(مقاله پژوهشی)

طراحی یک شبکه‌ی ارتباطی با قابلیت اطمینان از پیش‌تعریف‌شده با استفاده از یک الگوریتم تکرارشونده در شبکه‌های حسگر بی‌سیم زیرآب

مسعود شکرنژاد[۱] ، مجید یوسفی[۲]

m.shokrnezhad@aut.ac.ir

۱- دکتری مهندسی فناوری اطلاعات اطلاعات دانشکده‌ی مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر
۲- دانشجوی دکترای مهندسی فناوری اطلاعات دانشگاه صنعتی امیرکبیر

چکیده

امرزه مزایای تجاری و اقتصادی بیشماری از اعماق دریاها و اقیانوس‌ها قابل حصول است. بدیهی است که در راستای بالفعل کردن هر چه بیشتر این مزایا باید بتوان به شکل برخط بر این پهنه‌های آبی نظارت نمود و با تصمیم‌گیری‌های مناسب بر آن‌ها تأثیر گذاشت. یکی از فناوری‌هایی که می‌تواند در این راستا مورد استفاده قرار گیرد، شبکه‌ی حسگر بی‌سیم زیرآبی است. با توجه به گستردگی محیط‌های تحت پوشش و نیازمندی‌هایی مثل قابلیت اطمینان بالا و تأخیر کم، طراحی بهینه این شبکه با پیچیدگی بسیاری مواجه است.

هدف این پژوهش ارائه‌ی روشی برای طراحی بهینه یک شبکه‌ی بی‌سیم زیرآبی جهت تحقق قابلیت اطمینان قابل قبول است. ایده‌ی این مقاله برای کاهش پیچیدگی، تقسیم مسئله به دوقسمت و حل تکرارشونده آن است. در قسمت اول با استفاده از یک مسئله مبتنی بر برنامه‌ریزی خطی، یک شبکه از روترها برای پوشش کل حسگرها ساخته خواهد شد و در قسمت دوم و به شکل تکرارشونده، روترهای افزونه به شبکه ارتباطی اضافه می‌شوند تا شبکه به قابلیت اطمینان مورد نظر برسد. مسئله دوم ضمن متعادل کردن درجه روترها در گراف شبکه، سعی دارد بیشترین یال را به آن اضافه کند تا از این طریق قابلیت اطمینان شبکه بیشینه شود. نتایج شبیه‌سازی‌ها نشان می‌دهد که روش پیشنهادی می‌تواند در زمانی قابل قبول، قابلیت اطمینان شبکه را به شکل قابل توجهی بهبود دهد.

واژگان کلیدی : شبکه‌ی حسگر بی‌سیم زیرآبی، طراحی شبکه، جایگذاری حسگرها، قابلیت اطمینان، بهینه‌سازی، برنامه‌ریزی خطی

تاریخ دریافت مقاله :	۹۹/۰۴/۲۱
تاریخ پذیرش مقاله :	۹۹/۰۷/۲۴

صص ۹-۱

۱ – مقدمه

دریاها و اقیانوس‌ها وسیع‌ترین و مهمترین منابع کره‌ی زمین هستند که تسلط روی آن‌ها می‌تواند مزایای تجاری و اقتصادی بیشماری به ارمغان بیاورد. یکی از فناوری‌هایی که می‌توان در این راستا از آن استفاده کرد، شبکه‌ی حسگر بی‌سیم زیرآبی است که امکان مشاهده‌ی برخط و تصمیم‌گیری و تأثیرگذاری آنی بر اعماق آب‌ها را ممکن می‌سازد. این شبکه گونه‌ای از شبکه‌های حسگر است که در محیط زیر آب جهت جمع‌آوری داده‌های محیطی قرار گرفته و در کاربردهایی همچون نظارت محیطی، اکتشافات زیرآبی و اجتناب از وقوع حوادث کاربرد دارد.

کارایی شبکه‌های بی‌سیم زیرآبی با پارامترهای مختلفی قابل بررسی و ارزش‌گذاری است. با توجه به نامطمئن بودن ارتباطات بی‌سیم در اثر عواملی همچون تداخل (که در محیط زیرآب نسبت به روی آب شدیدتر است)، یکی از مهم‌ترین پارامترها جهت ارزیابی کارایی این نوع شبکه قابلیت اطمینان است. زیرا کاربردهای مختلف (از جمله کاربردهای نظارتی در زیر آب) نیازمند این هستند که شبکه حسگر بی‌سیم به نحوی طراحی شود که با وجود احتمال خطا یا عدم موفقیت در ارسال اطلاعات روی تمام لینک‌های بی‌سیم، احتمال رسیدن اطلاعات به مقصد از طریق آن بسیار بالا باشد. به طور خلاصه با توجه به بلادرنگ بودن کاربردهای مختلف (ایمنی، اقتصادی و دفاعی)، این نوع شبکه نیازمند قابلیت اطمینان ۹۹٪ هستند. به عبارت دقیق‌تر، اکثر کاربردها نیازمند این هستند که تمام اطلاعات جمع‌آوری‌شده توسط حسگرها به کنترل‌کننده‌ی مرکزی برسد. بنابراین باید شبکه‌ای طراحی شود که اطلاعات را از حسگرها سطح دریا یا زیر آب جمع کرده و آن‌ها را با قابلیت اطمینان بالا به دست کنترل‌کننده برساند.

برای حداکثر کردن قابلیت اطمینان شبکه‌ها در گذشته کارهای بسیاری انجام شده است. دسته ای از کارهای قبلی سعی در پیدا کردن بهترین ترکیب یال‌ها در شبکه را داشته‌اند. از جمله این کارها می‌توان به [۶-۱] اشاره کرد. ایراد اصلی این دسته از کارها این است که در شبکه های بی‌سیم نمی‌توان دقیقاً راجع به بودن یا نبودن لینک‌ها بحث کرد. همچنین ممکن است هیچ ترکیب یال ممکنی نتواند قابلیت اطمینان مورد نظر ما را تأمین کند. اشکال بعدی پیچیدگی این روش‌هاست، به طوری که برای شبکه های با تعداد حسگر های بسیار زیاد، قابل استفاده نیستند.

دسته‌ی دیگری از کارها قابلیت اطمینان را در قالب مقاومت در برابر خطا بررسی می‌کنند که از جمله این کارها می‌توان به [۱۰-۷] اشاره کرد. این کارها برای بالا بردن قابلیت اطمینان سعی در ایجاد k مسیر جداگانه دارند، ولی از آنجایی که ساختن این مسیرها پیچیدگی بسیار زیادی دارد، اعمال آن‌ها روی مسئله مدنظر این مقاله ممکن نیست.

دسته دیگر تحقیقات هم کارهایی هستند که روی شبکه های مش انجام شده‌اند. در این شبکه‌ها کارهای زیادی در حوزه جایگذاری حسگرها انجام شده که اهداف بعضی از آن‌ها بی شباهت به اهداف قابل اطمینان کردن شبکه نیست. به عنوان مثال در [۱۱] هدف از جایگذاری حسگرها، بالا بردن گذردهی شبکه است، که در این فعالیت بیشترین جریان ممکن با حل یک مدل خطی بدست می‌آید. سپس برای رسیدن به جریان بهینه بدست آمده، دو ساختار از پیش تعریف شده حسگرها تست می‌شود تا بهترین ساختار انتخاب شود. واضح است که این جایگذاری با حالت بهینه فاصله دارد. در [۱۲] نویسندگان سعی می‌کنند با انتخاب بهترین حسگر های فراگستر و بالا بردن کیفیت TCP ، مسیریابی قابل اطمینان را انجام دهند.

مقاله [۱۳] یکی از کامل‌ترین فعالیتهای انجام شده برای محاسبه قابلیت اطمینان و بهبود آن در شبکه مش است. در این پژوهش با اضافه کردن یک به یک حسگرهای افزونه به توپولوژی اولیه داده شده، مقدار قابلیت اطمینان را به صورت دقیق حساب می‌کنند و در نهایت میزان تغییرات قابلیت اطمینان به ازای توپولوژی‌های مختلف را بررسی می‌کنند. با توجه به این که مقاله، مکان‌های فرضی مشخصی برای اضافه کردن حسگرهای افزونه دارد، جواب بدست آمده نهایی الزاماً جواب بهینه از دیدگاه کمینه کردن تعداد حسگرهای افزونه نیست به طوری که در قسمت کارهای آینده مقاله پیشنهاد شده که مکان و تعداد بهینه این حسگرهای افزونه در شبکه محاسبه شود.

با توجه به موارد بالا می‌توان نتیجه گرفت که خلأ بزرگی در زمینه طراحی یک شبکه کم هزینه و قابل اطمینان برای شبکه‌های حسگر بی‌سیم زیرآبی وجود دارد که هدف

این مقاله طراحی چنین شبکه‌ای است. برای رسیدن به این هدف دو مدل بهینه‌سازی پیشنهاد شده است. مدل اول کمترین تعداد روتر را در شبکه پخش می‌کند به طوری که حسگرهای پخش‌شده بتوانند تمام محیط را پوشش دهند. مدل دوم نیز به ساختار اولیه بدست آمده، روتر اضافه می‌کند تا شبکه به قابلیت اطمینان مورد نظر برسد.

ادامه مقاله حاوی بخش‌های زیر است. در بخش دوم مدل شبکه و روش‌های محاسبه قابلیت اطمینان به طور دقیق بیان می‌شود. در بخش سوم مدل‌های پیشنهادی برای ساخت توپولوژی اولیه و قابل اطمینان کردن آن ارائه می‌شود. در ادامه شبیه‌سازی‌های انجام شده و نتایج آن‌ها بررسی و در بخش پایانی نتایج پژوهش بیان می‌شود.

۲- مدل سیستم

۲-۱- مدل شبکه

همان‌طور که گفته شد هدف این پژوهش، طراحی یک شبکه‌ی بی‌سیم حسگر زیرآبی مطمئن است. ورودی مسئله، مکان حسگرهای پخش‌شده در محیط آبی مورد نظر است. برای مدل کردن این ورودی از یک مجموعه به شکل $N=\{(x_1,y_1),(x_2,y_2),\ldots,(x_n,y_n)\}$ استفاده می‌شود که n تعداد حسگرها و (x_i,y_i) مختصات حسگر i را نشان می‌دهد.

خروجی مسئله نیز به شکل گراف $G=(V,E)$ مدل می‌شود که مجموعه V، روترهای جایگذاری شده در شبکه و مجموعه E یال‌هایی است که بین این روترها برقرار شده است. همچنین مکان این روترها نیز با مجموعه‌ی $R=\{(x_1,y_1),(x_2,y_2),\ldots,(x_m,y_m)\}$ نشان داده می‌شود که m نشان دهنده تعداد روترها و (x_i,y_i) نشان دهنده مختصات روتر i است.

۲-۲- قابلیت اطمینان دقیق k ترمینال

برای محاسبه دقیق قابلیت اطمینان یک شبکه‌ی بی‌سیم با k ترمینال، در [۱۳] فرمولی به شکل زیر ارائه شده است:

$$R^{n_1,\ldots,n_k}(G,p)=\sum_{i=w_{n_1,\ldots,n_k}(G)}^{\epsilon} T_i^{n_1,\ldots,n_k}(G)(1-p)^{\epsilon-i}p^i \quad (۱)$$

در این فرمول $R^{n_1,\ldots,n_k}(G,p)$ نشان‌دهنده مقدار قابلیت اطمینان برای k حسگر از گراف G است. p نیز احتمال ارسال موفق روی هر لینک را نشان می‌دهد. در طرف دوم تساوی، $T_i^{n_1,\ldots,n_k}$ نشان‌دهنده تعداد زیر گراف‌های همبند گراف G با k حسگر و i یال است. کران‌های سیگما نیز از کمترین تعداد یال ممکن برای ساختن یک زیر گراف همبند شروع شده و تا تعداد کل یال‌های گراف ادامه می‌یابد.

۲-۳- حد بالا برای قابلیت اطمینان k ترمینال

برای محاسبه دقیق قابلیت اطمینان نیاز به شمارش تعداد زیر گراف‌های همبند گراف G با k حسگر و i یال است که در فرمول دقیق با نماد $T_i^{n_1,\ldots,n_k}$ نشان داده می‌شود. از آنجایی که فرمول مشخصی برای محاسبه این مقدار وجود ندارد با بزرگ شدن شبکه، شمارش تعداد زیر گراف‌ها بسیار پرهزینه بوده و در شبکه های بزرگ از نظر زمانی ممکن است عملاً یافتن آن غیر ممکن باشد. به همین دلیل در [۱۴] برای محاسبه یک حد بالا برای قابلیت اطمینان از فرمول زیر استفاده شده است:

$$H(d)=1-\left\{\sum_{i=1}^{n} q_i^d \cdot \prod_{k=1}^{m_i}\left(1-q^{d_k-1}\right) \cdot \prod_{k=m_i+1}^{i-1}\left(1-q^{d_k}\right)\right\} \quad (۲)$$

در رابطه (۲) m_i برابر است با $\min(d_i,i-1)$، که d_i نشان دهنده درجه حسگر i و q نشان دهنده احتمال خرابی یک لینک (برابر با $1-p$) یا عدم موفقیت ارسال روی آن لینک است. در این مقاله ثابت شده است که مقدار بدست آمده از این فرمول همیشه یک حد بالا برای مقدار قابلیت اطمینان بهینه است و می‌توان از آن برای محاسبه‌ی قابلیت اطمینان (به جای رابطه‌ی اصلی) استفاده کرد.

۳- تعریف مسئله

مسئله این پژوهش، طراحی یک شبکه‌ی ارتباطی برای حسگرهای بی‌سیم پخش‌شده در محیط کف دریا از طریق جایگذاری روترها است، به‌طوری که شبکه طراحی شده حداقل قابلیت اطمنیان موردنیاز را داشته باشد. چالش مسئله، رسیدن به این هدف با جایگذاری حداقل تعداد روتر است. این مسئله در مدل ۱ بیان شده است:

مدل (۱) مسئله طراحی شبکه مطمئن

$$\min \sum_{r=1}^{R} Z_r$$

subject to

1. $X_{n,r} \le Z_r \qquad \forall\, n, \forall\, r$

2. $\sum_{r=1}^{R} X_{n,r}=1 \qquad \forall n$

3. $\sqrt{(XN_n-XR_r)^2+(YN_n-YR_r)^2} \le a+(1-X_{n,r})*M \qquad \forall n, \forall r$

4. $\text{Reliability}(G,p) \ge \hat{R}$

متغیرهای تصمیم‌گیر و پارامترهای ورودی این مسئله به شرح زیر می‌باشند:

۱) Z_r : متغیر باینری که در صورت قرار گرفتن روتر r ام در محیط مقدار ۱ و در غیر این صورت مقدار صفر می‌گیرد.

۲) $X_{n,r}$: متغیر باینری که در صورت وصل شدن حسگر n به روتر r مقدار یک و در غیر این صورت مقدار صفر می‌گیرد.

۳) XR_r: متغیر حقیقی که مؤلفه x مختصات قرارگیری روتر r را مشخص می‌کند.

۴) YR_r : متغیر حقیقی که مؤلفه y مختصات قرارگیری روتر r را مشخص می‌کند.

۵) $Reliability\ (G,p)$: رابطه مربوط به محاسبه قابلیت اطمینان شبکه حاصل از رله‌های کاشته‌شده در محیط که می‌توان فرمول دقیق آن را در روابط ۱ و ۲ دید.

۶) $\hat{R}$، XR_n ، YR_r و a ورودی‌های مدل هستند که به ترتیب نشان‌دهنده مقدار قابلیت اطمینان موردنظر، مولفه x و y مختصات قرارگیری حسگرها و شعاع تحت پوشش هر حسگر هستند.

تابع هدف این مسئله نشان دهنده کمترین تعداد روتری است که باید در محیط قرار داده شود. این هدف با توجه به این نکته انتخاب شده که هزینه‌ی تجهیزات زیرآبی بسیار زیاد است. در حالی که در شبکه‌های بی‌سیم معمولی ارزش حسگرها و سایر تجهیزات به مراتب کمتر از تجهیزاتزیرآبی است و در آن شبکه‌ها محدودیت اصلی تعداد حسگرها و روترها نیست و می‌توان هدف طراحی شبکه را به اهدافی همچون افزایش گذردهی شبکه تغییر داد.

محدودیت‌های مسئله نیز به شکل زیر قابل توضیح هستند:

۱) محدودیت اول بیان می‌کند که در صورتی می‌توان با یک روتر ارتباط برقرار کرد که آن روتر در محیط قرار داده شده باشد.

۲) محدودیت دوم تضمین می‌کند که هر حسگر باید با یک روتر ارتباط برقرار کند.

۳) محدودیت سوم بیان می‌کند که اگر حسگری در محدوده یک روتر بود باید به آن وصل شود. با توجه به استفاده از تکنیک Big M، این محدودیت فقط برای هر روتر و حسگرهای متصل شده به آن اعمال می‌شود. همچنین با اعمال این محدودیت، مکان روترها نیز تعیین می‌شود.

۴) محدودیت چهارم تضمین می‌کند که قابلیت اطمینان شبکه ایجاد شده روترها، حداقل به اندازه قابلیت اطمینان موردنظر باشد.

۴- راه حل پیشنهادی

در این مقاله، چهارچوب نظری پیشنهادی برای حل مسئله مطرح شده، استفاده از مدل‌های بهینه‌سازی است. با توجه به تعریف مسئله در بخش قبل، هدف نوشتن مدلی است که شبکه‌ای قابل اطمینان از روترها برای پوشش شبکه‌ی حسگر زیرآبی تولید کند. از آنجایی که محاسبه قابلیت اطمینان دقیق گراف شبکه پیچیدگی محاسباتی بسیار بالایی دارد، حل مسئله مطرح شده در مدل ۱ ، با توجه به ابزارهای حل موجود غیرممکن است. حتی اگر به جای محاسبه دقیق قابلیت اطمینان از مقدار حد بالای آن استفاده کنیم، باز هم به علت وجود روابط نمایی در فرمول نمی‌توان از قابلیت‌های برنامه‌ریزی خطی استفاده کرد و در نتیجه حل مسئله برای اندازه های واقعی غیر ممکن خواهد بود.

ایده پیشنهادی مقاله حاضر برای کاهش پیچیدگی، تقسیم کردن مسئله به دو بخش و حل جداگانه آن‌هاست. این دو بخش عبارتند از:

۱) تولید توپولوژی اولیه‌ای از روترها به‌طوری که تمام حسگر-ها تحت پوشش قرار گیرند.

۲) اضافه کردن روترهای افزونه برای بالا بردن قابلیت اطمینان توپولوژی اولیه

در ادامه این دو بخش توضیح داده خواهد شد.

۴-۱- ساختن توپولوژی اولیه

مسئله‌ای که برای ساختن توپولوژی اولیه‌ای از روترها نوشته شده در مدل ۲ نشان داده شده است.

مدل (۲) مسئله ساختن توپولوژی اولیه

$$min \sum_{r=1}^{R} Z_r$$

subject to

1. $X_{n,r} \le Z_r \qquad \forall n, \forall r$

2.
$$\sum_{r=1}^{R} X_{n,r}=1 \qquad \forall\, n$$
3. $|XN_n-XR_r|\le a+(1-X_{n,r})*M \qquad \forall\, n, \forall\, r$
4. $|YN_n-YR_r|\le a+(1-X_{n,r})*M \qquad \forall\, n, \forall\, r$
5. $XR_r\le Z_r*M \qquad \forall\, r$
6. $YR_r\le Z_r*M \qquad \forall\, r$

متغیرها و پارامترهای استفاده شده در این مدل مانند مدل ۱ است. تابع هدف این مدل تضمین می‌کند که برای پوشش محیط، کمترین تعداد روتر در آن قرار داده شود. محدودیت‌های مدل عبارتند از:

۱) محدودیت اول و دوم دقیقا مانند محدودیت‌های مدل ۱ هستند.
۲) محدودیت سوم تضمین میکند که هر حسگر باید با یک روتر ارتباط برقرار کند.
۳) محدودیت‌های سوم و چهارم بیان می‌کنند که اگر حسگری در محدوده یک روتر بود باید به آن وصل شود. از آن‌جایی که محدودیت سوم مدل ۱ خطی نیست، با هدف ساده‌سازی و کاهش پیچیدگی، در این مدل، این محدودیت با محدودیت‌های سوم و چهارم جایگزین شده است.
۴) محدودیت پنجم و ششم تضمین می‌کند که تنها در شرایطی مختصات یک روتر تعیین شود که آن روتر در محیط قرار داده شده باشد.

با توجه به ساده‌سازی‌های انجام شده، این مسئله در قالب برنامه‌ریزی صحیح خطی نوشته شده و به آسانی با استفاده از ابزارهای حل مسائل بهینه‌سازی مانند CVX یا Zimpl قابل حل است.

۴-۲- قابل اطمینان کردن توپولوژی اولیه

برای افزایش قابلیت اطمینان شبکه باید مدلی نوشته شود که با گرفتن خروجی‌های مدل ۱، مکان روترها و یال‌های افزونه را برگرداند. برای این کار لازم است رابطه ۱ یا ۲ وارد مدل شود. همان‌طور که ذکر شد، رابطه ۱ حاوی پارامتری است که نشان‌دهنده تعداد زیر گراف‌های همبند گراف ورودی است. از آنجایی که این پارامتر فرمولی برای محاسبه ندارد، پس نمی‌توان در حین اجرای مدل به صورت برخط مقدار آن را بدست آورد. رابطه ۲ نیز دارای عبارات نمایی است که حل مسئله حاوی این رابطه با استفاده از ابزارهای حل مسائل بهینه‌سازی ممکن نیست.

پیشنهاد این مقاله برای افزایش قابلیت اطمینان، اضافه کردن محدودیت‌هایی برای ایجاد افزونگی در یال‌های گراف شبکه به‌جای استفاده از رابطه ۱ یا ۲ در مدل است. با توجه به مطالعات انجام شده، که مراحل و نتایج آن در بخش ارزیابی ارائه شده است، برای افزایش حداکثری قابلیت اطمینان گراف شبکه باید حداکثر تعداد یال ممکن را به روترهایی با کمترین درجه اضافه کرد. مسئله‌ای که بتوان با حل آن به چنین هدفی رسید در مدل ۳ فرموله شده است:

مدل (۳) مسئله قابل اطمینان کردن توپولوژی اولیه

$$\max \sum_{n=1}^{N}\sum_{r=1}^{R} X_{n,r}$$
subject to
1. $X_{n,r}\le Z_r \qquad \forall\, n, \forall\, r$
2. $\sum_{r=1}^{R} Z_r=1 \qquad \forall\, n$
3. $|XS_n-XR_r|\le a+M(1-X_{n,r}) \qquad \forall\, n, \forall\, r$
4. $|YS_n-YR_r|\le a+M(1-X_{n,r}) \qquad \forall\, n, \forall\, r$
5. $XR_r\le Z_r*M \qquad \forall\, r$
6. $YR_r\le Z_r*M \qquad \forall\, r$
7. $Degree_n+\sum_{r=1}^{R} X_{(n,r)}\ge \beta*temp_n \qquad \forall\, n$
8. $\sum_{n=1}^{N} temp_n\ge\gamma$

در این مدل، علاوه بر متغیرهای مدل ۱ و ۲، متغیر $temp_n$ وجود دارد. این متغیر یک متغیر باینری است که اگر درجه روتر i بیشتر از مقدار درجه کمینه باشد، برابر با یک و در غیر این صورت برابر با صفر خواهد بود. علاوه بر پارامترهای مطرح شده در مدل‌های ۱ و ۲، پارامترهای زیر نیز به عنوان ورودی به این مدل داده می‌شوند:

۱) $Degree_n$: پارامتر حقیقی نشان‌دهنده درجه هر روتر.
۲) β : نشان‌دهنده درجه‌ای که روترهای با درجه کمینه باید به آن درجه برسند.
۳) γ : یک عدد است که کران پایین برای مجموع $temp_n$ تعیین کرده و تضمین می‌کند که در هر بار اجرا حداقل یک روتر با درجه کمینه پوشش داده شود.

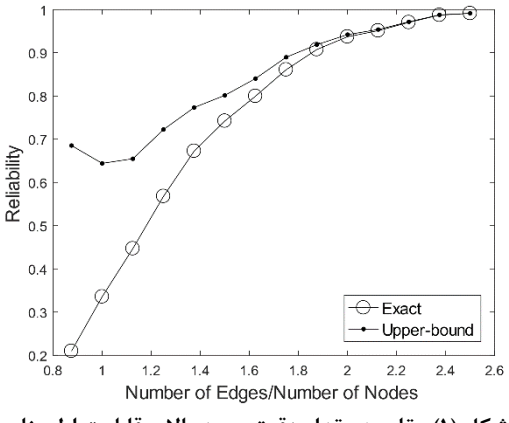
همچنین محدودیت‌های مدل عبارتند از:

۱) محدودیت اول و محدودیت‌های سوم تا ششم دقیقا مانند محدودیت‌های مدل ۲ هستند.

۲) محدودیت دوم تضمین می‌کند که در هر بار اجرا فقط یک روتر به شبکه اضافه شود. دلیل این کار کاهش پیچیدگی محاسباتی مدل است به طوری که در هر بار اجرا یک روتر با محدودیت‌های ذکر شده به شبکه اضافه می‌شود. بعد از هر تکرار مقدار قابلیت اطمینان برای شبکه حساب شده و مقدار آن با مقدار مورد انتظار مقایسه می‌شود. اگر مقدار مورد انتظار بدست آمده بود، روند حل مسئله پایان می‌یابد ولی اگر این اتفاق نیفتاده بود، اجرای مدل دوباره تکرار می‌شود. این فرایند تا جایی ادامه می‌یابد که حداقل مقدار قابلیت اطمینان مورد انتظار بدست آمده باشد.

۳) محدودیت‌های هفتم و هشتم تضمین می‌کنند که حداقل یکی از روترهای با درجه کمینه تحت پوش روتر افزونه قرار بگیرد. برای رسیدن به این هدف، مقدار γ، یک واحد بیشتر از تعداد روترهایی که درجه آن‌ها بیش از مقدار کمینه است درنظر گرفته می‌شود. این مقداردهی باعث می‌شود که در محدودیت هشتم، $temp_n$ برای حداقل γ روتر برابر با یک شود. در این شرایط محدودیت هفتم تضمین می‌کند که یال‌های افزونه به روترهایی با $temp_n$ برابر با یک اضافه شده و درجه آن‌ها حداقل برابر با β شود. چون یکی از این روترها، روتری با حداقل درجه است، قطعا روتر افزونه به جایی اضافه خواهد شد که در همسایگی این روتر بوده و در عین حال حداکثر یال ممکن را ایجاد کند.

به این ترتیب در هر بار اجرای این مدل یک روتر افزونه به نحوی به شبکه اضافه می‌شود که روترهای کم‌درجه پوشش داده شده و بیشترین یال افزونه در شبکه ایجاد شود. در اجرای اول این مدل، خروجی مدل ۲ و در اجرای i ام، روترهای حاصل از مدل ۲ به‌اضافه روترهای اضافه شده تا تکرار $(i-1)$ ام به عنوان ورودی آن درنظر گرفته می‌شوند.



شکل (۱) مقایسه مقدار دقیق و حد بالای قابلیت اطمینان

۵- ارزیابی

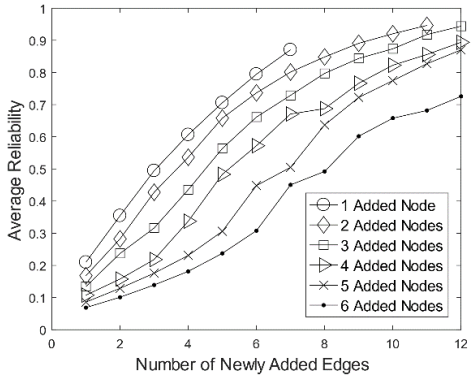
در این قسمت مطالب مطرح شده در قسمت‌های قبل با استفاده از شبیه‌سازی عددی ارزیابی می‌شود. بخش اول مربوط به مقایسه رابطه ۱ و ۲ و اعتبارسنجی رابطه ۲ برای محاسبه قابلیت اطمینان است. بخش دوم ایده پیشنهادی در مدل ۳ برای افزایش قابلیت اطمینان را نشان می‌دهد، در بخش سوم مثالی از طراحی شبکه مطمئن ارائه شده و بخش آخر مربوط به ارزیابی راه‌حل پیشنهادی است.

۵-۱- مقایسه روش‌های محاسبه قابلیت اطمینان

با استفاده از روابط ۱ و ۲ می‌توان قابلیت اطمینان گراف شبکه را محاسبه کرد. رابطه ۱ این مقدار را به شکل دقیق محاسبه می‌کند اما فرمول بسته‌ای برای یافتن جواب آن وجود ندارد. بنابراین ناچارا باید از رابطه ۲ استفاده کرد. این رابطه حد بالای قابلیت اطمینان را محاسبه می‌کند. اگر اختلاف حد بالا و مقدار دقیق قابلیت اطمینان، محسوس باشد عملاً نتایج دقیق نخواهد بود. برای ارزیابی رابطه ۲، به ازای ۱۰۰۰ گراف تصادفی مقدار دقیق و حد بالای قابلیت اطمینان با استفاده از روابط ۱ و ۲ محاسبه شده که میانگین نتایج بدست آمده را می‌توان در شکل ۱ دید.

همان‌طور که مشاهده می‌شود اگر نسبت تعداد یال‌ها به تعداد روترها در شبکه زیاد شود مقدار دقیق و مقدار حد بالا به هم نزدیک می‌شوند. از آنجایی که هدف پژوهش حاضر افزایش این نسبت است، در این پژوهش می‌توان از این اختلاف صرف نظر کرد و از رابطه ۲ برای محاسبه قابلیت اطمینان گراف شبکه استفاده کرد.

۵-۲- تأثیر پارامترهای مختلف در قابلیت اطمینان



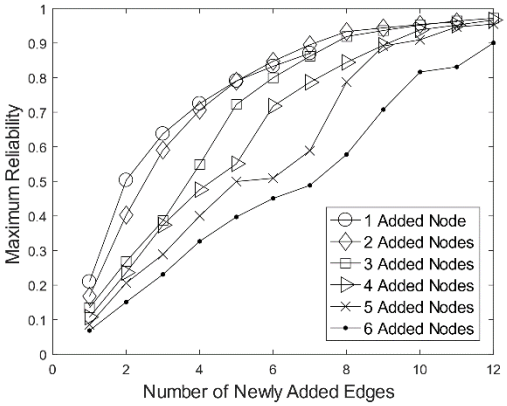
شکل (۲) میانگین تأثیر اضافه کردن روترها و یال‌های افزونه روی قابلیت اطمینان

همانطور که در بخش ۴-۲ اشاره شد، می‌توان با اضافه کردن محدودیت‌هایی که منجر به افزونگی در گراف شبکه شود، قابلیت اطمینان ان را افزایش داد. در این بخش سه نوع افزونگی بررسی شده و نشان داده شده که روش انتخاب شده بهترین نوع افزونگی است.

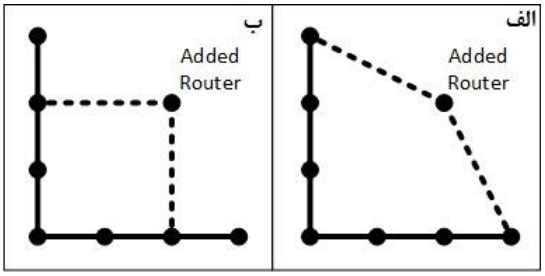
برای رسیدن به این هدف، توپولوژی اولیه [۱۳] به عنوان توپولوژی پایه در نظر گرفته شده است. سپس به صورت تصادفی روتر های افزونه به شبکه اضافه شده و قابلیت اطمینان با استفاده از رابطه ۲ محاسبه شده است. نتایج حاصل از شبیه‌سازی را می‌توان در شکل ۲ دید.

در این شکل محور عمودی نشان‌دهنده مقدار قابلیت اطمینان گراف شبکه و محور افقی نشان‌دهنده تعداد یال‌های افزونه‌ای است که با اضافه کردن تصادفی تعداد مشخصی روتر، ممکن است به گراف شبکه اضافه شود. هر کدام از منحنی‌ها نیز مربوط به افزودن تعداد مشخصی روتر به شبکه اولیه است. به عنوان مثال منحنی اول (دایره) مربوط به افزودن یک روتر است که قابلیت اضافه کردن یک تا هفت یال جدید به شبکه را دارد. این نمودارها حاصل میانگین گیری از ۱۰۰۰ نمونه تصادفی هستند.

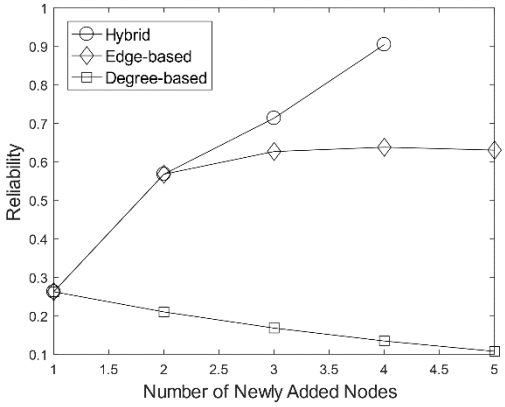
این نمودار نشان می‌دهد که قابلیت اطمینان گراف رابطه مستقیم با تعداد یال‌های آن دارد. این نتیجه منطقی است زیرا با افزایش تعداد یال‌ها، تعداد زیر گراف‌های همبند بیشتر شده و قابلیت اطمینان شبکه افزایش می‌یابد. البته همان‌طور که از شکل ۲ پیداست، اگر تعداد یال‌ها را ثابت فرض کنیم، به ازای افزایش تعداد روترها، قابلیت اطمینان کاهش می‌یابد که این نتیجه با توجه به کاهش تعداد



شکل (۳) حداکثر تأثیر اضافه کردن روترها و یال‌های افزونه روی قابلیت اطمینان



شکل (۴) الف) روتر افزونه یال‌های خود را به روتر های با درجه کمتر اضافه می‌کند. ب) روتر افزونه یال‌های خود را به روتر های با درجه کمتر اضافه نمی‌کند.



شکل (۵) مقایسه سه روش مکاشفه ای ارائه شده

زیرگراف‌ها منطقی است. پس می‌توان از شکل ۲ می‌توان نتیجه گرفت که اگر مکان روتر افزونه به نحوی انتخاب شود که بیشترین یال را در شبکه ایجاد کند، می‌توان قابلیت اطمینان را افزایش داد.

نمودارهای شکل ۳، برخلاف شکل ۲، حاصل ماکزیمم‌گیری از ۱۰۰۰ نمونه تصادفی هستند. با توجه به اختلافی که بین مقادیر میانگین در شکل ۲ و مقادیر بیشینه در شکل ۳ وجود دارد، واضح است که علاوه بر ایجاد افزونگی در یال‌های گراف شبکه، عوامل دیگری در افزایش قابلیت اطمینان شبکه تأثیرگذار هستند. مطالعات انجام شده بر روی نمونه‌های بیشینه نشان می‌دهد که اگر اضافه کردن روتر افزونه و ایجاد یال‌های افزونه در شبکه منجر به افزایش درجه روترهای کم‌درجه شود، قابلیت اطمینان رشد سریع‌تری نسبت به حالت‌های دیگر خواهد داشت. نمونه‌ای از این حالت در شکل ۴ قابل مشاهده است.

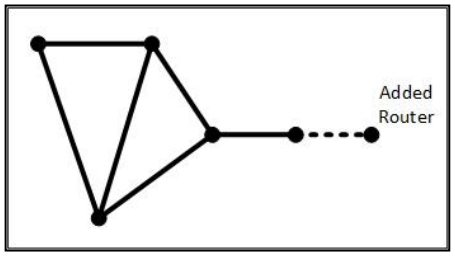
شکل ۴ نشان‌دهنده دو حالت مختلف افزودن یک روتر و دو یال به شبکه است. در شکل ۴-الف دو یال افزونه با

روترهایی که دارای درجه ۱ هستند برقرار و قابلیت اطمینان شبکه برابر با ۰,۴۶ شده است (با فرض این که احتمال ارسال موفق روی هر لینک برابر با ۰,۸ باشد) در حالی که در شکل ۴-ب یال‌های افزونه به روترهایی با درجه ۲ اضافه و قابلیت اطمینان گراف حاصل برابر با ۰,۳۷ شده است. پس می‌توان مشاهده کرد که افزایش درجه روترهای کم‌درجه، تأثیر قابل توجهی روی قابلیت اطمینان دارد.

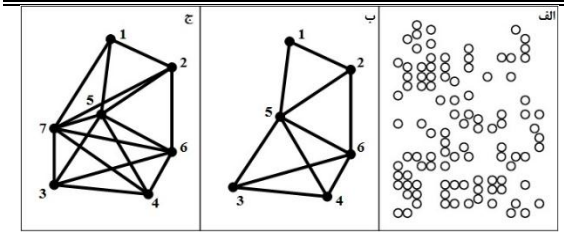
همانطور که اشاره شد، افزایش تعداد یال‌های گراف شبکه و درجه روترهای کم‌درجه، عوامل تأثیرگذار در افزایش قابلیت اطمینان هستند. قابل پیش‌بینی است که افزایش همزمان این دو عامل می‌تواند تأثیر بیشتری نسبت به افزایش تک‌تک آن‌ها داشته باشد.

شکل ۵ نتایج حاصل از افزایش یال‌ها، افزایش درجه روترهای کم‌درجه و افزایش همزمان این دو عامل در افزایش قابلیت اطمینان توپولوژی اولیه [۱۳] را نشان می‌دهد.

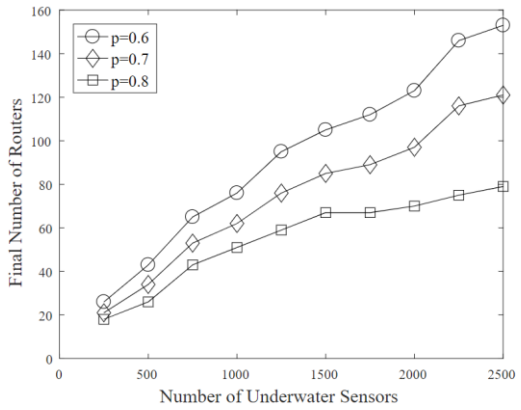
همان‌طور که در شکل ۵ قابل مشاهده است، افزایش تعداد یال‌ها (نمودار لوزی)، ابتدا رشد زیادی در قابلیت اطمینان ایجاد می‌کند، اما بعد از آن تقریباً رشد قابلیت اطمینان در شبکه متوقف می‌شود. دلیل این امر هم این است که توازن یال‌ها در شبکه به هم می‌خورد و روترهایی که درجه بالایی دارند در هر مرحله به درجه آن‌ها اضافه می‌شود، در حالی که روترهای دیگر همواره درجه پایینی دارند. این امر باعث توقف رشد قابلیت اطمینان در شبکه می‌شود. نمودار دوم (مربعی) نتیجه حاصل از افزایش درجه روترهای کم‌درجه را نشان می‌دهد. در بدترین حالت، این رویکرد یک روتر برگ افزونه به گراف شبکه اضافه کرده و تعداد یال‌های شبکه را تنها یک واحد افزایش می‌دهد. نمونه‌ای از این حالت را می‌توان در شکل ۶ دید.



شکل (۶) بدترین حالت افزودن روتر به شبکه با هدف افزایش درجه روترهای کم درجه



شکل (۷) الف) حسگر های اولیه ب)روترهای مدل اول ج) روترهای اضافه شده برای افزایش قابلیت اطمینان



شکل (۸) تأثیر اندازه شبکه حسگر زیرآبی و قابلیت اطمینان لینک‌ها در تعداد نهایی روترهای شبکه ارتباطی

در این شکل روتر افزونه با هدف افزایش درجه روتر کم‌درجه به شبکه اضافه شده اما خود به یک روتر کم‌درجه دیگر تبدیل شده است. بنابراین در بدترین حالت این روش بهبودی حاصل نمی‌کند. اما چون رویکرد سوم به طور همزمان بیشترین یال را به شبکه اضافه کرده و سعی در افزایش درجه روترهای کم‌درجه دارد، عملکرد بهتری نیز نسبت به بقیه از خود نشان می‌دهد و بعد از اضافه کردن ۳ روتر به قابلیت اطمینان ۹۰٪ می‌رسد. بنابراین رویکردی که برای نگارش مدل ۳ در نظر گرفته شده، موثرترین روش در افزایش قابلیت اطمینان گراف شبکه خواهد بود.

۵-۳- مثالی از طراحی شبکه مطمئن

در این بخش نمونه‌ای از طراحی شبکه ارتباطی مطمئن ارائه شده است. برای این کار به صورت تصادفی ۱۰۰ حسگر را در محیط پخش می‌کنیم.

شکل ۷-الف این حسگرها را نشان می‌دهد. در مرحله اول مدل ۱ اجرا شده و شبکه‌ای از روترها برای پوشش حسگرها ایجاد می‌شود. این شبکه در شکل ۷-ب قابل مشاهده است. با فرض این که احتمال ارسال موفق روی

هر لینک برابر با ۰,۸ است، قابلیت اطمینان شبکه حاصل ۰,۹۲ خواهد بود. اگر این عدد بزرگتر یا مساوی مقدار مدنظر باشد، می‌توان روند طراحی را پایان داد. در غیر این صورت مدل ۳ اجرا می‌شود تا روترهای افزونه به شبکه اضافه شود. نتیجه حاصل در شکل ۷-ج قابل مشاهده است. در این مرحله روتر ۷ به شبکه اضافه شده است. با اضافه شدن این روتر قابلیت اطمینان شبکه به ۰,۹۸ رسیده است که برابر با مقدار مدنظر است. بنابراین شبکه ارتباطی نهایی در شکل ۷-ج قابل مشاهده است.

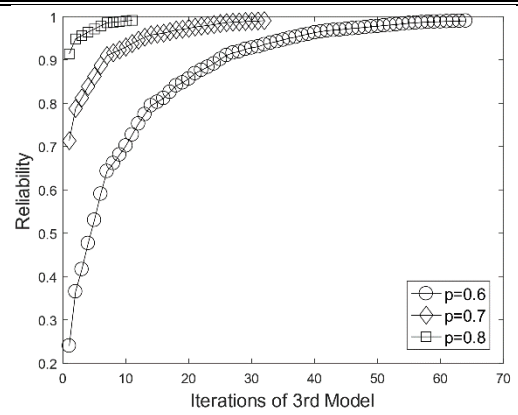
۵-۴- ارزیابی روش ارائه‌شده

پس از صحت‌سنجی روش پیشنهادی و ارائه مثالی از چگونگی اجرای آن، در این بخش به بررسی و ارزیابی نتایج راه‌حل پیشنهادی می‌پردازیم. شکل ۸ تأثیر اندازه شبکه حسگر زیرآبی و قابلیت اطمینان تک لینک (p) روی تعداد روترهای شبکه ارتباطی را بررسی می‌کند.

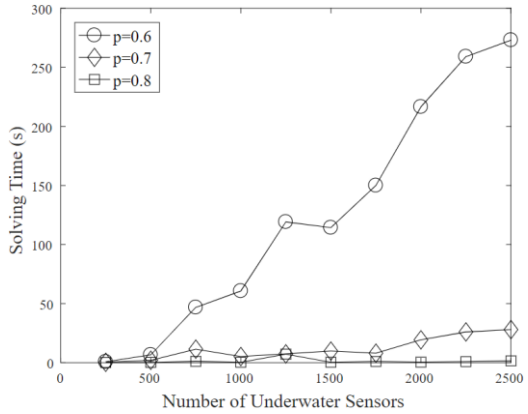
با فرض این‌که قابلیت اطمینان موردنیاز شبکه ۰,۹۹ باشد، می‌توان مشاهده کرد که با افزایش اندازه شبکه و کاهش قابلیت اطمینان لینک‌ها، تعداد روترهای بیشتری برای طراحی شبکه ارتباطی مورد نیاز خواهد بود. همچنین دیده می‌شود که شیب افزایشی تعداد رله‌ها در شبکه‌ای که لینک‌های نامطمئن دارد بیشتر از شبکه‌ای است که لینک‌های آن مطمئن هستند. دلیل این امر ناچیز بودن تأثیر افزودن هر روتر در افزایش قابلیت اطمینان

است به‌طوری که برای رسیدن به حد موردنظر، روترهای افزونه زیادی مورد نیاز خواهد بود.

در شکل ۹ تعداد دفعات اجرای مدل ۳ برای رسیدن به قابلیت اطمینان مورد نظر بررسی شده است. محور افقی این شکل نشان‌دهنده تعداد تکرارهای مدل ۳ و محور عمودی نشان‌دهنده قابلیت اطمینان بدست آمده در هر تکرار از این مدل است. در این شکل فرض شده که در شبکه حسگر زیرآبی ۲۵۰۰ حسگر وجود دارد و شبکه ارتباطی باید حداقل قابلیت اطمینان ۰,۹۹ داشته باشد. همان‌طور که در شکل دیده می‌شود، در صورتی که لینک‌های شبکه مطمئن باشند (p مقدار زیادی داشته باشد) تعداد دفعات تکرار



شکل (۹) تأثیر قابلیت اطمینان لینک‌ها در تعداد دفعات اجرای مدل ۳ برای رسیدن به قابلیت اطمینان ۰,۹۹



شکل (۱۰) تأثیر اندازه شبکه و قابلیت اطمینان لینک‌ها در زمان اجرای روش پیشنهادی

کمتر و در صورتی که لینک‌ها نامطمئن باشد، تعداد دفعات اجرا بیشتر خواهد بود. لازم به ذکر است که روش پیشنهادی برای افزایش قابلیت اطمینان در هر تکرار یک روتر افزونه به شبکه اضافه می‌کند (طبق محدودیت دوم مدل ۳).

حال که تعداد دفعات اجرای روش پیشنهادی بررسی شد می‌توان پیش‌بینی کرد که زمان اجرا رابطه عکس با قابلیت اطمینان لینک‌ها (p) داشته باشد به طوری که با افزایش p زمان لازم برای طراحی شبکه مطمئن کاهش یافته و با کاهش p این زمان افزایش خواهد یافت. این نتیجه‌گیری توسط شکل ۱۰ تایید می‌شود.

البته باید توجه داشت که زمان لازم برای اجرای مدل ۲ در هر مرحله فارغ از اندازه شبکه و مقدار p است و تنها دلیلی که باعث افزایش زمان اجرای روش به ازای p کم می‌شود، تعداد دفعات اجرای بالای آن است.

۶- نتیجه‌گیری

در این مقاله مسئله طراحی شبکه ارتباطی مطمئن برای برقراری ارتباط میان حسگرهای شبکه حسگر زیرآبی با توجه به نیازمندی‌های این شبکه مورد توجه قرار گرفت. با توجه به پیچیدگی مسئله، راه‌حل در دو بخش ساختن توپولوژی اولیه و قابل اطمینان کردن این توپولوژی ارائه شد. بخش اول شامل مدلی برای قرار دادن کمترین روتر در شبکه بود به نحوی که تمام حسگرهای شبکه حسگر زیرآبی پوشش داده شود. در بخش دوم نیز برای قابل اطمینان کردن توپولوژی اولیه، مدلی نوشته شد که با هدف افزایش تعداد یال‌های شبکه و درجه روترهای کم‌درجه، روترهای افزونه را به شبکه اضافه می‌کرد. همانطور که در بخش ارزیابی مشاهده شد، برای شبکه‌ای با اندازه واقعی، در صورتی که قابلیت اطمینان لینک‌های شبکه خیلی پایین نباشد، با استفاده از روش ارائه شده می‌توان در زمان قابل قبولی شبکه ارتباطی را طراحی کرد.

جهت ادامه‌ی کار حاضر و در راستای تکمیل آن می‌توان اهداف ارتباطی دیگری همچون کاهش تأخیر را در کنار بهبود قابلیت اطمینان در نظر گرفت. همچنین می‌توان احتمال خرابی حسگرها و رله‌ها را نیز در نظر گرفت، یا محدودیت‌های مربوط به قرار دادن حسگرها و روترها در محیط را از حالت دو بعدی به حالت سه بعدی گسترش داد تا نتایج دقیق‌تری حاصل شود.

۷- مراجع

[1] Lin Lin and M. Gen, "A Self-controlled Genetic Algorithm for Reliable Communication Network Design," in 2006 IEEE International Conference on Evolutionary Computation, Jul. 2006, pp. 640–647, doi: 10.1109/CEC.2006.1688371.

[2] T. H. Bhuiyan, H. R. Medal, and S. Harun, "A stochastic programming model with endogenous and exogenous uncertainty for reliable network design under random disruption," European Journal of Operational Research, vol. 285, no. 2, pp. 670–694, Sep. 2020, doi: 10.1016/j.ejor.2020.02.016.

[3] S. Kharbash and W. Wang, "All-Terminal Network Reliability Optimization in Fading Environment via Cross Entropy Method," in 2010 IEEE International Conference on Communications, May 2010, pp. 1–5, doi: 10.1109/ICC.2010.5501918.

[4] S. Duan, S. Lee, S. Chinthavali, and M. Shankar, "Reliable communication models in interdependent critical infrastructure networks," in 2016 Resilience Week (RWS), Aug. 2016, pp. 152–157, doi: 10.1109/RWEEK.2016.7573324.

[5] V. Kounev, M. Lévesque, D. Tipper, and T. Gomes, "Reliable Communication Networks for Smart Grid Transmission Systems," J Netw Syst Manage, vol. 24, no. 3, pp. 629–652, Jul. 2016, doi: 10.1007/s10922-016-9375-y.

[6] J. Nematian, "Reliable hub-and-spoke network design problems under uncertainty through multi-objective programming," Iranian Journal of Fuzzy Systems, vol. 17, no. 4, pp. 179–198, Aug. 2020, doi: 10.22111/ijfs.2020.5414.

[7] V. K. Akram, O. Dagdeviren, and B. Tavli, "Distributed k-Connectivity Restoration for Fault Tolerant Wireless Sensor and Actuator Networks: Algorithm Design and Experimental Evaluations," IEEE Transactions on Reliability, pp. 1–14, 2020, doi: 10.1109/TR.2020.2970268.

[8] Aditi, R. Pai, and S. Mini, "Optimization of Transmission Range for a Fault Tolerant Wireless Sensor Network," in Distributed Computing and Internet Technology, Cham, 2019, pp. 235–242, doi: 10.1007/978-3-030-05366-6_19.

[9] E. Szlachcic, "Fault Tolerant Topological Design for Computer Networks," in 2006 International Conference on Dependability of Computer Systems, May 2006, pp. 150–159, doi: 10.1109/DEPCOS-RELCOMEX.2006.25.

[10] D. Zili, Y. Nenghai, and L. Zheng, "Designing Fault Tolerant Networks Topologies Based on Greedy Algorithm," in 2008 Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, Jun. 2008, pp. 227–234, doi: 10.1109/DepCoS-RELCOMEX.2008.35.

[11] F. Li, Y. Wang, and X.-Y. Li, "Gateway Placement for Throughput Optimization in Wireless Mesh Networks," in 2007 IEEE International Conference on Communications, Jun. 2007, pp. 4955–4960, doi: 10.1109/ICC.2007.818.

[12] S. Roy, H. Pucha, Z. Zhang, Y. C. Hu, and L. Qiu, "Overlay Node Placement: Analysis, Algorithms and Impact on Applications," in 27th International Conference on Distributed Computing Systems (ICDCS '07), Jun. 2007, pp. 53–53, doi: 10.1109/ICDCS.2007.127.

[13] G. Egeland and P. Engelstad, "The availability and reliability of wireless multi-hop networks with stochastic link failures," Selected Areas in Communications, IEEE Journal on, vol. 27, no. 7, pp. 1132–1146, Sep. 2009, doi: 10.1109/JSAC.2009.090910.

[14] Rong-Hong Jan, "Design of reliable networks," in [Conference Record] SUPERCOMM/ICC '92 Discovering a New World of Communications, Jun. 1992, pp. 191–196 vol.1, doi: 10.1109/ICC.1992.268264