علوم رایانش و فناوری اطلاعات
نشریه علمی انجمن کامپیوتر ایران
مجلد ۲۰، شماره ۱، ۱۴۰۱
صفحات ۲۰ -۳۰
مقاله پژوهشی

ارائه یک طرح تشخیص بدرفتاری داده محور و آگاه از زمینه در شبکه‌ی بین خودرویی

زهرا گرجی[۱]، سعید شکرالهی[۲*]

*نویسنده مسئول، دریافت: ۱۴۰۱/۰۱/۲۸، بازنگری: ۱۴۰۱/۰۴/۱۳، پذیرش: ۱۴۰۱/۰۴/۲۰

[۱] کارشناسی ارشد، رشته‌ی مخابرات امن و رمزنگاری، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، تهران، ایران
[۲] استادیار، گروه امنیت شبکه و رمزنگاری، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، تهران، ایران

چکیده

شبکه‌های بین خودرویی فناوری‌های نوظهوری هستند که عملکردشان وابسته به در دسترس بودن اطلاعات دقیق و به‌روز وسایل نقلیه است. وسایل نقلیه‌ای که اطلاعات غیرعادی منتشر می‌کنند به‌راحتی می‌توانند در عملکرد شبکه‌ی بین خودرویی اختلال ایجاد کنند. بنابراین تشخیص چنین بدرفتاری‌هایی برای حفظ امنیت شبکه‌ی بین خودرویی در برابر مهاجمان، حیاتی است. در اکثر طرح‌های تشخیص بدرفتاری گذشته توجه کمی به استفاده از ویژگی‌های نظریه‌ی جریان ترافیک شده است، درحالی‌که این نظریه می‌تواند ابزاری قوی برای ارزیابی صحت اطلاعات زمینه‌ی منتشرشده در شبکه‌ی بین خودرویی باشد. در این مقاله برای بهبود چالش‌های طرح‌های تشخیص بدرفتاری گذشته، استفاده از نظریه‌ی جریان ترافیک را در تشخیص بدرفتاری‌های ناشی از ارسال اطلاعات غیرعادی در شبکه‌های بین خودرویی پیشنهاد شده است. در طرح پیشنهادی، علاوه بر واحدهای کنار جاده‌ای، واحدهای محاسباتی روی وسایل نقلیه نیز به‌عنوان منابع قابل‌اطمینان اطلاعات در نظر گرفته می‌شوند که این موضوع به کاهش هزینه‌های ناشی از پیاده‌سازی سراسری واحدهای کنار جاده کمک می‌کند. نتایج ارزیابی این طرح در انواع شرایط ترافیکی و با درصدهای مختلف اطلاعات غیرعادی نشان‌دهنده‌ی کاهش نرخ هشدارهای کاذب و بهبود دقت تشخیص است.

کلمات کلیدی: تشخیص بدرفتاری داده محور، آگاه از زمینه، شبکه‌ی بین خودرویی ، نظریه‌ی جریان ترافیک، داده‌های غیرعادی و امنیت شبکه‌ی بین خودرویی

۱- مقدمه

شبکه‌های بین خودرویی[۱] با کاربرد گسترده‌ای که در سیستم هشدار اضطراری، مدیریت ترافیک و کاربردهای نظامی دارند، اهداف سیستم حمل‌ونقل هوشمند را به واقعیت تبدیل می‌کنند. شبکه‌های بین خودرویی نوعی از شبکه‌های موردی متحرک[۲] هستند و عمدتاً برای بهبود ایمنی جاده‌ها، کاهش تراکم ترافیک و ایجاد آسایش مسافران پدید آمده‌اند. وسایل نقلیه به کمک حسگرها و قابلیت‌های محاسباتی و ارتباطی‌شان به‌طور مداوم اطلاعات تحرک خود شامل موقعیت، سرعت، شتاب، هشدارهای رویداد، اطلاعات ترافیک و غیره را در پیام‌های دوره‌ای که به‌عنوان پیام‌های آگاهی مشارکتی[۳] شناخته می‌شوند در فواصل زمانی منظم در محیط شبکه به اشتراک می‌گذارند تا وسایل نقلیه همسایه را از وضعیت وسایل نقلیه اطراف خود، آگاه کنند و درک رانندگان را از اطلاعات زمینه‌ی شبکه‌ی بین خودرویی افزایش دهند [۲]. در واقع این پیام‌ها حاوی اطلاعات زمینه‌ی شبکه‌ی بین خودرویی هستند.

بسیاری از برنامه‌ها و خدمات شبکه‌ی بین خودرویی به‌شدت بر دقت، یکپارچگی و قابلیت اطمینان اطلاعات شبکه متکی هستند. رفتار نادرست مهاجمان ازنظر سوءاستفاده یا دستکاری اطلاعات تحرک وسایل نقلیه، می‌تواند عملکرد برنامه‌های شبکه‌ی بین خودرویی را مختل کند. راه‌حل‌های امنیتی بسیاری برای حفظ امنیت پیام‌های شبکه‌ی بین خودرویی پیشنهاد شده است، این راه‌حل‌های امنیتی را می‌توان به راه‌حل‌های پیشگیری و تشخیص دسته‌بندی کرد. راه‌حل‌های امنیتی پیشگیرانه، مانند تکنیک‌های رمزنگاری، برای جلوگیری از دستکاری اطلاعات پیام‌های منتشرشده در شبکه‌ی بین خودرویی استفاده می‌شوند. بااین‌حال، تکنیک‌های مبتنی بر رمزنگاری برای ایمنی در برابر وسایل نقلیه‌ی بدرفتار داخلی که پیام‌های معتبر اما نادرست را ارسال می‌کنند، کافی نیستند [۳]. طرح‌های تشخیص بدرفتاری[۴] هنگامی‌که راه‌حل‌های پیشگیرانه شکسته می‌شوند، به‌عنوان دیوار دفاعی دوم در برابر مهاجمان بدرفتار عمل می‌کنند تا از صحت و کیفیت

داده‌هایی که توسط خودروهای همسایه به اشتراک گذاشته می‌شوند، اطمینان حاصل کنند [۴].

بر اساس اهداف تشخیص، روش‌های تشخیص بدرفتاری به دو دسته‌ی طرح‌های داده محور و گره محور طبقه‌بندی می‌شوند. درحالی‌که هدف طرح‌های گره محور شناسایی هویت وسایل نقلیه‌ی بدرفتار و جداسازی مهاجمان از شبکه است. هدف طرح‌های داده محور بررسی صحت اطلاعات به اشتراک گذاشته‌شده در وسایل نقلیه است [۵]. طرح‌های تشخیص بدرفتاری گره محور به طرح‌های مبتنی بر رفتار و طرح‌های مبتنی بر اعتماد دسته‌بندی می‌شوند [۶]. در طرح‌های گره محور مبتنی بر رفتار یک شخص ثالث قابل‌اعتماد که اعتبارنامه‌ها را صادر می‌کند وجود دارد که رفتار قابل‌مشاهده‌ی گره‌ها را بازرسی می‌کند و معیاری برای تعیین صحت عملکرد یک گره استخراج و تعریف می‌کند. در این طرح‌ها رفتار غیرطبیعی گره، دور انداختن یا تکثیر بسته‌ها در شبکه است. به دلیل پویایی شبکه، ممکن است وسایل نقلیه‌ی عادی مطابق انتظار رفتار نکنند و رفتار عادی به‌اشتباه بدرفتاری طبقه‌بندی شوند، که باعث کاهش دقت[۵] تشخیص و افزایش نرخ مثبت غلط[۶] در طرح‌های تشخیص گره محور مبتنی بر رفتار می‌شوند. از طرفی طرح‌های تشخیص بدرفتاری مبتنی بر اعتماد از اطلاعات حاصل از بررسی عملکرد گذشته و حال یک گره، برای به دست آوردن احتمال بدرفتاری آن گره در آینده استفاده می‌کنند. درواقع یک طرح تشخیص مبتنی بر اعتماد یک طرح مدیریت شهرت است که رفتار صحیح باعث افزایش و رفتار نادرست باعث کاهش شهرت می‌شوند.

در اغلب طرح‌های گره محور بعد از شناسایی گره‌ی بدرفتار بهترین اقدام، اعمال جریمه‌هایی است که گره‌ها را از بدرفتاری دلسرد کند. اما در طرح‌های گره محور اغلب بعد از شناسایی بدرفتاری، گره‌ی مخرب را از شبکه اخراج یا ابطال می‌کنند که ابطال و اخراج بیش‌ازحد گره‌های بدرفتار از شبکه علاوه بر ایجاد سربار ناشی از لیست ابطال باعث می‌شوند تا با کاهش تراکم شبکه، در عملکرد طرح‌های تعاونی اختلال ایجاد شود. همچنین با اخراج هریک از گره‌های بدرفتار یکی از منابع اطلاعات شبکه حذف می‌شود که ممکن است در آینده اطلاع مفیدی داشته باشد. درنهایت می‌توان گفت اغلب رویکردهای گره محور گران هستند و برای تشخیص طولانی‌مدت طراحی‌شده و فقط می‌تواند انواع خاصی از حملات آشکار را شناسایی کنند. بنابراین اکثر طرح‌های تشخیص بدرفتاری جدید داده محور یا ترکیبی هستند.

در طرح‌های تشخیص داده محور، تشخیص بدرفتاری با بررسی سازگاری[۷] و قابل‌قبول بودن[۸] اطلاعات دریافتی از وسایل نقلیه ارزیابی می‌شود. حفظ حریم خصوصی، شناسایی حملات در مراحل اولیه و در زمان واقعی از مزایای طرح‌های داده محور هستند که این طرح‌ها را برای استفاده در برنامه‌های مهم و حساس، کاربردی می‌کنند [۴]. اکثر راه‌حل‌های تشخیص بدرفتاری موجود برای ارزیابی سازگاری و معقول بودن اطلاعات به آستانه‌های امنیتی از پیش تعریف‌شده و ثابت تکیه می‌کنند که مناسب محیط پویای شبکه‌ی بین خودرویی نیستند و آن راه‌حل‌ها را مستعد نرخ بالای مثبت غلط و دقت تشخیص پایین می‌کنند. درنتیجه هدف ما ارائه‌ی طرحی قابل‌تعمیم است که نقاط ضعف طرح‌های گذشته را نداشته باشد و بتواند با دقت و سرعت بالایی بدرفتاری‌های ناشی از ارسال اطلاعات غیرعادی را تشخیص دهد و با جلوگیری از انتشار اطلاعات غلط در شبکه، مانع از ایجاد اختلال در عملکرد برنامه‌های شبکه‌ی بین خودرویی شود.

در این مقاله، یک طرح تشخیص بدرفتاری داده محور و آگاه از زمینه[۹] به کمک مفاهیم نظریه‌ی جریان ترافیک[۱۰] پیشنهاد شده است. طبق این نظریه، داده‌های ترافیکی که توسط گروهی از وسایل نقلیه از یک منطقه مشخص در یک زمان معین منتقل می‌شوند، باید با قوانین اساسی توصیف‌شده توسط نظریه‌ی جریان ترافیک، یعنی رابطه اساسی بین پارامترهای میکروسکوپی و ماکروسکوپی نظریه‌ی جریان ترافیک سازگار باشند و اطلاعات منتشرشده در پیام‌های دوره‌ای طبق این قوانین قابل‌قبول باشند. روش پیشنهادی داده‌های قابل‌اعتماد برای ساخت یک مرجع تشخیص را از طریق واحدهای کنار جاده[۱۱] در صورت وجود و یا از طریق واحدهای محاسباتی روی وسایل نقلیه[۱۲] به‌صورت محلی استنباط می‌کند. اطلاعات قابل‌اعتماد به‌دست‌آمده از واحدهای کنار جاده و واحدهای محاسباتی روی وسایل نقلیه به همراه قوانین نظریه‌ی جریان ترافیک برای تعیین اعتبار داده‌هایی که توسط هر وسیله نقلیه منتشر می‌شود در تشخیص اطلاعات غیرعادی[۱۳] مورداستفاده قرار می‌گیرد. در طرح پیشنهادی، بدرفتاری‌های ناشی از ارسال اطلاعات غیرعادی در شبکه‌ی بین خودرویی در انواع شرایط ترافیکی متراکم و آزاد طبق شرایط ترافیکی دنیای واقعی شناسایی می‌شوند. در این طرح، با بررسی سازگاری پارامترهای میکروسکوپی منتقل‌شده در پیام‌های دوره‌ای (سرفاصله‌ی زمانی، سرفاصله‌ی مکانی و سرعت فردی) و پارامترهای ماکروسکوپی محاسبه‌شده با استفاده از اطلاعات منابع قابل‌اطمینان (نرخ جریان، نرخ چگالی و میانگین سرعت) به دنبال تشخیص سریع و دقیق بدرفتاری‌های داده محور هستیم. ارزیابی نتایج پیاده‌سازی طرح تشخیص بدرفتاری به کمک نرم‌افزارهای SUMO و NS2 نشان می‌دهد که طرح پیشنهادی پیش‌بینی‌های قابل‌اعتمادی از تشخیص بدرفتاری‌های ناشی از داده‌های غیرعادی ارائه می‌دهد و نتایج این مدل تشخیص آگاه از زمینه به‌منظور کاهش هشدار کاذب و بهبود دقت تشخیص، امیدبخش هستند.

در ادامه ساختار مقاله به‌صورت زیر سازماندهی‌شده است. در بخش دوم برخی از طرح‌های ارائه‌شده در زمینه‌ی تشخیص بدرفتاری در شبکه‌ی بین خودرویی موردبررسی قرارگرفته است. در بخش سوم، بعد از تشریح نظریه‌ی جریان ترافیک، طرح پیشنهادی برای تشخیص بدرفتاری‌های داده محور ارائه شده است. بخش چهارم به نحوه‌ی پیاده‌سازی طرح پیشنهادی، خروجی‌ها و نتایج ارزیابی راه‌حل پیشنهادی می‌پردازد و درنهایت نتیجه‌گیری مقاله ارائه خواهد شد.

۲- کارهای مرتبط

با توجه به اهمیت شناخت و پیشگیری از بدرفتاری وسایل نقلیه‌ی مهاجم در مراحل اولیه‌ی حمله، برای حفظ امنیت شبکه‌های بین خودرویی، در چندین سال اخیر طرح‌های تشخیص بدرفتاری داده محور و گره محور متنوعی ارائه شده است. هدف طرح‌های تشخیص بدرفتاری گره محور ارائه‌شده، تشخیص هویت وسیله نقلیه‌ی بدرفتاری است که بسته‌های دریافتی را بیش از یک حد آستانه مشخص کپی می‌کنند یا دور می‌اندازند. طرح‌های داده محور، مستقل از هویت فرستنده‌ی پیام به بررسی سازگاری و قابل‌قبول بودن اطلاعات پیام‌های ارسال‌شده در شبکه می‌پردازند. در ادامه چندین نمونه از طرح‌های گره محور و داده محور مختلف به همراه روش‌های تشخیص و پارامترهای موردبررسی‌شان آورده شده است. در طرح گره محور DMV[۱۴]، هر وسیله نقلیه توسط وسایل نقلیه‌ی مورد اعتمادتر از خودش مورد نظارت قرار می‌گیرد. اگر ناظر یک رفتار غیرعادی از وسیله نقلیه مشاهده نماید، نمره‌ی بی‌اعتمادی او را یک واحد افزایش داده و اگر نمره‌ی بی‌اعتمادی یک وسیله‌ی نقلیه از یک حد آستانه‌ای عبور کرد، شناسه‌ی آن وسیله نقلیه به‌عنوان یک وسیله نقلیه بدرفتار به مراجع مربوطه‌اش گزارش می‌شود و وسیله نقلیه‌ی مخرب بدرفتار از شبکه اخراج می‌شود. هدف این طرح شناسایی وسایل نقلیه‌ای است که با انجام بدرفتاری‌هایی مانند رها کردن بسته یا تکرار در ارسال بسته منجر به حملاتی مانند حمله‌ی سیاه‌چاله[۱۵] می‌شوند. طبق نتایج ارزیابی، طرح DMV با شناسایی بدرفتاری‌های گره محور قادر است به‌طور مؤثری میزان افت بسته‌ها را کاهش دهد، اما زمان زیادی را صرف پردازش عملکرد گره‌ها می‌کند که باعث تأثیر بر پارامترهایی مانند تأخیر انتهایی و توان عملیاتی می‌شود که در هر نوع ارتباط بی‌سیم بسیار حیاتی هستند [۷]. برای غلبه بر این مسائل روش جدید D&PMV به‌عنوان بهبودی بر طرح DMV برای تشخیص و پیشگیری از بدرفتاری وسایل نقلیه مخرب ارائه شد که این روش در مقایسه با DMV کارآمدتر و ایمن‌تر است و تأثیر حمله‌ی سیاه‌چاله را کاهش می‌دهد [۸].

طرح DMN[۱۶] حالت بهبودیافته‌ی DMV است که تفاوتشان در اختصاص چند گره‌ی ناظر به‌جای انتخاب همه‌ی گره‌ها به‌عنوان ناظر و تأییدکننده است. این مسئله باعث ذخیره‌ی منابع شبکه و صرفه‌جویی در زمان پردازش رفتار گره‌ها و درنهایت منجر به بهبود عملکرد تشخیص می‌شود [۹].

امیرات، یک طرح خوشه‌بندی فازی را برای تشخیص حمله‌ی ارسال انتخابی با تمایز وسایل نقلیه بدرفتار از وسایل نقلیه عادی ارائه کرده است. در طرح او هر وسیله نقلیه با یک درجه عضویت مشخص متعلق به هر دو خوشه‌ی عادی و مخرب است. در این طرح برای بهبود عملکرد تشخیص، یک آستانه تصمیم‌گیری تعریف‌شده است که نشان می‌دهد هر وسیله نقلیه عضو کدام خوشه است [۱۰]. اگرچه ارزیابی تجربی طرح تشخیص بدرفتاری فازی نتایج رضایت بخشی با دقت تشخیص بالا دارد، اما این طرح برای شناسایی بدرفتاری‌ها به آستانه ایستا متکی است که با پویایی شبکه‌های بین خودرویی سازگار نیست. معایب طرح‌های گره محور باعث شده تا اکثر راه‌حل‌های تشخیص بدرفتاری جدید داده محور یا ترکیبی باشند. در ادامه چندین طرح مهم داده محور را بررسی خواهیم نمود.

راج و همکارانش یک طرح تشخیص بدرفتاری داده محور را برای ارزیابی صحت اطلاعات موقعیت گزارش‌شده در پیام‌های ایمنی ارائه کرده‌اند. در این طرح از رابطه‌ی بین موقعیت، مدت‌زمان بین ارسال دو پیام و سرعت نور استفاده می‌شود [۱۱]. اگرچه نویسندگان ادعا می‌کنند این طرح در برابر حملات سیبیل [۱۷] ایمن است اما فرض طراحان این است که یک گره مخرب نمی‌تواند موقعیت دقیق وسیله نقلیه هدف را بداند. بنابراین تشخیص موقعیت اشتباه با این روش آسان است اما این فرض ممکن است معتبر نباشد، زیرا وسایل نقلیه موقعیت خود را به‌صورت دوره‌ای از طریق پیام‌های آگاهی مشارکتی، پخش می‌کنند و مهاجم با دانستن موقعیت گیرنده، پیام اشتباه را طوری دستکاری می‌کند که با این قانون سازگار باشد به همین دلیل این روش با شبیه‌سازی پشتیبانی نمی‌شود. بیسمیر و همکارانش با بررسی وضعیت همپوشانی اطلاعات موقعیت‌های گزارش‌شده در پیام‌های دوره‌ای، یک مدل قابل‌اطمینان برای تشخیص بدرفتاری‌های ناشی از ارسال اطلاعات موقعیت نادرست ارائه کرده‌اند [۱۲]. طبق طرح آن‌ها موقعیت هر وسیله نقلیه با یک مستطیل به طول و عرض وسیله نقلیه مشخص می‌شود، حال اگر موقعیت گزارش‌شده توسط یک وسیله نقلیه با محل قرارگیری وسیله نقلیه دیگر همپوشانی داشته باشد، یک بدرفتاری شناسایی می‌شود. طبق طرح بیسمیر همیشه یک فاصله‌ی مشخص بین وسایل نقلیه مجاور وجود دارد و اگر دو مستطیل که نشان‌دهنده‌ی فضای اشغال‌شده و موقعیت هر وسیله‌ی نقلیه هستند، همدیگر را قطع کنند، می‌توان نتیجه گرفت که یک وسیله نقلیه اطلاعات موقعیت اشتباه را منتشر می‌کند. اگرچه این مدل می‌تواند برای تشخیص وسایل نقلیه شبح و حمله‌ی توهم مفید باشد، اما در این طرح محیط ارتباطی خشن و غیرقابل‌اعتماد در نظر گرفته نشده است و نتایج ارزیابی این طرح نشان‌دهنده‌ی نرخ مثبت غلط بالا و دقت تشخیص پایین است.

هانگ و همکارانش یک طرح تشخیص بدرفتاری که توانایی شناسایی خودروی مخربی که پیام هشدار ترافیک غلط را باانگیزه‌های سودجویانه پخش می‌کند و یا ممکن است هویت و موقعیت خودروها را جعل کند، ارائه داده‌اند. این روش بر پایه‌ی فیزیک ترافیک است و تشخیص با استفاده از امواج حرکتی که یک مدل برای توصیف جریان ترافیک است، انجام می‌شود. این روش یک روش متمرکز نیست بلکه هر خودرو از الگوی تراکم ترافیک محلی خودش برای تشخیص ازدحام و مشخص نمودن وسیله نقلیه‌ی بدرفتار، استفاده می‌کند. ازآنجایی‌که تشخیص به اطلاعات و مشاهدات محلی هر گره، وابسته است درنتیجه این طرح بسیار بهینه عمل می‌کند [۱۳]. زکریا و همکارانش یک طرح تشخیص بدرفتاری باهدف تفکیک ترافیک واقعی از ترافیک مجازی گزارش‌شده توسط وسیله نقلیه‌ی بدرفتار ارائه کرده‌اند. روش این طرح مقایسه‌ی تراکم ترافیک محلی بدست آمده بر اساس تعداد همسایه شناسایی‌شده توسط حسگرهای واحدهای محاسباتی روی وسایل نقلیه و تراکم ترافیک گزارش‌شده در پیام‌های دریافتی است [۱۴]. این طرح تراکم ترافیک محلی را با تلفیق هوشمندانه‌ی اطلاعات دو حسگر مستقل محاسبه می‌کند و با صحت سنجی اطلاعات تراکم ترافیک، بدرفتاری‌هایی که منجر به حملات توهم می‌شوند را شناسایی می‌کند. این روش تشخیص تنها در صورتی کار می‌کند که تشخیص تحت محدوده‌ی ادراک حسگرهای وسایل نقلیه صورت گیرد. همچنین این مطالعه فرض می‌کند که حداقل یکی از دو حسگر مستقل دست‌نخورده باقی می‌ماند و مهاجم به آن دسترسی ندارد که این فرض برای حملات پیچیده‌ای که می‌توانند همه حسگرها را در دست بگیرند و دستکاری کنند، صادق نیست.

یک طرح ترکیبی تشخیص بدرفتاری داده محور و شناسایی حملات سیبیل توسط ژوو و همکارانش ارائه شده است که در این الگوریتم دو نوع ساختار ترافیک متراکم و ترافیک پراکنده تعریف شده است. در این طرح، در ساختار ترافیک متراکم تشخیص حمله سیبیل و در ترافیک پراکنده تشخیص بدرفتاری انجام می‌شود. ایده‌ی اصلی این طرح مقایسه‌ی تراکم ترافیک گزارش‌شده در پیام‌ها با تعداد هشدارهای دریافتی هنگام یک رویداد خاص است [۱۵]. اگرچه این طرح امنیت نسبتاً قوی را در این تنظیمات فراهم می‌کند، اما وابسته به زیرساخت است و هیچ حریم خصوصی برای مقامات مرکزی وجود ندارد.

غالب و همکارانش، یک طرح تشخیص بدرفتاری داده محور و آگاه از زمینه ارائه کرده‌اند، که بر اساس اطلاعات تحرک وسایل نقلیه شامل موقعیت، زمان، سرعت، محدوده‌ی ارتباطات و الگوی ترافیکی به تشخیص رفتار نادرست می‌پردازد. هدف طرح آن‌ها کشف اطلاعات زمینه‌ی کاذب و الگوی ترافیکی کاذب است به‌طوری‌که ضمن کاهش نرخ مثبت غلط، دقت تشخیص را بهبود می‌بخشد [۴]. همچنین آن‌ها در طرحی دیگری تشخیص بدرفتاری آگاه از زمینه‌ی ترکیبی (ترکیب داده محور و گره محور) را پیشنهاد کرده‌اند. در این رویکرد ترکیبی برای ارزیابی صحت اطلاعات، چهار نوع امتیاز سازگاری، امتیاز قابل‌قبول بودن بر اساس محدوده‌ی ارتباطات، امتیاز قابل‌قبول بودن مبتنی بر همپوشانی موقعیت و نمره رفتاری در نظر گرفته شده است. برای تصمیم‌گیری نهایی اگر خروجی یکی از امتیازها مثبت باشد، بدرفتاری تشخیص داده می‌شود [۳]. اگرچه در این مدل آستانه‌های ایستا با مراجع پویا که سازگار با تغییرات توپولوژی شبکه‌ی بین خودرویی هستند جایگزین شده‌اند، این مدل بر اساس این فرض ساخته شد که اکثر وسایل نقلیه صادق هستند، که باعث می‌شوند در برابر حملات بات نت‌ها[۱۸] ضعیف عمل کنند. همچنین این مدل در برابر حملات آگاه از زمینه و پیچیده ارزیابی نشده است. در [۱] یک طرح تشخیص بدرفتاری داده محور و آگاه از زمینه ارائه شده که به کمک نظریه جریان ترافیک به صحت سنجی اطلاعات زمانی گزارش‌شده در پیام‌های دوره‌ای می‌پردازد. در طرح تشخیص بدرفتاری پیشنهادی در این مقاله سعی شده است با ارائه‌ی یک طرح جامع داده محور و آگاه از زمینه اطلاعات گزارش‌شده در پیام‌های دوره‌ای شامل اطلاعات زمانی، مکانی و سرعت در انواع شرایط ترافیکی با دقت بالا صحت سنجی شوند.

۳- تشریح مسئله و ارائه راهکار پیشنهادی

به‌طورکلی ارسال اطلاعات غیرعادی توسط وسایل نقلیه‌ی بدرفتار در شبکه‌ی بین خودرویی می‌تواند نتایج فاجعه باری را به همراه داشته باشد. برای مثال یک دشمن می‌تواند با ارسال گزارش‌های نادرست در مورد ترافیک، سیستم مدیریت و کنترل ترافیک را فریب دهد. ازآنجایی‌که اطلاعات جریان ترافیک گزارش‌شده بر روی رویدادها و رفتارهای وسایل نقلیه‌ی مسیر عبوری تأثیر می‌گذارد، می‌توان از آن به‌عنوان یک شاخص امنیتی برای ارزیابی معقول بودن و سازگاری اطلاعات ترافیک منتشرشده توسط گره‌ها در شبکه‌ی بین خودرویی استفاده کرد تا بدرفتاری‌های ناشی از ارسال اطلاعات غلط ترافیکی را به سرعت تشخیص داد. بنابراین ما یک طرح تشخیص بدرفتاری آگاه از زمینه ارائه می‌دهیم که شامل چهار مرحله‌ی کسب اطلاعات، اشتراک‌گذاری اطلاعات، تجزیه‌وتحلیل اطلاعات و تشخیص است که از خروجی هر مرحله به‌عنوان ورودی مرحله بعدی استفاده می‌شود.

جدول ۱-پارامترهای ماکروسکوپی در نظریه‌ی جریان ترافیک

پارامترهای مایکروسکوپی	تعریف	فرمول	واحد
نرخ جریان (Q)	تعداد وسیله نقلیه‌ای که دریک بازه زمانی از یک نقطه‌ی مشخص از مسیر عبور می‌کنند.	$Q=\frac{n}{t}$	تعداد وسیله نقلیه در ساعت
میانگین سرعت (V)	نسبت مسافت طی شده در طول مسیر به زمانی که یک وسیله نقلیه در مسیر می‌گذراند.	$V=\frac{d}{t}$	کیلومتر بر ساعت
نرخ چگالی (K)	تعداد وسایل نقلیه عبوری که طول مشخصی از مسیر را اشغال کرده‌اند.	$K=\frac{n}{d}$	تعداد وسیله نقلیه در هر کیلومتر

جدول ۲-پارامترهای میکروسکوپی در نظریه‌ی جریان ترافیک

پارامترهای میکروسکوپی	تعریف	رابطه با پارامترهای ماکروسکوپی
سرفاصله‌ی مکانی(s_i)	فاصله بین هر دو وسیله نقلیه متوالی در یک مسیر عبوری	$\overline{K}=\frac{1}{\overline{si}}$
سرعت فردی(v_i)	سرعت یک وسیله نقلیه در یک مسیر عبوری	$\overline{V}=\overline{vi}$
سرفاصله‌ی زمانی(h_i)	فاصله زمانی بین وسایل نقلیه متوالی که از نقطه‌ای مشخص در طول مسیر عبور می‌کنند.	$\overline{Q}=\frac{1}{\overline{hi}}$

در آخرین مرحله، اطلاعات منتشرشده در پیام‌های شبکه‌ی بین خودرویی با استفاده از نظریه‌ی جریان ترافیک و روابط نقض نشدنی بین پارامترهای آن به دو دسته‌ی اطلاعات عادی و غیرعادی طبقه‌بندی می‌شوند. برای این منظور در ابتدا مفاهیم نظریه‌ی جریان ترافیک و سپس مراحل راه‌حل پیشنهادی و شبیه‌سازی در زیر بخش‌های آتی ارائه‌شده است.

۱-۳-مفاهیم اولیه‌ی نظریه‌ی جریان ترافیک

قبل از تشریح مسئله و ارائه‌ی راه‌کار پیشنهادی ابتدا لازم است نظریه‌ی جریان ترافیک را به‌اختصار معرفی کنیم. نظریه جریان ترافیک، فیزیک ترافیک وسایل نقلیه را توصیف می‌کند [۱۶]. در این بخش هدف از توصیف جریان ترافیک، شناخت تغییرات ذاتی و ویژگی‌های جریان ترافیک برای تعریف محدوده‌هایی نرمال برای رفتار رانندگان است. برای توصیف جریان ترافیک باید مجموعه‌ای از پارامترهای کلیدی را تعریف نمود که قابلیت اندازه‌گیری و محاسبه داشته باشند. این پارامترها برای مهندسان ترافیک، نمادی از واقعیت بوده و زبان گویائی هستند که امکان توصیف جریان ترافیک را فراهم می‌آورند.

نظریه‌ی جریان ترافیک وضعیت ترافیک مسیر و تحرک وسایل نقلیه را با استفاده از سه پارامتر ماکروسکوپی[۱۹] (میانگین سرعت، نرخ جریان و نرخ چگالی) که کلیت جریان ترافیک را مورد ارزیابی قرار می‌دهند و سه پارامتر میکروسکوپی[۲۰] (سرعت فردی، سرفاصله‌ی زمانی[۲۱] و سرفاصله‌ی مکانی[۲۲]) که رفتار تک‌تک وسایل نقلیه یا یک جفت وسیله نقلیه را در نظریه‌ی جریان ترافیک بررسی می‌کنند، توصیف می‌کند. پارامترهای ماکروسکوپی در جدول ۱ و پارامترهای میکروسکوپی در جدول ۲ تشریح شده‌اند. در جدول ۱ پارامترهای Q و V ، K به ترتیب نرخ جریان، میانگین سرعت و نرخ چگالی و پارامترهای n و t ، d به ترتیب تعداد وسایل نقلیه، زمان و مسافتی که یک وسیله نقلیه در مسیر می‌گذراند هستند. در جدول ۲ پارامترهای s_i و h_i ، v_i به ترتیب نمایانگر سرفاصله‌ی مکانی، سرفاصله‌ی زمانی و سرعت فردی هستند. در ادامه به‌صورت مختصر به معرفی مفصل پارامترهای نظریه‌ی جریان ترافیک و روش اندازه‌گیری و محاسبه‌ی آن‌ها می‌پردازیم.

۱-۱-۳-پارامترهای ماکروسکوپی نظریه‌ی جریان ترافیک

- نرخ جریان

نرخ جریان در بازه زمانی مشخصی مثلاً یک ساعت برآورد می‌گردد و برحسب وسیله نقلیه بر ساعت بیان می‌شود. جریان شاخصی برای ارزیابی کیفیت ترافیک است که در اهداف و برنامه‌ریزی‌های حمل‌ونقل مورداستفاده قرار می‌گیرد. از مزایای دیگر کنترل جریان می‌توان پیش‌بینی زمان سفر و خدمات‌دهی بهتر در مسیر را بیان نمود.

- میانگین سرعت

یک وسیله نقلیه در یک جریان ترافیک با سرعت‌های متفاوت حرکت می‌کند. بنابراین نمی‌توان یک سرعت منحصربه‌فرد برای جریان ترافیک تعریف نمود بلکه در عمل، یک تابع توزیع سرعت وجود دارد. پارامتر سرعت به‌صورت سرعت متوسط زمانی (TMS)[۲۳] و سرعت متوسط مکانی (SMS)[24] قابل محاسبه است [۱۷].

سرعت متوسط زمانی، میانگین سرعت تمام وسایل نقلیه عبوری از نقطه‌ای از راه یا خط عبوری در یک بازه زمانی مشخص است و سرعت متوسط مکانی میانگین سرعت تمام وسایل نقلیه‌ای است که مقطعی از راه یا خط عبوری را در یک بازه زمانی مشخص اشغال کرده‌اند. سرعت متوسط زمانی، درواقع یک شاخص نقطه‌ای است درحالی‌که سرعت متوسط مکانی توصیف‌کننده‌ی سرعت در بخشی از بزرگراه یا مسیر است. به‌طورکلی سرعت متوسط مکانی با پارامتر میانگین سرعت برابر است.

- نرخ چگالی

چگالی سومین پارامتر ماکروسکوپی جریان ترافیک است که عبارت است از تعداد وسایل نقلیه که طول مشخصی از خط عبوری یا مسیر را اشغال کرده‌اند. به‌منظور اندازه‌گیری چگالی لازم است که مقطع راه را از ارتفاع بالا مشاهده نمود و یا با شمارش خروجی و ورودی ایستگاه‌ها چگالی را محاسبه نمود. همچنین چگالی با استفاده از روابط حاکم بین میانگین سرعت، نرخ جریان و چگالی قابل محاسبه است.

رابطه‌ی بین پارامترهای ماکروسکوپی به‌صورت معادله (۱) است که این رابطه به‌طور قطع نرخ جریان، چگالی و سرعت میانگین را به هم پیوند می‌دهد که دانستن دو مورد از این پارامترها بلافاصله منجر به پارامتر سوم می‌شود، برای مثال با داشتن مقادیر سرعت میانگین و نرخ جریان، نرخ چگالی قابل محاسبه است [۱۸].

$$Q=K\cdot V \qquad (۱)$$

۲-۱-۳-پارامترهای میکروسکوپی نظریه‌ی جریان ترافیک

- سرفاصله مکانی

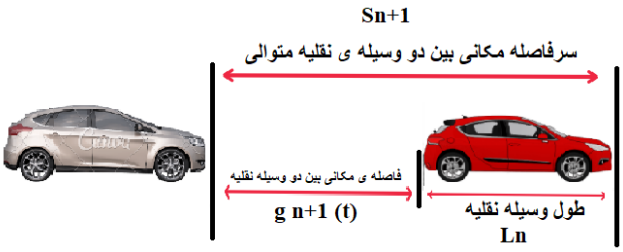
همان‌طور که در شکل ۱ نشان داده شده است، فاصله‌ی بین هر دو وسیله نقلیه‌ی متوالی در یک خط عبوری که از نقاط مشخص و متعارف مثلاً بین سپرهای جلو یا سپرهای عقب دو وسیله نقلیه‌ی متوالی اندازه‌گیری می‌شود، سرفاصله مکانی (s) نام

دارد. همان‌طور که در معادله (۲) نشان داده شده است، نرخ چگالی K در یک خط با معکوس میانگین مقادیر سرفاصله مکانی si در آن خط در ارتباط است [۱۹].

$$\overline{K} = \frac{1}{\overline{si}} \qquad (۲)$$

همچنین مقدار سرفاصله مکانی با استفاده از معادله (۳) قابل‌محاسبه است که Sn+1 سرفاصله‌ی زمانی خودروی n+1 در زمان t است اگر Ln طول خودروی nام و gn+1(t) فاصله‌ی مکانی بین دو وسیله‌ی نقلیه باشد.

$$Sn+1 = Ln + gn+1(t) \qquad (۳)$$



شکل ۱-پارامتر سرفاصله‌ی مکانی

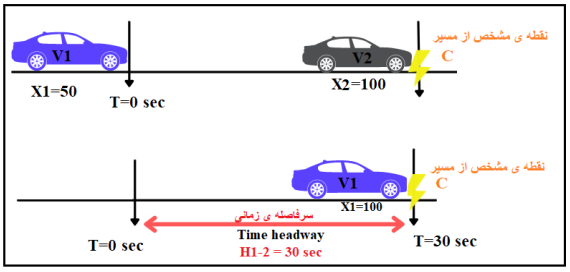
- سرفاصله زمانی

سرفاصله زمانی (h)، زمان بین عبور وسایل نقلیه متوالی از نقطه‌ای مشخص در طول مسیر است. طبق معادله (۴) میانگین مقادیر سرفاصله زمانی در یک خط عبوری با معکوس نرخ جریان در آن خط مرتبط است [۱۹]. به عبارتی سرفاصله‌ی زمانی، زمان سپری‌شده بین ورودی‌های متوالی وسیله نقلیه‌ی i و وسیله نقلیه‌ی i+1 است.

$$\overline{Q} = \frac{1}{\overline{hi}} \qquad (۴)$$

در شکل ۲ در ابتدا وسیله نقلیه‌ی مشکی (V2) که در موقعیت X2 قرار دارد، از نقطه‌ی مشخص C عبور می‌کند، سپس وسیله نقلیه‌ی آبی (V1) از موقعیت X1 حرکت و پس از 30 ثانیه از نقطه مشخص C عبور می‌کند. سرفاصله‌ی زمانی در شکل ۲، فاصله‌ی زمانی بین عبور دو وسیله نقلیه‌ی متوالی مشکی و آبی از نقطه‌ی C نشان داده شده است که طبق معادله (۵) برابر با ۳۰ ثانیه است. T2 و T1 زمان عبور این دو وسیله نقلیه متوالی هستند.

$$h = T_2 - T_1 = 30\text{-}0 = 30 \text{ ثانیه} \qquad (۵)$$



شکل ۲-پارامتر سرفاصله‌ی زمانی

- سرعت فردی

سرعت به‌صورت نسبت فاصله‌ی طی شده (تغییرات فاصله) به زمان سفر (تغییرات زمان) تعریف می‌شود که زمان سفر، مدت‌زمان لازم برای پیمودن یک مسیر با طول مشخص است. همان‌طور که در معادله ۶ نشان داده شده است، سرعت وسیله نقلیه در یک مسیر با زمان طی شدن آن مسیر در ارتباط است. در معادله (۶)، Δx فاصله‌ی طی شده و Δt زمان سفر است.

$$vi = \frac{\Delta x}{\Delta t} \qquad (۶)$$

سرعت میانگین یک مسیر را می‌توان با میانگین‌گیری از سرعت تمام وسایل نقلیه در این مسیر به دست آورد. بنابراین طبق معادله (۷) سرعت میانگین در یک بازه زمانی با میانگین سرعت‌های فردی متناسب است.

$$\overline{V} = \overline{vi} \qquad (۷)$$

۲-۳-طرح مسئله

انتشار اطلاعات غلط باعث تصمیم‌گیری‌های نادرست توسط وسایل نقلیه‌ی همسایه، بی‌نظمی، مشکلات ترافیکی و اختلالات جدی و فاجعه باری می‌شود که می‌تواند جان و مال انسان‌ها را به خطر بیندازد. با توجه به اهمیت صحت اطلاعات منتشرشده توسط پیام‌های دوره‌ای در شبکه‌ی بین خودرویی و وابستگی عملکرد این شبکه به دسترسی به اطلاعات صحیح، هدف ما ارائه‌ی یک طرح جدید تشخیص بدرفتاری داده محور برای شناسایی داده‌های غیرعادیِ منتشرشده در پیام‌های آگاهی مشارکتی، به کمک نظریه‌ی جریان ترافیک است. همان‌طور که در بخش قبل بیان شد، خواص و جامعیت نظریه‌ی جریان ترافیک آن را به یک ابزار قوی برای شناسایی اطلاعات غلط در پیام‌های شبکه‌ی بین خودرویی تبدیل کرده است. در بخش قبل گفتیم نظریه‌ی جریان ترافیک، فیزیک ترافیک وسایل نقلیه و تکامل فضایی- زمانی جریان ترافیک را توصیف می‌کند. بنابراین صحت هرگونه اطلاعات موجود در پیام‌های شبکه‌ی بین خودرویی را می‌توان با نظریه جریان ترافیک اثبات کرد. پس از معرفی این نظریه و تسلط بر روابط بین پارامترهای آن، در ادامه استفاده از نظریه جریان ترافیک برای تشخیص داده‌های غیرعادی در شبکه‌های بین خودرویی، با ارزیابی سازگاری پارامترهای میکروسکوپی با دیدگاه‌های ماکروسکوپی نظریه جریان ترافیک تحت شرایط مختلف ترافیک، پیشنهاد می‌شود.

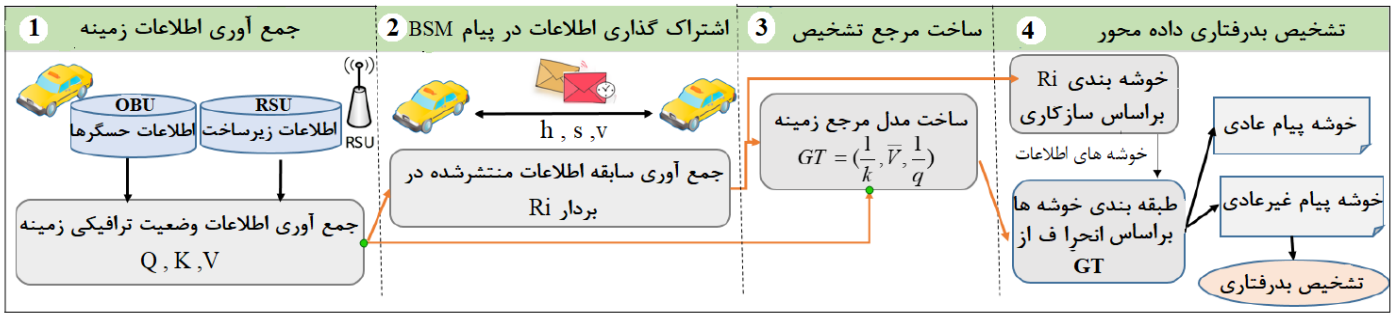
داده‌های غیرعادی در این مقاله به‌عنوان داده‌های منحرف از مقدار واقعی تعریف می‌شوند. برای مثال، اگر یک وسیله نقلیه ادعا کند که مسافت ۱۰۰ کیلومتری را با سرعت ۸۰ کیلومتر بر ساعت در مدت زمان ۱ ساعت پیموده است، درحالی‌که سرعت واقعی آن ۱۰۰ کیلومتر بر ساعت باشد، اطلاعات سرعت گزارش‌شده غیرعادی تلقی می‌شود و بدرفتاری تشخیص داده می‌شود. بنابراین ارسال پیام حاوی اطلاعات ترافیکی غیرعادی توسط وسایل نقلیه‌ی مخرب یا معیوب، طبق تعریف ما بدرفتاری است.

۳-۳- راه‌حل پیشنهادی

ماهیت نظریه‌ی جریان ترافیک باعث شده تا قوانین و روابط این نظریه ابزارهای مهم و کاربردی برای تشخیص بدرفتاری‌های داده محور باشند. در این مقاله پارامترهای کلیدی میکروسکوپی و ماکروسکوپی و روابط بین این پارامترها نقش اصلی در بررسی صحت اطلاعات ارسالی در پیام‌های شبکه‌ی بین خودرویی را ایفاء می‌کنند. طبق این روابط همان‌طور که در جدول ۲ نشان داده شده است، میانگین سرفاصله‌ی مکانی وسایل نقلیه باید متناسب با معکوس نرخ چگالی و میانگین سرعت وسایل نقلیه باید متناسب با سرعت متوسط مشاهده‌شده توسط واحدهای کنار جاده و میانگین سرفاصله‌ی زمانی وسایل نقلیه باید متناسب با معکوس نرخ جریان باشد. ما استدلال می‌کنیم که داده‌های غیرعادی سرفاصله‌ی مکانی و زمانی و سرعت که در پیام‌های دوره‌ای توسط وسایل نقلیه گزارش شده‌اند را با بررسی سازگاری‌شان با اطلاعات تراکم، جریان و میانگین سرعت به‌دست‌آمده از واحدهای کنار جاده یا حسگرهای وسایل نقلیه که منابع قابل‌اطمینان اطلاعات هستند، می‌توان تشخیص داد. در طرح پیشنهادی هر وسیله نقلیه‌ای که ادعای یک سرفاصله‌ی زمانی، سرفاصله‌ی مکانی یا یک سرعت نادرست می‌کند، طبق تعریف غیرعادی محسوب می‌شود. پس از معرفی قوانین و روابط بین پارامترهای نظریه‌ی جریان ترافیک در طرح تشخیص بدرفتاری پیشنهادی، در ادامه مراحل طرح تشخیص بدرفتاری پیشنهادی بیان شده است.

مراحل طرح تشخیص بدرفتاری پیشنهادی

طرح تشخیص بدرفتاری پیشنهادی یک طرح تشخیص بدرفتاری داده محور و آگاه به زمینه است که با کمک قواعد نظریه‌ی جریان ترافیک به تشخیص بدرفتاری‌های شبکه‌ی بین خودرویی می‌پردازد. طرح تشخیص بدرفتاری پیشنهادی، شامل چهار مرحله‌ی طرح‌های آگاه از زمینه است. این مراحل که در شکل ۳ نمایش داده شده‌اند، شامل کسب اطلاعات زمینه، اشتراک اطلاعات، تجزیه‌وتحلیل اطلاعات زمینه و مرحله تشخیص بدرفتاری هستند [۲۰]. در ادامه هریک از این مراحل را به‌طور مفصل بیان خواهیم نمود.



شکل ۳-مراحل طرح تشخیص بدرفتاری آگاه از زمینه‌ی پیشنهادی

۱-۳-۳- مرحله‌ی کسب اطلاعات زمینه

عملکرد اکثر برنامه‌های شبکه‌ی بین خودرویی به در دسترس بودن اطلاعات زمینه‌ی به‌روز و دقیق بستگی دارد. بنابراین در این مرحله برای فراهم نمودن اطلاعات موردنیاز شبکه، اطلاعات زمینه توسط منابع قابل‌اطمینان شبکه مانند واحدهای زیرساخت کنار جاده و واحدهای محاسباتی روی وسایل نقلیه جمع‌آوری می‌شوند. واحدهای کنار جاده که به‌عنوان منابع داده‌ی خارجی عمل می‌کنند که چگالی ترافیک، جریان و سرعت میانگین را در فواصل زمانی نسبتاً کوتاهی اندازه‌گیری می‌کنند. واحدهای کنار جاده‌ای را می‌توان به‌عنوان گره‌های قابل‌اعتماد در نظر گرفت زیرا توسط سازمان‌هایی که مسئول نگهداری شبکه‌های جاده‌ای هستند، نصب و نگهداری می‌شوند. داده‌های ماکروسکوپی جریان ترافیک معمولاً از طریق واحدهای کنار جاده تعیین می‌شوند. با توجه به اینکه پیاده‌سازی سراسری زیرساخت‌ها ازنظر مالی دشوار است و نمی‌توان آن‌ها را به‌طور کامل در یک شبکه توزیع کرد، داده‌های جریان ترافیک از طریق واحدهای کنار جاده در صورت وجود، یا توسط واحدهای محاسباتی روی وسایل نقلیه جمع‌آوری می‌شوند.

هر وسیله نقلیه به‌طور مداوم اطلاعات تحرک خود را از حسگرهای واحدهای محاسباتی خود مانند سیستم موقعیت‌یاب جهانی، سرعت‌سنج، شتاب‌سنج و ژیروسکوپ به دست می‌آورد همچنین وسایل نقلیه وظیفه‌ی اطمینان از سازگاری و یکپارچگی اطلاعات خود را دارند و با استفاده از تکنیک‌های امنیتی و حسگرهای اضافی در تلاش برای تأمین دقت، صحت و یکپارچگی اطلاعات به‌دست‌آمده هستند. اطلاعاتی که توسط واحدهای محاسباتی و حسگرهای روی وسایل نقلیه از زمینه‌ی شبکه‌ی بین خودرویی و همسایگان خود محاسبه و جمع‌آوری می‌شود، می‌تواند شامل، سرعت، چگالی، جریان، موقعیت و شناسه‌ی خودرو و پیام‌های رویداد وسایل نقلیه باشند. بنابراین در این مرحله مجموعه‌ای از ناظران قابل‌اطمینان اطلاعات جریان ترافیک را جمع‌آوری می‌کنند و مقادیر جریان ترافیک کلی را تولید می‌کنند. به‌عنوان‌مثال نرخ جریان Q در معادله (۸)، نرخ چگالی K در معادله (۹) و سرعت متوسط V در معادله (۱۰) برای یک مسیر با طول L در طول پنجره زمان T به‌صورت زیر محاسبه می‌شوند:

$$\bar{K} = \frac{\sum ti}{\frac{ni \in N}{LT}} \quad (۸)$$

$$\bar{V} = \frac{\sum di}{\frac{ni}{\sum ti}} \quad (۹)$$

$$\bar{Q} = \frac{\sum di}{\frac{ni}{LT}} \quad (۱۰)$$

که در آن‌ها ti زمانی است که وسیله نقلیه i در خط می‌گذراند و di مسافتی است که در خط طی می‌کند.

درنهایت می‌توان گفت با تلفیق اطلاعات حسگرهای روی وسایل نقلیه و اطلاعات واحدهای کنار جاده با کمک فن‌آوری‌های محاسباتی و ارتباطی، توانایی محاسبه‌ی اطلاعات ثانویه‌ی زمینه وجود دارد. به عبارتی می‌توان با ترکیب داده‌های میکروسکوپی تأییدشده با اطلاعات واحدهای کنار جاده‌ی آن منطقه، منابع قابل‌اطمینان اطلاعات را افزایش داد.

خروجی این مرحله، اطلاعات قابل‌اطمینان زمینه‌ی وضعیت ترافیک شامل نرخ چگالی، نرخ جریان و سرعت متوسط است که توسط زیرساخت‌های کنار جاده و واحدهای محاسباتی روی وسایل نقلیه از زمینه‌ی شبکه‌ی بین خودرویی جمع‌آوری می‌شوند. این خروجی به‌عنوان ورودی مراحل بعدی این طرح تشخیص بدرفتاری استفاده می‌شود.

۲-۳-۳-مرحله‌ی اشتراک‌گذاری اطلاعات زمینه

ازآنجایی‌که در شبکه‌ی بین خودرویی هر وسیله نقلیه باید اطلاعاتِ کسب‌شده‌ی خود را به‌صورت دوره‌ای تحت عنوان پیام‌های آگاهی مشارکتی بین وسایل نقلیه‌ی همسایه به اشتراک بگذارد، در این مرحله، اطلاعات زمینه‌ی اخیر تمام وسایل نقلیه همسایه برای هر وسیله نقلیه در دسترس قرار می‌گیرد. بااینکه، نرخ بالای پخش پیام‌های حاوی اطلاعات زمینه یک نیاز اساسی برای ردیابی مداوم وضعیت تحرک وسایل نقلیه همسایه و اطمینان از به‌روز بودن برنامه‌ها است اما نرخ بالای پخش پیام، کانال ارتباطی را متراکم و غیرقابل‌اعتماد می‌کند. به عبارتی باعث اتلاف اطلاعات در شبکه می‌شوند که بر عملکرد شبکه و برنامه‌ها تأثیر منفی می‌گذارند. درنتیجه یک طرح پخش باید بتواند ضمن حفظ کیفیت اطلاعات به اشتراک گذاشته‌شده، میزان پخش را به حداقل برساند [۲۱].

تا این مرحله از طرح پیشنهادی اطلاعات زمینه‌ی هر وسیله نقلیه توسط قابلیت‌های محاسباتی و ارتباطیِ وسایل نقلیه جمع‌آوری و در میان همسایگان به اشتراک گذاشته شده است. حال فرض کنید N مجموعه‌ای از گره‌های وسیله نقلیه در یک مسیر مشخص در طول پنجره‌ی زمان T=(t1,t2) باشد که هر وسیله نقلیه ni، اطلاعات تحرک خود را مانند سرفاصله‌ی مکانی، سرفاصله‌ی زمانی و سرعت، در قالب پیام‌های دوره‌ای به همسایگانش ارسال می‌کند. گره‌ها می‌توانند پیام‌هایی شامل اطلاعات غیرعادی ارسال کنند. بنابراین اطلاعات منتشرشده در این مرحله

باید صحت سنجی شوند تا بتوانیم بدرفتاری‌های ناشی از ارسال اطلاعات غیرعادی را به‌موقع تشخیص دهیم و مانع از پیشرفت حملات مهاجمان داخلی شویم.

طبق این طرح پیشنهادی ، هر گره در طول پنجره‌ی زمانی T سابقه‌ی اطلاعات گزارش‌شده توسط همسایگان را به‌صورت بردار R_i حفظ می‌کند که این بردار می‌تواند سابقه‌ای از اطلاعات هر یک از پارامترهای میکروسکوپی مانند سرفاصله زمانی و مکانی و سرعت را ضبط و جمع‌آوری کند، برای مثال معادله (۱۱) سابقه‌ای از اطلاعات سرفاصله‌ی زمانی جمع‌آوری شده است.

$$R_i(t)=\begin{bmatrix}\frac{\sum_t^{t+T} h_1(t)}{T}\\ \frac{\sum_t^{t+T} h_2(t)}{T}\\ \vdots\\ \frac{\sum_t^{t+T} h_{i-1}(t)}{T}\\ \frac{\sum_t^{t+T} h_{i+1}(t)}{T}\\ \vdots\\ \frac{\sum_t^{t+T} h_N(t)}{T}\end{bmatrix} \quad (11)$$

پس‌ازاینکه با کمک بردارRi سابقه‌ی اطلاعات به اشتراک گذاشته‌شده در شبکه را جمع‌آوری کردیم حال زمان صحت سنجی اطلاعات به اشتراک گذاشته‌شده فرارسیده است. برای تشخیص بدرفتاری‌های ناشی از ارسال اطلاعات غلط در شبکه‌ی بین خودرویی ما نیاز به یک معیار تشخیص داریم تا با مقایسه‌ی اطلاعات هر پیام دریافتی با آن معیار، اطلاعات را صحت سنجی کنیم و بدرفتاری‌ها را تشخیص بدهیم. معیار تشخیص در طرح پیشنهادی یک مرجع تشخیص مبتنی بر زمینه است که طبق این مرجع، تشخیص بدرفتاری با آگاهی از زمینه و منطبق با تغییرات زمینه انجام می‌شود. چگونگی ساخت این مرجع و تجزیه‌وتحلیل اطلاعات زمینه در مرحله‌ی بعد تشریح خواهد شد.

۳-۳-۳-مرحله‌ی تجزیه‌وتحلیل زمینه و ساخت مرجع تشخیص

تا این مرحله از طرح پیشنهادی اطلاعات دو منبع مستقل شامل اطلاعات زمینه‌ی قابل‌اطمینان و سابقه‌ی اطلاعات منتشرشده در شبکه، جمع‌آوری شده است. در مرحله سوم، معیارهای تشخیص بدرفتاری برای ارزیابی صحت اطلاعات منتشرشده در پیام‌های دوره‌ای به کمک اطلاعات زمینه‌ی قابل‌اطمینان استخراج می‌شوند و مدل مرجع زمینه با کمک قواعد نظریه‌ی جریان ترافیک ساخته می‌شود. به عبارتی در این مرحله، زمینه بازنمایی و ویژگی‌های تشخیصی طرح پیشنهادی استخراج می‌شوند. در طرح پیشنهادی ما از ویژگی‌های وضعیت ترافیکی زمینه برای ارائه‌ی یک طرح تشخیص بدرفتاری جدید استفاده می‌شود که اطلاعات وضعیت ترافیک زمینه شامل پارامترهای نرخ چگالی، نرخ جریان و میانگین سرعت است [۲۲]. اطلاعات وضعیت ترافیک زمینه درواقع همان پارامترهای مایکروسکوپی نظریه‌ی جریان هستند. در طرح پیشنهادی از روابط ثابت‌شده‌ی بین پارامترهای ماکروسکوپی زمینه و پارامترهای میکروسکوپی نظریه‌ی جریان ترافیک برای تخمین مقادیر مورد انتظار گزارش‌شده در پیام‌های دوره‌ای به شرح زیر استفاده می‌شود:

تخمین مقادیر مورد انتظار سرفاصله‌ی زمانیِ گزارش‌شده در پیام‌های دوره‌ای با کمک اطلاعات قابل‌اطمینان نرخ جریان، طبق معادله (۱۲) که می‌گوید مقدار جریان با مقدار متوسط سرفاصله‌ی زمانی رابطه‌ی عکس دارد.

$$\overline{hi}=\frac{1}{\overline{Q}} \quad (12)$$

تخمین مقادیر مورد انتظار سرفاصله‌ی مکانیِ گزارش‌شده در پیام‌های دوره‌ای با کمک اطلاعات قابل‌اطمینان نرخ چگالی، طبق معادله (۱۳) که می‌گوید مقدار چگالی با مقدار متوسط سرفاصله‌ی مکانی رابطه‌ی عکس دارد.

$$\overline{si}=\frac{1}{\overline{K}} \quad (13)$$

تخمین مقادیر مورد انتظار سرعت گزارش‌شده در پیام‌های دوره‌ای با کمک اطلاعات قابل‌اطمینان سرعت میانگین، طبق معادله (۱۴) که می‌گوید میانگین سرعت‌های فردی با مقدار متوسط سرعت رابطه‌ی مستقیم دارد.

$$\overline{vi}=\overline{V} \quad (14)$$

-ساخت مرجع زمینه

در طرح تشخیص بدرفتاری پیشنهادی برای ساخت مدل مرجع زمینه از این واقعیت استفاده می‌شود که اطلاعات منتشرشده در پیام‌ها توسط فیزیک جریان ترافیک، تحت شرایط حالت پایدار[۲۵]محدود شده‌اند. شرایط حالت پایدار فرضیات مفیدی هستند که در نظریه جریان ترافیک برای تجزیه‌وتحلیل و درک پدیده‌های ترافیک در دنیای واقعی به کار می‌روند [۱۶]. تحت شرایط حالت پایدار، میانگین فاصله‌ی مکانی بین وسایل نقلیه باید برابر با معکوس نرخ چگالی (k)، میانگین فاصله‌ی زمانی بین وسایل نقلیه باید برابر با معکوس نرخ جریان (Q) و میانگین سرعت وسایل نقلیه باید برابر با سرعت میانگین مشاهده‌شده توسط واحدهای کنار جاده باشد. هدف از این مرحله ایجاد یک مدل مرجع زمینه‌ی پویا برای ارزیابی سازگاری و معقول بودن اطلاعات جمع‌آوری‌شده از مرحله قبل است. در این مرحله ما برای ساخت مدل مرجع زمینه، اطلاعات به‌دست‌آمده از منابع قابل‌اطمینان شبکه را با نظریه جریان ترافیک ترکیب می‌کنیم.

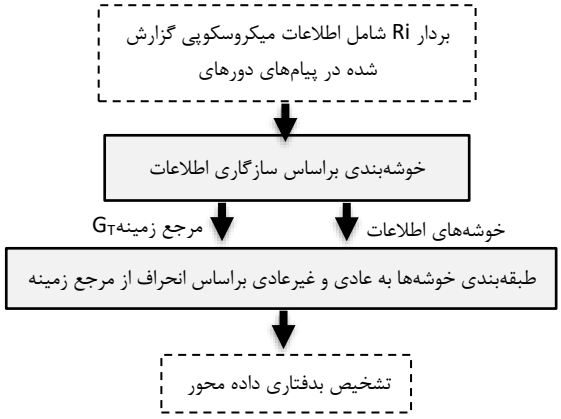
در طرح پیشنهادی، ساخت مرجع زمینه و طبقه‌بندی داده‌ها بر اساس پارامترها و قوانین فیزیک است که توسط نظریه جریان ترافیک تعیین می‌شوند. بنابراین در این مرحله ما یک مرجع زمینهGT در نظر می‌گیریم که با معادله (۱۵) بیان می‌شود. این مرجع زمینه به کمک ویژگی‌های وضعیت ترافیکی زمینه شامل اطلاعات قابل‌اطمینان جریان، تراکم و سرعت که توسط واحدهای کنار جاده جمع‌آوری می‌شود، ساخته می‌شود. هنگامی‌که اطلاعات واحدهای کنار جاده در دسترس نیستند، یک وسیله نقلیه می‌تواند مرجع زمینه‌ی محلی را با استفاده از داده‌های جمع‌آوری‌شده توسط واحدهای محاسباتی روی وسایل نقلیه ایجاد کند. در مرحله‌ی آخر از طرح پیشنهادی از این مرجع زمینه برای اعتبار سنجی اطلاعات پیام‌های دوره‌ای شبکه‌ی بین خودرویی و تشخیص بدرفتاری‌های داده محور استفاده می‌شود. مرجع زمینه در طول پنجره زمانی T به‌صورت معادله (۱۵) تعریف می‌شود:

$$GT=(\frac{1}{\overline{k}},\overline{V},\frac{1}{\overline{Q}}) \quad (15)$$

که V میانگین سرعت‌های فردی تخمین‌زده‌شده با کمک میانگین سرعت بدست‌آمده از منابع قابل‌اطمینان است و$\frac{1}{K}$ متوسط سرفاصله‌ی مکانی تخمین‌زده‌شده با استفاده از نرخ چگالی k است و $\frac{1}{Q}$ متوسط سرفاصله‌ی زمانی تخمین زده‌شده با استفاده از نرخ جریان Q را به ما می‌دهد. اطلاعات سرفاصله‌ی زمانی و مکانی و سرعت اعلام‌شده در پیام‌های دوره‌ای دریافتی باید طبق این مرجع، سازگار و قابل‌قبول باشند. قابل‌قبول بودن این اطلاعات به کمک روابط موجود در نظریه‌ی جریان ترافیک به این صورت تعریف می‌شود که اطلاعات گزارش‌شده در پیام‌های دوره‌ای از مقادیر مورد انتظار مرجع زمینه منحرف نباشند. برای مثال متوسط مقدار سرفاصله‌ی زمانی گزارش‌شده در پیام‌های دوره‌ای باید با معکوس جریان دریافتی از منابع قابل‌اعتماد اطلاعات متناسب باشد. در غیر این صورت مقدار سرفاصله‌ی زمانی غیرعادی شناخته می‌شود. در انتهای این مرحله یک مرجع زمینه خواهیم داشت که اطلاعاتی که از انتظارات و تخمین‌های این مرجع زمینه انحراف داشته باشند، غیرعادی شناخته می‌شوند.

۴-۳-۳-مرحله‌ی تشخیص بدرفتاری

در مرحله‌ی تشخیص بدرفتاری برای افزایش دقت و سرعت تشخیص به‌جای مقایسه‌ی تک‌تک اطلاعات پیام‌های دریافتی با مرجع زمینه از تکنیک خوشه‌بندی K-Means برای طبقه‌بندی اطلاعات استفاده می‌کنیم. در الگوریتم مبتنی بر تکرار K-Means سعی می‌شود داده‌های درون یک خوشه شبیه به یکدیگر و خوشه‌ها متفاوت (دور) از هم تعریف شوند [۲۳]. همان‌طور که در شکل ۴ نشان داده شده است، در این طرح با کمک الگوریتم خوشه‌بندی K-Means که سازگار با شرایط و ویژگی‌های شبکه‌ی بین خودرویی است، تمام اطلاعات به‌دست‌آمده از مرحله‌ی دوم تشخیص به دو خوشه‌ی اطلاعات عادی و غیرعادی دسته‌بندی می‌شوند. این خوشه‌بندی بر اساس سازگاری اطلاعات انجام می‌شود و اطلاعاتی که با یکدیگر سازگارند در یک خوشه قرار می‌گیرند؛ سپس با مقایسه‌ی مرکز خوشه‌ها با مرجع زمینه و بر اساس این قانون که اطلاعات منحرف از مرجع زمینه اطلاعات غیرعادی هستند، خوشه‌های اطلاعات به عادی و غیرعادی طبقه‌بندی می‌شوند. در ادامه به تشریح کامل این مرحله پرداخته شده است.



شکل ۴- ارزیابی سازگاری و قابل‌قبول بودن اطلاعات در تشخیص بدرفتاری

برای تشریح عملکرد طرح پیشنهادی فرض کنید سابقه‌ی اطلاعات سرفاصله‌ی زمانی به‌صورت $\{h_1,h_2,...,h_n\}$ را باید با استفاده از الگوریتم خوشه‌بندی تک متغیره k-means به k خوشه تقسیم کنیم که در آن K=2 است. برای به حداقل رساندن معیار مجموع مربعات در معادله (۱۶) داریم:

$$\min imize \sum_{k=1}^{k} \sum_{j \in C_k} \| \bar{h}_j - m_k \|^2 \qquad (۱۶)$$

که m_k مرکز هندسی خوشه‌ی C_k است. درنهایت مجموعه‌ی اطلاعات بردار Ri به دو خوشه با مرکز m_1 و m_2 با مجموعه‌های متناظر گره‌های ارسال‌کننده‌ی N_1 و N_2 تقسیم می‌شوند. پیش‌بینی می‌شود اطلاعات ارسال‌شده توسط یک گره‌ی n_r غیرعادی است اگر آن اطلاعات در خوشه‌ای باشد که مرکز آن بیشترین فاصله را با مرجع زمینه‌ی GT دارد. این اصل برای اطلاعات سرفاصله زمانی غیرعادی به‌صورت معادله (۱۷) نشان داده می‌شود. فاصله‌ی بین مرجع و مرکز خوشه به‌صورت m_i-GT محاسبه می‌شود و $\tilde{A}$ مجموعه گره‌های بدرفتار پیش‌بینی‌شده است.

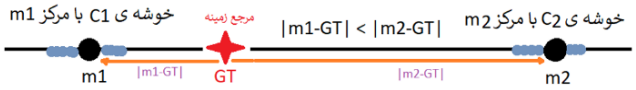
$$n_r \in \begin{cases} \tilde{A}, if ((|m_1 - 1/\bar{Q}| > |m_2 - 1/\bar{Q}|) \wedge n_r \in N_1) \vee \\ \quad ((|m_1 - 1/\bar{Q}| < |m_2 - 1/\bar{Q}|) \wedge n_r \in N_2);\ 1/\bar{Q} \in p \\ \bar{\tilde{A}}, \quad otherwise \end{cases} \qquad (۱۷)$$

با استفاده از همین روش، یک وسیله نقلیه بدرفتار که در حال انتشار سرعت غیرعادی یا در حال انتشار اطلاعات سرفاصله مکانی غیرعادی است را می‌توان به ترتیب با کمک معادله (۱۸) و معادله (۱۹) شناسایی کرد.

$$n_r \in \begin{cases} \tilde{A}, if ((|m_1 - \bar{V}| > |m_2 - \bar{V}|) \wedge n_r \in N_1) \vee \\ \quad ((|m_1 - \bar{V}| < |m_2 - \bar{V}|) \wedge n_r \in N_2);\ \bar{V} \in p \\ \bar{\tilde{A}}, \quad otherwise \end{cases} \qquad (۱۸)$$

$$n_r \in \begin{cases} \tilde{A}, if ((|m_1 - 1/\bar{K}| > |m_2 - 1/\bar{K}|) \wedge n_r \in N_1) \vee \\ \quad ((|m_1 - 1/\bar{K}| < |m_2 - 1/\bar{K}|) \wedge n_r \in N_2);\ 1/\bar{K} \in p \\ \bar{\tilde{A}}, \quad otherwise \end{cases} \qquad (۱۹)$$

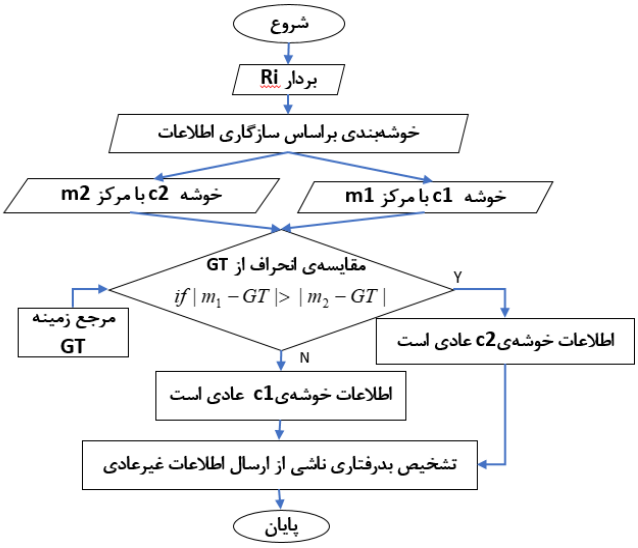
در این مرحله، مقادیر پارامترهای میکروسکوپی (سرفاصله‌ی زمانی، مکانی و سرعت متوسط) گزارش‌شده در پیام‌ها خوشه‌بندی می‌شوند و خوشه اطلاعاتی که نزدیک‌ترین مرکز را به مرجع زمینه دارد به‌عنوان خوشه اطلاعات عادی تشخیص داده می‌شود و گره‌های متناظر ارسال‌کننده‌ی این اطلاعات نیز به‌عنوان گره‌های صادق برچسب‌گذاری می‌شوند. به‌طورکلی در این طرح ما برای طبقه‌بندی داده‌ها، از میزان فاصله‌ی مرکز هر خوشه تا مرجع زمینه استفاده می‌کنیم. مرجع زمینه با اطلاعات گزارش‌شده در پیام‌های دوره‌ای تعیین نمی‌شود بلکه با داده‌های قابل‌اطمینان گزارش‌شده توسط زیرساخت‌ها و داده‌های به‌دست‌آمده از طریق حسگرهای وسیله نقلیه‌ی، تعیین می‌شود.



شکل ۵-الگوی تشخیص در طرح پیشنهادی

روش تشخیص پیشنهادی بر اکثریت صادق تکیه نمی‌کند و معیار طبقه‌بندی خوشه‌ها میزان انحراف از مرجع زمینه است و اطلاعات خوشه‌ای که بیشترین انحراف را از مرجع زمینه دارد، غیرعادی شناسایی می‌شوند. برای مثال، همان‌طور که در شکل ۵ نشان داده شده است، نقاط m_1 و m_2 مراکز خوشه‌های C1 و C2 هستند و GT مرجع زمینه است. با توجه به اینکه فاصله‌ی بین GT و m_1 کم‌تر از فاصله بین GT و m_2 است، خوشه‌ی اطلاعات با مرکز m_1 به‌عنوان خوشه‌ی عادی و خوشه‌ی اطلاعات با مرکز m_2 به‌عنوان خوشه‌ی غیرعادی طبقه‌بندی می‌شوند.

این روش پیشنهادی به تجزیه‌وتحلیل انحرافات بین اطلاعات پیام‌های دوره‌ای و مرجع زمینه برای شناسایی بدرفتاری‌های ناشی از ارسال اطلاعات غیرعادی می‌پردازد. هرچه انحراف بزرگ‌تر باشد، احتمال اینکه منبع پیام ارسال‌شده، گره‌ی بدرفتار باشد بیشتر است. بنابراین در مرحله‌ی چهارم برای تشخیص بدرفتاری‌ها صحت پیام‌های دریافت شده با استفاده از این مدل پیشنهادی ارزیابی می‌شوند. شکل ۶ فلوچارت مراحل طرح پیشنهادی را برای صحت سنجی اطلاعات غیرعادی مانند سرفاصله‌ی زمانی را نشان می‌دهد. به‌طورکلی با کمک مرجع زمینه‌ی جامع GT می‌توان انواع بدرفتاری‌های ناشی از دستکاری اطلاعات سرفاصله زمانی، مکانی و سرعت را تشخیص داد. طرح تشخیص بدرفتاری پیشنهادی، در شرایط ترافیک متراکم که دقت تشخیص با کمک پارامتر سرعت پایین است (سرعت دچار افزایش و کاهش‌های متوالی می‌شود) می‌تواند از صحت‌سنجی پارامتر سرفاصله مکانی استفاده کند و برای تشخیص در شرایط ترافیکی ادغام یا انشعاب مسیر که دقت تشخیص بر اساس پارامتر سرفاصله مکانی پایین است از تشخیص بدرفتاری مبتنی بر صحت سنجی اطلاعات سرفاصله زمانی و سرعت استفاده کند. به همین دلیل طرح پیشنهادی یک طرح جامع است که می‌تواند در اکثر شرایط ترافیکی بدرفتاری‌های ناشی از ارسال اطلاعات غلط را با دقت مطلوبی تشخیص دهد.



شکل ۶- فلوچارت طرح پیشنهادی برای تشخیص اطلاعات غیرعادی

۴- ارزیابی

به‌منظور اثبات عملکرد و کارایی طرح پیشنهادی در شبکه‌ی بین خودرویی، آن را به کمک نرم‌افزار SUMO و NS2 شبیه‌سازی کردیم. به کمک SUMO ترافیک وسایل نقلیه ایجادشده و با NS2 شبکه‌ی بین خودرویی برای انتقال اطلاعات و ایجاد ارتباطات بین وسایل نقلیه شبیه‌سازی شده است [۲۵-۲۴]. از الگوریتم خوشه‌بندی k-means تک متغیره در پیاده‌سازی طرح تشخیص بدرفتاری برای طبقه‌بندی اطلاعات به عادی و غیرعادی به کمک زبان برنامه‌نویسی پایتون در محیط ژوپیتر استفاده شده است. جدول ۳ پارامترها و تنظیمات شبیه‌سازی را نشان می‌دهد. مقادیر سرعت، چگالی و جریان برای ساخت مرجع زمینه به‌طور متوسط در دوره‌های ۱۰ ثانیه‌ای محاسبه شده‌اند.

برای ارزیابی عملکرد طرح تشخیص بدرفتاری پیشنهادی، شبیه‌سازی با ٪۲۰، ٪۴۰، ٪۶۰ و ٪۸۰ اطلاعات غیرعادی انجام شد. معیارهای ارزیابی ما دقت، یادآوری[۲۶]، امتیاز F[۲۷]، صحت[۲۸] و نرخ مثبت غلط هستند [۲۶].

معیار صحت، بیان‌کننده تعداد تشخیص‌های صحیح انجام‌شده توسط طرح تشخیص بدرفتاری، تقسیم‌بر تعداد کل تشخیص‌های انجام شده است. بااین‌حال، بررسی این معیار به‌تنهایی، برای ارزیابی عملکرد یک طرح تشخیص کافی نیست. به همین دلیل در ادامه پارامترهای دیگر ارزیابی را بیان خواهیم نمود تا در کنار این پارامتر از همه‌ی جوانب به ارزیابی طرح تشخیص بدرفتاری پیشنهادشده بپردازیم. معیار تشخیص کاذب تعداد پیام‌های عادی است که طرح تشخیص به‌اشتباه آن‌ها را به‌عنوان غیرعادی شناسایی می‌کند.

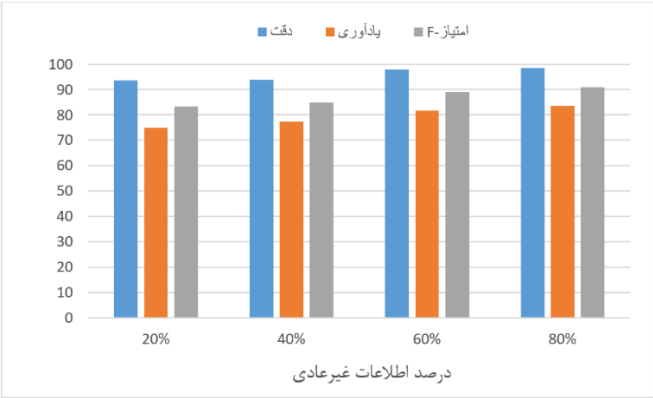
معیار دقت نسبت تعداد پیام‌های غیرعادی که به‌درستی طبقه‌بندی شده‌اند به تعداد کل پیام‌هایی است که به‌عنوان غیرعادی طبقه‌بندی‌شده‌اند. در هنگام ارزیابی عملکرد یک طرح تشخیص بدرفتاری، بهتر است که از معیار دقت در کنار معیار یادآوری استفاده شود که معیار یادآوری، بیان‌کننده‌ی نسبت تعداد پیام‌های غیرعادی درست طبقه‌بندی‌شده در یک طرح تشخیص بدرفتاری، به تعداد کل پیام‌ها غیرعادی موجود است که باید به‌عنوان بدرفتار طبقه‌بندی شوند. معیار امتیاز F میانگین متوازن دو معیار دقت و یادآوری نیز گفته می‌شود. این معیار، نسبت به معیار صحت، تصویر دقیق‌تری از نحوه عملکرد طرح تشخیص بدرفتاری نشان می‌دهد زیرا مقادیر منفی واقعی را در نظر نمی‌گیرد [۲۷].

همان‌طور که در شکل ۷ نشان داده شده است، معیارهای دقت و یادآوری برای ارزیابی یک طرح تشخیص باید در کنار یکدیگر بررسی شوند. همچنین برای ارائه دید متعادل‌تری از دقت و یادآوری، معیار امتیاز F به‌عنوان یک معیار ارزیابی مناسب در نظر گرفته می‌شود، زیرا منفی واقعی را در نظر نمی‌گیرد. نتایج ارزیابی در شکل ۷ نشان می‌دهد که طرح پیشنهادی دقت و یادآوری بالایی در تشخیص بدرفتاری‌های داده محور دارد.

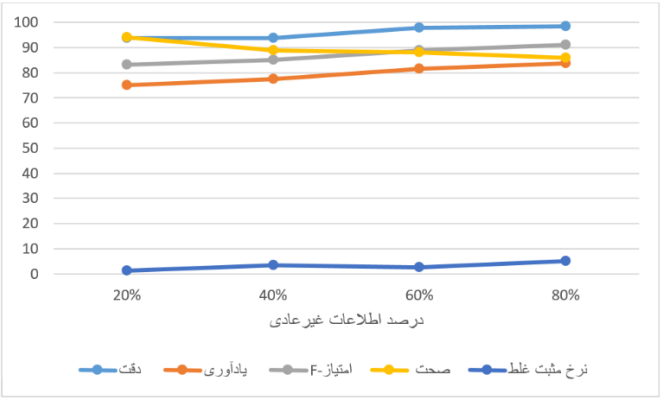
جدول ۳-جدول پارامترها و تنظیمات شبیه‌سازی

پارامترهای شبیه‌سازی	مقدار
شبیه‌ساز شبکه	NS2.35
مولد تحرک و پویایی	SUMO
اندازه‌ی بسته	۲۵۶ بایت
زمان شبیه‌سازی	۶۰ دقیقه
محدوده‌ی شبیه‌سازی	۷۰۰*۱۰۰۰ متر
حداکثر سرعت وسایل نقلیه	۱۲۰ کیلومتر بر ساعت
mac/phy	۸۰۲.۱۱p
پروتکل مسیریابی	AODV
تعداد وسایل نقلیه	۰-۲۰۰۰
توپولوژی	بزرگراه
محدوده‌ی انتقال	۳۰۰ متر
طول وسایل نقلیه	۵ متر
درصد داده‌های غیرعادی	٪۲۰، ٪۴۰، ٪۶۰ و٪۸۰

شکل ۸ نتایج جامع ارزیابی عملکرد طرح تشخیص بدرفتاری پیشنهادی را نشان می‌دهد که نرخ مثبت غلط در طرح پیشنهادی به‌طور مطلوبی کم و صحت، دقت و یادآوری تشخیص بدرفتاری‌ها بالا است. درنهایت می‌توان گفت که عملکرد طرح ما در تشخیص بدرفتاری‌های داده محور قابل‌قبول بوده و پیش‌بینی‌های قابل‌اعتمادی از تشخیص داده‌های غیرعادی ارائه می‌دهد.



شکل ۷- نتایج ارزیابی طرح پیشنهادی بر اساس معیار دقت و یادآوری و امتیاز F



شکل ۸- نتایج ارزیابی جامع طرح پیشنهادی

۵- نتیجه‌گیری

طرح‌های تشخیص بدرفتاری داده محور در مقایسه با طرح‌های گره محور، به دلیل تشخیص مهاجمان در مراحل اولیه‌ی حمله، مزایای زیادی دارند. اکثر مطالعات گذشته بر روی سیستم‌های مبتنی بر اعتماد و رویکردهای یادگیری ماشین متمرکزشده‌اند و ویژگی‌های خاص زمینه‌ی شبکه‌ی بین خودرویی را نادیده گرفته‌اند. در این مقاله، استفاده از نظریه‌ی جریان ترافیک برای تشخیص بدرفتاری در شبکه‌ی بین خودرویی پیشنهاد و ارزیابی شد. این واقعیت که اطلاعات منابع قابل‌اطمینان مانند زیرساخت‌ها و اطلاعات موجود در پیام‌های دوره‌ای دو منبع جداگانه از داده‌ها هستند، اما قوانین فیزیک ترافیک آن‌ها را ملزم به سازگاری می‌کند، روشی است که برای ارزیابی صحت داده‌ها در این طرح مورداستفاده قرار می‌گیرد. طبق نتایج ارزیابی، طرح پیشنهادی قادر است انواع مهاجمان را که اطلاعات زمینه را دستکاری می‌کنند در اکثر شرایط ترافیکی با دقت بالایی شناسایی کند. همچنین استفاده از تکنیک خوشه‌بندی باعث کوتاه شدن فرایند تشخیص می‌شود. درنهایت با توجه به نتایج ارزیابی روش پیشنهادی به‌راحتی می‌توان به نتایج طرح تشخیص بدرفتاری پیشنهادی اعتماد نمود و با گره‌های بدرفتار ارسال‌کننده‌ی اطلاعات غلط در شبکه‌ی بین خودرویی برخورد کرد.

۶- مراجع

[۱] ز. گرجی، س. شکرالهی، "ارائه‌ی یک طرح تشخیص بدرفتاری داده محور و آگاه به زمینه با استفاده از نظریه‌ی جریان ترافیک در شبکه‌ی موردی بین خودرویی"، در *مجموعه مقالات بیست و هفتمین کنفرانس بین‌المللی کامپیوتر انجمن کامپیوتر ایران*، ص ۲۳۲-۲۲۶، ۱۴۰۰.

[2] N. Lyamin, A. Vinel, M. Jonsson and B. Bellalta, "Cooperative awareness in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp.17-28, 2017.

[3] A. Ghaleb, M. A. Maarof, A. Zainal, B. A. S, Al-Rimy, F. Saeed and T. Al-Hadhrami, "Hybrid and multifaceted context-aware misbehavior detection model for vehicular ad hoc network, " *IEEE Access*, vol. *7*, pp.159119-159140, 2019.

[4] F.A. Ghaleb, M.A. Maarof, A. Zainal, M.A. Rassam, S .Faisal, and M. Alsaedi, "Context-aware data-centric misbehaviour detection scheme for vehicular ad hoc networks using sequential analysis of the temporal and spatial correlation of the consistency between the cooperative awareness messages," *Vehicular Communications*, vol. 20 , p.100186, 2019.

[5] D. Manivannan, S.S. Moni, S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)," *Vehicular Communications* 25, p.100247,2020.

[6] R. van der Heijden, S. Dietzel and F. Kargl,"Misbehavior detection in vehicular ad-hoc networks," *1st GI/ITG KuVS Fachgespräch Inter-Vehicle Communication, University of Innsbruck*, pp.23-25, 2013.

[7] A. Daeinabi and A.G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks," *Multimedia tools and applications*, vol. 6*6*, no. 2, pp.325-338, 2013.

[8] M. Kadam and S. Limkar, "Performance investigation of DMV (detecting malicious vehicle) and D&PMV (detection and prevention of misbehave/malicious vehicles): Future road map," *In Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA),* pp.379-387, 2014.

[9] U. Khan, S. Agrawal and S. Silakari, "Detection of malicious nodes (DMN) in vehicular ad-hoc networks." *Procedia computer science 46*, pp.965-972, 2015.

[10] H. Amirat, N. Lagraa, C.A. Kerrach, and Y. Ouinten, "Fuzzy clustering for misbehaviour detection in vanet," In *2018 International Conference on Smart Communications in Network Technologies (SaCoNeT)*, pp. 200-204, 2018.

[11] S. Ruj, M.A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," In *2011 IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1-5, 2011.

[12] N. Bißmeyer, C. Stresing, and M. Bayarou, "Intrusion detection in vanets through verification of vehicle movement data," In *IEEE Vehicular Networking Conference*, pp. 166-173, 2010.

[13] D. Huang, S.A. Williams and S. Shere, "Cheater detection in vehicular networks," In *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 193-200, 2012.

[14] J. Zacharias and S. Fröschle, "Misbehavior detection system in VANETs using local traffic density." *In 2018 IEEE Vehicular Networking Conference (VNC),* pp. 1-4, 2018.

[15] T. Zhou, R.R. Choudhury, P. Ning, and K. Chakrabarty. "P2DAP—Sybil attacks detection in vehicular ad hoc networks." *IEEE journal on selected areas in communications 29*, pp.582-594, 2011.

[16] M. Ranaweera, A. Seneviratne, D. Rey, M. Saberi and V. Dixit. "Anomalous data detection in vehicular networks using traffic flow theory," In *IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pp. 1-5, 2019.

[17] A. D. May, *Traffic flow fundamentals*, 1990.

[18] L. H. Immers and S. L. ogghe, "Traffic flow theory," *Faculty of Engineering, Department of Civil Engineering, Section Traffic and Infrastructure, Kasteelpark Arenberg*, vol. 40, no. 21 ,2002.

[19] S. Hoogendoorn and V. Knoop, "Traffic flow theory and modelling," *The transport system and transport policy: an introduction*, pp.125-159, 2013.

[20] H. Vahdat-Nejad, A. Ramazani, T. Mohammadi, and W. Mansoor, "A survey on context-aware vehicular network applications," *Vehicular Communications*, vol. 3, pp.43-57 ,2016.

[21] J. Breu, A. Brakemeier and M. Menth. "Analysis of cooperative awareness message rates in vanets." *In 2013 13th International Conference on ITS Telecommunications (ITST),* pp. 8-13, 2013.

[22] F.A. Ghaleb, A. Zainal, M.A. Maroof, M.A. Rassam, and , F. Saeed, "Detecting Bogus Information Attack in Vehicular Ad Hoc Network: A Context-Aware Approach," *Procedia Computer Science*, vol. 163, pp. 180-189, 2019.

[23] H. Wang and M. Song, "Ckmeans. 1d. dp: optimal k-means clustering in one dimension by dynamic programming," *The R journal*, vol. 3, no. 2, p.29, 2011.

[24] M. Behrisch, , L. Bieker, , J. Erdmann, M. Knocke, , D. Krajzewicz, and P. Wagner, "Evolution of SUMO's simulation model". *Transportation Research Board Circular*, pp.1-21,2014.

[25] K. Raja Kumar, N. Karyemsetty and B. Samatha "Performance Analysis of Vehicular Network Scenarios Using SUMO and NS2 Simulators". *In Data Engineering and Communication Technology.* pp. 337-344, Springer 2021.

[26] G. Kumar, "Evaluation metrics for intrusion detection systems-a study". *Evaluation*. no. 11, pp.11-7, 2014.

[27] Y. M. Chen and Y. C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *Journal of Communications and Networks*, vol. 15, no. 2, pp. 153-163, 2013.

زهرا گرجی دانشجوی دکتری مهندسی برق گرایش مخابرات سیستم در دانشگاه تهران است که مدرک کارشناسی ارشد خود را در رشته مهندسی برق گرایش مخابرات امن و رمزنگاری از دانشگاه شهید بهشتی تهران در سال ۱۴۰۰ کسب کرده است. ازجمله زمینه‌های پژوهشی موردعلاقه ایشان می‌توان به امنیت و کنترل دسترسی، تشخیص بدرفتاری و شبکه‌های بین خودرویی اشاره کرد. آدرس پست الکترونیکی ایشان عبارت است از:
zah.gorji@mail.sbu.ac.ir

سعید شکرالهی تحصیلات خود را در مقطع کارشناسی کامپیوتر - نرم افزار در سال ۱۳۸۱ از دانشگاه اصفهان و در مقاطع کارشناسی ارشد و دکتری کامپیوتر - نرم‌افزار به ترتیب در سال‌های ۱۳۸۴ و ۱۳۹۳ از دانشگاه شهید بهشتی به پایان رسانده است. ایشان دوره فرصت مطالعاتی خود را در سال ۱۳۹۱در آزمایشگاه امنیت دانشگاه میلان سپری کرده است. وی در حال حاضر استادیار گروه امنیت شبکه و رمزنگاری پژوهشکده فضای مجازی در دانشگاه بهشتی است. زمینه‌های تحقیقاتی موردعلاقه ایشان عبارت‌اند از: سیستم‌های فوق مقیاس وسیع، معماری نرم‌افزار، معماری سرویس گرا، معماری سازمانی، امنیت و کنترل دسترسی، اینترنت اشیاء، میان‌افزارهای مبتنی بر رویداد و شبکه‌های بین خودرویی. آدرس پست الکترونیکی ایشان عبارت است از:
s_shokrollahi@sbu.ac.ir

---

[1] Vehicular Ad hoc Networks (VANETs)
[2] Mobile Ad hoc Networks (MANETs)
[3] Cooperative Awareness Message (CAM)
[4] Misbehavior Detection Scheme
[5] Precision
[6] False Positive Rate
[7] Consistency
[8] Plausibility
[9] Context-Aware
[10] Traffic Flow Theory
[11] Road Side Unit (RSU)
[12] On-Board Unit (OBU)
[13] Anomalous Data
[14] Detection of Malicious Vehicles
[15] Blackhole Attack
[16] Detection of Malicious Nodes
[17] Sybil Attack
[18] Botnets
[19] Macroscopic
[20] Microscopic
[21] Time Headway
[22] Space Headway
[23] Time Mean Speed
[24] Space Mean Speed
[25] Steady State
[26] Recall
[27] F-measure
[28] Accuracy

The CSI Journal on Computing Science and Information Technology

The CSI Journal on
Computing Science and
Information Technology
Vol. 20, No.1, 2022

A context-aware data-centric misbehaviour detection scheme for VANETs

Zahra Gorji[1], Saeed Shokrollahi[2]

[1, 2] Cyberspace Research Institute, Shahid Beheshti University (SBU), Tehran, Iran

Abstract

Vehicular ad hoc networks (VANETs) are promising technologies whose performance depends on the availability of accurate and up-to-date vehicle information. Vehicles that share anomalous data can easily degrade the performance of vehicular ad hoc networks. As a result, detecting such misbehavior is critical for ensuring a vehicular network's security against attackers. The use of traffic flow theory features has received little attention in most previous misbehavior detection schemes. The accuracy of cooperative awareness messages (CAMs) shared in VANETs can be assessed using this theory. To overcome the limitations of previous misbehavior detection schemes, we propose a data-centric misbehaviour detection system that detects anomalous data VANETs using traffic flow theory rules. In the proposed scheme, we consider on-board units as reliable sources of information alongside roadside units that together help to decrease the costs associated with the nationwide implementation of roadside units.The results of a simulation evaluation of this misbehavior detection scheme in various traffic conditions and with various percentages of anomalous information sent by malicious nodes show that false positive rates are reduced and detection accuracy is improved.

Keywords: Data-Centric Misbehaviour Detection, Context-Awareness, Vehicular Ad Hoc Networks, Traffic Flow Theory, Anomalous Data, VANET Security