نشریه علمی‌پژوهشی مهندسی و مدیریت انرژی

سال دوازدهم، شمارهٔ سوم/ پاییز ۱۴۰۱/ صفحه ۳۴ـ۵۱

نوع مقاله: پژوهشی

تاریخ دریافت: ۱۳۹۹/۱۰/۲۲ تاریخ پذیرش: ۱۴۰۰/۹/۹

حفاظت تطبیقی مبتنی بر هوشمندسازی شبکه‌های توزیع به‌کمک عاملی کردن شبکه در حضور منابع تولید پراکنده

سپیده تیموریان[۱،۴]، غضنفر شاهقلیان[۲،۴*]، بهادر فانی[۳،۴]

[۱] دانش‌آموخته کارشناسی‌ارشد، دانشکده مهندسی برق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران
sepideh_teymouriyan@yahoo.com

[۲] دانشیار، دانشکده مهندسی برق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران
shahgholian@iaun.ac.ir

[۳] دانشیار، دانشکده مهندسی برق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران
bahadorfani@gmail.com

[۴] مرکز تحقیقات ریزشبکه‌های هوشمند، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران

چکیده: یکی از روش‌های مناسب هوشمندسازی یک سیستم، عاملی کردن آن است. با عاملی کردن سیستم حفاظتی و مهیا ساختن ارتباط مناسب عامل‌ها با یکدیگر و انتقال هرچه سریع‌تر و مطمئن‌تر اطلاعات، می‌توان عملکرد یک سیستم حفاظتی را بهبود بخشید و قابلیت اطمینان سیستم را در مقابل منابع تولید پراکنده حفظ کرد. در این مقاله با استفاده از دستگاه‌های الکتریکی هوشمند، الگوریتم‌های کنترلی و زیرساخت مخابراتی، روشی جدید برای هماهنگی سیستم حفاظتی شبکه در حضور منابع تولید پراکنده ارائه شده است. به‌منظور انعطاف بیشتر و ایجاد عدم وابستگی به واحد پردازش مرکزی، در این نوع پیاده‌سازی تصمیمات توسط خود عامل‌ها انجام می‌گیرد. عامل‌ها یک ارتباط نقطه‌به‌نقطه دارند که به‌منظور جبران عدم حضور واحد مرکزی با یکدیگر ارتباط برقرار می‌کنند. نقش واحد پردازش مرکزی به‌کمک مدل‌سازی اطلاعات و تعریف توابع بر روی عامل‌ها پیاده‌سازی می‌شود. الگوریتم ارائه‌شده در این مقاله با استفاده از یک بستر مخابراتی ساده و پیاده‌سازی یک روند محاسباتی به‌منظور اصلاح تنظیمات رله‌های حفاظتی هماهنگی ازدست‌رفته در حضور منابع تولید پراکنده را بازیابی می‌کند. به این منظور برای هماهنگی بین رله‌های حفاظتی و نیز تبادل اطلاعات مابین آن‌ها، یک سیستم چندعاملی اصلاح‌شده پیش‌بینی شده است. در این طرح، رله‌های حفاظتی اطلاعات مربوط به وضعیت عملکرد خود را با دیگر رله‌های مجاور به‌منظور حفظ هماهنگی به اشتراک می‌گذارند. روش پیشنهادی بر روی یک شبکهٔ آزمایشی توسط نرم‌افزار ETAP شبیه‌سازی شده، مورد ارزیابی قرار گرفته و درستی آن نشان داده شده است. قابلیت تشخیص تغییرات جریان و ساختار شبکه وجود دارد و با استفاده از جدول اطلاعاتی حالت‌های حفاظتی جدید تشخیص داده می‌شود و بر مبنای آن ناحیهٔ حفاظتی مشخص می‌گردد. سپس با استفاده از اطلاعات جریانی به‌دست‌آمده، عملکرد رلهٔ پشتیبان بهبود می‌یابد.

واژه‌های کلیدی: حفاظت تطبیقی، هوشمندسازی شبکه، منابع تولید پراکنده.

---

* نویسنده مسئول

۱. مقدمه

امروزه استفاده از نیروگاه‌های تولید پراکنده[1] مانند نیروگاه بادی، میکروتوربین، پیل سوختی، سلول خورشیدی، ژنراتور دیزلی، سیستم ذخیرهٔ انرژی در ابررسانا و سیستم ذخیرهٔ انرژی در باتری در سیستم‌های قدرت اهمیت زیادی پیدا کرده است [۱ و ۲]. از مزایای استفاده از تولیدات پراکنده در سیستم توزیع می‌توان به رعایت مسائل زیست‌محیطی، کاهش تلفات انتقال و پایین بودن هزینه‌ها اشاره کرد؛ بنابراین تولیدات پراکنده باید دارای اندازهٔ مناسب بوده و در مکان‌های مناسب نصب شوند [۳ و ۴]. بیشترین اثر منفی احتمالی منابع پراکنده روی شبکهٔ توزیع مربوط به سطح ولتاژ و هماهنگی حفاظتی است. همچنین منابع پراکنده باعث پیچیده شدن شبکه و در نتیجه توسعهٔ سیستم حفاظت شبکه شده و بهره‌برداری و کنترل شبکه را مشکل می‌سازد [۵ و ۶].

روش‌های مختلفی برای تعدیل اثر تولیدات پراکنده بر سیستم حفاظت وجود دارد [۷ و ۸]. این روش‌ها می‌توانند مشکلات حفاظتی را به‌طور موفقیت‌آمیزی برطرف کنند اما هریک از نقاط ضعفی دارند [۹ و ۱۰]. این روش‌ها عبارت‌اند از:

ـ خاموش کردن تولید پراکنده بعد از تشخیص خطا با این احتمال که امکان آسیب به واحدهای تولید پراکنده افزایش می‌یابد؛

ـ محدود کردن ضریب نفوذ تولید پراکنده که در این روش مزایای حضور تولیدات پراکنده در حالت عملکرد نرمال متصل به شبکه کاهش می‌یابد؛

ـ تغییر سیستم حفاظتی که هزینه‌بر است و منجر به پیچیده شدن ساختار حفاظتی می‌شود؛

ـ استفاده از محدودکننده‌های جریان خطا که هزینهٔ زیادی در بر دارد و در نهایت استفاده از حفاظت تطبیقی که نیاز به زیرساخت‌های ارتباطی و کنترلر پردازش سریع دارد.

در کل حضور هریک از این روش‌ها شبکهٔ توزیع توان و شرایط عملکرد آن را پیچیده‌تر می‌کند.

ساختار حفاظت تطبیقی به‌دلیل پیدایش و گسترش سریع سیستم‌های چندعاملی مورد توجه قرار گرفته است. ماهیت مستقل، مشارکتی و پویای سیستم‌های چندعاملی باعث شده به‌منظور حفاظت از شبکه‌های توزیع در برابر تغییر بارها و منابع پراکندهٔ مختلف مورد استفاده قرار گیرند [۱۱ و ۱۲].

شبکه‌های برق نیاز به حفاظت الکتریکی دارند که در اکثر نقاط آن‌ها از رله‌های حفاظتی استفاده می‌شود. تنظیمات حفاظتی یک رلهٔ اضافه جریان عامل مهمی در عملکرد صحیح آن است و لازم است تا در ازای شروع هر تغییر یا وقوع رخداد در شبکه بر روی این تنظیمات بازنگری انجام گیرد [۱۳ و ۱۴]. سیستم حفاظت سنتی به‌علت نداشتن عملکرد آگاهانه نسبت به تغییرات و نبودن تنظیمات مناسب بر روی آن‌ها نمی‌تواند در شرایط تغییر شبکه عملکرد صحیحی داشته باشد؛ لذا با هوشمندسازی یک سیستم حفاظتی، می‌توان عملکرد آن را بهبود بخشید.

تاکنون مطالعات مختلفی برای هماهنگی سیستم حفاظتی شبکه در حضور منابع تولید پراکنده ارائه شده است [۱۵ و ۱۶].

هماهنگی حفاظتی بهینه مقید به پایداری سیستم به‌صورت مسئله تصادفی در ریزشبکه با مدهای عملکردی اتصال به شبکه و جزیره‌ای شامل منابع انرژی تجدیدپذیر و سیستم‌های ذخیره‌ساز انرژی در مرجع [۱۷] اشاره شده و محدودیت‌های فاصلهٔ زمانی هماهنگی، پارامترهای تنظیم رله‌ها، اندازهٔ محدودکنندهٔ جریان خطا و پایداری ریزشبکه در شرایط خطا در نظر گرفته شده است.

یک طرح حفاظتی مبتنی بر ارتباطات کارآمد که رله‌های جریان بیش از حد جهت‌دار را به‌جای ریکلوزرها در خط، با تداخل و انسداد توابع انتقال پیاده‌سازی می‌کند، در مرجع [۱۸] پیشنهاد شده است که در آن انتخاب‌پذیری را بدون توجه به اتصال واحدهای تولیدکننده به شبکه تضمین می‌کند.

هماهنگی حفاظتی بهینه برای شبکه‌های کوچک و جزیره‌ای متشکل از منابع انرژی تجدیدپذیر و سیستم ذخیرهٔ انرژی در مرجع [۱۹] ارائه شده است که هدف در آن به حداقل رساندن زمان کل عملکرد رله‌های جریان بیش از حد تنظیم‌کنندهٔ دوگانه در حالت حفاظت اولیه و پشتیبان در نظر گرفته شده است.

معایب چند روش برای حفاظت شبکه‌های قدرت در جدول (۱) بیان شده است.

در این مقاله روشی برای حل مشکلات مربوط به هماهنگی حفاظتی میان رله‌ها به‌کمک یک طرح جدید مبتنی بر عامل‌های هوشمند ارائه می‌شود. این روش که برای بازگردانی هماهنگی حفاظتی است، بر روی رلهٔ پشتیبان پیاده‌سازی می‌گردد و جهتِ تغییر نحوهٔ عملکرد آن فعال می‌شود. در روش پیشنهادی به‌صورت محلی بر روی رله تغییرات لازم اعمال و در شرایط مناسبی قرار داده می‌شود.

با توجه به اینکه رفع خطای شبکه، وظیفهٔ حیاتی برای شبکهٔ توزیع است، ممکن است فرایند جمع‌آوری اطلاعات شبکه، تحلیل و آنالیز آن‌ها و همچنین تصمیم‌گیری صحیح توسط واحد مرکزی

1. Distributed Generation

آنقدر زمان‌بر باشد که در زمان مناسب خطا را نتواند پاک‌سازی نماید. به همین منظور لازم است تا پس از رفع خطای شبکه تنظیمات حفاظتی به‌روزرسانی شوند.

جدول (۱): بررسی روش‌های پیشنهادی بر روی حفاظت شبکه‌های قدرت

	روش	معایب
مدیریت منابع تولید پراکنده	– محدود کردن جریان DG – بهینه کردن مکان قرارگیری و ظرفیت منابع – قطع اتصال DG از شبکه	قطع اتصال منبع تولید پراکنده در هر بار که خطایی رخ می‌دهد، ممکن است بر روی قابلیت اطمینان شبکهٔ توزیع اثرگذار باشد. همچنین مشخص کردن محدودیت بر روی نصب این منابع می‌تواند برای مالکان آن‌ها ناخوشایند باشد.
محدود کردن جریان خطا	– استفاده از SFCL – استفاده از FCL	تعیین مقادیر امپدانس FCL به‌سختی انجام می‌شود و هزینهٔ سرمایه‌گذاری هنگفتی برای تهیهٔ دستگاه‌های ذخیره‌سازی است که قادر به مقاومت در برابر مقادیر بالای خطای ناشی از DN هستند.
تغییر در سیستم حفاظتی	– حفاظت دیستانس – حفاظت دیفرانسیل – حفاظت جهتی – حفاظت پایلوت – کلیدهای اضافی	هزینهٔ سرمایه با افزایش تعداد رله، CT و CB زیاد است؛ به همین دلیل روش تنظیم رله‌ها می‌تواند سخت‌تر از رله‌های جریان زیاد معمولی باشد. از طرف دیگر برخی از این روش‌ها فقط برای محافظت از خط مؤثر است و توانایی محافظت از باس بارهای متصل به DG یا بار را ندارد.
سیستم حفاظت وفقی	– استفاده از تنظیمات چندتایی – بهینه کردن تنظیم حفاظتی – سیستم حفاظتی متمرکز	حجم داده‌های مورد نیاز برای تجزیه و تحلیل ممکن است مقدار زیادی از حافظهٔ محاسباتی را مصرف کنند و پرهزینه شوند. همچنین می‌توانند با تغییر شبکه نیازمند محاسبات جدید گردند. پیشنهاد یک راه‌حل بهینه نیز وابسته به وجود مقدار زیادی از داده‌هاست. در روش‌های متمرکز وابستگی به واحد مرکزی می‌تواند قابلیت اعتماد را کاهش دهد.
سیستم حفاظت هوشمند	– استفاده از ساختار سیستم‌های اندازه‌گیری و حفاظتی گستردهٔ شبکه – روش‌های مبتنی بر واحدهای اندازه‌گیری فازور و عامل – حالت ارتباطی نقطه‌به‌نقطه در ساختار چندعاملی	نیازهای فراوانی برای انتقال بموقع اطلاعات در کل شبکه دارد و محاسبات آن می‌تواند پیچیده‌تر و بسیار پرهزینه باشد. اما می‌تواند برای افزایش امنیت و قابلیت اطمینان مفید باشد. وقتی سیستم بزرگ است و عامل‌های زیادی وجود دارد، مدل‌های هماهنگی پیچیده می‌شوند. پیچیدگی ارتباطات و کنترل را ساده می‌کند و می‌تواند هدف بهینه‌سازی را بهتر محقق کند.

به‌عبارت دیگر هنگام وقوع خطا، در ابتدا به‌وسیلهٔ روش پیشنهادی خطای شبکه پاک‌سازی می‌شود و در ادامه رله‌ها تنظیمات مناسب خود را دریافت می‌کنند. در طرح حفاظتی پیشنهادی برخلاف ساختار حفاظتی چندعاملی معمول، فرایند محاسبه و به‌روزرسانی تنظیمات حفاظتی در شرایط وقوع رویداد در شبکه، به‌صورت همزمان با فرایند رفع خطا صورت می‌پذیرد. در این روش، درخواست‌های مربوط به انتقال اطلاعات جریان شبکه، محاسبه و به‌روزرسانی تنظیمات مجزا صورت می‌پذیرد. عامل‌های رله با توجه به ناحیهٔ مستقر در آن، اطلاعات مربوط به تنظیمات عضوهای ناحیه‌های محلی و همسایهٔ خود را ذخیره می‌کنند تا بتوانند در حالت عملکرد مستقل از این اطلاعات استفاده نمایند. این شیوهٔ عملکرد مانع از ایجاد تأخیرهای طولانی‌مدت در عملکرد سیستم حفاظت شبکه می‌شود؛ همچنین موجب می‌گردد تا فرایند رفع خطا و به‌روزرسانی تنظیمات به‌صورت دو فرایند کاملاً مستقل از یکدیگر عمل نمایند تا فرایند رفع خطا، وابستگی خود را نسبت به عملکرد واحد مرکزی حذف کند.

طرح پیشنهادی بدون در نظر گرفتن ضریب نفوذ منابع تولید پراکنده، تغییر در ساختار ریزشبکه و محل وقوع خطا، باعث عملکرد صحیح رله‌های اضافه جریان می‌شود. در این طرح عامل‌های رله در یک بستر مخابراتی تک‌لایه به تبادل اطلاعات با یکدیگر می‌پردازند. بر این اساس وضعیت عملکرد سیستم حفاظت تشخیص داده می‌شود و از عملکرد اشتباه رله‌ها در شرایط مختلف جلوگیری می‌گردد.

به‌طور کلی زمان عملکرد در سیستم چندعاملی می‌تواند به‌صورت زیر تخمین زده شود:

– زمان ارسال اطلاعات از هر عامل به واحد پردازش مرکزی؛
– زمان مربوط به پردازش و محاسبات اطلاعات؛
– زمان مربوط به بازگشت اطلاعات و تنظیمات جدید؛
– زمان مربوط به بارگذاری اطلاعات جدید بر روی رله‌ها؛
– بررسی وضعیت همکاری[1] در شرایط جدید؛

1. Relay Cooperation Checking

– زمان مورد نیاز برای عملکرد صحیح یک رله در لحظهٔ خطا.

همان‌گونه که مشخص است در یک ساختار چندعاملی چندلایه، کل زمان سپری‌شده برای عملکرد رله در شرایط خطا برابر مجموع زمان‌های اشاره‌شده است. در واقع طرح حفاظتی در این شرایط زمانی کامل می‌شود که این فرایند به‌طور کامل و پشت‌سرهم اجرا گردد. این مدت‌زمان با توجه به نظر نویسندگان در مرجع [۴] می‌تواند بسیار قابل ملاحظه باشد، به‌طوری که در آن برای جلوگیری از شکست سیستم حفاظتی راه‌حل قابل قبولی برای حل این مشکل ارائه نشده است. اما در این مقاله سعی شده است الگوریتمی ارائه شود که با مشخص کردن حالت شبکه در زمان وقوع خطا، نحوهٔ عملکرد سیستم چندعاملی به‌نحوی تغییر داده شود که عملکرد سیستم حفاظتی با مشکل مواجه نگردد.

در بخش دوم مقاله به مرور ساختار سیستم حفاظتی مبنی بر سیستم‌های چندعاملی و حفاظت مبتنی بر سیستم چندعاملی اشاره می‌شود. بخش سوم طرح هماهنگی حفاظتی پیشنهادشده بر روی تجهیزات هوشمند الکتریکی بیان می‌شود تا به‌عنوان مبنای ارائه الگوریتم طرح در بخش چهارم استفاده شود. بخش پنجم نیز ارزیابی‌ها و نتایج شبیه‌سازی بر اساس روش پیشنهادی نشان می‌دهد.

۲. طرح حفاظتی مبتنی بر ساختار سیستم‌های چندعاملی

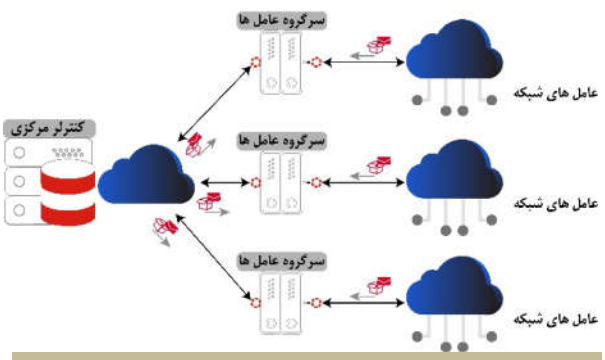
در این قسمت به تعریف عامل و چگونگی تشکیل ساختار سیستم چندعاملی پرداخته و عملکرد این ساختار در حفظ سلامت یک سیستم حفاظتی بررسی شده است.

۲. ۱. تعریف عامل

عامل، یک سخت‌افزار یا نرم‌افزار است که می‌تواند در یک شبکه قرار گیرد و به‌صورت کاملاً مستقل نسبت به تغییرات محیط عکس‌العمل نشان دهد. منظور از محیط، فضای پیرامون یک عامل است که توسط عامل قابل مشاهده بوده و می‌تواند از آن اطلاعات جمع‌آوری و آن‌ها را ذخیره کند و به تجهیزات پیرامون خود فرمان ارسال نماید. بر اساس این تعریف می‌توان وظایف یک عامل را به سه بخش تقسیم‌بندی کرد: الف. برقراری ارتباط با سایر عامل‌ها و اشتراک اطلاعات؛ ب. واکنش نسبت به تغییرات محیط؛ ج. تصمیم‌گیری و ارسال فرمان به سایر عامل‌ها.

۲. ۲. ساختار سیستم چندعاملی

سیستم چندعاملی سیستمی است که چند عامل با هم در ارتباط‌اند و هرکدام وظایف خود را به‌طور مستقل به‌منظور جمع‌آوری اطلاعات و آگاهی یافتن از وضعیت شبکه انجام می‌دهند. سیستم چندعاملی به‌عنوان بخشی از سیستم هوشمند قادر است تا به‌واسطهٔ این ارتباطات و اطلاعات جمع‌آوری‌شده از شبکه، در رسیدن به اهداف سیستم کمک‌رسان آن باشد [۲۰ و ۲۱]. یکی از این اهداف، دستیابی به یک طرح حفاظتی انعطاف‌پذیر در شرایط مختلف است. هر عامل به‌عنوان یک نقطهٔ هوشمند در همکاری با عوامل دیگر از طریق زیرساخت ارتباطی به‌منظور حل مشکل در حفاظت از سیستم قدرت عمل می‌کند [۲۲ و ۲۳]. طرح‌ها، ساختارها و پیکربندی مشخصی به‌همراه عوامل مختلف تاکنون پیشنهاد شده است که اغلب آن‌ها در طبقه‌بندی سلسله‌مراتبی دارای شباهت‌هایی هستند [۲۴ و ۲۵]. به‌طور کلی یک ساختار سیستم چندعاملی را می‌توان به سه لایه تقسیم کرد: لایهٔ اول مربوط به تجهیزات مستقر در شبکه است؛ لایهٔ دوم مربوط به سرگروه‌های هریک از دسته عامل‌های بخش اول بوده و در نهایت لایهٔ سوم مربوط به تحلیل اطلاعات و تصمیم‌گیرندهٔ نهایی است که با عنوان کنترلر مرکزی نام‌گذاری می‌شود. ساختار سیستم چندعاملی در شکل (۱) نشان داده شده است. در سطح اول این لایه که وظیفهٔ جمع‌آوری اطلاعات و اندازه‌گیری‌ها را بر عهده دارد، می‌توان تجهیزات مختلفی مانند رله‌ها، کلیدها، ترانس‌های جریان، ترانس‌های ولتاژ، منابع تولید پراکنده و... در نظر گرفت. هریک از این عامل‌ها در صورتی که در ساختار سیستم چندعاملی حضور داشته باشند، در یک دستهٔ مشخص قرار می‌گیرند. در سطح دوم اطلاعات مربوط به هریک از دسته‌بندی‌های سطح اول جمع‌آوری و مستقیماً به سطح سوم انتقال داده می‌شود. سطح سوم که کنترلر مرکزی در آن قرار دارد، وظیفهٔ سازمان‌دهی عملکرد همهٔ عامل‌های سطوح پایین‌تر را بر عهده دارد.



شکل (۱): ساختار سیستم چندعاملی

۲. ۳. پروتکل ارتباطی سیستم چندعاملی

برای برقراری ارتباط بین عامل‌ها به‌منظور انتقال اطلاعات در طول شبکه با استفاده از لینک‌های مخابراتی، از پروتکل IEC-61850 که یک پروتکل اختصاصی سیستم توزیع است، استفاده می‌شود [۲۶ و ۲۷]. این پروتکل می‌تواند بر روی شبکه‌های TCP/IP با استفاده از سرعت بالای خود در شبکه به انتقال داده بپردازد. بر اساس این پروتکل، مکانیزم کنترلی GOOSE قادر است تا هر نوع داده را در زمانی کمتر از چهار میلی‌ثانیه، بر روی شبکه انتقال دهد [۲۸]. سرعت بالای این پروتکل باعث شد تا از آن در طرح‌های جدید به‌منظور برقراری ارتباط میان تجهیزات حفاظتی استفاده شود.

۲. ۴. حفاظت مبتنی بر سیستم چندعاملی

در شیوهٔ حفاظت مبتنی بر سیستم‌های چندعاملی، عامل‌های مختلف شامل تجهیزات حفاظتی، منابع تولید پراکنده، باس بارها، کلیدها و غیره، در طرح حفاظتی شرکت دارند [۲۹ و ۳۰]. هنگامی که یک رویداد در شبکه، شامل تغییر ساختار، افزایش یا کاهش نفوذ منابع تولید پراکنده، تغییر بارها، وضعیت اتصال شبکه، رخداد خطا و... اتفاق می‌افتد، عامل‌ها اطلاعات را به سیستم کنترل مرکزی ارسال می‌کنند. در مرحلهٔ بعد، اطلاعات در سیستم مرکزی پردازش شده و تصمیم گرفته شده (مطابق با یک جدول برنامه‌ریزی) به لایه‌های مخابراتی زیرین انتقال داده می‌شود. در این ساختار با توجه به اینکه هر لحظه وضعیت شبکه مشخص است، همواره حفاظت‌ها در حال تغییر تنظیمات خود با توجه به فرمان دریافتی از سطوح بالاتر هستند. بنابراین با این ساختار می‌توان نسبت به مشکلات ناشی تغییرات شبکه که به‌موجب آن حفاظت‌های سنتی را دچار شکست می‌کرد، غلبه کرد. در ادامه این مشکلات بررسی و نشان داده شده است که سیستم حفاظت سنتی چگونه دچار شکست می‌گردد.

۳. طرح هماهنگی حفاظتی پیشنهادی بر روی تجهیزات هوشمند الکتریکی

تاکنون روش‌های متعددی برای محافظت مرکزی ریزشبکه‌ها با ساختارهای مختلف ارائه شده است [۳۱ و ۳۲]. یکی از این روش‌ها طرح‌های عاملی مبتنی بر سیستم چندعاملی سلسله‌مراتبی است. از معایب اصلی این طرح‌ها می‌توان به نیازمند بودن به ارتباطات وسیع و استفاده از یک کنترل‌کنندهٔ بسیار قدرتمند و قابل اعتماد اشاره کرد. بنابراین سیستم حفاظتی توزیع‌شدهٔ پیشرفته و ارتباطات اینترکتیو برای غلبه بر محدودیت‌های حفاظت از سیستم نیاز است. تلفیق کنترل‌کننده‌های توزیع‌شده با سیستم‌های چندعاملی برای حفاظت سیستم مفید است. برای مثال در سیستم‌های چندعاملی مجهز به کنترل‌کننده‌های توزیع‌شده، با مختل شدن عملکرد یک کنترل‌کننده، عملکرد کل ریزشکبه مختل نمی‌شود و سایر کنترل‌کننده‌های در ارتباط با آن کنترل‌کننده، وظیفهٔ آن را انجام می‌دهند. همچنین در این‌گونه سیستم‌ها احتیاج به کنترل‌کننده‌های بسیار قدرتمند وجود نخواهد داشت و به همین علت برای محافظت از ریزشبکه‌ها به روش‌های کنترل توزیع‌شده روی آورده شده است. در این مقاله طرحی ارائه شده است که در آن می‌توان مشکلات مربوط به هماهنگی حفاظتی میان رله‌ها را به‌کمک یک طرح جدید مبتنی بر عامل‌های هوشمند برطرف کرد. این طرح که به‌منظور بازگردانی هماهنگی حفاظتی است، بر روی رلهٔ پشتیبان پیاده‌سازی می‌گردد و جهتِ تغییر نحوهٔ عملکرد آن فعال می‌شود.

۳. ۱. مقایسهٔ ساختار عاملی سنتی با طرح پیشنهادی

شبکهٔ هوشمند حاصل ترکیب علم کنترل، مخابرات و قدرت در شبکه‌هاست. بنابراین ارسال و دریافت داده‌های شبکه با امنیت و استاندارد بالا، اهمیت فراوانی دارد. برای ایجاد بستر مخابراتی در شبکه‌های قدرت و همچنین بالا بردن امنیت و اطمینان در انتقال داده‌ها در شبکه‌های قدرت، می‌توان از تکنولوژی سیستم‌های چندعاملی استفاده کرد. برای پیاده‌سازی الگوریتم‌های کنترلی و هوشمندسازی عامل‌های موجود در شبکهٔ قدرت نیاز به دستگاه الکترونیکی هوشمند[1] (IED) است. همچنین برای کاهش هزینه و کاهش ادوات مورد نیاز برای عاملی کردن شبکهٔ قدرت، می‌توان با تنظیم مناسب IEDها و تبدیل آن‌ها به حفاظت IED، آن‌ها را جایگزین رله‌ها کرد. از طرفی هریک از این ادوات الکترونیکی هوشمند، توانایی اندازه‌گیری و ذخیره‌سازی برخی اطلاعات مانند جریان عبوری، اندازهٔ ولتاژ و... را دارند که باعث می‌شود دیگر به اضافه کردن تجهیزات اندازه‌گیری در شبکهٔ قدرت نیازی نباشد. یکی از روش‌های پیشنهادی عاملی کردن سیستم حفاظتی و طراحی یک کنترل‌کنندهٔ وفق‌پذیر برای کم کردن تأثیر خطای جریان در اثر اضافه شدن منابع تولید پراکنده به شبکه است. با در نظر گرفتن وضعیت منابع تولید پراکنده، یک استراتژی برای

1. Intelligent Electronic Device

پیش‌بینی تنظیمات رله‌ها طراحی می‌شود که رله‌ها را با توجه به توپولوژی مختلف سیستم و محل قرار گرفتن منابع تولید پراکنده، وفق‌پذیر با شرایط موجود می‌کند. برای وفق‌پذیر کردن تنظیمات رله‌ها، یک کنترل‌کنندهٔ مرکزی طراحی می‌شود که با در نظر گرفتن پارامترهای مختلف تنظیمات رله‌ها را تغییر می‌دهد. یکی از مشکلات اجرایی این طرح، کنترل‌کنندهٔ مرکزی آن است که پیاده‌سازی را ملزم به ارتباط وسیع کنترل‌کنندهٔ مرکزی با همهٔ عامل‌ها می‌کند. همچنین به یک کنترل‌کنندهٔ بسیار قوی و مطمئن نیاز است، زیرا اگر کنترل‌کننده دچار اختلال شود، عملکرد کل سیستم را مختل می‌کند. یکی دیگر از مشکلات پیاده‌سازی این طرح، تعداد بسیار زیاد عامل‌ها در عاملی کردن سیستم است. تعداد زیاد عامل‌ها، به‌معنای جمع‌آوری داده‌های بسیار زیاد است که می‌تواند سیستم را دچار اختلال کند. علاوه بر اشکال‌های فوق، استفاده از بستر مخابراتی همواره می‌تواند نگرانی‌های ناشی از بروز تهدیدات سایبری را نیز به همراه داشته باشد. با توجه به اینکه تصمیمات کنترل مرکزی وابسته به اطلاعات جمع‌آوری‌شده از شبکه است، تغییر در اطلاعات جمع‌آوری‌شده می‌تواند مشکلات زیادی به همراه داشته باشد که یکی از آن‌ها مشکلات مربوط به خروج خط بر اثر عملکرد اشتباه سیستم حفاظت شبکه است.

در این مقاله روشی ارائه می‌شود تا به‌صورت محلی بر روی رله تغییرات لازم اعمال شود و در شرایط مناسبی قرار داده شود. در این روش به‌کمک هوشمندسازی سیستم حفاظتی، شرایطی برنامه‌ریزی می‌شود که در عملکرد هر رله در شرایط قرار گرفتن در حالت پشتیبان بهبود می‌یابد. این طرح به جمع‌آوری اطلاعات شبکه وابسته نبوده و از میزان تهدیدات موجود بر روی ساختار سلسله‌مراتبی کاسته می‌شود. همچنین در این طرح با کاهش تعداد عامل‌های موجود در یک طرح حفاظتی مبتنی بر سیستم‌های چندعاملی، از هزینه‌های پیاده‌سازی آن کاسته می‌شود. با توجه به پیاده‌سازی ساختار به‌صورت محلی، نیازی به حضور یک سیستم مرکزی نیز وجود نخواهد داشت.

۳. ۲. طرح حفاظتی مبتنی بر عامل‌های هوشمند

با طرح پیشنهادی در این مقاله، می‌توان خطای به‌وجودآمده را شناسایی و برطرف کرد. همچنین این روش به‌دلیل انعطاف‌پذیر بودنش، به محل وقوع خطا و مکان منبع تولید پراکنده حساس نیست. در این روش با به‌کارگیری حفاظت‌های هوشمند در شبکه، رله‌ها قادرند در مقابل تغییرات شبکه، عملکرد خود را بهبود دهند. این روش که به‌منظور بهبود عملکرد حفاظت پشتیبان شبکه است، به‌کمک تغییر شرایط حضور عامل‌های رله و همچنین گزارش جریان عبوری از آن‌ها، به عملکرد سیستم حفاظت شبکه کمک می‌کند. روش پیشنهادی ارائه‌شده در این مقاله به این صورت دسته‌بندی می‌شود: الف. ساختار ارتباطی میان سیستم حفاظت هوشمند؛ ب. تبادل اطلاعات شبکه؛ ج. مشخص کردن رویداد در شبکه بر روی رله‌ها؛ د. محاسبهٔ تنظیمات جدید بر روی رلهٔ پشتیبان.

الف. ساختار ارتباطی میان سیستم حفاظت هوشمند

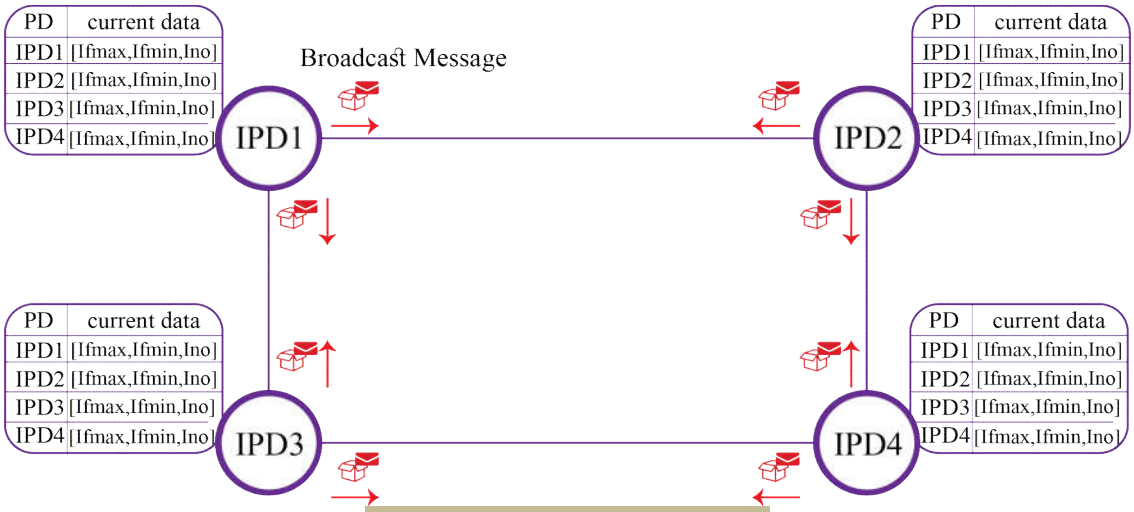
شکل (۲) ساختار ارتباطی میان عامل‌های رله را در طرح پیشنهادی نشان می‌دهد. در این شکل هر عامل بر روی بستر مخابراتی بر روی استاندارد IEC-61850 ارتباط خود را با سایر عامل‌ها برقرار می‌سازد. بر اساس این استاندارد، استفاده از پروتکل GOOSE به‌منظور ارسال اطلاعات وضعیت هر عامل هوشمند، کمک می‌کند تا بتوان سیگنال‌های لازم را مابین عامل‌ها انتقال داد. سرعت تبادل این سیگنال‌ها کمتر از ۴ میلی‌ثانیه است و کمترین تأخیر را در میان سایر پروتکل‌های این استاندارد به‌همراه پروتکل مسدود کردن پیام سرور[1] (SMV) دارد. هر عامل دارای جدولی است که در آن اطلاعات مربوط به سایر عامل‌ها را نگهداری می‌کند.

هر عامل قبل از قرارگیری در شبکه طوری برنامه‌ریزی می‌شود که در آن بخشی از اطلاعات پیش‌نیاز شبکه به آن داده می‌شود و زمان اتصال بر روی شبکه، با استفاده از پروتکل TCP/IP پیامی را به‌صورت پخشی بر روی شبکه ارسال می‌کند. این پیام برای تمام گره‌های موجود در شبکه ارسال می‌شود و سایر عامل‌ها را از عضو جدید شبکه باخبر می‌سازد. با توجه به مکانیزم این پروتکل شرایطی مهیا می‌شود که به‌کمک آن می‌توان همواره از وضعیت سایر گره‌های عاملی باخبر شد و در صورتی که یک عامل دچار تغییر شود یا ارتباط خود بر روی بستر مخابراتی از دست بدهد، می‌تواند شرایط ارتباطی خود را تغییر دهد.

شکل ارتباط میان تجهیزات حفاظتی هوشمند این وضعیت را به‌خوبی نشان می‌دهد. در این شکل، چهار تجهیز حفاظتی IPD1، IPD2، IPD3 و IPD4 بر روی یک بستر مخابراتی با هم در ارتباط‌اند. این چهار تجهیز جدولی را تشکیل می‌دهند که در آن اطلاعات مربوط به حضور هریک را به‌همراه سایر اطلاعات شبکه

1. Server Message Block

نشان می‌دهد. این جدول در زمان حضور هریک از عامل‌ها در شبکه مابین یکدیگر به اشتراک گذاشته می‌شود و در آن مشخص می‌گردد که اطلاعات به‌دست‌آمده از هر گره در چه زمانی دریافت شده است. بر اساس این زمان مشخص می‌شود که عامل هوشمند مورد نظر در شبکه توانایی تبادل داده را داشته است یا خیر. در صورتی که این اطلاعات از عامل مورد نظر به‌روزرسانی نگردد، عامل مذکور به‌عنوان یک گره ازدست‌رفته شناخته می‌شود و عامل‌های همسایه آن را از جدول خود حذف می‌کنند.



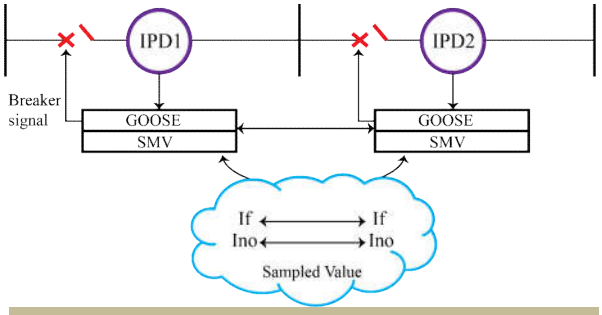
شکل (۲): ارتباط میان تجهیزات حفاظتی هوشمند

با توجه به این موضوع می‌توان شرایط بر هم خوردن ارتباط مخابراتی را نیز مدیریت کرد. به‌واسطهٔ استفاده از پیام‌های پخش همگانی یا به‌اصطلاح پخش پیام‌ها[1] کل شبکه را می‌توان در زمان کوتاه از وضعیت عامل‌های فعال شبکه مطلع کرد. این پیام‌ها در زمان ارسال به‌صورتی مدیریت می‌شوند که در صورت وقوع یک رویداد در شبکه یا از بین رفتن یک گره در حلقهٔ ارتباطی، توسط خود عامل یا توسط عامل‌های همسایه به سایر گره‌های شبکه فرستاده می‌شوند تا همهٔ گره‌ها متناسب با تغییر وضعیت پیش‌آمده، شرایط عملکرد خود را تغییر دهند.

ب. تبادل اطلاعات شبکه

معماری موجود بر روی استاندارد IEC-61850 این امکان را فراهم می‌کند تا بتوان بر اساس اطلاعاتی که نیازمند انتقال آن هستیم از دو پروتکل متفاوت استفاده شود. پروتکل GOOSE که به‌منظور ارسال سیگنال‌های وضعیت استفاده می‌شود، برای بررسی و ارسال وضعیت تجهیزات و کلید و یا ارسال شرایط گره‌ها در شبکه به کار گرفته می‌شود. این پروتکل متناسب با رویدادهای شبکه به ارسال سیگنال‌های صفر و یک در شبکه می‌پردازد و با توجه به واکنشی که هر بخش از دریافت سیگنال وضعیت می‌دهد، تصمیم‌گیری می‌کند.

پروتکل دیگری که برای برقراری ارتباط با تجهیزات هوشمند دیگر استفاده می‌شود، پروتکل SMV است. این پروتکل وظیفهٔ انتقال اطلاعات مربوط به جریان اندازه‌گیری‌شده را دارد. بر اساس این پروتکل، اطلاعات لحظه‌ای از جریان شبکه با دیگر گره‌های عاملی شبکه به اشتراک گذاشته می‌شود. شکل (۳) ارتباط میان دو تجهیز حفاظتی هوشمند را نشان می‌دهد که بر اساس دو پروتکل ذکرشده، در شبکه به انتقال داده می‌پردازند.



شکل (۳): تشکیل ارتباط میان تجهیزات هوشمند به‌منظور انتقال اطلاعات

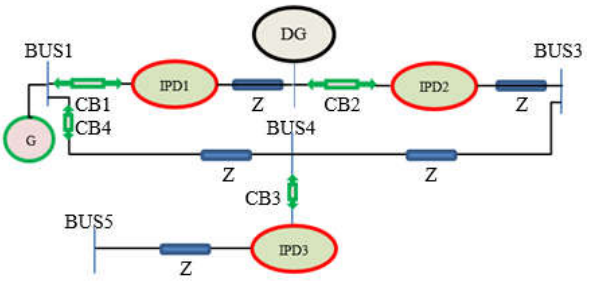
در این شکل وضعیت هر تجهیز به‌کمک ارسال و دریافت سیگنال وضعیت GOOSE مشخص می‌شود و در زمان مورد نظر نیز فرمان کلیدها به‌وسیلهٔ ارسال سیگنال قطع کلید انجام می‌گردد. اطلاعات مربوط به جریان‌های عبوری شبکه که وضعیت شرایط جاری شبکه بر اساس آن مشخص می‌شود، به‌وسیلهٔ پروتکل SMV شکل گرفته است. این اطلاعات با مقایسه با شرایط ابتدایی شبکه در تغییر وضعیت شبکه و همچنین تشخیص تغییرات جریان

1. Broadcast Messages

شبکه در حضور منابع تولید پراکنده بسیار مهم است. Ifmax و Ino مربوط به اطلاعات جریان خطا و جریان شرایط عادی شبکه هستند که برای مشخص شدن شرایط بهره‌برداری شبکه از آن‌ها استفاده می‌شود.

ج. مشخص کردن رویداد در شبکه بر روی رله‌ها

رویداد در شبکه شامل تغییر در ساختار شبکه یا وقوع تغییر در میزان خطای اتصال کوتاه شبکه است. تغییر ساختار شبکه می‌تواند شامل اضافه شدن تجهیزات حفاظتی جدید یا تغییر وضعیت کلیدهای خط باشد. میزان جریان خطای شبکه نیز تحت‌تأثیر مکان قرارگیری منابع تولید پراکنده و همچنین میزان سطح نفوذ این منابع می‌تواند دستخوش تغییر قرار گیرد. شکل (۴) به بررسی نحوهٔ تغییرات در شبکه می‌پردازد. در این شکل، کلید مانور S در ابتدا باز بوده و جریان شبکه از طریق مسیر IPD1 تغذیه می‌شود. اگر فرض شود در شرایط قبل از حضور منبع تولید پراکنده، میزان جریان عبوری از این رله برابر Ino1 باشد، در زمان وقوع خطا جریان if1 از آن عبور می‌کند. این اطلاعاتی است که یک تجهیز هوشمند در خود ذخیره می‌کند. در این شرایط برای IPD2 و IPD3 نیز این اطلاعات را برای خود ثبت می‌کنند.



شکل (۴): تشخیص رویداد بر روی حفاظت هوشمند

در این شرایط سیستم حفاظت شبکه به این صورت است که IPD2 پشتیبان عملکرد حفاظت IPD3 و IPD1 پشتیبان عملکرد IPD2 است. در این شرایط با توجه به ارتباط میان سه رله، اطلاعات جریان شبکه برای هر سه رله نشان از آن دارد که هر سه رله در حال حاضر جریان خطا را مشاهده کرده و ناحیه‌بندی حفاظتی آن‌ها تغییر نکرده است. در همین شرایط در صورت ورود منبع تولید پراکنده به شبکه، تغییر ایجادشده نشان از تغییر در مقادیر ثبت‌شده بر روی سیستم حفاظت هوشمند است که نشان‌دهندهٔ تغییر در سطح جریان اتصال کوتاه است. در شرایط دیگر فرض شود تا کلید S بسته و کلید CB1 باز گردد. در این شرایط حفاظت IPD1 دیگر جریانی را بر روی خود مشاهده نخواهد کرد. از طرف دیگر تغییری در میزان جریان Ino برای حفاظت‌های IPD2 و IPD3 اتفاق افتاده است.

در این شرایط ارتباط میان عامل‌های رله به‌صورت هوشمند تغییر کرده و سیستم حفاظت شبکه متوجه تغییر در وضعیت آرایش شبکه می‌شود. بنابراین با توجه به اینکه حفاظت IPD2 متوجه عدم مشاهدهٔ جریان توسط IPD1 می‌گردد، شرایط خود را به‌گونه‌ای فرض می‌کند که لازم است به‌جای حفاظت IPD1 ناحیهٔ حفاظتی آن را نیز پوشش دهد. پس لازم است پشتیبانی خود را با IPD4 حفظ کرده و حفاظت ناحیهٔ جدید را هم داشته باشد. بر این اساس می‌توان گفت که با توجه به تغییر اندازهٔ جریان شبکه و همچنین عدم مشاهدهٔ جریان توسط حفاظت IPD1 حفاظت‌های هوشمند متوجه تغییر شرایط شبکه و به‌دنبال آن تغییر ناحیهٔ حفاظتی خود می‌شوند. جدول (۲) این وضعیت را برای این شبکه در زمان تغییر ساختار شبکه نمایش می‌دهد.

جدول (۲): وضعیت ارتباطی در زمان تغییر ساختار

کلید S بسته و کلید CB1 باز	کلید S باز و کلید CB1 بسته
IPD2, IPD3	IPD1, IPD2, IPD3
{PD2:[if2,in2], PD3:[if3,in3]}	{PD1:[if1,in1], PD2:[if2,in2], PD3:[if3,in3]}

این جدول نشان‌دهندهٔ وضعیت تغییر سیستم حفاظتی به‌همراه جریان مشاهده‌شده توسط سیستم حفاظتی است. با توجه به اینکه این جدول میان عامل‌های هوشمند در شبکه تبادل می‌شود، با تغییرات ایجادشده در شبکه، این عامل‌های هوشمند هستند که به‌سرعت تغییرات شبکه را تشخیص می‌دهند. شرایط پیش‌آمده می‌تواند برای شرایطی که ارتباط مخابراتی به گره هوشمند به‌دلیل ایجاد مشکل بر روی سخت‌افزار یک تجهیز حفاظتی اتفاق می‌افتد، نیز قابل بسط باشد. در این شرایط همان طور که در بخش قبلی نیز توضیح داده شد، در صورت بروز مشکل بر روی گره هوشمند، پیام‌های پخشی به‌منظور آگاه کردن سایر گره‌های متصل به نقطهٔ آسیب‌دیده در شبکه انتشار داده می‌شوند.

د. محاسبهٔ تنظیمات جدید بر روی رلهٔ پشتیبان

در انتهای بحث انجام‌گرفته پس از مشخص شدن ساختار ارتباطی و اطلاعات اشتراک گذاشته‌شده میان تجهیزات حفاظتی هوشمند و آگاه شدن از شرایط وقوع رویداد در شبکه، لازم است تا حفاظت پشتیبان بتواند الگوی عملکرد خود را تغییر دهد. بر این اساس عامل‌های هوشمند با توجه به اطلاعات ابتدایی شبکه و اطلاعات شرایط بهره‌برداری شبکه به تغییر در پارامترهای خود اقدام می‌کنند. تجهیز هوشمند در شرایط ابتدایی شبکه و قبل از

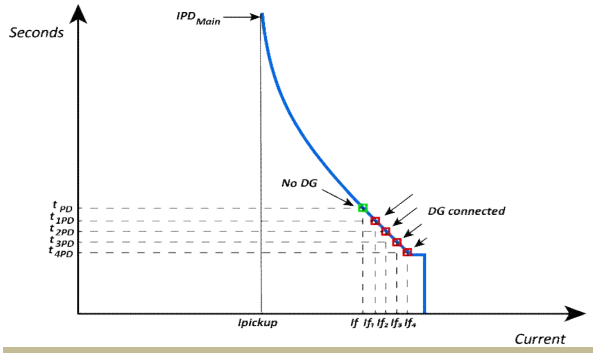
وقوع تغییرات در آن اطلاعات جریانی شبکه را دریافت کرده و در خود ذخیره می‌کند. این اطلاعات شامل میزان جریانی است که در شرایط عملکرد نرمال، بر روی خود و همچنین میزان جریان خطایی است که در ناحیهٔ اصلی و ناحیه مربوط به حفاظت پایین‌دست خود مشاهده می‌کنند. عامل‌های هوشمند در هر لحظه با تغییر در جریان خود به سایر عامل‌های همسایه تغییرات را گزارش می‌کنند. رله‌های اضافه جریان از نوع زمان معکوس با توجه به میزان جریان عبوری، بر اساس تنظیمات موجود بر روی آن‌ها قادر خواهند بود تا در صورت عبور جریانی به‌اندازهٔ آستانهٔ جریان تحریک آن‌ها، کلید خود را در زمان مشخصی باز نمایند. این زمان که زمان عملکرد رله است، از رابطهٔ زیر محاسبه می‌شود:

$$t_{PD} = [\frac{A}{m^{P}-1}] * TMS \qquad (۱)$$

که در آن I جریان خطا، m نسبت جریان خطا به جریان تحریک رله است، ضریب تنظیم زمانی[1] (TMS) تنظیم زمانی رله و A و p بر اساس نوع مشخصهٔ شکل‌موج رله انتخاب می‌شود. بر اساس این رابطه لازم است تابع عملکردی در لحظهٔ آگاه شدن از تغییر جریان شبکه، مقادیر پارامترهای رله را طوری تنظیم کند که هماهنگی با سایر عامل‌های شبکه برقرار شود. زمانی که قرار باشد تا دو رله هماهنگی حفاظتی خود را حفظ کنند، لازم است تا حاشیهٔ هماهنگی میان آن‌ها حفظ شود. برای دو حفاظت اصلی- پشتیبان لازم است تا رابطهٔ زیر برقرار باشد:

$$t_{PD1} - t_{PD2} > 0.3(s) \qquad (۲)$$

منظور از هماهنگی در بحث حفاظت اضافه جریان، تعیین مقادیر بهینهٔ ضریب تنظیم جریان و ضریب تنظیم زمان رله‌های اضافه جریان جهت‌دار است. این کار با هدف کاهش زمان عملکرد رله و با توجه به محدودیت‌های مختلف مانند قیود هماهنگی رله، قیود ساختمانی رله، قیود تغییر ساختار شبکه و... انجام می‌پذیرد. اما ساختار شبکه به‌دلیل تغییر شرایط بهره‌برداری، خروج خطوط، ترانسفورماتورها و واحدهای تولید دائماً در حال تغییر است. این عدم قطعیت باعث ناهماهنگی رله‌های اضافه جریان می‌شود. این مشکل با اضافه کردن قیود ساختارهای متفاوت شبکه در فرمول‌بندی مسئله، تا حد زیادی قابل قبول است که پیچیدگی مسئلهٔ هماهنگی را نسبت به حالت ساختار ثابت دوچندان می‌کند. در مورد زمان عملکرد رله‌های اصلی و پشتیبان، با توجه به تحت‌تأثیر قرار گرفتن جریان اتصال کوتاه در شرایط حضور منبع تولید پراکنده، می‌توان این نکته را ذکر کرد که همواره زمان عملکرد حفاظت اصلی شبکه در حال کاهش است. برای مثال شکل (۵) زمان عملکرد حفاظت اصلی شبکه را برای خطای ایجادشده در شرایط عدم حضور منبع تولید پراکنده و در زمان حضور آن نشان می‌دهد. همان طور که در شکل مشخص است، در حضور منبع تولید پراکنده، میزان جریان رلهٔ اصلی افزایش یافته و از طرفی T_{PD} مربوط به رلهٔ اصلی کم شده است. البته در طراحی این ساختار هوشمند این نکته در نظر گرفته شده است که حفاظت هوشمند پشتیبان، این مسئله را در نظر دارد و اقدام به تغییر تنظیمات خود می‌کند. با توجه به در نظر گرفتن شرایطی برای رلهٔ پشتیبان و دریافت اطلاعات رلهٔ اصلی در شرایط تغییر در تنظیمات رلهٔ اصلی، باید مسئلهٔ فوق صورت پذیرد. شرایط لازم برای رلهٔ پشتیبان به دو قسمت تقسیم می‌شود: شرایط تغییر جریان تحریک رله و شرایط تغییر میزان TMS.



شکل (۵): تغییر جریان در حضور منبع تولید پراکنده

با توجه به رابطهٔ (۳) مشخص است که رابطهٔ زیر لازم بوده تا جریان تحریک رله همواره برقرار گردد:

$$2 \times I_{load} < Ipickup < 0.5 \times I_{f\ min} \qquad (۳)$$

بنابراین در هر لحظه لازم است تا شرایط زیر برای جریان تحریک رله فراهم باشد، در غیر این صورت ممکن است رله حداقل جریان خطا را مشاهده نکند یا جریان اضافه‌بار را به‌اشتباه جریان خطا تشخیص دهد. حفاظت هر ناحیه وظیفه دارد تا خطای ناحیهٔ خود را نیز در زمان مناسب پوشش دهد؛ به‌بیان دیگر همان طور که لازم است تنظیمات حفاظت پشتیبان برای هماهنگی با رلهٔ اصلی انتخاب شود، لازم است این تنظیمات به‌گونه‌ای باشند که در صورت وقوع خطا در ناحیهٔ اصلی رلهٔ پشتیبان نیز به‌موقع قطع گردند. به‌منظور حفظ هماهنگی و عملکرد مناسب هر رله، دو پارامتر TMS و جریان پیکاپ[2] قابل تغییر و سایر پارامترها ثابت در نظر گرفته می‌شوند. پس با تغییر مناسب این دو پارامتر می‌توان

1. Time Multiplier Setting

2. Pickup

زمان عملکرد رله را به‌شکل مطلوب تغییر داد. هدف از عملکرد مطلوب هر رله به این صورت بیان می‌شود که در هر لحظه اختلاف زمان عملکرد رله و رلهٔ پشتیبان باید مقدار ثابتی باشد. این مقدار ثابت حدود ۰/۳ ثانیه در نظر گرفته می‌شود. متفاوت بودن این مقدار به این معنی است که هماهنگی سیستم حفاظتی دچار اختلال شده و رله عملکرد مطلوبی ندارد. حال باید زمان عملکرد رله را به‌وسیلهٔ دو پارامتر قابل تغییر آن به حالت مطلوب رساند. برای این منظور با طراحی یک تابع مناسب برای کنترل زمان عملکرد رله مشکل ناهماهنگی سیستم حفاظتی برطرف می‌شود. پس در هر لحظه با بررسی اختلاف زمان عملکرد رلهٔ پشتیبان و رلهٔ اصلی، ثابت بودن یا ثابت نبودن این اختلاف مشخص می‌شود. در صورت ثابت نبودن این مقدار، اختلاف زمانی به‌دست‌آمده از اختلاف زمانی ایدئال کم می‌شود و بدین ترتیب خطا[1] (error) محاسبه می‌شود. حال تابع طراحی شده وظیفه دارد تا خطای محاسبه‌شده را صفر نگه دارد. این تابع با استفاده از تغییر دو متغیر TMS و جریان پیکاپ سعی بر صفر نگه داشتن خطا دارد. اما باید به این نکته توجه داشت که جریان پیکاپ باید شرط موجود در رابطهٔ (۳) را رعایت کند. الگوریتم پیشنهادی به‌صورت زیر است:

Change Setting Method
1: Input: IPD_i for i = 1, …, n
2: All information is collected
3: if Fault then
4: if miscoordination then
5: Assuming that Ipcikup is fixed, TMS will be calculated
6: if TMS doesn't complies with the appropriate condition then
7: Ipickup is required to change the condition of (3)
8: else
9: pass

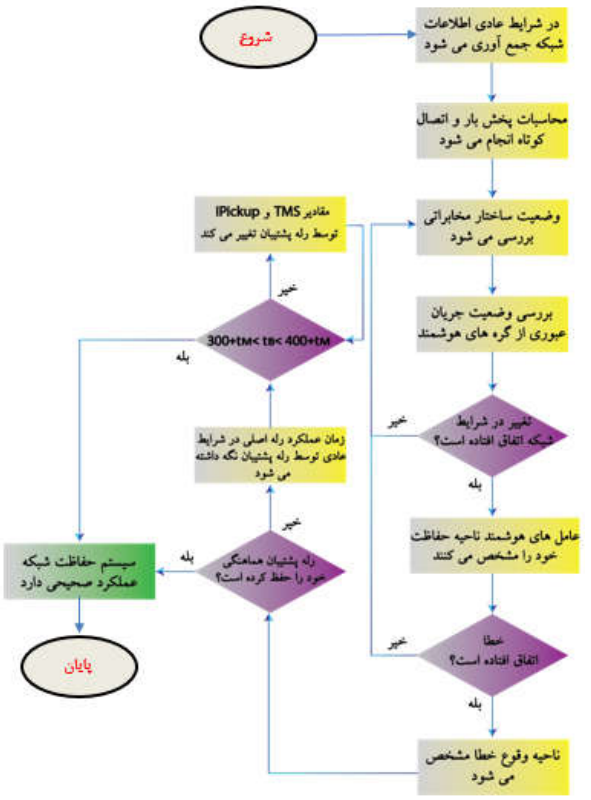
میزان شرایط مجاز برای تغییرات TMS در استاندارد IEC به‌صورت زیر است:

$$0.05 \le TMS \le 3.2 \qquad (۴)$$

در این مقاله با حذف رله‌های اضافه جریان و جایگزین کردن IED، هریک از این دستگاه‌های الکترونیکی هوشمند می‌توانند وظایف رله‌های اضافه جریان را به‌خوبی انجام دهند و از طرفی هر دستگاه الکترونیکی هوشمند دارای یک تابع کنترل‌کننده است که این عمل به پیاده‌سازی کنترل‌کنندهٔ توزیعی کمک می‌کند و کنترل‌کنندهٔ مرکزی حذف می‌شود. بنابراین با پیاده‌سازی کنترل‌کننده به‌صورت توزیعی، نیاز سیستم حفاظتی به کنترل‌کنندهٔ بزرگ و قدرتمند مرکزی برطرف می‌شود. با پیاده‌سازی کنترل‌کنندهٔ توزیع‌شده به‌جای کنترل‌کنندهٔ مرکزی سیستم حفاظتی عملکردی مطمئن‌تر و سریع‌تر دارد. از طرفی با در نظر گرفتن هریک از این دستگاه‌های الکترونیکی هوشمند به‌عنوان یک عامل، بستر سیستم چندعاملی مهیا می‌شود و با پیاده‌سازی استاندارد IEC-61850، بستر مخابراتی مناسب برای انتقال داده بین عامل‌های سیستم چندعاملی فراهم شده و سیستم حفاظتی به‌طور هماهنگ و کنترل‌شده به شناسایی و رفع خطاهای موجود در شبکه می‌پردازد.

۴. الگوریتم روش پیشنهادی

طرح‌وارهٔ روش پیشنهادی در شکل (۶) نشان داده شده است. الگوریتم طراحی‌شده به‌منظور بازگردانی هماهنگی حفاظتی به‌کمک استفاده از عامل‌های هوشمند شبکه به‌صورت زیر است:



شکل (۶): تشخیص رویداد بر روی حفاظت هوشمند

گام اول: در ابتدا لازم است تا اطلاعات شبکه جمع‌آوری شده و میزان جریان در شرایط طبیعی و جریان بار شبکه مشخص گردد.

گام دوم: محاسبات پخش بار و اتصال کوتاه شبکهٔ مورد بهره‌برداری محاسبه شده و بر اساس آن میزان جریان *Ifmax* و *Ifmin* شبکه مشخص می‌گردد.

1. Error

گام سوم: با توجه به اطلاعات جمع‌آوری‌شده از شبکه، بر اساس نحوهٔ ارتباط‌گیری سیستم حفاظت هوشمند شبکه، گره‌های عاملی فعال در شبکه مشخص می‌شوند.

گام چهارم: با توجه به محاسبات پخش بار و اتصال کوتاه شبکه، شرایط بهره‌برداری شبکه با اطلاعات وضعیت ابتدایی شبکه مقایسه می‌شود.

گام پنجم: در این مرحله بر اساس اطلاعات به‌دست‌آمده از گام سوم و چهارم مشخص می‌گردد که آیا تغییری در وضعیت شبکه اتفاق افتاده است یا خیر.

گام ششم: در این مرحله در صورتی که تغییری در شبکه رخ داده باشد، سیستم حفاظت هوشمند با توجه به نقاطی که با آن‌ها در ارتباط بوده است و هم‌اکنون آن‌ها را در شرایطی خارج از وضعیت قبلی مشاهده می‌کند، ناحیهٔ حفاظت خود را مشخص می‌کند.

گام هفتم: پس از مشخص شدن تغییرات شبکه در صورتی که خطایی در شبکه رخ دهد، لازم است تا ناحیهٔ وقوع خطا مشخص شود. این مسئله با توجه به مشخص شدن ناحیهٔ حفاظتی هر تجهیز حفاظتی هوشمند، به‌واسطهٔ مقایسهٔ جریان عبوری از سیستم حفاظت شبکه و مقایسهٔ آن با پارامترهای ابتدای شبکه و اطلاعاتی که از عامل همسایهٔ خود قبل از شرایط خطا ثبت کرده است مشخص می‌شود.

گام هشتم: در مرحلهٔ بعد لازم است هماهنگی میان عامل اصلی و پشتیبان بررسی شود. در این شرایط عامل پشتیبان با توجه به اینکه با دانش به‌دست‌آورده از شبکه تشخیص می‌دهد که میزان جریان رلهٔ اصلی همواره در حال افزایش بوده است، هماهنگی خود را با زمانی در شرایط جدید مقایسه می‌کند. در صورتی که این میزان در شرایط بازه زمانی استاندارد قرار داشته باشد، هماهنگی دو رله حفظ شده است.

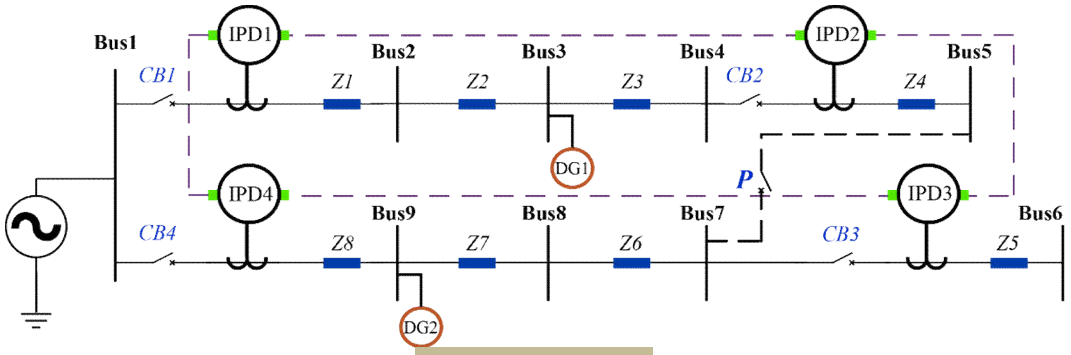
گام نهم: با توجه به اینکه شرایط زمان عملکرد رلهٔ اصلی در شرایط قبل از وقوع خطا به همسایگان گزارش شده است، رلهٔ پشتیبان وظیفه دارد تا تنظیمات عملکردی خود را در شرایط جدیدی قرار دهد. این شرایط جدید لازم است تا در بازهٔ زمانی استانداردی که برای شبکهٔ توزیع در نظر گرفته شده، بررسی گردد. با توجه به مرجع [۳۳] و [۳۴] برای رلهٔ پشتیبان لازم است تا شرایط زمانی عملکرد در محدودهٔ رابطهٔ (۵) تعریف شود:

$$0.3(s)+tPD2P<t_{PD1}<0.4(s)+t_{PD2} \qquad (۵)$$

گام دهم: در این مرحله تجهیز هوشمند با استفاده از برنامه‌ریزی صورت‌گرفته روی آن و با رعایت حدود تغییرات مجاز برای میزان جریان *Ipickup* و *TMS* تنظیمات خود را اصلاح می‌کند و در زمانی که تنظیم مناسب بتواند شرط رابطهٔ (۴) را مهیا سازد، خطا در زمان مناسب توسط رلهٔ پشتیبان برطرف می‌شود.

۵. نتایج شبیه‌سازی و بحث

برای ارزیابی و بررسی صحت عملکرد روش پیشنهادی با استفاده از نرم‌افزار ETAP، شبکهٔ آزمایشی مطابق شکل (۷) در نظر گرفته می‌شود. ساختار شبکهٔ پیاده‌سازی‌شده به‌صورتی است که دو فیدر خروجی از باس شمارهٔ یک همواره از هم مستقل‌اند و در صورت مانور کلید P این فیدر به یکدیگر متصل شده و یکی از کلیدهای ابتدای خط یعنی CB1 یا CB4 باز می‌گردد؛ به‌عبارت دیگر در ساختار سیستم فوق همواره امکان حلقوی شدن شبکه وجود نخواهد داشت. این شبکه در شرایط عدم حضور منابع تولید پراکنده طراحی شده است. در این قسمت طرح پیشنهادی در قالب وضعیت بهره‌برداری مختلف شبکه و در شرایط مختلف خطا و حضور منابع تولید پراکنده در نواحی مختلف بررسی می‌شود.

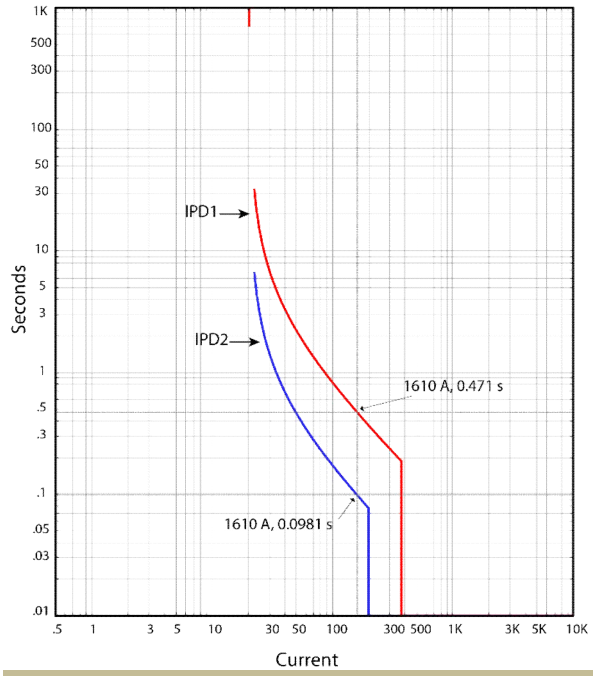


شکل (۷): شبکهٔ مورد مطالعه

ساختار مخابراتی عامل‌ها در این طرح مربوط به ارتباط میان عامل‌های رله در سطح اول سیستم چندعاملی است. این شبکه در طرح حفاظت لایهٔ اول خود متشکل از چهار عامل رله بوده که دو حفاظت IPD1 و IPD2 بر روی فیدر اول و دو حفاظت IPD3 و IPD4 بر روی فیدر دوم قرار گرفته است و به‌صورت نقطه‌به‌نقطه با یکدیگر ارتباط دارند. همچنین منابع تولیدی DG1 با ظرفیت ۱۰ مگاوات و DG2 با ظرفیت ۱۰ مگاوات می‌توانند به شبکه متصل شوند. برای حفاظت‌های IPD1 و IPD2 قبل از مانور کلید P، میزان جریان طبیعی که در شبکه مشاهده می‌شود به‌ترتیب برابر ۵۰ و ۳۰ آمپر است. برای این دو رله حداقل جریان خطا برابر ۴۰۳ آمپر و بیشترین جریان خطا برابر ۱۶۰۰ آمپر است. این دو حفاظت به‌منظور قرارگیری در شرایط پشتیبان یکدیگر تنظیماتی به‌صورت جدول (۳) دارا هستند.

جدول (۳): تنظیمات حفاظتی IPD1 و IPD2

IPD NUMBER	SETTINGS
IPD1	TMS=0.24, IPICKUP=204
IPD2	TMS=0.05, IPICKUP=204



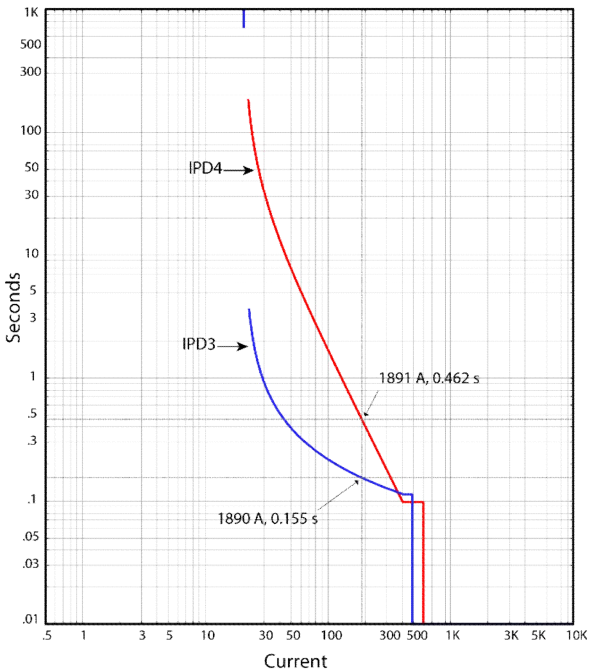
شکل (۸): شرایط هماهنگی میان حفاظت‌های IPD1 و IPD2 در زمان باز بودن کلید P

این دو حفاظت با تنظیمات موجود در جدول فوق با یکدیگر برای میزان جریان ۱۶۰۰ آمپر هماهنگ است که در شکل (۸) این هماهنگی نشان داده شده است. همان طور که دیده می‌شود حفاظت IPD1 جریان خطا را در زمان ۴۷۱ میلی‌ثانیه برطرف کرده و حفاظت IPD2 همین جریان خطا را در زمان ۹۸ میلی‌ثانیه برطرف می‌سازد. بنابراین با توجه به زمان عملکرد این دو رله، حاشیهٔ هماهنگی میان آن‌ها برقرار است. برای حفاظت‌های IPD3 و IPD4 جریان عبوری از آن‌ها در شرایط طبیعی شبکه برابر ۳۵ و ۴۳ آمپر است. در این شرایط میزان حداقل جریان خطای عبوری از این دو حفاظت برابر ۳۹۰ آمپر و بیشترین جریان خطا برابر ۱۸۹۰ آمپر است. تنظیمات مربوط به این دو حفاظت در جدول (۴) آمده است.

جدول (۴): تنظیمات حفاظتی IPD3 و IPD4

IPD NUMBER	SETTINGS
IPD3	TMS=0.05, IPICKUP=207
IPD4	TMS=0.49, IPICKUP=204

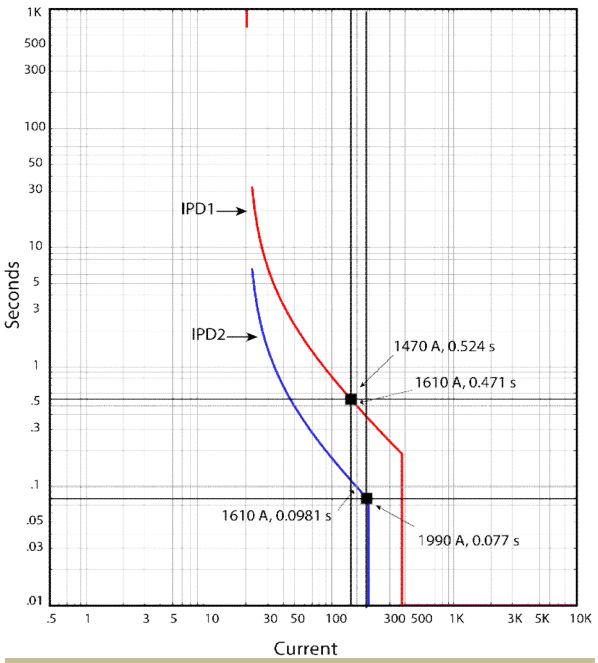
شکل (۹) هماهنگی ایجادشده میان این دو حفاظت را در زمان وقوع خطا نشان می‌دهد. همان طور که دیده می‌شود، با توجه به زمان عملکرد ۴۶۴ و ۱۵۵ میلی‌ثانیه حفاظت‌های پشتیبان و اصلی، هماهنگی میان آن‌ها برقرار است. این تنظیمات ابتدایی شبکه بوده‌اند که حفاظت‌های شبکه برای رویداد در آن شرایط با هم هماهنگ بوده و در صورت مانور شبکه ساختار سیستم حفاظت شبکه نیز تغییر می‌کند و در این شرایط لازم است تا نواحی حفاظتی تغییر کند و حفاظت‌های اصلی و پشتیبان نیز موقعیت یکدیگر را شناسایی نمایند.



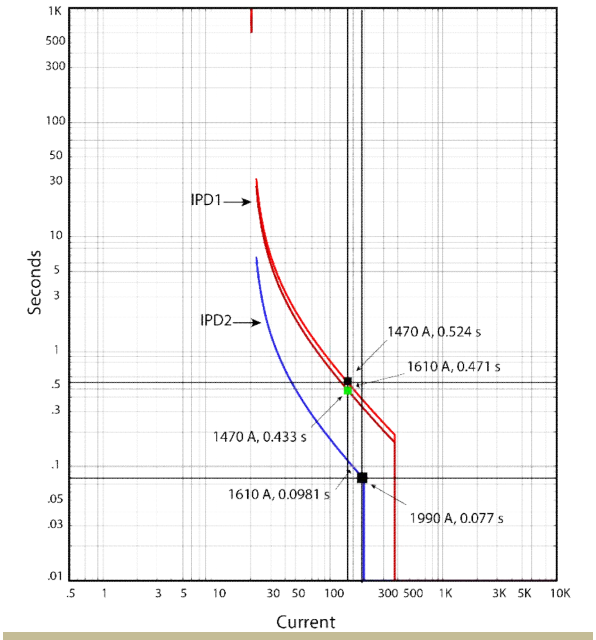
شکل (۹): شرایط هماهنگی میان حفاظت‌های IPD3 و IPD4 در زمان باز بودن کلید P

در شرایط جدید فرض می‌شود در این زمان منبع تولید پراکنده DG1 به شبکه متصل گردد. در این حالت میزان جریان عبوری از حفاظت‌های IPD1 و IPD2 به‌ترتیب برابر ۱۴۵ و ۲۲ آمپر می‌شود. حفاظت‌های هوشمند این تغییرات را احساس کرده و متوجه ایجاد تغییر در شبکه می‌شوند، اما با توجه به اینکه همچنان هر دوی آن‌ها جریان را مشاهده می‌کنند، شرایط را تغییر ساختار شبکه قلمداد نخواهند کرد. در این حالت اگر خطایی در ناحیهٔ اصلی حفاظت IPD2 اتفاق افتد، این حفاظت جریان ۱۹۹۰ آمپر را بر روی خود مشاهده می‌کند که نسبت به شرایط قبلی افزایش یافته است. برای حفاظت IPD1 این جریان خطا برابر ۱۴۷۰ آمپر است. در این شرایط زمان عملکرد حفاظت‌ها تغییر می‌کند و زمان‌های عملکرد حفاظت‌های اصلی و پشتیبان به‌ترتیب برابر ۷۷ و ۵۲۴ میلی‌ثانیه می‌شود.

شکل (۱۰) از دست رفتن این هماهنگی را نمایش می‌دهد. با توجه به اینکه هماهنگی میان این دو رله از دست رفته است، سیستم حفاظت هوشمند، قصد دارد تا تنظیمات حفاظت پشتیبان را تغییر دهد. در این شرایط حفاظت هوشمند با در نظر داشتن اینکه جریان رلهٔ اصلی افزایش یافته و میزان زمان عملکرد آن کاهش یافته است، سعی دارد تا زمان عملکرد خود را با توجه به زمان عملکرد حفاظت اصلی، به آن نزدیک کند.



شکل (۱۰): شرایط از دست رفتن هماهنگی میان حفاظت‌های IPD1 و IPD2 در زمان باز بودن کلید P



شکل (۱۱): بازیابی هماهنگی میان حفاظت‌های IPD1 و IPD2 در زمان باز بودن کلید P

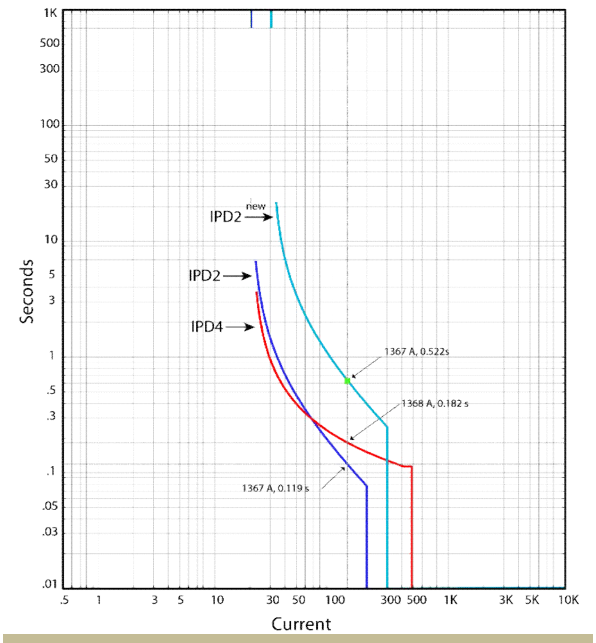
شکل (۱۱) تغییر تنظیمات مربوط به حفاظت پشتیبان را نشان می‌دهد. جدول (۵) تنظیمات جدید را برای حفاظت پشتیبان نمایش می‌دهد. با توجه به اینکه شرایط شبکهٔ توپولوژی شبکه تغییر نکرده و میزان جریانی که موجب بر هم خوردن هماهنگی شده است چندان قابل توجه نبوده، تنها با تنظیم میزان TMS مشکل مربوط به سیستم حفاظتی حل شده است. در شرایط جدید فرض می‌شود که کلید P بسته و کلید CB4 باز گردد. در این شرایط حفاظت‌های هوشمند شبکه در ابتدا تغییراتی را بر روی میزان جریان خود احساس می‌کنند. جریان بار عبوری از حفاظت‌ها به‌ترتیب برابر ۱۰۵، ۶۵، ۳۶ و صفر آمپر است.

جدول (۵): تغییر تنظیمات حفاظتی IPD1

IPD NUMBER	SETTINGS
IPD1	TMS=0.20, IPICKUP=204
IPD2	TMS=0.05, IPICKUP=204

این اطلاعاتی است که رله‌ها بر روی بستر مخابراتی برای یکدیگر ارسال می‌کنند. در این شرایط حفاظت IPD4 که جریانی را بر روی خود مشاهده نمی‌کند، پیامی را مخابره می‌کند که در آن برای سایر گره‌ها (عاملی همسایه)، حاکی از تغییر در ساختار شبکه است. علت آن‌هم مشاهده نکردن جریان توسط این حفاظت و مشاهده نکردن جریان خطا توسط سایر حفاظت‌هاست. در این حالت حفاظت‌های شبکه با اجتناب به این مسئله، درمی‌یابند که لازم است شرایط ارتباطی و حفاظتی جدیدی را برای خود انتخاب کنند. در این حالت با توجه به اینکه حفاظت IPD4 در ارتباط با حفاظت IPD3

بوده و به‌عنوان پشتیبان آن عمل می‌کند، لازم است تا پشتیبان جدیدی برای آن انتخاب گردد. سیستم حفاظت هوشمند شبکه بر اساس ارتباط و جدول اطلاعات که دربردارندهٔ اطلاعات سایر گره‌های عاملی است، حفاظت IPD2 را به‌عنوان پشتیبان جدید برای IPD3 و همچنین حفاظت از ناحیهٔ جدید اضافه‌شده به ناحیهٔ حفاظت IPD2 را مشخص می‌کند. در شرایط جدید اگر خطایی در ناحیهٔ حفاظت IPD3 اتفاق افتد، میزان جریان خطای عبوری از حفاظت IPD3 برابر ۱۳۷۰ آمپر است. همین میزان جریان خطا از حفاظت IPD2 نیز عبور می‌کند. در این شرایط زمان عملکرد حفاظت IPD3 برابر ۱۸۲ میلی‌ثانیه و زمان عملکرد IPD2 برابر ۱۱۸ میلی‌ثانیه است. با توجه به زمان عملکرد IPD2 کاملاً مشخص است که این حفاظت به‌اشتباه عمل کرده است. شکل (۱۲) اشتباه عملکرد حفاظت IPD2 را نشان می‌دهد. در این شرایط با توجه به اینکه هر دو رله یک جریان خطا را مشاهده می‌کنند، سیستم حفاظت هوشمند با در نظر داشتن اینکه حفاظت پشتیبان برای IPD3 تغییر کرده و ساختار شبکه عوض شده است، و نیز متناسب با شرایط اتصال کوتاهی که از قبل برنامه‌ریزی شده و آن‌ها را در اختیار دارد، تنظیمات مورد نیاز خود را اصلاح می‌کند. با توجه به منحنی مشخصهٔ جدید حفاظت IPD2 مشخص است که این حفاظت جریان خطا را در زمان ۵۲۲ میلی‌ثانیه برطرف ساخته و این نشان‌دهندهٔ هماهنگی برقرارشده میان حفاظت اصلی و پشتیبان است. جدول (۶) تغییرات تنظیمات مربوط به حفاظت IPD2 را نشان می‌دهد.



شکل (۱۲): عملکرد اشتباه حفاظت IPD2 در زمان بسته بودن کلید P و باز بودن کلید CB4

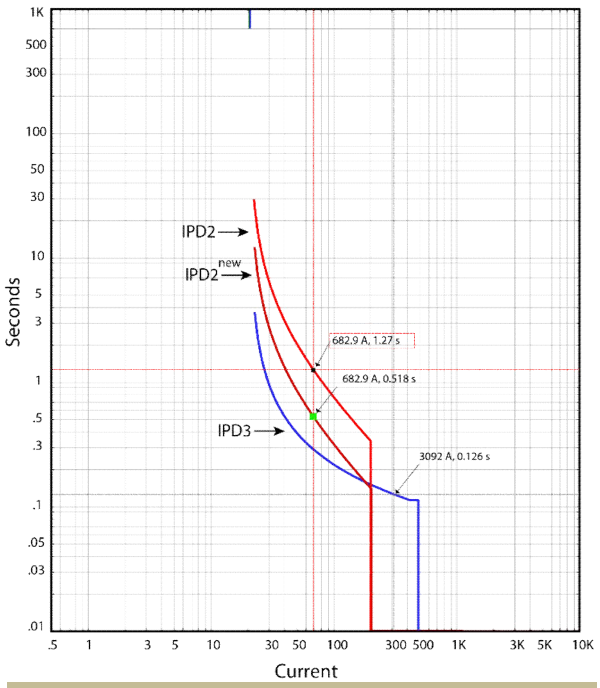
جدول (۶): تغییر تنظیمات حفاظتی IPD2 و باز بودن کلید CB4

IPD NUMBER	SETTINGS
IPD2	TMS=0.22, IPICKUP=202
IPD3	TMS=0.05, IPICKUP=204

در این قسمت فرض می‌شود که شرایط آرایش شبکه به‌گونهٔ دیگری تغییر کند. این بار فرض می‌شود CB1 باز شده و جریان عبوری از روی حفاظت IPD4 در شبکه جاری گردد. در این شرایط منبع تولید پراکندهٔ DG2 نیز به شبکه متصل می‌شود. میزان جریان عبوری از سیستم حفاظت شبکه به‌ترتیب برابر ۰، ۱۴۷، ۴۰، ۴۷۷ آمپر است. در این شرایط با توجه به اینکه حفاظت IPD1 جریانی عبوری را مشاهده نمی‌کند، پیغام پخشی را در شبکه انتشار داده تا سایر گره‌های عاملی دیگر از آن باخبر گردند. با توجه به این شرایط گره‌های عاملی جدول اطلاعات خود را به‌روزرسانی کرده و ارتباط خود را با حفاظت IPD1 تغییر داده و ناحیهٔ حفاظت جدید خود را مشخص می‌کنند. در این شرایط با آگاه شدن حفاظت IPD2 از خارج شدن IPD1، این حفاظت ناحیهٔ عملکرد خود را تغییر داده و وظیفه دارد تا حفاظت ناحیهٔ IPD1 را نیز پوشش دهد. در این شرایط فرض می‌شود خطایی در ناحیهٔ اصلی حفاظت IPD3 اتفاق افتد. حفاظت IPD3 وظیفه دارد تا این خطا را با توجه به وقوع آن در ناحیهٔ اصلی خود، سریع‌تر از سایر حفاظت‌ها عمل نماید. جریان خطای مشاهده‌شده بر روی این حفاظت برابر ۳۰۹۰ آمپر است که در زمان ۱۲۶ میلی‌ثانیه برطرف می‌شود. در این شرایط این جریان خطا را هر دو حفاظت IPD2 و IPD4 نیز بر روی خود مشاهده می‌کنند. پس لازم است تا در صورت عدم عملکرد حفاظت IPD3 این دو حفاظت با حاشیهٔ هماهنگ مناسبی خطا را برطرف سازند. شکل (۱۳) عملکرد حفاظت IPD2 را در زمان وقوع خطا نشان می‌دهد. همان طور که دیده می‌شود، این حفاظت جریان خطای ۶۸۳ آمپر را مشاهده کرده و در زمان ۱۲۷۰ میلی‌ثانیه عمل می‌کند که البته زمان زیادی برای باقی ماندن خطا بر روی شبکه است. در این شرایط، هماهنگی میان دو حفاظت اصلی و پشتیبان برقرار نیست و رلهٔ پشتیبان با تغییر مناسب میزان TMS خود هماهنگی حفاظت را بازمی‌گرداند. جدول (۷) تنظیم جدید حفاظت IPD2 را نشان می‌دهد.

جدول (۷): تغییر تنظیمات حفاظتی IPD2 در زمان بسته بودن کلید P و باز بودن کلید CB1

IPD NUMBER	SETTINGS
IPD2	TMS=0.09, IPICKUP=204
IPD3	TMS=0.05, IPICKUP=207

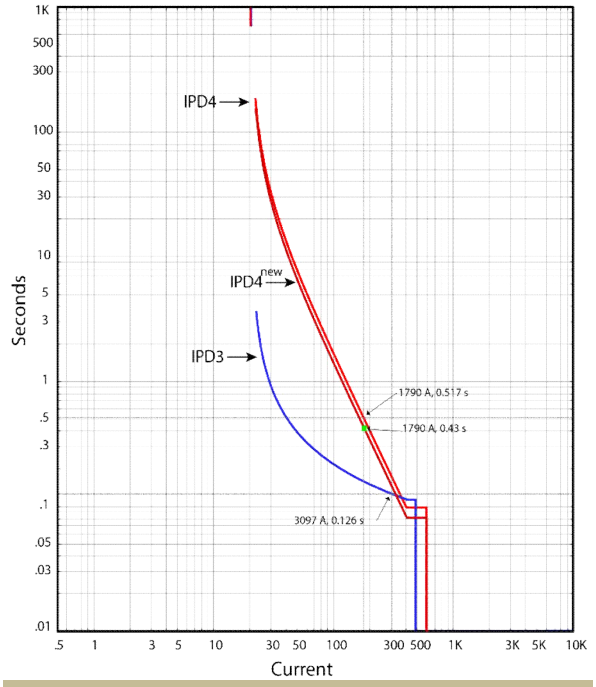


شکل (۱۳): بازیابی هماهنگی حفاظتی حفاظت IPD2 در زمان بسته بودن کلید P و باز بودن کلید CB1

اما برای حفاظت IPD4 شرایط دیگری برقرار است. جریان خطای عبوری از این حفاظت برابر ۱۷۹۰ آمپر بوده و این خطا را در زمان ۵۱۷ میلی‌ثانیه برطرف می‌سازد. با توجه به اینکه زمان عملکرد حفاظت IPD3 برابر ۱۲۶ میلی‌ثانیه است، هماهنگی میان دو حفاظت برقرار نیست و لازم است تا حفاظت IPD4 تنظیمات خود را تغییر دهد. شکل (۱۴) از دست رفتن هماهنگی و بازیابی آن را برای دو حفاظت اصلی و پشتیبان نشان می‌دهد. همان طور که دیده می‌شود حفاظت IPD4 در شرایط جدید، خطا را در زمان ۴۳۰ میلی‌ثانیه برطرف می‌سازد که نشان‌دهندهٔ بازیابی هماهنگی حفاظتی است. جدول (۸) تنظیمات جدید این حفاظت را نشان می‌دهد.

جدول (۸): تغییر تنظیمات حفاظتی IPD4 در زمان بسته بودن کلید P و باز بودن کلید CB1

IPD NUMBER	SETTINGS
IPD4	TMS=0.41, IPICKUP=200
IPD3	TMS=0.05, IPICKUP=207



شکل (۱۴): بازیابی هماهنگی حفاظتی حفاظت IPD4 در زمان بسته بودن کلید P و باز بودن کلید CB1

۶. نتیجه‌گیری

در روش پیشنهادی در این مقاله از ساختار سیستم‌های چندعاملی برای مدیریت شبکه و پیاده‌سازی ساختار حفاظتی با قابلیت اطمینان بالا استفاده شده است. با توجه به مشکلات موجود بر روی ساختار سیستم‌های چندعاملی، روش پیشنهادی با ارائهٔ راه‌حل جدیدی در به‌روزرسانی تنظیمات سیستم حفاظتی و همچنین آگاهی از تغییرات ساختار شبکه، سعی دارد تا یک طرح حفاظتی با قابلیت‌های کارآمدتری را در ساختار سیستم چندعاملی پیاده‌سازی کند. شرایط به‌صورتی برنامه‌ریزی می‌شود که در آن عملکرد هر رله در شرایط قرار گرفتن در حالت پشتیبان بهبود یابد. این طرح به جمع‌آوری اطلاعات شبکه وابسته نیست و از میزان تهدیدات موجود بر روی ساختار سلسله‌مراتبی و نیز از هزینه‌های پیاده‌سازی آن کاسته می‌شود. همچنین با توجه به پیاده‌سازی ساختار به‌صورت محلی، نیازی به حضور یک سیستم مرکزی وجود نخواهد داشت.

برای رفع محدودیت‌های ذکرشده در ساختار سیستم چندعاملی، لازم است میزان اطلاعات انتقال‌یافته در سطح شبکه کاهش یابد. به‌منظور کاهش این حجم از اطلاعات باید سطوح کنترلی سیستم چندعاملی را به‌نحوی تغییر داد که در انتقال اطلاعات ضروری و نیز در انجام تغییرات مربوط به تنظیمات تجهیزات حفاظتی، اختلالی ایجاد نشود. در حقیقت اگر ساختار

سیستم چندعاملی به‌نحوی بازسازی شود که دیگر نیازی به تصمیم‌گیری در واحد مرکزی پردازش اطلاعات نباشد، به‌طور طبیعی نیازی به عامل‌های لایهٔ دوم یا همان سرشاخه‌ها نخواهد بود. همچنین برای حداقل کردن حجم اطلاعات، لازم است تعداد عامل‌ها در لایهٔ اول کاهش داده شود. در این مقاله با استفاده از ساختار سیستم چندعاملی، الگوریتمی پیشنهاد شد که در آن بدون در نظر داشتن مکان نصب منابع، نوع و ظرفیت تولیدی آن‌ها، رله‌های اضافه جریان بدون شکست در عملکردشان، وظیفهٔ خود را به‌درستی انجام می‌دهند و خطا را برطرف می‌کنند. استفاده از ساختار سیستم‌های چندعاملی یکی از روش‌هایی است که به‌منظور رفع مشکلات حفاظتی مطرح شده است، اما به‌دلیل اینکه فرایند اجرایی آن با مشکل تأخیر زمانی همراه است، در شرایط خطا با مشکل مواجه می‌شود. بنابراین به‌منظور بالا بردن سرعت و کاهش تأخیر زمانی ساختار چندعاملی سنتی، روشی بر اساس حفاظت تطبیقی مبتنی بر هوشمندسازی شبکه‌های توزیع به‌کمک عاملی کردن شبکه در حضور منابع تولید پراکنده مطرح می‌شود. این طرح به جمع‌آوری اطلاعات شبکه وابسته نیست و از میزان تهدیدات موجود بر روی ساختار سلسله‌مراتبی و نیز از هزینه‌های پیاده‌سازی آن کاسته می‌شود. همچنین با توجه به پیاده‌سازی ساختار به‌صورت محلی، نیازی به حضور یک سیستم مرکزی نیست.

علائم

عنوان	کمیت
پروتکل اختصاصی سیستم توزیع	IEC-61850
مکانیزم کنترلی	GOOSE
ضریب تنظیم زمانی	TMS
زمان عملکرد رله	t_{PD}
مسدود کردن پیام سرور	SVM

مراجع

[1] Cui, Q., Bai, X. and Dong, W., "*Collaborative planning of distributed wind power generation and distribution network with large-scale heat pumps*", CSEE Journal of Power and Energy Systems, Vol. 5, No. 3, pp. 335-347, Sept. 2019.

[2] Kolasiński, P., "*Application of volumetric expanders in small vapour power plants used in distributed energy generation– Selected design and thermodynamic issues*", Energy Conversion and Management, Vol. 231, Article Number: 113859, March 2021.

[3] Karimi, H., Shahgholian, G., Fani, B., Sadeghkhani, I., Moazzami, M., "*A protection strategy for inverter interfaced islanded microgrids with looped configuration*", Electrical Engineering, Vol. 101, No. 3, pp. 1059-1073, Sep. 2019.

[4] Cintuglu, M.H., Ma, T. and Mohammed, O.A., "*Protection of autonomous microgrids using agent-based distributed communication*", IEEE Trans. on Power Delivery, Vol. 32, No. 1, pp. 351-360, Feb. 2017.

[5] Jafari, M. and Monsef, H., "*New method for optimum placement of DGs and reclosers*", Journal Energy Engineering and Management**,** Vol. 1, No. 1, pp. 28-37, 2011.

[6] Wan, H., Li, K.K. and Wong, K.P., "*An adaptive multiagent approach to protection relay coordination with distributed generators in industrial power distribution system*", IEEE Trans. on Industry Applications, Vol. 46, No. 5, pp. 2118-2124, Sep./Oct. 2010.

[7] He H., et al., "*Application of a SFCL for fault ride-through capability enhancement of DG in a microgrid system and relay protection coordination*", IEEE Trans. on Applied Superconductivity, Vol. 26, No. 7, pp. 1-8, Oct. 2016.

[8] Ustun, T.S., Ozansoy, C. and Ustun, A., "*Fault current coefficient and time delay assignment for microgrid protection system with central protection unit*", in IEEE Transactions on Power Systems, Vol. 28, No. 2, pp. 598-606, May 2013.

[9] Hashemi Zadeh, S., Zeidabadi Nejad, O., hasani, S., Gharaveisi, A. and Shahgholian, G., "*Optimal DG placement for power loss reduction and improvement voltage profile using smart methods*", International Journal of Smart Electrical Engineering, Vol.1, No. 3, pp. 141-147, Summer 2012.

[10] Abbasi, M., Nafar, M. and Simab, M., "*Management and control of microgrids connected to three-phase network with the approach of activating current limitation under unbalanced errors using fuzzy intelligent method with the presence of battery, wind, photovoltaic and diesel sources*", Journal of Intelligent Procedures in Electrical Technology, vol. 13, no. 49, pp. 59-71, June 2022.

[11] Hosseini, S.A., Sadeghi, S.H.H. and Nasiri, A., "*Decentralized adaptive protection coordination based on agents social activities for microgrids with topological and operational uncertainties*", IEEE Trans. on Industry Applications, Vol. 57, No. 1, pp.

702-713, Jan.-Feb. 2021.

[12] Reis, F.B., Pinto, J.P., Reis, F.S., Issicaba, D. and Rolim, J.G., "*Multi-agent dual strategy based adaptive protection for microgrids*", Sustainable Energy, Grids and Networks, Vol. 27, Article Number: 100501, Sept. 2021.

[13] Habib, H.F., Youssef, T., Cintuglu, M.H., Mohammed, O.A., "*A multi-agent based technique for fault location, isolation and service restoration*", IEEE Trans. Industry Applications, Vol. 53, No. 3, pp. 1841-1851, May/June 2017.

[14] Hassani Ahangar, A., Nafisi, H., Karami, H. and Gharehpetian, G., "*Overcurrent relay coordination using improved hyper-spherical search algorithm considering different relay characteristics and pickup current*", Iranian Journal of Electrical and Computer Engineering, vol. 16, no. 3, pp. 187-195. 1397.

[15] Nassif, A.B., "*A protection and grounding strategy for integrating inverter-based distributed energy resources in an isolated microgrid*", CPSS Transactions on Power Electronics and Applications, Vol. 5, No. 3, pp. 242-250, Sept. 2020.

[16] Matos, S.P.S., Vargas, M.C., Fracalossi, L.G.V., Encarnação, L.F. and Batista, O.E., "*Protection philosophy for distribution grids with high penetration of distributed generation*", Electric Power Systems Research, Vol. 196, Article Number: 107203, 2021.

[17] Abrisham Foroushan Asl, S., Gandomkar, M., Nikoukar, J., "*System stability-constrainted optimal protection coordination in the microgrid including renewable energy sources and energy storage*", Journal Energy Engineering and Management, Vol. 11, No. 2, pp. 16-31, 2021.

[18] Nikolaidis, V.C., Papanikolaou, E. and Safigianni, A.S., "*A communication-assisted overcurrent protection scheme for radial distribution systems with distributed generation*", IEEE Trans. on Smart Grid, Vol. 7, No. 1, pp. 114-123, Jan. 2016.

[19] Foroushan Asl, S.A., Gandomkar, M. and Nikoukar, J., "*Optimal protection coordination in the micro-grid including inverter-based distributed generations and energy storage system with considering grid-connected and islanded modes*", Electric Power Systems Research, Vol. 184, Article Number: 106317, July 2020.

[20] Dong, C., Zhang, W., Wang, Q. and Liu, Y., "*Time-varying anti-disturbance formation control for high-order non-linear* multi-agent systems *with switching directed topologies*", IET Control Theory & Applications, Vol. 14, No. 2, pp. 271 – 282, Jan. 2020.

[21] Dou, C., Yue, D., Guerrero, J.M., Xie, X. and Hu, S., "*Multiagent system-based distributed coordinated control for radial DC microgrid considering transmission time delays*", IEEE Trans on Smart Grid, Vol. 8, No. 5, pp. 2370-2381, Sept. 2017.

[22] Pesente, J.R., Rolim, J.G. and Moreto, M., "*Multiagent systems in power system protection: Review, classification and perspectives*", IEEE Latin America Transactions, Vol. 14, No. 7, pp. 3285-3290, July 2016.

[23] Tong, X., et al., "*The study of a regional decentralized peer-to-peer negotiation-based wide-area backup protection multi-agent system*", IEEE Trans. on Smart Grid, Vol. 4, No. 2, pp. 1197-1206, June 2013.

[24] Kazemi Karegar, H. and Abbasi, A., "*Appropriation of differential protection for optimal protection of active distribution networks under different configuration*s", Iranian Electric Industry Journal of Quality and Productivity, Vol. 7, No. 2, pp. 113-121, 2019.

[25] Bagheri, H. and Shakarami, M., "*Novel fuzzy-iwo method for reconfiguration simultaneous optimal DG units allocation*", Journal of Intelligent Procedures in Electrical Technology, Vol. 6, No. 21, pp. 13-20, 2015.

[26] Shahgholian, G. and Azimi, Z., "*Analysis and design of a DSTATCOM based on sliding mode control strategy for improvement of voltage sag in distribution systems*", Electronics, Vol. 5, No. 3, pp. 1-12, 2016.

[27] Ashrafi, A. and Shahrtash, S.M., "*Dynamic wide area voltage control strategy based on organized multi-agent system*", IEEE Trans on Power Systems, Vol. 29, No. 6, pp. 2590-2601, Nov. 2014.

[28] Ustun, T.S., Ozansoy, C. and Zayegh, A., "*Modeling of a centralized microgrid protection system and distributed energy resources according to IEC 61850-7-420*", IEEE Trans. on Power Systems, Vol. 27, No. 3, pp. 1560-1567, Aug. 2012.

[29] Barra, P.H.A., Coury, D.V. and Fernandes, R.A.S., "*A survey on adaptive protection of microgrids and distribution systems with distributed generators*", Renewable and Sustainable Energy Reviews, Vol. 118, Article Number: 109524, Feb. 2020.

[30] Ibrahim, A.M., El-Khattam, W., ElMesallamy, M. and Talaat, H.A., "*Adaptive protection coordination scheme for distribution network with distributed generation using ABC*", Journal of Electrical Systems and Information Technology, Vol. 3, No. 2, pp. 320-332, Sept. 2016.

[31] Giovanini, R., Hopkinson, K., Coury, D.V. and Thorp, J.S., "*A primary and backup cooperative protection system based on wide area agents*", IEEE Trans. on Power Delivery, Vol. 21, No. 3, pp. 1222-1230, July 2006.

[32] Liu, Z., Su, C., Høidalen, H.K. and Chen, Z., "*A multiagent system-based protection and control scheme for distribution system with distributed-generation integration*", IEEE Trans. on Power Delivery, Vol. 32, No. 1, pp. 536-545, Feb. 2017.

[33] Fani, F., Bisheh, H. and Karami-Horestani, A., "*An offline penetration-free protection scheme for PV-dominated distribution systems*", Electric Power Systems Research, Vol. 157, pp. 1-9, April 2018.

[34] Abbaspour, E., Fani, B. and Heydarian-Forushani, E., "*A bi-level multi agent based protection scheme for distribution networks with distributed generation"*, International Journal of Electrical Power and Energy Systems, Vol. 112, pp. 209-220, Nov. 2019.