یک معماری سلسله مراتبی نوین مبتنی بر الگوریتم های یادگیری بدون نظارت جهت ارتقاء توان عملیاتی و امنیتی شبکه های ادهاک خودرویی

حمید هادی

[۱] دانشجوی ارشد، گروه کامپیوتر، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران،

***کامبیز مجیدزاده**

[۲] استادیار، گروه کامپیوتر، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران،

چکیده

شبکه های ادهاک خودرویی (VANET) یک فناوری نوظهور با آینده امیدوار کننده است. VANET ها از نظر ویژگی ها، چالش ها، معماری سیستم و کاربرد کاملاً با شبکه های ادهاک موبایل (MANET) متفاوت هستند. اینترنت وسایل نقلیه (IoV) ، فناوری که به سرعت در حال رشد است و برای ارتباطات کارامد بین وسایل نقلیه استفاده می شود و توجهات را از شبکه های سنتی ادهاک وسایل نقلیه (VANET) به سمت خود جلب کرده است. مدیریت متمرکز IoV مستلزم منحصر به فرد بودن و مناسب بودن آن برای برنامه های ایمنی سیستم حمل و نقل هوشمند (ITS) است. شبکه‌های نرم‌افزاری (SDN) یکی دیگر از الگوهای شبکه نوظهور فناوری است که توانایی مدیریت کارآمد شبکه‌های کلی و تبدیل معماری‌های پیچیده شبکه به معماری‌های ساده و قابل مدیریت را دارد. طوفان داده پراکنی، به دلیل ماهیت داده پراکنی NDN، یک موضوع مهم در NDN مبتنی بر IoV است. سرعت بالا و تغییر سریع توپولوژی وسایل نقلیه در IoV باعث ایجاد مشکل قطع لینک و تاخیر غیر ضروری در انتقال داده می شود. یکی دیگر از چالش های امنیتی مهم VANET پیش بینی و پیشگیری از مهاجمان است. برای حل مشکلات ذکر شده معماری پیشنهادی در این مقاله شامل ارائه یک زیرساخت امنیتی نوین مبتنی بر الگوریتم های یادگیری بدون نظارت جهت شناسایی و مقابله با حملات مخرب در شبکه های ادهاک خودرویی می باشد. طرح پیشنهادی دو معماری شبکه های نرم افزار محور (SDN) و نقشه خودسازماندهی (SOM) را برای سیستم VANET مبتنی بر 5G ترکیب می کند. سیستم پیشنهادی ترکیبی جدید از SDN و یک راه حل شبکه مبتنی بر نقشه خود سازماندهی (SOM) برای افزایش امنیت در دو بعد، شناسایی و جلوگیری از حملات خواهد بود. این مقاله آسیب پذیری عملکرد شبکه را با در نظر گرفتن حملات انکار سرویس توزیع شده (DDoS) تجزیه و تحلیل می کند. سپس امنیت سیستم پیشنهادی با DDoS موجود مورد تجزیه و تحلیل و بررسی قرار گرفته است. نتایج پیاده سازی و شبیه‌سازی های معماری پیشنهادی در این مقاله نشان از افزایش دقت تشخیص حملات، افزایش توان عملیاتی شبکه، کاهش میانگین تاخیر انتقال داده و کاهش میانگین بسته های گم شده در شبکه های ادهاک خودرویی در مقایسه با سایر روشهای امنیتی موجود می باشد.

واژه گان کلیدی: شبکه های نرم افزار محو، شبکه های ادهاک، نرخ انتقال، تاخیر انتشار، حملات مخرب

۱. مقدمه

با افزایش تعداد وسایل نقلیه در جاده ها و پیشرفت در فناوری ارتباطات بی سیم، VANET ها به یک زمینه تحقیقاتی امیدوارکننده تبدیل شده اند. (VANET) که از وسایل نقلیه به عنوان گره های متحرک استفاده می کنند، زیرگروهی از MANET ها هستند و تعامل بین وسایل نقلیه در مجاورت نزدیک و بین وسایل نقلیه و تجهیزات کنار جاده را ارائه می دهند. با این حال، ویژگی های VANET ها آنها را از سایر شبکه ها متمایز می کند. ماشین بدون راننده به یک نوآوری فناوری اخیر در بخش حمل و نقل تبدیل شده است. پیش‌بینی می‌شود که آنها انقلابی در سفر ایجاد کنند و آن را بسیار راحتتر، کارآمدتر و ایمن‌تر کنند. مشکلات فنی متعددی در امنیت خودروهای بدون راننده و تأثیرات فاجعه باری که این مشکلات امنیتی می تواند بر مردم داشته باشد وجود دارد. فقدان سطح بالایی از امنیت فعلی در خودروهای بدون راننده یکی از بزرگترین عوامل بازدارنده استفاده گسترده از آنها است. VANET بر ترافیک جاده نظارت می کند و داده های هر وسیله نقلیه را با خودروهایی که در نزدیکی آن هستند به اشتراک می گذارد استخدام می کند. (Hartenstein et al, 2008).

VANET از گره های ثابت و متحرک استفاده می کند. این شبکه با به اشتراک گذاری داده های محرمانه در مورد تصادفات و ترافیک به نیازهای ایمنی راننده پاسخ می دهد.در شبکه، برخی از وسایل نقلیه ممکن است داده ها را به اشتراک نگذارند، درخواست های جعلی ارسال نکنند و تلاشی برای نقض امنیت شبکه نکنند. به ویژه، ارتباط با گره‌ها در VANET، هنگامی که در امتداد جاده حرکت می‌کنند، توسط توپولوژی جاده محدود می‌شود. بنابراین، تنها در صورتی که امکان به دست آوردن اطلاعات جاده وجود داشته باشد، می‌تواند موقعیت آینده یک وسیله نقلیه را نشان دهد. به راحتی قابل پیش بینی باشد (Schoch et al, 2008). VANET با ارائه خدمات شبکه به مسافران و رانندگان، نقش حیاتی در ایمنی خودرو ایفا می کند (Amadeo et al, 2016). در همین حال، معرفی شبکه های تلفن همراه 5G ارتباطات موجود بین وسایل نقلیه، عملکرد وسایل نقلیه، تجربه سواری برای کاربر و غیره را بهبود می بخشد. در رشد شبکه های VANET و 5G، VANET ها پایگاه ITS را تشکیل می دهند. که با هدف دستیابی به اتصال آنلاین برجسته بین وسایل نقلیه جاده ای است (Cisco, 2018). با رشد نسل جدید ارتباطات بی‌سیم و تکنیک‌های وسایل نقلیه هوشمند، وسایل نقلیه مجهز به رابط‌های بی‌سیم می‌توانند خدمات سیستم حمل‌ونقل هوشمند مانند ناوبری، نظارت بر ترافیک، سیار CC وسایل نقلیه و خدمات اطلاعات نزدیک را ارائه دهند. ظرفیت بیشتر و کاهش تاخیر ارتباطات ارائه شده توسط شبکه های تلفن همراه 5G برای ایمنی وسایل نقلیه در محیط های بسیار متحرک ضروری است و برای رفع نیازهای کاربردی ITS ضروری است. به دلیل کمبود منابع طیف، ممکن است برای شبکه های 5G آینده امکان مدیریت اطلاعات در حال تحول داخل خودرو وجود نداشته باشد. با توجه به تکامل مداوم فن آوری VANET، انتظار می رود VANET طیف وسیعی از خدمات مانند نظارت، کنترل خودرو، ایمنی، مدیریت ترافیک، تبلیغات مبتنی بر اینترنت اشیا و غیره را ارائه دهد (Jacobson et al, 2009). ویژگی های برجسته VANET ها، هماهنگی آنها را به چالش می کشد. انتظار می رود VANET ها به طور موثر خدماتی با نیازهای کیفیت متفاوت ارائه دهند. از این رو، معماری‌های شبکه قابل برنامه‌ریزی در حال تبدیل شدن به توانمندسازهای اصلی VANET برای کمک به عملیات متقابل بین شبکه‌های ناهمگن اساسی، سازماندهی وظایف تخصیص منابع، و مدیریت مؤثر تعداد زیادی از گره‌های سیار با دستگاه‌های هوشمند ناهمگام هستند (Gerla et al, 2014). را هدف اصلی شبکه‌های ادهاک وسایل نقلیه فراهم کردن راحتی و ایمنی برای رانندگان در محیط‌های اطراف خودرو است.

VANETها به عنوان زیرساختی برای یک سیستم حمل و نقل هوشمند برای کنترل چندین وسیله نقلیه خودران و پاسخگویی به نیازهای اتصال از طریق اینترنت در یک شهر هوشمند در نظر گرفته می شوند. VANET ها به دلیل گستره وسیعی از خدمات و کاربردها مانند سرگرمی اطلاعاتی، بهبود اثربخشی ترافیک و ایمنی مسافر به طور کامل مورد تجزیه و تحلیل قرار گرفته اند (Jaballah et al, 2014). با توسعه رشد غیرمنتظره و فناوری در تعداد خودروهای هوشمند، VANET های معمولی به دلیل مقیاس پذیری، هوش ناکافی، اتصال ضعیف و انعطاف پذیری کمتر، با مشکلات فنی مختلفی در بهره برداری و مدیریت مواجه می شوند. شبکه‌های تعریف‌شده نرم‌افزاری، بستر مناسب جدیدی را برای آزمایش و پیاده‌سازی مفاهیم جدید فراهم می‌کنند و با استفاده از قابلیت برنامه‌ریزی شبکه و این واقعیت که شبکه‌های مجازی ایزوله را می‌توان با صفحه کنترل ارجاع داد، به طراحی خلاقانه شبکه انگیزه می‌دهد. به دلیل توانایی آن برای به دست آوردن وضعیت فعلی شبکه، امکان کنترل متمرکز بلادرنگ را فراهم می کند. تکنیک SDN (شبکه‌سازی مبتنی بر نرم‌افزار) که مدیریت شبکه را از انتقال داده جدا می‌کند، یک روش ضروری برای ساختار یک شبکه خواهد بود (TalebiFard et al, 2015). یک VANET نرم‌افزاری با شبکه‌های 5G یک معماری ضروری شبکه برای VANETهای نسل بعدی خواهد

بود. شبکه‌های تعریف‌شده توسط نرم‌افزار، سطح داده و صفحه کنترل را از هم جدا می‌کنند و برنامه‌ریزی و انعطاف‌پذیری استقرار منابع و مدیریت شبکه را درک می‌کنند. به طور گسترده ای به عنوان یک تکنیک اصلی در شبکه های 5G برای تحقق مجازی سازی منابع شبکه و سفارشی سازی برنامه ها بر اساس درخواست کاربران پذیرفته شده است. یک نقشه خودسازماندهی برای ترتیب دادن VANET ها استفاده می شود که برای سیستم های خودکار بدون راننده و سیستم های پشتیبانی رانندگی خودرو در حوزه حمل و نقل هوشمند به کار گرفته شده اند. بر اساس داده‌های منطقه رانندگی و موقعیت مکانی پیام دوره‌ای هر وسیله نقلیه، وسایل نقلیه با توجه به تفاوت جهت و مقصد رانندگی در VANET مرتب شدند. وسایل نقلیه مرتب شده عمدتاً با وسایل نقلیه در همان VANET تعامل دارند و پیام های یک شبکه مشابه را مدیریت می کنند. پیش‌بینی جهت حرکت بعدی که توسط راننده وسیله نقلیه در هر تقاطع شبکه جاده‌ای انتخاب می‌شود، می‌تواند تا حد زیادی در برنامه‌های شبکه ادهاک وسایل نقلیه مورد استفاده قرار گیرد (شکست ۲۰۲۰). چندین برنامه کاربردی VANET ها در سرویس سیستم موقعیت یابی جهانی با موانعی مانند درختان، ساختمان های مرتفع و تونل ها مواجه است. سیستم موقعیت یابی جهانی برای یافتن جهت حرکت آینده وسایل نقلیه استفاده می شود. الگوهای حرکت وسیله نقلیه از طریق خوشه بندی مسیر حرکت وسیله نقلیه با استفاده از یک نقشه خودسازماندهی بازیابی می شوند. از این الگوها برای یافتن جهت حرکت بعدی استفاده می شود که توسط راننده در تقاطع بعدی انتخاب می شود. شبکه‌های نرم‌افزاری تعریف‌شده در سیستم 5G VANET ایجاد می‌شوند تا امکان اشتراک‌گذاری اطلاعات و هماهنگی بین ایستگاه‌های پایه را فراهم کند تا از خوشه‌بندی کارآمد و سازگار اطمینان حاصل شود (Ashraf et al, 2016). شبکه‌های نرم‌افزاری تعریف‌شده در VANET ایجاد شده است تا ارتباطات را در سراسر شبکه مدیریت کند کل ارتباط با کمک پروتکل های مسیریابی در خودرو کنترل می شود. با این حال، به دلیل افزایش تقاضا برای سیستم VANET، پروتکل های مسیریابی برای مدیریت امنیت، حریم خصوصی و ارتباطات سیستم بسیار مهم شده است. این مشکل را می توان به راحتی با کمک یک سیستم شبکه تعریف شده با نرم افزار (SDN) حل کرد. نقشه خود سازماندهی با ویژگی های آماری ترافیک شبکه برای تشخیص آموزش داده شده است (Vestin et al, 2013). پس از اولین داده‌های آموزش‌دیده، با ویژگی‌های ترافیک ورودی جدید به طور مکرر شناسایی می‌شود و ترافیک را بر اساس خودش دسته‌بندی می‌کند. به دلیل سازگاری و انعطاف پذیری آن در برابر تغییرات محیطی، از آن برای تشخیص استفاده شده است. ادغام یک SDN در VANETها رفتار شبکه کلی وسایل نقلیه را ساده کرده است. این مقاله یک رویکرد ترکیبی با ترکیب SDN و SOM برای افزایش امنیت در شبکه‌های ادهاک خودرو طراحی کرد. اهداف روش پیشنهادی در این مقاله بشرح زیر است:

- ارائه یک معماری نوین ترکیبی مبتنی بر SDN و SOM در شبکه‌های ادهاک خودرویی.
- احراز هویت و مجوزهای جدید همراه با سیستم ترکیبی SDN و SOM، که در آن هر دو کنترل کنار جاده و خودرو باید نمایه شوند و در پایگاه داده ایستگاه اصلی شبکه های 5G گنجانده شوند، استفاده می شود. بنابراین، فقط وسایل نقلیه احراز هویت شده می توانند از طریق شبکه های موجود ارتباط برقرار کنند.
- شناسایی و پیشگیری از حملات DDoS، با بررسی تمام بسته‌های جمع‌آوری‌شده در آدرس IP خاص با شناسایی و ردیابی تعداد بسته/ثانیه آن برای مقایسه آن با یک آستانه، علاوه بر این، حفظ پایگاه داده ای از اتصال داده های IP-اینترنت برای تشخیص هویت جعلی و پروتکل های اینترنتی است.
- در نهایت، شبیه‌سازی نشان می‌دهد که سیستم پیشنهادی می‌تواند امنیت را بهبود بخشد، که می‌تواند مستقیماً تأخیر انتها به انتها، از دست دادن بسته‌ها و افزایش توان عملیاتی را تحت تأثیر قرار دهد و کاهش دهد.

۲. پیشینه تحقیق

VANET ها یک تکنیک در حال توسعه از شبکه است که پیش بینی می شود سازگار و مقرون به صرفه باشد، و آن را برای ارائه خدمات اتصال شبکه به مسافران و رانندگان در جاده های امروزی ایده آل می کند.

در (Eichler, 2007) در نسل بعدی VANET ها، با شبکه های 5G، تکنیک SDN نقش اساسی در مدیریت شبکه ایفا خواهد کرد. با این حال، برای کاربردهای سرگرمی های اطلاعاتی، تأخیر بیشتر در ارتباطات VANET ها مانع بزرگی برای مدیریت شبکه می شود. استفاده از ارتباطات مستقیم از طریق شبکه‌های تلفن همراه، جایگزینی امکان‌پذیر نیست زیرا هزینه بیشتری را به همراه خواهد داشت.

در این مطالعه، یک استراتژی بهینه‌سازی برای متعادل کردن نیاز تأخیر و هزینه استفاده از شبکه‌های تلفن همراه ارائه شده است که خودروها تشویق می‌شوند تا از آن برای ارسال درخواست‌های کنترلی برای خدمات شبکه تعریف‌شده توسط نرم‌افزار با کاهش هزینه پهنای باند شبکه تلفن همراه استفاده کنند. علاوه بر این، ارتباط بین کنترلر و وسایل نقلیه به عنوان یک بازی دو مرحله ای Stackelberg مدل سازی شده و تعادل بازی مورد بررسی قرار می گیرد. از نتایج آزمایش، استراتژی بهینه Rebating تأخیر کمتری نسبت به سایر مدل‌های صفحه کنترل ارائه می‌دهد.

در (Bai et al, 2010) طبق این مطالعه، تقاضا برای سفرهای ایمن و ایمن در بزرگراه ها و جاده ها در دهه جاری قوت گرفته است به طور مشابه، پارادایم شهر هوشمند و مفهوم تحرک هوشمند برای ارتقای کیفیت زندگی شهروندان توسعه یافته است. VANET ها به طور گسترده ای به عنوان ابزاری در تحقق چنین مفاهیمی با فعال کردن خدمات اطلاعات سرگرمی و ایمنی جذاب شناخته می شوند. چنین شبکه‌هایی با مجموعه‌ای از موانع وجود دارند که از مشکلات در مدیریت تحرک بالای گره برای محافظت از حریم خصوصی کاربران و داده‌ها متغیر است. پارادایم SDN به عنوان یک راه حل کاربردی برای مدیریت محیط های شبکه پویا که با افزایش تعداد دستگاه های متصل و ناهمگونی برنامه ها مشخص می شود، شناخته شده است. در حالی که بررسی های اولیه خاصی برای تأیید کاربردهای الگوی SDN برای VANET ها انجام شده است، اما مزایای احتمالی SDN، مانند مدیریت تحرک و منابع، ثابت نشده است. مشخص نیست که SDN چه تأثیری بر حریم خصوصی و امنیت خواهد داشت. امنیت یک مشکل مرتبط در VANET است زیرا تهدیدها می توانند بر رفتار راننده و کیفیت زندگی راننده تأثیر بگذارند. این مطالعه تهدیدات امنیتی را مورد بحث قرار می‌دهد که VANETهای مبتنی بر شبکه تعریف‌شده نرم‌افزار آینده با آن‌ها مواجه خواهند شد و بررسی می‌کند که چگونه شبکه‌های تعریف‌شده توسط نرم‌افزار می‌توانند در ارائه اقدامات متقابل برای تهدیدات امنیتی آینده مفید باشند.

در (Ahlgren et al, 2012) مطالعه ای بر روی SDN VANET ها در معماری 5G برای سرویس های امنیتی انعطاف پذیر بیان می کند که VANET ها به عنوان یک تکنیک اصلی برای ارائه تعداد زیادی خدمات، از جمله ایمنی مسافر، مدیریت ترافیک، و راحتی مسافر و راحتی سفر VANETها به عنوان بخشی از فناوری 5G آینده همراه با SDN به عنوان فعال کننده اصلی 5G پیشنهاد می شوند. تکنیک محاسبات مه در 5G راه حل مناسبی برای پردازش سریع در کاربرد VANET های حساس به تاخیر است که ترکیبی از شبکه های کاملاً توزیع شده و کاملاً متمرکز هستند. یک ادغام سه طرفه بین SDN، VANET و 5G در این مطالعه برای طراحی امنیتی انعطاف پذیر VANET پیشنهاد شده است. این طراحی تعادل بهتری بین تحرک، شبکه، امنیت و عملکرد ایجاد می‌کند. این مطالعه نشان می‌دهد که چگونه چنین روشی می‌تواند VANETها را از انواع مختلف حملات، یعنی DDoS با هدف قرار دادن کنترل‌کننده‌ها یا وسایل نقلیه در شبکه، ایمن کند، و چگونه می‌توان حمله را به منبع آن ردیابی کرد.

بهینه‌سازی عملیات مدیریت ترافیک با مشکل افزایش شدید تعداد وسایل نقلیه در جاده‌ها، تصادفات جاده‌ای و ازدحام ترافیک مواجه است. ازدحام ترافیک می تواند بر کیفیت زندگی و ایمنی مسافران، فعالیت های روزانه، محیط زیست و اقتصاد شرکت ها و شهروندان تأثیر منفی بگذارد. در مرحله کنونی توسعه، دستگاه‌های هوشمند مجهز به پردازنده‌هایی با قدرت محاسباتی بالا و قابلیت ارتباط بی‌سیم در پارادایم‌های محاسباتی و ارتباطی ادغام شده‌اند. اینترنت اشیا امکان رشد اینترنت وسایل نقلیه را از VANET های موجود فراهم می کند. اکنون، استفاده از روش‌های محاسباتی ابری و مه برای استفاده در برنامه‌های مختلف 5G برای شبکه‌های خودرویی در نظر گرفته شده است. SDN به عنوان یک فناوری انعطاف پذیر برای اتصال مراکز محاسبات ابری و شبکه های دسترسی بی سیم در شبکه های خودرویی 5G در نظر گرفته می شود. کاستی هایی مانند عدم هوشمندی، انعطاف ناپذیری و دامنه کوتاه اتصال در VANET ها را می توان با ترکیب آنها با فناوری های نوظهور برطرف کرد. این مطالعه بررسی جامعی از فن‌آوری‌های کنونی و اثرات آن‌ها بر رشد سیستم‌های گردشگری هوشمند برای کنترل و مدیریت ازدحام ترافیک ارائه می‌کند.

در (Saini et al, 2015) ICN (شبکه اطلاعات محور) را به عنوان پارادایم آنلاین قابل استقرار مطلوب در آینده بررسی نمودند. انتظار می رود که ICN جایگزین مدل فعلی مبتنی بر پروتکل اینترنت (IP) شود، زیرا نویدبخش بهبود مقیاس پذیری، توزیع محتوا و امنیت است. با این حال، این یک کار چالش برانگیز است که تصور کنیم چگونه می توان ICN را به پارادایم در حال توسعه دیگر، یعنی VANET مرتبط کرد. مروری بر روش VANET مبتنی بر ICN همراه با تحقیق در آن و سهم آن در غلبه بر موانع ارائه شده است. علاوه بر این، مشکلات اتصال مدل های ICN خودرو با برخی از پارادایم های در حال توسعه دیگر، یعنی ابر، SDN، و محاسبات لبه

ارائه شده است. علاوه بر این، فرصت‌های تحقیقاتی خاصی در VANET مبتنی بر ICN از نظر تحرک، امنیت، نام‌گذاری، مسیریابی، ارتباطات 5G و حافظه پنهان نیز در این مطالعه مورد بحث قرار گرفته‌اند.

در (Kreutz et al, 2015) انتظار می‌رود که 5G انقلابی در شبکه‌های نسل بعدی ایجاد کند، که پیش‌بینی می‌شود نیازهای ارتباطی مختلف آینده ITS را برآورده کند.با انگیزه برآوردن نیازهای مشتریان از برنامه های کاربردی جدید در ITS، مانند سرعت بیشتر، فراگیر بودن شبکه و پهنای باند، مطالعات در حال حاضر در حال بررسی فناوری ها و معماری های مختلف شبکه برای استفاده احتمالی در نسل بعدی ITS هستند. برای ارائه مدیریت انعطاف‌پذیر شبکه‌ها، استفاده بیشتر از منابع و کنترل در VANET در مقیاس بزرگ، یک معماری نسل بعدی 5G سلسله‌مراتبی و جامع جدید پیشنهاد شده است. هدف اصلی این معماری کل نگر ترکیب انعطاف‌پذیری و تمرکز شبکه دسترسی رادیویی ابری (CRAN) و SDN با تکنیک‌های ارتباطی 5G برای تخصیص کارآمد منابع با دیدی جهانی است. علاوه بر این، یک ساختار محاسباتی مه برای جلوگیری از تحویل مکرر بین RSU و وسایل نقلیه پیشنهاد شده است. توان عملیاتی، کنترل سربار و تأخیر انتقال در کنترلر مورد بررسی قرار گرفته و با سایر معماری ها مقایسه می شود. نتایج شبیه‌سازی نشان‌دهنده کاهش سربار کنترل و کاهش تاخیر انتقال در کنترل‌کننده‌ها است.

در (Jaballah et al, 2016) تقاضای فعلی برای ایمنی مسافران، کارایی ترافیک حمل و نقل و سرگرمی بر نیاز سیستم ارتباطی بهتر وسایل نقلیه تاکید می کند. به همین دلیل است که شبکه های تلفن همراه 5G مهم هستند. آنها ظرفیت بیشتر و تاخیر کمتری را در ارتباطات خودرو در محیط های بسیار متحرک ارائه می دهند. علاوه بر این، تکنیک ارتباطی اختصاصی برد کوتاه مبتنی بر IEEE 802.11p برای VANET پیشنهاد شده است. ترکیب VANET های مبتنی بر خوشه با شبکه های تلفن همراه 5G برای صرفه جویی در منابع طیف کمیاب، جلوگیری از ازدحام شبکه و کاهش از دست دادن بسته ها مفید است. با این حال، برای ایجاد یک الگوریتم کارآمد برای خوشه بندی که پایدار و سازگار با VANET های پویا باشد. برای در نظر گرفتن مزایای SDN، این مطالعه یک الگوریتم خوشه‌بندی آگاه اجتماعی با قابلیت SDN را در سیستم‌های VANET 5G بررسی می‌کند که از یک مدل الگوی اجتماعی پیش‌بینی برای توسعه پایداری خوشه استفاده می‌کند. الگوهای اجتماعی کشف‌شده سپس برای ایجاد خوشه‌ها استفاده می‌شوند تا وسایل نقلیه در خوشه‌های مشابه، مسیرهای مشابهی را به اشتراک بگذارند. نتایج مطالعه نشان می‌دهد که از نظر طول عمر خوشه‌ها عملکرد خوبی دارد و از نظر سربار خوشه‌بندی در مقایسه با الگوریتم‌های سنتی خوشه‌بندی اقتصادی‌تر است.

VANET ها یکی از نقاط عطف اصلی در توسعه ITS هستند .پیش‌بینی می‌شود که آنها به وسایل نقلیه متحرک اتصال همه جا با شبکه را برای دسترسی به خدمات مختلف خدمات ITS ارائه دهند. با این حال، برای این، برخی از استانداردهای سختگیرانه از نظر قابلیت اطمینان و تأخیر باید رعایت شود. دو تکنیک از هر شبکه خودرویی برای کمک به طیف وسیعی از خدمات ITS، یعنی تکنیک‌های ارتباط کوتاه برد اختصاصی (DSRC) برای RSU مستقیم به ارتباطات سلولی وسیله نقلیه به وسیله نقلیه در نظر گرفته شده است. روش های مورد استفاده در ادبیات به طور کلی خدمات ITS را در هر شبکه طبقه بندی می کنند تا با نیازهای محققین مربوطه مطابقت داشته باشد و با این فرض که یک شبکه واحد تمام خدمات را ارائه می دهد. مطالعاتی که هر دو تکنیک شبکه را برای ارائه مسیریابی چند مسیری، تقسیم مسیر، یا تعادل بار برای یک تجربه با کیفیت خوب از ITSها در نظر می گیرند، شبکه های کنترل شده را جداگانه در نظر می گیرند. مفهوم SDN که این مطالعه پیشنهاد می‌کند، یک معماری ترکیبی از یک شبکه است که کنترل مشترک شبکه‌ها را افزایش می‌دهد و اتصال به وسایل نقلیه چند خانه را ارائه می‌دهد و فرصت‌هایی را که چنین معماری فراهم می‌کند نشان می‌دهد. رشد شبکه های 5G به عنوان محرک اصلی توسعه مدل های تجاری و برنامه های کاربردی جدید به راحتی در دسترس است. در (AbdAllah et al, 2015) SDN و VANET با رشد شبکه‌ها و برنامه‌های کاربردی هوشمند خودرویی نسل بعدی، توانمندسازهای اصلی تکنیک 5G هستند. در حال حاضر، مطالعات بر روی ترکیب VANET و SDN متمرکز شده‌اند و از این منظر، مفاهیم مختلف مرتبط با معماری، مزایای سرویس‌های VANET مبتنی بر SDN و قابلیت‌های جدید استفاده از آنها را در نظر می‌گیرند. با این حال، استحکام و امنیت کل معماری هنوز جای سوال دارد و تاکنون مورد توجه مطالعات قرار نگرفته است. علاوه بر این، ادغام و استقرار بسیاری از مؤلفه‌های معماری و موجودیت‌های جدید منجر به آسیب‌پذیری‌ها و تهدیدات امنیتی جدید می‌شود. این مطالعه به بررسی طراحی زیرساخت شبکه، مزایا، موانع، و قابلیت‌های معماری VANET مبتنی بر SDN می‌پردازد. سپس این مطالعه نیز آسیب‌پذیری معماری‌های شبکه وسایل نقلیه تعریف‌شده نرم‌افزاری (SDVN) را در برابر تهدیدات اصلی امنیتی که می‌توانند خدمات اصلی امنیت، یعنی محرمانگی، در دسترس بودن، یکپارچگی داده‌ها و احراز هویت را نقض کنند، بررسی می‌کند. این

مطالعه دفاع در برابر این تهدیدات را پیشنهاد می‌کند و همچنین درس‌های آموخته‌شده و جهت‌گیری‌های آینده برای تحقیقات را برای ارائه راه‌حل‌هایی برای تضمین حفظ حریم خصوصی و امنیت دقیق در معماری‌های آینده SDVN مورد بحث قرار می‌دهد.

در (TalebiFard et al, 2012) با هدف باز کردن موانع پوشش شبکه و تراکم ترافیک در شبکه‌های خودرویی است این معماری از تکنیک‌های SDN و محاسبات لبه موبایل برای افزایش مقیاس‌پذیری و قابلیت اطمینان کلی شبکه تحت شرایط تراکم ترافیک بالا استفاده می‌کند. سپس، یک رویکرد خوشه‌بندی دستگاه به دستگاه برای گسترش پوشش شبکه برای گره‌ها استفاده می‌شود. کار آنها یک ساختار قابل اعتماد برای کمک به کاربردهای تأخیر بسیار کم فراهم می کند.

۳. معماری پیشنهادی

معماری پیشنهادی نشان‌دهنده انحراف عمده از VANET سنتی برای برآوردن نیازهای نسل جدید و برآورده کردن خواسته‌های جدید است. بخش های اصلی معماری پیشنهادی در زیر توضیح داده شده است:

eNBC (کنترلر پایه گره تکامل یافته): eNBC بخشی از شبکه 5G آینده است. این معماری ترکیبی از eNBC و کنترلر SDN را پیشنهاد می کند. این ترکیب اجازه ساخت یک ایستگاه پایه SD را برای کنترل و مدیریت سیار می دهد. کنترل‌کننده پایه گره تکامل‌یافته، اطلاعات مرکزی پشت VANET را تشکیل می‌دهد و خط‌مشی، اجرای امنیت را کنترل می‌کند، ثبات را ایجاد می‌کند و ترافیک را مدیریت می‌کند.

RSC (کنترل کننده کنار جاده): این یک کنترلر هوشمند متشکل از میکروسل ها برای ارتباط مستقیم با وسایل نقلیه برای اطمینان از پردازش سریع، مقیاس پذیری، اجرای قوانین و انعطاف پذیری است. RSC بار اجرای امنیت و مدیریت ترافیک را با eNBC به اشتراک می گذارد. آنها با هم پارامترهای کنترلی و پارامترهای امنیتی و داده ای را با وسایل نقلیه مدیریت می کنند.

گره‌های بی‌سیم هوشمند (IWN) این گره‌ها خودروهایی را نشان می‌دهند که به عنوان میزبان بی‌سیم در نظر گرفته می‌شوند و قابلیت‌های خودرو به وسیله نقلیه را دارند. وسایل نقلیه توسط RSCها در مناطق خود مدیریت می شوند و آنها تمام داده های ضروری را جمع آوری می کنند و اطلاعات مربوط به امنیت را به عوامل محلی داخلی منتقل می کنند.

در معماری سنتی VANET، هر وسیله نقلیه ای از ماژول های مختلف پروتکل های بی سیم برای راه اندازی لینک های مختلف با RSU ها استفاده می کند(Davies et al, 2018). این معماری از این تکنیک برای تبدیل انواع مختلف اطلاعات جمع آوری شده بر روی تکنیک های بی سیم در مورد امنیت و تعادل بار استفاده می کند. در این معماری، گزینه ارتباط بی سیم دوربرد، یعنی WiMAX/LTE برای صفحه کنترل، پهنای باند بیشتر و کاهش هزینه ارتباطات بی سیم، یعنی وفاداری بی سیم برای صفحه داده انتخاب شد.

۳،۱ پیش بینی، پیشگیری و تشخیص حملات

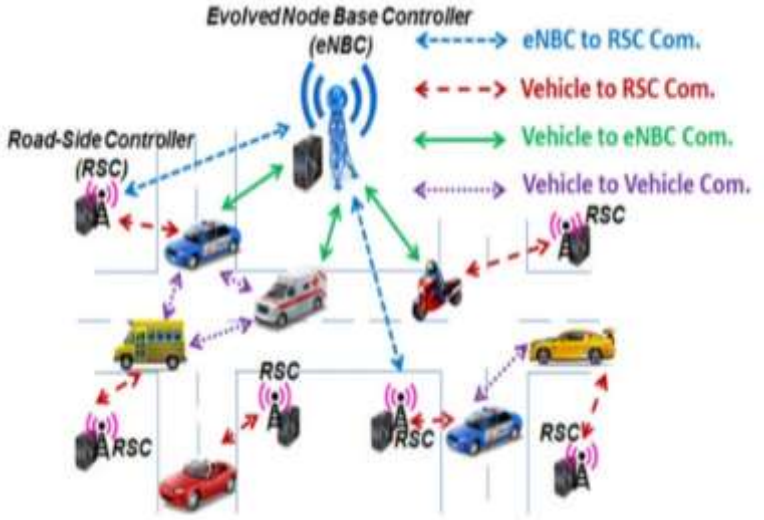
مجوز و احراز هویت سیستم پیشنهادی یک فرآیند جهانی از احراز هویت را برای جلوگیری از انواع مختلف حملات جعل هویت با هدف عناصر مختلف در شبکه فراهم می کند. در ابتدا، هر RSC باید توسط eNBC تأیید و تأیید شود. در این مورد، eNBC یک طرف مورد اعتماد در نظر گرفته می شود. RSC احراز هویت و تایید شده است، یعنی در پایگاه داده محلی RSC ذخیره می شود، جایی که هر وسیله نقلیه باید توسط eNBC و RSC احراز هویت شود. هنگامی که یک وسیله نقلیه جدید به دنبال پیوند با VANET است، درخواست احراز هویت را به RSC ارسال می کند. برای احراز هویت برای اولین بار، RSC این درخواست را به eNBC ارسال می‌کند، که باید ابتدا RSC را از طریق یک پروتکل چالش/پاسخ احراز هویت کند، جایی که درخواست در پاسخ به کاهش تبادل پیام‌های کنترل‌کننده کنار جاده از طریق چالش انجام می‌شود. پروتکل پاسخ در این پروتکل درخواست در پاسخ به کاهش تبادل پیام درگیر است. سپس باید خودرو را احراز هویت کند و گواهی را تولید کند، که در پایگاه داده تکامل یافته eNBC، پایگاه داده محلی RSC، ذخیره می شود و در اختیار خودرو قرار می گیرد. بار دوم که یک وسیله نقلیه درخواست پیوند می‌کند، که در آن احراز هویت توسط RSC مدیریت می‌شود و eNBC خودرو صرفاً نشان داده می‌شود. لازم به ذکر است که کلیدها ممکن است توسط eNBC یا RSC تولید شوند اما گواهینامه ها فقط توسط NBC تکامل یافته تولید می شوند. RSC در حین تحویل توسط eNBC احراز هویت می شود و

وسیله نقلیه از حوزه قضایی یک RSC به RSC بعدی منتقل می شود، RSC ها می توانند با استفاده از گواهینامه های ذخیره شده احراز هویت متقابل را انجام دهند. هنگامی که در ابتدا یک تحویل وجود دارد، RSC قدیمی یک درخواست برای تحویل به RSC جدید ایجاد می کند. بنابراین، پس از مرحله احراز هویت بعدی، RSC قدیمی اعتبار خودروها را به RSC جدید منتقل می کند. به طور مشابه، هنگامی که خودرو درخواست پیوند به RSC جدید می‌کند، خودرو به درستی احراز هویت می‌شود. در نهایت، پس از انجام تحویل، به روز رسانی از RSC جدید به eNBC در مورد مکان وسیله نقلیه ارسال می شود. هنگام ایجاد به روز رسانی، RSC جدید باید توسط eNBC احراز هویت شود. ماژول AA پیاده سازی شده در eNBC پایگاه داده احراز هویت و قوانین را در هر RSC ایجاد می کند و سیاست های مجوز عمومی شبکه را نصب می کند.

پیشگیری و شناسایی حملات گره های در معرض خطر و وسایل نقلیه مخرب منابع اصلی تهدید در VANET هستند. شکل اصلی حمله ای که باید مدیریت شود، حمله انکار سرویس توزیع شده است که مبتنی بر سیل شبکه با ترافیک به وسایل نقلیه دلخواه یا RSCها است تا eNBC را درگیر کند تا منابع خود را تمام کند و دید شبکه را در سطح کنترل کننده مختل کند تا روند کار را مختل کند. ارسال در صفحه داده یا انکار خدمات RSCها. جعل پروتکل اینترنت شکل دیگری از حمله است که در آن از فناوری‌هایی استفاده می‌شود که به منبع واقعی اجازه می‌دهد در طول حملات ناشناس بماند. هدف تکنیک پیشنهادی در این مقاله شناسایی حملات انکار سرویس توزیع شده از هر دو وسیله نقلیه یا وسایل نقلیه مخرب با هدف RSC های مختلف یا سایر وسایل نقلیه است. در زیر مروری بر سیستم پیشنهادی ارائه شده است:

- بررسی بسته های جمع آوری شده با هدف یک آدرس IP خاص با شناسایی و ردیابی تعداد بسته در ثانیه آن برای مقایسه آن با یک آستانه.
- نگهداری پایگاه داده ای از اتصال داده های IP-اینترنت برای تشخیص هویت جعلی و پروتکل های اینترنتی. یک هشدار با شناسه منبع/آدرس پروتکل اینترنت مهاجم ارسال می‌شود تا هنگام شناسایی حمله مسدود شود.
- جعل IP، یک فرآیند ردیابی برای تعیین محل منشا حمله به کار گرفته می شود تا بتوان حمله را در مبدا مسدود کرد.

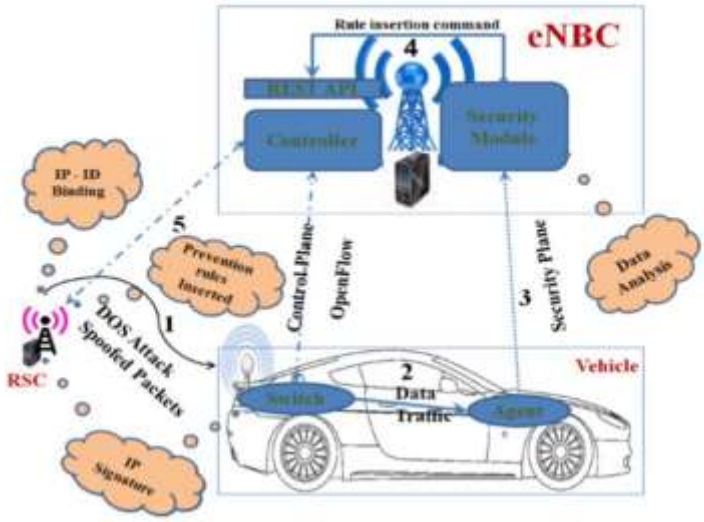
روند کلی در شکل ۱ و ۲ نشان داده شده است. در سطح خودرو: اتصال IPI از پیش طراحی شده به کنترل کننده اجازه می دهد تا هر وسیله نقلیه را در شبکه ردیابی کند. هنگامی که بسته ای که از یک منبع منتشر می شود با هنجارهای الزام آور روی سوئیچ مطابقت ندارد، یک هشدار به ماژول امنیتی در سمت سرور ارسال می شود. در داخل وسایل نقلیه، عامل امنیتی تمام سرصفحه های بسته های جعلی غیر مشابه را از طریق صفحه امنیتی به ماژول امنیتی منتقل می کند. سیاست ردیابی حمله در سطح سوئیچ با تنظیم شناسایی منبع بسته های جعلی که با قوانین اتصال مطابقت ندارند استفاده می شود. فقط بسته های غیر مشابه باید به ماژول امنیتی منتقل شوند. در سطح کنترل کننده: ماژول امنیتی به بسته های دریافتی از عامل گوش می دهد. نمودار جریان فرآیند در شکل ۱و۲ ارائه شده است.



شکل۱: معماری SDN VANET

پس از به دست آوردن بسته های اصلاح شده، کنترل کننده آنها را بر اساس آدرس های پروتکل اینترنتی امضا شده گروه بندی می کند. این تغییر به کنترل کننده اجازه می دهد تا منبع RSC و وسیله نقلیه حمله را پس از به دست آوردن بسته های امضا شده شناسایی کند. این بسته ها تنها در صورتی به عنوان بسته های حمله انکار سرویس توزیع شده در نظر گرفته می شوند که تعداد آنها از تعداد آستانه بیشتر شود، در غیر این صورت به عنوان بسته های غیرمجاز مدیریت می شوند و مسدود می شوند. در هر صورت، رویکرد پیشگیرانه در سمت RSC/ Vehicle استفاده خواهد شد. پس از اینکه فرآیند تشخیص تغییر حالت را مشاهده کرد، درخواست را از طریق رابط برنامه نویسی برنامه REST به کنترل کننده ارسال می کند تا در صورت حمله انکار سرویس جعلی پروتکل اینترنت، یک هنجار مسدودکننده IP/Identification را به همه سوئیچ ها یا یک پورت جداگانه وارد کند. . همانطور که در بخش‌های قبلی توضیح داده شد، پیام‌های بسته در برای تغییر ناپذیری تأیید می‌شوند که در صورت نقض برخی از سیاست‌ها توسط گروهی از بسته‌ها، پیام هشدار را نشان می‌دهد. مزایای تکنیک محاسبات مه در چنین شرایطی تجربه می شود که نیاز به قدرت پردازش نزدیک به کاربر برای بهره مندی از کاهش زمان پاسخ و به حداقل رساندن تاخیر دارد. در این معماری، تشخیص و پیشگیری از حملات مستلزم اقدامات متقابل سریع، به ویژه در هنگام کار با وسایل نقلیه سریع السیر است. از این رو توابع امنیتی در داخل سلول کوچک برای تجهیز RSC به قابلیت‌های پردازش ماژول امنیتی پیشنهاد می‌شوند. یک فرآیند بی خطر، روش کنترل تطبیقی است. در آن، خرابی یک RSC یا ایستگاه eNBC مشکل را پیش‌بینی می‌کند و دستور محصور کردن RSCها را برای افزایش قدرت انتقال می‌دهد.

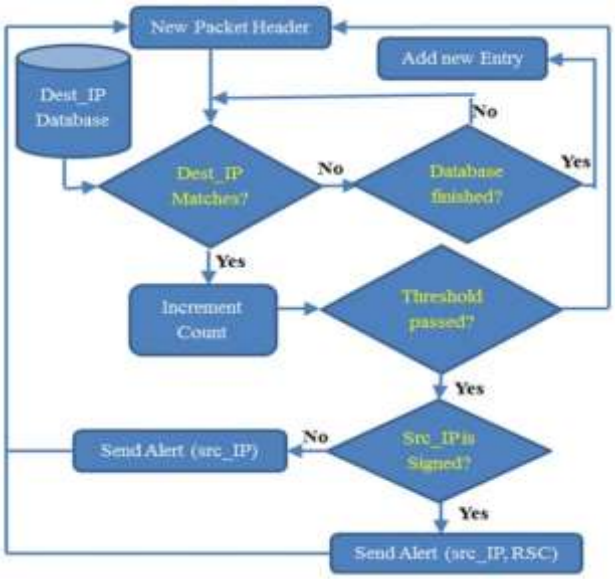
این منجر به گسترش دامنه انتقال وسایل نقلیه می شود به طوری که آنها می توانند به صورت توزیع شده به این RSC ها متصل شوند تا زمانی که مشکل حل شود. طرح پیشنهادی برای پیش‌بینی حملات در زمان واقعی با استفاده از حداقل منابع کنترل‌کننده طراحی شده است و با کمترین طراحی، نه تنها برای پیش‌بینی حملات انکار سرویس توزیع‌شده، بلکه برای جلوگیری از تخریب دید کنترل‌کننده از کل شبکه توسط میزبان‌های مخرب با جعل آدرس های پروتکل اینترنت خود طراحی شده است. هدف اصلی سیستم پیشنهادی طراحی و توسعه یک رویکرد ترکیبی برای افزایش امنیت در VANET با استفاده از شبکه‌های 5G است.



شکل۲: طرح کلی فرآیند

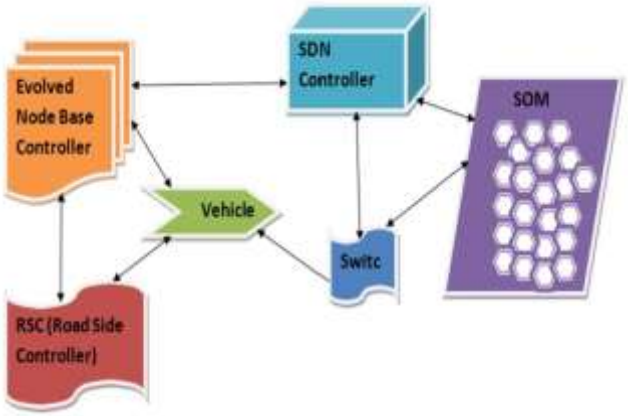
شکل ۲ نمودار SOM و SDN اعمال شده در شبکه VANET را نشان می دهد. اولین قدم طراحی یک VANET با استفاده از چندین گره برای درگیر کردن RSC و وسایل نقلیه است. این وسیله نقلیه به عنوان eNBC عمل می کند که بخشی از شبکه 5G آینده است. ایستگاه پایه گره تکامل‌یافته و SDN ابتدا یکپارچه شده‌اند تا اجازه ساخت یک SD BS برای کنترل و مدیریت سیار را بدهند. eNBC شامل اطلاعات مرکزی پشت VANET است و مسئولیت اجرای امنیت، کنترل خط مشی، و تأسیسات را بر عهده دارد. سازگاری و

مدیریت ترافیک RSC یک کنترل کننده میکروسل هوشمند برای ارتباط مستقیم با وسایل نقلیه برای ارائه پردازش سریع، مقیاس پذیری، مدیریت قوانین و انعطاف پذیری است. RSC بار اجرای امنیت و مدیریت ترافیک را با eNBC به اشتراک می گذارد(Jaballah et al, 2016). آنها با هم صفحه کنترل را مدیریت می کنند و همچنین هر دو پارامترهای امنیتی و داده را با گره های بی سیم (وسایل نقلیه) مدیریت می کنند.



شکل۳: فلوچارت تشخیص حمله

مرحله دوم اعمال SOM و SDN در شبکه VANET با استفاده از سوئیچ جریان باز است. سوئیچ و یک کنترلر در سوئیچ جریان باز استفاده می شود. ادغام SDN مشابه پلتفرم در مقاله "SDN VANETs در 5G" خواهد بود. (شکل ۳).



شکل۴: SOM و SDN به شبکه VANET با استفاده از سوئیچ جریان باز اعمال می شود

۳،۲ الگوریتم SOM

SOM یک تکنیک DM است که مبتنی بر یادگیری بدون نظارت است(Li et al, 2008). در الگوریتم SOM، اطلاعات ورودی مجدداً مرتب شده و در یک فضای کم ابعاد به نام شبکه گره یا نقشه نمایش داده می شود. از آنجایی که اطلاعات ورودی عموماً ابعاد بالایی دارند، نقشه خودسازماندهی به مشاهده نمای کم ابعاد اطلاعات با ابعاد بالا کمک می کند (شکل ۴). یادگیری SOM باعث می شود که بخش های مختلف یک شبکه به الگوهای ورودی خاصی پاسخ دهند. مراحل الگوریتم SOM در الگوریتم ۱ توضیح داده شده است:

الگوریتم۱: الگوریتم خودسامانده SOM

started with fixed or random values
Step 1: For every node in a map a vector is
Step 2: The Euclidean Distance (ED) to all nodesin the map is evaluated when an input vector i given in it
becomes the Best Matching Unit (BMU) Step 3: The node that is nearest to the input node evaluated to reduce time Step 4: The neighborhood radius of the BMU is
neighboring vector node is adjusted to make them Step 5: Using the following equation, every $W(t + 1) = W(t) + LR(t) * RD(t) * (V(t) – W(t))$ much like the input vector:
reduce over time gradually. $RD(t)$ is the Where $LR(t)$ indicates the learning rate which must distance to Best Matching Unit. The nearest a node is to Best Matching Unit the more its relative affected. vector gets
Step 6: Repeat Step 2 through several iterations

الگوریتم SOM و SDN در VANET با استفاده از کد موجود در MATLAB استفاده می شود. MATLAB یک برنامه کامپیوتری است که محیط مناسبی را برای انجام بسیاری از محاسبات در اختیار مشتری قرار می دهد. برای حل معادلات دیفرانسیل استفاده می شود و ابزاری سریع، کارآمد و موثر است. نوشتن برنامه در متلب و اشکال زدایی آن با دیباگر متلب و تغییر برنامه متناسب با محیط های مختلف آسان است.

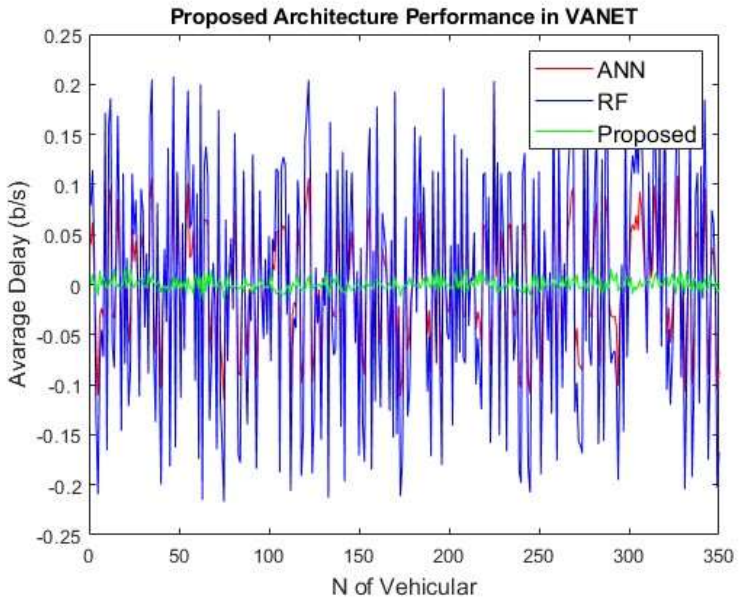
٤. نتایج شبیه سازی و پیاده سازی ها

سیستم پیشنهادی با استفاده از شبیه ساز NS-3 برای برآورد امکان سنجی و کارایی سیستم مدل سازی شد. کل منطقه از طریق یک eNBC واحد مدیریت می شود که در مرکز منطقه سیستم قرار گرفته است تا اتصال بی سیم را با همه RSC ها ارائه دهد. آزمایش‌ها با تمرکز بر نتایج عملکرد VANET در زمان‌های مختلف شبیه‌سازی انجام شد. سایر پارامترهای شبیه سازی در جدول ۱ نشان داده شده است.

جدول۱: پارامترهای شبیه سازی

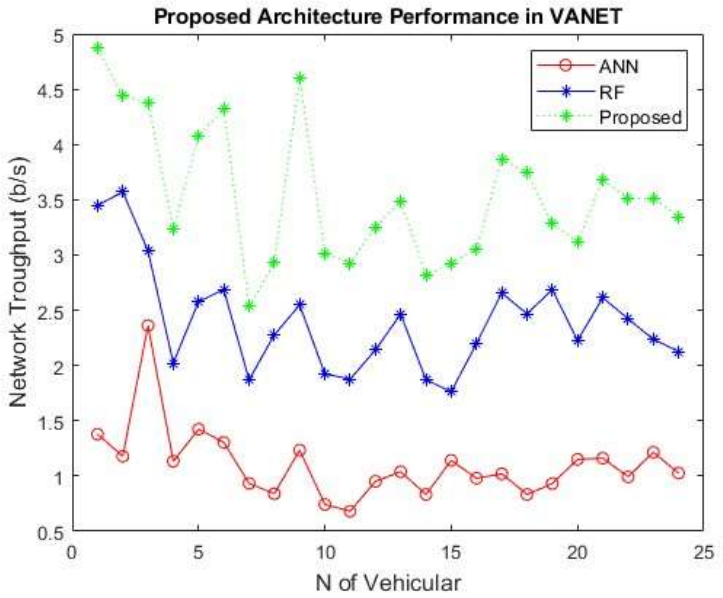
مولفه های	ارزش های
سیستم عامل	لینوکس (اوبونتو ۱۲.۰۴)
نسخه NS-3	NS-3.25
تعداد وسایل نقلیه	۱۰، ۲۰، ۳۰، ۴۰، ۵۰، ۶۰، ۷۰، ۸۰، ۹۰، ۱۰۰
تعداد RSU	۲۰، ۴۰، ۶۰، ۸۰، ۱۰۰
مدل تحرک برای وسیله نقلیه	تخصیص موقعیت تصادفی دیسک
مدل تحرک برای RSU	مدل تحرک موقعیت ثابت
اندازه بسته	۱۰۰۰ بایت
نوع ترافیک	UDP/CBR
زمان مکث	۱۰، ۲۰، ۳۰، ۴۰، ۵۰
لایه فیزیکی	استاندارد IEEE WIFI 80211
پروتکل مسیریابی	AODV

در این مقاله نتایج را بر اساس SDN، امنیت و SOM فعال VANET و مدل پایه VANET مقایسه کردیم. شکل ۵ نسبت تحویل بسته VANET را در تاخیر متوسط نشان می دهد. نتایج نشان می‌دهد که PDR کلی تقریباً پایدار است وقتی که امنیت، آشکارساز DOS و SOM صرف نظر از تغییر در زمان شبیه‌سازی اعمال شود.



شکل۵: میانگین تاخیر انتها به انتهای بسته های روش پیشنهادی در مقایسه با سایر روش ها در شبکه های ادهاک خودرویی

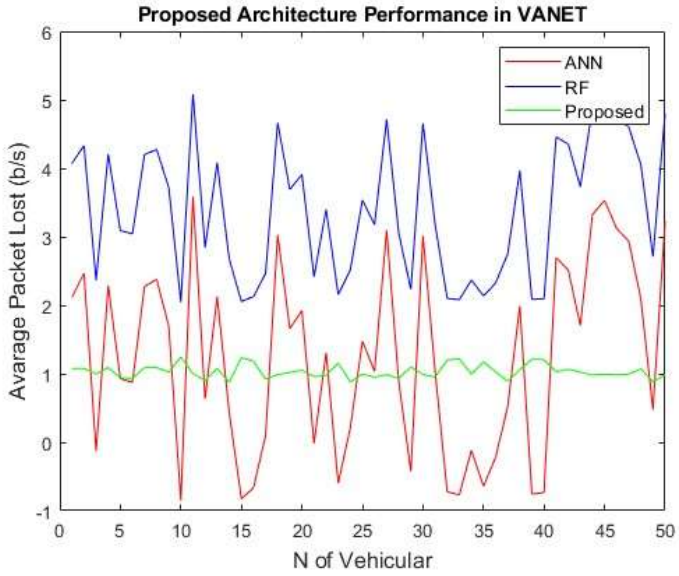
در شکل۵ تاخیر سرتاسر سیستم پیشنهادی و سیستم معمولی به عنوان تابعی از زمان شبیه سازی ارائه شده است. همانطور که انتظار می‌رود، عملکرد سیستم معمولی در مقایسه با سیستم پیشنهادی تاخیر انتها به انتها بالاتری داشت. شکل۶ توان عملیاتی بین سیستم موجود و پیشنهادی را بر اساس پارامترهای شبکه نشان می دهد.



شکل۶: توان عملیاتی روش پیشنهادی در مقایسه با سایر روش ها در شبکه های ادهاک خودرویی

در شکل۷ میانگین گم شدن بسته ها را نمایش داده می شود. VANET با SDN، به وضوح نشان می دهد، امنیت و SOM در مقایسه با VANET بدون SDN، امنیت و SOM تمایل به اتصالات کمتری دارد. از آنجایی که امنیت شبکه از اهمیت بالایی برخوردار است، پیشنهاد یک سیستم عامل مبتنی بر معماری VANET مبتنی بر SDN که بتواند حملات را پیش‌بینی و از آن جلوگیری کند، هدف اصلی این مقاله بود. VANET یک شبکه آینده نگر در ITS است که هدف آن ارائه راحتی و ایمنی بیشتر برای مسافران است. SDN

نقش اساسی در فناوری 5G ایفا می کند که منجر به ایده توسعه امنیت VANET شد. ارزیابی نشان داده شده توانایی سیستم پیشنهادی برای پیاده سازی را نشان داد.



شکل۷: میانگین گم شدن بسته های روش پیشنهادی در مقایسه با سایر روش ها در شبکه های ادهاک خودرویی

تمامی نتایج شبیه سازی و پیاده سازی حاکی از کاهش میانگین تاخیر انتها به انتهای بسته ها و افزایش توان عملیاتی شبکه و کاهش میانگین گم شدن بسته ها می باشد که تمامی مطالب مذکور نشانگر بهبود کارایی شبکه های ادهاک خودرویی می باشد. سطوح مختلف امنیت همزمان تعریف شده توسط کاربر در حالی که حداقل طراحی و سطوح سربار کاهش یافته است. به دلیل مزایای محیط 5G و تکنیک SDN/SOM، سیستم مطمئناً نیازهای VANET را با پاسخ‌های فوری و کاهش تأخیر برآورده می‌کند. این مقاله نشان می‌دهد که چگونه چنین رویکرد ترکیبی می‌تواند VANET را از انواع مختلف حملاتی که به خودروها یا کنترل‌کننده‌ها هدف قرار می‌گیرند، ایمن کند. بنابراین، ممکن است نتیجه بگیریم که 5G، SOM و SDN مقیاس پذیری مطلوب، مدیریت بهتر و انعطاف پذیری را به VANET اضافه می کنند.

۵. نتایج و کارهای آتی

معماری پیشنهادی در این مقاله شامل ارائه یک زیرساخت امنیتی نوین مبتنی بر الگوریتم های یادگیری بدون نظارت جهت شناسایی و مقابله با حملات مخرب در شبکه های ادهاک خودرویی می باشد. طرح پیشنهادی دو معماری شبکه های نرم افزار محور (SDN) و نقشه خودسازماندهی (SOM) را برای سیستم VANET مبتنی بر 5G ترکیب می کند. سیستم پیشنهادی ترکیبی جدید از SDN و یک راه حل شبکه مبتنی بر نقشه خود سازماندهی (SOM) برای افزایش امنیت در دو بعد، شناسایی و جلوگیری از حملات خواهد بود. این مقاله یک سیستم موثر جدید برای ایمن سازی VANET ارائه می دهد که بر ادغام SOM و SDN در یک محیط 5G بدون تنظیم پارامترهای کنترلی یا ایجاد تاخیر داده یا ازدحام کنترل کننده متکی است. سیستم پیشنهادی ممکن است به طور موثر مسائل امنیتی اساسی در VANET ها را مدیریت کند. یک تکنیک اجتناب از حمله و شناسایی که به پارامترهای امنیتی جدید بستگی دارد، راه حل شبکه مبتنی بر توسعه داده شد تا امنیت را در دو بعد، شناسایی و جلوگیری از حملات، افزایش دهد. این مقاله آسیب پذیری عملکرد شبکه را با در نظر گرفتن حملات انکار سرویس توزیع شده (DDoS) تجزیه و تحلیل می کند.

نتایج پیاده سازی و شبیه‌سازی های معماری پیشنهادی در این مقاله نشان از افزایش دقت تشخیص حملات، افزایش توان عملیاتی شبکه، کاهش میانگین تاخیر انتقال داده و کاهش میانگین بسته های گم شده در شبکه های ادهاک خودرویی در مقایسه با سایر

روشهای امنیتی موجود می باشد. در کارهای آتی می توان رویکرد پیشنهادی را با الگوریتم های فراابتکاری بهبود یافته پیاده سازی نمود.

منابع و مراجع:

Jacobson, V.; Smetters, D.K.; Thornton, J.D.; Plass, M.F.; Briggs, N.H.; raynard, R.L. Networking named content. In Proceedings of the 5th International Conference on Emerging networking Experiments and Technologies, Rome, Italy, 1–4 December 2009.

TalebiFard, P.; Leung, V.C.; Amadeo, M.; Campolo, C.; Molinaro, A. Information-centric networking for VANETs. In Vehicular Ad Hoc Networks; Springer: Berlin, Germany, 2015; pp. 503–524.

Gerla, M.; Lee, E.K.; Pau, G.; Lee, U. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In Proceedings of the 2014 IEEE World Forum on Internet of Things, Seoul, Korea, 6–8 March 2014.

Davies, E.; Tyson, G.; Ohlman, B.; Pentikousis, K.; Eum, S.; Corujo, D.; Molinaro, A.; Boggia, G. Information-Centric Networking: Baseline Scenarios. Available online: https://www.rfc-editor.org/rfc/pdfrfc/rfc7476.txt.pdf (accessed on 27 October, 2018).

TalebiFard, P.; Leung, V. A content centric approach to dissemination of information in vehicular networks. In Proceedings of the Second ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Paphos, Cyprus, 21–22 October 2012.

Bai, F.; Krishnamachari, B. Exploiting the wisdom of the crowd: localized, distributed information-centric VANETs [Topics in Automotive Networking]. IEEE Commun. Mag. 2010, 48, 138–146.

Saini, M.; Alelaiwi, A.; Saddik, A.E. How close are we to realizing a pragmatic vanet solution? A meta-survey. ACM Comput. Surv. 2015, 48.

Amadeo, M.; Campolo, C.; Molinaro, A. Information-centric networking for connected vehicles: A survey and future perspectives. IEEE Commun. Mag. 2016, 54, 98–104.

Ashraf, M.; Bilal, H.; Khan, I.A.; Ahmad, F. Vanet Challenges of Availability and Scalability. VFAST Trans. Softw. Eng. 2016, 10.

Ahlgren, B.; Dannewitz, C.; Imbrenda, C.; Kutscher, D.; Ohlman, B. A survey of information-centric networking. IEEE Commun. Mag. 2012, 50, 26–36.

AbdAllah, E.G.; Hassanein, H.S.; Zulkernine, M. A survey of security attacks in information-centric networking. IEEE Commun. Surv. Tutor. 2015, 17, 1441–1454

Cisco. Visual Networking index: Forecast and Methodology: 2016–2021. Available online: https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html (accessed on 27 October 2018).

J. Vestin, P. Dely, A. Kassler, N. Bayer, H. Einsiedler, and C. Peylo, “Cloudmac: Towards software defined wlans,” SIGMOBILE Mob. Comput. Commun. Rev., vol. 16, no. 4, pp. 42–45, 2013.

D. Kreutz, F. M. V. Ramos, P. E. Verssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-defined networking: A comprehensive survey,” Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, Jan 2015.

H. Hartenstein and L. P. Laberteaux, “A tutorial survey on vehicular ad hoc networks,” IEEE Communications Magazine, vol. 46, no. 6, pp.164–171, June 2008.

S. Eichler, “Performance evaluation of the ieee 802.11p wave communication standard,” in 2007 IEEE 66th Vehicular Technology Conference, Sept 2007, pp. 2199–2203.

E. Schoch, F. Kargl, and M. Weber, “Communication patterns in vanets,” IEEE Communications Magazine, vol. 46, no. 11, pp. 119–125, November 2008.

W. B. Jaballah, M. Conti, M. Mosbah, and C. E. Palazzi, “Fast and secure multihop broadcast solutions for intervehicular communication,” IEEE Transactions on Intelligent Transportation Systems, vol. 15, no. 1, pp. 433–450, Feb 2014.

C.-T. Li, M.-S. Hwang, and Y.-P. Chu, “A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks,” Computer Communications, vol. 31, no. 12, pp. 2803 – 2814, 2008.

W. B. Jaballah, M. Conti, M. Mosbah, and C. E. Palazzi, “The impact of malicious nodes positioning on vehicular alert messaging system,” Ad Hoc Networks, vol. 52, no. Supplement C, pp. 3 – 16, 2016.

A New Hierarchical Architecture Based on Unsupervised Learning Algorithms to Improve Operational Performance and Security of Vehicular Ad Hoc Networks

Hamid Hadi[1]
[1] **Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran,**
[*]**Kambiz Majidzadeh**[2]
[2]**Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran**

Vehicular Ad Hoc Networks (VANET) is an emerging technology with a promising future. VANETs are completely different from mobile ad hoc networks (MANETs) in terms of features, challenges, system architecture, and application. The Internet of Vehicles (IoV), a rapidly growing technology used for efficient communication between vehicles, has drawn attention from traditional vehicular ad hoc networks (VANETs). Software-Defined Networking (SDN) is another emerging technology network pattern that has the ability to efficiently manage overall networks and transform complex network architectures into simple and manageable architectures. Dispersive data storm is an important issue in IoV-based NDN due to the data dispersive nature of NDN. The high speed and fast topology change of vehicles in IoV causes the problem of link disconnection and unnecessary delay in data transmission. Another important VANET security challenge is predicting and preventing attackers. The proposed architecture in this thesis includes providing a new security infrastructure based on unsupervised learning algorithms to identify and deal with malicious attacks in automotive ad hoc networks. The proposed scheme combines two architectures of software-oriented networking (SDN) and self-organizing map (SOM) and will be a novel combination of SDN and a self-organizing map (SOM) based network solution to enhance security in two dimensions, detect and prevent attacks. This Article analyzes the security of the proposed system with existing DDoS has been analyzed and investigated. The results of the implementation and simulations of the proposed architecture in this thesis show an increase in attack detection accuracy, an increase in network throughput, a decrease in the average data transfer delay, and a decrease in the average lost packets in automotive ad hoc networks compared to other existing security methods.

Keywords: Software Defined Networks, Ad Hoc Networks, Transmission Rate, Propagation Delay, Malicious Attacks