Scientific Journal of Electronic & Cyber Defense
Vol. 11, No. 4, Winter 2024, Serial No. 44
ISSN: 2322-4347 , E-ISSN: 2980-8979

Cyber disruption in the hierarchical control of intelligent microgrid power sharing

lotfoallah vakili *

* Master , Khorasgan University , Khorasgan , Iran

(Received: 2023/08/08, Revised: 2023/10/30, Accepted: 2023/12/20, Published: 2024/01/18)

DOR: https://dorl.net/dor/20.1001.1.23224347.1402.11.4.7.4

ABSTRACT

Cyberphysical systems have achieved rapid development over the past decade due to their widespread applications in various domains, and are typically composed of sensing, communication, computing, and actuation capabilities. However, the communication network of physical security systems may be attacked by cyber attacks, which significantly destroys the performance of the system. Recently, DOS denial-of-service attacks (1) have attracted a lot of attention. In this article, a solution to deal with DoS attacks on the power sharing control system of the electrical energy distribution network, including distributed generation, is presented. So that a time-varying distributed estimator has been used. Based on the feature of service interruption communication duration, the convergent design conditions of observer parameters are obtained using Lebag2 integral theory and average dwell time method. It is also shown that the observer errors converge. Finally, the presented coping method is placed on the virtual impedance control line 3 of the power sharing control system and will neutralize service interruption attacks .

Keywords: Physical security systems, DoS attacks, power sharing control, virtual impedance control .

* Corresponding Author Email: lv122000@yahoo.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال یازدهم، شماره ۴، زمستان ۱۴۰۲، ص۸۳-۹۲
شاپا الکترونیکی: ۸۹۷۹-۲۹۸۰ شاپا چاپی: ۴۳۴۷-۲۳۲۲

علمی – پژوهشی

اختلال سایبری در کنترل سلسه‌مراتبی تسهیم توان ریزشبکه هوشمند

لطف اله وکیلی [1*]

۱. کارشناسی ارشد، دانشگاه خوراسگان، ایران.

(دریافت: ۱۴۰۲/۰۵/۱۷، بازنگری: ۱۴۰۲/۰۸/۰۸، پذیرش: ۱۴۰۲/۰۹/۲۹، انتشار: ۱۴۰۲/۱۰/۲۸)
DOR: https://dorl.net/dor/20.1001.1.23224347.1402.11.4.7.4

ناشر: دانشگاه جامع امام حسین (ع)

چکیده

سیستم‌های سایبری فیزیکی به دلیل کاربردهای گسترده آن در حوزه‌های مختلف در طول دهه گذشته به توسعه سریع دست یافته‌اند و معمولاً با توانایی‌های سنجش، ارتباط، محاسبات و فعال‌سازی تشکیل‌شده‌اند. بااین‌حال، شبکه ارتباطی سیستم‌های امنیت فیزیکی ممکن است توسط حملات سایبری مورد حمله قرار گیرد که عملکرد سیستم را به طور چشمگیری از بین می‌برد. اخیراً حملات قطع سرویس (DOS) توجه زیادی را به خود جلب کرده است. در این مقاله راهکاری برای مقابله با حملات DoS به سیستم کنترل تسهیم توان شبکه توزیع انرژی الکتریکی شامل تولیدات پراکنده ارائه‌شده است. طور یکه یک تخمین‌گر توزیع‌شده متغیر با زمان بکار برده شده است. بر اساس ویژگی مدت‌زمان ارتباط قطع سرویس، شرایط طراحی همگرا پارامترهای ناظر با استفاده از تئوری انتگرال لبگ و روش میانگین زمان ماند به دست می‌آید. همچنین نشان‌داده‌شده است که خطاهای ناظر همگرا می‌شوند. درنهایت روش مقابله ارائه‌شده بر روی خط کنترل امپدانس مجازی سیستم کنترل تسهیم توان قرار گرفته و حملات قطع سرویس را خنثی خواهد کرد.

کلید واژه‌ها: سیستم‌های سایبری فیزیکی، حملات *DoS* ، کنترل تسهیم توان، کنترل امپدانس مجازی.

۱- مقدمه

در میان متصدیان مهندسی برق محاسن محیطی انرژی تجدیدپذیر تأمین انرژی الکتریکی جاافتاده است. بااین‌وجود عدم بازگشت سرمایه‌های کلان مربوط به منابع انرژی تجدیدپذیر، استفاده از چنین منابع انرژی را با مشکل مواجه کرده است. هنوز سیستم‌های استفاده از منابع تغذیه سنتی مرسوم است بااین‌وجود به دلیل مسائلی مانند عدم ثبات قیمت نفت، هزینه‌های تعمیر و نگه‌داری بالا و ازدیاد آلایندگی در تولید((CO2)) استفاده از این منابع را برای دست‌اندرکاران مهندسی برق چالش‌برانگیز کرده است. راه‌حل فائق آمدن به این مسائل ترکیب انرژی تجدیدپذیر و منابع تغذیه سنتی در ریزشبکه‌های هوشمند است. ریزشبکه یا میکرو گرید، یک سیستم تولید و توزیع انرژی الکتریکی است که از بخش‌های مختلفی از جمله تولید پراکنده، سیستم‌های ذخیره انرژی، بارها و تجهیزات حفاظتی تشکیل شده است. ریزشبکه هوشمند سیستمی خودگردان است که قابلیت کنترل و مدیریت خود را داراست. گاهی در یک ریزشبکه انرژی، مصرف‌کنندگان علاوه بر انرژی الکتریکی، انرژی گرمایی برای گرمایش و سرمایش نیز دریافت می‌کنند. مهم‌ترین مزایای یک ریزشبکه به شرح زیر است:

- منابع توان کنترل پذیر و سیستم‌های ذخیره انرژی در یک ریزشبکه، می‌توانند تغییرات تولید توان منابع تجدیدپذیر را مدیریت و کنترل کرده و درنتیجه، کیفیت توان را بهبود دهند.
- یک ریزشبکه می‌تواند خدمات متنوعی به همه بارها ارائه کند؛ برای مثال، بارهای مهم را با توان مطمئن تغذیه کند، درحالی‌که بارهای بااهمیت کمتر را با توان ارزان‌تر و قابلیت اطمینان پایین‌تر تأمین نماید.
- در شبکه‌های توزیع، ریزشبکه، مانند یک منبع یا بار مجازی عمل می‌کند؛ بنابراین، اصلاح پیک‌بار را می‌توان از طریق کنترل هماهنگ شده تولید پراکنده و بارها محقق کرد. علاوه بر این، اثرات نامطلوب نفوذ تولیدات پراکنده را

*Corresponding Author E-mail: lv122000@yahoo.com

می‌توان با ریزشبکه‌ها کاهش داد و درنتیجه به کاربرهای شبکه توزیع برای مدیریت ساده‌تر آن کمک کرد.

- ریزشبکه‌ها، به دلیل توانایی عملکرد مستقلی که دارند، با خودترمیمی پس از وقوع خطا، به کمک شبکه‌های توزیع می‌آیند.

- یک ریزشبکه می‌تواند متشکل از مصرف‌کننده‌ها، شرکت‌های برق یا شرکت‌های ثالث مستقل باشد. این نوع رابطه و عملکرد چندجانبه، همه سهام‌داران را تشویق می‌کند تا به ساخت و گسترش منابع انرژی تجدیدپذیر ترغیب شده و تغییرات اساسی مدل بازار و سازوکارهای انرژی را ترویج دهند.

۲- بیان مساله

در دهه‌های گذشته توسعه شبکه‌های برق با پیشرفت‌های صنعتی و اجتماعی همگام نشده است. به‌طوری‌که در کشورهای توسعه‌یافته از دهه ۱۹۵۰ تاکنون تولید و مصرف انرژی به‌ترتیب تقریباً دو سه برابر افزایش یافته است.[۱] به‌طور خاص خدمات عمومی/ تجاری، صنعت و مناطق مسکونی بیشترین تقاضای برق را داشته‌اند. راه حل چالش اساسی افزایش تقاضا، مدیریت موثر انواع انرژی از جمله منابع سوخت فسیلی سنتی و منابع انرژی تجدیدپذیر است. [۲] بنابراین تلاش‌های بین‌المللی برای توسعه سیستم برق نسل جدید تحت عنوان "شبکه هوشمند[1]" آغاز شده است. [۳]

در مقایسه با سیستم‌های قدرت سنتی، شبکه هوشمند فن آوری‌های ارتباطی پرسرعت و دوطرفه [۴] را به طور کامل در میلیون‌ها تجهیز برق ادغام می‌کند تا زیرساختی پویا و تعاملی با قابلیت‌های جدید مدیریت انرژی مانند اندازه‌گیری پیشرفته زیرساخت (AMI[2]) [۵] و پاسخ تقاضا[3] [۶] ایجاد کند. چنین وابستگی شدیدی به شبکه‌های اطلاعاتی شبکه هوشمند را از لحاظ سیستم‌های ارتباطی و شبکه‌ای آسیب‌پذیر می‌کند. در واقع عملکرد قابل‌اعتماد و ایمن سیستم برق به خطر خواهد افتاد. به‌عنوان‌مثال نفوذ بالقوه دشمنان در شبکه منجر به انواع عواقب شدید در شبکه هوشمند از قبیل انتشار اطلاعات مشتری یا حتی خاموشی گسترده و تخریب زیرساخت‌ها خواهد شد. [۷]

بنابراین، هدف این مقاله، بررسی مسائل امنیتی،سایبری در ریزشبکه هوشمند می باشد. این مسئله برای طراحی شبکه‌های اطلاعاتی بسیار مهم است و به‌عنوان یکی از بالاترین اولویت‌های هوشمندسازی شبکه است. ازآنجاکه تحقیقات در مورد امنیت سایبری برای شبکه هوشمند هنوز در مراحل اولیه است [۸]، ابتدا به ارائه یک مرور کلی، تجزیه‌وتحلیل تهدیدات احتمالی امنیت سایبری خواهیم پرداخت.

۳- مروری بر ادبیات تحقیق

حفاظت در برابر حملات سایبری DoS[4] با گسترش جنگ نرم در دهه اخیر از اهمیت ویژه‌ای برخوردار شده است. سیستم‌های کنترل تسهیم توان به دلیل حساسیت بالای عدم خاموشی شبکه توزیع هوشمند از این قاعده مستثنی نبوده است.

در [۹] بررسی جامع از مسائل امنیت سایبری برای شبکه هوشمند ارائه‌شده است. این مرجع بر الزامات امنیتی، آسیب‌پذیری شبکه، اقدامات متقابل حمله، پروتکل‌های ارتباطی ایمن و معماری شبکه هوشمند متمرکز شده است. هدف ارائه درک عمیق از آسیب‌پذیری‌ها و راه‌حل‌های امنیتی در شبکه هوشمند و روشن کردن رهنمودهای تحقیقاتی آینده برای امنیت آن است.

در [۱۰] چارچوب کنترل سلسله مراتبی امنیتی شامل ناظران انعطاف‌پذیر و غیرمتمرکز ارائه‌شده است. کنترل‌کننده‌های سازگار تحت حملات DoS ارائه‌شده است. لذا ابتدا یک برآورد توزیع شده جدید برای هر زیرسیستم ساخته شده تا اطمینان حاصل شود که بزرگی حالت هر تخمینگر بزرگتر از محدوده مشتق مرتبه نهم مسیر مرجع پس از زمان نامشخص است. با مطالعه سیستم حلقه بسته حاصل، ثابت شده است که خطاهای ردیابی خروجی به یک مجموعه فشرده با روش پیشنهادی نزدیک می‌شوند.

در [۱۱] به مشکل تقسیم توان راکتیو میکرو شبکه تحت حملات DoS (انکار سرویس) می‌پردازد. در مرجع تقسیم دقیق توان راکتیو مبتنی بر روش به روزرسانی متناوب ناشی از رویداد پیشنهاد شده است، که می‌تواند برخی از ارتباطات را کاهش دهد و از پدیده زنو جلوگیری کند. با توجه به اینکه مهاجمان ممکن است حملات *DoS* را به شبکه هوشمند آغاز کنند، تحمل حملات DoS از سیستم کنترل توان راکتیو بررسی شده است.

در [۱۲] مشکلات کنترل امنیت سایبری برای تسهیم جریان بار و ترمیم ولتاژ یک میکروگرید جزیره‌ای با جریان مستقیم تحت حملات DoS مورد بررسی قرارگرفته است. برای اطمینان از عملکرد پایدار سیستم تحت حملات DoS، روش کنترل ارتجاعی توزیع شده در لایه کنترل ثانویه پیشنهاد شده است. با

[1] Smart Grid
[2] Advance Metering Infra-structur
[3] Demand Response
[4] Denial Of Service

توجه به حملات DoS، روش کنترل پیشنهادی نه تنها ترمیم ولتاژ باس را انجام داده بلکه بهینه‌سازی تسهیم جریان را انجام می‌دهد. علاوه بر این، علی‌رغم اکثر روش‌های کنترل ثانویه موجود با نرخ نمونه‌گیری ثابت، مکانیسم نمونه‌گیری جدید انعطاف‌پذیر در لایه ثانویه طراحی شده است تا امنیت کل سیستم را در برابر حملات DoS بهبود بخشد.

۴- مدل‌سازی تسهیم توان در شبکه توزیع هوشمند

سیستم‌های تولید پراکنده (DG[1]) طرحی مناسب برای ارائه منبع تغذیه الکتریکی با قابل‌اعتماد بالا ارائه می‌دهد. [۱۳] این مفهوم به‌ویژه زمانی جالب است که انواع مختلفی از منابع انرژی مانند پنل‌های فتوولتائیک، سلول‌های سوختی یا توربین‌های بادی در دسترس باشند. [۱۴]، بیشتر بخش‌های این منابع برای ایجاد شبکه‌های AC محلی نیاز به اینورتر الکترونیک قدرت دارند. به‌این‌ترتیب اینورترها یا مبدل‌های dc به ac به یک باس‌بار مشترک ac باهدف اشتراک‌گذاری مناسب بارهای پراکنده است. از این نظر چندین تکنیک کنترل بر اساس روش کنترل افتی پیشنهاد شده است. برای دستیابی به اشتراک توان، حلقه کنترل تنظیمات دقیقی را روی فرکانس ولتاژ خروجی و دامنه ولتاژ اینورتر انجام می‌دهد تا عدم تعادل توان اکتیو راکتیو را جبران کند. این مفهوم از تئوری سیستم قدرت نشأت می‌گیرد که در آن یک ژنراتور متصل به برق شهری فرکانس خود را با افزایش توان موردنیاز کاهش می‌دهد. [۱۵]

طرح‌های کنترل زیادی بر اساس روش افتی[2] برای به اشتراک گذاشتن بارهای خطی وجود دارد. [۱۶] بااین‌وجود، امروزه تکثیر بارهای غیرخطی به یک مشکل تبدیل شده است، زیرا واحدها باید هم جریان هارمونیک مشترک داشته باشند و هم توان فعال و راکتیو را متعادل کنند. این تکنیک دارای دو محدودیت اصلی است: کنترل‌کننده از الگوریتمی استفاده می‌کند که برای محاسبه محتوای جریان هارمونیک بسیار پیچیده است، و اشتراک جریان هارمونیک به قیمت کاهش پایداری سیستم به دست می‌آید. اخیراً حلقه‌های کنترلی جدیدی که امپدانس خروجی واحدها را با افزودن مقاومت‌های مجازی [۱۷] یا رآکتورها [۱۸] تنظیم می‌کنند، در روش افتی گنجانده شده‌اند تا محتوای جریان هارمونیک را به‌درستی به اشتراک بگذارند.

۵- سری فوریه و مفهوم هارمونیک

هارمونیک‌های سیستم قدرت عبارت‌اند از جریان‌ها ولتاژهای سینوسی در فرکانس‌هایی که مضرب‌های صحیحی از فرکانس اصلی هستند . آن‌ها اجزای اعوجاج[3]زا برای شکل موج ولتاژ و جریان بار را می‌سازند. بااین‌حال با افزایش محتوای میان هارمونیک‌هایی[4] که مضرب صحیحی از فرکانس اصلی نیستند می‌طلبد که توجه ویژه‌ای به آن‌ها کرد.

طبق نظریه فوریه هر موج پریودیک $x(t)$ با دوره تناوب T را می‌توان به‌صورت مجموع بی‌نهایت تابع سینوسی و کسینوسی نوشت به‌طوری که [۱۹]:

$$x(t) = a_0 + \sum_{n=1}^{\infty}\left\{a_n \cos(\frac{2\pi nt}{T}) + b_n \sin(\frac{2\pi nt}{T})\right\} \quad (۱-۵)$$

به‌طوری که شامل یک موج اصلی با فرکانس اصلی است که بیشترین دامنه را دارد و هرچه فرکانس جملات بعد به‌صورت مضرب صحیح از موج اصلی افزایش می‌یابد و از آن کم می‌شود.

با ارائه چنین نظریه ارزشمند در زمینه تحلیل سیگنال‌های الکتریکی، هر سیگنال پریودیک را به‌صورت بی‌نهایت سیگنال سینوسی و کسینوسی نوشت که به سیگنال با بیشترین دامنه، هارمونیک اصلی و به جملات با فرکانس بالاتر هارمونیک‌های موج داده شده می‌گویند.

معروف‌ترین شاخص هارمونیکی موج ولتاژ *THD* یا شاخص اعوجاج هارمونیکی کل نام دارد و عبارتنداز درصد مقدار مؤثر هارمونیک‌ها نسبت به هارمونیک اصلی.

$$THD = \frac{\sqrt{\sum_{n=2}^{N} V_n^2}}{V_1} \quad (۲-۵)$$

که V_n مقدار ولتاژ مؤثر هارمونیک n ام، N ماکزیمم مرتبه هارمونیکی است که باید لحاظ شود، V_1 مقدار مؤثر ولتاژ هارمونیک اصلی است.

۶- سیستمهای حفاظت سایبر

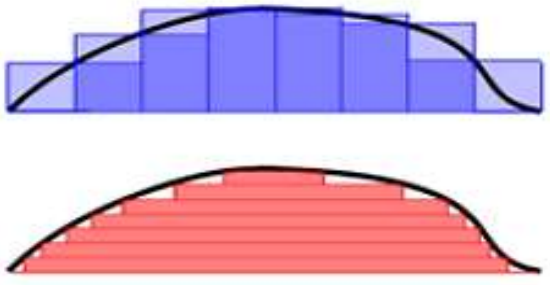
در طول دهه گذشته مسائل کنترل تطبیقی توزیع شده برای سیستم‌های حالت چندعاملی[5] غیرخطی شامل عدم قطعیت به طور گسترده موردمطالعه قرار گرفته است. [۲۰] ایده اصلی روش کنترل سیستم‌های حالت چندعاملی با استفاده از تخمین آنلاین پارامترهای ناشناخته است. هدف کنترل مسئله ردیابی مسیر مرجع متغیر با زمان برای هر زیرسیستم با استفاده از اطلاعات توزیع شده است. چالش‌های اصلی را می‌توان در دو جنبه زیر خلاصه کرد. اولاً نحوه تخمین مسیر مرجع متغیر با زمان در حضور حملات *DoS* که باعث می‌شود اطلاعات ارسال شده از همسایگان در دسترس نباشد. ثانیاً چگونگی یافتن تابع لیاپانوف مناسب برای تجزیه‌وتحلیل پایداری سیستم است. در حملات *DoS* عموماً مسیر تبادل اطلاعات بسته می‌گردد. برای بسط مسائل مربوطه توجه به نمادهای زیر ضروری است.

[4]Distributed Generation
[5]Droop
[6]Distortion
[7]Inter-Harmonic
[8]Multi-Agent system

برای بردارهای $xi \in R^m$، بردار $col\{x_1, ..., x_N\}$ با $[x^T_1, ..., x^T_N]^T$ نشان داده می‌شود. I و ۰ به ترتیب نشان‌دهنده ماتریس همانی و ماتریس صفر (بردار) هستند. $diag\{N_1, ..., N_m\}$ ماتریسی را با ماتریس‌های N_1، و ...، N_m در قطر اصلی آن نشان می‌دهد. $col\{1\} \in R^N$=۱. فرض کنید $A \in R^N$ یک ماتریس باشد، سپس $(\lambda_A = min_{i=1,...,N} \lambda_i(A$ و $\lambda_A = max_{i=1,...,N} \lambda_i(A$) بیانگر حداقل و حداکثر مقادیر ویژه A است. تعریف $\mu(S\ NU\{0\} := N_0)$ نشان‌دهنده اندازه لب گ[1] f روی مجموعه S یعنی $(S.f_S f d\mu = f_S f(\tau) d\mu(\tau$ است.

۷- انتگرال لبگ[2]

در ریاضیات، انتگرال یک تابع نامنفی تک‌متغیره را می‌توان در ساده‌ترین حالت، مساحت بین نمودار تابع و محور x ها در نظر گرفت. انتگرال لبگ مفهوم انتگرال‌گیری را به دسته بزرگ‌تری از توابع گسترش می‌دهد. همچنین این نوع انتگرال‌گیری دامنه‌ای که این توابع بر روی آن‌ها انتگرال‌گیری می‌شوند را نیز گسترش می‌دهند. در روش انتگرال‌گیری ریمان، بازه‌های انتگرال‌پذیری به تعدادی متناهی زیر بازه تقسیم می‌شد در روش لبگ به مجموعه‌های کلی‌تری به نام مجموعه‌های اندازه‌پذیر تقسیم می‌شوند. خیلی قبل‌تر از قرن بیستم، ریاضی‌دانان می‌دانستند که برای توابع نامنفی که نمودار آن به‌اندازه کافی هموار باشد، مثل توابع پیوسته بر روی بازه‌های کراندار بسته، مساحت زیر نمودار را می‌توان با کمک روش‌های تقریب‌زدن با چند ضلعی‌ها حساب کرد. بااین‌حال همچنان که توجهات بیشتری به سمت توابع نامنظم‌تر جلب شد (به‌عنوان‌مثال توابعی که از فرایند حدگیری در نظریه احتمال آنالیز ریاضی به وجود می‌آیند)، بیش‌ازپیش مشخص شد که برای تعریف انتگرال‌گیری از چنین توابعی، نیاز به تکنیک‌های تقریب محتاطانه‌تری وجود دارد. همچنین ممکن است بخواهیم بر روی فضاهایی کلی‌تر از خط حقیقی انتگرال‌گیری کنیم. انتگرال لبگ تجریدهای لازم برای این کار مهم را فراهم می‌آورد. اصطلاح انتگرال‌گیری لبگ می‌تواند هم به معنی نظریه کلی انتگرال‌گیری توابع باتوجه‌به یک اندازه کلی معرفی شده توسط لبگ باشد، یا در حالت خاص‌تر همان انتگرال‌گیری توابع روی بخشی از اعداد حقیقی باتوجه‌به اندازه لبگ. در شکل مقایسه شهودی انتگرال ریمان و لبگ نشان‌داده‌شده است.



شکل۱: مقایسه شهودی انتگرال ریمان (شکل بالایی) و انتگرال لبگ

۸- امپدانس مجازی

استفاده از اینورترهای موازی برای افزایش قابلیت اطمینان سودمند است و همچنین یکی از ویژگی‌های ریزشبکه‌های جزیره‌ای است. بااین‌حال نیز چالش‌هایی را به همراه دارد. تولید جریان‌های گردشی یکی از این موارد است که در این قسمت ارائه خواهد شد.

واحدهای تولید پراکنده که به‌موازات ولتاژهای خروجی مختلف، امپدانس خروجی یا فاز کار می‌کنند، می‌توانند نه‌تنها جریان‌هایی را از تولید به بارها بلکه بین واحدهای تولیدکننده نیز ایجاد کنند. این جریان‌ها به‌عنوان جریان‌های گردشی شناخته می‌شوند و می‌توانند بزرگ و بالقوه آسیب‌رسان باشند. در یک شبکه برق سنتی با ژنراتورهای سنکرون بزرگ، امپدانس‌های خط معمولاً این جریان‌ها را کاهش می‌دهند، درحالی‌که امپدانس‌های خط کوچک‌تر در ریزشبکه‌ها، جریان‌های در گردش را به یک چالش بزرگ تبدیل می‌کنند.

جریان‌های گردشی می‌توانند منجر به افزایش تلفات و اضافه‌بار اینورترها، علاوه بر کاهش کیفیت توان و راندمان شوند. ازآنجایی‌که ولتاژها در ریزشبکه‌های جزیره‌ای توسط اینورترهای موازی تنظیم می‌شوند، چالش‌های مربوط به جریان‌های گردشی در این حالت عملکرد موردتوجه ویژه‌ای هستند. اگر دو اینورتر هر کدام ۵۰ درصد بار را تغذیه کنند، جریان گردشی ایجاد نمی شود. با داشتن بار نسبی یکی از اینورترها که با حالت ایده‌آل متفاوت است، جریان‌های گردشی ممکن است ایجاد شود که باعث مشکلات فوق‌الذکر می‌شود. این حالت معمولاً برای دو اینورتر با ولتاژ خروجی برابر، اما امپدانس خط متفاوت است. در یک سیستم سه فاز نامتعادل، جریان‌های در گردش می‌توانند بین فازها اتفاق بیفتند و چالش را پیچیده‌تر می‌کنند. اختلاف بین دو اینورتر جریان خروجی اکتیو جریان گردشی اکتیو را ایجاد می کند، در حالی که اختلاف بین جریان های راکتیو جریان گردشی راکتیو را ایجاد می‌کند.

برای حداقل رساندن جریان‌های گردشی حالت پایدار امپدانس مجازی در محاسبات سیستم کنترلی می‌تواند برای این منظور استفاده شود. افزودن مقاومت مجازی باعث می‌شود که

[9] Lebesgue Measure
[2] Lebesgue

نوسانات سیستم کمتر شود. [۲۱] برخلاف مقاومت فیزیکی، مقاومت مجازی هیچ تلفات توانی ندارد و می‌توان آن را بدون کاهش بازده پیاده‌سازی کرد. همچنین اندوکتانس مجازی برای اطمینان از جداسازی P و Q قابل‌استفاده است؛ بنابراین امپدانس مجازی، کنترل‌کننده‌های افتی را پایدارتر می‌کند. [۲۲] امپدانس مجازی را می‌توان همان‌طور که در زیر نشان‌داده‌شده است، به دست آورد. R_v و L_v مقاومت و اندوکتانس مجازی هستند.

$$v_{V\alpha} = R_v.i^{+}_{O\alpha} - L_v.\omega.i^{+}_{O\beta} \quad (۱-۸)$$

$$v_{V\beta} = R_v.i^{+}_{O\beta} + L_v.\omega.i^{+}_{O\beta} \quad (۲-۸)$$

تنها جریان توالی مثبت از امپدانس مجازی عبور می‌کند. به‌این‌ترتیب از افزایش عدم تعادل ولتاژ خروجی DG به دلیل افت توالی منفی ولتاژ روی امپدانس مجازی جلوگیری می‌شود.

بنابراین، چنانچه خط مربوط به کنترل امپدانس مجازی دچار حمله سایبری شود، عملکرد سیستم مختل خواهد شد.

۹- حملات DoS

تحت حملات DoS خط ارتباطی متوقف می‌شود. اگر $\iota^{(i,j)} = [h_s^{ij}, h_s^{ij} + \tau_s^{ij})$، sامین بازه‌ای باشد که در طی آن ارتباط بین i و j مسدود می‌شود. $\{h^{ij}{}_s\}$ و $\{h^{ij}{}_s + \tau^{ij}{}_s\}$ دنباله‌ای از گذار روشن/خاموش حملات DoS را نشان می‌دهند. $\tau^{ij}{}_s$ نشان دهنده طول حمله sام است. فرض کنید $\prod_D^{(i,j)}(t1,t2) := \cup_{s=1}^{\infty} \iota_s^{(i,j)} \cap (t1,t2)$ مجموعه‌ای باشد که در آن ارتباط بین i و j در طول $(t1, t2)$ مسدود شده است):

$$\prod\nolimits_D(t_1,t_2) := [t_1,t_2] \bigcap \bigcup_{(i,j)\in\varepsilon} \prod\nolimits_D^{(i,j)}(t_1,t_2) \quad (۱-۹)$$

$$\prod\nolimits_N(t_1,t_2) := [t_1,t_2] \setminus \prod\nolimits_D(t_1,t_2)$$

که در آن $\Pi_D(t1, t2)$ مجموعه‌ای است که در آن حداقل یک یال مورد حمله قرار می‌گیرد،

و $\Pi_N(t1, t2)$ مجموعه‌ای است که همه شبکه‌ها به طور عادی کار می‌کنند.(مدت DoS) [۱۸]: ثابت‌های مثبت $\zeta > 0$ و $T > 1$ وجود دارد به‌طوری که:

$$\mu(\prod\nolimits_D(0,t)) < \xi + \frac{t}{T} \quad \forall t \geq 0 \quad (۲-۹)$$

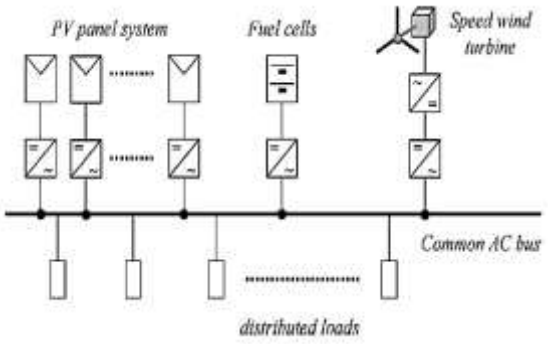
حملات DoS ممکن است در هر کانالی در نمودار G رخ دهد. محدودیت حملات DoS این است که $unionD(0, t)$ فواصل حملات DoS شرایط مدت‌زمان ارتباط DoS در فرض ۲ را برآورده می‌کند. هدف کنترل، طراحی کنترل‌کننده غیرمتمرکز تطبیقی مبتنی بر ناظران انعطاف‌پذیر توزیع‌شده به‌گونه‌ای است که ویژگی‌های زیر حفظ شود.

۱) همگرایی مجانبی خطای ردیابی خروجی $Yi(t)-Yr(t)$ را می‌توان تضمین کرد که اندازه‌گیری حملات DoS مجموعه $D(0)$، ∞) محدود باشد، یعنی $\mu(D(0), \infty)) < \infty$.

۲) خطای ردیابی خروجی زمانی که $\mu(D(0), \infty)) = \infty$ به صورت سراسری یکنواخت محدود می‌شود.

۱۰- روش کنترل سلسله مراتبی

شکل زیر یک سیستم DG را نشان می‌دهد که از انواع مختلفی از منابع، مانند پانل‌های خورشیدی، سلول‌های سوختی و توربین‌های بادی سرعتی تشکیل شده است. هر منبعی برای انتقال انرژی به باس مشترک نیاز به یک رابط توان الکتریکی دارد. همان‌طور که در ***Error! Reference source not found.*** نشان‌داده‌شده است، می‌توانیم هر واحد را به‌عنوان یک اینورتر متصل به باس مشترک از طریق یک امپدانس جداسازی مدل کنیم.



شکل ۲: سلسله مراتبِ DG

معمولاً امپدانس خروجی اینورتر بسیار القایی است. ازاین‌رو، توان‌های اکتیو،راکتیو کشیده شده به باس را می‌توان به‌صورت زیر بیان کرد.

$$P = \frac{EV}{X}\sin\phi \quad (۱-۱۰)$$

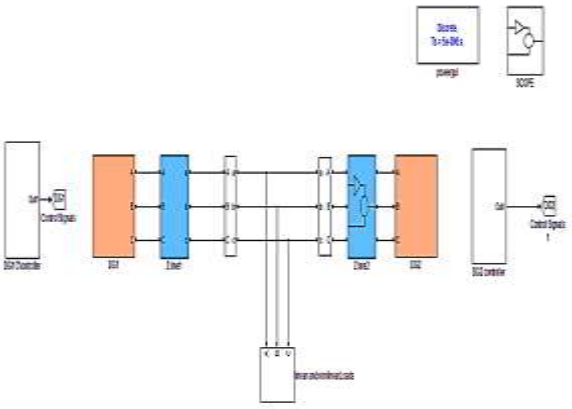
$$Q = \frac{EV\cos\phi - V^2}{X}$$

که X راکتانس خروجی اینورتر، φ زاویه فاز بین ولتاژ خروجی اینورتر ولتاژ شین مشترک است و E و V به ترتیب دامنه ولتاژ خروجی اینورتر ولتاژ بار است. از معادلات فوق می‌توان نتیجه گرفت که توان اکتیو P عمدتاً به زاویه توان وابسته است، درحالی‌که توان راکتیو Q بیشتر به دامنه ولتاژ خروجی بستگی دارد. درنتیجه اکثر کنترل بی‌سیم اینورترهای موازی از روش سلسله‌مراتبی معمولی استفاده می‌کنند.

واضح است که اگر ضرایب افت افزایش یابد، آنگاه اشتراک توان خوبی به قیمت کاهش تنظیم ولتاژ حاصل می‌شود. به‌عنوان‌مثال، انحرافات فرکانس و دامنه اغلب در ۲٪ و ۵ می‌تواند قابل‌قبول باشد. مصالحه ذاتی این طرح ضرایب ذکر شده را محدود می‌کند و می‌تواند محدودیت جدی از نظر پاسخ گذرا، دقت اشتراک توان و پایداری سیستم باشد. از سوی دیگر برای انجام توابع افت، لازم است مقدار متوسط در یک سیکل خط خروجی توان لحظه‌ای فعال و راکتیو محاسبه شود. می‌توان با استفاده از فیلترهای پایین گذر با پهنای باند کمتر از اینورتر حلقه بسته پیاده‌سازی کرد. درنتیجه فیلترهای محاسبه توان و ضرایب افت، تا حد زیادی دینامیک و پایداری اینورترهای موازی را تعیین می‌کنند. پدیده‌های میرایی و نوسانی اختلاف تغییر فاز می‌تواند باعث ناپایداری‌ها و جریان گردشی گذرا زیاد شود که می‌تواند باعث اضافه‌بار و آسیب به واحدها شود. درنتیجه روش سلسه‌مراتبی معمولی چندین مشکل ذاتی مرتبط با پاسخ گذرا دارد؛ بنابراین از اصلاح امپدانس مجازی استفاده خواهد شد.

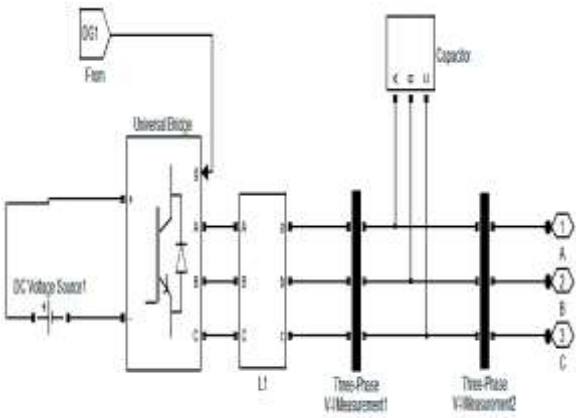
۱۱- سیستم پیشنهادی

یک شبکه توزیع هوشمند شامل دو واحد DG جریان مستقیم در کنترل تسهیم توان حضور دارند. در شکل(۳) شمای پیاده‌سازی شده در نرم‌افزار MATLAB/SIMULINK نشان‌داده‌شده است.



شکل ۳: مدل کلی تسهیم توان شبکه هوشمند

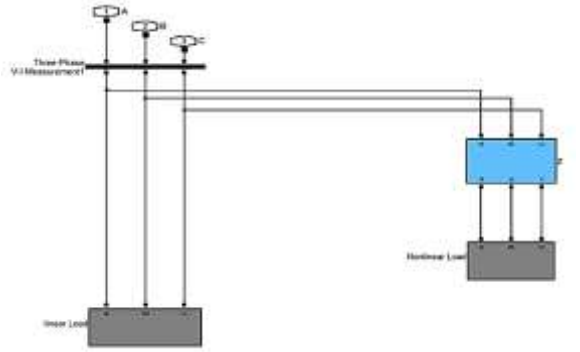
روش پیشنهادی بر روی سیستم شامل DG که بهترین حالت برای بررسی است، مناسب خواهد بود. بااین‌حال مطابق مطالعات گذشته برای هر تعداد واحد قابل‌اعمال می‌باشد. واحد DG اول و دوم با ولتاژ تغذیه ۶۵۰ ولت مستقیم تغذیه می‌شوند. اندوکتانس داخلی هر واحد ۱٫۸ میلی هانری است. شمای داخلی آن مطابق شکل (۴) پیاده‌سازی شده است.



شکل ۴: مدل DGها

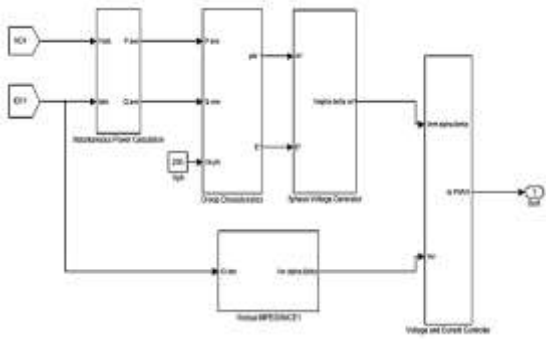
پل اینورتری با سه بازوی شامل IGBT و دیود ولتاژ DC را با فرکانس ۱۰کیلوهرتز به ولتاژ متناوب تبدیل می‌کند. بلوک‌های *L1* و Capacitor به ترتیب ماهیت سلفی و خازنی DG را مدل خواهند کرد.

مطابق شکل (۴) امپدانس سری خطوط DG اول و دوم که شامل مقاومت و اندوکتانس در هر فاز است، بترتیب مقادیر ۰٫۲ اهم، ۳٫۶ میلی‌هانری و ۰٫۱ اهم و ۱٫۸ میلی‌هانری را دارد. بدین ترتیب قدرت منبع تولید پراکنده اول حداقل نصف منبع تولید پراکنده دوم است. مدل بار مجموعه مطابق شکل (۵)می باشد.



شکل ۵: مدل بار شبکه هوشمند

مطابق شکل(۵) بارها شامل دو قسمت خطی و غیرخطی هستند. مدار کنترلی نمونه DGها در شکل(۶) نشان‌داده‌شده است.

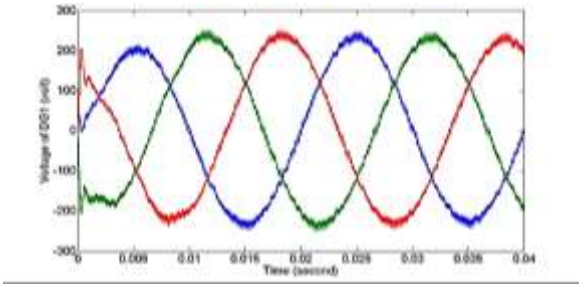


شکل ۶: مدار کنترلی نمونه DG ها شامل امپدانس مجازی

مطابق شکل ابتدا نمونه جریان‌های لحظهای برای محاسبه توان اکتیو ،راکتیو استفاده شده تا مطابق معادله **Error! Reference source not found.** در مشخصه افتی قرار گیرند. بلوک امپدانس مجازی به مدل اضافه گردیده تا نوسانات عدم تعادل توان را فروبنشاند.

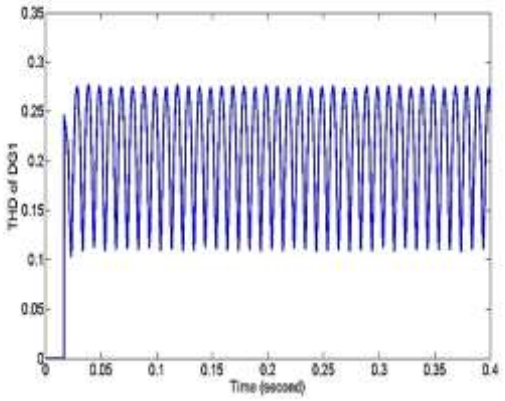
۱۱- نتایج شبیه‌سازی

در شکل(۷) ولتاژ و جریان لحظه‌ای ولتاژ ترمینال DG1 نشان‌داده‌شده است.



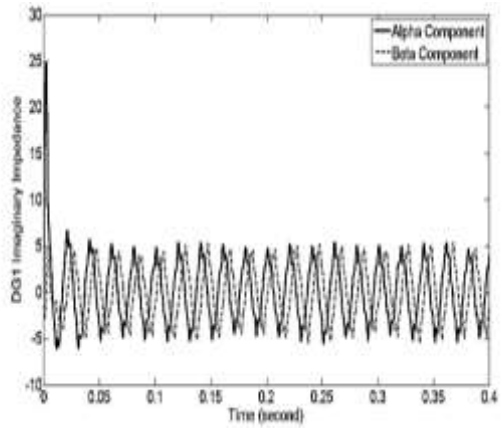
شکل۷: ولتاژ سه‌فاز لحظه‌ای ولتاژ ترمینال DG1

در شکل (۸) محتوای هارمونیکی ولتاژ با استفاده از شاخص THD بصورت لحظه‌ای نشان داده‌شده است.



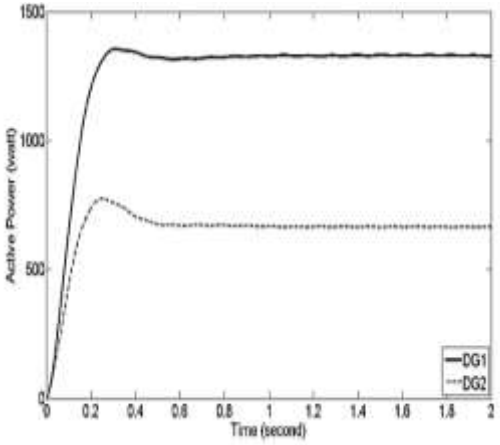
شکل ۸: محتوای هارمونیکی ولتاژ ترمینال DG

در شکل(۹) امپدانس مجازی اضافه شده به سیستم کنترل افتی DG1 نشان‌داده‌شده است. سیستم کنترل برداری مطابق قسمت (۸) می‌تواند با وجود محتوای هارمونیکی فوق وظیفه کنترل تسهیم توان را به‌خوبی انجام دهد.

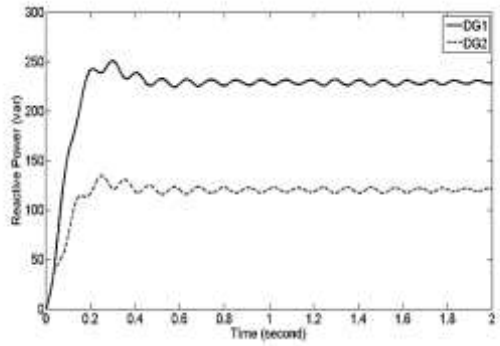


شکل۹: امپدانس مجازی جبرانگر

با استفاده از امپدانس مجازی جبرانگر فوق کنترل تسهیم توان به‌صورت دقیق مطابق شکل(۱۰) و(۱۱) انجام شده است.

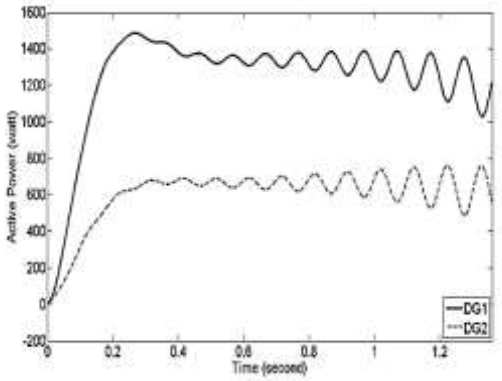


شکل ۱۰: تسهیم توان اکتیو

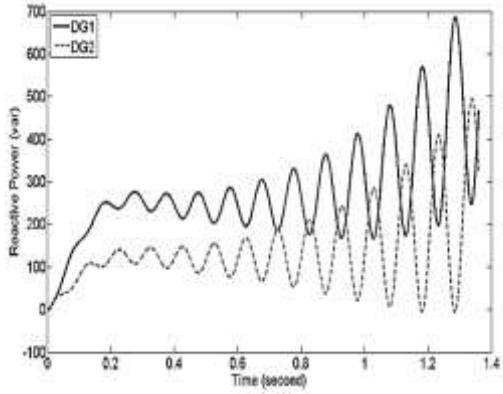


شکل ۱۱: تسهیم توان راکتیو

هدف از حفاظت سایبری در این مقاله، حفاظت از حملات DoS بر روی خط امپدانس مجازی DGها است. در شکل(۱۲) وشکل توان‌های اکتیو،راکتیو DGها در صورت قطع کامل خط امپدانس مجازی نشان‌داده‌شده است.



شکل ۱۲: توان‌های اکتیو دو DG درصورت قطع خط امپدانس

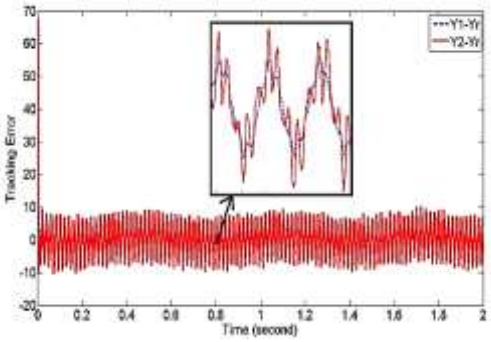


شکل ۱۳: توان‌های راکتیو دو DG درصورت قطع خط امپدانس

همان‌طور که در این دو شکل دیده می‌شود قطع خطوط امپدانس مجازی در اثر حمله سایبری موجب نوسانات شدید ولتاژ، جریان و بالطبع توان شده و شبکه هوشمند را ناپایدار کرده و موجب خاموشی بار خواهد شد.

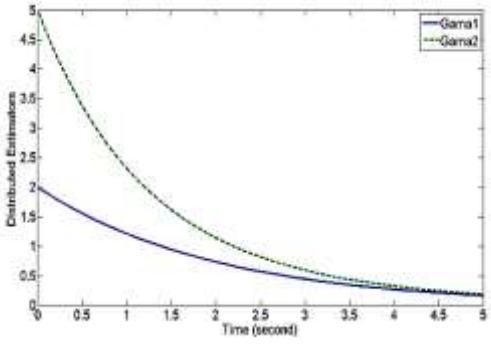
چنانچه بازه‌های حمله سایبری به خطوط ۱، ۲، ۲، ۱ و ۱ بترتیب در بازه‌های ۰,۶۵۶ باشد. اگر ضرایب Θ_1 و Θ_2 بترتیب برابر ۱ و ۰,۵، توابع غیرخطی $\phi_{1,1}$، $\phi_{2,1}$، $\phi_{1,2}$ و $\phi_{2,2}$ بترتیب برابر $sin(X_{1,1})$، $sin(X_{2,1})$، $X_{1,2}$و $X_{2,2}{}^2$ باشد و اختلال خروجی با ضابطه‌ها ی $D_1(t) = sin(t)$ و $D_2(t) = 2sin(t)$ مشخص شود و ثوابت b_1 و b_2 برابر یک باشد [***Error! Bookmark not defined.***].خط مرجع متغیر با زمان $Y_r(t)=$ $sin(10t)$ انتخاب شده است.

بنابراین، خطای ردیابی برای خطوط امپدانس اول و دوم مطابق شکل (۱۴) است.



شکل ۱۴: خطای ردیابی برای خطوط امپدانس اول و دوم

حالت تخمین‌گر توزیع‌شدهDG اول و دوم مطابق شکل(۱۵) است.

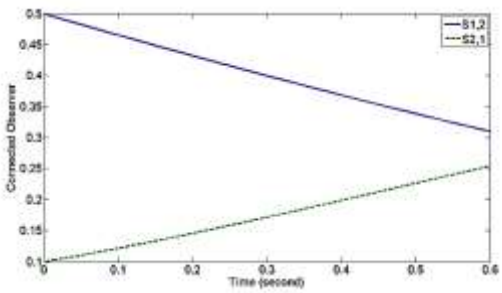


شکل (۱۵) :تخیمن‌گر توزیع‌شده DG اول و دوم

در حالت عدد ۴، ماتریس‌های A و B در ***Error! Reference source not found.*** بترتیب برابر $\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$ و $\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$ هستند. ماتریس P_i مطابق انتگرال لبک برابر $\begin{bmatrix}2 & 1\\1 & 2\end{bmatrix}$ درنظر گرفته شده و c برابر ۰,۵ است. با این اطلاعات a_{ij} در لحظه حمله برابر $\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$ و پس از حل دستگاه معادلات دیفرانسیل برای محاسبه S_i بصورت شکل بالا می باشد.

همان‌طور که در شکل (۱۵)دیده می‌شود دو نظاره‌گر کنترل کننده سایبری نشان داده‌شده است. این نظاره‌گرها روند افزایشی خروجی توان را تا رسیدن به لحظه حمله دنبال می‌کنند.

مقادیر نظاره‌گرهای ارتباطی کنترل‌کننده سایبری$S_{1,2}$ و $S_{2,1}$ نیز مطابق شکل(۱۶) می باشد.



شکل (۱۶): نظاره‌گرهای ارتباطی $S_{1,2}$ و $S_{2,1}$

مطابق آنچه انتظار می‌رفت خطای متوسط در لحظه حمله محدود و برابر ۱۲٪ بوده است. بدین ترتیب کنترل‌کننده سایبری توانسته در لحظه قطع ارتباط بطور موثری از نوسانات توان و ایجاد خاموشی در جزیره تسهیم توان جلوگیری کند.

۱۲- نتیجه‌گیری

در این مقاله روشی برای حفاظت سایبری به سیستم کنترل تسهیم توان جزیره هوشمند ارائه گردید. انواع مختلف حملات به تشکیلات تسهیم توان ممکن خواهد بود. آنچه که در مطالعات بیشتر موردتوجه بوده و نیاز به رفع مسائل مربوطه خواهد داشت، حملات قطع سرویس یا اصطلاحاً DoS است. علی‌رغم مطالعات گذشته که کل جزیره به‌صورت یک واحد یکجا در نظر گرفته می‌شده و حملات به اجزای ارتباطی لحاظ نمی‌گردید، در این مقاله حمله به خط جبرانگر امپدانس مجازی مدنظر قرار گرفته است. البته کنترل‌کننده اصلی و متعارف در تسهیم توان، کنترل افتی است. کنترل افتی با این واقعیت که کنترل فرکانس جزیره در دست توان اکتیو تولیدی و کنترل دامنه ولتاژ در دست توان راکتیو مبادله شده است، کار می‌کند. با حضور هارمونیک‌های بالا در مدارات شامل بارهای غیرخطی و اینورترهای تغذیه‌کننده که به‌وفور در شبکه‌های نوین هوشمند استفاده می‌شود، استفاده و حفاظت خط امپدانس مجازی اهمیت بالایی برخوردار خواهد شد و با قطع سرویس آن نوسانات ولتاژ و جریان و به دنبال آن توان اکتیو راکتیو آغاز و پس از طی فیدبک مثبتی در این مسیر موجب خاموشی بارها که اغلب می‌تواند استراتژیک باشند، گردد. ازاین‌رو با استفاده از روشی جدید جهت حفاظت سایبری آن مدل‌سازی‌های لازم ارائه شد.

نتایج حاصل از شبیه‌سازی‌ها نشان داد که اختلالات هارمونیکی موجود در روش ارائه‌شده هیچ خللی ایجاد نکرد و پس از حمله، سیستم کنترل بادقت ۱۲٪ توانست عملیات حفاظت را انجام دهد.

مراجع

[1] Yifa Liu, Long Cheng, "Energy Based Optimal Dynamic Stealth False Data Injection Attacks on the Smart Grid", Information Cybernetics and Computational Social Systems (ICCSS) 2020 7th International Conference on, pp. 90-95, 2020.

[2] Zhao Zhang, Xuemeng Zhang, Qifu Cheng, Yangyang Ge, Qiuye Sun, Haichang Yu, Gang Wang, "Power distribution strategy of the energy router based on energy storage multi-mode operation", Chinese Automation Congress (CAC) 2017, pp. 6279-6284, 2017.

[3] Office of the National Coordinator for Smart Grid Interoperability, NIST framework and roadmap for smart grid interoperability standards, release 1.0, NIST Special Publication 1108 (2010) 1–145.

[4] V.C. Gungor, F.C. Lambert, A survey on communication networks for electric system automation, Computer Networks (2006) 877–897.

[5] Mohammad Shahraeini, Zeinab Farmani, "Designing of Communication Systems in Advanced Metering Infrastructure (AMI) using Wi-Fi Offloading Technology", Computer and Knowledge Engineering (ICCKE) 2019 9th International Conference on, pp. 60-66, 2019.

[6] Sergi Rotger Griful, Ubbe Welling, Rune Hylsberg Jacobsen, "Multi-modal Building Energy Management System for Residential Demand Response", Digital System Design (DSD) 2016 Euromicro Conference on, pp. 252-259, 2016.

[7] Chun-I Fan, Yi-Fan Tseng, Yi-Hui Lin, Fangguo Zhang, Security with Intelligent Computing and Big-data Services, vol. 733, pp. 322, 2018.

[8] Isozaki, Y., Yoshizawa, S., Fujimoto, Y., Ishii, H., Ono, I., Onoda, T., & Hayashi, Y. (2015). Detection of cyber attacks against voltage control in distribution power grids with PVs. IEEE Transactions on Smart Grid, 7(4), 1824-1835.

[9] Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. Computer networks, 57(5), 1344-1371.

[10] Deng, C., Wen, C., Zou, Y., Wang, W., & Li, X. (2020). A Hierarchical Security Control Framework of Nonlinear CPSs against DoS Attacks with Application to Power Sharing of AC Microgrids. IEEE Transactions on Cybernetics.

[11] Wang, B., Sun, Q., & Ma, D. (2020, November). A Periodic Event-Triggering Reactive Power Sharing Control in an Islanded Microgrid considering DoS Attacks. In 2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 170-175). IEEE.

[12] Lian, Z., Guo, F., Wen, C., Deng, C., & Lin, P. (2021). Distributed Resilient Optimal Current Sharing Control for an Islanded DC Microgrid Under DoS Attacks. IEEE Transactions on Smart Grid.

[13] Fan, B., & Wang, X. (2021). Distributed Privacy-Preserving Active Power Sharing and Frequency Regulation in Microgrids. IEEE Transactions on Smart Grid.

[14] Ikram, M., Ahmed, S., & Marwat, S. N. K. (2019). Power Mismatch Estimation in Smart Grid Using Distributed Control. IEEE Access, 8, 8798-8811.

[15] Karimi, A., Ahmadi, A., Shahbazi, Z., Bevrani, H., & Shafiee, Q. (2020, December). On the Impact of Cyber-Attacks on Distributed Secondary Control of DC Microgrids. In 2020 10th Smart Grid Conference (SGC) (pp. 1-6). IEEE.

[16] O. Hafez, "The impact of smart PEV loads in the smart grid considering demand response provisions," 2016 Saudi Arabia Smart Grid (SASG), 2016, pp. 1-5, doi: 10.1109/SASG.2016.7849683.

[17] M. Liserre, T. Sauter, and J. Y. Hung, “Future energy systems: Integrating renewable energy sources into the smart power grid through industrial electronics,” IEEE Ind. Electron. Mag., vol. 4, no. 1, pp. 18–37, Mar. 2010.

[18] J. C. Vasquez, J. M. Guerrero, J. Miret, M. Castilla, and L. Garcia de Vicu˜na, “Hierarchical control of intelligent microgrids,” IEEE Ind. Electron. Mag., vol. 4, no. 4, pp. 23–29, Dec. 2010.

[19] H. Mahmood, D. Michaelson, J. Jiang, Mei Su, “Accurate reactive power sharing in an islanded microgrid using adaptive virtual impedances,”IEEE Trans. Power Electron. vol. 30, no. 3, pp. 1605-1617, 2015..

[20] J. He and Y. W. Li, J. M. Guerrero, F. Blaabjerg, J. C. Vasquez, “An islanding microgrid power sharing approach using enhanced virtual impedance control scheme ,” IEEE Trans. Power Electron., vol. 28, no. 11, pp. 5272–5282, Nov. 2013.

[21] C-.T. Lee, C-.C. Chu, P-.T. Cheng, A new droop control method for the autonomous operation of distributed energy resource interface converters, IEEE Trans. Power Electron. 28 (4) (2013) 1680-1993.

[22] H. Han, Y. Liu, Y. Sun, M. Su, J. M. Guerrero, “An improved droop control strategy for reactive power sharing in islanded microgrid,” IEEE Trans. Power Electron. Early access.

[23] A. Tuladhar, H. Jin, T. Unger, and K. Mauch, “Control of parallel inverters in distributed AC power systems with consideration of line impedance effect,” IEEE Trans. Ind.