همایش پژوهش های نوین در علوم و فناوری
Conference on Recent Research in Science and Technology

حفظ حریم خصوصی خودروها در شبکه‌های ارتباطات خودرویی

زهرا پوریوسف[۱]، مهری رجایی[۲]، نیک محمد بلوچزهی[۳]

[۱] دانشجوی کارشناسی ارشد، دانشکده مهندسی برق و کامپیوتر، دانشگاه سیستان و بلوچستان، زاهدان
z.pourusef@gmail.com

[۲] استاد، دانشکده مهندسی برق و کامپیوتر، دانشگاه سیستان و بلوچستان، زاهدان
rajayi@ece.usb.ac.ir

[۳] استاد، دانشکده مهندسی برق و کامپیوتر، دانشگاه سیستان و بلوچستان، زاهدان
nik.balouchzahi@gmail.com

چکیده

امروزه، بهره‌گیری از شبکه خودرویی موردی می‌تواند به طور قابل توجهی ایمنی ترافیک، بهره‌وری جاده‌ای را بهبود دهد و تاثیر سوء بر محیط زیست را نیزکاهش دهد. به طور کلی سرویس‌های ارائه شده در شبکه خودرویی شامل اطلاعات ترافیکی برای رانندگان مانند اطلاعات تصادفات، شرایط اضطراری، پیش بینی آب و هوا و به اشتراک گذاری اطلاعات چندرسانه‌ای می‌باشد، که به ایمنی رانندگان کمک می‌کند. اما مسأله امنیت و حفظ حریم خصوصی یک چالش بزرگ در عدم پذیرش برقراری ارتباط در محیط شبکه خودرویی می‌باشد. جهت اطمینان از صحت اطلاعات رد و بدل شده و جلوگیری از انکار در شبکه خودرویی فرستنده پیام باید احراز هویت شود. اما مشکل این است که رانندگان جهت حفظ حریم خصوصی خود تمایلی برای احراز هویت جهت ردیابی و مشکلات بعدی آن را ندارند. بنابراین احراز هویت ناشناس یکی از چالش‌های اصلی شبکه خوردرویی می‌باشد. در این مقاله راه‌کارهای ارائه شده برای حفظ حریم خصوصی را بررسی و آنها را در سه دسته تغییر نام مستعار، امضای گروهی، و ترکیبی قرار می‌دهیم.

کلمات کلیدی: حریم خصوصی، امنیت، شبکه خودرویی، نام مستعار، امضای گروهی.

۱. مقدمه

امروزه با رشد صنعت، تعداد خوردها در شهرها رو به افزایش است و یکی از معضلات زندگی شهری، مسائل مربوط به ترافیک و آلودگی هواست. با توجه به رشد تکنولوژی و فراهم آمدن زیرساخت‌های ارتباطات بی‌سیم در جوامع شهری، ترویج استفاده از شبکه‌های خودرویی موردی اثر قابل توجهی در کاهش اثرات مشکلات فوق خواهد داشت. از این طریق خودروها اطلاعات مربوط به ترافیک، آب و هوا و شرایط اضطراری را به یکدیگر اطلاع می‌دهند و می‌توان در مسیریابی و کاهش طول سفر و آلایندگی کمک شایانی بهم بکنند.

شبکه خودرویی موردی زیرمجموعه‌ای از شبکه تلفن همراه موردی می‌باشد. در شبکه خودرویی تهدیدها و حمله‌های امنیتی مانند اطلاعات غلط، انکار سرویس، جعل هویت، استراق سمع، تعلیق انداختن پیام، دستکاری سخت افزاری وجود دارد. برای امن بودن سیستم، نیازمندی‌های امنیتی شامل احراز هویت، یکپارچگی، محرمانگی، عدم‌انکار ضروری است. برای اطمینان

از اینکه بسته/داده توسط یک منبع قابل اعتماد ایجاد شده و جعلی نیست، بایستی احراز هویت صورت گیرد[1] در حالیکه از طریق احراز هویت، شبکه می‌تواند از محل دقیق یک کاربر خاص در یک زمان خاص آگاه باشد، و اجازه می‌دهد مرکز صدورگواهینامه در صورت ایجاد مشکل دخالت کند. این امر حریم خصوصی را نقض می‌کند [2]، [3]. افشای اطلاعات خصوصی رانندگان می‌تواند منجر به عواقب جدی شود. برای مثال، امکان ردیابی محل وسیله نقلیه هدف با توجه به مکان‌های گذشته وسیله نقلیه، زمینه سرقت وسایل نقلیه و تهدید صاحبان خودرو را توسط افراد بدخواه فراهم می‌آورد. این تهدیدها باعث می‌شود تا کاربران تمایلی برای عضویت در شبکه خودرویی نداشته باشند. پس باید به دنبال راهی باشیم که هویت واقعی کاربران قابل شناسایی نباشد [3]. بنابراین احراز هویت به صورت ناشناس یکی از راه‌کارهای حفظ حریم خصوصی در شبکه خودرویی می‌باشد. حفظ حریم خصوصی همیشه یک نگرانی کلیدی است. بسیاری از محققان برای حل چالش کلیدی و مهم حفظ حریم خصوصی چندین دهه تلاش کرده‌اند تا سطح حریم خصوصی را افزایش دهند، یا به عبارت دیگر احتمال افشای اطلاعات خصوصی را محدود کنند. از آنجائیکه، حفظ حریم خصوصی یک عامل تعیین کننده در پذیرش عمومی شبکه خودرویی است. با این وجود، در زمینه حفظ حریم خصوصی در شبکه خودرویی راه‌کارهایی اندک ارائه شده است که بر مبنای احراز هویت به‌صورت ناشناس می‌باشد. در این مقاله راه‌کارهای ارائه شده در این حوزه را در سه دسته زیر تقسیم شده است:

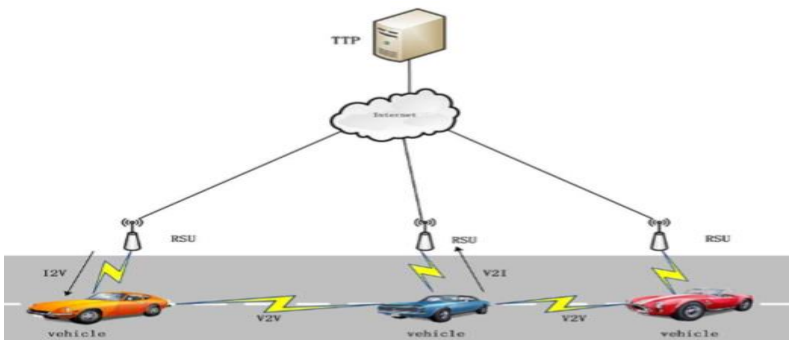
- احراز هویت با نام مستعار: این طرح با تغییرات مکرر نام مستعار حریم خصوصی را حفظ می‌کند [3].
- امضای گروهی: طرح امضای گروهی به اعضای معتبر گروه اجازه می‌دهد که به صورت ناشناس یک پیام را از طرف گروه امضا کند. بدین ترتیب، شناسایی فرستنده واقعی توسط هرکسی به جز مدیرگروه، بسیار مشکل است [3].
- روش‌های ترکیبی: از ترکیب طرح امضای گروهی و نام مستعار برای احراز هویت استفاده می‌شود.

ادامه مقاله بدین صورت سازماندهی شده است. در بخش ۲ مفاهیم پایه و کلی این حوزه بیان می‌شود. در بخش ۳ راه‌کارهای حفظ حریم خصوصی در شبکه خودرویی دسته‌بندی می‌شوند. بخش ۴ نتیجه گیری انجام می‌شود.

۲. تعاریف و مفاهیم مبنایی

اجزای اصلی شبکه خودرویی عبارتند از:

- مرکز صدور گواهینامه: یک شخص ثالث قابل اعتماد با منابع ذخیره‌سازی و محاسباتی مناسب که تمام وسایل نقلیه در آن ثبت می‌شوند و گواهینامه به آنها داده می‌شود. در (شکل-۱) با نام TTP نشان داده شده است. این واحد مسئولیت حفاظت از هویت واقعی وسایل نقلیه را دارد و درصورتی که گواهینامه آنها لغو شد هویت واقعی آنها را افشا می‌کند.
- OBU: واحد ارتباطی نصب شده بر روی خودرو که از طریق آن خودروها می‌توانند با یکدیگر و با زیرساخت ارتباط برقرار کنند.
- واحد کنارجاده‌ای (RAU): یک دستگاه رادیویی است که معمولا در امتداد جاده‌ها در مکان ثابت قرار دارد و باعث بهبود و ایمنی رانندگی می‌شود.



شکل-۱. معماری شبکه خودرویی [3]

ارتباط‌ها در شبکه خودرویی به دو صورت انجام می‌شود:

- خودرو با خودرو: خودروها می‌توانند با یکدیگر وقتی در محدوده بی‌سیم یکدیگر هستند ارتباط برقرار کنند و اطلاعات وضعیت جاده‌ای را برای خودروهای اطراف خود ارسال کنند.
- خودرو با زیر ساخت: خودروها می‌توانند در مواقعی که درخواستی دارند، یا می‌خواهند اطلاعاتی در مورد محیط بدست بیاورند، با زیرساخت ارتباط برقرار کنند.

حمله‌های گوناگونی در شبکه خودرویی وجود دارد که از جنبه‌های متفاوت به صورت زیر دسته‌بندی می‌شود [1]، [3]:

- موقعیت حمله کننده:
  - داخلی: یکی از گرهای متعلق به شبکه خودرویی می‌باشد که به صورت غیر مجاز رفتار می‌کند.
  - خارجی: حمله کننده متعلق به گره‌های شبکه خودرویی نمی‌باشد.
- هدف حمله کننده:
  - بدخواه: هدف آن آسیب رساندن به کاربران و شبکه به صورت کلی است. بنابراین هرگونه ابزاری را بدون توجه به هزینه‌ها و پیامدها بکار می‌گیرد.
  - منطقی: به دنبال اهداف شخصی خود است و به صورت هدف‌دار حمله را صورت می‌دهد. آن‌ها می‌توانند اطلاعات غلطی را در شبکه منتشر کنند تا رفتار دیگر راننده‌ها را تحت تأثیر قرار دهند.
- نوع مداخله در شبکه:
  - فعال: شامل اصلاح و تغییر بر روی جریان داده و ایجاد یک جریان نادرست در شبکه است. به طوری که پیام‌های اصلاح شده یا جعلی را برای وسایل نقلیه دیگر ارسال می‌کنند.
  - غیرفعال: شامل استراق سمع و نظارت بر بسته‌های مبادله شده در شبکه خودرویی است. فقط اطلاعات مفید را برای حملات آینده جمع‌آوری می‌کنند. مهاجم می‌تواند از زیرساخت‌های جاده‌ای و وسایل نقلیه اطراف وسیله نقلیه هدف سوءاستفاده کند.
- گسترده حمله:
  - محلی: مهاجم محدوده محدودی را کنترل می‌کند.
  - گسترش یافته: چندین موجودیت را در سراسر شبکه کنترل می‌کند.

در ادامه برخی از انواع حمله‌های شبکه خودرویی را مورد بررسی قرار می‌دهیم [1]، [3]:

- اطلاعات غلط: مهاجمان اطلاعات را جعل و تغییر می‌دهند، تا اطلاعات دروغین را در شبکه توزیع کنند.
- انکار سرویس: مهاجمان با هدف انسداد کانال ارتباطی و در پی آن از دسترس خارج کردن شبکه، پیام‌های پی‌درپی را به صورت غیرمستقیم به شبکه خودرویی وارد می‌کنند.
- جعل هویت: مهاجمان از اطلاعات سایر وسایل نقلیه برای تظاهر به گره‌ای قانونی و معتبر، سوءاستفاده می‌کنند، بدین ترتیب اطلاعات مخرب را به شبکه وارد می‌کنند. در صورتی که وسیله نقلیه شناسایی شود، از شبکه‌خودرویی حذف می‌شود، درحالی‌که گره سرویس را انکار می‌کند.
- استراق سمع: مهاجمان در وسایل نقلیه دروغین قرار دارند، و از طریق شنود به جمع‌آوری اطلاعات سایر وسایل نقلیه می‌پردازند.
- تعلق پیام: مهاجمان پیام را نگه می‌دارند و به صورت انتخابی پیام‌هایی که دارای اطلاعات مهم برای مقصد مورد نظر هستند را سرکوب می‌کنند، تا از ارائه گزارش در زمان مورد نیاز جلوگیری کنند و باعث ایجاد تصادم شوند.
- دستکاری سخت افزاری: مهاجمان به منظور برهم زدن نظم عمومی و اینکه به اهداف خاص خود برسند، برد سخت‌افزاری نصب شده بر روی وسایل نقلیه و واحد کنار جاده‌ای را دست‌کاری می‌کنند.

باتوجه به حمله‌هایی که ذکرشد، شبکه خودرویی باید نیازهای زیر را برآورده کند [3].

- محرمانگی: به معنی حفاظت داده‌های ارسال شده در مقابل اشخاص دیگر است. بدین ترتیب پیام به شکلی ساخته و ارسال می‌شود که فقط توسط گیرنده‌های مورد نظر قابل شناسایی باشد [4]. جنبه دیگر محرمانگی، حفاظت از جریان ترافیک در مقابل تحلیل است. این کار مستلزم این است که حمله کننده نتواند مبداء، مقصد، تعداد دفعات ارسال پیام، یا سایر ویژگی‌های ترافیک را در امکانات ارتباطی مشاهده نماید.
- یکپارچگی: به معنی اطمینان از اینکه پیام توسط شخص سومی دستکاری نشده باشد [4]. تغییر پیام از حمله‌های رایج در شبکه خودرویی است [1]. اگر یکپارچگی پیام تضمین نشود، یک وسیله نقلیه مخرب می‌تواند محتوای پیامی که توسط شخص دیگری ارسال شده را دستکاری کند تا رفتاردیگر وسیله نقلیه را تحت تأثیر قرار دهد [2].

- احراز هویت: به معنی اطمینان از اینکه طرفین ارتباط دارای هویت واقعی هستند [5]. بنابراین مهم‌ترین ضرورت در جلوگیری از اکثر حمله‌های ذکرشده در شبکه خودرویی احراز هویت است، و باید فرستنده پیام‌ها تایید هویت شود [3].
- عدم‌انکار: به معنی اطمینان از اینکه شخصی که پیام را ارسال کرده آن را انکار نکند [4]. رانندگانی که باعث ایجاد حوادث شده‌اند به طور قابل اعتماد قابل شناسایی هستند و مسئولیت آن را می‌پذیرند. بر اساس این اصل فرستنده پیام نمی‌تواند آن را انکار کند [3]. اگر عدم رد پشتیبانی نشود، وقتی یک وسیله نقلیه مخرب وضعیت اضطراری کاذب را گزارش می‌دهد تا شرایط رانندگی بهتری بدست آورد، حتی اگر راننده شناسایی شود نمی‌توان آن را از سرویس محروم کرد.

۲-۱. امنیت و حریم خصوصی

امنیت مکانیزمی برای حفاظت از شبکه و اطلاعات کاربران در برابر تهدیدها و حمله‌ها می‌باشد. در شبکه خودرویی به دلیل تحرک خودروها از زیرساخت دسترسی بی‌سیم در محیط خودرویی (WAVE) برای ارسال پیام‌ها و ارتباطات استفاده می‌شود. تا خدمات برای سیستم حمل و نقل ارائه شود. استاندارد IEEE1609.2، استاندارد ارتباطات دسترسی بی‌سیم در محیط خودرویی است که برای پشتیبانی از ارتباطات بی‌سیم در شبکه‌خودرویی شکل گرفته است. همچنین مسائل امنیتی پیام‌های ارتباطی WAVE را در برابر جعل، استراق سمع و سایر حملات بررسی می‌کند.

احراز هویت یک فرایند ابتدایی است که اجازه می‌دهد تا گیرنده پیام از اینکه محتوای پیام و منبع پیام در طول انتقال تغییر نمی‌کند، اطمینان یابد. اگر گیرنده نتواند تشخیص دهد که مهاجمان به نهادهای دیگر تظاهر می‌کنند یا اینکه پیام‌های دیگران را تغییر می‌دهند طرح احراز هویت کافی نیست. برای دستیابی به تأییدیه پخش در شبکه‌خودروی زیرساخت کلید عمومی به جای IEEE1609.2 پذیرفته می‌شود. زیرساخت کلید عمومی از یک جفت کلید عمومی و خصوصی رمزنگاری استفاده می‌کند تا بتواند ازشبکه خودرویی به طور کامل محافظت کند. با این وجود، زیرساخت کلید عمومی معمولی به تنهایی نمی‌تواند نیازمندی‌های امنیتی شبکه‌خودرویی را برآورده کند، زیرا تنها با رمزنگاری و امضای پیام، بدون هویت موقت نمی‌تواند حریم خصوصی رانندگان را حفظ کند و زمان تأیید بیش از حد طولانی است [3]. حریم خصوصی یعنی اینکه از افشای اطلاعات در برابر گره‌های دیگر جلوگیری شود و گره مورد نظر ناشناس باقی بماند.

۲-۲. پروتکل پایه و کلی شبکه خودرویی

پروتکل امنیتی پایه شبکه خودرویی و مراحل انجام‌کار آن در این بخش مورد بررسی قرار می‌گیرد. ابتدا، توضیحاتی در مورد لیست لغو گواهی و اینکه چه کاربردی در پروتکل امنیتی دارد می‌دهیم. لیست لغو گواهی حاوی گواهینامه‌هایی است که توسط مرکز صدورگواهینامه اخیرا لغو شده‌اند و درون لیست قرار داده می‌شوند، این لیست بین همه گره‌ها توزیع می‌شود تا عاملان ناشناس شناسایی شوند. بعلاوه وسایل نقلیه تأیید شده با بررسی آن از لغو گواهی خود مطلع می‌شوند، و اقدام به اخذ گواهینامه جدید که شامل جفت کلید جدید، امضای مرکز صدور و دوره اعتبار جدید می‌باشد، می‌کنند.

برای هر نوع ارتباط خودرو با خودرو، خودرو با زیرساخت بایستی خودرو دارای جفت کلید عمومی و خصوصی معتبر (گواهینامه معتبر) باشد. بنابراین پیش از هر اقدامی باید دو گام ذیل انجام شود:

۱- وسیله نقلیه اطلاعات هویتی خود را برای ثبت‌نام به شخص ثالث(مرکز صدور گواهینامه) ارائه می‌دهد، ثبت هر وسیله نقلیه ضروری است، زیرا فقط سرویس به مشتریان معتبر ارائه می‌شود و مرحله حفاظت اولیه است.

۲- شخص ثالث جفت کلید خصوصی و عمومی را همراه گواهینامه خودرو به هر وسیله نقلیه معتبر اختصاص می‌دهد. این روش شامل تولید جفت کلید می‌باشد [3].

در ارتباط بین خودرو با خودرو مراحل زیر انجام می‌گیرد:

۱- خودروی ارسال کننده پیام، قبل از ارسال پیام، پیام را به‌صورت دیجیتالی امضاء می‌کند تا از دسترس مستقیم مهاجمان جلوگیری کند، درحالی‌که همزمان به حفظ حریم خصوصی کمک می‌کند.

۲- دریافت کننده با بررسی امضای پیام، اعتبار پیام را تأیید می‌کند و از سوی دیگر باید اطمینان یابد که ارسال کننده پیام دارای اعتبار است، این روش جزء تکنیک‌های تأیید اعتبار است [3].

در ارتباط بین خودرو با زیر ساخت مراحل زیر صورت می‌گیرد:

۱- درخواست خودرو با روش رمزنگاری نامتقارن با کلید عمومی رمز می‌شود.

۲- گواهینامه آن به واحد کنارجاده‌ای ارسال می‌شود.

۳- واحد کنارجاده‌ای درخواست را رمزگشایی می‌کند.

۴- فهرست لغو تازه به‌روز شده توسط شخص ثالث (مرکز صدور گواهینامه) را بررسی می‌کند، که آیا خودرو حق دریافت سرویس را دارد.

۵- اگر گواهینامه خودرو در لیست لغو قرار داشت درخواست آن را رد می‌کند در غیر این صورت خودرو تأیید شده است.

۶- واحد کنارجاده‌ای پاسخ را با روش رمزنگاری نامتقارن رمز می‌کند و به وسیله نقلیه ارسال می‌کند.

۷- سرویس درخواستی را ارائه می‌دهد.

۸- خودرو پس از دریافت پاسخ را رمزگشایی می‌کند و اعتبار واحد کنار جاده‌ای را نیز بررسی می‌کند [3].

۳. دسته بندی راهکارهای حفظ حریم خصوصی

هدف از این بخش، بررسی و طبقه‌بندی راه‌کارهای پیشنهادی تحقیقات دیگر محققان در سطح دنیا در مورد حفظ حریم خصوصی در شبکه‌های خودرویی می‌باشد.

کاربران و رانندگان درصورتی که هویت واقعی آنها ناشناس باقی بماند و حریم خصوصی آنها حفظ شود، تمایل دارند وارد شبکه خودرویی شوند. حفظ حریم خصوصی مکان، یکی از اهداف اصلی حریم خصوصی در شبکه خودرویی است و برای موفقیت آن ضروری است. راه‌های حفاظت از حریم خصوصی نام مستعار، امضای گروهی و روش ترکیبی است که در بخش‌های زیر بررسی می‌شوند.

۳-۱. تغییر نام مستعار

نام مستعار یک هویت ناشناس موقت است که هویت واقعی کاربران را مخفی می‌کند، پس از دوره کوتاهی برای ناشناس ماندن آن را تغییر می‌دهند. به این ترتیب با تغییر مرتب جفت کلید آن، دیگر به راحتی خودرو قابل ردیابی توسط مهاجم نیست. روش های تغییر نام مستعار می‌تواند متفاوت باشد در برخی از روش‌ها نام مستعار درون خودرو از قبل توسط مرکز صدور بارگذاری می شود. رایا و همکارانش [6] پیشنهاد دادند که کلیدهای ناشناس از قبل درون خودرو بارگذاری شود. کلید عمومی مرکز صدور و شماره شناسه الکترونیکی، درون خودرو بارگذاری می‌شود. وسیله نقلیه ازکلید ناشناس خود در امضای

پیام اســـتفاده می‌کند و باید پس از مدت یک دقیقه کلید ناشـــناس خود را تغییر دهد. و هر وســـیله نقلیه باید ۴۳۸۰۰ کلید ناشناس در هر سال بارگذاری کند، این امر مستلزم داشتن یک فضای ذخیره سازی بزرگ درون خودرو می‌باشد.

در همین راستا سان و همکارانش [7] یک استراتژی پیش بارگذاری متفاوت پیشنهاد کردند، که در آن مرکز صدور محدوده خود را به چندین حوزه تقسـیم می‌کند. هر وسـیله نقلیه یک مجموعه بزرگ از گواهینامه‌های نام مسـتعار از مرکز صـدور را دریافت و ذخیره می‌کند و برای اسـتفاده از آنها از واحد کنار جاده ای درخواسـت امضـای مجدد گواهینامه نام مسـتعار خود را می‌کند. واحد کنار جادهای کلید امضـای مجدد را صـادر و گواهینامه نام مسـتعار را امضـاء می‌کند. از آن پس، خودرو فقط در همان حوزه می‌تواند از گواهینامه نام مسـتعار اسـتفاده کند. در این روش برخلاف روش‌های سنتی لیست لغو گواهینامه وابسته به تعداد گواهینامه‌های نام مسـتعار لغو شـده نیسـت، بلکه فقط به تعداد خودروهای لغو شـده، وابسـته اسـت. به همین دلیل توانسته هزینه لغو را کاهش دهد.

بعلاوه، وانگ و همکارانش [8] نیز روشـی پیشـنهاد داده‌اند که در آن وسـایل نقلیه نام مسـتعار خودرو را در نقاط اجتماعی تغییر می‌دهند، تا حریم خصـوصـی مکان حفظ شـود. در مدل پیشـنهادی شبکه خودرویی از تعداد زیادی وسیله نقلیه و نقاط اجتماعی تشـکیل شده است، که وسایل نقلیه پیام‌های ایمن شده خود را بایکدیگر به اشتراک می‌گذارند. به منظور تغییر مداوم نام مسـتعار، به هر وسـیله نقلیه تعداد زیادی نام مسـتعار اختصـاص داده می‌شـود. نقاط اجتماعی در این مدل یک پارکینگ با ظرفیت محدود می‌باشـد که تعداد زیادی وسـیله نقلیه در آن جمع شـده اند. درصـورت تکمیل بودن ظرفیت پارکینگ، خودرو محل را بدون تغییر نام مسـتعار ترک می‌کند. در غیر این صورت وارد پارکینگ می‌شود و قبل از خروج نام‌مستعار خود را تغییر داده. و سـپس، اولین پیام ایمنی که شـامل اطلاعاتی از جمله سـرعت برابر صـفر، نام‌مسـتعار غیرمرتبط و اطلاعات مکانی برابر نقطه اجتماعی می‌باشـد را منتشـر می‌کند. اگر فرض شـود همه وسـایل نقلیه قبل از ترک نام مسـتعار متفاوت بگیرند، نقطه اجتماعی به طور طبیعی به یک ناحیه مخلوط تبدیل می‌شـود. و با استفاده از یک مدل تحلیلی سطح حریم خصوصی را بررسی می‌کند.

در برخی از روش‌ها نیز هر وسـیله نقلیه می‌تواند نام مسـتعار خود را از نزدیکترین واحد کنار جاده‌ای دریافت کند. ژانگ و همکـارانش [9] یـک طرح تـأییـد پیـام به کمک واحدهای کنار جاده‌ای پیشـــنهاد کرده‌اند که وســـیله نقلیه از طریق واحد کنارجاده‌ای می‌تواند ارسـال کننده را تأیید کند. اگر وسیله نقلیه تشخیص دهد یک واحد کنار جاده‌ای در نزدیکی او قرار دارد، با آن ارتباط برقرار می‌کند. واحد کنارجاده‌ای یک کلید مخفی متقارن مشترک و شناسه ناشناس را به خودرو اختصاص می‌دهد و در پایگاه داده خود ذخیره می‌کند. واحد کنارجاده‌ای شـناسـه ناشـناس را دارد، می‌داند کدام خودرو پیام را ارسـال کرده و با اسـتفاده از کلید متقارن مشـترک پیام را تأیید می‌کند. به دلیل اینکه لازم نیسـت خود وسـیله نقلیه همه پیام‌ها را تأیید کند، سربارمحاسبات پایین آمده است. اما سربار ارتباطات افزایش پیدا می‌کند.

روش‌های دیگری نیز وجود دارد که هر وسـیله نقلیه می‌تواند خودش نام مسـتعار تولید کند. درصـورتی که وسیله نقلیه نام مستعار خود را در شرایط نامناسب تغییر دهد، می‌تواند بی‌فایده باشد، زیرا مهاجم می‌تواند یک ارتباط بین نام مستعار قدیمی و جدید ایجاد کند، برای بهبود این موضـوع، لیو [10] تغییر موثر نام مستعار در نقاط اجتماعی را ارائه می‌دهد تا حریم خصوصی موقعیت را اثبات کند. نقاط اجتماعی، نقاطی هسـتند که تعداد زیادی وسیله نقلیه با هم جمع می‌شوند. مثل، پارکینگ و محل تقاطع‌ها که چراغ راهنما قرمز است. اگر همه وسایل نقلیه نام مستعار خود را قبل از ترک آنجا تغییر دهند، به طور طبیعی نقاط اجتماعی به یک ناحیه مخلوط تبدیل می‌شـود و حریم خصـوصـی موقعیت قابل دست‌یابی است. در این روش، مرکز صدرو یک کلید ناشـناس به خودرو اختصـاص می‌دهد، کاربر کلید ناشناس را در یک محیط امن نگهداری می‌کند، سپس در زمان سفر به اندازه طول سفر نام مستعار تولید می‌کند و در نقاط اجتماعی آنها را تغییر می‌دهد. بعلاوه این پژوهش [10]، با دو مدل تحلیلی سطح حریم خصوصی در مقیاس کوچک و بزرگ را بررسی می‌کند.

هانگ و همکارانش [11] احراز هویت نام مستعار با طرح حریم خصوصی مشروط را پیشنهاد کردند که در هر منطقه یک مرکز صدور وجود دارد که وسایل نقلیه و واحدهای کنار جاده‌ای در آن ثبت می‌شوند. کلید عمومی وسایل نقلیه به صورت دوره‌ای از طریق واحد کنارجاده‌ای پخش می‌شود و کلید خصوصی فقط در اختیار مرکز صدور می‌باشد. وسایل نقلیه پس از دریافت کلید عمومی یک نام مستعار تولید یا بروزرسانی می‌کنند، که باعث می شود حریم خصوصی آنها حفظ شود. پس از تأیید واحد کنار جاده‌ای نام مستعار به صورت آفلاین توسط واحد کنار جاده‌ای امضا می‌شود، از طریق طریق اطلاعیه‌ای به خودروهای دیگر ارسال می‌شود. فرستنده با استفاده از نام مستعار آفلاین یک نام مستعار آنلاین تولید، پیام را امضا و ارسال می‌کند. دریافت کننده با استفاده از اطلاعیه پیام را بررسی و تأیید می‌کند.

۳-۲. امضای گروهی

امضای گروهی روشی است برای ناشناس ماندن هویت واقعی رانندگان که در آن، عضو معتبر گروه، یک پیام را از طرف کل گروه امضا می‌کند. در این مدل برای گروهی از خودروها یک کلید عمومی و چند کلید خصوصی تولید می‌شود. بنابراین هنگام ارسال پیام گیرنده نمی‌تواند تشخیص دهد دقیقا کدام یک از خودروهای گروه این پیام را ارسال کرده است، زیرا پیام رمز شده با هر یک از کلیدهای خصوصی خودروها با کلید عمومی مشترک رمزگشایی می‌شود. اما در صورتی‌که خودرو تخلف کند، تنها توسط مدیر گروه قابل شناسایی است.

لین و همکارانش [12] یک پروتکل حفظ حریم خصوصی مشروط برای شبکه خودرویی ارائه داده‌اند. در این روش خودرو از امضای گروهی کوتاه برای امضای پیام فرستاده شده جهت ناشناس بودن امضاکننده استفاده می‌کند. به این ترتیب، نیازمندی‌های قابل ردیابی و ناشناس بودن شبکه خودروی برآورده می‌شود. مرکز صدور گواهینامه که به عنوان مدیرگروه عمل می‌کند، می‌تواند شناسه وسیله نقلیه را در صورت لزوم شناسایی کند. در این طرح نقش مدیرگروه به دو نقش مدیرعضویت و مدیر ردیابی تقسیم می‌شود. تمام وسایل نقلیه ابتدا توسط مدیر عضویت ثبت نام می‌شوند. فرستنده قبل از ارسال، پیام را با کلید خصوصی خود امضا می‌کند. اگر امضا معتبر باشد، گیرنده پیام را معتبر و امضاکننده را عضو معتبر گروه می‌داند. در صورتی که مشکلی ایجاد شود عملیات ردیابی شناسه وسیله نقلیه، توسط مدیر ردیابی انجام می‌شود. این مدل از روش تأیید ترکیبی استفاده می‌کند: اگر تعداد وسایل نقلیه لغو شده کمتر از حد آستانه باشد، از روش بررسی لیست لغو، و درغیر اینصورت، از طریق روش بروزرسانی کلید عمومی گروه و کلید خصوصی انجام می‌شود.

لیو و همکارانش [13] یک پروتکل حفظ حریم خصوصی کارآمد ارائه داده‌اند. واحد کنار جاده‌ای، تحت مرکز صدور گواهینامه اداره می‌شود. واحد ذخیره‌سازی اطلاعات، بین مرکز صدور گواهینامه و وسیله نقلیه می‌باشد، هنگامی که وسیله نقلیه از کنار واحد کنار جاده‌ای عبور می‌کند درخواست گواهینامه کلید ناشناس کوتاه مدت می‌کند، واحد کنار جاده‌ای گواهینامه کلید ناشناس کوتاه مدت که با استفاده از امضای گروهی ساخته است را برای وسیله نقلیه ارسال می‌کند. سپس وسیله نقلیه می‌تواند پیام‌ها را در زمان معتبر تعیین شده، پخش کند، دریافت کننده پس از دریافت پیام ابتدا دوره زمانی و سپس کلید ناشناس و گواهینامه را بررسی می‌کند. در صورت تایید مرحله قبل، امضا را بررسی و تأیید می‌کند. بنابراین، داشتن یک کپی از لیست لغو گواهی غیر ضروری خواهد بود.

وانگ و همکارانش [5] طرح تأیید اعتبار برای حفظ حریم خصوصی که مبتنی بر امضای گروهی است، را پیشنهاد داده‌اند. هنگامی که یک وسیله نقلیه عضو گروه می‌شود نیازمند دوره اعتبار است و این اعتبار بررسی می‌شود تا عضویت خودرو در گروه را مشخص کند. این امر جایگزین بررسی فهرست لغو گواهی می‌باشد، که باعث کاهش هزینه تأیید امضا می‌شود، این طرح، تأیید هویت به صورت دسته‌ای را نیز پشتیبانی می‌کند. نهادهای اصلی این مدل عبارت اند از: ۱- عامل قابل اعتماد (شخص ثالث)، وسیله نقلیه و مدیر گروه را ثبت و گواهینامه آنها را تأیید می‌کند. ۲- ارائه کننده خدمات یا همان مدیر گروه که اعضای گروه به صورت دوره ای هزینه‌ای را برای داشتن اعتبار پرداخت می‌کنند و از خدمات استفاده می‌کنند. ۳- زیرساخت شبکه است که به عنوان رابطی بین واحد درون خودرویی و ارائه کننده خدمات عمل می‌کند. ۴- واحد درون خودرویی، مسئول ارتباط

خودرو با زیرساخت است و به صورت دوره‌ای اطلاعات مربوط به وضعیت ترافیکی را پخش می‌کند. قبل از امضا وسیله نقلیه اعتبار خود را بررسی می‌کند، اگر نامعتبر بود یک درخواست جدید برای عضویت به ارائه‌کننده خدمات ارسال می‌کند، اگر معتبر بود پیام را امضا و ارسال می‌کند. پس از دریافت ابتدا دوره اعتبار بررسی می‌شود، اگر نامعتبر باشد فرآیند تأیید امضا پیش نمی‌رود. به این معنی که خودروهای جعلی بعد از لغو نمی‌توانند دسترسی به خدمات را داشته باشند. زمانی که پیام مشکوکی دریافت شود، هویت فرستنده شناسایی می‌شود. مدیر گروه قانونی بودن فرستنده پیام را بررسی می‌کند و سپس با استفاده از کلید اصلی هویت واقعی وی شناسایی می‌شود. طرح پیشنهادی [5] از تأیید دسته‌ای پشتیبانی می‌کند که به بهبود تأیید امضا کمک می‌کند. فرض بر این است که وسیله نقلیه n پیام ترافیکی دریافت می‌کند و تأیید دسته‌ای باعث می‌شود تأیید n پیام با یکدیگر به طور کامل موفقیت آمیز باشد. این روش هزینه بررسی لیست لغو را کاهش می‌دهد و تأیید امضا بهبود می‌یابد.

۳-۳. روش ترکیبی

وسایل نقلیه به صورت دوره‌ای پیام‌های ایمنی را ارسال می‌کنند. پهنای باند و توان پردازشی دو منبع اصلی برای سیستم است. هر سیستم باید دارای توان پردازشی کافی برای وظایف تعیین شده داشته باشد، بنابراین طراح سیستم می‌تواند توان پردازشی را در ازای افزایش هزینه بالا ببرد. در [14] طرح جدید احراز هویت ناشناس ارائه می‌شود. روش ترکیبی پیشنهادی هر گره به یک کلید امضای گروهی gsk_v و یک کلید عمومی گروه gpk_{CA} مجهز می‌شود. برای این روش مرکز صدور گواهی ارائه نمی‌دهد، در عوض وسیله نقلیه از gsk_v برای تولید یک امضای گروهی $\Sigma_{CA,V}()$ برای هر نام‌مستعار K_v^i استفاده می‌کند. اگر پیام دریافت شود، امضای گروهی با استفاده از کلید عمومی گروه gpk_{CA} تأیید می‌شود و در صورتی که موفقیت آمیز بود، گیرنده پیام متوجه می‌شود که عضو قانونی گروه نام مستعار K_v^i را تولید کرده است. این روش برای کاهش سربار و افزایش کارایی بهینه‌سازی می‌شود. طرح ترکیبی هزینه محاسبات بالایی دارد ولی از مزایای لیست لغو کوچک برخوردار می‌باشد و به‌این‌ترتیب حافظه و پهنای باند کمتری برای ذخیره و انتقال نیاز دارد.

محمد خدایی و همکارانش [4]، طرح ترکیبی متفاوتی پیشنهاد داده‌اند. مناطق به چند ناحیه تقسیم می‌شود و توسط زیرساخت کلید عمومی برای اطمینان از برقراری ارتباط امن مدیریت می‌شود. در این مدل وسیله نقلیه از قبل درون مرکز صدور ثبت شده، وسیله نقلیه درخواست نام مستعار را به مرکز صدرو ارسال می‌کند، و نام مستعار دریافت می‌کند، در صورتی که وسیله نقلیه به زیرساخت دسترسی نداشته باشد، با استفاده از امضای گروهی نام مستعار تولید می‌کند. بنابراین نام مستعاری که توسط خودرو تولید می‌شود متفاوت از نام مستعاری است که توسط زیرساخت تولید می‌شود به همین دلیل به راحتی قابل ردیابی است. برای حل این مشکل طرح Rhythm ارائه شده است، وسیله نقلیه با کمک وسایل نقلیه همسایه پنهان می‌شود. از خودروهای همسایه درخواست می‌کند که نام مستعار را خود تولید کند تا امکان ردیابی کاهش یابد. وسایل نقلیه همسایه با احتمال R از نام مستعاری که خود تولید کرده استفاده می‌کند. بار محاسباتی افزایش می‌یابد، بیشترین هزینه مربوط به تأیید امضای گروهی می‌باشد.

۴-۳. مقایسه از لحاظ سربار محاسباتی و ارتباطی

در این بخش، روش‌های مطرح شده در سه دسته فوق از لحاظ سربار محاسباتی و ارتباطی مورد مقایسه قرار می‌گیرد. در روش‌های تغییر مکرر نام مستعار، سه استراتژی متفاوت برای تولید و اعتبارسنجی نام مستعار ارائه شد. در استراتژی اول، نام مستعار از ابتدا توسط مرکز صدور درون خودرو بارگذاری می‌شود که نیاز به فضای ذخیره سازی درون OBU هر خودرو دارد. در استراتژی دوم، وسیله نقلیه از طریق ارتباط با واحد کنار جاده‌ای نام مستعار بدست می‌آورد که به ارتباط مکرر با زیرساخت نیاز دارد. در استراتژی سوم، نام مستعار توسط خود خودرو با کلید ناشناسی که توسط مرکز صدرو گواهینامه صادر شده بود، تولید می‌شد که سربار محاسباتی برای خودرو دارد. در روش‌های این دسته ممکن است لیست بزرگ شود، چون اگر خودرویی لغو شود تمام نام مستعارهای آن در لیست لغو قرار می‌گیرد. در گروه دوم روش حفظ حریم خصوصی با امضای گروهی بررسی شد که به هر وسیله نقلیه یک کلید عمومی گروه و یک کلید خصوصی اختصاص داده می‌شد. در روش امضای گروهی تأیید

امضا در بررسی لیست لغو بسیار زمان بر است. در گروه سوم نیز روش ترکیبی بررسی می‌شود که وسیله نقلیه از امضای گروهی برای امضای نام مستعار خود استفاده می‌کند. در روش ترکیبی بررسی اعتبار فقط یک بار برای هر نام مستعار انجام می‌گیرد.

۴. نتیجه گیری

همانطور که بیان شد، لازمه جلوگیری از بسیاری از حمله‌ها در شبکه خودرویی شناسایی هویت واقعی ارسال کننده پیام می‌باشد. از آنجائیکه احراز هویت توسط بدخواهان می‌تواند منجر به افشای اطلاعات خصوصی رانندگان شود و حریم خصوصی آنان را نقض کند، احراز هویت به صورت ناشناس به عنوان راه‌کاری برای حفظ حریم خصوصی مطرح شده است. راه‌کاری موجود در این حوزه را در سه دسته تغییر نام مستعار، امضای گروهی و روش ترکیبی طبقه‌بندی شد. در آخر هر کدام از این روش ها را از لحاظ سربار محاسبات، ارتباطات، زمان تولید و تأیید امضا ، هزینه لیست لغو بررسی کردیم.

در کارهای آینده روش‌های ترکیبی می‌تواند مورد توجه قرار بگیرد، به این صورت که خودرو نام مستعار خود را از زیرساخت دریافت می‌کند، در صورتی که به زیرساخت دسترسی نداشته باشد، خودش نام مستعار را با استفاده از امضای گروهی تولید کند. یکی از کارهای آتی هماهنگ‌سازی طول عمر بین نام مستعاری که خودرو از زیرساخت دریافت می‌کند با نام مستعاری که خودرو تولید می‌کند. بعلاوه، میزان طول عمر نام‌های‌مستعار در روش‌های موجود به صورت ثابت است که می‌توان از روش‌های پویا برای مقداردهی آن بهره جست، بطوریکه که در مکان‌های پرتردد طول عمر آنها بیشتر باشد و به این ترتیب بار محاسباتی و ارتباطی برای تولید مجدد نام مستعار کاهش می‌یابد.

مراجع

[1] Razzaque, M., Salehi, A., Cheraghi, S. *"Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead*," in Wireless Networks and Security, Springer, Berlin, Heidelberg, 2013, pp. 107-132.

[2] Agrawal, A. , Garg, A., Chaudhiri, N. , Gupta, S., Pandey D., Roy, T., "*Security on Vehicular Ad Hoc Networks (VANET) A Review Paper*," IJETAE, vol. 3, no. 1, pp. 231-235, 2013.

[3] Qu, F., Wu, Z., Wang, F., Cho, W., "*A Security and Privacy Review of VANETs*," IEEE T-ITS, vol. 16, no. 6, pp. 2985-2996, 2015.

[4] Papadimitratos, P., KHodaei M., Messing, A., *A Privacy-preserving Pseudonym Acquisition Scheme for Vehicular Communication Systems, stockholm sweden*: Kth Royal Institute Of Technology School Of Computer Science And Communication, 2018.

[5] Wang, Y., Zhong, H., Xu, Y., Cui, J., "*ECPB: Efficient Conditional Privacy-Preserving Authentication Scheme Supporting Batch Verification for VANETs*," IJNS, vol. 18, no. 2, pp. 374-382, 2016.

[6] Raya, M., Hubaux, J., "*The security of vehicular ad hoc networks*," in SASN '05 Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, Alexandria, Virginia, USA, 2005.

[7] Sun, Y., Lu, R., Lin, X., Shen, X., Su, J., "*A secure and efficient revocation scheme for anonymous vehicular communications*," in IEEE ICC, Cape Town, South Africa, 2010.

[8] Wang, D., Li, D., Li, X., Xiao, Z., "*An Analysis Of Anonymity On Capacity Finile Social Spots Based Pseudonym Changing for Location Privacy in VANET*," in ICNC-FSKD, Zhangjiajie, China, 2015.

[9] Zhang, C., Lin, X., Lu, R., Ho, P., "*Raise: An efficient RSU-aided message authentication scheme in vehicular communication networks*," in IEEE ICC, Beijing, China, 2008.

[10] Lu, R., Lin, X., Luan, T., Liang, X., Shen, X. , "*Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANET*," IEEE T Veh Technol , vol. 61, no. 1, pp. 86-96, 2011.

[11] Li, J., Lu, H., Guizani, M., "*ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs*," IEEE TPDS, vol. 26, no. 4, pp. 938-948, 2015.

[12] Lin, X., Sun, X., Ho, P., Shen, X., "*A secure and privacy-preserving protocol for vehicular communications*," IEEE T Veh Technol, vol. 56, no. 6, pp. 3442-3456, 2007.

[13] Lu, R., Lin, X., Zhu, H., Ho, P. H., Shen, X., "*ECPP: Efficient conditional privacy preservation protocol for secure vehicular communication*," in IEEE INFOCOM 2008, Phoenix, AZ, USA, 2008.

[14] Calandriello, G., Papadimitratos, P., Hubaux, J., Lioy, A., "*On the Performance of Secure Vehicular Communication Systems*," IEEE TDSC, vol. 8, no. 6, pp. 898-912, 2011.

privacy-preserving for vehicular communication network

Zahra Pouryousef
Masters student, Faculty of Electrical and Computer Engineering, University of Sistan and Baluchestan, Zahedan, Iran, E-mail: z.pourusef@gmail.com

Mehri Rajaei
Professor, Faculty of Electrical and Computer Engineering, University of Sistan and Baluchestan, Zahedan, Iran, E-mail: rajayi@ece.usb.ac.ir

Nik Mohammad Balouchzahi
Professor, Faculty of Electrical and Computer Engineering, University of Sistan and Baluchestan, Zahedan, Iran, E-mail: nik.balouchzahi@gmail.com

Abstract. Today, exploitation of a vehicular ad hoc network can significantly improve traffic safety and road productivity, and reduce environmental impact. Generally, the services provided on the vehicular network include traffic information for drivers such as accident information, emergency conditions, weather forecasting and sharing multimedia information, which helps drivers to safety. But the issue of security and privacy is a major challenge in failing to communicate in a vehicular network environment. To ensure the accuracy of the information, the message sender must be authenticated to prevent denial of the vehicular network. But the problem is drivers for their privacy do not have the desire to authenticate for tracking and the next problems. Therefore, anonymous authentication is one of the main challenges of the vehicular network. In this article, we review the strategies proposed for privacy and we put them in three categories: pseudonyms, group signature, combined method.

Keywords: Privacy; Security, Vehicular ad-hoc network, Pseudonyms, Group signature.