www.NoavaranGermi.ir
سایت نوآوران گرمی - همیار دانشجو

بررسی و دسته بندی انواع حملات در شبکه های موردی بین خودرویی[1]

آرمینا ابراهیمی قلاتی[1]

[1] دانشکده کامپیوتر و فناوری اطلاعات، دانشگاه ازاد اسلامی، واحد علوم و تحقیقات بوشهر،
Ebrahimi.armina@gmail.com

پیشرفت های اخیر توسعه ارتباطات بی سیم در شبکه موردی بین خودرویی خط مشی جدیدی را برای صنعتگران و محققان فراهم کرده است. شبکه های موردی بین خودرویی شبکه های چند هاپ بدون زیرساخت های ثابت هستند. این شبکه ها شامل وسایل نقلیه در حال حرکت می باشند که قادر به برقراری ارتباط با یکدیگرند[9]. یکی از چالش های اصلی در VANET تعیین مسیر داده ها به طورموثر از منبع به مقصد است. طراحی پروتکل مسیریابی کارآمد برای VANET کاری خسته کننده است. همچنین به دلیل رسانه های بی سیم، VANET در برابر حملات آسیب پذیر است. از آنجا که حملات عملیات شبکه را مختل می کند، امنیت برای استقرار موفقیت آمیز چنین فناوری ای الزامی می باشد. در نتیجه ما باید به طور کامل این حملات را بشناسیم تا بتوانیم با آنها مقابله کنیم. این مقاله نظری اجمالی برانواع حملات در VANET دارد.

کلمات کلیدی : VANET ، امنیت ، وسایل نقلیه.

1- مقدمه

توسعه سریع شبکه های ارتباطی بی سیم در سال های اخیر ارتباطات بین خودرویی[2] و ارتباطات جاده وخودرو[3] را درشبکه سیار[4] امکان پذیر ساخته است. این امر سبب پیدایش نوع جدیدی از MANET شناخته شده به عنوان شبکه موردی بین خودرویی با هدف فعال کردن ایمنی جاده، رانندگی کارآمد و سرگرمی شناخته شده است[5].

زندگی درجهان امروز میدان نبرد نهفته در جاده ها است، تعداد مرگ و میر حدود 1,2 میلیون نفر سالانه در سراسر جهان تخمین زده می شود[16] و تعداد زخمی ها حدود چهل برابر است در ضمن فراموش نشود که تراکم ترافیک باعث اتلاف زیاد وقت و سوخت می گردد [3].

شبکه های موردی بین خودرویی بخشی از شبکه های Ad hoc تلفن همراه است، این بدان معنا است که هرگره می تواند آزادانه در پوشش شبکه حرکت کند، با دیگر گره ها در یک یا چند هاپ ارتباط برقرارکند و همچنین می تواند واحد کنار جاده خودرو[5] باشد[5].VANET به رانندگان وسایل نقلیه برای ارتباط و هماهنگی میان خود به منظور جلوگیری از هر گونه وضعیت بحرانی از طریق ارتباط خودرو به خودرو کمک می کند[1].

نخستین و بزرگترین چالش شبکه‌های بین خودرویی موردی، امنیت آنها است. به راحتی می‌توان تصور کرد که اگر کوچکترین تهدیدی متوجه این‌گونه شبکه‌ها گردد چه عواقب ناگوار جانی و مالی به دنبال خواهد داشت و برخلاف اینترنت یا وب، سلامت و جان انسان‌ها به طور مستقیم در معرض خطر قرار می‌گیرد. کافی است شبکه VANET اطلاعات دقیقی به راننده ندهد تا شاهد تصادف و واژگونی و صدها رخداد دیگر باشیم.

شبکه‌های « موردی بین خودرویی » می‌توانند بزرگترین فناوری متحول کننده خودروها در دهه دوم هزاره دوم باشند و امنیت را به رانندگان هدیه کنند. مسئله امنیت در شبکه‌های VANET آن‌قدر حساس و بحرانی است که یکی از عوامل اجرایی نشدن این شبکه‌ها در سال‌های گذشته محسوب می‌شود.

این مقاله در پنج بخش سازمان یافته است. در بخش دوم به تعریف امنیت پرداخته ایم؛ در بخش سوم خصوصیات یک ارتباط قابل اطمینان را بیان کرده ایم؛ بخش چهارم شامل بررسی اجمالی برنگرانی های امنیتیVANET که است و با یک نتیجه گیری در بخش پنجم مقاله را به اتمام رسانده ایم.

2- تعریف امنیت

امنیت شبکه یا Network Security پردازه ای است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می شود. پس از تعیین دارایی های شبکه و عوامل تهدیدکننده آنها، باید خطرات مختلف را ارزیابی کرد. در بهترین حالت باید بتوان از شبکه در مقابل تمامی انواع خطا محافظت کرد، اما امنیت ارزان به دست نمی آید.

بنابراین باید ارزیابی مناسبی را بر روی انواع خطرات انجام داد تا مهمترین آنها را تشخیص دهیم و از دیگر منابعی که باید در مقابل این خطرات محافظت شوند نیز شناسایی شوند. دو فاکتور اصلی در تحلیل خطر عبارتند از:

1. احتمال انجام حمله.
2. خسارت وارده به شبکه درصورت انجام حمله موفق.

3- امنیت و حریم خصوصی

وقتی اطلاعات در بین اشخاص ناشناس جمع‌آوری و تقسیم می‌شوند؛ نگرانی‌ها در خصوص موثق و قابل اعتماد بودن اطلاعات یک سیستم افزایش می‌یابد، برای مثال یک فرستنده می‌تواند در بیان مشاهدات به خاطر نفع خود سوء استفاده کند؛ مثلاً خودروی A به غلط اعلام می‌کند که جاده مطلوب خودروی B، پر ترافیک است و بدین ترتیب دیگران را از خودروی B دور می‌کند و بدین ترتیب مسیر خلوتی برای B ایجاد می‌کند. گزارش‌های شریرانه می‌تواند سایر خودروها را به تقلید رفتار همان خودرو یا زیر ساخت‌های کنار جاده برای ناامن کردن جاده وا دارد. خودروها می‌توانند با ایجاد شبکه معتمد، اطلاعات رسیده از فرستندگان نامعتبر را نادیده بگیرند. موفقیت و مقبولیت این فناوری در میان مشتریان نیازمند ایجاد سطح بالایی از قابلیت اعتماد و امنیت است. یک ارتباط قابل اعتماد عموماً باید دو خصوصیت داشته باشد:

- فرستنده در نهایت به عنوان یک منبع قابل اعتماد پذیرفته شود.
- پیام فرستنده در حین انتقال دست‌کاری نشود. یک چالش مهم در امنیت VANET فراهم آوردن اعتبارسنجی فرستنده در ارتباطات می‌باشد.

4- نگرانی های امنیتیVANET

نگرانی های امنیتی VANET در دو بخش ذیل مورد بحث قرار گرفته است[5]:

- حملات
- مهاجمان

1-4 حملات در VANET

هدف اصلی امنیت در VANET نگهداری اطلاعات و منابع در برابر حملات است.VANET می بایست امکانات امنیتی را که در حوزه اطمینان از محرمانگی اطلاعات [6] ، پنهان سازی اطلاعات شخصی[7] ، تصدیق و اعتبار دستگاه ها [8]، اعتبار داده[9] ،در دسترس بودن شبکه در طول ارتباطات [10] و مقوله انکارناپذیری [11] مهیا سازد[14,15].

1-1-4 حمله هایی که سبب تهدید احراز هویت هستند:

یعنی اطمینان دادن از اینکه نهاد ارتباطی همانی که ادعا می کند باشد. این امر گره را قادر به تایید هویت از گره برقراری ارتباط می سازد. همچنین مهم است که گره دریافت اطلاعات اطمینان یابد که داده ها از یک فرستنده معتبر فرستاده شده است. برای مثال انتقال وسایل نقلیه باید با کاربر معتبر ثبت شده درسازمان گواهی مربوطه به منظور شناسایی وسیله نقلیه منحصر به فردباشد[14].

در این نوع از حمله منطقه آسیب دیده منطقه شناسایی یا تصدیق هویت است. هر زمان که هر گونه وسیله نقلیه درVANET نیاز به ارتباطات امن دارد شناسایی و یا خروج ازگره تحت نظارت امری ضروری است. هنگامی که وسیله نقلیه دریافت کننده شناسایی یا تصدیق می شود سپس تنها خودرو فرستنده قابل اعتماد برای برقراری ارتباط میان آنها مجاز است[9]. انواع مختلفی از حمله به اعتبارهویت به شرح زیر مورد بحث قرار گرفته است:

1-1-1-4 نقاب(تغییرقیافه)[12]:

این حمله نتیجه ارائه هویت های دروغین درحین ارتباط توسط مهاجم است. نقاب [14] شامل ساخت پیام، تغییر و پخش پیام می باشد. به عنوان مثال برای کم کردن سرعت وسیله نقلیه دیگر مهاجم تلاش می کند به عنوان وسیله نقلیه اورژانس عمل کند و از این رو وسایل نقلیه دیگر را فریب می دهد[9].

2-1-1-4 حمله Sybil:

حمله Sybil نوعی جعل هویت است که در آن چندین هویت ازگره مهاجم حاضر است. با نهادهای مختلف در شبکه از آن خواهد شد قادر به کاهش اثر بخشی طرح های مقاوم در برابر خطا خواهد شد[7,12]. شکل 1 نشان می دهد که گره Sybil شخصیت های متعدد از گره مهاجم فرض می شود.

- درحمله Sybil یک گره مخرب هویتهای مختلف به شکل گره های متعدد می سازد[7,9,12].
- این ساختگی وسایل نقلیه همسایه را با برقراری ارتباط با سایر گره های فیزیکی و توزیع اطلاعات ترافیک نادرست گمراه می کند(به عنوان مثال، تراکم ترافیک و یا حوادث)[8,12].

- این حمله در مسیریابی جغرافیایی بسیار خطرناک است زیرا یک گره می تواند ادعا کند همان زمان در موقعیت های مختلفی است[12].

حملات Sybil می تواند سبب تهدید بزرگ امنیتی برای VANETها باشد.

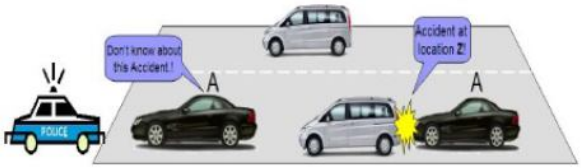
اولاً: گره Sybil ممکن است سبب ایجاد توهم تراکم ترافیک شود. راننده حریص ممکن است وسایل نقلیه مجاور را متقاعد کند که ازدحام قابل توجهی در پیش رو است به طوری که آنها مسیرهای جایگزین را انتخاب کنند و اجازه دهند راننده حریص در یک مسیر خلوت به مقصد خود برسد[8,12].

دوماً: گره Sybil ممکن است به طور مستقیم یا غیر مستقیم داده های غلط به شبکه ها تزریق کند که تا بطور گسترده ای درثبات داده از سیستم تأثیرگذار است. برای مثال ممکن است VANET ها برروی رای گیری وسایل نقلیه متعدد برای تولید یک گزارش وضعیت ترافیک تکیه کنند[7]. با این حال اگر برخی از رای دهندگان وسایل نقلیه Sybil هستند این گزارش ممکن است با توجه به منفعت مخرب از واقعیت انحراف یابد. در نهایت گره ها ممکن است حملات DoS بیشتر مانند حملات متراکم کانال و حملات سرکوب پیام راه اندازی کنند[12].

شکل1- حمله Sybil در شبکه VANET [7]

3-1-1-4 حمله جعل هویت گر[13]:

در VANET هر خودرو دارای یک شناسه منحصر به فرد است و با کمک این شناسه هر وسیله نقلیه در شبکه VANET شناخته شده است. زمانی است که حادثه اتفاق می افتد این شناسنامه مهم ترین سند است. در حمله جعل هویت گره یک مهاجم می تواند مانند یک مبتکر واقعی پیام تغییرات هویت و فعالیت اعمال نماید.مهاجم پیام را از پدیدآورنده پیام دریافت و محتویات پیام را به نفع خود تغییر می دهد. پس از آن مهاجم این پیام را به وسایل نقلیه دیگر می فرستد[7].



شکل2- حمله جعل هویت گر در VANET [7]

4-1-1-4 سرکوب پیام[14]:

در این حمله مهاجم بطورانتخابی می تواند بسته ها راکه ممکن است اطلاعات حیاتی برای گیرنده داشته باشند از شبکه رها کند . به عنوان مثال مهاجم ممکن است هشدار ازدحام را حذف نماید که به منظور جلوگیری ازترافیک گره وانتخاب مسیر جایگزین به مقصد است و آنها را وادار کند در ترافیک بمانند.مهاجم ممکن است از این بسته ها دوباره برای به دست آوردن مزایا استفاده کند. هدف اصلی مهاجم جلوگیری ازآگاهی مقامات و RSU در مورد تصادف است[5].

5-1-1-4 تغییر[15] :

همانطور که از نام آن پیداست، این حمله به معنای تغییر یا اصلاح داده های موجود است. این حمله می تواند توسط به تاخیر انداختن انتقال پیام به عمد با پخش دوباره پیام انتقالی قبلی یا تغییربخش خاصی از پیام رخ دهد. به عنوان مثال مهاجم داده هایی را که ازدحام در جاده ها عادی است بدست می اورد اما با دستکاری آن و به دروغ نشان می دهد که بزرگراه به شدت متراکم است[8,9].

6-1-1-4 پخش مجدد[16]:

این حمله است اساسا توسط کاربر مجاز و یا مخرب با چهره مبدل به عنوان یک کاربر مشروع و یا RSU استفاده می شود. همانطور که از نام آن پیداست این حمله اصولا زمانی اتفاق می افتد که مهاجم انتقال فریم های تولید شده پیشین را در اتصالات جدید پخش می کند. مهاجم فریم تولید شده را گرفته و از آن در بخش های دیگرشبکه ها استفاده می کند. در حال حاضر ما هیچ محافظت در برابر پخش مجدد سیگنال نداریم و حاوی برچسب زمان و یا شماره ی ترتیب نمی باشند. هدف اصلی از این حمله گیج کردن کارشناسان و جلوگیری از شناسایی وسیله نقلیه در هر حادثه است[5].

7-1-1-4 حقه بازی GPS[17]:

برای حفظ هویت و موقعیت جغرافیایی تمام وسایل نقلیه درجدول مکان یابی شبکه در ماهواره GPS نگهداری می شود. مهاجم از یک شبیه ساز ماهواره ای GPS برای تولید سیگنال موثر تر از ماهواره ی GPS اصلی استفاده می کند. مهاجم GPS های ساختگی تولید می کند از طریق شبیه ساز برای گمراهی وسایل نقلیه خوانده می شود تا گمان کنند که آنها در مکان های متفاوت می باشند[9].

8-1-1-4 تونل[18] :

مهاجم با استفاده از اتصال کانال های ارتباطی اضافی به عنوان یک تونل دو بخش دور از هم شبکه موردی را بهم وصل می کند. به این ترتیب

دو گره دور از هم فرض می کنند که مجاور هم هستند و با استفاده ازتونل اطلاعات می فرستند. مهاجم امکان انجام تجزیه و تحلیل ترافیک و یا حمله گزینشی حمل و نقل را دارد[9,10].

4-1-1-9 افشای آیدی [19]:

این یک حمله غیر فعال می باشد. در این حمله مهاجم کد مخرب را به همسایه ها ی گره هدف ارسال و اطلاعات مورد نیاز را جمع آوری می کند. آنها ID گره ی هدف و مکان فعلی آن را بر می دارند. با توجه به این هدف ID خودرو فاش خواهد شد و آنها حریم خصوصی خود را از دست می دهند. ناظر جهانی می تواند با نظارت بر مسیر وسیله نقلیه مورد نظر به داده های آنها دسترسی داشته باشد. برای این هدف مهاجم می تواند از RSU استفاده کند. به عنوان مثال، شرکت های اجاره ای از این روش برای حفظ ردیابی حرکت وسایل نقلیه خود استفاده می کنند[9].

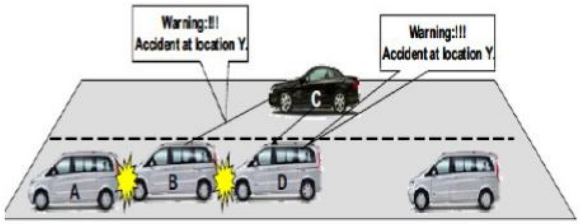
4-1-2 گروهی که تهدیدی برای محرمانه بودن راننده و موارد دیگراست:

محرمانه بودن به معنی حفاظت از داده ها از افشای غیر مجاز است. محرمانه بودن اطلاعات تضمین می کند که داده ها به بیرون درز نکرده است و یا به گره های غیر مجاز فاش نشده است. افشای این داده ها ممکن است منجر به شناسایی اطلاعات حیاتی گردد. برای مثال داده هایی که توسط وسایل نقلیه منتقل می شود باید تنها توسط وسایل نقلیه ثبت نام شده دریافت گردد[14].

محرمانه بودن پیام های رد و بدل شده بین گره های شبکه های بین خودرویی به طور خاص با برخی تکنیک ها آسیب پذیرند. مانند مجموعه پیام های غیرقانونی از طریق استراق سمع و جمع آوری اطلاعات مربوط به مکان که از طریق انتقال پیام های رسانه ای قابل دسترسی است. در مورد استراق سمع، مهاجمان خودی و یا خارجی می توانند اطلاعات مربوط به کاربران جاده را بدون اطلاع آنها جمع آوری کنند و از اطلاعات در زمانی که کاربر بی اطلاع از این مجموعه است استفاده کنند. حفظ حریم خصوصی از نظر مکانی وشخصی از مسائل مهم برای کاربران خودرو هستند. حفظ حریم موقعیت مکانی کاربران شامل پنهان کردن فاصله ی مکانی و زمانی کاربر است. با اختفای درخواست یک کاربر به طوری که از درخواست های کاربران دیگر غیر قابل تشخیص باشد تا حدی میتوان ناشناس باقی ماند[9].

4-2-1-1 حمله زمان بندی [20]:

زمان یکی از جنبه های بسیار مهم در هر برنامه است طوری که کاربران به اطلاعات دقیق در زمان مناسب و بدون هر گونه تاخیر نیازدارند. زمان همچنین موضوع مهمی در برنامه های کاربردی ایمنی ITS است. در این حمله مهاجم بدون دستکاری محتوای واقعی پیام با اضافه کردن شکاف زمانی برای ایجاد تاخیر درارسال پیام سبب می شود کاربر پیام را بعد از زمان مورد نیاز دریافت کند. برنامه های کاربردی ایمنی ITS زمان بندی شده اند که نیاز به انتقال داده ها در زمان مقرر دارند و در غیر این صورت حوادث عمده می تواند رخ دهد[7].



شکل3- حمله زمانبندی درVANET [7]

4-2-1-2 حمله صفحه اصلی [21] :

اینترنت جزء کلیدی از VANET است. در این حمله مهاجم کنترل وسیله نقلیه کاربررا با اتصال به اینترنت بدست می گیرد.سه رویکرد مختلف که مهاجم می تواند برای حمله به خانه استفاده کند[7].

- در این حمله مهاجم کنترل نرم افزار، وسیله نقلیه کاربررا بدست می گیرد؛ سپس او می تواند برخی پیام اشتباه تولید و به شبکه بفرستد[7].
- در این حمله مهاجم کنترل حسگر وسیله نقلیه کاربر را به دست گرفته و سپس می تواند با توجه به نیاز خود تغییر رفتار درسنسورایجاد کند[7].
- در این حمله مهاجم کنترل سخت افزار [22] وسیله نقلیه کاربررا داراست و سپس می تواند سبب تغییر افزایش یا کاهش سرعت وسیله نقلیه شود[7].

4-2-1-3 انسان دروسط حمله [23] :

همانگونه که از نام این حمله پیداست مهاجم با نشستن در وسط برقراری ارتباط دو وسیله نقلیه و این حمله را راه اندازی می کند. در این حمله مهاجم تمام ارتباط بین فرستنده و گیرنده را کنترل می کند، اما وسایل نقلیه چنین می پندارند که به طور مستقیم در ارتباط با یکدیگرند. در حمله MiMA [24]مهاجم مکالمه بین وسایل نقلیه را گوش می دهد و پیام نادرست و یا تغییریافته بین وسایل نقلیه تزریق می کند[7].

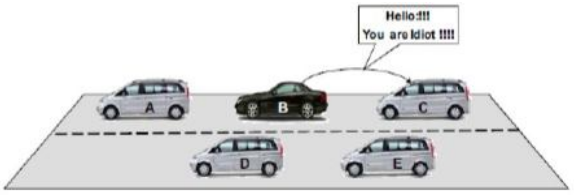
4-2-1-4 حمله تحلیل ترافیک[25]:

تجزیه و تحلیل ترافیک فرآیند رهگیری و بررسی پیام ها به منظور استنتاج اطلاعات ازالگوهای در ارتباط می باشد. این امر حتی زمانی که پیام ها رمزگذاری شده هستند و نمی توانند رمزگشایی شوند نیزمی تواند انجام شود. ترافیک داده ها شامل زمان و مدت ارتباط، شکل دقیق جریان ارتباط، هویت از احزاب برقراری ارتباط و محل آنها است.

این حمله بعنوان یک تهدید جدی در برابر حفظ حریم خصوصی کاربر VANET در نظر گرفته شده است. در این حمله تجزیه و تحلیل بسته ترافیک بین V2V و یا V2RSU است. مهاجم از بسته ی حاوی محل ID [26] خودرو و خط سیرخودرو استفاده می کندکه احتمالا برای استخراج اطلاعات مورد نیازدر رسیدن به هدف مهاجم مفید است[7].

5-2-1-4 حمله اجتماعی[27] :

ایده اولیه این حمله به اشتباه انداختن و مات و مبهوت کردن قربانی با ارسال پیام های غلط وغیر اخلاقی است به طوری که راننده برآشفته و مضطرب می شود. کاربر مشروع پس از دریافت این نوع پیام با ناراحتی واکنش نشان می دهد که هدف اصلی از حمله نیزهمین است. این امر درراندن وسیله نقلیه و به طور غیر مستقیم در شبکه مشکل ایجاد می نماید[7].



شکل 4- حمله اجتماعی درVANET [7]

6-2-1-4 نیروی بی رحم[28]:

اطلاعات مربوط به ایمنی در VANET بسیار مهم است. برای امنیت VANET استفاده مناسب از الگوریتم ها و روش های رمزنگاری به طور گسترده ای برای محافظت در برابر تهدید استفاده می شود. مهاجم می تواند از روش Brute force برای شکستن کلید رمزنگاری استفاده کند[7].

7-2-1-4 اطلاعات ساختگی[29]:

در این حمله مهاجم می تواند متجاوز خارجی و یا کاربر مشروع خودی باشد. مهاجم اطلاعات نادرست در شبکه بین خودرویی پخش می کند تا تصمیمات سایر وسایل نقلیه را با گسترش اطلاعات نادرست در شبکه تحت تاثیر قرار دهد. به عنوان مثال وسیله نقلیه می تواند ظاهرا ترافیک سنگین در یک جاده ایجاد کند تا از انتخاب آن جاده توسط وسایل نقلیه دیگر جلوگیری کند. این حمله نمونه ای ازحمله نرم افزاراست[7].

3-1-4 گروه که تهدیدی برای دسترسی را در برخواهد داشت:

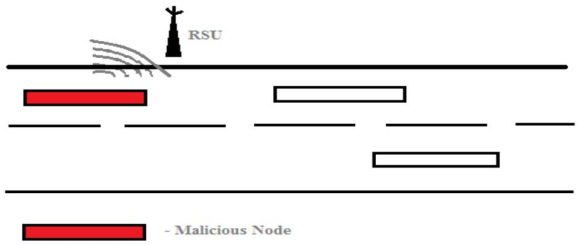
در دسترس بودن یعنی اطمینان از این که سیستم به درستی کار می کند و خدماتی که به کاربران مجاز ارائه شده به هنگام و درزمان مورد نیاز است. دشمن ممکن است با انباشتن کانال، با اخلال در پروتکل مسیریابی، باتخلیه باتری و مواردی از این قبیل مانع خدمات رسانی به گره های معتبرشود، برای مثال خدمات ارائه شده توسط RSU باید هر زمان که مورد نیاز است در دسترس وسایل نقلیه باشد[14].

در دسترس بودن در VANET به معنی دسترسی به هر گونه اطلاعات در هر زمان از ارتباطات است. این التزام امنیت در محیط زمانی متفاوت امری حیاتی است. دسترسی در VANET باید هم در ارتباطات کانال و هم گره های شرکت کننده قابل اطمینان باشد[9]. طبقه بندی این حملات با توجه به هدف آنها به شرح زیر است:

1-3-1-4 انکار سرویس[30]:

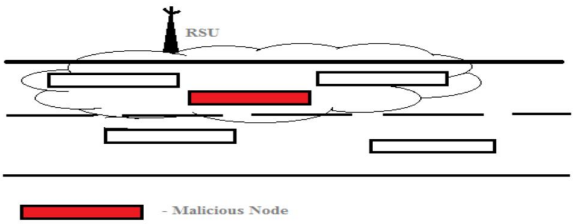
در حمله DoS هدف اصلی جلوگیری از دسترسی کاربر مجازبه خدمات و منابع می باشد. حمله توسط تراکم شبکه و یا سیستم انتقال رخ می دهد به طوری که هیچ وسیله نقلیه نمی تواند به آن دسترسی داشته باشد. این روش به طور کامل ارتباط در شبکه را متوقف می کند که دربرنامه های کاربردی زمان واقعی ویرانگراست. حملات به عنوان مثال عبارتند ازتراکم کانال و تزریق تهاجمی پیام های ساختگی. سه راه مختلف که مهاجم می تواند به آن دست یابد به شرح زیر است[8] :

- در سطح پایه ,مهاجم منبع گره را درهم می شکند به طوری که گره به طور مداوم مشغول می شود قادر به پردازش بیشترنخواهد بود [8]همانطور که در شکل 5 نشان داده شده است.



شکل 5- مهاجم به طور مداوم منبع گره را درهم می شکند[8].

- در سطح گسترده،مهاجم با تولید فرکانس بالا در کانال تراکم ایجاد می کند[8] همانطور که در شکل 6 نشان داده شده است. بنابراین وسیله نقلیه قادر به برقراری ارتباط در شبکه نخواهد بود.



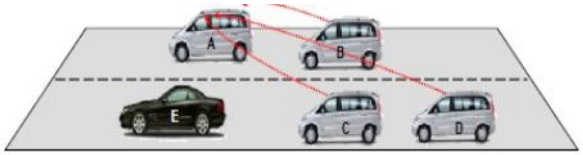
شکل 6- مهاجم با تولید فرکانس بالا در کانال تراکم ایجاد می کند[8].

- سقوط بسته[8].

2-3-1-4 حمله DOS توزیع شده [31]:

حمله DDOS از حمله DOS شدید تر است زیراکه به شکل توزیع شده است. در این حمله مهاجم از مکان های مختلف برای راه اندازی حمله استفاده می کند. آنها ممکن است از شکاف زمان های مختلف برای ارسال پیام استفاده کنند. شکاف زمان و ماهیت این پیام ممکن است از وسیله نقلیه به وسیله نقلیه مهاجمان متفاوت باشد. هدف اصلی این است که شبکه را پایین بکشند به طوری که شبکه برای استفاده در دسترس نخواهد بود. دو احتمال از حملات DDOS عبارتند از[7]:

- وسیله نقلیه به وسیله نقلیه.
- خودرو به زیرساخت.



شکل7- DDOS در وسیله نقلیه به وسیله ارتباطات وسایل نقلیه[7]

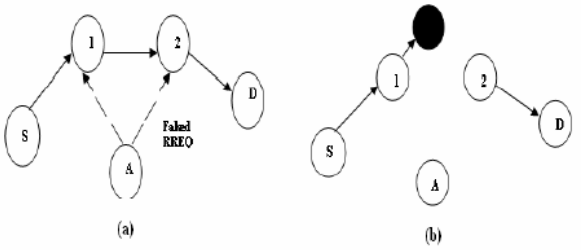
3-3-1-4 هرزه نگاره [32] :

برای مصرف پهنای باند شبکه و افزایش تاخیر انتقال مهاجم در شبکه پیام های spam می فرستد. کنترل این نوع حمله به دلیل فقدان زیرساخت های لازم و مدیریت متمرکز دشوار است. در این حمله انتشار پیام های spam به گروهی از کاربران صورت می گیرد[9]. این پیام ها درست مانند پیام های تبلیغاتی هستند و مورد توجه کاربرقرار نمی گیرند.

4-1-1-4 سیاه چاله[33]:

این نوع حمله به نام Black Hole و Gray Hole نیز در طی سال‌های 2003 تا 2010 مطرح شده و در دو سال اخیر به نقطه اوج خود رسیده است. در این مشکل گره از شرکت در شبکه امتناع می کند و ترافیک شبکه به سمت یک گره خاص هدایت می شود که در واقع وجود ندارد و سبب از دست دادن داده ها می شود[6]. کد مخرب انتخاب می کند که آیا بسته را برای رد خدمات رها کند و یا از جایگاه آن در مسیر به عنوان اولین گام انسان در حین حمله استفاده کند.

در این حمله ، یک نود مهاجم با دریافت بسته مسیریابی RREQ از نود مبداءS ، با اطلاعاتی که از قبل درباره وضعیت شماره توالی[34]و تعداد گام‌های مسیریابی [35] نود مقصد دارد، یک بسته RREP می‌سازد و خودش را به عنوان نود مقصد معرفی می‌کند و این بسته را برای نود مبداء S می‌فرستد. از آنجا که نود S یک بسته RREP زودتر از بسته RREP اصلی (که باید از سوی نود D مقصد ساخته شده و ارسال شود) دریافت می‌کند، جدول مسیریابی خود را به‌روز کرده و با پاک کردن مسیرهای قبلی، نود مهاجم را نود مقصد فرض کرده و شروع به ارسال اطلاعات برای آن می‌کند. نمایی از حمله حفره سیاه را می‌توانید در شکل 8 مشاهده کنید. بنابراین این نوع حملات بسیار خطرناک ارزیابی می‌شوند و در شبکه‌های موردی حساس یا نظامی تهدیدی جدی خواهند بود. مقابله با این حمله بسیار دشوار است چرا که شناسایی نود مهاجم در این وضعیت بسیار سخت است و نیاز به ابزارهای جست‌وجو، احراز هویت و اعتبارسنجی نودها دارد که سربار زیادی برای شبکه ایجاد می‌کند .



شکل8-نمایی از حمله black hole با یک بسته RREP جعلی[6]

5-3-1-4 پخش پیام دستکاری شده:

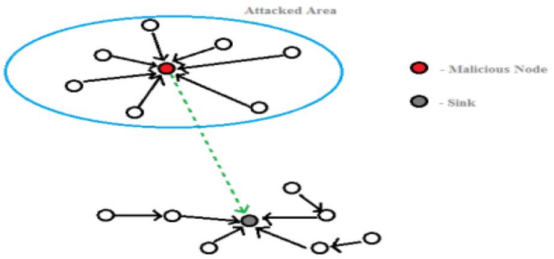
در این نوع از حمله مهاجمان پیام ایمنی کاذب به شبکه ارسال می کنند. این پیام ها گاهی اوقات هشدارها در مورد ترافیک را پنهان می کنند [2,11]. این امر منجر به بحرانی شدن وضعیت مانند حوادث رانندگی و تراکم جاده می شود.

6-3-1-4 رانندگان حریص:

رانندگان حریص کسانی هستند که سعی می کنند برای منفعت خود حمله کنند. این رانندگان باعث ایجاد مشکل اضافه بار برای RSU می شوند.این امر منجر به ایجاد تاخیر در ارائه خدمات به کاربران مجاز می شود. با افزایش تعداد این گونه رانندگان کاربران مجاز با خدمات پایین و کند مواجه می شوند[9].

7-3-1-4 حمله تله ی پولی (مالی)[36]:

در حملات تله ی پولی، تمام ترافیک از یک منطقه خاص از طریق گره مهاجم می گذرد. بنابراین مهاجم روی ترافیک کنترل خواهد داشت و قادر به وقوع بسیاری از حملات دیگر مانند حمل و نقل انتخابی خواهد بود. شکل 9 نشان می دهد گره ی مخرب داده ها را به گره سینک انتقال می دهد. حملات کرم چاله را می تواندبه عنوان زیرمجموعه ای از حملات منجلاب مالی در نظر گرفت طوری که در آن دو گره یک تونل بین خود ایجاد و بسته ها را از طریق آن رو به جلو می برند. این می تواند برای فریفتن گره مفید باشد که سبب عطف توجه گره از یک مسیر بهتر به سوی مقصد شود[8].



شکل9- حمله Sinkhole در شبکهVANET [8]

8-3-1-4 نرم افزارهای مخرب[37] تروجان :

حملات تروجان فقط ویروس ها مانند ویروس ها در VANET ها هستند که مانع عملکرد طبیعی شبکه می شوند. معمولا زمانی که به روز رسانی نرم افزاردر واحدهای VANET یا RSU وجود دارد VANET ها به این ویروس آلوده می شوند مهاجمان معمولا مخرب خودی به جای خارجی می باشند[9].

4-1-4 حمله هایی که باعث تهدید حریم خصوصی می شوند:

پنهان سازی اطلاعات شخصی اشاره با آن داردکه در طول ارتباط هویت ارسال کننده پیام برای دریافت کننده پیام پنهان بماند. با وجود این حفظ هویت ، مرکز بررسی اعتبارسنجی دستگاه ها در شبکه ، ارسال کننده پیام را ردیابی کرده و صحت هویت آن را بررسی می کند.

این نوع از حمله با دسترسی های غیر مجازبه اطلاعات مهم در مورد وسایل نقلیه مربوط می شود. ارتباط مستقیم بین راننده و خودرو وجود دارد. اگر مهاجم به طور غیرقانونی به برخی از داده ها دسترسی داشته باشد حفظ حریم خصوصی راننده به طور مستقیم تحت تاثیر قرار می گیرد[14]. معمولا صاحب وسیله نقلیه راننده ی آن می باشد، بنابراین اگر مهاجم به دنبال هویت مالک باشد سپس به طور غیر مستقیم خودرو حریم خصوصی او را در معرض خطر قرار خواهد داد .این نوع ازحمله به حریم خصوصی آشکارسازی هویت نامیده می شود. ردیابی مکانی نیزبه عنوان یکی از حملات حفظ حریم خصوصی شناخته شده است. دراین حمله محل خودرو یا مسیرپیموده شده توسط وسیله نقلیه در دوره خاصی از زمان است به عنوان اطلاعات شخصی در نظر گرفته می شود[9].

5-1-4 حمله هایی که باعث عدم انکار می شوند:

انکارناپذیری حفاظت در برابر انکار توسط یکی از نهادهای درگیر در ارتباطات که در تمام یا بخشی از ارتباطات شرکت کردندرا فراهم می کند. برای مثال پس از ارسال پیام وسیله نقلیه نباید انکارکند که پیام فرستاده شده است. این است که به نام فرستنده غیر قابل انکارنامیده شده است. همچنین پس از دریافت پیام وسیله نقلیه نباید انکار کند که پیام دریافت کرده است. به این دلیل نام گیرنده غیر قابل انکار را داراست[14].

وقتی دو یا چند کاربر کلید مشابه را به اشتراک می گذارند پس از آن عدم انکار رخ می دهد[14]. با توجه به این، دو کاربر از یکدیگر متمایزنیستند و در نتیجه اقداماتشان می تواند رد داده می شود. ازکلید مشابه در خودرو های مختلف باید با استفاده از ذخیره سازی قابل اطمینان اجتناب شود[9].

6-1-4 حمله به اعتبار داده ها:

اعتبار داده ها می تواند به سادگی توسط محاسبه اطلاعات نادرست و ارسال پیام های آسیب دیده به خطر بیافتد. این امر می تواند توسط دستکاری سنسور در خودرو و یا تغییر اطلاعات ارسالی انجام پذیرد [14]. که این مسئله بر قابلیت اطمینان کل سیستم تاثیر می گذارد. از این رو برخی از مکانیسم ها باید پیشرفت نماید تا در برابر چنین حملاتی به طورعملی درشبکه خودرویی محافظت صورت گیرد[9].

7-1-4 حملات موقعیت:

مکان یابی به موقعیت وسیله نقلیه در یک VANET اشاره دارد. این یکی از با ارزش ترین اطلاعات (مورد استفاده در مسیریابی جغرافیایی) است و اغلب از طریق خدمات موقعیت یابی مانند سیستم موقعیت یابی جهانی (GPS) به آسانی در دسترس است. حملات موقعیتی زمانی رخ می دهد که خط دید رادار مسدود شده است.مهاجم حمله موقعیت را با اصلاح بسته موقعیت،دوباره پخش بسته های موقعیت ساختگی و حذف بسته های موقعیت ضروری راه اندازی می کند[3].

1-7-1-4 تقلب موقعیت وانتشارموقعیت کاذب [38]:

VANET ها دارای شرایط خاص در شرایط تحرک گره و برنامه های کاربردی وابسته به موقعیت می باشند. این شرایط به اندازه کافی توسط پروتکل های مسیریابی جغرافیایی احراز گردیده است. روش مسیریابی جغرافیایی عمدتا بر اساس این اصول می باشد: هر گره موقعیت فعلی خود را با استفاده از سیستم موقعیت یابی مانند GPS ها تعیین می کند. موقعیت بصورت دوره ای در بسته های امواج رادیویی پخش می شود به طوری که هر گره درون محدوده انتقال بی سیم قادر به ساخت یک جدول از گره های همسایه از جمله موقعیت مکانی آنها است. اگر یک گره باید بسته را به جلوببرد hop بعدی را از جدول مجاور با توجه به قاعده از پیش تعریف شده (به عنوان مثال آن رااز گره نزدیک به مقصد) انتخاب می کند. هنگامی که یک گره موضع یابی غلط ارسال میکند پیام های مسیریابی در VANET تحت تاثیر قرار می گیرد. اطلاعات موقعیتی نادرست به دلیل مشکل سخت افزار است و یا عمدا توسط مهاجمان تحریف و محاسبه می شود.نقص گره ممکن است عملکرد سیستم را تا حدی تنزل دهد در حالی که محاسبه داده ها از طریق گره های مخرب اهداف امنیتی اساسی مانند محرمانه بودن، صحت، یکپارچگی و پاسخگویی را نقض می کند[3].

این حمله ها به حملات منفعل، حملات فعال و حملات خودی طبقه بندی می شود[3].

- **حمله منفعل** [39] ترافیک رمز گذاری نشده را نشان می دهد وبدنبال رمزعبورمشخص متن و اطلاعات حساس است که می تواند در انواع دیگرحملات مورد استفاده قرار گیرد. حملات منفعل عبارتند از: تجزیه و تحلیل ترافیک، نظارت بر ارتباطات محافظت نشده، و غیره . حملات منفعل حاصل افشای اطلاعات و یا فایل داده ها به یک مهاجم، بدون رضایت یا آگاهی کاربر است[3].
- در **حمله فعال**[40] مهاجم سعی دردور زدن و یا شکستن سیستم های امنیتی دارد. حملات فعال شامل تلاش برای دور زدن یا شکستن ویژگی های حفاظت، معرفی کدهای مخرب و به سرقت بردن و یا تغییر اطلاعات است. حملات فعال در نتیجه افشا یا انتشار فایل داده ها و اصلاح داده ها می باشد[3].
- **حمله خودی**[41] شامل کسی از داخل سازمان مانند حمله به شبکه و یا کاهش خدمات از طرف یک کارمند ناراضی است[3].

2-4 مهاجمان

1-2-4 راننده ی خودخواه:

ایده ی کلی برای اعتماد در شبکه های میان خودرویی این است که تمام وسایل نقلیه باید در ابتدا مورد اعتماد باشند، این وسایل نقلیه ملزم به پیروی از پروتکل های مشخص شده توسط نرم افزار می باشند، برخی از رانندگان بدون در نظر گرفتن هزینه سیستم سعی در کسب حداکثر سود خود از شبکه با بهره گیری از منابع شبکه به طور غیرقانونی را دارند[13]. راننده خودخواه می تواند به سایر وسایل نقلیه بگوید که ازدحام در جاده وجود دارد به طوری که آنها باید مسیر جایگزین را انتخاب کنند بنابراین راه برای او خلوت خواهد شد[5].

2-2-4 حمله های مخرب:

این نوع مهاجم سعی می کند از طریق برنامه های موجود در شبکه بین خودرویی سبب آسیب گردد. در بسیاری از موارد این مهاجمان اهداف خاصی داشته و به منابع شبکه نیز دسترسی خواهند داشت[3,13]. شبکه به عنوان مثال یک تروریست می تواند اخطار کاهش سرعت صدور نماید تا درجاده قبل از انفجار بمب ازدحام ایجاد کند[5].

3-2-4 افراد وقیح[42]:

شامل افرادی است که بدنبال حادثه اند و یا هکرهایی که در پی رسیدن به شهرت از طریق آسیب رسانی هستند[5,13]. به عنوان مثال فردی که شوخی زننده می کند، می تواند یک وسیله نقلیه را متقاعد کند که سرعتش را کاهش دهد و به وسیله نقلیه پشت سرآن بگوید سرعتش را افزایش دهد[4].

5- نتیجه گیری

در این مقاله حملات مختلف در VANET با توجه به در دسترس بودن، احراز هویت، محرمانه بودن، حفظ حریم خصوصی، عدم انکار، اعتماد داده ها و حملات موقعیت طبقه بندی شده اند. چنین به نظر می آید که این دسته بندی ها به مقابله با انواع مختلف حمله به پروتکل های مسیریابی در VANET کمک می کند. از آنجا که حمله وضعیت وخیم تری ایجاد می کند تجزیه و تحلیل اثر حمله به پروتکل های مسیریابی ضرورت می یابد تا فضای امن تر خودرویی ایجاد گردد.

مراجع

[1]Charles H., Festag A., and Papadimitratos P., "*Secure position-based routing for VANETs*.", IEEE Conference on Vehicular Technology, pp. 26-30, 2007.
[2]Krishnamurthi, Niyant, Ganguli A., Tiwari A., Shen B.H., Yadegar.J, and Hadynski.G, "*Topology control for future airborne networks*", IEEE Conference in Military Communications, pp. 1-7, 2009.

www.NoavaranGermi.ir
سایت نوآوران گرمی - همیار دانشجو

[3]Raya M., Papadimitratos P., Hubaux J.P., "*Securing Vehicular Communications*", IEEE Wireless Communications, Vol.13, 2006.
[4]Sumra, I.A. Hasbullah, H.; Manan, J.A. , "*VANET security research and development ecosystem*", National Postgraduate Conference (NPC), pp.1-4, 2011.
[5]Samara G., Al-Salihy W.A.H., Sures R. , "*Security Analysis of Vehicular Ad Hoc Networks (VANET)* ", Second International Conference on Network Applications Protocols and Services, pp.55-60, 2010.
[6]Sharma, Sheenu, Roopam Gupta M., "*Simulation Study Of Black hole Attack in the Mobile Ad hoc Networks* ", Journal of Engineering Science and Technology, Vol. 4, No. 2, pp. 243 - 250, 2008.
[7]Rawat A., Sharma S., Sushil R., "*VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS*", Journal of Information and Operations Management, ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-301-304, 2012,Available online at http://www.bioinfo.in/contents.php?id=55.
[8]Mathew M.E. and Raj Kumar A., "*Threat Analysis and Defense Mechanisms in VANET*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, 2013, Available online at: www.ijarcsse.com.
[9]Dhamgaye A., Chavhan N., "*Survey on security challenges in VANET*", IJCSN International Journal of Computer Science and Network, ISSN (Online): 2277-5420, Vol. 2, Issue 1, 2013.
[10]Panigrahi, Kumar S., Chakraborty S., and Mishra J., "*A Statistical Analysis of Bubble Sort in terms of Serial and Parallel Computation*"International Journal of Computer Science and Network (IJCSN), Volume 1, Issue 1, 2012.
[11]Saini, Akanksha and Kumar H., "*Comparison between Various Black Hole Detection Techniques in MANET*", National Conference on Computational Instrumentation , pp. 157-161, 2010.
[12]Douceur J.," the Sybil Attack", First International Workshop on Peer-to-Peer Systems, 1st ed, USA, Springer, 2003.
[13]Parno, Bryan, and Perrig A., "*Challenges in securing vehicular networks*", Workshop on Hot Topics in Networks, pp. 1-6, 2005.
[14]Fuentes J . M., González-Tablas A. E. and Ribagorda A., "*Overview of security issues in Vehicular Ad-hoc Networks.*", 2010.
[15]Zeadally, Sherali, Hunt R., Chen Y.S., Irwin A., and Hassan A., "*Vehicular ad hoc networks (VANETs): status, results, and challenges*", Telecommunication Systems, PP. 1-25, 2010.
[16] http://www.who.int/features/2004/road_safety/en/.

زیرنویس‌ها

[1] VANET
[2] IVC
[3] RVC
[4] MANETs
[5] RSU
[66] Confidentiality
[7] Privacy
[8] Authentication
[9] Integration
[10] Availability
[11] Non-Repudiation
[12] Masquerading
[13] Node Impersonation attack
[14] Message suppression
[15] Alteration
[16] Replay
[17] GPS spoofing
[18] Tunneling
[19] ID Disclosure
[20] Timing Attack
[21] Home attack
[22] ECU
[23] Man in the middle attack
[24] Man in the middle attack
[25] Traffic analysis
[26] شماره شناسایی خودرو
[27] Social attack
[28] Brute force
[29] Bogus information
[30] DoS
[31] DDoS
[32] spamming
[33] black hole
[34] Sequence Number
[35] Hop Count
[36] Sinkhole Attack
[37] malware
[38] *Position cheating and false position disseminating*
[39] passive attacks
[40] active attacks
[41] insider attacks
[42] Pranksters