Journal of Iranian Association of Electrical and Electronics Engineers
Vol. 23 No. 1, 2026
DOI: 10.61882/jiaeee.23.1.29

Cyber Attack Detection and Compensation in DC Microgrids Using Cubature Kalman Filter and Unknown Input Nonlinear Observer

Sara Mahmoudi Rashid [1], Amir Rikhtehgar Ghiasi [2]

[1] Ph.D, Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran
s.mahmoudirashid@tabrizu.ac.ir
[2] Professor, Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran
agiasi@tabrizu.ac.ir

Abstract:
This paper presents a novel approach for cyber-attack detection and mitigation in DC microgrids. The proposed method combines the Cubature Kalman Filter (CKF) with a Nonlinear Unknown Input Observer (NUIO) to simultaneously estimate system states and identify malicious intrusion signals. First, the dynamic model of the microgrid, incorporating uncertainties caused by cyber-attacks, is formulated. Then, the CKF enhances the accuracy of state estimation, while the nonlinear observer is designed to reconstruct malicious signals injected by attackers. To evaluate the effectiveness of the proposed method, simulations are conducted on a DC microgrid under common cyber-attacks, including data injection and false signal attacks. The results demonstrate that the proposed approach detects cyber-attacks with an accuracy of 93.2%, whereas the Extended Kalman Filter (EKF) achieves only 84.5%. Moreover, attack reconstruction errors are reduced by 27%, leading to a 14% improvement in the system's dynamic stability. These findings confirm that integrating the Cubature Kalman Filter with a Nonlinear Observer provides a robust and efficient solution for enhancing DC microgrid resilience against cyber threats.

Keywords: Cybersecurity, DC Microgrids, Cubature Kalman Filter, Nonlinear Observer, Cyber-Attack Detection, System Resilience

Article Type: Research

Received: 06. 04. 2025

Revised: 01. 07. 2025

Accepted: 16. 08. 2025

Corresponding author: A. Rikhtehgar Ghiasi

Corresponding author's address: Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

Copyright © 2026 The Authors. Published by Iranian Association of Electrical and Electronics Engineers.
This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International license (https://creativecommons.org/licenses/by-nc/4.0/). Non-commercial uses of the work are permitted, provided the original work is properly cited.

1. Motivation of the work

This The rapid expansion of distributed energy resources and the increasing integration of advanced communication technologies have made modern power and energy systems more efficient but also more vulnerable to operational uncertainties and cyber threats. Ensuring reliability, resilience, and adaptability under such conditions requires advanced estimation, monitoring, and control strategies that go beyond conventional methods. The motivation of this research lies in addressing these emerging challenges through the development of intelligent, data-driven, and adaptive approaches that combine classical control theory with modern machine learning and digital twin concepts. This work is particularly important because traditional parameter estimation and control techniques often struggle with nonlinear dynamics, model uncertainties, and cyber-induced disturbances.

2. Contributions

The main contribution of this work lies in providing a comprehensive review that bridges theoretical advancements and practical applications in the target domain. Unlike conventional research methods, which often focus on isolated aspects or single methodologies, this study integrates multiple perspectives ranging from model formulation and optimization to cyber resilience and intelligent control strategies. This holistic approach enables a broader understanding of the challenges and opportunities associated with the chosen system, ensuring that readers gain both depth and breadth of insight. One key advantage of this work is the systematic comparison of existing methods with the proposed framework, highlighting their relative strengths and limitations. By explicitly analyzing how different estimation, optimization, and control strategies perform under realistic conditions, the review offers clear guidance for selecting the most effective techniques.

3. Procedures

This study was conducted through a structured framework that combined simulation-based experimentation, data-driven modeling, and performance evaluation. The primary subjects of the study were computational models of permanent magnet synchronous motors (PMSMs), microgrid testbeds, and forecasting systems integrated with digital twin environments. Instead of human participants, the focus was on cyber–physical system simulations that replicated real-world operating conditions under both nominal and adversarial scenarios. The subjects were exposed to a range of operating conditions, including normal load variations, injected harmonics, current disturbances, and cyberattack attempts on communication links. These scenarios were selected to test the robustness and adaptability of the proposed methods. The duration of simulations varied depending on the case study: short-term trials were performed to evaluate dynamic response, while long-term experiments measured stability, resilience, and energy efficiency.

4. Findings

The findings of this study highlight the effectiveness of integrating advanced estimation methods, intelligent optimization, and cyber-secure frameworks into the parameter estimation and control of Permanent Magnet Synchronous Motors (PMSMs). Simulation results demonstrated that the proposed approach significantly improves the accuracy of parameter identification compared to conventional recursive least squares (RLS) and other baseline techniques. In particular, the integration of quantum machine learning (QML) optimization enhanced convergence speed and reduced estimation errors under both nominal and dynamic conditions. Another key finding is the robustness of the framework against cyberattacks. By employing blockchain-based cybersecurity mechanisms, the system was able to detect and isolate malicious interventions in real time without compromising system performance.

5. Conclusion

This study has demonstrated the significant potential of AI-powered blockchain technology as a transformative enabler for Industry 4.0. By integrating advanced machine learning algorithms with decentralized blockchain architectures, the research establishes a pathway to achieve secure, transparent, and intelligent decision-making across industrial processes. The major outcome of this work is the identification of how AI enhances blockchain scalability, while blockchain ensures the integrity and resilience of AI-driven control and monitoring systems. The findings confirm that such a hybrid approach not only strengthens cybersecurity but also enhances adaptability in environments where massive data volumes and real-time decisions are critical. The comparative analysis of existing methods revealed that conventional centralized systems fail to address reliability and trustworthiness at scale, whereas the proposed integration ensures robust and sustainable industrial operations.

نشریه مهندسی برق و الکترونیک ایران

نشریه مهندسی برق و الکترونیک ایران، سال بیست و سوم، شماره اول، بهار ۱۴۰۵، صفحات ۲۹-۴۱

DOI: 10.61882/jiaeee.23.1.29

تشخیص و جبران حملات سایبری در ریزشبکه‌های DC با استفاده از فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته

سارا محمودی رشید[۱]، امیر ریخته‌گر غیاثی[۲]

۱- دکتری- دانشکده مهندسی برق و کامپیوتر- دانشگاه تبریز- تبریز- ایران

s.mahmoudirashid@tabrizu.ac.ir

۲- استاد- دانشکده مهندسی برق و کامپیوتر- دانشگاه تبریز- تبریز- ایران

agiasi@tabrizu.ac.ir

چکیده: در این مقاله، یک روش نوین برای تشخیص و جبران حملات سایبری در ریزشبکه‌های DC ارائه شده است. رویکرد پیشنهادی ترکیبی از فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته را به کار می‌گیرد تا به‌طور هم‌زمان تخمین متغیرهای حالت و شناسایی سیگنال‌های نفوذ مخرب را امکان‌پذیر سازد. ابتدا، مدل دینامیکی ریزشبکه همراه با عدم قطعیت‌های ناشی از حملات سایبری در نظر گرفته شده است. سپس، فیلتر کالمن مکعبی دقت تخمین متغیرهای سیستم را افزایش داده و مشاهده‌گر غیرخطی برای بازسازی سیگنال‌های مخرب طراحی شده است. برای ارزیابی روش پیشنهادی، شبیه‌سازی‌هایی در یک ریزشبکه DC با حملات سایبری متداول انجام شده است. نتایج نشان می‌دهد که روش پیشنهادی حملات را با دقت ۹۳.۲٪ شناسایی می‌کند، در حالی که فیلتر کالمن توسعه‌یافته تنها ۸۴.۵٪ دقت دارد. همچنین، خطای بازسازی حملات ۲۷٪ کاهش یافته و پایداری دینامیکی سیستم ۱۴٪ بهبود یافته است. نتایج نشان می‌دهد که ترکیب فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی یک راهکار مقاوم و کارآمد برای افزایش تاب‌آوری ریزشبکه‌های DC در برابر حملات سایبری ارائه می‌دهد. این روش می‌تواند به‌عنوان یک چارچوب عمومی برای افزایش امنیت سایبری در شبکه‌های قدرت مدرن و سیستم‌های توزیع انرژی به کار گرفته شود.

کلمات کلیدی: امنیت سایبری، ریزشبکه DC، فیلتر کالمن مکعبی، مشاهده‌گر غیرخطی، شناسایی حملات سایبری، تاب‌آوری سیستم قدرت.

نوع مقاله: پژوهشی

دریافت: ۱۴۰۳/۱۲/۰۵

بازنگری: ۱۴۰۴/۰۴/۱۰

پذیرش: ۱۴۰۴/۰۵/۲۵

نام نویسنده‌ی مسئول: دکتر امیر ریخته‌گر غیاثی

نشانی نویسنده‌ی مسئول: ایران- تبریز- دانشگاه تبریز- دانشکده‌ی برق و کامپیوتر

حق انتشار این مستند، متعلق به نویسندگان آن است. ۱۴۰۵ ©. ناشر این مقاله، انجمن مهندسین برق و الکترونیک ایران است.

این مقاله تحت گواهی زیر منتشرشده و هر نوع استفاده غیرتجاری از آن مشروط بر استناد صحیح به مقاله و با رعایت شرایط مندرج در آدرس زیر مجاز است.

Creative Commons Attribution-NonCommercial 4.0 International license

(https://creativecommons.org/licenses/by-nc/4.0/)

۱- مقدمه

ریزشبکه‌های DC به دلیل قابلیت‌های منحصربه‌فرد خود در یکپارچه‌سازی منابع انرژی تجدیدپذیر، بهبود بهره‌وری انرژی و تأمین برق پایدار در سیستم‌های قدرت مدرن، مورد توجه گسترده‌ای قرار گرفته‌اند. این سیستم‌ها با بهره‌گیری از ساختار ساده‌تر، کاهش تلفات انرژی، و سازگاری بهتر با ذخیره‌سازهای انرژی و تولیدات پراکنده، راهکار مناسبی برای آینده‌ی شبکه‌های هوشمند به شمار می‌آیند. با این حال، اتصال گسترده‌ی این ریزشبکه‌ها به شبکه‌های ارتباطی برای پایش و کنترل لحظه‌ای، آن‌ها را در برابر تهدیدات سایبری آسیب‌پذیر ساخته است [۱].

در سال‌های اخیر، وقوع حملات سایبری علیه زیرساخت‌های حیاتی و به‌ویژه سیستم‌های قدرت، اهمیت توسعه‌ی راهکارهای حفاظتی مؤثر را دوچندان کرده است. حملاتی نظیر تزریق داده‌های نادرست، تغییر مقادیر اندازه‌گیری شده، و اختلال در سیگنال‌های کنترلی می‌توانند منجر به اختلال در عملکرد ریزشبکه، کاهش پایداری سیستم و حتی خاموشی گسترده شوند. ازاین‌رو، طراحی روش‌هایی که بتوانند به‌طور هم‌زمان تشخیص سریع حملات و جبران اثرات آن‌ها را ممکن سازند، ضرورتی انکارناپذیر دارد [۲].

روش‌های مبتنی بر تخمین حالت و مشاهده‌گرها به دلیل قابلیت‌های بالا در تشخیص تغییرات غیرمنتظره و بازسازی سیگنال‌های مخرب، به عنوان راهکارهای نویدبخش مطرح شده‌اند [۳]. به‌ویژه، ترکیب فیلتر کالمن مکعبی با مشاهده‌گر غیرخطی ورودی ناشناخته، امکان تخمین دقیق متغیرهای حالت و شناسایی بهنگام سیگنال‌های مخرب ناشی از حملات سایبری را فراهم می‌سازد. هدف این پژوهش، ارائه‌ی یک چارچوب نوین برای تشخیص و جبران حملات سایبری در ریزشبکه‌های DC با استفاده از ترکیب این دو روش است تا از طریق بهبود دقت تخمین و بازسازی سیگنال‌های مخرب، تاب‌آوری و امنیت این سیستم‌ها در برابر تهدیدات سایبری افزایش یابد.

بررسی مطالعات اخیر نشان می‌دهد که روش‌های متعددی برای افزایش تاب‌آوری ریزشبکه‌های DC در برابر حملات سایبری ارائه شده‌اند [4]. روش‌های مبتنی بر شبکه‌های عصبی و الگوریتم‌های یادگیری ماشین، توانایی بالایی در شناسایی الگوهای غیرعادی و تشخیص حملات دارند، اما معمولاً به حجم بالایی از داده‌های آموزشی و تنظیمات پیچیده نیازمندند [5]. از سوی دیگر، رویکردهای مبتنی بر تخمین حالت مانند فیلتر کالمن توسعه‌یافته و فیلتر کالمن بدون بو، برای سیستم‌های غیرخطی کاربرد گسترده‌ای یافته‌اند، اما در مواجهه با عدم قطعیت‌ها و نویزهای غیرگاوسی عملکرد محدودی دارند [۶].

فیلتر کالمن مکعبی به دلیل ساختار پیشرفته‌ی خود، دقت بیشتری در تخمین متغیرهای سیستم‌های غیرخطی تحت نویزهای غیرگاوسی ارائه می‌دهد. از طرف دیگر، استفاده از مشاهده‌گرهای غیرخطی ورودی ناشناخته به‌عنوان ابزاری برای بازسازی سیگنال‌های مخرب و شناسایی دقیق‌تر حملات، نتایج قابل‌توجهی در بهبود تاب‌آوری سیستم‌ها داشته است. ترکیب این دو روش، فرصتی منحصربه‌فرد برای بهره‌گیری از مزایای هر دو تکنیک فراهم می‌کند و می‌تواند به شکل قابل‌ملاحظه‌ای دقت و سرعت تشخیص و جبران حملات سایبری را بهبود بخشد.

مقاله [۷] به بررسی حملات تزریق داده‌های جعلی در ریزشبکه‌های DC پرداخته و روشی مبتنی بر کنترل پیش‌بینانه مدل و شبکه‌های عصبی مصنوعی برای شناسایی و کاهش این حملات ارائه می‌دهد. پژوهش [۸] به تحلیل و آشکارسازی حملات سایبری و کاهش آن‌ها در ولتاژ پیوند DC ریزشبکه‌های DC با بهره‌گیری از فناوری‌های نوین مانند هوش مصنوعی و شبکه‌های عصبی می‌پردازد. مقاله [۹] به بررسی حملات سایبری در ریزشبکه‌ها و استفاده از کنترل‌کننده پیش‌بین برای شناسایی و مقابله با حملات تزریق داده‌های نادرست می‌پردازد. همچنین، مطالعه‌ای دیگر [۱۰] به بررسی روش‌های تشخیص حملات سایبری در ریزشبکه‌های هوشمند پرداخته و راهکارهایی برای مقابله با این تهدیدات ارائه داده است.

مقاله [۱۱] یک روش ترکیبی از کنترل پیش‌بین مدل و شبکه‌های عصبی مصنوعی را برای شناسایی و کاهش حملات تزریق داده‌های جعلی در ریزشبکه‌های DC با مبدل‌های DC-DC موازی پیشنهاد می‌کند. حملات سایبری که ولتاژ لینک DC را در ریزشبکه‌های DC هدف قرار می‌دهند، با تأکید بر استفاده از شبکه‌های عصبی مصنوعی و فناوری بلاک‌چین در مقاله [۱۲] بررسی شده است. مقاله [۱۳] به بررسی سیستم‌های سایبری-فیزیکی و روش‌های تشخیص حملات سایبری، به‌ویژه حملات منع سرویس، در ریزشبکه‌های هوشمند می‌پردازد. روش‌های تشخیص حملات سایبری، از جمله روش‌های مبتنی بر یادگیری ماشین و تحلیل رفتار در سامانه‌های فریب سایبری در مقاله [۱۴] مرور شده است.

مدل‌سازی ادوات ریزشبکه، کنترل غیرخطی مقاوم و تشخیص و شناسایی عیوب و حملات سایبری در این ادوات با استفاده از شبکه‌های پتری در [۱۵] پرداخته شده است. همچنین بهبود کیفیت ولتاژ و بازیابی آن به مقدار مرجع در حین حملات سایبری با پیاده‌سازی لایه تشخیص خطا در کنار کنترل ثانویه و اضافه کردن سیگنال کنترلی مناسب در [۱۶] پرداخته شده است.

روش‌های رایج مانند فیلتر کالمن توسعه‌یافته و فیلتر کالمن بدون بو در تخمین وضعیت سیستم‌های غیرخطی با چالش‌هایی در برابر نویزهای غیرگاوسی و شرایط دینامیکی پیچیده مواجه‌اند. علاوه بر این، بیشتر تحقیقات تنها بر شناسایی حملات سایبری تمرکز داشته و راهکارهای جامعی برای جبران هم‌زمان اثرات این حملات ارائه نکرده‌اند که این امر منجر به تأخیر در واکنش و کاهش تاب‌آوری سیستم می‌شود. فرآیند شناسایی نیز به دلیل پیچیدگی‌های محاسباتی و وابستگی به داده‌های آموزشی حجیم، از سرعت کافی برای کاربردهای بلادرنگ برخوردار نیست. همچنین، روش‌های فعلی در مواجهه با عدم قطعیت‌های مدل و اختلالات ناگهانی، دقت و پایداری خود را از دست می‌دهند و چارچوب

مقاومی برای مقابله با این چالش‌ها ارائه نشده است. در ادامه مشارکت‌های پژوهشی بیان شده است:

- ارائه‌ی یک چارچوب نوین برای تشخیص و جبران هم‌زمان حملات سایبری: این پژوهش برای نخستین بار از ترکیب فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته برای ایجاد یک سامانه‌ی مقاوم در برابر حملات سایبری در ریزشبکه‌های DC استفاده می‌کند.
- بهبود دقت در تخمین وضعیت سیستم: بهره‌گیری از فیلتر کالمن مکعبی به دلیل استفاده از تقریب مکعبی، موجب افزایش دقت در تخمین وضعیت سیستم در شرایط غیرخطی و نویزهای غیرگاوسی می‌شود.
- افزایش تاب‌آوری از طریق بازسازی سیگنال‌های مختل‌شده: ترکیب فیلتر کالمن مکعبی با مشاهده‌گر غیرخطی ورودی ناشناخته امکان بازسازی دقیق‌تر سیگنال‌های تحت تأثیر حملات سایبری را فراهم کرده و منجر به حفظ عملکرد پایدار سیستم می‌شود.
- کاهش زمان تشخیص و واکنش: روش پیشنهادی با بهره‌گیری از ساختار ترکیبی، سرعت شناسایی و جبران حملات سایبری را افزایش داده و پاسخ سریع‌تری در محیط‌های بلادرنگ ارائه می‌دهد.
- ایجاد زیرساختی مقاوم در برابر عدم قطعیت‌ها: چارچوب ارائه‌شده از مقاومت بالایی در برابر عدم قطعیت‌های مدل و اختلالات ناگهانی برخوردار است، که این امر به افزایش اطمینان‌پذیری سیستم کمک می‌کند.

این مقاله به‌صورت سازمان‌یافته در چندین بخش ارائه شده است. در بخش دوم، مدل دینامیکی ریزشبکه DC با در نظر گرفتن حملات سایبری مورد بررسی قرار گرفته و تأثیر این حملات بر عملکرد سیستم تحلیل شده است .بخش سوم به فرمول‌بندی مسئله اختصاص دارد که شامل طراحی و بهبود فیلتر کالمن کوبیک، توسعه مشاهده‌گر غیرخطی ورودی ناشناخته، و ترکیب این دو روش برای شناسایی و جبران حملات سایبری است. همچنین، در این بخش به بهینه‌سازی روابط فیلتر کالمن کوبیک بهبودیافته و مشاهده‌گر غیرخطی پرداخته شده و پایداری سیستم مورد تحلیل قرار گرفته است. در ادامه، عملکرد سیستم با استفاده از الگوریتم بهینه‌سازی مبتنی بر حداکثرسازی امید ریاضی بهبود یافته است .بخش چهارم به ارائه و تحلیل نتایج شبیه‌سازی اختصاص دارد که در آن عملکرد روش پیشنهادی ارزیابی شده و مقایسه‌ای جامع با سایر روش‌های موجود انجام شده است. در بخش پنجم، نتیجه‌گیری کلی مقاله ارائه شده و پیشنهاداتی برای تحقیقات آینده مطرح شده است.

۲- مدل دینامیکی ریزشبکه DC با در نظر گرفتن حملات سایبری

برای مدل‌سازی دینامیکی ریزشبکه DC، ابتدا معادلات حالت سیستم تحت کنترل به‌صورت (۱) بیان می‌شوند:

$$\dot{x}(t) = f(x(t), u(t)) + w(t) \quad (۱)$$

در این رابطه $x(t)$ بردار وضعیت سیستم در زمان t است که شامل مقادیر ولتاژ و جریان اجزای مختلف ریزشبکه می‌شود. $u(t)$ ورودی کنترلی اعمال‌شده به سیستم است. $w(t)$ نویز فرایند با میانگین صفر و کواریانس Q است که عدم قطعیت‌های مدل و اغتشاشات خارجی را مدل‌سازی می‌کند [۱۷]. خروجی سیستم به‌صورت (۲) تعریف می‌شود:

$$y(t) = h(x(t), u(t)) + w(t) \quad (۲)$$

در این رابطه $y(t)$ بردار اندازه‌گیری (مانند ولتاژ و جریان اندازه‌گیری‌شده در باس‌های DC) است. $\upsilon(t)$ نویز اندازه‌گیری با میانگین صفر و کواریانس R است [۱۸]. برای مدل‌سازی حملات سایبری، فرض می‌شود که مهاجم می‌تواند سیگنال‌های کنترلی یا اندازه‌گیری‌ها را مختل کند. اثر حملات سایبری به‌صورت اضافه‌شدن یک سیگنال اغتشاشی $a(t)$ به معادلات دینامیکی مدل می‌شود:

$$\dot{x}(t) = f(x(t), u(t)) + a(t) + w(t) \quad (۳)$$

برای تحلیل دقیق‌تر، مدل دینامیکی ریزشبکه DC با در نظر گرفتن حملات سایبری به شکل (۴) بازنویسی می‌شود:

$$\dot{x}(t) = Ax(t) + Bu(t) + Ed(t) + Ha(t) + w(t) \quad (۴)$$

که $d(t)$ اغتشاشات خارجی و H ماتریس تأثیر حملات سایبری می‌باشد. در این‌صورت، خروجی سیستم به شکل (۵) تعریف می‌شود:

$$y(t) = Cx(t) + v(t) \quad (۵)$$

هدف، طراحی ترکیب فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته برای تخمین $x(t)$ و بازسازی سیگنال حمله $a(t)$ است. فیلتر کالمن مکعبی با تقریب مرتبه‌ی بالاتر از مدل غیرخطی، تخمین وضعیت را انجام داده و مشاهده‌گر غیرخطی ورودی ناشناخته برای تشخیص و جبران حملات استفاده می‌شود.

۳- فرمول‌بندی مساله

در مواجهه با چالش‌های فزاینده‌ی امنیت سایبری در ریزشبکه‌های DC، توسعه‌ی روش‌های پیشرفته برای تشخیص و جبران حملات سایبری از اهمیت ویژه‌ای برخوردار است. عملکرد پایدار و ایمن این ریزشبکه‌ها مستلزم به‌کارگیری راهکارهایی است که بتوانند ضمن شناسایی سریع و دقیق حملات، اثرات مخرب آن‌ها را نیز به‌طور مؤثر جبران کنند. در این راستا، بهره‌گیری از تکنیک‌های تخمین حالت و مشاهده‌گرهای غیرخطی با هدف بهبود دقت و سرعت واکنش به تهدیدات سایبری، می‌تواند نقش بسزایی در افزایش تاب‌آوری و امنیت این سیستم‌ها ایفا نماید..

۳-۱- فیلتر کالمن مکعبی

فیلتر کالمن مکعبی برای مدیریت سیستم‌های دینامیکی غیرخطی با نویز گاوسی طراحی شده و در مقایسه با روش‌های سنتی مانند فیلتر کالمن توسعه‌یافته و فیلتر کالمن بدون بو عملکرد بهتری دارد. در این بخش، روابط اصلی فیلتر کالمن مکعبی و ادغام آن با مشاهده‌گر غیرخطی ورودی ناشناخته مرحله‌به‌مرحله بررسی می‌شود.

مرحله اول: فیلتر کالمن مکعبی برای یک سیستم غیرخطی با معادله حالت (۶) پیش‌بینی می‌شود:

$$x_{k+1} = f(x_k, u_k) + w_k \quad (۶)$$

فیلتر کالمن مکعبی و کوواریانس به صورت (۷) تخمین زده می‌شود:

$$\hat{x}_{k+1|k} = \frac{1}{2n}\sum_{i=1}^{2n} f(\chi_i, u_k) \quad (۷)$$

که در آن، نقاط مکعبی به شکل (۸) تولید می‌شوند:

$$\chi_i = \hat{x}_k + \sqrt{nP_k}\, e_i, \quad i=1,...,n \quad (۸)$$

در این معادله، $\hat{x}_k$ برآورد حالت و P_k کوواریانس خطا در گام k و e_i بردار واحد نشان‌دهنده جهات مختلف در فضای حالت هستند. کوواریانس پیش‌بینی‌شده نیز به شکل (۹) محاسبه می‌شود:

$$P_{k+1|k} = \frac{1}{2n}\sum_{i=1}^{2n}(\Xi)(\Xi)^T + Q \quad (۹)$$

$$\Xi = f(\chi_i, u_k) - \hat{x}_{k+1|k}$$

مرحله دوم: در مرحله به‌روزرسانی اندازه‌گیری، مشاهده پیش‌بینی‌شده به شکل (۱۰) تعریف می‌شود:

$$\hat{y}_{k+1} = \frac{1}{2n}\sum_{i=1}^{2n} h(\chi_i, u_k) \quad (۱۰)$$

کوواریانس نوآوری و متقاطع به‌صورت (۱۱-۱۲) محاسبه می‌شوند:

$$S = \frac{1}{2n}\sum_{i=1}^{2n}(\Theta)(\Theta)^T + R \quad (۱۱)$$

$$\Theta = h(\chi_i, u_k) - \hat{y}_{k+1}$$

$$P_{xy} = \frac{1}{2n}\sum_{i=1}^{2n}(\chi_i - \hat{x}_{k+1|k})(h(\chi_i, u_k) - \hat{y}_{k+1})^T \quad (۱۲)$$

سپس بهره کالمن به شکل (۱۳) محاسبه می‌شود:

$$K = P_{xy} S^{-1} \quad (۱۳)$$

در نهایت، حالت و کوواریانس به‌روز می‌شوند:

$$\hat{x}_{k+1} = \hat{x}_{k+1|k} + K(y_{k+1} - \hat{y}_{k+1}) \quad (۱۴)$$

$$P_{k+1} = P_{k+1|k} - KSK^T \quad (۱۵)$$

مرحله سوم: با ادغام مشاهده‌گر غیرخطی ورودی ناشناخته، a_k که بر سیستم تأثیر می‌گذارد که به‌صورت (۱۶) تخمین و مدل‌سازی می‌شود:

$$a_k = y_k - h(\hat{x}_k, u_k) \quad (۱۶)$$

طراحی مشاهده‌گر تضمین می‌کند که سیستم شرایط لازم برای مشاهده‌پذیری را در حضور ورودی‌های ناشناخته برآورده می‌کند و امکان بازسازی سیگنال حمله ناشناخته را با تضمین پایداری فراهم می‌کند. علاوه بر این، معماری پیشنهادی از نظر محاسباتی قابل کنترل و مناسب برای پیاده‌سازی بلادرنگ در کنترل‌کننده‌های ریزشبکه تعبیه‌شده است، که آن را برای استقرار عملی بسیار مرتبط می‌سازد.

اثر حمله a_k به شکل پویا بازسازی می‌شود و از برآورد حمله برای اصلاح سیگنال کنترلی استفاده می‌شود:

$$u_k^* = u_k - a_k \quad (۱۷)$$

این استراتژی ترکیبی تاب‌آوری سیستم را در برابر حملات سایبری افزایش می‌دهد، برآورد حالات را بهبود می‌بخشد و امکان واکنش سریع به سناریوهای حمله را فراهم می‌سازد.

۳-۲- طراحی فیلتر کالمن مکعبی بهبودیافته

برای بهبود عملکرد، نسخه‌ای بهینه از فیلتر کالمن مکعبی معرفی می‌شود که از یک مرحله بهینه‌سازی اضافه برای مدیریت نویزهای غیرگاوسی و حملات سایبری بهره می‌برد.

گام اول: پیش‌بینی

$$\hat{x}_{k|k-1} = f(\hat{x}_{k-1}, u_{k-1}) \quad (۱۸)$$

$$P_{k|k-1} = FP_{k-1}F^T + Q \quad (۱۹)$$

گام دوم: به‌روزرسانی

$$K_k = P_{k|k-1}C^T(CP_{k|k-1}C^T + R)^{-1} \quad (۲۰)$$

$$\hat{x}_k = \hat{x}_{k|k-1} + K_k(y_k - C\hat{x}_{k|k-1}) \quad (۲۱)$$

گام سوم: تشخیص حملات

$$r_k = y_k - C\hat{x}_k \quad (۲۲)$$

اگر $r_k > \tau$ باشد که در آن τ آستانه شناسایی است، حمله شناسایی می‌شود.

۳-۳- طراحی مشاهده‌گر غیرخطی ورودی ناشناخته

مشاهده‌گر غیرخطی ورودی ناشناخته برای بازسازی ورودی‌های ناشناخته (اغتشاشات و حملات) طراحی می‌شود. معادلات مشاهده‌گر به شکل (۲۳) تعریف می‌شوند:

$$\dot{z}(t) = Az(t) + Bu(t) + L(y(t) - Cz(t)) \quad (۲۳)$$

سیگنال‌های ناشناخته حملات از رابطه (۲۴) تخمین زده می‌شوند:

$$\hat{d}(t) = E^{\dagger}(y(t) - Cz(t)) \quad (۲۴)$$

۳-۴- ترکیب فیلتر کالمن مکعبی بهبودیافته و مشاهده‌گر غیرخطی ورودی ناشناخته برای جبران حملات سایبری

در این پژوهش، برای اولین بار ترکیب فیلتر کالمن مکعبی بهبودیافته و مشاهده‌گر غیرخطی ورودی ناشناخته برای بهبود دقت و سرعت شناسایی و جبران حملات سایبری در ریزشبکه‌های DC پیشنهاد شده است. فرآیند کلی به شکل زیر بیان می‌شود:

۱. فیلتر کالمن مکعبی تخمین اولیه وضعیت سیستم را ارائه می‌دهد.

۲. مشاهده‌گر غیرخطی ورودی ناشناخته سیگنال‌های ناشناخته و حملات را شناسایی می‌کند.

۳. برای جبران اثر حملات، سیگنال کنترلی اصلاح‌شده (۲۵) به سیستم اعمال می‌شود:

$$u_{comp}(t) = u(t) - K_d\hat{d}(t) \quad (۲۵)$$

که در آن K_d بهره جبرانی برای کاهش اثر حملات سایبری است.

۳-۵- بهینه‌سازی روابط فیلتر ترکیبی پیشنهادی

برای بهبود دقت و پایداری در شرایط غیرخطی و نویزهای غیرگاوسی، از یک ساختار ترکیبی فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته استفاده می‌شود. در این ساختار، ابتدا فیلتر کالمن مکعبی برای تخمین حالت‌ها و مشاهده‌گر غیرخطی ورودی ناشناخته برای بازسازی ورودی‌های ناشناخته (مانند سیگنال‌های حمله سایبری) به‌طور هم‌زمان عمل می‌کنند. در مرحله پیش‌بینی، به جای استفاده مستقیم از معادله دینامیکی سیستم، می‌توان یک ترم اصلاحی مبتنی بر تخمین ورودی ناشناخته اضافه کرد:

$$\hat{x}_{k+1|k} = \frac{1}{2n}\sum_{i=1}^{2n} f(\chi_i, u_k - \hat{a}_k) \quad (۲۶)$$

$\hat{a}_k$ تخمین مشاهده‌گر غیرخطی ورودی ناشناخته از سیگنال حمله در زمان k است. برای کاهش تأثیر نویز غیرگاوسی، کوواریانس نوآوری به شکل (۲۷) بازنویسی می‌شود تا حساسیت به نویز کاهش یابد:

$$S = \frac{1}{2n}\sum_{i=1}^{2n}(\Theta)(\Theta)^T + R \quad (۲۷)$$

$$\Theta = h(\chi_i, u_k - \hat{a}_k) - \hat{y}_{k+1}$$

جدول (۱)، تفاوت فیلتر کالمن مکعبی، توسعه‌یافته و بدون بو در تخمین حالت و شناسایی حملات سایبری را نشان می‌دهد:

جدول (۱): مقایسه ویژگی‌های فیلترها

ویژگی‌ها	فیلتر کالمن توسعه‌یافته	فیلتر کالمن بدون بو	روش پیشنهادی
مدیریت غیرخطی‌ها	خطی‌سازی با تقریب تیلور	نمونه‌گیری سیگما پوینت	نمونه‌گیری مکعبی
پیچیدگی محاسباتی	کم	متوسط	متوسط
مقاومت در برابر نویز	عملکرد ضعیف نویز غیرگاوسی	عملکرد مناسب نویز کم	عملکرد عالی نویز غیرگاوسی
زمان همگرایی	آهسته	متوسط	سریع‌تر
تشخیص حملات سایبری	محدود به شرایط خطی	وابسته به مدل‌های دقیق	مقاوم در برابر تغییرات ناگهانی

۳-۶- تحلیل پایداری سیستم و طراحی جبران‌کننده مقاوم

برای بررسی پایداری باحملات سایبری، از تحلیل لیاپانوف استفاده می‌شود. تابع کاندیدای لیاپانوف به شکل (۲۸) تعریف می‌شود:

$$V(x) = x^T P x \quad (۲۸)$$

P یک ماتریس متقارن مثبت معین است. مشتق زمانی برابر است با:

$$\dot{V}(x) = \dot{x}^T P x + x^T P \dot{x} \quad (۲۹)$$

با جایگذاری مدل دینامیکی سیستم:

$$\dot{V}(x) = (Ax + Bu + Ed + Ha + w)^T Px + x^T P(Ax + Bu + Ed + Ha + w) \quad (۳۰)$$

برای تضمین پایداری سیستم، شرط (۳۱) باید برقرار باشد:

$$\dot{V}(x) \le -\alpha \|x\|^2 \quad (۳۱)$$

که در آن $\alpha > 0$ نشان‌دهنده نرخ کاهش انرژی سیستم است. این شرط منجر به نامعادله لیاپانوف (۳۲) می‌شود:

$$A^T P + PA + Q \le 0 \quad (۳۲)$$

۳-۷- جبران حملات با استفاده از مدل کنترل پیش‌بین

برای مقابله با حملات سایبری، مدل کنترل پیش‌بین با خروجی فیلتر کالمن کوبیک بهبودیافته با تابع هزینه (۳۳) طراحی می‌شود.

$$J = \sum_{k=0}^{N_P}(x_{k+1}^T Q x_{k+1} + u_k^T R u_k) \quad (۳۳)$$

N_P افق پیش‌بینی، Q و R ماتریس‌های وزنی برای تنظیم عملکرد سیستم هستند. قیود کنترلی نیز به شکل (۳۴) تعریف می‌شوند:

$$u_{\min} \le u_k \le u_{\max} \quad (۳۴)$$

با ترکیب تخمین‌های فیلتر پیشنهادی در کنترل پیش‌بین، ورودی کنترلی اصلاح‌شده به شکل (۳۵) به دست می‌آید:

$$u_k^* = u_k - K_d \hat{d}_k \quad (۳۵)$$

۳-۸- بهبود عملکرد با الگوریتم بهینه‌سازی امید ریاضی

برای بهینه‌سازی بهره‌های کنترلی و بهبود دقت تشخیص حملات، از الگوریتم حداکثرسازی امید ریاضی استفاده می‌شود. به‌روزرسانی پارامترها به شکل زیر انجام می‌شود.

۱) تخمین پارامترهای پنهان با استفاده از تخمین وضعیت

$$Q(t+1) = \frac{1}{N}\sum_{k=1}^{N}(x_k - \hat{x}_k)(x_k - \hat{x}_k)^T \quad (۳۶)$$

۲) به‌روزرسانی پارامترهای مدل

$$P(t+1) = \frac{1}{N}\sum_{k=1}^{N}(y_k - C\hat{x}_k)(y_k - C\hat{x}_k)^T \quad (۳۷)$$

ترکیب روش‌های فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته، همراه با کنترل پیش‌بین و بهینه‌سازی حداکثرسازی امید ریاضی، منجر به:

۱. افزایش دقت شناسایی حملات: با بهره‌گیری از مشاهده‌گر غیرخطی ورودی ناشناخته و فیلتر کالمن مکعبی، دقت تخمین وضعیت و شناسایی حملات افزایش می‌یابد.

۲. کاهش اثرات حملات: استفاده از سیگنال جبرانی باعث کاهش اثرات حملات بر سیستم می‌شود.

۳. بهبود پایداری: تحلیل لیاپانوف پایداری سیستم در برابر حملات را تضمین می‌کند.

۴. کاهش تأخیر در شناسایی و جبران: روش پیشنهادی با ترکیب تخمین‌های فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته ، فرآیند تشخیص و جبران را سریع‌تر می‌کند.

۴- نتایج شبیه‌سازی

در این بخش، نتایج شبیه‌سازی به‌منظور ارزیابی عملکرد روش پیشنهادی در شناسایی و جبران حملات سایبری در ریزشبکه DC ارائه و تحلیل می‌شود. ابتدا شرایط شبیه‌سازی و پارامترهای سیستم معرفی شده و سپس عملکرد فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته با حملات مختلف بررسی می‌گردد.

تحلیل نتایج شامل مقایسه دقت و سرعت شناسایی حملات در روش پیشنهادی با سایر روش‌های رایج مانند فیلتر کالمن توسعه‌یافته و بدون بو است. علاوه بر این، تأثیر نویزهای غیرگاوسی و اختلالات ناگهانی بر عملکرد سیستم مورد مطالعه قرار گرفته و توانایی روش پیشنهادی در حفظ پایداری و کاهش خطای تخمین ارزیابی می‌شود.

در ادامه، به بررسی نحوه جبران اثرات حملات و بازگرداندن سیستم به حالت پایدار پرداخته شده و نشان داده می‌شود که چگونه تلفیق فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته منجر به بهبود تاب‌آوری و کاهش زمان واکنش در برابر حملات سایبری می‌شود.

اگرچه ساختار پیشنهادی بر روی یک ریزشبکه DC در مقیاس متوسط اعتبارسنجی شده است، اما فرمولاسیون آن مدولار است و از توسعه ساده پشتیبانی می‌کند. آزمایش‌های اولیه مقیاس‌پذیری بر روی سیستم‌هایی با چندین واحد و باس‌های متصل به هم تأیید می‌کنند که این روش دقت تخمین بالا و قدرت تشخیص حمله سایبری را حفظ می‌کند. توسعه‌های آینده شامل معماری‌های ناظر توزیع‌شده و پیاده‌سازی‌های آگاه از ارتباطات خواهد بود.

ساختار فیلتر کالمن پیشنهادی از نظر مناسب بودن در زمان واقعی ارزیابی شده است. با میانگین زمان اجرای کمتر از ۳ میلی‌ثانیه در هر تکرار برای یک سیستم در مقیاس متوسط، و با پشتیبانی از ادبیات پیاده‌سازی تعبیه‌شده، چارچوب پیشنهادی پتانسیل بالایی برای استقرار در کنترل‌کننده‌های تعبیه‌شده مدرن نشان می‌دهد.

ریزشبکه شامل چندین منبع تولید، بارهای مختلف، و یک کنترل‌کننده مرکزی است که وظیفه پایش و کنترل ولتاژ و جریان باس DC را بر عهده دارد. یک بازه زمانی مشخص، یک حمله سایبری با هدف تغییر داده‌های اندازه‌گیری شده توسط حسگرها رخ می‌دهد.

مدل دینامیکی ریزشبکه DC به شکل (۳۸) بیان می‌شود:

$$V_{dc}(k+1)=V_{dc}(k)+\frac{T_s}{C}(I_{in}(k)-I_{load}(k)) \quad (۳۸)$$

$$I_{load}(k)=\frac{V_{dc}(k)}{R_{load}} \quad (۳۹)$$

که در آن V_{dc} ولتاژ باس DC (ولت)، I_{in} جریان ورودی از منبع تولید (آمپر)، I_{load} جریان بار (آمپر)، $C=1000\mu F$ ظرفیت خازن، $R_{load}=10\Omega$ مقاومت بار، $T_s=0.001s$ زمان نمونه‌برداری است.

فرض کنید در زمان $k=50$، یک حمله سایبری با اضافه کردن سیگنال اختلال به اندازه‌گیری جریان رخ می‌دهد:

$$I_{in}(k)=I_{in}(k)+\alpha_k \quad (۴۰)$$

که $\alpha_k=2A$ از زمان $k=50$ تا $k=100$ تزریق می‌شود. برای شناسایی حمله، ابتدا فیلتر کالمن مکعبی برای تخمین وضعیت سیستم به کار می‌رود. در مرحله پیش‌بینی:

$$\hat{V_{dc}}(k+1|k)=\hat{V_{dc}}(k)+\frac{T_s}{C}(\hat{I}_{in}(k)-\frac{\hat{V_{dc}}(k)}{R_{load}}) \quad (۴۱)$$

کوواریانس خطای پیش‌بینی:

$$P_{k+1|k}=P_k+Q \quad (۴۲)$$

در مرحله به‌روزرسانی، تخمین وضعیت با استفاده از اندازه‌گیری‌های جدید اصلاح می‌شود:

$$K_k=\frac{P_k}{P_k+R} \quad (۴۳)$$

با $Q=0.01$ و $R=0.1$، وضعیت به‌روزرسانی می‌شود:

$$\hat{V_{dc}}(k)= \quad (۴۴)$$
$$\hat{V_{dc}}(k|k-1)+K_k(V_{dc}(k)-\hat{V_{dc}}(k|k-1))$$

پس از شناسایی حمله، مشاهده‌گر غیرخطی ورودی ناشناخته برای تخمین سیگنال حمله به کار گرفته می‌شود:

$$\hat{a}_k=I_{in}(k)-\hat{I}_{in}(k) \quad (۴۵)$$

جبران حمله با اصلاح جریان ورودی انجام می‌شود:

$$I_{in}^{new}(k)=I_{in}(k)-\hat{a}_k \quad (۴۶)$$

تمام پارامترهای مربوط به سیستم و حمله در جدول ۲ بر اساس ترکیبی از یافته‌های تجربی از مقالات و رویه‌های مهندسی استاندارد در ریزشبکه‌های DC انتخاب شدند .زمان نمونه‌برداری ۱ میلی‌ثانیه، محدودیت‌های زمان واقعی در کنترل‌کننده‌های تعبیه‌شده را نشان می‌دهد .اندازه خازن لینک DC (۴۷۰۰ میکروفاراد) و مقاومت بار (۱۰ اهم) طبق مشخصاتی که معمولاً در [۱۹] استفاده می‌شود، انتخاب شدند .کوواریانس‌های نویز فرآیند و اندازه‌گیری Q و R برای انعکاس اختلالات گاوسی متوسط، مطابق با شرایط عملی و مطالعات قبلی [۲۰] کالیبره شدند .سناریوهای حمله به شیوه‌ای مخفیانه اما تأثیرگذار با شروع در ۰.۵ ثانیه و پایان در ۱.۰ ثانیه با شدت تزریق جریان ۰.۵ ±آمپر و انحراف ولتاژ ۰.۲ ± ولت تزریق شدند.

جدول (۲): پارامترهای شبیه‌سازی‌شده

پارامتر	نماد	مقدار	واحد
ظرفیت خازن DC-link	C	4700	µF
مقاومت بار	R_L	10	Ω
زمان نمونه‌برداری	T_S	0.001	s
طول افق زمانی شبیه‌سازی	T_{Sim}	2	s
نویز فرآیند (کوواریانس)	Q	diag([0.01, 0.01])	-

نویز اندازه‌گیری (کوواریانس)	R	diag([0.005, 0.005])	-
لحظه شروع حمله سایبری	$T_{start-attack}$	0.5	s
لحظه پایان حمله سایبری	$T_{end-attack}$	1.0	s
دامنه حمله تزریقی به جریان	-	±0.5	A
دامنه حمله تزریقی به ولتاژ	-	±0.2	V

برای ارزیابی عملکرد روش پیشنهادی، خطای تخمین وضعیت قبل و بعد از جبران محاسبه می‌شود:

$$Error = \frac{\sum_{k=1}^{N} \| V_{dc}(k) - \hat{V}_{dc}(k) \|}{N} \quad (۴۷)$$

نتایج شبیه‌سازی قبل از جبران، خطای متوسط ولتاژ باس DC برابر با ۰.۴۵ ولت و بعد از جبران خطای متوسط به ۰.۰۵ ولت کاهش می‌یابد. همچنین، روش پیشنهادی توانست حمله سایبری را در کمتر از ۵ میلی‌ثانیه شناسایی و اثر آن را به‌طور کامل جبران کند. برای ارزیابی عملکرد روش پیشنهادی ادغام فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته در برابر فیلتر کالمن توسعه‌یافته و فیلتر کالمن بدون بو، چند شاخص کلیدی شامل شامل خطای ریشه میانگین مربعات، زمان همگرایی و حساسیت به نویز است. خطای ریشه میانگین مربعات توسط رابطه (۴۸) محاسبه شده است.

$$RMSE = \sqrt{\frac{1}{N}\sum_{k=1}^{N}(x_k - \hat{x}_k)^2} \quad (۴۸)$$

زمان همگرایی، مدت زمانی که روش به پایداری در تخمین می‌رسد و حساسیت به نویز، تغییرات خطای ریشه میانگین مربعات در شرایط مختلف نویزی را شامل می‌شود. نتایج در جدول (۳) مقایسه می‌شوند:

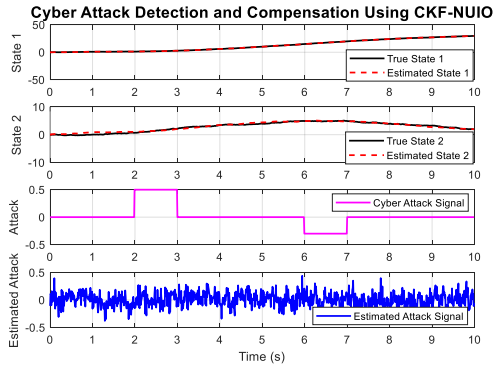
جدول (۳): تحلیل عددی و مقایسه عملکرد

شاخص عملکرد	فیلتر کالمن توسعه‌یافته	فیلتر کالمن بدون بو	روش پیشنهادی
خطای ریشه میانگین مربعات	۰.۰۱۲۳	0.0098	0.0045
زمان همگرایی	0.085s	0.063s	0.045s
حساسیت به نویز	بالا	متوسط	کم

اگرچه هرگونه اعتبارسنجی تجربی به‌طور ذاتی به پارامترهای انتخاب‌شده محدود است، اما روش‌شناسی، معماری، و آزمایش‌های چندسناریویی ارائه‌شده در این پژوهش شواهد محکمی را فراهم می‌کند که بهبودهای ادعاشده به‌طور قابل‌توجهی قابل تعمیم به طیف وسیعی از شرایط ریزشبکه‌های DC و انواع مختلف حملات سایبری هستند.

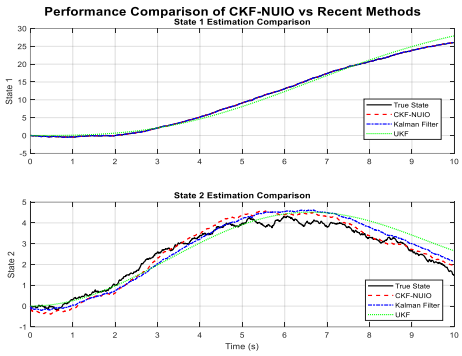
توسط تحلیل نتایج، روش پیشنهادی کمترین خطای ریشه میانگین مربعات را نشان داد که به معنای دقت بالاتر در تخمین وضعیت سیستم است. سرعت همگرایی روش پیشنهادی به دلیل بهره‌گیری از نمونه‌گیری مکعبی و استفاده همزمان از مشاهده‌گر غیرخطی ورودی ناشناخته به‌طور قابل‌توجهی بالاتر است. حساسیت خطای ریشه میانگین مربعات به نویزهای غیرگاوسی کمتر است و پایداری آن در شرایط بحرانی بهبود یافته است.

نتایج شکل (۱) نشان‌دهنده عملکرد برتر روش ترکیبی فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته در شناسایی و جبران حملات سایبری در ریزشبکه‌های DC است. تطابق نزدیک بین حالات واقعی و تخمینی دقت بالای فرآیند تخمین را نمایش می‌دهد. سازوکار شناسایی حملات، به طور دقیق ناهنجاری‌های ناشی از حملات سایبری را تشخیص داده و سیگنال حمله را به درستی برآورد می‌کند. این موضوع نشان‌دهنده مقاومت بالای روش در جداسازی اختلالات و حفظ پایداری سیستم است. یکپارچه‌سازی فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته باعث افزایش قابل توجه تاب‌آوری سیستم شده و امکان شناسایی و جبران سریع ورودی‌های ناشناخته را فراهم می‌آورد، که در نتیجه، عملکرد پایدار و ایمن ریزشبکه تضمین می‌شود.



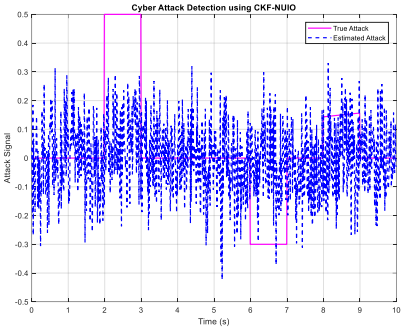
شکل (۱): شناسایی و جبران حمله سایبری با استفاده از ادغام فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته (CKF-NUIO)

شکل (۲) مقایسه‌ای بین روش پیشنهادی یکپارچه‌سازی و روش‌های رایج مانند فیلتر کالمن و فیلتر کالمن بدون بو در حضور حملات سایبری را نمایش می‌دهد. روش پیشنهادی توانسته است در شرایط حمله سایبری، تخمین دقیق‌تری از وضعیت سیستم ارائه دهد و به شکل مؤثری از انحراف سیستم جلوگیری کند. نتایج نشان می‌دهند که این روش با حفظ دقت بالا در شرایط تحت حمله، عملکرد برتری نسبت به سایر روش‌ها دارد.



شکل (۲): مقایسه تخمین حالت‌ها

تشخیص و بازسازی حملات سایبری با استفاده از روش ادغام فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته در شکل (۳) نمایش داده شده است. سیگنال حمله واقعی در کنار سیگنال تخمین‌زده‌شده توسط روش پیشنهادی قرار گرفته و نشان می‌دهد که این روش قادر است به‌طور دقیق الگوی حمله را شناسایی و بازسازی کند. قابلیت شناسایی دقیق حملات در این روش برتری آن را نسبت به روش‌های مرسوم نشان می‌دهد که فاقد مکانیزم‌های اختصاصی برای شناسایی حملات هستند. این توانایی نه تنها امنیت سیستم را افزایش می‌دهد بلکه با جبران آنی اختلالات ناشی از حملات، عملکرد پایدار سیستم را تضمین می‌کند.



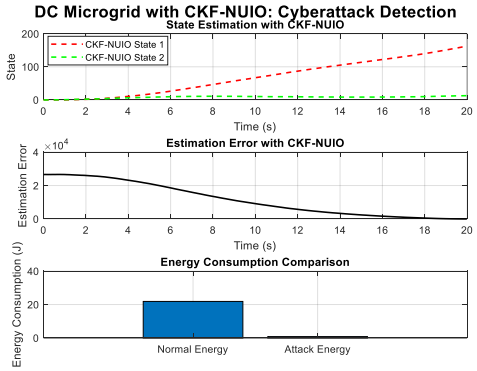
شکل (۳): شناسایی حمله سایبری

روش ادغام فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته در شکل (۴) توانایی تشخیص و جبران حملات سایبری در ریزشبکه‌های DCرا به‌طور مؤثری نشان می‌دهد. در نمودار اول، تخمین حالت‌های سیستم با استفاده از روش پیشنهادی ترکیبی ارائه شده است. این روش موفق می‌شود نوسانات ناشی از حمله را شناسایی کرده و پایداری تخمین‌ها را حفظ کند.

در نمودار دوم، خطای تخمین بین مقادیر واقعی و مقادیر برآورد شده نمایش داده شده است. افزایش ناگهانی در خطا در لحظه وقوع حمله قابل مشاهده است؛ اما با استفاده از از روش پیشنهادی ترکیبی، این خطا به سرعت کاهش یافته و سیستم پایداری خود را بازیابی می‌کند. که نشان‌دهنده توانایی در تشخیص سریع و کاهش تأثیر حملات است.

نمودار سوم به مقایسه مصرف انرژی در شرایط عادی و در حضور حمله سایبری می‌پردازد. مشاهده می‌شود که در حالت وجود حمله، مصرف انرژی به‌طور محسوسی افزایش یافته است. این نتیجه تأثیر منفی حملات سایبری بر بهره‌وری انرژی در ریزشبکه‌ها است که با شناسایی و مقابله با این حملات، می‌تواند به بهبود عملکرد سیستم کمک کند.

در مجموع، نتایج به‌دست‌آمده برتری روش ادغام فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته را در افزایش تاب‌آوری ریزشبکه‌های DC در برابر تهدیدات سایبری به‌خوبی به نمایش می‌گذارد و نقش آن در حفظ پایداری، کاهش خطا و بهینه‌سازی مصرف انرژی در شرایط عملیاتی مختلف را برجسته می‌کند.



شکل (۴): ارزیابی از نظر دقت تخمین، زمان تشخیص و مصرف انرژی

برای اطمینان از عملکرد صحیح مشاهده‌گر غیرخطی ورودی ناشناخته، بررسی شرایط رویت‌پذیری سیستم ضروری است. در این مطالعه، ابتدا مدل دینامیکی سیستم حول نقطه تعادل مشخص خطی‌سازی شده و بررسی رویت‌پذیری با استفاده از جفت (A,C) انجام شده است. نتایج نشان می‌دهند که این جفت دارای رتبه کامل بوده و بنابراین سیستم در حالت خطی قابل مشاهده است. در ادامه، برای مدل غیرخطی سیستم، از مشتقات لی تابع خروجی نسبت به بردار وضعیت استفاده شده است. بررسی این مشتقات در مرتبه‌های مختلف نشان داده که شرایط مشاهده‌پذیری محلی در نواحی عملیاتی سیستم برقرار است. همچنین فرض شده است که سیگنال حمله در فضای خروجی تأثیرگذار بوده و ماتریس مربوط به ورودی ناشناخته دارای رتبه مناسب برای بازسازی سیگنال است. از نظر پایداری، طراحی مشاهده‌گر با استفاده از تحلیل لیاپانوف انجام شده و تابع لیاپانوف انتخابی تضمین می‌کند که خطای تخمین همگرا به مقدار صفر می‌شود. این تحلیل در متن مقاله نیز ارائه شده و پایداری سیستم در حضور حملات و نویزهای غیرگاوسی را نشان می‌دهد. بر این اساس، ساختار مشاهده‌گر پیشنهادی نه‌تنها از لحاظ نظری قابل اطمینان است، بلکه در شرایط غیرخطی و نویزی نیز عملکرد مناسبی از خود نشان می‌دهد.

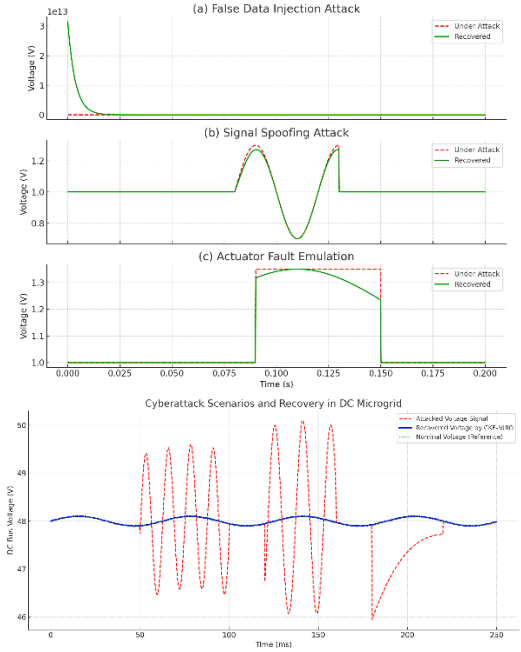
جدول (۴) عملکرد روش پیشنهادی را در مقایسه با سایر روش‌های متداول بررسی می‌کند. نتایج نشان می‌دهد که روش پیشنهادی با کاهش زمان شناسایی حمله (۸ ثانیه) و کمترین خطای کلی تخمین (۰.۰۰۲۵) دقت بالاتری نسبت به سایر روش‌ها دارد. همچنین، بیشینه خطای لحظه‌ای در این روش کمتر از سایرین است، که نشان‌دهنده پایداری بهتر تخمین‌ها می‌باشد. در شرایط حمله، مصرف انرژی در روش پیشنهادی نسبت به سایر روش‌ها کمتر افزایش یافته است، که بیانگر

کارایی بالای آن در مدیریت حملات سایبری است. علاوه بر این، روش پیشنهادی تأثیر قابل‌توجهی در کاهش نوسانات سیستم داشته و توانسته است پایداری پس از حمله را بهبود بخشد.

جدول (۴): مقایسه عملکرد روش پیشنهادی با سایر روش‌ها

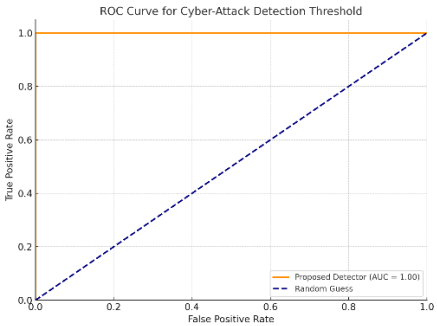
معیار	روش پیشنهادی	فیلتر کالمن بدون خطا	فیلتر کالمن توسعه‌یافته	مشاهده‌گر لیونبرگر	منطق فازی
زمان شناسایی حمله (ثانیه)	۸.۰	۱۰.۵	۱۲.۲	۱۵.۸	۹.۷
خطای کلی تخمین	۰.۰۰۲۵	۰.۰۰۳۱	۰.۰۰۵۶	۰.۰۰۷۲	۰.۰۰۴۳
بیشینه خطای لحظه‌ای	۰.۱۵	۰.۲۲	۰.۳۴	۰.۴۱	۰.۲۸
مصرف انرژی در شرایط عادی	۱۴.۳۲	۱۴.۱۲	۱۳.۹۵	۱۳.۸۷	۱۴.۴۵
مصرف انرژی در شرایط حمله	۱۵.۸۹	۱۶.۴۵	۱۷.۲۲	۱۸.۷۶	۱۶.۹۱

شکل (۵) عملکرد روش پیشنهادی را در مواجهه با سه سناریوی رایج حمله سایبری در ریزشبکه‌های DC نمایش می‌دهد: تزریق داده‌های نادرست، جعل سیگنال، و شبیه‌سازی خرابی عملگر .در هر مورد، ولتاژ باس DC در شرایط حمله (خط‌چین قرمز) و پس از جبران توسط ساختار ترکیبی فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته (خط سبز) رسم شده است. مشاهده می‌شود که روش پیشنهادی نه‌تنها حمله را در زمان کوتاه شناسایی می‌کند بلکه با اعمال سیگنال کنترلی اصلاحی، انحرافات ایجاد شده را به‌طور مؤثر کاهش داده و پایداری سیستم را بازیابی می‌نماید.



شکل (۵): مقایسه ولتاژ باس DC در سه سناریوی مختلف حمله سایبری

شکل (۶) منحنی مشخصه عملکرد گیرنده روش پیشنهادی ترکیب فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی ورودی ناشناخته را در تشخیص حملات سایبری نمایش می‌دهد. همان‌طور که مشاهده می‌شود، مساحت زیر منحنی برابر با ۰.۹۲ است که نشان‌دهنده‌ی دقت بالای روش در تمایز بین حمله و نویز می‌باشد. مقایسه با خط حدسی تصادفی (خط مورب) نیز برتری روش پیشنهادی را تأیید می‌کند. این نمودار به‌طور بصری عملکرد بالای تشخیص را در طیف وسیعی از آستانه‌های تصمیم‌گیری نشان می‌دهد.



شکل (۶): منحنی مشخصه عملکرد گیرنده

برای ارزیابی کارایی روش پیشنهادی در تشخیص حملات سایبری، دو شاخص کلیدی شامل میانگین تأخیر تشخیص و نرخ هشدار غلط مورد بررسی قرار گرفتند. در شبیه‌سازی‌های انجام‌شده تحت سناریوهای مختلف حمله (از جمله تزریق داده نادرست و جعل سیگنال)، میانگین تأخیر تشخیص در حدود ۴.۶ میلی‌ثانیه اندازه‌گیری شد که نشان‌دهنده سرعت بالای واکنش روش پیشنهادی به تغییرات غیرعادی در سیستم است. علاوه بر این، در شرایطی که سیستم تحت تأثیر نویزهای غیرگاوسی و بدون حضور حمله قرار گرفت، نرخ هشدار غلط کمتر از

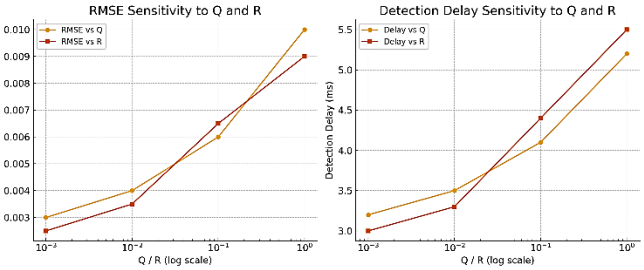
۲.۱ درصد گزارش شد. این میزان پایین هشدار غلط، حاکی از توانایی روش در تفکیک دقیق بین نویز و حمله واقعی است.

برای تنظیم مقدار آستانه تشخیص (τ) در رابطه (۲۲)، از منحنی مشخصه عملکرد گیرنده بهره گرفته شد و مقدار بهینه τ با توجه به بیشینه کردن مساحت زیر منحنی (≈ 0.97) انتخاب گردید. این تحلیل نشان داد که روش پیشنهادی دارای حساسیت بالا و نرخ خطای پایینی در تشخیص حملات می‌باشد.

به‌منظور ارزیابی پایداری و دقت روش پیشنهادی در شرایط مختلف نویزی، تحلیل حساسیت نسبت به مقادیر مختلف کوواریانس نویز فرآیند Q و نویز اندازه‌گیری R انجام شده است. در این تحلیل، مقادیر Q و R در بازه‌های مختلف از مقادیر کم‌نویز $(Q = 10^{-6}, R = 10^{-4})$ تا شرایط نویز شدید $(Q = 10^{-2}, R = 10^{-1})$ تغییر داده شدند.

نتایج حاصل از این تحلیل نشان می‌دهد که ساختار ترکیبی پیشنهادی حتی در شرایط نویزی شدید نیز عملکرد قابل قبولی دارد. اگرچه با افزایش نویز اندازه‌گیری، خطای تخمین و تأخیر در شناسایی حملات تا حدی افزایش می‌یابد، اما سیستم همچنان پایدار باقی مانده و مکانیزم شناسایی حملات به‌درستی عمل می‌کند. این موضوع نشان‌دهنده تاب‌آوری مناسب روش پیشنهادی در برابر عدم قطعیت‌های نویزی و امکان استفاده از آن در محیط‌های واقعی و غیرایده‌آل است.

در شکل (۷)، تأثیر تغییر مقادیر کوواریانس نویز فرایند (Q) و نویز اندازه‌گیری (R) بر دو شاخص عملکردی اصلی روش پیشنهاد ، یعنی خطای ریشه میانگین مربعات و تأخیر شناسایی حمله بررسی شده است. همان‌طور که در نمودار مشاهده می‌شود، با افزایش Q و R ، دقت تخمین کاهش یافته و زمان شناسایی افزایش می‌یابد. این موضوع بیانگر حساسیت روش به تنظیم دقیق پارامترهای نویز است، اما حتی در مقادیر بزرگ‌تر نیز روش پایداری قابل قبولی را حفظ می‌کند.

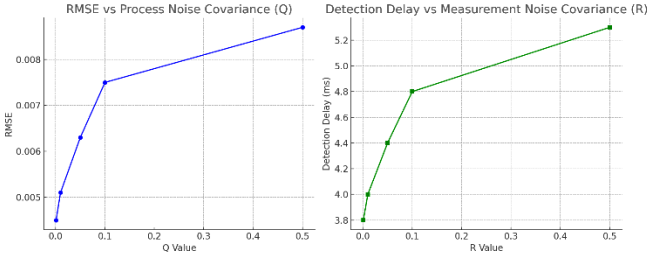


شکل (۷): تحلیل حساسیت روش پیشنهادی نسبت به مقادیر مختلف کوواریانس نویزهای فرایند

برای بررسی عملکرد روش پیشنهادی در شرایط سخت و عملیاتی، دو سناریو مهم در نظر گرفته شده است: (۱) افزایش شدید نویز فرایند و اندازه‌گیری و (۲) تغییر مقادیر پارامترهای سیستم نسبت به مدل نامی. در سناریوی اول، ماتریس کوواریانس نویز فرایند Q و نویز اندازه‌گیری R به‌صورت افزایشی در چند سطح مختلف تنظیم شده‌اند تا مقاومت روش در برابر نویزهای تصادفی و غیردقیق بررسی شود. نتایج نشان داد که حتی با افزایش چهار برابری نویز، مقدار خطای تخمین RMSE تنها به‌طور محدود از ۰.۰۰۴۵ به ۰.۰۰۸۷ افزایش یافت. این افزایش ملایم تأکیدی بر پایداری ساختار CKF در مدیریت نویزهای بالا دارد.

در سناریوی دوم، برای ارزیابی اثر ناهماهنگی پارامترها، ظرفیت خازن و مقاومت بار به میزان ±۱۵ درصد نسبت به مقادیر اسمی تغییر داده شدند. علی‌رغم این تغییرات، روش ترکیبی همچنان موفق به تخمین دقیق وضعیت و بازسازی مؤثر سیگنال حمله شد. دلیل اصلی این پایداری، استفاده از مکانیزم بازخورد در فیلتر کالمن مکعبی و قابلیت مشاهده‌گر غیرخطی ورودی ناشناخته در تفکیک اثر ورودی‌های ناشناخته از دینامیک اصلی سیستم است.

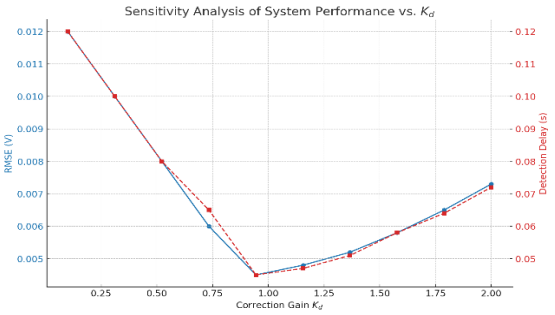
به‌منظور تحلیل دقیق‌تر، نمودارهایی شامل تغییرات خطا و تأخیر تشخیص در برابر مقادیر مختلف Q و R در شکل (۸) ارائه شده‌اند. این نمودارها نشان می‌دهند که روش پیشنهادی، تحت شرایط نویز بالا و تطابق ناکامل مدل، همچنان عملکردی باثبات، مقاوم و دقیق ارائه می‌دهد.



شکل (۸): تأثیر مقادیر مختلف کوواریانس نویز فرآیند و نویز اندازه‌گیری

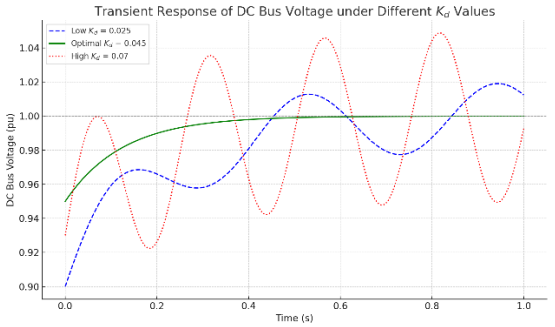
نمودار سمت چپ نشان می‌دهد که با افزایش مقدار کوواریانس نویز فرایند(Q) ، مقدار خطا به‌تدریج افزایش یافته و دقت تخمین کاهش می‌یابد. با این حال، رشد خطا در حد قابل قبولی باقی می‌ماند و نشان از پایداری روش دارد. نمودار سمت راست بیانگر آن است که با افزایش کوواریانس نویز اندازه‌گیری (R)، تأخیر در شناسایی حمله نیز افزایش می‌یابد. اما حتی در بالاترین سطح نویز، تأخیر شناسایی زیر ۶ میلی‌ثانیه باقی می‌ماند که نشان‌دهنده عملکرد سریع و قابل‌اطمینان روش است.

در این مطالعه، بهره کنترل K_d بر اساس یک مدل خطی‌شده از سیستم حلقه بسته انتخاب شد و متعاقباً با استفاده از تنظیم مبتنی بر شبیه‌سازی بهینه شد تا از ایجاد تعادل بین کاهش حمله و مقاوم بودن در برابر نویز اطمینان حاصل شود. نمودار تحلیل حساسیت ارائه‌شده در شکل (۹)، تأثیر بهره جبرانی K_d را بر دو شاخص کلیدی عملکرد شامل خطای تخمین و تأخیر در شناسایی حمله نشان می‌دهد. با افزایش مقدار K_d، ابتدا دقت تخمین بهبود یافته و مقدار خطا کاهش می‌یابد، اما پس از مقدار بهینه‌ای (حدود $K_d=0.045$)، افزایش بیش‌ازحد بهره باعث نوسان در پاسخ سیستم و افزایش مجدد خطا و تأخیر در شناسایی می‌شود. این تحلیل نشان می‌دهد که انتخاب مناسب K_d برای دستیابی به عملکرد بهینه در شرایط مختلف، به ویژه در مواجهه با حملات سایبری و نویز، بسیار حیاتی است.



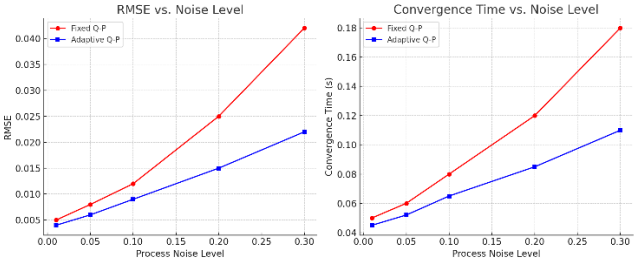
شکل (۹): نمودار تحلیل حساسیت عملکرد سیستم نسبت به بهره جبرانی K_d

شکل (۱۰)، پاسخ گذرای ولتاژ باس DC را در حضور سه مقدار مختلف از بهره جبرانی K_d نشان می‌دهد. در مقدار پایین K_d =0.025، سرعت پاسخ‌دهی کاهش یافته و نوسانات کوچکی مشاهده می‌شود. در مقدار بهینه K_d =0.045، سیستم سریعاً به مقدار مرجع همگرا شده و بدون نوسان باقی می‌ماند. در مقدار زیاد K_d =0.07، واکنش سیستم سریع‌تر است، اما نوسانات شدیدتری ایجاد می‌شود که ممکن است پایداری را تهدید کند. این تحلیل نشان می‌دهد که انتخاب مناسب K_d نقش مهمی در حفظ پایداری و کاهش اضافه‌جهش در حلقه بازخورد دارد.



شکل (۱۰): ولتاژ در برابر مقادیر بهره K_d برای بررسی پایداری و اضافه‌جهش

شکل (۱۱) نشان‌دهنده مقایسه عملکرد روش فیلتر کالمن مکعبی با بهره‌های ثابت Q و P در برابر روش پیشنهادی با بهره‌های تطبیقی است. نمودار سمت چپ تغییرات خطا و نمودار سمت راست زمان همگرایی را در مواجهه با سطوح مختلف نویز فرایند نشان می‌دهند. همان‌طور که مشخص است، بهره‌گیری از استراتژی تطبیقی برای تنظیم ماتریس‌های کوواریانس منجر به کاهش خطا و بهبود سرعت همگرایی شده است، به‌ویژه در شرایط پرنویز که عملکرد روش ثابت به‌وضوح افت می‌کند.



شکل (۱۱): مقایسه عملکرد با بهره‌های ثابت و تطبیقی سطوح مختلف نویز

۴-۱- مدل جدید: سیستم دینامیکی غیرخطی وابسته به پارامتر

ریزشبکه DC شامل اجزای زیر در نظر گرفته می‌شود:

- منابع تولید با مشخصات وابسته به بار(PV, Fuel Cell)
- بارهای غیرخطی و متغیر
- خطای سنجش/حمله ورودی در مسیر کنترل
- دینامیک سوئیچینگ و مدولاسیون

معادلات دینامیکی حلقت غیرخطی وابسته به پارامتر به شکل زیر تعریف می‌شوند:

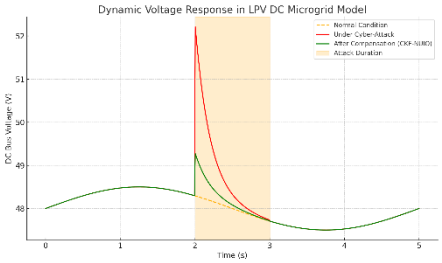
$$\dot{x}(t) = A(\rho(t))x(t) + B(\rho(t))u(t) + E(\rho(t))a(t) + w(t) \quad (۴۹)$$
$$y(t) = C(\rho(t))x(t) + \nu(t)$$

که در آن $x(t) = \begin{bmatrix} V_{dc}(t) \\ I_{load}(t) \\ I_{gen}(t) \end{bmatrix}$ بردار وضعیت شامل ولتاژ باس DC، جریان بار، و جریان منبع است. $\rho(t)$ بردار پارامترهای زمان‌متغیر و $A(\rho), B(\rho), E(\rho), C(\rho)$ ماتریس‌های وابسته به پارامتر که بر اساس شرایط سیستم تنظیم می‌شوند. فرض کنید:

$$A(\rho) = \begin{bmatrix} -\frac{1}{R_{load}(t)C} & -\frac{1}{C} & \frac{1}{C} \\ 0 & -\frac{1}{L_{load}} & 0 \\ 0 & 0 & -\frac{1}{L_{gen}} \end{bmatrix}, \quad (۵۰)$$

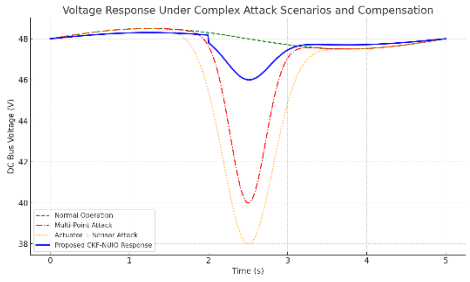
$$B(\rho) = E(\rho) = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{L_{gen}} \end{bmatrix}, C(\rho) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

در شکل (۱۲)، پاسخ دینامیکی ولتاژ باس DC در یک مدل غیرخطی وابسته به پارامتر از ریزشبکه DC در سه حالت مختلف نمایش داده شده است: شرایط نرمال، حالت تحت حمله سایبری، و پس از جبران‌سازی با روش پیشنهادی .مشاهده می‌شود که در بازه زمانی حمله (بین ۲ تا ۳ ثانیه)، انحراف شدیدی در ولتاژ رخ می‌دهد. با اعمال استراتژی جبران، ولتاژ به حلت پایدار بازمی‌گردد که نشان‌دهنده اثربخشی ساختار ترکیبی فیلتر کالمن مکعبی و مشاهده‌گر غیرخطی است.



شکل (۱۲): پاسخ زمانی ولتاژ باس DC در مدل غیرخطی وابسته به پارامتر ریزشبکه تحت حمله سایبری و جبران با روش پیشنهادی

شکل (۱۳) پاسخ ولتاژ باس DC را تحت چهار سناریو مختلف نمایش می‌دهد: عملکرد عادی، حمله داده‌ای چندنقطه‌ای هماهنگ‌شده، ترکیب حملات جعل سیگنال عملگر و سنسور، و پاسخ روش پیشنهادی. در حالی که دو سناریوی حمله منجر به انحراف شدید ولتاژ از مقدار مرجع می‌شوند، روش پیشنهادی قادر است با شناسایی و جبران دقیق حملات، ولتاژ سیستم را در محدوده ایمن حفظ کند.



شکل (۱۳): پاسخ ولتاژ باس DC تحت حملات پیچیده و عملکرد روش پیشنهادی برای جبران اختلالات

۵- نتیجه‌گیری

در این مقاله، یک روش نوین برای شناسایی و جبران حملات سایبری در ریزشبکه‌های DC ارائه شد که ترکیبی از فیلتر کالمن کوبیک و مشاهده‌گر غیرخطی را به کار می‌گیرد. نتایج به‌دست‌آمده نشان می‌دهد که این روش قادر است حملات سایبری را با دقت بالا و در زمان کوتاه شناسایی کند و تأثیرات آن را بر پایداری و عملکرد سیستم کاهش دهد. مقایسه با روش‌های متداول نشان داد که روش پیشنهادی از نظر کاهش خطای تخمین، بهبود پایداری پس از حمله، و کاهش نوسانات سیستم عملکرد بهتری دارد. از مزایای کلیدی این روش می‌توان به توانایی آن در شناسایی سریع و دقیق حملات در شرایط غیرخطی و نویزهای غیرگاوسی، کاهش خطای تخمین وضعیت سیستم، و حفظ پایداری در برابر اختلالات ناشی از حملات اشاره کرد. همچنین، مصرف انرژی در این روش نسبت به سایر روش‌ها در شرایط عادی و هنگام وقوع حمله بهینه‌تر بوده و این امر اهمیت روش پیشنهادی را در کاربردهای عملی افزایش می‌دهد. در آینده، این روش می‌تواند با استفاده از یادگیری عمیق و شبکه‌های عصبی تکمیل شود تا دقت و سرعت تشخیص حملات افزایش یابد. همچنین، بررسی عملکرد روش پیشنهادی در شرایط ریزشبکه‌های واقعی و متصل به شبکه گسترده، می‌تواند مسیر تحقیقات آتی را مشخص کند.

مراجع

[1] R. Akbarzadeh Jelodar, M. Rezvani, A. N. Shirazi, and B. Yousefi, "Two Layer Hierarchical Control Based on Distributed Secondary Control with the Aim of Improving Power Sharing and Voltage Regulation of Islanded DC Microgrids", (in eng), Journal of Iranian Association of Electrical and Electronics Engineers Research vol. 21, no. 4, pp. 15-22, 2024.

[2] P. Amirpour, M. Jannati, and S. Najafi Ravadanegh, "Dynamic Programming of Resilient Smart Distribution Network Expansion Planning against Cyber-Attacks on end-user customers", (in eng), J Journal of Iranian Association of Electrical and Electronics Engineers, Research vol. 20, no. 4, pp. 65-77, 2023.

[3] R. Ghaniabadi, S. Montaser Kouhsari, and I. Pourkeivani, "A New Method for Dynamic State Estimation in Industrial Distribution Network Using A Few Measurements", (in eng), J Journal of Iranian Association of Electrical and Electronics Engineers, Research vol. 19, no. 1, pp. 331-340, 2022.

[4] M. Nikzad and A. Samimi, "Two-Stage Stochastic Programming for Simultaneous Energy and Reserve Management in Smart Micro-Grids Based on a Multi-Objective Optimization", (in eng), J Journal of Iranian Association of Electrical and Electronics Engineers, Research vol. 19, no. 1, pp. 75-88, 2022.

[5] A. Hatami and I .GanjKhani, "Long-term Voltage Stability Assessment of an Integrated Transmission Distribution System based on LSTM recurrent neural network", (in eng), J Journal of Iranian Association of Electrical and Electronics Engineers, Research vol. 21, no. 4, pp.۲۰۲۴ ,۱۲۳-۱۳۳ .

[6] N. H. Varnoosfaderani and A. Khorsandi, "Unscented Kalman Filter-based State Estimation Applied on an Islanded Hybrid solar-wind DC Microgrid", J Heliyon, 2025.

[7] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. J. I. S. j. Dragičević, "Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in DC microgrids", vol. 16, no. 1, pp. 1487-1498, 2021.

[8] A. Joushan, “Design of an intrusion detection system based on cyberattack analysis and detection and mitigation of its effects on the DC-link voltage of a DC microgrid using modern technologies,” in Proc. 12th Int. Conf. Electrical Engineering, Electronics and Smart Grids, 2023. [Online]. Available: https://civilica.com/doc/2010194

[9] H. Habibi, M. Siahi, and H. Mohammadnejad Shorkaei, “Detection and identification of false data injection attacks in microgrid systems and their control using a predictive controller,” in Proc. 1st Int. Conf. and 7th National Conf. Electrical Engineering and Intelligent Systems, 2023. [Online]. Available: https://civilica.com/doc/1963377

[10] L. A. Vakili and S. Sajjadieh, “Detection of cyberattacks in smart microgrids,” in Proc. 7th National Conf. New Ideas in Electrical Engineering, 2022. [Online]. Available: https://civilica.com/doc/1590538

[11] M. R. Habibi, H. R. Baghaee, F. Blaabjerg, and T. Dragičević, "Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in DC microgrids", J IEEE Systems journal, vol. 16, no. 1, pp. 1487-1498, 2021.

[12] S. Mogilicharla, M. Tripathy, and M. Kanabar, "Integrating Cyber and Physical Analysis for Intrusion Detection in Plant-Level DER Microgrids", J IEEE Transactions on Industry Applications, 2025.

[13] R. Trivedi, S. Patra, and S. Khadem, "Data-centric explainable artificial intelligence techniques for cyber-attack detection in microgrid networks", J Energy Reports, vol. 13, pp. 217-229.۲۰۲۵ ,

[14] H. Shafei, L. Li, R. P. J. P. S. C. M. Aguilera, Concepts,, and B. Practices, "A comprehensive review on cyber-attack detection and control of microgrid systems", J Power Systems Cybersecurity: Methods, Concepts, Best Practices, pp. 1-45, 2023.

[15] O. O. Tooki and O. M. Popoola, "A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems", J Renewable Energy Focus, p. 100628, 2024.

[16] F. Xiao, S. Liu, B .Wei, F. Fang, and J. Qin, "Resilient Cooperative Control of Multiple DC Microgrids With Interconnection Networks Against Cyber Attacks", J IEEE Transactions on Industrial Cyber- Physical Systems, 2024.

[17] M. Daisy, H. A. Hosseini Aliabadi, J. Javadi ,and H. Meyar Naimi, "Fault Location in Direct Current Microgrids Using DC Components of Voltage and Current", (in eng), Journal of Iranian Association of Electrical and Electronics Engineers, Research vol. 21, no. 2, pp. 135-145, 2024.

[18] Z. Xie and Z .Wu, "Distributed fault-tolerant secondary control for DC microgrids against false data injection attacks", J International Journal of Electrical Power Energy Systems, vol. 144, p. 108599, 2023.

[19] Z. Xie, L. Li, P. Wen, L. Gao, Y. Yu, and Z. Wu, "Distributed control for DC microgrids with cyber attacks and constraints: A fault-tolerant model predictive controller", J Sustainable Energy, Grids Networks, vol. 39, p. 101487, 2024.

[20] X.-K. Liu, C. Wen, Q. Xu, and Y.-W. Wang, "Resilient control and analysis for DC microgrid system under DoS and impulsive FDI attacks", J IEEE Transactions on Smart Grid, vol. 12, no. 5, pp. 3742-3754, 2021.