

ارتقای تشخیص حملات DDoS با استفاده از انتخاب ویژگی ترکیبی و طبقه‌بندهای گروهی: رویکردی نویدبخش برای امنیت سایبری مقاوم

آرمین باقری فرد arminbagheri@gmail.com

کارشناس ارشد مهندسی کامپیوتر گرایش شبکه های کامپیوتری دانشگاه آزاد کیش

کارشناس امنیت اپراتور تلفن همراه منطقه آزاد کیش

چکیده

حملات محروم‌سازی از خدمات توزیع‌شده (DDoS) با ایجاد حجم عظیمی از ترافیک از منابع متعدد و اشباع سیستم‌های هدف، یکی از تهدیدهای جدی علیه شبکه‌ها و سامانه‌های رایانه‌ای به شمار می‌روند. از این رو، تشخیص بلادرنگ این حملات به یکی از وظایف مهم در حوزه امنیت سایبری تبدیل شده است. با این حال، بسیاری از روش‌های موجود برای تشخیص حملات DDoS با چالش‌هایی همچون نرخ بالای مثبت کاذب و توانایی محدود در شناسایی الگوهای پیچیده ترافیک حمله مواجه هستند. در این پژوهش، یک رویکرد بهبودیافته برای تشخیص حملات DDoS ارائه شده است که در آن، یک روش انتخاب ویژگی ترکیبی با طبقه‌بندهای گروهی (Ensemble-based) تلفیق می‌شود. در رویکرد گروهی، با ترکیب تعداد زیادی درخت تصمیم، دقت طبقه‌بندی افزایش یافته و احتمال بیش‌برازش کاهش می‌یابد؛ در نتیجه، استحکام مدل نیز بهبود پیدا می‌کند. روش انتخاب ویژگی پیشنهادی با ترکیب تحلیل همبستگی (Correlation Analysis)، اطلاعات متقابل (Mutual Information) و تحلیل مؤلفه‌های اصلی (Principal Component Analysis)، ویژگی‌های مؤثرتر برای تشخیص حملات را شناسایی می‌کند. در میان روش‌های مختلف یادگیری ماشین گروهی، طبقه‌بند جنگل تصادفی گروهی (Ensemble Random Forest) با استفاده از ویژگی‌های منتخب، بهترین عملکرد تشخیصی را ارائه می‌دهد. مدل پیشنهادی با استفاده از چندین مجموعه داده عمومی مرتبط با تشخیص حملات DDoS ارزیابی شده است. نتایج تجربی نشان می‌دهند که این مدل از نظر معیارهایی همچون دقت (Accuracy)، بازخوانی (Recall)، صحت (Precision)، امتیاز F1 و نرخ مثبت کاذب (False Positive Rate)، عملکرد بهتری نسبت به روش‌های موجود دارد. نتایج نشان می‌دهد که رویکرد پیشنهادی به دقتی نزدیک به ۱۰۰ درصد، نرخ مثبت واقعی (TPR) برابر با ۱۰۰ درصد و نرخ خطای ۰ درصد دست یافته است. این نتایج، روش پیشنهادی را به راهکاری نویدبخش برای تشخیص مؤثر حملات DDoS تبدیل می‌کند.

کلیدواژه‌ها: حملات DDoS؛ تشخیص حملات DDoS؛ انتخاب ویژگی ترکیبی؛ یادگیری ماشین گروهی؛ تشخیص حملات DDoS مبتنی بر روش‌های گروهی؛ جنگل تصادفی گروهی؛ امنیت سایبری

۱. مقدمه

حمله محروم‌سازی از خدمات توزیع‌شده (Distributed Denial-of-Service) یا DDoS نوعی حمله سایبری است که در آن مهاجمان با بهره‌گیری از تعداد زیادی دستگاه آلوده یا تحت کنترل، که گاه بخشی از یک بات‌نت هستند، حجم عظیمی از ترافیک را به سمت یک سیستم یا شبکه هدف هدایت می‌کنند. در نتیجه، منابع سیستم هدف اشباع شده و دسترسی کاربران مجاز به خدمات با اختلال مواجه می‌شود [1]، ۲. هدف اصلی حملات DDoS، مختل کردن عملکرد عادی سیستم یا شبکه و جلوگیری از دسترسی کاربران مجاز به خدمات موردنظر است [3]، ۴.

دستگاه‌های مورد استفاده در این حملات می‌توانند شامل رایانه‌های آلوده، روترها یا تجهیزات اینترنت اشیا (Internet of Things یا IoT) باشند که به بدافزار آلوده شده یا توسط مهاجمان در اختیار گرفته شده‌اند. مهاجمان پس از کنترل این تجهیزات، آنها را به ارسال حجم عظیمی از ترافیک به سمت سیستم یا شبکه هدف وادار می‌کنند؛ به‌گونه‌ای که سامانه هدف دیگر قادر به پاسخ‌گویی مناسب به درخواست‌های مشروع کاربران نخواهد بود. حملات DDoS می‌توانند از نقاط مختلف جهان آغاز شوند و به دلیل ماهیت توزیع‌شده خود، شناسایی، مهار و متوقف کردن آنها دشوار است. این حملات اغلب با اهدافی مانند اخاذی مالی یا ایجاد اختلال در فعالیت شرکت‌ها، سازمان‌های دولتی و سایر نهادها انجام می‌شوند. پیامدهای حملات DDoS می‌تواند شامل خسارت‌های مالی قابل توجه، آسیب به اعتبار سازمان و حتی پیامدهای حقوقی باشد [5]، ۶.

حملات DDoS به دلیل احتمال آسیب‌رسانی به داده‌های حساس و به خطر انداختن اطلاعات کاربران، نگرانی‌های جدی اخلاقی و حقوقی ایجاد می‌کنند. این حملات از نظر تعداد و پیچیدگی روندی افزایشی دارند و همین موضوع، شناسایی و مقابله با آنها را دشوارتر کرده است. [7] مهاجمان از طیف گسترده‌ای از تکنیک‌ها و فناوری‌ها استفاده می‌کنند و پیامدهای حملات DDoS نیز می‌تواند فراتر از سازمان هدف گسترش یابد. برای مثال، حمله به زیرساخت‌های حیاتی می‌تواند آثار گسترده‌ای داشته باشد و سازمان‌های دیگر، دولت‌ها و حتی افراد را تحت تأثیر قرار دهد.

از این رو، مقابله با حملات DDoS نه تنها برای سازمان‌های منفرد، بلکه برای جامعه و زیرساخت‌های گسترده‌تر نیز اهمیت دارد. بنابراین، توسعه روش‌ها و ابزارهای مؤثر برای شناسایی و کاهش اثرات حملات DDoS به یک ضرورت تبدیل شده است [8]، ۹. با افزایش پیچیدگی این حملات، مقابله با آنها نیز دشوارتر می‌شود؛ زیرا حملات DDoS می‌توانند لایه‌های مختلف شبکه را هدف قرار دهند و از منابع متنوعی سرچشمه بگیرند. [10] افزون بر این، تمایز میان ترافیک مشروع و ترافیک مخرب همچنان یکی از چالش‌های اصلی در شناسایی این حملات محسوب می‌شود. بنابراین، کاهش مؤثر آثار حملات DDoS مستلزم استفاده از رویکردهای نوآورانه و جامع برای مقابله با تهدیدهای در حال تحول است [11]، ۱۲.

در این پژوهش، یک روش بهبودیافته برای شناسایی حملات DDoS ارائه می‌شود که از ترکیب یک روش جدید انتخاب ویژگی با طبقه‌بندهای گروهی (Ensemble-based) بهره می‌گیرد. در روش پیشنهادی، تحلیل همبستگی (Correlation Analysis)، اطلاعات متقابل (Mutual Information) و تحلیل مؤلفه‌های اصلی (Principal Component Analysis) به صورت یکپارچه برای انتخاب ویژگی‌های معنادار مورد استفاده قرار می‌گیرند. سپس، از طبقه‌بند جنگل تصادفی (Random Forest) در میان تکنیک‌های مختلف یادگیری ماشین گروهی برای ایجاد مدل استفاده می‌شود.

هدف رویکرد پیشنهادی، افزایش دقت تشخیص حملات DDoS و در عین حال کاهش نرخ مثبت کاذب (False Positive Rate یا FPR) است. این روش با استفاده از مجموعه داده‌های واقعی مختلف ارزیابی شده و نتایج نشان می‌دهد که عملکرد آن از

نظر معیارهایی مانند دقت (Accuracy)، بازخوانی (Recall)، صحت (Precision) و سایر معیارهای ارزیابی، در مقایسه با روش‌های موجود بهبود یافته است.

مهم‌ترین دستاوردهای این پژوهش عبارت‌اند از:

۱. بررسی جدیدترین روش‌های تشخیص حملات DDoS و ارزیابی نقاط قوت و ضعف آنها.
۲. ارائه یک رویکرد ترکیبی برای انتخاب مرتبط‌ترین ویژگی‌ها.
۳. ارزیابی عملکرد چندین تکنیک کلاسیک یادگیری ماشین برای شناسایی حملات DDoS با استفاده از مدل پیشنهادی.
۴. توسعه یک چارچوب یادگیری ماشین مبتنی بر روش‌های گروهی (Ensemble) که با ترکیب چندین طبقه‌بند، دقت تشخیص را افزایش می‌دهد.
۵. ارزیابی اثربخشی راهکار پیشنهادی مبتنی بر روش‌های گروهی در مقایسه با تکنیک‌های موجود تشخیص DDoS، با استفاده از مجموعه داده‌های عمومی مختلف.

استفاده از جنگل تصادفی مبتنی بر روش‌های گروهی، با یکپارچه‌سازی پیش‌بینی‌های تعداد زیادی از درخت‌های تصمیم، می‌تواند دقت طبقه‌بندی را افزایش دهد و آن را به گزینه‌ای مناسب برای تشخیص حملات DDoS تبدیل کند. در مقایسه با استفاده از یک طبقه‌بند منفرد، روش جنگل تصادفی می‌تواند واریانس و سوگیری (Bias) مدل را کاهش داده، احتمال بیش‌برازش (Overfitting) را محدود کند و استحکام مدل را افزایش دهد. [13] افزون بر این، رویکردهای مبتنی بر روش‌های گروهی می‌توانند با درک بهتر ساختارهای پیچیده جریان ترافیک حملات DDoS، عملکرد دقیق‌تری نسبت به برخی روش‌های پیشین ارائه دهند. مقیاس‌پذیری و توانایی این روش‌ها در پردازش حجم زیادی از داده نیز آنها را برای شناسایی حملات DDoS در محیط‌های بلادرنگ مناسب می‌سازد. [14]

جدول ۱ شامل فهرست اختصارات و اصطلاحات مورد استفاده در این پژوهش است. ساختار ادامه مقاله نیز به این صورت است: در بخش دوم، پژوهش‌های مرتبط با تشخیص حملات DDoS بررسی می‌شوند. در بخش سوم، مراحل توسعه مدل پیشنهادی تشریح می‌شود. بخش چهارم به ارائه نتایج و بحث اختصاص دارد و شامل شکل‌ها و جداول مرتبط است. در نهایت، بخش پنجم به نتیجه‌گیری پژوهش می‌پردازد.

۲. پیشینه پژوهش

در طول زمان، تکنیک‌های مختلفی مانند روش‌های مبتنی بر قانون، روش‌های آماری و روش‌های مبتنی بر یادگیری ماشین برای شناسایی حملات DDoS پیشنهاد شده‌اند. در این بخش، جدیدترین تکنیک‌های تشخیص حملات DDoS و نقاط قوت و ضعف آنها مرور می‌شوند.

در راهبردهای مبتنی بر قانون، مجموعه‌ای از قوانین برای شناسایی حملات DDoS توسعه داده می‌شود. این قوانین اغلب بر اساس ویژگی‌های جریان ترافیک، مانند نرخ ارسال بسته‌ها، اندازه بسته‌ها و نوع پروتکل، تنظیم می‌شوند. اگرچه این رویکردها شفاف و استفاده از آنها آسان است، ممکن است در شناسایی حملات DDoS نوآورانه یا پیچیده‌ای که از معیارهای مشخص پیروی نمی‌کنند، عملکرد مناسبی نداشته باشند. همچنین، تکنیک‌های مبتنی بر قانون ممکن است نرخ مثبت کاذب بالایی ایجاد کنند و در نتیجه، ترافیک قانونی را به اشتباه به عنوان ترافیک حمله شناسایی کنند [15]، [۱۶].

روش‌های آماری از مدل‌های آماری برای شناسایی ناهنجاری‌ها در ترافیک شبکه استفاده می‌کنند. این تکنیک‌ها جریان ترافیک را بررسی کرده و انحراف از الگوی عادی را شناسایی می‌کنند. از آنجا که روش‌های آماری قادر به شناسایی حملات شناخته شده و ناشناخته هستند، در برخی موارد نسبت به سیستم‌های مبتنی بر قانون ترجیح داده می‌شوند. با این حال، روش‌های آماری ممکن است برای شناسایی الگوهای ترافیک عادی به حجم زیادی از داده‌های آموزشی نیاز داشته باشند که فراهم کردن آنها می‌تواند دشوار باشد. افزون بر این، تکنیک‌های آماری ممکن است نرخ بالایی از هشدارهای کاذب تولید کنند و در نتیجه، ترافیک واقعی به اشتباه به عنوان حمله برچسب‌گذاری شود [17]، [۱۸].

برای شناسایی حملات DDoS، رویکردهای یادگیری ماشین از طبقه‌بندهای مختلف برای شناسایی الگوهای ترافیک قانونی و مخرب استفاده می‌کنند. چنگ و همکاران [19] در سال ۲۰۲۰ یک تکنیک CNN چندمقیاسی برای شناسایی حملات DDoS ارائه کردند که دقت آن ۷۴ درصد بود و نرخ مثبت واقعی (TPR) پایینی داشت. در همان سال، سامبانگی و گوندی [20] روشی مبتنی بر رگرسیون خطی چندگانه ارائه کردند که به دقت ۷۵ درصد دست یافت و نرخ مثبت کاذب (FPR) بالایی داشت.

سایینی و همکاران [21] یک مدل یادگیری ماشین ارائه کردند که از طبقه‌بند J48 برای شناسایی حملات DDoS از نوع UDP Flood، HTTP Flood، Smurf و SIDDos استفاده می‌کند. یکی از محدودیت‌های قابل توجه این پژوهش، استفاده از مجموعه داده‌ای نسبتاً کوچک برای آموزش و آزمایش مدل بود. افزون بر این، پژوهش مذکور نرخ بالای FPR را به عنوان یکی از مشکلات مدل گزارش کرده است.

لوپس و همکاران [22] در سال ۲۰۲۱ چارچوبی برای سیستم تشخیص نفوذ (IDS) پیشنهاد کردند که مجموعه‌ای از روش‌های مهندسی ویژگی را با استفاده از شبکه‌های عصبی عمیق یکپارچه می‌کند. این روش به دقتی نزدیک به ۹۹ درصد دست یافت. با وجود ارائه یک چارچوب IDS، این روش تنها قادر به شناسایی حملات DDoS است.

برای محیط‌های شبکه نرم‌افزارمحور (SDN)، راجش و همکاران [23] رویکردی مبتنی بر جنگل تصادفی ارائه کردند که برای تشخیص حملات DDoS به دقت ۹۷ درصد دست یافت. داساری و دواراکوندا [24] نیز مدل دیگری مبتنی بر یادگیری ماشین برای تشخیص حملات DDoS پیشنهاد کردند. آنها از چندین طبقه‌بند منفرد یادگیری ماشین استفاده کردند. مدل مبتنی بر رگرسیون لجستیک بهترین عملکرد را در ارزیابی آنها داشت و به دقت ۹۹.۶۱ درصد دست یافت؛ با این حال، مقدار ویژگی‌ویژه

(Specificity) آن حدود ۸۴ درصد بود. از آنجا که این روش از یک طبقه‌بند منفرد استفاده می‌کند، عملکرد آن بسته به نوع حمله DDoS متفاوت است.

آهوجا و همکاران [25] طبقه‌بندی مبتنی بر RF-SVC را با دقت ۹۸.۸ درصد پیشنهاد کردند. این مدل پیچیده، تنها برای محیط SDN مناسب است.

در سال ۲۰۲۲، نوا و همکاران [26] تکنیک‌های بهینه‌سازی بهبودیافته‌ای را برای تشخیص حملات DDoS پیشنهاد کردند. مدل آنها با استفاده از طبقه‌بند KNN به دقت ۸۹.۵۹ درصد دست یافت. نویسندگان در پژوهش خود استفاده از روش‌های اضافی، مانند خوشه‌بندی یا شبکه‌های عصبی، را برای افزایش نرخ تشخیص و کاهش نرخ هشدار کاذب پیشنهاد کردند.

نالینی و کاتیراوان [27] مدلی با دقت بالا، اما نرخ هشدار کاذب ۰.۰۵ درصد، ارائه کردند. چوان و همکاران [28] نیز روشی برای تشخیص حملات DDoS ارائه کردند و از چندین طبقه‌بند یادگیری ماشین برای ارزیابی مدل خود استفاده کردند. آنها دریافتند که بالاترین دقت، مربوط به طبقه‌بند رگرسیون لجستیک و برابر با ۹۰.۴ درصد است. بر اساس متن مقاله، این میزان دقت در شرایط کنونی قابل قبول نیست. به دلیل حجم بالای ترافیک، مدل قادر به شناسایی مؤثر ترافیک مخرب مانند DDoS نیست و در نتیجه، نرخ مثبت کاذب (FPR) آن بالا خواهد بود.

در همان سال، الگندی و همکاران [29] روش DTEXNet را ارائه کردند که به دقت ۹۵ درصد دست یافت. این روش پیچیده‌تر است، زیرا دو مدل شبکه عصبی را با یکدیگر ترکیب می‌کند. همچنین، بر اساس متن پژوهش، دقت آن باید متناسب با اندازه مجموعه داده بهبود یابد.

در سال ۲۰۲۳، سمان و جیاد [30] روشی مبتنی بر تکنیک‌های درخت‌های تقویت‌شده گرادیانی (Gradient-Boosted Trees) پیشنهاد کردند که به دقت ۹۳ درصد دست یافت. باین‌حال، در این مدل، مقدار Precision و نرخ مثبت واقعی (TPR) همچنان نیازمند بهبود هستند.

صابر [31] از طبقه‌بندهای KNN، BayesNet و J48 برای تشخیص حملات DDoS استفاده کرد و دریافت که مدل مبتنی بر طبقه‌بند J48 بهترین عملکرد را با دقت ۹۸.۳۱ درصد ارائه می‌دهد. برخی پژوهشگران نیز روش‌های خاصی مبتنی بر یادگیری عمیق را برای محیط‌های مختلف پیشنهاد کرده‌اند. [32-35] این راهبردها برای استقرار در محیط‌هایی با منابع محدود، کاربرد کمتری دارند. افزون بر این، این روش‌ها در شناسایی حملات DDoS جدید و در حال تکامل با مشکل مواجه بوده‌اند؛ به‌ویژه زمانی که برخی انواع حملات در داده‌های آموزشی پوشش داده نشده باشند.

بیشتر پژوهشگران، مدل‌هایی مبتنی بر یک طبقه‌بند منفرد یادگیری ماشین پیشنهاد کرده‌اند. طبقه‌بندهای منفرد یادگیری ماشین در تشخیص حملات DDoS با چندین چالش اساسی مواجه هستند. این چالش‌ها شامل کمبود داده‌های آموزشی مربوط به حملات جدید، پیچیدگی و تنوع ویژگی‌های حملات، تغییر مفهوم در رفتار شبکه، سازگاری مهاجمان، نامتوازن بودن داده‌ها و احتمال بیش‌برازش (Overfitting) مدل‌ها است. افزون بر این، لازم است دقت و TPR در مقایسه با روش‌های موجود افزایش یابد و در عین حال، FPR به حداقل برسد. بنابراین، ایجاد یک مدل تشخیص حملات DDoS که بتواند در برابر انواع مختلف حملات عملکرد قابل‌اعتمادی داشته باشد، ضروری است. [36]

روش‌شناسی پیشنهادی، که از یک طبقه‌بند جنگل تصادفی مبتنی بر روش‌های گروهی با نام ERF-HFS استفاده می‌کند، راهکاری جامع و کارآمد برای محافظت از شبکه‌ها در برابر حملات مختلف DDoS ارائه می‌دهد. برای افزایش اثربخشی مدل، یک رویکرد جدید انتخاب ویژگی معرفی شده است که تحلیل همبستگی، اطلاعات متقابل و تحلیل مؤلفه‌های اصلی را با یکدیگر ترکیب می‌کند. بر اساس نتایج گزارش‌شده در پژوهش، این روش انتخاب ویژگی حتی در چارچوب یک طبقه‌بند منفرد نیز نتایج بهبودیافته‌ای ارائه می‌دهد.

با توجه به ماهیت همواره در حال تحول فناوری و تغییر چشم‌انداز حملات DDoS، مدل با استفاده از طبقه‌بندهای گروهی بهبود یافته است. این یکپارچه‌سازی، توانایی مدل را برای تشخیص انواع جدید و نوظهور حملات DDoS افزایش می‌دهد. بر اساس نتایج گزارش‌شده، این امر موجب افزایش TPR و کاهش FPR مدل می‌شود.

کارایی مدل با استفاده از مجموعه‌داده‌های عمومی مختلف به‌طور دقیق ارزیابی شده است و نتایج گزارش‌شده نشان می‌دهد که مدل در تشخیص انواع مختلف حملات DDoS عملکرد مناسبی دارد. به‌ویژه، استفاده از طبقه‌بند جنگل تصادفی مبتنی بر روش‌های گروهی، در مقایسه با سایر رویکردهای گروهی، در دستیابی به این هدف مؤثر گزارش شده است.

۳. مدل پیشنهادی

در این بخش، رویکرد پیشنهادی برای شناسایی حملات DDoS به‌طور کامل تشریح می‌شود. خط لوله (Pipeline) مدل یادگیری ماشین پیشنهادی شامل دو بخش اصلی، یعنی انتخاب ویژگی‌های مرتبط و طبقه‌بندی با استفاده از جنگل تصادفی مبتنی بر روش‌های گروهی (Ensemble-based Random Forest)، است. نمای کلی این فرایند در شکل ۱ ارائه شده است.

۳.۱ داده‌ها

مدل پیشنهادی با استفاده از مجموعه‌داده‌های مختلف آموزش داده می‌شود تا الگوها و روابط موجود در داده‌ها را فرا بگیرد. سپس، مدل با استفاده از مجموعه‌داده‌های جداگانه مورد آزمایش قرار می‌گیرد تا عملکرد آن ارزیابی شود. برای ارزیابی عملکرد مدل، چندین مجموعه‌داده عمومی مورد استفاده قرار گرفته است که در ادامه توضیح داده می‌شوند.

۳.۱.۱ مجموعه‌داده CIC-DDoS2019

مجموعه‌داده CIC-DDoS2019 که شباهت زیادی به داده‌های دنیای واقعی دارد، شامل جدیدترین حملات DDoS و همچنین ترافیک عادی است. این مجموعه‌داده شامل نتایج تحلیل ترافیک شبکه با استفاده از ابزار CICFlowMeter-V3 است. جریان‌های شبکه بر اساس مهر زمانی (Timestamp)، آدرس‌های IP مبدأ و مقصد، پورت‌های مبدأ و مقصد، پروتکل و نوع حمله برچسب‌گذاری شده‌اند.

این مجموعه‌داده شامل دو نوع اصلی حمله DDoS، یعنی حملات مبتنی بر بازتاب (Reflection-based) و حملات مبتنی بر سوءاستفاده (Exploitation-based)، است. حملات TCP و UDP نیز در هر یک از این دسته‌ها به شیوه‌های متفاوتی اجرا شده‌اند. جدول ۲ فهرست انواع حملات DDoS موجود در این مجموعه‌داده و ویژگی‌های مربوط به آنها را که در این پژوهش مورد استفاده قرار گرفته‌اند، ارائه می‌کند.

جدول ۲ - حملات مختلف در مجموعه داده CIC-DDoS2019

ردیف	تعداد ویژگی‌ها	تعداد ورودی‌ها	نوع حمله
۱	87	1,048,575	MSSQL
۲	88	2,611,374	SSDP
۳	88	2,181,542	LDAP
۴	87	1,048,575	NetBIOS
۵	88	1,217,007	NTP
۶	88	1,217,007	SNMP
۷	88	3,136,802	UDP Flood
۸	88	1,582,681	Syn Flood
۹	87	1,048,575	TFTP
۱۰	88	725,165	UDPLag

۳.۱.۲ مجموعه داده SDN-DDoS

از آنجا که مدل پیشنهادی برای انواع مختلف حملات DDoS و محیط‌های گوناگون طراحی شده است، این مدل با استفاده از یک مجموعه داده مرتبط با شبکه‌های نرم‌افزارمحور (SDN) نیز آموزش داده شده و مورد آزمایش قرار گرفته است.

مجموعه داده SDN-DDoS که در سال ۲۰۲۰ ایجاد شده است، شامل ۲۳ ویژگی و ۱۰۴۰۳۴۵ ردیف است. در این مجموعه داده، ترافیک مخرب شامل حملات طغیان TCP، طغیان UDP و حمله ICMP و همچنین ترافیک عادی شامل TCP، UDP و ICMP شبیه‌سازی شده است. نام کلاس در آخرین ستون قرار دارد و مشخص می‌کند که ترافیک مخرب است یا عادی. برچسب ۱ نشان‌دهنده ترافیک مخرب و برچسب ۰ نشان‌دهنده ترافیک عادی است.

۳.۱.۳ مجموعه داده CIC-IDS2018

مجموعه داده CIC-IDS2018 یک مجموعه داده عمومی است که شامل داده‌های ترافیک شبکه جمع‌آوری شده از یک محیط شبیه‌سازی شده با هدف ارزیابی سیستم‌های تشخیص نفوذ (IDS) است.

در تنظیمات آزمایشی این پژوهش، تنها از فایل 2018-02-21.csv استفاده شده است؛ زیرا این فایل هم شامل حملات، عمدتاً حملات DDoS، و هم شامل داده‌های ترافیک عادی شبکه است.

این مجموعه داده، نمایش جامعی از فعالیت‌های شبکه ارائه می‌دهد. پژوهش با مجموعه‌ای شامل ۱۰۴۸۵۷۵ ورودی آغاز شده است که هر ورودی شامل ۸۰ ویژگی متمایز بوده است. این ویژگی‌ها طیف گسترده‌ای از مشخصه‌های مرتبط با شبکه را پوشش می‌دهند و امکان بررسی و تحلیل ساختار مجموعه داده را فراهم می‌کنند. وجود هم‌زمان ترافیک عادی و داده‌های مربوط به حملات DDoS، محیطی جامع و چالش برانگیز برای ارزیابی عملکرد و اثربخشی مدل فراهم می‌کند.

۳.۱.۴ مجموعه داده DDoS-APA

با افزایش تعداد دستگاه‌های متصل، یکی از چالش‌های اصلی، شناسایی حملات در یک سیستم تشخیص نفوذ توسعه یافته است. انواع مختلفی از حملات DDoS در مجموعه داده DDoS-APA گنجانده شده‌اند. بیشتر حملات DDoS موجود در این مجموعه داده شامل حملات ACK و ACK-PUSH هستند.

از مجموعه داده DDoS-APA برای ارزیابی مدل پیشنهادی در تشخیص حملات DDoS استفاده شده است.

۳.۱.۵ مجموعه داده Botnet-DDoS

برای ارزیابی و پیش‌بینی بسته‌های مخرب ناشی از حملات باتنت DDoS، مجموعه داده‌ای با عنوان Botnet-DDoS وجود دارد. در این پژوهش، ۱۰۹۲۷۱۰۱ ورودی و ۴۷ ویژگی از این مجموعه داده برای ارزیابی مدل استفاده شده است.

حملات DDoS گاهی از باتنت‌ها استفاده می‌کنند؛ زیرا باتنت امکان دسترسی مهاجم به تعداد زیادی دستگاه را فراهم می‌کند که می‌توانند برای تولید حجم زیادی از ترافیک مورد استفاده قرار گیرند. در یک باتنت، رایانه‌ها، تلفن‌های همراه و سایر دستگاه‌های متصل به اینترنت می‌توانند تحت کنترل مهاجم قرار گرفته و به بدافزار آلوده شوند. به همین دلیل، این مجموعه داده برای آزمایش مدل انتخاب شده است.

۳.۲ پیش پردازش داده‌ها

پیش‌پردازش داده‌ها برای یک مدل یادگیری ماشین ضروری است؛ زیرا داده‌های خام را پاک‌سازی و به شکلی تبدیل می‌کند که مدل بتواند آنها را به صورت مؤثر تفسیر کند. مراحل پیش‌پردازش شامل مدیریت مقادیر گمشده، حذف مقادیر پرت (Outliers)، مقیاس‌بندی و نرمال‌سازی است که می‌توانند دقت و کارایی مدل را بهبود دهند.

کیفیت داده‌های ورودی تأثیر مستقیمی بر عملکرد مدل دارد. علاوه بر این، پیش‌پردازش می‌تواند احتمال بیش‌برازش (Overfitting) را کاهش داده و تفسیرپذیری داده‌ها را بهبود بخشد. بنابراین، پیش‌پردازش داده‌ها یکی از مراحل حیاتی خط لوله یادگیری ماشین است که به مدل‌ها امکان می‌دهد پیش‌بینی‌های دقیق و قابل اعتماد تولید کنند.

در مدل پیشنهادی، مراحل پیش‌پردازش شامل حذف داده‌های تکراری، جایگزینی مقادیر بی‌نهایت و مقادیر بزرگ با NaN، حذف ردیف‌های حاوی NaN، جداسازی ستون‌های عددی و دسته‌ای، نرمال‌سازی ستون‌های عددی، رمزگذاری ستون‌های دسته‌ای و تبدیل متغیر هدف به یک متغیر گسسته است.

ابتدا با استفاده از تابع `deduplicated` در کتابخانه `Pandas`، داده‌ها از نظر وجود ورودی‌های تکراری بررسی می‌شوند. در صورت شناسایی داده‌های تکراری، این تابع برای ردیف‌های مربوطه مقدار `True` برمی‌گرداند. سپس ردیف‌های تکراری با استفاده از تابع حذف داده‌های تکراری در `Pandas` از `DataFrame` حذف می‌شوند.

پس از آن، با استفاده از تابع `dropna` در `Pandas`، تمام ردیف‌هایی که دارای مقدار NaN هستند حذف می‌شوند. `DataFrame` باقی‌مانده به ستون‌های عددی و دسته‌ای تقسیم می‌شود. انواع `float64` و `int64` نشان‌دهنده ستون‌های عددی و نوع `Object` نشان‌دهنده ستون‌های دسته‌ای است.

سپس برای نرمال‌سازی ستون‌های عددی از تابع `StandardScaler` در بسته `Scikit-learn` استفاده شده است. این کار تضمین می‌کند که هر ویژگی دارای میانگین صفر و واریانس واحد باشد. برای رمزگذاری ستون‌های دسته‌ای نیز از تابع `LabelEncoder` در بسته `Scikit-learn` استفاده شده است. این فرایند متغیرهای دسته‌ای را به متغیرهای عددی تبدیل می‌کند و برای هر مقدار متمایز، یک مقدار صحیح منحصر به فرد اختصاص می‌دهد.

۳.۳ انتخاب ویژگی‌های مرتبط

انتخاب ویژگی‌های مرتبط با حذف ویژگی‌های غیرضروری و تکراری، موجب کاهش پیچیدگی مدل و بهبود تفسیرپذیری آن می‌شود و از این طریق می‌تواند دقت و اثربخشی مدل‌های یادگیری ماشین را افزایش دهد. در مدل پیشنهادی، ویژگی‌های مرتبط با استفاده از سه روش تحلیل همبستگی (`Correlation Analysis`) یا (`CA`)، اطلاعات متقابل (`Mutual Information`) یا (`MI`) و تحلیل مؤلفه‌های اصلی (`Principal Component Analysis`) یا (`PCA`) انتخاب شده‌اند.

۳.۳.۱ تحلیل همبستگی

تحلیل همبستگی به دلیل توانایی آن در شناسایی ویژگی‌هایی که همبستگی بالایی با یکدیگر دارند و ممکن است موجب بیش‌برازش یا تکرار اطلاعات در مدل شوند، در انتخاب ویژگی برای روش‌های گروهی اهمیت دارد.

استفاده از ویژگی‌های به‌شدت مرتبط می‌تواند موجب شود چندین مدل پیش‌بینی‌های مشابهی تولید کنند و در نتیجه، تنوع مجموعه کاهش یابد. روش‌های گروهی با ترکیب چندین مدل، دقت پیش‌بینی را افزایش می‌دهند. بنابراین، شناسایی و حذف ویژگی‌های دارای همبستگی بالا از طریق تحلیل همبستگی می‌تواند عملکرد و پایداری روش گروهی را بهبود دهد.

در پیاده‌سازی مدل، ابتدا ماتریس همبستگی `corr` برای ویژگی‌های موجود در `X` محاسبه شده و تنها ویژگی‌هایی که ضریب همبستگی مطلق آنها بیشتر از ۰.۵ است انتخاب می‌شوند. ضریب همبستگی به‌صورت کوواریانس بین دو متغیر `X` و `Y` تقسیم بر حاصل ضرب انحراف معیار آنها تعریف می‌شود:

[

$$\text{corr}(X,Y)=\frac{\text{cov}(X,Y)}{\text{std}(X)\times \text{std}(Y)}$$

]

در پیاده‌سازی، مقدار مطلق ماتریس همبستگی گرفته می‌شود تا متغیر `abs_corr` ایجاد شود. این کار باعث می‌شود قدرت رابطه خطی میان دو متغیر، صرف‌نظر از مثبت یا منفی بودن ضریب همبستگی، در نظر گرفته شود.

سپس با استفاده از اندیس ستون‌هایی که ضریب همبستگی مطلق آنها بزرگ‌تر از ۰.۵ است، فهرست ویژگی‌های مرتبط ایجاد می‌شود:

```
relevant_features_corr = corr_abs[corr_abs > 0.5].index.tolist()
```

فهرست `relevant_features_corr` نام ویژگی‌هایی را شامل می‌شود که ارتباط زیادی با یکدیگر دارند و بنابراین ممکن است اطلاعات تکراری داشته باشند. حذف یا ترکیب این ویژگی‌ها می‌تواند به کاهش ابعاد مجموعه داده و بهبود عملکرد مدل کمک کند.

۳.۳.۲ اطلاعات متقابل

اطلاعات متقابل (Mutual Information) معیاری برای ارزیابی وابستگی میان دو متغیر تصادفی است. در زمینه انتخاب ویژگی، این معیار میزان اطلاعاتی را که یک ویژگی درباره متغیر هدف ارائه می‌دهد، ارزیابی می‌کند.

در پیاده‌سازی این مدل، `k` ویژگی برتر که بیشترین اطلاعات را درباره متغیر هدف دارند انتخاب می‌شوند. ویژگی‌هایی که بر اساس اطلاعات متقابل انتخاب می‌شوند، انتظار می‌رود قوی‌ترین رابطه آماری را با متغیر هدف داشته باشند و از این رو برای مدل‌سازی و تحلیل اهمیت بیشتری داشته باشند.

در این پژوهش، از تابع `mutual_info_classif` و سپس تابع `SelectKBest` برای انتخاب `k` ویژگی برتر استفاده شده است:

```
mutual_info = SelectKBest(mutual_info_classif, k=20).fit(X, y)
```

سپس ویژگی‌های منتخب به شکل زیر استخراج می‌شوند:

```
relevant_features_mutual = X.columns[mutual_info.get_support()].tolist()
```

بنابراین، ۲۰ ویژگی دارای بالاترین امتیاز اطلاعات متقابل انتخاب می‌شوند.

۳.۳.۳ تحلیل مؤلفه‌های اصلی

تحلیل مؤلفه‌های اصلی (PCA) روشی برای کاهش ابعاد داده‌های ورودی است که با شناسایی مهم‌ترین مؤلفه‌هایی که بیشترین میزان واریانس داده‌ها را حفظ می‌کنند، تعداد ابعاد را کاهش می‌دهد.

اگر ماتریس داده X شامل n نمونه و m ویژگی باشد، PCA تلاش می‌کند مجموعه‌ای از k بردار متعامد را در فضای m -بعدی پیدا کند، به گونه‌ای که واریانس داده‌ها پس از تصویرسازی (Projection) روی زیرفضای ایجادشده توسط این بردارها به حداکثر برسد.

ستون‌های ماتریس حاصل از تصویرسازی داده‌های اصلی روی زیرفضای پوشش داده‌شده توسط بردارهای ویژه، مؤلفه‌های اصلی را تشکیل می‌دهند.

در پیاده‌سازی این پژوهش، تحلیل PCA روی داده‌های ورودی X با استفاده از کلاس PCA در بسته Scikit-learn انجام شده است. تعداد مؤلفه‌ها برابر با ۲۰ تنظیم شده است. ماتریس `components_` از شیء PCA ایجاد شده و اندیس ویژگی‌هایی که بیشترین مقدار مطلق را در هر مؤلفه دارند، با استفاده از تابع `argmax` تعیین می‌شوند. سپس ویژگی‌های کلیدی با نگاشت این اندیس‌ها به نام ویژگی‌های اصلی موجود در `X.columns` استخراج می‌شوند:

```
pca = PCA(n_components=20)
```

```
relevant_features_pca = X.columns[pca.components_.argmax(axis=1)].tolist()
```

۳.۳.۴ ترکیب ویژگی‌های منتخب

در نهایت، یک فهرست واحد از ویژگی‌های مرتبط که از هر سه روش تحلیل همبستگی، اطلاعات متقابل و تحلیل مؤلفه‌های اصلی انتخاب شده‌اند، ایجاد می‌شود. ترکیب نهایی این سه مجموعه با استفاده از اجتماع مجموعه‌ها انجام شده است:

```
relevant_features = list(set()).union(
```

```
    relevant_features_corr,
```

```
    relevant_features_mutual,
```

```
    relevant_features_pca
```

```
))
```

بر اساس متن پژوهش، این فرایند مجموعه‌ای قابل اعتمادتر و دقیق‌تر از ویژگی‌ها ایجاد می‌کند که مهم‌ترین اطلاعات داده را منعکس می‌کنند. در نتیجه، عملکرد مدل بهبود می‌یابد و اطلاعات بیشتری درباره روابط میان ویژگی‌ها و متغیر هدف به دست می‌آید. این روش انتخاب ویژگی یکی از اجزای اصلی مدل پیشنهادی برای بهبود عملکرد تشخیص حملات DDoS است.

۳.۴ انتخاب طبقه‌بندهای گروهی مبتنی بر جنگل تصادفی

طبقه‌بندهای یادگیری ماشین مبتنی بر روش‌های گروهی (Ensemble) به دلیل نرخ تشخیص بهتر و مقاومت در برابر حملات، گزینه‌ای برای سیستم‌های تشخیص نفوذ، به ویژه در تشخیص حملات DDoS، محسوب می‌شوند. این طبقه‌بندها چندین مدل مجزا را برای افزایش دقت کلی و پایداری پیش‌بینی با یکدیگر ترکیب می‌کنند.

از آنجا که روش‌های گروهی می‌توانند از طبقه‌بندهای متنوعی تشکیل شوند، امکان شناسایی انواع و الگوهای مختلف حملات DDoS فراهم می‌شود. مدل پیشنهادی از هر دو نوع تنوع، یعنی طبقه‌بندهای منفرد و طبقه‌بندهای گروهی یادگیری ماشین، استفاده می‌کند. بر اساس نتایج گزارش‌شده در پژوهش، در میان رویکردهای مختلف گروهی، جنگل تصادفی (Random Forest) بهترین نتایج را ارائه می‌دهد.

طبقه‌بندهای گروهی مبتنی بر جنگل تصادفی با ترکیب چندین درخت تصمیم برای افزایش دقت و استحکام مدل در تشخیص حملات DDoS به کار گرفته می‌شوند. این روش از تنوع موجود میان درخت‌های منفرد برای شناسایی جمعی الگوهای حمله استفاده می‌کند و از این نظر در تمایز میان ترافیک عادی شبکه و انواع مختلف حملات DDoS مؤثر است.

جنگل تصادفی با ترکیب تعداد زیادی درخت تصمیم و استفاده از رویکرد یادگیری ماشین مبتنی بر روش‌های گروهی، یک نتیجه نهایی برای طبقه‌بندی تولید می‌کند. هر درخت تصمیم به‌صورت مستقل و با استفاده از یک زیرمجموعه تصادفی از داده‌های آموزشی و ویژگی‌ها ساخته می‌شود. این فرایند با هدف کاهش بیش‌برازش (Overfitting) و بهبود قابلیت تعمیم مدل انجام می‌شود.

نتیجه نهایی جنگل تصادفی بر اساس رأی اکثریت درخت‌های تصمیم مختلف تعیین می‌شود. هر درخت، کلاس پیش‌بینی‌شده برای نمونه ورودی را اعلام می‌کند و کلاسی که بیشترین تعداد رأی را به دست آورد، به‌عنوان نتیجه نهایی در نظر گرفته می‌شود.

الگوریتم ۱ - فرایند عملکرد طبقه‌بند جنگل تصادفی مبتنی بر روش‌های گروهی برای تشخیص حملات DDoS

پارامترهای مورد استفاده برای طبقه‌بند جنگل تصادفی در مدل پیشنهادی در جدول ۳ ارائه شده‌اند.

۴. نتایج آزمایش و تحلیل

در این بخش، عملکرد مدل پیشنهادی برای تشخیص حملات DDoS ارزیابی می‌شود. پیش از ارائه نتایج، محیط آزمایش و معیارهای ارزیابی مورد استفاده به‌طور خلاصه تشریح می‌شوند.

در این پژوهش، از زبان برنامه‌نویسی Python و کتابخانه Scikit-learn استفاده شده است. آزمایش‌ها با استفاده از محیط Google Colaboratory که معمولاً با نام Google Colab شناخته می‌شود، انجام شده‌اند. برای پیش‌پردازش داده‌ها، از ماژول‌هایی مانند StandardScaler و LabelEncoder در Scikit-learn استفاده شده است. همچنین، برای انتخاب ویژگی‌های مرتبط، روش‌های PCA، `mutual_info_classif` و `SelectKBest` به کار گرفته شده‌اند.

برای ارزیابی طبقه‌بندهای مبتنی بر روش‌های گروهی، طبقه‌بندهای `AdaBoostClassifier`، `BaggingClassifier`، `XGBClassifier`، `RandomForestClassifier` و `GradientBoostingClassifier` مورد آزمایش قرار گرفتند. همچنین طبقه‌بندهای کلاسیک شامل `GaussianNB`، `MLPClassifier`، `KNeighborsClassifier` و `LogisticRegression` نیز ارزیابی شدند.

مدل با استفاده از معیارهای مختلفی شامل منحنی ROC، امتیاز ROC-AUC، ضریب کاپای کوهن (Cohen's Kappa)، ماتریس درهم‌ریختگی (Confusion Matrix)، دقت (Accuracy)، صحت (Precision)، نرخ مثبت کاذب (FPR)، بازخوانی (Recall)، دقت متوازن (BACC) و امتیاز F1 ارزیابی شد.

۴.۱ معیارهای ارزیابی

معیارهای ارزیابی برای سنجش عملکرد یک مدل مورد استفاده قرار می‌گیرند. در مدل پیشنهادی تشخیص حملات DDoS، معیارهایی مانند دقت (Accuracy)، بازخوانی (Recall)، صحت (Precision)، امتیاز F1، نرخ مثبت کاذب (FPR)، نرخ مثبت واقعی (TPR)، دقت متوازن (BACC)، مساحت زیر منحنی (AUC)، نرخ خطا، دقت آموزش، دقت آزمون و ضریب کلپای کوهن مورد استفاده قرار گرفته‌اند. این معیارها دیدگاهی جامع از عملکرد مدل ارائه می‌دهند و برای ارزیابی توانایی آن در تشخیص دقیق حملات DDoS و حفظ نرخ مثبت کاذب پایین به کار می‌روند.

۴.۱.۱ ماتریس درهم‌ریختگی

ماتریس درهم‌ریختگی تعداد پیش‌بینی‌های صحیح و نادرست مدل را در مقایسه با برچسب‌های واقعی داده‌های آزمون نشان می‌دهد. این ماتریس معمولاً مربعی است؛ به گونه‌ای که سطرها نشان‌دهنده کلاس‌های واقعی و ستون‌ها نشان‌دهنده کلاس‌های پیش‌بینی شده هستند.

در یک مسئله طبقه‌بندی دودویی، چهار حالت ممکن عبارت‌اند از:

- **مثبت واقعی (TP):** نمونه مثبت به درستی توسط مدل شناسایی شده است.
- **مثبت کاذب (FP):** نمونه منفی به اشتباه به عنوان نمونه مثبت شناسایی شده است.
- **منفی واقعی (TN):** نمونه منفی به درستی توسط مدل شناسایی شده است.
- **منفی کاذب (FN):** نمونه مثبت به اشتباه به عنوان نمونه منفی شناسایی شده است.

با استفاده از مقادیر حاصل از ماتریس درهم‌ریختگی، می‌توان معیارهای مختلف ارزیابی را محاسبه کرد. این معیارها برای ارزیابی استحکام و قابلیت اطمینان مدل در شناسایی حملات DDoS در شرایط و محیط‌های مختلف مورد استفاده قرار می‌گیرند.

۴.۱.۲ فرمول معیارهای ارزیابی

دقت (Accuracy):

$$[\text{Accuracy} = \frac{TP+TN}{TP+FP+FN+TN}]$$

این معیار عملکرد مدل را از نظر تشخیص صحیح نمونه‌ها ارزیابی می‌کند.

بازخوانی: (Recall)

$$\text{Recall} = \frac{TP}{FN + TP}$$

این معیار نسبت نمونه‌های مثبت واقعی را که مدل به درستی شناسایی کرده است، اندازه‌گیری می‌کند.

صحت: (Precision)

$$\text{Precision} = \frac{TP}{FP + TP}$$

این معیار میزان صحت پیش‌بینی‌های مثبت مدل را نشان می‌دهد.

امتیاز: F1

$$F1 = 2 \times \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}}$$

این معیار تعادلی میان توانایی مدل در شناسایی صحیح نمونه‌های مثبت و توانایی آن در کاهش مثبت‌های کاذب ایجاد می‌کند.

نرخ مثبت کاذب: (FPR)

$$\text{FPR} = \frac{FP}{TN + FP}$$

این معیار درصد نمونه‌های منفی را که مدل به اشتباه مثبت تشخیص داده است، نشان می‌دهد.

دقت متوازن: (BACC)

$$\text{BACC} = \frac{\text{Sensitivity} + \text{Specificity}}{2}$$

دقت متوازن میانگین حساسیت و ویژگی مندی است و یک مقدار واحد برای نمایش عملکرد کلی مدل ارائه می‌دهد.

نرخ خطا: (Error Rate)

$$\begin{aligned} &[\\ \text{Error\ Rate} &= \\ \frac{\text{Number\ of\ Misclassified\ Instances}}{\text{Total\ Number\ of\ Instances}} & \\ &] \end{aligned}$$

این معیار نسبت نمونه‌های اشتباه طبقه‌بندی شده به کل نمونه‌های موجود در مجموعه داده را اندازه‌گیری می‌کند.

ضریب کاپای کوهن: (Cohen's Kappa)

$$\begin{aligned} &[\\ K &= \frac{P_o - P_e}{1 - P_e} \\ &] \end{aligned}$$

در این رابطه، (P_o) نشان‌دهنده میزان توافق مشاهده شده میان پیش‌بینی‌های مدل و برچسب‌های واقعی و (P_e) نشان‌دهنده میزان توافق مورد انتظار در اثر شانس است. ضریب کاپای کوهن امکان ارزیابی میزان توافق میان پیش‌بینی‌های مدل و مقادیر واقعی را فراهم می‌کند و احتمال توافق تصادفی را نیز در نظر می‌گیرد.

دقت آموزش و دقت آزمون

دقت آموزش به صورت نسبت تعداد نمونه‌های صحیح طبقه‌بندی شده در داده‌های آموزشی به کل نمونه‌های آموزشی تعریف می‌شود:

$$\begin{aligned} &[\\ \text{Training\ Accuracy} &= \\ \frac{\text{Correctly\ Classified\ Training\ Instances}}{\text{Total\ Training\ Instances}} & \\ &] \end{aligned}$$

دقت آزمون نیز نسبت تعداد نمونه‌های صحیح طبقه‌بندی شده در داده‌های آزمون به کل نمونه‌های آزمون است:

$$\begin{aligned} &[\\ \text{Test\ Accuracy} &= \\ \frac{\text{Correctly\ Classified\ Test\ Instances}}{\text{Total\ Test\ Instances}} & \\ &] \end{aligned}$$

دقت آموزش عملکرد مدل را روی داده‌هایی که با آنها آموزش دیده است اندازه‌گیری می‌کند، در حالی که دقت آزمون عملکرد مدل را روی داده‌هایی که در فرایند آموزش مشاهده نکرده است ارزیابی می‌کند.

۴.۲ تحلیل یافته‌ها

جدول ۵ نتایج ارزیابی مدل پیشنهادی ERF-HFS را برای انواع مختلف حملات DDoS در مجموعه داده CIC-DDoS2019 نشان می‌دهد. حملات موجود در این مجموعه داده به دو گروه حملات بازتابی (Reflection) و حملات مبتنی بر بهره‌برداری (Exploitation) تقسیم شده‌اند. عملکرد مدل بر اساس معیارهای دقت، بازخوانی، صحت، امتیاز F1 و AUC ارزیابی شده است.

بر اساس نتایج جدول ۵، مدل برای حملات بازتابی شامل NetBIOS، LDAP، SSDP، MSSQL، SNMP، NTP و TFTP در تمامی معیارهای گزارش شده امتیاز ۱۰۰ کسب کرده است. برای حملات مبتنی بر بهره‌برداری، شامل UDP Flood و Syn Flood، نیز تمامی معیارها مقدار ۱۰۰ را نشان می‌دهند.

برای حمله UDPLag، مدل دقت ۰٫۹۹۹۹ را به دست آورده است. بازخوانی و امتیاز F1 برای این حمله هر دو برابر با ۱۰۰ گزارش شده‌اند. بر اساس نتایج ارائه شده در مقاله، این عملکرد نشان می‌دهد که مدل توانسته است نمونه‌های حمله را به درستی شناسایی کند.

در ادامه، همان روش‌های تشریح شده در بخش «مدل پیشنهادی» برای ثبت نتایج مدل روی مجموعه داده‌های مختلف استفاده شده‌اند و تنها مجموعه داده مورد استفاده در آزمایش تغییر کرده است. سپس عملکرد مدل در تشخیص حملات DDoS با عملکرد سایر مدل‌های تشخیص مقایسه شده است.

شکل ۲ عملکرد طبقه‌بندهای کلاسیک یادگیری ماشین، شامل رگرسیون لجستیک (LR)، بیز ساده گاوسی (GNB)، نزدیک‌ترین همسایه‌ها (KNN)، شبکه عصبی مصنوعی (ANN) و ماشین بردار پشتیبان (SVM)، را با مدل پیشنهادی مبتنی بر طبقه‌بند جنگل تصادفی گروهی (ERF) مقایسه می‌کند. این نمودار برای حمله NTP_DrDoS در مجموعه داده CIC-DDoS2019 تولید شده است.

۴.۲.۱ مقایسه طبقه‌بندهای گروهی

طبقه‌بند جنگل تصادفی در مقایسه با سایر طبقه‌بندهای مبتنی بر روش‌های گروهی، عملکرد بهتری از نظر تشخیص حملات DDoS، نرخ مثبت کاذب پایین و کارایی محاسباتی نشان داده است.

زمان آزمایش گزارش شده برای جنگل تصادفی ۰٫۱۶۲۱۶ ثانیه است. در مقایسه، زمان آزمایش Bagging برابر با ۰٫۸۶۱۴۵ ثانیه، AdaBoost برابر با ۰٫۴۴۹۶۲ ثانیه و Simple Stacking برابر با ۱۲٫۵۸۳۶۴ ثانیه گزارش شده است.

بر اساس جدول ۶، جنگل تصادفی دارای Recall برابر با ۱٫۰۰۰۰۰۰، F1 برابر با ۱٫۰۰۰۰۰۰ و FPR برابر با ۰٫۰۰۰۰۰۰ است. در مقابل، Bagging، AdaBoost و Simple Stacking هر سه Recall برابر با ۰٫۹۹۶۳۱، F1 برابر با ۰٫۹۹۸۱۵ و FPR برابر با ۰٫۰۰۳۶۹ دارند.

بنابراین، بر اساس نتایج گزارش شده، طبقه‌بند جنگل تصادفی در میان طبقه‌بندهای مبتنی بر روش‌های گروهی، گزینه برتر برای تشخیص حملات DDoS در مدل پیشنهادی در نظر گرفته شده است.

۴.۲.۲ منحنی ROC و AUC

منحنی ROC نمایش بصری رابطه میان نرخ مثبت واقعی (TPR) و نرخ مثبت کاذب (FPR) یک طبقه‌بند در آستانه‌های مختلف تشخیص است. در این نمودار، TPR روی محور عمودی و FPR روی محور افقی قرار دارد. یک طبقه‌بند ایده‌آل باید به TPR برابر با ۱ و FPR برابر با صفر دست یابد.

منحنی ROC ارائه‌شده در شکل ۳ عملکرد طبقه‌بندهای مختلف را روی مجموعه‌داده CIC-DDoS2019 برای حمله NTP_DrDoS نشان می‌دهد. بر اساس نتایج گزارش‌شده، طبقه‌بند جنگل تصادفی بالاترین مقدار AUC، برابر با ۱،۰۰۰۰۰۰ را در میان طبقه‌بندهای ارزیابی‌شده به دست آورده است.

پس از آن، مقادیر AUC مربوط به طبقه‌بندهای Bagging، Gradient Boosting، Stacking، شبکه عصبی مصنوعی (ANN)، KNN، AdaBoost، SVM، رگرسیون لجستیک (LR) و بیز ساده گاوسی (GNB) قرار دارند.

۴.۲.۳ ارزیابی روی مجموعه‌داده‌های مختلف

یافته‌های مربوط به عملکرد مدل ERF-HFS روی مجموعه‌داده‌های مختلف در جدول ۷ ارائه شده‌اند. نتایج گزارش‌شده عبارت‌اند از:

	Accuracy	Recall	Precision	F1-score	FPR	AUC	BACC
CSE-CIC-IDS2018	1.0000	1.0000	1.0000	1.0000	0.0000	1.0000	1.0000
DDoS-SDN	1.0000	1.0000	1.0000	1.0000	0.0000	1.0000	1.0000
APA-DDoS	1.0000	1.0000	1.0000	1.0000	0.0000	1.0000	1.0000
Botnet-DDoS	1.0000	1.0000	1.0000	1.0000	0.0000	1.0000	1.0000

بر اساس نتایج گزارش‌شده، مدل ERF-HFS در مجموعه‌داده‌های مختلف عملکرد بسیار بالایی در تشخیص حملات DDos نشان داده است.

در جدول ۸ نیز نتایج ارزیابی‌های تکمیلی مدل روی مجموعه‌داده‌های مختلف ارائه شده است. این نتایج برای بررسی اثربخشی مدل در سناریوهای مختلف حملات DDos و شرایط محیطی متفاوت گزارش شده‌اند.

طبق متن مقاله، دقت آموزش مدل برای تمام مجموعه‌داده‌ها برابر با ۱۰۰ بوده است. دقت آزمون نیز بسیار بالا گزارش شده و نرخ خطا برای بیشتر مجموعه‌داده‌ها تقریباً صفر بوده است.

در ادامه، ضریب کاپای کوهن با استفاده از دقت مشاهده‌شده (P_o) و دقت مورد انتظار (P_e) محاسبه شده است. بر اساس نتایج گزارش‌شده، مقدار (P_o) برای تمام مجموعه‌داده‌ها در بازه ۰،۹۹۹۹۹ تا ۱۰۰ قرار دارد.

برای مجموعه‌داده CIC-DDoS2019، مقادیر AUC گزارش‌شده برای انواع مختلف حملات نیز بسیار بالا هستند. برای مثال، AUC مربوط به MSSQL برابر با ۰،۹۹۸۸۲، SSDP برابر با ۰،۹۹۹۶۲، LDAP برابر با ۰،۹۹۸۸۴، NetBIOS برابر با ۰،۹۹۹۴۷، NTP برابر با ۰،۹۹۷۳۲، SNMP برابر با ۰،۹۹۹۸۲، UDP Flood برابر با ۰،۹۹۹۵۵، Syn Flood برابر با ۰،۹۹۹۵۵.

۰۰۹۹۹۵۲، TFTP برابر با ۰۰۹۹۹۳۱ و UDPLag برابر با ۰۰۹۹۸۸۴ گزارش شده است. برای DDoS-SDN مقدار AUC برابر با ۰۰۵۲۷۰۸ و برای Botnet-DDoS برابر با ۰۰۹۹۹۴۲ گزارش شده است.

۴.۲.۴ بررسی تعداد درخت‌های جنگل تصادفی

شکل ۵ رابطه میان تعداد درخت‌های تصمیم در طبقه‌بند جنگل تصادفی و دقت آموزش و آزمون مدل را نشان می‌دهد. این تحلیل بر اساس داده‌های آزمایشی مجموعه داده CIC-DDoS2019 برای نوع حمله NTP انجام شده است.

محور افقی تعداد درخت‌های تصمیم و محور عمودی دقت مدل را نشان می‌دهد. بر اساس متن مقاله، دقت آموزش از مقدار بسیار بالایی، نزدیک به ۱، آغاز شده و با افزایش تعداد درخت‌ها همچنان بالا باقی می‌ماند. دقت آزمون نیز با تغییر تعداد درخت‌ها در سطح بالایی حفظ شده است.

بر اساس نتایج گزارش شده، ۱۰ درخت به عنوان تعداد بهینه برای طبقه‌بند جنگل تصادفی مبتنی بر روش‌های گروهی تعیین شده است؛ زیرا این تعداد، بهترین دقت آموزش و آزمون را ایجاد کرده است. همچنین، عدم وجود تفاوت معنادار میان دقت آموزش و آزمون به عنوان نشانه‌ای از نبود مشکل قابل توجه بیش‌برازش در مدل تفسیر شده است.

۴.۳ مقایسه عملکرد با مدل‌های موجود

جدول ۹ عملکرد مدل پیشنهادی ERF-HFS را با مدل‌های مختلف یادگیری ماشین برای تشخیص حملات DDoS بر اساس چهار معیار Accuracy، Recall، Precision و F1-score مقایسه می‌کند.

	Accuracy (%)	Recall (%)	Precision (%)	F1-score (%)
GHLBO-based DSA [35]	91.40	90.90	*	*
GBT [30]	93.62	93.63	96.28	94.41
CNN-DSFO [57]	98.85	93.42	*	91.65
LSTM [33]	98.00	97.00	98.00	97.00
J48 [31]	98.31	98.30	98.30	98.30
MLP [34]	98.99	*	*	*
DCNN [32]	99.77	99.77	99.77	99.77
HFS-ERF پیشنهادی	100.0	100.0	100.0	100.0

*در مقاله مقدار این معیار گزارش نشده است.

بر اساس جدول ۹، مدل پیشنهادی ERF-HFS در هر چهار معیار گزارش شده عملکرد بالاتری نسبت به مدل‌های مقایسه شده دارد. بیشتر مدل‌های مورد مقایسه از مجموعه داده CIC-DDoS2019 استفاده کرده‌اند. بر اساس نتایج ارائه شده در مقاله، مدل پیشنهادی بهترین عملکرد را در تشخیص حملات DDoS نشان می‌دهد.

۵. نتیجه‌گیری و جهت‌گیری‌های آینده

رویکرد پیشرفته ارائه‌شده برای تشخیص حملات DDoS، با استفاده از روش انتخاب ویژگی ترکیبی و طبقه‌بند جنگل تصادفی مبتنی بر روش‌های گروهی (Ensemble)، عملکرد بسیار خوبی را در مقایسه با تکنیک‌های موجود نشان داده است.

ترکیب روش‌های مختلف انتخاب ویژگی و طبقه‌بندهای مبتنی بر روش‌های گروهی، نتایج بسیار مطلوبی به همراه داشته است. این رویکرد به دقتی نزدیک به کامل و عملکردی برجسته در طیف گسترده‌ای از معیارهای ارزیابی دست یافته است و بر اساس نتایج گزارش شده در پژوهش، راهکاری بسیار امیدوارکننده برای تشخیص حملات DDoS در محیط‌های واقعی محسوب می‌شود.

در این پژوهش، از یک روش نوین انتخاب ویژگی استفاده شده است که تحلیل همبستگی، اطلاعات متقابل و تحلیل مؤلفه‌های اصلی را با یکدیگر ترکیب می‌کند. سپس این روش انتخاب ویژگی با طبقه‌بندهای مختلف یادگیری ماشین، به‌ویژه طبقه‌بند جنگل تصادفی مبتنی بر روش‌های گروهی، یکپارچه شده است.

نتایج ارزیابی نشان می‌دهند که روش پیشنهادی در مقایسه با سایر روش‌های مورد بررسی، عملکرد بهتری ارائه می‌دهد. مدل پیشنهادی به دقت ۱۰۰ درصد، Recall برابر با ۱۰۰ درصد، Precision برابر با ۱۰۰ درصد و F1-score برابر با ۱۰۰ درصد دست یافته است. همچنین، نرخ مثبت کاذب (FPR) برابر با صفر گزارش شده است.

بر اساس نتایج ارائه‌شده، مدل پیشنهادی توانسته است در مجموعه داده‌های عمومی مختلف عملکرد بالایی داشته باشد و انواع مختلف حملات DDoS را شناسایی کند. این نتایج نشان می‌دهند که ترکیب انتخاب ویژگی و یادگیری ماشین مبتنی بر روش‌های گروهی می‌تواند برای تشخیص حملات DDoS مؤثر باشد.

در مجموع، پژوهش حاضر یک رویکرد جامع برای تشخیص حملات DDoS ارائه می‌کند که با استفاده از انتخاب ویژگی ترکیبی و طبقه‌بندی مبتنی بر روش‌های گروهی، عملکرد بالایی در معیارهای مختلف ارزیابی نشان داده است. این روش می‌تواند به‌عنوان یک راهکار امیدوارکننده برای بهبود تشخیص حملات DDoS مورد استفاده قرار گیرد.

Enhancing DDoS Attack Detection Using Hybrid Feature Selection and Ensemble Classifiers: A Promising Approach for Resilient Cybersecurity

Armin Bagheri Fard | arminbagheri@gmail.com

M.Sc. in Computer Engineering (Computer Networks), Islamic Azad University, Kish Branch

Security Specialist, Mobile Network Operator, Kish Free Zone

Abstract

Distributed Denial-of-Service (DDoS) attacks—which generate massive traffic volumes from multiple sources to saturate target systems—pose a serious threat to computer networks and systems. Consequently, the real-time detection of these attacks has become a critical task in cybersecurity. However, many existing DDoS detection methods face challenges such as high false-positive rates and limited ability to identify complex attack traffic patterns.

This research presents an improved approach to DDoS attack detection that integrates a hybrid feature selection method with ensemble classifiers. The ensemble approach enhances classification accuracy and reduces the likelihood of overfitting by combining multiple decision trees, thereby improving model robustness. The proposed feature selection method identifies the most effective features for attack detection by combining Correlation Analysis, Mutual Information, and Principal Component Analysis (PCA).

Among various ensemble machine learning methods, the Ensemble Random Forest classifier—utilizing the selected features—demonstrates the best detection performance. The proposed model has been evaluated using several public datasets related to DDoS attack detection. Experimental results demonstrate that the model outperforms existing methods in terms of metrics such as accuracy, recall, precision, F1-score, and false positive rate. The findings indicate that the proposed approach achieves an accuracy close to 100%, a true positive rate (TPR) of 100%, and an error rate of 0%. These results establish the proposed method as a promising solution for the effective detection of DDoS attacks.

Keywords: DDoS attacks; DDoS attack detection; hybrid feature selection; ensemble machine learning; ensemble-based DDoS attack detection; ensemble random forest; cybersecurity.