13th سیزدهمین کنفرانس بین المللی فناوری اطلاعات و دانش
۲۹ آذر ماه الی ۱ دی ماه ۱۴۰۱
International Conference on Information & Knowledge Technology
"ایران هوشمند در پرتو فناوری اطلاعات و دانش"

سیستم تشخیص نفوذ مبتنی برشبکه عصبی کانولوشن برای تشخیص حمله انکارسرویس در اینترنت‌وسایل‌نقلیه

زهراجانفدا[۱]، سیدامین حسینی سنو[۲]
[۱]دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر، zahra.janfada@mail.um.ac.ir
[۲] دانشگاه فردوسی مشهد، دانشکده مهندسی، گروه مهندسی کامپیوتر، hosseini@um.ac.ir

چکیده – اینترنت‌وسایل‌نقلیه (*IoV*) مفهومی نوظهور در سیستم‌های حمل‌ونقل‌هوشمند (*ITS*) است که هدف بهبود ایمنی عابران‌پیاده و رانندگان و نظارت بر ترافیک را دنبال می‌کند؛ اما ارتباطات اینترنت‌وسایل‌نقلیه در برابر حملات مختلف آسیب پذیر هستند. بنابراین امنیت در اینترنت‌وسایل‌نقلیه یک مسئله جدی است زیرا مستقیماً بر زندگی کاربران ان تأثیر می‌گذارد. یکی از مهم ترین حملات در این محیط، حمله انکارسرویس (*DoS*) است که از دسترسی به سرویس‌های اینترنت‌وسایل‌نقلیه جلوگیری می‌کند و از همه مهم‌تر باعث ترافیک و تصادفات جاده‌ای می‌شود و ایمنی کاربران را به خطر می‌اندازد. بنابراین، یک راه حل مبتنی بر یادگیری عمیق برای شناسایی حملات انکارسرویس در محیط اینترنت‌وسایل‌نقلیه پیشنهاد شده است. مدل پیشنهادی از شبکه عصبی کانولوشن ۱۰لایه تشکیل شده‌است که می‌تواند انواع مختلف حملات انکارسرویس را بطور موثر تشخیص دهد. عملکرد مدل پیشنهادی با مجموعه داده واقعی و جدید *VDoS-LRS* ارزیابی شده است. نتایج تجربی نشان می دهد که سیستم تشخیص نفوذ پیشنهادی به نرخ صحت ۱۰۰٪ رسیده است.

کلید واژه- اینترنت وسایل‌نقلیه، حمله انکارسرویس، سیستم تشخیص نفوذ، شبکه عصبی کانولوشن.

۱- مقدمه

هر روز بر تعداد وسایل‌نقلیه در جاده‌ها افزوده می‌شود، بنابراین نیاز به سیستم‌های حمل‌ونقل‌هوشمند (ITS) مدام درحال افزایش است. افزایش تعداد وسایل نقلیه در جاده‌ها می‌تواند منجر به افزایش تصادفات و ترافیک طولانی مدت شود [1]. برای حل این مشکلات به یک سیستم مدیریتی خوب نیاز است. یکی از راه حل‌های ارائه‌شده توسط محققان، اینترنت وسایل نقلیه (IoV) است که در مقایسه با شبکه‌های اقتضایی خودرو (VANET) از مقیاس پذیری بالاتری برخوردار هست و شبکه عظیمی از خدمات را برای شهرهای بزرگ فراهم می‌کند. بنابراین اینترنت‌وسایل‌نقلیه یکی از فعال‌ترین زمینه‌های تحقیقاتی در سیستم‌های حمل‌ونقل‌هوشمند محسوب می‌شود که ترکیبی از شبکه‌های اقتضایی خودرو و اینترنت‌اشیاء (IoT) است [2].

امنیت یکی از مهم ترین چالش‌ها برای پیاده سازی اینترنت‌وسایل‌نقلیه است؛ زیرا پیام‌های حیاتی در این محیط به صورت بلادرنگ به اشتراک گذاشته می‌شوند. تحویل بلادرنگ این پیام‌ها می‌تواند بر زندگی کاربران تأثیر بگذارد. بنابراین، قبل از استقرار اینترنت‌وسایل‌نقلیه برای استفاده عمومی، الزامات امنیتی مانند احراز هویت، دردسترس‌بودن، یکپارچگی و محرمانگی (AAIC) باید رعایت شود [3]. الزام دردسترس‌بودن بسیار مهم است زیرا پیام‌های بلادرنگ در اینترنت‌وسایل‌نقلیه رد و بدل می‌شوند. اگر دردسترس‌بودن پیام‌ها به خطر بیفتد، می‌تواند منجر به یک وضعیت

بسیار بحرانی مانند از دست دادن جان کاربران شود.

حمله انکارسرویس (DoS) یک حمله جدی است که می‌تواند شبکه خودرویی را از بین ببرد. درواقع، هدف اصلی هر نوع حمله انکارسرویس این است که خدمات شبکه برای کاربران مورد نظر در دسترس نباشد [4]. حملات انکارسرویس می‌توانند موجب هرج‌ومرج و نارضایتی کاربران شوند و جان انسان‌ها را به خطر بیندازند. هم‌چنین وقوع حملات انکارسرویس در یک بازه زمانی کوتاه، شناسایی آن‌ها را پیچیده‌تر می‌کند [5]. بنابراین یافتن راه‌حلی دقیق برای شناسایی انواع حملات انکارسرویس یکی از اقدامات لازم برای نجات جان کاربران، ارتقای سطح امنیت اینترنت‌وسایل‌نقلیه، حفظ کیفیت خدمات و جلب رضایت کاربران است [6].

رویکرد یادگیری عمیق برای شناسایی حملات در اینترنت‌وسایل‌نقلیه یکی از داغ‌ترین موضوعات در این زمینه محسوب می‌شود که نتایج بسیار خوبی به دست آورده است [7]. در این مقاله، ما یک مدل یادگیری عمیق برای تشخیص حمله انکارسرویس در اینترنت‌وسایل‌نقلیه با استفاده از مجموعه داده جدید VDoS-LRS [8] ارائه می‌کنیم. همچنین انواع مختلف حملات انکارسرویس را ارزیابی می‌کنیم و زمان تشخیص را برای داشتن یک مدل بلادرنگ در نظر می‌گیریم.

این مقاله دارای نواوری های زیر است:

۱) یک سیستم تشخیص نفوذ مبتنی بر شبکه عصبی کانولوشن (CNN) برای تشخیص حمله انکارسرویس در اینترنت‌وسایل‌نقلیه پیشنهاد می‌شود. سیستم تشخیص نفوذ پیشنهادی می‌تواند انواع مختلف حملات انکارسرویس از جمله سیلاب UDP، سیلاب SYN و Slowloris را شناسایی کند.

۲) دو مدل مختلف شبکه عصبی کانولوشن برای تشخیص حمله انکار سرویس در اینترنت‌وسایل‌نقلیه مقایسه می‌شود تا با انتخاب تعداد مناسب لایه‌ها به بهترین نرخ تشخیص و زمان تشخیص بلادرنگ برسیم.

۳) روش پیشنهادی بر روی مجموعه داده واقعی و جدید VDoS-LRS ،که داده‌های شبکه واقعی را در سه محیط بزرگراه، شهری و روستایی نشان می‌دهد، ارزیابی می‌شود. برخی از سیستم‌های تشخیص نفوذ ارائه شده از مجموعه داده‌های غیرخودرویی یا بسیار قدیمی استفاده می‌کنند که باعث ارزیابی نادرست می‌شود.

ادامه مقاله به شرح زیر سازماندهی شده است. بخش دوم کارهای مرتبط با تشخیص نفوذ مبتنی بر یادگیری عمیق در شبکه خودرویی را بررسی می‌کند. بخش سوم چارچوب پیشنهادی، از جمله شبکه عصبی کانولوشن را تشریح می‌کند. بخش چهارم نتایج ازمایش‌ها را ارائه می‌دهد و عملکرد مدل را ارزیابی می‌کند. در نهایت، در بخش پنجم خلاصه مقاله و نگاهی به کارهای آینده را خواهیم داشت.

۲- پیشینه

یادگیری عمیق از بهترین رویکردها برای محافظت از اینترنت‌وسایل‌نقلیه است، زیرا دقت بالایی در تشخیص حملات شناخته شده دارد [9]. اشرف و همکاران [10] یک سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق برای سیستم‌های حمل‌ونقل هوشمند پیشنهاد دادند که به صحت کلی ۹۹٪ و ۹۸٪ به‌ترتیب برای مجموعه داده‌های car hacking و UNSWNB-15، رسیده‌است. اله و همکاران [11] یک مدل یادگیری عمیق ترکیبی به منظور بهبود صحت تشخیص حمله سایبری در اینترنت‌وسایل‌نقلیه پیشنهاد دادند. همچنین علادی و همکاران [12] یک سیستم تشخیص نفوذ مبتنی بر شبکه عصبی عمیق (DNN) برای شبکه‌های خودرویی پیشنهاد دادند. این سیستم تشخیص نفوذ پیشنهادی با اسقرار در واحدهای کنارجاده‌ای (RSUs) و دریافت تمام داده های همه پخشی وسایل نقلیه و دسته‌بندی آن‌ها به ترافیک مخرب و عادی، تشخیص ناهنجاری را انجام می دهد. این سیستم به صحت بالای ۹۸٪ دست یافته‌است.

برخی از محققان از شبکه عصبی کانولوشن برای شناسایی حملات در اینترنت وسایل نقلیه استفاده کردند. نی و همکاران [13] یک سیستم تشخیص نفوذ مبتنی بر داده با چارچوب شبکه عصبی کانولوشن ارائه دادند که رفتارهای واحدکنارجاده‌ای در اینترنت‌وسایل‌نقلیه را در برابر حملات مختلف تجزیه و تحلیل می‌کند. سیستم تشخیص نفوذ پیشنهادی، محدودیت منابع واحدهای داخلی (OBU) وسایل‌نقلیه را درنظر گرفته است و داده های شبکه را از واحدهای کنارجاده‌ای جمع آوری می‌کند. در نهایت، صحت معماری عمیق پیشنهادی در مقایسه با شبکه‌های عصبی کم عمق، SVM و PCA به ۹۷.۶۰٪ رسیده است. همچنین احمد و همکاران [7] یک سیستم تشخیص نفوذ برای محافظت از درگاه CAN وسایل نقلیه در برابر حملات DoS و Fuzzy ارائه کردند. معماری VGG استفاده شده و سیستم یادگیری عمیق ارائه شده به طور قابل توجهی نرخ مثبت کاذب (FPR) را در مقایسه با تکنیک‌های یادگیری ماشین قدیمی کاهش می‌دهد. صحت کلی این سیستم به ۹۶٪ با نرخ مثبت کاذب ۰.۶٪ رسیده است. زنگ و همکاران [14] یک چارچوب DeepVCM برای تشخیص ترافیک مخرب در واحدهای داخلی وسایل‌نقلیه پیشنهاد دادند که از شبکه عصبی کانولوشن و LSTM تشکیل‌شده است. عملکرد این مدل با

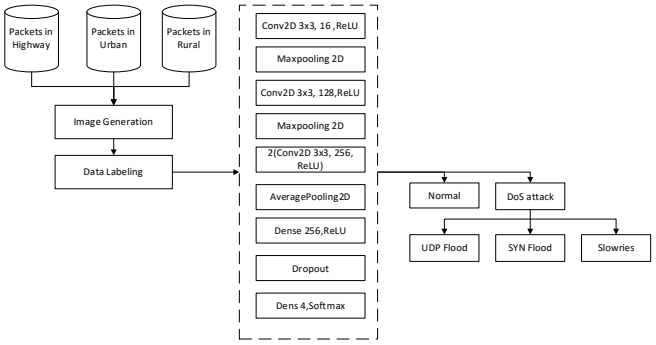
دقت، فراخوانی و معیار F1 ارزیابی شده است، اما معیارصحت موردبررسی قرار نگرفته است.

اگرچه سیستم‌های تشخیص نفوذ پیشنهادی در اینترنت‌وسایل‌نقلیه دقت بالایی دارند، اما هنوز جای زیادی برای بهبود عملکرد وجود دارد. هم‌چنین، شناسایی موثر انواع مختلف حمله انکارسرویس از نیازهای اساسی اینترنت وسایل نقلیه محسوب می شود تا از اثرات مخرب این حمله جلوگیری شود درحالی‌که اکثر سیستم‌های تشخیص نفوذ پیشنهادی به ان توجه نکردند. به منظور ارائه یک سیستم تشخیص نفوذ موثر وکارا، در نظر گرفتن تمام معیارهای ارزیابی و استفاده از مجموعه داده واقعی، ضروری هست. بنابراین، مدل پیشنهادی به تشخیص دقیق انواع حمله انکارسرویس در اینترنت وسایل نقلیه با استفاده از مجموعه داده VDoS-LRS می پردازد.

۳- راهکار پیشنهادی

هدف این مقاله، توسعه یک سیستم تشخیص نفوذ است که بتواند انواع مختلف حملات انکارسرویس از جمله سیلاب SYN، سیلاب UDP و Slowloris را در سه محیط بزرگراه، شهری و روستایی شبکه اینترنت‌وسایل‌نقلیه شناسایی کند. حمله سیلاب SYN با ارسال درخواست‌های زیاد SYN به وسیله‌نقلیه قربانی، از فرآیند دست دادن سه‌گانه TCP سوءاستفاده می‌کند؛ تا منابع وسیله‌نقلیه را تمام کند و آن را برای ارتباط با سایر گره‌ها غیرقابل دسترس کند. حمله سیلاب UDP تعداد زیادی بسته UDP را به پورت‌های یک سرور می‌فرستد و می‌تواند با پاسخ دادن به بسته‌های ارسالی، سرور را مشغول نگه دارد. بنابراین، برای تعداد زیادی از بسته‌های UDP، وسیله‌نقلیه قربانی مجبور به ارسال بسته‌های ICMP زیادی می‌شود و در نهایت برای سایر کاربران از دسترس خارج می‌شود [15]. Slowloris یک حمله انکارسرویس لایه کاربرد است که در آن تعداد زیادی درخواست HTTP به سرور ارسال می‌شود؛ داده ها به آرامی و به صورت دوره ای به سرور ارسال می شود، بنابراین سرور را مشغول می‌کند و از کار می‌اندازد.

در این مقاله، یک سیستم تشخیص مبتنی بر شبکه عصبی کانولوشن برای شناسایی انواع مختلف حملات انکارسرویس در اینترنت‌وسایل‌نقلیه پیشنهاد شده است. چارچوب سیستم تشخیص پیشنهادی ما شامل یک شبکه عصبی کانولوشن ۱۰ لایه است که سه نوع حمله انکارسرویس را شناسایی می‌کند: سیلاب UDP، سیلاب SYN و Slowloris. این چارچوب هم دسته‌بند باینری و هم دسته‌بند چندگانه است. دسته‌بند باینری برای دسته‌بندی بسته‌ها به عادی و مخرب و دسته‌بند چندگانه برای دسته‌بندی انواع مختلف حملات انکارسرویس (سیلاب SYN، سیلاب UDP و Slowloris) استفاده می‌شود. شکل ۱ معماری این چارچوب را نشان می‌دهد. همانطور که شکل ۱ نشان می‌دهد، بسته ها در سه محیط اینترنت‌وسایل‌نقلیه به تصاویر تبدیل می‌شوند و پس از برچسب‌گذاری، توسط مدل پیشنهادی ما مبتنی بر شبکه عصبی کانولوشن آموزش داده می‌شوند تا بسته‌ها در اینترنت‌وسایل‌نقلیه به عادی و مخرب دسته‌بندی شوند.



شکل ۱: چارچوب سیستم تشخیص نفوذ پیشنهادی مبتنی بر شبکه‌عصبی‌کانولوشن

۳-۱- پیش‌پردازش داده‌ها

برای توسعه سیستم تشخیص نفوذ پیشنهادی برای اینترنت‌وسایل‌نقلیه، از مجموعه داده VDoS-LRS [8] استفاده شده‌است که شامل سه نوع اصلی حمله انکارسرویس: سیلاب SYN، سیلاب UDP و Slowloris است. این مجموعه داده مختص اینترنت‌وسایل‌نقلیه است و سه محیط شهری، بزرگراه و روستایی را در نظر گرفته است؛ زیرا هر سه محیط دارای ویژگی‌های متمایزی از جمله پوشش شبکه و سرعت وسیله‌نقلیه هستند.

مجموعه داده VDoS-LRS دارای ۷۹ ویژگی و ۷۴۷۶۹۴ رکورد در محیط بزرگراه، ۲۶۱۸۹۱ رکورد در محیط شهری و ۶۴۶۴۲۶ رکورد در محیط روستایی می‌باشد. همچنین این مجموعه داده ویژگی‌های شبکه را بر اساس پنج دسته مختلف، زمان، بایت‌ها، بسته‌ها، رفتار و جریان در نظر گرفته است. ویژگی‌های مبتنی بر رفتار (مانند duration) برای ارزیابی گره براساس اقدامات قبل از رفتار آن استفاده می‌شود؛ به عنوان مثال، اگر یک اتصال برای مدت طولانی طول بکشد، این رفتار ممکن است رفتار یک حمله DoS باشد. ویژگی‌های مبتنی بر بایت‌ها و بسته‌ها (مانند total_f/b_Packets، Init_Win_bytes_forward/backward، f/b_AvgBytesPerBulk، total/min/max/mean/std_f/b_Pktl، f/b_PktsPerSecond وغیره) برای شمارش تعداد بایت‌ها یا بسته‌های مبادله شده استفاده می‌شود. ویژگی‌های مبتنی بر بایت و بسته، امکان تشخیص افزایش ترافیک زیاد و غیرعادی که نشانه حمله DoS است را فراهم می‌کند. علاوه‌براین، زمان صرف شده بین

انتقال بسته‌ها در یک حمله DoS خیلی کوتاه است؛ به همین دلیل، ویژگی‌های مبتنی بر زمان (مانند Min/mean/max/std_active، total/min/max/mean/std_f/b_iat، Min/mean/max/std_idle وغیره) می‌تواند نشان‌دهنده حملات DoS باشد. ویژگی‌های جریان داده (مانند Flow_Pkts/Byts_PerSecond، min/max_flowpktl، Min/max/mean/std_flowiat، Sflow_f/b_Packet و غیره) بجای تمرکز بر روی بسته‌ها، روی جریانی از بسته ها با فضای ذخیره‌سازی کمتر کار می‌کنند.

این مجموعه داده، پورت و آدرس IP مبدا و مقصد را درنظر نگرفته است، زیرا مهاجم‌ها می‌توانند به راحتی آن‌ها را تغییر دهند. همچنین ممکن است مدل دسته‌بندی را گمراه کند و از تجزیه و تحلیل دقیق بقیه ویژگی‌ها جلوگیری کند.

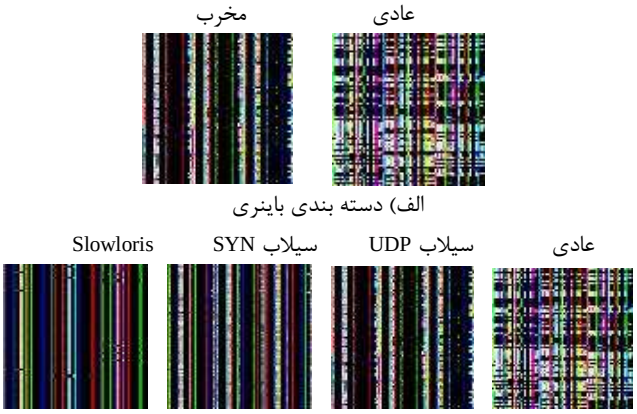
برای پیش پردازش بسته‌ها در سه محیط اینترنت‌وسایل‌نقلیه، از Dropna برای تمیز کردن داده‌ها استفاده کردیم. از طرفی با توجه به کم بودن نمونه‌های کلاس حمله Slowloris و کلاس عادی، با مشکل داده‌های نامتعادل روبرو شدیم که منجر به پیش‌بینی نادرست می‌شود [16]. بنابراین، برای داشتن داده‌های متعادل، از نمونه‌گیری بیش‌ازحدتصادفی استفاده کردیم که نمونه‌های کلاس را بدون از دست دادن اطلاعات تکرار می‌کند.

سپس داده‌ها را به فرم‌های تصویر تبدیل کردیم زیرا مدل‌های شبکه عصبی کانولوشن عملکرد بهتری روی تصاویر دارند [17]. هر تصویر یک تصویر مربع رنگی با سه کانال قرمز، آبی و سبز است. مجموعه داده VDoS-LRS دارای ۷۹ ویژگی است، بنابراین هر بسته به تصویری به شکل ۳*۷۹*۷۹ تبدیل می‌شود. برای دسته‌بندی باینری، اگر همه نمونه های یک تصویر، مخرب باشند آن تصویر به عنوان مخرب برچسب گذاری می‌شود. از طرف دیگر، تصاویر با نمونه‌های معمولی به عنوان عادی برچسب‌گذاری می‌شوند. برای نسخه دسته‌بند چندگانه چارچوب ما، تصویر با بیشترین نمونه از هر نوع حمله انکارسرویس به عنوان همان نوع حمله برچسب‌گذاری می‌شود.

پس از پیش‌پردازش داده‌ها، تصاویر آماده آموزش توسط مدل پیشنهادی ما مبتنی بر شبکه عصبی کانولوشن هستند. نمونه‌های هر کلاس در محیط بزرگراه در شکل ۲ نشان داده شده‌است. همانطور که شکل ۲ نشان می‌دهد نمونه‌های عادی و نمونه‌های مخرب دارای الگوهای ویژگی متفاوت هستند در حالی که انواع مختلف حمله انکارسرویس دارای الگوهای ویژگی مشابه هستند؛ که این مسئله تشخیص دقیق انواع مختلف حمله انکارسرویس را دشوار می‌کند.

۳-۲- مدل‌پیشنهادی مبتنی بر شبکه عصبی کانولوشن

شبکه عصبی کانولوشن زیرگروهی از شبکه‌های عصبی است که عمدتاً برای دسته‌بندی تصاویر استفاده می‌شود [18]. شبکه عصبی کانولوشن به طور خودکار ویژگی‌های مهم را بدون نظارت انسانی تشخیص می‌دهد و لایه‌های کانولوشنی آن بدون از دست دادن اطلاعات، ابعاد بالای تصاویر را کاهش می‌دهد. همچنین لایه‌های ادغام آن تعداد پارامترهای یادگیری را کاهش می‌دهد و از بیش‌برازش جلوگیری می‌کند.



شکل ۲: نمونه تصاویر هر کلاس در محیط بزرگراه: الف) دسته‌بندی باینری، ب) دسته‌بندی چندگانه.

پس از آموزش مدل‌های مختلف شبکه عصبی کانولوشن بر روی مجموعه داده VDoS-LRS، دو مدل شبکه عصبی کانولوشن با بهترین عملکرد انتخاب می‌شوند. مدل ۱ و مدل ۲ مدل های منتخبی هستند که با تعداد لایه‌های مناسب و چیدمان صحیح ان‌ها طراحی شده‌اند. این دو مدل ساختار مشابهی دارند، با این تفاوت که مدل ۲ دارای لایه های کانولوشن بیشتری است که در جدول ۱ توضیح داده شده است. 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 ارائه شده

لایه ها	مدل۱	مدل۲
لایه ۱	Conv(16)	Conv(16)
لایه ۲	Maxpooling	Maxpooling
لایه ۳	Conv(256)	Conv(128)
لایه ۴	Averagepooling	Maxpooling
لایه ۵	Dense(256)	Conv(256)
لایه ۶	Dropout	Conv(256)
لایه ۷	Dense(4)	Averagepooling
لایه ۸	–	Dense(256)
لایه ۹	–	Dropout
لایه ۱۰	–	Dense(4)

در هر دو مدل ۱ و ۲، فعال ساز واحدخطی‌اصلاح‌شده (ReLU) و لایه حداکثرادغام پس از لایه‌های کانولوشن استفاده می‌شود. لایه کانولوشن، تصویر را برای یک ویژگی خاص فیلتر می‌کند و فعال ساز واحدخطی‌اصلاح‌شده، آن ویژگی را در تصویر فیلتر شده تشخیص می‌دهد. در نهایت، لایه حداکثرادغام تصویر را متراکم می‌کند تا ویژگی‌ها را افزایش دهد. بنابراین، استفاده از واحد خطی اصلاح شده به جلوگیری از رشد نمایی در محاسبات مورد نیاز برای راه اندازی شبکه عصبی کمک می‌کند [19]. همچنین استفاده از لایه ادغام میانگین جهانی و لایه حذفی به جلوگیری از بیش برازش مدل پیشنهادی ما کمک می کنند.

در نهایت، از تابع softmax برای دسته‌بندی چندگانه به منظور برگرداندن احتمال‌های هر کلاس استفاده می‌شود که کلاس هدف بیشترین احتمال را دارد. سپس، آنتروپی متقاطع طبقه‌ای (categorical crossentropy) به عنوان تابع ضرر برای محاسبه تفاوت بین توزیع‌های احتمال استفاده می‌شود. از آنجایی که ما بیش از دو کلاس داریم، تابع ضرر آنتروپی متقاطع طبقه‌ای بهترین انتخاب است. همچنین از آدام به عنوان بهینه ساز برای کاهش تابع ضرر و ارائه دقیق ترین نتایج ممکن استفاده کردیم؛ زیرا این بهینه‌ساز بسیار سریع است [20].

مدل ۱ و مدل ۲ بر روی مجموعه داده آموزشی با تعداد تکرار لازم و یکسان آموزش داده می‌شوند. از بین این دو مدل، مدل ۲ انتخاب می‌شود زیرا نتایج بهتری در دسته‌بندی انواع مختلف حمله انکار سرویس به دست می‌آورد. شرح کامل ارزیابی این دو مدل در بخش چهارم آورده شده است. بهترین مدل پیشنهادی (مدل ۲) یک شبکه عصبی کانولوشن منحصر به فرد ۱۰ لایه است که دارای توپولوژی لایه زیر است: لایه کانولوشن، لایه حداکثرادغام، لایه کانولوشن، لایه حداکثرادغام، لایه کانولوشن، لایه کانولوشن، لایه ادغام میانگین جهانی، لایه متراکم، لایه حذفی و در نهایت لایه متراکم. داشتن چندین لایه کانولوشن که در امتداد عمق مدل قرار گرفته‌اند، به مدل اجازه می‌دهد تا ویژگی‌های سطح بالا (نه فقط لبه‌ها و گوشه‌ها) را از تصاویر ورودی استخراج کنند. همچنین با استفاده از دو لایه کانولوشن متوالی می‌توانیم نمایش بهتری از تصویر، بدون از دست‌دادن سریع تمام اطلاعات مکانی داشته باشیم.

۴- ارزیابی مدل پیشنهادی

سیستم تشخیص نفوذ مبتنی بر شبکه عصبی کانولوشن پیشنهادی بر روی مجموعه داده VDoS-LRS [8]، همانطور که در بخش ۱-۳ توضیح داده شده است، ارزیابی شده است. این مجموعه داده، جدید و مربوط به سال ۲۰۲۰ است. در این بخش، مدل شبکه عصبی کانولوشن پیشنهادی خود را از طریق دو سناریو ارزیابی می‌کنیم: دسته‌بندی باینری برای دسته‌بندی بسته‌ها به ترافیک عادی و مخرب و دسته‌بندی چندگانه برای دسته‌بندی انواع مختلف حمله انکارسرویس (سیلاب SYN، سیلاب UDP و Slowloris). ما از ۱۰۰٪ مجموعه داده VDoS-LRS برای آزمایش‌های خود استفاده کردیم. ۷۵ درصد آن برای آموزش و ۲۵ درصد ان برای تست استفاده شده است.

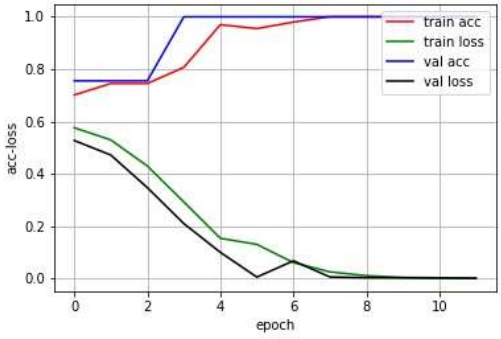
ما آزمایش‌های خود را با استفاده از کتابخانه‌های Keras و Scikit-learn در پایتون انجام دادیم. در آزمایش‌ها، Google colab برای آموزش سریع‌تر مدل استفاده شده است زیرا دارای GPU قدرتمند (Tesla K80) و پردازنده Intel Xeon با دو هسته ۲.۲۰ گیگاهرتز است.

معیارهای ارزیابی، از جمله صحت، دقت، فراخوانی، معیار F1، نرخ مثبت کاذب و نرخ منفی کاذب (FNR) برای ارزیابی عملکرد استفاده شده‌اند تا ارزیابی کاملی از سیستم تشخیص نفوذ پیشنهادی داشته باشیم [21]. علاوه بر این، برای ارزیابی کارآمد مدل پیشنهادی، زمان تست هر بسته نیز در نظر گرفته شده و مقایسه می‌شود. در آزمایش‌های ما، تعداد دوره‌ها برابر با ۲۰ درنظرگرفته شده است زیرا دوره‌های بسیار زیاد می‌تواند منجر به بیش برازش مجموعه داده آموزشی شود. همچنین، مقدار صبر برابر ۸ برای توقف زودهنگام انتخاب شده است. توقف زودهنگام روشی است که پس از بهبود عملکرد مدل در مجموعه داده اعتبارسنجی، آموزش را متوقف می‌کند تا از بیش‌برازش جلوگیری کند. همچنین به منظور افزایش سرعت آموزش، اندازه دسته را برابر ۱۲۸ درنظرگرفتیم؛ زیرا دسته‌های بزرگتر مراحل جستجوی کمتری را برای حل بهینه انجام می‌دهند.

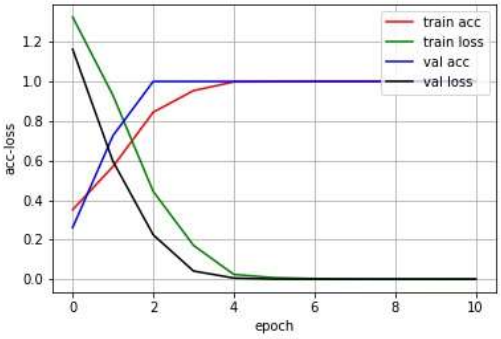
جداول ۲ تا ۴ نتایج دسته‌بندی این دو مدل را در سه محیط (بزرگراه، شهری و روستایی) شرح می‌دهند. همانطور که نتایج نشان می‌دهد، مدل پیشنهادی ما انواع مختلف حملات انکارسرویس را در هر سه محیط به طور موثر تشخیص می‌دهد. مدل ۲ لایه های کانولوشنی بیشتری نسبت به مدل ۱ دارد که باعث می شود ویژگی های سطح پایین بیشتری را یاد بگیرد و در دسته‌بندی چندگانه به نتایج بهتری دست یابد، اما زمان تشخیص حملات را افزایش می‌دهد. همچنین نتایج مختلف در سه محیط نشان می‌دهند که هر محیط با ویژگی‌های منحصربه‌فرد خود مانند تراکم شبکه و سرعت وسایل نقلیه بر نتایج تشخیص حمله تأثیر می‌گذارد.

همانطور که در شکل ۳ نشان داده شده است مدل پیشنهادی دارای صحت آموزشی ۱۰۰٪ و صحت اعتبار سنجی ۱۰۰٪ است. نمودارهای ابی و قرمز به ترتیب صحت اعتبارسنجی و اموزش و نمودارهای مشکی و سبز به ترتیب تابع ضرر اعتبارسنجی و اموزش

را نشان می‌دهند. فاصله بین نمودارهای اعتبارسنجی و دقت آموزش 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.



الف) دسته‌بندی باینری



ب) دسته‌بندی چندگانه

شکل ۳: نمودارهای صحت و ضرر به دوره در مدل (۲) برای محیط شهری: الف) دسته‌بندی باینری؛ ب) دسته‌بندی چندگانه.

برای محافظت از اینترنت‌وسایل‌نقلیه در برابر حملات بااستفاده از تکنیک‌های یادگیری ماشین، تحقیقات زیادی انجام شده است، اما از مجموعه داده‌های مختص شبکه خودرویی استفاده نکردند [22,14,12,10]. اکثر آنها از مجموعه داده‌های NSL-KDD، KDD99 و UNSW-NB15 که فاقد داده‌های شبکه خودرویی هستند، استفاده کردند که باعث ارزیابی نادرست مدل پیشنهادی می‌شود. از سوی دیگر، برخی از تحقیقات از داده‌های شبیه‌سازی‌شده استفاده کردند در حالی که پارامترهای شبیه‌سازی، محیط واقعی را منعکس نمی‌کنند. بنابراین، ما یک ارزیابی صحیح از مدل پیشنهادی خود داشتیم زیرا مجموعه داده VDoS-LRS، یک مجموعه داده جدید، واقعی و مختص اینترنت‌وسایل‌نقلیه است.

راحل و همکاران [8] با استفاده از الگوریتم درخت تصمیم (DT) به صحت ۹۹.۹۹٪ دست یافتند، اما زمان تشخیص را برای تشخیص بلادرنگ حملات مخرب انکارسرویس در نظر نگرفتند. همچنین، نتایج نشان می‌دهد که مدل‌های شبکه عصبی کانولوشن از سایر الگوریتم‌های یادگیری ماشین قدیمی در هر سه محیط بهتر عمل می‌کنند.

۵- نتیجه‌گیری

اینترنت‌وسایل‌نقلیه در مقایسه با شبکه‌های اقتضایی خودرو، مقیاس پذیرتر است و شبکه بزرگ‌تری را برای شهرهای بزرگ فراهم می‌کند اما امنیت و حریم خصوصی از چالش‌های اساسی این محیط محسوب می شوند؛ زیرا حملات مختلفی ممکن است در اینترنت‌وسایل‌نقلیه رخ دهد و باعث نارضایتی کاربر و ناکارآمدی شبکه شود. یکی از مهم ترین حملات، حمله انکارسرویس است که دردسترس بودن شبکه را به خطر می‌اندازد و موجب تصادفات جاده‌ای و ازدست دادن جان کاربران می‌شود. سیستم‌های تشخیص نفوذ موجود نمی توانند انواع مختلف حملات انکارسرویس را به طور موثر شناسایی کنند.

بنابراین برای محافظت از اینترنت‌وسایل‌نقلیه دربرابر حملات انکارسرویس، ما یک چارچوب تشخیص نفوذ مبتنی بر شبکه عصبی کانولوشن را پیشنهاد دادیم. سیستم تشخیص نفوذ پیشنهادی ما شامل یک شبکه عصبی کانولوشن ۱۰ لایه است که سه نوع حمله انکارسرویس: سیلاب UDP، سیلاب SYN و Slowloris را در سه محیط (بزرگراه، شهری و روستایی) شناسایی می‌کند. این چارچوب هم دسته‌بند باینری و هم دسته‌بند چندگانه است. سیستم تشخیص نفوذ پیشنهادی ما بر روی مجموعه داده VDoS-LRS ارزیابی شده است، زیرا استفاده از مجموعه داده‌های واقعی مختص اینترنت‌وسایل‌نقلیه چالشی برای ارزیابی صحیح است. همچنین، تمام معیارهای ارزیابی برای ارزیابی کامل این سیستم استفاده شده است. نتایج تجربی نشان می‌دهد که سیستم تشخیص نفوذ پیشنهادی ما می‌تواند به طور موثر انواع مختلف حملات انکارسرویس را با نرخ صحت ۱۰۰٪ نسبت به چارچوب موجود شناسایی کند. در کارهای آینده، سیستم تشخیص نفوذ پیشنهادی خود را برای شناسایی سایر حملات در محیط اینترنت‌وسایل‌نقلیه گسترش خواهیم داد.

جدول۲) ارزیابی و مقایسه عملکرد مدل ها در محیط بزرگراه

	روش	کلاس	دقت	فراخوانی	معیارF	میانگین مثبت کاذب	میانگین منفی کاذب	میانگین صحت	زمان تست هربسته (ثانیه)
دسته بندی چند کلاسه	مدل ۱	عادی	۱.۰۰	۱.۰۰	۱.۰۰	۰.۰۰۰۵۶	۰.۰۰۱۴۱	۰.۹۹۹۱۳	۰.۰۵۴۷۸
		حمله سیلاب UDP	۱.۰۰	۰.۹۹۴۳۵	۰.۹۹۷۱۷				
		حمله سیلاب SYN	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله Slowloris	۰.۹۹۲۵۷	۱.۰۰	۰.۹۹۶۲۷				
	مدل ۲	عادی	۱.۰۰	۱.۰۰	۱.۰۰	۰.۰۰	۰.۰۰	۱.۰۰	۰.۰۵۸۲۴
		حمله سیلاب UDP	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله سیلاب SYN	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله Slowloris	۱.۰۰	۱.۰۰	۱.۰۰				
	[۸]	عادی	۰.۹۹۹۸۸	۰.۹۹۹۹۲	۰.۹۹۹۹۰	۰.۰۰۰۰۳	۰.۰۰۰۲۵	۰.۹۹۹۹۸	-
		حمله سیلاب UDP	۰.۹۹۹۹۹	۰.۹۹۹۹۹	۰.۹۹۹۹۹				
		حمله سیلاب SYN	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله Slowloris	۰.۹۹۹۰۵	۰.۹۹۹۰۵	۰.۹۹۹۰۵				
دسته بندی باینری	مدل ۱	عادی	۱.۰۰	۰.۹۶۳۴۱	۰.۹۸۱۳۷	۰.۰۱۸۲۹	۰.۰۱۸۲۹	۰.۹۹۷۱۳	۰.۰۵۴۲۰
		مخرب	۰.۹۹۶۹۰	۱.۰۰	۰.۹۹۸۴۵				
	مدل ۲	عادی	۱.۰۰	۱.۰۰	۱.۰۰	۰.۰۰	۰.۰۰	۱.۰۰	۰.۰۶۰۲۲
		مخرب	۱.۰۰	۱.۰۰	۱.۰۰				
	[۸]	عادی	۰.۹۹۹۸۸	۰.۹۹۹۹۲	۰.۹۹۹۹۰	۰.۰۰۰۰۴	۰.۰۰۰۰۴	۰.۹۹۹۸۸	-
		مخرب	۰.۹۹۹۹۹	۰.۹۹۹۹۹	۰.۹۹۹۹۹				

جدول۳) ارزیابی و مقایسه عملکرد مدل ها در محیط شهری

	روش	کلاس	دقت	فراخوانی	معیارF	میانگین مثبت کاذب	میانگین منفی کاذب	میانگین صحت	زمان تست هربسته (ثانیه)
دسته بندی چند کلاسه	مدل ۱	عادی	۱.۰۰	۱.۰۰	۱.۰۰	۰.۰۰	۰.۰۰	۱.۰۰	۰.۰۵۱۳۹
		حمله سیلاب UDP	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله سیلاب SYN	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله Slowloris	۱.۰۰	۱.۰۰	۱.۰۰				
	مدل ۲	عادی	۱.۰۰	۱.۰۰	۱.۰۰	۰.۰۰	۰.۰۰	۱.۰۰	۰.۰۵۲۳۲
		حمله سیلاب UDP	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله سیلاب SYN	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله Slowloris	۱.۰۰	۱.۰۰	۱.۰۰				
	[۸]	عادی	۰.۹۹۹۸۹	۰.۹۹۹۶۹	۰.۹۹۹۷۹	۰.۰۰۰۰۸	۰.۰۰۰۰۸	۰.۹۹۹۹۷	-
		حمله سیلاب UDP	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله سیلاب SYN	۰.۹۹۹۹۸	۰.۹۹۹۹۸	۰.۹۹۹۹۸				
		حمله Slowloris	۰.۹۹۲۷۵	۱.۰۰	۰.۹۹۶۳۶				
دسته بندی باینری	مدل ۱	عادی	۱.۰۰	۱.۰۰	۱.۰۰	۰.۰۰	۰.۰۰	۱.۰۰	۰.۰۵۰۵۶
		مخرب	۱.۰۰	۱.۰۰	۱.۰۰				
	مدل ۲	عادی	۱.۰۰	۱.۰۰	۱.۰۰	۰.۰۰	۰.۰۰	۱.۰۰	۰.۰۵۰۷۸
		مخرب	۱.۰۰	۱.۰۰	۱.۰۰				
	[۸]	عادی	۱.۰۰	۰.۹۹۹۸۴	۰.۹۹۹۹۴	۰.۰۰۰۰۵	۰.۰۰۰۰۵	۰.۹۹۹۹۹	-
		مخرب	۰.۹۹۹۹۹	۱.۰۰	۰.۹۹۹۹۹				

جدول۴) ارزیابی و مقایسه عملکرد مدل ها در محیط روستایی

	روش	کلاس	دقت	فراخوانی	معیارF	میانگین مثبت کاذب	میانگین منفی کاذب	میانگین صحت	زمان تست هربسته (ثانیه)
دسته بندی چند کلاسه	مدل ۱	عادی	۰.۹۹۳۲۰	۱.۰۰	۰.۹۹۶۵۹	۰.۰۰۰۴۴	۰.۰۰۱۴۲	۰.۹۹۹۲۹	۰.۰۵۶۲۵
		حمله سیلاب UDP	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله سیلاب SYN	۱.۰۰	۰.۹۹۴۲۹	۰.۹۹۷۱۳				
		حمله Slowloris	۱.۰۰	۱.۰۰	۱.۰۰				
	مدل ۲	عادی	۱.۰۰	۱.۰۰	۱.۰۰	۰.۰۰	۰.۰۰	۱.۰۰	۰.۰۵۶۹۶
		حمله سیلاب UDP	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله سیلاب SYN	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله Slowloris	۱.۰۰	۱.۰۰	۱.۰۰				
	[۸]	عادی	۰.۹۹۹۵۹	۰.۹۹۹۸۹	۰.۹۹۹۷۴	۰.۰۰۰۰۴	۰.۰۰۰۳۷	۰.۹۹۹۹۸	-
		حمله سیلاب UDP	۱.۰۰	۱.۰۰	۱.۰۰				
		حمله سیلاب SYN	۱.۰۰	۰.۹۹۹۹۹	۰.۹۹۹۹۹				
		حمله Slowloris	۰.۹۹۹۵۴	۰.۹۹۸۶۲	۰.۹۹۹۰۸				
دسته بندی باینری	مدل ۱	عادی	۰.۹۲۳۰۸	۱.۰۰	۰.۹۶	۰.۰۰۵۱۴	۰.۰۰۵۱۴	۰.۹۹۰۸۳	۰.۰۵۶۱۰
		مخرب	۱.۰۰	۰.۹۸۹۷۰	۰.۹۹۴۸۲				
	مدل ۲	عادی	۱.۰۰	۱.۰۰	۱.۰۰	۰.۰۰	۰.۰۰	۱.۰۰	۰.۰۵۷۵۳
		مخرب	۱.۰۰	۱.۰۰	۱.۰۰				
	[۸]	عادی	۰.۹۹۹۸۹	۰.۹۹۹۶۹	۰.۹۹۹۷۹	۰.۰۰۰۱۵	۰.۰۰۰۱۵	۰.۹۹۹۹۸	-
		مخرب	۰.۹۹۹۹۸	۰.۹۹۹۹۹	۰.۹۹۹۹۹				

مراجع

[1] Adhikary, K., et al., *Hybrid algorithm to detect DDoS attacks in VANETs*. Wireless Personal Communications, 2020. 114(4): p. 3613-3634.

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

[3] Kelarestaghi, K.B., et al., *Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures*. arXiv preprint arXiv:1903.01541, 2019.

[4] Kumar, S. and K. Dutta, *Trust based intrusion detection technique to detect selfish nodes in mobile ad hoc networks*. Wireless Personal Communications, 2018. 101(4): p. 2029-2052.

[5] Sherazi, H.H.R., et al., DDoS attack detection: *A key enabler for sustainable communication in internet of vehicles*. Sustainable Computing: Informatics and Systems, 2019. 23: p. 13-20.

[6] Verma, A., et al., *The security perspectives of vehicular networks: a taxonomical analysis of attacks and solutions*. Applied Sciences, 2021. 11(10): p. 4682.

[7] Ahmed, I., A. Ahmad, and G. Jeon, *Deep Learning-based Intrusion Detection System for Internet of Vehicles*. IEEE Consumer Electronics Magazine, 2021.

[8] Rahal, R., A. Amara Korba, and N. Ghoualmi-Zine, *Towards the development of realistic dos dataset for intelligent transportation systems*. Wireless Personal Communications, 2020. 115(2): p. 1415-1444.

[9] Zhang, J., et al., *Intrusion detection system using deep learning for in-vehicle security*. Ad Hoc Networks, 2019. 95: p. 101974.

[10] Ashraf, J., et al., *Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems*. IEEE Transactions on Intelligent Transportation Systems, 2020. 22(7): p. 4507-4518.

[11] Ullah, S., et al., *HDL-IDS: a hybrid deep learning architecture for intrusion detection in the Internet of Vehicles*. Sensors, 2022. 22(4): p. 1340.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] Du, G., et al., *Towards graph-based class-imbalance learning for hospital readmission*. Expert Systems with Applications, 2021. 176: p. 114791.

[17] 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.

[18] Song, H.M., J. Woo, and H.K. Kim, *In-vehicle network intrusion detection using deep convolutional neural network*. Vehicular Communications, 2020. 21: p. 100198.

[19] Raghu, M., et al. *On the expressive power of deep neural networks*. in international conference on machine learning. 2017. PMLR.

[20] Li, W., G.-G. Wang, and A.H. Gandomi, *A survey of learning-based intelligent optimization algorithms*. Archives of Computational Methods in Engineering, 2021. 28(5): p. 3781-3799.

[21] Powers, D.M., *Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation*. arXiv preprint arXiv:2010.16061, 2020.

[22] 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.