بررسی عملکرد امنیتی یک‌پارچه‌سازی شبکه‌های اقتضایی خودرویی با شبکه‌های نرم‌افزارمحور

مژگان قصابی[1] و محمود دی پیر*[2]

[1] دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، باشگاه پژوهشگران جوان و نخبگان، تهران،ایران
mozhgan.ghasabi@srbiau.ac.ir

[2] استادیار، دانشکده رایانه و فناوری اطلاعات، دانشگاه هوایی شهید ستاری،تهران
mdeypir@ssau.ac.ir

چکیده

در سال‌های اخیر، شبکه‌های اقتضایی خودرویی به‌عنوان یکی از حوزه‌های فعال در زمینه ارائهٔ فناوری مطرح شده است که طیف گستردهٔ خدماتی را از جمله ایمنی جاده‌ای، ایمنی سرنشینان، امکانات سرگرمی برای سرنشینان و تسهیلات اضطراری ارائه می‌کند. توسعه و مدیریت شبکه‌های اقتضایی خودرویی فعلی با توجه به نبود انعطاف‌پذیری، پیچیدگی و پویایی هم‌بندی شبکه با چالش‌های زیادی مواجه است. به‌منظور تسهیل مدیریت شبکه‌های فعلی، معماری شبکه‌های مبتنی بر نرم‌افزار معرفی شده که این معماری با جداسازی بخش کنترل از بخش داده‌ای پیچیدگی‌های شبکه را کاهش می‌دهد. شبکه‌های نرم‌افزارمحور با ارائه قابلیت انعطاف‌پذیری و برنامه‌پذیری می‌تواند به انجام وظایف مدیریت و بهره‌وری در شبکه‌های اقتضایی خودرویی نیز کمک کند. ما در این مقاله بر امکان استفاده از شبکه‌های نرم‌افزارمحور در محیط شبکه‌های اقتضایی خودرویی متمرکز شده‌ایم. ابتدا، در این مقاله معماری شبکه‌های اقتضایی خودرویی مبتنی بر شبکه‌های نرم‌افزارمحور و حالت‌های عملیاتی آن بررسی و سپس مزایا و سرویس‌های ارائه‌شده توسط این معماری توصیف می‌شود؛ در نهایت برخی از چالش‌های محتمل در معماری شبکه‌های اقتضایی خودرویی مبتنی بر نرم‌افزار بیان می‌شود.

واژگان کلیدی: شبکه‌های اقتضایی خودرویی، شبکه‌های نرم‌افزارمحور، شبکه‌های اقتضایی خودرویی نرم‌افزارمحور، شبکه‌های بی‌سیم.

۱- مقدمه

خودرو در ابتدا فقط به‌عنوان یک وسیله حمل و نقل ساده شناخته می‌شد؛ سپس توانایی دریافت امواج رادیویی به این وسیله اضافه شد؛ به‌طوری‌که رانندگان اطلاعات ترافیکی را برای جلوگیری از ازدحام ترافیک از طریق رادیو دریافت می‌کردند. بعدها امکان ارتباطات بین خودرویی، سامانهٔ GPS[1]، امکانات سرگرمی صوتی- تصویری و عملکردهای متنوع به این سامانه افزوده شد. بر اساس برآوردها در سال ۲۰۱۹ ۶۵٪ از وسایل نقلیه جدید توانایی ارتباط با همه چیز[2](V2X) را خواهند داشت و تا سال ۲۰۲۰ تمام وسایل نقلیه به این عملکرد تجهیز خواهند شد. بنابراین، طراحی معماری مطمئن انعطاف‌پذیر برای ایجاد ایمنی و تسهیلات رفاهی رانندگی بسیار ضروری است [۱]. امروزه با ورود به عصر سامانه حمل و نقل هوشمند، مقیاس‌پذیری شبکه، تنوع خدمات ارائه‌شده، مدیریت سامانه و امکان نوآوری‌های سامانه‌ای بسیار حائز اهمیت است. شبکه‌های اقتضایی خودرویی(VANET)[3] به‌عنوان مهم‌ترین جزء سامانه حمل و نقل هوشمند محسوب می‌شوند [۲]. مدیریت و توسعه شبکه‌های اقتضایی خودرویی با توجه به ویژگی‌های ذاتی این ساختار از جمله تغییرات مکرر هم‌بندی، اتصالات متناوب شبکه، تراکم پویای شبکه‌ای و نبود توازن جریان‌های ترافیکی در هم‌بندی‌های چندمسیره بسیار دشوار است.

درهمین‌اواخر معماری شبکه‌های نرم‌افزارمحور (SDN)[4] به‌عنوان رویکرد انعطاف‌پذیر جهت کنترل و مدیریت شبکه ارائه شده است که این معماری برای حل مسایل کلاسیک شبکه‌ها نظیر کنترل ازدحام، مهندسی ترافیک، مسیریابی و توازن بار راه‌کارهای نرم‌افزاری و خلاقانه‌ای را ارائه می‌کند. در این معماری، عملکرد کنترلی شبکه از عملکرد

[1] Global Positioning System
[2] Vehicle-to-Everything
[3] Vehicular adhoc Networks
[4] Software-defined networks

*نویسندهٔ مسؤول

انتقالی آن جدا است. قابلیت برنامه‌پذیری این ساختار، علاوه‌بر تسهیل مدیریت شبکه موجب تسریع نوآوری‌های شبکه نیز می‌شود. در این معماری، اپراتورها به جای به‌روزرسانی تمام نرم‌افزارهای نصب‌شده روی همه سوئیچ‌ها، می‌توانند با به‌روزرسانی نرم‌افزاری کنترل‌کننده، عملکرد جدیدی را به شبکه بیافزایند.

در حال حاضر، راه‌حل‌های مبتنی بر شبکه‌های نرم‌افزارمحور به‌صورت گسترده در انواع مختلفی از شبکه‌های سیمی از قبیل شبکه‌های گسترده محلی(WAN)[1] و شبکه‌های مراکز داده‌ای مورد استفاده قرار می‌گیرد. درهمین‌اواخر تعدادی از پژوهشگران به پژوهش در زمینه ادغام شبکه‌های نرم‌افزارمحور با سایر شبکه‌های غیرسیمی پرداخته‌اند [۳]. با استفاده از معماری شبکه‌های نرم‌افزارمحور می‌توان بسیاری از چالش‌های موجود در شبکه‌های اقتضایی خودرویی را حل کرد [۱]. اعمال اصول معماری شبکه‌های نرم‌افزارمحور در محیط شبکه‌های اقتضایی خودرویی موجب انعطاف‌پذیری، مقیاس‌پذیری و برنامه‌پذیری شبکه می‌شود. با جداسازی بخش کنترل از بخش داده‌ای[2] شبکه‌های اقتضایی خودرویی، هوشمندی شبکه به حالت متمرکز منطقی تبدیل شده و اصول زیرساخت شبکه، انتزاعی از برنامه‌های کاربردی خواهد شد. بنابراین، ادغام معماری شبکه‌های نرم‌افزارمحور با محیط شبکه‌های اقتضایی خودرویی قابلیت‌های سازگاری بالا، انعطاف‌پذیری، مقیاس‌پذیری در این محیط را به ارمغان خواهد آورد.

در همین اواخر پژوهش‌های اندکی در زمینه شبکه‌های اقتضایی خودرویی مبتنی بر شبکه‌های نرم‌افزارمحور[3] (SDVN) انجام شده است. ما در این مقاله برای درک بهتر، بررسی جامعی بر معماری شبکه‌های اقتضایی خودرویی مبتنی نرم‌افزار خواهیم داشت. این مقاله به‌شرح زیر سازماندهی شده است:

در ابتدا معماری شبکه‌های نرم‌افزارمحور، معماری شبکه‌های اقتضایی خودرویی و چالش‌های امنیتی موجود در شبکه‌های اقتضایی خودرویی مورد بررسی قرار می‌گیرد؛ سپس هم‌گرایی شبکه‌های نرم‌افزار محور با شبکه‌های بی‌سیم و وظایف این ساختار در شبکه‌های اقتضایی خودرویی توصیف و در بخش بعدی معماری شبکه‌های خودرویی مبتنی بر نرم‌افزار معرفی شده و حالت‌های عملیاتی این معماری جهت سازگاری با معماری شبکه‌های نرم‌افزار محور بررسی می‌شود. سپس سرویس‌های ارائه‌شده و نحوه بهبود امنیت در معماری شبکه اقتضایی خودرویی مبتنی بر نرم‌افزار معرفی و در آخر نیز چالش‌های محتمل در این معماری تفسیر می‌شود.

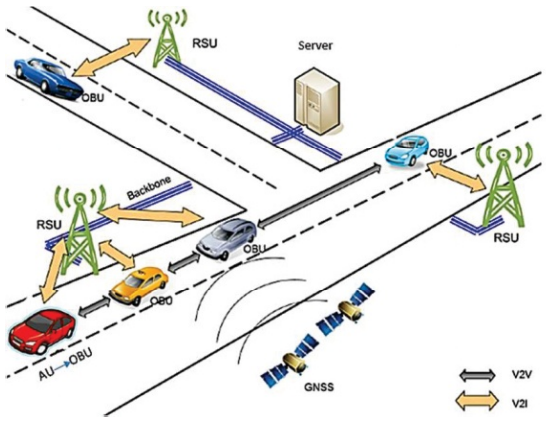
۲- شبکه‌های اقتضایی خودرویی

ارتباط میان خودروها در هنگام حرکت، رؤیای قدیمی بشر بوده و تاریخچهٔ نخستین تلاش‌ها برای تحقق این رؤیا به بیش از چهل سال پیش برمی‌گردد. در آن زمان با نصب آنتن روی خودروهای خاصی مانند خودروهای پلیس یا اورژانس و تنظیم‌کردن آنتن‌ها روی یک فرکانس خاص، سعی می‌کردند، ارتباط رادیویی و شبه‌تلفنی را ایجاد کنند. در سال ۱۹۹۹کمیسیون ارتباطات فدرال ایالات متحده با تصویب استانداردها و پهنای باند لازم برای ارتباط خودروها با تجهیزات ثابت کنار جاده درعمل مرحلهٔ جدیدی از شبکه‌های بین خودرویی را ایجاد کرده که این حرکت با تصویب استاندارد DSRC[4] در سال ۲۰۰۳ تکمیل شد. در این استاندارد پهنای باند ۵/۹ گیگا هرتز به ارتباطات بین خودرویی اختصاص داده شده است. روی این فرکانس بین هفت تا ده کانال تعریف می‌شود که یک کانال به‌صورت ویژه برای افزایش ضریب امنیت خودروها تعیین شده و سایر کانال‌ها به کاربردهای خاصی اختصاص می‌یابند [۴].

شبکه‌های بین خودرویی هوشمند در ایجاد سامانهٔ حمل و نقل هوشمند بسیار مؤثر است که نمونه‌ای از کاربرد هوش مصنوعی در خودروها هستند. در شبکه‌های بین خودرویی هر خودرو مانند یک گره در شبکه عمل می‌کند. این گره‌ها می‌توانند با یکدیگر همکاری کنند تا کارایی شبکه افزایش یابد؛ درواقع شبکه‌های اقتضایی خودرویی نوعی از شبکهٔ اقتضاعی هستند که زیرساختار ثابتی نداشته و برای انجام عملیات و توابع شبکه همچون مسیریابی بسته و مدیریت شبکه به خودروهای شبکه وابسته هستند. به عبارتی، شبکهٔ اقتضایی خودرویی یک فناوری ارتباطات داده‌ای مبتنی بر بی‌سیم با سرعت بالا برای ارتباطات بین خودرویی از جمله ارتباط خودرو با خودرو (V2V)[5] و ارتباط خودرو با زیرساخت (V2I)[6] است [۴]. از خدمات رایج این فناوری می‌توان خدمات ایمنی جاده‌ای، مدیریت ترافیک و خدمات اطلاعات سرگرمی را نام برد. در خدمات اطلاعات سرگرمی از شبکه VANET انتظار می‌رود که انتقال داده‌های چندرسانه‌ای و دسترسی به اینترنت را پشتیبانی کند [۵].

[1] Wide area network
[2] Data plane
[3] software-defined vehicular network
[4] Dedicated Short-Range Communication
[5] Vehicle-to-Vehicle
[6] Vehicle-to-Infrastructure

ارتباطات در شبکه‌های VANET توسط رسانه‌های بی‌سیم انجام می‌شود. انواع مختلفی از رابط‌های هوایی، پروتکل‌های ارتباطی برای این معماری پیشنهاد شده است. در این معماری انواع مختلفی از فناوری‌های ارتباطاتی از جمله Wimax[1], GSM[2] و GNSS[3] برای برقراری ارتباط خودرو با خودرو(V2V)، خودرو با زیرساخت (V2I) و زیرساخت با زیرساخت(I2I)[4] مورد استفاده قرار می‌گیرند [۶]. اجزای اصلی معماری شبکه‌های اقتضایی خودرویی در شکل (۱) نشان داده است که در ادامه معرفی می‌شوند.



شکل (۱): معماری شبکه VANET [۸]

- **واحد بخش جاده‌ای RSU:**

RSU[5]ها دستگاه‌های فیزیکی هستند که به‌صورت دائمی در یک سمت جاده‌ای یا ایستگاه پارکینگ قرار داده می‌شوند. این دستگاه‌ها به منابع اینترنتی متصل شده و زمینه ارتباطات بین وسایل نقلیه را فراهم می‌آورند. RSUها به‌منظور ارائه خدماتی به میزبانی یک برنامه، مورد استفاده قرار می‌گیرند و OBU[6]ها از این خدمت برای اجرای برنامه استفاده می‌کنند [۶].

- **واحد تابلو OBU:**

واحد OBU به یک رابط کاربری و دستگاه شبکه متصل شده است که امکان ارتباطات بی‌سیم کوتاه‌برد مبتنی بر فناوری رادیویی را فراهم می‌کند و برای تبادل اطلاعات با سایر OBUها و RSUها استفاده می‌شود. این بخش شامل منابع پردازنده فرامین و حافظه است که برای خواندن یا نوشتن اطلاعاتی که بعداً به RSU یا سایر وسایل نقلیه منتقل خواهد شد، مورد استفاده قرار می‌گیرد.

- **بخش برنامه‌های کاربردی AU:**

این بخش در داخل وسیله نقلیه تعبیه شده و حاوی یک برنامه یا رابط کاربری است که برای ایجاد قابلیت ارتباطی با بخش OBU استفاده می‌شود. ارتباطات AU[7] به‌کمک بخش OBU انجام می‌شود. برای این منظور بخش برنامه کاربردی از طریق ارتباطات بی‌سیم یا اتصالات سیمی با OBU ارتباط برقرار می‌کند [۷].

۳- چالش‌ها و تهدیدهای امنیتی در VANET

در میان چالش‌های شبکه اقتضایی خودرویی، مسأله امنیت این شبکه‌ها کمتر مورد توجه قرار گرفته شده است. اطمینان از صحت و عدم تغییر داده‌های مبادله‌شده در شبکهٔ اقتضایی خودرویی بسیار مهم است؛ زیرا این داده‌ها، اطلاعات حیاتی زندگی را شامل می‌شوند. تضمین امنیت این شبکه‌ها به‌دلیل عدم زیرساخت، تحرک بالا، اندازهٔ شبکه و وابستگی جغرافیایی بسیار دشوارتر از سایر شبکه‌ها است. چالش‌های امنیتی بایستی در هنگام طراحی معماری، الگوریتم‌های رمزنگاری، پروتکل‌های امنیتی مورد توجه قرار گیرند. برخی از چالش‌های امنیتی در شبکه‌های اقتضایی خودرویی در ادامه بیان می‌شود [۹].

- **محدودیت زمانی:**

در شبکه‌های اقتضایی خودرویی تأخیر زمانی بسیار حائز اهمیت است. در این شبکه، پیام‌ها بایستی با تأخیر زمانی بسیار کمی به گیرنده تحویل داده شوند. برای رسیدن به وضعیت ایده‌آل بایستی الگوریتم‌های رمزنگاری سریع استفاده شده و احراز هویت و تأیید تصدیق پیام به‌صورت بلادرنگ انجام گیرد.

- **مسئولیت پایداری داده[8]:**

در این شبکه حتی اگر گره‌ای تأیید اعتبار شود؛ می‌تواند اقدامات مخربی را در شبکه انجام دهد. این گره‌های آلوده ممکن است از انتقال داده‌های دریافتی از سایر گره‌ها اجتناب کند و به این ترتیب موجب صدمه به شبکه شود. برای جلوگیری از این مشکل، بایستی سازوکارهای مناسبی را پیش‌بینی کرد.

- **سطح تحمل‌پذیری خطا:**

اطلاعات در شبکه اقتضایی خودرویی حیاتی هستند و بایستی در زمان بسیار اندکی اقدامات انجام شود. برخی از پروتکل‌ها براساس احتمالات طراحی شده‌اند. خطای کوچک در این الگوریتم‌های احتمالی ممکن است منجر به تصادفات بسیار شدید شود.

[1] Worldwide Interoperability for Microwave Access
[2] Global System for Mobile communications
[3] Global Navigation Satellite System
[4] Infrastructure to Infrastructure

[5] Road Side Unit
[6] On-Board Unit
[7] Application Unit
[8] Data Consistency Liability

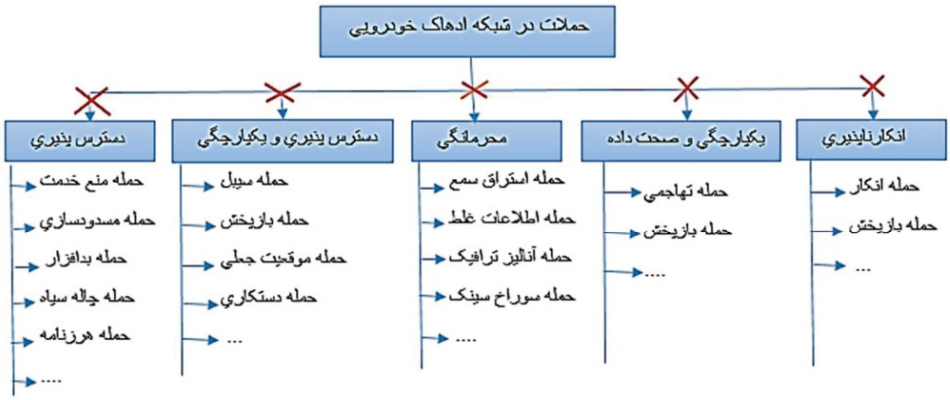
• **توزیع کلید رمزنگاری:**

تمامی سازوکارهای امنیتی انجام‌شده در شبکه اقتضایی خودرویی وابسته به کلید رمزنگاری هستند. در این شبکه‌ها هر پیام با کلید، رمزنگاری شده و در سمت گیرنده با همان کلید یا کلید خصوصی رمزگشایی می‌شود. یکی از چالش‌های عمده در طراحی پروتکل‌های امنیتی این شبکه‌ها نحوه توزیع کلید بین اجزای شبکه است.

• **پیچیدگی الگوریتم‌های امنیتی:**

پروتکل‌های امنیتی فعلی از جمله SSL/TLS[1]، DTLS[2] و WTLS[3] به‌طورمعمول از رمزنگاری کلید عمومی مبتنی بر RSA[4] استفاده می‌کنند. الگوریتم RSA از تقسیم عدد صحیح در نخستین مقدار بزرگ حاصل می‌شود که این الگوریتم NP سخت است. بنابراین، رمزنگاری پیامی که از RSA استفاده می‌کند، خیلی وقت‌گیر و پیچیده خواهد بود [۹]. در شبکه‌های اقتضایی خودرویی بایستی نیازهای اساسی امنیتی از جمله احراز هویت، یک‌پارچگی، محرمانگی، دسترس‌پذیری، نبود انکار و حریم خصوصی تأمین شود. در چنین شبکه‌هایی برآورده ساختن این الزامات به‌دلیل تحرک بالای گره‌ها، اتصالات متناوب بین گره‌ها و وضعیت‌های غیر قابل اطمینان کانال‌ها بسیار دشوار است [۱۰].

احراز هویت نمایان‌گر نخستین قدم به سمت امنیت شبکه‌های اقتضایی خودرویی است. در این شبکه‌ها بایستی همه RSUها و وسایل نقلیه در یک مرجع معتبر(TA)[5] ثبت نام کرده و گواهی تصدیق را دریافت کنند. هر وسیله نقلیه در ابتدا پیام را امضای دیجیتال کرده و ارسال می‌کند. گیرنده با بررسی امضای پیام به صحت پیام دریافتی و هویت فرستنده آگاهی می‌یابد. با توجه به اینکه TA در هر زمانی، موقعیت خاص هر کاربری را خواهد داشت؛ این موضوع یک ریسک حریم خصوصی محسوب می‌شود. درکل برای پنهان‌ماندن هویت خودرو و جلوگیری از ردیابی آن، طرح احراز هویت نام مستعار و طرح مبتنی بر امضای گروه پیشنهاد شده است. با وجود این‌که این طرح‌ها می‌توانند سطح حریم خصوصی را افزایش دهند، ولی به‌دلیل هزینه‌های محاسباتی بالا برای تأیید امضا، ممکن است بر روی دسترس‌پذیری تأثیر بگذارند. دست‌کاری یا تعلیق پیام در شبکه، اصل یک‌پارچگی امنیت داده‌ای را نقض می‌کند. اگر تغییرات داده‌ای با هدف محوکردن اثر عمل یا عدم شناسایی راننده انجام گیرد، اصل عدم انکار را زیر سؤال خواهد برد [۱۱]. در شبکه‌های اقتضایی خودرویی، وسایل نقلیه با اعتماد به پیام‌های مبادله‌شده تصمیم‌گیری کرده و اقدامات لحظه‌ای انجام می‌دهند. مهاجم با تغییر پیام یا ارسال داده‌های جعلی می‌تواند در چندین مورد، امنیت را تهدید کند. در شکل (۲) برخی از حملات اصلی در شبکه‌های اقتضایی خودرویی یاد شده است. با وجود روش‌های ارائه‌شده برای مقابله با این حملات، شبکه‌های اقتضایی خودرویی هنوز هم شبکه‌های ایمن محسوب نمی‌شوند. بنابراین؛ نیاز به طراحی رویکردهای جدیدی است که بتواند با حفظ الزامات امنیتی شبکه را از حملات محفوظ بدارد.



(شکل-۲): حملات محتمل در معماری شبکه VANET [۱۲]

۴- شبکه‌های نرم‌افزارمحور

شبکه مبتنی بر نرم‌افزار یک معماری نوظهوری است که بر اساس ایده جداسازی منطق نرم‌افزاری بستر کنترلی از بستر سخت‌افزاری انتقال داده‌ها شکل گرفته است [۱۳]. جداسازی بخش داده‌ای از بخش کنترل شبکه، برنامه‌های کاربردی و کنترل شبکه را برنامه‌پذیر می‌کند [۱۴]. همچنین ماشین‌های مجازی و زیرساخت شبکه را قادر به تعریف و ارائه انواع

[1] Transport Layer Security/ Secure Sockets Layer
[2] Datagram Transport Layer Security
[3] Wireless Transport Layer Security
[4] Rivest–Shamir–Adleman
[5] Trusted Authority

خدمات جدید می‌سازد و امکان ارتباط با طیف جدیدی از برنامه‌های کاربردی برای انعطاف‌پذیری بیشتر شبکه و دسترسی گسترده‌تر به داده‌های ردوبدل شده را فراهم می‌کند [۱۵]. مطابق شکل (۳) معماری شبکه‌های مبتنی بر نرم‌افزار را می‌توان به سه بخش لایه انتقال، لایه کنترل و لایه برنامه‌های کاربردی طبقه‌بندی کرد.

۴-۱- لایهٔ انتقال (زیرساخت) :

لایهٔ انتقال از تعداد زیادی سوئیچ‌های SDN تشکیل شده است که از طریق رسانه‌های بی‌سیم یا سیمی به‌صورت فیزیکی به هم‌دیگر متصل شده‌اند. سوئیچ SDN یک دستگاه ساده است که مسئول انتقال بسته‌های شبکه است. اغلب سوئیچ‌ها چندین جدول جریان دارند که به‌صورت خط لوله‌ای هستند. جدول جریان هر سوئیچ شامل هزاران قانون برای تنظیمات انتقالات است. گفتنی است که قوانین انتقال موجود در جداول جریان توسط خود سوئیچ‌ها تولید نمی‌شوند؛ بلکه توسط کنترل‌کننده از لایه کنترل به این لایه اعمال می‌شود. هر قانون موجود در جدول جریان سوئیچ از فیلدهای فراداده، کنش، شمارشگر و الگو ساخته شده است. فیلد فراداده در صورت وجود بیش از یک جدول، به‌منظور انجام فرآیند تطبیق بسته‌ها امکان حمل اطلاعات را از جدولی به جدول دیگر را فراهم می‌کند. فیلد الگو، مجموعه‌ای از مقادیر فیلدهای سرآیند بسته‌ها است که الگوی جریان را تعریف می‌کنند. در شبکه مبتنی بر نرم‌افزار هر بسته ورودی به سوئیچ با همه قوانین موجود در جداول جریان سوئیچ بررسی می‌شود. اگر تطبیقی با قوانین موجود در جداول یافت شد، کنش به‌روزرسانی می‌شود [۱۶]. شمارش‌گرها هرگز سرریز ندارند و شمارش‌گر هر جدول، شمارش‌گر هر صف را شامل می‌شوند. کنترل‌کننده از اطلاعات و آمار این شمارش‌گرها برای موارد مختلف استفاده می‌کند.

اگر بستهٔ ورودی، فیلدی برای مطابقت با قوانین موجود در جدول جریان نداشت، بسته به‌عنوان بسته نامعتبر و یا غیرقانونی شناخته شده و حذف می‌شود. هم‌چنین اگر تطبیقی بین بسته ورودی و قوانین جدول جریان یافت نشد، بسته به‌عنوان ورودی جدید به کنترل‌کننده ارسال خواهد شد. بسته می‌تواند به‌صورت کامل به کنترل‌کننده ارسال و یا می‌تواند در سوئیچ بافر شده و فقط سرآیند آن به کنترل‌کننده ارسال شود. هنگام ارسال بسته به کنترل‌کننده، بسته کپسوله‌شده و به‌عنوان پیام packet- in مشخص می‌شود. کنترل‌کننده با توجه به طول بسته، اولویت‌ها و سایر عوامل، بسته‌ها را پردازش می‌کند؛ سپس کنش‌های لازم در مواجهه با این بسته‌ها را که می‌تواند انتقال، حذف، اضافه‌کردن در صف، اصلاح و تغییر فیلد باشد، از طریق پیام packet-out به سوئیچ‌ها ارسال می‌کند [۱۷].

۴-۲- لایه کنترل:

لایه کنترل، کل شبکه را مدیریت و کنترل می‌کند. کنترل‌کننده، یک گره شبکه‌ای است که ویژگی مدیریت و کنترل شبکه در آن پیاده‌سازی شده و به طور کلی از دستگاه‌های فیزیکی با نرم‌افزارهای اختصاصی مجزا است. در واقع کنترل‌کننده به‌عنوان مغز معماری شبکه‌های مبتنی بر نرم‌افزار است که دید کلی از تمام هم‌بندی‌های شبکه از جمله سوئیچ‌ها و پیوندها را دارد. پروتکل‌های مسیریابی مختلفی از جمله OSPF[1], BGP[2] در کنترل‌کننده شبکه‌های مبتنی بر نرم‌افزار اجرا می‌شوند تا همه انتقالات داده‌ای در لایه انتقال بر اساس دستورالعمل‌های مقررشده توسط کنترل‌کننده انجام شود [۱۶].

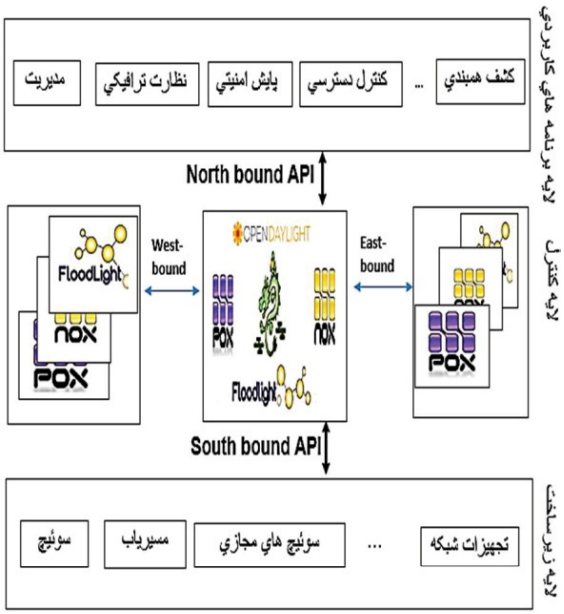
لایه کنترل از طریق واسط رابط جنوبی[3] با سوئیچ‌های لایه انتقال ارتباط برقرار می‌کند. امروزه اغلب معماری‌های شبکه‌های مبتنی بر نرم‌افزار با کنترل‌کننده‌هایی از جمله FloodLight ، Nox و OpenDayLight پیاده‌سازی می‌شوند و به‌منظور بهبود مقیاس‌پذیری و دسترس‌پذیری منابع از چندین کنترل‌کننده توزیع‌شده پشتیبانی می‌کنند. در این معماری‌ها هر کنترل‌کننده، مسئول بخشی از سوئیچ‌های لایه انتقال است. به‌منظور حفظ انسجام وضعیت شبکه و هماهنگی، هر کنترل‌کننده منحصربه‌فرد می‌تواند با سایر کنترل‌کننده‌های شبکه از طریق واسط رابط شرقی-غربی[4] ارتباط برقرار کند [۱۸].

۴-۳- لایهٔ برنامه‌های کاربردی

لایهٔ برنامه‌های کاربردی به اپراتورهای شبکه امکان پاسخ سریع به نیازهای کسب و کار را فراهم می‌کند. نرم‌افزارهای کاربردی نوآورانه در قسمت بالای کنترل‌کننده قرار می‌گیرند تا نیازهای مختلف از جمله مجازی‌سازی، کشف هم‌بندی، نظارت ترافیک، افزایش امنیت و تعادل بار را تأمین کند. لایه برنامه کاربردی از طریق واسط رابط شمالی[5] با لایه کنترل ارتباط برقرار می‌کند. لایه کنترل یک انتزاعی از منابع فیزیکی شبکه را برای لایه کاربردی فراهم می‌کند. به بیان دیگر

[1] Open Shortest Path First
[2] Border Gateway Protocol
[3] South-bound API
[4] East-West bound API
[5] North-bound API

اپراتورهای شبکه می‌توانند به جای تغییر پیکربندی سوئیچ‌های فیزیکی از برنامه‌نویسی نرم‌افزاری مرکزی کنترل‌کننده‌های شبکه‌های مبتنی بر نرم‌افزار برای تغییر مسیر داده‌ای بسته‌ها استفاده کنند.



(شکل-۳): معماری شبکه SDN [۱۹]

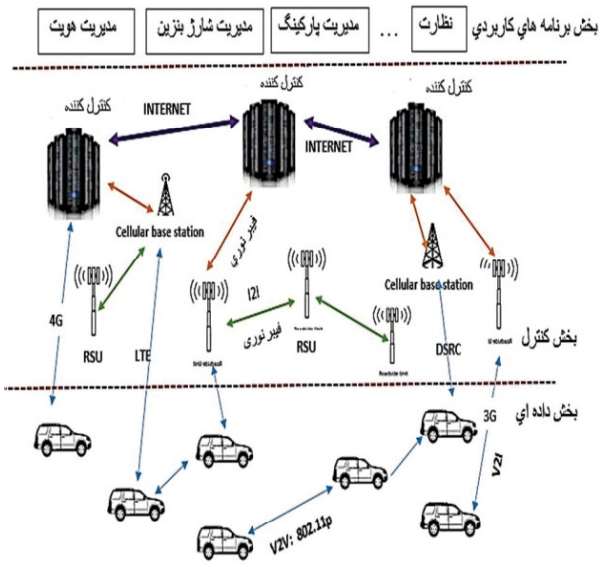
۵- سازگاری شبکه‌های نرم‌افزارمحور با VANET

در شبکه‌های فعلی، امکان کنترل کامل بخش پیکربندی در شبکه وجود ندارد. معماری SDN یک فناوری نوظهوری است که قابلیت برنامه‌پذیری و کنترل‌پذیری را به شبکه‌ها می‌افزاید. این معماری در ابتدا برای شبکه‌های سیمی ارائه شده بود؛ اما در حال حاضر پژوهشگران در تلاش جهت ادغام این فناوری با شبکه‌های بی‌سیم هستند[5,20,21]. در مقاله [۵] مدلی برای یک‌پارچه‌سازی فناوری SDN با محیط شبکه اقتضایی خودرویی ارائه شده است. در این مدل مشکل انعطاف‌پذیری و مقیاس‌پذیری شبکه اقتضایی خودرویی به‌کمک معماری شبکه نرم‌افزارمحور حل شده است. این معماری، با ارائه مجموعه‌ای از خدمات جدید از جمله نظارت و مجازی‌سازی زیرساخت شبکه، ویژگی انعطاف‌پذیری را به بخش کنترل‌کننده شبکه اقتضایی خودرویی افزوده است. علاوه‌براین، حالت عملیاتی SDN شبکه اقتضایی خودرویی را قادر به سازگاری با تغییرات هم‌بندی شبکه می‌سازد [۲۲].

مدیریت شبکه‌های اقتضایی خودرویی به‌دلیل ماهیت بدون زیرساخت، بسیار دشوار است. روش جداسازی بخش کنترلی از بخش داده‌ای SDN راه را برای کنترل و مدیریت شبکه اقتضایی خودرویی هموارتر می‌سازد [۲۳]. در مدیریت شبکه به اشتراک‌گذاری کارآمد منابع در میان وسایل نقلیه امر مهمی است. کنترل‌کننده متمرکز معماری شبکه نرم‌افزارمحور، کنترل بر روی جریان داده‌ای و توان وسایل نقلیه را ارائه می‌دهد. با به‌کارگیری فناوری SDN می‌توان مدیریت شبکه را از طریق حذف ناسازگاری‌های تجهیزاتی، ارائه تغییرات پویا، پشتیبانی سطح بالا از پیکربندی شبکه، عیب‌یابی و عیب‌زدایی شبکه بهبود بخشید. این طرح همچنین با ارائه انتزاعی از شبکه‌های ناهمگن خودرویی در محیط بی‌سیم، هزینه‌های مؤثر اشتراک‌گذاری داده‌ای بین وسایل نقلیه را کاهش می‌دهد [۲۴].

۶- معماری شبکه‌های اقتضایی خودرویی تعریف‌شده با نرم‌افزار (SDVN)

ادغام فناوری SDN با شبکه‌های اقتضایی خودرویی موجب پیدایش معماری شبکه‌های اقتضایی خودرویی مبتنی بر نرم‌افزار شد. فناوری SDN از ناهم‌گونی رابط‌های بی‌سیم در معماری ارتباطات خودرویی به‌منظور محاسبات بهتر، ذخیره و بهره‌وری با هزینه کم پشتیبانی می‌کند [۲۴]. شکل (۴) معماری شبکه اقتضایی خودرویی تعریف‌شده با نرم‌افزار را نشان می‌دهد.



(شکل-۴): معماری شبکه SDVN

در معماری SDVN با جداسازی بخش کنترل از بخش داده‌ای، مغز شبکه به‌صورت منطقی در بخش کنترلی متمرکز شده و بخش داده‌ای برای انتقال اطلاعات استفاده می‌شود. با به‌کارگیری فناوری SDN در محیط شبکه اقتضایی خودرویی، می‌توان تداخلات را کاهش داده و منابع بی‌سیم شبکه را بهبود

بخشید. بنابراین، می‌توان محیط انطباق‌پذیر، مقیاس‌پذیر و همه‌کاره را در محیط VANET پدید آورد [۲۵]. مطابق شکل (۴) معماری SDVN برای ارتباط بین موجودیت‌های شبکه از فناوری‌های مختلف استفاده می‌کند. در این معماری ارتباطات خودرو با خودرو (V2V) و ارتباطات خودرو با RSU به‌ترتیب از طریق 802.11p و LTE/4G[1] حاصل می‌شود [۲۴]. همچنین وسایل نقلیه خارج از محدودهٔ پوشش نیز از طریق شبکه سلولی می‌توانند با ایستگاه پایه[2] ارتباط برقرار کنند. ارتباطات بین ایستگاه‌های پایه، کنترل‌کننده و RSU ها از طریق فیبر نوری سیمی انجام می‌شود [۱]. اجزای شبکه اقتضایی خودرویی تعریف‌شده با نرم‌افزار در ادامه معرفی می‌شود.

- **کنترل‌کننده SDN**

بخش کنترل‌کننده، یک هوش منطقی است که به‌صورت متمرکز در شبکهSDVN قرار گرفته و تمام موجودیت‌های شبکه را کنترل می‌کند [۲۵]. در شبکه اقتضایی خودرویی تعریف‌شده با نرم‌افزار، یادگیری هم‌بندی برای تصمیم‌گیری بسیار مهم است. کشف هم‌بندی شبکه و تغییرات پویای هم‌بندی توسط این بخش، کنترل می‌شود. هر گره بی‌سیم SDN یک پیام Beacon را به‌منظور دریافت و شناخت اطلاعات گره‌های همسایه ارسال می‌کند. اطلاعات گره‌های همسایه به‌صورت دوره‌ای در کنترل‌کننده به‌روزرسانی می‌شوند تا کنترل‌کننده از این اطلاعات برای ساخت گراف اتصال برای تصمیم‌گیری استفاده کند [۲۶].

- **گره‌های بی‌سیم SDN**

درواقع این بخش شامل تمام وسایل نقلیه‌ای هست که سیگنال‌های کنترلی را از بخش کنترل‌کننده SDN برای انجام اقدامات لازم دریافت می‌کنند. هر گره بی‌سیم SDN دارای یک عامل محلی[3] است. در مواقعی که ارتباط بین وسایل نقلیه با بخش کنترل‌کننده متمرکز دچار اختلال شود، عامل محلی از پروتکل‌های مسیریابی بدون زیرساخت ازجمله AODV،[5]DSDV،[6]OLSR،[7]GPPSR[4] برای انتخاب مسیر استفاده می‌کند.

- **RSU مبتنی بر SDN**

این بخش شامل عناصر ثابت بخش داده‌ای ازجمله RSUهایی هست که سیگنال‌های کنترلی را از بخش کنترل‌کننده دریافت می‌کنند [۲۵].

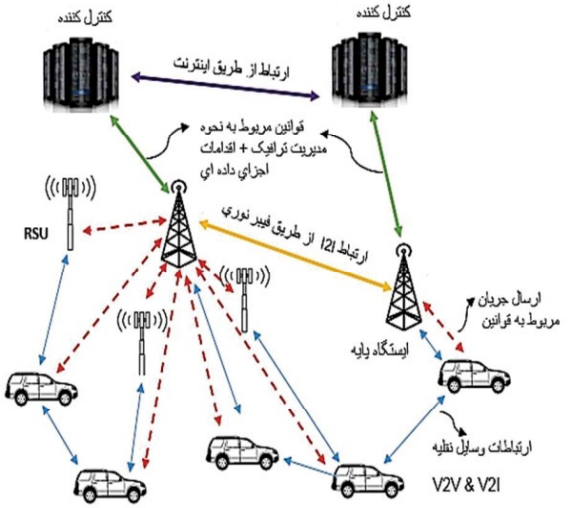
[1] Long-Term Evolution
[2] Cellular base station
[3] local agents
[4] Ad-hoc On Deman Distance Vector

۷- بررسی عملیاتی معماری SDVN

ایدهٔ اصلی معماری شبکه‌های نرم‌افزارمحور، جداسازی بخش داده‌ای از بخش کنترلی است. معماری SDVN بر اساس درجه کنترلی کنترل‌کنندهٔ شبکه نرم‌افزارمحور، به سه حالت عملیاتی زیر ارائه می‌شود:

۷-۱- حالت کنترل مرکزی

در این حالت عملیاتی، تمام عملیات مربوط به گره‌های بی‌سیم و RSUها توسط کنترل‌کننده SDN کنترل می‌شوند. کنترل‌کننده، قوانین مربوط به نحوه مدیریت ترافیک را به شبکه اعمال کرده و تمام اقدامات اجزای داده‌ای را نیز تعیین می‌کند [۹]. به بیان دیگر؛ حالت کنترل مرکزی رفتار مشابه با معماری شبکه‌های نرم‌افزار محور سیمی را دارد. با این حال، عدم اطمینان دسترس‌پذیری جزء مشکل ذاتی شبکه‌های بی‌سیم است. در این حالت عملیاتی نیز امکان قطع ارتباط بین گره‌های متحرک و کنترل‌کنندهٔ شبکه وجود دارد. بنابراین؛ معماری SDVN بایستی سازوکار بازیابی شکست را داشته باشد تا شبکه بتواند تا حد ممکن حتی با سطح عملکرد پایین پابرجا بماند [۵]. شکل (۵) حالت عملیاتی کنترل مرکزی را نشان می‌دهد.



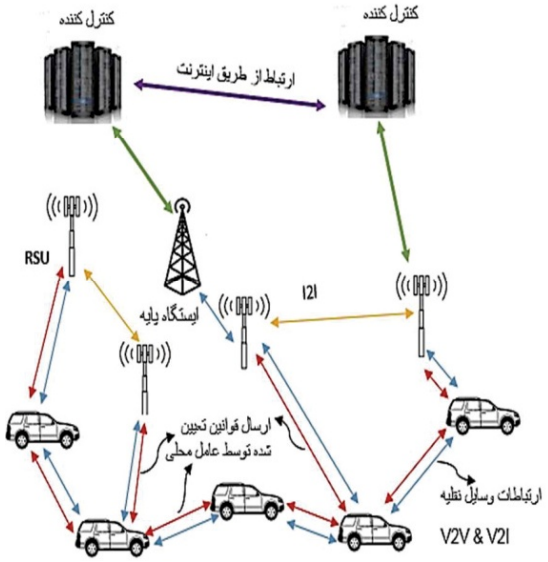
(شکل-۵): حالت عملیاتی کنترل مرکزی

۷-۲- حالت کنترل توزیع‌شده

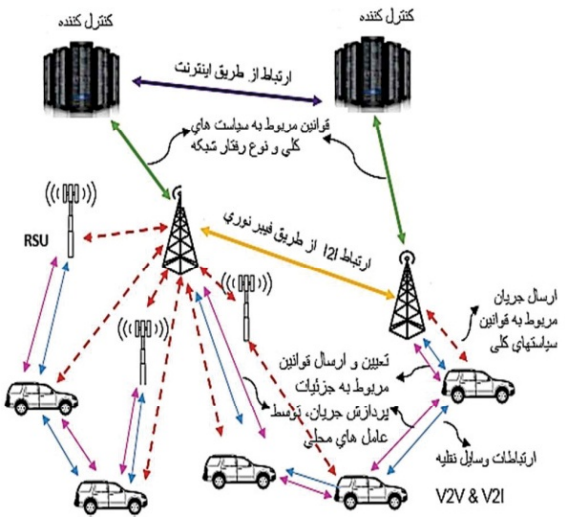
ماهیت این حالت کنترل عملیاتی در شبکه‌های توزیع‌شده خودسازمانده رایج است. طبق شکل (۶) در این حالت، در

[5] Destination Sequence Distance Vector
[6] Optimized link state routing
[7] Greedy Perimeter Stateless Routing

طول ارسال بسته، گره‌های بی‌سیم و RSUها بدون هیچ دستورالعملی از کنترل‌کننده، کار می‌کنند. در حالت عملیاتی توزیع شده، عامل‌های محلی روی هر گره بی‌سیم، اقدامات منحصر به فرد هر گره را کنترل می نماید[۹].



(شکل-۶): حالت عملیاتی کنترل توزیع شده



(شکل-۷): حالت عملیاتی کنترل ترکیبی

۷-۳- حالت کنترل ترکیبی

تمام حالت‌های عملیاتی یک سامانه که کنترل‌کننده SDN در آن تأثیر می‌گذارد، در حالت عملیاتی کنترل ترکیبی گنجانیده شده است. شکل (۷) حالت عملیاتی ترکیبی را نشان می‌دهد. در این مثال کنترل‌کننده، کنترل کاملی را بر شبکه داشته و از سوی دیگر، جزئیات پردازش بسته‌ها به عامل محلی واگذار شده است؛ بنابراین، ترافیک‌های کنترلی در بین تمامی عناصر منتقل می‌شود. به‌عنوان مثال، کنترل‌کننده، به جای ارسال تمامی قوانین جریان، تنها با ارسال سیاست‌ها، رفتار شبکه را مشخص می‌کند. درحالی‌که گره‌های بی‌سیم و RSUها از عامل محلی برای انتقالات بسته و پردازش سطح جریان بهره می‌گیرند [۹].

۸- سرویس‌های ارائه‌شده توسط شبکه‌های SDVN

یک‌پارچه‌سازی شبکه اقتضایی خودرویی و شبکه نرم‌افزارمحور، بسیاری از نیازهای ایمنی و غیرایمنی شبکه را برآورده می‌سازد. دراین بخش چندین استفاده موردی از شبکه SDVN بیان می‌شود.

• مسیریابی مبتنی بر تأخیر

پروتکل‌های مسیریابی سنتی از جمله IGRP[1], RIP[2], BGP[3] قادر به پاسخ‌گویی کارآمد در شبکه‌های پویای اقتضایی خودرویی نیستند. در این شبکه‌ها سازوکاری مورد نیاز است که قادر به پاسخ‌گویی پویا نسبت به تأخیر زمانی و تخصیص منابع باشد. در شبکه SDVN هنگامی که پیوندهای مسیریاب دچار ازدحام شده و تأخیرات ترافیکی در طول مسیر افزایش می‌یابد؛ فناوری SDN می‌تواند تأخیر را به‌عنوان یک پارامتر متریک برای هر مسیر درون شبکه مطرح نماید. به این ترتیب، امکان پاسخ بلادرنگ را به تأخیرات پیوندهای اولویت‌بندی شده فراهم می‌آورد. بنابراین، برنامه‌هایی مانند ترافیک‌های صوتی، پیام‌های امنیتی، پیام‌های اورژانسی که تأخیر[4] و نوسانات تأخیر[5] کمتری نیاز دارند، می‌توانند مسیری با تأخیر کم را از طریق شبکه در اختیار بگیرند و پیام را به‌صورت بلادرنگ به مقصد هدایت کنند [۲۴].

• نظارت بر وضعیت جاده‌ای

ارتباطات مبتنی بر معماری SDN با دریافت اطلاعات از حس‌گرهای مختلف امکان نظارت بر وضعیت جاده‌ای، کنترل ازدحام ترافیکی و مدیریت پیام‌های اضطراری را فراهم می‌آورد. در این معماری، اطلاعات جمع‌آوری‌شده به‌صورت

[1] Interior Gateway Routing Protocol
[2] Routing Information Protocol
[3] Border Gateway Protocol
[4] Delay
[5] Jitter

بلادرنگ بین وسایل نقلیه و زیرساخت‌های ثابت مبادله می‌شوند. همچنین کنترل‌کننده SDN توسط مسیریاب‌ها به‌صورت دوره‌ای با پارامترهایی همچون تراکم، تأخیر، نوسانات تأخیر و نرخ فقدان بسته‌ها به‌روزرسانی می‌شوند. به این ترتیب ارتباطات مبتنی بر SDN موجب بهبود عملکرد شبکه‌ای می‌شود.

• مدیریت پهنای باند

شبکه‌های سنتی پویایی لازم را جهت ارائه امکانات شبکه‌ای تحت استانداردهای پهنای باند بر اساس تقاضا (BWOD)[1] را ندارند. امروزه ارتباطات بین خودرویی با توجه به رشد روزافزون اطلاعات و الزامات ارتباطاتی به پهنای باند بیشتری نیاز دارند. فناوری SDN امکان ارائه پهنای باند براساس تقاضا در محیط پویای VANET را فراهم می‌کند. ارائه‌دهندگان خدمات در ارتباطات مبتنی بر SDN به وسایل نقلیه اجازه می‌دهند که به‌صورت پویا میزان پهنای باند مصرفی خود را براساس نیازشان تغییر دهند و فقط هزینه را براساس میزان منابع مصرفی پرداخت کنند. ارتباطات براساس تقاضا توسط دستگاه‌های ارسال با برنامه‌های زمان‌بندی پهنای باند سازگار با کنترل‌کننده SDN برقرار می‌شوند. طراحان شبکه به‌راحتی می‌توانند از طریق رابط جنوبی کنترل‌کننده، پهنای باند به اشتراک گذاشته شده را کنترل کنند. هم‌چنین این نوع کنترل می‌تواند از طریق رابط شمالی جهت تهیه تجهیزات، سیاست‌های سامانه برای دسترسی به پهنای باند مورد نیاز یا تغییر سیاست‌های تضمین کیفیت به‌صورت بلادرنگ قابل دسترسی باشد.

• دستیار تغییر خط مسیر

سامانه‌های تغییر مسیر سنتی قادر به کمک در تغییر تک‌مسیری هستند. این سامانه‌ها چالش‌های زیادی از جمله شرایط جاده‌ای، تراکم ترافیک، سرعت و جهت خودرو را دارند. کنترل‌کننده SDN به‌دلیل داشتن دید کلی از اطلاعات سامانهٔ جاده‌ای قادر است، دستیار تغییر مسیر خودجهته را ایجاد کند. در این سامانه RSUها اطلاعات مورد نیاز مانند خط مسیر، سرعت، فضا و نقشه راه را به‌صورت موقتی ذخیره می‌کنند و هنگامی که خودرویی نیاز به تغییر مسیر داشت، بخش کنترلی درخواست تغییر مسیر را به RSUهای اطراف ارسال می‌کند. سپس کنترل‌کننده SDN براساس اطلاعات در دسترس RSUها در مورد نحوه تغییر مسیر تصمیم‌گیری می‌کند[۲۴].

• خدمات ایمنی

یکی از اهداف اصلی شبکه‌های اقتضایی خودرویی، ایمن‌سازی جاده از طریق ارتباطات V2V است. شبکه اقتضایی تعریف‌شده با نرم‌افزار، ایمنی جاده‌ای را در مقایسه با شبکه اقتضایی خودرویی بهبود می‌بخشد. در این شبکه، فناوری SDN می‌تواند ترافیک‌های خاص ازجمله پیام‌های امنیتی و اضطراری را از مسیر رزروشده هدایت کند. در این معماری رزرو کانال به‌صورت پویا انجام می‌گیرد [۵].

• مجازی‌سازی شبکه‌های بی‌سیم

با رشد چشم‌گیر ترافیک و خدمات بی‌سیم، ایده مجازی‌سازی محبوبیت خاصی پیدا کرده است. مجازی‌سازی، کل شبکه را به یک شبکه انتزاعی منطقی با زیرساخت‌ها و منابع مشترک تبدیل می‌کند. این روش امکان به اشتراک‌گذاری طیفی، مجازی‌سازی رابط‌ها، مجازی‌سازی دستگاه‌های انتقال و ایزوله‌سازی کاربران را فراهم می‌کند. در شبکه‌های SDVN می‌توان روش مجازی‌سازی را در ارتباطات خودرویی با کانال‌ها و فرکانس‌های مختلف اعمال کرد. در این شبکه‌ها، با توجه به ایزوله‌بودن خودروها و RSU ها می‌توان شبکه بی‌سیم مجازی را با بخش‌بندی[2] مؤثر در کل شبکه خودرویی ایجاد کرد. همچین ارتباطات خودرویی می‌توانند با استفاده از بخش‌بندی زمانی برای تقسیم فرکانس قائم(OFDM)[3] یک شبکه مجازی بی‌سیم را در هر زمان فراهم کنند. مجازی‌سازی عملکرد شبکه (NVF)[4] امکان ارائه خدمات چندرسانه‌ای و نظارت بر رویدادهای بلادرنگ را مهیا می‌سازد [۵].

• جریان ویدئویی

برنامه‌های سرگرمی شبکه‌های VANET شامل به اشتراک‌گذاری چندرسانه‌ای و ویدئو کنفرانس است. با توجه به تحرک بالای هم‌بندی این شبکه‌ها، می‌توان از فناوری SDN در جهت بهبود کیفیت ویدئو مورد آزمایش(QOE)[5] در شبکه VANET استفاده نمود. کنترل‌کننده SDN به دلیل دید کلی نسبت به تمام مسیرها، خودروها و RSUها می‌تواند بهترین مسیر جریان ویدئویی را با اعمال الگوریتم کوتاه ترین مسیر بر روی پروتکل (MPLS)[6] جستجو کند. همچنین کنترل‌کننده در نظارت پهنای باند در دسترس، پیوندهای خراب، نوسانات تأخیرات و به‌روزرسانی مسیرهای انتقال کمک می‌کند. بدین ترتیب این فناوری، پیکربندی مجدد بهینه‌ای را برای تغییرات همبندی ارائه کرده و QOE را تضمین می‌کند[۲۴].

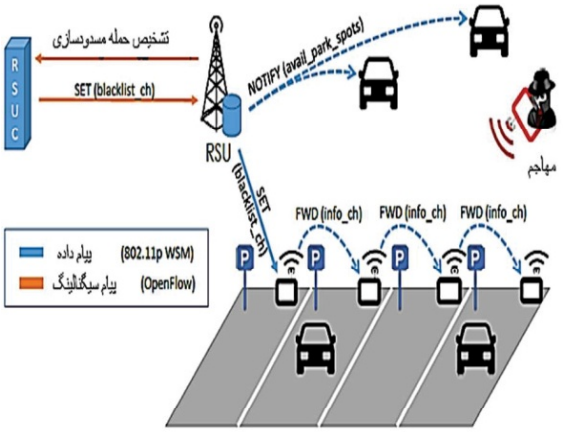
[1] Band Width-On-Demand
[2] Slice
[3] Orthogonal Frequency Division MultiPlexing
[4] Network Virtualization Function
[5] Quality-Of-Experience
[6] Multi Protocol Label Switching

۹- بهبود امنیت شبکه‌های بین خودرویی در SDVN

این بخش بر مزایای امنیتی شبکه اقتضایی خودرویی تعریف شده با نرم‌افزار تمرکز دارد. ما در این بخش ویژگی‌های نظارتی و برنامه‌پذیری فناوری نرم‌افزارمحور را که موجب ایجاد اقدامات جدید علیه حملات کلاسیک در شبکه‌های اقتضایی خودرویی سنتی می‌شود، بررسی می‌کنیم.

۹-۱- مقابله با حملات محتمل در پارکینگ هوشمند

پارکینگ هوشمند بر ارتباطات بین حس‌گرهای هوشمند مستقر در نقاط مختلف پارکینگ و دروازه[1] با استفاده از فناوری‌هایLoRa,ZigBee,Wi-Fi متکی است. این سامانه در معرض طیف وسیعی از حملات قرار دارد. ما در ادامه حملات مسدودسازی[2] و استراق سمع[3] که به‌ترتیب در دسترس‌پذیری سرویس و محرمانگی/حریم خصوصی اطلاعات را مورد هدف قرار می‌دهند، شرح داده و اقدامات مقابله‌ای علیه این حملات توسط فناوری نرم‌افزارمحور را بیان خواهیم کرد.



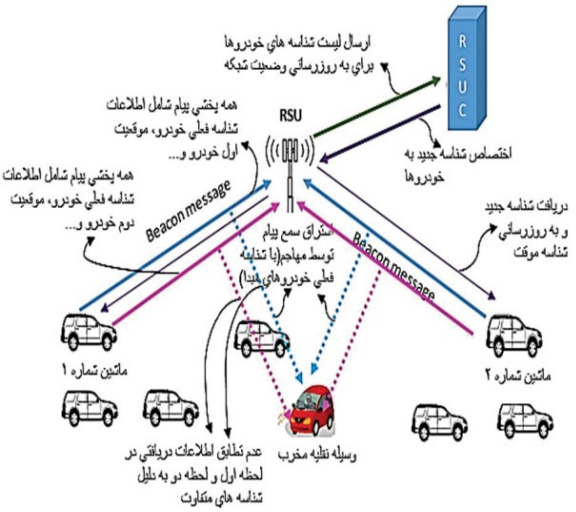
(شکل-۸): حملات مسدودسازی بر روی پارکینگ هوشمند [۱۱]

با توجه به ماهیت همه پخشی[4] ارتباطات بی‌سیم در شبکه‌های اقتضایی خودرویی، مطابق شکل (۸) مهاجم می‌تواند با استفاده از فرستنده‌های قوی‌تر موجب مسدودسازی کانال‌های ارتباطی شود. این حمله از پذیرش داده‌های حساس توسط دروازه‌های شبکه‌های حس‌گر بی‌سیم جلوگیری می‌کند و بدین ترتیب از مخابره اطلاعات در مورد نقاط قابل دسترس پارکینگ به RSUها جلوگیری می‌کند. بنابراین، در چنین شرایطی RSUها قادر به هدایت وسایل نقلیه درخواست‌دهنده پارکینگ نخواهند بود.

در شبکه‌های SDVN قابلیت هوشمندی و برنامه‌پذیری فناوری نرم‌افزارمحور می‌تواند مشکل قطع سرویس را در حمله مسدودسازی حل کند. در شبکه اقتضایی خودرویی تعریف‌شده با نرم‌افزار، RSUها اطلاعات دقیقی را در مورد کیفیت کانال‌های مورد استفاده در منطقه پارکینگ هوشمند جمع‌آوری کرده و گزارش‌های مربوطه را از طریق پیام‌های سیگنالینگ ویژه (تشخیص مسدودسازی) به RSUC[5] ارسال می‌کنند. RSUC فهرستی از کانال‌های خراب را ایجاد کرده و این فهرست از طریق RSUها به حس‌گرهای مستقر در منطقه پارکینگ ارسال می‌شود. علاوه‌براین، RSUC با ارائه طرح آموزشی جستجو می‌تواند حس‌گرها را در مورد چگونگی انجام جستجو کانال به‌منظور کاهش تداخلات سنگین یاری رساند. با توجه به اینکه کنترل‌کننده SDN برای داشتن دید کلی از شبکه، اطلاعاتی را در مورد موقعیت وسایل نقلیه به دست می‌آورد. یکی از نگرانی‌های عمده در پارکینگ هوشمند، اطمینان از حریم خصوصی رانندگان است. یک وسیله نقلیه مخرب می‌تواند با رانندگی در منطقه پارکینگ، اطلاعاتی در مورد وسایل نقلیه پارک‌شده یا در حال پارک را جمع‌آوری، ذخیره، تجزیه و تحلیل کند. این حمله به‌صورت کلاسیک به‌عنوان حمله استراق سمع شناخته می شود. هدف اصلی از این حمله، به‌دست‌آوردن اطلاعات مربوط به قربانی به‌منظور بازسازی عادات یا مسیرهای رانندگی وی از طریق تجزیه و تحلیل beacon های شخص قربانی است.

شکل (۹) یک سناریوی حملهٔ استراق را سمع در پارکینگ هوشمند نشان می‌دهد. در این سناریو وسایل نقلیه ۱ و ۲ با فرکانس مشخصی Beaconها را به‌صورت همه‌پخشی به RSUها ارسال می‌کنند. این پیام‌ها توسط مهاجم نیز استراق سمع می‌شود. در شبکه SDVN برای حل این مشکل از ID(شناسه موقت) استفاده می‌شود. در این سامانه RSUها فهرستی را از شناسه‌های موقت ایجاد کرده و به RSUC ارسال می‌کنند. طبق سیاست‌های اعمال‌شده در کنترل‌کننده، شناسه‌ها به وسایل نقلیه تخصیص داده می‌شوند. بدین ترتیب، هنگامی که وسایل نقلیه Beaconها را با شناسه موقت خود همه‌پخشی مجدد بکنند، مهاجم قادر به ارتباط دادن اطلاعات گذشته با اطلاعات جاری نخواهد بود. بدین صورت ردیابی تمام حرکات وسایل نقلیه غیرممکن شده و ریسک حملات تک‌هدف از بین می‌رود [۱۱].

[1] Gateway
[2] Jamming
[3] Eaves dropping
[4] BroodCast
[5] RSU Controller



(شکل-۹): حملات استراق سمع در منطقه پارکینگ هوشمند

۹-۲- مقابله با حملات احتمالی به خدمات اضطراری

اطلاع‌رسانی اضطراری یکی از سرویس‌های حیاتی در شبکه‌های اقتضایی خودرویی است که به معیارهای امنیتی ویژه‌ای نیاز دارد. مهاجم می‌تواند بدون مختل‌سازی دسترسی شبکه، درخواست‌های اضطراری را حذف کرده و مانع رسیدن تیم‌های نجات یا ایجاد هشدار شود. حمله سوراخ سینک[1] مثالی از این نوع حملات است که مهاجم، همه درخواست‌های اضطراری را از وسایل نقلیه یک منطقه دریافت کرده و حذف می‌کند. بدین ترتیب مانع از انتقال پیام‌های اضطراری و درخواست تخصیص منابع ویژه می‌شود.

راه حل این مشکل تکیه بر فناوری SDN است تا بتوان گره‌های واسط معتبر را برای ارتباطات V2V انتخاب کرد. در شبکه SDVN هنگامی که یک وسیله نقلیه بایستی به‌عنوان گره واسط ارتباطی V2V عمل کند؛ کنترل‌کننده یک مجوز مبتنی بر اعتماد را برای گره واسط طراحی و سپس کنترل‌کننده اعتبار این گره را توسط نظرسنجی از سایر گره‌ها محاسبه می‌کند. فناوری شبکه‌های نرم‌افزارمحور قادر است، معیارهای امنیتی را تقویت کند. SDN در شرایط اضطراری می‌تواند مقادیر منابع تخصیص‌یافته را به‌صورت پویا تغییر داده و جریان اضطراری را به‌صورت کارآمد و ایمن هدایت کند.

۹-۳- مقابله با حملات منع خدمت

مهاجم در شبکه اقتضایی خودرویی سنتی می‌تواند با کنترل زیرمجموعه‌ای از وسایل نقلیه آلوده‌شده توسط بدافزار، حمله منع خدمت توزیع‌شده را نیز راه‌اندازی کند. در این حمله هر گره آلوده، درخواست‌های اضطراری جعلی را با هدف سربار کانال و نقض اصل دسترس‌پذیری در شبکه ارسال می‌کند. در این نوع حمله SDN می‌تواند منابع ترافیک مخرب را شناسایی کرده و سپس با آموزش بخش داده‌ای، بسته‌های مربوط به جریان‌های جعلی را دور بریزد. علاوه‌براین، طرح مدیریت اعتبار وسایل نقلیه با استفاده از الگوریتم توافقی مشترک می‌تواند در شناسایی کاربران مخرب و حذف آنها از شبکه مفید واقع شود.

۹-۴- مقابله با حملات اطلاعات غلط

یک وسیله نقلیه مخرب می‌تواند یک تصادف کذب را در یک موقعیت جغرافیایی خاص با هدف منافع شخصی گزارش دهد تا سایر وسایل نقلیه به مسیری دیگری هدایت شوند. این نوع حمله با عنوان حمله اطلاعات غلط[2] شناخته می‌شود. فناوری SDN می‌تواند با استفاده از رویکرد توافقی جمعی این نوع حملات را در شبکه‌های SDVN خنثی کند. کنترل‌کننده، پس از دریافت سیگنال‌های پیام اضطراری در یک منطقه خاص، اطلاعات مربوطه را از سایر وسایل نقلیه موجود در آن محیط جغرافیایی جمع‌آوری می‌کند. کنترل‌کننده درصورت تناقض اطلاعات جمع‌آوری‌شده با اطلاعات گزارش‌شده توسط کاربر مخرب احتمالی، دستور حذف بسته‌های جریان مربوط به کاربر مخرب را به‌صورت یک قانون به RSUها ارسال می‌کند [۱۱].

۱۰- چالش‌های محتمل در شبکه‌های SDVN

فناوری SDN با ارائه راه‌حل‌هایی برخی از مشکلات موجود در سامانهٔ شبکه‌های اقتضایی خودرویی را برطرف می‌کند. با این حال، با پیاده‌سازی شبکه اقتضایی خودرویی مبتنی بر نرم‌افزارمحور مسایل جدیدی از جمله کنترل ترافیک پویا، تأمین پهنای باند بالا برای ارتباطات بین بخش‌های مختلف مطرح می‌شود. ما در این بخش به بررسی چالش‌های محتمل در شبکه‌های SDVN می‌پردازیم.

۱۰-۱- ارتباطات SDN با شبکه‌های سنتی

سامانه‌های مبتنی بر SDN، سیاست‌های خاصی را برای ارتباطات داده‌ای دارند؛ اما ساختار شبکه‌های سنتی به‌طورکامل متفاوتند. توسعه سامانه‌های مبتنی بر SDN در کنار شبکه‌های سنتی مسایل جدیدی را به همراه خواهد داشت. با توجه به اینکه شبکه‌های سنتی از برنامه‌های

[1] Sink hole

[2] Bogus Information

پیچیده‌ای پشتیبانی می‌کنند؛ شبکه‌های اقتضایی خودرویی مبتنی بر SDN به‌منظور ایجاد اطمینان تمام عملیات، بایستی با شبکه‌های سنتی در ارتباط باشند. راه‌حل بالقوه این مشکل، طراحی پروتکل مسیریابی جدیدی است که متناسب با ساختار این شبکه‌ها باشد [۶].

۱۰-۲- مسایل امنیتی

بیشتر پژوهش‌ها بر روی توسعه سامانه شبکه‌های اقتضایی خودرویی مبتنی بر نرم‌افزار متمرکز شده و توجه کمتری به مسایل امنیتی این ساختار شده است. بدون تضمین امنیت، سامانه در معرض حملات مهاجمان قرار خواهد گرفت. بنابراین، توسعه این سامانه نیازمند طراحی سازوکار امنیتی مؤثر و حفاظت از تهدیدهای داخلی و خارجی است.

۱۰-۳- چالش‌های مرتبط با دسترس‌پذیری خدمات

در شبکه‌های اقتضایی خورویی سنتی هنگامی که گره‌ای خراب می‌شود، به‌منظور حفاظت و دسترس‌پذیری خدمات، ترافیک‌ها از مسیر جایگزین هدایت می‌شوند؛ اما در صورت خرابی کنترل‌کننده در شبکه اقتضایی خودرویی مبتنی بر نرم‌افزار، عملکرد کل شبکه مختل خواهد شد. برای حل این مشکل می‌توان از کنترل‌کننده جانشین برای ارائه پشتیبان‌گیری از سامانه استفاده کرد. همچنین برای حل این مشکل می‌توان از کنترل‌کننده‌های توزیع‌شده در این شبکه بهره برد که این راه حل موجب می‌شود عملکرد شبکه با پیاده‌سازی روند تعادل بار کنترل شود؛ اما نحوه ارتباطات کنترل‌کننده‌ها با همدیگر نیز نیاز به بررسی و مطالعات بیشتری دارد.

۱۰-۴- حملات بر بخش‌های مختلف SDVN

در این بخش به بررسی حملات محتمل به لایه‌های مختلف معماری شبکه‌های نرم‌افزار محور استفاده شده در شبکه‌های SDVN می‌پردازیم.

۱۰-۴-۱- حمله به لایهٔ انتقال

در شبکه SDVN قوانین تعریف‌شده توسط کنترل‌کننده، در مناطق گره‌های خودرویی ذخیره می‌شوند. هنگامی که گره‌ای از این شبکه، مسیری را برای جریان بسته ورودی پیدا نکند، بسته به‌صورت موقت در حافظهٔ گره ذخیره می‌شود. هم‌زمان گره مورد نظر یک پرس‌وجو را به RSUها ارسال کرده و همچنین از کنترل‌کننده در مورد قوانین بسته‌های مفقودی پرس‌وجو می‌کند. هنگامی که گره، قوانین مربوطه را دریافت کرد، مطابق با قوانین دریافتی با بسته‌های ذخیره شده رفتار می‌کند. در این شبکه‌ها وسایل نقلیه به‌عنوان گره‌های شبکه، ظرفیت ذخیره‌سازی محدودی دارند. بنابراین، مهاجم می‌تواند با ارسال تعداد زیادی دادهٔ جدید با قوانین مختلف به سمت گره‌ها، حمله منع خدمت را راه‌اندازی کند. بدین ترتیب شبکه برای پاسخ‌گویی مجبور به ذخیره‌سازی موقت داده‌ها، ارسال پرس و جو به RSU و کنترل‌کننده می‌شود. با توجه به محدودیت ظرفیت حافظه گره، هنگامی که حافظه پر شود، بسته‌های ورودی جدید دور ریخته خواهند شد.

۱۰-۴-۲- حمله به لایهٔ کنترل

کنترل سامانه‌های مبتنی بر SDN توسط بخش کنترلی صورت می‌گیرد. در شبکهSDVN حملات منع خدمت توزیع‌شده ممکن است، بخش کنترلی این سامانه را مورد هدف قرار دهند. در این حمله تعداد زیادی خودروی آلوده به‌طور همزمان صدها یا هزاران بسته را به سمت یک یا تعدادی خودرو ارسال می‌کنند. با توجه به اینکه تمام قوانین در سوئیچ‌ها وجود ندارد، گرهٔ مورد نظر پرس‌وجوهای زیادی را تولید و به سمت کنترل‌کننده ارسال می‌کند؛ بنابراین، توان پردازشی عظیمی استفاده شده و درنتیجه موجب تأخیر در نتایج و درنهایت دور ریخته شدن پرس‌وجوها می‌شود.

در شبکه SDVN حمله کنترل‌کننده جعلی[1] نوعی دیگر از حملات به بخش کنترلی است. در این حمله، مهاجم با میزبانی یک کنترل‌کننده جعلی (برای اجرای سیاست‌هایی به نفع مهاجم استفاده می‌شود) قادر به دسترسی به کنترل‌کننده SDN خواهد شد. کنترل‌کننده جعلی، RSUها را مجبور به قطع ارتباط، دور ریختن بسته‌ها و تزریق اطلاعات کرده و از این اجزا به‌عنوان گره پایه‌ای برای راه اندازی حمله به کل سامانه استفاده می‌کند[۶].

۱۰-۵-آسیب پذیری‌های استاندارد OpenFlow

استاندارد OpenFlow نخستین سازوکار ارتباطات داده‌ای در سامانه‌های مبتنی بر SDN است. این استاندارد چندین بار بازبینی شده است و در حال حاضر در سامانه‌های مبتنی بر شبکه نرم‌افزار محور به‌صورت گسترده مورد استفاده قرار می‌گیرد. با این حال، این استاندارد نسبت به قوانین اجراشده

[1] fake controller

بر روی گره‌ها، بی توجه است. استاندارد OpenFlow نمی‌تواند بر فعالیت خراب‌کارانه در RSUهایی که به‌صورت مستقیم با کنترل‌کننده در ارتباط هستند، رسیدگی کند. بنابراین، فعالیت‌های خراب‌کارانه به‌راحتی به لایهٔ کنترل، نفوذ خواهند کرد. همچنین در این استاندارد ارتباطات رمزنگاری نمی‌شوند؛ بنابراین، امنیت سامانه را پایین می‌آورند [۲۷].

۱۱- نتیجه‌گیری

شبکه‌های نرم‌افزارمحور یک فناوری با نفوذ در زمینه شبکه‌های رایانه‌ای است که انعطاف‌پذیری، مقیاس‌پذیری، انطباق‌پذیری، تسهیل مدیریتی و نوآوری را به شبکه می‌افزاید. تاکنون این فنآوری در شبکه‌های سیمی از جمله مراکز داده‌ای و شبکه‌های گسترده محبوبیت خاصی پیدا کرده و درهمین‌اواخر در شبکه‌های بی‌سیم نیز مورد توجه قرار گرفته است. شبکه‌های اقتضایی خودرویی به‌دلیل ویژگی‌های ذاتی چالش‌ها و محدودیت‌هایی دارند. هم‌گرایی SDN با شبکه‌های اقتضایی خودرویی زمینه را برای ادغام این معماری‌ها و ظهور معماری نوآورانه SDVN فراهم می‌سازد. ما در این مقاله معماری شبکهٔ اقتضایی خودرویی مبتنی بر نرم‌افزار را معرفی و مزایای و فرصت‌های حاصله از این معماری را بیان کرده‌ایم. اگرچه در معماری شبکه اقتضایی خودوریی مبتنی بر نرم‌افزار، فنآوری SDN توانایی حل بسیاری از مشکلات شبکه اقتضایی خودرویی و مدیریت شبکه را دارد، ولی این معماری نوظهور چالش‌هایی را نیز به همراه خواهد داشت. ما در این مقاله به‌منظور ارتقای امنیت شبکه SDVN چالش‌های محتمل در این معماری را بیان کردیم که این چالش‌ها می‌توانند به‌عنوان مسیر پژوهش‌های آینده مورد توجه قرار گیرند.

۱۲- مراجع

[1] F. Yi, N. Zhang, "A Survey on Software-defined Vehicular Networks." *Journal of Computers*, vol.28, no.4, pp236-244, 2017.

[2] M. Zhu, Z.P.Cai, M.Xu, and J. N. Cao, "Software-defined vehicular networks: oppor-tunities and challenges," In *Energy Science and Applied Technology: Proceedings of the 2nd International Conference on Energy Science and Applied Technology*, 2015, pp.247.

[3] Brief OS. OpenFlow™-Enabled Mobile and Wireless Networks. White paper. 2013 Sep 30.

[4] S. Indriyanto, M.N.D. Satria, A.R. Sulaeman, R. Hakimi, and E.Mulyana, "Performance analysis of VANET simulation on software defined network".

In *2017 3rd International Conference on Wireless and Telematics (ICWT),* July 2017, pp. 81-85.

[5] K. Ian, Y. Lu, M. Gerla, R. Lopes Gomes, F. Ongaro, and E. Cerqueira, "Towards software-defined VANET: Architecture and services," *In Med-Hoc-Net*, 2014, pp. 103-110.

[6] H.Shafiq, R. Asif Rehman, and . Kim, "Services and security threats in sdn based vanets: A survey," *Wireless Communications and Mobile Computing 2018*,2018.

[7] M. Ealias and R. N. Gaur, "A survey on different routing models in cognitive radio ad-hoc network," *International Journal of Advanced Research in Electronics and Instrumentation Engineering*, vol. 03, no. 12, pp. 13741–13748,2014.

[8] J.Sanguesa, J. Barrachina, M. Fogue, P. Garrido, F. Martinez, J. Cano, C. Calafate, and P. Manzoni. "Sensing traffic density combining V2V and V2I wireless communications," Sensors 15, no. 12 pp.31794-31810, 2015.

[9] T. Stoyanova, and S. Todorova, "DDoS Attack Detection in SDN-based VANET Architectures," AALBORG UNIVERSITY Innovative Communication Technologies and Entrepreneurship (ICTE), 2016.

[10] N. Bhaskar, A. Ranjan, V, Gunawat, P. Kumar, and S. Majhi, "A brilliant public transportation system linked with electric vehicles in coordination with the grid," *In 2014 Annual IEEE India Conference (INDICON)*, 2014, pp. 1-6.

[11] D. Antonio, M. Palattella, R. Soua, L. Lamorte, X. Vilajosana, J.Alonso-Zarate, and T. Engel, "Enabling SDN in VANETs: What is the impact on security?," *Sensors*, 16, no. 12, 2016, pp.2077.

[12] M.Mejri, J. Ben-Othman, and M.Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications 1*, no. 2, 2014, pp. 53-66.

[13] N.Dao, J. Park, M. Park, S.Cho, "A feasible method to combat against DDoS attack in SDN network," *In Information Networking (ICOIN), 2015 International Conference*, 2015, pp. 309-311.

[14] S.Hartman, M.Wasserman, D.Zhang, "Software driven networks problem statement," Network Working Group Internet-Draft, Oct. 2013.

[15] A.Bates, K. Butler, A. Haeberlen,M. Sherr, W. Zhou, "Let SDN be your eyes: Secure forensics in data center networks," In *Proceedings of the NDSS workshop on security of emerging network technologies,SENT'14*,Feb, 2014.

[16] Z.Shu, J.Wan, D. Li, J Lin, A.Vasilakos, M. Imran, "Security in software-defined networking: Threats and countermeasures," *Mobile Networks and Applications*, Oct 2016, 21, no.5, pp.764-76.

[17] S.M.Mousavi, M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," *In-Computing, Networking and Communications (ICNC), 2015 International Conference, IEEE*, Feb 2016, pp. 77-81.

[18] D.Kreutz, F.M. Ramos, P.E.Verissimo, C.E.Rothenberg, S.Azodolmolky, S.Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, Jan 2015, 103, no.1, pp.14-76.

[19] Sezer, Sakir, Sandra Scott-Hayward, Pushpinder Kaur Chouhan, Barbara Fraser, David Lake, Jim Finnegan, Niel Viljoen, Marc Miller, and Navneet Rao. "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Communications Magazine*, Vol. 51, no. 7, 36-43, 2013.

[20] M.Mendonca, K. Obraczka, and T. Turletti. "The case for software-defined networking in heterogeneous networked environments." In in submission, ACM New York, NY, USA, 2012, December, pp. 59-60.

[21] M. A. Salahuddin, A. Al-Fuqaha, and M. Guizani. "Software-defined networking for rsu clouds in support of the internet of vehicles." *IEEE Internet of Things journal*, 2015, Vol.2, no.2, pp.133-144.

[22] Yaqoob, Ibrar, I. Ahmad, E. Ahmed, A.Gani, M. Imran, and N. Guizani, "Overcoming the key challenges to establishing vehicular communication: Is SDN the answer?," *IEEE Communications Magazine*, vol.55, no. pp. 128-134, 2017.

[23] K. Hyojoon, and N. Feamster, "Improving network management with software defined networking," *IEEE Communications Magazine*, vol. 51, no. 2, pp 114-119, 2013.

[24] M.Chahal, S.Harit, K.Mishra, K. Sangaiah, and Z Zheng, "A survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases," *Sustainable cities and society*, vol. 35, pp.830-840,2017.

[25] K. Asif Uddin, and B. Kesari Ratha, "Time series prediction QoS routing in software defined vehicular ad-hoc network," In *International Conference on Man and Machine Interfacing (MAMI)*, 2015,pp. 1-6.

[26] Truong, B. Nguyen, G. Myoung Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular adhoc network with fog computing,." In *IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2015, pp. 1202-1207.

[27] Zhang, Peng, H. Wang, Ch. Hu, and Ch. Lin. "On denial of service attacks in software defined networks," *IEEE Network* 30, no. 6 pp. 28-33,2016.

مژگان قصابی مدرک کارشناسی را در رشته مهندسی فناوری اطلاعات با کسب رتبه نخست از دانشگاه زنجان اخذ کرد. دوره کارشناسی ارشد را نیز در رشته مهندسی فناوری اطلاعات گرایش شبکه‌های کامپیوتری با کسب رتبه نخست از دانشگاه علوم تحقیقات تهران به پایان رساند. زمینه‌های پژوهشی مورد علاقه وی امنیت شبکه‌های نرم‌افزارمحور، امنیت اینترنت اشیا، شبکه‌های اقتضایی خودرویی و شبکه‌های اقتضایی پروازی است.

محمود دی‌پیر مدرک دکترای خود را در رشتهٔ کامپیوتر-سامانه‌های نرم‌افزاری و مدرک کارشناسی ارشد خود را در رشتهٔ کامپیوتر-نرم‌افزار هر دو از دانشگاه شیراز دریافت کرده است. مقطع کارشناسی خود را نیز در همین رشته از دانشگاه هوایی شهید ستاری دریافت کرده است. هم‌اکنون عضو هیئت علمی دانشکده رایانه و فناوری اطلاعات دانشگاه هوایی شهید ستاری است. زمینه‌های پژوهشی ایشان شامل داده‌کاوی و امنیت فضای سایبر و دارای مقالات متعددی در مجلات و کنفرانس‌های معتبر ملی و بین‌المللی است. نامبرده در پروژه‌های پژوهشی و صنعتی متعددی مشارکت داشته است.