استفاده از طبقه بندی برای افزایش دقت سیستم تشخیص نفوذ در شبکه اینترنت اشیاء خودرویی

مهدی رضائی [1]، دکتر علیرضا تقی زاده [2]

1- دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد پرند – mrp.1052@gmail.com

2- دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد پرند – Alireza.taghizadeh@iau.ac.ir

زمینه و هدف: وسایل نقلیه مدرن امروزی، شامل وسایل نقلیه متصل و خودران(AVs) ، به‌طور گسترده از سیستم‌های کنترل الکترونیکی استفاده می‌کنند که از طریق شبکه‌های داخلی خودرو متصل شده و عملکردهای مختلفی را اجرا می‌کنند. این وسایل نقلیه همچنین از فناوری‌های Vehicle-to-Everything (V2X) بهره می‌برند که ارتباط بین وسایل نقلیه، زیرساخت‌ها و دستگاه‌های هوشمند را تسهیل می‌کند. با این حال، این اتصالات به‌ویژه در برابر حملات سایبری آسیب‌پذیر هستند. حملات به شبکه‌های داخل خودرو و شبکه‌های خارجی می‌توانند بر عملکرد و ایمنی وسایل نقلیه تأثیر بگذارند. هدف این تحقیق، شناسایی و مقابله با تهدیدات سایبری در سیستم‌های حمل و نقل هوشمند از طریق توسعه یک سیستم تشخیص نفوذ (IDS) مبتنی بر یادگیری ماشینی است.

روش: در این تحقیق، یک سیستم تشخیص نفوذ ترکیبی مبتنی بر امضا و ناهنجاری برای شناسایی حملات سایبری در شبکه‌های داخل خودرو و شبکه‌های خارجی پیشنهاد شده است. این سیستم به‌طور خاص برای شناسایی حملات سایبری شناخته‌شده و ناشناخته طراحی شده است. به‌منظور ارزیابی عملکرد سیستم، از دو مجموعه داده مختلف شامل داده‌های شبکه‌های CAN-intrusion و CICIDS2017 استفاده شده است. این داده‌ها شامل اطلاعات مربوط به حملات سایبری مختلف در شبکه‌های خودرو می‌باشند.

یافته‌ها: نتایج تجربی نشان می‌دهند که سیستم پیشنهادی می‌تواند انواع مختلفی از حملات سایبری شناخته‌شده را با دقت بالای 99 درصد شناسایی کند. این سیستم به‌ویژه در شناسایی حملات در شبکه‌های داخلی خودرو و همچنین در شبکه‌های خارجی، عملکرد بسیار خوبی از خود نشان داده است. این دقت بالا نشان‌دهنده توانمندی سیستم در شناسایی دقیق تهدیدات سایبری و افزایش ایمنی و کارایی سیستم‌های حمل و نقل هوشمند است.

نتیجه‌گیری: سیستم تشخیص نفوذ مبتنی بر امضا و ناهنجاری که در این تحقیق پیشنهاد شده است، می‌تواند به‌طور مؤثری حملات سایبری را در شبکه‌های خودرو شناسایی کند. با توجه به دقت بالای سیستم در شناسایی حملات شناخته‌شده و ناشناخته، این سیستم می‌تواند به‌عنوان یک ابزار قدرتمند برای ایمن‌سازی شبکه‌های داخل خودرو و شبکه‌های خارجی استفاده شود. این تحقیق نشان می‌دهد که استفاده از روش‌های یادگیری ماشینی برای تشخیص حملات سایبری در سیستم‌های حمل و نقل هوشمند می‌تواند به بهبود امنیت این سیستم‌ها کمک کند.

واژه‌های کلیدی: سیستم تشخیص نفوذ –طبقه بندی – انتخاب ویژگی – اینترنت خودرو

1. مقدمه

با سرعت رشد تکنولوژی و استفاده گسترده از دستگاه‌های جدید جهت برقراری ارتباط و همچنین متصل بودن تمامی دستگاه‌های شبکه به اینترنت، اینترنت اشیا به عنوان راه‌حلی مناسب برای تبدیل اشیاء معمولی

به اشیاء هوشمند از طریق اتصال آن‌ها به اینترنت مطرح شده است. اینترنت اشیا، که متشکل از تجهیزات هوشمند و شبکه‌های مرتبط با آن است، به دلیل تغییرات سریع و چشمگیر در فناوری و نیازهای ارتباطی، بسیار مورد توجه قرار گرفته است[1].

در حال حاضر، وسایل نقلیه روزانه توسط تعداد بیشتری از افراد استفاده می‌شوند که این امر منجر به افزایش ترافیک و تصادفات در جاده‌ها شده است. این مسئله به عنوان یکی از مشکلات اساسی در زندگی روزمره مطرح می‌شود. در طول دهه گذشته، شبکه‌های ad hoc خودرو (VANET) و شبکه‌های ad hoc موبایل (MANET)به عنوان شبکه‌هایی با کارایی بالا برای مدیریت این چالش‌ها شناخته شده‌اند .VANET از ارتباطات وسیله نقلیه به خودرو (V2V) و وسیله نقلیه به جاده (V2R) برای انتقال سیگنال‌ها بین وسایل نقلیه استفاده می‌کند و به این ترتیب، بهبود ارتباطات جاده‌ای را ممکن می‌سازد[2].

به منظور ارتقای قابلیت‌های VANET و کاهش ترافیک و تصادفات در جاده‌ها، اینترنت وسایل نقلیه (IoV) به عنوان بخشی از شبکه‌های اینترنت اشیا (IoT) شناسایی شده است IoV .به عنوان نسخه‌ای پیشرفته از اینترنت اشیا، برای حل مسائل مختلف در محیط ترافیک شهری به کار گرفته می‌شود. این فناوری نه تنها به بهبود سیستم‌های نظارت بر ترافیک کمک می‌کند، بلکه امکان ارائه برنامه‌های سفر و دسترسی به شبکه‌های اطلاعاتی برای رانندگان، مسافران و مدیران ترافیک را نیز فراهم می‌آورد. به عبارت دیگر، اینترنت وسایل نقلیه (IoV) به ایجاد یک اتصال متقابل بین فناوری‌های شبکه بی‌سیم و شبکه‌های جاده‌ای مختلف کمک می‌کند. این پیشرفت در سیستم حمل و نقل هوشمند (ITS) با هدف بهبود نظارت بر ترافیک، افزایش ایمنی جاده‌ها و ارتقای تجربه سفر مورد استفاده قرار می‌گیرد[3].در این راستا، هدف کلی از این تحقیق، بررسی و ارزیابی نقش اینترنت وسایل نقلیه (IoV) و شبکه‌های ad hoc خودرو (VANET) به عنوان بخشی از فناوری‌های نوین اینترنت اشیا (IoT) در بهبود سیستم‌های حمل و نقل هوشمند (ITS) است. این مطالعه به دنبال ارائه راهکارهایی برای کاهش ترافیک، پیشگیری از تصادفات جاده‌ای و بهینه‌سازی تجربه سفر از طریق ایجاد ارتباطات هوشمند بین وسایل نقلیه و زیرساخت‌های جاده‌ای است.در مجموع، توسعه و استفاده از IoV و VANETبه عنوان بخشی از تحولات نوین در اینترنت اشیا، نقشی کلیدی در افزایش کارایی سیستم‌های حمل و نقل هوشمند و کاهش چالش‌های مرتبط با ترافیک شهری ایفا می‌کند.

2. مبانی نظری و پیشینه پژوهش

با توجه به پیشرفت‌های سریع فناوری و نیاز روزافزون به بهبود ایمنی و کارایی در حمل‌ونقل، اینترنت وسایل نقلیه (IoV) به عنوان بخشی از سیستم‌های حمل‌ونقل هوشمند (ITS) و توسعه شبکه‌های ارتباطی بین خودروها، توجه بسیاری از پژوهشگران را به خود جلب کرده است. بررسی مفاهیم و تحقیقات مرتبط با این فناوری‌ها، مبنایی برای درک بهتر و استفاده بهینه از آن‌ها فراهم می‌کند.

2.1 چالش‌های امنیت، حریم خصوصی و اعتماد در شبکه‌های VANET

یکی از مسائل اساسی در شبکه‌های ad hoc خودرو(VANET)، تأمین امنیت ارتباطات در کانال‌های وسیله نقلیه به وسیله نقلیه (V2V) و وسیله نقلیه به زیرساخت (V2I) است. برای اطمینان از امنیت این کانال‌ها، ارائه خدماتی با کیفیت بالا از نظر دسترسی‌پذیری، محرمانه بودن، احراز هویت، تمامیت، و انکارناپذیری ضروری است[4]. این رویکردها برای مقابله با تهدیدات و حملات مشابه سایر حوزه‌های شبکه، مانند شبکه‌های ad

hoc موبایلی (MANET) و اینترنت، مورد استفاده قرار می‌گیرند.

در بخش حریم خصوصی، حفظ امنیت اطلاعات خودروها از اهمیت بالایی برخوردار است. حریم خصوصی به این معنا است که تنها افراد خاصی در شبکه VANET حق دسترسی و کنترل اطلاعات خودرو، از جمله هویت واقعی و موقعیت مکانی، را داشته باشند. برای حفظ حریم خصوصی، از روش‌های احراز هویت ناشناس استفاده می‌شود که بر اساس مکانیزم‌های رمزنگاری مختلفی مانند رمزنگاری متقارن، زیرساخت کلید عمومی، امضای هویت‌محور، امضای بدون مجوز، و امضای گروهی دسته‌بندی می‌شوند. با این حال، صرف احراز هویت ناشناس برای جلوگیری از ردیابی مسیر وسیله نقلیه توسط مهاجمان کافی نیست، حتی در صورتی که پیام‌های ارسالی به صورت کاملاً ناشناس باقی بمانند[5].

در نهایت، مدیریت اعتماد در شبکه‌های VANET مسئله‌ای حیاتی است که به این می‌پردازد که چگونه یک خودرو به سایر خودروها و پیام‌های دریافتی اعتماد می‌کند. سه مدل اصلی مدیریت اعتماد در این شبکه‌ها شامل مدل‌های اعتماد هویت‌محور، مدل‌های اعتماد داده‌محور، و مدل‌های اعتماد ترکیبی است. کارایی این مدل‌ها بر اساس ویژگی‌های مطلوب مدیریت اعتماد در شبکه‌های VANET مورد تحلیل قرار می‌گیرد تا اطمینان حاصل شود که ارتباطات بین خودروها از اعتبار و صحت برخوردار است

2.2 شبکه‌های موردی متحرک (MANET) و شبکه‌های خودرویی موردی(VANET)

شبکه‌های موردی متحرک (MANET) به شبکه‌های بی‌سیمی اشاره دارد که بدون نیاز به زیرساخت و به‌صورت خودپیکربندی عمل می‌کنند. در این شبکه‌ها، گره‌های متحرک (نظیر تلفن‌های همراه یا لپ‌تاپ‌ها) مستقیماً از طریق لینک‌های بی‌سیم با یکدیگر در ارتباط‌اند. گره‌های دورتر از طریق تقویت پیام توسط گره‌های واسط به یکدیگر متصل می‌شوند .MANET دارای توپولوژی پویا و متغیر است؛ چراکه هر گره هم‌زمان نقش مشارکت‌کننده و روتر شبکه را ایفا می‌کند[6].

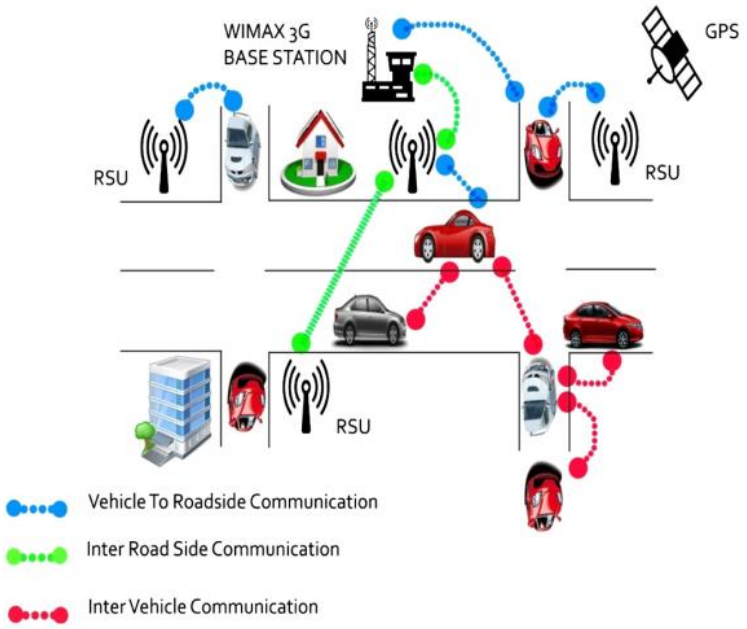
شبکه‌های خودرویی موردی (VANET) نوعی خاص از MANET هستند که در آن گره‌ها خودروها می‌باشند. با استفاده از این شبکه‌ها، خودروها قادرند با یکدیگر و با زیرساخت‌های جاده‌ای ارتباط برقرار کنند، که این امر می‌تواند منجر به افزایش ایمنی، کاهش ترافیک و بهبود خدمات مسیریابی شود. خودروها به‌صورت خودکار و بدون نیاز به ایستگاه مرکزی به یکدیگر متصل می‌شوند و داده‌ها را از طریق امواج رادیویی منتقل می‌کنند[7].

در شبکه‌هایVANET ، ارتباطات خودرو با خودرو (V2V) و خودرو با زیرساخت (V2I) به‌سرعت در حال توسعه هستند. این شبکه‌ها با استفاده از استانداردهایی نظیرWAVE ، انتقال اطلاعات بین خودروها و ایستگاه‌های کنار جاده را بهبود می‌بخشند. این ساختار توزیع‌شده امکان ایجاد ارتباطات چندهابی را فراهم می‌کند که به‌ویژه برای ارسال پیام‌های هشدار و اطلاعات اضطراری مفید است.

ویژگی اصلی شبکه‌های خودرویی، تحرک بالا و تغییر سریع توپولوژی است. این شبکه‌ها به خودروها امکان می‌دهند با استفاده از اطلاعات موقعیتی، ارتباطات چندهابی را برای انتقال داده‌های ایمنی و کاربردهای غیرایمنی بهینه‌سازی کنند. به‌عنوان‌مثال، خودروها می‌توانند هم‌زمان به چندین شبکه متصل شده و اطلاعات لازم را در مورد ترافیک یا تصادفات دریافت کنند[8].

کاربردهای شبکه‌های خودرویی شامل افزایش ایمنی، مدیریت ترافیک، سرویس‌های اطلاعاتی و سرگرمی، و بهبود تجربه رانندگی است. این شبکه‌ها با استفاده از تکنولوژی‌های بی‌سیم و دستگاه‌های تعبیه‌شده در خودرو، به ارتقای خدمات ارتباطی و امنیتی می‌پردازند .VANET با ارائه برنامه‌های امنیتی و

غیر امنیتی می‌تواند نقش مؤثری در بهبود رانندگی ایمن و کاهش تصادفات جاده‌ای داشته باشد[9].



شکل 1- ساختار شبکه خودرویی موردی

2.3 امنیت

عامل اصلی حاکم بر VANET ایجاد راحتی و امنیت برای رانندگان و مسافران است. لذا باید مکانیزم‌های امنیتی موثری توسعه یابند تا عملیات مطلوب VANET تضمین شود. خدمات امنیتی کلیدی شامل دسترسی‌پذیری، محرمانگی، احراز هویت، تمامیت داده و انکارناپذیری است. دسترسی‌پذیری تضمین می‌کند که شبکه و کاربردها، حتی در صورت وجود شرایط مخرب و خطا، عملیاتی باقی بمانند. حملات انکار سرویس (DOS)به این صورت انجام می‌شود که مهاجمان با جمینگ کانال ارتباطی یا اشغال غیرضروری منابع، دسترسی گره‌های مجاز را به خدمات محدود می‌کنند و در حالت توزیعی به حمله DOS توزیع شده (DDOS) تبدیل می‌شود. همچنین، حملات جمینگ باعث اختلال در کانال ارتباطی از طریق ارسال سیگنال‌های قوی می‌شود. بدافزارها نیز با نفوذ به سیستم‌های OBU و RSU عملکرد شبکه را مختل می‌کنند. حملات جعل پیام موجب ارسال پیام‌های هشدار جعلی توسط مهاجمان داخلی می‌شود که پیام‌های امنیتی واقعی را از دسترس خودروهای مجاز خارج می‌کند. حملات سیاهچاله و چاله خاکستری، بسته‌های انتقالی را رها می‌کنند و تشخیص حملات چاله خاکستری دشوارتر است زیرا ابتدا مهاجم به طور عادی عمل می‌کند و سپس بسته‌ها را بدون هدف خاصی رها می‌کند[10].

رفتار حریصانه توسط خودروهای خرابکار انجام می‌شود که با استفاده از پروتکلMAC ، پهنای باند بیشتری به ضرر سایر خودروها به دست می‌آورند. در حملات اسپمینگ، مهاجم تعداد زیادی پیام اسپم به سیستم VANET تزریق می‌کند که منجر به اشغال پهنای باند و احتمال تصادفات می‌شود. محرمانگی تضمین می‌کند که تنها گیرنده خاص قادر به دسترسی به داده‌ها باشد و دیگران نتوانند به اطلاعات دسترسی یابند. این امر معمولاً با استفاده از روش‌های رمزنگاری حاصل می‌شود. حملات استراق سمع با هدف استخراج

اطلاعات محرمانه انجام می‌شوند. حملات تحلیل ترافیک نیز تلاش می‌کنند تا از طریق گوش دادن به ارسال پیام‌ها، اطلاعات محرمانه به دست آورند[11].

احراز هویت در VANET مکانیزمی برای محافظت از شبکه در برابر مولفه‌های خرابکار است و اولین خط دفاع در برابر حملات محسوب می‌شود. حمله سیبیل شامل ایجاد هویت‌های جعلی توسط مهاجمان برای اخلال در عملکرد شبکه است. در حمله تونل‌زنی، دو بخش دوردست از طریق تونل به هم متصل می‌شوند تا گره‌های دوردست به عنوان گره‌های مجاور به اشتباه شناسایی شوند. اسپوفینگ GPS نیز شامل ارسال سیگنال‌های جعلی برای فریب خودروها است. حمله سواری رایگان در احراز هویت مشارکتی رخ می‌دهد، زمانی که خودروهای خودخواه از دیگران استفاده می‌کنند بدون اینکه خودشان نقشی در کمک به شبکه داشته باشند[12].

تمامیت داده‌ها تضمین می‌کند که محتوای پیام‌ها در طول ارسال تغییر نمی‌کند و از دستکاری غیرمجاز جلوگیری می‌شود. مهاجمان ممکن است پیام‌ها را ایجاد، دستکاری یا حذف کنند تا اطلاعات غلطی را به شبکه ارسال کنند. حمله جعل هویت شامل استفاده از رمز عبورهای سرقت شده برای ورود به VANET است. حمله بازپخش شامل تزریق مجدد بیکن‌ها و پیام‌های قبلی است که ممکن است در مواقع اضطراری موجب اختلال شود[13].

برای حفظ حریم خصوصی درVANET ، احراز هویت ناشناس به عنوان یک راهکار استفاده می‌شود. هویت مستعار دیجیتال به صورت رشته بیتی برای احراز هویت، بدون افشای اطلاعات شخصی به کار می‌رود. بر اساس مکانیزم‌های رمزنگاری، روش‌های احراز هویت ناشناس به چند دسته تقسیم می‌شوند. در روش‌های مبتنی بر رمزنگاری متقارن، کلیدهای مشترک بین خودروها وRSU ها استفاده می‌شود که با چالش‌هایی از جمله مدیریت کلید و عدم انکارناپذیری مواجه است. روش احراز هویت دوگانه به منظور بهبود امنیت و مدیریت کلیدها به کار گرفته می‌شود[14].

در روش مبتنی بر زیرساخت کلید عمومی(PKI) ، خودروها به زوج کلیدهای عمومی و خصوصی مجهز هستند که برای ارتباطات ناشناس و احراز هویت استفاده می‌شوند. مجوزهای کلید عمومی برای احراز هویت خودروها توسط CA صادر می‌شود و هویت‌های مستعار کوتاه‌مدت از CA درخواست می‌شوند. نگاشت‌های هویت مستعار برای تعیین هویت واقعی در صورت بروز تضاد نگهداری می‌شوند. در روش مبتنی بر امضای هویتی(IBS) ، شناسه گره به عنوان کلید عمومی استفاده می‌شود و پیام‌ها با کلید خصوصی امضا می‌شوند. این روش نیازی به مجوزهای اضافی ندارد، اما مشکل اصلی آن این است که PKG از کلید خصوصی هر خودرو آگاه است[12].

2.4 پیشینه پژوهش

در هر تحقیق علمی، مرور پیشینه تحقیق یکی از مهم‌ترین بخش‌ها است که به بررسی و تحلیل آثار و دستاوردهای قبلی در حوزه مورد نظر می‌پردازد. این بخش به محقق این امکان را می‌دهد تا با آگاهی از روندهای موجود در زمینه تحقیقاتی خود، به شناسایی خلأها، مشکلات و نقاط قوت تحقیقات پیشین پرداخته و بر اساس آن‌ها، اهداف و فرضیات تحقیق خود را تنظیم نماید. همچنین، بررسی پیشینه تحقیق کمک می‌کند تا روش‌های استفاده‌شده در تحقیقات قبلی شناسایی شده و محقق بتواند از آن‌ها برای طراحی روش‌شناسی دقیق و بهینه در تحقیق خود بهره گیرد. در این بخش، هدف این است که با بررسی جامع و

دقیق منابع موجود، بتوان به تحلیل و تبیین سوالات تحقیق پرداخته و مسیر جدیدی برای توسعه و تکامل علمی فراهم آورد.منابع این پیشینه شماره‌های 15-16-17-18-19-20-21-22 است.

جدول1- خلاصه پیشینه پژوهش

نام نویسندگان/ سال	عنوان مقاله	روش پیشنهادی / نتایج	نتایج اصلی / مقایسه‌ها
مغنیان و همکاران(2020)	تشخیص نفوذ شبکه با استفاده از ANN و الگوریتم GOA	استفاده از شبکه عصبی مصنوعی برای تشخیص نفوذ با استفاده از الگوریتم بهینه‌سازی ملخ (GOA)	عملکرد بهتر نسبت به RF، XGBoost و ANN با الگوریتم‌های HHO، BOA و BWO در تشخیص نفوذ
پونگودی و همکاران(2022)	احراز هویت و تعویض کلید در VANETها	استفاده از روش‌های PKI، ID، مبتنی بر MAC و مبتنی بر برای ایمن‌سازی ارتباطات	استفاده از تکنیک استنتاج عصبی فازی برای پیش‌بینی رتبه‌بندی امنیتی VANET
آمائوچی و همکاران(2023)	تشخیص نفوذ در اینترنت اشیا	استفاده از تکنیک اطلاعات متقابل برای انتخاب ویژگی برای SMOTE و بیش‌نمونه‌برداری	مقایسه با روش‌های دیگر طبقه‌بندی با استفاده از مجموعه داده‌های واقعی
آریا و همکاران(2023)	تشخیص نفوذ با استفاده از یادگیری فدرال توزیع‌شده در VANET	استفاده از یادگیری فدرال برای توسعه طبقه‌بندی‌کننده‌های IDS	کاهش هزینه‌های ارتباطی و افزایش دقت تشخیص با استفاده از شبکه‌های عصبی ناهمگن فدرال
حیدری و همکاران(2022)	حملات DDoS در VANET و راه‌حل‌های آن	استفاده از تکنیک‌های یادگیری ماشین برای کاهش حملات DdoS در VANET	بهبود تشخیص حملات مخفیانه DdoS در VANET

فتحی و همکاران(2023)	تشخیص حملات Jamming و Spoofing در VANET	استفاده از الگوریتم‌های درخت تصمیم، SVM و K-NN برای تشخیص حملات	دقت 98٪ در شناسایی حملات پارازیت و جعل
الوشاح و همکاران(2023)	انتخاب ویژگی در اینترنت اشیا	استفاده از الگوریتم K-NN و EPC برای انتخاب ویژگی	دقت طبقه‌بندی EPC ٪98 با مدل برای چالش‌های IoT
حنفی و همکاران(2023)	توسعه جدید IDS و GJO با استفاده از LSTM	استفاده از الگوریتم GJO برای انتخاب ویژگی‌ها و LSTM برای طبقه‌بندی	دقت 98.21٪ در مجموعه داده‌های NSL-KDD و CICIDS2017

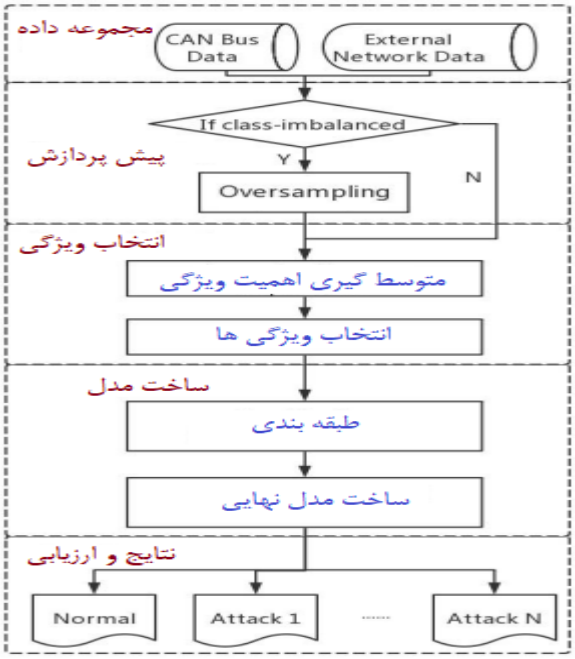
3. روش شناسی

فناوری V2X (وسیله نقلیه به همه چیز) به‌طور فزاینده‌ای برای اتصال دستگاه‌های اینترنت اشیا (IoT) به‌ویژه در خودروها استفاده می‌شود. این فناوری در هسته وسایل نقلیه خودران (AV) قرار دارد و شامل ارتباطات خودرو به وسیله نقلیه(V2V) ، وسیله نقلیه به عابر پیاده(V2P) ، خودرو به زیرساخت (V2I) و دیگر سیستم‌ها می‌باشد. با افزایش اتصال خودروها، تهدیدات سایبری به‌ویژه حملات به شبکه‌های این خودروها، به یک نگرانی عمده تبدیل شده است. حملات بدخواهانه می‌توانند عواقب جدی برای ایمنی انسان‌ها به همراه داشته باشند. سیستم‌های تشخیص نفوذ (IDS) ابزاری برای شناسایی حملات از طریق ترافیک شبکه بین وسایل نقلیه و سایر دستگاه‌ها هستندIDS .ها برای شناسایی تهدیدات و اطلاعات غیرعادی از داده‌های ترافیک شبکه استفاده می‌کنند.

در خودروهای مدرن، واحدهای کنترل الکترونیکی (ECU) برای انجام عملکردهای مختلف از طریق شبکه CAN (Controller Area Network) به هم متصل می‌شوند. همچنین این خودروها به شبکه‌های خارجی از طریق فناوری V2X متصل هستند. با این حال، به دلیل افزایش پیچیدگی، خودروها در معرض تهدیدات سایبری مختلفی قرار دارند که می‌توانند باعث نقص در عملکرد و یا حوادث ترافیکی شوند. حملات رایج شامل حملات انکار سرویس(DoS) ، شنود، جعل GPS و حملات تزریق پیام بر روی شبکه CAN است. بسیاری از سیستم‌های امنیتی سنتی برای شبکه‌های داخلی خودرو مناسب نیستند زیرا محدودیت‌هایی در ارتباطات دارند.

به‌منظور ایمن‌سازی شبکه‌های داخل خودرو و ارتباطات خارجی، IDSدر مکان‌های مختلف خودرو پیاده‌سازی می‌شود. این سیستم‌ها قادرند حملات مختلف مانند تزریق پیام‌های مخرب، حملات DoS و جعل GPSرا شناسایی کنند. در شبکه‌های داخلی خودرو، IDSمی‌تواند در بالای شبکه CAN قرار گیرد تا پیام‌های مخرب را شناسایی کند. همچنین، IDSمی‌تواند در دروازه‌های شبکه برای نظارت بر ترافیک شبکه خارجی نصب شود. این سیستم‌ها با شناسایی ترافیک غیرعادی و حملات سایبری، از ایمنی سیستم‌ها و وسایل نقلیه

حفاظت می‌کنند. یکی از انواع حملات رایج در شبکه‌های خودرو، حملات تزریق پیام است که در آن مهاجمان پیام‌های مخربی به شبکه CAN ارسال می‌کنند. این پیام‌ها می‌توانند بر روی گره‌ها اثر بگذارند و عملکرد خودرو را مختل کنند. سیستم IDS برای شناسایی این حملات و جلوگیری از تاثیرات منفی آن‌ها، به‌طور مداوم پیام‌های ارسالی را بررسی می‌کند.



شکل2- چارچوب روش شناسی

در این بخش، پیش پردازش داده‌ها برای طراحی سیستم تشخیص نفوذ (IDS) در شبکه‌های خودرو و سیستم‌های CAN (Controller Area Network) مورد بررسی قرار می‌گیرد. مراحل پیش پردازش شامل جمع‌آوری داده‌ها، آماده‌سازی آن‌ها برای استفاده در مدل‌های یادگیری ماشین و انجام اصلاحات برای بهبود کیفیت داده‌ها است. در ادامه مراحل مختلف پیش پردازش و انتخاب ویژگی‌ها به تفصیل توضیح داده می‌شود.

3.1 جمع‌آوری داده‌ها

برای طراحی یک سیستم تشخیص نفوذ مؤثر، اولین گام جمع‌آوری داده‌های کافی است. این داده‌ها شامل ترافیک شبکه از شبکه‌های داخلی و بیرونی وسایل نقلیه می‌شود. داده‌ها باید شامل اطلاعات در حالت عادی و غیرعادی (حملات) باشند. استفاده از sniffers (ابزارهای جمع‌آوری بسته‌ها) برای ضبط داده‌ها پیشنهاد می‌شود. ویژگی‌هایی که برای تشخیص حملات مهم هستند، باید در نظر گرفته شوند.

در مورد شبکهCAN ، که تهدیدات عمده آن حملات تزریق پیام است، داده‌ها باید شامل پیام‌ها و فریم‌هایCAN، به‌ویژه شناسه‌های CAN و میدان داده آن‌ها باشند. برای شبکه‌های خارجی که مستعد حملات مختلف هستند، ویژگی‌هایی مانند طول بسته، سرعت انتقال، توان عملیاتی، زمان بین ورود داده‌ها، پرچم‌های TCPو تعداد آن‌ها باید جمع‌آوری شوند.

3.2 پیش پردازش داده‌ها

پس از جمع‌آوری داده‌ها، چندین مرحله از پیش پردازش انجام می‌شود:

- **کدگذاری داده‌ها** :داده‌ها می‌توانند با استفاده از بردار داغ (One-Hot Encoding) کدگذاری شوند تا ویژگی‌های شبکه بهتر تفکیک شوند.
- **نرمال‌سازی** :داده‌ها معمولاً باید نرمال شوند تا الگوریتم‌های یادگیری ماشین عملکرد بهتری داشته باشند.
- **مقابله با نامتعادلی داده‌ها** :چون داده‌های حمله معمولاً کمتر از داده‌های عادی هستند، باید از روش‌هایی مانند **بیش از حد نمونه‌برداری تصادفی** یا **SMOTE** (Synthetic Minority Over-sampling Technique) برای تعادل داده‌ها استفاده شود.

3.3 انتخاب ویژگی

در مرحله انتخاب ویژگی، هدف این است که ویژگی‌های مهم‌تر از بین تمامی ویژگی‌ها شناسایی شوند تا دقت مدل افزایش یابد و هزینه محاسباتی کاهش یابد. این مرحله شامل حذف ویژگی‌های نامربوط و زائد است. برخی از ویژگی‌ها می‌توانند اطلاعات مشابهی داشته باشند و نیاز به حذف دارند.

برای انتخاب ویژگی‌های بهینه، از الگوریتم‌های بهینه‌سازی مانند **الگوریتم بهینه‌سازی سفره ماهی (MRFO)** استفاده می‌شود. این الگوریتم از رفتارهای جستجوی مختلف مانند جستجوی زنجیره‌ای، سیکلون و سالوتا برای بهینه‌سازی انتخاب ویژگی‌ها استفاده می‌کند.

3.4 طبقه‌بندی و ساخت مدل

پس از انتخاب ویژگی‌ها، مرحله بعدی طبقه‌بندی داده‌ها است. در این مرحله، مدل‌های یادگیری ماشین برای شناسایی داده‌های نفوذ آموزش داده می‌شوندIDS .ها می‌توانند به دو دسته عمده تقسیم شوند:

1. **IDS مبتنی بر امضا** :این سیستم‌ها به شناسایی الگوهای حمله شناخته‌شده با استفاده از مدل‌های نظارت‌شده می‌پردازند. در این سیستم‌ها، معمولاً از درخت تصمیم (DT) به عنوان الگوریتم یادگیری استفاده می‌شود.
2. **IDS مبتنی بر ناهنجاری** :این سیستم‌ها قادر به شناسایی حملات ناشناخته هستند. آن‌ها از داده‌های بدون برچسب برای تشخیص ناهنجاری‌ها استفاده می‌کنند و به دلیل این که می‌توانند حملات جدید را شناسایی کنند، می‌توانند هشدارهای نادرست زیادی ایجاد کنند.

در این سیستم پیشنهادی، الگوریتم **درخت تصمیم (DT)** به عنوان یادگیرنده پایه برای توسعه IDS مبتنی بر امضا انتخاب می‌شود. الگوریتم‌های درخت تصمیم برای پیش‌بینی وضعیت‌ها از ساختار درختی استفاده می‌کنند و دارای پارامترهایی هستند که باید تنظیم شوند تا به بهترین عملکرد برسند.

4. یافته ها

از آنجایی که وسایل نقلیه خودران و وسایل نقلیه متصل در برابر حملات سایبری مختلف آسیب پذیر هستند، IDS یکی از راه حل های کارآمد برای شناسایی حملات شبکه راه اندازی شده و ایمن سازی شبکه های خودرو است. در فصل قبل، یک IDS مبتنی بر الگوریتم‌های یادگیری ماشینی برای شناسایی تهدیدات در شبکه‌های خودرویی ارائه گردید. در ادامه به ارزیابی روش پیشنهادی، بر روی دو مجموعه داده برای شبکه‌های درون خودرو و شبکه‌های خارجی پرداخته می شود.

4.1 مجموعه داده و پیاده سازی روش پیشنهادی

برای ارزیابی روش پیشنهادی، مهندسی ویژگی و الگوریتم‌های یادگیری ماشین در پایتون پیاده‌سازی شدند، آزمایش‌ها بر روی دستگاه با واحد پردازش مرکزی (CPU) i7-8700 شش هسته‌ای 3.20 گیگاهرتز و رم 16 گیگابایتی انجام شده است.

آزمایش‌ها به سه بخش تقسیم می‌شوند، یکی برای تشخیص نفوذ شناخته شده با ارزیابی مؤلفه IDS مبتنی بر امضا در مجموعه داده‌های برچسب‌گذاری‌شده، یکی برای تشخیص نفوذ ناشناخته با ارزیابی مؤلفه IDS مبتنی بر ناهنجاری در مجموعه داده‌های بدون برچسب، و دیگری برای کل مجموعه داده‌های برچسب‌گذاری‌شده.

به منظور توسعه سیستم تشخیص نفوذ در رویکرد پیشنهادی شبکه درون خودرو، مجموعه داده مورد استفاده مجموعه داده CAN-intrusion است که در سال 2018 پیشنهاد شد [9]. این مجموعه داده با ثبت ترافیک CAN از طریق درگاه OBD-II یک وسیله نقلیه هنگام راه اندازی حملات CAN تولید می شود.

ویژگی های این مجموعه داده شامل timestamp ، شناسه CAN، کد طول داده* (DLC) و فیلد داده 8 بیتی بسته های CAN (DATA[0]-DATA[7]) است. از آنجایی که ویژگی "timestamp " همبستگی قوی با دوره های شبیه سازی حمله سایبری دارد و می تواند به مدل ها و نتایج مغرضانه منجر شود، این ویژگی از فضای ویژگی حذف شده است. همانطور که نویسندگان در [9] مجموعه داده CAN-intrusion را با تزریق حملات به شناسه های تصادفی CAN ایجاد کردند، این ویژگی CAN ID حفظ می شود.

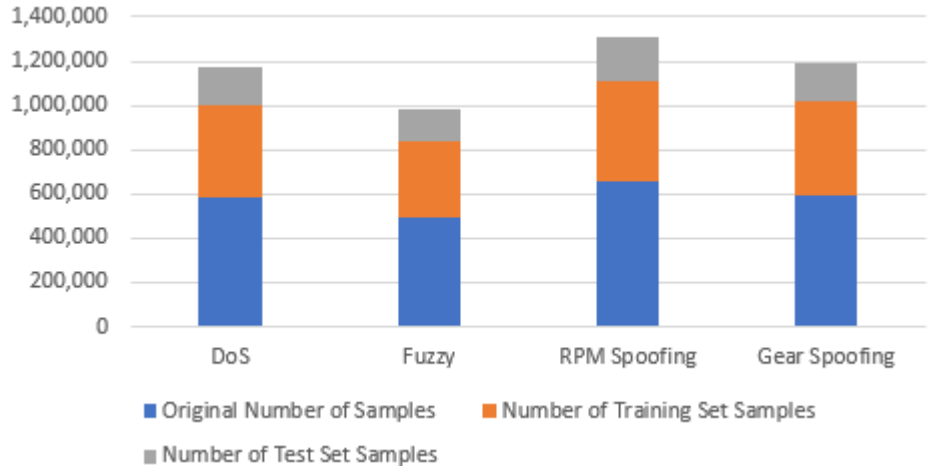
بر اساس ساختار بسته CAN نشان داده شده، ده ویژگی استخراج شده از فیلد شناسه و فیلد داده بسته های CAN، از جمله CAN ID، DLC، و DATA[0]-DATA[7]، به طور مقدماتی برای توسعه IDS انتخاب شدند. انواع حمله مجموعه داده CANintrusion در جدول زیر نشان داده شده است.

جدول 2- برچسب کلاس و اطلاعات مجموعه داده CAN-Intrusion

Class Label	Original Number of Samples	Number of Training Set Samples	Number of Test Set Samples
Normal	14,037,293	9,826,105	4,211,188
DoS	587,521	411,265	176,256
Fuzzy	491,847	344,293	147,554
RPM Spoofing	654,897	458,428	196,469
Gear Spoofing	597,252	418,076	179,176

علاوه بر این، توزیع برچسب مجموعه داده اصلی، مجموعه آموزشی و مجموعه آزمایشی در این جدول نشان داده شده است. از آنجایی که این مجموعه داده دارای تعداد زیادی نمونه هست (حداقل 491847 نمونه)، SMOTE برای متعادل کردن مجموعه داده CAN-intrusion-data مورد نیاز نیست.

* data length code



نمودار 1- اطلاعات مجموعه داده CAN-Intrusion

بسیاری از پروژه‌ها و مقالات تحقیقاتی شناسه‌های شبکه خودروهای خارجی را با استفاده از مجموعه داده‌های عمومی امنیت شبکه، از جمله KDD-99، NSL-KDD، Kyoto 2006+، UNSW-NB15، و CICIDS2017 توسعه می‌دهند. در میان این مجموعه داده‌های امنیت سایبری، CICIDS2017 [23] نماینده‌ترین مجموعه داده شبکه‌های خارجی کنونی است زیرا پیشرفته‌ترین مجموعه داده است و دارای ویژگی‌ها، نمونه‌ها و انواع حملات سایبری بیشتری نسبت به سایر مجموعه‌های داده است [24]. بنابراین، داده‌های جریان ترافیک شبکه در مجموعه داده CICIDS2017 در رویکرد پیشنهادی برای نمایش داده‌های پیچیده شبکه خودروهای خارجی انتخاب شده‌اند.

جدول3- برچسب کلاس، نوع حمله و اندازه مجموعه داده CICIDS2017

Number of Test Set Samples	Number of Training Set Samples After Balancing	Original Number of Samples	Corresponding Attack Type	Class Label
681,929	1,591,168	2,273,097	-	BENIGN
590	100,000	1,966	Botnets	Bot
114,210	266,489	380,699	DoS	DDoS
				DoS GoldenEye
				DoS Hulk
				DoS Slow-httptest
				DoS Slowloris

				Heartbleed
47,679	111,251	158,930	Sniffing	Port-Scan
4,150	100,000	13,835	Brute-Force	SSH-Patator
				FTP-Patator
11	100,000	36	Infiltration	Infiltration
654	100,000	2,180	Web Attack	Web Attack – Brute Force
				Web Attack – Sql Injection
				Web Attack – XSS

از آنجایی که کلاس های Bot، brute-force، نفوذ و حمله وب کلاس های اقلیت با تعداد کمی نمونه (از 36 تا 13835) هستند، روش SMOTE برای سنتز نمونه های بیشتری به کار گرفته شد تا طبقات اقلیت بتوانند حداقل 100000 نمونه داشته باشند. پرداختن به عدم تعادل کلاس می تواند از به دست آوردن مدل های مغرضانه با نرخ تشخیص حمله پایین جلوگیری کند.

برای ارزیابی IDS پیشنهادی برای تشخیص نفوذ شناخته شده، مدل‌های ML در IDS مبتنی بر امضا آموزش داده می‌شوند و روی دو مجموعه داده برچسب‌گذاری‌شده که نشان‌دهنده داده‌های ترافیک شبکه داخل خودرو و خارجی هستند، آزمایش می‌شوند.

جدول 4- مقایسه کارایی عملکرد طبقه‌بندی‌کننده‌های مختلف برروی مجموعه داده CAN-INTRUSION

Execution Time (S)	F1	FAR (%)	DR (%)	Acc (%)	Method
911.6	0.934	5.3	96.3	97.4	KNN
13765.6	0.933	4.8	95.7	96.5	SVM
-	0.9879	0.0	98	98.1	XYF-K
-	0.92	1.76	86.66	87.21	SAIDuCANT

-	0.98	2.0	98.5	-	SSAE
-	0.98	0.16	99.84	99.93	DCNN
-	0.99	0.0	99.0	99.0	LSTM-Autoencoder
359.4	0.99	0.0005	99.99	99.99	Proposed- Method

همانطور که در جدول 4نشان داده شده است، پس از استفاده از روش انتخاب ویژگی پیشنهادی برای انتخاب ویژگی های مهم IDS مبتنی بر امضای پیشنهادی می‌تواند به دقت بالای 99.99 درصد در مجموعه داده نفوذ CAN برسد. روش پیشنهادی با رویکردهای امیدوارکننده دیگر در جداول 4-4 و 4-5، مقایسه شده است. همچنین نتایج تجربی روی مجموعه داده CICIDS2017 در جدول 4-5 نشان داده شده است که ویژگی های بهینه از مجموعه ویژگی ها با استفاده از مدل‌های بهینه ML پیشنهادی، معیارهای ارزیابی مختلف از جمله، امتیاز F1، IDS بهبود یافته است. نتایج چند طبقه‌بندی مورد استفاده برای ارزیابی ظرفیت IDS برای شناسایی انواع مختلف حملات، IDS همچنین برای آموزش یک مدل طبقه‌بندی باینری که می‌تواند داده‌های ترافیک شبکه عادی و غیرعادی را تشخیص دهد و یکی از این دو برچسب را برگرداند، پیاده‌سازی شده است.

جدول5- مقایسه کارایی عملکرد طبقه‌بندی‌کننده‌های مختلف برروی مجموعه داده CICIDS2017

Execution Time (S)	F1	FAR (%)	DR (%)	Acc (%)	Method
15243.6	0.963	6.3	96.2	96.3	KNN
49953.1	0.978	1.48	97.58	98.01	SVM
-	0.98	1.1	98	98.4	MLP
2349.6	0.934	0.001	93.35	93.43	ET
1848.3	0.988	0.145	98.8	98.82	RF

-	-	1.4	98.65	98.13	SU-IDS
-	-	1.3	98.6	98.4	STDeepGraph
-	0.9581	4.19	95.82	98.95	DBN
-	0.9504	7.24	98.68	99.63	GAN-RF
-	-	0.986	94.10	99.811	DeepCoin
486	0.99	0.078	99.83	99.9	Proposed- Method

تمام مدل‌های IDS مبتنی بر ناهنجاری برای طبقه‌بندی باینری با برچسب‌گذاری نمونه‌های انواع حملات به عنوان «حمله» و نمونه‌های عادی به عنوان «عادی» آموزش داده می‌شوند. در سیستم پیشنهادی، پس از ارزیابی توسط IDS مبتنی بر امضا، تمام نمونه‌های داده از انواع حمله شناخته شده بازگردانده می‌شوند و سایر نمونه‌های عادی برچسب «مشکوک» داده می‌شوند و به IDS مبتنی بر ناهنجاری ارسال می‌شوند تا مشخص شود که آیا حملات ناشناخته وجود دارد یا خیر.

برای مجموعه داده CAN-intrusion که داده های ترافیک شبکه درون وسیله نقلیه را نشان می دهد، هر نوع حمله CAN به عنوان یک نوع حمله جدید در هر آزمایش در نظر گرفته می شود. نتایج ارزیابی تشخیص حمله ناشناخته CAN در جدول 4-6 نشان داده شده است. برای انواع حملات DoS، gear spoofing و جعل RPM، سیستم پیشنهادی می تواند به نرخ تشخیص 100٪، نرخ هشدار نادرست نزدیک به صفر و امتیاز F1 نزدیک به یک برسد. با این حال، DR و F1 برای حمله فازی کمتر است. دلیل این امر این است که مقادیر ویژگی بسته‌های حمله فازی مقادیر عددی تصادفی هستند و مقادیر تصادفی خاصی می‌توانند بسیار شبیه به بسته‌های معمولی باشند و تشخیص آنها را برای الگوریتم‌های یادگیری بدون نظارت مشکل کنند.

جدول6- ارزیابی عملکرد در مورد هر نوع حمله ناشناس مجموعه داده CAN-Intrusion

F1	FAR (%)	DR (%)	Validation Instances	Attack Type
1.0	0.0	100.0	1,289,386	DoS
0.848	0.057	73.23	1,193,712	Fuzzy
0.99	0.446	100.0	1,299,117	Gear Spoofing

0.827	0.258	79.36	5,138,977	Average (CL-k-means)
0.999	0.003	100.0	1,356,762	RPM Spoofing
0.964	0.125	93.81	5,138,977	Proposed-Method

جدول 6 نشان می دهد که امتیاز F1 MTH-IDS پیشنهادی در مجموعه داده CAN-intrusion را می توان تا حد زیادی از 0.827 به 0.964 با اجرای دو طبقه بندی گر بایاس نسبت به مدل CL-k-means بهبود داده است. به طور خلاصه، سیستم پیشنهادی می تواند به طور موثر اکثر حملات ناشناخته را در شبکه های درون وسیله نقلیه به جز حملات فازی شناسایی کند. آموزش انواع مختلف نمونه‌های حمله ما را قادر می‌سازد تا یک IDS جامع‌تر طراحی کنیم که می‌تواند انواع حملات ناشناخته بیشتری را به طور موثر تشخیص دهد. رویکرد IDS پیشنهادی می‌تواند بسیاری از انواع حملات را که قبلاً دیده نشده بود، با نرخ تشخیص نسبتاً بالا و نرخ هشدار نادرست نسبتاً پایین در شبکه‌های درون خودرویی و خارجی شناسایی کند.

جدول 7- ارزیابی عملکرد در مجموعه تست دست نخورده

F1	FAR (%)	DR (%)	Acc (%)	Dataset
0.9999	0.00004	100.0	99.99	CAN-intrusion-dataset
0.999	0.0923	99.81	99.91	CICIDS2017

روش پیشنهادی می تواند به طور دقیق تمام نمونه های حمله DoS، RPM جعل و gear spoofing را شناسایی کند، و تنها دارای دو آلارم کاذب برای تشخیص حمله فازی است. این نتایج با سایر آثار مشابه از ادبیاتی که از مجموعه داده‌های مشابهی استفاده کرده‌اند، همسو هستند. دستیابی به دقت بالا به دلیل تفاوت زیاد بین الگوهای حمله و عادی در مجموعه داده‌های CAN-intrusion به وضوح قابل تشخیص است. تعداد نمونه های داده برای حمله نفوذی تنها 36 است که برای آموزش یک طبقه بندی کننده موثر برای شناسایی دقیق این حمله کافی نیست. با این وجود، مدل پیشنهادی می‌تواند حملات دیگر را با امتیاز کلی F1 99 ٪ به دقت شناسایی کند. از آنجایی که مجموعه‌های آزمایشی قبل از اعتبار سنجی نگه‌دارنده دست نخورده بودند، عملکرد بالا نشان‌دهنده تعمیم‌پذیری قوی چارچوب پیشنهادی در مجموعه‌های داده جدید است.

5. نتیجه‌گیری

با توسعه سریع فناوری‌های اینترنت اشیا (IoT) و اینترنت وسایل نقلیه (IoV)، وسایل نقلیه مدرن به وسایل نقلیه تحت کنترل شبکه، از جمله وسایل نقلیه خودکار (AVs) و وسایل نقلیه متصل (CV) تبدیل شده‌اند. سیستم‌های IoV معمولی شامل شبکه‌های داخل خودرو (IVN) و شبکه‌های خارجی است. در IVN ها، گذرگاه شبکه کنترل کننده (CAN) سیستم مرکزی است که ارتباطات بین واحدهای کنترل الکترونیکی (ECU) را قادر می سازد تا اقدامات را انجام دهند و عملکردها را اتخاذ کنند. از سوی دیگر، شبکه‌های خودروهای خارجی امکان اتصال بین وسایل نقلیه هوشمند و سایر نهادها در IoV، از جمله واحدهای کنار جاده، زیرساخت‌ها و کاربران جاده را فراهم می‌کنند. برای افزایش امنیت IoV، در این پژوهش یک مدل سیستم تشخیص نفوذ چند لایه پیشنهاد شده است که موجب افزایش مقاومت شبکه در برابر حملات مختلف شده و می‌تواند انواع مختلفی از حملات سایبری شناخته شده در شبکه‌های درون خودرویی و خارجی خودرویی برای وسایل نقلیه مدرن شناسایی کند. رویکرد پیشنهادی شامل بخش یادگیری ماشین، پیش‌پردازش داده‌ها و مهندسی ویژگی است. همچنین از الگوریتم سفره ماهی برای افزایش کارایی سیستم استفاده شده است. از طریق پیش پردازش داده ها و مهندسی ویژگی، کیفیت داده های ورودی می تواند به طور قابل توجهی برای یادگیری مدل دقیق تر بهبود یابد. مدل یادگیری پیشنهادی، قادر است تا به عملکرد بهینه برای تشخیص حمله شناخته شده و ناشناخته در شبکه‌های خودرو دست یابد. از طریق ارزیابی عملکرد IDS پیشنهادی بر روی دو مجموعه داده عمومی که داده‌های شبکه داخل خودرو و خارجی را نشان می‌دهند، سیستم پیشنهادی می‌تواند به طور موثر انواع مختلف حملات شناخته شده را با دقت بالای 99 درصد بر روی مجموعه داده های CAN-intrusion و CICIDS2017 شناسایی می کند. علاوه بر این، سیستم پیشنهادی می‌تواند انواع مختلفی از حملات ناشناخته را با میانگین امتیازات F1 ، 0.97 و 0.83 به ترتیب در مجموعه داده‌های CAN-intrusion و CICIDS2017 شناسایی کند. نتایج بر روی هر دو مجموعه داده به ازای معیارهای مختلف ارزیابی مورد بررسی قرار گرفته است و با سایر روش های کارامد مورد ارزیابی و مقایسه گرفته است. نتای بدست آمده نشان می دهد که روش پیشنهادی در مقایسه با سایر روش ها بسیار کارامد می باشد و می تواند به افزایش مقاومت شبکه در برابر نفوذ و حمله کمک نماید.

منابع

[1] Koohang, A., Sargent, C.S., Nord, J.H. and Paliszkiewicz, J., 2022. Internet of Things (IoT): From awareness to continued use. International Journal of Information Management, 62, p.102442.

[2] Wang, Y., Zen, H., Sabri, M.F.M., Wang, X. and Kho, L.C., 2022. Towards Strengthening the Resilience of IoV Networks—A Trust Management Perspective. Future Internet, 14(7), p.202.

[3] Khalid, M., Hamza, L.A., Kareem, Z.H., Malik, R.Q., Muneer, R.M. and Hamza, S.A., 2023, March. A review on IoV: Architecture, issues, challenges, and its applications. In AIP Conference Proceedings (Vol. 2591, No. 1, p. 020041). AIP Publishing LLC.

[4] Agarwal, E., 2022. A Review on VANET Security Attacks. Barak Education Society, p.45.

[5] Garg, A., Chauhan, A. and Shambharkar, P.G., 2022, August. Security Threats & Attacks in IoV Environment: Open Research Issues and Challenges. In 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT) (pp. 803-810). IEEE.

[6] Avasthi, S., Sanwal, T., Sharma, S. and Roy, S., 2023. VANETs and the Use of IoT: Approaches, Applications, and Challenges. Revolutionizing Industrial Automation Through the Convergence of Artificial Intelligence and the Internet of Things, pp.1-23.

[7] Kaur, K. and Verma, H.K., 2023. IoV-Health: an intelligent integrated emergency health monitoring and alert generation system. Soft Computing, pp.1-17.

[8] Santhosh Kumar, S.V.N., Selvi, M. and Kannan, A., 2023. A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things. Computational Intelligence and Neuroscience, 2023.

[9] Khan, A.R., Jamlos, M.F., Osman, N., Ishak, M.I., Dzaharudin, F., Yeow, Y.K. and Khairi, K.A., 2022. DSRC technology in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) IoT system for intelligent transportation system (ITS): A review. *Recent Trends in Mechatronics Towards Industry 4.0: Selected Articles from iM3F 2020, Malaysia*, pp.97-106.

[10] Iturbe-Olleta, N., Bilbao, J., Iparraguirre, O., Mendizabal, J. and Brazalez, A., 2024. An adjusted propagation model for ITS-G5 communications for improving the location of RSUs in real V2I deployments. *Vehicular Communications*, *45*, p.100716.

[11] Radi, W., Samir, R., El-Badawy, H. and Serag, E., 2024. Decentralized Vehicle-to-Vehicle (V2V) Intelligent and Sustainable Communications for Improving Traffic Safety. *Journal of Communication Sciences and Information Technology*, *3*(1), pp.9-18.

[12] Xie, Q., Ding, Z. and Zheng, P., 2023. Provably secure and anonymous V2I and V2V authentication protocol for VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *24*(7), pp.7318-7327.

[13] Khalil, A., Farman, H., Nasralla, M.M., Jan, B. and Ahmad, J., 2024. Artificial Intelligence-based intrusion detection system for V2V communication in vehicular adhoc networks. *Ain Shams Engineering Journal*, *15*(4), p.102616.

[14] Raja, G., Anbalagan, S., Vijayaraghavan, G., Theerthagiri, S., Suryanarayan, S.V. and Wu, X.W., 2020. SP-CIDS: Secure and private collaborative IDS for VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), pp.4385-4393.

[15] Moghanian, S., Saravi, F.B., Javidi, G. and Sheybani, E.O., 2020. GOAMLP: Network intrusion detection with multilayer perceptron and grasshopper optimization algorithm. *IEEE Access*, *8*, pp.215202-215213.

[16] Poongodi, M., Bourouis, S., Ahmed, A.N., Vijayaragavan, M., Venkatesan, K.G.S., Alhakami, W. and Hamdi, M., 2022. A novel secured multi-access edge computing based vanet with neuro fuzzy systems based blockchain framework. *Computer Communications*, *192*, pp.48-56.

[17] Amaouche, S., Benkirane, S., Guezzaz, A. and Azrour, M., 2023. A Proposed Machine Learning Model for Intrusion Detection in VANET. In *Artificial Intelligence and Smart Environment: ICAISE'2022* (pp. 103-108). Cham: Springer International Publishing.

[18] Arya, M., Sastry, H., Dewangan, B.K., Rahmani, M.K.I., Bhatia, S., Muzaffar, A.W. and Bivi, M.A., 2023. Intruder Detection in VANET Data Streams Using Federated Learning for Smart City Environments. *Electronics*, *12*(4), p.894.

[19] Haydari, A. and Yilmaz, Y., 2022. RSU-based online intrusion detection and mitigation for VANET. *Sensors*, *22*(19), p.7612.

[20] Fathi, M. and naeim Sobhani, S., 2023. A Lightweight Cross-Layer Intrusion Detection System on Jamming, Spoofing, and Mixed Attacks in Vehicular Communication.

[21] Alweshah, M., Hammouri, A., Alkhalaileh, S. and Alzubi, O., 2023. Intrusion detection for the internet of things (IoT) based on the emperor penguin colony optimization algorithm. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), pp.6349-6366.

[22] Hanafi, A.V., Ghaffari, A., Rezaei, H., Valipour, A. and arasteh, B., 2023. Intrusion detection in internet of things using improved binary golden jackal optimization algorithm and LSTM. *Cluster Computing*, pp.1-18.

[23] KUMAR, Yogendra; KUMAR, Vijay; SUBBA, Basant. Optimization techniques for IDS-Generated traffic congestion control in VANET. *Internet Technology Letters*, e518.

[24] CHEN, Xiuzhen, et al. Fast and practical intrusion detection system based on federated learning for VANET. *Computers & Security*, 2024, 103881.