Electronic & Cyber Defense
Vol. 14, No. 2, 2026 (Serial No. 54). pp. 41- 60
ISSN: 2322-4347, E-ISSN: 2980-8979

Designing A Robust Algorithm For Cyber Attack of DC Micro Grids Based on Kalman Filter And Its Comparison With Sliding Mode Observer Method

Mohammad-Sadegh Ghafouri[1], Mohammad-Mahdi Rezaei*[2], Sayyed-Mohammad Tabatabaei[3]

[1] Ph.D. Student, Department of Electrical Engineering, Kho.C., Islamic Azad University, Khomeinishahr, Iran. *Mohammadsadegh.ghafoori@iau.ac.ir*
[2] Associate Professor, Department of Electrical Engineering, Kho.C., Islamic Azad University, Khomeinishahr, Iran. (Correspondence: *mm.rezaei@iau.ac.ir)*
[3] Associate Professor, Department of Electrical Engineering, Kho.C., Islamic Azad University, Khomeinishahr, Iran. *tabatabaei@iau.ac.ir*

ARTICLE INFO

Article history:

Article Type: Research paper
Received: 23 May 2026
Revised: 12 July 2026
Accepted: 25 July 2026
Available online: 23 August 2026

Keywords:
DC Microgrids
Cyber-attacks
Unknown input observer
Kalman Filter

ABSTRACT

High reliance of micro grids on communication networks makes them vulnerable to deliberate cyber-attacks. Thus, this paper not only models MGs in state space, but also presents a Kalman filter algorithm to detect and identify of cyber attacks. In other words, a kind of robust detection algorithm is proposed through combining unknown input observer method and Kalman filter for robust attack detection. To highlight the proper impact of the proposed method, a different method (designed with nonlinear observer based on sliding mode one) is simulated,, and the results are compared. The comparison and simulation results confirm the outstanding and robust response of the designed method, as it detects, identifies, and neutralizes the effect of cyber-attacks in the presence of disturbance and noise, and the comparison shows the superiority of the proposed method.

Cite this article: M. Ghafoori, M.M. Rezaei, S.M. Tabatabaei. "Designing A Robust Algorithm for Cyber attack of DC micro grids based on Kalman filter and its comparison with sliding mode observer method," *Electronic and Cyber Defense*, *14*(2), 41-60, 2026, Dor: 20.1001.1.23224347.1405.14.2.6.0

© The Author(s). retain the copyright and full publishing rights

Publisher: Imam Hossein University

Introduction

The increasing integration of distributed energy resources, power electronic converters, and advanced communication infrastructures has significantly contributed to the development of DC microgrids. These systems offer promising advantages for integrating renewable energy sources, energy storage units, and DC loads while facilitating efficient power management and voltage regulation. However, the extensive dependence of distributed control architectures on communication networks introduces critical cybersecurity vulnerabilities. In particular, false data injection attacks (FDIAs) can compromise sensor measurements and communication links, thereby disrupting the coordinated operation and dynamic performance of DC microgrids.

Cyberattacks with cyber-physical power systems can affect both the cyber and physical layers of the system, potentially resulting in inaccurate state estimation, voltage deviations, and compromised control performance. Consequently, the development of reliable and robust attack detection, identification, and mitigation strategies is essential for maintaining the operational security and resilience of DC microgrids. Conventional residual-based detection approaches generally rely on the measured system outputs with model-based estimates. Nevertheless, system disturbances, measurement noise, and model uncertainties can adversely affect residual generation and increase the likelihood of false alarms or missed detections.

State observers and model-based estimation techniques have been extensively investigated for the detection of cyberattacks in power systems. Among these approaches, unknown input observers (UIOs) provide an effective framework for removing unknown disturbances from state estimation errors, provided that the required observability and rank conditions are satisfied. However, the design of disturbance-decoupled observers may involve a trade-off between robustness against unknown inputs and sensitivity to defective attacks. In parallel, Kalman filter-based estimation methods have demonstrated considerable potential for state estimation and attack detection in the presence of stochastic disturbances and measurement noise. Combining the disturbance rejection capabilities of UIOs with the statistical estimation properties of Kalman filters therefore provides a promising approach for enhancing the robustness of cyberattack detection in DC microgrids.

In this study, a robust cyberattack detection and reconstruction algorithm is developed by integrating a linear unknown input observer with a Kalman filter. The proposed approach is designing based on a state-space model of a distributed DC microgrid and is designed to estimate system states while reducing the influence of unknown disturbances on the generated residuals. The reconstructed attack signal is subsequently used to identify compromised measurements and mitigate the impact of false data injection attacks on the system.

The performance of the proposed UIO-KF approach is evaluated through numerical simulations of a distributed DC microgrid comprising four distributed generation units (DGUs). The effectiveness of the proposed method is further assessed under measurement noise and unknown disturbances, and it is compared with a nonlinear sliding-mode observer (SMO)-based approach. The main contributions of this study include the development of a distributed state-space representation, robust reconstruction of false data injection signals, disturbance-resilient state estimation, and evaluation of the proposed method against a sliding-mode observer-based detection strategy.

2. Results and Discussion

2.1. DC Microgrid Modeling and Simulation Configuration

The proposed cyberattack detection and reconstruction algorithm is evaluated using a DC microgrid consisting of four distributed generation units (DGUs) interconnected with electrical loads, as it shown in Figure 1. The microgrid operates under a distributed control architecture incorporating dynamic average consensus for voltage coordination and current sharing. A secondary voltage controller is designed to regulate the average DC bus voltage toward its reference value of 200 V.

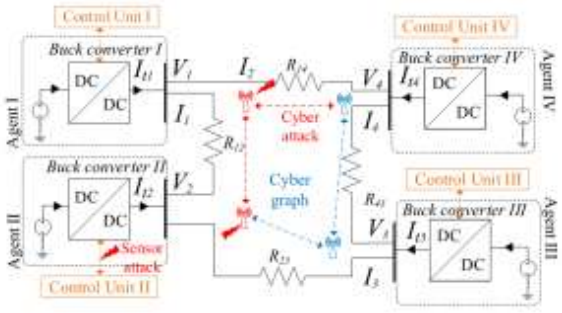


Figure 1. Topology of the four-DGU DC microgrid, illustrating the cyber layer (blue arrows) and physical power flow (black arrows).

The dynamic model of the microgrid is formulated in state-space form based on the averaged model of the boost converters. The continuous-time model is discretized using the fourth-order Runge–Kutta method to facilitate the implementation of the estimation algorithm. The Kalman filter parameters are selected to represent the statistical characteristics of the process and measurement uncertainties. The simulation framework is designed to investigate the capability of the proposed observer to distinguish cyberattack signals from unknown disturbances and measurement noise.

2.2. Robust Residual Generation in the Presence of Unknown Disturbances

The first stage of the simulation study investigates the effect of unknown disturbances on residual generation. When disturbance decoupling is not incorporated into the observer structure, the generated residual can deviate from zero even in the absence of a cyberattack. This behavior may lead to incorrect attack declarations and reduce the reliability of residual-based detection mechanisms.

To address this limitation, the proposed unknown input observer-based Kalman filter is employed to separate the influence of unknown disturbances from the state estimation process. The simulation results demonstrate that the residual generated by the proposed method converges toward zero under attack-free operating conditions. Accordingly, the observer provides a more reliable residual signal for distinguishing malicious data alterations from normal disturbances and measurement noise.

These results highlight the importance of incorporating disturbance decoupling into the state estimation framework. By reducing the effect of unknown inputs on the residual, the proposed approach improves the reliability of the decision mechanism used for cyberattack detection.

2.3. Detection and Reconstruction of False Data Injection Attacks

The proposed detection strategy is examined under two false data injection attack scenarios. In the first scenario, a sudden attack with a magnitude corresponding to a 10% deviation from the nominal measurement is introduced into the first output. The attack is applied after 50 sampling steps, corresponding to 5 s, when the microgrid has reached its steady-state operating condition. In the second scenario, a cyberattack is introduced into the sensor measurements to evaluate the observer's ability to reconstruct compromised signals.

The simulation results indicate that the proposed UIO-KF method successfully detects the injected attacks through the generated residual signals. Despite the presence of measurement noise and unknown disturbances, the observer estimates the system output and the attacked variable with satisfactory accuracy. The residual signals exhibit a detectable deviation following the occurrence of the attack, thereby enabling the identification of compromised measurements.

Furthermore, the reconstructed attack signal can be employed to compensate for corrupted measurements and reduce the adverse impact of the attack on the closed-loop system. The simulation results show that the DC microgrid remains stable during the investigated attack scenarios, and the average voltage converges toward its reference value of 200 V. These observations demonstrate the potential of the proposed method to support attack mitigation through local reconstruction of compromised signals.

The simulation results also indicate that the proposed reconstruction framework can be implemented at individual DGUs. Its distributed structure facilitates scalability, as the estimation accuracy is reported to remain independent of the DC microgrid topology and the presence of cyberattacks in other DGUs under the investigated conditions. Consequently, additional generation units can be integrated into the microgrid with limited modifications to the proposed reconstruction strategy.

2.4. Comparative Evaluation of the UIO-KF and SMO Approaches

The performance of the proposed unknown input observer-based Kalman filter is compared with a nonlinear sliding-mode observer-based method. The comparison is performed using the same DC microgrid topology and attack scenario to provide a consistent evaluation of the two estimation approaches.

Both methods successfully reconstruct the injected cyberattack signal in the presence of measurement noise. However, the simulation results reveal differences in their estimation characteristics. The sliding-mode observer requires appropriate tuning of its design parameters to achieve satisfactory attack signal estimation. Its performance is consequently influenced by the selection of observer gains and filtering parameters. In contrast, the proposed UIO-KF approach estimates the attack signal without requiring the specific tuning procedure associated with the sliding-mode observer in the investigated implementation.

The results further indicate that measurement noise affects the transient estimation response of the sliding-mode observer. A low-pass filter can be employed to reduce the influence of high-frequency noise components; however, increasing the filter time constant introduces a trade-off between noise attenuation and estimation convergence speed. The proposed UIO-KF approach provides an alternative estimation framework that exhibits reduced sensitivity to the investigated measurement noise.

According to the simulation results presented in Figure 2, the attack estimate obtained using the proposed UIO-KF approach converges immediately to the actual attack signal, whereas the SMO-based estimate requires approximately 0.2 s to converge. This difference indicates an improved transient estimation response for the proposed method under the tested operating conditions. Overall, the comparative analysis demonstrates that the UIO-KF approach provides effective attack reconstruction, disturbance-resilient residual generation, and favorable transient estimation characteristics in the investigated DC microgrid. Nevertheless, the reported findings are based on numerical simulations, and further validation under experimental operating conditions and a broader range of attack scenarios is required to establish the generalizability of the results.

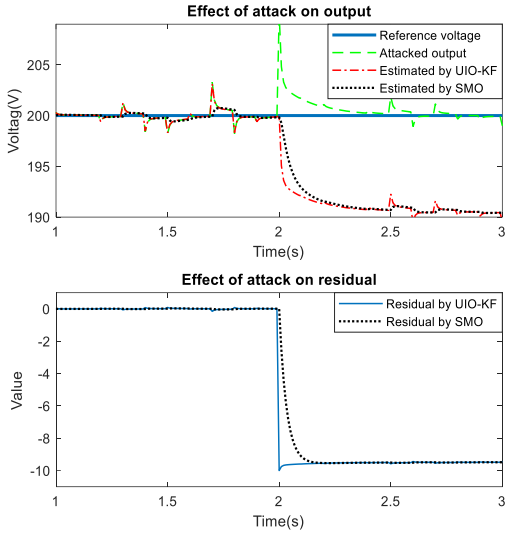


Figure 2. Cyberattack Detection in the Presence of Unknown Inputs Using the UIO-KF and SMO Approaches.

3. Conclusion

This study presented a robust cyberattack detection and reconstruction strategy for distributed DC microgrids based on the integration of a linear unknown input observer and a Kalman filter. A state-space model of the DC microgrid was developed to facilitate state estimation and the generation of disturbance-resilient residual signals. The proposed methodology was designed to reduce the influence of unknown disturbances and measurement noise on the detection process while enabling the reconstruction of false data injection attacks.

The simulation results demonstrated that the proposed UIO-KF approach can successfully detect and reconstruct false data injection attacks under the investigated disturbance and noise conditions. The reconstructed attack signal can be used to compensate for compromised measurements and mitigate the adverse effects of cyberattacks on microgrid operation. In the considered four-DGU DC microgrid, the average voltage converged toward the 200 V reference during the simulated attack scenarios, indicating that the microgrid remained stable under the investigated conditions.

A comparative evaluation with a nonlinear sliding-mode observer-based approach showed that both methods were capable of reconstructing the attack signal in the presence of measurement noise. However, the proposed UIO-KF method exhibited a faster transient estimation response in the investigated simulation, with immediate convergence of the estimated attack signal compared with the approximately 0.2 s convergence time observed for the SMO-based method. The comparison also highlighted the influence of observer parameter tuning and low-pass filtering on the transient performance of the sliding-mode observer.

The distributed structure of the proposed detection framework provides a basis for scalable implementation across multiple distributed generation units. The simulation results suggest that the approach can be adapted to DC microgrids with additional DGUs and different network configurations. However, further investigations are necessary to assess its performance under a wider range of operating conditions, including time-varying disturbances, coordinated cyberattacks, communication delays, and model uncertainties.

Future research may focus on experimental validation using a real-time digital simulation platform or a laboratory-scale DC microgrid. In addition, the integration of adaptive estimation mechanisms, communication-aware detection strategies, and coordinated attack mitigation techniques could further improve the applicability of the proposed framework to complex cyber-physical power systems.

«پدافند الکترونیکی و سایبری»
سال چهاردهم، شماره 2، تابستان 1405، ص 41- 60
شاپا الکترونیکی: 8979- 2980 شاپا چاپی: 4347 -2322

طراحی الگوریتم مقاوم در برابر حمله سایبری ریزشبکه‌های الکتریکی DC مبتنی بر فیلتر کالمن و مقایسه عملکرد آن با نوع مشاهده‌گر مد لغزشی

محمدصادق غفوری [۱]، محمدمهدی رضایی* [۲]، سید محمد طباطبایی [۳]

[۱] دانشجوی دکتری، گروه مهندسی برق، واحد خمینی‌شهر، دانشگاه آزاد اسلامی، خمینی‌شهر، ایران. *Mohammadsadegh.ghafoori@iau.ac.ir*

[۲] دانشیار، گروه مهندسی برق، واحد خمینی‌شهر، دانشگاه آزاد اسلامی، خمینی‌شهر، ایران. (نویسنده مسئول *mm.rezaei@iau.ac.ir*).

[۳] دانشیار، گروه مهندسی برق، واحد خمینی‌شهر، دانشگاه آزاد اسلامی، خمینی‌شهر، ایران. *tabatabaei@iau.ac.ir*

چکیده

وابستگی شدید ریزشبکه‌های الکتریکی به شبکه‌های مخابراتی حاکی از آسیب‌پذیربودن شدید ریزشبکه‌ها در برابر حملات سایبری است؛ لذا در این مقاله، ضمن مدل‌سازی ریزشبکه‌ها در فضای حالت، الگوریتم فیلتر کالمن جهت نظارت به همراه یک الگوریتم تشخیص و شناسایی حمله نوین پیاده می‌گردد. در واقع با استفاده از ترکیب روش مشاهده‌گر ورودی نامعلوم و فیلتر کالمن نوعی آشکارسازی برای مقابله با حملات سایبری طراحی شده است. نتایج شبیه‌سازی حاکی از عملکرد درخشان روش پیشنهادی در زمینه تشخیص، شناسایی و خنثی نمودن اثر حمله سایبری در حضور اغتشاش و نویز است. همچنین به‌منظور ارائه کارایی رویکرد پیشنهادی؛ نتایج حاصل با روش مشاهده‌گر غیرخطی مبتنی بر رویتگر حالت لغزشی نیز مقایسه شده است و مقایسه نتایج نشان‌دهنده برتری روش پیشنهادی است.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۵/۰۳/۰۲

بازنگری: ۱۴۰۵/۰۴/۲۱

پذیرش: ۱۴۰۵/۰۵/۰۳

ارائه آنلاین: ۱۴۰۵/۰۶/۰۱

کلیدواژه‌ها:

ریزشبکه‌های DC

حملات سایبری

مشاهده‌گر ورودی نامعلوم

فیلتر کالمن

استناد: محمد صادق. غفوری، محمد مهدی. رضایی، سید محمد. طباطبایی. طراحی الگوریتم مقاوم در برابر حمله سایبری ریز شبکه های الکتریکی DC مبتنی بر فیلتر کالمن و مقایسه عملکرد آن با نوع مشاهده گر مد لغزشی .*پدافند الکترونیکی و سایبری*، 14(2)، 4(1405).1- 60.

DOR:20.1001.1.23224347.1405.14.2.6.0

© نویسنده(گان) حق نشر و حقوق کامل انتشار را برای خود محفوظ می‌دارند.

ناشر: دانشگاه جامع امام حسین(ع).

1- مقدمه

در سال‌های اخیر به‌خاطر محدودیت سوخت‌های فسیلی و آلودگی هوا، فناوری تولیدات پراکنده برق به‌صورت روزافزون در حال گسترش است. علاوه بر این تولید برق در نزدیکی محل مصرف، ضمن کاهش تلفات، می‌تواند خدمات متنوعی به مصرف‌کنندگان ارائه دهد و بسیاری از چالش‌ها و دغدغه‌های زیست‌محیطی را پوشش دهد. یکی از دیدگاه‌هایی که برای مشارکت مؤثر منابع تولید پراکنده پیشنهاد می‌شود، تجمیع این منابع با اهداف مشاهده‌پذیری، ارتباط مناسب با شبکه‌های برق و کنترل مؤثر آنان در قالب ریزشبکه‌های قدرت است.

ریزشبکه‌ها معمولاً شامل شبکه‌ای از واحدهای متقابل با دستگاه‌های فیزیکی و عناصر محاسباتی است [۱]. وابستگی شدید به شبکه‌های ارتباطی سیستم را در برابر حملات سایبری آسیب‌پذیر می‌کند [۲, ۳] مانند حملات انکاری و حملات فریب [۱, ۴]. این حملات را می‌توان هم در لایه سایبری و هم در لایه فیزیکی به سامانه‌ها تزریق نمود [۵]. علاوه بر این، برخی از مهاجمان مخرب بر حملات بین لایه‌های سایبری و فیزیکی تمرکز می‌کنند که به طور بالقوه‌ای می‌تواند صدمات قابل‌توجهی به دستگاه‌های فیزیکی وارد کند. لازم به ذکر است که مهاجم می‌تواند به طور خودسرانه پویایی سیستم را مختل نماید یا هرگونه اختلال در حفاظت امنیتی کافی از راهبُردهای سخت‌افزاری یا نرم‌افزاری ممکن است منجر به آسیب به سیستم شود و یا حتی جان انسان‌ها را تهدید کند [۶, ۷]. ازاین‌رو نیاز فوری به طرح‌های تشخیص حمله قابل‌اعتماد برای مقابله با حملات مخرب و حفظ عملکرد ریزشبکه‌ها وجود دارد. اگر حملات سایبری را بتوان سریعاً شناسایی نمود، آسیب کلی سامانه‌ها در محدوده قابل‌تحمل کنترل می‌شود.

بیشتر مراجع تحقیقاتی موجود در مورد تشخیص حمله بر اساس ساختار سیستم متمرکز است [۸, ۹]. روش‌های متمرکز تشخیص حمله را می‌توان به دو روش مبتنی بر دانش و مبتنی بر داده تقسیم نمود [۱۰]. تفاوت‌های اصلی این دو روش، مربوط به نحوه‌ی ایجاد مدل سیستم است. در روش‌های مبتنی بر دانش، سیستم را به‌صورت تحلیلی مدل می‌کنند، درحالی‌که روش‌های داده‌محور، یک مدل را مستقیماً از داده‌ها استنباط می‌کنند. در اکثر روش‌های مبتنی بر دانش، یک راهبُرد تشخیص نماینده، رویکرد تولید باقیمانده[1] است [۱۱, ۱۲]. به طور معمول، باقیمانده با مقایسه اندازه‌گیری سنسورها با مدل تحلیلی سیستم طراحی می‌شود. این باقیمانده سپس با یک آستانه ثابت یا متغیر با زمان جهت تصمیم‌گیری در وقوع حمله مقایسه می‌شود. لازم به ذکر است که رویکردهای تولید نسل باقیمانده همیشه با روش‌های مبتنی بر ناظر یا رویکردهای تجزیه‌وتحلیل آماری ترکیب می‌شوند.

در مورد رویکردهای مبتنی بر داده، یادگیری عمیق و الگوریتم‌های ابتکاری [۱۳, ۱۴] اغلب برای ساختن یک مدل استفاده می‌شود. اگرچه روش یادگیری ماشین یک ابزار مفید برای ایجاد یک مدل سیستم است؛ اما ممکن است بار محاسباتی سنگینی را وارد نماید؛ لذا آموزش شبکه متصل‌به‌هم در بسیاری از موارد دشواری‌های خاص خود را دارد [۱۵].

روش برآورد حالت در سیستم برای تخمین حالات سیستم از طریق تجزیه‌وتحلیل اندازه‌گیری‌ها و مدل‌های سیستم استفاده می‌شود [۱۶, ۱۷]. حداقل مربعات وزنی[2] (WLS) یکی از روش‌های پر کاربرد تخمین حالت است [۱۸, ۱۹]. اگرچه چنین روش‌هایی می‌توانند حملات اساسی را تشخیص دهند، اما ممکن است در حضور مهاجمان باهوش‌تری که مایل به عدم شناسایی هستند، شکست بخورند، جایی که داده‌های نادرست را می‌توان با یک شیوه هماهنگ وارد نمود تا با مکانیسم تشخیص سازگار به نظر به رشد، بنابراین الگوریتم تشخیص مذکور دور زده می‌شود.

برای مقابله با این مسئله، روش‌های تخمین مبتنی بر مشاهده‌گر به طور گسترده در مراجع [۲۰-۲۲] به کار گرفته شده است. یک مشاهده‌گر لیون برگر[3] در [۱۱, ۱۴] به ترتیب برای نظارت بر سیستم قدرت و ریزشبکه مورداستفاده قرار گرفته است. در [۲۰] یک طرح حالت مبتنی بر برانگیختگی رویداد[4] بر اساس مشاهده‌گر شبه لیون برگر[5] ارائه شده است. در [۲۱]، یک مشاهده‌گر مد لغزشی تطبیقی[6] (SMO) در تشخیص حمله سایبری به سامانه‌های قدرت طراحی شد.

یکی دیگر از رویکردهای پرکاربرد تخمین، مشاهده‌گرهای ورودی ناشناخته[7] (UIOs) هستند [۲۳-۲۵]. باید توجه داشت که طراحی یک باقیمانده که ورودی ناشناخته کاملاً مجزا[8] (PUID) از اغتشاش باشد مستلزم فرض شرایطی است و تنها زمانی می‌توان به آن دست‌یافت که تعداد کافی سنسور در دسترس باشد که ممکن است تحقق این تکنیک در عمل بسیار قوی باشد. توسعه منطقی طرح باقیمانده PUID، ایجاد مصالحه بین مقاومت در برابر ورودی ناشناخته و حساسیت به حملات است. علاوه بر این، فیلتر کالمن[9] (KF) در تشخیص حملات مختلف از جمله حملات تصادفی کوتاه‌مدت و بلندمدت همراه با حملات فریبی قوی مؤثر

[1] Residual
[2] Weighted Least Square
[3] Luenberger Observer
[4] Event-Triggered
[5] Luenberger-Like
[6] Adaptive Sliding-Mode Observer
[7] Unknown Input Observers
[8] Perfect Unknown Input Decoupled
[9] Kalman Filter

بوده اســـت [۲۶]. ازاین‌رو در این تحقیق، جهت تشـــخیص و شـناسـایی مقاوم حملات سـایبری در ریزشـبکه‌های قدرت توزیع شـــده، سـیگنال حمله با به‌کارگیری الگوریتم مشـاهده‌گر ورودی ناشناخته و فیلتر کالمن بازسازی شده است. از جمله مزایای روش پیشـنهادی می‌توان به موارد زیر اشـاره نمود: ۱) بازسـازی سـیگنال حمله فرایندی محدودتر از شـــناســـایی و جداســـازی یک حمله سـایبری است و دارای مزایای قابل‌توجهی است. جداسـازی عامل در معرض خطر گزینه‌های محدودی را از نظر کاهش پیامدهای حمله بر روی سیسـتم ارائه می‌دهد. به‌طورکلی، تنها گزینه موجود این اسـت که عامل مورد حمله را از سـیسـتم جدا نمود. ۲) مقدار سـیگنال حمله بازسـازی شـده را می‌توان برای پاک‌سـازی‌کردن حسـگر/پیوند سـایبری آسـیب‌دیده اسـتفاده نمود که اثر حمله سـایبری را بر سـیسـتم کاهش می‌دهد و انعطاف‌پذیری ریزشـبکه جریان مسـتقیم[1] (DC) را افزایش می‌دهند. ۳) الگوریتم بازسـازی حملات به‌صـــورت مقاوم اســـت، به‌نحوی که اثر عدم قطعیت یا اغتشـاش تأثیرگذار بر رفتار سـیسـتم را در آشـکارسـازی حملات سـایبری به حداقل رسـاند. ۴) رویکرد پیشـنهادی می‌تواند حملات را تنها با اطلاعات محلی ریزشبکه‌ها بازسازی کند، بنابراین اجرای مقیاس‌پذیر را تسهیل می‌کند.

نوآوری‌های این مقاله به طور خلاصه در زیر نوشته شده است:

- مدل‌سازی ریزشبکه‌های توزیع شده در فضای حالت
- طراحی راهبُرد مبتنی بر UIO ادغام شده با فیلتر کالمن جهت تخمین حالت ایمن در مدل ریزشبکه DC باوجود عدم قطعیت در مدل سیستم
- بازسازی مقاوم سیگنال حملات تزریق داده نادرست[2] (FDIAs) در ریزشبکه‌های توزیع شده
- تخمین مطمئن متغیر مورد حمله قرار گرفته در حضـور نویز و اغتشاش و خنثی نمودن اثر حمله

ســـاختار این مقاله به‌صـــورت زیر اســـت: در بخش دوم ســـاختار ریزشـــبکه‌ها به همراه کنترل‌کننده اولیه و ثانویه معرفی می‌گردد. مدل‌سـازی ریزشـبکه‌های توزیع شـده در فضـای حالت در بخش سـوم ارائه می‌شـود. بخش چهارم به طراحی مشـاهده‌گر ورودی نامعلوم خطی بر اســـاس فیلتر کالمن اختصـــاص خواهد یافت. تحلیل نتایج شبیه‌سازی الگوریتم پیشنهادی و مقایسه آن با روش مشـــاهده‌گر غیرخطی مبتنی بر رویتگر حالت لغزشـــی [۲۲] در بخش پنجم آمده اسـت و در نهایت نتیجه‌گیری در بخش شـشـم ارائه شده است.

2- ساختار ریزشبکه

در شـکل (۱) دیاگرام یک ریزشـبکه نمایش‌داده‌شـده اسـت. طبق این شکل، ریزشبکه بخش کوچکی از شبکه توزیع است که شامل انواع مختلفی از منابع تولید پراکنده و مصـــرف‌کننده‌های برق و انرژی گرمایی اسـت. ریزشـبکه توسـط یک کلید و ترانسـفورماتور همراه آن تحت عنوان PCC[3] توانایی اتصال و جداشدن از شبکه را دارد و مشـــترکین مختلفی ماننـد خانگی، تجاری، صـــنعتی را سرویس می‌دهد.



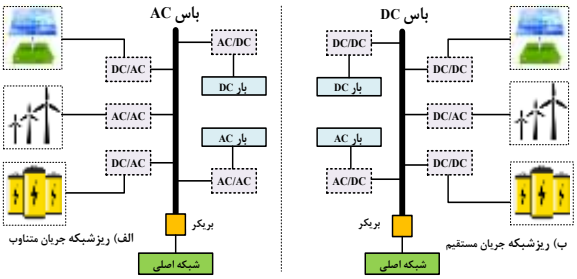
شکل (۱). نمای گرافیکی از ریزشبکه‌ها

در حالت کلی، یک ریزشـبکه به‌صـورت زیر دسـته‌بندی می‌گردد: ۱) ریزشـبکه جریان متناوب[4] (AC) ۲) ریزشـبکه جریان مسـتقیم ۳) ریزشبکه ترکیبی

اگر اجزای یک ریزشبکه از قبیل منابع تولید پراکنده، ذخیره‌سازها و بارها حول یک باس AC تجمع یابند، یک ریزشـــبکه جریان متناوب تشـکیل می‌گردد. لازم به ذکر اسـت که در دهه‌های اخیر، اکثر ریزشـبکه‌ها بر اسـاس سـامانه‌های جریان متناوب بوده که در این زمینه نیز پیشـرفت‌های قابل‌توجهی همانند تشـخیص عملکرد جزیره‌ای ریزشبکه، انتقال توان در سامانه‌های چندمبدلی موازی و غیره، حاصل شده است.

همانند ریزشـبکه‌های جریان متناوب، اگر اجزای یک ریزشـبکه از قبیل منابع تولید پراکنده، ذخیره‌سازها و بارها حول یک باس DC تجمع یابند، یک ریزشبکه جریان مستقیم تشکیل می‌شود. شکل (۲) ریزشـــبکه‌های جریان مســـتقیم و جریان متناوب را نشـــان می‌دهد. درصـــورتی‌که ریزشـــبکه‌های جریان مســـتقیم و جریان متناوب به‌وسیله‌ی واسط‌های الکترونیک قدرت به همدیگر اتصال یابند، یک ریزشبکه ترکیبی یا هیبریدی را تشکیل خواهند داد.

[1] Direct Current
[2] False Data Injection Attacks
[3] Point Of Common Coupling
[4] Alternative Current Microgrid



شکل (۲). ریزشبکه‌های جریان مستقیم و جریان متناوب.

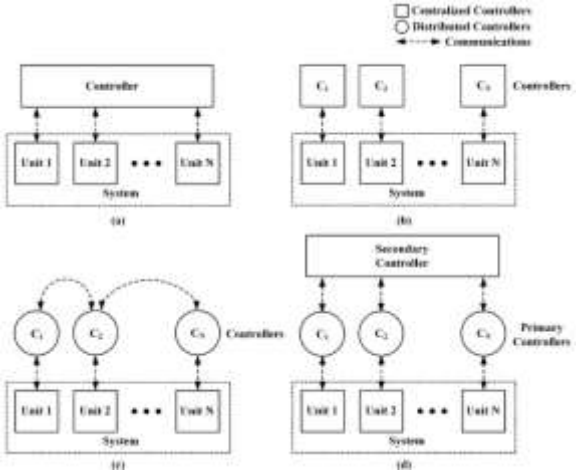
در چند دهه‌ی گذشته اکثر ریزشبکه‌ها بر اساس سامانه‌های جریان متناوب طراحی شده‌اند که در این طراحی‌ها محدودیت‌ها و موانع بسیاری وجود دارد. یکی از این موانع، DC بودن اکثر بارهای موجود است که نیاز به تعداد بیشتری از اینورترها است. از طرفی دیگر به دلیل متغیر بودن ماهیت انرژی‌های تجدیدپذیر، حفظ پایداری و قابلیت اطمینان این نوع از ریزشبکه‌ها با چالش مواجه شده است. اگرچه در دهه‌های اخیر پیشرفت‌های خوبی در بهبود عملکرد ریزشبکه‌های جریان متناوب حاصل گردیده است، اما همچنان چالش‌های زیادی همانند کنترل توان راکتیو و کنترل فرکانس این ریزشبکه وجود دارد. ازاین‌رو مدل موردمطالعه در این تحقیق ریزشبکه جریان مستقیم است.

۱-۲- ساختارهای کنترلی ریزشبکه

همان‌گونه که ذکر گردید، تعادل میان توان تولیدی و مصرفی بسیار اهمیت دارد که متعادل‌سازی باید توسط کنترل‌کننده‌ها صورت گیرد. هدف از کنترل‌کننده‌ها در ریزشبکه جریان مستقیم تعادل ولتاژ و کنترل توان خواهد بود.

قبل از حل مسئله تشخیص حمله برای یک سیستم خاص، چندین جنبه باید موردتوجه قرار گیرد. معماری سیستم و لینک ارتباطی که حمله احتمالی بر روی آن قرار دارد، دو جنبه اصلی این مورد هستند. همان‌طور که در شکل (۳) مشاهده می‌شود، روش‌های کنترل برای اکثر سامانه‌ها می‌تواند متمرکز، غیرمتمرکز، توزیع شده یا به‌صورت سلسه‌مراتبی باشند [۱۷].

الف) کنترل متمرکز: در این ساختار برای تمامی واحدهای تولید پراکنده یک کنترل‌کننده موجود است که این تنظیم‌کننده عموماً از طریق لینک مخابراتی به واحدها متصل است (شکل (۳)). لازم به ذکر است که کنترل متمرکز بهترین اساس برای به‌کارگیری قابلیت‌های کنترل پیشرفته را فراهم می‌کند، چون همه داده‌های مرتبط را می‌تواند جمع‌آوری کرده و در یک کنترل‌کننده واحد پردازش کند. اما اگر در ساختار ذکر شده خطایی در حین انتقال اطلاعات از واحدها به کنترل‌کننده رخ دهد، تمامی سیستم تحت‌تأثیر این خطا قرار خواهند گرفت.



شکل (۳). انواع ساختار کنترل الف) متمرکز، ب) غیرمتمرکز، ج) توزیع شده د) سلسه‌مراتبی [۱۷]

ب) کنترل غیرمتمرکز: در کنترل غیرمتمرکز تعدادی کنترل‌کننده به‌صورت محلی وجود دارد که با واحدها در ارتباط است. در این ساختار، هر واحدی کنترل‌کننده خاص خود را در اختیار دارد و هیچ‌گونه مخابراتی برای انتقال داده‌ها نخواهد بود و صرفاً از متغیرهای محلی برای رساندن ولتاژ به مقدار نامی خود استفاده می‌کنند.

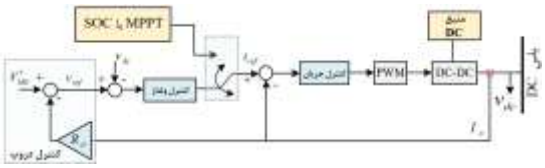
ج) کنترل توزیع شده: این نوع کنترل‌کننده دقیقاً ساختاری مشابه کنترل غیرمتمرکز دارد، با این تفاوت که بین کنترل‌کننده ثانویه واحدهای تولید پراکنده، لینک‌های ارتباطی دیجیتال وجود دارد. الگوریتم‌های کنترلی توزیع‌یافته را می‌توان برای تقسیم اطلاعات میان مولدهای پراکنده در یک ریزشبکه و به‌منظور هماهنگ‌کردن آنها به کاربرد. شکل (۳) ساختار توزیع‌یافته را نشان می‌دهد. به‌طورکلی، با درنظرگرفتن سرمایه‌گذاری اولیه در شبکه‌ی ارتباطی، همچنین انعطاف‌پذیری و قابلیت اطمینان سیستم، روش‌های کنترل توزیعی در مقایسه با روش‌های کنترل متمرکز معمولاً ترجیح داده می‌شوند، اما تحلیل دقیق ریاضی راهبُردهای کنترل توزیع‌یافته به دلیل ارتباط دینامیک‌های الکتریکی و مخابراتی مولدهای پراکنده با هم به‌خصوص در محیط‌های غیرایده‌آل که معمولاً در زندگی واقعی با آن مواجه هستیم، یک موضوع تحقیقاتی چالش‌برانگیز است.

د) کنترل سلسه‌مراتبی: در این ساختار کنترل‌کننده‌های محلی و سطوح کنترلی بالاتر از آن موجود هستند که این سطوح از طریق لینک‌های مخابراتی به هم متصل شده‌اند و به کنترل‌کننده محلی دسترسی خواهند داشت. لازم به ذکر است که ساختار کنترل سلسله‌مراتبی ریزشبکه‌ها از ساختار کنترل سه‌لایه سامانه‌های قدرت در مقیاس بزرگ الهام‌گرفته است. با نظر به اهمیت بالای این نوع از ساختار کنترلی به‌تفصیل به بررسی آن خواهیم

پرداخت. کنترل سلسله‌مراتبی ریزشبکه‌ها از سه سطح زیر تشکیل‌یافته است:

- *کنترل اولیه*[1]

کنترل اولیه معمولاً به‌صورت محلی در هر مولد پراکنده پیاده‌سازی می‌شود. هر واحد تولیدی، یک کنترل‌کننده مربوط به خود را دارد که به‌صورت غیرمتمرکز است. غیرمتمرکز بدین معنی که بین واحدهای تولیدی نیاز به مخابرات ندارد. کنترل اولیه شامل حلقه‌های کنترلی درونی جریان و ولتاژ، کنترل افتی و در برخی موارد حلقه‌ی امپدانس مجازی است. حلقه کنترل ولتاژ (قسمت بیرونی حلقه‌های کنترل درونی) مسئول تولید سیگنال جریان مرجع برای حلقه کنترل جریان (حلقه درونی‌تر)، است. حلقه کنترل جریان نیز که سریع‌تر از حلقه‌ی کنترل ولتاژ است، باید جریان خروجی را برای ردیابی مرجع تولید کند. در گام اول کنترل اولیه باید قادر به حفظ پایداری فرکانس و ولتاژ باشد و با نگه‌داشتن مقادیر آن‌ها در رنج‌های از پیش تعیین شده، از ناپایداری آن‌ها جلوگیری کند. برای دستیابی به این هدف، باید مراجع ولتاژی و فرکانسی از طریق مشخصه‌ی افتی[2] یا دروپ تعیین شوند. ساختار یک کنترل‌کننده اولیه در ریزشبکه‌های جریان مستقیم در شکل (۴) نشان‌داده‌شده است.



شکل (۴). ساختار کنترل اولیه ریزشبکه‌های جریان مستقیم

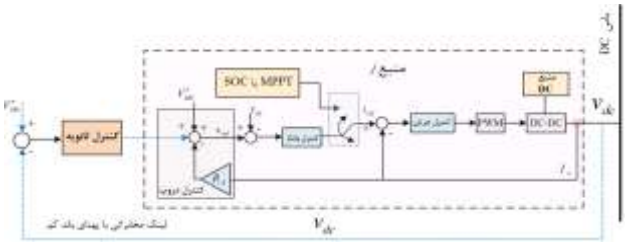
- *کنترل ثانویه*[3]

کنترل اولیه، همان‌طور که در مورد آن بحث شد، ممکن است با تغییرات بار، باعث انحرافات ولتاژی، در حالت ماندگار شود. اگر چه دستگاه‌های ذخیره‌ساز می‌توانند این انحرافات را جبران کنند، اما (به دلیل ظرفیت محدود انرژی) قادر به فراهم نمودن توان برای کنترل ولتاژ در شرایط طولانی نیستند؛ بنابراین هرچند که در حضور کنترل اولیه ولتاژ ریزشبکه‌ها ناپایدار نخواهند شد، اما می‌توانند از مقادیر واقعی خود منحرف شوند. ازاین‌رو یک سطح کنترلی دیگر برای بازگردانی مقادیر نامی ولتاژ آنها لازم است؛ لذا کنترل ثانویه برای خنثی‌کردن انحرافات ایجاد شده توسط کنترل اولیه به کار گرفته می‌شود؛ لذا به‌طورکلی وظایف کنترل ثانویه در ریزشبکه‌ها به‌صورت زیر است [۲۰]: الف) حذف انحرافات ولتاژی ناشی از کنترل اولیه ب) بهبود تسهیم توان ج) افزایش کیفیت توان.

همان‌گونه که بیان شد، حذف انحرافات ایجاد شده در ولتاژ ریزشبکه توسط اضافه‌کردن یک ترم جبران‌ساز از جانب کنترل ثانویه صورت می‌گیرد. این روال برای ریزشبکه‌های جریان مستقیم که در آن‌ها انحراف ولتاژی توسط V-I دروپ‌ها تولید می‌شود، نیز برقرار است. در ریزشبکه‌ی جریان مستقیم، نحوه‌ی ایجاد ترم جبران‌ساز به این صورت است که ابتدا ولتاژ باس مشترک DC اندازه‌گیری شده و پس از مقایسه با مرجع ولتاژی از پیش تعیین شده در ریزشبکه، اختلاف آنها به‌عنوان ورودی به یک کنترل‌کننده داده می‌شود، سپس برای جبران انحراف ولتاژی ایجاد شده به کنترل افتی خروجی این کنترل‌کننده به‌عنوان مرجع داده می‌شود (شکل (۵)). مشخصه‌ی کنترل ثانویه ریزشبکه جریان مستقیم در رابطه‌ی زیر بیان شده است که دراین‌رابطه، δV_{DC} ترم جبران‌ساز انحراف ایجاد شده توسط V-I دروپ در کنترل اولیه است.

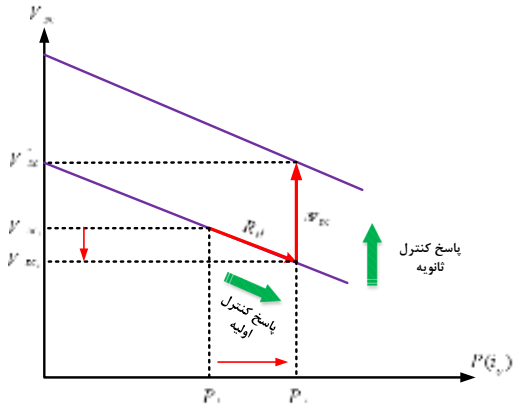
$$V_{DC} = V_{DC}^{*} - R_d \cdot i_o + \delta V_{DC} \qquad (۱)$$

نحوه عملکرد رابطه‌ی فوق در شکل (۵) نشان‌داده‌شده است.



شکل (۵). نحوه پیاده‌سازی کنترل ثانویه ریزشبکه‌های جریان مستقیم

شایان‌ذکر است که به طور معمول در مقالات، کنترل ثانویه متشکل از یک کنترل‌کننده تناسبی - انتگرالی[4] (PI) است.



شکل (۶). نحوه عملکرد کنترل ثانویه ریزشبکه‌های جریان مستقیم

[1] Primary Control
[2] Droop Characteristic
[3] Secondary Control
[4] Proportional-Integral

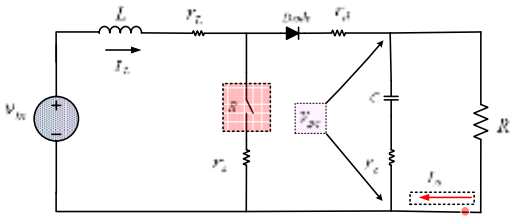
در کنترل ثانویه سه معماری مهم تحت عنوان‌های معماری متمرکز، غیرمتمرکز و توزیع‌یافته وجود دارند که کنترل‌کننده می‌تواند بر حسب سلیقه یا نیاز، مطابق آن معماری پیاده‌سازی شود.

3-مدل‌سازی و طراحی واحدهای تولیدی ریزشبکه موردمطالعه

مبدل افزاینده به‌عنوان یکی از مهم‌ترین مبدل‌های DC، یک ابزار کارآمد برای تقویت یک سطح ولتاژ DC به سطح ولتاژ موردنظر، به‌حساب می‌آید. توان مبدل افزاینده می‌تواند از هر منبع مناسب مانند ژنراتورهای DC، باتری، پنل‌های خورشیدی و یکسوکننده‌ها تأمین شود.

این مبدل‌ها را می‌توان به‌عنوان سامانه‌های غیرخطی و متغیر با زمان توصیف کرد، پس مدل سیگنال کوچک از مدل فضای حالت میانگین برای طراحی یک کنترل‌کننده خطی موردنیاز است. ازاین‌رو در ادامه، نحوه‌ی به‌دست‌آوردن مدل فضای حالت میانگین به‌تفصیل بیان می‌گردد.

شکل (۷) مدار قدرت یک مبدل افزاینده را نشان می‌دهد. گام اساسی در طراحی کنترل‌کننده ولتاژ این مبدل‌ها، در اختیار داشتن مدل کاملی از این مبدل‌ها (شامل تمامی عامل‌های سیستم نظیر مقاومت، دیود و کلید (ترانزیستور ماسفت)، سلف و خازن، همراه با مقاومت داخلی آن‌ها) است.



شکل (۷). ساختار مداری مبدل افزاینده.

در واقع، اجزای اصلی مبدل افزاینده همان کلید اکتیو و دیود است. خازن C در خروجی مدار موردنظر و سلف L در ورودی، نقش فیلتر را دارند. معمولاً فیلترهای ورودی برای حذف نویز یا تداخل الکترومغناطیسی و فیلترهای خروجی برای حفظ عملکرد دینامیکی و مقاومت در برابر تغییرات بار و نوسانات ولتاژ هستند. r_l، r_c، r_d و r_s به ترتیب مقاومت‌های داخلی سلف، خازن، دیود و کلید را نشان می‌دهند. در ادامه، به نحوه‌ی مدل‌سازی این مبدل جهت دستیابی به مدل میانگین فضای حالت برای طراحی کنترل‌کننده‌های اولیه جریان و ولتاژ پرداخته می‌شود.

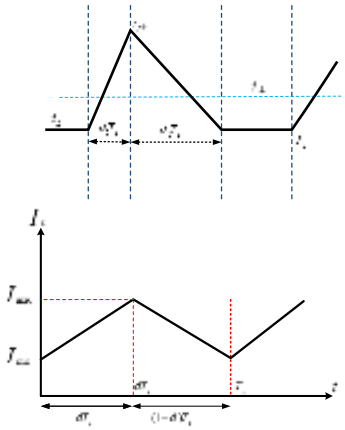
۱-۳- مدل میانگین فضای حالت مبدل افزاینده

در این بخش بر اساس روش میانگین فضای حالت، ابتدا معادلات فضای حالت افزاینده در حالت‌های کلید مختلف را به دست می‌آوریم. عامل چرخه وظیفه[1] (d) که مدت‌زمان بسته‌بودن کلید به کل زمان را نشان می‌دهد، به‌عنوان ورودی کنترلی مبدل افزاینده در نظر گرفته می‌شود.

مبدل‌های افزاینده در دو حالت کاری هدایت پیوسته[2] (CCM) و هدایت گسسته[3] (DCM) می‌توانند عمل کنند. در حالت کاری CCM جریان سلف یا ولتاژ خازن همواره برقرار است ($i_L(t) > 0$. $v_C(t) > 0$). اما در حالت DCM علاوه بر دو حالت فوق، حالت سومی نیز وجود دارد که ممکن است جریان سلف یا ولتاژ خازن صفر شود. شکل (۸) به ترتیب نشان‌دهنده حالت‌های کاری CCM و DCM هستند.

(الف)

(ب)



شکل (۸). حالت کاری مبدل افزاینده: الف) CCM، ب) DCM

در شکل (۸)، هنگامی که کلید بسته و دیود خاموش است، جریان سلف به مقدار i_{pk} یعنی حداکثر مقدار خود می‌رسد و این مقدار در انتهای حالتی که کلید باز بوده و دیود روشن است به مقدار صفر می‌رسد. لازم به ذکر است که ریپل‌های کلیدزنی در جریان سلف یا ولتاژ خازن، باعث معکوس‌سازی پلاریته ولتاژ یا جریان کلید و بنابراین یک حالت جریان صفر می‌شود؛ بنابراین، مقدار میانگین جریان سلف $\bar{i}_L$ از رابطه (۲) محاسبه می‌گردد:

$$\bar{i}_L = \frac{i_{pk}}{2}(d_1 + d_2) \qquad (۲)$$

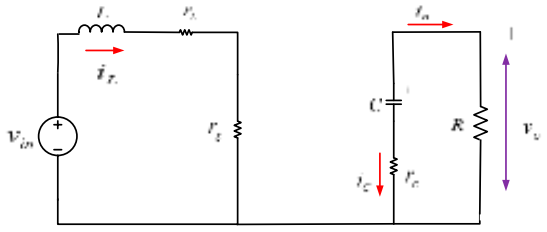
بر اساس مقادیر عامل‌های مبدل افزاینده یعنی L، R و C ولتاژ ورودی، ولتاژ خروجی مطلوب و فرکانس کلیدزنی، می‌توان

[1] Duty Cycle
[2] Continuous Conduction Mode
[3] Discontinuous Conduction Mode

تشخیص داد که مبدل افزاینده در چه حالتی از CCM یا DCM کار می‌کند. در مدل‌سازی فضای حالت، متغیرهای حالت عمدتاً المان‌های ذخیره‌کننده انرژی سیستم، انتخاب می‌شوند (جریان سلف و ولتاژ خازن). در یک مدار الکتریکی اولین گام برای مدل‌سازی، تبدیل مدار پیچیده به مدار پایه‌ای به‌گونه‌ای است که قوانین مداری بتوانند پیاده‌سازی شوند.

برای مدل‌سازی مبدل افزاینده در حالت CCM، دو حالت را پیش‌رو داریم. باتوجه‌به شکل (۸) هیچ‌گاه دیود و کلید با هم روشن یا با هم خاموش نمی‌شوند. زمان روشن بودن کلید با dT و زمان خاموش بودن آن توسط $d'T = (1-d)T$ که T دوره ولتاژ خروجی در حالت ماندگار است، مشخص می‌شود. لازم به ذکر است که چون ترانزیستور ماسفت دارای سرعت بالایی برای کلیدزنی است، از آن می‌توان به‌عنوان کلید در مبدل افزاینده استفاده کرد و همچنین اغلب دیود شاتکی، مورداستفاده در این مدارها خواهد بود.

شکل (۹) مربوط به حالت اول مبدل افزاینده است که کلید کنترل‌شونده در زمان $t = 0$ روشن بوده و دیود خاموش است. در این صورت جریان سلف بالا می‌رود و از طریق سلف و ترانزیستور ماسفت جریان می‌یابد.



شکل (۹). حالت اول کاری CCM

حال با نوشتن معادلات قانون ولتاژ کیرشهف[1] (KVL) برای مدار فوق داریم:

$$\frac{di_L}{dt} = \frac{v_{in}}{L} - \frac{(r_s+r_l)}{L} i_L \quad (۳)$$

$$C\frac{dv_C}{dt} = -\frac{1}{(r_c+R)C} v_C \quad (۴)$$

$$-v_C - r_c i_C + v_o = 0 \quad (۵)$$

که با جای‌گذاری رابطه‌ی (۴) در رابطه (۵) می‌توان نوشت:

$$v_o = \frac{R}{r_c+R} v_C \quad (۶)$$

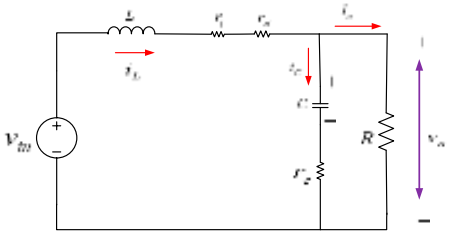
بنابراین، با در دست‌داشتن معادلات فضای حالت برای این مد کاری، می‌توان ماتریس فضای حالت مربوطه آن را با درنظرگرفتن $x = [i_L \ v_c]^T$ به‌عنوان متغیرهای حالت، $u = v_{in}$ به‌عنوان ورودی و v_o به‌عنوان خروجی مدار فوق، فضای حالت اول را می‌توان به‌صورت زیر نوشت:

$$y = v_o = \begin{bmatrix} 0 & \frac{R}{r_c+R} \end{bmatrix} \begin{bmatrix} i_L \\ v_C \end{bmatrix} \quad (۷)$$

$$\dot{x} = A_1 x + B_1 u: \quad (۸)$$

$$\begin{bmatrix} \frac{di_L}{dt} \\ \frac{dv_C}{dt} \end{bmatrix} = \begin{bmatrix} -\frac{(r_s+r_l)}{L} & 0 \\ 0 & -\frac{1}{(r_c+R)C} \end{bmatrix} \begin{bmatrix} i_L \\ v_c \end{bmatrix} + \begin{bmatrix} \frac{1}{L} \\ 0 \end{bmatrix} v_{in}$$

حالت دوم مربوط به زمانی است که کلید کنترل‌شونده در زمان $t = t_1$ باز و دیود روشن می‌شود. در این صورت جریان ورودی از طریق سلف، خازن، دیود یکسوکننده و مقاومت بار، جریان می‌یابد؛ بنابراین، جریان سلف تا دوره بعدی افت خواهد کرد و انرژی ذخیره شده در سلف از مسیر مقاومت بار، جریان می‌یابد. شکل (۱۰) این حالت را نشان می‌دهد.



شکل (۱۰). حالت کاری دوم CCM

از مدار فوق مشخص است که $i_L = i_C + i_o$، ازاین‌رو می‌توان نوشت:

$$i_C = i_L - \frac{v_C + r_c i_C}{R} \quad (۹)$$

که نهایتاً رابطه‌ی جریان خازن در این حالت، به‌صورت زیر نوشته خواهد شد.

$$i_C = \frac{R}{R+r_c} i_L - \frac{1}{R+r_c} v_C \quad (۱۰)$$

که می‌توان نوشت:

$$\frac{dv_C}{dt} = \frac{R}{(R+r_c)C} i_L - \frac{1}{(R+r_c)C} v_C \quad (۱۱)$$

حال با نوشتن KVL داریم:

$$v_{in} = (r_d + r_l) i_L + v_o + v_L \quad (۱۲)$$

با جای‌گذاری $v_o = R(i_L - i_C)$ در رابطه قبل و با داشتن رابطه‌ی مربوط به قانون جریان کیرشهف[2] (KCL) می‌توان نوشت:

[1] Kirchhoff's Voltage Law

[2] Kirchhoff's Current Law

$$\frac{di_L}{dt} = \frac{1}{L}v_{in} - \frac{(r_d+r_l)(R+r_c)+Rr_c}{(R+r_c)L} i_L - \frac{R}{(R+r_c)L} v_C \quad (۱۳)$$

و رابطه‌ی خروجی نیز به فرم (۱۴) می‌تواند نوشته شود:

$$v_o = \frac{Rr_c}{R+r_c} i_L + \frac{R}{R+r_c} v_C \quad (۱۴)$$

اکنون می‌توان ماتریس فضای حالت $\dot{x} = A_2 x + B_2\, u$ را به‌صورت زیر بیان کرد.

$$\begin{bmatrix} \frac{di_L}{dt} \\ \frac{dv_C}{dt} \end{bmatrix} = \begin{bmatrix} -\frac{(r_d+r_l)(R+r_c)+Rr_c}{(R+r_c)L} & -\frac{R}{(R+r_c)L} \\ \frac{R}{(R+r_c)C} & -\frac{1}{(R+r_c)C} \end{bmatrix} \begin{bmatrix} i_L \\ v_c \end{bmatrix} + \begin{bmatrix} \frac{1}{L} \\ 0 \end{bmatrix} v_{in} \quad (۱۵)$$

$$y = v_o = \begin{bmatrix} \frac{Rr_c}{R+r_c} & \frac{R}{R+r_c} \end{bmatrix} \begin{bmatrix} i_L \\ v_C \end{bmatrix}$$

در این حالت مدل میانگین فضای حالت به‌صورت زیر خواهد بود:

$$\dot{x} = A_p x + B_p\, u \quad (۱۶)$$

$$y = C_p x + D_p$$

$$A_p = A_1 d_1 + A_2 d_2 \quad (۱۷)$$

$$B_p = B_1 d_1 + B_2 d_2$$

$$C_p = C_1 d_1 + C_2 d_2$$

$$D_p = D_1 d_1 + D_2 d_2$$

لازم به ذکر است که $d_1 = d$ دوره کاری مربوط به بسته‌بودن کلید کنترل‌شونده و دوره کاری $d_2 = 1 - d$ مربوط به زمان باز بودن آن است؛ لذا ماتریس فضای حالت میانگین مبدل افزاینده به فرم زیر خواهد بود.

$$A_p = \begin{bmatrix} -\frac{(r_s+r_l)}{L} & 0 \\ 0 & -\frac{1}{(r_c+R)C} \end{bmatrix} d + \begin{bmatrix} -\frac{(r_d+r_l)(R+r_c)+Rr_c}{(R+r_c)L} & -\frac{R}{(R+r_c)L} \\ \frac{R}{(R+r_c)C} & -\frac{1}{(R+r_c)C} \end{bmatrix} (1-d) \quad (۱۸)$$

$$B_p = \begin{bmatrix} \frac{1}{L} \\ 0 \end{bmatrix} d + \begin{bmatrix} \frac{1}{L} \\ 0 \end{bmatrix} (1-d)\,,$$

$$C_p = \begin{bmatrix} 0 & \frac{R}{r_c+R} \end{bmatrix} d + \begin{bmatrix} \frac{Rr_c}{R+r_c} & \frac{R}{R+r_c} \end{bmatrix} (1-d)$$

با مرتب‌سازی ماتریس‌های فوق داریم:

$$A_p = \begin{bmatrix} Ap11 & Ap12 \\ Ap21 & Ap22 \end{bmatrix} \quad (۱۹)$$

$$B_p = \begin{bmatrix} \frac{1}{L} \\ 0 \end{bmatrix}$$

$$C_p = \begin{bmatrix} \frac{Rr_c}{R+r_c}(1-d) & \frac{R}{R+r_c} \end{bmatrix}$$

که

$$Ap11 = -\left(\frac{Rr_c}{(R+r_c)L} - \frac{r_s - r_d}{L}\right)(1-d) - \frac{(r_s+r_l)}{L}$$

$$Ap12 = -\frac{R}{(R+r_c)L}(1-d)$$

$$Ap21 = \frac{R}{(R+r_c)C}(1-d)$$

$$Ap22 = -\frac{1}{(R+r_c)C}$$

با فرض $x_1 = i_L$ و $x_2 = v_c$ معادلات فضای حالت میانگین را بر اساس ماتریس‌های فوق به‌صورت زیر می‌توان نوشت:

$$\dot{x}_1 = -\left[\left(\frac{Rr_c}{(R+r_c)L} - \frac{r_s - r_d}{L}\right)(1-d) + \frac{(r_s+r_l)}{L}\right] x_1 - \frac{R}{(R+r_c)L}(1-d)x_2 + \frac{1}{L}u \quad (۲۰)$$

$$\dot{x}_2 = \frac{R}{(R+r_c)C}(1-d)x_1 - \frac{1}{(R+r_c)C} x_2$$

$$y = \frac{Rr_c}{R+r_c}(1-d)x_1 + \frac{R}{R+r_c} x_2$$

۲-۳- ساده‌سازی حلقه‌های داخلی

در قسمت قبل توضیحات کاملی در راستای دلیل انتخاب مبدل‌های افزاینده و چگونگی محاسبه مدل فضای حالت آن‌ها جهت طراحی کنترل ارائه شد که می‌توان بر اساس آن‌ها، یک ریزشبکه جریان مستقیم متشکل از چند عامل تولیدی همراه مبدل افزاینده را تشکیل داد. همان‌گونه که در قبل نیز بیان شد، عوامل در سامانه‌های چندعامله، نیاز به تبادل اطلاعات با واحدهای مجاور را دارند که این تبادل معمولاً به‌وسیله زیرساخت مخابراتی است. باید توجه داشت که تبادل اطلاعات میان واحدها باعث تغییر ماهیت سیستم کنترلی یک‌واحدی به کنترل یک سیستم چندعامله می‌شود که نیاز عوامل به هم‌زمانی خواهد بود، یعنی باید در یک‌زمان مشخص هر عامل بایستی به‌صورت هماهنگ اطلاعات را با واحدهای مجاور خود به اشتراک بگذارند. به‌منظور مدل‌سازی مناسب سیستم موردمطالعه جهت طراحی یک تخمین‌گر حالت برای آشکارسازی حملات سایبری، نیاز است در ادامه همه مدل‌سازی‌های قبلی را با هم تلفیق کرده و پس از آن به طراحی تخمین‌گر در سطح ثانویه برای تشخیص حملات سایبری بپردازیم. برای این منظور لازم است تا دیاگرام زیر را دوباره مدنظر قرار دهیم که ساختار یک ریزشبکه که در حالت بهره‌برداری توسط کنترل سلسله‌مراتبی است را نشان می‌دهد. همان‌طور که در شکل (۱۱) نشان‌داده‌شده است در بلوک اول و دوم توافق میانگین دینامیکی ولتاژ انجام شده و خروجی آن به لایه کنترل ثانویه می‌رود. سپس کنترل ثانویه سیگنال کنترلی مناسب جهت کنترل و بازیابی ولتاژ واحدها را تولید و به سطح

اولیه کنترل (لایه دروپ کنترل) می‌رساند. باید توجه داشت که حمله سایبری ممکن است که در همین قسمت رخ دهد. در ادامه به نحوه ادغام و مدل‌سازی کل واحد تولید پراکنده می‌پردازیم.

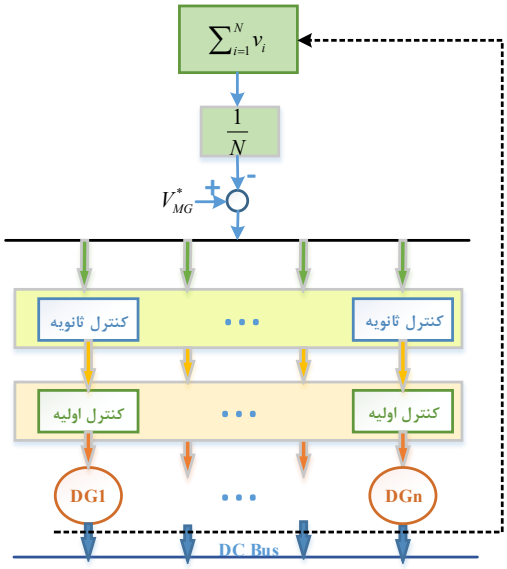
در الگوریتم توافق، ولتاژ واحدها پس از اندازه‌گیری از طریق وسایل مخابراتی، همان‌طور که در شکل به‌صورت خط‌چین مشکی نمایش‌داده‌شده است، ارسال، و در آنجا توافقی بر اساس میانگین‌گیری به‌صورت زیر شکل می‌گیرد:

$$\frac{1}{N}\sum_{i=1}^{N} v_i \qquad (۲۱)$$

که در آن N تعداد واحدها و v_i نیز ولتاژ مخابره شده خروجی واحدها است. البته این توافق را می‌توان به‌صورت زیر نیز نوشت:

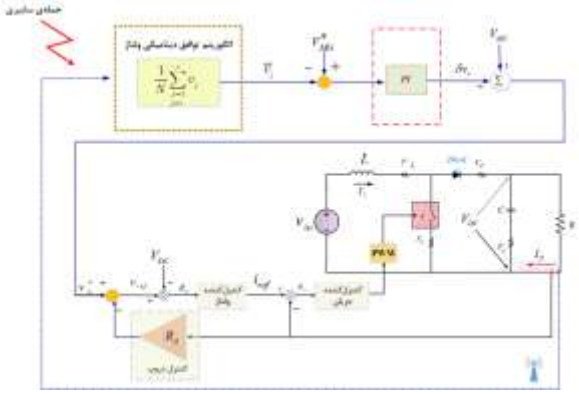
$$v_i - \frac{1}{N}\sum_{j=1,j\neq i}^{N} v_i \qquad (۲۲)$$

که در این صورت به‌جای اینکه میانگین ولتاژ خروجی واحدها به‌عنوان ورودی کنترلی وارد کنترلر شود، اختلاف و خطای واحدی که از نظر تنظیم ولتاژ اهمیت بیشتری دارد، از میانگین ولتاژ واحدهای دیگر وارد کنترل ثانویه می‌شود.



شکل (۱۱). ساختار متمرکز معماری ریزشبکه از دید کنترل ثانویه با الگوریتم توافق میانگین دینامیکی در حضور مبدل افزاینده و کنترل اولیه

نمایی از الگوریتم توافق میانگین دینامیکی ولتاژ در سطح کنترل ثانویه و در حضور کنترل اولیه و مبدل افزاینده در شکل (۱۱) نشان‌داده‌شده است. در این شکل، از الگوریتم توافق دینامیکی ولتاژ جهت دست‌یابی به میانگین ولتاژ و حل مسئله بازیابی و کنترل ولتاژ واحدها استفاده شده است.



شکل (۱۲). ساختار متمرکز معماری ریزشبکه دارای تابع کنترل ثانویه با الگوریتم توافق میانگین دینامیکی در حضور حمله سایبری

همان‌طور که پیش‌تر نیز بیان شد می‌توان به‌جای مبدل افزاینده مدل فضای حالت آن را استفاده کرد. در این صورت مدل کنترلی به فرم شکل (۱۲) ساده می‌شود. در این صورت با تبدیل مدل فضای حالت میانگین مبدل، می‌توان به‌جای مبدل افزاینده، تابع تبدیل مدل آن را به کاربرد.

4- طراحی مشاهده‌گر ورودی نامعلوم خطی بر اساس فیلتر کالمن

در این بخش جهت بازسازی سیگنال حمله و تولید مانده‌ی مقاوم در سامانه‌های خطی از روش ترکیب مشاهده‌گر ورودی نامعلوم و فیلتر کالمن خطی استفاده می‌کنیم و یک مشاهده‌گر ورودی نامعلوم خطی را ارائه می‌دهیم.

۴-۱- مشاهده‌گر ورودی نامعلوم خطی

در این بخش مشاهده‌گری که تخمین حالت را در حضور عدم قطعیتی که به‌صورت یک اغتشاش نامعلوم[1] جمع‌شونده بیان می‌شود، معرفی می‌شود. دینامیک سیستم به‌صورت زیر در نظر گرفته می‌شود. سیستم گسسته زمان زیر مفروض است.

$$x_{k+1} = A_k x_k + B_k u_k + L_{1,k} f_{k+1} + E_k d_k + \zeta_k \qquad (۲۳)$$

$$y_k = C_k x_k + L_{2,k} f_k + \eta_k \qquad (۲۴)$$

که $x_k \in \mathbb{R}^n$ بردار حالت، $y_k \in \mathbb{R}^m$ بردار خروجی، $u_k \in \mathbb{R}^r$ بردار ورودی معلوم و $d_k \in \mathbb{R}^q$ بردار اغتشاش (ورودی نامعلوم) است و $f_k \in \mathbb{R}^p$ حمله سنسورها را نمایش می‌دهد، $L_{1,k} \in \mathbb{R}^{n\times s}$، $L_{2,k} \in \mathbb{R}^{m\times s}$ ماتریس‌های توزیع حمله هستند. هر چند که d_k یک ورودی نامعلوم است؛ اما ضریب آن E_k معلوم و دارای رتبه کامل است. ζ_k و η_k نویزهای با میانگین صفر و مستقل از هم

[1] Unknown Disturbance

با کوواریانس‌های Q_k و R_k هستند. A_k، B_k، C_kوE_k ماتریس‌های معلوم با ابعاد مناسب هستند.

جمله $E_k d_k$ می‌تواند مدل‌های مختلفی از عدم قطعیت مانند ترم‌های بین اجزا مختلف سامانه‌های با ابعاد بالا[1]، ترم‌های غیرخطی در دینامیک سیستم [۲۷] و همچنین خطی‌سازی و کاهش خطا در مدل و تغییرات عامل‌ها، را بیان کند. جزئیات مدل‌سازی و مثال‌هایی از آن را می‌توان در فصل پنجم مرجع [۲۸] یافت.

برای تخمین حالت‌های سیستم مفروض (۲۳) و (۲۴) با ورودی نامعلوم، یک مشاهده‌گر بهینه جداساز حمله با ساختار زیر پیشنهاد می‌شود:

$$z_{k+1} = (I - H_{k+1}C_{k+1})(A_k\hat{x}_k + B_k u_k) + K_{k+1}(y_k - \hat{y}_k) \quad (۲۵)$$

$$\hat{x}_{k+1} = z_{k+1} + H_{k+1}y_{k+1}$$

که $\hat{x}_k \in \mathbb{R}^n$ تخمین حالت‌های سیستم است و $z_{k+1} \in \mathbb{R}^n$ حالت‌های مشاهده‌گر است. $\hat{y}_k \in \mathbb{R}^m$ تخمین خروجی است. ماتریس‌های $H_{k+1} \in \mathbb{R}^{n\times m}$و$K_{k+1} \in \mathbb{R}^{n\times m}$ چنان باید طراحی شوند که ورودی نامعلوم از خطای تخمین جدا شود.

به‌منظور طراحی مشاهده‌گر ذکر شده دینامیک خطای تخمین در حالتی که حمله‌ها صفر در نظر گرفته می‌شوند را محاسبه می‌کنیم.

$$e_{k+1} = x_{k+1} - \hat{x}_{k+1} = (I - H_{k+1}C_{k+1})A_k(x_k - \hat{x}_k) + (I - H_{k+1}C_{k+1})E_k d_k - K_{k+1}(y_k - \hat{y}_k) \quad (۲۶)$$

اگر خطای تخمین حالت e_{k+1} به‌صورت مجانبی در حضور ورودی نامعلوم به سمت صفر میل کند آنگاه حالت تخمین زده شده به سمت حالت واقعی همگرا خواهد شد $\hat{x}_{k+1} \to x_{k+1}$ [۳۱- ۳۴] .

در این صورت ورودی مشاهده‌گر نامعلوم تعریف شده به وسیله‌ی معادله (۲۵) به‌عنوان ورودی مشاهده‌گر نامعلوم می‌تواند در نظر گرفته شود. ضریب ترم اول خطا و ضریب ورودی نامعلوم را برابر صفر قرار می‌دهیم. برای حل این معادلات و همگرایی مجانبی خطای تخمین حالت شرایط زیر باید برقرار باشد:

$$\text{I. } \operatorname{rank}(C_{k+1}E_k) = \operatorname{rank}(E_k) \quad (27)$$

$$\text{II. } E_k = H_{k+1}C_{k+1}E_k \quad (۲۸)$$

III. K_{k+1} به‌گونه‌ای طراحی شود که مشاهده‌گر پایدار شود.

جزئیات بیشتر و توضیح کامل در مورد شرایط اول و دوم در مرجع [۲۹] آمده است. اگر شرط اول برقرار باشد آنگاه یک حل برای معادله (۲۸) به‌صورت زیر است [۲۹]:

$$H_{k+1} = E_{k+1}(C_{k+1}E_{k+1})^+ + H_0[C_{k+1}E_{k+1}(C_{k+1}E_{k+1})^+] \quad (۲۹)$$

H_0 یک ماتریس دلخواه است. برای سادگی در اکثر موارد می‌توان H_0 را صفر در نظر گرفت؛ بنابراین H_{k+1} می‌تواند به‌صورت زیر نوشته شود:

$$H_{k+1} = E_{k+1}H^1_{k+1} \quad (۳۰)$$

$$H^1_{k+1} = (C_{k+1}E_{k+1})^+ = [(C_{k+1}E_{k+1})^T C_{k+1}E_{k+1}]^{-1}(C_{k+1}E_{k+1})^T \quad (۳۱)$$

سیستم را در حالت بدون حمله، $f_k = 0$ در نظر بگیرید. با ضرب‌کردن (۲۴) در H^1_{k+1} و جای‌گذاری آن در معادله (۲۳) می‌توان نشان داد:

$$d_k = H^1_{k+1}[y_{k+1} - C_{k+1}(A_k x_k + B_k u_k)] \quad (۳۲)$$

جای‌گذاری رابطه (۳۲) در (۲۳) می‌دهد:

$$\hat{x}_{k+1|k} = \bar{A}_k\hat{x}_k + \bar{B}_k u_k + \bar{E}_k y_{k+1} \quad (۳۳)$$

که $\bar{A}_k = \bar{F}_k A_k$، $\bar{B}_k = \bar{F}_k B_k$ و $\bar{F}_k = I - E_k H^1_{k+1}C_{k+1}$ و $\bar{E}_k = E_k H^1_{k+1}$ است.

بنابراین، مشاهده‌گر ورودی نامعلوم خطی به‌صورت زیر می‌تواند نوشته شود:

$$\hat{x}_{k+1} = \hat{x}_{k+1|k} + K_{k+1}(y_k - \hat{y}_k) \quad (۳۴)$$

$$\hat{x}_{k+1|k} = \bar{A}_k\hat{x}_k + \bar{B}_k u_k + \bar{E}_k y_{k+1} \quad (۳۵)$$

$$\hat{y}_k = C_k\hat{x}_k \quad (۳۶)$$

مشاهده‌گر به‌دست‌آمده در (۳۴) و (۳۵) با مشاهده‌گر معرفی شده در (۲۵) برابر است و می‌توانیم از آن برای معادلات مشاهده‌گر ورودی نامعلوم استفاده کنیم. تا اینجا طراحی کلی مشاهده‌گر مورد بررسی واقع شد در قسمت‌های بعد به نحوه‌ی تولید مانده و تحلیل آن می‌پردازیم.

۲-۴- تولید و تحلیل مانده

راه‌حل معمول برای اهداف تشخیص حمله تولید یک سیگنال شاخص است که آن را مانده می‌نامند. این سیگنال در حالت بدون حمله باید مقدار صفر (میانگین صفر) را داشته باشد و در هنگام رخداد حمله مقدار آن مخالف صفر (میانگین صفر) باشد. در کاربردهای عملی نیاز است که این سیگنال مانده نسبت به اغتشاش، نویز و عدم قطعیت‌ها مقاوم باشد. اگر مشاهده‌گر ورودی نامعلوم خطی طراحی شده پایدار باشد، آنگاه خطای تخمین $e_{k+1} = x_{k+1} - \hat{x}_{k+1}$ به‌صورت مجانبی به صفر همگرا می‌شود؛ بنابراین در حالت ماندگار و بدون حمله سیگنال مانده برابر است با:

[1] Large Scale System

$$\boldsymbol{r_k} = y_k - \hat{y}_k = 0 \quad (۳۷)$$

درکل، علامت رخداد حمله می‌تواند اختلاف داشتن با صفر در حالت ماندگار تعریف شود یعنی $r_k \neq 0$ باشد.

با اعمال یک تابع تصمیم‌گیری به مانده می‌توان مشخص کرد که چه هنگامی حمله رخداده است. برای جلوگیری از تصمیمات اشتباه همانند نادیده‌گرفتن یک حمله یا اشتباه اعلام‌کردن یک حمله باید یک تابع تصمیم‌گیری مناسب انتخاب شود [۳۰]. هنگام رخداد یک حمله هر چه میزان دامنه مانده از صفر مقدار بیشتری باشد تحلیل مانده برای شناسایی حمله مطمئن‌تر خواهد بود. در روش پیشنهادی (که در بخش بعدی توضیح داده می‌شود) این مهم اعمال شده است. راه‌حل‌های بسیاری برای انتخاب تابع تصمیم‌گیری وجود دارد. یک روش ساده و پرکاربرد انتخاب تابع تصمیم‌گیری باینری S_r با یک حد آستانه ثابت T_k است.

$$J(\boldsymbol{r_k}) \leq T_k \quad for \ f_k = 0 \quad (۳۸)$$
$$\Rightarrow S_r = 0 \ attck \ free \ case$$
$$J(\boldsymbol{r_k}) > T_k \quad for \ f_k \neq 0 \ \Rightarrow S_r = 1 \ attacked \ case$$

البته روش‌های مناسب‌تری برای انتخاب حد آستانه T_k وجود دارد. در اینجا T_k به‌صورت تطبیقی و باتوجه‌به خصوصیات آماری سیستم در حالت سالم انتخاب شده است. با استفاده از میانگین و واریانس سیگنال مانده در حالت سالم یک حد آستانه به‌صورت زیر تعریف می‌شود:

$$\bar{r} = \mathbb{E}[\boldsymbol{r_k}] = \frac{1}{m}\sum_{k=1}^{m} r_k \quad (۳۹)$$

$$\sigma_r^2 = \mathbb{E}[(\boldsymbol{r_k} - \bar{r})^2] = \frac{1}{m}\sum_{k=1}^{m}(r_k - \bar{r})^2$$

m تعداد نمونه‌ها است، $\bar{r}$ و σ_r^2 مقادیر میانگین و واریانس مانده در حالت بدون حمله است. متعاقباً، برای تست سیگنال مانده می‌توان آن را با مقادیر آماری به‌دست‌آمده مقایسه نمود؛ بنابراین تابع تصمیم‌گیری (۳۸) به‌صورت زیر می‌تواند بازنویسی شود [۳۱]:

$$\bar{r} - \lambda\sigma_r \leq \boldsymbol{r_k} \leq \bar{r} + \lambda\sigma_r \quad for \ f_k = 0 \quad (۴۰)$$

$$\Rightarrow S_r = 0 \ attck \ free \ case$$

$$\boldsymbol{r_k} < \bar{r} - \lambda\sigma_r \ or \ \boldsymbol{r_k} > \bar{r} + \lambda\sigma_r \quad for \ f_k \neq 0$$

$$\Rightarrow S_r = 1 \ attacked \ case$$

عامل سازگاری[1]، λ به‌صورت معمول $\lambda \geq 3$ انتخاب می‌شود و باید به‌گونه‌ای انتخاب شود که مصالحه‌ای بین بیشترین احتمال آشکارسازی حمله و کمترین احتمال اعلام اشتباه حمله برقرار شود.

۳-۴- مشاهده‌گر ورودی نامعلوم مبتنی بر فیلتر کالمن

در اینجا الگوریتم مشاهده‌گر ورودی نامعلوم مبتنی بر فیلتر کالمن را به‌منظور تشخیص و شناسایی حمله سایبری به‌صورت زیر ارائه خواهد شد:

$$\hat{x}_{k+1|k} = \bar{A}_k\hat{x}_k + \bar{B}_k u_k + \bar{E}_k y_{k+1} \quad (۴۱)$$

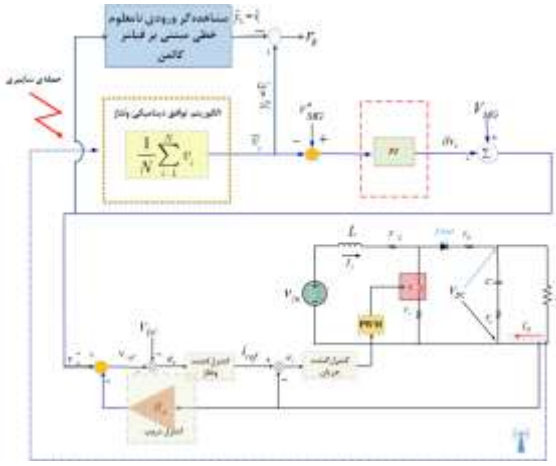
$$P_{k+1|k} = \bar{A}_k P_k \bar{A}_k^T + Q_{k+1} \quad (۴۲)$$

$$K_{k+1} = P_{k+1|k}C_{k+1}^T\left(C_{k+1}P_{k+1|k}\,C_{k+1}^T + R_{k+1}\right)^{-1} \quad (۴۳)$$

$$\hat{x}_{k+1} = \hat{x}_{k+1|k} + K_{k+1}(y_{k+1} - C_{k+1}\hat{x}_{k+1|k}) \quad (۴۴)$$

$$P_{k+1} = [I - K_{k+1}C_{k+1}]P_{k+1|k} \quad (۴۵)$$

با استفاده از الگوریتم توضیح داده شده می‌توان اغتشاش را از معادلات تخمین حلت جدا کرد، یا به عبارتی تخمین حلت را در مقابل اغتشاش (ورودی نامعلوم) مقاوم نمود. سپس با استفاده از مقایسه رفتار واقعی سیستم و رفتار نامی آن، سیگنال باقیمانده را برای آشکارسازی حمله تولید نمود. در شکل (۱۳) بلوک دیاگرام الگوریتم پیشنهادی (الگوریتم بازسازی و شناسایی حملات سایبری در ریزشبکه DC توسط مشاهده‌گر ورودی نامعلوم خطی مبتنی بر فیلتر کالمن) باهدف درک بهتر از نحوی اجرا و پیاده‌سازی آن ارائه شده است.



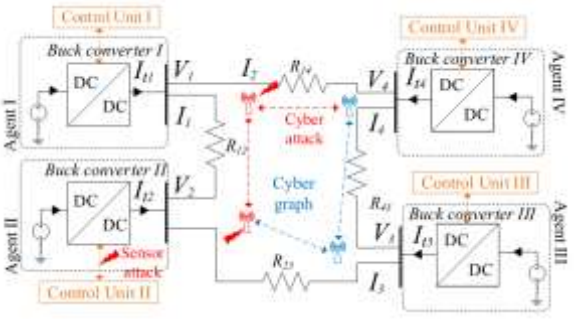
شکل (۱۳). الگوریتم بازسازی و شناسایی حملات سایبری به ریزشبکه DC توسط مشاهده‌گر ورودی نامعلوم خطی مبتنی بر فیلتر کالمن

5-نتایج شبیه‌سازی

هدف این بخش طراحی یک مشاهده‌گر ورودی نامعلوم برای بازسازی و خنثی‌کردن اثر حمله سایبری بر ریزشبکه‌های قدرت شده است؛ بنابراین یک ریزشبکه DC را در نظر بگیرید که از ۴ واحدهای تولید پراکنده[2] (DGU) با بارهای ناشناخته به هم متصل شده تشکیل شده است. توپولوژی ریزشبکه مذکور در شکل (۱۴) نشان‌داده‌شده است. کل ریزشبکه با استفاده از راهبُرد کنترل توزیع شده ارائه شده در مرجع [۲۲] کنترل می‌شود که اشتراک جریان معادل و کنترل ولتاژ متوسط را تضمین می‌کند. همچنین یک کنترل‌کننده برای اطمینان از همگرایی ولتاژ متوسط به مقدار ۲۰۰ ولت طراحی شده است.

[1] Tolerance Parameter

[2] Distributed Generation Unit



شکل (۱۴). توپولوژی ریزشبکه DC با چهار DGU. فلش آبی نشان‌دهنده لایه سایبری و فلش سیاه نشان‌دهنده جریان فیزیکی است.

مقادیر عامل‌های ریزشبکه قدرت و بارها در جدول (۱) مقداردهی شده است:

جدول ۱. مقداردهی عامل‌های ریزشبکه‌های قدرت

عامل	مقدار	عامل	مقدار
R	$0/23\Omega$	r_d	$0/005\Omega$
L	$0/35mH$	r_L	$0/1\Omega$
C	$50\mu F$	r_C	$0/03\Omega$
R_{12}	2Ω	R_{14}	$1/6\Omega$
R_{23}	$2/5\Omega$	R_{34}	2Ω

برای طراحی مشاهده‌گر نیاز است تا ماتریس E_k معلوم باشد هر چند که مقدار واقعی d_k نامعلوم است [۲۹]. در مدل لحاظ شده در این مطالعه، فرض بر این است که ریزشبکه‌ها در حالت ماندگار کار می‌کند و همه‌ی حالت‌ها به‌وسیله‌ی ورودی نامعلوم (اغتشاش) به‌صورت یکسان تحت‌تأثیر قرار می‌گیرند، بنابراین ضریب اغتشاش به‌صورت زیر می‌تواند نوشته شود:

$$E_k = [1,1,1,1]^T \quad (۴۶)$$

در شبیه‌سازی نیاز به مدل گسسته‌ی سیستم است. برای این منظور، معادله (۲۰) با استفاده از روش رانگ - کوتا[1] مرتبه‌ی چهارم با $\Delta t = 0.01s$ گسسته‌سازی شده است. علاوه بر این عامل‌های طراحی فیلتر به شرح زیر است:

$$Q = diag\{10^{-4}, 10^{-4}, 10^{-4}, 10^{-4}\}$$

$$R = 10^{-3}$$

$$x_0 = [0,0,0,0]^T$$

$$\hat{x}_0 = [0,0,0,0]^T$$

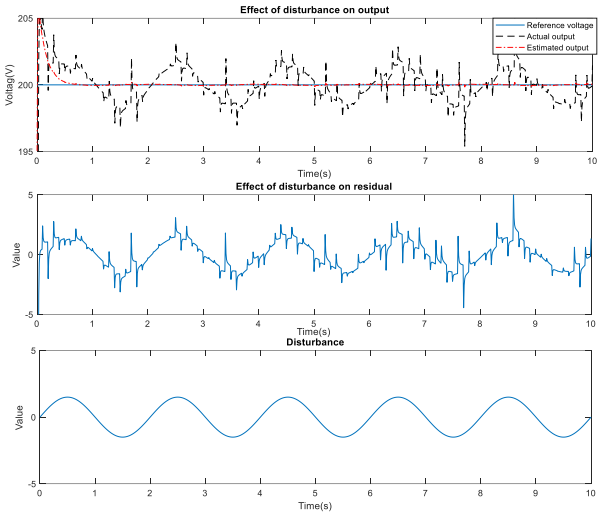
$$\hat{P}_0 = diag\{10^{-2}, 10^{-2}, 10^{-2}, 10^{-2}\}$$

که x_0، R و Q تولید داده‌های واقعی به کار می‌روند و $\hat{Q}, \hat{R}, \hat{x}_0$ و $\hat{P}_0$در مشاهده‌گر استفاده می‌شوند. توجه شود که باتوجه‌به مقادیر ماتریس‌های E_k و C_k شرط II همیشه برقرار است و مشاهده‌گر ورودی نامعلوم وجود دارد.

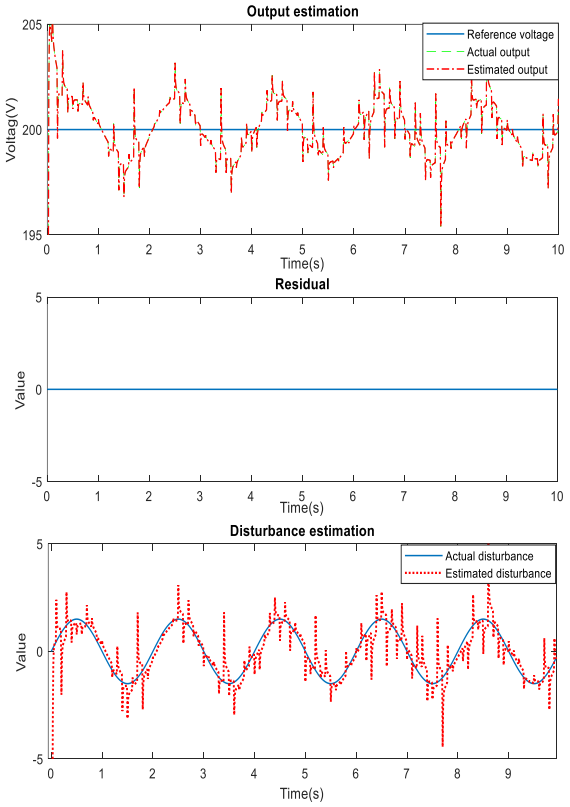
۱-۵- تحلیل جداسازی اغتشاش از مانده‌ها

برای بررسی اثر ورودی نامعلوم بر مانده، می‌توان d_k را به شکل زیر انتخاب کرد:

$$d_k = sin(0.5\pi t_k)\, cos(0.5\pi t_k) \quad (۴۷)$$



شکل (۱۵). اثر اغتشاش برمانده بدون جداسازی



شکل (۱۶). اثر اغتشاش برمانده با جداسازی

اثر جداسازی اغتشاش از مانده‌ها در شکل‌های (۱۵) و (۱۶) نشان‌داده‌شده است. شکل (۱۵) هنگامی که جداسازی اغتشاش انجام نمی‌شود و مانده به‌صورت غیرمقاوم تولید می‌شود، را نشان می‌دهد. همان‌طور که در این شکل مشخص است، هنگامی که

[1] Rung-Kutta

حمله‌ای رخ نداده است، سیگنال مانده برابر با صفر نیست و ممکن است که به‌اشتباه سیگنال مانده حمله را اعلام کند.
در شکل (۱۶) تولید مانده مقاوم با جداسازی اغتشاش نشان‌داده‌شده است. می‌توان مشاهده نمود که در این حالت مانده‌ها به سمت صفر میل می‌کنند و هنگامی که حمله‌ای رخ نداده است، مانده هم به‌درستی مقدار صفر را دارد.

۲-۵-شبیه‌سازی حالت‌های مورد حمله قرار گرفته

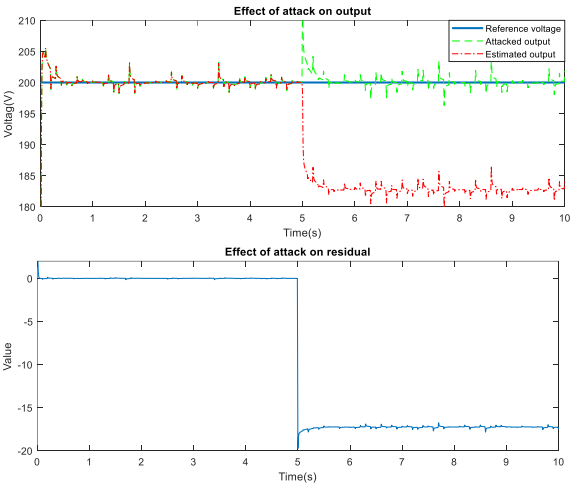
این بخش به بررسی روش پیشنهادی هنگام رخ‌دادن حمله می‌پردازد. بعد از تولید مانده‌ی مقاوم نیز به بررسی رفتار مانده‌ها در وضعیت حمله پرداخته می‌شود.
حملات سایبری را می‌توان در چند دسته طبقه‌بندی نمود: حملات تزریق داده‌های نادرست، محروم‌سازی سرویس[1]، حملات بازپخش[2]. این مقاله بر روی مورد اول تمرکز خواهد داشت زیرا شایع‌ترین نوع حمله سایبری است. این نوع حمله مبتنی بر تزریق اندازه‌گیری‌های مخرب در حسگرها/ لینک‌های سایبری آسیب‌پذیر به‌منظور دست‌کاری در عملکرد سیستم حلقه بسته است.
بنابراین، حمله تزریق داده‌های نادرست به ریزشبکه به دو صورتی که در زیر توضیح داده شده است، شبیه‌سازی خواهد شد:
حالت اول) یک حمله ناگهانی که ۱۰٪+ با اندازه‌گیری‌های معمولی اختلاف دارد، در اولین خروجی رخ می‌دهد. بعد از ۵۰ گام زمانی (۵ ثانیه) از تولید مانده حمله سایبری در حسگر مربوط به ولتاژ باس خروجی رخ می‌دهد:

$$f_k = \begin{cases} 0 & t < 5s \\ 0.1y_{1,k} & t \geq 5s \end{cases} \quad (۴۸)$$

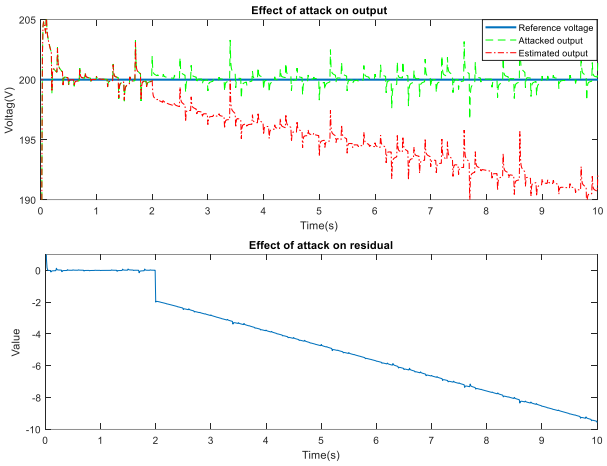
حالت دوم) در این حالت یک حمله در حسگرها اتفاق می‌افتد:

$$f_k = \begin{cases} 0 & t < 2s \\ t & t \geq 2s \end{cases} \quad (۴۹)$$

نتایج شبیه‌سازی برای حالت‌های اول و دوم به ترتیب در شکل‌های (۱۷) و (۱۸) نمایش‌داده‌شده است.



شکل (۱۷). آشکارسازی موفق حمله در حضور ورودی نامعلوم هنگامی که حمله در مقدار ولتاژ باس خروجی رخ می‌دهد.



شکل (۱۸). آشکارسازی موفق حمله در حضور ورودی نامعلوم هنگامی که حمله در حسگرها رخ می‌دهد.

باتوجه‌به حالت‌های اول تا دوم که در شکل‌های (۱۷) و (۱۸) نشان‌داده‌شده است. توجه شود که در تمامی حالت‌ها، حمله وقتی که ریزشبکه به حالت ماندگار خود رسیده به وقوع پیوسته است. همان‌طور که در شکل (۱۷) دیده می‌شود، رفتار سیستم به طور قابل‌توجهی در طی حملات تحت‌تأثیر قرار گرفته است. بااین‌وجود ریزشبکه ناپایدار نشده است و ولتاژ متوسط به مقدار مرجع ۲۰۰ ولت همگرا می‌شود. هر حمله را می‌توان با اجرای مشاهده‌گر حالت پیشنهادی در هر DGU شناسایی و بازسازی نمود. سپس می‌توان از بازسازی حمله جهت "حذف" حسگرها و لینک‌های سایبری مورد حمله واقع شده استفاده نمود.

باتوجه‌به شکل‌های (۱۷) و (۱۸) می‌توان دریافت که ولتاژ خروجی و باقیمانده در رویکرد پیشنهادی به‌درستی تخمین زده شده است؛ بنابراین، حالت‌های مورد حمله واقع شده به‌وضوح آشکار می‌شوند. نتایج شبیه‌سازی تأیید می‌کنند که روش پیشنهادی تحت نویزهای مختلف مانده‌ای درست را تولید می‌کنند، این رویکرد می‌تواند در این شرایط حمله را به‌درستی آشکار سازد. همچنین باتوجه‌به شکل‌های مذکور می‌توان دریافت که می‌شود، حمله را جبران نمود و مقدار متغیر مورد حمله را به‌درستی تخمین زد.

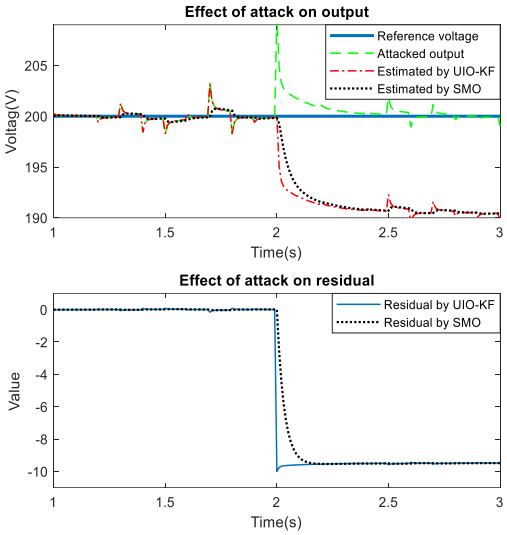
باتوجه‌به نتایج شبیه‌سازی می‌توان دریافت که بازسازی حملات تزریق داده نادرست تأثیر حملات را بر سیستم نشان می‌دهد. این شبیه‌سازی راهبُرد بازسازی پیشنهادی را تأیید می‌کند. علاوه بر این مقیاس‌پذیری این طرح را نشان می‌دهد. دقت تخمین رویکرد پیشنهادی مستقل از توپولوژی ریزشبکه DC و وجود حملات سایبری در سایر DGUها است. در نتیجه، DGUهای جدید می‌توانند در ریزشبکه گنجانده شوند و طرح بازسازی پیشنهادی همچنان با تغییرات جزئی قابل‌پیاده‌سازی باشد.

[1] *Denial Of Service*

[2] *Replay Attacks*

۳-۵- مقایسه رویکردبازسازی حمله سایبری پیشنهادی با رویکرد ارائه شده در مرجع [۲۲]

در این بخش کارایی رویکرد مشاهده‌گر ورودی نامعلوم مبتنی بر فیلتر کالمن پیشنهادی با روش مشاهده‌گر غیرخطی مبتنی بر رویتگر حالت لغزشی ارائه شده در مرجع [۲۲] مقایسه خواهد شد. عامل‌های طراحی رویتگر حالت لغزشی[1] (*SMO*) به‌صورت $\lambda_0 = 16$ و $\lambda_1 = 121.7, \lambda_2 = 11$ تنظیم شده است که همگرایی تخمین حالت را تضمین می‌کند. بااین‌وجود، دقت تخمین رویتگر حالت لغزشی با مرتبه بالا به نویز اندازه‌گیری حساس است. به همین دلیل تخمین سیگنال حمله از طریق یک فیلتر پایین گذر فیلتر شده است. بیشتر مؤلفه‌های طیفی نویز فرکانس بالا مربوطه در حدود یک کیلوهرتز هستند، بنابراین سیگنال‌ها از طریق یک فیلتر پایین گذر با فرکانس قطع در یک کیلوهرتز فیلتر شده‌اند. لازم به ذکر است که در اینجا توپولوژی ریزشبکه همان توپولوژی نشان‌داده‌شده در شکل (۱۴) خواهد بود. همچنین به‌منظور مقایسه حمله سایبری به‌صورت رابطه (۴۸) به سیستم اعمال خواهد شد.



شکل (۱۹). آشکارسازی حمله در حضور ورودی نامعلوم توسط دو رویکرد UIO-KF و SMO

آشکارسازی حمله در حضور ورودی نامعلوم توسط دو رویکرد *UIO-KF* و *SMO* در شکل (۱۹) نشان‌داده‌شده است. همان‌طور که در این شکل مشاهده می‌شود، در هر دو رویکرد مذکور وجود نویز اندازه‌گیری مانع از پایداری تخمین سیگنال حمله نشده است و هر دو رویکرد مذکور به‌درستی توانسته‌اند سیگنال حمله را بازسازی نمایند. اما رویکرد پیشنهادی در این مطالعه نسبت به روش رویتگر حالت لغزشی دارای دو مزیت مهم است: ۱) روش رویتگر حالت لغزشی به‌منظور تخمین سیگنال حمله نیازمند تنظیم عامل‌های λ است و عدم تنظیم درست این عامل‌ها بر روی دقت تخمین تأثیرگذار است. اما رویکرد پیشنهادی فارغ از عامل‌های تنظیمی جهت تخمین سیگنال حمله است. ۲) به طور طبیعی تخمین سیگنال حمله توسط رویتگر حالت لغزشی در حضور نویز اندازه‌گیری به یک خطای محدود حول مقدار سیگنال حمله واقعی همگرا می‌شود. این خطا را می‌توان با افزایش ثابت زمانی فیلترهای پایین گذر پیاده‌سازی شده کاهش داد. بااین‌حال، وجود یک فیلتر پایین گذر (و افزایش ثابت زمانی آن) نرخ همگرایی رویتگر را کاهش می‌دهد که عملکرد گذرا تخمین سیگنال را بدتر می‌کند. اما تخمین سیگنال حمله توسط رویکرد رویتگر ورودی نامعلوم مبتنی بر فیلتر کالمن پیشنهادی به نویز اندازه‌گیری حساس نبوده و در نتیجه عملکرد حالت گذرای آن تحت‌تأثیر نویز اندازه‌گیری قرار نمی‌گیرد. این واقعیت را می‌توان با مقایسه تخمین سیگنال در زمان $t = 2s$ در شکل (۱۹) مشاهده نمود، جایی که تخمین حمله توسط رویتگر ورودی نامعلوم مبتنی بر فیلتر کالمن بلافاصله به مقدار واقعی همگرا می‌شود، ولی تخمین حمله توسط رویتگر حالت لغزشی به مدت‌زمان ۰.۲ ثانیه برای همگرایی نیاز دارد؛ بنابراین به‌طورکلی در جدول ۲ برخی از مزایای رویکرد پیشنهادی *UIO-KF* با رویکرد *SMO* به طور خلاصه فهرست شده است.

جدول ۲. خلاصه‌ای از نتایج حاصل از مقایسه دو روش

روش پیشنهادی *UIO-KF*	عدم وابستگی به عامل‌های تنظیمی خاص	حساسیت کمتر به میزان نویز و ارائه پاسخ گذرا و ماندگار بهتر در صورت بروز حمله سایبری
رویکرد *SMO*	وابستگی شدید عملکرد به تنظیم دقیق عامل λ	حساسیت بیشتر به میزان نویز و ارائه پاسخ ضعیف‌تر در مقایسه با رویکرد پیشنهادی

6- نتیجه‌گیری

در این مقاله، نخست مدل ریزشبکه در فضای حالت تدوین گردید. سپس، یک الگوریتم تشخیص و شناسایی حمله نوین با استفاده از ترکیب روش مشاهده‌گر ورودی نامعلوم و فیلتر کالمن جهت آشکارسازی مقاوم حمله معرفی و پیاده‌سازی شده است. رویکرد پیشنهادی به طور کامل توزیع شده است. این ویژگی مقیاس‌پذیری را برای ریزشبکه‌های مقیاس بزرگ ساده‌تر می‌کند و همچنین منجر به بی‌اثربودن تعداد عوامل حمله در عملکرد الگوریتم پیشنهادی می‌گردد. نتایج شبیه‌سازی موید عملکرد مناسب روش پیشنهادی در زمینه تشخیص و شناسایی حمله سایبری در حضور اغتشاش و نویز است، به‌نحوی که مشاهده‌گر ورودی نامعلوم با ترکیب فیلتر کالمن ضمن آشکارسازی حمله، اثر آن را نیز خنثی نماید. همچنین به‌درستی مقدار واقعی متغیر

[1] Sliding Mode Observer

مورد حمله تخمین زده شد؛ بنابراین امید است بر اساس رویکرد ارائه شده بتوان سایر ریزشبکه‌ها را در برابر حملات سایبری مقاوم نمود.

7-مراجع

[1] C. Peng, H. Sun, M. Yang, and Y.-L. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol. 49, pp. 1569-1554, .2019

[2] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic control,* vol. 59, pp. 1467-1454, .2014

[3] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing,* vol. 338, pp. -101 115, .2019

[4] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica,* vol. 51, pp. 148-135, .2015

[5] Y. Zhou, K. G. Vamvoudakis, W. M. Haddad, and Z.-P. Jiang, "A secure control learning framework for cyber-physical systems under sensor and actuator attacks," *IEEE Transactions on Cybernetics,* .2020

[6] R .Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy,* vol. 9, pp. 51-49, .2011

[7] Y. Liu and S. Hu, "Cyberthreat analysis and detection for energy theft in social networking of smart homes," *IEEE Transactions on Computational Social Systems,* vol. 2, pp. 158-148, .2015

[8] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Transactions on Power Systems,* vol. 31, pp. 3872-3864, .2015

[9] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics,* vol. 13, pp. 423-411, .2016

[10] K. Paridari, N. O'Mahony, A. E.-D. Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg, "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration," *Proceedings of the IEEE,* vol. 106, pp. 128-113, .2017

[11] Y. Shoukry, P .Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, "Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach," *IEEE Transactions on Automatic Control,* vol. 62, pp. .2017 ,4932-4917

[12] S. Zuo, T. Altun, F. L. Lewis, and A. Davoudi, "Distributed resilient secondary control of DC microgrids against unbounded attacks," *IEEE Transactions on Smart Grid,* vol. 11, pp. 3859-3850, .2020

[13] A. Begum and S. Badugu, "A study of malicious url detection using machine learning and heuristic approaches," in *Advances in Decision Sciences, Image Processing, Security and Computer Vision*, ed: Springer, 2020, pp. .597-587

[14] J. A. Santhi and T. V. Saradhi, "Attack detection in medical Internet of things using optimized deep learning: enhanced security in healthcare sector," *Data Technologies and Applications,* .2021

[15] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid,* vol. 8, pp. 2516-2505, .2017

[16] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE transactions on automatic control,* vol. 58, pp.2013 ,2729-2715 .

[17] L. Meng, Q. Shafiee, G. F. Trecate, H. Karimi, D. Fulwani, X. Lu*, et al.*, "Review on control of DC microgrids and multiple microgrid clusters," *IEEE Journal of Emerging and Selected Topics in Power Electronics,* vol. 5, pp. .2017 ,948-928

[18] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on smart grid,* vol. 3, pp. 1370-1362, .2012

[19] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J .C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Systems Journal,* vol. 14, pp. 5339-5329, .2020

[20] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Transactions on Automatic Control,* vol. 61, pp. -2079 2091, .2015

[21] W. Ao, Y. Song, and C. Wen, "Adaptive cyber-physical system attack detection and reconstruction with application to power systems," *IET Control Theory & Applications,* vol. 10, pp. 1468-1458, .2016

[22] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló, and F. Blaabjerg, "Detection and mitigation of false data in cooperative dc microgrids with unknown constant power loads," *IEEE Transactions on Power Electronics,* vol. 36, pp. 9577-9565, .2021

[23] M. Darouach, M. Zasadzinski, and S. J. Xu, "Full-order observers for linear systems with unknown inputs," *IEEE transactions on automatic control,* vol. 39, pp. 609-606, .1994

[24] I. Shames, A. M. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed fault detection for interconnected second-order systems," *Automatica,* vol. 47, pp. 2764-2757, .2011

[25] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—Part II: Attack detection using enhanced hydrodynamic models ",*IEEE Transactions on Control Systems Technology,* vol. 21, pp. 1693-1679, .2013

[26] Y. H. Chang, Q. Hu, and C. J. Tomlin, "Secure estimation based Kalman filter for cyber–physical systems against sensor attacks," *Automatica,* vol. 95, pp. 412-399, .2018

[27] J. CHEN and H. ZHANG, "Robust detection of faulty actuators via unknown input observers," *International Journal of Systems Science,* vol. 22, pp. 1839-1829, .1991

[28] J. Chen and R. J. Patton, *Robust model-based fault diagnosis for dynamic systems* vol. 3: Springer Science & Business Media, .2012

[29] J. Chen and R. J. Patton, "Robust residual generation using unknown input observers," in *Robust model-based fault diagnosis for dynamic systems*, ed: Springer, 1999, pp. .108-65

[30] K. Xiong, C. Chan, and H. Zhang, "Detection of satellite attitude sensor faults using the UKF," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 43, pp. 491-480, .2007

[31] D. Zhang, Q.-G. Wang, G. Feng, Y. Shi, and A. V. Vasilakos, "A survey on attack detection, estimation and control of industrial cyber–physical systems," *ISA transactions,* .2021

[32] J. Li, C. Sun, S. Yang, and Q. Su, "Dynamic load altering attack detection based on adaptive fading Kalman filter in smart grid," IET Generation, Transmission & Distribution, vol. 18, no. 2, pp. 303–313, 2024, doi: 10.1049/gtd2.13057.

[33] Y. Huang, X. Rong, G. Li, C. Chen, and Z. Bie, "Resilience assessment of active distribution systems considering microgrid formation based on grid-edge DERs," IET Generation, Transmission & Distribution, vol. 18, no. 2, pp. 233–247, 2024, doi: 10.1049/gtd2.12865.

[34] A. H. El-Ebiary, M. A. Attia, F. H. Awad, A. K. Ibrahim, and M. Mokhtar, "Kalman filters based distributed cyber-attack mitigation layers for DC microgrids," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 71, no. 3, pp. 1358–1370, 2024, doi: 10.1109/TCSI.2023.3348928.