

# چارچوب دوکلوبی دیجیتال تقویت شده با هوش مصنوعی برای شبکه های اینترنت وسایل نقلیه با تاب آوری سایبری 6G

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 دوکلوبی دیجیتال نقشی حیاتی در توسعه اینترنت وسایل نقلیه نسل ششم 10V6 G دارد، زیرا امکان پایش و ارزیابی محیط پویا و پیچیده وسایل نقلیه را فراهم می کند. با این حال، شبکه های 6 10V G با چالش های مهمی در زمینه امنیت شبکه و کارایی محاسباتی روبرو هستند که باید برطرف شوند. فناوری های موجود دوکلوبی دیجیتال در شبکه های 6 10V G معمولاً با محدودیت هایی مانند تکیه بر مدل های ایستا و نیازهای بالای محاسباتی مواجه اند که منجر به ناپایداری در تشخیص حملات و کاهش کارایی می شود. عملکرد این سامانه ها در شاخص های تشخیص حمله- از جمله دقت، نرخ تشخیص، و امتیاز F1- برای الزامات 6 10V G کافی نیست. علاوه بر این، آن ها تمام پردازش ها را در لایه خدمات دوکلوبی دیجیتال متتمرکز می کنند که موجب ناکارآمدی می شود. برای رفع این چالش ها، ما یک چارچوب نوآورانه دوکلوبی دیجیتال تقویت شده با هوش مصنوعی معرفی می کنیم که با هدف بهبود چشمگیر امنیت شبکه و کارایی محاسباتی در شرایط پویا برای شبکه های 6 10V G طراحی شده است. چارچوب پیشنهادی ما از یک مازول مهندسی ویژگی پیشرفت بهره می برد که با استفاده از روش های انتخاب ویژگی و خودرنگنارهای تنک پشتہ ای (ssAE) ابعاد ویژگی ها را در لایه دوکلوبی سایبری کاهش می دهد و بدین ترتیب بار محاسباتی را به طور مؤثر توزیع می کند. همچنین از یک مازول یادگیری برخط استفاده می کند که یک سازوکار تشخیص حمله آکاه از وضعیت شبکه را برای تشخیص دقیق حملات فراهم می سازد. راهکار پیشنهادی ما عملکردی پایدار در حدود ۹۸٪ نرخ موفقیت در شاخص های تشخیص حمله روی دو مجموعه داده ارائه می دهد. به طور مشخص، این سامانه ۱۲٪ کاهش تأخیر سیستم، ۱۵٪ کاهش مصرف انرژی، ۶٪ ۲۰٪ کاهش استفاده از RAM و ۶٪ افزایش نرخ تحویل بسته ها را نشان می دهد. این نتایج نشان می دهد که چارچوب ما ظرفیت قابل توجهی در ارتقای امنیت و کارایی شبکه های 6 10V G دارد. این پیشرفت ها، Robustness و پاسخ دهنده سامانه های 6 10V G را به شکل چشمگیری افزایش می دهد و سهمی مهم در بهبود امنیت و مدیریت شبکه های خودرویی ایفا می کند.

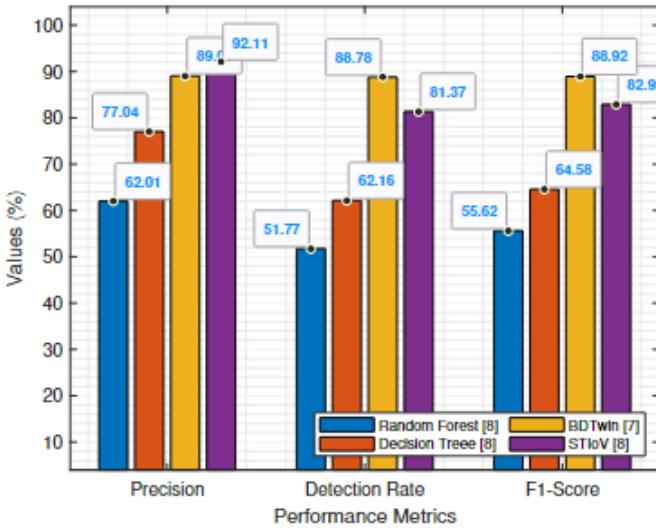
وازگان کلیدی - هوش مصنوعی (AI)، امنیت، دوکلوبی دیجیتال، اینترنت وسایل نقلیه (10V)، سامانه های حمل و نقل هوشمند (ITS)، شبکه های خودرویی (VANET).

۱. مقدمه

تحول شبکه های خودرویی موردی (VANETs) یک پیشرفت مهم در اینمی جاده و کارآمدی حمل و نقل به شمار می رود؛ موضوعی که سازمان جهانی بهداشت در گزارش وضعیت جهانی اینمی جاده سال ۲۰۲۳ بر آن تأکید کرده است [1] شبکه های VANET در عصر اینترنت وسایل نقلیه نسل ششم 10V6 G اهمیت رو به رشدی یافته اند، زیرا سامانه های متصل به اینترنت در وسایل نقلیه- which شامل حسگرها، عملگرها و دستگاه های هوشمند هستند- به اشیاء مختلف امکان می دهند داده ها را جمع آوری، انتقال و پردازش کنند. انتظار می رود شبکه های 6 G با ارائه نرخ های داده بسیار بالا، کاهش تأخیر تا حد تقریباً آنی، و افزایش پوشش دهی، باعث تحول بیشتر در VANET شوند و بر پیشرفت های نسل پنجم G5 بنا کنند. برای فعال سازی شبکه های 10V6 G، فناوری دوکلوبی دیجیتال نقش اساسی دارد، زیرا این فناوری امکان نظارت و تحلیل محیط پویا و پیچیده خودرویی را فراهم می کند [2، 3] در شبکه 10V6 G، شبکه های خودرویی اهمیت ویژه ای دارند زیرا به وسایل نقليه اجازه می دهند با یکدیگر ارتباط خودرو به خودرو (V2V)- و با زیرساخت (V2I)- ارتباط خودرو به زیرساخت ارتباط برقرار کنند. با ارائه اطلاعات دقیق و به موقع ترافیکی، ارتباطات خودرویی موجب افزایش راحتی، اینمی جاده و امکان پذیری توسعه خودروهای خودران می شود [4] با این حال، این پیشرفت ها چالش های جدیدی را نیز در مدیریت پیچیدگی و امنیت شبکه های خودرویی ایجاد می کنند، که ضرورت بهره گیری از راهکارهای نوآورانه را برجسته می سازد.

A. انگیزه

در حال حاضر به دلیل ناهمگنی و توبولوژی پویا در شبکه های خودرویی، به ویژه در ارتباطات V2I، افزایش چشمگیری در حملات مخرب مشاهده می شود [5]-[7]. مهاجمان با استفاده از حملات پیچیده و ایجاد اختلال در خدمات مرتبط با وسایل نقلیه، آسیب قابل توجهی وارد می کنند. در یک حمله سایبری مانند حمله انکار سرویس توزیع شده (DDOS)، مهاجم تلاش می کند شبکه 6 10V G را برای کاربران موردنظر غیرقابل دسترس یا بدون پاسخ کند و از این طریق در خدمات و سامانه های خودرویی اختلال ایجاد کند. این نوع حمله می تواند وسایل نقلیه را ناتوان سازد و پیامدهای منفی برای ارائه دهنده ای خدمات و کاربران به همراه داشته باشد. علاوه بر این، چنین حمله ای ممکن است منجر به بروز مشکلات در خودرو، ایجاد ازدحام ترافیکی، اختلال در ارتباطات خودرویی، و حتی بروز تصادفات شود.



شکل ۱. تحلیل عملکرد راه حل های فعلی.

[8] [9] بنابراین، ایجاد سامانه های دفاعی پیشرفته برای محافظت از شبکه های VANET در برابر حملات و حفظ قابلیت اعتماد آنها در عصر IoT ضروری است. کارهای اخیر در زمینه شناسایی حملات شبکه های خودرویی با استفاده از فناوری دو قلوی دیجیتال [10]، [11] برای برآورده کردن شاخص های عملکردی شبکه های IoT همچون نرخ تشخیص، دقت، و F1-Score کافی نیستند؛ همانگونه که در شکل ۱ نشان داده شده است. این راه کارها از مدل های ایستا استفاده می کنند، که برای شبکه های IoT 6G مناسب نیست؛ زیرا این شبکه ها نیازمند راه کارهای پویا برای مدیریت انواع مختلف حملات و ناهمگونی موجود در شبکه هاستند. افزون بر این، عملکرد آنها در برابر داده های مختلف ناپایدار است. برای نمونه، هنگام مقایسه نتایج عملکردی راه کارهای ارائه شده در [10]، [11] روی دو مجموعه داده، اختلاف در حدود ۱۵٪ مشاهده می شود. همچنین نتایج حاصل از الگوریتم های جنگل تصادفی و درخت تصمیم در [11] حدود ۲۵٪ اختلاف بین دو مجموعه داده نشان می دهد. بنابراین، راه کارهای کنونی پایدار نبوده و قادر به مدیریت حملات متنوع در محیط های پویا و دینامیک IoT 6G نیستند. در نتیجه، یک راه کار پیشرفته و پویا لازم است که بتواند حملات را به صورت دینامیک شناسایی کرده و عملکردی پایدار در محیط های IoT 6G ارائه دهد. چالش دیگر، بار محاسباتی بالا در راه کارهای فعلی شناسایی شبکه های خودرویی است، که مستقیم بر تأخیر انتها به انتهای تأثیر می گذارد؛ پارامتری حیاتی برای زمان شناسایی حمله. رشد سامانه های ارتباطی خودروی، بار محاسباتی را در محیط های IoT 6G افزایش داده است. پژوهش های کنونی در مورد شبکه های خودرویی بر پایه فناوری دو قلوی دیجیتال، بار سنگینی بر کل سامانه محاسباتی وارد می کنند؛ زیرا تمام عملیات محاسباتی در لایه سرویس دو قلوی دیجیتال انجام می شود [12]، [13]. در نتیجه، مقادیر تأخیر انتها به انتهای، مصرف انرژی، میزان RAM و نرخ تحويل بسته ها در آنها برای مدیریت شبکه های IoT 6G کافی نیست. برای عملکرد بهتر سیستم و

شناسایی سریع تر حملات، این بار محاسباتی باید توزیع شود. برای رفع این دو چالش اصلی، می توان از یادگیری آنلاین برای شناسایی پویای حملات استفاده کرد و از لایه دوقلوی دیجیتال. به جای لایه سرویس. برای مهندسی ویژگی و کاهش ابعاد ویژگی با هدف تقسیم بار محاسباتی بهره برد. افزون بر این، داده های شبکه می توانند با استفاده از توانایی های خود رمزگذار پراکنده پشتہ ای (ssAE) به صورت مؤثر پردازش و تحلیل شوند [14]، [15]. روش ssAE ویژگی های مرتبط برای کاربردهای امنیت سایری مانند تشخیص ناهنجاری، شناسایی الگو و تشخیص حمله را استخراج کرده و در عین کاهش ابعاد داده، ویژگی های کلیدی را حفظ می کند.

## ب. پوشش مقاله و مشارکت ها

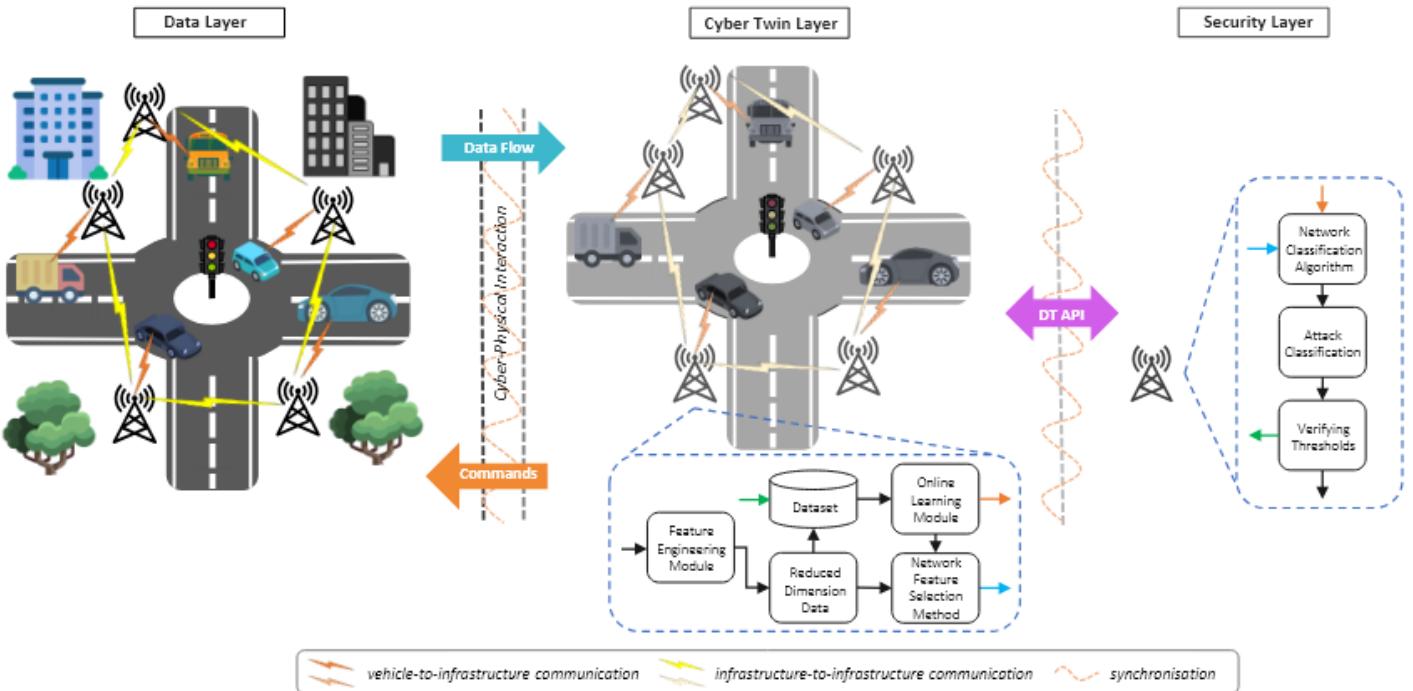
در این مقاله، از ssAE به دلیل قابلیت های بهبود یافته در استخراج ویژگی و کاهش مؤثر ابعاد داده استفاده شده است. برای مقابله با چالش های پیش گفته، این پژوهش بر ارتباطات V2I و به طور مشخص بر تقویت امنیت RSU (واحد کنار جاده ای) تمرکز دارد. علاوه بر این، ما رویکردی نوآورانه مبتنی بر هوش مصنوعی برای تقویت امنیت شبکه های IoT 6G ارائه می کنیم که از فناوری دو قلوی دیجیتال و الگوریتم های هوش مصنوعی بهره می برد و تمرکز آن بر امنیت سایری و کاری محاسباتی است. تمایز اصلی کار ما، ارائه یک معماری لایه ای جامع شامل لایه داده، لایه دو قلوی سایری، و لایه امنیت است که چالش های تحرک پذیری بالا و ناهمگونی شبکه های IoT 6G را برطرف می کند (طبق شکل ۲). ما از مازول مهندسی ویژگی شامل ssAE برای کاهش مؤثر ابعاد داده و از مازول یادگیری آنلاین برای ارائه عملکرد پایدار در شناسایی حملات استفاده می کنیم. این مازول ها در لایه دو قلوی سایری قرار دارند تا بار محاسباتی سیستم را به طور مؤثر تقسیم کنند. همچنین، ما یک سازوکار اشتراک گذاری خودکار بین RSU های همسایه معرفی می کنیم TAI های مخرب میان آنها به اشتراک گذاشته شود. مشارکت های اصلی مقاله به صورت خلاصه :- ارائه یک چارچوب هوشمند شناسایی حملات مبتنی بر دو قلوی دیجیتال برای مقابله با حملات در محیط IoT 6G، به ویژه حملات هدفمند RSU ها- ارائه یک مازول یادگیری آنلاین برای تضمین عملکرد پایدار و آگاه از وضعیت شبکه در شناسایی حملات شامل AutoCM و AutoFS - AutoCM وضعیت شبکه در شناسایی حملات در مازول مهندسی ویژگی مبتنی بر ssAE برای کاهش ابعاد داده و ارائه مازول مهندسی ویژگی معرفی سازوکار اشتراک گذاری خودکار تقسیم بار محاسباتی- معرفی سازوکار اشتراک گذاری خودکار اطلاعات بین RSU های همسایه برای تبادل IP های مخرب این مقاله، چارچوب ارائه شده در مقاله کنفرانسی ما [2] را با وارد کردن چندین پیشرفت مهم که برای شبکه های IoT 6G طراحی شده اند، گسترش می دهد. در این مقاله، ما از یک مازول مهندسی ویژگی، گسترش می دهد. در حالی که [2] تنها از پرسپترون چندلایه مؤلفه AutoCM در حالی که (MLP) برای طبقه بندی استفاده می کند، تقسیم بار محاسباتی کلی سیستم بین لایه دو قلوی RSU های همسایه. برخلاف [2]. بهره بدهایم. مازول AutoFS در مقاله کنفرانسی شامل حذف بازگشتی ویژگی (RFE)، حذف ویژگی به صورت پسرو، کایدو، امتیاز فیشر، و

الگوریتم انتخاب مقدار F آنوا (ANOVA) بود. پس از انجام آزمایش‌های جامع، در این مقاله حذف ویژگی به صورت پسر 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 بخش III، 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 قابل توجهی را در توسعه سامانه‌های حمل و نقل 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 حمل و نقل از طریق فراهم‌سازی ارتباطات بلاذرنگ و تحلیل‌های پیش‌بینی کننده تأکید می‌شود. یک چارچوب دوقلوی دیجیتال برای مدیریت ترافیک شهر هوشمند پیشنهاد شد که از داده‌های بلاذرنگ برای بهینه‌سازی جریان ترافیک و افزایش ایمنی استفاده می‌کند. با این حال، این رویکرد عمدتاً بر کارایی ترافیک تمرکز دارد و قادر سازوکارهای اختصاصی برای تشخیص حملات در شبکه‌های خودرویی است. به طور مشابه، همگرایی اینترنت اشیا (IoT) و فناوری‌های هوش مصنوعی مسیر را برای معماری‌های نوآورانه دوقلوی دیجیتال هموار کرده است. مطالعه [18] راهبردهای cache offloading کردن وظایف در سرورهای لبه‌ای نزدیک را برای کاهش تأخیر بررسی می‌کند و یک زیرساخت محاسباتی قدرتمند مبتنی بر ارتباطات فوق‌قابل اعتماد و کم‌تأخر 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 به کار گرفته شدند، اما این راهکار از یک مدل ایستا استفاده می‌کرد و قادر به سازگاری با ماهیت پویای شبکه خودروی نبود. افزون بر این، این کار هیچ معیاری مرتبط با بر 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 به روزرسانی نمی‌کند؛ بنابراین برای استفاده در شبکه‌های خودرویی مناسب نیست. همچنین عملکرد تنها از نظر سریار انتقال ارزیابی شده است که برای تعیین بر محاسباتی سیستم کافی نیست. مطالعه [10] یک چارچوب مبتنی بر بلاک‌چین و

LSTM دوسویه مجهز به مکانیزم توجه را معرفی کرد که از دوقلوی vehicle-to-grid استفاده می‌کند. نویسنده‌گان این چارچوب را با دو مجموعه داده شناخته شده IoT ارزیابی کردند؛ اما نتایج حدود 14٪ اختلاف بین مجموعه داده‌ها را نشان داد که اختلاف زیادی بوده و عملکردی نایاب‌دار در مطالعه‌ای دیگر [11] یک چارچوب مبتنی بر یادگیری عمیق برای تشخیص نفوذ در IoT اپیشنهاد شد که از یک variational autoencoder پشتیبانی داده شده ارزیابی شد؛ اما نتایج اختلاف حدود 15٪ بین مجموعه داده‌ها را نشان داد و عملکرد نایاب‌دار آن را در شبکه‌های پویا به اثبات رساند. همچنین، این کار نیز معیارهای بر محاسباتی را در نظر نگرفته است. نویسنده‌گان [20] یک سامانه یادگیری تقویتی عمیق مبتنی بر LSTM و actor-critic با بهره‌گیری از دوقلوی سامانه‌های سایر-فیزیکی از دوقلوی vehicle-to-grid در ارتباطات خودرویی به کار رفت. این راهکار روی دو مدل ارتباطات خودرویی مبنی بر توجه استفاده می‌کند. در این مطالعه، فناوری دوقلوی دیجیتال برای نگاشت سرورهای RSU و ساخت مجموعه داده شناخته شده ارزیابی شد؛ اما نتایج اختلاف حدود 15٪ بین مجموعه داده‌ها را نشان داد و عملکرد نایاب‌دار آن را در شبکه‌های پویا به اثبات رساند. همچنین، این کار نیز معیارهای بر محاسباتی را در نظر نگرفته است. نویسنده‌گان [20] یک سامانه یادگیری تقویتی در ارتباطات IoT و honeypot مبنی بر ارزیابی کافی تشخیص حملات در هم‌زمان را نشان می‌دهد. این سامانه از روش به روزرسانی پویا برای مقابله با انواع حملات استفاده می‌کند؛ اما همچنان تمامی پردازش‌ها و الگوریتم‌ها در لایه سرویس دوقلوی دیجیتال انجام می‌شوند و برای هم‌زمان شیوه 6 IoT مناسب نیست. نویسنده‌گان [22] رویکردی ترکیبی از یادگیری عمیق و رمزگاری مبتنی بر هویت برای بررسی ناهنجاری‌ها در ارتباطات IoT ارائه کردند. با وجود اینکه نرخ تشخیص حدود 97٪ گزارش شده است، ارزیابی تنها با یک مجموعه داده انجام شده و عملکرد آن در برابر مجموعه داده‌های مختلف نامشخص است. همچنین معیارهای بر محاسباتی در [23] رویکردی نوین برای بهبود بهره‌وری انرژی و عملکرد عملیاتی هواگردان 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 محیط‌های IoT، از بینش‌های این مطالعه بهره گرفتیم. بررسی‌های فوق بر توانایی‌های مهم اما کمتر بهره‌برداری شده. در این‌سازی شبکه‌های IoT تأکید می‌کنند. با این حال، یک کمبود قابل توجه در ادغام کارآمد دوقلوهای دیجیتال و مدل‌های هوش مصنوعی برای تقویت امنیت و ارائه عملکرد پایدار در شبکه‌های IoT امشاهده می‌شود. یک سامانه تشخیص حمله پویا در محیط‌های IoT 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...



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

بررسی‌های فوق‌الذکر نشان می‌دهد که اگرچه قابلیت‌های چشمگیری برای ایمن‌سازی شبکه‌های IoT وجود دارد، این ظرفیت‌ها به طور کامل مورد بهره‌برداری قرار نگرفته‌اند. با این حال، یک کمبود قابل توجه در یکپارچه‌سازی کارآمد دوکلوی دیجیتال و مدل‌های هوش مصنوعی برای تقویت امنیت و ارائه عملکرد پایدار در شبکه‌های 6G IoT مشاهده می‌شود. یک سیستم تشخیص حمله پویا در محیط‌های IoT لازم است تا بتواند با تغییرات داده‌های شبکه سازگار شود و عملکرد تشخیص حمله پایدار ارائه دهد. افزون بر این، مطالعات مبتنی بر دوکلوی دیجیتال در شبکه‌های خودرویی نشان می‌دهند که بار پردازشی سیستم به طور قابل ملاحظه‌ای بالا است، و این امر نیازمند توزیع بار برای بهبود عملکرد سیستم و امکان تشخیص سریع تر حملات می‌باشد. در این نقطه، فناوری دوکلوی دیجیتال می‌تواند به طور مؤثری برای تقسیم بار پردازشی در سراسر سیستم خودرویی به کار 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 IoT ارائه دهیم.

### III. چارچوب پیشنهادی

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

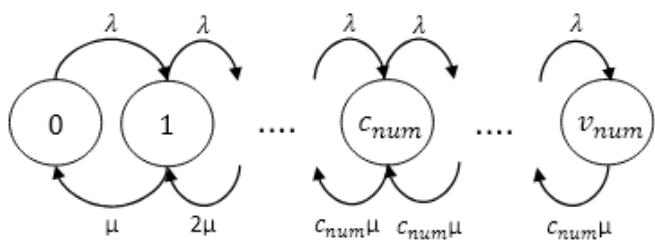
#### A. مدل‌سازی ریاضی ترافیکی RSU

فرض می‌کنیم وسائل نقلیه کانال‌های مناسب یک RSU را در محدوده پوشش آن به اشتراک می‌گذارند و هر وسیله نقلیه دارای اولویت برابر است؛ یعنی هیچ اولویتی میان آن‌ها وجود ندارد. برای مدل‌سازی درخواست‌های ارتباطی وسائل نقلیه، ما از مدل صفاتی M/M/m استفاده می‌کنیم که یک مفهوم بنیادین در نظریه صفات است. نظریه صفات، مطالعه ریاضی صفاتی صفاتی یا خطوط انتظار است که به پیش‌بینی طول صفاتی و زمان انتظار کمک می‌کند. مدل M/M/m به طور مشخص یک سیستم با چند سرور (m) را نمایش می‌دهد که در آن ورودها از یک فرایند پواسون پیروی می‌کنند و زمان‌های خدمت دارای توزیع نمایی هستند. در این پژوهش، مدل درخواست‌های ارتباطی وسائل نقلیه را به صورت اولین وارد شده، اولین خارج شده (FIFO) در نظر می‌گیرد؛ یعنی درخواست‌ها دقیقاً به ترتیب ورود پردازش می‌شوند. جدول نام‌گذاری مدل در جدول ۱ ارائه شده است که تعاریف نمادهای استفاده شده در سراسر مقاله را برای افزایش شفافیت و درک بهتر فرمول‌بندی‌های ریاضی فراهم می‌کند.

جدول ا نام‌گذاری (Nomenclature Table)

Symbol	Description	Icon
$v_{num}$	Number of vehicles	Car icon
$c_{num}$	Number of channels available at the RSU	Network icon
$\lambda$	Arrival rate of communication demands	
$\mu$	Service rate of each channel per request	
$\rho$	Traffic intensity	
$P_0$	Probability of zero communication requests	
$P_{vnum}$	Probability of having $v_{num}$ vehicles	
$\varphi$	Probability that all requests are accepted	
$\xi$	Probability that requests are queued	
$P_{Queue}$	Probability of a communication request waiting	
$T_{AVGQ}$	Average waiting time in the queue	
$\Theta$	Sparsity constraint weighting factor	
$\sigma$	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	
$\varphi_1, \varphi_2$	Bias vectors for hidden and output layers in ssAE	
$\rho$	Predefined sparsity parameter in the ssAE algorithm	
$J(W, b)$	Loss function for reconstruction error in ssAE	
$J_{sparse}(W, b)$	Total loss function with sparsity penalty in ssAE	
$\lambda$	Weight attenuation coefficient in ssAE loss function	
$\gamma_i$	Threshold factor for the $i$ -th classification algorithm	
$\mathcal{V}(\mathcal{I})$	Verifying threshold function for system reliability	
$R$	System reliability metric	

تعداد درخواست‌های ارتباطی در هر بازه زمانی برای توصیف وضعیت سیستم استفاده می‌شود. سروهای به صورت کانال‌ها مدل‌سازی شده‌اند. در هر بازه زمانی، مجموع تعداد درخواست‌های ارتباطی با تعداد کانال‌ها در دسترس در همان بازه مقایسه می‌شود. اگر هیچ کانالی برای ارائه سرویس موجود نباشد، درخواست‌ها تا بازه زمانی بعدی نگه داشته می‌شوند تا دوباره وضعیت دسترس پذیری کانال‌ها برسی شود. شکل ۳ نمودار حالت را نشان می‌دهد که تقاضاهای ارتباطی خودروها در محدوده پوشش یک RSU را با استفاده از مدل صفحه‌نمایش M/M/m مینمایش 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  $c_{num}$  تعداد کانال‌های RSU را نشان می‌دهد،  $v_{num}$  تعداد خودروهایی را نشان می‌دهد که درخواست ارتباط دارند، آنچه در خواست‌های ارتباطی را نشان می‌دهد،  $\mu$  نرخ سرویس دهی هر کانال را نشان می‌دهد که وابسته به زمان است.



شکل ۳. نمودار حالت مربوط به تقاضاهای ارتباطی خودروها در محدوده پوشش RSU.

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

تفعیرات مبتنی بر میزان دسترسی کانال‌های ارتباطی و ورود درخواست‌های خودروها کمتر یا برابر با تعداد کانال‌های در دسترس باشد ( $v_{num} \leq c_{num}$ )، RSU می‌تواند تمام این درخواست‌ها را به طور مستقیم پردازش کند و همه درخواست‌ها پذیرفته می‌شوند. در مقابل، اگر تعداد درخواست‌ها بیشتر از کانال‌های موجود باشد ( $v_{num} > c_{num}$ )، درخواست‌های اضافی در صفحه 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 سرویس دهی 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 صفحه ( $T_{AVGQ}$ ) را به صورت بصری نمایش می‌دهد. با تحلیل این احتمالات و زمان‌های انتظار، نمودار نشان می‌دهد که RSU چگونه به صورت کارآمد، سطح‌های متفاوت تقاضای ارتباطی را مدیریت می‌کند. معادله (۱) احتمال وجود تعداد مشخصی خودرو ( $v_{num}$ ) را در سیستم توصیف می‌کند و در آن تعداد کانال‌های قابل دسترس ( $c_{num}$ )، نرخ سرویس دهی ( $\mu$ ) و نرخ ورود درخواست‌ها ( $\lambda$ ) نیز در نظر گرفته شده‌اند.

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

در این رابطه،  $v_{tot}$  نشان‌دهنده تعداد کل خودروها است. احتمال اشغال بودن تمامی کانال‌ها با استفاده از معادله (۲) محاسبه می‌شود.

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

که در آن  $P_0$  احتمال صفر بودن درخواست‌های ارتباطی در سیستم را نشان می‌دهد، که مقدار آن در معادله (۴) ارائه شده است. همچنین،  $\rho$  شدت ترافیک (Traffic Intensity) است که مقدار آن با استفاده از معادله (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  $v_{num}$  محسوبه می‌شود (۵). نشان‌دهنده احتمال پذیرفته شدن تمامی درخواست‌های ارتباطی است که مقدار آن در معادله (۵) ارائه شده است. همچنین، (۶) احتمال انتظار درخواست ارتباطی در صفحه را نشان می‌دهد که مقدار آن در معادله (۶) بیان شده است.

خواهد شد. این فرایند موجب می‌شود RSU بتواند در عین حفظ امنیت، مدیریت ترافیک ارتباطی را نیز به صورت 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 فیزیک و دیجیتال را با هدف ایجاد یک چارچوب امنیتی جامع در شبکه‌های IoT 6G ادغام 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 IoT 6G ایفا می‌کنند. یکی از نوآوری‌های مهم سیستم پیشنهادی، استفاده از مازول 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 تاکتیک مهاجمان همواره به روز باقی بماند و نرخ تشخیص حملات را افزایش دهد. علاوه بر این، معماری پیشنهادی با چارچوب IETF Digital Twin Network Architecture سازگار بوده و طراحی آن با اصول و استانداردهای شبکه‌های همزاد دیجیتال در حوزه ITS 6G هماهنگ است. همچنین، این ساختار به گونه‌ای توسعه یافته که امکان توزیع بار پردازشی میان لایه‌ها را فراهم کرده و در نتیجه موجب تسريع در تشخیص حملات و کاهش بار محاسباتی RSU‌های فیزیکی می‌شود.

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

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

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

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

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

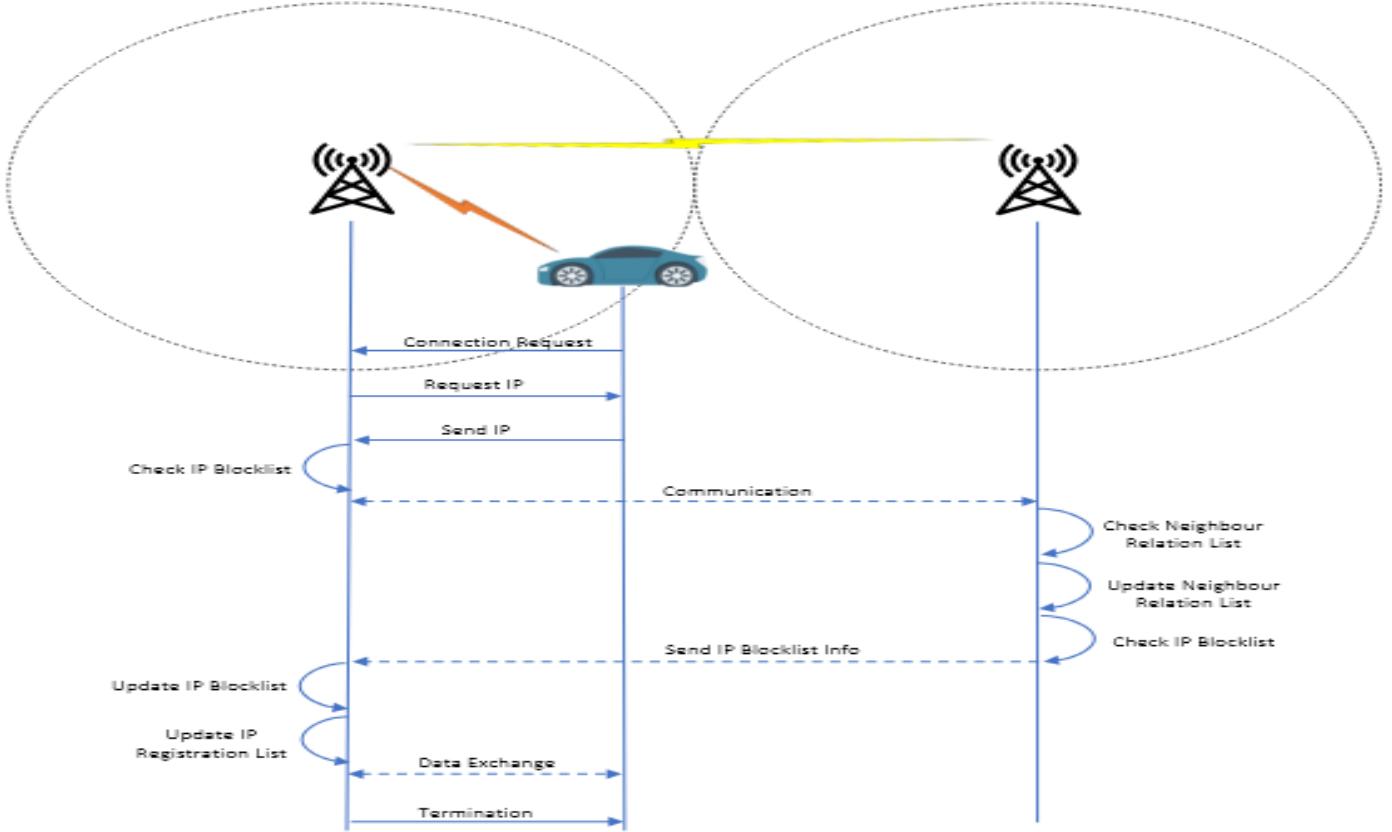
$$P_{Queue} = \frac{P_0 (c_{num}\rho)^{c_{num}}}{c_{num}! (1 - \rho)} \quad (7)$$

زمان میانگین انتظار در صف برای یک درخواست ارتباطی در مدل صف با استفاده از فرمول Erlang C به صورت زیر محاسبه می‌شود:

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

### B. Automated Neighbour RSU Relations

پس از مدل‌سازی درخواست‌های ارتباطی مربوط به هر RSU، گام بعدی در چارچوب پیشنهادی ما بررسی روابط میان RSU‌های همسایه است. در سیستم پیشنهادی، هر RSU یک فهرست مسدودسازی IP اختصاصی در اختیار دارد که شامل آدرس‌های IP مربوط به وسائل نقلیه مخرب شناسایی شده در گذشته است. به منظور افزایش کارایی سازوکارهای امنیتی، ما یک سازوکار رابطه خودکار میان RSU‌های همسایه تعریف می‌کنیم که مشابه با کار پیشین ما در [24] است؛ با این تفاوت که هدف اصلی در این پژوهش اشتراک گذاری خودکار آدرس‌های IP مخرب میان RSU‌های همسایه است. شکل 4، نمودار توالی سازوکار پیشنهادی برای ایجاد رابطه خودکار میان RSU‌های همسایه را نشان می‌دهد. این سازوکار هنگام دریافت یک درخواست اتصال از سوی یک وسیله نقلیه فعال می‌شود. در مرحله نخست، آدرس IP فرستنده را با فهرست مسدودسازی داخلی خود مقایسه می‌کند. سپس، برای افزایش دقت شناسایی تهدیدات، فهرست مسدودسازی RSU‌های همسایه نیز بررسی می‌شود. اگر IP موردنظر در هیچ‌یک از فهرست‌ها وجود نداشته باشد، سامانه هوشمند تشخیص حمله آغاز به کار 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 ۵ در رابطه (5) به یکی از کانال‌های در دسترس RSU تخصیص می‌یابد. اگر کانال آزاد موجود نباشد، درخواست مطابق با وضعیت ۶ در رابطه (6) وارد صف انتظار



شکل 4. نمودار توالی سازوکار خودکار میان RSU های همسایه برای فهرست آدرس های IP وسایل نقلیه مخرب در شبکه های G IoTV6

اصل Gemini با تعریف شفاف هدف، تضمین اعتماد و ارائه کارکردهای حیاتی برای شبکه های IoTG هم راست است. هدف این چارچوب، ارتقای امنیت و کارایی شبکه های خودرویی است و به ضرورت راهکارهای سارگارپذیر در محیط های پویای IoTV باخ می دهد. اعتماد از طریق یکپارچه سازی تحلیل های مبتنی بر هوش مصنوعی و پردازش داده های بلاذرنگ ایجاد می شود و این امر تشخیص تهدیدات را دقیق و قابل اطمینان می سازد. از نظر کارکردی، این چارچوب در چندین لایه فعالیت می کند که هر لایه نقش مهمی در دستیابی به هدف اصلی یعنی ارائه امنیت مقاوم، کارآمد و مقیاس پذیر برای شبکه های خودروی نسل بعدی دارد. با تمرکز بر این مؤلفه های اصلی، این چارچوب گامی مهم در به کارگیری فناوری دو قلوی دیجیتال در سامانه های حمل و نقل هوشمند به شمار می رود و عملکرد و تاب آوری بهبود یافته ای را در برابر تهدیدهای سایبری ارائه می دهد.

1. لایه داده

لایه داده به عنوان لایه پایه ای چارچوب، نقش حیاتی در جمع آوری و توزیع اطلاعات در لایه های مختلف شبکه خودروی 6G دارد. این لایه با ادغام مؤثر خودروها و RSU ها، داده هایی گردآوری می کند که از یک نمایش دقیق از اشیای فیزیک در لایه دو قلوی سایبری و نیز از ارزیابی های امنیتی راهکار پیشنهادی پشتیبانی می کنند. دقت لایه داده در نمایش بلاذرنگ و ارتباطات، برای حفظ کارایی و یکپارچگی سیستم مبتنی بر دو قلوی دیجیتال ضروری است.

## 2. لایه دو قلوی سایبری

لایه دو قلوی سایبری نقشی کلیدی در ایجاد مدل های دیجیتال پویا دارد که عناصر فیزیکی شبکه های IoTG را بازتاب می دهد و به افزایش سازگاری و دقت سیستم در تطبیق با شرایط واقعی کمک می کند. این لایه عملیات مهندسی ویژگی را انجام می دهد تا باز پردازشی لایه امنیتی کاهش یابد. این لایه شامل مأمور مهندسی ویژگی و مأمور یادگیری آنلاین است.

## ماژول مهندسی ویژگی

این ماژول از یک الگوریتم ssAE برای کاهش ابعاد ویژگی‌های داده استفاده می‌کند. یک معماری پیشرفته شبکه عصبی است که عمدها برای کاهش ابعاد و استخراج ویژگی به کار می‌رود. در این ساختار، چندین لایه خودرمزنگار پراکنده روی یکدیگر قرار می‌گیرند؛ به گونه‌ای که خروجی هر لایه ورودی لایه بعدی است. این ساختار سلسه‌مراتبی کمک می‌کند تا شبکه بتواند به تدریج ویژگی‌های پیچیده‌تر و سطح بالاتری از داده را بیاموزد.

عملکرد ssAE شامل دو مرحله اصلی است: کدگذاری و بازکدگذاری. در مرحله کدگذاری، شبکه داده‌های ورودی  $X$  را به یک نمایش کم‌بعدتر  $H$  با استفاده از تبدیل زیر فشرده می‌کند:

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

که در آن  $W_{ij}$  ماتریس وزن بین لایه ورودی و لایه پنهان در ssAE را تعريف می‌کند،  $\sigma$  یک تابع فعال‌ساز غیرخطی است، و  $\phi_1$  بردار بایاس برای لایه پنهان می‌باشد. مرحله کدگذایی (Decoding) تلاش می‌کند داده ورودی را از شکل فشرده‌شده آن بازسازی کند و بازسازی‌ای به نام  $Z$  را از طریق تبدیل زیر تولید می‌کند:

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

که در آن بردار بایاس برای لایه خروجی با  $\phi_2$  نشان داده می‌شود و ماتریس وزن از لایه پنهان به لایه خروجی با  $W_{jk}$  تعريف می‌گردد. هدف، کمینه‌سازی خطای بازسازی است تا شبکه تشویق شود اطلاعات ضروری را حفظ کرده و نویز را حذف نماید. علاوه بر این، ssAE یک قید پراکنده (sparsity constraint) بر فعال‌سازی لایه پنهان اعمال می‌کند تا اطمینان حاصل شود که تنها بخش کوچکی از نورون‌ها در هر زمان فعال باشند. این امر با جریمه کردن انحراف میانگین فعال‌سازی نورون‌های پنهان از یک پارامتر پراکنده از پیش تعیین شده  $\rho$ ، با استفاده از واگرایی کولبک-لایبلر (Kullback-Leibler divergence) [25] به دست می‌آید. تابع هزینه کلی ssAE ترکیبی از خطای بازسازی و جریمه پراکنده است و بدین ترتیب استخراج نمایش‌های فشرده و معنادار از داده‌های با ابعاد بالا را تسهیل می‌کند.

$$J_{\text{sparse}}(W, b) = J(W, b) + \Theta \sum_{j=1}^m \text{KL}(\rho \parallel \hat{\rho}_j) \quad (11)$$

که در آن  $m$  تعداد واحدهای پنهان را نشان می‌دهد، در حالی که  $\Theta$  یک 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]

$$\begin{aligned} J_{\text{sparse}}(W, b) &= J_E(W, b) + \Theta \sum_{j=1}^m \text{KL}(\rho \parallel \hat{\rho}_j) \\ &\quad + \frac{\lambda}{2} \sum_{r=1}^3 \sum_{i=1}^m \sum_{j=1}^{m+1} (w_{ij}^r)^2 \end{aligned} \quad (12)$$

که در آن  $\lambda$  ضریب تضعیف وزن‌ها (weight attenuation coefficient) نشان می‌دهد. الگوریتم 1 شبکه کدگذاری (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 رمزگشایش (decoder) در خطوط ۴ و ۵ مقداردهی اولیه می‌شوند. خطوط ۶ تا ۹ داده رمزگذاری شده را برای هر لایه از ۱ تا  $k$  نشان می‌دهند. سپس نمایش نهایی رمزگذاری شده  $X_k$  به عنوان  $Z$  نشان می‌شود که همان داده کاهش بُعد یافته است. داده رمزگذاری شده برای بازسازی ورودی رمزگشایی می‌شود. در خط ۱۳، برای هر رمزگشایی از  $k$  رو به ۱، رمزگشایی از  $m$  روی خروجی لایه بعدی یا روی نمایش نهایی رمزگذاری شده اعمال می‌شود (اگر اولین رمزگشا در توالی باشد). در نهایت، الگوریتم داده کاهش بُعد یافته  $Z$  را بازی گرداند. پس از کاهش تعداد ویژگی‌ها در ماژول ssAE، داده‌های کم بعد 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 مؤلفه AutoFS، یک عنصر AutoCM و یک الگوریتم انتخاب نهایی است. ما مؤلفه‌های AutoFS و AutoCM را از کارهای قبلی مان [27]، [28] گرفته‌ایم و آن‌ها را متناسب با نیازهای خاص محیط IoT 6G به روزرسانی کرده‌ایم. به لطف این ماژول، سیستم ما به صورت 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  $E_1, E_2, \dots, E_k$ 
5:   Initialise decoder layers  $D_1, D_2, \dots, D_k$ 
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

```

مولفه AutoFS شامل پنج الگوریتم انتخاب ویژگی (FS) است: کایدو (chi-square)، حذف بازگشته ویژگی ها (RFE)، تحلیل مؤلفه های اصلی (PCA)، جنگل تصادفی برای اهمیت ویژگی ها، و انتخاب ویژگی بر اساس مقدار F آنوا (ANOVA F-value). هر الگوریتم برای انواع خاصی از داده و نیازهای متفاوت طراحی شده است و به سیستم اجازه می دهد تا بر اساس ویژگی های داده های جاری و شرایط شبکه، به صورت پویا مناسب ترین روش را انتخاب کند. مولفه AutoCM شامل چهار روش طبقه بندی (CM) است: LSTM، XGBoost، MLP و ماشین های بردار پشتیبان (SVM) تا انعطاف پذیری و سازگاری لازم برای مدیریت انواع مختلف سناریوهای حمله در محیط های IoTG را فراهم کند. هر الگوریتم برای هدف خاص به کار می رود: برای شناسایی الگوهای پیچیده، برای XGBoost تحلیل کارآمد داده های ساخت یافته، برای LSTM تشخیص الگوهای ترتیبی، و SVM برای طبقه بندی در فضاهای با ابعاد بالا. از آنجا که ما از الگوریتم های یادگیری نظارت شده استفاده می کنیم، یک الگوریتم بر جسب گذاری نیز تعریف می کنیم تا هنگام به روزرسانی روش های CM و FS شبکه، داده های بدون بر جسب را بر جسب گذاری کند. این الگوریتم از هزار نمونه از داده های جاری شبکه — که با udata در ۷ نمایش داده شده — و هزار نمونه از داده های مبنا — که با bdata مخصوص شده — استفاده می کند. شبکه کد این الگوریتم در الگوریتم ۲ آمده است. ابتدا ورودی ها و خروجی ها در خطوط ۱ تا ۲ مشخص می شوند. سپس خوش بندی K-Means برای جداسازی اولیه udata به دو گروه استفاده می شود ( $K = 2$ ) تا داده ها بر اساس احتمال وجود یا عدم وجود حمله دسته بندی شوند (خطوط ۴-۵). این خوش های اولیه برای پیکربندی الگوریتم انتظار بیشینه سازی (EM) به کار گرفته می شوند. الگوریتم EM در خط ۹ برای اختصاص بر جسب های احتمالی اعمال می شود. پس از آن، ابتدا bdata افزایش دقت بر جسب گذاری استفاده می شود و یک فرآیند EM دوم برای بر جسب گذاری بهینه انجام می گیرد.

در نهایت، بر جسب های جدید 'ابا داده های مبنا' bdata ادغام شده و داده های کاملاً بر جسب گذاری شده data ادار خطوط ۱۶-۱۸ بازگردانده می شوند. این الگوریتم نقش بسیار مهمی در به روزرسانی پویا روش های چارچوب ما دارد. ما دقت این الگوریتم را با استفاده از تکنیک های اعتبار سنجی متقابل (cross-validation) به طور دقیق ارزیابی کرده ایم. در مجموعه ای از ارزیابی ها، این الگوریتم به دقت الگوریتم بر جسب گذاری به دقتی در حدود ۹۷/۲۱٪ دست یافته است؛ این معیار بسیار مهم است زیرا تضمین می کند که سیستم قادر است داده های جدید و در حال تغییر را به درستی پردازش و طبقه بندی کند. دقت بالای بر جسب گذاری به طور مستقیم باعث بهبود عملکرد ماژول انتخاب ویژگی (FS) و الگوریتم های طبقه بندی می شود و در نتیجه شناسایی تهدید های بالقوه در محیط IoTG با دقت بیشتری انجام می گیرد. برای حفظ این سطح از عملکرد در طول زمان، مجموعه داده مبنا در بازه های زمانی از پیش تعیین شده به روزرسانی می شود.

این به روزرسانی ها تضمین می کند که الگوریتم بر جسب گذاری با جدید ترین رفتارهای شبکه و تهدید های نوظهور همسو باقی بماند. با همگام سازی مداوم با الگوهای داده ای روز، سیستم دقت و سازگاری بالای خود را حقی در شرایط پرتلاطم و متغیر محیط های IoTG حفظ می کند.

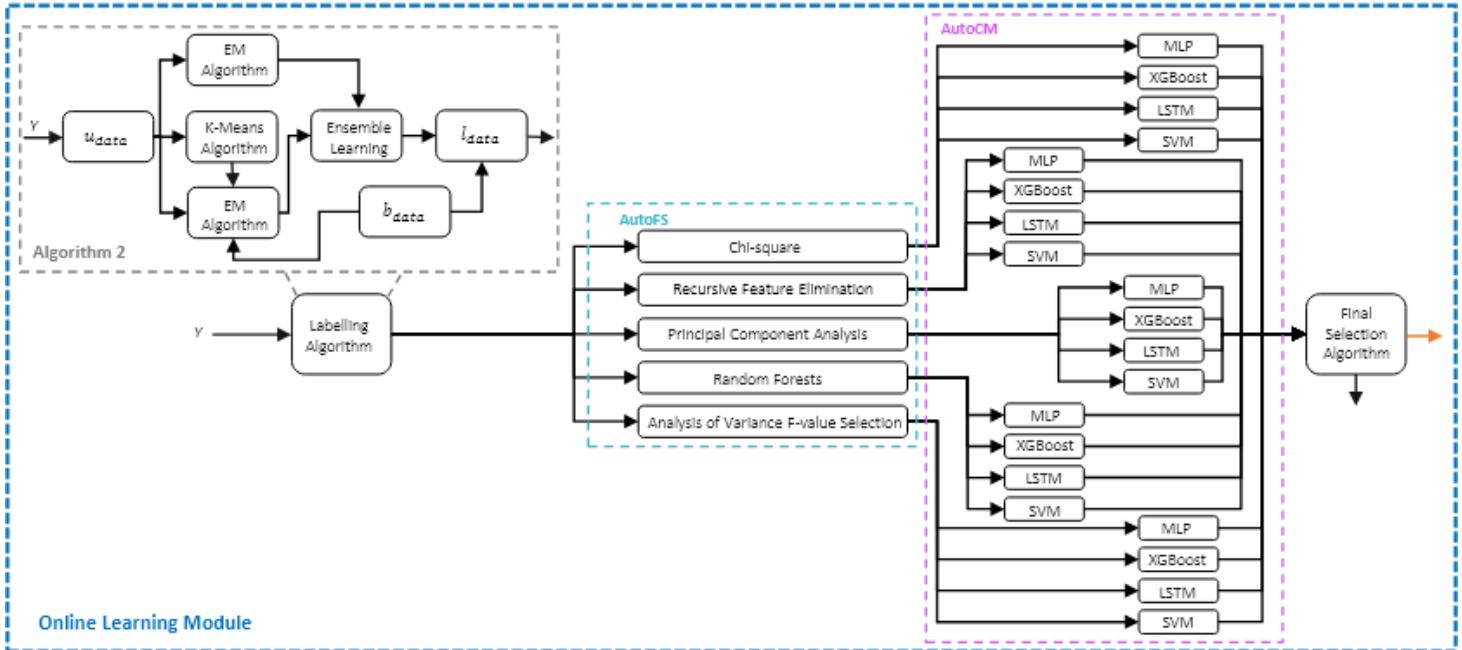
اگر هر یک از معیارهای عملکردی کمتر از آستانه تعیین شده خود قرار گیرد، ماژول یادگیری آنلاین روش انتخاب ویژگی شبکه (FS) و روش طبقه بندی شبکه (CM) را به روزرسانی می کند. برای این منظور، این ماژول از طریق الگوریتم های بر جسب گذاری و انتخاب نهایی، هزار نمونه از داده های فعلی شبکه را پردازش می کند. این اطلاعات به روزرسانی از لایه امنیتی دریافت می شود؛ لایه ای که مسئول بررسی میزان قابلیت اطمینان و سلامت سیستم است.

پس از دریافت اطلاعات به روزرسانی از لایه امنیتی، هزار نمونه از داده های فعلی شبکه وارد ماژول یادگیری آنلاین می شود. این داده ها ابتدا با استفاده از الگوریتم بر جسب گذاری، بر جسب دار می شوند. پس از بر جسب گذاری، مولفه AutoFS از این داده های بر جسب دار استفاده می کند. سپس خروجی AutoFS به عنصر AutoCM ارسال می شود.

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

الگوریتم ۳ شبکه کد الگوریتم انتخاب نهایی ما را ارائه می دهد. این الگوریتم، با توجه به معیارهای دقت (precision)، بازیابی (recall) و زمان تشخیص الگوریتم ها، درباره انتخاب روش های انتخاب ویژگی (FS) و طبقه بندی (CM) شبکه تصمیم گیری می کند.

الگوریتم انتخاب نهایی، اطلاعات مربوط به بهترین روش FS را به روش انتخاب ویژگی شبکه در لایه دولوی سایری ارسال می کند، و سپس روش FS شبکه با الگوریتم جدید شروع به کار می کند. همچنین، الگوریتم انتخاب نهایی اطلاعات مربوط به بهترین تکنیک CM را به الگوریتم طبقه بندی شبکه در لایه امنیتی ارسال می کند و این لایه نیز با روش جدید فعالیت خود را آغاز می نماید.



شکل ۵. منطق کاری مژول یادگیری آنلاین پیشنهادی.

#### Algorithm 2 Labelling Algorithm.

```

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

```

چندین الگوریتم، مازیک معماری مبتنی بر ریزخدمات (microservice) استفاده می‌کنیم که در آن اجزای مختلف مژول یادگیری آنلاین به عنوان سرویس‌های مستقل و کوچک‌تر اجرا شوند. این رویکرد مقیاس‌پذیری را افزایش می‌دهد و امکان مدیریت مؤثر اجزای مختلف را فراهم می‌سازد.

#### Algorithm 3 Final Selection Algorithm

```

1: Input: precision (P), recall (R), and detection time ( $d_t$ ) for each CM method and its pair FS techniques
2: Output: bestFS and bestCM for the system
3: procedure FINAL-METHODS(P, R,  $d_t$ )
4:   # to store precision, recall, and detection time for each FS and CM combination
5:   Initialize matrix M
6:   for  $i = 1$  to  $5$  do
7:     for  $j = 1$  to  $4$  do
8:       # metric vector for  $i^{th}$  FS and  $j^{th}$  CM
9:        $V_{ij} \leftarrow$  vector of P, R,  $d_t$ 
10:       $M[i, j] \leftarrow V_{ij}$ 
11:    end for
12:   end for
13:   #  $\alpha_{ij}$ ,  $\beta_{ij}$  are the weights for  $i^{th}$  FS and  $j^{th}$  CM
14:   #  $\psi_{ij}$  is the weighted sum of P and R
15:   bestFS, bestCM  $\leftarrow 0, 0$ 
16:   maxScore  $\leftarrow -\infty$ 
17:   for  $i = 1$  to  $5$  do
18:     for  $j = 1$  to  $4$  do
19:        $\psi_{ij} \leftarrow (0.55) \times R + (0.45) \times P$ 
20:       score $_{ij} \leftarrow \alpha_{ij} \times \psi_{ij} + \beta_{ij} \times d_t$ 
21:       if (score $_{ij} > maxScore$ )
22:         maxScore  $\leftarrow score_{ij}$ 
23:         bestFS, bestCM  $\leftarrow i, j$ 
24:       end if
25:     end for
26:   end for
27:   Return bestFS, bestCM
28: end procedure

```

این انتخاب سازگارپذیر تضمین می‌کند که سیستم بتواند به طور 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 به صورت شبکه‌آه حفظ می‌کند. این سازوکار تقریباً در زمان واقعی کار می‌کند. برای مدیریت کارآمد باز محاسبات ناشی از اجرای

اجرای همزمان الگوریتم‌های مختلف تضمین می‌کند که چارچوب ما هم مؤثر و هم کارآمد باقی بماند و قادر باشد نیازهای سخت‌گیرانه شبکه‌های ۱۰V در ۶G را برآورده کند. علاوه بر این، فعالسازی شرطی روش‌ها تضمین می‌کند که منابع محاسباتی به صورت 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 ۱۰V است. رویکرد ما یک معماری طبقه‌بندی پیشرفته را برای دسته‌بندی ترافیک شبکه به دو دسته «حمله» و «غیرحمله» ادغام می‌کند. این لایه شامل الگوریتم طبقه‌بندی شبکه، طبقه‌بندی حمله، و مولفه آستانه تأیید است. با توجه به ماهیت پویا در محیط ۶ – ۱۰V که در آن جریان داده و ویژگی‌های شبکه دائم تغییر می‌کنند – سیستم ما از مژویل یادگیری آنلاین در لایه دوقلوی سایبری استفاده می‌کند. این فرایند یادگیری پیوسته از طریق پایش معیار قابلیت اعتماد سیستم نسبت به یک آستانه از پیش تعیین شده پشتیبانی می‌شود. اگر مقدار معیار قابلیت اعتماد کمتر از آستانه شود، یک مکانیزم بهروزرسانی فعال می‌شود و مژویل یادگیری آنلاین را فراخوانی می‌کند. این مژویل شامل فرآیندهای انتخاب آگاه از شبکه 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 دقیق باشی در تشخیص حملات را حفظ کند. ما به همین منظور هدف زیر را تعیین می‌کنیم.

$$V(\mathfrak{S}) = \begin{cases} 1, & \text{if } \mathfrak{R} < \mathfrak{S} \\ 0, & \text{otherwise} \end{cases}$$

که در آن  $(\mathfrak{S})V$  تابع آستانه تأیید یا *verifying threshold function* نشان می‌دهد و  $\mathfrak{R}$  مقدار آستانه است. اگر خروجی تابع مقدار «۱» باشد، مکانیزم بهروزرسانی برای مژویل یادگیری آنلاین فعال می‌شود. برای محاسبه میانگین قابلیت اعتماد سیستم (system) (system) زیر استفاده می‌شود:

$$\mathfrak{R} = \frac{TP}{FN + TP} \quad (13)$$

که در آن  $\mathfrak{R}$  نشان‌دهنده 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، مژویل آستانه تأیید (verifying threshold component) به طور کامل قابلیت اعتماد الگوریتم

دسته‌بندی سیستم را بررسی می‌کند. مقدار آستانه ( $\mathfrak{S}$ ) به صورت زیر محاسبه می‌شود:

$$\mathfrak{S} = \tau + \gamma_i \varrho, \quad \forall i \in [1, 4] \quad (14)$$

که در آن  $\mathfrak{S}$  میانگین و  $\varrho$  انحراف معیار است  $\tau$ . ضریب آستانه برای الگوریتم دسته‌بندی  $i$  می‌باشد.

این چارچوب شناسایی حمله پیش‌گیرانه و تطبیقی، گامی مهم در جهت حفاظت از شبکه‌های ۱۰V در برابر طیف رو به گسترش تهدیدات سایبری محسوب می‌شود و به این ترتیب یکپارچگی و قابلیت اطمینان سیستم‌های ارتباطی وسایل نقلیه را حفظ می‌کند.

### ۴. ارزیابی عملکرد

در این بخش، هدف ما نشان دادن کارایی چارچوب پیشنهادی در یک محیط شبیه‌سازی شده ۱۰V است. 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:

- ۵.۱ نسخه OMNeT++
- ۰.۳۰.۰ نسخه SUMO
- ۳.۶ نسخه INET
- ۴.۷ نسخه Veins

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 به طور غیرقابل پیش‌بینی تغییر کنند. تنظیمات شبیه‌سازی ما شامل تغییرات پویا در شرایط شبکه است که سناریوهای دنیای واقعی را شبیه‌سازی می‌کند. با استفاده از SUMO، الگوهای ترافیکی مختلف از جمله ساعت‌الوج با تراکم بالا و ساعات غیر الوج با تراکم کم شبیه‌سازی شدند. این کار به ما ممکن می‌کند تا توانایی چارچوب در مدیریت انتقال و پردازش داده‌ها تحت بارهای مختلف را ارزیابی کنیم. با استفاده از INET، 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 ۱۰V رایج است، مورد بررسی قرار گیرد.

ما همزادهای سایبری (Cyber Twins) از گرههای فیزیک (وسایل نقلیه) در VANET ایجاد کردیم با استفاده از Ditto Eclipse، یک چارچوب متن باز که مقیاس پذیر و چندمنظوره است [30]. با استفاده از این ابزار، می توانیم پارامترهای شبیه سازی را به طور پویا و در زمان واقعی بر اساس داده های تازه دریافتی از شبکه وسایل نقلیه تنظیم کنیم. این تنظیمات اطمینان می دهد که پاسخ سیستم با شرایط متغیر محیط شبیه سازی تطبیق پیدا کند و به این ترتیب، کاربرد عملی چارچوب ما در یک محیط پویا نشان داده می شود. 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 داده RF Jamming Dataset: RF Jamming در مجموعه شامل چندین سناریوی حمله RF Jamming در محیط های VANET است و دارای دو زیرمجموعه برای سرعت های نسبی تخمینی مختلف می باشد [31]. ما این زیرمجموعه ها را ادغام کردیم تا راهکار پیشنهادی خود را به طور جامع ارزیابی کنیم. این مجموعه داده شامل سناریوهایی با حملات RF Jamming است و بینش های دریاره چگونگی عملکرد سیستم در مواجهه با تداخل های شدید ارائه می دهد. دومین مجموعه داده ToN-IoT: این مجموعه برای آزمون پایداری و اثربخشی ابزارهای امنیت سایبری مبتنی بر هوش مصنوعی در نسل بعدی IoT و محیط های صنعتی طراحی شده است [32]. این مجموعه شامل انواع مختلف حملات IoT است و پیچیدگی را افزایش داده و به اعتبار سنجی کارایی چارچوب در مقابل تهدیدات سایبری پیشرفت کمک می کند.

جدول II توزیع مجموعه داده ترکیبی: ادغام مجموعه داده های RF Jamming و ToN-IoT

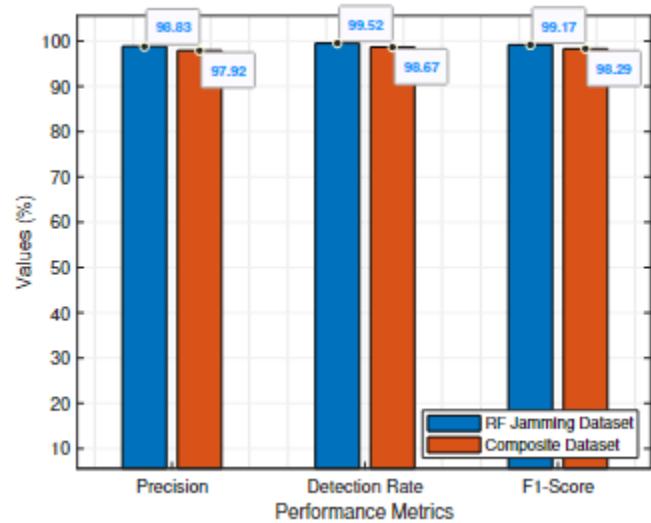
Dataset Name	Number of Samples
RF Jamming Dataset-1 (No Attack Samples)	1000
RF Jamming Dataset-2 (No Attack Samples)	1000
ToN-IoT Network Dataset (Attack Samples)	600

اگرچه مجموعه داده ToN-IoT به طور اولیه بر روی VANET تمرکز ندارد، با ادغام نمونه های بدون حمله از مجموعه داده RF Jamming با نمونه های حمله از مجموعه داده ToN-IoT، ما یک مجموعه داده جدید مناسب با تحلیل امنیتی VANET خود ایجاد کردیم. این مجموعه داده ترکیبی، که در جدول II به تفصیل آمده است، با دقت برای تعادل نمونه های حمله و غیرحمله انتخاب شد تا پایه ای جامع برای ارزیابی عملکرد ما فراهم کند. مجموعه داده جدید، که ترکیبی از دو مجموعه داده است، بیشتر بر IoT و VANET متمرکز است. بنابراین، هدف ما دستیابی به نتایج جامع تر برای سیستم های حمل و نقل هوشمند (ITS) با استفاده از داده های

VANET و IoT است. همچنین، نمونه های داده حمله به صورت تصادفی در طول شبیه سازی ها به داده های وسایل نقلیه اضافه شدند تا قابلیت مجموعه داده در آزمایش چارچوب تحت شرایط متنوع و غیرمنتظره افزایش یابد.

## ب. نتایج

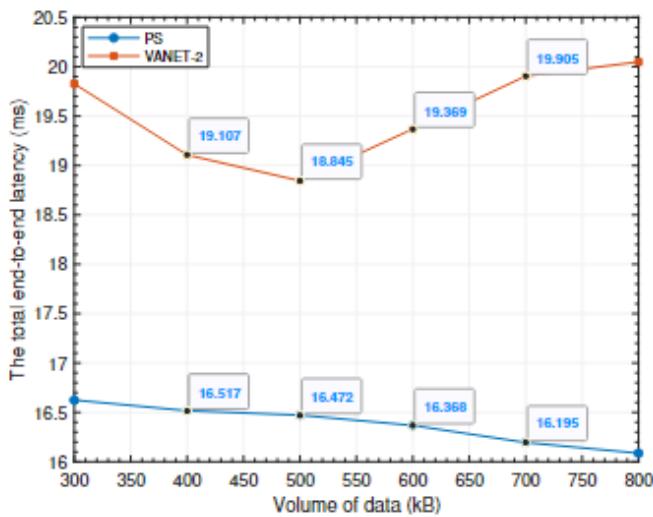
ابتدا، عملکرد شناسایی حمله راه حل پیشنهادی خود را با استفاده از هر دو مجموعه داده RF Jamming و مجموعه داده ترکیبی بررسی کردیم. شکل 6 نتایج عملکرد راه حل ما را از نظر نرخ شناسایی حمله، دقت و معیار F1 نشان می دهد. نتایج مجموعه داده RF Jamming تقریباً ۹۹٪ و نتایج مجموعه داده ترکیبی تقریباً ۹۸٪ موفقیت در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



شکل 6. تحلیل عملکرد راه حل پیشنهادی در مجموعه داده ها

سپس، اثربخشی راه حل خود را در شرایط پویا بررسی کردیم. برای این منظور، به طور دوره ای نمونه های حمله از مجموعه داده ترکیبی را وارد شبیه سازی کردیم تا قابلیت های سیستم در زمینه تأخیر انتها به انتها، مصرف انرژی، استفاده از حافظه RAM و نرخ تحویل بسته ها را در زمان واقعی بسنجیم. این روش به ما امکان می دهد پاسخ دهنده و سازگاری سیستم با تغییرات ناگهانی در محیط حمله را درک کنیم. تأخیر انتها به انتها (End-to-End Latency): زمان انتقال داده ها از منبع به مقصد را اندازه گیری می کند که برای برنامه های زمان واقعی حیاتی است. مصرف انرژی (Energy Consumption): کارایی انرژی سیستم را تحت بارهای شبکه و الگوهای حرکتی متغیر ارزیابی می کند. استفاده از RAM: کارایی حافظه سیستم را بررسی می کند که بر سرعت و پاسخ دهنده بردازش داده ها تأثیر می گذارد. نرخ تحویل بسته ها (Packet Delivery Rate): اطمینان از تحویل صحیح و کامل بسته های داده را با وجود

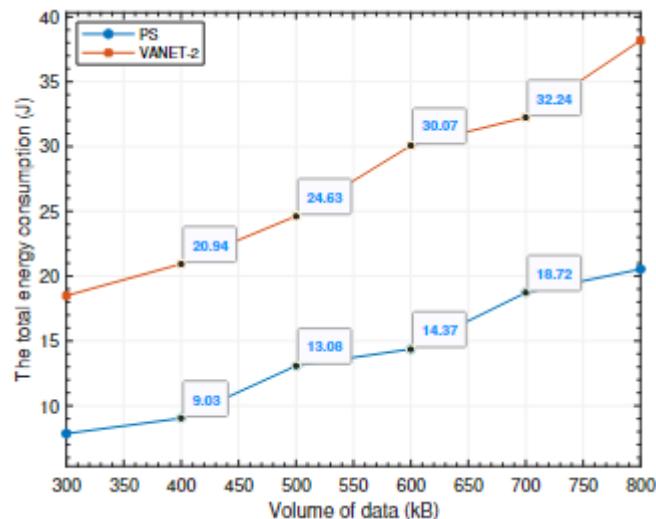
تغییرات دینامیک شبکه ارزیابی می‌کند. برای مقایسه عملکرد راه حل پیشنهادی ما (PS)، شبکه دیجیتال توین VANET کردیم که تمام اجزای پردازشی آن در لایه امنیت قرار دارند و از مهندسی ویژگی‌ها استفاده نمی‌کند. این شبکه از الگوریتم LSTM برای شناسایی حمله بهره می‌برد، زیرا این روش در مطالعات شناسایی حمله در VANET 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-2 و راه حل ما ویژگی‌های عملکردی متفاوتی را با افزایش حجم داده نشان می‌دهد. در VANET-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 به طور مؤثر مدیریت می‌کنند، اما زمانی که بارها از ظرفیت سیستم فراتر می‌روند، عملکردشان کاهش می‌یابد. بر عکس، راه حل ما عملکرد به مرتب بهتری نشان می‌دهد. این به دلیل تقسیم استراتژیک بار محاسباتی بین لایه‌های سایر توین 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-2 می‌شود. به طور مشابه، شکل ۸ نشان می‌دهد که راه حل 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.



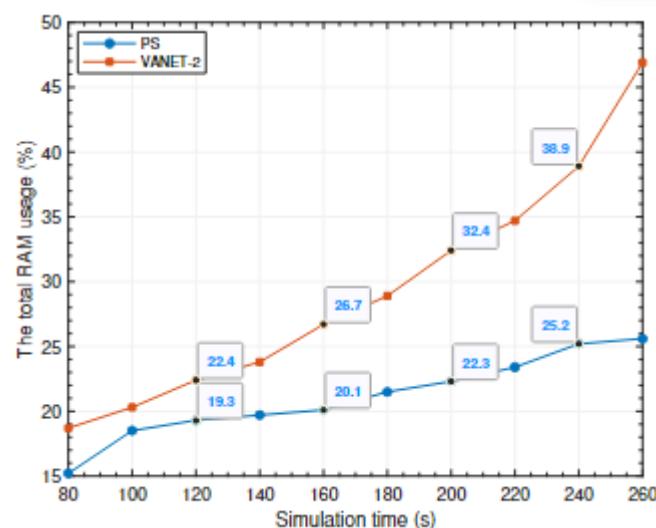
شکل ۷. مقایسه تأخیر کل انتها به انتها بر اساس حجم داده‌ها.

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

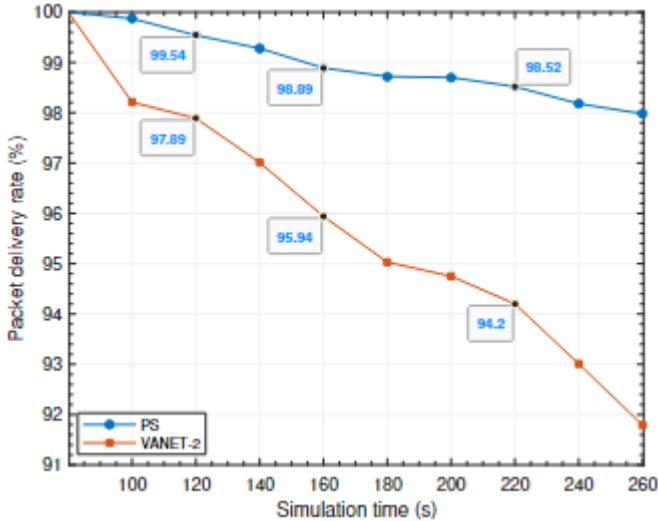
تحویل بسته‌ها بین راه حل ما و VANET-2 را می‌توان در شکل ۱۰ در طول زمان‌های مختلف شبیه‌سازی مشاهده کرد. در حالی که VANET-2 به شدت بسته‌ها را از دست می‌دهد، راه حل ما عملکرد پایداری نشان می‌دهد. راه حل ما با افتی حدود ۱/۸٪ از مقدار شروع تا مقدار نهایی روبرو است، در حالی که سیستم VANET-2 کاهش چشمگیرتری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



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



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



شکل ۱۰. مقایسه 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 مقرن به صرفه‌تر می‌شود، امری که برای پیاده‌سازی شبکه‌های پیشرفته و اینمن خودروها حیاتی است. از طریق شبیه‌سازی دقیق و تحلیل‌ها، توانسته‌ایم کاهش مصرف RAM، قابلیت‌های قوی شناسایی حمله و افزایش نرخ تحویل بسته‌ها در چارچوب دیجیتال تؤیین خود را نشان دهیم. این پیشرفته‌ها گامی مهم به سوی شبکه‌های حمل و نقل 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 حمل و نقل هوشمند است.

## ۷. بحث

پیاده‌سازی عملی سیستم پیشنهادی برای شبکه‌های 6G 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، به گونه‌ای که RSU‌ها 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 راه حل‌های 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

به این جنبه‌های عملی، چارچوب پیشنهادی می‌تواند امنیت و کارایی شبکه‌های 6G را به طور قابل توجهی بهبود بخشد و به توسعه سیستم‌های حمل و نقل هوشمند و مقاوم کم کند.

چارچوب پیشنهادی برای شبکه‌های 6G پیشرفت‌های 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 و UEs است، در حالی که تأخیر پایین و پردازش به موقع 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 بزرگ مقیاس 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 6G حیاتی است.

## ۷. نتیجه‌گیری

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

با شبیه‌سازی‌های جامع، نشان دادیم که چارچوب ما هم کارایی محاسباتی را بهبود می‌بخشد و هم ارتباطات در VANET‌ها را اینم می‌کند. در مقابل دو مجموعه داده، چارچوب ما حدود ۹۸٪ موفقیت در معیارهای شناسایی حمله به دست می‌آورد که پتانسیل آن برای اینم‌سازی 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 ۶۱٪ بهبود می‌بخشد، در مقایسه با معماری سنتی از نظر کارایی محاسباتی.

چارچوب ما آینده‌ای ایمن‌تر و مؤثرتر برای ارتباطات خودروها و عده 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.