وزارت علوم تحقیقات و فناوری

دانشگاه علم و فرهنگ
واحد همدان

عنوان پروژه :

Vehiche -to- Vehiche Safety Messaging in VANET

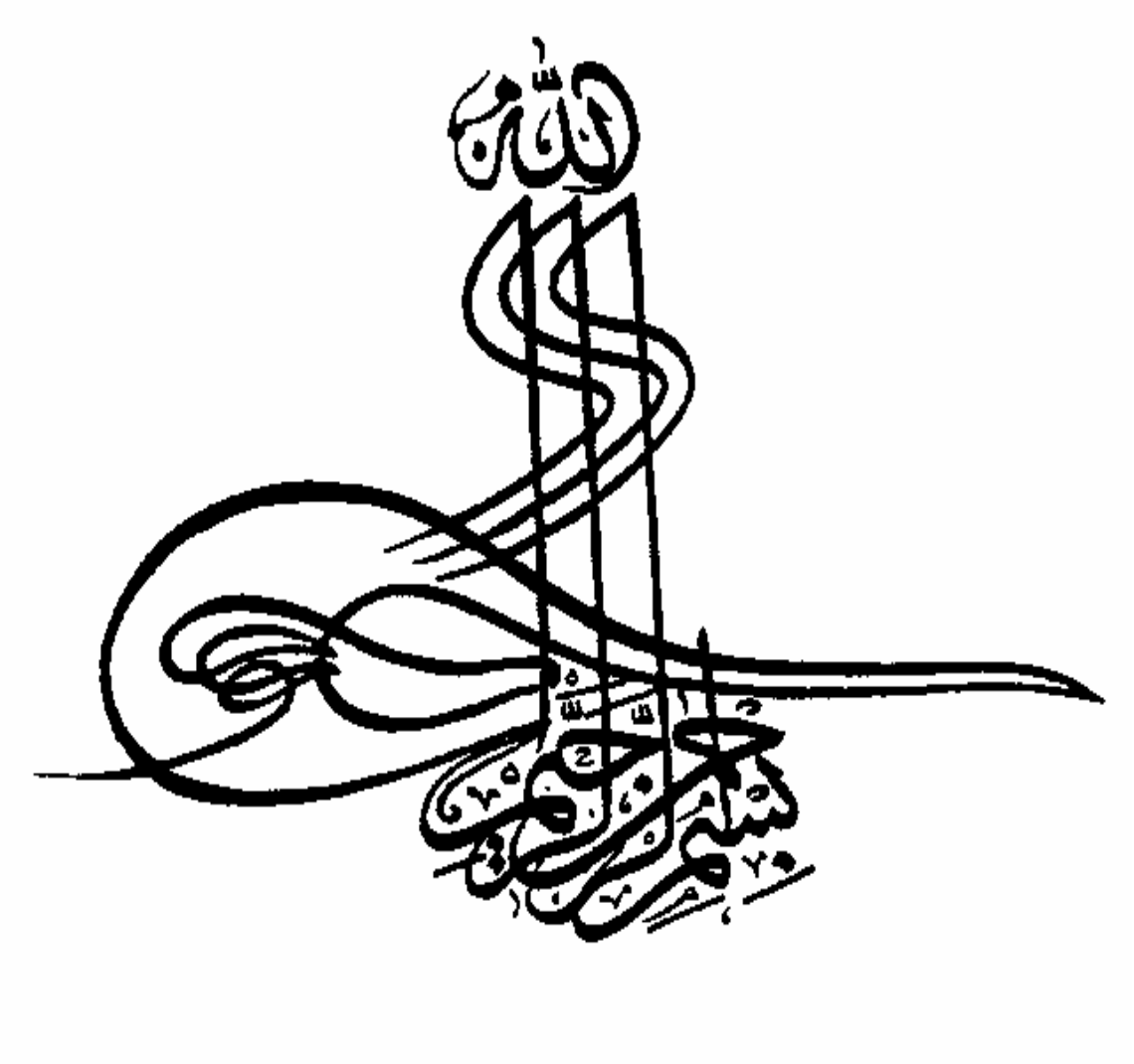
استاد راهنما:

مهندس شیرزاد بیات

دانشجو:

مسعود پارسانیا

تابستان ۹۱



وزارت علوم تحقیقات و فناوری

دانشگاه علم و فرهنگ
واحد همدان

عنوان پروژه :

Vehiche -to- Vehiche Safety Messaging in VANET

استاد راهنما:

مهندس شیرزاد بیات

دانشجو:

مسعود پارسانیا

تابستان ۹۱

تقدیم و سپاس:

منت خدای راعزّوجلّ که طاعتش موجب قربت است و به شکر اندرش مزید نعمت.

به نام خداوندی که علم و دانایی از آن اوست.

امید است این پایان نامه زمینه سازی باشد برای فعالیت ها و کارهای بزرگ برای کشور و سرزمین مان ایران.

از پدر و مادرم به جهت زحمات فراوانی که در پرورش اینجانب تحمل شده اند سپاسگزاری نمیده و این دستاورد خود را به آنان تقدیم میدارم.

در آخر از جناب آقای مهندس شیرزاد بیات جهت راهنمایی های شایان و بی دریغشان کمال تشکر و سپاس را دارم.

چکیده

پیام رسانی امن خودرو به خودرو و امنیت ارتباطات در VANET

شبکه تک کاره وابسته به خودرو (**VANET**) یک شبکه تک کاره **ad-hoc** است برای فراهم کردن ارتباط بین وسایل نقلیه. در این پایان نامه، ابتدا یک نمونه واقعی معماری شبکه ای **VANET** توضیح داده شده سپس نگاهی به فعالیت های مربوط به تدارک امنیت پیام امن انداخته می شود که در آن محققان چندین راه حل برای محافظت پیام های امن پیشنهاد کرده اند. ملزومات امنیت شامل تصدیق، غیر قابل انکار بودن، حریم خصوصی و صحت داده هستند که در انتشار پیام امن دخالت دارند، و مفروضات سیستم که شامل روش های پویا و ثابت است. پروتکل های مبتنی بر زیر ساخت کلید ثابت در مقایسه با ساختارهای پویا، در پیاده سازی و اجرا کار آمدتر و امنیت قوی تری را پشتیبانی می کنند. این پروتکل ها از تفکیک ناحیه برای تأسیس زیر ساخت کلید ممتاز تحت سرپرستی **CA** (اعتبار تصدیق) در نواحی متفاوت استفاده می کنند.

SAB (انتشار بی نام ایمن) یکی از پروتکل های پیشنهادی است که اکثر ملزومات امنیتی را حفظ می کند اما در عمل کمبود های نیز دارد. یک موضوع خیلی مهم، تغییر ناحیه یک خودرو است. تغییر نواحی، شبکه را به سوی تغییر **CA** و ضرورت معین کردن کلید جدید برای ادامه ارتباط سوق می دهد. سپس راه حل های برای آگاهی دادن به وسایل نقلیه در مورد تغییر ناحیه کرانه ای برای کسب کلید جدید قبل از وارد شدن به ناحیه بعدی پیشنهاد می شود. همچنین پیام های درخواست کلید امن توسط تأیید کلید عمومی **CA** قبلی ساخته شده بنابراین امنیت قویتر برای انتشار پیام امن بدست می آید. در آخر طرح پیشنهادی از سه منظر تأخیر زمانی، محافظت پیام امن و پیام کنترلی و مقایسه روش پیشنهادی (**D-SAB**) با دیگر روش ها مورد ارزیابی کارایی قرار می گیرد.

در ادامه نحوه ارسال پیام‌های امن از یک خودرو به دیگر خودروها را مورد مطالعه قرار می‌گیرد. هدف، ارسال پیام‌های امن در وسایل نقلیه با ضریب اطمینان بالا و تأخیر کم است، این ارتباط یک به چند و محلی است. شبکه ارتباط نقلیه‌ای از نوع **ad-hoc**، با قابلیت تحرک بالا و تعداد زیادی گره‌های رقیب می‌باشد. پیام‌های خیلی کوتاه و دارای یک عمر کوتاه مفید می‌باشند اما باید با احتمالی بالا دریافت شوند.

این پایان نامه، تأثیر تکرار سریع فرا بخشی پیام‌ها را مورد پژوهش قرار می‌دهد. همچنین چندین پروتکل با دسترسی تصادفی برای کنترل دسترسی رسانه پیشنهاد می‌شود. تمامی پروتکل‌های طراحی شده در دو کلاس همزمان و غیر همزمان قرار می گیرند. پروتکل‌ها با معماری چند کانال ارتباطات اختصاصی با وسعت کم (**DSRC**) سازگار هستند. شاخص‌های کیفیت سرویس (**Qos**) در دو مبحث محیط امن **DSRC** و کیفیت سرویس برای پیام‌های امنیتی **DSRC** مورد بحث قرار می‌گیرد. کیفیت سرویس برای پیام‌های امنیتی **DSRC** با توجه به احتمال خطای پذیرش (**PRF**) تعریف می‌شود. زمان اشغال کانال کنترل توسط پیام‌های امنیتی ارزیابی خواهد شد، این امر توسط **CBT** شاخص بندی می‌شود و **CBT** در نواحی مختلف شبکه برای به دست آوردن شاخص برای کل شبیه سازی در نظر گرفته می‌شود.

نهایتاً، مدل تحلیلی شبکه ساخته شده و شبیه سازی‌ها برای تشخیص اطمینان گیرنده و میزان مصرف کانال پروتکل به کار گرفته شده‌اند. نتایج تحلیلی و شبیه سازی به خوبی با هم می‌خوانند و نتایج شبیه سازی از نوع تحلیلی آن نسبت به محیط واقعی سازگارتر است. بررسی‌ها و شبیه سازی‌ها نشان می‌دهد در حالت ایده آل هر دو **PRF** و **CBT** باید کم باشند و تحلیل‌های انجام شده دارای دو محدودیت مهم هستند، مدل کانال بدون حافظه است و همچنین **CBT** تنها یک مفهوم غیر مستقیم برای تخمین ترافیک غیر امن می باشد. با این حال نتایج، نزدیک شدن ما را به امکان پذیر شدن پیام‌های امن نقلیه‌ای نشان می‌دهد.

فهرست مطالب

فهرست شکل‌ها

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

مقدمه

با توجه به گستردگی برنامه‌های ارتباط بی سیم و شبکه‌ها در زندگی روزمره انسان‌ها، تقریباً این برنامه‌ها تمام جنبه‌های زندگی انسان را در بر گرفته‌اند. یکی از این برنامه‌ها وابسته به خودروها و رانندگی است، بطوریکه هدف این شبکه فراهم کردن امنیت و یک مدیریت بهتر برای ترافیک است.

بر اساس نیاز، یک نوع خاص از شبکه بی سیم برای ارتباطات حمل و نقل تعیین شده است. گره‌های این شبکه، اتومبیل‌ها هستند و یک طبیعت تک منظوره (**Ad-hoc**) دارد که شبکه حمل و نقل تک منظوره **VANET** نامیده می‌شود. در **VANET**، یک خودرو با خودرویی دیگر ارتباط بر قرار می‌کند (**V2V**) و همچنین با زیر ساخت های کنار جاده‌ای نیز به معنای امکانات ارتباط، رابطه دارد (**V2I**).

مهمترین کاربرد این شبکه‌ها، آگاهی دادن خودروها در موارد اورژانسی مثل تصادف، نقص عضو حاد یا تراکم ترافیکی است. در این قبیل موارد، یک خودرو می‌تواند از طریق انتشار پیام امن، سایر خودروها را مطلع کند. در نتیجه سایر خودروها می‌توانند عکس‌العمل مناسبی در قبال حادثه داشته باشند.

فصل اول

معرفی شبکه VANET و مقدمه‌ای بر امنیت شبکه

- معرفی شبکه **VANET**
- مقدمه‌ای بر امنیت شبکه **VANET**
- معماری شبکه
- تعاریف و مفاهیم اولیه

فصل اول- معرفی شبکه VANET و مقدمه‌ای بر امنیت شبکه

۱-۱- معرفی شبکه VANET

بر اساس سازمان بهداشت جهانی (**WHO**)، تصادفات جاده‌ای، سالیانه سبب مرگ ۱/۲ میلیون و آسیب دیدن ۵۰ نفر در سراسر جهان است. اگر عامل پیشگیری لحاظ نشود، مرگ و میر ناشی از تصادفات به عامل سوم کاهش طول عمر و یا ناتوانی جسمی انسان‌ها در سال ۲۰۲۰ تبدیل می‌شود و این در حالی است که این عامل در سال ۱۹۹۰ در جایگاه نهم قرار داشته است. مطالعات در اروپای غربی نشان می‌دهد که تنها کاهش میانگین ۵ کیلومتر بر ساعتی خودروها سبب کاهش ۲۵ درصدی کاهش مرگ و میر جاده‌ای می‌شود.

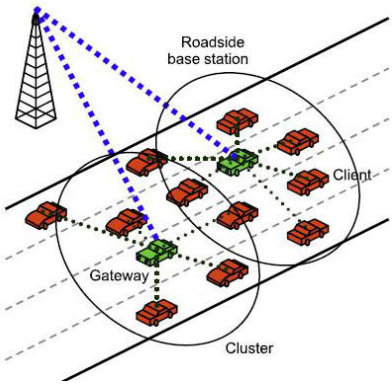
شکل ۱-۱- تصادفات جاده‌ای

با استفاده از تکنولوژی ارتباطات بی سیم، کنترل سرعت توسط مأموران پلیس به طور قابل ملاحظه‌ای آسانتر و کارآمدتر خواهد شد. دولت‌ها و تولید کنندگان به طور عمده به دنبال راهی برای بهبود امنیت رانندگان، کارمندان و عابران پیاده هستند. اخیراً این تلاش‌ها سبب پیدایش دیدگاه" غیر فعال "[1] شده است.

یک سیستم امنیتی غیر فعال تلاش می‌کند تا با استفاده از وسایلی مانند کیسه هوا و جذب کننده شوک، صدمات و میزان تصادفات را به حداقل برساند. اما این کار قادر به جلوگیری از تصادفات نیست. بنابراین بر آن شد تا از سیستم‌های امنیتی غیر فعال به سیستم‌های " فعال " که می‌توانند از تصادفات جلوگیری کنند، حرکت شود.

سیستم‌های امنیتی فعال، به عنوان قسمتی از بخش وسیع ارتباطات و تکنولوژی انفورماتیک تحت سیستم انتقال هوشمند (**ITS**) به صورت یکپارچه پدیدار شدند و اساساً برای بالا بردن بهروری و امنیت نقل و انتقالات گسترش پیدا کرده‌اند. تکنولوژی‌های **ITS** به منظور بهبود سفرهای جاده‌ای با پیشگیری از تصادفات، کاهش تراکم و ازدحام، در هم قفلی و بالا بردن مدیریت و تنفیذ ترافیک طراحی شده‌اند.

شبکه تک کاره وابسته به خودرو (**VANET**) یک شبکه تک کاره بی سیم است که در یک محیط وابسته به خودرو عمل می‌کند، شبکه‌ای که ارتباطات خودرو به خودرو (**V2V**) و خودرو به جاده (**V2I**) را سازماندهی می‌کند.



شکل ۱-۲- انواع ارتباطات

[1] **Passive**

تکنولوژی که ارتباطات مطمئن " **V2V** " و " **V2I** " را فراهم می‌کند به عنوان **IEEE 802.11p** و دسترسی‌های بی سیم وابسته به خودرو (**WAVE**) پیشنهاد و استاندارد شده است. **VANET** می‌تواند توسط محدوده‌ی گوناگونی از کاربردها برای بهبود امنیت جاده مورد استفاده قرار بگیرد. یکی از این کاربردها، سیستم هشدار تصادف (**CCWS**) است.

امنیت انتقال یکی از کاربردهای شبکه‌های وابسته به خودرو است. وسایل نقلیه می‌توانند اطلاعات ترافیکی و یا وضعیت جاده را به خوبی یک گره ثابت در شبکه، برای هم مخابره کنند. برای مثال، پیام‌های اخطاری که توسط یک وسیله نقلیه‌ی اورژانسی و خودرو های که در تونل‌های جاده‌ای به علت تصادف متوقف شده‌اند، تولید می‌شود. به طور نمونه، پیام‌های امنیتی نیاز دارند تا به تمامی وسایل نقلیه در حال حرکت در سراسر منطقه جغرافیایی به طور فراگیر با امنیت و ضریب اطمینان بالا و همچنین تأخیر کم تحویل داده شوند.

در این مبحث به مطالعات در مورد انتشار پیام‌های امنیتی در سراسر شبکه‌های وابسته به خودرو در فواصل جاده‌ای، جایی که گره ای ثابت وجود ندارند و فقط انتشار مطمئن در ارتباطات **ad-hoc** وجود دارد، پرداخته می‌شود.

دو نوع پیام امنیتی قابل بهروری در **CCWS** وجود دارد:

۱. پیام‌های امنیتی عادی

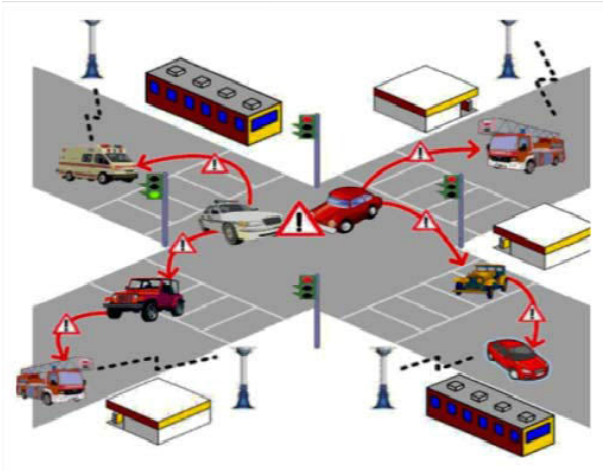
پیام‌های امنیتی عادی که به نام پیام‌های دیده بانی[۲] نیز معروف هستند، پیام‌های بروز رسانی وضعیتی هستند که مرتباً توسط خودروی که اطلاعاتی از قبیل موقعیت و سرعت را در اختیار دارد ارسال می‌شود. پیام‌های دیده بانی یک خودرو را برای دریافت وضعیت خودروهای اطراف و ارائه یک اخطار پیشرفته به راننده هر تصادف احتمالی، قادر می‌سازد.

[2] **beacom**

۲. پیام‌های امنیتی رخدادی

پیام‌های امنیتی رخدادی، پیام‌های اخطاری هستند که توسط خودروی که ممکن است سبب بروز حادثه شود، بکار گرفته می‌شود. برای مثال، ترمز شدید، حرکت ناگهانی و یا نقص فنی.

خودروهای که ممکن است خودروهای دیگر را به مخاطره بی اندازند، خودروی " غیر عادی " نامیده می‌شوند. یک خودروی غیر عادی باید پیام‌های اخطاری را به تمامی خودرو های به خطر افتاده برای جلوگیری از تصادف و برخورد، بفرستد. ممکن است پیام‌های اخطاری نیاز به تکثیر در طول مسیر جاده و فراتر از پوشش منطقه‌ای فرستنده‌ی اصلی داشته باشد.



شکل ۱-۳- انواع ارتباطات

نتیجه می‌گیریم در پروژه‌های چندگانه، پیام‌های اخطاری توسط سایر وسایل نقلیه باز پخش می‌شوند. انتشار به موقع پیام‌های اخطاری می‌تواند مانع بروز تصادفات زنجیره‌ای خودروها شوند. زیرا پیام‌های اخطاری می‌توانند سریع‌تر از نمایشگرهای دیداری مانند چراغ قرمز عقب خودرو دیده شوند.

در این مبحث سعی می‌شود روی پروژه انتشار پیام‌های اخطاری از خودروی به خودرو دیگر و محافظت پیام‌های امن (اخطار) تمرکز شود و جزییات فنی و تحقیق روی پیام‌های دیده بانی خارج از حوزه‌ای این مبحث است.

هر خودرو به یک دستگاه ارتباطی که **OBU** (واحد سر خود) نامیده می‌شود، مجهز است. همچنین **RSU** (واحد کنار جاده‌ای) می‌تواند پیام‌های اضافی وابسته به ترافیک را برای خودروها فراهم آورد تا به آنها وضعیت جاده را مانند ساختارهای جاده پیش ور و حداکثر سرعت در منحنی پیچ را نشان می‌دهد.

۱-۲- مقدمه‌ای بر امنیت شبکه VANET

امنیت همیشه یک چالش در شبکه‌ها است اما در **VANET** اساسی و مهمتر است. حفظ امنیت در این شبکه‌ها از طریق مفهوم تبادل پیام امن، انجام شده است. زمانی که این پیام‌ها، تأثیر مستقیم بر زندگی مردم خواهند داشت، حفظ شبکه حمل و نقل به یک امر حیاتی تبدیل خواهد شد. پیام‌های امن باید از فرستنده‌ای معتبر فرستاده شوند (اعتبار) و حاوی اطلاعات مناسب و تغییر ناپذیر باشد (درستی داده). حریم که در بر گیرنده اطلاعات محرمانه خودروها است برای جلوگیری از ردیابی خودرو بسیار مهم است. رفتار غیر قابل انکار در موارد تصادفی و جنایی ضرورت دار، بنابراین هویت رانندگان می‌تواند از پیام بازیابی شود و نمی‌توان آن را انکار کرد.

جلوگیری از حملات ممکن، مثل حمله جوابیه و حمله پیام غلط در این شبکه‌ها از اهمیت برخوردار است. بنابراین مکانیزم‌های حفاظتی باید در ارسال و دریافت پیام امن بکار گرفته شوند.

بیشتر کارهای صورت گرفته، همه نیازهای قابل اجرا برای حفظ پیام امن، اجابت نکرده اند. از این رو ابتدا نیازها را برای امنیت شبکه‌ها تعیین می‌کنیم، سپس بر اساس آن نیازها، مناسب‌ترین پروتکل امنیتی را انتخاب می‌کنیم. در نهایت، چالش‌های پیاده سازی را از طریق پیشنهاد راهکارهایی برای افزایش کارایی در مقیاس بزرگتر، بر طرف می‌کنیم.

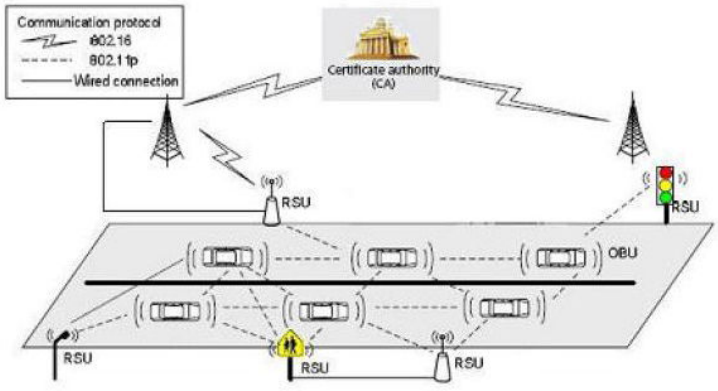
۱-۲-۱- معماری شبکه

در ابتدا، وابستگی بین اجزای **VANET** مورد مطالعه قرار گرفته و دو لایه را مانند آنچه در شکل ۱-۴ نمایش داده شده ارائه می‌شود:

۱- لایه پایینی: این لایه شامل **RUS** ، **OBU** و پیام‌های منتشر شده مبتنی بر پروتکل ارتباط **DSRC** است. برای تبادل پیام کنترلی، خودروها از پروتکل **802.11e** برای ارتباط با **RSU** استفاده می‌کنند. (در رابطه با پروتکل‌های ارتباط **DSRC** در فصل‌های آینده به صورت مفصل توضیحاتی داده خواهد شد).

۲- لایه بالایی: شامل ایستگاه‌های پایه (**BS**) و سیستم‌های مرکزی مثل **CA** است. ارتباطات بین اجزاء سیمی و یا بی سیم مبتنی بر پروتکل **802.11e** است. یک **RSU** تمامی پیام‌ها را از لایه پایینی درخواست می‌کند و آنها را به **BS** در لایه بالاتر می‌فرستد. همچنین پاسخ‌ها را از **CA** دریافت و آنها را به **OBU** می‌فرستد.

سر نخ[۳] : پیام‌های کنترلی برای اهداف سیگنالینگ استفاده می‌شوند مثل در خواست و جواب کلید.



شکل ۱-۴- معماری شبکه

[3] **Hint**

۱-۲-۲- تعاریف و مفاهیم اولیه

چندین کار در زمینه امنیت شبکه‌های حمل و نقل انجام شده است. در اکثر آنها، امنیت بیشتر مورد توجه قرار گرفته است. به ندرت، حفاظت پیام امن به عنوان یک روش قابل اجرا در شبکه حمل و نقل مورد توجه بوده است. یک پروتکل مسیریابی بر اساس موقعیت جغرافیایی مورد استفاده قرار می‌گیرد تا کاربردها و سرویس‌هایش را امنیت ببخشد. بعد از اینکه موقعیت هر خودرو از طریق گیرنده‌های **GPS** بدست آمد، موقعیت‌های آنها در طول هویت آنها در یک جدول در **OBU** ذخیره می‌شوند. این جدول از طریق پیام دریافتی به صورت دوره‌ای با سایر خودروها مبادله می‌شود. این روش‌ها جنبه‌های امنیتی را از قبیل احراز هویت، درستی داده و عدم انکار را می‌پذیرد، اما پروتکل هیچ دخالتی در حریم شخصی ندارد. یکی از مفاهیم به کار برده شده، زیر ساخت کلید عمومی (**PKI**) است و تایید پیام‌های دریافت شده منطقاً بر اساس سرعت، زمان و موقعیت فرستنده پیام بکار برده شده است. اطلاعات موقعیتی برای تمامی خودروها فرستاده می‌شود. این پروتکل قدرتش را برای حملات **sybil** (نوعی حمله امنیتی) حفظ می‌کند. همچنین حملات پیام‌های غلط می‌تواند به راحتی تشخیص داده شود چرا که رسیدگی و باز جویی منطقی انجام شده است.

زمانی که این پروتکل‌ها مبتنی بر موقعیت اند و در باقی نگاه داشتن گمنامی (نا شناس بودن) و حریم شخصی ناتوان، آنها در برابر حملات ردیابی شکننده‌اند و این ایراد اصلی این نوع روش‌ها است.

محققان از امضای گروهی برای باقی نگاه داشتن گمنامی و حریم شخصی خودروها استفاده می‌کنند. در این روش‌ها، هر خودرو به گروهی از خودروها تعلق دارد. این به منظور نگهداری گمنامی در داخل گروه است، هنگامی که اطلاعات محرمانه گره‌ها تنها برای مدیر گروه قابل دسترسی است.

مدیر گروه، سرآمد این گروه است که وظایفش تولید کلید، تولید امضاء و تایید ثبت نام عضو، باطل کردن عضویت و بازیابی هویت خودروها است. اگر چه یک مدیر گروه، وظایف بی شماری را برای انجام دادن دارد اما سربار آن با افزایش جهت گروه، اضافه می‌شود. مدیر گروه از یک جفت کلید عمومی- خصوصی برای

حفظ حریم و یک کلید ویژه برای نگهداری اعتبار در یک گروه استفاده می‌کند. گمنامی خودروها از طریق استفاده از یک پروتکل معتبر مبتنی بر کلیدهای قرینه دار تصادفی، بر آورده می‌شود.

در ابتدا، تعدادی کلید قرینه دار از میان مجموعه کلیدها به صورت تصادفی انتخاب می‌شود. زمانی که چندین خودرو ممکن است در این واگذاری تصادفی کلید، کلیدهای مشابهی دریافت کنند، هویت یک خودرو نمی‌تواند فاش شود بنابراین گمنامی حاصل می‌شود. همچنین ابطال کلید آسانتر می‌شود چرا که هر خودرو چندین کلید دارد.

یکی از معایب روش گفته شده، احتمال بالای حملات است چون دشمنان می‌توانند به راحتی به برخی کلیدها دسترسی داشته و از آنها برای ارسال پیام غلط استفاده می‌کنند. به علاوه، برای شناسایی هویت یک خودرو، به تمامی کلیدهای وابسته به آن خودرو نیاز است، این دومین عیب این پروتکل است. این کارها تبادل پیام برای شناسایی یک خودرو را پر زحمت و هزینه می‌کنند.

امضای دیجیتال، تکنیکی برای امن ساختن شبکه حمل و نقل است. در این مقاله، ترکیبی از چندین مکانیزم برای امنیت **VANET** بکار گرفته می‌شود. در ارتباط خودرو به خودرو جفت کلیدها، کلیدهای نشست (**session**) در نظر گرفته می‌شوند اما در مورد ارتباط گروهی و انتشار چند پخشی[۴] یک کلید اشتراکی قبل از آغاز هر گونه ارتباط، بین اعضاء توزیع می‌شود.

برای مدیریت گروه یک تفکیک سلولی صورت می‌گیرد و نزدیکترین گره به سلول اصلی به عنوان مدیر گروه انتخاب می‌شود که وظیفه‌اش ارسال کلید عمومی است. یکی از نقص‌های مهم این روش، نداشتن حراست و محافظت غیر انکاری در تبادل اطلاعات است. چون که هیچ هویت معینی را در داخل پیام برای شناخته شدن در آینده، رها نمی‌کند. ضمناً طبیعت پویای مدیران گروه وابسته به تغییر وضعیت متوالی اعضاء و نبود نظارت بر اعضاء، چالش‌های موجود در این پروتکل بشمار می‌رود.

[4] **broad casting**

یک راهکار برای امن ساختن انتشار در ارتباط حمل و نقلی، استفاده از یک ابر کلید برای حفظ جنبه‌های امنیتی است. اعتبار از طریق کلید قرینه دار به اشتراک گذاشته شده در هر ناحیه بدست می‌آید، بنابراین، گمنامی و حریم خصوصی به صورت هم زمان حاصل می‌شود. غیر قابل انکار بودن یکی دیگر از جنبه‌های است که از طریق استفاده کردن از یک کلید خصوصی قرینه دار برای پنهان کردن هویت فرستنده پیام استفاده می‌شود. از مزایای این پروتکل می‌توان به قدرت آن در برابر اکثر حملات و سهولت پیاده سازی آن اشاره کرد.

سرانجام، هر راه حل پیشنهادی مزایا و معایب خاص خودش را دارد اما پروتکل پیشنهادی **SAB** نسبت به بقیه جامع و سریعتر است. در این کار، بر حفظ امنیت در مدل انتشار پیام امن تمرکز می‌شود. با توجه به تغییر سریع پیکر بندی در این شبکه‌ها و زمان پاسخ کوتاه رانندگان به حوادث، یک روش انتخاب شده باید تأخیر پنهان سازی – آشکار سازی را کاهش و طول پیام را به حداقل برساند.

۱-۲-۳- ملزومات امنیت و مفروضات سیستم

۱-۲-۳-۱- ملزومات امنیت

چهار جنبه امنیتی در انتشار پیام امن دخالت دارند:

- تصدیق: هر خودروی گیرنده باید از اعتبار فرستنده پیام مطمئن شود و آن را به رسمیت بشناسد.
- غیر قابل انکار بودن: تمامی خودروها باید بخشی از اطلاعات شخصی خود را اعلام کنند، بنابراین این اطلاعات می‌تواند در موارد وقوع جنایت و بیمه تشخیص داده شوند. بنابراین انکار توسط فرستنده غیر ممکن می‌شود.
- حریم خصوصی: اطلاعات شخصی خودروها و رانندگان نباید توسط سایر خودروها قابل دسترسی باشد و گمنامی برای توقف ردیابی باید باقی نگاه داشته شود. البته سازمان‌های دارای مجوز از این قاعده مستثنی هستند.

- صحت داده: پیام ارسال شده باید حاوی اطلاعات معتبری باشد نه اینکه توسط هکرها تغییر داده شده باشد.

بر اساس موضوعات بالا، مکانیزم امنیتی باید راه حلی را ارائه دهد که جنبه‌های مطلوب را بر آورده کند. در زمینه‌های امنیتی برای حفظ هر دو اعتبار و گمنامی، یک زیر ساخت گروهی را مورد استفاده قرار می‌گیرد. در این سبک هر خودرو باید در یک گره ثبت شود و کلید تصدیق عمومی‌اش (**AK**) را قبل از ارسال هر گونه پیام، دریافت کند. برای علامت گذاری یک پیام، خودرو از کلید تصدیق گروه و تابع پنهان سازی استفاده کرده و آن را با پیام اصلی می‌فرستد. بنابراین لزومی ندارد که هر عضو، اطلاعات خصوصی سایر اعضاء مثل هویت آنها و کلید عمومی برای تصدیق آنها را داشته باشد. گیرنده‌ها اعتبار اعضاء را از طریق تأیید امضاء، تأیید می‌کنند. ابن امر از طریق تأیید دوباره تابع پنهان سازی با کلید تصدیق برای پیام دریافت شده و مقایسه حاصل با امضاء به دست می‌آید.

$$\mathbf{V \rightarrow *, M, HMAC_{AK}\ (M)} \qquad (۱-۱)$$

همچنین گیرنده‌ها می‌توانند از صحت داده ارسال شده بعد از اینکه امضاء را تأیید کردند، اطمینان حاصل کنند.

با اعمال موضوعات بالا، ابعاد سه‌گانه امنیت: تصدیق، صحت داده و حریم خصوصی محفوظ خواهد ماند. باید به یاد داشت که در این کاربرد، جنبه‌های محرمانه امنیت لازم و ضروری نیست. دلیل آن نیز طبیعت چند پخشی پیام امن است، جایی که پیام‌ها بتوانند توسط همه خودروها دریافت شوند (معتبر یا غیر معتبر) و اطلاعات آنها برای همه آشکار است، این امر مشکلی ایجاد نمی‌کند.

در مورد حفظ کننده غیر قابل انکار، هویت یک خودرو باید به پیام ضمیمه گردد، بنابراین می‌توان در هر زمان دلخواه ردیابی شود. بر این اساس، ردیابی خودرو تنها برای سازمان دارای مجوز امکان پذیر است. بنابراین خودرو باید هویتش را پنهان کند و تنها سازمان‌های مجاز قادر به آشکار سازی هستند. بنابراین

پنهان سازی هویت خودرو باید از طریق مفهوم کلید عمومی (**PK**) از سازمان مجاز صورت گیرد و در یک فیلد شخص در داخل پیام اصلی جا داده شود.

$$\mathbf{V \longrightarrow *, M, HMAC_{AK}\,(M), E\,(id_V)_{PU}} \qquad (۲-۱)$$

وقتی که هویت یک خودرو توسط یک کلید عمومی پنهان می‌شود، سایر خودروها قادر به تشخیص آن نبوده و فقط سازمان مجاز می‌توانند به هویت آن دسترسی پیدا کنند. این گفته اشتباه است که کلید عمومی باید مانند **AK**، همزمان با تولید خودروها به آنها تخصیص داده شود.

همان‌طور که قبلا گفته شد، هدف پیشنهاد یک راه حل کارآمد برای نگهداری امنیت انتشار پیام امن در **VANET** است، بنابراین پیاده سازی عملی آن در اولویت است. فعالیت‌های گوناگونی برای توسعه امنیت در شبکه‌های حمل و نقل تک منظوره انجام شده است اما تعداد کمی به نگهداری امنیت در انتشار چند پخشی توجه کرده‌اند. طرح پیشنهادی، یکی از پروتکل‌های است که به انتشار چند پخشی توجه می‌کند و موضوعات امنیتی مثل امضاء گروه و سایر موارد مورد نیاز به منظور حفظ امنیت را شامل می‌شود.

۱-۲-۳-۲- مفروضات سیستم

همانطور که قبلاً اشاره شد یک زیر ساخت کلیدی برای تولید و توزیع **AK** و **PU** نیاز وجود دارد. می‌توان تمامی روش‌های پیشنهاد شده را به دو دسته اصلی تقسیم کرد:

۱. روش‌های پویا: روش‌های که بر امضاء گروه بر انتخاب یک مدیر گروه پویا تکیه دارد.
۲. روش‌های ثابت: روش‌های که از یک زیر ساخت ثابت برای مدیریت کلید استفاده می‌کند.

در روش‌های پویا قبل از هر ارتباطی، گره‌ها نیاز به عضویت در یک گروه دریافت کلیدها دارند. با توجه به سرعت بالای خودروها و تغییر سریع توپولوژی شبکه، گروه‌های تأسیس شده پایدار نبوده و ممکن است از

هم متلاشی شوند. تعیین مدیر گروه و توزیع کلید پیچیده و زمان بر است. در هر گروه فقط یک خودرو شانس مدیریت گروه را دارد. پس تمامی خودروها باید به تجهیزات کامل مجهز باشند.

مطالب گفته شده در بالا شبکه را در برابر اکثر حملات آسیب پذیر می‌کند. برای مثال: یک هکر می‌تواند به عنوان مدیر گروه انتخاب شود و کاربردها و وظایف شبکه را مختل کند. این موارد انتخاب روش‌های ثابت را نشان می‌دهد. در روش‌های ثابت، مدیریت کلید نسبت به طرح پویا مناسب‌تر و کاربردی‌تر است.

اینجا در روش‌های ثابت یک موجودیت ثابت مرکزی برای مدیریت کلید داریم. برای مقیاس پذیری بزرگتر بهتر است از یک ساختار سلسله مراتبی وابسته به تعداد زیاد خودرو و بسط اندازه شبکه استفاده کنیم. به همین دلیل یک کشور را با توجه به تراکم خودروها به چندین ناحیه تقسیم می‌کنیم و به هر ناحیه یک **CA** (اعتبار تصدیق) اختصاص می‌دهیم. برای مدیریت همزمان، تمامی **CA** ها را به یک **CA** مرکزی که $\mathbf{CA_{ROOT}}$ نامیده می‌شود، متصل می‌کنیم. هر **CA** مسئول تولید، توزیع و مدیریت کلید است و تنها موجودیت مورد اعتماد در ردیابی خودروها است.

وقتی روش‌های ثابت انتخاب می‌شود باید به ملزومات ویژه آن توجه کرد. در روش‌های ثابت نواحی تحت نظارت **CA** تعریف می‌شود. هنگامی که هر **CA**یک مجموعه کلید برای امنیت بخشیدن به تبادل پیام در داخل ناحیه خودش تعریف می‌کند با تغییرات ناحیه‌اش مشکلات بروز می‌کنند. مشکل خودروی است که هنوز مجموعه کلید قدیمی‌اش را دارد و برای ارتباط در منطقه‌ای جدید **CA** نیاز به یک مجموعه کلید جدید دارد.

با توجه به تحرک و انتقال بالا بین نواحی، مدیریت نواحی کرانه‌ای برای جایگذاری کلید یک موضوع بحرانی است. بنابراین نگهداری اتصال و اجتناب از قطعی در نواحی کرانه از وظایف **CA** است. یک مدیر مناسب نواحی کرانه ای، نقاط آسیب پذیر و تجاوز هکرها را کاهش می دهد.

فصل دوم

امنیت در نواحی کرانه‌ای و ارزیابی آن و بررسی پروتکل DSRC در پیام رسانی امن

- طرح پیشنهادی به منظور امنیت در نواحی کرانه ای
- تحلیل و ارزیابی
- معرفی ارتباطات اختصاصی با وسعت کم (**DSRC**)
- مرور ادبیات و فناوری های مربوط
- فرمول سازی مسئله
- طراحی پروتکل

فصل دوم- امنیت در نواحی کرانه‌ای و ارزیابی آن و بررسی پروتکل DSRC در پیام رسانی امن

۲-۱- طرح پیشنهادی به منظور امنیت در نواحی کرانه‌ای

در این پایان نامه یک رویکرد کاربردی مبتنی بر پروتکل **SAB** را پیشنهاد می‌شود؛ و آن در نواحی کرانه‌ای بهینه سازی خواهد شد. پروتکل **SAB** هیچ استراتژی برای مدیریت نواحی کرانه‌ای ندارد. به خاطر اینکه تبادل پیام امن بین خودروها به مجموعه کلید **CA** وابسته است تغییر مکان از یک ناحیه به ناحیه جدید ممکن است مشکلاتی را برای تبادل پیام ایجاد کند. بنابراین آگاهی از تغییر ناحیه و ارسال در خواست برای مجموعه کلید جدید (**AK** و $\mathbf{PU_{CA}}$) یک وظیفه اساسی برای خودروها است.

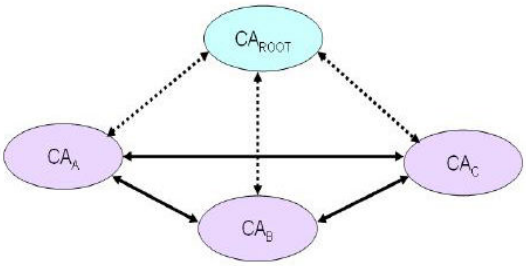
وقتی مرزهای ناحیه ای دور از **CA** قرار بگیرند پردازش‌های ارسال و درخواست کلید، تصدیق اعتبار و تخصیص کلید، زمان بندی می‌شود به همین خاطر به علت فقدان کلیدهای جدید مخصوصاً وقتی سرعت خودرو زیاد است قطعی اتصال رخ می‌دهد. این قطعی موجب از دست رفتن اطلاعات حیاتی در مورد تصادفات و وقایع غیر قابل پیش بینی می‌شود بنابراین ضرر جانی و مالی اجتناب نا پذیر می‌شود جون همه

خودروها به تجهیزات شبکه سیستم‌های هشدار متکی هستند. ضمناً این قطعی می‌تواند شانسی برای متجاوزان و دشمنان برای یک حمله جدی به شبکه باشد.

به همین خاطر؛ طرح تبادل اطلاعات در نواحی کرانه‌ای تبدیل به یک چالش جدی شده است که می‌تواند تبدیل به یک مشکل برای پروتکل‌های مبتنی بر تفکیک ناحیه که در هر ناحیه وابسته به مدیر مرکزی هستند؛ شود. در نتیجه اگر نواحی تخصیص **CA** را مشخص و خطوط یال منحنی‌های ناحیه را قبل از تبادل پیام تعریف شود، وظایف راحت‌تر می‌شوند.

۲-۱-۱- طرح انتخاب CA

با تکیه بر کلیدها در روش‌های امنیتی؛ تولید و توزیع کلیدها نیازمند یک زیرساخت و پردازش واضح و مشخص است. برای مقیاس پذیر تر کردن پروتکل باید ابتدا مدیریت و کنترل را توزیع کرد. این بدین معنی است که به جای انتخاب یک **CA** می‌توان چندین **CA** انتخاب کرده و یک **CA** مرکزی برای مدیریت **CA** ها داشت. سبک ارتباط بین **CA** ها در شکل ۲-۱ نشان داده شده است.



شکل ۲- ۱- روابط بین CA

روش تعریف و تعیین **CA** در یک کشور بستگی به ناحیه‌ی جغرافیایی و چگالی خودرو آن منطقه دارد. تاکید می‌شود که **CA** ها نباید خیلی به هم نزدیک باشند تا از فراوانی درخواست کلید جلوگیری شود. به این دلیل که وقتی دو **CA** به هم نزدیک هستند، نرخ انتقال افزایش می‌یابد. در صورت چگالی بالای خودرو در یک **CA**، می‌توان چندین **RSU** قطعی تحت کنترل **CA** تعیین کرد و بار سنگین **CA** را بین آنها توزیع کرد. یک واگذاری منطقی **CA** برای چندین ناحیه مطلوب است به این خاطر که این واگذاری مناسب، تأخیر

تبادل پیام را کاهش می‌دهد و از مزاحمان و تبلیغات جلوگیری می‌کند. در نتیجه، در ادامه روی چگونگی تعریف خطوط کرانه‌ای تمرکز خواهد شد که یک نقش مهم در کاهش وقفه در کرانه‌های منطقه‌ای بازی می‌کند.

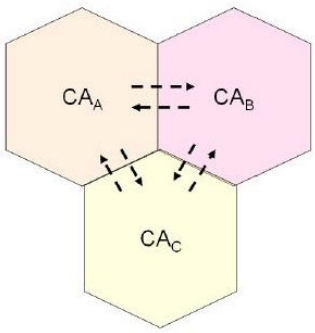
۲-۱-۲- تعریف خط کرانه‌ای

همیشه تعریف کرانه‌ها برای **CA** و واگذاری نواحی آنها در یک روش بهینه مطلوب بوده است. بهتر است خطوط منطقه‌ای را در دورترین فاصله‌ی نسبی **CA** مرکزی انتخاب کنیم. آنها معمولاً در جاده‌ها و درون شهرها قرار داده می‌شوند.

برای اجتناب از تبادل درخواست کلید متوالی، خطوط ناحیه‌ای باید در وضعیت‌های باشند که جهت حرکت خودروها به صورت متوالی تغییر نکند و تغییر باید قابل پیش بینی باشد. به عنوان مثال خطوط منطقه‌ای در اطراف پیچ‌ها، میدان‌ها یا تقاطع‌ها قرار داده شود. این بدین دلیل است که وقتی یک خودرو از قلمرو یک **CA** خارج و وارد ناحیه یک **CA** جدید می‌شود، قبل از اینکه **CA** جدید، درخواست کلیدش را پردازش کند، به ناحیه **CA** قبلی بر می‌گردد و درخواست را مجدداً برای**CA** قبلی می‌فرستد، این کار، بار **CA** را به صورت قابل توجهی افزایش می‌دهد.

راه حل دیگر، استفاده از روش‌های پیش بینی تحرک برای تشخیص جهت حرکت و مسیر است. با اعمال این روش، پیام‌های درخواست کلید در نواحی کرانه‌ای کاهش پیدا می‌کند. قابل ذکر است که جفت کلیدهای شناسایی و عمومی برای تبادل پیام در هر منطقه مورد نیاز است، بنابراین مناطق تحت پوشش **CA** نباید ناحیه مشترک داشته باشند.

$$\forall\, i,j \Rightarrow R_i \cap R_j = \phi \qquad (۱-۲)$$



شکل ۲-۲- کرانه‌های منطقه‌ای

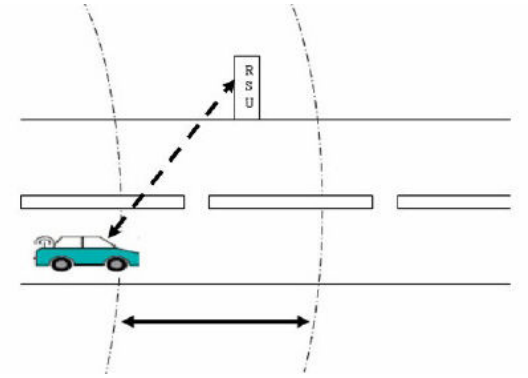
۲-۱-۳- تبادل پیام در خطوط منطقه‌ای

وقتی یک خودرو پیام‌های را دریافت می‌کند که نمی‌تواند آنها را رمزگشایی کند، تغییر منطقه را حس می‌کند. برای جلوگیری از تأخیر زمانی و از دست دادن داده؛ خودروها باید کلید عمومی و کلید تصدیق **CA** جدید را قبل از ورود به قلمرو آن، دریافت کنند. بنابراین باید خودروها قادر به تشخیص **CA** همسایه باشند. دو روش که می‌تواند توسط **CA** یا خود خودرو انجام شود را پیشنهاد می‌شود:

۱- توسط CA قدیمی

در این راه حل، **CA** جاری پیام تغییر منطقه را می‌فرستد و منتظر درخواست کلیدهای جدید از طرف خودروها می‌نشیند. این کار را به وسیله‌ی مفاهیم **RSU** کرانه‌ای انجام می‌دهد. اگر **RSU**، پیامی شامل درخواست کلید را دریافت کند، این پیام را به **CA** جاری می‌فرستد. این **CA** همچنین درخواست را به **CA** جدید اعلام می‌کند و منتظر پاسخ می‌شود سپس **CA** جدید از **CA** خانگی($\mathbf{CA_h}$) برای اعتبار این خودرو سوال می‌کند. اگر $\mathbf{CA_h}$ آن را تایید کند، **CA** جدید کلید تصدیق و کلید عمومی را به وسیله‌ی مفاهیم **RSU** کرانه‌ای برای خودرو می‌فرستد، مگر اینکه این خودرو را در پایگاه داده $\mathbf{CA_h}$، نا معتبر تلقی کند.

بنابراین خودرو، قبل از رسیدن به منطقه جدید، کلید جدید را می‌گیرد. در این روش، خودرو قبل از ورود به ناحیه به **CA** جدید مطلع است پس وقتی پیامی را به وسیله‌ی کلیدهای قبلی دریافت می‌کند قابل رمزگشایی نیست. کلیدهای قدیمی را با نوع جدیدش جایگزین می‌شود.



شکل ۲-۳- منطقه کرانه‌ای

لازم به ذکر است که ناحیه‌ی کرانه‌ای به اندازه‌ی کافی وسیع است که همه‌ی خودروها بتوانند مجموعه کلید **CA** جدید را قبل از ورود به ناحیه جدید دریافت کنند.

۲- توسط خودرو

در روش قبلی؛ وجود **RSU** در اطراف مناطق کرانه‌ای برای اطلاع خودروها ضروری است. این روش ممکن است به علت فقدان زیرساخت اطراف مرز یا وقوع خطا در مراحل ارسال پیام، ناموفق باشد. در این روش خود خودرو مأمور اطلاع رسانی در مورد تغییر منطقه است. خودروها تمامی کرانه‌های منطقه‌ای را بعد از ورود به منطقه‌ی یک **CA** دریافت می‌کنند. هر خودرو یک جدول هماهنگی کرانه‌ای با **CA** مربوطه دارد بنابراین از طریق محاسبه دوره‌ای مسافت می‌تواند درجه‌ی نزدیکی به کرانه را اندازه گیری کند.

اگر مسافت کمتر از یک آستانه (مرز) باشد، دوباره درخواست‌های کلید را به **RSU** نزدیک کرانه ارسال می‌کند. از آنجای که این درخواست‌ها بسیار مهم هستند، خودروها باید تصدیق را از **RSU** مربوطه دریافت کنند و در صورت عدم دریافت تصدیق، درخواست را دوباره بفرستند. در حقیقت؛ این

روش به وسیله‌ی مفاهیمی چون جدول مراجعه‌ای و محاسبه مسافت تا کرانه انجام شده است. بنابراین خودرو، قبل از ورود به منطقه جدید صاحب مجموعه کلید خواهد شد. برای افزایش اطمینان، از یک روش پیوندی استفاده می‌شود که یک ترکیب از دو راه حل ارائه شده در بالا است.

۲-۱-۴- پردازش تبادل کلید امنیتی

وقتی یک خودرو منطقه‌اش را تغییر دهد، یکی از موضوعات مهم، دریافت کلیدهای درست و صحیح است. زمانی که محتویات پیام‌های امن بحرانی هستند و امنیت بخشیدن به آنها به وسیله‌ی مفهوم کلیدها بدست آمده باشد، درستی و تمامیت نگهداری کلیدها، اصل و قاعده است.

برای انجام این کار، نیاز به اعمال یک مکانیسم امنیتی برای محافظت کلیدها است. ساختار یک پیام مناسب، امنیت کلید را در مقابل هکرها، قرنطینه می‌کند و از تغییر کلید در طول پروسه‌ی تبادل جلوگیری خواهد شد.

در روش پیشنهادی، از کلیدهای مشابهی که در **CA** قدیمی برای امنیت پیام امن استفاده می‌شد، به منظور رمزدار کردن پیام درخواست کلید که به **CA** جدید ارسال می‌شود استفاده خواهد شد. جدول ۲-۱، فرمت پیام درخواست کلید را نشان می‌دهد:

جدول ۲-۱ : فرمت پیام درخواست کلید

Req
ID_{OCA} ,ID_{CAh}
$E(M, ID_V, E(Req, ID_{OCA}, ID_{CAh})_{SK})_{PUOCA}$

- فیلد اول، **Req** نوع درخواست را مشخص می‌کند که درخواست برای کلید عمومی و کلید تصدیق **CA** جدید است.
- فیلد دوم، ID_{OCA} و ID_{CAh} به ترتیب هویت **CA** قدیمی و **CA** خانگی هستند.

- فیلد سوم، **M** شامل سرعت، وضعیت، زمان و جهت است. $\mathbf{ID_V}$ هویت خودرو و $\mathbf{E(Req, ID_{OCA}, ID_{CAh})}$ رمزگذاری اولین و دومین فیلد پیام با کلید راز (**SK**) خودرو است.

نکته: تمامی سه ورودی ذکر شده با کلید عمومی **CA** جاری رمزگذاری شده‌اند.

رمزگذاری محتویات فیلد سوم با کلید $\mathbf{PU_{OCA}}$ برای نگهداری حریم خودروها در مقابل هکرها برای جلوگیری از ردیابی است. حقیقتاً رمزگذاری **Req** و $\mathbf{ID_{OCA}}$ و **SK**، پیام را در مقابل حملات مبدل، قوی می‌کند. همچنین یک فرمت برای پیام پاسخ طبق شکل زیر تعریف می‌شود :

جدول ۲-۲ : فرمت پیام پاسخ

Rep
ID_{NCA}
$E(PU_{NCA}, AK)_{SK}$

- فیلد اول **Rep** نوع درخواست را مشخص می‌کند که در اینجا پاسخ برای پیام درخواست کلید است.
- فیلد دوم $\mathbf{ID_{NCA}}$ هویت **CA** جدید است.
- فیلد سوم، کلید عمومی و کلید تصدیق **CA** جدید با کلید راز خودرو (**SK**) رمزگذاری شده‌اند. رمزگذاری $\mathbf{PU_{NCA}}$ و **AK** با کلید راز، این کلیدها را از فاش شدن محافظت می‌کند.

۲-۲- تحلیل و ارزیابی

۲-۲-۱- تحلیل تهدید

۲-۲-۱-۱- حملات جدی بر منطقه کرانه

مناطق کرانه نقاط آسیب پذیر در زیرساخت ثابت هستند. هکرها و مزاحمان می‌توانند با سوء استفاده از وقفه‌ها، جای را برای دریافت کلید جدید بگیرند. حملات با بیشترین احتمال در زیر آمده است:

حمله پیام غلط: در این حملات، هدف مهاجم گمراه کردن خودروهای است که از کرانه‌ها عبور کرده و وارد منطقه جدید می‌شوند. این حمله از طرف خودروهای معتبر از طریق ارسال پیام‌های رمزگذاری شده تکراری با کلیدهای معتبر منطقه **CA** قدیمی است. اگر حمله‌ای صورت نگیرد، خودرو می‌تواند از تغییر منطقه با خبر شود زمانی که چندین پیام را دریافت کند و قادر به رمزگشایی آنها نباشد. بنابراین درخواست کلید را به **CA** می‌فرستد و وقتی مجموعه کلید جدید را دریافت کند از تغییر منطقه مطمئن می‌شود. در حمله پیام غلط، مهاجمان سعی در به عقب انداختن خودروها از اطلاع تغییر منطقه دارند. روش پیشنهادی، این حمله را از طریق اطلاع رسانی تغییر منطقه خودرو متوقف می‌سازد. بنابراین مجموعه کلید جدید را قبل از ورود به منطقه جدید دارا خواهد بود.

فقدان اعتبار: اگر حمله پیام غلط یا هر دلیل دیگری که مانع از متوجه شدن خودروها از تغییر منطقه شود، خودرو به انتشار پیام امن با کلید قدیمی ادامه می‌دهد در حالی که کلیدها در این منطقه معتبر نمی‌باشند. این باعث می‌شود که خودرو به عنوان یک مهاجم در منطقه‌ی جدید شناخته شود. بنابراین خودرو، اعتبارش را از دست خواهد داد. همچنین روش پیشنهادی از طریق اطلاع رسانی به خودرو و معتبر ساختن آن از طریق واگذاری کلید جدید قبل از عبور آن از کرانه، این رخداد را نیز متوقف می‌کند.

۲-۲-۱-۲- حملات به پیام کنترلی

پیام‌های کنترلی در کرانه‌های منطقه‌ای دارای اطلاعات مهمی در مورد کلیدها هستند، بنابراین امنیت ارسال آنها خیلی مهم است. پس در اینجا فرمت امنیت برای آن پیشنهاد می‌شود. در این بخش، پایداری این فرمت در مقابل بعضی حملات مهم مورد تجزیه و تحلیل قرار می‌گیرد.

ردیابی: زمانی که کرانه‌ها، گلوگاه‌های مناطق هستند و چگالی (تراکم) خودرو نسبت به شهرها پایین‌تر است، مهاجمان از طریق دست‌یابی به هویت خودرو یا آماده سازی یک لیست از خودروهای وارد شده به یک منطقه به دلایل خاص، تمایل به ردیابی خودروها دارند. این کار می‌تواند توسط پیام تبادل کلید حاصل شود. برای مقابله با این حمله، هویت خودروها با کلید عمومی **CA** نشان داده شده در جدول ۲-۱ رمز گذاری می‌شود که تنها **CA** قادر به رمز گشایی آن برای چک کردن اعتبار خودرو می‌باشد.

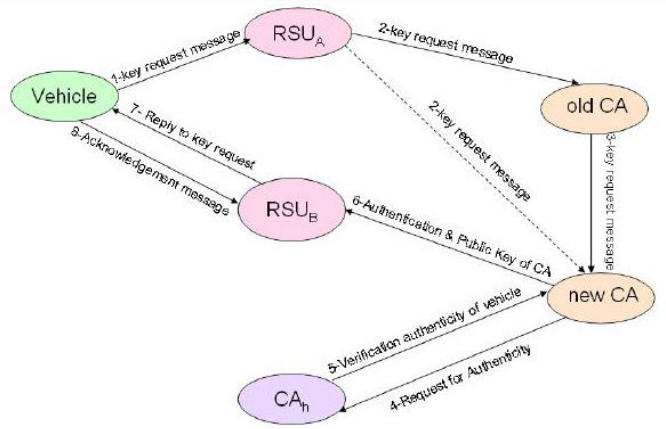
مبدل سازی: یک حمله‌ی خیلی مهم در کرانه‌های منطقه‌ای این است که مهاجمان سعی می‌کنند با ارسال پیام درخواست کلید به خوبی دیگر خودروهای معتبر، به مجموعه کلید دسترسی پیدا کنند. مهاجم ممکن است به هویت خودرو دست پیدا کند اما نمی‌تواند این قسمت از پیام را $\mathbf{E(Req, ID_{OCA})_{SK}}$ با کلید راز خودرو تولید کند، این بدین خاطر است که فقط $\mathbf{CA_h}$ و خودرو مربوطه دارای **SK** هستند و می‌توانند آن قسمت را تولید کنند در نتیجه، حمله دفع می‌شود.

۲-۲-۲- ارزیابی کارایی

۲-۲-۲-۱- تأخیر زمانی

یک مکانیزم امنیتی خوب دارای تأخیر زمان کوتاهی برای رمز گذاری (پنهان سازی)، رمزگشایی (آشکار سازی) و تبادل کلید است. در روش پیشنهادی، برای ارسال پیام امن، خودروها خلاصه پیام را به وسیله تابع **HMAC** و رمزگذاری **ID** با خط منحنی **P-224** تولید می‌کنند. عملیات **HMAC** خیلی سریعتر از

رمزگذاری است و تأخیر آن در مقایسه با تأخیر رمز گذاری بسیار ناچیز است. هنگام دریافت پیام، خودرو فقط خلاصه پیام را با **AK** تولید می‌کند و آن را با خلاصه‌ی پیام دریافتی که زمان کمی طول کشیده است، مقایسه می‌کند. دیگر پروسه‌های رمزگشایی از طریق **CA** انجام شده‌اند که تأثیر بر تأخیر نهایی ندارد. زمانی که فرکانس دریافت پیام امن از ارسال آن بیشتر باشد، روش قابل قبول است. برای تبادل مجموعه کلید در کرانه‌های منطقه‌ای، این مراحل ضروری است، طبق شکل زیر:



شکل ۲-۴- مراحل درخواست تا دریافت کلید

۱- ارسال درخواست کلید به نزدیکترین **RSU** ، (**D_1**).

۲- تشخیص نوع پیام توسط **RSU** و ارسال آن به **CA** قدیمی. در پروتکل **SAB** این نوع پیام به **CA** جدید بعد از ورود به آن فرستاده می‌شود. (خط تیره در شکل ۷) و در این پروتکل، مرحله ۳ کنار گذاشته شده است، (**D_2**).

۳- تشخیص نوع پیام توسط **CA** و فرستادن آن به **CA** جدیدی که خودرو در حال ورود به قلمرو آن است که این کار مبتنی بر جهت حرکت است، (**D_3**).

۴- تشخیص نوع پیام توسط **CA** جدید و بازبینی هویت خودرو از طریق ارسال درخواست هویت به **CA_h**، (**D_4**).

۵- بازبینی هویت خودرو از طریق **CA_h** و ارسال جواب به **CA** جدید، (**D_5**).

۶- اگر خودرو شناسایی شده باشد، **CA** جدید هویت و کلید عمومی را به عنوان پیام پاسخ به خودرو ارسال می‌کند، مگر اینکه پیامی را به $\mathbf{CA_h}$ برای رد کردن هویت خودرو ارسال کند، ($\mathbf{D_6}$).

۷- پیام پاسخ توسط **RSU** به صورت فرا پخشی ارسال می‌شود تا توسط خودرو مورد نظر دریافت شود، ($\mathbf{D_7}$)

۸- رمزگشایی پیام توسط خودرو و ارسال پیام تصدیق (**ACK**) به آن **RSU**، ($\mathbf{D_8}$).

$$\mathbf{D=D_1+D_2+D_3+D_4+D_5+D_6+D_7+D_8} \qquad (۲-۲)$$

طبق پروسه‌ی ذکر شده بالا، یک تأخیر کلی رخ می‌دهد که این تأخیر به ضرایبی چون درجه‌ی نزدیکی به **RSU**، سبک ارتباط اجزا و بار اضافی اجزا (**RSU,CA**) وابسته است.

طولانی‌ترین تأخیر($\mathbf{D'}$) زمانی اتفاق می‌افتد که خودرو وارد **CA** جدید شده و از ورود به منطقه جدید آگاهی پیدا کند و پیام درخواست کلید را ارسال کند. در پروتکل **SAB**، این تأخیر به **D** اضافه شده و بنابراین ممکن است خیلی از حملات اتفاق بی افتد.

$$\mathbf{D_{Total} = D+ D',\quad D' >> D} \qquad (۳-۲)$$

از طریق دو روش پیشنهاد شده، خودروها قبل از ورود به **CA** جدید توسط **CA** جاری خبردار می‌شوند و $\mathbf{D'}$ حذف می‌شود. بنابراین این روش تأخیر پروسه‌ی تبادل کلید را کاهش می‌دهد.

۲-۲-۲-۲- محافظت پیام امن و پیام کنترلی با مجموعه کلید مشابه

استفاده از حداقل تعداد کلید برای امنیت یک سیستم بسیار حائز اهمیت است. در بعضی روش‌های امنیتی برای **VANET**، کلیدهای متفاوتی برای امنیت هر ارتباط به کار گرفته می‌شود که مدیریت کلید را پیچیده‌تر و زمان‌بر می‌کند. در این صورت، پروسه تبادل کلید بیشتری مورد نیاز است و بنابراین بسیار آسیب پذیر تر خواهد بود.

روش پیشنهادی در اینجا از سه کلید (**AK, PU_{CA}, SK**) برای امنیت هـر دو پیـام امـن و تبـادل کلیـد، تشکیل شده است. همچنین یک فرمت امن مبتنی بر آنها ارائه شده است. بنابراین این روش بـه یـک امنیـت قوی دست پیدا می‌کند و خطرات کمتری صورت می‌گیرد.

۲-۲-۲-۳- مقایسه با دیگر روش‌ها

در این بخش چند روش را برای امنیت فرا پخشی پیام‌های امن مقایسه می‌شود. طبق جدول ۲-۳، چهـار روش را که دارای مکانیزم‌های برای امنیت پیام‌های امن هستند مقایسه می‌شوند. معیار کارایی برای مقایـسه عبارتند از: از پایداری در برابر حملات مهم، اجابت کردن چهار بعد امنیت، تـأخیر زمـانی و تعـداد کلیـدهای مورد نیاز است.

روش پیشنهادی تحت عنوان **D-SAB** (**SAB** توسعه یافته) در جدول نشان داده شده است:

جدول ۲-۳ : مقایسه‌ی چهار روش امنیتی برای پیام‌های امن

Method / Performance Criteria		Position Base	Group Signature	Random Symmetric Key	SAB	D-SAB
4 Security Dimensions		Except Privacy	✓	✓	✓	✓
Attacks To Safety Messages	Tracking		✓	✓	✓	✓
	Masquerading	✓	✓	✓	✓	✓
	False Message	✓				✓
Attacks To Control Messages	Tracking		✓	✓		✓
	Masquerading					✓
Delay	Generate Message	T_E	T_E	T_E	T_E	T_E
	Receipt Message	T_D	T_D	T_D	T_H	T_H
	Key Exchange	-	T_{EX}	T_{EX}	T_{EX}	-
Number of Key		$2n+N_G$	$2n+N_G$	n.k	$n+2N_{CA}$	$n+2N_{CA}$
Type of Infrastructure		Dynamic	Dynamic	Dynamic	Static	Static

T_E : زمان رمز گذاری (پنهان سازی)

T_D : زمان رمز گشایی (آشکار سازی)

T_H : زمان تولید خلاصه‌ی پیام با **HMAC**

T_{EX} : زمان تبادل کلید

N : تعداد خودروها

N_G : تعداد گروه‌ها

N_{CA} : تعداد **CA** ها

روش پیشنهادی از طریق پایداری در برابر حملات، تأخیر زمانی، معیارهای سرآمد و مقایسه آن با دیگر روش‌ها مورد ارزیابی قرار گرفت. در این فصل، بیشتر به امنیت پیام امن مبتنی بر زیرساخت کلید ثابت پرداخته شد و بعضی مسائل چالش برانگیز از میان برداشته شد. بنابراین، امنیت دیگر کاربردها مثل ارتباطات هوشمند، اطلاعات ترافیکی مبتنی بر این زیرساخت کلید ممکن است برای فعالیت‌های آینده حائز اهمیت باشد.

در ادامه پروتکل‌های مربوط به ارتباطات از نوع **DSRC** که در لایه پایینی از زیر ساخت معماری شبکه **VANET** قرار دارد به منظور بررسی پیام رسانی امن خودرو به خودرو مورد بحث قرار می‌گیرد.

۲-۳- معرفی ارتباطات اختصاصی با وسعت کم (DSRC)

ارزشیابی کارایی استاندارد اولیه **IEEE 802.11** نشان می‌دهد این تکنولوژی نمی‌تواند زمان را برای انتشار پیام بحرانی در محیط ترافیکی متراکم یا کانال با بار بالا تأمین و تضمین کند. بنابراین لازم است پروتکل‌های مؤثر ارتباط امن را برای کاهش بار کانال به کار برد و این مهم با طراحی درست و به جای استراتژی تکرار و یا انتقال دوباره پیام به دست می‌آید. این استراتژی‌ها با هدف کاهش تعداد دوباره انتقال از طریق محدود کردن انتشار پیام به یک منطقه و جهت خاص استفاده می‌شوند. قائده اصلی این است که به

فرستندگان اجازه ارسال فراگیر پیام به همه خودروهای در محدوده پوشش رادیویی آن و تصمیم گیری گیرندگان پیام بر اساس یک سری قوانین را می‌دهد. به طور کلی، اولویت ارسال پیام به دورترین خودروی ممکن در محدوده انتقال فرستنده پیام است.

یک پیام امن قبل از دوباره پخشی معرفی شده است به طوری که یک خودرو توانایی تشخیص پیام یکسان را می‌دهد به این معنا که اگر یک خودرو همان پیام مشابه را تشخیص دهد آن خودرو تلاش خود را برای ارسال مجدد آن پیام متوقف می‌کند.

پس در ادامه، ارسال پیام‌های مطمئن از یک خودرو به دیگر خودروها در **DSRC** در شبکه ارتباط نقلیه‌ای از نوع **ad-hoc**، معرفی شده، بررسی و تحلیل می‌شود سپس بهترین پروتکل از میان پروتکل‌های معرفی شده انتخاب می‌شود و بهینه سازی آن مورد بحث قرار خواهد گرفت.

ارتباطات اختصاصی با وسعت کم (**DSRC**) توسط کمیسیون ارتباطات فدرال (**FCC**) برای افزایش امنیت مسافران، کاهش مصرف سوخت و پیشرفت اقتصاد ملی تعیین شده است. این توسعه امید بخش، برای پشتیبانی ارتباط خودرو به خودرو و خودرو به سازمان با استفاده از انواع تکنولوژی **IEEE 802.11A** طراحی شده است. **DSRC**، ارتباطات بحرانی و امن را از قبیل اخطارها تصادم و برخورد، به خوبی دیگر سیستم‌های انتقال هوشمند مانند پرداخت الکترونیکی عوارض، بروز رسانی دیجیتالی نقشه و ... پشتیبانی می‌کند. تنوع **DSRC**، احتمال گسترش را از طریق تنوع صنایع و تایید مشتریان به شدت ارتقاء می‌بخشد.

قانون سال ۲۰۰۴ کمیسیون ارتباطات فدرال مشخص می‌کند که **DSRC**، شش کانال سرویس و یک کانال کنترل دارد. کانال کنترل عموماً توسط تمامی خودروها دیده بانی می‌شوند**FCC**، پیام‌های امنیتی و پیام‌های " امنیت زندگی " را تشخیص و به رسمیت می‌شناسد. پیام‌های امنیت زندگی باید بالاترین اولویت را داشته باشند، خواه توسط خودروها ارسال شده باشند خواه توسط فرستنده‌های کنار جاده‌ای. ارسالات داده‌های غیر امن پایین‌ترین اولویت را دارند.

این مبحث این فرض را که ارتباطات امن در کانال کنترل جای می‌گیرد می‌پذیرد، به علاوه یک واحد ثبت کننده کنار جاده‌ای می‌تواند از کانال کنترل برای آماده کردن وسایل نقلیه برای سرویس و هدایت آنها به یکی از کانال‌های سرویس استفاده کند. برای مثال یک واحد کنار جاده‌ای می‌تواند بروز رسانی دیجیتال یک نقشه محلی را اعلان کند و این اطلاعات را برای جلب توجه وسایل نقلیه در یک کانال سرویس مخابره کند. این مقاله امکان ارسال پیام‌های امنیتی خودرو به خودرو را در کانال کنترل **DSRC** مورد پژوهش قرار می‌دهد.

استدلال کاربردهای امنیتی و میزان ترافیک داده‌ای که ممکن است تولید شوند را برآورد می‌شود، همچنین شاخص‌های مناسب کیفیت سرویس را برای کاربردهای امن ارائه می‌گردد. نهایتاً، مدل تحلیلی شبکه را ساخته می‌شود و در شبیه سازی برای تشخیص امکان پشتیبانی کاربردهای امن بر ارتباط خودرو به خودرو روی امواج رادیویی **802.11A** در منابع اختصاص داده شده توسط **DSRC** تکیه خواهد شد.

در هر دو، شبیه سازی و تجزیه تحلیل از یک مدل سازی ساده تصادم استفاده خواهد شد. چنانچه هر دو گره در محدوده‌ی متداخل همدیگر بسته‌ها را به صورت همزمان ارسال کنند، بسته‌ها گم می‌شوند. (محدوده‌ی متداخل از فرض **Friis** و **Two-ray** اقتباس شده است).

مدل سازی تصادم به صورت گسترده در تحلیل‌های شبکه مورد استفاده قرار گرفته است. این مدل سازی به اندازه کافی برای شبیه سازی با مقیاس بزرگ، ساده است. ما شبکه‌ها را با بیش از ۱۰۰۰ خودروی متحرک شبیه سازی می‌کنیم. این مدل سازی در مدل ساز شبکه **NS-2** انجام شده است. شبیه ساز استفاده شده در اینجا بر اساس **NS-2** می‌باشد.

۲-۴- مرور ادبیات و فناوری‌های مربوط

در شبکه‌های نقلیه‌ای **ad-hoc** ، **TDMA** ، **FDMA** یا **CDMA** اختصاص دینامیک شکاف‌ها، کدها یا کانال‌ها بودن کنترل متمرکز دشوار است. پس اساس طراحی‌ها را دسترسی تصادفی گذارده خواهد شد. **ALOHA** و **CSMA** جدیدترین پروتکل‌های دسترسی تصادفی مورد مطالعه می‌باشند.

MACA ، **MACAW** ، **FAMA** و انواع آن همگی از طرح **RTS/CTS** استفاده می‌کنند.ارتباط فراگیر (**Broadcast**) می‌باشد بنابراین نمی‌توان از **RTS/CTS** استفاده کرد (مطالعه بخش ۲-۵).

در ادبیات، پروتکل‌های بیشتری هستند که از **Qos** (کیفیت سرویس) پشتیبانی می‌کنند اما هیچکدام از آنها برای پیام رسانی نقلیه‌ای مناسب نیست. **HIPERLAN/1** ، " انفجار سیاه (**Black burst**) " و تابع هماهنگی منتشر شده پیشرفته (**EDCF**) **802.11e** ، همگی برای کاهش تأخیر دسترسی ارتباطات حساس به زمان طراحی شده‌اند. **HIPERLAN/1** و **Black burst** برنامه‌ای برای نبرد با ترمینال‌های مخفی ندارد. در **EDCF**، وقتی تعداد بسته‌ای رقیب با اولویت یکسان بالا می‌رود، احتمال تصادم نیز بالا است. که این مورد بحث ارتباطات امن نقلیه‌ای است.

مرجع شماره [۶] یک نگاه کلی بر **DCRS** ارائه می‌دهد و مشخصات لایه‌های **MAC** و فیزیکی **802.11** را تعیین می‌کند. انتظار می‌رود که مشخصات فعلی **802.11** برای اشتراک با تجهیزات **Qos** نیاز به یک اصلاح مناسب پیدا خواهد کرد.

مرجع شماره [۹] (که در پایان این مقاله آمده است) انواع **802.11 DCF** که از **Qos** پشتیبانی می‌کنند را مرور می‌کند. گردآورنده آن نتیجه می‌گیرد که طراحی یک مکانیسم قابل استناد برای **Qos** در یک شبکه‌ی **802.11** هنوز یک مسئله باز است. در اینجا از یک تعریف متفاوت برای **Qos** استفاده می‌شود.

شبکه‌های سلولی برای حرکت خودروها در سرعت بالا به ارتباط حساس به زمان دست پیدا کرده‌اند. اگرچه این کار به کمک مراکز اولیه انجام شده است. مراکز اولیه سلولی به میزان قابل توجهی گرانتر از

معادل **DSRC** آن مثل نقاط دسترسی **802.11** است[5] . به علاوه، کاربردهای سلولی فقط زیر بنای ارتباط متحرک است.

۲-۵- فرمول سازی مسئله

در این بخش مفروضات طراحی را روشن خواهد شد و سپس سطوح داده ترافیکی عرضه شده توسط برنامه‌های امنیتی را برآورده و شاخص‌های کیفیت سرویس (**Qos**) خود را به ترتیب در دو بخش ارائه می‌شود.

بیشترین پیام‌های امنیتی تولید شده توسط یک خودرو برای تعداد زیادی از خودروهای دیگر پر استفاده است. برای مثال پیام توقف یک خودرو برای خودروهای مجاور آن بسیار سودمند است. بنابراین سرویس ارتباط فرا بخش را فرض قرار می‌گیرد.

طراحی بر سرویس ارتباط که قادر به اجرای ارتباط خودرو به خودرو بدون هیچ واحد کنار جاده یا سازمان مرکزی اولیه است محصور خواهد شد مانند یک سرویس تک کاره (**Ad-hoc**). این کار، توسعه را تسهیل می‌کند.

امواج رادیویی **802.11a** برای انتقال مسافتی بین ۲۰۰ تا ۳۰۰ متر طراحی شده است. این مقدار، بالاترین حد در محدوده پیام در جدول یک است. بنابراین یک سرویس ارتباط تکی را پیشنهاد می‌شود. به طور خلاصه، یک سرویس ارتباط تکی را برای پخش فراگیر پیام‌ها زمانی که با تجهیزات **Qos** در شبکه‌های محلی نقلیه‌ای **Ad-hoc** اشتراک پیدا می‌کند، پیشنهاد می‌شود.

[5] **802.11 access Points**

۲-۵-۱- محیط امن DSRC

جدول ۱ این بخش را خلاصه می‌کند. این جدول محدوده‌ها را برای تعیین پارامترها در ترافیک ارائه می‌کند. ارزیابی بر اساس این محدوده‌ها است.

جدول ۲-۴- محدوده‌های پارامتر ترافیک ارائه شده

Message Generation Interval (msec)	50, 100, 200	
Packet Payload Size (Bytes)	100, 250, 400	
Data Rate (Mbps)	6, 9, 12, 18, 24, 36, 48, 54	
Average Vehicle Distance (m)	10 (jammed)	30 (smooth)
Message Range (m)	10-100	30-300
Lane Number	4, 8	

وقتی ترافیک ارائه شده بزرگ است، قابلیت اطمینان، تأخیر و بهره روی کانال را بدتر و خراب‌تر می‌کند. در شبکه‌های سیمی، ترافیک ارائه شده با کل ثانیه/بیت تولید شده توسط تمامی فرستندگان اداره گیری شده است. اگر چه در شبکه‌های بی سیم، شاخص مناسبتر در ترافیک ارائه شده، بیت-متر \ ثانیه است. مثلاً یک شبکه قادر به ارسال یک بیت در ۱۰۰ متر است که ممکن است قادر به ارسال همان بیت در ۲۰۰ متر نباشد. بنابراین ترافیک ارائه شده به نرخ پیام امنیتی (پیام \ ثانیه)، اندازه (پیام \ بایت)، محدوده پیام (متر) و تراکم خودروهای که این پیام‌ها را تولید می‌کنند، بستگی دارد.

استدلال جدول ۲-۴ به شرح زیر است :

یک خودرو در یک آزاد راه با سرعت بالا (۹۰ مایل \ ساعت)، ۲ متر را در لاین خودش طی ۵ میلی ثانیه حرکت می‌کند. این معمولاً یک جابجایی قابل توجه در سرعت بالا نیست . بنابراین تکرار پیام‌های سریعتر از یک‌بار در هر ۵۰ میلی ثانیه برای عرضه اطلاعات مهم جدید، بعید است. به عبارت دیگر یک بروز رسانی آهسته‌تر از هر ۵۰۰ میلی ثانیه احتمالاً خیلی کند است . بنابراین اگر بروز رسانی از هر ۵۰۰ میلی ثانیه

آهسته‌تر شود ممکن است راننده زودتر از سیستم امنیتی متوجه برخی از خرابی‌ها شود. این ممکن است باعث شود که راننده فکر کند که سیستم امنیتی کارآمد نیست.

اندازه پیام‌ها در جدول ۲-۴ برای مجاز کردن موقعیت فرستنده یا گیرنده بر طبق استاندارد **SAE J1746**، کدهای هازارد **NTCIP** ، **GPS** و سر بخش پروتکل استاندارد، انتخاب شده‌اند. پیام‌های امنیتی معمولاً کوتاه هستند . ارتباط در تراکم زیاد وسایل نقلیه بسیار دشوارتر است.۱۰ متر برای خودرو، بزرگراه را گره خورده و متراکم نشان می‌دهد. به علاوه محدوده لاین ۴ به ۸ جاده را وسیع نشان می‌دهد.

محدوده پیام، بیشترین مسافتی که یک پیام می‌تواند دریافت شود را نشان می‌دهد.

برای مثال یک پیام توقف خودرو ممکن است محدوده ۳۰۰ متری داشته باشد، این بدین معنا است که هر وسیله نقلیه در شعاع ۳۰۰ متری فرستنده، پیام را با احتمال بالا دریافت خواهد کرد. طراحان برنامه‌های امنیتی محدوده بزرگ‌تر پیام را به کوچک‌تر آن ترجیح می‌دهند. به عبارت دیگر، محدوده بزرگ‌تر پیام، طراحی شبکه را مشکل‌تر می‌کند. وقتی که جاده متراکم است، خودروهای مجاور نزدیکترند. بنابراین لزومی ندارد که پیام‌های امنیتی با مسافت‌های مشابه ارسال شوند. برای جاده‌های متراکم محدوده‌ی ۱۰۰ متری را فرض قرار می‌گیرد.

۲-۵-۲- مبحث کیفیت سرویس برای پیام‌های امنیتی DSRC

اطمینان از ارتباط در شبکه‌ها عموماً با تکرار ارسال یک پیام تا زمانی که توسط گیرنده تصدیق شود، تعبیر می‌شود. این برای ارسال فایل مناسب است وقتی از دست دادن یک بایت ممکن است خواندن کل فایل را نا ممکن‌کند و عملاً آن فایل غیر قابل استفاده شود . بنابراین پروتکل‌های انتقال مطمئن مانند**TCP**، هر بایت را تصدیق و هر بسته را که به صورت مطلوب دریافت نشده است دوباره ارسال می‌کند.

اگر یک برنامه کاربردی امنیتی بروز رسانی را در هر ۱۰۰ میلی ثانیه انجام دهد و یک پیام ویژه بعد از گذشت ۱۰۰ میلی ثانیه از ساخت آن دریافت نشود، یک پیام جدید، پیام قبلی را که تولید شده بود را از کار

می اندازد. بنابراین روی یک سرویس تحویل پیام ها در مدت عمرشان با احتمال بالا در یک ارتباط محلی متمرکز خواهد شد. برای رسیدن به این مفهوم کیفیت سرویس (**QOS**) احتمال خطای پذیرش (**PRF**) را به شرح زیر تعریف می شود:

تعریف ۱: احتمال خطای یک شبکه نقلیه، **PRF(L,T)**، برای مسافت فرستنده- گیرنده **L** و مدت عمر پیام **T**، احتمالی است که یک پیام ارسال شده به صورت تصادفی توسط یک خودروی اتفاقی توسط یک گیرنده ی اتفاقی در طول مسافت **L** و در زمان **T** دریافت نشده است. در پیش بینی آینده، سیستم‌های امنیتی فعال روی خودرو، راننده را بیشتر از جانشین آن کمک و یاری خواهد کرد.

در زیر بخش ۳-۱ (تحلیل ریاضی) دیده می‌شود که تداخل توسط یک گیرنده وقتی که از فرستنده‌ها بیشتر است بزرگتر است. بدترین حالت زمانی است که فاصله فرستنده- گیرنده، همان محدوده‌ی پیام است. بنابراین همه نتایج **RPF**[6] که در این مقاله نشان داده شد طبق الگوریتم‌های جدول ۲-۴ می‌باشند.

فرض می‌شود که پیام‌های امنیتی روی کانال کنترل ارسال شده‌اند. اگر چه استانداردهای **DSRC** نشان می‌دهد که کانال کنترل برای سودمند شدن کانال‌های باقی مانده باید با سایر پیام‌های غیر امن ارتباط برقرار کند. پروتکل کانال کنترل و انواع گوناگون پیام‌های غیر امن در یک زمان ناشناخته‌اند. بنابراین در عوض مدل سازی صریح پیام‌های غیر امن، بخش زمان تصرف شده کانال کنترل توسط پیام‌های امنیتی ارزیابی خواهد شد. این امر توسط زمان اشغال کانال (**CBT**) شاخص بندی شده است.

CBT به شرح زیر تعریف می‌شود:

یک گره به صورت تصادفی انتخاب می‌شود و در یک محدوده متداخل مجموعه‌ای از گره‌ها قرار می‌گیرد. برای هر دوره زمانی **T** در کانال کنترل، بخشی از آن توسط پیام‌های امنیتی موفق یا نا موفق ارسال شده توسط گره‌های این مجموعه اشغال شده است و بقیه ی زمان تلف خواهد شد. $\mathbf{T_{safety}}$، طول کل دوره زمان‌های **T** اشغال شده توسط پیام‌های امنیتی است.

[6] **Message_range_Message Life_Time**

پس یک تعریف به شرح زیر وجود دارد:

تعریف ۲: زمان اشغال کانال یک شبکه به صورت زیر تعریف می‌شود:

$$CBT \triangleq \frac{T_{safety}}{T} \quad (۴-۲)$$

در شبیه سازی، **T** را به عنوان کل زمان شبیه سازی و **CBT** در نواحی مختلف شبکه برای به دست آوردن شاخص برای کل شبیه سازی در نظر گرفته می‌شود. پس **CBT**، شاخص هزینه‌ی برنامه‌های غیر امن است. به صورت ایده آل هر دو **PRF** و **CBT** باید کم باشند.

۲-۶- طراحی پروتکل

۲-۶-۱- رسیدگی کلی

در یک شبکه بی سیم **Ad-hoc** دو مانع برای اطمینان از پذیرش پیام‌ها وجود دارد. اگر دو فرستنده به صورت همزمان چیزی را در محدوده‌ی متداخل یک گیرنده مشابه ارسال کنند، ارسالات آنها در گیرنده بهم می‌خورد و تصادم رخ می‌دهد. گیرنده هیچ یک از پیام‌ها را دریافت نمی‌کند. یک راه برای مقابله با این مشکل طراحی پروتکل کنترل رسانه (**MAC**) است مانند یک مجموعه قوانین که تصمیم می‌گیرد یک فرستنده، پیامش را ارسال کند یا بیکار بماند.

ثانیاً، حتی اگر تصادمی در کار نباشد، کانال بی سیم ممکن است قدرت فرستنده‌ها را تضعیف کند که این کار توسط نویز حرارتی اتفاق می‌افتد. برای مبارزه با این کار از طریق انتخاب بالای انرژی ارسال برای دسترسی به همه گیرندگان با احتمال بالا وقتی که تصادم نباشد عمل می‌شود. انرژی ارسال توسط قدرت ارسال، فرکانس و کدینگ خطا تعیین می‌شود. امواج رادیویی **DSRC** روی بر اساس امواج **802.11a** می‌باشد. در ارزیابی انجام شده، پارامترهای کنترل انرژی ارسال را برای مدل ارسال رادیویی **802.11a** روی

یک کانال ۲۰ مگا هرتزی در ۵/۴ گیگا هرتز قرار می‌گیرد و روی مسئله طراحی **MAC** تمرکز خواهد شد، مثلاً آیا **MAC** قادر به تحویل پیام‌های امنیتی با قابلیت اطمینان بالا در مدت عمر پیام می‌باشد یا خیر؟

در ارتباط تک پخشی[۷] اطمینان از طریق اعمال سیاست‌ها روی بازخورد گیرنده ارتقاء داده می‌شود مثل **RTS/CTS**، **TCP** یا **WTP**. در این‌ها، فرستنده نیاز دارد تا هویت گیرنده یا گیرند های خودش را یاد بگیرد. وقتی تعداد گیرندگان زیاد است یا شبکه قابلیت تحریک بالایی دارد. معنی مجموعه‌ی گیرندگان می‌تواند به میزانی تغییر کند، یاد گرفتن هویت‌ها ممکن است خود نیازمند ارتباط مهمی شود. بنابراین راه‌های ارزیابی را برای ارتقای اطمینان بدون بازخورد گیرنده را انتخاب می‌شود.

استراتژی‌های مورد نظر این است که هر پیامی را در ترکیب **CSMA** و انواع آن بدون تصدیق، تکرار کند. طرح تکرار پیشنهادی برای پوشش روی **CSMA** طراحی شده است که در ادامه مشخصات طراحی‌های متنوع آن آمده است.

۲-۶-۲- مشخصات پروتکل

شکل ۲-۵، یک نما از ایده‌ی ارسال تکراری است. این شکل دو فرستنده با محدوده متداخل روی یک گیرنده خاص که هر کدام یک پیام را در یک زمان مشابه ارسال می‌کنند را نشان می‌دهد. هر تکرار از هر پیام یک بسته جدید است.

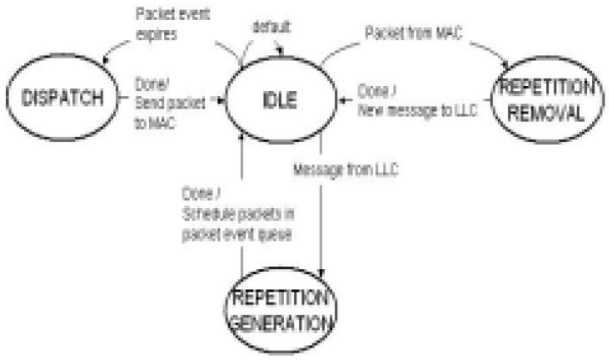
شکل ۲-۵- مفهوم ارسال مکرر

[7] **Unicast**

پروتکل‌های پیشنهادی از دو طرح برای کاهش **PRF** استفاده می‌کنند:

۱. تکرار
۲. احساس ناقل

احساس ناقل که در **MAC 802.11** آمده است. در همه موارد به جزء دو مورد، پروتکل پیشنهادی یک پوشش روی یک **MAC** استاندارد مانند **ALOHA** یا احساس ناقل است. این پوشش را لایه‌ی الحاقی **MAC** می‌شود. لایه‌ی الحاقی **MAC**، بین لایه کنترل پیوند منطقی و لایه **MAC** استاندارد قرار می‌گیرد. قانون و قاعده آن تولید و حذف تکرارها است. ماشین حالت لایه‌ی الحاقی **MAC** در شکل نشان داده شده است. به محض دریافت یک پیام از **LLC** ، **MAC** از حالت بیکار (**Idle**) به تولید تکرار[۸] می‌رود.



شکل ۲-۶- ماشین حالت لایه الحاقی MAC

در این حالت، سیستم تکرار چندگانه‌ی این پیام را در شکاف زمان انتخاب شده در مدت عمر پیام زمان بندی می‌کند. هر تکرار، یک رویداد با شماره شکاف است. تمامی این رویدادها به ترتیب شماره شکاف در صفی به نام صف رویداد بسته قرار می‌گیرند. وقتی که یک صف شکل می‌گیرد، سیستم به حالت **IDEL** (بیکار) بر می‌گردد. هر وقت یک رویداد بسته تمام می‌شود، لایه الحاقی **MAC** به حالت مخابره (**DISPATCH**) می‌رود و بسته را به **MAC** ، می‌فرستند. سپس سیستم به حالت **IDEL** می‌رود.

[8] **REPETITION GENERATION**

هر گاه که لایه الحاق **MAC**، یک بسته را از **MAC** دریافت می‌کند، سیستم از حالت **IDEL** بـه حالـت حذف تکرار[9] می‌رود. اگر شناسه پیام در این بسته قبلاً دیده شده باشد، بسته حذف شده است.

تمامی پروتکل‌های طراحی شده در دو کلاس طبقه بندی می‌شوند:

همزمان و غیر همزمان

۲-۶-۲-۱- پروتکل‌های طراحی شده

۱- تکرار ثابت غیر همزمان (**AFR**)

AFR توسط اختصاص شماره تکرار **.K** پیکر بندی شده است. پروتکل به صورت تصادفی **K** شکاف برتر را از میان **n** شکاف کلی در مدت عمرشان انتخاب می‌کند. این پروتکل "ثابت" نامیده می‌شود زیرا بسته همیـشه در میزان مشخصی از زمان تکرار می‌شود. رادیو قبل از ارسال یک بسته با **AFR** به کانال گوش نمی‌کند.

۲- تکرار ماندگار غیر همزمان (**APR**)

پروتکل تکرار ماندگار ارسال یک بسته در هر **n** شکاف در مدت عمر بـا احتمـال **P=k/n** را تعیـین مـی‌کنـد. **K**، میانگین ارسال یک پیام است. اگر چه برای هر مفهومی، تعداد دقیق تکرارها تغییر می‌کند. ماننـد **AFR**، رادیو قبل از ارسال یک بسته به کانال گوش نمی‌کند.

۳- تکرار ثابت همزمان (**SFR**)

این پروتکل شبیه **AFR** است فقط همه شکاف‌ها در همه گره‌ها با یک ساعت سراسری همزمان شده‌اند.

۴- تکرار ماندگار همزمان (**SPR**)

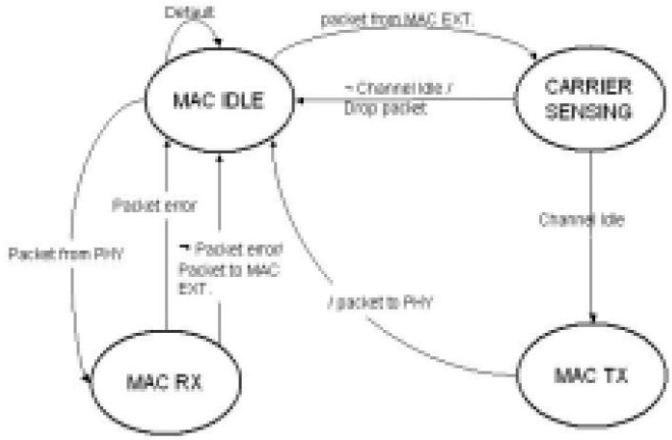
این پروتکل شبیه **APR** است فقط برای همزمان سازی ارسالات توسط همه گـره‌هـا بـه داخـل شـکاف‌هـای عمومی است.

---

[9] **REPETITION REMOVAL**

۵- تکرار ثابت غیر همزمان با احساس ناقل (**AFR-CS**)

AFR-CS، **MAC** مربوط به خودش را دارد که در شکل ۲-۷ نشان داده شده است.



شکل ۲-۷- ماشین حالت لایه MAC در پروتکل AFR-CS

AFR-CS، تکرارها را از راه مشابه موجود در **AFR** تولید می‌کند.

هر وقت که یک بسته از لایه الحاق **MAC** پاس می‌شود، **MAC** از حالت **IDLE** به حالت احساس ناقل می‌رود. در حالت احساس ناقل[10] ، سیستم وضعیت کانال را با استفاده از احساس ناقل بررسی می‌کند. اگر کانال مشغول باشد، سیستم بسته را رها می‌کند و به حالت **IDLE** می‌رود. اگر کانال بیکار باشد سیستم به حالت **MAC TX** می‌رود و بسته را به لایه فیزیکی باز می‌گرداند و سپس به حالت **MAC IDLE** باز می‌گردد. در **MAC IDLE**، اگر لایه فیزیکی یک بسته را به بالا هدایت کند، سیستم به حالت **MAC RX** رفته و بی عیب بودن بسته را بررسی می‌کند. اگر بسته ناقص باشد سیستم آن را رها کرده و به حالت **IDLE** می‌رود. در غیر این صورت، بسته به لایه‌ی بالایی که لایه‌ی الحاقی **MAC** است سپرده می‌شود و سیستم به حالت **MAC IDLE** باز می‌گردد.

۶- تکرار ماندگار غیر همزمان با احساس ناقل (**APR-CS**)

این همانند **AFR-CS** است فقط اینکه شکاف‌ها برای تکرار پیام در نوع ماندگار انتخاب شده‌اند.

---

[10] **CARRER SENSING**

فصل سوم

روش‌های ارزیابی و نتایج حاصله

- تحلیل ریاضی
- شبیه سازی
- نتایج ارزیابی

فصل سوم- روش‌های ارزیابی و نتایج حاصله

دو روش ارزیابی داریم : آنالیز ریاضی و شبیه سازی

از نتایج ریاضیاتی برای یک درک کیفی از آنچه که شبیه ساز ممکن است نمایش دهد، استفاده می‌شود. از بیان ریاضی همچنین برای انتخاب بخش‌هایی از فضای پارامتر برای شبیه سازی متمرکز استفاده می‌شود.

۳-۱- تحلیل ریاضی

برای پروتکل‌های **SPR** و **APR**، بیان ریاضی را برای احتمال خطای پذیرش ارائه می‌شود. این بیانات ریاضی می‌توانند توسط نرم افزار **Matlab** پردازش شوند. فرض می‌شود پروسه تولید پیام یک توزیع پوآسن است. پروسه پوآسن یک مقدار قریب به صحت عدد بزرگ پردازش‌های دوره‌ای مستقل با فاصله و زمان شروع متفاوت است.

بیشتر فرض می‌شود که پروسه تولید پیام در خودروهای مختلف، از هم مستقل هستند. در آن حالت پروسه تولید پیام تمامی خودروها با یک محدوده گیرنده متداخل در نهایت یک توزیع پوآسن می‌باشد. هر چند ترافیک شبکه مرکب از تکرار پیام‌ها است، این‌ها فقط در مدت عمر پیام اتفاق می‌افتد بنابراین پردازش

نهایی بسته روی کانال، پوآسن نمی‌باشد. پس نا مساوی زیـر کـران‌هـای بـالا و پـایین روی **PRF** و **SPR** را می‌دهد:

$$\left(1-\frac{k}{n}e^{-m\lambda\tau\frac{k}{n}}\right)^{n} < P(\neg S) < \left(1-\frac{k}{n}e^{-m\lambda\tau\frac{k}{n}}+\frac{k}{n}e^{-m\lambda\tau}\right)^{n} \quad (۳-۱).$$

برای پروتکل **APR** و **PRF** یک گیرنده با **m** تداخل، نا مساوی زیر را ارائه می‌دهد:

$$\left(1-\frac{k}{n}e^{-m\lambda\tau\left[2\frac{k}{n}-\frac{k^2}{n^2}\right]}\right)^{n} < P(\neg S) < \left(1-\frac{k}{n}e^{-m\lambda\tau\left[2\frac{k}{n}-\frac{k^2}{n^2}\right]}+\frac{k}{n}e^{-m\lambda\tau}\right)^{n} \quad (۳-۲)$$

n : تعداد کلی شکاف

k : تعداد تکرارها برای پیام (مقدار میانگین برای پروتکل‌های ماندگار و مقدار دقیق برای پروتکل‌هـای تکـرار ثابت)

s : رویدادی است که حداقل یکی از تکرارها موفق شود.

t : مدت عمر پیام

λ : نرخ تولید پیام در هر گره منحصر به فرد

m : تعداد کلی مداخلات در اطراف یک گیرنده باشد.

در هر دو **SPR** و **APR**، کران‌ها کاملاً روی محدوده ترافیک ارائه شده در جدول ۱ محکم شده‌اند. در ادامه این مقاله، نتایج تحلیلی را بـا طـرف راسـت هـر دو معادلـه‌هـا نـشان مـی‌دهـیم. نقـشه متنـاظر بـرای طرف‌های چپ غیر قابل تشخیص است.

تعداد **m** مداخله گر در معادله‌های بالا به صورت زیر محاسبه می‌شود:

$$\text{تعداد مداخله گر} = \frac{\text{شماره لاین} \times \text{محدوده تداخل} \times ۲}{\text{متر بر خودرو}}$$

۳-۲- شبیه سازی

یک شبیه ساز **DSRC** را ارائه می شود که این شبیه ساز خودش بر اساس دو شبیه ساز دیگر به نام‌های **SHIFT** و **NS-2** است.

SHIFT یک شبیه ساز ترافیک تولید شده مناسب است که مسیر راندن خودروها را بر اساس مدل‌های معتبر شبکه‌های جاده‌ای واقعی نشان می‌دهد. شکل ۳-۱ یک تصویر از ترافیک شبیه سازی توسط **SHIFT** می‌باشد. از **SHIFT** برای تولید حرکت امواج رادیویی استفاده خواهد شد. این حرکت به عنوان ورودی در **NS-2** استفاده می‌شود.

NS-2 یک شبیه ساز شبکه منبع باز[11] است که به صورت گسترده در انجمن آکادمی استفاده شده است. **NS-2**، ترافیک را تولید می‌کند، ارسال و پذیرش‌ها را شبیه سازی می‌کند و داده پذیرش بسته را به خروجی می‌دهد. سپس داده را برای به دست آوردن مدت اشغال کانال، احتمال خطای پذیرش و احتمال انفجارهای طولانی مورد استفاده قرار می‌گیرد.

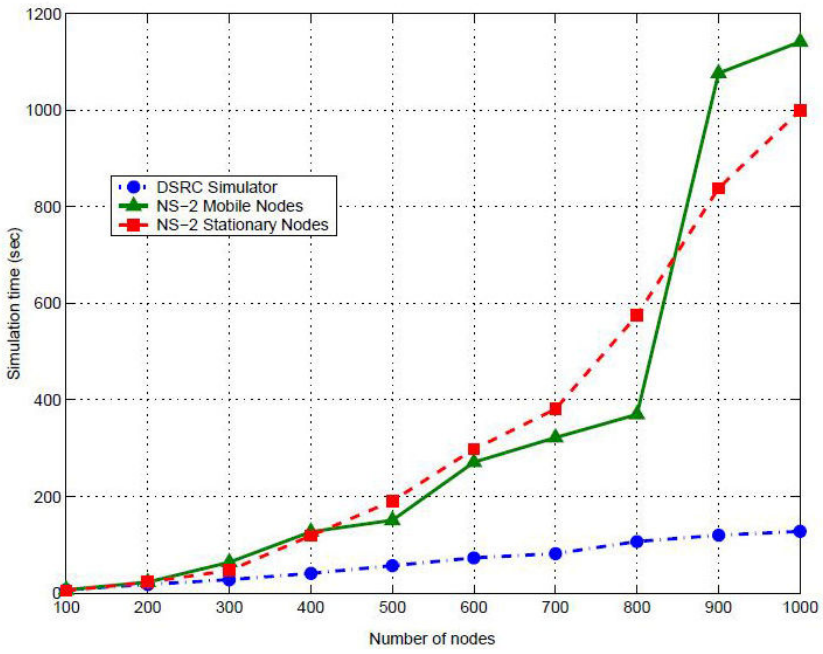
شکل ۳-۱- یک نمای ترافیک کلی در SHIFT

[11] **Open source**

بنابراین شبیه ساز **DSRC** نسخه‌ی استاندارد **NS-2** می‌باشد به اضافه :

- **SHIFT**
- مدل رادیویی برای **802.11 a** در ۵/۴ گیگا هرتزی
- پروتکل‌های تکرار
- یک ساختار داده‌ای متفاوت که زمان اجرای **NS-2** را از درجه دوم به خطی در تعداد گره‌ها تغییر می‌دهد.

شکل ۳-۲، مقایسه زمان اجرا را نمایش می‌دهد. این افزایش و پیشرفت ما را برای شبیه سازی شبکه‌های با بیش از هزار خودرو قادر می‌سازد.



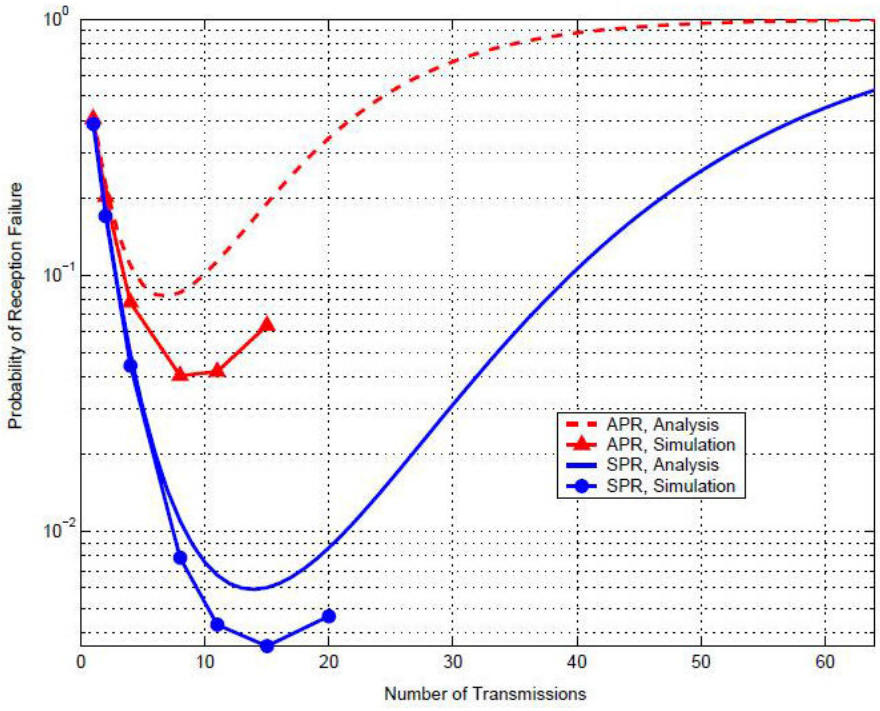
شکل ۳-۲- بهبود مقیاس پذیری در شبیه ساز NS-2

از مدل قطعی **Friis** برای مسافت‌های کوتاه و از مدل **Two-ray** برای مسافت‌های طولانی‌تر برای تعیین نیروی دریافت شده استفاده می‌شود. اگر مسافت بین آنتن فرستنده و گیرنده **d** باشد، نیروی سیگنال وقتی که مسافت کوتاه باشد $\mathbf{d^2}$ و وقتی مسافت زیاد باشد $\mathbf{d^4}$ است.

۳-۳- نتایج ارزیابی

ترافیک‌های ارائه شده مشابه بررسی شد، تعداد تکرار **K**، نیروی ارسال، نرخ داده و اندازه بسته برای همه گره‌ها یکسان است. در تحلیل‌های ریاضی فرض می‌شود فاصله بین خودروها یکسان است و در شبیه سازی میانگین جریان بزرگراه را در نظر گرفته می‌شود.

شکل ۳-۳، تحلیل و **PRF** شبیه سازی شده برای پروتکل‌های **APR** و **SPR** برای مقادیر اسمی جدول ۳-۱ را نشان می‌دهد طرح‌های تحلیلی از نا مساوی‌ها آمده‌اند. نتایج تحلیلی و شبیه سازی به خوبی با هم می‌خوانند (با هم **Match** می‌شوند).



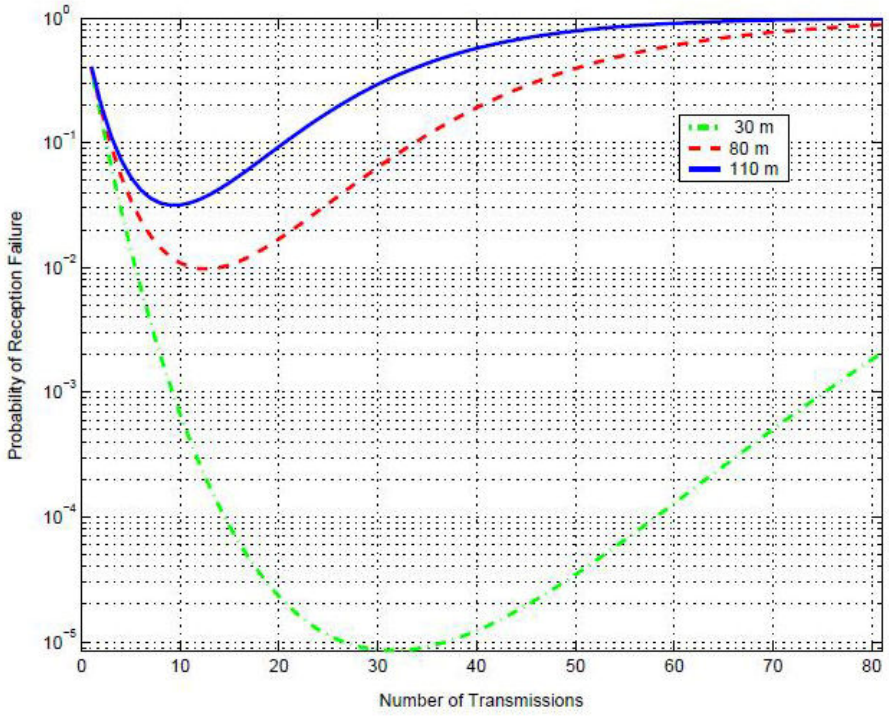
شکل ۳-۳- تصدیق نتایج شبیه سازی با مدل تحلیلی

هر چه تعداد تکرارها افزایش پیدا کند، مجموع تصادم‌ها بالا می‌رود. (شکل ۳-۵ این را تایید می‌کند)

در هر دو، تحلیل و شبیه سازی یک تعداد تکرار بهینه وجود دارد. این مقدار بهینه برای انواع متفاوت محدوده پیام، نرخ تولید پیام، تراکم ترافیکی خودرو، اندازه پیام و متفاوت است. شکل ۳-۴، ناپایداری تعداد تکرار بهینه و حداقل **PRF** با محدوده پیام را نشان می‌دهد. بقیه پارامترها مانند جدول ۳-۱ می‌باشد.

با توجه به این دلایل نتایج شبیه سازی در شکل ۳-۳ آمده است از نوع تحلیلی آن سازگارتر است. زمانی که پروسه تولید پیام بیشتر پوآسن است تا دوره‌ای، مدت عمر دو یا چند پیام متوالی از یک گره مشابه می‌تواند همپوشانی شود. پیام تکرار شده از روی پیام قبلی می‌تواند با یک شکاف زمان مشابه برای ارسال مانند بسته‌های قبلی پیام انتخاب شود.

در تحلیل ریاضی، پیام قبلی را مانند پیام‌های مشابه از سایر گره‌ها مورد بحث قرار می‌گیرد یعنی بسته‌های پیام قبلی گره می‌تواند با بسته‌های پیام اخیرش تصادم داشته باشد. در شبیه سازی، بسته‌های پیام قبلی هر تصادمی را با بسته‌های پیام جدید بازنویسی می‌کند. این به واقعیت نزدیک‌تر است، بنابراین می‌توان کار آرایی و بازدهی قابل توجهی را در شبیه سازی دید.



شکل ۳-۴- احتمال خطای پذیرش در محدوده‌های مختلف پیام

جدول ۳-۱- پارامترهای اسمی تنظیم

Message Generation Interval (msec)	100
Useful Life Time (msec)	100
Packet Payload Size (Bytes)	100
Message Range (m)	80
Average Distance Between Vehicles (m)	30
Lane Number	4

شکل ۳-۵، کارایی پروتکل‌ها را به صورت کاربرد تعداد تکرار نشان می‌دهد، بقیه پارامترها در جدول ۳-۱ آمده است. خطوط منحنی بر اساس خروجی شبیه ساز **DSRC** رسم شده‌اند. پارامترهای **CSMA** (مثل **DIFS**) مقادیر نشان را در **802.11** شان به طور ثابت حفظ کرده‌اند. طبق مبحثی که در آینده به اختصار توضیح داده می‌شود، یک نرخ داده بهینه شده طبق تنظیماتش برای یک پروتکل وجود دارد. در این شکل نتایج شبیه سازی برای تمامی پروتکل‌ها را با نرخ بهینه‌ی آنها نمایش داده شده است.

بهترین پروتکل‌ها **AFR-CS , SPR** هستند.

SFR به یک زیر ساخت همگام سازی ساعت (**clock**) نیاز دارد. بنابراین **AFR-CS** راه حل بهتری است. به یاد داشته باشید که بهبود **PRF** روی **802.11a** یک مزیت حساب می‌آید. این نشان می‌دهد که تکرار، با دادن شانس بیشتر برای ارسال به فرستنده و امکان ارسال متضاد گره‌ها در زمان‌های متفاوت به مبارزه با تداخل کمک می‌کند.

کارایی بهتر پروتکل **AFR-CS** در مقایسه با **802.11** نشان می‌دهد که سبک کردن تکرار ترمینال مخفی حتی بدون استفاده از **RTS-CS** روی کانال فشار وارد می‌کند. واضح است که برای متدهای تکرار یکسان (تکرار ثابت یا تکرار ماندگار) پروتکل‌های همزمان بهتر از پروتکل‌های غیر همزمان عمل می‌کنند. پروتکل‌های همزمان همپوشانی‌های جزئی بین بسته‌های گره‌های متفاوت را از بین می‌برد.

این نظریه با نتایج قبلی روی **ALOHA** شکاف بندی شده و شکاف بندی نشده موافق است. همچنین برای متدهای تکرار یکسان یک پروتکل **CSMA** بهتر از پروتکل غیر **CSMA** می‌باشد. **CSMA** قبلا از هر ارسال به خط گوش می‌دهد تا از هر تصادمی جلوگیری کند. خطاهای پذیرش **CSMA** بیشتر به خاطر ترمینال‌های مخفی است.

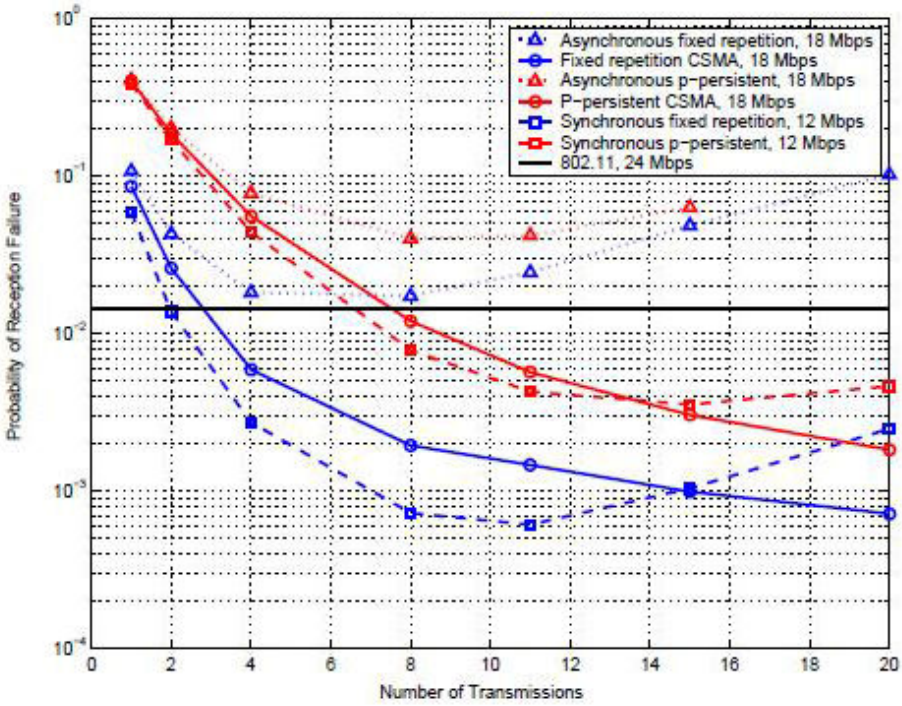
پروتکل‌های تکرار ثابت از پروتکل‌های ماندگار بهتر عمل می‌کنند، به این دلیل که پروتکل‌های تکرار ثابت در نگهداری تعداد تکرارها برای هر پیام بهتر هستند یعنی نوسان کمتری بین مقدار واقعی تکرار و مقدار پیش بینی شده وجود دارد. تنوع زیاد موارد ماندگار از ارزش آنها می‌کاهد.

این نتیجه بر گرفته می‌شود که وقتی پیامی بر اثر ارسال متوالی از دست می‌رود نسبت به زمانی که پیامی را با توالی کمتر از دست می‌رود، منفعت کمتری دارد.

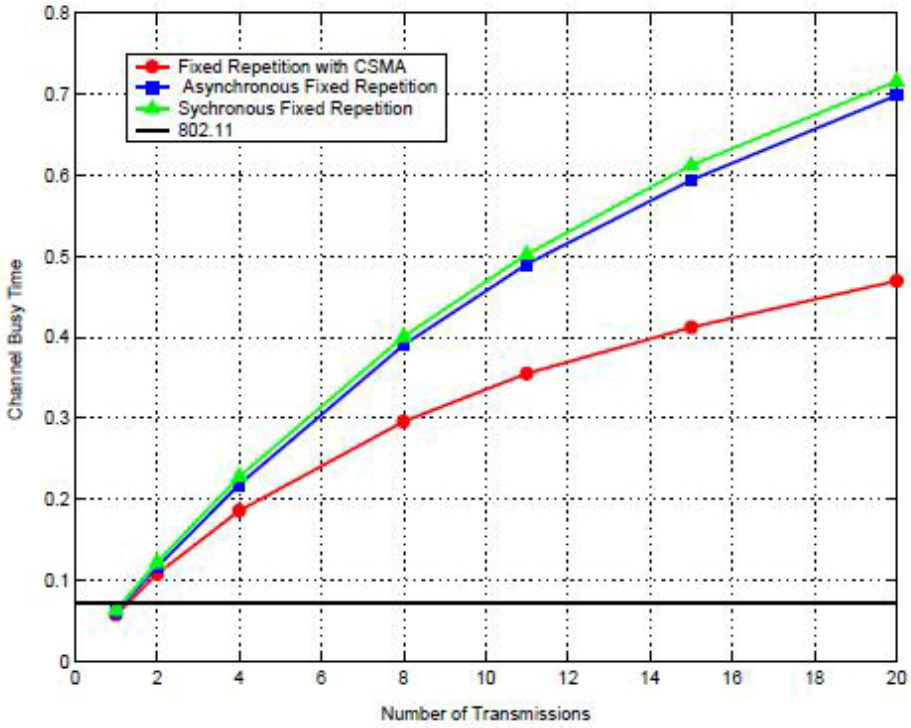
شکل ۳-۶ یک طرح **CBT** در مقابل تعداد تکرار برای دو پروتکل را نشان می‌دهد. این شکل نشان می‌دهد که **CBT** به تناسب تعداد تکرار، افزایش می‌یابد. با تعداد تکرار یکسان، **AFR-CS** نسبت به دیگر پروتکل‌های پیشنهاد شده، **CBT** کمتری دارد.

تعجبی ندارد که **802.11** زمانی که تکرار ندارد، **CBT** کمی دارد. این طرح و نقشه‌ها طبق پارامترهای اسمی موجود در جدول ۳-۱ است. بنابراین در ادامه ارزیابی از **AFR-CS** استفاده می‌شود. در شکل ۳-۵، **PRF** پروتکل **AFR-CS** با تعداد ارسال رو به کاهش است. در آزمایش بعدی، تعداد تکرار را بالا برده می‌شود و دیده می‌شود که به نسبت دیگر پروتکل‌ها، پروتکل **AFR-CS** احتمال خطای پذیرش آن با حجم زیادی از تعداد تکرارها، افزایش پیدا نمی‌کند. از نمایش این نتایج صرف نظر شده است.

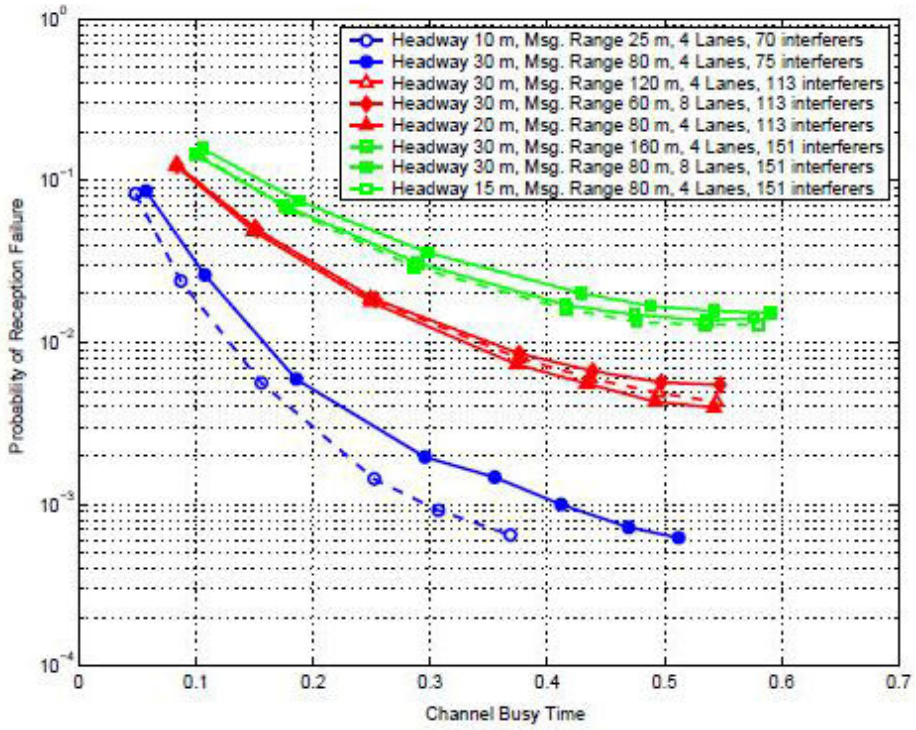
زمان اشغال کانال یک شاخص برای تقسیم بندی ظرفیت باقیمانده کانال برای پیام‌های غیر امن است. برای تعداد تکرار بهینه برای **CBT** و **PRF** یک رابطه معکوس وجود دارد. شکل ۳-۷ این سبک سنگین را نشان می‌دهد.



شکل ۳-۵- احتمال خطای پذیرش در تنظیمات اسمی پروتکل‌های پیشنهاد شده



شکل ۳-۶- زمان اشغال کانال در تنظیمات اسمی



شکل ۳-۷- کارایی پروتکل AFR-CS

جدول ۳-۲- نرخ داده بهینه را برای تمامی پروتکل‌ها با تنظیمات پارامتری

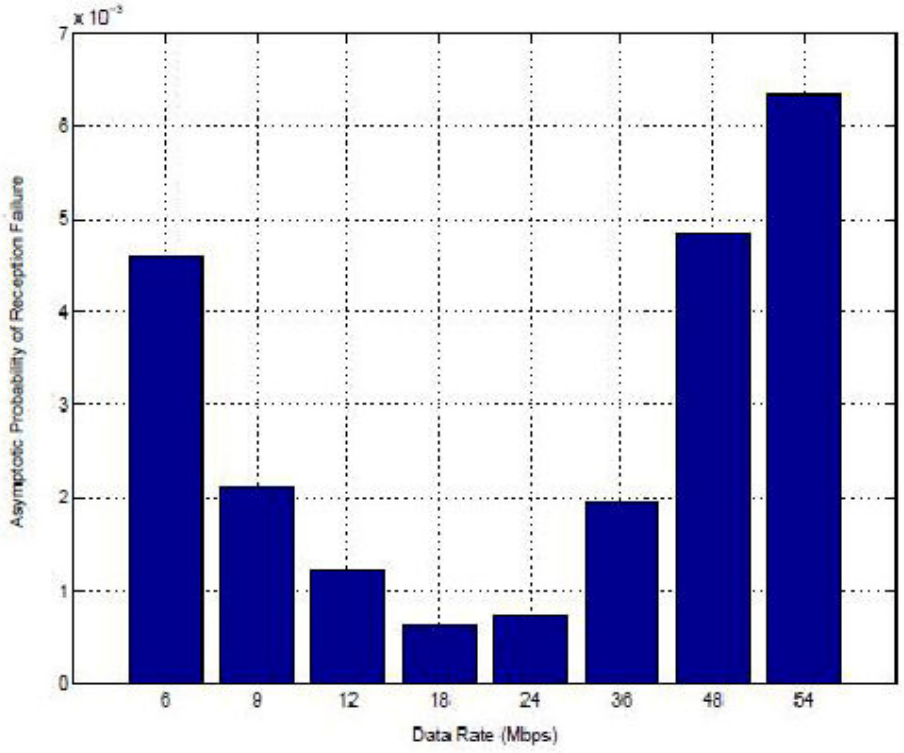
Protocol	Optimal Data Rate (Mbps)
SFR	12
AFR	18
SPR	12
APR	18
APR-CS	18
AFR-CS	18
802.11	24

وقتی که کیفیت سرویس در برنامه‌های امنیتی بالا می‌رود، در دیگر برنامه‌های کنترل کانال، کاهش می‌یابد. بنابراین این خطوط منحنی یک راه مناسب برای ارزیابی کارایی پروتکل‌ها هستند.

معادله‌های نا مساوی کارایی وابسته به تعداد مداخلات را نشان می‌دهد. در شبیه سازی واقعی ترافیک ، این رقم به الگوهای پیچیده‌ای در می‌آید. شکل ۳-۷ نشان می‌دهد که برای ارسال با زمان کوتاه، پویایی

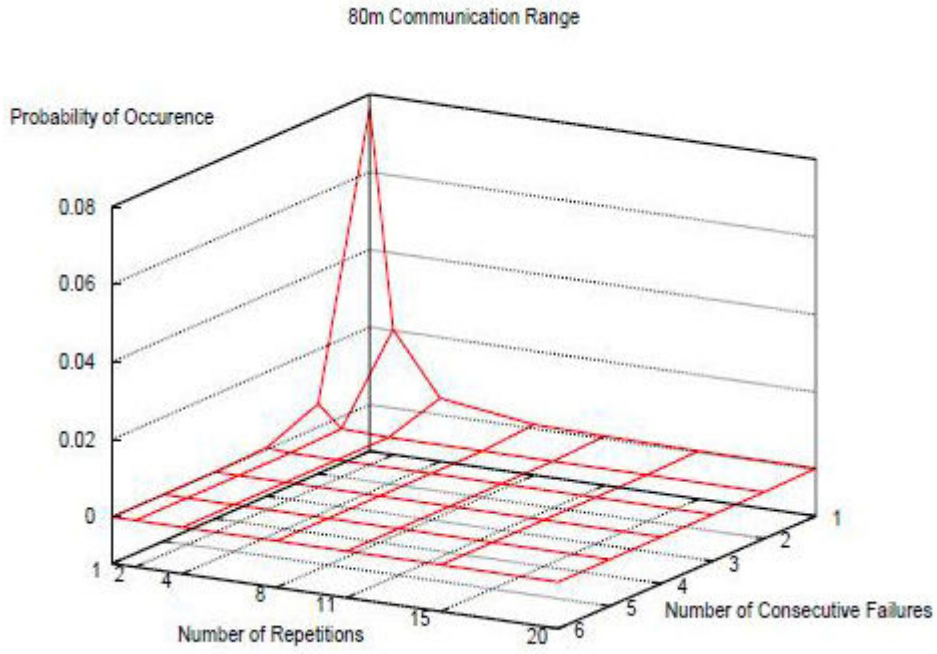
توپولوژی تقریباً اختلاف ی برای کارایی کل شبکه به وجود نمی‌آورد. بر اساس شکل ۳-۷، منحنی ۳۰ متری با محدوده پیام ۶۰ متر و تعداد لاین ۸ با منحنی ۲۰ متری با محدوده پیام ۸۰ متر و تعداد لاین ۴ برخورد کرده است چرا که هر دو انها بر اساس محاسبه توسط فرمول (تعداد **m** مداخله گر) یک مقدار مداخله مشابه را نتیجه داده‌اند یعنی ۱۱۳.

شواهد نشان می‌دهد که برای هر تعداد تکرار و هر تعداد مداخلات یک نرخ داده بهینه وجود دارد. اگر نرخ ارسال بالا رود، زمان ارسال و به نسبت آن احتمال تصادم کاهش می‌یابد. به عبارت دیگر، نیروی لازم برای پوشش محدوده پیام معمولاً بالا می‌رود، در نتیجه، تعداد مداخلات نیز بالا می‌رود. شکل ۳-۸ این قضیه را برای پروتکل **AFR-CS** با پارامترهای اسمی جدول ۳-۱ نشان می‌دهد. جدول ۳-۲، نرخ داده بهینه را برای تمامی پروتکل‌ها با تنظیمات پارامتری نشان می‌دهد.



شکل ۳-۸- احتمال خطای پذیرش برای انواع نرخ داده با تنظیمات اسمی در پورت کل AFR-CS

شکل ۳-۹، احتمال انفجار خطاهای مسافت‌های متفاوت برای پارامترهای اسمی جدول ۳-۱ را نشان می‌دهد. احتمالات کوچک هستند، این به خاطر خاصیت بدون حافظه[۱۲] بدون کانال در شبیه سازی است. احتمال دیدن دو یا چند خطای متوالی توسط گیرنده، جزئی یا نا چیز است که این برای برآورده کردن خوب است.

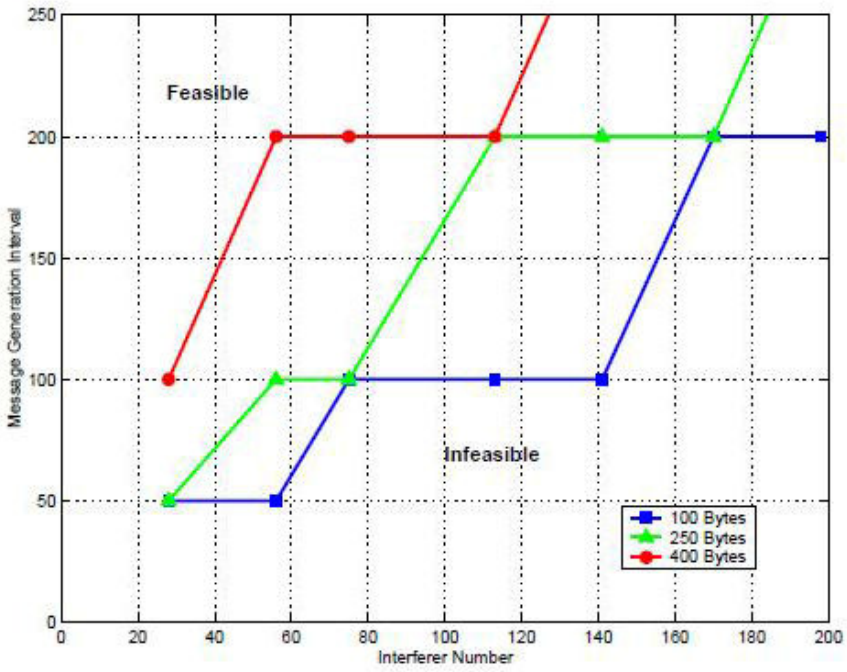


شکل ۳-۹- احتمال انفجار خطای پیام در مقابل تعداد تکرار برای پروتکل AFR-CS

شکل ۳-۱۰، تمامی این نتایج را با هم برای رسیدن به امکان پشتیبانی برنامه‌های امنیتی روی کانال کنترل استفاده می‌کند. این امکان بستگی به تجهیزات **PRF** و **CBT** دارد. تجهیزات **PRF** و **CBT** داده شده و ترکیبی از مقادیر پارامترهای جدول ۲-۴ داده شده‌اند، این مدل شبیه سازی می‌تواند هر تجهیزاتی را نشان دهد. این کار با فرض پروتکل **AFR-CS** و بهینه سازی پروتکل برای تعداد تکرار، نرخ ارسال و انتخاب مدل سازی و نرخ کد برای به حداقل رساندن نیروی لازم برای پوشش محدوده پیام، انجام می‌گیرد.

[12] **Memory Less**

شکل ۳-۱۰، این امکان را برای یک **PRF** کمتر از یک صد و یک **CBT** کمتر از پنجـاه درصـد را نـشان می‌دهد. مثلاً : نرخ پیام ۲۰۰ میلی ثانیه‌ای و ۲۵۰ بایت پیام در ۱۴۰ مداخله، امکان پذیر است.



شکل ۳-۱۰- نواحی ممکن برای CBT < 50% و PRF < 0/01 در پروتکل AFR-CS

فصل چهارم

نتیجه گیری و پیشنهادات

- نتیجه گیری
- پیشنهادات

فصل چهارم- نتیجه گیری و پیشنهادات

۴-۱- نتیجه گیری

در این پایان نامه، یک متد کارآمد برای امنیت پیام امن پیشنهاد شده و مسائل و مشکلات پیاده سازی آن بر طرف شد. نخست، روش‌های پیشنهاد شده را به دو دسته اصلی روش‌های که بر امضاء گروه بر انتخاب یک مدیر گروه پویا تکیه دارد (روش‌های پویا) و روش‌های که از یک زیر ساخت ثابت برای مدیریت کلید استفاده می‌کند (روش‌های ثابت) تقسیم گردید. که با توجه به ارزیابی‌ها یک زیرساخت کلید ثابت که اضافه بار و تأخیر کمتری دارد انتخاب شد. این زیرساخت چندین منطقه ثابت با مدیر مرکزی که **CA** نامیده می‌شود را دارا می‌باشد که کلیدهای مخصوص به خودش را برای تعیین و واگذاری هر خودرو در اختیار دارد.

مهم‌ترین مشکل در این زیر ساخت، تبادل کلید در کرانه‌های بین منطقه‌ها است. در این پایان نامه، این مشکل از طریق اطلاع رسانی خودروها برای دریافت کلید جدید، مرتفع شد. در این روش خودروها قبل از اینکه وارد منطقه‌ی جدید شوند به وسیله **CA** جاری یا خود خودروها از تغییر منطقه با خبر می‌شوند. با استفاده از این راه حل، از بسیاری از حملاتی که ممکن است در این نقاط رخ دهد دوری می‌شود و از هرگونه بی اعتباری ممکن برای خودروها جلوگیری خواهد شد. همچنین یک فرمت امن برای پیام تبادل کلید از طریق کلیدهای مشابه برای امنیت پیام امن، پیشنهاد شد.

در آخر، روش پیشنهادی (**SAB** توسعه یافته) از طریق پایداری در برابر حملات، تأخیر زمانی، معیارهای سرآمد و مقایسه آن با دیگر روش‌ها مورد ارزیابی قرار گرفت. در این پایان نامه، بیشتر به امنیت پیام امن مبتنی بر زیرساخت کلید ثابت پرداخته شد و بعضی مسائل چالش برانگیز حل شد. بنابراین، کاربردهای امنیت در دیگر مسائل مثل ارتباطات هوشمند، اطلاعات ترافیکی مبتنی بر این زیرساخت کلید ثابت ممکن است برای فعالیت‌های آینده حائز اهمیت باشد.

در ادامه نیز پروتکل‌های مربوط به ارتباطات از نوع **DSRC** که در لایه پایینی از زیر ساخت معماری شبکه **VANET** قرار دارد به منظور بررسی پیام رسانی امن خودرو به خودرو مورد بحث قرار گرفت. که نتایج و زیر به دست آمد:

امکان تبادل پیام‌های امنیتی بین خودروها در استاندارد **802.11a** ارزیابی و بررسی شده و مشخص شد این تکنولوژی نمی‌تواند زمان را برای انتشار پیام بحرانی در محیط ترافیکی متراکم یا کانال با بار بالا تأمین و تضمین کند. پس ارسال پیام‌های امن در **DSRC** در شبکه ارتباط نقلیه‌ای از نوع **ad-hoc**، معرفی شد، سپس بهترین پروتکل از میان پروتکل‌های معرفی شده انتخاب شد و بهینه سازی آن مورد بحث قرار گرفت. محدوده‌های قابل قبول را برای ترافیک امن ارائه شده مورد ارزیابی قرار گرفت و دو شاخص **PRF** و **CBT** را برای کیفیت سرویس ارائه شد.

- **PRF**، کیفیت سرویس تجربه شده توسط برنامه‌های امنیتی است، که مقدار کم آن بهتر است. پروتکل‌های پیشنهادی از دو طرح برای کاهش **PRF** استفاده می‌کنند: تکرار و احساس ناقل

- **CBT**، مورد علاقه است چرا که انتظار می‌رود کانال با بقیه پیام‌های غیر امنیتی به صورت اشتراکی استفاده شود. به عبارت دیگر **CBT**، شاخص پتانسیل همساز کردن این پیام‌ها است، که مقدار کم آن نیز بهتر است.

با مشاهده شکل ۳-۱۰ با مقادیر ۲۰۰ میلی ثانیه، نقطه ۱۴۰ مداخله و ۲۵۰ بایت حاصل می‌شود که زمان عکس‌العمل راننده در موقعیت‌های تصادفی که رفع می‌شود ۰/۷ ثانیه یا بیشتر است که این به یک سیستم امنیتی سرخود اشاره می‌کند که باید کادر به تشخیص هر چه سریع‌تر موقعیت و ارائه یک مساعدت

و کمک به موقع باشد. به علاوه، اطلاعات موقعیت خودرو در پیام‌های امنیتی از طریق **GPS** صادر می‌شود که معمولاً زودتر از ۵ هرتز به روز رسانی نمی‌شود. اندازه ۲۵۰ بایت برای پیام مناسب است، تعداد ۱۴۰ مداخله برای یک بزرگراه با ۴ لاین با سرعت بین ۵۰ تا ۵۵ مایل بر ساعت و یک محدوده پیام ۱۵۰ متری برابر است. در این سرعتتقریباً همه خودروهای مسافربری قادر به توقف در ۱۵۰ متری هستند. بنابراین این که مقدار مناسب، برای محدوده پیام است. طراحان سیستم امنیتی یک شانس برای طراحی سیستم‌های امنیتی با این محدودیت‌ها دارند.

همچنین وقتی‌یک بزرگراه متراکم است، مثلاً میانگین تراکم ۱۵ متر بر خودرو باشد، یک پیام با محدوده ۸۰ متری، ۵ خودرو را در هر دو سمت پوشش می‌دهد. بنابراین در این نقطه، یک **PRF** با مقدار ۰/۰۱ یا کمتر امکان پذیر است. احتمال گم کردن‌های متوالی، یکی از دلایل کاهش محبوبیت است. اما به کنترل سازگار کننده در لایه های فیزیکی و **MAC** ارتباطات فرا بخش[۱۳] نیاز است. اکثر طرح‌های کنترل سازگار کننده به بازخورد گیرنده بستگی دارد. این یک مسئله مهم در ارتباطات فرا پخشی است.

این تحلیل‌ها چندین محدودیت دارد، مدل کانال بدون حافظه است. اگر یک کامیون بین دو خودرو ظاهر شود و همانجا بماند، برای چندین ثانیه ارتباط را قطع می‌کند، بنابراین احتمالات خطاهای پی رد پی نسبت به احتمالات پیش بینی شده در این تحلیل‌ها و وخیم‌تر می‌شود. بنابراین خصوصیات کانال خودرو به خودرو نیاز به تفهیم و آموزش بهتر دارد. همچنین **CBT** تنها یک مفهوم غیر مستقیم برای تخمین ترافیک غیر امن است.

[13] **Broad Cast**

۴-۲- پیشنهادات

جدول ۳-۱، برآوردی از ترافیک داده‌ای که ممکن است توسط طراحان برنامه‌های امنیتی ارائه شود را نشان می‌دهد:

- اولین کشف این است که تمامی محدوده‌ها امکان پذیر نیستند. **PRF** ها در بعضی مقادیر بسیار بالا می‌رود. (۰/۱ یا بیشتر).
- کشف دوم این است که پیشنهاد می‌شود اگر طراحان شبکه و طراحان برنامه‌های امنیتی با هم کار کنند، بعضی سطوح ترافیک ارائه شده، امکان پذیر است.

ارتباط **DSRC** نیاز به توصیف دیگر کلاس‌های ترافیک دارد. این کار امکان مطالعه بهتر را فراهم می‌آورد. علاوه بر این ترافیک امن، خود به چندین کلاس متفاوت دسته بندی می‌شود. پیشنهاد می‌شود کلاس‌های چندگانه ترافیک امن، مدل سازی گردد و آنالیزهای بیشتری روی آنها صورت گرفته و ارزیابی کیفیت سرویس را برای هر کلاس انجام گیرد.

منابع

[1] Anjum F, Mouchtaris P**,** ***"Security For Wireless Ad Hoc Networks",*** Wiley-Interscience Publishing, chapter 8, IEEE 2007**.**

[2] C. Harsch, A. Festag, and P. Papadimitratos**,** ***"Secure Position-Based Routing for VANETs",*** 2007 IEEE 66th Vehicular Technology Conference (VTC 2007), September 2007.

[3] G. Anastasi, L. Lanzini, and E. Mingozzi**.** ***"HIPERLAN/1 MAC protocol: stability and performance analysis. IEEE Journal on Selected Areas in Communications"*****,** 18(9):1787–1798, September 2000.

[4] Q. Xu. Control**,** ***"Estimation and Communication Design Applied to Vehicle Safety Systems. PhD thesis"*****,** University of California at Berkeley, 2004.

[5] M. Raya and J. P. Hubaux**, "***Securing vehicular ad hoc networks, Journal of Computer Security***",** Vol. 15, No. 1, pp. 39-68, 2007

[6] J. Zhu and S. Roy**.** ***"MAC for Dedicated Short Range Communications in Intelligent Transporation System".*** IEEE Communications Magazine, pages 60–67**,** December 2003**.**

[7] C. Harsch, A. Festag, and P. Papadimitratos**,** ***"Secure Position-Based Routing for VANETs"*****,** 2007 IEEE 66th Vehicular Technology Conference (VTC 2007), September 2007.

[8] J. Sobrinho and A. Krishnakumar**,** ***"Quality-of-service in ad hoc carrier sense multiple access wireless networks***". IEEE Journal on Selected Areas in Communications, 17(8):1353–1368, August 1999**.**

[9] W. Pattra-Atikom, P. Krishnamurthy, and S. Banerjee, ***"Distributed mechanisms for quality of serivce in wireless LAN".*** IEEE Wireless Communications, pages 26–34, June 2003.

[10] Yong Xi, Kewei Sha, Weisong Shi, Loren Schwiebert, Tao Zhang**,** ***"Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks"*****,** In Proceedings of the 8th International Symposium on Autonomous Decentralized Systems (ISADS), March 2007