مجله‌ی علمی پژوهش در علوم رایانه، شماره ۲۵، بهار ۱۴۰۱، ص ۴۳- ۳۴

ISSN: 2745-3673
http://www.Rcsj.ir

مجله علمی پژوهش در علوم رایانه (سال هفتم)
شماره ۲۵ / بهار ۱۴۰۱ / ص ۴۳- ۳۴

ارتقای امنیت وکارایی مسیریابی در شبکه های خودرویی با توجه به اعتماد مبتنی بر تئوری توابع برآورد

عقیل جلیلی کیا

کارشناس ارشد مهندسی کامپیوتر گرایش نرم افزار، دانشگاه غیر انتفاعی کارون، موسسه آموزش عالی کارون.

نام نویسنده مسئول:
عقیل جلیلی کیا

تاریخ دریافت: ۱۴۰۱/۰۱/۰۵
تاریخ پذیرش: ۱۴۰۱/۰۳/۰۸

چکیده

طرحهای مبتنی بر اعتماد تکنیک‌های امیدوار کننده ای برای مقابله با حملات در شبکه های خود سازمان یافته توزیع شده، مانند شبکه های ***Ad hoc*** و شبکه های ویژه خودرویی است. در سیستم مدیریت اعتماد، اعتماد به عنوان درجه‌ای از باور وجود دارد که یک نهاد می‌تواند در دیدگاه ناظر به طور صحیح رفتار کند. در مقایسه با طرحهای مبتنی بر پیشگیری، طرحهای مبتنی بر تشخیص، مانند مدیریت اعتماد، به صورت پویا رفتار گره داخلی را تخمین می‌زنند. براساس نتایج تخمین، سیستم تشخیص تصمیم می‌گیرد که آیا گره یک مهاجم مخرب است یا خیر. این طرحهای مبتنی بر آشکارسازی به دلیل رفتار غیرقابل پیش‌بینی هر گره در شبکه، باعدم قطعیت بالایی مواجه هستند. بنابراین، در سیستم مدیریت اعتماد، ارزیابی دقیق اعتماد نقش اساسی در مدیریت اعتماد دارد. برای به دست آوردن اعتماد دقیق هر یک از مولفه ها در شبکه، از استدلال نامشخص استفاده می‌کنیم در این تحقیق، ما بر روی مدیریت اعتماد با روشهای احتمالی تمرکز می‌کنیم. دلیل این امر آن است که فرضیه دمپستر شفر می‌تواند اعتماد به شبکه های خود سازمان یافته توزیع شده را بهتر از طرحهای مبتنی بر قانون شکل دهد. در چارچوب استدلال نامشخص، ما رویکرد دمپستر-شیفر را را برای ارزیابی دقیق اعتماد اتخاذ می‌کنیم. ابتدا محیط شبکه Ad hoc Network (VANET) را با مهاجمان خودی مخرب در نظر می‌گیریم. ما از روش استنباط بیزی برای ارزیابی اعتماد گره ها در VANET ها بر اساس رفتار هر گره استفاده می‌کنیم. اعتماد هر گره با احتمال پسین شکل می‌گیرد. سیستم مدیریت اعتماد گره های مخرب که ارزش اعتماد پایینی دارند را حذف نمی‌کند. ما نشان می‌دهیم.که در سناریوهای مخرب، طرحهای پیشنهادی می‌توانند از لحاظ اعتماد پویا، توان عملیاتی، تأخیر پایان تا پایان و غیره از طرحهای موجود پیشی بگیرند. نتایج شبیه سازی گسترده نشان می‌دهد که روش پیشنهادی ما عملکرد بهتری نسبت به طرحهای موجود دارد.

واژگان کلیدی: شبکه های خودرویی، اعتماد، تئوری دمپستر-شیفر، واحد های کنار جاده ای.

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

برای ورود به بحث ادبیاتی ابتدا برخی از تعاریف ارائه می‌شوند و در ادامه برخی از کارهای پیشین بررسی می‌شوند. در این بخش، سه روش در استدلال نامشخص ارائه می‌دهیم: استنتاج بیزی،DST[1] و مدل شبکه های بیزی نظریه دمپستر-شفر (DST) به عنوان مکانیسم مفیدی در استدلال نامشخص در نظر گرفته می‌شود و در سیستم‌های خبره و سیستم‌های چند عامل بسیار کاربرد دارد [۱۳، ۱۴]. در [۱۵]، تئوری دمپستر-شیفر در همجوشی حسگر استفاده می‌شود. سیستم‌های تشخیص نفوذ [۱۶، ۱۵] از نظریه دمپستر-شفر برای ارزیابی اطلاعات غیرقابل اطمینان از سنسورهای IDS استفاده می‌کنند. در [۱۵، ۱۴] از تئوری Dempster-Shafer برای شناسایی گره های مخرب و جداسازی آنها در شبکه های ad hoc استفاده می‌شود.

ما از نظریه استدلال نامشخص از هوش مصنوعی برای ارزیابی اعتماد گره ها در VANET استفاده می‌کنیم. عدم قطعیت یک مشکل قدیمی‌در دنیای قماربازان است. این مشکل را می‌توان با نظریه احتمال اداره کرد. استدلال رفتار مهم دیگری در زندگی روزمره است. بسیاری از محققان، حتی ارسطو (۳۸۴ پیش از میلاد - ۳۲۲ پیش از میلاد) (فیلسوف یونانی)، سعی در فهم و تدوین آن دارند. استدلال بر اساس عدم اطمینان به دلیل توسعه نظریه احتمال و منطق نمادین در جامعه هوش مصنوعی رونق داشته است. استدلال احتمالی به سیستمهای اطلاعاتی معرفی شده است [۱۲]، که برای مقابله با استثنائات در استدلال خودکار استفاده می‌شود. برای غلبه بر اشکالات سیستمهای سنتی مبتنی بر قاعده که مبتنی بر جداول حقیقت و بدون استثناء نیستند، استدلال احتمالی پیشنهاد می‌شود، که در آن عدم اطمینان دانش در نظر گرفته می‌شود و به عنوان زیر مجموعه های "جهان های ممکن" توصیف می‌شود. استدلال احتمالی می‌تواند در زمینه های مختلف، از هوش مصنوعی گرفته تا فلسفه، روانشناسی شناختی و علم مدیریت استفاده شود. در زمینه امنیت درVANETs ، درمی‌یابیم که این تئوری براساس تفسیر اعتماد در این تحقیق برای ارزیابی اعتماد بسیار مناسب است. نظریه استنتاج بیزی و نظریه شواهد دمپستر-شفر دو رویکرد در استدلال نامشخص است. ما آنها را مورد استفاده قرار می‌دهیم تا اعتماد گره ها را با مشاهده مستقیم و غیرمستقیم ارزیابی کنند.

با توجه به ویژگی‌های ویژه شبکه های بیزی، بسیاری از کارهای تحقیقاتی سعی کردند از این ابزار برای ارزیابی اعتماد به شبکه های توزیع شده استفاده کنند [۹-۱۱]. یک مدل اعتماد به نفس مبتنی بر شبکه بیزی ساده لوحانه در شبکه های همتا به همتا ارائه می‌شود [۱۱]. نویسندگان از مدل شبکه بیزی برای ارزیابی اعتماد بر اساس ویژگی‌های مختلف سرویس استفاده می‌کنند. مدل اعتماد به نفس دیگر مبتنی بر شبکه بیزی در VANETs استفاده می‌شود [۱۰]. نویسندگان این مقاله، اعتماد مستقیم و اعتماد غیرمستقیم را به الگوی اعتماد پیشنهادی ارائه می‌دهند. اگرچه در این مقاله به تشخیص بدخواهی اشاره شده است، اما مدل اعتماد هنوز هم خدمات ارائه شده را در نظر می‌گیرد، که مشابه [۱۱] است. نویسندگان در [۹] یک مدل اعتماد مبتنی بر شبکه های بیزی را در شبکه های حسگر بی سیم پیشنهاد داده اند. اعتماد به این مدل از اعتماد به نفس ارتباطات و اعتماد داده ها تشکیل شده است که با استفاده از یک شبکه بیزی ترکیب می‌شوند. با این حال، نویسندگان در [۹] چگونگی تجزیه و تحلیل هر مؤلفه اعتماد توسط شبکه بیزی را نشان نمی‌دهند. در [۱۲]، نویسندگان برای طبقه بندی گره ها درVANET ها از یک فیلتر ساده بیزی، نوع ساده شبکه های بیزی استفاده می‌کنند. این روش پروفایلهای گره اولیه را بدون تبادل توصیه اضافی ایجاد می‌کند. نویسندگان در [۱۳] رویکردی برای ارزیابی اعتماد بر اساس یک مدل اطمینان مبتنی بر بیزی ارائه داده اند. این روش مسیرهای مسیریابی قابل اطمینان را بین گره های منبع و گره های سینک‌های مبتنی بر اعتماد فراهم می‌کند.

مدیریت اعتماد

با پیشرفت‌های اخیر در فن آوری‌های بی سیم و دستگاه های تلفن همراه، شبکه های Ad-hoc Mobile (VANETs) به عنوان یک فناوری ارتباطی کلیدی در محیط‌های تاکتیکی نظامی‌مانند ایجاد شبکه های ارتباطی که برای هماهنگی استقرار نظامی‌در بین سربازان، وسایل نقلیه مورد استفاده قرار می‌گیرند، رایج شدهاند. و مراکز فرماندهی عملیاتی، خطرات زیادی در محیط‌های نظامی‌وجود دارد که باید با توجه به ویژگی‌های متمایزVANET ها، از جمله رسانه انتقال بی سیم باز، طبیعت

ISSN: 2745-3673
http://www.Rcsj.ir

عشایری و توزیع شده، نبود زیرساخت‌های متمرکز حفاظت از امنیت، به طور جدی مورد توجه قرار گیرد. بنابراین، امنیت در VANETs تاکتیکی یک موضوع تحقیق چالش برانگیز است.

دو روش مکمل رویکرد وجود دارد که می‌توانند ازVANET های تاکتیکی محافظت کنند: رویکردهای مبتنی بر پیشگیری و تشخیص مبتنی بر [۱۶]. رویکردهای مبتنی بر پیشگیری به طور جامع در VANETs مورد بررسی قرار می‌گیرد. یکی از مشکلات این رویکردهای مبتنی بر پیشگیری این است که یک زیرساخت مدیریتی متمرکز کلید مورد نیاز است که ممکن است در شبکه های توزیع شده مانند VANET واقع بینانه نباشد. علاوه بر این، یک زیرساخت متمرکز هدف اصلی رقبا در میادین نبرد خواهد بود.

اگر زیرساخت‌ها از بین برود، ممکن است کل شبکه فلج شود [۱۵]. علاوه بر این، گرچه رویکردهای مبتنی بر پیشگیری می‌تواند از بروز رفتار نادرست جلوگیری کند، اما هنوز احتمال وجود دارد که گره های مخرب برای شرکت در روش مسیریابی و ایجاد مسیریابی مناسب اختلال ایجاد کنند. از تجربه در زمینه طراحی امنیت در شبکه های سیمی، مکانیزمهای امنیتی چند سطحی مورد نیاز است. درVANETs ، این امر به ویژه با توجه به امنیت بدنی پایین دستگاه های تلفن همراه صادق است. با استفاده از دومین دیوار محافظت، رویکردهای مبتنی بر تشخیص می‌توانند به طور مؤثر در شناسایی فعالیتهای مخرب کمک کنند.

اگرچه برخی کارهای عالی رویکردهای مبتنی بر تشخیص مبتنی بر اعتماد بهVANET ها انجام شده است، اما اکثر رویکردهای موجود از مشاهده مستقیم و غیرمستقیم (همچنین اطلاعات دست دوم نیز نامیده می‌شود که از گره های شخص ثالث به دست می‌آید) در همان زمان برای ارزیابی اعتماد به یک گره مشاهده شده علاوه بر این، مشاهده غیرمستقیم در اکثر روشها فقط برای ارزیابی قابلیت اطمینان گره ها استفاده می‌شود، که در محدوده گره ناظر نیستند [۱۵، ۱۴، ۱۳]. بنابراین ممکن است مقادیر اعتماد نادرست حاصل شود. علاوه بر این، اکثر روشهای ارزیابی اعتماد از مشاهده مستقیم هیچ تفاوتی بین بسته های داده و بسته های کنترل ندارند. با این حال، درVANET ها، بسته های کنترلمعمولاً از بسته های داده اهمیت بیشتری دارند.

در این بخش، اعتماد را به عنوان درجه‌ای از اعتقاد عمل می‌کنیم که یک گره آنطور که انتظار می‌رود انجام می‌دهد. ما همچنین عدم اطمینان در ارزیابی اعتماد را تشخیص می‌دهیم. بر اساس این تفسیر، ما یک طرح مدیریت اعتماد را برای تقویت امنیتVANET ها پیشنهاد می‌کنیم. تفاوت بین طرح ما و طرحهای موجود در این است که ما از استدلال نامشخص برای به دست آوردن ارزش اعتماد استفاده می‌کنیم. استدلال نامشخص در ابتدا از جامعه هوش مصنوعی برای حل مشکلات در سیستم‌های خبره که دارای نتایج مکرر ضد واقعی هستند، پیشنهاد شده است [۱۲]. انعطاف پذیری و انعطاف پذیری استدلال نامشخص، آن را در بسیاری از زمینه ها، مانند سیستم‌های خبره، سیستم‌های چند عامل و ادغام داده ها، موفق می‌سازد.

در این بخش تعریف و ویژگی‌های اعتماد در VANETs را شرح می‌دهیم. براساس تعریف، ما یک مدل اعتماد را نشان می‌دهیم که برای شکل دادن اعتماد بین دو گره در VANETها استفاده می‌شود و چارچوبی ما نیز برای VANET از طرح پیشنهادی را ارائه می‌دهد.

تعریف و ویژگی‌های اعتماد

اعتماد در رشته های مختلف از روانشناسی گرفته تا اقتصاد معانی متفاوتی دارد [۴، ۱۴]. تعریف اعتماد به VANETها شبیه به توضیحات در جامعه شناسی است، جایی که اعتماد به عنوان درجه‌ای از اعتقاد تعبیر می‌شود که یک گره در یک شبکه (یا یک عامل در یک سیستم توزیع شده) وظایفی را که باید انجام دهد. با توجه به ویژگی‌های خاص VANETs، اعتماد به VANETs دارای پنج ویژگی اساسی است: ذهنیت، پویایی، عدم انعطاف پذیری، عدم تقارن و وابستگی به متن [۴، ۱۴]. ذهنیت به این معنی است که یک گره ناظر حق دارد اعتماد یک گره مشاهده شده را تعیین کند. گره های مختلف مشاهده گر ممکن است دارای ارزش اعتماد متفاوتی از یک گره مشاهده شده باشند. پویایی به این معنی است که باید اعتماد به یک گره بسته به رفتارهای آن تغییر یابد. عدم انعطاف پذیری به این معنی است که اگر گره A به گره B اعتماد کرده باشد، گره باند B به گره C

ISSN: 2745-3673
http://www.Rcsj.ir

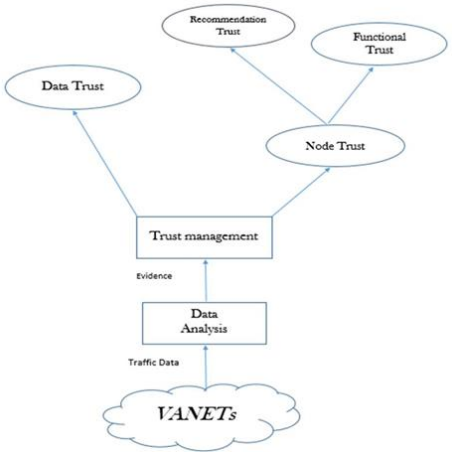
اعتماد دارد، بنابراین گره A لزوما به گره Cاعتماد ندارد. عدم تقارن به این معنی است که اگر گره A به گره B اعتماد کند، گره Bلزوماً به گره A اعتماد ندارد. به این معنی است که ارزیابی اعتمادمعمولاً مبتنی بر رفتارهای یک گره است. با اعتماد متفاوت می‌توان جنبه های مختلف اعمال را ارزیابی کرد. به عنوان مثال، اگر یک گره قدرت کمتری داشته باشد، ممکن است نتواند پیامهای خود را به همسایگان خود ارسال کند. در این شرایط، اعتماد به نفس در این گره کاهش می‌یابد، اما اعتماد به امنیت در این گره به دلیل وضعیت آن تغییر نخواهد کرد.

اعتبار یکی دیگر از مفاهیم مهم در ارزیابی اعتماد است. اعتبار منعکس کننده نظرات عمومی‌اعضای یک جامعه است [۶]. در VANETها، شهرت می‌تواند مجموعه ای از اعتماد از گره های شبکه باشد. اعتبار جهانی از اعتماد به نفس از دیدگاه کل شبکه است.

مدل اعتماد

بر اساس تعریف و ویژگی‌های اعتماد به VANETs، ما اعتماد به طرح پیشنهادی را با یک عدد واقعی، T با ارزش مداوم بین ۰ و ۱ ارزیابی می‌کنیم. گرچه اعتماد و اعتماد به نفس ممکن است در زمینه هایی متفاوت باشد، که در آن لازم است متولی ریسک را در نظر بگیرید [۴]، اعتماد و اعتماد به نفس برای سادگی در طرح پیشنهادی یکسان هستند.

در این مدل، اعتماد از دو مؤلفه تشکیل شده است: اعتماد مشاهده مستقیم و اعتماد به مشاهدات غیرمستقیم. این مؤلفه ها شبیه به موارد استفاده شده در [۶] هستند. در اعتماد مستقیم مشاهده، ناظر اعتماد همسایه یک‌هاپ خود را براساس عقیده خودش تخمین می‌زند. بنابراین، ارزش اعتماد، انتظار یک احتمال ذهنی است که یک متولی برای تصمیم گیری در مورد اعتماد بودن یا عدم استفاده از معتمد از آن استفاده می‌کند. این شبیه به اطلاعات دست اول است که توسط تعریف شده است. ما T5 را به عنوان یک مقدار اطمینان از مشاهده مستقیم بیان می‌کنیم و می‌توان با استنباط بیزی محاسبه کرد. اگر فقط مشاهده مستقیم را در نظر بگیریم، تعصب در محاسبه ارزش اعتماد وجود دارد. به منظور به دست آوردن اعتماد به نفس کمتری، نظرات سایر ناظران را نیز در نظر می‌گیریم. اگرچه نظرات همسایگان در [۶] معرفی شده است، روشی که‌صرفاً معنی حسابی از تمام مقادیر اعتماد را در بر می‌گیرد، برای بازتاب معنای واقعی نظرات سایر ناظران غیرقابل اعتماد کافی نیست زیرا دو موقعیت وجود دارد که ممکن است شواهد مؤثر را به شدت مختل کند. همسایگان: همسایگان غیر قابل اعتماد و مشاهده غیرقابل اعتماد [۷]. همسایگان غیر قابل اعتماد خود مظنون هستند. حتی اگر همسایگان قابل اعتماد باشند، ممکن است به دلیل شرایط مشاهده شواهد غیرقابل اعتماد ارائه دهند. نظریه دمپستر-شفر کاندیدای خوبی برای کمک به این وضعیت است که در آن شواهدی از همسایگان جمع آوری می‌شود که غیرقابل اطمینان است. بنابراین، ما ارزش اعتماد به دست آمده از مشاهده غیرمستقیم همسایگان یک‌هاپ را به عنوان TN، ترکیب ارزش اعتماد، T5، از مشاهده مستقیم و ارزش اعتماد، TN، از مشاهده غیرمستقیم، می‌توانیم یک ارزش اعتماد واقعی تر و دقیق تر بدست آوریم.



شکل (۱): بررسی طرح

ISSN: 2745-3673
http://www.Rcsj.ir

در طرح ART برای اولین بار داده های ترافیک را از ونت‌ها برای تجزیه و تحلیل داده ها جمع آوری شد. یافته ها از تجزیه و تحلیل داده به عنوان مدارک برای طرح مدیریت اعتماد خلاصه شد تا قابلیت اعتماد ارزیابی شود. جزئیات شواهد درادامه شکل توضیح داده شدهاند و سپس این شواهد استفاده خواهند شد تا اعتماد داده و نود را بررسی کنند.

VANET یک نمونه شبکه سیار است که برای برقراری ارتباط بین وسایل نقلیه مجاور و همچنین وسایل نقلیه با تجهیزات ثابت مجاور که معمولاً تجهیزات کنارجاده ای هستند ایجادشده است. چنین شبکه‌ای باید بدون محدودیت‌های ساختارهای ارتباطی شبکه‌ای کلاینت- سرور پیاده سازی شود. هر وسیله نقلیه ای که به یک دستگاه VANET مجهز شده باشد همانند یک گره در شبکه Ad Hoc است و قادر به دریافت و ارسال پیامهای دیگران از طریق شبکه بی سیم خواهد بود. هشدارهای ترافیکی، علائم جادهای و مشاهده ترافیک به صورت لحظه‌ای که از طریق چنین شبکه‌ای می‌تواند منتقل شود، ابزارهای لازم را برای تصمیم گیری در مورد بهترین مسیر به راننده می‌دهد. همچنین ارتباطات چند رسانه‌ای و اینترنت در رنج بی سیم هر وسیله نقلیه فراهم می‌شود. پرداخت خودکار هزینه پارکینگ و عوارض جادهای از دیگر کاربردهای شبکهVANET است. In VANET یاVANET هوشمند (Intelligent VANET) در واقع بیانگر یک روش هوشمند در به کارگیری شبکه‌ی بین خودروهاست.

در مرجع [۱] از یک مرکز اصلی با نام مرکز صدور گواهی (CA)برای جمع آوری اطلاعات نام برده شده است که مراکز RSUکه در سطح شهر به صورت متعدد وجود دارند و اطلاعات را از خودروهای موجود در سطح شهر جمع آوری می‌کنند به این مراکز می‌فرستند تا این اطلاعات در آنجا تجمیع شوند و از صحت اطلاعات از طریق این مرکز مطمئن شوند.در واقع این اطلاعات را با نام گواهی به آن مرکز می‌فرستند و در صورت صحت نداشتن اطلاعات لیست لغو گواهی(CRL) صادر می‌شود.

در مرجع[۲]بحث جعلی بودن پیام مورد برسی قرار گرفته شده است چون ممکن است پیامی‌که از RSU از طرف خودرو مجاور فرستاده می‌شود دستکاری شده باشد بنابراین پیام مورد نظر را همرا با یک کلید رمزنگاری شده و با استفاده از امضاء دیجیتال می‌فرستد.

در مرجع [۳] از دو مبحث V2Vو V2Iاستفاده شده که به ترتیب بیان می‌کنند که ارتباطات در شبکه های بین خودرویی به صورت ارتباطات موردی بین خودرو یی و ارتباطات بین خودرو با تجهیزات ثابت کنار جادهای صورت می‌گیرد.

در مرجع [۴] انواع حملات در شبکه های VANETsمورد برسی قرار گرفته است که از مهم ترین این حملات حمله ی پخش پیام مجدد می‌باشدکه این حمله اساسا توسط کاربر مجاز و یا مخرب با چهرا مبدل به عنوان یک کاربر مشروع و یا RSU استفاده می‌شود.

در مرجع[۵] شبکه های ادهاک مربوط به وسایل نقلیه یک فناوری نویدبخش است که فرصت زیادی به مهاجمان برای حمله به شبکه و به چالش کشیدن شبکه با حملات بدخواهانه می‌دهد. این مقاله آنالیز گسترده چالش‌های فعلی و راه حل‌های حملات را فراهم می‌کند. ما تصدیق را با استفاده از مرجع مجوز مجازی پیشنهاد کردیم. این تصدیق به شناسایی آسان گره های بدخواه کمک می‌کند. گره های قابل اعتماد می‌توانند از رسیدن پیام به گره های بدخواه جلوگیری کنند. این راه حل به رانندگان کمک می‌کند تا ایمن و آسان برانند. بحرانهای این راه حل‌ها، در کار آتی بررسی می‌شوند و راه حل جدیدی ارائه می‌شود که به حفظ شبکه VANET ایمن کمک می‌کند و با شبیه سازی آزمایش می‌شود.

شبیه سازی VANET در MATLAB

در ابتدا پروتکل‌های واکنشی برای ویژگی تحرک بالا در طول کشف مسیر طراحی نشدهاند. به دلیل تغییر پویا در VANET، این تغییرات اغلب به دلیل خرابی صورت می‌گیرد که باعث پخش بیش از حد کل شبکه می‌شود تا مسیرهای جدید کشف شود. علاوه بر این، ابتدای مسیر یابی نیاز به زمان دارد و این تاخیر به راحتی می‌تواند همه چیز را تغییر دهد. به همین دلایل، پروتکل‌های واکنشی معمولی، در قالب فعلی خود، برای برنامه های حساس زمان مانند اجتناب از برخورد تعاونی‌کاملاً مناسب نیستند. جلوگیری از برخورد تعاونی یک کلاس مهم از کاربردهای ایمنی در VANET است که هدف آن ارائه هشدار قبلی به رانندگان با استفاده از ارتباطات وسیله نقلیه به وسیله نقلیه (V2V) است [۱۳]. بردار مسافت بر اساس تقاضا (AODV) یک پروتکل مسیریابی واکنشی است که قادر به یکپارچه سازی و چند مرحله ای است. در AODV، مانند تمام پروتکل‌های

ISSN: 2745-3673
http://www.Rcsj.ir

واکنشی، اطلاعات توپولوژی فقط توسط گره های در صورت تقاضا انتقال می‌یابد. هنگامی‌که یک منبع برای ارسال چیزی دارد، ابتدا پیام RREQ را که توسط گره میانی تا رسیدن به مقصد ارسال می‌شود، پخش می‌کند. اگر گیرنده یا گره ای است که از آدرس درخواست شده استفاده می‌کند، یا یک مسیر معتبر به آدرس درخواست شده دارد، یک پیام پاسخ مسیر به یک منبع منحصر به فرد است.

پس از وارد کردن مقادیر ورودی برنامه اجرا شده و برای نمایش بهتر حرکات وسایل بصورت لحظه به لحظه و همچنین ارتباط آنها با RSU و با همدیگر در نمودار گرافیکی نشان داه می‌شود. (شکل ۲).

شکل (۲): محیط اجرای برنامه

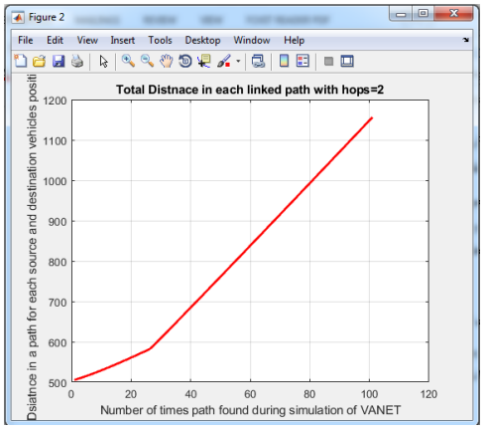
در شکل بالا گره های RSU با مقادیر ۲۰۰۱ تا ۲۰۰۸ و هر تعدادی که در فضای تعریف شده قرار گیرد نشان داده شدهاند و گره های وسایل نقلیه بصورت تصادفی انتخاب شده و حرکت می‌کنند.

جهت حرکت نیز بصورت تصادفی می‌باشند و دو گره منتخب مبدا و مقصد بصورت پیوسته در حال ارسال اطلاعات بین خود و RSU هستند موقعیت RSUها بصورت فاصله های یکسان در فضای تعریف شده برای نشان دادن محاسبات می‌باشند و فاصله آنها طبق فرمولی بصورت یکسان قرار دارد.

- **ارزیابی**

پس از اجرای برنامه خروجی‌ها شامل موارد زیر بودند:

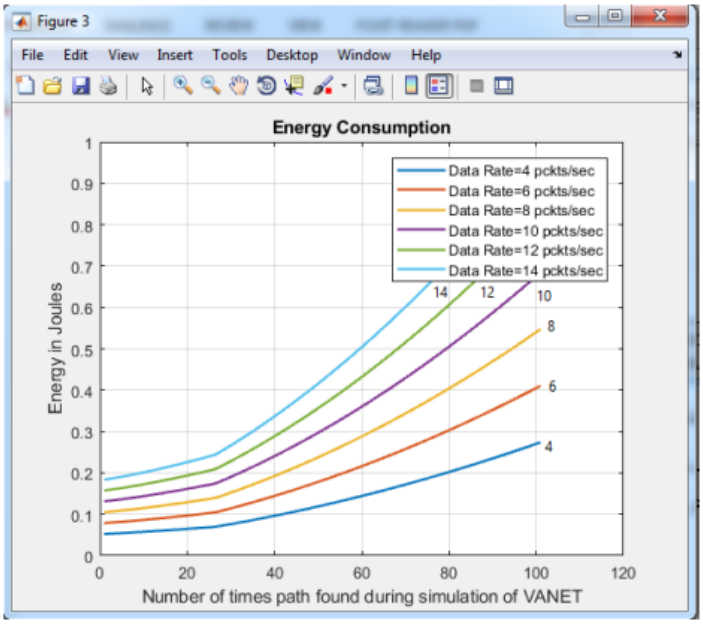
مجموع مسافتهای پیموده شده : برای دو گره مبدا و قصد در نگرفته شد است. شکل ۳ نتیجه اجرای یک شبیه سازی را نشان می‌دهد.



شکل (۳): مجموع مسافتهای طی شده

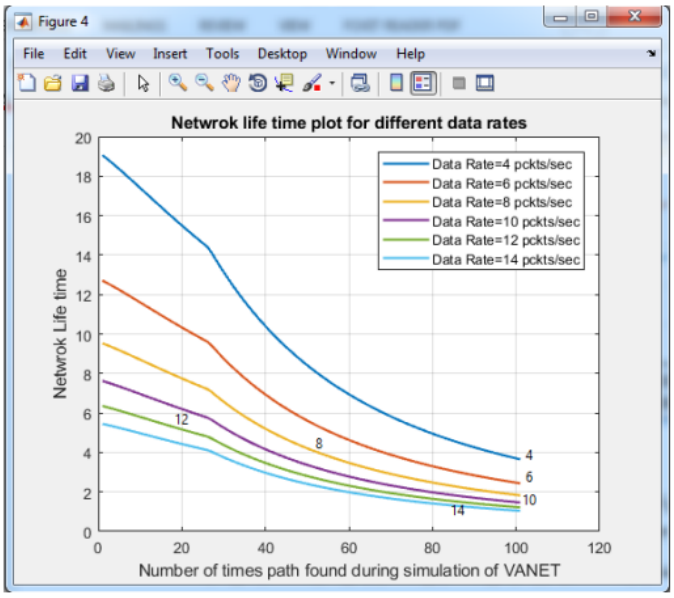
ISSN: 2745-3673
http://www.Rcsj.ir

مقدار انرژی مصرف شده: مقادیر انرژی برحسب واحد ژول باتوجه به نرخ ارسال بسته برحسب ثانیه توسط وسایل نقلیه به هم در مسیرهایی که در گذر زمان پیدا می‌شود محاسبه و مطابق شکل ۴ نشان داده می‌شود.



شکل(۴): مصرف انرژی بر حسب بسته های ارسالی

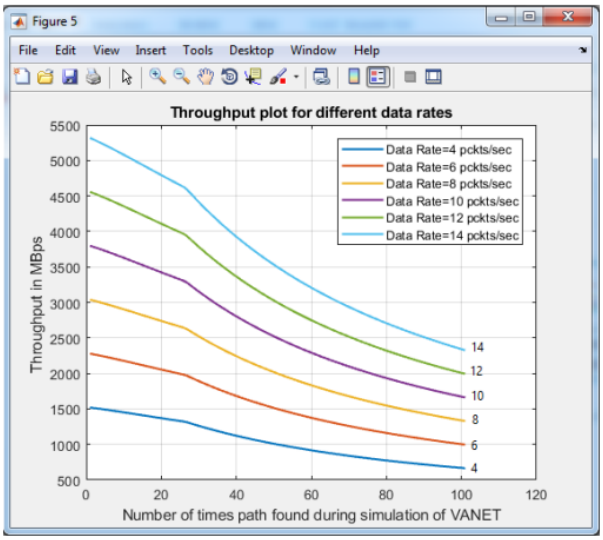
طول عمر شبکه: براساس بسته های ارسالی با اندازه های مختلف طول عمر شبکه را محاسبه کردیم. نتایج مطابق شکل ۵ بدست آمدند. همانطور که مشاهده می‌کنید در ابتدا طول عمر برای بسته های با اندازه کوچکتر بیشتر از بسته های بزرگتر می‌باشد ولی با گذر زمان تقریبا همگرا می‌شوند.



شکل(۵): طول عمر شبکه برای اندازه های مختلف نرخ بسته ها

توان عملیاتی: محاسبه توان عملیاتی شبکه بر اساس بسته های ارسالی در شکل ۴-۵ نمایش داده شده است با اینکه توان رو به کاهش است با اینحال در انتهای زمان فضای مشخص شده با توجه به کاربرد فرضیه دمپستر شفر مقادیر آن کاملا از بین نرفته است.

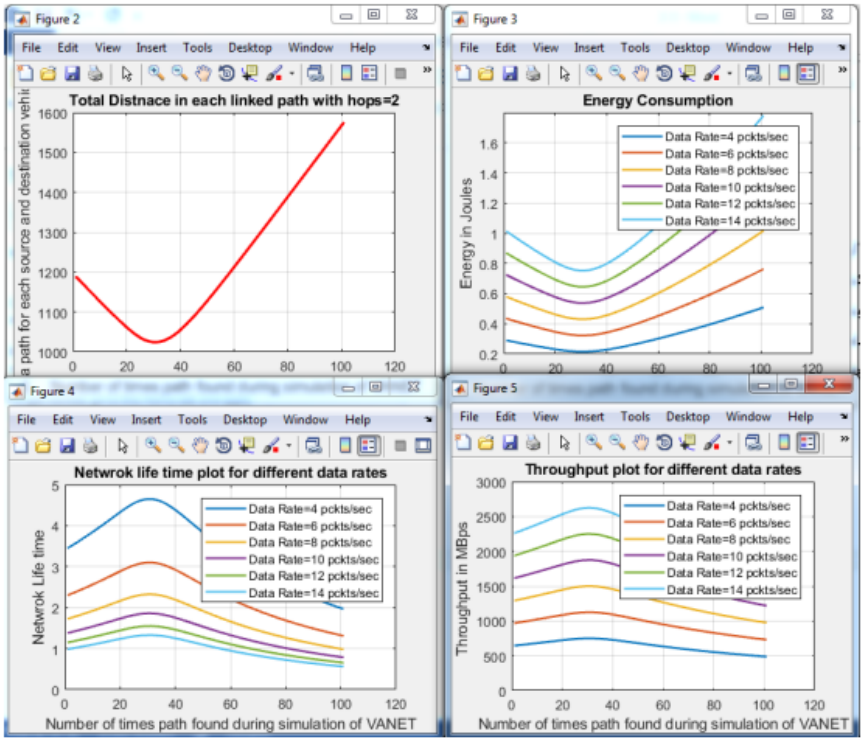
ISSN: 2745-3673
http://www.Rcsj.ir



شکل (۶): توان عملیاتی

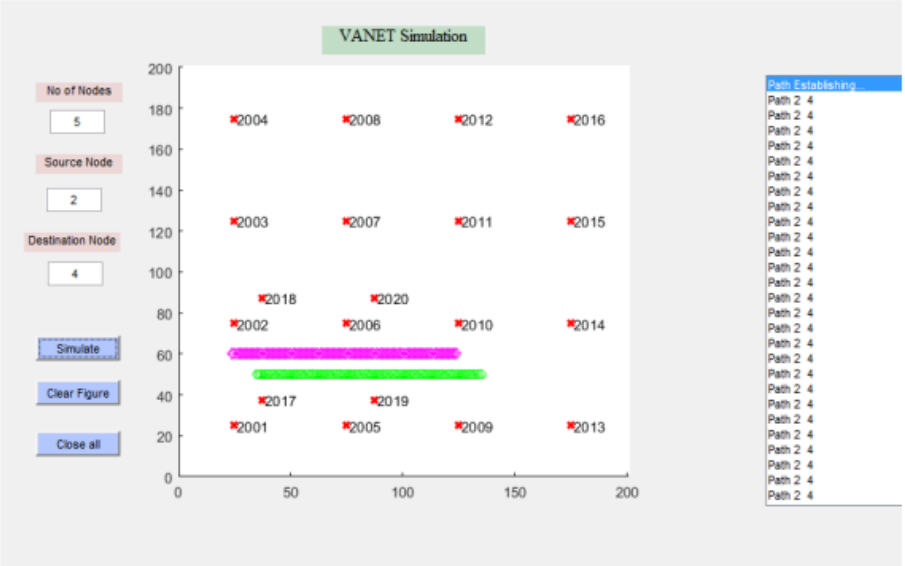
- **ارزیابی سناریوی پیشنهادی**

در طی ارزیابی با توجه به تصادفی بودن مکان گره ها ممکن است حالتی برخورد کنیم که گره مبدا و مقصد بصورت موازی در کنار هم و در یک جهت حرکت کنند در این صورت باتوجه به نرخ بسته ارسالی نمودارهای تحلیلی متفاوت خواهند بود به اینصورت که در ابتدا مقادیر انرژی و توان و طول عمر شبکه افزایش یافته سپس طی گذشت زمان کاهش یابند دلیل افزایش مساله ترافیک بین خودرویی هست که بعلت نبودن ترافیک مقادیر افزایش می‌باند و پس از عبور و فاصله گرفتن کاهش می‌یابند. (شکل ۷ و ۸)



شکل (۷): تحلیل سناریوی خاص

ISSN: 2745-3673
http://www.Rcsj.ir



شکل (۸): حرکت گره ها به موازات یکدیگر

نتیجه گیری

در این تحقیق موضوعات کلی امنیت و حریم خصوصی موجود در VANET بررسی شده است. اول، اهمیت قابلیت همکاری برای احراز هویت VANET، همراه با تمام چالش‌هایی که منتقل می‌کند، معرفی شده است. به منظور ایجاد روابط متقابل ایمن و پویا بین CAهای غیر قابل اعتماد، یک مدل امنیتی که از سیستم تأیید اعتبار (AS) استفاده می‌کند، ارائه شده است. AS وظیفه انجام فرآیند اعتبارسنجی مسیر توسعه یافته مشارکت شده را با تأیید اعتبار در زمان واقعی با استفاده از پروتکل آنلاین وضعیت صدور گواهینامه (OCSP) و ارزیابی کمی‌سطح امنیتی CA از طریق یک مؤلفه معتبر CA که پیاده سازی روش ارزیابی ارزیابی مرجع را بر عهده دارد. (REM) ثانیا، موضوعات مربوط به حریم خصوصی که علیرغم اجرای AS، باز باقی مانده اند، به طور گسترده مورد بحث قرار گرفت. همانطور که توضیح داده شد، برای اینکه بتوانید حریم خصوصی / ناشناس بودن شرطی را فراهم کرده و از حملات مربوط به سناریوی برادر بزرگ جلوگیری کنید، مکانیزمهای اضافی لازم است. برای ارائه ناشناس بودن شرطی و افشای حداقل اطلاعات، پروتکل حفظ حریم خصوصی مبتنی بر ویژگی (P-ABC) ارائه شده است. پروتکل اعتبارنامه های مبتنی بر حفظ حریم خصوصی را پیاده سازی می‌کند، تا به طور انتخابی خصوصیاتی را که باید برای یک حزب مجاز فاش شود انتخاب کند. P-ABCها همچنین یک راه حل مبتنی بر نام مستعار را اجرا می‌کنند که قادر است ناشناس بودن شرطی را فراهم کند. با تکیه بر پروتکل‌های پیشنهادی، یک مدل اعتبار سنجی اعتماد پیشنهاد شده است تا به اعتبار اعتماد به نفس و حمایت از تصمیم گیری در سناریوهای کم زیرساخت بپردازد. سرانجام، تجزیه و تحلیل معاملات بین امنیت و عملکرد هنگام اجرای احراز هویت بین خودرویی در حوزه های مختلف PKI ارائه شده است.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] R. G. Engoulou, M. Bellache, S. Pierre, and A. Quintero, “VANET security surveys,” Comput. Commun, 44, 1-13, 2014.
[2] M. Kakkasageri and S. Manvi, “Information management in vehicular adhocnetworks:Areview,” J.Netw. Comput. Appl, 39,334- 350, 2014
[3] B. T. Sharef, R. A. Alsaqour, and M. Ismail, “Vehicular communication ad hoc routing protocols: A survey,” J. Netw. Comput. Appl., 40, 363-396, 2014
[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular ad hoc network,” J. Netw. Comput. Appl., 37, 380-392, 2014.
[5] M. Raya and J .-P. Hubaux, “Securing vehicular ad hoc networks,” J. Comput. Security, 15(1), 39-68, 2007.
[6] Y. Lin and H. Song, “DynaCHINA: Real -time traffic estimation and prediction, IEEEPervasiveComput., 5(4), 65-65,2006.
[7] J. Angwin and J. Valentino-Devries, Apple, Google Collect User Data,. [Online]. Available: http: //www.wsj.com/articles/ SB10001424052748703983704576277101723453610 .2011.
[8] Waze Mobile, Free Community-Based Mapping, Traf c & Navigation App. [Online]. Available: https: //www.waze.com/.2011.
[9] J. R. Douceur, “The sybil attack,” in International Workshop on Peerto-Peer Systems, ser. Lecture Notes in Computer Science,
[10] P . Druschel, F. Kaashoek, and A. Rowstron,Berlin, Germany: SpringerVerlag, 251-260. 2002
[11] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol 12th Annu. Int. Conf. MobiCom Netw., Atlanta, GA, USA,۸ for ad hoc networks,” in Proc. 2002.
[12] F. Nait-Abdesselam, B. Bensaou, and T. Taleb, “Detecting and avoiding wormhole attacks in wireless ad hoc networks,” IEEE Commun. Mag., 46(4),127-133, 2008.
[13] S.Buchegger andJ.-Y.LeBoudee, “Self-policing mobile adhocnetworks byreputation systems,”IEEECommun. Mag. 43(7),101-107, 2005.
[14] P.-W. Yau and C. J. Mitchell, “Security vulnerabilities in ad hoc networks,” in Proc. Int. Symp. Commun. 99-104. 2003.
[15] M. N.Mejri, J. Ben-Othman, and M. Hamdi, “Survey onVANETsecurity challenges and possible cryptographic solutions,” Veh. Commun., 1(2),53-66, 2014.
[16] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil, “Aggregation and probabilistic verification for data authentication in VANETs,” Inf. Sci., 262, 172-189, 2014.
[17] N. Ekedebe, W. Yu, C. Lu, H. Song, and Y. Wan, “Securing transportation cyber-physical systems,” in Securing Cyber-Physical Systems. Boca Raton, FL, USA: CRC Press, 163-196.2015.
[18] Y. Zhang and W. Lee, “ Intrusion detection in wireless ad-hoc networks,” in Proc. ACM 6th Annu. Int. Conf. MobiCom Netw., Boston, MA, USA, 275-283. 2000. Journal fNetworkandComputerApplications Journal homepage: www.elsevier.com/locate/jnca Authentication Solution for Security Attacks in VANETs
[19] M. Baharat Hubaux, J.P., Capkun, S. & Luo, J. (2004). The security and privacy of smart vehicles. In Security and Privacy, IEEE, 02