چارچوب دوقلوی دیجیتال تقویت‌شده با هوش مصنوعی برای با تاب‌آوری سایبری Gشبکه‌های اینترنت وسایل نقلیه 6

Yagmur Yigit, Student Member, IEEE, Leandros Maglaras, Senior Member, IEEE, William J. Buchanan, Senior Member, IEEE, Berk Canberk, Senior Member, IEEE, Hyundong Shin, Fellow, IEEE, and Trung Q. Duong, Fellow, IEEE

چکیده-فناوری دوقلوی دیجیتال نقشی حیاتی در توسعه اینترنتِ وسایل نقلیه نسل ششم IoV6 Gدارد، زیرا امکان پایش و ارزیابی محیط پویا و پیچیده‌ی وسایل نقلیه را فراهم می‌کند. با این حال، شبکه‌های IoV 6 Gبا چالش‌های مهمی در زمینه امنیت شبکه و کارایی محاسباتی روبه‌رو هستند که باید برطرف شوند. فناوری‌های موجود دوقلوی دیجیتال در شبکه‌های IoV 6 Gمعمولاً با محدودیت‌هایی مانند تکیه بر مدل‌های ایستا و نیازهای بالای محاسباتی مواجه‌اند که منجر به ناپایداری در تشخیص حملات و کاهش کارایی می‌شود. عملکرد این سامانه‌ها در شاخص‌های تشخیص حمله—از جمله دقت، نرخ تشخیص، و امتیاز—F1 برای الزامات IoV 6 Gکافی نیست. علاوه بر این، آن‌ها تمام پردازش‌ها را در لایه خدمات دوقلوی دیجیتال متمرکز می‌کنند که موجب ناکارآمدی می‌شود. برای رفع این چالش‌ها، ما یک چارچوب نوآورانه دوقلوی دیجیتال تقویت‌شده با هوش مصنوعی معرفی می‌کنیم که با هدف بهبود چشمگیر امنیت شبکه و کارایی محاسباتی در شرایط پویا برای شبکه‌های IoV 6 Gطراحی شده است. چارچوب پیشنهادی ما از یک ماژول مهندسی ویژگی پیشرفته بهره می‌برد که با استفاده از روش‌های انتخاب ویژگی و *خودرمزگذارهای تنک پشته‌ای* (ssAE) ابعاد ویژگی‌ها را در لایه دوقلوی سایبری کاهش می‌دهد و بدین ترتیب بار محاسباتی را به‌طور مؤثر توزیع می‌کند. همچنین از یک ماژول یادگیری برخط استفاده می‌کند که یک سازوکار تشخیص حمله آگاه از وضعیت شبکه را برای تشخیص دقیق حملات فراهم می‌سازد. راهکار پیشنهادی ما عملکردی پایدار در حدود ۹۸٪ نرخ موفقیت در شاخص‌های تشخیص حمله روی دو مجموعه‌داده ارائه می‌دهد. به‌طور مشخص، این سامانه ۱۲٪ کاهش تأخیر سیستم، ۱۵٪ کاهش مصرف انرژی، ۲۰٪ کاهش استفاده از RAM و ۶٫۱٪ افزایش نرخ تحویل بسته‌ها را نشان می‌دهد. این نتایج نشان می‌دهد که چارچوب ما ظرفیت قابل‌توجهی در ارتقای امنیت و کارایی شبکه‌های IoV 6 Gدارد. این پیشرفت‌ها، Robustnessو پاسخ‌دهی سامانه‌های IoV 6 Gرا به شکل چشمگیری افزایش می‌دهد و سهمی مهم در بهبود امنیت و مدیریت شبکه‌های خودرویی ایفا می‌کند.

واژگان کلیدی — هوش مصنوعی(AI) ، امنیت، دوقلوی دیجیتال، اینترنت وسایل نقلیه(IoV) ، سامانه‌های حمل‌ونقل هوشمند (ITS)، شبکه‌های خودرویی.(VANET)

I.مقدمه

تحول شبکه‌های خودرویی موردی (VANETs) یک پیشرفت مهم در ایمنی جاده و کارآمدی حمل‌ونقل به شمار می‌رود؛ موضوعی که سازمان جهانی بهداشت در گزارش وضعیت جهانی ایمنی جاده سال ۲۰۲۳ بر آن تأکید کرده است [1]شبکه‌های VANET در عصر اینترنت وسایل نقلیه نسل ششم IoV6 Gاهمیت رو به رشدی یافته‌اند، زیرا سامانه‌های متصل به اینترنت در وسایل نقلیه—whichشامل حسگرها، عملگرها و دستگاه‌های هوشمند هستند—به اشیای مختلف امکان می‌دهند داده‌ها را جمع‌آوری، انتقال و پردازش کنند. انتظار می‌رود شبکه‌های 6 Gبا ارائه نرخ‌های داده بسیار بالا، کاهش تأخیر تا حد تقریباً آنی، و افزایش پوشش‌دهی، باعث تحول بیشتر در VANET شوند و بر پیشرفت‌های نسل پنجم G5بنا کنند. برای فعال‌سازی شبکه‌های IoV6 G، فناوری دوقلوی دیجیتال نقش اساسی دارد، زیرا این فناوری امکان نظارت و تحلیل محیط پویا و پیچیده خودرویی را فراهم می‌کند [2] ,[3] در شبکه IoV6 G، شبکه‌های خودرویی اهمیت ویژه‌ای دارند زیرا به وسایل نقلیه اجازه می‌دهند با یکدیگر ارتباط خودرو به خودرو (V2V—و با زیرساخت) ارتباط خودرو به زیرساختV2I—ارتباط برقرار کنند. با ارائه اطلاعات دقیق و به‌موقع ترافیکی، ارتباطات خودرویی موجب افزایش راحتی، ایمنی جاده و امکان‌پذیری توسعه خودروهای خودران می‌شود [4] با این حال، این پیشرفت‌ها چالش‌های جدیدی را نیز در مدیریت پیچیدگی و امنیت شبکه‌های خودرویی ایجاد می‌کنند، که ضرورت بهره‌گیری از راهکارهای نوآورانه را برجسته می‌سازد.

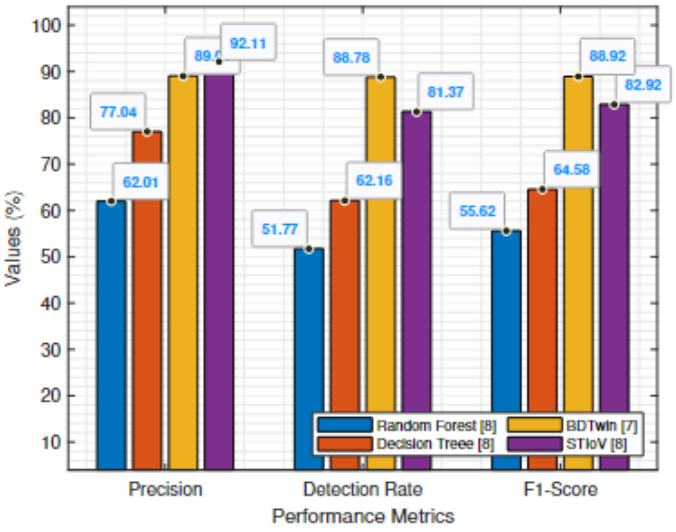
A.انگیزه

در حال حاضر به دلیل ناهمگنی و توپولوژی پویا در شبکه‌های خودرویی، به‌ویژه در ارتباطاتV2I ، افزایش چشمگیری در حملات مخرب مشاهده می‌شود [5]–[7]. مهاجمان با استفاده از حملات پیچیده و ایجاد اختلال در خدمات مرتبط با وسایل نقلیه، آسیب قابل‌توجهی وارد می‌کنند. در یک حمله سایبری مانند حمله انکار سرویس توزیع‌شده(DDoS) ، مهاجم تلاش می‌کند شبکه IoV 6 G را برای کاربران موردنظر غیرقابل‌دسترس یا بدون پاسخ کند و از این طریق در خدمات و سامانه‌های خودرویی اختلال ایجاد کند. این نوع حمله می‌تواند وسایل نقلیه را ناتوان سازد و پیامدهای منفی برای ارائه‌دهندگان خدمات و کاربران به همراه داشته باشد. علاوه بر این، چنین حمله‌ای ممکن است منجر به بروز مشکلات در خودرو، ایجاد ازدحام ترافیکی، اختلال در ارتباطات خودرویی، و حتی بروز تصادفات شود.

شناسایی سریع‌تر حملات، این بار محاسباتی باید توزیع شود. برای رفع این دو چالش اصلی، می‌توان از یادگیری آنلاین برای شناسایی پویای حملات استفاده کرد و از لایه دوقلوی دیجیتال ـ به‌جای لایه سرویس ـ برای مهندسی ویژگی و کاهش ابعاد ویژگی با هدف تقسیم بار محاسباتی بهره برد. افزون بر این، داده‌های شبکه می‌توانند با استفاده از توانایی‌های خودرمزگذار پراکنده پشته‌ای (ssAE) به‌صورت مؤثر پردازش و تحلیل شوند [14]، [15]. روش ssAE ویژگی‌های مرتبط برای کاربردهای امنیت سایبری مانند تشخیص ناهنجاری، شناسایی الگو و تشخیص حمله را استخراج کرده و در عین کاهش ابعاد داده، ویژگی‌های کلیدی را حفظ می‌کند.

ب. پوشش مقاله و مشارکت‌ها

در این مقاله، از ssAE به دلیل قابلیت‌های بهبودیافته در استخراج ویژگی و کاهش مؤثر ابعاد داده استفاده شده است. برای مقابله با چالش‌های پیش‌گفته، این پژوهش بر ارتباطات V2I و به‌طور مشخص بر تقویت امنیت RSU (واحد کنار جاده‌ای) تمرکز دارد. علاوه بر این، ما رویکردی نوآورانه مبتنی بر هوش مصنوعی برای تقویت امنیت شبکه‌های IoV 6G ارائه می‌کنیم که از فناوری دوقلوی دیجیتال و الگوریتم‌های هوش مصنوعی بهره می‌برد و تمرکز آن بر امنیت سایبری و کارایی محاسباتی است. تمایز اصلی کار ما، ارائه یک معماری لایه‌ای جامع شامل لایه داده، لایه دوقلوی سایبری، و لایه امنیت است که چالش‌های تحرک‌پذیری بالا و ناهمگونی شبکه‌های IoV 6G را برطرف می‌کند (طبق شکل ۲). ما از ماژول مهندسی ویژگی شامل ssAE برای کاهش مؤثر ابعاد داده و از ماژول یادگیری آنلاین برای ارائه عملکرد پایدار در شناسایی حملات استفاده می‌کنیم. این ماژول‌ها در لایه دوقلوی سایبری قرار دارند تا بار محاسباتی سیستم را به‌طور مؤثر تقسیم کنند. همچنین، ما یک سازوکار اشتراک‌گذاری خودکار بین RSU های همسایه معرفی می‌کنیم تا IP های مخرب میان آن‌ها به اشتراک گذاشته شود. مشارکت‌های اصلی مقاله به‌صورت خلاصه :- ارائه یک چارچوب هوشمند شناسایی حملات مبتنی بر دوقلوی دیجیتال برای مقابله با حملات در محیط IoV6G، به‌ویژه حملات هدفمند RSU ها- ارائه یک ماژول یادگیری آنلاین برای تضمین عملکرد پایدار و آگاه از وضعیت شبکه در شناسایی حملات شامل AutoFS و AutoCM - ارائه ماژول مهندسی ویژگی مبتنی بر ssAE برای کاهش ابعاد داده و تقسیم بار محاسباتی- معرفی سازوکار اشتراک‌گذاری خودکار اطلاعات بین RSU های همسایه برای تبادل IP های مخرب این مقاله، چارچوب ارائه‌شده در مقاله کنفرانسی ما [2] را با وارد کردن چندین پیشرفت مهم که برای شبکه‌های 6G طراحی شده‌اند، گسترش می‌دهد. در این مقاله، ما از یک ماژول مهندسی ویژگی، مؤلفه AutoCM در حالی که [2] تنها از پرسپترون چندلایه (MLP) برای طبقه‌بندی استفاده می‌کند(، تقسیم بار محاسباتی کلی سیستم بین لایه دوقلوی سایبری و لایه امنیت، و همچنین یک سازوکار خودکار ارتباط RSU همسایه . برخلاف [2] . بهره برده‌ایم. ماژول AutoFS در مقاله کنفرانسی شامل حذف بازگشتی ویژگی (RFE)، حذف ویژگی به‌صورت پسرو، کای‌دو، امتیاز فیشر، و



شکل ۱. تحلیل عملکرد راه‌حل‌های فعلی.

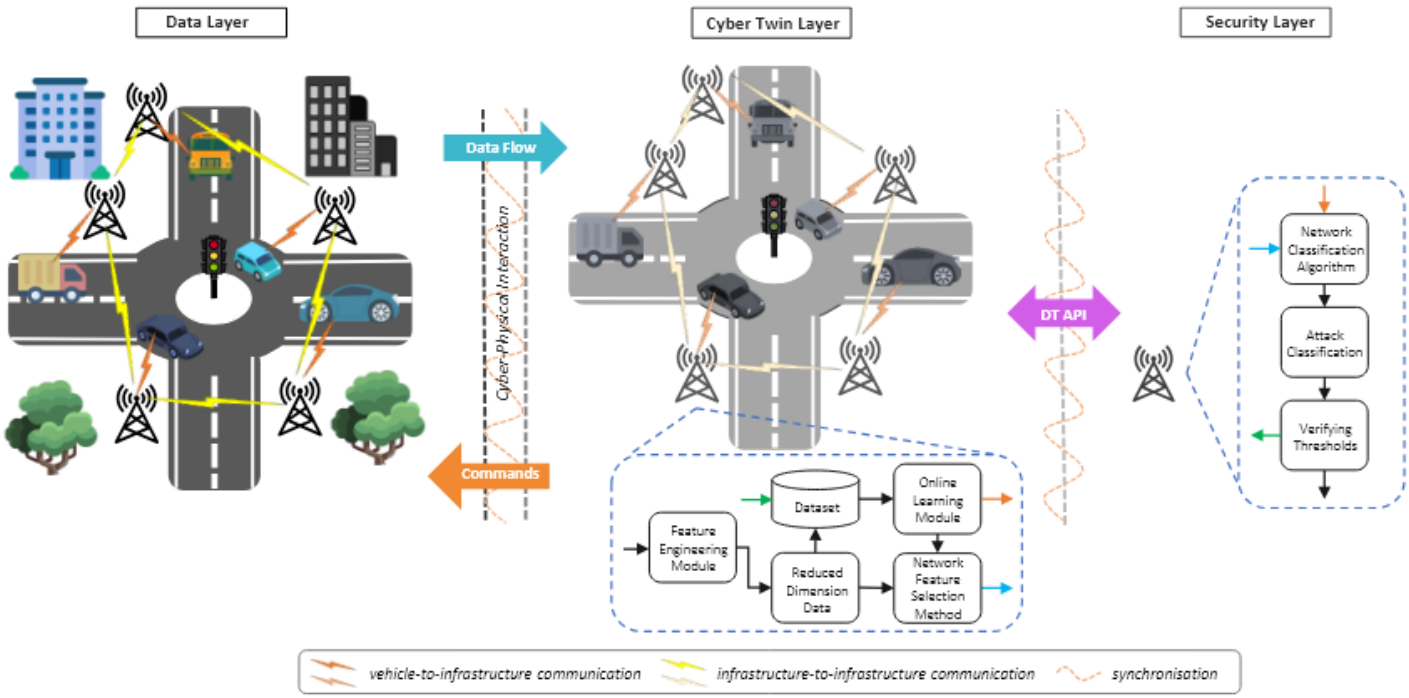
[8] [9]بنابراین، ایجاد سامانه‌های دفاعی پیشرفته برای محافظت از شبکه‌های VANET در برابر حملات و حفظ قابلیت‌اعتماد آن‌ها در عصر IoV 6G ضروری است. کارهای اخیر در زمینه شناسایی حملات شبکه‌های خودرویی با استفاده از فناوری دوقلوی دیجیتال [10]، [11] برای برآورده کردن شاخص‌های عملکردی شبکه‌های IoV 6G همچون نرخ تشخیص، دقت، و F1-Score کافی نیستند؛ همان‌گونه که در شکل ۱ نشان داده شده است. این راهکارها از *مدل‌های ایستا* استفاده می‌کنند، که برای شبکه‌های IoV 6G مناسب نیست؛ زیرا این شبکه‌ها نیازمند راهکارهای *پویا* برای مدیریت انواع مختلف حملات و ناهمگونی موجود در شبکه هستند. افزون بر این، عملکرد آن‌ها در برابر داده‌های مختلف *ناپایدار* است. برای نمونه، هنگام مقایسه‌ی نتایج عملکردی راهکارهای ارائه‌شده در [10]، [11] روی دو مجموعه‌داده، اختلافی در حدود ۱۵٪ مشاهده می‌شود. همچنین نتایج حاصل از الگوریتم‌های جنگل تصادفی و درخت تصمیم در [11] حدود ۲۵٪ اختلاف بین دو مجموعه‌داده نشان می‌دهد. بنابراین، راهکارهای کنونی پایدار نبوده و قادر به مدیریت حملات متنوع در محیط‌های پویا و دینامیک IoV 6G نیستند. در نتیجه، یک راهکار پیشرفته و پویا لازم است که بتواند حملات را به‌صورت دینامیک شناسایی کرده و عملکردی پایدار در محیط‌های IoV 6G ارائه دهد. چالش دیگر، بار محاسباتی بالا در راهکارهای فعلی شناسایی شبکه‌های خودرویی است، که مستقیم بر *تأخیر انتها به انتها* تأثیر می‌گذارد؛ پارامتری حیاتی برای زمان شناسایی حمله. رشد سامانه‌های ارتباطی خودرویی، بار محاسباتی را در محیط‌های IoV 6G افزایش داده است. پژوهش‌های کنونی در مورد شبکه‌های خودرویی بر پایه فناوری دوقلوی دیجیتال، بار سنگینی بر کل سامانه محاسباتی وارد می‌کنند؛ زیرا تمام عملیات محاسباتی در لایه سرویس دوقلوی دیجیتال انجام می‌شود [12]، [13]. در نتیجه، مقادیر تأخیر انتها به انتها، مصرف انرژی، میزان RAM و نرخ تحویل بسته‌ها در آن‌ها برای مدیریت شبکه‌های IoV 6G کافی نیست. برای عملکرد بهتر سیستم و

LSTMدوسویه مجهز به مکانیزم توجه را معرفی کرد که از دوقلوی دیجیتال برای تشخیص حملات در محیط vehicle-to-everythingاستفاده می‌کند. نویسندگان این چارچوب را با دو مجموعه‌داده شناخته‌شده IoT ارزیابی کردند؛ اما نتایج حدود 14٪ اختلاف بین مجموعه‌داده‌ها را نشان داد که اختلاف زیادی بوده و عملکردی ناپایدار در محیط پویا IoV ارائه می‌کند. افزون بر این، هیچ معیار بار محاسباتی نیز ارائه نشده است. در مطالعه‌ای دیگر [11] یک چارچوب مبتنی بر یادگیری عمیق برای تشخیص نفوذ در IoVپیشنهاد شد که از یک variational autoencoder پشته‌ای و LSTM دوسویه مبتنی بر توجه استفاده می‌کند. در این مطالعه، فناوری دوقلوی دیجیتال برای نگاشت سرورهای RSU و ساخت مدل ارتباطات خودرویی به‌کار رفت. این راهکار روی دو مجموعه‌داده شناخته‌شده ارزیابی شد؛ اما نتایج اختلافی حدود 15٪ بین مجموعه‌داده‌ها را نشان داد و عملکرد ناپایدار آن را در شبکه‌های پویا به‌اثبات رساند. همچنین، این کار نیز معیارهای بار محاسباتی را در نظر نگرفته است. نویسندگان [20] یک سامانه یادگیری تقویتی عمیق مبتنی بر LSTM و actor-critic را برای تشخیص حملات در سامانه‌های سایبر-فیزیکی vehicle-to-grid با بهره‌گیری از دوقلوی دیجیتال ارائه کردند. نتایج عملکرد برای ارزیابی کافی تشخیص حمله مناسب نیست. مدل مورد استفاده نیز ایستا بوده و هیچ روش به‌روزرسانی ندارد؛ بنابراین برای عملکرد پایدار در شبکه‌های پویای خودرویی مناسب نیست. در [21] یک سامانه honeypot مبتنی بر دوقلوی دیجیتال پیشنهاد شد که با ارائه بینش درباره حملات، امنیت را افزایش می‌دهد و توانایی خود در تشخیص و کاهش حملات هم‌زمان را نشان می‌دهد. این سامانه از روش به‌روزرسانی پویا برای مقابله با انواع حملات استفاده می‌کند؛ اما همچنان تمامی پردازش‌ها و الگوریتم‌ها در لایه سرویس دوقلوی دیجیتال انجام می‌شوند و برای شبکه 6 G IoVمناسب نیست. نویسندگان [22] رویکردی ترکیبی از یادگیری عمیق و رمزنگاری مبتنی بر هویت برای بررسی ناهنجاری‌ها در ارتباطات 6 G IoVارائه کردند. با وجود اینکه نرخ تشخیص حدود 97٪ گزارش شده است، ارزیابی تنها با یک مجموعه‌داده انجام شده و عملکرد آن در برابر مجموعه‌داده‌های مختلف نامشخص است. همچنین معیارهای بار محاسباتی سیستم نیز ارائه نشده‌اند. در [23] رویکردی نوین برای بهبود بهره‌وری انرژی و عملکرد عملیاتی هواگردهای بدون سرنشین (UAVs) در ارائه خدمات به IoT زمینی از طریق فناوری دوقلوی دیجیتال معرفی شد. برای ارائه توضیح شفاف‌تر درباره مراحل پیاده‌سازی دوقلوی دیجیتال در ویژگی‌های پویا محیط‌هایIoV ، از بینش‌های این مطالعه بهره گرفتیم. بررسی‌های فوق بر توانایی‌های مهم . اما کمتر بهره‌برداری‌شده . در ایمن‌سازی شبکه‌های IoV تأکید می‌کنند. با این حال، یک کمبود قابل‌توجه در ادغام کارآمد دوقلوهای دیجیتال و مدل‌های هوش مصنوعی برای تقویت امنیت و ارائه عملکرد پایدار در شبکه‌های 6 G IoVمشاهده می‌شود. یک سامانه تشخیص حمله پویا در محیط‌های IoV موردنیاز است تا بتواند با تغییرات داده‌های شبکه سازگار شود و در عین حال عملکردی پایدار در تشخیص حملات ارائه دهد. افزون بر این، مطالعات موجود مبتنی بر دوقلوی دیجیتال در شبکه‌های خودرویی نشان می‌دهند که بار سیستم...

الگوریتم انتخاب مقدار F آنووا (ANOVA) بود. پس از انجام آزمایش‌های جامع، در این مقاله حذف ویژگی به‌صورت پسرو و امتیاز فیشر را حذف کرده و آن‌ها را با تحلیل مؤلفه‌های اصلی (PCA)و الگوریتم اهمیت ویژگی جنگل تصادفی جایگزین کردیم، زیرا نتایج این دو بهتر بودند. ساختار باقی‌مانده این سند به این صورت است: بخش II مروری بر کارهای مرتبط ارائه می‌دهد. در بخشIII ، ابتدا مدل سیستم پیشنهادی خود را معرفی کرده و توضیح مفصلی ارائه می‌دهیم. سپس در بخش IV عملکرد راهکار خود را تحلیل کرده و در بخش V بحثی در این زمینه ارائه می‌کنیم. در نهایت، مقاله در بخش VI جمع‌بندی می‌شود.

II .کارهای مرتبط

در سال‌های اخیر، فناوری دوقلوی دیجیتال توجه قابل‌توجهی را در توسعه سامانه‌های حمل‌ونقل هوشمند به خود جلب کرده است. برای مثال، در [17] نقش دوقلوهای دیجیتال در خودروهای متصل و خودکار بررسی شده و بر پتانسیل آن‌ها برای متحول ساختن حوزه حمل‌ونقل از طریق فراهم‌سازی ارتباطات بلادرنگ و تحلیل‌های پیش‌بینی‌کننده تأکید می‌شود. یک چارچوب دوقلوی دیجیتال برای مدیریت ترافیک شهر هوشمند پیشنهاد شد که از داده‌های بلادرنگ برای بهینه‌سازی جریان ترافیک و افزایش ایمنی استفاده می‌کند. با این حال، این رویکرد عمدتاً بر کارایی ترافیک تمرکز دارد و فاقد سازوکارهای اختصاصی برای تشخیص حملات در شبکه‌های خودرویی است. به‌طور مشابه، همگرایی اینترنت اشیا (IoT) و فناوری‌های هوش مصنوعی مسیر را برای معماری‌های نوآورانه دوقلوی دیجیتال هموار کرده است. مطالعه [18] راهبردهای offloadingو cache کردن وظایف در سرورهای لبه‌ای نزدیک را برای کاهش تأخیر بررسی می‌کند و یک زیرساخت محاسباتی قدرتمند مبتنی بر ارتباطات فوق‌قابل‌اعتماد و کم‌تأخیر ایجاد می‌کند. با این حال، این کار نیز شامل هیچ روش مشخصی برای تشخیص حمله نیست. تنها تعداد محدودی از مطالعات موجود به شناسایی حملات با استفاده از فناوری دوقلوی دیجیتال در شبکه‌های خودرویی پرداخته‌اند. در [19] از الگوریتم ماشین بردار پشتیبان مبتنی بر دوقلوی دیجیتال برای شناسایی گره‌های مخرب استفاده شد. دوقلوهای دیجیتال برای شناسایی و حذف گره‌های مخرب در معماری VANET به‌کار گرفته شدند، اما این راهکار از یک مدل ایستا استفاده می‌کرد و قادر به سازگاری با ماهیت پویای شبکه خودرویی نبود. افزون بر این، این کار هیچ معیاری مرتبط با بار محاسباتی ارائه نمی‌کند که برای تشخیص مؤثر حملات ضروری است. مطالعه [13] یک سامانه مدیریت اعتماد غیرمتمرکز مبتنی بر بلاک‌چین را برای شناسایی خودروهای مخرب با استفاده از دوقلوهای دیجیتال پیشنهاد داد. با این حال، این روش نسبت به وضعیت شبکه آگاه نیست و بر اساس شرایط شبکه برای ارائه عملکرد پایدار در تشخیص حمله، خود را به‌روزرسانی نمی‌کند؛ بنابراین برای استفاده در شبکه‌های خودرویی مناسب نیست. همچنین عملکرد تنها از نظر سربار انتقال ارزیابی شده است که برای تعیین بار محاسباتی سیستم کافی نیست. مطالعه [10] یک چارچوب مبتنی بر بلاک‌چین و



شکل ۲. معماری سیستم پیشنهادی برای شبکه‌های IoV نسل ششم مقاوم در برابر حملات سایبری.

در این چارچوب، RSUها تمامی درخواست‌های ارتباطی وسایل نقلیه را که در محدودهٔ پوشش آن‌ها قرار دارند جمع‌آوری می‌کنند.

A. مدل‌سازی ریاضی ترافیکRSU

فرض می‌کنیم وسایل نقلیه کانال‌های مناسب یک RSU را در محدودهٔ پوشش آن به اشتراک می‌گذارند و هر وسیلهٔ نقلیه دارای اولویت برابر است؛ یعنی هیچ اولویتی میان آن‌ها وجود ندارد. برای مدل‌سازی درخواست‌های ارتباطی وسایل نقلیه، ما از مدل صف M/M/mاستفاده می‌کنیم که یک مفهوم بنیادین در نظریهٔ صف‌ها است. نظریهٔ صف، مطالعهٔ ریاضی صف‌ها یا خطوط انتظار است که به پیش‌بینی طول صف و زمان انتظار کمک می‌کند. مدل M/M/mبه‌طور مشخص یک سیستم با چند سرور (m) را نمایش می‌دهد که در آن ورودها از یک فرآیند پواسون پیروی می‌کنند و زمان‌های خدمت دارای توزیع نمایی هستند. در این پژوهش، مدل، درخواست‌های ارتباطی وسایل نقلیه را به‌صورت اولین وارد شده، اولین خارج‌شده (FIFO) در نظر می‌گیرد؛ یعنی درخواست‌ها دقیقاً به‌ترتیب ورود پردازش می‌شوند. جدول نام‌گذاری مدل در جدول I ارائه شده است که تعاریف نمادهای استفاده‌شده در سراسر مقاله را برای افزایش شفافیت و درک بهتر فرمول‌بندی‌های ریاضی فراهم می‌کند.

بررسی‌های فوق‌الذکر نشان می‌دهد که اگرچه قابلیت‌های چشمگیری برای ایمن‌سازی شبکه‌های IoV وجود دارد، این ظرفیت‌ها به‌طور کامل مورد بهره‌برداری قرار نگرفته‌اند. بااین‌حال، یک کمبود قابل توجه در یکپارچه‌سازی کارآمد دوقلوی دیجیتال و مدل‌های هوش مصنوعی برای تقویت امنیت و ارائه عملکرد پایدار در شبکه‌های 6G IoV مشاهده می‌شود. یک سیستم تشخیص حملهٔ پویا در محیط‌های IoV لازم است تا بتواند با تغییرات داده‌های شبکه سازگار شود و عملکرد تشخیص حملهٔ پایدار ارائه دهد. افزون بر این، مطالعات مبتنی بر دوقلوی دیجیتال در شبکه‌های خودرویی نشان می‌دهند که بار پردازشی سیستم به‌طور قابل ملاحظه‌ای بالا است، و این امر نیازمند توزیع بار برای بهبود عملکرد سیستم و امکان تشخیص سریع‌تر حملات می‌باشد. در این نقطه، فناوری دوقلوی دیجیتال می‌تواند به‌طور مؤثری برای تقسیم بار پردازشی در سراسر سیستم خودرویی به‌کار گرفته شود. در این مقاله، ما قصد داریم این دو نقص را برطرف کنیم و راهبردی نوآورانه برای ایمن‌سازی ارتباطات V2I و کاهش بار کاری در محیط‌های 6G IoV ارائه دهیم.

III. چارچوب پیشنهادی

جدول۱ نام‌گذاری(Nomenclature Table)

Symbol	Description
v_{num}	Number of ve… nding communication
c_{num}	Number of channels available at the RSU
λ	Arrival rate of communication demands
μ	Service rate of each channel per request
ρ	Traffic intensity
P_0	Probability of zero communication requests
P_{vnum}	Probability of having v_{num} vehicles
$\wp$	Probability that all requests are accepted
ξ	Probability that requests are queued
P_{Queue}	Probability of a communication request waiting
T_{AVGQ}	Average waiting time in the queue
Θ	Sparsity constraint weighting factor
σ	Nonlinear activation function used in neural networks
W_{ij}	ssAE weight matrix between input and hidden layers
W_{jk}	ssAE weight matrix between hidden and output layers
φ_1, φ_2	Bias vectors for hidden and output layers in ssAE
ρ	Predefined sparsity parameter in the ssAE algorithm
$J(W,b)$	Loss function for reconstruction error in ssAE
$J_{\text{sparse}}(W,b)$	Total loss function with sparsity penalty in ssAE
λ	Weight attenuation coefficient in ssAE loss function
γ_i	Threshold factor for the i-th classification algorithm
$\mathcal{V}(\mathcal{I})$	Verifying threshold function for system reliability
$\mathcal{R}$	System reliability metric

تغییرات مبتنی بر میزان دسترسی کانال‌های ارتباطی و ورود درخواست‌های جدید را نمایش می‌دهد. برای مثال، زمانی که تعداد درخواست‌های خودروها کمتر یا برابر با تعداد کانال‌های در دسترس باشد(vnum ≤ cnum) ، RSU می‌تواند تمام این درخواست‌ها را به طور مستقیم پردازش کند و همهٔ درخواست‌ها پذیرفته می‌شوند. در مقابل، اگر تعداد درخواست‌ها بیشتر از کانال‌های موجود باشد (vnum > cnum)، درخواست‌های اضافی در صف قرار می‌گیرند و طبق سیاست اولین ورودی–اولین خروجی (FIFO) منتظر می‌مانند. این سازوکار تضمین می‌کند که تمام درخواست‌ها در نهایت با آزاد شدن کانال‌ها سرویس‌دهی شوند. این نمودار، شاخص‌های کلیدی مانند: احتمال بی‌کار بودن سیستم(P_0) احتمال حضور تعداد مشخصی از درخواست‌ها در حال پردازش(P_{vnum}) میانگین زمان انتظار در صف(T_AVG^Q) را به‌صورت بصری نمایش می‌دهد. با تحلیل این احتمالات و زمان‌های انتظار، نمودار نشان می‌دهد که RSUچگونه به‌صورت کارآمد، سطح‌های متفاوت تقاضای ارتباطی را مدیریت می‌کند. معادلهٔ (۱) احتمال وجود تعداد مشخصی خودرو (vnum) را در سیستم توصیف می‌کند و در آن تعداد کانال‌های قابل دسترس(cnum) ، نرخ سرویس‌دهی (μ) و نرخ ورود درخواست‌ها (λ) نیز در نظر گرفته شده‌اند.

$$P_{v_{num}-1} = min(v_{num}, c_{num})\frac{\mu P_{v_{num}}}{\lambda}, \ \forall\, v_{num} \in [1, .., v_{tot}] \quad (1)$$

در این رابطه، vtotنشان‌دهندهٔ تعداد کل خودروها است. احتمال اشغال بودن تمامی کانال‌ها با استفاده از معادلهٔ (۲) محاسبه می‌شود.

$$P_{v_{num}} = P_0\frac{(c_{num}\rho)^{v_{num}}}{v_{num}\ !}, \ \forall\, v_{num} \in [0, 1, .., c_{num}] \quad (2)$$

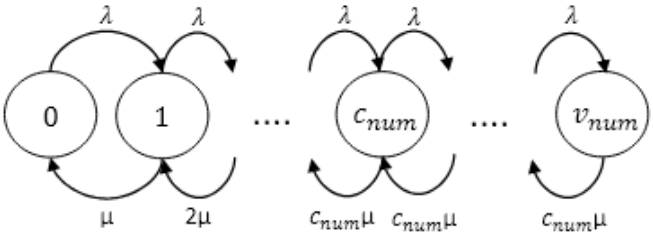
که در آن P_0احتمال صفر بودن درخواست‌های ارتباطی در سیستم را نشان می‌دهد، که مقدار آن در معادلهٔ (۴) ارائه شده است. همچنین، ρ شدت ترافیک (Traffic Intensity) است که مقدار آن با استفاده از معادلهٔ (۳) محاسبه می‌شود.

$$\rho = \frac{\lambda}{c_{num}\mu} \quad (3)$$

$$P_0 = \left[\sum_{v_{num}=0}^{c_{num}-1}\frac{(c_{num}\rho)^{v_{num}}}{v_{num}\ !} + \frac{(c_{num}\rho)^{c_{num}}}{c_{num}\ !(1-\rho)}\right]^{-1} \quad (4)$$

احتمال حضور vnumوسیله نقلیه در سیستم با استفاده از Pvnumمحاسبه می‌شود $\wp$.نشان‌دهندهٔ احتمال پذیرفته‌شدن تمامی درخواست‌های ارتباطی است که مقدار آن در معادلهٔ (۵) ارائه شده است. همچنین ξاحتمال انتظارِ درخواست ارتباطی در صف را نشان می‌دهد که مقدار آن در معادلهٔ (۶) بیان شده است.

تعداد درخواست‌های ارتباطی در هر بازهٔ زمانی برای توصیف وضعیت سیستم استفاده می‌شود. سرورها به‌صورت کانال‌ها مدل‌سازی شده‌اند. در هر بازهٔ زمانی، مجموع تعداد درخواست‌های ارتباطی با تعداد کانال‌های در دسترس در همان بازه مقایسه می‌شود. اگر هیچ کانالی برای ارائهٔ سرویس موجود نباشد، درخواست‌ها تا بازهٔ زمانی بعدی نگه داشته می‌شوند تا دوباره وضعیت دسترس‌پذیری کانال‌ها بررسی شود. شکل ۳ نمودار حالت را نشان می‌دهد که تقاضاهای ارتباطی خودروها در محدودهٔ پوشش یک RSU را با استفاده از مدل صف M/M/mنمایش می‌دهد. این مدل به درک جریان و پردازش درخواست‌های ارتباطی کمک می‌کند، جایی که هر درخواست خودرو بر اساس در دسترس بودن کانال‌ها پردازش می‌شود. در این مدل cnum :تعداد کانال‌های RSU را نشان می‌دهد، vnumتعداد خودروهایی را نشان می‌دهد که درخواست ارتباط دارند، λنرخ ورود درخواست‌های ارتباطی را نشان می‌دهد، μ نرخ سرویس‌دهی هر کانال را نشان می‌دهد که وابسته به زمان است.



شکل ۳ .نمودار حالت مربوط به تقاضاهای ارتباطی خودروها در محدودهٔ پوشش.RS*U*

در این نمودار، هر حالت نشان‌دهندهٔ وضعیت مشخصی از RSU هنگام پردازش درخواست‌های ارتباطی است. انتقال بین حالت‌ها

خواهد شد. این فرایند موجب می‌شود RSU بتواند در عین حفظ امنیت، مدیریت ترافیک ارتباطی را نیز به‌صورت کارآمد انجام دهد.

C. Proposed Attack Detection

معماری سیستم پیشنهادی برای تشخیص حملات، بر اساس یک طراحی لایه‌ای توسعه یافته است و تعاملات میان لایه‌های فیزیکی و دیجیتال را با هدف ایجاد یک چارچوب امنیتی جامع در شبکه‌های 6 IoV Gادغام می‌کند. این معماری شامل سه لایه اصلی است:

1. لایه داده(Data Layer)
2. لایه همزاد سایبری(Cyber Twin Layer)
3. لایه امنیتی(Security Layer)

همان‌گونه که در شکل 2 نشان داده شده، هر یک از این لایه‌ها نقش کلیدی در امنیت و کارکرد کلی شبکه 6 IoV Gایفا می‌کنند. یکی از نوآوری‌های مهم سیستم پیشنهادی، استفاده از ماژول یادگیری آنلاین (Online Learning Module) است که امکان بازآموزی مداوم مدل‌ها را با استفاده از جدیدترین داده‌های ترافیکی فراهم می‌کند. این ویژگی موجب می‌شود سیستم بتواند در برابر تغییرات تاکتیکی مهاجمان همواره به‌روز باقی بماند و نرخ تشخیص حملات را افزایش دهد. علاوه بر این، معماری پیشنهادی با چارچوب IETF Digital Twin Network Architectureسازگار بوده و طراحی آن با اصول و استانداردهای شبکه‌های همزاد دیجیتال در حوزه ITSو IoV هماهنگ است. همچنین، این ساختار به‌گونه‌ای توسعه یافته که امکان توزیع بار پردازشی میان لایه‌ها را فراهم کرده و در نتیجه موجب تسریع در تشخیص حملات و کاهش بار محاسباتی RSUهای فیزیکی می‌شود.

(به دلیل حجیم بودن شکل در صفحه بعد بارگذاری میشود)

$$P_{v_{num}} = \begin{cases} \wp, & v_{num} \le c_{num} \\ \xi, & v_{num} > c_{num} \end{cases}$$

$$\wp = P_0 \frac{(c_{num}\rho)^{v_{num}}}{v_{num}\ !} \tag{5}$$

$$\xi = P_0 \frac{(c_{num})^{c_{num}}(\rho)^{v_{num}}}{c_{num}\ !} \tag{6}$$

احتمال انتظار یک درخواست ارتباطی در صف با استفاده از فرمول Erlang Cبه‌صورت زیر محاسبه می‌شود:

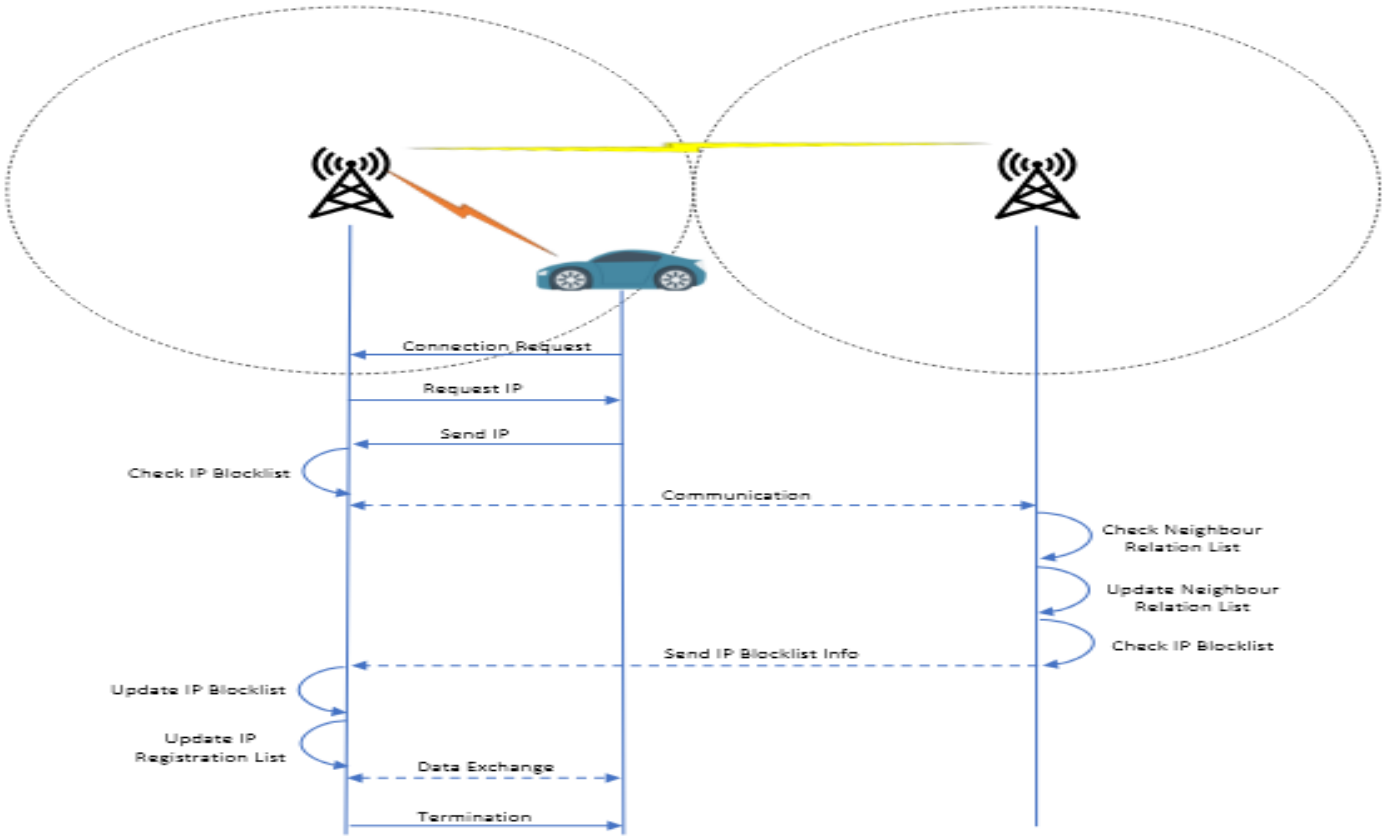
$$P_{Queue} = \frac{P_0\ (c_{num}\rho)^{c_{num}}}{c_{num}\ !\ (1-\rho)} \tag{7}$$

زمان میانگین انتظار در صف برای یک درخواست ارتباطی در مدل صف M/M/mبا استفاده از فرمول Erlang C به‌صورت زیر محاسبه می‌شود:

$$T_{AVG_Q} = \frac{\rho\, P_{Queue}}{\lambda\,(1-\rho)} \tag{8}$$

B. Automated Neighbour RSU Relations

پس از مدل‌سازی درخواست‌های ارتباطی مربوط به هرRSU ، گام بعدی در چارچوب پیشنهادی ما بررسی روابط میانRSU های همسایه است. در سیستم پیشنهادی، هر RSU یک فهرست مسدودسازی IP اختصاصی در اختیار دارد که شامل آدرس‌های IP مربوط به وسایل نقلیه مخربِ شناسایی‌شده در گذشته است. به منظور افزایش کارایی سازوکارهای امنیتی، ما یک سازوکار رابطه خودکار میانRSU های همسایه تعریف می‌کنیم که مشابه با کار پیشین ما در [24] است؛ با این تفاوت که هدف اصلی در این پژوهش اشتراک‌گذاری خودکار آدرس‌های IP مخرب میانRSU های همسایه است. شکل 4، نمودار توالی سازوکار پیشنهادی برای ایجاد رابطه خودکار میانRSU های همسایه را نشان می‌دهد. این سازوکار هنگام دریافت یک درخواست اتصال از سوی یک وسیله نقلیه فعال می‌شود. در مرحله نخست، RSUآدرس IP فرستنده را با فهرست مسدودسازی داخلی خود مقایسه می‌کند. سپس، برای افزایش دقت شناسایی تهدیدات، فهرست مسدودسازیRSU های همسایه نیز بررسی می‌شود. اگر IP موردنظر در هیچ‌یک از فهرست‌ها وجود نداشته باشد، سامانه هوشمند تشخیص حمله آغاز به‌کار می‌کند تا مشخص کند آیا درخواست شامل نشانه‌ای از حمله سایبری است یا خیر. در صورتی که حمله‌ای تشخیص داده نشود، درخواست ارتباطی مطابق با شرایط $\wp$در رابطه (5) به یکی از کانال‌های در دسترس RSU تخصیص می‌یابد. اگر کانال آزاد موجود نباشد، درخواست مطابق با وضعیت ξدر رابطه (6) وارد صف انتظار



شکل 4. نمودار توالی سازوکار خودکار رابطه میانRSU های همسایه برای فهرست آدرس‌های IP وسایل نقلیه مخرب در شبکه‌های G IoV6

لایهٔ داده به‌عنوان لایهٔ پایه‌ای چارچوب، نقش حیاتی در جمع‌آوری و توزیع اطلاعات در لایه‌های مختلف شبکهٔ خودرویی 6 Gدارد. این لایه با ادغام مؤثر خودروها وRSU ها، داده‌هایی گردآوری می‌کند که از یک نمایش دقیق از اشیای فیزیکی در لایهٔ دوقلوی سایبری و نیز از ارزیابی‌های امنیتی راهکار پیشنهادی پشتیبانی می‌کنند. دقت لایهٔ داده در نمایش بلادرنگ و ارتباطات، برای حفظ کارایی و یکپارچگی سیستم مبتنی بر دوقلوی دیجیتال ضروری است.

2.لایهٔ دوقلوی سایبری

لایهٔ دوقلوی سایبری نقشی کلیدی در ایجاد مدل‌های دیجیتال پویا دارد که عناصر فیزیکی شبکه‌های 6 IoV Gرا بازتاب می‌دهند و به افزایش سازگاری و دقت سیستم در تطبیق با شرایط واقعی کمک می‌کنند. این لایه عملیات مهندسی ویژگی را انجام می‌دهد تا بار پردازشی لایهٔ امنیتی کاهش یابد. این لایه شامل ماژول مهندسی ویژگی و ماژول یادگیری آنلاین است.

اصل *Gemini* با تعریف شفاف هدف، تضمین اعتماد و ارائهٔ کارکردهای حیاتی برای شبکه‌های 6 IoV Gهم‌راستا است. هدف این چارچوب، ارتقای امنیت و کارایی شبکه‌های خودرویی است و به ضرورت راهکارهای سازگارپذیر در محیط‌های پویای IoV پاسخ می‌دهد. اعتماد از طریق یکپارچه‌سازی تحلیل‌های مبتنی بر هوش مصنوعی و پردازش داده‌های بلادرنگ ایجاد می‌شود و این امر تشخیص تهدیدات را دقیق و قابل‌اطمینان می‌سازد. از نظر کارکردی، این چارچوب در چندین لایه فعالیت می‌کند که هر لایه نقش مهمی در دستیابی به هدف اصلی یعنی ارائهٔ امنیت مقاوم، کارآمد و مقیاس‌پذیر برای شبکه‌های خودرویی نسل بعدی دارد. با تمرکز بر این مؤلفه‌های اصلی، این چارچوب گامی مهم در به‌کارگیری فناوری دوقلوی دیجیتال در سامانه‌های حمل‌ونقل هوشمند به شمار می‌رود و عملکرد و تاب‌آوری بهبودیافته‌ای را در برابر تهدیدهای سایبری ارائه می‌دهد.

1 .لایهٔ داده

ماژول مهندسی ویژگی

این ماژول از یک الگوریتم ssAEبرای کاهش ابعاد ویژگی‌های داده استفاده می‌کند .یک معماری پیشرفتهٔ شبکهٔ عصبی است که عمدتاً برای کاهش ابعاد و استخراج ویژگی به‌کار می‌رود. در این ساختار، چندین لایهٔ خودرمزگذار پراکنده روی یکدیگر قرار می‌گیرند؛ به‌گونه‌ای که خروجی هر لایه ورودی لایهٔ بعدی است. این ساختار سلسله‌مراتبی کمک می‌کند تا شبکه بتواند به‌تدریج ویژگی‌های پیچیده‌تر و سطح‌بالاتری از داده را بیاموزد.

عملکرد ssAE شامل دو مرحلهٔ اصلی است :کدگذاری و بازکدگذاری. در مرحلهٔ کدگذاری، شبکه داده‌های ورودی Xرا به یک نمایش کم‌بُعدتر Hبا استفاده از تبدیل زیر فشرده می‌کند:

$$H = \sigma(W_{ij}X + \phi_1) \tag{9}$$

که در آن Wijماتریس وزن بین لایه ورودی و لایه پنهان در ssAE را تعریف می‌کند، σیک تابع فعال‌ساز غیرخطی است، و φ1بردار بایاس برای لایه پنهان می‌باشد. مرحلهٔ کدگشایی (Decoding) تلاش می‌کند دادهٔ ورودی را از شکل فشرده‌شدهٔ آن بازسازی کند و بازسازی‌ای به نام Yرا از طریق تبدیل زیر تولید می‌کند:

$$Y = \sigma(W_{jk}H + \phi_2) \tag{10}$$

که در آن بردار بایاس برای لایهٔ خروجی با φ2نشان داده می‌شود و ماتریس وزن از لایهٔ پنهان به لایهٔ خروجی با Wjkتعریف می‌گردد. هدف، کمینه‌سازی خطای بازسازی است تا شبکه تشویق شود اطلاعات ضروری را حفظ کرده و نویز را حذف نماید. علاوه بر این، ssAEیک قید پراکندگی (sparsity constraint) بر فعال‌سازی لایهٔ پنهان اعمال می‌کند تا اطمینان حاصل شود که تنها بخش کوچکی از نورون‌ها در هر زمان فعال باشند. این امر با جریمه‌کردن انحراف میانگین فعال‌سازی نورون‌های پنهان از یک پارامتر پراکندگی از پیش تعیین‌شده ρ، با استفاده از واگرایی کولبک–لایبلر(Kullback–Leibler divergence) [25] به دست می‌آید. تابع هزینهٔ کلی ssAEترکیبی از خطای بازسازی و جریمهٔ پراکندگی است و بدین ترتیب استخراج نمایش‌های فشرده و معنادار از داده‌های با ابعاد بالا را تسهیل می‌کند.

$$J_{\text{sparse}}(W,b) = J(W,b) + \Theta \sum_{j=1}^{m} \text{KL}\left(\rho \middle\| \hat{\rho}_j\right) \tag{11}$$

که در آن mتعداد واحدهای پنهان را نشان می‌دهد، در حالی که Θیک عامل وزنی است که شدت این مؤلفه را تعیین می‌کند. علاوه بر این، برای جلوگیری از بیش‌برازش(overfitting) ، تابع خطا شامل ترم‌های کاهش وزن (weight decay) نیز می‌باشد [25]

$$J_{\text{sparse}}(W,b) = J_E(W,b) + \Theta \sum_{j=1}^{m} \text{KL}\left(\rho \middle\| \hat{\rho}_j\right) + \frac{\lambda}{2} \sum_{r=1}^{3} \sum_{i=1}^{m} \sum_{j=1}^{m+1} (w_{ij}^{r})^2 \tag{12}$$

که در آن λضریب تضعیف وزن‌ها (weight attenuation coefficient)را نشان می‌دهد. الگوریتم 1 شبه‌کد (pseudocode)مربوط به الگوریتم ssAE را نمایش می‌دهد و بیان می‌کند که ماژول ssAE ما برای کاهش بُعد داده‌ها این الگوریتم را اجرا می‌کند. ابتدا ورودی‌ها و خروجی‌ها در خطوط ۱ و ۲ مشخص می‌شوند. سپس لایه‌های رمزگذار (encoder) و رمزگشا (decoder)در خطوط ۴ و ۵ مقداردهی اولیه می‌شوند. خطوط ۶ تا ۹ دادهٔ رمزگذاری‌شده را برای هر لایه از ۱ تا k نشان می‌دهند. سپس نمایش نهایی رمزگذاری‌شده Xkبه‌عنوان Yتنظیم می‌شود که همان دادهٔ کاهش‌بُعد یافته است. دادهٔ رمزگذاری‌شده برای بازسازی ورودی رمزگشایی می‌شود. در خط ۱۳، برای هر رمزگشا از k رو به ۱، رمزگشایi ام روی خروجی لایهٔ بعدی یا روی نمایش نهایی رمزگذاری‌شده اعمال می‌شود (اگر اولین رمزگشا در توالی باشد). در نهایت، الگوریتم دادهٔ کاهش‌بُعد یافته Yرا بازمی‌گرداند. پس از کاهش تعداد ویژگی‌ها در ماژولssAE ، داده‌های کم‌بعد به ماژول یادگیری آنلاین ارسال می‌شوند تا روش انتخاب ویژگی و روش طبقه‌بندی مناسب شبکه تعیین شود. ماژول یادگیری آنلاین شامل یک الگوریتم برچسب‌گذاری از مطالعهٔ قبلی ما [26]، یک مؤلفهٔ AutoFS، یک عنصر AutoCMو یک الگوریتم انتخاب نهایی است. ما مؤلفه‌های AutoFS و AutoCM را از کارهای قبلی‌مان [27], [28] گرفته‌ایم و آن‌ها را متناسب با نیازهای خاص محیط G IoV 6 به‌روزرسانی کرده‌ایم. به لطف این ماژول، سیستم ما به‌صورت آگاه از شبکه (network-aware) کار می‌کند.

Algorithm 1 Feature Dimension Reduction using ssAE.

1: **Input:** for every data point $X \in \mathbb{R}^{n \times m}$, n stands the number of samples, and m is the number of features
2: **Output:** Reduced dimension data Y
3: **procedure** ssAE(X)
4: Initialise encoder layers $E_1, E_2, ..., E_k$
5: Initialise decoder layers $D_1, D_2, ..., D_k$
6: **for** $i = 1$ to k **do**
7: $X_i \leftarrow$ Apply encoder E_i to X or X_{i-1} if $i > 1$
8: $X_i \leftarrow$ Apply sparsity constraint to X_i
9: **end for**
10: *# Encoded representation with reduced dimension*
11: $Y \leftarrow X_k$
12: **for** $i = k$ down to 1 **do**
13: $Y \leftarrow$ Apply decoder D_i to Y
14: **end for**
15: **return** Y
16: **end procedure**

این به‌روزرسانی‌ها تضمین می‌کند که الگوریتم برچسب‌گذاری با جدیدترین رفتارهای شبکه و تهدیدهای نوظهور همسو باقی بماند. با همگام‌سازی مداوم با الگوهای داده‌ای روز، سیستم دقت و سازگاری بالای خود را حتی در شرایط پرتلاطم و متغیر محیط‌های 6 IoV Gحفظ می‌کند.

اگر هر یک از معیارهای عملکردی کمتر از آستانه تعیین‌شده خود قرار گیرد، ماژول یادگیری آنلاین روش انتخاب ویژگی شبکه (FS) و روش طبقه‌بندی شبکه (CM) را به‌روزرسانی می‌کند. برای این منظور، این ماژول از طریق الگوریتم‌های برچسب‌گذاری و انتخاب نهایی، هزار نمونه از داده‌های فعلی شبکه را پردازش می‌کند. این اطلاعات به‌روزرسانی از لایه امنیتی دریافت می‌شود؛ لایه‌ای که مسئول بررسی میزان قابلیت اطمینان و سلامت سیستم است.

پس از دریافت اطلاعات به‌روزرسانی از لایه امنیتی، هزار نمونه از داده‌های فعلی شبکه وارد ماژول یادگیری آنلاین می‌شود. این داده‌ها ابتدا با استفاده از الگوریتم برچسب‌گذاری، برچسب‌دار می‌شوند. پس از برچسب‌گذاری، مؤلفه AutoFS از این داده‌های برچسب‌دار استفاده می‌کند. سپس خروجی AutoFS به عنصر AutoCM ارسال می‌شود.

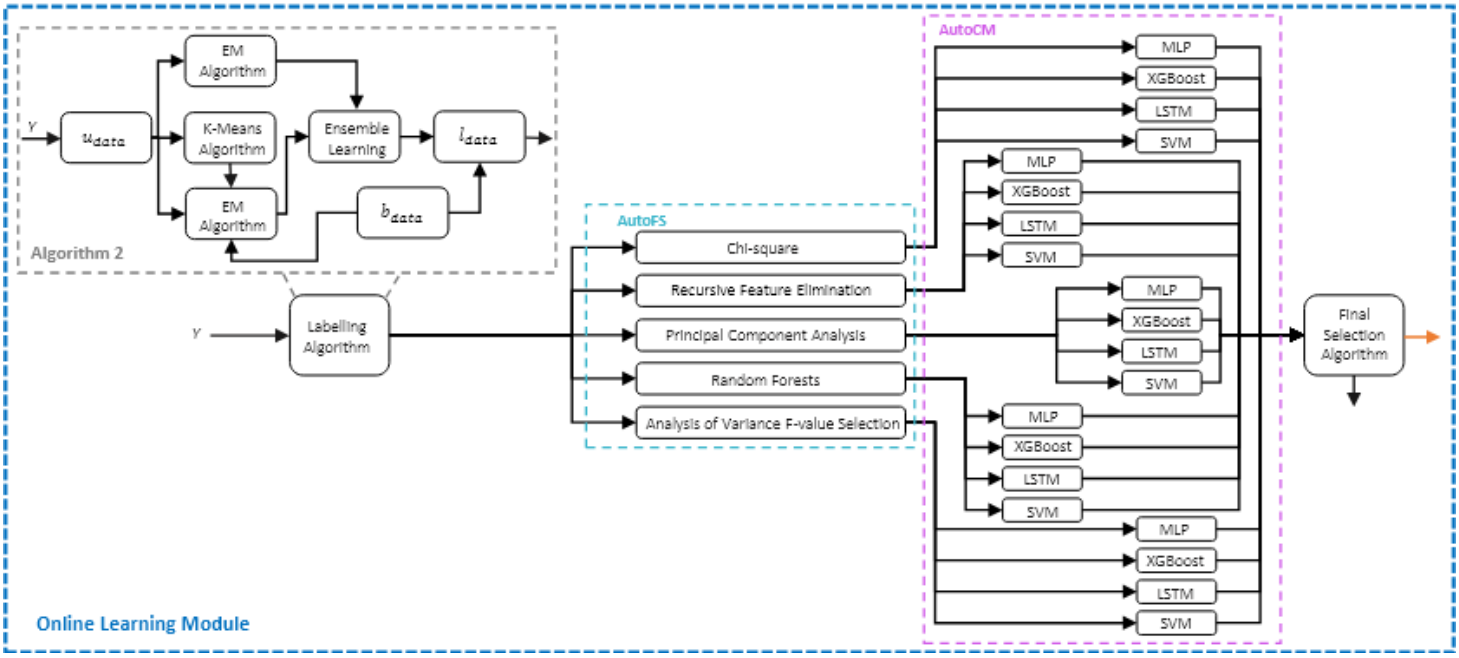
عنصر AutoCM داده‌ها را به‌صورت جداگانه برای هر الگوریتم آموزش داده و ارزیابی می‌کند. پس از آن، مقادیر دقت(precision) ، بازیابی (recall) و زمان تشخیص هر الگوریتم را به الگوریتم انتخاب نهایی ارسال می‌کند. منطق کاری ماژول یادگیری آنلاین در شکل ۵ نمایش داده شده است.

الگوریتم ۳ شبه‌کد الگوریتم انتخاب نهایی ما را ارائه می‌دهد. این الگوریتم، با توجه به معیارهای دقت(precision) ، بازیابی (recall)و زمان تشخیص الگوریتم‌ها، دربارهٔ انتخاب روش‌های انتخاب ویژگی (FS) و طبقه‌بندی (CM) شبکه تصمیم‌گیری می‌کند.

الگوریتم انتخاب نهایی، اطلاعات مربوط به بهترین روش FS را به روش انتخاب ویژگی شبکه در لایه دوقلوی سایبری ارسال می‌کند، و سپس روش FS شبکه با الگوریتم جدید شروع به کار می‌کند. همچنین، الگوریتم انتخاب نهایی اطلاعات مربوط به بهترین تکنیک CMرا به الگوریتم طبقه‌بندی شبکه در لایه امنیتی ارسال می‌کند و این لایه نیز با روش جدید فعالیت خود را آغاز می‌نماید.

مولفهٔ AutoFSشامل پنج الگوریتم انتخاب ویژگی (FS) است :کای-دو(chi-square) ، حذف بازگشتی ویژگی‌ها(RFE) ، تحلیل مؤلفه‌های اصلی(PCA) ، جنگل تصادفی برای اهمیت ویژگی‌ها، و انتخاب ویژگی بر اساس مقدار F آنووا .(ANOVA F-value) هر الگوریتم برای انواع خاصی از داده و نیازهای متفاوت طراحی شده است و به سیستم اجازه می‌دهد تا بر اساس ویژگی‌های داده‌های جاری و شرایط شبکه، به‌صورت پویا مناسب‌ترین روش را انتخاب کند. مولفهٔ AutoCMشامل چهار روش طبقه‌بندی (CM) است : MLP، XGBoost، LSTMو ماشین‌های بردار پشتیبان (SVM) تا انعطاف‌پذیری و سازگاری لازم برای مدیریت انواع مختلف سناریوهای حمله در محیط‌های 6 IoV Gرا فراهم کند. هر الگوریتم برای هدفی خاص به کار می‌رود MLP :برای شناسایی الگوهای پیچیده، XGBoostبرای تحلیل کارآمد داده‌های ساخت‌یافته، LSTMبرای تشخیص الگوهای ترتیبی، و SVM برای طبقه‌بندی در فضاهای با ابعاد بالا. از آنجا که ما از الگوریتم‌های یادگیری نظارت‌شده استفاده می‌کنیم، یک الگوریتم برچسب‌گذاری نیز تعریف می‌کنیم تا هنگام به‌روزرسانی روش‌های FSو CM شبکه، داده‌های بدون برچسب را برچسب‌گذاری کند. این الگوریتم از هزار نمونه از داده‌های جاری شبکه — که با udata در Yنمایش داده شده — و هزار نمونه از داده‌های مبنا — که با bdataمشخص شده — استفاده می‌کند. شبه‌کد این الگوریتم در الگوریتم ۲ آمده است. ابتدا ورودی‌ها و خروجی‌ها در خطوط ۱ تا ۲ مشخص می‌شوند. سپس خوشه‌بندی K-Means برای جداسازی اولیه udata به دو گروه استفاده می‌شود (K = 2) تا داده‌ها بر اساس احتمال وجود یا عدم وجود حمله دسته‌بندی شوند (خطوط ۵-۴). این خوشه‌های اولیه برای پیکربندی الگوریتم انتظار–بیشینه‌سازی (EM)به‌کار گرفته می‌شوند. الگوریتم EM در خط ۹ برای اختصاص برچسب‌های احتمالاتی اعمال می‌شود. پس از آن، bdataبرای افزایش دقت برچسب‌گذاری استفاده می‌شود و یک فرآیند EM دوم برای برچسب‌گذاری بهینه انجام می‌گیرد.

در نهایت، برچسب‌های جدید ’lبا داده‌های مبنا bdataادغام شده و داده‌های کاملاً برچسب‌گذاری‌شده ldataدر خطوط ۱۸-۱۶ بازگردانده می‌شوند. این الگوریتم نقش بسیار مهمی در به‌روزرسانی پویا روش‌های چارچوب ما دارد. ما دقت این الگوریتم را با استفاده از تکنیک‌های اعتبارسنجی متقابل (cross-validation) به‌طور دقیق ارزیابی کرده‌ایم. در مجموعه‌ای از ارزیابی‌ها، این الگوریتم به دقت الگوریتم برچسب‌گذاری به دقتی در حدود ٪۹۷٫۲۱ دست یافته است؛ این معیار بسیار مهم است زیرا تضمین می‌کند که سیستم قادر است داده‌های جدید و در حال تغییر را به‌درستی پردازش و طبقه‌بندی کند. دقت بالای برچسب‌گذاری به‌طور مستقیم باعث بهبود عملکرد ماژول انتخاب ویژگی (FS) و الگوریتم‌های طبقه‌بندی می‌شود و در نتیجه شناسایی تهدیدهای بالقوه در محیط 6 IoV Gبا دقت بیشتری انجام می‌گیرد. برای حفظ این سطح از عملکرد در طول زمان، مجموعه‌داده‌ی مبنا در بازه‌های زمانی از پیش تعیین‌شده به‌روزرسانی می‌شود.



شکل ۵. منطق کاری ماژول یادگیری آنلاین پیشنهادی.

چندین الگوریتم، ما از یک معماری مبتنی بر ریزخدمات (microservice) استفاده می‌کنیم که در آن اجزای مختلف ماژول یادگیری آنلاین به‌عنوان سرویس‌های مستقل و کوچک‌تر اجرا می‌شوند. این رویکرد مقیاس‌پذیری را افزایش می‌دهد و امکان مدیریت مؤثر اجزای مختلف را فراهم می‌سازد.

Algorithm 2 Labelling Algorithm.

Input: unlabelled data (u_{data}), baseline dataset (b_{data})
Output: labelled data (l_{data})
procedure LABEL(u_{data}, b_{data})
    Define $K = 2$ for K-Means algorithm
    Cluster u_{data} into two groups using K-Means
    # to determine the range of initial values
    Use the clusters for EM
    # to assign weighted probabilistic labels to u_{data}
    $x' \leftarrow$ Apply EM algorithm
    # b_{data} *includes 65% attack samples*
    Use b_{data} with its one thousand samples
    # to find the local maximum likelihood estimation
    $y' \leftarrow$ Combine b_{data} and u_{data}
    $y'' \leftarrow$ Apply the other EM algorithm using y'
    # to decide the final labels, take both EM outputs
    $l' \leftarrow$ Use ensemble learning x' and y''
    $l_{data} \leftarrow$ Merge l' with the b_{data}
    Return l_{data} with two thousand samples
end procedure

Algorithm 3 Final Selection Algorithm

Input: precision (P), recall (R), and detection time (d_t) for each CM method and its pair FS techniques
Output: $bestFS$ and $bestCM$ for the system
procedure FINAL-METHODS(P, R, d_t)
    # to store precision, recall, and detection time for each FS and CM combination
    Initialize matrix M
    for $i = 1$ to 5 **do**
        for $j = 1$ to 4 **do**
            # metric vector for i^{th} *FS and* j^{th} *CM*
            $V_{ij} \leftarrow$ vector of P, R, d_t
            $M[i, j] \leftarrow V_{ij}$
        end for
    end for
    # α_{ij}, β_{ij} *are the weights for* i^{th} *FS and* j^{th} *CM*
    # ψ_{ij} *is the weighted sum of P and R*
    $bestFS$, $bestCM \leftarrow$ 0, 0
    $maxScore \leftarrow -\infty$
    for $i = 1$ to 5 **do**
        for $j = 1$ to 4 **do**
            $\psi_{ij} \leftarrow$ (%55) $\times$ R + (%45) $\times$ P
            $score_{ij} \leftarrow \alpha_{ij} \times \psi_{ij} + \beta_{ij} \times d_t$
            if ($score_{ij} > maxScore$)
            $maxScore \leftarrow score_{ij}$
            $bestFS$, $bestCM \leftarrow$ i, j
            end if
        end for
    end for
    Return $bestFS$, $bestCM$
end procedure

این انتخاب سازگارپذیر تضمین می‌کند که سیستم بتواند به‌طور کارآمد به تهدیدات نوظهور یا تغییرات موجود در داده‌ها و محیط شبکه واکنش نشان دهد و کارایی بالا را در تشخیص حملات و بهره‌وری سیستم حفظ کند. بنابراین، سازوکار یادگیری آنلاین، عملکرد پایدار سیستم را به‌صورت شبکه‌آگاه حفظ می‌کند. این سازوکار تقریباً در زمان واقعی کار می‌کند. برای مدیریت کارآمد بار محاسباتی ناشی از اجرای

دسته‌بندی سیستم را بررسی می‌کند. مقدار آستانه ($\Im$) به‌صورت زیر محاسبه می‌شود:

$$\Im = \tau + \gamma_i \varrho, \quad \forall i \in [1,4] \tag{14}$$

که در آن τمیانگین و ϱانحراف معیار است γ_i .ضریب آستانه برای الگوریتم دسته‌بندیi ام می‌باشد.

این چارچوب شناسایی حمله پیش‌گیرانه و تطبیقی، گامی مهم در جهت حفاظت از شبکه‌های IoV 6 Gدر برابر طیف رو به گسترش تهدیدات سایبری محسوب می‌شود و به این ترتیب یکپارچگی و قابلیت اطمینان سیستم‌های ارتباطی وسایل نقلیه را حفظ می‌کند.

IV .ارزیابی عملکرد

در این بخش، هدف ما نشان دادن کارایی چارچوب پیشنهادی در یک محیط شبیه‌سازی‌شده IoV 6 Gاست. هدف اصلی این آزمایش، اعتبارسنجی توانایی چارچوب در مدیریت سناریوهای پویا و با تحرک بالا است که در شبکه‌های وسایل نقلیه رایج هستند، در حالی که امنیت قوی و مدیریت مؤثر منابع را نیز تضمین می‌کند.

A .محیط و استراتژی شبیه‌سازی

برای ارزیابی جامع سازگاری و پایداری چارچوب پیشنهادی، ما از ترکیبی از ابزارهای شبیه‌سازی پیشرفته استفاده کردیم:

- OMNeT++نسخه 5.1
- SUMOنسخه 0.30.0
- INETنسخه 3.6
- Veinsنسخه 4.7

این ابزارها به ما امکان می‌دهند یک محیط شبکه وسایل نقلیه پویا و واقعی را شبیه‌سازی کنیم که در آن شرایطی مانند سرعت خودروها، تراکم ترافیک، و تداخل‌های ارتباطی می‌توانند به سرعت و به‌طور غیرقابل پیش‌بینی تغییر کنند. تنظیمات شبیه‌سازی ما شامل تغییرات پویا در شرایط شبکه است که سناریوهای دنیای واقعی را شبیه‌سازی می‌کند. با استفاده ازSUMO ، الگوهای ترافیکی مختلف از جمله ساعات اوج با تراکم بالا و ساعات غیر اوج با تراکم کم شبیه‌سازی شدند. این کار به ما کمک می‌کند تا توانایی چارچوب در مدیریت انتقال و پردازش داده‌ها تحت بارهای مختلف را ارزیابی کنیم. با استفاده ازINET ، کیفیت و تداخل‌های مختلف کانال‌های ارتباطی شبیه‌سازی شد. همچنین، الگوهای حرکت خودروها با سرعت‌های مختلف و تغییرات ناگهانی جهت شبیه‌سازی شدند تا توانایی سیستم در مدیریت سناریوهای با تحرک بالا که در محیط‌های IoV 6 Gرایج است، مورد بررسی قرار گیرد.

اجرای هم‌زمان الگوریتم‌های مختلف تضمین می‌کند که چارچوب ما هم مؤثر و هم کارآمد باقی بماند و قادر باشد نیازهای سخت‌گیرانهٔ شبکه‌های IoV در 6 Gرا برآورده کند. علاوه بر این، فعال‌سازی شرطی روش‌ها تضمین می‌کند که منابع محاسباتی به‌صورت بهینه استفاده شوند و از مصرف غیرضروری جلوگیری شود. این استراتژی‌ها موجب می‌شوند چارچوب ما همواره کارآمد و مقاوم باشد.

۳. لایه امنیتی

این لایه مسئول تشخیص حملات در شبکه IoV است. رویکرد ما یک معماری طبقه‌بندی پیشرفته را برای دسته‌بندی ترافیک شبکه به دو دستهٔ «حمله» و «غیرحمله» ادغام می‌کند. این لایه شامل الگوریتم طبقه‌بندی شبکه، طبقه‌بندی حمله، و مولفهٔ آستانه تأیید است. با توجه به ماهیت پویا در محیط IoV 6 — Gکه در آن جریان داده و ویژگی‌های شبکه دائماً تغییر می‌کنند — سیستم ما از ماژول یادگیری آنلاین در لایه دوقلوی سایبری استفاده می‌کند. این فرایند یادگیری پیوسته از طریق پایش معیار قابلیت‌اعتماد سیستم نسبت به یک آستانهٔ ازپیش‌تعریف‌شده پشتیبانی می‌شود. اگر مقدار معیار قابلیت‌اعتماد کمتر از آستانه شود، یک مکانیزم به‌روزرسانی فعال می‌شود و ماژول یادگیری آنلاین را فراخوانی می‌کند. این ماژول شامل فرآیندهای انتخاب آگاه از شبکهٔ ویژگی‌ها (FS) و روش‌های طبقه‌بندی (CM) در لایه سایبری است تا بهترین روش‌های سازگار با شرایط فعلی شبکه را در زمان تقریباً واقعی پیدا کند. این سازوکار تضمین می‌کند که عملکرد مدل پایدار و قابل اعتماد باقی بماند، با تغییرات شبکه سازگار شود و همچنان دقت بالایی در تشخیص حملات را حفظ کند. ما به همین منظور هدف زیر را تعریف می‌کنیم.

$$V(\Im) = \begin{cases} 1, & \text{if } \Re < \Im \\ 0, & \text{otherwise} \end{cases}$$

که در آن $V(\Im)$تابع آستانهٔ تأیید یا *verifying threshold function*را نشان می‌دهد و $\Im$مقدار آستانه است. اگر خروجی تابع مقدار «۱» باشد، مکانیزم به‌روزرسانی برای ماژول یادگیری آنلاین فعال می‌شود. برای محاسبهٔ معیار قابلیت‌اعتماد سیستم (system reliability metric)، از هدف (objective) زیر استفاده می‌شود:

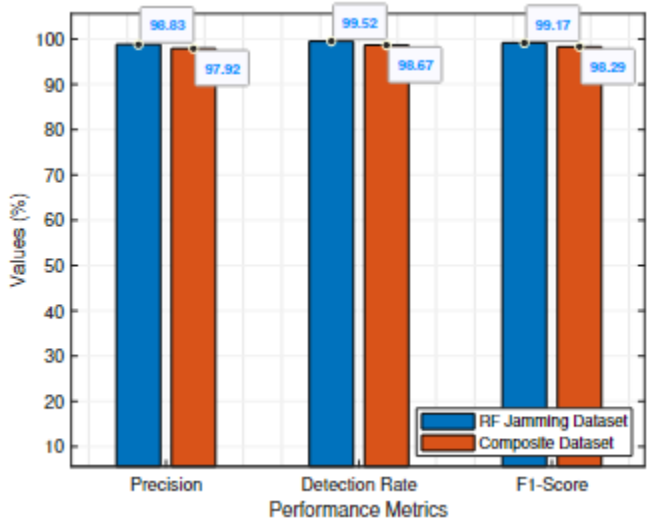
$$\Re = \frac{TP}{FN + TP} \tag{13}$$

که در آن $\Re$نشان‌دهندهٔ قابلیت اعتماد الگوریتم دسته‌بندی شبکه (network classification algorithm reliability)است و بر روی مقادیر منفی کاذب (FN) و مثبت واقعی (TP) تأکید دارد، چرا که این مقادیر در دسته‌بندی داده‌ها اهمیت زیادی دارند. هنگامی که حمله‌ای شناسایی نشود، ماژول آستانهٔ تأیید (verifying threshold component)به‌طور کامل قابلیت اعتماد الگوریتم

IoTو VANET است. همچنین، نمونه‌های داده حمله به‌صورت تصادفی در طول شبیه‌سازی‌ها به داده‌های وسایل نقلیه اضافه شدند تا قابلیت مجموعه داده در آزمایش چارچوب تحت شرایط متنوع و غیرمنتظره افزایش یابد.

ب. نتایج

ابتدا، عملکرد شناسایی حمله راه‌حل پیشنهادی خود را با استفاده از هر دو مجموعه داده RF Jamming و مجموعه داده ترکیبی بررسی کردیم. شکل 6 نتایج عملکرد راه‌حل ما را از نظر نرخ شناسایی حمله، دقت و معیار F1 نشان می‌دهد. نتایج مجموعه داده RF Jamming تقریباً ٪۹۹ و نتایج مجموعه داده ترکیبی تقریباً ٪۹۸ موفقیت در معیارهای عملکرد راه‌حل پیشنهادی را نشان می‌دهد. این نتایج بر پایداری راه‌حل پیشنهادی ما تأکید دارند و علاوه بر آن، این راه‌حل ویژگی مهمی برای شناسایی تهدیدات احتمالی به‌منظور تضمین امنیتVANET ها ارائه می‌دهد.



شکل ۶. تحلیل عملکرد راه‌حل پیشنهادی در مجموعه داده‌ها

سپس، اثربخشی راه‌حل خود را در شرایط پویا بررسی کردیم. برای این منظور، به‌طور دوره‌ای نمونه‌های حمله از مجموعه داده ترکیبی را وارد شبیه‌سازی کردیم تا قابلیت‌های سیستم در زمینه تأخیر انتها به انتها، مصرف انرژی، استفاده از حافظه RAM و نرخ تحویل بسته‌ها را در زمان واقعی بسنجیم. این روش به ما امکان می‌دهد پاسخ‌دهی و سازگاری سیستم با تغییرات ناگهانی در محیط حمله را درک کنیم. تأخیر انتها به انتها (End-to-End Latency): مدت زمان انتقال داده‌ها از منبع به مقصد را اندازه‌گیری می‌کند که برای برنامه‌های زمان واقعی حیاتی است. مصرف انرژی (Energy Consumption): کارایی انرژی سیستم را تحت بارهای شبکه و الگوهای حرکتی متغیر ارزیابی می‌کند. استفاده از RAM: کارایی حافظه سیستم را بررسی می‌کند که بر سرعت و پاسخ‌دهی پردازش داده‌ها تأثیر می‌گذارد. نرخ تحویل بسته‌ها (Packet Delivery Rate): اطمینان از تحویل صحیح و کامل بسته‌های داده را با وجود

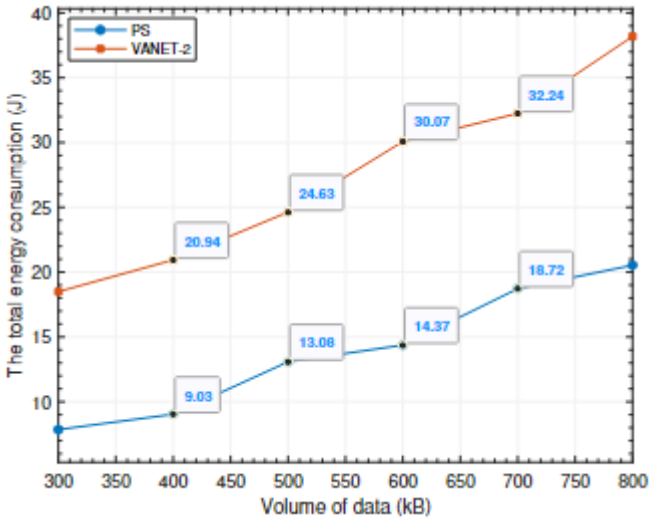
ما همزادهای سایبری (Cyber Twins) از گره‌های فیزیکی (وسایل نقلیه) در VANETایجاد کردیم با استفاده از Eclipse Ditto، یک چارچوب متن‌باز که مقیاس‌پذیر و چندمنظوره است [30]. با استفاده از این ابزار، می‌توانیم پارامترهای شبیه‌سازی را به‌طور پویا و در زمان واقعی بر اساس داده‌های تازه دریافتی از شبکه وسایل نقلیه تنظیم کنیم. این تنظیمات اطمینان می‌دهد که پاسخ سیستم با شرایط متغیر محیط شبیه‌سازی تطبیق پیدا کند و به این ترتیب، کاربرد عملی چارچوب ما در یک محیط پویا نشان داده می‌شود. ارزیابی ما بر توانایی سیستم در کاهش تأخیر انتها به انتها و بهبود تشخیص تهدیدات سایبری تمرکز داشت تا کارایی و اثربخشی راهکار پیشنهادی در بهبود عملکرد و امنیت شبکه نشان داده شود. ما چارچوب پیشنهادی خود را با استفاده از دو مجموعه داده متفاوت ارزیابی کردیم: اولین مجموعه دادهRF Jamming Dataset: این مجموعه شامل چندین سناریوی حمله RF Jamming در محیط‌های VANET است و دارای دو زیرمجموعه برای سرعت‌های نسبی تخمینی مختلف می‌باشد [31]. ما این زیرمجموعه‌ها را ادغام کردیم تا راهکار پیشنهادی خود را به‌طور جامع ارزیابی کنیم .این مجموعه داده شامل سناریوهایی با حملات RF Jamming است و بینش‌هایی درباره چگونگی عملکرد سیستم در مواجهه با تداخل‌های شدید ارائه می‌دهد. دومین مجموعه دادهToN-IoT: این مجموعه برای آزمون پایداری و اثربخشی ابزارهای امنیت سایبری مبتنی بر هوش مصنوعی در نسل بعدی IoT و محیط‌های صنعتی طراحی شده است [32]. این مجموعه شامل انواع مختلف حملات IoT است و پیچیدگی را افزایش داده و به اعتبارسنجی کارایی چارچوب در مقابل تهدیدات سایبری پیشرفته کمک می‌کند.

جدولII توزیع مجموعه داده ترکیبی: ادغام مجموعه داده‌های RF JammingوToN-IoT

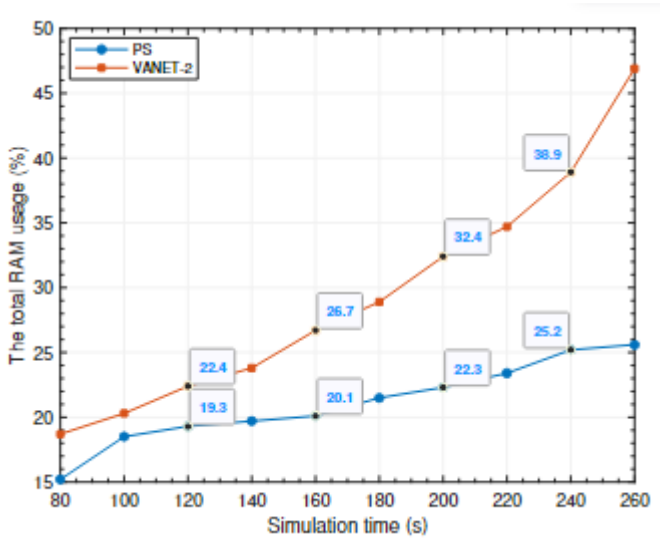
Dataset Name	Number of Samples
RF Jamming Dataset-1 (No Attack Samples)	1000
RF Jamming Dataset-2 (No Attack Samples)	1000
ToN-IoT Network Dataset (Attack Samples)	600

اگرچه مجموعه داده ToN-IoT به‌طور اولیه بر روی VANET تمرکز ندارد، با ادغام نمونه‌های بدون حمله از مجموعه داده RF Jammingبا نمونه‌های حمله از مجموعه دادهToN-IoT ، ما یک مجموعه داده جدید متناسب با تحلیل امنیتی VANET خود ایجاد کردیم. این مجموعه داده ترکیبی، که در جدول II به تفصیل آمده است، با دقت برای تعادل نمونه‌های حمله و غیرحمله انتخاب شد تا پایه‌ای جامع برای ارزیابی عملکرد ما فراهم کند. مجموعه داده جدید، که ترکیبی از دو مجموعه داده است، بیشتر بر IoT و VANETمتمرکز است. بنابراین، هدف ما دستیابی به نتایج جامع‌تر برای سیستم‌های حمل‌ونقل هوشمند (ITS) با استفاده از داده‌های

تحویل بسته‌ها بین راه‌حل ما و VANET-2 را می‌توان در شکل ۱۰ در طول زمان‌های مختلف شبیه‌سازی مشاهده کرد. در حالی که VANET-2به‌شدت بسته‌ها را از دست می‌دهد، راه‌حل ما عملکرد پایداری نشان می‌دهد. راه‌حل ما با افتی حدود ٪۱٫۸ از مقدار شروع تا مقدار نهایی روبه‌رو است، در حالی که سیستم VANET-2 کاهش چشمگیرتری دارد، حدود ٪۷٫۹. این نشان می‌دهد که راه‌حل ما در حفظ نرخ بالای تحویل بسته‌ها تقریباً ٪۶٫۱ عملکرد بهتری نسبت به VANET-2 دارد و بنابراین به‌طور قابل توجهی قابل اعتمادتر است.

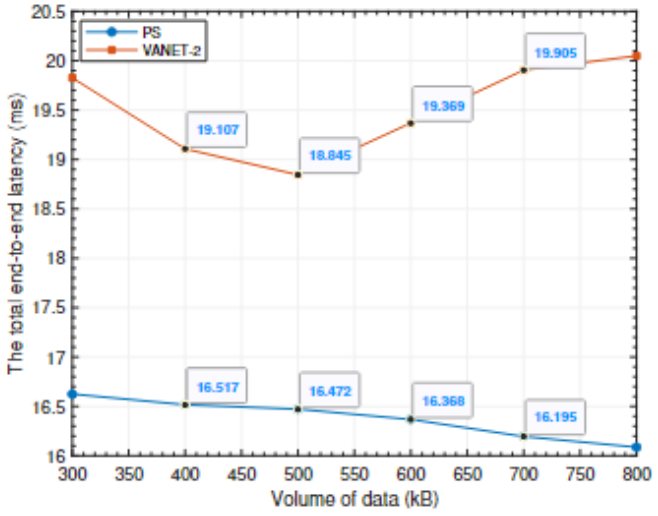


شکل ۸. مقایسهٔ مصرف کل انرژی در رابطه با حجم داده‌ها.



شکل ۹. مقایسهٔ کل مصرف حافظه (RAM) بر اساس زمان شبیه‌سازی.

تغییرات دینامیک شبکه ارزیابی می‌کند. برای مقایسه عملکرد راه‌حل پیشنهادی ما(PS) ، شبکه دیجیتال توپین VANET دیگری ایجاد کردیم که تمام اجزای پردازشی آن در لایه امنیت قرار دارند و از مهندسی ویژگی‌ها استفاده نمی‌کند. این شبکه از الگوریتم LSTM برای شناسایی حمله بهره می‌برد، زیرا این روش در مطالعات شناسایی حمله در VANET بیشتر استفاده شده است و با نام "VANET-2" شناخته می‌شود. این مقایسه نشان می‌دهد سیستم ما چقدر بهتر می‌تواند با تغییرات دینامیک شبکه سازگار شود. برای ارزیابی جامع عملکرد چارچوب پیشنهادی تحت بارهای مختلف شبکه، روندهای تأخیر را به دقت تحلیل کردیم. در شکل ۷، روند تأخیر در VANET-2و راه‌حل ما ویژگی‌های عملکردی متفاوتی را با افزایش حجم داده نشان می‌دهد. درVANET-2 ، ابتدا کاهش و سپس افزایش در تأخیر انتها به انتها مشاهده می‌شود که الگوی رایجی برای سیستم‌های سنتی است؛ این سیستم‌ها ابتدا بارهای افزایش یافته را به‌طور مؤثر مدیریت می‌کنند، اما زمانی که بارها از ظرفیت سیستم فراتر می‌روند، عملکردشان کاهش می‌یابد. برعکس، راه‌حل ما عملکرد به‌مراتب بهتری نشان می‌دهد. این به دلیل تقسیم استراتژیک بار محاسباتی بین لایه سایبر توپین و لایه امنیت است که پردازش داده‌ها را کارآمدتر می‌کند و احتمال ازدحام را حتی با افزایش حجم داده کاهش می‌دهد. این بهبود باعث کاهش تقریباً ٪۱۲ تأخیر سیستم نسبت به VANET-2می‌شود. به‌طور مشابه، شکل ۸ نشان می‌دهد که راه‌حل پیشنهادی مصرف انرژی کل سیستم را حدود ٪۱۵ کاهش داده است. این معیار اهمیت دارد زیرا بهبود کارایی سیستم از نظر مصرف انرژی را نشان می‌دهد.



شکل ۷. مقایسهٔ تأخیر کل انتها به انتها بر اساس حجم داده‌ها.

سپس، مصرف کل RAM و نرخ تحویل بسته‌های راه‌حل پیشنهادی ما بررسی شد. شکل ۹ مقایسهٔ مصرف کل RAM بین راه‌حل ما و VANET-2را نشان می‌دهد. در حالی که راه‌حل ما عملکرد پایداری دارد و مصرف RAM را به حداقل می‌رساند، VANET-2به‌طور قابل توجهی RAM بیشتری مصرف می‌کند. راه‌حل ما مصرف کل RAM را تقریباً ٪۲۰ نسبت به VANET-2 بهبود می‌بخشد. مقایسهٔ نرخ

به این جنبه‌های عملی، چارچوب پیشنهادی می‌تواند امنیت و کارایی شبکه‌های 6 IoV Gرا به طور قابل‌توجهی بهبود بخشد و به توسعه سیستم‌های حمل‌ونقل هوشمند و مقاوم کمک کند.

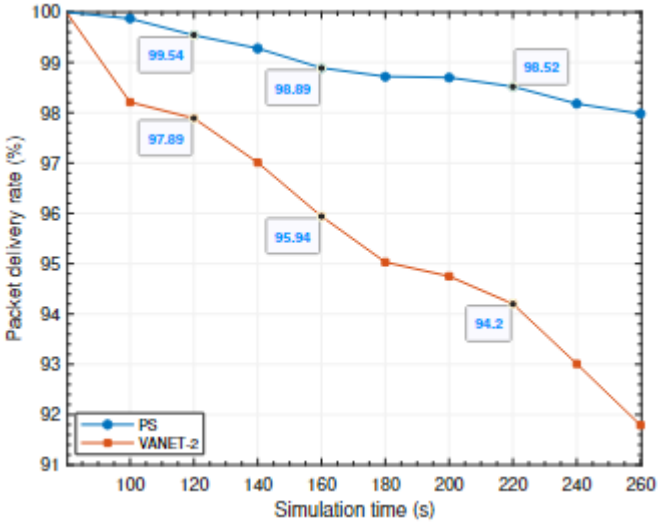
چارچوب پیشنهادی برای شبکه‌های 6 IoV Gپیشرفت‌های قابل توجهی ارائه می‌دهد، اما با چالش‌ها و محدودیت‌هایی نیز مواجه است که نیازمند توجه هستند. یکی از چالش‌های اصلی مدیریت حجم زیاد داده‌های تولید شده توسط خودروها وRSU هاست، در حالی که تأخیر پایین و پردازش به‌موقع حفظ شود. چالش دیگر ادغام سیستم با زیرساخت‌های قدیمی موجود است که ممکن است به‌راحتی از فناوری‌های پیشرفته پشتیبانی نکنند. همچنین، تعادل بین وظایف محاسباتی و تضمین تأخیر کم و بهره‌وری انرژی در سناریوهای زمان واقعی پیچیده است. مقیاس‌پذیری نیز مسئله‌ای کلیدی است، زیرا گسترش چارچوب برای پیاده‌سازی‌های بزرگ‌مقیاس در محیط‌های واقعی نیازمند تحقیقات و توسعه بیشتر است. علاوه بر این، چارچوب باید بتواند در زمان واقعی خود را با شرایط متغیر شبکه وفق دهد که این امر باید در محیط‌های مختلف آزمایش شود تا از مقاومت و قابلیت اطمینان آن اطمینان حاصل شود.

غلبه بر این چالش‌ها برای بهینه‌سازی عملکرد چارچوب و اطمینان از کارایی آن در شبکه‌های واقعی 6 IoV Gحیاتی است.

VI .نتیجه‌گیری

در پایان، ما یک چارچوب نوآورانه دیجیتال توئین تقویت‌شده با هوش مصنوعی معرفی کردیم که برای افزایش امنیت و کارایی محاسباتی شبکه 6 IoV Gطراحی شده است. سیستم پیشنهادی از یک ماژول پیشرفته مهندسی ویژگی‌ها با الگوریتم ssAE برای کاهش مؤثر ابعاد ویژگی‌ها و یک ماژول یادگیری آنلاین پویا برای حفظ عملکرد پایدار شناسایی حمله در زمان واقعی استفاده می‌کند. رویکرد ما بارهای محاسباتی را به‌طور مؤثری بین لایه‌های سایبر توئین و امنیت توزیع می‌کند و باعث بهبود قابل توجهی در تأخیر سیستم، مصرف انرژی و استفاده از RAM می‌شود. این چارچوب امنیت RSUها را افزایش داده و با بهبود کارایی محاسباتی، ارتباطات پایدارتر را ترویج می‌کند.

با شبیه‌سازی‌های جامع، نشان دادیم که چارچوب ما هم کارایی محاسباتی را بهبود می‌بخشد و هم ارتباطات درVANET ها را ایمن می‌کند. در مقابل دو مجموعه داده، چارچوب ما حدود ۹۸٪ موفقیت در معیارهای شناسایی حمله به دست می‌آورد که پتانسیل آن برای ایمن‌سازی شبکه‌های خودرو و ترویج ارتباطات پایدار را نشان می‌دهد. به‌طور خاص، این چارچوب تأخیر سیستم را حدود ۱۲٪، مصرف RAM را حدود ۲۰٪ کاهش داده، مصرف کل انرژی را تقریباً ۱۵٪ کم کرده و نرخ تحویل بسته‌ها را در طول دوره شبیه‌سازی تقریباً ۶/۱٪ بهبود می‌بخشد، در مقایسه با معماری سنتی از نظر کارایی محاسباتی.



شکل ۱۰. مقایسهٔ نرخ تحویل بسته‌ها (Packet Delivery Rate) بر اساس زمان شبیه‌سازی.

این نتایج عملکردی نشان‌دهنده بهینه‌سازی راهکار پیشنهادی ما هستند که منجر به عملیات شبکه‌ای پایدارتر و مقرون‌به‌صرفه‌تر می شود، امری که برای پیاده‌سازی شبکه‌های پیشرفته و ایمن خودروها حیاتی است. از طریق شبیه‌سازی دقیق و تحلیل‌ها، توانسته‌ایم کاهش مصرفRAM ، قابلیت‌های قوی شناسایی حمله و افزایش نرخ تحویل بسته‌ها در چارچوب دیجیتال توئین خود را نشان دهیم. این پیشرفت‌ها گامی مهم به سوی شبکه‌های حمل‌ونقل هوشمند مقاوم و دوستدار محیط زیست محسوب می‌شوند و مقیاس‌پذیری و اثربخشی سیستم ما را در حمایت از دفاع VANET در برابر تهدیدات سایبری پویا برجسته می‌کنند. این امر به پایداری شبکه‌های خودرو کمک کرده و یک معیار جدید برای پیاده‌سازی ارتباطات پیشرفته خودروها ایجاد می‌کند که نقطه عطفی در توسعه حمل‌ونقل هوشمند است.

V. بحث

پیاده‌سازی عملی سیستم پیشنهادی برای شبکه‌های 6 IoV G نیازمند توجه دقیق به چند عامل کلیدی در استقرار، ادغام و عملیات است. ابتدا، زیرساخت‌ها باید از ارتباط و پردازش در زمان واقعی پشتیبانی کنند، به‌گونه‌ای کهRSU ها قادر به اجرای الگوریتم‌های پیشرفته هوش مصنوعی برای تحلیل داده باشند. همچنین، ادغام نرم‌افزار و سخت‌افزار ضروری است تا سازگاری با استانداردهای موجود ارتباطات خودرو حفظ شده و عملکرد روان در لایه‌های مختلف شبکه تضمین شود. برای استقرار موفق، چارچوب باید با سیستم‌های موجود هماهنگ باشد و از راه‌حل‌های میدل‌ور برای مدیریت ترجمه داده‌ها استفاده کند.

مقیاس‌پذیری و انعطاف‌پذیری برای مدیریت حجم بالای داده‌ها و تغییرات فناوری اهمیت زیادی دارد، بنابراین محاسبات ابری و لبه‌ای بخش‌های ضروری سیستم هستند. پردازش مؤثر داده‌های زمان واقعی حیاتی است تا تأخیر کم و پاسخگویی بالا حفظ شود. با توجه

چارچوب ما آینده‌ای ایمن‌تر و مؤثرتر برای ارتباطات خودروها وعده می‌دهد و گامی حیاتی در جهت تحقق سیستم‌های ارتباطی قابل اعتماد، ایمن و هوشمند خودروها محسوب می‌شود. تحقیقات آینده بر بهبود بیشتر سازگاری و مقیاس‌پذیری چارچوب پیشنهادی متمرکز خواهد بود.

منابع

[1] SAM&SDH. Global Status Report on Road Safety 2023. [Online]. Available: https://www.who.int/publications/i/item/9789240086517, Accessed Date: Jan 15, 2024.

[2] Y. Yigit, I. Panitsas, L. Maglaras, L. Tassiulas, and B. Canberk, “Cyber-Twin: Digital Twin-Boosted Autonomous Attack Detection for Vehicular Ad-Hoc Networks,” in ICC 2024 - IEEE International Conference on Communications, Denver, CO, USA, June 2024, pp. 2167–2172.

[3] T. Bilen, H. Ahmadi, B. Canberk, and T. Q. Duong, “Aeronautical Networks for In-Flight Connectivity: A Tutorial of the State-of-the-Art and Survey of Research Challenges,” IEEE Access, vol. 10, pp. 20 053–20 079, 2022.

[4] H. Baharlouei, A. Makanju, and N. Zincir-Heywood, “Exploring Realistic VANET Simulations for Anomaly Detection of DDoS Attacks,” in 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), Helsinki, Finland, June 2022, pp. 1–7.

[5] B. Lampe and W. Meng, “Intrusion Detection in the Automotive Domain: A Comprehensive Review,” IEEE Communications Surveys & Tutorials, vol. 25, no. 4, pp. 2356–2426, 2023.

[6] Y. Yigit, K. Huseynov, H. Ahmadi, and B. Canberk, “YA-DA: YAng-Based DAta Model for Fine-Grained IIoT Air Quality Monitoring,” in 2022 IEEE Globecom Workshops (GC Wkshps), Rio de Janeiro, Brazil, December 2022, pp. 438–443.

[7] S. Dong, H. Su, Y. Xia, F. Zhu, X. Hu, and B. Wang, “A Comprehensive Survey on Authentication and Attack Detection Schemes That Threaten It in Vehicular Ad-Hoc Networks,” IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 12, pp. 13 573–13 602, 2023.

[8] E. Bozkaya, K.-T. Foerster, S. Schmid, and B. Canberk, “AirNet: Energy-Aware Deployment and Scheduling of Aerial Networks,” IEEE Transactions on Vehicular Technology, vol. 69, no. 10, pp. 12 252–12 263, 2020.

[9] M. Ariman, G. Seçinti, M. Erel, and B. Canberk, “Software defined wireless network testbed using Raspberry Pi of switches with routing add-on,” in 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), San Francisco, CA, USA, November 2015, pp. 20–21.

[10] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, “BDTwin: An Integrated Framework for Enhancing Security and Privacy in Cybertwin-Driven Automotive Industrial Internet of Things,” IEEE Internet of Things Journal, vol. 9, no. 18, pp. 17 110–17 119, 2022.

[11] R. Kumar, P. Kumar, A. Aljuhani, A. Jolfaei, A. N. Islam, and N. Mohammad, “Secure Data Dissemination Scheme for Digital Twin Empowered Vehicular Networks in Open RAN,” IEEE Transactions on Vehicular Technology, pp. 1–13, 2023.

[12] H. Feng, D. Chen, and Z. Lv, “Blockchain in Digital Twins-Based Vehicle Management in VANETs,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 10, pp. 19 613–19 623, 2022.

[13] B. Li, X. Song, T. Dai, W. Wu, D. Zhu, X. Zhai, H. Wen, Q. Lin, H. Chen, and K. Cai, “Trust Management Strategy for Digital Twins in Vehicular Ad Hoc Networks,” IEEE Journal on Selected Areas in Communications, vol. 41, no. 10, pp. 3279–3292, 2023.

[14] E. Ak and B. Canberk, “FSC: Two-Scale AI-Driven Fair Sensitivity Control for 802.11ax Networks,” in GLOBECOM 2020 - 2020 IEEE Global

Communications Conference, Taipei, Taiwan, December 2020, pp. 1–6.

[15] D. M. Gutierrez-Estevez, B. Canberk, and I. F. Akyildiz, “Spatio-temporal estimation for interference management in femtocell networks,” in 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC), Sydney, NSW, Australia, September 2012, pp. 1137–1142.

[16] Y. Yigit, H. Ahmadi, G. Yurdakul, B. Canberk, T. Hoang, and T. Q. Duong, “Digi-Infrastructure: Digital Twin-enabled Traffic Shaping with Low-Latency for 6G Smart Cities,” IEEE Communications Standards Magazine, vol. 8, no. 3, pp. 2–8, 2024.

[17] C. Schwarz and Z. Wang, “The Role of Digital Twins in Connected and Automated Vehicles,” IEEE Intelligent Transportation Systems Magazine, vol. 14, no. 6, pp. 41–51, 2022.

[18] D. Van Huynh, S. R. Khosravirad, A. Masaracchia, O. A. Dobre, and T. Q. Duong, “Edge Intelligence-Based Ultra-Reliable and Low-Latency Communications for Digital Twin-Enabled Metaverse,” IEEE Wireless Communications Letters, vol. 11, no. 8, pp. 1733–1737, 2022.

[19] V. Arya, A. Gaurav, B. B. Gupta, C.-H. Hsu, and H. Baghban, “Detection of Malicious Node in VANETs Using Digital Twin,” in Big Data Intelligence and Computing, C.-H. Hsu, M. Xu, H. Cao, H. Baghban, and A. B. M. Shawkat Ali, Eds. Singapore: Springer Nature Singapore, 2023, pp. 204–212.

[20] M. Ali, G. Kaddoum, W.-T. Li, C. Yuen, M. Tariq, and H. V. Poor, “A Smart Digital Twin Enabled Security Framework for Vehicle-to-Grid Cyber-Physical Systems,” IEEE Transactions on Information Forensics and Security, vol. 18, pp. 5258–5271, 2023.

[21] Y. Yigit, O. K. Kinaci, T. Q. Duong, and B. Canberk, “TwinPot: Digital Twin-assisted Honeypot for Cyber-Secure Smart Seaports,” in 2023 IEEE International Conference on Communications Workshops (ICC Workshops), Rome, Italy, May-June 2023, pp. 740–745.

[22] Z. Zhou, A. Gaurav, B. B. Gupta, M. D. Lytras, and I. Razzak, “A fine-grained access control and security approach for intelligent vehicular transport in 6g communication system,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 9726–9735, 2022.

[23] L. Zhao, S. Li, Y. Guan, S. Wan, A. Hawbani, Y. Bi, and M. Guizani, “Adaptive Multi-UAV Trajectory Planning Leveraging Digital Twin Technology for Urban IIoT Applications,” IEEE Transactions on Network Science and Engineering, pp. 1–16, 2023.

[24] Y. Yigit, L. D. Nguyen, M. Ozdem, O. K. Kinaci, T. Hoang, B. Canberk, and T. Q. Duong, “TwinPort: 5G Drone-assisted Data Collection with Digital Twin for Smart Seaports,” Scientific Reports, vol. 13, p. 12310, 2023.

[25] B. Yan and G. Han, “Effective Feature Extraction via Stacked Sparse Autoencoder to Improve Intrusion Detection System,” IEEE Access, vol. 6, pp. 41 238–41 248, 2018.

[26] Y. Yigit, B. Bal, A. Karameseoglu, T. Q. Duong, and B. Canberk, “Digital Twin-Enabled Intelligent DDoS Detection Mechanism for Autonomous Core Networks,” IEEE Communications Standards Magazine, vol. 6, no. 3, pp. 38–44, 2022.

[27] Y. Yigit, C. Chrysoulas, G. Yurdakul, L. Maglaras, and B. Canberk, “Digital Twin-Empowered Smart Attack Detection System for 6G Edge of Things Networks,” in 2023 IEEE Globecom Workshops (GC Wkshps), Kuala Lumpur, Malaysia, December 2023, pp. 178–183.

[28] E. Horsanali, Y. Yigit, G. Secinti, A. Karameseoglu, and B. Canberk, “Network-Aware AutoML Framework for Software-Defined Sensor Networks,” in 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2021, pp. 451–457.

[29] F. A. Alhaidari and A. M. Alrehan, “A Simulation Work for Generating a Novel Dataset to Detect Distributed Denial of Service Attacks on Vehicular Ad hoc NETwork systems,” International Journal of Distributed Sensor Networks, vol. 17, no. 3, p. 15501477211000287, 2021.

[30] Eclipse. Eclipse Ditto Documentation. [Online]. Available: https://www.eclipse.org/hono/docs/, Accessed Date: June 18, 2023.

[31] D. Kosmanos, D. Karagiannis, A. Argyriou, S. Lalis, Y. Yigit, and L. Maglaras. RF Jamming Dataset for Vehicular Wireless Networks. [Online]. Available: https://dx.doi.org/10.21227/4zwk-yw78, Accessed Date: May 20, 2023.

[32] N. Moustafa. ToN IoT datasets. [Online]. Available: https://ieee-dataport.org/documents/toniot-datasets, Accessed Date: May 20, 2023.

[33] Y. Yu, X. Zeng, X. Xue, and J. Ma, “LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 12, pp. 23 906–23 918, 2022.