Journal of Iranian Association of Electrical and Electronics Engineers
Vol. 21 No. 4, 2024
DOI: 10.61186/jiaeee.21.4.92

Feedback Linearization-Based Control Strategy with the Ability to Detect and Compensate False Data Injection Attack for Multi-Level DSTATCOM in Smart Grids

Hamidreza Toodeji[1] , Mohsen Jannati[2]

[1]Assistant Professor, Electrical Engineering Department, Yazd University, Yazd, Iran
toodeji@yazd.ac.ir
[2]Associate Professor, Department of Electrical Engineering, Shahreza Campus, University of Isfahan, Iran
m.jannati@shr.ui.ac.ir

Abstract:
Modern voltage control strategies in the present distribution networks require efficient equipment and appropriate communication channels between these equipment, sensors, and control centers, leading to smart distribution networks with a complex cyber-physical nature. One of the efficient equipment for voltage control in modern distribution networks is the DSTATCOM, which uses multilevel converters in its structure, provides many advantages, such as direct connection to the grid. A DSTATCOM with a multilevel converter requires a cyber-physical network between the controller and its components due to the presence of many controllable components, which makes it vulnerable to cyber-attacks when connected to the present smart distribution networks. In this paper, a feedback linearization-based controller is developed for the cascaded multilevel DSTATCOM, and a discrete Kalman filter-based method is proposed to detect and compensate for false data injection cyber-attacks on voltage sensors of the multilevel converter. The abilities of the proposed nonlinear controller to control the multilevel DSTATCOM and the reliable operation against false data injection attacks are verified through the simulation of a test power network in the MATLAB/Simulink environment.

Keywords: **DSTATCOM, Cascaded multilevel converter, False data injection attack, Kalman filter, Feedback linearization-based controller, Smart grid.**

Article Type: **Research**

Received: 05. 14. 2023

Revised: 18. 11. 2023

Accepted: 01. 06. 2024

Corresponding author: H. Toodeji

Corresponding author's address: Elec. Eng. Dep., Yazd Uni., University Blvd., Safayieh, Yazd, Iran

[Downloaded from jiaeee.com on 2026-11-20]

[DOI: 10.61186/jiaeee.21.4.77]

Copyright © 2024 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

The integration of advanced voltage control methods within contemporary distribution grids necessitates not only robust equipment but also seamless communication infrastructures bridging diverse devices, sensors, and central control units. The evolution towards smart grids has accentuated this need, rendering these systems intricate in their cyber-physical architecture. Among the apparatuses facilitating voltage regulation in these modern networks is the DSTATCOM, which uses multi-level converters and offers direct grid connectivity. However, integration of a multilevel DSTATCOM in a comprehensive cyber-physical distribution grid, makes it susceptible to cyber-attacks.

This paper addresses this vulnerability by presenting a feedback linearization-based control strategy developed for cascaded multilevel DSTATCOM systems. Additionally, a discrete Kalman filter-based method is proposed to detect and compensate for false data injection cyber-attacks targeted at voltage sensors embedded within the multilevel converter. The efficacy of the proposed nonlinear controller in regulating the multilevel DSTATCOM is rigorously assessed, coupled with its robustness against false data injection attacks, through simulations of a test system in MATLAB/Simulink. The outcomes of this study aim to contribute substantially to enhancing the security and performance of multi-level DSTATCOMs within the interconnected framework of smart grids.

2. Contributions

Development of feedback linearization-based controller for the cascaded multilevel DSTATCOM in modern smart grids: The controller's design considers the complex cyber-physical nature of these networks and enhances voltage control in smart grids, contributing significantly to improved network performance and stability.

Cyber-physical vulnerability mitigation: recognizing the vulnerability of multilevel DSTATCOM to cyber-attacks when integrated into smart distribution networks, this paper proposes a discrete Kalman filter-based method. This method effectively detects and compensates for false data injection cyber-attacks on voltage sensors, ensuring the system's resilience against potential security threats.

3. Procedures

The research methodology encompasses a comprehensive series of steps to devise and assess the effectiveness of the proposed feedback linearization-based control strategy and the discrete Kalman filter-based method for countering false data injection attacks on multilevel DSTATCOM voltage sensors. Initially, an in-depth analysis of the multilevel DSTATCOM architecture and its integration into smart distribution grids is conducted. Mathematical modeling of the DSTATCOM and its control system is formulated, incorporating the feedback linearization approach for controller design.

Subsequently, potential attacks and vulnerabilities within the DSTATCOM system are identified. A discrete Kalman filter-based algorithm is developed to detect and compensate for false data injection attacks specifically targeting voltage sensors integrated into the multilevel converter.

Implementation of the proposed control strategy and cyber-attack detection method involves simulations of various scenarios using MATLAB/Simulink. Extensive validation is performed using a test system to evaluate the efficacy and robustness of the proposed controller in controlling the multilevel DSTATCOM while ensuring resilience against cyber-attacks.

4. Findings

this paper presents a robust control strategy based on feedback linearization developed for the cascaded multilevel DSTATCOM. The proposed nonlinear controller aims to efficiently regulate the operation of the multilevel DSTATCOM, ensuring precise voltage control and stability in varying grid conditions. Additionally, a discrete Kalman filter-based method is introduced as a novel approach to detect and compensate for false data injection cyber-attacks targeting voltage sensors embedded within the multilevel converter.

The effectiveness and resilience of the developed controller against both conventional operational demands and deliberate cyber-attacks are assessed through simulations in MATLAB/Simulink. Specifically, a test system is employed to evaluate the performance of the proposed controller under diverse operating conditions, including transient disturbances and cyber-attacks aimed at compromising the accuracy of voltage sensor readings.

The simulation results demonstrate the proficiency of the feedback linearization-based controller in effectively regulating the multilevel DSTATCOM's performance, ensuring precise voltage control and system stability. Furthermore, the integration of the discrete Kalman filter-based approach showcases promising capabilities in swiftly detecting and compensating false data injection cyber-attacks on voltage sensors, thereby reinforcing the cyber-physical security of the DSTATCOM within smart grids. The findings underscore the importance of integrating advanced control methods with cybersecurity measures to fortify the resilience of distribution systems against emerging threats, thereby fostering a more resilient and secure smart grid infrastructure.

5. Conclusion

Integrating sophisticated control strategies and cybersecurity measures has become imperative in ensuring the efficient and secure operation of modern smart grids. This paper addresses the critical challenges associated with voltage control in such networks. DSTATCOM with multilevel converters has emerged as a promising solution for voltage control due to its direct grid connection and numerous advantages in enhancing

[Downloaded from jiaeee.com on 2026-11-20]

[DOI: 10.61186/jiaeee.21.4.77]

power quality. However, the complexity of these systems, coupled with their integration into cyber-physical networks, renders them susceptible to cyber-attacks.

To mitigate these vulnerabilities, the present study proposes a novel approach combining a feedback linearization-based controller for the multilevel DSTATCOM with a discrete Kalman filter-based method. The controller design offers enhanced capabilities in regulating the DSTATCOM's performance, ensuring effective voltage control within the distribution network. Furthermore, the integration of the discrete Kalman filter-based method enables the detection and compensation of false data injection cyber-attacks targeting the voltage sensors of the multilevel converter.

This research c combines an advanced control method with cybersecurity measures to enhance the resilience and reliability of voltage control systems in smart grids. And, pave the way for further research for enhancing the performance and security of smart grids, ensuring their efficient and resilient operation in the face of evolving cyber threats.

[Downloaded from jiaeee.com on 2026-11-20]

[DOI: 10.61186/jiaeee.21.4.77]

نشریه مهندسی برق و الکترونیک ایران

نشریه مهندسی برق و الکترونیک ایران، سال بیست و یکم، شماره چهارم، زمستان ۱۴۰۳، صفحات ۹۲-۱۰۳

DOI: 10.61186/jiaeee.21.4.92

طراحی کنترل‌کننده براساس خطی‌سازی بازخورد با قابلیت تشخیص و جبران حمله تزریق داده نادرست برای DSTATCOM چندسطحی در شبکه‌های توزیع هوشمند

حمیدرضا تودجی[۱]، محسن جنتی[۲]

۱- استادیار- دانشکده مهندسی برق- دانشگاه یزد- ایران

toodeji@yazd.ac.ir

۲- دانشیار- دانشکده فنی و مهندسی- مرکز آموزش عالی شهرضا- دانشگاه اصفهان- ایران

m.jannati@shr.ui.ac.ir

چکیده: طرح‌های نوین کنترل ولتاژ در شبکه‌های توزیع امروزی به تجهیزات کارآمد و نیز کانال‌های ارتباطی مناسب بین این تجهیزات، حسگرها و مراکز کنترل نیاز دارند که منتهی به شبکه‌های توزیع هوشمندی با ماهیت سایبری-فیزیکی پیچیده‌ای شده است. یکی از تجهیزات کارآمد کنترل ولتاژ در شبکه‌های توزیع مدرن، جبرانساز DSTATCOM می‌باشد که استفاده از ساختار مبدل‌های چندسطحی در معماری آن، مزایای زیادی نظیر امکان اتصال مستقیم به شبکه را ایجاد خواهد نمود. یک DSTATCOM با ساختار چندسطحی به دلیل وجود اجزای کنترل پذیر زیاد، نیاز به شبکه سایبری-فیزیکی بین کنترل‌کننده و اجزای خود دارد که در اتصال با شبکه‌های توزیع هوشمند امروزی، آن را مستعد حملات سایبری می‌نماید. در مقاله حاضر، یک کنترل‌کننده غیرخطی براساس خطی‌سازی بازخورد برای DSTATCOM چندسطحی آبشاری توسعه داده شده و برای تشخیص و جبران حملات سایبری از نوع تزریق داده نادرست به حسگرهای ولتاژ مبدل چندسطحی، روشی مبتنی بر الگوریتم فیلتر کالمن گسسته پیشنهاد می‌گردد. قابلیت‌های کنترل‌کننده غیرخطی پیشنهادی برای کنترل DSTATCOM چندسطحی و نیز عملکرد قابل اعتماد در مقابله با حملات تزریق داده نادرست، از طریق شبیه‌سازی یک سیستم قدرت نمونه در محیط نرم‌افزار MATLAB/Simulink نشان داده خواهد شد.

کلمات کلیدی: جبرانساز DSTATCOM، مبدل چندسطحی آبشاری، حمله تزریق داده نادرست، فیلتر کالمن، کنترل‌کننده غیرخطی برمبنای خطی‌سازی بازخورد، شبکه توزیع هوشمند.

نوع مقاله: پژوهشی

دریافت : ۱۴۰۲/۲/۲۴

بازنگری: ۱۴۰۲/۰۸/۲۷

پذیرش: ۱۴۰۲/۱۰/۱۶

نام نویسنده‌ی مسئول: دکتر حمیدرضا تودجی

نشانی نویسنده‌ی مسئول: ایران – یزد – صفائیه- خیابان دانشگاه – دانشگاه یزد – دانشکده‌ی مهندسی برق

[Downloaded from jiaeee.com on 2026-11-20]

[DOI: 10.61186/jiaeee.21.4.77]

حق انتشار این مستند، متعلق به نویسندگان آن است. ۱۴۰۳ ©. 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

در شبکه‌های توزیع، پروفیل ولتاژ یکی از مهم‌ترین شاخص‌های عملکردی بوده و بهره‌برداران شبکه از راهبردهای متعددی برای حفظ ولتاژ مصرف‌کنندگان در محدوده قابل قبول و نیز حفظ پایداری ولتاژ استفاده می‌کنند [۱، ۲]. گسترش استفاده از منابع تولید پراکنده و خصوصا افزایش نفوذ منابع انرژی تجدیدپذیر مانند توربین‌های بادی و پنل‌های فتوولتاییک مقیاس کوچک در شبکه‌های توزیع، منجر به بروز مشکلاتی نظیر نامتعادلی، افزایش تلفات، نوسانات ولتاژ و اضافه ولتاژ شده است [۳، ۴]. به دنبال بروز این‌گونه مشکلات در شبکه‌های توزیع مدرن و نیز به دلیل لزوم رعایت استانداردهای موجود [۵]، طرح‌های نوینی برای کنترل ولتاژ در شبکه‌های توزیع پیشنهاد شده است که آن‌ها را می‌توان در چهار دسته تقسیم‌بندی نمود: راهبرد کنترل محلی، غیرمتمرکز، توزیع‌شده و متمرکز. در راهبرد کنترل محلی ولتاژ، تصمیمات کنترلی براساس اندازه‌گیری‌های ولتاژ/جریان محلی در نقطه اتصال گرفته می‌شود. اگرچه در این راهبرد، نیازی به شبکه تبادل اطلاعات وجود ندارد ولی نمی‌توان عملکرد هماهنگی با بهره‌بردار شبکه داشت [۶]. در راهبرد غیرمتمرکز، کنترل محلی ولتاژ با استفاده از یک سیستم ارتباطی محلی بهبود پیدا نموده [۷، ۸] و در راهبرد کنترل ولتاژ توزیع شده، اطلاعات گره‌های همسایه از طریق کانال‌های ارتباطی تقویت‌شده، دریافت می‌شود [۹]. در راهبرد کنترل متمرکز ولتاژ، از شبکه‌های ارتباطی پیچیده برای تنظیم ولتاژ از طریق کنترل هماهنگ تجهیزات موجود استفاده می‌شود [۱، ۱۰].

با این توضیحات مشخص می‌گردد که در راهبردهای مدرن کنترل ولتاژ در شبکه‌های توزیع، به کانال‌های ارتباطی مناسب بین حسگرها، اجزای شبکه و کنترل‌کننده‌ها نیاز است که در عمل، شبکه‌های توزیع را به سیستم‌های سایبری- فیزیکی پیچیده‌ای تبدیل می‌کند [۱۰]. این موضوع، آسیب‌پذیری شبکه توزیع را در برابر حملات سایبری افزایش می‌دهد. به عنوان نمونه، یک حمله سایبری به سیستم کنترل نظارتی و جمع‌آوری داده‌ها (اسکادا) ممکن است به مهاجم اجازه دسترسی به تمام تجهیزات، به ویژه سیستم‌های کنترلی را بدهد؛ چرا که نشان داده شده است پروتکل‌های ارتباطی مرسوم سیستم‌های اسکادا در برابر حملات سایبری، آسیب‌پذیر هستند [۱۱]. اجرای یک حمله سایبری نسبت به حملات فیزیکی بسیار آسان‌تر بوده و به علاوه، با هماهنگ کردن حملات فیزیکی و سایبری می‌توان خسارات گسترده‌تری به شبکه وارد نمود. مسائل مربوط به حملات سایبری در سیستم‌های الکتریکی مانند ریزشبکه‌ها [۱۲]، شبکه‌های هوشمند [۱۳، ۱۶-۱۴] و سیستم‌های قدرت مدرن [۱۷] مورد مطالعه قرار گرفته‌اند. در سال ۲۰۱۵، شبکه برق اوکراین پس از یک حمله تزریق داده نادرست به مقادیر اندازه‌گیری‌شده حسگرهای شبکه برق، ناپایدار شد و ۲۲۵ هزار مشترک، خاموشی گسترده و خسارات ناشی از آن را تجربه کردند [۱۸]. نمونه‌هایی از انواع متداول حملات سایبری عبارتند از: حمله تزریق داده نادرست، حمله به تمامیت اطلاعات، حمله منع خدمت و حمله بازسازی اطلاعات [۱۹]. در حمله تزریق داده نادرست که در این مقاله مورد توجه قرار می‌گیرد، داده‌های خرابکارانه‌ای توسط مهاجم به سیستم نظارت و کنترل اعمال می‌گردد تا فرآیند کنترل را دچار اشتباه نماید. روش‌های پیشنهادی برای آشکارسازهای حمله تزریق داده نادرست، عمدتاً از روش‌های تخمین مبتنی بر مشاهده مانند فیلتر کالمن [۲۰]، فیلتر ذرات [۲۱] و نیز ناظران مبتنی بر هوش مصنوعی مانند روش‌های مبتنی بر شبکه‌های عصبی [۲۲] و یادگیری تقویتی [۲۳] استفاده کرده‌اند.

یکی از تجهیزاتی که در شبکه‌های توزیع مدرن برای کنترل ولتاژ استفاده می‌شود، جبران‌کننده ایستای توزیع (DSTATCOM) می‌باشد که پاسخی سریع و ظرفیتی بزرگ برای تبادل توان راکتیو دارد [۲۴]. به طور معمول، نمی‌توان DSTATCOM که از یک مبدل دو یا سه سطحی مرسوم استفاده می‌کند را به صورت مستقیم به شبکه توزیع متصل نمود و نیاز به استفاده از یک ترانسفورماتور برای اتصال وجود دارد که مشکلات خاص خود را ایجاد می‌کند. راه‌حل این مشکل استفاده از مبدل‌های چندسطحی است که امروزه به دلیل مزایای متعددی نظیر ماژولار بودن، امکان اتصال مستقیم به شبکه ولتاژ زیاد، راندمان بالا و اعوجاج هارمونیکی کم، کاربرد گسترده‌ای پیدا کرده‌اند [۲۵]. از سوی دیگر، کنترل متمرکز یک DSTATCOM با معماری چندسطحی به دلیل وجود اجزای کنترل‌پذیر زیاد، نیاز به شبکه ارتباطی پیچیده‌ای دارد که با استفاده از رویکرد کنترل توزیع‌شده، یک سیستم ماژولار با سیم سیگنال کمتر به دست می‌آید [۲۶]. اگر چه در رویکرد کنترل توزیع‌شده، شبکه ارتباطی ساده‌تری استفاده می‌گردد ولی اتصال آن به کانال‌های ارتباطی شبکه توزیع هوشمند در مقیاسی بزرگتر، آن را مستعد حملات سایبری می‌نماید. در چنین شرایطی یک حمله سایبری برنامه‌ریزی‌شده به DSTATCOM که هماهنگ با اجزای دیگر شبکه، وظیفه کنترل ولتاژ را برعهده دارد می‌تواند منجر به خروج آن از مدار شده و یا باعث عملکرد نامطلوب آن در جهت تشدید افت/اضافه ولتاژها شبکه گردد. روشن است که چنین وضعیتی می‌تواند شبکه توزیع را در معرض ناپایداری ولتاژ قرار دهد. نوآوری‌های اصلی مقاله حاضر عبارتند از:

- طراحی یک کنترل‌کننده غیرخطی براساس خطی‌سازی بازخورد برای DSTATCOM چندسطحی آبشاری با قابلیت کنترل مستقل ولتاژ خازن مبدل‌ها
- پیشنهاد واحد تشخیص و جبران حمله تزریق داده نادرست برمبنای الگوریتم فیلتر کالمن گسسته برای این جبرانساز.

سازماندهی مقاله حاضر بدین صورت می‌باشد که در بخش دوم، ابتدا یک پیکربندی چندسطحی آبشاری برای DSTATCOM پیشنهاد شده و سپس یک کنترل‌کننده غیرخطی براساس خطی‌سازی بازخورد برای متعادل‌سازی ولتاژ خازن‌های این مبدل چندسطحی و نیز انجام وظایف کنترلی سطح بالای آن (مانند کنترل ولتاژ/ توان راکتیو شبکه توزیع) طراحی می‌گردد. در ادامه، به منظور مقابله با

[Downloaded from jiaeee.com on 2026-11-20]

[DOI: 10.61186/jiaeee.21.4.77]

حملات سایبری به این جبرانساز، قابلیت تشخیص و جبران حمله تزریق داده نادرست برمبنای الگوریتم فیلتر کالمن گسسته به این کنترل‌کننده افزوده می‌شود. لازم به ذکر است که حملات سایبری به مبدل‌های چندسطحی، به صورت محدود و فقط در کاربردهای مربوط به HVDC مورد مطالعه قرار گرفته است [۱۷، ۲۷]. از سوی دیگر، اگر چه موضوع امنیت سایبری شبکه توزیع هوشمند در پژوهش‌های متعددی بررسی گردیده است ولی حمله سایبری به جبرانساز DSTATCOM با ساختار چندسطحی تاکنون موردمطالعه قرار نگرفته است [۱۰، ۱۴ – ۱۶]. بنابراین مقاله حاضر، پژوهشی پیشگام در این زمینه می‌باشد. در بخش سوم مقاله، برای نشان دادن قابلیت‌های کنترل‌کننده غیرخطی پیشنهادی برای انجام وظایف کنترلی و نیز مقابله با حملات تزریق داده نادرست، یک سیستم قدرت نمونه در محیط نرم‌افزار MATLAB/Simulink شبیه‌سازی شده و نتایج آن مورد بررسی و تحلیل قرار خواهند گرفت.

۲- کنترل‌کننده غیرخطی برمبنای خطی‌سازی بازخورد با قابلیت تشخیص و جبران حمله سایبری

در این قسمت، ابتدا پیکربندی کلی یک DSTATCOM چندسطحی معرفی شده و سپس مدل فضای حالت آن به دست آورده می‌شود. در ادامه، یک قانون کنترل غیرخطی براساس راهبرد خطی‌سازی بازخورد برای این سیستم طراحی شده و روشی مبتنی بر الگوریتم فیلتر کالمن گسسته به منظور تشخیص و جبران حمله تزریق داده نادرست برای آن توسعه داده می‌شود.

۲-۱- پیکربندی DSTATCOM چندسطحی

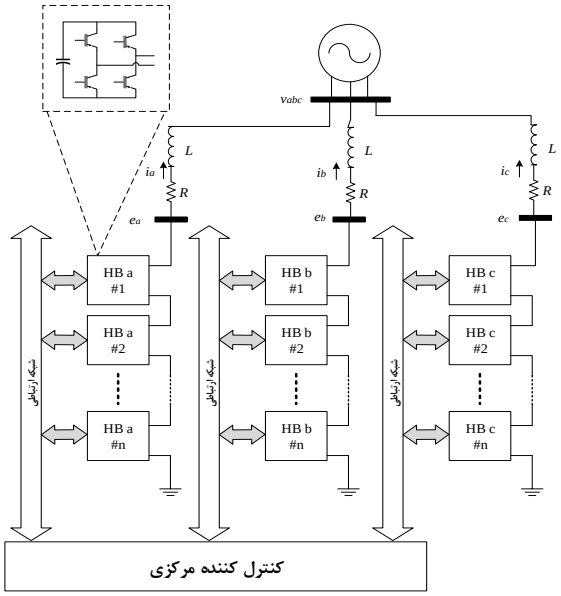
ساختار یک DSTATCOM چندسطحی آبشاری سه‌فاز برای کاربرد در شبکه توزیع در شکل (۱) نشان داده شده است. مشاهده می‌شود که در هر فاز، n مبدل تمام پل به صورت آبشاری قرار گرفته و توسط شاخص‌های مدولاسیون $m_i\ i\ ,=1,\dots,n$ و همچنین یک زاویه فاز δ کنترل می‌شوند. همچنین، مبدل‌هایی که در فازهای مختلف قرار داشته ولی شماره یکسانی دارند، شاخص‌های مدولاسیون همسانی دارند. همان‌گونه که از شکل (۱) مشخص است، مبدل‌های آبشاری موجود در این ساختار به صورت مستقل از یکدیگر عمل نموده و برای ارسال داده‌های اندازه‌گیری و نیز دریافت فرامین کنترلی، از طریق یک شبکه ارتباطی محلی به کنترل‌کننده مرکزی متصل هستند.

۲-۲- مدلسازی سیستم در فضای حالت

در این بخش، یک مدل فضای حالت زمان پیوسته از DSTATCOM چندسطحی آبشاری به دست آورده می‌شود تا در قسمت بعد، کنترل‌کننده غیرخطی براساس آن طراحی گردد. برای این منظور معادلات الکتریکی حاکم بر سمت AC جبرانساز DSTATCOM با اعمال KVL و KCL و استفاده از تبدیل $abc \rightarrow dq0$ به دست آورده می‌شوند که در (۱) نشان داده شده‌اند:

$$\begin{cases} L\dfrac{dI_d}{dt}+RI_d-\omega I_q-V_d+\left(E_{d,1}+\cdots+E_{d,n}\right)=0 \\ L\dfrac{dI_q}{dt}+\omega I_d+RI_q-V_q+\left(E_{q,1}+\cdots+E_{q,n}\right)=0 \end{cases} \quad (۱)$$

در این رابطه، I_d، I_q و V_d، V_q به ترتیب مولفه‌های جریان و ولتاژ محور d و q در محل اتصال به شبکه توزیع هستند. مولفه‌های ولتاژ محور d و q سمت AC مبدل i اُم نیز با $E_{d,i}$,$E_{q,i}$;$i\ =1,\dots,n$ نشان داده شده‌اند. با انتخاب ولتاژ شبکه AC به عنوان قاب دوار در تبدیل $abc \rightarrow dq0$، مقادیر $V_d=|V|$, $V_q=0$ به دست می‌آید.



شکل (۱): پیکربندی DSTATCOM چندسطحی آبشاری سه فاز

با مدلسازی تلفات مبدل‌های چندسطحی به صورت یک مقاومت و ادغام آن در R، می‌توان مبدل‌ها را بدون تلفات فرض نمود. در نتیجه، توان در سمت AC و DC هر مبدل با هم برابر بوده و می‌توان رابطه تعادل توان برای مبدل i اُم در مختصات dq را به صورت (۲) نوشت. لازم به ذکر است که در پژوهش حاضر، به دلیل آن‌که ساختاری جدید برای مبدل چندسطحی و یا روش کلیدزنی جدیدی با هدف کاهش تلفات ارائه نگردیده است [۲۸، ۲۹]، کنترل‌کننده غیرخطی پیشنهادی تاثیر قابل ملاحظه‌ای بر تلفات مبدل نخواهد داشت.

$$C_i\cdot\frac{dV_{dc,i}}{dt}\cdot V_{dc,i}=\frac{1}{2}\left(E_{d,i}\cdot I_d+E_{q,i}\cdot I_q\right) \quad (۲)$$

در این رابطه، $V_{dc,i}$, C_i ;$i\ =1,\dots,n$ به ترتیب، مقدار خازن و ولتاژ DC مبدل i اُم می‌باشد. باید توجه نمود که مبدل‌هایی که در فازهای مختلف قرار داشته ولی شماره یکسانی دارند، وضعیت کاملا مشابهی را تجربه می‌کنند.

[Downloaded from jiaeee.com on 2026-11-20]

[DOI: 10.61186/jiaeee.21.4.77]

برای تحلیل مبدل‌هایی که از روش کلیدزنی PWM استفاده نموده و فرکانس موج مرجع به‌طور قابل‌توجهی از فرکانس کلیدزنی کوچک‌تر است، می‌توان با کمک میانگین‌گیری از متغیرها در یک دوره کلیدزنی، فقط مولفه‌های فرکانس پایین آن‌ها در نظر گرفت و مدلی ساده‌تر با دقتی قابل قبول به دست آورد [۳۰]. با میانگین‌گیری از $E_{d,i}$ و $E_{q,i}$ در یک دوره تناوب کلیدزنی، روابط ساده شده (۳) به دست می‌آید.

$$\begin{cases} |E_i| = \sqrt{E_{d,i}^2 + E_{q,i}^2} \\ |E_i| = m_i . V_{dc,i} \end{cases} \Rightarrow \begin{cases} E_{d,i} = m_i . V_{dc,i} . \cos\delta \\ E_{q,i} = m_i . V_{dc,i} . \sin\delta \end{cases}, \; i = 1, \cdots, n \qquad (۳)$$

با جایگزینی (۳) در (۱) و (۲)، معادلات حالت جبرانساز DSTATCOM چندسطحی آبشاری به صورت (۴) به دست می‌آید:

$$\begin{cases} \frac{d}{dt} I_d = -\frac{R}{L} I_d + \omega I_q + \frac{m_1 \cos\delta}{L} V_{dc,1} \cdots + \frac{m_n \cos\delta}{L} V_{dc,n} - \frac{|V|}{L} \\ \frac{d}{dt} I_q = -\frac{R}{L} I_q - \omega I_d + \frac{m_1 \sin\delta}{L} V_{dc,1} \cdots + \frac{m_n \sin\delta}{L} V_{dc,n} \\ \frac{dV_{dc,i}}{dt} = \frac{1}{2} \frac{m_i \cos\delta}{C_i} I_d - \frac{1}{2} \frac{m_i \sin\delta}{C_i} I_q \quad , \quad i = 1, \ldots, n \end{cases} \qquad (۴)$$

توجه دقیق‌تر به این معادلات نشان می‌دهد که شاخص‌های مدولاسیون $m_i \; i = 1, \ldots, n$ و زاویه فاز δ در مدل فضای حالت، به صورت $m_i \cos\delta$ ،$m_i \sin\delta$ ظاهر شده‌اند. بنابراین، ورودی‌های کنترل را می‌توان به شکل (۵) در نظر گرفت:

$$\begin{bmatrix} u_1 & u_2 & \cdots & u_{n+1} \end{bmatrix}^T = \begin{bmatrix} \tan\delta & m_1 \cos(\delta) & \cdots & m_n \cos(\delta) \end{bmatrix}^T \qquad (۵)$$

با جایگزینی (۵) در (۴)، مدل فضای حالت جبرانساز DSTATCOM چندسطحی با ورودی‌های کنترلی (۵) به صورت (۶) به دست می‌آید:

$$\begin{bmatrix} \frac{d}{dt}x_1 \\ \frac{d}{dt}x_2 \\ \frac{d}{dt}x_3 \\ \vdots \\ \frac{d}{dt}x_{n+2} \end{bmatrix} = \begin{bmatrix} -\frac{R}{L}x_1 + \omega x_2 - \frac{|V|}{L} \\ -\omega x_1 - \frac{R}{L}x_2 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} -\frac{x_3}{L} \\ -\frac{x_3}{L}u_1 \\ -\frac{x_1}{2C_1} - \frac{x_2}{2C_1}u_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} u_2 + \cdots + \begin{bmatrix} -\frac{x_{n+2}}{L} & -\frac{x_{n+2}}{L}u_1 & 0 & \cdots & 0 & -\frac{x_1}{2C_n} - \frac{x_2}{2C_n}u_1 \end{bmatrix}^T u_{n+1} \qquad (۶)$$

$$\mathrm{Y} = \begin{bmatrix} h_1(x) & h_2(x) & \cdots & h_{n+1}(x) \end{bmatrix}^T = \begin{bmatrix} x_2 & x_3 & \cdots & x_{n+2} \end{bmatrix}^T$$

$$\mathrm{X} = \begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_{n+2} \end{bmatrix}^T = \begin{bmatrix} I_d & I_q & V_{dc,1} & \cdots & V_{dc,n} \end{bmatrix}^T$$

از (۶) مشاهده می‌شود که ولتاژهای DC مبدل چندسطحی آبشاری $V_{dc,i} \; i = 1, \ldots, n$ به همراه مولفه‌های جریان محور d و q، تعداد $n+2$ متغیر حالت را تشکیل می‌دهند. با توجه به (۵)، $n+1$ ورودی کنترل وجود دارد بنابراین می‌توان فقط $n+1$ متغیر حالت را کنترل کرد. از آن‌جا که برای تداوم عملکرد صحیح مبدل چندسطحی آبشاری، تنظیم و متعادل‌سازی ولتاژ خازن‌های آن اهمیت زیادی دارد، کنترل ولتاژ n خازن به عنوان یکی از اهداف اصلی کنترل‌کننده در نظر گرفته می‌شود. در نتیجه، تنها یک حالت دیگر را می‌توان کنترل نمود که مولفه جریان محور q برای این منظور انتخاب می‌شود، زیرا توسط این مولفه می‌توان ضریب قدرت / دامنه ولتاژ را کنترل نمود. بنابراین در مدل فضای حالت، ولتاژهای $V_{dc,i} \; i = 1, \ldots, n$ و همچنین I_q به عنوان متغیرهای کنترل‌شده $y_i \; i = 1, \ldots, n+1$ انتخاب می‌شوند.

۲-۳- طراحی کنترل‌کننده با خطی‌سازی بازخورد

در این بخش، یک قانون کنترل غیرخطی براساس خطی‌سازی بازخورد برای جبرانساز DSTATCOM که با (۶) توصیف می‌گردد، توسعه داده می‌شود. در رویکردهای مرسوم خطی‌سازی ورودی-خروجی از طریق بازخورد، مدل غیرخطی سیستم دارای شکل استاندارد (۷) می‌باشد:

$$\frac{d}{dt}\boldsymbol{x} = \boldsymbol{f}(x) + \boldsymbol{g}(x)\boldsymbol{u} \;\; , \boldsymbol{y} = \boldsymbol{h}(x) \qquad (۷)$$

که در آن، $x = [x_1, x_2, \cdots, x_n]^T \in \mathbb{R}^n$ بردار متغیرهای حالت، $u = [u_1, u_2, \cdots, u_k]^T \in \mathbb{R}^k$ بردار ورودی دستکاری شده، $y = [y_1, y_2, \cdots, y_k]^T \in \mathbb{R}^k$ بردار متغیرهای کنترل شده، $f(x) \in \mathbb{R}^n$ بردار توابع غیرخطی، $g(x) \in \mathbb{R}^{n \times k}$ ماتریسی از توابع غیرخطی و $h(x) \in \mathbb{R}^k$ بردار توابع غیرخطی است. از آن‌جا که مدل فضای حالت غیرخطی سیستم در (۶) به صورت non-affine می‌باشد بنابراین برای خطی‌سازی ورودی-خروجی باید شکل عمومی‌تری از سیستم‌های غیرخطی به شکل (۸) مورد توجه قرار گیرد:

$$\frac{d}{dt}\boldsymbol{x} = \boldsymbol{f}(x,u) \;\; , \;\; \boldsymbol{y} = \boldsymbol{h}(x) \qquad (۸)$$

در مدل فضای حالت (۶)، رابطه‌ای خطی بین $h(x)$ و خروجی‌های کنترلی به صورت (۹) وجود دارد:

$$\begin{bmatrix} y_1 & \cdots & y_{n+1} \end{bmatrix}^T = \begin{bmatrix} x_2 & \cdots & x_{n+2} \end{bmatrix}^T \Rightarrow \boldsymbol{y} = \boldsymbol{h}(x) = \begin{bmatrix} 0_{(n+1)\times 1} & I_{(n+1)\times(n+1)} \end{bmatrix} \boldsymbol{x} \qquad (۹)$$

اکنون با جایگذاری (۹) در (۶)، مدل فضای حالت سیستم به شکل ساده‌تر (۷) قابل بازنویسی بوده و در نتیجه با روشی سرراست می‌توان قوانین خطی‌سازی ورودی-خروجی از طریق بازخورد را به دست آورد:

$$\begin{bmatrix} \frac{d}{dt}y_1 \\ \frac{d}{dt}y_2 \\ \vdots \\ \frac{d}{dt}y_{n+1} \\ \frac{d}{dt}x_1 \end{bmatrix} = \begin{bmatrix} -\omega x_1 - \frac{R}{L}y_1 \\ 0 \\ \vdots \\ 0 \\ -\frac{R}{L}x_1 + \omega y_1 - \frac{|V|}{L} \end{bmatrix} + \begin{bmatrix} -\frac{y_2}{L}u_1 \\ -\frac{x_1}{2C_1} - \frac{y_1}{2C_1}u_1 \\ 0 \\ \vdots \\ 0 \\ -\frac{y_2}{L} \end{bmatrix} u_2 + \cdots + \begin{bmatrix} -\frac{y_{n+1}}{L}u_1 & 0 & \cdots & 0 & -\frac{x_1}{2C_n} - \frac{y_1}{2C_n}u_1 & -\frac{y_{n+1}}{L} \end{bmatrix}^T u_{n+1} \qquad (۱۰)$$

با تعریف $v_i \; i = 1, \ldots, n+1$ به عنوان ورودی‌های تبدیل شده، (۱۱) به دست می‌آید:

[Downloaded from jiaeee.com on 2026-11-20]

[DOI: 10.61186/jiaeee.21.4.77]

$$\begin{cases} \dfrac{d}{dt}y_1 = f_2(y,x_1,u) = v_1 \\ \quad\vdots \\ \dfrac{d}{dt}y_{n+1} = f_{n+2}(y,x_1,u) = v_{n+1} \end{cases}, \quad \frac{d}{dt}x_1 = f_1(y,x_1,u) \quad (۱۱)$$

اکنون می‌توان قوانین کنترل $u_i\ i=1,\dots,n+1$ را مستقیماً با حل $n+1$ معادله جبری غیرخطی (۱۱) به دست آورد:

$$u_1 = \frac{2C_1 v_2}{u_2 x_2} - \frac{x_1}{x_2}$$

$$u_2 = \frac{2C_1 v_2}{x_1} - \left(\frac{\frac{x_2}{x_1}\times\left(v_1 + \omega x_1 + \frac{R}{L}x_2\right)}{\frac{x_3}{L} + \frac{x_4}{L}\times\left(\frac{C_2}{C_1}.\frac{v_3}{v_2}\right) + \cdots + \frac{x_{n+1}}{L}\times\left(\frac{C_n}{C_1}.\frac{v_{n+1}}{v_2}\right)} \right)$$

$$u_3 = \frac{C_2}{C_1}.\frac{v_3}{v_2}\,u_2\,,\ \cdots,\ u_{n+1} = \frac{C_n}{C_1}.\frac{v_{n+1}}{v_2}\,u_2 \quad (۱۲)$$

با اعمال قوانین کنترلی (۱۲) در مدل فضای حالت (۶)، سیستم از v_i به y_i برای $i=1,\dots,n+1$ به صورت خطی در می‌آید:

$$\frac{d}{dt}\begin{bmatrix} y_1 & \cdots & y_{n+1}\end{bmatrix}^T = \frac{d}{dt}\begin{bmatrix} x_2 & \cdots & x_{n+2}\end{bmatrix}^T = \begin{bmatrix} v_1 & \cdots & v_{n+1}\end{bmatrix}^T \quad (۱۳)$$

بنابراین می‌توان این سیستم خطی‌شده را با استفاده از بهره مناسب بازخورد، به سادگی کنترل نمود:

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_{n+1}\end{bmatrix} = \begin{bmatrix} \lambda_1 & & \cdots & 0 \\ & \ddots & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & \lambda_{n+1}\end{bmatrix}\begin{bmatrix} I_{q,ref} - y_1 \\ V_{dc,1,ref} - y_2 \\ \vdots \\ V_{dc,n,ref} - y_{n+1}\end{bmatrix} \quad (۱۴)$$

که در آن، مقادیر منفی $\lambda_i \in \mathbb{R}$ برای همه $i=1,\dots,n+1$، بهره کنترل‌کننده خطی حلقه بسته هستند. حال باید نشان داده شود که استفاده از کنترل‌کننده خطی‌ساز ورودی - خروجی (۱۲) و قوانین کنترل خطی (۱۴)، همگرایی مجانبی متغیرهای کنترل‌شده و همچنین ورودی را تضمین می‌کند. استفاده از قوانین کنترل خطی (۱۴) برای مدل خطی (۱۳) به (۱۵) منتهی می‌شود:

$$\frac{d}{dt}\begin{bmatrix} y_1 & \cdots & y_{n+1}\end{bmatrix}^T = \begin{bmatrix} \lambda_1 & & \cdots & 0 \\ & \ddots & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & \lambda_{n+1}\end{bmatrix}\begin{bmatrix} I_{q,ref} - y_1 \\ V_{dc,1,ref} - y_2 \\ \vdots \\ V_{dc,n,ref} - y_{n+1}\end{bmatrix} \quad (۱۵)$$

اگر خطای ردیابی مربوط به هر خروجی $y_i\ i=1,\dots,n+1$ به صورت e_i تعریف شود:

$$\begin{bmatrix} I_{q,ref} - y_1 & V_{dc,1,ref} - y_2 & \cdots & V_{dc,n,ref} - y_{n+1}\end{bmatrix}^T = \begin{bmatrix} e_1 & e_2 & \cdots & e_{n+1}\end{bmatrix}^T \quad (۱۶)$$

چون مقادیر مرجع ثابت هستند، می‌توان (۱۶) را در (۱۵) جایگزین نموده و مدل دینامیکی خطای ردیابی را به صورت (۱۷) بدست آورد:

$$\frac{d}{dt}\begin{bmatrix} e_1 & \cdots & e_{n+1}\end{bmatrix}^T = \begin{bmatrix} \lambda_1 & & \cdots & 0 \\ & \ddots & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & \lambda_{n+1}\end{bmatrix}\begin{bmatrix} e_1 \\ \vdots \\ e_{n+1}\end{bmatrix} \quad (۱۷)$$

با توجه به معیار پایداری سیستم‌های خطی که به صورت $\lim_{t\to\infty} e_i = 0$ می‌باشد، انتخاب مقادیر منفی $\lambda_i \in \mathbb{R}$ برای همه $i=1,\dots,n+1$ پایداری مجانبی خطای ردیابی حلقه بسته (۱۷) را برای هر $i=1,\dots,n+1$ تضمین می‌کند [۳۱]. با توجه به (۱۶)، پایداری مجانبی خطای ردیابی و همچنین کران‌دار بودن ورودی‌های مرجع، کران‌دار بودن و همگرایی مجانبی خروجی‌ها را مشخص می‌کند:

$$\lim_{t\to\infty}\begin{bmatrix} y_1 & \cdots & y_{n+1}\end{bmatrix}^T = \begin{bmatrix} I_{q,ref} & V_{dc,1,ref} & \cdots & V_{dc,n,ref}\end{bmatrix}^T \quad (۱۸)$$

با توجه به (۶) و (۱۸) می‌توان پایداری تمام حالت‌ها به جز x_1 را در کنترل‌کننده طراحی‌شده به ازای همه ورودی‌های مرجع کران‌دار نتیجه گرفت. برای بررسی پایداری حالت x_1، معادله دینامیکی آن با توجه به (۶) به صورت (۱۹) در نظر گرفته می‌شود. نشان داده شد که $x_2,\cdots,x_{n+2}$ کران‌دار بوده و همچنین بقیه پارامترها و متغیرهای داخل پرانتز در (۱۹) نیز کران‌های شناخته شده‌ای دارند. بنابراین، عبارت موجود در پرانتز را می‌توان به عنوان ورودی کران‌دار برای سیستم (۱۹) در نظر گرفت. اکنون به سادگی با توجه به منفی بودن $-R/L$، پایداری مجانبی x_1 اثبات می‌گردد:

$$\frac{d}{dt}x_1 = -\frac{R}{L}x_1 + \left(\omega x_2 + \frac{m_1\cos\delta}{L}x_3 + \cdots + \frac{m_n\cos\delta}{L}x_{n+2} - \frac{|V|}{L}\right) \quad (۱۹)$$

همان‌گونه که اشاره گردید، اندازه جریان محور q یکی از متغیرهایی است که توسط کنترل‌کننده غیرخطی قابل کنترل است. از آن‌جا که تبادل جریان راکتیو با شبکه بر تنظیم ولتاژ و نیز ضریب قدرت سیستم تأثیر می‌گذارد بنابراین در کنترل‌کننده شکل (۲)، دو حالت کنترل ولتاژ و کنترل ضریب قدرت پیش‌بینی شده است.

۲-۴- شناسایی و جبران حمله تزریق داده نادرست

در بخش قبل، یک کنترل‌کننده غیرخطی براساس خطی‌سازی بازخورد برای جبرانساز DSTATCOM چندسطحی آبشاری توسعه داده شد. همان‌گونه که قوانین کنترلی به دست آمده نشان می‌دهند، کنترل‌کننده طراحی‌شده، محاسبات خود را براساس ولتاژ اندازه‌گیری‌شده خازن‌های مبدل چندسطحی انجام می‌دهد. از آن‌جا که اندازه‌گیری ولتاژ خازن‌ها با استفاده از یک شبکه فیزیکی- سایبری در شکل (۱) به کنترل‌کننده مرکزی منتقل می‌شود، حمله‌های تزریق

[Downloaded from jiaeee.com on 2026-11-20]

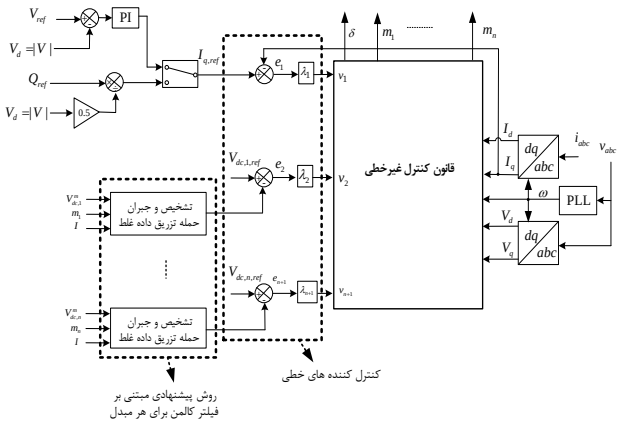
[DOI: 10.61186/jiaeee.21.4.77]

داده نادرست به این شبکه ارتباطی می‌تواند اندازه‌گیری حسگرهای ولتاژ خازن‌ها را هدف قرار دهد. این حمله، تأثیر زیادی بر تعادل ولتاژ خازن‌ها که برای عملکرد مبدل چندسطحی ضروری است دارد. ولتاژ خازن‌های منفرد بسته به علامت ولتاژ حمله، به مقادیری بیشتر/ کمتر از محدوده مجاز افزایش/کاهش یافته و به دنبال عملکرد سیستم حفاظتی، از مدار خارج می‌شوند. به دنبال این موضوع، مبدل‌های سالم نیز که به تنهایی قادر به تحمل ولتاژ شبکه نیستند به صورت آبشاری از مدار خارج شده و در نهایت کل DSTATCOM غیرفعال می‌شود.

خروج DSTATCOM از مدار، عملکرد سیستم توزیع را تحت تأثیر قرار داده و آسیب‌پذیری آن در برابر وقوع اتفاقات بعدی (که ممکن است توسط مهاجمان به صورت سایبری و یا فیزیکی برنامه‌ریزی شده باشد) را افزایش می‌دهد. به همین دلیل ضروری است وجود حملات تزریق داده نادرست تشخیص داده شده و اقدامات جبرانی در مقابل آن انجام گیرد. در این مقاله، فرض می‌شود اندازه‌گیری‌های ولتاژ در خازن‌های مبدل چندسطحی، مستعد حمله تزریق داده نادرست بوده و این حمله با هدف قرار دادن اندازه‌گیری ولتاژ خازن i امین مبدل به صورت (۲۰) مدل‌سازی می‌شود:

$$V_{dc,i}^{Observed}(k)=V_{dc,i}(k)+V_{dc,i}^{attacked}(k) \qquad (۲۰)$$

در این رابطه، $V_{dc,i}^{Observed}(k)$ ولتاژ دریافتی سیستم کنترل در لحظه k، $V_{dc,i}(k)$ ولتاژ واقعی و $V_{dc,i}^{attacked}(k)$ مقداری است که در هنگام حمله تزریق داده نادرست، دارای مقداری مثبت و یا منفی بوده و در شرایط عادی برابر با صفر است. همانگونه که در شکل (۲) نشان داده شده است، قبل از اعمال ولتاژ اندازه‌گیری‌شده خازن‌های مبدل به کنترل‌کننده توسعه داده شده برای DSTATCOM چندسطحی، این ولتاژهای دریافت شده به صورت جداگانه از لحاظ وقوع حمله تزریق داده نادرست مورد ارزیابی قرار گرفته و در صورت تایید وقوع چنین حمله‌ای، مقادیر اندازه‌گیری‌شده اصلاح می‌شوند.



شکل (۲): کنترل‌کننده توسعه داده شده برای DSTATCOM چندسطحی با قابلیت تشخیص و جبران حمله تزریق داده نادرست

در روش پیشنهادی برای تشخیص و جبران حمله تزریق داده نادرست، نیاز به تخمینی از ولتاژ خازن‌ها وجود دارد که به این منظور از ابزار فیلتر کالمن گسسته استفاده می‌شود. این فیلتر یک الگوریتم شناخته شده است که به دلیل سهولت پیاده‌سازی و نیز سرعت همگرایی زیاد، به طور گسترده در بسیاری از زمینه‌ها استفاده می‌شود [۲۰، ۳۲]. باید توجه داشت که در روش استاندارد، همه داده‌ها جمع‌آوری شده و برای انجام تخمین، محاسبات ماتریسی به صورت متمرکز صورت می‌گیرد. در این کاربرد خاص که تعداد زیادی مبدل وجود دارد، انجام این عملیات ماتریسی همراه با پیچیدگی محاسباتی بوده و نیاز به زمان قابل ملاحظه‌ای دارد [۳۳]. بنابراین استفاده از فیلتر کالمن توزیع‌شده در این پژوهش که تخمین ولتاژ خازن هر مبدل را به صورت مستقل از بقیه مبدل‌ها انجام می‌دهد باعث می‌شود فقط به عملیات ریاضی اسکالر نیاز بوده و حجم محاسبات به شدت کاهش پیدا نماید.

معادله حالت توصیف‌کننده ولتاژ خازن مبدل i اُم $V_{dc,i}(k)$ در حوزه زمان گسسته به منظور تخمین ولتاژ خازن، به صورت (۲۱) می‌باشد:

$$V_{dc,i}(k)=V_{dc,i}(k-1)+\frac{T.\,m_i(k-1).I(k-1)}{C_i}+\omega_i(k) \qquad (۲۱)$$

که در آن، T زمان نمونه‌برداری، $m_i(k-۱)$ شاخص مدولاسیون مبدل i اُم در لحظه زمانی k-1، $I(k-۱)$ جریان سمت AC مبدل، C_i ظرفیت خازن DC مبدل و $\omega_i(k)$ نویز گوسی فرآیند با توزیع نرمال، میانگین صفر و کوواریانس $Q_i(k)$ است [۳۴]. الگوریتم فیلتر کالمن شامل دو بخش تخمین حالت و به‌روزرسانی زمان/تخمین می‌باشد. در این الگوریتم، ابتدا با استفاده از (۲۲) و براساس اطلاعات قبلی در لحظه k-1، مقدار تخمین ولتاژ خازن مبدل i اُم $\widehat{V_{dc,i}}(k|k-۱)$ و نیز تخمین کوواریانس $P_i(k|k-۱)$ در لحظه k به دست می‌آید:

$$\hat{V}_{dc,i}(k\,|\,k-1)=\hat{V}_{dc,i}(k-1|\,k-1)+\frac{T.\,m_i(k-1)}{C_i}.I(k-1) \qquad (۲۲)$$
$$P_i(k\,|\,k-1)=P_i(k-1|\,k-1)+Q_i(k)$$

در مرحله بعد، با ترکیب این مقادیر تخمین‌زده شده برای ولتاژ خازن مبدل i اُم و کوواریانس آن در لحظه k و نیز مشاهدات فعلی از ولتاژ خازن در همین لحظه، تخمینی از حالت فعلی سیستم در لحظه k به دست آورده می‌شود. مشاهده فعلی ولتاژ خازن مبدل i اُم با در نظر گرفتن نویز اندازه‌گیری در لحظه k در (۲۳) قابل مشاهده است که در آن، $V_{dc,i}^{m}(k)$ ولتاژ اندازه‌گیری‌شده مبدل i اُم و $v_i(k)$ نویز اندازه‌گیری گوسی با میانگین صفر و کوواریانس $R_i(k)$ می‌باشد:

$$z_i(k)=V_{dc,i}^{m}(k)+v_i(k) \qquad (۲۳)$$

مشکلی که در این میان وجود دارد آن است که در (۲۳)، الگوریتم فیلتر کالمن از ولتاژ اندازه‌گیری‌شده خازن $V_{dc,i}^{Observed}(k)$ در (۲۰) برای به‌روزرسانی تخمین استفاده می‌کند. اگر این ولتاژ توسط تزریق داده نادرست مورد حمله قرار گرفته باشد، علاوه بر آن که به‌روزرسانی تخمین به پاسخی اشتباه منجر می‌شود، وقوع حمله را نیز نمی‌توان

[Downloaded from jiaeee.com on 2026-11-20]
[DOI: 10.61186/jiaeee.21.4.77]

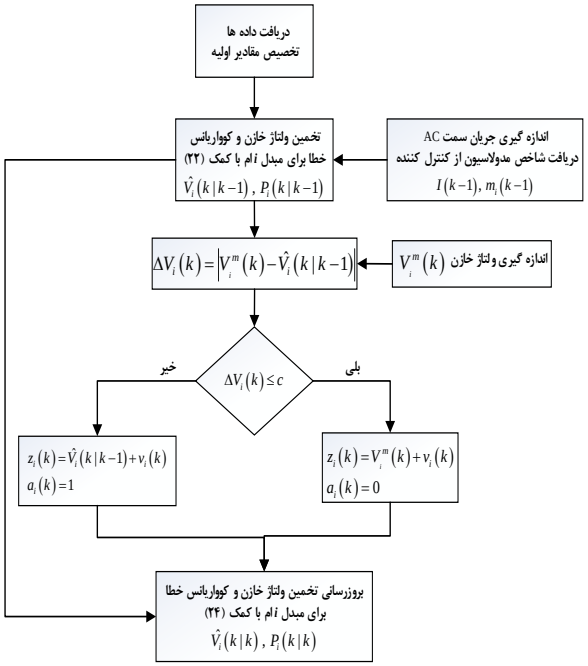
تشخیص داد. بنابراین قبل از به‌روزرسانی تخمین، ابتدا باید درستی ولتاژ اندازه‌گیری‌شده که در (۲۳) مورد استفاده قرار می‌گیرد، بررسی شود. به این منظور، ولتاژ اندازه‌گیری‌شده مبدل i اُم در لحظه k یعنی $V_{dc,i}^{m}(k)$ با ولتاژ تخمین‌زده برای همین لحظه که از داده‌های لحظه k-1 محاسبه شده است یعنی $\widehat{V_{dc,i}}(k|k-1)$ مقایسه می‌شود. اگر مبدل i اُم مورد حمله واقع نشده باشد، تفاوت این دو ولتاژ، مقدار بزرگی نبوده و می‌توان با اطمینان از درستی اندازه‌گیری و صحت (۲۳)، مرحله به‌روزرسانی تخمین در فیلتر کالمن را انجام داد. ولی اگر تفاوت این دو ولتاژ از یک مقدار آستانه از پیش تعریف شده c بیشتر شده باشد به این معنا است که حسگر ولتاژی که $V_{dc,i}^{m}(k)$ را اندازه می‌گیرد، در لحظه k مورد حمله قرار گرفته است. در این صورت، حمله تزریق داده نادرست تشخیص داده شده و برای جبران آن، ولتاژ تخمین‌زده شده $\widehat{V_{\mathrm{dc,i}}}(k|k-1)$ جایگزین ولتاژ مورد حمله قرار گرفته $V_{i,dc}^{m}(k)$ در (۲۳) می‌شود. برای اطلاع کنترل‌کننده مرکزی از وقوع حمله تزریق داده نادرست، یک شاخص حمله $a_i(k)$ با مقدار پیش فرض صفر تعریف می‌شود و در مواقعی که اختلاف ولتاژ تخمینی و اندازه‌گیری‌شده بیشتر از مقدار آستانه c باشد، مقدار این شاخص روی عدد ۱ تنظیم می‌گردد.

اکنون با استفاده از داده‌هایی که از درستی آن‌ها اطمینان حاصل شده است می‌توان به‌روزرسانی تخمین ولتاژ خازن مبدل i اُم یعنی $\widehat{V_{\mathrm{dc,i}}}(k|k)$ و نیز تخمین کوواریانس آن یعنی $P_i(k|k)$ در لحظه k را با استفاده از (۲۴) انجام داد. در رابطه (۲۴)، $K_i(k)$ بهره کالمن نام دارد و نشان داده شده است که این بهره پس از چند تکرار همگرا شده و در نتیجه می‌توان از مقدار حالت ماندگار آن در روابط فیلتر کالمن استفاده نمود. همچنین در ادامه فرض می‌شود که فیلتر کالمن مورد استفاده با انتخاب بهره کالمن مناسب، پایدار است [۳۲].

$$\begin{aligned}
&\hat{V}_{dc,i}(k|k)=\hat{V}_{dc,i}(k|k-1)+K_i(k).\left(z_i(k)-\hat{V}_{dc,i}(k|k-1)\right)\\
&K_i(k)=P_i(k|k-1).\left[P_i(k|k-1)+R_i(k)\right]^{-1}\\
&P_i(k|k)=\left[1-K_i(k)\right].P_i(k|k-1)
\end{aligned} \qquad (۲۴)$$

شکل (۳) روندنمای الگوریتم پیشنهادی برای تشخیص و جبران حمله تزریق داده نادرست را نشان می‌دهد. رابطه (۲۴) نشان می‌دهد که بروزرسانی تخمین ولتاژ خازن در لحظه k ، هم به تخمین قبلی ولتاژ خازن و هم به $z_i(k)$ نیاز دارد. به همین دلیل در روندنمای شکل (۳)، دو مسیر از سمت بلوک تخمین ولتاژ خازن در ابتدای روندنما به سمت بلوک بروزرسانی تخمین ولتاژ خازن وجود دارد.

به دلیل آن‌که عملکرد واحد تشخیص و جبران حمله سایبری، وابسته به مقدار آستانه تشخیص حمله است، لذا انتخاب مقدار مناسب برای آن از اهمیت زیادی برخوردار است. از آن‌جا که داده نادرست می‌تواند با هر دامنه‌ای تزریق شود، بنابراین اختلاف ولتاژ اندازه‌گیری‌شده و تخمینی، می‌تواند هر مقداری داشته باشد. هرچه مهاجم سایبری برای ایجاد اختلال بزرگتر، داده نادرست با دامنه بزرگتری تزریق کند، مقدار اختلاف حاصله بزرگتر شده و انتخاب مقدار آستانه مناسب برای تشخیص وقوع حمله، آسان‌تر می‌شود. حال اگر برای تشخیص حمله‌های سایبری با دامنه‌های اندک، مقادیر آستانه بسیار کوچکی انتخاب شوند، خطاهای اندازه‌گیری حسگرها در کنار خطاهای محاسباتی کنترل‌کننده پیشنهادی می‌تواند منجر به عملکرد اشتباه واحد تشخیص و جبران حمله سایبری شود. لازم به ذکر است به دلیل فاصله زمانی اندکی که بین دو نمونه ولتاژ خازن در لحظات k و k-1 وجود دارد، هیچ نوع حالت گذرایی در خازن نمی‌تواند باعث ایجاد اختلاف قابل توجه بین این دو نمونه ولتاژ و در نتیجه، عملکرد اشتباه واحد تشخیص حمله سایبری گردد. باید توجه نمود که حمله‌های سایبری با دامنه بسیار اندک، عملا تاثیر قابل توجهی بر عملکرد جبرانساز DSTATCOM نداشته و از این رو می‌توان برای جلوگیری از عملکرد اشتباه واحد تشخیص حمله سایبری، مقدار آستانه را خیلی کوچک انتخاب ننمود.



شکل (۳): روندنمای الگوریتم پیشنهادی برای تشخیص و جبران حمله تزریق داده نادرست

سرعت پاسخ الگوریتم پیشنهادی در تشخیص و جبران حمله سایبری، از اهمیت زیادی برخوردار است چراکه هرگونه تاخیری می‌تواند باعث موفقیت مهاجمان سایبری و اختلال در عملکرد جبرانساز شود. در الگوریتم پیشنهادی مقاله حاضر، ولتاژهای اندازه‌گیری شده به عنوان ورودی، با فرکانس بالایی (f_s) نمونه‌برداری می‌شوند. هر نمونه ولتاژ در لحظه k با ولتاژ تخمینی برای همین لحظه -که از داده‌های لحظه k-1 محاسبه شده است- مقایسه می‌شود و اگر تفاوت این دو ولتاژ از یک مقدار آستانه بیشتر بود، ولتاژ تخمینی جایگزین ولتاژ معیوب می‌شود. بنابراین کنترل‌کننده غیرخطی به هیچ وجه ولتاژ معیوب را دریافت ننموده و تحت تاثیر آن قرار نمی‌گیرد. باید توجه نمود که استفاده از شکل گسسته فیلتر کالمن باعث شده

[Downloaded from jiaeee.com on 2026-11-20]
[DOI: 10.61186/jiaeee.21.4.77]

است الگوریتم پیشنهادی بتواند در فاصله زمانی بسیار کوچک بین دو نمونه‌برداری $\left(T_s = \frac{1}{f_s}\right)$، تشخیص و جبران حمله سایبری را به صورت تقریبا آنی انجام دهد.

۳- نتایج شبیه‌سازی

در این بخش، کارایی کنترل‌کننده پیشنهادی با قابلیت تشخیص و جبران حمله تزریق داده نادرست برای DSTATCOM چندسطحی، به کمک شبیه‌سازی یک سیستم نمونه در محیط نرم‌افزار MATLAB/Simulink تحت شرایط مختلف نشان داده می‌شود.

۳-۱- پیاده‌سازی سیستم نمونه

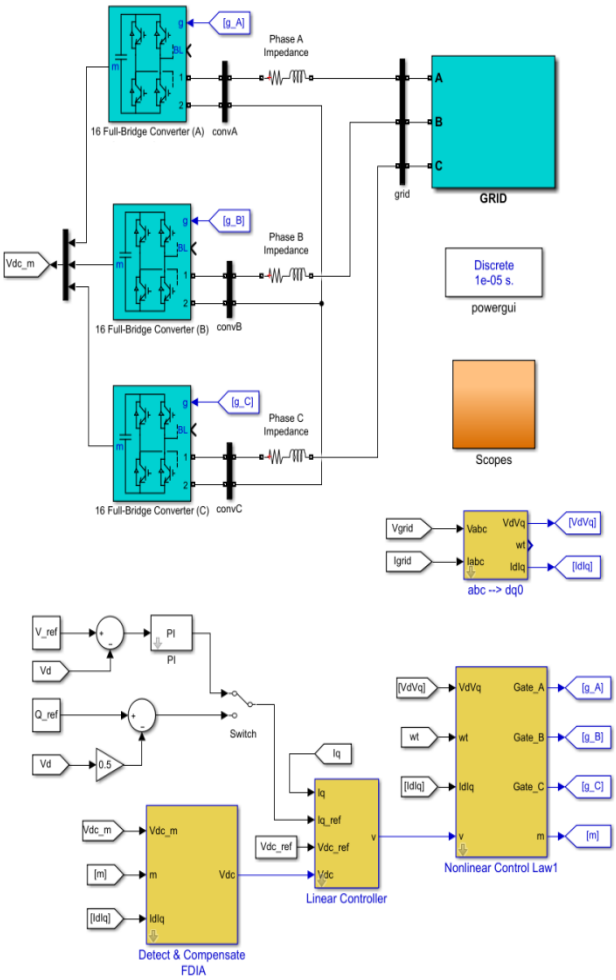
در این قسمت، چگونگی پیاده‌سازی سیستم نمونه در محیط نرم‌افزار که گام اولیه در شبیه‌سازی می‌باشد، شرح داده می‌شود. جبرانساز DSTATCOM چندسطحی مورداستفاده در این سیستم نمونه به صورت مستقیم به شبکه ولتاژ متوسط ۲۰ kV متصل می‌شود. بنابراین با درنظر گرفتن دامنه ولتاژی که بر روی مبدل‌های آبشاری هر فاز آن قرار می‌گیرد و نیز لحاظ کردن یک حاشیه اطمینان مناسب، تعداد ۱۶ مبدل پل در هر فاز DSTATCOM استفاده شده است. مقدار پارامترهای این سیستم نمونه در جدول (۱) آورده شده است.

جدول (۱): مقدار پارامترهای DSTATCOM چندسطحی

شبکه توزیع	مقدار موثر ولتاژ سه فاز	۲۰ kV
	فرکانس	۵۰ Hz
DSTATCOM چندسطحی	تعداد مبدل پل در هر فاز	۱۶
	خازن هر مبدل پل	۵ mF
	مقاومت سری خروجی	۵/۵ mΩ
	سلف سری خروجی	۱/۵ mH
	فرکانس کلیدزنی PWM	۱ kHz
	مقدار مرجع ولتاژ خازن	۱۱۰۰ V
کنترل‌کننده‌های خطی	بهره تناسبی λ_i	-۴۰
واحد تشخیص و جبران حمله تزریق داده نادرست	بهره کالمن	۵
	کوواریانس نویز اندازه‌گیری	۰/۵
	کوواریانس نویز فرآیند	۰/۰۱
	آستانه تشخیص حمله	۱۰٪ ولتاژمرجع‌خازن‌ها
	مقدار اولیه کوواریانس خطا	۰/۵
	فرکانس نمونه‌برداری	۵۰ kHz

تصویر کلی مدل سیستم نمونه که در محیط نرم‌افزار پیاده‌سازی گردیده، در شکل (۴) نشان داده شده است. در نیمه بالایی این شکل، بخش قدرت سیستم نمونه که متشکل از شبکه توزیع و DSTATCOM چندسطحی می‌باشد، دیده می‌شود. از آن جا که جزئیات زیادی در مدلسازی این سیستم وجود دارد، با استفاده از بلوک‌ها سعی شده است تصویر کلی به نمایش داده شود. بلوک شبکه، شامل منبع سه فاز، یک شبکه توزیع ساده و بار سه فاز با ضریب توان غیرواحد می‌باشد. هر یک از مبدل‌های نشان داده شده در هر فاز نیز مطابق جدول (۱)، نماینده ۱۶ مبدل پل هستند که به صورت آبشاری به یکدیگر متصل شده‌اند. بخش کنترلی این سیستم نمونه نیز از چهار بلوک در نیمه پایینی شکل (۴) تشکیل شده است. در اولین بلوک، تبدیل abc به $dq0$ انجام شده و نتیجه آن در بلوک‌های کنترلی دیگر مورداستفاده قرار می‌گیرد.

واحد تشخیص و جبران حمله سایبری با الگوریتم نشان داده شده در شکل (۳)، با دریافت خروجی بلوک قوانین کنترل غیرخطی و نیز اندازه‌گیری‌های انجام شده در مبدل‌های چندسطحی، ولتاژ خازن‌های DC مبدل چندسطحی که از صحت آن‌ها اطمینان حاصل شده است را به بلوک کنترل‌کننده خطی می‌دهد که توسط (۱۴) توصیف می‌شود. این بلوک، ورودی دیگری نیز به عنوان مرجع جریان محور q دارد که چگونگی تولید آن در شکل (۴) مشخص می‌باشد. خروجی بلوک کنترل‌کننده خطی -به عنوان ورودی‌های تبدیل شده- به همراه مولفه‌های محور d و q ولتاژ و جریان به بلوک قوانین کنترل غیرخطی که توسط (۱۲) توصیف شده است داده می‌شوند. به این ترتیب شاخص‌های مدولاسیون موردنیاز تولید شده و به صورت سیگنال کلیدزنی به مبدل چندسطحی داده می‌شود.



شکل (۴): تصویر کلی از مدل سیستم نمونه در نرم‌افزار MATLAB/Simulink

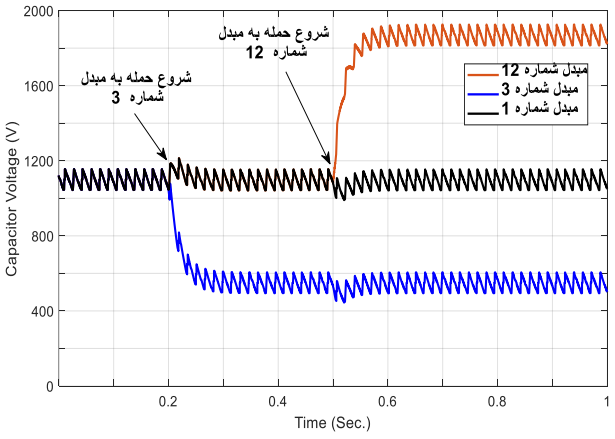
[Downloaded from jiaeee.com on 2026-11-20]

[DOI: 10.61186/jiaeee.21.4.77]

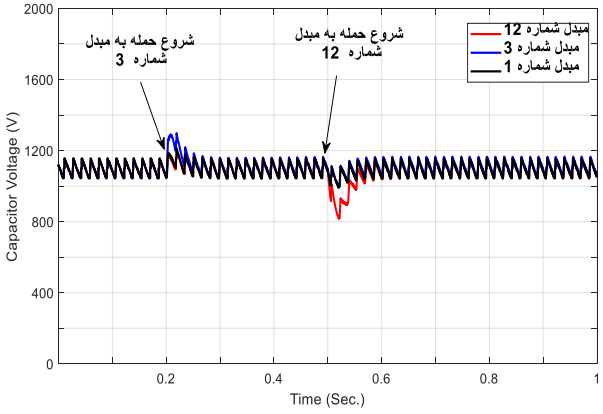
۳-۲- بررسی تأثیر حمله تزریق داده نادرست

در این بخش هدف آن است که اولاً نشان داده شود حمله تزریق داده نادرست چه تأثیری بر عملکرد DSTATCOM چندسطحی داشته و ثانیاً توانایی الگوریتم پیشنهادی برای تشخیص و جبران چنین حمله‌ای ارزیابی شود. برای این منظور ابتدا فرض می‌شود واحد تشخیص و جبران حمله سایبری غیرفعال بوده و در چنین شرایطی، برخی از مبدل‌های موجود در ساختار چندسطحی آبشاری مورد یک حمله تزریق داده نادرست برنامه‌ریزی شده قرار می‌گیرند. فرض می‌شود که در این حمله برنامه‌ریزی شده در لحظه $t = 0.2$ sec.، حسگر ولتاژ مبدل شماره ۳ در فاز a جبرانساز DSTATCOM تحت تزریق داده نادرست ۰/۵+ پریونیت قرار می‌گیرد. در ادامه و در لحظه $t = 0.5$ sec. حسگر ولتاژ مبدل شماره ۱۲ در فاز b جبرانساز مورد حمله تزریق داده نادرست به اندازه ۰/۷- پریونیت واقع می‌شود.

این حمله سایبری باعث می‌گردد کنترل‌کننده مرکزی تصور کند ولتاژ مبدل شماره ۳ در لحظه $t = 0.2$ sec.، به اندازه ۵۰۰ ولت بیشتر از مقدار مرجع شده و ولتاژ مبدل شماره ۱۲ نیز نسبت به مقدار مرجع، ۷۰۰ ولت کاهش یافته است. شکل (۵) (الف) نشان می‌دهد که کنترل‌کننده غیرخطی طراحی شده به سرعت و در کمتر از ۰/۱ ثانیه، ولتاژ مبدل‌های شماره ۳ و ۷ را به ترتیب ۵۰۰ ولت کاهش و ۷۰۰ ولت افزایش داده است. از دید کنترل‌کننده مرکزی و طبق داده‌های دریافت‌شده از حسگرهای ولتاژ، انحراف ولتاژی از مقدار مرجع در این دو مبدل رخ داده و کنترل‌کننده نیز تلاش موفقیت‌آمیزی در جهت رفع این انحراف‌های بزرگ ولتاژ انجام داده است. به عبارت دیگر از منظر کنترل‌کننده مرکزی، تغییرات ولتاژ خازن این دو مبدل به صورت شکل (۵) (ب) به نظر می‌رسد. ولی واقعیت به صورت شکل (۵) (الف) بوده و ولتاژ مبدل‌های مورد حمله واقع‌شده درست به اندازه‌ای که مهاجم سایبری طراحی نموده است، از مقدار مرجع منحرف شده‌اند. پس کنترل‌کننده به صورت معمول قادر به تفاوت‌گذاری بین انحراف ولتاژ واقعی ناشی از تغییر شرایط و یک حمله تزریق داده نادرست به حسگرهای ولتاژ نمی‌باشد.



(الف)



(ب)

شکل (۵): (الف) ولتاژ واقعی خازن مبدل‌های مورد حمله قرار گرفته شماره ۳ و ۱۲ و مبدل سالم شماره ۱ (فقط ولتاژ یکی از مبدل‌های سالم به عنوان نمونه نشان داده شده است)، (ب) ولتاژهای خازن مبدل‌های مورد حمله قرارگرفته از دید کنترل‌کننده مرکزی

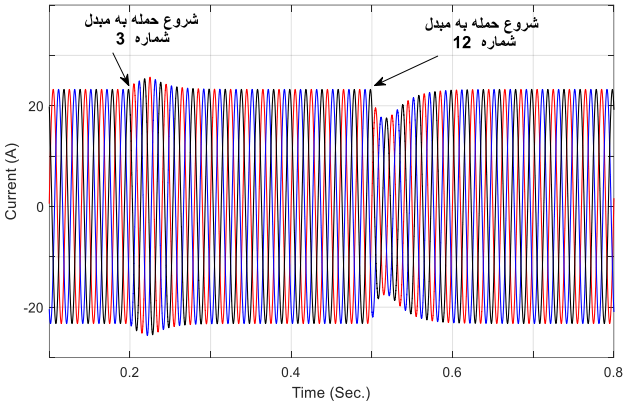
همانگونه که شکل (۵) (الف) نشان می‌دهد، وقوع حمله تزریق داده نادرست باعث می‌گردد ولتاژ خازن در برخی از مبدل‌ها افزایش و برخی دیگر کاهش یابد. بسته به گستردگی و شدت حمله، اگر این ولتاژهای تغییریافته به آستانه اضافه/کاهش ولتاژ برسند، سیستم حفاظت ولتاژ مبدل‌ها را فعال نموده و در نهایت می‌توانند منجر به خروج کامل DSTATCOM چندسطحی از مدار شوند.

باید توجه نمود که کنترل‌کننده غیرخطی پیشنهادی به گونه‌ای طراحی شده است که مبدل‌های دارای شماره یکسان در فازهای مختلف، مشابه با یکدیگر کار می‌کنند. بنابراین حمله به حسگر ولتاژ یکی از مبدل‌ها در یک فاز، عملا باعث تغییر ولتاژ دو مبدل همسان در دو فاز دیگر نیز خواهد شد. در نگاه اول، شاید این موضوع به عنوان یک نقطه ضعف در طراحی کنترل‌کننده به حساب آید ولی باید توجه داشت که توانایی کنترل‌کننده پیشنهادی برای تشخیص و جبران حمله تزریق داده نادرست، مانع از گسترش مشکل به مبدل‌های سالم خواهد شد.

شکل (۶)، تأثیر تغییرات ولتاژ خازن مبدل‌ها در اثر توالی حمله سایبری توصیف شده در شکل (۵) (الف) بر جریان DSTATCOM چندسطحی را نشان می‌دهد. مشاهده می‌شود که حمله تزریق داده نادرست به حسگرهای ولتاژ خازن در مبدل چندسطحی منجر به بروز تغییرات در جریان جبرانساز شده است. باید توجه داشت که نه تنها این رفتار جریانی DSTATCOM به دنبال بروز یک اختلال در شبکه توزیع و برای جبران آن رخ نداده است، بلکه خود می‌تواند باعث بروز مشکلاتی نظیر مشکلات کیفیت توان در شبکه توزیع گردد.

[Downloaded from jiaeee.com on 2026-11-20]

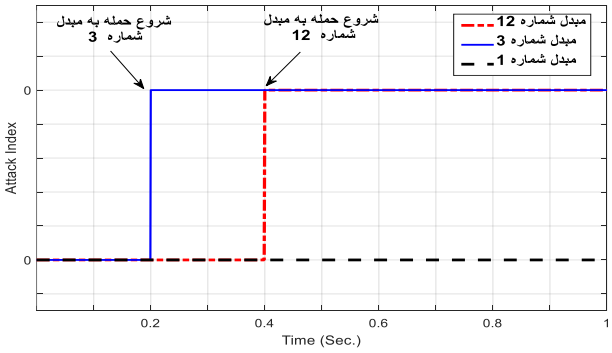
[DOI: 10.61186/jiaeee.21.4.77]



شکل (۶): جریان جبرانساز DSTATCOM چندسطحی به دنبال حمله تزریق داده نادرست توصیف شده در شکل (۵) (الف)

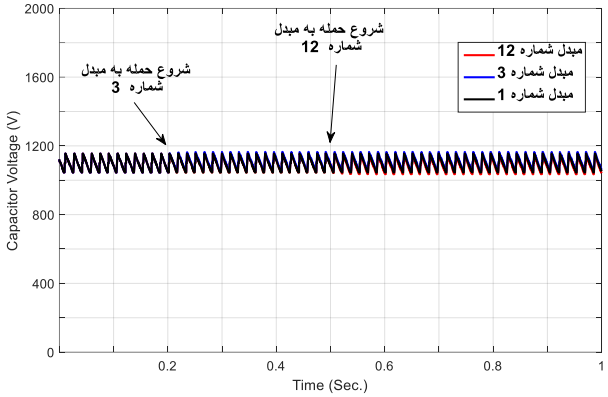
۳-۳- بررسی کارایی کنترل‌کننده پیشنهادی در تشخیص و جبران حمله تزریق داده نادرست

نتایج شبیه‌سازی در قسمت قبل نشان داد که یک توالی حمله تزریق داده نادرست می‌تواند تا چه اندازه بر عملکرد DSTATCOM چندسطحی و نیز شبکه توزیع تأثیر بگذارد و بنابراین لازم است با این حملات مقابله شود. در این قسمت، فرض می‌شود که حسگرهای ولتاژ DSTATCOM چندسطحی با همان توالی توصیف شده در شکل (۵) (الف) مورد حمله تزریق داده نادرست قرار گرفته‌اند ولی واحد تشخیص و جبران حمله سایبری پیشنهادی فعال می‌باشد. شاخص حمله نشان داده شده در شکل (۷) برای مبدل‌های مورد حمله واقع شده و نیز مبدل‌های سالم اثبات می‌کند که الگوریتم فیلتر کالمن پیشنهادی توانسته است وقوع حمله به مبدل‌ها را به درستی تشخیص دهد. اگر در شکل (۷) به زمان وقوع حملات و نیز زمان تغییر شاخص حمله در مبدل‌های شماره ۳ و ۱۲ توجه شود، روشن می‌شود که هیچ‌گونه تاخیر قابل مشاهده‌ای در تشخیص وقوع حمله وجود ندارد. این موضوع نشان می‌دهد کنترل‌کننده پیشنهادی توانسته است به صورت تقریبا آنی (با تاخیری برابر با فاصله زمانی بسیار اندک بین ولتاژهای نمونه‌برداری‌شده (T_s)) عمل نماید.



شکل (۷): شاخص حمله برای مبدل‌های مورد حمله واقع شده و مبدل‌های سالم (فقط برای یکی از مبدل‌های سالم به عنوان نمونه نشان داده شده است)

علاوه بر این، یکسان بودن ولتاژ خازن مبدل‌های موردحمله قرار گرفته و مبدل‌های سالم در شکل (۸) و مقایسه آن‌ها با شکل (۵) (الف) نشان می‌دهد که عملیات جبران حمله تزریق داده نادرست نیز به خوبی انجام شده و هیچ داده نادرستی به کنترل‌کننده غیرخطی DSTATCOM نرسیده است. این موضوع علاوه بر رفع خطر خروج DSTATCOM از مدار، باعث خواهد شد جریان‌های تزریقی جبرانساز برخلاف شکل (۶)، باعث بروز اختلال در شبکه توزیع نشوند.



شکل (۸): ولتاژ واقعی خازن مبدل‌های مورد حمله قرار گرفته و ولتاژ یکی از مبدل‌های سالم (به عنوان نمونه)

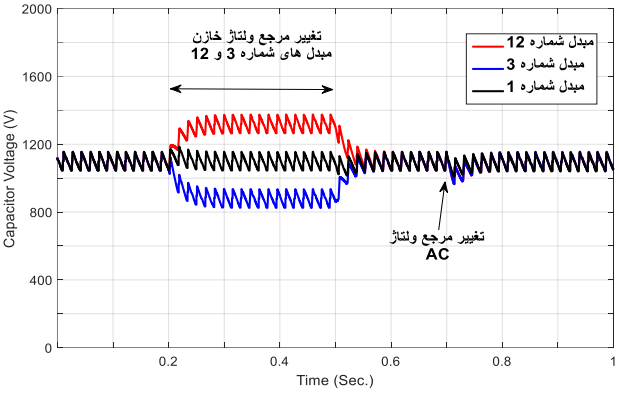
۴-۳- بررسی رفتار کنترل‌کننده در شرایط گذرا

در قسمت قبل، توانایی الگوریتم پیشنهادی برای خنثی نمودن یک توالی حمله تزریق داده نادرست نشان داده شد. از آن‌جا که بروز شرایط گذرا نظیر تغییر در شرایط شبکه و یا تغییر مقادیر مرجع، شباهت زیادی به حملات تزریق داده نادرست دارند، در این قسمت هدف آن است که توانایی کنترل‌کننده پیشنهادی برای تفاوت‌گذاری بین شرایط گذرا و شرایط بروز حمله سایبری به منظور اطمینان از عملکرد قابل اطینان مورد ارزیابی قرار گیرد. به علاوه، از آن‌جا که یکی از نوآوری‌های مقاله حاضر، طراحی کنترل‌کننده غیرخطی برای DSTATCOM چندسطحی است، توانایی آن برای دنبال کردن مقادیر مرجع در شرایط عدم وجود حمله تزریق داده نادرست، هم کارایی و هم قابلیت اطمینان کنترل‌کننده طراحی‌شده را نشان خواهد داد.

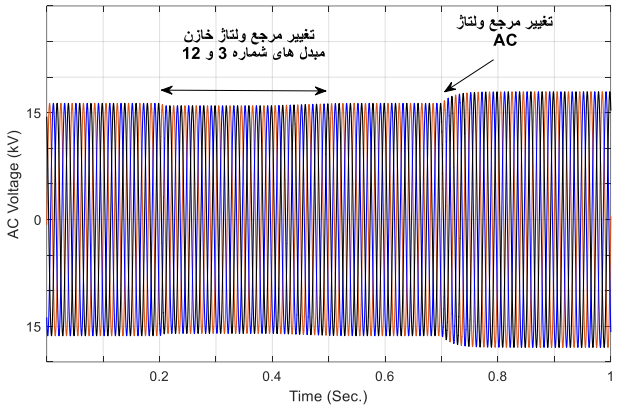
در این قسمت، تغییر در مقدار مرجع ولتاژ خازن‌ها و نیز مقدار مرجع ولتاژ AC به عنوان حالت گذرا مورد مطالعه قرار می‌گیرد. با وجودی که یکی از اهداف کنترل‌کننده DSTATCOM چندسطحی، تثبیت ولتاژ همه خازن‌های مبدل در مقداری ثابت می‌باشد ولی کنترل‌کننده طراحی شده قادر است ولتاژ خازن‌ها را به صورت مستقل از یکدیگر نیز در مقادیر متفاوتی تنظیم نماید. به این منظور در سناریویی غیرواقعی و صرفاً به منظور بررسی قابلیت‌های کنترل‌کننده پیشنهادی فرض می‌شود در شکل (۹) و در حالی که ولتاژ همه خازن‌ها در مقدار ۱۱۰۰ ولت قرار دارد، کنترل‌کننده مرکزی در زمان $t = 0.2$ sec. و برای مدت ۰/۳ ثانیه، مقدار مرجع ولتاژ خازن

[Downloaded from jiaeee.com on 2026-11-20]
[DOI: 10.61186/jiaeee.21.4.77]

مبدل‌های شماره ۱۲ و ۳ را به ترتیب به اندازه ۰/۲- پریونیت و ۰/۲+ پریونیت تغییر دهد. در ادامه و در زمان $t = 0.7$ sec.، مقدار مرجع ولتاژ AC از یک پریونیت به ۱/۱ پریونیت تغییر داده می‌شود.



(الف)



(ب)

شکل (۹): (الف) تغییر مرجع ولتاژ خازن مبدل‌های شماره ۳ و ۱۲ و عدم تغییر ولتاژ خازن مبدل شماره ۱ (نمونه‌ای از مبدل‌هایی که مقدار مرجع آن‌ها تغییر داده نشده است)، (ب) تغییر مرجع ولتاژ AC

شکل (۹) (الف) نشان می‌دهد که ولتاژ خازن مبدل‌های شماره ۳ و ۱۲ در زمانی کمتر از ۰/۱ ثانیه و بدون حالت گذرای قابل ملاحظه‌ای، مقدار مرجع را دنبال کرده‌اند و این تغییر مقدار مرجع، تأثیری بر تنظیم ولتاژ مبدل‌های دیگر نداشته است. دنبال کردن ولتاژ مرجع AC در شکل (۹) (ب) نیز قابل مشاهده است. این نتایج، قابلیت‌های بالای کنترل‌کننده پیشنهادی و عملکرد قابل اطمینان آن را نشان می‌دهند.

۴- نتیجه‌گیری

در این مقاله، تأثیر حملات سایبری از نوع تزریق داده نادرست به جبرانساز DSTATCOM با معماری چندسطحی آبشاری مورد مطالعه قرار گرفت و نتایج شبیه‌سازی در نرم‌افزار MATLAB/Simulink نشان داد این ساختار در برابر حمله تزریق داده نادرست آسیب‌پذیر می‌باشد. یک حمله سایبری موفق می‌تواند باعث خروج جبرانساز DSTATCOM از مدار شده و آسیب‌پذیری شبکه توزیع در پی خروج این جبرانساز که هماهنگ با تجهیزات دیگر موجود در شبکه، وظیفه کنترل ولتاژ شبکه را برعهده دارد، افزایش می‌یابد. در چنین شرایطی، وقوع یک حمله سایبری-فیزیکی برنامه‌ریزی شده دیگر و یا بروز یک شرایط گذرا، می‌تواند منجر به ناپایداری ولتاژ و خاموشی در شبکه شود.

با توجه به اهمیت موضوع، یک کنترل‌کننده غیرخطی براساس خطی‌سازی بازخورد با قابلیت تشخیص و جبران حمله تزریق داده نادرست برمبنای الگوریتم فیلتر کالمن گسسته برای DSTATCOM چندسطحی آبشاری طراحی شد. به دلیل آن‌که محاسبات مربوط به کنترل‌کننده و نیز الگوریتم فیلتر کالمن گسسته پیشنهادی به صورت اسکالر می‌باشد، سیستم کنترل پیشنهادی قابلیت پیاده‌سازی به منظور عملکرد زمان واقعی را دارد. نتایج شبیه‌سازی DSTATCOM نمونه، کارایی سیستم کنترل پیشنهادی در خنثی‌سازی یک رشته تصادفی از حملات تزریق داده نادرست به حسگرهای ولتاژ مبدل چندسطحی را تایید نمود. همچنین نشان داده شد که سیستم پیشنهادی دارای خاصیت تفاوت‌گذاری بین شرایط گذرا نظیر تغییر مقادیر مرجع کنترلی و نیز شرایط وقوع حمله سایبری بوده و از این رو قابلیت اطمینان بالایی در عملکرد آن وجود دارد. بررسی تأثیر حمله تزریق داده نادرست به جبرانساز DSTATCOM چندسطحی در این مقاله، پژوهشی پیشگام در این زمینه بوده و در پژوهش‌های آتی، تشخیص و جبران حملات سایبری پیچیده‌تر مورد توجه قرار خواهد گرفت.

مراجع

[1] H. Sun et al., “Review of Challenges and Research Opportunities for Voltage Control in Smart Grids”, IEEE Transactions on Power Systems, vol. 34, no. 4, pp. 2790-2801, Jul. 2019.

[2] M., Shirkhani et al., “A Review on Microgrid Decentralized Energy/Voltage Control Structures and Methods”, Energy Reports, vol. 10, pp. 368-380, Nov. 2023.

[3] S. E., Razavi et al., “Impact of Distributed Generation on Protection and Voltage Regulation of Distribution Systems: A Review”, Renewable and Sustainable Energy Reviews, vol.105, pp. 157-167, May 2019.

[4] M., Bajaj and A. K. Singh, “Grid integrated renewable DG systems: A Review of Power Quality Challenges and State-of-The-Art Mitigation Techniques”, International Journal of Energy Research, vol. 44, no. 1, pp. 26-69, Jan. 2020.

[5] IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, IEEE Std 1547-2018, 2018, pp. 36–41.

[6] S. Chalise, H. R. Atia, B. Poudel and R. Tonkoski, “Impact of active power curtailment of Wind Turbines Connected to Residential Feeders for Overvoltage Prevention”, IEEE Transactions on Sustainable Energy, vol. 7, no. 2, pp. 471–479, Apr. 2016.

[7] G. Fusco and M. Russo, “A Decentralized Approach for Voltage Control by Multiple Distributed Energy Resources”, IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3115-3127, July 2021.

[Downloaded from jiaeee.com on 2026-11-20]

[DOI: 10.61186/jiaeee.21.4.77]

networks", IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 5, pp. 5294–5310, 2020.

[23] C. Burgos-Mellado et al., "Reinforcement Learning-Based Method to Exploit Vulnerabilities of False Data Injection Attack Detectors in Modular Multilevel Converters", IEEE Transactions on Power Electronics, vol. 38, no. 7, pp. 8907-8921, July 2023.

[24] A. Iqbal et al., "Stability Assessment and Performance Analysis of New Controller for Power Quality Conditioning in Microgrids", International Transactions on Electrical Energy Systems, vol. 31, no. 6, Jun. 2021, Art. no. e12891.

[25] Hosseinpour M, Seifi A. Design and Implementation of a New Switch-Diode based Single Source Multilevel Inverter Topology. Journal of Iranian Association of Electrical and Electronics Engineers 2022; 19 (4) :57-69

[26] S. Yang, Y. Tang and P. Wang, "Distributed Control for A Modular Multilevel Converter", IEEE Transactions on Power Electeronics, vol. 33, no. 7, pp. 5578–5591, 2017.

[27] C. Burgos-Mellado et al., "Cyber-Attacks in Modular Multilevel Converters", IEEE Transactions on Power Electronics, vol. 37, no. 7, pp. 8488-8501, July 2022.

[28] N. Deshmukh, S. Prabhakar and S. Anand, "Power Loss Reduction in Buck Converter Based Active Power Decoupling Circuit", IEEE Transactions on Power Electronics, vol. 36, no. 4, pp. 4316-4325, April 2021.

[29] H. Toodeji, "A Hybrid Switching Technique for Single-Phase AC-Module PV System to Reduce Power Losses and Minimize THD", Iranian Journal of Electrical & Electronic Engineering, vol. 16, no.1, pp. 13-25, 2020.

[30] K. J. P., Veeramraju, J. A., Mueller and J. W. Kimball, "An Extended Generalized Average Modeling Framework for Power Converters", IEEE Transactions on Power Electronics, vol. 38, no. 8, pp. 9581-9592, Aug. 2023.

[31] J. P. Hespanha, Linear Systems Theory. 2nd ed., Princeton University Press, 2018.

[32] H., Liu, F., Hu, J., Su, X., Wei and R. Qin, "Comparisons on Kalman-Filter-Based Dynamic State Estimation Algorithms of Power Systems", IEEE Access, vol. 8, pp. 51035-51043, 2020.

[33] O. S. M. Abushafa, M. S. Dahidah, S. M. Gadoue and D. J. Atkinson, "Submodule Voltage Estimation Scheme in Modular Multilevel Converters with Reduced Voltage Sensors Based on Kalman Filter Approach", IEEE Transactions on Industrial Electronics, vol. 65, no. 9, pp. 7025–7035, 2018.

[34] C. Burgos, D. Saez, M. E. Orchard and R. C´ardenas, "Fuzzy Modelling for The State-of-Charge Estimation of Lead-Acid Batteries", Journal of Power Sources, vol. 274, pp. 355–366, 2015.

[8] G. Fusco, M. Russo and M. De Santis, "Decentralized Voltage Control in Active Distribution Systems: Features and Open Issues", Energies, vol. 14, no. 9, pp. 2563, Apr. 2021.

[9] Z. Li, Q. Guo, H. Sun, J. Wang, Y. Xu and M. Fan, "A Distributed Transmission-Distribution-Coupled Static Voltage Stability Assessment Method Considering Distributed Generation", IEEE Transactions on Power Systems, vol. 33, no. 3, pp. 2621–2632, May 2018.

[10] S. Bolognani, R. Carli, G. Cavraro and S. Zampieri, "On the Need for Communication for Voltage Regulation of Power Distribution Grids", IEEE Transactions on Control of Network Systems, vol. 6, no. 3, pp. 1111-1123, Sept. 2019.

[11] L. Che, X. Liu, Z. Li and Y. Wen, "False Data Injection Attacks Induced Sequential Outages in Power Systems", IEEE Transactions on Power Systems, vol. 34, no. 2, pp. 1513–1523, 2018.

[12] A. J. Abianeh, Y. Wan, F. Ferdowsi, N. Mijatovic and T. Dragiˇcevi´c, "Vulnerability Identification and Remediation of FDI Attacks in Islanded DC Microgrids Using Multiagent Reinforcement Learning", IEEE Transactions on Power Electronics, vol. 37, no. 6, pp. 6359–6370, 2021.

[13] M., Ghiasi, T., Niknam, Z., Wang, M., Mehrandezh, M., Dehghani and N. Ghadimi, "A Comprehensive Review of Cyber-Attacks and Defense Mechanisms for Improving Security in Smart Grid Energy Systems: Past, Present and Future", Electric Power Systems Research, vol. 215, 108975, Feb. 2023.

[14] J. C. Olivares-Rojas, E. Reyes-Archundia, J. A. Gutiérrez-Gnecchi, I. Molina-Moreno, J. Cerda-Jacobo and A. Méndez-Patiño, "Towards Cybersecurity of the Smart Grid Using Digital Twins", IEEE Internet Computing, vol. 26, no. 3, pp. 52-57, May-June 2022.

[15] Y. Li and J. Yan, "Cybersecurity of Smart Inverters in the Smart Grid: A Survey", IEEE Transactions on Power Electronics, vol. 38, no. 2, pp. 2364-2383, Feb. 2023.

[16] V. Cobilean et al., "A Review of Visualization Methods for Cyber-Physical Security: Smart Grid Case Study," IEEE Access, vol. 11, pp. 59788-59803, June 2023.

[17] A. Pinceti, L. Sankar and O. Kosut, "Detection and Localization of Load Redistribution Attacks on Large-Scale Systems", Journal of Modern Power Systems and Clean Energy, vol. 10, no. 2, pp. 361–370, 2021.

[18] G. Liang, S. R. Weller, J. Zhao, F. Luo and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks", IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317–3318, 2016.

[19] Keramati M. A Novel Approach for Amending Vulnerability Scoring in CVSS. Journal of Iranian Association of Electrical and Electronics Engineers 2022; 19 (1) :35-41

[20] A. S. L. V. Tummala and R. K. Inapakurthi, "A Two-stage Kalman Filter for Cyber-attack Detection in Automatic Generation Control System", Journal of Modern Power Systems and Clean Energy, vol. 10, no. 1, pp. 50-59, Jan. 2022.

[21] H. Li, X. He, Y. Zhang and W. Guan, "Attack Detection in cyber-physical Systems Using Particle Filter: An Illustration on Three-Tank System", in 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control and Intelligent Systems (CYBER), 2018, pp. 504–509.

[22] M. R. Habibi, H. R. Baghaee, T. Dragiˇcevi´c and F. Blaabjerg, "Detection of False Data Injection Cyber-Attacks in DC Microgrids Based on Recurrent Neural

[Downloaded from jiaeee.com on 2026-11-20]

[DOI: 10.61186/jiaeee.21.4.77]