مقاله پژوهشی

تحلیل اثرات حمله‌های سایبری مختلف بر کنترل‌کننده ثانویه در ریزشبکه‌های جزیره‌ای

عبدالله میرزابیگی و علی کلانترنیا

چکیده: با پیشرفت علم در بسیاری از روش‌های کنترلی از اطلاعات سیستم همجوار به‌منظور کنترل بهتر و همگام‌سازی بین واحدهای مختلف ریزشبکه‌ها استفاده می‌شود. در دسترسی و انتقال اطلاعات از طریق لینک‌های ارتباطی، مشکلاتی مختلفی به‌وجود می‌آید. در این مقاله آسیب‌پذیری و انعطاف‌پذیری روش‌های کنترل ثانویه توزیع‌شده اشتراکی مورد مطالعه قرار گرفته و همچنین اثرات حمله‌های سایبری منع سرویس (DoS)، سنسوری و عملگری و ربودن اطلاعات بر ریزشبکه جزیره‌ای بررسی شده است. علاوه بر پایداری در این مقاله، همگام‌سازی نیز تحلیل گردیده است. برای بررسی همزمان پایداری و همگام‌سازی ریزشبکه از دیدگاه سیستم‌های چندعامله استفاده شده است. اثرات حمله‌های سایبری در کنترل‌کننده ثانویه فرمول‌بندی ریاضی شده و کنترل‌کننده مناسب برای حذف حمله‌ها طراحی شده است. در اثبات پایداری و همگام‌سازی فرکانس و ولتاژ، تابع لیاپانوف مناسب ارائه و تحلیل هم‌زمان پایداری و همگام‌سازی با اثبات قضیه‌های کاربردی انجام شده است. ضریب تاب‌آوری برای حمله‌های مختلف محاسبه گردیده و نشان داده شده که سیستم در مقابل حمله‌های سایبری تاب‌آور است. به‌منظور تأیید مباحث تئوری، یک مدل نمونه با وجود حمله‌های سایبری در متلب/ سیمولینک شبیه‌سازی گردیده و با توجه به نتایج شبیه‌سازی، همگام‌سازی و پایدارسازی انجام شده است.

کلیدواژه: **ریزشبکه جزیره‌ای، حمله‌های سایبری، سیستم‌های چندعامله، کنترل‌کننده سلسله‌مراتبی توزیع‌شده.**

اختصارات

A_G : ماتریس انتقال در گراف
$E(G)$: ماتریس لینک ارتباطی
A : ماتریس سیستم
$x(t)$: حالت سیستم بدون حمله
$x^*(t)$: میانگین پارامتر $x(t)$
G : ماتریس اتصال به اسلک[1]
L : ماتریس لاپلاسین
g_i : بهره اتصال[2]
g_i^f : بهره فیدبک
g_i^p : بهره فیدبک مثبت
a_{ij} : درایه‌های ماتریس مجاورت[3]
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
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_{Pi} : ضریب دروپ فرکانس
n_{Qi} : ضریب دروپ ولتاژ
δ : سیگنال عدم تطابق
e_{vi} : خطای ردیابی محلی ولتاژ
$e_{\omega i}$: خطای ردیابی محلی[5] فرکانس
ϕ : متغیر کمکی کنترل‌کننده ولتاژ
γ : متغیر کمکی کنترل‌کننده جریان
ν : گره[6] در تئوری گراف
L_{line} : اندوکتانس خطوط بین DG ها
R_{line} : مقاومت خطوط بین DG ها
σ : مقدار تکین

این مقاله در تاریخ ۱۵ تیر ماه ۱۴۰۲ دریافت و در تاریخ ۲۰ بهمن ماه ۱۴۰۲ بازنگری شد.

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

علی کلانترنیا، گروه مهندسی برق، دانشکده مهندسی، دانشگاه بوعلی سینا، همدان، ایران، (email: a.kalantarnia@uast.ac.ir).

1. Slack Bus
2. Pinning Gain
3. Adjacency Matrix
4. Auxiliary Control
5. The Local Neighborhood Tracking Error
6. Node

x^c: پارامتر x مختل‌شده با حمله
C_V: بهره کنترلی ولتاژ
C_P: بهره کنترلی توان اکتیو
C_ω: بهره کنترلی فرکانس زاویه‌ای
y: اطلاعات اندازه‌گیری‌شده سنسور
y^c: خروجی مختل‌شده با حمله
y^a: اطلاعات غلط تزریق‌شده توسط حمله‌کننده
y_i^s: سیگنال مختل‌شده ناشی از حمله عملگری و سنسوری
y^a: سیگنال حمله
x_i^s: حالت مختل‌شده با حمله عملگری و سنسوری
u_i^{cc}: سیگنال کنترلی با حمله عملگری و سنسوری
e_i^c: خطا با درنظرگرفتن خطای سنسوری
u_i^a: سیگنال حمله عملگری
$\overline{\kappa}_\omega$، $\overline{\kappa}_v$ و $\overline{\kappa}_P$: حداکثر مقادیر خطاهای سنسوری
t_s^{ij}: زمان شروع حمله DoS[۱] ام s
τ_s^{ij}: بازه زمانی حمله DoS بین دو DG_i و DG_j
Ξ_D^{ij}: مجموع زمانی حمله DoS
$\theta^x(t)$: ماتریس حمله سایبری DoS در حالت
$\theta^u(t)$: ماتریس حمله سایبری DoS در ورودی کنترلی
$\theta_{jv}^x(t)$: ماتریس حمله سایبری به ولتاژ اندازه‌گیری‌شده
$\theta_{i\omega}^x(t)$: ماتریس حمله سایبری به فرکانس زاویه‌ای اندازه‌گیری‌شده
$\theta_{jp}^x(t)$: ماتریس حمله سایبری به توان اکتیو اندازه‌گیری‌شده
$\theta_{jv}^u(t)$: ماتریس حمله سایبری به ورودی کنترلی ولتاژ
$\theta_{i\omega}^u(t)$: ماتریس حمله سایبری به ورودی کنترلی فرکانس زاویه‌ای
$\theta_{jp}^u(t)$: ماتریس حمله سایبری به ورودی کنترلی توان
LPF: فیلتر پایین‌گذر

۱- مقدمه

مفهوم ریزشبکه در دهه‌های اخیر مورد توجه طیف وسیعی از پژوهشگران و صنعتگران واقع شده است. علت این امر توسعه منابع انرژی تجدیدپذیر، پیشرفت فناوری و سیاست دولت‌ها برای کاهش مصرف سوخت‌های فسیلی و بهبود شرایط زیست‌محیطی است.

در زمینه منابع انرژی تجدیدپذیر می‌توان به انرژی‌های خورشیدی، بادی، زمین‌گرمایی، جزر و مد، پیل سوختی و زیست توده اشاره نمود [۱]. برای همگام‌سازی بین ریزشبکه، استفاده از شبکه‌های مخابراتی ضروری شده و بنابراین ریزشبکه‌ها را به سیستم‌های فیزیکی- سایبری تبدیل کرده است [۲]. ریزشبکه از تعدادی منبع تولید پراکنده تشکیل شده است. یک ریزشبکه در دو حالت وصل به شبکه[۲] و جزیره‌ای[۳] مورد بهره‌برداری قرار می‌گیرد. در وصل به شبکه، کنترل اغلب از طریق شبکه اصلی انجام می‌گردد. ریزشبکه جزیره‌ای برای مکان‌های دوردست کاربرد زیادی دارد و باید خروجی‌های منابع تولید پراکنده با هم همگام باشند. کنترل‌کننده‌ها در حالت جزیره‌ای باید علاوه بر پایداری، تنظیم و یکسان‌سازی مقادیر ولتاژ و فرکانس خروجی همه منابع را انجام دهند [۳].

پارامترهای مهمی که در منابع تولید پراکنده باید کنترل شوند، فرکانس و ولتاژ، کنترل تبادل توان اکتیو و راکتیو بین واحدهای منابع تولید پراکنده و نیز با شبکه اصلی و همگام‌سازی ریزشبکه با شبکه اصلی[۴] هستند [۴]. در حالت کلی سه روش کنترلی مختلف برای ریزشبکه وجود دارد: ۱) کنترل متمرکز[۵]، ۲) کنترل غیرمتمرکز[۶] و ۳) کنترل توزیع‌شده[۷]. کنترل‌کننده متمرکز از یک کنترل‌کننده مرکزی استفاده کرده و اطلاعات همه واحدها به این کنترل‌کننده ارسال می‌گردد و کنترل در آن به‌صورت یکپارچه انجام می‌شود. در کنترل‌کننده غیرمتمرکز برای هر واحد، کنترل‌کننده جداگانه طراحی می‌گردد. کنترل‌کننده‌ها و واحدهای مختلف، ارتباطی با هم ندارند و هر واحد توسط کنترل‌کننده خودش مدیریت می‌شود. با توجه به آنکه در این روش امکان همگام‌سازی وجود ندارد، معمولاً در حالت جزیره‌ای از این روش استفاده نمی‌شود [۵]. در روش کنترلی توزیع‌شده برای هر واحد، کنترل‌کننده مجزا طراحی می‌گردد و کنترل‌کننده‌ها از اطلاعات واحدهای همجوار نیز استفاده می‌کنند.

کنترل‌کننده‌های بالا معمولاً به‌صورت سلسه‌مراتبی مورد استفاده قرار می‌گیرند. 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[۸]، ثانویه[۹] و ثالثیه[۱۰] تقسیم می‌شود [۶] و [۷].

کنترل‌کننده دروپ، یک کنترل‌کننده غیرمتمرکز و کنترل‌کننده ثالثیه، یک کنترل‌کننده متمرکز است. با توجه به استفاده از اطلاعات عامل‌های همجوار، روش توزیع‌شده برای همگام‌سازی و پایدارسازی، مناسب‌تر از بقیه کنترل‌کننده‌هاست و به همین دلیل در کنترل ریزشبکه‌ها بسیار پرکاربرد است [۸].

در کنترل‌کننده متمرکز و توزیع‌شده برای کنترل به لینک‌های ارتباطی نیاز است. در استفاده از لینک‌های ارتباطی مشکلات مختلفی از جمله اختلال، تلفات، عدم قطعیت، نویز، تأخیر و حمله‌های سایبری به‌وجود می‌آید. در این مقاله به تأثیر حمله‌های سایبری بر ریزشبکه‌ها و حذف اثر آنها با استفاده از کنترل‌کننده ثانویه پرداخته شده است.

امروزه با پیشرفت تحقیقات در حوزه‌های ارتباطی، حمله‌های سایبری اهمیت ویژه‌ای پیدا کرده‌اند. حمله‌های سایبری مختلفی در شبکه‌های ارتباطی ایجاد شده و باعث تخریب و آسیب به سیستم‌ها می‌گردند. 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 [۹]. بحث مشکلات کانال ارتباطی و حمله‌های سایبری بر روی ریزشبکه نیز در مراجع مختلفی بحث شده است [۱۰] تا [۱۳].

در [۱۴] حملات سایبری به سنسورها و عملگرها بر روی سیستم‌های چندعامله[۱۱] بحث گردیده و در [۱۵] حمله سایبری تزریق اطلاعات غلط با طراحی کنترل‌کننده مقاوم حذف می‌گردد. در [۱۶] اثر حمله سایبری DoS در یک کنترل‌کننده سلسه‌مراتبی با استفاده از روش اجماع[۱۲] برای ریزشبکه بررسی شده است. نویسندگان در [۱۷]، آسیب‌پذیری سایبری و

1. Denial of Service Attack
2. Grid Connected Mode
3. Islanded Mode
4. Main Grid
5. Centralized Control
6. Decentralized Control
7. Distributed Control
8. Primary Control
9. Secondary Control
10. Tertiary Control
11. Multi Agent Systems
12. Consensus

پایداری ریزشبکه‌های DC کنترل‌شده ثانویه را تحت حملات DoS ارزیابی می‌کنند. در [۱۸] اثر حمله DoS بر کنترل‌کننده ثانویه با روش اجماع میانگین بررسی شده که این روش در همگام‌سازی، دقیق نیست و امکان خطا دارد. در [۱۹] اثر حمله سنسوری و عملگری در معادلات ریزشبکه، وارد و با استفاده از روش کنترل مقاوم H_∞ اثر خطا کنترل شده است. مرجع [۲۰] به گم‌شدن داده بین ریزشبکه و شبکه اصلی پرداخته است. در [۱۳] اثر ازبین‌رفتن دیتا در ریزشبکه بررسی شده و نیز تأخیر در اثر این حمله مورد ارزیابی قرار گرفته است. در [۲۱] حمله سایبری DoS به‌صورت مسدودشدن موقت کانال مخابراتی و تأخیر در یک ریزشبکه در نظر گرفته شده و اثر آن بر سیستم‌ها نشان داده شده است؛ البته بررسی حمله به‌صورت تأخیر با واقعیت حمله DoS سازگاری ندارد. در [۲۲] برای ازبین‌بردن اثر حمله سایبری منع سرویس در ریزشبکه از کنترل‌کننده غیرمتمرکز و با دیدگاه سیستم‌های چندعامله استفاده گردیده است. در [۲۳] اثر حمله‌های سنسوری، ربودن اطلاعات و منع سرویس بر روی کنترل‌کننده ثانویه آمده است؛ اما پایداری و همگام‌سازی آن بحث و تحلیل نشده است. در [۱۸] از کنترل‌کننده توزیع‌شده برای کنترل ریزشبکه و رفع اثر حمله DoS استفاده شده و سپس با استفاده از کنترل‌کننده توزیع‌شده به‌صورت استفاده از میانگین خروجی‌ها به‌عنوان مرجع و با وجود محدودیت بار توانی ثابت، اثر حمله تحلیل شده است. در [۱۸] برای ازبین‌بردن اثر حمله از میانگین ولتاژ و فرکانس خروجی استفاده شده و در مقاله ارائه‌شده از مرجع استفاده گردیده است. استفاده از میانگین علی‌رغم اینکه اثر حمله را از بین می‌برد، ممکن است باعث شود خروجی‌ها از مقدار مرجع فاصله بگیرند و به سمت مقدار میانگین بازیابی شوند. در [۲۴] اثر حمله سایبری DoS در ریزشبکه برای فرکانس با استفاده از روش کنترل‌کننده ثانویه و با درنظرگرفتن مرجع توان اکتیو تحلیل شده است؛ اما بررسی در مورد ولتاژ صورت نگرفته و با استفاده از این روش ولتاژ بازیابی نمی‌گردد. در [۱۰] با درنظرگرفتن حمله تزریق اطلاعات غلط نامحدود در ریزشبکه‌های DC، یک کنترل ولتاژ انعطاف‌پذیر پیشنهاد شده است. در [۲۵]، یک روش کنترل انعطاف‌پذیر چندلایه در برابر حمله سایبری ارائه شده است. با این حال، این تحقیقات فقط حمله لینک را در نظر می‌گیرند و حمله حسگر در نظر گرفته نشده است. در [۲۶] یک زنجیره بلوکی[1] برای افزایش امنیت سیستم‌های کنترل کنترل توزیع‌شده در ریزشبکه‌ها و در [۲۷]، ارتباطات کوانتومی برای افزایش امنیت سایبری در ارتباطات کنترل توزیع‌شده ریزشبکه پیشنهاد شده است. در [۲۸] بر اساس تکنیک‌های کنترل تطبیقی، یک کنترل انعطاف‌پذیر سایبری توزیع‌شده برای چندین DG پیشنهاد گردیده که در معرض خطاها و حملات تزریق اطلاعات غلط به کنترل‌کننده‌های ثانویه خود هستند. در [۲۹] فقط فرکانس مورد تحلیل قرار گرفته و حمله سایبری تزریق داده غلط فقط در فرکانس تحلیل شده است. مرجع [۳۰] برای محافظت جامع از سیستم کنترل ثانویه ریزشبکه‌ها در برابر حملات تزریق اطلاعات غلط، یک کنترل مقاوم در برابر حمله را برای همگام‌سازی فرکانس ریزشبکه‌های جزیره‌ای معرفی می‌کند.

در کاربرد حمله‌های سایبری در ریزشبکه‌ها اغلب مقاله‌های منتشرشده بر روی شناسایی و یا اثر حمله بر ریزشبکه‌ها بوده و به مباحث کنترلی و همگام‌سازی پرداخته نشده است. در اکثر پژوهش‌های انجام‌شده مباحث پایداری، توابع لیاپانوف، مقاوم‌بودن و همگام‌سازی به‌اختصار بررسی شده و همچنین مهم‌ترین مسئله در حمله‌های سایبری، میزان تاب‌آوری در برابر این حملات است. از آنجایی که ریزشبکه‌ها به‌طور مداوم توسط حمله‌های سایبری تحت شرایط متغیر محیطی و عملیاتی تهدید می‌شوند، افزایش انعطاف‌پذیری سیستم در برابر چنین رویدادهایی باید افزایش یابد.

در این مقاله اثر حملات سایبری مختلف بر کنترل‌کننده سلسله‌مراتبی در ریزشبکه با دیدگاه سیستم‌های چندعامله تحلیل شده است. DGها به‌صورت عامل و لینک‌های مخابراتی بین آنها با ماتریس مجاورتی مورد مطالعه قرار گرفته است. به‌منظور کنترل بهتر از روش مرجع استفاده شده و ولتاژ، فرکانس و توان با هم کنترل گردیده است. برای تحلیل ابتدا معادلات ریاضی ریزشبکه به همراه حمله استخراج شده و سپس اثر حمله در کنترل‌کننده آمده و پایداری و همگام‌سازی ارزیابی گردیده است. نهایتاً باید با طراحی کنترل‌کننده، پایدارسازی و همگام‌سازی انجام گردد. در این مقاله سعی شده که اثرات این حمله بر پایداری و همگام‌سازی کنترل‌کننده ثانویه ریزشبکه تحلیل گردد و شرایط همگام‌سازی و پایدارسازی به‌دست آید. همچنین برای مقایسه اثرات و تاب‌آوری حمله‌های سایبری، شاخص تاب‌آوری[2] (RI) ارائه و محاسبه شده تا اثر هر حمله بر ریزشبکه به‌دست آید. نوآوری‌های این مقاله به شرح زیر است:

۱) مدل‌سازی و فرمول‌بندی حمله‌های سایبری (DoS، سنسوری و عملگری و ربودن اطلاعات) و همچنین اختلالات مختلف کانال ارتباطی در مدل منابع تولید پراکنده در کنترل‌کننده ثانویه (اثر حملات سایبری بر این نوع کنترل‌کننده برای اولین بار بررسی شده است.)

۲) ارائه قضیه‌های لیاپانوف مرتبط و بررسی پایداری و شرایط همگام‌سازی با وجود حمله‌های مختلف در سیستم ریزشبکه برای کنترل‌کننده ثانویه

۳) بررسی و مقایسه تاب‌آوری کنترل‌کننده سلسه‌مراتبی توزیع‌شده اشتراکی برای حذف اثرات حمله‌های سایبری DoS، حمله سنسوری سنسوری و عملگری و ربودن اطلاعات در کنترل‌کننده ثانویه

۴) مقایسه توانایی کنترل‌کننده در همگام‌سازی و مشخص‌کردن انعطاف‌پذیری و مقاوم‌بودن همه DGها با به‌دست‌آوردن ضریب RI

۵) تحلیل حمله DoS در انتقال خروجی‌های سنسوری

در بخش دوم، مدل دینامیکی منابع تولید پراکنده و لینک‌های ارتباطی بحث می‌گردد و در بخش سوم، روش کنترلی طراحی‌شده مورد مطالعه قرار می‌گیرد. در بخش چهارم بررسی اثر حملات سایبری و فرمول‌بندی حمله‌های سایبری در کنترل‌کننده سلسه‌مراتبی توزیع‌شده اشتراکی و در بخش پنجم تابع لیاپانوف و شرایط پایداری آورده شده است. در بخش ششم شبیه‌سازی و نهایتاً در بخش هفتم نتیجه‌گیری و پیشنهادها ارائه گردیده است.

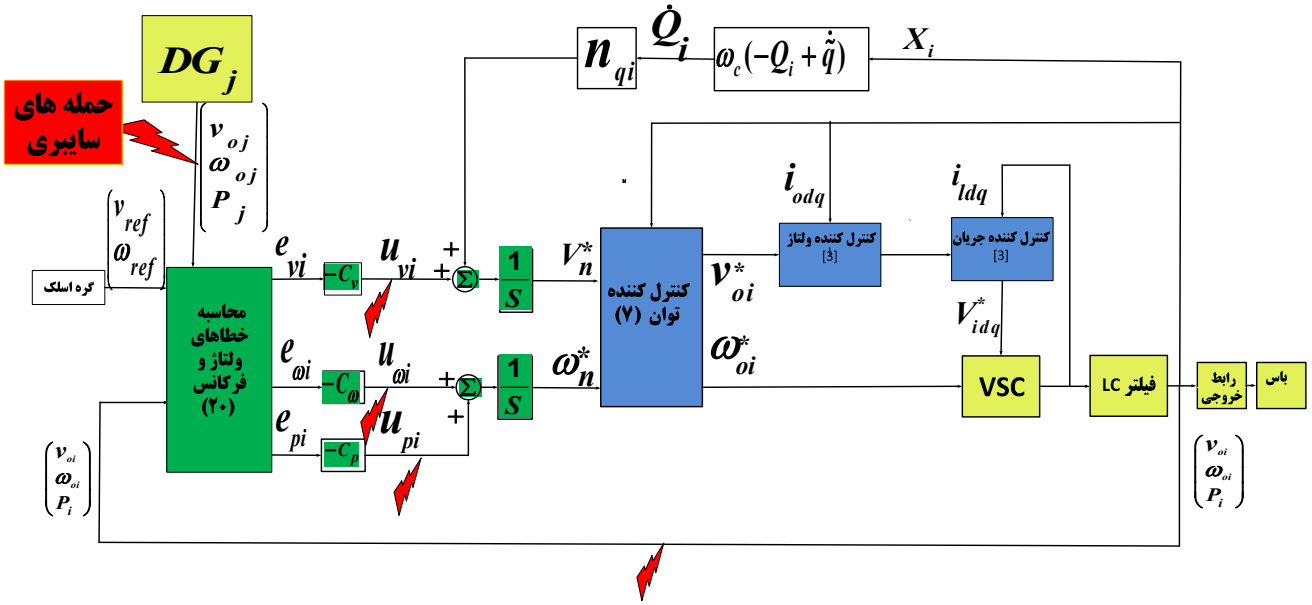
۲- مدل منابع تولید پراکنده و لینک‌های ارتباطی

مدل استفاده‌شده در این مقاله به‌صورت مدل ۱۳حالته (۱) در نظر گرفته شده که مدلی غیرخطی است و به‌طور کامل همه جزئیات را در بر می‌گیرد. جزئیات کامل این مدل در [۶] بررسی شده است

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

1. Blockchain

2. Resilience Indices



شکل ۱: ریزشبکه به همراه حمله‌های سایبری.

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} به‌ترتیب مقادیر جریان و ولتاژ خروجی و جریان بار هستند. مقادیر ورودی کنترلی و خروجی $u_i = (V_{ni}^* \ \omega_{ni}^*)^T$ و $y_i = (v_{odi} \ \omega_{odi})^T$ هستند.

برای تحلیل ریزشبکه و پایداری و همگام‌سازی در این مقاله از تئوری گراف[1] استفاده شده است. برای سیستم‌های چندعامله، چند قانون اصلی (قوانین رینولد[2]) 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 به‌طور کامل قابل پیاده‌سازی است. در این حالت هر منبع تولید پراکنده به‌صورت یک عامل[3] با (۱) در نظر گرفته می‌شود و سیستم مخابراتی با استفاده از گراف مستقیم[4] تئوری گراف مدل می‌گردد. از ماتریس مجاورتی برای نشان‌دادن ارتباطات و همچنین در مباحث پایداری و تابع لیاپانوف استفاده می‌شود [۳۲]. در این مقاله فرض گردیده که توپولوژی ثابت و درخت ریشه‌دار پیوسته[5] بوده و به‌صورت $G(V,E,A_G)$ نشان داده می‌شود. گراف به‌صورت (۲) است

$$G = (V(G), E(G)) \qquad (۲)$$

$V(G) = \{v_1, v_2, \ldots, v_N\}$، $E(G) \subset V(G) \times V(G)$ و $A_G \subset R \times R$ به‌ترتیب گره‌ها (منابع تولید پراکنده)، لینک‌های ارتباطی و ماتریس مجاورتی می‌باشند. درایه‌های ماتریس مجاورتی a_{ij} وزن ضلع‌های گراف است که اگر گراف iام به گراف j ام اطلاعات بدهد یک و در غیر این صورت صفر است. محل اتصال گره‌ها به هم به شکل $(v_j, v_i) \subset E(G)$ است. ماتریس G را غیرمستقیم[6] در نظر می‌گیرند اگر

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

برای تحلیل پایداری ماتریس Δ و لاپلاسین L تعریف می‌شوند

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

۳- روش کنترلی طراحی‌شده

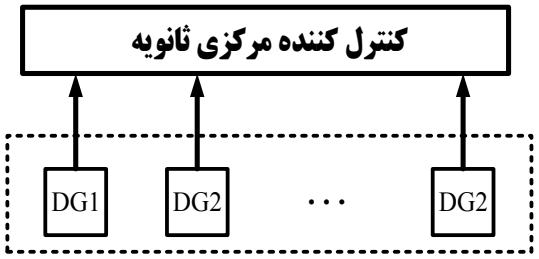
در این مقاله از کنترل‌کننده توزیع‌شده اشتراکی ریزشبکه در دو سطح (کنترل‌کننده اولیه و ثانویه) استفاده گردیده و شکل کلی منابع تولید پراکنده و کنترل‌کننده اولیه و ثانویه استفاده‌شده در شکل ۱ آمده است. با توجه به شکل V_{ni}^* و ω_i^* باید توسط کنترل‌کننده ثانویه بازنشانی گردند تا انحراف کمتری در ورودی کنترل‌کننده اولیه ایجاد شود.

چند هدف اصلی برای کنترل، همگام‌سازی فرکانس و ولتاژ خروجی و تقسیم توان مناسب توان DGهاست؛ البته شروط همگام‌سازی فرکانس و ولتاژ مهم‌تر است. طراحی کنترل‌کننده باید به‌نحوی باشد که همه حالت‌ها به مقدار توافقی یا مقدار مرجع برسند و همگام‌سازی به‌درستی انجام شود. این شرط اصلی‌ترین شرط برای برقراری قوانین رینولد است.

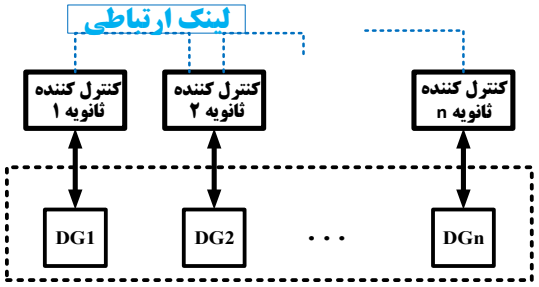
۳-۱ کنترل‌کننده اولیه

کنترل‌کننده اولیه بیشتر برای تقسیم توان بین واحدهای مختلف منابع تولید پراکنده استفاده می‌گردد و به‌صورت داخلی و اغلب دروپ[7] است. مزیت اصلی دروپ این است که امکان اختلال از بیرون وجود ندارد و پایداری سیستم را تأمین می‌کند. مشکل اصلی دروپ، انحراف مقادیر خروجی از مرجع است که برای رفع این مشکل از کنترل‌کننده ثانویه استفاده می‌شود. کنترل‌کننده‌های جریان، ولتاژ و توان به‌صورت اولیه در نظر گرفته می‌شوند که در [۳۳] توضیح داده شده است. لازم به ذکر است دروپ ولتاژ و فرکانس تا اندازه زیادی مجزا بوده و طراحی کنترل‌کننده دروپ ولتاژ و فرکانس، جداگانه انجام می‌شود. خروجی کنترل‌کننده ثانویه $((V_{ni}^* \ \omega_{ni}^*)^T)$ و خروجی DG_i $((V_{oi} \ \omega_{oi})^T)$ به‌عنوان ورودی کنترل‌کننده اولیه است.

1. Graph Theory
2. Reynold
3. Agent
4. Direct Graph
5. Spinning Tree
6. Indirected
7. Droop Controller



شکل ۲: کنترل‌کننده ثانویه متمرکز.



شکل ۴: کنترل‌کننده ثانویه توزیع‌شده.

در کنترل‌کننده توان ابتدا با استفاده از خروجی‌های منابع تولید پراکنده، توان لحظه‌ای از (۵) به‌دست می‌آید و با عبور این توان از یک فیلتر پایین‌گذر با (۶)، توان متوسط به‌صورت $(P\ \ Q)^T$ حاصل می‌شود

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

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

با صرف نظر از دینامیک‌های سریع سیستم و با درنظرگرفتن مدل سیستم در چارچوب dq[1]، کنترل‌کننده توان در کنترل‌کننده اولیه (۷) در نظر گرفته می‌شود [۶] و [۷]

$$\begin{cases} v_{oi}^* = V_{ni}^* - n_{qi} Q_i \\ \omega_{oi}^* = \omega_{ni}^* - m_{pi} P_i \\ v_{odi}^* = V_{ni}^* - n_{qi} Q_i \\ v_{oqi}^* = 0 \end{cases} \quad (۷)$$

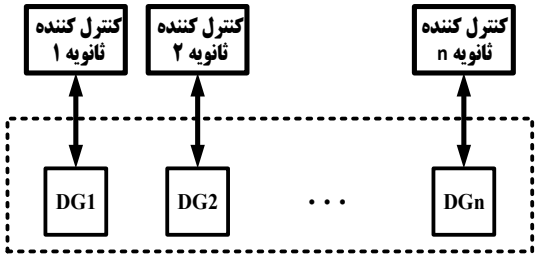
سپس با توجه به (۷)، خروجی کنترل‌کننده توان به‌دست می‌آید و خروجی v_o^* به کنترل‌کننده ولتاژ و ω_o^* به VSC داده می‌شود. در این معادله n_{qi} و m_{pi} ضرایب دروپ و V_{ni}^* و ω_{ni}^* مقدارهای مرجع کنترل‌کننده اولیه هستند.

در کنترل‌کننده ولتاژ و جریان از کنترل‌کننده PI استفاده شده است. کنترل‌کننده ولتاژ، مرجع جریان‌ها را مشخص می‌نماید و خروجی آن به‌عنوان ورودی‌های مرجع وارد کنترل‌کننده جریان می‌شوند.

۳-۲ کنترل‌کننده ثانویه

در شکل ۱ طرح کلی کنترل‌کننده ثانویه آمده و برای مشخص‌کردن مرجع در کنترل‌کننده ثانویه، معمولاً از میانگین[2] مقادیر خروجی ولتاژ و

1. Direct-Quadratic
2. Averaging Consensus



شکل ۳: کنترل‌کننده ثانویه غیرمتمرکز.

فرکانس منابع تولید پراکنده و یا مقدار مرجع توافقی[3] استفاده می‌گردد. در این مقاله، کنترل‌کننده ثانویه با استفاده از روش خطی‌سازی فیدبک طراحی شده است. کنترل‌کننده ثانویه به سه طریق می‌تواند در ریزشبکه مورد استفاده قرار گیرد:

۱) ثانویه متمرکز که به‌صورت شکل ۲ است. در این روش، کانال ارتباطی برای گرفتن اطلاعات از همه منابع لازم است. مزیت روش این است که سیستم ارتباطی پیچیده‌ای نیاز ندارد؛ ولی مشکل اصلی آن است که همگام‌سازی به‌درستی انجام نمی‌گردد و همچنین اگر یک منبع خراب شود، در عملکرد همه منابع تأثیر دارد.

۲) کنترل‌کننده ثانویه غیرمتمرکز که به‌صورت شکل ۳ است. مشکل اصلی این روش آن است همگام‌سازی به‌درستی انجام نمی‌گردد.

۳) کنترل‌کننده ثانویه توزیع‌شده که به‌صورت شکل ۴ است. در این روش از خروجی منبع تولید پراکنده همسایه برای همگام‌سازی استفاده می‌شود. مشکل اصلی این است که سیستم، ارتباط بهتری لازم دارد و همچنین در این روش محاسبات پیچیده‌تر می‌گردد؛ اما مزیت اصلی‌اش آن است که همگام‌سازی بهتر انجام می‌گردد [۳۴].

سیستم کنترل ثانویه را می‌توان به‌صورت زیر در نظر گرفت

$$\begin{cases} v_{oi}^* = V_{ni}^* - n_{qi} Q_i + \delta_v \\ \omega_{oi}^* = \omega_{ni}^* - m_{pi} P_i + \delta_\omega \end{cases} \quad (۸)$$

در عبارت بالا مقادیر δ_v و δ_ω توسط کنترل‌کننده ثانویه و برای کم‌کردن انحراف مقادیر کنترل‌کننده اولیه استفاده می‌گردد. در این مقاله برای کنترل و همگام‌سازی از کنترل‌کننده توزیع‌شده استفاده شده است. کنترل‌کننده توزیع‌شده به سه نوع مختلف می‌تواند طراحی گردد.

۳-۲-۱ کنترل توزیع‌شده اجماع [۳۵] و [۳۶]

کنترل فرکانس توزیع‌شده بر روی الگوریتم اجماع[4] به‌صورت زیر است

$$\begin{aligned} e_{\omega i} = {} & g_i^f \sum_{j \in N_i} a_{ij} (\omega_{oi} - \omega_{oj}) + g_i (\omega_{oi} - \omega_{ref}) + \\ & g_i^p \sum_{j \in N_i} a_{ij} (m_{Pi} P_i - m_{Pj} P_j) \end{aligned} \quad (۹)$$

برای کنترل ولتاژ نیز به همین ترتیب می‌توان عمل کرد. کنترل ولتاژ توزیع‌شده بر روی الگوریتم اجماع به‌صورت زیر است

$$\begin{aligned} e_{vi} = {} & g_i^f \sum_{j \in N_i} a_{ij} (v_{oi} - v_{oj}) + g_i (v_{oi} - v_{ref}) + \\ & g_i^p \sum_{j \in N_i} a_{ij} (n_{Qi} Q_i - n_{Qj} Q_j) \end{aligned} \quad (۱۰)$$

در عبارت بالا g_i^p و g_i^f بهره فیدبک مثبت[5] است.

3. Reference Consensus
4. Consensus-Based Distributed Secondary Control
5. Positive Feedback Gains

۳-۲-۲ کنترل توزیع‌شده بر پایه میانگین [۳۷]

کنترل فرکانس توزیع‌شده روی الگوریتم میانگین[1] به‌صورت زیر است

$$e_{\omega i} = g_i^f(\omega_{oi} - \overline{\omega}) + g_i^p(m_{Pi}P_i - \overline{nP}) \quad (۱۱)$$

در عبارت بالا مقادیر $\overline{mP}$ و $\overline{\omega}$ مقادیر میانگین هستند که به‌صورت (۱۴) به‌دست می‌آیند. خصوصیت این روش آن است که با تعریف مرجع توان از آن در کنترل سیستم استفاده می‌گردد. این مسئله باعث می‌شود که خصوصیات دیگری نیز در سیستم مورد استفاده قرار گیرند

$$\begin{aligned} \overline{\omega} &= \frac{1}{N}\sum_{j\varepsilon N}\omega_j \\ \overline{mP} &= \frac{1}{N}\sum_{j\varepsilon N} m_{Pj}P_j \end{aligned} \quad (۱۲)$$

برای کنترل ولتاژ نیز به همین ترتیب می‌توان عمل کرد. کنترل ولتاژ توزیع‌شده بر روی الگوریتم میانگین به‌صورت (۱۶) است

$$e_{vi} = g_i^f(v_{oi} - \overline{v}) + g_i^p(n_{Qi}Q_i - \overline{nQ}) \quad (۱۳)$$

در عبارت بالا مقادیر $\overline{nQ}$ و $\overline{v}$ مقادیر میانگین هستند که به‌صورت (۱۴) به‌دست می‌آیند

$$\begin{aligned} \overline{v} &= \frac{1}{N}\sum_{j\varepsilon N} v_j \\ \overline{nQ} &= \frac{1}{N}\sum_{j\varepsilon N} n_{Qj}Q_j \end{aligned} \quad (۱۴)$$

۳-۲-۳ روش کنترل فرکانس ثانویه زمان محدود قوی توزیع‌شده

کنترل فرکانس توزیع‌شده روی الگوریتم زمان محدود قوی توزیع‌شده[2] به‌صورت (۱۵) است

$$\begin{aligned} e_{\omega i} = {} & C_\omega \sum_{j\varepsilon N_i} sig(\omega_{oi} - \omega_{oj})^{a_\omega} + g_i sig(\omega_{oi} - \omega_{ref})^{a_\omega} + \\ & C_\omega \sum_{j\varepsilon N_i} sig(m_{Pi}P_i - m_{Pj}P_j)^{a_\omega} \end{aligned} \quad (۱۵)$$

برای کنترل ولتاژ نیز به همین ترتیب می‌توان عمل کرد. کنترل فرکانس توزیع‌شده بر روی الگوریتم زمان محدود قوی توزیع‌شده به‌صورت (۱۶) است

$$\begin{aligned} e_{vi} = {} & C_v \sum_{j\varepsilon N_i} sig(v_{oi} - v_{oj})^{a_v} + g_i sig(v_{oi} - v_{ref})^{a_v} + \\ & C_v \sum_{j\varepsilon N_i} sig(n_{Qi}Q_i - n_{Qj}Q_j)^{a_v} \end{aligned} \quad (۱۶)$$

که a_v، C_v، a_ω و C_ω پارامترهای کنترلی فرکانس و ولتاژ هستند

$$sig(x)^a = |x|^a \operatorname{sgn}(x) \quad (۱۷)$$

در این مقاله از روش اول کنترلی استفاده گردیده و $g_i^p = ۱$ و $g_i^f = ۱$ در نظر گرفته شده است. هدف اصلی در طراحی این کنترل‌کننده، اعمال ورودی کنترلی مناسب $(V_{ni}^* \;\; \omega_{ni}^*)^T$ به کنترل‌کننده اولیه برای پایداری و همگام‌سازی سیستم است. با استفاده از روش خطی‌سازی فیدبک از (۷) مشتق گرفته می‌شود و برابر با ورودی کنترلی در نظر گرفته می‌شود. ورودی کنترلی به‌نحوی طراحی می‌گردد که خطا به سمت صفر میل کند و بنابراین نتیجه به‌صورت (۱۸) درمی‌آید [۷]

$$\begin{cases} \dot{v}_{odi}^* = \dot{V}_{ni}^* - n_{qi}\dot{Q}_i = u_{vi} \\ \dot{\omega}_{oi}^* = \dot{\omega}_{ni}^* - m_{pi}\dot{P}_i = u_{\omega i} \end{cases} \quad (۱۸)$$

در معادله بالا u_{vi} و $u_{\omega i}$ به‌ترتیب سیگنال کنترلی کمکی ولتاژ و جریان در روش خطی‌سازی فیدبک سیستم‌های چندعامله هستند. به‌منظور پایداری‌سازی سیستم و با توجه به اینکه سیستم به‌صورت چندعامله در نظر گرفته شده است، ورودی کنترلی به‌صورت (۱۹) با استفاده از خطاهای دنبال‌سازی در نظر گرفته می‌شود [۳۱]

$$\begin{cases} u_{vi} = -C_v e_{vi}(t) \\ u_{\omega i}(t) = -C_\omega e_{\omega i}(t) \\ u_{pi} = m_{Pi}\dot{P}_i = -C_P e_{Pi}(t) \end{cases} \quad (۱۹)$$

در این رابطه $e_{vi}(t)$، $e_{\omega i}(t)$ و $e_{Pi}(t)$ به‌ترتیب خطای دنبال‌سازی و C_v، C_ω و C_P بهره کنترلی ولتاژ، فرکانس و توان اکتیو هستند. خطای دنبال‌سازی به‌صورت (۲۰) در سیستم‌های چندعامله می‌باشد که در همگام‌سازی، هدف آن است که این خطاها صفر شوند. این خطاها با استفاده از خروجی DG و همسایه به‌دست می‌آیند

$$\begin{cases} u_{vi} = -C_v e_{vi}(t) = -C_v \sum [a_{ij}(v_{.i}(t) - v_{.j}(t)) + \\ \quad g_i(v_{.i}(t) - v_{ref}) + a_{ij}(n_{Qi}Q_i(t) - n_{Qj}Q_j(t))] \\ u_{\omega i}(t) = -C_\omega e_{\omega i}(t) = -C_\omega \sum_{j\varepsilon N_j} [a_{ij}(\omega_{oi}(t) - \omega_{oj}(t)) + \\ \quad g_i(\omega_{oi}(t) - \omega_{ref}) + a_{ij}(m_{Pi}P_i(t) - m_{Pj}P_j(t))] \end{cases} \quad (۲۰)$$

در (۲۰) $v_{.i}(t)$، $\omega_{oi}(t)$ و P_i و $v_{.j}(t)$، $\omega_{oj}(t)$ و P_j 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 هستند. g_i فقط زمانی برابر یک است که DG به گره اسلک وصل باشد و در غیر این صورت صفر است.

با استفاده از (۷) سیگنال کنترلی از روش خطی‌سازی فیدبک به‌صورت (۲۱) به‌دست می‌آید

$$\begin{cases} V_{ni}^* = \int (u_{vi} + n_{qi}\dot{Q}_i)\mathrm{d}t \\ \omega_{ni}^* = \int (u_{\omega i} + u_{pi})\mathrm{d}t \end{cases} \quad (۲۱)$$

در (۲۱) مقدار $\dot{Q}_i$ به‌صورت زیر تعریف شده است

$$\dot{Q}_i = -\omega_c Q_i + \omega_c(v_{oqi}i_{odi} - v_{odi}i_{oqi}) = -\omega_c Q_i + \omega_c \dot{\tilde{q}} \quad (۲۲)$$

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 [۷] و [۳۸].

٤- حمله سایبری روی کنترل‌کننده ثانویه

سیستم ریزشبکه تحت آسیب‌پذیری از حمله‌های سایبری است. حمله‌های سایبری به سه گروه کلی تقسیم می‌شوند: ۱) حمله منع سرویس (DoS)، ۲) حمله تکرار[3] و ۳) حمله فریب[4]. حمله DoS، در دسترس‌بودن و حمله تکرار و فریب، محرمانه‌بودن و یکپارچگی اطلاعات

1. Average-Based Distributed Secondary Frequency Control
2. Distributed Robust Finite-Time Secondary Frequency Control
3. Reply Attack
4. Deception Attack

سیستم را دچار مشکل می‌کنند. در حمله منع سرویس (DoS) کانال ارتباطی مسدود می‌گردد. در حمله تکرار از خروجی‌های قبلی سیستم استفاده شده و در زمان‌های حمله به‌عنوان خروجی اصلی جایگزین می‌گردند. در حمله فریب به خروجی سیستم پارامتری اضافه می‌گردد و باعث اختلال در خروجی می‌شود [۳۹] و [۴۰]. در کل فرمول همه حملات را می‌توان به‌صورت زیر در نظر گرفت

$$y^c(t)=\alpha(t)y(t)+(1-\alpha(t))g(y(t)) \qquad (۲۳)$$

که y اطلاعات اندازه‌گیری‌شده و y^c اطلاعات دریافت‌شده همان لحظه است. در (۲۴) تا (۲۶) فرمول حمله‌های سایبری DoS، تکرار و فریب به‌ترتیب آمده‌اند

$$\begin{aligned} &y^c \in 0\\ &\alpha(t)=0\\ &g(y(t))=0 \end{aligned} \qquad (۲۴)$$

$$\begin{aligned} &y^c \in Y\\ &\alpha(t)=0\\ &g(y(t))=y^c \end{aligned} \qquad (۲۵)$$

$$\begin{aligned} &y^c = y+y^a\\ &\alpha(t)=0\\ &g(y(t))=y^a \end{aligned} \qquad (۲۶)$$

که y اطلاعات گذشته و y^a اطلاعات تزریق‌شده توسط مهاجم هستند [۴۰].

شکل کلی منابع تولید پراکنده به همراه حمله سایبری و کنترل‌کننده مورد استفاده به‌صورت شکل ۱ در نظر گرفته شده است. با توجه به شکل، حمله DoS ممکن است در کنترل‌کننده ثانویه و یا بین اولیه و ثانویه اتفاق بیفتد. حمله سایبری سنسوری و عملگری و ربودن اطلاعات در کانال ارتباطی و خطای سنسوری و عملگری در گره‌ها اتفاق می‌افتد.

در این بخش، حمله سنسوری و عملگری در کنترل‌کننده ثانویه آمده است و در این حمله، خروجی سنسورها هنگام انتقال مورد حمله قرار می‌گیرند. در بسیاری از مواقع شباهت‌های زیادی بین حمله سایبری و عیب[1] سنسوری وجود دارد و تفاوت اساسی آنها در این است که حمله سایبری به لینک ارتباطی وارد می‌گردد؛ اما خطا به خروجی سنسور اضافه می‌شود [۴۱].

در کنترل‌کننده سلسه‌مراتبی، حمله سنسوری در میان سنسورهای کنترل‌کننده ثانویه و حمله عملگری بین کنترل‌کننده اولیه و ثانویه اتفاق می‌افتد. حمله سایبری سنسوری و عملگری باعث می‌شود که خروجی ولتاژ و فرکانس یک DG به DG همجوار اشتباه برسد و ممکن است باعث ناپایداری سیستم گردد. با توجه به (۲۳) حمله سایبری سنسوری به‌صورت (۲۷) است

$$\begin{aligned} &y^c = y+y^a\\ &\alpha(t)=0\\ &g(y(t))=y+\alpha y^a \end{aligned} \qquad (۲۷)$$

که y_i^c سیگنال مختل‌شده ناشی از حمله عملگری و سنسوری، y سیگنال واقعی و y^a سیگنال حمله عملگر و سنسوری است. در این فرمول $\alpha=0$ بدون حمله و $\alpha_i,\beta_i=1$ با حمله سایبری است.

۴-۱ اثر حمله سایبری سنسوری و عملگری بر کنترل‌کننده ثانویه

بررسی اثر حمله سایبری سنسوری و عملگری می‌تواند در کنترل‌کننده‌های ثانویه مختلف انجام پذیرد. در این مقاله، اثر حمله در (۲۰) مورد بررسی قرار گرفته است. اثر این حمله بر کنترل‌کننده ثانویه به‌صورت زیر است

$$\begin{aligned} u_{v_i}^c &= -C_v e_{vi}^c = -C_v\sum[a_{ij}(v_{oi}-v_{oj}^c)+g_i(v_{oi}-v_{ref})+\\ &\quad a_{ij}(n_{Qi}Q_i-n_{Qj}Q_j^c)] \end{aligned} \qquad (۲۸)$$

با استفاده از رابطه ریاضی حمله سنسوری در (۲۷)، رابطه بالا مجدداً بازنویسی می‌شود. اثر حمله سنسوری و عملگری در کنترل‌کننده ثانویه به‌صورت زیر است

$$\begin{aligned} &u_{v_i}^{cc} = u_{vi}^c+\alpha_i' u_{vi}^a = u_{vi}+f_{iv}^s\\ &f_{iv}^s = C_v\sum a_{ij}\alpha_i(v_{oi}^a+n_{Qj}Q_j^a(t))+\alpha_i' u_{v_i}^a \end{aligned} \qquad (۲۹)$$

بنابراین سیگنال ورودی کنترل‌کننده اولیه برابر است با

$$V_{ni}^* = \int(u_{vi}^c+n_{Q_i}\dot{Q}_i)\mathrm{d}t=\int(u_{vi}+f_{iv}^s+n_{Q_i}\dot{Q}_i)\mathrm{d}t \qquad (۳۰)$$

و به همین ترتیب برای کنترل‌کننده فرکانس با حمله سایبری به‌صورت (۳۱) بازنویسی می‌گردد

$$\omega_{ni}^* = \int(u_{\omega i}^c+m_{Pi}\dot{P}_i)\mathrm{d}t=\int(u_{\omega_i}^c+u_{P_i}^c)\mathrm{d}t \qquad (۳۱)$$

اگر حمله به عملگر و سنسور در فرکانس اتفاق بیفتد، به‌صورت (۳۲) نشان داده می‌شود

$$\begin{aligned} u_{\omega_i}^c &= -C_\omega e_{\omega i}^c = -C_\omega\sum[a_{ij}(\omega_{oi}-\omega_{oj}^c)+g_i(\omega_{oi}-\omega_{ref})\\ &\quad +a_{ij}(m_{pi}P_i(t)-m_{pj}P_j^c(t))] \end{aligned} \qquad (۳۲)$$

حمله سنسوری مقادیر توان، ولتاژ و فرکانس به‌صورت (۳۳) است

$$\begin{aligned} &u_{P_i}^{cc} = u_{Pi}^c+\alpha_i' u_{Pi}^a\\ &u_{\omega i}^{cc} = u_{\omega i}^c+\alpha_i' u_{\omega i}^a\\ &P_j^c = P_j+\alpha_i P_i^a\\ &\omega_{oj}^c = \omega_{oj}+\alpha_i\omega_{oi}^a \end{aligned} \qquad (۳۳)$$

که $u_{\omega i}^{cc}$، $u_{\omega i}^c$ و $u_{\omega i}^a$ به‌ترتیب سیگنال کنترلی فرکانس مختل‌شده، سیگنال کنترلی با حمله سنسوری و سیگنال حمله عملگری است و به همین ترتیب برای فرکانس و توان، سیگنال کنترلی برای حمله سنسوری به‌صورت زیر است

$$\begin{cases} u_{\omega i}^c = u_{\omega_i}^s+\alpha' u_{\omega_i}^a = u_{\omega_i}+f_{i\omega}^s\\ f_{i\omega}^s = C_{i\omega}\sum a_{ij}\alpha(\omega_{oj}^a+m_{pj}P_j^a(t))+\alpha' u_{\omega_i}^a\\ u_{Pi}^c = u_{Pi}^s+\alpha' u_{Pi}^a = u_{Pi}+f_{iP}\\ f_{iP}^s = C_P\sum a_{ij}m_{Pj}\alpha P_j^a+\alpha' u_{Pi}^a \end{cases} \qquad (۳۴)$$

بنابراین سیگنال کنترلی فرکانس با حمله سنسوری و عملگری برابر است با

$$\omega_{ni}^* = \int(u_{\omega i}^c+u_{Pi}^c)\mathrm{d}t=\int(u_{\omega i}+f_{i\omega}^s+u_{Pi}+f_{iP}^s)\mathrm{d}t \qquad (۳۵)$$

فرض: خطا در این حالت محدود است و هر حمله سنسوری رابطه زیر را برآورده می‌کند

1. Fault

$$\begin{aligned}&\left|f_{i\omega}^{s}\right|<\bar{\kappa}_{\omega}\\&\left|f_{iv}^{s}\right|<\bar{\kappa}_{v}\\&\left|f_{iP}^{s}\right|<\bar{\kappa}_{P}\end{aligned}\qquad(۳۶)$$

در عبارت بالا مقادیر $\bar{\kappa}_{\omega}$، $\bar{\kappa}_{v}$ و $\bar{\kappa}_{P}$ حداکثر مقدار خطاهای سنسوری و ثابت و مثبت هستند.

٤-۲ اثر حمله سایبری ربودن اطلاعات بر کنترل‌کننده ثانویه

در حمله سایبری ربودن اطلاعات، خروجی سیستم حذف و مقدار حمله جایگزین آن می‌گردد. اثر حمله سایبری ربودن اطلاعات به‌صورت (۳۷) نشان داده شده است

$$x^{c}(t)=(1-\alpha)x(t)+\alpha x^{a}(t)\qquad(۳۷)$$

که $\alpha=0$ بدون حمله و $\alpha=1$ با حمله سایبری ربودن اطلاعات است. در فرمول بالا $x^{c}(t)$، $x(t)$ و $x^{a}(t)$ به‌ترتیب سیگنال مختل‌شده، سیگنال بدون حمله و سیگنال حمله است [۴۲]. به‌منظور کنترل ریزشبکه ابتدا به فرمول‌بندی مسئله پرداخته می‌شود.

با استفاده از جایگذاری (۳۷) در سیگنال کنترلی می‌توان سیگنال خطا و کنترلی DG را به‌صورت زیر در نظر گرفت

$$\begin{aligned}u_{vi}^{c}&=u_{vi}+f_{iv}^{H}=-C_{v}\sum[a_{ij}(v_{oi}-v_{oj}^{c})+g_{i}(v_{oi}-v_{ref})\\&\quad+a_{ij}(n_{Qi}Q_{i}(t)-n_{Qj}Q_{j}^{c}(t))\\f_{iv}^{H}&=-C_{v}\sum a_{ij}\alpha(v_{oj}-v_{oj}^{a}+n_{Qj}Q_{j}-n_{Qj}Q_{j}^{a})\end{aligned}\qquad(۳۸)$$

بنابراین سیگنال کنترلی با حمله سایبری ربودن اطلاعات به‌صورت (۳۹) به‌دست می‌آید

$$V_{ni}^{*}=\int(u_{vi}^{c}+n_{Qi}\dot{Q}_{i})\mathrm{d}t\qquad(۳۹)$$

کنترل‌کننده فرکانس نیز مانند ولتاژ به‌صورت زیر طراحی می‌گردد

$$\begin{aligned}u_{\omega i}^{c}&=u_{\omega i}+f_{i\omega}^{H}=-C_{\omega}\sum[a_{ij}(\omega_{oi}-\omega_{oj}^{c})+\\&\quad g_{i}(\omega_{oi}-\omega_{ref})+m_{Pi}P_{i}(t)-m_{Pj}P_{j}^{c}(t)]\\f_{i\omega}^{H}&=-C_{\omega}\sum a_{ij}\alpha(\omega_{oj}-\omega_{oj}^{a}+m_{Pj}P_{j}-m_{Pj}P_{j}^{a})\end{aligned}\qquad(۴۰)$$

همچنین سیگنال کنترلی توان را نیز می‌توان محاسبه نمود

$$\begin{aligned}u_{Pi}^{c}&=u_{Pi}+f_{iP}^{H}=-C_{P}\sum a_{ij}(m_{Pi}P_{i}-m_{Pj}P_{j}^{c})\\f_{iP}^{H}&=-C_{P}\sum a_{ij}\alpha m_{Pj}(P_{j}-P_{j}^{a})\end{aligned}\qquad(۴۱)$$

بنابراین سیگنال کنترلی فرکانس زاویه‌ای به‌صورت (۴۲) به‌دست می‌آید

$$\omega_{ni}^{*}=\int(u_{\omega i}^{c}+u_{Pi}^{c})\mathrm{d}t=\int(u_{\omega i}+f_{i\omega}^{H}+u_{Pi}+f_{iP}^{H})\mathrm{d}t\qquad(۴۲)$$

٤-۳ حمله DoS

مهاجم در حمله سایبری DoS باید کانال ارتباطی را از طریق انسداد انتقال دیتا قطع کند و باعث ازبین‌رفتن اطلاعات شود [۴۳]. حمله سایبری DoS ناشی از قطع سیستم ارتباطی است؛ اما حمله ربودن اطلاعات، سنسوری و ... مقادیر اندازه‌گیری‌شده را خراب می‌کنند. در این حمله نیاز به اطلاعات خروجی سیستم نیست و ارتباط بین عامل‌ها قطع می‌گردد [۴۴] و [۴۵]. در حمله DoS $\psi_{s}^{ij}=[t_{s}^{ij},t_{s}^{ij}+\tau_{s}^{ij}]$ در نظر گرفته می‌شود. در این عبارت t_{s}^{ij} زمان شروع حمله sام با بازه زمانی τ_{s}^{ij} بین دو DG_{i} و DG_{j} و در این صورت مجموع زمانی حمله (Ξ_{D}^{ij}) به‌صورت (۴۳) است

$$\Xi_{D}^{ij}(t_{1},t_{2})=\bigcup_{s=1}^{\infty}\psi_{s}^{ij}\cap(t_{1},t_{2})\qquad(۴۳)$$

در زمان حمله ماتریس همجواری به‌صورت (۴۴) تغییر می‌کند و در واقع به زمان وابسته می‌شوند

$$a_{ij}=\begin{cases}0 & ,\ t\in\Xi_{D}^{ij}(t_{1},t_{2})\\a_{ij} & ,\ \text{otherwise}\end{cases}\qquad(۴۴)$$

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 قطع لینک ارتباطی شده و تعدادی از گره‌ها را مجزا یا یک گره را کلاً از دسترس خارج کند. مقادیر گره‌ها در صورت حمله سایبری DoS به‌صورت (۴۵) است

$$\begin{cases}x^{c}(t)=\theta^{x}(t)x(t)\\u^{c}(t)=\theta^{u}(t)u(t)\end{cases}\qquad(۴۵)$$

که در آن $\theta^{c}(t)$ و $\theta^{x}(t)$ ماتریس‌های قطری هستند که به‌ترتیب برای مشخص‌شدن حمله DoS به حالت‌ها و ورودی کنترلی تعریف شده‌اند. مقادیر $x^{c}(t)$، $u^{c}(t)$، $x(t)$ و $u(t)$ به‌ترتیب مقادیر حالت و ورودی کنترل‌کننده با وجود حمله و بدون حمله هستند. در سیستم بدون حمله سایبری DoS، ضرایب $\theta^{x}(t)$ و $\theta^{u}(t)$ برابر یک و با وجود حمله، صفر هستند. با توجه به ایده بالا، ورودی کنترلی و مقادیر سنسوری با وجود حمله سایبری DoS به‌صورت زیر به‌دست می‌آیند [۳]

$$\begin{cases}u_{vi}^{c}=\theta_{iv}^{u}(t)u_{vi}\\u_{\omega i}^{c}=\theta_{i\omega}^{u}(t)u_{\omega i}\\u_{Pi}^{c}=\theta_{iP}^{u}u_{Pi}\end{cases}\qquad\begin{cases}\omega_{oj}^{c}=\theta_{j\omega}^{x}\omega_{oj}(t)\\v_{oj}^{c}=\theta_{jv}^{x}(t)v_{oj}(t)\\P_{j}^{c}=\theta_{jP}^{x}P_{j}\end{cases}\qquad(۴۶)$$

که $\theta_{jP}^{x}(t)$، $\theta_{j\omega}^{x}(t)$ و $\theta_{jv}^{x}(t)$ به‌ترتیب ضرایب حمله DoS به سنسور فرکانس، ولتاژ و توان اکتیو و $\theta_{iP}^{u}(t)$، $\theta_{i\omega}^{u}(t)$ و $\theta_{iv}^{u}(t)$ ضرایب حمله به عملگر فرکانس، ولتاژ و توان هستند. در این مقاله حمله DoS در سنسور در نظر گرفته شده و از حملات DoS در کنترل‌کننده‌ها صرف نظر گردیده است $(\theta_{i\omega}^{u}=\theta_{iP}^{u}=\theta_{iv}^{u}=1)$. با جایگذاری (۴۶) در سیگنال، ورودی کنترلی به‌صورت زیر به‌دست می‌آید

$$\begin{cases}u_{vi}^{c}=u_{vi}+f_{iv}^{D}=-C_{v}\sum[a_{ij}(v_{oi}-v_{oj}^{c})+g_{i}(v_{oi}-v_{ref})\\\quad+a_{ij}(n_{Qi}Q_{i}(t)-n_{Qj}Q_{j}^{c}(t))]\\f_{iv}^{D}=-C_{v}\sum a_{ij}[(1-\theta_{jv}^{x})v_{oj}+n_{Qj}(1-\theta_{jQ}^{x})Q_{j}\end{cases}\qquad(۴۷)$$

بنابراین سیگنال کنترلی ولتاژ با جایگذاری در (۲۱) به‌صورت زیر به‌دست می‌آید

$$V_{ni}^{*}=\int[u_{vi}^{c}+n_{Q_{i}}\dot{Q}_{i}]\mathrm{d}t\qquad(۴۸)$$

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

$$\begin{aligned}u_{\omega i}^{c}&=u_{\omega i}+f_{i\omega}^{D}=-C_{\omega}\sum a_{ij}[(\omega_{oi}-\omega_{oj}^{c})+\\&\quad g_{i}(\omega_{oi}-\omega_{ref})+m_{Pi}P_{i}(t)-m_{Pj}P_{j}^{c}(t)]\\f_{i\omega}^{D}&=-C_{\omega}\sum a_{ij}[(1-\theta_{j\omega}^{x})v_{oj}+m_{Pj}(1-\theta_{jP}^{x})P_{j}]\end{aligned}\qquad(۴۹)$$

با جایگذاری مقادیر (۴۷) در (۴۸) و (۴۹) ورودی کنترلی به‌دست می‌آید

$$\omega_{ni}^{*}=\int(u_{\omega i}^{c}+u_{Pi}^{c})\mathrm{d}t \qquad (۵۰)$$

٤-٤ کارایی و آسیب‌پذیری کنترل‌کننده ثانویه

تاب‌آوری، پارامتری است که نشان می‌دهد سیستم در مقابل یک اختلال چقدر مقاومت دارد. تاب‌آوری با مفهوم کاهش عملکرد[1] به‌صورت (۵۱) ارتباط معکوس دارد

$$RI(Resilience\ Indices)=\frac{1}{Loss} \qquad (۵۱)$$

کاهش عملکرد می‌تواند با مفاهیم مختلفی تعریف شود. در ادامه سه تعریف اصلی بیان می‌گردد.

۱) تعریف ساده

$$Loss=\frac{x_{\cdot}-x(t)}{x(t)} \qquad (۵۲)$$

که $x(t)$ مقدار تابع در زمان t و $x_{\cdot}$ مقدار نامی تابع است.

۲) کاهش عملکرد همچنین می‌تواند با ادغام انحراف نسبی در طول مدت کاهش عملکرد محاسبه شود. در این حالت تأثیرات رویداد شدید بر عملکرد سیستم را از منظری جامع‌تر نشان می‌دهد و نه‌تنها میزان استحکام و پاسخگویی به اختلالات، بلکه سرعت بازیابی را نیز نشان می‌دهد

$$Loss=\int_{t_1}^{t_2}\frac{x_{\cdot}-x(t)}{x(t)}\mathrm{d}t \qquad (۵۳)$$

۳) برای بازیابی سریع می‌توان از عبارت زیر نیز استفاده کرد

$$Loss=\frac{1}{t_2-t_1}\int_{t_1}^{t_2}\frac{x_{\cdot}-x(t)}{x(t)}\mathrm{d}t \qquad (۵۴)$$

کاهش عملکرد از صفر تا بی‌نهایت تغییر می‌کند [۴۶]. به‌منظور بررسی آسیب‌پذیری کنترل‌کننده ثانویه ناشی از حمله‌های سایبری از مقایسه شاخص تاب‌آوری استفاده می‌شود. در این مقاله از تعریف سوم استفاده شده است.

۵- اثبات پایداری

اثبات پایداری برای حمله به لینک مخابراتی و گره به‌صورت جداگانه انجام می‌گردد. در این مقاله فرض شده که درخت پیوسته می‌ماند و ارتباط بین DGهای مختلف طبق ماتریس مجاورت حفظ می‌شود. خطای سیستم (e_{vi}) و بردار مغایرت[2] (δ) به‌صورت (۴۱) تعریف شده‌اند

$$\begin{aligned}&\delta=v_{od}-v_{ref}\\&e_{vi}=(L+G)(v_{odi}-v_{ref})\end{aligned} \qquad (۵۵)$$

با فرض حمله سایبری، سیگنال کنترلی با وجود حمله و بر اساس سیگنال خطا به‌صورت (۵۶) به‌دست می‌آید

$$u_{v}^{c}=-C_{v}e_{v}^{c}=-C_{v}(L+G)(v_{odi}^{c}-v_{ref}) \qquad (۵۶)$$

در فرمول بالا u_{v}^{c}، e_{v}^{c} و v_{odi}^{c} به‌ترتیب سیگنال کنترلی، خطا و مقدار خروجی ولتاژ DG با وجود حمله سایبری است. با فرض حمله سایبری در کانال ارتباطی، سیگنال کنترلی با وجود حمله بر اساس سیگنال خطا به‌صورت (۵۷) به‌دست می‌آید. در این مقاله حمله سایبری در کنترل ثانویه و برای انتقال خروجی سنسورها در نظر گرفته شده است. با درنظرگرفتن (۱۹) و (۲۰) روابط زیر به‌دست می‌آیند

$$\begin{aligned}&u_{vi}^{c}=-C_{v}e_{vi}^{c}\\&e_{vi}^{c}=\sum a_{ij}(v_{\cdot i}(t)-v_{\cdot j}^{c}(t))+g_{i}(v_{\cdot i}(t)-v_{ref})+\\&\quad a_{ij}(n_{Qi}Q_{i}(t)-n_{Qj}Q_{j}^{c}(t))\end{aligned} \qquad (۵۷)$$

برای اثبات پایداری رابطه بالا، لم ۱ و ۲ و قضیه در ادامه در نظر گرفته شده است. در [۴۷] و [۴۸] توضیحات جامعی در رابطه با لم ۱ و ۲ برای همگام‌سازی سیستم‌ها آمده است.

لم ۱: فرض کنید گراف G یک درخت پیوسته است و حداقل در یک گره ریشه $g_i\neq 0$ داشته باشد؛ بنابراین

$$\sigma_{\min}(L+G)\|\delta\|\le\|e\|\Rightarrow\|\delta\|\le\frac{\|e\|}{\sigma_{\min}(L+G)} \qquad (۵۸)$$

که $\sigma_{\min}$ مقدار تکین مینیمم ماتریس $L+G$ است. در این صورت e برابر صفر است اگر و فقط اگر همه گره‌ها همگام باشند. به این ترتیب اصلی‌ترین شرایط برای برقراری قوانین رینولد برقرار می‌گردد [۴۷].

لم ۲: فرض کنید گراف مستقیم G یک درخت پیوسته و برای حداقل یکی از گره‌های ریشه $g_i\neq 0$ است. ماتریس $D+G$ را در نظر بگیرید. 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 [۴۸].

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

قضیه ۱: فرض کنید که G یک درخت پیوسته و حداقل برای یکی از DGها $g_i\neq 0$ باشد. اگر ورودی کنترلی ثانویه u_{vi}^{c} با حمله سایبری به‌صورت $u_{vi}^{c}=-C_{v}e_{vi}^{c}$ باشد، خطای e_{vi}^{c} در $e_{vi}^{c}=(L+G)\delta^{c}$ پایدار مجانبی است و همچنین ولتاژ خروجی DGها به v_{ref} همگام می‌شوند.

با وجود حملات سایبری خطا به‌صورت (۵۹) است

$$e_{v}^{c}=e_{v}+e_{v}^{a} \qquad (۵۹)$$

در (۵۹) e_{v}^{a}، e_{v} و e_{v}^{c} به‌ترتیب خطای ناشی از حمله، خطای ذاتی سیستم و مجموع خطاهاست.

اثبات: با توجه به اینکه $u_{v}^{c}=[u_{v1}^{c}\ u_{v2}^{c}\ \dots\ u_{vn}^{c}]^{T}=-C_{v}e_{v}^{c}$ می‌باشد، برای اثبات پایداری، تابع کاندیدای لیاپانوف به‌صورت رابطه زیر در نظر گرفته می‌شود

$$\begin{aligned}&V=V_1+V_2\\&V_1=\frac{1}{2}(e_{v})^{T}(D+G)e_{v}\\&V_2=\frac{1}{2}(e_{v}^{a})^{T}(D+G)e_{v}^{a}\end{aligned} \qquad (۶۰)$$

برای اثبات پایداری از تابع لیاپانوف مشتق گرفته می‌شود

$$\begin{aligned}&\dot{V}=\dot{V}_1+\dot{V}_2\\&\dot{V}_1=(e_{v})^{T}(D+G)\dot{e}_{v}\\&\dot{V}_2=(e_{v}^{a})^{T}(D+G)\dot{e}_{v}^{a}\end{aligned} \qquad (۶۱)$$

1. Loss
2. Disagreement

$$\begin{cases} e_v = (L+G)\delta = (L+G)(v_{od} - v_{ref}) \\ e_v^a = (L+G)\delta^a = (L+G)(v_{od}^a - v_{ref}) \end{cases}$$
$$\begin{cases} \dot{e}_v = (L+G)\dot{\delta} = (L+G)\dot{v}_{od} = (L+G)(-C_v e_v) \\ \dot{e}_v^a = (L+G)\dot{\delta}^a = (L+G)\dot{v}_{od}^a = (L+G)(-C_v e_v^a) \end{cases} \quad (۶۲)$$

بنابراین مشتق توابع لیاپانوف به‌صورت زیر بازنویسی می‌گردد

$$\dot{V}_1 = -C_v (e_v)^T (D+G)(L+G)(e_v)$$
$$\dot{V}_2 = -C_v (e_v^a)^T (D+G)(L+G)(e_v^a) \quad (۶۳)$$

در معادله بالا $X = (D+G)(L+G)$ در نظر گرفته می‌شود. هر ماتریس مربعی را می‌توان به‌صورت زیر نوشت

$$X = \frac{1}{2}[X + X^T] + \frac{1}{2}[X - X^T] \quad (۶۴)$$

برای دو عبارت بالا

$$e_v \frac{X - X^T}{2} e_v = 0$$
$$e_v^a \frac{X - X^T}{2} e_v^a = 0 \quad (۶۵)$$

است و بنابراین

$$\dot{V} = -\frac{C_v}{2} e_v^T (X + X^T) e_v - \frac{C_v}{2} (e_v^a)^T (X + X^T) e_v^a \quad (۶۶)$$

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

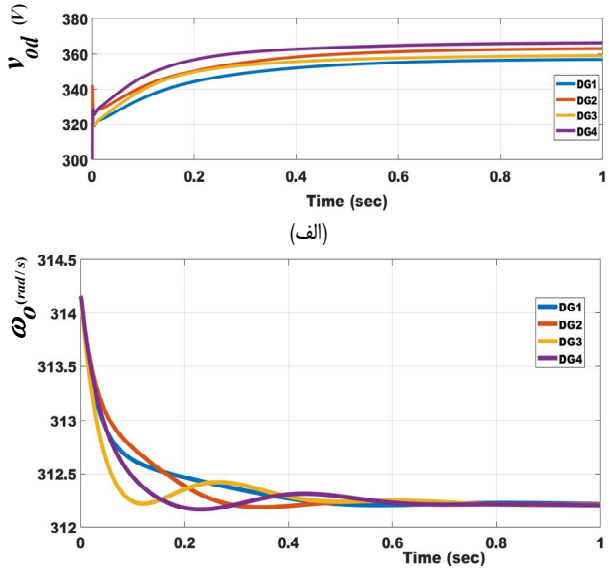
$$\dot{V} = -\frac{C_v}{2} e_v^T Q e_v - \frac{C_v}{2} (e_v^a)^T Q e_v^a < 0 \quad (۶۷)$$

منفی معین است و در نتیجه ریزشبکه با وجود حمله سایبری پایدار مجانبی است.

برای همگام‌سازی باید اثبات شود که خطای حالت ماندگار صفر می‌شود و به عبارتی $\lim_{t\to\infty} e^c \to 0$ و سپس با توجه به لم ۱، بردار δ^c پایدار مجانبی است و ولتاژ خروجی DGها به v_{ref} همگام می‌شوند. با توجه به فرمول زیر

$$\dot{V}_1 = -\frac{C_v}{2} e_v^T Q e_v$$
$$\dot{V}_2 = -\frac{C_v}{2} (e_v^a)^T Q e_v^a$$
$$\dot{V}_1 \le -\frac{C_v}{2} \sigma_{\min} Q \|e_v\|^2 \le -\frac{C_v}{2} \frac{\sigma_{\min}(Q)}{\sigma_{\max}(D)} V_1 =$$
$$-\gamma_1 V_1 \to V_1 \le e_v^{-\gamma_1 t} V_1(t_0)$$
$$\lim_{t\to\infty} e^{-\gamma_1 t} V_1(t_0) \to 0 \to \lim_{t\to\infty} V_1 \to 0 \quad (۶۸)$$
$$\dot{V}_2 \le -\frac{C_v}{2} \sigma_{\min} Q \|e_v^{sa}\|^2 \le -\frac{C_v}{2} \frac{\sigma_{\min}(Q)}{\sigma_{\max}(D)} V_2 =$$
$$-\gamma_2 V_2 \to V_2 \le e_v^{-\gamma_2 t} V_2(t_0)$$
$$\lim_{t\to\infty} e^{-\gamma_2 t} V_2(t_0) \to 0 \to \lim_{t\to\infty} V_2 \to 0$$

و بنابراین $\lim_{t\to\infty} V \to 0 \Rightarrow e_v^c \to 0 \Rightarrow \delta^c \to 0$ و نتیجه می‌شود که همگام‌سازی انجام می‌گردد. همچنین هرچه C_v بزرگ‌تر باشد سرعت همگام‌سازی مناسب‌تر است و بنابراین با انتخاب مناسب C_v و تأثیر آن در u_v^c همگام‌سازی بهینه‌ای انجام می‌پذیرد. □



(الف)

(ب)

شکل ۵: خروجی ولتاژ و فرکانس با کنترل‌کننده اولیه.

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

۶- نتایج شبیه‌سازی

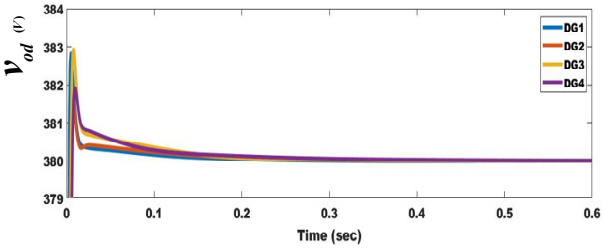
برای شبیه‌سازی از یک مدل نمونه مطابق با [۳۳] استفاده گردیده و DG۱ به‌عنوان شین مرجع یا اسلک در نظر گرفته شده و پارامترهای این DGها شامل چهار منبع توزیع‌شده در [۳۳] آمده‌اند.

در این مدل ولتاژ مرجع ۳۸۰ ولت و فرکانس مرجع ۵۰ هرتز (فرکانس زاویه‌ای $\omega_{ref} = 2\pi f_{ref} = 314.16$ rad/sec) در نظر گرفته شده است. منابع تولید پراکنده به دو طریق قدرتی و مخابراتی با هم ارتباط دارند. اثرات حمله‌های سایبری مختلف بر کنترل‌کننده ثانویه با استفاده از شبیه‌سازی در سیمولینک متلب مورد ارزیابی قرار گرفته است.

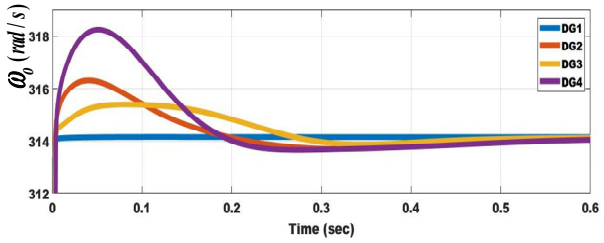
۶-۱ کنترل ریزشبکه با کنترل‌کننده اولیه و ثانویه

در صورت کنترل ریزشبکه فقط با کنترل‌کننده اولیه، خروجی‌ها از مقدار مرجع انحراف دارند و همگام‌سازی به‌درستی انجام نمی‌شود. شکل ۵- الف و ۵- ب، خروجی ولتاژ و فرکانس بدون کنترل‌کننده ثانویه و شکل ۶- الف و ۶- ب خروجی ولتاژ و فرکانس با کنترل‌کننده ثانویه را نشان می‌دهند. ولتاژ با توجه به نتایج شبیه‌سازی، افت شدیدی دارد و همگام‌سازی نیز در این حالت انجام نشده و همچنین فرکانس و ولتاژ انحراف پیدا کرده‌اند. با توجه به اینکه فرکانس بسیار به انحراف حساس است، انحراف قابل قبول نیست و در نتیجه، کم‌کردن انحراف در این حالت ضروری است. همچنین در این حالت سیستم به نویز، اغتشاش و دینامیک مدل‌نشده حساس است. کنترل‌کننده اولیه پایداری سیستم را تا حد زیادی ایجاد کرده است؛ اما نتوانسته همگام‌سازی را به‌درستی انجام دهد.

شکل ۶- الف و ۶- ب خروجی ولتاژ و فرکانس با کنترل‌کننده ثانویه و اولیه را در این حالت نشان می‌دهد. در این کنترل‌کننده ضرایب به‌صورت $C_p = C_\omega = C_v = 3000$ در نظر گرفته شده‌اند. با توجه به نتایج،

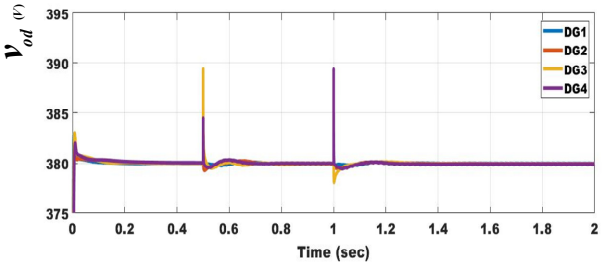


(الف)

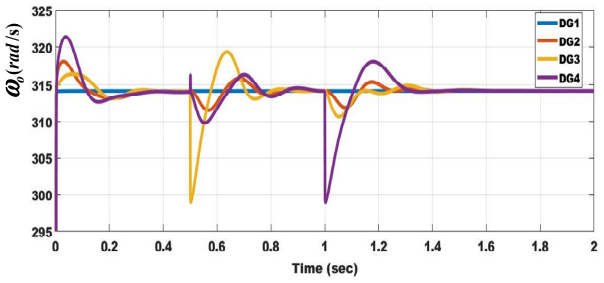


(ب)

شکل ۶: خروجی (الف) ولتاژ و (ب) فرکانس ریزشبکه با کنترل‌کننده اولیه و ثانویه.



(الف)



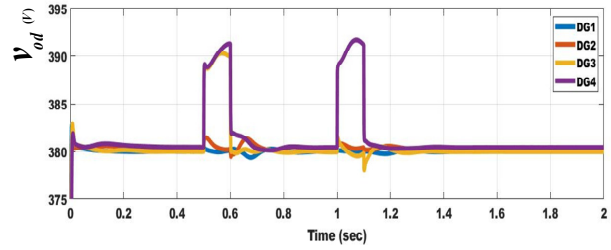
(ب)

شکل ۷: (الف) ولتاژ و (ب) فرکانس خروجی با حمله سایبری سنسوری در کانال ارتباطی بین DG۲ و DG۳ و بین DG۳ و DG۴.

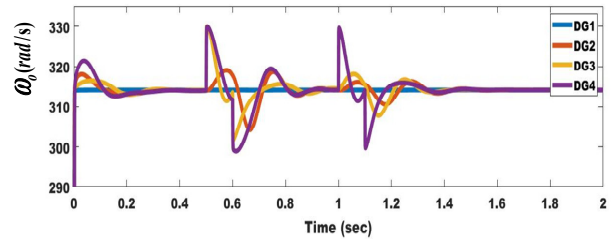
کنترل‌کننده توانسته که به‌خوبی فرکانس و ولتاژ را به حالت مرجع خود برگرداند و در رنج بسیار خوبی قرار دهد. زمان عبور از حالت گذرا کمتر از ۰٫۳ ثانیه بوده که زمان مناسبی است. مقدار بالازدگی سیستم به‌نحوی است که قابل تحمل باشد و نیاز به خارج‌کردن بارها از شبکه نیست.

۶-۲ حمله سنسوری و عملگری

برای تحلیل بهتر، حمله سایبری در سنسورها و عملگرهای مختلف بررسی می‌شود. به‌منظور بررسی اثرات حمله و اثر موقعیت DG بر تأثیرات حمله سایبری، موقعیت‌های مختلف DGها بررسی گردیده است. در این سناریو در $t=0.5\text{sec}$ حمله سنسوری به کانال ارتباطی، بین DG۱ و DG۲ اتفاق افتاده و همچنین در $t=1\text{sec}$ حمله به کانال ارتباطی، بین DG۳ و DG۴ در نظر گرفته شده است. در اینجا حمله‌های سنسوری برای مقایسه با حمله سایبری ربودن اطلاعات در محدوده هم در نظر گرفته شده‌اند و اثر آن بر روی DGهای دیگر بررسی می‌گردد. با توجه به شکل ۷ و همچنین جدول ۱ مشخص است هنگامی که حمله سایبری به کانال ارتباطی DG۱ و DG۲ اتفاق می‌افتد، اثر این حمله در DG۲ بیشتر



(الف)



(ب)

شکل ۸: (الف) ولتاژ و (ب) فرکانس خروجی DGها با حمله سایبری هم‌زمان ربودن اطلاعات در کانال‌های ارتباطی مختلف.

جدول ۱: ضریب تاب‌آوری با حضور حمله سنسوری.

	DG۱	DG۲	DG۳	DG۴
RI of voltage	۳۱۰۹	۱۵۸۵	۱۳۳۵	۱۲۱۳
RI of frequancy	۶۲۸۸۴	۲۲۷	۱۲۲	۹۳

جدول ۲: ضریب تاب‌آوری با حضور حمله ربودن اطلاعات.

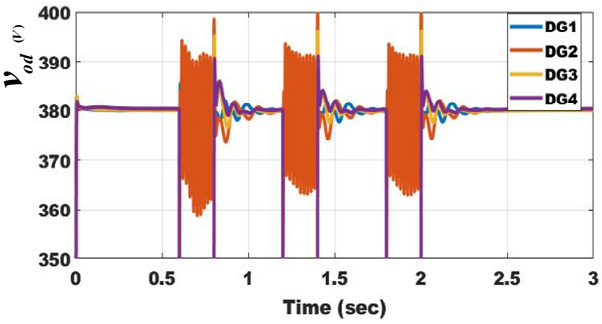
	DG۱	DG۲	DG۳	DG۴
RI of voltage	۲۱۶۰	۳۰۱	۲۲۵	۸۶
RI of frequency	۴۰۹۱۰	۱۰۰	۸۴	۵۵

از بقیه DGهاست و به‌ترتیب DG۳ و DG۴ اثرات بیشتری را از حمله می‌پذیرند. پس حمله سایبری سنسوری DGهای همجوار را بیشتر تحت تأثیر قرار می‌دهد. با توجه به نتایج شبیه‌سازی این کنترل‌کننده توانسته که اثرات حمله سایبری را به‌خوبی حذف کند. نکته دیگر این است که حمله سایبری به سنسور ولتاژ بر مقدار فرکانس نیز تأثیر دارد.

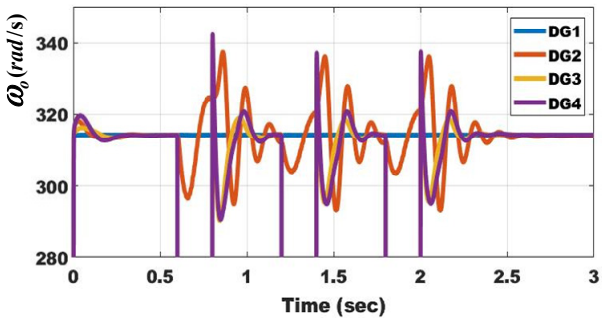
با توجه به شکل ۷ همه DGها توانستند با وجود حمله سایبری سنسوری به پایداری و همگام‌سازی برسند. مقدار ضریب تاب‌آوری با حضور این حمله به‌صورت جدول ۱ است.

۶-۳ حمله سایبری ربودن اطلاعات هم‌زمان ولتاژ و فرکانس

در این سناریو به‌منظور بررسی اثر ولتاژ و فرکانس حمله سایبری ربودن اطلاعات، حمله در $t=1\text{sec}$ تا $t=0.6\text{sec}$ و با مقدار ولتاژ $v_{odj}^{a}=390\text{v}$ و فرکانس $\omega_{oj}^{a}=330\text{rad/sec}$ در کانال ارتباطی بین DG۲ و DG۳ و در $t=1\text{sec}$ تا $t=1.1\text{sec}$ بین DG۳ و DG۴ وارد می‌شود (شکل ۸ و جدول ۲). با توجه به شکل، حمله سایبری فرکانس و ولتاژ بر همدیگر تأثیر دارند و با توجه به مسیر درخت تعریف‌شده، اثر حمله بر DGها با هم متفاوت است؛ هرچند که این کنترل‌کننده به‌خوبی توانسته با وجود حمله سایبری ربودن اطلاعات در رنج محدودی در کمتر از ۰٫۵ ثانیه خروجی‌ها را به مقدار مرجع برساند و همگام‌سازی را نیز انجام دهد. نتایج شبیه‌سازی نشان می‌دهند با توجه به نحوه گرفتن اطلاعات و به عبارتی شکل درخت، اثر حمله بر منابع متفاوت است. همچنین خطا توسط لایه ثانویه کنترل می‌شود و همگام‌سازی با اتمام حمله انجام می‌گردد.



(الف)



(ب)

شکل ۹: ولتاژ و فرکانس خروجی منابع تولید پراکنده با حملات سایبری DoS متناوب بین کانال ارتباطی DG۲ و DG۳.

جدول ۳: ضریب تاب‌آوری با حضور حمله DoS.

	DG۱	DG۲	DG۳	DG۴
RI of voltage	۹۳	۵۱	۰٫۰۲	۰٫۰۲
RI of frequancy	۷۹۹۷	۲۲	۰٫۰۰۱	٫۰۰۱

٤-٦ 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. با توجه به (۲۵)، $\tau_s^{۲۳}=۰٫۲$ و $\Xi_D^{ij}(t_۱,t_۲)=۰٫۶$ است. این سناریو به‌منظور بررسی توانایی روش کنترلی ارائه‌شده در قطع و وصل‌های پیوسته و همچنین در مقابل یک حمله سایبری شدیدتر است. نتایج این شبیه‌سازی در شکل ۹ و جدول ۳ آمده است. با توجه به شکل و با توجه به اینکه 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، خروجی‌ها بازیابی و همگام می‌شوند.

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

۷- نتیجه‌گیری

در این مقاله اثر حمله‌های سایبری بر کنترل‌کننده ثانویه مورد بررسی قرار گرفته و منابع تولید پراکنده با گره‌های سیستم چندعامله و لینک‌های مخابراتی بین آنها با ماترس مجاورتی بحث گردیده است. نتایج نشان می‌دهند که کنترل‌کننده اولیه به‌تنهایی نمی‌تواند همگام‌سازی را انجام دهد و باید از کنترل‌کننده ثانویه استفاده گردد. کنترل‌کننده بدون حمله سایبری و اغتشاش، پایداری و همگام‌سازی ریزشبکه را حفظ می‌کند و قوانین سیستم‌های چندعامله رینولد با این کنترل‌کننده رعایت می‌گردد.

فرمول‌بندی ریاضی اثرات حمله‌های سایبری بر ریزشبکه انجام شده و اثر سه نوع حمله سایبری پرکاربرد شامل حمله سایبری سنسوری و عملگری، ربودن اطلاعات و DoS در این مقاله بررسی گردیده است. حمله‌های سایبری در معادلات منابع تولید پراکنده با کنترل‌کننده سلسه‌مراتبی توزیع‌شده وارد گردیده و اثرات این حمله سایبری مورد بررسی قرار گرفته است. به‌منظور تحلیل پایداری سیستم، تابع لیاپانوف مناسب با حضور حمله‌های سایبری پیشنهاد گردیده است. با فرمول‌بندی ریاضی و ارائه قضایای مناسب، پایداری و همگام‌سازی ریزشبکه با حضور حمله‌های سایبری اثبات شده است. نهایتاً برای اطمینان از نتایج تئوری با استفاده از شبیه‌سازی در نرم‌افزار سیمولینک متلب، اثر حمله در لینک‌های مختلف برای یک شبکه نمونه آمده است.

به‌منظور بررسی کارایی تاب‌آوری سیستم در مقابل حملات مختلف از ضریب تاب‌آوری استفاده شده است. با استفاده از این ضریب، اثر حمله سایبری DoS در سیستم بسیار بیشتر است و در صورت بروز حمله، DGهایی که به گره اسلک وصل نباشند، ناپایدار شده و باید از مدار خارج شوند. حمله سایبری ربودن اطلاعات نیز اثر زیادی در سیستم دارد؛ چون در زمان حمله مقدار خروجی را جایگزین می‌کند. حمله سایبری سنسوری و عملگری به مقدار حمله بستگی دارد و اگر حمله سایبری مستقیماً به اطلاعات رسیده به DG وارد شود، اثر بیشتری بر آن دارد.

با توجه به نتایج شبیه‌سازی در صورت حمله سایبری و به شرط پیوستگی درخت، این کنترل‌کننده توانسته است 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 وجود داشته باشد، این روش کنترلی بهتر پایداری را حفظ خواهد کرد.

مراجع

[1] J. J. Justo, F. Mwasilu, J. Lee, and J. W. Jung, "AC-microgrids versus DC-microgrids with distributed energy resources: a review," *Renewable and Sustainable Energy Reviews*, vol. 24, pp. 387-405, Aug. 2013.

[2] A. Solat, G. B. Gharehpetian, M. S. Naderi, and A. Anvari-Moghaddam, "On the control of microgrids against cyber-attacks: a review of methods and applications," *Applied Energy*, *pt A*, vol. 353, Article ID: 122037, 2024.

[۳] ع. میرزابیگی، ع. کاظمی، م. رمضانی و س. م. عظیمی، "طراحی کنترل‌کننده ثانویه پایه‌ریزی‌شده بر روی کنترل اشتراکی توزیع شده منابع تولید پراکنده (DGها) با رویکرد سیستم‌های چندعامله با درنظرگرفتن حملات سایبری DoS"، *نشریه مهندسی برق و مهندسی کامپیوتر ایران، الف- مهندسی برق*، سال ۲۰، شماره ۴، صص. ۲۹۲-۲۸۰، زمستان ۱۴۰۱.

[4] O. Ali, T. L. Nguyen, and O. A. Mohammed, "Assessment of cyber-physical inverter-based microgrid control performance under communication delay and cyber-attacks," *Applied Sciences*, vol. 14, no. 3, Article ID: 997, 23 pp., 2024.

[5] 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. IEEE*, *11th Power Electronics, Drive Systems, and Technologies Conf., PEDSTC'24,* 6 pp., Tehran, Iran, 4-6 Feb. 2020.

[6] 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.

[7] 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.

[8] Y. Wang, C. Deng, Y. Liu, and Z. Wei, "A cyber-resilient control approach for islanded microgrids under hybrid attacks," *International J. of Electrical Power & Energy Systems*, vol. 147, Article ID: 108889, May 2023.

[9] 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.

[10] 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.

[11] 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 Applications, ICIEA'20*, pp. 170-175, Kristiansand, Norway, 9-13 Nov. 2020.

[12] R. Lu and J. Wang, "Distributed control for AC microgrids with false data injection attacks and time delays," in *Proc. 5th Int. Conf. on Advances in Energy and Environment Research*, *ICAERA'24*, vol. 194, Article ID: 03023, 5 pp., Shanghai, China, 18-20 Sept. 2020.

[13] 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.

[۱۴] ع. میرزابیگی، ع. کاظمی، م. رمضانی و س. م. عظیمی، " پایدارسازی و سنکرون‌سازی ریزشبکه جزیره‌ای با حضور خطا و حمله سایبری سنسوری و عملگری با طراحی کنترل‌کننده ثانویه،" *نشریه مهندسی برق و مهندسی کامپیوتر ایران، الف- مهندسی برق*، سال ۲۱، شماره ۳، صص. ۱۵۴-۱۴۱، پاییز ۱۴۰۲.

[15] B. Xia, S. Fan, L. Ding, and C. Deng, "Distributed dynamic event-triggered resilient control for AC microgrids under FDI attacks," *IEEE Trans. on Circuits and Systems I: Regular Papers*, vol. 71, no. 3, pp. 1406-1416, Mar. 2024.

[16] 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. 2021.

[17] J. Liu, X. Lu, and J. Wang, "Resilience analysis of DC microgrids under denial of service threats," *IEEE Trans. on Power Systems*, vol. 34, no. 4, pp. 3199-3208, Jul. 2019.

[18] 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.

[19] 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.

[20] 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.

[21] S. Deng, L. Chen, X. Lu, T. Zheng, and S. Mei, "Distributed finite-time secondary frequency control of islanded microgrids with enhanced operational flexibility," *IEEE Trans. on Energy Conversion*, vol. 36, no. 3, pp. 1733-1742, Sept. 2021.

[22] 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.

[23] 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. IEEE 10th Smart Grid Conf., SGC'20,* 6 pp., Kashan, Iran, 16-17 Dec. 2020.

[24] 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.

[25] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Multilayer resilience paradigm against cyber attacks in DC microgrids," *IEEE Trans. on Power Electronics*, vol. 36, no. 3, pp. 2522-2532, Mar. 2020.

[26] J. Yang, J. Dai, H. B. Gooi, H. D. Nguyen, and A. Paudel, "A proof-of-authority blockchain-based distributed control system for islanded microgrids," *IEEE Trans. on Industrial Informatics*, vol. 18, no. 11, pp. 8287-8297, Nov. 2022.

[27] R. Yan, Y. Wang, J. Dai, Y. Xu, and A. Q. Liu, "Quantum-key-distribution-based microgrid control for cybersecurity enhancement," *IEEE Trans. on Industry Applications*, vol. 58, no. 3, pp. 3076-3086, May/Jun. 2022.

[28] C. Deng, Y. Wang, C. Wen, Y. Xu, and P. Lin, "Distributed resilient control for energy storage systems in cyber-physical microgrids," *IEEE Trans. on Industrial Informatics*, vol. 17, no. 2, pp. 1331-1341, Feb. 2021.

[29] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A FDI attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Trans. on Smart Grid*, vol. 12, no. 3, pp. 1929-1938, May 2021.

[30] H. Dong, C. Li, and Y. Zhang, "Resilient consensus of multi-agent systems against malicious data injections," *J. of the Franklin Institute*, vol. 357, no. 4, pp. 2217-2231, Mar. 2020.

[31] F. L. Lewis, H. Zhang, K. Hengster-Movric, and A. Das, *Cooperative Control of Multi-Agent Systems: Optimal and Adaptive Design Approaches*, SpringerLink, 2014.

[32] B. P. Poudel, A. Mustafa, A. Bidram, and H. Modares, "Detection and mitigation of cyber-threats in the DC microgrid distributed control system," *International J. of Electrical Power & Energy Systems*, vol. 120, Article ID: 105968, Sept. 2020.

[33] A. Mirzabeigi, A. Kazemy, M. Ramezani, and S. M. Azimi, "Distributed robust cooperative hierarchical control for island microgrids under hijacking attacks based on multiagent systems," *International Trans. on Electrical Energy Systems*, vol. 2023, Article ID: 6622346, 15 pp., 2023.

[34] 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.

[35] M. Shi, *et al.*, "PI-consensus based distributed control of AC microgrids," *IEEE Trans. on Power Systems*, vol. 35, no. 3, pp. 2268-2278, May. 2020.

[36] 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. 2012.

[37] 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.

[38] 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.

[39] 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.

[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. 52, no. 7, pp. 1426-1439, May 2021.

[41] 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 2020.

[42] 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. 2020.

[43] W. Yao, Y. Wang, Y. Xu, and C. Deng, "Cyber-resilient control of an islanded microgrid under latency attacks and random DoS attacks," *IEEE Trans. on Industrial Informatics*, vol. 19, no. 4, pp. 5858-5869, Apr. 2023.

[44] A. Karimi, A. Ahmadi, Z. Shahbazi, Q. Shafiee, and H. Bevrani, "A resilient control method against false data injection attack in DC microgrids," in *Proc. IEEE 7th Int. Conf. on Control, Instrumentation and Automation, ICCIA'21,* 6 pp., Tabriz, Iran, 23-24 Feb. 2021.

[45] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Trans. on Industrial Informatics*, vol. 16, no. 6, pp. 3881-3894, Jun. 2020.

[46] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, "Networked microgrids for enhancing the power system resilience," in *Proceeding of the IEEE*, vol. 105, no. 7, pp. 1289-1310, Jul. 2017.

[47] 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.

[48] 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، کارشناسی ارشد مهندسی برق کنترل در سال ۱۳۸۵ از دانشگاه علم و صنعت ایران و دکترای مهندسی برق کنترل دانشگاه تفرش در سال ۱۴۰۲ به پایان رسانده است. هم‌اکنون استادیار دانشکده مهندسی برق موسسه آموزش عالی جهاد دانشگاهی همدان می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: ریزشبکه، آنالیز و کنترل سیستم‌های با تاخیر زمانی، سیستم‌های چندعامله و حملات سایبری.

علی کلانترنیا تحصیلات خود را در مقاطع کارشناسی مهندسی برق قدرت از دانشگاه بوعلی سینای همدان در سال ۱۳۸۲، کارشناسی ارشد مهندسی برق مخابرات از دانشگاه تبریز در سال ۱۳۸۶ و دکترا مهندسی برق مخابرات دانشگاه بین المللی امام خمینی قزوین در سال ۱۳۹۹ به پایان رسانده است. هم‌اکنون استادیار دانشکده مهندسی برق دانشگاه بوعلی سینای همدان می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: آنتن، سازگاری الکترومغناطیسی، پرتابگرهای الکترومغناطیسی و سیستم‌های مخابراتی در ریزشبکه‌ها.