مقاله پژوهشی

طراحی کنترل‌کننده ثانویه پایه‌ریزی‌شده بر روی کنترل اشتراکی توزیع‌شده منابع تولید پراکنده با رویکرد سیستم‌های چندعامله با درنظرگرفتن حمله سایبری منع سرویس

عبدالله میرزابیگی، علی کاظمی، مهدی رمضانی و سیدمحمد عظیمی

چکیده: امروزه در بسیاری از روش‌های کنترلی از اطلاعات سیستم همجوار به منظور کنترل بهتر و سنکرون‌سازی بین واحدهای مختلف استفاده می‌شود و بنابراین در دسترسی و انتقال اطلاعات از طریق لینک‌های ارتباطی، مشکلاتی مانند اختلال، عدم قطعیت، نویز، تأخیر و حمله‌های سایبری به وجود می‌آید. در این مقاله اثر حمله سایبری منع سرویس (DoS) بر ریزشبکه در حالت جزیره‌ای بررسی و کنترل‌کننده سلسله‌مراتبی توزیع‌شده اشتراکی با حضور این حمله سایبری طراحی گردیده است. منابع تولید پراکنده به کمک سیستم‌های چندعامله و شبکه ارتباطی بین آنها با استفاده از تئوری گراف تحلیل شده است. اثرات این حمله سایبری در کنترل منابع تولید پراکنده، فرمول‌بندی ریاضی شده و در اثبات پایداری و سنکرون‌سازی فرکانس و ولتاژ، تابع لیاپانوف مناسب ارائه گردیده و تحلیل پایداری در برابر این حمله سایبری انجام شده و همچنین شرایط پایداری و سنکرون‌سازی اثبات گردیده است. به منظور تأیید مباحث تئوری ارائه‌شده، یک مدل نمونه با وجود حمله سایبری منع سرویس در لینک‌های ارتباطی در محیط متلب/ سیمولینک شبیه‌سازی گردیده است. نتایج در شرایط مختلف، کارایی کنترل‌کننده طراحی‌شده را تحت شرایط معینی به خوبی نشان می‌دهند.

کلیدواژه: **منابع تولید پراکنده، حمله سایبری منع سرویس، سیستم‌های چندعامله، کنترل سلسله‌مراتبی توزیع‌شده اشتراکی، کنترل‌کننده ثانویه.**

اختصارات

x_{dq}: پارامتر x در مرجع dq
x_q: مؤلفه q مرجع dq
x_d: مؤلفه d مرجع dq
A_G: ماتریس انتقال در گراف
$E(G)$: ماتریس لینک ارتباطی
A: ماتریس سیستم
A^c: ماتریس سیستم با DoS[1]
$x(t)$: حالت سیستم بدون حمله
G: ماتریس اتصال به اسلک[2]
L: ماتریس لاپلاسین
g_i: بهره اتصال[3]
a_{ij}: درایه‌های ماتریس مجاورت
P_i: توان اکتیو متوسط
Q_i: توان راکتیو متوسط
$\tilde{p}_i$: توان اکتیو لحظه‌ای
$\tilde{q}_i$: توان راکتیو لحظه‌ای
v_{oi}: ولتاژ خروجی DG_i
ω_{oi}: فرکانس زاویه‌ای خروجی DG_i
i_{oi}: جریان خروجی DG_i
V_{ni}^*: ولتاژ خروجی کنترل‌کننده ثانویه
ω_{ni}^*: فرکانس خروجی کنترل‌کننده ثانویه
v_{oi}^*: ولتاژ خروجی کنترل‌کننده اولیه
ω_{oi}^*: خروجی فرکانس زاویه‌ای کنترل‌کننده اولیه
f: فرکانس
ω_{com}: فرکانس زاویه‌ای در چارچوب معمول
i_l: جریان خروجی بار
ω_c: فرکانس قطع فیلتر پایین‌گذر
v_{ref}: ولتاژ مرجع
ω_{ref}: فرکانس زاویه‌ای مرجع
v_b: ولتاژ باس
u_v: سیگنال کنترل کمکی[4] ولتاژ
u_ω: سیگنال کنترل کمکی فرکانس
C_v: بهره کنترلی ولتاژ
m_{p_i}: ضریب دروپ فرکانس
n_{q_i}: ضریب دروپ ولتاژ
δ: سیگنال عدم تطابق
e_{vi}: خطای ردیابی محلی[5] ولتاژ
$e_{\omega i}$: خطای ردیابی محلی فرکانس

این مقاله در تاریخ ۲ تیر ماه ۱۴۰۱ دریافت و در تاریخ ۳ مهر ماه ۱۴۰۱ بازنگری شد.
عبدالله میرزابیگی، دانشکده مهندسی برق، دانشگاه تفرش، تفرش، ایران، (email: mirzabeigi@acecr.ac.ir).
علی کاظمی (نویسنده مسئول)، دانشکده مهندسی برق، دانشگاه تفرش، تفرش، ایران، (email: kazemy@tafreshhu.ac.ir).
مهدی رمضانی، دانشکده ریاضی، دانشگاه تفرش، تفرش، ایران، (email: ramezani@tafreshhu.ac.ir).
سیدمحمد عظیمی، دانشکده مهندسی برق، دانشگاه صنعتی همدان، همدان، ایران، (email: azimi@hut.ac.ir).

1. Denial of Service Attack
2. Slack Bus
3. Pinning Gain
4. Auxiliary Control
5. The Local Neighborhood Tracking Error

ϕ: متغیر کمکی کنترل‌کننده ولتاژ
γ: متغیر کمکی کنترل‌کننده جریان
ν: گره در تئوری گراف
L_{line}: اندوکتانس خطوط بین DGها
R_{line}: مقاومت خطوط بین DGها
σ: مقدار ویژه
x^c: پارامتر x مختل‌شده با حمله
$\theta^x(t)$: ماتریس حمله سایبری DoS در حالت
$\theta^u(t)$: ماتریس حمله سایبری DoS در ورودی کنترلی
$\theta^x_{jv}(t)$: ماتریس حمله سایبری به ولتاژ اندازه‌گیری‌شده
$\theta^x_{i\omega}(t)$: ماتریس حمله سایبری به فرکانس زاویه‌ای اندازه‌گیری‌شده
$\theta^x_{jp}(t)$: ماتریس حمله سایبری به توان اکتیو اندازه‌گیری‌شده
$\theta^u_{jv}(t)$: ماتریس حمله سایبری به ورودی کنترلی ولتاژ
$\theta^u_{i\omega}(t)$: ماتریس حمله سایبری به ورودی کنترلی فرکانس زاویه‌ای
$\theta^u_{jp}(t)$: ماتریس حمله سایبری به ورودی کنترلی توان
C_ω: بهره کنترلی فرکانس زاویه‌ای

۱- مقدمه

کاهش منابع سوخت‌های فسیلی، اثرات نامطلوب زیست‌محیطی و پایین‌بودن بازدهی شبکه‌های برق سنتی، تمایل به تولید برق در نزدیکی بار و در سطح شبکه توزیع با استفاده از منابع تجدیدپذیر را افزایش داده است.

یکی از راهکارهای اساسی به منظور حل مشکلات مطرح‌شده، استفاده از ریزشبکه و منابع تولید پراکنده [1] (DG) است. فرکانس و ولتاژ، کنترل تبادل توان اکتیو و راکتیو بین واحدهای منابع تولید پراکنده و همچنین با شبکه اصلی، سنکرون‌سازی ریزشبکه با شبکه اصلی[2]، مدیریت انرژی و بهینه‌سازی اقتصادی، پارامترهای مهمی هستند که در منابع تولید پراکنده باید کنترل شوند [۱].

یک ریزشبکه در دو حالت وصل به شبکه[3] و جزیره‌ای[4] می‌تواند مورد بهره‌برداری قرار بگیرد. در حالت وصل به شبکه، کنترل اغلب از طریق شبکه اصلی انجام می‌گردد. کنترل‌کننده‌هایی که در حالت جزیره‌ای طراحی می‌گردند باید تنظیم و یکسان‌سازی مقادیر ولتاژ و فرکانس خروجی همه منابع را انجام دهند. در حالت کلی ۴ روش کنترلی مختلف برای ریزشبکه وجود دارد: ۱) کنترل متمرکز[5]، ۲) کنترل غیر متمرکز[6]، ۳) کنترل توزیع‌شده[7] و ۴) کنترل سلسله‌مراتبی[8]. کنترل‌کننده متمرکز از یک کنترل‌کننده مرکزی استفاده می‌کند و اطلاعات همه واحدها به این کنترل‌کننده ارسال و کنترل به صورت یکپارچه انجام می‌شود. در کنترل‌کننده غیر متمرکز برای هر واحد، کنترل‌کننده جداگانه طراحی می‌گردد و عملاً کنترل‌کننده‌ها و واحدهای مختلف، ارتباطی با هم ندارند و هر واحد توسط کنترل‌کننده خودش مدیریت می‌شود [۲]. در روش کنترلی توزیع‌شده، برای هر واحد کنترل‌کننده مجزا در نظر گرفته می‌شود ولی کنترل‌کننده‌ها از اطلاعات واحدهای همجوار نیز استفاده می‌کنند و بنابراین نیاز به سیستم‌های ارتباطی دارند. کنترل‌کننده سلسله‌مراتبی در چند لایه، مقادیر ولتاژ، فرکانس و توان را به مقادیر مطلوب می‌رساند. با استفاده از این استراتژی کنترلی، کل ساختار کنترلی به سه سطح اولیه[9]، ثانویه[10] و ثالثیه[11] می‌شود. کنترل‌کننده اولیه به صورت داخلی و اغلب دروپ[12] است. کنترل‌کننده‌های دروپ با انجام عمل تقسیم توان بین منابع تولید پراکنده، توان مورد نیاز بار را تقسیم می‌کنند. مزیت اصلی دروپ این است که امکان اختلال یا حمله سایبری از بیرون وجود ندارد، اما مشکل اصلی آن انحراف مقادیر خروجی آن از مرجع است. در این کنترل‌کننده، کنترل فرکانس توسط توان اکتیو و کنترل ولتاژ توسط توان راکتیو انجام می‌گردد. بازنشانی فرکانس و ولتاژ ورودی دروپ به مقدار نامی در صورت تغییرات و اغتشاشات، هم‌زمان‌کردن ریزشبکه با شبکه اصلی برای حالت انتقال از مد جزیره‌ای به مد متصل به شبکه، حذف هر گونه خطای حالت دائمی با کمک کنترل‌کننده اولیه، سنکرون‌سازی هنگام تبدیل حالت وصل به شبکه به حالت جزیره‌ای و کنترل DGها، از کاربردهای اصلی کنترل‌کننده ثانویه است. در کنترل‌کننده ثانویه، خروجی کنترل‌کننده به دروپ ارسال می‌گردد تا خطای حالت ماندگار صفر شود و سنکرون‌سازی به درستی انجام گردد. قاعده اصلی کنترل‌کننده ثانویه، تبادل اطلاعات با DGهمجوار و مقایسه با میانگین ولتاژ و فرکانس اندازه‌گیری‌شده و یا مقدار مرجع و سپس پایدارسازی و سنکرون‌سازی کل شبکه است. برای مشخص‌کردن مرجع در کنترل‌کننده ثانویه، معمولاً از میانگین[13] مقادیر خروجی ولتاژ و فرکانس منابع تولید پراکنده و یا مقدار توافقی[14] استفاده می‌گردد [۳] و [۴].

مقادیر مرجع فرکانس و ولتاژ برای شین اسلک یا مرجع را کنترل‌کننده ثالثیه ایجاد می‌کند. در شبکه‌های قدرت برای حل معادلات و به دست آوردن ولتاژها و فرکانس‌ها، انتخاب ولتاژ یک شین به عنوان مرجع ولتاژ کاملاً ضروری است که توسط کنترل‌کننده ثالثیه انجام می‌گیرد. این کنترل‌کننده، توان بین ریزشبکه و شبکه اصلی را نیز مدیریت کرده و به کاهش هارمونیک و انحراف در حالت وصل از جزیره‌ای به متصل به شبکه کمک می‌کند و کیفیت توان را نیز افزایش می‌دهد. در مواقع بسیاری از این کنترل‌کننده استفاده نمی‌شود و کنترل صرفاً از طریق کنترل‌کننده اولیه و ثانویه انجام می‌گردد [۵] و [۶].

اختلالات مختلفی سبب برهم‌خوردن تنظیم و یکسان‌سازی فرکانس و ولتاژ خروجی می‌گردند. برای رفع این مشکلات در ساختارهای مختلف کنترلی (اغلب برای سنکرون‌سازی)، نیاز به اطلاعات از DGهای همجوار و ارسال آنها با استفاده از لینک‌های ارتباطی است. هر کجا که کانال ارتباطی وجود داشته باشد، مشکلاتی از قبیل از بین رفتن اطلاعات، حمله سایبری، نویز خطوط، اختلال در دسترسی و غیره ایجاد می‌شود. امروزه حمله‌های سایبری مختلفی در شبکه‌های ارتباطی ایجاد شده و باعث تخریب و آسیب به سیستم‌ها می‌گردند. یکی از مهم‌ترین و متداول‌ترین حمله‌های سایبری، حمله منع سرویس است که باعث قطع‌شدن لینک‌های ارتباطی و بعضاً ناپایداری سیستم‌ها می‌گردد. این حمله می‌تواند در DGها نیز اتفاق بیفتد و در شرایط حمله، تثبیت فرکانس و ولتاژ و یکسان‌سازی

1. Distributed Generation
2. Main Grid
3. Grid Connected Mode
4. Islanded Mode
5. Centralized Control
6. Decentralized Control
7. Distributed Control
8. Hierarchical Control
9. Primary Control
10. Secondary Control
11. Tertiary Control
12. Droop Controller
13. Averaging
14. Consensus

آنها ضروری است [۷].

بررسی حمله‌های سایبری در مراجع زیادی بر روی سیستم‌های مختلف بررسی گردیده و طی چند سال گذشته، کارهای پژوهشی زیادی در زمینه امنیت سایبری سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی توسط متخصصین رشته کنترل و سایر رشته‌های مرتبط ارائه شده است [۸] تا [۱۰]. در [۱۱] طریقه واردشدن و اثرات حملات سایبری در سیستم‌ها آمده و انواع روش‌های حمله‌های سایبری در [۱۲] و [۱۳] شرح داده شده است. در [۱۴] حمله سایبری به سنسورها و عملگرها بر روی سیستم‌های چندعامله[1] بحث گردیده است. در [۱۵] تا [۱۷] اثر حمله DoS و نحوه شناسایی آن در سیستم NCS[2] مورد بررسی و ارزیابی قرار گرفته و بحث حمله‌های سایبری بر روی ریزشبکه نیز در مراجع مختلفی انجام شده است [۱۸] تا [۲۱]. در [۲۱] اثر از بین رفتن دیتا در ریزشبکه بررسی گردیده و همچنین تأخیر در اثر این حمله مورد ارزیابی قرار گرفته است. در [۲۲] پایداری سیستم با در نظر گرفتن حمله DoS به همراه جزئیات این حمله مورد بحث قرار گرفته است. در [۲۳] حمله سایبری DoS به صورت مسدودشدن موقت کانال مخابراتی و تأخیری در یک ریزشبکه در نظر گرفته شده و اثر آن بر سیستم‌ها نشان داده شده است. البته بررسی حمله به صورت تأخیر با واقعیت حمله سازگاری ندارد، اما در مقاله ارائه‌شده، این حمله به صورت مسدودشدن کانال است. در [۲۴] برای از بین بردن اثر حمله سایبری منع سرویس در ریزشبکه از کنترل‌کننده غیر متمرکز و با دیدگاه سیستم‌های چندعامله استفاده گردیده است. در [۲۵] اثر حمله‌های سنسوری، ربودن اطلاعات و منع سرویس بر روی کنترل‌کننده ثانویه نشان داده شده است، اما درباره پایداری و سنکرون‌سازی آن بحث و تحلیل نشده است. در [۲۶] از کنترل‌کننده توزیع‌شده برای کنترل ریزشبکه و رفع اثر حمله DoS استفاده گردیده و با استفاده از کنترل‌کننده توزیع‌شده به صورت استفاده از میانگین خروجی‌ها به عنوان مرجع و با وجود محدودیت بار توانی ثابت، اثر حمله تحلیل گردیده است. تفاوت مقاله ارائه‌شده با [۲۶] این است که در [۲۶] برای از بین بردن اثر حمله از میانگین ولتاژ و فرکانس استفاده شده و در مقاله ارائه‌شده از مرجع استفاده گردیده است. استفاده از میانگین، علی‌رغم این که اثر حمله را از بین می‌برد ممکن است باعث شود که خروجی‌ها از مقدار مرجع فاصله بگیرند و به سمت مقدار میانگین بازیابی شوند. در [۲۷] اثر حمله سایبری DoS در ریزشبکه برای فرکانس با استفاده از روش کنترل‌کننده ثانویه و با در نظر گرفتن مرجع توان اکتیو تحلیل شده است، اما بررسی در مورد ولتاژ صورت نگرفته و با استفاده از این روش، ولتاژ بازیابی نمی‌گردد. در اکثر پژوهش‌های انجام‌شده مباحث پایداری، توابع لیاپانوف، مقاوم‌بودن و سنکرون‌سازی به اختصار بررسی شده‌اند. یکی از اصلی‌ترین اهداف در تحقیقات حمله‌های سایبری آن است که کنترل‌کننده به نحوی طراحی شود که رنج وسیع‌تری از حملات را تحمل کند. انتخاب و طراحی کنترل‌کننده مناسب با توجه به نوع حمله سایبری و شرایط آن انجام می‌گردد.

در اکثر منابع، دیدگاه پایداری و سنکرون‌سازی در نظر گرفته نشده و همچنین تحلیل پایداری با حضور حمله سایبری DoS وجود ندارد. برای تحلیل باید ابتدا معادلات ریاضی ریزشبکه به همراه حمله استخراج شده و سپس اثر حمله در پایداری ارزیابی گردد. نهایتاً سیستم باید با طراحی کنترل‌کننده، پایدار و هماهنگ شود. در این مقاله سعی شده که اثرات این حمله بر پایداری و سنکرون‌سازی تحلیل گردد و شرایط سنکرون‌سازی و پایدارسازی به دست آید. برای بررسی دقیق‌تر حملات سایبری، سیستم به صورت یک شبکه NCS و در دو لایه سایبری و فیزیکی در نظر گرفته می‌شود و برای سنکرون‌سازی از دیدگاه سیستم‌های چندعامله استفاده گردیده است. به منظور کنترل اثرات حمله DoS از کنترل‌کننده ثانویه بر پایه کنترل‌کننده سلسله‌مراتبی اشتراکی توزیع‌شده[3] استفاده گردیده است. تفاوت اصلی این مقاله با کارهای مشابه قبلی آن است که در این مقاله، منابع تولید پراکنده به صورت سیستم‌های چندعامله و در نظر گرفتن حمله DoS در روابط کنترل‌کننده بحث گردیده و تابع لیاپانوف مناسب ارائه و همچنین شرایط سنکرون‌سازی همه منابع تولید پراکنده اثبات شده است. نوآوری‌های این مقاله به اختصار به شرح زیر است:

۱) مدل‌سازی و فرمول‌بندی حمله سایبری منع سرویس در مدل منابع تولید پراکنده با در نظر گرفتن به صورت سیستم‌های چندعامله

۲) بررسی پایداری سیستم ریزشبکه با معرفی تابع لیاپانوف جدید با حضور حملات سایبری منع سرویس و به دست آوردن شرایط پایداری سیستم

۳) طراحی و شبیه‌سازی کنترل‌کننده ثانویه در منابع تولید پراکنده با در نظر گرفتن حمله سایبری منع سرویس

۴) بررسی سنکرون‌سازی همه منابع تولید پراکنده و به دست آوردن شرایط سنکرون‌سازی

۵) مشخص‌کردن انعطاف‌پذیری سیستم در برابر حمله منع سرویس

۶) بررسی اثر حمله سایبری DoS در کنترل‌کننده ثانویه

در بخش دوم مدل دینامیکی منابع تولید پراکنده و در بخش سوم تئوری گراف بحث می‌گردد. در بخش چهارم روش کنترلی طراحی‌شده مورد مطالعه قرار می‌گیرد. در بخش پنجم بررسی انواع حملات سایبری و فرمول‌بندی حمله سایبری DoS در منابع تولید پراکنده و در بخش ششم تابع لیاپانوف و شرایط پایداری آمده است. در بخش هفتم شبیه‌سازی و نهایتاً در بخش هشتم نتیجه‌گیری ارائه گردیده است.

۲- مدل دینامیکی منابع تولید پراکنده

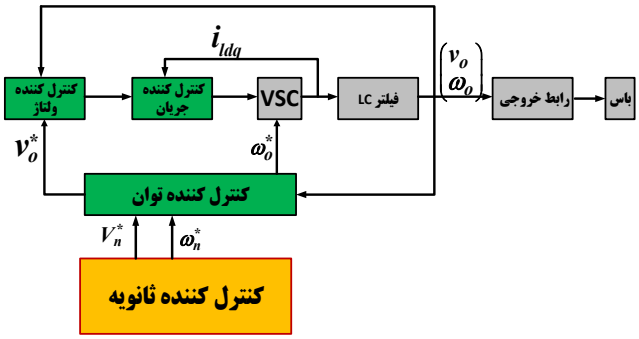
مدل استفاده‌شده در این مقاله به صورت مدل ۱۳حالته (۱) در نظر گرفته شده که یک مدل غیر خطی است و به طور کامل همه جزئیات را در بر می‌گیرد [۲۸]

$$\begin{cases} \dot{x}_i = f_i(x_i) + k_i(x_i)D_i + g_i(x_i)u_i \\ y_i = h_i(x_i) \\ x_i = [\delta_i \;\; P_i \;\; Q_i \;\; \phi_{di} \;\; \phi_{qi} \;\; \gamma_{di} \;\; \gamma_{qi} \;\; i_{ldi} \;\; i_{lqi} \;\; v_{odi} \;\; v_{oqi} \;\; i_{odi} \;\; i_{oqi}] \\ D_i = [\omega_{com} \;\; v_{bdi} \;\; v_{bqi}]^T \end{cases} \quad (۱)$$

که δ_i زاویه چارچوب مرجع DG_i با چارچوب مرجع معمول، P_i و Q_i توان متوسط اکتیو و راکتیو خروجی، ϕ_{dq} متغیر کمکی در کنترل‌کننده ولتاژ، γ_{di} متغیر کمکی در کنترل‌کننده جریان و i_{odq}، v_{odq} و i_{ldq} به ترتیب مقادیر جریان و ولتاژ خروجی و جریان بار هستند. مقادیر ورودی کنترلی و خروجی $u_i = (V_{ni}^* \;\; \omega_{ni}^*)^T$ و $y_i = (v_{odi} \;\; \omega_{odi})^T$ می‌باشند. جزئیات مقادیر (۱) در [۲۸] آمده است.

توجه: با توجه به معلوم‌بودن پارامترهای منابع تولید پراکنده، این

1. Multi Agent Systems
2. Network Control System
3. Secondary Control Based on Distributed Cooperative Control



شکل ۱: منبع تولید پراکنده به همراه کنترل‌کننده اولیه و ثانویه.

سیستم‌ها مبتنی بر مدل[1] در نظر گرفته می‌شوند. در این مدل‌سازی، قسمت‌های مختلف شامل منابع توزیع‌شده، قسمت‌های اندازه‌گیری، شبکه اصلی، قسمت‌های کنترلی و قسمت مخابراتی، بلوک‌های کنترل‌کننده توان، کنترل‌کننده ولتاژ و جریان، فیلتر LC و بار خروجی در نظر گرفته شده و از بین مدل‌های مختلف DGها، کامل‌ترین مدل است [۳]، [۵]، [۶] و [۲۸] تا [۳۰].

۳- تئوری گراف

برای تحلیل ریزشبکه و پایداری و سنکرون‌سازی در این مقاله از تئوری گراف[2] استفاده گردیده است. در سیستم‌های چندعامله، سیگنال کنترلی با توجه به مقداری که از اطلاعات همسایه گرفته می‌شود، طراحی می‌گردد. برای سیستم‌های چندعامله، چند قانون اصلی (قوانین رینولد[3]) وجود دارد: ۱) اجتناب از برخورد با همسایگان، ۲) تطبیق حرکت با بقیه گروه و ۳) باقی‌ماندن در اطراف یک مرکز [۳۱]. این قوانین در ریزشبکه نیز به طور کامل قابل پیاده‌سازی هستند. در این حالت هر منبع تولید پراکنده به صورت یک عامل[4] در نظر گرفته می‌شود و سیستم مخابراتی با استفاده از گراف مستقیم[5] تئوری گراف، مدل می‌گردد. تئوری گراف مشخص می‌کند که منابع تولید پراکنده به چه طریقی با هم در ارتباط هستند و به یکدیگر اطلاعات می‌دهند. در این تئوری از ماتریس مجاورت برای نشان‌دادن ارتباطات و همچنین در مباحث پایداری و تابع لیاپانوف استفاده می‌شود [۳۲] و [۳۳].

تعاریف

گراف پیوسته: گرافی است که در بین دو گره آن حداقل یک مسیر وجود دارد.

گره ریشه: گرهی است که از آن گره با یک گراف مستقیم بتوان به گره‌های دیگر رسید.

گره سردسته[6]: گرهی که از گره دیگری مقدار نمی‌گیرد و مقدار اصلی را مشخص می‌کند.

درخت: یک گراف پیوسته که هیچ حلقه‌ای ندارد.

درخت ریشه‌دار: درختی که یک رأس آن ریشه است که مقدار مرجع را نیز مشخص می‌کند.

در این مقاله فرض شده که توپولوژی ثابت و درخت ریشه‌دار پیوسته[7] بوده و به صورت $G(v,E,A_G)$ نشان داده می‌شود. گراف به صورت زیر در نظر گرفته می‌شود

$$G=(V(G),E(G)) \qquad (۲)$$

$V(G)=\{v_1,v_2,\ldots,v_N\}$ ، $E(G)\subset V(G)\times V(G)$ و $A_G\subset R\times R$ به ترتیب گره‌ها[8] (منابع تولید پراکنده)، لینک‌های ارتباطی و ماتریس مجاورت[9] می‌باشند. درایه‌های ماتریس مجاورت a_{ij}، وزن ضلع‌های گراف هستند که اگر گراف iام به گراف jام اطلاعات بدهد، یک و در غیر این صورت صفر در نظر گرفته می‌شوند. محل اتصال گره‌ها به یکدیگر به صورت $(v_j,v_i)\subset E(G)$ است. ماتریس G را غیر مستقیم[10] در نظر می‌گیرند اگر

$$\begin{aligned}&(v_i,v_j)\subset E\\&(v_j,v_i)\subset E\\&N_i=\{v_j\in V(G)\,|\,(v_j,v_i)\subset E(G)\ ,\ i\neq j\}\end{aligned} \qquad (۳)$$

برای تحلیل پایداری، ماتریس Δ و لاپلاسین L به صورت رابطه زیر تعریف می‌شود

$$\begin{aligned}&D=diag(\Delta_i)\\&\Delta_i=\sum_{v_j=N_i}a_{ij}\\&L=D-A\end{aligned} \qquad (۴)$$

در این مقاله فرض می‌گردد که گراف جهت‌دار به صورت درخت پیوسته و ثابت است و هیچ حلقه خودی[11] در آن نیست [۴] و [۲۹].

۴- روش کنترلی طراحی‌شده

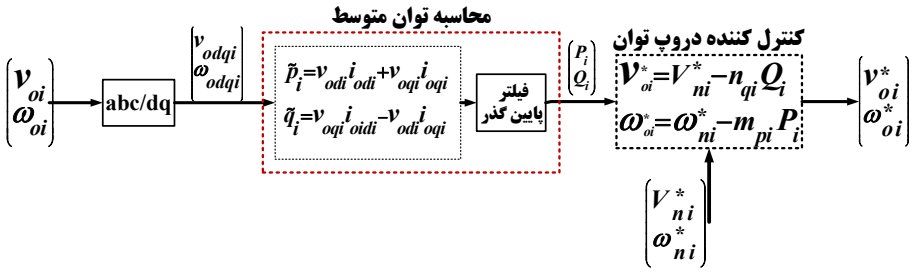
کنترل ریزشبکه در ۲ سطح (کنترل‌کننده اولیه و ثانویه) انجام می‌گیرد. شکل کلی منابع تولید پراکنده و کنترل‌کننده اولیه و ثانویه استفاده‌گردیده در شکل ۱ آمده است. با توجه به شکل، V_{ni}^* و ω_i^* باید توسط کنترل‌کننده ثانویه بازنشانی گردند تا انحراف کمتری در ورودی کنترل‌کننده اولیه ایجاد شود.

۴-۱ کنترل‌کننده اولیه

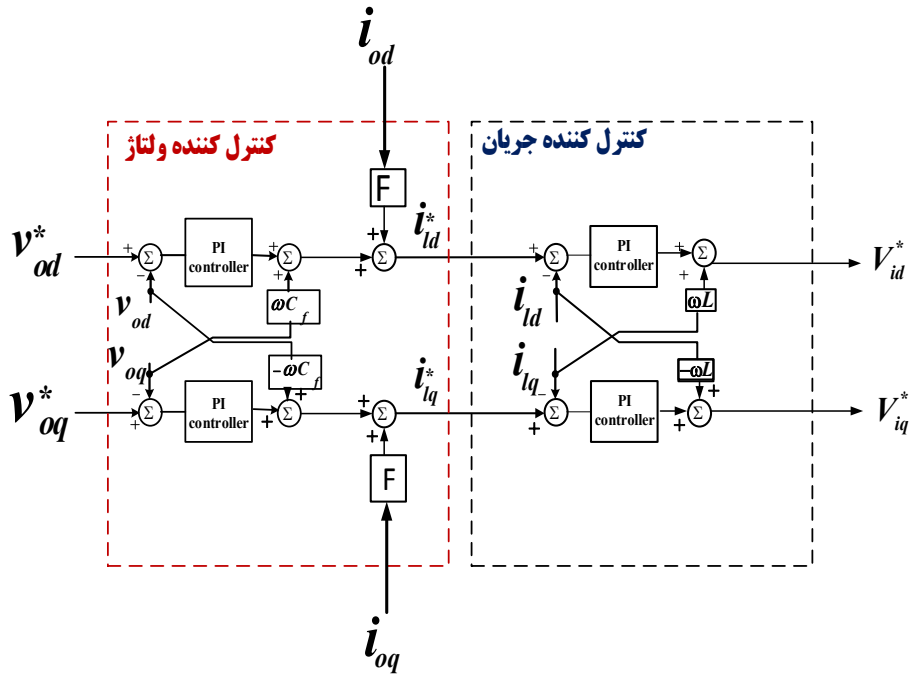
کنترل‌کننده‌های جریان، ولتاژ و توان به صورت اولیه در نظر گرفته می‌شوند که در شکل‌های ۲ و ۳ نشان داده شده‌اند. لازم به ذکر است که در بعضی مراجع، کنترل‌کننده اولیه، کنترل‌کننده داخلی DG در نظر گرفته می‌شود. نکته دیگر این که دروپ ولتاژ و فرکانس تا اندازه زیادی مجزا بوده و طراحی کنترل‌کننده دروپ ولتاژ و فرکانس به صورت جداگانه انجام می‌شود. خروجی کنترل‌کننده ثانویه $(V_{ni}^*\quad \omega_{ni}^*)^T$ و خروجی DG_i $(V_{oi}\quad \omega_{oi})^T$ به عنوان ورودی کنترل‌کننده اولیه است.

در کنترل‌کننده توان که در شکل ۲ نشان داده شده است، ابتدا با استفاده از خروجی‌های منابع تولید پراکنده، توان لحظه‌ای از (۵) به دست می‌آید و با عبور این توان از یک فیلتر پایین‌گذر با (۶)، توان متوسط به صورت $(P\ \ Q)^T$ حاصل می‌شود

1. Model Base
2. Graph Theory
3. Reynold
4. Agent
5. Direct Graph
6. Leader
7. Spinning Tree
8. Node
9. Adjacency Matrix
10. Indirected
11. Self-Loop



شکل ۲: کنترل‌کننده توان در کنترل‌کننده اولیه.



شکل ۳: کنترل‌کننده ولتاژ و جریان در کنترل‌کننده اولیه.

$$\begin{cases} \tilde{p}_i = v_{odi} i_{odi} + v_{oqi} i_{oqi} \\ \tilde{q}_i = v_{oqi} i_{odi} - v_{odi} i_{oqi} \end{cases} \quad (۵)$$

$$P_i = \frac{s}{s+\omega_c} \tilde{p}_i$$
$$Q_i = \frac{s}{s+\omega_c} \tilde{q}_i \quad (۶)$$

با صرف نظر از دینامیک‌های سریع سیستم و با در نظر گرفتن مدل سیستم در چارچوب dq[1]، کنترل‌کننده توان در کنترل‌کننده اولیه به فرم زیر در نظر گرفته می‌شود [۳] و [۴]

$$\begin{cases} v_{oi}^* = V_{ni}^* - n_{qi} Q_i \\ \omega_{oi}^* = \omega_{ni}^* - m_{pi} P_i \end{cases} \quad (۷)$$

معادله ولتاژ در چارچوب dq به صورت زیر درمی‌آید

$$v_{odi}^* = V_{ni}^* - n_{qi} Q_i$$
$$v_{oqi}^* = 0 \quad (۸)$$

سپس با توجه به (۷)، خروجی کنترل‌کننده توان به دست می‌آید و خروجی v_o^* به کنترل‌کننده ولتاژ و ω_o^* به VSC داده می‌شود. در این معادله n_{qi} و m_{pi} ضرایب دروپ و V_{ni}^* و ω_{ni}^* مقدارهای مرجع کنترل‌کننده اولیه‌اند.

1. Direct-Quadratic

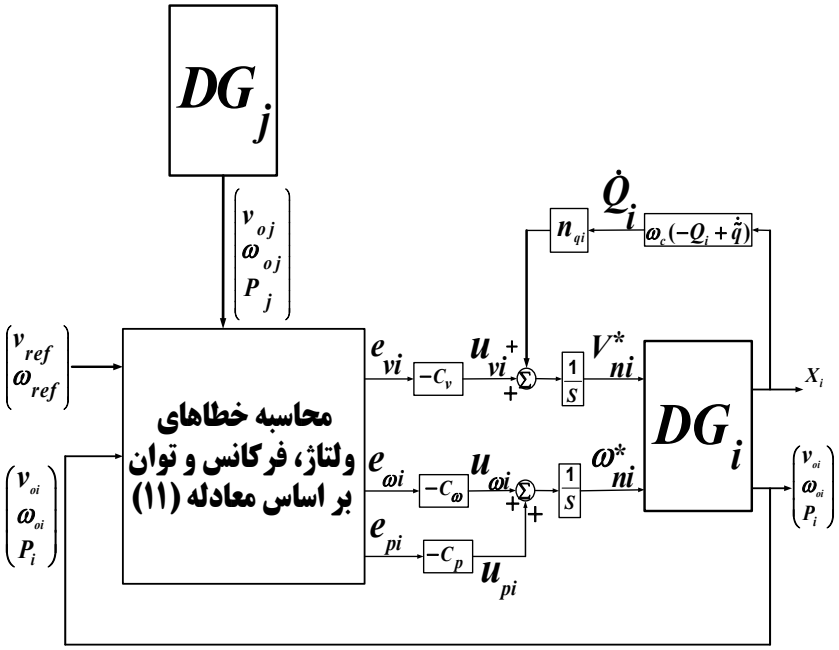
بلوک دیاگرام کنترل‌کننده ولتاژ و جریان در شکل ۳ آمده و در کنترل‌کننده ولتاژ و جریان از کنترل‌کننده PI استفاده گردیده است. کنترل‌کننده ولتاژ، مرجع جریان‌ها را مشخص می‌نماید و خروجی آن به عنوان ورودی‌های مرجع وارد کنترل‌کننده جریان می‌شود.

۴-۲ کنترل‌کننده ثانویه

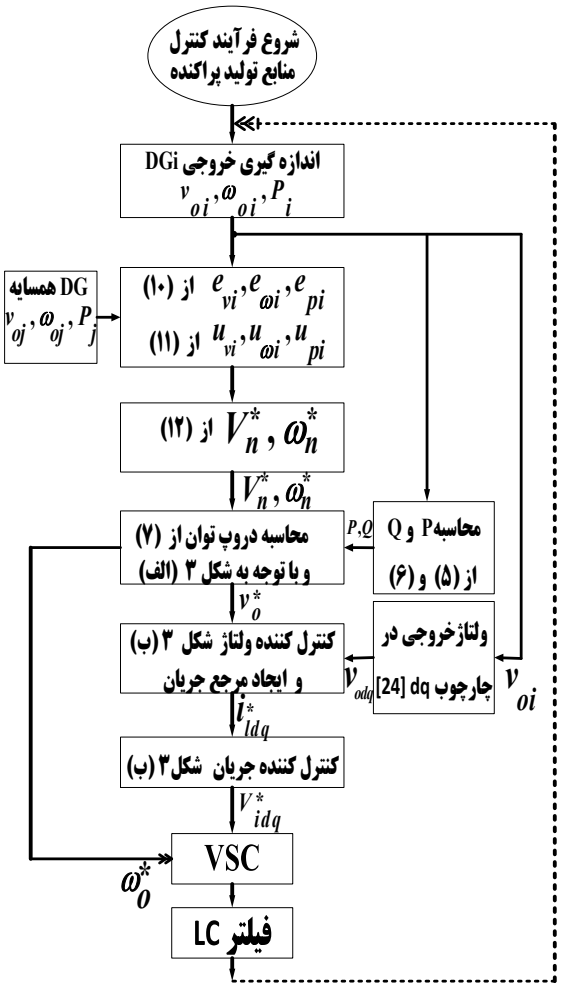
شکل ۴ طرح کلی کنترل‌کننده ثانویه را نشان می‌دهد. در این مقاله، کنترل‌کننده ثانویه با استفاده از روش خطی‌سازی فیدبک طراحی شده است. هدف اصلی در طراحی این کنترل‌کننده، اعمال ورودی کنترلی مناسب $(V_{ni}^* \quad \omega_{ni}^*)^T$ به کنترل‌کننده اولیه برای پایداری و سنکرون‌سازی سیستم است. با استفاده از روش خطی‌سازی فیدبک از (۷) و (۸) مشتق گرفته می‌شود و آن را برابر با ورودی کنترلی قرار می‌دهیم و ورودی کنترلی را به نحوی طراحی می‌کنیم که خطا به سمت صفر میل کند. بنابراین نتیجه به صورت (۹) درمی‌آید [۴]

$$\begin{cases} \dot{v}_{odi}^* = \dot{V}_{ni}^* - n_{qi} \dot{Q}_i = u_{vi} \\ \dot{\omega}_{oi}^* = \dot{\omega}_{ni}^* - m_{pi} \dot{P}_i = u_{\omega i} \end{cases} \quad (۹)$$

در معادله بالا، u_{vi} و $u_{\omega i}$ به ترتیب سیگنال کنترلی کمکی ولتاژ و جریان در روش خطی‌سازی فیدبک سیستم‌های چندعامله هستند. به منظور پایدارسازی سیستم و با توجه به این که سیستم به صورت چندعامله در نظر گرفته شده است، ورودی کنترلی به صورت (۱۰) با استفاده از خطاهای دنبال‌سازی در نظر گرفته می‌شود [۳۱]



شکل ۴: کنترل‌کننده ثانویه.



شکل ۵: روندنمای کنترل‌کننده اولیه و ثانویه طراحی‌شده.

$$\begin{cases} u_{vi} = -C_v e_{vi}(t) \\ u_{\omega i}(t) = -C_\omega e_{\omega i}(t) \\ u_{pi} = m_{pi}\dot{P}_i = -C_p e_{pi}(t) \end{cases} \quad (۱۰)$$

در این رابطه $e_{vi}(t)$، $e_{\omega i}(t)$ و $e_{pi}(t)$ به ترتیب خطای دنبال‌سازی و C_v، C_ω و C_p بهره کنترلی ولتاژ، فرکانس و توان اکتیو هستند. خطای دنبال‌سازی به صورت (۱۱) در سیستم‌های چندعامله می‌باشد که در سنکرون‌سازی، هدف این است که این خطاها صفر شوند. این خطاها با استفاده از خروجی DG و همسایه به دست می‌آیند

$$\begin{cases} e_{v_i} = \sum a_{ij}(v_{.i}(t) - v_{.j}(t)) + g_i(v_{.i}(t) - v_{ref}) \\ e_{\omega i}(t) = \sum_{j\in N_j} a_{ij}(\omega_{oi}(t) - \omega_{oj}(t)) + g_i(\omega_{oi}(t) - \omega_{ref}) \\ e_{pi} = \sum a_{ij}(m_{p_i}P_i - m_{pj}P_j) \end{cases} \quad (۱۱)$$

که P_i، $\omega_{oi}(t)$ و $v_{.i}(t)$ و P_j، $\omega_{oj}(t)$ و $v_{.j}(t)$ ولتاژ، فرکانس و توان متوسط خروجی DG_i و DG_j هستند. v_{ref} و ω_{ref} ولتاژ و فرکانس زاویه‌ای مرجع، a_{ij} درایه‌های ماتریس مجاورت و g_i بهره اتصال می‌باشند. g_i فقط زمانی برابر یک است که DG به گره اسلک وصل باشد و در غیر این صورت صفر است.

با استفاده از (۹) تا (۱۱)، سیگنال کنترلی از روش خطی‌سازی فیدبک به صورت (۱۲) به دست می‌آید

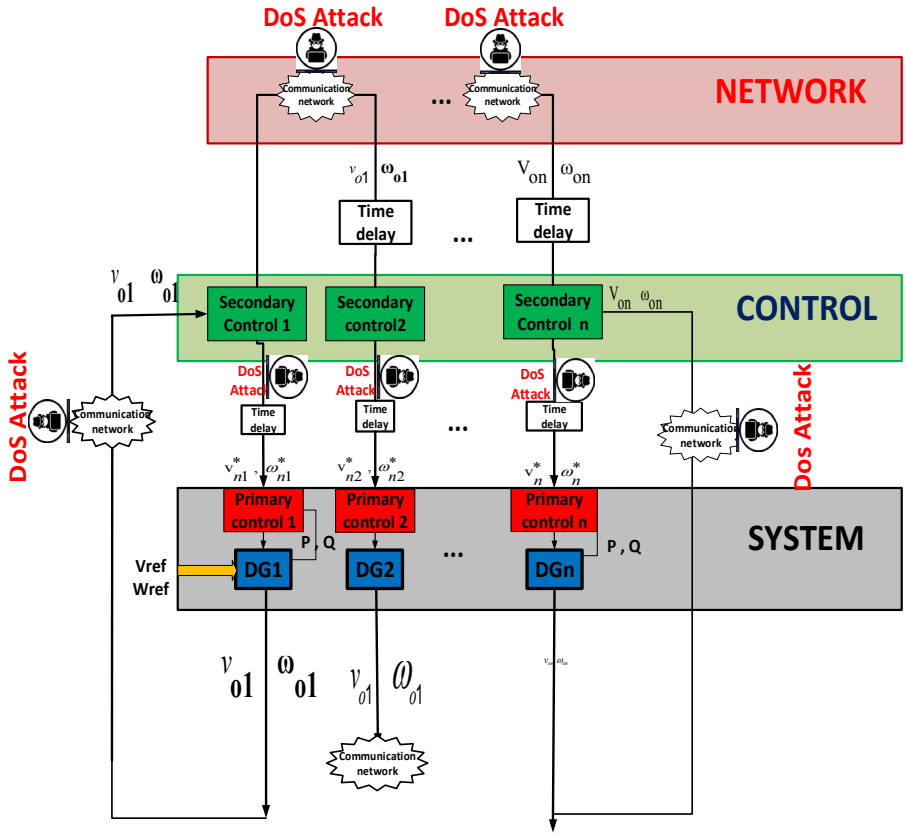
$$\begin{cases} V_{ni}^* = \int (u_{vi} + n_{qi}\dot{Q}_i)\mathrm{d}t \\ \omega_{ni}^* = \int (u_{\omega i} + u_{pi})\mathrm{d}t \end{cases} \quad (۱۲)$$

در (۱۲) مقدار $\dot{Q}_i$ به صورت زیر تعریف شده است

$$\dot{Q}_i = -\omega_c Q_i + \omega_c(v_{oqi}i_{odi} - v_{odi}i_{oqi}) = -\omega_c Q_i + \omega_c\tilde{q} \quad (۱۳)$$

که $\dot{Q}_i$ مربوط به اطلاعات داخلی DG می‌باشد و بنابراین تحت تأثیر اختلالات خارجی قرار نمی‌گیرد. $\tilde{q}$ توان راکتیو لحظه‌ای، ω_c فرکانس قطع فیلتر پایین‌گذر و v_o و i_o ولتاژ و جریان خروجی DG_i است [۴] و [۲۸]. برای درک دقیق روش کنترلی، روندنمای[1] روش طراحی‌شده در شکل ۵ آمده است.

1. Flowchart



شکل ۶ منابع تولید پراکنده با کنترل‌کننده‌ها و با در نظر گرفتن حمله سایبری DoS.

توجه: طراحی ورودی کنترلی باید به نحوی باشد که همه حالت‌ها به مقدار توافقی یا مرجع برسند و سنکرون‌سازی به درستی انجام شود که این، اصلی‌ترین شرط برای برقراری قوانین رینولد است. در سنکرون‌سازی خطای حدود ۳٪ برای ولتاژ نامی و برای فرکانس نیز ۰٫۳٪ قابل قبول می‌باشد، اما هدف اصلی این است که در حالت پایدار مقادیر با هم یکسان شوند و در عامل‌ها $\lim_{t\to\infty}\|x_j(t)-x_i(t)\|=0$ گردد [۳۴] و [۳۵].

با توجه به روابط بالا برای کنترل و سنکرون‌سازی سیستم باید فرکانس، ولتاژ و توان اکتیو متوسط DG همجوار را داشته باشیم. برای انتقال اطلاعات همسایه باید از کانال‌های ارتباطی استفاده گردد و در این انتقال، مشکلات مختلفی ایجاد می‌شود (از جمله حملات سایبری که بسیار در سال‌های اخیر مورد توجه بوده و در این مقاله هم در نظر گرفته شده است).

۵- انواع حملات سایبری و تأثیر در منابع تولید پراکنده

مباحث امنیتی شبکه در سه مفهوم پایه‌ای شامل محرمانگی[۱]، یکپارچگی[۲] و در دسترس بودن[۳] مطرح می‌شوند. در حملات سایبری بسته به نوع حمله، یک و یا چند نوع از این مباحث از بین می‌روند. فضای حمله طبق ۳ اصل دانسته‌های[۴] مهاجم، منابع افشا[۵] و منابع اختلال[۶] تعریف می‌شود و بسته به نوع حمله به یک و یا چند اصل از اصول بالا نیاز است.

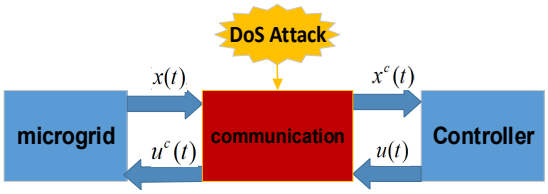
1. Confidentiality
2. Integrity
3. Availability
4. Knowledge
5. Disclosure
6. Disruption

حمله‌های سایبری به سه گروه کلی تقسیم می‌شوند: ۱) حمله منع سرویس (DoS)، ۲) حمله تکرار[۷] و ۳) حمله فریب[۸]. حمله DoS، در دسترس بودن و حمله فریب، محرمانه‌بودن و یکپارچگی اطلاعات سیستم را دچار مشکل می‌کنند. در روش DoS مهاجم سعی می‌کند که کانال ارتباطی را از طریق انسداد انتقال دیتا قطع کند و باعث از بین رفتن اطلاعات شود. در حمله تکرار از خروجی‌های قبلی سیستم استفاده شده و در زمان‌های حمله به عنوان خروجی اصلی جایگزین می‌گردند. در حمله فریب به خروجی سیستم پارامتری اضافه می‌گردد و باعث اختلال در خروجی می‌شود [۱۵] و [۳۶].

با توجه به این که DGها را به صورت سیستم چندعامله در نظر گرفتیم، حمله را می‌توان به ۲ نوع دیگر نیز دسته‌بندی کرد: ۱) حمله به گره‌ها و ۲) حمله به لینک‌های مخابراتی بین عامل‌ها. در حمله به گره‌ها، حمله به سنسور و عملگر اتفاق می‌افتد (حمله به $x_i(t)$ و $u_i(t)$). در حمله به لینک‌های مخابراتی، حمله به a_{ij} یعنی ارتباط بین DGهای مختلف مطرح شده و باعث می‌گردد که در لینک مخابراتی اطلاعات صحیح منتقل نشوند.

شکل کلی منابع تولید پراکنده به همراه حمله منع سرویس و کنترل‌کننده مورد استفاده به صورت شکل ۶ در نظر گرفته شده است. با توجه به شکل، حمله DoS ممکن است در کنترل‌کننده ثانویه یا بین اولیه و ثانویه اتفاق بیفتد و سیستم مخابراتی که با استفاده از تئوری گراف مدل شده است، ممکن است که دچار حمله سایبری گردد. در این حالت، منابع تولید پراکنده به صورت یک سیستم NCS در نظر گرفته می‌شوند و به ۲ قسمت لایه سایبری و فیزیکی تقسیم می‌گردند.

7. Reply Attack
8. Deception Attack



شکل ۷: تغییرات حالت و ورودی کنترل‌کننده DG در اثر حمله سایبری DoS.

در این مقاله حمله DoS باعث قطع‌شدن لینک‌های ارتباطی می‌گردد و حمله به a_{ij} یعنی لینک‌های ارتباطی بین عامل‌ها وارد می‌شود. حمله ممکن است باعث شود که لینک ارتباطی قطع شده و تعدادی از گره‌ها مجزا شوند و یا یک گره کلاً از دسترس خارج گردد. اگر حمله سایبری باعث شود که یک DG از دسترس خارج شود، امکان کنترل آن به این شیوه وجود ندارد.

شکل ۷ تغییرات حالت‌ها و عملگرها را در اثر حمله سایبری DoS نشان می‌دهد. با توجه به شکل در صورت حمله در انتقال اطلاعات از شبکه‌های ارتباطی، سیگنال حالت و کنترلی تغییر می‌کنند.

برای تحلیل درست منابع تولید پراکنده با در نظر گرفتن حمله‌های سایبری، ابتدا فرمول‌بندی مسأله ارائه می‌گردد. مقادیر گره‌ها در صورت حمله سایبری DoS با توجه به شکل ۷ به صورت رابطه زیر نشان داده می‌شوند

$$\begin{cases} x^c(t) = \theta^x(t)x(t) \\ u^c(t) = \theta^u(t)u(t) \end{cases} \quad (۱۴)$$

که $\theta^c(t)$ و $\theta^x(t)$ ماتریس‌های قطری هستند و به ترتیب برای مشخص‌شدن حمله DoS به حالت‌ها و ورودی کنترلی تعریف شده‌اند و می‌توان هر دو را در یک ماتریس به صورت $\theta = diag(\theta^x(t), \theta^u(t))$ در نظر گرفت. مقادیر $x^c(t)$، $u^c(t)$، $x(t)$ و $u(t)$ به ترتیب مقادیر حالت و ورودی کنترل‌کننده با وجود حمله و بدون حمله هستند. در سیستم بدون حمله سایبری DoS، ضرایب $\theta^x(t), \theta^u(t) = ۱$ و با وجود حمله $\theta^x(t), \theta^u(t) = ۰$ هستند. با توجه به شکل ۷ حمله سایبری DoS باعث تغییر مقادیر حالت‌ها و عملگرها به صورت زیر می‌گردد

$$\dot{x} = Ax + Bu^c(t)x + ch(x(t), w(t)) \quad (۱۵)$$

با در نظر گرفتن $u = kx^c(t) = k\theta^x(t)x(t)$

$$\dot{x} = Ax + B\theta^u(t)k\theta^x(t)x + ch(x(t), w(t)) \quad (۱۶)$$

و در نتیجه، ماتریس سیستم مختل‌شده به صورت رابطه $A^c(\theta(t)) = A + B\theta^u(t)k\theta^x(t)$ درمی‌آید

$$\dot{x}(t) = A^c\theta(t)x(t) + ch(x(t), w(t)) \quad (۱۷)$$

با توجه به ایده بالا و با توجه به (۹) تا (۱۲)، ورودی کنترلی و مقادیر سنسوری با وجود حمله سایبری DoS به صورت زیر به دست می‌آید

$$\begin{cases} u^c_{vi} = \theta^u_{iv}(t)u_{vi} \\ u^c_{\omega i} = \theta^u_{i\omega}(t)u_{\omega i} \\ u^c_{Pi} = \theta^u_{iP}u_{Pi} \end{cases}$$
$$\begin{cases} \omega^c_{oj} = \theta^x_{j\omega}\omega_{oj}(t) \\ v^c_{oj} = \theta^x_{jv}(t)v_{oj}(t) \\ P^c_j = \theta^x_{jP}P_j \end{cases} \quad (۱۸)$$

که $\theta^x_{jv}(t)$، $\theta^x_{i\omega}(t)$ و $\theta^x_{jP}(t)$ به ترتیب مربوط به حمله DoS به سنسور فرکانس، ولتاژ و توان اکتیو و $\theta^u_{iv}(t)$، $\theta^u_{i\omega}(t)$ و $\theta^u_{iP}(t)$ مربوط به حمله به عملگر فرکانس، ولتاژ و توان هستند. با جایگذاری (۱۸) در (۱۰) و (۱۱) ورودی کنترلی به صورت زیر به دست می‌آید

$$\begin{cases} u^c_{vi} = \theta^u_{iv}(t)u_{vi} \\ \quad = -\theta^u_{iv}(t)C_v\sum a_{ij}(v_{oi} - v^c_{oj}) + g_i(v_{oi} - v_{ref}) \\ u^c_{\omega i} = \theta^u_{i\omega}(t)u_{\omega i} \\ \quad = -\theta^u_{i\omega}C_\omega\sum a_{ij}(\omega_{oi} - \omega^c_{oj}) + g_i(\omega_{oi} - \omega_{ref}) \\ u^c_{Pi} = \theta^u_{iP}u_{Pi} = -\theta^u_{iP}C_P\sum a_{ij}(m_{pi}P_i - m_{pj}P^c_j) \end{cases} \quad (۱۹)$$

و بنابراین سیگنال کنترلی ولتاژ با جایگذاری در (۱۲) به صورت زیر به دست می‌آید

$$V^*_{ni} = \int[-\theta^u_{iv}C_v\sum a_{ij}(v_{oi} - \theta^x_{jv}v_{oj}) + g_i(v_{oi} - v_{ref}) + \dot{Q}_i]\mathrm{d}t \quad (۲۰)$$

و به همین ترتیب کنترل‌کننده فرکانس با حمله سایبری به صورت زیر بازنویسی می‌گردد

$$\omega^*_{ni} = \int(u^c_{\omega i} + u^c_{Pi})\mathrm{d}t \quad (۲۱)$$

با جایگذاری مقادیر (۱۸) در (۲۱)، ورودی کنترلی به دست می‌آید

$$\omega^*_{ni} = \int[-\theta^u_{i\omega}C_\omega[a_{ij}(\omega_{oi} - \theta^x_{j\omega}\omega^c_{oj}) + g_i(\omega_{oi} - \omega_{ref}) - \theta^u_{ip}C_P[a_{ij}(m_{pi}P_i - m_{Pj}\theta^x_{jP}P_j]\mathrm{d}t \quad (۲۲)$$

۶- اثبات پایداری

با فرض حمله DoS در کانال ارتباطی، سیگنال کنترلی با وجود حمله سایبری بر اساس سیگنال خطا به صورت (۲۳) به دست می‌آید. در این مقاله حمله سایبری در کنترل ثانویه برای سنسورها در نظر گرفته نشده است، یعنی $\theta^x_{iv}(t), \theta^x_{i\omega}(t), \theta^x_{ip}(t) = ۱$ می‌باشد. با در نظر گرفتن (۱۸) و (۱۹)، روابط زیر به دست می‌آیند

$$\begin{aligned} u^c_{vi} &= -\theta_{iv}C_v e_{vi} \\ e_{vi} &= \sum a_{ij}(v_{.i}(t) - v_{.j}(t)) + g_i(v_{.i}(t) - v_{ref}) \\ u^c_{vi} &= -\theta^c_{iv}C_v[\sum a_{ij}(v_{.i}(t) - v_{.j}(t)) + g_i(v_{.i}(t) - v_{ref})] \end{aligned} \quad (۲۳)$$

برای اثبات پایداری رابطه بالا، لم ۱، لم ۲ و قضیه در ادامه در نظر گرفته می‌شود. در [۳۷] و [۳۸] توضیحات جامعی در رابطه با لم ۱ و ۲ برای سنکرون‌سازی سیستم‌های خطی آمده که در این مقاله از آنها برای سنکرون‌سازی منابع تولید پراکنده استفاده گردیده است. در ابتدا برای سنکرون‌سازی، سیگنال عدم تطابق به صورت (۲۴) تعریف می‌گردد

$$\delta = v_{od} - v_{ref} \quad (۲۴)$$

لم ۱: فرض کنید گراف G یک درخت پیوسته بوده و حداقل یک گره ریشه $g_i \neq ۰$ داشته باشد. ارتباط خطای سیستم و سیگنال عدم تطابق به صورت $e = (L+G)\delta$ تعریف می‌شود و بنابراین

$$\sigma_{\min}(L+G)\|\delta\| \le \|e\| \Rightarrow \|\delta\| \le \frac{\|e\|}{\sigma_{\min}}(L+G) \quad (۲۵)$$

در این فرمول $\sigma_{\min}$ مقدار ویژه مینیمم ماتریس $L+G$ است. در این صورت e برابر صفر است، اگر و فقط اگر همه گره‌ها سنکرون باشند.

توجه: اگر همه گره‌ها سنکرون باشند، در نتیجه $\|\delta\| \to ۰$ و بنابراین $v_{od} = v_{ref}$ است (علاوه بر سنکرون‌بودن، مقادیر برابر با v_{ref} می‌گردند). پس یکی از اصلی‌ترین شرایط برای برقراری قوانین رینولد برقرار می‌شود.

اثبات لم ۱: بردار خطای کل به صورت زیر در نظر گرفته می‌شود

$$e_v = (L+G)(v_{od} - v_{ref}) = (L+G)\delta \qquad (۲۶)$$

که در رابطه بالا $v_{od} = [v_{od۱}\ v_{od۲} \dots v_{odn}]^T$ و $e_v = [e_{v۱}\ e_{v۲} \dots e_{vn}]^T$ به صورت ماتریس هستند. $v_{ref} = ۱_N \otimes v_{ref}$ که ۱_N بردار یک با طول N است و $\otimes$ ضرب کرونکر می‌باشد. بردار G ماتریس قطری با مقدار قطر g_i و L ماتریس لاپلاسین است. با استفاده از (۲۶) بر اساس قوانین نرم تابع داریم

$$\begin{aligned} &\|e_v\| = \|L+G\|\|\delta\| \\ &\sigma_{\min}(L+G) \le \|L+G\| \le \sigma_{\max}(L+G) \\ &\|e\| = \|L+G\|\|\delta\| \Rightarrow \|e\| \ge \sigma_{\min}(L+G)\|\delta\| \\ &\|\delta\| \le \frac{\|e\|}{\sigma_{\min}(L+G)} \end{aligned} \qquad (۲۷)$$

با توجه به رابطه بالا، اگر $\|e\| \to ۰$ برود، آن گاه $\|\delta\| \to ۰$ می‌رود $(v_{.di} = v_{ref})$ و سنکرون‌سازی انجام می‌گردد. همچنین در صورت سنکرون‌سازی، $\delta = v_{.d_i} - v_{ref} = ۰$ و با توجه به (۲۶) خطا صفر می‌شود. □

لم ۲: فرض کنید گراف مستقیم G یک درخت پیوسته و برای حداقل یکی از گره‌های ریشه، $g_i \neq ۰$ است. ماتریس $D+G$ را در نظر بگیرید. با توجه به این که $D+G = (D+G)^T$ و $A = L+G$ است، در این صورت $Q = (D+G)A + A^T(D+G)$ مثبت معین است [۳۸].

توجه: $D+G$ در (۲) و (۴) تعریف گردیده و ماتریس مثبت معین است و به همین دلیل در معادله بالا استفاده شده است.

قضیه ۱: فرض کنید که G یک درخت پیوسته است و حداقل برای یکی از منابع تولید پراکنده، $g_i \neq ۰$ باشد. اگر ورودی کنترلی ثانویه u_{vi} به صورت $u_{vi}^c = -C_v \theta_{vi}^c e_{vi}$ تعریف شود، در این صورت خطای e در $e = (L+G)\delta$ پایدار مجانبی است. همچنین ولتاژ خروجی DGها به v_{ref} سنکرون می‌شوند.

اثبات: از معادله قبل، بردار $u_v = [u_{v_۱}\ u_{v_۲} \dots u_{vn}]^T = -C_v e_v$ تعریف می‌گردد و به منظور اثبات پایداری، تابع کاندیدای لیاپانوف به صورت زیر در نظر گرفته می‌شود

$$\begin{aligned} &V = \frac{۱}{۲} e_v^T (D+G) e_v \\ &D+G = (D+G)^T \\ &D+G > ۰ \end{aligned} \qquad (۲۸)$$

با توجه به این که $(e_v^T(D+G)\dot{e}_v)^T = \dot{e}_v(D+G)e_v$ می‌باشد، مشتق تابع لیاپانوف برابر است با

$$\dot{V} = \frac{۱}{۲}\dot{e}_v^T(D+G)e_v + \frac{۱}{۲}e_v^T(D+G)\dot{e}_v = e_v^T(D+G)\dot{e}_v \qquad (۲۹)$$

با توجه به (۲۴) و (۲۵) و با در نظر گرفتن حمله سایبری DoS در معادله‌های خروجی، معادله مشتق خطا به صورت زیر به دست می‌آید

$$\dot{e}_v = (L+G)\dot{\delta} = (L+G)\dot{v}_{od} \qquad (۳۰)$$

با توجه به (۹)، (۱۰) و (۱۸) و جایگذاری آنها در (۲۹)، مشتق لیاپانوف به دست می‌آید

$$\begin{aligned} &\dot{v}_{od} = u_v^c = -C_v \theta_v^c e_{vi} \\ &\dot{V} = e_v^T(D+G)(L+G)\dot{\delta} = e_v^T(D+G)(L+G)\dot{v}_{od} \end{aligned} \qquad (۳۱)$$

از دو معادله بالا نتیجه گرفته می‌شود

$$\begin{aligned} &\dot{V} = e^T(D+G)(L+G)(-C_V\theta_v^C e_{vi}) \\ &X = (D+G)(L+G)\theta_v^C \end{aligned} \qquad (۳۲)$$

$$\dot{V} = -C_V e_v^T X e_v \qquad (۳۳)$$

هر ماتریس مربعی را می‌توان به صورت جمع دو ماتریس زیر نوشت

$$X = \frac{۱}{۲}[X + X^T] + \frac{۱}{۲}[X - X^T] \qquad (۳۴)$$

با جایگذاری در (۳۳)، $\dot{V} = -C_V\{e_v^T[\frac{۱}{۲}(X+X^T + \frac{۱}{۲}(X-X^T)]e_v$ و با توجه به این که $e_v^T \frac{X-X^T}{۲} e_v = ۰$ است

$$\dot{V} = -\frac{C_v}{۲} e_V^T (X + X^T) e_v \qquad (۳۵)$$

با توجه به لم ۲، $Q = X + X^T$ مثبت معین است و بنابراین

$$\dot{V} = \frac{-C_v}{۲} e_v^T Q e_v \le ۰ \qquad (۳۶)$$

با توجه به منفی معین بودن مشتق تابع لیاپانوف، خطای e_v پایدار مجانبی است.

با توجه به لم ۱ اگر e_v پایدار مجانبی باشد، بردار δ نیز پایدار مجانبی است و V_{ref} به $V_{.di}$ سنکرون می‌شود. برای اثبات سنکرون‌سازی مجانبی باید اثبات کنیم که خطای حالت ماندگار صفر می‌شود و $\lim_{t\to\infty} e \to ۰$.

فرمول $\dot{V} = -\frac{C_v}{۲} e_v^T Q e_v$ و $V = \frac{۱}{۲} e^T D e$ را در نظر بگیرید

$$\begin{aligned} &\dot{V} \le -\frac{C_v}{۲}\sigma_{\min}(Q)\|e\|^۲ \le -\frac{C_v}{۲}\frac{\sigma_{\min}(Q)}{\sigma_{\max}(D)} V = -\gamma V \\ &\to V \le e^{-\gamma t} V(t_۰) \\ &\lim_{t\to\infty} e^{-\gamma t} V(t_۰) \to ۰ \Rightarrow \lim_{t\to\infty} V \to ۰ \Rightarrow e \to ۰ \Rightarrow \delta \to ۰ \end{aligned} \qquad (۳۷)$$

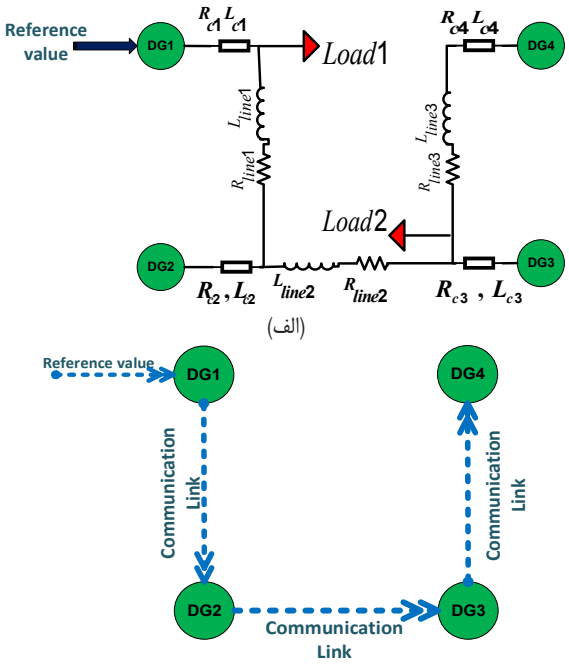
که $\sigma_{\min}$ و $\sigma_{\max}$ به ترتیب مینیمم و ماکسیمم مقدار ویژه می‌باشند.

نتیجه می‌شود که سنکرون‌سازی انجام می‌گردد و یکی از اهداف سیستم به عنوان سیستم چندعامله تحقق می‌یابد. همچنین هرچه C_v بزرگ‌تر باشد، سرعت سنکرون‌سازی مناسب‌تر است و بنابراین با انتخاب مناسب C_v و تأثیر آن در u_v، سنکرون‌سازی بهینه‌ای انجام می‌پذیرد. □

با اثبات بالا نتیجه می‌گیریم که در صورت پیوستگی درخت و این که حداقل یکی از منابع تولید پراکنده به شین اسلک وصل باشد، این کنترل‌کننده حتی با حمله سایبری DoS پایداری سیستم را حفظ می‌کند و می‌تواند به صورت یک سیستم چندعامله ولتاژ و فرکانس همه DGها را یکسان کند.

۷- نتایج شبیه‌سازی

برای شبیه‌سازی از یک مدل نمونه طبق [۴] با شکل ۸ استفاده گردیده و DG۱ به عنوان شین مرجع یا اسلک در نظر گرفته شده است. پارامترهای این DGها (شامل ۴ منبع توزیع‌شده) در جدول ۱ آمده است.



(الف)

(ب)

شکل ۸: (الف) مدل نمونه شبیه‌سازی‌شده اتصال سیستم قدرتی و (ب) به همراه لینک‌های مخابراتی.

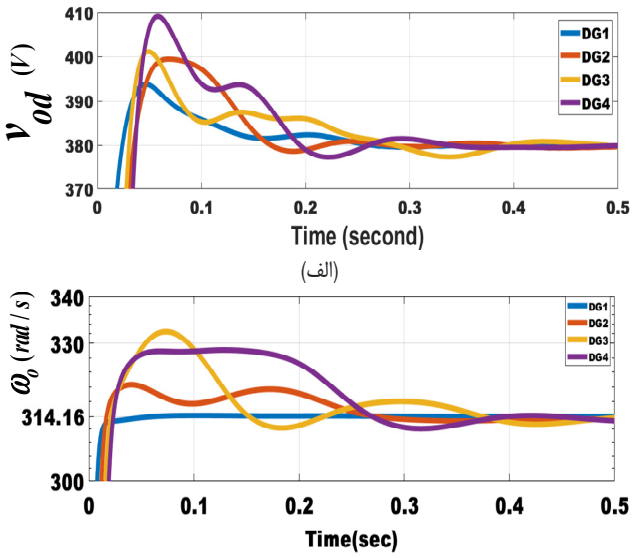
جدول ۱: مقادیر پارامترهای مدل نمونه شبیه‌سازی‌شده [۴].

DG۱ و DG۲	DG۳ و DG۴
$n_q = ۱/۳\times۱۰^{-۳}$	$n_q = ۱/۵\times۱۰^{-۳}$
$m_p = ۹/۴\times۱۰^{-۵}$	$m_p = ۱۲/۵\times۱۰^{-۵}$
$R_{c۱,۲} = ۰/۰۳\Omega$	$R_{c۲,۴} = ۰/۰۳\Omega$
$L_{c۱,۲} = ۰/۳۵\,\text{mH}$	$L_{c۲,۴} = ۰/۳۵\,\text{mH}$
$K_{pv} = ۱$	$K_{pv} = ۱$
$K_{IV} = ۴$	$K_{IV} = ۴$
$K_{PC} = ۱۵$	$K_{PC} = ۱۰/۵$
$K_{IC} = ۲۰۰$	$K_{IC} = ۱۶۰$
$R_{line۱} = ۰/۲۳\Omega$ $R_{line۲} = ۰/۳۵\Omega$ $R_{line۳} = ۰/۲۳\Omega$	
$L_{line۱} = ۰/۳۱۸\,\text{mH}$ $L_{line۲} = ۱/۸۴۷\,\text{mH}$ $L_{line۱} = ۰/۳۱۸\,\text{mH}$	
$P_{load۱(per\ phase)} = ۱۲\,\text{Kw}$ $Q_{load۱(per\ phase)} = ۱۲\,\text{Kvar}$	
$P_{load۲(per\ phase)} = ۱۵/۳\,\text{Kw}$ $Q_{load۲(per\ phase)} = ۷/۶\,\text{Kvar}$	

L_{ci} و R_{ci} اندوکتانس و مقاومت رابط‌های خروجی DG_i[1] می‌باشند. همچنین خطوط بین DGها با یک شاخه RL سری مدل شده و R_{line} و L_{line} مقاومت و اندوکتانس آنها هستند و نیز بارها به صورت $P_{load} + jQ_{load}$ در نظر گرفته شده‌اند. K_{IC}، K_{PC} و K_{IV} و K_{PV} ضرایب کنترل‌کننده PI کنترل‌کننده ولتاژ و جریان در شکل ۱ و شکل ۳- ب می‌باشند.

در این مدل، ولتاژ مرجع ۳۸۰ ولت و فرکانس مرجع ۵۰ هرتز (فرکانس زاویه‌ای $\omega_{ref} = ۲\pi f_{ref} = ۳۱۴/۱۶^{\text{rad/sec}}$) در نظر گرفته شده است. منابع تولید پراکنده به دو طریق قدرتی و مخابراتی با هم ارتباط دارند. در شکل ۸- الف توپولوژی قدرتی و همچنین توپولوژی ارتباطی آن در شکل ۸- ب آمده است. به منظور تحلیل بهتر سیستم، نتایج شبیه‌سازی در محیط سیمولینک متلب به صورت سناریوهای مختلف مورد ارزیابی قرار گرفته است.

1. Output Connector



(الف)

(ب)

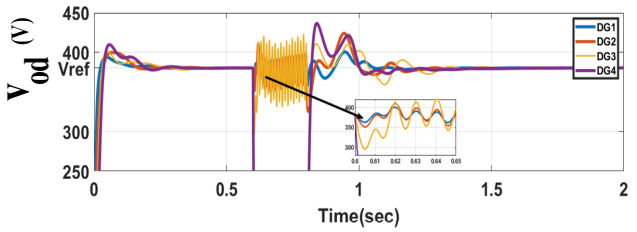
شکل ۹: (الف) ولتاژ خروجی و (ب) فرکانس زاویه‌ای خروجی DGها بدون حمله سایبری، اغتشاش و نویز.

سناریوی اول: عملکرد کنترل‌کننده اولیه و ثانویه بدون اغتشاش، نویز و حملات سایبری

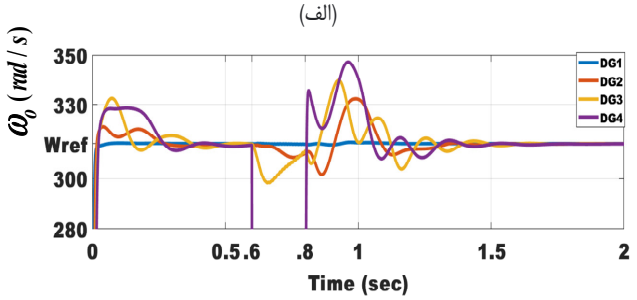
در ابتدا خروجی، بدون واردکردن اغتشاش، نویز یا حمله سایبری در نظر گرفته می‌شود تا عملکرد کنترل‌کننده طراحی‌شده مشخص گردد. شکل ۹- الف و ۹- ب خروجی ولتاژ و فرکانس با کنترل‌کننده ثانویه و اولیه را در این حالت نشان می‌دهند. با توجه به نتایج، کنترل‌کننده توانسته که به خوبی فرکانس و ولتاژ را به حالت مرجع خود برگرداند و در رنج بسیار خوبی قرار دهد. زمان عبور از حالت گذرا کمتر از ۰/۳ ثانیه بوده که زمان مناسبی می‌باشد و مقدار بالازدگی سیستم به نحوی است که قابل تحمل می‌باشد و نیاز به خارج‌کردن بارها از شبکه نداریم. همچنین سنکرون‌سازی بسیار خوب انجام شده است.

سناریوی دوم: حمله سایبری DoS بین DG۳ و DG٤

در این سناریو بررسی می‌شود که این کنترل‌کننده چقدر می‌تواند در برابر حمله سایبری DoS از خود مقاومت نشان داده و حمله را کنترل کند. برای تحلیل بهتر، حمله سایبری در لینک‌های مختلف بررسی می‌گردد. اگر حمله سایبری در کانال ارتباطی بین DG۳ و DG۴ اتفاق بیفتد، از ریزشبکه سوم به چهارم اطلاعاتی نمی‌رسد. در اینجا فرض شده که از زمان ۰/۶ تا ۰/۸ ثانیه حمله سایبری اتفاق افتاده و لینک ارتباطی را در این زمان قطع می‌کند. نتایج در شکل ۱۰ نشان داده شده است. سیستم کنترل‌کننده با توجه به نتایج، توانایی کنترل خروجی‌های DG۱، DG۲ و DG۳ را دارد، ولی با توجه به این که DG۴ از شبکه قطع می‌گردد و اطلاعاتی به آن نمی‌رسد، ارتباطش با گره اسلک قطع شده و این منبع نمی‌تواند در زمان حمله، مقادیر خروجی را بازیابی کند. هر وقت حمله سایبری باعث شود که پیوستگی گراف از بین برود، آن منبع از مدار خارج می‌شود و از نظر سیستم‌های چندعامله، علت اصلی که DG۴ در زمان حمله از پایداری خارج شده است، آن است که در این حالت منبع تولید پراکنده از شین اسلک جدا می‌گردد. اما با توجه به شکل ۱۰، DGهای اول، دوم و سوم توانستند با وجود حمله سایبری DoS به پایداری برسند و سنکرون‌سازی را انجام دهند. همچنین بعد از اتمام حمله خروجی، همه منابع تولید پراکنده بعد از چند لحظه به مقدار قبلی برگشته و خروجی‌ها بازیابی می‌گردند. نکته مهم دیگر این که حمله در این حالت در DG۳

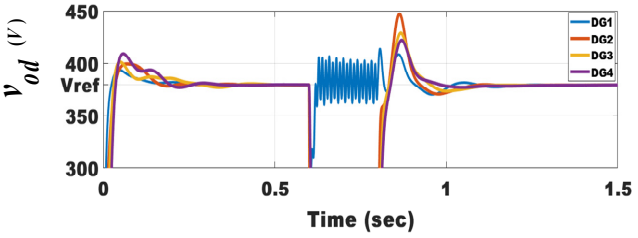


(الف)

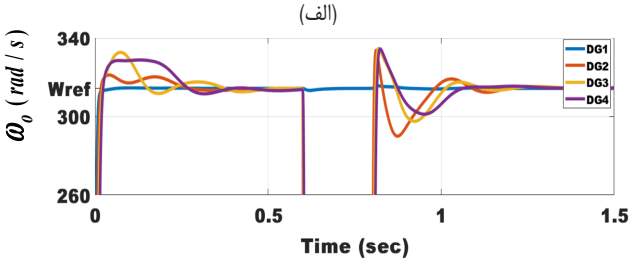


(ب)

شکل ۱۰: (الف) ولتاژ و (ب) فرکانس زاویه‌ای خروجی منابع تولید پراکنده با حمله سایبری DoS در لینک ارتباطی بین DG۳ و DG۴.



(الف)



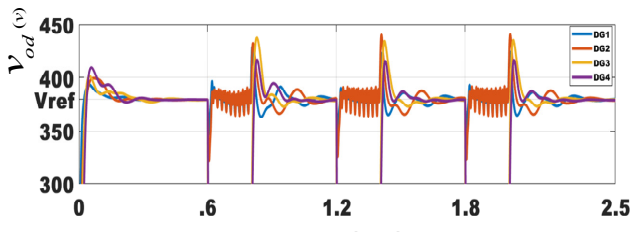
(ب)

شکل ۱۱: (الف) ولتاژ و (ب) فرکانس خروجی منابع تولید پراکنده با حملات سایبری DoS بین کانال ارتباطی DG۱ و DG۲.

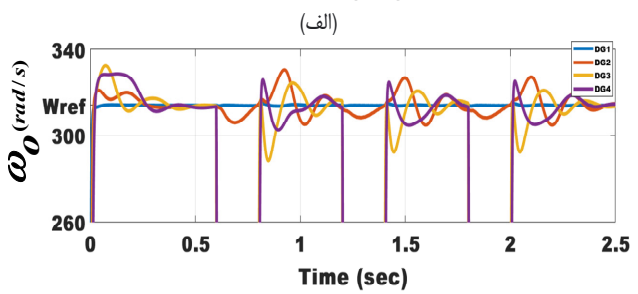
بیشتر از بقیه منابع تأثیر می‌گذارد و به ترتیب DG۲ و DG۱ اثرپذیری دارند. این نتیجه نشان می‌دهد که هر قدر به مبدأ حمله نزدیک‌تر باشند، اثرپذیری بیشتری دارند.

سناریوی سوم: حمله سایبری DoS در لینک ارتباطی بین DG۱ و DG۲

در این سناریو فرض شده که حمله بین لینک‌های منبع تولید پراکنده اول و دوم اتفاق بیفتد و ارتباط بین این لینک‌ها از ۰٫۶ تا ۰٫۸ قطع می‌گردد. نتایج این شبیه‌سازی در شکل ۱۱ آمده است. با توجه به شکل مشخص است که با توجه به این که DG۲، DG۳ و DG۴ از باس اسلک قطع می‌شوند، به همین دلیل خروجی این منابع به مقدار مرجع در زمان حمله بازیابی نمی‌گردد. در نتیجه درخت پیوستگی خود را از دست می‌دهد و آن منابع، رها و کلاً از مدار خارج می‌شوند. در این حالت از بین منابع موجود، فقط منبع اول توانسته است تا به پایداری قابل قبولی برسد و عملیات سنکرون‌سازی در حین حمله را انجام دهد. ولی بعد از رفع حمله، همه منابع توانسته‌اند که مقادیر خروجی خود را بازیابی کنند و نشان می‌دهد که کنترل‌کننده به خوبی می‌تواند به حالت سنکرون خود برگردد.



(الف)



(ب)

شکل ۱۲: (الف) ولتاژ و (ب) فرکانس خروجی منابع تولید پراکنده با حملات سایبری DoS متناوب بین کانال ارتباطی DG۲ و DG۳.

سناریوی چهارم: حمله سایبری DoS متناوب در لینک ارتباطی بین DG۲ و DG۳

در این سناریو، حمله DoS متناوب با دوره تناوب ۰٫۶ ثانیه بین لینک‌های ارتباطی منبع تولید پراکنده دوم و سوم اتفاق می‌افتد. این سناریو برای بررسی توانایی روش کنترلی ارائه‌شده در قطع و وصل‌های پیوسته و همچنین در مقابل یک حمله سایبری شدیدتر است. نتایج این شبیه‌سازی در شکل ۱۲ آمده است. با توجه به شکل و این که DG۳ و DG۴ در هر بار حمله از باس اسلک قطع می‌شوند، به همین دلیل خروجی‌ها به مقدار مرجع در زمان حمله بازیابی نمی‌گردند. بعد از رفع حمله، حدود ۰٫۴ ثانیه طول می‌کشد تا همه منابع بتوانند مقادیر خروجی خود را بازیابی کنند. عملکرد کنترل‌کننده در مقابله این حمله شدید نیز بسیار خوب ارزیابی می‌گردد و به محض اتمام حمله توانسته تا خروجی‌ها را بازیابی و سنکرون کند.

با توجه به نتایج شبیه‌سازی، اگر حمله سایبری باعث شود تا ارتباط هر منبع تولید پراکنده با عامل ریشه قطع گردد، آن منبع از مدار خارج می‌شود، ولی اگر حمله سایبری DoS در لینک‌هایی اتفاق بیفتد که پیوستگی درخت قطع نشود، می‌توان مقادیر ولتاژ و فرکانس بقیه را با مقدار مرجع هماهنگ کرد و پایداری سیستم حفظ می‌گردد.

۸- نتیجه‌گیری

در این مقاله با در نظر گرفتن منابع تولید پراکنده به صورت سیستم‌های چندعامله، در مورد کنترل و سنکرون‌سازی ریزشبکه بحث گردید و به منظور تحلیل این منابع و همچنین لینک‌های ارتباطی بین آنها از تئوری گراف استفاده شد. از کنترل‌کننده سلسه‌مراتبی توزیع‌شده اشتراکی که شامل کنترل‌کننده اولیه و ثانویه است برای کنترل DGها استفاده گردید و نتایج نشان می‌دهند که کنترل‌کننده، بدون حمله سایبری و اغتشاش، هم پایداری و هم سنکرون‌سازی ریزشبکه را حفظ می‌کند و قوانین سیستم‌های چندعامله ریموند با این کنترل‌کننده رعایت می‌گردد و نهایتاً ولتاژ و فرکانس همه منابع توزیع پراکنده با هم برابر می‌شوند. سپس به عنوان نوآوری مقاله، حمله سایبری منع سرویس در معادلات منابع تولید پراکنده با کنترل‌کننده سلسه‌مراتبی توزیع‌شده وارد گردید و اثرات

این حمله سایبری مورد بررسی قرار گرفت. به منظور تحلیل پایداری سیستم، تابع لیاپانوف مناسب با حضور حمله سایبری منع سرویس پیشنهاد گردید و با کمک فرمول‌بندی ریاضی، پایداری آن اثبات شد. همچنین برای اثبات سنکرون‌سازی ولتاژ و فرکانس خروجی منابع مختلف، لم‌های مناسب با شرایط حمله سایبری ارائه شد و شرایط پایداری و سنکرون‌سازی به دست آمد.

نهایتاً برای اطمینان از نتایج تئوری با استفاده از شبیه‌سازی در محیط سیمولینک نرم‌افزار متلب، اثر حمله در لینک‌های مختلف برای یک شبکه نمونه نشان داده شده است. با توجه به نتایج شبیه‌سازی در صورت حمله سایبری منع سرویس و به شرط پیوستگی درخت در نظر گرفته شده از لینک‌های ارتباطی، این کنترل‌کننده توانسته است که پایداری را حفظ کند و همچنین مقادیر فرکانس و ولتاژ با مقادیر مرجع هماهنگ می‌گردند. DGهایی که به گره اسلک وصل نباشند، ناپایدار شده و باید از مدار خارج شوند. نتایج حاصل از شبیه‌سازی نشان می‌دهند که هر قدر اطلاعات بیشتری از سیستم DG همجوار داشته باشیم، این روش کنترلی بهتر پایداری را حفظ خواهد کرد.

مراجع

[1] S. M. Azimi and S. Lotfifard, "Supplementary controller for inverter-based resources in weak power grids," *IEEE Trans. on Smart Grid*, vol. 13, no. 4, pp. 2886 - 2896, Jul. 2022.

[2] S. Derakhshan, M. Shafiee-Rad, Q. Shafiee, and M. R. Jahed-Motlagh, "Decentralized robust voltage control of islanded AC microgrids: an LMI-based H_∞ approach," in *Proc. 11th IEEE Power Electronics, Drive Systems, and Technologies Conf., PEDSTC'20,* 6 pp., Tehran, Iran, 4-6 Feb. 2020.

[3] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Trans. on Smart Grid*, vol. 3, no. 4, pp. 1963-1976, Dec. 2012.

[4] A. Bidram, F. L. Lewis, and A. Davoudi, "Distributed control systems for small-scale power networks: using multiagent cooperative control theory," *IEEE Control Systems Magazine*, vol. 34, no. 6, pp. 56-77, Dec. 2014.

[5] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed secondary control for islanded microgrids-a novel approach," *IEEE Trans. on Power Electronics*, vol. 29, no. 2, pp. 1018-1031, Feb. 2014.

[6] A. Bidram, A. Davoudi, F. L. Lewis, and Z. Qu, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Generation, Transmission & Distribution*, vol. 7, no. 8, pp. 822-831, Aug. 2013.

[7] Z. Shahbazi, A. Ahmadi, A. Karimi, and Q. Shafiee, "Performance and vulnerability of distributed secondary control of AC microgrids under cyber-attack," in *Proc. 7th IEEE Int, Conf. on Control, Instrumentation and Automation, ICCIA'21,* 6 pp., Tabriz, Iran, 23-24 Feb. 2021.

[8] X. Wang and M. Lemmon, "On event design in event-triggered feedback systems," *Automatica*, vol. 47, no. 10, pp. 2319-2322, Oct. 2011.

[9] Z. Gu, Z. Huan, D. Yue, and F. Yang, "Event-triggered dynamic output feedback control for networked control systems with probabilistic nonlinearities," *Information Sciences*, vol. 457-458, pp. 99-112, Aug. 2018.

[10] Y. L. Wang, P. Shi, C. C. Lim, and Y. Liu, "Event-triggered fault detection filter design for a continuous-time networked control system," *IEEE Trans. on Cybernetics*, vol. 46, no. 12, pp. 3414-3426, Dec. 2016.

[11] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101-115, Apr. 2019.

[12] H. Yan, J. Wang, H. Zhang, H. Shen, and X. Zhan, "Event-based security control for stochastic networked systems subject to attacks," *IEEE Trans. on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 11, pp. 4643-4654, Nov. 2018.

[13] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under DoS attacks: a unified game approach," *IEEE Trans. on Industrial Informatics*, vol. 12, no. 5, pp. 1786-1794, Oct. 2016.

[14] H. Modares, B. Kiumarsi, F. L. Lewis, F. Ferrese, and A. Davoudi, "Resilient and robust synchronization of multiagent systems under attacks on sensors and actuators," *IEEE Trans. on Cybernetics*, vol. 50, no. 3, pp. 1240-1250, Mar. 2020.

[15] X. M. Zhang, Q. L. Han, X. Ge, and L. Ding, "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Trans. on Cybernetics*, vol. 50, no. 8, pp. 3616-3626, Aug. 2020.

[16] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proc. of the 1st Int. Conf. on High Confidence Networked Systems*, *HiCoNS'12*,pp. 55-64, Beijing, China, 17-18 Apr. 2012.

[17] E. Mousavinejad, F. Yang, Q. L. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Trans. on Cybernetics*, vol. 48, no. 11, pp. 3254-3264, Nov. 2018.

[18] S. Zuo, T. Altun, F. L. Lewis, and A. Davoudi, "Distributed resilient secondary control of DC microgrids against unbounded attacks," *IEEE Trans. on Smart Grid*, vol. 11, no. 5, pp. 3850-3859, Sept. 2020.

[19] B. Wang, Q. Sun, and D. Ma, "A periodic event-triggering reactive power sharing control in an islanded microgrid considering DoS attacks," in *Proc. of the 15th IEEE Conf. on Industrial Electronics and Applications, ICIEA'20*, pp. 170-175, Kristiansand, Norway, 9-13 Nov. 2020.

[20] R. Lu and J. Wang, "Distributed control for AC microgrids with false data injection attacks and time delays," in *Proc. of the E3S Web of Conf.*, vol. 194, Article ID: 03023, Shanghai, China, 18-20 Sept. 2020.

[21] S. Tan, P. Xie, J. M. Guerrero, and J. C. Vasquez, "False data injection cyber-attacks detection for multiple DC microgrid clusters," *Applied Energy*, vol. 310, Article ID: 118425, Mar. 2022.

[22] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. on Automatic Control*, vol. 60, no. 11, pp. 2930-2944, Nov. 2015.

[23] B. Wang, Q. Sun, R. Han, and D. Ma, "Consensus-based secondary frequency control under denial-of-service attacks of distributed generations for microgrids," *J. of the Franklin Institute*, vol. 358, no. 1, pp. 114-130, Jan. 2019.

[24] P. Chen, S. Liu, B. Chen, and L. Yu, "Multi-agent reinforcement learning for decentralized resilient secondary control of energy storage systems against DoS attacks," *IEEE Trans. on Smart Grid*, vol. 13, no. 3, pp. 1739-1750, May 2022.

[25] A. Karimi, A. Ahmadi, Z. Shahbazi, H. Bevrani, and Q. Shafiee, "On the impact of cyber-attacks on distributed secondary control of DC microgrids," in *Proc. 10th of the IEEE Smart Grid Conf., SGC'20,* , 6 pp., Kashan, Iran, 16-17 Dec. 2020.

[26] X. Chen, J. Zhou, M. Shi, Y. Chen, and J. Wen, "Distributed resilient control against denial of service attacks in DC microgrids with constant power load," *Renewable and Sustainable Energy Reviews*, vol. 153, Article ID: 111792, Jan. 2022.

[27] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Trans. on Industrial Informatics*, vol. 15, no. 7, pp. 4066-4075, Jul. 2018.

[28] N. Pogaku, M. Prodanovic, and T. C. Green, "Modeling, analysis and testing of autonomous operation of an inverter-based microgrid," *IEEE Trans. on Power Electronics*, vol. 22, no. 2, pp. 613-625, Mar. 2007.

[29] A. Bidram, A. Davoudi, F. L. Lewis, and J. M. Guerrero, "Distributed cooperative secondary control of microgrids using feedback linearization," *IEEE Trans. on Power Systems*, vol. 28, no. 3, pp. 3462-3470, Aug. 2013.

[30] J. W. Simpson-Porco, *et al*., "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Trans. on Industrial Electronics*, vol. 62, no. 11, pp. 7025-7038, Nov. 2015.

[31] H. Z. Frank L. Lewis, Kristian Hengster-Movric, and A. Das, *Cooperative Control of Multi-Agent Systems Optimal and Adaptive Design Approaches*, SpringerLink, 2014.

[32] F. Guo, C. Wen, J. Mao, J. Chen, and Y. D. Song, "Distributed cooperative secondary control for voltage unbalance compensation in an islanded microgrid," *IEEE Trans. on Industrial Informatics*, vol. 11, no. 5, pp. 1078-1088, Oct. 2015.

[33] H. Cai, F. L. Lewis, G. Hu, and J. Huang, "The adaptive distributed observer approach to the cooperative output regulation of linear multi-agent systems," *Automatica*, vol. 75, pp. 299-305, Jan. 2017.

[34] J. C. Vasquez, J. M. Guerrero, J. Miret, M. Castilla, and L. G. De Vicuna, "Hierarchical control of intelligent microgrids," *IEEE Industrial Electronics Magazine*, vol. 4, no. 4, pp. 23-29, Dec. 2010.
[35] J. P. Lopes, C. Moreira, and A. Madureira, "Defining control strategies for microgrids islanded operation," *IEEE Trans. on Power Systems*, vol. 21, no. 2, pp. 916-924, May 2006.
[36] A. Kazemy, J. Lam, and Z. Chang, "Adaptive event-triggered mechanism for networked control systems under deception attacks with uncertain occurring probability," *International J. of Systems Science*, vol. 21, no. 7, pp. 1426-1439, 2020.
[37] H. Zhang, F. L. Lewis, and A. Das, "Optimal design for synchronization of cooperative systems: state feedback, observer and output feedback," *IEEE Trans. on Automatic Control*, vol. 56, no. 8, pp. 1948-1952, Aug. 2011.
[38] Z. Qu, *Cooperative Control of Dynamical Systems: Applications to Autonomous Vehicles*, Springer Science & Business Media, 2009.

عبدالله میرزابیگی تحصیلات خود را در مقاطع کارشناسی مهندسی برق الکترونیک در سال ۱۳۸۲ از دانشگاه تبریز و کارشناسی ارشد مهندسی برق کنترل در سال ۱۳۸۵ از دانشگاه علم و صنعت ایران به پایان رسانده است و هم‌اکنون دانشجوی دکتری برق کنترل دانشگاه تفرش می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: ریزشبکه، آنالیز و کنترل سیستم‌های با تاخیر زمانی، سیستم‌های چندعامله و حملات سایبری.

علی کاظمی تحصیلات خود را در مقاطع کارشناسی ارشد و دکتری مهندسی برق کنترل به‌ترتیب در سال‌های ۱۳۸۶ و ۱۳۹۲ از دانشگاه علم و صنعت ایران به پایان رسانده است و هم‌اکنون دانشیار دانشکده مهندسی برق دانشگاه تفرش می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: آنالیز و کنترل سیستم‌های با تاخیر زمانی، سیستم‌های چندعامله، سیستم‌های پیچیده و حملات سایبری.

مهدی رمضانی در سال ۱۳۷۲ مدرک کارشناسی ریاضی کامپیوتر خود را از دانشگاه صنعتی امیرکبیر و در سال ۱۳۷۵ مدرک کارشناسی ارشد ریاضی کاربردی آنالیز عددی خود را از دانشگاه علم و صنعت ایران دریافت نمود. در سال ۱۳۸۵ مدرک دکتری ریاضی کاربردی کنترل بهینه خود را از دانشگاه امیرکبیر دریافت نمود و هم‌اکنون استادیار ریاضی دانشگاه تفرش می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: کنترل بهینه، کنترل تصادفی، شناسایی سیستم و آنالیز عددی.

سیدمحمد عظیمی تحصیلات خود را در مقاطع کارشناسی ارشد و دکتری برق قدرت به‌ترتیب در سال‌های ۱۳۸۵ و ۱۳۹۵ از دانشگاه تهران به پایان رسانده است و هم‌اکنون استادیار دانشکده مهندسی برق دانشگاه صنعتی همدان می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: ریزشبکه، کنترل و پایداری در ریزشبکه‌ها و سیستم‌های قدرت.