

دریافت‌شده در ۱۱ سپتامبر ۲۰۲۴، پذیرفته‌شده در ۱۵ اکتبر ۲۰۲۴، تاریخ انتشار ۲۴ اکتبر ۲۰۲۴، تاریخ نسخه فعلی ۱۹ نوامبر ۲۰۲۴.

*دیجیتال شیء شناسه ‎۱۰.۱۱۰۹/دسترسی.۲۰۲۴.۳۴۸۶۰۳۴‎*

**

تشخیص حملات انسداد سرویس (DDOS) تهدیدها با استفاده از دستگاه تحت نظارت یادگیری برای ترافیک طبقه‌بندی در شبکه سازی تعریف شده توسط نرم افزار

عبدیناسیر هیرسی [](https://orcid.org/0000-0001-8543-6134)۱ ، (فارغ التحصیل دانشجو عضو، IEEE)،

LUKMAN AUDAH [](https://orcid.org/0000-0002-0958-4474)1,2 , (Member, IEEE), ADEB SALH [](https://orcid.org/0000-0001-8880-6153)3 , (Member, IEEE), MOHAMMED الف. الهارتومی [](https://orcid.org/0000-0002-5955-8864)۴ ، (عضو، IEEE)،

و سلمان احمد [](https://orcid.org/0009-0003-7129-7892)۵ ، (فارغ التحصیل دانشجو عضو، IEEE)

۱ مرکز تحقیقات پیشرفته مخابرات (ATRC)، دانشکده مهندسی برق و الکترونیک، دانشگاه تون حسین اون مالزی، پاریت راجا ۸۶۴۰۰، مالزی

۲ دانشکده از برق و الکترونیکی مهندسی، دانشگاه تون حسین اون مالزی، پاریت راجا ۸۶۴۰۰، مالزی

۳ دانشکده اطلاعات و ارتباطات فناوری، دانشگاه تونکو عبدل رحمان (اوتار)، کامپار ۳۱۹۰۰، مالزی

۴ دپارتمان مهندسی برق، دانشگاه تبوک، تبوک ۷۱۴۹۱، عربستان سعودی

۵ گروه تخصصی VLSI و فناوری نهفته (VEST)، دانشکده مهندسی برق و الکترونیک، دانشگاه تون حسین اون مالزی، پاریت راجا ۸۶۴۰۰، مالزی

متناظر نویسندگان: لقمان عوده [(hanif@uthm.edu.my)](mailto:(hanif@uthm.edu.my) و ادب صالح [(adebali@utar.edu.my)](mailto:(adebali@utar.edu.my)

این کار توسط وزارت آموزش عالی (MOHE) از طریق طرح کمک هزینه تحقیقات بنیادی تحت عنوان کمک هزینه حمایت شد. FRGS/1/2022/TK07/UTHM/02/25.

 **چکیده** شبکه نرم‌افزار محور (SDN) یک راهکار امیدوارکننده برای مدیریت شبکه‌های بزرگ مقیاس است. که پیشنهادات گسترده فرصت‌ها برای بهینه سازی. با این حال، ‎‏ ... متمرکز کنترل ویژگی‌های ذاتی SDN، شبکه‌ها را در معرض تهدیدات امنیتی، به‌ویژه حملات انکار سرویس توزیع‌شده (DDoS) قرار می‌دهد. برای پرداختن به این چالش‌ها، تکنیک‌های یادگیری ماشین (ML) به عنوان ابزارهای قدرتمندی برای تشخیص و کاهش ناهنجاری ظهور کرده‌اند. این مقاله رویکرد جدیدی را برای طبقه‌بندی ترافیک در محیط‌های SDN ارائه می‌دهد که با استفاده از تکنیک‌های یادگیری ماشین نظارت‌شده، بین ترافیک خوش‌خیم و مخرب تمایز قائل می‌شود. مطالعه معرفی می‌کند الف منحصر به فرد مجموعه داده‌ها متناسب سازی شده برای حملات انسداد سرویس (DDOS) حمله تشخیص، غلبه بر ‎‏ ... محدودیت‌های مجموعه داده‌های موجود، مانند توپولوژی‌های غیرواقعی و عدم دسترسی عمومی. معیارسنجی در برابر CICDDoS2019 مجموعه داده‌ها اعتبارسنجی شده ‎‏ ... اثربخشی و اهمیت از ‎‏ ... سفارشی مجموعه داده‌ها. این این تحقیق پیامدهای قابل توجهی برای کاربردهای دنیای واقعی دارد و قابلیت‌های بهبود یافته‌ای را برای تشخیص و کاهش خطرات ارائه می‌دهد. حملات انسداد سرویس (DDOS) حملات در شبکه SDN زیرساخت. تجربی نتایج نشان داده شده ‎‏ ... اثربخشی از پیشنهادی تصادفی جنگل مدل، دستیابی به الف قابل توجه دقت از ۹۸.۹۷٪ و الف حداقل نادرست زنگ هشدار نرخ (FAR) برابر با 0.023. این یافته‌ها پتانسیل رویکردهای مبتنی بر یادگیری ماشینی را در افزایش امنیت شبکه برجسته می‌کند. و تاب‌آوری علیه حملات انسداد سرویس (DDOS) حملات در شبکه SDN محیط‌ها، سنگفرش ‎‏ ... راه برای آینده پیشرفت‌ها در استراتژی‌های دفاع شبکه‌ای

 **اصطلاحات شاخص** تشخیص ناهنجاری، هوش مصنوعی، حملات انکار سرویس توزیع‌شده (DDoS)، یادگیری ماشین، شبکه تعریف‌شده توسط نرم‌افزار (SDN)، یادگیری نظارت‌شده، طبقه‌بندی ترافیک.

1. **مقدمه**

نرم‌افزار محور شبکه‌سازی (اس‌دی‌ان) دارد پدیدار شد به عنوان الف معماری فناوری نوین که راه‌حل‌های بالقوه‌ای برای مسائل همواره در حال تکامل ارائه می‌دهد چالش‌ها مواجه شد توسط صنایع در مدیریت و

[](https://orcid.org/0000-0002-0917-2277) وابسته ویرایشگر هماهنگ کننده ‎‏ ... بررسی از این نسخه خطی و ییمینگ تانگ آن را برای انتشار تأیید کرد .

بهینه‌سازی زیرساخت شبکه [[1] .](#_bookmark81) علاوه بر این، با آن متمرکز کنترل و قابل برنامه‌ریزی ویژگی‌ها، شبکه SDN به دست آورده است قابل توجه توجه زیرا از آن توانایی به افزایش انعطاف‌پذیری، مقیاس‌پذیری و کارایی شبکه [[2 ]](#_bookmark82) [[3] .](#_bookmark83) شبکه SDN معماری شامل می‌شود سه متمایز لایه‌ها: کاربرد، کنترل و داده‌ها. شکل [1](#_bookmark5) این رویکرد لایه‌ای را نشان می‌دهد، که تسهیل می‌کند ‎‏ ... جداسازی از ‎‏ ... به طور سنتی محکم

جلد ۱۲، ۲۰۲۴

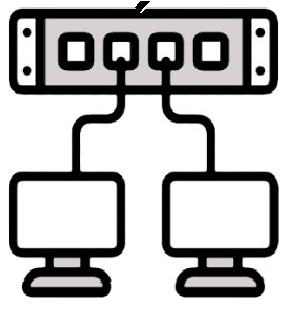
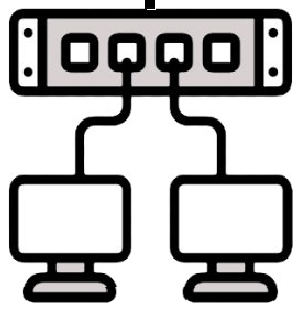
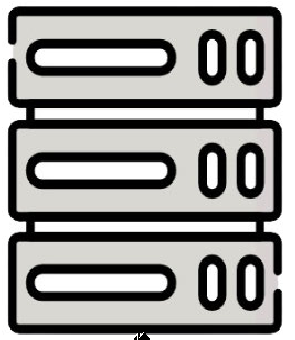
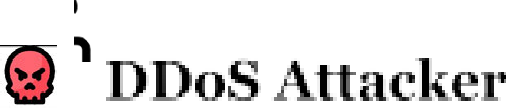
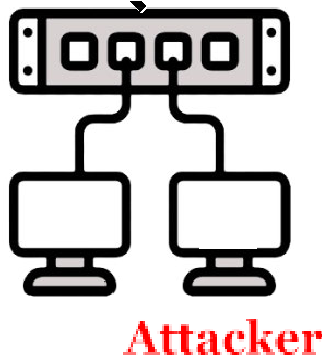
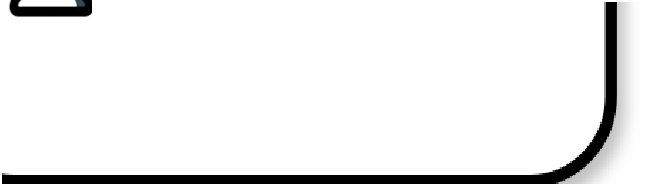
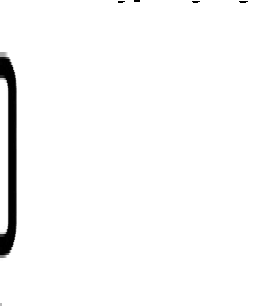
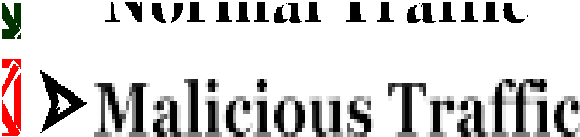
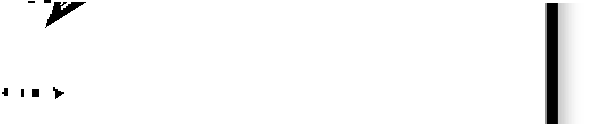
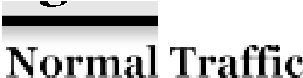
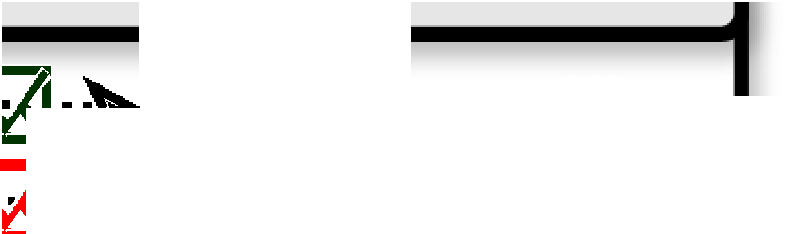
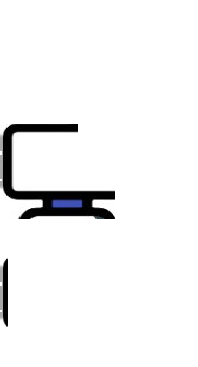
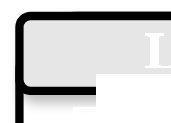
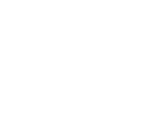
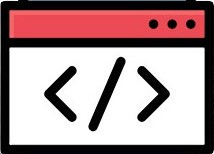
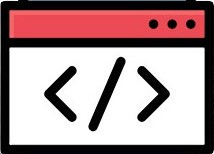
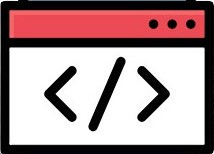
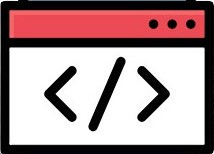
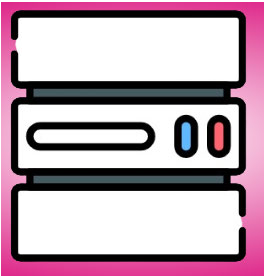
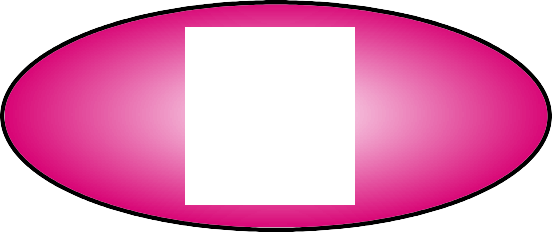
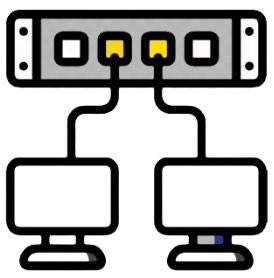
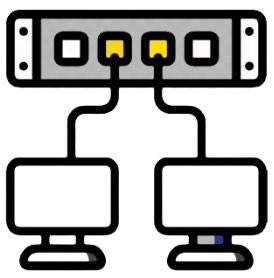
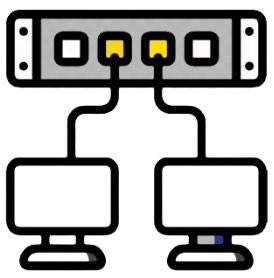
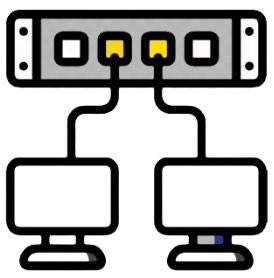
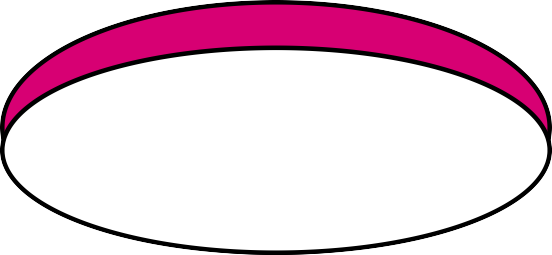
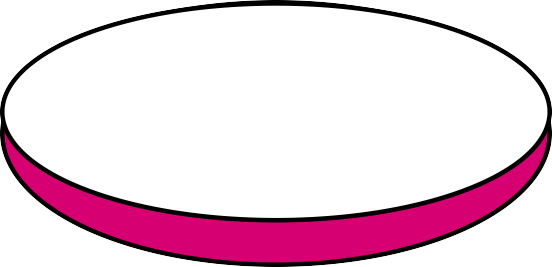
© ۲۰۲۴ نویسندگان. این اثر دارای مجوز است تحت مجوز Creative Commons مجوز انتساب-غیرتجاری-بدون مشتق ۴.۰ .

برای بیشتر اطلاعات، دیدن https://creativecommons.org/licenses/by-nc-nd/4.0/ 166675 ​

سطوح داده، کنترل و برنامه کاربردی یکپارچه. در SDN، ‎‏ ... داده‌ها هواپیما مسئول برای حمل و نقل شبکه ترافیک است جدا شده از ‎‏ ... کنترل هواپیما، که نحوه مدیریت ترافیک را تعیین می‌کند. این جداسازی، انعطاف‌پذیری و چابکی بیشتری را در مدیریت شبکه فراهم می‌کند. علاوه بر این، در ‎‏ ... کاربرد لایه، شبکه مدیران می‌توانند با تعریف قوانین و سیاست‌های حاکم بر رفتار ترافیک و تخصیص منابع، بر کل شبکه کنترل اعمال کنند. این کنترل متمرکز، مدیریت کارآمد شبکه را امکان‌پذیر می‌سازد. و بهینه سازی. متن‌باز پلتفرم‌ها، مانند OpenFlow و OpenDaylight، با ارائه راه‌حل‌های سازگار که به هیچ فروشنده خاصی وابسته نیستند، نقش مهمی در پذیرش SDN ایفا کرده‌اند [[4] ،](#_bookmark84) [[5] .](#_bookmark85) این امر نوآوری و انعطاف‌پذیری را در استقرار شبکه تقویت می‌کند.

خرابی‌های گسترده شبکه. این امر حملات DDoS را به یک تهدید حیاتی برای محیط‌های SDN تبدیل می‌کند.

**شکل ۲.** حملات انسداد سرویس (DDOS) حمله سناریو.



**شکل ۱.** نرم‌افزار تعریف شده شبکه معماری.

با این حال، ‎‏ ... متمرکز طبیعت از شبکه SDN معرفی می‌کند قابل توجه امنیت چالش‌ها، به ویژه ‎‏ ... ریسک از حملات انکار سرویس توزیع‌شده (DDoS). یک کنترل‌کننده واحد که کل شبکه را اداره می‌کند، می‌تواند به یک نقطه شکست واحد تبدیل شود، بدین وسیله افشاگری ‎‏ ... شبکه به امنیت تهدیدها [[6] .](#_bookmark86) حملات DDoS حملات، مشخصه‌یابی شده توسط آنها توزیع شده ماهیت و هماهنگی از منابع متعدد، می‌تواند یک شبکه یا سرویس هدف را تحت الشعاع قرار دهد و منجر به اختلالات شدید در دسترس‌پذیری و عملکرد شود [[7] .](#_bookmark87) همانطور که در شکل [2 نشان داده شده است](#_bookmark6) ، کنترل متمرکز در SDN تأثیر این حملات را افزایش می‌دهد. زیرا الف به خطر افتاده کنترل کننده می‌تواند سرب به

روش‌های سنتی تشخیص و کاهش حملات DDoS در SDN اغلب به دلیل ویژگی‌های منحصر به فرد این شبکه‌ها ناکافی هستند. تکنیک‌هایی مانند فیلترینگ مبتنی بر آدرس IP با تاکتیک‌هایی مانند جعل IP، سازی آن دشوار​ به تمایز قائل شدن بین ترافیک مشروع و مخرب [[8] .](#_bookmark88) در محیط‌های SDN، حملات DDoS که صفحه داده را هدف قرار می‌دهند، می‌توانند باعث ازدحام و اختلال در سرویس شوند. تخریب [[9] ،](#_bookmark89) در حالی که حملات هدف‌گیری ‎‏ ... هواپیمای کنترل می‌تواند عواقب شدیدتری داشته باشد و باعث اختلال در کل کار شبکه‌ای عملیات توسط سازشکارانه ‎‏ ... کنترل کننده متمرکز [[10] .](#_bookmark90) علاوه بر این، حملات انسداد سرویس (DDOS) حملات می‌تواند هدف رابط‌های شبکه، سوءاستفاده از آسیب‌پذیری‌های دستگاه‌های شبکه و ایجاد اختلال ‎‏ ... ارتباط بین متفاوت اجزا شبکه، منجر به قطع سرویس و به خطر افتادن یکپارچگی شبکه می‌شود [[11] .](#_bookmark91)

تشخیص حملات DDoS در SDN همچنان یک چالش اساسی است مدیون به ‎‏ ... پیچیدگی و پویا ماهیت ترافیک شبکه. روش‌های تشخیص سنتی اغلب در شناسایی حملات در مراحل اولیه خود با مشکل مواجه می‌شوند و شبکه‌ها را در برابر اختلالات طولانی مدت و داده‌های بالقوه آسیب‌پذیر می‌کنند. نقض‌ها [[12] .](#_bookmark92) این دارد رهبری کرد به افزایش یافته علاقه در ادغام تکنیک‌های یادگیری ماشین (ML) برای افزایش قابلیت‌های تشخیص DDoS. الگوریتم‌های ML می‌توانند مقادیر زیادی از داده‌های ترافیک شبکه را به صورت بلادرنگ تجزیه و تحلیل کنند و این امکان را فراهم کنند ‎‏ ... اوایل تشخیص از غیرعادی الگوها نشان دهنده حملات DDoS [[13] . با یادگیری از](#_bookmark93) داده‌های حمله تاریخی ، میلی لیتر مدل‌ها می‌تواند تشخیص ظریف انحرافات از رفتار عادی شبکه و فعال کردن هشدارها قبل از اینکه حمله به طور کامل خود را نشان دهد.

با این حال، اعمال تکنیک‌های یادگیری ماشینی در محیط‌های SDN، ... خاص چالش‌ها که باید باش خطاب شده به اثربخشی آنها را تضمین کند. یکی از چالش‌های اصلی، الزام طبقه‌بندی ترافیک در لحظه در داده‌های بسیار پویا است. شبکه محیط‌ها [[14] .](#_bookmark94) SDN ها تولید کردن الف بزرگ

حجم الگوهای ترافیکی متنوع، تمایز بین ترافیک بی‌خطر و مخرب را در زمان واقعی دشوار می‌کند. در نتیجه، این پیچیدگی می‌تواند منجر به نرخ بالای مثبت کاذب شود که با طبقه‌بندی نادرست ترافیک مشروع به عنوان مخرب، عملکرد شبکه را کاهش می‌دهد [[15] .](#_bookmark95) علاوه بر این، ‎‏ ... اثربخشی از مبتنی بر یادگیری ماشینی حملات انسداد سرویس (DDOS) تشخیص بستگی به در دسترس بودن داده‌های آموزشی با کیفیت بالا دارد. مجموعه داده‌های موجود اغلب از محدودیت‌هایی مانند توپولوژی‌های شبکه قدیمی، سناریوهای حمله غیرواقعی و عدم دسترسی عمومی رنج می‌برند که قابلیت‌های تعمیم مدل‌های یادگیری ماشینی آموزش دیده بر روی آنها را تضعیف می‌کند [[16] ،](#_bookmark96) [[17] .](#_bookmark97)

برای پرداختن به این چالش‌ها، این مطالعه یک رویکرد جدید برای بهبود طبقه‌بندی ترافیک در محیط‌های SDN با استفاده از تکنیک‌های یادگیری ماشینی نظارت‌شده ارائه می‌دهد. با تمرکز بر پیکربندی‌های واقع‌بینانه شبکه و حمله DDoS معاصر سناریوها، این مطالعه اهداف به غلبه بر ‎‏ ... محدودیت‌های موجود مجموعه داده‌ها و افزایش ‎‏ ... تشخیص قابلیت‌ها از ML مدل‌ها برای متمایز کننده بین خوش‌خیم و ترافیک مخرب [[18] .](#_bookmark98) علاوه بر این، این رویکرد در برابر مجموعه داده‌های معتبر مانند CICDDoS2019 اعتبارسنجی شده است که پتانسیل آن را برای بهبود امنیت و قابلیت اطمینان زیرساخت‌های شبکه مبتنی بر SDN نشان می‌دهد.

* 1. *ادبیات زمینه و مشارکت‌های پژوهشی*

این بخش، مروری انتقادی بر متون موجود در مورد حملات DDoS به SDN با استفاده از تکنیک‌های یادگیری ماشین ارائه می‌دهد. چندین مطالعات داشته باشند کاوش شده ‎‏ ... کاربرد از میلی لیتر به تشخیص و کاهش دادن حملات انسداد سرویس (DDOS) حملات در شبکه SDN محیط‌ها. با این حال، یک شکاف قابل توجه که در این مطالعات شناسایی شده است، عدم توجه به انتخاب ویژگی‌های مهم در ... مجموعه داده‌ها. با وجود ‎‏ ... تکثیر از تحقیق در این در این حوزه، مطالعات موجود اغلب اهمیت انتخاب ویژگی را نادیده گرفته‌اند، که برای اثربخشی و کارایی بسیار مهم است. از میلی لیتر مدل‌ها برای حملات انسداد سرویس (DDOS) تشخیص و کاهش. علاوه بر این، در حالی که محققان متعددی مجموعه داده‌هایی را برای تجزیه و تحلیل حمله DDoS در SDN ایجاد کرده‌اند، این مجموعه داده‌ها اغلب فقدان مفصل ویژگی‌ها و هستند نه عمومی موجود است. این فقدان شفافیت و دسترسی، مانع تکرارپذیری و مقایسه‌پذیری یافته‌های تحقیق می‌شود و در نتیجه پیشرفت دانش در این زمینه را محدود می‌کند. علاوه بر این، بسیاری از مطالعات نتوانسته‌اند مجموعه داده‌های خود را با مجموعه داده‌های عمومی موجود محک بزنند یا معیارهای عملکرد را ایجاد کنند، در نتیجه ارزیابی و اعتبارسنجی روش‌های پیشنهادی خود را محدود می‌کنند. عدم وجود محک‌زنی نه تنها اعتبار تحقیقات را تضعیف می‌کند، بلکه با جلوگیری از مقایسه‌ها و نتیجه‌گیری‌های معنادار، مانع پیشرفت در این زمینه نیز می‌شود. پیشرفت‌ها به طور کلی، ما تحقیق مشارکت‌ها از چندین جنبه با مطالعات قبلی متمایز است .

ساهو و همکاران [[19]](#_bookmark99) مجموعه داده‌ای که به عنوان «مجموعه داده-I» شناخته می‌شود در این مطالعه، شامل ۲,۱۶۰,۶۶۸ سوابق با ۲۷ ویژگی‌ها، به عنوان یک مجموعه داده DDoS مدرن توصیف می‌شود که برای آموزش و ... استفاده می‌شود. آزمایش اهداف. در تضاد، مجموعه داده-II، شناخته شده به عنوان NSL-KDD، به صراحت به عنوان نسخه اصلاح‌شده KDD'99 ذکر شده است. مجموعه داده‌ها. آن است قابل توجه که مجموعه داده-۱ است نه عمومی

در دسترس نیست زیرا منبع یا روش تولید آن به صراحت در این مطالعه بیان نشده است. این عدم دسترسی به مجموعه داده‌ها، اهمیت شفافیت و تکرارپذیری را برجسته می‌کند. در تحقیق، برجسته سازی ‎‏ ... نیاز برای مجموعه داده‌های در دسترس عموم برای تسهیل اعتبارسنجی و مقایسه نتایج در زمینه تشخیص حمله DDoS.

مطالعه انجام شده توسط کوجور و پاتل [[20]](#_bookmark100) برای ارائه اطلاعات دقیق در مورد ویژگی‌ها و ترکیب مجموعه داده‌ها ناکافی بود. بدون درک کامل از ویژگی‌های یک مجموعه داده، تعیین مناسب بودن و نماینده بودن آن دشوار است. در ارزیابی مدل‌های تشخیص حملات DDoS در محیط‌های SDN. علاوه بر این، این مطالعه هیچ اعتبارسنجی را ذکر نکرده است. یا تأیید فرآیندها برای ‎‏ ... مندلی مجموعه داده‌ها. غیبت از مناسب اعتبارسنجی رویه‌ها بالا می برد نگرانی‌ها در مورد قابلیت اطمینان و تکرارپذیری یافته‌های تجربی.

ایسیاکو و همکاران [[21]](#_bookmark101) مطالعه‌ای انجام دادند که در آن اثربخشی هشت طبقه‌بندی‌کننده یادگیری ماشینی در تشخیص و کاهش حملات DDoS در SDNها مقایسه شده بود. آن‌ها از یک مجموعه داده تولید شده استفاده کردند، اما این مطالعه فاقد شفافیت در مورد منبع و در دسترس بودن مجموعه داده بود. این امر نگرانی‌هایی را در مورد مقیاس‌پذیری و نمایندگی نتایج ایجاد می‌کند. اعتبارسنجی خارجی مجموعه داده‌های دنیای واقعی برای افزایش اعتبار و تأثیر تحقیق بسیار مهم است. این مطالعه همچنین طبقه‌بندی‌کننده‌های یادگیری ماشینی را بر اساس زمان پیش‌بینی، زمان یادگیری و دقت ارزیابی کرد. با این حال، آن است مهم به در نظر بگیرید ‎‏ ... دقت، فراخوانی و امتیاز F1، که درک جامع‌تری از عملکرد طبقه‌بندی‌کننده، به‌ویژه برای مجموعه داده‌های نامتوازن، ارائه می‌دهند. مطالعه ما می‌تواند با گنجاندن معیارهای ارزیابی اضافی برای ارائه ارزیابی جامع‌تر از عملکرد طبقه‌بندی‌کننده، این امر را بهبود بخشد و در نتیجه کیفیت کلی تحقیق را افزایش دهد.

رحمان و ال. [[22]](#_bookmark102) ایجاد شده یک آنلاین مجموعه داده‌ها توسط تولید بسته‌های نرمال و DDoS با استفاده از برنامه hping3 در پایتون. آنها ترافیک DDoS و عادی را به طور جداگانه با استفاده از Tshark ثبت کردند تا از سردرگمی هنگام برچسب‌گذاری مجموعه داده‌ها جلوگیری شود. ترافیک DDoS با سرعت 78 بسته در ثانیه ارسال و به مدت 30 دقیقه ثبت شد، در حالی که ترافیک عادی به مدت 3 ساعت برای متعادل کردن مجموعه داده‌ها ثبت شد. سه مدل یادگیری نظارت شده، یعنی Support SVM، Naive Bayes (NB) و Nearest centroid (NC)، برای طبقه‌بندی ترافیک شبکه بر اساس برنامه‌ها در یک پلتفرم SDN اعمال شدند. این این مطالعه در مورد مجموعه داده‌های مورد استفاده برای آموزش، شفافیت لازم را ندارد. و آزمایش میلی لیتر مدل‌ها، شکست خورده به مشخص کردن آن منبع، ویژگی‌ها و نمایندگی. علاوه بر این، در حالی که از 24 ویژگی سطح بسته برای تشخیص DDoS استفاده می‌کنند، فهرست یا توضیح جامعی از این ویژگی‌ها ارائه نمی‌دهند، که مانع می‌شود ‎‏ ... ارزیابی از آنها اثربخشی. علاوه بر این، ‎‏ ... عملکرد ارزیابی از ‎‏ ... مدل‌ها فاقد عمق است، زیرا فقط معیارهای اساسی را بدون تجزیه و تحلیل مدل گزارش می‌دهد. عملکرد تحت متفاوت شرایط یا مقایسه کردن آن با موجود رویکردها. در نهایت، ‎‏ ... تازگی از این کار است کاهش یافته توسط ‎‏ ... فقدان از جامع آزمایش، بنچمارک یا نوآوری‌های قابل توجه در روش‌شناسی، که در پیشبرد امنیت SDN پیشرفته شکست خورده‌اند.

رایکار و همکاران [[23]](#_bookmark103) طبقه‌بندی دقیق ترافیک در SDN با استفاده از تکنیک‌های یادگیری نظارت‌شده مورد بحث قرار گرفت. این مطالعه محدودیت‌های تکنیک‌های طبقه‌بندی ترافیک سنتی و نیاز به راه‌حل‌های دقیق‌تر و مقیاس‌پذیرتر را برجسته می‌کند. این مقاله فاقد اطلاعات دقیقی در مورد مجموعه داده‌های مورد استفاده برای آموزش و آزمایش مدل‌های یادگیری نظارت‌شده است. بدون جزئیات کافی در مورد مجموعه داده‌ها، از جمله اندازه، تنوع و نمایندگی آن، ارزیابی تعمیم‌پذیری مدل‌های پیشنهادی چالش‌برانگیز است. علاوه بر این، تجزیه و تحلیل معیارهای ارزیابی و مقایسه‌ها با موجود روش‌ها هستند فاقد. بحث در مورد این چالش‌ها ناقص است و از اهمیت عملی مطالعه می‌کاهد. در نهایت، این مطالعه می‌تواند از بهبود یافته‌ها بهره‌مند شود. سازمان و وضوح به افزایش درک و انسجام و بررسی کاربردپذیری مدل در سناریوهای مختلف شبکه.

آشودیه و مکادیه [[24]](#_bookmark104) الگوریتم‌های RF و DT را برای ارائه دقت و نرخ تصمیم‌گیری بهتر در مقایسه با سایر الگوریتم‌های ML برای تشخیص ترافیک مخرب در محیط‌های SDN مورد بحث قرار داد. این مطالعه در مورد استراتژی‌ها یا تکنیک‌های اعتبارسنجی مورد استفاده برای ارزیابی کیفیت، اصالت و نمایندگی مجموعه داده‌ها بحث نمی‌کند. در علاوه بر این، ‎‏ ... مجموعه داده‌ها ممکن است فقدان تنوع در اصطلاحات از توپولوژی‌های شبکه، ترافیک ویژگی‌ها، و حمله سناریوها، به طور بالقوه کاربرد آن را برای ارزیابی جامع عملکرد محدود می‌کند و معیارسنجی از تشخیص الگوریتم‌ها. در مطالعه آنها ، ‎‏ ... نویسندگان شکست خورده به افشا ‎‏ ... منشأ از مجموعه داده‌های به کار رفته، و در نتیجه شفافیت را به خطر می‌اندازد و مانع از توانایی آنها در تکرار و اعتبارسنجی نتایجشان می‌شود. این عدم شفافیت در مورد منشأ مجموعه داده‌ها، سوالات جدی در مورد قابل اعتماد بودن آن ایجاد می‌کند. و مناسب بودن برای ارزیابی دقیق روش‌های تشخیص DDoS.

مطالعاتی، مانند مواردی که در [[25] به آنها اشاره شده است](#_bookmark105) و [[26] که](#_bookmark106) متکی هستند منحصراً روی فردی مجموعه داده‌ها، چنین به عنوان CICDDoS2019

[[25]](#_bookmark105) و سی آی سی داس [[26] ،](#_bookmark106) دویدن ‎‏ ... ریسک از محدود کردن تعمیم پذیری از آنها یافته‌ها توسط منحصراً با استفاده از یک عدد مجموعه داده‌ها، اینها مطالعات ممکن است چشم‌پوشی کردن ‎‏ ... چشم‌انداز وسیع‌تر از امنیت سایبری تهدیدها و شکست به گرفتن ‎‏ ... طیف کامل از دنیای واقعی سناریوها، بالقوه تأثیرگذار کاربردپذیری​ از آنها نتایج. بدون آزمایش چندگانه مجموعه داده‌ها با متغیر ویژگی‌ها، ‎‏ ... استحکام و کاربردپذیری​ ‎‏ ... پیشنهادی سیستم در متفاوت​ زمینه‌ها باقی ماندن نامشخص است. اگرچه سودار و ال. [[27]](#_bookmark107) به دست آمده قابل توجه پیشرفت در حال بهبود حملات انسداد سرویس (DDOS) حمله تشخیص در شبکه امنیت از طریق استفاده از مدل‌های یادگیری ماشین، اتکای آنها به مجموعه داده KDD99 بالا می برد نگرانی‌ها در خصوص ‎‏ ... جامعیت و استحکام از آنها روش‌شناسی. غیبت از معیارسنجی علیه دیگر به طور گسترده به رسمیت شناخته شده مجموعه داده‌ها که معمولاً در سیستم‌های تشخیص نفوذ به کار گرفته می‌شود، مانع از توانایی... رفتار الف مقایسه‌ای تحلیل و ارزیابی کردن ‎‏ ... نقاط قوت نسبی و نقاط ضعف از ‎‏ ... پیشنهادی میلی لیتر مدل‌ها.

در نتیجه، ‎‏ ... نتیجه‌گیری‌ها کشیده شده از این مطالعه ممکن است از نظر اعتبار و کاربردپذیری به خطر بیفتند.

ما مطالعه معرفی می‌کند الف رمان مجموعه داده‌ها به طور خاص طراحی شده برای حملات انسداد سرویس (DDOS) حمله طبقه بندی که است عمومی موجود است

برای اهداف تحقیقاتی. در بخش [چهارم](#_bookmark51) می‌توان توضیحات مفصلی از ویژگی‌های مجموعه داده‌ها و توپولوژی‌های شبکه مورد استفاده در تولید آن را یافت. نوآوری کار ما در ادغام سه ماژول مجزا نهفته است.

* اول ماژول تمرکزها روی خلق کردن الف مجموعه داده‌ها، تضمین جامعیت و ارتباط آن با سناریوهای حمله DDoS در محیط‌های SDN.
* در ماژول دوم، ما از پنج مدل یادگیری ماشین برای طبقه‌بندی حملات DDoS استفاده کردیم. این رویکرد امکان ارزیابی جامع از اثربخشی مجموعه داده‌ها برای آموزش و آزمایش الگوریتم‌های طبقه‌بندی مختلف را فراهم می‌کند.
* ماژول سوم، مجموعه داده‌های ما را با موارد زیر مقایسه می‌کند: سایر مجموعه داده‌های در دسترس عموم، با یک مورد خاص تمرکز بر مقایسه عملکرد آن با مجموعه داده CICDDoS2019 که به طور گسترده استفاده می‌شود. این تحلیل مقایسه‌ای فراهم می‌کند ارزشمند بینش‌ها به ‎‏ ... نقاط قوت و محدودیت‌ها از ما مجموعه داده‌ها و آن پتانسیل سودمندی در کاربردهای دنیای واقعی.

تازگی از این مطالعه می‌تواند باش خلاصه شده به عنوان به شرح زیر است :

* **ایجاد مجموعه داده‌های سفارشی جدید:** یکی از مشارکت‌های اصلی از این مطالعه بود ‎‏ ... توسعه از الف رمان سفارشی مجموعه داده‌ها با استفاده از ‎‏ ... مینی‌نت شبیه‌ساز. با استفاده از این شبیه‌ساز، ما توانستیم محیط‌های شبکه واقع‌گرایانه را شبیه‌سازی کنیم و داده‌هایی تولید کنیم که سناریوهای دنیای واقعی را به دقت منعکس می‌کردند. این مجموعه داده سفارشی با ارائه اطلاعات لازم به محققان، شکاف مهمی را در ادبیات مربوطه پر می‌کند. با الف جدید منبع برای ارزیابی کردن الگوریتم‌ها و روش‌های امنیت شبکه
* **ارزیابی از یادگیری ماشینی الگوریتم‌ها:** ما یک ارزیابی جامع از پنج الگوریتم یادگیری ماشین تحت نظارت انجام دادیم؛ رگرسیون لجستیک، ماشین بردار پشتیبان، جنگل تصادفی، نزدیکترین همسایه K (KNN) و XGBoo در مجموعه داده‌های سفارشی‌مان. از طریق آزمایش‌ها و تحلیل‌های دقیق، عملکرد را ارزیابی کردیم. از اینها الگوریتم‌ها برای تشخیص و طبقه‌بندی نفوذها و ناهنجاری‌های شبکه. یافته‌های ما روشن می‌کند روی ‎‏ ... نقاط قوت و محدودیت‌ها از هر کدام الگوریتم در ‎‏ ... زمینه از ما مجموعه داده‌ها، فراهم کردن ارزشمند بینش‌هایی برای محققان و پژوهشگران.
* **مقایسه با مجموعه داده‌های عمومی:** علاوه بر ارزیابی مجموعه داده‌های سفارشی خود، عملکرد الگوریتم‌های یادگیری ماشین را روی ... مقایسه کردیم. مجموعه داده ما با مجموعه داده CICDDoS2019، یک پایگاه داده عمومی که به طور گسترده استفاده می‌شود مجموعه داده‌ها. این مقایسه‌ای تحلیل مجاز ما برای زمینه‌سازی اثربخشی مجموعه داده‌ها و الگوریتم‌های سفارشی ما نسبت به معیارهای تعیین‌شده. با شناسایی حوزه‌های بهبود و تحقیقات بالقوه جهت‌ها، ما مطالعه مشارکت می‌کند به ‎‏ ... پیشرفت مداوم از شبکه امنیت تحقیق و شیوه‌ها
* **پیامدهایی برای کاربردهای دنیای واقعی:** تحقیقات ما یافته‌ها داشته باشند عملی پیامدها برای کاربردهای امنیت شبکه در دنیای واقعی. با شناسایی مؤثرترین الگوریتم‌های یادگیری ماشین برای تشخیص شبکه نفوذها و ناهنجاری‌ها،

سازمان‌ها می‌توانند دفاع امنیت سایبری خود را افزایش داده و تهدیدات بالقوه را به طور مؤثرتری کاهش دهند. علاوه بر این، در دسترس بودن مجموعه داده‌های سفارشی ما، محققان و متخصصان را قادر ساخت تا مطالعات بیشتری انجام دهند و راه‌حل‌های نوآورانه‌ای متناسب با محیط‌ها و الزامات خاص شبکه توسعه دهند.

به ‎‏ ... بهترین از ما دانش، قبلی مطالعات نداشته اند به طور جامع یکپارچه ویژگی انتخاب، شفافیت مجموعه داده‌ها، و معیارسنجی علیه تأسیس شد مجموعه داده‌ها در الف مجرد مطالعه که تمرکزها روی حملات انسداد سرویس (DDOS) حمله طبقه بندی.

برای پرداختن به این اهداف، ادامه این مقاله به شرح زیر سازماندهی شده است. بخش [دوم](#_bookmark29) تحقیقات مرتبط را بررسی می‌کنیم. در بخش [سوم](#_bookmark37) ، مدل‌های یادگیری ماشینی انتخاب‌شده برای تشخیص تهدید SDN را بررسی می‌کنیم. بخش [چهارم](#_bookmark51) فرآیند ایجاد مجموعه داده‌ها با استفاده از شبیه‌ساز Mininet را شرح می‌دهد. بخش [پنجم](#_bookmark54) چارچوب پیشنهادی برای تشخیص DDoS در SDN را ارائه می‌دهد. با استفاده از دستگاه یادگیری طبقه بندی. جزئیات تنظیمات آزمایش در بخش [VI ارائه شده است](#_bookmark57) ، و پس از آن نتایج و بحث در بخش [VII آمده است](#_bookmark68) . در نهایت، بخش [VIII](#_bookmark79) مقاله را به پایان می‌رساند.

1. **مرتبط کار**

در این بخش، ما بررسی ‎‏ ... موجود ادبیات و تحقیقات مرتبط با مطالعه ما. ما این زمینه را بررسی کردیم، یافته‌های کلیدی را شناسایی کردیم ، و مورد بحث قرار گرفت چگونه قبلی کار می‌کند داشته باشند کمک کرد ما درک از این موضوع. به طور خاص، ما مطالعات تحلیل‌شده روی حملات انسداد سرویس (DDOS) حمله تشخیص و طبقه بندی با استفاده از مدل‌های یادگیری ماشین برای تحلیل ترافیک

ساهو و ال. [[19]](#_bookmark99) پیشنهادی یک تکاملی ماشین بردار پشتیبان مدل برای حملات DDoS حمله تشخیص در SDN ها، تمرکز کردن روی ارتقاء دهنده دقت ، کاهش زمان آموزش، و پرداختن به چالش‌های مطرح‌شده توسط حملات انسداد سرویس (DDOS) حملات در شبکه SDN محیط‌ها. در این در این مطالعه، از تکنیک‌های یادگیری ماشین برای تشخیص حمله DDoS در SDNها استفاده شد . به طور خاص، آن استخدام می‌کند یک ماشین بردار پشتیبان به عنوان ‎‏ ... نخست طبقه بندی کننده برای پیش‌بینی بدخواه ترافیک. ماشین بردار پشتیبان است الف تحت نظارت الگوریتم یادگیری ماشینی که برای وظایف طبقه‌بندی و رگرسیون استفاده می‌شود. علاوه بر این، این مطالعه تحلیل مؤلفه اصلی هسته (KPCA) را با یک الگوریتم ژنتیک (GA) ترکیب کرد تا افزایش ‎‏ ... عملکرد از ‎‏ ... ماشین بردار پشتیبان مدل. KPCA یک تکنیک کاهش ابعاد است، در حالی که GA یک روش فراابتکاری است. بهینه‌سازی الگوریتم الهام گرفته توسط ‎‏ ... فرآیند انتخاب طبیعی. بنابراین، تکنیک‌های یادگیری ماشین مورد استفاده در این مطالعه در درجه اول SVM بودند. طبقه‌بندی و KPCA

با جی ای برای ویژگی استخراج و بهینه‌سازی، به ترتیب. دقت مدل N-KPCA + GA + SVM گزارش شد به باش ۹۸.۹۰۷٪، عملکرد برتر دیگر مدل‌ها چنین به عنوان مدل‌های ترکیبی و مدل‌های منفرد مانند SVM، KNN و Random جنگل طبقه بندی کننده ها با این حال، مجموعه داده‌ها من، که بود

استفاده شده برای ‎‏ ... ارزیابی، است نه عمومی موجود، محدود کردن تکرارپذیری نتایج مطالعه.

جواهر و همکاران [[25]](#_bookmark105) یک سیستم جدید برای تشخیص و کاهش حملات DDoS به صورت بلادرنگ با استفاده از الگوریتم‌های یادگیری ماشین و فناوری بلاکچین پیشنهاد می‌دهیم. هدف این سیستم، ارتقای اقدامات امنیتی فراتر از روش‌های سنتی کاهش حملات DDoS است. سیستم‌ها توسط اعمال نفوذ پیشرفته تکنیک‌ها.

نتایج شبیه‌سازی نشان می‌دهد که مدل شبکه عصبی مصنوعی (ANN) با امتیاز دقت ۹۸.۵۷٪ از سایر الگوریتم‌های یادگیری ماشینی بهتر عمل می‌کند. ادغام فناوری بلاکچین، امنیت و تمرکززدایی را افزایش می‌دهد و شفافیت و تغییرناپذیری را برای حفظ فهرست بلوکی آدرس‌های IP مخرب فراهم می‌کند. علاوه بر این، از ابزار Mininet برای ساخت شبکه‌های مجازی برای آزمایش استفاده شد. یک کنترلر متن‌باز و OpenFlow (POX) مبتنی بر پایتون به همراه Mininet برای مدیریت ترافیک استفاده شد. یک جریان‌سنج CIC برای استخراج اطلاعات ضروری از بسته‌های ورودی به کار گرفته شد و ۸۴ ترافیک شبکه ایجاد کرد. ویژگی‌ها. CICDDoS2019 مجموعه داده‌ها بود استفاده شده تربیت کردن و آزمون ‎‏ ... طبقه بندی میلی لیتر تکنیک‌ها. در به طور کلی، این مطالعه فاقد یک ارزیابی از ‎‏ ... عملکرد از ‎‏ ... سیستم پیشنهادی در دنیای واقعی سناریوها علاوه بر این، ‎‏ ... مطالعه رویکرد پیشنهادی را در مقایسه با سایر روش‌های پیشرفته ارزیابی نمی‌کند، که این امر تعمیم‌پذیری نتایج را محدود می‌کند .

پرز-دیاز و همکاران [[26]](#_bookmark106) یک معماری ماژولار برای تشخیص و کاهش حملات DDoS با نرخ پایین در SDN با استفاده از ... معرفی می‌کند. شش میلی لیتر تکنیک‌ها. اینها مدل‌ها شامل شدن ‎‏ ... جی۴۸، آر تی، نماینده درخت، آر اف، چند لایه پرسپترون (MLP)، و ماشین بردار پشتیبان (SVM). این مطالعه تأکید می‌کند ‎‏ ... توسعه از الف انعطاف‌پذیر و معماری ماژولار که قادر به شناسایی و کاهش خطرات مختلف است حملات انسداد سرویس (DDOS) حمله سناریوها با این حال، الف کلید محدودیت بخش عمده‌ای از این کار، اتکا به یک مجموعه داده واحد، یعنی مجموعه داده DoS موسسه امنیت سایبری کانادا (CIC) است که ممکن است به طور کامل تنوع الگوهای حمله DDoS در دنیای واقعی را نشان نمی‌دهد. غیبت از معیارسنجی علیه دیگر مجموعه داده‌ها، تعمیم‌پذیری نتایج را محدود می‌کند. علاوه بر این، در حالی که پیشنهادی معماری است مدولار، ‎‏ ... مطالعه فاقد عمیق تحلیل از ‎‏ ... پتانسیل سربار معرفی شده توسط اجزای ماژولار، به ویژه در محیط‌های بزرگ و واقعی. مدل‌ها بودند آموزش دیده و ارزیابی شده با استفاده از سی آی سی داس مجموعه داده‌ها، دستیابی به الف تشخیص نرخ از ۹۵٪. معماری است طراحی شده به باش انعطاف‌پذیر و مدولار، اجازه دادن به آسان جایگزینی یا ارتقاء از اجزا بدون تأثیر گذاشتن ‎‏ ... به طور کلی سیستم. معماری است مستقر شده در یک شبیه‌سازی شده محیط زیست به تقلید کردن دنیای واقعی شبکه SDN تنظیمات. آنها از یک کنترلر سیستم عامل شبکه باز (ONOS) که روی یک ماشین مجازی Mininet اجرا می‌شود، برای ایجاد یک محیط آزمایش واقع‌بینانه استفاده کردند. علاوه بر این، اتکا به یک محیط شبیه‌سازی‌شده به این معنی است که عملکرد معماری در شبکه‌های پرترافیک و زنده هنوز آزمایش نشده است.

سودار و همکاران [[27]](#_bookmark107) از طریق شناسایی و کاهش ترافیک مخرب با استفاده از مدل‌های یادگیری ماشین، تشخیص حملات DDoS در امنیت شبکه را به طور قابل توجهی افزایش داده‌اند. این مطالعه تأکید می‌کند ‎‏ ... بحرانی تهدید که حملات DDoS به دلیل ظرفیت آنها در از بین بردن منابع شبکه، SDN ها را تحت تأثیر قرار می‌دهند. در این مطالعه از دو مدل برجسته یادگیری ماشین استفاده شده است: DT که برای طبقه‌بندی و تمایز ترافیک عادی و مخرب استفاده می‌شود و SVM که است شاغل برای ‎‏ ... دقیق طبقه بندی و تشخیص​ حملات انسداد سرویس (DDOS) حملات. پیشنهادی مدل‌ها بودند ارزیابی شده با استفاده از تثبیت‌شده معیارها، چنین به عنوان دقت، به یاد آوردن، دقت، و معیار F. در علاوه بر این، با وجود ‎‏ ... جامد عملکرد معیارها،

یکی از محدودیت‌های اصلی این مطالعه، تکیه انحصاری بر ‎‏ ... کی دی دی ۹۹ مجموعه داده‌ها. این مجموعه داده‌ها است شناخته شده به باش قدیمی هستند و ممکن است پیچیدگی و تنوع الگوهای حمله DDoS فعلی را منعکس نکنند. علاوه بر این، نویسندگان عملکرد مدل‌های خود را با سایر مجموعه داده‌های معیار که معمولاً در سیستم‌های تشخیص نفوذ استفاده می‌شوند، مقایسه نکردند، که محدودیت‌ها ‎‏ ... استحکام از آنها یافته‌ها آدرس‌دهی این شکاف خواهد بود افزایش ‎‏ ... کاربردپذیری از آنها رویکرد در تنظیمات معاصرتر .

صاحبی و همکاران [[28]](#_bookmark108) سیستم‌های تشخیص نفوذ (IDS) پیشنهادی برای بهبود مجازی‌سازی عملکرد شبکه (NFV) با استفاده از الگوریتم‌های یادگیری ماشین. هدف این مطالعه پرداختن به چالش‌های امنیتی نوظهور ناشی از SDN و پیشنهاد ... یک هوشمند راه حل برای شناسایی نفوذها درون این شبکه‌ها. این مطالعه از طیف وسیعی از طبقه‌بندی‌کننده‌های یادگیری ماشین، از جمله DT، RF، LR، Gradient Boosting (GB)، Perceptron (Prc)، Gaussian Naive Bayes (GNB)، Stochastic Gradient Descent (کاهش گرادیان تصادفی) استفاده می‌کند. (دلار سنگاپور)، و خطی اس وی سی (LSVC). اینها الگوریتم‌ها دارند شده اعمال شده به تحلیل کردن شبکه ترافیک داده‌ها و انواع مختلف نفوذ را شناسایی کند . علاوه بر این، ارزیابی راه‌حل پیشنهادی شامل معیارهایی مانند دقت، صحت، فراخوانی و امتیاز F1 بود. عملکرد هر الگوریتم یادگیری ماشین بر اساس توانایی آن در طبقه‌بندی صحیح انواع مختلف ترافیک شبکه، از جمله ترافیک بی‌خطر، ارزیابی شد. و مختلف انواع از حملات، از جمله حملات انسداد سرویس (DDOS) حملات. این مطالعه استفاده می‌کند الف عمومی موجود است SDN گرا مجموعه داده‌ای به نام اس دی ان نفوذ''، که است ارائه شده توسط سایبری پلیس و توزیع شده تحت ‎‏ ... گنو آفرو عمومی عمومی مجوز

۳.۰. این مجموعه داده شامل پنج دسته ترافیک است: DDoS، نفوذ XSS، نفوذ brute-force، تزریق SQL و حملات خوش‌خیم ترافیک. آن متشکل از از ۷۹ ویژگی‌ها و بیش از ۱.۱ میلیون‌ها مشاهده از نفوذ به شبکه و ترافیک لیست سفید. نویسندگان پیش پردازش شده و تحلیل شده این مجموعه داده‌ها برای آموزش و ارزیابی مدل‌های یادگیری ماشینی خود. علاوه بر این، اگرچه از چندین طبقه‌بندی‌کننده یادگیری ماشینی استفاده شد، اما فقدان یک تحلیل مقایسه‌ای نسبی در مقایسه با سایر رویکردهای پیشرفته، قدرت یافته‌های آنها را کاهش می‌دهد.

وانگ و همکاران [[29]](#_bookmark109) به تهدیدات امنیتی فزاینده ناشی از حملات DDoS در SDN رسیدگی کنید و هدف آن توسعه یک راه حل است. که می‌تواند به طور موثر تشخیص و کاهش دادن چنین حملات. این مطالعه اثربخشی مدل SL پیشنهادی را در تشخیص حملات DDoS سیل‌آسا علیه SDN نشان می‌دهد. کنترل کننده. از طریق شبیه‌سازی‌ها و با اندازه‌گیری‌ها روی بسترهای آزمایشی واقعی، نویسندگان تأیید کردند که مدل SL، به ویژه الگوریتم درخت کیسه‌ای، به دقت بالایی دست یافته است. از ۹۹.۶۴٪ در تشخیص حملات انسداد سرویس (DDOS) حملات. علاوه بر این، این مطالعه بر اهمیت انتخاب تکنیک‌ها و پارامترهای مناسب SL برای بهینه‌سازی عملکرد تشخیص تأکید می‌کند. این مطالعه عملکرد روش‌های مختلف را مقایسه کرد. اس ال تکنیک‌ها در اصطلاحات از تشخیص دقت با استفاده از هر دو تجربی و دنیای واقعی شبکه SDN مجموعه داده‌ها، از جمله مجموعه داده‌های DARPA و InSDN. علاوه بر این، یکی از محدودیت‌های کلیدی این مطالعه این است که در درجه اول بر حملات DDoS سیل‌آسا تمرکز دارد، که ممکن است به طور کامل نمایانگر طیف گسترده حملات DDoS نباشد. حمله انواع دیده شده در دنیای واقعی سناریوها علاوه بر این،

‎‏ ... استفاده از ‎‏ ... دارپا و InSDN مجموعه داده‌ها، در حالی که مفید، ممکن است جدیدترین الگوهای حمله به محیط‌های SDN را پوشش ندهد.

یک مطالعه اخیر که توسط گاربا و همکارانش انجام شده است [[30]](#_bookmark110) متمرکز بر اینترنت از چیزها (اینترنت اشیا) درون یک شبکه SDN به آدرس حملات DDoS با طبقه‌بندی الگوریتم‌های یادگیری ماشین، دستگاه‌های اینترنت اشیا را هدف قرار می‌دهند. چارچوب پیشنهادی به‌طور خاص شبکه‌های خانگی هوشمند را که در آن‌ها دستگاه‌های اینترنت اشیا رایج هستند، هدف قرار می‌دهد. این مقاله یک چارچوب تشخیص و کاهش حمله DDoS در زمان واقعی متناسب با شبکه‌های خانگی هوشمند مجهز به SDN ارائه می‌دهد و بر اهمیت ایمن‌سازی دستگاه‌های اینترنت اشیا در چنین محیط‌هایی تأکید دارد. علاوه بر این، تأکید بر استفاده از مدل‌های یادگیری ماشین مانند DT، SVM، LR و KNN است. تمایز قائل شدن بین خوش‌خیم و حمله ترافیک، در عین حال، کنترل‌کننده SDN را با استفاده از یک رویکرد تشخیص مبتنی بر امضا ایمن‌سازی کرد. این مطالعه از چندین مجموعه داده استفاده کرد: مجموعه داده‌های بستر آزمایشی IoT که از سوئیچ‌های OpenFlow گرفته شده بود، که شامل ترافیک معمولی و حمله بود. مجموعه داده‌های UNSW- NB15: گرفتن انواع مختلف حمله، از جمله DDoS، شناسایی و سوءاستفاده. الگوریتم DT به موفقیت دست یافت. الف تشخیص دقت از ۹۹.۵۷٪ با استفاده از ‎‏ ... مجموعه داده‌های گرفته شده از بستر آزمایشی اینترنت اشیا خانه هوشمند. علاوه بر این، هنگام ارزیابی روی مجموعه داده‌های دیگر، مانند CICDDoS2019 و دانشگاه نیوساوت ولز-NB15، ‎‏ ... تصمیم درخت الگوریتم به طور مداوم از الگوریتم‌های دیگر پیشی گرفت و به دقت ۹۹.۹۵٪ دست یافت و ۹۸.۲٪، به ترتیب. با این حال، با وجود ‎‏ ... با وجود دقت بالای حاصل از چارچوب پیشنهادی، این مطالعه فاقد بحث در مورد محدودیت‌های بالقوه است. به عنوان مثال، استفاده از رویکرد تشخیص مبتنی بر امضا ممکن است توانایی آن را محدود کند. به تشخیص جدید یا ناشناخته حملات انسداد سرویس (DDOS) حمله الگوها، به عنوان به امضاهای از پیش تعریف شده متکی است.

محدود استفاده از واقعی اینترنت اشیا ترافیک ویژگی‌ها در مدل‌های تشخیص ساختمان . خضر و همکاران. [[31]](#_bookmark111) اثر دیگری را بر اساس ارائه داد روی شبکه SDN چارچوب برای تشخیص و کاهش دهنده حملات DDoS در شبکه‌های اینترنت اشیا. این چارچوب شامل چهار ماژول است که برای شناسایی و کاهش موثر حملات و در عین حال به حداقل رساندن بار محاسباتی روی گره‌های شبکه اینترنت اشیا طراحی شده‌اند. مدل پیشنهادی از رویکردهای موجود بهتر عمل کرده است. در سراسر مختلف ارزیابی معیارها و به طور موثر به چالش‌های ناشی از حملات DDoS در شبکه‌های اینترنت اشیا پرداخت. مبتنی بر یادگیری ماشینی تشخیص ماژول استخدام می‌کند الگوریتم‌های مختلف یادگیری ماشین، از جمله رگرسیون لجستیک بیزی (BLR)، گاوسی ساده‌لوح بیز (GNB)، ماشین بردار پشتیبان، کی ان ان، دی تی، و آر اف. در میان اینها، ‎‏ ... تصادفی جنگل مدل انجام شده از نظر ارزیابی عملکرد، بهترین عملکرد را داشت. ارزیابی این چارچوب با استفاده از ترافیک واقعی اینترنت اشیا تولید و در Mininet-IoT مستقر شد. سه مورد آزمایشی در نظر گرفته شد: الف تک گره‌ای حمله آزمون مورد، و دو حمله چند گره‌ای آزمون موارد در به طور کلی، یکی از ‎‏ ... محدودیت‌ها از این مطالعه است ‎‏ ... فقدان از تنوع در ‎‏ ... ارزیابی شده آزمون موارد فقط سه مورد آزمایشی در نظر گرفته شد که ممکن است به طور کامل انواع سناریوهای حمله DDoS موجود در شبکه‌های IoT دنیای واقعی را پوشش ندهند.

بایو و همکاران [[32]](#_bookmark112) رویکردی مبتنی بر یادگیری ماشین برای حملات DDoS در یک محیط اینترنت اشیا SDN پیشنهاد دهید. ادغام شبکه SDN با اینترنت اشیا اهداف به بهبود بخشیدن امنیت و دسترسی کنترل

سه مدل، NB، SVM و DT، برای طبقه‌بندی بسته‌های شبکه در کنترل‌کننده SDN ادغام شدند. عملکرد چارچوب پیشنهادی با استفاده از ... ارزیابی شد. متفاوت ترافیک شبیه‌سازی سناریوها پارامترها مانند میزان استفاده از CPU، زمان تشخیص حمله و میزان استفاده از حافظه تحلیل شده به اندازه گیری ‎‏ ... عملکرد از ‎‏ ... چارچوب. گزارش‌های شبکه که توسط کنترل‌کننده SDN ضبط شده‌اند، پیش‌پردازش شده‌اند و تبدیل شده به الف مجموعه داده‌ها برای ‎‏ ... آموزش و آزمایش از ‎‏ ... میلی لیتر مدل‌ها. پیشنهادی چارچوب به سطح بالایی دست یافت دقت نرخ‌ها، با الف دی تی از ۹۸.۱٪، توجه از ۹۷.۴٪، و ماشین بردار پشتیبان از ۹۶.۱٪. اگرچه ‎‏ ... پیشنهادی چارچوب تمرکزها در حال تشخیص سیل انواع از حملات انسداد سرویس (DDOS) حملات، آن دارد ‎‏ ... پتانسیل برای گسترش دادن تحقیق به پوشش دیگر انواع از حملات انسداد سرویس (DDOS) حملات و انواع مختلفی از شبکه‌های اینترنت اشیا را در بر می‌گیرند. با این حال، این مطالعه فاقد ارزیابی دقیقی از میزان تعمیم‌پذیری مدل‌ها است. به متفاوت اینترنت اشیا شبکه‌ها، که می‌توانست تحت تأثیر قرار دادن کاربردپذیری آنها در بیشتر متنوع دنیای واقعی محیط‌ها. کارهای آینده شامل گسترش این تحقیق برای گنجاندن سایر الگوریتم‌های یادگیری تحت نظارت، مانند RF و XGBoost، و بررسی رویکردهای یادگیری بدون نظارت و نیمه نظارت خواهد بود. علاوه بر این، ادغام یک ماژول کاهش حمله DDoS و گسترش چارچوب برای پوشش موارد مختلف انواع از حملات انسداد سرویس (DDOS) حملات و اینترنت اشیا شبکه‌ها است برای بهبود بیشتر پیشنهاد شده است.

آنیانوو و ال. [[33]](#_bookmark113) مورد بحث قرار گرفت ‎‏ ... امنیت چالش‌های سیستم‌های حمل و نقل هوشمند (ITS) در چارچوب SDN این مطالعه به ویژه آدرس‌ها ‎‏ ... آسیب‌پذیری حملات DDoS مبتنی بر SDN به دلیل ساختار متمرکز آنها. راه‌حل پیشنهادی شامل ادغام ابزارهای هوش مصنوعی، به‌ویژه یک بسط جدید از الگوریتم Radial است. اساس عملکرد پشتیبانی بردار ماشین هسته (RBF-SVM)، برای تشخیص حمله DDoS. ارزیابی مدل پیشنهادی راه حل درگیر ‎‏ ... استفاده از عملکرد معیارها برای ارزیابی اثربخشی الگوریتم‌های مختلف. تکنیک‌هایی مانند اعتبارسنجی متقابل جستجوی شبکه‌ای (GSCV) و بهینه‌سازی پارامتر برای افزایش عملکرد ... مورد استفاده قرار گرفته‌اند. ‎‏ ... تشخیص مدل. این مطالعه بحث می‌کند ‎‏ ... استفاده دو مجموعه داده برای ارزیابی: مجموعه داده‌های SDN-DDoS و CICDDoS. اینها مجموعه داده‌ها بودند استفاده شده به اعتبارسنجی ‎‏ ... اثربخشی از پیشنهادی چارچوب تحت مختلف شرایط، شامل شرایط مقیاس‌بندی. مدل پیشنهادی در تشخیص حمله DDoS با دقت 99.40٪ و 99.26٪ به دقت بالایی دست یافت. با این حال، این مطالعه به این موضوع نمی‌پردازد استحکام از ‎‏ ... مدل علیه در حال تکامل حمله استراتژی‌هایی که برای امنیت شبکه در درازمدت بسیار مهم است. تحقیقات آینده می‌تواند استقرار در دنیای واقعی، مقاومت در برابر استراتژی‌های حمله در حال تحول و مقیاس‌پذیری در شبکه‌های بزرگتر را در نظر بگیرد.

تحقیقات محدودی در مورد ادغام یادگیری ماشین با SDN برای دفاع در برابر حملات DDoS در شبکه‌های زنجیره تأمین وجود دارد. سبار و زکیک [[34]](#_bookmark114) با پیشنهاد استفاده از تکنیک‌های یادگیری ماشین برای شناسایی و کاهش حملات DDoS در شبکه‌های زنجیره تأمین مبتنی بر SDN، این شکاف را برطرف کردند. مطالعه آنها نشان داد که ادغام یادگیری ماشین با SDN به طور قابل توجهی افزایش می‌دهد ‎‏ ... اثربخشی از حملات انسداد سرویس (DDOS) تشخیص حمله و کاهش. آنها به دست آمده بالا عملکرد،

با ‎‏ ... تصادفی جنگل مدل دستیابی به دقت، دقت، یادآوری، و امتیاز f1 ارزش‌ها همه تجاوز کردن ۹۸٪. ارزیابی مورد استفاده شبکه ترافیک داده‌ها جمع‌آوری‌شده از مختلف گره‌ها در یک شبکه زنجیره تأمین مبتنی بر SDN، و در نتیجه برجسته کردن عملی بودن و اثربخشی راه‌حل پیشنهادی در سناریوهای دنیای واقعی. علاوه بر این، این مطالعه ارائه نمی‌دهد جزئیات روی ‎‏ ... مقیاس‌پذیری از ‎‏ ... مدل در بزرگتر یا بیشتر پیچیده شبکه SDN محیط‌ها، که می‌توانست محدود کردن کاربرد آن به موارد استفاده گسترده‌تر. پرداختن به این کاستی‌ها خواهد بود افزایش ‎‏ ... استحکام و کاربردی بودن یافته‌های آنها.

**بینش:** جدول [۱](#_bookmark38) خلاصه‌ای از کارهای مرتبط. ما از LR، SVM، RF، KNN و XGBoost برای تشخیص DDoS در SDN استفاده کردیم. ما یک مجموعه داده جدید ایجاد کردیم که سناریوهای حمله را شبیه‌سازی می‌کرد و آن را در برابر مجموعه داده‌های موجود محک زدیم. نکته مهم این است که مجموعه داده ما برای تحقیقات بیشتر در دسترس عموم قرار داشت. نویسندگان [[28]](#_bookmark108) از SVM، GLM، NB، DA، FNN و BT برای تشخیص DDoS استفاده کردند. آنها ادعا کردند که یک مجموعه داده سفارشی ایجاد کرده‌اند اما اطلاعات دقیقی در مورد فرآیند تولید آن ارائه ندادند و مجموعه داده برای آزمایش توسط سایر محققان در دسترس عموم قرار نگرفت. در حالی که هر دو مطالعه، تشخیص DDoS را با استفاده از یادگیری ماشین بررسی می‌کنند. تکنیک‌ها، ما مطالعه استخدام می‌کند الف گسترده‌تر محدوده ای از الگوریتم‌ها و فراهم می‌کند الف عمومی موجود است مجموعه داده‌ها برای محک‌زنی. کار ما با به اشتراک گذاشتن مجموعه داده‌ها با جامعه تحقیقاتی، بر شفافیت و تکرارپذیری تأکید دارد و به این ترتیب سایر محققان را قادر می‌سازد تا یافته‌های ما را اعتبارسنجی کرده و بر اساس آنها کار کنند. در مقابل، مطالعات دیگر فاقد شفافیت در مورد فرآیند ایجاد مجموعه داده‌ها هستند و آن را برای ارزیابی عمومی ارائه نمی‌دهند و این امر قابلیت استفاده و تکرارپذیری آن را محدود می‌کند.

1. **انتخاب شده ماشین یادگیری مدل‌ها برای تشخیص تهدید SDN**

در این بخش، ما معرفی کردن ما روش‌شناسی برای تشخیص

حملات انسداد سرویس (DDOS) حملات در شبکه SDN محیط‌ها توسط با استفاده از تحت نظارت تکنیک‌های یادگیری ماشینی با تأکید ‎‏ ... بحرانی نیاز به تقویت امنیت شبکه در برابر تهدیدات سایبری در حال تحول، رویکرد ما با هدف برای مهار قابلیت‌های یادگیری ماشینی جهت شناسایی موارد غیرعادی شبکه رفتار نشانگر از حملات انسداد سرویس (DDOS) حملات، بنابراین افزایش ‎‏ ... تاب‌آوری از ‎‏ ... شبکه SDN زیرساخت. به ارزیابی کنید عملکرد از ‎‏ ... پیشنهادی حملات انسداد سرویس (DDOS) تشخیص چارچوب، ما استفاده شده الف سفارشی مجموعه داده‌ها حاوی متنوع شبکه سناریوهای ترافیکی، شامل الگوهای عادی و حملات DDoS شبیه‌سازی شده. ما آزمایش‌های گسترده‌ای را با استفاده از پنج ML تحت نظارت انجام دادیم که به دلیل تطبیق‌پذیری، استحکام و ... شناخته شده‌اند. اثربخشی در طبقه بندی. اینجا، ما فراهم کردن توضیحات مفصل از چرا ما انتخاب کرد هر کدام مدل و چگونه آنها در مطالعه ما مورد استفاده قرار گرفتند .

* 1. *لجستیک رگرسیون (LR)*

LR یک الگوریتم طبقه‌بندی محبوب است که در یادگیری ماشین مورد استفاده قرار می‌گیرد. برخلاف خطی رگرسیون، که پیش‌بینی می‌کند مقادیر پیوسته، رگرسیون لجستیک برای وظایف طبقه‌بندی دودویی استفاده می‌شود، کجا ‎‏ ... نتیجه است یا 0 یا ۱. ال آر مدل‌ها احتمال که الف داده شده ورودی تعلق دارد به الف قطعی

**جدول ۱.** مقایسه با دیگر مرتبط کار می‌کند. **ج.:** سفارشی مجموعه داده‌ها، **پ.:** عمومی مجموعه داده‌ها، **.:سی اند پی** این مطالعه استفاده شده الف سفارشی عمومی مجموعه داده‌ها.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | | |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | | | | | | |

کلاس توسط با استفاده از الف لجستیک تابع. آن متناسب است الف منحنی به نقاط داده، که امکان روابط غیرخطی بین ویژگی‌ها را فراهم می‌کند و هدف متغیر. ال آر است به طور گسترده استفاده شده به دلیل به سادگی، قابلیت تفسیر و اثربخشی آن در حوزه‌های مختلف، از جمله امنیت سایبری. مطالعات متعدد امنیت سایبری از رگرسیون لجستیک برای کارهایی مانند تشخیص نفوذ، تجزیه و تحلیل بدافزار و تشخیص حمله DDoS استفاده کرده‌اند. [[35] ،](#_bookmark115) [[36] ،](#_bookmark116) [[37] .](#_bookmark117) لجستیک رگرسیون نمایشنامه‌ها الف نقش حیاتی در راهکارهای امنیتی SDN با کمک به تشخیص و کاهش از مختلف تهدیدها، از جمله حملات انسداد سرویس (DDOS) حملات. توانایی آن در مدل‌سازی احتمال فعالیت مخرب بر اساس شبکه ترافیک ویژگی‌ها باعث می‌شود آن ارزشمند برای شناسایی موارد مشکوک رفتارها و محافظت کردن شبکه SDN زیرساخت از

سایبری تهدیدها معادله برای لجستیک رگرسیون است :

*پ* ( *ی* = ۱ | *ایکس* ) = ۱ */* ۱ + *e* - *(β* 1 *x* 1 + *.....* + *β n x n )* (1)

کجا *پ* ( *ی* = ۱ | *ضربدر* ) نشان دهنده احتمال کلاس مثبت است داده شده ورودی ویژگی‌ها *ایکس* ، *بتا* ۱ است ‎‏ ... رهگیری، *بتا* ۱ *، . . . ، بتا ن*

هستند ‎‏ ... ضرایب، و *ایکس* ۱ *، . . . ، ایکس ن* هستند ‎‏ ... ویژگی ارزش‌ها. از آنجا که رگرسیون لجستیک در امنیت سایبری بسیار مهم است و به طور گسترده استفاده می‌شود، ما آزمایش‌هایی را روی مجموعه داده‌های امنیتی SDN که به طور ویژه طراحی شده بود، انجام دادیم. آزمایش‌های ما نتایج امیدوارکننده‌ای به همراه داشت، با ال آر دستیابی به یک چشمگیر دقت از ۸۴.۳۱ *٪ در تشخیص و طبقه‌بندی تهدیدات امنیتی در محیط‌های SDN. این دقت بالا* ، اثربخشی رگرسیون لجستیک را به عنوان ابزاری قابل اعتماد برای افزایش امنیت SDN برجسته می‌کند.

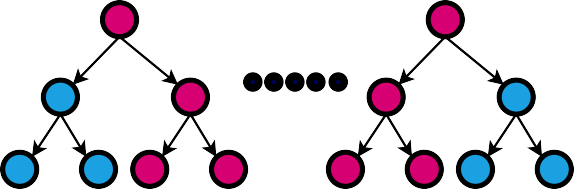
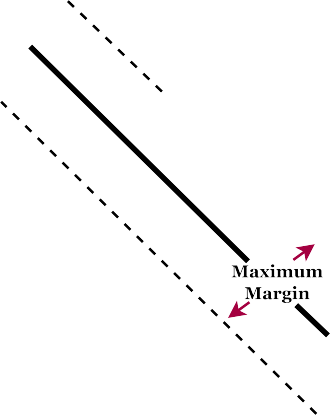
* 1. *پشتیبانی وکتور ماشین آلات (ماشین بردار پشتیبان)*

SVM الگوریتم‌های یادگیری نظارت‌شده‌ای هستند که به طور گسترده برای طبقه‌بندی و رگرسیون استفاده می‌شوند. در طبقه‌بندی، این ماشین بردار پشتیبان (SVM) کشف می‌کند که بهینه ابرصفحه که جدا می‌کند متفاوت کلاس‌هایی با بزرگترین حاشیه در فضای ویژگی، در نتیجه افزایش ‎‏ ... تعمیم توانایی از ‎‏ ... مدل. ماشین بردار پشتیبان (SVM) برای داده‌های با ابعاد بالا مناسب است و در برابر بیش‌برازش مقاوم است. سازی آن مناسب برای پیچیده مجموعه داده‌ها با

مرزهای غیرخطی. اگرچه SVM در درجه اول برای کارهای طبقه‌بندی استفاده می‌شود، اما می‌تواند برای کارهای رگرسیون نیز مورد استفاده قرار گیرد. طبقه بندی، ماشین بردار پشتیبان اهداف به حداکثر کردن ‎‏ ... حاشیه بین کلاس‌ها، که منجر به تعمیم بهتر و مقاومت در برابر نویز در داده‌ها می‌شود [[38] .](#_bookmark118) صفحه تصمیم‌گیری، که به عنوان ... نیز شناخته می‌شود ابرصفحه، توسط بردارهای پشتیبان تعیین می‌شود، که نقاط داده‌ای هستند که به صفحه تصمیم‌گیری نزدیک‌ترند. این ابرصفحه جدا می‌کند ‎‏ ... متفاوت کلاس‌ها در ‎‏ ... ویژگی فضا، همانطور که در شکل [3 نشان داده شده است](#_bookmark44) . هدف اصلی ما استفاده از ابرصفحه بود رویکرد در ما مشکل زیرا آن است مناسب برای طبقه بندی وظایف. علاوه بر این، یک ماشین بردار پشتیبان است ضروری برای SDN امنیت زیرا آن به طور موثر طبقه بندی می کند شبکه ترافیک به داخل عادی و بدخواه فعالیت‌ها. ما آزمایش‌ها با یک مجموعه داده سفارشی که برای امنیت SDN طراحی شده بود، اثربخشی SVM را نشان داد و به دقت 96.52٪ در طبقه‌بندی تهدیدات امنیتی دست یافت. این دقت بالا، قابل اعتماد بودن و عملکرد SVM را در افزایش امنیت SDN برجسته می‌کند. توسط به طور دقیق شناسایی و پاسخ دادن به تهدیدات بالقوه در زمان واقعی.

مدل را روی k-1 لایه بررسی می‌کند و مدل را روی لایه‌های باقی‌مانده ارزیابی می‌کند. این فرآیند k بار تکرار می‌شود و تضمین می‌کند که ‎‏ ... مدل عملکرد تخمین‌ها هستند قابل اعتماد و بیش از حد به انتخاب یک تقسیم آموزش-آزمون واحد حساس نیست. RF به طور گسترده در مطالعات مختلف در مورد تشخیص حمله DDoS [[40] مورد استفاده قرار گرفته است .](#_bookmark120) قابلیت آن در مدیریت مجموعه داده‌های بزرگ و پر سر و صدا داده‌ها دارد فعال شده محققان به به طور موثر تشخیص دهید و طبقه بندی کردن متفاوت انواع از حملات انسداد سرویس (DDOS) حمله کردن. علاوه بر این، توسط اعمال نفوذ آر اف، شبکه SDN کنترل کننده ها می‌تواند به سرعت شناسایی و کاهش حملات DDoS و در نتیجه افزایش امنیت شبکه و قابلیت اطمینان. در ما تحقیق، ما اعمال شده جنگل تصادفی به ما سفارشی مجموعه داده‌ها برای حملات انسداد سرویس (DDOS) حمله تشخیص در محیط‌های SDN. آزمایش‌های ما نشان داد که مدل جنگل تصادفی به بالاترین دقت ۹۸.۹۷٪ دست یافته است، نشان دهنده آن اثربخشی در به طور دقیق شناسایی و طبقه‌بندی حملات DDoS در سناریوهای دنیای واقعی.

**شکل ۴.** تصادفی جنگل



**شکل ۳.** تجسم از بهینه ابرصفحه با حداکثر حاشیه و بردارهای پشتیبان. ابرصفحه به عنوان مرز تصمیم‌گیری عمل می‌کند و حاشیه بین کلاس‌ها را به حداکثر می‌رساند، در حالی که بردارهای پشتیبان (هایلایت شده) امتیاز) تعیین آنها موقعیت، کمک رسانی طبقه بندی موثر

* 1. *تصادفی جنگل (RF)*

جنگل تصادفی یک روش یادگیری گروهی قدرتمند است که از درخت‌های تصمیم‌گیری تشکیل شده است [[39] .](#_bookmark119) هر درخت در جنگل با استفاده از زیرمجموعه‌ای تصادفی از داده‌های آموزشی و ویژگی‌ها ساخته شده است. در طول طبقه‌بندی، هر درخت به طور مستقل کلاس را پیش‌بینی می‌کند، و ‎‏ ... نهایی پیش‌بینی بود مصمم توسط ترکیب آرای همه درخت‌ها. همانطور که در شکل [4 نشان داده شده است](#_bookmark45) ، تصمیم گروهی درختان شامل الف مجموعه از تصمیم درختان، که در آن هر درخت در پیش‌بینی نهایی نقش دارد. این درخت‌ها به طور مستقل آموزش دیده و در طول پیش‌بینی به صورت موازی عمل کردند. برای ارزیابی عملکرد مدل‌های یادگیری ماشین، از اعتبارسنجی متقابل k-fold استفاده کردیم. این تکنیک انشعابات ‎‏ ... مجموعه داده‌ها به ک هم اندازه چین‌ها، قطارها

* 1. *K-نزدیکترین همسایه‌ها (کی ان ان)*

KNN به عنوان یک رویکرد جذاب برای تشخیص حملات DDoS در محیط‌های SDN ظهور کرده است. تحقیق ما با بهره‌گیری از KNN، اثربخشی آن را در تشخیص رفتار غیرعادی شبکه که نشان‌دهنده حملات DDoS است، بررسی کرد. سادگی و شفافیت. بنیادی اصل از KNN، که طبقه بندی می کند موارد مبتنی بر روی ‎‏ ... اکثریت کلاس نزدیکترین همسایگانشان در فضای ویژگی، به طور یکپارچه هم‌تراز می‌شود با ‎‏ ... پویا طبیعت از ‎‏ ... شبکه ترافیک در SDN. KNN در شناسایی و کاهش تهدیدات DDoS بدون نیاز به فرضیات پیچیده در مورد توزیع داده‌ها، قدرت و پایداری نشان می‌دهد [[41] .](#_bookmark121) ایده اساسی الگوریتم KNN برای طبقه‌بندی یا پیش‌بینی برچسب یک نقطه داده جدید بر اساس برچسب‌های نزدیکترین همسایگان آن است. در ‎‏ ... ویژگی فضا [[42] .](#_bookmark122) در دیگر کلمات، کی ان ان K نمونه (نقاط داده) نزدیک به نقطه داده جدید x را از نظر مقادیر ویژگی آنها شناسایی می‌کند. نزدیکترین نمونه‌ها، شناخته شده به عنوان ‎‏ ... نزدیکترین همسایه‌ها، هستند مصمم مبتنی بر روی الف معیار فاصله ، معمولاً ‎‏ ... اقلیدسی فاصله، به عنوان نمایندگی شده توسط​

دنبال کردن معادله :

، u u X *n*  2

*d* (*x, u*) = t*v*−1 *(xi* − *ui)* (2)

*من* = ۱

کجا *د* ( *ایکس ، شما* ) است ‎‏ ... فاصله بین بردارها *ایکس* و *تو* ، و *v* نشان‌دهنده‌ی بُعد یا طول بردارها است، که در آن *n* تعداد بُعدها در هر بردار است. *x i* و *تو من به ترتیب* عناصر متناظر بردارهای *x* و *u هستند* . جمع محاسبه می‌کند ‎‏ ... مربع تفاوت‌ها برای هر کدام بُعد و ‎‏ ... کل بیان است ریشه مربعی برای بدست آوردن اندازه نهایی فاصله

علاوه بر این، قابلیت تفسیر KNN و سهولت پیاده‌سازی KNN، آن را به گزینه‌ای سودمند برای تشخیص حمله DDoS تبدیل می‌کند. فرآیند تصمیم‌گیری شفاف آن، اعتبارسنجی و تفسیر مؤثر تشخیص را امکان‌پذیر می‌سازد. نتایج علاوه بر این، KNN توانایی از کی ان ان مدیریت داده‌های با ابعاد بالا در محیط‌های SDN، آن را برای تحلیل ویژگی‌های شبکه بسیار مناسب می‌کند. این سادگی و تفسیرپذیری ساختن کی ان ان الف ارزشمند دارایی در دفاع از امنیت سایبری، سازمان‌ها را قادر می‌سازد تا به صورت پیشگیرانه شناسایی کنند. و کاهش دادن حملات انسداد سرویس (DDOS) تهدیدها در در زمان واقعی. ما تحقیقات در مورد استفاده از الگوریتم KNN برای تشخیص حمله DDoS نتایج امیدوارکننده‌ای را با دقت 97.60٪ نشان داد. این نشان دهنده پتانسیل KNN برای تمایز قائل شدن بین ... منظم شبکه ترافیک و بدخواه حملات انسداد سرویس (DDOS) حملات. با گنجاندن KNN در چارچوب تشخیص خود و استفاده از تکنیک‌های دقیق انتخاب ویژگی، زمینه را فراهم می‌کنیم برای در حال بهبود ‎‏ ... امنیت و تاب‌آوری از زیرساخت SDN در برابر تهدیدات سایبری در حال تحول

* 1. *اکستریم گرادیان تقویت (ایکس‌جی‌بوست)*

XGBoost یک جزء کلیدی از شیوه‌های فعلی یادگیری ماشین است و به ویژه به دلیل مهارتش در مدیریت ساختاریافته شناخته شده است داده‌ها و تحویل دادن برتر پیش بینی کننده نتایج [[43] .](#_bookmark123) در ما تحقیق، که متمرکز روی شناسایی حملات انسداد سرویس (DDOS) حملات درون تنظیمات SDN، ما از نقاط قوت XGBoost بهره بردیم، مدیون به آن تاب‌آوری و مقیاس پذیری. توسط با استفاده از یک طرح تقویت گرادیان، XGBoost دنباله ای از صدها درخت تصمیم گیری را می سازد و به تدریج پیش بینی ها را اصلاح می کند تا تابع زیان را به حداقل برساند. این فرآیند تکراری نه تنها دقت پیش بینی را افزایش می دهد، بلکه سازگاری مدل را با محیط های شبکه پیچیده و پویا نیز تضمین می کند. بنابراین، اهمیت XGBoost در شبکه SDN امنیت راه حل ها نمی‌تواند باش نادیده گرفته شده. ظرفیت آن به رسیدگی بزرگ مجموعه داده‌ها و مقاومت به بیش‌برازش، آن را به ابزاری ایده‌آل برای تشخیص حملات DDoS در دنیای واقعی تبدیل می‌کند. زمان [[44] .](#_bookmark124) برخلاف روش‌های سنتی، XGBoost یک چارچوب همه‌کاره ارائه می‌دهد که می‌تواند با تهدیدهای جدید سازگار شود و خطرات را به طور مؤثر کاهش دهد. علاوه بر این، قابلیت تفسیر آن اجازه می‌دهد مدیران شبکه برای به دست آوردن بینش‌های ارزشمند به ویژگی‌هایی که فرآیند تشخیص را هدایت می‌کنند، دسترسی پیدا می‌کنند و آنها را قادر می‌سازند تا تصمیمات آگاهانه بگیرند و استراتژی‌های دفاعی پیشگیرانه را پیاده‌سازی کنند. در ما آزمایش، ما ارزیابی شده ‎‏ ... عملکرد​ ایکس‌جی‌باووست توسط با استفاده از الف سفارشی مجموعه داده‌ها. نتایج نشان داد چشمگیر​ ۹۲.۳۶٪ دقت نرخ، نشان دهنده آن اثربخشی در تشخیص ترافیک مخرب از فعالیت‌های مشروع شبکه. در علاوه بر این، ایکس‌جی‌باووست انجام شده خب در سراسر سایر معیارها چنین به عنوان دقت، به یاد آوردن، و امتیاز F1، نشان دادن آن ارزش به عنوان الف کلید جزء از ما حملات انسداد سرویس (DDOS) تشخیص

این عملکرد قوی، اهمیت XGBoost در امنیت SDN و پتانسیل آن برای تقویت زیرساخت شبکه در برابر تهدیدات سایبری نوظهور را برجسته می‌کند.

* 1. *تنظیم فراپارامتر*

در این مطالعه، مرحله پیش‌پردازش داده‌ها با دقت طراحی شد تا اطمینان حاصل شود که الگوریتم‌های یادگیری ماشین می‌توانند به طور بهینه عمل کنند. روی ‎‏ ... مجموعه داده‌ها، در حالی که اجتناب کردن هر پتانسیل بایاس‌ها. مراحل پیش‌پردازش پس از مرحله تقسیم‌بندی داده‌ها، به‌طور مستقل بر روی مجموعه داده‌های آموزشی و آزمایشی اعمال شدند تا اطمینان حاصل شود که تقسیم‌بندی آزمایشی در طول مدل دیده نمی‌شود. آموزش فرآیند. دنبال کردن مراحل بودند انجام شده:

* + - **جابجایی از مفقود ارزش‌ها:** مفقود یا تهی ارزش‌ها در​ مجموعه داده‌ها بودند رسیدگی شده توسط یا برداشتن یا جایگذاری آنها. این مرحله تضمین می‌کرد که مجموعه داده‌ها کامل و عاری از ناسازگاری‌هایی باشد که می‌توانند فرآیند یادگیری را مختل کنند. استراتژی جایگذاری به طور جداگانه برای مجموعه‌های آموزشی و آزمایشی اعمال شد تا از نشت داده‌ها جلوگیری شود.
    - **کدگذاری مقادیر دسته‌بندی‌شده:** متغیرهای دسته‌بندی‌شده، مانند Source\_IP و Destination\_IP، به صورت کدگذاری‌شده در آمدند. عددی فرمت‌ها به باش پردازش شده با استفاده از ام ال رویکرد. ما استفاده شده آدمک متغیر کدگذاری برای تبدیل این ویژگی‌های دسته‌بندی‌شده به مجموعه‌ای از متغیرهای دودویی. این تبدیل، مجموعه داده‌ها را گسترش داد و فعال شده ‎‏ ... الگوریتم‌ها به رسیدگی داده‌های دسته‌بندی‌شده به طور موثر. قابل توجه، این کدگذاری بود به طور مستقل انجام شد برای ‎‏ ... آموزش و آزمون مجموعه داده‌ها به اطمینان حاصل شود که هیچ اطلاعاتی از مجموعه تست در طول فرآیند آموزش فاش نشده است.
    - **نرمال‌سازی:** به اطمینان حاصل کردن که ویژگی‌ها با بزرگ محدوده‌های مقادیر انجام داد نه به طور نامتناسب نفوذ ‎‏ ... فرآیند یادگیری، نرمال‌سازی انجام شد . همه ویژگی‌ها مقیاس بندی شده پایین به الف رایج محدوده، معمولاً بین ۰ و ۱. این عادی سازی گام جلوگیری می‌کند ویژگی‌ها با مقیاس‌های بزرگتر از تسلط بر فرآیند یادگیری جلوگیری می‌کند و تضمین می‌کند که همه ویژگی‌ها به طور مساوی در تصمیم‌گیری مدل نقش دارند. مانند مراحل قبلی، نرمال‌سازی بود انجام شده جداگانه برای ‎‏ ... مجموعه داده‌های آموزشی و آزمایشی.
    - **گسترش از مجموعه داده‌ها:** بعد از پیش‌پردازش، ‎‏ ... مجموعه داده‌ها گسترش‌یافته است از ۱۶ به ۵۷ ستون‌ها مدیون به ‎‏ ... افزودن متغیرهای ساختگی برای ویژگی‌های دسته‌بندی‌شده. این گسترش، ابعاد مجموعه داده‌ها را افزایش می‌دهد و به روش‌های یادگیری ماشین اجازه می‌دهد تا روابط پیچیده‌تری بین ویژگی‌ها را ثبت کرده و عملکرد طبقه‌بندی را بهبود بخشند.

پس از آن، این پیش‌پردازش گام است ضروری به اطمینان حاصل کردن که الگوریتم‌ها کار به طور موثر روی ‎‏ ... مجموعه داده‌ها بدون با اعمال این مراحل پیش‌پردازش پس از تقسیم مجموعه داده‌ها به مجموعه‌های آموزشی و آزمایشی، خطر ایجاد یک بایاس مثبت را کاهش دادیم و اطمینان حاصل کردیم که ارزیابی مدل‌ها منصفانه و بی‌طرفانه است.

علاوه بر ارزیابی عملکرد چارچوب‌های یادگیری ماشین با استفاده از اعتبارسنجی متقابل k-fold، تنظیم فراپارامتری بود همچنین انجام شده به بهینه سازی ‎‏ ... عملکرد هر الگوریتم. تنظیم فراپارامتر با استفاده از جستجوی شبکه‌ای همراه با اعتبارسنجی متقابل k-fold انجام شد. این روش مجاز ما به کاوش کردن متفاوت ترکیبی از فراپارامترها و انتخاب بهترین پیکربندی‌ها بر اساس میانگین عملکرد در سراسر چین‌ها

* 1. *روش پیشنهادی*

پیشنهادی روش پیشنهادات متمایز بهبودها بیش از موجود میلی لیتر تکنیک‌ها توسط تمرکز کردن روی چندین بحرانی مناطق.

* + - **عملکرد مدل بهبود یافته از طریق نمایش داده‌ها:** روش‌های انتخاب‌شده‌ی یادگیری ماشین، مانند RF و XGBoost، به دلیل ...، عملکرد برتر را نشان می‌دهند. توانایی به به طور موثر اهرم ‎‏ ... انتخاب شده ویژگی‌ها. تأکید بر مهندسی ویژگی‌های قوی و استفاده از مدل‌هایی که الگوهای پیچیده را در داده‌ها مدیریت می‌کنند، به دستیابی به دقت بالاتر (۹۸.۹۷٪) کمک می‌کند. و FAR پایین‌تری در مقایسه با تکنیک‌های موجود، که اغلب رنج کشیدن از محدود سازگاری به محیط‌های شبکه پویا
    - **مدیریت بهینه داده‌های نامتوازن:** برخلاف روش‌های قبلی مطالعات، ‎‏ ... پیشنهادی روش استخدام می‌کند مدل‌هایی که به‌طور خاص به دلیل استحکامشان در مدیریت مجموعه داده‌های نامتوازن انتخاب شده‌اند. RF به دلیل توانایی‌اش در مدیریت ... شناخته شده است. داده‌ها عدم تعادل‌ها بدون بیش‌برازش، پیشرو برای بهتر شدن دقت و به یاد بیاورید نرخ ها. این رویکرد تضمین می‌کند بیشتر متعادل و قابل اعتماد تشخیص، که دارد یک چالش رایج در تحقیقات قبلی بوده است که به تکنیک‌هایی متکی است که توانایی کمتری در برخورد با عدم تعادل داده‌ها دارند.
    - **انتخاب ویژگی هدفمند:** استفاده از الگوریتم کای-اسکوئر (Chi2) برای انتخاب ویژگی، تضمین می‌کند که مدل بر روی مرتبط‌ترین داده‌ها تمرکز می‌کند و در نتیجه دقت و کارایی را بهبود می‌بخشد. این فرآیند بهینه سازی می کند ‎‏ ... عملکرد از ‎‏ ... با تمرکز بر ویژگی‌های کلیدی، مدلی را ارائه می‌دهد که به محدودیتی در مطالعات قبلی که انتخاب ویژگی هدفمند را در اولویت قرار نمی‌دادند و منجر به عملکرد غیربهینه می‌شد، می‌پردازد.
    - **جامع ارزیابی با استفاده از چندگانه معیارها:** برخلاف مطالعات قبلی که اغلب ارزیابی‌های خود را به مجموعه‌ای محدود از معیارها محدود می‌کردند، روش پیشنهادی شامل موارد زیر است: الف گسترده ارزیابی در سراسر چندگانه شاخص‌های عملکرد ، مانند دقت، صحت، فراخوانی و امتیاز F1. این تضمین می‌کند الف بیشتر کامل ارزیابی از قابلیت‌ها و استحکام مدل، به ویژه در دنیای واقعی سناریوها، کجا چندگانه معیارها هستند حیاتی برای عملکرد اعتبارسنجی. جامع نتایج در جدول [7](#_bookmark78) خلاصه شده است. عملکرد برتر روش پیشنهادی را در این معیارها برجسته کنید.

1. **مجموعه داده‌ها آفرینش استفاده کردن مینی‌نت شبیه‌ساز**

در این بخش، مراحلی را که برای ایجاد یک سفارشی مجموعه داده‌ها توسط با استفاده از ‎‏ ... مینی‌نت شبیه ساز به گرفتن دینامیک پیچیده یک محیط SDN. مجموعه داده حاصل متشکل از ۱,۰۴۸,۵۷۵ ردیف‌ها و ۲۱ ستون‌ها، که منعکس کننده طیف متنوعی از رفتارها، پیکربندی‌ها و ویژگی‌های عملکردی شبکه است. معماری شبکه مورد استفاده برای جمع‌آوری داده‌ها شامل ۱۲ سوئیچ است که توسط Ryu مدیریت می‌شوند. کنترل کننده، تسهیل‌گری اتصال برای ۲۴ دستگاه‌های به هم پیوسته . مراحل درگیر در مجموعه داده‌ها آفرینش هستند در زیر فهرست شده است .

* **توپولوژی طراحی:**  اول گام درگیر طراحی توپولوژی شبکه‌ای که ویژگی‌های مورد نظر را در بر می‌گیرد و پیچیدگی‌ها از شبکه SDN محیط‌ها. ما ساخته شده الف توپولوژی شامل ۱۲ سوئیچ‌ها و ۲۴ میزبان‌ها به هم پیوسته در الف شیوه مساعد به الگوهای ترافیکی و رفتارهای شبکه متنوع ، همانطور که در شکل نشان داده شده است [۵](#_bookmark53) . شکل [۵(الف)](#_bookmark53) نشان می‌دهد ‎‏ ... اول توپولوژی سناریو، در که ‎‏ ... شبکه توپولوژی شامل می‌شود مختلف میزبان‌هایی که توسط سوئیچ‌ها به هم متصل شده‌اند. PC5، PC8 و PC17 به عنوان میزبان‌های مهاجم شناسایی شدند که به طور جمعی حمله‌ای را علیه PC12، میزبان هدف، آغاز کردند. این توپولوژی مرحله اولیه سناریوی حمله را نشان می‌دهد و تعاملات بین مهاجم و هدف را برجسته می‌کند. میزبان‌ها درون ‎‏ ... شبکه محیط زیست. شکل [5(ب)](#_bookmark53) سناریوی توپولوژی دوم را نشان می‌دهد، که در آن یک سناریوی توپولوژی شبکه متفاوت به تصویر کشیده شده است، که در آن PC15 و PC22 به عنوان میزبان‌های مهاجم شناسایی شده‌اند. این میزبان‌ها حمله‌ای را علیه PC20، میزبان هدف، انجام می‌دهند. این یک سناریوی جایگزین را به تصویر می‌کشد که در آن میزبان‌های مختلف میزبان‌ها هستند درگیر در یک حمله علیه الف هدف متمایز در زیرساخت شبکه.
* **راه‌اندازی Mininet:** با تعریف توپولوژی، به راه‌اندازی محیط شبیه‌ساز Mininet پرداختیم. با بهره‌گیری از انعطاف‌پذیری و مقیاس‌پذیری ارائه شده توسط Mininet، عناصر شبکه مجازی، از جمله موارد زیر را نمونه‌سازی کردیم. سوئیچ‌ها، میزبان‌ها، پیوندها، و کنترل کننده ها، به سناریوهای شبکه دنیای واقعی را شبیه‌سازی کنید.
* **یکپارچه‌سازی کنترلر ریو:** یکپارچه‌سازی کنترلر ریو، کنترل و هماهنگی متمرکز را تسهیل می‌کند. از شبکه عملیات در ‎‏ ... مینی‌نت محیط. با استقرار Ryu، ما کنترل دقیقی بر روی شبکه رفتار، اجرا شده شبکه SDN سیاست‌ها، و داده‌های بلادرنگ را برای تجزیه و تحلیل‌های بعدی جمع‌آوری کرد.
* **تولید ترافیک:** تولید جریان‌های ترافیکی متنوع در یک شبکه برای ثبت طیف گسترده‌ای از رفتارهای شبکه و معیارهای عملکرد، امری محوری است. ما شبیه‌سازی شده مختلف ترافیک الگوها، از جمله ترافیک عادی و غیرعادی، برای شبیه‌سازی حجم کار در دنیای واقعی و سناریوها ام‌جن ابزار تولید شده مختلف انواع ترافیک، شامل TCP، UDP و ICMP، با نرخ‌های کنترل‌شده برای شبیه‌سازی ترافیک شبکه قانونی. برای ترافیک حمله DDoS، از hping3 برای شبیه‌سازی SYN استفاده شد. سیل، بی سیم سیل، و آی‌سی‌ام‌پی سیل‌ها حمله ترافیک

با شدت‌های مختلف، از متوسط (۱۰۰ بسته در ثانیه) تا زیاد (۱۰۰۰ بسته در ثانیه) تولید شد، برای نمایش سطوح مختلف حملات DDoS. این تنوع تضمین می‌کند که مجموعه داده‌ها مراحل و شدت‌های مختلف حملات را در بر می‌گیرد.

* + **نمای کلی ویژگی‌ها:** از ۲۶ ویژگی اولیه استخراج شده از شبکه جریان‌ها، ما اعمال شده ‎‏ ... الگوریتم انتخاب ویژگی کای-اسکوئر (Chi2). این روش، ویژگی‌هایی را که بیشترین ارتباط را با تشخیص DDoS دارند، بر اساس ... اولویت‌بندی کرد. آنها آماری اهمیت. همانطور که الف نتیجه، ما ۱۶ ویژگی ضروری، مانند مدت زمان جریان، تعداد بسته به ازای هر جریان (PPF)، تعداد بایت به ازای هر جریان (BPF) و نرخ بسته را حفظ کرد که برای آموزش و ارزیابی مدل‌های یادگیری نظارت‌شده استفاده شدند.
  + **جمع‌آوری داده‌ها:** سازوکارهای جمع‌آوری داده‌های بلادرنگ مستقر شده به گرفتن مربوط شبکه پارامترها، معیارهای عملکرد و آمار جریان هر 30 ثانیه.
  + **ذخیره‌سازی و ساختاردهی داده‌ها:** داده‌های جمع‌آوری‌شده در قالبی ساختاریافته و مناسب برای استفاده‌های بعدی ذخیره شدند . تحلیل و پردازش. ما ساختار یافته ‎‏ ... مجموعه داده‌ها در ۱,۰۴۸,۵۷۵ ردیف و ۲۱ ستون، که هر ردیف نشان‌دهنده یک مشاهده شبکه متمایز است و هر ستون ویژگی‌های خاص شبکه را در بر می‌گیرد. مجموعه داده‌ها در یک فایل با مقادیر جدا شده با کاما (CVS) با نام ''SDN-DDoS\_Traffic\_Dataset.cvs'' ذخیره شد.
  + **داده‌ها پیش‌پردازش:** پیش‌پردازش مراحل بودند برای تمیز کردن، نرمال‌سازی و تبدیل داده‌های خام به فرمت قابل استفاده اعمال می‌شود.
  1. *ویژگی نمای کلی: درک این ترکیب مجموعه داده‌ها*

در این بخش، ما فراهم کردن الف جامع نمای کلی از ویژگی‌های کلیدی جمع‌آوری‌شده در مجموعه داده‌های ما برای آزمایش ترافیک DDoS طبقه بندی با استفاده از ام ال. هر کدام ویژگی کپسوله می‌کند

به نمایندگی الف جدید جریان.

*ف* = *طول* ( *فلو تیبل* ) (3)

علاوه بر این، ‎‏ ... بالا بیان محاسبه می‌کند ‎‏ ... طول یا اندازه جدول جریان، که نشان دهنده تعداد کل جریان‌های فعال ذخیره شده در جدول است. که در آن، طول ( *flowtable* ) نشان دهنده تابعی است که تعداد ورودی‌ها یا ردیف‌های جدول جریان را برمی‌گرداند.

* **بسته در هر جریان (PPF)** نشان دهنده میانگین تعداد از بسته‌ها در ‎‏ ... شبکه ارتباط جریان. این است محاسبه شده توسط تقسیم کردن ‎‏ ... مجموع شماره از بسته‌های موجود در یک جریان بر اساس تعداد کل جریان‌ها، همانطور که در زیر بیان شده است.

*پی پی اف* = تعداد *بسته / جریان (* 4)

این ویژگی، بینشی در مورد تراکم معمول بسته‌ها در جریان‌های ارتباطی منفرد ارائه می‌دهد. در این زمینه از حملات انسداد سرویس (DDOS) حمله طبقه بندی، ناهنجاری‌ها در مقادیر *PPF* می‌توانند فعالیت‌های مخرب بالقوه را نشان دهند. به عنوان مثال، افزایش یا کاهش ناگهانی *PPF* در مقایسه با حالت پایه عادی می‌تواند نشان‌دهنده وجود یک حمله DDoS باشد. حمله کردن. مهاجمان اغلب تولید کردن غیرطبیعی نرخ بسته‌ها را به گونه‌ای تنظیم می‌کند که سیستم یا شبکه هدف را تحت الشعاع قرار دهد، و نظارت بر PPF به تشخیص چنین ناهنجاری‌هایی کمک می‌کند.

* **بایت پر جریان (بی‌پی‌اف):** به طور غیرمعمول بالا بی پی اف ارزش‌ها ممکن است نشان‌دهنده رفتار غیرعادی، مانند انتقال داده‌های بزرگ مرتبط با حملات DDoS یا سایر فعالیت‌های مخرب باشد. بنابراین، BPF می‌تواند به عنوان شاخصی برای تشخیص غیرعادی ترافیک الگوها بی پی اف نشان دهنده میانگین شماره از بایت منتقل شده به ازای هر جریان در شبکه ترافیک مجموعه داده‌ها. این بود محاسبه شده توسط تقسیم تعداد کل بایت‌های منتقل شده در تمام جریان‌ها بر تعداد کل جریان‌ها. از نظر ریاضی، BPF به صورت زیر نمایش داده می‌شود.

پ *ن ب سی آی آی*

ضروری اطلاعات درباره شبکه ترافیک، محدوده‌بندی از پایه شناسه‌ها، چنین به عنوان سوئیچ‌ها و میزبان‌ها، به بیشتر

*ل* = ۱

جریان‌ها

(5)

معیارهای پیچیده، مانند نرخ بسته‌ها و انتقال داده نرخ‌ها. این بخش به عنوان پایه‌ای برای درک ترکیب مجموعه داده‌ها و معیارهای مورد استفاده برای تجزیه و تحلیل بعدی عمل می‌کند. و طبقه بندی وظایف. دنبال کردن فهرست ویژگی‌های این ویژگی‌ها را ارائه می‌دهد:

* **جریان (F):** جریان در شبکه، مجموعه‌ای از بسته‌ها است که بین یک آدرس IP منبع و مقصد خاص، معمولاً در یک بازه زمانی خاص، با استفاده از پروتکل‌ها و شماره پورت‌های مشترک ارسال می‌شود. دستگاه‌های شبکه مانند روترها و سوئیچ‌ها، جداول جریان را برای ذخیره اطلاعات مربوط به جریان‌های فعال عبوری از دستگاه نگهداری می‌کنند. جداول جریان شامل اطلاعاتی مانند آدرس‌های IP منبع و مقصد، پروتکل‌ها،

جایی که bc *i* تعداد بایت‌های منتقل شده در جریان *i* ام است. و جریان‌ها است ‎‏ ... مجموع شماره از جریان‌ها در ‎‏ ... مجموعه داده‌ها. مقدار BPF بالاتر نشان می‌دهد که به طور متوسط، مقادیر بزرگتری از داده‌ها هستند منتقل شده در هر کدام جریان، در حالی که پایین‌تر​ ارزش پیشنهاد می‌کند کوچکتر داده‌ها انتقال اندازه‌ها به ازای هر جریان.

* **بسته نرخ (روابط عمومی):** روابط عمومی است یک مهم ویژگی برای طبقه‌بندی حمله زیرا آن می‌تواند نشان دادن غیرطبیعی رفتار در ترافیک شبکه. به عنوان مثال، حملات DDoS اغلب شامل نرخ بسته‌بندی بسیار بالاتری نسبت به حالت عادی هستند. ترافیک. توسط نظارت ‎‏ ... بسته نرخ، ناهنجاری‌ها در رفتار شبکه قابل تشخیص هستند و این امکان را فراهم می‌کنند

‎‏ ... شناسایی و کاهش از پتانسیل حملات. نرخ بسته به صورت زیر محاسبه شد :

شماره پورت‌ها، تعداد بسته‌ها و بایت‌ها و مهرهای زمانی. بسته‌ها سفر از طریق الف شبکه دستگاه، ‎‏ ... جریان

***روابط عمومی*** = *∆ پ*

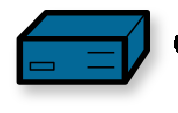
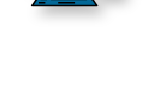
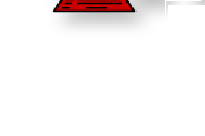
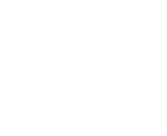
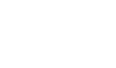
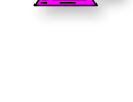
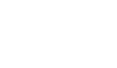
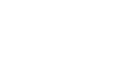
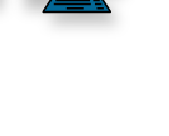
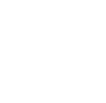
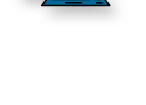
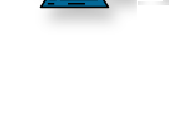
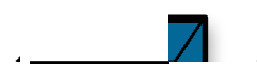
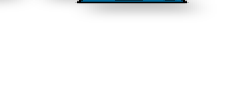
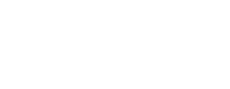
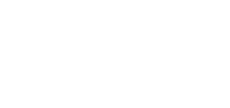
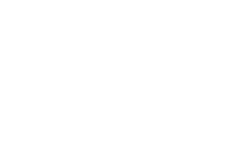
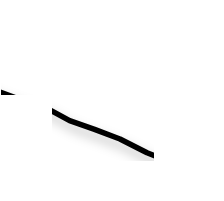
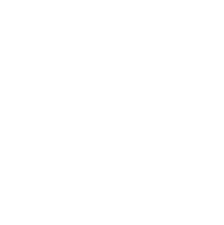
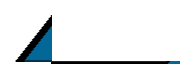
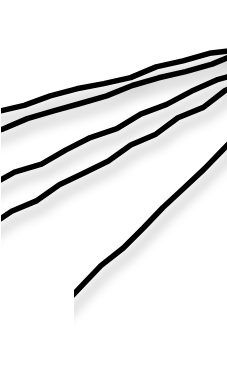
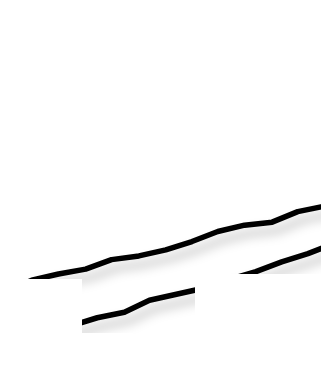
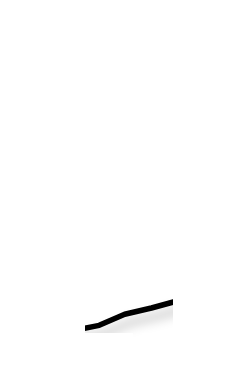
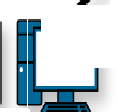
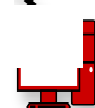
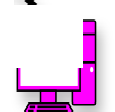
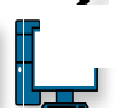
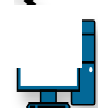
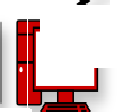
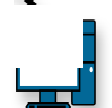
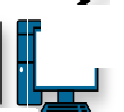
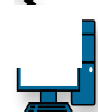
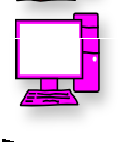
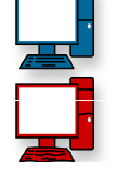
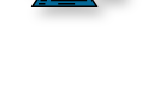
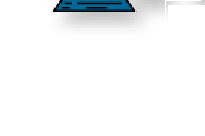
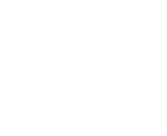
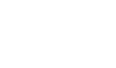
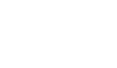
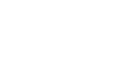
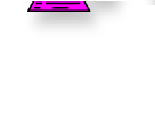
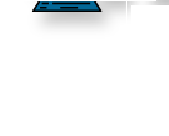
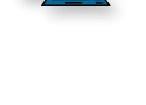
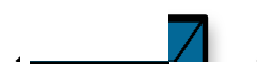
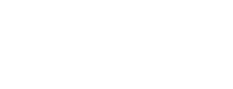
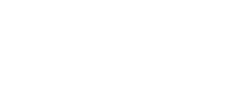
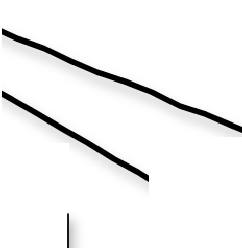
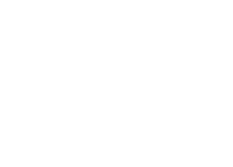
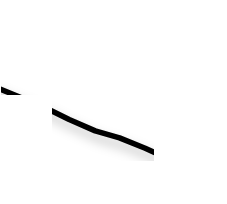
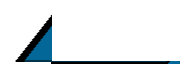
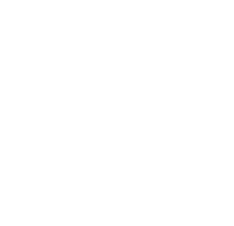
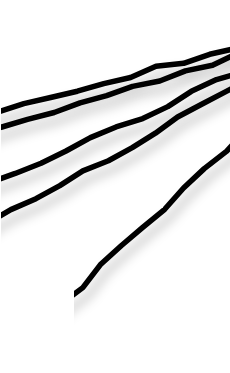
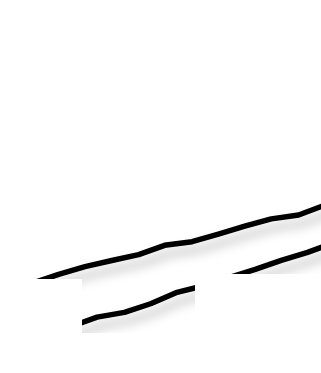
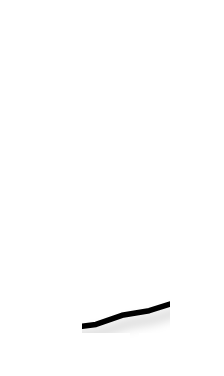
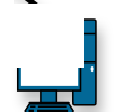
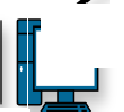
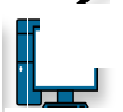
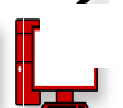
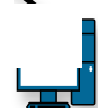
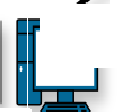
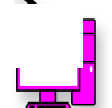
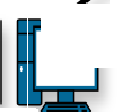
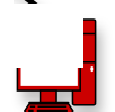
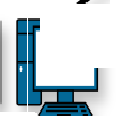
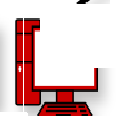
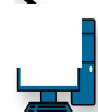
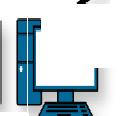
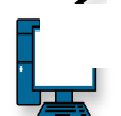
*∆ تی*

(6)

جدول با استفاده از ورودی‌ها و آمارهای جدید به‌روزرسانی می‌شود. اگر یک بسته جدید با ورودی جریان موجود مطابقت داشته باشد، آمارهای مربوطه هستند به‌روزرسانی شد. در غیر این صورت، الف جدید ورود است ایجاد شده

که در آن *∆p* نشان دهنده تغییر در تعداد بسته‌ها در یک بازه زمانی و *∆t است .* نشان دهنده زمان سپری شده در طول

که ‎‏ ... تغییر در بسته بشمار رخ می‌دهد. فرض کنید که



**شکل ۵.** توپولوژی‌های شبکه مورد استفاده برای تولید مجموعه داده‌ها. (الف): مهاجمان PC 5، PC 8 و PC 17، PC 12 را هدف قرار می‌دهند. (ب): مهاجمان PC 15 و PC 22 هدف کامپیوتر ۲۰. (یا: ۲۰)

جریان شبکه ۱۰۰۰ بسته را در ۱۰ ثانیه منتقل می‌کند. نرخ بسته ۱۰۰ بسته در ثانیه (PPS) بود.

* + **پروتکل:** این ویژگی اطلاعات ارزشمندی را برای درک الگوهای ترافیک شبکه، شناسایی تهدیدات امنیتی بالقوه و توسعه استراتژی‌های دفاعی مؤثر در برابر حملات ارائه می‌دهد. این تحلیل به ... کمک می‌کند. به الف جامع طبقه بندی و تشخیص حملات مبتنی بر شبکه. به عنوان مثال، افزایش استفاده از ترافیک ICMP (پروتکل کنترل پیام اینترنت)، که است اغلب مرتبط با شبکه اسکن، می‌تواند نشان‌دهنده یک حمله DDoS در حال انجام باشد.
  + **تأخیر:** الف تأخیر است ‎‏ ... زمان گرفته شده برای الف داده‌ها بسته به رسیدن آن مقصد، و شامل می‌شود عوامل چنین مانند تأخیر در انتشار، انتقال، صف‌بندی و پردازش. این است الف حیاتی عامل برای شناسایی فعالیت‌های مخرب در شبکه ارتباطات. برای مثال، در یک حمله DDoS حمله، بیش از حد ترافیک سیل ‎‏ ... شبکه،

خاص اهداف. علاوه بر این، غیرمنتظره بندر کاربرد می‌تواند نشان دهد بالقوه بدخواه فعالیت. برای مثال، اگر یک بندر معمولاً مرتبط با یکی پروتکل است ناگهان برای نوع دیگری از ترافیک استفاده شود، ممکن است نشان دهنده یک تلاش باشد به طفره رفتن تشخیص یا به سوءاستفاده الف آسیب پذیری.

* **مدت زمان کل ارتباط (TDC):** این ویژگی است مهم برای حمله طبقه بندی زیرا بینشی از رفتار ترافیک شبکه ارائه می‌دهد. به عنوان مثال، یک حمله DDoS ممکن است شامل سیلی از بسته‌ها باشد که یک سرویس یا سرور خاص را هدف قرار می‌دهند و منجر به مدت زمان ارتباط غیرمعمول طولانی یا کوتاه می‌شوند. علاوه بر این، برای شناسایی حملات با استفاده از مدت زمان ویژگی، یکی معمولاً به نظر می‌رسد برای انحرافات از رفتار عادی. برای محاسبه کل جریان TDC بر حسب میکروثانیه، ما یکپارچه ‎‏ ... مدت زمان از ‎‏ ... جریان

در ثانیه ( *د* ) به همراه مدت زمان آن بر حسب میکروثانیه ( *dµ s )* با استفاده از معادله زیر :

باعث ازدحام و افزایش یافته تأخیر در مشروع

۶

ترافیک. نظارت بر معیارهای تأخیر، تشخیص موارد زیر را امکان‌پذیر می‌سازد: غیرطبیعی الگوها و کمک شناسایی و کاهش دادن

*تی دی سی* =

*د* ∗ ۱۰

+ *د میکرو ثانیه*

(7)

حملات انسداد سرویس (DDOS) حملات.

* + **شماره پورت (PNO):** پورت یک نقطه پایانی ارتباطی است که با استفاده از یک مقدار عددی مشخص می‌شود. پورت‌ها اجازه می‌دهند متفاوت کاربردها و خدمات به اشتراک گذاری الف یک اتصال فیزیکی یا مجازی واحد در یک شبکه. PNO در محدوده از 0 به ۶۵۵۳۵، با قطعی محدوده‌ها رزرو شده برای

فرض کنید ما داشته باشند الف ارتباط جریان با مدت زمان ۳ ثانیه و ۵۰۰ میکروثانیه. با استفاده از معادله فوق، کل مدت زمان جریان ارتباط ۳۰۰۰ و ۵۰۰ میکروثانیه است.

* **سوئیچ:**  سوئیچ ویژگی خدمت می‌کند به عنوان الف شبکه مجرایی برای مسیریابی ترافیک و کمک به شناسایی منابع حمله.

الگوهای ترافیک از دستگاه‌های آلوده که به یک سوئیچ متصل هستند، ممکن است ویژگی‌های مشابهی را نشان دهند. الگوهای ترافیک غیرعادی که به طور مداوم از یک سوئیچ خاص ساطع می‌شوند، ممکن است نشان‌دهنده یک حمله هماهنگ باشند.

* + **میزبان:** ویژگی میزبان، میزبان مبدأ یا مقصد درگیر در ارتباط را شناسایی می‌کند. در این مورد در صورت وقوع حمله، شناسایی میزبان آسیب‌دیده می‌تواند به جداسازی و کاهش حملات کمک کند. به عنوان مثال، اگر ترافیک یک میزبان خاص به طور ناگهانی به طور غیرعادی افزایش یابد یا رفتار مشکوکی مانند اسکن چندین پورت از خود نشان دهد، می‌تواند نشان‌دهنده یک حمله بالقوه باشد.
  + **پروتکل اینترنت مبدا (SIP) و اینترنت مقصد پروتکل (دی آی پی):** سیپ و دیپ آدرس‌ها از ویژگی‌های اساسی در تحلیل ترافیک شبکه هستند. الگوهای ترافیکی غیرعادی، مانند حجم بالای ترافیک ناشی از یک یا چند آدرس IP منبع مشکوک به سمت یک آدرس IP مقصد خاص، می‌تواند نشان‌دهنده حمله DDoS یا تلاش برای دسترسی غیرمجاز باشد.
  + **بسته به ازای هر پیام (پی پی ام):** پی پی ام اشاره دارد به ‎‏ ... تعدادی از بسته‌ها مورد نیاز به انتقال دادن الف مجرد پیام یا واحد داده بیش از الف شبکه. داس حملات اغلب شامل کردن سیل ترافیک سنگین به شبکه یا سرور هدف. نظارت ‎‏ ... پی پی ام نسبت اجازه می‌دهد برای ‎‏ ... تشخیص غیرمعمول الگوها، کجا الف قابل توجه افزایش در تعداد بسته‌های ارسالی به ازای هر پیام، که نشان‌دهنده فعالیت مخرب بالقوه است.
  + **لرزش (Jitter):** لرزش به تغییر در زمان رسیدن بسته‌ها اشاره دارد. مقادیر بالای لرزش ممکن است نشان‌دهنده‌ی شبکه‌ی شلوغ یا مسدود شده باشد که می‌تواند به یک نقض امنیتی مانند حمله‌ی DDoS به زیرساخت شبکه نسبت داده شود.
  + **بسته ضرر نرخ (PLR):** این ویژگی نشان دهنده نرخ از بسته ضرر در ‎‏ ... ارتباط جریان. یک PLR قابل توجه می‌تواند عملکرد شبکه را کاهش دهد و نشان‌دهنده حملات احتمالی شبکه مانند قطعه قطعه شدن بسته یا حملات سیل‌آسای ICMP باشد.
  + **برچسب:**  برچسب ویژگی دسته‌ها ترافیک به کلاس‌های مختلف، مانند ترافیک عادی و حمله. این به عنوان حقیقت پایه برای آموزش مدل‌های یادگیری ماشین برای طبقه‌بندی و تشخیص دقیق حملات عمل می‌کند. با تجزیه و تحلیل با توجه به ویژگی‌های ترافیک حمله برچسب‌گذاری شده، مانند الگوهای موجود در ویژگی‌های فوق‌الذکر، مدل‌های یادگیری ماشین می‌توانند حملات را به طور مؤثر شناسایی و طبقه‌بندی کنند.
  + **داده‌ها انتقال معیارها (دی تی ام):** دیگر ویژگی‌ها شامل بایت‌های ارسالی ( *tx\_bytes* )، بایت‌های دریافتی ( *rx\_bytes* )، کیلوبیت‌های ارسالی در ثانیه ( *tx\_kbps* )، کیلوبیت‌های دریافتی در ثانیه ( *rx\_kbps* ) و کل کیلوبیت‌ها در ثانیه ( *tot\_kbps* ) می‌شود که بینشی در مورد نرخ و حجم انتقال و دریافت داده‌ها ارائه می‌دهد. افزایش غیرعادی در *tx\_kbps* یا *tot\_kbps* در مقایسه با ‎‏ ... عادی خط پایه سطوح می‌توانست نشان دادن الف حمله احتمالی ، مانند استخراج داده‌ها یا حملات DDoS حجمی.
  1. *تمایز از موجود مجموعه داده‌ها*

با این وجود، ‎‏ ... مجموعه داده‌های ترافیک DDoS در SDN خود را متمایز می‌کند از موجود مجموعه داده‌ها توسط آدرس‌دهی ‎‏ ... کلید محدودیت‌هایی که داشته باشند مقید قبلی تحقیق روی حملات انسداد سرویس (DDOS) تشخیص. برخلاف مجموعه داده‌هایی مانند KDD99 و NSL-KDD که محدود هستند توسط منسوخ شده شبکه معماری‌ها، این مجموعه داده‌ها با استفاده از شبیه‌ساز Mininet برای شبیه‌سازی توپولوژی‌های SDN واقع‌بینانه که به طور دقیق زیرساخت شبکه مدرن را منعکس می‌کنند، تولید شد. برای اطمینان از مرتبط بودن، سناریوهای حمله معاصر بودند یکپارچه، و مفصل مبتنی بر جریان معیارها برای پرداختن به انواع حملات منسوخ‌شده و ویژگی‌های ساده‌انگارانه موجود در مجموعه داده‌های قدیمی‌تر، جمع‌آوری شدند. علاوه بر این، در حالی که مجموعه داده‌های سنتی اغلب بر طیف محدودی از انواع حملات تمرکز دارند، ‎‏ ... رمان مجموعه داده‌ها شامل می‌شود الف گسترده‌تر طیفی از حملات DDoS پیچیده و چندوجهی، که منعکس کننده ماهیت در حال تحول تهدیدات امنیت سایبری است و آن را پیچیده‌تر می‌کند. قابل اجرا به ‎‏ ... فعلی امنیت چالش‌ها. در برخلاف مجموعه داده‌هایی که عمدتاً بر معیارهای سطح بسته متمرکز هستند، این مجموعه داده بر ویژگی‌های مبتنی بر جریان مانند بسته به ازای هر جریان (PPF) و بایت به ازای هر جریان (BPF) تأکید دارد که برای تشخیص ... بسیار مهم هستند. ظریف ناهنجاری‌ها درون شبکه جریان می‌یابد. این تمرکز، تجزیه و تحلیل دقیق‌تری از رفتار شبکه را ممکن می‌سازد، در نتیجه ارتقاء دهنده ‎‏ ... اثربخشی از میلی لیتر تکنیک‌ها بر اساس این داده‌ها آموزش داده شده‌اند . علاوه بر این، برای غلبه بر چالش‌های دسترسی که از نظر تاریخی قابلیت استفاده از بسیاری از مجموعه داده‌ها را محدود کرده‌اند، یک مجموعه داده سفارشی در Mendeley Data به صورت عمومی در دسترس قرار گرفته است که شفافیت را ارتقا داده و همکاری تحقیقاتی گسترده‌تری را ممکن می‌سازد. علاوه بر این، از طریق معیارسنجی دقیق در برابر مجموعه داده‌های پرکاربرد، مانند این مجموعه داده، مانند CICDDoS2019، عملکرد فوق‌العاده‌ای در تشخیص حملات DDoS، به‌ویژه از نظر دقت و نرخ هشدار اشتباه، نشان داده است. ترکیب شبیه‌سازی واقع‌گرایانه، نمایش حمله معاصر، معیارهای مبتنی بر جریان و دسترسی عمومی، مجموعه داده‌های ترافیک SDN-DDoS را به عنوان یک پیشرفت قابل توجه نسبت به گزینه‌های موجود تثبیت می‌کند.

* 1. *پرداختن به محدودیت‌های ترافیک مصنوعی نسل*

اگرچه ابزارهای تولید ترافیک مصنوعی مانند MGEN و hping3 بودند مفید برای شبیه‌سازی حملات انسداد سرویس (DDOS) حمله سناریوهای موجود در این مطالعه، پیچیدگی و غیرقابل پیش‌بینی بودن را به طور کامل نشان نمی‌دهند. از دنیای واقعی شبکه ترافیک. این می‌تواند سرب به مدل‌ها که انجام دادن خب در کنترل شده محیط‌ها، اما ممکن است نه تعمیم دادن به عنوان به طور موثر به دنیای واقعی شرایط، که در آن الگوهای ترافیک و رفتارهای حمله متنوع‌تر و پیچیده‌تر هستند [[19] ،](#_bookmark99) [[23] ،](#_bookmark103) [[32] .](#_bookmark112) برای پرداختن به این محدودیت‌ها، ما اذعان داریم که فقدان تنوع در دنیای واقعی در مجموعه داده‌های مصنوعی ممکن است بر دقت نتایج ما هنگام استقرار در محیط‌های عملیاتی تأثیر بگذارد [[25] .](#_bookmark105) [[27] .](#_bookmark107) مقایسه با مجموعه داده‌های CICDDoS2019 تا حدودی اعتبارسنجی را ارائه می‌دهد، اما کارهای آینده باید مجموعه داده‌های ترکیبی را در بر بگیرند که ترافیک مصنوعی را با داده‌های دنیای واقعی از منابعی مانند MAWI یا CAIDA ترکیب می‌کنند تا بهتر منعکس شوند. زنده شبکه شرایط. علاوه بر این، ‎‏ ... استفاده از

پیشرفته شبیه‌سازی پلتفرم‌ها، چنین به عنوان جنی یا DETERLab می‌تواند سناریوهای ترافیکی پویاتر و واقع‌بینانه‌تری ارائه دهد و استحکام مدل‌های یادگیری ماشین را برای تشخیص DDoS افزایش دهد.

1. **پیشنهادی چارچوب برای حملات انسداد سرویس (DDOS) تشخیص در SDN استفاده کردن ماشین یادگیری طبقه‌بندی**

در این بخش، ما حاضر الف جامع چارچوب برای

تشخیص حملات انسداد سرویس (DDOS) حملات در شبکه SDN محیط‌ها. حملات انسداد سرویس (DDOS) حملات، تهدید قابل توجهی برای زیرساخت شبکه محسوب می‌شوند، دسترسی به خدمات را مختل می‌کنند و باعث خسارات مالی می‌شوند [[45] .](#_bookmark125) با استفاده از تکنیک‌های طبقه‌بندی ML، چارچوب پیشنهادی اهداف به به طور موثر شناسایی و کاهش دادن حملات در محیط‌های SDN. شکل [6](#_bookmark56) تشخیص DDoS پیشنهادی را نشان می‌دهد. چارچوب برای اس دی ان. این چارچوب شامل می‌شود از چندین کلید مراحل، هر کدام حیاتی برای ‎‏ ... موفق تشخیص و کاهش حملات DDoS.

فرآیند ایجاد یک مجموعه داده ترافیک شبکه برچسب‌گذاری شده شامل چندین مرحله است. مرحله اول شامل جمع‌آوری داده‌ها بود که مستلزم جمع‌آوری داده‌های ترافیک شبکه از ‎‏ ... ام‌جن (مولتی ژنراتور) و hping3 ابزارها MGEN ابزاری همه‌کاره برای تولید انواع مختلف تومورهای خوش‌خیم است. شبکه ترافیک از جمله تی سی پی، بی سیم، و آی‌سی‌ام‌پی ترافیک. در مقابل، hping3 برای شبیه‌سازی انواع مختلف حملات DDoS مانند SYN، UDP و ICMP استفاده می‌شود. هر دو ابزار برای اطمینان از اینکه داده‌های جمع‌آوری‌شده طیف متنوعی از فعالیت‌های شبکه، از جمله ترافیک عادی و حملات DDoS را در بر می‌گیرند، مورد استفاده قرار گرفتند. مرحله دوم حاشیه‌نویسی بود که شامل برچسب‌گذاری دستی یا خودکار هر نمونه می‌شد. در ‎‏ ... مجموعه داده‌ها، با برچسب‌ها نشان دهنده آن کلاس: ترافیک عادی یا حمله DDoS. در این مرحله، موارد حمله DDoS بر اساس الگوهای حمله، امضاها و ... شناخته شده، حاشیه نویسی می‌شوند. یا رفتار ناهنجاری‌ها سوم مرحله است ویژگی استخراج، که شامل استخراج ویژگی‌های مرتبط از داده‌های ترافیک شبکه برای نمایش هر نمونه است. ویژگی‌های مشترک برای تشخیص DDoS شامل ویژگی‌های سطح بسته مانند اندازه بسته و نوع پروتکل؛ ویژگی‌های سطح جریان مانند جریان مدت زمان، بسته بشمار، بایت بشمار، بسته نرخ، و نرخ جریان؛ و ویژگی‌های آماری مانند آنتروپی اندازه بسته‌ها یا زمان‌های بین رسیدن. علاوه بر این، ویژگی‌های خاص دامنه یا فراداده‌هایی مانند آدرس‌های IP منبع/مقصد، شماره پورت‌ها، و بسته زمان‌بندی باید باش در نظر گرفته شده است. مرحله چهارم پیش‌پردازش داده‌ها بود که شامل پاکسازی و پیش‌پردازش مجموعه داده‌های ترافیکی حاشیه‌نویسی شده برای اطمینان از کیفیت و سازگاری داده‌ها بود. مرحله پنجم تقسیم مجموعه داده‌ها است که شامل تقسیم مجموعه داده‌های حاشیه‌نویسی شده به مجموعه‌های آموزشی، اعتبارسنجی و آزمایش است. مجموعه آموزشی برای آموزش مدل‌های یادگیری ماشین و مجموعه اعتبارسنجی برای ... مورد استفاده قرار گرفت. برای هایپرپارامتر تنظیم و مدل انتخاب، و مجموعه تست برای ارزیابی عملکرد مدل نهایی مورد استفاده قرار گرفت.

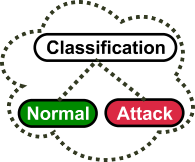
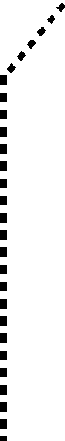
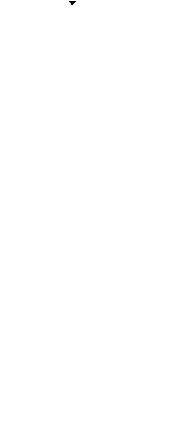
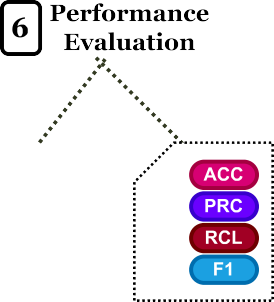
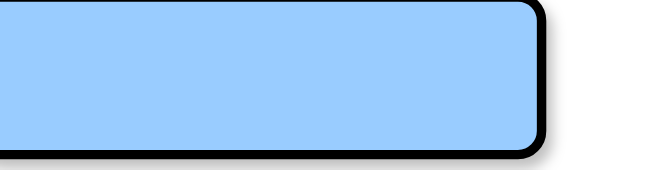
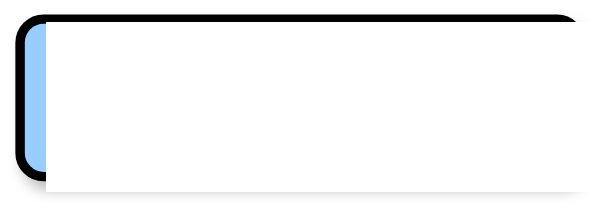
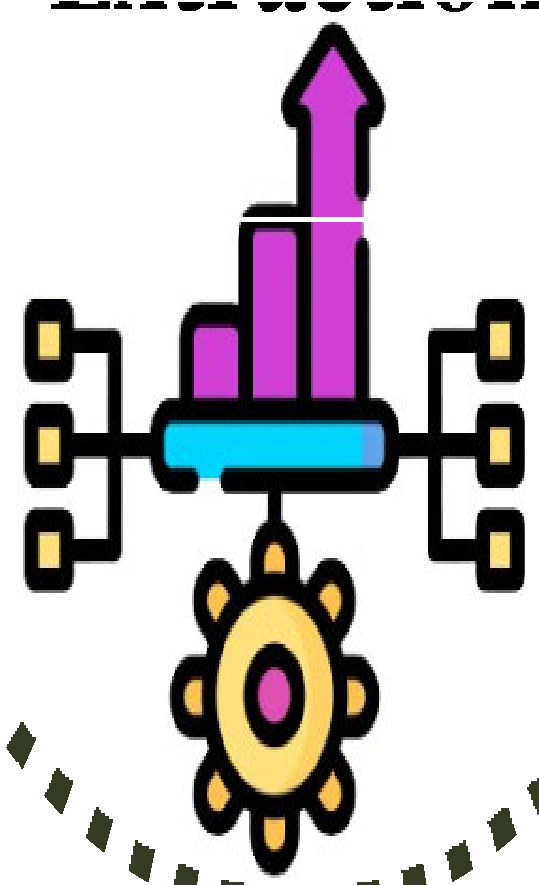
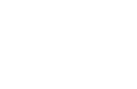
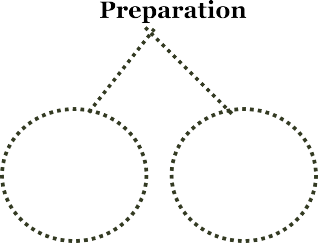
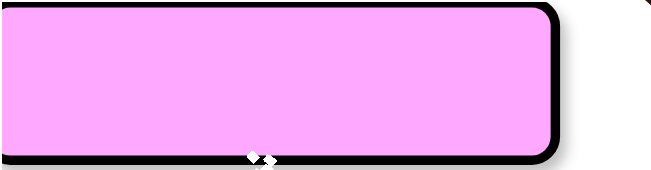
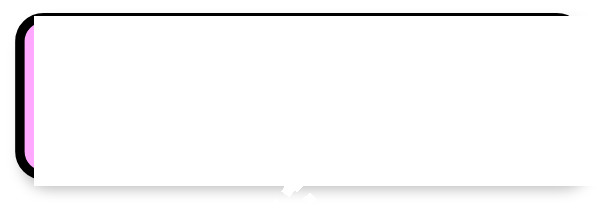
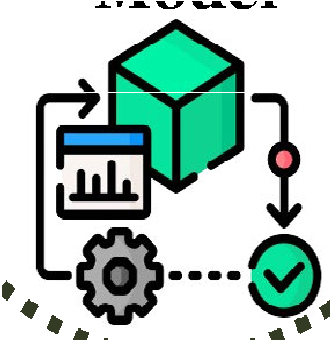
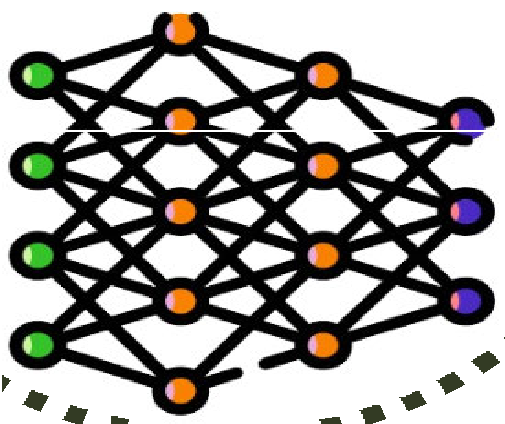
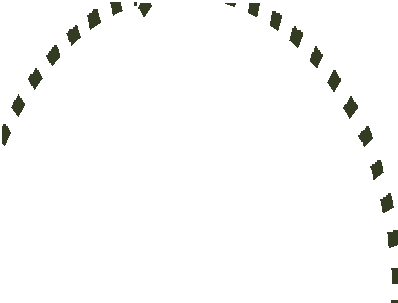
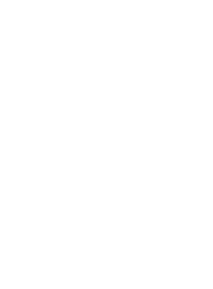
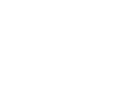
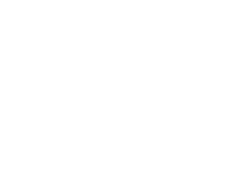
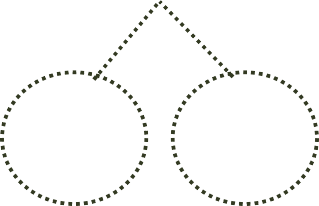
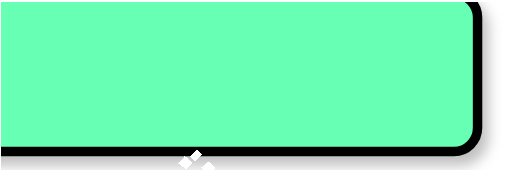
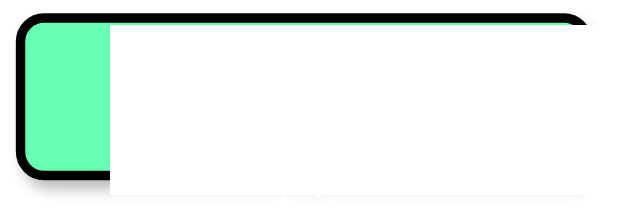
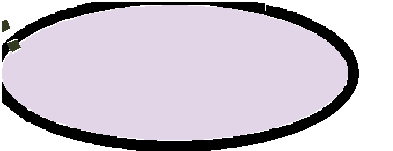
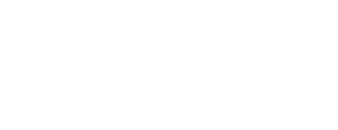
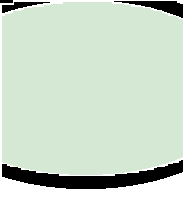
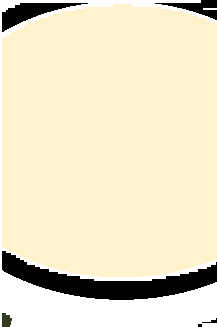
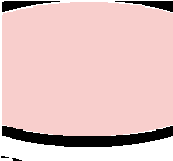
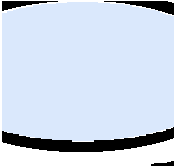
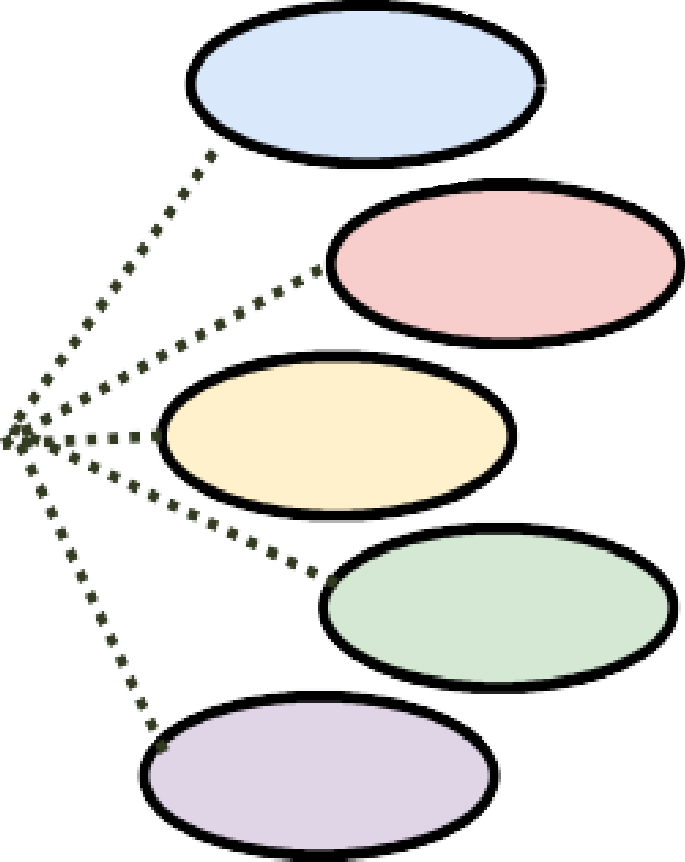
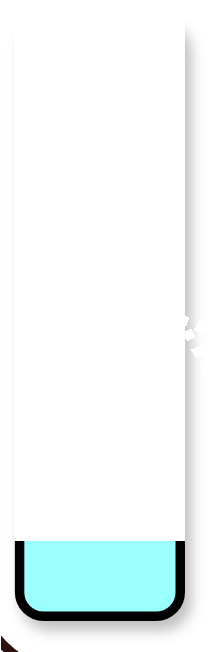
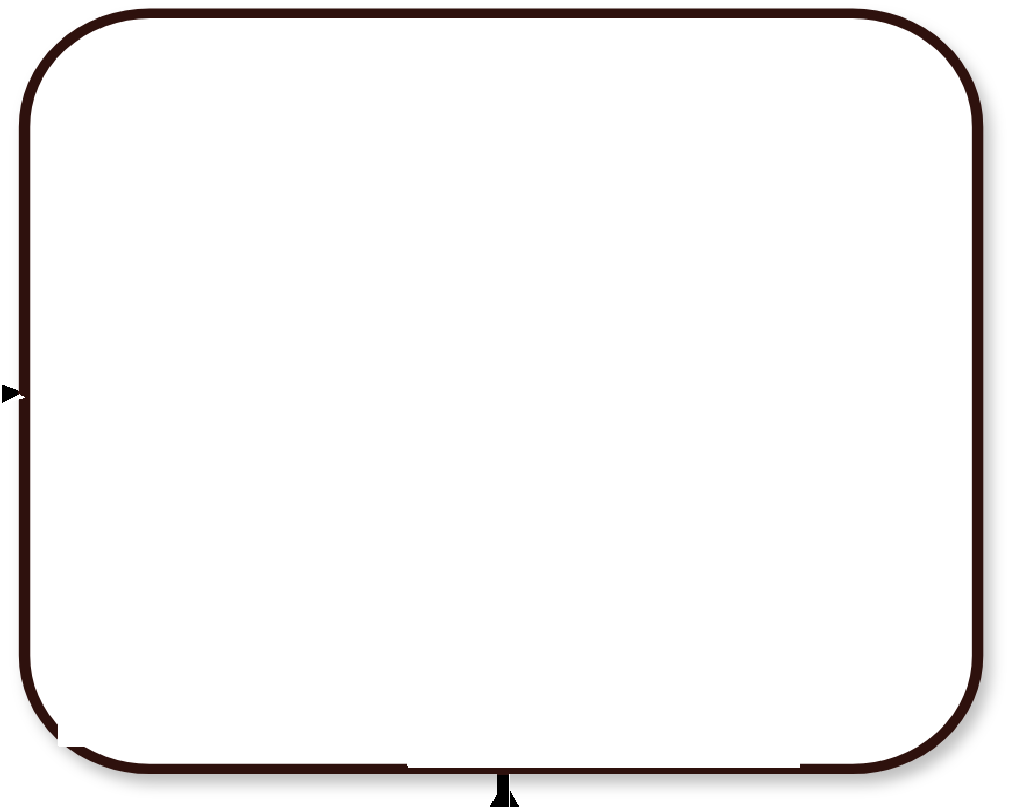
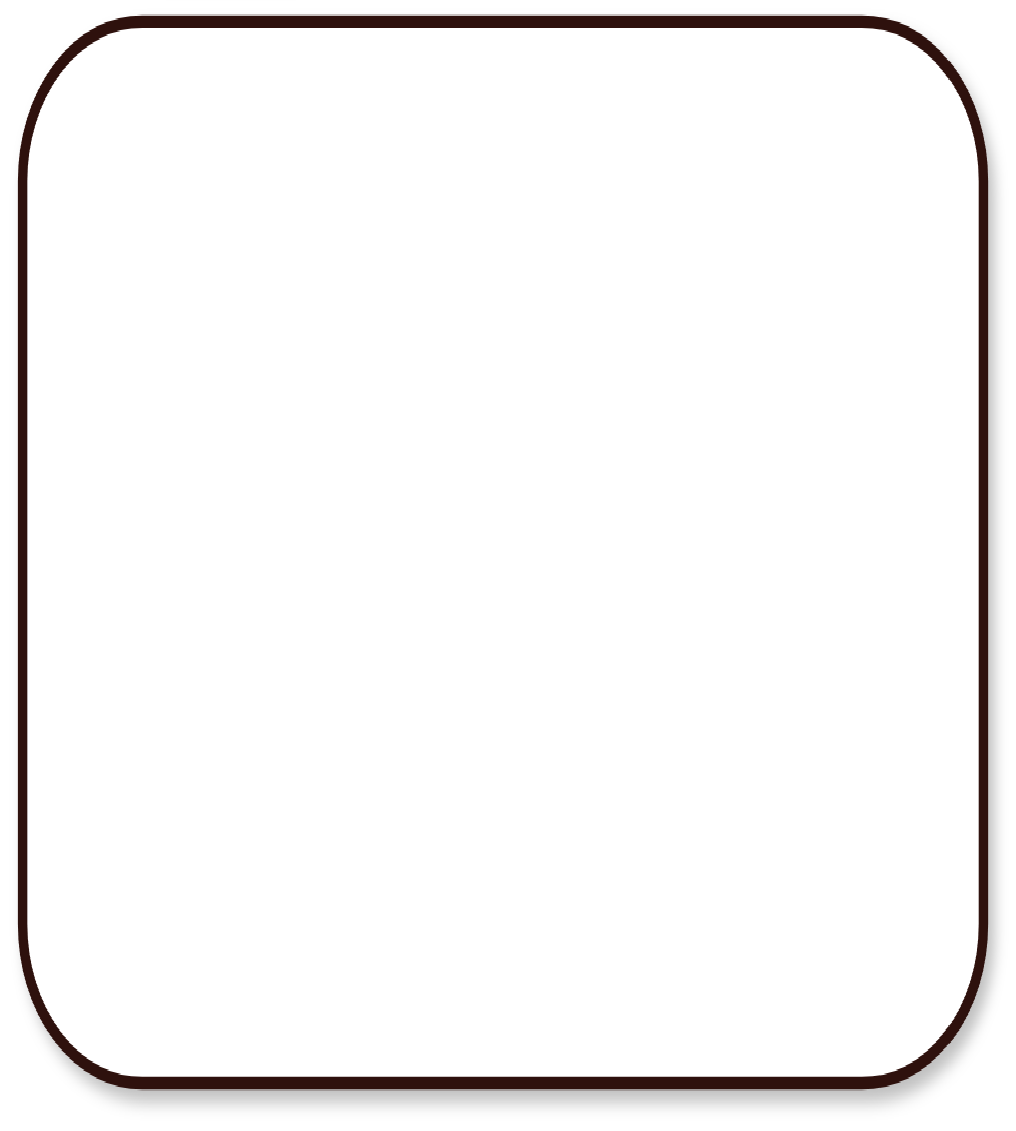
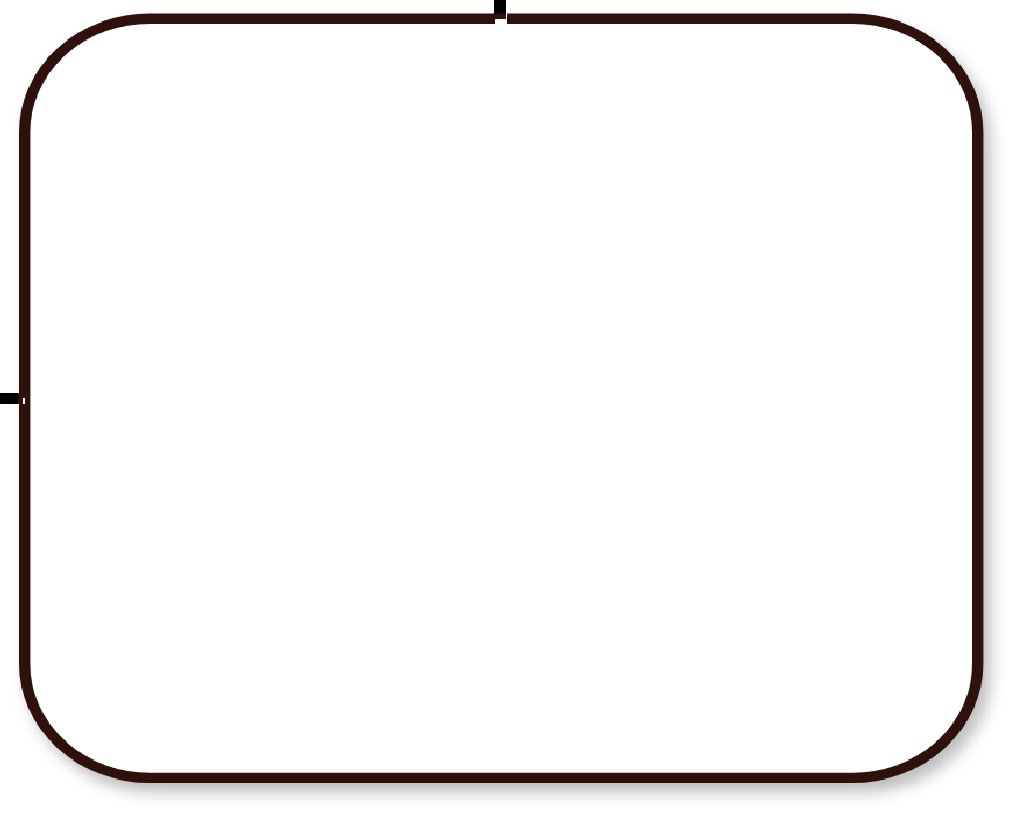
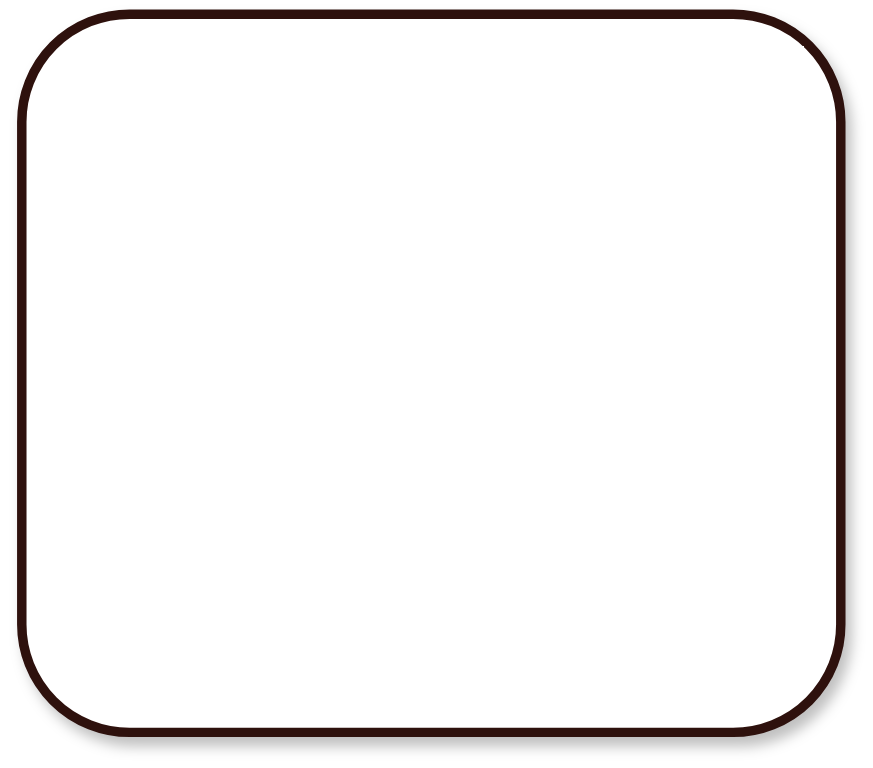
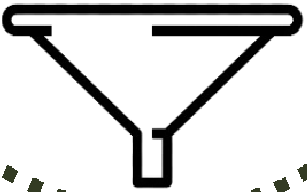
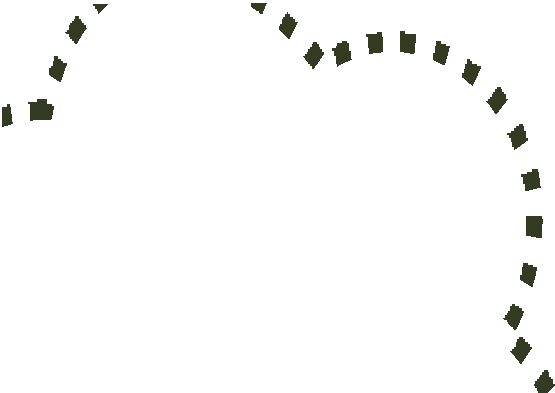
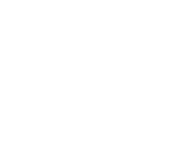
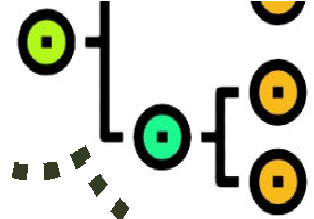
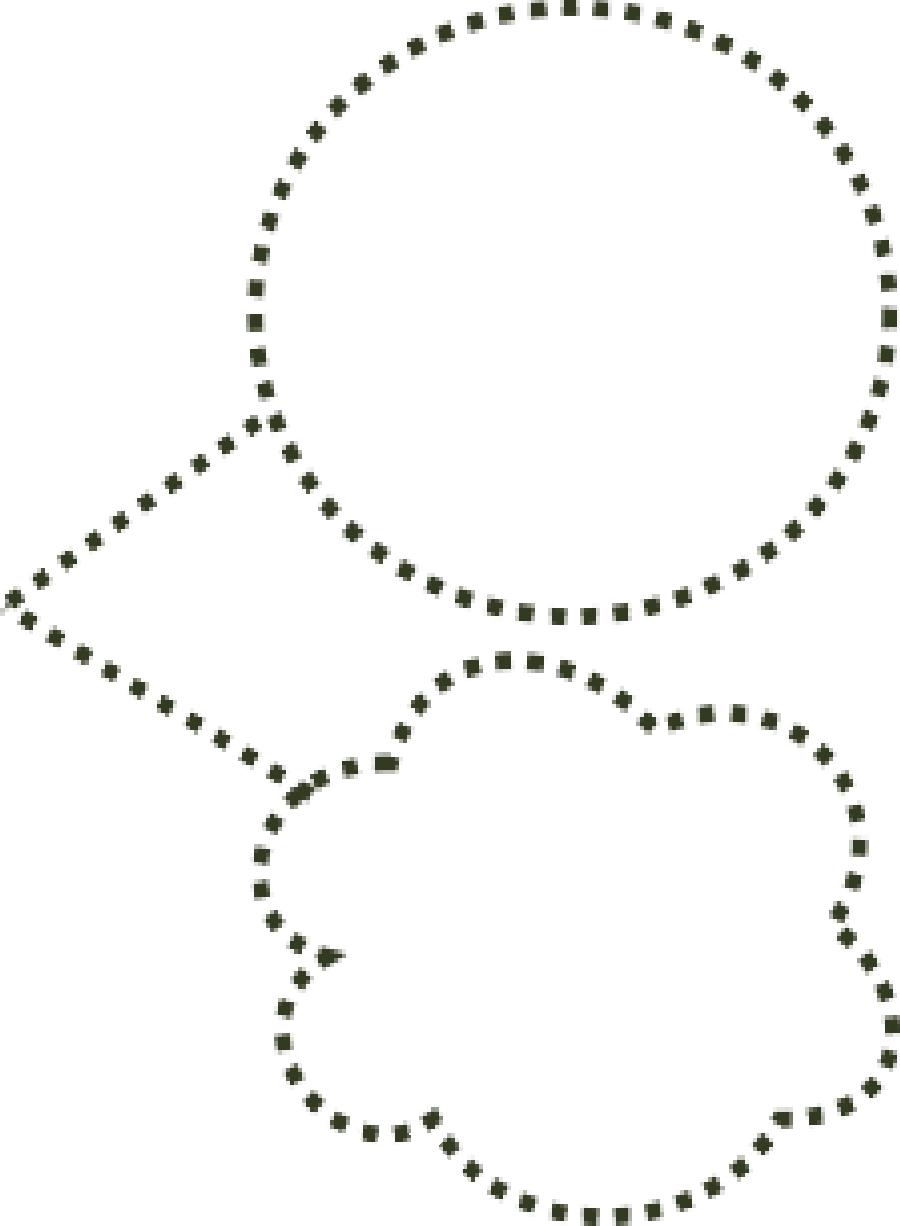
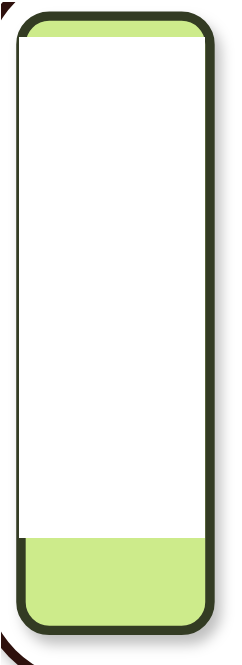
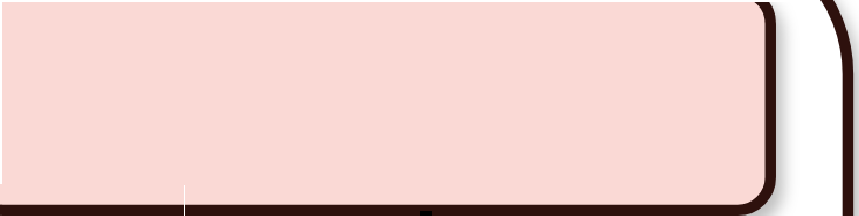
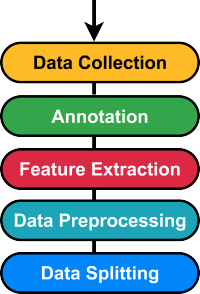
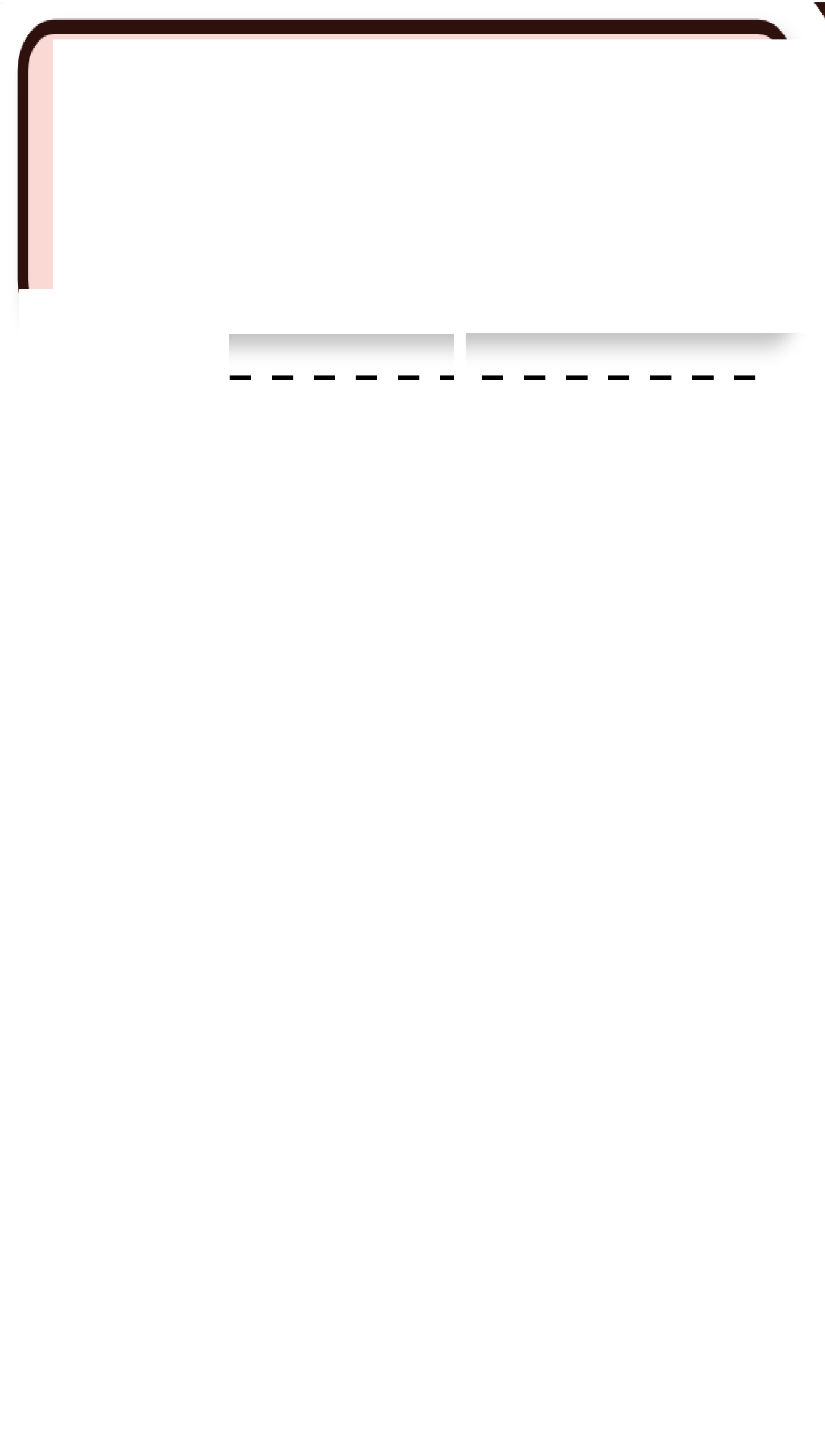
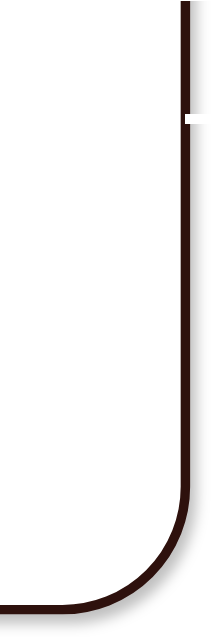
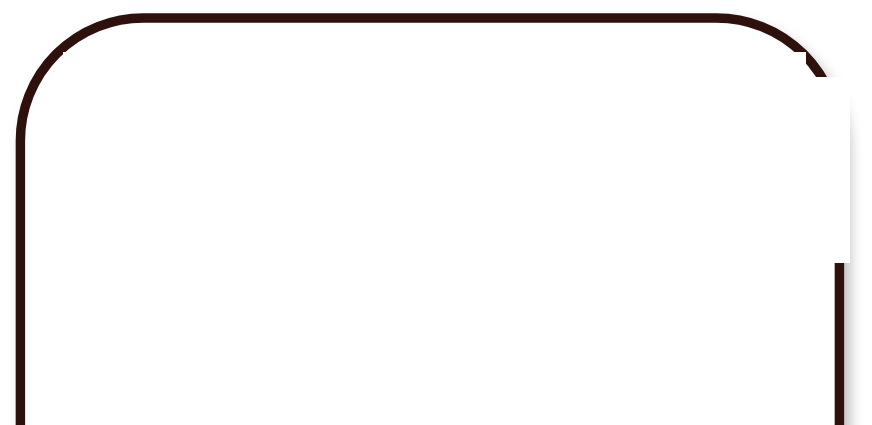
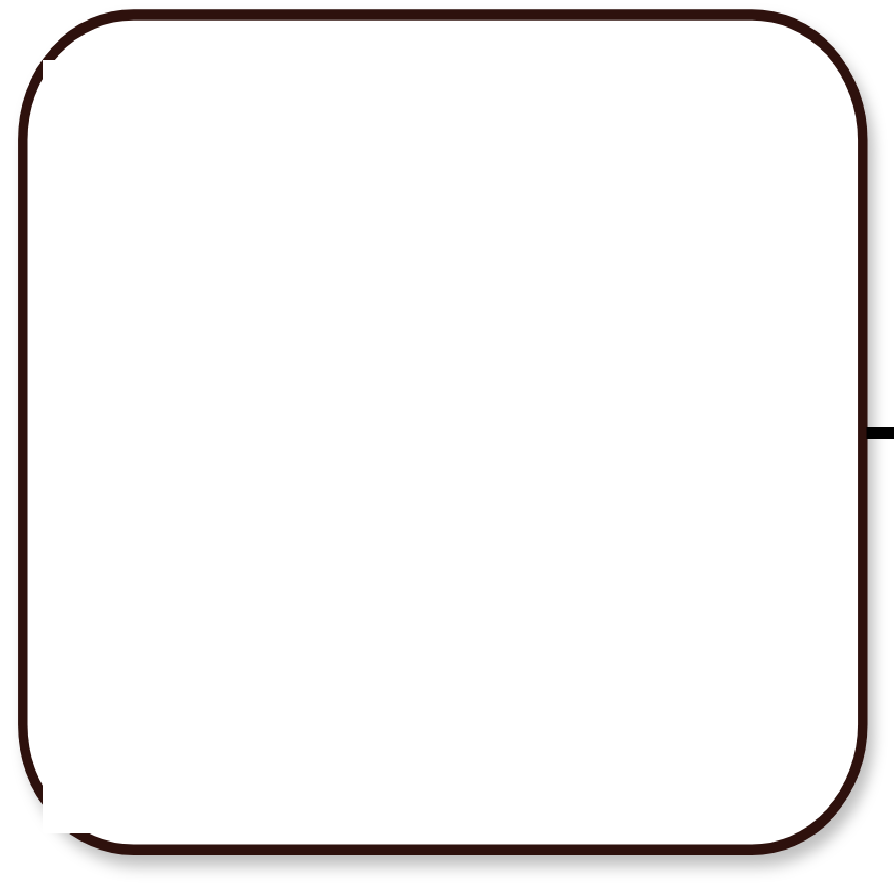
پس از به دست آوردن مجموعه داده‌های ترافیکی حاشیه‌نویسی‌شده، گام مهم بعدی آماده‌سازی داده‌ها برای آموزش مدل‌های یادگیری ماشینی بود. این کار تضمین می‌کرد که داده‌های آموزشی به درستی سازماندهی شده و آماده استفاده مؤثر باشند. کیفیت داده‌های ما آموزش داده‌ها به طور قابل توجهی تحت تأثیر قرار گرفته ‎‏ ... عملکرد

از مدل‌های یادگیری ماشین. داده‌های آموزشی نقش حیاتی در آموزش مدل‌ها برای تشخیص الگوها و روابط درون داده‌ها دارند و آنها را قادر می‌سازند تا پیش‌بینی‌های دقیقی انجام دهند یا طبقه بندی ها از دیده نشده داده‌ها چندین فازها هستند درگیر در آماده‌سازی داده‌های آموزشی. ابتدا، انتخاب/استخراج ویژگی را انجام می‌دهیم به شناسایی ‎‏ ... بیشترین مربوطه ویژگی‌ها برای آموزش ‎‏ ... مدل‌ها. در این مطالعه، ما مورد استفاده قرار گرفت ‎‏ ... الگوریتم کای-اسکوئر (Chi2) برای انتخاب آموزنده‌ترین ویژگی‌ها از مجموعه داده‌ها. پس از انتخاب ویژگی، مجموعه داده‌ها را به ویژگی‌ها (X) و برچسب‌ها (y) تقسیم می‌کنیم. متعاقباً، تقسیم شده ‎‏ ... مجموعه داده‌ها به آموزش و آزمایش مجموعه داده‌ها. معمولی تقسیم شده نسبت استفاده شده در ما مطالعه بود ۸۰-۲۰، کجا ۸۰٪ از داده‌ها بود استفاده شده برای آموزش ‎‏ ... مدل‌ها، و ‎‏ ... ۲۰٪ باقی‌مانده برای آزمایش عملکرد مدل در نظر گرفته شد.

در ‎‏ ... آموزش مرحله، ما آموزش دیده ما میلی لیتر مدل‌ها با استفاده از آموزش داده‌ها از ‎‏ ... حاشیه نویسی شده ترافیک مجموعه داده‌ها. ما مختلف به کار گرفته شده است میلی لیتر الگوریتم‌ها چنین به عنوان ال آر، ماشین بردار پشتیبان، آر اف، کی ان ان، و XGBoost به شناسایی الگوها و روابط درون داده‌ها. هر کدام الگوریتم است مبتنی بر روی متمایز اصول و ریاضی تکنیک‌ها برای یادگیری از داده‌ها، به عنوان مورد بحث در بخش [آی وی -الف](#_bookmark52) . بعد از ‎‏ ... تکمیل از آموزش برای هر الگوریتم، ما ارزیابی شده و مقایسه شده آنها عملکرد با استفاده از معیارها چنین به عنوان ‎‏ ... ای سی سی، جمهوری خلق چین، آر سی ال، و نمره F1 (ببینید بخش [هفتم](#_bookmark68) ). صرفه جویی ‎‏ ... آموزش دیده مدل‌ها امکان استقرار را فراهم می‌کند در شبکه SDN محیط‌ها به پیش‌بینی کردن دیده نشده داده‌ها. برای ‎‏ ... آزمایش داده‌ها، ما آماده شده آزمون داده‌ها از رسم ما مجموعه داده‌ها، متشکل از از ۶۹ ستون‌ها و تقریباً ۱,۰۴۸,۵۷۵ ردیف‌ها، بعد از پیش‌پردازش آزمون داده‌ها بودند جدا شدن از ‎‏ ... پیش پردازش شده مجموعه داده‌ها با استفاده از الف استاندارد تقسیم آموزش-آزمون. هر سطر در داده‌های آزمون، یک نمونه واحد از ‎‏ ... مجموعه داده‌ها با حاشیه نویسی شده برچسب‌ها برای ‎‏ ... هدف متغیر. در طول ‎‏ ... ارزیابی، آزمون داده‌ها بودند استفاده شده به ارزیابی کردن عملکرد از ‎‏ ... پنج میلی لیتر مدل‌ها. در ‎‏ ... زمینه از حمله DDoS طبقه بندی، عملکرد ارزیابی شامل می‌شود یک ارزیابی از ‎‏ ... توانایی از میلی لیتر مدل‌ها به به طور دقیق شبکه طبقه‌بندی ترافیک به دو دسته بندی ها: عادی و حمله کرد. از طریق سخت‌گیرانه ارزیابی معیارها و تکنیک‌ها چنین به عنوان دقت، دقت، به یاد آوردن، و امتیاز F1، ‎‏ ... اثربخشی از این مدل‌ها در تمایز بین ترافیک خوش‌خیم و مخرب الگوها بود به طور جامع تحلیل شده، تسهیل‌گری آگاهانه تصمیمات برای ارتقاء دهنده شبکه امنیت اقدامات. علاوه بر این، فقدان مجموعه داده‌های عمومی با داده‌های واقع‌بینانه ترافیک و جریان اطلاعات ژست‌ها الف چالش برای محققان در حال توسعه و ارزیابی کردن شناسه‌ها سیستم‌ها در SDN محیط‌ها. در این مطالعه، ما آدرس این شکاف با ارائه الگوریتمی برای تولید مجموعه داده با ترافیک و جریان اطلاعات در اس دی ان. الگوریتم [۱](#_bookmark58) طرح کلی فرآیند از مولد یک شبکه SDN ترافیک مجموعه داده‌ها با استفاده از مینی‌نت آزمایش‌ها الگوریتم متشکل از از دو اصلی

مراحل: مقداردهی اولیه و مینی‌نت آزمایش‌ها

* **مقداردهی اولیه:** در این مرحله، پارامترهایی را برای استخراج ترافیک آمار از مینی‌نت و معیارهای برچسب‌گذاری حملات و ترافیک عادی را مشخص کنید. این شامل راه‌اندازی یک توپولوژی Mininet با پیکربندی‌های مورد نظر، از جمله کنترل‌کننده‌ها، سوئیچ‌ها،



**شکل ۶.** چارچوب تشخیص DDoS پیشنهادی برای SDN را نشان می‌دهد و از تکنیک‌های طبقه‌بندی یادگیری ماشین برای شناسایی مؤثر حملات استفاده می‌کند. شناسایی و کاهش دادن حملات انسداد سرویس (DDOS) حملات. قدم ۱ به تصویر می‌کشد ‎‏ ... برچسب گذاری شده شبکه ترافیک مجموعه داده‌ها، قدم ۲ نشان می‌دهد ‎‏ ... آموزش مجموعه داده‌ها آماده سازی،

مرحله ۳ آموزش مدل را نشان می‌دهد، مرحله ۴ مدل آموزش‌دیده را مصورسازی می‌کند، مرحله ۵ آماده‌سازی داده‌های آزمایشی را نشان می‌دهد و مرحله ۶ عملکرد را برجسته می‌کند. ارزیابی.

و میزبانان در علاوه بر این، ما اجرا شده حمله سناریوهایی مانند حملات DDoS برای شبیه‌سازی ترافیک شبکه واقع‌گرایانه.

* + **رفتار مینی‌نت آزمایش‌ها:** در ‎‏ ... مینی‌نت در مرحله آزمایش‌ها، ما تولید ترافیک و ثبت ترافیک را اجرا می‌کنیم آمار در منظم فواصل برای هر کدام جریان در در شبکه، آمار جریان و پورت را از سوئیچ‌های SDN استخراج کردیم و ویژگی‌های اضافی مانند به عنوان تأخیر، لرزش، و بسته ضرر نرخ. اینها سپس آمارها در یک مجموعه داده ساختاریافته گردآوری می‌شوند.

پس از جمع‌آوری آمار، داده‌ها را برای تشخیص ترافیک حمله از ترافیک عادی تجزیه و تحلیل کردیم. بر اساس معیارهای از پیش تعریف شده، مجموعه داده‌ها را برچسب‌گذاری می‌کنیم و بر این اساس برچسب ۱ را به نمونه‌هایی که نشان‌دهنده ترافیک حمله هستند و برچسب ۰ را به نمونه‌هایی که نشان‌دهنده ترافیک عادی هستند، اختصاص می‌دهیم. در نهایت، مجموعه داده‌های ترافیک SDN حاشیه‌نویسی شده که از آزمایش Mininet مشتق شده‌اند، بازگردانده می‌شوند.

شکل [۷](#_bookmark59) نشان می‌دهد الف سفارشی مجموعه داده‌ها آفرینش بلوک نمودار ارزیابی سیستم‌های IDS و تشخیص ناهنجاری در SDN. مراحل مربوطه به شرح زیر است :

* + **طراحی توپولوژی:** توپولوژی شبکه، شامل کنترل‌کننده‌ها، سوئیچ‌ها و میزبان‌ها، برای شبیه‌سازی محیط SDN تعریف می‌شود.
* **راه‌اندازی Mininet:** محیط Mininet را با توپولوژی شبکه تعریف‌شده پیکربندی کنید تا از اتصال و عملکرد مناسب اطمینان حاصل شود.
* **کنترل کننده ادغام:** ادغام ‎‏ ... شبکه SDN کنترل‌کننده(ها) با ‎‏ ... مینی‌نت توپولوژی به مدیریت کردن شبکه عملیات و کنترل جریان ترافیک.
* **تولید ترافیک:** پیاده‌سازی تکنیک‌های مختلف تولید ترافیک، از جمله ترافیک عادی و سناریوهای حمله (مثلاً حملات DDoS)، برای شبیه‌سازی شرایط واقعی شبکه.
* **جمع‌آوری داده‌ها:** ثبت آمار ترافیک و اطلاعات جریان از سوئیچ‌های SDN در فواصل منظم، از جمله جریان و بندر آمار، تأخیر، لرزش، و نرخ از دست دادن بسته
* **ذخیره‌سازی و ساختاردهی:** داده‌های جمع‌آوری‌شده در یک ... ذخیره می‌شوند. ساختار یافته قالب و سازمان یافته به الف مجموعه داده‌ها مناسب برای تحلیل و آموزش مدل.

1. **آزمایش‌ها راه‌اندازی**

برای انجام آزمایش‌ها، انتخاب یک کنترل‌کننده مناسب برای شبیه‌سازی نقش حیاتی در تأثیرگذاری بر ... اثربخشی و اصالت از ‎‏ ... تحقیق. انتخاب کنترلر اعمال به عنوان الف بحرانی عامل تأثیرگذاری ‎‏ ... حکومتداری

**الگوریتم ۱** : الگوریتم تولید می‌کند الف مجموعه داده‌ها حاوی

ترافیک و جریان اطلاعات در شبکه SDN

# ۱: مقداردهی اولیه:

۲: تعریف کنید پارامترها برای استخراج ترافیک آمار از مینی‌نت.

۳: مشخص کنید معیارها برای برچسب زدن حمله و عادی ترافیک.

# ۴: رفتار مینی‌نت آزمایش‌ها:

۵: تنظیم بالا مینی‌نت توپولوژی با مورد نظر پیکربندی‌ها (کنترل‌کننده‌ها، سوئیچ‌ها، میزبان‌ها).

۶: پیاده‌سازی حمله سناریوها (مثلاً، حملات انسداد سرویس (DDOS) حملات).

۷: اجرا ترافیک نسل و گرفتن ترافیک آمار در فواصل منظم.

۸: **برای** هر کدام جریان **انجام دادن**

۹: استخراج جریان و بندر آمار از شبکه SDN سوئیچ ها

۱۰: محاسبه اضافی ویژگی‌ها (تاخیر، لرزش، بسته نرخ ضرر ).

۱۱: کامپایل کردن آمار به الف ساختار یافته مجموعه داده‌ها فرمت

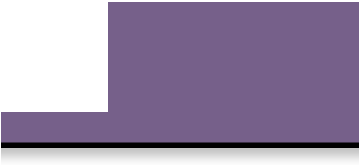
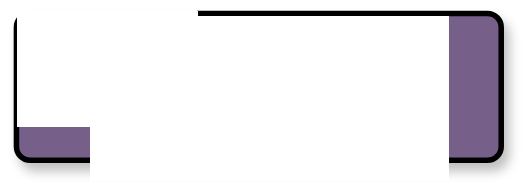
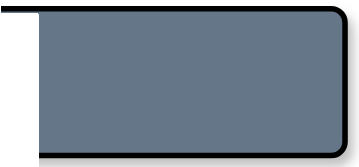
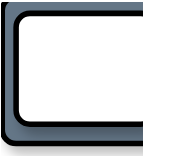
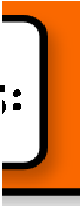
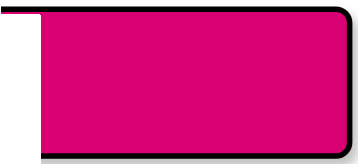
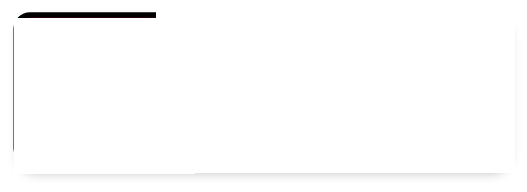
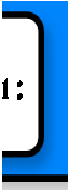
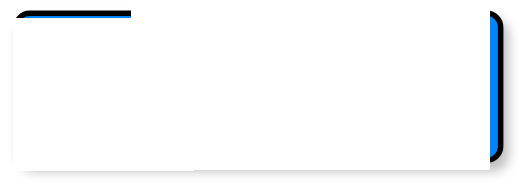
۱۲: **پایان برای**

# ۱۳: حاشیه‌نویسی ‎‏ ... مجموعه داده‌ها:

۱۴: تحلیل جمع‌آوری‌شده آمار به تمایز قائل شدن حمله ترافیک.

۱۵: برچسب ‎‏ ... مجموعه داده‌ها:

۱۶: برچسب ۱ را به نمونه‌های ترافیک حمله اختصاص دهید. ۱۷: اختصاص دادن برچسب 0 به عادی ترافیک موارد. ۱۸: **بازگشت:** مجموعه داده‌های ترافیک SDN حاشیه‌نویسی شده.



**شکل ۷.** چارچوب تولید مجموعه داده‌های سفارشی برای ارزیابی امنیت SDN.

از منابع شبکه و هماهنگی، که در نتیجه مستقیماً بر آن تأثیر می‌گذارد ‎‏ ... عملیاتی رفتار و عملکرد شاخص‌های شبکه SDN که تحت ارزیابی قرار دارند. کنترل‌کننده عمل می‌کند به عنوان ‎‏ ... مغز از SDN، ارکستراسیون ‎‏ ... جریان از داده‌ها و دستورات بین ‎‏ ... کنترل و داده‌ها هواپیماها آن انتخاب عمیقاً بر جنبه‌های مختلفی مانند مقیاس‌پذیری شبکه، استفاده از منابع، تأخیر و تحمل خطا تأثیر می‌گذارد. بنابراین، مراقب باشید ملاحظه است ضروری به اطمینان حاصل کردن اینکه کنترل‌کننده انتخاب‌شده با الزامات و اهداف خاص یک آزمایش همسو باشد. پس از ارزیابی گزینه‌های مختلف، ما انتخاب شده ‎‏ ... ریو کنترل کننده زیرا از آن

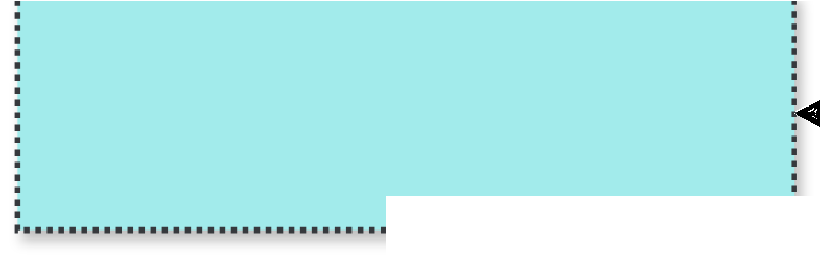
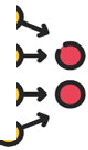
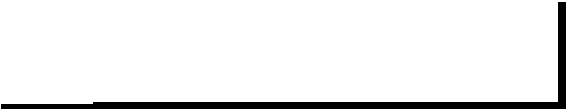
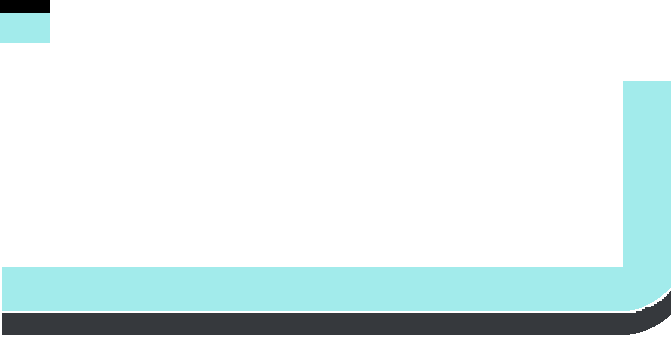
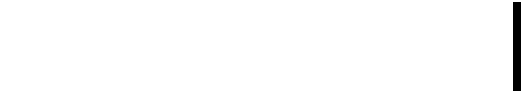
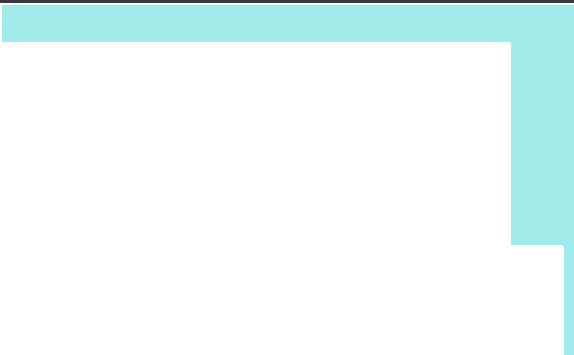
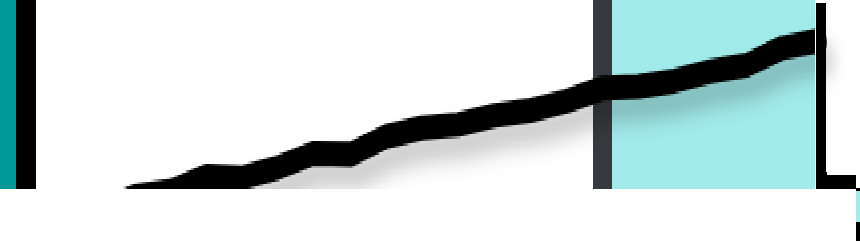
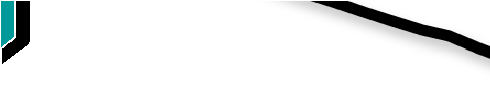
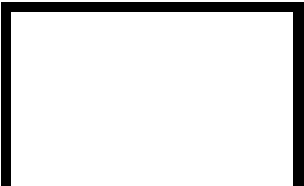
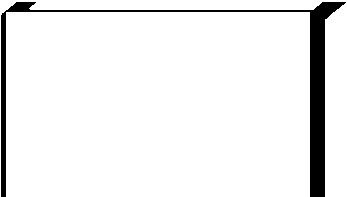
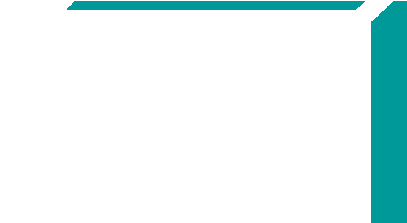
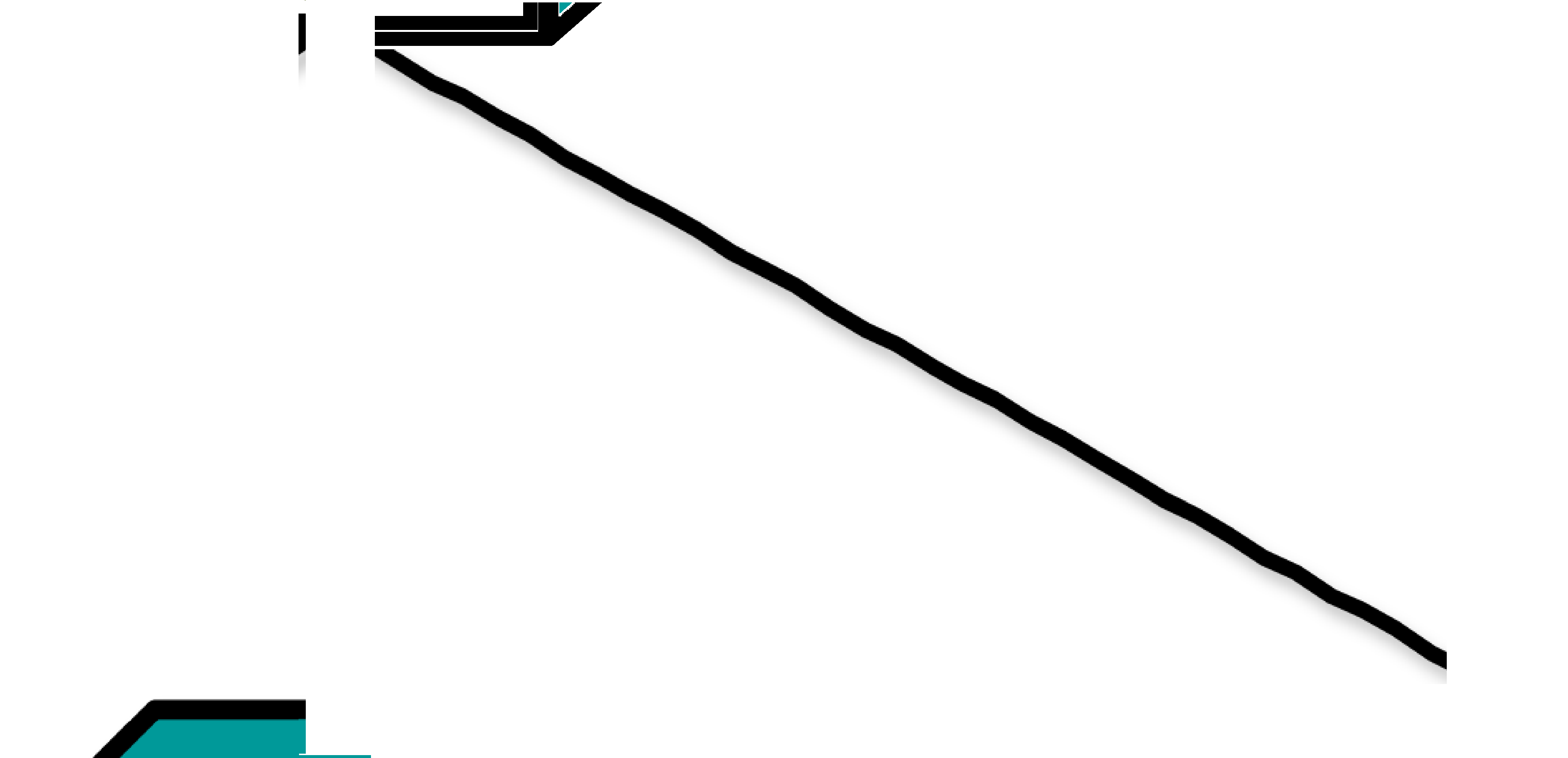
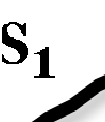
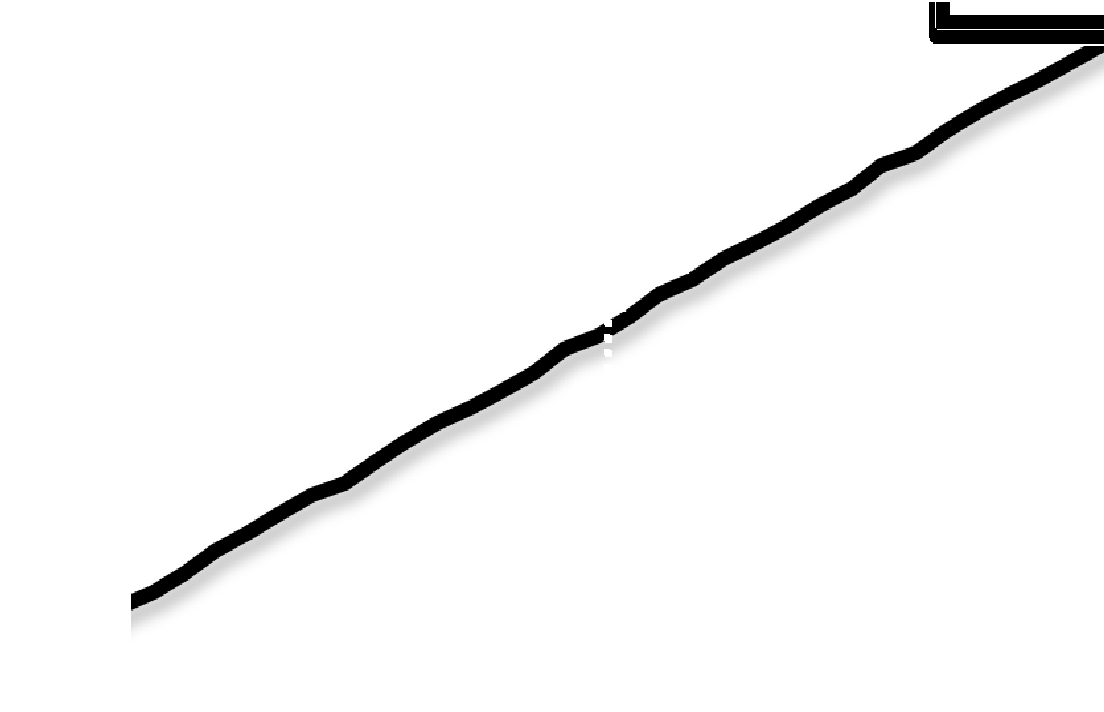
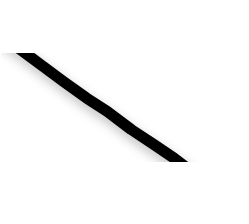
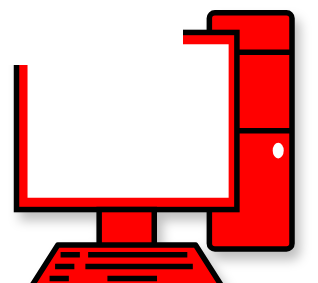
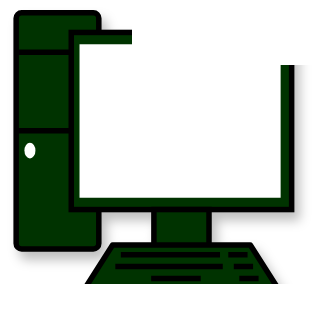
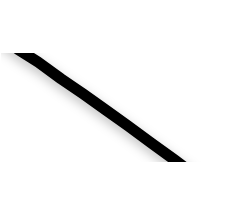
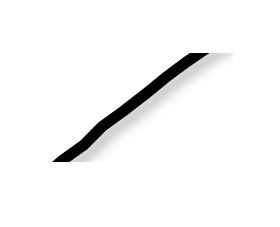
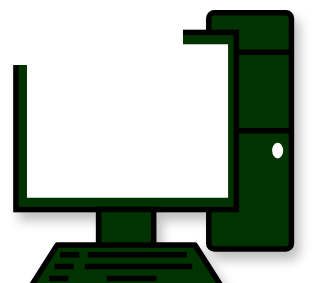
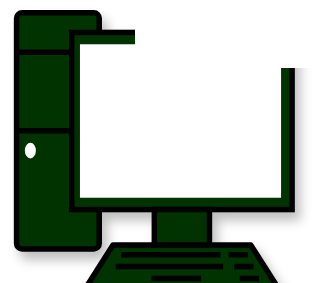
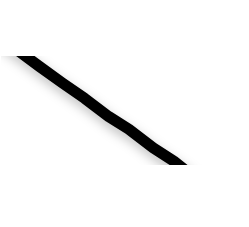
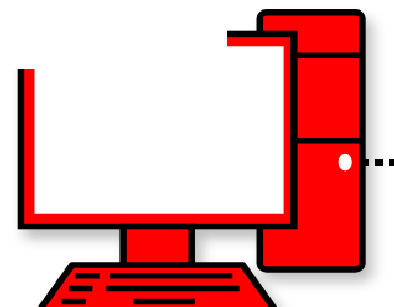
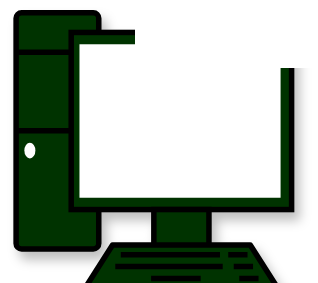
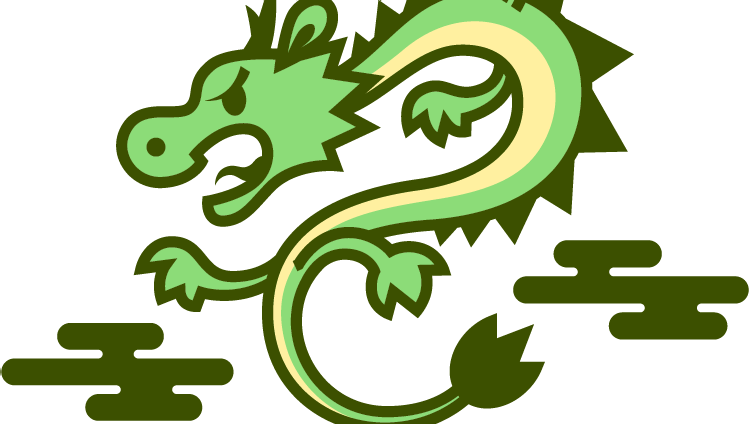
**جدول ۲.** پارامترها استفاده شده شبیه‌سازی محیط زیست.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

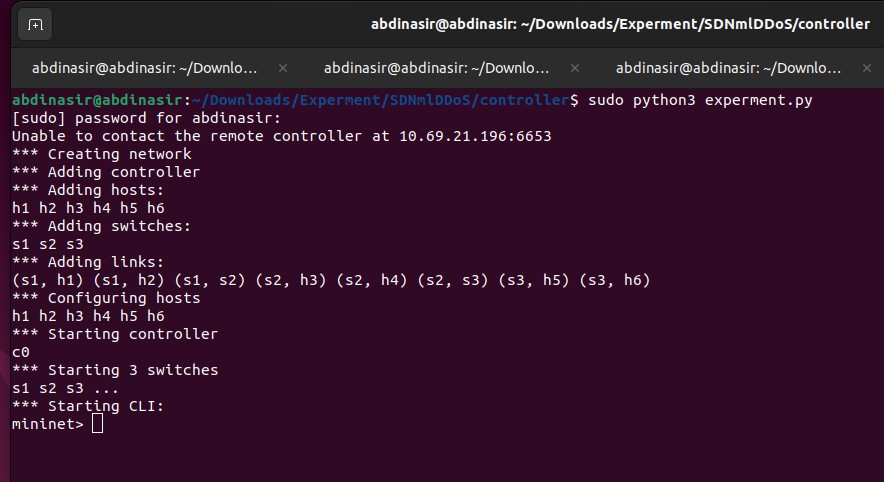
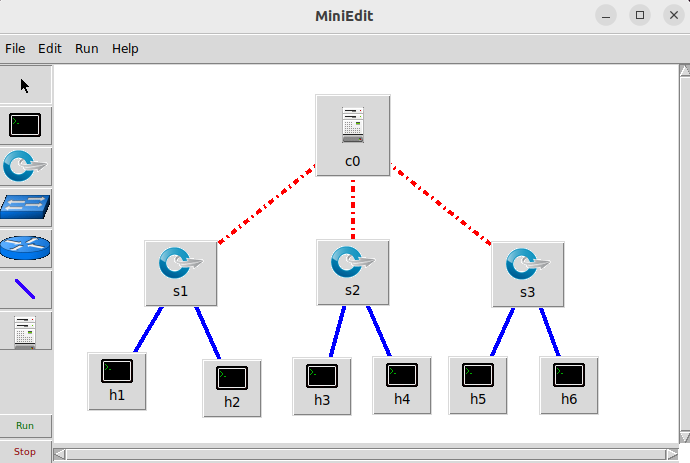
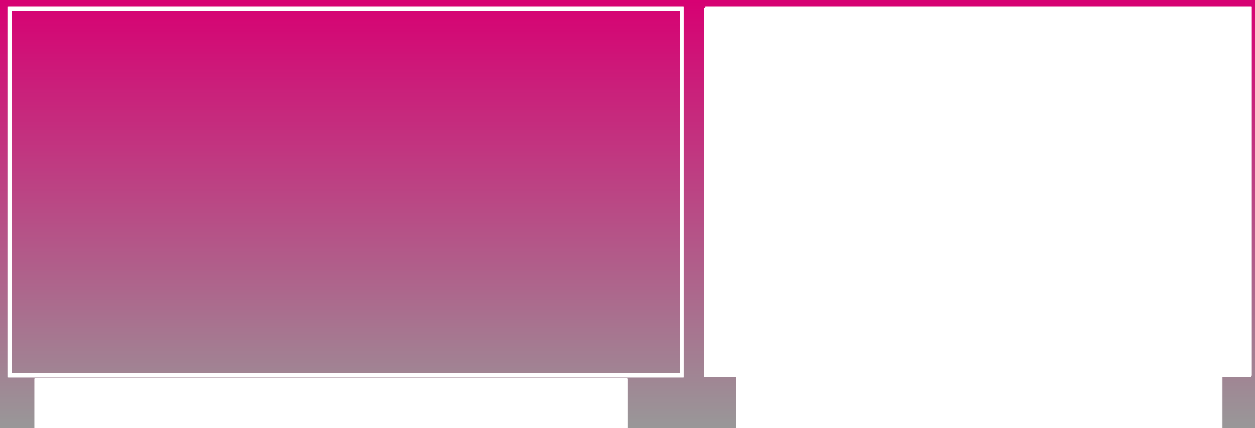
متعدد مزایا. ریو است یک متن‌باز کنترلر SDN مبتنی بر پایتون با سازگاری، توسعه‌پذیری و قابلیت اطمینان عالی [[46] .](#_bookmark126) پشتیبانی گسترده جامعه آن و توسعه مداوم، آن را برای محققان و متخصصان جذاب کرده است. سازگاری کنترلر با پروتکل OpenFlow همچنین امکان ادغام روان با اجزای مختلف شبکه را فراهم می‌کند و آزمایش‌ها و شخصی‌سازی‌های گسترده را تسهیل می‌کند.

برای شبیه‌سازی محیط SDN و تسهیل آزمایش‌ها، ما شاغل الف مینی‌نت شبیه ساز. Mininet یک پلتفرم سبک و مقیاس‌پذیر برای ایجاد شبکه‌های SDN مجازی با توپولوژی‌های قابل تنظیم و الگوهای ترافیکی واقع‌گرایانه فراهم می‌کند [[47] .](#_bookmark127) ادغام آن با کنترل‌کننده RYU فرآیند شبیه‌سازی را ساده می‌کند و محققان را قادر می‌سازد تا سناریوهای پیچیده شبکه را شبیه‌سازی کرده و ارزیابی کنند. ‎‏ ... عملکرد از شبکه SDN کاربردها و الگوریتم‌ها در کنترل شده محیط‌ها. شبیه‌سازی محیط زیست این سیستم بر روی یک دستگاه دسکتاپ با سیستم عامل اوبونتو ۲۲.۰۴.۳ LTS، مجهز به مشخصات سخت‌افزاری قوی از جمله ظرفیت دیسک ۱ ترابایت، گرافیک AMD Caicos، ۳۲ گیگابایت حافظه و یک پردازنده Intel Core i5 با فرکانس ۳.۴۰ گیگاهرتز و چهار هسته، میزبانی شد. توپولوژی شبکه شامل سه سوئیچ و شش میزبان است که با استفاده از بسته گرافیکی MiniEdit به طور دقیق طراحی شده‌اند تا پیکربندی‌های شبکه دنیای واقعی را شبیه‌سازی کرده و آزمایش‌های جامع را تسهیل کنند. جزئیات از هر کدام پارامتر استفاده شده در ‎‏ ... آزمایش هستند در جدول [2](#_bookmark60) فهرست شده است .

شکل [۸](#_bookmark63) توپولوژی شبکه‌ای متشکل از شش مورد را نشان می‌دهد میزبان‌ها متصل به سه باز وی‌سوئیچ (او وی اس) سوئیچ ها هر کدام



**شکل ۸.** شبکه SDN توپولوژی (آزمایشی تنظیم).



**شکل ۹.** مینی‌نت توپولوژی با یکی کنترل کننده و سه سوئیچ‌ها

سوئیچ OVS به یک کنترلر RYU متصل است. برنامه هواپیما شامل می‌شود سه اصلی اجزا: ‎‏ ... طبقه‌بندی‌کننده ترافیک یادگیری ماشینی، انتخابگر ویژگی و تجمیع‌کننده معیار جریان. طبقه‌بندی‌کننده ترافیک یادگیری ماشینی از الگوریتم‌های یادگیری ماشینی برای دسته‌بندی ترافیک شبکه بر اساس معیارهای از پیش تعریف‌شده استفاده می‌کند. این مؤلفه با بررسی بسته‌های داده ورودی، ترافیک بی‌خطر و مخرب را از هم تشخیص می‌دهد. توانمند سازی هوشمند تصمیم سازی و ترافیک مدیریت. ویژگی انتخابگر جزء شناسایی می‌کند مربوطه

ویژگی‌ها از ورودی شبکه ترافیک داده‌ها به افزایش کارایی عملیات بعدی. این امر ابعاد را کاهش می‌دهد از ‎‏ ... داده‌ها در حالی که حفظ حیاتی اطلاعات برای تحلیل یا تصمیم‌گیری فرآیندها. جریان تجمیع‌کننده معیارها جزء خلاصه می‌کند ‎‏ ... مرتبط با جریان معیارهایی برای جریان‌های مختلف شبکه، مانند تعداد بسته‌ها، تعداد بایت‌ها و مدت زمان. این تجمیع، بینش‌های ارزشمندی در مورد کل شبکه ارائه می‌دهد و نظارت بر عملکرد و عیب‌یابی را تسهیل می‌کند.

در این آزمایش، میزبان‌های ۲ (H2) و H6 به عنوان میزبان‌های مهاجمان در یک تلاش به سازش دیگر میزبان‌های درون شبکه. ما از پروتکل OpenFlow برای ارتباط استفاده کردیم بین ‎‏ ... کنترل کننده و شبکه عناصر، با شماره پورت کنترلر تنظیم شده روی ۶۶۵۳ برای ادغام و کنترل یکپارچه. برای تولید ترافیک بی‌خطر و مخرب، ما از دو ابزار مجزا استفاده کردیم: hping3 و MGEN. Hping3، یک ابزار شبکه خط فرمان، برای تولید و تجزیه و تحلیل بسته‌های TCP/IP، UDP و ICMP برای شبیه‌سازی ترافیک مخرب به کار گرفته شد. این شامل داده‌های شبکه‌ای است که برای ایجاد آسیب، اختلال یا دسترسی غیرمجاز طراحی شده‌اند. در مقابل، MGEN برای تولید ترافیک بی‌خطر استفاده شد که نشان‌دهنده داده‌های شبکه‌ای است که توسط کاربران یا دستگاه‌های مشروع برای اهداف معمولاً مجاز تولید می‌شوند.

علاوه بر این، شکل [9](#_bookmark64) دو توپولوژی مینی‌نت را نشان می‌دهد: الف) یک توپولوژی ساخته شده با برنامه نویسی و ب) یک توپولوژی طراحی شده با استفاده از بسته MiniEdit. توپولوژی اول نشان می دهد الف شبکه راه اندازی ایجاد شده از طریق کد، نمایش سه سوئیچ‌ها به هم پیوسته با میزبان‌ها، در حالی که ‎‏ ... توپولوژی دوم، یک طرح شبکه بصری طراحی شده را با استفاده از ... نشان می‌دهد. ‎‏ ... مینی ادیت گرافیکی کاربر رابط. اینها بازنمایی‌ها​ پیشنهاد بینش‌ها به متفاوت روش‌شناسی‌ها برای ایجاد و تجسم توپولوژی‌های شبکه در چارچوب Mininet، که نیازهای تحقیقاتی و تجربی متنوعی را در SDN برآورده می‌کند.

ما از تکنیک اعتبارسنجی متقابل ۵-لایه برای ارزیابی عملکرد مدل‌های خود استفاده کردیم. این تکنیک تضمین می‌کند که هر کدام داده‌ها زیرمجموعه خدمت می‌کند به عنوان الف آزمایش مجموعه یک بار در حالی که داده‌های باقی‌مانده برای آموزش استفاده می‌شوند و تخمین قابل اعتمادی از عملکرد مدل ارائه می‌دهند.



**شکل ۱۰. (یا: ۱۰.)** انتخاب شده ویژگی‌ها برای ‎‏ ... پیشنهادی مجموعه داده‌ها.

* 1. *مجموعه داده‌ها ویژگی‌ها انتخاب برای مدل آموزش*

شکل [۱۰](#_bookmark65) نمایش بصری از رتبه‌بندی اهمیت ویژگی‌ها را ارائه می‌دهد و متغیرهای انتخاب‌شده مشتق‌شده را برجسته می‌کند. از طریق ‎‏ ... سخت‌گیرانه چی۲ ویژگی انتخاب فرآیند. در ابتدا، این مطالعه شامل ۲۶ ویژگی بود، همانطور که در بخش [چهارم](#_bookmark51) . بهره گیری ‎‏ ... چی۲ ویژگی انتخاب روش‌شناسی، جدول [۳](#_bookmark66) ارائه می‌دهد الف گردآوری شده فهرست از انتخاب شده ویژگی‌ها، همراه با آنها مربوطه توضیحات این روش خدمت می‌کند به عنوان الف ابزار حیاتی برای نکته سنج آموزنده ویژگی‌ها از غیر آموزنده

**جدول ۳.** ویژگی‌های انتخاب‌شده از ‎‏ ... مجموعه داده‌ها.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

مواردی که در نتیجه، استحکام مجموعه داده‌های تولید شده را افزایش می‌دهند. تأکید بر فرآیند دقیق گزینش، که هدف آن جلوگیری از اثرات مضر بیش‌برازش است، با فشرده‌سازی مجموعه ویژگی‌ها به ۱۶ متغیر ضروری، بسیار مهم است. این رویکرد است پشتیبانی شده توسط قبلی تحقیق، مانند که از *زولپینی* و ال. [[48] ،](#_bookmark128) که نشان داده شده آن اثربخشی در مشابه تجربی زمینه‌ها سیستماتیک محاسبه کای اسکوئر با دقت ویژگی‌ها را بر اساس ارتباطشان ارزیابی می‌کند به ‎‏ ... هدف متغیر، بدین وسیله فراهم کردن الف چارچوب دقیقی برای تعیین اهمیت ویژگی‌ها. به طور کلی، این روش، اثربخشی مکانیسم‌های تشخیص حمله DDoS را افزایش می‌دهد و منجر به استراتژی‌های دقیق‌تر و مؤثرتر برای کاهش تهدید می‌شود.

* 1. *معیارهای ارزیابی الگوریتم‌های یادگیری ماشین در حمله DDoS کاهش خطر*

در این بخش، پارامترهای ارزیابی مورد استفاده برای ارزیابی اثربخشی الگوریتم‌های یادگیری ماشین در کاهش حملات SDN در برابر DDoS را شرح می‌دهیم. هر مدل یادگیری ماشین بر اساس معیارهای کلیدی، از جمله دقت، صحت، فراخوانی و ... ارزیابی شد. اف۱ امتیاز. درک ‎‏ ... پارامترها از ‎‏ ... ماتریس سردرگمی است ضروری برای ارزیابی کردن ‎‏ ... عملکرد از ‎‏ ... الگوریتم‌های یادگیری ماشینی الف بالا ارزش برای درست نکات مثبت و درست منفی‌ها، در امتداد با الف کم ارزش برای نادرست نکات مثبت و منفی‌ها، است حیاتی برای یک مؤثر نفوذ تشخیص سیستم (IDS) در

شبکه SDN محیط‌ها. تعاریف از هر کدام پارامتر از ماتریس درهم‌ریختگی به صورت زیر است.

* + - **حالت مثبت واقعی (Tpst):** یک مثبت واقعی نشان‌دهنده مواردی است که در آن‌ها مدل، کلاس مثبت را به درستی پیش‌بینی می‌کند، در حالی که کلاس واقعی مثبت است. در متن از شبکه SDN حملات انسداد سرویس (DDOS) تشخیص، الف درست مثبت زمانی رخ می‌دهد که الگوریتم یادگیری ماشین (ML) حمله DDoS را در حین وقوع حمله به درستی شناسایی کند.
    - **حالت منفی واقعی (Tnst):** یک منفی واقعی مواردی را نشان می‌دهد که در آن‌ها مدل به درستی کلاس منفی را پیش‌بینی می‌کند، در حالی که کلاس واقعی منفی است. به عنوان مثال، در تشخیص SDN DDoS، یک منفی واقعی زمانی رخ می‌دهد که الگوریتم ML به درستی حالت عادی را شناسایی کند. شبکه ترافیک به عنوان غیر مخرب در طول عملیات منظم .
    - **مثبت کاذب ایالت (فریم بر ثانیه):** مثبت کاذب رخ دادن وقتی مدل به اشتباه یک کلاس مثبت را پیش‌بینی می‌کند کلاس واقعی منفی است. برای مثال، در SDN حملات انسداد سرویس (DDOS) تشخیص، الف نادرست مثبت رخ می‌دهد چه زمانی الگوریتم یادگیری ماشین به اشتباه ترافیک عادی شبکه را به عنوان ترافیک مخرب شناسایی می‌کند و در نتیجه یک پاسخ غیرضروری یا هشدار را فعال می‌کند.
    - **حالت منفی کاذب (Fnst):** منفی‌های کاذب مواردی را نشان می‌دهند که در آن‌ها مدل به اشتباه کلاس منفی را پیش‌بینی می‌کند در حالی که کلاس واقعی مثبت است. به عنوان مثال، در تشخیص SDN DDoS، یک منفی کاذب رخ می‌دهد . چه زمانی ‎‏ ... میلی لیتر الگوریتم شکست می‌خورد به شناسایی الف حمله واقعی DDoS، که به طور بالقوه باعث می‌شود ترافیک مخرب ناشناخته باقی بماند.

یک IDS نقش حیاتی در دستیابی به سطوح بالای این پارامترهای عملکرد ایفا می‌کند. با نظارت مداوم بر ترافیک شبکه و اعمال الگوریتم‌های یادگیری ماشین، یک IDS می‌تواند فعالیت‌های مشکوک را به طور دقیق شناسایی و طبقه‌بندی کند و در نتیجه امکان سریع پاسخ‌ها به پتانسیل حملات انسداد سرویس (DDOS) حملات. در ماتریس درهم‌ریختگی، *Tpst* نشان‌دهنده‌ی نمونه‌های مثبتِ به‌درستی طبقه‌بندی‌شده، *Tnst* نشان‌دهنده‌ی نمونه‌های منفیِ به‌درستی طبقه‌بندی‌شده، *Fpst* نشان‌دهنده‌ی نمونه‌های منفیِ به‌غلط طبقه‌بندی‌شده به‌عنوان مثبت و *Fnst* نشان‌دهنده‌ی نمونه‌های مثبتی است که به‌غلط طبقه‌بندی‌شده به‌عنوان منفی هستند.

دقت (ای سی سی) اقدامات ‎‏ ... نسبت از به درستی موارد پیش‌بینی‌شده به ‎‏ ... مجموع شماره از موارد در ‎‏ ... مجموعه داده‌ها. این ارائه داد یک به طور کلی ارزیابی از ‎‏ ... دقت از ‎‏ ... مدل. ACC در ارزیابی اثربخشی کلی یک مدل یادگیری ماشین در شناسایی صحیح نمونه‌های حمله و عادی بسیار مهم است. بالا دقت نشان می‌دهد که ‎‏ ... مدل در طبقه‌بندی نمونه‌ها اشتباهات کمتری مرتکب می‌شود که منجر به تشخیص بهتر می‌شود. و کاهش از حملات انسداد سرویس (DDOS) حملات. معادلات ریاضی به شرح زیر است.

*ای سی سی* = *تی پی اس تی* + *تنست​* */ تی پی اس تی* + *تنست​* + *ف پِست* + *اف انست* (8)

دقت (PRC) نسبت مقادیر مثبت پیش‌بینی‌شده‌ی صحیح را اندازه‌گیری می‌کند. مشاهدات ( *تی پی اس تی* ) به مجموع پیش‌بینی شده مثبت مشاهدات ( *تپست + فریم در ثانیه* ). این نشان می‌دهد ‎‏ ... توانایی از ‎‏ ... مدلی برای طبقه‌بندی دقیق نمونه‌های مثبت. PRC ضروری است برای ارزیابی کردن ‎‏ ... قابلیت اطمینان از ‎‏ ... میلی لیتر مدل در به درستی

شناسایی حملات DDoS. امتیاز دقت بالا نشان می‌دهد که مدل نرخ مثبت کاذب پایینی دارد و احتمال طبقه‌بندی اشتباه نمونه‌های عادی به عنوان حمله را به حداقل می‌رساند. فرمول PRC به شرح زیر است :

*جمهوری خلق چین* = *تی پی اس تی /* *تی پی اس تی* + *پست*  *پیشتاز* (9)

فراخوانی (RCL)، که به عنوان حساسیت نیز شناخته می‌شود، نسبت مشاهدات مثبت پیش‌بینی‌شده‌ی صحیح ( *Tpst* ) به تمام مشاهدات در کلاس مثبت واقعی ( *Tpst + Fnst* ). این موضوع توانایی مدل را در شناسایی صحیح موارد مثبت برجسته می‌کند. موارد. آر سی ال است بحرانی برای ارزیابی ‎‏ ... توانایی مدل باید بتواند تمام نمونه‌های حملات DDoS را بدون از دست دادن هیچ نمونه‌ای ثبت کند. امتیاز بازخوانی بالا نشان می‌دهد که مدل دارد الف کم منفی کاذب نرخ، اطمینان از که آن تشخیص می‌دهد

‎‏ ... اکثریت از حملات انسداد سرویس (DDOS) حملات حاضر در شبکه ترافیک. معادله RCL به صورت زیر است :

*آر سی ال* = *تی پی اس تی /* *تی پی اس تی* + *اف انست*  (10)

اف۱ امتیاز (F1) است ‎‏ ... هارمونیک معنی از ‎‏ ... PRC و RCL را محاسبه می‌کند و معیاری متعادل از عملکرد مدل ارائه می‌دهد. این معیار، دقت و فراخوانی را در یک معیار واحد ترکیب می‌کند و در نتیجه ارزیابی جامعی از اثربخشی مدل ارائه می‌دهد. امتیاز *F1 برای* ارزیابی ... بسیار مهم است. ‎‏ ... به طور کلی عملکرد از ‎‏ ... میلی لیتر مدل برای تشخیص حمله DDoS . این روش هم موارد مثبت کاذب و هم موارد منفی کاذب را در نظر می‌گیرد، سازی آن الف قابل اعتماد نشانگر از الف مدل توانایی

برای حفظ تعادل بین دقت و فراخوانی. معادله زیر امتیاز *F1 را نشان می‌دهد* :

*ف* ۱ = ۲ ∗ ( *جمهوری خلق چین* ∗ *RCL* ) */* ( *جمهوری خلق چین)* + *RCL* ) (11)

1. **نتیجه و بحث**

تهدید حملات DDoS در محیط آنلاین رو به افزایش است؛ بنابراین، مکانیسم‌های دفاعی مؤثر بسیار مهم هستند. متعدد مطالعات داشته باشند مورد بررسی قرار گرفت ‎‏ ... کاربرد از ML تکنیک‌ها به شمارنده اینها حملات توسط اعمال نفوذ مجموعه داده‌های متنوع به بهبود بخشیدن ‎‏ ... تشخیص دقت. با این حال، قبلی​ مطالعات [[19] ،](#_bookmark99) [[23] ،](#_bookmark103) [[30] ،](#_bookmark110) [[32] ،](#_bookmark112) [[33] ،](#_bookmark113) [[34]](#_bookmark114) تولید شده مجموعه داده‌ها بدون توضیح کافی ویژگی‌های منحصر به فرد آنها. این مطالعه با معرفی یک رویکرد شفاف و عمومی موجود است مجموعه داده‌ها. توسط با دقت با مستندسازی جزئیات مجموعه داده‌ها، ما پایه و اساس روشنی برای آزمایش و اعتبارسنجی در اختیار محققان قرار دادیم. با استفاده از این مجموعه داده‌ها، پنج مدل یادگیری ماشین (جدول [4](#_bookmark69) ) را بر اساس ... ارزیابی کردیم. آنها ای سی سی، جمهوری خلق چین، ضبط، و اف۱ نمرات. نتیجه تجزیه و تحلیل مشخص می‌کند تصادفی جنگل به عنوان ‎‏ ... بیشترین مؤثر مدل برای تشخیص حمله DDoS

شکل [۱۱](#_bookmark70) توزیع نمونه‌های خوش‌خیم و مخرب را در کلاس‌های مختلف ترافیک (ICMP، UDP و TCP) در مجموعه داده‌ها نشان می‌دهد. این تجسم برای درک مجموعه داده‌ها بسیار مهم است زیرا بینشی در مورد ... ارائه می‌دهد. نسبی شیوع از خوش‌خیم و بدخواه ترافیک در هر کلاس ترافیک. با بررسی شکل [11](#_bookmark70) ، موارد زیر را مشاهده می‌کنیم .

* **ترافیک کلاس توزیع:**  افقی میله‌ها نماینده​ ‎‏ ... متفاوت ترافیک کلاس‌ها، با هر کدام بار بخش بندی شده

**جدول ۴.** معیارهای ارزیابی عملکرد برای پنج الگوریتم یادگیری تحت نظارت با استفاده از ‎‏ ... پیشنهادی مجموعه داده‌ها.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

به دو قطعات: یکی برای خوش‌خیم موارد و ‎‏ ... دیگر برای بدخواهی موارد. این خرابی اجازه می‌دهد برای الف درک روشن از چگونه هر کدام ترافیک کلاس مشارکت می‌کند به مجموعه داده کلی.

* + **اهمیت نسبی کلاس‌های ترافیک:** طول هر نوار، تعداد کل نمونه‌های مربوط به آن را نشان می‌دهد. ترافیک کلاس الف مقایسه از ‎‏ ... طول میله‌ها در کلاس‌های ترافیکی به درک اینکه کدام کلاس‌های ترافیکی در مجموعه داده‌ها رایج‌تر هستند، کمک می‌کند.
  + **خوش‌خیم در مقابل مخرب ترکیب:**  تقسیم‌بندی میله‌ها به نمونه‌های خوش‌خیم و مخرب، این امکان را فراهم می‌کند الف مستقیم مقایسه از آنها نسبت‌ها در هر کلاس ترافیک. این اطلاعات برای درک شیوع فعالیت‌های مخرب در انواع مختلف ترافیک شبکه ارزشمند است.



**شکل ۱۱. (یا: ۱۱.)** معیارهای عملکرد در بین دسته‌های ترافیکی برای هر نمونه ترافیکی.

جدول [۵](#_bookmark71) خلاصه‌ای از نمونه‌های ترافیک شبکه را ارائه می‌دهد که به دو دسته اصلی طبقه‌بندی می‌شوند: ترافیک مبهم و پروتکل‌های شبکه.

* + **دسته اول (ترافیک مبهم):** این دسته شامل نمونه‌های ترافیکی است که هم به صورت عادی و هم به صورت مشکوک طبقه‌بندی شده‌اند. ستون تعداد موارد نشان می‌دهد که ۵۲۳۱۹۵ مورد به صورت عادی و ۵۲۳۳۸۰ مورد به صورت مشکوک طبقه‌بندی شده‌اند. کل موارد ستون نشان می‌دهد ‎‏ ... تجمعی بشمار، کجا نمونه می شمارد برای عادی و مشکوک موارد با هم ترکیب می‌شوند و در مجموع ۱,۰۴۸,۵۷۵ نمونه به دست می‌آید.

**جدول ۵.** خلاصه از شبکه ترافیک موارد.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |
|  |  |  |
|  |  |
|  |  |





**شکل ۱۲.** آموزش و اعتبارسنجی دقت ها از کی ان ان مدل بیش از دوره‌ها

* **دسته دوم (پروتکل شبکه):** این دسته بر نمونه‌هایی که توسط پروتکل‌های شبکه مانند TCP، UDP و ICMP طبقه‌بندی شده‌اند، تمرکز دارد. ستون تعداد نمونه‌ها، تعداد هر پروتکل خاص را ارائه می‌دهد، که در آن 350358 نمونه به TCP، 348790 نمونه به UDP، و ۳۴۹,۷۲۷ به آی‌سی‌ام‌پی مجموع نمونه نمایش ستونی ‎‏ ... مجموع بشمار برای همه پروتکل‌ها، در نتیجه در ۱,۰۴۸,۵۷۵ مورد، وقتی TCP، UDP و ICMP را به صورت جمعی در نظر بگیریم.

شکل [۱۲](#_bookmark72) نشان می‌دهد که مدل KNN ما چقدر خوب از ... یاد گرفته است. ‎‏ ... داده‌ها بیش از زمان. آبی خط نشان می‌دهد چگونه ‎‏ ... دقت مدل با یادگیری از داده‌های آموزشی بهبود یافت، از ۷۴٪ شروع شد و پس از ۶۰ دوره به ۹۳.۵٪ رسید. این نشان می‌دهد که ما مدل تطبیق می‌دهد به سرعت به الگوها در ‎‏ ... داده‌ها. به طور مشابه، خط قرمز نشان دهنده دقت مدل برای جدید، دیده نشده داده‌ها (اعتبارسنجی دقت). آن شروع شده در ۸۳٪ و به طور پیوسته در همان ۶۰ دوره به ۹۴.۲٪ افزایش یافت. همسویی نزدیک بین دقت آموزش و اعتبارسنجی نشان می‌دهد که مدل KNN ما به طور مؤثر از داده‌ها بدون بیش‌برازش یا کم‌برازش یاد می‌گیرد، در نتیجه نشان می‌دهد آن توانایی به تعمیم دادن خب به جدید موارد.

* 1. *مدل عملکرد تحلیل و مقایسه*

شکل [۱۳(الف)](#_bookmark73) نشان می‌دهد الف جامع تحلیل از ‎‏ ... دقت‌ها از پنج متمایز تحت نظارت مدل‌ها. متغیر درجه دقت بین مدل‌ها، بینشی در مورد اثربخشی آنها ارائه داد. در ‎‏ ... تشخیص وظیفه تصادفی جنگل پدیدار شد

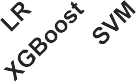
   



**شکل ۱۳. (یا: ۱۳.)** تحلیل مقایسه‌ای معیارهای عملکرد الگوریتم. زیرشکل‌های (الف) تا (ه) مقایسه عملکرد الگوریتم‌های مختلف را نشان می‌دهند. معیارهای کلیدی: (الف) دقت، (ب) دقت، (ج) فراخوانی، (د) نرخ تشخیص، و (ه) نرخ هشدار اشتباه. هر زیرشکل، معیارهای مرتب‌شده از کمترین تا بیشترین مقادیر را نشان می‌دهد و بینش‌های ارزشمندی در مورد اثربخشی الگوریتم‌ها در وظایف تشخیص و طبقه‌بندی ارائه می‌دهد.



به عنوان الف برجسته اجراکننده، با یک دقت از ۹۸.۹۷٪. این دقت استثنایی را می‌توان به مجموعه RF نسبت داد. یادگیری رویکرد که ترکیب می‌کند چندگانه درخت‌های تصمیم برای تولید پیش‌بینی‌های قوی. برخلاف درخت‌های تصمیم تکی، RF با تجمیع، خطر بیش‌برازش را کاهش می‌دهد. پیش‌بینی‌های تک تک درختان، که منجر به یک مدل عمومی‌تر و قابل اعتمادتر می‌شود. علاوه بر این، RF در ثبت تعاملات پیچیده داده‌ها عالی عمل می‌کند، و آن را به ویژه برای کارهایی که شامل داده‌های با ابعاد بالا یا روابط غیرخطی هستند، مناسب می‌سازد . عملکرد برتر آن ، ... را برجسته می‌کند. اثربخشی از گروه یادگیری در طبقه بندی وظایف، و موقعیت‌ها آر اف به عنوان ‎‏ ... مدل از انتخاب برای پیش‌بینی‌های دقیق و قابل اعتماد. رگرسیون لجستیک کمترین میزان را نشان داد دقت در میان ‎‏ ... مدل‌ها، با الف امتیاز از ۸۴.۳۱٪. سادگی و قابلیت تفسیر LR آن را به انتخابی محبوب برای... تبدیل کرده است. طبقه‌بندی دودویی وظایف. با این حال، آن خطی طبیعت ممکن است توانایی آن را در ثبت روابط پیچیده موجود در داده‌ها، در نتیجه در پایین‌تر پیش بینی کننده دقت. LR فعالیت می‌کند



با فرض خطی بودن بین متغیرهای مستقل و لگاریتم شانس از ‎‏ ... وابسته متغیر، که ممکن است در مجموعه داده‌هایی با الگوهای پیچیده یا روابط غیرخطی صادق نباشد . با وجود آن کاستی‌ها در دقت، ال آر به عنوان یک مبنای اساسی برای مقایسه عمل می‌کند و در موقعیت‌هایی که تفسیرپذیری مدل از اهمیت بالایی برخوردار است، ابزاری ارزشمند باقی می‌ماند. در ادامه، این مدل‌ها را به شرح زیر توضیح می‌دهیم.

* + - ال آر است ‎‏ ... ساده‌ترین مدل از ‎‏ ... گروه، به عنوان در شکل [13 (الف) نشان داده شده است](#_bookmark73) . با وجود سادگی، LR درک اساسی از روابط خطی ذاتی داده‌ها ارائه می‌دهد. با این حال، دقت 84.31٪ آن محدودیت‌هایی را در ثبت الگوهای ظریف در مجموعه داده‌ها نشان می‌دهد. اگرچه LR به عنوان یک مبنای ارزشمند عمل می‌کند، بیشتر پیشرفته مدل‌ها ممکن است پیشنهاد اثربخشی پیش‌بینی‌کننده برتر.
    - [13 (الف)](#_bookmark73) نشان داده شده است، SVM عملکرد فوق‌العاده‌ای از خود نشان داد. دقت از ۹۶.۵۲٪. توسط اعمال نفوذ بهینه

با وجود ابرصفحه‌ها برای مشخص کردن بین کلاس‌ها، SVM در تشخیص الگوهای داده پیچیده برتری دارد. با این حال، عملکرد آن ممکن است به انتخاب هسته و تنظیم پارامتر بستگی داشته باشد (شکل [13 (الف)](#_bookmark73) ). علیرغم این ملاحظات، SVM همچنان یک مدل قوی برای وظایف طبقه‌بندی است، همانطور که از دقت رقابتی آن مشهود است .

* + - * همانطور که به تصویر کشیده شده در شکل [۱۳(الف)](#_bookmark73) ، ‎‏ ... آر اف پدیدار شد به عنوان الف برجسته اجراکننده با یک دقت از ۹۸.۹۷٪. آن رویکرد گروهی، با تجمیع چندین درخت تصمیم‌گیری، RF را قادر می‌سازد تا تعاملات پیچیده داده‌ها را به طور مؤثر ثبت کند. علاوه بر این، ‎‏ ... تاب‌آوری از ‎‏ ... آر اف به بیش‌برازش قابلیت اطمینان آن را در کاربردهای دنیای واقعی تقویت می‌کند و موقعیت آن را به عنوان مدل برتر تثبیت می‌کند.
      * KNN دقت معقول ۹۷.۶۰٪ را نشان داد. KNN با طبقه‌بندی اشیاء بر اساس طبقه اکثریت نزدیکترین همسایگانشان، الگوهای پیچیده داده را به طور ماهرانه‌ای تشخیص می‌دهد. با این حال، اثربخشی آن ممکن است مشروط باشد. روی ‎‏ ... پارامتر تنظیمات، تأثیرگذار آن عملکرد​ در قطعی سناریوها (شکل [۱۳ (الف)](#_bookmark73) ). با این وجود، KNN همچنان یک مدل همه‌کاره و شهودی برای وظایف طبقه‌بندی است.
      * ایکس‌جی‌باووست تسلیم شد یک دقت از ۹۲.۳۶٪. اوینگ با توجه به مقیاس‌پذیری و عملکرد آن، XGBoost به طور متوالی دقت پیش‌بینی یادگیرنده‌های ضعیف را افزایش می‌دهد (شکل [۱۳ (الف)](#_bookmark73) ). اگرچه ایکس‌جی‌باووست پیشنهادات الف عملکرد رقابتی، بهینه نتایج نیاز داشتن دقیق تنظیم پارامتر برای کاهش بیش‌برازش و افزایش استحکام مدل.

شکل [۱۳ (ه)](#_bookmark73) نرخ هشدار اشتباه (FAR) مرتبط با هر مدل را نشان می‌دهد. RF کمترین FAR (0.023) را دارد و پس از آن SVM (0.036) و KNN (0.045) قرار دارند (شکل [13 (ه)](#_bookmark73) ). برعکس، ال آر و ایکس‌جی‌باووست به نمایش گذاشته شده به طور نسبی مقادیر بالاتر FAR، نشان‌دهنده تمایل بیشتر به هشدارهای کاذب است (شکل [1(e)](#_bookmark5) ). تحلیل FAR بر اهمیت قابلیت اطمینان و دقت مدل در به حداقل رساندن هشدارهای کاذب در وظایف تشخیص تأکید می‌کند.

* 1. *تحلیل از پهنای باند کاربرد در طول حمله و کاهش اثرات آن*

شکل [۱۴](#_bookmark74) میزان استفاده از پهنای باند را در طول زمان برای پورت‌های مختلف در طول یک حمله سایبری هماهنگ و اجرای اقدامات کاهش‌دهنده متعاقب آن نشان می‌دهد. هر خط روی ‎‏ ... گراف نشان دهنده ‎‏ ... پهنای باند استفاده یک پورت خاص در یک بازه زمانی ۳۰۰ ثانیه‌ای. در طول مرحله حمله که در نمودار نشان داده شده است، افزایش قابل توجهی در استفاده از پهنای باند در تمام پورت‌ها مشاهده می‌شود. پورت ۱ افزایش قابل توجهی در پهنای باند را تجربه کرد و به اوج تقریباً ۳۰۵۰ کیلوبیت بر ثانیه رسید. به طور مشابه، پورت‌های ۲ و ۳ نیز مصرف پهنای باند بالایی را نشان دادند که به ترتیب اوج‌هایی تقریباً ۹۵۰ و ۲۱۰۰ کیلوبیت بر ثانیه داشتند. پس از پیاده‌سازی از کاهش اقدامات، به عنوان نشان داده شده توسط ‎‏ ... خط‌چین خطوط در ‎‏ ... نمودار، آنجا است الف کاهش قابل مشاهده در استفاده از پهنای باند برای همه پورت‌ها. به ویژه، پورت ۱ نشان داده شده الف قابل توجه کاهش در پهنای باند

مصرف، به طور موثر کاهش دهنده ‎‏ ... تأثیر از ‎‏ ... حمله. پورت‌های ۲ و ۳ نیز پس از کاهش حمله، کاهش استفاده از پهنای باند را نشان دادند. هرچند به الف کمتر وسعت. الف مقایسه میزان استفاده از پهنای باند قبل و بعد از اقدامات کاهش، اثربخشی استراتژی‌های اجرا شده را برجسته می‌کند. نمودار به وضوح نشان می‌دهد که چگونه اقدامات کاهش ریسک موفقیت‌آمیز بوده‌اند. در کاهش تأثیر حمله، منجر به کاهش مصرف پهنای باند در تمام پورت‌ها می‌شود. کاهش مشاهده شده در استفاده از پهنای باند پس از کاهش حمله، تأکید می‌کند اثربخشی از ‎‏ ... اجرا شده استراتژی‌ها در کاهش تأثیر حملات سایبری. کاهش قابل توجه پهنای باند مصرف برای بندر ۱، در خاص، نشان می‌دهد موفق مهار از ‎‏ ... اثرات از ‎‏ ... حمله روی عملکرد شبکه. علاوه بر این، ‎‏ ... تحلیل در شکل [۱۴](#_bookmark74) ارزشمندی را فراهم می‌کند بینش‌ها به ‎‏ ... دینامیک از شبکه ترافیک در هر دو مرحله حمله و کاهش آسیب. این امر بر اهمیت اقدامات پیشگیرانه برای کاهش آسیب برای محافظت از یکپارچگی و ثبات شبکه، به ویژه در مواجهه با تغییرات روزافزون، تأکید می‌کند. تهدیدات سایبری. در نتیجه‌گیری، شکل [۱۴](#_bookmark74) خدمت می‌کند به عنوان نمایش بصری از اثربخشی استراتژی‌های کاهش اثرات برای کاهش دهنده ‎‏ ... تأثیر از الف شبیه‌سازی شده حمله سایبری بر عملکرد شبکه. این نمودار نقش حیاتی اقدامات پیشگیرانه در افزایش امنیت و تاب‌آوری شبکه را تقویت می‌کند و در نتیجه عملکرد بی‌وقفه زیرساخت‌ها و خدمات حیاتی را تضمین می‌کند.



**شکل ۱۴.** پهنای باند کاربرد بیش از زمان در طول حمله و کاهش.

* 1. *مقایسه‌ای تحلیل: رمان مجموعه داده‌ها در مقابل CICDDoS2019*

CICDDoS2019 شامل حملات DDoS و ترافیک شبکه بی‌خطر است، که آن را به منبعی ارزشمند برای مطالعه و مقایسه رفتارهای مخرب و مشروع شبکه تبدیل می‌کند. iors [[49] .](#_bookmark129) این دوگانگی محققان را قادر می‌سازد تا سیستم‌های تشخیص نفوذ را به طور مؤثر توسعه داده و ارزیابی کنند. به دلیل ویژگی‌های جامع آن، مجموعه داده CICDDoS2019 به طور گسترده در تحقیقات امنیت سایبری مورد استفاده قرار گرفته است. محققان برای آزمایش عملکرد مدل‌های مختلف یادگیری ماشینی به منظور تمایز بین حملات خوش‌خیم و حملات بی‌خطر، به این مجموعه داده تکیه کرده‌اند. و بدخواه شبکه فعالیت‌ها. برای ارزیابی اهداف،

**جدول ۶.** مقایسه عملکرد مدل RF با استفاده از مجموعه داده جدید و CICDDoS2019.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

معیارهای ارزیابی مانند دقت، صحت، بازخوانی و امتیاز F1 برای مقایسه عملکرد مدل‌ها استفاده شدند (به جدول [6 مراجعه کنید](#_bookmark76) ). مدل RF هنگام اعمال بر روی CICDDoS2019، با دقت ...، نتایج قابل توجهی به دست آورد. ۹۷.۶۲٪، دقت ۹۸.۷۰٪، فراخوانی ۹۷.۷۳٪ و امتیاز F1 از ۹۷.۶۹٪. به طور مقایسه‌ای، روی ‎‏ ... رمان مجموعه داده‌ها، ‎‏ ... مدل RF با دقت ۹۸.۹۷٪، عملکرد برتر را نشان داد. دقت از ۹۸.۳۳٪، به یاد بیاورید از ۹۶.۳۷٪، و امتیاز F1 برابر با ۹۷.۳۴٪. این یافته‌ها بر اهمیت عرف تأکید دارند. مجموعه داده‌ها در امنیت سایبری تحقیق، ارائه دقت و استحکام بهبود یافته در مقایسه با CICDDoS2019. این مجموعه داده جدید، منبع ارزشمندی را در اختیار محققان قرار می‌دهد. برای در حال پیشرفت نفوذ تشخیص روش‌شناسی‌ها و بررسی تکنیک‌های پیشرفته مانند یادگیری عمیق.

در خلاصه، به ارزیابی کردن ‎‏ ... تأثیر از ویژگی با توجه به انتخاب بر اساس عملکرد مدل، ما یک مطالعه فرسایش انجام دادیم که مقایسه‌ای بین مدل دقت قبل از و بعد از اعمال کردن انتخاب ویژگی تکنیک‌ها. نتایج نشان داد که مدل‌ها چنین به عنوان آر اف، ماشین بردار پشتیبان، و کی ان ان به طور قابل توجهی بهبود یافته در دقت، دقت ، و به یاد بیاورید چه زمانی با استفاده از کای اسکوئر و بازگشتی تکنیک‌های حذف ویژگی (RFE). این تحلیل نشان می‌دهد که انتخاب ویژگی نه تنها توانایی مدل را در تشخیص حملات DDoS افزایش می‌دهد، بلکه با حذف ویژگی‌های نامربوط، خطرات بیش‌برازش را نیز کاهش می‌دهد. با به حداقل رساندن نویز در داده‌ها، ویژگی‌های انتخاب شده مدل‌ها را قادر می‌سازند تا به الگوهای ترافیکی دیده نشده، بهتر تعمیم دهند.

* 1. *مقایسه‌ای تحلیل از رمان و تأسیس شد مجموعه داده‌ها*

علاوه بر ارزیابی عملکرد مجموعه داده پیشنهادی، الف مقایسه بود انجام شده با ‎‏ ... مجموعه داده CICDDoS2019 . این مقایسه به این دلیل انتخاب شد که CICD-DoS2019 شامل ترافیک شبکه جدیدتر و متنوع‌تری است ، که باعث می‌شود آن به ویژه مربوطه برای تشخیص DDoS معاصر . در مقابل، اگرچه مجموعه داده‌های NSL-KDD و KDD داشته باشند شده به طور گسترده استفاده شده در قبلی مطالعات، آنها محدودیت‌هایی را ارائه می‌دهند که کاربردپذیری آنها را در چشم‌اندازهای تهدید فعلی کاهش می‌دهد. به طور خاص، مجموعه داده NSL-KDD، که از مجموعه داده قدیمی‌تر KDD Cup 1999 مشتق شده است، الگوهای ترافیک شبکه مدرن یا استراتژی‌های حمله را به طور دقیق منعکس نمی‌کند. هم KDD و هم NSL-KDD مجموعه داده‌های ایستا هستند، به این معنی که با گذشت زمان تکامل نمی‌یابند. از آنجایی که ترافیک شبکه الگوها تغییر و جدید حمله روش‌ها پدیدار شدن، این مجموعه داده‌ها ممکن است شکست به فراهم کردن مربوطه آموزش داده‌ها برای IDS مدرن، که به طور بالقوه منجر به کاهش عملکرد در دنیای واقعی می‌شود برنامه های کاربردی. علاوه بر این، آنها فقدان ‎‏ ... پیچیده و متنوع حمله بردارها پیدا شد در فعلی شبکه‌ها، که هستند

در CICDDoS2019 به طور مؤثرتری نمایش داده شده است. تحقیقات قبلی رویکردهای یادگیری ماشین را با استفاده از مجموعه داده‌های NSL-KDD و KDD بررسی کرده‌اند [[19] ،](#_bookmark99) [[27] .](#_bookmark107) این مطالعات نشان می‌دهد که در حالی که بالا دقت می‌تواند باش به دست آمده، ‎‏ ... نتایج اغلب به خوبی به سناریوهای واقع‌بینانه و مدرن تعمیم داده نمی‌شوند. این نکته تأکید می‌کند ‎‏ ... نیاز برای به‌روزرسانی‌شده مجموعه داده‌ها که به چالش‌های تشخیص حملات پیچیده DDoS در محیط‌های SDN معاصر می‌پردازد. در نتیجه، این مطالعه بر روی در حال توسعه و ارزیابی کردن الف جدید مجموعه داده‌ها که دقیق تر منعکس می‌کند فعلی تهدیدها یافته‌ها نشان دهید که این مجموعه داده‌ها پیشنهادات برتر تشخیص قابلیت‌ها برای طیف گسترده‌ای از سناریوهای حمله DDoS در مقایسه با CICDDoS2019.



**شکل ۱۵.** دقت مقایسه با دیگر مطالعات.

* 1. *مقایسه روش‌های تشخیص حمله DDoS با استفاده از یادگیری ماشین در امنیت SDN*

این مطالعه ارائه می‌دهد الف قابل توجه پیشرفت در حملات انسداد سرویس (DDOS) تشخیص حمله در شبکه SDN محیط‌ها مقایسه شده به موجود مطالعات (به جدول [7 مراجعه کنید](#_bookmark78) ). برخلاف مطالعات قبلی، که اغلب فاقد شفافیت هستند و محدود کردن دسترسی به آنها مجموعه داده‌ها، الف مجموعه داده جدید است با دقت ساخته شده به شبیه‌سازی واقع‌بینانه حمله DDoS سناریوها مهم‌تر از همه، این مجموعه داده‌ها است عمومی موجود و تسهیل می‌کند شفافیت، تکرارپذیری، و همکاری در جامعه تحقیقاتی. برای مثال، موارد زیر را در نظر بگیرید مطالعه توسط جواهر و ال. [[25] ،](#_bookmark105) که به دست آمده یک دقت​ ۹۸.۵۷٪ با استفاده از یک ان. در حالی که ‎‏ ... ادغام از عمومی چندگانه مجموعه داده‌ها افزایش می‌دهد ‎‏ ... اعتبار از آنها یافته‌ها، رویکرد در این مطالعه پیشی می‌گیرد مال آنها توسط فراهم کردن الف مجموعه داده‌های سفارشی که امکان ارزیابی هدفمندتر و جامع‌تر را فراهم می‌کند از حملات انسداد سرویس (DDOS) تشخیص روش‌ها در اس دی ان. علاوه بر این، نتایج نشان داده شده برتر عملکرد در مقایسه با دیگر مطالعات. همانطور که مصور در شکل [۱۵](#_bookmark77) ، ‎‏ ... مدل‌های پیشنهادی به دست آمده یک دقت از ۹۸.۹۷٪، که است ‎‏ ... بالاترین در میان همه ‎‏ ... مقایسه شده روش‌ها. این استثنایی دقت تأکید می‌کند ‎‏ ... اثربخشی از ‎‏ ... رویکرد برای تشخیص دقیق و کاهش دهنده حملات انسداد سرویس (DDOS) حملات در شبکه SDN محیط‌ها. به دلیل به منبع محدودیت‌ها، دقیق محاسباتی معیارهای هزینه بودند نه اندازه‌گیری شده در این مطالعه کردن. آینده کار

**جدول ۷.** مقایسه با مطالعات دیگر.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

باید بر ارزیابی‌های دقیق الزامات محاسباتی تمرکز کند از اینها مدل‌ها به بهتر ارزیابی کردن آنها کاربردپذیری بلادرنگ در محیط‌های SDN. علاوه بر این، مطالعاتی مانند به عنوان آن توسط ساهو و ال. [[19]](#_bookmark99) و کجور و پاتل [[20] ،](#_bookmark100) دقت بالایی را گزارش کردند، اما محدودیت دسترسی و تنوع مجموعه داده‌های آنها می‌تواند به طور بالقوه مانع تعمیم‌پذیری و استحکام مدل‌های آنها شود. در مقابل، عمومی موجود است مجموعه داده‌ها شامل می‌شود الف پهن طیف وسیعی از سناریوهای حمله، تضمین ارزیابی و اعتبارسنجی جامع از ‎‏ ... پیشنهادی روش‌ها. علاوه بر این، بیشترین مطالعات در این زمینه به طور سنتی برای انتخاب ویژگی به PCA متکی بوده‌اند، در حالی که اتخاذ الگوریتم کای دو (Chi2) در این مطالعه است حیاتی. چی۲ این الگوریتم به طور خاص برای انتخاب ویژگی دسته‌ای طراحی شده است، و آن مناسب برای ‎‏ ... مجموعه داده‌ها، که شامل می‌شود شبکه های مختلف ترافیک صفات. برخلاف پی سی ای، که فرض می‌کند روابط خطی بین متغیرها، Chi2 مهمترین آنها را مشخص می‌کند. ویژگی‌ها مبتنی بر روی آنها استقلال از متغیر هدف، و در نتیجه ثبت بهتر روابط غیرخطی ذاتی در داده‌های ترافیک شبکه. علاوه بر این، این مطالعه به محدودیت‌های شناسایی‌شده در مطالعات قبلی، مانند فقدان جزئیات و تنوع مجموعه داده‌ها، اتکا به یک مجموعه داده واحد برای ارزیابی و شفافیت محدود، پرداخت. توسط فراهم کردن الف مفصل و عمومی مجموعه داده‌های موجود، همراه با دستیابی به استثنایی دقت در این مطالعه با هدف تشخیص DDoS، معیاری برای تحقیقات آینده در مورد امنیت SDN ایجاد می‌کند. جزئیات و مقایسه‌های بیشتر در جدول [7 ارائه شده است](#_bookmark78) که برتری و ارزش این دستاورد را در حوزه SDN برجسته می‌کند.

1. **نتیجه‌گیری**

شبکه نرم‌افزارمحور (SDN) به عنوان یک معماری فناوری متحول‌کننده با پتانسیل ایجاد انقلابی عظیم، آماده است. شبکه مدیریت. با این حال، این نوآوری چالش‌های امنیتی جدیدی را ایجاد کرده است. کنترل متمرکز ذاتی در شبکه SDN افشا می‌کند شبکه‌ها به آسیب‌پذیری‌ها، از جمله حملات انسداد سرویس (DDOS) حملات، که می‌تواند داشته باشند ویرانگر تأثیرات بر عملکرد و دسترسی‌پذیری شبکه. یافته‌های این مطالعه هستند از قابل توجه اهمیت. توسط پرداختن به امنیت چالش‌ها ذاتی در شبکه SDN محیط‌ها، این

مطالعه به پر کردن شکاف‌های اساسی در دانش و پرداختن به مسائل موجود کمک می‌کند. از طریق توسعه یک رمان مجموعه داده‌ها و جامع ارزیابی از پنج یادگیری ماشینی تکنیک‌ها، همراه با معیارسنجی علیه مجموعه داده‌های ایجاد شده مانند CICDDoS2019، بینش‌های ارزشمندی در مورد استراتژی‌های مؤثر تشخیص و کاهش DDoS در داخل شبکه SDN هستند ارائه شده است. تولید شده مجموعه داده‌ها به عنوان یک منبع ارزشمند برای ارزیابی تکنیک‌های تشخیص نفوذ عمل می‌کند. و ناهنجاری تشخیص الگوریتم‌ها در SDN. این مطالعه چندین یافته کلیدی را به همراه داشت که از اهداف آن پشتیبانی می‌کردند. یک مجموعه داده سفارشی با موفقیت توسعه داده شد برای شبیه‌سازی سناریوهای واقعی حمله DDoS، و ارائه منابع ارزشمند به محققان برای ارزیابی امنیت شبکه الگوریتم‌ها. علاوه بر این، ‎‏ ... ارزیابی از تکنیک‌های یادگیری ماشین، شامل رگرسیون لجستیک، ماشین بردار پشتیبان، جنگل تصادفی، همسایه K-نزدیک‌ترین و XGBoost، سوله ها نور روی آنها اثربخشی در طبقه‌بندی حملات DDoS در محیط‌های SDN. مقایسه با تأسیس شد مجموعه داده‌ها، چنین به عنوان CICDDoS2019، اثربخشی این رویکرد را بیشتر تأیید کرد. پیامدهای یافته‌ها گسترش دادن به دنیای واقعی برنامه های کاربردی، اطلاع رسانی فرآیندهای تصمیم‌گیری مدیران شبکه و متخصصان امنیت سایبری. این تحقیق با شناسایی استراتژی‌های مؤثر تشخیص و کاهش حملات DDoS در محیط‌های SDN، تاب‌آوری زیرساخت‌های SDN را در برابر حملات DDoS افزایش داده و عملکرد و در دسترس بودن شبکه را تضمین می‌کند. برای اذعان به اهمیت این مطالعه، آن است مهم به آدرس آن محدودیت‌ها. یکی محدودیت بالقوه، دامنه مجموعه داده‌ها است که ممکن است شامل موارد زیر نباشد: همه ‎‏ ... ممکن است حملات انسداد سرویس (DDOS) حمله سناریوها علاوه بر این، عملکرد ‎‏ ... میلی لیتر رویکردها می‌توانند باش تحت تأثیر قرار گرفته توسط عواملی مانند اندازه و ترکیب مجموعه داده‌ها..

تحقیقات آینده باید مدل‌های یادگیری عمیق، مانند شبکه‌های عصبی پیچشی (CNN) و شبکه‌های حافظه کوتاه‌مدت بلندمدت (LSTM) را بررسی کنند. این مدل‌ها می‌توانند با ثبت الگوهای پیچیده، دقت تشخیص را بیشتر افزایش دهند. و زمانی وابستگی‌ها در شبکه ترافیک. علاوه بر این، ناهنجاری تشخیص تکنیک‌ها، چنین به عنوان رمزگذارهای خودکار و جنگل‌های ایزوله، می‌توانند با یادگیری نظارت‌شده ادغام شوند مدل‌ها به شناسایی قبلاً دیده نشده حمله الگوها،

**جدول ۸.** فهرست از اختصارات

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

ارائه الف بیشتر جامع نگر رویکرد به حملات انسداد سرویس (DDOS) کاهش. کارهای آینده اراده همچنین گسترش دادن ‎‏ ... محدوده از حمله سناریوها به موارد بیشتری را شامل شود پیشرفته حملات انسداد سرویس (DDOS) بردارها، چنین به عنوان حملات تقویتی (مثلاً، دی‌ان‌اس و ان تی پی تقویت)، حملات لایه کاربرد (مثلاً، اچ‌تی‌پی سیل)، و مبتنی بر بات‌نت حملات چند برداری. این امر با تضمین پایداری مدل‌ها در سناریوهای مختلف دنیای واقعی، تعمیم‌پذیری آن‌ها را افزایش می‌دهد. یکی دیگر نویدبخش جهت شامل می‌شود تحقیق و تفحص مقیاس پذیری از تشخیص سیستم‌ها در در مقیاس بزرگ شبکه SDN محیط‌ها. تحقیق به چگونه متفاوت شبکه توپولوژی‌ها عملکرد تشخیص نفوذ می‌تواند بینش‌هایی در مورد بهینه‌سازی مکانیسم‌های دفاعی DDoS ارائه دهد. علاوه بر این، داده‌های ترافیک دنیای واقعی از منابعی مانند MAWI یا CAIDA با هم ادغام می‌شوند. اطمینان حاصل کردن که ‎‏ ... مدل‌ها هستند آموزش دیده و اعتبارسنجی شده تحت پخش زنده شبکه شرایط، بیشتر ارتقاء دهنده آنها قابلیت کاربرد در استقرارهای عملی. برای تقویت بیشتر این جنبه، هدف ما همکاری با شرکای صنعتی برای دسترسی به SDN واقعی است. ترافیک، فراهم کردن بحرانی بینش‌ها به ‎‏ ... عملیاتی

عملکرد چارچوب ما و شناسایی چالش‌های استقرار.

در نهایت، بررسی ادغام چارچوب‌های تشخیص ترکیبی که ترکیب کردن مبتنی بر امضا تشخیص با تکنیک‌های یادگیری ماشین می‌توانند استراتژی‌های دفاعی قوی در زمان واقعی ارائه دهند. در حال تعقیب اینها راه‌ها، آینده مطالعات می‌تواند به پیشبرد امنیت SDN ادامه دهید و اطمینان حاصل کنید که شبکه‌ها در برابر تهدیدات DDoS در حال تحول مقاوم باقی می‌مانند.

**پیوست**

جدول [۸](#_bookmark80) برای اختصارات استفاده شده در این مطالعه، منابعی ارائه می‌دهد.

**منابع**

1. وی. بالاسوبرامانیان، ام. آلوگایلی، و ام. ریسلین، «معماری SDN» برای اینترنت اشیا صنعتی حساس به زمان، « *شبکه محاسبات»* ، جلد ۱۸۶، فوریه ۲۰۲۱، شماره ماده ۱۰۷۷۳۹.
2. م. کاراکوس و ا. دورسی، «یک بررسی: مسائل مربوط به مقیاس‌پذیری صفحه کنترل» و رویکردهای موجود در شبکه‌سازی تعریف‌شده توسط نرم‌افزار (SDN)، « *شبکه محاسباتی »* ، جلد 112، صفحات 279-293، ژانویه 2017.
3. الف. ابوعرقوب، «الف» بررسی از ‎‏ ... کنترل هواپیما مقیاس‌پذیری رویکردها در شبکه‌سازی تعریف‌شده توسط نرم‌افزار، « *اینترنت آینده »* ، جلد ۱۲، شماره ۳، ص. ۴۹، مارس ۲۰۲۰. (۲۰۲۰)
4. جی. میگل-آلونسو، «بررسی پژوهشی OpenFlow برای مراکز داده» «شبکه‌سازی»، *IEEE Access* ، جلد ۱۱، صفحات ۷۷۰-۷۸۶، ۲۰۲۳.
5. الف. اس آر، ک. مهادف، س. پراساد، س. اسواران، و پ. هوناوالی، «روز درهای باز» نور به عنوان نرم‌افزار تعریف شده شبکه سازی کنترل کننده: کاستی‌ها و ممکن است راه حل ها،'' در *مجموعه مقالات IEEE بین المللی کنفرانس الکترون.، محاسبه. ارتباطات فناوری (CONECCT)* ، ژوئیه ۲۰۲۲، صفحات ۱ تا ۶.
6. ز. الف. بوییان، س. اسلام، م. م. اسلام، الف. ب. م. الف. الله، ف. ناز، و م. س. رحمان، «درباره (عدم)امنیت صفحه کنترل SDN» معماری: یک بررسی، « *IEEE Access* »، جلد ۱۱، صفحات ۹۱۵۵۰–۹۱۵۸۲، ۲۰۲۳.
7. S. Khorsandroo, AG Sánchez, AS Tosun, J. Arco, and R. Doriguzzi- کورین، «تکامل SDN هیبریدی: بررسی جامع وضعیت...» «هنر»، « *مجله محاسبات»* ، جلد ۱۹۲، ژوئن ۲۰۲۱، شماره ماده ۱۰۷۹۸۱.
8. AL Aliyu، A. Aneiba، M. Patwary، و P. Bull، "مدیریت اعتماد چارچوبی برای کنترل‌کننده و شبکه مبتنی بر نرم‌افزار (SDN) «کاربردها»، « *مجله محاسبات شبکه»* ، جلد ۱۸۱، نوامبر ۲۰۲۰، شماره ماده ۱۰۷۴۲۱.
9. اسلام، ن. اسلام و رفعت، «عملکرد گره به گره» ارزیابی از طریق ریو شبکه SDN کنترل کننده، *بی‌سیم پرس. ارتباطات* . جلد ۱۱۲، شماره ۱، صفحات ۵۵۵-۵۷۰، مه ۲۰۲۰.
10. اچ. لکینگ، چگونه به متوجه شدن ‎‏ ... صاف گذار از سنتی شبکه معماری به اس‌دی‌ان، در *مجموعه مقالات پنجم بین المللی کنفرانس مکانیک.، کنترل محاسبه. مهندس (ICMCCE)* ، دسامبر ۲۰۲۰، صفحات ۱۹۴۸–۱۹۵۲.
11. H. Facchini, S. Perez, R. Blanchet, B. Roberti, and R. Azcarate, ''Exper- تفاوت عملکرد ذهنی بین SDN و شبکه‌های سنتی، در *مجموعه مقالات IEEE شیلی، کنفرانس برق، مهندسی الکترون، فناوری اطلاعات و ارتباطات (شیلیکن)* ، دسامبر 2021، صفحات 1-6.
12. 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.
13. آر. کی. باچو و اچ. سیتا، «درباره بهبود عملکرد حملات DDoS» حمله تشخیص سیستم،'' *ریزپردازنده‌ها میکروسیستم* . جلد ۹۳، سپتامبر ۲۰۲۲، شماره ماده ۱۰۴۵۷۱.
14. اچ. س. عبدالکریم و الف. داوود، حملات منع سرویس توزیع‌شده (DDoS) حمله تشخیص و کاهش در لایه صفحه داده SDN، در *مجموعه مقالات دومین کنفرانس جهانی برق، ارتباطات انرژی. کنفرانس (GPECOM)* ، اکتبر ۲۰۲۰، صفحات ۳۲۲-۳۲۶.
15. ک.-ی. چن، س. لیو، ی. خو، من. ک. سیدراو، س. ژو، ز. گو، و اچ. جی. چائو، SDNShield: چارچوب دفاعی مبتنی بر NFV در برابر حملات DDoS به ... صفحه کنترل SDN، « *شبکه انتقال IEEE/ACM»* ، جلد 30، شماره 1، صفحات ... ۱–۱۷، فوریه ۲۰۲۲.
16. ل. ف. الیان و آر. دی پیترو، «داس» و حملات انسداد سرویس (DDOS) حملات در نرم‌افزار تعریف شده شبکه‌ها: الف نظرسنجی از موجود راه حل ها و تحقیق چالش‌ها،'' *آینده عمومی. محاسبات. سیستم.* ، جلد. ۱۲۲، صفحات. ۱۴۹–۱۷۱، سپتامبر ۲۰۲۱.
17. م. رواتی، وی. وی. رامالینگام، و ب. آموتا، «الف» دستگاه یادگیری مبتنی بر تشخیص و کاهش حمله DDOS با استفاده از کنترل‌کننده SDN چارچوب، « *ارتباطات بی‌سیم پرس.»* ، جلد ۱۲۷، شماره ۳، صفحات. ۲۴۱۷–۲۴۴۱، دسامبر ۲۰۲۲.
18. الف. هیرسی، ل. عوده، و الف. صالح، SDN-DDoS مجموعه داده‌های ترافیکی، مندلی داده‌ها، جلد ۱، ۲۰۲۴، doi: [10.17632/b7vw628825.1.](http://dx.doi.org/10.17632/b7vw628825.1) [آنلاین]. موجود است: https://data.mendeley.com/datasets/b7vw628825/1
19. ک. س. ساهو، ب. ک. سه‌پاتی، ک. نایک، س. راماسوباردی ب. بالوسامی،

م. خاری، و د. بورگوس، «یک مدل SVM تکاملی برای DDOS» حمله تشخیص در نرم‌افزار تعریف شده شبکه‌ها، *IEEE دسترسی* ، جلد ۸،

ص. ۱۳۲۵۰۲–۱۳۲۵۱۳، ۲۰۲۰. (۲۰۲۰)

1. پ. کجور و س. پاتل، مقایسه از مختلف میلی لیتر رویکردها برای تشخیص از حملات DDoS در SDN، در *پانزدهمین کنفرانس بین‌المللی کامپیوتر و اطلاعات Proc. IEEE. شبکه ارتباطات (CICN)* ، دسامبر 2023، صفحات 245-249.
2. B. Isyaku, KBA Bakar, MS Ali, and MN Yusuf, ''Performance مقایسه طبقه‌بندی‌کننده‌های یادگیری ماشین برای تشخیص DDoS و کاهش آسیب‌پذیری در شبکه‌های نرم‌افزار محور، در *مجموعه مقالات کنفرانس بین‌المللی IEEE. خودکار. اینتل را کنترل کنید سیستم (I2CACIS)* ، ژوئن 2023، صفحات 69-74.
3. اُ. رحمان، م. الف. جی. قریشی، و سی.-اچ. ریه، حملات منع سرویس توزیع‌شده (DDoS) حملات تشخیص و کاهش خطرات در SDN با استفاده از یادگیری ماشین، در *مجموعه مقالات IEEE World کنگره خدمات (خدمات)* ، جلد ۲۶۴۲، ژوئیه ۲۰۱۹، صفحات ۱۸۴-۱۸۹.
4. م. م. رایکار، م. م. ملا، م. م. ملا، ن. س. شتی، و م. کارناندی، طبقه‌بندی ترافیک داده‌ها در شبکه‌های نرم‌افزار محور (SDN) با استفاده از یادگیری تحت نظارت *مجموعه مقالات محاسبه. علمی* ، جلد ۱۷۱، ص. ۲۷۵۰–۲۷۵۹، جان ۲۰۲۰. (۲۰۲۰)
5. N. Ashodia and K. Makadiya، "تشخیص حملات DDoS در SDN با استفاده از یادگیری ماشینی، در *مجموعه مقالات کنفرانس بین‌المللی الکترون. تجدید. سیستم (ICEARS)* ، مارس ۲۰۲۲، صفحات ۱۳۲۲-۱۳۲۷.
6. الف. جواهر، پ. کایتری، وی. سی. کومار، آر. وینو، آر. امریش، ک. باواپریان، و وی. گوپینات، حملات منع سرویس توزیع‌شده (DDoS) کاهش با استفاده از بلاکچین و دستگاه یاد بگیرید- ینگ تکنیک‌ها، *چندرسانه‌ای ابزارها کاربردی* ، جلد ۸۳، نه. ۲۱، ص. ۶۰۲۶۵–۶۰۲۷۸، جان ۲۰۲۴.
7. جی. الف. پرز-دیاز، من. الف. والدوینوس، ک. آر. چو، و دی. ژو، «الف» انعطاف‌پذیر مبتنی بر SDN معماری برای شناسایی و کاهش دهنده کم- نرخ حملات انسداد سرویس (DDOS) حملات با استفاده از دستگاه یادگیری،'' *IEEE دسترسی* ، جلد ۸،

ص. ۱۵۵۸۵۹–۱۵۵۸۷۲، ۲۰۲۰. (۲۰۲۰)

1. 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.
2. الف. صاحبی، ف. جایدی، و ا. بوحولا، «الگوریتم‌های یادگیری ماشین برای» بهبود تشخیص نفوذ در SDN/NFV، در *Proc. Int. Wireless ارتباطات. محاسبات سیار. (IWCMC)* ، ژوئن ۲۰۲۳، صفحات ۶۰۲-۶۰۷.
3. 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. یو. اچ. گاربا، الف. ن. طوسی، م. ف. پاشا، و س. خان، مبتنی بر SDN تشخیص و کاهش حملات DDoS به خانه‌های هوشمند، « *ارتباطات کامپیوتری »* ، جلد ۲۲۱، صفحات ۲۹-۴۱، مه ۲۰۲۴.
2. دبلیو آی خدر، ای ای گودا، و ای آر محمد، «FMDADM: یک... چارچوب تشخیص و کاهش حمله DDoS لایه‌ای با استفاده از ماشین یادگیری برای دولتی مبتنی بر SDN اینترنت اشیا شبکه‌ها، *IEEE دسترسی* ، جلد ۱۱،

ص. ۲۸۹۳۴–۲۸۹۵۴، ۲۰۲۳.

1. J. Bhayo، SA شاه، S. Hameed، A. Ahmed، J. Nasir، و D. Draheim، ''به سوی الف دستگاه مبتنی بر یادگیری چارچوب برای حملات منع سرویس دابلیو‌اس حمله تشخیص در شبکه‌های اینترنت اشیا تعریف‌شده توسط نرم‌افزار (SD-IoT)، *مهندس، برنامه کاربردی، هوش* مصنوعی جلد 123، آگوست 2023، هنر. نه 106432.
2. GO Anyanwu، CI Nwakanma، J.-M. لی، و D.-S. کیم، RBF- مدل مبتنی بر هسته SVM برای تشخیص حملات DDoS در شبکه نرم‌افزار محور یکپارچه «شبکه خودرویی»، « *شبکه موردی»* ، جلد ۱۴۰، مارس ۲۰۲۳، شماره ماده ۱۰۳۰۲۶.
3. ای. سبار و کی. زیک، «افزایش تاب‌آوری در برابر حملات DDoS در شبکه‌های زنجیره تأمین مبتنی بر SDN با استفاده از یادگیری ماشینی، در *مجموعه مقالات نهم بین المللی Conf. کنترل، تصمیم گیری Inf. تکنولوژی (CoDIT)* ، ژوئیه 2023، صفحات 230-234.
4. ب. سوبا، س. بیسواس، و س. کارماکار، ''نفوذ'' تشخیص سیستم‌ها با استفاده از خطی تبعیض آمیز تحلیل و لجستیک رگرسیون، در *مجموعه مقالات آنو. IEEE هند Conf. (INDICON)* ، دسامبر 2015، صفحات 1-6.
5. ز. اکرم، م. مجید، و س. حبیب، «الف» سیستماتیک ادبیات بررسی: کاربرد «رگرسیون لجستیک برای تشخیص بدافزار»، در *مجموعه مقالات کنفرانس بین‌المللی نوآوری. محاسبه کنید. (ICIC)* ، نوامبر 2021، صفحات 1-8.
6. س. یاداو و س. سلواکومار، تشخیص از کاربرد لایه حملات انسداد سرویس (DDOS) حمله با مدل‌سازی رفتار کاربر با استفاده از رگرسیون لجستیک، در *مجموعه مقالات چهارمین دوره بین‌المللی. کنفرانس نسبی.، اینفوکام فناوری بهینه سازی. (ایکریتو) (روندها آینده دستورالعمل‌ها)* ، سپتامبر ۲۰۱۵، صفحات ۱ تا ۶.
7. ز. لانگ و دبلیو. جینسونگ، «یک روش ترکیبی آنتروپی و SSAE-SVM» مکانیزم تشخیص و کاهش حملات DDoS مبتنی بر SDN، " *محاسبات". سکیور* ، جلد ۱۱۵، آوریل ۲۰۲۲، ماده ۱۰۲۶۰۴.
8. وی. سونای و آی. بهاراتی، «طبقه‌بندی بسته‌ها با استفاده از الگوریتم تصادفی بهبود یافته» الگوریتم جنگل، در *مجموعه مقالات کنفرانس بین‌المللی ماشین یادگیری، یادگیری عمیق. محاسبه. هوش. بی‌سیم ارتباطات* چم، سوئیس: اسپرینگر، ۲۰۲۳،

ص. ۱۵۷–۱۶۸.

1. وای. چن، جی. هو، کیو. لی، و اچ. لانگ، «تشخیص حمله DDoS مبتنی بر جنگل تصادفی، در *مجموعه مقالات IEEE Int. Conf. Prog. Informat. Comput. (PIC)* ، سپتامبر ۲۰۲۰، صفحات ۳۲۸-۳۳۴.
2. س. دونگ و م. صارم، حملات منع سرویس توزیع‌شده (DDoS) حمله تشخیص مبتنی بر روش روی بهبود یافته کی ان ان با ‎‏ ... مدرک از حملات انسداد سرویس (DDOS) حمله در نرم‌افزار محور شبکه‌ها، *IEEE* *اکسس* ، جلد ۸، صفحات ۵۰۳۹–۵۰۴۸، ۲۰۲۰.
3. س. کومار، جی. بانسال، و وی. س. شیخاوات، «الف» دستگاه یادگیری رویکرد برای تأمین جریان ترافیک در شبکه‌های نرم‌افزار محور،» در *مجموعه مقالات بین‌المللی.* *کنفرانس اطلاعات شبکه (ICOIN)* ، ژانویه ۲۰۲۰، صفحات ۶۰۲-۶۰۷.
4. ای. زین‌الدین، لاک آهاکونیه، آر. اکتر، دی.-اس. کیم، و جی.-ام. لی، یک شبکه عصبی عمیق ترکیبی کارآمد برای تشخیص و طبقه‌بندی DDoS در نرم‌افزار محور اینترنت اشیا صنعتی شبکه‌ها، *IEEE اینترنت چیزها جی* .، جلد ۱۰، نه. ۱۰،

ص. ۸۴۹۱–۸۵۰۴، مه ۲۰۲۳.

1. اچ. ای. آلمری و وی. تایانانتان، «تحلیل یادگیری ماشینی برای» ایمن سازی نرم‌افزار محور شبکه‌سازی،'' *مجموعه مقالات محاسبه. علمی* ، جلد ۱۹۴،

ص. ۲۲۹–۲۳۶، جان ۲۰۲۱. (یا: ۲۰۲۱)

1. A. Abhishta، R. Joosten، S. Dragomiretskiy، و L. جی. م. نیوون‌هویس، «تأثیر حملات موفق DDoS بر یک ارز دیجیتال بزرگ» «مبادله»، در *مجموعه مقالات بیست و هفتمین کنفرانس بین‌المللی یورومیکرو، موازی، توزیع شبکه‌ای* *فرآیند مبتنی بر (PDP)* ، فوریه ۲۰۱۹، صفحات ۳۷۹-۳۸۴.
2. اس. بهاردواج و اس. ان. پاندا، «ارزیابی عملکرد با استفاده از RYU SDN» کنترل‌کننده در محیط شبکه تعریف‌شده توسط نرم‌افزار، « *پرسش‌های بی‌سیم».* *اشتراک.* ، جلد 122، شماره 1، صفحات 701-723، ژانویه 2022.
3. D. Dholakiya، T. Kshirsagar، و A. نایاک، «بررسی چالش‌های مینی‌نت»، فرصت‌ها، و کاربرد در نرم‌افزار محور شبکه (SDN) *مجموعه مقالات* *کنفرانس بین‌المللی، ارتباطات، فناوری، سیستم اطلاعاتی* ، جلد ۲، ۲۰۲۱، صفحات ۲۱۳–۲۲۱.
4. ز. آر. ساپوترا السی، دی. استیاوان، الف. ف. اوکلیلاس، ک. سوسانتو، وای. ان. کونانگ، م.

ی. ادریس، و ر. بودیارتو، «انتخاب ویژگی با استفاده از مربع کای برای بهبود» حمله تشخیص طبقه بندی در اینترنت اشیا شبکه: کار در پیشرفت،'' در *مجموعه مقالات نهم بین المللی کنفرانس برق مهندس، محاسبه. علمی اطلاعات (EECSI)* ، اکتبر ۲۰۲۲،

ص. ۲۲۶–۲۳۲.

1. من. شرفالدین، الف. اچ. لشکری، س. حکاک، و الف. الف. قربانی، ''در حال توسعه'' مجموعه داده و طبقه‌بندی حمله انکار سرویس توزیع‌شده (DDoS) واقع‌بینانه «اومی»، در *کنفرانس بین‌المللی فناوری امنیت کارنهان (ICCST)* ، اکتبر ۲۰۱۹،

ص. ۱–۸.

عبدیناسیر هیرسی (فارغ التحصیل دانشجو عضو، IEEE) مدرک کارشناسی خود را در رشته مخابرات دریافت کرد. مهندسی کاتیون از محمد علی جناح دانشگاه (MAJU)، کراچی، پاکستان، در سال 2019، و مدرک کارشناسی ارشد مهندسی برق، متخصص در مهندسی ارتباطات از دانشگاه بحریا، کراچی، در سال 2021. او تحصیل کرده است به صورت اجاره‌ای در حال تعقیب ‎‏ ... دکترا مدرک در الکتریکی مهندسی- نیرنگ با دانشگاه تون حسین اون مالزی (UTHM)، جوهور، مالزی. او است فعلاً الف

فارغ التحصیل تحقیق دستیار (GRA) با ‎‏ ... پیشرفت مخابرات مرکز تحقیقات (ATRC)، FKEE، UTHM. علایق تحقیقاتی او عبارتند از: امنیت شبکه تعریف‌شده توسط نرم‌افزار (SDN)، تشخیص حمله DDoS و کاهش، امنیت سایبری، و هوش مصنوعی تکنیک‌ها، چنین به عنوان دستگاه یادگیری و تکنیک‌های یادگیری عمیق برای تشخیص نفوذ در شبکه

LUKMAN AUDAH (عضو، IEEE) دریافت کرد مدرک لیسانس مهندسی در رشته مخابرات ارتباطات از دانشگاه فناوری مالزی، در سال ۲۰۰۵، و مدرک کارشناسی ارشد در رشته ارتباطات شبکه‌ها و نرم‌افزار و مدرک دکترا در رشته مهندسی الکترونیک از دانشگاه ساری، انگلستان. او در حال حاضر مدرس ارشد است. با دپارتمان مهندسی ارتباطات- دانشگاه تون حسین اون مالزی. او تحقیق علایق شامل شدن بی‌سیم و موبایل

ارتباطات، اینترنت ترافیک مهندسی، شبکه سیستم مدیریت، امنیت داده‌ها و ارتباطات ماهواره‌ای

محمد الف. الهارتومی (عضو،

IEEE) مدرک دکترا در رشته الکترونیک دریافت کرد. و الکتریکی مهندسی از لیدز دانشگاه، بریتانیا، در ۲۰۱۶. او است فعلاً یک دستیار متخصصان- با دانشکده مهندسی برق، دانشگاه از تبوک. او تحقیق علایق شامل شدن ارتباطات بی‌سیم و سیار، سیگنال پردازش، طراحی سیستم‌های بی‌سیم نوری، و ارتباطات نور مرئی.

ADEB SALH (عضو، IEEE) این جایزه را دریافت کرد. لیسانس برق و الکترونیک مهندسی از آی بی بی دانشگاه، یمن، در ۲۰۰۷، و مدارک کارشناسی ارشد و دکتری در رشته برق و مهندسی الکترونیک از دانشگاه تون حسین اون مالزی، در ۲۰۱۵ و ۲۰۲۰، احترام- از سال ۲۰۰۷ تا ۲۰۱۲، او مدرس بود. دستیار کالج محلی یاریم. از سال ۲۰۲۰ تا ۲۰۲۳، او دانشجوی فوق دکترا بود. محقق با یوتم و یو تی ام، به ترتیب.

در حال حاضر، او استادیار دانشکده اطلاعات و ... است. فناوری ارتباطات، دانشگاه تونکو عبدالرحمن. تحقیقات او علایق شامل ارتباطات بی‌سیم 5G، 6G، MIMO گسترده، هوش مصنوعی هوش مصنوعی (AI) و اینترنت اشیا (IoT).

سلمان احمد (دانشجوی کارشناسی ارشد عضو، IEEE) مدرک لیسانس خود را در رشته برق دریافت کرد. ترونیک مهندسی از ‎‏ ... مهران دانشگاه از مهندسی و فناوری جامشورو، پاکستان، در سال ۲۰۱۵، و مدرک کارشناسی ارشد مهندسی در صنعتی اتوماسیون و کنترل از ‎‏ ... کوئید دانشگاه علوم و فناوری عوام نوابشاه، پاکستان، در سال ۲۰۲۱. او در حال حاضر ادامه تحصیل در مقطع دکترا با دانشکده برق و الکترونیک مهندسی، دانشگاه

تون حسین، مالزی (UTHM). او در حال حاضر دانشجوی کارشناسی ارشد و پژوهشگر است. دستیار (GRA) با ‎‏ ... دانشکده از برق و الکترونیک مهندسی، UTHM. او مدرس مهندسی الکترونیک در Sukkur IBA بود. دانشگاه، پاکستان، از سال ۲۰۱۷ تا ۲۰۲۲. علایق پژوهشی او عبارتند از: امنیت شبکه، رمزنگاری و اینترنت اشیا با محدودیت منابع دستگاه‌ها.