

# پایدارسازی و سنکرون سازی ریز شبکه جزیره‌ای با حضور خطا و حمله سایبری سنسوری و عملگری با طراحی کنترل کننده ثانویه

عبدالله میرزاییگی، علی کاظمی، مهدی رضانی و سیدمحمد عظیمی

$x(t)$ : حالت سیستم بدون حمله

$x^*(t)$ : میانگین پارامتر  $x(t)$

$G$ : ماتریس اتصال به اسلک<sup>۲</sup>

$L$ : ماتریس لاپلاسین

$g_i$ : بهره اتصال<sup>۳</sup>

$a_{ij}$ : درایه‌های ماتریس مجاورت<sup>۴</sup>

$P_i$ : توان اکتیو متوسط

$Q_i$ : توان راکتیو متوسط

$\tilde{p}_i$ : توان اکتیو لحظه‌ای

$\tilde{q}_i$ : توان راکتیو لحظه‌ای

$v_{oi}$ : ولتاژ خروجی  $DG_i$

$\omega_{oi}$ : فرکانس زاویه‌ای خروجی  $DG_i$

$i_{oi}$ : جریان خروجی  $DG_i$

$V_{ni}^*$ : ولتاژ خروجی کنترل کننده ثانویه

$\omega_{ni}^*$ : فرکانس خروجی کنترل کننده ثانویه

$v_{oi}^*$ : ولتاژ خروجی کنترل کننده اولیه

$\omega_{oi}^*$ : فرکانس زاویه‌ای کنترل کننده اولیه

$f$ : فرکانس

$\omega_{com}$ : فرکانس زاویه‌ای در چارچوب معمول

$i_l$ : جریان خروجی بار

$\omega_c$ : فرکانس قطع فیلتر پایین‌گذر

$v_{ref}$ : ولتاژ مرجع

$\omega_{ref}$ : فرکانس زاویه‌ای مرجع

$v_b$ : ولتاژ باس

$u_v$ : سیگنال کنترل کمکی<sup>۵</sup> ولتاژ

$u_\omega$ : سیگنال کنترل کمکی فرکانس

$C_v$ : بهره کنترلی ولتاژ

$m_{p_i}$ : ضریب دروپ فرکانس

$n_{q_i}$ : ضریب دروپ ولتاژ

$\delta$ : سیگنال عدم تطابق

$e_{v_i}$ : خطای ردیابی محلی ولتاژ

$e_{\omega_i}$ : خطای ردیابی محلی فرکانس

$\phi$ : متغیر کمکی کنترل کننده ولتاژ

چکیده: در بسیاری از روش‌های کنترلی ریز شبکه برای پایداری و سنکرون سازی ولتاژ و فرکانس از اطلاعات خروجی سنسورها و عملگرهای منابع تولید پراکنده همجوار استفاده می‌شود. بسیاری از مشکلات مانند اختلالات، عدم قطعیت، دینامیک مدل نشده، حملات سایبری، نویز، تأخیر و خطاهای اندازه‌گیری، مشکلات داده نامعتبر و خطا را در سیستم ایجاد می‌کند. کنترل بهتر ریز شبکه به کیفیت داده‌های اندازه‌گیری شده و یا ارسال شده از خروجی سنسورها و عملگرها بستگی دارد. در این مقاله با توجه به مزیت‌های روش کنترلی سلسله‌مراتبی توزیع شده اشتراکی<sup>۱</sup> از آن برای کنترل و سنکرون سازی در ریز شبکه جزیره‌ای با حضور خطای سنسوری و عملگری استفاده می‌گردد. برای سنکرون سازی منابع تولید پراکنده با سیستم‌های چندعامله و شبکه ارتباطی با تئوری گراف مدل می‌گردد. به منظور پایدارسازی و سنکرون سازی، خطای سنسوری و عملگری در مدل منابع تولید پراکنده فرمول‌بندی ریاضی می‌شود. در اثبات پایداری و سنکرون سازی تابع لیاپانوف مناسب ارائه شده و شرایط پایداری و سنکرون سازی اثبات می‌گردد. در نهایت برای نشان دادن کارایی کنترل کننده طراحی شده در حل مشکلات کانال ارتباطی و تأیید تئوری ارائه شده، یک مدل نمونه با وجود خطا و حمله سایبری سنسوری و عملگری در محیط نرم‌افزار متلب/سیمولینک شبیه‌سازی می‌شود.

کلیدواژه: ریز شبکه، خطای سنسوری و عملگری، حمله سایبری سنسوری و عملگری، سیستم‌های چندعامله، کنترل سلسله‌مراتبی توزیع شده اشتراکی، سنکرون سازی، پایداری لیاپانوف.

## 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

این مقاله در تاریخ ۱۳ آذر ماه ۱۴۰۱ دریافت و در تاریخ ۳ خرداد ماه ۱۴۰۲ بازنگری شد.

عبدالله میرزاییگی، دانشکده مهندسی برق، مؤسسه آموزش عالی جهاد دانشگاهی همدان، همدان، ایران، (email: mirzabeigi@acecr.ac.ir).

علی کاظمی (نویسنده مسئول)، دانشکده مهندسی برق، دانشگاه تفرش، تفرش، ایران، (email: kazemy@tafreshhu.ac.ir).

مهدی رضانی، 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).

2. Slack Bus

3. Pinning Gain

4. Adjacency Matrix

5. Auxiliary Control

6. The Local Neighborhood Tracking Error

1. The Cooperative Distributed Hierarchical Control

مرجع برابر باشند و یا به عبارتی سنکرون سازی انجام پذیرد [۲] تا [۴]. استفاده از لینک‌های مخابراتی به منظور کنترل بهتر در کنترل کننده توزیع شده سلسه‌مراتبی، مسأله‌ای بسیار ضروری است. هنگامی که از لینک‌های مخابراتی استفاده می‌شود، اختلالات مختلفی سبب برهم خوردن تنظیم و سنکرون سازی فرکانس و ولتاژ DGها می‌شود. از جمله اختلالات نویز، اغتشاش، دینامیک مدل نشده، تأخیر، تداخل‌های الکترومغناطیسی، خطاهای سنسوری و عملگری، از بین رفتن اطلاعات، حملات سایبری و اختلال در دسترسی است. کنترل و سنکرون سازی ریزشبهه تا حد زیادی به کیفیت داده‌های دریافتی از سنسورها و عملگرها بستگی دارد. برای رفع این مشکلات، ساختارهای مختلف کنترلی در ریزشبهه‌ها مورد استفاده قرار می‌گیرد که اغلب نیاز به اطلاعات از واحدهای همجوار و ارسال آنها با استفاده از لینک‌های ارتباطی و مقایسه با همدیگر دارند. رفع مشکلات کانال‌های ارتباطی مسأله مهمی است که در استفاده از کنترل کننده‌ها باید مورد توجه قرار گیرد تا با انتقال داده‌های باکیفیت بتوان پایدارسازی و سنکرون سازی بهتری انجام داد.

برای کنترل منابع تولید پراکنده، سه روش کنترلی وجود دارد: (۱) کنترل متمرکز<sup>۶</sup>، (۲) کنترل غیرمتمرکز<sup>۷</sup> و (۳) کنترل توزیع شده<sup>۸</sup> [۱]. کنترل کننده کنترلی متمرکز از یک کنترل کننده مرکزی استفاده می‌کند و اطلاعات همه منابع به این کنترل کننده، ارسال و کنترل به صورت یکپارچه انجام می‌شود و به شبکه ارتباطی نیاز دارد. در کنترل کننده غیرمتمرکز برای هر منبع، کنترل کننده جداگانه طراحی شده و نیازی به شبکه ارتباطی ندارد. در کنترل کننده توزیع شده برای هر واحد، کنترل کننده مجزا طراحی شده و از اطلاعات واحدهای همجوار نیز استفاده می‌کند و برای انتقال اطلاعات به سیستم‌های ارتباطی نیاز است [۵].

یکی از اساسی‌ترین مسائل در کنترل و سنکرون سازی بهتر منابع تولید پراکنده، کیفیت داده‌های دریافتی از سنسورهاست. برای سنکرون سازی و کنترل بهتر، روش‌هایی که از خروجی منابع همجوار استفاده می‌کنند، نتایج بهتری می‌دهند. در این حالت کیفیت داده به دقت اندازه‌گیری سنسورها و همچنین حل مشکلات کانال‌های ارتباطی بستگی دارد. مشکلات کانال ارتباطی در مراجع مختلفی آمده است. در [۶] حمله سایبری به سنسورها و عملگرها بر روی سیستم‌های چندعامله<sup>۹</sup> بحث گردیده است؛ اما از مدل خطی یک سیستم چندعامله استفاده شده و فقط مبحث پایداری مورد مطالعه قرار گرفته و به سنکرون سازی سیستم توجهی نشده است. در [۷] تا [۹] اثر حمله DoS و نحوه شناسایی آن در سیستم NCS<sup>۱۰</sup> بررسی و ارزیابی گردیده و مبحث پایداری و سنکرون سازی بحث نشده است. در [۱۰] شناسایی حمله سایبری تزریق اطلاعات غلط در سنسور بررسی گردیده و سنکرون سازی بحث نشده است. در [۱۱] حمله سایبری DoS به صورت تأخیر در یک ریزشبهه در نظر گرفته شده و فقط اثر فرکانس تحلیل گردیده و ولتاژ بررسی نشده است. در [۶] و [۱۲] مشکلات سنسورها و عملگرها روی سیستم‌های چندعامله بحث گردیده و برای چند عامل خطی، سیستم چندعامله به سمت سنکرون سازی رفته است. در [۱۰] اثر از بین رفتن دیتا در ریزشبهه بررسی گردیده و بر روی سیستم گسسته، ریزشبهه کنترل مقاوم طراحی شده است. در [۱۳] به گم شدن

$\gamma$ : متغیر کمکی کنترل کننده جریان  
 $\nu$ : گره<sup>۱</sup> در تئوری گراف  
 $L_{line}$ : اندوکتانس خطوط بین DGها  
 $R_{line}$ : مقاومت خطوط بین DGها  
 $\sigma$ : مقدار تکین  
 $x^c$ : پارامتر  $x$  مختل شده با حمله  
 $C_V$ : بهره کنترلی ولتاژ  
 $C_P$ : بهره کنترلی توان اکتیو  
 $C_\omega$ : بهره کنترلی فرکانس زاویه‌ای  
 $y$ : اطلاعات اندازه‌گیری شده سنسور  
 $\bar{y}$ : اطلاعات دریافت شده همان لحظه از سنسور  
 $y^a$ : اطلاعات غلط تزریق شده توسط حمله کننده  
 $x_i^{as}$ : حالت مختل شده با حمله عملگری و سنسوری  
 $u_i^{ac}$ : سیگنال کنترلی با حمله عملگری و سنسوری  
 $x_i^s$ : حالت مختل شده ناشی از خطای عملگری و سنسوری  
 $u_i^c$ : سیگنال کنترلی با خطای عملگری و سنسوری  
 $\delta_i^s$ : سیگنال خطای تزریق شده سنسوری  
 $\delta_i^a$ : سیگنال خطای تزریق شده عملگری  
 $e_i^s$ : خطا با در نظر گرفتن خطای سنسوری  
 $u_i^s$ : ورودی کنترلی با در نظر گرفتن خطای سنسوری  
 $x_i^{as}$ : حالت مختل شده سیگنال حمله عملگر و سنسوری  
 $u_i^{ac}$ : سیگنال کنترلی با حمله عملگری و سنسوری  
 $x_i^a$ : سیگنال حمله سنسوری  
 $u_i^a$ : سیگنال حمله عملگری  
 $LPF$ : فیلتر پایین گذر

## ۱- مقدمه

وجود شبکه‌های گسترده انتقال انرژی الکتریکی از نقاط دوردست به مراکز مصرف، یکی از شاخصه‌های شبکه‌های برق جهان است. این چیدمان شبکه، مشکلات و مصائب فراوانی مانند تلفات انرژی الکتریکی در مسیرهای طولانی و همچنین تهدید پایداری شبکه را سبب می‌شود. مزایای منابع انرژی تجدیدپذیر سبب افزایش استفاده آنها در صنعت برق و گسترش روزافزون ریزشبهه‌ها شده است.

ریزشبهه‌ها شامل مجموعه‌ای از منابع تولید پراکنده<sup>۲</sup> (DG) نظیر توربین بادی، دیزل ژنراتور، پیل سوختی و سیستم فتوولتائیک، سیستم ذخیره انرژی و بارها بوده که قابلیت کنترل داشته و تأمین کننده توان الکتریکی هستند. موارد مهمی که در منابع تولید پراکنده باید کنترل شوند فرکانس و ولتاژ، توان اکتیو و راکتیو DGها، سنکرون سازی ریزشبهه با شبکه اصلی<sup>۳</sup>، مدیریت انرژی و بهینه‌سازی اقتصادی است [۱].

یک ریزشبهه در دو حالت وصل به شبکه<sup>۴</sup> و حالت جزیره‌ای<sup>۵</sup> مورد بهره‌برداری قرار می‌گیرد. کنترل در حالت وصل به شبکه، اغلب از طریق شبکه اصلی انجام می‌گردد و در حالت جزیره‌ای باید به نحوی انجام پذیرد که همه DGها دارای فرکانس و ولتاژ یکسانی باشند که اغلب باید با

6. Centralized Control
7. Decentralized Control
8. Distributed Control
9. Multi Agent Systems
10. Network Control System

1. Node
2. Distributed Generator
3. Main Grid
4. Grid Connected Mode
5. Islanded Mode

همچنین در این مقاله، کارآمدی کنترل‌کننده طراحی‌شده در مشکلات مختلف سنسوری و عملگری بررسی گردیده است. در این راستا اثرات ناشی از حمله سایبری سنسوری و عملگری و خطای سنسوری و عملگری با هم مقایسه شده و اثر تأخیر به‌عنوان یکی از مشکلات اصلی کانال‌های ارتباطی نیز تحلیل گردیده است. نوآوری‌های این مقاله به اختصار به شرح زیر هستند:

۱) پایدارسازی و سنکرون‌سازی همزمان سیستم ریزشبه‌خطا با حضور خطای سنسوری و عملگری با تعریف یک تابع لیاپانوف جدید و به‌دست‌آوردن شرایط پایدارسازی و سنکرون‌سازی. در اکثر تحقیقات پیشین ولتاژ، فرکانس و یا توان اکتیو کنترل شده است. در این پژوهش با طراحی کنترل‌کننده مناسب، کنترل همزمان ولتاژ، فرکانس و توان اکتیو انجام شده است. به‌عنوان نوآوری در این پژوهش، تابع لیاپانوف جدید ارائه گردیده و با انتخاب ضرایب مناسب، پایداری سیستم تضمین شده است.

۲) مدل‌سازی و فرمول‌بندی خطای سنسوری و عملگری در مدل منابع تولید پراکنده و حصول همه قوانین رینولد در ریزشبه‌خطا. در این نوآوری با استفاده از ماهیت خطاهای سنسوری و عملگری، فرمول‌بندی در معادلات ریزشبه‌خطا با دیدگاه سیستم‌های چندعامله انجام شده است. همه قوانین رینولد در سیستم‌های چندعامله در ریزشبه‌خطا نیز در نظر گرفته شده‌اند.

۳) طراحی و شبیه‌سازی کنترل‌کننده ثانویه در DGها با در نظر گرفتن مدل کامل ریزشبه‌خطا به‌صورت سیستم چندعامله و با حضور خطای سنسوری و عملگری.

۴) بررسی و تحلیل شرایط سنکرون‌سازی و مشخص کردن انعطاف و مقاومت همه DGها با استفاده از قضایای جدید. علاوه بر بررسی پایداری سیستم، در این پژوهش قضیه‌های مرتبط با سنکرون‌سازی آمده و با ارائه شرایط سنکرون‌سازی، کنترل‌کننده مناسب ارائه شده است. طراحی کنترل‌کننده به‌نحوی است که می‌تواند در شرایط مناسب با وجود حملات سایبری مختلف و خطاهای سنکرون‌سازی را انجام دهد.

۵) مقایسه اثر خطای سنسوری و عملگری با حمله سایبری سنسوری و عملگری در کنترل‌کننده ثانویه سلسله‌مراتبی<sup>۳</sup>. خطا و حمله، دو اختلال متفاوت هستند که در تحقیقات قبلی، برخورد یکسانی با آنها شده است. در این پژوهش برای نوآوری، تفاوت‌های آنها بررسی گردیده و تاب‌آوری اثر آنها در ریزشبه‌خطا نشان داده شده است. اثر خطا به‌طور دقیق در سنسور و اثر حمله در لینک ارتباطی، تحلیل و تأثیر آنها در ریزشبه‌خطا با هم مقایسه شده است.

۶) در نظر گرفتن تأخیر کانال ارتباطی در کنترل‌کننده سلسله‌مراتبی توزیع‌شده اشتراکی. با در نظر گرفتن ریزشبه‌خطا به‌صورت سیستم‌های چندعامله در انتقال اطلاعات تأخیر ایجاد می‌گردد. در این پژوهش تأخیر در این کانال تحلیل گردیده است.

در بخش دوم، مدل دینامیکی منابع تولید پراکنده و در بخش سوم، مدل سیستم ارتباطی و تئوری گراف بحث می‌گردد. در بخش چهارم، طراحی کنترلی سلسله‌مراتبی توزیع‌شده اشتراکی مورد مطالعه قرار می‌گیرد. در بخش پنجم، خطای سنسوری و عملگری و مقایسه آن با حمله سنسوری و عملگری و بررسی اثر آنها در منابع تولید پراکنده و در بخش ششم تحلیل پایداری سیستم ارائه شده است. در بخش هفتم شبیه‌سازی و نهایتاً

داده بین ریزشبه‌خطا و شبکه اصلی پرداخته شده است؛ اما مدل ریزشبه‌خطا به‌صورت خطی در نظر گرفته شده و از جزئیات مدل ریزشبه‌خطا صرف نظر گردیده است. همچنین در [۱۴] به جبران خطای ناشی از حمله سایبری سنسوری با استفاده از کنترل مقاوم پرداخته شده است. در [۱۵] عدم قطعیت‌های سیستم ارتباطی مورد مطالعه قرار گرفته است. اثر تأخیر زمانی در کانال‌های ارتباطی در [۱۶]، تغییرپذیری شبکه‌ای در [۱۷] و نویز اندازه‌گیری در [۱۸] بررسی شده و عملکرد و پایداری کنترل ثانویه توزیع‌شده مورد ارزیابی قرار گرفته است. مراجع [۱۹] و [۲۰] اثر خطای سنسوری در سیستم‌های چندعامله را بررسی کرده‌اند. حملات سایبری سنسوری و خطای سنسوری بر روی DGها در مراجع مختلفی بحث شده است [۱۰] و [۲۱] تا [۲۳]. در [۲۴] حمله سایبری در ریزشبه‌خطا بحث گردیده و حمله سنسوری و عملگری مورد مطالعه قرار گرفته است؛ ولی حمله به‌صورت یک اغتشاش وارد معادلات گردیده است؛ در صورتی که حمله سایبری باید به‌صورت هوشمند در معادلات وارد شود.

در [۱۴]، جبران خطای ناشی از حمله حسگر با استفاده از کنترل مقاوم مورد بحث قرار گرفته و در حملات سایبری از سنسور و خروجی محرک استفاده شده است. در [۴] روش جدیدی برای از بین بردن اثرات حمله ربودن اطلاعات<sup>۱</sup> ارائه شده است. در [۲۵]، اثر حملات تزریق اطلاعات نادرست ناشناخته در ریزشبه‌خطا DC با طراحی یک مشاهده‌گر حالت توسعه‌یافته توزیع‌شده با کنترل ولتاژ و جریان حذف شده است. در [۲۶] اثر حمله‌های سنسوری، ربودن اطلاعات و DoS بر روی کنترل‌کننده ثانویه نشان داده شده است؛ اما پایداری و سنکرون‌سازی آن بحث و تحلیل نشده است. تفاوت مقاله ارائه‌شده با [۲۷] آن است که در اینجا از مقدار مرجع برای سنکرون‌سازی استفاده شده است؛ ولی در [۲۷] برای از بین بردن اثر حمله از میانگین ولتاژ و فرکانس استفاده گردیده است. استفاده از میانگین، علی‌رغم اینکه اثر حمله را از بین می‌برد ممکن است باعث شود که خروجی‌ها از مقدار مرجع فاصله بگیرند و به سمت مقدار میانگین بازبایی شوند. در هیچ کدام از منابع ارائه‌شده، بحث همزمان سنکرون‌سازی و پایداری در منابع تولید پراکنده مطرح نشده است. در این مقاله با دیدگاه سیستم‌های چندعامله، سنکرون‌سازی و پایداری و شرایط محقق شدن آنها بررسی شده است. یکی از اصلی‌ترین اهداف در تحقیقات خطاهای سنسوری و عملگری آن است که کنترل‌کننده به‌نحوی طراحی شود که رنج وسیع‌تری از خطاها را تحمل کند و بتواند مقاومت سیستم در برابر اختلالات کانال ارتباطی را حفظ کند. راهکار ارائه‌شده در این مقاله آن است که با استفاده از دیدگاه سیستم‌های چندعامله، مشکلات ناشی از سنسور و عملگر برطرف گردد و همچنین شرایط همزمان پایدارسازی و سنکرون‌سازی به‌دست آمده است.

در این مقاله، ابتدا معادلات خطای سنسوری و عملگری در ریزشبه‌خطا، فرمول‌بندی ریاضی گردیده است. با طراحی کنترل‌کننده سلسله‌مراتبی توزیع‌شده اشتراکی، سیستم پایدار شده و سنکرون‌سازی با دیدگاه سیستم‌های چندعامله و در نظر گرفتن قوانین رینولد<sup>۲</sup> انجام گردیده است. با معرفی تابع لیاپانوف مناسب، اثر خطا در پایداری ریزشبه‌خطا ارزیابی گردیده و شرایط سنکرون‌سازی و پایدارسازی به‌دست آمده است. برای به‌دست‌آوردن شرایط سنکرون‌سازی، قضیه مناسب ارائه گردیده و نشان داده شده که با حضور خطا در سنسورها و عملگرها، خروجی‌های منابع تولید پراکنده با هم و با مقدار مرجع برابر شده است.

1. Hijacking Attack

2. Reynold

در بخش هشتم نتیجه‌گیری ارائه گردیده است.

## ۲- مدل دینامیکی منابع تولید پراکنده (DGs)

مدل استفاده‌شده در این مقاله به صورت (۱) در نظر گرفته شده که غیرخطی است و کاملاً همه جزئیات منابع تولید پراکنده را در بر می‌گیرد. در این مدل‌سازی، قسمت‌های مختلف شامل توزیع‌شده، قسمت‌های اندازه‌گیری، شبکه اصلی، قسمت‌های کنترلی و لینک‌های ارتباطی، بلوک‌های کنترل‌کننده توان، کنترل‌کننده ولتاژ و جریان، فیلتر LC و بار خروجی در نظر گرفته شده است [۲] و [۲۸] تا [۳۲]

$$\begin{cases} \dot{x}_i = f_i(x_i) + k_i(x_i)D_i + g_i(x_i)u_i \\ y_i = h_i(x_i) \\ x_i = [\delta_i \ P_i \ Q_i \ \phi_{di} \ \phi_{qi} \ \gamma_{di} \ \gamma_{qi} \ i_{di} \ i_{dq} \ v_{odi} \ v_{oqi} \ i_{odi} \ i_{oqi}] \\ D_i = [\omega_{com} \ v_{bdi} \ v_{bqi}]^T \end{cases} \quad (1)$$

که  $x_i$  و  $D_i$  حالت و اغتشاش سیستم است.  $\delta_i$  زاویه چارچوب مرجع  $DG_i$  با چارچوب مرجع معمول،  $P_i$  و  $Q_i$  توان متوسط اکتیو و راکتیو خروجی،  $\phi_{dq}$  متغیر کمکی در کنترل‌کننده ولتاژ،  $\gamma_{di}$  متغیر کمکی در کنترل‌کننده جریان،  $i_{odq}$ ،  $i_{dq}$  و  $v_{odq}$  به ترتیب مقادیر جریان و ولتاژ خروجی و جریان بار و  $u_i = (V_{ni}^* \ \omega_{ni}^*)^T$  و  $y_i = (v_{odi} \ \omega_{odi})^T$  مقادیر ورودی کنترلی و خروجی هستند. جزئیات مقادیر (۱) در [۲۸] آمده است. در این مدل‌سازی، قسمت‌های مختلف شامل منابع توزیع‌شده، قسمت‌های اندازه‌گیری، شبکه اصلی، قسمت‌های کنترلی و لینک‌های ارتباطی، 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 [۲] و [۲۸] تا [۳۲].

## ۳- مدل کانال ارتباطی و تئوری گراف

برای تعیین مسیر تبادل داده‌ها (ولتاژ، فرکانس، توان اکتیو و راکتیو) بین DGها از سیستم مخابراتی استفاده شده است. برای تحلیل لینک‌های مخابراتی، تحلیل پایداری و سنکرون‌سازی در این مقاله از تئوری گراف<sup>۱</sup> و با دیدگاه سیستم‌های چندعامله استفاده گردیده است. در سیستم‌های چندعامله، کنترل یک عامل به خروجی‌های عامل همجوار نیز بستگی دارد. در این مدل، منابع تولید پراکنده به صورت عامل و لینک‌های مخابراتی بین آنها با ماتریس همجوار مدل می‌شوند.

برای سنکرون‌سازی سیستم‌های چندعامله، سه قانون اصلی به نام قوانین رینولد وجود دارد:

- (۱) اجتناب از برخورد با همسایگان
- (۲) تطبیق حرکت با بقیه گروه
- (۳) باقی‌ماندن در اطراف یک مرکز

برای کنترل و سنکرون‌سازی منابع، همه این قوانین باید پیاده‌سازی گردد. مزایای اصلی سیستم‌های چندعامله، افزایش عملکرد سیستم، افزایش قابلیت تطابق، پایداری و انعطاف بیشتر، افزایش مقاوم‌بودن سیستم، مقابله با خطا و هزینه کمتر است [۳۳] و [۳۴].

خطاهای ناشی از دریافت صحیح داده‌های خروجی در سیستم‌های چندعامله به سه دسته تقسیم می‌شوند:

- (۱) خطا در عملگرها (عملگر کارایی‌اش را از دست داده است)
- (۲) خطا در سنسورها (سنسور اطلاعات را درست اندازه‌گیری نمی‌کند)

(۳) خطا در ارتباطات (اطلاعات از همسایه‌ها گرفته نمی‌شود)  
توجه: اساسی‌ترین تفاوت خطای سنسوری و حمله سایبری سنسوری در آن است که خطا به دلیل مشکلات سنسوری و حمله سایبری سنسوری به دلیل مشکلات کانال ارتباطی است. بنابراین خطای سنسوری از نوع دوم و حمله سایبری سنسوری از نوع سوم خطای تعریف‌شده در نقص در خروجی‌هاست؛ هرچند هر دو در سیستم تأثیرات تقریباً یکسانی دارند و نهایتاً باعث اختلال در مقدار خروجی می‌گردند.

### تعاریف

**گراف پیوسته:** در بین دو گره آن حداقل یک مسیر وجود دارد.  
**گره رهبر:**<sup>۲</sup> گرهی که از گره دیگری مقدار نمی‌گیرد و مقدار مرجع همه عامل‌ها را مشخص می‌کند.

**درخت ریشه‌دار:** یک گراف پیوسته با گره رهبر که هیچ حلقه‌ای ندارد. به‌منظور تحلیل سیستم ارتباطی از تئوری گراف استفاده می‌گردد و شبکه ارتباطی به صورت (۲) نشان داده شده است

$$G = (V(G), E(G)) \quad (2)$$

$V(G) = \{v_1, v_2, \dots, v_N\}$  به ترتیب گره‌ها (منابع تولید پراکنده)، لینک‌های ارتباطی و ماتریس مجاورتی هستند. درایه‌های ماتریس مجاورتی  $a_{ij}$  وزن اضلاع گراف است که اگر گراف  $i$ ام به گراف  $j$ ام اطلاعات دهد یک و در غیر این صورت صفر است [۳۵]. ماتریس  $\Delta$  و لاپلاسیان  $L$  به صورت زیر تعریف می‌شود

$$\begin{aligned} D &= \text{diag}(\Delta_i) \\ \Delta_i &= \sum_{v_j=N_i} a_{ij} \\ L &= D - A \end{aligned} \quad (3)$$

$\Delta_i$  تعداد اضلاعی است که به گره  $i$ ام وارد می‌شود (درجه داخلی)<sup>۳</sup> [۶]. در این مقاله گراف به صورت متعادل (همه وزن ضلع‌ها برابر و مقدار آنها یک و صفر)، توپولوژی ثابت و درخت پیوسته ریشه‌دار<sup>۴</sup> فرض شده است.

**توجه:** در سیستم‌های چندعامله دو نکته بسیار مهم است: پایداری و سنکرون‌سازی. سنکرون‌سازی سیستم‌های چندعامله به این معنی است که همه عامل‌ها طبق قانون دوم رینولد در حالت ماندگار با هم هماهنگ باشند. این اصل با (۴) نشان داده شده است

$$\lim_{t \rightarrow \infty} \|x_i(t) - x_j(t)\| = 0, \quad i, j = 1, 2, 3, \dots, N \quad (4)$$

با توجه به قانون سوم رینولد، سنکرون‌سازی مشخص‌کردن مرکز در سیستم‌های چندعامله به دو روش انجام می‌گردد: (۱) با در نظر گرفتن مرکز به صورت میانگین همه خروجی‌ها که در (۵) آمده و (۲) به صورت توافقی<sup>۵</sup> و در نظر گرفتن مرجع که در (۶) نشان داده شده است

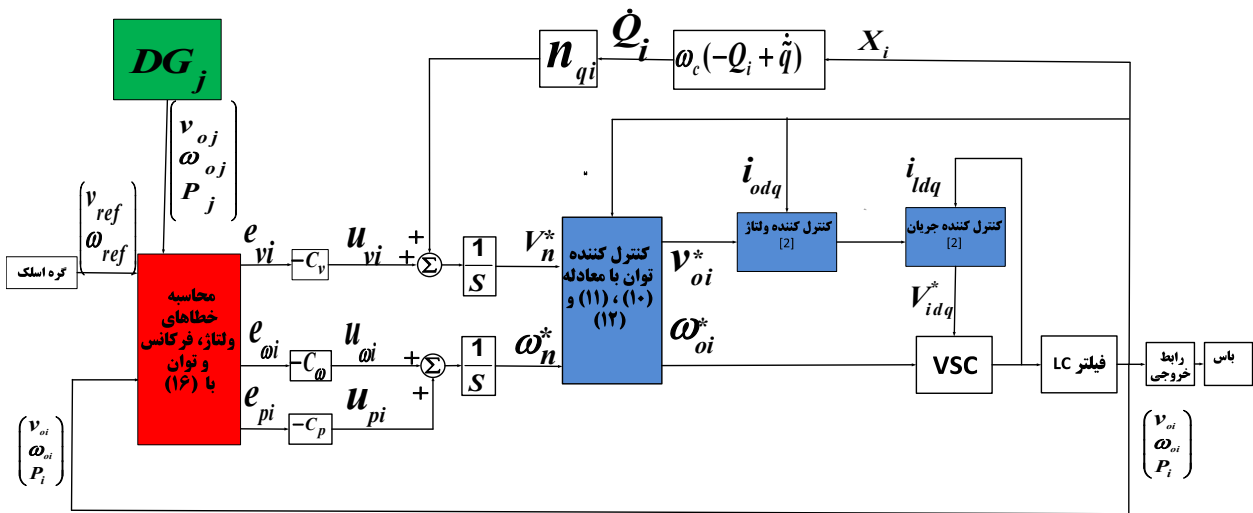
$$\lim_{t \rightarrow \infty} \|x_i(t) - x^*(t)\| = 0, \quad i, j = 1, 2, 3, \dots, N \quad (5)$$

$$\lim_{t \rightarrow \infty} \|x_i(t) - x_{ref}(t)\| = 0, \quad i = 1, 2, 3, \dots, N \quad (6)$$

که در (۵)،  $x^*(t) = \frac{1}{N} \sum_{i=1}^N x_i(t)$  میانگین خروجی‌های سیستم است

[۳۵] و [۳۶]. از جنبه دیگری سنکرون‌سازی را به صورت محلی و کلی نیز در نظر می‌گیرند. سنکرون‌سازی محلی به صورت (۷) تعریف می‌شود که

2. Leader
3. In-Degree
4. Spinning Tree
5. Consensus



شکل ۱: ساختار کلی DG به همراه کنترل کننده اولیه و ثانویه.

اولیه به عنوان یک کنترل کننده محلی ایجاد گردد [۲]، [۲۹] و [۳۸].

به شرایط اولیه حالات بستگی دارد

### ۴-۱ کنترل کننده اولیه

$$\forall \varepsilon > 0 \exists \delta, T > 0 \rightarrow \|x_i(\cdot) - x_j(\cdot)\| < \delta \rightarrow \quad (7)$$

$$\|x_i(t) - x_j(t)\| < \varepsilon \text{ for } t > T, i, j = 1, 2, \dots, N$$

در سنکرون سازی کلی برای همه شرایط اولیه ها می توان نوشت

$$\forall \varepsilon > 0 \exists T > 0 \rightarrow \|x_i(t) - x_j(t)\| < \varepsilon \quad (8)$$

$$\text{for } t > T, i, j = 1, 2, \dots, N$$

در سیستم های چندعامله کنترل کننده باید به نحوی طراحی شود که شرط پرهیز از برخورد و پیروی از رهبر تحقق یابد. به این منظور سیگنال کنترلی به صورت (۹) تعریف می گردد

$$u = \sum a_{ij}(x_i - x_j) + g_i(x_i - x_{ref}) \quad (9)$$

که  $g_i$  بهره اتصال است [۳۵]. در این مقاله طراحی کنترل کننده به نحوی است که همه شرایط رینولد تحقق یابد و خروجی ها به صورت کلی سنکرون باشند.

### ۴-۲ طراحی کنترلی سلسله مراتبی توزیع شده اشتراکی

در این مقاله از کنترل کننده توزیع شده به صورت سلسله مراتبی در چند لایه استفاده شده است. در روش سلسله مراتبی، کل ساختار کنترلی به سه سطح اولیه<sup>۱</sup>، ثانویه<sup>۲</sup> و ثالثیه<sup>۳</sup> تقسیم می شود. هر لایه مرجع، لایه بالاتر را تنظیم می کند و بنابراین باعث می شود که در لایه پایین تر خطا کمتر گردد [۳] و [۳۷].

در این مقاله از کنترل کننده اولیه و ثانویه استفاده شده و شکل ۱ منابع تولید پراکنده و این کنترل کننده ها را نشان می دهد. کنترل کننده اولیه شامل کنترل کننده توان، ولتاژ و جریان و کنترل کننده ثانویه برای حذف انحراف کنترل کننده اولیه است که در آن می توان از کنترل کننده های مختلفی استفاده کرد. در این مقاله با دیدگاه سیستم های چندعامله در کنترل کننده ثانویه از روش خطی سازی فیدبک استفاده شده است. با توجه به شکل ۱،  $V_{ni}^*$  و  $\omega_{ni}^*$  باید توسط کنترل کننده ثانویه و به عنوان ورودی کنترل کننده اولیه ایجاد شوند تا انحراف کمتری در ورودی کنترل کننده

کنترل کننده های جریان، ولتاژ و توان به صورت اولیه در نظر گرفته می شوند. خروجی کنترل کننده ثانویه  $(V_{ni}^* \omega_{ni}^*)^T$  و خروجی  $DG_i$   $(V_{oi}^* \omega_{oi}^*)^T$  به عنوان ورودی کنترل کننده اولیه است. در کنترل کننده توان، ابتدا با استفاده از خروجی های منابع تولید پراکنده، توان لحظه ای از (۱۰) به دست می آید و با عبور این توان از یک فیلتر پایین گذر با (۱۱)، توان متوسط به صورت  $(P \ Q)^T$  حاصل می شود

$$\begin{cases} \tilde{P}_i = v_{odi} i_{odi} + v_{oqi} i_{oqi} \\ \tilde{Q}_i = v_{oqi} i_{odi} - v_{odi} i_{oqi} \end{cases} \quad (10)$$

$$P_i = \frac{s}{s + \omega_c} \tilde{P}_i \quad (11)$$

$$Q_i = \frac{s}{s + \omega_c} \tilde{Q}_i$$

با صرف نظر از دینامیک های سریع سیستم و با در نظر گرفتن مدل سیستم در چارچوب dq، کنترل کننده توان در کنترل کننده اولیه به صورت (۱۲) در نظر گرفته می شود [۲] و [۳۷]

$$\begin{cases} v_{oi}^* = V_{ni}^* - n_{qi} Q_i \\ \omega_{oi}^* = \omega_{ni}^* - m_{pi} P_i \end{cases} \quad (12)$$

معادله ولتاژ در چارچوب dq به صورت زیر در می آید

$$\begin{cases} v_{odi}^* = V_{ni}^* - n_{qi} Q_i \\ v_{oqi}^* = 0 \end{cases} \quad (13)$$

سپس با توجه به (۱۲)، خروجی کنترل کننده توان به دست می آید و خروجی  $v_o^*$  به کنترل کننده ولتاژ و  $\omega_o^*$  به VSC داده می شود. در این معادله  $n_{qi}$  و  $m_{pi}$  ضرایب دروپ و  $V_{ni}^*$  و  $\omega_{ni}^*$  مقادیر مرجع کنترل کننده اولیه هستند. در کنترل کننده ولتاژ و جریان از کنترل کننده PI استفاده شده است. کنترل کننده ولتاژ، مرجع جریان ها را مشخص می نماید و خروجی آن به عنوان ورودی های مرجع وارد کنترل کننده جریان می شوند.

1. Primary Control
2. Secondary Control
3. Tertiary Control

## ۴-۲ کنترل کننده ثانویه

شکل ۱ طرح کلی کنترل کننده ثانویه را نیز نشان می‌دهد. در این مقاله، کنترل کننده ثانویه با استفاده از روش خطی سازی فیدبک طراحی شده است. هدف اصلی در طراحی کنترل کننده، اعمال ورودی کنترلی مناسب است.  $(V_{ni}^* \ \omega_{ni}^*)^T$  به کنترل کننده اولیه به منظور پایداری و سنکرون سازی سیستم است. با استفاده از روش خطی سازی فیدبک از (۱۲) و (۱۳) 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 (۱۴) درمی‌آید [۳۷]

$$\begin{cases} \dot{v}_{odi}^* = \dot{V}_{ni}^* - n_{qi} \dot{Q}_i = u_{vi} \\ \dot{\omega}_{oi}^* = \dot{\omega}_{ni}^* - m_{pi} \dot{P}_i = u_{oi} \end{cases} \quad (14)$$

که  $u_{oi}$  و  $u_{vi}$  به ترتیب سیگنال کنترلی کمکی ولتاژ و جریان در روش خطی سازی فیدبک سیستم‌های چندعامله هستند. به منظور پایداری سازی سیستم و با توجه به اینکه سیستم به صورت چندعامله در نظر گرفته می‌شود، ورودی کنترلی به صورت (۱۵) با استفاده از خطاهای دنبال سازی است [۳۵]

$$\begin{cases} u_{vi} = -C_v e_{vi}(t) \\ u_{oi}(t) = -C_\omega e_{oi}(t) \\ u_{pi} = m_{pi} \dot{P}_i = -C_p e_{pi}(t) \end{cases} \quad (15)$$

در این رابطه  $e_{vi}(t)$ ،  $e_{oi}(t)$  و  $e_{pi}(t)$  به ترتیب خطای دنبال سازی و  $C_v$ ،  $C_\omega$  و  $C_p$  بهره کنترلی ولتاژ، فرکانس و توان اکتیو هستند. خطاهای دنبال سازی به صورت (۱۶) در سیستم‌های چندعامله می‌باشند که در سنکرون سازی، هدف آن است که این خطاها صفر شوند. این خطاها با استفاده از خروجی DG و همسایه به دست می‌آیند

$$\begin{cases} e_{vi} = \sum a_{ij} (v_{i,j}(t) - v_{j,i}(t)) + g_i (v_{i,i}(t) - v_{ref}) \\ e_{oi}(t) = \sum_{j \in N_j} a_{ij} (\omega_{oi}(t) - \omega_{oj}(t)) + g_i (\omega_{oi}(t) - \omega_{ref}) \\ e_{pi} = \sum a_{ij} (m_{pi} P_i - m_{pj} P_j) \end{cases} \quad (16)$$

که در (۱۶)،  $v_{i,j}(t)$  و  $v_{j,i}(t)$  و  $P_i$  و  $\omega_{oi}(t)$ ،  $v_{i,i}(t)$ ،  $\omega_{oj}(t)$  و  $P_j$  ولتاژ، فرکانس و توان متوسط خروجی  $DG_i$  و  $DG_j$  هستند.  $\omega_{ref}$  و  $v_{ref}$  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 (۱۲) تا (۱۶) سیگنال کنترلی از روش خطی سازی فیدبک به صورت (۱۷) به دست می‌آید

$$\begin{cases} V_{ni}^* = \int (u_{vi} + n_{qi} \dot{Q}_i) dt \\ \omega_{ni}^* = \int (u_{oi} + u_{pi}) dt \end{cases} \quad (17)$$

در (۱۷) مقدار  $\dot{Q}_i$  به صورت زیر تعریف شده است

$$\dot{Q}_i = -\omega_c Q_i + \omega_c (v_{oqi} i_{odi} - v_{odi} i_{oqi}) = -\omega_c Q_i + \omega_c \dot{q} \quad (18)$$

$\dot{Q}_i$  مربوط به اطلاعات داخلی DG است و بنابراین تحت تأثیر اختلالات خارجی قرار نمی‌گیرد.  $\dot{q}$  توان راکتیو لحظه‌ای،  $\omega_c$  فرکانس قطع فیلتر پایین‌گذر و  $v_o$  و  $i_o$  ولتاژ و جریان خروجی  $DG_i$  است [۲۸] و [۳۷].

خطای عدم تطابق به صورت (۱۹) تعریف می‌شود که اگر صفر شود سنکرون سازی انجام می‌گردد

$$e_{vi} = (L + G)(v_{odi} - v_{ref}) \quad (19)$$

به این ترتیب برای کنترل و سنکرون سازی سیستم و با توجه به (۱۲) تا (۱۹) باید در این حالت، فرکانس، ولتاژ و توان اکتیو متوسط DG همجوار را داشته باشیم.

## ۵- خطای سنسوری و عملگری و مقایسه آن با حمله سایبری سنسوری و عملگری در DGها

در کنترل، خطا<sup>۱</sup> در نتیجه هر نوع آسیب نرم افزاری و سخت افزاری به محرک و سنسور تعریف می‌شود. نقص در سنسورهای ریزشبهه، اثرات مخربی بر عملکرد آنها دارد و ممکن است اطلاعات از بین رفته و بازایی ولتاژ و فرکانس اتفاق نیفتد. در تئوری کنترل، خطا و حمله سایبری یکسان نیستند؛ هرچند نهایتاً اتفاق یکسانی می‌افتد و خروجی سنسور تحت تأثیر قرار می‌گیرد (هم در حمله و هم در خطا). در [۲۴] و [۳۹] به اختصار این تفاوت‌ها شرح داده شده است. تفاوت‌های اصلی این دو به شرح زیر است:

۱) در DGها حمله سنسوری در لینک‌های مخابراتی بین سنسورهای کنترل کننده‌های ثانویه و حمله عملگری بین کنترل کننده اولیه و ثانویه اتفاق می‌افتد؛ در حالی که خطا در سنسورها و عملگرها به معادلات اضافه می‌گردد.

۲) در حمله سایبری، اطلاعات دقیقی از خروجی نیاز است و به صورت هوشمند اتفاق می‌افتد؛ ولی در خطا مقادیر به صورت ناخواسته به خروجی اضافه می‌گردد و هوشمندی ندارد.

۳) خطا به دلیل اعوجاج عملکرد سنسور یا محرک در طول زمان است؛ در حالی که حمله ممکن است به صورت لحظه‌ای باشد یا در بازه‌ای از زمان محدود گردد.

۴) حمله از بیرون به ریزشبهه وارد می‌شود؛ ولی خطا معمولاً از داخل ایجاد می‌گردد.

۵) خطاها معمولاً ناخواسته هستند و به منظور تخریب استفاده نمی‌شوند؛ اما حملات سایبری به صورت عمدی و به منظور اختلال در کارایی سیستم اضافه می‌گردند.

اما شباهت آنها در این است که اثر هر دو در منابع تولید پراکنده یکسان است و هم در خطا و هم در حمله سنسوری و عملگری، اطلاعات ولتاژ و فرکانس یک DG به DG همجوار، اشتباه می‌رسد و ممکن است باعث ناپایداری سیستم گردد.

حملات سایبری به سه گروه کلی تقسیم می‌شوند:

- ۱) حمله منع سرویس (DoS)<sup>۲</sup>
- ۲) حمله فریب<sup>۳</sup>
- ۳) حمله تکرار<sup>۴</sup>

فرض کنید  $\gamma$  اطلاعات اندازه‌گیری شده و  $\bar{\gamma}$  اطلاعات دریافت شده همان لحظه باشد. در حمله DoS مهاجم از طریق کانال ارتباطی، انتقال اطلاعات را بلوکه می‌کند. این نوع حمله بعضی مواقع به عنوان از بین رفتن اطلاعات نیز مطرح می‌گردد و اطلاعات دریافت شده صفر می‌گردد

1. Fault
2. Denial of Service Attack
3. Deception Attack
4. Replay Attacks

$$\begin{aligned} u_{p_i}^c &= u_{p_i}^s + \delta_{p_i}^a \\ u_{oi}^c &= u_{oi}^s + \delta_{oi}^a \\ P_i^s &= P_i + \delta_{p_i}^s \\ \omega_{oi}^s &= \omega_{oi} + \delta_{\omega_{oi}}^s \end{aligned} \quad (28)$$

که  $u_{oi}^c, u_{oi}^s, \delta_{oi}^a$  به ترتیب سیگنال کنترلی فرکانس مختل شده، سیگنال کنترلی با خطای سنسوری و سیگنال خطای عملگری است و به همین ترتیب برای فرکانس و توان، سیگنال کنترلی برای حمله سنسوری به صورت زیر به دست می‌آید

$$\begin{cases} u_{oi}^c = u_{oi}^s + \delta_{oi}^a = u_{oi} + f_{i\omega} \\ u_{p_i}^c = u_{p_i}^s + \delta_{p_i}^a = u_{p_i} + f_{iP} \\ f_{i\omega} = -C_{\omega} \sum a_{ij} (\delta_{oi}^s - \delta_{oj}^s) + g_i \delta_{oi}^s + \delta_{oi}^a \\ f_{iP} = -C_P \sum a_{ij} [m_{p_i} \delta_{p_i}^a - m_{p_j} \delta_{p_j}^a] \end{cases} \quad (29)$$

نهایتاً سیگنال کنترلی فرکانس برابر است با

$$\omega_{ni}^* = \int (u_{oi}^c + u_{p_i}^c) dt = \int (u_{oi} + f_{i\omega} + u_{p_i} + f_{iP}) dt \quad (30)$$

### ۶- اثبات پایداری

در این مقاله فرض شده که مقدار خطا محدود و ناشناخته است [۴۱]، درخت گراف پیوسته می‌ماند و ارتباط بین منابع تولید پراکنده مختلف طبق ماتریس مجاورت حفظ می‌شود [۳۰] و [۳۷]. خطای سیستم به صورت (۳۱) و بردار مغایرت<sup>۱</sup> به صورت (۳۲) تعریف می‌شود

$$e_{vi} = (L + G)(v_{odi} - v_{ref}) \quad (31)$$

$$\delta = v_{od} - v_{ref} \quad (32)$$

با فرض خطای سنسوری و عملگری ولتاژ، سیگنال کنترلی با وجود خطا و بر اساس سیگنال خطا به صورت (۳۳) به دست می‌آید

$$u_v^c = -C_v e_v^c = -C_v (L + G)(v_{odi} - v_{ref}) \quad (33)$$

در فرمول بالا  $u_v^c, e_v^c$  و  $v_{odi}$  به ترتیب سیگنال کنترلی، سیگنال خطا و مقدار خروجی ولتاژ با وجود خطای سنسوری و عملگری است. برای اثبات پایداری و سنکرون سازی، لم و قضیه زیر در نظر گرفته می‌شود.

لم ۱: فرضاً گراف  $G$  یک درخت پیوسته و حداقل در یک گره ریشه  $g_i \neq 0$  باشد. با تعریف خطا به صورت  $e = (L + G)\delta$ ، (۳۴) برقرار است

$$\sigma_{\min}(L + G) \|\delta\| \leq \|e\| \Rightarrow \|\delta\| \leq \frac{\|e\|}{\sigma_{\min}}(L + G) \quad (34)$$

که  $\sigma$  مقدار تکین<sup>۲</sup> ماتریس است. در این صورت  $e$  برابر صفر است اگر و فقط اگر همه گره‌ها سنکرون باشند [۴۲]. بنابراین یکی از اصلی‌ترین شرایط برای برقراری قوانین رینولد در منابع برقرار می‌گردد.

لم ۲: فرض کنید گراف مستقیم  $G$  یک درخت پیوسته باشد و برای حداقل یکی از گره‌های ریشه  $g_i \neq 0$  باشد. ماتریس  $D + G$  را در نظر بگیرید و با توجه به اینکه  $D + G = (D + G)^T$  و  $A = L + G$  است، در این صورت  $Q = (D + G)A + A^T(D + G)$  مثبت معین است.

توجه:  $D + G$  در (۲) و (۳) تعریف شد و ماتریس مثبت معین است و به همین دلیل در معادله بالا قرار گرفته است.

( $\bar{y} \in \mathcal{E}$ ). در حمله تکرار، یک سری از اطلاعات گذشته جایگزین اطلاعات فعلی می‌گردند و از نظر مدل ریاضی  $\bar{y} \in \mathcal{E}Y$  است که  $Y$  اطلاعات گذشته است. در حمله فریب، مهاجم یک سری اطلاعات غلط را به اطلاعات ارسالی اصلی تزریق می‌کند و از نظر ریاضی به صورت لازم به ذکر است که  $\bar{y} = y + y^a$  می‌باشد که  $y^a$  اطلاعات تزریق شده توسط مهاجم است. حمله سنسوری و عملگری نیز جزء همین دسته از حمله‌ها به حساب می‌آید و البته به صورت هوشمند، مقادیر خروجی را ذخیره و در همان لحظه به سیستم تزریق می‌کند [۴۰]. حمله روی عملگرها و سنسورها به صورت رابطه زیر مدل می‌شود

$$\begin{aligned} u_i^{ac} &= u_i + \alpha_i u_i^a \\ x_i^{as} &= x_i + \beta_i x_i^a \end{aligned} \quad (20)$$

در این فرمول به ترتیب  $u_i^{ac}$  و  $x_i^{as}$  سیگنال کنترلی و حالت مختل شده ناشی از حمله سایبری عملگری و سنسوری،  $u_i$  و  $x_i$  سیگنال کنترل و حالت واقعی و  $u_i^a$  و  $x_i^a$  سیگنال حمله عملگر و سنسوری است. در این فرمول بدون حمله  $\alpha_i, \beta_i = 0$  و با حمله  $\alpha_i, \beta_i = 1$  است. خطا روی عملگرها و سنسورها به صورت (۲۱) مدل می‌شود

$$\begin{aligned} u_i^c &= u_i + \delta_i^a \\ x_i^s &= x_i + \delta_i^s \end{aligned} \quad (21)$$

که در رابطه بالا،  $u_i^c$  و  $u_i^s$  به ترتیب سیگنال کنترلی و حالت مختل شده ناشی از خطای عملگری و سنسوری،  $u_i$  و  $x_i$  سیگنال کنترل و حالت واقعی و  $\delta_i^a$  و  $\delta_i^s$  به ترتیب سیگنال خطای عملگری و سنسوری هستند.

با در نظر گرفتن خطا در عملگرها در (۲۱) و سیگنال کنترلی (۱۵) برای سیستم‌های چندعامله، سیگنال کنترلی به فرم روابط زیر بازنویسی می‌گردد

$$u_i^c = u_i^s + \delta_i^a \quad (22)$$

$$\begin{aligned} u_i^s &= -k e_i^s = -k \sum a_{ij} (x_i^s - x_j^s) + g_i (x_i^s - x_o) \\ u_i^s &= -k \sum a_{ij} (x_i + \delta_i^s - x_j - \delta_j^s) + g_i (x_i + \delta_i^s - x_o) \end{aligned} \quad (23)$$

که  $u_i^s$  و  $e_i^s$  مقدار ورودی کنترلی و خطا با در نظر گرفتن خطای سنسوری است. سیگنال کنترلی مختل شده برابر است با

$$u_i^c = u_i + \delta_i^a - k \sum a_{ij} (\delta_i^s - \delta_j^s) + g_i \delta_i^s = u_i + f_i \quad (24)$$

در منابع تولید پراکنده نیز به همین روش و با استفاده از (۲۱) تا (۲۴) کنترل کننده طراحی می‌شود.

#### الف) کنترل کننده ولتاژ

با استفاده از (۱۷) و (۲۱) سیگنال کنترلی ولتاژ به صورت زیر است

$$\begin{aligned} u_{vi}^s &= -C_v e_{vi}^s = -C_v \sum a_{ij} (v_{oi}^s - v_{oj}^s) + g_i (v_{oi}^s - v_{ref}) \\ u_{vi}^c &= u_{vi}^s + \delta_{vi}^a = -C_v \sum a_{ij} (v_{oi} - v_{oj}) + g_i (v_{oi} - v_{ref}) - \\ & C_v \sum a_{ij} (\delta_{voi}^s - \delta_{voj}^s) + g_i \delta_{voi}^s + \delta_{vi}^a = u_{vi} + f_{iv} \end{aligned} \quad (25)$$

$$V_{ni}^* = \int (u_{vi}^c + n_{Q_i} \dot{Q}_i) dt = \int (u_{vi} + f_{iv} + n_{Q_i} \dot{Q}_i) dt \quad (26)$$

#### ب) کنترل کننده فرکانس

در کنترل کننده فرکانس (۱۷) نیز معادله با خطای سنسوری به دست می‌آید

$$\omega_{ni}^* = \int (u_{oi}^c + m_p \dot{P}) dt = \int (u_{oi}^c + u_{p_i}^c) dt \quad (27)$$

با استفاده از (۲۱)

1. Disagreement  
2. Singular Value

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

$$\dot{V} = -\frac{C_v}{\gamma} e_v^T Q e_v - \frac{C_v}{\gamma} (e_v^{sa})^T Q e_v^{sa} \leq 0 \quad (40)$$

منفی معین و ریزشکبه با وجود خطای سنسوری و عملگری، پایدار مجانبی است. برای سنکرون سازی باید اثبات شود که خطای حالت ماندگار صفر است و به عبارتی  $\lim_{t \rightarrow \infty} e^c \rightarrow 0$  و سپس با توجه به لم ۱، بردار  $\delta^c$  پایدار مجانبی است و ولتاژ خروجی DGها به  $V_{ref}$  سنکرون می شوند. بنابراین

$$\begin{aligned} \dot{V}_1 &= -\frac{C_v}{\gamma} e_v^T Q e_v \\ \dot{V}_2 &= -\frac{C_v}{\gamma} (e_v^{sa})^T Q e_v^{sa} \\ \dot{V}_1 &\leq -\frac{C_v}{\gamma} \sigma_{\min}(Q) \|e_v\|^2 \leq -\frac{C_v}{\gamma} \frac{\sigma_{\min}(Q)}{\sigma_{\max}(D)} V_1 = \\ &-\gamma V_1 \rightarrow V_1 \leq e^{-\gamma t} V_1(t) \\ \lim_{t \rightarrow \infty} e^{-\gamma t} V_1(t) &\rightarrow 0 \rightarrow \lim_{t \rightarrow \infty} V_1 \rightarrow 0 \\ \dot{V}_2 &\leq -\frac{C_v}{\gamma} \sigma_{\min}(Q) \|e_v^{sa}\|^2 \leq -\frac{C_v}{\gamma} \frac{\sigma_{\min}(Q)}{\sigma_{\max}(D)} V_2 = \\ &-\gamma V_2 \rightarrow V_2 \leq e^{-\gamma t} V_2(t) \\ \lim_{t \rightarrow \infty} e^{-\gamma t} V_2(t) &\rightarrow 0 \rightarrow \lim_{t \rightarrow \infty} V_2 \rightarrow 0 \end{aligned} \quad (41)$$

و بنابراین  $\lim_{t \rightarrow \infty} V \rightarrow 0 \Rightarrow e_v^c \rightarrow 0 \Rightarrow \delta^c \rightarrow 0$  و سنکرون سازی انجام می گردد. همچنین هرچه  $C_v$  بزرگ تر باشد سرعت سنکرون سازی مناسب تر است و با انتخاب مناسب  $C_v$  و تأثیر آن در  $u_v^c$ ، سنکرون سازی بهینه ای انجام می پذیرد.

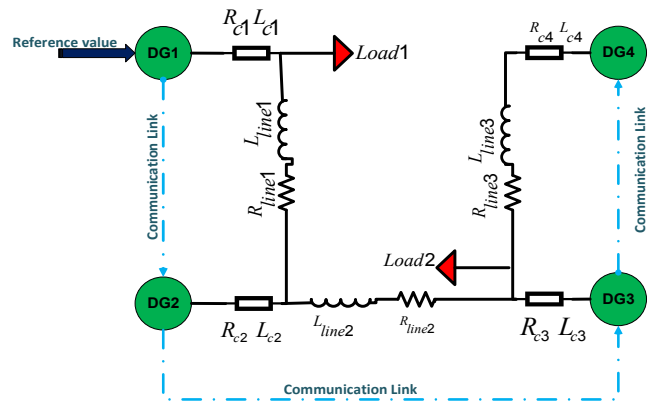
### ۷- نتایج شبیه سازی

برای شبیه سازی از یک مدل نمونه مطابق [۳۰] و [۳۷] با شکل ۲ استفاده شده و DG۱ به عنوان شین مرجع و یا اسلک در نظر گرفته می شود. شبیه سازی در محیط سیمولینک متلب است. پارامتر این DGها شامل چهار منبع توزیع شده در جدول ۱ است.  $R_{ci}$  و  $L_{ci}$  اندوکتانس و مقاومت رابط های خروجی  $DG_i$  هستند. خطوط بین DGها با یک شاخه RL سری مدل شده و  $R_{line}$  و  $L_{line}$  مقاومت و اندوکتانس آنها، بارها به صورت  $P_{load} + jQ_{load}$ ،  $K_{PC}$ ،  $K_{IC}$ ،  $K_{IV}$  و  $K_{PV}$  ضرایب PI کنترل کننده ولتاژ و جریان هستند.

در این مدل ولتاژ مرجع ۳۸۰ ولت، فرکانس ۵۰ هرتز (فرکانس زاویه ای  $\omega_{ref} = 2\pi f_{ref} = 314.159 \text{ rad/sec}$ ) و نیز ضرایب کنترل کننده ثانویه  $C_p = C_\omega = C_v = 40$  است. به منظور بررسی دقیق تر DGها و تحلیل درست آنها سناریوهای مختلف، شبیه سازی می گردد.

**سناریوی اول: عملکرد کنترل کننده اولیه و ثانویه بدون خطای سنسوری و عملگری، اغتشاش، نویز و حملات سایبری**

در ابتدا خروجی بدون وارد کردن اغتشاش و یا نامعینی ها در نظر گرفته می شود تا عملکرد کنترل کننده اولیه و ثانویه مشخص گردد. در صورت کنترل ریزشکبه فقط با کنترل کننده اولیه، خروجی ها از مقدار مرجع انحراف خواهند داشت و سنکرون سازی به درستی انجام نمی شود. شکل ۳- الف و ۳- ب خروجی ولتاژ و فرکانس را بدون کنترل کننده ثانویه و صرفاً با کنترل کننده اولیه نشان می دهند.



شکل ۲: مدل نمونه شبیه سازی شده اتصال سیستم قدرتی (خطوط ممتد) به همراه لینک های مخابراتی (خطوط نقطه چین).

**قضیه ۱:** فرض کنید که  $G$  یک درخت پیوسته و حداقل برای یکی از DGها  $g_i \neq 0$  باشد. اگر ورودی کنترلی ثانویه با خطای سنسوری و عملگری به صورت  $u_{vi}^c = -C_v e_{vi}^c$  باشد در این صورت، خطای  $e_{vi}^c = (L + G)\delta^c$  پایدار مجانبی است. همچنین ولتاژ خروجی DGها به  $V_{ref}$  سنکرون می شوند.

**اثبات:** بردار کلی  $u_v^c = [u_{v1}^c \ u_{v2}^c \ \dots \ u_{vn}^c]^T = -C_v e_v^c$  تعریف می شود که از معادلات قبلی  $u_{vi}^c = u_{vi}^s + \delta_{vi}^a$  به دست می آید. برای اثبات پایداری، تابع کاندیدای لیاپانوف به صورت (۳۵) در نظر گرفته می شود

$$\begin{aligned} V &= V_1 + V_2 \\ V_1 &= \frac{1}{\gamma} (e_v)^T (D + G) e_v \\ V_2 &= \frac{1}{\gamma} (e_v^{sa})^T (D + G) e_v^{sa} \end{aligned} \quad (35)$$

$e_v$  خطای بدون نقص سنسوری و عملگری و  $e_v^{sa}$  خطای ناشی از نقص سنسوری و عملگری است. برای اثبات پایداری از تابع لیاپانوف مشتق گرفته می شود

$$\begin{aligned} \dot{V} &= \dot{V}_1 + \dot{V}_2 \\ \dot{V}_1 &= (e_v)^T (D + G) \dot{e}_v \\ \dot{V}_2 &= (e_v^{sa})^T (D + G) \dot{e}_v^{sa} \\ \dot{V}_1 &= -C_v (e_v)^T (D + G) (L + G) e_v \\ \dot{V}_2 &= -C_v (e_v^{sa})^T (D + G) (L + G) e_v^{sa} \end{aligned} \quad (36)$$

$$\begin{cases} e_v = (L + G)\delta = (L + G)(v_{od} - v_{ref}) \\ e_v^{sa} = (L + G)\delta^{sa} = (L + G)(v_{od}^{sa} - v_{ref}) \\ \dot{e}_v = (L + G)\dot{\delta} = (L + G)\dot{v}_{od} = (L + G) - C_v e_v \\ \dot{e}_v^{sa} = (L + G)\dot{\delta}^{sa} = (L + G)\dot{v}_{od}^{sa} = (L + G) - C_v e_v^{sa} \end{cases} \quad (37)$$

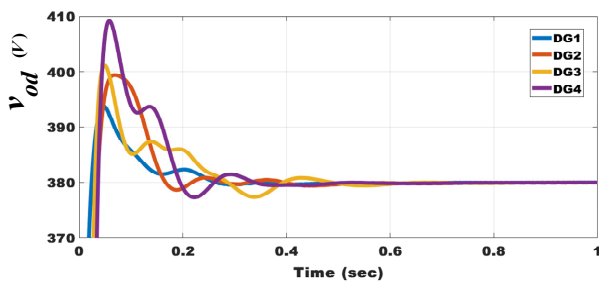
که در معادله بالا  $X = (D + G)(L + G)$  در نظر گرفته می شود. هر ماتریس مربعی را می توان به صورت زیر نوشت

$$X = \frac{1}{\gamma} [X + X^T] + \frac{1}{\gamma} [X - X^T] \quad (38)$$

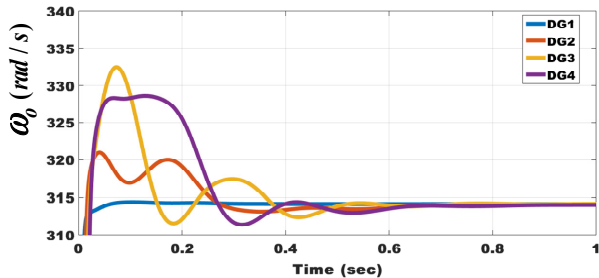
عبارت منفی برای دو عبارت بالا صفر می شود ( $e_v \frac{X - X^T}{\gamma} e_v = 0$ ) و بنابراین

$$\dot{V} = -\frac{C_v}{\gamma} e_v^T (X + X^T) e_v - \frac{C_v}{\gamma} (e_v^{sa})^T (X + X^T) e_v^{sa} \quad (39)$$



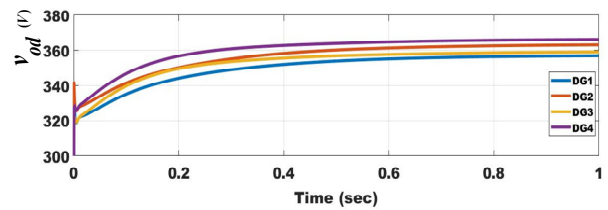


(الف)

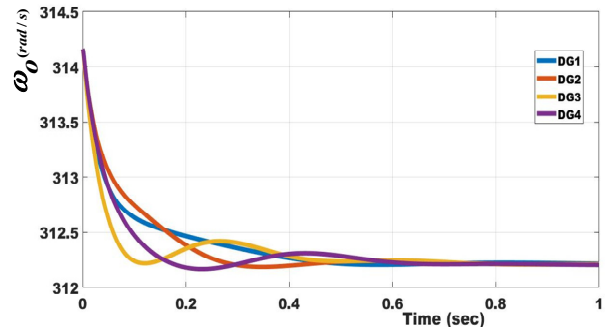


(ب)

شکل ۴: (الف) ولتاژ خروجی و (ب) فرکانس زاویه‌ای خروجی DGها بدون حمله سایبری، اغتشاش و نویز.



(الف)



(ب)

شکل ۳: (الف) خروجی ولتاژ و (ب) خروجی فرکانس ریزشبه با کنترل کننده اولیه (بدون کنترل کننده ثانویه).

جدول ۱: مقادیر پارامترهای مدل نمونه شبیه‌سازی شده [۳۷].

DG۱ & DG۲		DG۳ & DG۴	
$m_p$	$9.4 \times 10^{-2}$	$m_p$	$12.5 \times 10^{-2}$
$n_q$	$1.3 \times 10^{-7}$	$n_q$	$1.5 \times 10^{-7}$
$R_c$	$0.3 \Omega$	$R_c$	$0.3 \Omega$
$L_c$	$0.35 \text{ mH}$	$L_c$	$0.35 \text{ mH}$
$K_{PV}$	۱	$K_{PV}$	۱
$K_{IV}$	۴	$K_{IV}$	۴
$K_{PC}$	۱۵	$K_{PC}$	۱۰.۵
$K_{IC}$	۲۰۰	$K_{IC}$	۱۶۰

	Line ۱		Line ۲		Line ۳	
Lines	$R_{line}$	$0.23$	$R_{line}$	$0.25$	$R_{line}$	$0.23$
	$L_{line}$	$0.318 \text{ mH}$	$L_{line}$	$1.847 \text{ mH}$	$L_{line}$	$0.318 \text{ mH}$

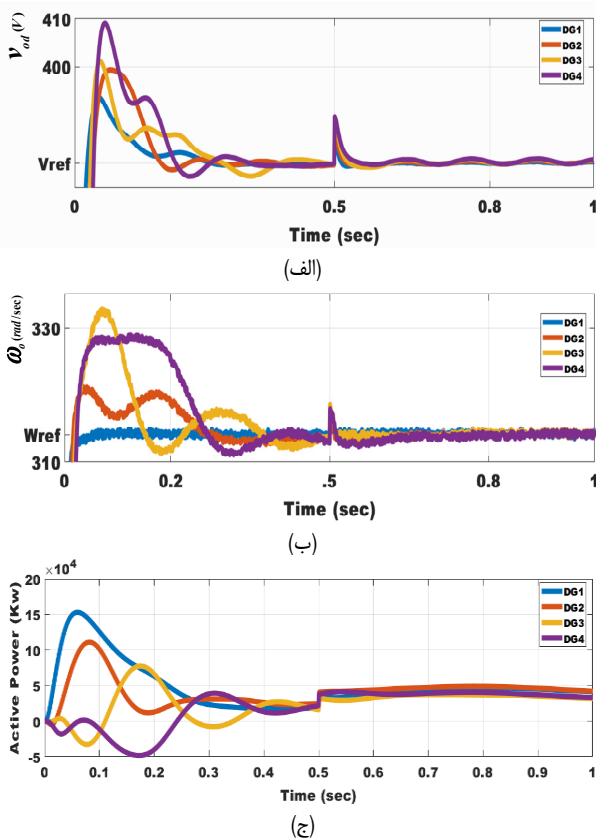
  

	Load ۱		Load ۲	
Loads	$P_{load}$	۱۲ Kw	$P_{load}$	۱۵.۳ Kw
	$Q_{load}$	۱۲ Kvar	$Q_{load}$	۷.۶ Kvar

### سناریوی دوم: خطای سنسوری ولتاژ در DG۱ و DG۳

به منظور بررسی اثرات خطا و تأثیر موقعیت منابع تولید پراکنده در خطای سنسوری و عملگری، موقعیت‌های مختلف بررسی گردیده و نتایج در شکل ۵ آمده است. با توجه به شکل در این سناریو در  $t = 0.5 \text{ sec}$  خطای سنسوری ولتاژ با اندازه  $\delta_{v1}^s = 10 + 3 \sin(10t)^\circ$  در DG۱ وارد شده و همین خطا در  $t = 1 \text{ sec}$  در سنسور ولتاژ DG۳ وارد می‌گردد. با توجه به شکل، هنگامی که خطای سنسوری در DG۱ اتفاق می‌افتد، اثر این حمله در DG۱ بیشتر از بقیه DGها است و به ترتیب DG۲، DG۳ و DG۴ اثرات بیشتری از خطا را می‌پذیرند و خطای سنسوری، DGهای همجوار را بیشتر تحت تأثیر قرار می‌دهد. با توجه به نتایج شبیه‌سازی، خطا در سنسور ولتاژ بر فرکانس خروجی DGها نیز تأثیر کمی دارد. در این سناریو همه DGها توانسته‌اند با وجود خطای سنسوری به پایداری برسند و سنکرون‌سازی نیز در زمان مناسبی انجام پذیرد.

با توجه به نتایج شبیه‌سازی، ولتاژ افت شدید دارد و سنکرون‌سازی نیز در این حالت انجام نشده و همچنین فرکانس و ولتاژ، انحراف پیدا کرده‌اند. با توجه به اینکه فرکانس بسیار به انحراف حساس است، بنابراین انحراف قابل قبول نیست؛ در نتیجه کم کردن انحراف در این حالت ضروری است. همچنین در این حالت سیستم به نویز، اغتشاش و دینامیک مدل نشده حساس است. کنترل کننده اولیه، پایداری سیستم را تا حد زیادی ایجاد کرده است؛ اما نتوانسته سنکرون‌سازی را به درستی انجام دهد. شکل ۴ کنترل ولتاژ و فرکانس توسط کنترل کننده اولیه و ثانویه را نشان می‌دهد. با توجه به شکل ۴ این کنترل کننده توانسته که به خوبی فرکانس و ولتاژ را به حالت مرجع خود برگرداند و در رنج ولتاژ و فرکانسی بسیار خوبی قرار دهد. زمان عبور از حالت گذرا کمتر از  $0.3$  ثانیه بوده که زمان مناسبی می‌باشد و همچنین سنکرون‌سازی بسیار خوب انجام شده است. در سنکرون‌سازی، خطای ماندگار حدود ۳ درصد برای ولتاژ نامی و برای فرکانس نیز  $0.3$  درصد قابل قبول می‌باشد.

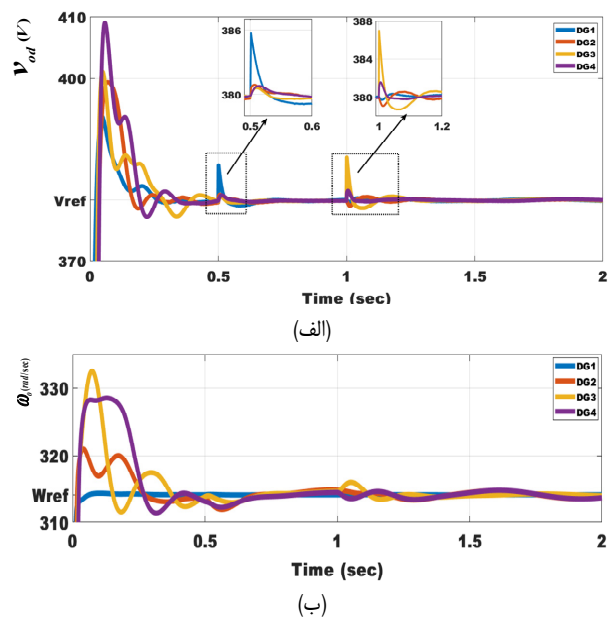


شکل ۷: (الف) ولتاژ، (ب) فرکانس و (ج) توان خروجی DGها با خطای سنسوری و عملگری در همه DGها.

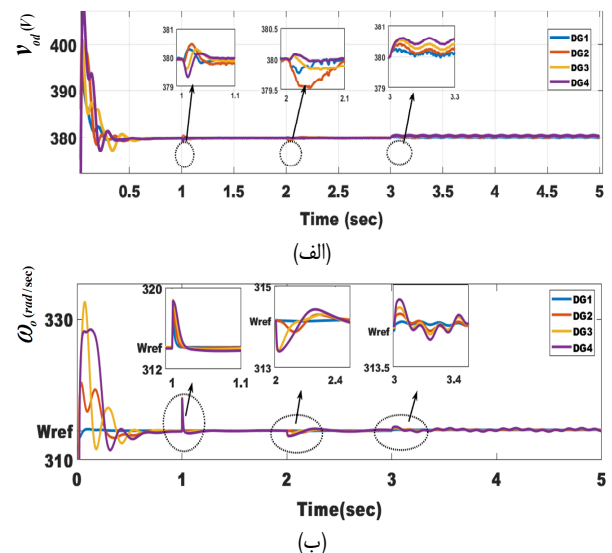
نیز انجام دهد. نکته دیگر اینکه خطای سنسوری فرکانس بر روی ولتاژ خروجی نیز تأثیر می‌گذارد و باعث تغییرات در ولتاژ DGها می‌گردد؛ به این معنی که خطا در فرکانس و ولتاژ بر روی همدیگر اثر دارند. خطای سنسوری توان نیز در همه DGها اتفاق افتاده است ولی به دلیل ضریب کوچک  $m_p$  تأثیر کمی در تغییر فرکانس و ولتاژ دارد و حتی با خطای سنسوری بزرگ در توان نیز مقادیر ولتاژ و فرکانس در رنج قابل قبولی کنترل می‌شود. هر قدر ضریب  $m_p$  بزرگ‌تر باشد اثر خطای سنسوری توان در خروجی بیشتر می‌گردد. نتایج شبیه‌سازی خطای عملگری نشان می‌دهد با توجه به آنکه این خطا توسط لایه ثانویه کنترل می‌شود، تأثیر کمتری در خروجی‌های ولتاژ و فرکانس دارد. البته نکته مهم آن است علی‌رغم اینکه در خطای عملگری سنکرون‌سازی انجام می‌شود ولی این مقادیر با مقدار مرجع، اختلاف کمی پیدا می‌کنند.

**سناریوی چهارم: خطای سنسوری و عملگری در همه سنسورها و با در نظر گرفتن نویز سنسوری**

برای تحلیل بهتر خطای سنسوری و عملگری در بدترین حالت، این خطا در همه سنسورهای ولتاژ، فرکانس، توان و همه عملگر شده است. در شکل ۷ نحوه انعطاف‌پذیری و مقاومت کنترل‌کننده در مقابل این اختلالات آمده است. خطا به همه سنسورها و عملگرها در  $t = 0.5 \text{ sec}$  و با مقادیر سناریوهای قبلی وارد شده است. در این سناریو، توان اکتیو نیز در شبیه‌سازی، بررسی گردیده تا توانایی کنترل‌کننده اولیه در تقسیم توان مشخص شود. همچنین برای بررسی توانایی کنترل‌کننده، نویز سنسوری نیز برای سنسورهای فرکانس به صورت تصادفی با میانگین صفر و با دامنه یک در نظر گرفته شده است. با توجه به نتایج شکل ۷، کنترل‌کننده توانسته که به خوبی پایدار بماند و فرکانس و ولتاژ همه DGها به مرجع رسیده‌اند و خطای حالت ماندگار سیستم، صفر و سنکرون‌سازی عامل‌ها نیز



شکل ۵: (الف) ولتاژ و (ب) فرکانس خروجی با خطای سنسوری ولتاژ در DG۱ و DG۳.

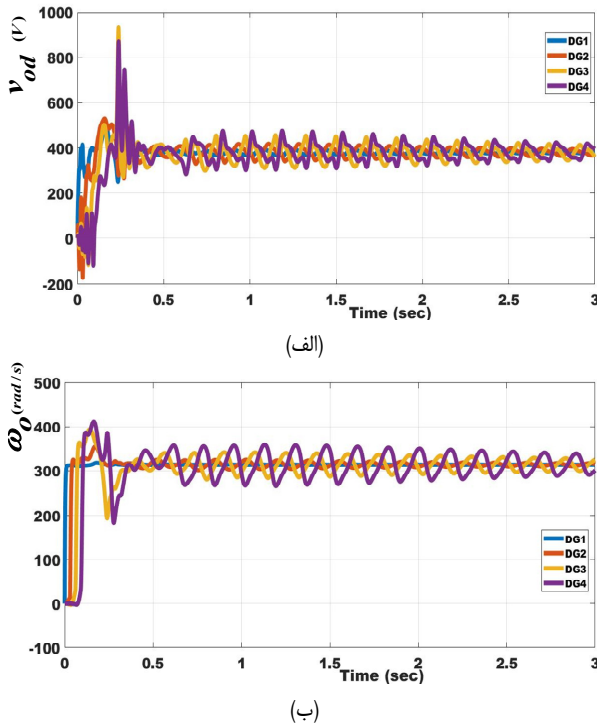


شکل ۶: (الف) ولتاژ و (ب) فرکانس خروجی با خطای سنسوری فرکانس و توان و خطای عملگری در همه DGها.

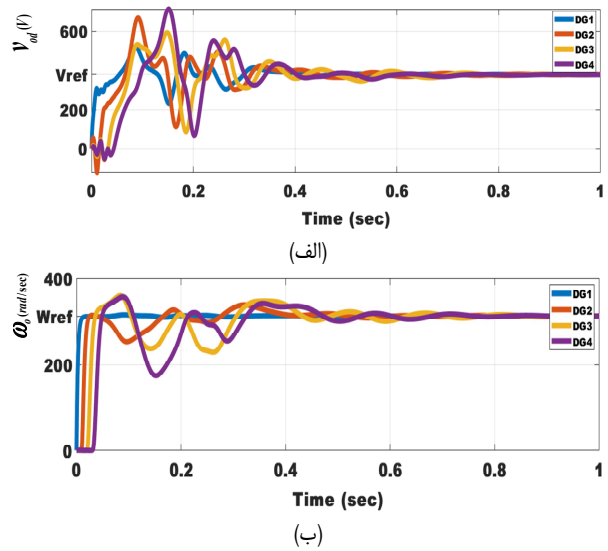
**سناریوی سوم: خطای سنسوری فرکانس و توان و خطای عملگری**

در این سناریو به منظور نشان دادن کارایی کنترل‌کننده در پایدارسازی و سنکرون‌سازی، خطاهای مختلف و در زمان‌های متفاوت در ریزشبهه وارد گردیده است. در  $t = 1 \text{ sec}$  خطای سنسوری فرکانس به صورت  $\delta_{fi}^s = 5 + 0.5 \sin(1 \cdot t) \text{ Hz}$  و در  $t = 2 \text{ sec}$  خطای سنسوری توان اکتیو به صورت  $\delta_{pi}^s = 20 + 4 \sin(1 \cdot t) \text{ Kw}$  و در همه DGها اتفاق می‌افتند. در  $t = 3 \text{ sec}$  خطای عملگری  $\delta_{vi}^u = \delta_{vi}^u = 50 + 10 \sin(5 \cdot t)$  در همه عملگرها وارد سیستم می‌گردد. شکل ۶ نتیجه این شبیه‌سازی را نشان می‌دهد. با توجه به نتایج خطای سنسوری، فرکانس تأثیر بیشتری در ریزشبهه دارد و رنج تغییرات قابل تحمل خطای فرکانس از ولتاژ کمتر است.

در عمل نیز ریزشبهه‌ها تغییرات فرکانسی محدودی را تحمل می‌کنند و رنج مقاومت فرکانس حدود ۰/۳ درصد است. هر چند این کنترل‌کننده به خوبی توانسته با وجود خطاهای سنسوری در رنج معلومی در کمتر از یک ثانیه، خروجی‌ها را به مقدار مرجع برساند و همچنین سنکرون‌سازی را



شکل ۹: عملکرد سیستم با تأخیر ۳۰ میلی‌ثانیه.



شکل ۸: (الف) ولتاژ و (ب) فرکانس خروجی DGها با تأخیر سنسوری و عملگری در خطوط ارتباطی.

انجام شده است. در این حالت دروپ توانسته که توان‌ها را به درستی بین DGها تقسیم کند. نویز سنسوری فرکانس فقط در خروجی فرکانس به مقدار کمی وارد شده و در ولتاژ و توان تأثیری ندارد.

### سناریوی پنجم: در نظر گرفتن تأخیر در کانال‌های ارتباطی

یکی از مشکلات همیشگی کانال‌های ارتباطی، تأخیر است. تأخیر به عوامل متعددی مانند ظرفیت انتقال لینک، تأخیر ارسال به نرخ ارسال، طول پیام و تأخیر دسترسی به کانال بستگی دارد. در کنترل ثانویه، اطلاعاتی که به کنترل‌کننده اولیه فرستاده می‌شود ممکن است دارای تأخیر باشد. تأخیر می‌تواند در این حالت ثابت، تصادفی یا محدود باشد. نکته مهم در مورد تأخیر این است که مسأله تأخیر در ریزشبه‌ها معمولاً حداکثر ۱۰ میلی‌ثانیه است. تأخیر زمانی ناشی از تأخیر پردازش، انتقال و محاسبه است. ماکسیمم تأخیر قابل تحمل، حداکثر مقداری می‌تواند باشد که باعث از بین رفتن پایداری نشود. تأخیر در دو مکان و به دو صورت ممکن است اتفاق بیفتد:

- در محل تبادل اطلاعات بین دو ریزشبه همجوار
- در محل بین کنترل‌کننده ثانویه و اولیه

می‌توان هر دو تأخیر را به صورت جداگانه بحث کرد و یا هر دو را با هم، یک تأخیر یکپارچه در نظر گرفت. در ریزشبه، تأخیر یکپارچه در نظر گرفته شده و معادله تأخیر سیستم DG به صورت یک جا و ثابت با زمان در (۴۲) آمده است

$$u_{vi}(t) = -C_v e_{vi}(t) = -C_v \sum a_{ij} (v_{oi}(t) - v_{oj}(t - \tau)) + g_i (v_{oi}(t) - v_{ref}) \quad (42)$$

که  $\tau$  تأخیر سیستم در انتقال اطلاعات از یک DG به همجوار است. شکل ۸ اثر تأخیر ۱۰ msec در ریزشبه را نشان داده است. با توجه به نتایج شبیه‌سازی، تأخیر تأثیر زیادی در مباحث پایداری و سنکرون سازی ریزشبه دارد. البته روش کنترلی توانسته حدود ۰/۵ ثانیه سنکرون سازی و پایداری را با تأخیر محدود انجام دهد؛ ولی در زمان‌های اولیه، افزایش ناگهانی فرکانس و ولتاژ مطلوب نیست.

### سناریوی ششم: تأخیر ۳۰ میلی‌ثانیه

تأخیر برای درک بهتر مسأله، بیشتر در نظر گرفته می‌شود که در این حالت، ۳۰ میلی‌ثانیه می‌باشد. نتایج شبیه‌سازی در شکل ۹ آمده است.

تأخیر با توجه به نتایج بالا بسیار در پایداری و سنکرون سازی سیستم ریزشبه مؤثر است؛ به نحوی که اگر تأخیر افزایش یابد ممکن است که سیستم به ناپایداری برود. همچنین با افزایش تأخیر حتی اگر پایداری تضمین شود، سنکرون سازی در زمان بیشتری اتفاق خواهد افتاد و یا بعضاً با مشکل مواجه می‌شود. لازم به ذکر است که تأخیرهای ریزشبه حداکثر ۱۰ میلی‌ثانیه است و بنابراین روش ارائه شده توانسته که تأخیر را در ریزشبه کنترل کند.

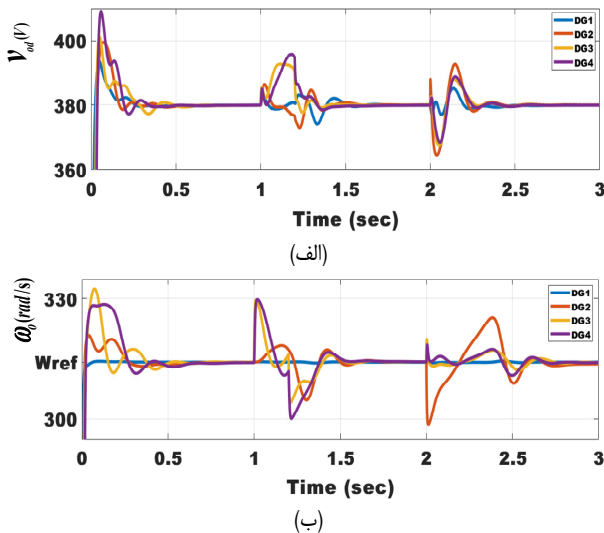
### سناریوی هفتم: مقایسه حمله سایبری سنسوری و عملگری با خطا و نقص در سنسورها و عملگرها

حمله سنسوری و عملگری و خطا از نظر عملکرد تقریباً نتایج یکسان دارند و دو روی یک سکه هستند (همان طور که اشاره شد، حمله در لینک ارتباطی و خطا در سنسور و عملگر اتفاق می‌افتد)؛ ولی اگر مقدار نرمال حمله و خطا در نظر گرفته شود قیاس این دو امکان پذیر است. مقدار نرمال خطای سنسوری ولتاژ با دامنه  $\delta_{vi}^s = 10$  در  $t = 0.5 \text{ sec}$  به سیستم وارد شده و حمله سنسوری ۲۰ درصد خروجی و در  $t = 1 \text{ sec}$  و برای همه سنسورها در نظر گرفته شده است. نتیجه شبیه‌سازی در شکل ۱۰ آمده است. به منظور مقایسه، حمله و خطا در سنسورهای ولتاژ وارد شده‌اند که با توجه به شکل، اثر خطای سنسوری کمتر است و حمله سنسوری با توجه به هوشمندبودنش تأثیر بیشتری دارد. همچنین تأثیر هر دو در تغییر فرکانس کم می‌باشد و به این معنی است که کنترل ولتاژ و فرکانس اثر کمی در همدیگر دارند.

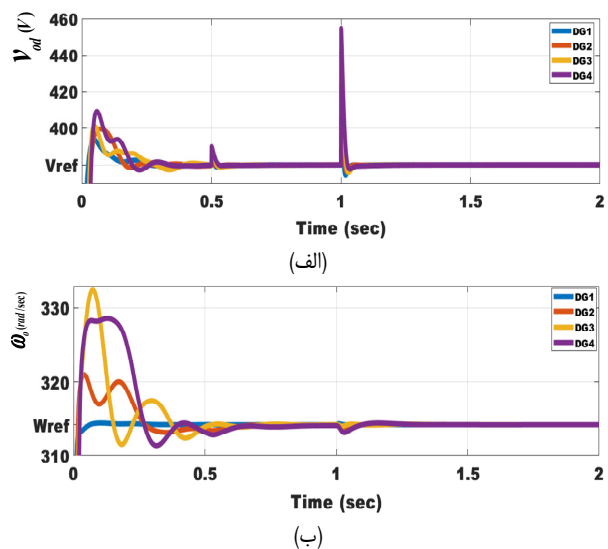
### سناریوی هشتم: مقایسه حمله سایبری ربودن اطلاعات با تزریق داده غلط به سنسورها

در حمله ربودن، اطلاعات مقادیر خروجی حذف شده و با مقدار جدید ناشی از حمله جایگزین می‌گردد. فرمول زیر اثر حمله ربودن اطلاعات را نشان می‌دهد

$$x^c(t) = (1 - \alpha)x(t) + \alpha x^a(t) \quad (43)$$



شکل ۱۱: مقایسه اثر حمله سایبری ربودن اطلاعات و خطای سنسوری ولتاژ.



شکل ۱۰: الف) ولتاژ و (ب) فرکانس خروجی DGها در مقایسه اثر حمله سایبری و خطای سنسوری ولتاژ.

پایدارسازی و سنکرون‌سازی منابع تولید پراکنده با تعریف قضیه‌های جدید بحث گردید. از کنترل‌کننده سلسه‌مراتبی توزیع‌شده اشتراکی که شامل کنترل‌کننده اولیه و ثانویه است برای کنترل DGها استفاده شده و نتایج نشان می‌دهند که کنترل‌کننده، پایداری و سنکرون‌سازی را با وجود خطای سنسوری و عملگری تضمین می‌کند و قوانین سیستم‌های چندعامله ریموند با این کنترل‌کننده رعایت می‌گردد. به‌منظور مشخص کردن اثرات خطای سنسوری و عملگری بر DGها، پایداری، عملکرد مقاوم و انعطاف‌پذیری کنترل‌کننده، فرمول‌بندی مناسب در معادلات ریزش‌بکه انجام شده است. تابع لیاپانوف مناسب برای تحلیل پایداری سیستم با حضور خطای سنسوری و عملگری پیشنهاد گردیده و نیز سنکرون‌سازی سیستم با کنترل‌کننده سلسه‌مراتبی توزیع‌شده اثبات گردیده است. نهایتاً برای اطمینان از نتایج تئوری ارائه‌شده با استفاده از شبیه‌سازی در متلب/سیمولینک، اثر خطا در DGهای مختلف نشان داده شده است. اثر خطای سنسوری با توجه به ماتریس مجاورت، تأثیرهای متفاوتی بر DGهای مختلف دارد و موقعیت DG در تأثیر خطا بر پایداری و سنکرون‌سازی مؤثر است. DGهای هم‌جوار که از هم اطلاعات می‌گیرند، تأثیر بیشتری بر هم دارند و هر قدر با هم فاصله داشته باشند و مستقیم از هم اطلاعات نگیرند، تأثیرپذیری کمتر می‌شود. نکته مهم دیگر اینکه خطای سنسوری فرکانس، تأثیر زیادی در ناپایداری ریزش‌بکه دارد و رنج خطای سنسوری در فرکانس، محدودتر از ولتاژ است. خطای سنسوری توان و خطای عملگری، تأثیر کمی در سیستم دارند. همچنین در شبیه‌سازی، حمله سایبری سنسوری و عملگری، حمله ربودن اطلاعات و خطای سنسوری و عملگری با هم مقایسه شده است. نتایج شبیه‌سازی نشان می‌دهند که کنترل حمله سایبری از خطا و نقص سنسوری، مشکل‌تر و همچنین رنج تغییرات نقص سنسوری از حمله‌های سایبری بیشتر است. به‌منظور بررسی مشکلات کانال‌های ارتباطی و عملکرد کنترل‌کننده، اثر تأخیر نیز در ریزش‌بکه شبیه‌سازی شده است. نتایج نشان می‌دهند که تأخیر، تأثیر زیادی در بحث پایداری و سنکرون‌سازی ریزش‌بکه دارد.

### مراجعه

- [1] L. Meng, et al., "Review on control of DC microgrids and multiple microgrid clusters," *IEEE J. of Emerging and Selected Topics in Power Electronics*, vol. 5, no. 3, pp. 928-948, Sept. 2017.
- [2] 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.

در این رابطه اگر  $\alpha = 0$  باشد، حمله اتفاق نیفتاده و اگر  $\alpha = 1$  باشد به این معنی است که حمله سایبری ربودن اطلاعات وجود دارد.  $x^c(t)$ ،  $x(t)$  و به‌ترتیب سیگنال مختل‌شده، سیگنال بدون حمله و سیگنال حمله است [۴۳].

به‌منظور مقایسه حمله سایبری ربودن اطلاعات و تزریق داده غلط سنسوری باید دقت شود که از نظر عملکرد این دو نوع با هم تفاوت دارند و همان‌طور که اشاره شد، حمله سایبری در لینک ارتباطی بین DGها اتفاق می‌افتد و تزریق داده غلط در سنسور و عملگر ایجاد می‌گردد. ولی اگر مقدار نرمال حمله و تزریق داده غلط در نظر گرفته شود، قیاس این دو و اثرشان بر سیستم امکان‌پذیر است. به‌منظور مقایسه، تزریق داده غلط سنسوری در DG۲ در نظر گرفته شده تا مقدار منتقل‌شده به DG۳ قابل مقایسه با حمله سایبری ربودن اطلاعات بین کانال ارتباطی DG۲ و DG۳ باشد.

تزریق داده غلط با (۲۱) و (۲۲) و حمله ربودن اطلاعات با (۴۳) تعریف می‌گردد و برای ولتاژ، فرکانس با (۴۴) در معادلات وارد می‌گردد

$$\begin{cases} v_{oj}^c(t) = (1-\alpha)v_{oj}(t) + \alpha v_{oj}^a(t) \\ \omega_{oj}^c(t) = (1-\alpha)\omega_{oj}(t) + \alpha \omega_{oj}^a(t) \end{cases} \quad (44)$$

در تزریق داده غلط،  $\delta_{vi}^s$  و  $\delta_{oi}^s$  مقادیر غلط داده سنسوری ولتاژ و فرکانس هستند که به DG۲ وارد می‌گردند. داده غلط تزریق سنسوری ولتاژ با دامنه  $\delta_{vr}^s = 10v$  و سنسوری فرکانس  $\delta_{or}^s = 16 \text{ rad/sec}$  در لحظه  $t = 2 \text{ sec}$  به سیستم وارد می‌شود. حمله ربودن اطلاعات با مقدار ولتاژ  $v_{adj}^a = 390v$  و فرکانس  $\omega_{oj}^a = 330 \text{ rad/sec}$  در کانال ارتباطی بین DG۲ و DG۳ در نظر گرفته شده است.

نتیجه شبیه‌سازی در شکل ۱۱ آمده است. حمله سایبری ربودن اطلاعات نسبت به تزریق داده غلط سنسوری در زمان بیشتری به حالت سنکرون برمی‌گردد و به عبارتی، پایدارسازی و سنکرون‌سازی حمله سایبری سخت‌تر است. دلیل اصلی آن است که حمله سایبری، هوشمند و کنترل آن نسبت به تزریق داده غلط که هوشمندی ندارد مشکل‌تر است.

### ۸- نتیجه‌گیری

در این مقاله با در نظر گرفتن DGها به‌صورت سیستم‌های چندعامله، اثر خطا و حمله سایبری سنسوری و عملگری بر ریزش‌بکه بحث گردیده است.

- Applications, ICIEA'20*, pp. 170-175, Kristiansand, Norway, 9-13 Nov. 2020.
- [23] R. Lu and J. Wang, "Distributed control for AC microgrids with false data injection attacks and time delays," in *Proc. E3S Web of Conf.*, vol. 194, Article ID: 03023, 2020.
- [24] N. M. Dehkordi and S. Z. Moussavi, "Distributed resilient adaptive control of islanded microgrids under sensor/actuator faults," *IEEE Trans. on Smart Grid*, vol. 11, no. 3, pp. 2699-2708, May 2019.
- [25] Z. Xie and Z. Wu, "Distributed fault-tolerant secondary control for DC microgrids against false data injection attacks," *International J. of Electrical Power & Energy Systems*, vol. 144, Article ID: 108599, Jan. 2023.
- [26] 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 Smart Grid Conf., SGC'2020*, 6 pp., Kashan, Iran, 16-17 Dec. 2020.
- [27] 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.
- [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] 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. 2013.
- [30] 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.
- [31] 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.
- [32] 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.
- [33] 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.
- [34] 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.
- [35] F. L. Lewis, H. Zhang, K. Hengster-Movric, and A. Das, *Cooperative Control of Multi-Agent Systems Optimal and Adaptive Design Approaches*, SpringerLink, 2014.
- [36] A. Mustafa, H. Modares, and R. Moghadam, "Resilient synchronization of distributed multi-agent systems under attacks," *Automatica*, vol. 115, Article ID: 108869, May 2020.
- [37] 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.
- [38] F. D. Mohammadi, H. K. Vanashi, and A. Feliachi, "State-space modeling, analysis, and distributed secondary frequency control of isolated microgrids," *IEEE Trans. on Energy Conversion*, vol. 33, no. 1, pp. 155-165, Mar. 2017.
- [39] D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X. M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674-1683, 31 Jan. 2018.
- [40] 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. 2020, pp. 1426-1439, 2020.
- [41] C. Chen, et al., "Resilient adaptive and  $H_\infty$  controls of multi-agent systems under sensor and actuator faults," *Automatica*, vol. 102, pp. 19-26, Apr. 2019.
- [42] 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.
- [43] S. Sahoo, J. C. H. Peng, S. Mishra, and T. Dragičević, "Distributed screening of hijacking attacks in DC microgrids," *IEEE Trans. on Power Electronics*, vol. 35, no. 7, pp. 7574-7582, Jul. 2019.
- [3] M. Chen, X. Xiao, and J. M. Guerrero, "Secondary restoration control of islanded microgrids with a decentralized event-triggered strategy," *IEEE Trans. on Industrial Informatics*, vol. 14, no. 9, pp. 3870-3880, Sept. 2017.
- [4] A. Mirzabeigi, A. Kazemy, M. Ramezani, and S. M. Azimi, "Distributed robust cooperative hierarchical control for island microgrids under hijacking attacks based on multi-agent systems," *Hindawi International Trans. on Electrical Energy Systems*, vol. 2023, Article ID 6622346, 15 pp., 2023.
- [۵] ع. میرزاییگی، ع. کاظمی، م. رضائی، و س. م. عظیمی "طراحی کنترل کننده ثانویه پایه ریزی شده بر روی کنترل اشتراکی توزیع شده منابع تولید پراکنده (DGها) با رویکرد سیستم های چندعامله با در نظر گرفتن حملات سایبری DoS"، *تشریح مهندسی برق و مهندسی کامپیوتر ایران، الف- مهندسی برق، سال ۲۰، شماره ۴، صص. ۲۹۰-۲۸۲، زمستان ۱۴۰۱.*
- [6] 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. 2019.
- [7] 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. 2019.
- [8] 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.
- [9] 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.
- [10] 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, 15 Mar. 2022.
- [11] 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.
- [12] M. Xie, Y. Song, and S. Shen, "Event-based consensus control for multi-agent systems against joint sensor and actuator attacks," *ISA Trans.*, vol. 127, pp. 156-167, Aug. 2022.
- [13] H. Yan, J. Han, H. Zhang, X. Zhan, and Y. Wang, "Adaptive event-triggered predictive control for finite time microgrid," *IEEE Trans. on Circuits and Systems I: Regular Papers*, vol. 67, no. 3, pp. 1035-1044, Mar. 2020.
- [14] M. Shi, X. Chen, M. Shahidehpour, Q. Zhou, and J. Wen, "Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded AC microgrids," *IEEE Trans. on Smart Grid*, vol. 12, no. 3, pp. 1953-1963, May 2021.
- [15] X. Lu, X. Yu, J. Lai, J. M. Guerrero, and H. Zhou, "Distributed secondary voltage and frequency control for islanded microgrids with uncertain communication links," *IEEE Trans. on Industrial Informatics*, vol. 13, no. 2, pp. 448-460, Apr. 2016.
- [16] J. Lai, H. Zhou, X. Lu, X. Yu, and W. Hu, "Droop-based distributed cooperative control for microgrids with time-varying delays," *IEEE Trans. on Smart Grid*, vol. 7, no. 4, pp. 1775-1789, Jul. 2016.
- [17] H. Xin, Z. Qu, J. Seuss, and A. Maknouninejad, "A self-organizing strategy for power flow control of photovoltaic generators in a distribution network," *IEEE Trans. on Power Systems*, vol. 26, no. 3, pp. 1462-1473, Aug. 2010.
- [18] S. Abhinav, I. D. Schizas, F. L. Lewis, and A. Davoudi, "Distributed noise-resilient networked synchrony of active distribution systems," *IEEE Trans. on Smart Grid*, vol. 9, no. 2, pp. 836-846, Mar. 2016.
- [19] D. Ye, X. Zhao, and B. Cao, "Distributed adaptive fault-tolerant consensus tracking of multi-agent systems against time-varying actuator faults," *IET Control Theory & Applications*, vol. 10, no. 5, pp. 554-563, Mar. 2016.
- [20] Y. Wang, Y. Song, and F. L. Lewis, "Robust adaptive fault-tolerant control of multiagent systems with uncertain nonidentical dynamics and undetectable actuation failures," *IEEE Trans. on Industrial Electronics*, vol. 62, no. 6, pp. 3978-3988, Jun. 2015.
- [21] 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.
- [22] B. Wang, Q. Sun, and D. Ma, "A periodic event-triggering reactive power sharing control in an islanded microgrid considering DoS attacks," in *Proc. 15th IEEE Conf. on Industrial Electronics and*

**مهدی رضانی** 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 دانشیار دانشکده مهندسی برق دانشگاه صنعتی همدان می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: ریزشبکه، کنترل و پایداری در ریزشبکه‌ها و سیستم‌های قدرت.

**عبدالله میرزابیگی** تحصیلات خود را در مقاطع کارشناسی مهندسی برق الکترونیک در سال ۱۳۸۲ از دانشگاه تبریز، کارشناسی ارشد مهندسی برق کنترل در سال ۱۳۸۵ از دانشگاه علم و صنعت ایران و دکتری مهندسی برق کنترل از دانشگاه تفرش را در سال ۱۴۰۲ به پایان رسانده است. از سال ۱۳۸۷ به عنوان عضو هیأت علمی در موسسه آموزش عالی جهاد دانشگاهی همدان مشغول به فعالیت می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: ریزشبکه، آنالیز و کنترل سیستم‌های با تاخیر زمانی، سیستم‌های چندانگله 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 چندانگله، سیستم‌های پیچیده و حملات سایبری.