تشخیص حملات DDoS در ترافیک شبکه با استفاده از مدل گروهی مبتنی بر CNN-LSTM

حسین رازقندی
دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
کوثر طالبی
دانشکده مهندسی کامپیوتر، دانشگاه علم و فرهنگ، تهران، ایران
هستی زیودار
دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
علی نوراله
دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران،

۱- چکیده

با گسترش روزافزون حملات سایبری، تشخیص نفوذ در شبکه به یکی از چالش‌های مهم در حوزه امنیت اطلاعات تبدیل شده است. حملات انکار سرویس توزیع‌شده (DDoS) یکی از تهدیدهای اساسی برای امنیت شبکه‌های کامپیوتری محسوب می‌شوند. شناسایی به‌موقع این حملات می‌تواند از اختلال در سرویس‌های حیاتی جلوگیری کند. (Kaur et al, ۲۰۱۷) در این مقاله، یک مدل یادگیری عمیق مبتنی بر ترکیب شبکه‌های عصبی پیچشی (CNN) و حافظه طولانی-کوتاه‌مدت (LSTM) برای تشخیص حملات DDoS ارائه شده است. مدل پیشنهادی با بهره‌گیری از ویژگی‌های استخراج‌شده توسط CNN و توانایی LSTM در یادگیری وابستگی‌های زمانی، دقت بالایی در شناسایی حملات دارد. آزمایش‌ها بر روی مجموعه داده Network Intrusion dataset (CIC-IDS-۲۰۱۷) از Kaggle انجام شده و نتایج نشان می‌دهند که مدل پیشنهادی به دقت ۹۹.۸۲ درصد، صحت (Precision) ۹۹.۹۳ درصد و بازخوانی (Recall) ۹۹.۷۳ درصد دست یافته است. این نتایج نشان‌دهنده کارایی بالای روش پیشنهادی در تشخیص حملات DDoS است. این روش می‌تواند به عنوان یک راهکار مؤثر برای سیستم‌های تشخیص نفوذ (IDS) مورد استفاده قرار گیرد و به افزایش امنیت شبکه‌ها کمک کند.

واژه‌های کلیدی: DDoS، یادگیری عمیق، CNN، LSTM، امنیت سایبری

۲- مقدمه

در عصر دیجیتال، استفاده از اینترنت و شبکه‌های کامپیوتری به‌طور فزاینده‌ای در حال گسترش است. این افزایش وابستگی به فناوری‌های ارتباطی، چالش‌های امنیتی متعددی را به همراه داشته است. سازمان‌ها و کاربران با تهدیدات متنوعی مانند بدافزارها، حملات سایبری و نفوذهای غیرمجاز مواجه هستند که می‌توانند منجر به افشای اطلاعات حساس، تخریب داده‌ها و اختلال در عملکرد سیستم‌ها شوند. (Mubeen et al, ۲۰۲۲), (Perwej et al, ۲۰۲۱)

سیستم‌های تشخیص نفوذ (IDS) به عنوان یکی از راهکارهای مهم برای شناسایی و مقابله با تهدیدات سایبری مطرح شده‌اند. این سیستم‌ها قادرند الگوهای غیرعادی را در ترافیک شبکه شناسایی کرده و از وقوع حملات جلوگیری کنند. روش‌های سنتی تشخیص نفوذ شامل روش‌های مبتنی بر امضا (Signature-based) و تحلیل رفتار (Anomaly-based) بوده‌اند که علی‌رغم کارایی نسبی، با چالش‌هایی همچون عدم توانایی در شناسایی تهدیدات جدید، وابستگی به به‌روزرسانی مداوم پایگاه داده و نرخ هشدارهای نادرست بالا مواجه هستند. (Panagiotou et al, ۲۰۲۱), (Garcia-Teodoro et al, ۲۰۰۹), (Kumar, I., ۲۰۲۳)

با پیشرفت فناوری، استفاده از روش‌های هوشمند و یادگیری ماشین برای بهبود دقت تشخیص نفوذ مورد توجه قرار گرفته است. این روش‌ها با تحلیل حجم بالایی از داده‌های شبکه، قابلیت شناسایی تهدیدات ناشناخته را دارند و می‌توانند به‌عنوان یک راهکار مکمل برای بهبود امنیت سایبری مورد استفاده قرار گیرند. علاوه بر این، مدل‌های یادگیری عمیق به دلیل توانایی آن‌ها در شناسایی الگوهای پیچیده و ارتباطات غیرخطی بین داده‌ها، عملکرد بهتری نسبت به روش‌های سنتی از خود نشان داده‌اند. (Liu, H. and Lang, B., ۲۰۱۹), (Patel et al, ۲۰۱۰)

در این مقاله، یک مدل یادگیری عمیق گروهی مبتنی بر CNN-LSTM برای تشخیص حملات DDoS ارائه شده است. این مدل ابتدا ویژگی‌های ترافیک شبکه را با استفاده از CNN استخراج کرده و سپس از LSTM برای درک وابستگی‌های زمانی میان داده‌ها استفاده می‌کند. سپس به کمک استفاده از تکنیک bagging نتایج مدل‌های مختلف را ترکیب کرده و با کاهش واریانس مدلی با دقت بالا ارائه می‌دهد. برای ارزیابی عملکرد مدل، از مجموعه داده CIC-IDS-۲۰۱۷ استفاده شده و معیارهای ارزیابی مانند دقت (Accuracy)، صحت (Precision) و بازخوانی (Recall) مورد بررسی قرار گرفته‌اند. (Akgun, D. et al, ۲۰۲۲) , (Yeom et al, ۲۰۲۲), (Bi et al, ۲۰۲۱)

هدف این مقاله ارائه یک روش بهینه برای تشخیص حملات DDoS در شبکه‌های کامپیوتری است که می‌تواند در سیستم‌های امنیتی و مراکز داده برای کاهش تهدیدات سایبری مورد استفاده قرار گیرد. نتایج حاصل از آزمایش‌ها نشان می‌دهند که مدل پیشنهادی نسبت به روش‌های سنتی و برخی از مدل‌های یادگیری عمیق قبلی، عملکرد بهتری داشته و می‌تواند به عنوان یک راهکار کارآمد در امنیت شبکه‌ها مورد استفاده قرار گیرد. (Bawany, N. Z. et al, ۲۰۱۷)

۳- روش تحقیق

در این پژوهش، یک مدل یادگیری عمیق گروهی مبتنی بر CNN-LSTM برای تشخیص حملات DDoS طراحی شده است. این مدل از شبکه عصبی پیچشی (CNN) برای استخراج ویژگی‌های محلی و از حافظه طولانی-کوتاه‌مدت (LSTM) برای یادگیری الگوهای وابسته به زمان در ترافیک شبکه استفاده می‌کند.

۳-۱- مجموعه داده و پیش‌پردازش

برای آموزش و ارزیابی مدل، از مجموعه داده Network Intrusion Dataset از Kaggle استفاده شده است. تنها نمونه‌های مربوط به حملات DDoS و ترافیک عادی انتخاب شده و به‌عنوان یک مسئله دسته‌بندی دودویی بررسی شده‌اند. داده‌های نامعتبر شناسایی و جایگزین شده‌اند، ویژگی‌های عددی با Min-Max Scaling نرمال‌سازی شده و داده‌ها به فرمت مناسب برای شبکه عصبی تبدیل شده‌اند.

۳-۲- معماری مدل پیشنهادی

شبکه عصبی پیچشی (CNN - Convolutional Neural Network)

یکی از پرکاربردترین مدل‌های یادگیری عمیق برای استخراج ویژگی‌های پیچیده از داده‌ها، شبکه عصبی پیچشی (CNN) است که به طور خاص برای پردازش داده‌های تصویری و داده‌هایی با ساختار فضایی طراحی شده، اما در حیطه های دیگر مانند پردازش زبان طبیعی (NLP) و تحلیل سری‌های زمانی نیز استفاده می‌شود. (Jogin et al, ۲۰۱۸), (Feghali et al, ۲۰۲۱)

در زمینه تحلیل داده‌های آموزشی، به جای استخراج ویژگی‌ها بصورت دستی، از CNN به عنوان یک ابزار برای استخراج خودکار ویژگی‌های مهم از مجموعه داده استفاده شده که می‌تواند این الگوها را از داده‌های خام شناسایی کند. البته این مدل می‌تواند روابط محلی بین متغیرهای ورودی را شناسایی و ویژگی‌های مهم را بدون نیاز به پیش‌پردازش دستی استخراج کند و همچنین دقت مدل را نسبت به روش‌های سنتی ارتقا دهد. (Lukwaro et al, ۲۰۲٤)

شبکه حافظه کوتاه‌مدت بلندمدت (LSTM - Long Short-Term Memory)

شبکه LSTM یک نوع خاص از شبکه‌های عصبی بازگشتی (RNN) است که برای پردازش داده‌های سری زمانی و داده‌هایی که دارای وابستگی طولانی‌مدت هستند، طراحی شده است. LSTM بر خلاف RNN معمولی که مشکل محو شدن گرادیان (Vanishing Gradient) دارد، مکانیزم دروازه‌ای دارد که اجازه می‌دهد اطلاعات مهم برای مدت طولانی در حافظه شبکه باقی بماند. این مکانیزم از سه دروازه تشکیل شده است. دروازه فراموشی (Forget Gate) که تعیین می‌کند چه مقدار از اطلاعات قبلی باید حذف شود. دروازه ورودی (Input Gate) که مشخص می‌کند چه اطلاعاتی باید به حافظه افزوده شود. دروازه خروجی (Output Gate) که مقدار نهایی حافظه را که باید به مرحله بعدی منتقل شود، مشخص می‌کند. این مدل قادر است روندهای رفتاری را در طول زمان در نظر بگیرد و الگوهای مرتبط را شناسایی کند. LSTM کمک می‌کند تا روندهای زمانی و وابستگی‌های طولانی‌مدت مدل‌سازی شوند.
(Sherstinsky, A., ۲۰۲۰), (Hu et al, ۲۰۱۸)

مدل پیشنهادی این پژوهش از ترکیب دو نوع شبکه عصبی CNN (شبکه عصبی پیچشی) و LSTM (شبکه حافظه طولانی-کوتاه‌مدت) برای شناسایی حملات DDoS در ترافیک شبکه استفاده می‌کند. این ترکیب به مدل کمک می‌کند تا ویژگی‌های مکانی (فضایی) و وابستگی‌های زمانی در داده‌ها را به‌طور همزمان یاد بگیرد و عملکرد بالایی در تشخیص حملات ارائه دهد. (Sathishkumar et al, ۲۰۲٤)

مدل پیشنهادی شامل چندین لایه مختلف است که هرکدام وظیفه خاصی در پردازش داده‌ها دارند. معماری مدل به‌طور کلی از سه بخش اصلی تشکیل شده است: لایه‌های CNN برای استخراج ویژگی‌های مکانی، لایه LSTM برای یادگیری وابستگی‌های زمانی، و

لایه‌های خروجی برای تصمیم‌گیری نهایی. ابتدا، داده‌های ورودی به مدل وارد می‌شوند. این داده‌ها پس از پیش‌پردازش و نرمال‌سازی، به‌صورت بردارهای سه‌بعدی (n_samples, time_steps, ۱) استفاده می‌کنند که n_samples تعداد نمونه‌ها، time_steps تعداد گام‌های زمانی در هر نمونه و ۱ نشان‌دهنده ویژگی تک‌بعدی هر گام زمانی است، به مدل وارد می‌شوند. این لایه ورودی از ابعاد مشخص‌شده برای داده‌های شبکه استفاده می‌کند.

لایه بعدی مدل، لایه Conv۱D است که وظیفه استخراج ویژگی‌های مکانی از داده‌های شبکه را بر عهده دارد. این لایه با استفاده از ۵۱۲ فیلتر و کرنل ۳×۱ برای شناسایی الگوهای محلی در داده‌های ورودی به‌کار می‌رود. استفاده از فیلترهای متعدد به مدل کمک می‌کند تا ویژگی‌های مختلف ترافیک شبکه را شناسایی کند. پس از لایه Conv۱D، یک لایه MaxPooling۱D با اندازه پنجره ۲ قرار می‌گیرد. این لایه به کاهش ابعاد ویژگی‌ها کمک می‌کند و باعث کاهش محاسبات و جلوگیری از بیش‌برازش می‌شود. در این لایه، بیشترین مقدار از هر پنجره انتخاب می‌شود تا ویژگی‌های مهم ترافیک شبکه حفظ شوند.

سپس، داده‌ها وارد لایه LSTM می‌شوند که قادر به یادگیری وابستگی‌های زمانی در توالی داده‌ها است. این لایه شامل ۵۱۲ واحد حافظه است و به‌طور خاص برای پردازش داده‌های سری زمانی طراحی شده است .LSTM به‌عنوان یک مدل بازگشتی قادر است اطلاعات مرتبط با زمان و توالی‌های طولانی را به‌خوبی ذخیره و پردازش کند. برای جلوگیری از بیش‌برازش، در لایه LSTM از تکنیک Dropout با مقدار ۰.۵ استفاده شده است. این تکنیک به مدل کمک می‌کند تا از یادگیری ویژگی‌های تصادفی و غیرضروری که ممکن است منجر به بیش‌برازش شود، جلوگیری کند. در نهایت، یک لایه Dense با یک نورون به مدل اضافه می‌شود که وظیفه تصمیم‌گیری نهایی را بر عهده دارد. این لایه دارای تابع فعال‌سازی Sigmoid است که خروجی آن یک مقدار احتمال است که نشان‌دهنده احتمال تعلق نمونه به کلاس حمله DDoS است. اگر این مقدار بیشتر از ۰.۵ باشد، نمونه به‌عنوان حمله DDoS تشخیص داده می‌شود؛ در غیر این صورت، به‌عنوان ترافیک عادی شناخته می‌شود.

مدل با استفاده از الگوریتم Adam بهینه‌سازی شده است. Adam به‌عنوان یک روش بهینه‌سازی تطبیقی برای شبکه‌های عصبی شناخته می‌شود که عملکرد خوبی در تنظیم یادگیری دارد. (Reyad, M. et al, ۲۰۲۳) به عنوان تابع هزینه، از binary cross-entropy استفاده شده است. این تابع هزینه برای مسائل دسته‌بندی دودویی مناسب است و میزان خطای مدل را در پیش‌بینی صحیح کلاس‌ها اندازه‌گیری می‌کند. (Ruby, U. and Yendapalli, V., ۲۰۲۰)

برای آموزش مدل، داده‌ها به دو بخش آموزشی (۷۰ درصد داده‌ها) و آزمایشی (۳۰ درصد داده‌ها) تقسیم می‌شوند. داده‌های آموزشی برای آموزش مدل و داده‌های آزمایشی برای ارزیابی آن مورد استفاده قرار می‌گیرند. برای جلوگیری از بیش‌برازش، از تکنیک‌های مختلفی مانند Dropout در لایه‌های CNN و LSTM استفاده شده است. این تکنیک‌ها به مدل کمک می‌کنند تا از یادگیری ویژگی‌های غیرضروری که باعث کاهش دقت مدل در داده‌های جدید می‌شوند، جلوگیری کند.

۴- معرفی کلی مجموعه داده

مجموعه داده Network Intrusion dataset (CIC-IDS-۲۰۱۷) یک مجموعه داده جامع برای تحلیل و شناسایی نفوذهای شبکه‌ای است که در پلتفرم Kaggle منتشر شده است. این مجموعه داده شامل نمونه‌های متعددی از ترافیک شبکه‌ای است که به دو دسته کلی ترافیک عادی و ترافیک مخرب تقسیم می‌شوند. هدف اصلی این مجموعه داده، ایجاد بستری مناسب برای توسعه و ارزیابی مدل‌های یادگیری ماشین و یادگیری عمیق در زمینه تشخیص نفوذ به شبکه است. (Thakkar, A. and Lohiya, R., ۲۰۲۰)

این مجموعه داده دارای چندین ویژگی کلیدی است که آن را به گزینه‌ای مناسب برای پژوهش‌های مرتبط با امنیت سایبری تبدیل کرده است. این ویژگی‌ها عبارتند از:

- تنوع حملات: شامل انواع مختلف حملات سایبری مانند DoS (Denial of Service)، DDoS (Distributed Denial of Service)، Port Scan، Brute Force، XSS، SQL Injection و موارد دیگر است.
- ترافیک واقعی شبکه: داده‌ها از یک محیط شبیه‌سازی‌شده واقعی که شامل کاربران و تعاملات طبیعی در یک شبکه است، جمع‌آوری شده‌اند.
- برچسب‌گذاری دقیق: تمامی نمونه‌های ترافیک دارای برچسب‌هایی هستند که نوع ارتباط (عادی یا مخرب) را مشخص می‌کنند و به این موضوع به آموزش بهتر مدل‌ها کمک می‌کند.

مجموعه داده شامل چندین فایل CSV است که هرکدام نمایانگر بخش خاصی از ترافیک شبکه هستند. (Stiawan et al, ۲۰۲۰)
به‌طور کلی، این فایل‌ها شامل موارد زیر هستند:

- ویژگی‌های ارتباطی: شامل اطلاعاتی درباره تعداد بسته‌های ارسالی و دریافتی، مدت‌زمان هر ارتباط و نرخ انتقال داده.
- ویژگی‌های مبتنی بر محتوا: شامل اطلاعاتی درباره محتوای بسته‌ها و مشخصات فنی آنها.
- ویژگی‌های آماری: شامل تحلیل‌های آماری بر روی بسته‌های ترافیکی جهت شناسایی الگوهای مشکوک.

از این مجموعه داده می‌توان در زمینه‌های مختلف امنیت شبکه و تحلیل ترافیک از جمله توسعه سیستم‌های تشخیص نفوذ (IDS)، بهبود الگوریتم‌های تحلیل ترافیک شبکه، شناسایی الگوهای رفتاری کاربران و شناسایی فعالیت‌های غیرمجاز، پژوهش‌های مرتبط با یادگیری ماشین و امنیت سایبری، استفاده کرد. (BANDARUPALLI, G., ۲۰۲٤) با توجه به اینکه در مقاله هدف تشخیص حملات DDoS با استفاده از مدل‌های یادگیری عمیق می‌باشد، تنها از بخش حملات DDoS در مجموعه داده فوق استفاده شده است.

۵ – نتایج

جهت درک بهتر تأثیر روش پیشنهادی، عملکرد مدل گروهی CNN-LSTM با چندین مدل دیگر مقایسه شده است. جدول ۱ نتایج این مقایسه را نشان می‌دهد.

جدول ۱: مقایسه عملکرد مدل‌های مختلف در تشخیص حملات DDoS

مدل	دقت (Accuracy)	بازخوانی (Recall)	صحت (precision)	F۱-Score
RNN	۸۸.۶۹	۹۸.۳۵	۹۴.۰۴	۹۰.۲۰
GRU	۸۷.۷۸	۹۶.۷۳	۹۳.۰۶	۸۹.۷۴
Conv-LSTM	۹۰.۸۱	۹۸.۲۰	۹۴.۷۷	۹۱.۶۳
LSTM	۹۷.۶۸	۹۸.۱۲	۹۸.۹۵	۹۹.۱۷
CNN	۹۸.۷۳	۹۸.۷۷	۹۷.۳۰	۹۷.۱۴
LR	۸۷.۲۱	۹۶.۲۹	۹۱.۲۵	۸۸.۱۴
DT	۸۳.۵۰	۹۳.۲۹	۸۹.۰۲	۸۶.۱۷
CNN-LSTM	**۹۹.۸۲**	**۹۹.۷۳**	**۹۹.۸۴**	**۹۹.۹۴**

روش‌های سنتی مانند درخت تصمیم (DT) و رگرسیون لجستیک (LR) به دلیل سادگی و سرعت بالای اجرا، از دیرباز در مسائل تشخیص نفوذ مورد استفاده قرار گرفته‌اند. اما این مدل‌ها به دلیل وابستگی به ویژگی‌های از پیش تعیین‌شده و ناتوانی در استخراج روابط پیچیده، عملکرد مطلوبی ندارند. درخت تصمیم به شدت تحت تأثیر نویز داده‌ها قرار می‌گیرد و در برابر تغییرات جزئی در ورودی‌ها حساس است. از سوی دیگر، رگرسیون لجستیک که مدلی خطی محسوب می‌شود، در تشخیص الگوهای پیچیده موجود در ترافیک شبکه محدودیت دارد. (Mohmand et al, ۲۰۲۲), (Ali, T. E. et al, ۲۰۲۳)

مدل‌های یادگیری عمیق مبتنی بر پردازش سری‌زمانی مانند شبکه‌های عصبی بازگشتی و حافظه طولانی-کوتاه‌مدت عملکرد بهتری نسبت به روش‌های سنتی ارائه می‌دهند. شبکه‌های عصبی بازگشتی قادر به یادگیری وابستگی‌های زمانی در داده‌ها هستند، اما مشکل محوشدگی گرادیان باعث کاهش توانایی آن‌ها در پردازش توالی‌های طولانی می‌شود. مدل‌های LSTM و GRU این مشکل را با معرفی مکانیزم‌های دروازه‌ای کاهش داده‌اند. با این حال، این مدل‌ها به‌تنهایی قادر به استخراج ویژگی‌های مکانی مهم از داده‌های خام نیستند و این موضوع می‌تواند بر دقت نهایی تأثیر منفی بگذارد. (Anitha et al, ۲۰۲۳)

مدل‌های مبتنی بر شبکه‌های عصبی پیچشی مانند CNN در تحلیل الگوهای مکانی موجود در داده‌ها بسیار مؤثر عمل می‌کنند. این مدل‌ها به‌ویژه در پردازش داده‌های تصویری موفقیت بالایی داشته‌اند و در مسائل مرتبط با پردازش ترافیک شبکه نیز توانسته‌اند عملکرد مطلوبی ارائه دهند. اما مشکل اصلی CNN این است که قادر به درک ارتباطات زمانی بین بسته‌های شبکه نیست و این ضعف می‌تواند در تشخیص حملات که وابستگی زمانی بالایی دارند، محدودیت ایجاد کند. برای رفع این چالش، مدل Conv-LSTM پیشنهاد شده که تلاش دارد با ترکیب ویژگی‌های CNN و LSTM، وابستگی‌های زمانی و مکانی را به‌طور همزمان یاد بگیرد. با این حال، پیچیدگی این

مدل و تنظیمات خاص آن باعث شده که عملکرد آن در مقایسه با ترکیب CNN-LSTM بهینه نباشد. (Khan et al, ۲۰۱۹) مدل پیشنهادی این پژوهش با ترکیب CNN و LSTM سعی دارد از نقاط قوت هر دو روش بهره ببرد. شبکه عصبی پیچشی CNN ویژگی‌های مکانی مهم را از داده‌های ترافیک شبکه استخراج می‌کند، درحالی‌که LSTM با در نظر گرفتن اطلاعات زمانی، روند تغییرات رفتاری حملات را تحلیل می‌کند. این ترکیب باعث شده که دقت مدل پیشنهادی نسبت به سایر مدل‌ها بهبود یابد و نرخ هشدارهای نادرست کاهش پیدا کند. با این وجود، یکی از چالش‌های این مدل افزایش پیچیدگی محاسباتی و زمان اجرای آن در مقایسه با روش‌های ساده‌تر است، که ممکن است در پیاده‌سازی‌های بلادرنگ نیاز به بهینه‌سازی بیشتر داشته باشد.

۶- نتیجه‌گیری

حملات DDoS می‌توانند منجر به ازکارافتادن سرویس‌های حیاتی، ایجاد خسارت مالی و اختلال در عملکرد زیرساخت‌های حیاتی شوند. با توجه به افزایش روزافزون این نوع حملات، پیش‌بینی و شناسایی سریع آن‌ها برای جلوگیری از خسارات احتمالی بسیار حائز اهمیت است. روش پیشنهادی در این پژوهش می‌تواند به سازمان‌ها و شرکت‌های ارائه‌دهنده خدمات اینترنتی کمک کند تا با تشخیص زودهنگام حملات، از تأثیرات مخرب آن جلوگیری کنند. (Lehto, M., ۲۰۲۲)

در این پژوهش، یک مدل یادگیری عمیق گروهی مبتنی بر CNN-LSTM برای تشخیص حملات DDoS در ترافیک شبکه ارائه شد. ترکیب شبکه عصبی پیچشی (CNN) برای استخراج ویژگی‌های مکانی و حافظه طولانی-کوتاه‌مدت (LSTM) برای تحلیل وابستگی‌های زمانی در داده‌های شبکه، توانست عملکرد بالایی در شناسایی این نوع حملات ارائه دهد. مدل پیشنهادی با استفاده از مجموعه داده Network Intrusion Dataset آموزش داده شد و توانست به دقت ۹۹.۸۲ درصد، دقت مثبت ۹۹.۹۴ درصد و بازخوانی ۹۹.۷۳ درصد دست یابد.

نتایج مقایسه‌ای نشان می‌دهند که مدل پیشنهادی عملکرد بهتری نسبت به سایر مدل‌های یادگیری عمیق و روش‌های سنتی دارد. به‌عنوان مثال، مدل‌های مبتنی بر LSTM به‌تنهایی ممکن است در استخراج ویژگی‌های مکانی داده‌های شبکه ضعیف باشند، درحالی‌که مدل‌های CNN بدون در نظر گرفتن وابستگی‌های زمانی ممکن است اطلاعات حیاتی را از دست بدهند. ترکیب این دو مدل باعث شده است که شبکه بتواند هم ویژگی‌های مهم را استخراج کند و هم روند تغییرات ترافیک شبکه را در طول زمان در نظر بگیرد، که این امر به دقت بالاتر در تشخیص حملات DDoS منجر شده است.

با وجود عملکرد بالای مدل، همچنان چالش‌هایی مانند بهبود تعمیم‌پذیری مدل برای داده‌های شبکه‌ی واقعی، کاهش پیچیدگی محاسباتی و افزایش سرعت پردازش وجود دارند که می‌توانند در تحقیقات آینده مورد بررسی قرار گیرند. برای کارهای آینده، می‌توان از مدل‌های بهینه‌تری مانند Transformer یا ترکیب CNN با GRU برای کاهش پیچیدگی محاسباتی و افزایش سرعت تشخیص حملات استفاده کرد. (Wang, H. and Li, W., ۲۰۲۱), (Goud, K. S. and Rao, G. S., ۲۰۲٤)

منابع

Kaur, P., Kumar, M., & Bhandari, A. (۲۰۱۷). A review of detection approaches for distributed denial of service attacks. Systems Science & Control Engineering, ۵(۱), ۳۰۱-۳۲۰.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (۲۰۲۱). A systematic literature review on the cyber security. International Journal of scientific research and management, ۹(۱۲), ۶۶۹-۷۱۰.

Mubeen, M., Arslan, M., & Anandhi, G. (۲۰۲۲). Strategies to Avoid Illegal Data Access. Journal of Communication Engineering & Systems, ۱۲(۳), ۲۹-۴۰p.

Kumar, I. (۲۰۲۳). Emerging threats in cybersecurity: a review article. International Journal of Applied and Natural Sciences, ۱(۱), ۰۱-۰۸.

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (۲۰۰۹). Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security, ۲۸(۱-۲), ۱۸-۲۸.

Panagiotou, P., Mengidis, N., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (۲۰۲۱). Host-based intrusion detection using signature-based and ai-driven anomaly detection methods. Information & Security, ۵۰(۱), ۳۷-۴۸.

Patel, A., Qassim, Q., & Wills, C. (۲۰۱۰). A survey of intrusion detection and prevention systems. Information Management & Computer Security, ۱۸(۴), ۲۷۷-۲۹۰.

Liu, H., & Lang, B. (۲۰۱۹). Machine learning and deep learning methods for intrusion detection systems: A survey. applied sciences, ۹(۲۰), ۴۳۹۶.

Akgun, D., Hizal, S., & Cavusoglu, U. (۲۰۲۲). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. Computers & Security, ۱۱۸, ۱۰۲۷۴۸.

Yeom, S., Choi, C., & Kim, K. (۲۰۲۲). LSTM-based collaborative source-side DDoS attack detection. IEEE Access, ۱۰, ۴۴۰۳۳-۴۴۰۴۵.

Bi, J., Zhang, X., Yuan, H., Zhang, J., & Zhou, M. (۲۰۲۱). A hybrid prediction method for realistic network traffic with temporal convolutional network and LSTM. IEEE Transactions on Automation Science and Engineering, ۱۹(۳), ۱۸۶۹-۱۸۷۹.

Bawany, N. Z., Shamsi, J. A., & Salah, K. (۲۰۱۷). DDoS attack detection and mitigation using SDN: methods, practices, and solutions. Arabian Journal for Science and Engineering, ۴۲, ۴۲۵-۴۴۱.

Thakkar, A., & Lohiya, R. (۲۰۲۰). A review of the advancement in intrusion detection datasets. Procedia Computer Science, ۱۶۷, ۶۳۶-۶۴۵.

Stiawan, D., Idris, M. Y. B., Bamhdi, A. M., & Budiarto, R. (۲۰۲۰). CICIDS-۲۰۱۷ dataset feature analysis with information gain for anomaly detection. IEEE Access, ۸, ۱۳۲۹۱۱-۱۳۲۹۲۱.

BANDARUPALLI, G. (۲۰۲۴). Efficient Deep Neural Network for Intrusion Detection Using CIC-IDS-۲۰۱۷ Dataset.

Jogin, M., Madhulika, M. S., Divya, G. D., Meghana, R. K., & Apoorva, S. (۲۰۱۸, May). Feature extraction using convolution neural networks (CNN) and deep learning. In ۲۰۱۸ ۳rd IEEE international conference on recent trends in electronics, information & communication technology (RTEICT) (pp. ۲۳۱۹-۲۳۲۳). IEEE.

Feghali, J., Jimenez, A. E., Schilling, A. T., & Azad, T. D. (۲۰۲۱). Overview of algorithms for natural language processing and time series analyses. *Machine learning in clinical neuroscience: Foundations and applications*, ۲۲۱-۲۴۲.

Lukwaro, E., Kalegele, K., & Nyambo, D. (۲۰۲٤). A Review on NLP Techniques and Associated Challenges in Extracting Features from Education Data.

Sherstinsky, A. (۲۰۲۰). Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network. Physica D: Nonlinear Phenomena, ٤۰٤, ۱۳۲۳۰٦..

Hu, Y., Huber, A., Anumula, J., & Liu, S. C. (۲۰۱۸). Overcoming the vanishing gradient problem in plain recurrent networks. arXiv preprint arXiv:۱۸۰۱,۰٦۱۰٥.

Sathishkumar, P., Gnanabaskaran, A., Saradha, M., & Gopinath, R. (۲۰۲٤). Dos attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network. Ain Shams Engineering Journal, ۱٥(۱۲), ۱۰۳۰٥۲.

Reyad, M., Sarhan, A. M., & Arafa, M. (۲۰۲۳). A modified Adam algorithm for deep neural network optimization. Neural Computing and Applications, ۳٥(۲۳), ۱۷۰۹٥-۱۷۱۱۲.

Ruby, U., & Yendapalli, V. (۲۰۲۰). Binary cross entropy with deep learning technique for image classification. Int. J. Adv. Trends Comput. Sci. Eng, ۹(۱۰).

Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., ... & Haleem, M. (۲۰۲۲). A machine learning-based classification and prediction technique for DDoS attacks. IEEE Access, ۱۰, ۲۱٤٤۳-۲۱٤٥٤.

Ali, T. E., Chong, Y. W., & Manickam, S. (۲۰۲۳). Machine learning techniques to detect a DDoS attack in SDN: A systematic review. Applied Sciences, ۱۳(٥), ۳۱۸۳.

Anitha, T., Aanjankumar, S., Poonkuntran, S., & Nayyar, A. (۲۰۲۳). A novel methodology for malicious traffic detection in smart devices using BI-LSTM–CNN-dependent deep learning methodology. Neural Computing and Applications, ۳٥(۲۷), ۲۰۳۱۹-۲۰۳۳۸.

Khan, M. A., Karim, M. R., & Kim, Y. (۲۰۱۹). A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. Symmetry, ۱۱(٤), ٥۸۳.

Lehto, M. (۲۰۲۲). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. ۳-٤۲). Cham: Springer International Publishing.

Wang, H., & Li, W. (۲۰۲۱). DDosTC: A transformer-based network attack detection hybrid mechanism in SDN. Sensors, ۲۱(۱٥), ٥۰٤۷.

Goud, K. S., & Rao, G. S. (۲۰۲٤, January). Towards an Efficient DDoS Attack Detection in SDN: An Approach with CNN-GRU Fusion. In ۲۰۲٤ Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. ۱-۱۰). IEEE.

CESNET-TLS۲۲ Dataset. (۲۰۲۲). Liberouter.org. https://www.liberouter.org/technology-v۲/tools-services-datasets/datasets/cesnet-tls۲۲/

DDoS Attack Detection in Network Traffic Using an Ensemble Model Based on CNN-LSTM

Hossein Razghandi
Department of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran, Postal code: ۱۶۷۸۸-۱۵۸۱۱
Kowsar Talebi
Faculty of Computer Engineering, University of Science and Culture, Tehran, Iran, Postal Code: ۱٤٦۱۹٦۸۱٥۱
Hasti Zivdar
Department of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran, Postal code: ۱۶۷۸۸-۱۵۸۱۱
Ali Nourollah
Department of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran, Postal code: ۱۶۷۸۸-۱۵۸۱۱

Abstract

With the rapid increase in cyberattacks, network intrusion detection has become a significant challenge in the field of information security. Distributed Denial-of-Service (DDoS) attacks are among the most critical threats to computer network security, as they can overwhelm network resources and disrupt essential services. Timely and accurate detection of these attacks is crucial for maintaining the availability and integrity of online systems.

In this paper, we propose a deep learning-based model that integrates Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks for DDoS attack detection. The proposed model utilizes CNNs to extract spatial features from network traffic data while leveraging LSTMs to capture temporal dependencies, leading to improved detection accuracy. The model is trained and evaluated using the Network Intrusion dataset (CIC-IDS-۲۰۱۷) from Kaggle. Experimental results demonstrate that the proposed approach achieves an accuracy of ۹۹,۸۲٪, a precision of ۹۹,۹۳٪, and a recall of ۹۹,۷۳٪, outperforming traditional detection methods.

These findings highlight the effectiveness of the proposed model in identifying DDoS attacks with high accuracy and reliability. The proposed approach can serve as an efficient solution for Intrusion Detection Systems (IDS) and contribute to strengthening cybersecurity by mitigating the impact of malicious network activities.

Keywords: DDoS, deep learning, CNN, LSTM, cybersecurity