در حوزه SDN. این مطالعه بر فناوری SDN و حوزه امنیت شبکه تمرکز دارد، که هدف اصلی آن عینی از شناسایی مؤثر روش‌هایی برای مقابله با تهدیدات امنیتی در SDN، به ویژه افزایش دقت و کارایی تشخیص حمله DDoS. این مطالعه به بررسی تهدید فزاینده حملات DDoS در SDN می‌پردازد. محیط‌ها. موجود راه حل ها شامل شدن روش‌های سنتی مبتنی بر قانون و رویکردهای مبتنی بر یادگیری ماشین؛ با این حال، این‌ها روش‌ها چنگ زدن با محدودیت‌ها مربوط به دقت، کارایی و مقیاس‌پذیری. هدف تحقیق، ارزیابی و مقایسه عملکرد الگوریتم‌های مختلف یادگیری ماشین و یادگیری عمیق برای تشخیص حمله DDoS در SDN است و در نهایت پیشنهاد می‌دهد یک تطبیقی مکانیسم که آمیختگی‌ها الگوریتم‌های چندگانه به بهینه سازی ‎‏ ... تشخیص فرآیند. سیستم پیش‌بینی‌شده، داده‌های ترافیک شبکه را از طریق ترکیبی از الگوریتم‌های یادگیری ماشینی و یادگیری عمیق، شامل ماشین‌های بردار پشتیبان، نزدیکترین همسایه‌های K، درخت‌های تصمیم‌گیری، پرسپترون چندلایه و شبکه‌های عصبی کانولوشنی، پردازش می‌کند. هدف این ادغام، طبقه‌بندی ترافیک شبکه و شناسایی ناهنجاری‌ها است و یک پیش‌بینی خروجی ارائه می‌دهد که نشان می‌دهد آیا مشاهده شده شبکه ترافیک است عادی یا نشانگر از الف حمله DDoS . آزمایش درگیر با استفاده از مجموعه داده‌های CICIDS2017 و CICDDoS2019، شامل انواع مختلف ترافیک شبکه و حملات DDoS. معیارهای عملکرد، مانند دقت، امتیاز F1 و ضریب همبستگی متیوز (MCC)، همراه با معیارهای امنیتی مانند نرخ مثبت کاذب، نرخ منفی کاذب، دقت و فراخوانی، مورد استفاده قرار گرفتند. نتایج، برتری سیستم پیشنهادی را در دقت، کارایی، و مقیاس‌پذیری، دستیابی به یک دقت از بالا به ۹۹.۹٪ و الف حداقل نادرست مثبت نرخ از ۰.۰۱٪. نتایج تشخیص DDoS با استفاده از DL، اثربخشی سیستم را در برابر انواع مختلف حمله، از جمله سیل UDP، سیل TCP SYN و سیل HTTP، با نرخ بالای مداوم، نشان می‌دهد. دقت و کم نادرست مثبت نرخ ها. مشارکت‌های این مطالعه دروغ در شناسایی قوی میلی لیتر و دی ال الگوریتم‌هایی برای تشخیص حمله DDoS در SDN، که یک مکانیسم تطبیقی برای تشخیص پیشرفته پیشنهاد می‌دهد. این تحقیق با تأکید بر ماهیت ضروری پرداختن به تهدیدات امنیتی در محیط‌های SDN، عملکرد و محدودیت‌های راه‌حل‌های موجود را روشن می‌کند. پیشنهادهای کاری آینده شامل موارد زیر است: ارزیابی کردن ‎‏ ... پیشنهادی سیستم در در شبکه‌های واقعی به صورت بلادرنگ برای سنجش اثربخشی و مقیاس‌پذیری. این مطالعه از بررسی یادگیری تقویتی و یادگیری پیشرفته حمایت می‌کند. میلی لیتر تکنیک‌ها برای حملات انسداد سرویس (DDOS) حمله تشخیص در SDN. محدودیت‌های اذعان شده شامل استفاده از شبیه‌سازی شده و آفلاین است تحلیل، بالقوه افتادن کوتاه از کپسوله سازی پیچیدگی کامل از دنیای واقعی شبکه‌ها. مطالعه محدود شده

تجزیه و تحلیل ترافیک شبکه در یک روز، فراخوانی برای آینده را برمی‌انگیزد. تحقیق استخدام بزرگتر مجموعه داده‌ها برای بیشتر یافته‌های قطعی.

گبرمسکل و ال. [[37]](#_bookmark53) کاوش می‌کند به ‎‏ ... تخصصی حوزه‌های اعمال یادگیری ماشینی (DL) برای تشخیص حملات DDoS در چارچوب SDN. سیستم پیش‌بینی‌شده به‌طور خاص موارد زیر را هدف قرار می‌دهد : ‎‏ ... شناسایی و طبقه بندی از حملات انسداد سرویس (DDOS) حوادث درون الف چندکنترلگر شبکه SDN تنظیم. تحقیقات هدف اولیه است به مبله کردن الف راه حل که است هر دو مؤثر و در خنثی کردن پیشگیرانه حملات DDoS کارآمد است. سیستم پیشنهادی ادغام می‌کند یک مبتنی بر آنتروپی مدل با عمیق روش‌های یادگیری برای بررسی دقیق و طبقه‌بندی ترافیک شبکه، که هوشیاری بیشتری را در برابر تهدیدات احتمالی DDoS ارائه می‌دهد. نگرانی اصلی که در این تحقیق به آن پرداخته شده است، آسیب‌پذیری است . از نرم‌افزار محور شبکه‌ها به حملات انسداد سرویس (DDOS) حملات. اقدامات متقابل موجود شامل کردن متعارف ابزارها مانند فایروال ها و سیستم‌های تشخیص نفوذ، همراه با الگوریتم‌های یادگیری ماشین و یادگیری عمیق. با این حال، این راه‌حل‌های موجود، به‌ویژه در شناسایی دقیق، کاستی‌هایی را نشان می‌دهند. ناشناخته حملات انسداد سرویس (DDOS) تهدیدها تحقیق تلاش برای ارائه یک مدل ترکیبی که قادر به تشخیص و طبقه‌بندی دقیق باشد از حملات انسداد سرویس (DDOS) حملات درون الف چندکنترلگر محیط SDN. این سیستم با نظارت جامع بر ترافیک ورودی در یک چارچوب SDN چندکنترلی عمل می‌کند، به طور فعال به دنبال ناهنجاری‌ها نشانگر از DDoS بالقوه حملات. استخدام شبکه ترافیک داده‌ها به عنوان ورودی، سیستم اطلاعات را از طریق ادغام یک مدل مبتنی بر آنتروپی و تکنیک‌های یادگیری عمیق پردازش می‌کند. خروجی سیستم مستلزم طبقه‌بندی ترافیک شبکه است. به عادی یا حملات انسداد سرویس (DDOS) حمله دسته بندی ها. ارزیابی‌های تجربی شاغل ‎‏ ... CICDDoS2019 مجموعه داده‌ها برای آموزش و آزمایش سیستم پیشنهادی. معیارهای عملکرد شامل موارد زیر است دقت، دقت، به یاد آوردن، و امتیاز F1، در حالی که معیارهای امنیتی شامل نرخ مثبت کاذب، نرخ منفی کاذب و نرخ تشخیص بودند. نتایج، دقت و کارایی برتر سیستم را در تشخیص حمله DDoS در مقایسه با راه‌حل‌های موجود نشان داد. نتایج، عملکرد استثنایی سیستم را با دقت، صحت، فراخوانی و امتیاز F1 99٪ برجسته کرد. نرخ مثبت کاذب و منفی کاذب با 0.01٪ حداقل بود، همراه با نرخ تشخیص چشمگیر 99٪. سهم این از ویژگی‌های این کار می‌توان به معرفی یک مدل ترکیبی با استفاده از یادگیری عمیق برای تشخیص DDoS در یک محیط SDN چندکنترلی اشاره کرد. این سیستم نسبت به راه‌حل‌های موجود، دقت و اثربخشی بالاتری را نشان داد. کار آینده می‌تواند مستلزم اصلاح قابلیت سیستم برای شناسایی تهدیدهای DDoS ناشناخته، همراه با پرداختن به هرگونه چالش پیاده‌سازی در دنیای واقعی باشد. محدودیت‌های اذعان شده شامل موارد زیر است: ‎‏ ... ضرورت برای اضافی آزمایش و ارزیابی در محیط‌های شبکه‌ای متنوع

منصور و ال. [[38]](#_bookmark54) کاوش می‌کند به ‎‏ ... دامنه از شبکه SDN برای پرداختن به تشخیص حملات DDoS، با استفاده از روش‌های DL. نقطه کانونی این مطالعه، آسیب‌پذیری‌های امنیتی در لایه‌های SDN است، به طور خاص بر آسیب‌پذیری معماری‌های SDN در برابر تهدیدات DDoS تأکید دارد. موجود راه حل ها شرح داده شده شامل شدن الف طیف از میلی لیتر و

روش‌های مبتنی بر DL متناسب با تشخیص DDoS در برابر کنترل‌کننده‌های SDN. این تحقیق تلاش می‌کند تا با معرفی یک رویکرد مبتنی بر RNN برای تشخیص DDoS در SDN، با تأکید بر FPR پایین و دقت تشخیص بالاتر، بر محدودیت‌های روش‌های موجود غلبه کند. مشارکت‌ها شامل پیشنهاد یک مکانیسم انتخاب ویژگی متقابل مبتنی بر IGR و Chi-square، توسعه یک مدل RNN DL قوی آموزش دیده با ویژگی‌های انتخاب شده و رفع کاستی‌های موجود در رویکردهای قبلی است. پیشنهادی سیستم استخدام می‌کند الف دی ال آر ان ان مدل آموزش دیده با انتخاب ویژگی‌ها به تشخیص دادن بی سیم، تی سی پی، و آی‌سی‌ام‌پی حملات با گرفتن آنها پیچیده رفتاری الگوها ورودی ویژگی‌ها از طریق یک IGR و انتخاب ویژگی متقاطع مبتنی بر کای اسکوئر انتخاب می‌شوند . فرآیند، ‎‏ ... دی ال آر ان ان مدل است آموزش دیده بر این اساس، و خروجی مستلزم تشخیص دقیق حملات DDoS است روی کنترل‌کننده‌های شبکه SDN. ارزیابی تجربی شامل ارزیابی مدل DL RNN پیشنهادی با انتخاب ویژگی‌ها. نتایج احاطه شده عملکرد معیارهایی مانند دقت تشخیص و FPR، همراه با معیارهای امنیتی متناسب با تشخیص DDoS در SDN با استفاده از DL. این مطالعه در نظر گرفته شده تشخیص دقت و اف پی آر به عنوان معیارهای عملکرد. امنیت معیارها مربوط به حملات انسداد سرویس (DDOS) تشخیص در استفاده از SDN دی ال بودند انتگرال به ‎‏ ... مطالعه کردن. نکات برجسته از ‎‏ ... تشخیص DDoS نتایج در شبکه SDN با استفاده از دی ال شامل شدن ‎‏ ... کم اف پی آر و دقت تشخیص بالا که توسط مدل DL RNN آموزش دیده حاصل شده است با انتخاب شده ویژگی‌ها. مشارکت‌ها کپسوله کردن پیشنهاد یک رویکرد نوآورانه مبتنی بر DL برای تشخیص DDoS در SDN، غلبه بر محدودیت‌های ذاتی روش‌های موجود، و ارائه بینش‌هایی در مورد امنیت شبکه SDN. کار آینده ممکن است شامل اصلاح بیشتر موارد زیر باشد: ‎‏ ... پیشنهادی مبتنی بر DL رویکرد و آدرس‌دهی محدودیت‌های باقیمانده در تشخیص DDoS در دنیای واقعی در SDN. محدودیت‌های مطالعه شامل شدن محدودیت‌ها مرتبط به ‎‏ ... تنظیمات آزمایشی، دامنه رویکرد پیشنهادی و چالش‌های بالقوه در پیاده‌سازی در دنیای واقعی.

نووا و همکاران [[39]](#_bookmark55) بر به کارگیری یک عمق خصمانه تمرکز دارد یادگیری رویکرد برای ‎‏ ... شناسایی و کاهش حملات DDoS در محیط‌های SDN. این مطالعه به آسیب‌پذیری تنظیمات SDN در برابر حملات DDoS می‌پردازد و تأکید می‌کند ‎‏ ... لازم و ملزوم برای ماهر تشخیص و مکانیسم‌های دفاعی . در حالی که سنتی روش‌ها وجود داشته باشد، آنها ممکن است با کنترل پویا و متمرکز ذاتی معماری‌های SDN به طور بهینه همسو نیستند. هدف اصلی، غلبه بر معایب مکانیسم‌های تشخیص و دفاع DDoS موجود با معرفی یک یادگیری عمیق تخاصمی است. رویکرد متناسب سازی شده برای اس دی ان. تحقیق مشارکت‌ها آشکار در ‎‏ ... آفرینش از الف سیستم که ادغام می‌کند یادگیری عمیق و شبکه‌های مولد تخاصمی (GAN) برای زمان واقعی حملات انسداد سرویس (DDOS) تشخیص و دفاع در SDN. سیستم پیشنهادی با استفاده از الگوریتم‌های یادگیری عمیق برای تشخیص ناهنجاری، به جمع‌آوری و تجزیه و تحلیل تقریباً بلادرنگ ترافیک شبکه می‌پردازد. ورودی شامل داده‌های شبکه است. ترافیک داده‌ها پردازش شده از طریق عمیق یادگیری مدل‌ها، شناسایی و کاهش حملات DDoS را به همراه داشت. مرحله آزمایشی سناریوهای حمله DDoS رایج را نشان داد، از جمله ان تی پی، دی‌ان‌اس، LDAP، MSSQL، نت بایوس، SNMP SSDP، بی سیم، تأخیر UDP، وب DDoS (آرمِه)، سین،

و TFTP. معیارهای عملکرد شامل تشخیص بودند نرخ، نرخ مثبت کاذب و زمان پاسخ، در حالی که معیارهای امنیتی، دقت و استحکام تشخیص حمله را اندازه‌گیری می‌کردند. نتایج نشان داد که سیستم پیشنهادی با استفاده از روش‌های یادگیری عمیق، نرخ تشخیص برتر و حساسیت کمتری نسبت به نمونه‌های خصمانه در مقایسه با روش‌های مرسوم نشان می‌دهد. این سیستم، اثربخشی امیدوارکننده‌ای را در تشخیص و کاهش حملات DDoS در SDN نشان داد. محیط‌ها. تحقیق مشارکت می‌کند توسط فرموله کردن مؤثر خصمانه عمیق یادگیری رویکرد متناسب سازی شده برای تشخیص و دفاع در برابر DDoS در محیط‌های SDN. کارهای آینده مستلزم پالایش ‎‏ ... پیشنهادی سیستم و پهن شدن کاربردپذیری آن به آدرس مختلف شبکه حملات. محدودیت‌ها شامل لزوم سازگاری مداوم با استراتژی‌های در حال تکامل حمله DDoS می‌شود.

نووا و همکاران [[40]](#_bookmark56) به حوزه شبکه‌های کامپیوتری می‌پردازد، به طور خاص آدرس‌دهی ‎‏ ... چالش‌ها درون SDN. این مطالعه بر تقویت امنیت در محیط‌های SDN با توسعه سیستم LSTM-FUZZY تمرکز دارد که از ... استفاده می‌کند. LSTM و فازی منطق به تشخیص و کاهش دادن حملات DDoS و پورتسکن حملات. هسته تحقیق مشکل مربوط به ‎‏ ... امنیت آسیب‌پذیری‌ها شایع در SDN، به ویژه مستعد حملات DDoS و Portscan هستند. اقدامات امنیتی سنتی ممکن است در پرداختن به چالش‌های منحصر به فرد ناشی از SDN ناکافی باشند. هدف این تحقیق ایجاد یک مدل ماژولار است. سیستم برای ناهنجاری تشخیص و کاهش در شبکه‌های SDN ، که به طور خاص در توصیف ویژگی‌ها نقش دارند ترافیک شبکه، تشخیص ناهنجاری با استفاده از یادگیری عمیق و منطق فازی، و کاهش خودکار. سیستم LSTM-FUZZY در سه مرحله انجام می‌شود: توصیف، تشخیص ناهنجاری و کاهش. این سیستم داده‌های ترافیک شبکه را به عنوان ورودی دریافت می‌کند و از LSTM برای توصیف ترافیک استفاده می‌کند. و تشخیص ناهنجاری. این سیستم، سیاست‌های کاهش خودکار را برای کاهش تأثیر ناهنجاری‌های شناسایی‌شده، ارائه می‌دهد. آزمایش تجربی شامل اعمال LSTM-FUZZY بود. سیستم به مجموعه داده‌ها حاوی متنوع حملات DDoS. معیارهای عملکرد، از جمله دقت تشخیص، نرخ مثبت کاذب و زمان پاسخ، در کنار هم ارزیابی شدند. امنیت معیارها چنین به عنوان حمله تشخیص نرخ و اثربخشی کاهش. نتایج مربوط به تشخیص DDoS با استفاده از یادگیری عمیق، دقت بالا، نرخ پایین مثبت کاذب و زمان پاسخ سریع را نشان داد. مشارکت‌ها شامل ایجاد یک تشخیص ناهنجاری مدولار است. و سیستم کاهش خطرات برای SDN، با استفاده از تکنیک‌های پیشرفته‌ای مانند یادگیری عمیق و منطق فازی. تلاش‌های آینده می‌توانست تمرکز روی پالایش ‎‏ ... سیستم عملکرد و گسترش سازگاری آن با حملات مختلف شبکه. محدودیت‌ها ممکن است شامل تنظیمات مداوم در استراتژی‌های حمله در حال تحول و پیامدهای احتمالی منابع هنگام استقرار سیستم در محیط‌های شبکه گسترده باشد.

وانگ و همکاران [[41]](#_bookmark57) به بررسی کاربرد فناوری یادگیری عمیق در حوزه سیستم‌های تشخیص نفوذ شبکه می‌پردازد، به طور خاص از مجموعه داده‌های CSE-CIC-IDS2018 برای بهبود تشخیص حملات شبکه استفاده می‌کند. تمرکز اصلی بر رفع کاستی‌های موجود است. در فعلی نفوذ تشخیص سیستم‌ها و تقویت

توانایی آنها در تشخیص روش‌های حمله معاصر و متنوع. مشکل تحقیقاتی شناسایی‌شده حول محور کاستی‌های سیستم‌های تشخیص نفوذ شبکه موجود، به‌ویژه در تشخیص روش‌های حمله مدرن و متنوع، می‌چرخد. راه‌حل‌های رایج شامل سیستم‌های تشخیص نفوذ مرسوم متکی بر امضا هستند. تشخیص، اثبات کردن ناکافی در شناسایی مؤثر رمان و پیچیده شبکه حملات. علاوه بر این، ماهیت قدیمی و غیرقابل اعتماد بودن مجموعه داده‌هایی مانند KDD Cup ۱۹۹۹ (KDD99) و NSL-KDD بیشتر محدودیت‌های موجود در تطبیق روش‌های حمله فعلی را تشدید می‌کند. هدف اصلی این تحقیق، ارزیابی اثربخشی است. از عمیق یادگیری روش‌شناسی‌ها در واقعی شبکه سناریوهای تشخیص نفوذ ، با استفاده از مجموعه داده CSE-CIC-IDS2018. کلید مشارکت‌ها شامل شدن ‎‏ ... کاربرد از

مدل‌های متنوع یادگیری عمیق، از جمله DNN، CNN، RNN، LSTM، سی‌ان‌ان + آر ان ان، و سی‌ان‌ان + LSTM، برای هر دو وظایف طبقه‌بندی دودویی و چند کلاسی. هدف این مطالعه برای نشان دادن بهبود عملکرد تشخیص در مقایسه با به موجود نفوذ تشخیص سیستم‌ها.

سیستم پیشنهادی از مجموعه داده CSE-CIC-IDS2018 استفاده می‌کند. برای انجام آزمایش‌های تشخیص نفوذ. ورودی شامل موارد زیر است شبکه ترافیک داده‌ها استخراج شده از ‎‏ ... CSE-CIC -IDS2018 مجموعه داده‌ها، موضوع به پیش‌پردازش این داده‌های پیش‌پردازش‌شده خدمت می‌کند به عنوان ورودی برای مختلف عمیق یادگیری مدل‌ها،

چنین به عنوان دی‌ان‌ان، سی‌ان‌ان، آر ان ان، LSTM، سی‌ان‌ان + آر ان ان، و

سی‌ان‌ان + LSTM. خروجی شامل می‌شود نتایج از دودویی و چند کلاسه طبقه بندی، تعیین کننده آیا مشاهده شده

ترافیک نشان دهنده یک حمله مخرب است. پیکربندی آزمایشی شامل CSE-CIC- IDS2018 جامع است. مجموعه داده‌ها، اعمال کردن عمیق یادگیری مدل‌ها برای تشخیص نفوذ . نتایج به دست آمده، سطوح دقت بیش از حد را نشان می‌دهد ۹۸٪ چه زمانی استخدام مناسب داده‌ها تکنیک‌های پیش‌پردازش و هایپرپارامتر تنظیم. عملکرد معیارها، از جمله دقت، فراخوانی، معیار F، ROC و زمان استنتاج، در ترکیب‌های مختلف مدل ارزیابی می‌شوند. معیارهای عملکرد در نظر گرفته شده شامل دقت، فراخوانی، معیار F، آر او سی، و استنباط زمان. امنیت معیارها، تشخیص حملات مختلف شبکه، از جمله حملات انکار سرویس توزیع‌شده (DDoS) را در بر می‌گیرند. این مطالعه بر دقت قابل توجه در تشخیص حملات DDoS تأکید می‌کند، به طوری که دقت طبقه‌بندی چند کلاسه برای تشخیص DDoS به طور مداوم از 98٪ فراتر می‌رود. یافته‌های مربوط به حملات انسداد سرویس (DDOS) تشخیص در SDN با استفاده از دی ال زیرخط دار ‎‏ ... اثربخشی ‎‏ ... پیشنهادی مدل در بالا بردن تشخیص عملکرد برای حملات DDoS حملات. تحقیق باعث می‌شود قابل توجه مشارکت‌ها از طریق ارزیابی روش‌های یادگیری عمیق در سناریوهای تشخیص نفوذ شبکه واقعی، با بهره‌گیری از مجموعه داده CSE-CIC-IDS2018. پیشرفت‌های قابل توجه در عملکرد تشخیص، در مقایسه با سیستم‌های تشخیص نفوذ موجود، هستند نشان داد. آینده‌نگر راه‌ها برای آینده کار شامل کاوش اضافی عمیق یادگیری مدل‌ها و ارزیابی​ زمان واقعی تشخیص قابلیت‌ها. محدودیت‌ها ذاتی در ‎‏ ... مطالعه شامل شدن ‎‏ ... ضروری برای بیشتر اعتبارسنجی در محیط‌های شبکه متنوع و بررسی روش‌های حمله در حال تکامل.

پرز-دیاز و همکاران [[42]](#_bookmark58) به حوزه امنیت شبکه می‌پردازد، با تمرکز ویژه بر تشخیص حملات انکار سرویس توزیع‌شده (DDoS) در شبکه‌های نرم‌افزاری تعریف‌شده (SDN) با استفاده از یادگیری ماشین (ML) و یادگیری عمیق (دی ال) تکنیک‌ها. تحقیق تکل‌ها ‎‏ ... تهدید فزاینده ناشی از حملات DDoS در شبکه‌های امروزی، به‌ویژه در شبکه SDN محیط‌ها. فعلی راه حل ها، از روش‌های سنتی مبتنی بر قانون گرفته تا برخی رویکردهای مبتنی بر یادگیری ماشین، با چالش‌هایی در شناسایی مؤثر مسائل پیچیده مواجه هستند. و در حال تکامل حملات انسداد سرویس (DDOS) حملات، به ویژه در ‎‏ ... لایه کاربرد. هدف اصلی ارائه یک معماری مبتنی بر SDN ماژولار است که در تشخیص حملات DDoS لایه انتقال و لایه کاربرد از طریق تکنیک‌های هوش مصنوعی مهارت داشته باشد. کلید مشارکت‌ها شامل کردن فرموله کردن الف معماری انعطاف‌پذیر و ماژولار، بررسی مدل‌های مختلف یادگیری ماشینی و یادگیری عمیق برای تشخیص DDoS و ارزیابی راه‌حل پیشنهادی درون الف شبیه‌سازی شده بستر آزمایشی محیط زیست. سیستم، داده‌های ترافیک شبکه را با استفاده از مدل‌های یادگیری ماشینی و یادگیری عمیق (ML) برای شناسایی حملات DDoS پردازش می‌کند. ردپاهای ترافیک شبکه به عنوان ورودی برای مدل‌ها عمل می‌کنند که تحت آموزش و آزمایش با مجموعه داده‌های فعلی شامل ردپاهای شبکه واقعی قرار می‌گیرند. خروجی شامل بینش‌هایی در مورد نوع و ویژگی‌های ‎‏ ... تشخیص داده شد حملات انسداد سرویس (DDOS) حملات. تجربی راه اندازی از Mininet و کنترلر ONOS برای شبیه‌سازی محیط شبکه استفاده می‌کند. نتایج شامل معیارهای عملکردی مانند دقت، نرخ مثبت کاذب، دقت، فراخوانی و امتیاز F1 است. معیارهای امنیتی، توانایی تشخیص حملات DDoS لایه انتقال و لایه کاربرد و همچنین استحکام و پیچیدگی زمانی مدل‌های تشخیص را ارزیابی می‌کنند. دی ال مدل‌ها، از جمله سی‌ان‌ان، جی آر یو، و LSTM، به نمایش گذاشته شده دقت بالا در تشخیص هر دو لایه انتقال و کاربرد حملات انسداد سرویس (DDOS) حملات. سی‌ان‌ان مدل، در خاص، به دقت قابل توجه ۹۸.۸۸٪ در تشخیص لایه کاربرد دست یافت. حملات. زمان و فضا پیچیدگی تحلیل مطلوب نشان داد شرایط برای استقرار ‎‏ ... پیشنهادی راه حل در یک محیط آزمایشی شبیه سازی شده. مشارکت ها شامل موارد زیر است یک معماری مبتنی بر SDN ماژولار برای تشخیص DDoS، بررسی مدل‌های متنوع ML و DL و عملکرد بلادرنگ ارزیابی در الف شبیه‌سازی شده بستر آزمایشی محیط. کارهای آینده ممکن است در کنار استقرار بالقوه، بر افزایش بیشتر استحکام و کارایی راه‌حل تمرکز کنند. در واقعی تولید محیط‌ها. محدودیت‌ها شامل لزوم اعتبارسنجی اضافی در محیط‌های شبکه متنوع باشد و ‎‏ ... ملاحظه از در حال تکامل حملات انسداد سرویس (DDOS) تکنیک های حمله

گادزه و ال. [[43]](#_bookmark59) کاوش می‌کند به ‎‏ ... قلمرو از شبکه امنیت و محافظت در برابر تهدیدات سایبری، به طور خاص با تمرکز بر استفاده از یادگیری عمیق برای تشخیص و کاهش حملات DDoS بر روی کنترل‌کننده‌های SDN. سیستم پیشنهادی از یک مدل یادگیری عمیق برای تشخیص و کاهش موثر حملات DDoS استفاده می‌کند و عملکرد برتر را به نمایش می‌گذارد. از نظر دقت و کارایی در مقایسه با راه‌حل‌های موجود. مطالعه آدرس‌ها ‎‏ ... تشدید شونده تهدید چشم‌انداز حملات DDoS به کنترل‌کننده‌های SDN، با اذعان به محدودیت‌ها از متعارف مبتنی بر قاعده روش‌ها و یادگیری ماشینی الگوریتم‌ها. تحقیق عینی است به معرفی کردن الف

رمان عمیق مبتنی بر یادگیری سیستم قادر از به طور دقیق و به طور کارآمد شناسایی و کاهش دهنده حملات انسداد سرویس (DDOS) حملات روی کنترل‌کننده‌های SDN. مشارکت‌ها شامل توسعه این مورد می‌شود نوآورانه سیستم و تجربی شواهد این سیستم داده‌های ترافیک شبکه را از طریق یک مدل یادگیری عمیق پردازش می‌کند و یک خروجی دودویی ارائه می‌دهد که نشان می‌دهد ‎‏ ... حضور یا غیبت از الف حملات انسداد سرویس (DDOS) حمله. داده‌های ورودی تحت پیش‌پردازش قرار می‌گیرند تا ویژگی‌های مرتبط استخراج شوند و متعاقباً برای آموزش و آزمایش به یک شبکه عصبی عمیق داده شوند. سیستم پیشنهادی از یک معماری ترکیبی استفاده می‌کند که شبکه‌های عصبی کانولوشن و بازگشتی را برای ثبت ویژگی‌های مکانی و زمانی ترافیک شبکه ترکیب می‌کند. آزمایش تجربی با مجموعه داده‌های تولید شده توسط ابزار حمله DDoS، برتری سیستم پیشنهادی را نشان داد. معیارهای عملکرد، از جمله دقت، صحت، فراخوانی و امتیاز F1، در کنار معیارهای امنیتی مانند نرخ مثبت کاذب، نرخ منفی کاذب و نرخ تشخیص، برای ارزیابی به کار گرفته شدند. نتایج، عملکرد چشمگیری را نشان داد. دقت از ۹۸.۵٪، دقت از ۹۸.۶٪، به یاد بیاورید ۹۸.۴٪ و امتیاز F1 برابر با ۹۸.۵٪. علاوه بر این، مثبت کاذب نرخ بود ۰.۵٪، ‎‏ ... نادرست منفی نرخ بود ۱.۶٪، و میزان تشخیص به ۹۸.۴٪ رسید. این تحقیق کمک می‌کند یک سیستم پیشگامانه مبتنی بر یادگیری عمیق برای تشخیص و کاهش حملات DDoS، که با نتایج تجربی اثبات شده است آن برتر دقت و کارایی در مقایسه با راه‌حل‌های موجود. تلاش‌های آینده شامل آزمایش مقیاس‌پذیری با مجموعه داده‌های بزرگتر و ارزیابی در دنیای واقعی است. درون یک SDN محیط زیست. محدودیت‌ها شامل شدن مجموعه داده‌ها محدودیت‌های اندازه و ‎‏ ... غیبت از ارزیابی در الف عملی تنظیمات SDN .

الغزاوی و همکاران [[44]](#_bookmark60) به بررسی دقیق تشخیص حملات DDoS می‌پردازد حملات از طریق الف هیبریدی عمیق یادگیری مدل با انتخاب ویژگی‌های اصلاح‌شده تقویت‌شده است. دامنه آن شامل کاربرد می‌شود دامنه از امنیت سایبری، هدف گیری به تقویت امنیت اقدامات با پیشرفته تکنولوژیکی راه حل ها. تحقیق تکل‌ها ‎‏ ... مداوم چالش از در حال توسعه روش‌های مؤثرتری برای شناسایی و کاهش حملات DDoS که به عنوان تهدیدهای اساسی برای امنیت شبکه شناخته می‌شوند. نویسندگان تلاش به پیشی گرفتن فعلی محدودیت‌هایی در دقت، کارایی و سازگاری با استراتژی‌های حمله در حال تکامل. راه‌حل‌های معرفی‌شده شامل مدل‌های مبتنی بر ویژگی مرسوم و مدل‌های یادگیری عمیق برای تشخیص حمله DDoS هستند. با اذعان به اشکالات آنها در دقت ، کارایی، و سازگاری به در حال تکامل حمله استراتژی‌ها ، تحقیق تلاش ها به حاضر یک نوآورانه رویکرد.

اهداف تحقیق شامل پیشنهاد ~~یک~~ سیستم هیبریدی قوی و عمیق است. یادگیری مدل (سی‌ان‌ان) + بی ال اس تی ام) تقویت شده با انتخاب ویژگی برای تشخیص حمله DDoS. مشارکت‌ها شامل موارد زیر است پیشگام ‎‏ ... رمان رویکرد که آمالگام‌های پیشرفته عمیق یادگیری تکنیک‌ها با بهبود یافته ویژگی

روش‌های انتخاب. سیستم پیشنهادی از یک روش ترکیبی عمیق استفاده می‌کند. یادگیری مدل (سی‌ان‌ان) + بی ال اس تی ام) با تصفیه شده انتخاب ویژگی. داده‌های ترافیک شبکه به عنوان ورودی عمل می‌کنند و از طریق آزمون x2 تحت انتخاب ویژگی قرار می‌گیرند و به دنبال آن ... دارای رتبه ویژگی استخراج از طریق الف سی‌ان‌ان و پردازش از طریق الف

بی‌ال‌اس‌تی‌ام مدل. خروجی شامل می‌شود پیش‌بینی‌ها از حملات انسداد سرویس (DDOS)

حمله پیامدها مبتنی بر روی ‎‏ ... پردازش شده داده‌ها آزمایش مورد استفاده قرار گرفت ‎‏ ... CICDDoS2019 مجموعه داده‌ها، اجرای پیشنهادی هیبریدی عمیق یادگیری مدل. معیارهای عملکرد چنین به عنوان دقت، دقت، به یاد آوردن، و اف۱ امتیاز در نظر گرفته شد. یافته‌ها بر برتری پیشنهادی هیبریدی عمیق یادگیری مدل در حملات انسداد سرویس (DDOS) تشخیص حمله، نشان دادن دقت، صحت، یادآوری و ... بهبود یافته اف۱ امتیاز. امنیت معیارها، فراگیر دقت، صحت، به یاد آوردن، و اف۱ امتیاز، بودند حیاتی در ارزیابی اثربخشی سیستم. نتایج مربوط به تشخیص DDoS در شبکه SDN با استفاده از عمیق یادگیری نشان داده شده پیشرفت‌های قابل توجه در دقت و به طور کلی عملکرد. این اثر مشارکت‌ها دروغ در ‎‏ ... فرمولاسیون از یک هیبرید کارآمد عمیق یادگیری مدل شامل تصفیه شده ویژگی انتخاب برای حملات انسداد سرویس (DDOS) حمله تشخیص، تقویت کننده شبکه تاب‌آوری. آینده تلاش ها ممکن است شامل کردن کاردستی مجموعه داده‌ها شبیه به CICDDoS2019 برای زمان واقعی حملات انسداد سرویس (DDOS) حمله شناسایی و اصلاح مدل پیشنهادی برای کاربرد وسیع‌تر. یک محدودیت مستلزم ‎‏ ... چالش از قابلیت مقایسه به دلیل به مجموعه داده‌ها و روش‌شناسی تغییرات در سراسر موجود سیستم‌ها. این اثر جامع مرتبط با دانشگاه، نگاهی عمیق به اکتشاف از ‎‏ ... کاربرد و فناوری حوزه، تحقیق مشکلات، موجود راه حل ها، تحقیق اهداف پیشنهادی سیستم روش‌شناسی، تجربی تنظیم، نتایج به دست آمده، امنیت معیارها، و پیامدها برای حملات انسداد سرویس (DDOS) تشخیص در نرم‌افزار تعریف شده شبکه با استفاده از عمیق یادگیری. لی و همکاران [[45]](#_bookmark61) به بررسی حوزه تشخیص حملات انکار سرویس توزیع‌شده (DDoS) در SDN از طریق به‌کارگیری تکنیک‌های DL می‌پردازد. مسئله اصلی مورد بحث، ضروری نیاز برای مقاوم و کارآمد حملات انسداد سرویس (DDOS) تشخیص حمله در محیط‌های SDN، که به عنوان محیط‌های آسیب‌پذیر در برابر چنین فعالیت‌های مخربی شناخته می‌شوند. با توجه به پیامدهای بالقوه‌ی حملات انسداد سرویس (DDOS) حملات روی شبکه عملکرد و امنیت، مطالعه تأکید می‌کند ‎‏ ... ضرورت برای پیشرفته تشخیص مکانیسم ها. موجود راه حل ها شامل شدن مبتنی بر امضای سنتی تشخیص روش‌ها، ناهنجاری تشخیص تکنیک‌ها، و دستگاه یادگیری رویکردها. با این حال، این راه‌حل‌ها ممکن است فاقد سازگاری لازم برای مقابله با پویایی باشند و در حال تکامل طبیعت از حملات انسداد سرویس (DDOS) حملات در محیط‌های SDN تحقیق اهداف و مشارکت‌ها شامل کردن آغاز به کار از یک نوآورانه حملات انسداد سرویس (DDOS) تشخیص اهرم‌بندی سیستم عمیق یادگیری برای SDN، عملکرد ارزیابی از طریق جامع تجربی تنظیمات، و تحلیل نتایج به نمایش گذاشتن آن اثربخشی در کاهش دهنده حملات انسداد سرویس (DDOS) تهدیدات. سیستم پیشنهادی با دریافت داده‌های ترافیک شبکه عمل می‌کند، پردازش آن از طریق الف عمیق یادگیری مدل ماهر در تشخیص الگوها نشانگر از حملات انسداد سرویس (DDOS) حملات، و تولید خروجی که حملات DDoS بالقوه را شناسایی و کاهش می‌دهد تهدیدها در شبکه SDN محیط‌ها. چارچوب تجربی مستلزم جمع‌آوری شبکه ترافیک داده‌ها از الف شبیه‌سازی شده شبکه SDN محیط زیست، متعاقباً شاغل تربیت کردن و آزمون ‎‏ ... عمیق یادگیری مدل. کلید معیارهای عملکرد، شامل دقت، صحت، یادآوری و امتیاز F1، بودند. بررسی شده، در کنار امنیت معیارها شامل نرخ تشخیص حمله، نرخ مثبت کاذب و زمان پاسخ. به طور خاص مربوط به حملات انسداد سرویس (DDOS) تشخیص در شبکه SDN از طریق

با استفاده از یادگیری عمیق، نتایج نشان‌دهنده افزایش قابل توجه نرخ تشخیص در مقایسه با روش‌های سنتی بود. سیستم مبتنی بر یادگیری عمیق، حساسیت بیشتری نسبت به الگوهای DDoS ظریف و قبلاً دیده نشده نشان داد و در نتیجه، تاب‌آوری امنیتی کلی محیط‌های SDN را تقویت کرد. سهم این مطالعه شامل ایجاد و اعتبارسنجی یک سیستم تشخیص DDoS نوآورانه مبتنی بر یادگیری عمیق برای SDN است که نشان می‌دهد تشدید شده دقت و کارایی در شناسایی و کاهش دهنده حملات انسداد سرویس (DDOS) تهدیدها آینده تلاش ها ممکن است شامل ادغام مکانیسم‌های یادگیری تطبیقی در زمان واقعی و بررسی رویکردهای تشخیص ترکیبی برای تقویت بیشتر است ‎‏ ... سیستم قابلیت‌ها. محدودیت‌ها شامل شدن ‎‏ ... اتکا در محیط‌های شبیه‌سازی‌شده SDN و نیاز مبرم به اعتبارسنجی اضافی در سناریوهای استقرار در دنیای واقعی.

ژائو و همکاران [[46]](#_bookmark62) به کاوش در حوزه تشخیص حملات DDoS می‌پردازد درون شبکه SDN از طریق ‎‏ ... استفاده از الف دی‌ان‌ان مدل. اولیه تحقیق عینی است به افزایش ‎‏ ... دقت از DDoS حمله تشخیص در حالی که همزمان کاهش دهنده ‎‏ ... هشدار کاذب نرخ. پیشنهادی سیستم شامل می‌شود الف جریان ماژول جمع‌کننده برای جمع‌آوری ورودی‌های جدول جریان، که شامل ویژگی‌های طراحی‌شده دستی و ویژگی‌های به‌دست‌آمده به‌طور خودکار است. ارزیابی سیستم با استفاده از معیارهای عملکرد و امنیت انجام می‌شود و نشان‌دهنده کارایی برتر مدل DNN در تشخیص ترافیک حمله در مقایسه با الگوریتم‌های یادگیری ماشین مرسوم است. این مقاله به چالش ابداع یک روش دقیق و کارآمد می‌پردازد. حملات انسداد سرویس (DDOS) حمله تشخیص سیستم درون اس دی ان. راه‌حل‌های موجود شامل روش‌هایی هستند که ریشه در نظریه اطلاعات، ماشین‌آلات و... دارند. یادگیری، و عصبی شبکه‌ها؛ با این حال، آنها کاستی‌هایی مانند دقت کمتر از حد مطلوب، نرخ بالای هشدار کاذب و پیچیدگی محاسباتی بالا را نشان می‌دهند . این مطالعه اهداف به معرفی کردن الف مبتنی بر DNN حملات انسداد سرویس (DDOS) حمله سیستم تشخیص، که از نظر دقت، کاهش نرخ هشدار اشتباه و کارایی محاسباتی از اسلاف خود پیشی می‌گیرد. سیستم ابداع‌شده عمل می‌کند توسط مهار کردن الف جریان گردآورنده ماژول برای انباشت از جریان میز ورودی‌ها استخدام هر دو با طراحی دستی و استخراج خودکار ویژگی‌ها، سیستم یک مدل DNN را آموزش می‌دهد. ورودی شامل ورودی‌های جدول جریان است که خروجی‌ای تولید می‌کند که ماهیت ترافیک را به صورت عادی پیش‌بینی می‌کند. یا بدخواه پیاده‌سازی از ‎‏ ... سیستم درون کنترل‌کننده SDN رخ می‌دهد . این آزمایش از موارد زیر استفاده می‌کند: مجموعه داده‌ای که از طریق شبیه‌ساز شبکه Mininet تولید شده است و کنترلر Ryu در یک محیط SDN. مجموعه داده‌ها شامل ترافیک بی‌خطر TCP، UDP، ICMP به همراه موارد مخرب مانند حمله TCP Syn، حمله UDP Flood و حمله ICMP است. معیارهای عملکرد، از جمله دقت، دقت، به یاد بیاورید، و اف۱ امتیاز، هستند شاغل برای ارزیابی سیستم، در کنار معیارهای امنیتی نرخ هشدار اشتباه و تشخیص نرخ. نتایج نشان دادن ‎‏ ... دی‌ان‌ان مدل برتر دقت و کاهش یافته نادرست زنگ هشدار نرخ در مقایسه با الگوریتم‌های یادگیری ماشین سنتی، از نظر دقت نیز از مدل‌های LSTM و CNN بهتر عمل می‌کند. این مقاله یک سیستم تشخیص حمله DDoS مبتنی بر DNN ارائه می‌دهد که نشان می‌دهد مرتفع دقت، کاهش یافته نادرست زنگ هشدار نرخ‌ها، و تشدید شده محاسباتی کارایی. آینده‌نگر کار

مستلزم تدبیر کردن راه حل ها به افزایش تشخیص کارایی و کاهش تشخیص زمان، در حالی که حمایت کردن مدل دقت. محدودیت‌ها شامل شدن اتکا روی الف مجرد مجموعه داده‌ها، ترغیب کردن نیاز به ارزیابی‌های بیشتر شبکه در دنیای واقعی.

کریستیلا و ال. [[47]](#_bookmark63) تمرکزها روی ‎‏ ... قلمرو از تشخیص و محافظت در برابر حملات DDoS در محیط‌های SDN، با استفاده از تکنیک‌های پیشرفته یادگیری عمیق. موضوع اصلی مورد بحث، آسیب‌پذیری محیط‌های SDN در برابر حملات DDoS است و بر لزوم ... تأکید دارد. مقاوم تشخیص و دفاع مکانیسم‌ها به کاهش دادن تأثیر بالقوه چنین حملاتی. راه‌حل‌های موجود، ریشه در سنتی حملات انسداد سرویس (DDOS) تشخیص و دفاع روش‌ها، ممکن است کوتاهی کردن در تطبیق دادن به ‎‏ ... پویا و پیچیده طبیعت از محیط‌های SDN. در حالی که تحقیقات قبلی کاربرد از عمیق یادگیری برای حملات انسداد سرویس (DDOS) تشخیص، آنجا همچنان تقاضا برای رویکردهای مقاوم‌تر و خصمانه‌تر برای تقویت [سیاست‌های دفاعی] وجود دارد. ‎‏ ... امنیت از شبکه SDN کنترل کننده ها این کار هدف دارد معرفی کردن یک خصمانه DBN-LSTM چارچوب برای تشخیص و دفاع در برابر حملات DDoS در محیط‌های SDN. اولیه مشارکت‌ها شامل کردن افزایش تاب‌آوری کنترل‌کننده‌های SDN در برابر حملات خصمانه و تقویت امنیت کلی زیرساخت‌های SDN. سیستم پیشنهادی با جمع‌آوری داده‌ها از سوئیچ‌های فیزیکی و مجازی در محیط SDN عمل می‌کند. داده‌های جمع‌آوری‌شده تحت پیش‌پردازش قرار می‌گیرند و ویژگی‌های غیرعددی را به ویژگی‌های عددی تبدیل می‌کنند. متعاقباً، یک چارچوب DBN-LSTM خصمانه برای تشخیص استفاده می‌شود. و دفاع علیه حملات انسداد سرویس (DDOS) حملات، حفاظت SDN​ کنترل کننده ها در ‎‏ ... کنترل هواپیما تجربی تنظیمات درگیر بود الف مجموعه داده‌ها شامل بیش از ۸۰ ویژگی‌ها، شامل بیش از ۵۰ میلیون حمله DDoS و نمونه‌های عادی متعدد. معیارهای ارزیابی شامل دقت، صحت، فراخوانی و امتیاز F1 بودند. نتایج نشان داد که نرخ دقت روش پیشنهادی ۹۶.۵۵٪ است که از سایر روش‌های یادگیری عمیق پیشی می‌گیرد. روش‌ها برای حملات انسداد سرویس (DDOS) تشخیص در شبکه SDN معیارهای امنیتی، اثربخشی سیستم را در تشخیص و دفاع در برابر حملات DDoS خصمانه ارزیابی کردند و کنترل‌کننده‌های SDN را در برابر چنین تهدیداتی کمتر آسیب‌پذیر ساختند. این کار مشارکت می‌کند یک خصمانه DBN-LSTM چارچوبی برای تشخیص و دفاع در برابر حملات DDoS در محیط‌های SDN، که به نمایش می‌گذارد نتایج امیدوارکننده در افزایش امنیت کنترل‌کننده‌های SDN و کاهش تأثیر از حملات DDoS. تلاش‌های آینده ممکن است شامل تقویت بیشتر قابلیت‌های خصمانه این چارچوب برای مقابله با استراتژی‌های در حال تحول حمله DDoS و بررسی عملی بودن آن در تنظیمات SDN در دنیای واقعی باشد. محدودیت‌ها شامل ضرورت اعتبارسنجی بیشتر در سناریوهای مختلف SDN و در نظر گرفتن تکنیک‌های فرار بالقوه خصمانه است.

چتوان و همکاران [[48]](#_bookmark64) به حوزه SDN می‌پردازد و از آن استفاده می‌کند دی ال روش‌شناسی‌ها به افزایش ‎‏ ... دقت از تشخیص ناهنجاری ترافیک ، با تمرکز ویژه بر شناسایی حملات DDoS. این مقاله با ارائه یک روش ترکیبی جدید DL، با ترکیب تکنیک‌های DNN و LSTM، به دنبال غلبه بر محدودیت‌های تشخیص نفوذ سنتی است. سیستم‌ها و دستگاه مبتنی بر یادگیری رویکردها.

نتایج تجربی و معیارها، هم از نظر عملکرد و هم از نظر امنیت، ارائه شده‌اند و بینش‌هایی در مورد اثربخشی تشخیص DDoS در SDN با استفاده از DL ارائه می‌دهند. موضوع اصلی تحقیق مورد بررسی، ضرورت تشخیص ناهنجاری ترافیک قابل اعتماد و دقیق در محیط‌های SDN، به ویژه در مورد حملات DDoS است. راه‌حل‌های موجود، شامل سیستم‌های تشخیص نفوذ مرسوم و روش‌های یادگیری ماشین، محدودیت‌هایی را از نظر دقت نشان می‌دهند. و کارایی. اولیه تحقیق عینی است معرفی کردن یک نوآورانه هیبریدی دی ال روش متناسب سازی شده برای تشخیص DDoS در SDN، با الف متعاقباً ارزیابی از آن عملکرد​ با استفاده از مربوط معیارها پیشنهادی سیستم توسط عمل می‌کند گرفتن شبکه ترافیک داده‌ها به عنوان ورودی و استخدام الف روش ترکیبی DL که تکنیک‌های DNN و LSTM را با هم ترکیب می‌کند. خروجی مستلزم طبقه‌بندی ترافیک به عنوان بی‌خطر یا نشان‌دهنده حمله DDoS است. این سیستم همچنین ادغام می‌کند الف روش‌شناسی به ارزیابی کردن مجموعه داده‌ها انطباق با الزامات از پیش تعریف‌شده . تنظیمات آزمایشی شامل استفاده از مجموعه داده‌های SDN حمله DDoS است که شامل روش‌های مختلف DL مانند شبکه عصبی کانولوشن، شبکه عصبی عمیق، شبکه عصبی مصنوعی (ANN)، LSTM و روش DL ترکیبی پیشنهادی می‌شود. معیارهای عملکرد شامل دقت، دقت، به یاد آوردن، امتیاز F1، و منطقه تحت ‎‏ ... منحنی (AUC)، در حالی که معیارهای امنیتی شامل مثبت کاذب (FP)، منفی کاذب (FN)، مثبت واقعی (TP) و منفی واقعی (TN) هستند. نتایج، برتری روش DL ترکیبی پیشنهادی را نشان می‌دهد و از سایر روش‌ها در دقت، دقت، فراخوانی و امتیاز F1 پیشی می‌گیرد. AUC نیز به طور قابل توجهی بالاتر است، در حالی که معیارهای امنیتی تعداد کمتری از FP و FN را نشان می‌دهند. مقایسه شده به جایگزین روش‌ها. این کاغذ مشارکت توسط ارائه الف پیشگامانه هیبریدی دی ال روش برای تشخیص DDoS در SDN، جفت شده با الف جامع ارزیابی با استفاده از معیارهای مربوطه. تلاش‌های آینده ممکن است شامل این پیشنهاد باشد از یک رویکرد برای مجموعه داده‌ها پردازش و دی ال آموزش/آزمایش مدل درون الف متمایز ابر مجازی ماشین (VM) قبل از استقرار SDN. محدودیت‌ها شامل اتکا به یک واحد است مجموعه داده‌ها، ایجاب کننده بیشتر ارزیابی در سناریوهای دنیای واقعی.

امباسوا و همکاران [[49]](#_bookmark65) به حوزه تشخیص DDoS می‌پردازد. در شبکه SDN با استفاده از دی ال. مطالعه آدرس‌ها ‎‏ ... چالش حیاتی تشخیص و کاهش موثر حملات DDoS در بافت پویا و قابل برنامه‌ریزی محیط‌های SDN. سنتی حملات انسداد سرویس (DDOS) تشخیص روش‌ها سقوط کوتاهی در تطبیق ویژگی‌های منحصر به فرد SDNها، باعث شده است که نیاز برای یک نوآورانه حملات انسداد سرویس (DDOS) تشخیص سیستم ریشه دار در عمیق یادگیری تکنیک‌ها طراحی شده به طور خاص برای SDNها. مسئله اصلی تحقیق حول پیچیدگی شناسایی و مقابله با حملات DDoS در محیط‌های SDN می‌چرخد، داده شده آنها حساسیت به بدخواه فعالیت‌ها به دلیل ذاتی پویایی و قابلیت برنامه ریزی موجود راه‌حل‌هایی که ریشه در روش‌های سنتی تشخیص DDoS دارند، فاقد همسویی بهینه با ویژگی‌های متمایز SDNها هستند. این تحقیق اهداف به پل این شکاف توسط معرفی کردن الف رمان تشخیص DDoS سیستم استخدام عمیق یادگیری تکنیک‌ها متناسب با ‎‏ ... ظریف الزامات از SDN ها. پیشنهادی سیستم شامل می‌شود جمع‌آوری شبکه ترافیک داده‌ها از شبکه SDN سوئیچ‌ها

به عنوان ورودی، در معرض قرار دادن آن به پردازش از طریق الف عمیق مبتنی بر یادگیری تشخیص مدل، و مولد حملات انسداد سرویس (DDOS) حمله خروجی‌های تشخیص به عنوان ‎‏ ... سیستم نتیجه. در ‎‏ ... تجربی فاز، واقعی شبکه SDN شبکه ترافیک داده‌ها بود شاغل به مدل یادگیری عمیق را برای تشخیص حمله DDoS آموزش دهید. نتایج اثبات شده ‎‏ ... اثربخشی از ‎‏ ... پیشنهادی سیستمی در تشخیص دقیق و کاهش حملات DDoS در SDNها. ارزیابی شامل معیارهای عملکردی مانند تشخیص دقت، نادرست مثبت نرخ، و کارایی محاسباتی، در کنار معیارهای امنیتی مربوط به تشخیص و پیشگیری از حمله. نتایجی که به طور خاص به تشخیص DDoS در SDN با استفاده از DL مرتبط بودند، ظرفیت سیستم را برای تشخیص دقیق و کاهش حملات DDoS برجسته کردند، که از طریق معیارهای عملکرد ارزیابی شده و امنیت معیارها. تحقیق مشارکت می‌کند توسط معرفی یک تخصصی حملات انسداد سرویس (DDOS) تشخیص سیستم به طور ریز تنظیم شده برای SDNها، با بهره‌گیری از تکنیک‌های یادگیری عمیق برای تقویت چشم‌انداز امنیتی چنین شبکه‌هایی. تلاش‌های آینده ممکن است شامل اصلاح بیشتر مدل یادگیری عمیق، گسترش طیف معیارهای امنیتی و انجام آزمایش‌های واقعی باشد. استقرار و آزمایش جهانی. محدودیت‌ها ممکن است شامل سازگاری مداوم با استراتژی‌های در حال تکامل حمله DDoS و سربار محاسباتی مرتبط با سیستم‌های تشخیص مبتنی بر یادگیری عمیق باشد.

سعید و همکاران [[50]](#_bookmark66) به بررسی حوزه استفاده از روش‌های یادگیری عمیق برای تشخیص حملات DDoS در SDNها می‌پردازد. آن تمرکز است ‎‏ ... ارزیابی از ‎‏ ... اثربخشی از مدل‌های یادگیری عمیق در شناسایی و کاهش حملات DDoS در بافت پویای SDNها. نگرانی اصلی مورد بررسی قرار گرفت در این بررسی است ‎‏ ... تشدید شونده آسیب‌پذیری از SDN ها به حملات DDoS به دلیل قابلیت انطباق و پویایی آنها طبیعت. سنتی نفوذ تشخیص سیستم‌ها، غالب​ راه حل ها، ممکن است سقوط کوتاه در گرفتن ‎‏ ... الگوها و پویایی‌های پیچیده ذاتی در داده‌های ترافیک شبکه. هدف این تحقیق ارزیابی عملکرد مدل‌های یادگیری عمیق است. در حملات انسداد سرویس (DDOS) تشخیص برای SDN ها و تشخیص دادن نقش آنها در تقویت امنیت شبکه در این حوزه. سیستم پیشنهادی از مدل‌های یادگیری عمیق، به ویژه رویکرد CNN-BiLSTM مبتنی بر توجه، برای تشخیص DDoS در SDNها استفاده می‌کند. داده‌های ترافیک شبکه به عنوان ورودی عمل می‌کنند و از طریق لایه‌های شبکه عصبی کانولوشن و بازگشتی پردازش می‌شوند تا وابستگی‌های زمانی محلی و جهانی را درک کنند. خروجی مستلزم ‎‏ ... طبقه بندی از ترافیک شبکه را بر اساس وجود حمله DDoS، به صورت عادی یا مخرب طبقه‌بندی می‌کند. تجربی چارچوب مورد استفاده قرار گرفت الف پیشگامی در SDN نفوذ مجموعه داده‌ها، ارزیابی کردن مختلف عمیق یادگیری مدل‌هایی برای تشخیص DDoS. معیارهای ارزیابی شامل دقت، یادآوری، امتیاز F1 و دقت، در کنار معیارهای امنیتی مانند نرخ تشخیص، نرخ مثبت کاذب و نرخ منفی کاذب بود. نتایج، اثربخشی مدل پیشنهادی CNN-BiLSTM مبتنی بر توجه را نشان داد و به نرخ تشخیص بسیار بالایی برای حملات DDoS در SDNها دست یافت. یافته‌های مربوط به تشخیص DDoS در SDNها از طریق یادگیری عمیق ، مدل CNN-BiLSTM مبتنی بر توجه پیشنهادی را برجسته کرد . مدل چشمگیر ۹۸.۰۳٪ تشخیص نرخ برای شناسایی حملات انسداد سرویس (DDOS) حملات. این تأکید می‌کند ‎‏ ... محوری نقش

ادغام مکانیسم‌های توجه در چارچوب یادگیری عمیق برای شناسایی مؤثر تهدیدات DDoS در SDNها. سهم این بررسی در اثبات سودمندی آن است. مدل‌های یادگیری عمیق، به ویژه CNN-BiLSTM مبتنی بر توجه رویکرد، در بالا بردن حملات انسداد سرویس (DDOS) تشخیص درون SDNها. مسیرهای تحقیقاتی آینده ممکن است شامل ایجاد زمینه‌های بیشتر باشد مقاوم عمیق یادگیری مدل‌ها ماهر در مقابله استراتژی‌های حمله DDoS در حال تکامل. محدودیت‌ها شامل اتکا به خاص مجموعه داده‌ها و ‎‏ ... ضروری برای بیشتر اعتبارسنجی در محیط‌های SDN دنیای واقعی. این بررسی جامع دانشگاهی، بینش‌های دقیقی در مورد کاربرد یادگیری عمیق برای تشخیص DDoS در SDNها ارائه می‌دهد و روشن می‌کند که ‎‏ ... پتانسیل از پیشرفته مدل‌ها به تقویت کردن شبکه امنیت در برابر تهدیدات سایبری در حال تکامل

1. **تحقیق شکاف‌ها**

کارهای موجود در زمینه تشخیص DDoS در SDN دارای محدودیت‌ها و شکاف‌های متعددی است که برای افزایش عملکرد و اثربخشی سیستم‌های پیشنهادی باید به آنها پرداخته شود. این موارد شامل فقدان روش‌های مؤثر و کارآمد برای تشخیص DDoS در SDN [[5] ،](#_bookmark21) [[6] ،](#_bookmark22) فقدان تحلیل تطبیقی جامع از یادگیری ماشینی متنوع و یادگیری عمیق الگوریتم‌ها برای حملات انسداد سرویس (DDOS) تشخیص در SDN، ارزیابی ناکافی رویکردهای پیشنهادی روی دستگاه‌های SDN واقعی و دنیای واقعی شبکه ترافیک، تمرکز روی دستیابی آموزش بلادرنگ برای تشخیص DDoS در SDN [[2] ،](#_bookmark18) [[21] ،](#_bookmark37) تحلیل محدود داده‌هایی که یک روز از یک مجموعه داده گسترده‌تر که چندین روز را در بر می‌گیرد را پوشش می‌دهد، اندازه‌گیری ترافیک به اندازه کافی دقیق در محیط‌های SDN، محدودیت‌ها از متعارف اندازه‌گیری روش‌شناسی‌ها برای ترافیک شبکه در SDN، عدم توانایی در مقابله با حملات DDoS در محیط‌های SDN [[1] ،](#_bookmark17) نیاز به کاوش در زمینه‌های پیشرفته‌تر دستگاه یادگیری الگوریتم‌ها به افزایش قابلیت‌های تشخیص و کاهش، و نیاز به ادغام پیشنهادها سیستم‌ها با دیگر موجود امنیت مکانیسم‌ها برای افزایش بیشتر امنیت شبکه [[20] .](#_bookmark36)

مطالعه پیشنهاد می‌کند چندین مناطق برای بهبود مربوط به تشخیص DDoS در SDN با استفاده از یادگیری ماشین و عمیق یادگیری تکنیک‌ها. اینها شامل شدن اکتشاف از الگوریتم‌های پیشرفته‌تر یادگیری ماشین و یادگیری عمیق برای افزایش قابلیت‌های تشخیص و کاهش آسیب‌پذیری سیستم، ادغام سیستم پیشنهادی با سایر سازوکارهای امنیتی موجود برای افزایش بیشتر امنیت شبکه، بهینه‌سازی بیشتر و جامع آزمایش درون در مقیاس بزرگتر شبکه محیط‌هایی برای اطمینان از اثربخشی سیستم در سناریوهای دنیای واقعی، گسترش مجموعه داده‌های سیستم برای شامل شدن در مقیاس بزرگتری از داده‌های ترافیک شبکه و سناریوهای آزمایش دنیای واقعی، افزایش قابلیت‌های سیستم برای گنجاندن الگوریتم‌های یادگیری ماشینی که می‌توانند با تهدیدات امنیتی در حال تحول سازگار شوند و عملکرد کلی سیستم را بهبود بخشند، سناریوهای آزمایش دنیای واقعی برای اعتبارسنجی قابلیت‌های سیستم اثربخشی، تطبیق دادن ‎‏ ... سیستم به دفاع کردن در برابر انواع دیگر حملات سایبری، گسترش عملکرد نرم‌افزار موجود، پرداختن به مسئله‌ی تشخیص‌های مثبت کاذب و نادرست منفی‌ها به بهبود بخشیدن ‎‏ ... دقت و کامل بودن حملات انسداد سرویس (DDOS) حمله تشخیص، و در حال توسعه معیارسنجی شده

مجموعه داده‌هایی که به‌طور خاص برای تشخیص حمله DDoS طراحی شده‌اند تا توسعه و آزمایش سیستم‌های تشخیص جدید را تسهیل کنند. به طور کلی، آنجا است قابل توجه محدوده برای پیشرفت‌هایی در چندین زمینه مرتبط با تشخیص DDoS در SDN وجود دارد و تحقیقات مداوم برای افزایش عملکرد و اثربخشی سیستم‌های پیشنهادی ضروری است.

1. **نتیجه‌گیری و آینده کار**

این مقاله مروری جامع بر وضعیت فعلی تشخیص انکار سرویس (DoS) در سیستم‌های نرم‌افزاری تعریف‌شده ارائه می‌دهد. شبکه‌ها (SDN) با استفاده از ماشین یادگیری (میلی لیتر) و تکنیک‌های یادگیری عمیق (DL). دامنه کاربرد

از این کار است متمرکز روی آدرس‌دهی ‎‏ ... ذاتی آسیب‌پذیری‌های امنیتی محیط‌های SDN و توسعه یک سیستم خودکار برای تشخیص و کاهش حملات شبکه. مشکل بیانیه از این تحقیق است ‎‏ ... نیاز برای موثر بودن دفاعی مکانیسم‌ها و تشخیص روش‌هایی برای رفع این آسیب‌پذیری‌ها. راه‌حل‌های پیشنهادی شامل موارد زیر است مختلف میلی لیتر و دی ال تکنیک‌ها. نتایج به دست آمده از ‎‏ ... ارزیابی معیارها تایید ‎‏ ... علامت گذاری شده اثربخشی سیستم‌های پیشنهادی در تشخیص و کاهش انواع حملات، از جمله حملات انکار سرویس توزیع‌شده (DDoS).

در ‎‏ ... قلمرو از حملات انسداد سرویس (DDOS) حمله تشخیص روی شبکه‌های تعریف‌شده توسط نرم‌افزار (SDN)، تحلیل مقایسه‌ای بین یادگیری ماشینی (میلی لیتر) و عمیق یادگیری (دی ال) رویکردها نقاط قوت متمایزی را آشکار می‌کند. مدل ML، که در مطالعه [[22] به تفصیل شرح داده شده است ،](#_bookmark38) از طبقه‌بندی‌کننده‌هایی مانند SVM، RF، DT، LR و KNN در یک آزمایش استفاده می‌کند. راه اندازی درون یک شبکه SDN محیط زیست. آن با طبقه‌بندی‌کننده‌های خاصی که به دقت ۱۰۰٪ می‌رسند، به نتایج قابل توجهی دست می‌یابد. ارزیابی شامل می‌شود عملکرد معیارها مانند​ دقت، دقت، به یاد آوردن، اف۱ امتیاز، و ROC-AUC، همراه با معیارهای امنیتی مانند نرخ مثبت کاذب و نرخ تشخیص. از سوی دیگر، مدل DL، همانطور که در تحقیق [[34] ارائه شده است ،](#_bookmark50) یک معماری یادگیری عمیق جدید مبتنی بر یک رمزگذار خودکار ترکیبی و شبکه ایست بازرسی را معرفی می‌کند. این مدل که بر روی داده‌های ترافیک شبکه جمع‌آوری‌شده توسط SDN آموزش دیده است، بین ترافیک عادی و حمله تمایز قائل می‌شود و به دقت قابل توجه 100٪، نرخ مثبت کاذب پایین و شناسایی موفقیت‌آمیز حملات DDoS فردی دست می‌یابد. در سراسر مختلف مجموعه داده‌ها. این تحقیق یک مدل پیشگام DL متناسب با تشخیص DDoS در SDNها ارائه می‌دهد، مشخصه‌یابی شده توسط بالا موفقیت نرخ‌ها و حداقل مثبت‌های کاذب .

کارهای آینده: مشارکت‌های بنیادی سیستم‌های پیشنهادی هستند آشکار در آنها اثربخشی برای هر دو حملات انسداد سرویس (DDOS) تشخیص حمله و دفاع درون ‎‏ ... شبکه SDN محیط زیست. با این حال، این بررسی محدودیت‌های ذاتی خاصی را تصدیق می‌کند و نیاز مبرم به اعتبارسنجی بیشتر در سناریوهای دنیای واقعی برای ارزیابی عملی بودن و اثربخشی روش‌های پیشنهادی. چشم‌انداز تحقیقات آینده ممکن است بر کاوش الگوریتم‌های یادگیری ماشین پیشرفته‌تر، در کنار ادغام سیستم پیشنهادی با سایر سازوکارهای امنیتی موجود برای افزایش بیشتر امنیت شبکه متمرکز باشد. علاوه بر این، اصلاح و بهینه‌سازی عملکرد سیستم، با تأکید ویژه بر متناسب‌سازی

برای پرداختن به جزئیات انواع خاص حمله، ضروری است. پیشنهادی سیستم‌ها مقیاس‌پذیری و تطبیق پذیری متفاوت شبکه محیط‌ها و پیکربندی‌ها هستند همچنین زمینه‌هایی برای تحقیقات آینده. علاوه بر این، توسعه موارد بیشتر جامع و دقیق مجموعه داده‌ها برای ارزیابی کردن اثربخشی سیستم‌های پیشنهادی ضروری است. علاوه بر این، ادغام سیستم‌های پیشنهادی با سایر سازوکارهای امنیتی، مانند فایروال‌ها و سیستم‌های تشخیص نفوذ، می‌تواند امنیت شبکه را افزایش داده و رویکردی جامع‌تر برای تشخیص و کاهش حملات شبکه ارائه دهد. بررسی تکنیک‌های پیشرفته‌تر، مانند خصمانه دستگاه یادگیری، می‌تواند همچنین فراهم کردن بیشتر مکانیسم‌های دفاعی قوی و مؤثر در برابر حملات پیچیده. در نتیجه، اثربخشی سیستم‌های پیشنهادی در تشخیص و کاهش انواع مختلف حملات، از جمله حملات DDoS، بر اهمیت توسعه بیشتر تأکید می‌کند. مؤثر و کارآمد تشخیص و کاهش روش‌های حملات DDoS در SDNها. محدودیت‌های سیستم‌های پیشنهادی و ‎‏ ... فشار دادن نیاز برای بیشتر اعتبارسنجی در سناریوهای دنیای واقعی، اهمیت تحقیق و توسعه مداوم در این زمینه را برجسته می‌کند. چشم‌اندازهای تحقیقاتی آینده که در این بررسی شناسایی شده‌اند، بینش‌های ارزشمندی در مورد حوزه‌های تحقیق و توسعه آینده در این زمینه ارائه می‌دهند.

**منابع**

1. ز. لیو، ی. وانگ، ف. فنگ، ی. لیو، ز. لی، و ی. شان، «الف» حملات انسداد سرویس (DDOS) تشخیص روشی مبتنی بر مهندسی ویژگی و یادگیری ماشین در نرم‌افزار «شبکه‌های تعریف‌شده» ، *حسگرها* ، جلد ۲۳، شماره ۱۳، ص ۶۱۷۶، ژوئیه ۲۰۲۳.
2. م. حماد، ن. هیواهی، و دبلیو. المدنی، «افزایش نفوذ به شبکه» بازیابی در SDN با یادگیری ماشین: یک رویکرد نوآورانه، *عرب*

*جی. پایه کاربرد علمی* ، جلد ۳۰، نه. ۱، ص. ۵۶۱–۵۷۲، دسامبر ۲۰۲۳.

1. جی. رامپراسات، ن. کریشناراج، و وی. سیتالاکشمی، کاهش اثرات خدمات روی شبکه SDN برای توزیع شده انکار از خدمات و انکار از خدمات حملات با استفاده از تکنیک‌های یادگیری ماشین، « *IETE J. Res.* ، صفحات ۱-۱۲، نوامبر ۲۰۲۲».
2. س. وانگ، جی. ف. بالارزو، ک. جی. چاوز، الف. الحورانی، س. کندیپان،

آقای اصغر و جی. راسللو، «تشخیص حملات DDoS سیل‌آسا در شبکه‌های تعریف‌شده توسط نرم‌افزار با استفاده از تکنیک‌های یادگیری نظارت‌شده،» *مهندس. علم و فناوری، مجله بین‌المللی* ، جلد ۳۵، نوامبر ۲۰۲۲، شماره ماده ۱۰۱۱۷۶.

1. آر. سانتوس، دی. سوزا، دبلیو. سانتو، ای. ریبیرو، و ای. مورنو، «ماشین» الگوریتم‌های یادگیری برای تشخیص حملات DDoS در SDN، " *همزمانی " محاسبات، تجربه عملی* ، جلد ۳۲، شماره ۱۶، اوت ۲۰۲۰، شماره ماده e5402.
2. ل. قهوهای مایل به زرد، ی. پان، جی. وو، جی. ژو، اچ. جیانگ، و ی. دنگ، «الف» جدید چارچوب برای تشخیص و دفاع در برابر حمله DDoS در محیط SDN، *IEEE اکسس* ، جلد ۸، صفحات ۱۶۱۹۰۸–۱۶۱۹۱۹، ۲۰۲۰.
3. M. Shakil، AFY Mohammed، R. Arul، AK بشیر، و JK Choi، یک چارچوب پویای جدید برای تشخیص DDoS در SDN با استفاده از فراابتکار خوشه‌بندی تیک، « *ترانس. امرگ. تله‌کامیون. تکنول.»* ، جلد ۳۳، شماره ۳، مارس ۲۰۲۲، شماره ماده e3622.
4. الف. اُ. سنگودوین، م. اُ. آکینسولو، پ. پیلای، و وی. دوغاب، تشخیص و طبقه‌بندی حملات سیل‌آسای DDoS به شبکه‌های نرم‌افزار محور: الف مطالعه موردی برای کاربرد یادگیری ماشین، « *IEEE Access* »، جلد ۹،

ص. ۱۲۲۴۹۵–۱۲۲۵۰۸، ۲۰۲۱. (یا: ۲۰۲۱)

1. جی. الف. پرز-دیاز، من. الف. والدوینوس، ک. آر. چو، و دی. ژو، یک معماری انعطاف‌پذیر مبتنی بر SDN برای شناسایی و کاهش آسیب‌پذیری‌های کم نرخ حملات انسداد سرویس (DDOS) حملات با استفاده از دستگاه یادگیری،'' *IEEE دسترسی* ، جلد ۸،

ص. ۱۵۵۸۵۹–۱۵۵۸۷۲، ۲۰۲۰. (۲۰۲۰)

1. م. الف. ریبیرو، م. س. پ. فونسکا، و جی. د سانتی، ''تشخیص'' و کاهش دهنده حملات DDoS با رویکرد دفاع هدف متحرک مبتنی بر خودکارسازی جریان طبقه بندی در شبکه SDN شبکه‌ها، *محاسبه. امن* . جلد ۱۳۴، نوامبر ۲۰۲۳، شماره ماده ۱۰۳۴۶۲.
2. ای. سبار و کی. زیک، «افزایش تاب‌آوری در برابر حملات DDoS در شبکه SDN مبتنی بر عرضه زنجیره ای شبکه‌ها با استفاده از دستگاه یادگیری،'' در *مجموعه مقالات نهم بین المللی Conf. کنترل، تصمیم گیری Inf. تکنولوژی (CoDIT)* ، ژوئیه 2023، صفحات 230-234.
3. آر. راج و اس. اس. کانگ، «کاهش حمله DDoS با استفاده از یادگیری ماشین» رویکرد در اس‌دی‌ان، در *مجموعه مقالات چهارم بین المللی کنفرانس پیشرفته محاسبه.، ارتباطات کنترل شبکه (ICAC3N)* ، دسامبر 2022، صفحات 462-467.
4. ک. م. سودار، م. بیولا، پ. دیپالاکشمی، پ. ناگاراج، و پ. چیناسامی، تشخیص حملات انکار سرویس توزیع‌شده در SDN با استفاده از ماشین «تکنیک‌های یادگیری»، در *مجموعه مقالات کنفرانس بین‌المللی کامپیوتر، ارتباطات، اطلاعات. (ICCCCI)* ، ژانویه ۲۰۲۱، صفحات ۱ تا ۵.
5. م. کاویتا، م. سوگانتی، الف. بیسواس، آر. سرینیوسان، آر. کاویتا، و

الف. راتش، «ماشین» یادگیری تکنیک‌ها برای تشخیص حملات انسداد سرویس (DDOS) حملات در SDN، در *مجموعه مقالات کنفرانس بین‌المللی خودکار، محاسبات، نوسازی، سیستم‌ها (ICACRS)* ، دسامبر ۲۰۲۲، صفحات ۶۳۴-۶۳۸.

1. ک. الحمامی و س. آلبرتانی، «تشخیص حمله DDOS با استفاده از دستگاه» «الگوریتم یادگیری در شبکه SDN»، در *مجموعه مقالات کنفرانس بین‌المللی الصادق. فناوری اطلاعات (AICCIT)* ، ژوئیه ۲۰۲۳، صفحات ۹۷-۱۰۲.
2. الف. تی. کیاو، م. زین اوه، و سی. س. خین، «یادگیری ماشینی» مبتنی بر حملات منع سرویس دابلیو‌اس «طبقه‌بندی‌کننده حمله در شبکه نرم‌افزار محور»، در *مجموعه مقالات هفدهمین کنفرانس بین‌المللی. برق مهندسی/الکترون محاسبه.، مخابرات اطلاعات فناوری (ECTI-CON)* ، ژوئن ۲۰۲۰، صفحات ۴۳۱-۴۳۴.
3. آر. آر. سکار، الف. م. جنی، دی. سرشتا، م. ویکاس، دی. ب. ن. آجی، و

ام. گانش، «پیش‌بینی حملات انکار سرویس توزیع‌شده در SDN» با استفاده از دستگاه یادگیری تکنیک‌ها، در *مجموعه مقالات سوم بین المللی کنفرانس هوش. فناوری (CONIT)* ، ژوئن ۲۰۲۳، صفحات ۱ تا ۵.

1. AK Kurakula، K. Akhila، M. Bhavya، و MV Sai، "تشخیص حملات DoS توزیع‌شده بر روی SDN با استفاده از روش‌های یادگیری ماشین (ML) در *مجموعه مقالات بین المللی کنفرانس نوآوری داده‌ها ارتباطات فناوری کاربرد (ICIDCA)* ، مارس ۲۰۲۳، صفحات ۷۶۷–۷۷۲.
2. ای. کی. تاهیرو، کی. کونات، و ام. ام. سودریدین، «تشخیص و کاهش» حملات DDoS در SDN با استفاده از یادگیری ماشینی (ML)، در مجموعه مقالات *Proc. Int. کنفرانس. رقمی. فناوری. سن. پیشرفته. حفظ. توسعه. (ICDATA)* ، مه 2023،

ص. ۵۲–۵۹.

1. س. ساناپالا، دی. دی. ردی، جی. ل. چوداری، و ک. س. ویکیات، «ماشین» تشخیص حمله DDoS مبتنی بر یادگیری در شبکه‌های نرم‌افزار محور (SDN) در *مجموعه مقالات دوم بین المللی کنفرانس لبه محاسبه. کاربرد (ICECAA)* ، ژوئیه ۲۰۲۳،

ص. ۱۱۲۴–۱۱۲۶.

1. س. فنگ، جی. یانگ، و دبلیو. مرد، «تحقیق» روی حملات انسداد سرویس (DDOS) حمله تشخیص مبتنی بر روی دستگاه یادگیری در شبکه SDN محیط زیست،'' در *مجموعه مقالات IEEE هفتم اطلاعات فناوری کنفرانس مهندسی مکاترونیک (ITOEC)* ، سپتامبر 2023، صفحات 821-825.
2. س. بالا و س. م. م. احسان، ''تشخیص'' حملات انسداد سرویس (DDOS) حملات در نرم‌افزار تعریف شبکه: رویکردی مبتنی بر یادگیری ماشین، در *مجموعه مقالات بین‌المللی. کنفرانس نسل بعدی. محاسبه.، اینترنت اشیا ماخ یاد بگیرید. (NCIM)* ، جون ۲۰۲۳،

ص. ۱–۶.

1. آ. ا. الاشاب، ام. اس. ام. زاهد، م. الاشاب، و س. الاشاب، «آنلاین» دستگاه یادگیری رویکرد به تشخیص و کاهش دادن نرخ پایین حملات انسداد سرویس (DDOS) حملات در مبتنی بر SDN شبکه‌ها، در *مجموعه مقالات IEEE بین المللی کنفرانس مصنوع هوش. مهندس فناوری (IICAIET)* ، سپتامبر ۲۰۲۳، صفحات ۱۵۲-۱۵۷.
2. BA المحگری، محمدعلی سعید، HM Alazaby، و AI محمد، رویکرد یادگیری ماشین برای حمله توزیع‌شده دانیل آف سرویس تشخیص در SDNها،» در *مجموعه مقالات سومین کنفرانس بین‌المللی فناوری هوشمند نوظهور. (eSmarTA)* ، اکتبر ۲۰۲۳، صفحات ۱ تا ۷.
3. الف. بنی‌طالبی دهکردی، م. سلطان آقایی، و ف. ز. بروجنی، «» حملات انسداد سرویس (DDOS) تشخیص حملات از طریق روش‌های یادگیری ماشین و آماری در SDN، *مجله سوپرکامپیوتر* ، جلد ۷۷، شماره ۳، صفحات ۲۳۸۳-۲۴۱۵، مارس ۲۰۲۱.
4. آ. لازاریس و وی. کی. پراسانا، «یک چارچوب LSTM برای نرم‌افزار- تعریف شده اندازه‌گیری، *IEEE ترانس. شبکه خدمات مدیریت کنید.* ، جلد ۱۸، نه. ۱،

صفحات ۸۵۵–۸۶۹، مارس. ۲۰۲۱. (یا: ۲۰۲۱)

1. اچ.-ام. چوانگ و ال.-جی. آره، ''درخواست دادن'' انتقال یادگیری رویکردها برای تشخیص نفوذ در شبکه‌های نرم‌افزار محور، « *پایداری »* ، جلد 15، نه 12، ص. 9395، ژوئن 2023.
2. ام اس ای سید، ن.-ای. لو-خاک، ام.ای. آذر، و ای.دی. جورکات، «یک جریان-» رویکرد تشخیص ناهنجاری مبتنی بر روش انتخاب ویژگی در برابر حملات انسداد سرویس (DDOS) حملات در SDN ها، *IEEE ترانس. شناختی ارتباطات شبکه* ، جلد ۸، نه. ۴،

ص. ۱۸۶۲–۱۸۸۰، دسامبر ۲۰۲۲.

1. ل. چن، ز. وانگ، آر. هو، و تی. هوانگ، «آن» خصمانه دی‌بی‌ان- روش LSTM برای تشخیص و دفاع در برابر حملات DDoS در SDN محیط‌ها، « *الگوریتم‌ها »* ، جلد ۱۶، شماره ۴، صفحه ۱۹۷، آوریل ۲۰۲۳.
2. تی. وی. فان، تی. جی. نگوین، ن.-ن. دائو، تی. تی. هونگ، ن. اچ. تان، و

تی. باوشرت، «دیپ گارد»: کارآمد ناهنجاری تشخیص در شبکه SDN با خوب- نظارت بر جریان ترافیک دانه‌بندی‌شده، « *مدیریت خدمات شبکه انتقال IEEE»* ، جلد ۱۷، شماره ۳، صفحات ۱۳۴۹–۱۳۶۲، سپتامبر ۲۰۲۰.

1. NS Shaji، T. Jain، R. Muthalagu، و PM Pawar، "کشف عمیق: کشف ناهنجاری در شبکه‌های نرم‌افزاری با استفاده از شبکه عصبی مصنوعی شبکه‌ها، '' *Comput. Secur.* ، جلد ۱۳۲، سپتامبر ۲۰۲۳، شماره ماده ۱۰۳۳۲۰.
2. NM Yungaicela-Naula، C. Vargas-Rosales، و JA Pérez-Díaz، چارچوب مبتنی بر SDN/NFV برای دفاع خودمختار در برابر حملات با نرخ پایین حملات DDoS با استفاده از یادگیری تقویتی، « *محاسبات نسل آینده».* *سیستم* ، جلد ۱۴۹، صفحات ۶۳۷-۶۴۹، دسامبر ۲۰۲۳.
3. س. حیدر، الف. آخندزاده، من. مصطفی، تی. ب. پاتل، الف. فرناندز،

ک. آر. چو، و جی. اقبال، «الف» عمیق سی‌ان‌ان گروه چارچوب برای کارآمد حملات انسداد سرویس (DDOS) حمله تشخیص در نرم‌افزار تعریف شده شبکه‌ها، *IEEE دسترسی* ، جلد ۸،

ص. ۵۳۹۷۲–۵۳۹۸۳، ۲۰۲۰. (۲۰۲۰)

1. ای. کی. موسی و ام. ان. عبدالله، «یک مدل یادگیری عمیق بهبود یافته» برای تشخیص DDoS مبتنی بر رمزگذار خودکار ترکیبی و ایست بازرسی «شبکه»، « *اینترنت آینده* »، جلد ۱۵، شماره ۸، صفحه ۲۷۸، آگوست ۲۰۲۳.
2. جی. وانگ و ل. وانگ، دفاع از SDN: الف سبک وزن آنلاین حمله تشخیص

و کاهش سیستم برای حملات انسداد سرویس (DDOS) حملات در اس‌دی‌ان، *حسگرها* ، جلد ۲۲، نه. ۲۱،

ص. ۸۲۸۷، اکتبر ۲۰۲۲.

1. تی.ای. علی، وای.-دبلیو. چونگ، و اس. مانیکام، «مقایسه یادگیری ماشینی/یادگیری یادگیری عمیق» رویکردها برای تشخیص حملات انسداد سرویس (DDOS) حملات در اس‌دی‌ان، *کاربرد علمی* ، جلد ۱۳، نه. ۵،

ص ۳۰۳۳، فوریه ۲۰۲۳.

1. تی. جی. گبرمسکل، ک. الف. گمدا، تی. جی. کریشنا، و پ. جی. رامولو، حملات منع سرویس توزیع‌شده (DDoS) تشخیص و طبقه‌بندی حمله با استفاده از مدل ترکیبی برای چندکنترل‌کننده اس‌دی‌ان، *بی‌سیم ارتباطات موبایل محاسبه.* ، جلد ۲۰۲۳، ص. ۱–۱۸، جون ۲۰۲۳.
2. الف. منصور، م. انبار، الف. باشوان، ب. العبسی، و س. ریحان، عمیق

رویکرد مبتنی بر یادگیری برای تشخیص حمله DDoS به سیستم‌های تعریف‌شده توسط نرم‌افزار کنترل‌کننده شبکه، « *سیستم‌ها »* ، جلد ۱۱، شماره ۶، صفحه ۲۹۶، ژوئن ۲۰۲۳.

1. م. پ. نواها، ل. ف. کاروالیو، جی. لورِت، و م. ل. پروئنسا، ''خصومت‌آمیز''

رویکرد یادگیری عمیق در تشخیص و دفاع در برابر حملات DDoS شبکه SDN محیط‌ها، *آینده ژنرال محاسبه. سیستم.* ، جلد ۱۲۵، ص. ۱۵۶–۱۶۷، دسامبر ۲۰۲۱. (یا: ۲۰۲۱)

1. م. پ. نواها، ل. ف. کاروالیو، جی. لورِت، و م. ل. پروئنسا، طولانی

حافظه کوتاه‌مدت و منطق فازی برای تشخیص و کاهش ناهنجاری بخش در نرم‌افزار محور شبکه محیط زیست،'' *IEEE دسترسی* ، جلد ۸،

ص. ۸۳۷۶۵–۸۳۷۸۱، ۲۰۲۰. (۲۰۲۰)

1. Y.-C. وانگ، Y.-C. هونگ، اچ.- ایکس. چن، و S.-M. Tseng، "شبکه تشخیص نفوذ ناهنجاری مبتنی بر رویکرد یادگیری عمیق، *حسگرها* ، جلد 23، شماره 4، ص. 2171، فوریه 2023.
2. ن. M. Yungaicela-Naula، C. Vargas-Rosales و جی. ای. پرز-دیاز، «اس‌دی‌ان-»

معماری مبتنی بر حمله DDoS در لایه انتقال و کاربرد تشخیص توسط با استفاده از دستگاه و عمیق یادگیری،'' IEEE دسترسی ، جلد ۹،

ص. ۱۰۸۴۹۵–۱۰۸۵۱۲، ۲۰۲۱. (یا: ۲۰۲۱)

1. جی. دی. گادز، الف. الف. بامفو-آسانته، جی. اُ. آگیمانگ، اچ. نونو-منسا و

KA-B. Opare، «تحقیقی در مورد کاربرد یادگیری عمیق» در تشخیص و کاهش حملات DDOS به کنترل‌کننده‌های SDN، *فناوری‌ها* ، جلد ۹، شماره ۱، ص ۱۴، فوریه ۲۰۲۱.

1. دی. الغزاوی، اُ. باماساگ، اچ. الله، و م. ز. اصغر، ''کارآمد''

تشخیص حملات DDoS با استفاده از یک مدل یادگیری عمیق ترکیبی با بهبود یافته ویژگی انتخاب،'' *کاربرد علمی* ، جلد ۱۱، نه. ۲۴، ص. ۱۱۶۳۴، دسامبر ۲۰۲۱. (یا: ۲۰۲۱)

1. م. لی، ب. ژانگ، جی. وانگ، ب. ژوگه، ایکس. جیانگ، و ل. دونگ، «الف» حملات انسداد سرویس (DDOS)

روش تشخیص حمله مبتنی بر مدل دو سطحی یادگیری عمیق CNN- LSTM در شبکه SDN، در *Proc. Int. Conf. Cloud Computing.، کلان داده* *Appl. نرم افزار مهندس (CBASE)* ، سپتامبر 2022، صفحات 282-287.

1. دبلیو. ژائو، اچ. خورشید، و دی. ژانگ، «تحقیق» روی حملات انسداد سرویس (DDOS) حمله تشخیص

روشی مبتنی بر مدل شبکه عصبی عمیق در SDN، در *مجموعه مقالات کنفرانس بین‌المللی.* *Netw. Netw. Appl. (NaNA)* ، دسامبر ۲۰۲۲، صفحات ۱۸۴-۱۸۸.

1. س. الف. کریستیلا و آر. سیواکومار، ''چند لایه گروه عمیق تقویت-

تشخیص و کاهش حملات DDoS مبتنی بر یادگیری ماشینی در شبکه ابری SDN محیط زیست،'' در *مجموعه مقالات چهارم بین المللی کنفرانس مدارها، کنترل، ارتباطات محاسبه.* *(I4C)* ، دسامبر ۲۰۲۲، صفحات ۴۵۱-۴۵۵.

1. الف. چتوان و ک. کارویی، ''عملکرد'' بهبود از حملات انسداد سرویس (DDOS)

مدل تشخیص نفوذ با استفاده از روش یادگیری عمیق ترکیبی در SDN محیط زیست،'' در *مجموعه مقالات IEEE بیست و یکم بین المللی کنفرانس فراگیر محاسبه. ارتباطات* *(IUCC/CIT/DSCI/SmartCNS)* ، دسامبر 2022، صفحات 159-166.

1. یو. امباسووا و جی. ل. زودی، طراحی گروه عمیق نفوذ یادگیری

تشخیص سیستم برای حملات انسداد سرویس (DDOS) حملات در نرم‌افزار تعریف شده شبکه‌ها، در *مجموعه مقالات شانزدهم بین المللی کنفرانس فراگیر اطلاعات مدیریت کنید. ارتباطات (ایمکام)* ، جان ۲۰۲۲،

ص. ۱–۸.

1. آر. ب. گفت و من. عسکرزاده، «مبتنی بر توجه» CNN-BiLSTM عمیق

رویکرد یادگیری برای سیستم تشخیص نفوذ شبکه در نرم‌افزار «شبکه‌های تعریف‌شده»، در *مجموعه مقالات پنجمین کنفرانس بین‌المللی مسائل سایبری. اطلاعات.* *(PCI)* ، اوت ۲۰۲۳، صفحات ۱ تا ۵.

1. سیسکو. (سپتامبر ۲۰۱۸). *سیسکو سالانه اینترنت گزارش (۲۰۱۸–۲۰۲۳) سفید*

*کاغذ* . [آنلاین]. موجود است: [https://www.cisco.com/c/en/us/solutions/](http://www.cisco.com/c/en/us/solutions/) وثیقه/دیدگاه‌های اجرایی/گزارش-اینترنتی-سالانه/گزارش-وایت-کاغذ-c11- ۷۴۱۴۹۰.html

1. *CSE-CIC-IDS2018 روی آمازون کانادایی موسسه برای امنیت سایبری* .

دسترسی‌ها: جان ۲۴، ۲۰۲۴. [آنلاین]. موجود است: [https://www.unb.ca/](http://www.unb.ca/) cic/datasets/ids-2018.html

نورا شفا موسی مدرک لیسانس خود را دریافت کرد مدرک مهندسی کامپیوتر از دانشگاه قطر تنوع (QU)، قطر، و ‎‏ ... کارشناسی ارشد مدرک در امنیت اطلاعات از کالج فناوری اطلاعات، امارات متحده عربی دانشگاه (امارات متحده عربی)، امارات متحده عربی. او در حال حاضر سرپرست ارشد آزمایشگاه است کالج از مهندسی، آل عین دانشگاه (AAU)، یونایتد عرب امارات. تظاهرات الف عمیق فداکاری به در حال پیشرفت سایبری امنیت اقدامات،

علایق تحقیقاتی او شامل توسعه راه‌حل‌های نوآورانه برای بهبود امنیت دیجیتال، بررسی تهدیدات سایبری، کاوش در محاسبات ابری فناوری و انجام تحقیقات پزشکی قانونی دیجیتال. او دریافت کرد جوایز و افتخارات.

ندا مسعود میرزا نشان BE را دریافت کرد و مدرک کارشناسی ارشد در رشته مهندسی مکاترونیک از دانشکده برق و مکانیک مهندسی، دانشگاه ملی علوم و فناوری (دانشگاه ملی علوم و فناوری) پاکستان او است فعلاً یک مربی با ‎‏ ... کالج از مهندسی، یونایتد دانشگاه امارات متحده عربی (UAEU)، امارات متحده عربی امارات. تحقیقات کارشناسی ارشد او عمدتاً متمرکز روی ‎‏ ... کاربرد از مصنوعی هوش، رباتیک، و بی‌سیم نظارت از تجدیدپذیر

سیستم‌های انرژی. او چند سالی در دانشگاه‌های پاکستان کار کرد، کجا او تحقیق علاقه شامل می‌شود خودمختار بی‌سیم هوشمند رباتیک سیستم‌ها. از آنجایی که ۲۰۱۴، او دارد شده درگیر در دانشگاهی فعالیت‌ها مرتبط به مهندسی کنترل و الکترونیک در امارات متحده عربی

سعیده حفصه رفیق مدرک لیسانس خود را در رشته تلفن همراه و زیست‌شناسی مولکولی از دانشگاه امارات متحده عربی (UAEU)، ایالات متحده امارات متحده عربی، در سال ۲۰۱۹، و مدرک کارشناسی ارشد علوم جنایی از ... دانشگاه از استراتکلاید، بریتانیا، در ۲۰۲۰. (۲۰۲۰) او است فعلاً در حال تعقیب ‎‏ ... کارشناسی ارشد مدرک کارشناسی ارشد امنیت اطلاعات از دانشگاه امارات متحده عربی. علایق پژوهشی او عبارتند از: ابر امنیت، ‎‏ ... اینترنت اشیا امنیت، مصنوعی هوش، دیجیتال پزشکی قانونی، و پزشکی قانونی علم.

امیرا ماهات عبدالله دریافت شده ‎‏ ...

مدرک لیسانس علوم کامپیوتر از دانشگاه طیبه دانشگاه، سعودی عربستان، در ۲۰۱۸. (۲۰۱۸) او است فعلاً ادامه تحصیل در مقطع کارشناسی ارشد در رشته امنیت اطلاعات با دانشگاه امارات متحده عربی، ایالات متحده امارات متحده عربی. علایق پژوهشی او شامل موارد زیر است: امنیت ابری، سیستم‌های تشخیص نفوذ و مصنوعی هوش.

تانگاول موروگان (عضو ارشد، IEEE) مدرک لیسانس (BE) را دریافت کرد (با افتخار) در علوم کامپیوتر و مهندسی از کالج مهندسی MAM (تریچی)، آنا دانشگاه، چنای، ‎‏ ... کارشناسی ارشد (کارشناسی ارشد) مدرک (افتخاری) در علوم کامپیوتر و مهندسی از ‎‏ ... جی. جی. کالج از مهندسی و فناوری (تریچی)، دانشگاه آنا، و مدرک دکترا از موسسه مدرس فناوری (دانشگاه ام آی تی) پردیس، آنا دانشگاه.

او در حال حاضر استادیار گروه اطلاع رسانی است. سیستم‌ها و امنیت، دانشکده فناوری اطلاعات، امارات متحده عربی دانشگاه امارات. او همچنین بیش از ۱۱ سال سابقه تدریس و تجربه تحقیقاتی از موسسات دانشگاهی مختلف. او مقالاتی منتشر کرده است بیشتر از ده مقالات در بین‌المللی مجلات، بیشتر از ۱۵ کتاب فصل‌ها در بین‌المللی ناشران، بیشتر از ۲۵ در ‎‏ ... دادرسی از بین‌المللی کنفرانس‌ها، و سه در ‎‏ ... دادرسی از ملی کنفرانس‌ها/سمینارها. علایق علمی و پژوهشی او شامل امنیت اطلاعات، ... محاسبات عملکردی، هک اخلاقی، جرم‌شناسی سایبری، بلاکچین، اطلاعات امنیت سایبری و فناوری آموزشی.