Journal of Applied And Basic Machine Intelligence Research (ABMIR)

پژوهش‌های نظری و کاربردی هوش ماشینی

سال دوم، شماره اول، بهار و تابستان ۱۴۰۳، صفحات۳۸-۱۴

کاربرد شبکه‌های عصبی «حافظه بلندمدت-کوتاه‌مدت» و «پیچشی» برای شناسایی حملات ممانعت از سرویس توزیع‌شده

سید مجتبی متین خواه [۱*]، علی خاک‌باز [۲]، فضل اله ادیب نیا [۳]

[۱]استادیار دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران

[۲]دانشجوی کارشناسی ارشد دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران

[۳]دانشیار دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران

چکیده

مقاله پژوهشی

یادگیری عمیق به دلیل توانایی در تجزیه‌وتحلیل الگوهای پیچیده ترافیک شبکه باقابلیت پاسخ‌های خودکار بلادرنگ، ابزار مهمی برای تشخیص حمله ممانعت از سرویس توزیع‌شده است. ولی در اینجا مسئله اصلی نوظهور بودن آن است که باعث شده بررسی کامل فرصت‌ها و چالش‌ها در این زمینه با پیاده‌سازی‌های واقعی یا نمونه داده‌های محک انجام‌نشده باشد. در این مقاله دو روش تشخیص حمله ممانعت از سرویس به‌وسیله یادگیری عمیق LSTM و CNN و همچنین روش پیشنهادی جدیدی با ترکیب آن‌ها معرفی می‌شود. نتایج نشان می‌دهد که هر دو روش LSTM و LSTM-CNN به‌طور مداوم ازنظر درستی، دقت، بازیابی و امتیازات F1 بهتر از CNN عمل می‌کنند. بررسی‌های ما نشان داد که CNN می‌تواند به‌طور خودکار ویژگی‌هایی مانند اندازه بسته، زمان، و آدرس‌های منبع/مقصد را از ترافیک خام شبکه یاد بگیرد؛ از سوی دیگر، LSTM به‌ویژه برای تشخیص الگوهای توالی زمانی حملات در ترافیک شبکه مفید است. از طرف دیگر انتخاب بین استفاده از CNN یا LSTM برای تشخیص DDoS به ویژگی‌های خاص مجموعه داده حمله، و اهمیت نسبی ویژگی‌های مکانی و زمانی در شناسایی حملات DDoS بستگی دارد. درنهایت، چالش‌هایی مثل بیش‌برازش، پیچیدگی رایانشی، تفسیرپذیری، محدودیت‌های داده و حملات خصمانه بررسی می‌شود و دلیل تردیدها در گزارش نتایج مقالات می‌تواند به مشکلات مجموعه داده محک مورداستفاده مانند عدم کیفیت نمونه‌ها بر اساس اندازه و تنوع محدود، عدم برچسب‌گذاری، داده‌های نامتعادل، نسبت داده شود.

تاریخ دریافت:
۱۴۰۱/۱۲/۰۵
تاریخ پذیرش:
۱۴۰۲/۶/۱۸

کلیدواژه‌ها:
یادگیری ماشین، یادگیری عمیق، CNN، DDoS, LSTM, RNN.

نویسنده‌مسئول:
matinkhah@yazd.ac.ir

: 10.22034/ABMIR.2023.19764.1025

E-ISSN: 2821-2037

۱- مقدمه

تشخیص حمله «ممانعت از سرویس توزیع‌شده»[1] شامل شناسایی و کاهش حملاتی است که هدف آن غلبه بر سیستم یا شبکه هدف با سیلی از ترافیک از چندین منبع است. حملات ممانعت از سرویس توزیع‌شده تلاش‌های مخربی برای برهم زدن عملکرد عادی یک شبکه رایانه‌ای، سرویس یا وب‌سایت با غلبه بر آن با سیل ترافیک نامشروع است. هدف از حمله ممانعت از سرویس توزیع‌شده این است که منابع سیستم یا شبکه مورد هدف (مانند پهنای باند، قدرت پردازش یا حافظه) را تمام کند و سرویس را برای کاربران عادی غیرقابل‌دسترس کند. انواع مختلفی از حملات ممانعت از سرویس توزیع‌شده وجود دارد. مانند حملات حجمی که هدف آن مصرف پهنای باند شبکه است، حملات پروتکل TCP/IP، که از آسیب‌پذیری‌ها در پروتکل‌های شبکه سوءاستفاده می‌کنند و حملات لایه برنامه، که برنامه‌ها یا خدمات خاصی را هدف قرار می‌دهند. مهاجمان به‌طور مداوم فن‌های خود را برای دور زدن اقدامات شناسایی و کاهش توسعه می‌دهند و حملات ممانعت از سرویس توزیع‌شده را به چالشی دائمی برای متخصصان امنیت سایبری تبدیل می‌کنند.

برای شناسایی و کاهش حملات ممانعت از سرویس توزیع‌شده، روش‌های مختلفی ازجمله الگوریتم‌های یادگیری ماشین مانند LSTM (حافظه کوتاه‌مدت-بلندمدت)[2] و CNN (شبکه عصبی پیچشی)[3] استفاده می‌شود. این الگوریتم‌ها الگوهای ترافیک شبکه را تجزیه‌وتحلیل می‌کنند، ناهنجاری‌ها را شناسایی می‌کنند و آن‌ها را به‌عنوان حملات احتمالی طبقه‌بندی می‌کنند. مدل‌های یادگیری عمیق، ازجمله حافظه کوتاه‌مدت-بلندمدت و شبکه عصبی پیچشی، می‌توانند در شناسایی حملات تجربه‌نشده نیز مؤثر باشند، که این به‌ویژه با چشم‌انداز سریعاً در حال تحول حملات سایبری که مهاجمان دائماً درحال‌توسعه تاکتیک‌ها و تکنیک‌های جدید هستند، بسیار ارزشمند است. علاوه بر این، مدل‌های یادگیری عمیق می‌توانند به‌طور خودکار استخراج ویژگی‌های مرتبط از داده‌های ورودی را بیاموزند و نیاز به مهندسی ویژگی‌های دستی را کاهش دهند و عملکرد کلی مدل را بهبود بخشند.

استفاده از یادگیری ماشین برای شناسایی و کاهش حملات ممانعت از سرویس توزیع‌شده با چالش‌ها و معایبی همراه است. الگوریتم‌های یادگیری ماشین مثل حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی قدرتمند هستند، اما نیاز به به‌روزرسانی مداوم برای مقابله با حملات در حال تکامل دارند و تشخیص دقیق تمام انواع حملات را دشوار می‌کنند. بیش‌برازش، پیچیدگی مدل‌ها و مشکلات تفسیری نیز ممکن است مواردی باشند که باعث محدودیت استفاده از این مدل‌ها در برخی موارد می‌شوند. ترکیب حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی نیز چالش‌های خود را دارد و نیاز به تلاش و تحقیقات بیشتر برای ادغام مؤثر آن‌ها و سازگاری مناسب دارد. درنهایت، پیچیدگی مدل ترکیبی می‌تواند فرآیند آموزش و بهینه‌سازی آن را مشکل‌تر کند و شفافیت نتایج را کاهش دهد.

همچنین مجموعه داده‌های حمله ممانعت از سرویس توزیع‌شده می‌تواند دارای معایب و چالش‌هایی باشد که بر اثربخشی مدل‌های یادگیری ماشین تأثیر می‌گذارد. اندازه و تنوع محدود، فقدان برچسب‌گذاری، داده‌های نامتعادل، نگرانی‌های مربوط به حریم خصوصی داده‌ها، و کیفیت داده‌های متفاوت برخی از مسائلی هستند که می‌توانند بر عملکرد مدل‌های آموزش‌دیده‌شده در چنین مجموعه‌های داده تأثیر بگذارند.

در این مقاله، برای نخستین بار مروری بر کاربردهای ترکیب شبکه عصبی پیچشی و حافظه بلندمدت-کوتاه‌مدت برای مقابله با حملات ممانعت از سرویس در سناریوها و محیط‌های مختلف ارائه می‌شود. همچنین روشی جدید با ترکیب دو معماری ذکرشده، پیاده می‌شود و نتایج آن موردبررسی قرار می‌گیرد.

در ادامه، در فصل ۲ روش‌های ترکیب شبکه عصبی پیچشی و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت بررسی خواهد شد. در فصل ۳، بعضی مجموعه داده‌های محک و مزایا و معایب آن‌ها

[1] Distributed Denial of Service
[2] Long Short-Term Memory
[3] Convolutional Neural Network

موردبررسی قرار می‌گیرد. در فصل ٤، تهدیداتی که با استفاده از حمله ممانعت از سرویس در محیط‌های مختلف ایجاد می‌شود موردبررسی قرار می‌گیرد و در فصل ۵ انتقادات وارده به شبکه‌های عصبی و چالش‌های کاربرد این شبکه‌ها موردبحث قرار می‌گیرد. در فصل ٦، روش‌هایی بر اساس شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و حافظه عصبی پیچشی و همچنین روشی ترکیبی بر روی مجموعه داده UNSW-NB15 پیاده‌سازی می‌شود و نتایج حاصل از این روش‌ها بررسی می‌شود و درنهایت در فصل ۷، خلاصه‌ای از مطالب ارائه خواهد شد.

۱-۱ شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی

شبکه‌های عصبی مصنوعی[1] «حافظه بلندمدت-کوتاه‌مدت» و «پیچشی» نوعی از شبکه‌های عصبی هستند که در یادگیری عمیق استفاده می‌شوند، اما معماری‌های متفاوتی دارند و برای انواع مختلف داده‌ها طراحی‌شده‌اند. شبکه عصبی «حافظه بلندمدت-کوتاه‌مدت» نوعی معماری شبکه عصبی است که معمولاً در یادگیری عمیق برای کارهایی که شامل داده‌های متوالی (دارای ترتیب) هستند، مانند پردازش زبان طبیعی، تشخیص گفتار و پیش‌بینی سری‌های زمانی استفاده می‌شود. شبکه عصبی حافظه بلندمدت-کوتاه‌مدت برای حل مسئلهٔ گرادیان محوشونده[2] که می‌تواند در شبکه‌های عصبی بازگشتی[3] رخ دهد، طراحی‌شده است و به آن امکان می‌دهد وابستگی‌های بلندمدت در داده‌ها را بیاموزد. شبکه عصبی حافظه بلندمدت-کوتاه‌مدت به دلیل توانایی‌اش درگرفتن الگوهای کوتاه‌مدت و بلندمدت در داده‌ها به یک انتخاب مناسب برای بسیاری از برنامه‌های کاربردی یادگیری عمیق (که شامل داده‌های متوالی است) تبدیل‌شده است. سازوکار این روش با استفاده از سلول‌های حافظه انجام می‌شود که می‌تواند اطلاعات را برای مدت طولانی ذخیره کند و به‌طور انتخابی اطلاعات را بر اساس سیگنال‌های ورودی فراموش کند یا به خاطر بسپارد.

شبکه عصبی پیچشی نوعی معماری شبکه عصبی است که معمولاً در یادگیری عمیق برای تشخیص تصویر و ویدئو استفاده می‌شود. شبکه‌های عصبی پیچشی برای شناسایی و استخراج خودکار ویژگی‌ها از تصاویر با اعمال یک سری پالایه‌های پیچشی بر روی تصویر ورودی طراحی‌شده‌اند که به آن‌ها امکان می‌دهد الگوهای موجود در داده‌های تصویر را یاد بگیرند و شناسایی کنند. خروجی لایه‌های پیچشی معمولاً از طریق یک سری لایه‌های کاملاً متصل منتقل می‌شود که وظایف طبقه‌بندی یا رگرسیون را بر اساس ویژگی‌های استخراج‌شده انجام می‌دهند. وقتی صحبت از مقایسه شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی می‌شود، باید چند تفاوت کلیدی را در نظر گرفت:

۱- **نوع داده**: شبکه عصبی حافظه بلندمدت-کوتاه‌مدت برای داده‌های متوالی طراحی‌شده است، درحالی‌که شبکه عصبی پیچشی برای داده‌های هم‌زمان مثل داده‌های تصویری و ویدئویی طراحی‌شده است. بعداً در بررسی ترافیک شبکه خاطرنشان خواهیم کرد که پارامترهایی مثل بررسی مشخصات و محتوای بسته‌های شبکه با شبکه عصبی پیچشی بهتر عمل می‌کند؛ ولی بااین‌وجود بررسی توالی دریافت و ارسال بسته‌های ترافیکی توسط پروتکل‌های شبکه با شبکه عصبی حافظه بلندمدت-کوتاه‌مدت مناسب‌تر است.

۲- **معماری**: شبکه عصبی حافظه بلندمدت-کوتاه‌مدت نوعی شبکه عصبی بازگشتی است که برای ثبت وابستگی‌های طولانی‌مدت در داده‌ها طراحی‌شده است، درحالی‌که شبکه عصبی پیچشی نوعی شبکه عصبی پیش‌خورند[4] است که برای شناسایی و استخراج خودکار ویژگی‌ها از داده‌های هم‌زمان (و نه متوالی) طراحی‌شده است.

۳- **عملکرد**: هر دو شبکه عصبی «حافظه بلندمدت-کوتاه‌مدت» و «پیچشی» برای وظایف مربوطه خود بسیار مؤثر هستند. شبکه عصبی حافظه بلندمدت-کوتاه‌مدت به‌طور ویژه برای کارهایی که شامل داده‌های سری زمانی است مفید است، درحالی‌که شبکه

[1] Artificial Neural Network
[2] Vanishing Gradient Problem
[3] Recurrent Neural Networks
[4] Feedforward Neural Network

عصبی پیچشی به‌طور ویژه برای کارهایی که شامل داده‌های تصویری و ویدئویی است مفید است.

٤- آموزش: آموزش شبکه عصبی حافظه بلندمدت-کوتاه‌مدت، می‌تواند به‌خصوص برای توالی‌های طولانی از داده‌ها، به دلیل مشکل گرادیان محوشونده دشوارتر از شبکه عصبی پیچشی باشد. بااین‌حال، فن‌هایی مانند برش گرادیان[1] و نرمال‌سازی دسته‌ای وجود دارد که می‌تواند به کاستن این مشکل کمک کند. از سوی دیگر، شبکه عصبی پیچشی به‌طورکلی برای آموزش آسان‌تر است و به تکرارهای آموزشی کمتری نسبت به شبکه عصبی حافظه بلندمدت-کوتاه‌مدت نیاز دارد.

کاربرد این دو ابزار باهم ناسازگار نیست؛ بلکه امکان ترکیب هر دو شبکه عصبی پیچشی و عصبی حافظه بلندمدت-کوتاه‌مدت وجود دارد. این به‌عنوان یک معماری ترکیبی CNN-LSTM شناخته می‌شود. در این معماری، شبکه عصبی پیچشی برای استخراج ویژگی‌های فضایی از داده‌های ورودی، و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت برای مدل‌سازی وابستگی‌های زمانی در نقشه‌های ویژگی تولیدشده توسط شبکه عصبی پیچشی استفاده می‌شود. خروجی شبکه عصبی پیچشی به شبکه عصبی حافظه بلندمدت-کوتاه‌مدت وارد می‌شود که از اتصالات بازگشتی خود برای ثبت روابط زمانی بین ویژگی‌ها استفاده می‌کند. به‌طورکلی، معماری ترکیبی CNN-LSTM زمانی مفید است که داده‌های ورودی دارای ابعاد مکانی و زمانی هستند و زمانی که روابط زمانی بین ویژگی‌ها مهم هستند.

۱-۲ مقابله با حملات ممانعت از سرویس با استفاده از شبکه‌های عصبی

به‌طورکلی شبکه‌های عصبی به‌ویژه شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی انتخاب مناسبی برای مقابله با ممانعت از سرویس به‌وسیله یادگیری ماشین هستند؛ زیرا ویژگی‌های مناسب زیر رادارند:

۱- غیرخطی بودن: شبکه‌های عصبی قادر به مدل‌سازی روابط پیچیده غیرخطی بین ورودی‌ها و خروجی‌ها هستند. این به‌ویژه برای برنامه‌هایی مفید است که مثل ترافیک شبکه، داده‌های ورودی ابعاد زیادی دارند و روابط بین ورودی‌ها و خروجی‌ها می‌تواند غیرخطی باشد.

۲- استحکام در برابر نویز: شبکه‌های عصبی عموماً در برابر نویز در داده‌های ورودی مقاوم هستند که آن‌ها را به انتخاب خوبی برای مقابله با مجموعه‌داده‌های شبکه که ممکن است حاوی خطا یا مقادیر گم‌شده باشند، تبدیل می‌کند.

۳- تعمیم: شبکه‌های عصبی قادر به تعمیم داده‌های آموزشی به داده‌های غیرقابل مشاهده هستند که آن‌ها را به انتخاب خوبی برای کارهای پیش‌بینی تبدیل می‌کند. این به‌ویژه در شبکه‌هایی مفید است که هدف، آموزش مدلی باشد که بتوان آن را روی‌داده‌های جدیدی که در طول آموزش‌دیده نشده‌اند، اعمال کرد.

٤- توانایی یادگیری از داده‌ها: شبکه‌های عصبی با استفاده از رویکرد داده محور آموزش داده می‌شوند، به این معنی که می‌توانند الگوها و روابط موجود در ترافیک شبکه را بدون برنامه‌نویسی صریح برای انجام این کار بیاموزند. این باعث می‌شود که آن‌ها برای کارهایی که روابط اساسی بین ورودی‌ها و خروجی‌ها به‌خوبی درک نشده است یا برای مواردی که مدل‌سازی با استفاده از تکنیک‌های دیگر بسیار پیچیده است، انتخاب خوبی باشند.

۵- مقیاس‌پذیری: شبکه‌های عصبی را می‌توان برای مدیریت داده‌های کلان شبکه و اینترنت اشیا مقیاس‌بندی کرد و می‌توان آن‌ها را بر روی معماری‌های رایانشی موازی آموزش داد که آن‌ها را به انتخاب خوبی برای برنامه‌های کلان‌داده۲ تبدیل می‌کند.

شبکه عصبی پیچشی و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت به‌طورخاص برای تشخیص حملات ممانعت از سرویس نیز استفاده‌شده‌اند و انتخاب بین آن‌ها به نیازهای خاص کار و ویژگی‌های داده بستگی دارد. درزمینه تشخیص حملات ممانعت از سرویس، انتخاب بین استفاده از شبکه عصبی پیچشی یا شبکه عصبی حافظه بلندمدت-کوتاه‌مدت، به نوع داده‌های مورد تجزیه‌وتحلیل و ویژگی‌های خاصی که برای شناسایی حملات مهم هستند بستگی دارد. به‌عنوان‌مثال، اگر داده‌های مورد تجزیه‌وتحلیل، شامل جریان‌های ترافیک شبکه باشد (که می‌تواند به‌عنوان دنباله‌ای

[1] Gradient Clipping

[2] Big Data Applications

از بسته‌ها در طول زمان نمایش داده شود) یک شبکه عصبی حافظه بلندمدت-کوتاه‌مدت ممکن است برای شناسایی حملات ممانعت از سرویس مناسب‌تر باشد، زیرا شبکه‌های عصبی حافظه بلندمدت-کوتاه‌مدت برای ثبت وابستگی‌ها و الگوهای زمانی در داده‌های متوالی طراحی‌شده‌اند. شبکه‌های عصبی حافظه بلندمدت-کوتاه‌مدت می‌توانند روابط زمانی بین بسته‌ها را در جریان بیاموزند و الگوهای غیرعادی ترافیک را که نشان‌دهنده حمله ممانعت از سرویس هستند، شناسایی کنند.

۲- روش‌های ترکیب شبکه عصبی پیچشی و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت

شبکه عصبی پیچشی و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت به دلیل توانایی خود در یادگیری الگوها و روابط پیچیده در داده‌ها (که برای تمایز بین ترافیک شبکه عادی و مخرب ضروری است) ابزارهای ارزشمندی برای شناسایی حملات ممانعت از سرویس هستند. در این بخش، روش‌های ترکیب شبکه عصبی پیچشی و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت را بررسی خواهیم کرد.

۲-۱ روش رأی‌گیری برای ترکیب شبکه‌های عصبی

یادگیری عمیق مبتنی بر رأی روشی است که برای ترکیب پیش‌بینی‌های چندین مدل یا ساختار یادگیری عمیق و بهبود دقت کلی پیش‌بینی‌ها استفاده می‌شود. روش رأی‌گیری می‌تواند از هر نوع ساختار یادگیری عمیق، ازجمله شبکه عصبی پیچشی، شبکه‌های عصبی بازگشتی و مدل‌های ترکیبی استفاده کند. در یادگیری عمیق مبتنی بر رأی، چندین مدل یادگیری عمیق بر روی یک مجموعه داده یا زیرمجموعه‌های مختلف مجموعه داده آموزش داده می‌شوند. هر مدل یک پیش‌بینی را روی یک ورودی داده‌شده انجام می‌دهد و پیش‌بینی نهایی بر اساس یک روش رأی‌گیری انجام می‌شود. روش رأی‌گیری می‌تواند بر اساس رأی‌گیری سخت یا نرم باشد. رأی‌گیری سخت شامل انتخاب رایج‌ترین پیش‌بینی در بین مدل‌ها است. رأی‌گیری نرم شامل محاسبه میانگین احتمالات پیش‌بینی‌شده هر مدل و انتخاب کلاس با بالاترین میانگین احتمال است. این رویکرد سطوح اطمینان پیش‌بینی‌های هر مدل را در نظر می‌گیرد. یادگیری عمیق مبتنی بر رأی‌گیری می‌تواند در چندین سناریو مفید باشد، مانند موارد زیر:

- هنگامی‌که در مورد اینکه کدام مدل یا ساختار یادگیری عمیق برای یک کار خاص مناسب‌تر است، تردید وجود دارد.
- هنگامی‌که مدل‌های مختلف نقاط قوت و ضعف متفاوتی دارند و ترکیب آن‌ها می‌تواند به پیش‌بینی دقیق‌تری منجر شود.
- هنگامی‌که مجموعه داده بزرگ و متنوع است و مدل‌های مختلف ممکن است در جنبه‌های مختلف مجموعه داده برتری داشته باشند.

به‌طورکلی، یادگیری عمیق مبتنی بر رأی‌گیری یک‌راه ساده و مؤثر برای بهبود دقت مدل‌ها و ساختارهای یادگیری عمیق با ترکیب پیش‌بینی‌های چند مدل است. حقیقت و لی [۱۷] یک چارچوب جدید یادگیری عمیق مبتنی بر رأی به نام VNN را پیشنهاد می‌کنند تا از هر نوع ساختار یادگیری عمیق بهره گیرند. با در نظر گرفتن چندین مدل ایجادشده توسط جنبه‌های مختلف داده‌ها و ساختارهای مختلف یادگیری عمیق، VNN توانایی جمع‌آوری بهترین مدل‌ها را به‌منظور ایجاد نتایج دقیق‌تر و قوی‌تر فراهم می‌کند؛ بنابراین، VNN به متخصصان امنیتی کمک می‌کند تا حملات پیچیده‌تر را شناسایی کنند.

روش رأی‌گیری ماتریس وزن پویا به ما امکان می‌دهد از نقاط قوت هر دو طبقه‌بندی‌کننده شبکه عصبی پیچشی و RNN استفاده کنیم، زیرا هر دو می‌توانند انواع مختلفی از ورودی‌های داده را مدیریت کنند و جنبه‌های مختلف داده را ضبط کنند. با تنظیم وزن‌ها بر اساس عملکرد، می‌توانیم با الگوهای تغییر داده‌ها سازگار شویم و به‌طور بالقوه دقت کلی طبقه‌بندی‌کننده یکپارچه را بهبود ببخشیم. زین‌الدین و همکاران [۵] یک روش رأی‌گیری ماتریس وزن پویا برای ادغام همه طبقه‌بندی‌کننده‌های پایه پیشنهاد می‌کنند. روش تشخیص نفوذ مجموعه مبتنی بر طبقه‌بندی‌کننده‌هایی مانند شبکه عصبی پیچشی و RNN، یک رویکرد مؤثر و دقیق برای شناسایی و کاهش نفوذ شبکه در شبکه‌های اترنت قطار ارائه می‌دهد. این یک رویکرد مبتنی بر یادگیری ماشینی است که می‌تواند با انواع مختلف داده‌های ترافیک شبکه سازگار شود و تشخیص و کاهش نفوذ

شبکه را به‌صورت بی‌درنگ ارائه دهد. بر اساس مجموعه داده‌ها روش پیشنهادی نشان می‌دهد که توانایی فوق‌العاده‌ای نسبت به طبقه‌بندی‌کننده‌های پایه دارد و به عملکرد تشخیص برتری با دقت ۰,۹۷۵ دست می‌یابد.

۲-۲ ترکیب روش‌های بهینه‌سازی با یادگیری عمیق

ترکیبی از تکنیک‌های یادگیری عمیق و روش‌های بهینه‌سازی چندهدفه شامل ترکیب مدل‌های یادگیری عمیق با تکنیک‌های بهینه‌سازی است که می‌تواند چندین هدف را به‌طور هم‌زمان حل کند. هدف یافتن راه‌حل‌های بهینه است که اهداف متعددی ازجمله دقت، کارایی رایانشی و توانمندی را برآورده کند. هدف روش‌های بهینه‌سازی چندهدفه یافتن مجموعه‌ای از راه‌حل‌هایی است که هیچ راه‌حل دیگری در فضای جستجو بر آن‌ها غالب نیست. این روش‌ها معمولاً شامل استفاده از الگوریتم‌هایی مانند الگوریتم‌های تکاملی، هوش ازدحامی[1] و برنامه‌ریزی ژنتیکی هستند. این روش‌ها به دنبال راه‌حل‌هایی می‌گردند که با توجه به اهداف متعدد، به‌جای یک هدف واحد، بهینه باشند. از سوی دیگر، تکنیک‌های یادگیری عمیق در بسیاری از کاربردها مانند تشخیص تصویر و گفتار، پردازش زبان طبیعی و موارد دیگر بسیار مؤثر هستند. مدل‌های یادگیری عمیق معمولاً با استفاده از تکنیک‌های بهینه‌سازی مانند گرادیان کاهشی برای به حداقل رساندن خطا بین خروجی‌های پیش‌بینی‌شده و واقعی، آموزش داده می‌شوند. ترکیب این دو رویکرد شامل استفاده از تکنیک‌های بهینه‌سازی است که می‌تواند راه‌حل‌هایی را پیدا کند که با توجه به اهداف چندگانه بهینه هستند، درحالی‌که درعین‌حال از مدل‌های یادگیری عمیق برای ارزیابی کیفیت راه‌حل‌های یافت شده استفاده می‌کنند. این رویکرد می‌تواند به رفع چالش‌های یادگیری عمیق، مانند بیش‌برازش، و درعین‌حال بهینه‌سازی چندین هدف به‌طور هم‌زمان کمک کند. برخی از نمونه‌های ترکیبی روش‌های یادگیری عمیق و بهینه‌سازی چندهدفه عبارت‌اند از:

۱- استفاده از الگوریتم‌های بهینه‌سازی چندهدفه برای بهینه‌سازی فراپارامترهای مدل‌های یادگیری عمیق، مانند تعداد لایه‌ها، تعداد نورون‌ها و نرخ یادگیری.

۲- استفاده از الگوریتم‌های بهینه‌سازی چندهدفه برای بهینه‌سازی وزن مدل‌های یادگیری عمیق برای به حداقل رساندن خطاها و به حداکثر رساندن توانمندی در برابر نویز و سایر اختلالات.

۳- استفاده از مدل‌های یادگیری عمیق برای ارزیابی کیفیت راه‌حل‌های تولیدشده توسط الگوریتم‌های بهینه‌سازی چندهدفه در وظایف یادگیری تقویتی.

به‌طورکلی، ترکیب تکنیک‌های یادگیری عمیق و روش‌های بهینه‌سازی چندهدفه می‌تواند به عملکرد بهتر و ایجاد مدل‌های یادگیری عمیق قوی‌تر منجر شود که چندین هدف را به‌طور هم‌زمان برآورده می‌کنند.

۲-۳ ارزیابی استحکام آشکارسازهای ناهنجاری

تشخیص ناهنجاری یک تکنیک کلیدی است که در بسیاری از کاربردها ازجمله تشخیص نفوذ، تشخیص تقلب و تشخیص خطا استفاده می‌شود. حملات خصمانه[2] می‌تواند استحکام آشکارسازهای ناهنجاری[3] را به خطر بیندازد و منجر به مثبت کاذب یا منفی کاذب شود. در اینجا چندراه برای ارزیابی استحکام آشکارسازهای ناهنجاری در برابر حملات خصمانه وجود دارد:

۱- تکنیک‌های حمله خصمانه: انواع مختلفی از حملات خصمانه وجود دارد، مانند اضافه کردن اغتشاشات کوچک[4] به داده‌های ورودی یا دست‌کاری داده‌های ورودی برای گمراه کردن آشکارساز. ارزیابی استحکام آشکارساز ناهنجاری شامل آزمایش آن در برابر حملات خصمانه مختلف است تا مشخص شود که آیا می‌تواند این حملات را شناسایی کند یا خیر.

۲- معیارهای ارزیابی: چندین معیار ارزیابی را می‌توان برای ارزیابی استحکام آشکارسازهای ناهنجاری در برابر حملات خصمانه استفاده کرد. این موارد عبارت‌اند از دقت[5]، درستی[6]، نرخ

[1] Swarm Intelligence
[2] Adverserial attacks
[3] Robustness of anomaly detectors
[4] small perturbations
[5] Precision
[6] Accuracy

مثبت کاذب، نرخ منفی کاذب، بازیابی و امتیاز F1. انتخاب سنجه[1] ارزیابی بستگی به کاربرد و نوع آشکارساز ناهنجاری مورد ارزیابی دارد.

۳- آموزش خصمانه: آموزش خصمانه فنی است که شامل آموزش آشکارسازهای ناهنجاری با نمونه‌های متخاصم برای بهبود استحکام آن‌ها در برابر حملات آینده است. با گنجاندن نمونه‌های متخاصم در مجموعه داده آموزشی، آشکارساز می‌تواند یاد بگیرد که حملات را بهتر تشخیص دهد و مثبت‌ها و منفی‌های کاذب را کاهش دهد.

برای تعیین اینکه آیا یک نمونه متخاصم در آشکارساز غیرعادی باقی می‌ماند، نمونه باید در برابر آشکارساز آزمایش شود و ممکن است برای تشخیص بهتر حمله، آشکارساز نیاز به بهبود یا تعویض داشته باشد. گومز و همکاران [۳] یک روش برای محاسبه توانمندی[2] مدل‌های تشخیص ناهنجاری در سناریوهای صنعتی ارائه می‌کنند. این روش شامل چهار مرحله است و از مجموعه‌ای از مدل‌های اضافی به نام مدل‌های پشتیبانی استفاده می‌کند تا تعیین کند که آیا یک نمونه متخاصم ناهنجار باقی می‌ماند یا خیر. اعتبارسنجی توسط فرآیند تنسی ایستمن[3]، یک بستر آزمایشی شبیه‌سازی‌شده از یک فرآیند شیمیایی، برای شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و برای شبکه عصبی پیچشی یک‌بعدی اعمال می‌شود که بر تشخیص ناهنجاری‌های تولیدشده توسط حملات سایبری مختلف متمرکز است. آزمایش‌ها نشان داد که شبکه عصبی پیچشی یک‌بعدی به‌طور قابل‌توجهی قوی‌تر از شبکه عصبی حافظه بلندمدت-کوتاه‌مدت برای این بستر آزمایش است. به‌طور خاص، اغتشاش ۶۰٪ (استحکام تجربی ۰,۶) از نمونه اصلی برای تولید نمونه‌های خصمانه برای شبکه عصبی حافظه بلندمدت-کوتاه‌مدت موردنیاز است، درحالی‌که در شبکه عصبی پیچشی یک‌بعدی اغتشاش موردنیاز تا ۱۱۱٪ افزایش می‌یابد (استحکام تجربی ۱,۱۱).

۳- بررسی مجموعه‌داده‌های محک

داده‌های آموزش‌دیده از یک مجموعه داده واقعی به‌دست‌آمده است که اشکال مختلفی از حجم ذاتی[4]، پروتکل و حملات مبتنی بر وب را در خود جای‌داده است. مجموعه داده CSE-CIC-IDS2018 مجموعه‌ای از داده‌های ترافیک شبکه است که در سال ۲۰۱۸ به‌عنوان بخشی از تلاش مؤسسه کانادایی امنیت سایبری (CIC) برای بهبود دقت سامانه‌های تشخیص نفوذ منتشر شد. مجموعه داده شامل تعداد زیادی از نمونه‌های ترافیک شبکه برچسب‌گذاری‌شده، ازجمله ترافیک عادی و انواع حملات سایبری است. مجموعه داده CSE-CIC-IDS2018 با جمع‌آوری داده‌های ترافیک شبکه از طیف گسترده‌ای از منابع، ازجمله یک شبکه تحقیقاتی، یک شبکه خصوصی و یک شبکه تله ظرف عسل[5] ایجادشده است. ترافیک در یک دوره چندماهه جمع‌آوری شد و مجموعه داده شامل بیش از ۹ میلیون نمونه از ترافیک شبکه است. مجموعه داده شامل انواع مختلفی از حملات سایبری، ازجمله ممانعت از سرویس توزیع‌شده، حمله پویش درگاه[6]، حمله جستجوی فراگیر[7] و بدافزار است. این حملات با استفاده از ابزارها و تکنیک‌های مختلف ازجمله Metasploit، Nmap و بات‌نت Mirai ایجادشده‌اند. هر نمونه در مجموعه داده به‌عنوان عادی یا مخرب برچسب‌گذاری می‌شود و شامل ویژگی‌های مختلفی مانند نوع پروتکل، نشانی‌های IP مبدأ و مقصد، درگاه‌های مبدأ و مقصد و اندازه بسته‌ها است. مجموعه داده همچنین شامل یک فایل جداگانه با توضیحات انواع حملات است که می‌تواند برای کمک به محققان و متخصصان در درک بهتر ویژگی‌های حملات استفاده شود. مجموعه داده CSE-CIC-IDS2018 به یک معیار مناسب برای ارزیابی سامانه‌های تشخیص نفوذ تبدیل‌شده است و در انواع مطالعات تحقیقاتی مورداستفاده قرارگرفته است. مجموعه داده به‌صورت عمومی در دسترس است و می‌توان آن را از وب‌سایت CIC دانلود کرد.

[1] Metric
[2] Robustness
[3] Tennessee Eastman process
[4] Intrinsic volume
[5] Honeypot
[6] Port Scans
[7] brute force attack

KDDCUP'99 و CTU-13 دو مجموعه داده پرکاربرد در حوزه شبکه کامپیوتری هستند و هرکدام مزایا و معایب خود رادارند.

مزایای KDDCUP'99

۱- در دسترس بودن: KDDCUP'99 یک مجموعه داده در دسترس عموم است و به‌طور گسترده در تحقیقات مورداستفاده قرارگرفته است، و این کار را برای محققان آسان می‌کند تا نتایج را تولید کنند و رویکردهای خود را با دیگران مقایسه کنند.

۲- داده‌های دنیای واقعی: KDDCUP'99 از ترافیک شبکه دنیای واقعی تولیدشده است و حاوی تعداد زیادی حملات مبتنی بر شبکه و ترافیک عادی است که آن را به مجموعه داده خوبی برای ارزیابی سامانه‌های تشخیص نفوذ تبدیل می‌کند.

۳- تنوع: KDDCUP'99 شامل طیف گسترده‌ای از حملات، ازجمله حملات ممانعت از سرویس، کاوشگری[1]، و حملات کاربر به ریشه است که آن را برای ارزیابی عملکرد سامانه‌های تشخیص نفوذ در برابر انواع مختلف حملات مفید می‌کند.

معایب KDDCUP'99:

۱- منسوخ‌شده: KDDCUP'99 در سال ۱۹۹۸ جمع‌آوری شد و وضعیت فعلی امنیت شبکه را منعکس نمی‌کند. ممکن است شامل الگوها و تکنیک‌های حمله اخیر نباشد که کاربرد آن را برای سامانه‌های تشخیص نفوذ مدرن محدود می‌کند.

۲- دامنه محدود: مجموعه داده KDDCUP'99 تنها زیرمجموعه کوچکی از ترافیک شبکه و سناریوهای حمله را پوشش می‌دهد، و قابلیت تعمیم و توانایی آن را برای ارزیابی سامانه‌های تشخیص نفوذ تحت طیف وسیع‌تری از شرایط محدود می‌کند.

مزایای CTU-13:

۱- داده‌های دنیای واقعی: مجموعه‌داده‌های CTU-13 از یک شبکه تله ظرف عسل جمع‌آوری‌شده است و حاوی ترافیک شبکه دنیای واقعی است که آن را بیشتر نماینده سناریوهای حمله فعلی می‌کند.

۲- بهنگام بودن: CTU-13 بعد از KDDCUP'99 جمع‌آوری‌شده است که آن را به‌روزتر و منعکس‌کننده چالش‌های امنیتی شبکه فعلی می‌کند.

۳- تنوع: CTU-13 شامل طیف گسترده‌ای از حملات، ازجمله DoS، کاوشگری و بدافزار است که آن را برای ارزیابی سامانه‌های تشخیص نفوذ در برابر انواع مختلف حملات مفید می‌کند.

معایب CTU-13:

۱- در دسترس بودن محدود: مجموعه داده CTU-13 به‌صورت عمومی در دسترس نیست و محققان باید برای دسترسی به آن مجوز بگیرند که می‌تواند استفاده و بازتولید پذیری[2] آن را محدود کند.

۲- اندازه محدود: CTU-13 مجموعه داده‌ای کوچک‌تر از KDDCUP'99 است که می‌تواند توانایی آن را برای ارائه یک ارزیابی جامع از سامانه‌های تشخیص نفوذ محدود کند.

همچنین مجموعه داده CIC-DDOS2019 شامل ۱۵ ویژگی مختلف است که می‌تواند برای مدل‌های یادگیری ماشین استفاده شود، مانند نشانی‌های IP مبدأ و مقصد، درگاه‌های مبدأ و مقصد، نوع پروتکل، طول بسته و موارد دیگر. مجموعه داده همچنین شامل یک برچسب باینری است که نشان می‌دهد که ترافیک بی‌آزار یا مخرب است.

۳-۱ مدل‌سازی شبکه با جریان ترافیک دوجهته

جریان ترافیک دوجهته مبتنی بر بسته[3] به جریان ترافیک شبکه در هر دو جهت بین مشتری و سرور اشاره دارد. درزمینه محک[4] ممانعت از سرویس، مجموعه‌داده‌هایی که شامل سناریوهای حمله به‌روز هستند، اغلب از جریان ترافیک دوجهته مبتنی بر بسته برای شبیه‌سازی ترافیک واقعی شبکه و ترافیک جعلی مربوط به حملات استفاده می‌کنند. این مجموعه‌داده‌ها معمولاً شامل طیف گسترده‌ای از سناریوهای حمله مانند حملات حجمی، حملات پروتکل و حملات لایه برنامه هستند و ممکن است از الگوهای ترافیکی مختلف برای شبیه‌سازی ترافیک واقعی، مانند رگبارهای[5] ترافیک

[1] Probing
[2] Reproducibility
[3] Packet-Based Bi-Directional Traffic Flow
[4] benchmarking
[5] bursts

یا ترافیک دوره‌ای استفاده کنند. استفاده از جریان ترافیک دوجهته مبتنی بر بسته در این مجموعه‌داده‌ها تضمین می‌کند که ترافیک و حملات شبکه به‌طور دقیق نمایش داده می‌شوند و می‌توان از آن‌ها برای ارزیابی اثربخشی راه‌حل‌های شناسایی و کاهش ممانعت از سرویس استفاده کرد. مجموعه‌داده‌های محک‌گذاری ممانعت از سرویس که شامل جریان ترافیک دوجهته مبتنی بر بسته می‌شود، ممکن است ویژگی‌های دیگری مانند نرخ‌ها و اندازه‌های مختلف حمله، انواع مختلف ترافیک حمله، و ترکیب‌های مختلف حملات را نیز شامل شود. این ویژگی‌ها می‌تواند به محققان و متخصصان کمک کند تا استحکام و اثربخشی سازوکارهای دفاعی مختلف ممانعت از سرویس را ارزیابی کرده و نقاط قوت و ضعف آن‌ها را شناسایی کنند.

معین‌الاسلام و همکاران [٤] یک مدل چندطبقه‌بندی را با استفاده از مجموعه شبکه‌های عصبی عمیق انباشته[1] ارائه می‌کنند که انواع مختلفی از حملات ممانعت از سرویس را برای رسیدگی به ترافیک شبیه‌سازی‌شده ذکرشده در بالا شناسایی می‌کند. مدل ترکیبی پیشنهادی، شبکه عصبی پیچشی، شبکه عصبی حافظهٔ بلندمدت-کوتاه‌مدت و واحد بازگشتی با گیت[2] را در خود جای‌داده است. نتایج نشان می‌دهد که در ارزیابی مدل با مجموعه‌داده‌های بزرگ مانند CIC-DDoS2019، تکنیک انباشته‌سازی عملکرد مدل را افزایش می‌دهد. مدل پیشنهادی می‌تواند به‌دقت ۸۹,٤ درصد برسد که از سایر روش‌های مشابه بهتر است.

زین‌الدین و همکاران [٥] یک روش انتخاب ویژگی مناسب به نام تقویت گرادیان شدید[3] برای تعیین مرتبط‌ترین ویژگی‌های داده با یک شبکه عصبی پیچشی و شبکه عصبی حافظهٔ بلندمدت-کوتاه‌مدت ترکیبی (CNN-LSTM) برای طبقه‌بندی حملات ممانعت از سرویس پیشنهاد می‌کنند. مدل پیشنهادی مجموعه داده CIC-DDoS2019 را با دقت بهبودیافته و پیچیدگی کم و با شرایط خاص اینترنت اشیای صنعتی یعنی تأخیر کم ارزیابی کرد. نتایج عملکرد نشان می‌دهد که مدل پیشنهادی به‌دقت بالای ۹۹,٥۰ درصد با هزینه زمانی ۰,۱۷۹ میلی‌ثانیه دست می‌یابد.

٤- تهدیدها

٤-۱ مقابله با ممانعت از سرویس توزیع‌شده با نرخ پایین

«ممانعت از سرویس توزیع‌شده با نرخ پایین»[4] نوعی از حملات ممانعت از سرویس است که از یک رویکرد آهسته و پنهانی برای مسدود کردن یک سرور یا شبکه با ارسال ترافیک بیهوده استفاده می‌کنند. هدف حملات ممانعت از سرویس توزیع‌شده با نرخ پایین مصرف منابع سیستم موردنظر و غیرقابل‌دسترس کردن آن برای کاربران عادی است. سازوکار حملات ممانعت از سرویس توزیع‌شده با نرخ پایین شامل تعداد زیادی دستگاه آسیب‌دیده، (بخشی از بات‌نت[5]) است که حجم کمی از ترافیک را به سیستم قربانی می‌فرستند. این ترافیک اغلب به‌اندازه‌ای است که باعث شود سیستم هدف از منابع خود مانند قدرت پردازش یا حافظه استفاده کند تا زمانی که نتواند به ترافیک قانونی خود پاسخ دهد. برخلاف حملات ممانعت از سرویس سنتی که شامل حجم بالایی از ترافیک ارسال‌شونده به‌یک‌باره است، شناسایی حملات ممانعت از سرویس توزیع‌شده با نرخ پایین می‌تواند دشوارتر باشد؛ زیرا ترافیک در مدت‌زمان طولانی‌تری پخش می‌شود. این باعث می‌شود مهاجم راحت‌تر از شناسایی فرار کند و حمله را برای مدت طولانی‌تری ادامه دهد. لئو و همکاران [۱] یک مدل جدید، کاربردی و سریع (FastCBLA -EM) برای تشخیص حملات ممانعت از سرویس توزیع‌شده با نرخ پایین پیشنهاد می‌کند. در FastCBLA -EM، یک روش لغزشی دوگانه بسط بسته‌ها[6] برای تولید نمونه‌های ترتیب زمانی با طول ثابتی از جریان‌ها، استفاده می‌شود. در مرحله بعد، یک شبکه رقابتی متشکل از شبکه عصبی پیچشی یک‌بعدی و یک شبکه دوطرفه عصبی حافظه بلندمدت-کوتاه‌مدت[7] برای یادگیری نمونه‌های مکانی و زمانی به‌طور موازی استفاده می‌شود.

[1] Stacking Ensemble
[2] Gated Recurrent Unit
[3] Extreme Gradient Boosting
[4] Low-rate Distributed Denial of Service
[5] botnet
[6] Dilated Padding-Based Dual Sliding Method
[7] bi-LSTM

درنهایت، از یک سازوکار داوری مبتنی بر روش توجه بهبودیافته[1] برای جمع‌آوری و وزن‌گذاری نمونه‌ها برای شناسایی حملات ممانعت از سرویس توزیع‌شده با نرخ پایین استفاده می‌شود. عملکرد FastCBLA -EM با سایر مدل‌ها، با به دست آوردن گروهی از فراپارامترهای تنظیم‌شده در مجموعه داده مبتنی بر جریان ISCX-2016-SlowDos بازبینی و مقایسه شده است. نتایج تجربی نشان می‌دهد که دقت تشخیص FastCBLA -EM می‌تواند تا ۹۹,۷٪ باشد و پیچیدگی زمانی این الگوریتم O(n) است.

حملات آهسته ممانعت از سرویس، شناسایی و کاهش خود را به‌ویژه در محیط «شبکه نرم‌افزارمحور[2]» که بر مدیریت و کنترل متمرکز متکی هستند، چالش‌برانگیز می‌کند. حملات آهسته ممانعت از سرویس می‌توانند به‌تدریج منابع شبکه را مصرف کنند و تشخیص را سخت‌تر از انفجارهای ترافیکی با حجم بالا کنند. بنابراین، شناسایی و کاهش حملات ممانعت از سرویس آهسته نیازمند فن‌ها و رویکردهای تخصصی است، مانند الگوریتم‌های یادگیری ماشینی که می‌توانند الگوهای رفتار ترافیک را در طول زمان شناسایی کنند و سازوکارهای تشخیص ناهنجاری که می‌توانند الگوهای ترافیک غیرمعمول را به‌صورت بی‌درنگ شناسایی کنند. نوگرها و مورتی [۱۳] استفاده از یک مدل ترکیبی CNN-LSTM را برای شناسایی حملات ممانعت از سرویس آهسته در شبکه‌های مبتنی بر شبکه نرم‌افزارمحور پیشنهاد می‌کنند. عملکرد این روش بر اساس مجموعه‌داده‌های سفارشی ارزیابی می‌شود. نتایج به‌دست‌آمده کاملاً چشمگیر هستند – همه معیارهای عملکرد در نظر گرفته‌شده بالای ۹۹٪ هستند. مدل ترکیبی CNN-LSTM همچنین از سایر مدل‌های یادگیری عمیق مانند پرسپترون چندلایه[3] و مدل‌های یادگیری ماشین استاندارد مانند ماشین‌های بردار پشتیبانی کلاس یک[4] بهتر عمل می‌کند.

۴-۲ مقابله با حمله ممانعت از سرویس توزیع‌شده مبتنی بر باج‌افزار

حمله ممانعت از سرویس توزیع‌شده مبتنی بر باج‌افزار[5] یک نوع حمله سایبری است که توسط یک باج‌افزار انجام می‌شود. در این حمله، باج‌افزار زیادی دستگاه را مانند رایانه‌ها، سرورها یا دستگاه‌های اینترنت اشیا آلوده کرده و سپس باهدف تنظیم حمله ممانعت از سرویس علیه یک شبکه یا سرویس هدف، از آن‌ها استفاده می‌کند. مهاجم در این حمله تهدید می‌کند که اگر سازمان هدف باج پرداخت نکند، باج‌افزار را اجرا می‌کند.

بسنت و همکاران [۲۰] چارچوب تشخیص باج افزار جدیدی مبتنی بر یادگیری عمیق را در اسکادای ایستگاه شارژ خودروی الکتریکی با تجزیه‌وتحلیل عملکرد سه الگوریتم یادگیری عمیق، یعنی شبکه عصبی عمیق، شبکه عصبی پیچشی یک‌بُعدی، و شبکه عصبی بازگشتی حافظه بلندمدت-کوتاه‌مدت پیشنهاد می‌کند. نمایه وضعیت شارژ[6] عملکرد مدل را اندازه‌گیری می‌کند و می‌توان از آن برای ارزیابی مدل‌های پیش‌بینی در این مثال خاص استفاده کرد.

۴-۳ تهدیدات امنیتی در شبکه‌های کنترلی راه‌آهن

هدف یک سیستم تشخیص نفوذ امنیتی برای شبکه اترنت قطار[7] (ECN) شناسایی و کاهش حملات شبکه و تهدیدات امنیتی در قطارهای راه‌آهن است. ECN شبکه‌ای است که دستگاه‌ها و سامانه‌های مختلف را در قطارها به هم متصل می‌کند؛ ولی در برابر حملات امنیتی که می‌تواند ایمنی و امنیت مسافران و خود قطار را به خطر بیندازد آسیب‌پذیر است. هدف خاص سامانه تشخیص نفوذ برای ECN قطار تضمین امنیت و ایمنی مسافران، خدمه و خود قطار با شناسایی و کاهش هرگونه تهدید امنیتی است که ممکن است شبکه را به خطر بیندازد. علاوه بر این، سامانه تشخیص نفوذ همچنین می‌تواند به شناسایی منبع حمله، نوع حمله و میزان آسیب ناشی از حمله کمک کند. استفاده از سامانه تشخیص نفوذ برای قطار ECN می‌تواند چندین مزیت داشته باشد، ازجمله:

[1] Enhanced Attention Method
[2] Software-defined Network
[3] MultiLayer Perceptron
[4] l-Class Support Vector Machines
[5] Ransomware-Driven Distributed Denial of Service
[6] State of Charge
[7] Ethernet Consist Network

۱. امنیت شبکه بهبودیافته: یک سامانه تشخیص نفوذ می‌تواند تهدیدات امنیتی را به‌صورت بی‌درنگ شناسایی و کاهش دهد و امنیت کلی ECN قطار را بهبود بخشد.

۲. تشخیص زودهنگام: یک سامانه تشخیص نفوذ می‌تواند تهدیدات امنیتی را قبل از ایجاد آسیب قابل‌توجه شناسایی کند و امکان مداخله زودهنگام و کاهش آن را فراهم کند.

۳. کاهش خطر خرابی: سامانه تشخیص نفوذ می‌تواند به جلوگیری از خرابی ناشی از حملات شبکه که می‌تواند منجر به تأخیر و لغو برنامه قطارها شود کمک کند.

٤. ایمنی مسافر: سامانه تشخیص نفوذ می‌تواند با جلوگیری از تهدیدات امنیتی ناشی از به خطر انداختن ECN قطار، به تضمین ایمنی و امنیت مسافران و خدمه کمک کند.

یو و همکاران [٦] یک روش جدید تشخیص نفوذ را برای حملات شبکه دفاعی در برابر تهدیدات ECN، به‌ویژه اسکن IP، اسکن درگاه، ممانعت از سرویس و MITM[1] پیشنهاد می‌کند. سی‌وچهار ویژگی از محتویات پروتکل‌های مختلف از داده‌های خام تولیدشده از بستر آزمایش ECN استخراج می‌شوند تا یک مجموعه داده خاص را تشکیل دهند.

٤-٤ تهدیدات شبکه‌های تولید و توزیع برق

اینورترهای فتوولتائیک (PV) متصل به شبکه[2] جزء حیاتی سامانه‌های برق PV هستند که خروجی DC پانل‌های PV را به برق AC تبدیل می‌کنند و به شبکه برق تغذیه می‌شود. این اینورترها نقش مهمی در ادغام منابع انرژی تجدیدپذیر در شبکه برق دارند و وسیله‌ای مطمئن و کارآمد برای تولید برق از انرژی خورشیدی ارائه می‌کنند. استفاده از اینورترهای فتوولتائیک متصل به شبکه برای ادغام منابع انرژی تجدیدپذیر در شبکه برق، بهبود کیفیت توان، بهینه‌سازی مدیریت انرژی و محافظت از سیستم در برابر خطرات احتمالی ضروری است. اینورترهای فتوولتائیک متصل به شبکه (PV) به دلیل افزایش اتصال و ادغام این سامانه‌ها با اینترنت و شبکه برق، مستعد حملات سایبری هستند. یک حمله سایبری مبتنی برداده به اینورترهای PV شامل سوءاستفاده از آسیب‌پذیری‌های سیستم برای دست‌کاری یا اختلال در عملکرد اینورتر است.

به‌طورکلی، حملات سایبری مبتنی برداده به اینورترهای فتوولتائیک متصل به شبکه می‌تواند عواقب شدیدی ازجمله مشکلات کیفیت برق و خاموشی داشته باشد. استراتژی‌های تشخیص مانند تشخیص ناهنجاری، سامانه‌های دفاعی چندلایه، نرم‌افزارهای ضد بدافزار و سازوکارهای رمزگذاری و احراز هویت را می‌توان برای کاهش اثرات این حملات و اطمینان از عملکرد ایمن و قابل‌اعتماد پیاده‌سازی کرد.

مائو و همکاران [٨] یک استراتژی تشخیص حمله سایبری مبتنی برداده برای اینورترهای فتوولتائیک متصل به شبکه (PV) را پیشنهاد کردند. شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی به‌عنوان هسته تشخیص، برای طبقه‌بندی سری‌های زمانی و تشخیص هدف و حالت حمله سایبری به کار می‌روند. حذف افزونگی ورودی و انتخاب فراپارامتر برای بهینه‌سازی تشخیص انجام می‌شود. در همین حال، ابزارهای حمله سایبری قدرتمند تزریق داده‌های نادرست[3]، ممانعت از سرویس و تأخیر هم بر روی اتصال سیگنال‌های نمونه‌برداری‌شده و هم بر دستورات صادرشده در یک مدل اینورتر متصل به شبکه اعمال می‌شوند. با مشاهده عملکرد سیستم از طریق اندازه‌گیری‌های الکتریکی، این مطالعه موردی تشخیص مبتنی بر شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و CNN-LSTM و LSTM پیچشی را ارزیابی می‌کند و کیفیت بالایی از طبقه‌بندی را به دست می‌آورد.

گور و کومار در [٩] از یک مدل شبکه عصبی حافظه بلندمدت-کوتاه‌مدت مبتنی بر شبکه عصبی بازگشتی استفاده کردند که بر روی داده‌های سری زمانی کار می‌کند و ورودی‌های وابسته به زمان طولانی را مدیریت می‌کند، درنتیجه حملات ممانعت از سرویس را شناسایی می‌کند. برای افزایش عملکرد طبقه‌بندی مدل شبکه عصبی حافظه بلندمدت-کوتاه‌مدت، از مدل شبکه عصبی حافظه بلندمدت-کوتاه‌مدت چندلایه برای داده‌های باینری و چندکلاسه استفاده‌شده است و حداکثر دقت به‌دست‌آمده ٩٩,٤٦٪ (با ١ لایه) و سپس ٩٩,١٦٪ برای شبکه عصبی حافظه بلندمدت-کوتاه‌مدت

[1] Man in the Middle
[2] Grid-connected photovoltaic (PV) inverters
[3] False Data Injection

(۲ لایه) با داده‌های Multiclass است. داده‌های گروه‌بندی‌شده مدل DDoSLSTM پیشنهادی از دیگر تکنیک‌های پیشرفته، ازجمله شبکه‌های عصبی عمیق، RNN، شبکه عصبی پیچشی و ترانسفورماتورها بهتر عمل می‌کند.

٤-٥ تهدیدات شبکه‌های نرم‌افزارمحور

مجموعه‌داده‌های شبکه نرم‌افزارمحور دارای ویژگی‌های منحصربه‌فردی هستند که آن‌ها را از مجموعه‌داده‌های معیار ایجادشده برای اینترنت متمایز می‌کند که می‌تواند آن‌ها را برای ارزیابی سامانه‌های تشخیص حمله ممانعت از سرویس مناسب‌تر کند. برخی از این ویژگی‌ها عبارت‌اند از:

۱- دانه‌بندی[1]: مجموعه‌داده‌های شبکه نرم‌افزارمحور می‌توانند جزئیات دقیقی در مورد ترافیک شبکه ارائه دهند، مانند داده‌های سطح جریان که می‌تواند تشخیص حملات ممانعت از سرویس با نرخ پایین را که ممکن است در مجموعه‌داده‌های درشت‌دانه قابل‌تشخیص نباشد، امکان‌پذیر می‌کند.

۲- قابلیت برنامه‌ریزی: توانایی پیکربندی و کنترل برنامه‌نویسی دستگاه‌های شبکه در یک محیط شبکه نرم‌افزارمحور، انعطاف‌پذیری بیشتری در جمع‌آوری و تجزیه‌وتحلیل داده‌ها برای اهداف تشخیص ممانعت از سرویس فراهم می‌کند.

۳- برچسب‌گذاری حقیقت زمینی: در یک محیط شبکه نرم‌افزارمحور، امکان ایجاد برچسب‌های حقیقت زمینی برای ترافیک شبکه وجود دارد که می‌تواند به ارزیابی سامانه‌های تشخیص ممانعت از سرویس کمک کند.

٤- رفتار پویای شبکه: قابلیت برنامه‌پذیری شبکه نرم‌افزارمحور، تغییرات پویا در رفتار شبکه (مانند ایجاد جریان‌های جدید یا تغییر مسیر ترافیک) را امکان‌پذیر می‌کند که می‌تواند سناریوهای دنیای واقعی و ماهیت در حال تحول حملات ممانعت از سرویس را با دقت بیشتری منعکس کند.

۵- داده‌های چندبعدی: مجموعه‌داده‌های شبکه نرم‌افزارمحور می‌توانند شامل داده‌های چندبعدی مانند اندازه بسته، جهت بسته‌ها و توپولوژی شبکه باشند که می‌تواند تصویر کامل‌تری از رفتار شبکه ارائه دهد و به تشخیص حملات ممانعت از سرویس پیشرفته کمک کند.

کاچاویمث و نارایان [۱۵] سه مجموعه داده شبکه نرم‌افزارمحور را برای طبقه‌بندی حملات ممانعت از سرویس با سه ماژول یادگیری عمیق به نام‌های پرسپترون چندلایه (MLP)، شبکه عصبی پیچشی و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت در نظر می‌گیرند. عملکرد مدل‌ها با استفاده از دقت مدل و تلفات[2] مدل اندازه‌گیری می‌شود. نتایج نشان می‌دهد که شبکه عصبی حافظه بلندمدت-کوتاه‌مدت برای هر سه مجموعه داده شبکه نرم‌افزارمحور بهتر از MLP و شبکه عصبی پیچشی عمل می‌کند.

به‌عنوان یک نمونه دیگر از تهدیدات روی شبکه‌های نرم‌افزارمحور می‌توان به مورد زیر اشاره کرد: یک مهاجم می‌تواند از حملات جستجوی فراگیر[3] روی SSH برای ایجاد ممانعت از سرویس در یک شبکه نرم افزارمحور استفاده کند. در یک شبکه نرم‌افزارمحور، شبکه توسط یک کنترل‌کننده متمرکز مدیریت می‌شود که با سوئیچ‌ها برای ارسال بسته‌ها ارتباط برقرار می‌کند. مهاجم می‌تواند از باتنت سوئیچ‌های شبکه نرم‌افزارمحور در معرض خطر برای ارسال ترافیک به سیستم قربانی استفاده کند. مهاجم می‌تواند از ترکیبی از حملات جستجوی فراگیر SSH و بدافزار برای به خطر انداختن سوئیچ‌های شبکه نرم‌افزارمحور و نصب ابزار تولید ترافیک بر روی آن‌ها استفاده کند. ابزار تولید ترافیک می‌تواند برای ایجاد حجم زیادی از ترافیک و ایجاد یک حمله ممانعت از سرویس استفاده شود. مهاجم می‌تواند از سوئیچ‌های شبکه نرم‌افزارمحور آسیب‌دیده برای تقویت حمله با ایجاد تعداد زیادی قوانین جریان و ارسال حجم بالایی از ترافیک به یک هدف خاص استفاده کند و منابع سیستم هدف را تحت تأثیر قرار دهد. مهاجم همچنین می‌تواند از REST API کنترل‌کننده شبکه نرم‌افزارمحور برای ایجاد و حذف قوانین جریان استفاده کند که به آن‌ها اجازه می‌دهد حملات را انجام دهند و به‌سرعت تاکتیک‌ها را برای فرار از شناسایی تغییر دهند. برای جلوگیری از این نوع حملات، لازم است که اطمینان حاصل شود که تمام سوئیچ‌های شبکه نرم‌افزارمحور به‌درستی پیکربندی و ایمن شده‌اند. همچنین نظارت بر ترافیک

[1] Granularity
[2] Loss
[3] Brute-force

شبکه برای فعالیت غیرمعمول و داشتن استراتژی‌های کاهش[1] برای پاسخ سریع به حملات ممانعت از سرویس بالقوه مهم است. اجرای اقدامات کنترل دسترسی، مانند احراز هویت دومرحله‌ای، می‌تواند به جلوگیری از حملات جستجوی فراگیر SSH نیز کمک کند. علاوه بر این، استفاده از سامانه‌های تشخیص نفوذ و پیشگیری (IDPS) می‌تواند به شناسایی و کاهش حملات در زمان واقعی کمک کند. لی و همکاران [۱۱] یک سیستم تشخیص نفوذ و پیشگیری از یادگیری عمیق (DL-IDPS) را معرفی کرده‌اند تا از حملات جستجوی فراگیر SSH و حملات ممانعت از سرویس توزیع‌شده در شبکه نرم‌افزارمحور جلوگیری کند. طول بسته در سوئیچ شبکه نرم‌افزارمحور به‌عنوان دنباله‌ای برای مدل‌های یادگیری عمیق برای شناسایی بسته‌های غیرعادی و مخرب جمع‌آوری‌شده است. چهار مدل یادگیری عمیق، ازجمله پرسپترون چندلایه[2] (MLP)، شبکه عصبی پیچشی، شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و رمزگذار خودکار پشته‌ای[3] (SAE)، پیاده‌سازی و برای DL-IDPS پیشنهادی مقایسه شده‌اند. MLP ها شبکه‌های عصبی پیش خورنده[4] هستند که از چندین لایه نورون تشکیل‌شده‌اند. هر لایه به‌طور کامل به لایه بعدی متصل است و خروجی یک‌لایه، ورودی لایه بعدی است. MLP ها معمولاً برای کارهای طبقه‌بندی و رگرسیون استفاده می‌شوند. از سوی دیگر از شبکه‌های عصبی حافظه بلندمدت-کوتاه‌مدت دارای سلول حافظه‌ای که می‌تواند اطلاعات را برای مدت‌زمان طولانی و سه گیت حفظ کند که جریان اطلاعات را به داخل و خارج از سلول کنترل می‌کند استفاده‌شده است. بااین‌حال، SAE ها شبکه‌های عصبی‌ای هستند که از لایه‌های متعددی از ماژول‌های رمزگذار و رمزگشا تشکیل‌شده‌اند و برای بازسازی داده‌های ورودی آموزش‌دیده‌اند. SAE ها اغلب برای کاهش ابعاد و یادگیری ویژگی استفاده می‌شوند و می‌توانند به‌عنوان اجزای سازنده سایر مدل‌های یادگیری عمیق استفاده شوند. تجربه لی و همکاران [۱۱] نشان می‌دهد که DL-IDPS مبتنی بر MLP پیشنهادی بالاترین درستی را دارد که می‌تواند به ترتیب نزدیک به ۹۹٪ و ۱۰۰٪ درستی را برای جلوگیری از حملات جستجوی SSH و ممانعت از سرویس به دست آورد.

٤-٦ تهدیدات خاص کاربرد اینترنت اشیا

مدل‌های یادگیری عمیق برای تشخیص حملات ممانعت از سرویس برای محیط‌های اینترنت اشیا مناسب هستند، زیرا می‌توانند حجم زیادی از داده‌های تولیدشده توسط دستگاه‌های اینترنت اشیا را مدیریت کرده و ناهنجاری‌ها را در زمان واقعی شناسایی کنند. دستگاه‌های اینترنت اشیا حجم زیادی از داده‌ها را تولید می‌کنند، ازجمله خوانش حسگرها، ترافیک شبکه و رفتار کاربر. تکنیک‌های یادگیری ماشینی سنتی ممکن است نتوانند حجم و تنوع داده‌های تولیدشده توسط دستگاه‌های اینترنت اشیا را مدیریت کنند، اما مدل‌های یادگیری عمیق می‌توانند به‌طور خودکار ویژگی‌ها و الگوها را از مقادیر زیادی داده یاد بگیرند. یکی از مدل‌های یادگیری عمیق مناسب برای تشخیص حمله ممانعت از سرویس، توسط دستگاه‌های اینترنت اشیا شبکه عصبی بازگشتی (RNN) است، به‌ویژه مدل شبکه عصبی حافظه بلندمدت-کوتاه‌مدت. شبکه‌های عصبی حافظه بلندمدت-کوتاه‌مدت برای مدیریت داده‌های متوالی، مانند ترافیک دستگاه‌های اینترنت اشیا، مناسب هستند و می‌توانند الگوها و ناهنجاری‌ها را در داده‌ها تشخیص دهند. مدل مناسب دیگر شبکه عصبی پیچشی است که می‌تواند ویژگی‌های بسامد زمانی داده‌های ترافیک دستگاه‌های اینترنت اشیا را تجزیه‌وتحلیل کند و طبقه‌بندی دقیق انواع ترافیک و شناسایی حملات ممانعت از سرویس را ارائه دهد. مدل‌های یادگیری عمیق برای تشخیص حملات ممانعت از سرویس را می‌توان در دستگاه‌ها یا دروازه‌های[5] اینترنت اشیا مستقر کرد و به حملات احتمالی شناسایی و پاسخ به‌موقع ارائه کرد. علاوه بر این، این مدل‌ها می‌توانند با سایر اقدامات امنیتی مانند فایروال‌ها و سامانه‌های تشخیص نفوذ ترکیب شوند تا یک‌راه حل امنیتی جامع برای محیط‌های اینترنت اشیا ارائه کنند. به‌طور خلاصه، مدل‌های یادگیری عمیق برای تشخیص حملات ممانعت از سرویس برای محیط‌های اینترنت اشیا مناسب هستند، زیرا می‌توانند حجم زیادی از داده‌های تولیدشده توسط دستگاه‌های

[1] Mitigation strategies
[2] Multilayer Perceptron
[3] Stacked Auto-encoder
[4] Feedforward Neural Networks
[5] gateways

اینترنت اشیا را کنترل کنند، ناهنجاری‌ها را در زمان واقعی شناسایی کنند، و می‌توانند در دستگاه‌های اینترنت اشیا یا دروازه‌ها برای بهبود امنیت مستقر شوند.

روپک و همکاران [۱۲] مدل‌های یادگیری عمیقی را پیشنهاد کرده‌اند و آن‌هایی را با مجموعه داده CICIDS2017 برای تشخیص حمله ممانعت از سرویس، ارزیابی کرده‌اند که دقت ٪۹۷,۱۶ را ارائه می‌دهد، همچنین مدل‌های پیشنهادی با الگوریتم‌های یادگیری ماشین پایه مقایسه می‌شوند. این مقاله همچنین چالش‌های تحقیقاتی باز را برای استفاده از الگوریتم یادگیری عمیق برای امنیت سایبری اینترنت اشیا شناسایی می‌کند.

احسن و همکاران [۱۶] با استفاده از مجموعه داده CICIDS-2017، یک مدل تشخیص نفوذ مبتنی بر شبکه عصبی عمیق را برای شناسایی حملات ممانعت از سرویس توزیع‌شده و چند حمله سایبری دیگر ارائه کرد. علاوه بر این، مدل‌های یادگیری عمیق مؤثری برای نشان دادن دانش امنیت سایبری در شبکه‌های اینترنت اشیا، ازجمله DenseNet، شبکه عصبی پیچشی، و مدل ترکیبی شبکه عصبی پیچشی و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت موردبررسی قرارگرفته‌اند. نتایج تجربی بر روی KDDCUP'99 و CTU-13، به‌عنوان دو مجموعه داده محک[1] شناخته‌شده و پرکاربردتر در ناحیه شبکه کامپیوتری، هستند که هشدارهای اشتباه تا ۷۵ درصد کاهش‌یافته است. مقایسه با مدل‌های اصلی یادگیری عمیق، ازجمله شبکه عصبی عمیق (DNN)، شبکه عصبی پیچشی، شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و واحد بازگشتی دارای گیت (GRU) انجام‌شده است.

حکمتی و همکاران [۱۹] دریافتند که یک توزیع کوشی کوتاه‌شده[2] برای حجم ترافیک بی‌آزار از دستگاه‌های اینترنت اشیا مناسب است و حجم ترافیک حمله به دنبال توزیع یکسان اما با پارامترهای مختلف برای مکان و مقیاس مدل شده است. با شبیه‌سازی ترافیک بی‌آزار و ترافیک حمله با هم‌پوشانی توزیع‌های حجم ترافیک بر روی یک ردیابی[3] از داده‌های وضعیت فعالیت یک استقرار واقعی اینترنت اشیای شهری متشکل از حدود ۴۰۰۰ گره و با استفاده از مجموعه‌داده‌های پیشرفته چهار مدل شبکه عصبی مقایسه می‌شوند: پرسپترون چندلایه (MLP)، شبکه عصبی پیچشی، شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و رمزگذار خودکار (AEN). عملکرد آن‌ها را به‌عنوان تابعی از پارامتری که انحراف حملات از داده‌های بی‌آزار را اندازه‌گیری می‌کند، تجزیه‌وتحلیل می‌کند. پرسپترون چندلایه نوعی شبکه عصبی پیش‌خورنده است که برای کاربردهای مختلفی ازجمله تشخیص حمله ممانعت از سرویس استفاده‌شده است. پرسپترون چندلایه عموماً در ثبت روابط و الگوهای پیچیده غیرخطی در داده‌ها مؤثر است. بااین‌حال، ممکن است برای شناسایی حملات ممانعت از سرویس که شامل تغییرات پویا در ترافیک شبکه هستند، بهینه نباشد. از طرف دیگر شبکه عصبی پیچشی که معمولاً برای وظایف پردازش تصویر و سیگنال استفاده می‌شود، برای تشخیص حملات ممانعت از سرویس با نتایج امیدوارکننده استفاده‌شده است. شبکه عصبی پیچشی در استخراج ویژگی‌های فضایی از داده‌ها خوب است و می‌تواند برای شناسایی حملات ممانعت از سرویس که شامل الگوهای فضایی در ترافیک شبکه هستند، استفاده شود. شبکه عصبی حافظه بلندمدت-کوتاه‌مدت که معمولاً برای وظایف پردازش توالی استفاده می‌شود برای تشخیص حملات ممانعت از سرویس نیز با نتایج خوبی استفاده‌شده است. شبکه عصبی حافظهٔ بلندمدت-کوتاه‌مدت در کشف وابستگی‌های زمانی در داده‌ها کارآمدتر است و توانسته برای شناسایی حملات ممانعت از سرویس که شامل تغییرات پویا در ترافیک شبکه در طول زمان هستند، استفاده شود. AEN یک تکنیک یادگیری بدون نظارت است که برای تشخیص ناهنجاری ازجمله تشخیص حمله ممانعت از سرویس استفاده‌شده است. AEN را می‌توان برای یادگیری یک نمایش با ابعاد کم از ترافیک عادی شبکه و تشخیص انحرافات از این رفتار عادی استفاده کرد. بااین‌حال، AEN ممکن است برای شناسایی انواع جدید یا دیده‌نشده حملات ممانعت از سرویس بهینه نباشد. به‌طور خلاصه، هر رویکرد مزایا و معایب خود را دارد و انتخاب بهترین رویکرد به نیازهای خاص برنامه بستگی دارد. محققان معمولاً عملکرد هر رویکرد را بر روی یک مجموعه داده خاص ارزیابی می‌کنند تا تعیین کنند که کدام رویکرد برای تشخیص حمله ممانعت از

[1] Benchmark Dataset
[2] Truncated Cauchy Distribution
[3] tracing

سرویس در یک سناریوی معین بهتر عمل می‌کند. حکمتی و همکاران [۱۹] مشاهده کردند که هر چهار مدل به فاصله بین ترافیک بی‌آزار و حمله حساس هستند و علاوه بر این، شبکه عصبی حافظه بلندمدت-کوتاه‌مدت بهترین عملکرد کلی را ازنظر دقت بالا و بازیابی بالا ارائه می‌دهد.

٤-٧ محافظت در لایه مه اینترنت اشیا

لایه مه[1] در اینترنت اشیا به یک زیرساخت رایانشی توزیع‌شده اشاره دارد که الگوواره[2] رایانش ابری را تا لبه شبکه، نزدیک‌تر به محل قرارگیری دستگاه‌های اینترنت اشیا، گسترش می‌دهد. لایه مه راهی برای تجزیه‌وتحلیل و پردازش داده‌ها درجایی نزدیک‌تر به منبع، کاهش تأخیر و بهبود عملکرد کلی سیستم را فراهم می‌کند. ازنظر شناسایی و کاهش حملات ممانعت از سرویس، لایه مه می‌تواند جای خوبی برای استقرار الگوریتم‌های یادگیری ماشین بی‌درنگ باشد، ازآن‌رو که لایه مه می‌تواند قدرت رایانشی و منابع لازم را برای تجزیه‌وتحلیل ترافیک شبکه و تشخیص ناهنجاری‌هایی که می‌تواند نشان‌دهنده حمله ممانعت از سرویس باشد فراهم کند. استقرار الگوریتم‌های یادگیری ماشین مقابله با حمله ممانعت از سرویس در لایه مه می‌تواند به کاهش ترافیک کلی شبکه و تخلیه ابر کمک کند و میزان تأثیر حمله‌بر سیستم را کاهش دهد. الگوریتم‌های یادگیری ماشینی می‌توانند الگوهای ترافیک را تجزیه‌وتحلیل کنند و ترافیک غیرعادی را شناسایی کنند و به سیستم اجازه دهند که آن ترافیک را در زمان واقعی مسدود یا کاهش دهد. بااین‌حال، توجه به این نکته مهم است که استقرار الگوریتم‌های یادگیری ماشین در لایه مه مستلزم برنامه‌نویسی و اجرای دقیق است. الگوریتم‌ها باید برای محیط رایانش لبه[3] و منابع موجود بهینه شوند. علاوه بر این، لایه مه، باید ایمن شود تا مهاجمان از به خطر انداختن سیستم و استفاده از آن برای انجام حملات جلوگیری کنند. بااین‌حال، باوجود مزایای گفته‌شده، برنامه‌ریزی و اجرای دقیق برای اطمینان از امنیت و بهینه بودن سیستم برای محیط رایانش لبه ضروری است. به این منظور، بیشنوی و همکاران [۲] معماری یک‌لایه مه باقدرت رایانشی کافی در بالای لایه دستگاه انتهایی را پیاده‌سازی کرده‌اند و از دو مدل مبتنی بر یادگیری عمیق استفاده کرده‌اند. مدل اول شبکه عصبی حافظهٔ بلندمدت-کوتاه‌مدت برای شناسایی داده‌های مخرب از داده‌های معمولی و مدل دوم شبکه عصبی پیچشی برای طبقه‌بندی بیشتر داده‌ها در دسته‌های مختلف حمله. مدل شبکه عصبی حافظهٔ بلندمدت-کوتاه‌مدت دارای دقت ۹۸ درصد و مدل شبکه عصبی پیچشی دارای دقت ۸٦ درصد است.

٤-٨ حملات روز صفر

طبقه‌بندی بسته‌ها با استفاده از شبکه عصبی[4] (NNPC) فنی است که برای طبقه‌بندی بسته‌های شبکه بر اساس محتوای آن‌ها استفاده می‌شود و می‌توان از آن برای محافظت از سرویس‌های شبکه در برابر حملات، ازجمله حملات روز صفر استفاده کرد. حملات روز صفر نوعی حمله هستند که از آسیب‌پذیری‌های ناشناخته در نرم‌افزار سوءاستفاده می‌کنند و شناسایی و جلوگیری از آن را با استفاده از اقدامات امنیتی سنتی دشوار می‌کنند. بااین‌حال، NNPC می‌تواند برای شناسایی و مسدود کردن حملات روز صفر با تجزیه‌وتحلیل محتوای بسته‌های شبکه در زمان واقعی و طبقه‌بندی آن‌ها به‌عنوان مخرب یا بی‌آزار استفاده شود. NNPC را می‌توان بر روی مجموعه‌داده‌های بزرگ ترافیک شبکه برچسب‌گذاری شده آموزش داد تا الگوها و ویژگی‌های مرتبط با انواع مختلف بسته‌های شبکه را یاد بگیرد. پس از آموزش، شبکه عصبی می‌تواند برای طبقه‌بندی بسته‌های دریافتی در زمان واقعی و شناسایی بسته‌های مخربی که با الگوهای آموخته‌شده مطابقت دارند، استفاده شود. با استفاده از NNPC برای طبقه‌بندی بسته‌ها، می‌توان حملات روز صفر را که با هیچ الگوی حمله یا امضای شناخته‌شده‌ای مطابقت ندارند، شناسایی کرد که آن را به یک تکنیک مفید برای محافظت از خدمات شبکه در برابر انواع جدید و ناشناخته حملات تبدیل می‌کند. علاوه بر این، از NNPC می‌توان برای مسدود کردن اتصالات مخرب با حذف بسته‌هایی که به‌عنوان مخرب طبقه‌بندی می‌شوند، استفاده کرد و از رسیدن آن‌ها به مقصد موردنظر جلوگیری کرد. رویز و همکاران [۱۸] عملکرد شبکه‌های عصبی

[1] Fog Layer
[2] Paradigm
[3] Edge Computing Environment
[4] Neural Network Packet Classification

ساده، شبکه عصبی پیچشی و شبکه‌های عصبی بازگشتی را در تشخیص حملات ممانعت از سرویس هنگامی‌که با مجموعه داده CSE-CIC-IDS2018 آموزش داده می‌شوند، ارزیابی کردند. این تحقیق مجموعه‌داده‌های ارائه‌شده و کارایی شبکه‌های پیشنهادی را موردبحث قرارداد.

۴-۹ تهدیدات نام‌های دامنه مخرب

مهاجمان می‌توانند از نام‌های دامنه مخرب[1] برای به خطر انداختن دستگاه‌های اینترنت اشیا که معمولاً فاقد اقدامات امنیتی هستند، به چند روش سوءاستفاده کنند:

۱. فیشینگ: مهاجمان می‌توانند وب‌سایت‌های جعلی بانام‌های دامنه مشابه نام واقعی را برای تولیدکنندگان دستگاه‌های اینترنت اشیا یا ارائه‌دهندگان خدمات قانونی ایجاد کنند. سپس می‌توانند از تکنیک‌های مهندسی اجتماعی، مانند ارسال ایمیل‌های فیشینگ یا پیام‌های متنی برای فریب کاربران برای بازدید از این وب‌سایت‌های جعلی و واردکردن اعتبار ورود به سیستم یا سایر اطلاعات حساس استفاده کنند. هنگامی‌که مهاجمان این اطلاعات را به دست آوردند، می‌توانند از آن برای دسترسی غیرمجاز به دستگاه‌های اینترنت اشیا یا حساب‌های آنلاین کاربر استفاده کنند.

۲. فرمان و کنترل[2] (C2): مهاجمان می‌توانند نام‌های دامنه مخربی ایجاد کنند که میزبان سرورهای C2 مورداستفاده برای کنترل بات‌نت دستگاه‌های اینترنت اشیای در معرض خطر هستند. این بات‌نت‌ها می‌توانند برای راه‌اندازی حملات ممانعت از سرویس، توزیع بدافزار یا سرقت داده‌ها از دستگاه‌های در معرض خطر استفاده شوند.

۳. توزیع بدافزار: مهاجمان می‌توانند نام‌های دامنه مخربی ایجاد کنند که میزبان بدافزار یا کیت‌های سوءاستفاده‌کننده طراحی‌شده برای سوءاستفاده از آسیب‌پذیری‌ها در دستگاه‌های اینترنت اشیا هستند. سپس می‌توانند از ایمیل‌های فیشینگ یا سایر تکنیک‌های مهندسی اجتماعی برای فریب کاربران برای دانلود و نصب بدافزار بر روی دستگاه‌هایشان استفاده کنند. پس از نصب، بدافزار می‌تواند کنترل دستگاه را به مهاجمان بدهد و آن‌ها را قادر به انجام فعالیت‌های مخرب، مانند سرقت داده‌ها یا استفاده از دستگاه به‌عنوان بخشی از بات‌نت کند.

برای کاهش خطر این نوع حملات، سازندگان دستگاه‌های اینترنت اشیا و ارائه‌دهندگان خدمات می‌توانند اقدامات امنیتی مانند احراز هویت دومرحله‌ای، فرآیندهای راه‌اندازی امن و به‌روزرسانی‌های منظم میان‌افزار را برای اصلاح آسیب‌پذیری‌ها انجام دهند. علاوه بر این، کاربران می‌توانند در مورد خطرات حملات فیشینگ و اهمیت هوشیاری هنگام بازدید از وب‌سایت‌ها یا واردکردن اعتبارنامه‌های ورود، آموزش ببینند. فهرست سیاه دامنه و پالایه ترافیک را نیز می‌توان برای مسدود کردن ترافیک به دامنه‌های مخرب شناخته‌شده پیاده‌سازی کرد. درنهایت، الگوریتم‌های یادگیری ماشین می‌توانند برای شناسایی و مسدود کردن ترافیک به دامنه‌های مخرب جدید و ناشناخته استفاده شوند. اسپولدینگ و مُحَیسِن [۱۴] سامانه‌ای به نام D-FENS (سیستم شبکه فیلترینگ و استخراج DNS) را ارائه می‌کند که به‌صورت پشت سر هم با فهرست‌های سیاه‌کار می‌کند و دارای یک سرور DNS زنده و طبقه‌بندی‌کننده باینری برای پیش‌بینی دقیق نام‌های دامنه مخرب گزارش‌نشده است. مدل طبقه‌بندی‌کننده D-FENS در سطح کاراکتر عمل می‌کند و از استفاده از معماری‌های یادگیری عمیق مانند شبکه عصبی پیچشی و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت برای طبقه‌بندی بلادرنگ استفاده می‌کند که نیاز به مهندسی ویژگی که معمولاً با رویکردهای یادگیری ماشین سنتی مرتبط است را کنار می‌گذارد. با منبع‌یابی از مجموعه‌داده‌های آزاد و باز، سیستم ارزیابی می‌شود و به ناحیه ۰,۹۵ زیر منحنی مشخصه عملکرد گیرنده برای طبقه‌بندی باینری دست می‌یابد. با پیش‌بینی دقیق نام‌های دامنه مخرب گزارش‌نشده در زمان واقعی، D-FENS از اتصال ناآگاهانه دستگاه‌های متصل به اینترنت به نام‌های دامنه بالقوه مخرب جلوگیری می‌کند.

۵- انتقادات و چالش‌ها

درحالی‌که یادگیری ماشینی می‌تواند ابزار قدرتمندی برای شناسایی حملات ممانعت از سرویس باشد، شناخت محدودیت‌های آن و ادامه توسعه و اصلاح فناوری برای بهبود دقت و اثربخشی آن در

[1] Malicious Domain Names

[2] Command and Control

طول زمان بسیار مهم است. علاوه بر این، استفاده از یادگیری ماشین در ارتباط با سایر روش‌های تشخیص، مانند تشخیص مبتنی بر امضا و تشخیص ناهنجاری، مهم است تا اطمینان حاصل شود که حملات تا حد امکان دقیق و جامع شناسایی می‌شوند.

یکی از اصلی‌ترین انتقادات به استفاده از یادگیری ماشین برای تشخیص حملات مسدودسازی توزیع‌شده این است که ممکن است به‌سختی اطمینان حاصل شود که مدل یادگیری ماشین به‌اندازه کافی قوی و دقیق باشد تا طیف گسترده‌ای از حملات را تشخیص دهد، درحالی‌که تعداد خیلی کمی از تشخیص‌های مثبت نادرست انجام شود. به‌عبارت‌دیگر، درحالی‌که مدل‌های یادگیری ماشینی می‌توانند در شناسایی انواع خاصی از حملات بسیار مؤثر باشند، ممکن است نتوانند به‌طور دقیق همه انواع حملات ممانعت از سرویس را شناسایی کنند که می‌تواند منجر به هشدارهای نادرست یا شناسایی ازدست‌رفته شود. ازآن‌رو که حملات ممانعت از سرویس می‌توانند ازنظر مقیاس، پیچیدگی و تکنیک‌های مورداستفاده بسیار متفاوت باشند و آموزش یک مدل یادگیری ماشین برای شناسایی دقیق همه این تغییرات می‌تواند چالش‌برانگیز باشد. از سوی دیگر، درحالی‌که شبکه عصبی حافظه بلندمدت–کوتاه‌مدت و شبکه عصبی پیچشی تکنیک‌های یادگیری ماشینی قدرتمندی هستند، اما بدون اشکال نیستند. برخی از معایب احتمالی استفاده از این روش‌ها عبارت‌اند از:

۱– پیچیدگی: طراحی و آموزش مدل‌های شبکه عصبی حافظه بلندمدت–کوتاه‌مدت و شبکه عصبی پیچشی می‌تواند بسیار پیچیده و دشوار باشد، به‌ویژه برای افرادی که با یادگیری عمیق آشنا نیستند. این مدل‌ها ممکن است به منابع رایانشی و زمان قابل‌توجهی برای آموزش نیاز داشته باشند که می‌تواند مانع قابل‌توجهی برای برخی از کاربردها باشد.

۲– بیش‌برازش: مدل‌های یادگیری عمیق در معرض خطر بیش‌برازش هستند که زمانی اتفاق می‌افتد که یک مدل بیش‌ازحد به داده‌های آموزشی فعلی احاطه‌مند می‌شود و در داده‌های جدید و دیده نشده ضعیف عمل می‌کند. اگر مدل بیش‌ازحد پیچیده باشد، یا اگر داده‌های متنوع کافی برای آموزش وجود نداشته باشد، ممکن است بیش‌برازش رخ دهد.

۳– ماهیت جعبه‌سیاه‌گونه: تفسیر یا توضیح مدل‌های یادگیری عمیق ممکن است دشوار باشد. این موضوع می‌تواند در مسائلی که شفافیت و پاسخگویی در آن مهم هستند، مانند مراقبت‌های سلامتی یا مالی، نگران‌کننده باشد.

٤– عدم شفافیت: ویژگی‌هایی که یک مدل شبکه عصبی پیچشی یا شبکه عصبی حافظه بلندمدت–کوتاه‌مدت برای تصمیم‌گیری استفاده می‌کند، اغلب شفاف یا قابل توضیح نیستند. این می‌تواند درک نحوه پردازش داده‌ها توسط مدل و شناسایی و تصحیح خطاها یا سوگیری‌ها را دشوار کند.

۵– الزامات داده: مدل‌های یادگیری عمیق به مقادیر زیادی از داده‌های برچسب‌دار برای آموزش نیاز دارند که ممکن است در برخی از مسائل دسترسی‌ناپذیر یا گران باشد. علاوه بر این، کیفیت و نمایندگی داده‌ها می‌تواند بر عملکرد مدل تأثیر بگذارد.

باوجوداین واقعیت که ترکیب شبکه عصبی حافظه بلندمدت–کوتاه‌مدت و شبکه عصبی پیچشی برای تشخیص ممانعت از سرویس مزایای بالقوه‌ای نیز دارد، بااین‌حال، هنگام ترکیب این دو تکنیک، چالش‌های بالقوه‌ای وجود دارد که باید در نظر گرفته شود. یکی از چالش‌های اصلی این است که شبکه عصبی حافظه بلندمدت–کوتاه‌مدت و شبکه عصبی پیچشی دارای معماری‌های متفاوتی هستند و ممکن است به مراحل پیش‌پردازش متفاوتی برای داده‌های ورودی نیاز داشته باشند. این امر می‌تواند ادغام مؤثر این دو مدل را چالش‌برانگیز کند، زیرا ممکن است به تلاش قابل‌توجهی برای بهینه‌سازی طراحی و آموزش هر مدل به‌طور جداگانه و اطمینان از سازگاری آن‌ها با یکدیگر نیاز باشد. چالش دیگر این است که ترکیب شبکه عصبی حافظه بلندمدت–کوتاه‌مدت و شبکه عصبی پیچشی ممکن است پیچیدگی مدل را افزایش دهد که می‌تواند آموزش و بهینه‌سازی آن را دشوارتر کند. علاوه بر این، ممکن است تفسیر نتایج یک مدل ترکیبی چالش‌برانگیزتر باشد، زیرا عملکرد درونی هر مدل ممکن است شفاف یا به‌راحتی قابل وصف نباشد.

معایب و چالش‌های متعددی در مورد مجموعه‌داده‌های حمله ممانعت از سرویس وجود دارد که می‌تواند بر اثربخشی مدل‌های

یادگیری ماشین برای تشخیص ممانعت از سرویس تأثیر بگذارد. برخی از معایب و چالش‌های اصلی عبارت‌اند از:

۱- اندازه و تنوع محدود: بسیاری از مجموعه‌داده‌های ممانعت از سرویس در دسترس عموم ازنظر اندازه محدود هستند و ممکن است طیف وسیعی از انواع یا تغییرات حمله را شامل نشوند. این می‌تواند آموزش مدل‌های یادگیری ماشینی را که برای تشخیص طیف گسترده‌ای از حملات به‌اندازه کافی قوی و دقیق هستند، دشوار کند.

۲- عدم برچسب‌گذاری: استفاده از مجموعه‌های داده‌هایی که برچسب‌گذاری نشده‌اند برای یادگیری ماشینی نظارت‌شده ممکن است دشوار باشد. برچسب‌گذاری داده‌ها می‌تواند زمان‌بر و منابع‌بر باشد، به‌ویژه برای حملات ممانعت از سرویس که تشخیص آن از ترافیک عادی دشوار است.

۳- داده‌های نامتعادل: حملات ممانعت از سرویس در مقایسه با ترافیک عادی شبکه نسبتاً نادر هستند و این می‌تواند منجر به ایجاد مجموعه‌داده‌های نامتعادل شود که می‌تواند بر عملکرد مدل‌های یادگیری ماشین تأثیر منفی بگذارد. مدل‌ها ممکن است به سمت طبقه اکثریت (ترافیک عادی) سوگیری داشته باشند که منجر به نرخ‌های منفی کاذب بالا می‌شود.

٤- نگرانی‌های مربوط به حریم خصوصی داده‌ها: داده‌های حمله ممانعت از سرویس ممکن است حاوی اطلاعات حساسی باشد که نتوان آن‌ها را به‌صورت عمومی به اشتراک گذاشت و در دسترس بودن مجموعه‌داده‌های با کیفیت بالا برای یادگیری ماشین را محدود می‌کند. علاوه بر این، سازمان‌ها ممکن است تمایلی به اشتراک‌گذاری داده‌های مربوط به ترافیک شبکه خود نداشته باشند، به‌ویژه اگر حمله ممانعت از سرویس را تجربه کرده باشند.

۵- کیفیت داده‌ها: کیفیت مجموعه‌داده‌های حمله ممانعت از سرویس می‌تواند بسیار متفاوت باشد، به‌ویژه اگر داده‌ها از منابع مختلف با ابزارها یا روش‌های اندازه‌گیری متفاوت به‌دست‌آمده باشند. داده‌های با کیفیت پایین می‌توانند بر عملکرد مدل‌های یادگیری ماشین تأثیر منفی بگذارند.

انتقادات متعددی در مورداستفاده از شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی برای شناسایی حملات ممانعت از سرویس توزیع‌شده مطرح شده است. برخی از انتقادات اصلی عبارت‌اند از:

۱- بیش‌برازش: مدل‌های یادگیری عمیق، ازجمله شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی، می‌توانند مستعد بیش‌برازش باشند که در آن مدل بیش‌ازحد پیچیده است و یاد می‌گیرد که داده‌های آموزشی را دقیقاً تقلید کند. این می‌تواند منجر به تعمیم ضعیف به داده‌های جدید و دیده نشده شود که می‌تواند بر اثربخشی مدل برای شناسایی حملات ممانعت از سرویس تأثیر بگذارد.

۲- پیچیدگی رایانشی: آموزش و استفاده از مدل‌های یادگیری عمیق، به‌ویژه آن‌هایی که لایه‌های زیادی دارند، می‌توانند ازنظر رایانشی گران باشند. این می‌تواند مفید بودن آن‌ها را در برنامه‌های بلادرنگ که در آن شناسایی با تأخیر کم موردنیاز است، محدود کند.

۳- تفسیرپذیری: تفسیر مدل‌های یادگیری عمیق ممکن است دشوار باشد، و درک اینکه چگونه مدل به پیش‌بینی‌هایش می‌رسد، چالش‌برانگیز است. این موضوع می‌تواند شناسایی مشخصات یا ویژگی‌های خاصی را که مدل برای شناسایی حملات ممانعت از سرویس استفاده می‌کند، دشوار کند.

٤- محدودیت‌های داده: همان‌طور که در قبل ذکر شد، مجموعه‌داده‌های حمله ممانعت از سرویس می‌تواند محدودیت‌هایی داشته باشد که می‌تواند بر اثربخشی مدل‌های یادگیری ماشین تأثیر بگذارد. این محدودیت‌ها می‌تواند شامل داده‌های نامتعادل، اندازه و تنوع محدود، عدم برچسب‌گذاری و مسائل مربوط به کیفیت داده باشد.

۵- حملات خصمانه: حملات ممانعت از سرویس می‌توانند هدفمند و پیچیده باشند و این امکان برای مهاجمان وجود دارد که با توسعه حملاتی که به‌طور خاص برای دور زدن مدل‌های یادگیری ماشین طراحی‌شده‌اند، از شناسایی فرار کنند.

٦- محدودیت‌های متنی: مدل‌های یادگیری ماشین، ازجمله شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی، می‌توانند به تغییرات در محیط یا زمینه‌ای که در آن آموزش داده‌شده یا به کار گرفته‌شده‌اند حساس باشند. این می‌تواند توانایی مدل را

برای تعمیم به محیط‌های جدید یا سازگاری با تغییرات در ترافیک شبکه محدود کند.

درحالی‌که مطمئناً انتقادات و محدودیت‌هایی در رابطه با استفاده از شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی برای شناسایی حملات ممانعت از سرویس توزیع‌شده وجود دارد، مزایای متعددی نیز وجود دارد که می‌تواند این انتقادات را جبران کند. برخی از جنبه‌های واضح اصلی استفاده از شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی برای تشخیص ممانعت از سرویس عبارت‌اند از:

۱- توانایی مدیریت داده‌های پیچیده: شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی برای مدیریت داده‌های پیچیده، مانند داده‌های سری زمانی یا داده‌هایی با روابط فضایی، مناسب هستند. این باعث می‌شود که آن‌ها برای شناسایی حملات ممانعت از سرویس هم مناسب باشند که می‌تواند طیف گسترده‌ای از انواع و روش‌های مختلف حمله را شامل شود.

۲- دقت بالا: هنگامی‌که مدل‌های شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی به‌درستی آموزش داده‌شده و به کار گرفته شوند، می‌توانند به سطوح بالایی از دقت در تشخیص حملات ممانعت از سرویس دست یابند. این می‌تواند به بهبود امنیت کلی یک شبکه و کاهش تأثیر حملات کمک کند.

۳- شناسایی بلادرنگ: شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی را می‌توان برای شناسایی بلادرنگ حملات ممانعت از سرویس مورداستفاده قرارداد که به مدیران شبکه اجازه می‌دهد به‌سرعت به تهدیدات پاسخ دهند و تأثیر حمله را به حداقل برسانند.

٤- توانایی تشخیص حملات تجربه‌نشده قبلی: مدل‌های یادگیری عمیق، ازجمله شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی، می‌توانند در تشخیص حملات تجربه‌نشده یا جدید قبلی مؤثر باشند. این امر می‌تواند به‌ویژه در چشم‌انداز حملات سایبری به‌سرعت در حال تحول ارزشمند باشد.

۵- استخراج خودکار ویژگی‌ها: مدل‌های یادگیری عمیق می‌توانند به‌طور خودکار استخراج ویژگی‌های مرتبط از داده‌های ورودی را بیاموزند که می‌تواند به کاهش نیاز به کشف ویژگی‌های دستی کمک کند. این می‌تواند باعث صرفه‌جویی در زمان و بهبود عملکرد کلی مدل شود.

با آموزش و استقرار دقیق، مدل‌های شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی می‌توانند ابزار قدرتمندی برای بهبود امنیت و انعطاف‌پذیری شبکه‌ها در برابر حملات ممانعت از سرویس باشند.

٦- پیاده‌سازی و بررسی نتایج

با استفاده از مجموعه داده UNSW-NB15 که توسط دانشگاه نیوساوت‌ولز استرالیا منتشر شده است [۲۱]، و تقسیم داده‌ها به دو گروه آموزش و آزمون، هر دو شبکه عصبی پیچشی و حافظه بلندمدت-کوتاه‌مدت و همچنین مدلی ترکیبی جدیدی بر اساس ادغام هر دو روش پیاده‌سازی شده است. مجموعه داده UNSW-NB15، شامل ٤٩ ویژگی (ستون) و حدود ۲/۵ میلیون سطر ترافیک است. مجموعه داده UNSW-NB15 یک مجموعه داده معیار شناخته‌شده و با کاربرد گسترده درزمینه امنیت شبکه است. این مجموعه داده برای تسهیل تحقیق و توسعه درزمینه سیستم‌های تشخیص نفوذ و تحلیل رفتار شبکه ایجادشده است. این مجموعه داده شامل مجموعه‌ای جامع از داده‌های ترافیک شبکه در دنیای واقعی است که در یک محیط شبکه کنترل‌شده ضبط‌شده است و طیف وسیعی از حملات شبکه و فعالیت‌های عادی را در برمی‌گیرد و منبع ارزشمندی برای ارزیابی و بهبود اثربخشی الگوریتم‌ها و تکنیک‌های مختلف امنیت سایبری است. مجموعه داده UNSW-NB15 نقشی اساسی در پیشرفت درک تهدیدات امنیتی شبکه ایفا کرده است و محققان و متخصصان را قادر می‌سازد تا انعطاف‌پذیری و حفاظت از شبکه‌های کامپیوتری را افزایش دهند.

در ادامه فرمول‌های ریاضی برای معیارهای ارزیابی با استفاده از حروف لاتین و نام‌گذاری متغیرها آمده است. در این فرمول‌ها، متغیرها به مفهوم زیر است:

- TP: تعداد مثبت‌های صحیح (True Positives) - تعداد نمونه‌هایی که به‌درستی به‌عنوان مثبت تشخیص داده‌شده‌اند
- TN: تعداد منفی‌های صحیح (True Negatives) - تعداد نمونه‌هایی که به‌درستی به‌عنوان منفی تشخیص داده‌شده‌اند

- FP: تعداد مثبت‌های غلط (False Positives) – تعداد نمونه‌هایی که به‌طور نادرست به‌عنوان مثبت تشخیص داده‌شده‌اند
- FN: تعداد منفی‌های غلط (False Negatives) – تعداد نمونه‌هایی که به‌طور نادرست به‌عنوان منفی تشخیص داده‌شده‌اند.

۱- درستی (Accuracy):

درستی میزان تشخیص‌های صحیح در میان کل تشخیص‌ها را نمایش می‌دهد. یعنی میزان صحت کلی تشخیص‌های منفی یا مثبت ترافیک مورد ارزیابی. این معیار نشان می‌دهد که سیستم تشخیص نفوذ چه میزان در به‌درستی حمله یا عادی ارزیابی کردن ترافیک شبکه موفق است.

$$Accuracy = (TP + TN) / (TP + TN + FP + FN)$$

۲- دقت (Precision):

دقت، میزان صحیح بودن مواردی که به‌درستی به‌عنوان مثبت درنظر گرفته شدند به‌کل نمونه‌های مثبت‌فرض‌شده را نمایش می‌دهد، یعنی میزان پیش‌بینی‌های مثبت صحیح به‌کل پیش‌بینی‌های مثبت (مثبت صحیح و مثبت ناصحیح). این معیار نشان می‌دهد که از نمونه‌هایی که سیستم تشخیص نفوذ آن‌ها را به‌عنوان حمله تشخیص داده است، چه میزانی واقعاً حمله بوده‌اند.

$$Precision = TP / (TP + FP)$$

۳- بازیابی (Recall):

نسبت تعداد نمونه‌های مثبت به‌درستی تشخیص‌داده‌شده به‌کل نمونه‌های واقعی مثبت (تشخیص‌داده‌شده یا نشده) را نشان می‌دهد. برای محاسبه بازیابی، تعداد نمونه‌های حقیقی مثبت (حمله) تشخیص‌داده‌شده بر تعداد کل نمونه‌های حقیقی مثبت، شامل نمونه‌های مثبتی که سیستم تشخیص نفوذ آن‌ها را به‌درستی تشخیص داده و نمونه‌های مثبتی که آن‌ها را به اشتباه به‌عنوان منفی تشخیص داده است، تقسیم می‌شود.

$$Recall = TP / (TP + FN)$$

٤- امتیاز F1:

یک معیار ترکیبی است که دقت و بازیابی را ترکیب می‌کند. این معیار نشان می‌دهد چه توازنی بین دقت و بازیابی مدل وجود دارد. امتیاز F1 بین ۰ و ۱ قرار می‌گیرد، و هرچه به ۱ نزدیک‌تر باشد، نشان‌دهنده عملکرد بهتر مدل است.

$$F1\ Score = 2 * (Precision * Recall) / (Precision + Recall)$$

با استفاده از این فرمول‌ها و نام‌گذاری مناسب متغیرها، می‌توان عملکرد مدل را به‌صورت کمّی ارزیابی کرد.

همان‌طور که در **Error! Reference source not found.** آمده است، برای بررسی تأثیر میزان اثرگذاری مقادیر آموزش بر نتیجه نهایی، آموزش ابتدا با ده درصد داده‌ها انجام می‌شود و آزمون بر روی نود درصد باقی‌مانده انجام می‌شود. در مراحل بعدی داده‌های گروه آموزش به میزان ده درصد دیگر از کل داده‌ها افزایش‌یافته و داده‌های گروه آزمون به همین میزان کاهش می‌یابد. نتایج به‌دست‌آمده از تحقیقات ما، که در آن الگوریتم‌های حافظه بلندمدت-کوتاه‌مدت، شبکه عصبی پیچشی و مدل جدیدی که در این پژوهش از ترکیب دو روش قبلی ساخته‌شده است، را برای شناسایی حملات ممانعت از سرویس بر روی مجموعه داده به کار بردیم، بینش‌های ارزشمندی را در مورد عملکرد این الگوریتم‌ها در درصدهای مختلف داده‌های آموزشی ارائه می‌دهد. در ادامه نتایج حاصله تفسیر می‌شود که خروجی‌ها درزمینه تشخیص ممانعت از سرویس چه چیزی را نشان می‌دهد.

٦-١ نتایج حافظه بلندمدت-کوتاه‌مدت

الگوریتم حافظه بلندمدت-کوتاه‌مدت به‌طور مداوم عملکرد قدرتمندی را در تشخیص حملات ممانعت از سرویس در درصدهای مختلف داده‌های آموزشی نشان می‌دهد. مقادیر درستی بالا از ۰,۹۹۰ تا ۰,۹۹٤ نشان می‌دهد که الگوریتم حافظه بلندمدت-کوتاه‌مدت در طبقه‌بندی دقیق نمونه‌های عادی و حمله کارآمد است. مقادیر دقت از ۰,۸۱۳ تا ۰,۹۰۹ توانایی الگوریتم را در شناسایی صحیح حملات ممانعت از سرویس و به حداقل رساندن موارد مثبت کاذب نشان می‌دهد. مقادیر بازیابی از ۰,۷۹۲ تا ۰,۹۷۰ نشان می‌دهد که الگوریتم حافظه بلندمدت-کوتاه‌مدت نسبت بالایی از حملات ممانعت از سرویس واقعی را کشف می‌کند. امتیاز F1 از ۰,۸٤۷ تا ۰,۹۱٤ نشان‌دهنده یک توازن بالا بین دقت و بازیابی است که اثربخشی کلی الگوریتم را در تشخیص حملات ممانعت از سرویس نشان می‌دهد.

جدول ۱- مقایسه عملکرد الگوریتم‌های تشخیص حمله ممانعت از سرویس با استفاده از LSTM، CNN و روش پیشنهادی

F1 روش پیشنهادی	بازیابی روش پیشنهادی	دقت روش پیشنهادی	درستی روش پیشنهادی	F1 امتیاز CNN	بازیابی CNN	دقت CNN	درستی CNN	امتیاز F1 LSTM	بازیابی LSTM	دقت LSTM	درستی LSTM	معیار/درصد آموزش انجام‌شده
۰/۹۰۱	۰/۹۲۹	۰/۸۷٤	**۰/۹۹٤**	۰/۳۵۷	۰/۲۳۹	۰/۷۰۲	۰/۹۷۳	۰/۷۹٦	۰/۸۰۰	۰/۷۹۳	۰/۹۸۷	۱۰
۰/۸۹٤	۰/۸۹۳	۰/۸۹٦	**۰/۹۹۳**	۰/۷۹٦	**۰/۹۹۹**	۰/٦٦۱	۰/۹۸٤	۰/۸۱۸	۰/۸۱٤	۰/۸۲۲	۰/۹۸۹	۲۰
۰/۸٤۷	۰/۷۹۲	۰/۹۱۰	**۰/۹۹۱**	۰/۷۱۵	۱/۰۰۰	۰/۵۵۷	۰/۹۷۵	۰/۷۹۳	۰/۷۹٤	۰/۷۹۳	۰/۹۸۷	۳۰
۰/۹۰٤	۰/۹۳۱	۰/۸۷۹	**۰/۹۹٤**	۰/۸۹۳	۱/۰۰۰	۰/۸۰۷	**۰/۹۹۲**	۰/۷۹۵	۰/۷۸٦	۰/۸۰۳	۰/۹۸۷	٤۰
۰/۸۹۸	۰/۹۳۱	۰/۸٦۷	**۰/۹۹۳**	۰/۰۰۱	۱/۰۰۰	۱/۰۰۰	۰/۹٦۸	۰/۸۵۱	۰/۹۰۷	۰/۸۰۲	**۰/۹۹۰**	۵۰
۰/۹۰٦	۰/۹۷۱	۰/۸۵۰	**۰/۹۹٤**	۰/۷۹۳	۱/۰۰۰	۰/٦۵۷	۰/۹۸٤	۰/۸۵۳	۰/۹۱۸	۰/۷۹۷	**۰/۹۹۰**	٦۰
۰/۹۱٤	۰/۹۲۹	۰/۹۰۰	**۰/۹۹٤**	۰/۰۰۱	۰/۰۰۰	۱/۰۰۰	۰/۹٦۸	۰/۸۵٦	۰/۹۰۲	۰/۸۱٤	**۰/۹۹۰**	۷۰
۰/۹۱۳	۰/۹۷۹	۰/۸۵۵	**۰/۹۹٤**	۰/۰۰۱	۰/۰۰۰	۱/۰۰۰	۰/۹٦۸	۰/۸۷۳	۰/۹۳۹	۰/۸۱۵	**۰/۹۹۱**	۸۰
۰/۹۰۰	۰/۹٤۰	۰/۸٦۲	**۰/۹۹۳**	۰/۷۸۳	۱/۰۰۰	۰/٦٤۳	۰/۹۸۲	۰/۸٦۵	۰/۹۲٤	۰/۸۱۳	**۰/۹۹۱**	۹۰

٦-۲ نتایج شبکه عصبی پیچشی

الگوریتم شبکه عصبی پیچشی عملکرد متغیری را در تشخیص حملات ممانعت از سرویس در درصدهای مختلف آموزش بر روی داده‌های آموزشی را نشان می‌دهد. درحالی‌که درستی آن از ۰,۹٦۷ تا ۰,۹۹۲ متغیر است، که نوسانات زیادی را نشان می‌دهد، به مقادیر دقت نسبتاً بالایی در محدوده ۰,۵۵٦ تا ۱,۰۰۰ دست می‌یابد که نشان‌دهنده توانایی آن در طبقه‌بندی صحیح حملات ممانعت از سرویس است. بااین‌حال، مقادیر بازیابی برای شبکه عصبی پیچشی محدودیت‌هایی را نشان می‌دهد، با مقادیری از ۰,۰۰۰۲۷۱ تا ۱,۰۰۰ این نشان می‌دهد که الگوریتم شبکه عصبی پیچشی ممکن است برای ثبت دقیق تمام نمونه‌های حملات تلاش کند. درنتیجه، امتیازات F1 از ۰,۰۰۰۵٤۳ تا ۰,۸۹۵ تأثیر مقادیر بازیابی نامتعادل را بر عملکرد کلی را برجسته می‌کند.

٦-۳ نتایج روش ترکیبی پیشنهادی

روش ترکیبی مبتنی بر LSTM-CNN به‌طور مداوم عملکرد بالایی در شناسایی حملات ممانعت از سرویس در تمام درصدهای ارزیابی‌شده داده‌های آموزشی ارائه می‌دهد. مقادیر درستی از ۰,۹۹۰ تا ۰,۹۹٤ توانایی الگوریتم را در طبقه‌بندی دقیق هر دو نمونه ترافیک عادی و حمله نشان می‌دهد. مقادیر دقت از ۰,۸٤۳ تا ۰,۹۰۹ نشان‌دهنده اثربخشی الگوریتم در شناسایی صحیح حملات ممانعت از سرویس است. مقادیر بازیابی از ۰,۷۹۲ تا ۰,۹۷۰ نشان می‌دهد که الگوریتم نسبت بالایی از حملات واقعی را ثبت می‌کند. نمرات F1 از ۰,۸٤۷ تا ۰,۹۱٤ نشان‌دهنده توازن بالایی بین دقت و بازیابی است.

٦-٤ تفسیر

نتایج نشان می‌دهد که هر دو الگوریتم حافظه بلندمدت-کوتاه‌مدت و الگوریتم ترکیبی پیشنهادی LSTM-CNN به‌طور مداوم در

تشخیص حملات ممانعت از سرویس از الگوریتم شبکه عصبی پیچشی بهتر عمل می‌کنند، همان‌طور که با درستی، دقت، بازیابی و امتیازات F1 بالاتر نشان داده می‌شوند. این نتایج باقابلیت‌های ذاتی معماری‌های حافظه بلندمدت-کوتاه‌مدت و LSTM-CNN درگرفتن وابستگی‌ها و الگوهای زمانی در داده‌های متوالی هماهنگ است.

الگوریتم حافظه بلندمدت-کوتاه‌مدت، که به دلیل توانایی خود در گرفتن وابستگی‌های طولانی‌مدت شناخته‌شده است، در اکثر درصد داده‌های آموزشی عملکرد قابل‌توجهی دارد. این نشان می‌دهد که این الگوریتم به‌طور مؤثر الگوهای زمانی مرتبط با حملات ممانعت از سرویس را یاد می‌گیرد و منجر به تشخیص دقیق می‌شود. روش LSTM-CNN، با ترکیب نقاط قوت حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی، به‌طور مداوم به عملکرد بالایی دست می‌یابد و آن را به یک انتخاب قابل‌اتکا برای تشخیص ممانعت از سرویس تبدیل می‌کند، به‌ویژه هنگامی‌که با داده‌های پیچیده‌ای که شامل جنبه‌های ترتیبی و فضایی هستند، سروکار داریم.

از سوی دیگر، عملکرد الگوریتم شبکه عصبی پیچشی نوسان دارد و محدودیت‌هایی را در ثبت دقیق تمام نمونه‌های حملات ممانعت از سرویس نشان می‌دهد. درحالی‌که شبکه‌های عصبی پیچشی در گرفتن اطلاعات فضایی عالی هستند، ناتوانی آن‌ها در مدل‌سازی مؤثر وابستگی‌های بلندمدت ممکن است منجر به عملکرد کمتر بهینه آن‌ها در تشخیص ممانعت از سرویس شود.

به‌طورکلی، نتایج، اهمیت در نظر گرفتن ویژگی‌های داده‌ها و الزامات خاص وظیفه تشخیص ممانعت از سرویس را هنگام انتخاب یک الگوریتم برجسته می‌کند. الگوریتم‌های حافظه بلندمدت-کوتاه‌مدت و LSTM-CNN، با توانایی خود در گرفتن وابستگی‌های زمانی، گزینه‌های قدرتمندی برای تشخیص دقیق ممانعت از سرویس هستند. تحقیقات آینده ممکن است رویکردهای ترکیبی یا روش‌های مجموعه‌ای را برای افزایش بیشتر عملکرد با استفاده از نقاط قوت مکمل معماری‌های حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی بررسی کنند.

نتایج پیاده‌سازی ما بینش‌های ارزشمندی در مورد عملکرد الگوریتم‌های حافظه بلندمدت-کوتاه‌مدت، شبکه عصبی پیچشی و LSTM-CNN در تشخیص ممانعت از سرویس ارائه می‌کند. با درک پیامدهای نتایج، محققان و دست‌اندرکاران می‌توانند تصمیمات آگاهانه‌ای در مورد انتخاب الگوریتم‌های مناسب بر اساس ویژگی‌های خاص داده‌ها و معیارهای عملکرد موردنظر بگیرند.

۷- نتیجه‌گیری

شبکه‌های عصبی پیچشی و حافظه بلندمدت-کوتاه‌مدت می‌توانند به شناسایی حملات ممانعت از سرویس توزیع‌شده کمک کنند، زیرا آن‌ها قادر به یادگیری الگوها و روابط پیچیده در داده‌ها هستند که برای تمایز بین ترافیک عادی و مخرب مهم است. شبکه‌های عصبی پیچشی، به‌ویژه در تشخیص الگوهای چندبعدی در داده‌ها، مانند انواع و اندازه‌های بسته‌های شبکه مؤثر هستند که می‌تواند برای شناسایی حملات ممانعت از سرویس که شامل اندازه‌ها یا ساختارهای بسته غیرعادی است، مفید باشد. شبکه‌های عصبی پیچشی همچنین می‌توانند در مورد ویژگی‌های پروتکل‌ها یا سرویس‌های شبکه‌ای مانند DNS یا HTTP آموزش ببینند که می‌تواند به شناسایی حملاتی که آن سرویس‌ها را هدف قرار می‌دهند کمک کند. از سوی دیگر، شبکه‌های عصبی حافظه بلندمدت-کوتاه‌مدت برای تجزیه‌وتحلیل توالی داده‌ها طراحی‌شده‌اند و برای تشخیص الگوهای زمانی در داده‌های سری زمانی، مانند جریان‌های ترافیک شبکه، مناسب هستند. آن‌ها می‌توانند یاد بگیرند که الگوهای ترافیک عادی را تشخیص دهند و انحرافات از آن الگوها را که می‌تواند نشان‌دهنده حمله ممانعت از سرویس باشد، شناسایی کنند. هر دو شبکه عصبی پیچشی و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت را می‌توان برای ایجاد مدل‌های ترکیبی که از نقاط قوت هر دو معماری بهره می‌برد، ترکیب کرد. به‌عنوان‌مثال، یک شبکه عصبی پیچشی می‌تواند برای استخراج ویژگی‌های اولیه داده‌های ورودی استفاده شود و ویژگی‌های حاصل می‌تواند برای تجزیه‌وتحلیل بیشتر و تشخیص الگوهای زمانی به یک شبکه عصبی حافظه بلندمدت-کوتاه‌مدت وارد شود.

انتخاب بین استفاده از یک شبکه عصبی پیچشی یا یک شبکه عصبی حافظه بلندمدت-کوتاه‌مدت برای شناسایی حملات ممانعت

از سرویس به ویژگی‌های خاص داده‌های مورد تجزیه‌وتحلیل و ویژگی‌هایی که برای شناسایی حملات مهم هستند، بستگی دارد. به‌طورکلی، برای تشخیص حمله ممانعت از سرویس، انتخاب بین استفاده از شبکه عصبی پیچشی یا شبکه عصبی حافظه بلندمدت-کوتاه‌مدت ممکن است به نوع داده‌های مورد تجزیه‌وتحلیل بستگی داشته باشد. برای مثال، اگر داده‌های مورد تجزیه‌وتحلیل شامل بسته‌های شبکه باشد، شبکه‌های عصبی پیچشی ممکن است برای شناسایی حملات ممانعت از سرویس مناسب‌تر باشند. شبکه‌های عصبی پیچشی می‌توانند ویژگی‌های چندبعدی مانند اندازه و شکل بسته‌های شبکه را بیاموزند و می‌توانند برای تشخیص ناهنجاری‌ها در ساختار بسته‌های شبکه یا ترافیک شبکه استفاده شوند. از سوی دیگر، اگر داده‌های مورد تجزیه‌وتحلیل شامل جریان‌های ترافیک شبکه باشد که می‌تواند به‌صورت دنباله‌ای از بسته‌ها در طول زمان نمایش داده شود، یک شبکه عصبی حافظه بلندمدت-کوتاه‌مدت ممکن است برای شناسایی حملات ممانعت از سرویس مناسب‌تر باشد. شبکه‌های عصبی حافظه بلندمدت-کوتاه‌مدت می‌توانند روابط زمانی بین بسته‌ها را در جریان ترافیک بیاموزند و الگوهای غیرعادی ترافیک را که نشان‌دهنده حمله ممانعت از سرویس هستند، شناسایی کنند.

درحالی‌که شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی می‌توانند تکنیک‌های قدرتمندی برای شناسایی حملات ممانعت از سرویس باشند، مهم است که از محدودیت‌ها و چالش‌های بالقوه مرتبط با این فن‌ها آگاه باشیم. با تلاش برای رفع آن‌ها، ممکن است بتوان مدل‌های مؤثرتری برای شناسایی حملات ممانعت از سرویس با استفاده از یادگیری عمیق ایجاد کرد. شبکه‌های عصبی پیچشی برای شناسایی حملات ممانعت از سرویس مناسب هستند زیرا می‌توانند به‌طور خودکار ویژگی‌هایی را از داده‌های ترافیک شبکه خام یاد بگیرند، مانند اندازه بسته، زمان‌بندی و آدرس‌های منبع/مقصد. این باعث می‌شود که آن‌ها به‌ویژه برای شناسایی حملاتی که با استفاده از روش‌های سنتی مبتنی بر قاعده تشخیص آن‌ها دشوار است مفید باشند. علاوه بر این، شبکه‌های عصبی پیچشی قادر به پردازش موازی هستند که آن‌ها را برای پردازش حجم زیادی از داده‌های ترافیک شبکه کارآمد می‌کند. از سوی دیگر، شبکه‌های عصبی حافظه بلندمدت-کوتاه‌مدت به‌ویژه برای تشخیص الگوهای غیرعادی در داده‌های ترافیک شبکه مفید هستند. آن‌ها می‌توانند وابستگی‌های زمانی در داده‌ها را یاد بگیرند و می‌توانند برای مدل‌سازی توالی بسته‌های شبکه در طول زمان استفاده شوند. این باعث می‌شود که آن‌ها برای تشخیص حملات آهسته مناسب باشند که ممکن است الگوهای مشابه حملات با حجم بالا را نشان ندهند.

ما پیش‌بینی می‌کنیم که در آینده، شبکه عصبی حافظه بلندمدت-کوتاه‌مدت و شبکه عصبی پیچشی به‌طور گسترده برای شناسایی حملات ممانعت از سرویس مورداستفاده قرار می‌گیرند و حتی ممکن است با ادامه پیشرفت حوزه یادگیری عمیق، پیچیده‌تر و دقیق‌تر شوند. به‌طورکلی، ترکیب شبکه عصبی پیچشی و شبکه عصبی حافظه بلندمدت-کوتاه‌مدت یک رویکرد قدرتمند برای شناسایی حملات ممانعت از سرویس است و ما معتقدیم که با ادامه تکامل فناوری، شاهد پیشرفت و بهبود در این زمینه خواهیم بود.

References

[1] Z. Liu, J. Yu, B. Yan, and G. Wang, “A deep 1-D CNN and bidirectional LSTM ensemble model with arbitration mechanism for LDDoS attack detection,” IEEE Trans. Emerg. Top. Comput. Intell., vol. 6, no. 6, pp. 1396–1410, Dec. 2022.

[2] S. Bishnoi, S. Mohanty, and B. Sahoo, “A deep learning-based methodology in fog environment for DDoS attack detection,” in 2021 5th international conference on computing methodologies and communication (ICCMC), Apr. 2021, pp. 201–206.

[3] Á. L. Perales Gómez, L. F. Maimó, F. J. G. Clemente, J. A. M. Morales, A. H. Celdrán, and G. Bovet, “A methodology for evaluating the robustness of anomaly detectors to adversarial attacks in industrial scenarios,” IEEE Access Pract. Innov. Open Solut., vol. 10, pp. 124582–124594, 2022.

[4] M. I. Sayed, I. M. Sayem, S. Saha, and A. Haque, “A multi-classifier for DDoS attacks using stacking ensemble deep neural network,” in 2022 international wireless communications and mobile computing (IWCMC), May 2022, pp 1125–1130.

[5] A. Zainudin, L. A. C. Ahakonye, R. Akter, D.-S. Kim, and J.-M. Lee, “An efficient hybrid-DNN for DDoS detection and classification in software-

[16] M. Ahsan, N. Rifat, M. Chowdhury, and R. Gomes, “Intrusion detection for IoT network security with deep neural network,” in 2022 IEEE international conference on electro information technology (eIT), May 2022, pp. 467–472.
[17] M. H. Haghighat and J. Li, “Intrusion detection system using voting-based neural network,” Tsinghua Sci. Technol., vol. 26, no. 4, pp. 484–495, Aug. 2021.
[18] N. Ruiz, B. Tavera, and A.-S. Abuzneid, “Intrusion detection system: The use of neural network packet classification,” in 2020 international conference on computational science and computational intelligence (CSCI), Dec. 2020, pp. 1276–1281.
[19] Hekmati, E. Grippo, and B. Krishnamachari, “Neural networks for DoS attack detection using an enhanced urban IoT dataset,” in 2022 international conference on computer communications and networks (ICCCN), Jul. 2022, pp. 1–8.
[20] M. Basnet, S. Poudyal, Mohd. H. Ali, and D. Dasgupta, “Ransomware detection using deep learning in the SCADA system of electric vehicle charging station,” in 2021 IEEE PES innovative smart grid technologies conference - latin america (ISGT latin america), Sep. 2021, pp. 1–5.
[21] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "Netflow datasets for machine learning-based network intrusion detection systems," in Big Data Technologies and Applications: 10th EAI International Conference, BDTA 2020, and 13th EAI International Conference on Wireless Internet, WiCON 2020, Virtual Event, December 11, 2020, Proceedings, vol. 10, pp. 117-135, Springer International Publishing, 2021.
defined IIoT networks,” IEEE Internet Things J., pp. 1–1, 2022.
[6] C. Yue, L. Wang, D. Wang, R. Duo, and X. Nie, “An ensemble intrusion detection method for train ethernet consist network based on CNN and RNN,” IEEE Access Pract. Innov. Open Solut., vol. 9, pp. 59527–59539, 2021.
[7] M. Roopak, G. Y. Tian, and J. Chambers, “An intrusion detection system against DDoS attacks in IoT networks,” in 2020 10th annual computing and communication workshop and conference (CCWC), Jan. 2020, pp. 0562–0567.
[8] J. Mao, M. Zhang, and Q. Xu, “CNN and LSTM based data-driven cyberattack detection for grid-connected PV inverter,” in 2022 IEEE 17th international conference on control & automation (ICCA), Jun. 2022, pp. 704–709.
[9] V. Gaur and R. Kumar, “DDoSLSTM: Detection of distributed denial of service attacks on IoT devices using LSTM model,” in 2022 international conference on communication, computing and internet of things (IC3IoT), Mar. 2022, pp. 01–07.
[10] Vaswani et al., “Attention is all you need,” in Advances in neural information processing systems, 2017, vol. 30.
[11] T. Lee, L. Chang, and C. Syu, “Deep Learning Enabled Intrusion Detection and Prevention System over SDN Networks,” in 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Jun. 2020, pp. 1–6.
[12] M. Roopak, G. Yun Tian, and J. Chambers, “Deep learning models for cyber security in IoT networks,” in 2019 IEEE 9th annual computing and communication workshop and conference (CCWC), Jan. 2019, pp. 0452–0457.
[13] B. Nugraha and R. N. Murthy, “Deep learning-based slow DDoS attack detection in SDN-based networks,” in 2020 IEEE conference on network function virtualization and software defined networks (NFV-SDN), Nov. 2020, pp. 51–56.
[14] J. Spaulding and A. Mohaisen, “Defending internet of things against malicious domain names using D-FENS,” in 2018 IEEE/ACM symposium on edge computing (SEC), Oct. 2018, pp. 387–392.
[15] V. Kachavimath and Narayan D. G, “Distributed denial of service attacks detection using deep learning in software defined network,” in 2022 13th international conference on computing communication and networking technologies (ICCCNT), Oct. 2022, pp. 1–5.

Journal of Applied And Basic Machine Intelligence Research (ABMIR)

Applied and Basic Machine Intelligence Research

Vol. 2, No. 1, Spring & Summer 2024, pp. 14 - 38

Application of 'long-term-short-term memory' and 'convolutional neural networks' to detect distributed denial of service attacks

S. Mojtaba Matinkhah[1*], Ali Khakbaz[2], Fazlolah Adibnia[3]

[1] Computer Engineering Department, Yazd University, Yazd, Iran

Article Information

Original Research Paper

Received:
2023 Febuary 24

Accepted:
2023 September 25

Keywords:
CNN، DDoS، Deep Learning, Machine Learning, LSTM, RNN

Corresponding Author*:
matinkhah@yazd.ac.ir

Abstract

Deep learning is an essential tool for detecting distributed denial of service (DDoS) attacks due to its ability to analyze complex network traffic patterns and respond in real-time. However, a comprehensive examination of the opportunities and challenges in this field is necessary, given its emerging nature. This examination should include real implementations or benchmark data samples. In this paper, we introduce two methods for detecting DDoS attacks: one using Long Short-Term Memory (LSTM) and the other using Convolutional Neural Networks (CNN). Additionally, we propose a new method that combines LSTM and CNN. The results demonstrate that both LSTM and LSTM-CNN methods consistently outperform CNN in terms of accuracy, precision, recovery, and F1 scores. Our investigations reveal that CNN can automatically learn features such as packet size, timing, and source/destination addresses from raw network traffic. On the other hand, LSTM is particularly useful for detecting temporal sequence patterns of attacks in network traffic. The choice between CNN or LSTM for DDoS detection depends on the specific characteristics of the attack dataset and the relative importance of spatial and temporal features in identifying DDoS attacks. Finally, we examine challenges such as overfitting, computational complexity, interpretability, data limitations, and hostile attacks. Doubts surrounding the reporting of results in literature can be attributed to problems with the benchmark dataset used, including limited sample size and variety, lack of labeling, and unbalanced data.

: 10.22034/ABMIR.2023.19764.1025

E-ISSN: 2821-2037