طراحی شبکه ارتباطی بی‌سیم قابل اطمینان برای شبکه هوشمند برق با استفاده از برنامه‌ریزی خطی

مسعود شکرنژاد[1] سیاوش خرسندی[2]

۱- کارشناسی ارشد- دانشکده مهندسی کامپیوتر و فناوری اطلاعات - دانشگاه صنعتی امیرکبیر- تهران- ایران
m.shokrnezhad@aut.ac.ir
۲- دانشیار- دانشکده مهندسی کامپیوتر و فناوری اطلاعات - دانشگاه صنعتی امیرکبیر - تهران- ایران
khorsandi@aut.ac.ir

چکیده: ویژگی‌های متناقض شبکه هوشمند برق همچون گستردگی در پهنای شهر و نیازمندی‌هایی مثل قابلیت اطمینان بالا (بالاتر از ۰,۹۸) و تأخیر کم (در حد ثانیه و میلی ثانیه)، طراحی شبکه ارتباطی برای آن را با پیچیدگی زیادی مواجه کرده است. هدف این پژوهش در نظر گرفتن نیازمندی قابلیت اطمینان برای طراحی شبکه ارتباطی شبکه هوشمند برق است. ایده این مقاله برای کاهش پیچیدگی، تقسیم مسئله به دوقسمت و حل تکرارشونده آن است به‌طوری که در قسمت اول با استفاده از یک مسئله مبتنی بر برنامه‌ریزی خطی، یک شبکه از روترها برای پوشش کل گره‌های شبکه هوشمند برق ساخته شده و در قسمت دوم با حل تکرارشونده مسئله دوم، روترهای افزونه به شبکه ارتباطی اضافه شود. 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 زمان قابل قبول قابلیت اطمینان شبکه را به مقدار مورد نظر برساند.

کلمات کلیدی شبکه برق هوشمند، طراحی شبکه، جایگذاری گره‌ها، قابلیت اطمینان، بهینه‌سازی، برنامه ریزی خطی

تاریخ ارسال مقاله: ۱۳۹۲/۲/۲۳
تاریخ پذیرش مشروط مقاله: ۱۳۹۳/۱۰/۶
تاریخ پذیرش مقاله: ۱۳۹۴/۱۰/۱
نام نویسنده‌ی مسئول: سیاوش خرسندی
نشانی نویسنده‌ی مسئول: ایران – تهران – خیابان حافظ – پلاک ۴۲۴ – دانشگاه صنعتی امیرکبیر – دانشکده‌ی مهندسی کامپیوتر و فناوری اطلاعات

۱- مقدمه

شبکه هوشمند برق یک زیر ساخت ارتباطی جامع برای انتقال همزمان انرژی الکتریکی و داده به صورت بلادرنگ و دو طرفه است. این شبکه از قرار گرفتن یک شبکه ارتباطی سریع و مطمئن در کنار شبکه برق حاضر به وجود می‌آید. گره‌های تولید کننده داده در این شبکه، کنتورهای هوشمند خانگی و سنسورهای سطح شبکه برق هستند که داده‌های خود را به صورت متناوب یا دوره‌ای به سمت کنترل‌کننده[۱] مرکزی می‌فرستند. مهم‌ترین گره‌های این شبکه کنتورهای خانگی هستند که می‌توان آن‌ها را دارای توزیع یکنواخت با چگالی بالا و فواصل نزدیک به هم در گستره شهر فرض کرد. ساختار شبکه برق به گونه‌ای است که تعدادی از این گره‌ها (که این تعداد بسته به نوع کاربرد – صنعتی یا خانگی- و همچنین تعداد کل گره‌های موجود در شهر متغیر است) توسط یک کنترل‌کننده مرکزی کنترل می‌شوند. یک شهر از چند کنترل‌کننده تشکیل شده که هر یک وظیفه مدیریت گره‌های محدوده خود را دارد. [۱]، [۲]

از دیدگاه پردازش داده، وظیفه این کنترل‌کننده این است که اطلاعات را از گره‌ها گرفته، پردازش‌های لازم را روی آن‌ها انجام داده و سپس نتایج را به آن‌ها باز گرداند. البته باید توجه کرد که ممکن است هر کنترل‌کننده برای پردازش‌های خود نیازمند ارتباط با دیگر کنترل کننده‌ها باشد.

از مهم‌ترین و به خصوص‌ترین ویژگی‌ها و نیازمندی‌های این شبکه قابلیت اطمینان آن است. به طوری که کاربردهای مختلف شبکه هوشمند برق نیازمند این هستند که شبکه ارتباطی شبکه بسیار مطمئنی باشد. به طور خلاصه با توجه به بلادرنگ بودن کاربردهای این شبکه و سروکار داشتن آن‌ها با مسائل ایمنی و اقتصادی، اکثر آن‌ها نیازمند قابلیت اطمینان بالغ بر ۹۸٪ هستند. [۳]

علاوه بر قابلیت اطمینان، یکی دیگر از مهم‌ترین ویژگی‌های این شبکه حساسیت شدید به تأخیر است. به عنوان مثال کاربردی مثل زیرساخت اندازه‌گیری پیشرفته[۲] حداکثر ۲ تا ۱۵ ثانیه تأخیر را می‌تواند تحمل کند. [۳]

پس با توجه به جریان داده در این شبکه و نیازمندی‌های مطرح شده، هدف ما طراحی شبکه‌ای است که اطلاعات را از گره‌های سطح شهر جمع کرده و آن‌ها را به دست کنترل‌کننده برساند. همچنین این شبکه باید ارتباط بین کنترل کننده‌ها را نیز برقرار کند. با توجه به نیازمندی‌های کیفی، این شبکه باید قابلیت اطمینان بالایی داشته باشد و بسته‌های ارسالی روی آن، تأخیر کمی را متحمل شوند. البته در این پروژه حل مسئله با در نظر گرفتن تأخیر مد نظر نیست و فقط راجع به طراحی شبکه با در نظر گرفتن قابلیت اطمینان بحث می‌شود.

برای حداکثر کردن قابلیت اطمینان یک شبکه در گذشته کارهای بسیاری انجام شده است. دسته ای از این کارها که نسبتاً قدیمی‌تر هم هستند سعی در پیدا کردن بهترین ترکیب یال‌ها در شبکه را داشته‌اند. از جمله این کارها می‌توان به [۸-۴] 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. از جمله دیگر اشکالات وارده پیچیدگی این روش‌هاست به طوری که برای شبکه های با تعداد گره های بسیار زیاد اصلاً تست نشده‌اند.

دسته‌ی دیگری از کارها هم وجود دارند که قابلیت اطمینان را در قالب مقاومت در برابر خطا[۳] بررسی می‌کنند که از جمله این کارها می‌توان به [۹] و [۱۰] اشاره کرد. این کارها برای بالا بردن قابلیت اطمینان سعی در ایجاد k مسیر جداگانه دارند. از آنجایی که ساختن این مسیرها پیچیدگی بسیار زیادی دارد، پس اعمال آن‌ها روی مسئله ما ممکن نیست.

دسته دیگر تحقیقات هم کارهایی هستند که روی شبکه های مش[۴] انجام شده‌اند. در این شبکه‌ها کارهای زیادی در حوزه جایگذاری گره‌ها[۵] انجام شده که اهداف بعضی از آن‌ها بی شباهت به اهداف قابل اطمینان کردن شبکه نیست. به عنوان مثال هدف [۱۱] جایگذاری گره‌ها برای بالا بردن گذردهی شبکه است. در این کار بیشترین جریان ممکن با حل یک مدل خطی بدست می‌آید. سپس برای رسیدن به جریان بهینه بدست آمده، دو ساختار از پیش تعریف شده گره‌ها 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 گره های فرا گستر[۶] و بالا بردن کیفیت TCP ، مسیریابی قابل اطمینان را انجام دهند. عیب این روش هم این است که سعی در بیشینه کردن قابلیت اطمینان دارد در حالی که ممکن است این مقدار بیشینه کمتر از مقدار مورد نظر ما باشد.

یکی از کامل‌ترین کارها برای محاسبه قابلیت اطمینان و بهبود آن در شبکه مش، [۱۳] است. در این مقاله نویسندگان با اضافه کردن یک به یک گره‌های افزونه به توپولوژی اولیه داده شده، مقدار قابلیت اطمینان آن 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

نگارندگان این مقاله، مکان‌های فرضی مشخصی برای اضافه کردن گره‌های افزونه دارند، جواب بدست آمده نهایی الزاماً جواب بهینه از دیدگاه کمینه کردن تعداد گره‌های افزونه نیست به طوری که آن‌ها هم در قسمت کارهای آینده مقاله خود، به این نکته اشاره دارند که باید مکان و تعداد بهینه این گره‌های افزونه در شبکه محاسبه شود.

در حوزه شبکه های هوشمند برق هم کارهایی در زمینه قابلیت اطمینان انجام شده است که از جمله آن‌ها می‌توان به [۱۴-۱۶] اشاره کرد. با مطالعه دقیق این کارها می‌توان دید که قابلیت اطمینان در این حوزه فعلاً در حد تعریف باقی مانده است.

بنابراین می‌توان نتیجه گرفت که خلأ بزرگی در زمینه طراحی یک شبکه کم هزینه و قابل اطمینان برای شبکه وسیع برق شهری وجود دارد که هدف ما در این مقاله طراحی چنین شبکه‌ای است. برای طراحی چنین شبکه‌ای ما دو مدل بهینه‌سازی پیشنهاد دادیم. مدل اول کمترین تعداد روتر را در شبکه پخش می‌کند به طوری که کل گره‌های شبکه هوشمند برق پوشش داده شوند. مدل دوم نیز به ساختار اولیه بدست آمده روتر اضافه می‌کند تا شبکه به قابلیت اطمینان مورد نظر برسد.

ادامه مقاله نیز حاوی بخش‌های زیر است. در بخش ۲ مدل شبکه و روش‌های محاسبه قابلیت اطمینان به طور دقیق بیان می‌شود. در بخش ۳، مدل‌های پیشنهادی برای ساخت توپولوژی اولیه و قابل اطمینان کردن آن ارائه خواهد شد. بخش ۴، شبیه‌سازی‌های انجام شده و نتایج آن‌ها بررسی خواهد شد. در بخش ۵ نیز نتایج پژوهش بیان می‌شود.

۲- مدل سیستم

۲-۱- مدل شبکه

همان‌طور که گفته شد هدف این پژوهش، طراحی یک شبکه مطمئن برای شبکه هوشمند برق است. ورودی مسئله، مکان گره های شبکه برق از جمله کنتورهای خانگی، سنسورهای شبکه برق و ... هستند. برای مدل کردن این ورودی‌ها از یک مجموعه به شکل $N = \{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$ استفاده می‌شود که n تعداد گره‌ها و (x_i, y_i) مختصات گره i را نشان می دهد.

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 مجموعه $R = \{(x_1, y_1), (x_2, y_2), \dots, (x_m, y_m)\}$ 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 شبکه با k ترمینال، Geir Egeland و Paal E. Engelstad در [۱۳] فرمولی ارائه کرده‌اند که این فرمول به شکل زیر است:

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

در این فرمول $R^{n_1,\dots,n_k}(G,p)$ نشان‌دهنده مقدار قابلیت اطمینان برای k گره از گراف G است. p نیز احتمال خرابی هر لینک را نشان می‌دهد. در طرف دوم تساوی، $T_i^{n_1,\dots,n_k}$ نشان-دهنده تعداد زیر گراف‌های همبند گراف G با k گره و i یال است. کران‌های سیگما نیز کمترین تعداد یال ممکن بای 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 گره و i یال است که در فرمول دقیق با نماد $T_i^{n_1,\dots,n_k}$ نشان داده می‌شود. از آنجایی که فرمول مشخصی برای محاسبه این مقدار وجود ندارد با بزرگ شدن شبکه شمارش زیر گراف‌ها بسیار پر هزینه شده و از نظر زمانی ممکن است در شبکه های بزرگ عملاً یافتن آن غیر ممکن باشد. به همین دلیل نویسندگان در [۱۷] از یک فرمول برای محاسبه یک حد بالا برای قابلیت اطمینان استفاده می‌کنند که به شکل زیر است:

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

در رابطه (۲) m_i برابر است با $min(d_i, i-1)$، d_i نشان دهنده درجه گره i و q نشان دهنده احتمال خرابی یک لینک یا عدم موفقیت ارسال روی آن لینک است. در همین مقاله ثابت می‌شود که مقدار بدست آمده از این فرمول همیشه یک حد بالا برای مقدار قابلیت اطمینان بهینه است.

۳- تعریف مسئله

مسئله این پژوهش، طراحی شبکه ارتباطی شبکه هوشمند برق از طریق جایگذاری روترها در محیط است به‌طوری که شبکه حاصل، حداقل قابلیت اطمنیان موردنیاز را داشته باشد. چالش

مسئله، رسیدن به این هدف با جایگذاری حداقل تعداد روتر است. این مسئله در مدل ۱ فرموله شده است.

مدل (۱): مسئله طراحی شبکه مطمئن

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

$$subject\ to$$

1. $X_{n,r} \leq Z_r \qquad \forall n, \forall r$
2. $\sum_{r=1}^{R} X_{n,r} = 1 \qquad \forall n$
3. $\sqrt{(XN_n - XR_r)^2 + (YN_n - YR_r)^2} \leq a + (1 - X_{n,r}) * M \qquad \forall n, \forall r$
4. $Reliability\ (G,p) \geq \hat{R}$

این مسئله دارای متغیرها و پارامترهای زیر است :

۱) Z_r : متغیر باینری که در صورت انتخاب شدن روتر rام مقدار ۱ و در غیر این صورت مقدار صفر می‌گیرد.

۲) $X_{n,r}$: متغیر باینری که در صورت وصل شدن گره 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 کاشته شده در محیط که می توان فرمول دقیق آن را در روابط ۱ و ۲ دید.

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

تابع هدف این مسئله نشان می‌دهد که کمترین تعداد روتر باید در محیط قرار داده شود. محدودیت‌های این مسئله به شکل زیر است:

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 گره باید با یک روتر ارتباط برقرار کند.

۳) محدودیت سوم بیان می‌کند که اگر گرهی 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 گره‌های متصل شده به آن اعمال می‌شود. همچنین طی این محدودیت مکان روترها نیز تعیین می‌شود.

۴) محدودیت چهارم نیز تضمین می‌کند که قابلیت اطمینان شبکه روترها حداقل به اندازه قابلیت اطمینان مورد نظر 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 شبکه هوشمند برق 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 برنامه ریزی خطی استفاده کرد و در نتیجه حل مسئله برای اندازه های واقعی غیر ممکن خواهد بود.

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

۱) تولید توپولوژی اولیه‌ای از روترها به‌طوری که تمام گره‌های شهری تحت پوشش قرار گیرند.

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

در ادامه این دو بخش توضیح داده خواد 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. $X_{n,r} \leq Z_r \qquad \forall n, \forall r$
2. $\sum_{r=1}^{R} X_{n,r} = 1 \qquad \forall n$
3. $|XN_n - XR_r| \leq a + (1 - X_{n,r}) * M \qquad \forall n, \forall r$
4. $|YN_n - YR_r| \leq a + (1 - X_{n,r}) * M \qquad \forall n, \forall r$

5. $XR_r \le Z_r * M$ $\forall r$
6. $YR_r \le Z_r * M$ $\forall r$

متغیرها و پارامترهای استفاده شده در این مدل مانند مدل ۱ است. تابع هدف این مدل تضمین می‌کند که کمترین تعداد روتر برای پوشش محیط 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 گره باید با یک روتر ارتباط برقرار کند.

۳) محدودیت‌های سوم و چهارم بیان می‌کنند که اگر گرهی 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 جایگذین شده است.

۴) محدودیت پنجم و ششم تضمین می‌کند که تنها در شرایطی مختصات یک روتر تعیین شود که آن روتر وجود داشته 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.

۲-۴- 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 نشان-دهنده 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 مقاله حاضر 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. $X_{n,r} \le Z_r$ $\forall n, \forall r$
2. $\sum_{r=1}^{R} Z_r = 1$ $\forall n$
3. $|XS_n - XR_r| \le a + (1 - X_{n,r}) * M$ $\forall n, \forall r$
4. $|YS_n - YR_r| \le a + (1 - X_{n,r}) * M$ $\forall n, \forall r$
5. $XR_r \le Z_r * M$ $\forall r$
6. $YR_r \le Z_r * M$ $\forall r$
7. $Degree_n + \sum_{r=1}^{R} X_{(n,r)} \ge \beta * temp_n$ $\forall n$
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 گره 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 نیز، پارامترهای زیر به عنوان ورودی به این مدل داده می‌شود:

۱) $Degree_n$: پارامتر حقیقی نشان‌دهنده درجه هر گره.

۲) β : نشان‌دهنده درجه‌ای که گره‌های 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 گره با درجه کمینه پوشش داده شود.

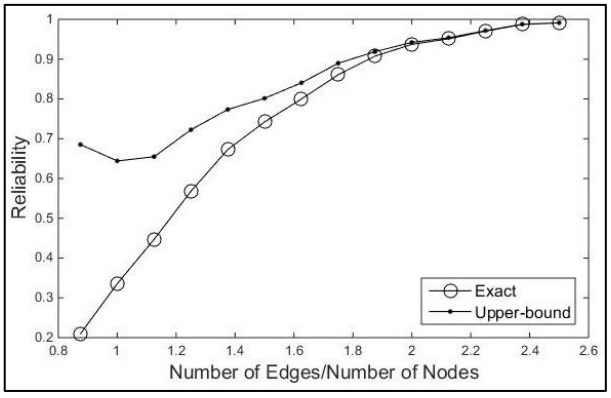
محدودیت‌های مدل عبارتند از:

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 مقدار مورد انتظار قابلیت اطمینان 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 گره‌هایی با $temp_n$ یک اضافه شده و درجه آن‌ها حداقل برابر با β شود. چون یکی از



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

این گره‌ها، گرهی با حداقل درجه است، قطعا روتر افزونه به جایی اضافه خواهد شد که در همسایگی این گره 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.

۵- ارزیابی

در این قسمت مطالب مطرح شده در قسمت‌های قبل با استفاده از شبیه‌سازی عددی ارزیابی خواهد شد. بخش اول مربوط به مقایسه رابطه ۱ و ۲ و اعتبارسنجی رابطه ۲ برای محاسبه قابلیت اطمینان است. بخش دوم ایده پیشنهادی برای افزایش قابلیت اطمینان در مدل ۳ 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 گره‌ها 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

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 گره های افزونه به شبکه اضافه شده و قابلیت اطمینان با استفاده از رابطه ۲ محاسبه شده است. نتایج حاصل از شبیه-سازی 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 گره، ممکن است به گراف شبکه اضافه شود. هر کدام از منحنی‌ها نیز مربوط به افزودن تعداد مشخصی گره به شبکه اولیه است. به

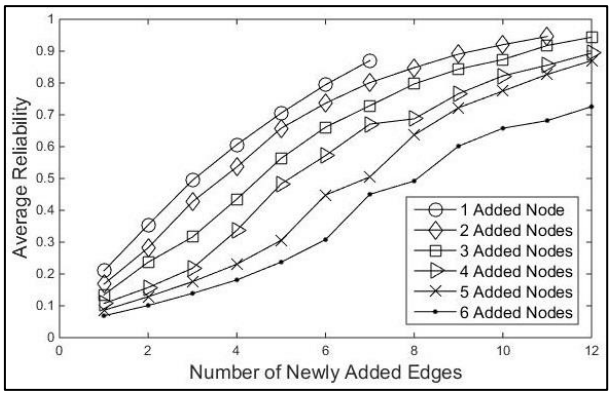
عنوان مثال منحنی اول (دایره) مربوط به افزودن یک گره است که قابلیت اضافه کردن یک تا هفت یال جدید به شبکه را دارد. این نمودارها حاصل میانگین گیری از ۱۰۰۰ نمونه تصادفی هستند.

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 گره‌ها، قابلیت اطمینان کاهش می‌یابد که این نتیجه با توجه به کاهش تعداد زیر گراف‌ها منطقی است. پس می‌توان از شکل ۲ می‌توان نتیجه گرفت که اگر مکان گره افزونه به نحوی انتخاب شود که بیشترین یال را در شبکه ایجاد کند، می‌توان قابلیت اطمینان را افزایش داد.

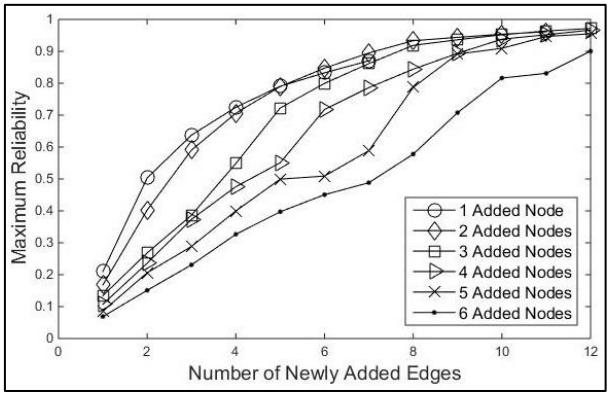
نمودارهای شکل ۴، برخلاف شکل ۳، حاصل ماکزیمم‌گیری از ۱۰۰۰ نمونه تصادفی هستند. با توجه به اختلافی که بین مقادیر میانگین در شکل ۳ و مقادیر بیشینه در شکل ۴ وجود دارد، واضح است که علاوه بر ایجاد افزونگی در یال‌های گراف شبکه، عوامل دیگری در افزایش قابلیت اطمینان شبکه تأثیرگذار هستند. مطالعات انجام شده بر روی نمونه‌های بیشینه نشان می‌دهد که اگر اضافه کردن گره افزونه و ایجاد یال‌های افزونه در شبکه منجر به افزایش درجه گره‌های 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 گره و دو یال به شبکه است. در شکل ۴-الف دو یال افزونه با گره‌هایی 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 گره‌هایی با درجه ۲ اضافه و قابلیت اطمینان گراف حاصل برابر با ۰,۳۷ شده است. پس می‌توان مشاهده کرد که افزایش درجه گره‌های کم‌درجه، تأثیر قابل توجهی روی قابلیت اطمینان دارد.

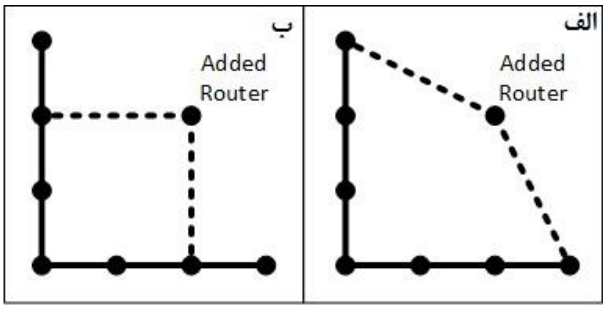
همانطور که اشاره شد، افزایش تعداد یال‌های گراف شبکه و درجه گره‌های کم‌درجه، عوامل تأثیرگذار در افزایش قابلیت اطمینان هستند. قابل پیش‌بینی است که افزایش همزمان این دو عامل می‌تواند تأثیر بیشتری نسبت به افزایش تک‌تک آن‌ها داشته باشد.



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



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



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

نتیجه ۵ نتایج حاصل از افزایش یال‌ها، افزایش درجه گره‌های 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 گره‌هایی که درجه بالایی دارند در هر مرحله به درجه آن‌ها اضافه می‌شود، در حالی که گره‌های دیگر همواره درجه

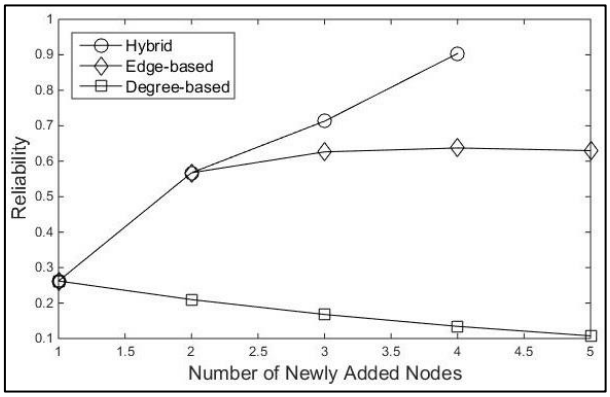
پایینی دارند. این امر باعث توقف رشد قابلیت اطمینان در شبکه می‌شود. نمودار دوم (مربعی) نتیجه حاصل از افزایش درجه گره‌های کم‌درجه را نشان می‌دهد. در بدترین حالت، این رویکرد یک گره برگ افزونه به گراف شبکه اضافه کرده و تعداد یال‌های شبکه را تنها یک واحد افزایش می‌دهد. نمونه‌ای از این حالت را می‌توان در شکل ۶ دید. در این شکل گره افزونه با هدف افزایش درجه گره کم‌درجه به شبکه اضافه شده اما خود به یک گره 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 گره‌های کم‌درجه دارد، عملکرد بهتری نیز نسبت به بقیه از خود نشان می‌دهد و بعد از اضافه کردن ۳ گره 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.

۳-۵- مثالی از طراحی شبکه مطمئن

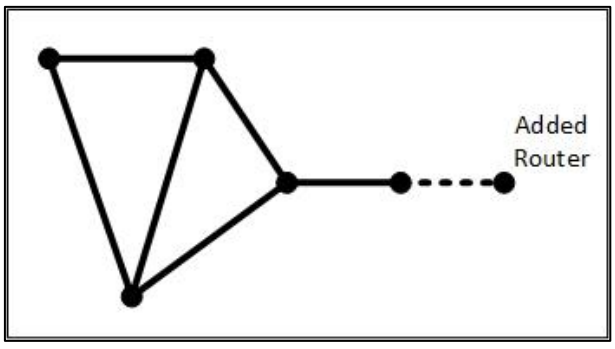
در بخش نمونه‌ای از طراحی شبکه ارتباطی مطمئن ارائه شده است. برای این کار به صورت تصادفی ۱۰۰ گره شهری را در محیط پخش می‌کنیم. شکل ۷-الف این گره‌ها را نشان می‌دهد. در مرحله اول مدل ۱ اجرا شده و شبکه‌ای از روترها برای پوشش گره‌ها ایجاد می‌شود. این شبکه در شکل ۷-ب قابل مشاهده است. با فرض این که احتمال ارسال 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.

۴-۵- ارزیابی روش ارائه شده

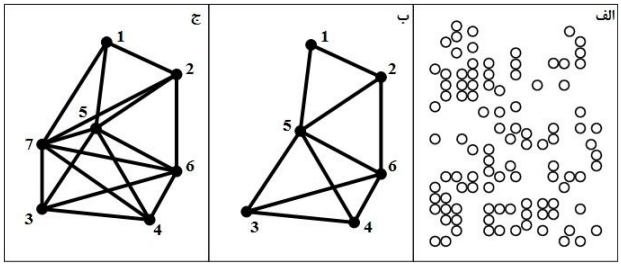
پس از صحت‌سنجی روش پیشنهادی و ارائه مثالی از چگونگی اجرای آن، در این بخش به بررسی و ارزیابی نتایج راه‌حل پیشنهادی می‌پردازیم. شکل ۸ تأثیر اندازه شبکه هوشمند برق و قابلیت اطمینان تک لینک (p) روی تعداد روترهای شبکه ارتباطی را بررسی می‌کند. با فرض این‌که قابلیت اطمینان موردنیاز شبکه ۰,۹۹ باشد، می‌توان مشاهده 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.



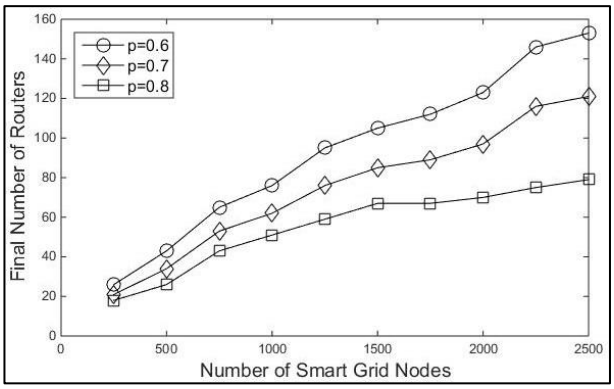
شکل (۵): مقایسه سه روش مکاشفه ای ارائه شده



شکل (۶): بدترین حالت افزودن گره به شبکه با هدف افزایش درجه گره‌های کم درجه



شکل (۷): الف) گره های اولیه توزیع شده ب)روترهای کاشته شده توسط مدل اول ج) روترهای افزونه اضافه شده برای افزایش قابلیت اطمینان



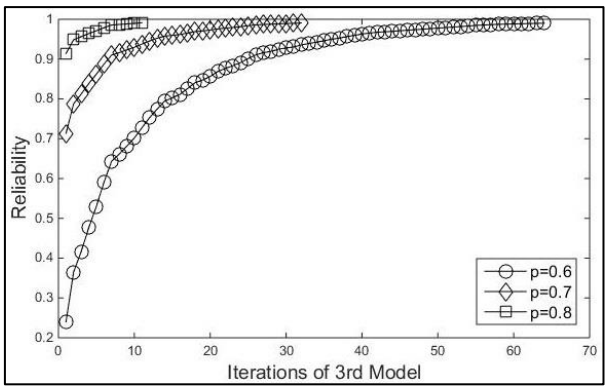
شکل (۸): تأثیر اندازه شبکه هوشمند برق و قابلیت اطمینان لینک‌ها در تعداد نهایی روترهای شبکه ارتباطی

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 هوشمند برق ۲۵۰۰ گره 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 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).

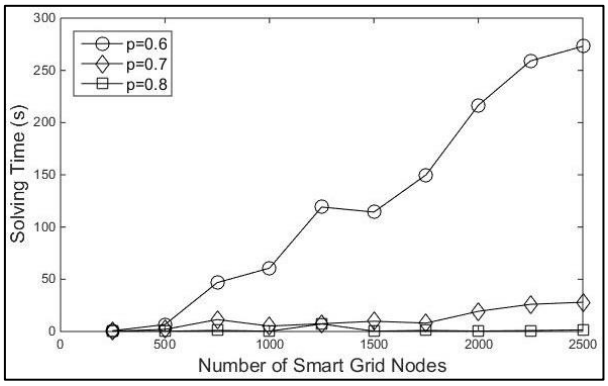
حال که تعداد دفعات اجرای روش پیشنهادی بررسی شد می‌توان پیش‌بینی کرد که زمان اجرا رابطه عکس با قابلیت اطمینان لینک‌ها (p) داشته باشد به طوری که با افزایش p زمان لازم برای طراحی شبکه مطمئن کاهش یافته و با کاهش p این زمان افزایش خواهد یافت. این نتیجه‌گیری توسط شکل ۱۰ تایید می‌شود. البته توجه شود که زمان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



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

۷- منابع

[1] B. Zaker and M. Mohammadi, "Probabilistic Optimal Operation of a Smart Grid Including Wind Power Generator Units," Journal of Iranian Association of Electrical and Electronics Engineers, vol. 3, no. 12, 19-Nov-2012.

[2] S. Jadid, O. Homaee, and A. Zakariazadeh, "Voltage Control Approach in Smart Distribution Network with Renewable Distributed Generation," Journal of Iranian Association of Electrical and Electronics Engineers, vol. 10, no. 2, 19-May-2013.

[3] "NBP RFI: Communications Requirements - Reply Comments of Utilities Telecom Council." [Online]. Available: http://energy.gov/gc/downloads/nbp-rfi-

communications-requirements-reply-comments-utilities-telecom-council. [Accessed: 12-May-2013].

[4] D. L. Deeter and A. E. Smith, "Heuristic optimization of network design considering all-terminal reliability," in Reliability and Maintainability Symposium. 1997 Proceedings, Annual, 1997, pp. 194–199.

[5] L. Lin and M. Gen, "A Self-controlled Genetic Algorithm for Reliable Communication Network Design," in IEEE Congress on Evolutionary Computation, 2006. CEC 2006, 2006, pp. 640–647.

[6] H. M. F. AboElFotoh and L. S. Al-Sumait, "A neural approach to topological optimization of communication networks, with reliability constraints," IEEE Transactions on Reliability, vol. 50, no. 4, pp. 397–408, 2001.

[7] S. Kharbash and W. Wang, "All-Terminal Network Reliability Optimization in Fading Environment via Cross Entropy Method," in 2010 IEEE International Conference on Communications (ICC), 2010, pp. 1–5.

[8] F.-M. Shao, X. Shen, and P.-H. Ho, "Reliability optimization of distributed access networks with constrained total cost," IEEE Transactions on Reliability, vol. 54, no. 3, pp. 421–430, 2005.

[9] E. Szlachcic, "Fault Tolerant Topological Design for Computer Networks," in International Conference on Dependability of Computer Systems, 2006. DepCos-RELCOMEX '06, 2006, pp. 150–159.

[10] D. Zili, Y. Nenghai, and L. Zheng, "Designing Fault Tolerant Networks Topologies Based on Greedy Algorithm," in Third International Conference on Dependability of Computer Systems, 2008. DepCos-RELCOMEX '08, 2008, pp. 227–234.

[11] F. Li, Y. Wang, and M. Li, "Gateway Placement for Throughput Optimization in Wireless Mesh Networks," in IEEE International Conference on Communications, 2007. ICC '07, 2007, pp. 4955–4960.

[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, 2007. ICDCS '07, 2007, p. 53-53.

[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.

[14] D. Niyato, P. Wang, and E. Hossain, "Reliability analysis and redundancy design of smart grid wireless communications system for demand side management," IEEE Wireless Communications, vol. 19, no. 3, pp. 38–46, 2012.

[15] R. Zhang, Z. Zhao, and X. Chen, "An overall reliability and security assessment architecture for electric power communication network in Smart Grid," in 2010 International Conference on Power System Technology (POWERCON), 2010, pp. 1–6.

[16] H. Li and A. D. Dimitrovski, "Reliability engineering for wireless communications in special protection schemes of smart grid," in 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), 2012, pp. 240–245.

[17] R.-H. Jan, "Design of reliable networks," in , IEEE International Conference on Communications, 1992. ICC '92, Conference record, SUPERCOMM/ICC '92, Discovering a New World of Communications, 1992, pp. 191-196 vol.1.

[1] Substation
[2] Advanced Metering Infrastructure
[3] Fault Tolerant
[4] Mesh
[5] Node Placement
[6] Overlay