New Researches in the Smart City
Vol 2 (Issue 4), 46-71
nrsc.apadana.ac.ir

Apadana Institute of Higher Education

Enhancing Reliability in Wireless Sensor Networks Using Multipath Routing Protocols

Reza Erfani
Master's Student, Faculty of Electrical and Computer Engineering, Islamic Azad University, Zahedshahr Branch, Iran.

Seyed Ebrahim Dashti *
Assistant Professor, Faculty of Electrical and Computer Engineering, Islamic Azad University, Jahrom Branch, Iran.

Received: 06/April/2024
Accepted: 31/August/2024
eISSN: 3060-6144
ISSN: 2980-8936

Abstract

With the increasing application of the Internet of Things, the use of wireless sensor networks for monitoring and control has expanded. One of the most critical topics in data transmission within these networks is developing solutions for selecting the best possible path for data transmission to minimize energy consumption and maximize network lifespan. However, significant challenges remain in data transmission. This study aims to enhance reliability in wireless sensor networks using multipath routing protocols. Initially, the multipath routing protocol LOMDD was designed based on the Directed Diffusion protocol. The TPP filter was selected for the LOMDD multipath routing protocol design, and the necessary implementations were carried out using the NS2 simulator. Subsequently, a solution for estimating reliability using an Ordered Binary Decision Diagram (OBDD) was proposed. Finally, an adaptive multipath protocol for ensuring reliability, AMPRS, based on LOMDD, was introduced. Simulation results indicate that AMPRS adapts exceptionally well to network conditions and effectively adjusts reliability for the network compared to static protocols, reduces computational overhead and energy consumption, and determines the optimal number of paths for resources. The performance of the AMPRS protocol, with an expected reliability of 90%, demonstrates a more reliable protocol compared to other studies.

Keywords: wireless sensor network, data transmission, multipath routing protocols, LOMDD protocol, AMPRS protocol

* Corresponding Author: sayed.dashty@gmail.com

فصلنامه پژوهش‌های نوین در شهر هوشمند
دوره ۲، شماره ۴، تابستان ۱۴۰۳، ۴۶-۷۱
nrsc.apadana.ac.ir

تاریخ دریافت: ۱۴۰۳/۰۱/۱۸ تاریخ پذیرش: ۱۴۰۳/۰۶/۱۰ eISSN: 3060-6144 ISSN: 2980-8936

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

رضا عرفانی دانشجوی کارشناسی ارشد، دانشکده برق و کامپیوتر، دانشگاه آزاد اسلامی، واحد زاهدشهر، زاهدشهر، ایران.

سید ابراهیم دشتی * استادیار گروه کامپیوتر، دانشکده برق و کامپیوتر، دانشگاه آزاد اسلامی، واحد جهرم، جهرم، ایران.

چکیده

با افزایش کاربرد اینترنت اشیاء، استفاده از شبکه حسگر بی‌سیم برای نظارت و کنترل افزایش یافته است. از مهم‌ترین مباحث حوزه انتقال داده در این شبکه‌ها، ارائه راهکارهایی جهت انتخاب بهترین مسیر ممکن برای انتقال اطلاعات است به‌نحوی که انرژی مصرفی در کمترین و طول عمر شبکه در بیشترین میزان باشد. با وجود این، مشکلات عمده‌ای در مبحث انتقال داده وجود دارد. پژوهش حاضر به‌منظور افزایش قابلیت اطمینان در شبکه‌های حسگر بی‌سیم با استفاده از پروتکل‌های مسیریابی چند مسیره صورت گرفته است. لذا، ابتدا پروتکل مسیریابی چند مسیره LOMDD بر مبنای پروتکل انتشار هدایت‌شده طراحی شد. برای طراحی پروتکل مسیریابی چند مسیره LOMDD، فیلتر TPP انتخاب شد که پیاده‌سازی‌های لازم بر روی این فیلتر و تحت شبیه‌ساز NS2 صورت پذیرفت. سپس، یک راهکار برای تخمین قابلیت اطمینان با استفاده از دیاگرام تصمیم‌گیری دودویی مرتب‌شده پیشنهاد شد. درنهایت، یک پروتکل چند مسیره تطبیقی برای اقناع قابلیت اطمینان AMPRS مبتنی بر LOMDD معرفی شد. نتایج شبیه‌سازی حاکی از تطبیق بسیار بالای AMPRS با شرایط شبکه بوده و نشان داده شد که نسبت به پروتکل‌های ایستا، قابلیت اطمینان را به‌صورت کارا برای شبکه تنظیم می‌کند، سربار محاسباتی و انرژی مصرف‌شده را کاهش می‌دهد و همچنین، تعداد مسیر بهینه را برای منابع تعیین می‌کند. عملکرد پروتکل AMPRS با قابلیت اطمینان مورد انتظار ۹۰ درصد نشان از پروتکلی مطمئن‌تر در مقایسه با سایر پژوهش‌ها دارد.

کلیدواژه‌ها: شبکه حسگر بی‌سیم، انتقال داده، پروتکل‌های مسیریابی چند مسیره، پروتکل LOMDD، پروتکل AMPRS

* نویسندهٔ مسئول: sayed.dashty@gmail.com

مقدمه

شبکه حسگر بی‌سیم به‌عنوان موضوعی نوین و بسیار بااهمیت در حوزه فناوری اطلاعات مطرح است. این شبکه‌ها به‌صورت مستقل و بدون دخالت فعالیت می‌کنند و بهترین گزینه برای حالت‌هایی هستند که ما به محیط هدایت‌شده دسترسی نداشته باشیم (کیهانی، ۱۳۹۱). شبکه حسگر بی‌سیم متشکل از صدها یا هزاران حسگر به‌صورت گره بوده که در اطراف عامل فیزیکی موردنظر 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، به‌صورت مستقیم و یا به‌واسطه گره‌های کناری خود با ایستگاه اصلی ارتباط گرفته و بدین طریق، اطلاعات جمع‌آوری‌شده را در دسترس آن قرار دهد (کردافشاری، ۱۳۹۸). استفاده از شبکه حسگر بی‌سیم برای اندازه‌گیری کمیت‌های فیزیکی یا شرایط محیطی همچون لرزش، فشار، دما، صدا و غیره در مکان‌ها و قسمت‌های مختلف یک محدوده کاربرد دارد. ازاین‌رو، دامنه استفاده از این حسگرها موضوعات مهمی همچون امنیت ملی، خدمات درمانی، نظامی، نظارت بر محیط و غیره را در بر می‌گیرد. گستردگی حوزه کاربرد این حسگرها توجه بسیاری از محققان را به خود معطوف کرده است. از سوی دیگر، بنا بر پیشرفت‌های صورت‌گرفته در حوزه‌های مخابرات و الکترونیک به طراحی و ساخت حسگرهایی در سایزهای کوچک‌تر، توان مصرفی کمتر و با قیمت مناسب‌تر منجر شده است. آنچه تأثیر بسزایی در تحویل داده‌ها و اطلاعات از گره‌های حسگر دارد، در دسترس بودن شبکه و قابلیت اطمینان از پارامترهای مهم دسترس‌پذیری است. در حقیقت، انتقال و ارسال داده‌ها با ضریب اطمینان بالا از موضوعات اساسی در شبکه حسگر بی‌سیم به شمار می‌آید. درنتیجه، بررسی افزایش قابلیت اطمینان در شبکه‌های حسگر بی‌سیم با استفاده از پروتکل‌های مسیریابی چند مسیره به‌عنوان هدف این پژوهش مطرح است. تاکنون پژوهش‌های بسیاری در این حوزه صورت گرفته است.

مروری بر مطالعات پیشین

صادقی نژاد و همکاران (۱۴۰۰)، دو روش دست‌یابی به قابلیت اطمینان ارسال مجدد و افزونگی را برای رسیدن به درجه بالایی از کارآمدی و بهره‌وری سیستم معرفی کرده و ویژگی‌های پروتکل‌های قابلیت اطمینان موجود بر پایه هر یک از تکنیک‌های بیان‌شده را تجزیه‌وتحلیل کردند.

واعظی و همکاران (۱۴۰۰)، یک پروتکل مسیریابی جدید مبتنی بر کیفیت خدمات را پیشنهاد داده و اعلام کردند، ازآنجاکه روش پیشنهادی سعی در انتخاب کوتاه‌ترین مسیرها و به‌کارگیری ارسال مجدد بسته‌های گمشده دارد، می‌تواند میانگین تأخیر را حدود ۳۰ درصد در شبکه‌های با مقیاس بزرگ بهبود داده و قابلیت اطمینان بالایی داشته باشد.

نوری و زینالی (۱۳۹۹) در پژوهشی با هدف ارزیابی کارایی پروتکل‌های مسیریابی چند مسیره در تضمین امنیت و حریم خصوصی شبکه‌های بی‌سیم، دسته‌بندی سه‌بخشی از پروتکل‌های مسیریابی چند مسیره را ارائه کرده و ضمن تحلیل نقاط ضعف و قوت پروتکل‌های مطرح‌شده، مزیت پروتکل‌ها مبنی بر کاهش نفوذ نفوذگر و جلوگیری از حملات فریبکارانه را اعلام کردند.

بهروان و همکاران (۱۳۹۹) از بهینه‌سازی کلونی مورچه از روش بهینه‌سازی کلونی مورچه برای ایجاد مسیرهای چند پرشه و انرژی کارآمد استفاده کردند. نتایج شبیه‌سازی آن‌ها، کارآمد بودن پروتکل EEMCA در مقایسه با دو پروتکل دیگر را نشان داد.

القحطانی[1] (۲۰۲۱) در نتایج پژوهش خود اعلام کرد مسیریابی هم‌زمان در کنار چند مسیر، توانایی رسیدگی به این خرابی‌ها را به میزان قابل‌توجهی افزایش داده و برنامه چندرسانه‌ای بی‌سیم را به دست می‌آورد.

جیا[2] (۲۰۲۱) با بررسی الگوریتم مسیریابی تعادل انرژی توزیع‌شده برای شبکه حسگر بی‌سیم، شبکه Ad Hoc با بار بالا، تحرک بالا و محدودیت انرژی، پروتکل مسیریابی چند مسیری تعادل انرژی بار را پیشنهاد داد.

دالمن و همکاران[3] (۲۰۰۳) با بررسی جامع پروتکل‌های مسیریابی خوشه‌ای مبتنی بر LEACH در شبکه‌های حسگر بی‌سیم، نقاط قوت و محدودیت‌های هر پروتکل LEACH-variant را مورد بحث قرار داد. درنهایت، مقاله با توصیه‌هایی در زمینه تحقیقات آینده در WSN خاتمه می‌یابد.

لیانگ و همکاران[4] (۲۰۲۱) با بررسی انتقال مسیریابی تعاونی تطبیقی برای شبکه‌های حسگر بی‌سیم ناهمگن انرژی، یک الگوریتم مسیریابی تعاونی تطبیقی جدید همراه با DEEC را پیشنهاد داد که نتایج شبیه‌سازی، عملکرد بهتر الگوریتم مسیریابی پیشنهادی نسبت به طرح‌های معیار را نشان داد. همچنین، الگوریتم مسیریابی پیشنهادی توانست به‌طور مؤثر مصرف انرژی شبکه را کاهش دهد و طول عمر شبکه را افزایش دهد.

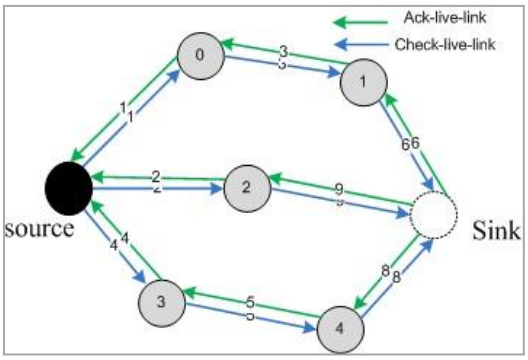
روش پیشنهادی

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 شبیه‌ساز 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 آن، به ارائه راهکار به‌منظور تخمین قابلیت اطمینان با استفاده از دیاگرام تصمیم‌گیری دودویی مرتب‌شده پرداخته شد. راهکار پیشنهادشده قابلیت اطمینان را با یک تقریب خوب به دست آورده و برای شبکه‌های حسگر بی‌سیم مناسب است (AboElFotoh, 2006).

روش گام‌به‌گام

این روش برخلاف روش انتها به انتها، مسیرها را مورد آزمایش قرار می‌دهد؛ هر گره‌ای که روی یک مسیر قرار دارد، گره بعدی[5] بعد از خود مربوط به آن مسیر را بررسی می‌کند. هنگامی‌که 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 و برای گره قبلی ارسال می‌کند. گره اول با دریافت هر بسته از نوع Ack-live-link مقدار شمارنده خود را صفر می‌کند. درصورتی‌که مقدار این شمارنده بیشتر از ۳ شود، گره متوجه خرابی گره بعدی شده 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 موردنظر روی مسیرهای آن واقع شده است، ارسال می‌کند. این بسته گام‌به‌گام ارسال می‌شود تا به منبع موردنظر برسد. منبع نیز با دریافت این بسته آن را از جداول مسیریابی خود حذف می‌کند.

1. Alqahtani, A. S.
2. Jia, L.
3. Dulman et al.
4. Liang et al.
5. next-hop



شکل ۱. نحوه بررسی زنده بودن گره‌های بعدی روی هر مسیر

راهکار پیشنهادی برای تخمین قابلیت اطمینان با استفاده از دیاگرام تصمیم‌گیری دودویی مرتب‌شده

تحلیل قابلیت اطمینان شبکه برای طراحی، نگهداری و ارزیابی موردنیاز است. قابلیت اطمینان سیستم‌های پیچیده بسیار حیاتی بوده و خرابی قطعه‌ها، نتایج بسیار 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. به دلیل بالا بودن میزان خرابی در این شبکه‌ها، تکنیک‌های سنتی نمی‌توانند یک مدل دقیق و کارا برای شبکه‌های حسگر بی‌سیم فراهم کنند.

شبکه‌های حسگر بی‌سیم، دارای پروتکل‌های پویا بوده زیرا 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 به‌صورت 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 جزء مسائل #P_Hard به شمار می‌رود. به همین سبب، وجود یک راهکار برای محاسبه قابلیت اطمینان به‌ویژه در شبکه‌های نظارتی و شبکه‌هایی که محدودیتی بر روی آن‌ها وجود دارد، ضروری است. در این قسمت، یک راهکار برای تخمین قابلیت اطمینان با استفاده از دیاگرام تصمیم‌گیری دودویی مرتب‌شده (OBDD) پیشنهاد می‌شود. راهکار پیشنهادشده قابلیت اطمینان را با یک تقریب خوب به دست می‌آورد و برای شبکه‌های حسگر بی‌سیم مناسب است (ابولفتوح و همکاران، ۲۰۱۶).

دیاگرام تصمیم‌گیری دودویی مرتب‌شده

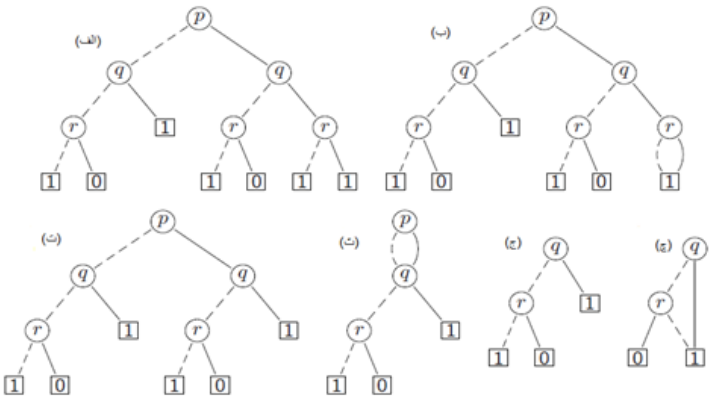
تصور کنید یک برنامه کاربردی، فرمول‌های گزاره‌ای بزرگی دارد که چندین بار استفاده می‌شوند و می‌توان از روی این فرمول‌ها، فرمول‌های دیگری برای ارزیابی هم‌ارزی و ارضا شدن محدودیت‌ها ساخت (اکر، ۲۰۰۸). برای کار با این برنامه‌ها به یک ساختار داده با ویژگی‌های زیر نیاز است:

- دارا بودن یک نمایش فشرده از فرمول‌ها یا یک تابع بولی که بتواند فرمول‌ها را نمایش دهد.
- عملیات بولی روی فرمول‌ها به‌راحتی انجام شود. به‌طور مثال با داشتن فرمول‌های ,fn f1,.....، یک نمایشی از حرف ربط به‌صورت f1^.....^fn امکان‌پذیر باشد.
- تسهیلاتی برای بررسی کردن ویژگی‌های فرمول‌ها وجود داشته باشد.

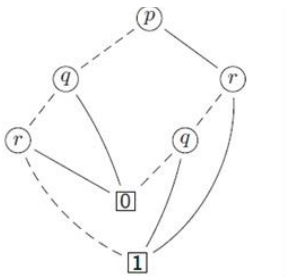
BDD به‌عنوان یک ساختار داده برای نمایش فشرده از درخت‌ها است. بررسی ارضاپذیری در BDD کاری آسان است. با وجود این، پیاده‌سازی تابع‌های بولی مشکل است. با اضافه کردن ترتیب به BDD، BDD مرتب‌شده

(OBDD) به دست می‌آید. OBDD یک نوع خاصی از BDD بوده 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.

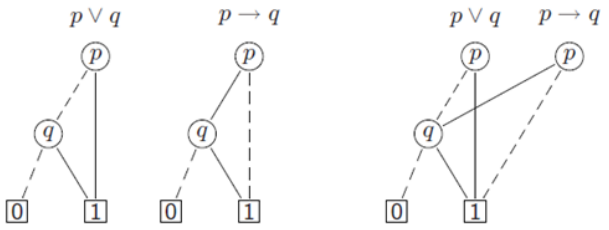


شکل ۲. تبدیل درخت دودویی به BDD

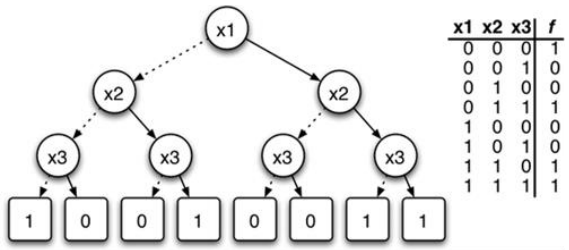


شکل ۳. یک درخت دودویی با آزمایش روی فرمول $f(x_1, x_2, x_3) = \overline{x}_1\overline{x}_2\overline{x}_3 + x_1x_2 + x_2x_3$

با حذف آزمایش اضافی و ادغام زیر گراف‌های هم‌ریخت، یک ساختار داده تحت عنوان نمودار تصمیم‌گیری دودویی (BDD) به دست آمد.



شکل ۴. یک BDD مرتب‌نشده



شکل ۵. 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 است. درنهایت، یک پروتکل چند مسیره تطبیقی برای اقناع قابلیت اطمینان AMPRS مبتنی بر LOMDD معرفی شد.

یافته‌های تحقیق

با توجه به کاربرد گسترده شبکه‌های حسگر بی‌سیم، همچنان قابلیت اطمینان به‌عنوان یکی از الزامات عملکردی شبکه‌ها مطرح است. استفاده از مسیریابی چند مسیره[1] که بر اساس آن مسیرها نقش پشتیبان[2] را برای یکدیگر ایفا می‌نمایند، به‌عنوان یکی از راه‌حل‌های ارائه‌شده برای افزایش قابلیت اطمینان مطرح شده است.

- نحوه پیاده‌سازی و ارزیابی پروتکل مسیریابی چند مسیره LOMDD بر مبنای پروتکل انتشار هدایت‌شده

بستر پیاده‌سازی

به‌منظور پیاده‌سازی پروتکل از کد diffusion 3.2 که همراه بسته نرم‌افزاری NS2.34[3] عرضه شده است، استفاده شد. در این بسته، دو نسخه از پروتکل انتشار هدایت‌شده وجود دارد که عبارت‌اند از diffusion و diffusion3. نسخه diffusion، پیاده‌سازی ساده‌شده الگوریتم است و جزئیات کمتری را در بر می‌گیرد. در پروتکل LOMDD از فیلتر TPP[4] در diffusion3 استفاده شده است.

سناریوهای شبیه‌سازی

جهت بررسی عملکرد این پروتکل از یک شبکه با مقیاس ۱۰۰۰m × ۱۰۰۰m استفاده شده که ۱۲۰ گره به‌صورت یکنواخت در این فضا پخش شده‌اند. دامنه ارسال هر گره برابر ۸۰ متر است. 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 ۱۲۰ ثانیه بوده و نرخ ارسال بسته‌ها توسط منبع ۱۰ بسته در هر ثانیه است. مدل انرژی استفاده‌شده Energy model است. از IEEE 802.11 در لایه MAC استفاده می‌شود.

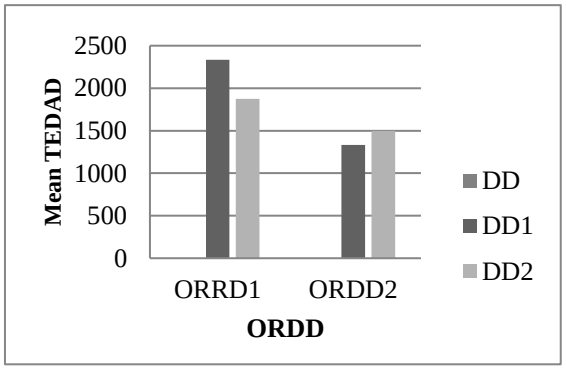
برای محاسبه سربار[5] بسته‌های اکتشافی، کل بسته‌های رد و بدل‌شده در شبکه را در مدت‌زمان شبیه‌سازی، شمارش و آن‌ها را در دو حالت DD و LOMDD مقایسه می‌کنیم. در طول مدت شبیه‌سازی، وضعیت ارسال داده و در دسترس بودن مسیرها را در دو حالت LOMDD و DD مقایسه می‌کنیم. همچنین، میانگین بسته‌های دریافتی در هر لحظه توسط چاهک نیز مقایسه می‌شود. برای محاسبه سربار بسته‌های غیر داده، کل بسته‌های غیر داده رد و بدل‌شده در شبکه را در مدت‌زمان شبیه‌سازی، شمارش و نتایج را در دو حالت DD و LOMDD بررسی می‌کنیم. برای محاسبه قابلیت اطمینان نسبت تعداد بسته‌های دریافت‌شده توسط چاهک به تعداد بسته‌های ارسال‌شده توسط منابع در طول زمان شبیه‌سازی را به دست می‌آوریم و در دو حالت DD و LOMDD با یکدیگر مقایسه می‌کنیم.

1. multipath routing
2. backup
3. NS, "network simulator version 3."
4. two-phase-pull
5. overhead

بررسی نتایج شبیه‌سازی

- سربار بسته‌های اکتشافی

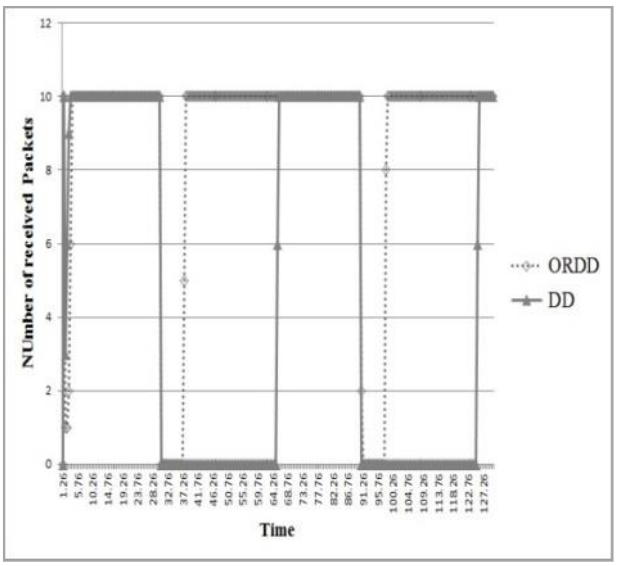
بنا بر شکل زیر، تعداد بسته‌های اکتشافی رد و بدل‌شده در حالت LOMDD کاهش چشمگیری نسبت به DD داشته است که این به نوبه خود سربارها و مصرف انرژی را کاهش می‌دهد. این کاهش چشمگیر بدین دلیل است که در پروتکل انتشار هدایت‌شده، بسته‌های اکتشافی توسط هر گره به تمام گرادیان‌های موجود در جدول مسیریابی ارسال می‌شوند درحالی‌که در پروتکل LOMDD، بسته‌های اکتشافی به بهترین گرادیان ارسال می‌شوند.



نمودار ۱. سربار بسته‌های اکتشافی

- میانگین تعداد بسته‌های دریافتی در هر لحظه توسط چاهک

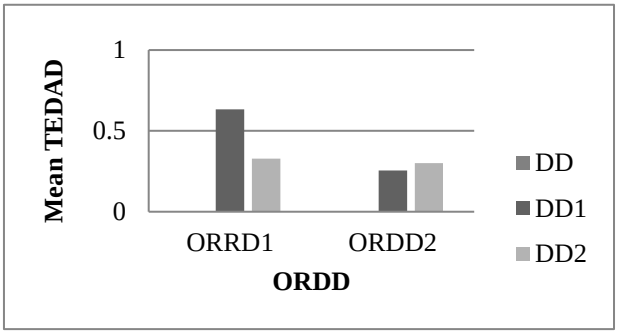
همان‌طور که در شکل پیداست، در ثانیه ۳۰ یک گره روی مسیر اصلی خراب می‌شود. در پروتکل DD به خاطر ویژگی‌های ذاتی آن تقریباً ۳۰ ثانیه طول می‌کشد تا بسته‌های علاقه‌مندی دوباره توسط چاهک ارسال و عملیات مسیریابی انجام شود. سپس، منبع با پیدا کردن مسیر جدید داده‌های خود را به چاهک ارسال می‌کند اما در پروتکل LOMDD، این خرابی بعد از چند ثانیه تشخیص داده می‌شود؛ آنگاه منبع سریعاً مسیر جایگزین را انتخاب 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 بوده و سبب می‌شود بسته‌های زیادی در گره‌های میانی از بین بروند.



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

قابلیت اطمینان

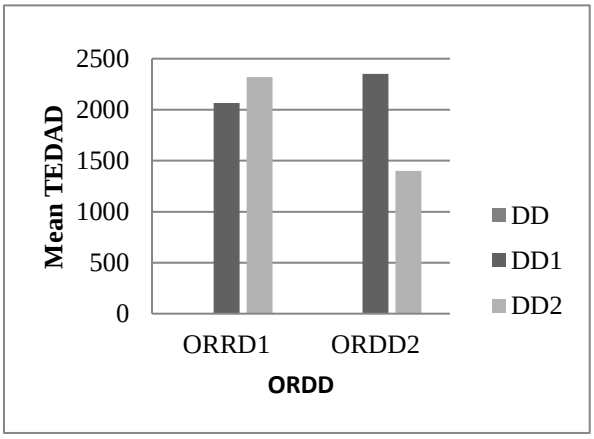
قابلیت اطمینان در پروتکل LOMDD نسبت به DD افزایش چشمگیری داشته است که این بدین دلیل است که در پروتکل DD هنگام خراب شدن مسیر زمان زیادی طول می‌کشد تا یک مسیر جدید بین چاهک و منبع برقرار گردد و این سبب می‌شود که در این حین، بسته‌های زیادی از دست بروند و به مقصد نرسند؛ اما در پروتکل LOMDD، بعد از آنکه مسیر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



نمودار ۳. قابلیت اطمینان

سربار بسته‌های غیر داده

سربار کل بسته‌های غیر داده در دو پروتکل مقایسه شده که این نتایج باز حاکی از بهبود LOMDD نسبت به DD است. سربار پروتکل LOMDD ناشی از بسته‌های کنترلی رد و بدل‌شده برای بررسی وضعیت مسیرها است.



نمودار ۴. سربار بسته‌های غیر داده

تحلیل و تخمین قابلیت اطمینان با استفاده از یک راهکار پیشنهادشده مبتنی بر OBDD

راهکار پیشنهادشده یک راهکار بازگشتی است که با کاهش محاسبات اضافی و حذف زیرگراف‌ها[1] یک الگوریتم کارا برای محاسبه قابلیت اطمینان شده است. برای یک لینک مشخص در گراف به‌دست‌آمده، ممکن است چندین گره در یک سطح وجود داشته باشد.

1. sub-graph

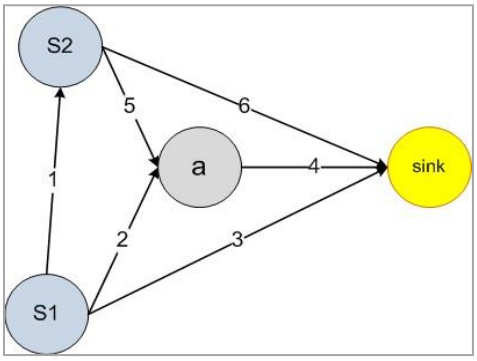
نمادهای استفاده‌شده در راهکار پیشنهادشده

به‌جای 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 به‌صورت یک متغیر بولی به‌صورتی‌که در فرمول ۱ آمده است، تعریف می‌شوند.

$$\text{link}_i = \begin{cases} 1 & \text{اگر لینک i فعال باشد} \\ 0 & \text{اگر لینک i فعال نباشد} \end{cases} \qquad (۱)$$

در اینجا، لینک‌ها نشان‌دهنده گره‌ها در گراف (گرافی که برای محاسبه قابلیت اطمینان از شبکه به‌دست‌آمده) هستند که در شکل، یک نمونه از آن نمایش داده می‌شود. همان‌طور که در شکل مشاهده می‌شود، یک گره به دو قسمت تبدیل شده است. درصورتی‌که لینک فعال در نظر گرفته شود، قسمت ۱ را بسط می‌دهیم و کمان خروجی از این لینک را به‌صورت یک خط پررنگ پیوسته نمایش می‌دهیم. در غیر این صورت، قسمت صفر را بسط می‌دهیم و کمان خروجی از آن را به‌وسیله خطوط تیره منقطع نمایش می‌دهیم.

در اینجا تنها دو برگ به‌صورت $\boxed{1}$ 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 غیرفعال در این پیمایش غیر قابل اطمینان است و این گره را Unreliable می‌نامیم.



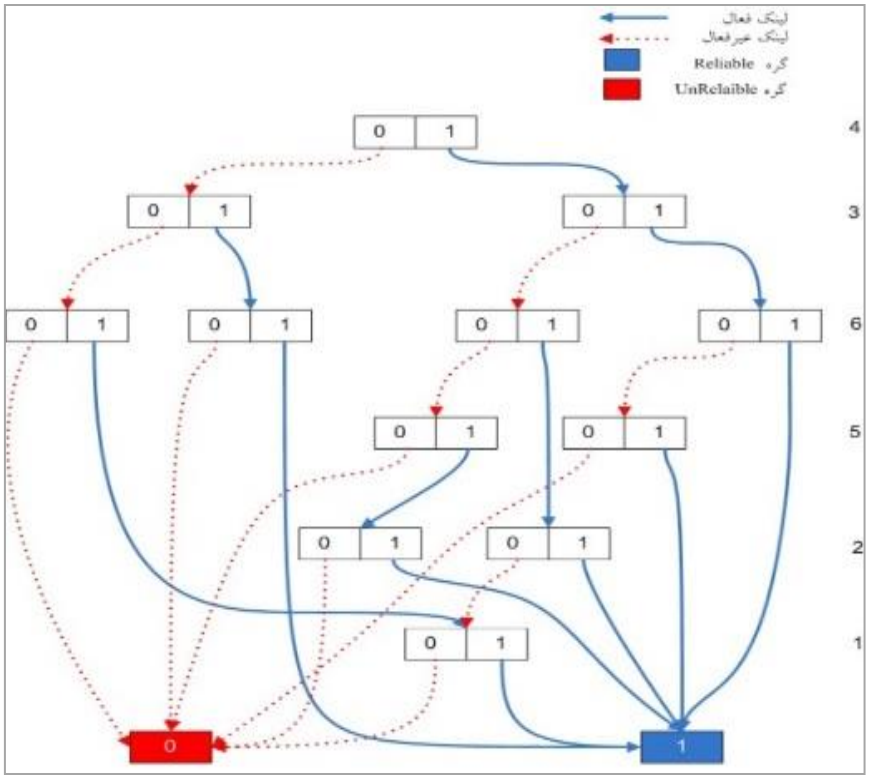
شکل ۶. شبکه با دو منبع و یک چاهک

نحوه عملکرد راهکار پیشنهادشده

در ابتدا با توجه به لینک‌ها و مسیرهایی که برای هر منبع در نظر گرفته می‌شود، با توجه به تعریف قابلیت اطمینان یک گراف به دست می‌آوریم. سپس، قابلیت اطمینان را با استفاده از یک فرمول که بر روی گراف اعمال می‌شود، محاسبه می‌کنیم. در ادامه، مراحل اجرای راهکار پیشنهادشده تشریح می‌شود. برای واضح شدن موضوع، یک مثال را همراه با تشریح راهکار پیشنهاد می‌کنیم. فرض کنید شبکه‌ای مشابه شکل داریم که می‌خواهیم گراف مبتنی بر OBDD را با توجه به راهکار پیشنهادشده برای محاسبه قابلیت اطمینان به دست 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 S1 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 پیمایش‌شده از ریشه تعیین شود که شبکه قابل اطمینان یا غیر قابل اطمینان است. با پیمایش از ریشه در هر یک از شاخه‌های این گراف، درصورتی‌که به گره Reliable برسیم، نشان‌دهنده این است که با وجود لینک‌های فعال در این پیمایش شبکه قابل اطمینان است و درصورتی‌که به گره Unreliable برسیم، نشان‌دهنده این است که با وجود لینک‌های غیرفعال در این پیمایش، شبکه قابل اطمینان نیست و نیازهای لازم بر اساس تعریف قابلیت اطمینان برآورده نمی‌شود. شماره‌هایی که در یک ستون در سمت راست شکل نشان داده شده است، بیانگر شماره لینکی است که در سطح موردنظر مورد آزمایش قرار می‌گیرد. مثلاً لینک شماره ۵ در سطح چهارم مورد بررسی قرار گرفته است.



شکل ۷. گراف به‌دست‌آمده از شبکه شکل با استفاده از راهکار پیشنهادشده

جدول ۱. مشخصات لینک شماره ۴

Success probability	۰/۹۵
Count repeat	۲
prev node	A
next node	Sink

در شکل دو نوع از کمان‌ها برای اتصال بین گره‌ها داریم. همان‌طور که ذکر شد، در راهکار پیشنهادشده این گره‌ها بیانگر لینک‌ها هستند. اگر لینک موردنظر فعال در نظر گرفته شود، یک کمان پررنگ پیوسته از قسمت 1 گره مربوطه به گره بعدی (درواقع، گره مربوط به لینک بعدی) وصل می‌شود و اگر لینک موردنظر غیرفعال در نظر گرفته شود، یک کمان با خط‌چین قرمزرنگ به گره بعدی اتصال پیدا می‌کند. مثلاً در شکل سمت راست‌ترین گره، مربوط به لینک شماره ۶ در سطح سوم از گراف را در نظر بگیرید. درصورتی‌که لینک شماره ۶ فعال در نظر گرفته شود، یک

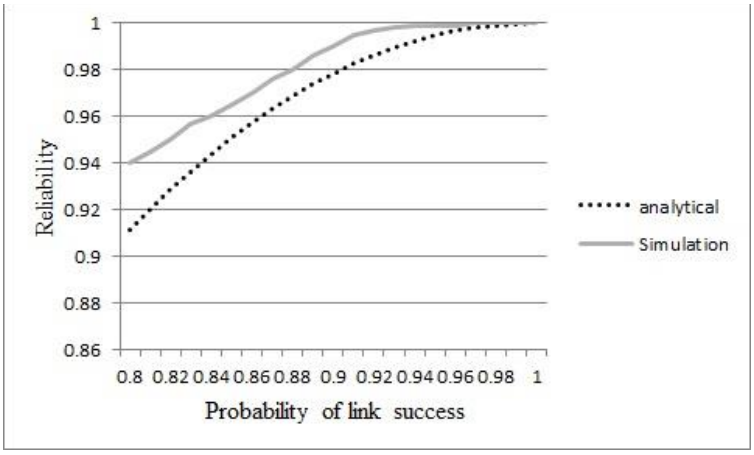
کمان پررنگ پیوسته به گره Reliable وصل می‌شود. در غیر این صورت، یک کمان خط‌چین به گره مربوط به لینک ۵ در سطح پایین‌تر متصل می‌گردد.

```
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
 N_L =Create-node(Link)
Connect last arc in LinkList-v to N_L

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

 L=T_SL+L-1
```

شکل ۸. شبه کد مراحل راهکار پیشنهادشده برای تشکیل گراف جهت تخمین قابلیت اطمینان



نمودار ۵. قابلیت اطمینان شبکه شکل به‌صورت تحلیلی و شبیه‌سازی

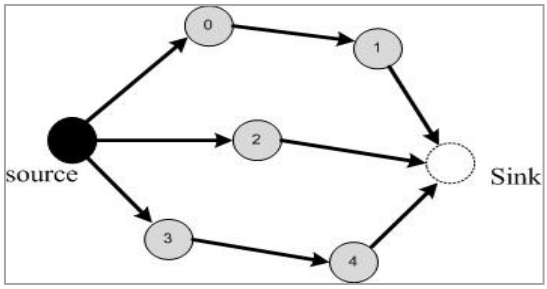
پیشنهاد یک پروتکل چند مسیره تطبیقی برای اقناع قابلیت اطمینان

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 است که از این لینک استفاده می‌کنند. درنتیجه، روی قابلیت اطمینان کل شبکه تأثیر می‌گذارد. کم یا زیاد شدن احتمال موفقیت لینک‌ها، تعداد مسیرهای استفاده‌شده را تحت تأثیر قرار می‌دهد. تعداد مسیرهایی که استفاده می‌شود، بر روی کارایی شبکه نیز مؤثر است. با کم شدن احتمال موفقیت لینک مسیرهای موجود ممکن است

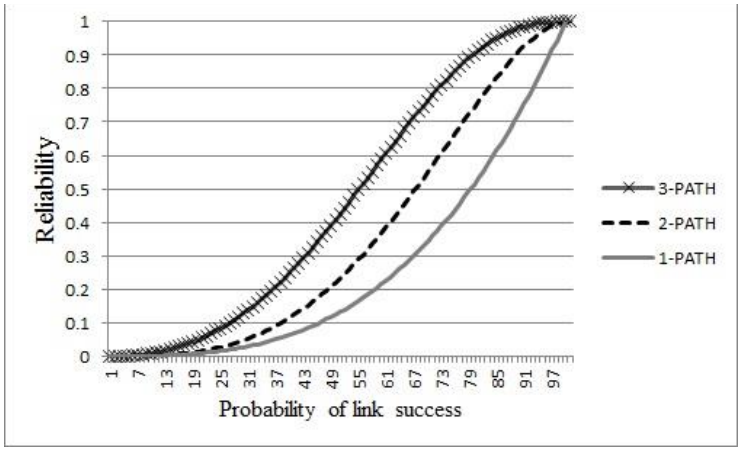
قابلیت اطمینان مورد انتظار را ارضا نکند و با زیاد شدن احتمال موفقیت لینک استفاده از مسیرهای موجود ممکن است سربار زیادی را به شبکه تحمیل کند.

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.

به‌طور 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 و با استفاده از فرمول‌های سری و موازی به دست آمده است.



شکل ۹. شبکه با سه مسیر مستقل از منبع به چاهک



نمودار ۶. قابلیت اطمینان مسیرهای مختلف برای توپولوژی شکل بالا

با توجه به شکل فرض می‌شود قابلیت اطمینان مورد انتظار برابر ۹۰ درصد و احتمال موفقیت لینک‌ها نیز برابر ۹۰ درصد باشد. در اینجا مقدار بهینه برای تعداد مسیرهای استفاده‌شده، ۲ است. اگر از یک مسیر استفاده شود، قابلیت اطمینان به‌دست‌آمده در حدود ۷۰ درصد بوده که قابلیت اطمینان مورد انتظار را ارضا نمی‌کند. همچنین، اگر از ۳ مسیر استفاده شود، قابلیت اطمینان به‌دست‌آمده 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 استفاده‌شده توسط هر یک از منابع برای ارضای قابلیت اطمینان طراحی شده است. در LOMDD از یک

مسیر به‌عنوان مسیر اصلی استفاده و سایر مسیرها به‌عنوان جایگزین انتخاب می‌شوند. پروتکل AMPRS به‌منظور تعیین تعداد مسیرها برای هر یک از منابع طراحی می‌شود. چاهک بر اساس اطلاعاتی که در دوره‌های زمانی از شبکه به دست می‌آورد، تصمیم می‌گیرد که هر یک از منابع از چه مسیرهایی و چند مسیر برای ارسال اطلاعات استفاده کنند. در ادامه، ابتدا یک سری از ویژگی‌ها و پیش‌فرض‌ها را برای AMPRS بیان و سپس نحوه عملکرد آن را تشریح می‌کنیم.

تنظیمات اولیه

بعد از مسیریابی که مبتنی بر پروتکل پیشنهادشده 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، باخبر 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. به‌طورکلی می‌توان گفت، چاهک یک دید کلی نسبت به منابع و مسیرهای تنظیم‌شده برای آن‌ها و همچنین، ویژگی‌های این مسیرها دارد. این اطلاعات برای تصمیم‌گیری چاهک در مورد انتخاب مسیرها و نحوه توزیع بار در شبکه لازم است. 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 باقی‌مانده روی هر مسیر
- لینک‌های روی هر مسیر
- احتمال موفقیت لینک‌ها
- قابلیت اطمینان هر یک از مسیرها
- تعداد بسته‌های ارسالی از منبع تا زمان جاری
- تعداد بسته‌های دریافتی از منبع تا زمان جاری توسط چاهک
- وضعیت هر یک از مسیرها که آیا فعال است یا غیرفعال (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 تصمیم‌گیری چاهک

در این پروتکل همواره سعی بر این است که قابلیت اطمینان همواره در حول‌وحوش 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 و قابلیت اطمینان به‌دست‌آمده از شبکه را R بنامیم، همواره سعی می‌شود نامعادله (۲) حفظ شود.

$$R_D - \propto < R < R_D + \propto \qquad (۲)$$

مراحل الگوریتم تصمیم‌گیری چاهک در زیر گام‌به‌گام بیان می‌شود:

1. identify

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

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

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

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

گام ۵. اگر قابلیت اطمینان به‌دست‌آمده کوچک‌تر از $R_D - \propto$ باشد، چاهک در میان مسیرهایی که غیرفعال هستند، جست‌وجو 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 موردنظر ارسال می‌کند. منبع با دریافت این بسته مسیر موردنظر را فعال و از این به بعد یک نسخه از بسته‌ها را روی این مسیر نیز ارسال می‌کند و سپس به گام ۴ می‌رود. در این مرحله، اگر هیچ مسیری پیدا نشود، نشان‌دهنده 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.

گام ۶. اگر قابلیت اطمینان به‌دست‌آمده بزرگ‌تر از مقدار $R_D \propto +$ باشد، چاهک در میان مسیرهای فعال، مسیر با کمترین تأثیر در قابلیت اطمینان را انتخاب می‌کند. درواقع، بدترین مسیر را انتخاب می‌کند. مسیر انتخاب شده به‌صورت موقت غیرفعال در نظر گرفته می‌شود. قابلیت اطمینان با توجه به راهکار پیشنهادشده در بخش قبل برای مسیرهای فعال موجود تخمین زده می‌شود که در اینجا دو حالت پیش می‌آید:

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

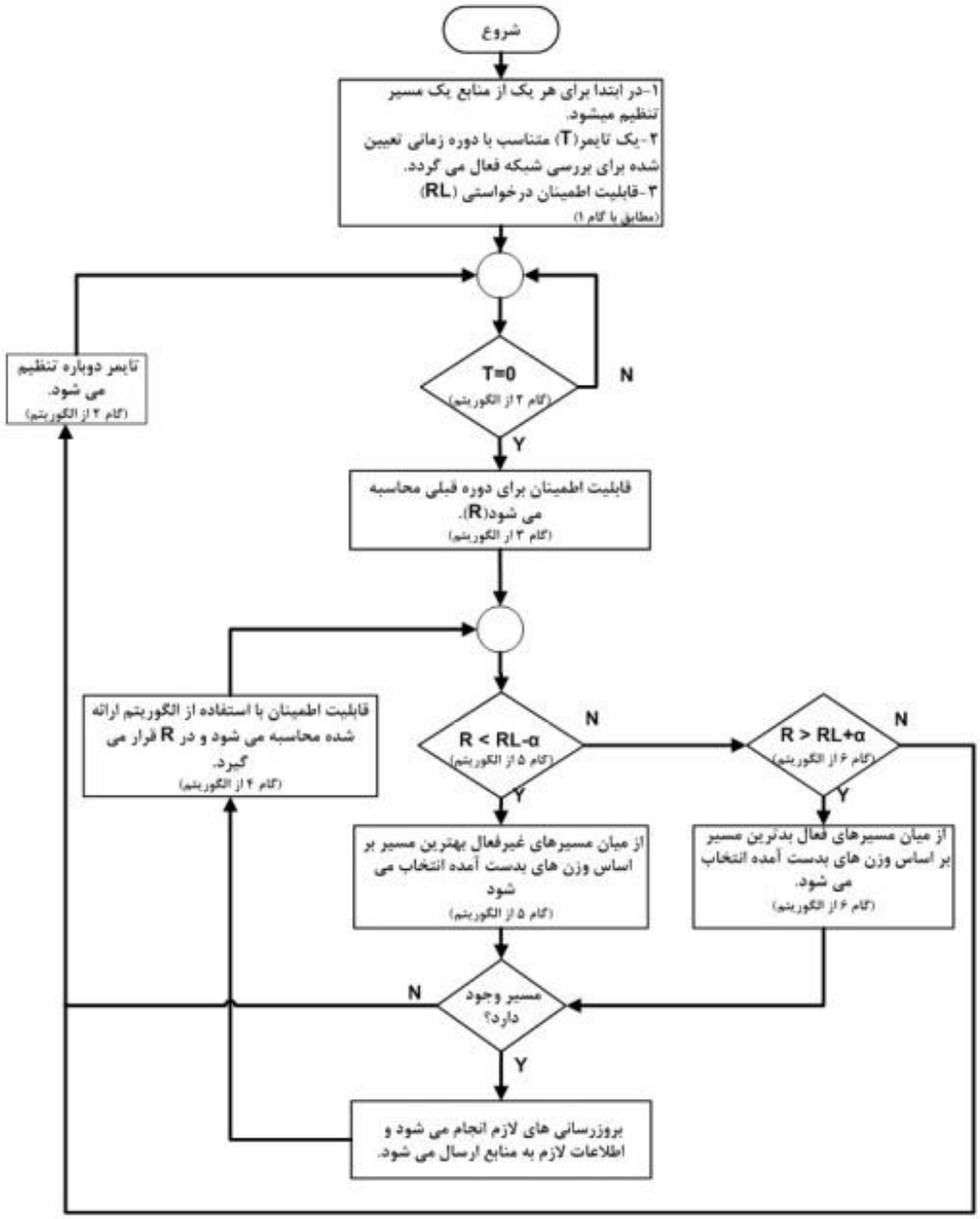
در غیر این صورت، یک بسته از نوع Ack- live-path برای منبع مربوطه در مسیر عقب‌گرد ارسال می‌شود که در فیلد مربوط به فعال بودن مسیر، مقدار ۱ تنظیم می‌شود. منبع با دریافت این بسته و بررسی آن متوجه می‌شود که باید بسته‌های داده را روی این مسیر ارسال نکند و چاهک نیز جدول Info-Source خود را به‌روزرسانی می‌کند.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

در این مرحله، اگر هیچ مسیری به دست نیاید، نشان‌دهنده این است که قابلیت اطمینان نمی‌تواند از این مقدار کمتر باشد و به گام ۸ می‌رود.

گام ۷. اگر قابلیت اطمینان محاسبه‌شده کوچک‌تر از $R_D - \propto$ و بزرگ‌تر از $R_D \propto +$ باشد، بیانگر این است که قابلیت اطمینان شبکه در دامنه موردنظر است و نیاز به هیچ‌گونه تغییری نیست. سپس به گام ۸ می‌رود.

گام ۸. تایمر دوباره تنظیم شده و به گام ۲ می‌رود.

این الگوریتم توسط چاهک در دوره‌های تصمیم‌گیری چاهک، تکرار و در هر مرحله بر اساس شرایط شبکه مسیرها برای منابع تعیین می‌شود. مراحل الگوریتم به‌صورت خلاصه در فلوچارت شکل ۱۰ نمایش داده شده است.



شکل ۱۰. فلوچارت عملکرد و تصمیم‌گیری چاهک در AMPRS

نحوه انتخاب مسیر هنگام افزایش یا کاهش مسیرها

به هر یک از مسیرها یک وزن اختصاص داده می‌شود. وزن‌های اختصاص داده‌شده بر اساس پارامترهای زیر محاسبه می‌شود:

- قابلیت اطمینان: هم می‌توان از قابلیت اطمینان مسیرها و هم از قابلیت اطمینان تخمین زده‌شده در صورت اضافه یا کم کردن مسیرها برای مقایسه استفاده کرد.
- انرژی باقیمانده مسیر
- تعداد گام‌های مسیر

$$W_i = R_i + \left(\frac{E_i}{E} \times \frac{1}{C_i}\right) \quad (۳)$$

$$W_i = RL_i + \left(\frac{E_i}{E} \times \frac{1}{C_i}\right) \quad (۴)$$

در فرمول‌های بالا، Wi وزن به‌دست‌آمده را برای مسیر iام، Ei انرژی باقی‌مانده روی مسیر iام، E انرژی اولیه را برای گره‌ها، Ri قابلیت اطمینان مسیر iام، RL_i قابلیت اطمینان تخمین زده‌شده که با اضافه یا کم کردن مسیر iام به دست می‌آید و Ci تعداد گام‌های مسیر iام را نشان می‌دهد. مسیری که بیشترین وزن را داشته، به‌عنوان بهترین مسیر انتخاب می‌شود. نحوه محاسبه وزن‌ها سبب می‌شود مسیرهایی انتخاب شوند که قابلیت اطمینان را افزایش دهند، سبب توزیع بار در شبکه شوند و طول عمر شبکه را افزایش دهند.

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.

نحوه پیاده‌سازی و ارزیابی

جدول ۲. مشخصات پارامترهای شبیه‌سازی

پارامتر	مقدار			توضیحات
برد انتقال	۸۰ m			----
مدل انرژی	Energy Model	ارسال	۲۹.۵mW	در شبیه‌ساز NS پیاده‌سازی شده است
		دریافت	۲۴.۵mW	
شبیه‌ساز	NS۲.۳۴			بر پایه پلتفرم لینوکس
لایه MAC	IEEE ۸۰۲.۱۱			---
مدت زمان دوره تصمیم‌گیری چندگانه	۱۰۰ s			---
ابعاد فضای شبیه‌سازی	۳۰۰*۳۰۰			
زمان شبیه‌سازی	۴۰۰ s			---
نرخ ارسال	۱۰ Pps			---
تعداد گره‌ها	۵۰			---
تعداد منابع	۳			به صورت تصادفی انتخاب می‌شوند
α	۰.۰۱			------
مدل خطا	Error Model			در شبیه‌ساز NS پیاده‌سازی شده است
حداکثر تعداد مسیر برای هر منبع	۵			----

نمودار ۷. احتمال موفقیت لینک‌ها با توجه به نرخ خطا

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 انجام‌شده 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) به‌صورت معادله (۵) محاسبه می‌شود.

$$P = (1-q) + q(1-q) + q(1-q)^2 + q(1-q)^3 \qquad (۵)$$

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

نتایج شبیه‌سازی

در این قسمت، نتایج شبیه‌سازی برای هر یک از سناریوهای مطرح‌شده در قسمت قبل آورده شده و نمودار مربوط به نتایج به‌دست‌آمده، نشان داده شده است.

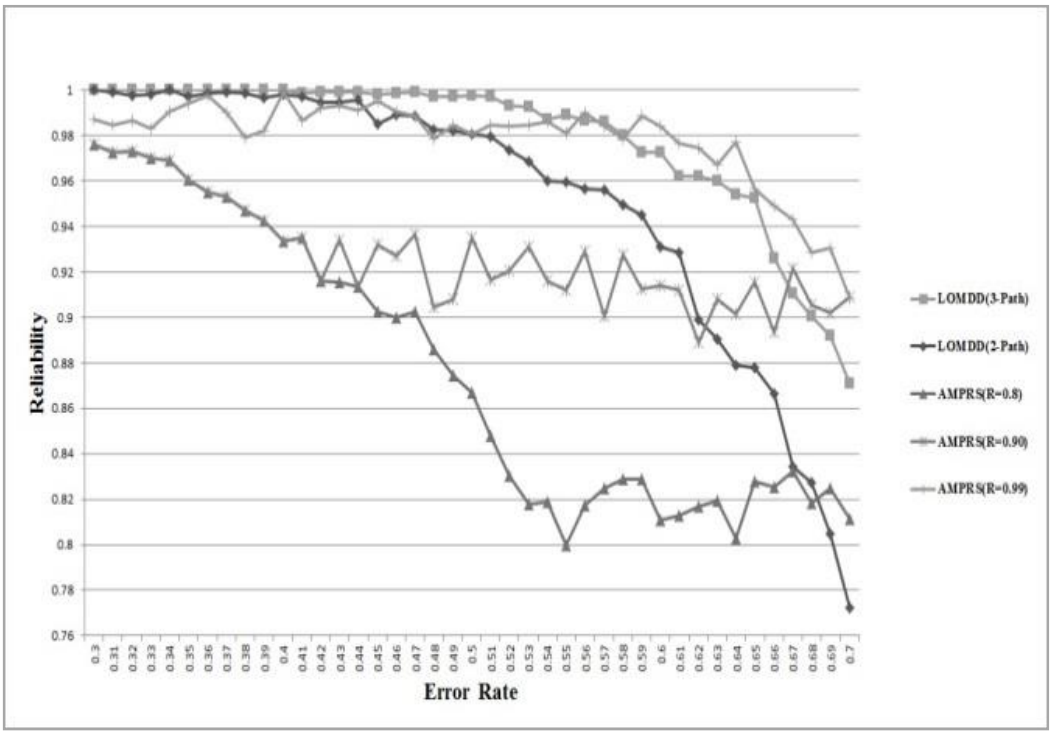
قابلیت اطمینان

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 تطبیق‌پذیری بسیار بالای AMPRS با شرایط شبکه است. قابلیت اطمینان همواره در محدوده قابلیت اطمینان مورد انتظار شبکه نگه داشته شده و با افزایش نرخ خطا، تغییرات لازم انجام می‌شود.

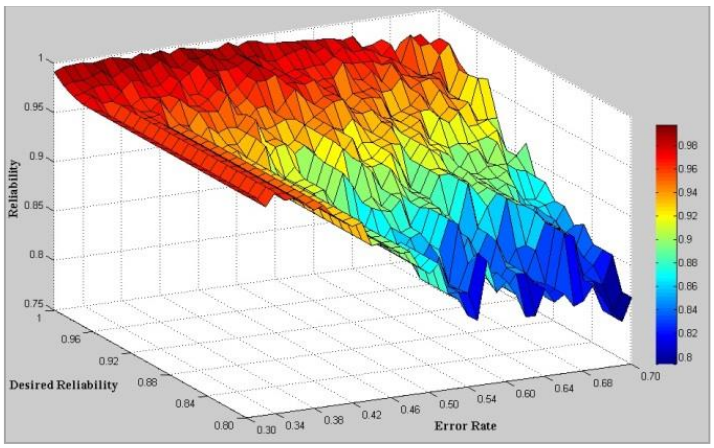
مشاهده می‌شود با افزایش درصد خطای شبکه و قابلیت اطمینان مورد انتظار، AMPRS قابلیت اطمینان را در محدوده موردنظر نگه می‌دارد. در این شکل مشاهده می‌شود که استفاده از تعداد مسیرهای ثابت در بیشتر مواقع کارا نیست. در نمودارهای مربوط به استفاده از تعداد مسیرهای ثابت، با افزایش نرخ خطا مشاهده می‌شود که قابلیت اطمینان به‌تدریج کاهش پیدا می‌کند. کاهش قابلیت اطمینان سبب می‌شود 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 غیرضروری است. در بخش‌های بعدی خواهیم دید که استفاده از مسیرهای ثابت سربار زیادی بی‌جهت به شبکه اعمال می‌شود.

به‌طور مثال، اگر عملکرد پروتکل AMPRS را برای حالتی در نظر بگیریم که قابلیت اطمینان مورد انتظار ۹۰ درصد ((AMPRS(R=0.90) باشد، با توجه به شکل برای نرخ خطای بین ۳۰ تا ۳۸ درصد قابلیت اطمینان به‌دست‌آمده بیشتر از قابلیت اطمینان مورد انتظار (۹۰ درصد) است. این امر بدین دلیل است که حداقل قابلیت اطمینان به‌دست‌آمده نمی‌تواند از این مقدار کمتر شود. برای نرخ خطاهای بزرگ‌تر از ۳۰ درصد برای این حالت، قابلیت اطمینان همواره حول‌وحوش ۹۰ درصد نگه داشته می‌شود. اگر حالت ((AMPRS(R=0.90) با حالتی مقایسه شود که از ۲ مسیر ثابت ((LOMDD(2-Path) استفاده شده است، مشاهده می‌شود که در LOMDD با دو مسیر ثابت قابلیت اطمینان به‌دست‌آمده 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.

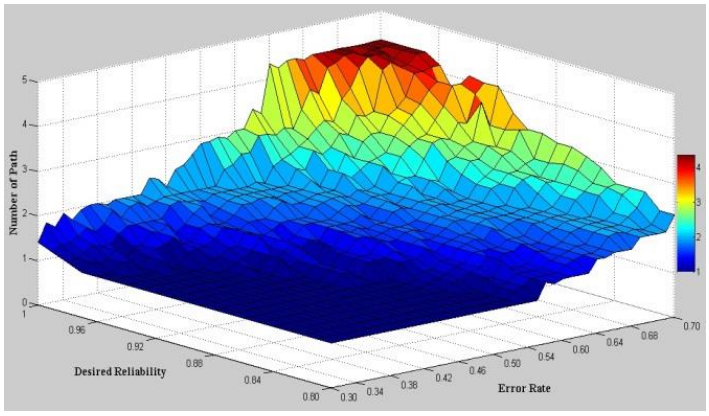
با توجه به نتایج به‌دست‌آمده می‌توان گفت که پروتکل AMPRS یک انتخاب مناسب برای ارضای قابلیت اطمینان مورد انتظار در شبکه‌های حسگر بی‌سیم است.



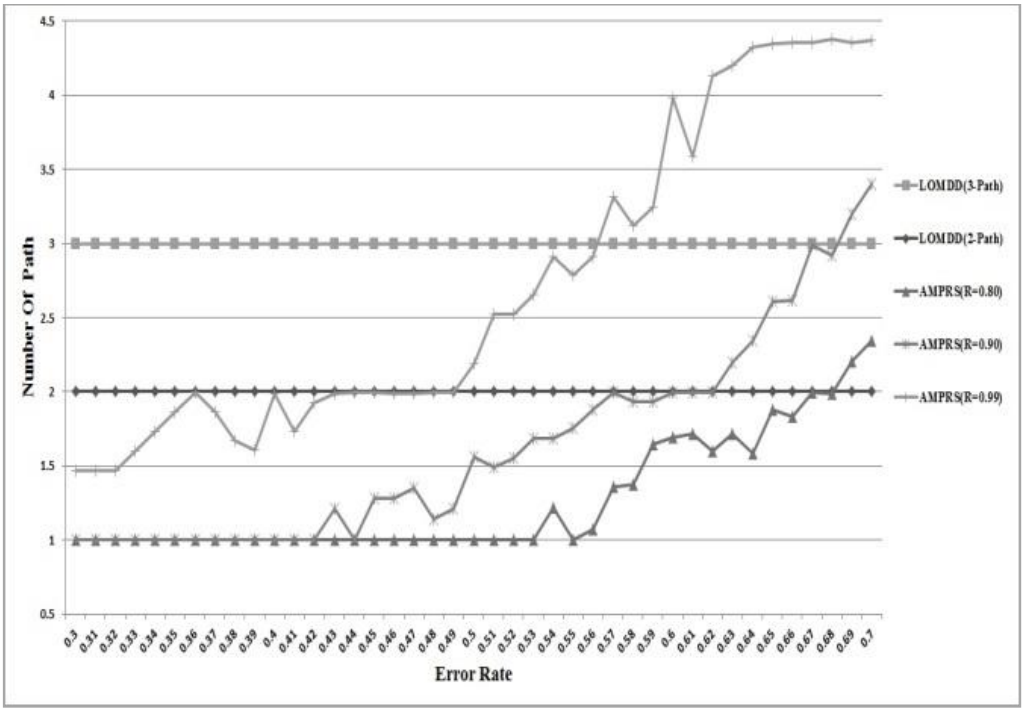
نمودار ۸. مقایسه قابلیت اطمینان AMPRS در حالت‌های مختلف با LOMDD در حالت استاتیک



شکل ۱۱. تطبیق‌پذیری قابلیت اطمینان در AMPRS با تغییرات قابلیت اطمینان مورد انتظار و نرخ خطا



شکل ۱۲. تطبیق‌پذیری تعداد مسیر انتخاب‌شده در AMPRS با تغییرات قابلیت اطمینان مورد انتظار و نرخ خطا



نمودار ۹. مقایسه تعداد مسیرهای استفاده‌شده در AMPRS با LOMDD

تعداد میانگین مسیرها

نتایج حاکی از این است که پروتکل AMPRS همواره حداقل تعداد مسیر را با توجه به محدودیت‌های خواسته‌شده 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، به استفاده از مسیرهای بیشتری نیاز است. AMPRS همواره سعی می‌کند تعداد مسیر بهینه را برای منابع انتخاب کند.

عملکرد پروتکل AMPRS را برای حالتی مقایسه می‌کنیم که قابلیت اطمینان مورد انتظار ۹۹ درصد (AMPRS(R=0.99)) است و از ۳ مسیر ثابت (LOMDD(3-Path)) برای ارسال داده‌ها استفاده شده است. در پروتکل AMPRS برای نرخ خطای کمتر از ۵۸ درصد از تعداد مسیر کمتری استفاده می‌شود و نیازی به استفاده از مسیرهای بیشتر نیست. برای همین حالت (AMPRS(R=0.99)) قابلیت اطمینان مورد انتظار را نیز برآورده می‌کند.

لذا، نیازی به استفاده از مسیرهای بیشتر نیست. همچنین، با افزایش نرخ خطا تعداد مسیرهای استفاده‌شده، از حالتی که از ۳ مسیر ثابت استفاده می‌شود، بیشتر است که 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 درحالی‌که قابلیت اطمینان LOMDD با ۳ مسیر ثابت به‌شدت افت می‌کند.

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

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 کمترین سربار ممکن به شبکه اعمال گردد.

اگر با حالتی مقایسه کنیم که از ۳ مسیر ثابت ((LOMDD(3-Path) برای ارسال داده‌ها استفاده شده، قابل مشاهده است که این حالت همواره سربار زیادی را به شبکه تحمیل می‌کند که در بیشتر مواقع این سربار، اضافی است. 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-Path) می‌شود.

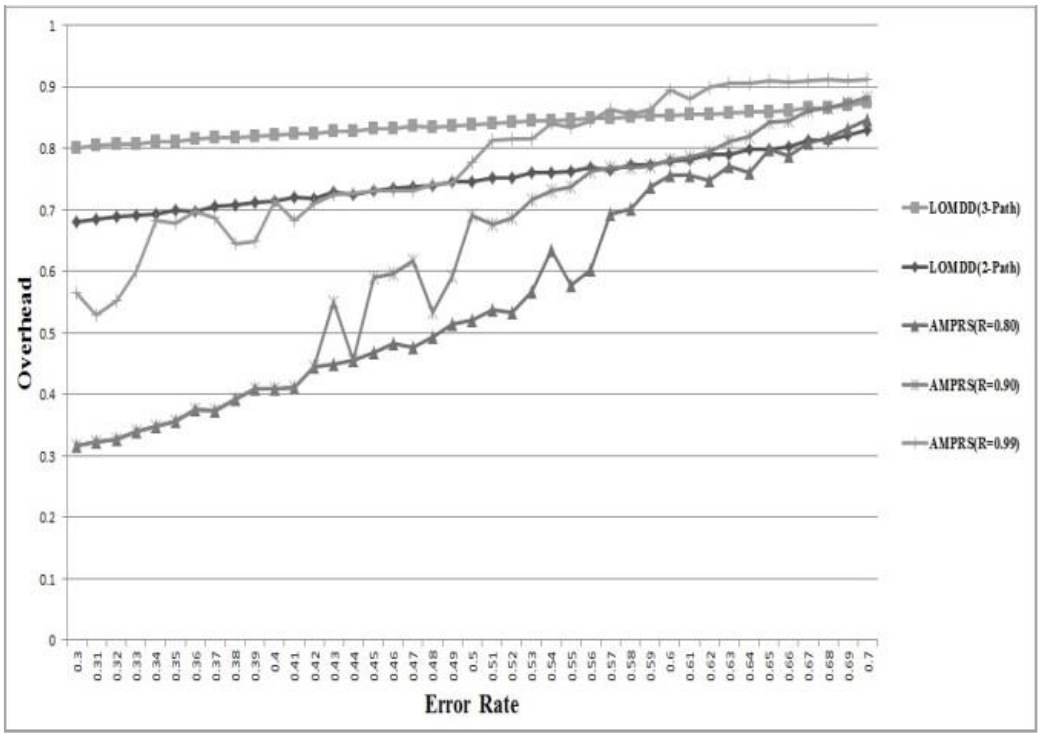
عملکرد پروتکل AMPRS را برای حالتی در نظر می‌گیریم که قابلیت اطمینان مورد انتظار ۹۰ درصد ((AMPRS(R=0.90) با حالتی که از ۳ مسیر ثابت ((LOMDD(3-Path) برای ارسال داده‌ها استفاده شده است، مقایسه شود. AMPRS همواره نسبت به LOMDD با ۳ مسیر ثابت سربار کمتری را به شبکه تحمیل می‌کند. تنها در مقادیر بالا از نرخ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

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

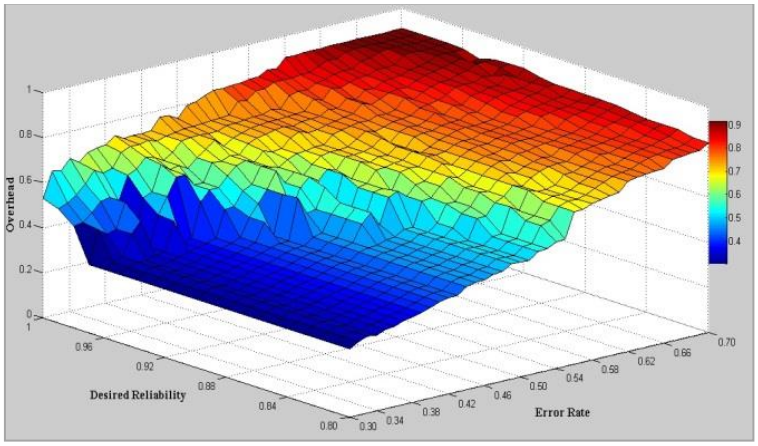
انرژی مصرف‌شده

نتایج نمودارهای مربوط به انرژی مصرف‌شده حاکی از این است که پروتکل AMPRS انرژی مصرف‌شده در شبکه را با توجه به محدودیت‌های خواسته‌شده، مینیمم نموده و از مصرف انرژی بی‌جهت در شبکه جلوگیری می‌کند.

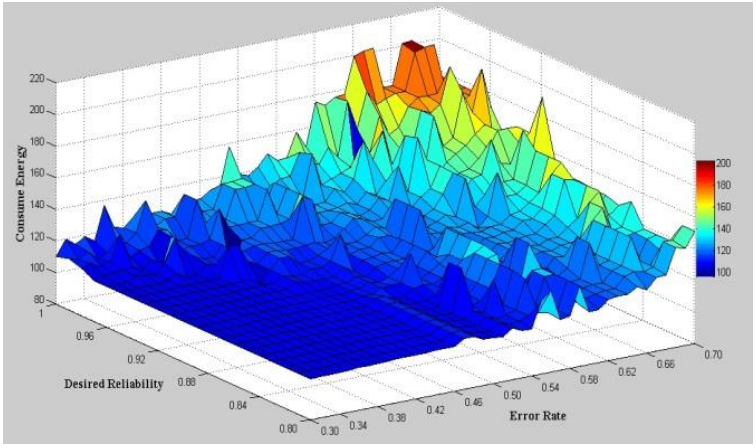
به‌طور مثال، اگر عملکرد پروتکل AMPRS برای حالتی که قابلیت اطمینان مورد انتظار ۹۰ درصد باشد، با حالتی مقایسه شود که از ۳ مسیر ثابت ((LOMDD(3-Path) برای ارسال داده‌ها استفاده شده، قابل مشاهده است که انرژی مصرف‌شده در (AMPRS(R=0.90 همواره انرژی کمتری را مصرف می‌کند. در شکل قابل مشاهده است که در بقیه حالات نیز این‌چنین است.



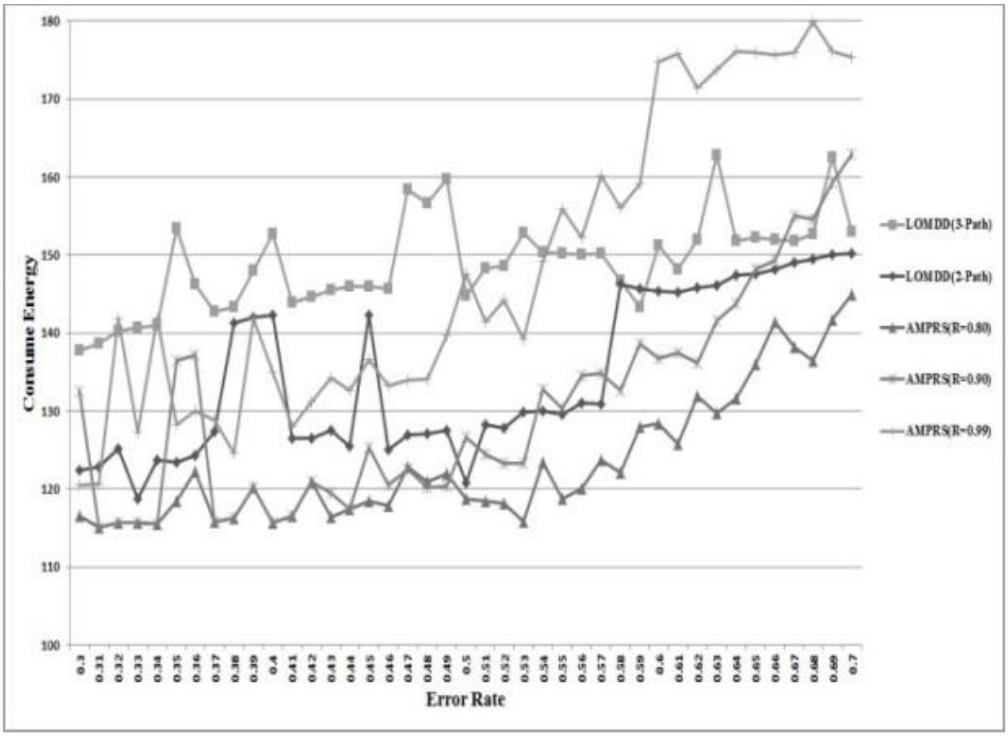
نمودار ۱۰. مقایسه سربار ناشی از مسیرها در AMPRS



شکل ۱۳. سربار اعمال‌شده به شبکه در AMPRS با تغییرات قابلیت اطمینان مورد انتظار و نرخ خطا



شکل ۱۴. انرژی مصرف‌شده در AMPRS با تغییرات قابلیت اطمینان مورد انتظار و نرخ خطا



نمودار ۱۱. میانگین انرژی مصرف‌شده گره‌ها در AMPRS

بحث و نتیجه‌گیری

امروزه، استفاده از شبکه‌های بی‌سیم با توجه به گستردگی دامنه کاربردی و سهولت استفاده، جایگاه ویژه‌ای یافته است. از مسائل مهمی که در حوزه شبکه‌های بی‌سیم توجه محققان را به خود جلب کرده است، چگونگی انتقال اطلاعات از گره‌های داخلی شبکه به ایستگاه اصلی و برگزیدن بهترین مسیر ممکن برای انتقال اطلاعات است به‌نحوی 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 است که در این پروتکل به کار رفته است.

مقایسه پروتکل پیشنهادی با چند پروتکل دیگر مسیریابی

استفاده از پروتکل مناسب برای شبکه حسگر بی‌سیم از ابتدای ایجاد این نوع از شبکه به‌عنوان 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 الگوریتم‌ها و روش‌های گوناگون، این پروتکل‌ها دچار تغییرات اساسی شده و بهبود یافته‌اند. این تغییرات و تکامل باعث گردیده که شبکه حسگر بی‌سیم، یکی از مهم‌ترین گزینه‌های مورد آزمایش و تحقیق در علوم مختلف باشد.

پروتکل‌های مبتنی بر داده

مسیریابی در این شبکه‌ها، به‌جای آنکه مبتنی بر آدرس باشد، مبتنی بر داده است؛ یعنی ما بیشتر دنبال گره‌هایی هستیم که اطلاعات خاصی را دارند؛ برخلاف حالت سنتی که در مسیریابی غالباً به دنبال گرهای با شناسه خاص هستیم.

در پروتکل‌های مبتنی بر داده، گره چاهک پرس‌وجوهای خود را به مناطق موردنظر خود می‌فرستد و منتظر می‌شود تا داده‌ها از حسگرهایی که در آن ناحیه قرار دارند، بازگردند؛ بنابراین، در این روش مشخصات یک حسگر مهم‌تر از آدرس آن است. این مشخصات شامل مکان حسگر، پارامترهایی که حسگر می‌تواند اندازه بگیرد و غیره است.

پروتکل‌های سلسله‌مراتبی

هدف اصلی پروتکل‌های سلسل مراتبی، به‌کارگیری یک روش مناسب جهت استفاده بهینه از منابع انرژی است. در این شبکه مانند شبکه‌های مخابراتی دیگر، قابلیت مقیاس‌پذیری شبکه یکی از مهم‌ترین پارامترهای طراحی در شبکه‌های حسگر بی‌سیم به شمار می‌رود. اگر قرار باشد تمامی بار شبکه روی یک یا چند مسیر خاص باشد، با گسترش شبکه، حجم ترافیک در شبکه به‌شدت افزایش یافته و درنتیجه با بالا رفتن تأخیر، کارایی شبکه افت خواهد کرد. برای بالا بردن قابلیت پوشش مناطق بزرگ‌تر بدون اینکه مشکلی در کیفیت سرویس شبکه به وجود آید، تقسیم‌بندی شبکه به چند خوشه پیشنهاد شده است.

با هدف مصرف بهینه انرژی از ارسال به‌صورت چند گامی در درون یک گروه و همچنین، ترکیب اطلاعات یک گروه با هدف کم کردن داده‌های ارسالی صورت می‌گیرد. پروتکل لیچ، از اولین پروتکل‌های سلسله‌مراتبی بود که برای شبکه‌های حسگر بی‌سیم معرفی شد و دیگر پروتکل‌ها بر مبنای آن طراحی شدند.

پروتکل‌های مبتنی بر موقعیت مکانی

بسیاری از پروتکل‌های مسیریابی برای شبکه‌های حسگر بی‌سیم، به اطلاعات مکانی حسگرها نیاز دارند. در موارد متعددی این اطلاعات برای محاسبه فاصله بین حسگرها به‌منظور تخمین مقدار انرژی موردنیاز برای ارسال داده‌ها به کار گرفته می‌شوند. با توجه به اینکه هیچ شمای آدرس‌دهی اساسی مثل IP در شبکه‌های حسگر بی‌سیم وجود ندارد، اطلاعات جغرافیایی می‌تواند کمک شایانی برای استفاده کارآمد از انرژی باشد؛ به این معنا که اگر حسگرها مکان خود را بدانند، درخواست گره چاهک می‌تواند فقط به آن منطقه‌ای ارسال شود که موردنظر است و بدین‌صورت از حجم اطلاعات ارسالی تا حد زیادی کاسته می‌شود. برخی از پروتکل‌های این دسته در ابتدا برای شبکه‌های اقتضایی طراحی شده‌اند ولی با وجود این، در شبکه‌های حسگر بی‌سیم نیز کاربرد دارند. برخی از پروتکل‌هایی که برای شبکه‌های اقتضایی طراحی شده‌اند، برای شبکه‌های 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 شبکه‌های حسگر بی‌سیم، قابلیت‌ها و نیازمندی‌های جدیدی را طلب می‌کنند، ازجمله:

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

داده‌محور بودن: ارسال داده را کاهش می‌دهد و نیز به علت هم‌آمیزی داده، کاهش افزونگی اطلاعات را شاهد هستیم.

بر اساس توپولوژی محلی: جهت ذخیره‌سازی انرژی ارتباطی، از روش ارتباطی چند پرشه استفاده می‌شود. گره قادر به ذخیره‌سازی حجم زیادی از اطلاعات مسیریابی نیست و مسیریابی نمی‌تواند و نباید محاسبات پیچیده انجام دهد و مکانیسم مسیریابی می‌بایست ساده و کارآمد باشد.

مقیاس‌پذیر توپولوژی شبکه‌ای پویا: پروتکل‌های مسیریابی از روش کاربری توزیع‌شده استفاده می‌کنند و نیز باید جهت بسط در شبکه، راحت و آسان باشند.

تحمل‌پذیری خرابی: ایجاد خرابی در گره و یا خرابی به علت‌های گوناگون نباید در مکانیسم عملکردی مسیریابی خللی ایجاد کند؛ بدین معنا که پروتکل باید در مقابل خرابی تحمل‌پذیر باشد.

همگرایی سریع: الگوریتم مسیریابی می‌بایست ساده بوده و قابلیت سازگاری با تغییر توپولوژی پویا در شبکه را داشته باشد. همچنین، هزینه‌های ارتباطی را کاهش داده و کارایی 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 (Kap & Kung, 2000).

بر اساس نتایج پژوهش حاضر راهکار پیشنهادشده مبتنی بر OBDD برای تخمین قابلیت اطمینان در شبکه‌های حسگر بی‌سیم به‌عنوان یک راهکار بازگشتی است که با کاهش محاسبات اضافی و حذف زیرگراف‌ها توانست الگوریتمی کارا از نظر قابلیت اطمینان را پیشنهاد کند.

نتیجه حاصل از تحلیل و شبیه‌سازی 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، الگوریتم‌هایی پیشنهاد شد که درحالی‌که قابلیت اطمینان مورد انتظار شبکه را برآورده کند، سربار ارسال بسته‌ها نیز افزایش نیابد و مصرف انرژی، کاهش و طول عمر شبکه نیز بالا رود.

LOMDD، یک مسیر را به‌عنوان مسیر اصلی انتخاب می‌کند و سایر مسیرها به‌عنوان 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 به دست 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 بوده و نشان داده شد که نسبت به پروتکل‌های ایستا قابلیت اطمینان را به‌صورت کارا برای شبکه تنظیم می‌کند، سربار محاسباتی و انرژی مصرف‌شده را کاهش می‌دهد و تعداد مسیر بهینه را برای منابع تعیین می‌کند.

واعظی و همکاران (۱۴۰۰) به‌وسیله پروتکل مسیریابی جدید مبتنی بر کیفیت خدمات (QoS) در شبکه‌های حسگر بی‌سیم، میانگین تأخیر را حدود ۳۰ درصد در شبکه‌های با مقیاس بزرگ بهبود دادند. نوری و زینالی (۱۳۹۹) مدلی معرفی کردند که به‌صورت فراگیر باعث کاهش نفوذ نفوذگر برای تضعیف عملکرد شبکه و جلوگیری از حملات فریبکارانه توسط مهاجمان می‌گردد. بهروان و همکاران (۱۳۹۹)، پروتکل کارآمد EEMCA را معرفی کردند. القحطانی در سال ۲۰۲۱، پروتکل مسیریابی با استفاده از چند مسیر (IQMRP) را معرفی کرد. جیا (۲۰۲۱) بیان کرد در پروتکل SEP-EC پیشنهادشده متوسط تأخیر سرتاسری ۰/۵۲ ثانیه است و میانگین گره‌های باقی‌مانده ۸۳/۵ درصد است. لیانگ و همکاران (۲۰۲۱)، الگوریتم مسیریابی تعاونی تطبیقی جدید همراه با DEEC را پیشنهاد دادند. شن و همکاران (۲۰۲۰)، شبکه EECRP با طول عمر بیشتر را معرفی کردند. ژِیکسین و همکاران (۲۰۱۹)، یک پروتکل به نام DETR ارائه دادند.

تاکنون پژوهش‌های بسیاری جهت یافتن پروتکل مناسب انجام شده است. گرچه بسیاری از این تلاش‌ها منجر به ارائه پروتکل‌هایی بهینه شده‌اند اما در مقایسه با سایر پژوهش‌های انجام‌شده، پروتکل AMPRS با قابلیت اطمینان مورد انتظار ۹۰ درصد، پروتکلی مطمئن‌تر به حساب می‌آید.

با توجه به مزیت‌های استفاده از شبکه‌های حسگر بی‌سیم، برطرف کردن مشکلات موجود و ارائه راهکارهای بهتر همچنان مورد توجه است. لذا، به‌منظور پژوهش‌های آتی، گسترش LOMDD برای توزیع بار در میان مسیرهای موجود و گسترش LOMDD برای توزیع بار در میان مسیرهای موجود با استفاده از کدینگ پیشنهاد می‌شود.

همچنین، با هدف بهینه‌سازی مسئله قابلیت اطمینان می‌توان شبکه‌ای را مدل کرد که مسیرهای موردنظر را بر اساس افزایش طول عمر شبکه و کاهش انرژی مصرف‌شده انتخاب کند به‌نحوی‌که قابلیت اطمینان مورد انتظار نیز برآورده شود.

در ضمن می‌توان مسیرهای موجود در شبکه را به‌گونه‌ای تقسیم کرد که از هرکدام از آن‌ها در بازه زمانی خاص و به مدت مشخصی استفاده شود تا علاوه بر تأمین قابلیت اطمینان مورد انتظار، افزایش طول عمر شبکه را موجب شود.

به‌عنوان راهکار سوم، استفاده از یک کدینگ به‌جای کپی بسته‌ها پیشنهاد می‌شود.

منابع

بهروان، کبری، منصفی، رضا، و احمدی ترشیزی، حسن. (۱۳۹۹). پروتکل مسیریابی چندپرشه انرژی- کارآمد در شبکه‌های حسگر بی‌سیم مبتنی بر خوشه با استفاده از بهینه‌سازی کلونی مورچه. *مجله فناوری اطلاعات در طراحی مهندسی*، ۵(۲).

طهماسبی کهیانی. (۱۳۹۱). فیوژن داده در شبکه‌های حسگر بی‌سیم. *دومین کنفرانس ملی مهندسی نرم‌افزار لاهیجان*، لاهیجان.

کردافشاری محمدصادق، موقر رحیم‌آبادی، علی، و میبدی، محمدرضا. (۱۳۹۸). مسیریابی چندپخشی در شبکه‌های حسگر بی‌سیم مقیاس وسیع با استفاده از چارچوب یادگیری تقویتی توزیع‌شده. *پژوهش‌های نوین در ریاضی*، ۵(۲۰).

نوری، حسن، و زینالی، خسرقی. (۱۳۹۹). ارزیابی کارایی پروتکل‌های مسیریابی چند مسیره در تضمین امنیت و حریم خصوصی شبکه‌های حسگر بی‌سیم. *پنجمین کنفرانس ملی محاسبات توزیعی و پردازش داده‌های بزرگ*.

AboElFotoh, H. M., ElMallah, E. S., & Hassanein, H. S. (2006). On the reliability of wireless sensor networks. In *2006 IEEE International Conference on Communications* (Vol. 8, pp. 3455-3460). IEEE.

Alqahtani, A. S. (2021). Improve the QoS using multi-path routing protocol for Wireless Multimedia Sensor Network. *Environmental Technology & Innovation*, *24*, 101850.

Dulman, S., Nieberg, T., Wu, J., & Havinga, P. (2003). Trade-off between traffic overhead and reliability in multipath routing for wireless sensor networks. In *2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003.* (Vol. 3, pp. 1918-1922). IEEE.

Jia, L. (2021). Distributed energy balance routing algorithm for wireless sensor network based on multi-attribute decision-making. *Sustainable Energy Technologies and Assessments*, *45*, 101192.

Kap, B., & Kung, H. T. (2000). GPSR: greedy perimeter stateless routing for wireless sensor networks. In *Proceedings of the ACM/IEEE In· temational Conference on Mobile Computing and Netw orking, Boston, USA* (pp. 243-254).

Liang, J., Xu, Z., Xu, Y., Zhou, W., & Li, C. (2021). Adaptive cooperative routing transmission for energy heterogeneous wireless sensor networks. *Physical Communication*, *49*, 101460.

استناد به این مقاله: عرفانی، رضا، و دشتی، سید ابراهیم. (۱۴۰۳). افزایش قابلیت اطمینان در شبکه‌های حسگر بی‌سیم با استفاده از پروتکل‌های مسیریابی چند مسیره. *فصلنامه پژوهش‌های نوین در شهر هوشمند*، ۲(۴)، ۴۶-۷۱.