بیست و هشتمین کنفرانس بین‌المللی کامپیوتر انجمن کامپیوتر ایران

تشخیص حمله انکارسرویس‌توزیع‌شده مبتنی بر بازتاب در اینترنت‌وسایل‌نقلیه با استفاده از یادگیری گروهی

زهرا جانفدا[۱]، سید امین حسینی سنو[۲]، سمیه سلطانی[۳]

[۱] گروه مهندسی کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی مشهد
zahra.janfada@mail.um.ac.ir

[۲] دانشیار، گروه مهندسی کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی مشهد
hosseini@um.ac.ir

[۳] گروه مهندسی کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی مشهد
somayeh.soltani@mail.um.ac.ir

چکیده

امروزه با افزایش تعداد وسایل‌نقلیه متصل به اینترنت‌اشیا (IoT)، شبکه‌های اقتضایی خودرو (VANET) در حال تغییر به اینترنت‌وسایل‌نقلیه (IoV) هستند. یکی از اهداف مهم اینترنت‌وسایل‌نقلیه این است که وسایل نقلیه بتوانند با رانندگان، عابران پیاده، سایر وسایل‌نقلیه و زیرساخت‌های کنارجاده‌ای بصورت بلادرنگ ارتباط برقرار کنند. اما حمله انکارسرویس توزیع شده (DDoS) یکی از حمله‌های جدی در این محیط محسوب می‌شود. این حمله می‌تواند سرویس‌های اینترنت‌وسایل‌نقلیه را مختل کند و باعث ترافیک و تصادفات جاده‌ای شده و ایمنی کاربران را به خطر اندازد. از طرفی، تشخیص حمله انکارسرویس توزیع شده مبتنی بر بازتاب (DrDoS) به دلیل هویت پنهان آن دشوارتر است. بنابراین یک راه حل مبتنی بر یادگیری گروهی برای شناسایی انواع مختلف حمله انکارسرویس‌توزیع شده مبتنی بر بازتاب در محیط اینترنت‌وسایل‌نقلیه پیشنهاد شده است. مدل پیشنهادی از الحاق دو مدل شبکه عصبی کانولوشن تشکیل شده است که این دو مدل با رویکرد بیزی با استفاده از براوردگرهای Parzen باساختار درختی، بهینه سازی شدند. عملکرد مدل پیشنهادی با مجموعه داده جدید CICDDoS2019 ارزیابی شده است. نتایج تجربی نشان می‌دهد که سیستم تشخیص نفوذ پیشنهادی به نرخ صحت ۹۹٪ رسیده است.

کلمات کلیدی

اینترنت‌وسایل‌نقلیه، امنیت، حمله انکارسرویس‌توزیع شده مبتنی بر بازتاب، سیستم تشخیص نفوذ، یادگیری گروهی

۱- مقدمه

اینترنت‌وسایل‌نقلیه (IoV[۱]) یک نوع خاص از اینترنت‌اشیا است که دستیابی به مدیریت یکپارچه درحمل‌ونقل‌هوشمند و سایر کاربردهای شهرهوشمند را فراهم می‌کند [1]. بهبود ایمنی عابران و رانندگان، نظارت بر ترافیک و راحتی مسافران از اهداف اصلی در طراحی محیط اینترنت‌وسایل‌نقلیه است [2].

اما ارتباطات اینترنت‌وسایل‌نقلیه در برابر حملات مختلف آسیب‌پذیر هستند. اگر محیط اینترنت‌وسایل‌نقلیه توسط حمله نفوذی به خطر بیفتد، می‌تواند عامل ایمنی را به خطر بیاندازد زیرا هکرها می‌توانند کنترل مستقیمی بر وسایل‌نقلیه داشته باشند و منجر به تصادف شوند [3]. بنابراین سیستم‌های تشخیص نفوذ از الزامات اساسی در محیط اینترنت‌وسایل‌نقلیه محسوب می‌شوند زیرا وظیفه شناسایی و تشخیص هر گونه استفاده غیرمجاز یا سوءاستفاده از شبکه را بر عهده دارند.

حمله انکارسرویس (DoS[۲]) حمله مهمی هست که دردسترس‌بودن اینترنت‌وسایل‌نقلیه را به خطر می اندازد. بنابراین یک مشکل جدی است. ارتباطات در برنامه‌های ایمنی و حیاتی اینترنت‌وسایل‌نقلیه مهم است و برای جلوگیری از حوادث، به اطلاعات بلادرنگ نیاز است [4]. از سوی دیگر، حمله انکارسرویس‌توزیع‌شده (DDoS[۳]) نوع شدیدتری از حمله انکارسرویس است که به صورت توزیع شده انجام می‌شود. در یک حمله انکارسرویس‌توزیع‌شده، چندین وسیله‌نقلیه مخرب به گره قانونی حمله می‌کنند و از زمان‌ها و مکان‌های مختلف برای دستیابی به اهداف خود که جلوگیری از دسترسی کاربران به خدمات شبکه است، استفاده می‌کنند [5]. این حمله می‌تواند بر روی وسایل نقلیه یا واحدهای کنار جاده‌ای (RSU[۴]) انجام شود.

از طرفی در حمله انکارسرویس‌توزیع‌شده مبتنی بر بازتاب (DrDoS[۵])، چندین وسیله نقلیه قربانی بطورناخواسته اما با هدف مهاجم در حمله انکارسرویس‌توزیع‌شده شرکت می‌کنند تا درخواست‌ها را به سمت مقصد ارسال کنند. بنابراین تشخیص این حملات دشوارتر است زیرا هویت مهاجم پنهان است [6].

اخیراً تکنیک‌های یادگیری ماشین و یادگیری عمیق باتوجه به کاربرد آن‌ها در امنیت شبکه خودرویی، توجه محققان را به خود جلب کرده است [7]. تکنیک‌های یادگیری عمیق به طور گسترده برای توسعه سیستم های تشخیص نفوذ (IDS[۶]) استفاده می‌شوند که می‌توانند حملات سایبری مختلف را از ترافیک عادی شبکه تشخیص دهند.

علادی و همکاران [8] یک سیستم تشخیص نفوذ مبتنی بر شبکه عصبی عمیق (DNN[۷]) برای شبکه‌های خودرویی پیشنهاد دادند. این سیستم تشخیص نفوذ پیشنهادی با اسقرار در واحدهای کنارجاده‌ای و دریافت تمام داده‌های همه‌پخشی وسایل‌نقلیه و دسته‌بندی آن‌ها به ترافیک مخرب و عادی، تشخیص ناهنجاری را انجام می‌دهد. برای ارزیابی عملکرد این سیستم تشخیص نفوذ پیشنهادی، سه سناریو، فقط خطا، فقط حمله و ناهنجاری کامل (هم خطا و هم حمله) با ۶ معماری مختلف شبکه عصبی عمیق بررسی شده‌است. این سیستم به صحت ۹۸٪ دست یافته‌است. هم‌چنین احمد و همکاران [9] یک سیستم تشخیص نفوذ برای محافظت از درگاه CAN وسایل نقلیه در برابر حملات انکارسرویس و Fuzzy ارائه کردند. معماری VGG استفاده شده و سیستم یادگیری عمیق ارائه شده به طور قابل توجهی نرخ مثبت کاذب را در مقایسه با تکنیک‌های یادگیری ماشین قدیمی کاهش می‌دهد. صحت کلی این سیستم به ۹۶٪ با نرخ مثبت کاذب ۰.۶٪ رسیده‌است.

برخی از محققان از یک شبکه عصبی کانولوشن (CNN[۸]) برای شناسایی حملات در اینترنت وسایل نقلیه استفاده کردند . نی و همکاران [10] یک سیستم تشخیص نفوذ مبتنی بر داده با چارچوب شبکه عصبی کانولوشن پیشنهاد دادند که رفتار واحدهای کنار جاده‌ای در اینترنت‌وسایل‌نقلیه را در برابر حملات مختلف تجزیه و تحلیل می‌کند. سیستم تشخیص نفوذ پیشنهادی، محدودیت منابع واحدهای داخلی (OBU[۹]) وسایل‌نقلیه را درنظر گرفته است و داده‌های شبکه را از واحدهای کنارجاده‌ای جمع آوری می‌کند. در نهایت، صحت معماری عمیق پیشنهادی در مقایسه با شبکه‌های عصبی کم عمق، به ۹۷.۶۰٪ رسیده است. زنگ و همکاران [11] یک چارچوب DeepVCM برای تشخیص ترافیک مخرب در واحدهای داخلی وسایل‌نقلیه پیشنهاد کردند که از شبکه عصبی کانولوشن و LSTM تشکیل‌شده است. عملکرد این مدل با دقت، فراخوانی و معیارF1 ارزیابی شده است، اما معیارصحت موردبررسی قرار نگرفته است.

اکثر سیستم‌های تشخیص نفوذ پیشنهادی از مدل منحصربه‌فردی استفاده کردند که عملکرد پایینی دارد درحالیکه یادگیری گروهی بااستفاده از مزایای این مدل های منحصربه فرد موجب بهبود عملکرد مدل نهایی می‌شود. در [12, 13] از یک تکنیک یادگیری گروهی انباشته[۱۰] برای شناسایی حملات در اینترنت‌وسایل‌نقلیه استفاده شده است. نتایج آن‌ها نشان می‌دهد که این تکنیک بسیار بهتر از هر یک از تکنیک‌های یادگیری ماشین فردی عمل می‌کند. همچنین نویسندگان در [14] از یادگیری گروهی توزیع شده برای بهبود تشخیص ناهنجاری‌ها در شبکه‌خودرویی استفاده کردند و توانستند به معیارF1 ۹۷٪ برسند.

اما تاکنون به تشخیص دقیق انواع حملات انکارسرویس توزیع‌شده مبتنی بر بازتاب در محیط اینترنت وسایل نقلیه پرداخته نشده است درحالیکه این حملات مخرب می توانند عامل مهم ایمنی را بخطر اندازند. بنابراین دراین مقاله یک سیستم تشخیص نفوذ گروهی مبتنی بر شبکه عصبی کانولوشن برای محافظت از اینترنت وسایل نقلیه پیشنهاد شده است. هایپرپارامترهای مدل‌های شبکه عصبی کانولوشن با رویکرد بیزی با استفاده از براوردگرهای Parzen باساختار درختی (BO-TPE[۱۱]) تنظیم شده‌اند تا مدل یادگیری بهینه را به دست آوریم. کارایی سیستم تشخیص نفوذ پیشنهادی با استفاده از مجموعه داده CICDDoS2019 [۶] ارزیابی می‌شود.

بطور خلاصه، این مقاله مشارکت های زیر را انجام می دهد:

۱) یک سیستم تشخیص نفوذ مبتنی بر یادگیری گروهی برای تشخیص انواع حملات انکارسرویس توزیع شده مبتنی بر بازتاب در اینترنت‌وسایل نقلیه پیشنهاد می‌شود. از رویکرد بیزی با استفاده از براوردگرهای Parzen باساختار درختی برای رسیدن به بهترین نرخ تشخیص استفاده می شود.

۲) سیستم تشخیص نفوذ پیشنهادی می‌تواند ۸ نوع مهم حمله انکارسرویس توزیع شده مبتنی بر بازتاب از جمله NTP[۱۲]، SSDP[۱۳]، LDAP[۱۴]، DNS[۱۵]، SNMP[۱۶]، MSSQL[۱۷]، NetBIOS[۱۸] و TFTP[۱۹] را به طور موثر تشخیص دهد.

۳) روش پیشنهادی بر روی مجموعه داده CICDDoS2019 ارزیابی می‌شود و عملکرد مدل پیشنهادی با مدل اخیر مقایسه می‌شود. اکثر

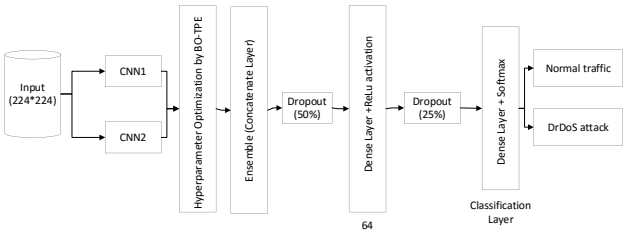
سیستم‌های تشخیص نفوذ پیشنهادی از مجموعه داده قدیمی برای ارزیابی مدل خود استفاده کردند که موجب ارزیابی نادرست می‌شود.

در ادامه، بخش دوم مدل پیشنهادی را تشریح می‌کند. بخش سوم، نتایج ارزیابی این مدل را ارائه و مورد بحث قرار می‌دهد. در نهایت، در بخش چهارم جمع بندی مقاله و نگاه کلی به کارهای اینده را خواهیم داشت.

۲- راهکارپیشنهادی

در این مقاله، یک سیستم تشخیص نفوذ مبتنی بر یادگیری گروهی برای شناسایی انواع مختلف حمله انکارسرویس توزیع شده مبتنی بر بازتاب در اینترنت‌وسایل‌نقلیه پیشنهاد شده است. چارچوب سیستم تشخیص نفوذ پیشنهادی ما از الحاق دو شبکه عصبی کانولوشن متفاوت تشکیل شده است که هشت نوع حمله انکارسرویس توزیع شده مبتنی بر بازتاب (NTP، SSDP، LDAP، DNS، SNMP، MSSQL، NetBIOS و TFTP) را شناسایی می‌کند. حملات انکارسرویس توزیع شده مبتنی بر بازتاب با استفاده از پروتکل‌های لایه انتقال، ازجمله TCP، UDP یا ترکیبی از هردو رخ می‌دهند. حملات MSSQL و SSDP از دسته حملات مبتنی بر TCP و حملات NTP و TFTP از دسته حملات مبتنی بر UDP هستند. همچنین حملاتی مانند DNS، LDAP، NETBIOS و SNMP می‌توانند با استفاده از TCP یا UDP انجام شوند.

شکل ۱ معماری این چارچوب را نشان می‌دهد. همانطور که شکل ۱ نشان می‌دهد، بسته‌ها در محیط اینترنت‌وسایل‌نقلیه به تصاویر تبدیل می‌شوند و پس از برچسب‌گذاری، توسط دو شبکه عصبی کانولوشن متفاوت آموزش داده می‌شوند. سپس این دو شبکه توسط روش BO-TPE، یک روش تنظیم خودکار هایپرپارامترها، بهینه می‌شوند. در نهایت مدل یادگیری گروهی با الحاق این دوشبکه بهینه، تشکیل می‌شود و بسته‌های مخرب در اینترنت‌وسایل‌نقلیه را شناسایی می‌کند.



شکل (۱) : چارچوب سیستم تشخیص نفوذ پیشنهادی مبتنی بر یادگیری گروهی

۲-۱- پیش‌پردازش داده‌ها

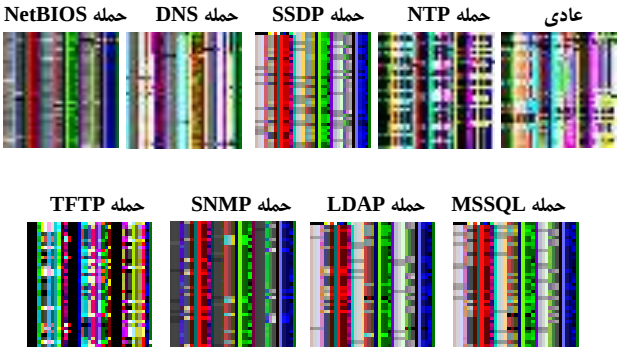
برای توسعه سیستم تشخیص نفوذ پیشنهادی برای اینترنت‌وسایل‌نقلیه، از مجموعه داده CICDDoS2019 [6] استفاده شده‌است که حملات انکارسرویس توزیع شده را به دودسته مبتنی بر بازتاب و مبتنی بر انقضا دسته‌بندی کرده است. این مجموعه داده توسط مؤسسه امنیت سایبری کانادا (CIC) و دانشگاه نیوبرانزویک (UNB) جمع‌اوری شده است و یکی از جدیدترین مجموعه داده‌های مربوط به نفوذ است. اما این مجموعه داده از مشکل کلاس نامتعادل رنج می برد که ممکن است بر عملکرد مدل‌ها تأثیر بگذارد [15]. علاوه بر این، بسیاری از بسته‌ها در مجموعه داده نامتعادل ممکن است به قدرت محاسباتی و زمان پردازش بالایی نیاز داشته باشند. بنابراین، ما به‌طور تصادفی تعداد مساوی از انواع حملات انکارسرویس توزیع‌شده مبتنی بربازتاب را از مجموعه داده CICDDoS 2019 انتخاب کردیم. از آنجایی که کمترین میزان ترافیک عادی برای یک حمله انکارسرویس توزیع شده، ۲۹۸۰۸ نمونه است، ما به همین اندازه از هر نوع حمله انکارسرویس توزیع شده مبتنی بربازتاب، انتخاب کردیم.

برای پیش پردازش بسته‌ها، از Dropna به منظور پاکسازی داده‌ها از مقادیر ازدست‌رفته، استفاده کردیم. سپس داده‌ها را به فرم‌های تصویر تبدیل کردیم زیرا مدل‌های شبکه عصبی کانولوشن عملکرد بهتری روی تصاویر دارند [16].

فرآیند تبدیل داده‌ها با نرمال سازی داده‌ها شروع می‌شود. از آنجایی که مقادیر پیکسل تصاویر از ۰ تا ۲۵۵ هست، داده‌های شبکه نیز باید به مقیاس ۰–۲۵۵ نرمال‌سازی شوند. در میان تکنیک‌های نرمال‌سازی، min-max و کمی[۲۰] دو موردی هستند که معمولا استفاده می‌شوند تا مقادیر داده را به همان محدوده تبدیل کنند. نرمال سازی min-max به خوبی با موارد پرت[۲۱] برخورد نمی‌کند و ممکن است باعث شود که اکثر نمونه داده‌ها مقادیر بسیار کمی داشته باشند، بنابراین از نرمال‌سازی کمی در مدل پیشنهادی خود استفاده کردیم. روش نرمال‌سازی کمی، توزیع ویژگی‌ها را به یک توزیع نرمال تبدیل می‌کند و دوباره مقادیر ویژگی‌ها بر اساس توزیع نرمال محاسبه می‌شود [17]. از این رو، اکثر مقادیر متغیر نزدیک به مقادیر میانه هستند،که در رسیدگی به موارد پرت موثر است.

پس از نرمال‌سازی داده‌ها، نمونه داده‌ها به تصاویری بر اساس برچسب زمانی و تعداد ویژگی‌های مجموعه داده تبدیل می شوند. هر تصویر یک تصویر مربع رنگی با سه کانال ابی، سبز و قرمز است. مجموعه داده CICDDoS2019 دارای ۸۰ ویژگی است، بنابراین هر بسته به تصویری به شکل ۳*۸۰*۸۰ تبدیل می‌شود. اگر تمام نمونه های یک تصویر، معمولی باشند ان تصویر به عنوان عادی برچسب‌گذاری می‌شود. ازطرف دیگر، اگر تصویر دارای نمونه حمله باشد به عنوان همان نوع حمله‌ای که بیشترین نمونه را دارد، برچسب‌گذاری می‌شود.

پس از تبدیل داده‌ها، تصاویر آماده آموزش توسط مدل‌های مبتنی بر شبکه عصبی کانولوشن هستند. نمونه‌های هر کلاس از حمله DrDoS در شکل ۲ نشان داده شده‌است. همانطور که شکل ۲ نشان می‌دهد نمونه‌های مخرب و نمونه‌های عادی دارای الگوهای ویژگی متفاوت هستند در حالی که انواع مختلف حمله انکارسرویس توزیع شده مبتنی بربازتاب دارای الگوهای ویژگی مشابه هستند.



شکل (۲) : نمونه تصاویر هر کلاس از حمله انکارسرویس توزیع‌شده مبتنی بر بازتاب

۲-۲- مدل‌های شبکه‌عصبی کانولوشن بهینه

شبکه عصبی کانولوشن زیرگروهی از شبکه‌های عصبی است که به دقت بالایی در دسته‌بندی تصاویر رسیده است [11]. شبکه عصبی کانولوشن به طور خودکار ویژگی‌های مهم را تشخیص می‌دهد و لایه‌های کانولوشنی آن بدون از دست دادن اطلاعات، ابعاد بالای تصاویر را کاهش می‌دهند. همچنین لایه‌های ادغام آن تعداد پارامترهای یادگیری را کاهش داده و از بیش‌برازش جلوگیری می‌کنند.

دو مدل مختلف شبکه عصبی کانولوشن با تعداد لایه‌های متفاوت برای یادگیری گروهی انتخاب شده‌اند. این دو مدل ساختار مشابهی دارند، با این تفاوت که مدل ۲ دارای لایه‌های کانولوشنی بیشتری است که در جدول ۱ توضیح داده شده است. داشتن چندین لایه کانولوشنی که در امتداد عمق دو مدل قرار گرفته‌اند، به مدل‌ها اجازه می‌دهد تا ویژگی‌های سطح بالا (نه فقط لبه‌ها و گوشه‌ها) را از تصاویر ورودی استخراج کنند. همچنین استفاده از دو لایه کانولوشنی متوالی در مدل۲، باعث می‌شود نمایش بهتری از تصویر، بدون از دست‌دادن سریع تمام اطلاعات مکانی داشته باشیم. جدول ۱ ساختار این دو مدل را توضیح می‌دهد. تعداد نورون‌ها در هر لایه در پرانتز نشان داده شده‌است.

جدول (۱) : چیدمان لایه‌ها در دو مدل پایه برای یادگیری گروهی

لایه ها	مدل۱	مدل۲
لایه ۱	Conv(16)	Conv(16)
لایه ۲	Maxpooling	Maxpooling
لایه ۳	Conv(256)	Conv(128)
لایه ۴	Maxpooling	Maxpooling
لایه ۵	Conv(512)	Conv(256)
لایه ۶	GlobalAveragePooling	Maxpooling
لایه ۷	Dense(512)	Conv(512)
لایه ۸	Dropout	Conv(512)
لایه ۹	Dense(9)	GlobalAveragePooling
لایه ۱۰	-	Dense(512)
لایه ۱۱	-	Dropout
لایه ۱۲	-	Dense(9)

در هر دو مدل ۱ و ۲، از فعال ساز واحدخطی‌اصلاح‌شده (ReLU) استفاده شده است زیرا به جلوگیری از رشد نمایی در محاسبات مورد نیاز برای راه‌اندازی شبکه عصبی کمک می‌کند [12]. همچنین استفاده از لایه ادغام میانگین جهانی[۲۳] بجای لایه مسطح[۲۳] به جلوگیری از بیش برازش مدل‌ها کمک می‌کند زیرا هیچ پارامتری برای بهینه سازی در لایه ادغام میانگین جهانی وجود ندارد. لایه مسطح به سادگی یک نقشه ویژگی چند بعدی را با چیدمان مجدد عناصر به یک بعدی تبدیل می‌کند. در حالی که لایه ادغام میانگین جهانی ازیک پنجره تجزیه کننده استفاده می‌کند که در سراسر نقشه ویژگی حرکت می‌کند و داده‌ها را با میانگین کردن آن جمع می‌کند.

همچنین از آنتروپی متقاطع طبقه‌ای[۲۴] به عنوان تابع ضرر برای محاسبه تفاوت بین توزیع‌های احتمال استفاده شده است. از آنجایی که ما بیش از دو کلاس داریم، تابع ضرر آنتروپی متقاطع طبقه‌ای بهترین انتخاب است. سپس از Adam به عنوان بهینه ساز برای کاهش تابع ضرر و ارائه دقیق ترین نتایج ممکن استفاده کردیم؛ زیرا این بهینه‌ساز بسیار سریع است.

مشابه سایر مدل‌های یادگیری عمیق، مدل‌های شبکه عصبی کانولوشن دارای تعدا زیادی هایپرپارامتر هستندکه نیاز به تنظیم دارند. این هایپرپارامترها را می توان به هایپرپارامترهای طراحی مدل و هایپرپارامترهای آموزش مدل دسته‌بندی کرد [18]. هایپرپارامترهای طراحی مدل، هایپرپارامترهایی هستند که باید در فرآیند طراحی مدل تنظیم شوند. در چارچوب دو مدل ارائه شده، هایپرپارامترهای طراحی مدل شامل نرخ یادگیری و نرخ ریزش[۲۵] هستند. ازسوی دیگر، هایپرپارامترهای آموزش مدل برای متعادل کردن سرعت اموزش و عملکرد مدل استفاده می شوند؛ که شامل اندازه دسته[۲۶] ، تعداد دوره‌ها[۲۷] و صبر توقف زودهنگام[۲۸] هستند. هایپرپارامترهای فوق تاثیر مستقیمی بر ساختار، اثربخشی و کارایی مدل‌های شبکه عصبی کانولوشن دارند.

بهینه سازی هایپرپارامترها (HPO)[۲۹] یک فرآیند خودکار تنظیم هایپرپارامترهای مدل های یادگیری عمیق با استفاده از تکنیک های بهینه‌سازی هست [18]. در میان تکنیک‌های بهینه‌سازی مورد استفاده برای مسائل بهینه‌سازی هایپرپارامترها، مدل بیزی می‌تواند بهترین هایپرپارامترها را در زمان کمتر (در تکرارهای کمتر) نسبت به جستجوی شبکه‌ای و جستجوی تصادفی پیدا کند؛ زیرا اساس مدل‌های بیزی، به روزرسانی دانش پیشین با استفاده از اطلاعات جدید، به منظور تولید دانش پسین است.

دراینجا ما از مدل بیزی با استفاده از الگوریتم برآوردگرهای Parzen با ساختار درختی (TPE) استفاده کردیم که به مقادیر اولیه یا مجموعه‌های آموزشی نیاز ندارد و قادر به یافتن هایپرپارامترهای بهتر است. روش TPE، نمونه پارامترهای جدید را جمع‌آوری می‌کند و توزیع قبلی را با نمونه پارامترهای داده شده در هر تکرار تعریف می‌کند، و سپس نمونه‌ای با بالاترین پیشرفت را برای تکرار بعدی انتخاب می‌کند [19]. در ابتدا، TPE فضای پارامتر را به طور تصادفی جستجو می‌کند. سپس، نمونه‌های جمع‌آوری‌شده به دو گروه تقسیم می‌شوند: گروه اول بهترین نمونه پارامترهایی هستند که توسط تابع هزینه ارزیابی می‌شوند، و گروه دوم، بخش باقی‌مانده است که برای مدل‌سازی احتمال استفاده می‌شوند. ایده اصلی این است که مجموعه‌ای از پارامترها را انتخاب می‌کند که احتمال بیشتری در گروه اول دارند. بهبود مورد انتظار (EI)[۳۰] در هر تکرار توسط رابطه زیر محاسبه می‌شود:

$$E(I) = \frac{l(x)}{g(x)} \qquad (۱)$$

که در آن l(x) و g(x) به ترتیب احتمال در گروه اول و دوم هستند. TPE به تست هر نمونه پارامتر نیاز ندارد و همچنین از تست پارامترهایی که احتمالاً عملکرد پایینی در مقایسه با سایر پارامترها دارند صرف‌نظر می‌کند، که منجر به کاهش پیچیدگی محاسباتی می‌شود.

جدول۲، محدوده جستجوی اولیه و مقادیر بهینه هایپرپارامترهای دو مدل شبکه عصبی کانولشن را بااستفاده از BO-TPE نشان می‌دهد. پس از بهینه‌سازی هایپرپارامترها، از این دو مدل بهینه به عنوان یادگیرندگان پایه برای ساخت مدل پیشنهادی مبتنی بر یادگیری گروهی استفاده می‌شود.

جدول (۲) : تنظیم هایپرپارامترهای دو مدل پایه

هایپرپارامتر	محدوده جستجو	مقدار بهینه برای مدل (۱)	مقدار بهینه برای مدل (۲)
تعداد دوره	[۵ , ۱۰۰]	۶۰	۷۰
اندازه دسته	[۳۲ , ۱۲۸]	۱۲۸	۱۲۸
نرخ یادگیری	(۰.۰۰۱ , ۰.۱)	۰.۰۰۴	۰.۰۰۲
نرخ ریزش	(۰.۲ , ۰.۸)	۰.۵	۰.۴
صبر توقف زودهنگام	[۲ , ۱۰]	۵	۴

۲-۳- مدل پیشنهادی مبتنی بر یادگیری گروهی

یادگیری گروهی تکنیکی است که چند مدل یادگیری پایه را برای ساخت یک مدل گروهی با عملکرد بهبود یافته ادغام می‌کند. یادگیری گروهی به طور گسترده‌ای در مشکلات تجزیه و تحلیل داده‌ها مورد استفاده قرار می‌گیرد زیرا مجموعه‌ای از چند یادگیرنده بهتر از یادگیرنده‌های مجرد عمل می‌کنند [13]. الحاق [20] یکی از استراتژی‌های گروهی برای مدل‌های یادگیری عمیق است که می‌تواند بالاترین ویژگی‌ها را برای ساختن یک مدل جامع و جدید ترکیب کند.

مدل پیشنهادی ما به کمک روش الحاق و با استفاده از آخرین لایه متراکم (Dense) دو شبکه عصبی کانولوشن بهینه ساخته شده است. هدف یک شبکه عصبی کانولوشن الحاق شده، استخراج بالاترین ویژگی های ایجادشده از لایه متراکم بالای مدل‌های شبکه عصبی کانولوشن پایه است و از عملیات الحاق برای ادغام همه ویژگی‌ها در یک لایه الحاق جدید استفاده می‌کند. پس از لایه الحاق، بااستفاده از لایه‌های حذفی، متراکم و softmax، مدل جدید مبتنی بر یادگیری گروهی ساخته می‌شود. استفاده از لایه‌های حذفی با کاهش ویژگی‌های اضافی به جلوگیری از بیش برازش مدل پیشنهادی ما کمک می‌کنند. در نهایت، لایه متراکم به همراه softmax، لایه دسته‌بندی مدل پیشنهادی را به منظور برگرداندن احتمال‌های هر کلاس تشکیل می‌دهند.

از انجایی که مدل ۲ ما لایه‌های کانولوشنی بیشتری نسبت به مدل ۱ دارد، باعث می‌شود ویژگی های سطح پایین بیشتری را یاد بگیرد و در دسته‌بندی چندگانه به نتایج بهتری دست یابد، اما زمان تشخیص حملات را افزایش می‌دهد. بنابراین با الحاق این دو مدل، مصالحه ای بین زمان تشخیص و نرخ تشخیص ایجاد کردیم و عملکرد مدل نهایی را بهبود بخشیدیم.

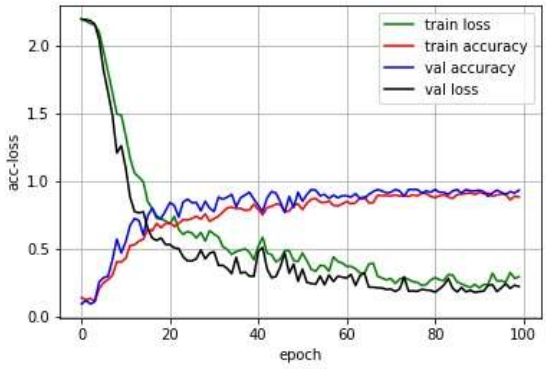
پیچیدگی محاسباتی روش الحاق O(NF) است که N تعدا نمونه داده‌ها، و F تعداد کل ویژگی‌های استخراج شده از لایه‌های متراکم مدل‌های پایه است.

۳- ارزیابی مدل پیشنهادی

مدل پیشنهادی بر روی مجموعه داده CICIDDoS2019 ارزیابی شده‌است. این مجموعه داده، جدید و مربوط به سال ۲۰۱۹ است. بنابراین برخلاف سایر مقالات که از مجموعه داده‌های قدیمی (ازجمله NSL-KDD ، KDD99 و UNSW-NB15) استفاده کردند [11, 21]؛ ارزیابی صحیح تری از مدل پیشنهادی خود خواهیم داشت.

ما از ۸۰ درصد داده‌ها برای آموزش و ۲۰ درصد ان برای تست استفاده کردیم. همچنین از اعتبار سنجی متقابل پنج برابری[۳۱] برای جلوگیری از بیش برازش در طول فرایند اموزش مدل پیشنهادی استفاده شده است. در روش اعتبارسنجی متقابل پنج برابری ، مجموعه داده اموزشی به طورتصادفی به ۵ زیرنمونه با حجم یکسان تبدیل می‌شود که ۴ زیرنمونه به عنوان مجموعه داده اموزشی و یک زیرنمونه به عنوان مجموعه داده اعتبارسنجی درنظر گرفته می‌شود.

به منظور ارزیابی دقیق و کامل سیستم تشخیص نفوذ پیشنهادی، تمامی معیارهای مهم ازجمله ۱)صحت، ۲)دقت، ۳)فراخوانی ، ۴)معیار F ۵)نرخ مثبت کاذب[۳۲]، ۶)نرخ منفی کاذب[۳۳] و ۷)نرخ مثبت واقعی[۳۴] مورد استفاده قرار گرفتند. علاوه بر این، برای ارزیابی کارآمد مدل پیشنهادی، زمان تست هر بسته نیز در نظر گرفته شده تا حملات مخرب در زمان کمتری شناسایی شود.



شکل (۳) : نمودارهای صحت و ضرر به دوره در مدل پیشنهادی

همانطور که در جدول۳ مشاهده می‌کنید مدل پیشنهادی می تواند ۸ نوع مهم حمله انکارسرویس توزیع شده مبتنی بر بازتاب (NTP، SSDP، LDAP، DNS، SNMP، MSSQL، NetBIOS و TFTP) را با دقت بالایی تشخیص دهد.

ما آزمایش‌های خود را با استفاده از کتابخانه‌های Scikit-learn و Keras در پایتون انجام دادیم. و ازانجایی که روش الحاق موجب افزایش زمان اموزش مدل می‌شود، از Google colab برای آموزش سریع‌تر مدل پیشنهادی خود استفاده کردیم؛ زیرا دارای GPU قدرتمند (Tesla K80) و پردازنده Intel Xeon با دو هسته ۲.۲۰ گیگاهرتز است. در آزمایش‌های ما، تعداد دوره‌ها برابر با ۱۰۰ درنظرگرفته شده است تا روند اموزش مدل پیشنهادی کامل شود؛ سپس بااستفاده از توقف زودهنگام، پس از بهبود عملکرد مدل در مجموعه داده اعتبارسنجی، آموزش مدل متوقف می‌شود تا از بیش‌برازش جلوگیری شود. همچنین اندازه دسته برابر ۱۲۸ موجب افزایش سرعت آموزش می‌شود؛ زیرا دسته‌های بزرگتر مراحل جستجوی کمتری را برای حل بهینه انجام می‌دهند.

همانطور که در شکل ۳ نشان داده شده است مدل پیشنهادی دارای صحت ۹۹.۸٪ است؛ نمودارهای قرمز و ابی به ترتیب صحت اموزش و اعتبارسنجی و نمودارهای سبز و مشکی به ترتیب تابع ضرر اموزش و اعتبارسنجی را نشان می‌دهند. فاصله بین نمودارهای صحت اموزش و اعتبارسنجی در دوره‌های پایانی، بیش برازش را نشان می‌دهد؛ اگر فاصله

بیشتر باشد، بیش‌برازش بیشتر است. اما همانطور که شکل ۳ نشان می‌دهد، ما کمترین بیش‌برازش را داریم.

جدول (۳) : ارزیابی کارایی مدل پیشنهادی

کلاس	دقت	فراخوانی	معیارF	میانگین صحت	زمان تست هر بسته (ثانیه)
عادی	۱.۰۰	۱.۰۰	۱.۰۰	۰.۹۹۸۱۹	۰.۰۶۴
حمله NTP	۱.۰۰	۱.۰۰	۱.۰۰		
حمله SSDP	۰.۹۷۶۷۴	۱.۰۰	۰.۹۸۸۲۴		
حمله DNS	۱.۰۰	۱.۰۰	۱.۰۰		
حمله NetBIOS	۱.۰۰	۱.۰۰	۱.۰۰		
حمله MSSQL	۱.۰۰	۰.۹۰۹۰۹	۰.۹۵۲۳۸		
حمله LDAP	۰.۹۶۲۹۶	۱.۰۰	۰.۹۸۱۱۳		
حمله SNMP	۱.۰۰	۱.۰۰	۱.۰۰		
حمله TFTP	۱.۰۰	۱.۰۰	۱.۰۰		

اکثر مقالاتی که به تشخیص حملات در اینترنت وسایل نقلیه پرداختند، حملات مخرب انکار سرویس توزیع شده را درنظر نگرفتند [8,13,21-24]. هم‌چنین مقاله [9] از مجموعه داده CAN-intrusion استفاده می‌کند که می‌تواند صرفا حملات انکارسرویس در گذرگاه CAN وسایل نقلیه را تشخیص دهد، درحالیکه که تشخیص حملات جدی انکارسرویس توزیع شده نیاز به دید وسیع تری از شبکه خودرویی و مجموعه‌داده جامع‌تری دارد.

خویی و همکاران [15] به تشخیص حملات انکار سرویس توزیع شده مبتنی بر بازتاب در شبکه هوشمند پرداختند و با استفاده از یادگیری گروهی مبتنی بر پشته (stacking) به صحت ۹۳.۴٪ دست یافتند. همانطور که جدول ۴ نشان می دهد مدل پیشنهادی ما توانسته انواع حملات انکار سرویس توزیع شده مبتنی بر بازتاب را با میانگین صحت ۹۹.۸٪ تشخیص دهد. نتایج مدل پیشنهادی ما نشان می‌دهد که مدل‌های یادگیری گروهی مبتنی بر الحاق از سایر مدل‌های یادگیری گروهی بهتر عمل می‌کنند. ازطرفی دیگر، مدل [۱۵] زمان تشخیص را برای تشخیص بلادرنگ حملات مخرب انکارسرویس در نظر نگرفته است.

جدول (٤) : مقایسه مدل پیشنهادی با سیستم تشخیص نفوذ موجود

روش	صحت	نرخ منفی کاذب	نرخ مثبت کاذب	نرخ مثبت واقعی
مدل پیشنهادی ما	۰.۹۹۸	۰.۰۱۰	۰.۰۰۱	۰.۹۸
[۱۵]	۰.۹۳۴	۰.۰۴۱	۰.۰۸۹	۰.۹۶

نویسندگان در [25] با کمک ماشین قوی Raspberry Pi3 به زمان تست ۱.۸ میلی‌ثانیه و [8] با کمک پردازنده قوی Nvidia Jetson Nano به زمان تست ۰.۲۹۹میلی ثانیه رسیدند؛ ما با توجه به محدودیت‌های Google Colab توانستیم در زمان نسبتا کمی بسته‌های مخرب را شناسایی کنیم. همچنین در محیط اینترنت‌وسایل‌نقلیه، امکان استفاده از پردازنده‌های قوی و گران قیمت در تمام وسایل‌نقلیه و زیرساخت‌های کنارجاده‌ای برای تشخیص بسته‌های مخرب وجود ندارد. بنابراین زمان تست بسته‌ها باید باتوجه به محدودیت منابع وسایل نقلیه درنظر گرفته شود.

٤- نتیجه‌گیری

درحال حاضربسیاری از نویسندگان برروی محیط اینترنت‌وسایل‌نقلیه به دلیل نقش مهم ان درارائه کاربردهای حمل و نقل هوشمند ازجمله مدیریت ترافیک و ایمنی راننده تمرکزکردند. اما حملات مختلفی ممکن است در اینترنت‌وسایل‌نقلیه رخ دهد و موجب نارضایتی کاربران و ناکارامدی شبکه شود که از مهم‌ترین ان‌ها می توان به حمله انکارسرویس توزیع شده اشاره کرد که دردسترس بودن شبکه را به خطر می‌اندازد.

در دسترس نبودن خدمات اینترنت‌وسایل‌نقلیه، برنامه‌های کاربردی مبتنی بر ایمنی را مختل می‌کند و می تواند جان انسان‌ها را به خطر بیندازد. ازطرفی حملات انکارسرویس توزیع شده مبتنی بر بازتاب نوع شدیدتر حمله انکارسرویس توزیع شده محسوب می‌شوند و تشخیص ان به دلیل هویت پنهان مهاجم دشوارتر است. تاکنون کارهای تحقیقاتی موجود به تشخیص دقیق انواع این حملات در محیط اینترنت وسایل نقلیه نپرداختند.

بنابراین، یک راه‌حل مبتنی بر یادگیری گروهی برای شناسایی انواع مختلف حمله انکارسرویس توزیع شده مبتنی بر بازتاب در محیط اینترنت‌وسایل‌نقلیه پیشنهاد شده است. سیستم تشخیص نفوذ پیشنهادی می‌تواند ۸ نوع مهم این حمله را به طور موثر تشخیص دهد. طبق مدل پیشنهادی، بسته‌ها در محیط اینترنت‌وسایل‌نقلیه به تصاویر تبدیل می‌شوند و پس از برچسب‌گذاری، توسط دو شبکه عصبی کانولوشن متفاوت آموزش داده می‌شوند. سپس این دو شبکه توسط روش BO-TPE، یک روش تنظیم خودکار هایپرپارامترها، بهینه می‌شوند. در نهایت مدل یادگیری گروهی با الحاق این دوشبکه بهینه، تشکیل می‌شود و بسته‌های مخرب در اینترنت‌وسایل‌نقلیه را شناسایی می‌کند. عملکرد مدل پیشنهادی با مجموعه داده جدید CICIDDoS2019 ارزیابی شده است. همچنین همه معیارهای ارزیابی برای ارزیابی کامل و دقیق مدل پیشنهادی مورد استفاده قرار گرفتند. نتایج، کارایی بالای سیستم تشخیص نفوذ پیشنهادی را نشان می‌دهد.

در نتیجه، با شناسایی به موقع و دقیق حملات انکارسرویس توزیع شده مبتنی بر بازتاب، می توانیم از شبکه اینترنت وسایل نقلیه محافظت کنیم تا محیط امن‌تر و مطمئن‌تری برای کاربران فراهم شده و از همه مهم‌تر جان کاربران نجات یابد. درکارهای اینده سعی داریم چارچوب خودرا برای تشخیص حملات انکارسرویس توزیع شده مبتنی بر انقضا گسترش دهیم.

مراجع

[1] Ang, L.-M., et al., *Deployment of IoV for smart cities: Applications, architecture, and challenges*. IEEE access, 2018. 7: p. 6473-6492.

[2] Sharma, S. and B. Kaushik, *A survey on internet of vehicles: Applications, security issues & solutions*. Vehicular Communications, 2019. 20: p. 100182.

[3] Sharma, S. and A. Kaul, *A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud*. Vehicular communications, 2018. 12: p. 138-164.

[4] Gao, Y., et al., *A distributed network intrusion detection system for distributed denial of service attacks in vehicular ad hoc network*. IEEE Access, 2019. 7: p. 154560-154571.

[5] Adhikary, K., et al., *Evaluating the performance of various machine learning algorithms for detecting DDOS attacks in vanets*. International Journal of Control Automation, 2019. 12(5): p. 478-486.
[6] Sharafaldin, I., et al. *Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy*. in 2019 International Carnahan Conference on Security Technology (ICCST). 2019. IEEE.
[7] Zhang, J., et al., *Intrusion detection system using deep learning for in-vehicle security*. Ad Hoc Networks, 2019. 95: p. 101974.
[8] Alladi, T., et al., *DeepADV: A Deep Neural Network Framework for Anomaly Detection in VANETs*. IEEE Transactions on Vehicular Technology, 2021. 70(11): p. 12013-12023.
[9] Ahmed, I., A. Ahmad, and G. Jeon, *Deep Learning-based Intrusion Detection System for Internet of Vehicles*. IEEE Consumer Electronics Magazine, 2021.
[10] Nie, L., et al., *Data-driven intrusion detection for intelligent Internet of vehicles: A deep convolutional neural network-based method*. IEEE Transactions on Network Science and Engineering, 2020. 7(4): p. 2219-2230.
[11] Zeng, Y., et al. *Deepvcm: a deep learning based intrusion detection method in vanet*. in 2019 IEEE 5th intl conference on big data security on cloud (BigDataSecurity), IEEE intl conference on high performance and smart computing,(HPSC) and IEEE intl conference on intelligent data and security (IDS). 2019. IEEE.
[12] Yang, L., et al. *Tree-based intelligent intrusion detection system in internet of vehicles*. in 2019 IEEE global communications conference (GLOBECOM). 2019. IEEE.
[13] Yang, L., A. Moubayed, and A. Shami, *MTH-IDS: a multitiered hybrid intrusion detection system for Internet of vehicles*. IEEE Internet of Things Journal, 2021. 9(1): p. 616-632.
[14] A. Ghaleb, F., et al., *Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET*. Electronics, 2020. 9(9): p. 1411.
[15] Khoei, T.T., et al. *Ensemble learning methods for anomaly intrusion detection system in smart grid*. in 2021 IEEE International Conference on Electro Information Technology (EIT). 2021. IEEE.
[16] Hussain, F., et al. *IoT DoS and DDoS attack detection using ResNet*. in 2020 IEEE 23rd International Multitopic Conference (INMIC). 2020. IEEE.
[17] Lokman, S.-F., et al. *The Impact of Different Feature Scaling Methods on Intrusion Detection for in-Vehicle Controller Area Network (CAN)*. in International Conference on Advances in Cyber Security. 2020. Springer.
[18] Yang, L. and A. Shami, *On hyperparameter optimization of machine learning algorithms: Theory and practice. Neurocomputing*, 2020. 415: p. 295-316.
[19] Jiang, B., et al., *Attention-LSTM architecture combined with Bayesian hyperparameter optimization for indoor temperature prediction*. Building and Environment, 2022. 224: p. 109536.
[20] Rahimzadeh, M. and A. Attar, *A modified deep convolutional neural network for detecting COVID-19 and pneumonia from chest X-ray images based on the concatenation of Xception and ResNet50V2*. Informatics in medicine unlocked, 2020. 19: p. 100360.
[21] Shu, J., et al., *Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach*. IEEE Transactions on Intelligent Transportation Systems, 2020. 22(7): p. 4519-4530.
[22] Zhou, M., et al., *Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant*. Computer Networks, 2020. 172: p. 107174.
[23] Sunny, J., S. Sankaran, and V. Saraswat. *A hybrid approach for fast anomaly detection in controller area networks*. in 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). 2020. IEEE.
[24] Gonçalves, F., J. Macedo, and A. Santos. *Intelligent Hierarchical Intrusion Detection System for VANETs*. in 2021 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2021. IEEE.
[25] Yang, L. and A. Shami, *A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles*. arXiv preprint arXiv:2201.11812, 2022.

پانویس ها

[1] Internet of Vehicles
[2] Denial of Service
[3] Distributed Denial of Service
[4] Roadside Unite
[5] Distributed Reflection-based Denial of Service
[6] Intrusion Detection System
[7] Deep Neural Network
[8] Convolutional Neural Network
[9] On-Board Unite
[10] Stacked
[11] Bayesian Optimization-Tree Parzen Estimator
[12] Network Time Protocol
[13] Simple Service Discovery Protocol
[14] Lightweight Directory Access Protocol
[15] Domain Name System
[16] Simple Network Management Protocol
[17] Microsoft Structured Query Language
[18] Network Basic Input/Output System
[19] Trivial File Transfer Protocol
[20] Quantile
[21] Outliers
[22] GlobalAveragePooling
[23] Flatten
[24] Categorical cross entropy
[25] Dropout rate
[26] Batchsize
[27] Epochs
[28] Early stopping patience
[29] Hyper Parameter Optimization
[30] Expected Improvement
[31] Five-fold cross validation
[32] False positive rate
[33] False negative rate
[34] True positive rate