یک رویکرد مسیریابی مبتنی بر اعتماد و انرژی–آگاه در شبکه‌های حسگر بی‌سیم با استفاده از الگوریتم ODMA

مریم حاجی‌بی[۱]، مهدی فرتاش[۲،*] و نفیسه اوسطی عراقی[۲]

اطلاعات مقاله

دریافت مقاله: ۱۳۹۹/۱۲/۱۸

پذیرش مقاله: ۱۴۰۰/۰۳/۰۲

واژگان کلیدی:

شبکهٔ حسگر بی‌سیم،

اعتماد،

ثابت تحمل،

مسیریابی چند-مسیر،

انرژی-آگاه.

چکیده

تحوّلات سریع در زمینهٔ فنّاوری‌های رادیویی، ظهور گره‌های حسگر کوچکی را فراهم کرده که توانایی برقراری ارتباط در شبکه‌های حسگر بی‌سیم را دارند. گره‌ها در شبکه‌های حسگر بی‌سیم با همکاری یکدیگر و با استفاده از مسیریابی چند-پرشه اقدام به انتقال اطلاعات می‌کنند. این مشارکت باعث آسیب‌پذیری این نوع شبکه‌ها در مقابل بسیاری از حملات شده است. به‌منظور تشخیص قابلیت اطمینان گره‌ها در تفکیک گره‌های مخرّب از سایر گره‌ها باید یک طرح هوشمند مدیریت اعتماد به کار گرفته شود. در سال‌های اخیر، پروتکل‌های مسیریابی مبتنی بر اعتماد و انرژی-آگاه به ابزارهای مهمی برای افزایش امنیت و کارایی شبکه‌های حسگر بی‌سیم تبدیل شده است. در این مقاله یک الگوریتم مسیریابی مبتنی بر اعتماد و انرژی-آگاه براساس یک تابع برازندگی ترکیبی جدید پیشنهاد شده است. این الگوریتم دو جنبهٔ اساسی دارد: یکی، انتخاب گره‌های ایمن براساس ثابت تحمل و دیگری، انتخاب مناسب‌ترین گره‌ها از بین گره‌های ایمن برای انجام مسیریابی. الگوریتم پیشنهادی از تکنیک مسیریابی چند-مسیر همراه با یک مکانیزم ارتباطی چند-پرشه درون‌خوشه‌ای و برون‌خوشه‌ای استفاده می‌کند، جایی که خوشه‌بندی با الگوریتم ODMA انجام می‌شود. علاوه بر این، مسیر بهینه و ایمن براساس یک تابع برازندگی ترکیبی با پارامترهای انرژی، اعتماد، کیفیت سرویس، اتصال، فاصله، تعداد-پرش و ترافیک شبکه انتخاب می‌شود. شبیه‌سازی براساس معیارهای ارزیابی مختلف در حضور حمله منع سرویس انجام شده است. نتایج آزمایش‌ها نشان می‌دهد معیارهای ارزیابی در الگوریتم پیشنهادی نسبت به سایر الگوریتم‌های مسیریابی ایمن، بهبود یافته است.

۱- مقدمه

معماری شبکه‌های حسگر بی‌سیم براساس همکاری گره‌های حسگر کوچک ساخته شده است. هر گره دارای یک باتری است که ظرفیت انرژی آن را نشان می‌دهد. در این شبکه‌ها گره‌های حسگر داده‌های جمع‌آوری‌شده را از طریق گره‌های میانی و پیوندهای بی‌سیم مسیریابی می‌کنند تا داده‌ها را به سینک ارسال نمایند [۱]. بنابراین یک پروتکل مسیریابی مناسب برای انتقال داده‌ها به گره سینک ضروری است [۲]. شبکه‌های حسگر بی‌سیم کاربردهای گسترده‌ای در زمینه‌های صنعت، نظارت بر محیط، نظارت بر سلامت، نظامی و غیره دارند، با این حال، این شبکه‌ها از نظر قدرت محاسباتی، انرژی محدود و امنیت رنج می‌برند [۳]. خوشه‌بندی گره‌ها، انتخاب سرخوشه‌ها و انجام مسیریابی از طریق آن‌ها می‌تواند تعداد گره‌های شرکت‌کننده در مسیر را کاهش داده، درنتیجه منجر به کاهش مصرف انرژی شود [۴].

* پست الکترونیک نویسنده مسئول: m-fartash@iau-arak.ac.ir

۱. دانشجوی دکتری، گروه مهندسی کامپیوتر، واحد اراک، دانشگاه آزاد اسلامی، اراک، ایران

۲. استادیار، گروه مهندسی کامپیوتر، واحد اراک، دانشگاه آزاد اسلامی، اراک، ایران

در مسیریابی مبتنی برخوشه‌بندی، سرخوشه داده‌ها را از گره‌های عضو دریافت می‌کند و سپس داده‌ها را از طریق مسیریابی تک-پرشه یا چند-پرشه به سینک انتقال می‌دهد [۵]. مسیریابی چند-پرشه فرصتی برای گره‌ها فراهم می‌کند تا فعالیت‌های مخرّب موجود در شبکه‌های حسگر بی‌سیم را کنترل کنند. بنابراین توسعهٔ این شبکه‌ها براساس انرژی و اعتماد ضروری است.

امنیت داده‌ها و شناسایی گره‌های مخرّب در شبکه‌های حسگر بی‌سیم با استفاده از مدل اعتماد در بسیاری از مقالات مورد توجه قرار گرفته است [۶-۹]. در سال‌های اخیر، مسیریابی فرصت‌طلبانه[1] یکی از فنّاوری‌هایی است که برای تأمین امنیت شبکه‌های حسگر بی‌سیم محبوبیت یافته است [۱۰]. مسیریابی فرصت‌طلبانه به‌طور مؤثر پیوندهای ضعیف را به‌عنوان پیوندهای قوی متحد کرده، از مزایای زیادی نسبت به انتقال سنّتی بهره می‌برد [۱۱]. در تحقیقات متعددی از الگوریتم‌های مبتنی بر اعتماد برای شناسایی گره‌های مخرّب استفاده شده است، با این حال، چالش‌های موجود در خوشه‌بندی، مسیریابی و تشخیص گره‌های مهاجم هنوز هم نیاز به پیشرفت دارند.

پارامترهای حائز اهمیت در شبکه‌های حسگر بی‌سیم شامل طول عمر شبکه، تعداد بسته‌های ارسال‌شده و انرژی است که باید بهبود یابند. با توجه به احتمال حملات گره‌های مخرّب، استراتژی مسیریابی مبتنی بر مدل اعتماد و فرصت، یک روش مؤثر و محبوب در شبکه‌های حسگر بی‌سیم است. از این رو، در این مقاله یک الگوریتم مسیریابی مبتنی بر اعتماد و انرژی-آگاه براساس تکنیک مسیریابی چند-مسیر پیشنهاد شده است، جایی که بهترین مسیر براساس یک تابع برازندگی ترکیبی جدید انتخاب می‌شود. برای کار خوشه‌بندی، از الگوریتم ODMA[2] استفاده شده است. استفاده از الگوریتم‌های بهینه‌سازی برای خوشه‌بندی گره های حسگر در تحقیقات مختلف توصیه گردیده است [۱۲ و ۱۳]. در این میان، الگوریتم ODMA با الهام از مدل توسعه باز و جوامع از مزایای دو الگوریتم ازدحام ذرّات و تکاملی بهره می‌برد و دارای پارامترهای زیادی به‌منظور کنترل جست‌وجو در فضاهای بزرگ است.

ادامهٔ مقاله به شرح زیر سازماندهی شده است: بخش ۲ بررسی ادبیات را شرح می‌دهد. در بخش ۳ توپولوژی شبکهٔ مورد استفاده بحث شده است. بخش ۴ الگوریتم مسیریابی مبتنی بر اعتماد و انرژی-آگاه پیشنهادی را توضیح می‌دهد. بخش ۵ نتایج حاصل از شبیه‌سازی را به تصویر می‌کشد و درنهایت، بخش ۶ نتیجه‌گیری و کارهای آینده را ارائه می‌دهد.

۲- کارهای مرتبط

در ادبیات گذشته، بسیاری از پروتکل‌های مسیریابی برای بهبود کیفیت سرویس[3] (QoS) با هدف افزایش اعتماد و کاهش مصرف انرژی ارائه شده است [۱۲-۱۴]. در این میان، الگوریتم QEER[4] یکی از تحقیقات برجسته در این زمینه است [۱۲]. این الگوریتم بیشتر روی معیارهای کیفیت سرویس متمرکز شده است و قابلیت اطمینان را نسبت به تأخیر و امنیت نادیده می‌گیرد. کالیدوس و همکاران [۱۳] یک الگوریتم مسیریابی مبتنی بر کیفیت سرویس کارآمد با احراز هویت و مدل‌سازی اعتماد مبتنی بر کلید به‌منظور افزایش قابلیت اطمینان ارتباطات ارائه دادند. این پروتکل برای انجام مسیریابی کارآمد انرژی کیفیت سرویس آگاه ایمن[5] (SQEER) با بهبود پروتکل QEER توسعه یافته است. این پروتکل براساس مسیریابی مؤثر مبتنی بر خوشه‌بندی ارائه شده است، جایی که گره های سرخوشه با محدودیت‌های امنیتی بالا برای فراهم سازی پروتکل مسیریابی ایمن و مؤثر انتخاب می‌شوند.

در این راستا، بسیاری از محققان پروتکل‌های کارآمد انرژی را با استفاده از مدل‌های مختلف نظیر مسیریابی مبتنی بر خوشه‌بندی ارائه دادند [۱۵-۱۷]. تانگراج و سلوی [۱۵] یک پروتکل مسیریابی کارآمد و ایمن براساس مکانیزم‌های خوشه‌بندی پویا مبتنی بر نسبت سیگنال به نویز ارائه دادند. در اینجا فرایند بازیابی خطا در مسیریابی مبتنی بر خوشه بندی در نظر گرفته شده است.

بسیاری از محققان روی توسعهٔ پروتکل‌های مسیریابی ایمن کار کردند و بسیاری از این پروتکل‌ها در ادبیات موجود است [۱۸-۲۰]. زاهدی و پارما [۱۸] یک الگوریتم مسیریابی به‌عنوان رویکرد جست‌وجوی گرانشی مبتنی بر اعتماد[6] (ETGSA) برای شبکه‌های حسگر بی‌سیم ارائه دادند. این

[1] Opportunistic Routing
[2] Open source Development Model Algorithm
[3] Quality of Service
[4] QoS aware Energy Efficient Routing
[5] Secured QoS aware Energy Efficient Routing
[6] Energy-aware Trust-based Gravitational Search Approach

الگوریتم با در نظر گرفتن اعتماد مستقیم و اعتماد غیرمستقیم گره‌ها و همچنین مسئلهٔ صرفه‌جویی در مصرف انرژی، پارامترهای مسیریابی را با رویکرد جست‌وجوی گرانشی بهینه می‌کند. در این الگوریتم، مسیر بهینه براساس تعداد-پرش، انرژی، نرخ ترافیک مسیرها و اعتماد انتخاب می‌شود. با این حال، این رویکرد برای مسیریابی مبتنی بر خوشه‌بندی در شبکه‌های حسگر بی‌سیم با دو یا چند گره سینک کارایی ندارد.

پاتیل و همکاران [۱۹] یک چارچوب مسیریابی مبتنی بر اعتماد و فرصت در شبکه‌های حسگر بی‌سیم با استفاده از الگوریتم بهینه‌سازی ترکیبی پیشنهاد دادند. این الگوریتم به‌عنوان ازدحام گربه- سلطنتی[1] (M-CSO) معرفی شده که ترکیبی از بهینه‌سازی پروانه-سلطنتی و بهینه‌سازی ازدحام گربه است. این چارچوب دو جنبهٔ اساسی شامل انتخاب گره‌های ایمن و انتخاب گره‌های فرصت‌طلب از بین گره‌های ایمن دارد. شلکه و همکاران [۲۱] یک پروتکل مسیریابی فرصت‌طلبانه ازدحام-آگاه برای حداقل‌سازی ترافیک شبکه و دستیابی به عملکرد پایدار ارائه دادند. با این حال، این روش فاقد استراتژی زمان‌بندی خواب-بیدار برای کاهش مصرف انرژی و تأخیر است.

در [۲۹] یک طرح اعتماد فعال برای مسیریابی در WSN مدل‌سازی شده است. این طرح درجهٔ امنیت بیشتر، احتمال مسیریابی موفق، مقیاس‌پذیری و بهره‌وری انرژی بهتری را ارائه می‌دهد. مشکل این طرح، حصول اعتماد با مصرف انرژی بالاست که بر طول عمر شبکه و یافتن گره‌های مخرّب تأثیر می‌گذارد. در [۳۰] یک الگوریتم بهینه‌سازی کلونی مورچه برای مسیریابی ایمن[2] (ACOSR) مدل‌سازی شده است. این الگوریتم تلفات بسته و مصرف انرژی را کاهش داده، مسیری کاملاً ایمن را در WSN فراهم می‌کند. با این حال، این الگوریتم فاقد ارزیابی گره‌ها در وضعیت پیچیده حملات است. به‌طور کلی، نوآوری این تحقیق و تفاوت آن با کارهای موجود به شرح زیر است: ۱. خوشه‌بندی گره‌ها با الگوریتم ODMA؛ ۲. بهبود مسیریابی براساس یک تابع برازندگی ترکیبی؛ ۳. استفاده از تکنیک مسیرهای چند-مسیر برای انتقال داده‌ها برپایهٔ یک مکانیزم ارتباطی چند-پرشه درون‌خوشه‌ای و برون‌خوشه‌ای.

۳- توپولوژی شبکه

در این مقاله، توپولوژی شبکهٔ مورد استفاده از سه نوع گره شامل حسگر معمولی، حمله‌کننده و سینک تشکیل شده است. گره‌های حسگر معمولی وظیفهٔ جمع‌آوری داده‌ها از محیط و ارسال آن به گره سینک را برعهده دارند. نوع حمله منع سرویس[3] (DoS) برای آزمایش امنیت شبکه در نظر گرفته شده است [۱۸]. برد رادیویی همهٔ گره‌های شبکه برابر فرض شده است. همچنین گره‌ها مجهّز به GPS[4] بوده، از قابلیت گزارش موقعیت خود به سینک برخوردار هستند. گره‌ها در دو حالت ثابت و متحرّک (براساس مدل نقطه تصادفی) شبیه‌سازی می‌شوند. علاوه بر این، رفتار گره‌های همسایه براساس بسته‌های ارسالی و دریافتی کنترل می‌گردد.

۴- طرح پیشنهادی

در این مقاله برای بهبود امنیت در شبکه‌های حسگر بی سیم، یک الگوریتم مسیریابی مبتنی بر اعتماد و انرژی-آگاه پیشنهاد شده است. الگوریتم پیشنهادی برپایهٔ پروتکل مسیریابی AODV[5] [۱۸] توسعه یافته، از تکنیک مسیریابی چند-مسیر استفاده می‌کند. مسیریابی چند-مسیر به مفهوم ایجاد بیش از یک مسیر بین مبدأ و مقصد است. این الگوریتم در دو گام اصلی اعمال می‌گردد. اولین گام بر انتخاب گره‌های ایمن از میان گره‌های اولیه متمرکز است. گره‌های ایمن انتخاب‌شده به گام دوم منتقل و براساس آن‌ها مسیریابی انجام می‌شود. در اینجا گره‌های ایمن با استفاده از ثابت تحمل تعیین شده، فرایند مسیریابی از میان این گره‌ها برپایهٔ یک تابع برازندگی ترکیبی انجام می‌گیرد. به‌طور کلی، خوشه‌بندی گره‌ها در شبکه‌های حسگر بی‌سیم یک تکنیک اصلی برای کاهش مصرف انرژی حسگرهاست که طول عمر شبکه را افزایش می‌دهد. از آنجا که گره‌های حسگر به‌راحتی مستعد حملات امنیتی هستند، برای انتخاب ایمن سرخوشه‌ها به یک روش خوشه‌بندی کارآمد نیاز است. برای دستیابی به این هدف، از معیار ثابت تحمل برای انتخاب سرخوشه‌های قابل اعتماد، همراه با الگوریتم ODMA برای کار برای خوشه‌بندی استفاده می شود.

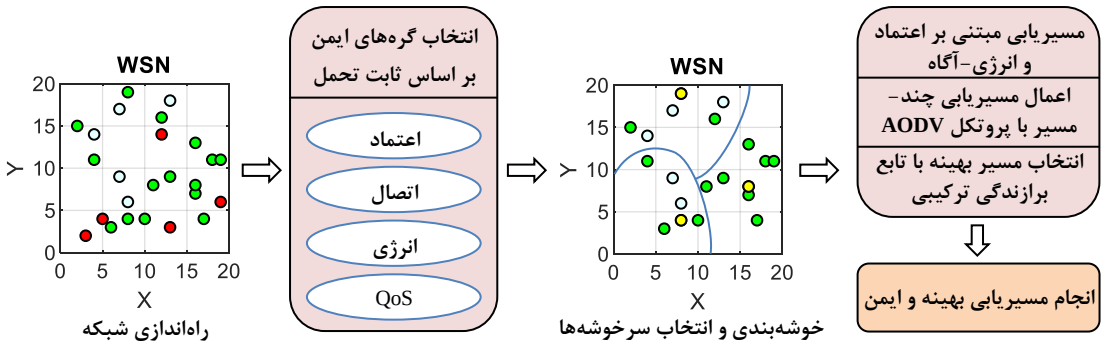
شکل (۱) معماری الگوریتم پیشنهادی را نشان می‌دهد،

[1] Monarch-Cat Swarm Optimization
[2] Ant colony optimization algorithm for secured routing
[3] Denial of Service
[4] *Global Positioning System*
[5] Ad-hoc On-demand Distance Vector

جایی که نوآوری این تحقیق در بخش‌های خوشه‌بندی و انتخاب سرخوشه، تابع برازندگی و مسیریابی است.

۴-۱- راه‌اندازی شبکه

پس از استقرار گره‌ها و تعیین انرژی اولیهٔ آن‌ها، سینک یک بستهٔ سلام در شبکه پخش می‌کند. همهٔ گره‌هایی که بسته را دریافت کردند، حضور خود را با ارسال یک بسته به سینک اعلام می‌کنند. گره‌ها در شکاف‌های زمانی مشخص بستهٔ سلام را در شبکه پخش می‌کنند. در این بسته، یک گره علاوه بر اعلام حضور خود به سایر گره‌ها، انرژی و اعتماد خود را نیز به گره‌های همسایه اعلام می‌نماید.



شکل ۱- معماری الگوریتم مسیریابی پیشنهادی

پارامتر اعتماد برای تخمین اعتماد غیرمستقیم گره‌ها استفاده می‌شود. علاوه بر این، از پارامتر انرژی برای محاسبهٔ اعتماد مستقیم استفاده می‌شود. در اینجا گره‌هایی که بستهٔ سلام را دریافت می‌کنند، این دو پارامتر را در جدول همسایگی خود ذخیره می‌نمایند.

در اغلب پروتکل‌های کلاسیک، جدول مسیریابی فقط شامل پارامتر تعداد-پرش برای انتخاب بهترین مسیر است؛ اما در الگوریتم پیشنهادی به‌ازای هر مسیر کشف‌شده به مقصد، پارامترهای طول عمر، انرژی، اعتماد، کیفیت سرویس، اتصال، فاصله، تعداد-پرش و ترافیک شبکه در جدول مسیریابی ذخیره می‌شود. با توجه به این پارامترها ارجاع های متعدد به جدول کاهش یافته، مسیر بهینه با سرعت بالاتری انتخاب می‌شود.

۴-۲- انتخاب گره‌های ایمن با استفاده از ثابت تحمل

در این مقاله گره‌های قابل اعتماد با استفاده از ثابت تحمل تعیین شده، فرایند مسیریابی براساس آن‌ها انجام می‌شود. ثابت تحمل برای انتخاب گره‌های ایمن مدل‌سازی شده تا امنیت مؤثر را در شبکه فراهم کند. TC_j ثابت تحمل برای گره j-ام است که طبق رابطهٔ (۱) تعریف می‌شود.

$$TC_j = \frac{1}{4}\left[T_j + C_j + E_j + QoS_j\right] \qquad (۱)$$

T_j، C_j، E_j و QoS_j به‌ترتیب به اعتماد، اتصال، نرخ انرژی و کیفیت سرویس گره j-ام اشاره دارند. این رابطه ارزشی را برای یک گره محاسبه می‌کند که این ارزش نشان می‌دهد چقدر احتمال دارد این گره مورد حمله قرار گرفته باشد. با توجه به تفاوت میان محدودهٔ پارامترها، همهٔ پارامترها با تقسیم بر بزرگ‌ترین مقدار نرمال می‌شوند.

در اینجا گره‌های ایمن براساس یک حد آستانه انتخاب می شود. بنابراین اگر TC_j بزرگ‌تر از آستانه باشد، گره j-ام یک گره ایمن است، در غیر این صورت، به‌عنوان گره مخرّب شناسایی می‌شود.

نمرهٔ اعتماد گره j-ام به‌صورت مجموع وزنی نمره‌های اعتماد مستقیم و غیرمستقیم تعریف می‌شود. رابطهٔ (۲) نمرهٔ اعتماد گره j-ام را تعریف می‌کند.

$$T_j = \alpha.DT_j + (1-\alpha).IT_j \qquad (۲)$$

DT_j و IT_j به‌ترتیب به نمرهٔ اعتماد مستقیم و اعتماد غیرمستقیم برای گره j-ام اشاره دارند. α ضریب وزن برای در نظر گرفتن تأثیر این پارامترها در محاسبهٔ نمرهٔ اعتماد نهایی است.

اعتماد مستقیم برای گره j-ام به‌صورت رابطهٔ (۳) محاسبه می‌شود.

$$DT_j = \beta.e_j + (1-\beta).\frac{nc_j}{nt_j} \qquad (۳)$$

e_j به انرژی باقیماندهٔ گره j-ام اشاره دارد. nc_j و nt_j به‌ترتیب تعداد بسته‌های صحیح ارسال‌شده و تعداد کل بسته‌های ارسال‌شده توسط گره j-ام است. β ضریب وزنی برای اعمال تأثیر این پارامترهاست.

اعتماد غیرمستقیم برای گره j با توجه به داده‌های موجود

در جدول همسایگی به‌صورت رابطهٔ (۴) محاسبه می‌شود.

$$IT_j = \frac{\sum_{k \in nn_j} T_k^j + T_k}{|nn_j|} \quad (۴)$$

T_k^j اعتماد توصیه‌شده از گره k-ام به گره j-ام است و براساس نسبت تعداد تراکنش‌های موفق به تعداد کل گره‌ها محاسبه می‌شود. T_k نمرهٔ اعتماد گره k-ام است و nn_j و $|nn_j|$ به‌ترتیب به مجموعه گره‌های همسایه و تعداد آن‌ها اشاره دارند.

اتصال گره j-ام (C_j) بین سایر گره‌های شبکه، مطابق رابطهٔ (۵) محاسبه می‌شود.

$$C_j = \frac{|nn_j|}{L} \quad (۵)$$

L تعداد کل اتصالات شبکه را نشان می‌دهد. بنابراین تعداد پیوندهای بیشتر به همسایه‌ها برای یک گره بیانگر تأثیر بیشتر آن در شبکه است.

پارامتر نرخ انرژی برای گره j-ام (E_j) براساس میزان مصرف انرژی گره j-ام، بیشترین انرژی موجود در شبکه و همچنین انرژی اولیهٔ گره‌ها تعریف می‌شود. بر این اساس، E_j با رابطهٔ (۶) محاسبه می‌شود.

$$E_j = E_0 - [e_{max} - e_j] \quad (۶)$$

E_0 انرژی اولیهٔ گره‌ها، e_{max} بیشترین انرژی موجود در شبکه و e_j انرژی مربوط به گره j-ام است.

حداکثر کیفیت سرویس براساس حداکثر طول عمر پیوند و حداقل تأخیر در گره‌های شبکه اندازه‌گیری می‌شود [۱۹]. رابطهٔ (۷) محاسبهٔ کیفیت سرویس را برای گره j-ام نشان می‌دهد.

$$QoS_j = LLT_j + d_j \quad (۷)$$

LLT_j طول عمر پیوند مربوط به گره j-ام و d_j تأخیر مربوط به گره j-ام در فرایند انتقال است. d_j براساس نسبت تعداد گره‌های موجود در یک مسیر خاص به کل گره‌های موجود در شبکه اندازه‌گیری می‌شود. همچنین LLT_j براساس تحرّک گره‌ها، جهت حرکت گره‌ها و مختصات گره ها طبق رابطهٔ (۸) محاسبه می‌شود.

$$LLT_j = \frac{-(AB + CD) + \sqrt{(B^2 + C^2).V^2 - (AD - CB)}}{(B^2 + C^2)} \quad (۸)$$

V دامنهٔ انتقال است و A، B، C و D طبق رابطهٔ (۹) بیان می‌شوند.

$$\begin{cases} A = S_k.sin\,\varphi_k - S_j.sin\,\varphi_j \\ B = x_k - x_j \\ C = S_k.cos\,\varphi_k - S_j.cos\,\varphi_j \\ D = y_k - y_j \end{cases} \quad (۹)$$

S_k سرعت تحرّک گره k-ام، S_j سرعت تحرّک گره j-ام، φ_k جهت حرکت گره k-ام و φ_j جهت حرکت گره j-ام است. (x_k, y_k) و (x_j, y_j) نیز به‌ترتیب مختصات گره‌های k و j هستند. در اینجا LLT_j به‌ازای میانگین برای همه $k \in nn_j$ محاسبه می‌شود.

۴-۳- خوشه‌بندی و انتخاب سرخوشه‌ها

خوشه‌بندی گره‌ها، انتخاب سرخوشه‌ها و انجام مسیریابی از طریق سرخوشه‌ها می‌تواند تعداد گره‌های شرکت‌کننده در مسیر را کاهش دهد و درنتیجه منجر به کاهش مصرف انرژی شود. برای خوشه‌بندی گره‌ها الگوریتم‌های مختلفی وجود دارد که می‌تواند مورد استفاده قرار گیرد [۲۲]. در این میان، الگوریتم‌های تکاملی مبتنی بر جمعیت برای خوشه‌بندی بسیار محبوب هستند [۲۳].

در اینجا از الگوریتم مدل توسعه متن باز (ODMA) [۲۴] برای خوشه‌بندی و یافتن تعداد خوشه‌های بهینه (K) استفاده می‌شود. در ODMA هر راه‌حل با عنوان یک نرم افزار شناخته شده، کار بهینه‌سازی با ارتقای نرم‌افزارها انجام می‌شود. نرم‌افزارها در طول زمان، تکامل و توسعه می‌یابند و برخی نیز منسوخ می‌شوند. هر نرم‌افزار در مسئلهٔ حاضر یک خوشه‌بندی از گره‌ها ارائه می‌دهد. در این تحقیق، کدگذاری نرم‌افزارها به‌صورت یک بردار از اعداد حقیقی به طول تعداد گره‌های شبکه ارائه می‌شود که هر عنصر شمارهٔ خوشهٔ گره متناظر با آن را نشان می‌دهد. پس از مشخص شدن ساختار نرم‌افزارها، جمعیت اولیه به‌صورت تصادفی ایجاد می‌شود.

هدف ODMA توزیع مناسب تعداد گره‌های کاندیدا در خوشه‌بندی است. گره‌هایی از خوشه k-ام که در برد رادیویی همهٔ اعضای این خوشه باشند، می‌توانند داده‌ها را به‌صورت تک-پرشه دریافت کنند. این گره‌ها به‌عنوان گره های کاندیدای سرخوشه شناخته و با Δ_k نشان داده می شوند. در اینجا باید Γ گره از هر خوشه دارای فاصله (برد رادیویی) کمتر با تمام گره‌های آن خوشه باشد. با توجه به متغیّر بودن تعداد اعضای هر خوشه، Γ به‌صورت $\theta.n_k$ تعریف می‌شود که n_k تعداد اعضای خوشه k-ام و θ حد آستانه برای تعیین تعداد گره‌های کاندیداست. در این مقاله

از یک تابع هدف ترکیبی شامل فاصله، انرژی و گره‌های کاندیدا به‌منظور تعیین کیفیت خوشه‌بندی استفاده شده، همان طور که در رابطهٔ (۱۰) نشان داده شده است.

$$Fitness = \sum_{k=1}^{K}\left[(\Delta_k - \theta.n_k) + \sum_{j=1}^{n_k}\frac{e_j}{d_{j,v_k}}\right] \qquad (۱۰)$$

در این رابطه، e_j انرژی گره j-ام و d_{j,v_k} فاصلهٔ گره j-ام از مرکز خوشه k-ام است.

مطابق ODMA، راه‌حل‌ها برمبنای مقدار تابع هدف مرتب سازی صعودی می‌شوند. سپس z راه‌حل با بالاترین تابع هدف به‌عنوان راه‌حل‌های پیشرو انتخاب می‌شوند، جایی که سایر راه‌حل‌ها امیدبخش هستند. به‌طور کلی مراحل تکامل ODMA به‌صورت زیر است: ۱. حرکت راه‌حل‌ها به‌سمت راه‌حل‌های پیشرو؛ ۲. بهبود راه‌حل‌های پیشرو براساس سابقهٔ خود؛ ۳. انشعاب از راه‌حل‌های پیشرو و ایجاد راه‌حل‌های جدید.

در مرحلهٔ اول راه‌حل‌های امیدبخش براساس راه‌حل‌های پیشرو توسعه می‌یابند. برای این کار به‌ازای هر راه‌حل امیدبخش، یک راه‌حل پیشرو براساس تابع هدف انتخاب و فرایند تکامل انجام می‌شود. در اینجا مفهوم تکامل با تعریف یک متغیّر احتمالی بیان می‌شود که هر عنصر از راه‌حل امیدبخش با احتمال ρ با توجه به راه‌حل پیشرو تغییر می کند. احتمال $\rho = 1$ باعث می‌شود راه‌حل امیدبخش کاملاً شبیه راه‌حل پیشرو شود و احتمال $\rho = 0$ موجب می‌گردد هیچ تغییری در راه‌حل امیدبخش انجام نگیرد. شکل (۲) مثالی از این فرایند را نشان می‌دهد. در اینجا خوشه‌های مربوط به گره‌های ۲، ۶ و ۷ براساس احتمال ρ تغییر کرده اند. بنابراین احتمال برای عناصر برجسته در این شکل برقرار شده و محتوای آن‌ها براساس محتوای راه‌حل پیشرو به‌روز است.

راه‌حل امیدبخش قبل از تکامل

۳	۱	۱	۲	۳	۳	۲	۱	۳	۱

راه‌حل پیشرو

۱	۲	۱	۳	۳	۲	۳	۳	۱	۲

راه‌حل امیدبخش بعد از تمامل

۳	۲	۱	۲	۳	۲	۳	۱	۳	۱

شکل ۲- تکامل راه‌حل امیدبخش براساس راه‌حل پیشرو

در مرحلهٔ دوم راه‌حل‌های پیشرو براساس سابقهٔ خود تکامل می‌یابند. در اینجا تکامل براساس موقعیت جاری (s_{cur}) و آخرین موقعیت (s_{old}) راه‌حل پیشرو انجام می‌شود. از این رو s_{new} موقعیت جدید راه‌حل پیشرو است و به‌صورت رابطهٔ (۱۱) تعریف می‌شود.

$$s_{new,q} = \left\|\frac{(s_{cur,q} + s_{old,q})}{2}\right\| + R, \quad \forall q = 1,2,\dots,N \qquad (۱۱)$$

در این رابطه، R یک عدد تصادفی در بازهٔ $[-1,+1]$ برای جست‌وجوی همسایگی است و $\|*\|$ یک تابع گرد کردن عدد است.

در مرحله سوم از راه‌حل‌های پیشرو راه‌حل‌های جدیدی تولید می‌شود. در اینجا تعدادی راه‌حل ضعیف با حداقل پیشرفت (کمترین تابع هدف) حذف شده، به‌جای آن‌ها راه‌حل‌های جدیدی تولید می‌شود. رابطهٔ (۱۲) فرایند تولید یک راه‌حل جدید را از یک راه‌حل پیشرو (s_L) نشان می دهد.

$$s_{new,q} = s_{L,q} + R \quad \forall q = 1,2,\dots,N \qquad (۱۲)$$

در اینجا برای هر مرحله محدودیت شمارهٔ خوشه‌ها از ۱ تا K اعمال می‌گردد.

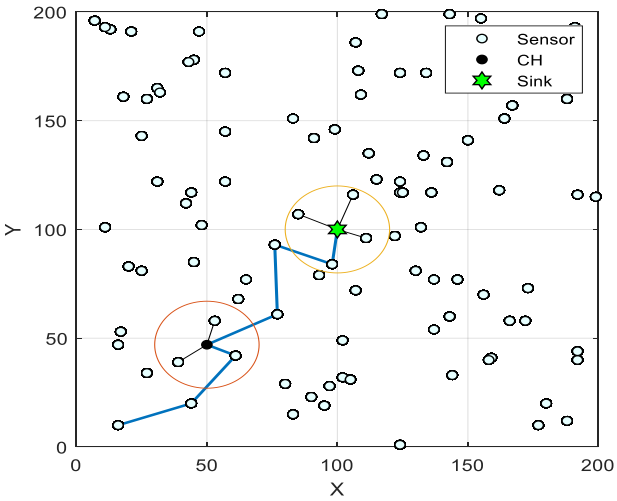
پس از ایجاد خوشه‌ها، سرخوشه‌ها براساس بالاترین ثابت تحمل از میان گره‌های کاندیدا انتخاب می‌شوند. درنهایت این گره‌ها سرخوشه شدن خود را به گره‌های همسایه با ارسال یک بسته سلام اطلاع می‌دهد. به‌طور کلی، به‌روزرسانی خوشه‌بندی و همچنین سرخوشه‌ها می‌تواند کارایی کلی سیستم را بهبود ببخشد؛ زیرا پارامترهای گره ها نظیر انرژی، فاصله، اعتماد و غیره در فرایند مسیریابی تغییر می‌کنند. انجام به‌روزرسانی پس از هر دور مسیریابی به‌دلیل ایجاد پیچیدگی محاسباتی امکان‌پذیر نیست. بنابراین در این مقاله خوشه‌بندی و انتخاب سرخوشه‌ها براساس یک حد آستانه به‌روزرسانی می‌شود.

۴-۴- الگوریتم مسیریابی پیشنهادی

مسیریابی توسط گره‌های مختلف براساس جدول زمان بندی TDMA[1] انجام می‌شود. در این مطالعه محتویات این جدول به‌صورت تصادفی در نظر گرفته شده است [۲۵]. در مسیریابی مبتنی بر خوشه‌بندی، سرخوشه داده‌ها را از گره‌های عضو خود جمع‌آوری و تجمیع می‌کند.

[1] Time Division Multiple Access

سپس داده‌ها را از طریق مسیریابی تک-پرشه یا چند-پرشه به سینک انتقال می‌دهد. در این مقاله، مسیریابی با استفاده از یک تکنیک ارتباطی چند-پرشه درون‌خوشه‌ای و برون‌خوشه‌ای براساس یک حد آستانه انجام می‌شود. اگر فاصلهٔ گره مبدأ از سرخوشه بزرگ‌تر از حد آستانه باشد، گره مبدأ مناسب‌ترین گره دیگر را برای انتقال داده‌ها به سرخوشه انتخاب می‌کند. به همین ترتیب، اگر فاصلهٔ سرخوشه از سینک بیشتر از حد آستانه باشد، از یک مسیر چند-پرشه برای ارسال داده‌ها استفاده می‌شود. در اینجا حد آستانه برابر برد رادیویی گره‌ها در نظر گرفته شده است. شکل (۳) ساختار کلی تکنیک ارتباطی چند-پرشه درون‌خوشه‌ای و برون‌خوشه‌ای پیشنهادی را نشان می‌دهد.



شکل ۳- ساختار کلی تکنیک ارتباطی پیشنهادی

هدف اصلی از توسعهٔ الگوریتم مسیریابی پیشنهادی، ایجاد مسیر مطمئن برای انتقال بسته‌ها از مبدأ به سرخوشه و همچنین از سرخوشه به سینک در حالت چند-پرشه است. یکی از پروتکل‌های اصلی مسیریابی در شبکه‌های حسگر بی‌سیم، AODV است [۲۶]. در این مقاله، این پروتکل به عنوان پروتکل مسیریابی پایه استفاده می‌شود. این پروتکل از بسته‌های کنترلی درخواست مسیر، پاسخ مسیر و خطای مسیر برای تعیین بهترین مسیر استفاده می‌کند. بسته‌های درخواست مسیر و پاسخ مسیر به‌ترتیب برای نشان دادن تعداد توالی مقصد و تعداد پرش‌ها در مسیر است. در فرایند جست‌وجوی مسیر در AODV، ابتدا بسته درخواست مسیر توسط گره مبدأ برای همسایه‌های خود ارسال می شود. هر گره میانی که مسیر معتبری به گره مقصد داشته باشد، گره مبدأ را با ارسال یک بسته پاسخ مسیر آگاه می سازد. اگر مسیر معتبری وجود نداشته باشد، گره میانی بسته درخواست مسیر را برای همسایه‌های خود ارسال می کند. این فرایند تا زمانی که بسته درخواست مسیر به مقصد یا یک گره با یک مسیر معتبر به مقصد برسد، تکرار می شود.

الگوریتم مسیریابی پیشنهادی مبتنی بر اعتماد و انرژی آگاه است و تنها از گره‌های ایمن در مسیریابی استفاده می‌کند. بنابراین بسته‌های درخواست مسیر را تنها به گره‌های همسایه ایمن ارسال می‌کند. علاوه بر این، الگوریتم پیشنهادی از تکنیک مسیریابی چند-مسیر استفاده می‌کند. در این تکنیک، بسته‌های درخواست مسیر از چند مسیر به سمت مقصد حرکت می‌کنند. بنابراین مبدأ ممکن است بسته‌های پاسخ مسیر متعددی را دریافت کند که به مسیرهای مختلف اشاره دارد. در AODV کلاسیک، همواره کوتاه‌ترین مسیر در نظر گرفته می‌شود. با این حال، در الگوریتم پیشنهادی، همهٔ مسیرها در جدول مسیریابی ذخیره و بهترین مسیر انتخاب می‌شود.

به‌طور کلی، الگوریتم مسیریابی پیشنهادی بر بهبود قابلیت اطمینان پیوند و توان کلی سیستم متمرکز است. در اینجا انتخاب گره‌های مناسب برای مسیریابی براساس یک تابع برازندگی ترکیبی جدید با چند هدف انجام می‌شود. تابع برازندگی در الگوریتم پیشنهادی مطابق رابطهٔ (۱۳) برای انتخاب بهترین مسیر تعریف شده است.

$$Fitness = \frac{w_1.E + w_2.T + w_3.QoS + w_4.C}{w_5.D + w_6.HC + w_7.NT} \quad (۱۳)$$

E، T، QoS و C به‌ترتیب به انرژی، نمرهٔ اعتماد، کیفیت سرویس و اتصال بین گره‌های مسیر اشاره دارد که ارزش بهینهٔ آن‌ها باید حداکثر باشد. همچنین D، HC و NT

به‌ترتیب فاصله، تعداد-پرش و ترافیک مسیر است که ارزش بهینهٔ آن‌ها باید حداقل باشد. وزن‌های w_1 تا w_7 برای تعیین اثربخشی هر پارامتر در تابع برازندگی است.

۴-۵- شبه کد الگوریتم پیشنهادی

شکل (۴) شبه کد الگوریتم مسیریابی پیشنهادی را نشان می‌دهد.

الگوریتم مسیریابی مبتنی بر اعتماد و انرژی-آگاه

۱- شروع
۲- راه‌اندازی شبکه با N گره (شامل حسگر، حمله‌کننده و سینک) در یک محیط $M \times M$ متر
۳- محاسبهٔ ثابت تحمل برای گره‌ها براساس پارامترهای اعتماد، اتصال، انرژی و کیفیت سرویس
۴- شناسایی گره‌های ایمن براساس ثابت تحمل و یک مقدار آستانه
۵- خوشه‌بندی گره‌ها با الگوریتم ODMA و تعیین گره‌های کاندیدای سرخوشه
۶- تعیین سرخوشه‌ها براساس ثابت تحمل از میان گره‌های کاندیدا
۷- درخواست ارسال داده به سینک مطابق جدول زمان‌بندی TDMA
۸- اعمال مکانیزم ارتباطی چند-پرشه درون‌خوشه‌ای و برون‌خوشه‌ای برای ارسال بسته
۹- استفاده از پروتکل AODV برای شناسایی مسیرهای ایمن از مبدأ به سرخوشه و همچنین از سرخوشه به مقصد
۱۰- ذخیرهٔ همهٔ مسیرهای یافت‌شده توسط AODV در جدول مسیریابی
۱۱- محاسبهٔ برازندگی مسیرها براساس پارامترهای انرژی، اعتماد، کیفیت سرویس، اتصال، فاصله، تعداد-پرش و ترافیک شبکه
۱۲- تعیین مسیر بهینه، ایمن و فرصت‌طلب براساس مقادیر تابع برازندگی
۱۳- انتقال بسته از مبدأ به مقصد براساس مسیر انتخاب‌شده
۱۴- به‌روزرسانی خوشه‌بندی و سرخوشه‌ها براساس یک مقدار حد آستانه
۱۵- تکرار مراحل ۷ تا ۱۴ تا پایان زمان شبیه‌سازی
۱۶- پایان

شکل ۴- شبه کد الگوریتم مسیریابی پیشنهادی

۵- نتایج و بحث

در این بخش، یک مطالعهٔ تجربی برای ارزیابی و مقایسهٔ عملکرد الگوریتم مسیریابی پیشنهادی انجام می‌شود. همهٔ آزمایش‌ها روی پردازندهٔ اینتل ۷ هسته‌ای با ۳٫۰ گیگاهرتز و ۱۶ گیگابایت حافظه انجام شده است. علاوه بر این، نرم افزار متلب ۲۰۱۹ برای شبیه‌سازی استفاده می‌شود.

۵-۱- پارامترهای شبیه‌سازی

آزمایش‌ها در یک توپولوژی شبکهٔ حسگر بی‌سیم با پنج سناریو شامل ۲۰، ۴۰، ۶۰، ۸۰ و ۱۰۰ گره با موقعیت اولیهٔ تصادفی بررسی شده است. در هر سناریوها تعداد گره‌های مخرّب ۵٪ از کل گره‌های شبکه است. گره‌ها در این شبکه با ارتباط بی‌سیم در دامنهٔ ۲۰۰×۲۰۰ متر مربع پخش می شوند. در اینجا همهٔ گره‌ها با نمرهٔ اعتماد اولیه برابر ۰٫۵ راه اندازی می‌شوند. فاصلهٔ نمونه‌برداری از هر گره ۱۲ ثانیه و کل زمان اجرا شبیه‌سازی ۳۶۰۰ ثانیه است. این شبیه‌سازی برای انتقال بسته‌های داده با ۱۵۰۰ بایت و بسته‌های سلام با ۲۵ بایت با نوع ترافیک نرخ بیت ثابت اجرا می‌شود. در تمام آزمایش‌ها انرژی اولیهٔ گره‌ها ۵ ژول فرض شده است. گره سینک همواره در مرکز ناحیه قرار دارد. نرخ انتقال همهٔ گره‌ها ۱۵ متر در نظر گرفته شده است. در این مقاله مدل مصرف انرژی مطابق [۲۷ و ۲۸] است.

نتایج به‌دست‌آمده از روش پیشنهادی با الگوریتم‌های ETGSA [۱۸]، M-CSO [۱۹] و SQEER [۱۳] مقایسه می‌شود. همچنین الگوریتم پیشنهادی در حالت گره ثابت (ETR-FN) در مقایسه با حالت گره متحرّک (ETR-MN) تجزیه و تحلیل شده است. علاوه بر این، الگوریتم پیشنهادی با نسخه بدون اعتماد آن یعنی مسیریابی مبتنی بر انرژی-آگاه (ER) مقایسه شده است.

۵-۲- معیارهای ارزیابی

معیارهای مورد استفاده برای مقایسهٔ توان عملیاتی، نرخ تشخیص، انرژی نرخ تحویل بسته و طول عمر شبکه هستند. توان عملیاتی شبکه کل نرخ داده‌های منتقل‌شده از طریق شبکه در یک زمان خاص است و شناسایی دقیق گره‌های مهاجم بیانگر معیار نرخ تشخیص. معیار انرژی به مصرف انرژی گره‌های شبکه اشاره دارد. نرخ تحویل بسته مرتبط با تعداد بسته‌های داده‌ای است که به‌صورت موفقیت آمیز ارسال شده و طول عمر شبکه برابر تعداد دورهای مسیریابی موفق قبل از مرگ اولین گره است. یک الگوریتم

مسیریابی مؤثر به دنبال حداکثرسازی توان عملیاتی، نرخ تشخیص، انرژی، نرخ تحویل بسته و طول عمر شبکه است.

۵-۳- مدل مصرف انرژی

در این مقاله، مدل انرژی مورد استفاده مطابق [۲۷ و ۲۸] است. انرژی مورد نیاز برای ارسال بسته داده یک بیتی در فاصلهٔ d متر مطابق رابطهٔ (۱۴) محاسبه می‌شود.

$$E_T(l,d)=\begin{cases} l.E_{elec}+l.\varepsilon_{fs}.d^2, & d<d_0 \\ l.E_{elec}+l.\varepsilon_{mp}.d^4, & d\geq d_0 \end{cases} \quad (۱۴)$$

همچنین انرژی مورد نیاز برای دریافت بسته داده یک بیتی مطابق رابطهٔ (۱۵) است.

$$E_R(l,d)=l.E_{elec} \quad (۱۵)$$

E_{elec} انرژی لازم برای ارسال یا دریافت یک بیت داده، ε_{fs} انرژی آمپلی فایر در فضای آزاد و ε_{mp} انرژی تقویت‌کنندهٔ سیگنال در طول مسافت مورد نظر است. علاوه بر این، l طول بسته و d_0 یک حد آستانه برای ارسال بسته برمبنای فاصله است. معمولاً $d_0=\sqrt{\varepsilon_{fs}/\varepsilon_{mp}}$ در نظر گرفته می شود. جدول ۱ جزئیات پارامترهای مدل مصرف انرژی را در شبیه‌سازی نشان می‌دهد.

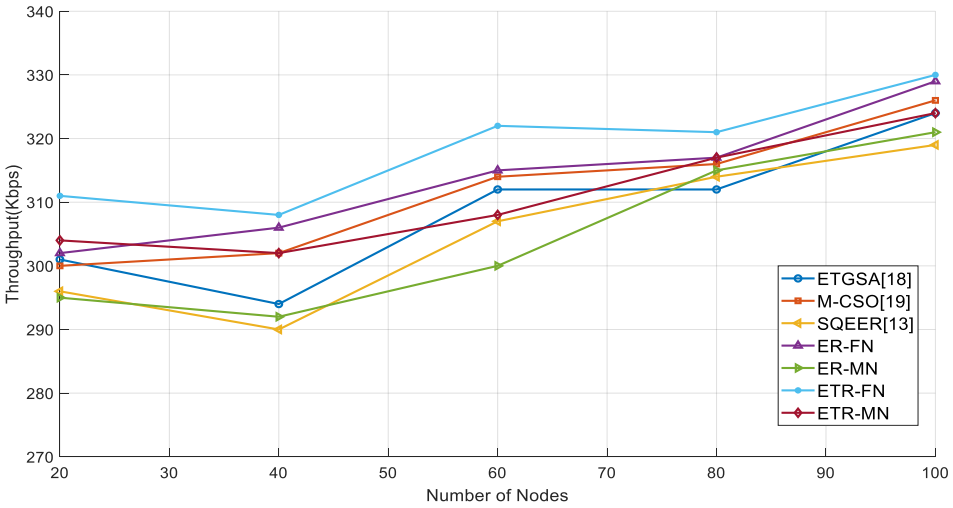
جدول ۱- پارامترهای مدل مصرف انرژی

پارامتر	مقدار
انرژی ارسال یا دریافت یک بیت (E_{elec})	50 nJ/bit
انرژی تقویت سیگنال ارسالی (ε_{mp})	0.0013 pJ/bit/m4
انرژی آمپلی‌فایر در فضای آزاد (ε_{fs})	10 pJ/bit/m2
انرژی حس محیط برای یک گره (E_{sense})	5 nJ/bit/packet
انرژی ایجاد بسته داده توسط سرخوشه (E_{DA})	5 nJ/bit/packet
انرژی راه‌اندازی یک گره (E_{wake})	2 nJ

۵-۴- نتایج شبیه‌سازی

شکل (۵) نتایج حاصل از الگوریتم‌های مورد مطالعه را از نظر توان عملیاتی نشان می‌دهد. نتایج مقایسه نشان می‌دهد با توجه به مکانیزم امنیتی تعریف شده، الگوریتم پیشنهادی توان عملیاتی بیشتری دارد. با افزایش تعداد گره‌ها توان عملیاتی شبکه افزایش می‌یابد، هرچند این افزایش بسیار ناچیز است. بنابراین الگوریتم پیشنهادی تعداد بسته‌های مخرّب ایجادشده توسط مهاجمان را کاهش می‌دهد. علاوه بر این، توان عملیاتی الگوریتم پیشنهادی از نسخهٔ بدون اعتماد آن بهتر است؛ زیرا ER در فرایند مسیریابی، قابلیت شناسایی گره‌های مخرّب را ندارد و این می‌تواند به تلفات بیشتر بسته‌ها منجر شود. با این حال، در الگوریتم پیشنهادی، گره‌های مخرّب شناسایی شده، تلفات بسته‌ها کاهش می‌یابد. به‌دلیل احتمال خرابی لینک و بسته‌های سلام بیشتر در حالت گره‌های متحرّک، توان عملیاتی در این حالت کمتر است.

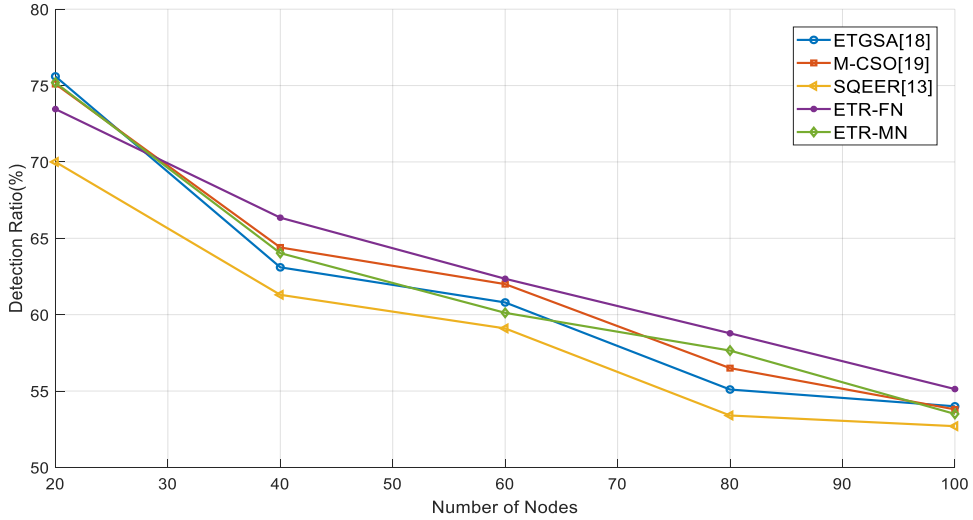
نتایج به وضوح نشان می‌دهد میانگین توان عملیاتی الگوریتم پیشنهادی در حالت گره‌های ثابت بالاتر از سایر الگوریتم‌هاست. در پایان دورهای مسیریابی، میانگین توان عملیاتی الگوریتم‌های ETR-FN، ETR-MN، ER-FN و ER-MN برای پنج سناریوی تعریف‌شده به‌ترتیب ۳۱۸، ۳۱۱، ۳۱۴ و ۳۰۵ گزارش شده است. همچنین میانگین توان عملیاتی برای الگوریتم‌های ETGSA، M-CSO و SQEER به‌ترتیب ۳۱۲ ،۳,۹ و ۳۰۵ است. براساس نتایج می‌توان نشان داد الگوریتم مسیریابی پیشنهادی در مقایسه با الگوریتم‌های مسیریابی موجود، به نتایج بهتری رسیده است.



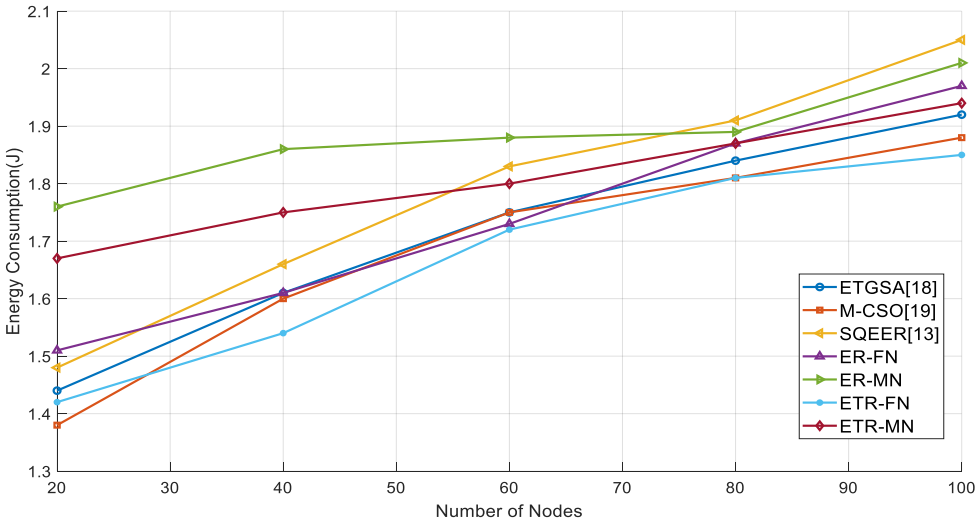
شکل ۵- تجزیه و تحلیل توان عملیاتی در الگوریتم‌های مسیریابی

شکل (۶) نرخ تشخیص گره‌های مخرّب به تعداد کل گره‌ها را توسط الگوریتم‌های مورد مطالعه نشان می‌دهد. نتایج این آزمایش بیان می‌کند که دقت تشخیص گره‌های مخرّب در الگوریتم پیشنهادی امیدوارکننده است. دلیل این کارایی، شناسایی گره‌های مخرّب در فرایند خوشه‌بندی و همچنین هنگام مسیریابی است. نرخ تشخیص گره‌های مخرّب در الگوریتم پیشنهادی با گره‌های متحرّک کمتر از حالت گره های ثابت است که این به‌دلیل تأثیر تحرّک گره‌ها و پیچیدگی شناسایی آن‌هاست. علاوه بر این، نسخه بدون اعتماد الگوریتم پیشنهادی، قابلیت تشخیص بسته‌های مخرّب را ندارد و قابل مقایسه در این معیار نیست.

تجزیه و تحلیل الگوریتم‌های مختلف براساس معیار نرخ تشخیص، برتری الگوریتم پیشنهادی با گره‌های ثابت را نشان می‌دهد. میانگین نرخ تشخیص در پایان دورهای مسیریابی برای الگوریتم‌های ETR-FN و ETR-MN به ترتیب ۶۲,۱ و ۶۳,۲۱ مشاهده شده است. علاوه بر این، میانگین نرخ تشخیص برای الگوریتم‌های ETGSA، M-CSO و SQEER به‌ترتیب ۶۱,۷۲، ۶۲,۳۶ و ۵۹,۳ است. نتایج تجزیه و تحلیل انرژی برای الگوریتم‌های مورد مطالعه در شکل (۷) نشان داده شده است. در الگوریتم پیشنهادی، ارسال بسته در مسیرهایی با ترافیک بالا کمتر انجام می شود و این منجر به کاهش برخوردها در مقایسه با ER شده است. واضح است که الگوریتم پیشنهادی در حالت گره‌های ثابت در مقایسه با حالت گره‌های متحرّک، مصرف انرژی کمتری دارد. به‌طور کلی، تحرّک گره‌ها باعث خرابی‌های لینک و مصرف انرژی بیشتر می‌شود.



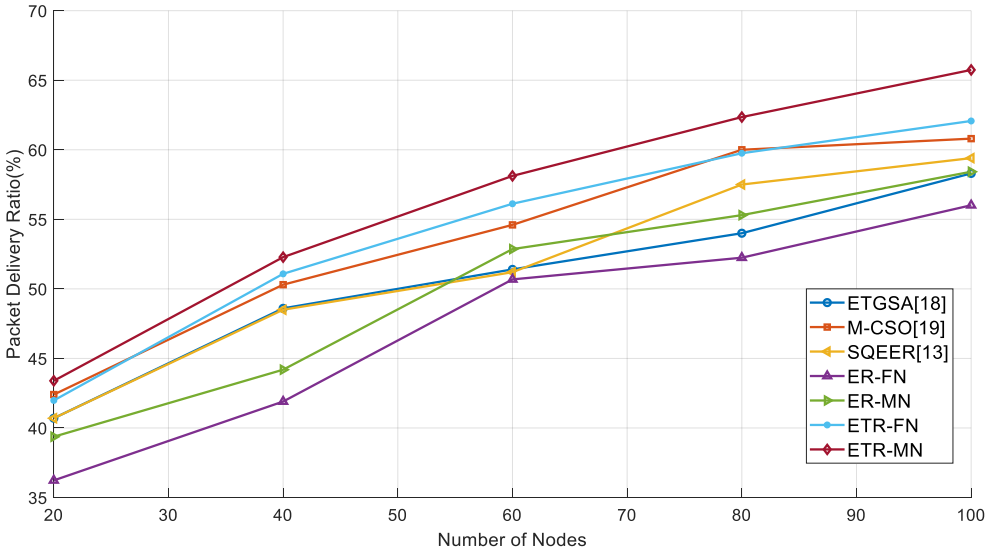
شکل ۶- تجزیه و تحلیل نرخ تشخیص گره‌های مخرّب در الگوریتم‌های مسیریابی



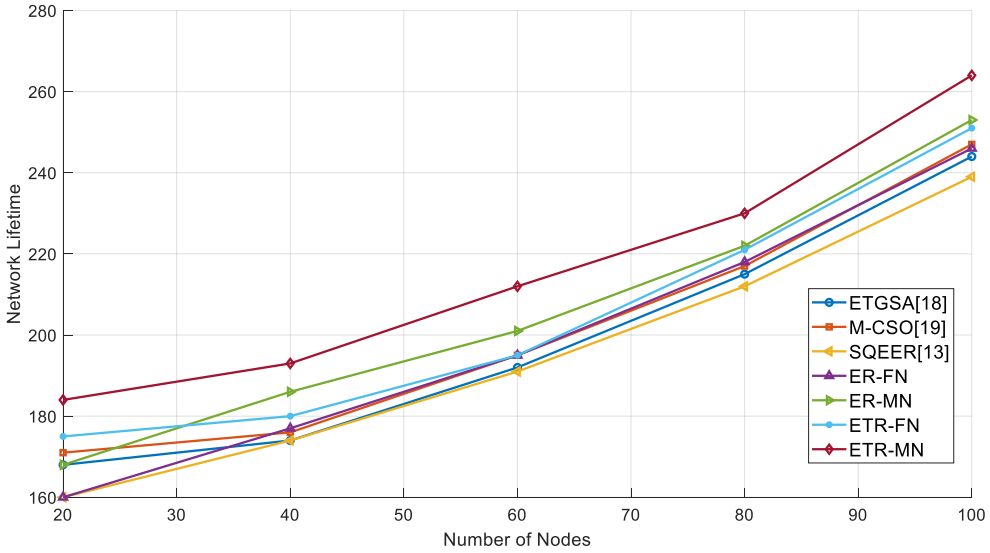
شکل ۷- تجزیه و تحلیل انرژی در الگوریتم‌های مسیریابی

تجزیه و تحلیل الگوریتم‌های مختلف براساس انرژی، برتری الگوریتم پیشنهادی با گره‌های ثابت را نشان می‌دهد. میانگین انرژی در پایان دورهای مسیریابی برای الگوریتم‌های ETR-FN، ETR-MN، ER-FN و ER-MN به‌ترتیب ۱,۶۷، ۱,۸۱، ۱,۷۴ و ۱,۸۸ اندازه‌گیری شده است. علاوه بر این، میانگین انرژی مصرفی برای الگوریتم های ETGSA، M-CSO و SQEER به‌ترتیب ۱,۷۱، ۱,۶۸ و ۱,۷۷ است. الگوریتم پیشنهادی در حالت گره‌های ثابت، نتایج بهتری را در مقایسه با سایر الگوریتم‌ها ارائه داده است. شکل (۸) تجزیه و تحلیل تعداد بسته‌های تحویل داده شده را برای الگوریتم‌های مورد مطالعه نشان می‌دهد.

با افزایش تعداد گره‌ها، نرخ تحویل بسته افزایش می‌یابد؛ زیرا تعداد گره‌های بیشتری در مسیریابی مشارکت می‌کنند. نتایج نشان‌دهندهٔ برتری الگوریتم پیشنهادی نسبت به نسخهٔ بدون اعتماد آن در هر دو حالت گره‌های ثابت و متحرّک است. دلیل این برتری، استفاده از مسیریابی مبتنی بر اعتماد است که باعث شناسایی گره‌های مخرّب و انتقال تعداد بسته‌های بیشتری شده است. علاوه بر این، عملکرد الگوریتم پیشنهادی با گره‌های متحرّک نسبت به حالت گره های ثابت کمی بهتر است؛ زیرا تحرّک گره‌ها می‌تواند باعث نزدیک شدن گره‌ها به هم و درنهایت کاهش فاصله شود.



شکل ۸- تجزیه و تحلیل نرخ تحویل بسته‌ها در الگوریتم‌های مسیریابی



شکل ۹- تجزیه و تحلیل طول عمر شبکه در الگوریتم‌های مسیریابی

تجزیه و تحلیل الگوریتم‌های مختلف براساس نرخ تحویل بسته‌ها، برتری الگوریتم پیشنهادی با گره‌های متحرّک را با میانگین ۵۶,۳۸ نشان می‌دهد. میانگین نرخ تحویل بسته‌ها در پایان دورهای مسیریابی برای الگوریتم‌های ETR-FN، ER-FN و ER-MN به‌ترتیب ۵۴,۲، ۴۷,۴۱ و ۵۰,۰۳ است. علاوه بر این، میانگین نرخ تحویل بسته‌ها برای الگوریتم‌های ETGSA، M-CSO و SQEER به‌ترتیب ۵۰,۶، ۵۳,۶۲ و ۵۱,۴۶ است، جایی که برتری الگوریتم پیشنهادی به‌وضوح قابل مشاهده است.

طول عمر شبکه، به مفهوم تعداد مسیریابی‌های مستقل انجام‌شده از یک سرخوشه به سینک قبل از اتمام انرژی اولین گره شبکه است. تجزیه و تحلیل مربوط به طول عمر شبکه برای الگوریتم‌های مورد مطالعه در شکل (۹) نشان داده شده است. با افزایش تعداد گره‌ها طول عمر شبکه افزایش می‌یابد؛ زیرا تعداد گره‌های ایمن بیشتری برای مسیریابی در دسترس هستند. طول عمر شبکه برای روش پیشنهادی ۲۰۴ است؛ یعنی انرژی اولین گره در این دور از مسیریابی تخلیه شده است. این مقدار در مقایسه با ER برتری قابل توجهی را نشان می‌دهد. استفاده از گره‌های ایمن موجود در شبکه از طریق به‌روزرسانی خوشه‌بندی، باعث توزیع صحیح مصرف انرژی و درنهایت افزایش طول عمر شبکه در الگوریتم پیشنهادی شده است. علاوه بر این، الگوریتم پیشنهادی در حالت گره‌های متحرّک در مقایسه با حالت گره‌های ثابت، طول عمر شبکهٔ بهتری را فراهم می کند.

تجزیه و تحلیل الگوریتم‌های مختلف براساس طول عمر شبکه، برتری الگوریتم پیشنهادی را در حالت گره‌های متحرّک نشان می‌دهد. با این حال، نتایج الگوریتم پیشنهادی در حالت گره‌های ثابت نیز امیدارکننده است. میانگین طول عمر شبکه در پایان دورهای مسیریابی برای پنج سناریو محاسبه گردیده و برای الگوریتم‌های ETR-FN، ETR-MN، ER-FN و ER-MN به‌ترتیب ۲۰۴، ۲۱۷، ۱۹۹ و ۲۰۶ گزارش شده است. علاوه بر این، میانگین طول عمر شبکه برای الگوریتم‌های ETGSA، M-CSO و SQEER به‌ترتیب ۱۹۸، ۲۰۱ و ۱۹۵ است، جایی که الگوریتم پیشنهادی با گره‌های متحرّک به‌وضوح بهترین است.

۵-۵- بحث و مقایسه

در این بخش، تجزیه و تحلیل و مقایسهٔ الگوریتم پیشنهادی براساس معیارهای ارزیابی مختلف در مقابل سایر الگوریتم های مسیریابی ایمن بررسی می‌شود. نتایج معیارهای ارزیابی برای الگوریتم‌های مسیریابی ETGSA [۱۸]، M-CSO [۱۹] و SQEER [۱۳] و همچنین الگوریتم مسیریابی پیشنهادی پس از پایان دورهای مسیریابی با وجود حمله منع سرویس در شکل‌های ۴ تا ۸ ارائه شده است. نتایج شبیه‌سازی نشان می‌دهند الگوریتم مسیریابی پیشنهادی در هر دو حالت گره‌های ثابت و متحرّک، کارایی بهتری را نسبت به الگوریتم‌های مورد مقایسه ارائه می‌دهد. این برتری در معیارهای توان عملیاتی، نرخ تشخیص، انرژی، نرخ تحویل بسته و طول عمر شبکه قابل مشاهده است. علاوه بر این، نتایج به‌وضوح نشان می‌دهد کارایی براساس توان عملیاتی، به تعداد گره‌ها وابسته نیست. علاوه بر این، الگوریتم پیشنهادی مقیاس‌پذیر است، جایی که توان عملیاتی در کل زمان شبیه‌سازی برای تعداد گره‌های مختلف تقریباً یکسان است.

الگوریتم ETGSA هنگامی که تغییرات تصادفی روی ترافیک گره‌ها باشد، عملکرد ضعیفی گزارش می‌دهد. الگوریتم M-CSO دارای همگرایی آهسته است و این باعث افزایش تلفات بسته در اثر گره‌های مخرّب و درنتیجه کاهش توان عملیاتی می‌شود. همچنین ارسال متوالی بسته‌های سلام در SQEER باعث تخریب گره‌های زیادی شده، منجر به کاهش توان عملیاتی می‌گردد. دلیل برتری الگوریتم پیشنهادی، استفاده از ثابت تحمل برای انتخاب گره‌های سرخوشه از میان گره‌های کاندیداست. علاوه بر این، گره‌های مخرّب با یک مقدار آستانه مشخص می‌شوند و تنها گره‌های ایمن در ایجاد خوشه‌ها و مسیریابی شرکت می‌کنند.

به‌طور کلی، الگوریتم پیشنهادی به شکل مؤثر بسته‌های مخرّب را شناسایی می‌کند و در مقایسه با سایر الگوریتم‌های مسیریابی ایمن، عملکرد بهتری دارد. دلیل این برتری، شناسایی گره‌های مخرّب در فرایند خوشه‌بندی و همچنین هنگام مسیریابی است. الگوریتم‌های ETGSA و M-CSO هیچ مکانیزمی برای کنترل انرژی در شبکه ندارند؛ بنابراین مصرف انرژی بالایی دارند. در مقایسه با SQEER، الگوریتم پیشنهادی می‌تواند چند مسیر بهینه را به‌جای یک مسیر پیدا کند. به‌دلیل وجود فقط یک مسیر برای هر گره در SQEER، نیاز به ارسال بسته‌های سلام زیادی است، جایی که باعث مصرف انرژی بیشتر و بازده

کمتری می‌شود. استفاده از تکنیک مسیریابی چند-مسیر موجب کاهش تعداد برخوردها و همچنین کاهش مصرف انرژی می‌گردد.

برای ارائهٔ تجزیه و تحلیل جامع، میانگین نتایج برای معیارهای ارزیابی مختلف در پایان دورهای مسیریابی گزارش شده است. در اینجا برای هر معیار ارزیابی میانگین نتایج در پنج سناریوی تعریف‌شده به‌منظور مقایسه استفاده می‌شود. این مقایسه در جدول ۲ برای الگوریتم‌های مختلف در حضور حملهٔ DoS ارائه شده است. مقادیر برجسته، بیانگر نتایج بهتر در مقایسه است.

جدول ۲- میانگین نتایج کارایی برای الگوریتم‌های مسیریابی مختلف

معیارها	ETGSA [۱۸]	M-CSO [۱۹]	SQEER [۱۳]	ETR-FN	ETR-MN
توان عملیاتی	۳۰۸,۶	۳۱۱,۶	۳۰۵,۲	۳۱۸,۴	۳۱۱,۰
نرخ تشخیص	۶۱,۷۲	۶۲,۳۶	۵۹,۳	۶۳,۲۱	۶۲,۱
انرژی	۱,۷۱	۱,۶۸	۱,۷۹	۱,۶۷	۱,۸۱
نرخ تحویل بسته	۵۰,۶	۵۳,۶۲	۵۱,۴۶	۵۴,۲	۵۶,۳۸
طول عمر شبکه	۱۹۸,۶	۲۰۱,۲	۱۹۵,۲	۲۰۴,۶	۲۱۶,۶
زمان اجرا (ثانیه)	۱۸۰	۴۱۸	۱۰۶	۲۱۵	۲۲۷

نرخ تشخیص و توان عملیاتی برای الگوریتم پیشنهادی به‌ترتیب ۶۳,۲۱ و ۳۱۸,۴ برای حالت ثابت و ۶۲,۱ و ۳۱۱ برای حالت متحرّک است. بنابراین می‌توان نشان داد الگوریتم پیشنهادی، عملکرد بهتری نسبت به الگوریتم‌های مورد مقایسه در معیارهای نرخ تشخیص و توان عملیاتی دارد. در معیار زمان اجرا الگوریتم پیشنهادی نسبت به ETGSA و SQEER پیچیدگی بیشتری دارد؛ زیرا این روش‌ها از الگوریتم‌های بهینه‌سازی استفاده نمی‌کنند. علاوه بر این، در سایر معیارهای ارزیابی نیز الگوریتم پیشنهادی، میانگین نتایج بهتری را ارائه داده است.

۶- نتیجه‌گیری و پیشنهادها

در این مقاله یک الگوریتم مسیریابی مبتنی بر اعتماد و انرژی-آگاه با استفاده از یک تابع برازندگی ترکیبی برای انتخاب مسیرهای بهینه در شبکه‌های حسگر بی‌سیم ارائه شد، جایی که علاوه بر گره‌های معمولی در شبکه، گره‌های مهاجم نیز حضور دارند. در الگوریتم پیشنهادی، مسیریابی ایمن شامل دو مرحلهٔ اصلی، یعنی انتخاب گره‌های ایمن و مسیریابی از بین گره‌های ایمن است. ابتدا گره‌های ایمن براساس ثابت تحمل انتخاب شده، سپس گره‌های مناسب برای مسیریابی براساس یک تابع برازندگی ترکیبی از میان گره‌های ایمن انجام می‌شود. مزیت اصلی الگوریتم مسیریابی ایمن پیشنهادی شامل اعمال تغییرات در خوشه بندی با تغییر گره‌های سرخوشه، افزایش دقت تشخیص گره‌های مخرّب، عدم استفاده از گره‌های مخرّب، استفاده از مسیریابی مبتنی بر خوشه‌بندی و بهبود عملکرد مسیریابی با تکنیک مسیریابی چند-مسیر است. کارایی الگوریتم مسیریابی پیشنهادی از طریق شبیه‌سازی یک شبکه حسگر بی‌سیم با تعداد گره‌های مختلف و در حضور حمله منع سرویس انجام شده است. نتایج شبیه‌سازی نشان می‌دهد الگوریتم پیشنهادی مقیاس‌پذیر است؛ زیرا توان عملیاتی در کل دورهای مسیریابی برای تعداد گره‌های مختلف تقریباً یکسان می‌باشد. برای کارهای آینده می‌توان الگوریتم پیشنهادی را در یک شبکه حسگر بی‌سیم مبتنی بر چند سینک متحرّک ارزیابی کرد. در اینجا گره‌های سینک می‌توانند برای کاهش مصرف انرژی، به مجموعه گره‌هایی با انرژی کم نزدیک شوند.

مراجع

[1] D.C. Mehetre, S.E. Roslin and S.J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust", Cluster Computing, Vol. 22, No. 1, 2019, pp. 1313–1328.

[2] Z. Heidary Ghiri and G.H. Mirjalily, "Energy-Harvesting Aware Multi-Hop Routing in Wireless Sensor Networks for Defense Applications", Journal of Electronical & Cyber Defence, Vol. 8, No. 4, 2021, pp. 63–73.

[3] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks", Ad hoc networks, Vol. 3, No. 3, 2005, pp. 325–349.

[4] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks", Computer communications, Vol. 30, No. 14, 2007, pp. 2826–2841.

[5] X. Fu, Y. Yang and O. Postolache, "Invulnerability of clustering wireless sensor networks against cascading failures", IEEE Systems Journal, Vol. 13, No. 2, 2018, pp. 1431–1442.

[6] T. Khan, K. Singh, M. Abdel-Basset, H.V. Long, S.P. Singh and M. Manjul, "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks", IEEE Access, Vo. 7, 2019, pp. 58221–58240.

[7] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H.K. Nehemiah and A. Kannan, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks", Wireless Personal Communications, Vol. 105, No. 4, 2019, pp. 1475–1490.

[8] O. AlFarraj, A. AlZubi and A. Tolba, "Trust-based neighbor selection using activation function for secure routing in wireless sensor networks", Journal of Ambient Intelligence and Humanized Computing, Vol. 9, 2018, pp. 1–11.

[9] E.P.K. Gilbert, K. Baskaran, E.B. Rajsingh, M. Lydia and A.I. Selvakumar, "Trust aware nature inspired optimised routing in clustered wireless sensor networks", International Journal of Bio-Inspired Computation, Vol. 14, No. 2, 2019, pp. 103–113.

[10] C. Lyu, X. Zhang, Z. Liu and C.H. Chi, "Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks", IEEE Access, Vol. 7, 2019, pp. 31068–31082.

[11] N. Kumar and Y. Singh, “Trust and packet load balancing based secure opportunistic routing protocol for WSN”, In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2017, pp. 463–467.

[12] R. Logambigai and A. Kannan, “QEER: QoS aware energy efficient routing protocol for wireless sensor networks”, In 2014 Sixth international conference on advanced computing (ICoAC), Chennai, India, 2014, pp. 57–60.

[13] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks", Wireless Personal Communications, Vol. 110, No. 4, 2020, pp. 1637–1658.

[14] H. Wang, G. Zhou, L. Bhatia, Z. Zhu, W. Li and J.A. McCann, "Energy-Neutral and QoS-Aware Protocol in Wireless Sensor Networks for Health Monitoring of Hoisting Systems", IEEE Transactions on Industrial Informatics, Vol. 16, No. 8, 2020, pp. 5543–5553.

[15] K. Thangaraj and T. Selvi, "Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR Based Dynamic Clustering Mechanisms", Journal on Wireless Communication Networks, Vol. 3, No. 4, 2015, pp. 14–23.

[16] O.O. Ogundile, M.B. Balogun, O.E. Ijiga E.O. Falayi, "Energy-balanced and energy-efficient clustering routing protocol for wireless sensor networks", IET Communications, Vol. 13, No. 10, 2019, pp. 1449–1457.

[17] K. Haseeb, K.A. Bakar, A.H. Abdullah and T. Darwish, "Adaptive energy aware cluster-based routing protocol for wireless sensor networks", Wireless Networks, Vol. 23, No. 6, 2017, pp. 1953–1966.

[18] A. Zahedi and F. Parma, "An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks", Peer-to-Peer Networking and Applications, Vol. 12, No. 1, 2019, pp. 167–176.

[19] P.A. Patil, R.S. Deshpande and P.B. Mane, "Trust and Opportunity Based Routing Framework in Wireless Sensor Network Using Hybrid Optimization Algorithm", Wireless Personal Communications, Vol. 115, No. 1, 2020, pp.415–437.

[۲۰] نسیبه سیادتی و کریم محمدی، «طراحی و شبیه‌سازی الگوریتم های مسیریابی تحمل‌پذیر نقص در شبکه بر روی تراشه»، مجلهٔ مدل سازی در مهندسی، دورهٔ ۲، شمارهٔ ۱۶، بهار ۱۳۸۷، صفحهٔ ۳۳-۴۳.

[21] M. Shelke, A. Malhotra and P.N. Mahalle, ”Congestion-aware opportunistic routing protocol in wireless sensor networks”, In smart computing and informatics, Singapore, 2018, pp. 63–72.

[۲۲] احمد عاشوری و ابولفضل جلیلوند، «ارزیابی امنیت سیستم حفاظتی شبکهٔ توزیع در حضور تولید پراکنده با استفاده از شبکهٔ پتری»، مجلهٔ مدل‌سازی در مهندسی، دورهٔ ۱۴، شمارهٔ ۴۴، تابستان ۱۳۹۵، صفحهٔ ۱۲۹-۱۴۲.

[۲۳] علی ابراهیمی، احمد حاجی‌پور و حمیدرضا توکلی، «موقعیت‌یابی در اینترنت اشیا با استفاده از الگوریتم بهینه‌سازی ازدحام ذرّات مرتبهٔ کسری آشوبی»، مجلهٔ مدل‌سازی در مهندسی، دورهٔ ۱۸، شمارهٔ ۶۰، بهار ۱۳۹۹، صفحهٔ ۱۵۷-۱۶۸.

[24] H. Hajipour, H. Behzadi Khormuji and H. Rostami, "ODMA: a novel swarm-evolutionary metaheuristic optimizer inspired by open source development model and communities", Soft Computing, Vol. 20, No. 2, 2016, pp. 727–747.

[25] S. Islam, M.N.I. Khan, M.Z. Ferdus, S.J. Islam and M.A. Kashem, “Improving Throughput using Cooperating TDMA Scheduling of Wireless Sensor Networks”, In 2020 International Conference on Computing and Information Technology, Tabuk, Saudi Arabia, 2020, pp. 1–4.

[26] A. Carie, M. Li, B. Marapelli, P. Reddy, H. Dino and M. Gohar, "Cognitive radio assisted WSN with interference aware AODV routing protocol", Journal of Ambient Intelligence and Humanized Computing, Vol. 10, No. 10, 2019, pp. 4033–4042.

[27] A. Rezaeipanah, H. Nazari, and G.R. Ahmadi, "A Hybrid Approach for Prolonging Lifetime of Wireless Sensor Networks Using Genetic Algorithm and Online Clustering", Journal of Computing Science and Engineering, Vol. 13, No. 4, 2019, pp. 163–174.

[28] R. Mhemed, N. Aslam, W. Phillips and F. Comeau, "An energy efficient fuzzy logic cluster formation protocol in wireless sensor networks", Procedia Computer Science, Vol. 10, 2012, pp. 255–262.

[29] Y. Liu, M. Dong, K. Ota and A. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks", IEEE Transactions on Information Forensics and Security, Vol. 11, No. 9, 2016, pp. 2013-2027.

[30] Y. Wang, M. Zhang and W. Shu, "An emerging intelligent optimization algorithm based on trust sensing model for wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, Vol. 2018, No. 1, 2018, pp. 1-10.