علوم رایانش و فناوری اطلاعات
نشریه علمی انجمن کامپیوتر ایران
مجلد ۱۹، شماره ۱، ۱۴۰۰
صفحات ۳۶- ۵۱
مقاله عادی

شناسایی و جلوگیری از رفتار خودخواهانه‌ی گره‌های شبکه‌های سیار موردی با استفاده از نظریه‌ی بازی

غلامرضا فراهانی[1*]

[*]نویسنده مسئول، دریافت: ۱۴۰۰/۰۲/۱۶، بازنگری: ۱۴۰۰/۰۳/۲۳، پذیرش: ۱۴۰۰/۰۴/۱۸

[1] دانشیار، پژوهشکده برق و فناوری اطلاعات، سازمان پژوهشهای علمی و صنعتی ایران، تهران، ایران

چکیده

یکی از مشکلات موجود در شبکه سیار موردی، شناسایی گره‌های خودخواه و جلوگیری از رفتار خودخواهانه آن‌ها است. در این مقاله الگوریتم جدیدی با نام DMS پیشنهاد شده است که بتواند به طور موثری گره‌های خودخواه را شناسایی کرده و بسته اطلاعاتی را تنها از طریق مسیر با بالاترین تابع وزن از گره مبدأ به گره مقصد منتقل کند. در DMS رفتار خودخواهانه گره‌ها در فاز اول با ترکیب الگوریتمهای نرخ دریافت و ارسال بسته و آستانه تطبیقی اصلاح‌شده، تشخیص داده شده است. در فاز دوم از رفتار خودخواهانه با استفاده از نظریه بازی‌های تکراری جلوگیری می‌شود. نتایج شبیه‌سازی نشان‌دهنده بهبود عملکرد روش پیشنهادی نسبت به سایر روش‌ها در نسبت تحویل بسته، تأخیر انتها به انتها، نسبت از دست دادن بسته و توان عملیاتی است. نسبت تحویل بسته در روش DMS به ترتیب نسبت به WSISB، LTCF، RDG، HGT و CRG برابر ۴۹.۸۲٪، ۳۹.۹۸٪، ۷۱.۴۳٪، ۲۴٪ و ۱۱.۵۷٪ افزایش یافته است. این میزان بهبود در توان عملیاتی به ترتیب نسبت به WSISB، LTCF، RDG، HGT و CRG برابر ۳۷.۷۴٪، ۳۹.۹۵٪، ۴۸.۴۰٪، ۲۱.۶۵٪ و ۱۰.۸۹٪ است. همچنین DMS تأخیر انتها به انتها و میزان از دست دادن بسته را نسبت به سایر روش‌ها کاهش داده است.

کلمات کلیدی: نظریه بازی، گره خودخواه، رفتار خودخواهانه، شبکه سیار موردی، نظریه بازی‌های تکراری

۱- مقدمه

با ظهور دستگاه‌های رایانه‌ای قابل‌حمل پیشرفته و در کنار آن پیشرفت محسوس در فناوریهای ارتباط بی‌سیم، پردازش بی‌سیم از یک رؤیا به واقعیتی روزمره تبدیل‌شده است. رایانه‌ها از قابلیت‌های بیشتر همچون پردازش قوی و فضای کافی برخوردار شده‌اند که جلوه‌ای نو به شبکه‌های سیار موردی (MANETs[1]) می‌بخشد. شبکه سیار موردی یک شبکه سیار و بی‌سیم نظیر به نظیر است که فاقد هرگونه زیرساخت ثابت و یا سرویس‌دهنده مرکزی می‌باشد. این شبکه‌ها بدون زیرساخت، پویا و غیرمتمرکز هستند و به دلیل راحتی، پویایی، مقیاس‌پذیری، هزینه کم و راه‌اندازی آسان، توجه زیادی را به خود جلب می‌کند. هدف شبکه‌های سیار موردی، گسترش پویایی در ناحیه‌ای است که مجموعه‌ای از گره‌ها ساختار مسیریابی شبکه را به‌صورت بی‌سیم شکل می‌دهند. این شبکه‌ها اغلب در مناطقی که پیشرفت سریع و پیکربندی دوباره‌ی پویا لازم است و شبکه‌های سیمی در دسترس نیستند، کاربرد فراوان دارند. شبکه‌های سیار موردی زیرمجموعه شبکه‌های ویژه هستند که نشان‌دهنده‌ی سیستم‌های توزیع‌شده‌ی پیچیده‌ای هستند که شامل گره‌های بی‌سیم می‌باشند، با این قابلیت که گره‌ها می‌توانند آزادانه حرکت کنند [۱].

هر گره در شبکه‌های سیار موردی به‌عنوان یک مسیریاب عمل کرده و با سایر گره‌ها ارتباط برقرار می‌کند؛ بنابراین، در شبکه سیار موردی، ارتباطات شبکه بر همکاری متقابل بین گره‌ها برای انتقال داده بزرگ تکیه دارد که این یک مزیت محسوب می‌شود. اما شبکه سیار موردی بر این فرض است که هر گره، همکار و قابل اعتماد است. بااین‌حال، برخی از گره‌ها ممکن است در واقعیت رفتاری خودخواهانه داشته باشند [۲].

حضور گره‌های خودخواه[2] در شبکه سیار موردی ممکن است به کل سیستم ارتباطی آسیب برساند. گره‌ها ممکن است در شبکه خودخواهانه رفتار کنند و به‌جای ارسال بسته‌ها، آن‌ها را دور بیاندازند. بنابراین، شناسایی این گره‌های

خودخواه و ترویج همکاری در شبکه ضروری است [۳]. برای دسترسی بیشتر، داده‌ها اغلب در گره‌هایی به‌جز دارنده اصلی آن کپی شده تا دسترسی داده در صورت بروز از هم گسیختگی، قابل حصول‌تر باشد. به‌طورکلی مکانیزم تکرار داده می‌تواند به‌طور هم‌زمان دسترسی داده را بیشتر کرده و در عین‌حال تأخیر درخواست را نیز کاهش دهد؛ البته اگر گره‌های شبکه، فضای کافی برای ذخیره داده‌ها داشته باشند [۴].

در این شبکه‌ها ممکن است گره‌ها مایل به همکاری تمام و کمال در راستای به ثمر رسیدن اهداف شبکه نباشند؛ مواردی همچون ارسال بسته‌های دریافتی و نیز مشارکت در فرآیند ذخیره‌سازی موقتِ تکرار داده از این جمله‌اند. رفتار خودخواهانه در قالب گره‌هایی که سعی در حفظ منابع خود، مانند عمر باتری و پهنای باند دارند و در تلاش برای دریافت بیشترین مزایا از شبکه سیار موردی هستند، رخ می‌دهد [۵].

با این وجود عدم همکاری گره خودخواه در فرآیندهای گروهی در نهایت باعث پایین آمدن کارایی شبکه می‌شود که منجر به متضرر شدن خود گره خودخواه نیز خواهد شد. در نتیجه رفتار خودخواهانه به‌طور بالقوه توان عملیاتی را کاهش داده، تأخیر را افزایش داده و عملکرد شبکه سیار موردی را کاهش می‌دهد. بنابراین، اگر هر گره شبکه تصمیم بگیرد که خودخواهانه عمل کند، کل شبکه می‌تواند از بین برود. چنین شرایطی موقعیت راهبردی و عدم تعادل نامیده می‌شود؛ یعنی شرایطی که باید یک توازن بین داشته‌ها و داده‌ها، در دسترس بودن داده و تأخیر درخواست با منابع هر گره ایجاد کرد، وجود ندارد. در نتیجه طراحی روشی که سبب همکاری میان گره‌های خودخواه شبکه شود، ضروری به نظر می‌رسد. شیوه‌های شناسایی گره‌های خودخواه و برخورد با آن‌ها در مبحث تکرار داده‌ها با استفاده از مفاهیم مطرح‌شده در نظریه‌ی بازی‌ها قابل پیاده‌سازی می‌باشند [۶].

هدف در این مقاله شناسایی حداکثری گره‌هایی که دارای رفتار خودخواهانه هستند و جلوگیری از بروز رفتارهای خودخواهانه در آنها به‌منظور بهره‌برداری حداکثری از منابع شبکه و اجبار گره‌های خودخواه به شرکت در ارتباطات شبکه سیار موردی می‌باشد.

در بخش دوم این مقاله، نحوه مسیریابی و برقراری ارتباط در شبکه‌های سیار موردی مورد بررسی قرارگرفته است. در بخش سوم، نظریه بازی به همراه انواع بازی‌ها به طور مختصر بیان شده است. در بخش چهارم، راهبردهای مختلف کشف گره خودخواه در شبکه‌های سیار موردی مورد بررسی قرار گرفته و الگوریتمهای مختلف مورد مقایسه قرار گرفته‌اند. بخش پنجم، روش پیشنهادی را بیان می‌کند که نحوه مسیریابی، الگوریتم‌های تشخیص گره خودخواه و نحوه جلوگیری از رفتار خودخواهانه گره‌ها بر اساس نظریه بازی ارائه شده است.

در بخش ششم سناریوی شبیه‌سازی، نحوه شبیه‌سازی و پارامترهای شبیه‌سازی بیان شده و در ادامه این بخش پارامترهای مورد استفاده جهت ارزیابی روش پیشنهادی و مقایسه آن با روش‌های دیگر ارائه شده است. در انتهای بخش به ارزیابی عملکرد و تحلیل نمودارها پرداخته شده است. بخش هفتم نتیجه‌گیری مقاله را بیان می‌کند.

۲- مسیریابی در شبکه‌های سیار موردی

هدف اولیه شبکه‌های موردی برقراری یک یا چند مسیر مابین دو گره است که آن‌ها بتوانند با یکدیگر ارتباط قابل اعتمادی را برقرار نمایند. در این شبکه‌ها هر گره‌ای ممکن است وارد شبکه شود و یا شبکه را ترک نماید؛ بنابراین پروتکل‌های این شبکه می‌بایست خود را با این شرایط سازگار نمایند. ازاین‌رو، این مسئله موجب می‌شود که عملیات مسیریابی بین مبدأ و مقصد دچار مشکل گردد؛ بنابراین پیدا کردن مسیر و نگهداری آن از مسائل مهم موردبحث در این‌گونه شبکه‌ها است.

تاکنون پروتکل‌های مسیریابی زیادی در این زمینه معرفی شده‌اند. به‌طورکلی، مسیریابی در شبکه‌های موردی به دو گروه واکنشی[۳] و کنشی[۴] تقسیم می‌شوند. روش‌های مسیریابی کنشی، به ازای هر مقصد، یک جدول مسیریابی ایجاد می‌کنند و برای به‌روز نگه‌داشتن اطلاعات هم‌بندی، تغییرات مسیر را به‌طور مداوم ثبت کرده و مسیرها را تا همه‌ی مقصدها، جدا محاسبه می‌کنند. روش‌های واکنشی، مسیرهای بین مبدأ و مقصد را بلافاصله پس از تقاضای مسیر ایجاد می‌کنند [۷]. عمده روش‌های مورد استفاده برای مسیریابی در شبکه‌های سیار موردی عبارتند از:

- روش‌های مبتنی بر جدول[۵]
- روش‌های مبتنی بر درخواست[۶]
- روش‌های ترکیبی[۷]

در ادامه هرکدام از این روشهای مسیریابی مختصراً توضیح داده شده است.

۲-۱- روش‌های مبتنی بر جدول یا کنشی

پروتکل‌های مسیریابی کنشی از دسته پروتکل‌های اینترنتی حالت - پیوند[۸] و بردار - فاصله[۹] مشتق شده‌اند [۷]. این پروتکل‌ها سعی می‌کنند که برای هر جفت از گره‌های شبکه، اطلاعات مسیریابی را با انتشار اطلاعات مسیر و در مدت‌زمانی ثابت، پایدار و به‌روز نگه‌دارند. این روشها اغلب از جداول برای نگهداری اطلاعات مسیریابی استفاده می‌کنند، لذا عنوان مبتنی بر جدول به آن‌ها داده‌اند.

این پروتکل‌ها، مسیرهای مستقل از الگوی ترافیکی را تشخیص می‌دهند و آن را در تمام مدت حفظ می‌کنند. ویژگی اصلی این پروتکل‌ها، نگهداری مسیری ثابت به تمام گره‌های دیگر شبکه توسط هر گره است. تشکیل و نگهداری مسیر، هم به‌صورت پیام‌های دوره‌ای[۱۰] و هم پیام‌های مبتنی بر رویداد انجام می‌شود. مزیت این روش در این است که در هر لحظه که به مسیر احتیاج داشتند، مسیر برای آن‌ها موجود است. چون تمام گره‌ها یک مسیر به‌روز شده را برای هر گره دیگر در شبکه مدیریت می‌کنند؛ لذا یک مبدأ به‌سادگی جدول مسیریابی خود را به سمت مقصد چک کرده و بسته‌های مرتبط با آن را در صورت وجود مسیر، ارسال می‌کند [۷].

در این پروتکل‌ها، هر گره اطلاعات مسیریابی همه‌ی گره‌های دیگر شبکه را نگهداری می‌کند. بنابراین برای این پروتکل‌ها در شبکه‌های بزرگ یا در شبکه‌هایی که حرکت سریع گره‌ها وجود دارد، مسئله‌ی کنترل سربار چالش مهمی است [۱،۷].

۲-۲- روش‌های مبتنی بر درخواست یا واکنشی

پروتکل‌های مبتنی بر درخواست، فقط زمانی که به مسیری نیاز باشد آن را تشکیل می‌دهند. گره مبدأ در فرآیند اکتشاف مسیر، یک درخواست مسیر ساخته و تا هنگامی‌که مقصد غیرقابل‌دسترس و یا آن مسیر منقضی نشده باشد، نگه‌داشته می‌شود. این روش مصالحه بهتری نسبت به روش مبتنی بر جدول دارد و وابسته به ترافیک و الگوی حرکتی گره‌ها می‌باشد. در ضمن سربار کمتری دارد، زیرا هر زمان که نیاز باشد، مسیر بین دو گره را جستجو می‌کنند [۸].

تکنیک‌های مسیریابی مبتنی بر درخواست که پایه‌ی مکانیزم درخواست - پاسخ می‌باشند، برای ارسال بسته‌های درخواست و کشف مسیر، متکی به روش‌های سیل‌آسا هستند. الگوریتم‌های مبتنی بر درخواست، مشکل تأخیر در کشف مسیر برای کاربردهای زمان واقعی دارند و همچنین مکانیزم جستجوی سراسری به‌صورت سیل‌آسا، ترافیک کنترلی قابل‌توجهی را به دنبال دارد. از سوی دیگر الگوریتم‌های مبتنی بر جدول نیز برای محیط‌های شبکه بی‌سیم بلادرنگ مناسب نیستند؛ زیرا بخش بزرگی از ظرفیت‌های شبکه را صرف نگهداری اطلاعات مسیریابی می‌کنند.

از آنجایی که گره‌ها در محیط‌های شبکه بی‌سیم بلادرنگ ممکن است خیلی سریع حرکت کنند و نرخ تغییرات در هم‌بندی از نرخ درخواست‌های کشف مسیر بیشتر باشد، بسیاری از این اطلاعات حتی یک‌بار هم استفاده نمی‌شوند. در این دسته، مسیرها تنها در هنگام نیاز ساخته می‌شوند و مشتمل بر دو مرحله کشف مسیر و نگهداری مسیر می‌باشند. این دسته پروتکل‌ها در مصرف منابع شبکه صرفه‌جویی می‌کنند، اما تأخیر بیشتری در مقایسه با روش مبتنی بر جدول دارند [۷].

پروتکل‌های مسیریابی واکنشی برای کاهش سربار پروتکل‌های مبتنی بر کنش طراحی‌شده‌اند که فقط اطلاعات مربوط به مسیرهای فعال را نگهداری می‌کنند. برای کشف مسیر، بسته‌های درخواست مسیر (RREQ[۱۱]) در شبکه به‌صورت سیل‌آسا ارسال می‌شوند و گره‌ی دریافت‌کننده‌ی RREQ درصورتی‌که مقصد موردنظر باشد یا مسیری به مقصد داشته باشد، برای ساخت مسیر، بسته پاسخ مسیر (RREP[۱۲]) را تولید و به مبدأ ارسال می‌کند. مزیت این پروتکل‌ها کاهش سربار و عیب آن‌ها معرفی مرحله‌ی پنهانی کشف مسیر می‌باشد [۱,۹].

۲-۲-۱- الگوریتم مسیریابی AODV

الگوریتم مسیریابی AODV[۱۳] [۱۰]، در سال ۱۹۹۹ توسط Royer و Perkins توسعه پیدا کرد. این الگوریتم با قابلیت پویایی مسیریابی چند گامی طراحی‌شده و اساساً ترکیبی از الگوریتم‌های DSDV[۱۴] و DSR[۱۵] می‌باشد و بسیاری از خصوصیات الگوریتم DSR را برای افزایش کارایی و اطمینان به کار می‌برد. در اغلب موارد AODV همانند DSR عمل می‌کند، اما بهینه‌سازی‌های اندکی در آن انجام شده که این بهبودها در زمینه‌ی انتشار محلی، جداول مسیریابی محلی و توانایی ترمیم بهتر مسیر می‌باشد و در الگوریتم AODV گره‌ها با انتشار دوره‌ای پیام hello، لیستی از همسایگان خود را به‌صورت فعال نگه می‌دارند.

پیام‌های hello دو مزیت دارند. اولاً در حین اکتشاف مسیر گره مجاور مقصد، از وجود مقصد اطلاع پیدا می‌کند و پاسخ مسیر را بدون آنکه با مقصد ارتباط برقرار کند، به روش DSR به مبدأ ارسال می‌کند. دوماً تغییر در هم‌بندی شبکه به سرعت در گره‌های همسایه مشاهده می‌شود. AODV نه‌تنها با جداول مسیریابی مبدأ و مقصد همکاری می‌کند، بلکه از جداول مسیریابی گره میانی هم کمک می‌گیرد [۱۰].

۲-۳- روش‌های ترکیبی

چیزی که بدان نیاز است پروتکلی است که عملیات کشف مسیر را به‌صورت مبتنی بر درخواست انجام دهد و در عین حال هزینه جستجوی کمی هم داشته باشد. پروتکل مسیریابی ناحیه‌ای، امکان کشف به صورتی کارا و سریع با ترکیب دو کلاس مذکور از الگوریتم مسیریابی سنتی را فراهم می‌آورد.

یک پروتکل کنشی برای شبکه‌های بزرگ در هر زمان نیاز به جدول مسیریابی بزرگ دارد، بنابراین برای شبکه‌های بزرگ مناسب نیست. از طرفی بر اساس فرآیند کشف مسیر، یک پروتکل واکنشی برای شبکه‌های بزرگ تأخیر بسیار دارد؛ بنابراین استفاده از پروتکلی که ترکیب هر دو روش باشد به نظر راه‌حل بهتری می‌آید. اکثر پروتکل‌های طراحی‌شده تا به امروز، مبتنی بر منطقه‌اند به این معنی که شبکه به‌عنوان تعدادی از مناطق توسط هر گره در نظر گرفته می‌شود. گره‌های دیگر به درختان یا خوشه‌ها گروه‌بندی می‌شوند [۹].

۳- نظریه بازی

در حال حاضر نظریه بازی در حوزه اقتصادی به عنوان شاخه‌ای مستقل، مهم و متفاوت از نظریات سنتی علم اقتصاد برای تحلیل روابط اقتصادی به کار گرفته می‌شود. این نظریه به مطالعه مواردی می‌پردازد که در آن تصمیم و رفتار بازیگر اقتصادی علاوه بر رفتار و تصمیمات خود او، به رفتار و تصمیمات بازیکنان دیگر نیز بستگی دارد.

در بازی‌های موسوم به «بازی با حاصل جمع صفر»، منافع بازیکن‌ها به‌طور کامل با یکدیگر تعارض پیدا می‌کند؛ به‌گونه‌ای که کسب بهره توسط یک فرد، همواره معادل ضرر فرد دیگر است [۱۱].

مفاهیم نظریه بازی زمانی بکار می‌رود که عمل و نقش چند عامل روی‌هم اثر می‌گذارند. این عوامل ممکن است افراد، گروه‌ها، شرکت‌ها و یا هر ترکیبی از آن‌ها باشد. مفاهیم نظریه بازی زبانی را ارائه می‌دهد که بتوان سناریوهای راهبردی را فرموله کرد، ساختار آن را معین نمود، آن‌ها را تجزیه و تحلیل کرده و درک نمود [۱۲].

در نظریه بازی یک «حرکت» تا آنجایی که قواعد بازی اجازه می‌دهند، انتخابی از یک مکان به مکان دیگر است. حرکت‌ها به دو دسته «شخصی» و «تصادفی» تقسیم می‌شوند؛ حرکت شخصی، انتخاب آگاهانه بازیگر در تمامی حرکات ممکن در یک وضعیت فرضی است. در مقابل حرکت تصادفی، انتخابی است مابین تعدادی از امکانات که نه به وسیله تصمیم بازیگر بلکه به وسیله بعضی وسایل تصادفی تحقق می‌یابد [۱۳].

۳-۱- تفسیر نظریه بازی

تفسیر کلاسیک نظریه بازی این است که بازی‌ها باید نمایانگر قواعد فیزیکی و سازمانی بازی‌ها در جهان واقعی باشند. اما مدل‌های نظری بازی به‌طورکلی نمی‌توانند منعکس‌کننده قواعد فیزیکی و سازمانی جهان واقعی باشند و قواعد بازی‌ها معمولاً اختراع نظریه‌پردازان است.

هر یک از تصمیم‌گیران در محیط راهبردی «بازیگر» نامیده می‌شوند. فرض اساسی این است که در محیط راهبردی، بازیکن عاقلانه رفتار می‌کند؛ یعنی با در نظر گرفتن تأثیر احتمالی تصمیم خود بر دیگران، بازیکن تصمیمی را اتخاذ می‌کند که بیشترین منافع را در برداشته باشد [۱۳].

۳-۲- عناصر بازی‌ها

برای تعریف فضای بازی، مشخص کردن عناصر زیر لازم و کافی است [۱۴]:

- بازیکنان یا تصمیم‌گیرندگان: طرف‌های بازی که هرکدام حداقل دو راهبرد در اختیار دارند.
- راهبرد در اختیار هر بازیکن: زنجیرهای مرتب از اقداماتی است که بازیکن می‌تواند در قدم‌های مختلف بازی برگزیند.
- ترتیب بازی: این‌که در هر قدمی از بازی، چه بازیکنی حرکت می‌کند. ساختار اطلاعاتی در هر لحظه از بازی هر بازیکن، می‌تواند چه اطلاعاتی را از حرکت‌ها و ترجیحات طرف مقابلش بداند.
- خروجی‌های بازی: وقتی بازی به انتها می‌رسد چه نتایجی به بار می‌آید.

۳-۳- هدف نظریه بازی

هدف نظریه بازی، محاسبه راهبرد بهینه (مطلوب‌ترین رفتار) بازیگر در شرایط مخاصمه می‌باشد. در نظریه بازی، راهبرد بهینه برای یک بازیگر، آن است که وقتی به‌دفعات تکرار شود، بیشترین بهره متوسط را برای او به ارمغان آورد. در انتخاب این راهبرد، همواره فرض بر این است که حریف لااقل به‌اندازه خود ما در گزینش معقول مهارت دارد و اینکه هیچ‌چیز نمی‌تواند از رسیدن ما به مقصود جلوگیری نماید [۵].

۳-۴- فواید نظریه بازی

این نظریه می‌تواند برای کسانی که در موقعیت‌های خاص قرار می‌گیرند، بینشی جهت انتخاب گزینه‌های راهبردی ایجاد کند. با توجه به این بینش،

تصمیم‌گیرندگان بهتر می‌توانند به ارزیابی اثرات بالقوه از اعمال خود بپردازند و به احتمال زیاد به اهداف موردنظر خود دست پیدا کنند و مانع از درگیری شوند [۱۴].

۳-۵- تعادل نش[۱۶]

این تعادل غیرتعاونی را ابتدا جان-اف-نش برنده جایزه نوبل اقتصاد در سال ۱۹۹۴ میلادی مطرح نمود [۱۳]. در این مورد تعادل هر یک از بازیکنان بدون تبانی یا همکاری با دیگران و بدون توجه به رفاه جامعه یا هر یک از بازیکنان دیگر، بهترین راهبرد ممکن را در راستای منافع خویش اتخاذ می‌کند.

تعادل نش که تعادل راهبردی هم نامیده می‌شود، لیستی از راهبردهایی است که هیچ بازیکنی نمی‌تواند برای به دست آوردن نتیجه نهایی بهتر، آن‌ها را به‌طور یک‌جانبه تغییر دهد. در نظریه بازی، این قضیه مفروض را داریم که هر بازیکن پرداخت خودش را حداکثر می‌کند و همچنین هر بازیکن می‌داند که این هدف هر بازیکن دیگر است. به عبارتی لازمه سازگاری طبیعی این است که اعتقاد هر بازیکن درباره انتخاب‌های بازیکن دیگر، با انتخاب‌های واقعی بازیکن دیگر که قصد انجام آن را دارد، منطبق شود. تعادل نش نوع خاصی از «تعادل انتظارات عقلایی» است [۱۳].

دو دلیل اصلی برای اهمیت تعادل نش وجود دارد. دلیل اول فرض می‌کند که بازیکنان عاقل راه خود را به سمت حل بازی استدلال می‌کنند. دلیل دوم فرض می‌کند که مردم راه خود را به سمت حل بازی با تعدادی فرآیندهای تکاملی سعی و خطا می‌یابند. اغلب قدرت پیش‌بینی نظریه بازی از امکان رفت و برگشت در میان این دو تفسیر بر می‌خیزد [۱۵].

۴- راهبردهای مختلف کشف گره‌های خودخواه در شبکه سیار موردی

مشکل رفتار خودخواهانه در شبکه‌های سیار موردی در طول سالیان به‌طور گسترده مورد مطالعه قرارگرفته است و چندین رویکرد برای حل مشکل پیشنهاد شده است. این رویکردها را می‌توان به سه دسته تقسیم کرد: رویکرد مبتنی بر شهرت، رویکرد مبتنی بر اعتبار و رویکرد مبتنی بر بازی [۱۶].

۴-۱- رویکرد مبتنی بر شهرت

رویکرد مبتنی بر شهرت[۱۷] به ایجاد معیار معروفیت برای هر گره بر اساس الگوی رفتاری آن تکیه می‌کند. شناسایی و واکنش، دو ماژول پروتکل‌های مبتنی بر شهرت هستند. گره‌ها از ماژول تشخیص برای مشاهده اینکه گره‌های مجاور بسته‌ها را از دیگر گره‌ها باز انتقال می‌دهند، استفاده می‌کنند و از ماژول واکنش برای تغییر یا به‌روزرسانی جدول شهرت استفاده می‌کنند. معروف‌ترین الگوی مبتنی بر شهرت، طرح نظارت است که مواردی از ارسال بسته‌ها را با گوش دادن به انتقال گره همسایه خود شناسایی می‌کند [۱۷].

۴-۲- رویکرد مبتنی بر اعتبار

رویکرد مبتنی بر اعتبار[۱۸] از یک واحد پول مجازی یا پول واقعی برای پرداخت داده‌های باز ارسال‌شده توسط سایر گره‌ها استفاده می‌کند. همچنین از اعتبار برای جبران کاربرد منابع در فرآیند تقویت‌کردن استفاده می‌شود. گره‌ها می‌توانند با ارسال مجدد بسته‌ها یا تبادل پول واقعی اعتبار خود را افزایش دهند [۱۷].

۴-۳- رویکرد مبتنی بر نظریه بازی[۱۹]

در این رویکرد، ارسال و یا ارسال مجدد بین گره‌ها به‌صورت یک بازی مدل شده است که این بازی می‌تواند به‌صورت دو به دو و یا یک به چند باشد که برای هر بازی، تابع مطلوبیت[۲۰] تعریف می‌شود؛ به‌طوری‌که هر گره سعی در به دست آوردن ماکزیمم مقدار از تابع مطلوبیت دارد. هر گره‌ای که باعث شود تابع مطلوبیت دیگر گره‌ها کاهش یابد به عنوان گره خودخواه شناخته می‌شود و همچنین معادله نشی[۲۱] ارائه می‌شود که در آن‌همه گره‌ها به تعادل رسیده و علاقه‌ای به تعدی از آن ندارند [۱۸].

یک رویکرد مبتنی بر نظریه بازی ایستا، غیر همکار و تکرار متناهی برای شناسایی گره‌های خودخواه و تحریک آن‌ها جهت همکاری با سایر گره‌های شبکه در [۱۹] ارائه شده است. مکانیسم استفاده‌شده در این رویکرد، حراج دومین کمترین قیمت در چارچوب[۲۲] امنیت شبکه است. در این رویکرد گره مبدأ سعی در یافتن مسیری با کمترین هزینه برای ارسال بسته‌هایش را دارد و در حراجی، دومین کمترین مقدار را بکار می‌برد؛ چراکه اگر اولین کمترین مقدار را بکار ببرد ممکن است منجر به تبانی گره‌های خودخواه شود. مزایای این رویکرد، بالا بودن دقت کشف گره‌های خودخواه و بالا بودن کارایی و معایب آن بالا بودن سربار مسیریابی و به موازات آن پایین بودن کارایی در مقیاس بالا است.

رویکرد دیگری که برای شناسایی گره‌های خودخواه در شبکه ارائه شده است، شامل دو مرحله است. مرحله حفظ همکاری گره‌ها، به این معنی که عملکرد گره‌ها مورد نظارت قرار گرفته و در صورت عدم همکاری تنبیه می‌شوند. مرحله یادگیری، با این مفهوم که انتخاب بهترین گره برای پیش‌رانی بسته با به‌روزرسانی احتمالات انتخاب گره بعدی تشکیل‌شده و برای هر دو مرحله دو حالت مشاهده کل گره‌ها توسط همه و مشاهده محلی مفروض است. در این رویکرد استفاده از یک بازی تکراری بی‌نهایت منجر به تحریک بالای گره‌های خودخواه برای همکاری با سایر گره‌ها شده است. همچنین رویکرد ارائه‌شده یک رویکرد توزیعی بوده و در آن‌همه گره‌ها در تصمیم‌گیری دخالت دارند [۲۰].

یک رویکرد مبتنی بر نظریه بازی برای تشخیص ایستگاه‌های بی‌سیم خودخواه در شبکه‌های بی‌سیم چند نرخی در [۲۱] ارائه شده است. بازی مورد استفاده در این رویکرد برای تجمیع کاربران ایستگاه‌های بی‌سیم جهت جلوگیری از کارایی ناهمگن و ضعیف است که بر اساس تناسب و تجمیع تخصیص منابع و ایستگاه‌های بی‌سیم است.

سودی که در بازی نصیب ایستگاه‌های بی‌سیم می‌شود، بر اساس توان عملیاتی فردی هر ایستگاه است. روش پیشنهادی از یک بازی چانه‌زنی بهبودیافته و برخی خواص مربوط به کاربران، انگیزه بازیکنان را کنترل می‌کند. مکانیسم پیشنهادی می‌تواند به‌صورت یک‌لایه مجازی برای دستیابی به کارایی بهتر در کنترل دسترسی به رسانه کاربران اضافه شود. اگرچه روش پیشنهادی برای کنترل تجمیع کاربران پیشنهاد شده است؛ اما قابلیت کنترل ایستگاه‌های خودخواه و تحریک آن‌ها به همکاری را نیز دارد.

۴-۴- سایر رویکردها

در [۲۲] از یک طرح بهبودیافته مبتنی بر سیستم ایمنی مصنوعی (AIS[۲۳]) که از درخت تصمیم استفاده می‌شود، برای شناسایی گره‌های خودخواه استفاده می‌کند. در این روش گره‌های شبکه، گره‌های خودخواه یا گره‌هایی را که سعی دارند با جداسازی خود از مسیرهای مسیریابی، کارایی شبکه سیار موردی را کاهش دهند، جدا می‌کنند. در طرح ارائه شده از آنجائیکه نیاز به ارسال بسته‌های بیشتری جهت شناسایی گره‌های خودخواه و یافتن مسیری جایگزین به مقصد موردنظر است، لذا سربار مسیریابی بیشتری دارد.

یک طرح بهبودیافته برای شناسایی گره خودخواه در شبکه سیار موردی مبتنی بر پروتکل مسیریابی AODV در [۲۳] ارائه شده است. در این طرح، دو الگوریتم برای اطمینان از کمترین تصمیم خطای مثبت در تشخیص گره‌های خودخواه ادغام شده‌اند. ابتدا از تشخیص خطای مثبت گره‌های خودخواه در RREQ جلوگیری

می‌شود و سپس از تشخیص خطای مثبت گره‌های خودخواه در ارسال بسته‌های داده جلوگیری به عمل می‌آید. طرح ارائه شده بهبود عملکرد ارسال بسته از نظر نرخ تحویل بسته و تأخیر انتها به انتها را تضمین می‌کند.

۴-۵- مقایسه الگوریتم‌ها

در جدول ۱ روش‌ها و راهبردهای پیشنهادی مختلف برای کشف گره‌های خودخواه با یکدیگر مقایسه شده‌اند. هر کدام از روش‌ها دارای مزایا و معایبی می‌باشند؛ اما با نگاه اجمالی به جدول مشخص می‌شود که روش‌های ترکیبی و مبتنی بر نظریه بازی بهتر از سایر روش‌ها نتیجه می‌دهد.

۴-۶- مروری بر کارهای گذشته جهت مقابله با رفتار خودخواهانه گره‌ها

مشکل رفتار خودخواهانه در شبکه‌های سیار موردی در طول سالیان به‌طور گسترده مورد مطالعه قرار گرفته است و چندین طرح برای حل مشکل پیشنهاد شده است. نتایج کمی نشان می‌دهد که نسبت گره خودخواه در شبکه و تحرک گره‌ها، تأثیرات قابل توجهی بر عملکرد شبکه‌های سیار موردی از لحاظ معیارهای شبکه دارند. گره‌های خودخواه ساکن اثرات مخرب بیشتری نسبت به گره‌های پویا در شبکه به وجود می‌آورند، زیرا بسته‌های بیشتری توسط گره‌های خودخواه ساکن دور انداخته می‌شوند [۲۴].

در جدول ۲ خلاصه‌ی فعالیتهای مهم انجام‌گرفته در زمینه مقابله با رفتار خودخواهانه گره‌ها در شبکه‌های سیار موردی به طور خلاصه آورده شده است.

۵- روش پیشنهادی

رفتار خودخواهانه بر گذردهی و تأخیر در شبکه‌ها تأثیر می‌گذارد. از این‌رو، اگر بعضی از گره‌ها رفتار خودخواهانه در یک شبکه سیار موردی نشان دهند، گذردهی کاهش می‌یابد و تأخیر آن به‌سرعت افزایش می‌یابد. برای حل این مشکل، همان‌طور که در شکل ۱ نشان داده شده است یک طرح تشخیص و جلوگیری از رفتار خودخواهانه پیشنهاد شده است که DMS[۲۴] نامیده می‌شود.

این طرح شامل دو مرحله است: مرحله شناسایی و مرحله جلوگیری. در مرحله شناسایی، از یک الگوریتم بررسی بسته‌های دریافتی و ارسالی در هر گره و همچنین یک الگوریتم آستانه تطبیقی برای شناسایی گره‌ها یا رفتار خودخواهانه استفاده شده است. در مرحله جلوگیری از رفتار خودخواهانه، بر اساس نظریه بازی‌های تکراری عمل خواهد شد.

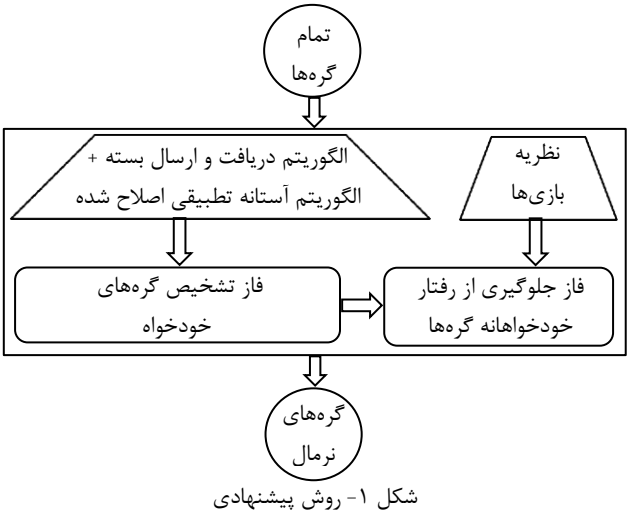
در روش پیشنهادی جهت مسیریابی از پروتکل مسیریابی AODV اصلاح‌شده استفاده می‌شود. علاوه بر این، با استفاده از فاکتور بالاترین تابع وزن (HWF [۲۵]) بسته‌های داده همیشه از گره مبدا به گره مقصد تنها از طریق مسیر با بالاترین وزن ارسال خواهد شد که در نتیجه آن، کوتاه‌ترین مسیر با بیشترین انرژی گره‌ها انتخاب خواهد شد. بنابراین این طرح، کمترین مقدار زمان بیکاری گره‌ها را تضمین می‌کند و همکاری در شبکه را افزایش می‌دهد. فلوچارت ارائه شده در شکل ۲، مراحل مختلف روش پیشنهادی را نشان می‌دهد.

جدول ۱- مقایسه الگوریتم‌ها برای کشف گره‌های خودخواه

عنوان	نوع	مزایا	معایب
رویکرد مبتنی بر پول مجازی [۱۷]	مبتنی بر اعتبار	منصفانه بودن، بهبود عملکرد شبکه، کشف سریع گره‌های خودخواه	عدم تعیین دقیق گره خودخواه، مصرف انرژی زیاد
روش Ji [۱۹]	مبتنی بر نظریه بازی	بالا بودن دقت کشف، بالا بودن کارایی	سربار بالا در مقیاس‌های بزرگ، مصرف انرژی زیاد
روش Pandana [۲۰]	مبتنی بر نظریه بازی	قابل‌اعتماد، کم بودن سربار	مناسب برای شبکه‌های کوچک، مصرف انرژی زیاد
روش Touati [۲۱]	مبتنی بر نظریه بازی	مصرف کم انرژی، کارایی بالا، کم بودن سربار	امکان قضاوت نادرست
روش AIS [۲۲]	مبتی بر سیستم ایمنی مصنوعی	جداسازی گره‌های خودخواه با دقت بالا و یافتن مسیر جایگزین برای بسته-های ارسالی در شبکه	بالا بودن سربار بسته‌ها برای مسیریابی
روش گره نگهبان Watchdog [۲۵]	مبتنی بر شهرت	کشف تعداد زیادی از گره‌های خودخواه در شبکه	تصادم مبهم، تصادم در گیرنده، برد محدود ارسال، تبانی، دور انداختن مقطعی بسته، سوء رفتار با تغییر برد ارسالی
روش HEAD [۲۶]	مبتنی بر شهرت	کشف زیاد و دقیق گره‌های خودخواه، کشف سریع	مصرف انرژی بالا، غیرقابل اعتماد
روش SDA[۲۶] [۲۷]	مبتنی بر شهرت	قابل‌اطمینان بودن	مصرف انرژی بالا، سریع نبودن، سرعت کشف
روش SNRRM[۲۷] [۲۸]	مبتنی بر شهرت	حذف گره خودخواه در حین مسیریابی، مصرف بهینه انرژی	عدم تعیین دقیق گره خودخواه
روش GRTS[۲۸] [۲۹]	مبتنی بر شهرت	در نظر گرفتن عامل پاداش برای شهرت گره، یافتن مسیر قابل اعتماد	افزایش سربار شبکه، نیاز به حافظه
روش SPRIT [۳۰]	مبتنی بر اعتبار	مصرف انرژی کمتر، عدم وجود سربار نظارت گره	سربار بسته‌ها، مناسب برای شبکه‌های کوچک، مشکل محاسبه اعتبار
روش MODSPRIT [۳۱]	مبتنی بر اعتبار	کاهش احتمال شکست، مصرف انرژی کمتر، عدم وجود سربار نظارت گره	سربار بسته‌ها، محاسبه اعتبار و پرداختی‌ها، انتخاب سرخوشه
روش NUGLETS [۳۲]	مبتنی بر اعتبار	عدم وجود سربار نظارت گره	مصرف انرژی زیاد، نیاز به حافظه، سربار بالای بسته‌ها
روشهای NCV[۲۹] و iNCV[۳۰] [۳۳]	مبتنی بر اعتبار	ارسال تعدادی بسته ساختگی از گره‌های بیکار در NCV-AODV جهت جلوگیری از تشخیص آنها به عنوان گره خودخواه، در روش iNCV-AODV فرض می‌شود که گره‌ها ذاتاً خودخواه نیستند و فقط بعضی از گره‌ها ممکن است توسط دشمنان اضافه شوند تا رفتار خودخواهانه داشته باشند، محاسبه مقدار اعتبار همسایگان به روش موثر	افزایش سربار شبکه

جدول ۲- مرور روش‌های مختلف مقابله با رفتار خودخواهانه گره‌ها در شبکه‌های سیار موردی

روش	توضیح
Reputation-based and Credit-based	در [۳۴] از دو روش تغییر در دو پروتکل DSR و AODV برای خنثی کردن اثر گره‌های خودخواه در شبکه‌ی سیار موردی استفاده شده است. در [۳۵] یک رویکرد امن مبتنی بر وزن برای شناسایی رفتار خودخواهانه در شبکه سیار موردی پیشنهاد می‌شود (WSISB[۳۱]). روش پیشنهادی از تابع وزن برای تشخیص فعالیت‌های خودخواهانه استفاده کرده و گره خودخواه را شناسایی و برای جلوگیری از رفتار خودخواهانه، آن را حذف می‌کند. همچنین مسیر مورد اعتماد برای انتقال داده را کشف خواهد کرد.
Security-based algorithm	تمرکز بر روی تعداد بسته‌هایی است که توسط گره‌ها از دست می‌روند [۳۶,۳۷].
Watchdog approach	این روش با استفاده از یک یا چند گره‌ی نگهبان، میزان خودخواهی گره‌ها را ارزیابی می‌کند. ایده اصلی تخمین زمان شناسایی سربارى که در گره‌های نگهبان برای شناسایی گره‌ی خودخواه به وجود می‌آید، می‌باشد [۳۸].
RTBD[۳۲]	در تکنیک RTBD، اساس بر ارزیابی و سنجش اعتبار همسایه قرار داده‌شده است. در طی زمان، گره‌های خودخواه شناسایی شده و اطلاعات جدید در اختیار همسایه قرار می‌گیرد [۳۹].
Game theoretical method	در [۴۰] استفاده از ایده‌ی معمای داوطلب (تنها از ایده نه فرمول‌ها) برای ترغیب گره‌ها به تکرار داده استفاده شده است و تمرکز بر روی تکرار داده است. در [۴۱] استفاده از بازی‌های تصادفی (بازی توسط خود نویسندگان طراحی‌شده) برای مسئله‌ی ارسال روبه‌جلوی بسته[۳۳] در شبکه‌های رله مطرح و بررسی شده است که از کانال مشترک استفاده می‌کنند. در [۴۲] یک بازی طراحی‌شده توسط نویسندگان ارائه شده که به هر گره تابع ارزش اختصاص داده شده است، تا بتواند تشخیص دهد که هر گره چه هزینه‌ای برای خواندن یا به‌روزرسانی بکار خواهد برد. تمرکز این روش بر روی تکرار داده می‌باشد. در [۴۳] از یک الگوریتم آستانه تطبیقی برای تشخیص رفتار خودخواهانه استفاده می‌شود و بر پایه یک طرح بازی‌های تکراری از آن جلوگیری می‌شود. در[۴۴] یک پروتکل مسیریابی تحمل‌پذیر خطا و در زمان واقعی مبتنی بر نظریه بازی (GTRF[۳۴]) پیشنهاد شده است. در[۴۵] یک الگوریتم کنترل هم‌بندی بهره‌ور انرژی (EETCA[۳۵]) با استفاده از رویکرد نظریه بازی پیشنهاد می‌شود که در آن کاربرد گره به خودخواهی همسایگان، نرخ ترافیک لینک و طول لینک وابسته است. در [۴۶] از روش بازی دیلمای تکراری (RDG[۳۶]) جهت جلوگیری از رفتار خودخواهانه گره‌ها در شبکه استفاده می‌کند. در این روش از هیچ تابع وزنی برای تعیین مسیر مناسب استفاده نمی‌شود. در [۴۷]، یک طرح نظریه بازی جدید برای تشخیص گره خودخواه در شبکه سیار موردی پیشنهاد شده است که علاوه بر تشخیص گره‌های خودخواه، با استفاده از کم‌ترین ضریب هزینه (LTCF[۳۷])، بسته‌های داده از گره مبدا به گره مقصد تنها از طریق مسیر با کمترین هزینه منتقل خواهند شد. شناسایی گره‌های خودخواه بر اساس تئوری بازی سلسله مراتبی (HGT[۳۸]) در [۴۸] ارائه شده است. روش پیشنهادی شامل سه مرحله است. رویه راه-اندازی و الگوریتم خوشه‌بندی در مرحله اول اجرا می‌شود. در مرحله دوم، گره‌های هر خوشه برای اجرای یک بازی تکراری بی‌نهایت، در حالیکه بسته‌های داده خود یا همسایه را انتقال می‌دهند؛ با یکدیگر همکاری می‌کنند. در مرحله سوم، هر گره عملکرد گره‌های همسایه خود را برای ارسال بسته‌های داده رصد می‌کند و روند همکاری برای تعیین گره‌های خودخواه که بسته‌های داده را با تأخیر ارسال می‌کنند یا حتی آنها را ارسال نمی‌کند، مورد تجزیه و تحلیل قرار می‌گیرد. گره‌های دیگر شهرت گره‌هایی که با آنها همکاری نمی‌کنند را کاهش می‌دهند و آنها به عنوان مجازات با گره‌های خودخواه همکاری نمی‌کنند. بنابراین، گره‌های خودخواه برای همکاری تحریک می‌شوند. در [۴۹] یک طرح مجازات پویا برای گره‌های خودخواه با استفاده از بازی تکراری مشارکتی (CRG[۳۹]) جهت جلوگیری از رفتارهای خودخواهانه گره در شبکه سیار موردی و تحریک آنها به مشارکت ارائه شده است. این طرح مربوط به مجازات مشارکتی همه گره‌های شبکه، برای مجزا کردن گره خودخواه است تا این گره را برای همکاری با سایر اعضا تحریک کند. راهبرد مجازات استفاده شده به صورت چهار مرحله ذیل اجرا می‌شود. حالت برده[۴۰]: که در آن همه همسایگان از این گره برای انتقال یا تبادل داده با گره‌های دیگر استفاده می‌کنند. فرسودگی منابع[۴۱]: که از منابع گره مجازات شده به صورت حریصانه برای تصحیح رفتار گره خودخواه استفاده می‌شود. تعیین تعداد تکرار مجازات: که تعداد تکرارهایی است که گره خودخواه در حالت برده باقی بماند تا از تصحیح رفتار گره خودخواه اطمینان حاصل شود. نظارت: برای نظارت بر عملکرد گره خودخواه قبل از اینکه یک گره قانونی در نظر گرفته شود.

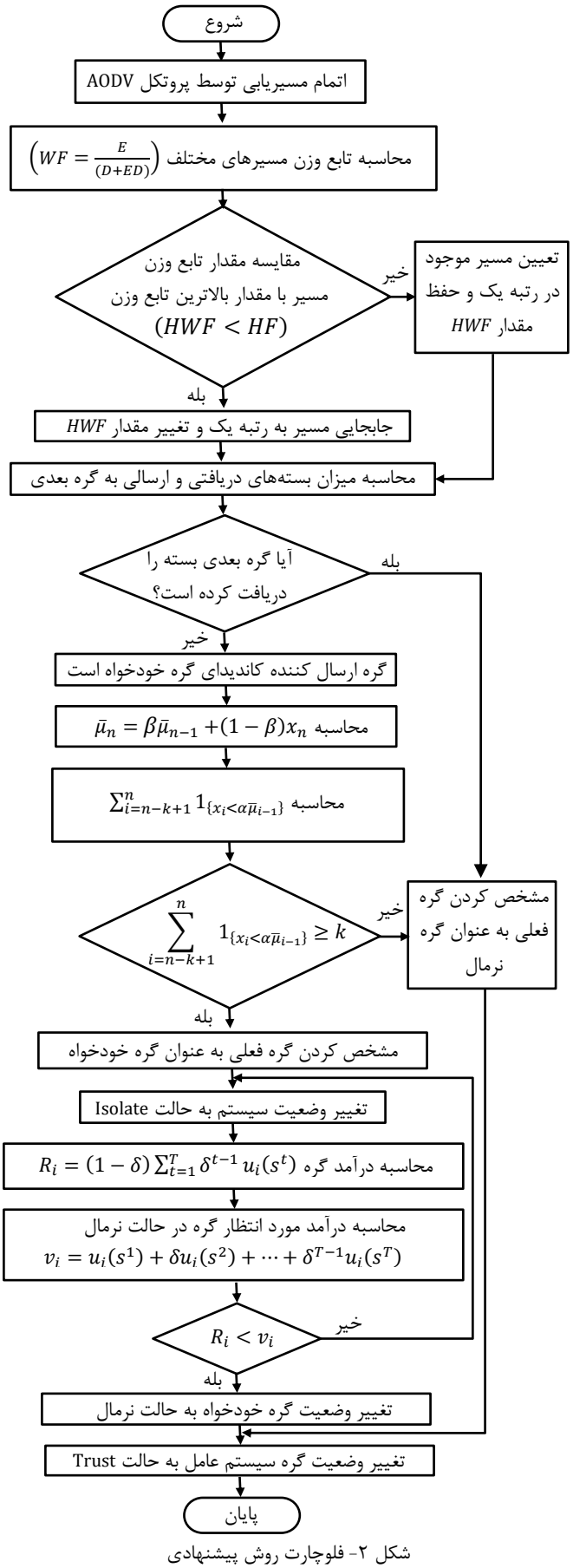


شکل ۱- روش پیشنهادی

۵-۱- مسیریابی

مطابق با پروتکل مسیریابی AODV، در ابتدا هر گره منفرد از شبکه، پیام "سلام" (hello) را به تمام گره‌های همسایه خود که به‌طور مستقیم به آن متصل هستند، ارسال خواهد کرد. بعد از دریافت پیام "سلام"، تمام گره‌های همسایه اطلاعات گره‌های مجاور را که پیام "سلام" ارسال کرده‌اند را به جدول مسیریابی خود اضافه خواهند کرد. هر گره یک جدول مسیریابی دارد که شناسه‌های گره‌های همسایه خود را همراه با بالاترین تابع وزن ذخیره می‌کند.

اگر یک گره مبدا بخواهد داده‌ها را به گره مقصد ارسال کند، ابتدا گره مبدا جدول مسیریابی خود را چک خواهد کرد تا گره مقصد را جستجو کند. اگر گره مقصد در جدول مسیریابی گره مبدا وجود نداشته باشد، آنگاه گره مبدا پیام RREQ را به تمام گره‌های همسایه خود ارسال خواهد کرد. هر یک از گره‌های همسایه آن، پیام RREQ دریافت شده به گره‌های همسایه خود را مجدداً مورد همه پخشی قرار خواهند داد.



شکل ۲- فلوچارت روش پیشنهادی

این فرآیند چندین بار به این روش ادامه می‌یابد تا زمانی که به گره مقصد برسد. وقتی‌که گره مقصد پیام‌های RREQ ارسال‌شده توسط همسایگان خود را دریافت می‌کند، گره مقصد پیام RREP را به گره همسایه خود که از آن پیام RREQ توسط گره مقصد دریافت شده است، پاسخ خواهد داد. در این فرآیند وقتی گره مقصد ابتدا با پیام RREP پاسخ می‌دهد، پیام RREP به گره همسایه ارسال خواهد شد که از آن گره مقصد پیام RREQ دریافت می‌کند و سپس تابع وزن (*WF* [۴۲]) آن گره مطابق با رابطه (۱) به‌عنوان تابع وزن کل (*TWF* [۴۳]) تعیین خواهد شد.

$$WF_{(i,j)} = \frac{E_i}{D_{(i,j)}+ED_{(i,des)}} \quad (۱)$$

در رابطه (۱)، $WF_{(i,j)}$ وزن لینک بین گره‌های i و j می‌باشد، E_i انرژی گره iام است، $D_{(i,j)}$ فاصله بین گره i و گره j بوده و $ED_{(i,des)}$ فاصله اقلیدسی بین گره i و گره مقصد (des) می‌باشد که طبق رابطه (۲) محاسبه خواهد شد.

$$ED_{(i,des)} = \sqrt{(x_i - x_{des})^2 + (y_i - y_{des})^2} \quad (۲)$$

در رابطه (۲)، x و y مختصات گره‌های i و گره مقصد را مشخص می‌کنند. در هر گام از مسیر، گره پیام RREP را به گره همسایه بعدی ارسال خواهد کرد که پیام RREQ را با توجه به سوابق ذخیره‌شده در جدول مسیریابی آن دریافت کرده است. این بار هم هنگامی‌که پیام RREP به گره قبل می‌رسد، تابع وزن محاسبه‌شده و به تابع وزن کل مسیر افزوده خواهد شد و تابع وزن جدید به‌عنوان مجموع توابع وزن دو گره مسیر تعیین خواهد شد. سپس گره مجدداً پیام RREP را به گره قبل ارسال می‌کند و این فرآیند به این روش ادامه می‌یابد؛ بنابراین هنگامی‌که پیام RREP به گره مبدأ می‌رسد، مسیر انتقال می‌تواند ایجاد شود و این مسیر به عنوان یک مسیر معتبر علامت‌گذاری خواهد شد.

در این روش، پیام‌های RREQ را می‌توان از طریق مسیرهای مختلف به گره مقصد ارسال کرد و برای هر مسیر، پیام RREP را می‌توان از گره مقصد به گره مبدا ارسال کرد. برای هر مسیر زمانی که پیام RREP به گره مبدا ارسال می‌شود، *WF* از هر گره آن مسیر تا زمانی که به مبدا برسد اضافه خواهد شد. در یک‌زمان از پیش تنظیم‌شده مشخص می‌شود که اگر تعداد X مسیرهای انتقال برقرار باشد، آن مسیرها به‌عنوان مسیرهای معتبر شبکه برای ارسال اطلاعات از گره مبدا به گره مقصد ذخیره می‌شوند. زمانیکه تنها راه اول ایجاد می‌شود، *TWF* آن به عنوان بالاترین تابع وزن (*HWF*) تعیین خواهد شد؛ اما وقتی مسیر دیگری ایجاد شود، *TWF* آن با ارزش *HWF* مقایسه خواهد شد. اگر *TWF* مسیر دوم بالاتر از مقدار *HWF* باشد، پس این مسیر به‌صورت رتبه ۱ ذخیره خواهد شد و *HWF* و مسیر اول در رتبه ۲ ذخیره خواهد شد. در غیر این صورت مسیر اول در رتبه ۱ باقی خواهد ماند و مسیر تازه خلق‌شده به رتبه ۲ خواهد رسید.

اگر به هر دلیلی در طول انتقال داده، یک گره قادر به ارتباط با گره همسایه خود نباشد، آنگاه آن گره یک پیغام خطا (RERR [۴۴]) را به گره مبدا می‌فرستد و تمام اطلاعات مربوط به آن مسیر انتقال را از جدول مسیریابی حذف می‌کند.

به‌طور مشابه، در طول انتقال داده، می‌توان فهمید که گره‌های خودخواهی وجود دارند که در شبکه حضور دارند. گره‌های خودخواه از نوع «عدم ارسال داده‌ها»، ممکن است از ارسال بسته‌ها به جلو برای سایر گره‌ها در طول انتقال داده جلوگیری کنند؛ بنابراین، این نوع گره‌های خودخواه باید با استفاده از الگوریتم تشخیص رفتار خودخواهانه شناسایی شوند. بعد از اینکه مشخص شد که یک گره در طبیعت خودخواه است، پس تمام مسیرهای انتقال معتبر کنترل می‌شوند و اگر گره خودخواه در هر مسیر انتقال معتبر پیدا شود، مسیر انتقال از پایگاه داده برداشته خواهد شد و مسیرهای انتقال باقی‌مانده با توجه به *TWF* دوباره رتبه‌بندی خواهد شد و در صورت نیاز *HWF* تغییر داده خواهد شد.

۵-۲- مرحله تشخیص

در این مرحله تشخیص رفتار خودخواهانه گره‌ها انجام می‌شود. در شبکه‌های سیار موردی، گره اغلب بسته‌ها را در زمانی که رفتار خودخواهانه دارد ارسال نمی‌کند، در نتیجه تعداد بسته‌های ارسالی با رفتار خودخواهانه به مراتب کم‌تر از حالت نرمال است. برای تشخیص رفتار خودخواهانه، تعداد بسته‌ها بین زمان فعلی و رفتار نرمال باید مقایسه شود. برای این کار، در روش پیشنهادی از الگوریتم بررسی بسته‌های داده دریافت شده و ارسال‌شده توسط گره‌ها و یک الگوریتم آستانه تطبیقی [۵۰] استفاده می‌شود. الگوریتم آستانه تطبیقی اغلب برای تشخیص تغییرات غیر نرمال یا مقایسه یک مقدار فعلی با مقادیر قبلی بکار می‌رود.

۵-۲-۱- الگوریتم تشخیص گره خودخواه بر اساس عدم ارسال بسته‌های داده

مطابق توضیحات ارائه شده در بخش ۵-۱، در پروتکل مسیریابی AODV، ابتدا هر گره پیام سلام را به تمامی گره‌های همسایه خود ارسال می‌کند. بسته اطلاعاتی همراه با داده‌ها، حاوی موارد زیر است:

- آدرس گره مبدا
- آدرس گره مقصد
- تعداد بسته‌های ارسالی
- دوره‌های زمانی: مدت‌زمانی است که ارسال و دریافت بسته‌های داده مورد بررسی قرار می‌گیرد. این مورد در هر یک از گره‌ها مشخص می‌گردد.
- گره گیرنده، یعنی گره مسیر انتقال که در آن بسته داده باید توسط گره فعلی فرستنده، فرستاده شود.

این الگوریتم تشخیص را می‌توان با یک مثال توضیح داد. فرض شود مسیر انتقال داده A - B - C - D - E است که در آن گره مبدا A و گره مقصد E است. تعداد بسته‌های انتقالی در بسته داده ذخیره می‌شود. در ابتدا گره فرستنده به صورت A و گره گیرنده بعدی B تنظیم شده است که در اینجا فرستنده تعداد بسته‌های داده‌ای که قصد ارسال آن‌ها را دارد در سرآیند بسته‌ها مشخص می‌نماید. هنگامی‌که بسته‌های داده به B می‌رسد؛ در انتهای دوره زمانی، گره گیرنده B تعداد بسته‌های دریافتی را با تعداد بسته‌های ارسالی مشخص شده در فرستنده مقایسه می‌نماید. در صورتی که تعداد بسته‌های دریافتی کمتر از تعداد بسته‌های ایجاد شده در فرستنده باشد سه احتمال وجود خواهد داشت.

- احتمال اول این است که گره فرستنده به دلایل مختلفی از جمله اتمام انرژی و یا خرابی، خاموش شده است و یا از محدوده پوششی گره گیرنده خارج شده است؛ در نتیجه قادر به ارسال تمامی بسته‌ها نبوده است. در این صورت هیچگونه عمل خودخواهانه‌ای توسط گره فرستنده انجام نگرفته است. در این مورد با ارسال مجدد پیام‌های سلام در دروه زمانی، مشخص می‌گردد که گره فرستنده در همسایگی گره گیرنده قرار ندارد و از لیست همسایگان گره گیرنده حذف خواهد شد و به عنوان گره خودخواه معرفی نخواهد شد.
- احتمال دوم این است که گره فرستنده تمامی بسته‌ها را ارسال نموده و در مسیر ارسال به گیرنده، بسته‌های داده از بین رفته‌اند. در این صورت گره گیرنده B قادر به دریافت بسته‌ها نبوده و گره فرستنده را به عنوان گره خودخواه به ایستگاه پایه معرفی می‌نماید. سپس الگوریتم آستانه تطبیقی برای اطمینان از خودخواه بودن گره اجرا خواهد شد. در صورتیکه بسته‌های داده در مسیر انتقال دچار مشکل شده باشند؛ در دوره‌های زمانی بعدی با رفع مشکل انتقال با انجام مسیریابی و یا قرار گیری گره در نقطه مناسب‌تر، گره در الگوریتم آستانه تطبیقی به عنوان گره نرمال در نظر گرفته خواهد شد و انتقال بسته‌های داده ادامه خواهد یافت.
- احتمال سوم این است که گره فرستنده رفتار خودهانه انجام داده و یک گره خودخواه باشد و گره فرستنده تمامی بسته‌های ایجادشده توسط گره مبدا را ارسال نکرده است. در اینصورت گره خودخواه یا فرستنده به عنوان گره خودخواه بالقوه به ایستگاه پایه معرفی شده و الگوریتم آستانه تطبیقی برای گره خودخواه اجرا خواهد شد. در الگوریتم آستانه تطبیقی، اگر رفتار خودخواهانه گره در چند دوره زمانی تکرار شود؛ گره به عنوان گره خودخواه قطعی انتخاب خواهد شد و رفتار خودخواهانه آن تشخیص داده می‌شود. الگوریتم آستانه تطبیقی در بخش ۵-۲-۲ توضیح داده شده است.

این روال برای تمام گره‌های میانی تکرار شده و نسبت دریافت بسته‌های داده در این گره‌ها بررسی می‌گردد. بنابراین، در این بخش گره‌هایی که بسته‌های داده را ارسال نمی‌کنند به عنوان گره خودخواه بالقوه علامت‌گذاری خواهند شد.

اگر هیچ گره خودخواهی وجود نداشته باشد، در نهایت گره D با موفقیت بسته داده‌ها را به گره E ارسال می‌کند. زمانیکه بسته‌های داده به مقصد برسند آدرس مقصد مشخص شده در سرآیند بسته‌ها با آدرس گره مقصد مطابقت داده شده و در صورت یکسان بودن، انتقال موفقیت‌آمیز بسته داده به پایان می‌رسد.

۵-۲-۲- الگوریتم آستانه تطبیقی اصلاح‌شده

از الگوریتم آستانه تطبیقی برای تشخیص رفتار خودخواهانه در فرستنده استفاده شده است. روش مورد استفاده در این فاز شامل سه مرحله است. ابتدا، مقدار آستانه مطابق با مقادیر مشاهدات قبلی تعیین می‌شود. سپس نسبت ارسال بسته (PFR[۴۵]) محاسبه می‌شود. این مقدار نشان‌دهنده نسبت تعداد بسته‌های ارسالی به تعداد بسته‌های دریافت شده در بازه زمانی حاضر است. در نهایت، مقدار PFR فعلی با مقدار آستانه برای تعیین رفتار خودخواهانه گره فعلی استفاده می‌شود. اگر PFR کم‌تر از مقدار آستانه باشد، گره خودخواه تشخیص داده می‌شود. در غیر این صورت، مقدار آستانه با توجه به PFR فعلی و مقدار آستانه جدید برای بازه زمانی بعدی به‌روز می‌شود.

اگر فرض شود که x_n تعداد بسته‌های داده دریافتی خودخواه بالقوه در بازه زمانی nام را نشان می‌دهد و μ_n نرخ تخمین زده شده از اندازه‌گیری‌های قبلی است؛ به عبارت دیگر x_n نشان‌دهنده بسته‌های دریافتی گره بوده و μ_n تعداد بسته‌های داده‌ای را نشان می‌دهد که با توجه به شرایط شبکه انتظار دریافت این تعداد بسته وجود دارد و دریافت این تعداد بسته نشان‌دهنده حالت نرمال است. بنابراین وضعیت هشدار برای گره خودخواه مطابق رابطه (۳) بیان خواهد شد:

$$if\ x_n \geq (1-\alpha)\bar{\mu}_{n-1} \quad (۳)$$

سپس یک هشدار در فاصله زمانی n به وجود می‌آید که در آن $\alpha>0$ پارامتری است که نشانه رفتار غیر نرمال گره است و نشان‌دهنده درصد بالای مقدار میانگین بسته‌های دریافتی در حالت نرمال است. می‌توان μ_n را با استفاده از دو فاکتور محاسبه کرد. یکی تعداد بسته‌های دریافتی در بازه‌های زمانی و دیگری استفاده از میانگین متحرک وزنی نمایی (EWMA[۴۶]) اندازه‌گیری‌های قبلی که در رابطه (۴) تعریف شده است.

$$\bar{\mu}_n = \beta\bar{\mu}_{n-1} + (1-\beta)x_n \quad (۴)$$

که در آن β $(0 \leq \beta \leq 1)$ فاکتور EWMA است. μ_n از حاصل جمع تعداد بسته‌های داده دریافتی با میزان بسته‌های داده دریافتی مورد انتظار در دوره‌های زمانی قبلی به دست می‌آید.

پارامتر μ نرخی را تعیین می‌کند که در آن داده‌های قدیمی به محاسبه آمار EWMA وارد می‌شوند. مقدار μ=1 نشان می‌دهد که تنها جدیدترین اندازه‌گیری بر EWMA اثر می‌گذارد. بنابراین، مقدار بزرگ β (نزدیک به ۱) وزن بیشتری را به داده‌های اخیر و وزن کمتری به داده‌های قدیمی‌تر می‌دهد. به عبارت دیگر هر چه مقدار β نزدیک به یک باشد، تاثیر بیشتری در فاکتور $\bar{\mu}_{n-1}$ که نشان‌دهنده

بسته‌های دریافتی مورد انتظار در دوره‌های زمانی گذشته است می‌گذارد. مقدار کوچک β (نزدیک به ۰) وزن بیشتری را به داده‌های قدیمی‌تر می‌دهد؛ چون مقدار $1-\beta$ ارزش بالاتری خواهد داشت و تاثیر x_n بالاتر خواهد بود. مقدار β معمولاً بین ۰.۲ تا ۰.۳ تنظیم می‌شود.

اگر به‌طور مستقیم از الگوریتم آستانه تطبیقی برای تشخیص رفتار خودخواهانه استفاده شود، ممکن است منجر به نسبت بالای هشدارهای غلط شود. بنابراین در این بخش یک الگوریتم آستانه تطبیقی اصلاح‌شده پیشنهاد شده است که در آن یک مقدار k (k=1,2,3,...) تعیین می‌شود. سپس، اگر تعداد موارد نقض پیاپی آشکار آستانه بیشتر از k باشد، آژیر هشدار افزایش می‌یابد. در الگوریتم آستانه تطبیقی اصلاح‌شده وضعیت هشدار به صورت رابطه (۵) تغییر کرده است.

$$\sum_{i=n-k+1}^{n} 1_{\{x_i \geq (1-\alpha)\bar{\mu}_{i-1}\}} \geq k \qquad (۵)$$

که در آن k>1 است و نشان‌دهنده تعداد بازه‌های زمانی متوالی است که آستانه مورد تجاوز قرار می‌گیرد. اگر رفتار خودخواهانه رخ دهد، آنگاه زنگ هشدار در فاصله زمانی n به صدا درمی‌آید.

رابطه (۵) رفتار غیر نرمال را در دوره‌های زمانی شبکه نشان می‌دهد. رفتار غیر نرمال این رابطه در اثر دریافت بسته‌های داده بیشتر از میزان تخمین زده شده اتفاق می‌افتد. به عبارت دیگر در صورتی که بسته‌های دریافت شده توسط گره بیشتر از حد انتظار تخمین زده شده باشد، این رابطه عمل خواهد کرد. به بیان دیگر این رابطه نشان‌دهنده حالت غیر نرمال مثبت در شبکه است. با توجه به اینکه این نوع رفتار نشان‌دهنده رفتار خودخواهانه نیست؛ بنابراین از این رابطه برای شناسایی گره‌های خودخواه استفاده نخواهد شد و صرفاً برای نشان دادن رفتارهای غیر نرمال مثبت می‌باشد.

گره‌هایی که رفتار خودخواهانه در شبکه از خود نشان می‌دهند مایل به ارسال بسته‌های داده نیستند و ممکن است بسته‌هایی که هیچ ارتباطی با این گره‌ها ندارند را حذف کنند؛ بنابراین می‌توان از الگوریتم آستانه تطبیقی اصلاح‌شده برای تشخیص رفتار خودخواهانه به وسیله محاسبه PFR در هر گره از شبکه استفاده کرد.

برای تشخیص رفتار خودخواهانه، به آمار x_n و y_n نیاز است که در آن x_n تعداد بسته‌هایی که وارد یک گره می‌شوند را نشان می‌دهد و y_n نشان‌دهنده تعداد بسته‌های ارسال‌شده توسط گره در فاصله زمانی n است. پارامتر z_n، نسبت y_n و x_n در بازه زمانی n را نشان می‌دهد، یعنی z_n، PFR است. در حالت ایده‌آل، فرض می‌شود که PFR را می‌توان به‌دقت در شبکه سیار موردی شمرد. در نتیجه قضیه ۱ قابل بیان است.

قضیه ۱: یک گره که رفتار خودخواهانه از خود نشان می‌دهد را با احتمال بالا می‌توان با محاسبه n امین نسبت z_n و تخمین مقدار $\bar{\mu}_n$ با الگوریتم آستانه تطبیقی تشخیص داد، با این فرض که PFR را می‌توان به دقت شمارش کرد.

اثبات در شرایط نرمال:

z_n یا PFR روی گره‌های نرمال در یک محدوده کوچک تغییر می‌کند. اگر یک گره رفتاری خودخواهانه داشته باشد، PFR آن باید بسیار متفاوت از حالت نرمال باشد، بنابراین می‌توان از یک پارامتر آستانه α (α€[0,1]) برای نظارت بر این‌که PFR گره‌ها در محدوده نرمال است، استفاده کرد. رفتار خودخواهانه وقتی می‌تواند تشخیص داده شود که PFR در محدوده تخمینی قرار دارد. بنابراین، شرط مقدار آستانه $z_n<\alpha\times\bar{\mu}_{n-1}$ است که در آن $\bar{\mu}_{n-1}$ میزان تخمین زده‌شده از اندازه‌گیری‌های قبل از n است. اگر $z_n>\alpha\times\bar{\mu}_{n-1}$ در بازه زمانی nام وضعیت نرمال گره را نشان دهد، می‌توان $\bar{\mu}_{n-1}$ را با استفاده از رابطه (۳) محاسبه کرد. بالعکس، زمانی که PFR یک گره کم‌تر از مقدار آستانه در بازه زمانی nام است، این مقدار تغییر نمی‌کند. یعنی $\bar{\mu}_n=\bar{\mu}_{n-1}$. مطابق با توضیحات ارائه شده، معادله وضعیت هشدار به صورت رابطه (۶) تغییر می‌کند.

$$\sum_{i=n-k+1}^{n} 1_{\{x_i<\alpha\bar{\mu}_{i-1}\}} \geq k \qquad (۶)$$

در این حالت اگر مقدار رابطه (۶) بیشتر از k باشد، آنگاه هشدار در بازه زمانی nام رخ می‌دهد. مقدار k بر اساس شرایط شبکه و ارتباطات، از جمله میزان تحرک گره‌ها، همپوشانی گره‌ها و تعداد گره‌ها می‌تواند متفاوت باشد. این مقدار بر اساس توابع هزینه محاسبه شده و با توجه به شرایط شبکه تعیین می‌گردد. به‌عبارت‌دیگر، می‌توان رفتار خودخواهانه را به احتمال زیاد از طریق الگوریتم آستانه تطبیقی اصلاح‌شده شناسایی کرد.

۵-۳- مرحله جلوگیری

اکثر مکانیسم‌های پیشنهادشده برای جلوگیری از رفتار خودخواهانه (بخش ۴) گره‌های خودخواه را جداسازی می‌کنند تا تضمین شود که شبکه سیار موردی به حالت نرمال بر می‌گردد. با این‌حال، چنین اقداماتی منجر به تصاحب منابع موجود توسط آن گره‌ها می‌شود که برای استفاده در شبکه‌های سیار موردی در دسترس نیستند. چون منابع در شبکه‌های سیار موردی حیاتی هستند؛ بنابراین، اینکار یک اتلاف بزرگ برای شبکه است تا یک گره که رفتارهای خودخواهانه از خود نشان می‌دهد را جدا کند. در نتیجه مهم است که از رفتار خودخواهانه جلوگیری شود و تمام گره‌ها برای مشارکت در ارسال بسته‌های داده در شبکه تحریک شوند. با توجه به اینکه بازی‌های تکراری همیشه برای ایجاد یک تعادل استفاده می‌شوند که می‌تواند برای هر دو طرف در یک بازی رضایت‌بخش باشد؛ بنابراین در این فاز، می‌توان از بازی‌های تکراری برای تنبیه گره‌هایی که رفتار خودخواهانه نشان می‌دهند استفاده کرد.

در ادامه جزئیات چگونگی استفاده از بازی‌های تکراری برای جلوگیری از رفتارهای خودخواهانه در شبکه‌های سیار موردی بیان شده است.

۵-۳-۱- بازی‌های تکراری

بازی‌های تکراری [۵۱] به سناریویی اشاره می‌کنند که در آن یک ساختار در یک بازی در بازه‌های زمانی مختلف تکرار می‌شود. هر بازی یک «مرحله بازی» نامیده می‌شود. بازی تکراری را می‌توان به صورت زیر تعریف کرد. اول، بازیکنان باید حالت‌های راهبردی و نحوه پرداخت را مشخص کنند. سپس تمام بازیکنان اقدامات تحقق‌یافته را در پایان هر دوره زمانی مجزا از هر مرحله اجرای بازی مشاهده می‌کنند. بازی‌های تکراری سه راهبرد مشترک دارند: راهبرد تحریک (راه‌اندازی)، راهبرد تنبیه محدود و راهبرد تلافی‌جویانه. در راهبرد راه‌اندازی، فرض کنید که دو بازیکن، راستی (درستی) را در مرحله t (t=2,3,...) انتخاب می‌کنند و یکی از آن‌ها راهبرد تقلب را در مرحله t (t=2,3,...) انتخاب می‌کند. سپس سایر بازیکنان می‌توانند راهبرد تقلب را فوراً انتخاب کنند. راهبرد مجازات محدود، مجازات در انتهای فاصله زمانی k (k=0,1,2,...) اتفاق می‌افتد، اما مجازات در این راهبرد، پایدار و همیشگی نیست (موقت است). در یک راهبرد تلافی‌جویانه، اگر یک بازیکن انتخاب کند که در یک فاصله زمانی تقلب کند، بازیکن دیگر می‌تواند بلافاصله در فواصل زمانی بعدی تقلب کند تا حریف خود را تنبیه نماید.

زمانی که بازی تنها در یک فاصله زمانی رخ می‌دهد، هر شرکت‌کننده تنها به پول قابل‌عرضه خود اهمیت می‌دهد. اگر این بازی بارها تکرار شود، شرکت‌کنندگان ممکن است قربانی کردن سود قابل‌عرضه برای منافع بلندمدت را در نظر بگیرند و سپس یک راهبرد متفاوت را انتخاب کنند؛ بنابراین، تعداد مراحل بازی‌ها بر نتیجه تعادل بازی تأثیر خواهد گذاشت. در بازی‌های تکراری، یک عامل تخفیف معرفی

می‌شود که به توضیح بازی‌های تکراری به عنوان بازی‌های تکراری محدودشده کمک می‌کند؛ با این‌حال، زمان‌بندی‌ها قبل از به پایان رسیدن بازی تصادفی هستند.

تعریف ۱: متوسط ضرر واردشده

اگر δ فاکتور تخفیف باشد، این فاکتور نشان‌دهنده میزان تخفیف درآمدی است که در هر دوره زمانی برای درآمد هر یک از بازیکنان در نظر گرفته خواهد شد. به عبارت دیگر فاکتور تخفیف δ میزان درآمدی است که در صورت کاهش، آن گره به رفتار خود ادامه خواهد داد. سپس مقدار متوسط درآمد جریان واردشده (R_1، R_2، R_3 ...) را می‌توان به صورت رابطه (۷) محاسبه کرد.

$$R = (1-\delta)\sum_{t=1}^{infinit} \delta^{t-1} R_t \qquad (۷)$$

جایی که R_t (t=1,2,...)، نشان‌دهنده درآمد هر مرحله از بازی است و δ^{t-1} R_t (t = 1,2,...) مقدار ضرر هر مرحله از بازی است.

از آنجا که میانگین تخفیف درآمد R، 1-δ برابر بیشتر از مجموع تمام مقادیر تخفیف است، حداکثر کردن R برابر حداکثر کردن مجموع کلیه مقادیر تخفیف است. به عبارت دیگر برای اینکه مقدار R به ماکزیمم مقدار خود که برابر V_i یا درآمد مورد انتظار است برسد باید مجموع مقادیر δ^{t-1} را بتوان ماکزیمم کرد. در نتیجه با ماکزیمم کردن δ می‌توان میزان درآمد را نیز افزایش داده و به ماکزیمم مقدار رساند. بنابراین، می‌توان با مقایسه R در مراحل مختلف بازی تصمیم گرفت که کدام راهبرد انتخاب شود.

تعریف ۲: نوع بازی

نوع بازی راهبرد $G = \{N,S,u\}$ است، جایی که $N= \{1,2,... n\}$، مجموعه شرکت‌کنندگان را نشان می‌دهد، $S= \{S_1,S_2,...,S_n\}$، مجموعه‌ای از راهبردها و $u= \{u_1,u_2,... u_n\}$، مجموع درآمد شرکت‌کنندگان در هر مرحله از بازی است. اگر G، T (T = 1,2,...) بار تکرار شود، $G(T)$، بازی‌های تکرارشده در فاصله‌های زمانی T را نشان می‌دهد. v_i نشان‌دهنده درآمد مورد انتظار شرکت‌کننده i در بازی‌های تکراری G (T) می‌باشد و می‌توان از طریق رابطه (۸) آن را به دست آورد.

$$v_i = u_i(s^1) + \delta u_i(s^2) + \cdots + \delta^{T-1} u_i(s^T) = \frac{R_i}{1-\delta} \qquad (۸)$$

جایی که $u(s^T)$ تابع بازگشتی بازنویسی برنولی است، s^t $(1 \le t \le T)$ ترکیبی از اقدامات در مرحله t را در بازی‌های تکراری نشان می‌دهد، δ عامل تخفیف است و R_i مقدار میانگین درآمد شرکت‌کننده i است. درآمد هر راهبرد می‌تواند توسط رابطه (۹) بدست آید.

$$R_i = (1-\delta)\sum_{t=1}^{T} \delta^{t-1} u_i(s^t) \qquad (۹)$$

در این مقاله، بازی خودخواهانه به صورت چهار قاعده تنظیم می‌شود:

$G = \{N,SSN,SOS,u\}$، جایی که N = {Nodes,OS}، تمام شرکت‌کنندگان در بازی شامل تمام گره‌ها (Nodes) و سیستم‌عامل شبکه (OS) که در یک ایستگاه پایه در شبکه قرار دارد، می‌باشد. SSN و SOS دو شرکت‌کننده در بازی‌های تکراری را نشان می‌دهند. بازی از دو شرکت کننده تشکیل شده است که نام‌های آن‌ها را به صورت SSN یا شرکت‌کننده با راهبرد Selfish, Normal و شرکت‌کننده SOS یا شرکت‌کننده با راهبرد سیستم‌عامل نامگذاری شده است.

{Normal,Selfish} = SSN و {Trust,Isolate} = SOS، به ترتیب به‌صورت $\{N,S\}$ و $\{T,I\}$ تعریف می‌شود. بازی‌های تکراری ماتریس u را پرداخت می‌کنند که اولویت راهبرد انتخاب را نشان می‌دهد.

بر اساس اولویت شرکت‌کنندگان، هر دو سود را می‌توان تعیین کرد. $a< b$ به صورت b سود بیشتری از a به‌دست‌آورده، تعریف شده است. بر اساس هر چهار ترکیب راهبرد در بازی‌های تکراری، درآمد هر دو طرف شرکت‌کنندگان مورد بررسی قرار خواهد گرفت. در طرح پیشنهادی، هنگامی‌که رفتار خودخواهانه به موفقیت برسد، گره‌ها دارای بیشترین درآمد هستند و هیچ جداسازی وجود ندارد. زمانی که یک گره نرمال است و برنامه به آن اعتماد دارد، این یک انتخاب بهینه در کار است. از سوی دیگر، زمانی که یک گره رفتار خودخواهانه نشان دهد، بلافاصله جدا می‌شود که درآمد در این حالت پایین‌ترین است. از توضیحات ارائه شده، مجموعه اولویت گره‌ها به‌صورت زیر حاصل می‌شود:

$$SI < NI < NT < ST$$

هنگامی‌که گره نرمال است و طرح پیشنهادی به گره اعتماد دارد، درآمد به حداکثر می‌رسد. سناریوی بعدی جدا کردن گره در زمانی است که رفتار خودخواهانه را نشان می‌دهد. بدترین حالت زمانی رخ می‌دهد که یک گره در وضعیت خودخواهانه قرار دارد و برنامه آن را کشف نمی‌کند؛ بنابراین، در این حالت مجموعه اولویت طرح پیشنهادی به صورت زیر است:

$$TS < IN < IS < TN$$

نحوه درآمد راهبرد خالص برای هر دو طرف در بازی مطابق جدول ۳ درنظر گرفته شده است که در رابطه با گره‌ها $e>a>c>g$ و در مورد طرح $b>h>d>f$ است. این مقادیر همان مقادیر راهبردهای انتخابی بالا هستند که برای ساده‌سازی از آن‌ها استفاده شده است.

جدول ۳- نحوه درآمد راهبردها

راهبرد	Trust	Isolate
نرمال	(a,b)	(c,d)
خودخواه	(e,f)	(g,h)

۵-۳-۲- جلوگیری از رفتار خودخواهانه

هنگامیکه گره‌هایی که رفتار خودخواهانه از خود نشان می‌دهند در مرحله تشخیص شناسایی شوند، در این مرحله مجازات خواهند شد. طبیعتاً وقتی یک گره مجازات می‌شود، باید درآمدش را چک کند. اگر درآمد کم‌تر از حد نرمال است، ممکن است در فاصله زمانی بعدی نرمال شود. البته، بعضی از گره‌ها ممکن است گاهی یک راهبرد خودخواهانه را انتخاب کنند، اما بعد از یک بازه زمانی خاص، آن‌ها راهبرد نرمال را انتخاب کنند.

بنابراین در مرحله جلوگیری از رفتار خودخواهانه، می‌توان با وادار کردن گره‌ها برای انتخاب راهبرد نرمال در شبکه، از رفتار خودخواهانه آنها جلوگیری کرد. برای انجام این کار، الگوریتمی بر اساس بازی‌های تکراری پیشنهاد شده است که از راهبرد مجازات محدودشده استفاده می‌کند. برای اینکار ابتدا با مقایسه PFR و مقدار آستانه مشخص می‌شود که کدام گره‌ها رفتار خودخواهانه از خود نشان می‌دهند. سپس با فرض اینکه رفتار خودخواهانه می‌تواند با استفاده از الگوریتم آستانه تطبیقی اصلاح‌شده شناسایی شود، قضیه ۲ قابل بیان است.

قضیه ۲: در زمینه بازی، اگر ضریب تخفیف $\delta > max\left(\frac{e-a}{e-c}, \frac{d}{b}\right)$ باشد، همیشه می‌توان دو مقدار مناسب از (k,δ) را برای منصرف کردن گره‌ها از انتخاب راهبرد خودخواهانه بر اساس راهبرد مجازات محدود، تعیین کرد.

اثبات: در وضعیت بازی، هر دو طرف در زمان انتخاب راهبردهای متفاوت، درآمد متفاوتی دارند. باید اجازه داده شود تا زمانیکه گره‌ها راهبرد نرمال را انتخاب می‌کنند و طرح راهبرد اعتماد[۴۷] را انتخاب می‌کند هر دو بازیکن در این بازی حداکثر درآمد را به دست آورند؛ بنابراین، طبق جدول ۳، می‌توان درآمدها را در مراحل مختلف محاسبه کرد. درآمدها به صورت R_{N1}، R_{N2} و R_{N3} تنظیم شده است که در آن R_{N1} نشان‌دهنده درآمد گره در زمانی است که راهبرد نرمال را انتخاب می‌کند و طرح راهبرد اعتماد را در مراحل زمانی k انتخاب می‌کند.

R_{N2} و R_{N3} نشان‌دهنده درآمد گره‌ها هستند که راهبرد خودخواهانه و طرح راهبرد اعتماد را در مرحله اول انتخاب می‌کنند. سپس گره‌ها یک راهبرد نرمال و

خودخواهانه را انتخاب می‌کنند، اما طرح پیشنهادی به ترتیب راهبرد مجزا را در بازه‌های زمانی k (k=1,2,...) انتخاب می‌کند.

R_{N1} نشان‌دهنده این است که در تمامی دوره‌های زمانی گره رفتار نرمال از خودش نشان داده است، در نتیجه سیستم عامل نیز به آن اعتماد داشته است. بنابراین میزان درآمد برابر a است که در تمامی دوره‌های زمانی کسب شده است. R_{N2} رفتار گره در زمانی را نشان می‌دهد که راهبرد گره خودخواهانه بوده و راهبرد سیستم عامل اعتماد می‌باشد. سپس در دوره‌های زمانی بعدی سیستم عامل راهبرد جداسازی[۴۸] را انتخاب نموده است تا گره رفتار خود را اصلاح نماید. R_{N3} بعد از اینکه گره رفتار خودخواهانه انجام داده است رفتار خود را به حالت نرمال تغییر داده است. این در حالی است که توسط سیستم عامل مجازات شده و راهبرد سیستم عامل حالت جداسازی می‌باشد. مطابق با روابط (۸) و (۹) و جدول ۳، درآمدها به‌صورت روابط (۱۰) الی (۱۲) قابل محاسبه است.

$$R_{N1} = a + a\delta + a\delta^2 + a\delta^2 + \cdots + a\delta^k + \cdots \quad (۱۰)$$

$$R_{N2} = e + g\delta + g\delta^2 + ag + \cdots + g\delta^k + \cdots \quad (۱۱)$$

$$R_{N3} = e + c\delta + c\delta^2 + c\delta^2 + \cdots + c\delta^k + \cdots \quad (۱۲)$$

که در آن δ فاکتور تخفیف را نشان می‌دهد. برای جلوگیری از رفتار خودخواهانه گره‌ها نیاز است تا یک راهبرد نرمال در این بازی‌ها انتخاب شود. به‌عبارت‌دیگر، به بیشینه کردن درآمد گره‌ها نیاز است. از این‌رو، به نتایج δ در زمانی نیاز است که $R_{N1} > R_{N2}$ و $R_{N1} > R_{N3}$ باشد. سپس، نتیجه مقدار فاکتور تخفیف از $\delta > \left(\frac{e-a}{e-c}\right)$ محاسبه می‌شود. با استفاده از روش مشابه برای محاسبه درآمد طرح پیشنهادی، می‌توان مقدار فاکتور تخفیف دیگر را به‌صورت $\delta > \frac{d}{b}$ به دست آورد. در نتیجه، ماکزیمم فاکتور تخفیف مطابق رابطه (۱۳) خواهد بود.

$$\delta > max\left(\frac{e-a}{e-c}, \frac{d}{b}\right) \quad (۱۳)$$

این مقدار می‌تواند شرایط حداکثرسازی برای هر دو درآمد را در بازی‌های تکراری برآورده کند؛ بنابراین، می‌توان یک مقدار ضریب تخفیف پیدا کرد که به گره‌ها اجازه می‌دهد تا راهبرد نرمال را انتخاب کنند. در محیط واقعی، گره‌ها ممکن است گاهی یک راهبرد خودخواهانه را برای فرار از تشخیص انتخاب کنند، اما وقتی طرح پیشنهادی رفتار خودخواهانه را تشخیص می‌دهد، می‌تواند راهبرد مجازات را در مراحل بعدی k (k =1,2,...) آغاز کند. از قضیه ۲، مشخص است که درآمد گره‌ها در زمانی که گره‌ها راهبرد خودخواهانه را انتخاب می‌کنند، پایین‌ترین است. بنابراین، گره‌ها تمایل دارند بعد از تعداد متناهی از فواصل زمانی، راهبرد نرمال را انتخاب کنند.

۶- شبیه‌سازی

مفروضات و محدودیت‌های مدنظر در شبیه‌سازی به شرح ذیل هستند:

- به‌صورت پیش‌فرض تمامی گره‌ها همکار و قابل‌اعتماد هستند.
- گره‌های خودخواه در فرآیند مسیریابی شرکت می‌کنند.
- مسیر از مبدأ به مقصد پیدا شده و مسیریابی به‌درستی انجام شده است.
- گره‌های شرکت‌کننده دارای رفتار منطقی هستند (دارای رفتار سوء و آسیب‌رسان به شبکه نیستند).
- در شروع، هر گره با یک احتمال پیش‌فرض اقدام به ذخیره سازی داده می‌کند.
- در همسایگی هر گره حداقل یک گره وجود دارد.
- حداقل یک بسته انتقال می‌یابد.

بسته اطلاعاتی همراه با داده‌ها، حاوی اطلاعات ارائه شده در بخش ۵-۲-۱ است.

۶-۱- سناریوی شبیه‌سازی

هم‌بندی شبکه با استفاده از محیط واقعی شهری به کمک Openstreetmap و نرم‌افزار شبیه‌سازی ترافیک شهری SUMO [۵۲] ایجاد شده و برای شبیه‌سازی و ارزیابی عملکرد از شبیه‌ساز NS-3.29 [۵۳] استفاده شده است. در شبیه‌سازی پروتکل مسیریابی AODV [۵۴] مورد استفاده قرارگرفته است. نتایج شبیه‌سازی روش پیشنهادی با نام DMS با روش‌های WSISB [۳۵]، RDG [۴۶]، LTCF [۴۷]، HGT [۴۸] و CRG [۴۹] مقایسه شده است. پارامترهای شبیه‌سازی در جدول ۴ نشان داده شده‌اند. در شبیه‌سازی فرض می‌شود که یک گره قبل از مرحله t (t=2,3, ...) یک راهبرد نرمال را انتخاب کرده است. از آنجا که طرح پیشنهادی راهبرد خود را مطابق با آخرین راهبرد انتخابی گره، انتخاب کرده است، بنابراین می‌تواند راهبرد اعتماد را در مرحله اول انتخاب کند. اگر گره راهبرد خودخواهانه را در مرحله tام انتخاب کند، طرح در فاز جلوگیری، از یک راهبرد مجازات محدود در مرحله t+1 برای مجازات آن استفاده می‌کند.

جدول ۴- پارامترهای شبیه‌سازی

پارامترها	مقدار
محدوده شبیه‌سازی	۲۰۰۰m×۳۰۰۰m
تعداد گره‌ها	۲۰
پروتکل Mac	IEEE 802.11
نوع ترافیک	CBR[۴۹]
اندازه بسته	۵۱۲ بایت
محدوده ارتباطی	۲۵۰m
نرخ انتقال	۰.۱ Mbps
مدت‌زمان شبیه‌سازی	۳۰۰s
نوع کانال	بی‌سیم
نوع پروتکل مسیریابی	AODV

در این مقاله از نظریه منفعت مورد انتظار [۵۵] برای ارزیابی ارزش مجموعه اولویت‌ها استفاده شده است که مقادیر بدین صورت مقداردهی می‌شوند: SI =0، NI=0.2، NT=0.4 و ST=0.5. سپس در محدوده فرکانس ۱۰ ضرب می‌شود تا بتوان ارزش هر راهبرد را به دست آورد. همچنین TN=0.3، IS=0.2، IN=0.1 و TS=0 مقداردهی اولیه می‌شوند که در نتیجه آن مقادیر جدول ۳ پس از مقداردهی اولیه به مقادیر نشان‌داده‌شده در جدول ۵ تغییر کرده است.

جدول ۵- مقداردهی اولیه حالات درآمد

Strategy	Trust	Isolate
Normal	(4,3)	(2,1)
Selfish	(5,0)	(0,2)

مقداردهی‌ها بر اساس میزان سود هر یک از شرکت‌کنندگان در بازی تعیین شده است. بر اساس راهبردهای بازی، حالت‌هایی که گره خودخواه بوده و سیستم عامل به آن اعتماد دارد باید بیشترین درآمد را داشته باشد و بعد از آن گره در حالت نرمال و اعتماد دارای بیشترین درآمد می‌باشد. کمترین درآمد هم مربوط به زمانی است که گره توسط سیستم عامل به علت رفتار خودخواهانه مجازات شده است؛ یعنی راهبرد گره خودخواهانه بوده و راهبرد سیستم عامل، جداسازی می‌باشد. برای سیستم عامل نیز بیشترین درآمد مربوط به زمانی است که گره حالت نرمال داشته و سیستم عامل به او اعتماد دارد. این باعث خواهد شد که در صورت رفتار نرمال گره، سیستم عامل حالت اعتماد خود را حفظ نموده و تغییر راهبرد ندهد. کمترین میزان درآمد سیستم عامل هم زمانی است که گره حالت خودخواه داشته و سیستم عامل به او اعتماد دارد. در این بین باید درآمد گره در راهبرد جداسازی و رفتار خودخواهانه گره بیشتر از حالت راهبرد نرمال گره و

جداسازی سیستم عامل باشد تا در صورت اصلاح رفتار گره به حالت نرمال، سیستم عامل درآمد کمتری کسب کرده و برای دریافت سود بیشتر حالت خود را به اعتماد تغییر دهد.

علاوه بر این، مطابق با قضیه ۲، فاکتور تخفیف $\delta = 1/3$ محاسبه شده است که نشان می‌دهد درآمد راهبرد نرمال، حداکثرسازی مجازات در فواصل زمانی k $(k = 1, 2, \dots)$ است. با این‌حال، در شرایط واقعی نمی‌توان مقدار k را به صورت نامحدود در نظر گرفت؛ بنابراین مقادیر مقداردهی اولیه در روابط (۱۰) الی (۱۲) اعمال شده است و نتایج محاسبه‌شده از این معادلات به شرح زیر است:

$$R_{N1}(k) = 4(1 + \delta + \delta^2 + \cdots + \delta^k)$$
$$R_{N2}(k) = 5$$
$$R_{N3}(k) = 5 + 2\delta(1 + \delta + \delta^2 + \cdots + \delta^k)$$

برای پیداکردن یک جفت مقادیر مناسب برای (δ,k) می‌توان مقدار δ_k را محاسبه کرد که نشان‌دهنده مقدار ضریب تخفیف δ در شرایط مختلف k $(k = 1,2,\dots)$ است. در نتیجه:

$$R_k(\delta) = \left(R_{N1}(k) - R_{N3}(k)\right) > 0$$

در اینجا، تغییر در مقدار δ تغییر در هر جفت k مجاور را نشان می‌دهد. فرض می‌شود که جفت مقادیر (δ,k) زمانی مؤثر است که $\Delta\delta$ <0.001. با توجه به اینکه $\lim_{k\to inf} k_\delta = 1/3$ ، در نتیجه $\delta = 0.334$ تعیین می‌شود. سپس این مقدار در رابطه (۶) برای پیدا کردن حداقل مقدار برای k $(k = 1,2,\dots)$ اعمال می‌شود. در انجام این کار، حداقل مقدار k =5 از طریق محاسبه به‌دست می‌آید و جفت مقادیر به‌صورت (۵،۰.۳۳۴) حاصل می‌گردد.

با توجه به جدول ۴، شبکه دارای ابعاد ۲۰۰۰ متر در ۳۰۰۰ متر است و تعداد ۲۰ گره در شبیه‌سازی استفاده شده است. گره‌های موجود در فضای شبکه با توجه به مدل حرکتی تصادفی به کمک شبیه‌ساز تحرک شهری SUMO ایجاد شده است. در این مدل، هر گره به یک مکان تصادفی در درون یک شبکه مشخص حرکت می‌کند که یک گره به محل هدف می‌رسد و در موقعیت باقی می‌ماند.

در نهایت یک شبکه سیار موردی IEEE 802.11 مورد ارزیابی قرار گرفته است که در بین گره‌ها، ۳ گره رفتار خودخواهانه داشته‌اند. شعاع ارتباطی همه گره‌ها ۲۵۰ متر است. خروجی در شکل ۳ نشان داده شده است. در این شکل گره‌های قرمز گره‌های مقصد، گره‌های آبی گره‌های مبدأ، گره‌های مشکی گره‌های نرمال و گره‌های سبز، گره‌های خودخواه را نشان می‌دهند.

۶-۲- پارامترهای ارزیابی

برای ارزیابی عملکرد طرح پیشنهادی نیاز به معیارهایی است که این معیارها در ادامه تعریف شده‌اند.

- نسبت تحویل بسته: این معیار قابلیت اطمینان مسیریابی موفق را نشان می‌دهد و به صورت زیر تعریف می‌شود:

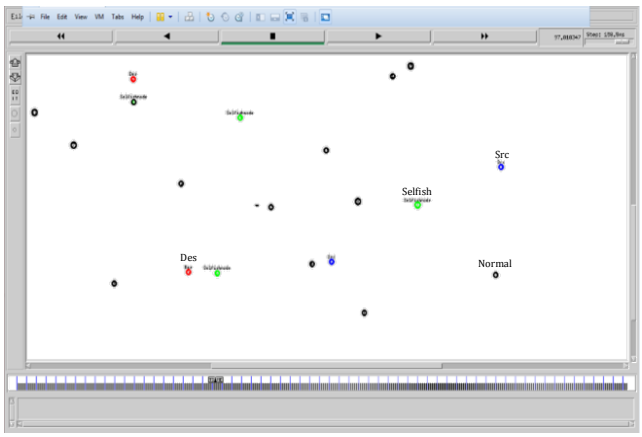
  مجموع بسته‌های ارسالی/ بسته‌های دریافت‌شده

- زمان تأخیر تحویل: این معیار به‌صورت میانگین تأخیر انتقال بسته داده از گره مبدا به مقصد تعریف می‌شود. متوسط تأخیر، تأخیری را که رویکرد مسیریابی ایجاد کرده است مشخص می‌کند.

- نسبت از دست دادن بسته: این معیار در گره‌های خودخواه، میزان بسته‌های از دست‌رفته در اثر رفتار خودخواهانه را نشان می‌دهد و به‌صورت زیر محاسبه می‌گردد:

  کل بسته‌های تولیدشده/ تعداد بسته‌های از دست‌رفته

- توان عملیاتی: متوسط نرخ تحویل موفق پیام در یک کانال ارتباطی است. توان عملیاتی معمولاً به‌وسیله بیت بر ثانیه اندازه‌گیری می‌شود.



شکل ۳- خروجی حاصل از شبیه‌سازی

۶-۳- بحث و ارزیابی عملکرد روش پیشنهادی

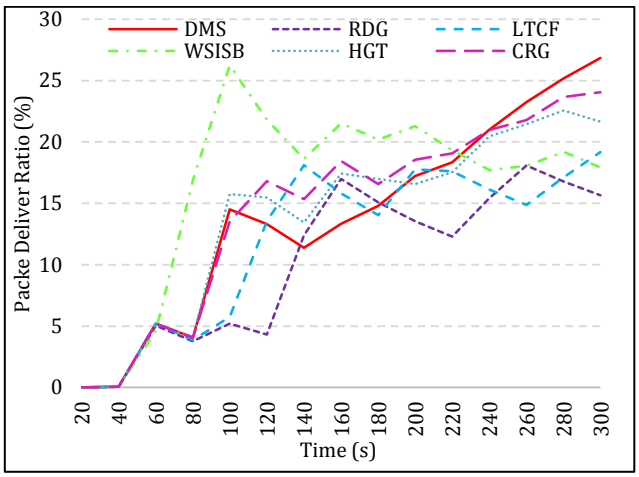
در این بخش عملکرد روش پیشنهادی با سایر روشها از نظر نسبت تحویل بسته، تأخیر انتها به انتها، نسبت از دست دادن بسته و توان عملیاتی مقایسه شده و مورد تحلیل و ارزیابی قرارگرفته است.

شکل ۴ نشان‌دهنده نسبت تحویل بسته است. همان‌طور که مشاهده می‌شود DMS با گذشت زمان نسبت تحویل بالاتری نسبت به دیگر روشهای موجود دارد. دلیل این امر این است که DMS از الگوریتم نرخ بسته دریافتی و ارسالی در گره و همچنین الگوریتم آستانه تطبیقی اصلاح‌شده برای تشخیص گره خودخواه استفاده می‌کند. DMS به کمک این دو الگوریتم می‌تواند با دقت بالایی گره خودخواه را تشخیص دهد.

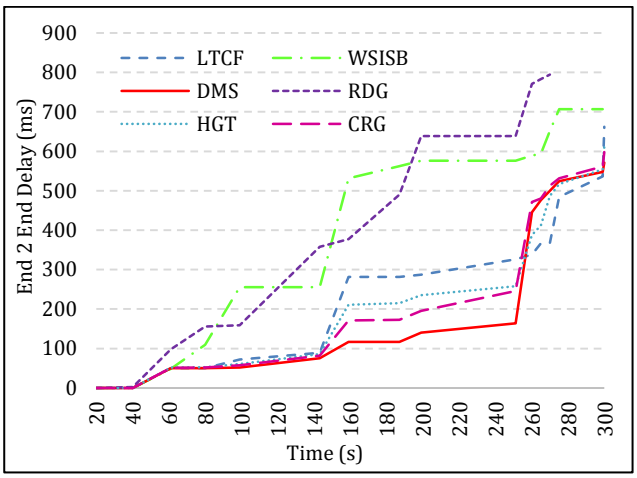
علاوه بر این DMS از نظریه بازی‌ها برای جلوگیری از رفتار خودخواهانه استفاده می‌کند که باعث می‌شود در طول زمان، گره از حالت خودخواه به حالت نرمال تغییر وضعیت بدهد. همچنین با استفاده از بالاترین تابع وزن (HWF) پیشنهادشده برای مسیریابی DMS، مسیر با کمترین طول و بیشترین انرژی گره‌ها را انتخاب می‌نماید. در این صورت تعداد گام‌ها کاهش یافته، که در نتیجه ایجاد یک ارتباط کارآمد و قابل‌اطمینان بین گره‌های شبکه تضمین شده و بسته‌های داده با احتمال بالاتری به مقصد خواهند رسید. DMS نسبت تحویل بسته بالاتری را در مقایسه با RDG دارد. دلیل این امر این است که DMS از تابع وزن استفاده می‌کند که تعداد گام تا رسیدن به مقصد را کاهش می‌دهد.

همچنین DMS نسبت تحویل بسته بالاتری را نسبت به LTCF دارد که دلیل آن این است که DMS به علت استفاده از الگوریتم آستانه تطبیقی سریع‌تر و با دقت بالاتری گره‌های خودخواه را تشخیص داده و از رفتار خودخواهانه آن‌ها جلوگیری می‌نماید. در روش WSISB ابتدا میزان تحویل بسته بالاتری قابل مشاهده است و به مرور زمان این مقدار کاهش یافته است. WSISB پس از تشخیص گره خودخواه برای جلوگیری از رفتار خودخواهانه، گره را حذف می‌کند. در نتیجه گره از فرآیند مسیریابی خارج می‌شود؛ بنابراین در این روش به مرور زمان گره‌های خودخواه بیشتری حذف شده و با گذشت زمان میزان تحویل بسته کاهش یافته است.

در مقایسه با روش HGT، روش DMS بهتر عمل کرده است که دلیل آن احتمال ایجاد خطا در خوشه‌بندی گره‌ها و تشخیص گره‌های خودخواه با زیاد شدن تعداد گره‌ها در روش HGT می‌باشد. همچنین روش CRG که نزدیکترین نسبت تحویل بسته را در مقایسه با سایر روشها به DMS دارد، به علت راهبرد مجازات سختگیرانه (جدول ۲)، باعث بازگشت دیرهنگام گره‌های خودخواه به فرآیند مسیریابی شبکه خواهد شد و در نتیجه روش CRG نسبت تحویل بسته کمتری در مقایسه با روش DMS خواهد داشت.



شکل ۴- نسبت تحویل بسته‌ها



شکل ۵- تأخیر انتها به انتها

تأخیر انتها به انتها برای روش‌های مختلف در شکل ۵ نشان داده شده است. همانطور که از شکل مشخص است، DMS عملکرد بهتری نسبت به سایر روش‌ها در تأخیر انتها به انتها داشته است. دلیل آن این است که در DMS بر اساس وزن هر یک از مسیرها، بهترین مسیر برای ارسال بسته‌های داده تعیین می‌شود. بر اساس وزن هر یک از مسیرها، مسیری انتخاب می‌شود که دارای کوتاه‌ترین طول و فاصله اقلیدسی بوده و سطح انرژی گره‌های میانی بالاتری را داراست. کوتاه‌تر بودن مسیر باعث کاهش تأخیر انتشار که وابسته به طول ارتباط است می‌گردد. همچنین بر اساس الگوریتم‌های تشخیص رفتار خودخواهانه می‌توان در زمان کوتاه‌تر و با دقت بالاتری گره‌های خودخواه را تشخیص داد و از رفتار خودخواهانه آن‌ها جلوگیری نمود. انتخاب مسیر با انرژی گره‌های بالاتر و فاصله کمتر تا مقصد، اتصال شبکه را بهبود داده و تعداد گام‌ها در ارتباط بین گره‌ها را کاهش می‌دهد که باعث کاهش تأخیر انتقال ناشی از ارسال بسته‌های داده در هر گره می‌شود.

دلیل اختلاف تأخیر بین WSISB و DMS این است که DMS پس از تشخیص گره خودخواه از روش تنبیه جهت جلوگیری از رفتار خودخواهانه استفاده می‌نماید و گره‌ها از دسترس خارج نمی‌شوند، اما در روش WSISB پس از تشخیص گره خودخواه در فاز جلوگیری، گره خودخواه حذف خواهد شد. علت اختلاف تأخیر بین DMS و LTCF این است که LTCF از الگوریتم آستانه تطبیقی برای شناسایی گره‌های خودخواه استفاده نمی‌کند. همچنین در DMS نظریه بازی بین گره‌های موجود در شبکه و سیستم‌عامل نصب‌شده در ایستگاه پایه اجرا می‌شود که این امر باعث می‌شود که برای تنبیه گره‌های خودخواه، خود گره‌های شبکه وارد عمل نشوند و بتوان از آن گره‌ها برای ارسال پیام استفاده کرد. RDG فاقد الگوریتم‌های تشخیص گره خودخواه بوده و فقط از رفتار خودخواهانه جلوگیری می‌نماید. همچنین در RDG هیچ تابع وزنی برای تعیین مسیر مناسب ارائه نشده است؛ در نتیجه مسیر انتخاب‌شده از تأخیر بالاتری برخوردار بوده است. روش HGT با توجه به زمان موردنیاز برای خوشه‌بندی و تشخیص گره خودخواه، دارای تاخیر انتها به انتهای بیشتری در مقایسه با DMS است. همچنین روش CRG با توجه به تعداد مراحل بالا و زمانبر برای مجازات گره‌ها، در مقایسه با روش DMS دارای تاخیر انتها به انتهای بیشتری است.

شکل ۶ نسبت از دست رفتن بسته‌ها را نشان می‌دهد. با افزایش زمان، میزان از دست رفتن بسته‌ها کاهش یافته است؛ دلیل آن این است که با گذشت زمان و اجرای بازی‌های تکراری در مراحل مختلف، تمایل گره‌ها به رفتار خودخواهانه کاهش یافته است. در نتیجه از دست رفتن بسته‌های کمتری اتفاق می‌افتد.

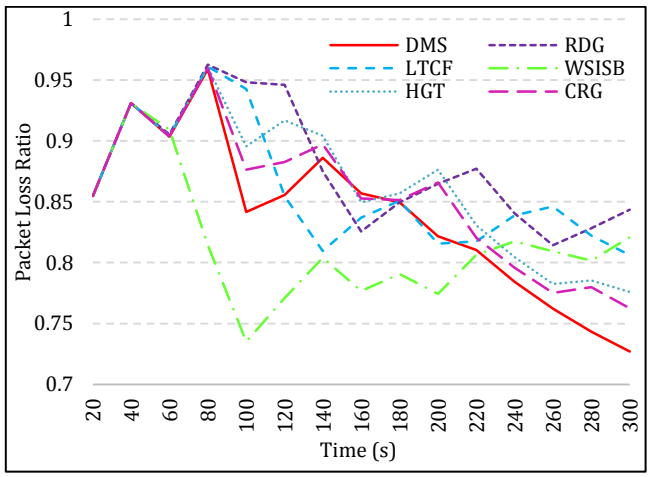
از آنجایی‌که DMS از الگوریتم‌های نرخ دریافت و ارسال بسته در گره‌ها و الگوریتم آستانه تطبیقی اصلاح‌شده استفاده می‌کند، می‌تواند در مدت زمان کمتر و به‌صورت دقیق‌تری گره‌های با رفتار خودخواهانه را تشخیص دهد و به کمک نظریه بازی‌های تکراری پیاده‌سازی شده، هر چه سریع‌تر از رفتار خودخواهانه جلوگیری نماید. در نتیجه میزان از دست رفتن بسته در DMS نسبت به سایر روش‌های شبیه‌سازی‌شده کمتر بوده است. از طرفی DMS از تابع وزن برای انتخاب مسیر استفاده می‌کند که کوتاه‌ترین مسیر با بالاترین انرژی گره‌ها جهت ارسال بسته انتخاب می‌شود. کاهش تعداد گام برای انتقال پیام در شبکه باعث کاهش میزان از دست رفتن بسته در اثر سرریز بافر، صف‌بندی و یا مسائل دیگر می‌شود که این امر هم موجب کاهش میزان از دست دادن بسته در DMS شده است. LTCF به دلیل عدم استفاده از الگوریتم آستانه تطبیقی برای تشخیص رفتار خودخواهانه و همچنین در نظر نگرفتن پارامترهای فاصله اقلیدسی و انرژی گره‌ها در تعیین مسیر مناسب ارسال بسته‌ها، میزان از دست دادن بسته بالاتری را نسبت به DMS داشته است.

WSISB از تابع وزن برای تشخیص گره خودخواه استفاده می‌کند و پس از تشخیص گره خودخواه، آن را حذف می‌نماید. حذف گره‌های خودخواه باعث می‌شود میزان از دست رفتن بسته در اثر رفتار خودخواهانه کاهش یابد و از طرفی به دلیل عدم امکان استفاده از گره، میزان تحویل بسته‌های داده نیز کاهش می‌یابد. از این‌رو WSISB میزان از دست دادن بسته بالاتری را نسبت به DMS خواهد داشت.

از آنجایی‌که RDG فقط از نظریه بازی برای جلوگیری از رفتار خودخواهانه استفاده کرده و برای این کار از خود گره‌ها استفاده می‌نماید و اینکه RDG فاقد روشی برای محاسبه مسیر مناسب است، میزان از دست دادن بسته در آن نسبت به سایر روش‌ها بالاتر بوده است. با توجه به دقت کمتر روش HGT در مقایسه با روش DMS در تشخیص گره‌های خودخواه، نسبت از دست رفتن بسته‌ها در روش HGT نسبت به روش DMS بیشتر است.

همچنین روش CRG نیز به دلیل عدم استفاده از تابع وزن در مسیریابی، بسته‌ها مسیر بیشتری در مقایسه با DMS طی کرده و نسبت از دست رفتن بسته‌ها افزایش یافته است.

در جدول ۶، مقادیر کلیه پارامترهای ارزیابی برای چهار روش بیان شده در این مقاله آورده شده است. در این جدول، نسبت کل بسته‌های از دست‌رفته در اثر رفتار خودخواهانه گره‌ها نیز ارائه شده است. در این حالت صرفاً بسته‌هایی که در زمان رفتار خودخواهانه یک گره دور انداخته‌شده‌اند، اندازه‌گیری شده است.



شکل ۶- نسبت از دست دادن بسته‌ها

جدول ۶- مقادیر پارامترهای ارزیابی در روش‌های مختلف

پارامتر / روش	نسبت تحویل بسته‌ها (٪)	میانگین تأخیر انتها به انتها (ms)	نسبت کل از دست دادن بسته‌ها	نسبت کل از دست دادن بسته‌ها در رفتار خودخواهانه	توان عملیاتی (kbps)
DMS	۲۶.۸۵۰۴	۱۴۳.۸۴۱	۰.۷۲۷۰۴۸	۰.۲۲۵۳۹۹	۵۵.۸
WSISB	۱۷.۹۲۱۲	۲۷۱.۰۳۶	۰.۸۲۰۹۱۸	۰.۲۳۰۴۱۵	۴۰.۵۱
LTCF	۱۹.۱۸۰۸	۲۳۴.۷۳۸	۰.۸۰۶۲۸۱	۰.۳۷۳۷۶۳	۳۹.۸۷
RDG	۱۵.۶۶۲۲	۳۴۸.۷۸۷	۰.۸۴۳۵۷۴	۰.۴۶۴۸۸۵	۳۷.۶۰
HGT	۲۱.۶۵۳۲	۱۹۲.۵۷۶	۰.۷۷۵۸۷۴	۰.۲۲۹۸۹	۴۵.۸۷
CRG	۲۴.۰۶۴۳	۱۷۶.۴۷۸	۰.۷۶۲۵۴۷	۰.۲۲۸۶۵	۵۰.۳۲

همان‌طور که مشخص است DMS میزان بسته‌های از دست‌رفته کمتری را در اثر رفتار خودخواهانه داشته است. بدین دلیل که از الگوریتم‌های نسبت دریافت و ارسال بسته و آستانه تطبیقی اصلاح‌شده برای تشخیص رفتار خودخواهانه استفاده می‌کند که در زمان کوتاه‌تر و با دقت بالاتری می‌تواند رفتار خودخواهانه را تشخیص دهد. پس از تشخیص گره‌های خودخواه، DMS با استفاده از نظریه بازی‌های تکراری سعی در جلوگیری از رفتار خودخواهانه با تنبیه گره‌ها می‌نماید.

همچنین جدول ۶ نشان می‌دهد که DMS میزان توان عملیاتی بالاتری را نسبت به روشهای WSISB، LTCF، RDG، HGT و CRG داشته است. از آنجایی‌که DMS عملکرد بهتری را در تشخیص و جلوگیری از رفتار خودخواهانه گره‌ها دارد، در نتیجه مدت‌زمان بروز رفتار خودخواهانه در گره‌ها کاهش‌یافته و این امر موجب افزایش نرخ تحویل موفق پیام در مسیرهای موجود شده است. RDG به دلیل نداشتن روشی برای تعیین مسیر مناسب و عدم استفاده از سیستم‌عامل مرکزی در فاز جلوگیری، دارای پایین‌ترین توان عملیاتی بوده است. WSISB میزان توان عملیاتی پایین‌تری را نسبت به DMS داشته است. WSISB فقط از تابع وزن محاسبه‌شده بر اساس پارامترهای نسبت ارسال به دریافت بسته‌های داده، میزان انرژی باقی‌مانده و میزان از دست دادن بسته برای تشخیص رفتار خودخواهانه استفاده می‌نماید و پس از شناسایی گره خودخواه آن را حذف می‌کند. در نتیجه نسبت به روش DMS از قدرت شناسایی گره خودخواه پایین‌تری برخوردار بوده و فاقد فاز جلوگیری از رفتار خودخواهانه است. LTCF نیز فاقد الگوریتم آستانه تطبیقی برای تشخیص دقیق و سریع گره خودخواه بوده و همچنین در فاز جلوگیری از رفتار خودخواهانه، از خود گره‌ها برای مقابله با رفتار خودخواهانه استفاده می‌کند که دارای کارایی پایین‌تری نسبت به روش DMS می‌باشد. در نتیجه میزان توان عملیاتی در LTCF نسبت به DMS پایین‌تر بوده است. HGT به علت استفاده از خوشه‌بندی و مجازات گره‌های خودخواه به صورت عدم همکاری دیگر گره‌ها با آنها، باعث کاهش توان عملیاتی در مقایسه با DMS شده است. همچنین روش CRG نیز دارای طرح مجازات سختگیرانه چهار مرحله-ای جهت اجازه بازگشت گره خودخواه به فرآیند مسیریابی شبکه است که این امر باعث کاهش توان عملیاتی این روش در مقایسه با روش DMS شده است.

مطابق جدول ۷ میزان بهبود عملکرد شبکه بر اساس پارامترهای ارزیابی بدین شرح است. نسبت تحویل بسته در روش پیشنهادی DMS نسبت به روش WSISB، ۴۹.۸۲٪، نسبت به روش LTCF، ۳۹.۹۸٪، نسبت به روش RDG، ۷۱.۴۳٪، نسبت به روش HGT، ۲۴٪ و نسبت به روش CRG، ۱۱.۵۸٪ افزایش داشته است.

این میزان بهبود در توان عملیاتی به ترتیب نسبت به WSISB، LTCF، RDG، HGT و CRG برابر ۳۷.۷۴٪، ۳۹.۹۵٪، ۴۸.۴۰٪، ۲۱.۶۵٪ و ۱۰.۸۹٪ است. DMS همچنین تأخیر انتها به انتها را به میزان ۴۶.۹۳٪ نسبت به WSISB، ۳۸.۷۲٪ نسبت به LTCF، ۵۸.۷۵٪ نسبت به RDG، ۲۶.۰۷٪ نسبت به HGT و ۱۸.۴۹٪ نسبت به CRG کاهش داده است.

میزان کاهش نسبت از دست دادن بسته در DMS نسبت به WSISB، LTCF، RDG، HGT و CRG به ترتیب برابر ۱۱.۴۳٪، ۹.۸۳٪، ۱۳.۸۱٪، ۶.۲۹٪ و ۴.۶۵٪ است. همچنین در DMS میزان بهبود نسبت از دست دادن بسته‌ها در اثر رفتار خودخواهانه گره‌ها نسبت به WSISB برابر ۲.۱۸٪، نسبت به LTCF، برابر ۳۹.۶۲٪، نسبت به RDG، برابر ۵۱.۵۱٪، نسبت به HGT، برابر ۱.۹۵٪ و نسبت به CRG، ۱.۴۲٪ بوده است.

جدول ۷- میزان بهبود پارامترهای روش DMS نسبت به سایر روش‌ها

پارامتر / روش	نسبت تحویل بسته‌ها	میانگین تأخیر انتها به انتها	نسبت کل از دست دادن بسته‌ها	نسبت کل از دست دادن بسته‌ها در رفتار خودخواهانه	توان عملیاتی
WSISB	۴۹.۸۲٪	۴۶.۹۳٪	۱۱.۴۳٪	۲.۱۸٪	۳۷.۷۴٪
LTCF	۳۹.۹۸٪	۳۸.۷۲٪	۹.۸۳٪	۳۹.۶۹٪	۳۹.۹۵٪
RDG	۷۱.۴۳٪	۵۸.۷۵٪	۱۳.۸۱٪	۵۱.۵۱٪	۴۸.۴۰٪
HGT	۲۴٪	۲۶.۰۷٪	۶.۲۹٪	۱.۹۵٪	۲۱.۶۵٪
CRG	۱۱.۵۸٪	۱۸.۴۹٪	۴.۶۵٪	۱.۴۲٪	۱۰.۸۹٪

۷- نتیجه‌گیری

حضور یک گره خودخواه در شبکه سیار موردی ممکن است به کل سیستم ارتباطی آسیب برساند؛ بنابراین، لازم است که این گره‌های خودخواه شناسایی شوند و همکاری در شبکه را افزایش دهند.

در این مقاله الگوریتمی پیشنهاد شده است که بتواند گره‌های خودخواه در شبکه سیار موردی را شناسایی کند و اطمینان حاصل کند که بسته اطلاعاتی تنها از طریق مسیر با بالاترین تابع وزن از گره مبدأ به گره مقصد منتقل خواهد شد.

روش پیشنهادی مقابله با رفتار خودخواهانه گره‌ها را در شبکه سیار موردی، در دو فاز انجام داده است. در فاز تشخیص رفتار خودخواهانه، با ترکیب دو الگوریتم نرخ دریافت و ارسال بسته و الگوریتم آستانه تطبیقی اصلاح‌شده، رفتار خودخواهانه را تشخیص داده و سپس در فاز جلوگیری، از نظریه بازی‌های تکراری بهره برده است تا میزان رفتار خودخواهانه در شبکه کاهش پیدا کند.

در روش پیشنهادی، تابع وزن هر یک از مسیرهای یافت شده توسط پروتکل AODV محاسبه شده و بر اساس فاکتور HWF مسیر با بالاترین وزن انتخاب شده است. وزن بالاتر نشان‌دهنده مسیر کوتاه‌تر با سطح انرژی بالاتر گره‌های میانی است. پس از تعیین مسیر، بر اساس الگوریتم نرخ دریافت و ارسال بسته‌ها، میزان بسته‌های داده دریافتی و ارسالی توسط گره‌های موجود در مسیر، جهت تعیین گره خودخواه مورد مقایسه قرار گرفته است. علاوه بر این، رفتار خودخواهانه بر اساس مقایسه تعداد بسته‌ها در یک الگوریتم آستانه تطبیقی اصلاح‌شده با مقایسه PFR هر گره با مقدار آستانه تخمین زده‌شده بر اساس نرخ ارسال بسته‌ها تشخیص داده شده است. سپس از بازی‌های تکراری جهت جلوگیری از رفتار خودخواهانه گره‌ها استفاده شده است. وقتی یک گره رفتار خودخواهانه را در یک مرحله از بازی انتخاب کند، آن گره در مرحله بعدی مجازات خواهد شد که منجر به درآمد کم‌تر گره نسبت به شرایط نرمال می‌شود. در نتیجه، گره‌ها تمایل به انتخاب یک راهبرد نرمال بعد از یک بازه زمانی خاص دارند. روش پیشنهادی با نام DMS مورد شبیه‌سازی قرار گرفته و با سایر روش‌های WSISB، RDG، LTCF، HGT و CRG مقایسه شده است. نتایج شبیه‌سازی نشان می‌دهند که روش DMS پیشنهادی عملکرد بهتری را در نسبت تحویل بسته‌ها، میزان تأخیر انتها به انتها، نسبت از دست دادن بسته‌ها در کل شبکه و در گره‌های خودخواه و همچنین میزان توان عملیاتی داشته است.

از آنجائیکه DMS از مسیریابی بر اساس بالاترین تابع وزن استفاده می‌کند، کوتاه‌ترین مسیر با بالاترین میزان انرژی گره‌های میانی جهت ارسال بسته‌های داده انتخاب می‌شود. یک مزیت انتخاب کوتاه‌ترین مسیر، کاهش تأخیر انتقال است. از طرفی DMS از الگوریتم‌های نسبت بسته دریافتی و ارسالی، همچنین الگوریتم آستانه تطبیقی اصلاح‌شده جهت تشخیص و شناسایی رفتار خودخواهانه استفاده می‌نماید که موجب شناسایی دقیق‌تر و سریع‌تر گره‌های خودخواه شده و میزان تحویل بسته، تأخیر، نسبت از دست دادن بسته‌ها و توان عملیاتی را تحت تأثیر قرار داده و باعث بهبود این پارامترها شده است. در فاز جلوگیری نیز DMS به دلیل استفاده از سیستم‌عامل موجود در ایستگاه‌های پایه، عملکرد بهتری داشته که موجب بهبود عملکرد شبکه نیز شده است.

۸- مراجع

[۱] ه. سلطانی گوهری، و م. جلالی نژاد، "بررسی شبکه‌های سیار موردی و پروتکل‌های مسیریابی آن،" در *مجموعه مقالات کنفرانس بین‌المللی مطالعات بین‌رشته‌ای در مدیریت و مهندسی*، تهران، ۱۳۹۷.

[2] M. Mohamed Musthafa, K. Vanitha, A. M. J. MD. Zubair Rahman, and K. Anitha, "An Efficient Approach to Identify Selfish Node in MANET," *Proc. IEEE Int. Conf. Computer Communication and Informatics*, 2020.

[3] A. Chauhan, D. K. Gupta, and M. K. Sah, "Detection of Packet Dropping Nodes in Manet using DSR Routing Protocol," *Int. J. Comput. Appl.*, vol. 123, no. 7, pp. 10-16, 2015.

[۴] س. نوبهاری، و ش. بابایی، "بررسی روش‌های کشف گره‌های خودخواه در شبکه‌های موردی سیار،" در *مجموعه مقالات دومین کنفرانس بین‌المللی پژوهش‌های دانش‌بنیان در مهندسی کامپیوتر و فناوری اطلاعات*، تهران، ۱۳۹۶.

[5] S. Kumar, and K. Dutta, "Trust Based Intrusion Detection Technique to Detect Selfish Nodes in Mobile Ad Hoc Networks," *Wirel. Pers. Commun.*, vol. 101, pp. 2029-2052, 2018.

[۶] م. حسن‌زاده کوچو، م. شجاعی، و آ. حسن‌زاده، "تئوری بازی‌ها،" در *مجموعه مقالات کنفرانس بین‌المللی حسابداری و مدیریت*، تهران، ۱۳۹۳.

[۷] د. جلالی، و م. اسلامی، "بررسی پروتکل‌های مسیریابی در شبکه‌های سیار موردی،" در *مجموعه مقالات سومین کنفرانس بین‌المللی پژوهش‌های کاربردی در مهندسی کامپیوتر و فن‌آوری اطلاعات*، تهران، ۱۳۹۴.

[8] S. Chen, and K. Nahrstedt, "Distributed Quality-of-Service Routing in Ad Hoc Networks," *IEEE J. Sel. areas Commun.*, vol. 17, pp. 1488-1505, 1999.

[9] A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Bölöni, and D. Turgut, "Routing Protocols in Ad Hoc Networks: A Survey," *Comput. Netw.*, vol. 55, pp. 3032-3080, 2011.

[10] C. E. Perkins, and E. M. Royer, "Ad-hoc On-demand Distance Vector Routing," *Proc. IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 1999.

[۱۱] ق. عبدلی، *تئوری بازی‌ها و کاربردهای آن*، انتشارات جهاد دانشگاهی دانشگاه تهران، تهران، ۱۳۸۶.

[12] M. J. Osborne, and A. Rubinstein, *A Course in Game Theory*, Massachusetts: MIT press, 1994.

[۱۳] س. شاهی، ف. اسکندری، س. سعادت، ک. رضایی، "تئوری بازی‌ها،" در *مجموعه مقالات اولین همایش ملی مدیریت کسب و کار*، همدان، ۱۳۹۲.

[14] A. Rapoport, *Game Theory as a Theory of Conflict Resolution*, vol. 2, Boston: Springer Science & Business Media, 2012.

[15] K. Binmore, *Game Theory: A Very Short Introduction*, vol. 173, Oxford: Oxford University Press, 2007.

[16] H. Yadav, and H. K. Pati, "A Survey on Selfish Node Detection in MANET," *Proc. Int. Conf. Advances in Computing, Communication Control and Networking*, pp. 217-221, 2018.

[17] A. Rodriguez-Mayol, and J. Gozalvez, "Reputation Based Selfishness Prevention Techniques for Mobile Ad-hoc Networks," *Telecommun. Syst.*, vol. 57, pp. 181-195, 2014.

[18] S. S. Shinde, and B. D. Phulpagar, "A Comparative Study of Selfish Node Detection Methods in Manet," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, 2015.

[19] Z. Ji, W. Yu, and K. R. Liu, "A Game Theoretical Framework for Dynamic Pricing-based Routing in Self-organized MANETs," *IEEE J. Sel. areas Commun.*, vol. 26, pp. 1204-1217, 2008.

[20] C. Pandana, Z. Han, and K. R. Liu, "Cooperation Enforcement and Learning for Optimizing Packet Forwarding in Autonomous Wireless Networks," *IEEE Trans. Wirel. Commun.*, vol. 7, pp. 3150-3163, 2008.

[21] M. Touati, R. El-Azouzi, M. Coupechoux, E. Altman, and J.-M. Kelif, "A Controlled Matching Game for WLANs," *IEEE J. Sel. areas Commun.*, vol. 35, pp. 707-720, 2017.

[22] L. E. Jim, and M. A. Gregory, "Improvised MANET Selfish Node Detection using Artificial Immune System based Decision Tree," *Proc. Int. Telecommunication Networks and Applications Conference*, 2019.

[23] A. A. Hadi, Z. Md. Ali, and Y. Aljeroudi, " Improved Selfish Node Detection Algorithm for Mobile Ad Hoc Network," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, pp. 103-108, 2017.

[24] A. Shan, X. Fan, C. Wu , X. Zhang, and S. Fan, "Quantitative Study on the *Impact* of Energy Consumption Based Dynamic Selfishness in MANETs," *Sensors*, vol. 21, 2021.

[25] O. A. Wahab, H. Otrok, and A. Mourad, "A Cooperative Watchdog Model Based on Dempster–Shafer for Detecting Misbehaving Vehicles," *Comput. Commun.*, vol. 41, pp. 43-54, 2014.

[26] J. Guo, H. Liu, J. Dong, and X. Yang, "HEAD: A Hybrid Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *Tsinghua Sci. Technol.* , vol. 12, pp. 202-207, 2007.

[27] Z. K. Chong, S. W. Tan, B. M. Goi, and B. C. K. Ng, "Outwitting Smart Selfish Nodes in Wireless Mesh Networks," *Int. J. Commun. Syst.*, vol. 26, pp. 1163-1175, 2013.

[28] M. Ponnusamy, Dr. A. Senthilkumar, and Dr. R. Manikandan, "Detection of Selfish Nodes Through Reputation Model in Mobile Adhoc Network – MANET," *Turk. J. Comput. Math. Educ.*, vol. 12, pp. 2404–2410, 2021.

[29] B. UI. Islam, , R. F. Olanrewaju, F. Anwar, A. R. Najeeb, and M. Yaacob, "A Survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, pp. 832-842, 2018.

[30] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad-hoc Networks," *Proc. Annual Joint Conf. IEEE Computer and Communications Societies*, pp. 1987-1997, 2003.

[31] R. Kaushik and J. Singhai, "Modspirite: A Credit Based Solution to Enforce Node Cooperation in an Ad-hoc Network," *Int. J. Comput. Sci. Issues*, vol. 8, 2011.

[32] L. Buttyan and J.-P. Hubaux, "Nuglets: A Virtual Currency to Stimulate Cooperation in Self-organized Mobile Ad Hoc Networks," 2001.

[33] K. R. Abirami, M. G. Sumithra, "Evaluation of Neighbor Credit Value based AODV Routing Algorithms for Selfish Node Behavior Detection," *Clust. Comput.*, Special Issue 6, 2019.

غلامرضا فراهانی مدرک کارشناسی خود را در رشته مهندسی برق از دانشگاه صنعتی شریف در سال ۱۳۷۷ دریافت نموده و مدارک کارشناسی ارشد و دکتری خود در رشته مهندسی برق را از دانشگاه صنعتی امیرکبیر به ترتیب در سالهای ۱۳۷۹ و ۱۳۸۵ اخذ نموده است. ایشان در حال حاضر عضو هیات علمی پژوهشکده برق و فناوری اطلاعات سازمان پژوهشهای علمی و صنعتی ایران با درجه دانشیاری است. از زمینه‌های تحقیقاتی مورد علاقه ایشان، شبکه‌های کامپیوتری، شبکه‌های سیار موردی، مسیریابی و تشخیص نفوذ در شبکه می‌باشد. آدرس پست الکترونیکی ایشان عبارت است از:

farahani.gh@irost.org

[1] Mobile Ad Hoc Networks
[2] Selfish
[3] Reactive
[4] Proactive
[5] Table Driven - Proactive
[6] Demand Driven - Reactive
[7] Hybrid
[8] Link - State
[9] Distance - Vector
[10] Periodic
[11] Route Request (RREQ)
[12] Route Reply (RREP)
[13] Ad hoc On-demand Distance Vector (AODV)
[14] Destination-Sequenced Distance Vector (DSDV)
[15] Dynamic Source Routing (DSR)
[16] Nash Equilibrium
[17] Reputation Based Schema
[18] Credit Based Schema
[19] Game Theory Based Schema
[20] Utility
[21] Nash
[22] Framework
[23] Artificial Immune System (AIS)
[24] Detection and Mitigating Selfish behavior (DMS)
[25] High Weight Function (HWF)
[26] Separation of Detection Authority (SDA)
[27] Selfish Node Removal using Reputation Model (SNRRM)
[28] Game-based Reputation and Trust Scheme (GRTS)
[29] Neighbor Credit Value (NCV)
[30] improved NCV (iNCV)
[31] Weight-based Secure approach for Identifying Selfishness Behavior
[32] Record-and Trust-Based Detection
[33] Packet Forwarding
[34] Game Theory-based Real-time & Fault-tolerant (GTRF)
[35] Energy Efficient Topology Control Algorithm (EETCA)
[36] Replication Dilemma Game (RDG)
[37] Least Total Cost Factor (LTCF)
[38] Hierarchical Game Theory (HGT)
[39] Least Total Cost Factor (LTCF)
[40] Slaved mode
[41] Resource exhausting
[42] Weight Function (WF)
[43] Total Weight Function (TWF)
[44] Route Error (RERR)
[45] Packet Forwarding Ratio (PFR)
[46] Exponentially Weighted Moving Average (EWMA)
[47] Trust
[48] Isolate
[49] Constant Bit Rate (CBR)

[34] D. Koshti and S. Kamoji, "Comparative Study of Techniques Used for Detection of Selfish Nodes in Mobile Ad Hoc Networks," *Int. J. Soft Comput. Eng.*, pp. 2231-2307, 2011.
[35] S. Khan, R. Prasad, P. Saurabh, and B. Verma, "Weight-Based Secure Approach for Identifying Selfishness Behavior of Node in MANET," in *Information and Decision Sciences*, Singapore: Springer, pp. 387-397, 2018.
[36] R. Singh, P. Singh, and M. Duhan, "An Effective Implementation of Security Based Algorithmic Approach in Mobile Adhoc Networks," *Hum. Cent. Comput. Inf. Sci.*, vol. 4, 2014.
[37] J. M. S. P. J. Kumar, A. Kathirvel, N. Kirubakaran, P. Sivaraman, and M. Subramaniam, "A Unified Approach for Detecting and Eliminating Selfish Nodes in MANETs Using TBUT," *EURASIP J. Wirel. Commun. Netw.*, vol. 2015, 2015.
[38] E. Hernandez-Orallo, M. D. S. Olmos, J.-C. Cano, C. T. Calafate, and P. Manzoni, "CoCoWa: A Collaborative Contact-based Watchdog for Detecting Selfish Nodes," *IEEE trans. Mob. Comput.*, vol. 14, pp. 1162-1175, 2014.
[39] S. Subramaniyan, W. Johnson, and K. Subramaniyan, "A Distributed Framework for Detecting Selfish Nodes in MANET Using Record- and Trust-Based Detection (RTBD) Technique," *EURASIP J. Wirel. Commun. Netw.*, vol. 2014, 2014.
[40] D. Hirsch and S. Madria, "Data Replication in Cooperative Mobile Ad-hoc Networks," *Mob. Netw. Appl.*, vol. 18, pp. 237-252, 2013.
[41] F. Afghah, A. Razi, and A. Abedi, "Stochastic Game Theoretical Model for Packet Forwarding in Relay Networks," *Telecommun. Syst.*, vol. 52, pp. 1877-1893, 2013.
[42] S. U. Khan, A. A. Maciejewski, H. J. Siegel, and I. Ahmad, "A Game Theoretical Data Replication Technique for Mobile Ad Hoc Networks," *Proc. IEEE Int. Symposium on Parallel and Distributed Processing*, pp. 1-12, 2008.
[43] T. Lei, S. Wang, J. Li, I. You, and F. Yang, "Detecting and Preventing Selfish Behaviour in Mobile Ad Hoc Network," *J. Supercompu.*, vol. 72, pp. 3156-3168, 2016.
[44] C. Lin, G. Wu, and P. Pirozmand, "GTRF: A Game Theory Approach for Regulating Node Behavior in Real-time Wireless Sensor Networks," *Sensors*, vol. 15, pp. 12932-12958, 2015.
[45] A. Waqas and H. Mahmood, "A Game Theoretical Approach for Topology Control in Wireless Ad Hoc Networks with Selfish Nodes," *Wirel. Pers. Commun.*, vol. 96, pp. 249-263, 2017.
[46] A. Tajalli, N. Sedigh, and S.-A. Hosseini-Seno, "A Replication Dilemma Game for Cooperative Data Replication in Ad Hoc Networks," *Proc. Int. Conf. Computer and Knowledge Engineering*, pp. 177-182, 2016.
[47] D. Das, K. Majumder, and A. Dasgupta, "Selfish Node Detection and Low Cost Data Transmission in MANET using Game Theory," *Procedia Comput. Sci.*, vol. 54, pp. 92-101, 2015.
[48] S. Nobahary, H. Gharaee Garakani, A. Khademzadeh, and A. M. Rahmani, "Selfish Node Detection based on Hierarchical Game Theory in IoT," *EURASIP J. Wirel. Commun. Netw.*, vol. 2019, 2019.
[49] A. Sharah, M. Alhaj, and M. Hassan, "Selfish Dynamic Punishment Scheme: Misbehavior Detection in MANETs Using Cooperative Repeated Game," *Int. J. Comput. Sci. Netw. Secur.*, vol. 20, pp. 168-173, 2020.
[50] V. A. Siris and F. Papagalou, "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks," *Comput. Commun.*, vol. 29, pp. 1433-1442, 2006.
[51] G. J. Mailath, and L. Samuelson, *Repeated Games and Reputations: Long-run Relationships*, Oxford: Oxford university press, 2006.
[52] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO–Simulation of Urban Mobility: An Overview," *Proc. Int. Conf. Advances in System Simulation*, 2011.
[53] Ns-3.29, https://www.nsnam.org/releases/ns-3-29, September 2018.
[54] C. Perkins, E. Belding-Royer, and S. Das, "RFC3561: Ad Hoc On-demand Distance Vector (AODV) Routing," 2003, DOI: https://doi.org/10.17487/RFC3561.
[55] L. Yu-rui, "Application of Desired Utility Function Theory to Library Administration," *College Math.* , vol. 2, 2008.

The CSI Journal on Computing Science and Information Technology
Vol. 19, No.1, 2021

Detecting and Preventing Selfish Behavior of Mobile Ad Hoc Network Nodes using Game Theory

Gholamreza Farahani[1]

[1] Department of Electrical Engineering and Information Technology, Iranian Research Organization for Science and Technology (IROST), Tehran, Iran

Abstract

One of the problems in the mobile ad hoc network is identifying selfish nodes and preventing their selfish behavior. In this paper, a new algorithm called DMS is proposed that can effectively detect selfish nodes and transfer the packet only through the path with the highest weight function from the source node to the destination node. In DMS, the selfish behavior of nodes is detected in the first phase by combining packet receiving and sending rate and modified adaptive threshold algorithms. In the second phase, selfish behavior is prevented by using repeated games theory. The simulation results show the performance improvement of the proposed method compared to other methods in packet delivery ratio, end-to-end delay, packet loss ratio, and throughput. The packet delivery ratio in the DMS method has increased by 49.82%, 39.98%, 71.43%, 24%, and 11.57% compared to WSISB, LTCF, RDG, HGT, and CRG, respectively. This improvement in throughput compared to WSISB, LTCF, RDG, HGT, and CRG is 37.74%, 39.95%, 48.40%, 21.65%, and 10.89% respectively. DMS also reduces end-to-end delay and packet loss ratio compared to other methods.

Keywords: Game Theory; Selfish Node; Selfish Behavior; Mobile Ad Hoc Network; Repeated Games Theory.