چالش های امنیتی VANet و راه‌حل ها: بررسی

چکیده

VANet یک فناوری نوظهور با آینده‌ای امیدوار است که با چالش‌های بزرگی به‌خصوص در حوزه‌ی امنیت روبه‌رو است. در این مقاله، به چارچوب امنیتی VANet در سه قسمت متمرکز می‌شویم. ابتدا یک نمای گسترده از ویژگی‌های امنیتی VANet و چالش‌ها و همچنین نیازمندی‌ها ارائه می‌کنیم. این الزامات باید برای پیاده‌سازی زیرساخت امن VANet با ارتباطات موثر بین بخش‌ها در نظر گرفته شود. جزئیات معماری امنیتی بیان شده و پروتکل شناخته شده استانداردهای امنیتی بیان شده است. در مرحله دوم، طبقه‌بندی جدیدی از حملات مختلف شناخته شده در کارهای گذشته مربوط به VANet و راه‌حل‌های مربوط به آنها، ارائه می‌شود. در مرحله سوم، یک مقایسه بین برخی از این معیارهای امنیتی شناخته شده در VANet انجام می‌گیرد. سپس به مسائل مختلف باز و چالش‌های مرتبط با امنیت VANet می‌پردازیم، که می‌تواند برای استفاده محققان در کارهای آتی کمک‌کننده باشد.

کلیدواژه‌ها: VANet، چالش‌های امنیتی، طبقه‌بندی حملات، ارتباطات V2V، راه‌حل‌های امنیتی

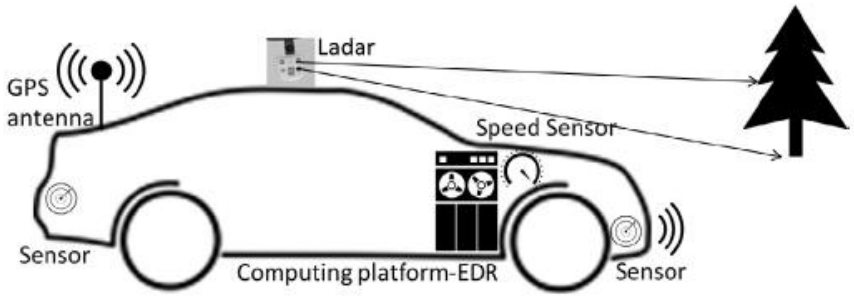
1. معرفی

هدف VANet، اطمینان از رانندگی امن با بهبود جریان ترافیک و در نتیجه کاهش قابل توجه حوادث رانندگی است. که اخیرا با ارائه اطلاعات مناسب به راننده و یا به وسیله نقلیه حل شده است. بااین حال، هر گونه تغییر این اطلاعات در زمان واقعی ممکن است به شکست سیستم تأثیر بگذارد و امنیت مردم در جاده‌ها را به خطر بیاندازد. برای اطمینان از عملکرد بدون اشکال آن، تامین امنیت این اطلاعات باید جزء اهداف مهم محققان امنیتی قرار گیرد.

VANET یک کلاس خاص از شبکه تلفن‌همراه Ad-hoc با مسیرهای از پیش تعریف شده (جاده) است. که به روش‌های خاص مدیریتی، واحدهای کنار جاده‌ای (RSUs) متکی است. RSU ها بر کناره‌های جاده برای انجام خدمات خاص قرار گرفته‌اند و OBUها در وسایل نقلیه موجود در VANET نصب شده‌اند. تمام وسایل نقلیه در حال حرکت آزادانه در شبکه جاده‌ای و ارتباط با یکدیگر و یا با RSUs و وسایل خاص هستند.

با استفاده از DSRC (ارتباطات اختصاصی با بردکوتاه) در یک و یا چند هاپ، حالت‌های ارتباطی، V2V (خودرو به خودرو)، V2I (خودرو به زیرساخت) و یا ترکیبی است.

در سال‌های آینده، بسیاری از وسایل نقلیه در VANET با وایرلس (OBU)، جی پی اس (سیستم موقعیت‌یاب جهانی)، EDR (ثبت روند داده) و سنسور (رادار و ladar) ارتباط برقرار خواهند کرد، همانطور که در شکل 1 نشان داده شده است. این تجهیزات برای نظارت و ثبت ترافیک استفاده خواهند شد.



شکل1. طراحی آینده وسایل نقلیه در VANET

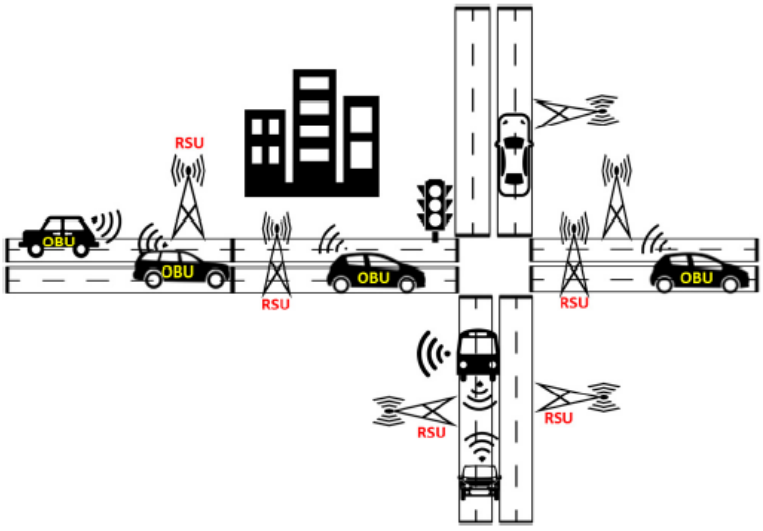
سپس به‌طور خودکار اقدامات مناسب بنا به اطلاعات V2V یا V2I در داخل شبکه وسایل نقلیه انجام خواهد گرفت.

کاربران VANET از بسیاری از برنامه‌های کاربردی که به ایمنی فعال جاده، سرگرمی، بهره‌وری ترافیک و مدیریت طبقه‌بندی شده‌اند بهره می‌برند[1]؛ سپس به مدیریت سرعت و ناوبری می‌پردازند.

امنیت حالتی از مصون ماندن نسبت به خطر یا تهدید است. امنیت به معنی ایمنی، و همچنین اقدامات انجام شده برای ایمنی یا محافظت است.

در VANET، محافظت در برابر فعالیت‌های سوء استفاده و تعریف معماری امنیتی بسیار مهم است چرا که برقراری ارتباط بی‌سیم امن سخت است. امنیت و سطح تضمین شده آن برای پیاده‌سازی ایمنی مردم است. چند سال پیش،

بسیاری از محققان حملات امنیتی را بررسی کرده‌اند و سعی در یافتن راه‌حل‌های مربوط به آنها داشتند. افراد دیگر در تلاش برای تعریف امنیت در زیرساخت یا رسمی کردن استانداردها و پروتکل‌ها هستند. اما هنوز هم، روند اعتماد نسبت به یک گره و تشخیص بسیار مشکل است.



شکل 2. شبکه VANET

این مقاله ویژگی‌های امنیتی VANET و بسیاری از چالش‌های امنیتی VANET و همچنین راه‌حل‌های موجود را به شیوه‌ای جامع بررسی می‌کند. پس از بررسی جزئیات معماری امنیتی و پروتکل‌های استاندارد امنیتی شناخته شده، در مورد چارچوب‌های اخیر و مسائل مرتبط بحث و بررسی انجام می‌دهیم. بنابراین بر طبقه‌بندی جدیدی از حملات مختلف شناخته شده در امنیت VANET و راه‌حل‌های آن تمرکز می‌کنیم. در نهایت، با وجود تمام فرصت‌های امیدوارکننده که همراه VANET است و پس از بحث در مورد آثار ارائه شده، به چالش‌های پژوهشی خاص جهت تحقیقات آینده می‌پردازیم. بنابراین VANET به پیاده‌سازی یک سیستم برای وسایل نقلیه و گره‌های مخرب می‌پردازد. این مقاله به شرح زیر سازماندهی شده است. بخش 2 مدل VANET و نیازمندی‌های امنیتی آن را بیان می‌کند. بخش 3 جزئیات و مدل حملات را بیان می‌کند. بخش 4 تلاش‌های استانداردسازی را بیان می‌کند. بخش 5 راه‌حل‌های طبقه‌بندی را به شیوه‌ای منسجم بیان می‌کند. بخش 6 به تجزیه‌وتحلیل شکاف‌ها می‌پردازد. بخش 7 مسائل درحال ظهور و باز را بیان می‌کند و در بخش 8 نتیجه‌گیری بیان می‌شود.

2. ویژگی‌های VANET ، چالش‌های امنیتی و محدودیت‌ها

2.1 ویژگی‌های VANET

VANET ها شبکه‌های ad hoc، بسیار پویا، با دسترسی کم به زیرساخت‌های شبکه و ارائه خدمات متعدد می‌باشند. حالت‌های ارتباطی در VANET که در شکل 2 نشان داده شده است می‌تواند به کلاس‌های خودرو به خودرو (V2V)، خودرو به زیرساخت (V2I) و ترکیبی طبقه‌بندی شود. در V2V، رسانه‌های ارتباطی استفاده شده، با زمان تاخیر کوتاه و نرخ انتقال بالا نشان داده شده‌اند. این معماری در حالات مختلف هشدار (ترمز اضطراری، برخورد، کاهش سرعت، و غیره) و یا در رانندگی مشارکتی استفاده شده است. در V2I شبکه وسایل نقلیه، برنامه‌های کاربردی با استفاده از زیرساخت RSU و از طریق پورتال اینترنتی مشترک ارتباط برقرار می‌کنند. حالت ترکیبی، ترکیبی از دو روش قبلی است. ویژگی‌های VANET بررسی شده در [1-6] را می‌توان به دو گروه تقسیم کرد: 1) توپولوژی شبکه و روش ارتباطات یا 2) وسایل نقلیه و رانندگان.

1) ویژگی‌هایVANET مربوط به توپولوژی شبکه و حالت ارتباطات:

• شبکه بی‌کران و مقیاس‌پذیر: VANET را می‌توان در یک یا چند شهر و حتی برای کشورها پیاده‌سازی کرد. بنابراین نیاز به همکاری و مدیریت برای برآوردن نیازمندی‌های امنیتی دارد.

• ارتباطات بی‌سیم: اتصال گره‌ها و تبادل اطلاعات بین آن‌ها، از طریق کانال‌های بی‌سیم انجام می‌شود. بنابراین نیاز به ارتباطات امن دارد.

• تحرک بالا و تغییر سریع توپولوژی شبکه: گره‌ها در حال حرکت با سرعت بالا / تصادفی هستند که پیش‌بینی موقعیت و توپولوژی شبکه را مشکل می‌کند. بنابراین افزایش حریم خصوصی موجب عدم قطع ارتباط، نوسانات و دستکاری می‌شود. که فاقد حیاتی نسبتا طولانی (به‌عنوان مثال، رمز عبور) است که برای ارتباطات امن وسایل نقلیه غیرعملی است. تحت این محدودیت‌ها، تاخیر انتشار هشدار باید مهم شمرده شود. عملکرد خوب تاخیر با استفاده از رمزنگاری سریع الگوریتم یا با تصدیق موجودیت و تحویل پیام در زمان مورد نیاز است. برای این کار، اولویت‌بندی پکیج داده و

روش ازدحام از اهمیت بالاتری برخوردار است؛ داده‌های مربوط به ایمنی ترافیک و بهره‌وری باید سریع تر از موارد دیگر باشد.

• علاوه بر قابلیت اعتماد، حمل و نقل بین لایه‌های شبکه برای پشتیبانی از زمان واقعی و برنامه‌های کاربردی چندرسانه‌ای پیشنهاد شده است.

2) ویژگی‌هاVANET مربوط به وسایل نقلیه و رانندگان:

• قدرت پردازش بالا و انرژی کافی: گره‌های VANET هیچ مسئله‌ای با منابع انرژی و محاسبات ندارند. آنها انرژی خود را در قالب باتری و قدرت پردازش بالا برای اجرای محاسبات پیچیده رمزنگاری دارند.

• حفاظت بهتر فیزیکی: گره‌های VANET از نظر فیزیکی بهتر محافظت می‌شوند. که این مسئله مقایسه به لحاظ فیزیکی را دچار مشکل می‌کند. بنابراین تاثیر حملات زیرساخت را کاهش می‌دهد.

• زمان شناخته شده و موقعیت: بسیاری از وسایل نقلیه مجهز به GPS هستند چرا که بسیاری از برنامه‌های کاربردی بر موقعیت جغرافیایی و یا منطقه تکیه دارند. GPS برای محلی‌سازی و محافظت امن از محل گره در برابر حملات استفاده می‌شود.

• اکثریت شرکت‌کنندگان صادق هستند: فرض می‌شود اکثر رانندگان برای یافتن تهدید خوب و مفید عمل می‌کنند.

• زیرساخت‌های اجرایی قانون: از طریق مأموران اجرای قانون، آنها می‌توانند تهدید وارد بر سیستم را شناسایی و مورد حمله قرار دهند.

• ثبت مرکزی با تعمیر و نگهداری دوره‌ای و بازرسی: وسایل نقلیه با قدرت مرکزی ثبت می‌شوند و شناسه منحصر به فرد (پلاک) دارند. تعمیر و نگهداری دوره‌ای وسایل نقلیه برای به روز رسانی سیستم عامل و نرم‌افزار است. در PKC (رمزنگاری کلید عمومی)، تعمیر و نگهداری برای به روز رسانی گواهینامه‌ها، کلیدها و به‌دست آوردن CRL جدید (لیست ابطال گواهی) است.

به‌طورخلاصه، شبکه وسایل نقلیه، تعامل بین رفتار رانندگان و همکاری توسط آنان در شبکه است. کاوش در یک راه‌حل امنیتی باید تمام موارد مرتبط را بیابد. پس از ارائه ویژگی‌های VANET، جزئیات چالش‌های امنیتی و محدودیت‌های VANET در بخش بعدی بررسی خواهد شد.

2.2 چالش‌های امنیتی و محدودیت‌های VANET

در VANET، امنیت باید تضمین کننده‌ی پیام‌های اضافه شده و یا اصلاح شده توسط مهاجمان باشد. همچنین، قابلیت اعتماد رانندگان برای اطلاع محیط ترافیک در درون محدودیت زمانی ضروری است. چالش‌های امنیتی منحصر به فرد به‌دلیل ویژگی‌های متمایز VANET افزایش می‌یابد. بدرفتاری این چالش‌های امنیتی منجر به بسیاری از محدودیت‌ها می‌شود. برخی از این چالش‌های امنیتی در زیر بیان شده است:

• اندازه شبکه، ارتباط جغرافیایی، تحرک بالا و توپولوژی پویا، مدت اتصال کوتاه، قطع فرکانس‌های کم‌حجم [1،2]: اندازه شبکه می‌تواند از لحاظ جغرافیایی بیکران و بسیار مقیاس‌پذیر و بنا به نفوذ استانداردهای لازم برای آن در حال رشد باشد.

• تایید اطلاعات با قابلیت اعتماد: اعتماد به‌عنوان طبیعت VANET برای ایجاد انگیزه و جمع‌آوری اطلاعات از سایر وسایل نقلیه و RSUs لازم است [7]. از این رو این تبادل اطلاعات تکراری است و باید قابل اعتماد و یکپارچگی آن مورد تأیید باشد. قابلیت اعتماد اطلاعات بیشتر از تایید توسط گره‌های انتقال مفید است [2].

• توزیع کلید: مکانیزم‌های امنیتی بر روی کلید، به توزیع مهم آنها بستگی دارد.

• الگوریتم حمل‌ونقل: چالش مربوط به تعداد بسته‌های منتقل شده و یافتن بهترین مسیر است. که ارتباط تک پخشی، پخش فراگیر، V2V، V2I یا ترکیبی است.

در حالی که برای محدودیت VANET و یا نیازمندی‌ها [1]، می‌توانیم موارد زیر را بیان کنیم:

• کنترل برخورد و ازدحام: توجه به اندازه شبکه محصور شده ضروری است.

• تحمل کم به هنگام وقوع خطا: برخی از پروتکل‌ها براساس احتمالات است و هر گونه خطایی می‌تواند بر زندگی مردم تأثیر گذارد.

• تاثیر محیطی: موانع موجب انتشار امواج مغناطیسی[1] می‌شود.

• تجزیه و تحلیل خطر و مدیریت: گاهی اوقات می‌توانیم راه‌حل حملات را پیدا کنیم اما پیدا کردن مدل‌ها بنا به رفتار مهاجمان هنوز غیرمعلوم است.

• Anonymity، حفظ حریم خصوصی و مسئولیت: گره‌های مسئول دریافت داده‌ها نیاز به اعتماد به فرستنده دارند. حفظ حریم خصوصی، هویت خودرو ناشناس را تضمین می‌کند. گاهی اوقات گره‌های تصدیق شده می‌توانند مسائل مالی داشته باشند. بنابراین، یک راه‌حل تجاری برای حفظ حریم خصوصی و مسئولیت موردنیاز است.

اگر سرویس‌های امنیتی ارائه شده در بخش بعدی را بهتر مدیریت کنیم این چالش‌های امنیتی و محدودیت‌ها را می‌توان به حداقل رساند.

2.3 نیازمندی‌های امنیتی (خدمات)

سرویس‌های امنیتی موجب افزایش امنیت پردازش‌ها و تبادل اطلاعات در VANET می‌شود. نیازمندی‌های امنیتی عبارتند از:

• احراز هویت: تضمین می‌کند که این پیام توسط یک کاربر قانونی با استفاده از گواهی تولید می‌شود. یا گیرنده، فرستنده پیام را از طریق یک نام مستعار شناسایی می‌کند [8].

• دردسترس بودن: با مقاومت در برابر حملات داس (انکار سرویس)، از عملکرد طبیعی اطمینان حاصل می‌کنیم. زیرا تاخیر چند ثانیه‌ای باعث می‌شود پیام بی‌معنی گردد [4].

• محرمانه: شامل مجموعه‌ای از قوانین است که موجب محدودیت دسترسی به منابع خاص می‌شود. این مسئله با استفاده از رمزگذاری و یا تبادل پیام ویژه بین OBUs و RSUs به‌عنوان نوعی تأیید اطلاعات انجام می‌گیرد [9].

• انکارناپذیری: فرستنده نمی‌تواند ارسال یک پیام را انکار کند. بنابراین می‌تواند پس از آسیب به دستگاه بازیابی(TPD) شود [4].

• صداقت: بدون تغییر برای داده. امضای دیجیتال برای پیام و تمامیت داده‌ها [3،10] استفاده می‌شود.

• حریم خصوصی و Anonymity: مخفی کردن هویت کاربر در برابر گره‌های غیرمجاز با استفاده از کلید موقت و ناشناس. بنابراین حریم خصوصی محل باید حفظ شود.

• بررسی داده: برای از بین بردن پیام‌های نادرست است. تایید انسجام داده‌ها با پیام‌های مشابه برای تشخیص صحت داده‌ها استفاده می‌شود، به خصوص در بین وسایل نقلیه همسایه.

• کنترل دسترسی: تمام گره‌ها با توجه به قوانین عمل می‌کنند [11].

• قابلیت ردیابی و انفصال: هویت واقعی خودرو باید از دیگران پنهان شود، بنابراین باید یک جزء با توانایی به‌دست آوردن هویت واقعی وسایل نقلیه برای لغو استفاده از آنها در آینده وجود داشته باشد.

جدول 1. طبقه‌بندی نیازمندی‌های امنیتی.

Classification of security requirements.

VANET communication mode	Security requirements
V2V, V2I	Availability Confidentiality Error detection Liability identification Authentication Non-repudiation Privacy and anonymity Flexibility and efficiency Location privacy Integrity Traceability Data verification
V2I	Revocability Access control
V2V	Data verification

• تشخیص خطا: برای تشخیص خرابکاری و انتقال نادرست.

• شناسایی مسئولیت: مسئولیت شناسایی کاربر به هنگام ارتباطات. پیام‌ها می‌توانند برای شناسایی کاربران مورد استفاده قرار گیرند.

• انعطاف‌پذیری و بهره‌وری: انعطاف‌پذیری در امنیت معماری و طراحی سیستم قابل توجه است. هر چند که برای استفاده ایمن از ترافیک ضروری است و نیاز به زمان و پهنای باند کمتری دارد. این مسئله در راندمان کانال و در تاخیر کم ناشی از آن بسیار مهم است.

پس از تعریف و تجزیه و تحلیل نیازمندی‌های امنیتی، آنها را در جدول 1 براساس نیاز آنها در ارتباطات VANET، برای V2V، V2I یا هر دو نشان دادیم. برای حالت ارتباطات VANET، پیش‌نیازهای آن برای خدمات امنیتی را تعریف می‌کنیم.

3. مدل مهاجم

استقرار یک سیستم امنیتی برای VANET یک مسئله چالش‌برانگیز است. در واقع، طبیعت بسیار پویا با قطع مکرر ارتباط، ورود و خروج آنی وسایل نقلیه، استفاده از کانال‌های بی‌سیم برای پیام‌های اضطراری و ایمنی، VANET را در معرض تهدیدها و حملات مختلف قرار می‌دهد. در این بخش حملات را طبقه‌بندی می‌کنیم، مهاجمان و تجزیه و تحلیل حالت‌های ارتباطی VANET را تحت تاثیر قرار می‌دهد.

3.1 حملات

بسیاری از محققان در [2،3،5،7،9،10،23] حملات در VANETs را بررسی کردند. طبقه‌بندی این حملات مفید است زیرا ماهیت VANET آسیب‌پذیری‌ها و محدودیت‌هایی دارد که نیاز به راه‌حل دارد. با تقسیم، می‌توانیم بهتر کنترل کنیم.

حملات را می‌توان به چهار گروه اصلی طبقه‌بندی کرد: (1) آنهایی که در معرض خطر رابط بی‌سیم هستند، (2) آنهایی که تهدیدی برای سخت‌افزار و نرم‌افزار هستند، (3) آنهایی که خطر مطرحی در سنسور خودرو ایجاد می‌کنند (4) آنهایی که خطر دسترسی بی‌سیم را پشت سر می‌گذارند، این بدان معنی است که در زیرساخت‌ها (CA یا وسیله نقلیه کارخانه سازنده) وجود خواهد داشت. زیر بخش زیر تهدیدات مربوط به هر یک از موارد ذکر شده در بالا را بیان می‌کند.

1) تهدیدات مربوط به رابط بی‌سیم

• هویت و موقعیت جغرافیایی آشکار (ردیابی مکان): یک مهاجم سعی می‌کند برای دریافت اطلاعات از راننده او را ردیابی کند. این مسئله موجب می‌شود یک گره خاص در معرض خطر قرار گیرد. به‌عنوان مثال، یک شرکت کرایه اتومبیل می‌خواهد به دنبال یک روش برای وسایل نقلیه خود باشد. کاربران می‌توانند ردیابی شوند و هیچ حریم خصوصی ندارند.

• DoS: یک مهاجم سعی می‌کند تا منابع و سرویس‌های غیرقابل دسترس کاربران در شبکه را مهیا کند. این مسئله از طریق تراکم کانال فیزیکی و "محرومیت از خواب" قابل دسترسی است.

DDoS (سرویس توزیع شده انکاری): یک حمله داس مجزا از مکان است.

• حمله Sybil: مهاجم، وسایل نقلیه متعددی در جاده‌ها با هویت یکسان ایجاد می‌کند. که با ارسال برخی پیام‌های اشتباه برای بهره‌گیری از مهاجم وارد عمل می‌شود.

• تروجان: مهاجم، پیام‌های اسپم در شبکه را برای مصرف پهنای باند شبکه و افزایش زمان تاخیر ماموریت می‌فرستد. کنترل این نوع حمله، به‌دلیل عدم وجود زیرساخت‌های لازم و مدیریت متمرکز دشوار است. پس شروع به انتشار پیام‌های اسپم مهاجم به یک گروه از کاربران می‌کند. پیام‌هایی که هیچ نگرانی برای کاربران ندارند.

• Spam: یک گره خودی، پیام‌های اسپم را برای افزایش انتقال، تاخیر و مصرف پهنای باند انتقال می‌دهد.

• Man in Middle Attack (MiM): یک گره مخرب به ارتباط بین دو وسیله نقلیه دیگر گوش می‌دهد. و وانمود می‌کند که هر یک از آنها به دیگری پاسخ می‌دهد. و موجب انتقال اطلاعات نادرست بین آنها می‌شود.

• حمله نیروی بی‌رحم: یک روش آزمون و خطای استفادهشده توسط مهاجم برای به دست آوردن اطلاعات مانند رمز عبور کاربران یا هر شماره شناسایی یا کرک داده‌های رمزگذاری شده، برای تست امنیت شبکه است.

• حمله سیاه چاله: یک گره مخرب کوتاه‌ترین مسیر برای دریافت داده‌ها را اعلام می‌کند و سپس آنها را ردیابی می‌کند. گره مخرب قادر به رهگیری داده و یا حفظ آن است. زمانی که مسیر جعلی است، گره تصمیم به رها کردن و یا به جلو بردن بسته می‌گیرد.

2) تهدید سخت‌افزار و نرم‌افزار

علاوه بر حملات داس، حمله Sybil، تروجان‌ها و هرزنامه، MIM و حملات نیروی بی‌رحم که در بالا عنوان شد (1) می‌توانیم موارد زیر را بیان کنیم:

• تزریق پیام‌های خطا (اطلاعات ساختگی): مهاجم عمدا اطلاعات ساختگی در داخل شبکه تزریق می‌کند. این مسئله رفتار کاربران را تحت تاثیر قرار می‌دهد. این امر باعث تصادفات و یا تغییر مسیر ترافیک در مسیر استفاده شده می‌شود.

• سرکوب پیام یا تغییر: مهاجم بسته را از شبکه ربوده یا تغییراتی در محتوای پیام ایجاد می‌کند. علاوه بر ساخت حمله که پیام جدید تولید می‌کند، حمله جواب، دوباره پیام‌های قدیمی و یا حقه‌بازی را با تزریق حجم بالایی از پیام‌های هشداردهنده نادرست برای وسایل نقلیه پخش می‌کند.

• Usurpation هویت یک گره (حقه‌بازی و یا Impersonation یا Masquerade): یک مهاجم سعی در جعل هویت یک گره دیگر برای دریافت پیام‌های آن و یا برای به‌دست آوردن امتیازات داده شده به او دارد.

• دستکاری سخت‌افزار: برخی از کارمندان مخرب در طول نگهداری سالانه، در تولیدکننده وسیله نقلیه، سعی در آسیب رساندن به سخت‌افزار با گرفتن یا دادن داده‌های خاص دارند.

• مسیریابی حمله: مهاجم از آسیب‌پذیری لایه شبکه، با حذف بسته و یا اخلال در مسیریابی سوء استفاده می‌کند. علاوه بر این به حمله سیاه چاله شامل:

- حمله Wormhole: استراق سمع داده‌ها؛ یک مهاجم بسته را دریافت و در یک نقطه دیگر در مسیر هدف قرار می‌دهد. او آن را از آنجا تکرار می‌کند.

- حمله Greyhole: یک گره مخرب، شبکه را با موافقت با ارسال بسته‌های اطلاعاتی گمراه می‌کند. اما گاهی اوقات، آنها را برای مدتی به حالت عادی خود بازمی‌گرداند.

• تقلب با اطلاعات موقعیت (حقه بازی GPS) و حمله تونل زنی: وسایل نقلیه مواضع نادرست تولید می‌کند که باعث تصادفات شده و GPS کار نمی‌کند.

• حمله زمان‌بندی: وسایل نقلیه مخرب برخی از زمان‌های مربوط به دریافت پیام را برای ایجاد تاخیر قبل از حمل و نقل آن اضافه می‌کنند. بنابراین، وسایل نقلیه همسایه آن را پس از مرتفع کردن نیازهایش دریافت می‌کند یا بعد از لحظه‌ای آنها را دریافت خواهد کرد.

• حمله پخش: کاربران مخرب و یا غیرمجاز سعی در جعل هویت یک کاربر قانونی / RSU با استفاده از فریم قبلا تولید شده در ارتباطات جدید می‌کنند.

3) تهدید سنسور ورودی در خودرو

علاوه بر حقه‌بازی GPS در بخش (2)، موارد زیر را ارائه می‌کنیم:

• حمله توهم: مهاجم هدف را در ماشین خود برای قرائت اشتباه سنسور مورد حمله قرار می‌دهد. بنابراین، پیام‌های نادرست هشداردهنده ترافیک به همسایه‌ها پخش می‌شود.

• انباشتن حمله: مهاجم در فرکانس رادیو استفاده شده توسط گره VANET تداخل ایجاد می‌کند.

4) تهدید زیرساخت

علاوه بر حقه‌بازی، Impersonation و Tampering message و حمله hardware در زیر بخش‌های (1) و (2)، موارد زیر را بیان می‌کنیم

• دسترسی‌های غیرمجاز: اشخاص مخرب سعی در دسترسی به خدمات شبکه بدون داشتن حقوق و امتیازات دارند. این مسئله باعث حوادث، آسیب و یا جاسوسی اطلاعات محرمانه می‌شود.

• Session Hijacking: احراز هویت در ابتدا انجام داده است. پس از آن، هکرها جلسه بین گره‌ها را کنترل می‌کنند.

• Repudiation (از دست دادن قابلیت ردیابی رویداد): محرومیت یک گره در یک ارتباط.

جدول 2 طبقه‌بندی حملات و حالت‌های ارتباطی VANET را (V2V، V2I یا هر دو) را ارائه کرده است. این طبقه‌بندی به شناسایی حملات از پیش تعریف شده (سخت‌افزار یا نرم‌افزار، کاربران و یا مقامات) کمک می‌کند و وضعیت ارتباط

آنها در VANET را تحت تاثیر قرار می‌دهد. در نتیجه جلوگیری از این حملات و تلاش برای به حداقل رساندن اثرات آنها آسان‌تر است

3.2 مهاجمان

حملات VANET یکی از مباحث مورد علاقه‌ی محققان در [2،3،9،24] است. نام‌های متعارف بسیاری از اقدامات و اهداف در زیر ذکر شده است:

• خودِ راننده: او می‌تواند ترافیک مسیر را تغییر دهد.

• حمله‌های مخرب: او اهداف خاصی دارد. که باعث خسارات و مضراتی از طریق برنامه‌های کاربردی در VANET می‌شود.

• Pranksters: مهاجم همه چیز را برای تفریح خود انجام می‌دهد. مانند داس یا تغییر پیام (هشدار خطر) به علت ترافیک جاده.

• رانندگان حریص: آنها برای منافع خود دست به حمله می‌زنند. به‌عنوان مثال: ارسال پیام تصادفی ممکن است موجب ازدحام در جاده یا ارسال پیام دروغین برای آزاد کردن جاده‌ها شود.

• جاسوسان/ استراق سمع: مهاجم سعی در جمع‌آوری اطلاعات در مورد منابع دیگر دارد.

• Industrial insider: درحال به‌روزرسانی سیستم‌عامل و یا توزیع کلید، کارکنان مخرب به دستکاری سخت‌افزار دست می‌زنند.

مهاجمان به چند بخش طبقه‌بندی می‌شوند:

- داخلی در مقابل خارجی: داخلی نشان‌دهنده تصدیق کاربر در شبکه، درمقابل خارجی با ظرفیت محدود برای حمله.

- Malicious در مقابل منطقی: حمله Malicious به هر شخصی در مقابل حملات منطقی که سود شخصی و قابل پیش‌بینی دارند.

جدول 2. طبقه‌بندی حملات براساس چهار دسته و حالات ارتباطی VANET

Attacks on	Attack name	Attack on VANET communication mode
Wireless interface	– Location Tracking – DoS, DDoS – Sybil – Malware and spam. – Tunnelling, Blackhole, Greyhole. – MiM – Brute force	V2V
Hardware and software	– DoS – Spoofing and forgery. – Cheating with position info (GPS spoofing). – Message suppression/ alteration/fabrication. – Replay – Masquerade – Malware and spam – MiM – Brute force	V2V, V2I
	– Sybil – Injection of erroneous messages (bogus info). – Tampering hardware – Routing, Blackhole, wormhole and Greyhole. – Timing.	V2V
Sensors input in vehicle	– Cheating with position info(GPS spoofing) – Illusion attack – Jamming attack	V2V
Infrastructure	– Session hijacking – DoS, DDoS – Unauthorized access – Tampering hardware – Repudiation – Spoofing, impersonation or masquerade	V2I and V2V

فعال سطحی در مقابل منفعل: مهاجم فعال سیگنال‌ها یا بسته را در مقابل یک مهاجم منفعل که فقط حواسش به شبکه است تولید می‌کند.

محلی در مقابل توسعه یافته: مهاجم محلی با دامنه محدود و در چند وسیله نقلیه و یا ایستگاه‌های پایه کار می‌کند درحالی‌که مهاجم توسعه یافته با دامنه‌ای گسترده و در سراسر شبکه کار می‌کند.

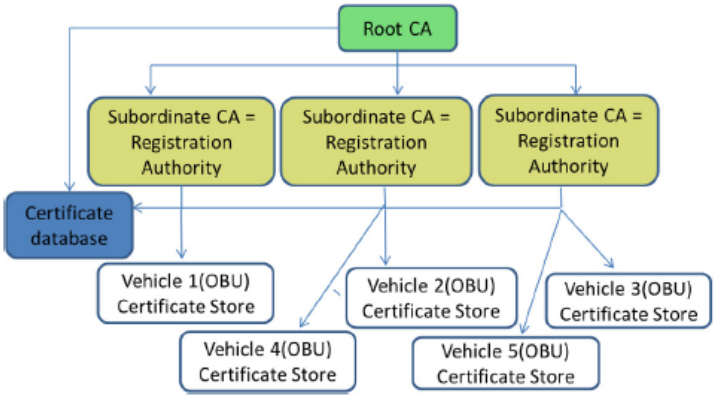
پس از بیان جزئیات حملات طبقه‌بندی شده و مهاجمان، در بخش بعدی استانداردسازی و تلاش‌های پروژه‌های اخیر بیان خواهد شد.

4. تلاش‌های استانداردسازی شده

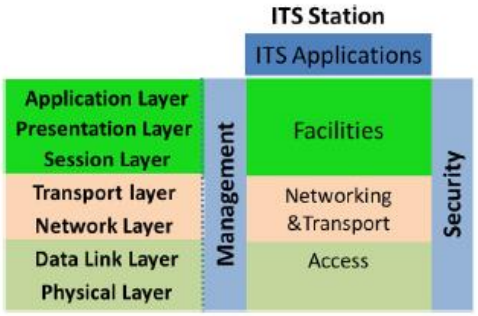
زیرساخت یک بنیاد اساسی برای یک سیستم است. معماری امنیت، طراحی امنیت است. که الزامات و خطرات بالقوه در یک محیط خاص را در کنترل‌های امنیتی اعمال می‌کند. استاندارد، جزئیات موردنیاز در مورد چگونگی اجرای یک

سیاست را بیان می‌کند. در VANET، بسیاری از گروه‌ها [12-16] شامل معماری امنیت و زیرساخت‌های بررسی شده است. که آنها پروتکل‌های امنیتی استاندارد [17،21] یا معماری امنیتی تولید و تعریف می‌کنند [18]. پروژه‌های دیگری مانند Scoop@F[20] و C-Roas در حال حاضر در مورد امنیت (سیستم حمل و نقل هوشمند) تحقیق می‌شوند.

در ادامه، ابتدا به جزئیات محبوب زیرساخت امنیت یعنی PKI (زیرساخت کلید عمومی)، سپس به معماری امنیتی VANET و استانداردهای پروتکل‌های امنیتی شناخته شده می‌پردازیم.



شکل 3. طرح PKI



شکل 4. نگاشت OSI به لایه‌های معماری ETSI

4.1 زیرساخت‌های امنیتی: PKI

در بررسی زیرساخت‌های امنیتی VANET، PKI جزء موارد پراستفاده است. همان‌طور که در شکل 3 نشان داده شده است PKI از توزیع و شناسایی کلیدهای رمزگذاری عمومی پشتیبانی می‌کند. این مسئله موجب می‌شود که کاربران

به تبادل اطلاعات امن بر روی شبکه و تایید هویت طرف دیگر بپردازند. PKI شامل سخت‌افزار، نرم‌افزار، سیاست‌ها و استانداردها است. که همه با هم ایجاد، توزیع و ابطال کلید و گواهی دیجیتال را مدیریت می‌کنند. PKI شامل عناصر کلیدی زیر است:

• A trusted party، یک گواهی مرجع اصلی (CA) است. که به‌عنوان اساس اعتماد عمل می‌کند و خدمات برای تصدیق هویت اشخاص ارائه می‌دهد.

• A registration authority، CA نامیده می‌شود، که توسط یک CA تایید شده است. که مسائل مربوط به گواهی را برای استفاده‌های خاص حل می‌کند. و برای محافظت از CA استفاده می‌شود. ارتباطات کاربران از طریق CA انجام می‌گیرد در نتیجه می‌تواند هرگونه حمله‌ای را قبل از رسیدن به CA شناسایی کند.

• پایگاه داده گواهی، که مسائل درخواست گواهی / لغو گواهی را پیگیری می‌کند. و توسط ریشه و CA قابل دسترسی است.

• فروشگاه گواهی، که بر روی هر خودرو برای ذخیره گواهی و کلیدهای خصوصی قرار دارد.

به‌طورخلاصه، فرآیندهای توزیع کلیدهای رمزنگاری و تایید گواهی توسط ریشه و CA انجام شده‌اند. آنها سطح دسترسی وسایل نقلیه را در شبکه وسایل نقلیه با استفاده از نرم‌افزار/سخت‌افزار خاص و ارتباطات بی‌سیم/باسیم شناسایی می‌کنند.

4.2 معماری امنیت

بسیاری از گروه‌ها در اروپا و ایالات متحده آمریکا معماری امنیت خود را براساس PKI می‌سازند. در اروپا (EU)، ETSI در [18] معماری امنیتی خود را برای ITS (سیستم حمل و نقل هوشمند) تعریف کرده است. در ایالات متحده آمریکا، در کنسرسیوم ایمنی ارتباطات خودرو (VSC)، VSC-A (نرم‌افزار ارتباطات ایمن خودرو)، NHTSA (اداره ایمنی ترافیک ملی) [12] را با معماری امنیتی خود برای VANETدر نظرگرفته است.

جدول 3. سرویس‌های امنیتی در معماری ETSI و NHTSA

Security service	Architectures
Authentication	NHTSA authenticates via digital signature and encryption. ETSI via signed messages.
Confidentiality	NHTSA and ETSI via symmetric and asymmetric encryption.
Integrity	NHTSA assures the integrity via Message Authentication Code. ETSI check the value of signed message.
Liability identification	NHTSA via Misbehavior Authority. ETSI via accountability and remote management.
Message security	NHTSA and ETSI use PKI. NHTSA use ECDSA.
Non-repudiation	ETSI and NHTSA have EDR for tracing.
Privacy	NHTSA uses an anonymizer proxy and privacy-preserving revocation via MA.

ETSI در [18] معماری امنیتی برای ارتباطات ITS مشخص می‌کند. براساس سرویس‌های امنیتی تعریف شده در [22]، عملکرد نهادها و روابط آنها را شناسایی می‌کند: EA (ثبت سازمان)، AA (مجوز سازمان) و ITS-S (ایستگاه سیستم ارتباطات هوشمند). چرخه عمر امنیت ITS-S ابتدا در تولیدکننده و سپس در ثبت، مجوز و تعمیر و نگهداری آغاز می‌شود. معماری ITS-S مبتنی بر چهار لایه پردازشی است: لایه دسترسی، لایه شبکه و حمل‌ونقل، لایه امکانات و لایه برنامه‌های کاربردی محدود شده توسط دو لایه عمودی: مدیریت و امنیت در شکل 4 نشان داده شده است. تایید EA (اعتباربخشی و کمک‌های مالی) که یک ITS-S قابل اعتماد است بنا به ارتباطات عمل می‌کند. AA اثبات ITS-S را برای استفاده از خدمات خاص با صدور مجوز فراهم می‌کند. CI (شناسایی متعارف) برای ITS-S منحصر به فرد در سطح جهانی است.

NHTSA یک معماری امنیتی [12] براساس PKI ارائه کرده است. آنها عملکرد دقیق نهادها را براساس گواهی‌نامه‌های بلندمدت برای OBU (توابع بوت استرپ) و گواهینامه‌های کوتاه مدت دیجیتال (توابع مستعار) با جزئیات بیان می‌کنند. موضوع اصلی آنها اعتماد است. نهادهای معماری NHTSA در شکل 5 نشان داده شده است. در پیشنهاد آنها، ارتباطات V2V متشکل از دو نوع پیام است: BSM (پیام عمومی ایمنی) و پیام مدیریت امنیت. در BSM، امضای دیجیتال و گواهی‌نامه برای تایید هدف استفاده می‌شود. برای ارتباطات بین وسایل نقلیه و SCMS (سیستم مدیریت امنیت گواهینامه)، رمزنگاری نامتقارن ECIES (طرح رمزگذاری منحنی بیضوی) برای محرمانه بودن و امضای دیجیتالی ECDSA (الگوریتم امضای دیجیتال منحنی بیضوی) برای اعتبارسنجی وسایل نقلیه استفاده شده است. برای ارتباطات داخل SCMS (نهاد به نهاد)، رمزنگاری متقارن AES-CCM (استاندارد رمزگذاری پیشرفته با CBC-MAC) برای

محرمانه بودن با MAC (کد تأیید هویت) و یکپارچگی استفاده می‌شود. این معماری امنیتی حریم خصوصی را در برابر حملات داخلی و خارجی حفظ می‌کند؛ SCMS تک جزئی نمی‌تواند دو گواهی را به یک دستگاه یکسان(بدون ردیابی) لینک کند و هیچ اطلاعات ذخیره شده‌ای در SCMS نمی‌تواند گواهی را به یک وسیله نقلیه خاص یا مالک پیوند دهد. MA (سوء رفتار سازمان) تداوم گره مورد اعتماد را، با تولید / نشر CRL و سوء رفتار در گزارش VANET اطمینان می‌دهد. LOP (پروکسی Obscurer محل) به‌عنوان پروکسی anonymizer عمل می‌کند و گزارش سوء رفتار توسط OBUs به MA ارسال می‌شود. حفظ کارآمد حریم خصوصی موجب ابطال حملات خطرناک می‌شود.

جدول 3 سرویس‌های امنیتی درون معماری ETSI و NHTSA را فراهم می‌کند. پس از ارائه معماری‌های امنیتی، در بخش بعدی به استانداردهای امنیتی شناخته شده در VANET می‌پردازیم.

4.3 استانداردهای امنیتی

برای استانداردسازی، استانداردهای امنیتی IEEE 1609.2 و ETSI را در نظر می‌گیریم.

استاندارد امنیتی IEEE 1609.2 [16،19] روشی برای تامین امنیت فرمت‌های پیام، پیام نرم‌افزار و پیام‌های پردازش استفاده شده توسط WAVE (دسترسی بی‌سیم در محیط) ارائه می‌کند. همه این مسائل امنیتی براساس PKI بااستفاده از کلید و گواهی مدیریتی هستند. رمزنگاری متقارن AES-CCM، امضای نامتقارنECDSA و رمزگذاری نامتقارن ECIES برای توزیع کلید و ایمنی پیام استفاده می‌شوند. نیازمندی‌های امنیتی در این استاندارد مانند محرمانه بودن، اصالت، عدم انکار و صداقت باید اندازه‌گیری شود اما نامش فاش نشود، هیچ مکانیزمی برای ارتباط چند هاپ در V2V تعریف نشده است.

ETSI در [13،18،22] خدمات امنیتی و معماری و مدیریت امنیت ارتباطات خود را تعریف کرده است. ما معماری امنیتی استاندارد ETSI را در بخش 4.2 مورد بحث قرار دادیم. جدول 4 خلاصه‌ای از نگاشت بین سرویس‌های امنیتی ETSI و IEEE 1609.2 بیان می‌کند [22].

از جدول 4 چنین نتیجه‌گیری می‌شود که، برخی از خدمات در ETSI از دست رفته‌اند و یا در حال توسعه در IEEE 1609.2 هستند. پاسخگویی، مدیریت از راه دور و گزارش به‌طور کامل در IEEE 1609.2 وجود ندارد. درحالی‌که در بررسی، IEEE 1069.2 از پارامترهای پویا استفاده می‌کند. برای حفاظت از پخش، IEEE 1609.2 از برچسب زمان استفاده می‌کند اما از شماره‌های سریال و به ترتیب استفاده نمی‌کند. در نهایت برای مدیریت انجمن امنیتی (جلسه)، IEEE 1609.2 امنیت در هر جلسه را با گواهی و امضا بررسی می‌کند اما یک انجمن امنیتی بین دو ITS-S ارتباطاتی ایجاد و مدیریت نمی‌کند.

پس از تشریح تلاش‌های استانداردسازی، به بخش بعدی می‌رویم و به گسترش بسیاری از راه‌حل‌های پیشنهادی برای حملات مختلف در VANET می‌پردازیم.

5. راه‌حل‌های پیشنهادی از کارهای گذشته برای حملات قبلا توضیح داده شده

بسیاری از محققان سعی در ارائه راه‌حل برای حملات قبلا توصیف شده دارند. ما این طرحها را براساس حملات ذکر شده در بخش 3.1 طبقه‌بندی می‌کنیم.

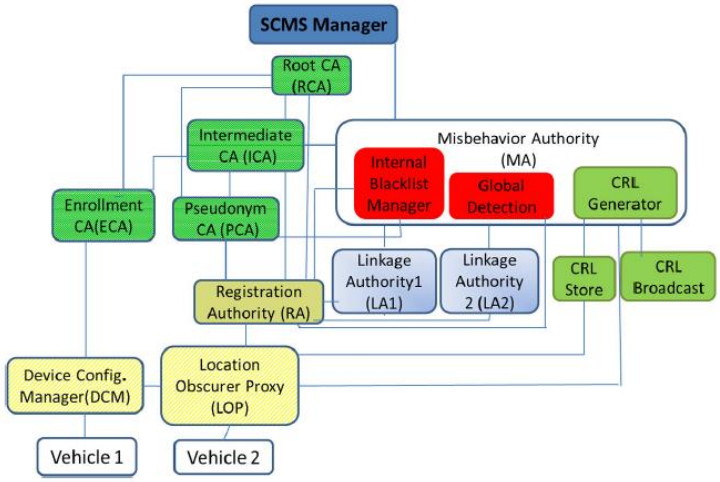
5.1 حمله به رابط‌های بی‌سیم:

برای ردیابی، استراق سمع و تجزیه و تحلیل ترافیک حملات:

حفظ حریم خصوصی یکی از درمان‌های اولیه برای این حملات است. بسیاری از محققان از تکنیک‌های مورد بررسی بسیاری برای حفظ حریم خصوصی در VANET استفاده کرده‌اند [53]: این مسئله می‌تواند توسط مجموعه‌ای از کلیدهای ناشناس با توجه به سرعت رانندگی و یا از طریق نام مستعار که می‌تواند به هویت واقعی کاربر مرتبط باشد تضمین شود [25]و[12،27،26].

استاندارد ETSI [28] مدیریت حفظ حریم خصوصی برای یک گره براساس فاش نشدن نامش، unobservability مشخص می‌شود. ارتباط بین گره‌ها با استفاده از SA (انجمن امنیت) و مدیریت کلید انجام می‌شود. نویسندگان در [3]

بارگذاری کلید ناشناس در TPD را پیشنهاد کردند که توسط CA و پلاک‌های الکترونیکی (ELP) قابل ترسیم است. [29] برای حفظ هویت گره و محل خصوصی پیشنهاد می‌دهد. بنابراین بااستفاده از یک گروه غیرمتمرکز احراز هویت با مجموعه‌ای از کلیدهای ناشناس، نام مستعار، امضا گروه و ECPP، پروتکل احراز هویت ناشناس می‌ماند. در [30]، وسایل نقلیه از گواهینامه‌های موقت بسیاری (نام مستعار) استفاده می‌کنند تا نتوانند با یکدیگر ارتباط داشته باشند. [24] استفاده از متغیرهای MAC (کنترل دسترسی رسانه) و آدرس IP را برای جدا کردن آدرس از هویت وسایل نقلیه و رانندگان پیشنهاد می‌دهد [23]. [31] VIPER (پروتکل اجرای حریم خودرو به زیرساخت) را برای ارتباطات V2I استفاده می‌کند.



شکل 5. طراحی سیستم امنیتی NHTSA

جدول 4. نگاشت سرویس‌های امنیتی ETSI با IEEE 1609.2.

Security service group	ETSI security service at Rx/Tx	Mapping definition IEEE 1609.2
Enrolment	Obtain/Remove/Update Enrolment Credentials	Certificate Signing Request
Authorization	Obtain/Update Authorization Ticket Publish/Update authorization Status Add/Validate authorization credential to single message	Certificate Signing Request Certificate Revocation List(CRL) request/update Signed Messages and processing signed messages
Security association management (session)	Establish/Remove/Update Security Association	Not supported: support on the fly security associations by identifying the trust hierarchy and security service applied to the message in the body and content of the public key certificate.
Authentication	Authenticate ITS user/network	Signed messages.
Confidentiality	Encrypt/Decrypt message Send/Receive secured message using Security Association	Encrypted messages Not supported
Integrity	Insert/Validate check value	Signed messages.
Replay protection	Timestamp message Insert/Validate sequence number	Supported Not supported
Accountability Plausibility validation	Record incoming/outgoing message Validate data plausibility and dynamic Parameters	Not supported Basic support: rejected if geographic location far or expiry time too far in the past.
Remote management	Activate/Deactivate ITS transmission	Not supported
Report misbehaving	Report Misbehavior Report of ITS-S	Not supported

برای امضا گروهی، پیام sign برای نیمی از گروه استفاده می‌شود، هیچ هویت آشکاری از امضاء کننده قبل از ردیابی منافذ و اطمینان از حریم خصوصی [26] وجود ندارد. فقط مدیر گروه می‌تواند هویت کاربران را باز کند و از طریق یک تله او را ردیابی کند. در [12]، گروه‌های داخلی V2V از کلید مخفی برای احراز هویت اصول اولیه شان استفاده می‌کنند. گروه‌ها یا حلقه امضا موجب افزایش حریم خصوصی با صرفه‌جویی کارآمد ارتباطات می‌گردد. در [27]، یک طرح احراز هویت غیرتعاملی ارائه شده است که حریم خصوصی در میان رانندگان یک گروه را برای شبکه ارتباطات V2V فراهم می‌کند؛ رانندگان ممکن است مجموعه خود را از کلیدهای عمومی بدون کنترل (TTP) تغییر دهند.

همچنین می‌توانیم این حملات را با رمزنگاری داده کاهش دهیم. نویسندگان در [2] یک رمزنگاری نامتقارن از طریق NMD (روش عدم افشای) پروتکل مسیریابی پیشنهاد می‌دهند، [12] که برای رمزنگاری متقارن برای جلوگیری از ردیابی استفاده می‌شود. معماری امنیتی مورد استفاده در ارتباطات V2V و V2I در [14،15،23] و [32] موفق به محافظت از حریم خصوصی شرکت‌کنندگان از نظر قابلیت‌های محاسباتی و پهنای باند ارتباطی بسیار کارآمد با استفاده از رمزنگاری نامتقارن و متقارن و مداخله سخت‌افزار شده است.

برای افشای اطلاعات:

نویسندگان در [2] SMT (انتقال امن پیام) و پروتکل مسیریابی NMD را برای حل این مشکل از طریق رمزنگاری غیرمتقارن MAC پیشنهاد کرده‌اند.

برای حملات DOS:

می‌توان آن را با استفاده از امضای دیجیتال [24]، روش احراز هویت خاص [33]، پروتکل‌های مسیریابی [1] و قابل اعتماد بودن یک گره [34] کاهش یابد. امضای دیجیتال برای ارتباطات امن و قابل اعتماد پیام و احراز هویت [35] استفاده می‌شود. امضای دیجیتالی داده‌های امنیتی در [1] بیان شده است. [36] استفاده از زمان زندگی کوتاه برای کلید خصوصی و عمومی را با یک تابع هش نشان می‌دهند. برای احراز هویت، Tesla++ [33] یک روش احراز هویت

برای جایگزینی موثر امضا است. که از رمزنگاری متقارن با افشای با تاخیرکلید استفاده می‌کند. امن و جلوگیری از حمله داس حافظه است. این نیاز به حافظه در پایان گیرنده را برای احراز هویت مکانیک-anism کاهش می دهد. برای پروتکل مسیریابی، [2] اعمال SEAD (موقت امن و کارآمد بردار فاصله) و یا پروتکل مسیریابی ARIADNE که با استفاده از یکی از راه های تابع هش و رمزنگاری متقارن. نگرانی نشستند اعتماد از یک وسیله نقلیه، [34] پیشنهاد یک مدل اعتماد است که محاسبه اعتماد مقادیر متریک از گره های شرکت کننده در VANET. یکی از عوامل مهم آن شامل محدود کردن تعدادی از پیام های دریافتی پذیرفته از همسایگان. هنگامی که بیش از یک آستانه خاص (که در مورد حمله DOS)، با استفاده از روش فازی مبتنی بر، گزارش مستقیم به MA برای غیر فعال کردن مهاجم ارسال می شود.

برای حمله Sybil:

استقرار یک اعتبار سنجی سازمان مرکزی (VA)، که تایید EN-tities در زمان واقعی مستقیم یا غیر مستقیم با استفاده از گواهی موقت [37]. استفاده از PKI برای توزیع کلید و ابطال [38]. درخواست ثبت نام، ECDSA برای امضا و استفاده برچسب زمان در هر VE-hicle [8]. مرجع [39] استفاده proposesto صدور گواهینامه تایید شده است. در صورت لینک معتبر و امن با گره مورد اعتماد، [40] پیشنهاد اعتبار گره ناشناخته با استفاده از روش محل امن نسخه-ification. کد عکس. [9] suggeststhe تایید موقعیت با تجزیه و تحلیل آزمایش قدرت سیگنال و منابع رادیویی. مرجع [41] advocatesstrengthening مکانیزم احراز هویت توسط استفاده از پروتکل های محدوده مساعدی بر اساس تکنیک های رمز نگاری. در [9] (مقاوم Sybil در تشخیص حمله) RobSAD برای غیر طبیعی / عادی TRA-jectory، با نرخ تشخیص بالاتر و سیستم مورد نیاز پایین تر است. این می تواند حملات به طور مستقل با مقایسه دیجیتال سیگنال-tures برای مدار حرکت مشابه را تشخیص دهد. مرجع [42] پیشنهاد بسیاری از طرحواره حریم خصوصی حفظ با معماری VANET تولید گواهی / نام مستعار و نظارت بر وسایل نقلیه پس از آن گزارش به CA. مرجع [43] استفاده proposesto در هیئت مدیره رادار (چشم مجازی). خودرو می توانید ببینید

وسایل نقلیه اطراف و دریافت گزارش از GPS خود را هماهنگ. با مقایسه، آنها می توانند موقعیت واقعی و وسایل نقلیه مخرب تشخیص دهد. در [3]، محل سکونت استفاده می شود برای جلوگیری از حملات Sybil در با چک کردن محل منطقی آن است. یک وسیله نقلیه دریافت پیام، به بررسی گواهی، طول عمر و محل آن است. اگر آن را درست و در محل منطقی است، آن را می پذیرد پیام دیگری آن را به نزدیکترین CA. گزارش آنها همچنین TCRL (به موقع جغرافیایی CRL) که شامل CRLs لغو تازه از یک منطقه خاص استفاده کنید. در نهایت، [44] در مقایسه حملات Sybil در راه حل های مختلف.

برای نرم افزارهای مخرب و اسپم:

امضای دیجیتال از نرم افزار و سنسورهای ضروری است. با استفاده از سخت افزار مورد اعتماد را غیر ممکن به تغییر پروتکل ها و ارزش های موجود، به جز توسط گره مجاز [41].

برای حمله مرد میانی:

استفاده از روش های تأیید هویت قوی مانند گواهینامه های دیجیتال و ارتباط محرمانه با کلید و یا قدرتمند cryptogra-PHY [9]. شامل چندین طرح احراز هویت ذکر شده در [45] که در آن نامش فاش نشود، نام مستعار، اعتماد و حفظ حریم خصوصی از طریق کلید های کوتاه مدت بطور متناوب تغییر تضمین شده و RSU برای احراز هویت و توزیع کلید استفاده می شود. در [36]، یک طرح احراز هویت بسیار سبک وزن و غیر متمرکز برای V2V داده شده است برای محافظت از کاربران معتبر در VANETs با از حملات مخرب بر اساس مفهوم روابط اعتماد متعدی. مرجع [46] احراز هویت proposesan طریق MM (مدیر عضویت) می تواند تشخیص بی ادبی گره از طریق RSUs که وسایل نقلیه ردیابی. در [47]، کارآمد کاربران تعاونی مجوز احراز هویت پیام وسیله نقلیه به همکاری تصدیق یک دسته از جفت پیام امضاء بدون عامل قابل اعتماد با استفاده از کلید عمومی رمزنگاری (PKC) و رمزنگاری کلید مخفی (SKC).

برای حمله نیروی بی رحم:

استفاده از رمزگذاری قوی و الگوریتم تولید کلید از Unbreak قادر است در مدت زمان در حال اجرا منطقی [49]. سپس دسترسی های غیر مجاز ممنوع است.

5.2 حمله به سخت‌افزار و نرم‌افزار

برای پیام دستکاری:

الگوریتم استفاده شباهت [50]، ارتباط داده ها [26] و چال-lenge روش احراز هویت پاسخ [33] برای اثبات قابلیت اطمینان از پیام. مرجع [50] اعتماد proposesa و شهرت انسان agement چارچوب بر اساس الگوریتم شباهت و اعتماد از محتوای پیام ها بین وسایل نقلیه برای کمک به راننده به باور کنید یا نه یک پیام دریافت کرده است. با محاسبه مقدار اعتماد اگر از آن فراتر از آستانه آنها اقدام مناسب و برنامه تکراری پخش کردن MES-مریم گلی. در غیر این صورت آنها آن را رها کنید.

در [26]، یک امضا گروه رمان بر اساس یک چارچوب امنیتی اطمینان از صحت، یکپارچگی، گمنامی، مسئولیت پذیری، رویکرد کنترل دسترسی و احتمالاتی طرح تایید امضا مورد استفاده برای شناسایی پیام های دستکاری برای گره های غیر مجاز. بر اساس دستگاه مقاومت رشوه دادن، آن ارتباط داده ها از وسایل نقلیه و آن را متقابل تایید از طریق مجموعه ای از قوانین. چک، توانایی ها، نسل امضا، فایروال، تایید امضا، چک مجوز، چک ناهنجاری: لایه های امنیتی از این چارچوب از تشکیل شده است.

در [33] یک روش احراز هویت چالش و پاسخ طرفدار مطرح است؛ ترکیبی از امضای دیجیتال و احراز هویت پاسخ به چالش. آن استفاده می شود برای به حداقل رساندن پیام نادرست است. گیرنده گرفتن هر پیام یک چالش به فرستنده ارسال می کند. با پاسخ، آن را انتقال مکان و زمان آن برای اثبات صحت آن است. محل سکونت می توانید به ما بگویید اگر وسیله نقلیه در مجاورت یک حادثه، که قابلیت اطمینان از پیام ایمنی را افزایش می دهد بود.

برای حقه بازی و جعل حملات:

استفاده از PKI فضایی (VPKI) برای احراز هویت بین وسایل نقلیه [51]، و یا ثبت نام پیام های هشدار دهنده [52]، و یا ایجاد گروه COMMUNI-کاتیونهای [54]، و یا شامل یک کنترلی غیر رمزنگاری هر پیام ارسال کنید و درخواست چک معقول در یک ورودی [25]. یا حتی استفاده از گواهی رمزنگاری از طریق پروتکل مسیریابی آران (Authen-ticated مسیریابی برای آگهی تک کاره شبکه) [1] و یا استفاده از هیئت مدیره در رادار (چشم مجازی) [43]، و سپس خودرو می توانید موقعیت واقعی و وسایل نقلیه مخرب تشخیص دهد.

برای VPKI، آن مجموعه ای از اشخاص ثالث مورد اعتماد، یکی CA در هر کشور، با CA واگذارشده در مناطق است، CA های متقابل تشخیص VE-hicles در مناطق مختلف. هر خودرو دارای کلید خصوصی و عمومی خود و طول عمر کوتاه از گواهی با کلید های ناشناس با توجه به سرعت راننده [51] حال تغییر است. فقط مراجع قانونی می تواند در میان الکترونیکی پلاک یک وسیله نقلیه و نام مستعار آن ارتباط دارد. بنابراین یک پیام امضا منتشر با گواهی در-tached از طریق CA. تصدیق بنابراین ارتباط بین کاربران تصدیق تنها به شیوه ای امن است.

استفاده از ECDSA های امضای دیجیتال [47]، آن را فراهم انتشار سریع و مطمئن از اطلاعات؛ پس از اعتبار کلید عمومی پس از آن authen-ticating کلید خصوصی یک کاربر امضای یک پیام است.

برای ارتباط گروه [54]، کلید را می توان با یک سیستم گروه مدیریت کلید اداره می شود. دریافت خواهید کرد امنیت نمی تواند قادر به برقراری ارتباط با این گروه است. رانندگان به دو گروه با کلید عمومی مشترک بین اعضای [55]، در مورد یک رفتار MA-licious در، هویت امضاء کننده می تواند تنها با تحریک طالبان پاکستان نشان داد سازمان یافته است. در [35]، آنها با استفاده SECA (امنیت تجزیه و تحلیل مهندسی خوشه) برای تامین امنیت این گروه است. برای امنیت چراغ، آنها با استفاده از گواهی و امضای دیجیتال در حالی که برای امنیت چند هاپ، موقعیت جغرافیایی استفاده شده است.

برای پیام اشباع:

کد عکس. [25] proposesto محدود کردن ترافیک پیام به V2I / I2V، IM-plement ثبت نام ایستگاه بنابراین وسایل نقلیه تنها ثبت شده و پردازش از زیرساخت های آن در محدوده های رادیویی خود را دریافت کرد، کاهش فرکانس از beaconing و اضافه کردن منبع iDEN را-تقدیس (معادل به آدرس IP) در پیام های V2V. در حالی که نویسندگان در [23،56] تلاش برای محدود کردن جاری شدن سیل از پیام امضا کرد، ساخته شده بر روی گروه بندی مبتنی بر مکان و امضای تجمع.

Table5Attacks، خدمات و راه حل های به خطر بیافتد.

حملات

برای حمله پخش:

استفاده از زمان مهر زنی روش برای بسته حساس [43] و یا برچسب زمان تمام پیام ها با زمان پخش (UTC یا GNSS)، و یا امضای دیجیتالی و شامل شماره توالی در هر پیام [25]. علاوه بر گواهی رمزنگاری یا رمزنگاری متقارن و مک از طریق آران و ARIADNE مسیریابی پروتکل [2].

برای گره جعل هویت:

استفاده از متغیرهای MAC و آدرس های IP برای V2V و V2I COMMUNI-کاتیونهای [39]. یا تصدیق از طریق گواهینامه های دیجیتال [37]. مرجع [41] proposesto تقویت مکانیزم احراز هویت با استفاده از فاصله پروتکل محدوده بر اساس تکنیک های رمز نگاری. و یا استفاده از گواهی رمزنگاری از طریق پروتکل مسیریابی آران به عنوان مردان، شک و تردید کرد در [2].

برای بیش از تغییر ظاهر:

[25] پیشنهاد می هویت معتبر در هر MES-مریم گلی و تصدیق آن، و یا به عنوان در [47] پیشنهاد، استفاده از امضای دیجیتال و شماره ترتیب.

برای مقاومت در برابر Routingattacks (Blackhole و Greyhole، چرخ دنده، سوراخ و تونل زنی):

امضای دیجیتال از نرم افزار و سنسور استفاده می شود. در آران و، Ariadne و SEAD پروتکل مسیریابی [2] گواهی رمزنگاری، رمزنگاری متقارن، MAC (پیام تایید کد) و تابع هش یکی از راه های به ترتیب مورد استفاده برای حل این مسائل است. در [9]، پشته یک روش کارآمد ارائه شده است برای دفاع در برابر حمله کرمچاله در شبکه است. این است که در پروتکل AODV است. از آن استفاده کنید دسته سه تایی جغرافیایی به منظور محدود کردن مسافت طی شده از منبع به مقصد، اگر در آستانه پیشی گرفته است و سپس بسته حذف شده است. آنها همچنین (از طریق مسنجر با کلید DIS-بسته شدن TESLA) پروتکل احراز هویت پیشنهاد TIK. [48] ارائه مکانیزم های مختلف برای بهبود پروتکل های مسیریابی موقت مختلف برای فرآیند مسیریابی امن با افزایش اعتماد در میان گره های مختلف در VANETs با.

برای زمان بندی حمله:

زمان ساز ماشین پرس برای بسته از برنامه های کاربردی حساس به تاخیر در یک پلت فرم قابل اعتماد با قوی رمزنگاری وزارت دفاع، ules استفاده [9،24،36].

5.3 حمله به ورودی سنسور در خودرو

برای متراکم حمله:

نویسندگان در [57] پیشنهاد برای تغییر انتقال چان-NEL و یا استفاده از روش فرکانس رقص است. در حالی که [35] پیشنهاد برای تغییر یا بین فن آوری های مختلف بی سیم.

برای GPS حقه بازی و یا تقلید می کنی مکان یا حمله توهم:

استفاده از امضا با سیستم موقعیت یابی به پذیرش تنها داده های مکان معتبر [58]. و یا اجرای نظارت دیفرانسیل به تغییرات غیر معمول iDEN را-tify در موقعیت [25]. و یا محاسبه نمره شهرت برای برنامه امنیت [35] با تجزیه و تحلیل و فیلتر نمایش داده شد به تشخیص موقعیت های مخرب و نادرست را دریافت کرد. از این رو دشمنان بالقوه شناسایی و خارج شده از VANET.

5.4 حمله به زیرساخت

کلید و / یا گواهی replicationthat باعث غیر مجاز AC-مالیات:

استفاده از کلید های گواهی و یکبار مصرف، و یا بررسی اعتبار گواهینامه های دیجیتال در زمان واقعی از طریق CRL [24]، و یا استفاده از پروتکل های ابطال جای CRL [3]. با استفاده از گواهینامه بین CA های مختلف درگیر در طرح امنیتی VANETs با [39]. یا اتخاذ یک CA های توزیع سلسله مراتبی با اعتماد رفتن را از طریق یک زنجیره طولانی [30].

A "طراوت" مفهوم در [38] زمان تایید ثابت مستقل از تعداد گواهی لغو، نتیجه بدون نیاز به PKI برای توزیع CRL و OBUs آنها را حفظ می کند. این مسئله موجب کاهش نیاز ذخیره سازی در OBUs.

مرجع [33] proposesto لغو گواهی یا زمانی که کلید cryp-tographic به خطر بیافتد یا زمانی که یک مسائل کاربران جعلی گواهی امضا برای انتقال اطلاعات جعلی. صدور گواهینامه شامل یک کلید عمومی، طول عمر گواهی، امضای CA و CRL اضافه خواهد شد.

برخی از پروتکل ابطال مناسب در آنها اشاره شده [3]: RTPD (لغو رشوه دادن دستگاه اثبات)، اگر در هر وسیله نقلیه فعال آن را ممنوع از ارسال پیام، و DRP (توزیع پروتکل لغو) که اجازه می دهد تا وسایل نقلیه برای برقراری ارتباط و متهم کردن دیگران که بی ادبی و وقتی گزارش ممکن است به CA. سپس TPD خود دیگر قادر به امضا پیام.

برای از دست دادن قابلیت ردیابی رویداد (انکار):

نویسندگان در [41] توصیه با استفاده از سخت افزار قابل اعتماد برای آن غیر ممکن است برای تغییر پروتکل های موجود و وال-ارزشهای جز با آنهایی که مجاز است. همانطور که در [33]، خواندن و به روز رسانی

از سنسورهای باید تصدیق و تأیید شده باشند به عنوان مثال، توسط یک مکانیسم چال-lenge / پاسخ. در حالی که [9] پیشنهاد PVN (موجه اعتبار سنجی شبکه) برای جمع آوری داده های خام از حسگرها و آنتن برای بررسی اگر قابل قبول است یا نه.

در نهایت، ETSI در [13] پیشنهاد برای حملات متقابل به استفاده از گزارش بازرسی، فعال و غیر فعال کردن از راه دور از گره.

در Table5، ما در حال حاضر حملات قبلا توضیح، خدمات به خطر بیافتد مربوط به آنها و راه حل پیشنهادی خود را.

6. تجزیه‌وتحلیل شکاف بین راه‌حل‌های مختلف

هنگام انجام یک تجزیه و تحلیل شکاف در VANET، هدف این است که IDEN-tify شکاف گم شده / نیازهای لازم در رابطه با آنچه نتایج مورد نظر است. باید مقایسه آنچه در منطقه انجام شده است، و مقایسه این به جاه طلبی های آنچه به هدف برای. احتمالا وجود یک شکاف در بین، که در آن صورت باید مشخص-حایز خواهد بود. هنگامی که این فرایند شناسایی کامل شده است تجزیه و تحلیل این امید-به طور کامل یک راه حل چگونه برای پر کردن شکاف پیشنهاد می کند.

محققان در VANET سعی برای دور زدن مقیاس پذیری پروب مشکلات است و صرفه جویی در ارتباطات در شیوه ای کارآمد ترین. آنها رسیدن به کاهش تاخیر در انتشار. آنها در احراز هویت، تحویل داده کار کرده و سعی کنید به پیشنهاد چگونه به اعتماد پیام بین وسایل نقلیه. آنها سعی برای پیدا کردن تعادل بین نیاز به حفظ حریم خصوصی کاربر و قابلیت ردیابی نیاز به-درمان برای مقامات اجرای قانون است. آنها رمزنگاری AP-رویکردهای مبتنی بر PKI برای توزیع

کلید متقارن و نامتقارن برای رمزگذاری پیام، و گواهی برای احراز هویت استفاده می شود. آنها تشکیل گروه بر اساس طرح های رمزنگاری متقارن و نامتقارن گرافیک اعتماد به منظور سرعت پردازش و تقویت امنیت و حفظ حریم خصوصی. آنها داده ها برای جلوگیری آهنگ نشستند رمز در آوردن. آنها با استفاده از امضای دیجیتال و مدل اعتماد در گیرنده از، برای جلوگیری از داس. آنها اطلاعات در زمان واقعی، با قدرت analyzingsignal یا خرید چشم مجازی برای تشخیص حمله Sybil اعتبار. آنها با استفاده از امضای دیجیتال و یا رابطه متعدی برای نرم افزارهای مخرب و تشخیص هرزه نگاره، وارد. آنها نشان می دهد رمزنگاری قوی و کلید الگوریتم نسل-eration نشکن در مدت زمان معقول در حال اجرا برای مقاومت در برابر به حمله نیروی بی رحم. آنها پیشنهاد الگوریتم شباهت برای بررسی و تشخیص دستکاری با محاسبه مقدار اعتماد بیش از یک آستانه خاص. آنها برگزیدن ارتباطات گروه به منظور محدود کردن unauthorizedaccess. آنها فرکانس ارسال به محدود اشباع پیام را کاهش دهد. آنها با استفاده از پروتکل مسیریابی ویژه و امضای دیجیتال برای جلوگیری از حمله پخش. آنها نشان می دهد سوئیچینگ بین فن آوری های مختلف بی سیم برای جلوگیری از متراکم کانال. آنها با استفاده از کلیدهای تأیید و یکبار مصرف، و بررسی VA-lidity از گواهینامه های دیجیتال در زمان واقعی از طریق CRL، و یا استفاده به جای پروتکل ابطال آن را. برای دسترسی غیر مجاز، آنها ابطال هنگامی که کلید رمزنگاری به خطر میافتند. آنها با استفاده از گزارش به قدرت خاص و فعال سازی از راه دور و DEAC-tivation گره. پیشنهاد آنها برای حملات متقابل به استفاده از ورود به سیستم حسابرسی.

به طور خلاصه، بسیاری از آنها در مورد استفاده از PKI، امضای دیجیتال و گواهی با تکنیک های رمزنگاری و گروه موقتی روش برای حفظ مسائل امنیتی اساسی در VANET به توافق رسیدند. اما هر یک از راه حل پیشنهادی یک میدان گسترده به اکتشاف است و کار در آینده مورد نیاز است برای آزمایش و اثبات بهترین است که می تواند مناسب است.

Table6below نشان می دهد مقایسه بین راه حل بر اساس معیارهای از پیش تعریف شده که مقابله عمیقا امنیت VANET مانند Centralizedor غیر متمرکز، حریم خصوصی حفظ شود یا نه، گواهی-تکثیر خودگردان / RSU استفاده شده است یا نه، پشتیبانی از پروتکل مسیریابی، پشتیبانی از الگوریتم رمزنگاری، پشتیبانی تشکیل گروه،

گزارش به مقام خاص، فعال سازی از راه دور و یا غیر فعال کردن، تأیید اطلاعات، نرخ کشف. این مقایسه بین برخی از راه حل های انتخاب شده و حملات خود را است. این حملات و خود SOLU-سیاسی در بخش 5. یکی گسترش می توانید از این جدول به نفع برای پیدا کردن یک راه حل به خطر بیافتد در این میان خدمات مختلف. پس از ارائه و تجزیه و تحلیل راه حل های مختلف در امنیت VANET، بسیاری از مسائل در حال ظهور و باز بلند می شوند. ما آنها را در بخش بعدی را گسترش خواهد داد.

7. مسائل باز و در حال ظهور

براساس روش‌های امنیتی ارائه شده در بخش 5، محققان در VANET سعی در دور زدن بسیاری از محدودیت‌ها یا حملات به شبکه وسایل نقلیه را دارند. اگرچه، بسیاری از مسائل هنوز باز هستند. در زیر برخی از این روش‌ها برجسته شده است که ممکن است به حوزه‌های تحقیقاتی جدید در آینده تبدیل شود:

1) ارزیابی اعتماد گره‌های شرکت‌کننده در VANET و تشخیص سوء رفتار آنها:

- ارزیابی اعتماد یک وسیله نقلیه در VANET یک مسئله باز است. در بالا بیان کردیم که هرگونه خرابی در ارتباطات و/ یا پیام‌ها زندگی مردم را در معرض خطر قرار می‌دهد. پس چه معیارهایی باید تعریف شود که یک گره قابل اعتماد است یا نه؟ آیا برای انتشار پیام‌های حیاتی قابل اعتماد است؟

- براساس این معیارها می‌توانیم سوء رفتار در وسیله نقلیه را تشخیص دهیم. هنگامی که سوء رفتار شناسایی می‌شود، چه اقداماتی مناسب است؟ عوامل مجازات به‌وضوح تعریف نشده است. هر دو عامل می‌تواند انگیزه‌ای برای محدود کردن گره‌های مخرب ایجاد کند.

2) فرایند ابطال و گواهی لیست ابطال مدیریت-درمان و توزیع: پس از آن که سوء رفتار است شناسایی شده است چگونه خواهد بود روند ابطال آن را؟ راه حل های مبتنی CRL-هنوز توسعه سازمان ملل متحد-DER. با استفاده از گواهینامه های عمر کوتاه در CRL و گواهی تغییر استراتژی تحت هیچ زیرساخت برای CRL تعریف نشده است و هنوز هم آسیب پذیری. گواهی نسخه-ification و ابطال دیگر در صورت زنجیره گواهی بنابراین جایگزین چه می باشد؟

3) توانایی شبکه به خود سازماندهی از طریق یک محیط شبکه تلفن همراه بالا: تشکیل گروه یک روند است، اما چگونه به ارائه در سراسر پارتیشن در VANET هنوز هم به خوبی تعریف نکرده است. در شکل گیری این گروه، رهبر گروه سرور مرکز برای تمام گره پیوستن به این گروه است. مدیریت کلید و پایه COM-ارتباطی از طریق او منتقل می کند. چه اتفاقی می افتد اگر این GL تصمیم می گیرد این گروه را ترک کنند؟ باید یک رهبر گروه پشتیبان گیری؟ چه در مورد مدیریت کلید زمانی که GL گروه را ترک می؟ آن را به خوبی روشن نیست. چه اتفاقی می افتد اگر GL گروه یا یک کاهش ارتباط رادیویی برگ؟ آیا راه حل با تلاش برای ادغام فن آوری های مختلف بی سیم در VANET و سوئیچ بین آنها در صورت هر گونه بروز مشکل؟

4) اعتماد زمینه داده و تایید: VANET هدف، تا مطمئن شویم درایو امن و تعاونی. این اتفاق می افتد با ارائه اطلاعات متناسب خوردند به راننده و یا وسیله نقلیه. بنابراین بسیار مهم است که برای بررسی و تأیید اطلاعات رد و بدل در VANET. برای اعتماد داده محور و تایید، رشوه دادن مقاومت سخت افزار مورد استفاده در یک وسیله نقلیه برای تشخیص غیر ضروری تصادف هشدار می دهند، و گردهمایی ها، باید با تحقیق بیشتر. برای زمینه verifica روش، یک وسیله نقلیه باید قادر به عنوان یک سیستم تشخیص نفوذ عمل با مقایسه اطلاعات دریافت شده در مورد وضعیت و محیط زیست با اطلاعات در دسترس خود را داشته باشد. علاوه بر این، مفهوم امنیت واکنش نیاز به افزایش یافته است.

5) رمزنگاری روش برای امنیت، حریم خصوصی و تضمین غیر قابلیت ردیابی: با توزیع کلید شروع، آن منحصر به فرد است به آنها، تولید کننده خودرو یا دولت؟ برای اندازه کلید، یک پیشنهاد اندازه کلید، تاخیر authentica روش و پروتکل های خاص وجود ندارد. چگونه به مقابله با کلید از مدت زمان کوتاه. چگونه به حذف کلید؟ ممکن است سربار شود. روش تعویض گواهینامه های دوره ای برای حفظ حریم خصوصی آشور-ance تعریف نشده است. همچنین برای غیر قابلیت ردیابی و حفظ حریم خصوصی، روش کارآمد تر برای توزیع مستعار جزئی و پروانه کلید ها و مقادیر ارتباط هنوز استخدام نشده. در آگهی-ضد تروجان و تشخیص نفو . به‌علاوه، استفاده از IP تلفن همراه و یا تغییر آی پی و یا آدرس MAC توسط وسایل نقلیه برای جلوگیری از ردیابی، هنوز هم تحت مطالعه است.

جدول 6. خلاصه‌ای از برخی راه‌حل‌ها برای حملات مختلف

جدول 6. (ادامه)

جدول 7. مسائل باز در VANET، حالات ارتباطات و طبقه‌بندی‌های مربوطه

Open issue	Communication mode	Corresponding categories
Trustworthiness evaluation of nodes and misbehavior detection	V2V, V2I	Wi-H&S-Si-I
Revocation process and certificate revocation list management and distribution	V2V, V2I	Wi-H&S-I
Ability of the network to self-organize via a high mobile network environment:	V2V	H&S-I
Data context trust and verification	V2V, V2I	Wi-H&S-Si
Cryptographic approaches for security, privacy and non-traceability assurance	V2I	H&S-I
Anti-malware and Intrusion Detection System	V2I	Wi-H&S-I

6) سیستم تشخیص نفوذ و نرم‌افزارهای ضد مخرب: چارچوب‌های ضدتروجان جاسازی شده هنوز هم جزء مسائل مشکل‌ساز در VANETs هستند. بنابراین باید یک مکانیزم تشخیص نفوذ برای افزایش امنیت شبکه توسعه یابد.

در جدول 7، مسائل باز ذکر شده در بالا را براساس حالت‌های ارتباطی آنها (V2V، V2I یا هر دو) و مقوله‌های نگرانی هریک را طبقه‌بندی می‌کنیم: (1) رابط بی‌سیم (Wi)، (2) سخت‌افزار و نرم‌افزار (H & S)، (3) سنسور ورودی در خودرو (Si)، (4) زیرساخت (I) (CA یا کارخانه سازنده خودرو).

همه این مسائل از یک طرف، برای یافتن یک تجارت بین امنیت و بهره وری، و از طرف دیگر به گمنامی/ اعتماد /حریم خصوصی مربوط هستند. در حفظ حریم خصوصی، کاربران مجاز به انتخاب سطح حریم خصوصی خود براساس محاسبه اعتماد خود بر روی دیگران هستند.

8. نتیجه‌گیری

کاربران ایمنی و امنیت بیشتری را در جاده‌ها می‌خواهند چرا که زندگی بسیاری از مردم در جاده‌ها با توجه به بدرفتاری و بی تجربگی دیگران به پایان می‌رسد. غلبه بر این مشکلات نیاز به تلاش بیشتر در آینده برای رسیدن به یک محیط

VANET امن دارد. در این مقاله یک مرور گسترده از بسیاری از چالش‌های امنیتی VANET و علل آنها و همچنین راه‌حل‌های موجود به شیوه‌ای جامع ارائه شده است. ما جزئیات معماری امنیتی اخیر و استانداردهای امنیتی شناخته شده و پروتکل‌ها را بیان می‌کنیم. ما به طبقه‌بندی حملات مختلف شناخته شده در کارهای گذشته و راه‌حل‌های آنها تمرکز می‌کنیم. در نهایت، چالش‌های خاص پژوهش و سؤالات باز که ممکن است آینده تحقیقات را تغییر دهد مشخص می‌کنیم. بنابراین VANET قادر به پیاده‌سازی یک سیستم موثر برای وسایل نقلیه قابل اعتماد از گره‌های مخرب است.

References

[1] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions, IEEE Commun. Surv. Tutor. 13 (4) (July 2011) 584–616.

[2] R.S. Raw, M. Kumar, N. Singh, Security challenges, issues and their solutions for VANET, Int. J. Netw. Secur. Appl. 5 (5) (September 2013).

[3] Gh. Samara, W.A.H. Al-Salihy, R. Sures, Security analysis of vehicular ad hoc networks (VANET), in: Second International Conference on Network Applications Protocols and Services (NETAPPS), IEEE, 2010, pp. 55–60.

[4] M.N. Mejri, J. Ben-Othman, M. Hamdi, Survey on VANET security challenges and possible cryptographic solutions, Veh. Commun. 1 (2014) 53–66, contents available at ScienceDirect, www.elsevier.com/locate/vehcom.

[5] N.K. Chauley, Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study, Int. J. Netw. Secur. Appl. 10 (5) (2016) 261–274.

[6] B. Mokhtar, M. Azab, Survey on security issues in vehicular ad hoc networks, Alex. Eng. J. 54 (2015) 115–1126, available at www.elsevier.com/locate/aej.

[7] K. Lim, D. Manivannan, An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks, Veh. Commun. 4 (2016) 30–37.

[8] R. van der Heijden, Security architectures in V2V and V2I communication, in: 13th Twenty Student Conference on IT June 21st, Enschede, The Netherlands, 2010.

[9] V. La Hoa, A. Cavalli, Security attacks and solutions in vehicular ad hoc networks: a survey, Int. J. Netw. Syst. 4 (2) (April 2014).

[10] A.Y. Dak, S. Yahya, M. Kassim, A literature survey on security challenges in VANETs, Int. J. Comput. Theory Eng. 4 (6) (December 2012).

[11] R.K. Sakib, Security issues in vanet, in: Department of Electronics and Communication Engineering, BRAC University, Dhaka, Bangladesh, 2010.

[12] W. Whyte, A. Weimerskirch, V. Kumar, T. Hehn, A security credential management system for V2V communications, in: IEEE Vehicular Networking Conference, 2013.

[13] ETSI TS 102 731 V1.1.1-ITS-Security services and architectures.

[14] K. Plößl, H. Federrath, A privacy aware and efficient security infrastructure for vehicular ad hoc networks, Comput. Stand. Interfaces 30 (6) (2008) 390–397.

[15] M. Abuelela, S. Olariu, Kh. Ibrahim, A secure and privacy aware data dissemination for the notification of traffic incidents, in: Proceedings of the IEEE Vehicular Technology Conference, Spring, Barcelona, April 2009.

[16] H. Hasrouny, C. Bassil, A.E. Samhat, A. Laouiti, Group-based authentication in V2V communications, in: DICTAP, Fifth International Conference, IEEE, 2015, pp. 173–177.

[17] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments: IEEE Std 1609.2™-2012.

[18] ETSI TS 102 940 V1.1.1-ITS – Communications security architecture and security management.

[19] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-transport/projects-by-country/multi-country/2014-eu-ta-0669-s.

[20] https://www.sbdautomotive.com/en/intelligence-news.

[21] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments: IEEE Std 1609.2™-2006.

[22] ETSI TS 102 867 V1.1.1- Security-Mapping for IEEE 1609.2.

[23] M. Raya, A. Aziz, J.P. Hubaux, Efficient secure aggregation in VANETs, in: Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks, VANET '06, 2006, pp. 67–75.

[24] M. Raya, J.P. Hubaux, The security of vehicular ad hoc networks, in: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN'05, November 7, Alexandria, Virginia, USA, 2005, pp. 11–21.

[25] ETSI TR 102 893 V1.1.1- ITS- Security- Threat, Vulnerability and Risk Analysis.

[26] J. Guo, J.P. Baugh, Sh. Wang, A group signature based secure and privacy-preserving vehicular communication framework, in: CD-ROM Proceedings of the Mobile Networking for Vehicular Environments (MOVE) Workshop in Conjunction with IEEE INFOCOM, Alaska, May 2007.

[27] F.M. Salem, M.H. Ibrahim, I. Ibrahim, Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks, in: Sixth International Conference on Networking and Services, 2010.

[28] ETSI TS 102 941 V1.1.1- ITS, Security- Trust and Privacy Management.

[29] R.G. Engoulou, M. Bellaïche, S. Pierre, A. Quintero, VANET security surveys, Comput. Commun. 44 (2014) 1–13, journal homepage: www.elsevier.com/locate/comcom.

[30] B. Aslam, C.C. Zou, Distributed certificate architecture for VANETs, in: Military Communications Conference, IEEE, 2009, pp. 1–7.

[31] A. Rawat, S. Sharma, R. Sushil, VANET: security attacks and its possible solutions, J. Inf. Oper. Manag. 3 (1) (2012) 301–304.

[32] G. Calandriello, P. Papadimitratos, J.P. Hubaux, A. Lioy, Efficient and robust pseudonymous authentication in VANET, in: Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks, VANET '07, 2007, pp. 19–28.

[33] A. Dahiya, V. Sharma, A Survey on Securing User Authentication in Vehicular Ad Hoc Networks, 2009.

[34] H. Hasrouny, C. Bassil, A. Samhat, A. Laouiti, Security risk analysis of a trust model for secure group leader-based communication in VANET, in: Second International Workshop on Vehicular Adhoc Networks for Smart Cities, IWVSC', 2016.

[35] R. Engoulou, Securisation des vanets par reputation des nœuds, Thesis Report, Ecole Polytechnique de Montreal, 2013.

[36] M.Ch. Chuang, J.F. Lee, TEAM: trust-extended authentication mechanism for vehicular ad hoc networks, IEEE Syst. J. 8 (3) (2013).

[37] M.S. Al-kahtani, Survey on security attacks in vehicular ad hoc networks (VANETs), in: 6th International Conference on Signal Processing and Communication Systems (ICSPCS), IEEE, 2012, pp. 1–9.

[38] A. Rao, A. Sangwan, A.A. Kherani, A. Varghese, B. Bellur, R. Shorey, Secure V2V communication with certificate revocations, in: IEEE Mobile Networking for Vehicular Environments, 2007.
[39] M. Raya, P. Papadimitratos, J.P. Hubaux, Securing vehicular communications, IEEE Wirel. Commun. 13 (5) (2006) 8–15.
[40] B. Xiao, B. Yu, C. Gao, Detection and localization of sybil nodes in VANETs, in: Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, ACM, 2006, pp. 1–8.
[41] D. Singelee, B. Preneel, Location verification using secure distance bounding protocols, in: IEEE International Conference on Mobile Adhoc and Sensor Systems, 2005, p. 7.
[42] T. Zhou, R.R. Choudhury, P. Ning, K. Chakrabarty, P2DAP – sybil attacks detection in vehicular ad hoc networks, IEEE J. Sel. Areas Commun. 29 (3) (March 2011).
[43] G. Yan, S. Olaruis, M. Weigle, Use of infrastructure in VANETs, Comput. Commun. 12 (2008) 2883–2897.
[44] D. Kushwaha, P.K. Shukla, R. Baraskar, A survey on sybil attack in vehicular ad-hoc network, Int. J. Comput. Appl. 98 (15) (July 2014).
[45] L. Song, Q. Han, J. Liu, Investigate key management and authentication models in VANETs, in: IEEE International Conference on Electronics, Communications and Control (ICECC), 2011.
[46] Ch.D. Jung, Ch. Sur, Y. Park, K.H. Rhee, A robust conditional privacy-preserving authentication protocol in VANET, in: First International ICST Conference, MobiSec, Italy, June 2009, pp. 35–45.
[47] R. Raiya, Sh. Gandhi, Survey of various security techniques in VANET, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 4 (6) (June 2014).
[48] N. Patel, R.H. Jhaveri, Trust Based Approaches for Secure Routing in VANET: A Survey, Elsevier, 2015, available online at www.sciencedirect.com, ICACTA.
[49] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (VANETs): status, results, and challenges, Telecommun. Syst. 50 (4) (2012) 217–241.
[50] P. Caballero-Gil, Security issues in VANET, available http://cdn.intechopen.com/pdfs-wm/12879.pdf, 2011.
[51] R. Rajadurai, N. Jayalakshmi, Vehicular network: properties, structure, challenges, attacks, solution for improving scalability and security, Int. J. Adv. Res. 1 (3) (March 2013), IJOAR.org.
[52] J. Blum, A. Eskandarian, The threat of intelligent collisions, IT Prof. 6 (1) (2004) 24–29.
[53] S.S. Kaushik, Review of different approaches for privacy scheme in VANETs, Int. J. Adv. Eng. Technol. (ISSN 2231-1963) 5 (2) (2012).
[54] V. Vèque, C. Johnen, Hiérarchisation dans les réseaux ad hoc de véhicules, in: UBIMOB, Bayonne, France. CEPADUES, 2012, pp. 45–52.
[55] P. Fan, J.G. Haran, J. Dillenburg, P.C. Nelson, Cluster-based framework in vehicular ad-hoc networks, in: 4th International Conference, ADHOC-NOW, Proceedings, 2005, pp. 32–42.
[56] A.M. Malla, R.K. Sahu, A review on vehicle to vehicle communication protocols in VANETs, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 3 (2) (February 2013).
[57] A.M. Malla, R.K. Sahu, Security attacks with an effective solution for Dos attacks in VANET, Int. J. Comput. Appl. (ISSN 0975-8887) 66 (22) (2013).
[58] L. He, W.T. Zhu Mitigating, Dos attacks against signature-based authentication in VANETs, IEEE Int. Conf. Comput. Sci. Automat. Eng. (CSAE) 3 (2012) 261–265.