مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۲، تابستان ۱۳۹۶، ص ۵۸-۴۷

روش راهبردی کنترلی مقابله با خاموشی ریزشبکه‌ها حین وقوع حملات سایبری به شبکه برق سراسری

مریم رحمانی[۱]، فرامرز فقیهی[۲*]، بابک مظفری[۳]

۱- دانشجوی کارشناسی ارشد، ۲- استادیار، ۳- دانشیار، دانشگاه آزاد اسلامی واحد علوم و تحقیقات

(دریافت: ۹۴/۱۱/۰۷، پذیرش: ۹۵/۱۰/۱۴)

چکیده

در این مقاله هدف اصلی حفظ پایداری درحالی است که با حملات سایبری دشمن هوشمند بر شبکه قدرت و فرامین کنترلی ریزشبکه دچار تنش شده و به حالت جزیره‌ای رفته و یا تغییرات دیگری را بر شبکه اعمال کرده است. حفظ پایداری با کنترل فرکانس در حدود نامی میسر می‌گردد. در جهت کنترل سریع فرکانس در هر لحظه باید تعادل توانی مابین تولید و مصرف برقرار شود که این مهم توسط منابع ذخیره انرژی از قبیل باتری با زمان پاسخ دینامیکی خیلی سریع، قابل انجام است. سیستم ذخیره انرژی باتری اگر به‌خوبی طراحی شده باشد می‌تواند به پایداری فرکانس سیستم از طریق تزریق یا جذب توان اکتیو کمک کند تا شبکه دچار خاموشی نشود که در راستای بیش‌ترین استفاده از ظرفیت باتری، روش کنترلی کارآ بسیار مهم خواهد بود. شبیه‌سازی در محیط MATLAB/SIMULINK انجام شده است.

واژه‌های کلیدی: حملات سایبری، امنیت شبکه قدرت، کنترل مشارکتی، ریزشبکه، کنترل فرکانس

۱- مقدمه

شبکه قدرت، ساختاری است که جامعه مدرن در آن نگه داشته می‌شود. قطع برق می‌تواند اثرات اقتصادی و اجتماعی جبران‌ناپذیری را به بار آورد. برای نمونه، قطع برق در سال ۲۰۰۳ در ساحل شرقی آمریکا، بر ۵۰ میلیون انسان تأثیر گذاشت و حدود ۶ تا ۱۳ میلیارد دلار خسارت بر جای گذاشت. درنتیجه، بازسازی صنعت به سمت محیط بازار با عوامل و منابع اضطراری جدید، استفاده از شبکه‌های مخابراتی، سیستم‌های کنترلی نظارتی و اکتساب داده (SCADA[1])، مخابرات بی‌سیم و اینترنت، پیچیدگی شبکه قدرت را افزایش داده است. این عوامل نو، آسیب‌پذیری جدیدی را به نام آسیب‌پذیری‌های سایبری به وجود آورده‌اند [۴-۱]. این آسیب‌پذیری‌های سایبری که مشخصه اصلی آن‌ها لزوم نداشتن اتصال فیزیکی با شبکه قدرت است به‌عنوان نسل جدیدی از آسیب‌پذیری فرض می‌شوند. این مشخصه غیرفیزیکی، سناریوی تازه‌ای را برای ملاحظات قابلیت اطمینان باز می‌کند و به‌طورکلی نظریه‌ها و ابزارهای بسیاری برای بررسی قابلیت اطمینان باید برای این محیط جدید به‌روز شده یا از نو ساخته شوند. نیروگاه‌های بزرگ اثر بیش‌تری را در این مورد نسبت به نیروگاه‌های کوچک می‌گذارند.

در این سناریوی سایبری جدید، اتصال به‌عنوان مهم‌ترین بحث نمایان می‌شود [۳]. درنتیجه، فرض می‌شود هنگامی‌که ریزشبکه بر اثر این حملات جزیره‌ای شده و به‌صورت مستقل کار می‌کند حفظ پایداری و کنترل فرکانس به‌منظور جلوگیری از قطع، مشخصه مهمی است. زیرا جزیره‌ای‌شدن شبکه دلایل مختلفی می‌تواند داشته باشد، ازجمله قطع‌شدن ناگهانی بریکرها، زمانی‌که یک دستگاه حفاظتی (مانند کلید، بازبست یا سکسیونر) که بین واحد تولید پراکنده و شبکه اصلی قرار دارد؛ عمل کند؛ امکان شکل‌گیری جزیره وجود خواهد داشت. احتمال حمله سایبری به خود ریزشبکه در حالت کلی بسیار پایین‌تر است. ریزشبکه قسمتی از شبکه توزیع (ولتاژ متوسط یا ولتاژ ضعیف) است که شامل منابع تولید پراکنده (اعم از منابع گازی، تجدیدپذیر و ذخیره‌ساز انرژی) و بارهای الکتریکی داخل آن می‌باشند. ریزشبکه قادر است در دو حالت متصل به شبکه و جدا از شبکه عمل کند. وظیفه انطباق‌دادن تولید و مصرف در حالت متصل به شبکه برعهده شبکه اصلی و در حالت جدا از شبکه برعهده منابع ذخیره‌ساز انرژی داخل ریزشبکه است [۶-۵]. در حالت جزیره‌ای، حفظ شاخصه‌های کیفیت توان ریزشبکه کاملاً به عهده منابع داخل ریزشبکه است درحالی‌که در حالت متصل به شبکه تا حد زیادی خود شبکه کیفیت توان مطلوب را برای بارهای ریزشبکه که مقدار زیادی از آن‌ها هارمونیکی و نامتعادل

* رایانامه نویسنده مسئول: faramarz_faghihi@hotmail.com

1- Supervisory Control and Data Acquisition

می‌باشند تأمین می‌نماید، هر چند که منابع داخل ریزشبکه نیز می‌توانند در این امر به شبکه اصلی کمک کنند [۷]. در جهت کنترل سریع فرکانس در هر لحظه باید تعادل توانی مابین تولید مصرف برقرار شود که این مهم توسط منابع ذخیره انرژی ازقبیل باتری قابل انجام است [۸]. واحد باتری همراه با واسط ادوات الکترونیک قدرت جهت دنبال‌کردن تغییرات میکروسکوپیک بار به‌کار برده می‌شود زیرا آن‌ها زمان پاسخ دینامیکی خیلی سریعی دارند. بالطبع، حد ظرفیت باتری مورد استفاده محدود است. در برخی از مطالعات پیشین درزمینه به‌کارگیری ESS[1] برای پایدارسازی سیستم‌های قدرت منابع انرژی تجدیدپذیر (RES[2]) وجود دارد. بحث معرفی ESS در ریزشبکه در [۱۳-۹] ارائه شده است. منابع تولید پراکنده با واسطه‌های الکترونیک قدرت در [۱۱-۹] ارائه شده‌اند. سیستم DG[3] شامل یک سیستم ذخیره‌ساز منبع انرژی اولیه یا باتری (ESS) و یک اینورتر است. ریزشبکه می‌تواند از طریق نصب ESS در DGهایی که دارای منبع انرژی اولیه با پاسخ نسبتاً آهسته هستند، در حالت عملکرد جزیره‌ای و حتی تغییرات ناگهانی بار به‌صورت پایداری عمل کند. با توجه به کارهای پیشین، طرح کنترلی مشارکتی بین سیستم ذخیره‌ساز انرژی (ESS) و سایر ریزمنابع در عملکرد جزیره‌ای مورد نیاز است. مفهوم کنترل که شامل کنترل اولیه و ثانویه است برای پایداری فرکانس در ریزشبکه پیشنهاد شده است [۱۳]. این مفهوم از روش کنترل فرکانس در شبکه قدرت بزرگ تقلید شده است. ESS توان را از طریق مشخص افت جذب یا تزریق می‌کند و انحراف فرکانس با AGC[4] کنترل‌کننده نظارتی حذف می‌شود در راستای بیش‌ترین استفاده از ظرفیت باتری، روش کنترلی کار بسیار مهم خواهد بود. بالطبع، پایداری ریزشبکه پس از قرارگرفتن در حالت جزیره‌ای، پارامتر بسیار مهم در سیستم تجدیدساختارشده خواهد بود. بدین ترتیب، اهمیت و ضرورت این تحقیق این‌گونه بیان می‌شود که درصورت وقوع حملات سایبری و مستقل‌شدن ریزشبکه شامل بارها و تولیدات پراکنده باید تعادل توان بین تولید و مصرف صورت گیرد تا از نوسانات فرکانس و ولتاژ جلوگیری به‌عمل آید و با کنترل دقیق فرکانس در مدت زمان کوتاه، پایداری شبکه را حفظ کرد و از خاموشی آن جلوگیری کرد تا اثرات اقتصادی و اجتماعی وحشتناک آن‌را کاهش داده و از بین برد. نوآوری در این تحقیق این‌گونه بیان می‌شود که تا به حال در حوزه امنیت از این جهت به موضوع حملات سایبری نگاه نشده و مورد بررسی قرار نگرفته است. در این مطالعه این‌گونه فرض می‌شود که دشمن بسیار هوشمند بوده و احتمال حمله سایبری به ادوات کنترلی و کلیدهای ریزشبکه بعد از جزیره‌ای‌شدن یعنی خارج‌کردن توربین بادی نیز وجود دارد و یا دشمن هوشمند به‌صورتی برنامه‌ریزی کرده است تا با اطلاعات زیست محیطی که به‌دست آورده است، زمانی‌که قدرت باد به حد لازم نمی‌رسد را تشخیص داده و خروج توربین بادی را مدتی بعد از جزیره‌ای‌شدن پیش‌بینی کند و درنتیجه باز هم به ریزشبکه تنش وارد کرده تا باعث خاموشی گردد. هم‌چنین آن‌چه در این مقاله انجام می‌شود میراکردن نوسانات فرکانس در حداقل زمان ممکن است که برای این کار از کنترل‌کننده مشارکتی PI استفاده می‌شود که در ادامه می‌آید.

۲- SCADA و انواع حملات سایبری

به‌منظور جمع‌آوری همه اطلاعات لازم و تحویل دستورات، داشتن شبکه‌ای که بتواند اطلاعات را از فاصله‌های بسیار دوری که شاید فراتر از صدها مایل باشد، جمع‌آوری کرده و بفرستد، امر مهمی است. سیستم‌های SCADA نه تنها در زیربناهای الکتریکی، بلکه در سیستم‌های گازی، آبی و مخابراتی نیز مورد استفاده قرار گرفته است [۲]. این سیستم اساساً از سه بخش تشکیل‌شده است: الف) اکتساب داده و توانایی سوئیچینگ، ب) سیستم ارتباطی و ج) کنترل نظارتی.

اکتساب داده و توانایی سوئیچینگ با دستگاهی که واحد ترمینال از راه دور (RTU[5]) نامیده می شود، انجام می‌گردد. RTU پارامترهای آنالوگ و دیجیتال میدان و داده‌های انتقالی به ایستگاه مانیتورینگ مرکزی را می‌فرستد. RTU می‌تواند با ایستگاه مرکزی به طرق مختلفی مرتبط باشد (اغلب سریال RS232, RS485, RS422 یا اترنت). RTU قابلیت پوشش پروتوکل‌های استاندارد با هر نرم‌افزار بخش سوم را دارد (مودباس، IEC61850 ،IEC60780-6-ICCP،DNP3،IEC60870-5-101/103/104 و غیره). در بعضی کاربردهای کنترلی، RTUها بر بردهای خروجی دیجیتال برای خاموش و روشن‌کردن دستگاه‌ها کاربرد دارند. این عمل بر برد خروجی دیجیتال که با کنتاکت‌های جریان بالا محصور شده‌اند، باعث عملکرد رله می شود. RTUها در ایستگاه‌ها جای‌گذاری می‌شوند و حالت‌های تجهیزات و پارامترهای سیستم مثل توان اکتیو و راکتیو، ولتاژها و غیره را جمع‌آوری می‌کنند. سیستم کنترل نظارتی همه RTU ها را در دوره اسکن از پیش تعیین‌شده‌ای اسکن می‌کند (برای مثال ۲ ثانیه) و اطلاعات از قبل جمع‌آوری‌شده را دوباره جمع می‌کند. هم‌چنین

1- Energy Storage System
2- Renewable Energy System
3- Distributed Generation
4- Automatic Gain Control
5- Remote Terminal Unit

سیستم کنترل نظارتی توانایی اجرای درخواست‌های سوئیچینگ اپراتور را دارد. این درخواست‌ها به RTUها فرستاده می‌شوند و از طریق عمل‌کردن رله‌های وابسته به سوئیچ‌ها اجرا می‌شوند. برای مثال، بعد از اسکن اطلاعات RTUها و ارائه به اپراتور، اپراتور مشاهده می‌کند که ولتاژ در بخشی پایین است و بهتر است خازنی سوئیچ شود تا ولتاژ را در باس افزایش دهد تا به سطح قابل قبول برسد، او این کار را با سوئیچ از راه دور خازن توسط RTU که مربوط به باز و بسته‌کردن کلید خازن است، انجام می‌دهد [۱۶]. اهمیت سیستم SCADA به سبب قابلیت جمع‌آوری اطلاعات و انجام عمل مورد نیاز بسته به لزوم آن، است. سیستم SCADA می‌تواند برای کمک به سیستم‌های تولید، انتقال و توزیع به‌کار رود تا کیفیت و پایداری پویایی (دینامیکی) شبکه را تثبیت کند. اگرچه، استفاده از سیستم SCADA آسیب‌پذیری‌هایی را نیز به شبکه قدرت وارد می‌کند. [۲]. به‌طورکلی، در یک سیستم SCADA نخست سطح اول (شبکه حسگر) تعریف می‌شود. در مرحله بعدی سطح دوم یا سطح بی یا تجهیزات الکترونیک هوشمند وجود دارد که این دو سطح سیستم محلی را تشکیل می‌دهند. تجهیزاتی که در محل، یعنی پست‌ها و نیروگاه‌ها نصب می‌شوند و وظیفه جمع‌آوری اطلاعات و اجرای فرمان‌ها را به‌عهده دارند سیستم محلی نامیده می‌شوند. سیستم مذکور این امکان را فراهم می‌آورد که داده‌ها، مقادیر جمع‌آوری‌شده و فرمان‌ها مرکز اسکادا به اجرا درآید. علاوه‌بر این، وظیفه گزارش‌دادن وضعیت‌ها و تغییرات آن‌ها را به‌عهده دارد. سیستم محلی، بخشی از سیستم اسکاد است که ارتباط فیزیکی با سیستم قدرت در آن‌جا برقرار می‌شود و تجهیزاتی که بایستی کنترل شوند و سیگنال‌هایی که بایستی ارسال شوند، بخش‌های مختلف این سیستم را تشکیل می‌دهند. سیستم ارتباطی سطح بعدی است که بخش مهمی از سیستم اسکادا است که بدون آن تصور داشتن کنترل از راه دور غیرممکن می‌نماید. این بخش وظیفه ایجاد ارتباط بین «سیستم محلی» و «سیستم مرکزی» را به‌عهده دارد. این بخش، نقش شبکه عصبی بدن را بازی می‌کند. بدین صورت که اطلاعات را از گوش و چشم (سیستم محلی) به مغز (سیستم مرکزی) مخابره کرده و از آن‌جا فرمان‌ها را به دست‌ها (سیستم محلی) ارسال می‌نماید. می‌توان اشاره نمود پایانه RTU که یک سیستم میکروپروسسوری نصب‌شده در محل پست‌ها می‌باشد و تمامی اطلاعات را از نقاط مختلف که کنترل و مانیتورینگ آن نیاز است جمع‌آوری کرده و بعد از پردازش، آن‌ها را از طریق سیستم‌های مخابراتی به‌عنوان نمونه شبکه سلسله مراتبی دیجیتال هم‌زمان (SHD[1]) به مرکز کنترل ارسال می‌کند. سطح چهارم، سطح اسکادا یا سیستم مرکزی است. رأس یک سیستم اسکادا در واقع تجهیزاتی هستند که مرکز کنترل را به‌وجود می‌آورند. به‌راحتی می‌توان دید که شبکه‌های مخابراتی که از «سیستم محلی» شروع می‌شوند، به مرکز کنترل خاتمه می‌یابند. «سیستم مرکزی» را می‌توان به دو بخش سخت‌افزار و نرم‌افزار تقسیم کرد که وظایف مربوطه را انجام می‌دهند. عمده وظیفه یک مرکز کنترل جمع‌آوری داده‌ها و اطلاعات دریافتی از شبکه قدرت، سپس آنالیز داده‌ها و ارائه نتایج به اپراتور و درصورت نیاز ارسال به سطوح بالاتر کنترلی و هم‌چنین ارسال فرمان‌ها اپراتور به پایانه‌ها است [۱۵]. با وابسته‌ترشدن سیستم به IT[2]، حساسیت به حملات امنیتی سایبری بیش‌تر شده است. به‌علاوه، بنا به اهمیت زیاد شبکه برق به‌عنوان یکی از مهم‌ترین زیرساخت‌ها، خطر مورد هدف قرارگرفتن حملات سایبری به‌طور چشم‌گیری افزایش می‌یابد. حتی درصورتی‌که حمله‌ای بدون این‌که صدمات دائمی به سیستم بزند، بتواند شبکه را برای چند ساعت قطع کند، تلفات در حد میلیارد دلار خواهند بود [۱۴]. علی‌رغم این‌که شبکه برق از بخش‌های مهم شبکه می‌باشد، اغلب در بحث امنیت شبکه هوشمند نادیده گرفته می‌شود. نرم‌افزارهای مخرب، هکرها را قادر می‌سازد تا با کنترل تجهیزات شبکه از طریق اینترنت، باعث قطع برق و خسارت‌های فراوان به همه بخش‌های اقتصادی شوند. در شبکه‌های هوشمند از سیستم‌های فیزیکی و نرم‌افزاری که به‌هم مرتبط می‌باشند و می‌توانند هر دو نیز دچار صدمه شوند، استفاده می‌نمایند. هکرها به معنای واقعی می‌توانند پس از نفوذ به تأسیسات برق باعث خاموشی در شهرهای مختلف شده و هم‌چنین خواستار دریافت اخاذی قبل از اختلال در سیستم قدرت شوند. تمام بهره‌برداران جهت بهره‌برداری از سیستم‌های الکتریکی نیازمند ارتباط تنگاتنگ با شبکه سراسری برق دارند و برای قابلیت اطمینان سیستم، بایستی در مقابل حوادث سایبری ایمن باشند. استفاده شبکه هوشمند از فناوری‌های اینترنتی بایستی حفاظت کاملی از شبکه به‌عنوان یک موضوع امنیت ملی را به عمل آورد. در زمینه امنیت، حتی بهترین نرم‌افزار نیز ممکن است دچار آسیب‌پذیری‌های غیرعمدی شود. آسیب‌پذیری‌های مربوط به امنیت سایبری سیستم قدرت شامل جزء اصلی یعنی کامپیوتر، ارتباطات و سیستم قدرت می‌باشد. حملات می‌توانند سیستم‌های خاص و زیرسیستم‌های مربوطه را به‌طور هم‌زمان و از راه دور مورد هدف قرار دهد. انواع مختلف حمله، مکانیزه‌های مربوطه و دیگر مشکلات ایجادشده بایستی در طراحی امن شبکه‌های هوشمند درنظر گرفته شود [۱۵]. درنتیجه آن،

[1] Synchronous Digital Hierarchy

2- Information Technology

حملات بسیاری ممکن است به سیستم SCADA وارد شوند که بیش‌تر آن‌ها در اینترنت و دیگر شبکه‌ها رایج می‌باشند. اگر بخواهیم از SCADA محافظت کنیم، همانند هر طرح اطلاعاتی متصل دیگری باید به سه عنصر امنیت اطلاعت توجه داشته باشیم: محرمانه‌بودن، درست‌بودن و دردسترس‌بودن.

محرمانه‌بودن، توانایی این‌که تنها سیستم مجاز بتواند به اطلاعات تعیین‌شده‌ای دسترسی داشته باشد، است؛ درست‌بودن، کیفیت این‌که اطلاعات فرستاده‌شده دقیقاً همان اطلاعات دریافت شده باشد، است؛ و در دسترس‌بودن، در دسترس‌بودن سیستمی در زمان نیاز به آن است. بررسی هر نوع حمله با توجه به این سه مشخصه، تشخیص نتایج هر حمله را آسان‌تر می‌کند. به‌عنوان مثال چند نوع حمله را نام می‌بریم:

- حمله بازدارنده سرویس (Denial of Service-DoS)
- حمله پاسخ (Replay)
- حمله انسان در وسط (Man-in-the-middle)
- حمله برنامه‌ریزی دوباره RTUها (Reprogramming RTUs)

همگی این حملات نیاز به دسترسی به یک شبکه SCADA دارند. این دسترسی اساساً به دو روش قابل انجام است: یا با دسترسی‌داشتن از طریق درون خود شبکه (محلی) یا با شبکه‌ای دیگر (کنترل از راه دور) [۶]. در اثر هرکدام از این حملات با عملکرد نادرست شبکه SCADA امکان بازشدن بریکر یا هر خطای دیگر و جداشدن ریزشبکه از شبکه اصلی، خروج توربین‌ها وجود دارد، در این حالت حفظ پایداری با کنترل فرکانس در همان ثانیه‌های اول بسیار مهم است. درنتیجه توضیحات اخیر، اهمیت و ضرورت جلوگیری از خاموشی شبکه و کنترل آن در ثانیه‌های ابتدایی پس از وقوع حمله به شبکه SCADA بیش‌تر مشخص می‌گردد.

۳- راهبرد کنترل مشارکتی ریزشبکه

برای عملکرد نرمال DGها با واسط مبدل‌های الکترونیک قدرت انتخاب راهبرد کنترل مناسب دارای اهمیت زیادی است. کنترل اینورترهای واسط منابع در ریزشبکه به روش‌های گوناگونی انجام می‌شود که متداول‌ترین آن‌ها عبارت‌اند از: کنترل PQ، کنترل افت و کنترل v/f. در این راستا کنترل ریزشبکه جزیره‌ای به روش‌های متمرکز و غیرمتمرکز انجام می‌شود که در این مقاله مبتنی بر اصول روش کنترل متمرکز ریزشبکه جزیره‌ای، از راهبرد کنترل مشارکتی استفاده می‌شود. مفهوم اصلی عملکرد مستقل شامل کنترل مشارکتی، منابع ذخیره انرژی و سایر ریزمنابع می‌شود. در طول عملکرد جزیره‌ای مبتنی بر حملات سایبری، میزان توان تولیدی و مصرفی در هر لحظه یکسان نیست. درنتیجه، فرکانس و ولتاژ ریزشبکه نوسان و سیستم یک خاموشی را تجربه خواهد کرد مگر این‌که یک فرآیند برقراری تعادل توان مناسب موجود باشد. کنترل‌کننده اینورتر سیستم ذخیره انرژی (ESS) در حد چندین میلی‌ثانیه پاسخ می‌دهد درحالی‌که دیزل ژنراتور، ماشین درون‌سوز، سلول سوختی یک زمان پاسخ نسبتاً آهسته دارد. به‌طور واضح، ESS یک نقش مهم در نگه‌داری ولتاژ و فرکانس ریزشبکه در محدوده مجاز در طول عملکرد جزیره‌ای بازی می‌کند. در حالت عملکرد جزیره‌ای با متعادل‌سازی مناسب توان ESS، ولتاژ و فرکانس ریزشبکه می‌توانند در مقادیر نامی تنظیم شوند این تحقیق روش کنترل مشارکتی ریزشبکه را در حالت عملکرد جزیره‌ای حین وقوع حملات سایبری برای فرکانس نشان می‌دهد. در این طرح کنترلی، ساختار کنترل مشارکتی دولایه به‌کار می‌رود. عمل کنترل اولیه در ESS و عمل کنترل ثانویه در سیستم مدیریت ریزشبکه (MMS[1]) انجام می‌شود [۸]. روش کنترل فرکانس در ESS توسط کنترل اولیه اعمال می‌شود و کنترل ثانویه سیستم مدیریت ریزشبکه توان خروجی ESS را درصورتی‌که خود ESS باری را تأمین نکند به صفر می‌رساند. اهداف کنترل مشارکتی در این تحقیق کنترل فرکانس و ولتاژ درنتیجه جلوگیری از خاموشی و بازگرداندن شبکه به حالت نرمال عملکرد خود در حد چند ثانیه در حالت جزیره‌ای حین وقوع حملات سایبری است. فرضیه نیز این‌طور تعریف شد که با کنترل مشارکتی می‌توان فرکانس را کنترل کرده و از خاموشی به‌علت وقوع حملات سایبری بر سیستم SCADA و عملکرد نادرست رله‌ها و بریکرها و ورود به حالت جزیره‌ای، جلوگیری کرد.

۴- مدل سیمولینک شبکه شبیه‌سازی‌شده

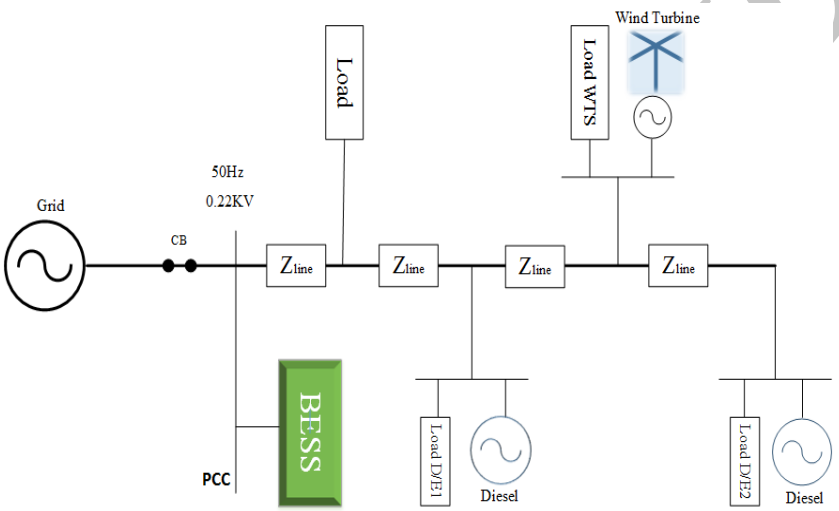
با توجه به توضیحات که از قبل داده شد و بیان سؤال اصلی که آیا جلوگیری از خاموشی ریزشبکه حین وقوع حملات سایبری امکان‌پذیر است و فرضیه مورد نظر که حفظ پایداری ریزشبکه با کنترل فرکانس مشارکتی برای آن را بیان می‌کند برای روش انجام تحقیق، تحلیل داده‌ها که همان مشخصات سیستم مورد نظر بوده و در جدول (۱) آمده است از نرم‌افزار MATLAB/SIMULINK استفاده شده است. جامعه آماری برای

1- Microgrid Management System

این فرضیه هر نوع از ریزشبکه متصل به شبکه اصلی برق با انواع مختلف واحدهای تولید پراکنده، بارها و ادوات دیگر می‌تواند باشد که شبکه مورد نظر برای شبیه‌سازی در این مقاله مطابق شکل (۱) از دو دیزل ژنراتور، یک توربین بادی و سیستم ذخیره انرژی باتری و ۳ بار حساس تشکیل شده است. ولتاژ سیستم ۲۲۰ ولت و فرکانس ۵۰ هرتز درنظر گرفته شده است. مدل‌سازی بارها در مقاله به‌صورت امپدانس ثابت R و X انجام شده است. هم‌چنین برای این شبکه نیز از سمت SCADA فرمان‌هایی بر بریکر وجود دارد.

جدول (۱): مشخصات سیستم

تجهیزات ریزشبکه	مشخصات بار و توان
دیزل ژنراتور ۱	۱۸ KVA
دیزل ژنراتور ۲	13 KVA
توربین بادی	۲۰ KW
سیستم ذخیره انرژی باتری	۵۶ KW
بار WTS	۳+۶ JK
بار دیزل ژنراتور ۱	15+8 JK
بار دیزل ژنراتور ۲	9+8 JK
بار	3 KW



شکل (۱): ریزشبکه تحت مطالعه

۵- مدل دیزل ژنراتور

دیزل به‌عنوان منبع تولید پراکنده جهت بالانس انحراف بار استفاده می‌شود. دیزل ژنراتور از یک ماشین سنکرون، یک تحریک‌کننده با ورودی‌های ولتاژ که شامل یک کنترل حلقه بسته با خروجی ولتاژ، تشکیل شده است و یک گاورنر با ورودی اختلاف سرعت ماشین سنکرون از مقدار مرجع آن است و خروجی آن، توان مکانیکی است که با ضرب گشتاور مکانیکی محاسبه‌شده در کنترلر حلقه باز آن در سرعت به‌دست می‌آید، تشکیل شده است. نقطه تنظیم توان خروجی دیزل ژنراتورها تغییر می‌کند. این دیزل ژنراتور حالت گذرای بالایی دارند. درنتیجه در ابتدا در شبیه‌سازی سیستم تا ۰/۴ ابتدایی مشاهده می‌شود.

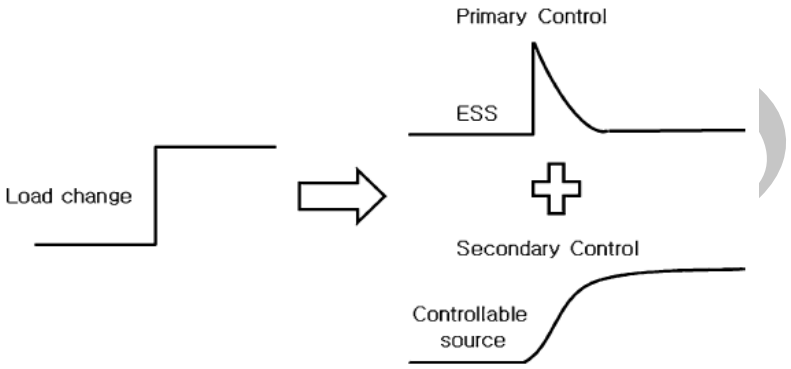
۶- مدل سیستم ذخیره انرژی باتری

مفهوم اصلی عملکرد مستقل شامل کنترل مشارکتی[1]، منابع ذخیره انرژی و سایر ریزمنابع می‌شود. مطابق شکل (۲) در طول عملکرد جزیره‌ای، میزان توان تولیدی و مصرفی در هر لحظه یکسان نیست. درنتیجه، فرکانس و ولتاژ ریزشبکه نوسان[2] و سیستم یک خاموشی[3] را تجربه خواهد کرد مگر این‌که یک فرآیند برقراری تعادل توان مناسب موجود باشد. کنترل‌کننده اینورتر ESS در حد چندین میلی‌ثانیه پاسخ می‌دهد درحالی‌که دیزل ژنراتور، ماشین درون‌سوز، سلول سوختی یک زمان پاسخ نسبتاً آهسته دارد. ESS یک نقش مهم در نگهداری ولتاژ و فرکانس ریزشبکه در محدوده مجاز در طول عملکرد جزیره‌ای بازی

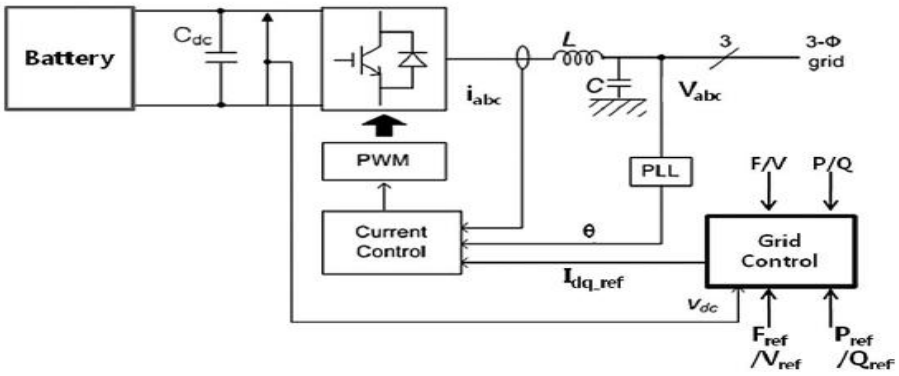
1- Cooperative Control
2- Fluctuate
3- blackout

می‌کند. در حالت عملکرد جزیره‌ای با متعادل‌سازی مناسب توان ESS، ولتاژ و فرکانس ریزشبکه می‌توانند در مقادیر نامی تنظیم شوند. قابلیت کنترل ESS برای تعادل توان مابین تولید و مصرف ممکن است به‌وسیله ظرفیت سیستم موجود محدود شود. بنابراین، توان خروجی ESS باید سریعاً توسط کنترل ثانویه در MMS به کمینه برگردد تا انرژی ذخیره‌شده ماکزیمم را در سیستم تضمین کند.

شکل (۳) ساختار BESS و کنترل‌کننده محلی آن را نشان می‌دهد. کنترل مشارکتی ساده شامل کنترل‌کننده عملکرد شبکه اصلی و کنترل‌کننده جریانی dq است. در حالت کنترل مشارکتی ساده معمول ESS و همه ریزمنابع در حالت کنترل PQ هستند اما با تغییر حالت کنترلی از PQ به v/f در حالت متصل نوعی از کنترل مشارکتی با نام کنترل مشارکتی ترکیبی پیشنهاد می‌شود. هم‌چنین نقطه تنظیم توان خروجی به‌وسیله MSS تعیین می‌شود.

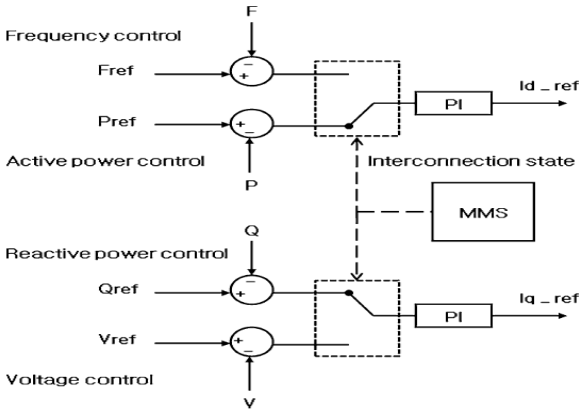


شکل (۲): مفهوم روش کنترلی برای عملکرد جزیره‌ای



شکل (۳): ساختار سیستم ذخیره انرژی باتری

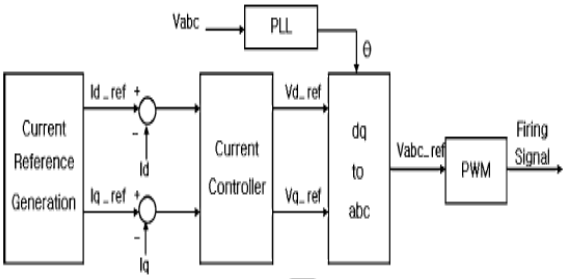
در این حالت کنترل‌کننده شبکه اصلی مقدار توان اکتیو و راکتیو تزریق‌شده به شبکه اصلی و نیز مؤلفه‌های مرجع d[1] و q جریانی خروجی یعنی $I_{d\text{-}ref}$ و $I_{q\text{-}ref}$ را تنظیم می‌کند. از سوی دیگر، در حالت عملکرد جزیره‌ای، کنترل‌کننده شبکه اصلی فرکانس و ولتاژ ریزشبکه و نیز مؤلفه‌های مرجع d و q جریان خروجی را تنظیم می‌کند که در شکل (۴) نشان داده شده است. مقادیر مرجع ولتاژ و فرکانس نیز همان‌طورکه از قبل گفته شد در این شبکه ۲۲۰ ولت و ۵۰ هرتز در نظر گرفته شده است.



شکل (۴): بلوک دیاگرام کنترل‌کننده شبکه اصلی

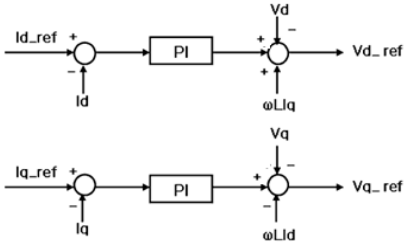
1- Reference

MMS حالت اتصال را از کلید اتصال استاتیکی (STS[1]) و سپس داده‌ها را از BESS دریافت می‌کند. طرح کنترلی جریان در شکل (۵) نشان داده شده است.



شکل (۵): طرح کنترلی جریان سیستم ذخیره انرژی

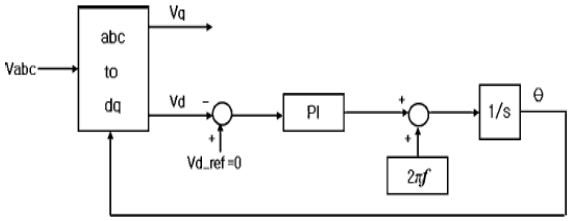
زمانی‌که مقدار مرجع جریان یعنی $I_{d\text{-}ref}$ و $I_{q\text{-}ref}$ تعیین شد، تبدیل dq اعمال می‌شود تا بتوان مؤلفه‌های اکتیو و راکتیو توان خروجی را به‌طور مستقل کنترل کرد. در کنترل‌کننده جریان، در شکل (۶) مؤلفه‌های مرجع d و q ولتاژ $V_{d\text{-}ref}$ و $V_{q\text{-}ref}$ با به‌کارگیری خطای مابین مؤلفه‌های مرجع d-q جریان ($I_{d\text{-}ref}$ و $I_{q\text{-}ref}$) و مؤلفه‌های d-q جریان اندازه‌گیری‌شده (I_d و I_q) حاصل می‌شوند. مقادیر به‌دست‌آمده $V_{d\text{-}ref}$ و $V_{q\text{-}ref}$ از طریق بلوک تبدیل dq به abc به مؤلفه‌های $V_{a\text{-}ref}$، $V_{b\text{-}ref}$ و $V_{c\text{-}ref}$ تبدیل می‌شوند.



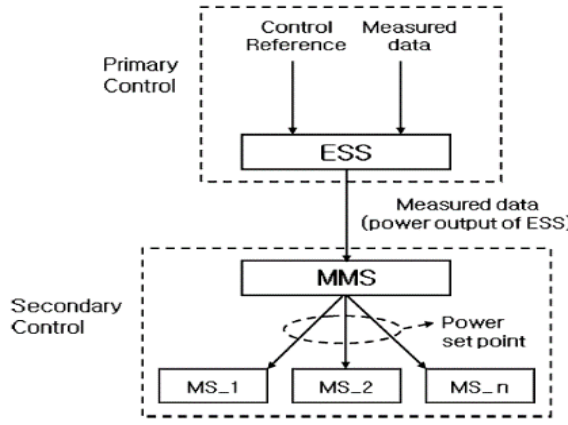
شکل (۶): بلوک دیاگرام کنترل‌کننده جریان

بلوک PLL[2] که در شکل (۷) نشان داده شده است سیگنال سنکرون‌سازی لازم را تولید می‌کند. هنگامی‌که ولتاژهای مطلوب در قاب چرخان a و b و c حاصل شدند روش مدولاسیون پهنای پالس (SPWM[3]) اعمال می‌شود. در مدولاسیون SPWM، پالس‌های فرمان و کنترل خروجی که بایستی به مدار قدرت اعمال شوند از مقایسه یک موج سینوسی مرجع که $V_{abc\text{-}ref}$ با موج حامل[4] مثلثی مقایسه می‌شوند. علت استفاده از این روش عملکرد عالی آن است. در بلوک SPWM، ولتاژهای مطلوب $V_{abc\text{-}ref}$ و سیگنال‌های کلیدزنی اعمال‌شده به شش عدد IGBT[5] وارد می‌شوند.

به‌منظور برگرداندن توان خروجی ESS به کمینه، MMS باید نقطه تنظیم توان خروجی هر ریزمنبع را محاسبه کند و از طریق کنترل ثانویه به ریزمنابع اعمال کند. MMS داده‌ها را از سیستم دریافت می‌کند و سپس از طریق کنترل حلقه بسته، نقاط تنظیم را به هر یک از ریزمنابع ارسال می‌کند. کنترل‌کننده‌های محلی درنهایت مسئول تنظیم توان خروجی هر یک از ریزمنابع به‌صورت محلی هستند. شکل (۸) ساختار کنترل اولیه و ثانویه را نشان می‌دهد.

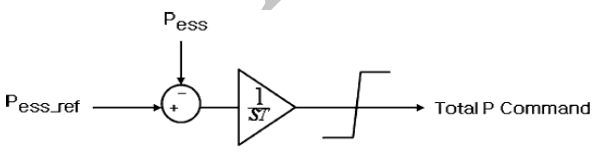


شکل (۷): بلوک دیاگرام PLL



شکل (۸): ساختار راهبرد کنترلی مشارکتی

الگوریتم کنترل ثانویه در MMS، توان خروجی اندازه‌گیری شده BESS (P_{ess}) و مقدار مرجع ($P_{ess\text{-}ref}$) را مقایسه می‌کند تا یک مقدار خطا به‌دست آید. از این مقدار خطا کل توان لازم (total P command) به‌دست می‌آید که در شکل (۹) نشان داده شده است.



شکل (۹): دیاگرام توان کل تولیدی

مقادیر کل توان به‌دست‌آمده مطابق فرمول (۱) بین ریزمنابع تقسیم می‌شود تا نقطه‌های تنظیم جدید را برای هر یک از منابع کنترل‌پذیر تولید کند.

$$\Delta P_{ref\_i} = p_{f\_P_i} . P_{total\_command} \qquad (۱)$$

که در آن، $\Delta P_{ref\text{-}i}$ مقدار تغییر نقطه تنظیم i امین ریزمنبع

1- Static Transfer Switch
2- Phase-Lock Loop
3- Sinuous Pulse Width Modulation
4- Carrier
5- Insulated Gate Bipolar Transistor

است. $P_{total\text{-}command}$ هم مقدار کل توان P به‌دست‌آمده از شکل (۹) است.

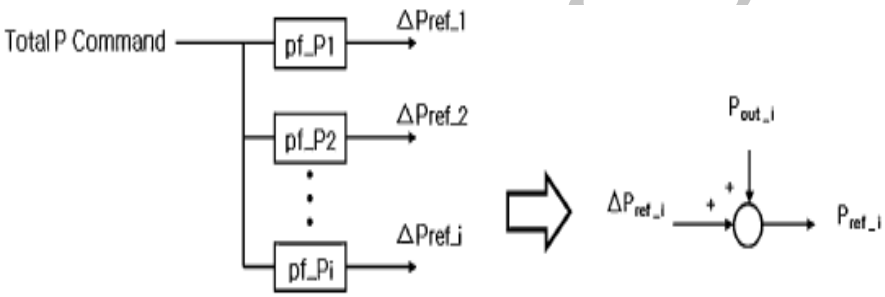
ضریب مشارکت i امین ریزمنبع مقدار ثابت و از پیش تعیین شده‌ای است و مقدار آن توسط ظرفیت منبع تعیین می‌شود. نقطه تنظیم توان اکتیو نهایی i امین منبع $P_{ref\text{-}I}$ از جمع توان خروجی فعلی $P_{out\text{-}i}$ و تغییر نقطه تنظیم $\Delta Pref_{\_i}$ مطابق شکل (۱۰) به‌دست می‌آید.

۷- مدل توربین بادی

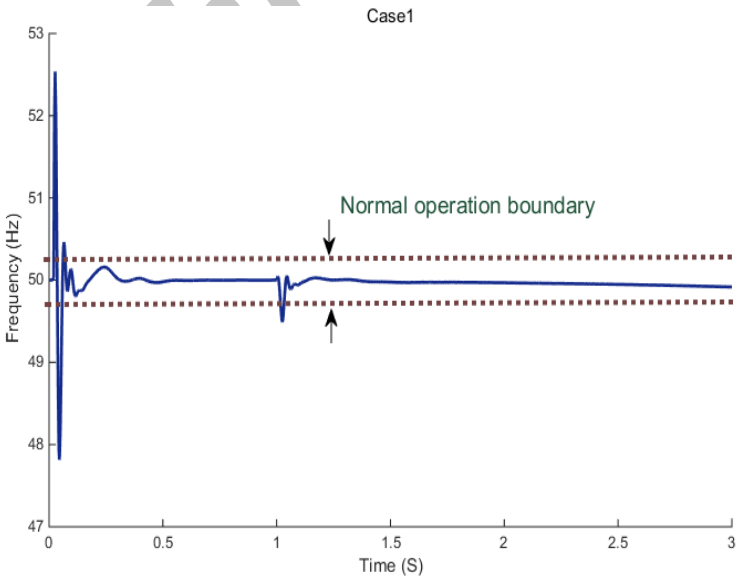
در این مقاله توربین بادی به‌صورت یک منبع ولتاژ با ادوات الکترونیک قدرت (اینورتر) و سیستم کنترلی مربوط به آن مدل و شبیه‌سازی‌شده است.

۸- شبیه‌سازی و نتایج

تحلیل و شبیه‌سازی کنترل فرکانس مشارکتی شبکه موردنظر علاوه‌بر زمانی‌که ریزشبکه به حالت جزیره‌ای می‌رود، در سناریو دیگری که توربین بادی نیز از شبکه به‌دلایل مختلفی همانند کاهش سرعت باد و یا وقوع خطا در توربین بادی و یا حتی حملات سایبری بر سیستم SCADA و عملکرد نادرست آن، خارج می‌شود نیز بررسی می‌گردد. حدود مجاز تغییرات ولتاژ در این شبیه‌سازی ۱۰ ± ولت و تغییرات مجاز فرکانس ۰/۳ ± هرتز با توجه به استانداردهای وزارت نیرو در نظر گرفته شده است. اطلاع سیستم از لحظه جزیره‌ای‌شدن در این مقاله با زمان‌دهی به بریکر انجام می‌شود. آشکارسازی جزیره‌ای‌شدن ریزشبکه هدف اصلی برای این مقاله نبوده و بررسی آن در مباحث دیگری تعریف می‌شود و روش‌های مختلفی برای شبیه‌سازی و تشخیص لحظه جزیره‌ای‌شدن وجود دارد و در واقع MMS حالت اتصال یا عدم آن را از کلید اتصال استاتیکی (STS) و سپس داده‌ها را از BESS دریافت می‌کند.



شکل (۱۰): روش تعیین نقطه تنظیم توان خروجی ریزمنبع

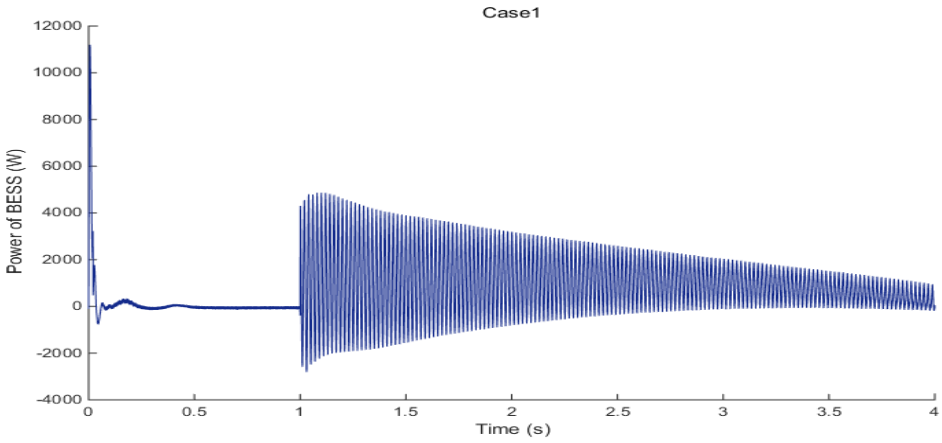


شکل (۱۱): تغییرات فرکانس سناریو اول

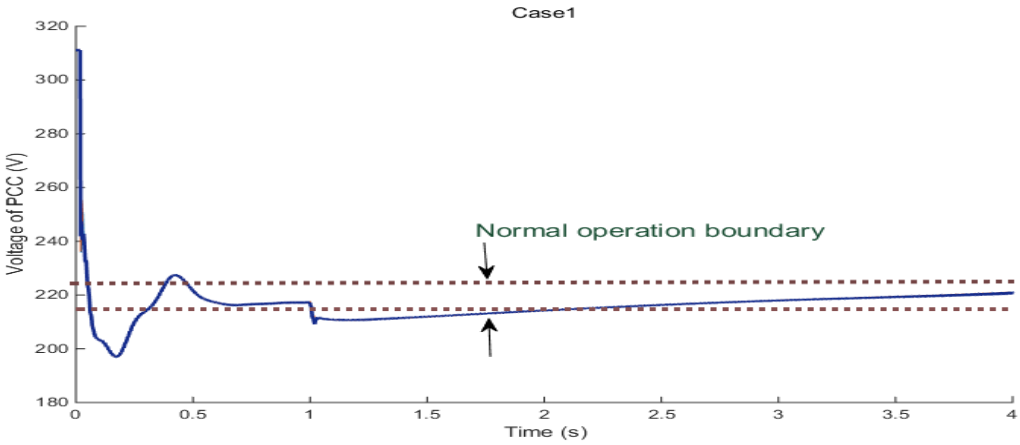
۹- سناریوی اول: ریزشبکه جزیره‌ای می‌شود

در این سناریو شبکه تحت تأثیر حملات سایبری توسط دشمن هوشمند دچار بحران شده و بریکر عملکرد نادرست داشته است، ریزشبکه را وارد حالت عملکرد جزیره‌ای می‌کند. ریزشبکه در

t=۱ s از شبکه اصلی جدا می‌شود تا لحظه جزیره‌ای‌شدن توان مبادله‌شده BESS با شبکه صفر است. همان‌طورکه شکل‌های (۱۲-۱۱) نشان می‌دهند با جزیره‌ای‌شدن فرکانس ۵۰ Hz تا ۴۹/۷ Hz می‌یابد در این لحظه BESS وارد عمل شده و با تزریق توان، نوسانات فرکانس را میرا و درنتیجه فرکانس به ۵۰ Hz برمی‌گردد. سپس با تغییر نقاط تنظیم دیزل ژنراتورها بعد از طی زمان حدودی ۳ ثانیه توان BESS نیز به مقدار کمینه بازمی‌گردد. هم‌چنین همان‌طورکه درشکل (۱۳) نشان داده می‌شود ولتاژ نقطه اتصال مشترک (PCC) در t=۱ s دچار افت شده و ۲۱۰ V می‌رسد با راهبرد کنترلی به‌کار برده شده حدوداً در t=۲ s به محدوده عملکرد نرمال خود بازمی‌گردد. درنتیجه با توجه به فرض بیان‌شده با وقوع حملات سایبری و عملکرد نادرست سیستم SCADA و درنتیجه STS، ریزشبکه از شبکه اصلی جدا شده است و در این شبکه چون از شبکه اصلی به ریزشبکه توان تزریق می‌شده است با قطع اتصال فرکانس کاهش یافته و این توان باید به طریقی جبران شود تا فرکانس به مقدار نامی خود بازگردد که این امر از طریق توانی که باتری به ریزشبکه وارد می‌کند، انجام می‌پذیرد. هم‌چنین توان باتری به‌دلیل آن‌که حد مشخصی دارد و برای ذخیره در سیستم با تزریق توان از دیزل‌ها به مقدار کمینه بازمی‌گردد. ولتاژ نیز با سیستم کنترلی مشابه طراحی‌شده به محدوده نرمال خود بازمی‌گردد. پس در این سناریو فرضیه بیان‌شده درست بوده است و این کنترل مشارکتی فرکانس توانسته به‌خوبی و در مدت زمان کمی در حدود ۱ s فرکانس و ولتاژ را به حد نرمال خود بازگرداند و از خاموشی ریزشبکه بعد از حمله سایبری جلوگیری کند.



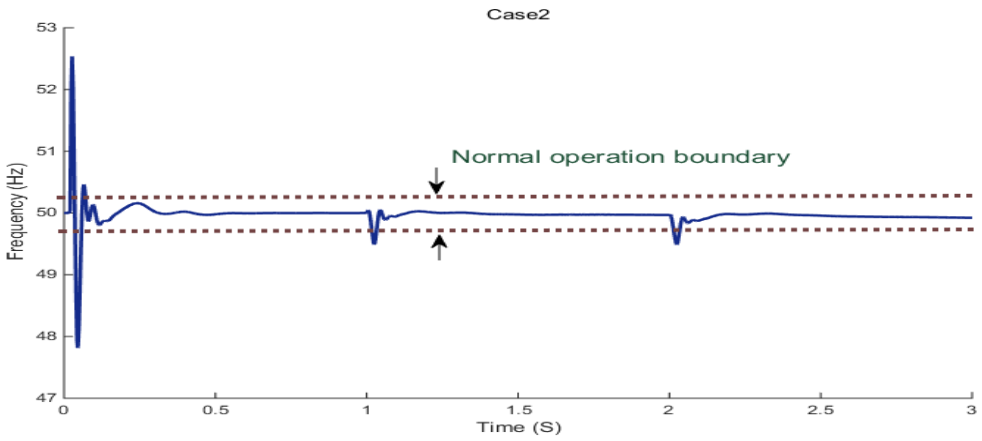
شکل (۱۲): تغییرات توان باتری سناریوی اول



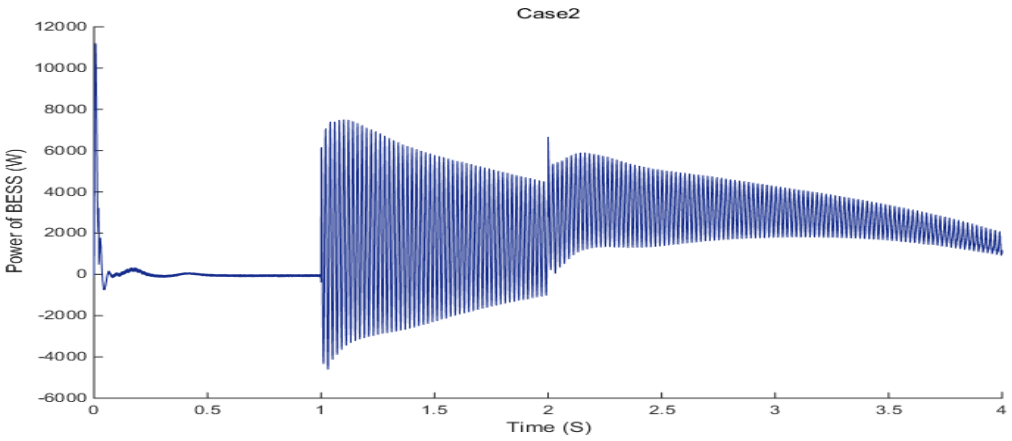
شکل (۱۳): تغییرات ولتاژ نقطه اتصال مشترک در سناریوی اول

۱۰- سناریوی دوم: ریزشبکه جزیره‌ای‌شده با برون‌رفت توربین بادی

در این سناریو نیز شبکه تحت تأثیر حملات سایبری توسط دشمن هوشمند دچار بحران شده و با فرمان به بریکر متصل به شبکه، ریزشبکه را وارد حالت عملکرد جزیره‌ای می‌کند. ریزشبکه در t=۱ s از شبکه اصلی جدا می‌شود تا لحظه جزیره‌ای‌شدن توان مبادله شده BESS با شبکه صفر است. همان‌طورکه اشکل (۱۴) نشان می‌دهند با جزیره‌ای شدن فرکانس ۵۰ Hz تا ۴۹/۷ Hz می‌یابد در این لحظه BESS وارد عمل شده و با تزریق توان، نوسانات فرکانس را میرا و درنتیجه فرکانس به ۵۰ Hz برمی‌گردد. سپس در t=۲ s توربین بادی به‌دلیل کاهش سرعت باد یا وقوع خطا در توربین و حتی حملات سایبری و عملکرد نادرست سیستم SCADA از ریزشبکه خارج شده و توانی مبادله نمی‌کند. در این سناریو فرض می‌شود که خروج توربین بادی به‌صورت عمدی یا برنامه‌ریزی‌شده بوده تا با ایجاد تنش مضاعف سبب خاموشی سیستم گردد به این صورت که یا دشمن بعد از به بحران‌کشاندن شبکه و جزیره‌ای‌شدن ریزشبکه با اعمال فرمان به سیستم‌های حفاظتی کنترلی توربین بادی را از ریزشبکه خارج می‌کند و یا با داشتن اطلاعات زیست محیطی از زمان دقیق کاهش باد که باعث خروج توربین بادی می شود از همان ابتدا ریزشبکه را با حمله سایبری به حالت جزیره‌ای برده است تا در زمان مشخصی پس از حمله توربین نیز از شبکه خارج شود. در این حالت مشاهده می‌شود که باز هم فرکانس از ۵۰ Hz به ۴۹/۶ Hz کاهش یافته و درنتیجه BESS با تزریق توان فرکانس را به ۵۰ Hz بازمی‌گرداند. از t=۱ s به بعد نقاط تنظیم دیزل ژنراتورها متناسب با توان BESS تغییر کرده و بعد از طی زمان حدودی ۳ s توان BESS نیز به مقدار کمینه بازمی‌گردد تا در ریزشبکه ذخیره شود.

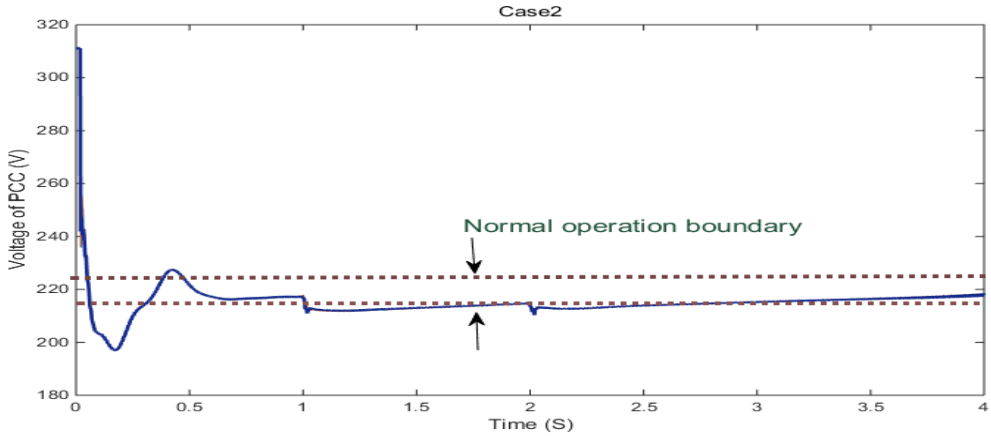


شکل (۱۴): تغییرات فرکانس سناریوی دوم



شکل (۱۵): تغییرات توان باتری سناریوی دوم

هم‌چنین همان‌طورکه در شکل (۱۶) نشان داده می‌شود، ولتاژ نقطه PCC در t=۱ s به‌دلیل جزیره‌ای‌شدن ریزشبکه و در t=۲ s به‌علت خروج ناگهانی توربین بادی به‌ترتیب به ۲۱۰ V و ۲۰۸ V می‌رسد و دچار افت می‌شود اما با راهبرد کنترلی به‌کار برده شده حدوداً در t=۲/۷ s به محدوده عملکرد نرمال خود بازمی‌گردد. درنتیجه با نتایج عددی بیان شده و فرضیه با وقوع حملات سایبری و عملکرد نادرست سیستم SCADA و درنتیجه آن جزیره‌ای‌شدن ریزشبکه و حتی بعد از آن خروج توربین بادی از این شبکه به نمونه‌ای نیز با این کنترل مشارکتی به اهداف اصلی و فرعی این مقاله رسیده‌ایم که هدف اصلی کنترل فرکانس ریزشبکه و اهداف فرعی کنترل ولتاژ و ذخیره توان باتری در ریزشبکه بوده‌اند. درنتیجه، برای پاسخ به فرضیه مورد نظر که حفظ پایداری ریزشبکه با کنترل مشارکتی فرکانس بیان شده است، می‌توان این‌گونه توضیح داد که با توجه به نتایج عددی و نموداری و توضیحات در این دو سناریو حفظ پایداری که همان حفظ فرکانس و ولتاژ بوده است به‌خوبی صورت گرفته و با این روش، کنترلی مشارکتی توانسته‌ایم به‌خوبی و در مدت‌زمان کمی ریزشبکه را حفظ کرده و از خاموشی ریز شبکه بعد از حمله سایبری جلوگیری کنیم.



شکل (۱۶): تغییرات ولتاژ نقطه اتصال مشترک سناریو دوم

۱۱- نتیجه‌گیری

روش کنترل فرکانس مشارکتی سیستم ذخیره انرژی باتری و دیزل ژنراتور هنگامی‌که با حمله سایبری ریزشبکه از شبکه اصلی جدا می‌شود، ارائه داده شد. هنگام وقوع حمله سایبری احتمال خروج چند المان از شبکه به‌صورت هم‌زمان و یا با تاخیز زمانی متفاوت وجود دارد که ما در این مطالعه دو سناریو ممکن الوقوع را بررسی کردیم اما سناریوهای دیگری هم‌چون خروج هم‌زمان توربین بادی و دیزل تیز می‌تواند مورد بررسی قرار بگیرد. با توجه به انواع حملات سایبری که امروزه شبکه قدرت کشورمان را تهدید می‌کند و در صورت بروز آن، صدمات اقتصادی و اجتماعی بالایی را متحمل خواهیم شد، کنترل مشارکتی روش کارآیی را درطول عملکرد جزیره‌ای حین بروز حمله برای کنترل نوسانات فرکانس و ولتاژ بازگرداندن توان BESS به کمینه مقدار ارائه می‌دهد تا شبکه را ایمن نگاه دارد و توان باتری در ریزشبکه ذخیره شود. در هر دو سناریو با حمله سایبری توسط دشمن هوشمند چه تنها با جزیره‌ای‌شدن و چه حتی با خروج توربین بادی به‌صورت برنامه‌ریزی‌شده توسط دشمن هوشمند، با روش کنترلی شبیه‌سازی‌شده، مشاهده شد که نوسانات فرکانس در حد یک‌دهم ثانیه و نوسانات ولتاژ در حد یک ثانیه با روند یکسانی میرا می‌شوند و در همین زمان باتری پس از اعمال توان به مقدار کمینه بازمی‌گردد حال آن‌که در کارهای پیشین برای این نوع از ریزشبکه‌ها روند بهبود به چند دقیقه نیز می‌رسیده است و این مقایسه خود سرعت این روش در رسیدن به پایداری که بعد از حملات سایبری مهم می‌باشد را نشان می‌دهد زیرا هدف اصلی دشمن، ناپایداری و خاموشی سیستم می‌باشد، هم‌چنین برای بهبود این روش می‌توان با تنظیم ضرایب کنترلی روند میرایی فرکانس و ولتاژ را بهبود بخشید که برای آن استفاده از الگوریتم‌های هوشمند همانند منطق فازی به‌عنوان کار آینده پیشنهاد می‌گردد.

۱۲- مراجع

[1] S. Masoud Amin and B. F. Wallenberg, "Toward a smart grid: power delivery for the 21st century," Power and Energy Magazine, vol. 3, no. 5, pp. 34-41, September 2005.

[2] P. A. S. Ralston, J. H. Graham, and J. L. Heir, "Cyber security risk assessment for SCADA and DCS networks," ISA Transaction, vol. 46, pp. 583-594, April 2007.

[3] J. Weiss, "Key Issues for Implementing a Prudent Control System Cyber Security Program," Electric Energy T & D Magazine, March/April 2008.

[4] C. Ten, C. Liu, and M. Govindarasu," Vulnerability assessment of cybersecurity for SCADA systems," Power Engineering Society General Meeting, IEEE, pp. 1-8 and pp. 24-28, June 2008.

[5] H. Nikkhajoei and R. Iravani, "Steady-state model and power flow analysis of electronically-coupled distributed resource units," IEEE Transaction on Power Delivery, vol. 22, no. 1, pp. 721–728, October 2007.

[6] C. K. Sao and P. W. Lehn, "Control and power management of converter fed micro grid," IEEE Transactions on Power Systems, vol. 20, no. 2, pp. 1009–1016, April 2005.

[7] Ch. Hen, Y. Wang, and J. Lai, et al, "Design of parallel inverters for smooth mode transfer micro grid applications," IEEE Transaction on Power Electronics, vol. 25, no. 1, pp. 6–16, January 2010.

[8] J. Yul Kim and J. Joen, et al "Cooperative Control Strategy of Energy Storage System and Micro sources for Stabilizing the Micro grid during Islanded Operation," IEEE Transaction on Power Electronics, vol. 25, no. 12, pp. 3037-3048, December 2010.

[9] P. Thounthong, S. Rael, and B. Davat, "Analysis of super capacitor as second source based on fuel cell power generation," IEEE Transaction on Energy Conversation, vol. 24, no. 1, pp. 247–255, March 2009.

[10] L. Yowie, D. Mahinda, and V. Poh, et al, "Design, analysis, and real-time testing of a controller for multi bus micro grid system," IEEE Transaction on Power Electronics, vol. 19, no. 5, pp. 1195–1204, September 2004.

[11] Y. W. Li and C. N. Kao, "An accurate power control strategy for power electronics-interfaced distributed generation units operating in a low voltage multi bus micro grid," IEEE Transaction on Power Electronics, vol. 24, no. 12, pp. 2977–2988, December 2009.

[12] T. Tanabe, S. Suzuki, and Y. Ueda, et al "Control performance verification of power system stabilizer with an EDLC in islanded micro grid," IEEE Transaction on Power and Energy, vol. 129, no. 1, pp. 139–147, November 2009.

[13] J. A. P. Lopes, C. L. Moreira, and A. G. Madureira, "Defining control strategies for micro grids islanded operation," IEEE Transaction on Power Systems, vol. 21, no. 2, pp. 916–924, March 2006.

[14] T. Fleury, H. Khurana, and V. Welch, "Towards a taxonomy of attacks against energy control systems," Proceedings of IFIP Inter, March 2008.

[15] M. Panteli and D. S. Krischen, "Assessing the effect of failures in the information and communication infrastructure on power system reliability," Power System Conference and Exposition (PSCE), 21-23 March 2011.

[16] E. Vahedi, "Practical power system operation," IEEE Press, ch. 2, sec. 2.3, pp. 8-9, 2014.

Journal Of Electronical & Cyber Defence
Vol. 5, No. 2, 2017, Serial No. 18

Control Strategy to Maintain Stability of Micro-grids, During Occurring Cyber Attacks on the Power Grid

M. Rahmani, F. Faghihi*, B. Mozafari

*Islamic Azad University, Science and Research Branch of Tehran

(Received: 27/01/2016, Accepted: 03/01/2017)

ABSTRACT

This paper proposes the stability state of micro-grid in islanding mode during occurring cyber-attacks on the power networks. By controlling the rated frequency, it is possible to achieve stability. In order to control rapid frequency, the power balance between production and consumption in every moment must be established; it can be obtained using energy storage system such as batteries with fast dynamic response time. If the battery is designed well, it can lead to the frequency stability of the system by injecting or absorbing reactive power. To contribute more understanding of maximum battery capacity using, an efficient control strategy is designed and simulated via MATLAB/SIMULINK software.

Keywords: Cyber-attacks, Power Network Security, Cooperative Control, Micro-grid, Frequency Control

* Corresponding Author Email: Faramarz_Faghihi@hotmail.com