نشریه علمی-تخصصی
پژوهش های نوین علوم مهندسی
ISSN: 2538-3809
سال هشتم، شماره ۴ (پیاپی: ۴۵)، پاییز ۱۴۰۲

افزایش قابلیت اطمینان در شبکه‌های حسگر بی‌سیم با استفاده از پروتکل‌های مسیر یابی چند مسیره

رضا عرفانی[1]*

تاریخ دریافت: ۱۴۰۲/۰۷/۲۵
تاریخ پذیرش: ۱۴۰۲/۰۸/۲۷
کد مقاله: ۸۲۳۷۹

چکـیده

شبکه حسگر بی سیم شبکه ای است که برای نظارت و کنترل محیط اطراف استفاده می شوند. استفاده از این شبکه ها به دلیل ویژگی خاص و کاربرهای بسیارشان مورد توجه قرار کرفته اند. از مهمترین مباحث در حوزه انتقال داده در این شبکه ها ارائه راهکارهایی در جهت انتخاب بهترین مسیر ممکن برای انتقال اطلاعات می باشد به نحویکه انرژی مصرفی در کمترین حد و طول عمر شبکه در بیشترین حد باشد. تاکنون الگوریتم های بسیاری در جهت جمع اوری، ارسال و پردازش داده ها در شبکه های بی سیم ارائه شده است با این حال هنوز مشکلات عمده ای در مبحث انتقال داده وجود دارد. پژوهش حاضر به منظور افزایش قابلیت اطمینان در شبکه های حسگر بی سیم با استفاده از پروتکل های مسیر یابی چند مسیره صورت گرفته است لذا ابتدا پروتکل مسیریابی چند مسیره LOMDD بر مبنای پروتکل انتشار هدایت شده طراحی شد. برای طراحی پروتکل مسیریابی چند مسیره LOMDD فیلتر TPP انتخاب شده است که پیاده‌سازی‌های لازم، بر روی این فیلتر و تحت شبیه ساز NS2 انجام می‌شود. سپس یک راهکار برای تخمین قابلیت اطمینان با استفاده از دیاگرام تصمیم گیری دودویی مرتب شده پیشنهاد شد. در نهایت یک پروتکل چند مسیره تطبیقی برای اقناع قابلیت اطمینان AMPRS مبتنی بر LOMDD معرفی شد. نتایج شبیه سازی حاکی از تطبیق بسیار بالای AMPRS با شرایط شبکه است و نشان داده شد که نسبت به پروتکل های ایستا قابلیت اطمینان را به صورت کارا برای شبکه تنظیم می کند، سربار محاسباتی و انرژی مصرف شده را کاهش می دهد و همچنین تعداد مسیر بهینه را برای منابع تعیین می کند. با توجه به اینکه عملکرد پروتکل AMPRS با قابلیت اطمینان مورد انتظار ۹۰ درصد انجام می پذیرد بنابر این در مقایسه با سایر پژوهش های انجام شده، پروتکلی مطمئن تر به حساب می آید.

واژگـان کلـیدی: شبکه حسگر بی سیم، انتقال داده، پروتکل‌های مسیر یابی چند مسیره،پروتوکل LOMDD ، پروتکل AMPRS

۱- دانشجوی دانشگاه آزاد واحد زاهدشهر
r.erfani2021@gmail.com

۱- مقدمه

شبکه حسگر بی سیم به عنوان موضوعی نو و بسیار با اهمیت در حوزه فناوری اطلاعات مطرح است. این شبکه ها به صورت مستقل و بدوت دخالت انشان فعالیت میکنند و بهترین گزینه برای حالت هایی هستند که ما به محیط هدایت شده دسترسی نداشته باشیم.(کیهانی، ۱۳۹۱) شبکه حسگر بی سیم متشکل از صدها یا هزاران حسگر به صورت گره هستند که در اطراف عامل فیزیکی مورد نظر قرار گرفته و توانایی برقراری ارتباط با محیط و انجام محاسبات را دارند. هر گره حسگر میتواند عناصر محیطی خویش را احساس کند و پس از انجام محاسبات ساده، به صورت مستقیم و یا با واسطه گره های کناری خود با ایستگاه اصلی مرتبط شده و بدین طریق اطلاعات جمع اوری شده را در دسترس ان قرار دهد.(کردافشاری، ۱۳۹۸)استفاده از شبکه حسگر بی سیم برای اندازه گیری کمیت های فیزیکی یا شرایط محیطی همچون لرزش ، فشار، دما، صدا و ... در مکان ها و قسمت های مختلف یک محدوده کاربرد دارند از این رو دامنه استفاده از این حسگرها موضوعات مهمی همچون امنیت ملی، خدمات درمانی، نظامی، نظارت بر محیط و ... را در برمیگیرد. . گسردگی حوزه کاربرد این حسگرها توجه بسیاری از محققان را به خود معطوف کرده و از سوی دیگر بنا بر پیشرفت های صورت گرفته در حوزه های مخابرات و الکترونیک منجر به طراحی و ساخت حسگرهایی در سایز های کوچکتر، توان مصرفی کمتر و با قیمت مناسب تر شده است. انچه در تحویل داده ها و اطلاعات از گره های حسگر تاثیر به سزایی دارد در دسترس بودن شبکه است و قابلیت اطمینان از پارامترهای مهم دسترس پذیری می باشد. در حقیقت انتقال و ارسال داده ها با ضریب اطمینان بالا از موضوعات اساسی در شبکه حسگر بی سیم به شمار می اید. لذا بررسی افزایش قابلیت اطمینان در شبکه های حسگر بی سیم با استفاده از پروتکل های مسیر یابی چند مسیره به عنوان هدف این پژوهش مطرح است. تا کنون پژوهش های بسیاری در این حوزه صورت گرفته است.

۲- مروری بر مطالعات پیشین

صادقی نژاد و همکاران در سال ۱۴۰۰ دو روش دست یابی به قابلیت اطمینان ارسال مجدد و افزونگی را برای رسیدن به درجه بالایی از کارامدی و بهره وری سیستم معرفی کرده و ویژگیهای پروتکلهای قابلیت اطمینان موجود بر پایه هر یک از تکنیک های بیان شده، را تجزیه و تحلیل کردند.

واعظی و همکاران در سال ۱۴۰۰ در پژوهشی یک پروتوکل مسیر یابی جدید مبتنی بر کیفیت خدمات را پیشنهاد داده و اعلام کردند ازآنجاییکه روش پیشنهادی سعی در انتخاب کوتاهترین مسیرها و به کارگیری ارسال مجدد بسته های گمشده دارد، آن می تواند میانگین تأخیر را حدود ۳۰٪ در شبکه های با مقیاس بزرگ بهبود داده و قابلیت اطمینان بالایی داشته باشد.

نوری و زینالی در سال ۱۳۹۹ در پژوهشی با هدف اریابی کارایی پروتوکل های مسیر یابی چند مسیره در تضمین امنیت و حریم خصوصی شبکه های بیسیم دسته بندی سه بخشی از پروتوکل های مسیریابی چند مسیره را ارائه کرده و ضمن تحلیل نقاط ضعف و قوت پروتوکل های مطرح شده ، مزیت پروتوکل ها مبنی بر کاهش نفوذ نفوذ گر و جلوگیری از حملات فریبکارانه را اعلام کردند.

بهروان و همکاران در سال ۱۳۹۹ از بهینه سازی کلونی مورچه از روش بهینه سازی کلونی مورچه برای ایجاد مسیرهای چند پرشه و انرژی کارآمد استفاده کرده و نتایج شبیه سازی انها کارمد بودن پروتکل EEMCA در مقایسه با دو پروتکل دیگر از نظر را نشان داد.

القحطانی در سال ۲۰۲۱ در نتیجه پژوهش خود اعلام کرد مسیریابی همزمان در کنار چند مسیر، توانایی رسیدگی به این خرابی ها را به میزان قابل توجهی افزایش می دهد و به طور قابل توجهی برنامه چند رسانه ای بی سیم را به دست می آورد.

جیا در سال ۲۰۲۱ با بررسی الگوریتم مسیریابی تعادل انرژی توزیع شده برای شبکه حسگر بی سیم ، شبکه Ad Hoc با بار بالا، تحرک بالا و محدودیت انرژی، پروتکل مسیریابی چند مسیری تعادل انرژی بار را پیشنهاد داد.

دانون و همکاران در سال ۲۰۲۱ با بررسی جامع پروتکل های مسیریابی خوشه ای مبتنی بر LEACH در شبکه های حسگر بی سیم، نقاط قوت و محدودیت های هر پروتکل LEACH-variant را مورد بحث قرار می دهد. در نهایت، مقاله با توصیه هایی در زمینه تحقیقات آینده در WSN خاتمه می یابد.

لیانگ و همکاران در سال ۲۰۲۱ با بررسی انتقال مسیریابی تعاونی تطبیقی برای شبکه‌های حسگر بی‌سیم ناهمگن انرژی ، یک الگوریتم مسیریابی تعاونی تطبیقی جدید همراه با DEEC را پیشنهاد داده و نتایج شبیه‌سازی عملکرد بهتر الگوریتم مسیریابی پیشنهادی نسبت به طرح‌های معیار را نشان داد . همچنین الگوریتم مسیریابی پیشنهادی توانست به طور موثر مصرف انرژی شبکه را کاهش دهد و طول عمر شبکه را افزایش دهد.

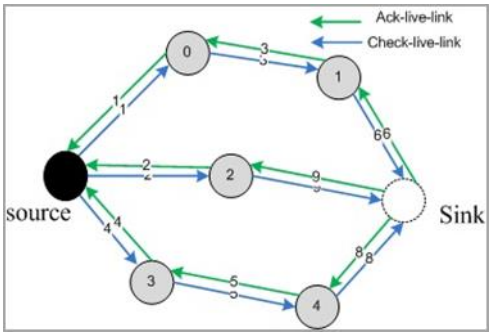
۳- روش

گام نخست در این پژوهش طراحی یک پروتکل مسیریابی چند مسیره LOMDD بر مبنای پروتکل انتشار هدایت بود. فیلتر TPP برای طراحی پروتکل مسیریابی چند مسیره LOMDD انتخاب و پیاده‌سازی‌های لازم، بر روی این فیلتر و تحت شبیه ساز

NS2 انجام شد. پروتکل LOMDD در چهار فاز: انتشار علاقه‌مندی‌ها- فاز انتشار بسته‌های اکتشافی - فاز ارسال داده‌های تقویتی - فاز ارسال داده‌ها و تعویض مسیرها انجام شد. پس از ان به ارائه راهکار به منظور تخمین قابلیت اطمینان با استفاده از دیاگرام تصمیم‌گیری دودویی مرتب شده پرداخته شد. راهکار پیشنهاد شده قابلیت اطمینان را با یک تقریب خوب بدست اورده و برای شبکه‌های حسگر بی‌سیم مناسب می‌باشد (ابولفتوح ، ۲۰۱۶). در شکل زیر نمایشی از درخت تصمیم‌گیری دودویی ارائه شده است.

۳-۱- روش گام به گام

در این روش برخلاف روش اول که انتها به انتها مسیرها را مورد آزمایش قرار می‌دهد، هر گره‌ای که روی یک مسیر قرار دارد گره بعدی[1] بعد از خود مربوط به آن مسیر را بررسی می‌کند. هنگامی که بسته‌های تقویتی روی مسیر عقبگرد (فاز سوم) ارسال می‌شوند. هر گره با دریافت این بسته، یک بسته از نوع Check-live-link را ایجاد می‌کند و آن را به گره بعدی خود ارسال می‌کند. در اینجا نیز یک شمارنده با مقدار اولیه صفر تنظیم شده است. با ارسال هر بسته از نوع Check-live-link شمارنده یک واحد افزایش پیدا می‌کند. گره بعدی با دریافت این بسته، یک بسته از نوع Ack-live-link ایجاد می‌کند و برای گره قبلی ارسال می‌کند .گره اول با دریافت هر بسته از نوع Ack-live-link مقدار شمارنده خود را صفر می‌کند.



شکل ۱: نحوه بررسی کردن زنده بودن گره‌های بعدی روی هر مسیر

در صورتی که مقدار این شمارنده بیشتر از ۳ شود گره متوجه می‌شود گره بعدی خراب شده است و گرادیان مربوط به آن را از جدول مسیریابی خود حذف می‌کند. در ادامه یک بسته از نوع Negative-Reinforcement در مسیر عقبگرد برای تمام منابعی که لینک مورد نظر روی مسیرهای آن واقع شده است ارسال می‌کند و این بسته گام به گام ارسال می‌شود تا به منبع مورد نظر برسد. منبع نیز با دریافت این بسته آن را از جداول مسیریابی خود حذف می‌کند.

الف- راهکار پیشنهادی برای تخمین قابلیت اطمینان با استفاده از دیاگرام تصمیم‌گیری دودویی مرتب شده: تحلیل قابلیت اطمینان شبکه برای طراحی، نگهداری و ارزیابی مورد نیاز است. قابلیت اطمینان سیستم‌های پیچیده بسیار حیاتی است و خرابی قطعه‌ها نتایج خیلی زیان‌آوری را در پی دارد. عملکرد موفق از شبکه‌های حسگر بی‌سیم وابسته به محدوده حس کردن و وضعیت اتصال گره‌ها به یکدیگر است. گره‌ها در شبکه‌های سنتی نسبت به یکدیگر متصل‌تر هستند. چون میزان خرابی در این شبکه‌ها بالا است لذا تکنیک‌های سنتی نمی‌توانند یک مدل دقیق و کارا برای شبکه‌های حسگر بی‌سیم فراهم کنند.

شبکه‌های حسگر بی‌سیم پروتکل‌های پویا دارد چون مبتنی بر درخواست برای وظیفه‌ها است؛ لذا انرژی حسگرها و توان مصرفی آن‌ها طوری تنظیم می‌شود که نیازهای محدوده حس کردن و اتصال را فراهم کند. ارزیابی قابلیت اطمینان به صورت گسترده در شبکه‌های کامپیوتری سنتی و سیستم‌های حساس غیر شبکه‌ای مورد بررسی قرار گرفته است. محاسبه قابلیت اطمینان همواره یکی از مشکلات طراحان شبکه‌های حسگر بی‌سیم و جزو مسائل #P_Hard می‌باشد؛ لذا وجود یک راهکار برای محاسبه قابلیت اطمینان به ویژه در شبکه‌های نظارتی و شبکه‌هایی که محدودیتی بر روی آن‌ها وجود دارد ضروری می‌باشد. در این قسمت یک راهکار برای تخمین قابلیت اطمینان با استفاده از دیاگرام تصمیم‌گیری دودویی مرتب شده (OBDD) پیشنهاد می‌شود. راهکار پیشنهاد شده قابلیت اطمینان را با یک تقریب خوب بدست می‌آورد و برای شبکه‌های حسگر بی‌سیم مناسب می‌باشد (ابولفتوح و همکاران، ۲۰۱۶).

ب- دیاگرام تصمیم گیری دودویی مرتب شده: تصور کنید که یک برنامه کاربردی فرمول‌های گزاره‌ای بزرگی دارد که چندین بار استفاده می‌شوند. می‌توان از روی این فرمول‌ها، فرمول‌های دیگری برای ارزیابی هم ارزی و ارضا شدن محدودیت‌ها ساخت (اکر، ۲۰۰۸). برای کار با این برنامه‌ها به یک ساختار داده که ویژگی‌های زیر را داشته باشد نیاز است:

دارا بودن یک نمایش فشرده از فرمول‌ها یا یک تابع بولی که بتواند فرمول‌ها را نمایش دهد.

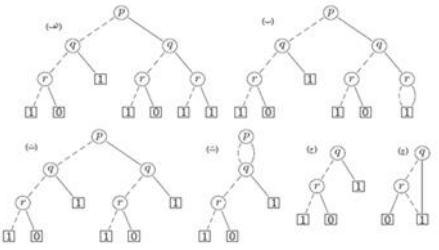
عملیات بولی روی فرمول‌ها به راحتی انجام شود. به طور مثال با داشتن فرمول‌های ,fn f1,……، یک نمایشی از حرف ربط به صورت fn^…..^f1 امکان پذیر باشد.

تسهیلاتی برای بررسی کردن ویژگی‌های فرمول‌ها وجود داشته باشد.

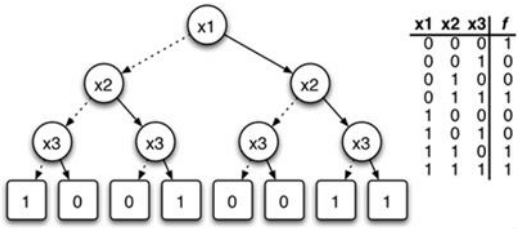
BDD به عنوان یک ساختار داده برای نمایش فشرده از درخت‌ها می‌باشد. بررسی ارضا پذیری در BDD کاری آسان است، با این وجود پیاده‌سازی تابع‌های بولی مشکل است. با اضافه کردن ترتیب به BDD، BDD مرتب شده (OBDD) بدست می‌آید.

1 Next-hop

OBDD یک نوع خاصی از BDD است که تابع‌های بولی را به شکلی کارا پیاده‌سازی می‌کند. درخت تصمیم‌گیری دودویی با حذف دو نوع از افزونگی‌ها می‌تواند به یک ساختار فشرده‌تر تبدیل شود.



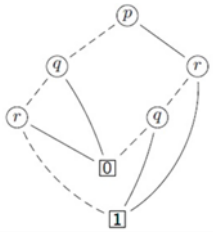
شکل ۲: تبدیل درخت دودویی به BDD



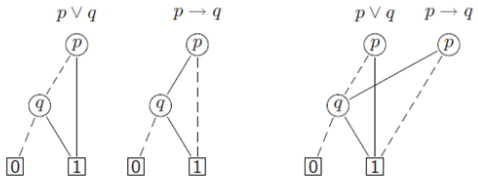
شکل ۳: یک درخت دودویی با آزمایش روی فرمول

$$f(x_1, x_2, x_3) = \overline{x}_1\overline{x}_2\overline{x}_3 + x_1x_2 + x_2x_3$$

با حذف آزمایش اضافی و ادغام زیر گراف‌های همریخت یک ساختار داده که نمودار تصمیم گیری دودویی (BDD) نامیده می‌شود بدست آمد.



شکل ٤: یک BDD مرتب نشده



شکل ٥: دو OBDD و یک گراف کلی که هر دو را در بردارد.

شکل و سایز BDD وابسته به ترتیب آزمایش‌هایی است که روی متغیرها انجام می‌شود. ترتیب‌های مختلف می‌تواند افزایش یا کاهش شدیدی در اندازه BDD داشته باشد. در OBDD ترتیب روی شاخه‌های مختلف یکسان اسدر نهایت یک پروتکل چند مسیره تطبیقی برای اقناع قابلیت اطمینان AMPRS مبتنی بر LOMDD معرفی شد.

۴- یافته‌های تحقیق

با توجه به کاربرد گسترده شبکه‌های حسگر بیسیم ، همچنان قابلیت اطمینان به عنوان یکی از الزامات عملکردی شبکه ها مطرح می باشد. استفاده از مسیریابی چند مسیره (Multipath Routing)که بر اساس آن مسیرها نقش پشتیبان (Backup) را برای یکدیگر ایفا می نمایند به عنوان یکی از راه حل های ارائه شده در جهت افزایش قابلیت اطمینان مطرح شده است.

نحوه پیاده‌سازی و ارزیابی پروتکل مسیریابی چند مسیره LOMDD بر مبنای پروتکل انتشار هدایت شده: بستر پیاده سازی: به منظور پیاده سازی پروتکل از کد diffusion 3.2 که همراه بسته نرم افزاری NS2.34[1] عرضه شده است، استفاده شد. در این بسته دو نسخه از پروتکل انتشار هدایت شده وجود دارد که عبارتند از diffusion و diffusion3. نسخه diffusion، پیاده سازی ساده شده الگوریتم است و جزئیات کمتری را در برمی‌گیرد. در پروتکل LOMDD از فیلترTPP۲[2] در diffusion3 استفاده شد. سناریوهای شبیه سازی: جهت بررسی عملکرد این پروتکل از یک شبکه با مقیاس ۱۰۰۰m × ۱۰۰۰m استفاده شده است که ۱۲۰ گره به صورت یکنواخت در این فضا پخش شده‌اند. دامنه ارسال هر گره برابر ۸۰ متر می‌باشد. برای شبیه‌سازی از یک چاهک استفاده شده است که در مرکز فضای شبیه‌سازی قرار دارد. همچنین از یک منبع برای ارسال بسته‌ها استفاده شده است. زمان شبیه‌سازی برای این سناریو برابر ۱۲۰ ثانیه می‌باشد و نرخ ارسال بسته‌ها توسط منبع ۱۰ بسته در هر ثانیه می‌باشد. مدل انرژی استفاده شده Energy model می‌باشد. از IEEE 802.11 در لایه MAC استفاده می‌شود.

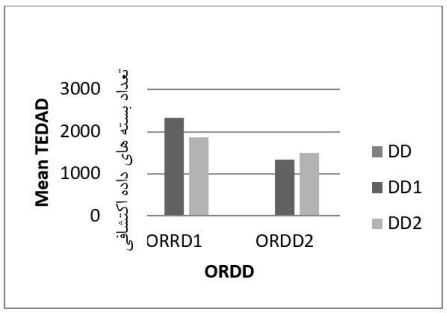
1 NS, "network simulator version 3."
2 Two-Phase-Pull

برای محاسبه سربار[1] بسته‌های اکتشافی کل بسته‌ها را که در شبکه رد و بدل شده را در مدت زمان شبیه‌سازی شمارش می‌کنیم و آن‌ها را در دو حالت DD و LOMDD مقایسه می‌کنیم. در طول مدت شبیه‌سازی وضعیت ارسال داده و در دسترس بودن مسیرها را در دو حالت LOMDD و DD مقایسه می‌کنیم. همچنین میانگین بسته‌های دریافتی در هر لحظه توسط چاهک نیز مقایسه می‌شود. برای محاسبه سربار بسته‌های غیر داده کل بسته‌های غیر داده را که در شبکه رد و بدل شده است، در مدت زمان شبیه سازی شمارش می‌کنیم و نتایج را در دو حالت DD و LOMDD بررسی می‌کنیم. برای محاسبه قابلیت اطمینان نسبت تعداد بسته‌های دریافت شده توسط چاهک به تعداد بسته‌های ارسال شده توسط منابع در طول زمان شبیه سازی را به دست می‌آوریم و در دو حالت DD و LOMDD با هم دیگر مقایسه می‌کنیم.

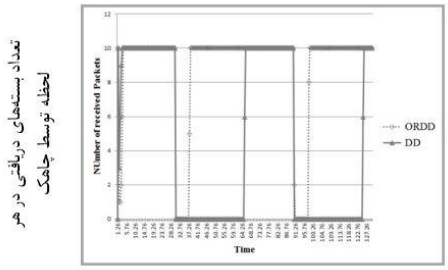
بررسی نتایج شبیه‌سازی

سربار بسته‌های اکتشافی: بنا بر شکل زیر تعداد بسته‌های اکتشافی رد و بدل شده در حالت LOMDD کاهش چشمگیری نسبت به DD داشته است که این به نوبه خود سربارها و مصرف انرژی را کاهش می‌دهد. این کاهش چشمگیر بدین دلیل است که در پروتکل انتشار هدایت شده بسته‌های اکتشافی توسط هر گره به تمام گرادیان‌های موجود در جدول مسیریابی ارسال می‌شوند در حالی که در پروتکل LOMDD بسته‌های اکتشافی به بهترین گرادیان ارسال می‌شود. (نمودار ۱)

میانگین تعداد بسته‌های دریافتی در هر لحظه توسط چاهک: همان‌طور که در شکل پیداست در ثانیه ۳۰ یک گره روی مسیر اصلی خراب می‌شود. در پروتکل DD به خاطر ویژگی‌های ذاتی آن تقریباً ۳۰ ثانیه طول می‌کشد تا بسته‌های علاقه‌مندی دوباره توسط چاهک ارسال شود و عملیات مسیریابی انجام شود. سپس منبع با پیدا کردن مسیر جدید داده‌های خود را به چاهک ارسال می‌کند. اما در پروتکل LOMDD این خرابی بعد از چند ثانیه تشخیص داده می‌شود. آنگاه منبع سریعاً مسیر جایگزین را انتخاب می‌کند و بسته‌های داده را روی مسیر جدید ارسال می‌کند. همان‌طور که در شکل پیداست در LOMDD فقط چند ثانیه ارتباط منبع با چاهک قطع می‌شود ولی طول این دوره برای DD بسیار زیاد است و سبب می‌شود بسته‌های زیادی در گره‌های میانی از بین بروند. (نمودار ۲)



نمودار ۱: سربار بسته‌های اکتشافی

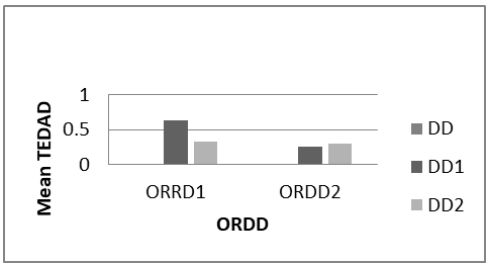


نمودار ۲: میانگین تعداد بسته‌های دریافتی در هر لحظه توسط چاهک

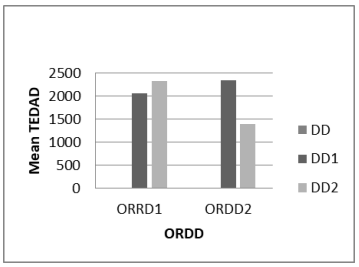
قابلیت اطمینان: قابلیت اطمینان در پروتکل LOMDD نسبت به DD افزایش چشمگیری داشته است که این بدین دلیل است که در پروتکل DD هنگام خراب شدن مسیر زمان زیادی طول می‌کشد تا یک مسیر جدید بین چاهک و منبع برقرار گردد و این سبب می‌شود که در این حین بسته‌های زیادی از دست بروند و به مقصد نرسند. اما در پروتکل LOMDD بعد از آنکه مسیر اصلی قطع شد سریعاً مسیر دیگری جایگزین می‌شود و بسته‌ها را به سمت مقصد هدایت می‌کند. (نمودار ۳)

سربار بسته‌های غیر داده: سربار کل بسته‌های غیر داده در دو پروتکل مقایسه شده است که این نتایج باز حاکی از بهبود LOMDD نسبت به DD است. سربار پروتکل LOMDD ناشی از بسته‌های کنترلی رد و بدل شده برای بررسی وضعیت مسیرها می‌باشد. (نمودار ۴)

1 Overhead



نمودار ۳: قابلیت اطمینان



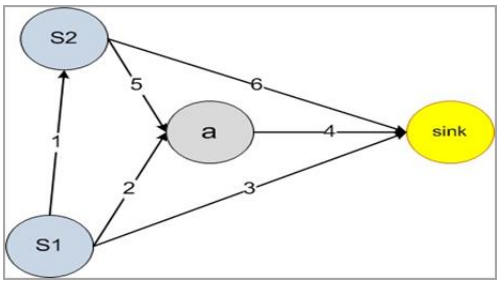
نمودار ٤: سربار بسته‌های غیر داده

تحلیل و تخمین قابلیت اطمینان با استفاده از یک راهکار پیشنهاد شده مبتنی بر OBDD: راهکار پیشنهاد شده یک راهکار بازگشتی است که با کاهش محاسبات اضافی و حذف زیر گراف‌ها[1] یک الگوریتم کارا برای محاسبه قابلیت اطمینان شده است. برای یک لینک مشخص در گراف بدست آمده چندین گره دریک سطح ممکن است وجود داشته باشد.

نمادهای استفاده شده در راهکار پیشنهاد شده: بجای متغیرهای بولی که در OBDD استفاده شد در راهکار جدید از لینک‌ها استفاده می‌کنیم و در هر مرحله آزمایش را بر روی لینک‌ها انجام می‌دهیم. لینک‌ها به صورت یک متغیر بولی به صورتی که در فرمول آمده است تعریف می‌شوند:

$$link_i = \begin{cases} 1 & \text{اگر لینک i فعال باشد} \\ 0 & \text{اگر لینک i فعال نباشد} \end{cases}$$

در اینجا لینک‌ها نشان‌دهنده گره‌ها در گراف (گرافی که برای محاسبه قابلیت اطمینان از شبکه بدست آمده) می‌باشند که در شکل یک نمونه از آن نمایش داده می‌شود. همان‌طور که در شکل مشاهده می‌شود یک گره به دو قسمت تبدیل شده است. در صورتی که لینک فعال در نظر گرفته شود قسمت ۱ را بسط می‌دهیم و کمان خروجی از این لینک را به صورت یک خط پر رنگ پیوسته نمایش می‌دهیم. در غیر این صورت قسمت صفر را بسط می‌دهیم و کمان خروجی از آن به وسیله خطوط تیره منقطع نمایش می‌دهیم.



شکل ٦: شبکه با دو منبع و یک چاهک

در اینجا تنها دو برگ به صورت $\boxed{1}$ و $\boxed{0}$ داریم که با پیمایش از ریشه لینک‌هایی که به $\boxed{1}$ ختم می‌شوند بیانگر این است که شبکه با حضور لینک‌های فعال در این پیمایش قابل اطمینان است و این گره را Reliable می‌نامیم، لینک‌هایی که به $\boxed{0}$ ختم می‌شوند بیانگر این است که شبکه با حضور لینک‌های غیر فعال در این پیمایش غیر قابل اطمینان است و این گره را Unreliable می‌نامیم.

نحوه عملکرد راهکار پیشنهاد شده: در ابتدا با توجه به لینک‌ها و مسیرهایی که برای هر منبع در نظر گرفته می‌شود با توجه به تعریف قابلیت اطمینان یک گراف بدست می‌آوریم. سپس قابلیت اطمینان را با استفاده از یک فرمول که بر روی گراف اعمال می‌شود محاسبه می‌کنیم. مراحل اجرای راهکار پیشنهاد شده در ادامه تشریح می‌شود. برای واضح شدن موضوع یک مثال را همراه با تشریح راهکار پیشنهاد می‌کنیم. فرض کنید شبکه مشابه شکل داریم که می‌خواهیم گراف مبتنی بر OBDD را با توجه به راهکار پیشنهاد شده برای محاسبه قابلیت اطمینان بدست آوریم. در توپولوژی شبکه شکل دو منبع S1 و S2 و یک چاهک در اختیار داریم. مسیرهای موجود از هر منبع به سمت چاهک، بر اساس ترتیب لینک‌های روی مسیر در زیر نمایش داده شده است:

$$s_1 = \begin{cases} 1-6 \\ 2-4 \\ 3 \end{cases} \qquad s_2 = \begin{cases} 5-4 \\ 6 \end{cases}$$

منبع S۱ شامل ۳ مسیر و منبع S2 شامل ۲ مسیر است. با توجه به تعریف قابلیت اطمینان، گراف را به صورتی ایجاد می‌کنیم که با توجه به لینک‌های پیمایش شده از ریشه تعیین شود که شبکه قابل اطمینان یا غیر قابل اطمینان است. با پیمایش از ریشه در هر یک از شاخه‌های این گراف در صورتی که به گره Reliable برسیم نشان دهنده این است که با وجود لینک‌های فعال در این پیمایش شبکه قابل اطمینان است و در صورتی که به گره Unreliable برسیم نشان دهنده این است که با وجود لینک‌های غیر فعال در این پیمایش شبکه قابل اطمینان نیست و نیازهای لازم بر اساس تعریف قابلیت اطمینان

1 Sub-Graph

برآورده نمی‌شود. شماره‌هایی که در یک ستون در سمت راست شکل نشان داده شده است بیانگر شماره لینکی است که در سطح مورد نظر مورد آزمایش قرار می‌گیرد. مثلاً لینک شماره ۵ در سطح چهارم مورد بررسی قرار گرفته است.

جدول ۱: مشخصات لینک شماره ٤

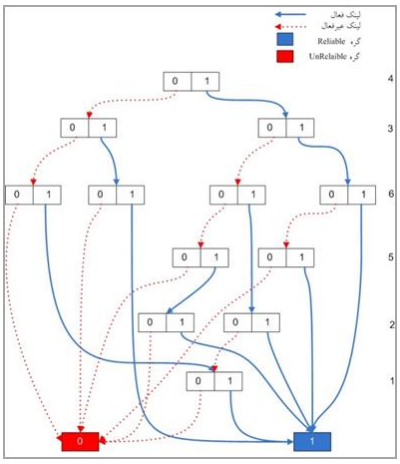
Success probability	0.95
Count repeat	2
prev node	a
next node	sink

در شکل دو نوع از کمان‌ها برای اتصال بین گره‌ها داریم. همان‌طور که در قبل ذکر شد در راهکار پیشنهاد شده این گره‌ها بیانگر لینک‌ها هستند. اگر لینک مورد نظر فعال در نظر گرفته شود یک کمان پر رنگ پیوسته از قسمت 1 گره مربوطه به گره بعدی (یا در واقع گره مربوط به لینک بعدی) وصل می‌شود و اگر لینک مورد نظر غیر فعال در نظر گرفته شود یک کمان با خط چین قرمز رنگ به گره بعدی اتصال پیدا می‌کند.

مثلاً در شکلسمت راست‌ترین گره، مربوط به لینک شماره ۶ در سطح سوم از گراف را در نظر بگیرید در صورتی که لینک شماره ۶ فعال در نظر گرفته شود یک کمان پر رنگ پیوسته به گره Reliable وصل می‌شود در غیر این صورت یک کمان خط چین به گره مربوط به لینک ۵ در سطح پایین‌تر متصل می‌گردد.

۴-۵- پیشنهاد یک پروتکل چند مسیره تطبیقی برای اقناع قابلیت اطمینان

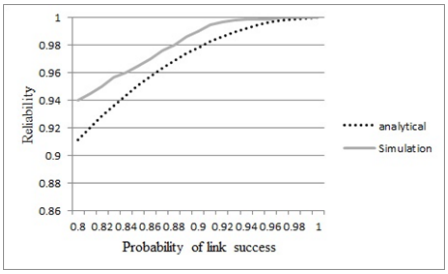
معمولاً در فاز طراحی شبکه با توجه به قابلیت اطمینان مورد انتظار از شبکه، تعداد مسیرهایی که باید بسته‌ها روی آن ارسال شوند تعیین می‌گردد. در شبکه‌های بی‌سیم احتمال موفقیت لینک در تحویل بسته‌ها به گام بعدی به عوامل زیادی بستگی دارد که سبب می‌شود در زمان‌های مختلف این مقدار تغییر کند. احتمال موفقیت لینک بر روی قابلیت اطمینان مسیرهایی که از این لینک استفاده می‌کنند. در نتیجه روی قابلیت اطمینان کل شبکه تأثیر می‌گذارد. کم یا زیاد شدن احتمال موفقیت لینک‌ها، تعداد مسیرهای استفاده شده را تحت تأثیر قرار می‌دهد. تعداد مسیرهایی که استفاده می‌شود بر روی کارایی شبکه نیز موثر است. با کم شدن احتمال موفقیت لینک مسیرهای موجود ممکن است قابلیت اطمینان مورد انتظار را ارضا نکند و با زیاد شدن احتمال موفقیت لینک استفاده از مسیرهای موجود ممکن است سربار زیادی را به شبکه تحمیل کند.



شکل ۷: گراف به دست آمده از شبکه شکل با استفاده از راهکار پیشنهاد شده

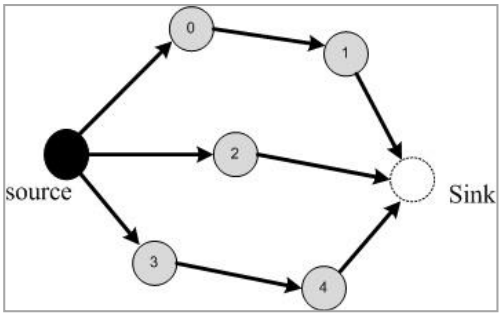
```
R_OBDD (LinkList-v) {
If (Network-Is-Reliable()){
Connect last arc in LinkList-v to Reliable Node
return}
If (Network-Is-UnReliable() or List-Is-
empty(LiskList)){
Connect last arc in LinkList-v to UnReliable Node
return}
Link=select-link(L)// Index L of LinkList
NL =Create-node(Link)
Connect last arc in LinkList-v to NL

L++;
Extract NL and create A+NL
Add A+NL to end of LinkList-v
Pos(NL)=R_OBDD(LinkList-v)
remove A+NL from end of LinkList-v

L=TSL+L-1
Extract NL and create A-NL
Add A-NL to end of LinkList-v
Neg(NL)=R_OBDD(LinkList-v)
remove A-NL from end of LinkList-v

if (check-Equal(Pos(NL), Neg(NL)))
merge Pos(NL) and Neg(NL)

if (pointer=Find-Isomorphic(Pos(NL)))
connect A+NL to pointer

if (pointer=Find-Isomorphic(Neg(NL)))
connect A-NL to pointer
return}
```

شکل ۸: شبه کد مراحل راهکار پیشنهاد شده برای تشکیل گراف جهت تخمین قابلیت اطمینان

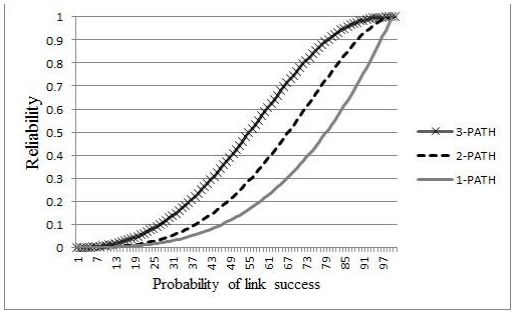


نمودار ۵: قابلیت اطمینان شبکه شکل به صورت تحلیلی و شبیه‌سازی

همچنین در بعضی کاربردها قابلیت اطمینان مورد انتظار در زمان‌های مختلف متفاوت است. در این مورد نیز با افزایش قابلیت اطمینان مورد انتظار، استفاده از مسیرهای موجود ممکن است قابلیت اطمینان مورد انتظار ارضا نشود یا با کاهش این مقدار، استفاده از مسیرهای موجود سربار زیادی را به شبکه تحمیل کند. به طور مثال شبکه یک منبع و یک چاهک دارد که سه مسیر مستقل از منبع به چاهک برقرار است. قابلیت اطمینان این شبکه برای احتمالات متفاوت از موفقیت لینک‌ها (احتمال همه لینک‌ها برابر است) با توجه به تعداد مسیرهایی که استفاده می‌شود در شکل زیر نشان داده شده است. محاسبات با استفاده از قوانین محاسبه قابلیت اطمینان با استفاده از فرمول‌های سری و موازی بدست آمده است.



شکل ۱۰: شبکه با سه مسیر مستقل از منبع به چاهک



نمودار ٦: قابلیت اطمینان مسیرهای مختلف برای توپولوژی شکل بالا

با توجه به شکل فرض می‌شود قابلیت اطمینان مورد انتظار برابر ۹۰ درصد باشد و احتمال موفقیت لینک‌ها نیز برابر ۹۰ درصد باشد. در اینجا مقدار بهینه برای تعداد مسیرهای استفاده شده ۲ می‌باشد. اگر از یک مسیر استفاده شود قابلیت اطمینان بدست آمده در حدود ۷۰ درصد است که قابلیت اطمینان مورد انتظار را ارضا نمی‌کند. همچنین اگر از ۳ مسیر استفاده شود قابلیت اطمینان بدست آمده در حدود ۹۸ درصد است. استفاده از ۳ مسیر قابلیت اطمینان را ارضا می‌کند ولی سربار بیشتری را به شبکه تحمیل می‌کند.

پروتکل چند مسیره تطبیقی پیشنهادی برای اقناع قابلیت اطمینان: پروتکل AMPRS یک پروتکل تخصیص مسیر دینامیک در شبکه‌های حسگر بی‌سیم است که جهت تعیین تعداد مسیرهای استفاده شده توسط هر یک از منابع برای ارضای قابلیت اطمینان طراحی شده است.در LOMDD از یک مسیر به عنوان مسیر اصلی استفاده می‌شد و سایر مسیرها به عنوان جایگزین انتخاب می‌شوند. پروتکل AMPRS به منظور تعیین تعداد مسیرها برای هر یک از منابع طراحی می‌شود. چاهک بر اساس اطلاعاتی که در دوره‌های زمانی از شبکه بدست می‌آورد تصمیم می‌گیرد که هر یک از منابع از چه مسیرهایی و چند مسیر برای ارسال اطلاعات استفاده کنند. در ادامه ابتدا یکسری از ویژگی‌های و پیش فرض‌ها را برای AMPRS بیان می‌کنیم سپس نحوه عملکرد آن را تشریح می‌کنیم.

تنظیمات اولیه: بعد از مسیریابی که مبتنی بر پروتکل پیشنهاد شده LOMDD است برای هر یک از منابع یک مسیر تنظیم می‌شود که منبع داده‌های خود را بر روی آن ارسال می‌کند. چاهک از حضور هر یک از منابعی که داده ارسال می‌کند با خبر است و اطلاعات هر منبع را در یک جدول به نام Info-Source در حافظه خود نگهداری می‌کند. با تشکیل هر مسیر اطلاعات مربوط به این مسیر در جدول ذخیره می‌شود. به طور کل می‌توان گفت چاهک یک دید کلی نسبت به منابع و مسیرهای تنظیم شده برای آن‌ها و همچنین ویژگی‌های این مسیرها دارد. این اطلاعات برای تصمیم گیری چاهک در مورد انتخاب مسیرها و نحوه توزیع بار در شبکه لازم می‌باشد.

برای هر منبع یک مدخل در جدول Info-Source ایجاد می‌گردد که اطلاعاتی از قبیل:

شماره شناسایی[1] منبع
مسیرهای موجود برای منبع
تعداد گام‌ها از منبع تا چاهک برای هر مسیر
مینیمم انرژی باقی مانده روی هر مسیر
لینک‌های روی هر مسیر
احتمال موفقیت لینک‌ها
قابلیت اطمینان هر یک از مسیرها
تعداد بسته‌های ارسالی از منبع تا زمان جاری

1 Identify

تعداد بسته‌های دریافتی از منبع تا زمان جاری توسط چاهک
وضعیت هر یک از مسیرها که آیا فعال است یا غیر فعال (داده روی آن انتقال داده می‌شود یا خیر)
و دیگر پارامترها در آن‌ها وجود دارد.
همچنین برای آزمایش زنده بودن مسیرها از روش انتها به انتها که در فصل ۳ تشریح شد استفاده می‌شود.

نحوه تصمیم گیری چاهک: در این پروتکل همواره سعی بر این است که قابلیت اطمینان همواره در حول و حوش قابلیت اطمینان مورد انتظار نگه داشته شود. برای این منظور از یک کران استفاده می‌کنیم که آن را $\propto$ می‌نامیم. اگر قابلیت اطمینان مورد انتظار را R_D بنامیم و قابلیت اطمینان بدست آمده از شبکه را R بنامیم همواره سعی می‌شود نامعادله ۴-۸ حفظ شود.

$$+R_D - \propto < R < R_D \propto \quad (۴-۸)$$

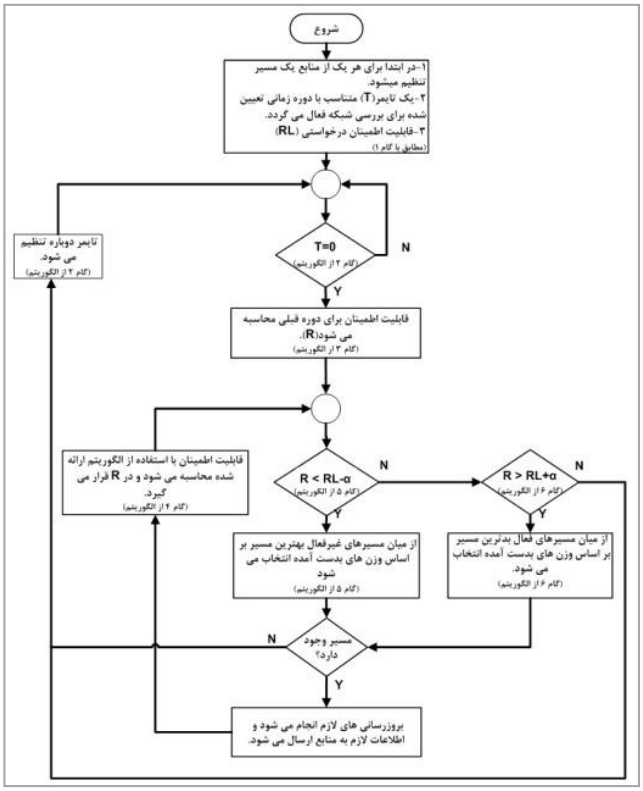
مراحل الگوریتم تصمیم‌گیری چاهک در زیر گام به گام بیان می‌شود:

گام ۱. در ابتدا برای هر یک از منابع یک مسیر تنظیم می‌شود، و یک تایمر t برای آن برابر با مدت زمان دوره پایداری شبکه تنظیم می‌شود.

گام ۲. چاهک منتظر می‌شود تا t=0 شود. هرگاه t=0 شد به گام بعد می‌رود.

گام ۴. قابلیت اطمینان با استفاده از راهکار پیشنهاد شده در فصل قبل برای مسیرهای فعال تخمین زده می‌شود سپس به گام بعد می‌رود.

گام ۵. اگر قابلیت اطمینان بدست آمده کوچک‌تر از $R_D - \propto$ باشد چاهک در میان مسیرهایی که غیر فعال هستند جستجو می‌کند و بهترین مسیر را انتخاب می‌کند (نحوه انتخاب بهترین مسیر در ادامه بیان می‌شود). یک بسته از نوع Ack-live-path که فیلد مربوط به فعال بودن مسیر برای آن ۱ تنظیم —شود؛ در مسیر عقبگرد برای منبع مورد نظر ارسال می‌کند. منبع با دریافت این بسته مسیر مورد نظر را فعال می‌کند و از این به بعد یک نسخه از بسته‌ها را روی این مسیر نیز ارسال می‌کند. سپس به گام ۴ می‌رود. در این مرحله اگر هیچ مسیری پیدا نشود نشان دهنده این است که همه مسیرهای موجود فعال هستند و با وجود این مسیرها قابلیت اطمینان مورد انتظار نمی‌تواند ارضا شود؛ در این حالت به گام ۸ می‌رود.



شکل ۱۱ : فلوچارت عملکرد و تصمیم‌گیری چاهک در AMPRS

گام ۳. چاهک قابلیت اطمینان شبکه در دوره قبلی تصمیم‌گیری چاهک را محاسبه می‌کند. قابلیت اطمینان به صورت نسبت بسته‌های دریافتی به ارسالی که توسط همه منابع ارسال می‌شود محاسبه می‌گردد، سپس به گام ۵ می‌رود.

گام ۶. اگر قابلیت اطمینان بدست آمده بزرگ‌تر از مقدار $R_D + \propto$ باشد چاهک در میان مسیرهایی که فعال هستند مسیری که کمترین تأثیر را در قابلیت اطمینان دارد انتخاب می‌کند در واقع بدترین مسیر را انتخاب می‌کند. مسیر انتخاب شده را به صورت موقت غیرفعال در نظر گرفته می‌شود. قابلیت اطمینان با توجه به راهکار پیشنهاد شده در بخش قبل برای مسیرهای فعال موجود تخمین زده می‌شود، که در اینجا دو حالت پیش می‌آید:

اگر مقدار بدست آمده از $R_D - \propto$ کوچک‌تر باشد، مسیر مجدداً فعال می‌شود و به گام ۸ می‌رود. این امر نشان دهنده این است که با شرایط موجود حداقل قابلیت اطمینانی که بدست آمده نمی‌تواند کمتر از این مقدار باشد.

در غیر این صورت یک بسته از نوع Ack- live-path برای منبع مربوطه در مسیر عقبگرد ارسال می‌شود که در فیلد مربوط به فعال بودن مسیر مقدار ۱ تنظیم می‌شود. منبع با دریافت این بسته و بررسی آن متوجه می‌شود که باید بسته‌های داده را روی این مسیر ارسال نکند و چاهک نیز جدول Info-Source خود را بروزرسانی می‌کند. سپس به گام ۴ می‌رود.

در این مرحله اگر هیچ مسیری بدست نیاید نشان دهنده این است که قابلیت اطمینان از این کمتر نمی‌تواند باشد و به گام ۸ می‌رود.

گام ۷. اگر قابلیت اطمینان محاسبه شده کوچک‌تر از $R_D - \propto$ و بزرگ‌تر از $R_D + \propto$ باشد، بیانگر این که قابلیت اطمینان شبکه در دامنه مورد نظر است و نیاز به هیچ‌گونه تغییری نیست. به گام ۸ می رود.

گام ۸. تایمر دوباره تنظیم می‌شود. به گام ۲ می‌رود.

این الگوریتم توسط چاهک در دوره‌های تصمیم‌گیری چاهک تکرار می‌شود و در هر مرحله بر اساس شرایط شبکه مسیرها برای منابع تعیین می‌شود. مراحل الگوریتم به صورت خلاصه در فلوچارت شکل ۴-۱۲ نمایش داده شده است.

نحوه انتخاب مسیر هنگام افزایش یا کاهش مسیرها: به هر یک از مسیرها یک وزن اختصاص داده می‌شود. وزن‌های اختصاص داده شده بر اساس پارامترهای زیر محاسبه می‌شود:

قابلیت اطمینان: هم می‌توان از قابلیت اطمینان مسیرها و هم از قابلیت اطمینان تخمین زده شده در صورت اضافه یا کم کردن مسیرها برای مقایسه استفاده کرد.

انرژی باقیمانده مسیر

تعداد گام‌های مسیر

$$W_i = R_i + \left(\frac{E_i}{E} \times \frac{1}{C_i}\right)$$

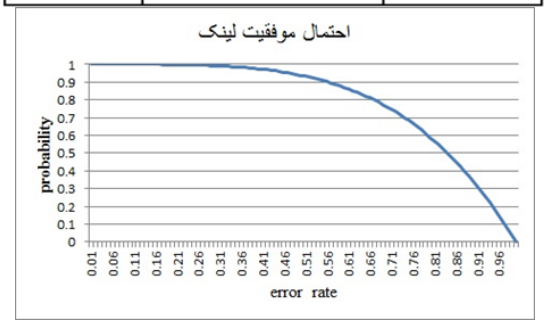
$$W_i = RL_i + \left(\frac{E_i}{E} \times \frac{1}{C_i}\right)$$

در فرمول‌های بالا W_i وزن بدست آمده را برای مسیر i ام، E_i انرژی باقی مانده روی مسیر i ام، E انرژی اولیه را برای گره‌ها، R_i قابلیت اطمینان مسیر i ام، RL_i قابلیت اطمینان تخمین زده شده که با اضافه یا کم کردن مسیر i ام بدست می‌آید و C_i تعداد گام‌های مسیر i ام را نشان می‌دهد. مسیری که بیشترین وزن را داشته باشد به عنوان بهترین مسیر انتخاب می‌شود. نحوه محاسبه وزن‌ها سبب می‌شود مسیرهایی انتخاب شوند که قابلیت اطمینان را افزایش دهند، سبب توزیع بار در شبکه شود و طول عمر شبکه را افزایش دهد.

برای انتخاب بدترین مسیر هنگامی در میان مسیرهایی فعال مسیری انتخاب می‌شود که از جریان انتقال داده حذف شود، با توجه به وزن‌ها مسیری انتخاب می‌شود که کمترین وزن را داشته باشد.

جدول ۲ : مشخصات پارامترهای شبیه سازی

	Energy Model			



نمودار ۷: احتمال موفقیت لینک‌ها با توجه به نرخ خطا

نحوه پیاده سازی و ارزیابی: خطاها می‌تواند قبل از ارسال بسته به کانال یا بعد از دریافت از کانال اعمال شوند که در اینجا قبل از ارسال به کانال اعمال می‌شود. در شبیه‌سازی‌های انجام شده مقدار rate_ را از ۳۰ درصد تا ۷۰ درصد تغییر می‌دهیم و پارامترهای لازم را بر طبق تغییر هر مقدار rate_محاسبه می‌کنیم. در IEEE802.11 برای ارسال هر بسته به گره بعدی حداکثر ۴ بار تلاش می‌شود؛ لذا با توجه به مقدار rate_می‌توان احتمال موفقیت لینک را با استفاده از معادله زیر محاسبه کرد. اگر مقدار rate_ برابر با q باشد آنگاه احتمال موفقیت لینک (P) به صورتی که در معادله ۶-۸ نشان داده شده است محاسبه می‌شود.

$$P = (1-q) + q(1-q) + q(1-q)^2 + q(1-q)^3$$

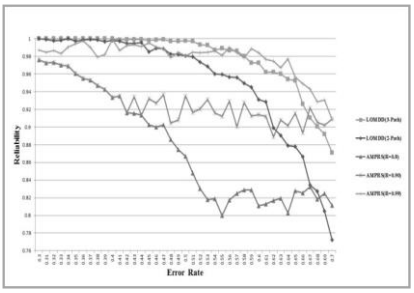
رابطه بین مقدار rate_و احتمال موفقیت لینک نشان داده شده است. به طور مثال در این شکل مشاهده می‌شود برای مقادیر کمتر از ۳۰ درصد از rate_ هنوز احتمال موفقیت لینک تقریباً برابر ۱۰۰ درصد است، چون در لایه MAC، ۴ بار برای ارسال هر بسته تلاش می‌شود.

نتایج شبیه‌سازی: در این قسمت نتایج شبیه‌سازی برای هر یک از سناریوهای مطرح شده در قسمت قبل آورده شده و نمودار مربوط به نتایج بدست آمده، نشان داده شده است.

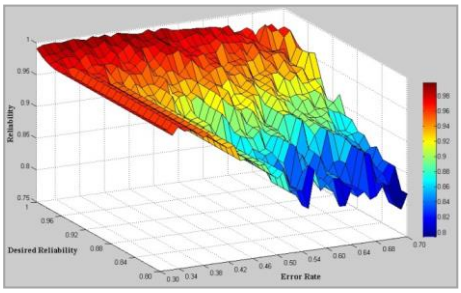
قابلیت اطمینان: نتایج حاکی از این است که پروتکل AMPRS همواره سعی می‌کند قابلیت اطمینان را در محدوده قابلیت اطمینان مورد انتظار نگه دارد. نتایج حاکی از تطبیق پذیری بسیار بالای AMPRS با شرایط شبکه می‌باشد . قابلیت اطمینان همواره در محدوده قابلیت اطمینان مورد انتظار شبکه نگه داشته می‌شود و با افزایش نرخ خطا تغییرات لازم انجام می‌شود.

مشاهده می‌شود با افزایش درصد خطای شبکه و قابلیت اطمینان مورد انتظار، AMPRS قابلیت اطمینان را در محدوده مورد نظر نگه می‌دارد. در این شکل مشاهده می‌شود که استفاده از تعداد مسیرهای ثابت در بیشتر مواقع کارا نمی‌باشد. در نمودارهای مربوط به استفاده از تعداد مسیرهای ثابت، با افزایش نرخ خطا مشاهده می‌شود که قابلیت اطمینان به تدریج کاهش پیدا می‌کند. کاهش قابلیت اطمینان سبب می‌شود که قابلیت اطمینان مورد انتظار شبکه ارضا نشود. همچنین در زمان‌هایی که نرخ خطا پایین است مشاهده می‌شود که استفاده از مسیرهای ثابت قابلیت اطمینان بسیار بالاتری نسبت به قابلیت اطمینان مورد انتظار را برآورده می‌کند؛ این مقدار غیر ضروری است. در بخش‌های بعدی خواهیم دید که استفاده از مسیرهای ثابت سربار زیادی بی‌جهت به شبکه اعمال می‌شود. به طور مثال اگر عملکرد پروتکل AMPRS برای حالتی که قابلیت اطمینان مورد انتظار ۹۰ درصد (AMPRS(R=0.90)) باشد در نظر بگیریم، با توجه به شکل برای نرخ خطای بین ۳۰ تا ۳۸ درصد قابلیت اطمینان بدست آمده بیشتر از قابلیت اطمینان مورد انتظار (یعنی ۹۰ درصد) می‌باشد. این امر بدین دلیل است که حداقل قابلیت اطمینان بدست آمده نمی‌تواند از این مقدار کمتر شود. برای نرخ خطاهای بزرگ‌تر از ۳۰ درصد برای این حالت، قابلیت اطمینان همواره حول وحوش ۹۰ درصد نگه داشته می‌شود. اگر حالت (AMPRS(R=0.90)) با حالتی که از ۲ مسیر ثابت (LOMDD(2-Path) استفاده شده است مقایسه شود، مشاهده می‌شود که در LOMDD با دو مسیر ثابت قابلیت اطمینان بدست آمده برای نرخ‌های خطای کمتر از ۶۲ درصد، خیلی بیشتر از مقدار قابلیت اطمینان مورد انتظار است. همچنین برای نرخ‌های بالاتر از ۶۲ درصد نیز نمی‌تواند قابلیت اطمینان مورد انتظار را ارضا کند.

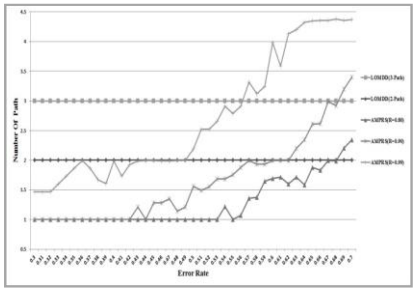
با توجه به نتایج بدست آمده می‌توان گفت که پروتکل AMPRS یک انتخاب مناسب برای ارضای قابلیت اطمینان مورد انتظار در شبکه‌های حسگر بی‌سیم می‌باشد.



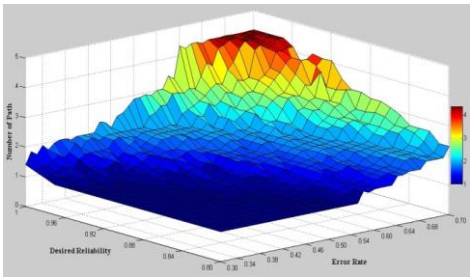
نمودار ۸ : مقایسه قابلیت اطمینان AMPRS در حالت‌های مختلف با LOMDD در حالت استاتیک



شکل ۱۲: تطبیق پذیری قابلیت اطمینان در AMPRS با تغییرات قابلیت اطمینان مورد انتظار و نرخ خطا



نمودار ۹: مقایسه تعداد مسیرهای استفاده شده در AMPRS با LOMDD



شکل ۱۳: تطبیق پذیری تعداد مسیر انتخاب شده در AMPRS با تغییرات قابلیت اطمینان مورد انتظار و نرخ خطا

تعداد میانگین مسیرها: نتایج حاکی از این است که پروتکل AMPRS همواره حداقل تعداد مسیر را با توجه به محدودیت‌های خواسته شده و شرایط شبکه برای ارسال داده‌ها توسط منابع در نظر می‌گیرد. مشاهده می‌شود که برای نرخ‌های پایین خطا تنها یک مسیر تنظیم می‌شود و نیازی به استفاده از مسیرهای بیشتر نیست. با افزایش تعداد نرخ خطا و افزایش قابلیت اطمینان مورد انتظار نیاز به استفاده از مسیرهای بیشتری می‌باشد. AMPRS همواره سعی می‌کند تعداد مسیر بهینه را برای منابع انتخاب کند. اگر عملکرد پروتکل AMPRS را برای حالتی که قابلیت اطمینان مورد انتظار ۹۹ درصد (AMPRS(R=0.99))

می‌باشد را با حالتی که از ۳ مسیر ثابت (((LOMDD(3-Pathبرای ارسال داده‌ها استفاده شده است مقایسه شود. در پروتکل AMPRS برای نرخ خطای کمتر از ۵۸ درصد از تعداد مسیر کمتری استفاده می‌شود و نیازی به استفاده از مسیرهای بیشتر نیستAMPRS . برای همین حالت ((AMPRS(R=0.99) قابلیت اطمینان مورد انتظار را نیز برآورده می‌کند؛ لذا نیازی به استفاده از مسیرهای بیشتر نیست. همچنین قابل مشاهده با افزایش نرخ خطا تعداد مسیرهای استفاده شده، از حالتی که از ۳ مسیر ثابت استفاده می‌شود بیشتر است که این بدین دلیل است که برای ارضای قابلیت اطمینان نیاز به مسیرهای بیشتری است. برای حالتی که قابلیت اطمینان ۹۹ درصد باشد برای نرخ خطای بیشتر از ۵۸ درصد APMRS قابلیت اطمینان را در محدوده قابلیت اطمینان مورد انتظار نگه می‌دارد در حالی که قابلیت اطمینان LOMDD با ۳ مسیر ثابت به شدت افت می‌کند.

با توجه به نتایج بدست آمده می‌توان گفت که پروتکل AMPRS یک انتخاب مناسب برای تعیین تعداد مسیرهای لازم جهت ارضای محدودیت‌ها در شبکه‌های حسگر بی‌سیم می‌باشد.

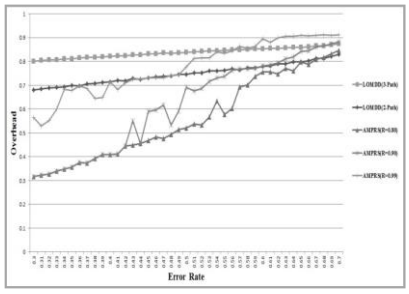
سربار شبکه: نتایج حاکی از این است که پروتکل AMPRS حداقل سربار ممکن را به شبکه اعمال می‌کند و از اعمال سربار اضافی جلوگیری می‌کند. AMPRS سربار شبکه را مطابق شرایط شبکه تنظیم می‌کند و از اعمال سربار اضافی به شبکه جلوگیری می‌کند. برای نرخ خطاهای پایین و قابلیت اطمینان مورد انتظار پایین حداقل سربار ممکن به شبکه تحمیل می‌شود که ناشی از خطاهایی است که در لایه MAC به بسته‌ها اعمال می‌شود. با افزایش نرخ خطا و قابلیت اطمینان مورد انتظار مشاهده می‌شود که سربار شبکه نیز تغییر می‌کند. در AMPRS همواره سعی می‌شود که کمترین سربار ممکن به شبکه اعمال شود.

با حالتی که از ۳ مسیر ثابت (((LOMDD(3-Pathبرای ارسال داده‌ها استفاده شده است مقایسه کنیم قابل مشاهده است که این حالت همواره سربار زیادی را به شبکه تحمیل می‌کند که در بیشتر مواقع این سربار اضافی می‌باشد. تنها در مواردی که نرخ خطا خیلی بالا و قابلیت اطمینان مورد انتظار نیز خیلی بالا باشد سربار ناشی از پروتکل AMPRS به اندازه سربار LOMDD با ۳ مسیر ایستا ((LOMDD(3-Pathمی‌شود.

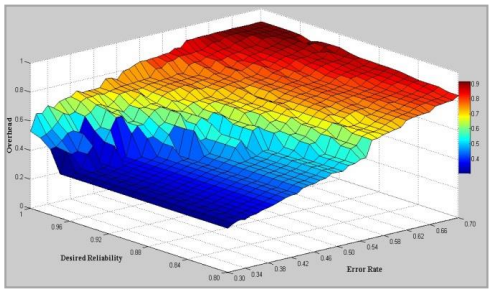
اگر عملکرد پروتکل AMPRS را برای حالتی که قابلیت اطمینان مورد انتظار ۹۰ درصد ((AMPRS(R=0.90) باشد، با حالتی که از ۳ مسیر ثابت ((LOMDD(3-Pathبرای ارسال داده‌ها استفاده شده است، مقایسه شود. AMPRS همواره نسبت به LOMDD با ۳ مسیر ثابت سربار کمتری را به شبکه تحمیل می‌کند. تنها در مقادیر بالا از نرخ خطا میزان سربارها یکسان است. با تطبیق این حالت مشاهده می‌کنیم که AMPRS با حداقل سربار ممکن قابلیت اطمینان مورد انتظار را بر آورده می‌کند در حالی که استفاده از مسیرهای ثابت اگرچه قابلیت اطمینان را بر آورده می‌کند ولی سربار زیادی را بی‌جهت به شبکه تحمیل می‌کند.

با توجه به نتایج بدست آمده می‌توان گفت که پروتکل AMPRS یک انتخاب مناسب برای ارضای قابلیت تنظیم سربار وارد شده در شبکه‌های حسگر بی‌سیم می‌باشد که باعث کاهش مصرف انرژی و افزایش طول عمر شبکه می‌شود.

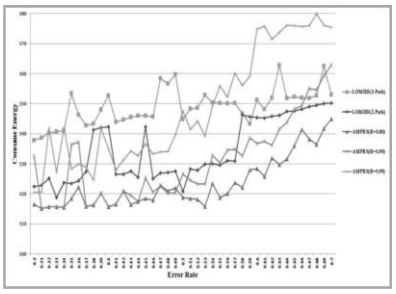
انرژی مصرف شده: نمودارهای مربوط به انرژی مصرف‌شده .نتایج حاکی از این است که پروتکل AMPRS انرژی مصرف شده در شبکه را با توجه به محدودیت‌های خواسته شده مینیمم می‌کند و از مصرف انرژی بی جهت در شبکه جلوگیری می‌کند. به طور مثال اگر عملکرد پروتکل AMPRS برای حالتی که قابلیت اطمینان مورد انتظار ۹۰ درصد باشد را با حالتی که از ۳ مسیر ثابت ((LOMDD(3-Pathبرای ارسال داده‌ها استفاده شده است مقایسه شود قابل مشاهده است که انرژی مصرف شده در AMPRS(R=0.90) همواره انرژی کمتری را مصرف می‌کند. در شکل قابل مشاهده است که در بقیه حالات نیز این چنین است.



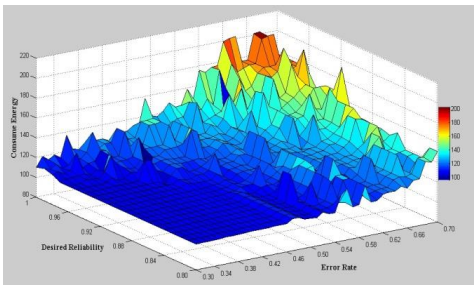
نمودار ۱۰: مقایسه سربار ناشی از مسیرها در AMPRS



شکل ۱٤: سربار اعمال شده به شبکه در AMPRS با تغییرات قابلیت اطمینان مورد انتظار و نرخ خطا



نمودار ۱۱: میانگین انرژی مصرف شده گره‌ها در AMPRS



شکل ۱۵: انرژی مصرف شده در AMPRS با تغییرات قابلیت اطمینان مورد انتظار و نرخ خطا

۵- بحث و نتیجه گیری

امروزه استفاده از شبکه های بی سیم با توجه به گستردگی دامنه کاربردی و سهولت استفاده جایگاه ویژه ای را یافته است. از مسائل مهمی که در حوزه شبکه های بی سیم توجه محققان را به خود جلب کرده است چگونگی انتقال اطلاعات از گره های داخلی شبکه به ایستگاه اصلی و برگزیدن بهترین مسیر ممکن برای انتقال اطلاعات است به نحوی که مصرف انرژی سیستم بهینه باشد و انتقال داده با بالاترین درجه اطمینان و امنیت صورت گیرد.

نتایج شبیه‌سازی حاکی از افزایش قابلیت اطمینان و کاهش شدید سربار مسیریابی، با توجه به راهکاری که در این پروتکل بکار رفته است، می‌باشد.

مقایسه پروتوکل پیشنهادی با چند پروتوکل دیگر مسیریابی: استفاده از پروتکل مناسب برای شبکه حسگر بیسیم از ابتدای ایجاد این نوع از شبکه به عنوان یکی از مهمترین مباحث مطرح در این زمینه بوده است و پژوهشگران بسیاری با بررسی قابلیتهای این شبکه و تلفیق آنها با تئوریهای مطرح در علوم مختلف سعی در رسیدن به یک پروتکل مناسب و کارآمد در این خصوص دارند . با گذشت زمان با استفاده از تلفیق الگوریتم ها و روش‌های گوناگون این پروتوکل ها دچار تغییرات اساسی شده و درنتیجه بهبود یافته اند. این تغییرات و تکامل باعث گردیده که شبکه حسگر بیسیم یکی از مهمترین موارد مورد آزمایش و تحقیق در علوم مختلف باشد.

پروتکل‌های مبتنی بر داده: مسیریابی در این شبکه ها، به جای آنکه مبتنی بر آدرس باشد مبتنی بر داده است .یعنی ما بیشتر دنبال گره هایی هستیم که اطلاعات خاصی را دارند بر خلاف حالت سنتی که در مسیریابی غالباً به دنبال گرهای با شناسه خاص هستیم .در پروتکلهای مبتنی بر داده، گره چاهک پرس و جوهای خود را به مناطق مورد نظر خود میفرستد و منتظر میشود تا داده ها از حسگرهایی که در آن ناحیه قرار دارند، باز گردند .بنابراین در این روش مشخصات یک حسگر مهمتر از آدرس آن میباشد . این مشخصات شامل مکان حسگر، پارامترهایی که حسگر میتواند اندازه بگیرد و ... میباشند

پروتکلهای سلسله مراتبی: هدف اصلی پروتکلهای سلسله مراتبی در واقع بکارگیری یک روش مناسب جهت استفاده بهینه از منابع انرژی میباشد . در این شبکه مانند شبکه های مخابراتی دیگر، قابلیت مقیاس پذیری شبکه یکی از مهمترین پارامترهای طراحی در شبکه های حسگر بیسیم میباشد .اگر قرار باشد که تمامی بار شبکه روی یک یا چند مسیر خاص باشد، با گسترش شبکه حجم ترافیک درشبکه به شدت افزایش یافته و در نتیجه با بالا رفتن تاخیر، کارایی شبکه افت خواهد کرد .برای بالا بردن قابلیت پوشش مناطق بزرگتر بدون اینکه مشکلی در کیفیت سرویس شبکه بوجود آید، تقسیم بندی شبکه به چند خوشه پیشنهاد شده است. با هدف مصرف بهینه انرژی از ارسال بصورت چند گامی در درون یک گروه و همچنین ترکیب اطلاعات یک گروه به جهت کم کردن دادههای ارسالی صورت میگیرد .پروتکل لیچ یکی از اولین پروتکلهای سلسله مراتبی بود که برای شبکههای حسگر بیسیم معرفی شد. دیگر پروتکلها بر مبنای آن طراحی شدند.

پروتکلهای مبتنی بر موقعیت مکانی: بسیاری از پروتکلهای مسیریابی برای شبکه های حسگر بیسیم، به اطلاعات مکانی حسگرها نیاز دارند .در موارد متعددی این اطلاعات برای محاسبه فاصله بین حسگرها به منظور تخمین مقدار انرژی مورد نیاز برای ارسال داده ها به کار گرفته میشوند .با توجه به اینکه هیچ شمای آدرسدهی اساسی مثل IP در شبکه های حسگر بیسیم وجود ندارد، اطلاعات جغرافیایی میتواند کمک شایانی برای استفاده کارآمد از انرژی باشد .به این معنی که اگر حسگرها مکان خود را بدانند، درخواست گره چاهک میتواند فقط به آن منطقه ای ارسال شود که مورد نظر است و بدین صورت از حجم اطلاعات ارسالی تا حد زیادی کاسته میشود .برخی از پروتکلهای این دسته در ابتدا برای شبکه های اقتضایی طراحی شدهاند ولی با این وجود در شبکه های حسگر بیسیم نیز کاربرد دارند .برخی از پروتکلهایی که برای شبکه های اقتضایی طراحی شدهاند برای شبکه های حسگر بیسیم مناسب نیستند، زیرا در طراحی آنها انرژی حسگرها مورد توجه قرار نگرفته است

در مقایسه با پروتکلهای مسیریابی سنتی و قدیمی، پروتکلهای مسیریابی شبکه های حسگر بیسیم قابلیتها و نیازمندیهای جدیدی را طلب می کنند از جمله:

اولویت انرژی: انرژی گره محدود است .این یک هدف مهم در طراحی پروتکل مسیریابی جهت توسعه و افزایش زمان حیات شبکه است.

داده محور بودن: ارسال داده را کاهش می دهد و نیز بعلت هم آمیزی داده، کاهش افزونگی اطلاعات را شاهد هستیم.

بر اساس توپولوژی محلی :جهت ذخیره سازی انرژی ارتباطی، از روش ارتباطی چند پرشه استفاده می شود .گره قادر به ذخیره سازی حجم زیادی از اطلاعات مسیریابی نیست، همچنین مسیریابی نمیتواند و نباید محاسبات پیچیده انجام دهد و مکانیزم مسیریابی میبایست ساده و کارآمد باشد.

مقیاس پذیر توپولوژی شبکه‌ای پویا :پروتکلهای مسیریابی از روش کاربری توزیع شده استفاده می کنند و نیز باید جهت بسط در شبکه، راحت و آسان باشند.

تحمل پذیری خرابی :ایجاد خرابی در گره و یا خرابی به علتهای گوناگون نباید در مکانیزم عملکردی مسیریابی خللی ایجاد کند .بدین معنی که پروتکل باید تحمل پذیر در مقابل خرابی باشد.

همگرایی سریع: الگوریتم مسیریابی میبایست ساده بوده و قابلیت سازگاری با تغییر توپولوژی پویا در شبکه را داشته باشد. همچنین هزینه های ارتباطی را کاهش داده و کارائی ارسال را بهبود بخشد.

امنیت :محافظت و مراقبت از دزدی و جعل داده توسط پروتکل انجام پذیرد .پروتکل مسیریاب میبایست امنیت مناسبی را فراهم آورد. (کارپ، ۲۰۲۰)

بر اساس نتایج پژوهش حاضر راهکار پیشنهاد شده مبتنی بر OBDD برای تخمین قابلیت اطمینان در شبکه‌های حسگر بی‌سیم به عنوان یک راهکار بازگشتی است با کاهش محاسبات اضافی و حذف زیر گراف‌ها توانست الگوریتمی کارا از نظر قابلیت اطمینان را پینهاد کند.

نتیجه حاصل از تحلیل و شبیه سازی بعد از ساخته شدن گراف مربوطه با توجه به قانون شانون و با پیمایش از ریشه دقت بالای راهکار پیشنهادی را نشان داد.

در پروتکل AMPRS الگوریتم هایی پیشنهاد شد که در حالیکه قابلیت اطمینان مورد انتظار شبکه را براورده کند سربار ارسال بسته‌ها نیز افزایش نیابد ، همچنین مصرف انرژی کاهش و طول عمر شبکه نیز بالا رود.

LOMDD یک مسیر را به عنوان مسیر اصلی انتخاب می کند و سایر مسیرها به عنوان جایگزین انتخاب می‌شوند. در این پژوهش پروتکل AMPRS با هدف تعیین تعداد مسیرها برای هر یک از منابع طراحی شد. چاهک بر اساس اطلاعاتی که در دوره‌های زمانی از شبکه بدست می‌آورد تصمیم می‌گیرد که هر یک از منابع از چه مسیرهایی و چند مسیر برای ارسال اطلاعات استفاده کنند.

نتایج شبیه‌سازی حاکی از تطبیق بسیار بالای AMPRS با شرایط شبکه می‌باشد و نشان داده شد که نسبت به پروتکل‌های ایستا قابلیت اطمینان را به صورت کارا برای شبکه تنظیم می‌کند، سربار محاسباتی و انرژی مصرف شده را کاهش می‌دهد و همچنین تعداد مسیر بهینه را برای منابع تعیین می‌کند.

واعظی و همکاران در سال ۱۴۰۰ به وسیله پروتکل مسیریابی جدید مبتنی بر کیفیت خدمات (QoS) در شبکه های حسگر بیسیم میانگین تأخیر را حدود ۳۰٪ در شبکه های با مقیاس بزرگ بهبود دادند. نوری و زینالی در سال ۱۳۹۹ مدلی معرفی کردند که به صورت فراگیر باعث کاهش نفوذ نفوذگر برای تضعیف عملکرد شبکه و جلوگیری از حملات فریبکارانه توسط مهاجمان می گردد. بهروان و همکاران در سال ۱۳۹۹ پروتکل کارامد EEMCA را معرفی کردند. القحطانی در سال ۲۰۲۱ پروتکل مسیریابی با استفاده از چند مسیر (IQMRP) را معرفی کرد. جیا در سال ۲۰۲۱ بیان کرد در پروتکل SEP-EC پیشنهاد شده متوسط تأخیر سرتاسر ۰,۵۲ ثانیه است و میانگین گره های باقی مانده ۸۳,۵ درصد است. لیانگ و همکاران در سال ۲۰۲۱ الگوریتم مسیریابی تعاونی تطبیقی جدید همراه با DEEC را پیشنهاد دادند. شن و همکاران در سال ۲۰۲۰ شبکه EECRP با طول عمر بیشتر معرفی کردند. ژِیکسین و همکاران در سال ۲۰۱۹ یک پروتکل بنام DETR ارائه دادند.

تا کنون پژوهش های بسیاری در جهت یافتن پروتوکل مناسب انجام شده است. گرچه بسیاری از این تلاش ها منجر به ارائه پروتوکل هایی بهینه شده اند با این حال در مقایسه با سایر پژوهش های انجام شده، پروتکل AMPRS با قابلیت اطمینان مورد انتظار ۹۰ درصد پروتکلی مطمئن تر به حساب می آید.

با توجه به مزیت های استفاده از شبکه های حسگر بی سیم برطرف کردن مشکلات موجود و ارائه راهکارهای بهتر همچنان مورد توجه م یباشد لذا به منظور پژوهش های اتی ،گسترش LOMDD برای توزیع بار در میان مسیرهای موجود، گسترش LOMDD برای توزیع بار در میان مسیرهای موجود با استفاده از کدینگ پیشنهاد می شود.

همچنین با اهدف بهینه سازی مساله قالیت اطمینان میتوان شبکه ای را مدل کرد که مسیرهای مورد نظر را بر اساس افزایش طول عمر شبکه و کاهش انرژی مصرف شده انتخاب کند به نحویکه قابلیت اطمینان مورد انتظار نیز برآورده شود.

همچنین میتوان مسیرهای موجود در شبکه را به گونه ای تقسیم کرد که از هرکدام از ان ها در بازه زمانی خاص و به مدت مشخصی استفاده شود تا علاوه بر تامین قابلیت اطمینان مورد انتظار ، افزایش طول عمر شبکه را موجب شود.

و به عنوان راهکار سوم استفاده از یک کدینگ به جای کپی بسته‌ها پیشنهاد میشود.

منابع

۱. کرد افشاری محمد صادق؛ موقر رحیم آبادی علی، میبدی محمد رضا؛ (۱۳۹۸)؛ مسیریابی چندپخشی در شبکه های حسگر بیسیم مقیاس وسیع با استفاده از چارچوب یادگیری تقویتی توزیع شده؛ پژوهش های نوین در ریاضی؛ سال پنجم، شماره بیستم، مهر و آبان ۱۳۹۸.

۲. طهماسبی کهیانی ، (۱۳۹۱) ، فیوژن داده در شبکه های حسگر بیسیم. دومین کنفرانس ملی مهندسی نرم افزار لاهیجان، دانشگاه آزاد اسلامی واحد لاهیجان.

۳. نوری حسن، زینالی خسرقی؛ (۱۳۹۹)؛ ارزیابی کارآیی پروتکل های مسیریابی چند مسیره در تضمین امنیت و حریم خصوصی شبکه های حسگر بی سیم؛ پنجمین کنفرانس ملی محاسبات توزیعی و پردازش داده های بزرگ.

۴. بهروان کبری، منصفی رضا، احمدی ترشیزی حسن؛ (۱۳۹۹)؛ پروتکل مسیریابی چندپرشه انرژی- کارآمد در شبکه های حسگر بیسیم مبتنی بر خوشه با استفاده از بهینه سازی کلونی مورچه؛ مجله فناوری اطلاعات در طراحی مهندسی؛ دوره پنجم، شماره دوم.

5. Alqahtani Abdulrahman Saad. (2021). Improve the QoS using multi-path routing protocol for Wireless Multimedia Sensor Network, Elsevier, nvironmental Technology & Innovation, Volume 24, November 2021, 101850
6. AboElFotoh H. M. F., E. S. ElMallah, and H. S. Hassanein, "On The Reliability of Wireless Sensor Networks," in Communications, 2016. ICC '06. IEEE International Conference on, 2016, pp. 3455-3460.
7. Dulman. S, T. Nieberg, J. Wu, P. Havinga; “Trade-Off between Traffic Overhead and Reliability in Multi-path Routing for Wireless Sensor Networks”, WCNC Workshop, 2016.
8. Jia Lanfang. (2021). Distributed energy balance routing algorithm for wireless sensor network based on multi-attribute decision-making, Sustainable Energy Technologies and Assessments Volume 45, June 2021, 101192
9. Liang Jiale., ZhenyueXu,. YananXu,. WenZhou,. ChunguoLib. (2021). Adaptive cooperative routing transmission for energy heterogeneous wireless sensor networks, Elsevier, Physical Communication, Volume 49, December 2021, 101460
10. B. Karp and H. T. Kung, “GPSR: Greedy perimeter stateless routing for wireless sensor networks,” in Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '11), Boston, MA, August 2020