بررسی آدرس تکراری بین لایه ای توزیع شده برای ارتباطات بحرانی و ایمن VANET

چکیده

شبکه‌های بین خودرویی، به دنبال استقرار انبوه در سالهای آینده هستند. این نوع شبکه های ادهاک متحرک اختصاصی در زمینه خودرو، تمایل بالایی به افزایش ایمنی رانندگی دارند. ما فهمیدیم که رویکردهای قبلی برای ردیابی آدرس تکراری در چنین شبکه هایی، موارد کاربردی مهم را تحت پوشش قرار نمی دهند. پهنای باند کم و شعاع ارتباطی محدود، همراه با تحرک گره، به کاهش داده های متا، همچون جداول مسیریابی منجر می شوند. این گفته، بویژه برای تبادل پیام بحرانی ایمن و مبتنی بر IP، با استفاده از پروتکل های تخصیصی VANET صدق می کند. با این حال، مکانیسم های بررسی آدرس تکراری، بر چنین داده های متا تکیه می کنند. ما نشان می‌دهیم که این می تواند به عدم شناسایی آدرس تکراری برای ETSI ITS و WAVE در موارد کاربرد بحرانی و ایمن منجر شود. علت این مسئله، نوع دیگری از مسئله پنهان معروف می باشد. برای غلبه بر این ضعف، طرح شناسایی آدرس تکراری بین لایه ای را، همراه با تغییر آدرس فعال، جهت حل تکرارها پیشنهاد می دهیم. ارزیابی در محیط شبیه سازی، عملی بودن رویکرد را نشان می دهد.

کلمات کلیدی: تشخیص آدرس تکراری، وضوح آدرس تکراری، وانت

1. مقدمه

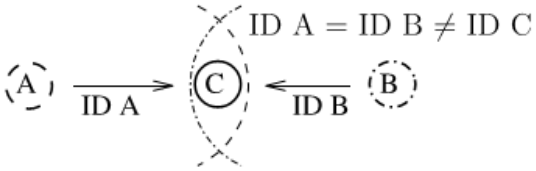
شبکه های ادهاک متحرک MANETs، موضوع مهم تحقیقی و عملی می باشند. شبکه‌های بین خودرویی VANET، زیرمجموعه مهمی از MANETs می باشند که گسترش انبوه آنها، در سالهای آینده پیش بینی شده است. استانداردسازی VANET، در محدوده چارچوب های دسترسی بی‌سیم US در محیط های وسیله نقلیه WAVE و سیستم های حمل و نقل هوشمند ITS ETSI اجرا می شود. سیستم امنیتی دقیق برای VANETها لازم است که ناشی از تبادل داده بیسیم و موارد کاربرد بحرانی و ایمن می باشد.

ارتباط بحرانی و ایمن در VANET معمولا نامشخص است، یعنی هر پیامی باید در جای خود استفاده شود. پروتکل های ارتباطی اختصاصی، برای این نوع تبادل داده استفاده می شوند. شرایط آنها، ناشی از مقاومت در

برابر از دست دادن داده ها، شرکت کنندگان بسیار متحرک و الزامات فوری موارد استفاده است. بنابراین، هر پیام بصورت دیجیتالی امضاء می شود تا یکپارچگی و صحت آن تضمین شود. پارامترهای رمزنگاری لازم، در بسته امنیتی قرار دارند که ظرفیت پیام را در سطح لایه شبکه تعبیه می کند. این بسته، پارامترهای پیام (برای مثال امضاء) و پارامترهای گره (برای مثال کلید عمومی) را نگه می دارد که در گواهیها بسته بندی می شوند. این گواهیها بصورت پراکنده بر پیام هایی سوار می شوند تا میانگین اندازه پیام را کاهش دهند.

آشکارسازی آدرس تکراری DAD، مسئله معروفی در پروتکل های ارتباطی است. این اشکارسازی، ناشی از انتخاب مستقل آدرس‌ها در گره ها است که در VANETها استفاده می شود. اقدامات متقابل، معمولا بر داده های متا همچون جداول مسیریابی تکیه دارند که در پروتکل های VANET وجود ندارند، همانند سیستم WAVE بدون حمایت از ارتباط چندهاپی. ما در می یابیم که این وضعیت به نوعی مسئله ایستگاه پنهان منجر می شود که در لایه های پروتکل متعدد روی می دهد. پروتکل های پشته VANET از شناسه های گره (یعنی آدرس) در چندین لایه پروتکل استفاده می کنند. بنابراین، DAD را باید در تمام این لایه ها اجرا کرد. با این حال، این کار توسط استانداردهای موجود صورت نمی گیرد. تنها لایه شبکه ETSI ITS از DAD استفاده می کند اما مکانیسم اعمالی، تنها موردی را پوشش می دهد که گره، باعث تکرار می شود. تعریف دقیق مسئله در بخش 2 ارائه شده است.

نیاز به DAD با توجه به IDهای گواهی، خاص VANETها می باشد. پهنای باند ارتباطی کم و تعداد بالای گره های متحرک، نیازمند توزیع گواهی پرواز در میان گره ها می باشد. این کار با سوار کردن گواهی ها روی پیام های بیکن انجام می شود. توزیع گواهی پیشین، به علت تعداد بالای گره ها و تغییرات گواهی توسط هر گره ناشی از شرایط حریم خصوصی، غیرعملی است. برای محدود کردن بار کانال، اغلب پیام ها گواهی امضاکننده خود را حمل نمی کنند بلکه ID آن را انتقال می دهند. چنین ID معمولا با استفاده از تابع هش روی گواهی تعیین می شود. برای محدودتر کردن اندازه پیام، IDها از نظر طولی محدود می شوند برای مثال، برای WAVE و ETSI ITS به هشت بیت. این نیز به خطر ID گواهی تکراری در محدوده ارتباطی گره، بویژه در سناریوهای دارای چگالی گرهی بالا منجر می شود.



تصویر 1. مسئله ایستگاه پنهان اعمالی به آدرس های تکراری. گره C پیام را از A دریافت کرده و B آدرس را به اشتراک می گذارد. A و C نمی توانند مستقیما از حضور همدیگر یادبگیرند.

ادامه مقاله بشرح زیر است. بخش 2، بیان مسئله را مطرح می کند. مروری بر آثار مرتبط، در بخش 3 ارائه می شود. بخش 4 به توصیف تاثیر آدرس های تکراری بر کاربرد لایه های مختلف پروتکل VANET و مکانیسم های شناسایی چنین تکرارهایی می پردازد. طرح غیرمتمرکز DAD سریع و راه حل تکراری نیزامند سربار کم، در بخش 5 ارائه شده است. بعلاوه، ارزیابی مکانیسم معرفی شده نیز ارائه گردیده است. در نهایت، بخش 6، به نتیجه گیری و موضوعات اثر آینده می پردازد.

2. بیان مسئله

DAD به وسیله مقایسه آدرس پروتکل پیام دریافتی با آدرس متناظر گره گیرنده اجرا می شود. در موردی که تکرار دیده می شود، الگوریتم راه حل تکراری اعمال می شود. این را DAD داخلی می نامند. آشکارسازی آن، مستقیم بوده و راه حل آن با برداشتن آدرس جدید و تصادفی توسط آشکارساز ارائه می شود. این مکانیسم، معمولا در شبکه های ارتباطی نقطه به نقطه اعمال می شود.

تاثیر دیگر تکرار آدرس، در VANETها و با استفاده از مکانیسم های پخش برای توزیع اطلاعات روی می دهد. در چنین شبکه هایی، گره ها از مسئله ایستگاه پنهان و از دست دادن دانش یا دانش ناقص درباره شبکه کامل هر گره رنج می برد. بنابراین، گره ها احتمالا از تکرار آدرس ناشی از خودشان اگاه نباشند. با این حال، گیرنده های پیام از چندین گره دیگر با استفاده از آدرس تکراری، احتمالا از آنها رنج ببرند. بنابراین، گیرنده ها باید به شناسایی چنین تکرارهایی در فرایندی بپردازند که ما DAD خارجی می نامیم. سناریوی مربوط به مسئله ایستگاه پنهان و تکرار آدرس در تصویر 1 ارائه شده است.

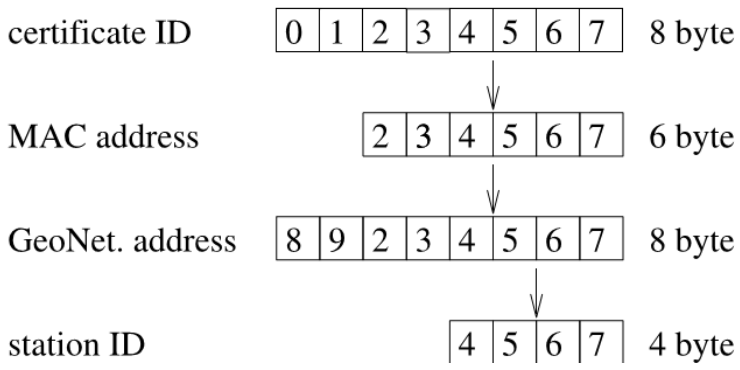
نیاز به تضمین منحصربفرد بودن شناسه های استفاده شده در پروتکل ارتباطی VANET، در [7] ذکر شده است اما هیچ روشی برای تضمین این ویژگی ارائه نشده است. بعلاوه، DAD درونی، برای لایه شبکه ETSI ITS [8] و [9] استانداردسازی شده است که بدنبال مکانیسم مشابه اعمالی برای شناسه گره لایه تاسیسات است. از نظر محقق، DAD برای لایه های پروتکل باقیمانده بررسی نشده است. بعلاوه، نیاز به DAD خارجی در VANETها تا کنون شناسایی نشده است. بنابراین، در اثر قبلی به این موضوع پرداخته نشده است.

برای اجرای DAD خارجی، یک گره به بررسی آدرسها در پیام دریافتی برای تساوی چنین آدرسهایی در پیام های قبلی می پردازد. در مقایسه با DAD داخلی، گره آشکارساز مستقیما قادر به حل تکرار خود نیست. باید چنین راه حلی را از حداقل یک گرهی درخواست کند که باعث تکرار می شود. چنین درخواست تغییر آدرس، برای دامنه VANET پیشنهادنشده است.

ما به بررسی تاثیر تکرار آدرس خارجی بر VANETها در مثلای از رویکردهایETSI ITS and WAVE در بخش 4 می پردازیم. DAD خارجی و موثر لایه متقاطع، و راه حل آدرس تکراری در بخش 5 مورد بحث قرارگرفته اند.

3. آثار مرتبط

تحقیق برای DAD غیرمتمرکز در MANETها، در شبکه های مبتنی بر IP یا دیگر پروتکل های کشف توپولوژی شبکه فعال در لایه شبکه مدنظر بوده است.



تصویر 2. مثالی از استخراج آدرس های متفاوت در لایه های متعدد نام مستعار ایستگاه (ID گواهی)

با این حال، بسیاری از پروتکل های VANET برای ارتباط ادهاک بحرانی، مبتنی بر IP نیستند. بنابراین، هیچ تبادل متاداده برای کشف توپولوژی شبکه اجرا نشده است. بعلاوه، طرح DAD منفعل معروف [6]، در حالت منفعل کار نمی کند. به جای آن، بر تبادل متاداده فعال ناشی از دیگر عملکردها تکیه دارد. این طرح از این اطلاعات، به جای انتقال مجموعه داده های رویکردهای دیگر استفاده مجدد می نماید که معمولا طرح DAD فعال نامیده می شوند.

در رویکرد منفعل DAD، گیرنده به مقایسه آدرسهای بسته های دریافتی با آدرسهای خود می پردازد. این رویکرد در ETSI ITS در لایه شبکه استفاده می شود. در مورد آدرس تکراری شناسایی شده، آشکارساز به تغییر ID لایه شبکه خود می پردازد. بسط این طرح به ID گره لایه تاسیسات، در [9] پیشنهاد شده است.

طرح جلوگیری از گواهی های تکراری در VANETها، با بررسی هماهنگ مسئولین گواهی، در [15] بررسی شده است. با این حال، این رویکرد نمی تواند از مسئله تکرار ID گواهی اجتناب کند. بنابراین، این رویکرد نیازمند بسط به سوی بررسی تمام آدرسهای استخراجی از تمام گواهی ها خواهد بود. تعداد بالای گواهی ها، به تلاش زیاد برای اجرای تمام بررسیهای متقاطع منجر خواهد شد. این کار نیز، تلاش لازم برای اجرای اعتبار گواهی را افزایش خواهد داد. بنابراین، چنین رویکردهایی در ادامه بررسی نمی شوند.

آدرسهای لایه های مختلف پروتکل درVANET معمولا جفت می شوند. این وضعیت ناشی از نیاز به ارتباط طول عمر آدرس لایه های دیگر به یکی از نام مستعارهای فعلی جهت اجتناب از ردیابی گره است (یعنی ID گواهی).

مثالی از جفت آدرس (یا ID)، در تصویر 2 ، همراه با واژه های ETSI ITS ارائه شده است. روش استخراجی آدرسها از نام مستعار، محدود به استانداردها نیست. با این حال، نیازی به استفاده از رویکرد دیگر به جای کوتاه سازی دیده نشده است. به خاطر جفت شدگی آدرس ها، تغییر هر آدرس را می توان با اجرای تغییر نام مستعار اجرا کرد.

4. تاثیر و آشکارسازی تکرار آدرس

خطر تصادم آدرس ها، همراه با کاهش دامنه آدرسها و افزایش تعداد گره ها، زیاد می شود. ما از معماری پروتکل WAVE/ ETSI ITS برای بحث درباره تاثیر آدرسهای تکراری در پیامهای دریافتی مربوط به لایه های پروتکل مختلف، استفاده می کنیم. امکان کشف تکرار خارجی نیز بررسی شده است.

4.1 ID گواهی

برای تکرار ID گواهی، دو مورد را باید مجزا ساخت. در مورد اول، پیام حاوی تنها یک ID گواهی امضاکننده دریافت می شود و گواهی صحیح فرستنده برای گیرنده شناخته شده نیست. بنابراین، گیرنده بدنبال گواهیهای ذخیره شده و متناظر با /ID گواهی دریافتی می پردازد تا پارامترهای رمزنگاری لازم برای تایید پیام را بدست آورد. به خاطر تکرار ID، به نظر موفق می رسد. با این حال، تایید پیام با شکست مواجه خواهد شد. بنابراین، پیام حذف می شود. این مسئله منبع دیگر از دست دادن بسته رمزنگاری است که در اثر قبلی بررسی نشده است. گیرنده نمی تواند تعیین کند که آیا پیام توسط حمله دستکاری شده است یا ID گواهی تکراری وجود دارد.

بعلاوه، بعد از حذف پیام، گیرنده آن نیاز به تصمیم گیری درباره پیشروی از جهت مکانیسم توزیع گواهی دارد. گیرنده بدبین با فرض حمله، پیام راحذف می کند. در مقابل، گیرنده خوش بین، تنها تصادمی را در ID گواهی فرض می کند. بنابراین، بعد از آشکارسازی همسایه جدید، پیش می رود. بعد از آن، زمان دریافت گواهی لازم به حداقل می رسد. بنابراین، استفاده از این روش خوش بین را توصیه می کنیم .

مهاجم هیچ مزیتی را از کاربرد رویکرد خوش بین دریافت نمی کند. او می تواند از آن، برای انتشار گواهی گیرنده سوء استفاده کند اما این کار را به روش های دیگر نیز می توان انجام داد. تنها ارسال پیام با ID گره جدید، جهت تحریک آشکارسازی همسایه جدید ضروری است که در [17] مطرح شده است. بنابراین، قابلیت های مهاجم، با روش پیشنهادی توسعه نمی یابند. بعد از دریافت گواهی نامعلوم قبلی، گواهی بصورت زیر پیش می رود.

مورد دوم، دریافت پیام با گواهی کامل است. جزئیات رسیدگی به پیام، مخصوص پیاده سازی هستند. توالی همچون مورد زیر استفاده می شود. ابتدا، ID گواهی تعیین می شود. ID برای بررسی این مسئله استفاده می شود که آیا گواهی قبلا شناسایی شده و تایید شده است یا نه. این کار به خاطر آدرس تکراری پیش خواهد رفت. سپس، گیرنده همانند مورد اول پیش می رود.

بعد از شکست تایید، گیرنده باید مقایسه دقیق تری از گواهی دریافتی و گواهی ذخیره شده قبلی انجام دهد بایت با بایت. به واسطه آن، اینها با احتمال بسیار بالا، متفاوت خواهند بود. بنابراین، تکرار ID گواهی را می توان شناسایی کرد. بنابراین، پیام حاوی گواهی که باعث تکرار ID گواهی می شود، با روش تایید حذف نمی شود.

بدون مکانیسم جایگزین بعد از عدم تایید پیام، پیام های گرهی که باعث تکرار ID می شوند، همیشه حذف خواهند شد حتی در موردی که گواهی و امضای معتبری با خود داشته باشند. بنابراین، گیرنده هرگز به آگاهی درباره فرستنده نخواهد رسید که این نیز، قابلیت کاربردهای متکی بر داده ها را محدود می سازد.

این یافته ها نشان می دهند که نهاد امنیتی می تواند به بررسی وجود تکرار ID گواهی بپردازد. با این حال، آدرسهای لایه های دیگر از IDهای گواهی استخراج شده و چنین لایه هایی نمی توانند آنها را حل کنند.

4.2 آدرس لایه کنترل دسترسی به واسط MAC

بسیاری از روشهای لایه MAC ویژه VANET می باشند، همچون 802.11p and ITS-G5 که فقط از ACKهای لایه MAC در حالت تک پخش استفاده می کنند، اما در حالت انتشار استفاده نمی کند. بنابراین، آدرس MAC تکراری، با ارتباط پخش تداخل نخواهد داشت. در حالت تک پخش، به پذیرش و تایید پیام گره هایی منجر خواهد شد که توسط فرستنده خود رسیدگی نشده اند. بنابراین، فرستنده به نادرستی فرض می کند که پیام وی دریافت شده است.

ACKهای سطحی و ساختگی نباید تاثیر معنی داری بر امنیت ارتباطی VANETها داشته باشند. با این حال، کاهش اطمینان به دریافت صحیح پیام ارسالی، بر جنبه های ایمنی تاثیرگذار خواهد بود.

آدرس MAC اغلب بعنوان بخشی از آدرس لایه شبکه در پشته های پروتکل استفاده می شود. بنابراین، آدرس MAC تکراری، به احتمال زیاد به آدرس لایه شبکه تکراری منجر خواهد شد. برای مثال، در ETSI ITS، آدرس لایه شبکه متشکل از آدرس MAC بوده و بقیه موارد، طبق خصوصیات گره پایدار پر می شوند که برای گره های مختلف، یکسان می باشند (بخش 4.3).

لایه MAC، بدون تجزیه محتوای لایه بالایی، هیچ گزینه ای برای آشکارسازی آدرسهای تکراری خارجی نخواهد داشت که بنابراین، برای حفظ جدایی لایه ها، مایوس می شود.

4.3 آدرس لایه شبکه

آدرس های لایه شبکه، معمولا برای مسیریابی بسته استفاده می شوند. VANETها بدون حمایت از ارتباط چند هاپی، برای مثال WAVE، استفاده بسیاری محدودی از این آدرس می کنند. ETSI ITS از آن برای آشکارسازی بسته تکراری DPD و شماره توالی و ارسال مهر زمان استفاده می کند.

برای حذف بسته های تاریخ گذشته/ تکراری، شماره توالی بالاترین پیام و آخرین مهر زمانی ارسالی، برای هر همتای ارتباطی شناخته شده ذخیره می شود. در موردی که مقدار کوچکتر پیدا شد، بسته حذف می شود. بنابراین، در مورد آدرس لایه شبکه ای که بصورت خارجی تکرار شده است، پیام گره، با استفاده از مهر زمان پایین تر، حذف می شود. در مورد مهر زمان ارسال برابر، پیام گرهی که از شماره توالی پایین تر استفاده می کند، حذف می شود. برای جزئیات بیشتر به [8] مراجعه نمایید.

حذف پیام ها به از دست دادن منبع داده دیگر منجر می شود که تا کنون در VANETها شناسایی نشده است. در مورد ETSI ITS، آدرس GeoNetworking معروف لایه شبکه، طولانی تر از آدرس MAC است. با این حال، بخشی که آدرس MAC را طویل تر می سازد، برای اغلب ایستگاه ها مشابه است، چون از خصوصیات ایستگاه استاتیک مشتق شده است (زمینه های دارای برچسب 8 و 9 تصویر 2). بنابراین، احتمال تصادف برای آدرس GeoNetworking تقریبا مشابه با آدرس MAC است.

لایه شبکه نمی تواند بسته های تاریخ گذشته/ تکراری را از آدرسهای تکراری خارجی مجزا سازد. بعلاوه، ETSI DAD ITS داخلی را با بررسی کیفیت شبکه و آدرس های لایه MAC اعمال می کند. این کار از DAD نادرست برای ارتباط پخش چند هاپ جلوگیری می کند، که در طول این ارتباط، فرستنده بسته خود را از گره فوروارد کننده (ارسال رو به جلو) دریافت می کند. با این حال، این کار، DAD اعمالی را به همسایه تک هاپ محدود می کند.

4.4 آدرس ایستگاه

به هر گره در کاربردهای VANET، معمولا یک ID (یعنی آدرس) تعیین می شود که بخشی از پیام کاربردهاست. برای مثال، بیکن های ETSI ITS and WAVE از ID ایستگاه برای ردیابی محلی وسایل نقلیه استفاده می کنند. این یک ID منحصربفرد است. همانند WAVE، هیچ مکانیسم حل یا آشکارسازی تکراری برای آن پیشنهاد نشده است. DADداخلی برای ID ایستگاه لایه تاسیسات ETSI ITS، در [9] پیشنهاد شده است.

کاربردهای VANET نیازمند تشخیص گره های دیگر هستند، برای مثال، تا اینکه ردیابی شیء برای جلوگیری از تصادفی را امکان پذیر سازند. فرض بر این است که چنین الگوریتم هایی، با IDهای گره تکراری، اشتباه

خواهند شد. برای مثال، برخی پیام ها را به این علت که غیرمحتمل می شوند، می توان حذف کرد. با این کار، موقعیت های خطرناک نادیده گرفته شده یا احتمالا هشدار اشتباهی ارسال شود. این مسئله برای موارد استفاده بحرانی و ایمن از VANETها، بسیار مهم است.

5. بررسی آدرس تکراری

برای تحقق DAD معتبر در VANET با آدرس های جفت در لایه های مختلف (تصویر 2)، مکانیسم آشکارسازی متقاطع در بخش 5.1 پیشنهاد شده است. وقتیکه تکرار آدرسی شناسایی شد، الگوریتم بخش 5.2 را می توان برای حل آن بکار برد. عملی بودن مکانیسم های پیشنهادی در VANETها، در بخش 5.3 آمده است.

5.1 آشکارسازی آدرس تکراری لایه متقاطع

همانگونه که در بخش 4 مطرح شد، بسیاری از لایه های پروتکل، نمی توانند تکرار آدرس خارجی را بطول کلی شناسایی کنند. با این حال، نهاد امنیتی می تواند این کار را با احتمال بالا انجام دهد. خوشبختانه، قبل از اینکه پیامها به مکانیسم های لایه شبکه اصلی و لایه های بالاتر (پشته پروتکل WAVE or ETSI ITS) تحویل داده شوند، نهاد امنیتی به پیامها رسیدگی می کند. بنابراین، نهاد امنیتی باید DAD را براساس گواهی های دریافتی و IDهای گواهی های آنها اجرا کند. چنین DAD هایی شامل بررسی تکرار آدرسهای سطح بالاتر تحویلی از ID گواهی می باشند.

کاربردهایی که از تبادل پیام غیراستاندارد با شناسه های گره استفاده می کنند، باید خود تکرارها را مدنظر داشته باشند. با این حال، استخراج ID از یکی از موارد استاندارد، بدون کوتاه کردن، بایدذخیره شود.

به خاطر معماری پروتکل ارائه شده، تصادم آدرس های MAC را می توان بعد از بررسی بسته توسط لایه MAC، آشکارسازی کرد. بنابراین، همانگونه که در بخش 4.2 گفته شد، با رویکرد ارائه شده نمی توان از ارسال ACK لایه AMC اجتناب کرد. برای انجام این کار، می توان ارسال چنین ACKهایی را به تاخیر انداخت تا زمانیکه DAD توسط لایه های بالاتر اجرا شود. با این حال، به خاطر شرایط زمانبندی سخت برای ارسال ACKهای لایه MAC، تحقیق این کار مشکل است.

5.2 حل آدرس تکراری

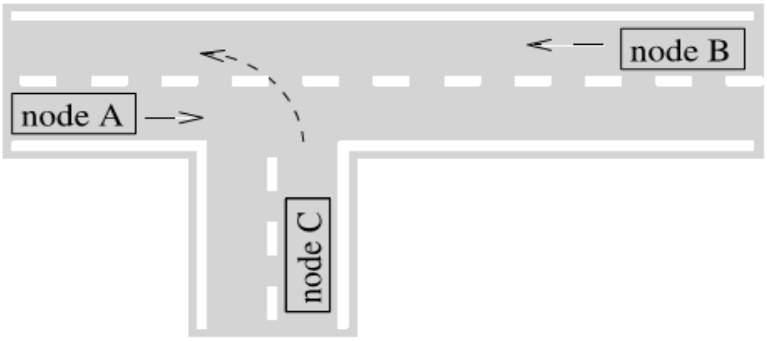
دو روش راه حل آدرس تکراری لایه متقاطع در چندین لایه را می توان در نظر داشت. یکی از روشها، پایین نگه داشتن تغییر آدرس ایستگاه است، برای مثال تنها با تغییر آدرس لایه شبکه یا تغییر تمام شناسه ها. روش دیگر، با مکانیسم تغییر نام مستعار در VANETهای موجود اجرا می شود. بنابراین، این روش را براساس مکانیسم های موجودی که استفاده می کند، توصیه می کنیم.

تغییرات آدرس در لایه های اختصاصی، رابطه ثابت بین آدرس لایه های مختلف را می شکند. برای مثال، لایه شبکه در ETSI ITS نیازمند تعیین آدرس GeoNetworking هدف تک پخش از ID ایستگاه است چون لایه تسهیلاتی که ارسال پیام را تحریک می کند، ID ایستگاه هدف را ارائه می دهد. وابستگی مشابه در نهاد امنیتی قرار دارد؛ مجبور است تا آدرسهای GeoNetworking گره های هدف را به گواهیهای آنها نگاشت کند و رمزنگاری پیام را امکان پذیر سازد. بنابراین، تغییر آدرس در یک لایه، باعث ایجاد مجموعه های پیچیده اپدیت ها در لایه های دیگر شود. از این جفت لایه های نزدیک و اضافی باید اجتناب کرد.

برای حل تکرار آدرس، حداقل یک گره باید تغییر نام مستعار را اجرا کند. بنابراین، حل آدرس تکراری، نیاز به منبع اضافی تغییر نام مستعار را باعث می شود که به حفظ حریم خصوصی مربوط نیست. نهاد امنیتی در ETSI ITS، رابط درخواست تغییر نام مستعار را ارائه می دهد. با این حال، کاربرد آن تا کنون تعریف نشده است.

برای حل آدرس تکراری، بعد از DAD داخلی، آشکارساز می تواند تغییر نام مستعار را تحریک کند. با این حال، زمانیکه DAD خارجی، تکرار آدرس را یافت، آشکارساز نیازمند تحریک گره دیگر برای انجام این کار است. تا کنون چنین مکانیسمی شناسایی نشده است. با افزودن زمینه هیدر به پاکت امنیت، این کار تحقق می یابد. چنین زمینه هیدر، نیازمند 9 بیت ETSI ITS و WAVE است. بنابراین، محتوای مازاد، در مقایسه با حداقل اندازه پاکت 93 بایت، کوچک است.

بعلاوه، زمینه هیدر تنها در صورت نیاز مدر نظر است. بنابراین، حداقل اندازه پاکت امنیت، توسط روش افزایش نمی یابد. برای کسب اطلاعات درباره اینکه این اندازه را تا حد ممکن کوچک نگه داریم، به [16] مراجعه نمایید. سوارکردن درخواست بر بیکن ها، در پیام های اختصاصی را ترجیح می دهیم. با این کار، می توان از سربار و پیچیدگی ناشی از پیام اضافی اجتناب کرد.



تصویر 3. طرح جاده ای که تقاطع T را نشان می دهد.

در موردی که گیرنده، ID گواهی خود را در زمینه هیدر اضافی پیشنهادی می یابد، نام مستعار خود را فورا تغییر می دهد. برای اجتناب از سوء استفاده از این ویژگی، درخواست را باید در صورت تایید پیام درخواست کننده، پذیرفت. این بدین معنی می باشد که درخواست تغییر نام مستعار از گره هایی که گواهی (زنجیره) آنها نامعلوم است، حذف می شوند.

تغییرات نام مستعار، به سربار قابل توجه در لایه های مختلف منجر می شود. بنابراین، میزان آنها را باید به حداقل رساند. بنابراین، آشکارساز تکرار آدرس خارجی، سعی در درخواست تنها یک تغییر نام مستعار است. با این حال، در مورد تکرار ID گواهی، با استفاده از مکانیسم توصیفی بالا، این کار ممکن نیست. باید کل گواهی را مدنظر گرفا یا ID گواهی مورد نظر را با احتمال تکرار پایین تعریف کرد تا این کار عمل شود. با این حال، توصیه نمی شود چون اندازه بدترین مورد پاکت امنیت را افزایش می دهد که باید از آن جلوگیری کرد.

5.3 ارزیابی

برای ارزیابی روشهای توصیفی در بخشهای 5.1 و 5.2، این روشها در محیط شبیه سازی چارچوب ezCar2X اجرا شدند که شبیه ETSI ITS مبتنی بر VANET است. این چارچوب، شبیه ساز جریان ترافیک SUMO، شبیه ساز شبکه ns-3 و پشته پروتکل سازگار ETSI ITS از ezCar2X را ترکیب می کند. SUMO and ns-3 از طریق رابط TraCI جفت می شوند تا محیط شبیه سازی رویداد گسسته را بدست آورند. حرکت گره، با SUMO شبیه سازی می شود در حالیکه ارتباط در لایه فیزیکی و MAC با ns-3 شبیه سازی می شود. پشته پروتکل ETSI ITS در هر گره و درون ns-3 نصب می شود.

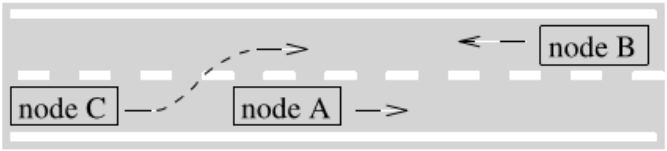
هر سناریوی ترافیک تست شده، با پشته پروتکل ETSI ITS اصلی و بدون مکانیسم های آشکارسازی آدرس تکراری پیشنهادی و با نسخه ارتقاء یافته پشته پروتکلی اجرا شد که روشهای بخشهای 5.1 و 5.2 را اجرا می کند. وسایل نقلیه اختصاصی با مجموعه آدرسهای یکسان در لایه های مختلف، در شبیه سازیها درج شدند.

اولین سناریوی ترافیکی استفاده شده در تصویر 3 نشان داده می شود. تقاطع T بعنوان طرح پایه شبکه جاده ای استفاده می شود.

این سناریوی ترافیکی، شبیه مورد کاربردی برای هشدار خطر تصادف در تقاطع می باشد. گره C می خواهد وارد جاده ای شود که گره های A و B در آن حرکت می کنند. لازم است که قبل از ورود C به به تقاطع و تا زمانیکه دو گره عبور کنند، C منتظر باشد تا از تصادف با یکی از آنها جلوگیری شود. بعنوان مرحله اول، سناریو با شناسه های متفاوت استفاده شده توسط هر گره اجرا می شود تا اطمینان حاصل شود که سیستم کمکی به خوبی عمل می کند. جزئیات مربوط به اجرای هشدار خطر تصادف تقاطع را می توان در [25] یافت.

بعلاوه، سناریوی دوم، شبیه سناریوی سبقت در جاده روستایی است. در تصویر 4 نمایش داده شده است.

سناریوی ترافیک دوم، شبیه مورد هشدار خطر تصادف سبقت می باشد. گره C خواستار سبقت از گره A است که قبل از آن و در لاین مشابه حرکت می کند. گره B در جهت مخالف به لاین دوم می رسد. گره C مجبور است مانور سبقت خود را تا زمانیکه گره B عبور کند، به تاخیر بیاندازد تا از تصادف ممانعت نماید. همانند سناریوی اول، آزمایشی با شناسه های مختلف برای تمام گره ها اجرا شد تا صحت اجتناب از تصادف بررسی شود. این کار با استفاده از مکانیسم پردازش داده توصیفی در[25] اجرا شد.



تصویر 4. طرح جاده ای که جاده روستایی را نشان می دهد

برای تست تاثیر آدرسهای تکراری بر لایه های پروتکل متعدد، در گره های A و B و زمانیکه گره ها تمایل به شبیه سازی داشتند، در مقادیر مشابه تنظیم شدند. این رویکرد برای شناسه هر لایه تست شد. با این کار، شناسه های وابسته (تصویر 2) نیز تعیین شدند.

نتایج حاصل نشان می دهند که جداشدن بسته توصیفی (بخش 4)، برای رویکرد استاندارد روی می دهد. هیچ آگاهی مشارکتی درباره گره A یا B –فرقی نمی کند که کدام یک بعدا با گره C ارتباط برقرار کند- به لایه کاربردی گره C نمی رسد. نوع ایستگاه گره های A,B به تکرار ID لایه شبکه منجر می شود، یعنی زمانیکه تکرار آدرس MAC موجود باشد. تنها در مورد تکرار ID ایستگاه، پیام های گره A یا B به لایه کاربرد گره C می رسد (که بعدا به دامنه ارتباطی گره C می آید). در غیر اینصورت، توسط خود لایه شبکه یا نهاد امنیتی، در لایه شبکه جدا می شوند. حتی در موردی که پیام به لایه کاربرد می رسد، نمی تواند فرستنده ها را متمایز سازد. بنابراین، پیام ها را جدا می سازد چون بعنوان اپدیت ناموجه، مبتنی بر اطلاعات دریافتی قبلی شناسایی می شوند. بنابراین، لایه کاربرد می تواند از تصادف با یکی از دو همتای تصادفی، جلوگیری کند.

در سناریوی اول (عبور T)، وجود گره A یا B، توسط لایه تاسیسات گره C در طول شبیه سازی شناسایی نشد. در سناریوی دوم (جاده روستایی)، گره B هرگز در لایه تاسیسات گره C شناسایی نشد چون ارتباط بین گره های A و C زودتر از ارتباط بین گره های B و C بود. این مسئله ناشی از این حقیقت است که گره C زودتر از گره A به گره B می رسد. بنابرای، شناسایی قبلی گره A، از شناسایی گره B در C ممانعت می کند.

طرح پیشنهادی بالا (بخشهای 5.1 و 5.2)، قادر به شناسایی و حل تکرار آدرس است. تنها بسته های منتهی به آشکارسازی اولیه تکرار، از بین رفتند. بعد از انتشار درخواست تغییر آدرس هدف، بسته های متوالی در آدرسهای متفاوت نگهداری شدند. بنابراین، توسط گره C پذیرفته شدند. بنابراین، گره C قادر به کسب آگاهی از هردو همتای تصادفی در یک زمان بود. بنابراین، سیستم کمکی همچون مورد بدن تکرار آدرس رفتارکرد و از تصادف جلوگیری به عمل آمد.

6. نتیجه گیری و آثار آینده

VANETها تکنولوژی نویدبخشی برای افزایش امنیت آینده رانندگی هستند. اثر قبلی به بررسی آشکارسازی آدر تکراری DAD در لایه های مختلف پروتکل ارتباط ایمن و بحرانی در چنین شبکه هایی نپرداخته اند. بنابراین، چنین تحلیلی را برای ETSI ITS و WAVE ارائه می دهمی. این تحلیل نشان می دهد که از دست دادن بسته در لایه های مختلف پروتکل، ناشی از آدرسهای تکراری است. این تاثیر به وسیله جفت شدگی نزدیک بین آدرس ها در لایه های مختلف پروتکل و در رویکردهای فعلی VANET تقویت می شود.

دانش ناقص درباره کل شبکه در گره، به گونه ای از مشکل ایستگاه پنهاان که بر آدرسهای پروتکل موثر است، منجر می شود. این نیز، نیاز به مکانیسم آشکارسازی و حل آدرسهای تکراری، توسط ایستگاه هایی را باعث می شود که خودشان چنین تکرارهایی را ندارند. مکانیسم آشکارسازی و حل چنین تکرار خارجی پیشنهاد شده است. این مکانیسم بر تبادل مجموعه داده های مازاد همچون جداول مسیریابی تکیه ندارد. بنابراین، مکانیسم توسعه یافته را می توان در سیستم هایی همچون WAVE بکار برد.

ارزیابی ارائه شده نشان می دهد که مشکلات حاصل از تحلیل، در مثال اجتناب از تصادف در تقاطع، روی می دهند. بعلاوه، نتایج حاصل، نشان از ناپایداری رویکرد مورد نظر دارند. بنابراین، باید برای استانداردهای آینده VANET مدنظر باشند.

اثر آینده می تواند به بررسی تعامل بین تغییرات لازم توسط راه حل آدرس تکراری و استراتژیهای تغییر مشارکتی و ارتقاء دهنده حریم خصوصی بپردازد.

References

[1] J. Harding, G.R. Powell, R. Yoon, et al., Vehicle-to-vehicle communications: readiness of V2V technology for application, Tech. rep. DOT HS 812 014, National Highway Traffic Safety Administration, Washington, DC, Aug. 2014.

[2] S. Rehman, M.A. Khan, T.A. Zia, L. Zheng, Vehicular ad-hoc networks (VANETs) – an overview and challenges, EURASIP J. Wirel. Commun. Netw. 3 (3) (2013) 29–38, http://dx.doi.org/10.5923/j.jwnc.20130303.02.

[3] C. Campolo, A. Molinaro, R. Scopigno (Eds.), Vehicular Ad Hoc Networks – Standards, Solutions, and Research, Springer, 2015.

[4] Intelligent Transport Systems (ITS); Security; Security header, certificate formats, June 2015.

[5] IEEE Standard for Wireless Access in Vehicular Environments, Security Services for Applications, Management Messages, Apr. 2013.

[6] K. Weniger, Passive duplicate address detection in mobile ad hoc networks, in: IEEE Wireless Communications and Networking, vol. 3, 2003, pp. 1504–1509.

[7] J. Petit, F. Schaub, M. Feiri, F. Kargl, Pseudonym schemes in vehicular networks: a survey, IEEE Commun. Surv. Tutor. 17 (1) (2015) 228–255, http://dx.doi.org/10.1109/COMST.2014.2345420.

[8] Intelligent Transport Systems ITS; Vehicular Communications, GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-independent functionality.

[9] T. Buburuzan, et al., Draft C2C-CC standards system profile, Tech. rep., CAR 2 CAR Communication Consortium, v1.0.4 Jan. 2014.

[10] C.E. Palazzi, M. Gerla, M. Fazio, S. Das, Facilitating real-time applications in VANETs through fast address auto-configuration, in: 4th IEEE Consumer Communications and Networking Conference, 2007, pp. 981–985.

[11] R. Baldessari, C.J. Bernardos, M. Calderon, GeoSAC – scalable address autoconfiguration for VANET using geographic networking concepts, in: IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, 2008, pp. 1–7.

[12] S. Boudjit, C. Adjih, A. Laouiti, P. Muhlethaler, A duplicate address detection and autoconfiguration mechanism for a single-interface OLSR network, in: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks, in: LNCS, vol. 3837, Springer, 2005, pp. 128–142.

[13] IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services, Dec. 2010.

[14] N.H. Vaidya, Weak duplicate address detection in mobile ad hoc networks, in: ACM International Symposium on Mobile Ad Hoc Networking & Computing, 2002, pp. 206–216.

[15] S. Pietrowicz, et al., Vehicle segment certificate management using short-lived, unlinked certificate schmes, 2012.

[16] S. Bittl, K. Roscher, A.A. Gonzalez, Security overhead and its impact in VANETs, in: 8th IFIP Wireless Mobile Networking Conference, 2015, pp. 192–199.

[17] S. Bittl, B. Aydinli, K. Roscher, Effective certificate distribution in ETSI ITS VANETs using implicit and explicit requests, in: M. Kassab, et al. (Eds.), 8th International Workshop Nets4Cars/Nets4Trains/Nets4Aircraft, in: LNCS, vol. 9066, 2015, pp. 72–83.

[18] Intelligent Transport Systems (ITS); STDMA recommended parameters and settings for cooperative ITS; Access Layer Part (Jan. 2012).

[19] Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer (Aug. 2014).

[20] K. Roscher, S. Bittl, A.A. Gonzalez, M. Myrtus, J. Jiru, EzCar2X: rapid-prototyping of communication technologies and cooperative ITS applications on real targets and inside simulation environments, in: 11th Conference Wireless Communication and Information, 2014, pp. 51–62.

[21] M. Behrisch, L. Bieker, J. Erdmann, D. Krajzewicz, SUMO – Simulation of Urban MObility: an overview, in: The Third International Conference on Advances in System Simulation, 2011, pp. 63–68.

[22] G.F. Riley, T.R. Henderson, The ns-3 network simulator, in: K. Wehrle, M. Günes, J. Gross (Eds.), Modeling and Tools for Network Simulation, Springer, Berlin, Heidelberg, 2010, pp. 15–34.

[23] A. Varga, Modeling and Tools for Network Simulation, Springer, 2010, pp. 35–59, Ch. OMNeT++.

[24] L. Cheng, B.E. Henty, F. Bai, D.D. Stancil, Highway and rural propagation channel modeling for vehicle-to-vehicle communications at 5.9 GHz, in: IEEE Antennas and Propagation Society International Symposium, 2008, pp. 1–4.

[25] D. Seydel, S. Bittl, J. Pfeiffer, J. Jiru, H. Beckmann, K. Frankl, B. Eissfeller, An evaluation methodology for VANET applications combining simulation and multi-sensor experiments, in: 2nd International Conference on Vehicular Intelligent Transport Systems, 2016, pp. 213–224.