مقاله پژوهشی

تشخیص و حذف تأثیر یک حمله سایبری ترکیبی به سیستم کنترل خودکار تولید

تینا حاجی‌عبداله، حسین سیفی و سیدحامد دلخوش

چکیده: پیشرفت‌های اخیر در سیستم‌های نظارت و کنترل شبکه‌های قدرت، نیازمند زیرساخت مخابراتی برای ارسال و دریافت داده‌های اندازه‌گیری و فرمان‌های کنترلی است. این تعاملات سایبری- فیزیکی، علی‌رغم افزایش کارایی و قابلیت اطمینان، شبکه‌های قدرت را در معرض حملات سایبری قرار داده است. سیستم کنترل خودکار تولید (AGC)، یکی از مهم‌ترین حلقه‌های کنترلی شبکه قدرت است که نیازمند زیرساخت مخابراتی بوده و بسیار مورد توجه حمله‌کنندگان سایبری قرار گرفته است؛ زیرا یک حمله موفق به سیستم AGC، نه تنها تأثیر مستقیمی بر فرکانس سیستم دارد، بلکه می‌تواند پایداری و عملکرد اقتصادی شبکه برق را نیز تحت تأثیر قرار دهد. لذا آشنایی با تأثیر حملات سایبری به AGC و تبیین راهکارهایی به منظور دفاع در برابر آنها دارای ضرورت و اهمیت تحقیقاتی است. در غالب تحقیقات صورت‌گرفته در حوزه حمله- دفاع سیستم AGC، از محدودیت‌های سیستم AGC نظیر باند راکد گاورنر و تأخیر انتقال شبکه مخابراتی در مدل‌سازی چشم‌پوشی شده است. از طرفی، تا کنون در نظر گرفتن هم‌زمان دو حمله سایبری مختلف به سیستم AGC و ارائه روشی به منظور دفاع در برابر آنها مورد بررسی واقع نشده است. در این مقاله، با توجه به کمبودهای پژوهش‌های پیشین، ضمن استفاده از مدل بهبودیافته AGC شامل باند راکد گاورنر و تأخیر انتقال شبکه مخابراتی، به بررسی تأثیر دو حمله تزریق داده‌های اشتباه (FDI) و تأخیر که از مهم‌ترین حملات سایبری به سیستم AGC هستند و همچنین، تأثیر هم‌زمان این دو حمله تحت عنوان حمله سایبری ترکیبی، پرداخته شده است. روش دفاع سه‌مرحله‌ای مبتنی بر فیلتر کالمن به منظور تشخیص، تخمین و حذف تأثیر حمله پیشنهاد شده و کارایی آن بر روی سیستم AGC دوناحیه‌ای مورد آزمایش قرار گرفته است.

کلیدواژه: **حمله تأخیر، حمله تزریق داده‌های اشتباه، حمله سایبری ترکیبی، دفاع سایبری، فیلتر کالمن، کنترل خودکار تولید.**

فهرست اندیس‌ها، پارامترها، ماتریس‌ها و بردارها

k: اندیس مربوط به گام زمانی
D: ضریب میرایی بار
H: ثابت اینرسی
R: مشخصه دروپ گاورنر
B: ضریب بایاس فرکانسی
ACE: سیگنال خطای ناحیه کنترلی
K_c: بهره کنترل‌کننده انتگرالی
T_g و T_t: ثابت زمانی گاورنر و توربین
$P_{s_{۱۲}}$: ضریب همگام‌سازی توان خط انتقال بین نواحی کنترلی ۱ و ۲
τ و $\hat{\tau}$: میزان واقعی و تخمین زده شده حمله تأخیر
d و $d_{۱۲}$: سیگنال حمله FDI به انحراف فرکانس و انحراف توان عبوری از خط انتقال بین نواحی ۱ و ۲
ΔP_g: تغییرات توان خروجی گاورنر
ΔP_m: تغییرات توان مکانیکی
ΔP_l: تغییرات بار ناحیه کنترلی
ΔP_c: تغییرات توان کنترل‌کننده (خروجی کنترل‌کننده AGC)
ΔF: انحراف فرکانس در ناحیه کنترلی از مقدار نامی
$\Delta P_{tie_{۱۲}}$: انحراف توان عبوری از خطوط انتقال بین نواحی ۱ و ۲
$\vec{X}$ و $\dot{\vec{X}}$: بردار متغیرهای حالت و بردار مشتق زمانی متغیرهای حالت
$\vec{X}(\tau)$: بردار تأخیردار متغیرهای حالت به اندازه τ
$\vec{Y}$: بردار خروجی
$\vec{U}$: بردار ورودی
$I\vec{n}j$ و $\hat{I\vec{n}j}$: بردار سیگنال‌های واقعی و تخمین زده شده حمله FDI
$\vec{W}_k$ و $\vec{V}_k$: بردار نویز فرایند و اندازه‌گیری در گام زمانی k
$\overline{R}$ و $\overline{Q}$: ماتریس کوواریانس نویز اندازه‌گیری و فرایند
μ_{noise} و δ_{noise}: میانگین و انحراف معیار نویز اندازه‌گیری و فرایند
$\overline{P}_k$ و $\overline{K}_k$: ماتریس‌های کوواریانس تخمین و بهره فیلتر کالمن در گام زمانی k
$\overline{P}_x^d$: ماتریس کوواریانس خطای تخمین حمله FDI در گام زمانی k
$\overline{P}_x^x$: ماتریس کوواریانس خطای تخمین متغیرهای حالت در گام زمانی k
$\overline{P}_x^{xd}$: ماتریس کوواریانس متغیرهای حالت و حمله FDI در گام زمانی k
$\overline{r}_k$: بردار باقیمانده خطای تخمین فیلتر کالمن در گام زمانی k
$\overline{e}_m$: خطای تخمین حالت با وجود تأخیر در شبکه
$\overline{\varphi}$: ماتریس کوواریانس باقیمانده خطای تخمین فیلتر کالمن
$norm_k$: نُرم ماهالانوبیس ماتریس باقیمانده خطای تخمین در گام زمانی k
μ_n و μ_a: میانگین نُرم ماهالانوبیس در شرایط نرمال و در صورت وجود حمله در شبکه
δ_n و δ_a: انحراف معیار نرم ماهالانوبیس در شرایط نرمال و در صورت وجود حمله در شبکه

این مقاله در تاریخ ۱۰ خرداد ماه ۱۴۰۰ دریافت و در تاریخ ۲۸ بهمن ماه ۱۴۰۰ بازنگری شد.

تینا حاجی‌عبداله، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران، (email: tina.hajiabdollah@modares.ac.ir).
حسین سیفی، استاد، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران، (email: seifi_ho@modares.ac.ir).
سیدحامد دلخوش، استادیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران، (email: h.delkhosh@modares.ac.ir).

q_n و q_a: ضرایب توزیع نرمال در شرایط نرمال و در صورت وجود حمله در شبکه

I_n: احتمال تشخیص وجود حمله در شرایط نرمال

I_a: احتمال عدم تشخیص وجود حمله در صورت وجود حمله در شبکه

I: آستانه

T_s: دوره نمونه‌برداری

$\overline{A}$ و $\overline{A}_d$: ماتریس‌های سیستم به ترتیب در فضای پیوسته و گسسته

$\overline{B}$ و $\overline{B}_d$: ماتریس‌های ورودی به ترتیب در فضای پیوسته و گسسته

$\overline{C}$ و $\overline{C}_d$: ماتریس‌های خروجی به ترتیب در فضای پیوسته و گسسته

$\overline{D}$ و $\overline{D}_d$: ماتریس پیش‌خور به ترتیب در فضای پیوسته و گسسته

$\overline{G}$، $\overline{H}$، $\overline{G}_d$ و $\overline{H}_d$: ماتریس‌های ضرب‌شونده در بردار حمله FDI به ترتیب در فضای پیوسته و گسسته

$\overline{E}$، $\overline{F}$، $\overline{E}_d$ و $\overline{F}_d$: ماتریس‌های ضرب‌شونده در بردار تأخیردار متغیرهای حالت به ترتیب در فضای پیوسته و گسسته

۱- مقدمه

شبکه‌های قدرت طی چند دهه گذشته، به طور مداوم در حال رشد و توسعه هستند. افزایش وسعت جغرافیایی و پیچیدگی‌های فنی شبکه قدرت و از طرف دیگر، وابستگی روزافزون جوامع مدرن به انرژی الکتریکی، عملکرد قابل اطمینان شبکه را بیش از پیش به امری چالش‌برانگیز برای بهره‌برداران سیستم بدل کرده است. پیشرفت‌های اخیر در سیستم‌های نظارت و کنترل از جمله اتوماسیون پست‌ها، واحدهای اندازه‌گیری فازور (PMU)[1]، زیرساخت‌های اندازه‌گیری پیشرفته (AMI)[2] و قابلیت‌های ارتباطی دیجیتال دوطرفه که همگی نیازمند زیرساخت مخابراتی برای ارسال و دریافت داده‌های اندازه‌گیری و فرمان‌های کنترلی هستند، می‌توانند به طور چشم‌گیری کارایی و قابلیت اطمینان شبکه قدرت را افزایش دهند. از طرفی، وابستگی بخش فیزیکی سیستم‌های قدرت به بخش سایبری به منزله تعامل سایبری- فیزیکی است که علی‌رغم این واقعیت که به منظور بهبود کنترل و نظارت بر سیستم قدرت طراحی شده است، آن را در معرض حملاتی سایبری قرار داده که می‌توانند به طور بالقوه منجر به اثرات اقتصادی و اجتماعی فاجعه‌بار شوند [۱].

شبکه برق بنا به دلایل متعدد به یکی از اهداف اصلی حملات سایبری تبدیل شده و توجه ویژه‌ای را به خود معطوف کرده است، چرا که ستون فقرات زیرساخت‌های اصلی یک کشور نظیر زیرساخت‌های دفاعی و اقتصادی را تشکیل می‌دهد. پیاده‌سازی حملات سایبری نسبت به حملات فیزیکی ارزان‌تر و آسان‌تر تمام شده و علاوه بر این، یک حمله‌کننده می‌تواند با هماهنگ‌کردن حملات فیزیکی و سایبری، به سیستم خسارات شدیدتری وارد کند [۲]. به منظور تأمین امنیت شبکه برق، اقدامات پدافند پیشگیرانه باید هم در زیرساخت‌های فیزیکی و هم در زیرساخت‌های سایبری گنجانده شوند. اقدامات امنیتی متداول نظیر تشخیص نفوذ[3] و دیوار آتش[4] می‌توانند به منظور جلوگیری از حملات ابتدایی مورد استفاده قرار گیرند. با این حال، این اقدامات دفاعیِ ابتدایی قادر به تشخیص حملات ماهرانه، پیچیده و هوشمند نخواهند بود. از این رو، نیاز فزاینده‌ای به روش‌های دفاعی در برابر حملات سایبری وجود داشته که فراتر از سازوکارهای امنیتی متداول عمل کنند. یک روش دفاعی موفق، مبتنی بر درک دقیق حمله است. در نتیجه، درک مقاصد و الگوهای رفتاری حمله‌کنندگان به عنوان اولین گام برای مقابله در برابر آنها، از اهمیت ویژه‌ای برخوردار است [۳].

سیستم کنترل خودکار تولید (AGC)[5]، یکی از حلقه‌های کنترلی است که بسیار مورد توجه حمله‌کنندگان سایبری قرار گرفته است، زیرا نوسانات فرکانس به دلیل تغییر بار یا حمله سایبری در یک ناحیه، بر تمام نواحی به هم پیوسته دیگر تأثیر گذاشته و نه‌تنها تأثیر مستقیمی بر فرکانس سیستم دارند، بلکه می‌توانند بر پایداری و عملکرد اقتصادی شبکه برق نیز تأثیر گذاشته و عواقب فاجعه‌باری را به همراه داشته باشند. از طرفی AGC سیستمی خودکار است که نیاز به حداقل نظارت و مداخله نیروی انسانی دارد و همین امر، امکان پیاده‌سازی حمله به آن را تسهیل می‌بخشد. از طرف دیگر، الگوریتم‌های کنترل پایداری فرکانس، سیگنال‌های کنترلی را در بازه زمانی چند ثانیه ارائه می‌دهند. بنابراین امکان استفاده از الگوریتم‌های پیچیده و زمان‌بر به منظور اعتبارسنجی داده‌ها وجود نداشته که همین امر باعث آسیب‌پذیری بیشتر آنها در برابر اختلالات و حملات سایبری می‌گردد [۴].

وجود سیستم AGC به منظور تنظیم فرکانس و حفظ تبادلات توان بین نواحی کنترلی مختلف در مقادیر برنامه‌ریزی‌شده، ضروری است. برای دستیابی به این اهداف، سیستم AGC با دریافت داده‌های اندازه‌گیری و پردازش آنها، در صورت لزوم دستوراتی را برای تغییر نقطه کار ژنراتورها ارسال می‌کند. بدین ترتیب، فرمان‌های کنترلی و اندازه‌گیری‌های به دست آمده در نقاط مختلف شبکه، از طریق زیرساخت سایبری مبادله می‌شوند. از این رو، در برابر حملات سایبری آسیب‌پذیر هستند و حملات سایبری به آنها، ممکن است محاسبات مربوط به الگوریتم AGC را گمراه کرده و عملکرد کلی سیستم را به شدت تحت تأثیر قرار دهد. با توجه به مطالب ذکرشده در خصوص آثار مخرب حملات سایبری، انعطاف‌پذیری بخش‌های مختلف سیستم قدرت نظیر AGC در برابر خطاها، خرابی‌ها و حملات، موضوعی جذاب در بین محققان است [۴]. از میان حملات سایبری مؤثر بر عملکرد سیستم‌های کنترل فرکانس، دو حمله تأخیر با ایجاد اختلال در دسترس‌پذیری داده‌ها[6] و حمله تزریق داده‌های اشتباه (FDI)[7] با تأثیر بر یکپارچگی داده‌ها[8] از طریق دستکاری و جعل آنها، از اهمیت بالایی برخوردارند. در ادبیات موضوع، تحقیقات بسیاری به طور خاص به بررسی حملات FDI به سیستم کنترل فرکانس از منظر روش‌های حمله و اقدامات متقابل پرداخته‌اند. نویسندگان در [۵]، تأثیر حمله FDI را بر اندازه‌گیری‌های مورد استفاده در سیستم AGC برای گمراه‌کردن بهره‌بردار در انجام اقدامات کنترلی مناسب که ممکن است باعث اقداماتی از قبیل کاهش بار غیر ضروری، قطع ژنراتور و یا حتی خطاهای آبشاری شود، بررسی کرده‌اند. در [۶]، داده‌های اندازه‌گیری فرکانس و توان عبوری از خط انتقال بین نواحی مختلف، هدف الگوهای مختلف حمله FDI قرار گرفته‌اند. در این مرجع، الگوریتمی به منظور تشخیص وجود حمله با استفاده از پیش‌بینی بار زمان واقعی پیشنهاد شده که به پیش‌بینی عملکرد AGC در یک بازه زمانی مشخص می‌پردازد. اگرچه الگوریتم تشخیص ناهنجاری پیشنهادی در [۶] قادر به شناسایی

1. Phasor Measurement Unit
2. Advanced Metering Infrastructure
3. Intrusion Detection
4. Firewall
5. Automatic Generation Control
6. Data Availability
7. False Data Injection
8. Data Integrity

الگوهای از پیش تعریف شده حمله است، اما هیچ تضمینی برای تشخیص حملات سایبری دلخواه توسط الگوریتم پیشنهادی وجود ندارد.

از طرفی، علاوه بر پیش‌بینی بار برای تشخیص وجود حمله، می‌توان از تخمین حالت سیستم و مقایسه آن با مقادیر اندازه‌گیری شده نیز استفاده نمود. الگوریتم‌های مختلفی نظیر فیلتر کالمن (KF)[1]، فیلتر کالمن توسعه‌یافته (EKF)[2]، فیلتر کالمن نمونه‌بردار (UKF)[3] و فیلتر ذره‌ای[4] برای تخمین حالت وجود دارند. ایده اصلی در تمام روش‌های ذکرشده، فیلتر کالمن است که نقشی اساسی در نظریه سیستم داشته و در بسیاری از زمینه‌ها مانند کنترل، پردازش سیگنال و ارتباطات، کاربردهایی گسترده دارد. مزیت اصلی فیلتر کالمن، توانایی آن در ارائه پیش‌بینی بسیار دقیق از حالت سیستم با پیچیدگی‌های محاسباتی نسبتاً کم است [۷]. نویسندگان در [۸]، روش فیلتر کالمن توسعه‌یافته را برای شناسایی حمله در یک سیستم دوناحیه‌ای با ۴ واحد تولیدی و یک سیستم با ۱۶ واحد تولیدی و ۶۴ شین پیشنهاد کرده‌اند. در [۹]، روشی برای تشخیص، تخمین و جبران هم‌زمان اثر حمله FDI در یک سیستم AGC دوناحیه‌ای با در نظر گرفتن نویزهای اندازه‌گیری و فرایند با استفاده از فیلتر کالمن به عنوان تخمین‌گر ورودی مجهول شامل سیگنال حمله FDI پیشنهاد شده است. سپس حالات به دست آمده سیستم برای مقایسه با داده‌های اندازه‌گیری شده، مورد استفاده قرار گرفته است. خطای به دست آمده برای شناسایی حمله FDI در سیستم AGC، در صورتی که از آستانه از پیش تعریف شده بیشتر باشد، مورد استفاده قرار گرفته است. در این مرجع، تعیین آستانه، بدون پشتوانه ریاضی و تنها به صورت کیفی صورت گرفته است. در [۱۰] با در نظر گرفتن باند راکد گاورنر و تأخیر انتقال در شبکه مخابراتی، از شبکه‌های عصبی بازگشتی برای شناسایی حملات FDI در سیستم AGC استفاده شده است. در [۱۱]، نویسندگان عملکرد یک فیلتر کالمن را تحت حمله FDI مورد بررسی قرار داده‌اند و شرایط لازم و کافی برای ایجاد خطای تخمین توسط حمله‌کننده را بدون این که شناسایی شوند، ارائه کرده‌اند. در [۱۲]، ابتدا نشان داده شده که یک حمله FDI علیه سیستم AGC می‌تواند به طور مخفیانه، نتایج مخربی را به دنبال داشته باشد. سپس، یک روش شناسایی حمله مبتنی بر ناهنجاری برای محافظت از سیستم AGC در برابر حملات سایبری پیشنهاد شده است. برای شناسایی حملات، روش پیشنهادی با استفاده از یک ناظر ورودی مجهول (UIO)[5] متغیرهای حالت را تخمین زده و اختلاف مقادیر اندازه‌گیری شده با مقادیر تخمین زده شده توسط UIO محاسبه می‌شود. سناریوهای مختلف حمله و یک استراتژی شناسایی حمله در [۱۳] پیشنهاد شده است. روش تشخیص پیشنهادی بر اساس طبقه‌بندی ادراک چندلایه (MLP)[6] است که برای محاسبه سیگنال ACE، تحت حمله و در شرایط نرمال، استفاده شده و قادر به جداسازی داده‌های اندازه‌گیری جعلی از داده‌های درست است. در [۱۴]، نویسندگان یک طرح اصلاح برای تأثیر حملات FDI علیه سیستم کنترل فرکانس را ارائه کرده‌اند. روش پیشنهادی در این مرجع، در همه سیستم‌ها کاربردی نخواهد بود؛ زیرا در این مقاله فرض شده که تعدادی مسیر ارتباطی اضافی وجود داشته که به طور هم‌زمان توسط حمله‌کننده قابل کنترل نیستند. پس از تشخیص وجود حمله FDI با استفاده از الگوریتم شبکه‌های عصبی، درخواستی مبنی بر استفاده از یک مسیر ارتباطی دیگر برای انتقال داده به فرستنده ارسال می‌شود. علاوه بر تجزیه و تحلیل‌های تئوری، [۱۵] و [۱۶] آسیب‌پذیری سیستم AGC را به صورت تجربی مورد بررسی قرار داده‌اند. در [۱۵]، با ارائه آزمایش‌هایی بر روی یک سیستم در آیووا در ایالات متحده، تأثیر حملات FDI به عنوان منابع بالقوه برای ایجاد افت فرکانس نشان داده شده که می‌توانند منجر به حذف بار غیر ضروری شوند. در [۱۶]، یک سیستم واقعی شامل ۱۶ شین مورد آزمایش قرار گرفته تا به طور عملی، تأثیرات حمله به سیستم AGC را نشان دهد. در این مرجع، روشی بهینه برای طراحی حمله پیشنهاد شده که با استفاده از آن، زمان باقیمانده برای غیر فعال کردن اقدامات اصلاحی نظیر حذف بار و قطع ژنراتور به حداقل می‌رسد. به منظور تشخیص وجود حمله نیز داده‌های اندازه‌گیری مربوط به توان عبوری از خطوط انتقال بین نواحی، با مقادیر به دست آمده با استفاده از داده‌های اندازه‌گیری فرکانس نواحی، مقایسه می‌شود. در این مقاله، همچنین تخمین حالت DC به عنوان یک لایه اضافی برای صحت‌سنجی داده‌های اندازه‌گیری قبل از آن که توسط AGC مورد استفاده قرار گیرند، اجرا می‌شود.

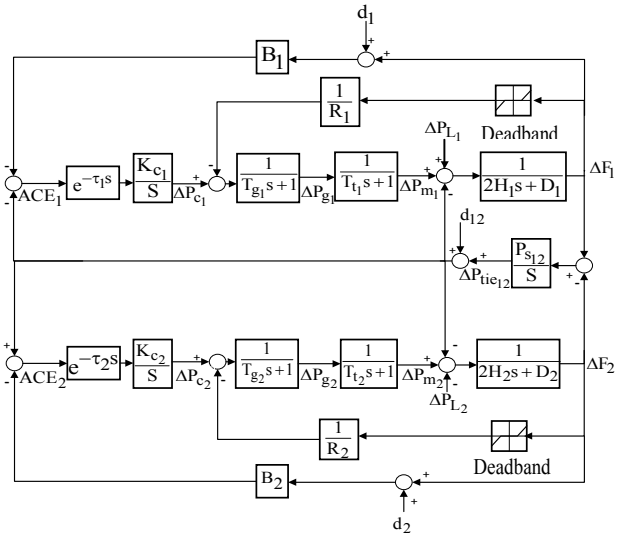
عملکرد سیستم کنترلی AGC در حضور حمله تأخیر و ارائه روش‌های دفاعی به منظور مقابل با حمله فوق، توجه پژوهشگران را به خود معطوف کرده است. در [۱۷] تأثیر حمله تأخیر در یک سیستم AGC سه‌ناحیه‌ای بر عملکرد سیستم کنترل فرکانس با در نظر گرفتن محدودیت‌های AGC و تأخیر انتقال شبکه مخابراتی مطالعه شده است. همچنین با استفاده از شاخص IAE[7]، عملکرد سیستم AGC را در حضور حمله تأخیر از نظر کمّی بررسی کرده است. مرجع [۱۸] ضمن اثبات ناکافی‌بودن روش‌های رمزنگاری در مقابله با حملات DoS و تأخیر، روشی را با فرض وجود مسیرهای ارتباطی اضافی برای مقابله با حمله ارائه داده است. در [۱۹] به طراحی کنترل‌کننده‌ای مقاوم در برابر تأخیرهای ارتباطی بر اساس تکنیک نابرابری ماتریس‌های خطی (LMI)[8] پرداخته شده و پایداری وابسته به تأخیر سیستم کنترل فرکانس در [۲۰] بررسی گردیده است. در این مقاله، تأثیر بهره کنترل‌کننده PI[9] بر حاشیه پایداری وابسته به تأخیر مورد بررسی قرار گرفته است. در [۲۱] یک روش ساده برای خنثی‌کردن حملات تأخیر ارائه شده است، به گونه‌ای که در صورت تشخیص وجود حمله تأخیر، ضرایب کنترل‌کننده، اصلاح‌شده و فرکانس سیستم را تحت حمله تأخیر کنترل می‌کند. در [۲۲]، روشی برای تخمین میزان تأخیر ناشی از حمله ارائه شده و در صورتی که میزان تأخیر از مقدار آستانه پایداری شبکه بیشتر باشد، سیستم در وضعیت هشدار قرار گرفته و به منظور جبران اثر حمله تأخیر، به جای استفاده از کنترل‌کننده اصلی از کنترل‌کننده کمکی استفاده می‌شود. نقد کلی مراجع و مقایسه آنها با مقاله حاضر در جدول ۱ ارائه شده است.

در بیشتر تحقیقات صورت‌گرفته در حوزه حمله- دفاع سیستم AGC، محدودیت‌های سیستم AGC نظیر باند راکد گاورنر و همچنین، تأخیر انتقال شبکه‌های مخابراتی در مدل‌سازی مورد توجه قرار نگرفته‌اند. از طرفی، تا کنون در نظر گرفتن هم‌زمان حمله FDI و تأخیر به سیستم AGC و ارائه روشی برای تشخیص، تخمین و اصلاح هم‌زمان تأثیر این ۲ حمله نیز مورد بررسی واقع نشده است. از این رو، با توجه به کمبودهای

1. Kalman Filter
2. Extended Kalman Filter
3. Unscented Kalman Filter
4. Particle Filter
5. Unknown Input Observer
6. Multi Layer Perceptron
7. Index of Absolute Error
8. Linear Matrix Inequality
9. Proportional Integral

جدول ۱: مقایسه مقاله حاضر با مطالعات پیشین.

مراجع	بهبود مدل‌سازی سیستم AGC				مدل حمله	
	مشخصه دروپ	باند راکد	تأخیر انتقال	حمله FDI	حمله تأخیر	حمله ترکیبی
[۵]، [۶]، [۹]، [۱۲]، [۱۳]، [۱۴] و [۱۶]	✓	×	×	✓	×	×
[۸]	×	×	×	✓	×	×
[۱۰]	✓	✓	×	✓	×	×
[۱۱]	×	×	×	✓	×	×
[۱۵]	✓	✓	✓	✓	×	×
[۱۷]	✓	✓	✓	×	✓	×
[۱۸]، [۱۹]، [۲۰] و [۲۲]	✓	×	×	×	✓	×
[۲۱]	✓	×	✓	×	✓	×
مقاله حاضر	✓	✓	✓	✓	✓	✓



شکل ۱: نمودار بلوکی مدل بهبودیافته سیستم AGC دوناحیه‌ای.

پژوهش‌های پیشین، اهداف و نوآوری‌های مطرح در این مقاله به شرح زیر است:

- استفاده از مدل بهبودیافته AGC با در نظر گرفتن باند راکد گاورنر و تأخیر انتقال شبکه مخابراتی
- پیاده‌سازی و بررسی تأثیر حمله سایبری ترکیبی متشکل از حمله FDI و حمله تأخیر
- پیشنهاد روشی مؤثر در دفاع حملات FDI، تأخیر و همچنین حمله سایبری ترکیبی شامل ۳ مرحله تشخیص و تخمین حمله و اصلاح داده‌های اندازه‌گیری متأثر از حملات با استفاده از تخمین‌گر فیلتر کالمن
- ارائه روشی به منظور تعیین آستانه در فرایند تشخیص حملات FDI، تأخیر و همچنین حمله سایبری ترکیبی

لازم به ذکر است که تمام شبیه‌سازی‌های این مقاله با استفاده از نرم‌افزار Matlab انجام شده است.

در ادامه و در بخش ۲ مدل توسعه‌یافته سیستم، در بخش ۳ مدل حمله، در بخش ۴ مدل دفاع، در بخش ۵ شبکه مورد آزمایش و نتایج عددی و نهایتاً در بخش ۶ نتیجه‌گیری ارائه شده است.

۲- مدل توسعه‌یافته سیستم

در شکل ۱، بلوک دیاگرام سیستم AGC بهبودیافته شامل باند راکد گاورنر، تأخیر انتقال شبکه مخابراتی و وجود حمله سایبری ترکیبی شامل سه سیگنال ورودی d_1، d_2 و d_3 برای اعمال حمله FDI به فرکانس نواحی و توان عبوری از خط انتقال بین دو ناحیه و همچنین، بلوک حمله تأخیر در دریافت داده‌های اندازه‌گیری توسط کنترل‌کننده هر ناحیه نشان داده شده است. در اکثر مطالعات انجام‌شده در حوزه سایبری، مدل AGC ارائه‌شده، مدلی خطی است که در آن تأثیر عواملی نظیر باند راکد عملکرد گاورنر و تأخیر شبکه مخابراتی، در نظر گرفته نشده‌اند. اگرچه در نظر گرفتن تمام محدودیت‌ها در مدل AGC امری نسبتاً دشوار و غیر ضروری است، اما برای مدل‌سازی و تحلیل دقیق‌تر و واقع‌بینانه‌تر، لازم است محدودیت‌های اساسی اعمال‌شده توسط سیستم فیزیکی در نظر گرفته شوند. باند راکد گاورنر به عنوان یکی از محدودیت‌های مهم در عملکرد سیستم کنترل فرکانس شناخته می‌شود. با تغییر سیگنال ورودی گاورنر، تنظیم‌کننده سرعت بلافاصله واکنش نشان نمی‌دهد، مگر این که سیگنال ورودی آن، به مقدار مشخصی رسیده باشد. به بیان دیگر، باند راکد به صورت محدوده‌ای از تغییرات فرکانس تعریف می‌شود که در آن گاورنر نسبت به تغییر وضعیت شیرهای ورودی و به دنبال آن، تغییر توان تولیدی از خود عملکردی نشان نمی‌دهد. نتایج، حاکی از آن است که افزایش باند راکد گاورنر می‌تواند عملکرد سیستم کنترل فرکانس را به میزان قابل توجهی تضعیف کند. در سیستم‌های چندناحیه‌ای، باند راکد معادل برای یک ناحیه برابر با بیشینه مقدار باند راکد گاورنر ژنراتورهای موجود در آن ناحیه فرض می‌شود. اگرچه این فرض، تا حدودی غیر دقیق و بدبینانه است، اما دقت مدل‌سازی را نسبت به حالت‌های دیگر نظیر مدل‌نکردن باند راکد، در نظر گرفتن میانگین و یا کمینه باند راکد گاورنر ژنراتورها به عنوان باند راکد معادل، بهبود می‌بخشد. از طرف دیگر، تأخیرهای شبکه مخابراتی در فرایند کنترل فرکانس به یک چالش مهم تبدیل شده است. این گونه تأخیرهای زمانی در یک سیستم AGC در مسیرهای ارتباطی بین مرکز کنترل و پست‌ها وجود دارد. به بیان دیگر، ارسال داده‌هایی نظیر توان اندازه‌گیری شده خطوط انتقال از واحدهای ترمینال از راه دور (RTU) به مرکز کنترل و همچنین، ارسال فرمان افزایش/ کاهش تولید از مرکز کنترل به واحدهای تولیدی با تأخیر اتفاق می‌افتد. تأخیرهای زمانی در سیستم AGC، باعث تضعیف عملکرد سیستم کنترل فرکانس می‌شود. به همین منظور، ضروری است تا در تحلیل‌های واقع‌بینانه فرایند کنترل فرکانس، به مدل‌سازی آنها پرداخته شود [۲۳]. به منظور تجزیه و تحلیل پاسخ فرکانسی یک سیستم قدرت در حضور تغییرات ناگهانی بار، معمولاً از مدل دینامیکی معادل استفاده می‌شود، به این صورت که مدل دینامیکی ژنراتورها و بارهای موجود در یک ناحیه کنترلی با یک ژنراتور و بار معادل، مدل می‌شوند که می‌توان از آن به عنوان مدل پاسخ فرکانسی معادل برای یک ناحیه کنترلی شامل چندین ژنراتور و بار استفاده کرد. حلقه کنترل اولیه فرکانس به طور معمول شامل توربین، ژنراتور، گاورنر و بار است. تأثیر بارها به صورت ضریب میرایی D و تأثیر ژنراتورها نیز با ثابت اینرسی H مدل می‌شوند. مدل‌های متعددی برای نمایش توربین و گاورنر به منظور استفاده در مطالعات فرکانسی ارائه گردیده که در آنها از حالات گذرای بویلر و ژنراتور چشم‌پوشی شده و فقط ثابت زمانی‌های توربین و گاورنر، T_t و T_g، مدل شده‌اند. به منظور کنترل اولیه فرکانس، از یک حلقه فیدبک شامل مشخصه دروپ R که تنظیم سرعت را بر عهده دارد، استفاده می‌شود. رابطه دینامیکی ژنراتور، بار، اختلاف توان‌های تولیدی و مصرفی و انحراف فرکانس در هر ناحیه توسط معادله دیفرانسیل

ارائه‌شده در (۱) و (۲) بیان می‌شود. ضریب میرایی معادل به صورت مجموع درصد تغییرات بارهای موجود در یک ناحیه به ازای یک درصد تغییر فرکانس آن ناحیه بیان می‌شود. ثابت اینرسی معادل نیز برابر با مجموع ثابت اینرسی‌های تمام ژنراتورها است

$$\Delta\dot{F}_1(t) = -\frac{D_1}{2H_1}\Delta F_1(t) + \frac{1}{2H_1}\Delta P_{m_1}(t) + \frac{1}{2H_1}\Delta P_{tie_{12}}(t) - \frac{1}{2H_1}\Delta P_{L_1}(t) \quad (1)$$

$$\Delta\dot{F}_2(t) = -\frac{D_2}{2H_2}\Delta F_2(t) + \frac{1}{2H_2}\Delta P_{m_2}(t) + \frac{1}{2H_2}\Delta P_{tie_{12}}(t) - \frac{1}{2H_2}\Delta P_{L_2}(t) \quad (2)$$

با توجه به شکل ۱، سایر روابط حاکم بر مدل کنترلی در قالب (۳) تا (۱۳) آورده شده‌اند. معادلات (۳) و (۴) بیانگر توان مکانیکی توربین در هر ناحیه است

$$\Delta\dot{P}_{m_1}(t) = \frac{1}{T_{t_1}}\Delta P_{g_1}(t) - \frac{1}{T_{t_1}}\Delta P_{m_1}(t) \quad (3)$$

$$\Delta\dot{P}_{m_2}(t) = \frac{1}{T_{t_2}}\Delta P_{g_2}(t) - \frac{1}{T_{t_2}}\Delta P_{m_2}(t) \quad (4)$$

وجود حلقه کنترل ثانویه، منجر به شکل‌گیری سیگنال کنترلی ΔP_c مطابق (۵) و (۶) شده و همچنین تغییرات توان گاورنر در هر ناحیه، ΔP_g، به صورت (۷) و (۸) محاسبه می‌شود. در این روابط، ضریب بایاس فرکانسی B، مطابق با (۹) و (۱۰) قابل محاسبه است

$$\Delta\dot{P}_{c_1}(t) = K_{c_1} ACE_1(t) \quad (5)$$

$$\Delta\dot{P}_{c_2}(t) = K_{c_2} ACE_2(t) \quad (6)$$

$$\Delta\dot{P}_{g_1}(t) = -\frac{1}{R_1 T_{g_1}}\Delta F_1(t) - \frac{1}{T_{g_1}}\Delta P_{g_1}(t) + \frac{1}{T_{g_1}}\Delta P_{c_1}(t) \quad (7)$$

$$\Delta\dot{P}_{g_2}(t) = -\frac{1}{R_2 T_{g_2}}\Delta F_2(t) - \frac{1}{T_{g_2}}\Delta P_{g_2}(t) + \frac{1}{T_{g_2}}\Delta P_{c_2}(t) \quad (8)$$

$$B_1 = \frac{1}{R_1} + D_1 \quad (9)$$

$$B_2 = \frac{1}{R_2} + D_2 \quad (10)$$

رابطه (۱۱)، بیانگر توان عبوری از خطوط انتقال بین نواحی کنترلی است. در این رابطه، $P_{s_{12}}$ ضریب همگام‌سازی توان است که با راکتانس خط عبوری بین نواحی یک و دو رابطه عکس دارد

$$\Delta\dot{P}_{tie_{12}}(t) = P_{s_{12}}\Delta F_1(t) - P_{s_{12}}\Delta F_2(t) \quad (11)$$

در سیستم AGC چندناحیه‌ای، کنترل ثانویه علاوه بر تنظیم فرکانس هر ناحیه، توان خالص مبادله‌شده بین نواحی را نیز در مقادیر برنامه‌ریزی شده حفظ می‌نماید که این امر، با افزودن تغییرات توان عبوری از خطوط انتقال به انحراف فرکانس در حلقه فیدبک ثانویه محقق می‌شود. از این رو، سیگنال خطای کنترل ناحیه ACE، به صورت یک ترکیب خطی از انحراف فرکانس و تغییرات توان خطوط انتقال برای ناحیه کنترلی مطابق (۱۲) و (۱۳) بیان می‌شود

$$ACE_1(t) = -B_1\Delta F_1(t) - \Delta P_{tie_{12}}(t) \quad (12)$$

$$ACE_2(t) = -B_2\Delta F_2(t) + \Delta P_{tie_{12}}(t) \quad (13)$$

۳- مدل حمله

همان طور که پیشتر نیز اشاره گردید، در این مقاله به پیاده‌سازی و بررسی تأثیر دو حمله FDI و تأخیر که در شمار مهم‌ترین حملات سایبری به AGC هستند، پرداخته شده است.

حمله FDI، یکی از انواع حمله به یکپارچگی داده‌ها است که معمولاً از الگوهای از پیش تعریف شده برای تزریق، جعل و تغییر داده‌های واقعی پیروی می‌کند [۲۴]. برای حمله FDI الگوهای مختلفی در نظر گرفته شده که در ادامه به معرفی آنها می‌پردازیم [۲۵]:

- **حمله وزن‌دهی:** در این نوع حمله، داده‌های اندازه‌گیری یا فرمان‌های کنترلی جدید، بسته به ضریب وزن‌دهی، بیشتر و یا کمتر از مقادیر واقعی خواهند شد. از نظر ریاضی، این حمله با ضرب داده‌های اندازه‌گیری و فرمان‌های کنترلی واقعی در ضریب وزن‌دهی قابل پیاده‌سازی است.
- **حمله شیب[1]:** این حمله را می‌توان با افزودن سیگنال حمله وابسته به زمان، به داده‌های اندازه‌گیری و یا فرمان‌های کنترلی واقعی پیاده کرد. داده‌های اندازه‌گیری و یا فرمان‌های کنترلی جدید، بسته به شیب سیگنال حمله، با گذشت زمان کمتر و یا بیشتر از مقادیر واقعی خواهند شد.
- **حمله پله[2]:** این حمله با افزودن یک سیگنال مثبت یا منفی ثابت به داده‌های اندازه‌گیری و یا فرمان‌های کنترلی واقعی، قابل پیاده‌سازی است. این سیگنال جمع‌شونده، به طور پیوسته در شبکه وجود دارد.
- **حمله پالس[3]:** این حمله نیز مانند حمله پله، با افزودن یک سیگنال مثبت و یا منفی ثابت به داده‌های اندازه‌گیری و یا فرمان‌های کنترلی واقعی قابل پیاده‌سازی است، با این تفاوت که برخلاف حمله پله، سیگنال جمع‌شونده حمله پالس، در بازه زمانی محدودی در شبکه وجود دارد.
- **حمله تصادفی[4]:** در این حمله، مقادیر تصادفی به عنوان سیگنال حمله به داده‌های اندازه‌گیری و یا فرمان‌های کنترلی واقعی افزوده می‌شوند.

مطابق شکل ۱، در صورت وجود حمله FDI با در نظر گرفتن امکان حمله به فرکانس نواحی و توان عبوری بین دو ناحیه، (۱۲) و (۱۳) به (۱۴) و (۱۵) تبدیل می‌شوند [۹]. در حالت تئوری، امکان حمله FDI به فرکانس نواحی و توان عبوری از خطوط انتقال بین نواحی وجود دارد، اما از آنجایی که فرکانس، کمیتی سراسری است و مقدار آن در هر لحظه و در هر نقطه از ناحیه یکسان است، حمله به آن در عمل با موفقیت انجام نخواهد شد و خیلی سریع تشخیص داده می‌شود. از این رو، حمله به توان عبوری از خط انتقال بین نواحی متداول‌تر است

$$ACE_1(t) = -B_1(\Delta F_1(t) - d_1) - (\Delta P_{tie_{12}}(t) + d_2) \quad (14)$$

1. Ramp Attack
2. Step Attack
3. Pulse Attack
4. Random Attack

$$ACE_2(t) = -B_2(\Delta F_2(t) - d_2) + (\Delta P_{tie_{12}}(t) + d_2) \quad (۱۵)$$

حملات تأخیر، با اعمال تأخیر زمانی در ارسال داده‌های اندازه‌گیری و یا فرمان‌های کنترلی در سیستم‌های کنترلی القا می‌شوند. تأخیرهای قابل توجه در ارسال داده‌های اندازه‌گیری و یا فرمان‌های کنترلی منجر به تضعیف عملکرد سیستم کنترل فرکانس شده و نهایتاً ناپایداری فرکانس را به دنبال خواهد داشت. در صورتی که فرض شود امکان اعمال تأخیر در دریافت داده‌های اندازه‌گیری (سیگنال ACE) توسط کنترل‌کننده‌ها وجود دارد، تأثیر حمله تأخیر در (۱۶) و (۱۷) دیده می‌شود [۲۶]

$$\Delta \dot{P}_{c_1}(t) = K_{c_1} e^{-\tau_1 s} ACE_1(t) \quad (۱۶)$$

$$\Delta \dot{P}_{c_2}(t) = K_{c_2} e^{-\tau_2 s} ACE_2(t) \quad (۱۷)$$

در نهایت، معادلات و ماتریس‌های فضای حالت سیستم AGC دوناحیه‌ای شکل ۱ در (۱۸) تا (۲۵) ارائه شده است. بردار $\vec{Inj}_k$ شامل سه سیگنال ورودی d_1، d_2 و d_3 معرف حمله FDI و بردار $X(\tau)$ بیانگر حمله تأخیر به اندازه τ است

$$\dot{\vec{X}} = \bar{A}\vec{X} + \bar{E}\overrightarrow{X(\tau)} + \bar{B}\vec{U} + \bar{G}\overrightarrow{Inj} \quad (۱۸)$$

$$\vec{Y} = \bar{C}\vec{X} + \bar{F}\overrightarrow{X(\tau)} + \bar{D}\vec{U} + \bar{H}\overrightarrow{Inj} \quad (۱۹)$$

$$\bar{B} = \begin{bmatrix} -\frac{1}{2H_1} & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & -\frac{1}{2H_2} \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \quad (۲۰)$$

$$\bar{A} = \begin{bmatrix} -\frac{D_1}{2H_1} & 0 & \frac{1}{2H_1} & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2H_1} \\ -\frac{1}{R_1 T_{g_1}} & -\frac{1}{T_{g_1}} & 0 & \frac{1}{T_{g_1}} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{T_{t_1}} & -\frac{1}{T_{t_1}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{D_2}{2H_2} & 0 & \frac{1}{2H_2} & 0 & \frac{1}{2H_2} \\ 0 & 0 & 0 & 0 & -\frac{1}{R_2 T_{g_2}} & -\frac{1}{T_{g_2}} & 0 & \frac{1}{T_{g_2}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{T_{t_2}} & -\frac{1}{T_{t_2}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ P_{s_{12}} & 0 & 0 & 0 & -P_{s_{12}} & 0 & 0 & 0 & 0 \end{bmatrix} \quad (۲۱)$$

$$\bar{C} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (۲۲)$$

$$\bar{D} = 0 \quad (۲۳)$$

$$\bar{E} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -K_{c_1}B_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -K_{c_1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -K_{c_2}B_2 & 0 & 0 & 0 & K_{c_2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (۲۴)$$

$$\bar{F} = 0 \quad (۲۵)$$

٤- مدل دفاع

روش‌های دفاع سایبری، معمولاً از سه بخش تشخیص وجود حمله، تخمین حمله و حذف تأثیر آن و اصلاح داده‌های اندازه‌گیری تشکیل می‌شوند. به عبارت دیگر، ابتدا باید وجود حمله سایبری تشخیص داده شده و نوع حمله شناسایی و تخمین زده شود. پس از آن، با سازوکارهای مختلف می‌توان به حذف اثرات حمله و اصلاح داده‌های اندازه‌گیری پرداخت. با وجود این، یک الگوریتم تشخیص حمله باید بتواند اطلاعات مربوط به مکان، اندازه و زمان حمله را ارائه دهد [۲۷].

٤-۱ تشخیص وجود حمله سایبری

یکی از روش‌های تشخیص وجود حملات سایبری در شبکه، تحلیل رفتار آن در طول زمان با استفاده از مدل ریاضی شبکه است که رفتار آن را در حالت بدون حمله پیش‌بینی می‌کند. سپس رفتار تخمینی شبکه با داده‌های اندازه‌گیری مربوط مورد مقایسه قرار می‌گیرند. اختلاف قابل توجه بین این مقادیر، نشان‌دهنده وجود حمله در شبکه است [۸].

فیلتر کالمن به عنوان یک تخمین‌گر حالت می‌تواند با تخمین حالت شبکه، به منظور تشخیص و شناسایی حملات سایبری مورد استفاده قرار گیرد. ورودی‌های فیلتر کالمن شامل مدل و ورودی شبکه و ماتریس کوواریانس نویزهای اندازه‌گیری و فرایند هستند. تخمین متغیرهای حالت نیز خروجی فیلتر کالمن را تشکیل می‌دهند. مدل شبکه از طریق ماتریس‌های فضای حالت به فیلتر شناسانده می‌شود. از آنجایی که فیلتر کالمن در فضای گسسته عمل می‌کند، ضروری است تا ماتریس‌های فضای حالت شبکه با استفاده از (۲۶) تا (۲۹) از فضای پیوسته به گسسته تبدیل شوند

$$\overline{A_d} = e^{\bar{A}\times T_s} \quad (۲۶)$$

$$\overline{B_d} = \int_{\tau=۰}^{T_s} e^{\bar{A}\times\tau}\bar{B}\mathrm{d}\tau \quad (۲۷)$$

$$\overline{C_d} = \bar{C} \quad (۲۸)$$

$$\overline{D_d} = \bar{D} \quad (۲۹)$$

معادلات فضای حالت گسسته که به عنوان ورودی فیلتر کالمن مورد استفاده قرار می‌گیرند، در (۳۰) و (۳۱) ارائه شده‌اند. مدل فیلتر کالمن به عنوان یک تخمین‌گر، مطابق (۳۲) تا (۳۶) تعریف گردیده است [۹]. پس از پیش‌بینی متغیرهای حالت و ماتریس کوواریانس خطای تخمین به ترتیب در (۳۲) و (۳۳)، بهره فیلتر مطابق (۳۴) محاسبه شده و با استفاده از آن، ماتریس کوواریانس خطای تخمین و متغیرهای حالت برای گام kام به ترتیب در (۳۵) و (۳۶) تخمین زده می‌شوند

$$\overrightarrow{X_{k+۱}} = \overline{A_d}\overrightarrow{X_k} + \overline{B_d}\overrightarrow{U_k} + \overrightarrow{W_k} \quad (۳۰)$$

$$\overrightarrow{Y_k} = \overline{C_d}\overrightarrow{X_k} + \overline{D_d}\overrightarrow{U_k} + \overrightarrow{V_k} \quad (۳۱)$$

$$\overrightarrow{\widehat{X_{k|k-۱}}} = \overline{A_d}\overrightarrow{\widehat{X_{k-۱}}} + \overline{B_d}\overrightarrow{U_{k-۱}} \quad (۳۲)$$

$$\overline{P_{k|k-۱}} = \overline{A_d}\,\overline{P_{k-۱}}\,\overline{A_d^T} + \bar{Q} \quad (۳۳)$$

$$\overline{K_k} = \overline{P_{k|k-۱}}\,\overline{C_d^T}(\overline{C_d}\,\overline{P_{k|k-۱}}\,\overline{C_d^T} + \bar{R})^{-۱} \quad (۳۴)$$

$$\overline{P_{k|k}} = \overline{P_{k|k-۱}} - \overline{K_k}\,\overline{C_d}\,\overline{P_{k|k-۱}} \quad (۳۵)$$

$$\overrightarrow{\widehat{X_k}} = \overrightarrow{\widehat{X_{k|k-۱}}} + \overline{K_k}(\overrightarrow{Y_k} - \overline{C_d}\overrightarrow{\widehat{X_{k|k-۱}}}) \quad (۳۶)$$

یکی از معیارهای مقایسه رفتار تخمینی شبکه با داده‌های اندازه‌گیری مربوط، نُرم ماهالانوبیس باقیمانده خطای تخمین[1] و مقایسه آن با یک مقدار آستانه می‌باشد. باقیمانده خطای تخمین حالت با استفاده از (۳۷) قابل محاسبه است که در واقع، همان اختلاف داده‌های اندازه‌گیری و مقدار آنها بر اساس تخمین حالت در هر گام زمانی است. پس از آن، مطابق (۳۸)، نُرم ماهالانوبیس باقیمانده خطای تخمین در هر گام زمانی محاسبه می‌شود

$$\overrightarrow{r_k} = \overrightarrow{Y_k} - \overline{C_d}(\overline{A_d}\overrightarrow{\widehat{X_{k-۱}}} + \overline{B_d}\overrightarrow{U_{k-۱}}) \quad (۳۷)$$

$$norm_k = \overrightarrow{r_k}\bar{\varphi}\overrightarrow{r_k^T} \quad (۳۸)$$

به منظور تشخیص وجود حمله سایبری در شبکه، ابتدا مقدار متغیرهای حالت با استفاده از داده‌های اندازه‌گیری در هر لحظه محاسبه می‌شوند. از طرفی، تخمین‌گر حالت نیز مقدار متغیرهای حالت را در هر لحظه تخمین می‌زند. سپس نُرم اختلاف این دو مقدار در هر لحظه محاسبه شده و در صورتی که از مقدار از پیش تعیین شده به عنوان آستانه عبور کند، وجود حمله تشخیص داده می‌شود. به منظور تعیین آستانه در این مقاله، برخلاف کارهای قبلی از یک مدل آماری با فرض ثابت‌بودن تمامی شرایط از جمله شرایط آب و هوایی و میزان تولید و مصرف شبکه استفاده می‌شود. در پژوهش‌های انجام‌شده نظیر [۹]، برای تعیین آستانه در حالتی که شبکه تحت هیچ گونه حمله سایبری نباشد، نُرم ماهالانوبیس باقیمانده خطای تخمین محاسبه شده و عددی بزرگ‌تر از آن به عنوان آستانه در نظر گرفته شده که از آن به عنوان یک شاخص به منظور تشخیص وجود حمله در شبکه استفاده می‌گردد. در این مقاله، روشی جدید به منظور تعیین آستانه در فرایند تشخیص حمله پیشنهاد شده است، به این صورت که میانگین و انحراف معیار نُرم ماهالانوبیس باقیمانده خطای تخمین، هم در شرایط نرمال (عدم وجود حمله سایبری) و هم در صورت وجود حمله (با انجام شبیه‌سازی‌های مختلف و مکرر) محاسبه می‌شوند. μ_n، δ_n، μ_a و δ_a به ترتیب میانگین و انحراف معیار نُرم ماهالانوبیس باقیمانده خطای تخمین در شرایط نرمال و در صورت وجود حمله هستند. با در نظر گرفتن توزیع نرمال برای نُرم باقیمانده خطای تخمین، مطابق (۳۹) و (۴۰)، I_n بیانگر احتمال تشخیص حمله در صورت عدم وجود حمله، I_a بیانگر احتمال عدم تشخیص حمله در صورت وجود حمله سایبری و q_n و q_a ضرایب توزیع نرمال هستند. با انتخاب مقادیر مناسب برای q_n و q_a، مقدار آستانه به گونه‌ای تعیین شده که (۴۱) برقرار شود

$$I_n = \mu_n + q_n\delta_n \quad (۳۹)$$

$$I_a = \mu_a - q_a\delta_a \quad (۴۰)$$

$$I = I_n = I_a \quad (۴۱)$$

این روش تشخیص برای انواع حملات FDI و تأخیر و همچنین، حمله سایبری ترکیبی قابل استفاده است، به شرطی که دامنه حمله از انحراف معیار نویزهای موجود در شبکه بیشتر باشد. در غیر این صورت، حمله با نویز اشتباه گرفته شده و این روش، قادر به تشخیص آن نیست. با وجود این، در صورتی که دامنه حمله از انحراف معیار نویزهای موجود در شبکه کمتر باشد، حمله به قدری کوچک خواهد بود که فاقد تأثیر بوده و عدم تشخیص آن، مشکل‌ساز نخواهد شد.

۴-۲ تخمین اندازه حمله

پس از تشخیص وجود حمله مطابق با آنچه پیشتر ذکر گردید، نوبت به تخمین میزان حمله FDI و حمله تأخیر موجود در شبکه است تا به عنوان ورودی الگوریتم حذف تأثیر حمله، مورد استفاده قرار گیرد. معادلات فضای حالت سیستم دوناحیه‌ای با وجود حمله FDI در قالب (۴۲) و (۴۳) آورده شده‌اند. الگوریتم فیلتر کالمن بازگشتی سه‌مرحله‌ای به منظور تخمین بردار حمله FDI در (۴۴) تا (۵۵) ارائه شده است [۹]. این فیلتر شامل سه مرحله تحت عنوان به‌روزرسانی زمان، به‌روزرسانی داده‌های اندازه‌گیری و تخمین ورودی مجهول است. در مرحله اول، داده‌های اندازه‌گیری تا زمان $k-۱$ جمع‌آوری می‌شوند. سپس متغیرهای حالت بعدی شبکه با استفاده از (۴۴) پیش‌بینی شده و ماتریس کوواریانس خطای تخمین حالت در (۴۵) محاسبه می‌شود. در مرحله دوم، متغیرهای حالت شبکه با استفاده از داده اندازه‌گیری گام kام مطابق (۴۹) به‌روزرسانی می‌شوند. پس از آن، ماتریس کواریانس خطای تخمین حالت به‌روزرسانی شده، طبق (۵۰) محاسبه گردیده و سرانجام در مرحله آخر،

1. Mahalanobis Norm of Estimation Error Residual

ورودی مجهول که همان سیگنال حمله FDI است، بر اساس (۵۴) تخمین زده می‌شود. از این رو، پس از تخمین حمله FDI، بردار $\hat{Inj}_k$ به منظور جبران اثر حمله FDI و تخمین حالت واقعی شبکه در گام kام، از داده اندازه‌گیری دریافت‌شده کسر می‌گردد

$$\overrightarrow{X_{k+1}} = \overline{A_d}\overrightarrow{X_k} + \overline{B_d}\overrightarrow{U_k} + \overline{G_d}\overrightarrow{Inj_k} + \overrightarrow{W_k} \quad (۴۲)$$

$$\overrightarrow{Y_k} = \overline{C_d}\overrightarrow{X_k} + \overline{D_d}\overrightarrow{U_k} + \overline{H_d}\overrightarrow{Inj_k} + \overrightarrow{V_k} \quad (۴۳)$$

به‌روزرسانی زمان

$$\overrightarrow{\widehat{X_{k|k-1}}} = \overline{A_d}\overrightarrow{\widehat{X_{k-1|k-1}}} + \overline{B_d}\overrightarrow{U_{k-1}} + \overline{G_d}\overrightarrow{\widehat{Inj_{k-1}}} \quad (۴۴)$$

$$\overline{P^x_{k|k-1}} = \overline{A_d}\overline{P^x_{k|k-1}}\overline{A_d^T} + \overline{G_d}\overline{P^{xdT}_{k-1}}\overline{A_d^T} + \overline{A_d}\overline{P^{xd}_{k-1}}\overline{G_d^T} + \overline{G_d}\overline{P^{d}_{k-1}}\overline{G_d^T} + \overline{Q_{k-1}} \quad (۴۵)$$

$$\overline{\widetilde{R}_k} = (C_d)\overline{P^x_{k|k-1}}(C_d^T) + \overline{R_k} \quad (۴۶)$$

به‌روزرسانی داده‌های اندازه‌گیری

$$\overline{K_k} = \overline{P^x_{k|k-1}}\overline{C_d^T}\overline{\widetilde{R}_k}^{-1} \quad (۴۷)$$

$$\overline{L_k} = \overline{K_k}(\overline{I} - \overline{H_d}(\overline{H_d^T}\overline{\widetilde{R}_k}^{-1}\overline{H_d})^{-1}\overline{H_d^T}\overline{\widetilde{R}_k}^{-1}) \quad (۴۸)$$

$$\overrightarrow{\widehat{X_{k|k}}} = \overrightarrow{\widehat{X_{k|k-1}}} + \overline{L_k}(\overrightarrow{Y_k} - \overline{C_d}\overrightarrow{\widehat{X_{k|k-1}}}) - \overline{D_d}\overrightarrow{U_k} \quad (۴۹)$$

$$\overline{P^x_{k|k}} = (\overline{I} - \overline{L_k}\overline{C_d})\overline{P^x_{k|k-1}}(\overline{I} - \overline{L_k}\overline{C_d})^T + \overline{L_k}\overline{R_k}\overline{L_k^T} \quad (۵۰)$$

تخمین ورودی مجهول

$$\overline{\widetilde{R}_k^*} = (\overline{I} - \overline{C_d}\overline{L_k})\overline{\widetilde{R}_k}(\overline{I} - \overline{C_d}\overline{L_k})^T \quad (۵۱)$$

$$\overline{P_k^d} = (\overline{H_d^T}\overline{\widetilde{R}_k^*}\overline{H_d})^{-1} \quad (۵۲)$$

$$\overline{M_k} = \overline{P_k^d}\overline{H_d}\overline{\widetilde{R}_k^*}^{-1} \quad (۵۳)$$

$$\overrightarrow{\widehat{Inj_k}} = \overline{M_k}(\overrightarrow{Y_k} - \overline{C_d}\overrightarrow{\widehat{X_{k|k}}} - \overline{D_d}\overrightarrow{U_k}) \quad (۵۴)$$

$$\overline{P_k^{xd}} = -\overline{P^x_{k|k}}\overline{C_d^T}\overline{M_k^T} + \overline{L_k}\overline{R_k}\overline{M_k^T} \quad (۵۵)$$

معادلات (۵۶) تا (۶۲) به منظور تخمین میزان تأخیر موجود در شبکه ناشی از حمله تأخیر، مورد استفاده قرار می‌گیرند [۲۲]. مطابق معادلات فضای حالت سیستم، با استفاده از (۵۶) بردار تخمین حالت استخراج می‌شود. با وجود تأخیر در سیستم به میزان τ، (۵۶) به (۵۷) و (۵۸) تبدیل می‌شود. رابطه (۵۷) بیانگر بردار متغیرهای حالت سیستم با در نظر گرفتن میزان واقعی تأخیر است و (۵۸) بردار متغیرهای حالت با در نظر گرفتن میزان تخمین زده شده تأخیر موجود در شبکه به اندازه $\hat{\tau}$ است. خطای تخمین حالت با وجود تأخیر در شبکه به صورت (۵۹) بیان می‌گردد و هدف، یافتن $\hat{\tau}$ به ازای کمینه‌شدن $\vec{e}_m$ است. با استفاده از روش گرادیان نزولی، (۶۰) به دست آمده که در آن η، نرخ یادگیری است. با جایگذاری (۵۹) و (۶۱) در (۶۰) و با فرض مقدار اولیه $\vec{U}(0)=0$، (۶۲) استخراج شده که با حل آن $\hat{\tau}$ به دست آمده و تأخیر موجود در شبکه تخمین زده می‌شود. اکنون $\hat{\tau}$ به عنوان یکی دیگر از ورودی‌های الگوریتم فیلتر کالمن مورد استفاده قرار می‌گیرد

$$\overrightarrow{X(t)} = e^{\overline{A}t}\overrightarrow{X_0} + \int_0^t e^{\overline{A}(t-s)}\overline{B}\overrightarrow{U(s)}\mathrm{d}s \quad (۵۶)$$

$$\overrightarrow{X(t-\tau)} = e^{\overline{A}(t-\tau)}\overrightarrow{X_0} + \int_0^{t-\tau} e^{\overline{A}(t-\tau-s)}\overline{B}\overrightarrow{U(s)}\mathrm{d}s \quad (۵۷)$$

$$\overrightarrow{X(t-\hat{\tau})} = e^{\overline{A}(t-\hat{\tau})}\overrightarrow{X_0} + \int_0^{t-\hat{\tau}} e^{\overline{A}(t-\hat{\tau}-s)}\overline{B}\overrightarrow{U(s)}\mathrm{d}s \quad (۵۸)$$

$$\overrightarrow{e_m} = \overrightarrow{X(t-\tau)} - \overrightarrow{X(t-\hat{\tau})} \quad (۵۹)$$

$$\frac{\mathrm{d}\hat{\tau}}{\mathrm{d}t} = -\frac{\partial V}{\partial \hat{\tau}} \quad (۶۰)$$

$$V = \frac{1}{2}e_m^2 \quad (۶۱)$$

$$\frac{\mathrm{d}\hat{\tau}}{\mathrm{d}t} = -\overrightarrow{e_m}(\overline{B}\overrightarrow{U(t-\hat{\tau})} - \overline{A}e^{\overline{A}(t-\hat{\tau})}\overrightarrow{X_0}) \quad (۶۲)$$

روش پیشنهادی در مقاله حاضر، برخلاف ادبیات موجود، قابلیت تشخیص هر دو حمله FDI و تأخیر و حمله سایبری ترکیبی را دارد. در صورتی که تأخیر تخمین زده شده، صفر و حداقل یکی از درایه‌های $\hat{Inj}_k$، غیر صفر باشد، حمله از نوع FDI بوده و در صورتی که تمامی درایه‌های بردار تخمین زده شده سیگنال حمله FDI، $\hat{Inj}_k$، صفر و $\hat{\tau}$ غیر صفر باشد، حمله از نوع تأخیر تشخیص داده می‌شود. حمله موجود در شبکه در صورتی از نوع حمله سایبری ترکیبی است که $\hat{\tau}$ و همچنین حداقل یکی از درایه‌های $\hat{Inj}_k$، غیر صفر باشد.

۴-۳ اصلاح تأثیر حمله

معادلات (۶۳) تا (۸۱) به منظور حذف تأثیر حمله سایبری ترکیبی از داده‌های اندازه‌گیری نوشته شده‌اند. دو معادله (۶۳) و (۶۴) بیانگر معادلات فضای حالت سیستم تحت حمله سایبری شامل حمله تأخیر به میزان $\hat{\tau}$ در دریافت ورودی‌ها توسط کنترل‌کننده AGC و حمله FDI هستند. با استفاده از ماتریس‌های تبدیل (۶۵) تا (۶۸)، (۶۳) و (۶۴) به (۶۹) و (۷۰) تبدیل شده و به این ترتیب عملاً تأثیر وجود حمله از بین رفته و می‌توان از آنها به عنوان ورودی فیلتر کالمن استفاده نمود. سایر روابط، به منظور تخمین حالت سیستم نوشته شده‌اند. مطابق آنچه پیشتر ذکر گردید، پس از جمع‌آوری داده‌های اندازه‌گیری تا گام $k-1$، متغیرهای حالت در (۷۱) به‌روزرسانی شده و در (۷۲) ماتریس کوواریانس خطای تخمین حالت، محاسبه گردیده است. پس از آن، مطابق با (۷۶) و (۷۷) متغیرهای حالت شبکه و ماتریس کواریانس خطای تخمین حالت با استفاده از داده‌های اندازه‌گیری گام kام به‌روزرسانی می‌شوند

$$\overrightarrow{X_{k+1}} = \overline{A_d}\overrightarrow{X_k} + \overline{E_d}\overrightarrow{X_k(\hat{\tau})} + \overline{B_d}\overrightarrow{U_k} + \overline{G_d}\overrightarrow{Inj_k} + \overrightarrow{W_k} \quad (۶۳)$$

$$\overrightarrow{Y_k} = \overline{C_d}\overrightarrow{X_k} + F\overrightarrow{X_k(\hat{\tau})} + \overline{D_d}\overrightarrow{U_k} + \overline{H_d}\overrightarrow{Inj_k} + \overrightarrow{V_k} \quad (۶۴)$$

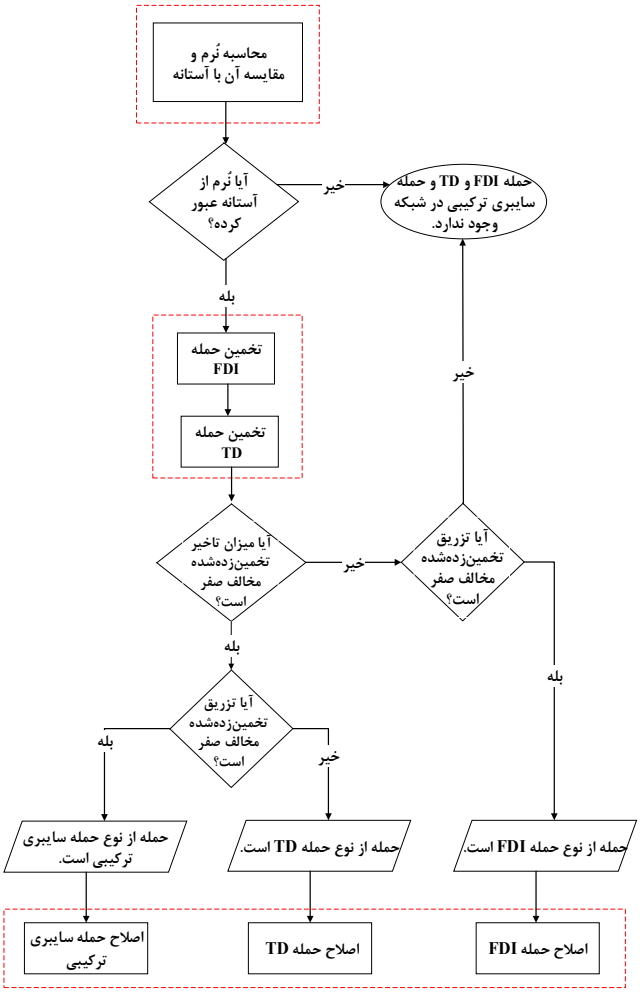
$$\overline{A'_d} = \begin{bmatrix} \overline{A_d} & \overline{E_d} \\ \overline{I_n} & 0 \end{bmatrix} \quad (۶۵)$$

$$\overline{B'_d} = \begin{bmatrix} \overline{B_d} \\ 0 \end{bmatrix} \quad (۶۶)$$

$$\overline{C'_d} = \begin{bmatrix} \overline{C_d} & 0 \end{bmatrix} \quad (۶۷)$$

$$\overline{D'_d} = \overline{D_d} \quad (۶۸)$$

$$\overrightarrow{X_{k+1}} = \overline{A'_d}\overrightarrow{X_k} + \overline{B'_d}\overrightarrow{U_k} + \overline{G_d}\overrightarrow{Inj_k} + \overrightarrow{W_k} \quad (۶۹)$$



شکل ۲: روندنمای حل مسئله.

$$\overrightarrow{Y_k} = \overline{C'_d}\overrightarrow{X_k} + \overline{D'_d}\overrightarrow{U_k} + \overline{H_d}\overrightarrow{Inj_k} + \overrightarrow{V_k} \quad (۷۰)$$

به‌روزرسانی زمان

$$\overrightarrow{\widehat{X_{k|k-1}}} = \overline{A'_d}\overrightarrow{\widehat{X_{k-1|k-1}}} + \overline{B'_d}\overrightarrow{U_{k-1}} + \overline{G_d}\overrightarrow{\widehat{Inj_{k-1}}} \quad (۷۱)$$

$$\overline{P^x_{k|k-1}} = \overline{A'_d}\,\overline{P^x_{k|k-1}}\,\overline{A'^T_d} + \overline{G_d}\,\overline{P^{xd\,T}_{k-1}}\,\overline{A'^T_d} + \overline{A'_d}\,\overline{P^{xd}_{k-1}}\,\overline{G^T_d} + \overline{G_d}\,\overline{P^d_{k-1}}\,\overline{G^T_d} + \overline{Q_{k-1}} \quad (۷۲)$$

$$\overline{\widetilde{R_k}} = \overline{C'_d}\,\overline{P^x_{k|k-1}}\,\overline{C'^T_d} + \overline{R_k} \quad (۷۳)$$

به‌روزرسانی داده‌های اندازه‌گیری

$$\overline{K_k} = \overline{P^x_{k|k-1}}\,\overline{C'^T_d}\,\overline{\widetilde{R_k}}^{-1} \quad (۷۴)$$

$$\overline{L_k} = \overline{K_k}(\overline{I} - \overline{H_d}(\overline{H^T_d}\,\overline{\widetilde{R_k}}^{-1}\,\overline{H_d})^{-1}\,\overline{H^T_d}\,\overline{\widetilde{R_k}}^{-1}) \quad (۷۵)$$

$$\overrightarrow{\widehat{X_{k|k}}} = \overrightarrow{\widehat{X_{k|k-1}}} + \overline{L_k}(\overrightarrow{Y_k} - \overline{C'_d}\,\overrightarrow{\widehat{X_{k|k-1}}}) - \overline{D'_d}\,\overrightarrow{U_k} \quad (۷۶)$$

$$\overline{P^x_{(k|k)}} = (\overline{I} - \overline{L_k C'_d})\,\overline{P^x_{(k|k-1)}}\,(\overline{I} - \overline{L_k C'_d})^T + \overline{L_k}\,\overline{R_k}\,\overline{L^T_k} \quad (۷۷)$$

$$\overline{\widetilde{R_k}^*} = (\overline{I} - \overline{C'_d L_k})\,\overline{\widetilde{R_k}}\,(\overline{I} - \overline{C'_d L_k})^T \quad (۷۸)$$

$$\overline{P^d_k} = (\overline{H^T_d}\,\overline{\widetilde{R_k}^*}\,\overline{H_d})^{-1} \quad (۷۹)$$

$$\overline{M_k} = \overline{P^d_k}\,\overline{H_d}\,\overline{\widetilde{R_k}^*}^{-1} \quad (۸۰)$$

$$\overline{P^{xd}_k} = -\overline{P^x_{k|k}}\,\overline{C'^T_d}\,\overline{M^T_k} + \overline{L_k}\,\overline{R_k}\,\overline{M^T_k} \quad (۸۱)$$

هدف اصلی مقاله حاضر، ارائه یک روش دفاع است که با ترکیب روش‌های موجود، قابلیت تشخیص، تخمین و اصلاح تأثیر حملات FDI و تأخیر را داشته باشد. روش پیشنهادی قابلیت استفاده در مراکز کنترل را داشته و می‌تواند به عنوان روش دفاع در برابر انواع حملات FDI و تأخیر کارامد واقع شود. از آنجایی که در شبکه‌های چندناحیه‌ای، هر ناحیه یک کنترل‌کننده مجزا داشته که مستقل از نواحی دیگر عمل می‌کند، الگوریتم دفاع پیشنهادی باید در هر ناحیه پیاده‌سازی شود. در صورت وجود حمله در یک ناحیه، وجود حمله در نواحی دیگر تشخیص داده می‌شود اما پس از تخمین نوع حمله، در صورت وجود حمله FDI به فرکانس ناحیه و یا حمله تأخیر، الگوریتم مربوط به اصلاح تأثیر حمله متناسب با نوع حمله در ناحیه مورد هدف اجرا شده و بدین ترتیب، تأثیر حمله حذف می‌شود. اما در صورت حمله به توان عبوری از خط انتقال بین نواحی، از آنجایی که مقدار توان برای محاسبه سیگنال ACE در هر دو ناحیه لازم است، ضروری است که اندازه‌گیری‌های توان در هر دو ناحیه اصلاح شوند. به منظور درک بهتر مطالب ارائه‌شده در خصوص روند حل مسئله توسط الگوریتم دفاع پیشنهادی، روندنمای حل مسئله در شکل ۲ ارائه شده است.

۵- مطالعه موردی و نتایج عددی

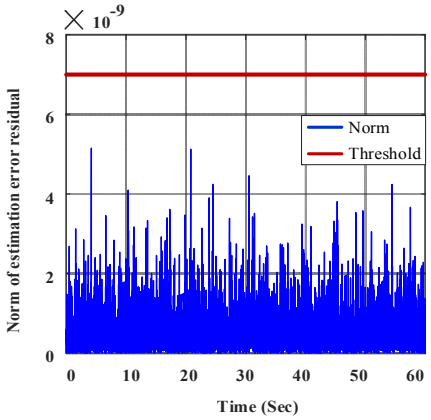
در این بخش، به بررسی عملکرد الگوریتم پیشنهادی بر روی شبکه دوناحیه‌ای شکل ۱ با مشخصات جدول ۲ پرداخته شده است. به این منظور، آزمایش‌هایی در قالب سناریوهای مختلف مطابق جدول ۳، طراحی گردیده که در هر سناریو تأثیر حمله و کارایی الگوریتم پیشنهادی در تشخیص، تخمین و اصلاح تأثیر حمله پیاده‌سازی شده، مورد بررسی قرار گرفته است. انواع دیگر آزمایش‌ها از قبیل حمله FDI به ΔF و انواع دیگر حملات سایبری ترکیبی نیز قابل انجام است که به دلیل کاهش حجم مطالب، از ارائه آنها خودداری شده است؛ لیکن علاقه‌مندان با ارجاع به [۲۸] می‌توانند به سایر آزمایش‌ها دسترسی پیدا کنند.

در تمامی آزمایش‌های انجام‌شده، فرض گردیده که در شبکه نویزهای اندازه‌گیری و فرایند از نوع نویز سفید با توزیع گوسی با مقدار میانگین صفر و انحراف معیاری برابر با 10^{-5} وجود دارد. پیش از انجام آزمایش‌ها، مطابق آنچه پیشتر در خصوص نحوه تشخیص حمله ارائه شده است، لازم است مقدار آستانه تعیین شود. به این منظور، نُرم ماهالانوبیس باقیمانده خطای تخمین تحت شرایط زیر برای هر دو ناحیه مطابق شکل ۳، محاسبه شده که با توجه به روش پیشنهادی، مقدار 7×10^{-9} برای آستانه در هر دو ناحیه کنترلی به دست آمده است.

- عدم وجود حمله سایبری در شبکه دوناحیه‌ای شکل ۱
- افزایش بار ناحیه اول به میزان ۰/۰۴ پریونیت بار کل ناحیه
- وجود نویزهای اندازه‌گیری و فرایند از نوع نویز سفید با توزیع گوسی با مقدار میانگین صفر و انحراف معیار 10^{-5}

۵-۱ بررسی تأثیر پارامترهای کنترلی

بهره کنترل‌کننده K_c از جمله عواملی است که در عملکرد کنترل ثانویه فرکانس از نظر سرعت، زمان و نحوه کنترل فرکانس تأثیر به‌سزایی دارد. در شکل ۴- الف، انحراف فرکانس به ازای بهره‌های مختلف از ۰/۰۱ تا ۱ ارائه شده است. مطابق با شکل، هرچه میزان K_c بزرگ‌تر باشد، عکس‌العمل سیستم کنترل فرکانس شدیدتر بوده، میزان فراجهش‌ها و نوسانات بیشتر شده و انحراف فرکانس در مدت زمان کمتری صفر



شکل ۳: نُرم ماهالانوبیس و تعیین آستانه.

جدول ۲: مشخصات سیستم AGC دوناحیه‌ای [۹].

پارامترها	ناحیه ۱	ناحیه ۲	پارامترها	ناحیه ۱	ناحیه ۲
D (PU/Hz)	۰٫۶	۰٫۳	T_t (sec)	۰٫۵	۰٫۶
H (sec)	۵	۴	K_c	۰٫۱	۰٫۱
R (Hz/PU)	۰٫۰۵	۰٫۰۶۲۵	$P_{s_{12}}$ (PU/Hz)	۲	۲
B (PU/Hz)	۲۰٫۶	۱۶٫۳	DB (mHz)	۲۰	۲۰
T_g (sec)	۰٫۲	۰٫۳	ΔP_l (PU)	۰٫۰۴	۰
μ_{noise}	۰	۰	*Transmission delay* (*mS*)	۱۰۰	۱۰۰
δ_{noise}	$۱۰^{-۵}$	$۱۰^{-۵}$			

جدول ۳: آزمایش‌های انجام‌شده.

زیربخش	شرح آزمایش	هدف
۵-۱	تغییر مقدار پارامترهای K_c و B	– بررسی عملکرد سیستم AGC ناشی از مقادیر مختلف پارامترهای K_c و B
۵-۲	اعمال مقادیر مختلف حمله تأخیر در دریافت داده‌های اندازه‌گیری توسط کنترل‌کننده ناحیه اول	– بررسی عملکرد سیستم AGC با وجود حمله تأخیر – بررسی کیفیت عملکرد روش دفاع پیشنهادی در تشخیص، تخمین و اصلاح تأثیر حمله تأخیر
۵-۳	اعمال حمله تأخیر در ناحیه اول + حمله FDI از نوع شیب به $\Delta P_{tie_{12}}$	– بررسی عملکرد سیستم AGC با وجود حمله سایبری ترکیبی
۵-۴	اعمال حمله تأخیر در ناحیه اول + حمله FDI از نوع پله به $\Delta P_{tie_{12}}$	– بررسی کیفیت عملکرد روش دفاع پیشنهادی در تشخیص، تخمین و اصلاح تأثیر حمله سایبری ترکیبی
۵-۵	اعمال حمله تأخیر در ناحیه اول + حمله FDI از نوع پالس به $\Delta P_{tie_{12}}$	

می‌شود؛ به گونه‌ای که به ازای $K_c = ۱$، فرکانس در ثانیه ۴۵ام به مقدار ۶۰ هرتز رسیده است، اما با انتخاب $K_c = ۰٫۰۱$، پس از گذشت یک دقیقه نیز انحراف فرکانس به مقدار صفر نرسیده و به بیان دیگر، عملکرد کنترل‌کننده نرم‌تر و کندتر است. از دیگر عواملی که در عملکرد کنترل ثانویه از نظر سرعت، زمان و نحوه کنترل فرکانس ایفای نقش می‌کند، می‌توان به ضریب بایاس فرکانسی B اشاره نمود. انحراف فرکانس به ازای مقادیر مختلف برای بایاس فرکانسی ۱ تا ۸۰ پریونیت بر هرتز در شکل ۴- ب ارائه شده است. مطابق با شکل، هرچه B بزرگ‌تر باشد، عکس‌العمل سیستم کنترل فرکانس شدیدتر و با فراجهش‌ها و نوسانات بیشتری همراه بوده و انحراف فرکانس در مدت زمان کمتری کاهش می‌یابد؛ به گونه‌ای که به ازای $B = ۸۰\,\text{pu/Hz}$، فرکانس در ثانیه ۲۰ام به مقدار ۶۰ هرتز رسیده است، اما با در نظر گرفتن $B = ۱\,\text{pu/Hz}$، پس از گذشت ۱ دقیقه، انحراف فرکانس همچنان به مقدار صفر نرسیده است. از این رو برای انتخاب K_c و B، مد نظر قرار دادن میزان فراجهش‌ها و نوسانات و همچنین مدت زمان پایدارشدن فرکانس ضروری است.

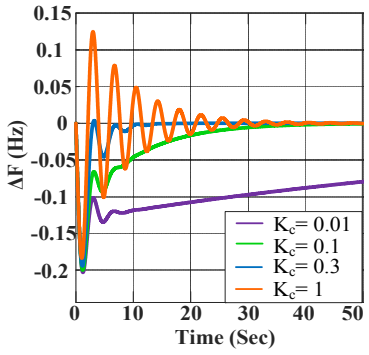
از آنجایی که کنترل ثانویه به صورت سراسری عمل می‌کند، لازم است تا داده‌هایی نظیر میزان تولید واحدها و فرمان‌های کنترلی و همچنین توان عبوری از خطوط انتقال از طریق شبکه مخابراتی به/ از مرکز کنترل ارسال شوند. از این رو، تأخیر مسیرهای ارتباطی مختلف می‌تواند بر سرعت انتقال داده‌های فوق و در نتیجه، عملکرد کنترل ثانویه فرکانس تأثیر داشته باشد. در شکل ۴- ج انحراف فرکانس با در نظر گرفتن فیبر نوری به عنوان جنس مسیر ارتباطی و فرض وجود تأخیر به میزان ۱۰۰ میلی‌ثانیه در دریافت داده‌ها نشان داده شده است. در این آزمایش، پارامترهای K_c و B به گونه‌ای انتخاب شده‌اند که AGC به نرمی و بدون فراجهش‌های شدید در فرکانس، در مدت زمان معقولی به تثبیت فرکانس بپردازد. مطابق شکل، تأخیر ناچیز مسیر ارتباطی، خللی در عملکرد کنترل فرکانس ایجاد نمی‌کند؛ اما تأخیرهای بیشتر ناشی از عوامل مختلف نظیر حمله سایبری که در ادامه به آن پرداخته شده است، می‌تواند عملکرد AGC را مختل سازد.

۵-۲ سناریوی تأخیر

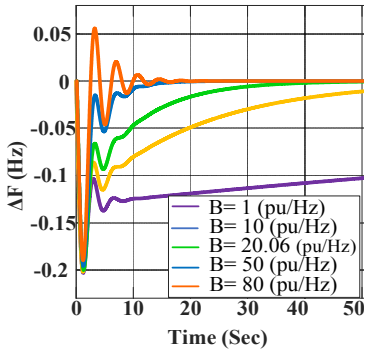
در این سناریو، تأثیر حمله تأخیر با دامنه‌های مختلف از ۰٫۵ ثانیه تا چهار ثانیه در ارسال داده‌های اندازه‌گیری در ثانیه اول شبیه‌سازی در ناحیه اول مورد بررسی قرار گرفته است. در شکل ۵- الف، نمودارهای انحراف فرکانس ناحیه اول به ازای مقادیر مختلف تأخیر ارائه شده‌اند. پارامترهای K_c و B در این آزمایش به گونه‌ای انتخاب شده‌اند که AGC به نرمی و بدون فراجهش‌های شدید در فرکانس، در مدت زمان معقولی به تثبیت فرکانس بپردازد. از این رو، حمله تأخیر حتی تا چهار ثانیه نیز تأثیر چندان شدید و مخربی بر پایداری نداشته است. با وجود این، در صورت انتخاب و تنظیم نامناسب ضرایب کنترل‌کننده‌ها، مقادیر کوچک تأخیر نیز منجر به ناپایداری می‌گردند. به منظور بررسی عملکرد روش دفاع پیشنهادی در جبران تأثیر حمله تأخیر، فرض می‌شود که حمله تأخیر با میزان چهار ثانیه در ارسال داده‌های اندازه‌گیری $\Delta F_۱$ و $\Delta P_{tie_{12}}$، به مرکز کنترل ناحیه اول اعمال شده است. در شکل ۵- ب، انحراف فرکانس ناحیه اول در پی وقوع حمله تأخیر آمده است. در صورت استفاده از الگوریتم پیشنهادی، وجود حمله مطابق شکل ۵- ج، توسط هر دو ناحیه تشخیص داده شده است (نُرم باقیمانده خطای تخمین و مقدار آستانه در هر دو ناحیه مشابه است). پس از تخمین میزان حمله تأخیر و تشخیص این که حمله در کدام ناحیه وجود دارد، الگوریتم اصلاح، تنها در ناحیه اول عمل کرده و نمودار $\Delta F_۱$ مطابق نمودار آبی‌رنگ در شکل ۵- ب اصلاح شده است. از آنجایی که تأخیر ناشی از حمله در ناحیه دوم اثرگذار نیست، نمودار $\Delta F_۲$ در صورت وجود حمله در ناحیه اول بر حالتی که در ناحیه اول حمله وجود ندارد، مطابق شکل ۵- د منطبق است.

۵-۳ سناریو تأخیر و شیب

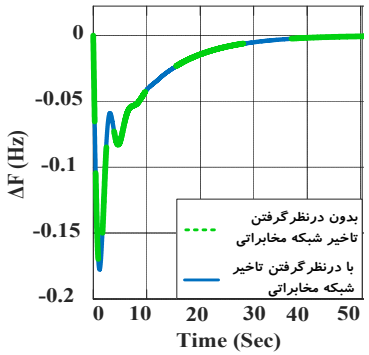
شکل‌های ۶- الف تا ۶- ج به ترتیب نمودارهای $\Delta F_۱$، $\Delta P_{tie_{12}}$ و $\Delta F_۲$



(الف)



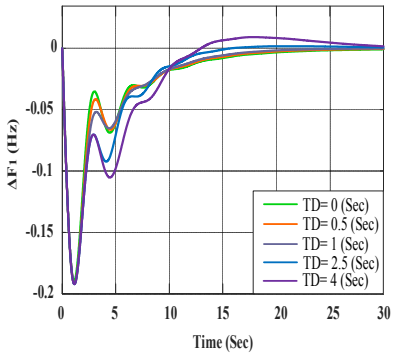
(ب)



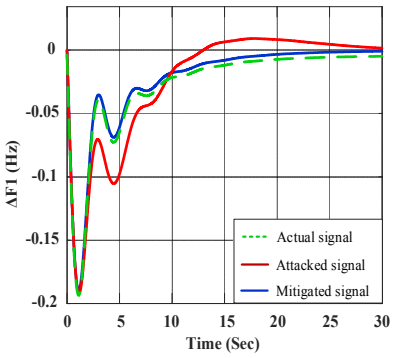
(ج)

شکل ۴: بررسی تأثیر پارامترهای کنترلی، (الف) تأثیر K_c روی ΔF، (ب) تأثیر B روی ΔF و (ج) نمودار ΔF با درنظرگرفتن تأخیر انتقال.

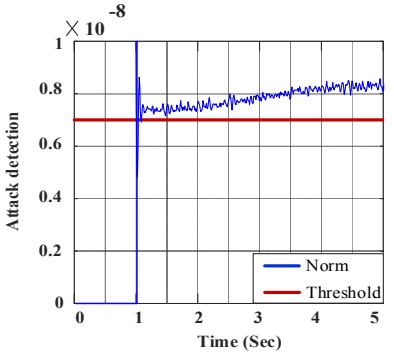
را با وجود حمله ترکیبی شامل حمله تأخیر و FDI با شیب ۰/۰۰۱ به $\Delta P_{tie_{۲}}$ در ثانیه یکم نشان می‌دهند. با افزایش بار ناحیه اول، فرکانس این ناحیه کاهش پیدا می‌کند و به دنبال آن، توان از ناحیه دوم به ناحیه اول انتقال پیدا کرده و به بیان دیگر، $\Delta P_{tie_{۲}}$ منفی شده است. با اعمال حمله شیب به $\Delta P_{tie_{۲}}$، مقادیر عددی $\Delta P_{tie_{۲}}$ دریافت‌شده توسط AGC کمتر از مقدار واقعی است. از این رو، سیگنال ACE کوچک‌تر از مقدار واقعی محاسبه شده و نهایتاً میزان افزایش تولید واحدها، کمتر از میزان مطلوب بوده که این امر منجر به افت بیشتر فرکانس گردیده است؛ به گونه‌ای که مطابق با شکل ۶- الف، AGC قادر به بازگرداندن فرکانس به مقدار نامی نبوده است. به بیان دیگر، مشتق سیگنال حمله شیب در حلقه کنترلی منجر به ایجاد خطای حالت ماندگار در $\Delta F_{۱}$ شده است. مطابق با شکل ۶- ب، $\Delta P_{tie_{۲}}$ نیز به دنبال افت بیشتر فرکانس، بیش از پیش کاهش یافته و به عبارت دیگر، توان بیشتری از ناحیه دوم به ناحیه اول منتقل گردیده و AGC قادر به کنترل توان عبوری بین نواحی در مقدار برنامه‌ریزی شده، نبوده است. نُرم محاسبه‌شده در الگوریتم پیشنهادی، مطابق شکل ۶- د، با عبور از مقدار آستانه، بیانگر وجود حمله سایبری در شبکه است. پس از آن، سیگنال حمله FDI در هر دو ناحیه به صورت



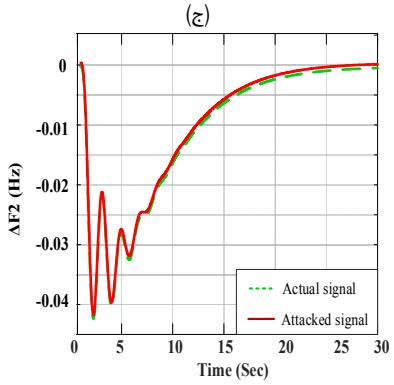
(الف)



(ب)



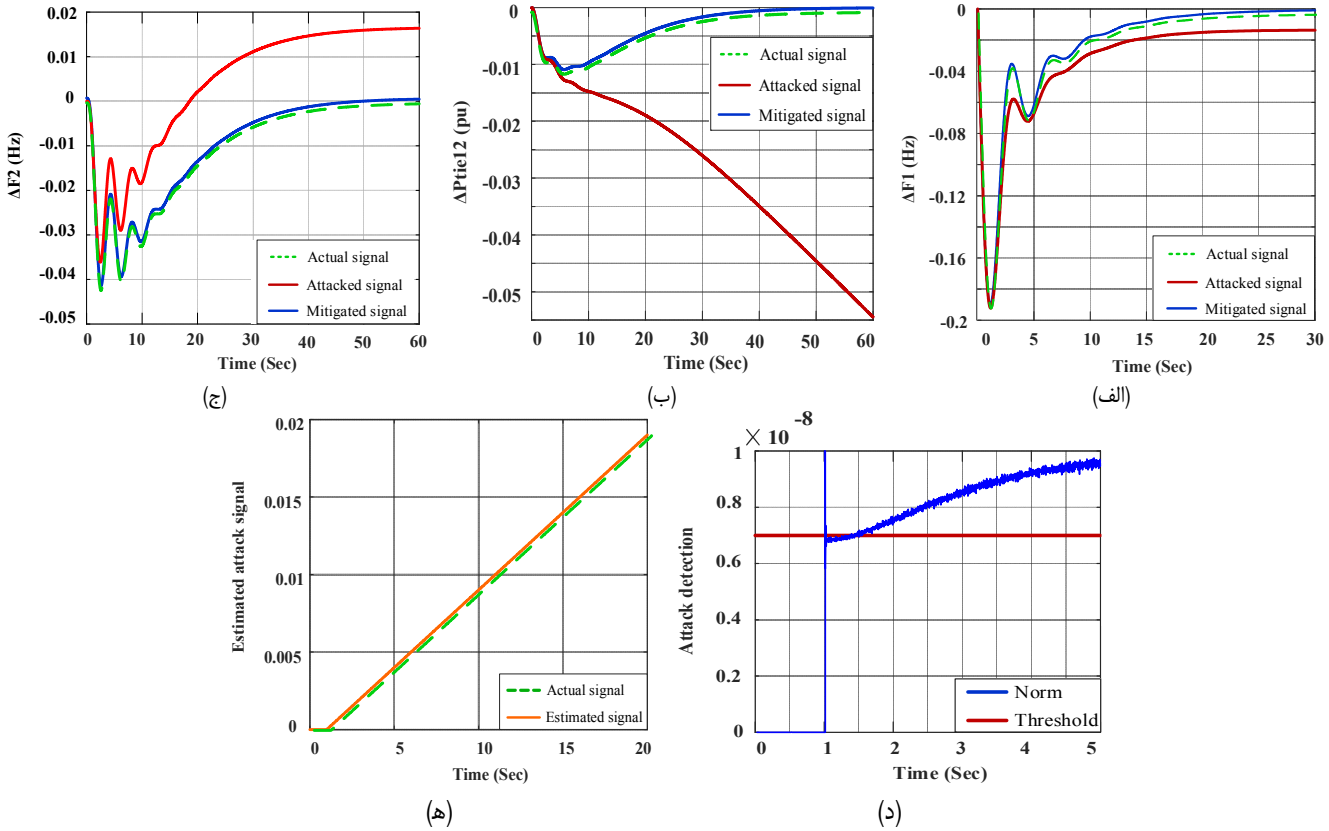
(ج)



(د)

شکل ۵: حمله تأخیر با میزان چهار ثانیه در ارسال داده‌های اندازه‌گیری $\Delta F_{۱}$ و $\Delta P_{tie_{۲}}$ به مرکز کنترل ناحیه اول، (الف) تأثیر حمله تأخیر در $\Delta F_{۱}$، (ب) نمودار $\Delta F_{۱}$ ناشی از چهار ثانیه حمله تأخیر، (ج) تشخیص حمله تأخیر و (د) نمودار $\Delta F_{۲}$ ناشی از حمله تأخیر در ناحیه اول.

شکل ۶- ه تخمین زده شده است. از آنجایی که حمله تأخیر تنها در ناحیه اول وجود دارد، الگوریتم اصلاح در ناحیه دوم مطابق شکل ۶- ج فقط به اصلاح تأثیر حمله شیب پرداخته و مطابق شکل، پس از اصلاح حمله، داده‌های اندازه‌گیری $\Delta F_{۲}$ بر داده‌های واقعی منطبق شده که این امر، حاکی از بی‌اثربودن حمله تأخیر در ناحیه اول بر ناحیه دوم است. نهایتاً پس از اصلاح تأثیر حمله شیب تخمین زده شده و تأخیر یک ثانیه‌ای در



شکل ۶. حمله ترکیبی شامل حمله تأخیر و شیب به $\Delta P_{tie_{12}}$، (الف) نمودار ΔF_1 ناشی از حمله شیب و تأخیر، (ب) نمودار $\Delta P_{tie_{12}}$ ناشی از حمله شیب و تأخیر، (ج) نمودار ΔF_2 ناشی از حمله شیب و تأخیر، (د) تشخیص حمله شیب در حمله سایبری ترکیبی و (ه) تخمین سیگنال حمله شیب در حمله سایبری ترکیبی.

ناحیه اول، نمودارهای ΔF_1 و $\Delta P_{tie_{12}}$ به ترتیب مطابق شکل‌های ۶- الف و ۶- ب با تقریب خوبی (تقریب ناشی از نویزهای فرایند و اندازه‌گیری و تأثیر آنها بر تخمین متغیرهای حالت و تخمین سیگنال حمله) اصلاح شده و با نمودارهای واقعی منطبق است.

۵-۴ سناریوی تأخیر و پله

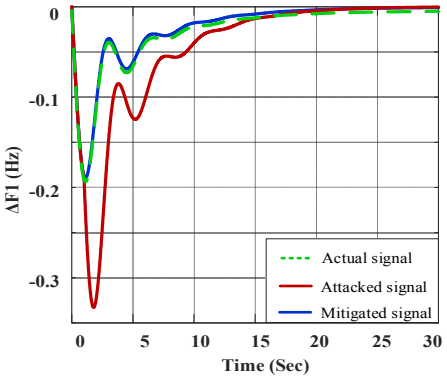
در آزمایش بعدی، فرض شده که حمله سایبری ترکیبی شامل یک ثانیه حمله تأخیر و حمله پله با دامنه ۰/۰۵ به $\Delta P_{tie_{12}}$ از ثانیه یکم است. در این حالت نیز مشابه سناریوی قبل، با افزایش بار ناحیه اول، فرکانس این ناحیه مطابق با نمودار قرمز شکل ۷- الف، کاهش پیدا کرده و به دلیل وجود حمله پله با دامنه مثبت، AGC انحراف توان کمتری نسبت به مقادیر واقعی دریافت می‌کند. از این رو، دستور افزایش تولید واحدهای ناحیه اول به منظور جبران افزایش بار، کمتر از مقدار لازم بوده و این امر مطابق با شکل‌های ۷- الف و ۷- ب منجر به افت بیشتر فرکانس و $\Delta P_{tie_{12}}$ می‌شود. نوع حمله FDI در این آزمایش، به گونه‌ای است که مشتق آن در حلقه کنترلی صفر شده و از این رو، خطای حالت ماندگار در فرکانس دیده نمی‌شود. از طرفی انحراف توان عبوری بین نواحی نیز در نهایت توسط AGC در مقدار ۰/۰۵- پریونیت پایدار شده که نشان‌دهنده اختلال در عملکرد AGC است. پس از محاسبه نُرم و تشخیص وجود حمله مطابق شکل ۷- ج، سیگنال حمله پله به صورت شکل ۷- د در هر دو ناحیه به درستی تخمین زده شده است. پس از جبران حمله سایبری ترکیبی در ناحیه اول و حمله پله در ناحیه دوم، AGC به جای دریافت مقادیر اشتباه (نمودارهای قرمز)، مقادیر واقعی و صحیح (نمودارهای آبی) ΔF_1 و $\Delta P_{tie_{12}}$ را مطابق شکل‌های ۷- الف و ۷- ب دریافت می‌کند. از این رو عملکرد سیستم کنترل فرکانس با به کارگیری الگوریتم پیشنهادی، تحت تأثیر حمله قرار نخواهد گرفت.

۵-۵ سناریوی تأخیر و پالس

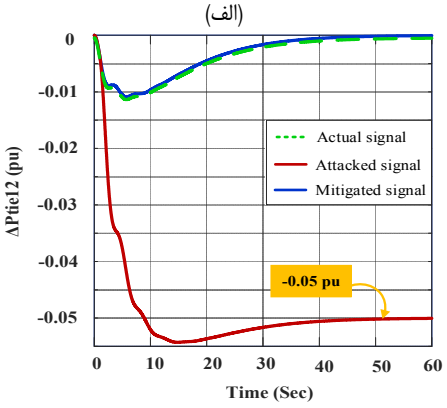
در صورتی که حمله سایبری ترکیبی متشکل از یک ثانیه حمله تأخیر و حمله پالس با دامنه ۰/۰۵ به $\Delta P_{tie_{12}}$ از ثانیه یکم تا پنجم اعمال شود، از آنجایی که سیگنال حمله پالس در بازه زمانی محدودی در شبکه وجود دارد، تأثیر آن نیز موقتی است. این امر مطابق شکل ۸- الف، منجر به بازگردانی فرکانس به مقدار نامی پس از گذشت مدت زمان کمتری نسبت به حالتی که حمله پله در شبکه وجود داشته، شده است. از طرفی با وجود حمله پله، انحراف توان در نهایت توسط AGC در مقداری برابر با دامنه حمله پایدار شده است، به طوری که در حمله پالس، توان عبوری مطابق شکل ۸- ب به مقدار برنامه‌ریزی شده رسیده که علت آن، موقتی‌بودن اثر حمله پالس در شبکه است. تشخیص وجود حمله و تخمین سیگنال حمله توسط الگوریتم پیشنهادی، به ترتیب مطابق شکل‌های ۸- ج و ۸- د به درستی انجام شده‌اند. در گام بعدی، مقادیر اشتباه ΔF_1 و $\Delta P_{tie_{12}}$، اصلاح شده که برابری آنها با نمودارهای واقعی به ترتیب در شکل‌های ۸- الف و ۸- ب حاکی از صحت عملکرد الگوریتم پیشنهادی است.

۶- نتیجه‌گیری

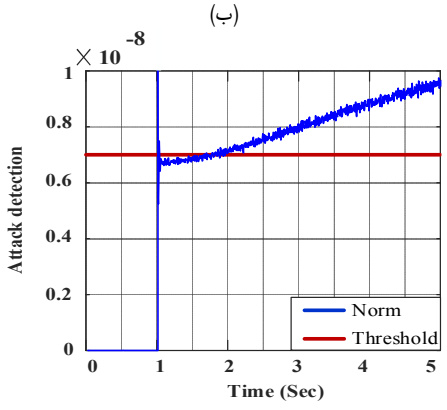
در مقاله حاضر، ضمن استفاده از مدل بهبودیافته AGC شامل باند راکد گاورنر و تأخیر انتقال، به بررسی عملکرد سیستم کنترل خودکار تولید تحت تأثیر حملات سایبری FDI و تأخیر و همچنین، حمله سایبری ترکیبی پرداخته شد. در ادامه، یک روش دفاع سه‌مرحله‌ای مبتنی بر فیلتر کالمن به منظور تشخیص و تخمین حمله و نیز اصلاح داده‌های اندازه‌گیری متأثر از حمله پیشنهاد شد. کارایی روش پیشنهادی بر روی سیستم AGC دوناحیه‌ای مورد آزمایش قرار گرفت. با توجه به آزمایش‌های انجام‌شده، نتیجه می‌شود در صورتی که حمله FDI از نوع



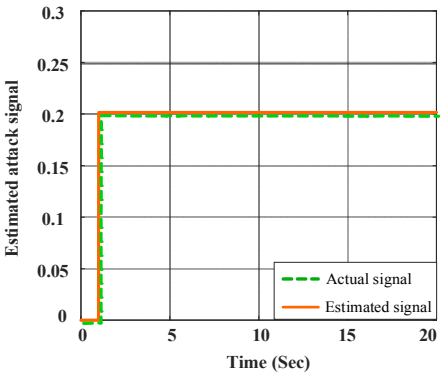
(الف)



(ب)



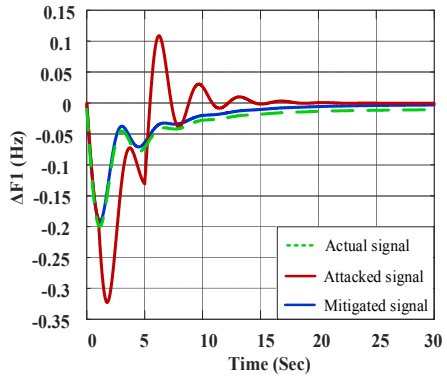
(ج)



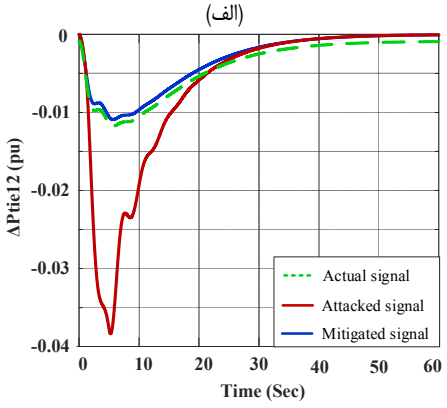
(د)

شکل ۷: حمله ترکیبی شامل حمله تأخیر و پله به $\Delta P_{tie_{۲}}$، (الف) نمودار $\Delta F_{۱}$ ناشی از حمله پله و تأخیر، (ب) نمودار $\Delta P_{tie_{۲}}$ ناشی از حمله پله و تأخیر، (ج) تشخیص حمله پله در حمله سایبری ترکیبی و (د) تخمین سیگنال حمله پله در حمله سایبری ترکیبی.

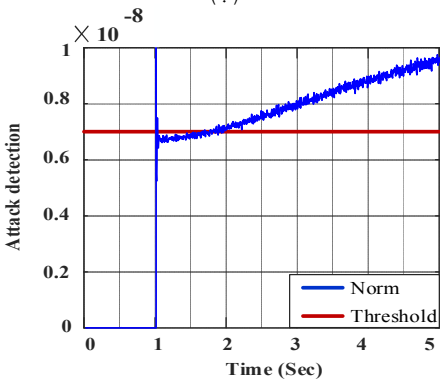
شیب باشد، مشتق سیگنال حمله در حلقه کنترلی منجر به ایجاد خطای حالت ماندگار در فرکانس ناحیه شده و انحراف توان عبوری بین نواحی نیز با توجه به شیب حمله، روند صعودی یا نزولی خواهد داشت و در صورتی که الگوی حمله FDI از نوع پله یا پالس باشد، مشتق آن در حلقه کنترلی صفر شده و از این رو، خطای حالت ماندگار در فرکانس دیده نمی‌شود. به



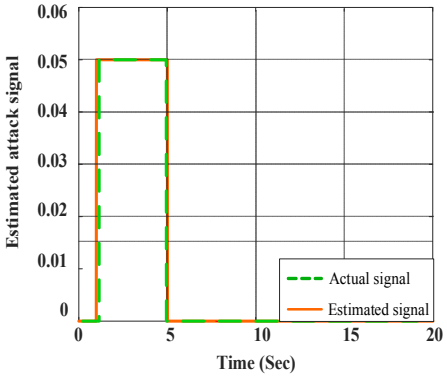
(الف)



(ب)



(ج)



(د)

شکل ۸: حمله ترکیبی شامل حمله تأخیر و پالس به $\Delta P_{tie_{۲}}$، (الف) نمودار $\Delta F_{۱}$ ناشی از حمله پالس و تأخیر، (ب) نمودار $\Delta P_{tie_{۲}}$ ناشی از حمله پالس و تأخیر، (ج) تشخیص حمله پالس در حمله سایبری ترکیبی و (د) تخمین سیگنال حمله پالس در حمله سایبری ترکیبی.

عبارت دیگر، فرکانس در مقدار نامی پایدار می‌شود. از این رو با توجه به هدف حمله‌کننده، الگوهای مختلف حمله FDI می‌توانند پیاده‌سازی شوند. همچنین تأثیر حمله تأخیر در شبکه تا حد زیادی به پارامترهای کنترلی آن وابسته است. به عنوان مثال در آزمایش‌های انجام‌شده، با تنظیم مناسب

ضرایب کنترل‌کننده‌ها، سیستم AGC قادر به پایدارسازی نوسانات ناشی از حمله تأخیر تا ۴ ثانیه نیز است، اما در صورتی که ضرایب کنترل‌کننده‌ها به خوبی تنظیم نشوند، حمله تأخیر می‌تواند منجر به ناپایداری فرکانسی شود.

مراجع

[1] X. Wang, X. Luo, M. Zhang, Z. Jiang, and X. Guan, "Detection and isolation of false data injection attacks in smart grid via unknown input interval observer," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3214-3229, Apr. 2020.

[2] A. J. E. Dagoumas, "Assessing the impact of cybersecurity attacks on power systems," *Energies*, vol. 12, no. 4, Article ID: 12040725, 2019.

[3] G. Wu, J. Sun, and J. Chen, "Optimal data injection attacks in cyber-physical systems," *IEEE Trans. on Cybernetics*, vol. 48, no. 12, pp. 3302-3312, Dec. 2018.

[4] A. M. Mohan, N. Meskin, and H. J. E. Mehrjerdi, "A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems," *Energies*, vol. 13, no. 15, Article ID: 13153860, 2020.

[5] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," in *Proc. IEEE PES General Meeting*, 6 pp., Minneapolis, MN, USA, 25-29 Jul. 2010.

[6] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. on Smart Grid*, vol. 5, no. 2, pp. 580-591, Mar. 2014.

[7] L. Shi, L. Xie, and R. Murray, "Kalman filtering over a packet-delaying network: a probabilistic approach," *Automatica*, vol. 45, no. 9, pp. 2134-2140, Sept. 2009.

[8] S. Akhlaghi, N. Zhou, and Z. Huang, "A multi-step adaptive interpolation approach to mitigating the impact of nonlinearity on dynamic state estimation," *IEEE Trans.on Smart Grid*, vol. 9, no. 4, pp. 3102-3111, Jul. 2016.

[9] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint detection and mitigation of false data injection attacks in AGC systems," *IEEE Trans. on Smart Grid*, vol. 10, no. 5, pp. 4985-4995, Sept. 2018.

[10] A. Ayad, M. Khalaf, and E. El-Saadany, "Detection of false data injection attacks in automatic generation control systems considering system nonlinearities," in *Proc. IEEE Electrical Power and Energy Conf., EPEC'18*, 6 pp. Toronto, Canada, 10-11 Oct. 2018.

[11] F. Hou and J. Sun, "Fasle data injection attacks in cyber-physical systems based on inaccurate model," in *Proc. 43rd Proc. Annual Conf. of the IEEE Industrial Electronics Society*, *IECON'17*, pp. 5791-5796, Beijing, China, 29 Oct.-1 Nov. 2017.

[12] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Trans. on Power Systems*, vol. 33, no. 5, pp. 4760-4774, Sept. 2018.

[13] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Trans. on Industrial Informatics*, vol. 14, no. 5, pp. 1932-1941, May 2017.

[14] A. Sargolzaei, A. Abbaspour, M. A. Al Faruque, A. S. Eddin, and K. Yen, "Security challenges of networked control systems," In *Sustainable Interdependent Networks: Springer*, pp. 77-95, 2018.

[15] A. Ashok, P. Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed," in *Proc. IEEE Power & Energy Society General Meeting*, 5 pp., Denver, CO, USA, 26-30 Jul. 2015.

[16] R. Tan, *et al.*, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. on Information Forensics and Security*, vol. 12, no. 7, pp. 1609-1624, Jul. 2017.

[17] K. Rahimi, A. Parchure, V. Centeno, and R. Broadwater, "Effect of communication time-delay attacks on the performance of automatic generation control," in *Proc. IEEE North American Power Symp., NAPS'15),* 6 pp., Charlotte, NC, USA,4-6 Oct. 2015.

[18] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei, and B. Carbunar, "Resilient design of networked control systems under time delay switch attacks, application in smart grid," *IEEE Access*, vol. 5, pp. 15901-15912, 2017.

[19] X. Yu and K. Tomsovic, "Application of linear matrix inequalities for load frequency control with communication delays," *IEEE Trans. on Power Systems*, vol. 19, no. 3, pp. 1508-1515, Aug. 2004.

[20] L. Jiang, W. Yao, Q. Wu, J. Wen, and S. Cheng, "Delay-dependent stability for load frequency control with constant and time-varying delays," *IEEE Trans. on Power Systems*, vol. 27, no. 2, pp. 932-941, May 2011.

[21] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control in distributed power systems," *IEEE Trans. on Smart Grid*, vol. 7, no. 2, pp. 1176-1185, Mar. 2016.

[22] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, A. Mehbodniya, and S. Sargolzaei, "A novel technique for detection of time delay switch attack on load frequency control," *Intelligent Control and Automation*, vol. 6, no. 4, Article ID: 60844, 9 pp., Nov. 2015.

[23] H. Bevrani, *Robust Power System Frequency Control*, Springer, 2009.

[۲۴] ب. همایی، "تشخیص حمله سایبری تزریق داده غلط در شبکه برق مبتنی بر PMU با استفاده از فیلتر کالمن،" *مجله مهندسی برق دانشگاه تبریز*، جلد ۴۹، شماره ۴، صص. ۱۹۰۳-۱۸۹۵، اسفند ۱۳۹۸.

[25] M. Khalaf, A. Youssef, and E. El-Saadany, "Detection of false data injection in automatic generation control systems using kalman filter," in *Proc. IEEE Electrical Power and Energy Conf., EPEC'17*, 6 pp., Saskatoon, Canada, 22-25 Oct. 2017.

[26] B. Safarinejadian and M. Mozaffari, "A new Kalman filter based state estimation method for multi-input multi-output unit time-delay systems," *Indian Journal of Science and* Technology, vol. 6, no. 3, pp. 4205-4212, Mar. 2013.

[27] S. Wang, S. Bi, and Y. Zhang, "Locational detection of the false data injection attack in a smart grid: a multilabel classification approach," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8218-8227, Sept. 2020.

[۲۸] ت. حاجی‌عبداله، *طراحی و پیاده‌سازی یک روش حمله و دفاع سایبری جدید به سیستم کنترل خودکار تولید*، پایان‌نامه کارشناسی ارشد، دانشگاه تربیت مدرس، ۱۴۰۰.

تینا حاجی‌عبداله در سال ۱۳۹۵ مدرک کارشناسی خود را در رشته‌ی مهندسی برق- قدرت از شهید بهشتی دریافت نمود و در سال ۱۴۰۰ موفق به اخذ مدرک کارشناسی ارشد در رشته‌ی مهندسی برق- سیستم‌های قدرت از دانشگاه تربیت مدرس شد. ایشان در سال ۱۳۹۸ به مدت یکسال به عنوان محقق با مرکز ملی مطالعات و برنامه‌ریزی شبکه‌های قدرت دانشگاه تربیت مدرس همکاری داشت. از زمینه‌های تحقیقاتی مورد علاقه وی می‌توان به کنترل فرکانس سیستم‌های قدرت و امنیت سایبری- فیزیکی شبکه‌ی قدرت اشاره نمود.

حسین سیفی در سال ۱۳۵۹ مدرک کارشناسی خود را از دانشگاه شیراز و در سال‌های ۱۳۶۶ و ۱۳۶۸ به ترتیب مدارک کارشناسی ارشد و دکتری خود را از دانشگاه منچستر (بریتانیا) اخذ نمود. وی از سال ۱۳۶۸ در دانشگاه تربیت مدرس مشغول به تدریس شده و در حال حاضر نیز به عنوان استاد تمام مشغول به کار است. ایشان همچنین به عنوان مشاور ارشد در اجرای چندین پروژه ملی برای شبکه برق ایران با وزارت نیرو همکاری نمود. دکتر سیفی موسس و رئیس مرکز ملی مطالعات و برنامه‌ریزی شبکه‌های قدرت دانشگاه تربیت مدرس است. زمینه‌های تحقیقاتی او برنامه‌ریزی و بهره‌برداری سیستم‌های قدرت، بازار برق و دینامیک سیستم‌های قدرت است.

سید حامد دلخوش مدارک کارشناسی و کارشناسی ارشد خود را در رشته‌ی مهندسی برق- سیستم‌های قدرت به ترتیب از دانشگاه صنعتی امیرکبیر (۱۳۹۲) و دانشگاه صنعتی شریف (۱۳۹۴) اخذ نمود. ایشان در سال ۱۳۹۸ موفق به پایان تحصیلات دوره دکتری در رشته‌ی مهندسی برق- سیستم‌های قدرت در دانشگاه تربیت مدرس شد و در سال ۱۳۹۹ به عضویت هیأت علمی گروه قدرت این دانشگاه درآمد. دکتر دلخوش همچنین به عنوان مدیر پروژه و محقق ارشد با مرکز ملی مطالعات و برنامه‌ریزی شبکه‌های قدرت دانشگاه تربیت مدرس همکاری دارد. زمینه‌های اصلی تحقیقاتی مورد علاقه ایشان بهره‌برداری سیستم‌های قدرت و انرژی‌های تجدیدپذیر است.