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

شبکه‌های بین خودروئی و چالش های امنیتی در آن

زهره باطنی [۱]، بهاره هادیگل [۲]

[۱] استادیار گروه کامپیوتر، دانشگاه آزاد اسلامی، واحد تهران مرکزی
zbateni@hotmail.com

[۲] دانشجوی کارشناسی ارشد گروه کامپیوتر ، دانشگاه آزاد اسلامی، واحد تهران مرکزی
b.hadigol@yahoo.com

چکیده

شبکه ارتباطات بین خودروئی (VANET) شبکه ای با توپولوژی پویا و با زیرساخت رسانه بی‌سیم محسوب می‌شود. علاوه بر ارتباطات بین خودروئی د ستر سی برنامه‌های ایمنی و سرگرمی مانند اطلاع از شرایط جاده، وضعیت ترافیک، گزارش تصادفات و ... نیز در این شبکه‌ها فراهم شده و این تنوع باعث فراگیری بیشتر شبکه‌های ارتباطات بین خودروئی شده است. از آنجا که امنیت این شبکه ها با زندگی روزمره و حتی زندگی انسان ها درگیر است، پس یکی از مطالعات مهم در زمینه گسترش سیستم های انتقال هوشمند (ITS) بررسی امنیت این شبکه ها ست. باتوجه به ویژگی های این شبکه مانند محدودیت پهنای باند، تبادل دائمی اطلاعات، لزوم پا سخد هی به موقع و سایر موارد بایستی معماری های امنیتی خا صی برای آن درنظر گرفته شود. در این متن به معرفی الزامات امنیتی این شبکه ها و حملات شاخص در حوزه های مختلف پرداخته شده است. در آن چند مکانیسم امنیتی و چالش های مطرح آن بررسی شده اند..

کلمات کلیدی: شبکه ارتباطات خودروئی، مهاجم، امنیت، محرمانگی، یکپارچگی، حریم خصوصی

۱. مقدمه

شبکه ارتباطات بین خودروئی یکی از اجزای ا صلی سی ستم‌های انتقال هو شمند به شمار می‌آید. در شبکه ارتباطات بین خودروئی وسایل نقلیه بی‌سیم در حین عبور و مرور باهم تشکیل یک شبکه می‌دهند. امکان استفاده از رسانه بی‌سیم به‌صورت مستقیم بین دو وسیله نقلیه، برقراری شبکه را بدون زیرساخت‌های مخابراتی ممکن می‌کند. در این شبکه‌ها برقراری اتصال بین گره ها هنگام حرکت و طبعاً پیاده سازی سی ستم‌های انتقال هو شمند هدف ا صلی ا ست. بی شتر تحقیقات و مطالعات جهت پیاده‌سازی معماری امنیتی در راستای محافظت از شبکه در مقابل مهاجمان و حملات آن‌هاست. دغدغه این شبکه انتقال اطلاعات به مقصد به‌صورت صحیح و بدون ایجاد تأثیر در اطلاعات می‌باشد.

شبکه‌های ارتباطات بین خودروئی زیرمجموعه‌ای از شبکه‌های موردی بی سیم(WANET) ها و گسترش‌یافته شبکه‌های مبتنی بر حرکت (MANET) هستند. در شبکه ارتباطات بین خودروئی گرهها به‌صورت نقطه‌به‌نقطه و مستقل از زیرساخت یا مدیریت مرکزی عمل می کنند. برای ایجاد ارتباط، گره های میانی می توانند اطلاعات را با عبور از چند هاب به گره مقصد برسانند. درواقع هر گره به‌عنوان یک مسیریاب میانی عمل کرده و داده مستقلی تولید می‌کند[۱] .

امنیت در شبکه ارتباطات بین خودروئی (VANET) به عنوان یک سیستم هوشمند نقل و انتقال از اهمیت بالایی برخوردار است. ولی زیر ساخت شبکه ارتباطات بین خودروئی از چالش زیادی برخوردار است.[۲]

با همه مزایایی که در شبکه ارتباطات بین خودروئی شامل مجموعه ای از حملات و تهدید ها است، ولی الگوریتم های زیادی را می توان برای حل انواع حمله در شبکه ارتباطات بین خودروئی طراحی کرد. این الگوریتم ها برای حل مشکلات انتقال اطلاعات در این شبکه ها استفاده می شود. بسیاری مشکلات از طریق حل مشکل مسدود کردن ( ) در VANET قابل حل است.[۳]

اتومبیل های بدون سرنشین آخرین دستاورد شبکه ارتباطات بین خودروئی است که باعث سلامتی، راحتی و تاثیر فراوان در نقل و انتقال فراهم می کند. [۴]

در شبکه ارتباطات بین خودروئی بیشترین اطلاعات میان یک ماشین و واحد های کنار جاده ای و اینترنت دارد. این حجم اطلاعات برای افزایش تجربیات رانندگی به منظور افزایش سلامتی بشر می باشد. [۵]

شبکه ارتباطات بین خودروئی شامل سیستم‌های ارتباطی رادیویی کوتاه برد است که روی خودروها نصب شده‌اند که به‌عنوان دستگاه‌های فرستنده گیرنده خودروئی (OBU) شناخته می شوند. این واحدها علاوه بر وظایف ارتباطی برای انجام عملیات ثبت‌نام در شبکه و مدیریت هویت نیز بکار می‌روند. دستگاه‌های فرستنده گیرنده کنارجاده‌ای یا (RSU) ها هم در این نوع شبکه‌ها نقش مهمی دارند. وسایل نقلیه می‌توانند به دستگاه‌های فرستنده گیرنده کنارجاده‌ای متصل شوند تا به زیرساخت‌های عمومی و خصوصی مانند اینترنت و اینترانت هم دست یابند [۶].

در راستای بررسی مسائل امنیتی شبکه ارتباطات بین خودروئی در این مطلب، مواردی مانند الزامات امنیتی، انواع مهاجمان، انواع حملات و چند مکانیسم مورد استفاده، مطرح می‌گردد.

۲. الزامات امنیتی

برای حفظ امنیت و جلوگیری از آسیب یا حمله به شبکه الزاماتی به شرح ذیل وجود دارد: [۲]

احراز هویت: وجود چارچوب احراز هویت باعث می‌شود تا گیرنده‌های داده‌های همه پخشی بتوانند صحت داده‌های دریافتی واقعی از گره موردنظر را تائید کنند. احراز هویت به دو صورت تائید هویت وجودی و احراز هویت پیام امکان‌پذیر است.

یکپارچگی: جلوگیری از تغییر غیرمجاز اطلاعات است و وجود آن بین دو گره برای حفظ دقت داده‌ها لازمست.

محرمانگی: وجود این پارامتر باعث حفظ محتویات داده از دشمن و جلوگیری از افشای غیرمجاز اطلاعات می‌شود.

حریم خصوصی: حفاظت از اطلاعات شخصی هر گره از سایر گره های شبکه رعایت حریم خصوصی آن گره است. البته دسترسی به این مشخصات برای مقامات ناظر در هنگام حوادث لازم و مطلوب است.

عدم انکار: به این معنی که هیچ موجودیتی در شبکه نتواند چیزی را انکار کند؛ مثلاً انکار اعتبار امضای یک سند یا پیام ارسال شده امکان‌پذیر نیست.

اسم مستعار: توصیفی از هویت مبدل است که یک موجودیت شناسایی شود اما اسم واقعی آن افشا نشود.

مقیاس‌پذیری: توانایی برای مدیریت رشد و تغییر اندازه شبکه تا جایی که شبکه امن باشد.

تحرک پذیری: با توجه به تغییر مکان گره ها با جهت‌ها و سرعت‌های مختلف، پویا بودن شبکه بدیهی است.

تائید موقعیت مکانی: برای جلوگیری از برخی حملات و همچنین اعتبار سنجی داده‌ها، اعتبارسنجی مکان گره ها لازم است.

مدیریت کلید: کلید برای رمزگذاری و رمزگشایی اطلاعات در طول ارتباط استفاده می‌شود.

رمزگذاری داده: با استفاده از رمزگذاری به وسیله کلید، به دلیل اینکه فقط گرههای مجاز به کلید دسترسی دارند، سایر گرهها نمی‌توانند به محتویات پیام دست یابند.

۳- دسته بندی مهاجمان

مهاجمان در شبکه ارتباطات بین خودروئی بر اساس ویژگی‌ها و نوع عملکردشان از چند لحاظ قابل دسته‌بندی هستند. طبقه‌بندی مهاجمان به تعیین محدوده منابع موردنیاز برای امن سازی شبکه کمک می‌کند. [۱ ، ۲]

- مهاجم داخلی یا خارجی: اگر مهاجمی یک کاربر معتبر در شبکه باشد و بتواند با بقیه اعضای شبکه ارتباط بگیرد، مهاجم داخلی محسوب شده و درواقع یک عضو احراز هویت شده از شبکه به شمار می‌آید. در مقابل مهاجمی خارجی است که بدون مجوز وارد شبکه شده باشد .
- مهاجم مخرب یا معقول: مهاجمین مخرب به شبکه آسیب زیادی نزده و در پی اهداف شخصی خود نیستند، بلکه هدف اصلی آن‌ها آسیب به عملکرد شبکه با استفاده از روش‌های مختلف است. در عوض مهاجمین معقول پیگیر اهداف شخصی خود از تهاجم می‌باشند.
- مهاجم فعال یا منفعل: مهاجم فعال برای ایجاد خرابی در پی دسترسی به بسته‌های جدید اطلاعاتی است تا بتواند با تغییر، از بین بردن یا پاسخ اشتباه به پیام‌ها در شبکه دستاوردهایش را بیشتر کند، ولی مهاجم منفعل تنها به استراق سمع کانال‌های رسانه بی‌سیم اکتفا می‌کند.
- مهاجم مستقل یا باهم: مهاجمینی که باهم عمل کنند با تبادل اطلاعات، توانایی ایجاد حملات مؤثرتری دارند.

به طرر کلی سه هدف اصلی مهاجمین شبکه را می‌توان در کسب پول، نیروی انسانی و ابزار خلاصه کرد.

۴- انواع حملات

با توجه به این موضوع که بستر اصلی گسترش این شبکه‌ها، رسانه بی‌سیم است، طبیعتاً شانس حمله به آن بیشتر و نقش پیاده‌سازی‌های امنیتی در آن‌ها پررنگ‌تر می‌شود. حملات محتمل را می‌توان به‌صورت ذیل طبقه‌بندی کرد: [۲ ، ۳ ، ۵]

۴-۱. حملات محرمانگی

استراق سمع: دسترسی غیرمجاز به ارتباطات خصوصی مانند تماس تلفنی، ویدئوکنفرانس و ... با هدف دسترسی به اطلاعات محرمانه است.

جمع‌آوری اطلاعات: توسط مهاجم داخلی یا خارجی می‌تواند صورت گیرد و هدف اصلی آن انتقال اطلاعات نادرست یا جعلی در شبکه می‌باشد.

آنالیز ترافیک: مهاجم با توجه به ترافیک ارتباطات بی‌سیم از طریق ارزیابی اطلاعات، مقدار دیتای انتقالی و گرایش انتقالات مکان گره را تعیین می‌کند. به این صورت که بسته‌های مربوط به ارتباطات بین دو خودرو (V2V) یا بین خودرو و زیرساخت‌ها (V2I) بررسی شده و از بسته‌های حاوی شناسه و مکان خودرو برای به دست آوردن اطلاعات لازم استفاده می‌شود.

۴-۲. حملات یکپارچگی

توقیف پیام: مهاجم قسمت‌های مهم بسته‌های انتقالی را برای تأثیر بر یکپارچگی بسته‌ها از بین می‌برد. پس گره دریافت‌کننده ممکن است پیام‌های مهم را گم کند و این موضوع منجر به وضعیت‌های بحرانی شود.

تغییر پیام: مهاجم می‌تواند پیام‌ها را بین دو گره ارتباطی قطع کرده، اطلاعات خاصی را تغییر دهد یا تأخیر در انتقال پیام ایجاد کند و منجر به وقفه در سرویس خاصی شود .

ساخت پیام: یک پیام تقلبی توسط یک کاربر غیرمجاز وارد شبکه می‌شود.

ارسال مجدد: مهاجم می‌تواند همه بسته‌های دریافت شده را مانند یک گره معمولی، هر بار با ایجاد یک ارتباط جدید ارسال مجدد کند. در این حالت بسته‌ها به‌صورت تقلبی تکرار می‌شود.

مبدل سازی : مهاجم از آدرس IP و MAC جعلی برای گرفتن شناسه سایر گرهها و پنهان کردن خود در شبکه استفاده می‌کند. اگر فرآیند احراز هویت برای امن سازی شبکه اجرا نشود، یک گره مخرب می‌تواند با شناسه تغییریافته از طرف سایر گرهها پیام‌هایی مبنی بر ترافیک، تصادف و ... برای نیل به اهداف خاصی ارسال نماید.[۲]

۴-۳. حملات شناسایی و احراز هویت

دست‌کاری سامانه مکان‌یاب جهانی :(gps) در شبکه‌های ارتباطات بین خودروئی یک جدول مکانی شامل شناسه و موقعیت مکانی هر گره وجود دارد که با تبعیت از اطلاعات ماهواره مکان یاب تکمیل، نگهداری و به‌روز می گردد. مهاجم می تواند با استفاده از یک شبیه‌ساز ماهواره مکان‌یاب و تولید سیگنال قوی‌تر از ماهواره اصلی، برای گره ها این اشتباه را به وجود آورد که به نظر بیاید در موقعیت جغرافیایی دیگری هستند.

حملهSybil : این حمله این‌گونه است که مهاجم چندین پیام به سایر گره ها ارسال می‌کند طوری که هر پیام حاوی شناسه منبع متفاوتی است. تا به نظر برسد این پیام‌ها از منابع مختلفی ارسال شده‌اند.

تونل زنی: مهاجم دو خودرو را بدون اطلاع گره قربانی مستقیماً توسط یک کانال ارتباطی باکیفیت بالا به‌عنوان یک تونل متصل می‌کند. خودرو قربانی فکر می‌کند که گره مهاجم همسایه آن است و از تونل برای ارسال پیام استفاده می‌کند؛ بنابراین مهاجم می‌تواند به آنالیز ترافیک پرداخته یا حملات دیگری را اجرا کند.

۴-۴. حملات دسترسی

حمله رد سرویس (DOS): این حمله می‌تواند با مصرف منابع خودرو قربانی طوری که قربانی از انجام سایر وظایف خود بماند یا با انتقال مقدار زیادی بسته‌های ناخواسته در شبکه و مسدود کردن کانال ایجاد شود. درواقع مهاجم، رسانه ارتباطی اصلی را با ارسال مداوم پیام‌های ناخواسته مسدود کرده و شبکه را به حالت قفل می‌برد. طوری‌که دسترسی به منابع و سرویس‌های شبکه امکان‌پذیر نباشد.

حمله رد سرویس توزیع شده (DDOS) : مهاجم از محل‌های مختلف و به‌صورت توزیع‌شده حمله می‌کند و می‌تواند از بازه‌های زمانی مختلفی برای ارسال پیام استفاده کند. به دلیل حرکت مداوم خودروها در این نوع شبکه ایجاد چنین حملاتی قابل‌انتظار است.

حمله انسداد: در این نوع حملات اختلال در ارتباطات کلی از طریق کاهش نرخ سیگنال توسط نویز و انتقال سیگنال‌های رادیویی مزاحم رخ می‌دهد. مهاجمین انسداد کننده به‌صورت مداوم سیگنال‌های تکراری به ناحیه آسیب‌دیده برای تداخل ارتباطات بین گرهها می‌فرستند.

سیاه‌چاله: ناحیه‌ای است که ترافیک به سمت آن هدایت می‌شود اما در آن ناحیه گرهی وجود ندارد یا گره های مستقر در آن منطقه به شبکه وارد نمی‌شوند. یک گره مخرب می‌تواند خود را به‌عنوان دارنده کوتاه‌ترین مسیر تا مقصد معرفی کرده و در پروتکل مسیریابی تقلب کند. بدین ترتیب می‌تواند مسیر جعلی را برقرار و بسته‌ها را انتقال داده یا از بین ببرد. درواقع مهاجم یک ارتباط برقرار کرده و بعد آن را از بین می‌برد تا ترافیک به سمت گره ناموجود هدایت شود یا خودش به‌عنوان سیاه‌چاله عمل کرده و همه ترافیک را جذب می‌کند.

بدافزار و هرزنامه : این پیام ها که می توانند اختلال جدی در عملکرد شبکه ایجاد کنند، معمولاً توسط عوامل داخلی اجرا می‌شوند، نه مهاجمین خارجی. بدافزارها هم پهنای باند زیادی مصرف کرده و تأخیر انتقال را افزایش می‌دهند، درواقع مانع عملکرد معمول شبکه می‌شوند.

۴-۵. حمله به حریم خصوصی

حمله زمانی: در این شبکه‌ها زمان بسیار موردتوجه است زیرا کاربران نیاز دارند اطلاعات دقیق را به صورت بلادرنگ دریافت کنند پس تحمل تأخیر بسیار کم است. در این حمله مهاجم با گرفتن پیام و تغییر در بازه های زمانی مربوطه بدون تغییر محتوای پیام، منجر به دیر رسیدن پیام‌ها می‌شود.

حمله فرد میانی: در این حمله مهاجم میان دو خودرو قرارگرفته و برای اجرای اهداف خود فرصت می یابد. این‌طور به نظر می‌آید که دو گره مستقیماً به هم متصل‌اند اما درواقع مهاجم همه ارتباطات بین آن‌ها کنترل کرده، پیام‌های نادرست می‌فرستد یا محتوای پیام‌ها را تغییر می‌دهد.

Brute force: این نوع حمله بسته به ویژگی‌های آماری متن رمز شده یا کلید رمز دارد و ابزار زیادی برای به دست آوردن اطلاعات مفید توسط آنالیز متن رمز دارد. این نوع حمله برای نفوذ به سیستم‌های رمزنگاری و هک کلید یا متن رمز استفاده شده و مستقیماً منجر به نقض حریم خصوصی می شود. این نوع حمله در بسیاری موارد به‌عنوان ابزار ارزیابی غیرمجاز برای بررسی توانایی امنیتی سیستمی خاص بکار می‌رود.

افشای شناسه: در این حمله مهاجم از همسایگان خودرو هدف برای ارسال برخی کدهای مخرب استفاده می‌کند که از راه دور و بدون اطلاع گره قربانی اطلاعات لازم را جمع‌آوری کند. این حمله اغلب محل و شناسه خودرو قربانی را هدف می‌گیرد و مستقیماً به حریم خصوصی کاربر حمله می‌کند .

اطلاعات جعلی: مهاجم می تواند کاربر مجاز داخلی یا خارجی باشد که در هر دو حالت اطلاعات گمراه‌کننده‌ای برای تأثیر بر تصمیم گره های شبکه پخش می‌کند.

۵. مکانیسم‌های امنیتی

استفاده از پلاک الکترونیکی: اعداد رمزنگاری شده و قابل تائیدی که معادل پلاک‌های سنتی هستند و به شناسایی و سایل نقلیه سرقت رفته یا ردیابی آن‌ها کمک می‌کنند؛ که این روش جز روش‌های سنتی به حساب می‌آید. انواع مکانیسم‌های امنیتی شامل: [۲، ۴]

مکانیسم‌های دفاعی: برای ورودی‌هایی با معیارهای امنیتی در شبکه‌های ارتباطات بین خودروئی، مکانیسم دفاعی از رویکرد نظریه بازی‌ها در سه مرحله استفاده می‌کند. ابتدا اکتشاف بر پایه بهینه سازی کلونی مورچگان برای شناسایی دشمن، سپس استفاده از تعادل نش برای انتخاب مدل مشکلات امنیتی و نهایتاً فعال‌سازی مکانیسم دفاعی انجام می‌شود.

استفاده از رمزنگاری: رمزنگاری جهت حفاظت داده‌های انتقال داده شده بکار می‌رود. استفاده از روش رمزنگاری کلید عمومی (PKI)روشی امن برای رمزگذاری اطلاعات به‌حساب می‌آید. در این حالت فرستنده پیام را به‌وسیله کلید عمومی گیرنده، کدگذاری می‌کند. به‌محض دریافت پیام، گیرنده از کلید خصوصی خود برای رمزگشایی استفاده می‌کند۰ روش RSA یک روش رمزنگاری کلید عمومی است که یک پیام را با استفاده از یک جفت کلید (کلید عمومی و کلید خصوصی) رمزنگاری و رمزگشایی می‌کند. امروزه اغلب پیاده سازی‌های این الگوریتم از یک عدد ۵۱۲ بیتی استفاده می شود، لذا ایجاد دستر سی به چنین سیستمی نیاز به توانایی تولید دو جفت عدد ۵۱۲ بیتی اولیه را دارد که فراتر از توانایی الگوریتم‌های امروزی است.

محلی سازی امن: در شبکه‌های خودروئی که توپولوژی مرتباً و به سرعت تغییر می‌کند، این موضوع چالش عمده‌ای است. هرگاه یک ارتباط یک‌به‌یک در خصوص مکان گرهها باید شروع شود و محل جغرافیایی گره مقصد قدیمی یا نامعلوم باشد از این روش برای تعیین محل به‌روز شده استفاده می‌شود.

فسخ گواهینامه: وقتی هر رفتار نامعمولی از وسیله نقلیه سر بزند یا وقتی چند گره به دستگاه فرستنده گیرنده کنارجاده‌ای اعلام کنند که یک وسیله نقلیه اطلاعات نادرست در شبکه پخش می‌کند، اعتبار آن گره فسخ می‌گردد. درواقع هربار که گیرنده‌ای اطلاعات نادرست دریافت کرد باید این موضوع را به دستگاه فرستنده گیرنده کنارجاده‌ای گزارش کند.

شبکه‌های عصبی مصنوعی (ANN) که الهام گرفته از شبکه‌های عصبی بیولوژیکی هستند. آن‌ها از رخ دادن حملات جلوگیری نمی‌کنند اما در عوض حملات را مسدود می‌کنند. این شبکه ها می توانند یاد بگیرند و رفتارهای غیرمعمول را از طریق فرآیندهای تکراری شان تشخیص دهند. قدرت این سیستم در یادگیری شبکه‌های عصبی مصنوعی و قابلیت تطابق آن‌ها با حملات مختلف است. تکنولوژی شبکه‌های تعریف‌شده نرم‌افزاری (SDN) یک رویکرد شبکه‌ای است درجایی که بین عملیات کنترلی و انتقال داده‌ها تمایز قائل شوند.SDNها می‌توانند بسته‌ها را فیلتر کرده و جریان داده‌های مشکوک را به کنترل‌های امنیتی لایه بالاتر هدایت کنند. ایده این روش کنترل اطلاعات توسط نرم‌افزار است. مزیت استفاده از SDN ها، سادگی نگهداری

و ارتقا و گسترش آن‌هاست که با قابلیت واکنش به‌موقع می‌توانند امنیت شبکه را بالا برده و اجازه تغییرات پویا برای سازگاری با شبکه را می‌دهد. این برنامه‌ها می‌توانند سیاست‌ها را با توجه به اطلاعات فراهم شده توسط ANN به‌روز کنند.

۶- چالش‌های مکانیسم‌های امنیتی

نوسان شبکه: در این نوع شبکه اتصال بین گره ها می‌تواند موقت و حتی یک‌بار رخ دهد مثلاً وقتی دو خودرو خلاف جهت هم حرکت می کنند. پس راه حل های مبتنی بر ایجاد گروهی از کاربران قابل‌اعتماد یا ایجاد ارتباط با یک نقطه امن پایانی یا رویکردهای مبتنی بر کلمات عبور در این شبکه‌ها به کار نمی‌آید و باید مکانیسم‌هایی طراحی شوند که این مسائل نوسانی شبکه را پوشش دهند . [۴]

در نوسان شبکه ها یکی از مشکلاتی که باعث بروز اختلالات در ارتباط میان دو گره می شود جابجایی گره هاست. با تغییرات اندازه جغرافیایی (مختصات x و y) گره ها نسبت به یک مبدا ثابت می تواند این اتفاق رخ دهد. به عبارت دیگر افزایش فاصله جغرافیایی بین دو گره می تواند علت بروز نوسان شبکه باشد. یکی از راه حل ها می تواند به جای انتخاب یک نقطه امن پایانی استفاده از گره های متحرک و مشترک میان دو گره باشد.

حفظ حریم شخصی در مقابل پاسخگویی: در این شبکه‌ها برای به دست آوردن اطلاعات ترافیکی و شناسایی خودروها در حوادث می‌بایست از هویت خودرو به‌عنوان منبع اطلاعاتی اطمینان حاصل کرد .[۴]

برنامه‌های حساس به تأخیر زمانی: در شبکه ارتباطات بین خودروئی اغلب برنامه‌های ایمنی و کمک به رانندگان حساس به زمان بوده و یک مهلت دقیق برای زمان تحویل پیام دارند.[۴]

دلایل تاخیر زمانی، تاخیر های متفاوت ناشی از بخش های شبکه می باشد. کاهش تاخیر زمانی به نوعی کارآیی شبکه محسوب می شود. برای افزایش کارآیی حتما هزینه اضافه تری به شبکه تحمیل می شود. بهبود سخت افزار سیستم می تواند سرعت انتقال داده ها را افزایش دهد که باعث کاهش تاخیر زمانی است.

نامتجانس بودن: با توجه به وجود زیر سیستم‌ها و خودروهای گوناگون در این نوع شبکه، نامتجانس بودن کاملاً مشهود است. این تنوع و همچنین تعداد زیاد برنامه‌هایی که پشتیبانی می‌شوند نیز چالش دیگری به شمار می‌رود. [۴]

۷. نتیجه‌گیری

شبکه ارتباطات بین خودروئی مانند هر شبکه دیگری بدون چالش‌های امنیتی نیست و چون برای انتقال داده یا هرگونه اطلاعات بین دو وسیله نقلیه از رسانه بی‌سیم استفاده می‌شود، همین موضوع زمینه‌ساز حملات مختلف شده است. مهاجمان سعی در تأثیرگذاری در شبکه از طریق ابزار مختلف و با رفتاری پویا که غیرقابل‌پیش‌بینی است، دارند. با کسب دسترسی غیرمجاز به شبکه یک مهاجم می‌تواند کنترل اجزای حیاتی وسیله نقلیه را گرفته، به وسیله نقلیه یا مسافران آسیب جدی وارد کرده و در سطوح مختلف تأثیرات متفاوتی بر شبکه بگذارد؛ بنابراین بایستی پروتکل‌هایی استفاده شوند تا ارتباطات شبکه ارتباطات بین خودروئی به‌صورت امن، قابل‌اطمینان و قابل‌کنترل به‌صورت بی‌وقفه کار کرده و مسائلی مانند منابع محدود، پهنای باند محدود، لزوم تأخیر کوتاه، ماهیت ارتباط نقطه‌به‌نقطه، تبادل مداوم اطلاعات و ... در راه‌حل‌های امنیتی خاص در نظر گرفته شوند.

امروزه روش‌های متعددی برای افزایش امنیت در این شبکه‌ها پیشنهاد شده است. روش‌هایی مانند رمزنگاری اطلاعات، پایش رفتار گره ها جهت تشخیص گره های مخرب و ... یکی از راهکارهای جدید در این حوزه استفاده از شبکه‌های عصبی مصنوعی با استفاده از تکنولوژی SDN است. درواقع ANNها می‌توانند برای تعیین رفتار غیرمعمول مهاجم مخرب یاد گرفته و برای محافظت از شبکه سازگار شوند. SDNها نیز می‌توانند سیاست‌های شبکه که توسط ANNها مشخص شده را اجرا کرده و به کنترل شبکه پویای ارتباطات بین خودروئی کمک کنند

مراجع

[1] Ajulo, E. B., 2018, “Security Threats and Privacy Issues in Vehicular Ad-Hoc Network (VANET): Survey and Perspective," Journal of Information, vol. 42, pp. 1-9.

[2] Nampally V., M. R. Sharma, 2017, "A Survey on Security Attacks for VANET," International Journal of Computer Science and Mobile Applications, vol. 52, pp. 58-70

[3] Abdelgader A. M. S., F. Shu, W. Zhu and K. Ayoub, 2017. "Security Challenges and Trends in Vehicular Communications”, Conference on System, Process and Control (ICSPC 2017), pp. 105-110.

[4] Ydenberg A., N. Heir, B. gill, 2018, "Security, SDN, and VANET Technology of Driver-less Cars," Electrical Engineering, School of Energy, British Columbia Institute of Technology Burnaby, Canada, vol. 2, pp. 313-316.

[5] Khelifi, H., S. Luo, B. Nour, S. C. Shah, 2018. "Security and Privacy Issues in Vehicular Named Data Networks: An Overview", Mobile Information System (ID 5672154), pp.1-11 .

[6] Ghori, M. R.,Kamal Zamli and *etal.* , 2018. "Vehicular Ad-hoc Network (VANET): Review", International Conference (ICIRD), pp. 1-6.

پیوست

کلمات زیر به ترتیب در متن ترجمه شده است.

۱- شبکه ارتباطات بین خودروئی : Vehicular Ad Hoc Network (VANET)

۲- سیستم های انتقال هوشمند : : Intelligent Transportation System (ITS)

۳- شبکه‌های موردی بی‌سیم : Wireless Ad Hoc Network (WANET)

۴- شبکه‌های مبتنی بر حرکت : Mobile Ad Hoc Network (MANET)

۵- دستگاه‌های فرستنده گیرنده خودروئی : On Board Unit (OBU)

۶- دستگاه‌های فرستنده گیرنده کنارجاده‌ای :Road Side Unit (RSU)

۷- احراز هویت : Authentication

۸- همه پخشی: Broadcast

۹- یکپارچگی : Integrity

۱۰- محرمانگی : Confidentiality

۱۱- عدم انکار : Non-Repudiation

۱۲- اسم مستعار : Pseudonymity

۱۳- مهاجم داخلی : attacker Insider

۱۴- مهاجم خارجی: Outsider attacker

۱۵- مهاجم مخرب: Malicious attacker

۱۶- مهاجم معقول : Rational attacker

۱۷- استراق سمع: Eavesdropping

۱۸- جمع‌آوری اطلاعات: Information Gathering

۱۹- ارتباطات بین دو خودرو: Vehicle to Vehicle (V2V)
۲۰- ارتباطات بین خودرو و زیرساخت‌ها: Vehicle to Infrastructure (V2I)
۲۱- توقیف پیام : Massage Suppression
۲۲- تغییر پیام: Massage Alteration
۲۳- ساخت پیام: Massage Fabrication
۲۴- ارسال مجدد: Replay
۲۵- مبدل سازی: Masquerade
۲۶- سامانه مکان‌یاب جهانی: Global Positioning System (gps)
۲۷- حمله رد سرویس: Denial of Service (DOS)
۲۸- حمله رد سرویس توزیعشده: Distributed Denial of Service (DDOS)
۲۹- حمله انسداد: attack Jamming
۳۰- سیاه‌چاله : Black hole
۳۱- بدافزار: Malware
۳۲- هرزنامه: Spam
۳۳- حمله فرد میانی: Man in the Middle attack
۳۴- افشای شناسه: Id Disclosure
۳۵- اطلاعات جعلی: Bogus
۳۶- تعادل نش : Nash Equilibrium
۳۷- روش رمزنگاری کلید عمومی: :Public Key Infrastructure (PKI)
۳۸- روش رمزنگاری کلید عمومی : : Rivest–Shamir–Adleman (RSA)
۳۹- محلی سازی امن : Localization
۴۰- شبکه‌های عصبی مصنوعی : : Artificial Neural Network (ANN)
۴۱- شبکه‌های تعریف‌شده نرم‌افزاری: : Software Define Network (SDN)

چکیده مقاله به زبان انگلیسی:

The Vehicular Ad Hoc Networks and Security Challenges

Zohreh Bateni
Department of Computer Enginerring, Faculty of Technical & Enginering,
University of Islamic Azad- Central Tehran Branch, Highway Ashrsfi
Esfahani , Ponak Square, Complex of University neyayesh, Iran,
E-mail: zbateni@hotmail.com

Bahareh Hadigol
Department of Computer Enginerring, Faculty of Technical & Enginering,
University of Islamic Azad- Central Tehran Branch, Highway Ashrsfi
Esfahani , Ponak Square, Complex of University neyayesh, Iran,

E-mail: b.hadigol@yahoo.com
Abstract. Vehicular Ad Hoc Network (VANET) is a dynamic network topology with wireless media infrastructure. In addition Vehicular Ad Hoc Network, access to safety and entertainment programs is provided on these networks. Such as information on road conditions, traffic conditions, crash reports, and more…, and this Variety has become more development the vehicular ad hoc network. Since the security of these networks is involved with everyday life and even human lives, so one of the major studies in the development of the Intelligent Transportation System (ITS) is to check the security of these networks. Due to the features of this network, Such as bandwidth restrictions, permanent information exchange, need to respond timely and more, certain security architectures should be considered. In this paper, the security requirements of these networks and important of attacks in various areas have been studied. Moreover several security mechanisms and challenges have been studied.
Keywords: Vehicular Ad Hoc Network (VANET), attacker, security, Confidentiality, Integrity