Journal of Applied And Basic Machine Intelligence Research (ABMIR)

پژوهش‌های نظری و کاربردی هوش ماشینی

سال دوم، شماره دوم، پاییز و زمستان ۱۴۰۳، صفحات۹۳ – ۸۳

تشخیص حملات در شبکه‌های خودرویی خودران با استفاده از یادگیری عمیق

عباس حری*، لیلا صمیمی دهکردی

استادیار گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه شهرکرد، شهرکرد، ایران

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۳/۹/۱۹
تاریخ پذیرش:
۱۴۰۳/۱۲/۹

کلیدواژه‌ها:
وسایل نقلیه خودران، تشخیص نفوذ، یادگیری عمیق، شبکه عصبی، یادگیری گروهی، اینترنت اشیاء

نویسنده‌مسئول:
horri@sku.ac.ir

چکیده

وسایل نقلیه مدرن، ازجمله وسایل نقلیه خودران و وسایل نقلیه متصل، به‌طور فزاینده‌ای به محیط خارج از خود متصل می‌شوند و از این طریق عملکردها و خدمات مختلفی را ارائه می‌کنند. افزایش اتصال‌پذیری باعث افزایش حملات اینترنتی به وسایل نقلیه خودران گردیده است و درنتیجه، باعث آسیب‌پذیری این وسایل در برابر تهدیدات سایبری شده است. به‌دلیل ضعف و یا عدم وجود رویه‌های احراز هویت و رمزگذاری در شبکه‌های خودرو، استفاده از سیستم‌های تشخیص نفوذ یکی از روش‌های ضروری برای محافظت از سیستم خودروهای مدرن در برابر حملات سایبری است. در این مقاله، یک سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق با استفاده از تشخیص تصاویر برای سیستم‌های وسایل نقلیه پیشنهادشده است. همچنین، از تکنیک تبدیل بردار ویژگی‌ها به تصاویر برای بهینه‌سازی تشخیص استفاده شده‌است. سیستم تشخیص نفوذ پیشنهادی با استفاده از تکنیک یادگیری گروهی مبتنی بر میانگین بهینه‌شده‌است. در آزمایش‌ها، روش پیشنهادی بیش از ۹۹,۲۵ درصد نرخ تشخیص و به همین مقدار معیار F1 را در دو مجموعه داده امنیتی استاندارد شامل مجموعه داده‌های Car-Hacking و مجموعه داده CICIDS2017 نشان داده است. همچنین، زمان اجرای روش بر روی تجهیزات اینترنت اشیاء اندازه‌گیری شده‌است که نشان‌دهنده قابلیت اجرای روش پیشنهادی است.

doi : 10.22034/ABMIR.2025.22510.1083

E-ISSN: 2821-2037

۱- مقدمه

با توسعه سریع فناوری‌های مرتبط با اینترنت اشیاء[1] و اینترنت وسایل نقلیه[2]، وسایل نقلیه مدرن از حالت سنتی به وسایل نقلیه تحت کنترل شبکه، ازجمله وسایل نقلیه خودمختار[3] و وسایل نقلیه متصل[4] به شبکه تبدیل‌شده‌اند [۱]. شبکه وسایل نقلیه، شامل شبکه‌های درون وسیله نقلیه و شبکه‌های خارج از آن است. شبکه‌های درون خودرو[5] شامل گذرگاه سیستم مرکزی به نام شبکه کنترل‌کننده[6] است که ارتباطات بین واحدهای کنترل الکترونیکی را امکان‌پذیر می‌سازد. واحدها از طریق شبکه کنترل وظایف خود را انجام می‌دهند و تصمیمات مناسب را اتخاذ می‌کنند [۲]. از سوی دیگر، شبکه‌های خارج از خودرو امکان ارتباط بین وسایل نقلیه هوشمند و سایر قسمت‌ها در اینترنت وسایل نقلیه، ازجمله واحدهای کنار جاده، زیرساخت‌ها و سایر کاربران در جاده را امکان‌پذیر می‌کنند [۳].

بهبود اتصال و دسترسی به شبکه‌های وسایل نقلیه میزان و عمق حملات سایبری علیه وسایل نقلیه مدرن را افزایش داده است [٤]. علاوه بر این، به‌دلیل محدودیت اندازه دربسته‌های شبکه کنترل، هیچ راهبرد احراز هویت یا رمزگذاری در پردازش این بسته‌ها وجود ندارد [۱]. فقدان اقدامات امنیتی اساسی، مهاجمان سایبری را قادر می‌سازد تا پیام‌های مخرب را به اینترنت وسایل نقلیه تزریق کنند و انواع مختلفی از حملات مانند حملات انکار سرویس[7] و حملات جعل هویت یا جعل داده را انجام دهند. از سوی دیگر، ارتباطات نوظهور سلولی بین وسایل نقلیه هوشمند و شبکه‌های خارجی، این وسایل نقلیه را در برابر انواع حملات سایبری متعارف نیز آسیب‌پذیر کرده است [۵]. بنابراین، توسعه سیستم‌های تشخیص نفوذ[8] برای محافظت از سیستم‌های اینترنت وسایل نقلیه، وسایل نقلیه هوشمند و شناسایی حملات سایبری در این حوزه بسیار مهم است.

اخیراً با توجه به پیشرفت تکنیک‌های یادگیری ماشین و یادگیری عمیق، کاربردهای آن‌ها در امنیت سایبری و سیستم‌های خودرو توجه محققان و سازندگان خودرو را به خود جلب کرده است [٦]. این تکنیک‌ها به‌طور گسترده برای توسعه سیستم تشخیص نفوذهای مبتنی بر طبقه‌بندی استفاده می‌شوند که می‌توانند بین ترافیک عادی شبکه و حملات سایبری مختلف از طریق تجزیه‌وتحلیل داده‌های ترافیکی تمایز قائل شوند [۷].

در این مقاله، یک مدل سیستم تشخیص نفوذ هوشمند مبتنی بر شبکه‌های عصبی پیچشی[9] بهینه‌شده، برای محافظت از سیستم‌های اینترنت وسایل نقلیه پیشنهادشده است. مدل پیشرفته شبکه عصبی پیچشی، براساس تبدیل بردار ویژگی‌ها به تصاویر برای آموزش شبکه عصبی بر روی داده‌های ترافیک شبکه خودرو استفاده شده است. اثربخشی و کارایی چارچوب سیستم تشخیص نفوذ پیشنهادی با استفاده از دو مجموعه داده شبکه وسایل نقلیه عمومی شامل مجموعه داده هک خودرو [۸] و مجموعه داده CICIDS2017 [۹] ارزیابی می‌شود. این مقاله شامل نوآوری‌های زیر است:

۱) چارچوب جدید و موثری را برای جلوگیری از حملات سایبری پیشنهاد می‌کند که قابلیت شناسایی در شبکه‌های درون خودرویی و بیرون خودرو را از طریق شبکه عصبی پیچشی، بر روی تصاویر دارد.

۲) یک روش تبدیل داده را پیشنهاد می‌کند که می‌تواند به‌طور مؤثر داده‌های ترافیک شبکه وسایل نقلیه را به تصاویر تبدیل کند تا الگوهای مختلف حمله سایبری را آسان‌تر تشخیص دهد.

۳) از یک روش یادگیری گروهی مبتنی بر میانگین برای به‌دست آوردن نتایج بهتر استفاده می‌کند.

مقاله به شرح زیر سازماندهی‌شده است. بخش دوم روش تحقیق است که کارهای مرتبط مانند الگوریتم‌های یادگیری ماشین و

[1] Internet Of Things
[2] Internet Of Vehicles
[3] Autonumus Vehicles
[4] Contected Vechile
[5] Internal Vechile Network
[6] Control Area Network
[7] Denal of service Attack
[8] Intrusion Detection Sysytem
[9] Convolutional Neural Network

یادگیری عمیق برای تشخیص نفوذ شبکه خودرو و چارچوب پیشنهادی را ارائه می‌کند. بخش ۳ نتایج حاصل از پیاده‌سازی را ارائه و مورد بحث قرار می‌دهد. درنهایت، نتیجه‌گیری در بخش ٤ مقاله آمده است.

۲- مرور کارهای گذشته

مدل‌های یادگیری ماشین و یادگیری عمیق به‌طور گسترده در تشخیص نفوذ استفاده‌شده‌اند. روزای و همکاران [۵] یک سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق برای وسایل نقلیه متصل با استفاده از پرسپترون چندلایه پیشنهاد کردند. این مدل بر روی یک ریزپردازنده خودرو با استفاده از مجموعه داده CICIDS2017 مورد ارزیابی قرارگرفته است.

آلورانی و همکاران [۱۰] به بررسی آسیب‌پذیری سیستم‌های تشخیص نفوذ (IDS) در شبکه‌های داخلی وسایل نقلیه خودران در برابر حملات خصمانه می‌پردازد. این تحقیق نشان می‌دهد که حملات خصمانه می‌توانند به کاهش شدید عملکرد مدل‌های IDS منجر شوند، که امنیت وسایل نقلیه را به خطر می‌اندازد. نویسندگان روشی برای شبیه‌سازی حملات در شرایط دنیای واقعی ارائه کرده‌اند و یافته‌ها نشان می‌دهد که هشدارهای نادرست یکی از استراتژی‌های مؤثر برای تضعیف اعتماد کاربران است.

فیراستا و همکاران [۱۱] روش‌های یادگیری ماشین و یادگیری عمیق را برای شناسایی حملات انکار سرویس در شبکه‌های داخلی خودروهای خودران بررسی کرده است. نتایج نشان می‌دهد که مدل‌های یادگیری عمیق در کشف الگوهای پیچیده و وابستگی‌های زمانی عملکرد بهتری داشته‌اند

یانگ و همکاران [۳،٤] یک الگوریتم انباشته مبتنی بر درخت برای تحلیل ترافیک شبکه در محیط‌های اینترنت وسایل نقلیه پیشنهاد کرده‌اند. روش انباشتگی پیشنهادی عملکرد بالایی را درمجموعه داده‌های اینترنت وسایل نقلیه و CICIDS2017 نشان می‌دهد. چندین کار موجود بر روی توسعه سیستم تشخیص نفوذ مبتنی بر شبکه عصبی پیچشی برای شبکه‌های خودرو متمرکزشده است. مهدی و همکاران [۱] روش PLeNet را برای تشخیص نفوذ شبکه در خودرو بر اساس یادگیری عمیق پیشنهاد کرده‌اند. مدل پیشنهادی ایشان به امتیاز F1 بالایی درمجموعه داده‌های Car-Hacking دست‌یافته است. حسین و همکاران [۱۲] یک سیستم تشخیص نفوذ مبتنی بر LSTM[1] را برای تشخیص نفوذ برای شبکه داخلی خودرو پیشنهاد کرده‌اند. استفاده از مدل‌های LSTM در بسیاری از مشکلات تجزیه‌وتحلیل داده‌های سری زمانی به‌خوبی کار می‌کنند. سونگ و همکاران [٦] یک مدل سیستم تشخیص نفوذ مبتنی بر شبکه عصبی پیچشی عمیق با استفاده از InceptionResnet کاهش‌یافته برای شناسایی حملات در شبکه‌های درون وسیله نقلیه‌ها پیشنهاد کرده‌اند. مدل شبکه عصبی پیچشی عمیق دقت بالایی را درمجموعه داده‌های Car-Hacking نشان می‌دهد. اگرچه روش‌های فوق در اینترنت وسایل نقلیه به‌دقت بالایی دست‌یافته‌اند، در تشخیص حملات سایبری، هنوز جای زیادی برای بهبود عملکرد وجود دارد. هدف راه‌حل پیشنهادی در این مقاله ایجاد یک چارچوب سیستم تشخیص نفوذ بهینه با استفاده از مدل‌های پیشرفته شبکه عصبی پیچشی است که براساس پردازش تصاویر بهینه‌شده‌اند.

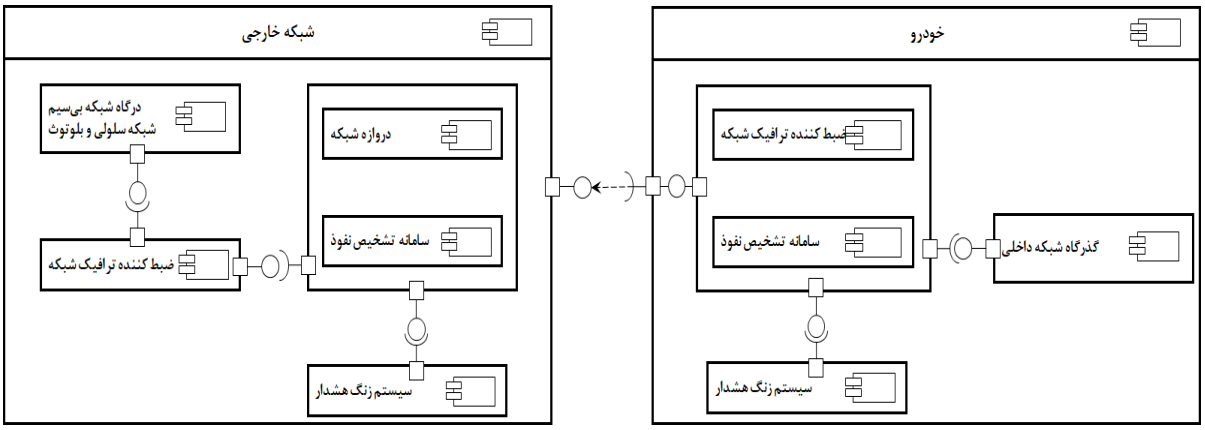
۳- روش پیشنهادی

۳-۱ نمای کلی سیستم

هدف از این کار ایجاد یک سیستم تشخیص نفوذ است که می‌تواند انواع حملات را در شبکه‌های درون خودرویی و بیرون خودرو شناسایی کند تا از هر دو شبکه محافظت کند. سناریوی حمله معمولی و معماری یک وسیله نقلیه محافظت‌شده با سیستم تشخیص نفوذ در شکل ۱ نشان داده‌شده است.

مهاجمان سایبری می‌توانند از طریق رابط گذرگاه شبکه داخلی حملات داخلی را به شبکه درون وسیله نقلیه‌ها انجام دهند و از طریق شبکه‌های خارجی حملات شبکه خارجی خودرویی را انجام دهند. همچنین، مهاجم می‌تواند از طریق رابط‌های بی‌سیم با ارسال بسته‌های ترافیکی مخرب در سیستم نفوذ کرده و یا در شبکه اختلال ایجاد کند. بنابراین، سیستم تشخیص نفوذ پیشنهادی باید هم در شبکه داخلی خودروها و هم در شبکه‌های خارجی مستقر شود. در خودروهای خودران، سیستم تشخیص نفوذ پیشنهادی را می‌توان در بالای گذرگاه داخلی مستقر کرد تا پیام‌های غیرعادی را شناسایی کرده و پیغام هشدار تولید کند [۳]. در شبکه‌های خارجی، سیستم

تشخیص نفوذ پیشنهادی می‌تواند در دروازه‌ها گنجانده شود تا همه بسته‌های مخربی که هدفشان نفوذ به وسایل نقلیه را شناسایی و مسدود کند [٤]. در این مقاله، یک شبکه عصبی پیچشی بهینه‌شده جدید و سیستم تشخیص نفوذ مبتنی بر یادگیری بر اساس تصاویر برای شناسایی انواع مختلف حملات در سیستم‌های اینترنت وسایل نقلیه پیشنهادشده است.



شکل (۱): نمای کلی شبکه خودرویی

شکل ۱ نمای کلی چارچوب سیستم تشخیص نفوذ پیشنهادی را نشان می‌دهد. ابتدا داده‌های شبکه درون وسیله نقلیه و داده‌های خارجی در تکه‌های مبتنی بر زمان جمع‌آوری می‌شوند و سپس، با استفاده از روش تبدیل برداری به تصاویر تبدیل می‌شوند. در مرحله بعد، مجموعه تصویر تولیدشده توسط مدل شبکه عصبی پیچشی آموزش داده می‌شود تا برای تشخیص نهایی استفاده شود.

۳-۲ تجزیه‌وتحلیل داده‌ها

برای توسعه سیستم تشخیص نفوذ پیشنهادی برای هر دو شبکه درون وسیله نقلیه و شبکه‌های خودروی خارجی، از دو مجموعه داده در این کار استفاده می‌شود. اولین مجموعه داده، مجموعه داده هک خودرو [۸] است که متعلق به داده‌های درون شبکه خودرو است. این داده‌ها با ارسال بسته‌ها به گذرگاه داخلی یک وسیله نقلیه واقعی تولیدشده‌اند. این مجموعه شامل شناسه شبکه کنترلی و فیلد داده ۸ بیتی است. مجموعه داده هک خودرو شامل چهار نوع حمله اصلی است: حملات منع سرویس، فازی، جعل داده از نوع چرخ‌دنده و حملات جعل داده از نوع چرخش. دومین مجموعه داده مورداستفاده مجموعه داده CICIDS2017[۹] است که داده‌های شبکه خارجی را نشان می‌دهد، این مجموعه داده شامل یک مجموعه داده امنیتی برای شبکه است و شامل به‌روزترین الگوهای حمله است. الگوهای حمله درمجموعه داده CICIDS2017 را می‌توان در پنج نوع اصلی حملات خلاصه کرد: حملات منع سرویس، حملات اسکن پورت، حملات جستجوی فراگیر[1]، حملات وب و حملات بات‌نت‌ها.

قبل از شروع الگوریتم تشخیص حمله، داده‌ها نیاز به پیش‌پردازش دارند. از آن‌جایی که مدل‌های شبکه عصبی پیچشی روی مجموعه‌های تصویر بهتر کار می‌کنند و مجموعه داده‌های ترافیک شبکه خودرویی معمولاً داده‌های جدولی هستند، در این پژوهش داده‌های اصلی شبکه به فرم‌های تصویر تبدیل شدند.

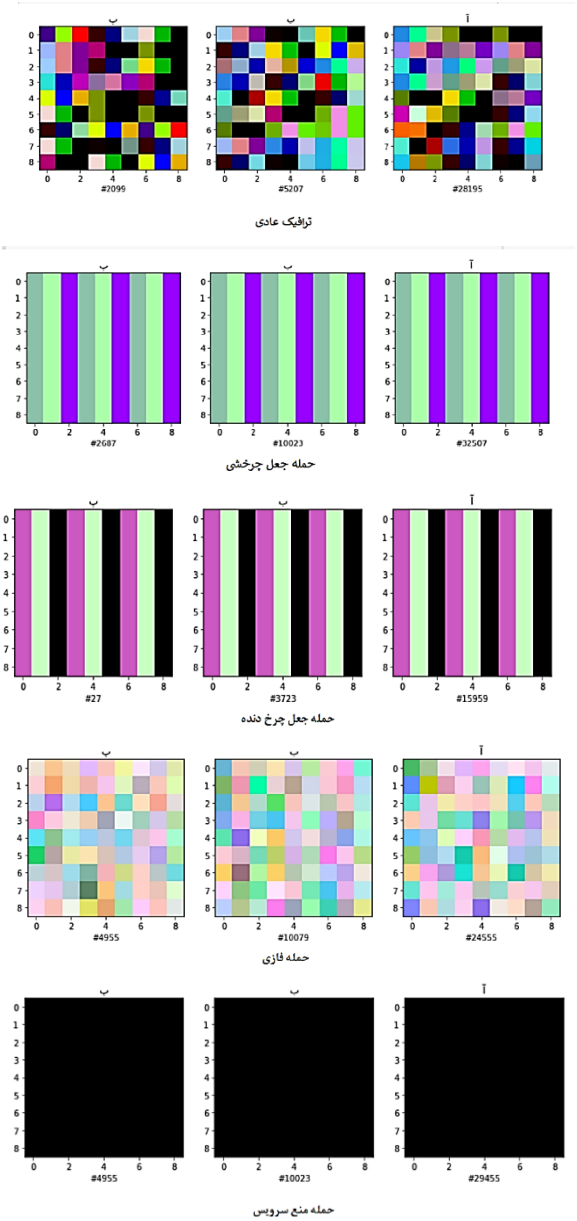
اگرچه شبکه عصبی پیچشی برای تجزیه‌وتحلیل تصویر با دقت بالا استفاده می‌شوند، داده‌های غیرتصویری در بسیاری از زمینه‌ها مانند بیوانفورماتیک، پزشکی، امور مالی و موارد دیگر رایج هستند که ممکن است این نوع شبکه عصبی مستقیماً برای آن‌ها قابل‌استفاده نباشد. برای داده‌های جدولی، ترتیب ویژگی‌ها را می‌توان در یک فضای دوبعدی بازآرایی کرد تا روابط بین ویژگی‌ها، مانند دسته‌های ویژگی یا شباهت‌ها را به‌وضوح نشان دهد. این موضوع انگیزه تبدیل داده‌های جدولی به تصاویر را ایجاد می‌کند [۱۳].

[1] Brute-Force

شبکه‌های عصبی پیچشی می‌توانند بر اساس این نوع داده آموزش داده شوند و بنابراین از روابط بین ویژگی‌ها برای بهبود عملکرد پیش‌بینی (در مقایسه با مدل‌های دیگری که بر روی داده‌های جدولی استفاده کنند) استفاده کنند. بنابراین روش ما از تبدیل داده‌های ویژگی به تصاویر به افزایش دقت طبقه‌بندی کمک می‌کند همچنین استفاده از یادگیری عمیق مبتنی بر تصویر، معمولاً به حافظه و زمان کمتری برای آموزش مدل نیاز دارد [۱۴].

فرآیند تبدیل داده‌ها با نرمال‌سازی داده‌ها شروع می‌شود. از آن‌جایی که مقادیر پیکسل تصاویر از ۰ تا ۲۵۵ متغیر است، داده‌های شبکه نیز باید به حالت نرمال و در مقیاس ۰–۲۵۵ تبدیل شوند. در میان تکنیک‌های نرمال‌سازی، حداکثر–حداقل[1] و نرمال‌سازی چندک[2] دو روش رایج مورداستفاده هستند. با توجه به این‌که نرمال‌سازی حداکثر–حداقل به‌خوبی با اقلام پرت برخورد نمی‌کند و ممکن است باعث شود که اکثر نمونه‌های داده مقادیر بسیار کمی داشته باشند، نرمال‌سازی چندک در چارچوب پیشنهادی استفاده می‌شود. روش نرمال‌سازی چندک مجموعه ویژگی‌ها را به یک توزیع نرمال تبدیل می‌کند و سپس، همه مقادیر ویژگی‌ها را بر اساس توزیع نرمال دوباره محاسبه می‌کند.

بنابراین، اکثر مقادیر نزدیک به مقادیرمیانه هستند که در مدیریت مقادیر پرت مؤثر است. پس از نرمال‌سازی داده‌ها، نمونه‌های داده بر اساس برچسب زمانی و همچنین اندازه ترافیک شبکه به تکه‌هایی تبدیل می‌شوند. مجموعه داده هک خودرو دارای ۹ ویژگی از هر تکه از ۲۷ نمونه متوالی با ۹ ویژگی (۲۷×۹ = ۲۴۳ مقدار ویژگی درمجموع) تبدیل می‌شود. بنابراین، تصویر حاصل به‌صورت ۳×۹×۹ خواهد بود. بنابراین، هر تصویر تبدیل‌شده یک تصویر رنگی مربع با سه کانال (قرمز، سبز و آبی) است. به‌طور مشابه، مجموعه داده CICIDS2017 با ۲۰ ویژگی مهم تولیدشده از [۴] به تصاویر رنگی ۳×۲۰×۲۰ تبدیل می‌شود، بنابراین هر تکه از این مجموعه داده شامل ۳×۲۰ = ۶۰ نمونه داده متوالی است. با توجه به این‌که تصاویر بر اساس مُهرهای زمانی نمونه‌های داده تولید می‌شوند، می‌توان همبستگی‌های سری زمانی داده‌های اصلی شبکه را حفظ کرد. شکل ۲ نمونه‌ای از تصاویر تولیدشده را نشان می‌دهد.



شکل (۲): تبدیل داده‌ها به فرمت تصویر

در مرحله بعد، تصاویر تبدیل‌شده از دو مجموعه داده هک خودرو و CICIDS2017 برچسب‌گذاری می‌شوند. در الگوهای حمله در تکه‌های داده اگر همه نمونه‌های موجود در یک قطعه/تصویر نمونه‌های معمولی باشند، این تصویر دارای برچسب «عادی» است.

[1] Min-Max

[2] Quantile Normalization

از سوی دیگر، اگر یک قطعه/تصویر حاوی نمونه‌های حمله باشد، این تصویر به‌عنوان متداول‌ترین نوع حمله در این قطعه برچسب‌گذاری می‌شود. به‌عنوان‌مثال، اگر یک حمله منع سرویس در قسمتی با بیشترین نسبت رخ دهد، تصویر مربوطه با عنوان «حمله منع سرویس» شناخته می‌شود. پس از مراحل پیش‌پردازش داده‌های فوق، مجموعه تصویر تبدیل‌شده نهایی به‌عنوان ورودی مدل‌های شبکه عصبی پیچشی تولید می‌شود. نمونه‌های نماینده برای هر نوع حمله درمجموعه داده هک خودرو در شکل ۲ نشان داده‌شده است. همان‌طورکه در شکل مشاهده می‌کنید الگوهای تصاویر حمله فازی تصادفی‌ترازتصاویرعادی هستند، درحالی‌که نمونه‌های حمله منع سرویس چون دارای پیام‌های خالی با فرکانس بالا هستند، باعث ایجاد الگوهای سیاه خالص می‌شوند. حملات جعل داده با تزریق پیام‌هایی با شناسه‌ها و بسته‌های خاص برای معرفی به‌عنوان کاربران قانونی راه‌اندازی می‌شوند، بنابراین تصاویر آن‌ها نیز دارای الگوهای ویژگی خاصی هستند [۱۰].

۳-۳ آموزش شبکه عصبی

شبکه عصبی پیچشی یک مدل شبکه عصبی عمیق است که به‌طور گسترده در طبقه‌بندی و تشخیص تصویر استفاده می‌شود. تصاویر را می‌توان مستقیماً در مدل‌های شبکه عصبی پیچشی بدون فرآیندهای استخراج ویژگی‌های اضافی و بازسازی داده‌ها به‌عنوان ورودی استفاده کرد. یک شبکه عصبی پیچشی معمولی شامل سه نوع لایه است: لایه‌های کانولوشن، لایه‌های ادغام و لایه‌های کاملاً متصل [۱۵]. در لایه‌های کانولوشن، الگوهای ویژگی تصاویر را می‌توان به‌طور خودکار توسط عملیات کانولوشن استخراج کرد. در لایه‌های ادغام، پیچیدگی داده‌ها را می‌توان بدون از دست دادن اطلاعات مهم از طریق همبستگی‌های محلی کاهش داد تا از برازش بیش‌ازحد جلوگیری شود. لایه‌های کاملاً متصل به‌عنوان رابط نهایی برای اتصال همه ویژگی‌ها و تولید خروجی عمل می‌کنند. در چارچوب پیشنهادی، ما VGG16، VGG19، Xception، Inception و InceptionResnet را به‌عنوان مدل‌های پایه شبکه عصبی پیچشی انتخاب کرده‌ایم که دلیل آن موفقیت آن‌ها در اکثر مسئله‌های طبقه‌بندی تصویر است [۹]. این مدل‌های شبکه عصبی پیچشی از قبل بر روی مجموعه داده ImageNet آموزش دیده‌اند و عملکرد فوق‌العاده‌ای را در وظایف طبقه‌بندی تصویر نشان داده‌اند. مجموعه داده ImageNet یک مجموعه داده استاندارد برای پردازش تصویر است که بیش از یک میلیون تصویر از ۱۰۰۰ کلاس مختلف دارد [۱۶]. پس از یادگیری برای آموزش پنج مدل پیشرفته شبکه عصبی پیچشی درمجموعه داده‌های شبکه خودرو، سه مدل برتر شبکه عصبی پیچشی با بهترین عملکرد به‌عنوان یادگیرندگان پایه برای ساخت مجموعه مدل‌های مورداستفاده در یادگیری گروهی انتخاب شدند.

۴-۳ مدل پیشنهادی یادگیری گروهی

یادگیری گروهی تکنیکی است که چندین مدل یادگیری پایه را برای ساخت یک مدل گروهی با عملکرد بهبودیافته ادغام می‌کند. یادگیری گروهی به‌طور گسترده‌ای در مسائل تجزیه‌وتحلیل داده‌ها استفاده می‌شود. زیرا مجموعه‌ای از چند یادگیرنده، معمولاً بهتر از یادگیرندگان تکی عمل می‌کند [۱۷].

در یادگیری گروهی، چند الگوریتم یادگیری در کنار یکدیگر به‌کار گرفته می‌شود تا نتیجه حاصل دقیق‌تر از محاسبه الگوریتم‌ها به‌صورت مستقل باشد. دقت و جامعیت روش یادگیری جمعی دلایل متعددی دارد.

در یادگیری گروهی، با تشکیل یک مجمع از چندین فرضیه گوناگون و میانگین‌گیری از پیش‌بینی‌های آن‌ها، می‌توان احتمال انتخاب رده‌بند نادرست را کاهش داد [۱۸].

یکی از شناخته‌شده‌ترین الگوریتم‌های یادگیری گروهی، الگوریتم جنگل تصادفی است. روش کار این الگوریتم برای تولید یک مدل رده‌بندی بدین‌صورت است که نخست بخش‌هایی از داده‌های آموزشی به‌صورت تصادفی انتخاب‌شده و بر اساس هرکدام یک درختی تصمیم‌گیری ساخته می‌شود. سپس، با تشکیل مجمعی از درخت‌های تصمیم‌گیری و میانگین‌گیری از خروجی آن‌ها، می‌توان به‌دقتی فراتر از دقت هر یک از درخت‌های تصمیم‌گیری به‌صورت جداگانه دست پیدا کرد [۱۹].

همان‌طور که بیان شد، میانگین‌گیری یک رویکرد یادگیری گروهی است که مقادیر احتمالی طبقه‌بندی در یادگیرندگان پایه را برای یافتن کلاسی با بالاترین ارزش اطمینان ترکیب می‌کند. در مدل‌های یادگیری عمیق، لایه‌های softmax می‌توانند یک لیست احتمالات

را که حاوی اطمینان طبقه‌بندی هر کلاس است، تولید کنند. روش میانگین‌گیری، میانگین احتمالی طبقه‌بندی یادگیرندگان پایه را برای هر کلاس محاسبه می‌کند و سپس، برچسب کلاس با بالاترین میانگین به‌عنوان نتیجه طبقه‌بندی نهایی برمی‌گرداند. مقدار میانگین هر کلاس با استفاده از تابع softmax محاسبه می‌شود:

$$Softmax(z)_i = \frac{e^{z_i}}{\sum_{j=1}^{C} e^{z_j}} \quad (۱)$$

در رابطه (۱)، z بردار ورودی، C تعداد کلاس‌های مجموعه داده، ezi و ezj به‌ترتیب توابع نمایی استاندارد برای بردارهای ورودی و خروجی هستند. برچسب کلاس پیش‌بینی‌شده به‌دست‌آمده با روش میانگین‌گیری را می‌توان با تابع زیر نشان داد:

$$\hat{y} = \text{argmax}_{i\epsilon\{1,\dots,c\}} \frac{\sum_{j=1}^{k} p_j(y = i|B_j, x)}{k} \quad (۲)$$

در رابطه (۲)، Bj j اُمین یادگیرنده پایه است، k تعداد یادگیرندگان پایه انتخاب‌شده (در چارچوب پیشنهادی k = 3 است) و Pj مقدار پیش‌بینی یک کلاس i را در نمونه داده x با استفاده از Bj را نشان می‌دهد. برخلاف روش رأی‌گیری مرسوم که فقط برچسب‌های کلاس را در نظر می‌گیرد، میانگین‌گیری از مجموعه مدل‌ها، یادگیری گروهی را قادر می‌سازد تا نتایج طبقه‌بندی نامشخص را تشخیص دهد و نمونه‌های طبقه‌بندی‌شده اشتباه را از طریق استفاده از میانگین طبقه‌بندی تصحیح کند.

```
Algorithm CNN-based IDS framework
Input: (CAN Bus Data, External Network Data) as a set of time-based data chunks S
Output: Type of Attack or normal T
1: ImageSet ← DataTransformation (S){
2:     S1 ← QuantileTransform(S);
3:     S2 ← ImageGeneration (S1);
4:     return (DataLabeling(S2))
5:     }
6: do in Parallel
7:     X1 ← VGG16(ImageSet);
8:     X2← VGG19(ImageSet);
9:     X3← Xception(ImageSet);
10:    X4 ← Inception(ImageSet);
11:    X5 ← InceptionResnet(ImageSet);
12: M = (M1, M2, M3) ← Select top three Performing Models from X1 .. X5;
13: L ← Generate confidence list from M;
14: M' ← ConfidenceAverageModel(L);
15: T ← ComputeTypeOfAttack(M');
```

شکل (۳): شبه کد روش پیشنهادی

٤- بحث و نتایج

در این بخش، مدل پیشنهادی اساس معیارهایی که در قسمت اول همین بخش معرفی می‌شوند با یکدیگر مقایسه می‌شوند.

٤-١ معیارهای ارزیابی نتایج

برای هر کلاس موجود، مدل‌ها می‌توانند مقدار ۱ یا ۰ (مثبت یا منفی) را بازگردانی کنند که به ترتیب نمایانگر تعلق یا عدم تعلق تصویر ورودی به آن کلاس است.

- **دقت**

این معیار مشخص می‌کند که چند درصد از مقادیر ۱ بازگردانی‌شده توسط مدل برای هر کلاس، تعلق تصویر برچسب‌دار به آن کلاس را به‌درستی نشان می‌دادند (یا به بیانی دیگر، چند درصد از ۱ ها را می‌توان تشخیص درستی به شمار بُرد).

$$P = \frac{\text{مثبت صحیح}}{\text{مثبت کاذب} + \text{مثبت صحیح}} = \frac{\text{هرآنچه به درستی مثبت تشخیص داده‌شده}}{\text{تمامی تشخیص‌های مثبت}} \quad (۳)$$

- **امتیاز F**

به‌عنوان شاخصی جهت سنجش صحت (accuracy) به کار می‌رود. امتیاز F1 به شیوه زیر محاسبه می‌شود:

$$F_1 = \frac{2.P.R}{P+R} \quad (٤)$$

معیار F1 نوعی میانگین هارمونیک بوده که به‌طورمعمول (و همچنین در تمامی مقالات بررسی‌شده در این پژوهش) برای سنجش صحبت رده‌بندهای دودویی مورداستفاده قرارگرفته است.

٤-٢ پیاده‌سازی

آزمایش‌ها با استفاده از کتابخانه‌های Scikit-learn و Keras در پایتون انجام‌شده است. در آزمایش‌ها، مدل‌های یادگیری عمیق پیشنهادی بر روی یک دستگاه کامپیوتر با پردازنده i7-8700 و حافظه ١٦ گیگابایتی آموزش دیدند و روی دستگاه Raspberry Pi 3 با پردازنده ٦٤ بیتی و ۱ گیگابایت حافظه آزمایش شدند که به‌ترتیب نشان‌دهنده یک دستگاه سرور مرکزی و یک دستگاه محلی در سطح خودرو است. چارچوب پیشنهادی بر روی دو مجموعه داده امنیتی شبکه وسیله نقلیه معیار، Car-Hacking [۱۳] و CICIDS2017 [١٤]، همان‌طور که در بخش‌های قبل توضیح داده‌شده است، ارزیابی گردید. با توجه به این‌که داده‌های ترافیک شبکه معمولاً داده‌های نامتعادلی هستند که تنها درصد کمی از نمونه‌های حمله را دارند، از چهار معیار مختلف شامل دقت،

صحت، یادآور و امتیازات F1 برای ارزیابی عملکرد استفاده شده است. علاوه بر این، برای ارزیابی کارایی روش پیشنهادی، زمان آموزش مدل در ماشین سطح سرور و زمان آزمون مدل بر روی ماشین سطح خودرو نیز پایش و مقایسه گردید.

٤-٣ نتایج

جدول ۱ نتایج ارزیابی عملکرد مدل‌ها درمجموعه داده‌های Car-Haking را نشان می‌دهد. نتایج ارزیابی مدل‌های شبکه عصبی پیچشی بهینه‌سازی شده و مدل‌های مجموعه پیشنهادی درمجموعه داده‌های Car-Haking و CICIDS2017 به‌ترتیب در جداول ۱ و ۲ نشان داده‌شده‌اند.

جدول (۱): نتایج مجموعه داده Car-Hacking

نام روش	زمان آزمون هر بسته (ms)	F1	دقت
شبکه عصبی انتقال‌دهنده [۱]	**	۹۷/۸۳	۹۸/۱
یادگیری گروهی میانگین (روش پیشنهادی)	٤	۱۰۰	۱۰۰

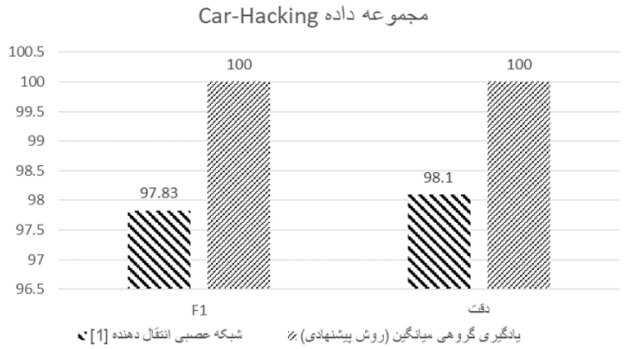
همان‌طور که در جدول ۱ نشان داده‌شده است، مدل بهینه‌سازی شده یادگیری گروهی براساس شبکه عصبی پیچشی به‌دقت ۱۰۰٪ و امتیازات F1 100 دست می‌یابد. این موضوع به این دلیل اتفاق افتاده است که الگوهای معمولی و حمله درمجموعه داده هک خودرو را می‌توان به‌وضوح از طریق تصاویر تبدیل‌شده نشان داده‌شده در شکل ۲ تشخیص داد.

جدول (۲): نتایج مجموعه داده CICIDS2017

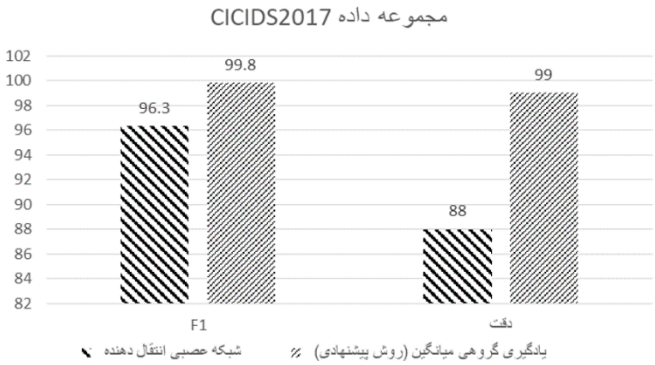
نام روش	زمان آزمون هر بسته (ms)	F1	دقت
شبکه عصبی انتقال‌دهنده [۱]	**	۹٦/۳	۸۸
یادگیری گروهی میانگین (روش پیشنهادی)	۷۵	۹۹/۹۳	۹۹

همان‌طور که در جدول ۲ نشان داده‌شده است، برای مجموعه داده CICIDS2017، مدل‌های بهینه‌سازی شده پایه شبکه عصبی پیچشی پس از اجرای تبدیل داده‌ها، روش میانگین‌گیری پیشنهادی به امتیاز F1 برابر با ۹۹/۹۲۵٪ می‌رسد. دو مدل مجموعه همچنین از سایر روش‌های اخیر در ادبیات [٤، ١٤] بهتر عمل می‌کنند.

شکل ٤ و شکل ۵، عملکرد بالاتر مدل‌های پیشنهادی در مقایسه با سایر سیستم تشخیص نفوذهای پیشرفته نشان می‌دهد و دلایل استفاده از تکنیک‌های شبکه عصبی پیچشی را توجیه می‌کند. علاوه بر این همان‌طور که در جداول ۱ و ۲ نشان داده‌شده است، میانگین زمان آزمایش/پیش‌بینی مدل‌های مجموعه پیشنهادی برای هر بسته در دستگاه رزبری پای در سطح پایینی است. با توجه به این‌که نیاز بلادرنگ سیستم‌های تشخیص ناهنجاری وسیله نقلیه معمولاً ۱۰ میلی‌ثانیه برای تجزیه‌وتحلیل هر بسته [۲۰] است، زمان پیش‌بینی پایین مدل پیشنهادی امکان‌پذیری اعمال سیستم تشخیص نفوذ پیشنهادی در سیستم‌های خودرو خودران بلادرنگ را نشان می‌دهد.



شکل (٤): نتایج بر روی مجموعه داده Car-Hacking



شکل (۵): نتایج بر روی مجموعه داد CICIDS2017

۵- نوآوری‌های پژوهش

این پژوهش یک سیستم تشخیص نفوذ (IDS) مبتنی بر یادگیری عمیق برای شبکه‌های خودرویی ارائه می‌دهد که در مقایسه با مطالعات قبلی دارای ویژگی‌های متمایزی است. مهم‌ترین نوآوری‌های این پژوهش عبارت‌اند از:

۱- تبدیل داده‌های شبکه به تصاویر برای استفاده در شبکه‌های عصبی پیچشی: برخلاف روش‌های سنتی که مستقیماً از داده‌های جدولی برای تشخیص نفوذ استفاده می‌کنند، در این پژوهش داده‌های شبکه به تصاویر تبدیل‌شده‌اند تا شبکه‌های پیچشی بتوانند بهتر الگوهای حمله را شناسایی کنند. این روش امکان استخراج ویژگی‌های مکانی و زمانی را به‌طور هم‌زمان فراهم می‌کند و به مدل اجازه می‌دهد روابط پیچیده بین داده‌های شبکه را درک کند.

۲- استفاده از یادگیری گروهی (Ensemble Learning) برای بهینه‌سازی دقت تشخیص: در این پژوهش، از چندین مدل پیشرفته شبکه عصبی پیچشی (مانند VGG16، VGG19، Xception، Inception و InceptionResnet) استفاده شده و نتایج آن‌ها با روش میانگین‌گیری ترکیب‌شده است. این رویکرد به بهبود دقت سیستم تشخیص نفوذ کمک کرده و دقت ۹۹/۹۳٪ و امتیاز F1 برابر با ۹۹/۹۲۵٪ را درمجموعه داده‌های استاندارد نشان داده است.

۳- بررسی قابلیت اجرای روش در تجهیزات کم‌مصرف اینترنت اشیاء: برخلاف مطالعات قبلی که عمدتاً روی سرورهای پردازشی قوی اجراشده‌اند، روش پیشنهادی روی Raspberry نیز پیاده‌سازی و ارزیابی‌شده است. این ارزیابی نشان داده که زمان پیش‌بینی مدل در سطحی است که امکان استفاده در سیستم‌های بلادرنگ خودروهای خودران را دارد.

٤- ارزیابی سیستم پیشنهادی بر روی دو مجموعه داده معتبر و مقایسه با جدیدترین کارهای مرتبط: عملکرد روش پیشنهادی بر روی مجموعه داده‌های Car-Hacking و CICIDS2017 ارزیابی‌شده است که هر دو از پایگاه‌های معتبر امنیت شبکه محسوب می‌شوند.

٦- نتیجه‌گیری

برای محافظت از وسایل نقلیه متصل در برابر نفوذ حملات سایبری، در این مقاله یک چارچوب یادگیری مبتنی بر سیستم تشخیص نفوذ پیشنهادشده است که از مدل‌های شبکه عصبی پیچشی بهینه‌سازی شده برای شناسایی انواع مختلف حملات در سیستم‌های خودرو خودران استفاده می‌کند. علاوه بر این، یک روش تبدیل داده مبتنی بر تکه برای تبدیل داده‌های ترافیک شبکه خودرو به داده‌های تصویری که به‌عنوان ورودی مدل‌های شبکه عصبی پیچشی استفاده می‌شود، پیشنهادشده است. سیستم تشخیص نفوذ پیشنهادی بر روی مجموعه داده‌های Car-Haking و CICIDS2017 ارزیابی می‌شود که به‌ترتیب داده‌های شبکه درون خودرو و داده‌های خارجی را نشان می‌دهند. نتایج تجربی نشان می‌دهد که چارچوب سیستم تشخیص نفوذ پیشنهادی می‌تواند به‌طور مؤثر انواع مختلف حملات را با امتیازات F1 ۱۰۰% و ۹۹/۹۲۵٪ نسبت به سایر روش‌های پیشرفته در مقایسه با مجموعه داده‌های استاندارد شناسایی کند. علاوه بر این، نتایج آزمایش مدل بر روی یک ماشین در سطح خودرو امکان‌سنجی سیستم تشخیص نفوذ پیشنهادی را در شبکه‌های خودروی بلادرنگ نشان می‌دهد. در کارهای آینده، این چارچوب برای توسعه یک مدل تطبیقی برخط که می‌تواند به یادگیری برخط دست یابد، گسترش خواهد یافت

References

[1] S. T. Mehedi, A. Anwar, Z. Rahman, and K. Ahmed, “Deep transfer learning based intrusion detection system for electric vehicular networks,” Sensors, vol. 21, no. 14, pp. 1–23, 2021, doi: 10.3390/s21144736.

[2] Ramezanzadeh, M. Barzegar, and H. Motameni, “Automatic Security Assessment of Petri Nets-Based Threat Routes,” Electronic and Cyber Defense, vol. 9, no. 4, pp. 87–98, 2022. [In Persian].

[3] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, “Tree-based intelligent intrusion detection system in internet of vehicles,” 2019 IEEE Glob. Commun. Conf. GLOBECOM 2019 - Proc., no. October, 2019, doi: 10.1109/GLOBECOM38437.2019.9013892.

[4] L. Yang, A. Moubayed, and A. Shami, “MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles,” IEEE Internet Things J., vol. 9, no. 1, pp. 616–632, 2022, doi: 10.1109/JIOT.2021.3084796.

[5] Rosay, F. Carlier, and P. Leroux, “Feed-forward neural network for Network Intrusion Detection,” IEEE Veh. Technol. Conf., vol. 2020-May, 2020, doi: 10.1109/VTC2020-Spring48590.2020.9129472.

[6] H. M. Song, J. Woo, and H. K. Kim, “In-vehicle network intrusion detection using deep convolutional neural network,” Veh. Commun.,

vol. 21, p. 100198, 2020, doi: 10.1016/j.vehcom.2019.100198.
[7] L. Yang, D. M. Manias, and A. Shami, “PWPAE: An Ensemble Framework for Concept Drift Adaptation in IoT Data Streams,” 2021 IEEE Glob. Commun. Conf. GLOBECOM 2021 - Proc., no. September, 2021, doi: 10.1109/GLOBECOM46510.2021.9685338.
[8] E. Seo, H. M. Song, and H. K. Kim, “GIDS: GAN based Intrusion Detection System for In-Vehicle Network,” 2018 16th Annu. Conf. Privacy, Secur. Trust. PST 2018, pp. 0–5, 2018, doi: 10.1109/PST.2018.8514157.
[9] Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secur. Priv., vol. 2018-Janua, no. Cic, pp. 108–116, 2018, doi: 10.5220/0006639801080116.
[10] F. Aloraini, A. Javed, and O. Rana, "Adversarial attacks on intrusion detection systems in in-vehicle networks of connected and autonomous vehicles," Sensors, vol. 24, no. 12, p. 3848, 2024. doi: 10.3390/s24123848.
[11] S. Firasta, Y. R. Srivastava and V. Rao, "Cognitive Detection of Anomalies in Autonomous In-Vehicle Network Communication," 2024 International Conference on Advancements in Power, Communication and Intelligent Systems (APCI), KANNUR, India, 2024, pp. 1-6, doi: 10.1109/APCI61480.2024.10617212.
[12] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, “LSTM-based intrusion detection system for in-vehicle can bus communications,” IEEE Access, vol. 8, pp. 185489–185502, 2020, doi: 10.1109/ACCESS.2020.3029307.
[13] Y. Zhu et al., “Converting tabular data into images for deep learning with convolutional neural networks,” Sci. Rep., vol. 11, no. 1, pp. 1–12, 2021 doi: 10.1038/s41598-021-90923-y.
[14] Rahali, A. H. Lashkari, G. Kaur, L. Taheri, F. Gagnon, and F. Massicotte, “DIDroid: Android malware classification and characterization using deep image learning,” ACM Int. Conf. Proceeding Ser., pp. 70–82, 2020, doi: 10.1145/3442520.3442522.
[15] T. H. De Huang and H. Y. Kao, “R2-D2: ColoR-inspired Convolutional NeuRal Network (CNN)-based AndroiD Malware Detections,” in Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018, Jan. 2019, pp. 2633–2642, doi: 10.1109/BigData.2018.8622324.
[16] Bruna and S. Mallat, “Invariant scattering convolution networks,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 35, no. 8, pp. 1872–1886, 2013, doi: 10.1109/TPAMI.2012.230.
[17] Q. Sun and B. Pfahringer, “Bagging ensemble selection,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7106 LNAI, pp. 251–260, 2011, doi: 10.1007/978-3-642-25832-9_26.
[18] Tanha, Y. Abdi, N. Samadi, N. Razzaghi, and M. Asadpour, “Boosting methods for multi-class imbalanced data classification: an experimental review,” J. Big Data, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00349-y.
[19] R. E. Schapire, "The boosting approach to machine learning: an overview," in Nonlinear Estimation and Classification, D. D. Denison, M. H. Hansen, C. C. Holmes, B. Mallick, and B. Yu, Eds. New York, NY: Springer, 2003, vol. 171, pp. 1-14. doi: 10.1007/978-0-387-21579-2_9.
[20] Moubayed, A. Shami, P. Heidari, A. Larabi, and R. Brunner, “Edge-Enabled V2X Service Placement for Intelligent Transportation Systems,” IEEE Trans. Mob. Comput., vol. 20, no. 4, pp. 1380–1392, 2021, doi: 10.1109/TMC.2020.2965929.

Journal of Applied And Basic Machine Intelligence Research (ABMIR)

Applied and Basic Machine Intelligence Research

Vol. 2, No. 2, Autumn & Winter 2024, pp. 83 - 93

Network Attacks Detection in Autonomous Vehicles using Deep Nerul Network

Abbas Horri*, Leila Samimi-Dehkordi

Assistant Professor, Department of Computer Engineering, Faculty of Engineering, Shahrekord University, Shahrekord Iran

Article Information

Original Research Paper

Received:
2024 December 9

Accepted:
2025 February 27

Keywords:
Self-driving, Intrusion detection, Deep Learning, IoT

Corresponding Author*:
horri@sku.ac.ir

Abstract

Modern vehicles, including autonomous vehicles and connected vehicles, are increasingly connected to their external environment, thereby providing various functions and services. Increasing connectivity has increased cyber attacks on self-driving vehicles and, as a result, has made these devices vulnerable to cyber threats. Due to the weakness or absence of authentication and encryption procedures in car networks, the use of intrusion detection systems is one of the necessary methods to protect the modern car system against cyber attacks. In this paper, an intrusion detection system based on deep learning using image recognition for vehicle systems is proposed. Also, the technique of converting feature vectors into images has been used to optimize detection. The proposed intrusion detection system is optimized using average-based ensemble learning technique. In experiments, the proposed method has shown more than 99.25% detection rate and the same amount of F1 criterion in two standard security datasets including Car-Hacking dataset and CICIDS2017 dataset. Therefore, the proposed method is effective for detecting cyber attacks in vehicular networks. Also, the execution time of the method has been measured on the Internet of Things equipment, which shows the feasibility of the proposed method.

: 10.22034/ABMIR.2025.22510.1083

E-ISSN: 2821-2037