علوم رایانش و فناوری اطلاعات
نشریه علمی انجمن کامپیوتر ایران
مجلد ۲۰، شماره ۱، ۱۴۰۱
صفحات ۳۱-۴۰
مقاله پژوهشی

ارائه یک پروتکل مسیریابی امن مبتنی بر اعتماد در شبکه‌های موردی بین خودرویی

مهتاب دهقان[۱]، سعید شکرالهی[۲*]

*نویسنده مسئول، دریافت: ۱۴۰۱/۰۳/۰۴، بازنگری: ۱۴۰۱/۰۴/۲۰، پذیرش: ۱۴۰۱/۰۴/۲۷

[۱] کارشناسی ارشد، رشته‌ی مخابرات امن و رمزنگاری، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، تهران، ایران
[۲] استادیار، گروه امنیت شبکه و رمزنگاری، پژوهشکده فضای مجازی، دانشگاه شهید بهشتی، تهران، ایران

چکیده

در سال‌های اخیر پژوهش و توسعه‌ی شبکه‌هایی که فاقد هرگونه وابستگی به زیرساخت‌های از پیش تعیین‌شده هستند، بسیار مورد توجه قرار گرفته است. شبکه‌های بین خودرویی یکی از انواع این شبکه‌ها هستند که به عنوان یک فناوری نوین، پتانسیل بالایی در افزایش ایمنی جاده‌ها و تأمین رفاه کاربران دارند. گره‌های ثابت و متحرک تشکیل‌دهنده‌ی این شبکه‌ها با تبادل داده‌های حیاتی در مسیریابی شرکت می‌کنند. این گره‌ها با اهداف مختلفی همچون بهبود ایمنی سرنشینان خودرو و کنترل ترافیک با یکدیگر در ارتباط هستند و طیف گسترده‌ای از اطلاعات را مبادله می‌کنند. تبادل باز اطلاعات بین گره‌ها در شبکه‌ای فاقد زیرساخت، زمینه‌ی مناسبی را برای ورود گره‌های مخرب به شبکه و ایجاد اختلال در فرآیندهای شبکه برای دستیابی به اهداف سودجویانه فراهم می‌کند. بنابراین ارسال اطلاعات از مسیری مورد اعتماد و بهینه یکی از چالش برانگیزترین جنبه‌های شبکه‌های بین خودرویی محسوب می‌شود. تاکنون پروتکل‌های مسیریابی مختلفی برای حل این چالش ارائه شده است که از معیارهای متفاوتی برای انتخاب گره‌های مناسب در مسیریابی خود بهره برده‌اند. در این مقاله یک پروتکل مسیریابی امن مبتنی بر موقعیت پیشنهاد شده است که در آن اعتماد جامع هر گره به‌عنوان یکی از معیارهای اساسی برای انتخاب آن گره در فرایند مسیریابی در نظر گرفته شده است. محاسبه‌ی مقدار اعتماد جامع برای هر گره‌ی ارزیابی‌شونده با استفاده از محاسبه‌ی اعتماد مستقیم توسط گره‌ی ارزیابی‌کننده و توصیه‌ی همسایه‌ها طی فرایند پرسش و پاسخ با استفاده از اعتماد غیرمستقیم انجام می‌شود. نتایج شبیه سازی و ارزیابی پروتکل پیشنهادی با کمک نرم‌افزار NS-2 نشان می‌دهد هرچقدر تعداد گره‌های مخرب در شبکه بیشتر باشد، پروتکل پیشنهادی عملکرد بهتری نسبت به پروتکل GPSR از نظر نرخ ارسال بسته، نرخ گذردهی و تأخیر انتها به انتها خواهد داشت.

کلمات کلیدی: مسیریابی امن، شبکه‌های بین خودرویی، مسیریابی مبتنی بر اعتماد، امنیت شبکه‌های بین خودرویی

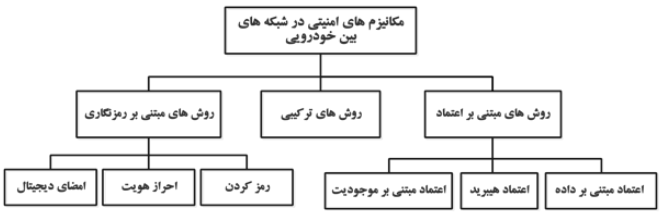
۱. مقدمه

صنعت خودرو در سراسر دنیا روز به روز در حال رشد است. پیشرفت وسایل نقلیه و افزایش استفاده از آنها، علاوه بر داشتن مزایای بیشمار، منجر به بروز مشکلاتی نیز شده است. فناوری شبکه‌های موردی بین خودرویی[۱]، راه حلی مناسب برای رفع مشکلات موجود است. شبکه‌های بین خودرویی به‌عنوان یک سیستم حمل‌ونقل هوشمند تأثیر به‌سزایی در بهبود ایمنی وسایل نقلیه و جاده‌ها، بهره‌برداری و تأمین رفاه کاربران دارد. شبکه‌های بین خودرویی زیر مجموعه‌ای از شبکه‌های موردی متحرک[۲] هستند. در این شبکه وسایل نقلیه مجهز به تجهیزات الکترونیکی واحد روی برد[۳] هستند و به‌عنوان گره‌های متحرک با سایر گره‌ها و واحدهای کنار جاده‌ای که نقش گره‌های ثابت را ایفاء می‌کنند در ارتباط بوده و پیام‌ها را منتقل می‌کنند. تعامل خودرو با خودرو[۴] (V2V) و خودرو با زیرساخت[۵] (V2I) مبتنی بر استاندارد DSRC[۶] بوده و با هدف کنترل ترافیک، بهبود ایمنی جاده‌ها و تأمین آسایش کاربران انجام می‌گیرد. هر گره در شبکه‌ی بین خودرویی از محدوده‌ی رادیویی مشخصی جهت برقراری ارتباط با سایر گره‌ها برخوردار است. به‌دلیل ماهیت شبکه‌ی بین خودرویی، تحرک بالای گره‌ها و ساختار متغیر آن در مقایسه با شبکه‌های موردی متحرک، استفاده از پروتکل‌های مسیریابی مبتنی بر موقعیت[۷] در مقایسه با پروتکل‌های مسیریابی مبتنی بر ساختار[۸] از سهولت بالاتری برخوردار است. برخی اوقات ممکن است به‌دلیل محدوده‌ی رادیویی پایین جهت انتقال اطلاعات در شبکه‌های بین خودرویی، ارتباط بین دو گره بوسیله‌ی تعدادی گره‌ی میانی انجام شود. به‌همین دلیل گره‌های میانی باید از سطح اعتماد مطلوبی برای شرکت در فرایند ارتباط برخوردار باشند [۱]. از طرفی دیگر، پروتکل‌های مسیریابی در شبکه‌های بین خودرویی به‌دلیل فقدان زیرساخت و خودسازماندهی شبکه در برابر تهدیدات آسیب پذیرتر هستند. در این شبکه، گره‌های مخرب[۹] می‌توانند در هر زمان

وارد شبکه شده و با تغییر پیام‌های شبکه یا عدم ارسال بسته‌ها و رها کردن آن‌ها سبب ایجاد اختلال در عملکرد شبکه شوند.

بنابراین تأمین امنیت در مسیریابی از اهمیت بالایی برخوردار است و شبکه باید توانایی برقراری امنیت در برابر مهاجمان داخلی و خارجی را داشته باشد. در این راستا، بسیاری از پژوهشگران تلاش کردند تا امنیت مسیریابی در شبکه‌های بین خودرویی را با پیاده‌سازی مکانیزم‌های امنیتی مختلفی براساس رمزنگاری، اعتماد و ترکیبی از دو روش بهبود بخشند. بررسی‌های اخیر نشان می‌دهد راه حل‌های مبتنی بر اعتماد[۱۰] می‌توانند روش مؤثرتری در برقراری ارتباط ایمن و تبادل مطمئن پیام‌ها بین گره‌های شبکه‌ی بین خودرویی باشند [۲]. شکل ۱، طبقه‌بندی مکانیزم‌های امنیتی مختلف در شبکه‌های بین خودرویی را نشان می‌دهد که در ادامه به تشریح آنها می‌پردازیم.

مکانیزم‌های مبتنی بر رمزنگاری: روش‌های مبتنی بر رمزنگاری شامل مجموعه‌ای از تکنیک‌ها جهت برقراری ارتباط ایمن با وجود گره‌های مخرب شبکه است [۳]. استفاده از روش‌های مبتنی بر رمزنگاری، شبکه‌ی بین خودرویی را در برابر طیف گسترده‌ای از حملات از جمله حملات دستکاری پیام[۱۱]، تزریق پیام جعلی[۱۲]و حملات سیبل [۱۳] محافظت می‌کنند. با این وجود، روش‌های مبتنی بر رمزنگاری، هزینه‌ی زیاد و سربار محاسباتی بالایی دارند. ارسال سریع پیام‌ها در شبکه‌های بین خودرویی یکی از موارد حائز اهمیت است به‌ویژه در هنگام وقوع رویدادهای مهم در شبکه و ارسال پیام‌های اضطراری، اهمیت این پارامتر دوچندان می‌شود. بنابراین استفاده از روش‌های مبتنی بر رمزنگاری هنگام تبادل پیام‌های اضطراری می‌تواند عملکرد شبکه را با اختلال مواجه کند. علاوه بر این، روش‌های مبتنی بر رمزنگاری ممکن است توسط گره‌های مخرب درون شبکه با شکست مواجه شوند که انتشار اطلاعات غیرقابل اعتماد را در شبکه به‌دنبال خواهد داشت. بنابراین استفاده از روش‌های مبتنی بر رمزنگاری می‌تواند منجر به بروز تأخیر در ارسال پیام‌ها و افزایش احتمال رها شدن بسته‌ها شود.



شکل ۱- مکانیزم‌های امنیتی در شبکه‌های بین خودرویی

مکانیزم‌های مبتنی بر اعتماد: روش‌های مبتنی بر اعتماد در مسیریابی شبکه‌های بین خودرویی به ارزیابی قابل اعتماد بودن یک گره جهت ارتباط با سایر گره‌ها می‌پردازند. میزان قابل اعتماد بودن یک گره براساس معیارهای مختلفی سنجیده می‌شود. ارزیابی نرخ تحویل بسته یکی از پارامترهایی است که عموماً برای شناسایی گره‌ی مورد اعتماد در پروتکل‌های مختلف استفاده می‌شود. در صورتیکه یک گره با توجه به معیارهای مورد نظر به‌عنوان گره‌ی مورد اعتماد شناخته شود، مجوز شرکت در فرایند مسیریابی را خواهد داشت. لازم به ذکر است که روش‌های مبتنی بر اعتماد هیچگونه سیستم دفاعی نسبت به دشمنان خارج از شبکه ایجاد نمی‌کنند و کارایی آنها تنها در برابر دشمنان حاضر در شبکه است. با این وجود این روش نسبت به روش‌های مبتنی بر رمزنگاری از سهولت بیشتری برخوردار بوده و پیچیدگی کمتری دارد.

به‌طور کلی روش‌های مبتنی بر اعتماد به بررسی قابل اعتماد بودن یک گره جهت ارسال اطلاعات یا بررسی صحت اطلاعات دریافت شده از آن‌ها می پردازند. بر این اساس روش‌های مبتنی بر اعتماد به دو گروه اصلی، موجودیت محور [۱۴]و داده محور [۱۵] تقسیم می‌شوند که هر کدام می‌توانند به شکل اعتماد مستقیم، اعتماد غیرمستقیم و اعتماد جامع[۱۶] ارزیابی شوند. اعتماد موجودیت محور به بررسی ویژگی قابل اعتماد بودن موجودیت‌های شبکه می‌پردازد در حالیکه اعتماد داده محور، ویژگی قابل اعتماد بودن داده‌های دریافتی را مورد بررسی قرار می‌دهد. مقدار اعتماد می‌تواند با توجه به پروتکل انتخابی با معیارهای مختلفی از جمله نرخ تحویل بسته‌ها، معیار صداقت، معیار مسئولیت‌پذیری، سطح اقتدار نقش گره‌ها و فرکانس فعالیت تخمین زده شود.

مکانیزم‌های ترکیبی: جدول ۱ نمایی مختصر از مزایا و معایب هریک از مکانیزم‌های امنیتی در شبکه‌های بین خودرویی را نشان می‌دهد که براساس نیازهای امنیتی مورد استفاده قرار می‌گیرند. روش‌های ترکیبی در واقع ترکیبی از روش‌های مبتنی بر رمزنگاری و روش‌های مبتنی بر اعتماد جهت تأمین امنیت در شبکه‌های بین خودرویی هستند. زمانی که استفاده از یکی از روش‌های مبتنی بر اعتماد یا مبتنی بر رمزنگاری در برابر برخی از گره‌های مخرب کافی نباشد، از ترکیب این دو رویکرد با یکدیگر استفاده می‌شود. برای پر کردن حفره‌های امنیتی مرتبط با روش‌های مبتنی بر رمزنگاری در برابر حملات داخلی، می‌توان روش‌های مبتنی بر اعتماد را به همراه روش‌های مبتنی بر رمزنگاری استفاده کرد [۴]. براساس ضعف‌های موجود در شبکه و پروتکل‌های ارائه شده، انتظار می‌رود که یک پروتکل مناسب برای تأمین امنیت در مسیریابی دارای ویژگی‌های کلی زیر باشد:

۱)برقراری ارتباط مطمئن بین گره‌ها: به منظور برقراری شبکه‌ای از ارتباطات مطمئن در شبکه‌های بین خودرویی، لازم است تا گره‌های مخرب شناسایی شده و از فرآیند مسیریابی حذف شوند. چرا که حضور گره‌های مخرب و ارسال اطلاعات غلط توسط آن‌ها می‌تواند ارتباط گره‌های مورد اعتماد شبکه را نیز دچار اختلال کند.

۲)کاهش تأخیر در تحویل پیام: تحویل به موقع اطلاعات حیاتی در شبکه‌های بین خودرویی یکی از ویژگی‌های ضروری در یک پروتکل مسیریابی مطمئن محسوب می‌شود. بنابراین یک پروتکل مطمئن باید علاوه بر تأمین اعتماد لازم جهت تبادل پیام‌ها، قابلیت تحویل به موقع بسته‌ها را نیز داشته باشد تا بدین ترتیب در دسترس بودن داده‌ها به‌عنوان یکی از اهداف مهم امنیتی حفظ شود. استفاده از روش‌هایی با سربار محاسباتی کمتر و حذف گره‌های مخرب می‌تواند این ویژگی را تأمین کند.

۳)حداقل نرخ رها شدن بسته: بسیاری از گره‌های مخرب پس از دریافت بسته آن‌ها را رها کرده یا با ایجاد تأخیر در ارسال بسته سبب افزایش نرخ رها شدن بسته‌ها می‌شوند. بنابراین با حضور گره‌های مخرب در شبکه‌های بین خودرویی علی‌رغم بکارگیری روش‌هایی مانند رمزنگاری همچنان احتمال رها شدن بسته‌ها وجود دارد. بنابراین یک پروتکل مسیریابی مناسب، باید توانایی شناسایی گره‌های مخرب و حذف آن‌ها از فرآیند مسیریابی شبکه را به منظور پیشگیری از افزایش نرخ رها شدن بسته داشته باشد.

در این مقاله، یک پروتکل مسیریابی امن مبتنی بر موقعیت با استفاده از اعتماد جامع برای مناطق شهری ارائه شده است. در این پروتکل میزان اعتماد هر گره با توجه به نقش گره و عملکرد آن در ارسال پیام‌ها و همچنین توصیه‌ی سایر همسایه‌ها محاسبه می‌شود. در این پروتکل می‌توان با شناسایی گره‌هایی که از سطح اعتماد کمتری برخوردارند و عدم شرکت‌دهی آن‌ها در فرایند مسیریابی، نرخ تحویل بسته را تا حد زیادی بهبود بخشید. علاوه بر این، تشخیص رفتارهای مخرب و جلوگیری از مشارکت عوامل این فعالیت‌ها در فرایندهای شبکه، تأخیر انتها به انتها را کاهش خواهد داد.

جدول ۱- مقایسه مزایا و معایب مکانیزم‌های امنیتی در شبکه‌های بین خودرویی

مکانیزم	مزایا و معایب
مبتنی بر اعتماد	راه اندازی آسان
	حداقل پیچیدگی
	سربار محاسباتی کم
	کارایی در برابر حملات داخلی
	عدم کارایی در برابر تمام حملات
مبتنی بر رمزنگاری	راه اندازی مشکل
	پیچیدگی زیاد
	سربار محاسباتی بالا
	کارایی در برابر حملات داخلی و خارجی
	کارایی در برابر طیف وسیعی از حملات

۱.۱. حملات وارد به روش‌های مبتنی بر اعتماد

گره‌های مخرب در شبکه‌های بین خودرویی حملات متعددی را به‌منظور ایجاد اختلال یا از بین بردن سامانه‌ی مدیریت اعتماد به شبکه اعمال می‌کنند. همانطور که شکل ۲ نشان می‌دهد، حملات وارد بر روش‌ها یا پروتکل‌های مبتنی بر اعتماد به دو دسته‌ی کلی تقسیم می‌شوند. در یک دسته از این حملات گره‌های مخرب با تغییر رفتار خود، ارزیابی سایر گره‌ها از آن‌ها را با خطا مواجه می‌کنند. در دسته‌ی دیگری از این حملات، گره‌های مخرب با ارائه‌ی توصیه‌ی نادرست درباره‌ی سایر گره‌ها، شهرت آن‌ها را نزد سایر گره‌ها تغییر می‌دهند. حملاتی که به‌وسیله‌ی گره‌های مخرب به سامانه‌ی مدیریت اعتماد اعمال می‌شوند به‌طورکلی با مفهوم اعتماد مرتبط هستند. این حملات به شرح زیر هستند.

حمله فرصت طلبانه[۱۷]: در این حمله به محض اینکه یک گره متوجه می‌شود که اعتماد خود را از دست داده، رفتار خود را تغییر می‌دهد.

حمله خاموش-روشن[۱۸]: در این حمله یک گره لزوماً به‌طور دائمی رفتار مخرب نخواهد داشت. بلکه گره‌ها به شکل هوشمندانه عمل کرده و رفتار خود را بین خوب و بد تغییر می‌دهند. این حمله، حمله‌ی روشن-خاموش نامیده می‌شود و به مهاجمان اجازه می‌دهد تا اهداف سودجویانه‌ی خود را بدون شناسایی به شبکه اعمال کرده و سپس از آن خارج شوند.

حمله رفتار متناقض[۱۹]: در این روش گره‌های مخرب با گره‌های دیگر رفتاری متناقض دارند و به برخی از گره‌ها اطلاعات درست و به برخی دیگر اطلاعات نادرست می‌دهند. همچنین گره‌های مخرب در این حمله می‌توانند برای دستیابی به اهداف سودجویانه‌ی خود نظرات نادرستی را درباره‌ی سایر گره‌ها به همسایگان خود ارائه دهند [۵].

حمله تازه وارد[۲۰]: در این حمله گره‌ی مخرب به‌منظور تازه کردن سطح اعتماد خود، با هویت جدید وارد سیستم می‌شود. به‌این‌ترتیب پیشینه‌ی بد یک گره از بین می‌رود [۶].

حمله رفتار هوشمندانه[۲۱]: در این حمله یک گره با پیشنهادهای نادرست یا درست و خدمات خوب یا بد تا پیش از رسیدن به حد آستانه‌ی قابل اعتماد ماندن، تغییر رفتار می‌دهد. این حمله می‌تواند با توجه به مقدار آستانه‌ی اعتماد منجر به شکسته شدن چارچوب اعتماد شود [۷].

حمله خوب‌گویی[۲۲]: این حمله به‌منظور افزایش شانس گره‌های مخرب برای انتخاب شدن به‌عنوان گره‌ی بعدی با ارائه‌ی پیشنهادهای خوب درباره‌ی آن‌ها انجام می‌شود.

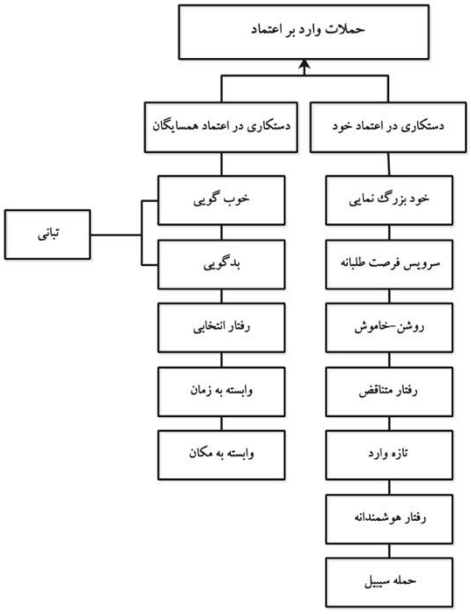
حمله بدگویی[۲۳]: در حمله‌ی بدگویی، گره‌های مخرب با ارائه‌ی پیشنهادهای منفی درباره‌ی یک گره، شانس انتخاب شدن آن‌را کاهش می‌دهند.

حمله رفتار انتخابی[۲۴]: در این حمله، برخی از گره‌ها از روی عمد درباره‌ی برخی دیگر از گره‌ها گزارش اشتباه می‌دهند، در حالیکه با سایر گره‌ها چنین رفتاری ندارند.

حمله وابسته به زمان[۲۵]: در حمله‌ی وابسته به زمان پیشنهاد یک گره با تغییر زمان متفاوت خواهد شد. در این حمله یک گره منتظر فرصتی مناسب برای ارائه‌ی پیشنهادهای نادرست است.

حمله وابسته به مکان[۲۶]: در این حمله پیشنهاد یک گره وابسته به مکان است و بازخورد آن با تغییر مکان تغییر خواهد کرد.

حمله‌ی خود بزرگ‌نمایی[۲۷]: در این حمله گره‌های مخرب تلاش می‌کنند از راه‌های مختلف، شهرت خود را ارتقا دهند. اما پس از انتخاب شدن ارائه‌ی خدمات را متوقف کرده یا خدمات نامطلوب ارائه می‌دهند [۸].



شکل ۲- حملات وارد بر مکانیزم‌های مبتنی بر اعتماد

ساختار مقاله به این ترتیب سازماندهی شده است. بخش ۲ به بررسی کارهای مرتبط می‌پردازد. در بخش ۳ یک پروتکل مسیریابی مبتنی بر اعتماد و مفاهیم اصلی آن ارائه می‌شود. در بخش ۴ شبیه‌سازی و ارزیابی پروتکل پیشنهادی ارائه شده و در آخر، نتیجه‌گیری پژوهش مورد بحث قرار می‌گیرد.

۲. کارهای مرتبط

در سال‌های اخیر، استفاده از روش‌های مبتنی بر اعتماد در مسیریابی شبکه‌های بین خودرویی به دلیل عدم پیچیدگی، سربار محاسباتی پایین و عدم تأخیر در ارسال پیام‌ها نسبت به روش‌های مبتنی بر رمزنگاری، مورد توجه پژوهشگران قرار گرفته است. در پژوهش‌های انجام شده از دو رویکرد اصلی شامل اعتماد مستقیم[۲۸] و اعتماد غیر مستقیم[۲۹] جهت ارزیابی اعتماد استفاده شده است.

اعتماد مستقیم: اعتماد مستقیم به‌عنوان اعتماد یک گره به گره‌ی دیگر جهت انجام خدمات خاص تعریف می‌شود [۹]. اعتماد مستقیم در واقع پیش‌بینی یک گره درباره‌ی رفتار آینده‌ی گره‌های دیگر است [۱۰]. این مقدار می‌تواند با ارزیابی داده‌های دریافتی از یک گره [۱۱] و یا با توجه به کیفیت تعاملات گذشته‌ی دو گره با یکدیگر تعیین شود. بنابراین در صورت وجود تجربه‌ی ارتباط بین یک جفت گره می‌توان نتایج حاصل از آن را در شاخص ارزیابی اعتماد این گره‌ها در نظر گرفت. اعتماد مستقیم در بیشتر موارد با محاسبه‌ی داده‌های حاصل از عملکرد یک گره که شامل نرخ تحویل و ارسال صحیح بسته‌ها هستند به‌دست می‌آید. البته در برخی

پژوهش‌ها [۱،۱۱،۱۲،۱۳] فاکتورهای امنیتی دیگری را نیز در ارزیابی اعتماد مستقیم لحاظ کرده‌اند. بنابراین برای ارزیابی دقیق‌تر سطح اعتماد مستقیم می‌توان به‌جای استفاده از یک یا دو معیار اعتماد، از چندین معیار متفاوت با ویژگی‌های کلیدی استفاده کرد [۱] که اصطلاحاً به آن اعتماد چند وجهی می‌گویند. البته به‌دلیل اینکه شبکه‌های بین خودرویی تحرک بالایی دارند و ساختار آن‌ها دائما تغییر می‌کند، اعتماد برای یک بازه‌ی زمانی بسیار کوتاه بین گره‌ها ایجاد می‌شود. لذا محاسبه و ارزیابی اعتماد براساس چندین عامل مختلف چالش برانگیزتر و دشوارتر است [۹]. به‌دلیل اینکه اعتماد مستقیم نرخ رشد آهسته‌ای دارد و تحت تأثیر تجربیات حاصل از تعاملات گذشته دو گره با یکدیگر است، محاسبه و به‌روزرسانی آن پیچیدگی‌هایی دارد. به همین دلیل در برخی از پژوهش‌ها [۱۰] مقدار اعتماد مستقیم تنها پس از تغییر تعامل بین دو گره به‌روزرسانی می‌شود. در صورتی‌که دو گره در گذشته با یکدیگر تعاملی نداشته باشند یا مقدار اعتماد مستقیم ارزیابی شده از حد آستانه کمتر باشد می‌توان به اعتماد غیرمستقیم (پیشنهادی) تکیه کرد.

اعتماد غیرمستقیم: برای پیشگیری از یک طرفه بودن ارزیابی اعتماد، از اعتماد غیرمستقیم که در قالب پیشنهاد حاصل از چندین دیدگاه ارائه می‌شود، استفاده می‌کنند. یک گره تنها زمانی می‌تواند در فرایند ارتباطات شبکه‌های بین خودرویی شرکت کند که برای سایر گره‌های شبکه نیز قابل اعتماد باشد و نیازمندی‌های اعتماد را تأمین کند. اگر بین یک جفت گره رابطه‌ی موفقیت‌آمیز در گذشته وجود داشته باشد آنها می‌توانند یکدیگر را به سایر اعضای شبکه نیز توصیه کنند [۱۴]. به‌دلیل اینکه الزامات و نیازمندی‌های دخیل در ارزیابی سطح اعتماد برای یک موجودیت توسط گره‌های مختلف متفاوت است مقدار اعتماد محاسبه‌شده برای هر گره توسط گره‌های دیگر نیز می‌تواند متفاوت باشد [۱۴]. از آنجایی‌که همواره اختلافی بین صرفه‌جویی در زمان برای تصمیم‌گیری سریع و انتظار برای دریافت تمام نظرات جهت تصمیم‌گیری دقیق وجود دارد، محاسبه‌ی اعتماد غیرمستقیم یک فرایند پرچالش در حوزه اعتماد مبتنی بر موجودیت‌ها محسوب می‌شود. خودروها دائما با این معضل روبرو هستند که آیا پس از دریافت پیام فوراً تصمیم‌گیری کنند یا منتظر دریافت نظرات بیشتر از سایر وسایل نقلیه بمانند. اگر وسایل نقلیه بلافاصله تصمیم‌گیری کنند ممکن است برخی نظرات مهم را از دست بدهند و اگر برای دریافت نظرات بیشتر از سایر همسایه‌ها صبر کنند، زمان زیادی به هدر می‌رود. برای حل این مشکل راه‌حل‌های مختلفی توسط پژوهشگران ارائه شده‌است. در پروتکل پیشنهادی تلاش کرده‌ایم با استفاده از ضرایب متغیر در محاسبه‌ی اعتماد، یک پروتکل مسیریابی پویا برای تعیین سطح اعتماد یک گره ارائه دهیم. در ادامه به مروری از خلاصه‌ی فعالیت‌های اخیر در روش‌های مبتنی بر اعتماد پرداخته می‌شود.

ژوانشیا یائو و همکاران یک روش اعتماد مبتنی بر موجودیت و براساس وزن ارائه داده‌اند. روش پیشنهادی آنها، انواع کاربردها و سطح اقتدار گره‌ها را در محاسبه‌ی مقدار اعتماد هر گره لحاظ می‌کند [۱۰]. عمر فاروق و همکاران یک رویکرد اعتماد چند وجهی مبتنی بر موجودیت ارائه داده‌اند که در آن تجربه، اولویت و نظر اکثریت در محاسبه‌ی مقدار اعتماد هر گره در نظر گرفته می‌شود. هسته‌ی مرکزی این رویکرد، اعتماد مبتنی بر نقش و نظر اکثریت است که در قالب اعتماد مبتنی بر اولویت با یکدیگر ادغام شده‌اند [۱]. سیری گولنگ و همکاران نیز یک روش اعتماد جامع را با استفاده از قوانین فازی جهت ارزیابی مقدار اعتماد همسایگان یک هاپ ارائه داده‌اند. در روش آن‌ها، مقدار اعتماد مستقیم با استفاده از سه معیار همکاری، صداقت و مسئولیت‌پذیری و مقدار اعتماد غیرمستقیم با استفاده از یادگیری ماشین به‌دست می‌آید [۱۲]. مامتاج و همکاران یک روش اعتماد مبتنی بر موجودیت را با در نظر گرفتن حداقل زمان تحویل پیام به مقصد ارائه داده‌اند. در این روش گره‌ی مورد اعتماد براساس دانش قبلی در مورد همسایگان انتخاب می‌شود و پس از آن، حداقل زمان تحویل پیام به مقصد در گره محاسبه می‌شود و در نهایت مسیری که بالاترین سطح اعتماد و حداقل زمان تأخیر در تحویل پیام را دارد به‌عنوان گره‌ی بعدی انتخاب می‌شود [۱۵].

شارما و همکاران نیز یک مدل مبتنی بر اعتماد جهت شناسایی گره‌های مخرب ارائه داده‌اند. در این روش بر خلاف سایر روش‌ها، به جای اینکه هر گره نقش ناظر را ایفاء کند، تنها گره‌هایی که از مقدار اعتماد بالایی برخوردار باشند نقش نظارت بر رفتار سایر گره‌ها را به عهده می‌گیرند. مقدار اعتماد مستقیم در این روش براساس عملکرد هر گره در ارسال پیام‌ها محاسبه می‌شود [۲]. کلدیپ و همکاران یک الگوریتم مبتنی بر شهرت ارائه داده‌اند. در این الگوریتم با استفاده از نرخ تحویل بسته‌ها، گره‌های مخرب و فعالیت‌های آن‌ها در شبکه شناسایی می‌شوند [۱۳]. همسا و همکاران یک چارچوب امنیتی مبتنی بر تحلیل رفتار وسایل نقلیه پیشنهاد داده‌اند که از یک مدل اعتماد ترکیبی و یک سیستم تشخیص رفتار نادرست تشکیل شده است. در این روش یک معیار اعتماد با توجه به رفتار گره به آن اختصاص داده می‌شود. با استفاده از این معیار، وسایل نقلیه به دو گروه مخرب و درستکار طبقه‌بندی می‌شوند [۱۱]. در مقاله‌ی [۱۶] جونکسیا ما و چن یانگ یک پروتکل مسیریابی پایدار مبتنی بر اعتماد به نام TBSR ارائه داده‌اند. در این پروتکل هر گره پس از رسیدن به حد آستانه‌ی اعتماد می‌تواند به‌عنوان گره‌ی بعدی انتخاب شود. برای ارزیابی اعتماد در این مدل از سطح اعتماد نقش هر گره، اعتماد چاپگر تعاملی و اعتماد توصیه شده توسط همسایه‌ها استفاده می‌شود. علاوه بر این، جهت ادغام نظرات توصیه شده توسط گره‌های همسایه، از یک الگوریتم تحلیل سلسله مراتبی استفاده می‌شود.

هوی شیا و همکاران [۱۷] یک پروتکل مسیریابی چند بخشی مبتنی بر اعتماد با نام TMR برای دفاع از شبکه در برابر حملات متعدد و بهبود کارایی مسیریابی پیشنهاد داده‌اند. در پروتکل TMR، محاسبه‌ی اعتماد مستقیم براساس نظریه‌ی بیز و محاسبه‌ی اعتماد غیرمستقیم براساس اعتبار و فعالیت انجام می‌شود. در این پروتکل، در نهایت مقدار اعتماد کل در یک گره با استفاده از قوانین فازی به‌دست می‌آید. به این ترتیب، با استفاده از اعتماد محاسبه شده برای هر گره، خودروهای مخرب از فرایند ایجاد و نگهداری مسیر حذف خواهند شد و مسیرهای قابل اعتماد جهت تحویل داده ایجاد می‌شوند. در [۱۸] یک پروتکل مسیریابی امن مبتنی بر اعتماد ارائه شده است. این پروتکل به منظور ایجاد مسیریابی مورد اعتماد و بهینه، گره‌ای که بیشترین امتیاز را نسبت به همسایگان خود کسب کرده است انتخاب می‌کند. امتیاز هر گره با استفاده از جمع وزن‌دار پویای مؤلفه‌های جغرافیایی و اعتماد محاسبه می‌شود.

۳. پروتکل پیشنهادی

مسیریابی یکی از فرایندهای مهم در شبکه‌های بین خودرویی است که به‌منظور بهبود کارایی شبکه با انتخاب مناسب‌ترین مسیر، بسته‌های حاوی اطلاعات حیاتی را از مبدأ به مقصد ارسال می‌کند [۱۹]. ارسال صحیح و بدون تأخیر پیام ها از اهمیّت بالایی در این شبکه‌ها برخوردار است. شبکه‌های بین خودرویی یک رسانه‌ی انتقال باز و حاوی گره‌هایی با حرکت خودسرانه هستند. مکاتبات فاقد مکانیسم‌های امنیتی در این شبکه‌ها، یکی از عوامل زمینه‌ساز برای اعمال حملات مختلف به این شبکه‌ها محسوب می‌شود . این شبکه‌ها، به منظور افزایش امنیت ارتباطات و به‌دنبال آن بهبود کارایی شبکه نیازمند مشارکت وسایل نقلیه‌ی قابل اعتماد در فرآیند مسیریابی هستند. در این مقاله، یک پروتکل مسیریابی امن مبتنی بر اعتماد جامع به منظور افزایش امنیت در ارتباط خودرو با خودرو در مناطق شهری ارائه شده است که براساس پروتکل‌های مسیریابی مبتنی بر موقعیت طراحی شده است. در پروتکل پیشنهادی، علاوه بر مقدار اعتماد جامع، معیارهای مؤثر در پروتکل GPSR نظیر سرعت، فاصله و جهت نیز در انتخاب یک گره لحاظ می‌شوند. پروتکل GPSR تنها با استفاده از اطلاعات مربوط به همسایه‌های یک گره و از طریق رویکرد حریصانه نسبت به انتخاب گره‌ی بعدی اقدام می‌کند [۲۰]. در واقع پروتکل پیشنهادی مدل بهبودیافته و ایمن شده‌ی پروتکل GPSR با استفاده از مسیریابی مبتنی بر اعتماد

است. اطلاعات مورد استفاده از طریق پیام‌های دوره‌ای بین همسایه‌های حاضر در یک محدوده‌ی رادیویی به اشتراک گذاشته می‌شود. در این پروتکل مقدار اعتماد مستقیم با استفاده از سوابق یک گره در ارسال بسته‌ها و سطح امنیتی نقش هر گره محاسبه می‌شود و مقدار اعتماد غیرمستقیم، حاصل نظر همسایه‌های گره‌ی مورد نظر از تعاملات پیشین خود با آن گره خواهد بود. جهت داشتن یک پروتکل پویا و در نظر گرفتن طیف گسترده‌تری از حالت‌ها، ضرایب متغیری در محاسبه‌ی گره‌ی ایده‌آل لحاظ شده است.

۱.۳ مدل شبکه در پروتکل پیشنهادی

در این پروتکل، گره‌های شبکه از طریق تبادل پیام‌های دوره‌ای از آخرین وضعیت همسایه‌های خود مطلع می‌شوند. همانطور که شکل ۳ نشان می‌دهد، ساختار پیام‌های دوره‌ای در این پروتکل متشکل از آدرس گره‌ی ارسال کننده، سرعت، جهت، موقعیت، نقش گره و شماره ترتیب جهت اثبات تازگی پیام است. پیام‌های دوره‌ای هر ۱ ثانیه بین گره‌های همسایه مبادله می‌شوند. در این فرایند هر گره پس از دریافت پیام، ابتدا آدرس ارسال کننده‌ی بسته را جهت تطبیق آن با آدرس‌های موجود در جدول همسایه‌های خود استخراج می‌کند. وجود آدرس ارسال کننده‌ی پیام در جدول همسایه‌های گره‌ی دریافت کننده، نشان دهنده‌ی وجود تعاملات پیشین بین آن دو گره است. جهت به‌روزرسانی اطلاعات موجود، لازم است تازگی پیام دریافتی از طریق مقایسه‌ی آخرین توالی اعداد ذخیره شده با توالی اعداد دریافتی تأیید گردد. در صورتی‌که توالی اعداد بسته‌ی دریافت شده از توالی اعداد آخرین بسته‌ی دریافتی بزرگتر باشد، اطلاعات گره در جدول به‌روزرسانی می‌شوند و در غیر این‌صورت بسته نادیده گرفته می‌شود. در صورت عدم مشاهده‌ی آدرس ارسال کننده‌ی بسته، مقدار آن به‌عنوان آدرس جدید توسط گره‌ی دریافت کننده‌ی بسته به جدول افزوده می‌شود. به‌منظور جلوگیری از ایجاد سربار شبکه، مقادیر تعیین‌شده در جدول اعتماد هر گره، تنها پس از قرارگیری مجدد دو گره در محدوده‌ی رادیویی یکدیگر به‌روزرسانی می‌شوند. بر این اساس زمانی‌که دریافت پیام دوره‌ای از یک گره در زمان مشخص متوقف شود، نشان‌دهنده‌ی خروج آن گره از محدوده‌ی رادیویی گره‌ی دیگر است. بنابراین به‌روزرسانی مقادیر درج شده در جدول اعتماد تا قرارگیری مجدد آن‌ها در محدوده‌ی انتقال یکدیگر متوقف خواهد شد. با مشاهده‌ی عملکرد هر گره پس از دریافت بسته، نرخ تحویل بسته‌ی مربوط به آن گره به‌وسیله‌ی گره‌ی قبلی محاسبه و در جدول مربوطه به‌روزرسانی می‌گردد. در ادامه به نحوه‌ی انتخاب گره‌ی ایده‌آل برای مسیریابی، محاسبه‌ی اعتماد جامع و مؤلفه‌های مؤثر در سطح اعتماد هر گره پرداخته می‌شود.

شماره ترتیب	نقش	سرعت	جهت	موقعیت	آدرس مبدأ

شکل ۳- ساختار پیام دوره‌ای در پروتکل پیشنهادی

پروتکل پیشنهادی دارای دو حالت حریصانه و محیطی[۳۰] برای ارسال بسته است که به وسیله‌ی ستون مرتبط با حالت ارسال[۳۱] در ساختار بسته‌های داده مشخص می‌شود. همانطور که شکل ۴ نشان می‌دهد، حالت ارسال بسته براساس مقادیر داده شده به ستون حالت حریصانه در ساختار بسته‌های داده تعیین می‌گردد. در صورتیکه بسته در حالت حریصانه ارسال شود به این ستون مقدار ۱ داده می‌شود و در صورتی که بسته در حالت محیطی ارسال شود، به آن مقدار ۰ داده می‌شود.

شماره ترتیب	حالت حریصانه	موقعیت مقصد	داده	آدرس گام قبلی	آدرس مقصد	آدرس مبدأ

شکل ۴- ساختار بسته‌های داده در پروتکل پیشنهادی

۲.۳.انتخاب گره‌ی ایده‌آل در حالت حریصانه

انتخاب گره‌ی ایده‌آل جهت ارسال بسته‌ها، توسط مبدأ یا گره‌های ارسال کننده‌ی واسط انجام می‌شود. هر گره با استفاده از سیستم موقعیت‌یاب جهانی از موقعیت خود مطلع است و پیش از ارسال بسته به‌وسیله‌ی خدمات مکان‌یابی شبکه، نسبت به موقعیت مقصد نیز آگاهی پیدا می‌کند. در بسیاری از مواقع فرایند ارسال اطلاعات هنگام مسیریابی به‌وسیله‌ی چندین گره‌ی میانی صورت می‌گیرد. بنابراین هر گره با استفاده از معادله (۱) نسبت به محاسبه امتیاز همسایه kام خود اقدام کرده و در نهایت همسایه با امتیاز بالاتر را به عنوان گره‌ی بعد از خود انتخاب می‌کند. با توجه به معادله (۱)، سرعت، فاصله، جهت و مقدار اعتماد جامع در انتخاب گره‌ی بعدی مؤثر خواهند بود.

$$Rank_k = S_k \times W_S + \frac{1}{Dist_k} \times W_{Dist} + CT_k \times W_{CT} + D_k \times W_D \quad (۱)$$

$$W_S + W_{Dist} + W_{CT} + W_D = 1$$

در این معادله، $Rank_k$ معرّف امتیاز همسایه kام است. S_k، CT_k، $Dist_k$ و D_k به ترتیب سرعت، فاصله تا مقصد، مقدار اعتماد جامع و جهت همسایه k را تعریف می‌کنند. در این فرمول به هر مؤلفه یک وزن پویا $(W_D, W_{CT}, W_{Dist}, W_S)$ اختصاص داده می‌شود. هدف از استفاده‌ی وزن‌های پویا در انتخاب گره‌ی بعدی، در نظر گرفتن طیف گسترده‌تری از حالت‌ها توسط هر گره است. برای مثال در صورتی‌که ارسال سریع بسته از اهمیت بیشتری نسبت به ارسال بسته در یک مسیر امن برخوردار باشد، یک گره می‌تواند وزن بیشتری را به مؤلفه‌های موقعیت و سرعت برای انتخاب گره‌ی بعدی اختصاص دهد. در مقابل، اگر ارسال اطلاعات در یک مسیر امن از اهمیت بیشتری برخوردار باشد، وزن بیشتری به اعتماد جامع اختصاص داده می‌شود. به‌همین ترتیب می‌توان با تعریف وزن‌های برابر، اهمیت یکسانی برای تمامی مؤلفه‌ها در نظر گرفت. به‌دلیل تصمیم‌گیری چند معیاره با واحدهای متفاوت لازم است تا داده‌های ورودی برای محاسبه امتیاز یک همسایه، بی مقیاس‌سازی شوند. در پروتکل پیشنهادی از بی‌مقیاس‌سازی مستقیم برای این منظور استفاده شده است. این روش مقایسه اعداد را ساده‌تر می‌کند. در بی‌مقیاس سازی مستقیم ترجیح گزینه‌ها به یکدیگر قبل و بعد از عملیات بی‌مقیاس‌سازی ثابت باقی می‌ماند. به عنوان مثال در معادله (۲)، مقدار S'_k مقدار بی‌مقیاس شده برای سرعت همسایه kام (S_k) از بین m همسایه را نشان می‌دهد. پس از بی‌مقیاس‌سازی، جمع سرعت بی‌مقیاس‌ساز شده برای کل همسایه‌ها یک خواهد شد.

$$S'_k = \frac{S_k}{\sum_{i=1}^{m} S_i} \quad (۲)$$

۱.۲.۳ محاسبه‌ی موقعیت هر گره

برای محاسبه‌ی موقعیت هر گره و فاصله‌ی آن تا مقصد، از معادله‌ی (۳) استفاده می‌شود. با توجه به اینکه پروتکل پیشنهادی برای مسیریابی از رویکرد حریصانه استفاده می‌کند، هرچقدر فاصله‌ی یک گره تا مقصد کمتر باشد، گره‌ی پیشنهادی از امتیاز بالاتری برخوردار خواهد بود.

$$Dist = \sqrt{(x_z - x_{dest})^2 + (y_z - y_{dest})^2} \quad (۳)$$

۲.۲.۳.محاسبه‌ی زاویه‌ی هر گره

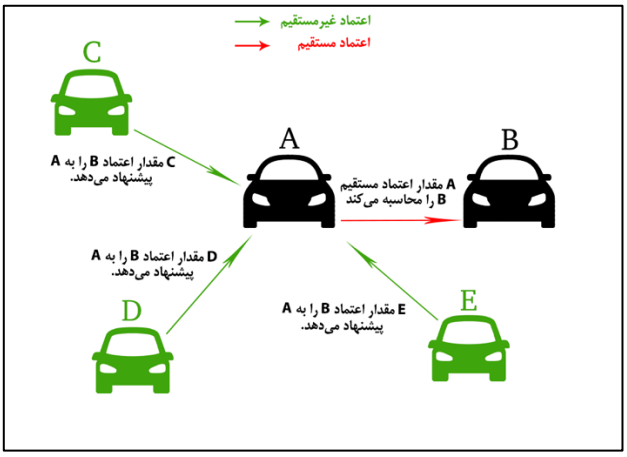
زاویه‌ی هر گره نسبت به مقصد نیز یکی از مؤلفه‌های مهم در محاسبه‌ی امتیاز هر گره محسوب می‌شود. به منظور محاسبه‌ی زاویه‌ی هر گره نسبت به مقصد از معادله‌ی (۴) استفاده می‌شود. در معادله‌ی (۴) V_{V_z}، بردار سرعت هر وسیله‌ی نقلیه است و $LOC_{V_z,dest}$ بیانگر بردار جهت گره‌ی V_{V_z} نسبت به وسیله‌ی نقلیه مقصد است. $(V_{V_z})(LOC_{V_z,dest})$ نیز نشان‌دهنده‌ی ضرب نقطه‌ای دو بردار است. $\|V_{V_z}\|$ و $\|LOC_{V_z,dest}\|$ نیز به ترتیب، طول V_{V_z} و $LOC_{V_z,dest}$ را نشان می‌دهند. اگر حاصل این معادله برابر صفر یا نزدیک به صفر شود یعنی گره‌ی مورد نظر در راستای مقصد حرکت می‌کند. در صورتیکه حاصل معادله برابر یا نزدیک به ۹۰ درجه شود، نشان‌دهنده‌ی عدم حرکت دو گره در یک جهت بوده و در صورتیکه حاصل معادله برابر ۱۸۰ درجه باشد، بیانگر حرکت دو گره در خلاف جهت یکدیگر است.

$$\theta_{V_z}=cos^{-1}\frac{(V_{V_Z})(LOC_{V_Z,dest})}{\|V_{V_Z}\|\|LOC_{V_Z,dest}\|} \quad (۴)$$

۳.۲.۳.محاسبه‌ی اعتماد جامع جهت انتخاب گره

همانطور که شکل ۵ نشان می‌دهد جهت ارزیابی سطح اعتماد هر گره در انتخاب گره‌ی ایده‌آل، از اعتماد جامع با تکیه بر موجودیت‌های شبکه استفاده می‌شود. با توجه به معادله (۵)، اعتماد جامع در واقع ترکیبی از اعتماد مستقیم (DT) و اعتماد غیرمستقیم (RT) است. با توجه به سوابق هر گره از تعاملات پیشین خود با گره‌ی مورد نظر، ضرایب متغیری (W_{RT}،W_{DT}) در محاسبه‌ی اعتماد جامع در نظر گرفته می‌شود. همیشه مصالحه‌ای بین انتظار برای دریافت نظرات بیشتر از همسایه‌ها با تصمیم‌گیری فوری و صرفه‌جویی در زمان نیاز است که به کمک وزن‌های پویا می‌توان آن را اعمال کرد. بر این اساس در صورتی‌که دو گره در گذشته تعاملات زیادی با یکدیگر برقرار کرده و هرکدام از آنها سطح اعتماد بالایی نسبت به یکدیگر داشته‌باشند، می‌توانند $W_{RT}=0$ (وزن پویای اعتماد غیر مستقیم) در نظر گرفته و مقدار کلی ضرایب پویا را به اعتماد مستقیم اختصاص دهند. به همین ترتیب این مقادیر از سوی هر گره قابل تغییر بوده و می‌توان مقادیری براساس نیاز به آن‌ها اختصاص داد.

$$CT = DT \times W_{DT} + RT \times W_{RT} \quad (۵)$$
$$W_{DT} + W_{RT} = ۱$$



شکل ۵- اعتماد جامع در شبکه‌های بین خودرویی

محاسبه‌ی اعتماد مستقیم

در این پروتکل مقدار اعتماد مستقیم برای هر گره به‌وسیله‌ی سطح امنیتی نقش گره‌ی مورد نظر و نرخ تحویل موفقیت‌آمیز بسته‌ها توسط آن گره محاسبه می‌شود. هر گره مقدار اعتماد مستقیم برای همسایه‌های خود را به‌وسیله‌ی آخرین اطلاعات ذخیره شده از آن‌ها در جدول خود محاسبه می‌کند. مقدار اعتماد مستقیم برای هر گره به‌وسیله‌ی معادله (۶) محاسبه می‌شود. PFR و $Role$ به ترتیب نشان دهنده‌ی نرخ تحویل بسته و نقش هر گره است که در وزن‌های پویای W_{PFR} و W_{Role} ضرب می‌شوند. در ادامه به پارامترهای مؤثر در ارزیابی اعتماد پرداخته می‌شود.

$$DT=PFR \times W_{PFR}+Role \times W_{Role} \quad (۶)$$
$$W_{PFR} + W_{Role} = ۱$$

الف)نقش گره: در پروتکل پیشنهادی سه ردیف نقش اصلی از دیدگاه امنیتی برای هر گره تعریف شده است. بر همین اساس با توجه به مسئولیت هریک از گره‌ها یک وزن امنیتی به آنها اختصاص داده می‌شود. با توجه به اینکه برای هر نقش سطح امنیتی خاصی در نظر گرفته می‌شود، از ماشین هایی که نقش یکسانی دارند رفتار مشابهی انتظار می‌رود به‌نحوی‌که هر گره پیش از هرگونه تعامل با سایر گره‌ها بتواند سطح اعتماد را در سایر گره‌ها با توجه به نقش آن‌ها تخمین بزند. سه نقش اصلی از بیشترین به کمترین تعریف شده‌است. ۱)گره‌های مرجع: مثل ماشین‌های پلیس، کنترل کنندگان ترافیک، واحدهای کنار جاده‌ای، ۲) خدمت دهندگان عمومی: مثل ماشین‌های آمبولانس، ماشین‌های آتش نشانی، ماشین‌های حمل‌ونقل عمومی، ماشین‌های نگهداری جاده و ۳) ماشین‌های تخصصی: ماشین‌های آموزش رانندگی، خودروهایی با بیش از ۱۰سال تجربه‌ی رانندگی ایمن و ماشین‌های محلی. جدول ۲ سطح اعتماد هر نقش را نشان می‌دهد.

جدول ۲- مقدار اعتماد نقش‌ها و داده‌ها

میزان اعتماد	وزن اعتماد
زیاد	۳
متوسط	۲
کم	۱

ب)نرخ ارسال داده‌های با ارزش: نرخ تحویل بسته نشان می‌دهد از تمام بسته‌های دریافت شده توسط یک گره چه تعدادی به گره‌ی بعدی ارسال شده‌اند [۱۳] و اندازه‌گیری آن در این پروتکل به‌عنوان یکی از پارامترهای محاسبه‌ی اعتماد مستقیم مبتنی بر موجودیت در نظر گرفته شده است. به‌طور کلی می‌توان گفت قابل اعتماد بودن یک گره با نرخ موفقیت‌آمیز تبادل پیام در آن گره ارتباط مستقیم دارد [۱۰].

در این روش هر گره می‌تواند پس از ارسال بسته به یک گره با استفاده از وضعیت بی‌حالت پیشرفته[۳۲] [۲۱، ۲۲]، رفتار آن گره را تا ارسال بسته به گره‌ی بعدی تحت نظر بگیرد. باید توجه داشت که برخی اوقات گره‌های خرابکار نرخ تحویل بسته‌ی بالای خود را از نقل و انتقال داده‌هایی با ارزش پایین (مثل داده‌های سرگرمی) در شبکه بدست می‌آورند. به همین دلیل علی‌رغم اهمیت این فاکتور در بررسی قابل اعتماد بودن یک گره، محاسبه‌ی اعتماد مستقیم صرفاً با در نظر گرفتن نرخ تحویل بسته از دقت کافی برخوردار نیست و لازم است وزن داده‌های ارسال شده از نظر ارزشی به شکل ضرایب پویا در محاسبه‌ی آنها لحاظ گردند. جدول (۲) مقدار اعتماد را برای سه سطح از داده‌ها نشان می‌دهد. نرخ تحویل بسته با استفاده از معادله (۷) و با در نظر گرفتن وزن داده‌ها محاسبه می‌شود. در این معادله n تعداد بسته‌هایی است که با موفقیت توسط یک گره ارسال شده است. m تعداد کل بسته‌هایی است که از یک گره درخواست شده تا ارسال شود و w ارزش هر بسته را

نشان می‌دهد. در واقع این معادله نسبت ارزش داده‌های ارسال شده به ارزش کل داده‌ها را بیان می‌کند.

$$PFR = \frac{\sum_{s=1}^{n} W_s}{\sum_{t=1}^{m} W_t}\ ,\ w = 1,2,or\ 3 \qquad (۷)$$

جهت تحلیل رفتار گره‌ها و جمع‌آوری اطلاعات در فرایند ارسال بسته‌ها از وضعیت بی‌حالت پیشرفته استفاده می‌شود. بطورکلی هر گره در شبکه تنها بسته‌هایی را که برایش ارسال شده یا پخش فراگیر شده است می‌پذیرد و سایر بسته‌ها را رد می‌کند (نادیده می‌گیرد). روش بی‌حالت این وضعیت را تغییر داده و به گره‌ها اجازه می‌دهد تا تمامی بسته‌هایی را که در محدوده‌ی رادیویی آنها قرار دارند، ضبط کنند. البته استفاده از این روش معایبی نیز دارد. در وضعیت بی‌حالت، هر گره با حجم زیادی از داده‌ها روبرو است که الزاماً تمامی بسته‌های دریافت شده برای گره‌ی دریافت کننده کارآمد نیستند. این امر باعث می‌شود که قدرت پردازشی و منبع انرژی زیادی هنگام دریافت تعداد زیادی از بسته‌ها مصرف شود و کارآمدی شبکه را به ویژه در مناطق شلوغ و پرترافیک کاهش دهد [۲۰]. علاوه بر این، ضبط و تجزیه و تحلیل تمام بسته‌های ارسال شده در محدوده‌ی رادیویی یک گره سبب به خطر افتادن محرمانگی به‌عنوان یکی از اهداف مهم امنیتی می‌شود. برای رفع این مشکل، در پروتکل مسیریابی مبتنی بر اعتماد ارائه شده از وضعیت بی‌حالت پیشرفته استفاده می‌شود. در چنین شرایطی هر گره فقط بسته‌هایی را که آدرس خودش را به‌عنوان گره‌ی قبلی در سرآمد آنها مشاهده کند، ضبط و تجزیه و تحلیل می‌کند [۲۱، ۲۲]. بنابراین هر گره می‌تواند پس از ارسال بسته، رفتار گره‌ی بعد از خود را تحت نظر داشته باشد و هر گونه سوءرفتار در فرایند ارسال بسته توسط گره‌ی بعدی را تشخیص دهد. این ماژول تنها هنگام مسیریابی فعال می شود و بطور موازی با فرایند مسیریابی بسته‌ها کار می‌کند. بنابراین هیچ بسته‌ای را در صف قرار نمی‌دهد. استفاده از این ماژول به‌دلیل عملکرد گزینشی آن مانع از مصرف غیرضروری انرژی و قدرت پردازشی می‌گردد. در وضعیت بی‌حالت پیشرفته، سرآمد هر بسته شامل آدرس گره‌ی قبلی خود است که امکان شناسایی آن را آسان می‌کند. با استفاده از این ماژول و در نظر گرفتن زمان خروج و ورود هر بسته می‌توان اطلاعات و خروجی‌های مد نظر را جمع‌آوری کرد. خروجی مورد نظر در پروتکل پیشنهادی، محاسبه‌ی نرخ تحویل صحیح بسته‌ها است.

محاسبه‌ی اعتماد غیرمستقیم

براساس معادله (۸) مقدار اعتماد غیرمستقیم با توجه به توصیه سایر گره‌ها محاسبه می‌شود. براین اساس هنگام انتخاب گره‌ی بعدی در فرایند مسیریابی، همسایه‌های گره‌ی کنونی، پیام درخواست توصیه توسط گره‌ی ارسال‌کننده، توصیه‌ی خود را درباره‌ی هر همسایه با رجوع به جدول اعتماد خود اعلام می‌کنند. نقش هر گره در شبکه تأثیر مستقیمی در مقدار اعتماد اعلام شده توسط آن گره دارد. در واقع هرچقدر یک گره از نقش معتبرتری برخوردار باشد، مقدار اعلام شده توسط آن گره ارزش بیشتری خواهد داشت. در معادله (۸)، O_r بیانگر نظر گره‌های همسایه و w_r ارزش وزنی است که با توجه به نقش گره تعریف می‌شود.

$$RT=\frac{\sum_{r=1}^{n} O_r \times W_r}{\sum w_r} \qquad (۸)$$

۳.۳.استراتژی بازیابی

هنگامی که گره‌ی ارسال کننده‌ی بسته، نزدیکترین گره به مقصد باشد با مشکل حداکثر محلی ناشی از نواحی خالی روبرو می‌شویم که یکی از چالش‌های اساسی در پروتکل‌های مسیریابی مبتنی بر موقعیت محسوب می‌شود. در چنین شرایطی گره‌ی ارسال‌کننده‌ی بسته نسبت به سایر همسایگان خود در کمترین فاصله نسبت به مقصد قرار دارد و از طرفی نمی‌توان از طریق یک گره به مقصد رسید. در این وضعیت پروتکل وارد حالت محلی شده و مسیریابی با استفاده از استراتژی بازیابی انجام می‌گیرد. استراتژی بازیابی دارای دو مرحله است. در مرحله‌ی اول به کمک نمودار همسایگی نسبی از ایجاد حلقه پیشگیری می‌شود و در مرحله‌ی بعد به ستون حریصانه در ساختار بسته مقدار صفر داده شده و با استفاده از قانون دست راست ارسال می‌گردد. قانون دست راست یک روش مرسوم برای خارج کردن پروتکل از حالت محیطی است که براساس آن، بسته برای نزدیکترین گره پس از گره‌ی فرستنده ارسال می‌شود. این وضعیت تا زمانی ادامه پیدا می‌کند که گره‌ی بعدی نسبت به گره‌ی شروع کننده‌ی وضعیت بی‌حالت در فاصله‌ی کمتری نسبت به مقصد قرار داشته باشد. به محض یافتن گره‌ای با فاصله‌ی نزدیک‌تر به مقصد، ستون حریصانه در ساختار بسته برابر ۱ قرار داده می‌شود و پروتکل به حالت حریصانه باز می‌گردد.

۴.۳.نحوه‌ی نگهداری از جدول اعتماد

همانطور که گفتیم در پروتکل پیشنهادی، هر گره پس از ارسال بسته‌ها بر اساس پروتکل مسیریابی ارائه شده، در وضعیت بی‌حالت پیشرفته قرار گرفته و رفتار گره‌ی بعدی خود را تحت نظر می‌گیرد تا بر اساس نحوه‌ی عملکرد گره‌ی بعدی در ارسال بسته به گام بعدی، مقدار نرخ ارسال بسته‌های مربوط به آن گره را به‌روزرسانی کند. در صورتیکه آدرس گره در جدول اعتماد وجود نداشته باشد، آدرس گره به همراه آخرین نرخ ارسال بسته در جدول ثبت خواهد شد تا در تعاملات بعدی به‌روزرسانی گردد. به‌روزرسانی اعتماد در پروتکل پیشنهادی مبتنی بر رویداد مشخص (ارسال بسته) است. بنابراین ارزش اعتماد در جدول تنها پس از قرارگیری هر گره در محدوده‌ی رادیویی گره‌ی دیگر و تبادل بسته، به‌روزرسانی می‌شوند. به‌همین دلیل به‌روزرسانی مقادیر درج‌شده در جدول اعتماد تا قرارگیری مجدد آن گره در محدوده‌ی انتقال و انجام تعامل مجدد، متوقف می‌گردد. به‌روزرسانی اعتماد بر اساس وقوع رویداد مشخص نقش مؤثری در کاهش سربار شبکه خواهد داشت. جدول ۳، پارامترهای موجود در جدول اعتماد هر گره را نشان می‌دهد. براین اساس جدول اعتماد هر گره، شامل آدرس گره‌های همسایه، نرخ ارسال بسته توسط آن‌ها، نقش گره‌ها و شمارنده‌ی تعاملات صورت گرفته است. وزن اختصاص داده شده به اعتماد مستقیم و غیرمستقیم در محاسبه‌ی اعتماد جامع، با توجه به تعداد تعاملات صورت گرفته تعیین می‌شود.

جدول ۳- پارامترهای جدول اعتماد

جدول اعتماد
آدرس گره
نرخ ارسال بسته‌ها
نقش گره‌ها
شمارنده‌ی تعاملات

۴. شبیه‌سازی و ارزیابی

شبیه‌سازی این مقاله با استفاده از نرم‌افزار NS-2.35 در سیستم عامل Ubuntu ۱۶.۰۴ روی ماشین مجازی Virtualbox انجام شده است. همانطور که شکل ۶ نشان می‌دهد، فضای شهری در این شبیه‌سازی با استفاده از نرم‌افزار SUMO ایجاد شده است. ابعاد فضای شبیه‌سازی ۹۰۵ متر در ۸۰۷ متر است. تعداد خودروها در شروع شبیه‌سازی ۱۰۰ عدد در نظر گرفته می‌شود. در جدول ۴ مقادیر بکار رفته در شبیه‌سازی نشان داده شده‌است.

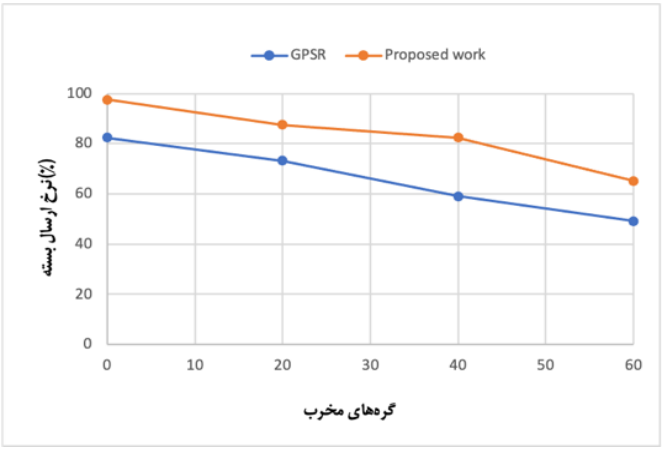
شکل ۶- فضای شهری ایجاد شده در نرم‌افزار SUMO

با کمک نرم‌افزار NS-2 عملکرد پروتکل پیشنهادی در برابر حملات رها کردن بسته‌ها (حمله‌ی سیاه چاله و حمله‌ی حفره‌ی خاکستری) با پروتکل GPSR در شرایط مشابه مورد ارزیابی قرار گرفته است. بدین منظور عملیات شبیه‌سازی یک‌بار بدون حضور گره‌های مخرب اجرا شده است و نتایج حاصل از عملکرد پروتکل پیشنهادی با پروتکل GPSR مقایسه شد. سپس عملیات شبیه‌سازی مجدداً اجرا شده و در هر مرحله به ترتیب ۲۰ درصد، ۴۰ درصد و ۶۰ درصد گره‌ی مخرب با هدف اجرای حملات رها کردن بسته‌ها به شبکه وارد شدند. در ابتدا عملکرد پروتکل پیشنهادی در حضور ۲۰ درصد گره‌ی‌مخرب با پروتکل GPSR در وضعیت مشابه مقایسه و ارزیابی می‌شود. سپس مقدار گره‌های مخرب در هر دو پروتکل به ترتیب ۴۰ درصد و ۶۰ درصد تعریف شده و نتایج حاصل از عملکرد آن‌ها با یکدیگر مقایسه می‌شوند. جهت تحلیل و ارزیابی عملکرد پروتکل پیشنهادی در مقایسه با پروتکل GPSR تحت حملات رها کردن بسته‌ها، از دو مؤلفه‌ی نرخ تحویل بسته‌ها و تأخیر انتها به انتها استفاده می‌شود.که در ادامه به آن‌ها می‌پردازیم.

جدول ۴- پارامترهای شبیه‌سازی

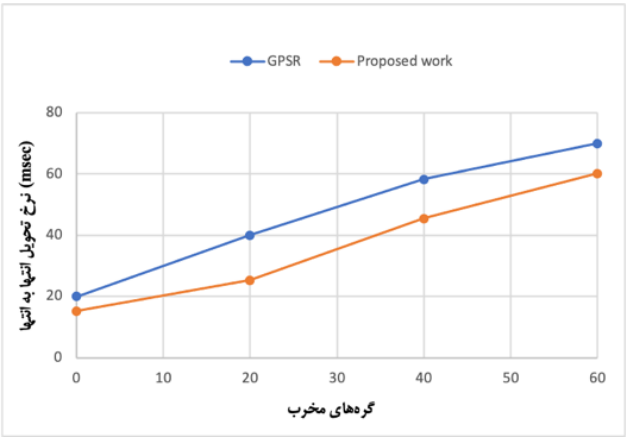
پارامترهای شبیه‌سازی	مقدار
ابزار شبیه‌سازی	NS 2.35
مولد تحرک و پویایی	SUMO
بستر شبیه‌سازی	Ubunto-16.04.7
محیط شبیه‌سازی	شهری
ابعاد فضای شبیه‌سازی	807m×905m
سرعت وسایل نقلیه	30m/s-70m/s
MAC	۸۰۲.۱۱p
پروتکل مسیریابی	مبتنی بر موقعیت
تعداد وسایل نقلیه	۱۰۰
مدل انتشار	Shadowing
محدوده‌ی انتقال	300m
طول وسایل نقلیه	۴ متر
تعداد گره‌های مخرب	20, 40, 60

نرخ تحویل بسته: نرخ تحویل بسته‌ها نشان دهنده‌ی تعداد بسته‌هایی است که با موفقیّت به مقصد رسیده‌اند. هر چقدر نرخ تحویل بسته‌ها بالاتر باشد، عملکرد شبکه بهتر است. برای تحلیل و بررسی نرخ تحویل بسته، عملکرد پروتکل پیشنهادی و پروتکل GPSR یک‌بار بدون گره‌های مخرب و سپس با حضور تعدادی گره‌ی مخرب (۲۰، ۴۰ و ۶۰) با یکدیگر مقایسه شدند. همانطور که شکل ۷ نشان می‌دهد با افزایش تعداد گره‌های مخرب، عملکرد پروتکل GPSR در مقایسه با پروتکل پیشنهادی از نظر نرخ ارسال بسته‌ها کاهش پیدا می‌کند. به‌دلیل عدم استفاده از مسیریابی امن در پروتکل GPSR کلاسیک، تعداد زیادی از بسته‌ها رها می‌شوند در نتیجه نرخ تحویل بسته‌ها کاهش پیدا می‌کند. پروتکل پیشنهادی پس از قرارگیری در معرض حملات رها کردن بسته، نرخ تحویل بسته‌ی موفّقیت‌آمیزتری نسبت به پروتکل GPSR در شرایط مشابه خواهد داشت. این پروتکل به‌دلیل محاسبه و ارزیابی مداوم سطح اعتماد در گره‌ها، توانایی بالایی در تشخیص گره‌های مخرب دارد، چراکه بسیاری از گره‌ها در حملات رها کردن بسته‌ها، هوشمندانه عمل کرده و به‌جای اعمال حمله‌ی سیاه‌چاله، بسته‌ها را به‌صورت انتخابی رها می‌کنند و با اجرای حمله‌ی حفره‌ی خاکستری، امکان تشخیص گره‌های حمله‌کننده را دشوار می‌کنند. پروتکل پیشنهادی با محاسبه‌ی مستمر سطح اعتماد در هر گره، از آخرین تغییرات در عملکرد گره‌های شبکه مطلع خواهد بود و سطح اعتماد هر گره با توجه به عملکرد اخیر آن تعیین می‌شود.



شکل ۷- مقایسه‌ی نرخ تحویل بسته

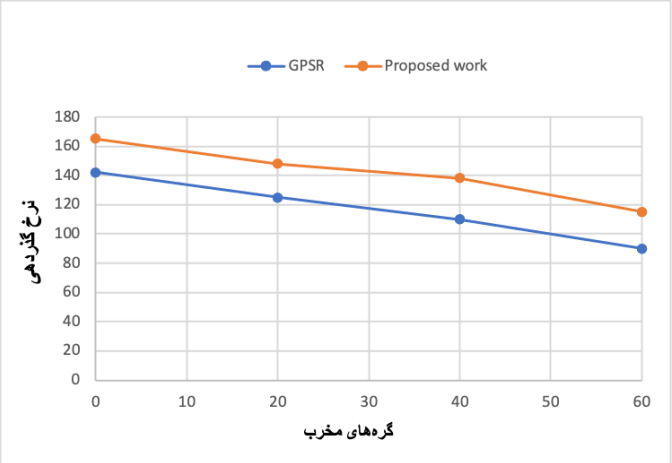
تأخیر انتها به انتها: میانگین زمانی که هر بسته تا رسیدن به مقصد صرف می‌کند، نشان‌دهنده‌ی تأخیر انتها به انتها است. در شبکه‌های بین خودرویی اطلاعات مهم حیاتی مبادله می‌شوند، بنابراین یک پروتکل مسیریابی مناسب باید از تأخیر انتها به انتهای پایینی برخوردار باشد. به‌طور کلی تأخیر انتها به انتها در حضور گره‌های مخرب افزایش پیدا می‌کند. گره‌های مخرب با انجام فعالیت‌های مخرب و ایجاد اختلال در شبکه، میانگین تأخیر انتها به انتها را افزایش می‌دهند. همانطور که شکل ۸ نشان می‌دهد، به‌دلیل محاسبه‌ی معیارهای امنیتی در پروتکل مسیریابی پیشنهادی، تأخیر انتها به انتهای آن در زمان عدم حضور گره‌های مخرب نیز از پروتکل GPSR پایین‌تر است.



شکل ۸- مقایسه‌ی تأخیر انتها به انتها

پس از وارد کردن و افزایش تعداد گره‌های مخرب، پروتکل پیشنهادی با تشخیص فعالیت‌های مخرب و محاسبه‌ی مکرر نرخ اعتماد برای هر گره با توجه به فعالیت‌های آنها، مانع از مشارکت گره‌های مخرب در فرایند مسیریابی شبکه می‌شود. بنابراین با افزایش گره‌های مخرب، نرخ تأخیر انتها به انتها در پروتکل پیشنهادی نسبت به پروتکل GPSR کاهش پیدا می‌کند.

نرخ گذردهی: نرخ گذردهی درواقع به تعداد بسته‌هایی اشاره دارد که در واحد زمان و از طریق یک پیوند ارتباطی خاص با موفّقیت ارسال شده‌اند. بنابراین هرچقدر نرخ گذردهی در یک شبکه بالاتر باشد، عملکرد آن شبکه بهتر است. به‌طورکلی انتظار می‌رود با افزایش گره‌های مخرب در شبکه، نرخ گذردهی کاهش پیدا کند. برای مشاهده‌ی نرخ گذردهی در پروتکل پیشنهادی، عملکرد آن را با پروتکل GPSR در حضور گره‌های مخرب مقایسه می‌کنیم. بر اساس شکل ۹، همان‌طور که پیش‌بینی شده بود، با افزایش گره‌های مخرب، نرخ گذردهی در پروتکل GPSR کلاسیک و پروتکل پیشنهادی کاهش پیدا می‌کند. با این وجود نرخ گذردهی در پروتکل پیشنهادی، همچنان از پروتکل GPSR بیشتر خواهد بود. چراکه ایم پروتکل با محاسبه‌ی مداوم سطح اعتماد در هر گره، گره‌های مخرب را شناسایی کرده و آن‌ها را از فرایند مسیریابی حذف می‌کند.



شکل ۹- مقایسه‌ی نرخ گذردهی

۱.۴ ارزیابی امنیتی پروتکل پیشنهادی

پروتکل‌های مبتنی بر اعتماد در برابر حملات مختلفی آسیب‌پذیری دارند. یکی از رایج‌ترین حملات وارد بر پروتکل‌های مبتنی بر اعتماد، حملات خوب گویی، بدگویی و خود بزرگ نمایی است. در این حملات که به شکل تبانی اعمال می‌گردد، دسته‌ای از گرهّای مخرب با یکدیگر همکاری کرده و نظرات منفی یا مثبت کاذبی را در قالب اعتماد غیرمستقیم درباره‌ی یک گره اعلام می‌کنند. یکی دیگر از حملات رایج بر پروتکل‌های مبتنی بر اعتماد، حمله‌ی خود بزرگنمایی است که در آن یک گره به‌طور کاذب خود را به‌عنوان گره‌ای مناسب برای ارائه‌ی خدمات معرفی می‌کنند. پروتکل پیشنهادی در برابر حملات نام‌برده از عملکرد مناسبی برخوردار است که در ادامه به تحلیل آن‌ها می‌پردازیم.

عملکرد پروتکل پیشنهادی در برابر حملات خوب‌گویی و بدگویی: در پروتکل پیشنهادی با تعریف ضرایب وزنی پویا هنگام محاسبه‌ی اعتماد جامع از حملات خوب‌گویی و بدگویی تا حد زیادی جلوگیری می‌شود. علاوه بر این، هنگام محاسبه‌ی اعتماد غیرمستقیم و درخواست نظرسنجی از سایر همسایگان درباره‌ی یک گره، نظر پیشنهاد دهندگان در مقدار ضرایب وزنی مربوط به نقش آن‌ها در شبکه لحاظ می‌شود. بدین ترتیب نظر پیشنهاد دهندگانی که از نقش معتبرتری برخوردارند، اهمیت بیشتری خواهد داشت. استفاده از جمع وزن‌دار دینامیک در محاسبه‌ی اعتماد جامع می‌تواند تا حد زیادی مقدار تأثیرگذاری اعتماد غیرمستقیم را کنترل کند و از نقش تبانی گره‌های مخرب در تصمیم‌گیری پیشگیری کند.

عملکرد پروتکل پیشنهادی در برابر حمله‌ی خودبزرگ‌نمایی: برخی مواقع گره‌ها سعی می‌کنند تا با ارسال داده‌هایی که از اهمیت کمتری برخوردارند، نرخ ارسال بسته‌ی خود را افزایش دهند و خود را به‌عنوان خدمات دهنده‌ی مناسبی معرفی می‌کنند. پروتکل پیشنهادی با تعریف مقادیر مختلفی از وزن‌ها با توجه به اهمیت داده‌ها مانع از افزایش کاذب نرخ ارسال بسته از طریق ارسال داده‌های کم اهمیت می‌شود. بدین ترتیب پروتکل پیشنهادی عملکرد مناسبی در برابر حمله‌ی خودبزرگ‌نمایی دارد.

عملکرد پروتکل پیشنهادی در برابر حمله ی رفتار هوشمندانه: در پروتکل پیشنهادی، مقداری به عنوان حد آستانه تعریف نشده است و انتخاب گره‌ی بعدی براساس مقایسه‌ی امتیاز گره‌ها با یکدیگر انجام می‌شود. بنابراین احتمال وقوع حملات رفتار هوشمندانه کاسته می‌شود.

۲.۴ نتیجه‌گیری

گره‌ها در شبکه‌ی بین خودرویی برای اهداف مختلفی همچون بهبود ایمنی سرنشینان و کنترل ترافیک با یکدیگر در ارتباط هستند. انتقال اطلاعات بین گره‌ها با انتخاب یک مسیر مناسب در فرایند مسیریابی صورت می‌گیرد. ساختار شبکه‌های بین خودرویی به‌نحوی است که گره‌ها در هر زمان می‌توانند وارد شبکه شده یا از آن خارج شوند. بسیاری از گره‌های وارد شده به شبکه ممکن است با اهداف مختلفی از ارسال بسته‌ها ممانعت کرده و سبب ایجاد اختلال در شبکه شوند. در بسیاری از مواقع گره‌های مخرب می‌توانند هوشمندانه عمل کرده و به‌جای رها کردن تمام بسته‌ها برخی از آن‌ها را ارسال کنند و یا با ارسال داده‌هایی که از ارزش کمتری برخوردارند، نرخ تحویل بسته‌ی خود را افزایش دهند. به‌همین دلیل مسیریابی امن و پویا یکی از چالش‌های مهم در شبکه‌های موردی بین خودرویی است. در این مقاله یک پروتکل مسیریابی امن مبتنی بر موقعیت ارائه شده است که مقدار اعتماد جامع را در هر گره به‌صورت مداوم محاسبه و به‌روزرسانی می‌کند. در این پروتکل برای هر یک از عناصر شبکه یک ضریب پویا در نظر گرفته می‌شود. بنابراین ارسال داده‌هایی با وزن پایین جهت افزایش نرخ تحویل بسته در گره‌ها تشخیص داده می‌شود. علاوه بر این استفاده از جمع وزن‌دار در محاسبات اعتماد سبب اختصاص سهم‌های پویا به هریک از مؤلفه‌ها و در نظر گرفتن طیف گسترده‌تری از حالت‌ها با دقت بالا می‌شود. با استفاده از پروتکل پیشنهادی، گره‌هایی که از سطح اعتماد پایین‌تری برخوردار باشند شناسایی شده و در فرایند مسیریابی شرکت داده نمی‌شوند. بنابراین اطلاعات شبکه در یک مسیر امن منتقل می‌گردند. پروتکل پیشنهادی از راه‌اندازی آسان و سربار محاسباتی پایین‌تری نسبت به سایر مکانیسم‌های امنیتی برخوردار است و ارتباط امن بین وسایل نقلیه را با هزینه‌ای پایین فراهم می‌کند. نتایج شبیه‌سازی نشان می‌دهد که عملکرد شبکه از نظر نرخ تحویل بسته‌ها و تأخیر انتها به انتها در حضور گره‌های مخرب در پروتکل پیشنهادی شرایط مطلوب‌تری در مقایسه با پروتکل GPSR که فاقد هرگونه مکانیزم‌های امنیتی است، دارد. البته پروتکل پیشنهادی تنها به شناسایی گروهی از فعالیت‌های مخرب محدود می‌شود و در برابر گره‌های مخرب درون شبکه کارایی دارد. تلاش می‌شود تا در آینده، پروتکل پیشنهادی را در برابر طیف گسترده‌تری از حملات ارتقاء دهیم و حفظ حریم خصوصی کاربران را به‌عنوان یکی از مؤلفه‌های جدید در مسیریابی امن، تعریف کنیم.

۵. مراجع

[1] Mi, U. Farooq, J. Zhang, T. Tran, R. Cohen, “A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks,” *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 3, pp. 407-420, 2010

[2] T, K. Narayan, S. C. Sharma, "A trust-based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS)," *International Journal of System Assurance Engineering and Management,* vol. 11, no. 2, pp 426-440, 2020
[3] S. C. Sakgreliya, N. H. Pandya, "PKI-SC: Public key infrastructure using symmetric key cryptography for authentication in VANETs," 2014 *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-6. IEEE, 2014.
[4] A. Slama, I. L, "Survey on Secure Routing in VANETs." *International Journal of Network Security & Its Applications (IJNSA) Vol*, vol. 11 2019.
[5] J. Hu, H. Lin, X. Guo, and J. Yang. "DTCS: An integrated strategy for enhancing data trustworthiness in mobile crowdsourcing." *IEEE Internet of Things Journal* 5, vol. 5, no. 6, pp. 4663-4671, 2018
[6] R. Su, A. Sfar, E. Natalizio, P. Moyal, and Y. Song, "PDTM: Phase-based dynamic trust management for Internet of things." In *2021 International Conference on Computer Communications and Networks (ICCCN)*, pp. 1-7, IEEE, 2021
[7] G. Yang, Q. Yang, and H. Jin, "A novel trust recommendation model for mobile social network based on user motivation." *Electronic Commerce Research*, vol. 21, no. 3, pp. 809-830, 2021
[8] W. Abdelghani, C. A. Zayani, I. Amous, and F. Sèdes, "Trust management in social internet of things: a survey." In *Conference on e-Business, e-Services and e-Society*, pp. 430-441, Springer, 2016
[9] A. Farhan, J. Hall, A. Adnane, and V. N. Franqueira, "Faith in vehicles: A set of evaluation criteria for trust management in vehicular ad-hoc network," 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 44-52. IEEE, 2017.
[10] X. Yao, X. Zhang, H. Huansheng, P. Li, "Using trust model to ensure reliable data acquisition in VANETs," Ad Hoc Networks, vol. 55, pp. 107-118, 2017 Feb.
[11] H. Hamssa, A. E. Samhat, C. Bassil, and A. Laouiti. "Trust model for secure group leader-based communications in VANET," Wireless Networks, vol. 25, no. 8, pp.4639-4661, 2019 Nov.
[12] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, "Decentralized trust evaluation in vehicular Internet of Things," *IEEE Access*, vol. 7, pp. 15980-15988, 2019
[13] K. N. Tripathi, S. C. Sharma, and G. Jain, "A New Reputation-Based Algorithm (RBA) to Detect Malicious Nodes in Vehicular Ad Hoc Networks (VANETs)," *Advances in Intelligent Systems and Computing Soft Computing: Theories and Applications*, pp.395-404. 2020.
[14] J. Grover, M. S. Gaur, and V. Laxmi. "Trust establishment techniques in VANET." *In Wireless Networks and Security*, pp. 273-301. Springer, Berlin, Heidelberg, 2013.
[15] M. J. Sataraddi, and M. S. Kakkasageri, "Trust and Delay based Routing for VANETs." *In 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1-6. IEEE, 2019.
[16] J. Ma, and C. Yang. "A trust-based stable routing protocol in vehicular ad-hoc networks." *Int J Secur Appl*, vol. 9, no. 4, pp.107-116, 2015.
[17] X. Hui, S. S. Zhang, B. X. Li, L. Li, and X. G. Cheng, "Towards a novel trust-based multicast routing for VANETs." *Security and Communication Networks*, vol. 2018, 2018.
[18] A. Srivastava, A. Prakash, and R. Tripathi, "Location based routing protocols in VANET: Issues and existing solutions," *Vehicular Communications*, vol. 23, pp. 100231, 2020 Jun.
[۱۹] م. دهقان، س. شکرالهی، "ارائه یک پروتکل مسیریابی امن مبتنی بر اعتماد در شبکه‌های موردی بین خودرویی،" *بیست و هفتمین کنفرانس بین‌المللی انجمن کامپیوتر ایران*، ۱۴۰۰.
[20] B. Karp, H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 243-254. 2000.
[21] E. A. Shams, A. Rizaner, and A. H. Ulusoy, "Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks," *Computers & Security,* vol. 78, pp.245-254, 2018 Sep.
[22] T. Nandy, R. M. Noor, M. Y. I. B. Idris, and S. Bhattacharyya. "T-BCIDS: Trust-based collaborative intrusion detection system for VANET," *In 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA),* pp. 1-5. IEEE, 2020.

مهتاب دهقان فارغ‌التحصیل کارشناسی ارشد در رشته مهندسی برق گرایش مخابرات امن و رمزنگاری در سال ۱۴۰۰ از پژوهشکده‌ی فضای مجازی از دانشگاه شهید بهشتی تهران است. از جمله زمینه‌های پژوهشی موردعلاقه وی می‌توان به امنیت شبکه و سیستم‌های تشخیص نفوذ، تشخیص حملات شبکه، شبکه‌های بین خودرویی و رویکردهای مدیریت اعتماد در شبکه‌های موردی متحرک اشاره کرد. آدرس الکترونیکی ایشان عبارت است از:
maht.dehghan@mail.sbu.ac.ir

سعید شکرالهی تحصیلات خود را در مقطع کارشناسی کامپیوتر- نرم افزار در سال ۱۳۸۱ از دانشگاه اصفهان و در مقاطع کارشناسی ارشد و دکتری کامپیوتر- نرم‌افزار به ترتیب در سال‌های ۱۳۸۴ و ۱۳۹۳ از دانشگاه شهید بهشتی به پایان رسانده است. ایشان دوره فرصت مطالعاتی خود را در سال ۱۳۹۱در آزمایشگاه امنیت دانشگاه میلان سپری کرده است. وی در حال حاضر استادیار گروه امنیت شبکه و رمزنگاری پژوهشکده فضای مجازی در دانشگاه بهشتی است. زمینه‌های تحقیقاتی موردعلاقه ایشان عبارت‌اند از: سیستم‌های فوق مقیاس وسیع، معماری نرم‌افزار، معماری سرویس گرا، معماری سازمانی، امنیت و کنترل دسترسی، اینترنت اشیاء، میان‌افزارهای مبتنی بر رویداد و شبکه‌های بین خودرویی. آدرس الکترونیکی ایشان عبارت است از:
s_shokrollahi@sbu.ac.ir

[1] Vehicular ad hoc networks (VANETs)
[2] Mobile ad hoc networks (MANETs)
[3] On-board unit (OBU)
[4] Vehicle-to-vehicle (V2V)
[5] Vehicle-to-infrastructure (V2I)
[6] Dedicated short-range communication (DSRC)
[7] Location-based routing protocols
[8] Topology-based routing protocols
[9] Malicious nodes
[10] Trust-based
[11] Message tampering attack
[12] Message falsification attack
[13] Sybil attack
[14] Entity-centric
[15] Data-centric
[16] Combination trust
[17] Opportunistic Service Attack
[18] On-off Attack
[19] Conflicting Behavior Attack
[20] Newcomer Attack
[21] Intelligent Behavior attack
[22] Good-mouthing Attack
[23] Bad-mouthing Attack
[24] Selective Behavior Attack
[25] Time-dependent Attack
[26] Location-dependent Attack
[27] Self-promoting Attack
[28] Direct trust
[29] Indirect trust (Recommendation trust)
[30] Perimeter mode
[31] Forwarding mode
[32] Modified promiscuous mode

The CSI Journal on Computing Science and Information Technology

The CSI Journal on
Computing Science and
Information Technology
Vol. 20, No.1, 2022

A trust-based secure routing in Vehicular ad hoc network

Mahtab Dehghan[1], Saeed Shokrollahi[2]

[1, 2] Cyberspace Research Institute, Shahid Beheshti University (SBU), Tehran, Iran

Abstract

In recent years, research and development of networks that do not have any dependence on a predetermined infrastructure have received much attention. Vehicular ad hoc networks are one of these types of networks that, as a new technology, have a high potential to increase road safety and ensure the well-being of users. The fixed and mobile nodes that make up these networks participate in routing by exchanging critical data. These nodes are interconnected for various purposes, such as improving passengers' safety and traffic control, and exchanging a wide range of information. The open exchange of information between nodes in networks without infrastructure provides a good opportunity for malicious nodes to enter the network and disrupt network processes to achieve profitable goals. Therefore, sending information over a trustworthy and optimal path is one of the most challenging aspects of vehicular ad networks. So far, various routing protocols have been proposed to solve this challenge, which have used different criteria to select the appropriate nodes in their routing. In this paper, a secure location-based routing protocol is proposed in which the combination trust of each node is considered as one of the basic criteria for selecting that node in the routing process. The calculation of the combination trust value for each evaluated node is performed using the direct trust calculation by the evaluating node and the neighbors' recommendation during the query process using indirect trust. The simulation and evaluation results of the proposed protocol using NS-2 software show that if the number of malicious nodes in the network increases, the proposed protocol will perform better than the GPSR protocol in terms of packet forwarding rate, throughput rate, and end-to-end latency.

Keywords: Secure routing, Vehicular ad hoc network, Trust-based routing protocol, Security of vehicular ad hoc network