اولین کنفرانس ملی علوم مهندسی،ایده‌های نو
مؤسسه آموزش عالی آیندگان- ۲۱ اردیبهشت ۹۳

ارائه یک پروتکل جدید مسیریابی امن مبتنی بر موقعیت گره با استفاده از رمزنگاری داده‌ها در شبکه‌های موردی بین خودرویی

هومن جمشیدی[۱]، صابر فتح الهی[۲]
[۱] دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد اراک ، Hooman.Jamshidi@Hotmail.com
[۲] کارشناس ارشد شبکه ، Saber_Fatholahi@Yahoo.com

چکیده - شبکه‌های موردی بین خودرویی (*VANET*) بستر مناسبی برای انجام پژوهش‌هایی در راستای ایجاد سیستمهای حمل‌ونقل هوشمند (*ITS*) است. افزایش تعداد وسایل نقلیه منجر به بروز تصادفات جاده‌ای و ترافیک در مناطق شهری شده است، بنابراین برای از بین بردن این مشکلات باید ارتباط مؤثر و امن بین وسایل نقلیه وجود داشته باشد. تحرک بالا و اختلال مکرر پیوند ارتباطی میان خودروها از موضوعات چالش‌برانگیز در این نوع شبکه‌ها هستند. اخیراً پژوهشگران موضوعات خاصی از این حوزه نظیر مسیریابی، کیفیت سرویس، امنیت، معماری، کاربرد و پروتکل‌ها را مورد بررسی قرار داده‌اند. امنیت مهم‌ترین مسئله در شبکه‌های *VANET* است زیرا رانندگان بدکار عملکرد شبکه را مختل می‌کنند. در این مقاله با استفاده از ترکیب دو پروتکل مسیریابی *MFR* و *B-MFR* یک پروتکل جدید مسیریابی امن مبتنی بر موقعیت را ارائه شده است. در این پروتکل از یک ماژول امنیتی که در آن از یک کلید توافقی رمزنگاری داده‌های ارسالی جهت محافظت سیستم در مقابل حملات گوناگون، استفاده شده است. این ماژول شامل ۳ فاز: آماده سازی، بهینه‌سازی انتخاب گره و تحویل داده امن می‌باشد. نتایج شبیه‌سازی نشان می‌دهد که پروتکل پیشنهادی از نظر تأخیر انتها به انتها و نرخ تحویل بسته، در شرایطی که رانندگان بدکار نیز در شبکه حضور داشته باشند، عملکرد بهتری را نسبت به دو پروتکل *MFR* و *B-MFR* خواهد داشت.

کلید واژه- شبکه‌های موردی بین خودرویی، مسیریابی، امنیت، رمزنگاری

۱- مقدمه

پیشرفت‌های جاری در فن‌آوری‌های بی‌سیم منجر به پیدایش بسیاری از انواع شبکه‌های جدید گردیده است که قابلیت پیاده‌سازی در محیط‌های مختلف را دارند. VANET، یکی از انواع شبکه‌های در حال ظهور است که انقلاب بزرگی را در زمینه ارتباطات شبکه‌های بی‌سیم به وجود آورده است [۲][۸]. ارتباط خودرویی در واقع به معنای ارتباط میان دو یا چند خودرو با یکدیگر است. برای پیاده‌سازی یک شبکه VANET در یک محیط خاص و ارائه سرویس، بسیاری از استانداردها، پروتکل‌ها، معماری‌ها و سایر نیازمندی‌ها استفاده می‌شوند. هدف اصلی ارائه امن خدمات به کاربر نهایی است. سازمان بهداشت جهانی (WHO) با ارائه آماری از مرگ و میرهایی که بر اثر تصادفات جاده‌ای در هر یک از کشورهای دنیا اتفاق می‌افتد، برآورد نموده در صورتی که روند بروز این نوع مرگ‌ومیر به این صورت افزایش و ادامه داشته باشد، پس از سال ۲۰۲۰، تصادفات جاده‌ای سومین عامل مرگ‌ومیر انسان‌ها خواهد بود. VANET یک کانال ارتباطی را میان وسایل نقلیه به منظور حفاظت از آن‌ها در مقابل خطرات تصادفات جاده‌ای، ایجاد می‌نماید. به عنوان نمونه‌هایی از کاربردهای شبکه‌های VANET می‌توان به سیستم هشدار به راننده، سیستم کاهش سرعت خودکار و غیره اشاره نمود. تا کنون پروژه‌های موفقی از پیاده‌سازی شبکه‌های بین خودرویی در بسیاری از کشورها مانند آمریکا، ژاپن و کشورهای اروپایی با حمایت دولت‌ها و برخی شرکت‌های خودروسازی مانند بی ام دبلیو، فورد، دیالمر و غیره، انجام‌شده‌اند [۸]. اهمیت شبکه‌های VANET در زندگی واقعی ما، به مزایای این نوع شبکه‌ها در پیاده‌سازی سیستم‌های کنترل ترافیک هوشمند مربوط می‌شود. معماری VANET عمدتاً از جاده‌ها، خیابان‌ها، وسایل نقلیه، واحد کنار جاده‌ای (RSU)، مجوزها و غیره تشکیل شده است [۸]. واحد کنار جاده‌ای مانند یک مسیریاب عمل می‌کند و برای ذخیره‌سازی اطلاعات و محاسبات مورد استفاده قرار می‌گیرد. در پیاده‌سازی و نصب این واحدها، به منظور پایش سرعت خودروها و همچنین پخش پیام میان آن‌ها از حسگر استفاده شده است. مجوز خودروها از طریق یک امضای دیجیتال با کلید خصوصی به آن‌ها اعطا می‌گردد و در واقع سطح اعتماد به یک خودرو را مشخص می‌نماید. خودروها هر یک مجهز به GPS می‌باشند که به وسیله آن هم از موقعیت خود را آگاه می‌شوند و

هم می‌توانند موقعیت سایر خودروها را ردیابی کنند. همچنین هر خودرو دارای یک قطعه الکترونیکی برای انجام ارتباطات بی‌سیم و یک پلاک الکترونیکی برای تخصیص شماره منحصر به فرد است. در حال حاضر، به امنیت شبکه‌های VANET به عنوان یک مسئله اصلی پرداخته می‌شود [۸][۱۰][۱۲]، زیرا همواره این مسئله وجود دارد که تعداد زیادی از رانندگان فاقد مجوز به شبکه واردشده و باعث ایجاد اختلال و کاهش عملکرد شبکه می‌گردند. در این مقاله، پروتکل مسیریابی امن جدیدی، مبتنی بر موقعیت گره در شبکه‌های موردی بین خودرویی ارائه گردیده است که داده‌ها را پیش از ارسال به منظور جلوگیری از دستیابی‌های غیرمجاز به آن‌ها با استفاده از کلیدی موسوم به کلید نشست (SK)، رمزنگاری می‌نماید و به اختصار SPRP نامیده می‌شود.

پروتکل پیشنهادی، یک پروتکل مسیریابی ترکیبی است که برای یافتن گره بهینه به منظور انتشار داده، از مفاهیم MFR و B-MFR [۷] استفاده می‌نماید. پس از یافتن گره بهینه، نکته اصلی بررسی این است که آیا گره یافته شده یک گره مجاز است یا خیر که برای این منظور مجوز گره مورد بررسی قرار می‌گیرد. نتایج شبیه‌سازی‌ها نشان می‌دهد که SPRP، در شرایطی که رانندگان غیرمجاز نیز در شبکه حضور دارند، عملکرد بهتری را نسبت به MFR و B-MFR از نظر تأخیر انتها به انتها و نرخ تحویل بسته داده، ارائه می‌کند.

بخش‌های مختلف این مقاله به این شرح خواهند بود: بخش ۲ پیرامون استانداردهای موجود در سیستم‌های حمل‌ونقل هوشمند خواهد بود، در بخش ۳ به مرور کارهای مرتبط انجام‌شده پیشین خواهیم پرداخت، سه فاز پروتکل پیشنهادی SPRP در بخش ۴ معرفی خواهد شد. بخش ۵ به شبیه‌سازی پروتکل SPRP و مقایسه عملکرد آن با MFR و B-MFR خواهد پرداخت و در نهایت در بخش ۶ به نتیجه‌گیری خواهیم پرداخت.

۲- سیستم حمل و نقل هوشمند

سیستم حمل‌ونقل هوشمند (ITS) سیستمی است که در آن هر خودرو در شبکه به عنوان یک مسیریاب، فرستنده و گیرنده ایفای نقش می‌کند [۸]. ITS شامل واحدهای کنار جاده‌ای، وسایل نقلیه، خیابان‌ها، مجوزها و غیره است. ارتباطات در VANET نیز یا به صورت خودرو با خودرو (V2V) و یا خودرو با زیرساخت جاده‌ای (V2I) است. ITS معمولاً از پروتکل‌هایی نظیر IEEE 802.11p، IEEE 802.15.1، IEEE 802.15.3، IEEE 802.15.4 و غیره برای تبادل و تحویل سریع‌تر داده‌ها و از پروتکل MAC برای ارتباطات داده‌ای استفاده می‌نماید [۸].

۲-۱- استانداردها

استانداردهای ارتباطی نظیر ارتباطات اختصاصی برد کوتاه[1] (DSRC) و دسترسی بی‌سیم در محیط‌های خودرویی[2] (WAVE) مورد استفاده قرار می‌گیرند [۸]. DSRC هر دو نوع ارتباط V2V و V2I را پوشش می‌دهد. این استاندارد در ایالات‌متحده از محدوده فرکانسی ۷۵ مگاهرتز تا ۵/۹ گیگاهرتز، در ژاپن ۸۰ مگاهرتز تا ۵/۸ گیگاهرتز و در کشورهای اروپایی نیز از ۲۰ مگاهرتز تا ۵/۸ مگاهرتز استفاده می‌نماید. این استاندارد نرخ بالایی از انتقال اطلاعات را فراهم می‌کند. ارتباطات WAVE برای تبادل بالای داده‌ها به وجود آمد و توسط ASTM 2313 از DSRC به IEEE 802.11p تغییر نام یافت. استاندارد IEEE 1609 در نسخه‌های مختلفی از جمله IEEE 1609.1، IEEE 1609.2، IEEE 1609.3 و IEEE 1609.4 ارائه گردیده است.

۲-۲- امنیت

بسیاری از حملاتی که در VANET وجود دارد مانند موقعیت‌های قلابی [۹]، تولید شناسه‌های جعلی، ایجاد اختلال در آمار و ارقام، تغییر داده‌ها، حملات DoS، حمله سیاه‌چاله ، حمله مرداب ، اطلاعات GPS جعلی، مکان جعلی و غیره است [۳][۱۳]. بسیاری از پروتکل‌های مسیریابی امن برای حفاظت از شبکه‌های VANET در مقابل تهدیدات امنیتی طراحی شده‌اند. از این دسته پروتکل‌ها می‌توان به مواردی همچون، ARAN، ARIADNE، TESLA، SPAAR، SAODV، SEAD، WATCHDOG-PATHRATER، ECDSA اشاره نمود. پروتکل ارائه‌شده در این مقاله، یک پروتکل امن مسیریابی است که در آن به صورت ایستگاه به ایستگاه، از پروتکل مدیریت کلید برای تولید کلید نشست (SK) به منظور رمزگذاری

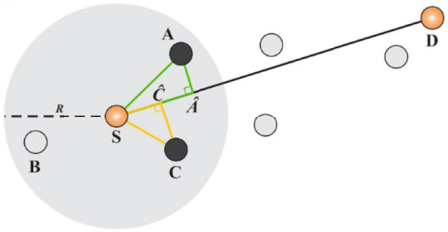
[1] Dedicated Short Range Communication
[2] Wireless Access in Vehicular Environment

بسته‌های داده، مورد استفاده قرار می‌گیرد.

۳- کارهای انجام شده پیشین

پروتکل‌های مسیریابی شبکه‌های VANET عمدتاً به پروتکل‌های مسیریابی مبتنی بر توپولوژی، مبتنی بر موقعیت، مبتنی بر خوشه، مبتنی بر پخش جغرافیایی و مبتنی بر بخش فراگیر تقسیم می‌گردد [۱][۵][۶][۱۱]. در مسیریابی مبتنی بر توپولوژی اطلاعات مسیر را در شبکه نگهداری می‌کند. مسیریابی مبتنی بر موقعیت از طرح خدمات مکانی برای ارتباطات استفاده می‌نماید. در روش مبتنی بر خوشه یک سر خوشه به عنوان مسئول برقراری ارتباط انتخاب می‌شود. پخش جغرافیایی برای پخش داده میان چند مورد خاص استفاده می‌شود. ارتباطات مبتنی بر پخش فراگیر غالباً در شبکه‌های VANET جهت پخش پیام میان تمام گره‌ها مورد استفاده قرار می‌گیرد.

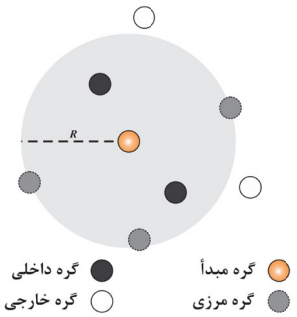
در این مقاله، عملکرد SPRP[3] با MFR[4] و B-MFR[5] با یکدیگر مقایسه می‌گردد. در MFR، هر گره دارای یک محدوده رادیویی تحت پوشش است که اندازه شعاع آن با R مشخص می‌گردد. همچنین گره‌هایی که در این محدوده قرار می‌گیرند به عنوان گره همسایه نامیده می‌شوند. انتخاب یک گره به عنوان گام بعدی برای انتقال داده به این صورت انجام می‌شود که گره‌های همسایه گره S در پاسخ به درخواست آن (بسته Hello)، اطلاعات مکان، سرعت، زمان، شناسه، جهت حرکت و گره‌های همسایه‌ای که در ناحیه مقابل و ناحیه پشت آن‌ها قرار دارند را اعلام می‌کنند. سپس خطی فرضی از گره مبدأ (S) به گره مقصد (D) در نظر گرفته می‌شود. از آنجا که در MFR طبق فرضیات، از گره‌های موجود در مقابل برای ارسال داده به سمت مقصد استفاده می‌گردد و همان طور که در شکل ۱ مشخص است، گره‌های مقابل گره S، گره A و C می‌باشند و تنها گره ناحیه پشت گره S گره B است.



شکل ۱: نحوه انتخاب گام بعدی در MFR

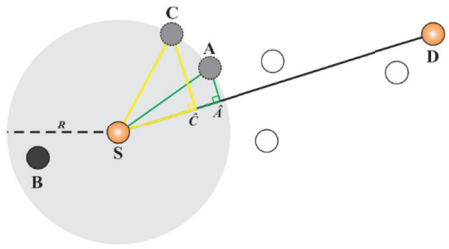
مطابق شکل ۱، در MFR گره S برای انتقال داده از میان گره‌های همسایه مقابل خود با توجه به بردار فرضی $\overrightarrow{SD}$ با محاسبه تصویر بردارهای فرضی $\overrightarrow{SA}$ و $\overrightarrow{SC}$، گره A را به جهت داشتن طول بیشتر بردار تصویر $\overrightarrow{S\hat{A}}$ نسبت به $\overrightarrow{S\hat{C}}$ بر روی بردار فرضی $\overrightarrow{SD}$، انتخاب می‌گردد. هدف اصلی انتقال اطلاعات به گرهی است که در که به گره مقصد نزدیک‌تر باشد.

در B-MFR، مانند آنچه در شکل ۲ دیده می‌شود، گره‌های همسایه یک گره مانند S به دو دسته تقسیم می‌گردند: دسته نخست گره‌هایی هستند که دقیقاً در محدوده رادیویی تحت پوشش گره S قرار می‌گیرند یعنی فاصله آن‌ها تا گره S کمتر از مقدار R باشد که گره‌های داخلی نامیده می‌شوند و دسته دوم گره‌هایی هستند که فاصله آن‌ها با S برابر با مقدار R است و گره‌های مرزی نامیده می‌شوند. در انتخاب گره به عنوان گام بعدی انتقال در B-MFR از گره‌های مرزی به منظور ارسال داده، گرهی که به مقصد نزدیک‌تر است استفاده می‌شود. لذا همان طور که در شکل ۳ نشان داده شده است گره A به دلیل داشتن تصویر بردار بیشتر نسبت به گره C به عنوان گام بعدی در مسیر انتقال انتخاب می‌گردد.



شکل ۲: انواع گره‌ها در B-MFR

[3] Secure Position-based Routing Protocol
[4] Most Forward within Radius
[5] Border-node based Most Forward within Radius



شکل ۳: نحوه انتخاب گام بعدی در B-MFR

بر اساس پژوهش‌های انجام‌شده پیشین، پروتکل B-MFR از نظر تأخیر انتها به انتها در شبکه‌های با تراکم بالا، عملکرد بهتری را در مقایسه با پروتکل MFR دارد. در این مقاله، SPRP با دو پروتکل MFR و B-MFR از نظر امنیت، زمانی که رانندگان فاقد مجوز در شبکه حضور دارند بررسی می‌گردد.

۴- پروتکل مسیریابی امن مبتنی بر مکان (SPRP)

۴-۱- مدل شبکه

در طرح پیشنهادی ما یک پروتکل مسیریابی ترکیبی طراحی شده است که در آن برای یافتن گره بهینه از مفاهیم موجود در پروتکل‌های MFR و B-MFR استفاده شده است، همچنین برای حفظ محرمانگی داده‌ها و محافظت از آن‌ها در برابر حملات فیزیکی و منطقی شبکه، یک ماژول امنیتی به این طرح اضافه گردیده است. SPRP به طور کلی شامل سه فاز عملیاتی است: فاز نخست، آماده سازی، دومین فاز انتخاب گره بهینه و فاز سوم تحویل داده امن است. فرضیات طرح به شرح زیر می‌باشند:

- شبکه را به صورت یک مجموعه از گره‌های N_i در نظر می‌گیریم که $i = (1, 2, 3, \dots, n)$ می باشد.
- هر گره N_i مسئول ارتباطات در شبکه است (پخش واحد، چندگانه و فراگیر).
- ارتباطات میان گره‌های N_i مبتنی بر پیام است.
- هر گره (خودرو) دارای یک شناسه منحصربه‌فرد در شبکه است.
- گره‌ها در VANET دارای منابع انرژی بالا هستند.
- هر گره دارای یک مجوز و یک کلید خصوصی (PK) مشخص است.
- همواره از گره‌هایی که در ناحیه مقابل یک گره، دارند برای انتخاب گام بعدی ارتباطات استفاده می‌گردد.
- سیستم هشداردهنده خودروها در یک بازه زمانی خاص، اطلاعات خود را با یکدیگر به‌روزرسانی می‌کنند.
- هر گره مسئول تولید یک کلید نشست (SK) برای کدگذاری و ارسال داده با رعایت محرمانگی آن‌هاست.
- هر یک از گره‌ها به گیرنده GPS و نقشه دیجیتال مجهز هستند که به وسیله آن‌ها می‌توانند از موقعیت خود و سایر گره‌ها مطلع شود.
- برای این پروتکل یک ناحیه متراکم در نظر گرفته شده است. به عنوان مثال، خیابان‌های پر ترافیک شهر که هر ماشین دارای همسایه‌های مجاوری برای خود است.

۴-۲- فازهای عملیاتی SPRP

۴-۲-۱- آماده سازی

فاز نخست، فاز آماده سازی است که در آن هر N_i بسته‌های پیام Hello را گره‌های همسایه ارسال می‌نماید. ساختار بسته پیام Hello شامل: شناسه گره، سرعت، زمان جاری، مکان، جهت حرکت و لیست گرههای همسایهای که در مقابل و پشت سر قرار دارند است. سپس گره مبدأ (S)، بررسی می‌کند که آیا گره مقصد (D)، در محدوده تحت پوشش آن قرار دارد یا خیر؟ برای این منظور حداکثر فاصله تحت پوشش خود (R) را با فاصله از گره مقایسه می‌نماید. در صورتی که در محدوده تحت پوشش آن باشد، ابتدا با استفاده از SK تولیدشده توسط دو گره (خودرو)، پیام‌ها را کدگذاری کرده و اقدام به ارسال داده می‌نماید. اگر گره D یک راننده فاقد مجوز باشد به راحتی شناخته می‌شود. پس از بررسی گره D چنانچه در محدوده تحت پوشش نباشد فاصله هندسی میان گره S با گره‌های همسایه که در سمت مقابل آن قرار دارند، با استفاده از رابطه ۱ محاسبه می‌گردد.

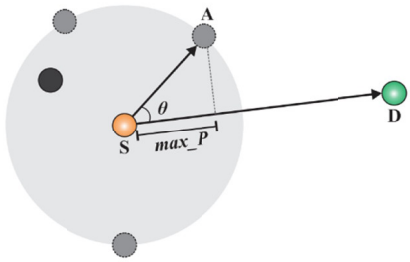
$$d(p,q) = \sqrt{((p_1 - q_1)^2 + (p_2 - q_2)^2)} \qquad (۱)$$

در این رابطه (p_1, p_2) مختصات گره S و (q_1, q_2) مختصات همسایه مورد بررسی را نشان می‌دهد. گره‌های همسایه گره S به دو گروه تقسیم می‌گردند: گروه نخست گره‌هایی هستند که دقیقاً در محدوده رادیویی تحت پوشش گره S قرار می‌گیرند یعنی فاصله آن‌ها تا گره S کمتر از مقدار

R باشد که در گروه گره‌های داخلی (IN[6]) قرار می‌گیرند و گروه دوم گره‌هایی هستند که فاصله آن‌ها با S برابر با مقدار R است و گره‌های مرزی نامیده می‌شوند و در گروه گره‌های مرزی (BN[7]) قرار می‌گیرند. هر دو گروه IN و BN شامل گره‌هایی هستند که برای انتخاب به عنوان گام بعدی برای انتقال داده مناسب می‌باشند.

۴-۲-۲- بهینه سازی انتخاب گره

فاز دوم به انتخاب گره بهینه از میان اعضای گروه‌های IN و BN می‌پردازد. طول بردار تصویر هر یک از گره‌های موجود در این گروه‌ها بر روی بردار فرضی $\overrightarrow{SD}$ با پارامتری تحت عنوان max_P مشخص می‌گردد که با توجه به شکل و با استفاده از رابطه ۲ محاسبه می‌گردد.



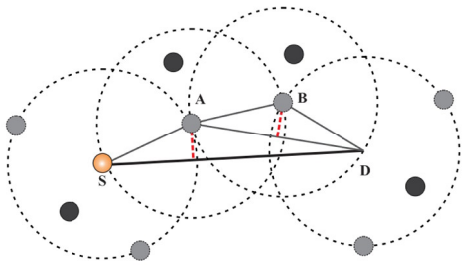
شکل۴: نمایش فاکتور max_P

$$|max\_P| = |A| \cos\theta \qquad (۲)$$

در ابتدای این فاز فاکتور max_P تمامی گره‌های موجود در گروه‌های IN و BN محاسبه می‌گردد. سپس گره‌ها بر اساس بیشترین مقدار max_P مرتب می‌شوند. از میان گره‌های موجود در BN گره‌ی را که دارای بیشترین مقدار max_P باشد، انتخاب می‌گردد. سپس بررسی می‌شود که آیا این گره دارای گره‌های همسایه در ناحیه جلوی خود است یا خیر؟ در صورتی که پاسخ مثبت باشد، به صورت حریصانه به عنوان گره بهینه برای ادامه عملیات انتخاب می‌شود. چنانچه فاقد این ویژگی باشد به سراغ گره دیگری در گروه BN می رود و همین روال را انجام می‌دهد. چنانچه گروه BN فاقد گره دیگری باشد، از میان اعضای گروه IN، طبق روش بالا گره بهینه را انتخاب می‌گردد.

۴-۲-۳- تحویل داده امن

فاز نهایی این پروتکل، به عنوان مهم‌ترین فاز پروتکل مسیریابی SPRP، شامل یک ماژول امنیتی است که برای تأمین امنیت ارتباطات داده‌ای در مقابل افزایش رانندگان فاقد مجوز در شبکه، به سیستم افزوده شده است. در این طرح از یک پروتکل کلید توافقی ایستگاه به ایستگاه برای تولید SK استفاده شده است. مزیت اصلی استفاده از این طرح بررسی و شناخت پیام‌های مزاحم است. اهمیت استفاده از این روش این است که برای بررسی و تأیید کردن گره‌های همسایه، به نفر (عامل) سومی نیاز نیست. به عنوان مثال اگر گره A به عنوان گره بهینه به عنوان گام بعدی مسیر ارتباطی انتخاب گردد، گره S با ارسال پیامی به آن خواستار ایجاد کلید نشست (SK) می‌گردد. گره A نیز پس از ایجاد SK، کلید ایجادشده را به همراه امضای الکترونیکی و مجوزهای خود به گره S ارسال می‌نماید. در این مرحله گره‌های فاقد مجوز قابل کشف و شناسایی هستند؛ زیرا مبنای عملکرد این فاز در تشخیص گره‌های دارا / فاقد مجوز بررسی مجوزها و امضای الکترونیکی دریافتی از گره‌ها در این مرحله است. پس از تأیید هویت گره A، گره S با استفاده از SK پیام‌ها را رمزنگاری کرده و منتقل می‌نماید. اجرای فازهای سهگانه فوق تا رسیدن بسته داده به مقصد ادامه می‌یابد. شکل (۵) یک تصویر ساده از الگوریتم SPRP را نشان می‌دهد که در آن گره‌های {A و B} که از اعضای گروه گره‌های بهینه است و داده‌ها از گره S به گره A سپس به گره B و در نهایت به گره D ارسال می‌گردد.



شکل۵: مدل انتقال داده در SPRP

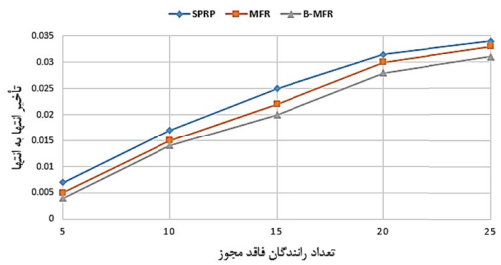
۵- نتایج شبیه سازی

در این بخش پروتکل SPRP با دو پروتکل MFR و B-MFR از نظر تأخیر انتها به انتها و نرخ بسته داده‌های تحویل داده‌شده، در شرایطی که رانندگان فاقد مجوز در شبکه وجود داشته باشند مورد مقایسه قرار گرفته است. برای مقایسه کارایی میان آن‌ها یک محیط با اندازه ۵۰۰×۵۰۰ مترمربع با ۲۰۰ گره

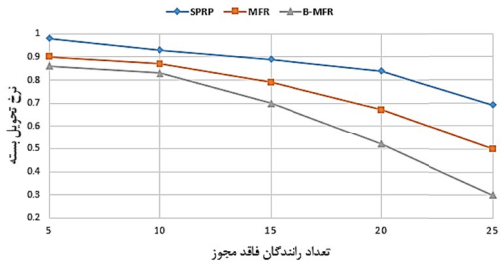
[6] Internal Node Group
[7] Border Node Group

که شامل گره‌های فاقد مجوز نیز می‌باشد و همچنین از پروتکل IEEE 802.11 DCF MAC برای ارتباط میان گره‌ها با نرخ ثابت انتقال داده استفاده گردیده است. سرعت خودروها بین ۳۰ تا ۶۰ کیلومتر بر ساعت و اندازه بسته‌های داده‌ها ۵۱۲ بایت در نظر گرفته شده است. کارایی با در نظر گرفتن دو فاکتور تأخیر انتها به انتها و نرخ بسته تحویل داده‌شده مورد بررسی قرار گرفته است. مکانیزم امنیتی استفاده‌شده در پروتکل مسیریابی SPRP، منجر به افزایش تأخیر انتها به انتها این پروتکل نسبت به پروتکل‌های MFR و B-MFR گردیده است، اما نرخ تحویل بسته در SPRP خیلی بالاتر از MFR و B-MFR است زیرا تنها داده‌ها به گره‌های دارای مجوز ارسال می‌گردد.

شکل ۶ تأخیر انتها به انتها را در شرایطی که گره‌های فاقد مجوز وجود داشته باشد را نشان می‌دهد. شکل ۷ نرخ تحویل بسته‌های داده در پروتکل MFR و B-MFR و SPRP را نشان می‌دهد.



شکل ۶: نمودار مقایسه میزان تأخیر انتها به انتها در پروتکل‌های MFR، B-MFR و SPRP



شکل ۷: نمودار مقایسه نرخ تحویل بسته‌ها در پروتکلهای MFR، B-MFR و SPRP

۶- نتیجه‌گیری

افزودن ماژول امنیتی به SPRP، منجر به افزایش تأخیر انتها به انتها و افزایش قابل‌توجه نرخ تحویل بسته در این پروتکل نسبت به پروتکل‌های MFR و B-MFR گردیده است. پروتکل‌های MFR و B-MFR به سختی می‌توانند در مقابل خطرات و حملات خودروهای غیرمجاز مقاومت نمایند اما PRSP با استفاده از پروتکل کلید توافقی ایستگاه به ایستگاه برای ایجاد کلید نشست، کمک می‌نماید تا خودروهای دارای مجوز یکدیگر را تشخیص دهند و ارتباطات امن و مطمئنی را برقرار نمایند. با این پروتکل شبکه در مقابل رانندگان فاقد مجوز و حملات فیزیکی و منطقی آنان حفاظت‌شده و مقاوم می‌گردد. در نتیجه امنیت در VANET افزایش می‌یابد و به یک شبکه امن برای مسافران و رانندگان تبدیل خواهد شد.

مراجع

[1] F. Li, and Y. Wang, “Routing in vehicular ad hoc networks: A survey,” IEEE Vehicular Technology Magazine, vol.2, no.2, pp.12-22, June 2007
[2] H. Hartenstein, and K. P. Laberteaux, “A Tutorial Survey on Vehicular Ad Hoc Networks,” IEEE Communications Magazine, pp. 164-171, Jun 2008
[3] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust Location Privacy Scheme for VANET”, IEEE Journal on Selected Areas in Communications, Vol. 25, No. 8, Oct. 2007.
[4] M. Burmester, E. Magkos, and V. Chrissikopoulos, “Strengthening Privacy Protection in VANETs,” IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, pp. 508-513, 2008
[5] M. de Fuentes, A. I. Gonz?lez-Tablas, and A. Ribagorda, “Overview of security issues in Vehicular Ad-hoc Networks”, IGI Global, 2011.
[6] M. Mauve, J. Widmer, and H. Hartenstein, “A survey on position-based routing in mobile ad hoc networks,” IEEE Network, vol.15, no.6, pp.30- ,۳۹Nov.-Dec. 2001
[7] R.S. Raw, and D.K. Lobiyal, “B-MFR routing protocol for vehicular ad hoc networks,” Networking and Information Technology (ICNIT), 2010 International Conference on, pp.420-423, 11-12 June 2010
[8] S. Zeadally, R. Hunt, Y. S. Chen , A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenge,” Telecommunication System, Volume 50, Issue 4, pp. 217-241, August 2010
[9] T. Leinmuller, E. Schoch, and F. Kargl, “Position Verification Approaches for Vehicular Ad Hoc Networks,” IEEE Wireless Communications, vol.13, no.5, pp.16-21, October 2006
[10] T. Leinmuller, E. Schoch, and C. Maihofer, “Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks,” IEEE 4th Annual Conference on Wireless on Demand Network Systems and Services, pp.84-91, 2007
[11] U. Nagaraj, M. U. Kharat, and P. Dhamal, “Study of Various Routing Protocols in VANET,” International Journal of Computer Science & Technology, vol. 2, Issue 4, pp 45- 52 Oct. - Dec. 2011
[12] X. Liu, Z. Fang, and L. Shi, “Securing Vehicular Ad Hoc Networks,” IEEE 2nd International Conference on

Pervasive Computing and Applications, pp.424-429, 26-27 July 2007
[13] Y. Gongjun, S. Olariu, and M. Weigle, “Providing location security in vehicular Ad Hoc networks,” IEEE Wireless Communications, vol.16, no.6, pp.48-55, December 2009