ارزیابی تاثیرگذاری عدم قطعیت لینک‌های مخابراتی بر قابلیت اطمینان طرح‌های حفاظت تطبیقی

سیدامیر حسینی[۱]، حسین عسکریان ابیانه[۱]، سیدحسین حسام‌الدین صادقی[۱] و فرزاد رضوی[۲]

۱- دانشکده مهندسی برق- دانشگاه صنعتی امیرکبیر- تهران- ایران
-hosseini.amir@aut.ac.ir - askarian@aut.ac.ir- sadeghi@aut.ac.ir
۲- دانشکده مهندسی برق- دانشگاه آزاد اسلامی واحد قزوین - قزوین- ایران
farzad.razavi@qiau.ac.ir -

چکیده: **هماهنگی حفاظتی تطبیقی که با استفاده از لینک‌های گسترده مخابراتی تحقق می‌یابد یک راه حل مناسب برای حل مشکلات هماهنگی حفاظتی در میکروگریدها است. مسئله‌ای که عملکرد صحیح این روش را می‌تواند تحت تاثیر قرار دهد عدم قطعیت در عملکرد صحیح لینک‌های مخابراتی است. به منظور بررسی میزان تاثیرپذیری عدم قطعیت لینک‌های مخابراتی بر عملکرد صحیح حفاظت تطبیقی و نیز قابلیت اطمینان میکروگریدها، در این مقاله یک الگوریتم جدید زنجیره مارکوف مبتنی بر مونت‌کارلو[۱] پیشنهاد شده است. در الگوریتم ارائه شده احتمال خرابی لینک‌های مخابراتی و سیستم‌های حفاظت ثابت درنظر گرفته نمی‌شوند بلکه به ترتیب متناسب با تاخیر زمانی لینک‌های مخابراتی و جریان خطای عبوری از بریکرها، متغیر خواهند بود. روش پیشنهادی در این مقاله بر روی میکروگرید نمونه که مجهز به حفاظت تطبیقی مرکزی و لینک‌های گسترده مخابراتی است، تست می‌شود. به منظور ارزیابی تاثیر عدم قطعیت لینک‌های مخابراتی بر قابلیت اطمینان میکروگرید از شاخص‌های متوسط مدت زمان خاموشی[۲]، میانگین انرژی تزریق نشده[۳] و هزینه قطعی مورد انتظار[۴] استفاده می‌شود. نتایج شبیه‌سازی نشان می‌دهند که طرح‌های سنتی هماهنگی حفاظتی نسبت به طرح‌هایی که از تصمیم‌گیری‌های کلی[۵] بهره می‌برند، تاثیرپذیری بیشتری از عدم قطعیت لینک-های مخابراتی دارند.**

واژه های کلیدی: **حفاظت تطبیقی- عدم قطعیت- لینک‌های مخابراتی- قابلیت اطمینان- زنجیره مارکوف مبتنی بر مونت‌کارلو**

تاریخ ارسال مقاله: ۱۳۹۵/۰۳/۲۵

تاریخ پذیرش مقاله : ۱۳۹۵/۰۵/۲۵

نام نویسنده‌ی مسئول : حسین عسکریان ابیانه

نشانی نویسنده‌ی مسئول : دانشکده مهندسی برق- دانشگاه صنعتی امیرکبیر- تهران- ایران

[1] Markov Chain Monte Carlo (MCMC)
[2] System Average Interruption Duration (SAIDI)
[3] Expected Energy Not Supplied (EENS)
[4] Expected COST of Interruption (ECOST)
[5] Global decisions

۱- مقدمه

حفاظت تطبیقی یک راه‌کار موثر برای ایجاد هماهنگی حفاظتی در میکروگریدها به منظور پاسخ‌گویی به تغییرات دینامیک توپولوژی آن‌ها است [۱]. با استفاده از حفاظت تطبیقی هر تغییر در توپولوژی میکروگرید شناسایی شده و تنظیمات هماهنگی حفاظتی مناسب برای آن تعیین می‌شود [۲].

پاسخ‌گویی به تغییرات دینامیک توپولوژی میکروگرید بدون استفاده از ارتباطات گسترده مخابراتی غیرممکن است [۳]. در واقع لینک‌های مخابراتی سرعت بالا، حفاظت تطبیقی را قادر به عملکرد بصورت آنلاین با انتخاب‌گری بالا می‌نمایند [۴]. براین‌اساس با استفاده از لینک‌های گسترده مخابراتی در مطالعات [۵-۷] به هنگام وقوع خطا، داده‌ها بین سیستم‌های حفاظتی به اشتراک گذاشته می‌شوند و بهترین هماهنگی حفاظتی براساس داده‌های به اشتراک گذاشته شده و براساس تصمیم‌گیری کلی، ایجاد می‌شود. مطالعه [۸] از ارتباطات مخابراتی میان کلید موجود در نقطه اتصال مشترک میکروگرید با شبکه بالادست[1] و هریک از رله‌های حفاظتی برای اعلام وقوع تغییر در مد بهره‌برداری از میکروگرید (اتصال به شبکه/جزیره‌ای) به رله‌های حفاظتی استفاده می‌کند. در [۹, ۱۰] با وقوع هر تغییر در توپولوژی میکروگرید، سرور مرکزی اقدام به محاسبه مجدد تنظیمات هماهنگی حفاظتی هریک از رله‌ها نموده و این تنظیمات را از طریق لینک‌های مخابراتی به آن‌ها ابلاغ می‌کند. به منظور ایجاد هماهنگی حفاظتی، مطالعه [۱۱] میکروگرید را به چند زون تقسیم می‌نماید که در آن زون‌ها اطلاعات خود را با استفاده از لینک‌های مخابراتی به اشتراک می‌گذارند.

آنچه که مشخص است این است که لینک‌های مخابراتی نمی‌توانند همواره بدون مشکل و با قابلیت اطمینان ۱۰۰ درصد فعال باشند [۱۲]. این در حالی است که مطالعات نشان می‌دهند شرایط غیرعادی حتی با درجه کم می‌تواند تاثیر زیادی بر عملکرد صحیح لینک‌های ارتباطی داشته باشند [۱۳]. وابستگی طرح‌های حفاظت تطبیقی به لینک‌های مخابراتی، قابلیت اطمینان این طرح‌ها را تحت تاثیر قرار می‌دهد. این مسئله بدلیل وجود عدم قطعیت‌های موجود در این لینک‌ها است [۱۴]. بطوریکه کاربرد مطمئن یک سیستم حفاظت تطبیقی مبتنی بر ارتباطات مخابراتی با سرعت، تاخیر و قابلیت اطمینان سیستم مخابرات آن تحت تاثیر قرار می‌گیرد [۱۵].

با توجه به وابستگی شدید طرح‌های حفاظت تطبیقی به لینک‌های مخابراتی، در این مقاله میزان تاثیرپذیری عدم قطعیت این لینک‌ها بر عملکرد صحیح حفاظت تطبیقی و نیز قابلیت اطمینان میکروگریدها مورد بررسی قرار گرفته است. بدین منظور در این مقاله استفاده از زنجیره مارکوف مبتنی بر مونت‌کارلو پیشنهاد شده است. در بررسی انجام شده در این مقاله احتمال خرابی لینک‌های مخابراتی و سیستم‌های حفاظت ثابت درنظر گرفته نشده است، بلکه به ترتیب متناسب با تاخیر زمانی لینک‌های مخابراتی و جریان خطای عبوری از بریکرها، متفاوت خواهند بود. متفاوت درنظر گرفتن احتمال عملکرد صحیح لینک‌های مخابراتی موجب می‌شود استراتژی‌های مختلف هماهنگی حفاظتی که از مسیرهای متفاوت مخابراتی برای ابلاغ فرامین سرور مرکزی به بریکرها استفاده می‌کنند، دارای احتمال عملکرد صحیح متفاوت و در نتیجه تاثیرات متفاوت بر قابلیت اطمینان میکروگرید باشند. به منظور ارزیابی تاثیر عدم قطعیت لینک‌های مخابراتی بر قابلیت اطمینان میکروگرید از شاخص‌های SAIDI، EENS و ECOST استفاده می‌شود. در این راستا یکی از مهمترین ابزارهای ارزیابی شاخص‌های قابلیت اطمینان که شبیه‌سازی مونت کارلو است و برای سیستم‌های بزرگ مناسب می‌باشد، استفاده شده است. نتایج پیاده‌سازی روش پیشنهادی بر روی میکروگرید نمونه که مجهز به سرور مرکزی است، نشان می‌دهد که استفاده از تصمیم‌گیری‌های محلی و سنتی نمی‌تواند قابلیت اطمینان لازم را برای حفاظت موثر میکروگریدها تضمین نماید.

بخش‌های دیگر این مقاله بدین شرح است. در بخش دوم به بررسی مشکلات پیش آمده در اثر نادیده گرفتن عدم قطعیت لینک‌های مخابراتی پرداخته می‌شود. در بخش سوم، روش جدید ارائه شده در این مقاله برای ارزیابی اثرات عدم قطعیت لینک‌های مخابراتی بر طرح‌های حفاظت تطبیقی میکروگرید و قابلیت اطمینان آن، ارائه شده است. در بخش چهارم الگوریتم پیاده‌سازی روش پیشنهادی و میکروگرید نمونه معرفی می‌شوند. بخش پنجم نیز به تحلیل نتایج حاصل از پیاده‌سازی روش پیشنهادی بر روی میکروگرید نمونه، پرداخته است.

۲- شرح مشکل

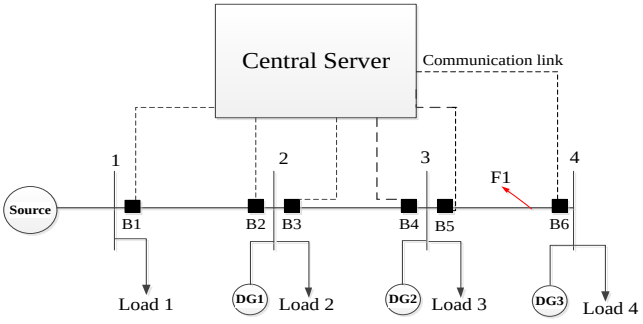
حفاظت تطبیقی یک روش قدرتمند در پاسخ‌گویی به عدم قطعیت‌های موجود در میکروگرید می‌باشد [۱]. این مسئله زمانی درست است که عدم قطعیت‌های تاثیرگذار بر حفاظت تطبیقی شناسایی شده و برنامه‌ریزی‌های لازم برای مواجه با آن‌ها ایجاد شود. چراکه بدون درنظر گرفتن این عدم قطعیت‌ها، حفاظت تطبیقی نمی‌تواند قابلیت اطمینان لازم را برای حفاظت از میکروگریدها ایجاد نماید [۱۲].

یکی از مهمترین عدم قطعیت‌هایی که عملکرد صحیح حفاظت تطبیقی را تحت تاثیر قرار می‌دهد، عدم قطعیت در عملکرد صحیح لینک‌های مخابراتی است. مطالعات نشان می‌دهند شرایط غیرعادی حتی با درجه کم می‌تواند تاثیر زیادی بر عملکرد لینک‌های ارتباطی داشته باشند. درواقع شرایط غیرعادی دارای دو تاثیر بر لینک‌های ارتباطی می‌باشند. اول آنکه موجب ایجاد تاخیر زمانی در ارسال اطلاعات می‌شوند و دوم موجب قطع کلی لینک می‌گردند [۱۳]. با توجه به آنکه در مطالعات

[1] Point of common coupling (PCC)

گذشته در حوزه حفاظت تطبیقی، قابلیت اطمینان لینک‌های مخابراتی ۱۰۰ درصد در نظر گرفته شده است، لذا بروز شرایط غیرعادی می‌تواند قابلیت اطمینان طرح‌های حفاظت تطبیقی را تحت تاثیر قرار دهد. این مسئله توسط شبکه شکل (۱) که در آن سرور مرکزی وظیفه ایجاد هماهنگی حفاظتی بهینه را دارد، توضیح داده شده است. همانطور که از شکل (۱) مشخص است، سرور مرکزی از طریق لینک‌های گسترده مخابراتی با کلیه بریکرها در ارتباط است. بریکرها در دو سر کلیه خطوط قرار دارند و وظیفه پیاده‌سازی دستورات ابلاغ شده توسط سرور مرکزی را دارند.

در شکل (۱)، فرض می‌شود تمام منابع تولید پراکنده در شبکه حضور داشته باشند و خطایی در F1 رخ دهد. در این حالت بهینه‌ترین استراتژی هماهنگی حفاظتی آن است که بریکرهای ۵ و ۶ عمل نموده و خطا را پاک کنند. به همین دلیل از طریق لینک‌های مخابراتی مرتبط، دستور قطع از سرور مرکزی به این دو بریکر ارسال می‌شود. اگر لینک مخابراتی ۵ به دلیل تاخیر زمانی زیاد یا قطع شدن کلی لینک نتواند پیغام قطع را به بریکر ۵ در زمان معین ارسال نماید، انتظار آن است که با ارسال فرمان از سرور مرکزی به بریکر ۳ (استراتژی جایگزین)، این بریکر بعنوان پشتیبان خطا را پاک نماید. با توجه به آنکه افزایش زمان عبور جریان خطا موجب افزایش احتمال بروز عیب در بریکرها می‌شود (بر طبق نتایج بررسی مطالعه [۱۶])، لذا در فاصله انتظار برای ارسال پیغام به بریکر شماره ۵ و قطع خطا توسط آن و سپس ارسال پیغام قطع به بریکر ۳، ممکن است این بریکر دچار خرابی شود و نتواند خطا را بعنوان پشتیبان قطع نماید. انتظار برای قطع خطا توسط بریکر ۳ می‌تواند بر سایر بریکرها تاثیر گذاشته و حتی موجب خاموشی گسترده شود. بنابراین مشخص است که درنظر گرفتن عدم قطعیت‌های لینک‌های مخابراتی می‌تواند موجب جلوگیری از خاموشی‌های گسترده و در نتیجه افزایش قابلیت اطمینان طرح‌های حفاظت تطبیقی شود.



شکل (۱): شبکه نمونه با حفاظت تطبیقی مرکزی

۳- روش جدید

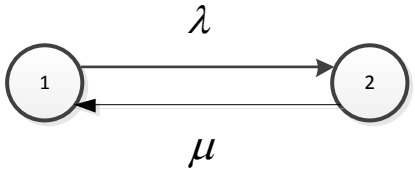
هدف از این مقاله بررسی میزان تاثیر عدم عملکرد صحیح لینک‌های مخابراتی بر قابلیت اطمینان طرح‌های حفاظت تطبیقی میکروگرید است. بدین منظور از شبیه‌سازی مونت‌کارلو برای ارزیابی شاخص‌های قابلیت اطمینان میکروگرید براساس اجزاء زنجیره مارکوف استفاده می‌شود. یک زنجیره مارکوف، پیکربندی سیستم را به تعدادی از حالات[1] می‌شکند که در آن هریک از حالات به حالت دیگر با استفاده از نرخ‌های انتقال[2] متصل است. پروسه از یک حالت شروع می‌شود و با توجه به نرخ‌های انتقال به حالت‌های دیگر منتقل می‌شود. در زنجیره مارکوف مبتنی بر مونت‌کارلو پیشنهاد شده، یک زنجیره مارکوف مرتبط با هریک از اجزاء تاثیرگذار بر عملکرد حفاظت تطبیقی میکروگرید بطور جداگانه ایجاد می‌شود. سپس با اعمال این مدل‌ها در پروسه راندوم مونت‌کارلو، رفتار دینامیک میکروگرید و لینک‌های مخابراتی با هدف ارزیابی شاخص‌های قابلیت اطمینان شبیه‌سازی می‌شود.

۳-۱- زنجیره مارکوف پیشنهاد شده

در حفاظت تطبیقی مرکزی مدنظر مقاله حاضر با فرض قابلیت اطمینان ۱۰۰ درصدی برای سرور مرکزی، عوامل تاثیرگذار بر عملکرد صحیح حفاظت تطبیقی شامل خطوط، لینک‌های مخابراتی و بریکرها می‌باشند. براین اساس در این مقاله سه زنجیره مارکوف مجزا برای نشان دادن حالات مختلف هریک از این المان‌ها پیشنهاد شده است.

۳-۱-۱- زنجیره مارکوف خطوط

همانطور که در شکل (۲) نشان داده شده است، زنجیره مارکوف مرتبط با خطوط دارای دو حالت در دسترس[3] (حالت ۱) و عدم دسترسی[4] (حالت ۲) می‌باشد [۱۶]. در این شکل، λ و μ به ترتیب نرخ خرابی[5] و نرخ تعمیرات[6] خطوط می‌باشند.



شکل (۲): زنجیره مارکوف خطوط

۳-۱-۲- زنجیره مارکوف بریکرها

شکل (۳) نشان دهنده زنجیره مارکوف مرتبط با بریکرها است. در این زنجیره سه حالت وجود دارد [۱۶].

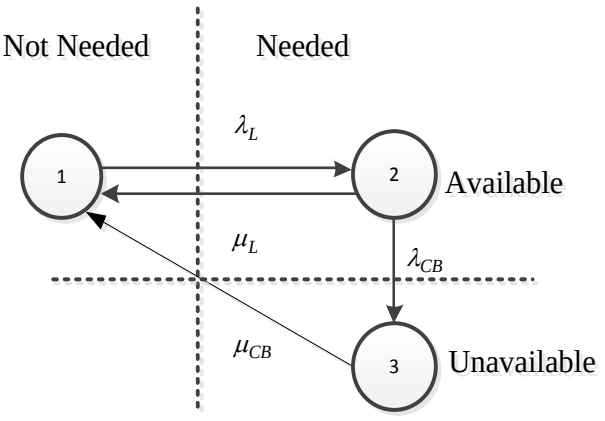
حالت ۱: در این حالت بریکر در دسترس است و نیاز به عملکرد آن نیست.

[1] States
[2] Transition rate
[3] Available
[4] Unavailable
[5] Failure rate
[6] Repair rate

حالت ۲: در این حالت بریکر در دسترس است و نیاز است که عمل کند. در واقع در این حالت خطایی در یک خط با نرخ خرابی λ_{Line} رخ داده است و بریکر مربوطه در استراتژی هماهنگی حفاظتی مدنظر سرور مرکزی برای پاک کردن خطای رخ داده، قرار دارد. بنابراین سرور مرکزی از طریق لینک‌های مخابراتی برای این بریکر دستور قطع را ارسال می‌نماید. بریکر با دریافت دستور قطع پس از زمان t_s اقدام به باز شدن و پاک کردن خطا می‌نماید. پس از پاک شدن خطا، خط خطا دیده با نرخ تعمیرات μ_{Line} به حالت اولیه باز می‌گردد.

با توجه به آنکه در این مقاله فرض می‌شود کلیه بریکرهای موجود در هر استراتژی هماهنگی حفاظتی در زمان یکسان اقدام به باز شدن و پاک کردن خطا نمایند، بنابراین t_s بعنوان زمان اعمال استراتژی s^{th} معرفی می‌شود که عبارت است از زمان رسیدن پیغام سرور مرکزی به دورترین بریکر موجود در استراتژی هماهنگی حفاظتی s^{th} ($t^s_{D\_Max}$).

حالت ۳: در این حالت، بریکری که در برنامه هماهنگی حفاظتی سرور مرکزی وجود دارد، در دسترس نیست. در این حالت سیگنال تریپ از طریق لینک‌های مخابراتی به درستی به بریکر مربوطه ابلاغ می‌شود اما به دلیل وجود خطای پنهان[1] در بریکر با نرخ λ_{CB}، این بریکر نمی‌تواند اقدام به قطع خطا نماید. در این حالت سرور مرکزی می‌بایست به بریکر دیگری بعنوان پشتیبان، فرمان قطع را ابلاغ نماید. بریکر معیوب شده با نرخ تعمیرات μ_{CB} به حالت ۱ باز می‌گردد.



شکل (۳): زنجیره مارکوف بریکرها

۳-۱-۳- زنجیره مارکوف لینک‌های مخابراتی

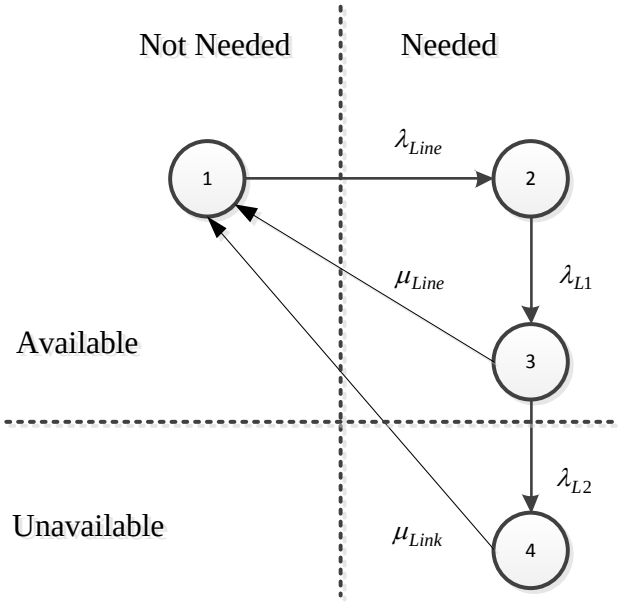
شکل (۴) زنجیره مارکوف پیشنهاد شده در این مقاله را برای مدلسازی لینک‌های مخابراتی نشان می‌دهد. همانطور که مشخص است این زنجیره از ۴ حالت تشکیل شده است.

حالت ۱: در این حالت لینک مخابراتی در دسترس است اما نیاز به استفاده از آن نیست. این مسئله به این دلیل است که بریکری که لینک مخابراتی مربوطه به آن متصل است در استراتژی هماهنگی حفاظتی مدنظر سرور مرکزی قرار ندارد.

حالت ۲: در این حالت بریکری که لینک مخابراتی مربوطه به آن متصل است در استراتژی هماهنگی حفاظتی مدنظر سرور مرکزی قرار دارد و لازم است از طریق این لینک مخابراتی، فرمان قطع به بریکر ابلاغ شود. در این حالت تاخیر زمانی لینک مخابراتی (t_D) دقیقا برابر با تاخیر زمانی استاندارد ($t_{D-Standard}$) آن است.

حالت ۳: در این حالت تاخیر زمانی لینک مخابراتی بیشتر از تاخیر زمانی استاندارد آن است اما این تاخیر کمتر از t_s است. بنابراین تاخیر زمانی لینک مخابراتی قابل قبول می‌باشد.

حالت ۴: در این حالت تاخیر زمانی لینک مخابراتی بیشتر از t_s است. بنابراین لینک مخابراتی در دسترس نمی‌باشد. در این حالت سرور مرکزی یا باید از لینک دیگری برای ارسال پیغام استفاده کند (در صورت وجود) و یا استراتژی هماهنگی حفاظتی را تغییر دهد. لینک معیوب شده با نرخ تعمیرات μ_{Link} به حالت اول باز می‌گردد.



شکل (۴): زنجیره مارکوف پیشنهادی برای لینک‌های مخابراتی

۳-۲- محاسبه احتمال خرابی بریکرها و لینک‌های مخابراتی

در مقاله حاضر برخلاف فرض‌های درنظر گرفته شده در مطالعات گذشته احتمال خرابی بریکرها و لینک‌های مخابراتی ثابت نیست بلکه به ترتیب با جریان خطای عبوری از بریکرها و تاخیر زمانی لینک‌های مخابراتی متغیر است [۱۶, ۱۷]. بنابراین در مقاله حاضر به جای درنظر

[1] Hidden failure

گرفتن یک مقدار ثابت برای λ_{CB} و λ_{L2} از روابطی که این پارامترها را با عوامل تغییر دهنده آن‌ها مدل می‌نماید، استفاده می‌شود.

۳-۲-۱- احتمال خرابی بریکرها

بریکر بطور مستقیم با جریان خطا درگیر بوده و بنابراین احتمال خرابی آن تابعی از شدت جریان خطا و مدت زمان عبور آن از بریکر است [۱۶, ۱۸]. بنابراین در این مقاله احتمال خرابی بریکرها از رابطه (۱) محاسبه خواهد شد [۱۶].

$$P_B(t_s)=\begin{cases}0 & ;if\ I_F^B(t)\le I_R^B\\ (I_F^B(t)-I_R^B).t_s & ;\ if\ I_M^U>I_F^B(t)>I_R^B\\ 1 & ;if\ I_F^B(t)\ge I_U^B\end{cases} \qquad (۱)$$

در این رابطه $P_B(t_s)$ تابع خرابی بریکر B^{th}، $I_F^B(t)$ جریان خطای عبوری از بریکر B^{th} و I_R^B جریان نامی این بریکر است. مطابق رابطه (۱)، اگر جریان خطای عبوری از بریکر B^{th} از I_R^B کمتر بود، آنگاه این بریکر بطور حتم عملکرد صحیح در انجام دستورات ابلاغ شده توسط سرور مرکزی خواهد داشت. همچنین اگر جریان خطای عبوری از این بریکر از I_U^B که حد آستانه خرابی بریکر است بالاتر بود، آنگاه بطور حتم این بریکر در اثر خطای بوقوع پیوسته معیوب خواهد شد. اگر جریان خطا بین I_R^B و I_U^B بود، آنگاه احتمال خرابی $0<P_B(t_s)<1$ است [۱۶].

۳-۲-۲- احتمال خرابی لینک‌های مخابراتی

منظور از احتمال خرابی لینک‌های مخابراتی آن است که دستورات صادر شده توسط سرور مرکزی در زمان مناسب به بریکرهای موجود در هر استراتژی هماهنگی، ارسال نشود. مطابق مطالعه [۱۷] احتمال خرابی لینک‌های مخابراتی متناسب با تاخیر زمانی آن‌ها است و تاخیر زمانی لینک‌های مخابراتی به نوع لینک و طول آن‌ها وابسته است [۱۹].

همانطور که عنوان شد در طرح پیشنهادی، بریکرهای موجود در هر استراتژی بطور همزمان اقدام به قطع خطا می‌نمایند. بنابراین در هر استراتژی برخی از لینک‌ها می‌توانند تاخیری بیشتر از مقدار تاخیر استاندارد تعریف شده که متناسب با طول لینک است و از رابطه (۲) محاسبه می‌شود را داشته باشند [۱۹].

$$t_{D-S\tan dard}=\tau\left(\frac{ms}{km}\right)\times d(km) \qquad (۲)$$

در این رابطه τ تاخیر انتشار است که به جنس لینک مخابراتی وابسته است و d طول لینک مخابراتی است.

زمان تاخیر اضافی برابر با زمانی است که دستور سرور مرکزی به بریکری که در دورترین مکان نسبت به سرور قرار دارد، برسد. بنابراین به کمک تابع چگالی احتمال ارائه شده در مطالعه [۱۷]، رابطه (۳) برای محاسبه احتمال عدم موفقیت لینک‌های مخابراتی در استراتژی هماهنگی حفاظتی s^{th} نوشته می‌شود. در این رابطه P_L شماره نقطه مرتبط با احتمال خرابی لینک L^{th} در جدول توزیع احتمال لینک-های مخابراتی و P_m^s شماره نقطه‌ی مرتبط با احتمال خرابی لینک مخابراتی است که دارای ماکزیمم تاخیر زمانی استاندارد در استراتژی ($t_{D\_Max}^s$) می‌باشد. همچنین در این رابطه L_s تعداد کل لینک‌های مخابراتی است که در استراتژی هماهنگی s^{th} مشارکت دارند.

$$P_L^s(t_D)=P_L^s(t_D^s>t_{D\_Max}^s)=1-\prod_{L=1}^{L_S}\Big(\sum_{i=p_L}^{P_m^s}P(i)\Big) \qquad (۳)$$

مطابق رابطه (۱) آنچه که علاوه بر دامنه جریان، موجب تغییر در احتمال خرابی بریکرها می‌شود، زمان اعمال استراتژی (t_s) است. براساس آنچه که بیان شد، زمان اعمال هر استراتژی، زمانی است که براساس ترتیب استراتژی‌های مدنظر سرور مرکزی، نوبت به اعمال یک استراتژی برای پاک کردن خطا می‌رسد. با توجه به آنکه ممکن است تا رسیدن نوبت به یک استراتژی، برخی از استراتژی‌های قبل از آن شکست خورده باشند، لذا لازم است زمان گذر از استراتژی‌های گذشته در تعیین زمان اعمال هر استراتژی مدنظر قرار گیرند. با توجه به آنچه که بیان شد، زمان گذر از هر استراتژی برابر با ماکزیمم تاخیر زمانی لینک‌های مخابراتی فعال در آن استراتژی است (t_{D-Max}). بنابراین مطابق رابطه (۴)، زمان اعمال استراتژی s^{th} برابر با مجموع ماکزیمم تاخیر زمانی لینک‌های مخابراتی استراتژی‌های قبلی، بعلاوه ماکزیمم تاخیر زمانی لینک‌های مخابراتی فعال در استراتژی s^{th} می‌باشد.

$$t_s=t_{D\_Max}^s+\sum_{j=1}^{s-1}t_{D\_Max}^j \qquad (۴)$$

۴- پیاده‌سازی روش پیشنهادی

۴-۱- الگوریتم پیشنهادی

با توجه به آنکه پارامترها و عدم قطعیت‌های مدنظر مقاله حاضر متغیر با زمان می‌باشند، لذا به منظور پیاده‌سازی روش پیشنهادی از شبیه-سازی مونت‌کارلوی ترتیبی[1] استفاده می‌شود. جزئیات استفاده از این روش در [۲۰] ارائه شده است. در مدت زمان شبیه‌سازی با توجه به احتمال وقوع خطا در خطوط مختلف شبکه، رفتار دینامیک سیستم حفاظت تطبیقی و لینک‌های مخابراتی و نیز شاخص‌های قابلیت اطمینان مدنظر، مورد ارزیابی قرار می‌گیرند. براین‌اساس فلوچارت پیاده‌سازی این روش در شکل (۵) نشان داده شده است. همانطور که مشخص است برای پیاده‌سازی روش پیشنهادی چهار زیربخش مدنظر قرار گرفته است.

زیربخش اول: در زیربخش اول تعمیر المان‌های معیوب مطابق با نرخ تعمیرات آن‌ها مدنظر است. برای اجرای این زیربخش سه گام درنظر گرفته شده است.

گام اول: در ابتدای هر ساعت از شبیه‌سازی چک می‌شود که خط، بریکر و یا لینک مخابراتی با توجه به نرخ‌های تعمیرات، تعمیر شده است یا خیر. همچنین چک می‌شود که توپولوژی میکروگرید تغییر کرده است یا خیر.

گام دوم: اگر المانی تعمیر شده بود و آن المان خط یا لینک مخابراتی بود، وضعیت آن‌ها از عدم امکان سرویس‌دهی به سرویس‌دهی تغییر می‌کند و اگر بریکر باشد، وضعیت آن از حالت باز به حالت بسته تغییر می‌کند.

گام سوم: اگر توپولوژی میکروگرید تغییر کرده بود، این تغییرات در شبکه اعمال می‌شود.

زیربخش دوم: در این بخش به تولید اعداد راندوم برای تعیین خطوط خطادار پرداخته می‌شود.

گام چهارم: در این گام با مقایسه اعداد راندوم تولید شده با نرخ خرابی خطوط اگر خطایی در خطی رخ داده باشد، الگوریتم به گام ۵ منتقل می‌شود. در غیراینصورت به گام ۴ منتقل می‌شود.

زیربخش سوم: شبیه‌سازی رفتار حفاظت تطبیقی

گام پنجم: محاسبه جریان اتصال‌کوتاه عبوری از هریک از خطوط.

گام ششم: جریان اتصال‌کوتاه عبوری از هریک از بریکرها در هریک از گام‌های زمانی شبیه‌سازی محاسبه می‌شود و با کمک رابطه (۱) احتمال خرابی هریک از بریکرها به ازای گام‌های زمانی مختلف تعیین می‌گردد.

گام هفتم: تولید استراتژی هماهنگی حفاظتی برای پاک کردن خطا.

گام هشتم: محاسبه احتمال خرابی لینک‌های مخابراتی موجود در استراتژی ایجاد شده در گام هفتم با استفاده از رابطه (۳).

گام نهم: اگر یکی از لینک‌های مخابراتی در زمان t_s موفق به تحویل پیغام سرور مرکزی به بریکر مربوطه نشد، وضعیت این لینک مخابراتی در حالت عدم دسترسی قرار گیرد. اگر لینک دیگری در این استراتژی برای ارسال پیغام سرور مرکزی وجود داشت، الگوریتم به گام دهم منتقل شود. در غیر اینصورت استراتژی شکست خورده است و الگوریتم باید به گام هفتم منتقل شود.

گام دهم: اگر هریک از بریکرهای استراتژی در اجرای فرمان سرور مرکزی ناتوان بود، وضعیت آن بریکر در حالت عدم دسترس قرار گیرد. در این حالت استراتژی شکست خورده است و الگوریتم باید به گام هفتم باز گردد. در غیر اینصورت الگوریتم به گام یازدهم منتقل می-شود.

گام یازدهم: موفقیت استراتژی در پاک کردن خطا. در این حالت بریکرهای معیوب، لینک‌های مخابراتی معیوب و خط معیوب برای تعمیرات باز می‌شوند.

زیربخش چهارم: محاسبه شاخص‌های قابلیت اطمینان

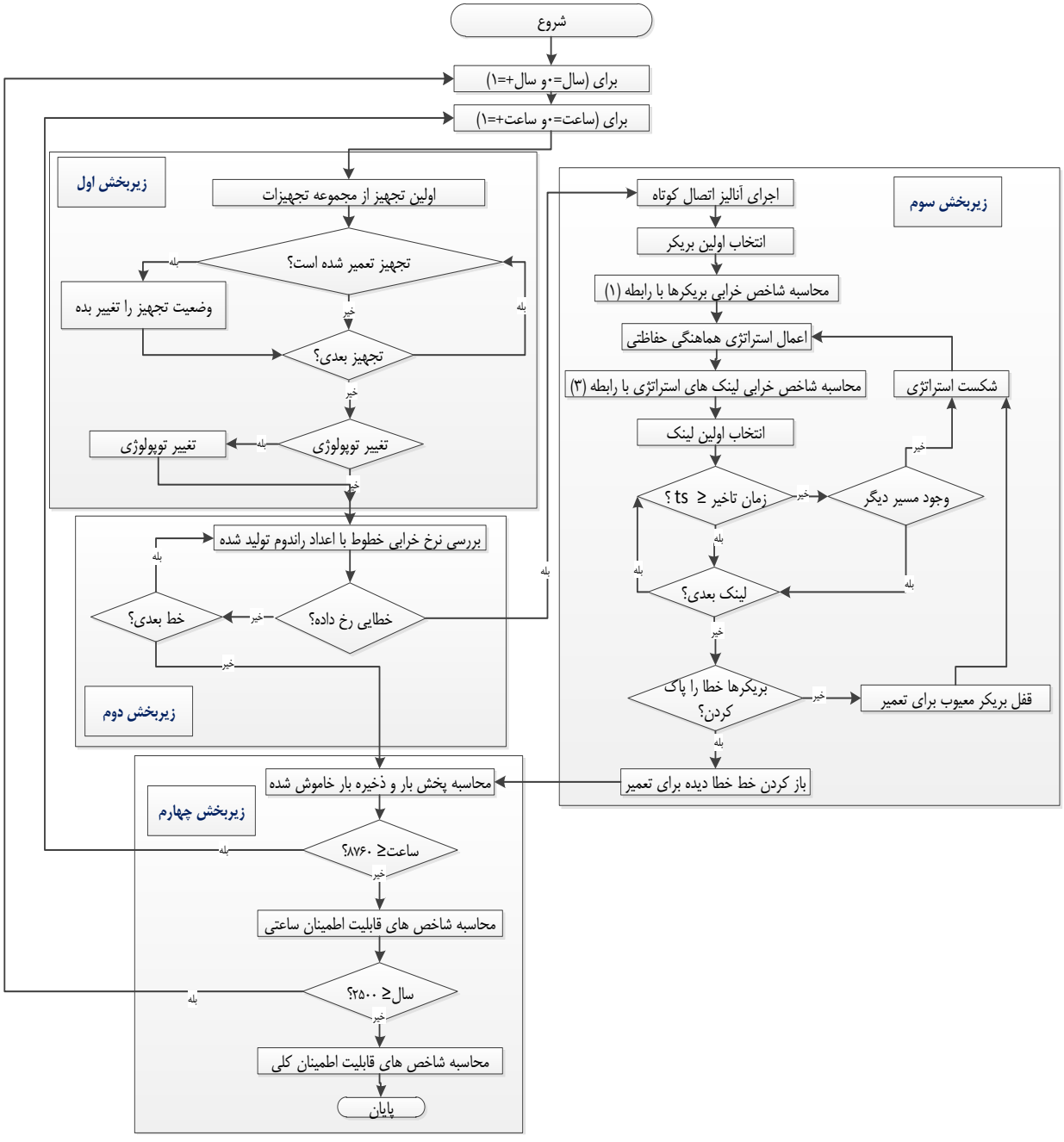
گام دوازدهم: اجرای پخش‌بار و محاسبه بارهای خاموش شده به همراه مدت زمان خاموشی هر بار.

گام سیزدهم: اگر مدت زمان شبیه‌سازی کمتر از ۸۷۶۰ ساعت (یک سال) است به گام اول برو و در غیر اینصورت مقدار سالیانه شاخص-های قابلیت اطمینان (SAIDI، EENS و ECOST) را محاسبه کن.

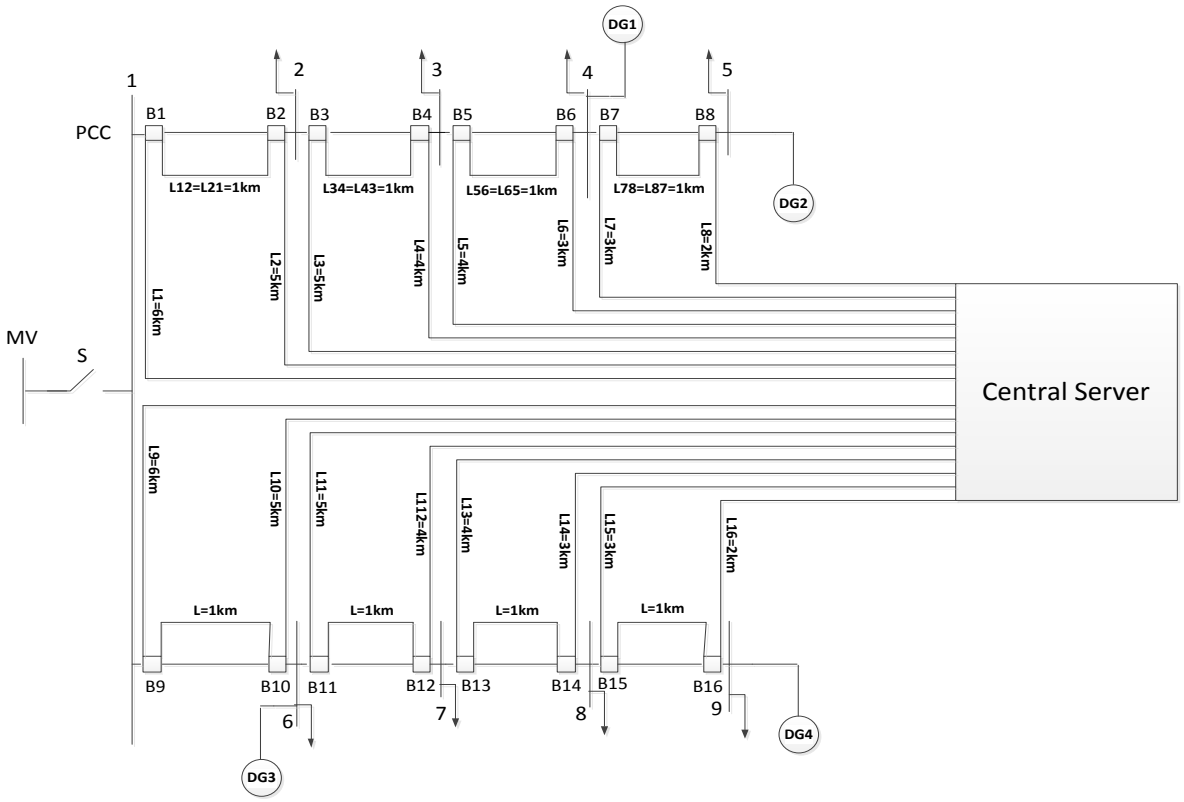
گام چهاردهم: مدت زمان شبیه‌سازی را با مقدار ۲۵۰۰ سال مقایسه کن. اگر کمتر از این مقدار بود به زیر بخش اول برو و در غیر اینصورت مقدار قابل انتظار شاخص‌های قابلیت اطمینان را بعنوان نتیجه نهایی محاسبه کن.

لازم به ذکر است با توجه به آنکه نرخ خرابی تجهیزات مدنظر این مقاله پایین است لذا برای بالا رفتن احتمال رخ دادن این خرابی‌ها، سال‌های شبیه‌سازی باید به اندازه کافی زیاد باشد تا نتایج حاصل شده به مقداری پایدار و قابل قبول همگرا شود. براین‌اساس در این مقاله سال-های شبیه‌سازی ۲۵۰۰ سال درنظر گرفته شده است.

[1] Sequential Monte Carol



شکل (۵): الگوریتم روش پیشنهادی



شکل (۶): میکروگرید مورد مطالعه به همراه حفاظت تطبیقی مرکزی

۴-۲- سیستم نمونه

به منظور ارزیابی روش پیشنهادی، این روش بر روی میکروگرید نمونه شکل (۶) که مجهز به سیستم حفاظت تطبیقی است و در مطالعه [۹] نیز استفاده شده است، پیاده‌سازی می‌شود. در این شبکه، بریکرها در دو سمت کلیه خطوط قرار دارند و سرور مرکزی از طریق دو لینک مخابراتی (یکی مستقیما به هر بریکر متصل است و دیگری از طریق لینک‌های مخابراتی که بین بریکرها قرار دارند) با هریک از بریکرها در ارتباط است. در محاسبه تاخیر زمانی مسیرهایی که از لینک‌های مخابراتی بین بریکرها استفاده می‌کنند، باید تاخیر زمانی لینک مخابراتی که این دستور را تا لینک مخابراتی بین بریکرها انتقال می‌دهد نیز مدنظر قرار گیرد. برای مثال تاخیر زمانی مسیر انتقال فرامین از طریق لینک L_{1-2} به بریکر B_2 برابر با مجموع تاخیر زمانی لینک‌های مخابراتی L_1 و L_{1-2} خواهد بود.

میکروگرید نمونه شکل (۶) به شبکه بالادست از طریق باس ۱ متصل است. چهار منبع تولید پراکنده (5(MW در باس‌های ۴، ۵، ۶ و ۹ متصل است. مشخصات بارهای شبکه در جدول (۱) آورده شده است. مطابق این جدول بارها به سه نوع مسکونی[1]، تجاری[2] و صنعتی[3] تقسیم شده‌اند. هزینه خاموشی هریک از بارها از مطالعه [۲۱] استخراج شده است. بعلاوه منحنی روزانه بارها مطابق الگوهای ارائه شده در [۲۲] می‌باشد. به منظور درنظر گرفتن حالت دینامیک توپولوژی میکروگرید، مشابه مطالعه [۲۳] فرض می‌شود منابع تولید پراکنده موجود در هر فیدر زمانی به شبکه متصل شوند که بار فیدر به ۹۷ درصد پیک بار برسد.

به منظور سادگی محاسبات، فرض می‌شود که کلیه خطوط دارای نرخ خرابی و تعمیرات یکسان هستند. این مقادیر به ترتیب ($\frac{f}{year}$) ۰.۸ و ($\frac{hrs}{f}$) ۳ در نظر گرفته شده‌اند. همانطور که بیان شد نرخ خرابی بریکرها متناسب با دامنه و مدت زمان عبور جریان خطا از آن‌ها می‌باشد و نرخ تعمیرات کلیه بریکرها ($\frac{hrs}{f}$) ۴ درنظر گرفته شده است [۱۶]. بطور مشابه نرخ خرابی لینک‌های مخابراتی با تاخیر زمانی آن‌ها مدل می‌شود و نرخ تعمیرات آن‌ها ($\frac{hrs}{f}$) ۵ درنظر گرفته شده است. لازم به ذکر است قابلیت اطمینان منابع تولید پراکنده ۱۰۰ درصد درنظر گرفته شده است.

مشابه مطالعه [۱۶]، I_R^B و I_U^B کلیه بریکرها به ترتیب (1.25(kA و (10(kA درنظر گرفته می‌شوند. همچنین با توجه به فاصله بریکرها تا سرور مرکزی، میزان تاخیر زمانی استاندارد لینک‌های مخابراتی در

[1] Residential
[2] Commercial
[3] Industrial

جدول (۲) آورده شده است. میزان تاخیر زمانی لینک‌های مخابراتی که بین بریکرها قرار دارند متناسب با طول خطوط و برابر (ms)۰.۰۰۵ است.

جدول (۱): مشخصات بارهای شبکه

شماره بار	توان اکتیو (MW)	توان راکتیو (MVar)	نوع بار
۲	۴.۸	۱.۵	۲
۳	۴.۵	۲.۵	۳
۴	۲.۷	۰.۸	۱
۵	۲.۵	۰.۵	۱
۶	۲.۲	۰.۷	۳
۷	۳.۴	۴	۲
۸	۲	۱	۱
۹	۳	۱	۱

۱: بار مسکونی، ۲: بار تجاری، ۳: بار صنعتی

جدول ۲: تاخیر زمانی لینک‌های مخابراتی بین سرور مرکزی و بریکرهای شکل (۶)

شماره بریکر	میزان تاخیر زمانی (ms)	شماره بریکر	میزان تاخیر زمانی (ms)
۱	۰.۰۳	۹	۰.۰۳
۲	۰.۰۲۵	۱۰	۰.۰۲۵
۳	۰.۰۲۵	۱۱	۰.۰۲۵
۴	۰.۰۲	۱۲	۰.۰۲
۵	۰.۰۲	۱۳	۰.۰۲
۶	۰.۰۱۵	۱۴	۰.۰۱۵
۷	۰.۰۱۵	۱۵	۰.۰۱۵
۸	۰.۰۱	۱۶	۰.۰۱

براساس تابع چگالی احتمال پیشنهاد شده در مطالعه [۱۷]، احتمال خرابی لینک‌های مخابراتی در مطالعه حاضر مطابق مقادیر جدول (۳) فرض شده است.

جدول (۳): احتمال خرابی لینک‌های مخابراتی

نقطه	تاخیر زمانی (ms)	احتمال خرابی
۱	۰.۰۰۵	۰.۲۵
۲	۰.۰۱	۰.۱۵
۳	۰.۰۱۵	۰.۱
۴	۰.۰۲	۰.۰۵
۵	۰.۰۲۵	۰.۱
۶	۰.۰۳	۰.۱۵
۷	۰.۰۳۵	۰.۲

به منظور ارزیابی تاثیر لینک‌های مخابراتی بر عملکرد سیستم حفاظت تطبیقی، دو سناریو بررسی می‌شود. در سناریوی اول فرض می‌شود حفاظت تطبیقی بر مبنای استراتژی‌های سنتی هماهنگی حفاظتی (نزدیکترین بریکرها به خطا بعنوان حفاظت اصلی عمل نموده و در صورت عدم موفقیت بریکرهای همسایه عمل کنند) عمل نماید. اما در سناریوی دوم لزوما نزدیکترین سیستم‌های حفاظت به خطا عمل نمی‌کنند. بلکه سرور مرکزی استراتژی‌های مختلفی که قادر به پاک کردن خطا هستند را بررسی می‌کند و با توجه به تابع هدف ارائه شده در رابطه (۵)، بهترین استراتژی را برای پاک کردن خطا انتخاب می‌نماید. به منظور بررسی میزان تاثیر استفاده از چندین مسیر مخابراتی برای رساندن فرمان‌ها به بریکرها، هر دو سناریوی معرفی شده یکبار با فرض وجود تنها یک لینک مخابراتی بین سرور مرکزی و هر بریکر اجرا می‌شود و یکبار فرض می‌شود علاوه بر لینک‌های مخابراتی حالت قبل، امکان ارسال پیغام سرور مرکزی از طریق لینک‌های مخابراتی بین دو بریکر نیز وجود دارد. لازم به ذکر است کلیه مراحل پیاده‌سازی روش پیشنهادی با استفاده از نرم‌افزار DIgSILENT Power Factory انجام شده است.

$$OF_s = Min\,(Load_{Loss}).\,Max\,(P_s) \qquad (۵)$$

براساس رابطه (۵)، در سناریوی دوم تعادل میان کمترین بار خاموش شده در اثر اعمال استراتژی ($Min(Load_{Loss})$) و بیشترین احتمال عملکرد صحیح سیستم حفاظت ($Max(P_s)$) (با توجه به عدم قطعیت موجود در عملکرد صحیح بریکرها و لینک‌های مخابراتی) عامل تعیین استراتژی‌ها می‌باشد.

۵- نتایج شبیه‌سازی

به منظور بررسی میزان تاثیر عدم قطعیت لینک‌های مخابراتی بر قابلیت اطمینان سیستم حفاظت، شاخص‌های قابلیت اطمینان SAIDI، EENS و ECOST برای سناریوهای مدنظر بترتیب در جدول (۴) و (۵) ارائه شده است.

جدول (۴): شاخص‌های قابلیت اطمینان حاصل شده با استفاده از روش پیشنهادی برای سناریوی اول

	یک مسیر مخابراتی	چند مسیر مخابراتی
SAIDI hrs/customer.yr	۱۳.۰۸	۹.۲۸
EENS (MWh/yr)	۱۷۶.۹۴	۱۴۸.۲۵
ECOST ($/yr)	۸۶۳۸.۶۷	۸۲۶۹.۶۴

جدول (۵): شاخص‌های قابلیت اطمینان حاصل شده با استفاده از روش پیشنهادی برای سناریوی دوم

	یک مسیر مخابراتی	چند مسیر مخابراتی
SAIDI hrs/customer.yr	۷.۴۸	۵.۹۷
EENS (MWh/yr)	۱۱۷.۲۴	۸۹.۴۳
ECOST ($/yr)	۶۲۱۸.۶۱	۵۵۱۰.۷

مقایسه جداول (۴) و (۵) بوضوح برتری سناریوهایی را که از تصمیم‌گیری‌های کلی برای پاک کردن خطا بهره می‌برند، نشان می‌دهد. در واقع همانطور که مشخص است، سناریوی دوم که در آن تعیین استراتژی برتر با توجه به احتمال عملکرد صحیح بریکرها و لینک‌های مخابراتی صورت می‌پذیرد، شاخص‌های قابلیت اطمینان بهتری را

نسبت به سناریوی اول که این کار بصورت سنتی و توسط نزدیکترین بریکرها به خطا انجام می‌پذیرد، ایجاد می‌نماید.

به منظور بررسی دو سناریوی مدنظر، رفتار این دو سناریو به ازای خطای راندوم رخ داده بین باس‌های ۲ و ۳ میکروگرید نمونه بررسی شده است. در این راستا در جدول (۶) برخی از استراتژی‌هایی که قادر به پاک کردن خطا هستند معرفی شده است. لازم به ذکر است استراتژی‌های معرفی شده برای حالتی است که سرور مرکزی از یک مسیر مخابراتی برای ارسال پیغام‌های خود استفاده می‌کند.

جدول (۶): اجزاء برخی استراتژی‌های ممکن برای پاک کردن خطای رخ داده بین باس‌های ۲ و ۳

شماره	اجزاء استراتژی	شماره	اجزاء استراتژی	شماره	اجزاء استراتژی
۱	$B_1 - B_4$	۴	$B_2 - B_4$	۷	$B_3 - B_5$
۲	$B_1 - B_5$	۵	$B_2 - B_5$	۸	$B_3 - B_6$
۳	$B_1 - B_6$	۶	$B_2 - B_6$	۹	$B_3 - B_4$

استراتژی‌های معرفی شده در جدول (۶) بلحاظ زمان اعمال، بار خاموش شده در اثر اعمال استراتژی و احتمال عملکرد صحیح هر استراتژی در جدول (۷) با هم مقایسه شده‌اند. با توجه به شکل‌های (۷) و (۸) مشخص است که در هر دو سناریو استراتژی شماره ۹ بعنوان اولین سطح برخورد با خطا (استراتژی اصلی برای پاک کردن خطا) انتخاب شده است. در سناریوی اول، ملاک انتخاب این استراتژی آن است که بریکرهای B_3 و B_4 نزدیکترین بریکرها به خطا هستند. اما در سناریوی دوم تعادل میان بار خاموش شده در اثر اعمال استراتژی و احتمال عملکرد صحیح استراتژی شماره ۹ ملاک انتخاب بوده‌اند. در این راستا مطابق جدول (۷) مشخص است که اگرچه استراتژی‌های شماره ۶ و ۸ دارای احتمال عملکرد صحیح بالاتری نسبت به استراتژی ۹ هستند اما این استراتژی‌ها بار خاموش شده بیشتری را به شبکه تحمیل می‌نمایند. بنابراین در سناریوی دوم نیز مشابه سناریوی اول استراتژی ۹ بعنوان استراتژی اصلی برای پاک کردن خطا برگزیده می‌شود.

جدول (۷): وضعیت استراتژی‌های کاندید اصلی برای پاک کردن خطای رخ داده بین باس‌های ۲ و ۳

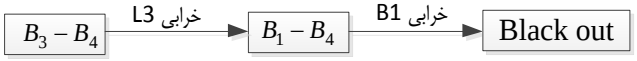
شماره	t_s (mS)	P_s	$Load_{Loss}$ (MW)
۱	۰.۰۳	۰.۰۴۹	۱
۲	۰.۰۳	۰.۰۴۹	۲
۳	۰.۰۳	۰.۰۶۶	۲
۴	۰.۰۲۵	۰.۰۸۵	۱
۵	۰.۰۲۵	۰.۰۸۵	۲
۶	۰.۰۲۵	۰.۱۲	۲
۷	۰.۰۲۵	۰.۰۸۵	۲
۸	۰.۰۲۵	۰.۱۲	۲
۹	۰.۰۲۵	۰.۰۹۵	۱

مطابق شکل‌های (۷) و (۸) در هر دو سناریو، استراتژی منتخب بدلیل خرابی در لینک L_3 شکست خورده است. براین‌اساس جدول (۸) وضعیت استراتژی‌های کاندید پشتیبان را نشان می‌دهد. مقایسه نتایج جدول‌های (۷) و (۸) حاکی از کاهش احتمال عملکرد صحیح استراتژی‌ها به دلیل باقی‌ماندن خطا برای مدت بیشتری در شبکه است.

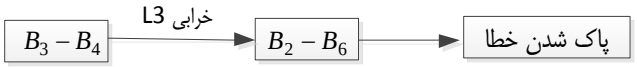
جدول (۸): وضعیت استراتژی‌های کاندید پشتیبان برای پاک کردن خطای رخ داده بین باس‌های ۲ و ۳

شماره	P_s	شماره	P_s
۱	۰.۰۴۲	۴	۰.۰۷۲
۲	۰.۰۴۲	۵	۰.۰۷۲
۳	۰.۰۵۶	۶	۰.۰۹۸

مطابق شکل (۷)، سناریوی اول بدون توجه به احتمال موفقیت استراتژی و مطابق با الگوی هماهنگی حفاظتی سنتی، استراتژی شماره یک را بعنوان استراتژی پشتیبان جایگزین می‌نماید. از جدول (۸) مشخص است که احتمال عملکرد صحیح این استراتژی بسیار پایین است. از این‌رو همانطور که از شکل (۷) مشخص است با وقوع خرابی پنهان در B_1 این استراتژی نیز شکست خورده است که منجر به خاموشی کلی در شبکه گردیده است. اما مطابق شکل (۸)، سناریوی دوم با تصمیم‌گیری کلی استراتژی که از بریکرهای B_2 و B_6 بهره می‌برد (استراتژی شماره ۶) را بعنوان استراتژی پشتیبان، برگزیده است که نتیجه آن پاک کردن موفق خطا بوده است. اگرچه این استراتژی بار خاموش شده بیشتری را به شبکه تحمیل می‌کند اما توانسته با موفقیت خطا را از شبکه پاک نماید و از خاموشی کلی جلوگیری کند. بنابراین استفاده از تصمیم‌گیری کلی می‌تواند نسبت به عدم قطعیت-های تاثیرگذار بر پروسه هماهنگی حفاظتی میکروگرید، پاسخ بهتری را ایجاد نماید و براین‌اساس تاثیرگذاری این عدم قطعیت‌ها را بر عملکرد سیستم حفاظت تا حد ممکن کاهش دهد.



شکل (۷): پاسخ سناریوی اول به خطا بین باس‌های ۲ و ۳



شکل (۸): پاسخ سناریوی دوم به خطا بین باس‌های ۲ و ۳

مطابق نتایج جداول (۴) و (۵) مشخص است که استفاده از چندین مسیر مخابراتی برای ابلاغ پیغام سرور مرکزی به بریکرهای موجود در هر استراتژی هماهنگی حفاظتی با توجه به عدم قطعیت‌های مدنظر در این لینک‌ها می‌تواند احتمال رسیدن پیغام به بریکرها و در نتیجه موفقیت استراتژی را افزایش داده و از این طریق شاخص‌های قابلیت اطمینان میکروگرید را بهبود ببخشد. براین‌اساس مطابق جدول (۵)، شاخص ECOST زمانیکه تنها از یک مسیر مخابراتی بین سرور

مرکزی و هر بریکر استفاده می‌شود ($\frac{\$}{yr}$) ۶۲۱۸.۶۱ می‌باشد این در حالی است که در همین سناریو زمانیکه امکان رساندن پیغام‌های سرور مرکزی از طریق لینک‌های مخابراتی بین بریکرها ممکن می‌شود، هزینه قطعی به ($\frac{\$}{yr}$) ۵۵۱۰.۷ کاهش می‌یابد. این مسئله به این خاطر است که وجود چندین مسیر مخابراتی شانس رسیدن پیغام به بریکرها را افزایش می‌دهد، ضمن آنکه در کاهش زمان رسیدن پیغام‌ها و در نتیجه افزایش احتمال عملکرد صحیح بریکرها، موثر خواهد بود. برای توضیح این مسئله، جدول (۹) احتمال عملکرد صحیح استراتژی که از بریکرهای B_3 و B_4 استفاده می‌کند (استراتژی شماره ۹) را در دو حالت استفاده از یک مسیر مخابراتی و نیز استفاده از مسیر مخابراتی بین بریکرها علاوه بر مسیرهای مخابراتی مستقیم بین هر بریکر و سرور مرکزی نشان می‌دهد. لازم به ذکر است استراتژی مدنظر برای پاک کردن خطای راندوم رخ داده در خط بین باس‌های ۲ و ۳ استفاده شده است. آنالیز اتصال‌کوتاه نشان می‌دهد که به ازای خطای راندوم رخ داده، جریان خطای عبوری از بریکرهای B_3 و B_4 به ترتیب ۳.۹۶ و ۴.۴۲ کیلوآمپر می‌باشد.

جدول (۹): احتمال عملکرد صحیح استراتژی شماره ۹ با یک و دو مسیر مخابراتی

احتمال عملکرد صحیح استراتژی با یک مسیر مخابراتی	احتمال عملکرد صحیح استراتژی با دو مسیر مخابراتی
۰.۰۹۵	۰.۱۹۴

در حالتی که تنها یک مسیر مخابراتی بین سرور مرکزی و هریک از بریکرهای B_3 و B_4 است، تنها پیغام سرور به ترتیب از طریق لینک‌های مخابراتی L_3 و L_4 باید به این بریکرها ارسال شود. در صورت خرابی هریک از لینک‌های مذکور، این استراتژی با شکست روبرو خواهد شد و لازم است استراتژی دیگری جایگزین شود (مانند پاسخ‌های ایجاد شده در شکل‌های (۷) و (۸)). با توجه به کاهش احتمال عملکرد صحیح بریکرها با مدت زمان جریان خطای عبوری، شکست یک استراتژی و جایگزینی استراتژی دیگر موجب کاهش احتمال عملکرد صحیح استراتژی جایگزین می‌شود. این در حالی است که اگر لینک‌های مخابراتی بین بریکرها نیز در ارسال پیغام‌ها مشارکت داشته باشند، به هریک از بریکرهای B_3 و B_4 به ترتیب از طریق لینک‌های مخابراتی L_3 یا L_4+L_{43} و L_4 یا L_3+L_{34} می‌توان پیغام قطع را ابلاغ نمود. همانطور که از جدول (۹) مشخص است، این مسئله موجب افزایش احتمال موفقیت استراتژی می‌شود.

۶- نتیجه‌گیری

با توجه به وابستگی شدید طرح‌های حفاظت تطبیقی میکروگرید به لینک‌های مخابراتی، در این مقاله به بررسی میزان تاثیرپذیری این طرح‌ها نسبت به عدم قطعیت‌های موجود در لینک‌های مخابراتی پرداخته شد. براین‌اساس یک الگوریتم جدید زنجیره مارکوف مبتنی بر مونت‌کارلو برای مدل کردن عدم قطعیت لینک‌های مخابراتی، ارائه گردید. با توجه به مدل ارائه شده، احتمال خرابی لینک‌های مخابراتی متغیر با تاخیر زمانی آن‌ها درنظر گرفته شد. تاخیر زمانی بیشتر در ارسال اطلاعات توسط لینک‌های مخابراتی موجب باقی ماندن بیشتر خطا در شبکه و در نتیجه افزایش احتمال خرابی بریکرها که با دامنه و مدت زمان عبور جریان خطا متغیر است، می‌شود. طرح پیشنهادی بر روی یک میکروگرید نمونه که مجهز به سیستم حفاظت تطبیقی مرکزی است، در دو سناریوی مختلف تست گردید. نتایج پیاده‌سازی روش پیشنهادی نشان می‌دهند که طرح‌های حفاظت تطبیقی که از الگوی تصمیم‌گیری کلی (پاک کرن خطا براساس احتمال موفقیت بریکرها و لینک‌های مخابراتی در کنار میزان خاموش شده بار) استفاده می‌کنند، شاخص‌های قابلیت اطمینان بهتری را نسبت به طرح‌هایی که از الگوهای سنتی (پاک کردن خطا توسط نزدیکترین بریکرها به خطا) استفاده می‌کنند، ایجاد می‌نمایند. همچنین براساس نتایج مشخص است که وجود چندین مسیر مخابراتی برای ارسال پیغام‌ها بین سرور مرکزی و هریک از بریکرها، موجب افزایش احتمال موفقیت استراتژی هماهنگی حفاظتی و در نتیجه بهبود شاخص‌های قابلیت اطمینان سیستم حفاظت، می‌گردد.

مراجع

[۱] P. Basak, et al., "A literature review on integration of distributed energy resources in the perspective of control, protection and stability of microgrid", *Renewable and Sustainable Energy Reviews*, vol. 16 , pp. 5545-5556, 2012.

[۲] P. Mahat, et al., "A simple adaptive overcurrent protection of distribution systems with distributed generation", *IEEE Transactions on Smart Grid*, vol. 2, pp. 428-437, 2011.

[۳] M. Kim, et al., "Wide-area adaptive protection using distributed control and high-speed communications", presented at the 14th PSCC, 2002.

[٤] S. Su, et al., "Agent-based self-healing protection system", *IEEE Transactions on Power Delivery*, vol. 21, pp. 610-618, 2006.

[٥] L. Chen-Ching, et al., "The strategic power infrastructure defense (SPID) system. A conceptual design", *IEEE Control Systems*, vol. 20, pp. 40-52, 2000.

[٦] R. Fenghui , et al., "Conceptual design of a multi-agent system for interconnected power systems restoration", *IEEE Transactions on Power Systems*, vol. 27, pp. 732-740, 2012.

[۷] I. H. Lim, et al., "Multi-agent system-based protection coordination of distribution feeders", *International Conference on Intelligent Systems Applications to Power Systems*, pp. 1-6, 2007.

[۸] M. Khederzadeh, "Adaptive setting of protective relays in microgrids in grid-connected and autonomous operation", *International Conference on Developments in Power Systems Protection*, pp. 1-4, 2012.

[۹] W. K. A. Najy, et al., "Optimal protection coordination for microgrids with grid-connected and islanded capability", *IEEE Transactions on Industrial Electronics*, vol. 60, pp. 1668-1677, 2013.

[۱۰] Y. Damchi, et al., "Optimal coordination of directional overcurrent relays in a microgrid system using a hybrid particle swarm optimization", *International Conference on Advanced Power System Automation and Protection (APAP)*, pp. 1135-1138, 2011.

[۱۱] T. Kato, et al., "Multi-agent based control and protection of power distributed system - protection scheme with simplified information utilization", *13th International Conference on, Intelligent Systems Application to Power Systems*, pp. 49-54, 2005.

[۱۲] S. A. Hosseini, et al., "An overview of microgrid protection methods and the factors involved", *Renewable and Sustainable Energy Reviews*, vol. 64, pp. 174-186, 2016.

[۱۳] C. Yun Hyun and H .Hoon, "Uncertainty modeling in communication for remote control system based on stochastic hybrid system approach", *13th International Conference on Control, Automation and Systems (ICCAS)*, pp. 1821-1824, 2013.

[۱٤] T. S. Ustun, et al., "Recent developments in microgrids and example cases around the world—A review", *Renewable and Sustainable Energy Reviews*, vol. 15, pp. 4030-4041, 2011.

[۱٥] M. M. Eissa, et al., "A novel back up wide area protection technique for power transmission grids using phasor measurement unit", *IEEE Transactions on Power Delivery*, vol. 25, pp. 270-278, 2010.

[۱٦] M. Jazaeri, et al., "Evaluation of the impacts of relay coordination on power system reliability", *International Transactions on Electrical Energy Systems*, vol. 25, pp. 3408–3421, 2015.

[۱۷] C. P. Nguyen and A. J. Flueck, "Modeling of communication latency in smart grid", *IEEE Power and Energy Society General Meeting*, pp. 1-7, 2011.

[۱۸] Q. Binh Dam and A. P. S. Meliopoulos, "Failure probability methodology for overdutied circuit breakers", *38th North American Power Symposium*, pp. 667-672, 2006.

[۱۹] T. Xiaoyang, et al., "The study of a regional decentralized peer-to-peer negotiation-based wide-area backup protection multi-agent system *IEEE Transactions on* ", *Smart Grid*, vol. 4, pp. 1197-1206, 2013.

[۲۰] R. Billinton and A. Sankarakrishnan, "A comparison of Monte Carlo simulation techniques for composite power system reliability assessment", *IEEE Communications, Power, and Computing. Conference Proceedings*, vol.1, pp. 145-150, 1995.

[۲۱] G. Wacker and R. Billinton, "Customer cost of electric service interruptions", *Proceedings of the IEEE*, vol. 77, pp. 919-930, 1989.

[۲۲] M. Gilvanejad, et al., "Estimation of the overload-related outages in distribution networks considering the random nature of the electrical loads", *IET Generation, Transmission & Distribution*, vol. 7, pp. 855-865, 2013.

[۲۳] S. A. Hosseini, et al., "A seven-state Markov model for determining the optimal operating mode of distributed generators", *Journal of Renewable and Sustainable Energy*, vol. 7, p. 033114, 2015.