Digital Twins for Detection, Localisation, and Attribution of Cyberattacks

Harsh Pathak[1], Rajeev Thakur[2]
[1,2]Department of Electrical and Electronics Engineering:
NRI Institute of Information Science & Technology
Bhopal (M.P.) India

Abstract—

The increasing dependence of active distribution networks on synchronized measurements and communication-based monitoring has introduced significant vulnerabilities to false data injection (FDI) and coordinated stealth cyberattacks. This paper presents a per-node digital twin (DT)-based framework for cyberattack detection, localisation, and attribution in the IEEE 33-bus radial distribution network. The proposed framework integrates distribution-level phasor measurement unit (D-PMU) data, node-specific digital twin predictions, residual analysis, cumulative sum (CUSUM)-based anomaly detection, persistence verification, and watermark-assisted validation. Four digital twins corresponding to buses 9, 13, 28, and 33 are considered to evaluate identification accuracy and attack detection performance. The estimated time constants range from 19.91 to 19.95 ms against a reference value of 20.00 ms, resulting in relative errors between 0.25% and 0.45%, with an average error of 0.325%. Under a ramp FDI attack targeting bus 33, the node-specific residuals reveal progressively increasing measurement deviations, with attack confirmation reported at approximately 2.52 s. Furthermore, a coordinated stealth attack involving buses 9 and 13 demonstrates how oppositely signed measurement manipulations can conceal abnormalities in aggregated monitoring indicators. The per-node detection framework preserves individual residual signatures and identifies the affected nodes, with attack confirmation reported at approximately 2.50 s. The results demonstrate the potential of combining spatially resolved digital-twin monitoring with sequential anomaly detection to identify gradual, coordinated cyberattacks. The proposed framework provides a promising approach for improving measurement integrity, attack localisation, and cyber-physical situational awareness in active distribution networks.

Keywords--- *Active distribution networks, coordinated stealth attacks, cumulative sum (CUSUM), cyberattack detection, digital twin, false data injection, IEEE 33-bus system, per-node monitoring, attack localisation.*

I. INTRODUCTION

This Measurement-driven supervision of active distribution feeders is vulnerable to false data injection (FDI), replay, and coordinated manipulation. Recent advancements in digital twin (DT) technology, artificial intelligence, and cyber-physical monitoring have created new opportunities for enhancing the security of active distribution networks. Digital twin-based cyberattack detection and mitigation for DC microgrids has been investigated in [1], highlighting the integration of virtual system representations with cybersecurity monitoring and corrective control. The combination of digital twin technology and support vector machines (SVMs) for fault and cyberattack detection was explored in [2]. Meanwhile, multi-scenario optimisation of distributed generation (DG), soft open points (SOPs), and electric vehicle charging stations (EVCSs) was examined in [3], providing insights into the planning and operation of active distribution systems. Real-time cyberattack detection and response using digital twins in protection relays was addressed in [4], while a real-time model for attack detection and prediction in smart grids was presented in [5]. These studies establish the relevance of integrating cyber-physical monitoring, virtual system models, and intelligent detection mechanisms.

Graph-based learning techniques have received considerable attention for identifying stealthy false data injection attacks (FDIAs). A graph neural network (GNN)-based framework for joint attack detection and localisation was investigated in [6], emphasising the importance of network connectivity in identifying compromised measurement locations. A generalised GNN-based detection approach was developed in [7] to exploit structural relationships among power-system measurements. The combination of dynamic and static state estimation for detecting FDIAs was examined in [8], demonstrating an alternative to purely data-driven monitoring. A graph convolutional attention network was introduced for locational attack detection in [9], whereas a Hodge graph neural network utilising edge-space information was explored in [10]. Furthermore, an interpretable detection approach incorporating graph attention mechanisms was investigated in [11]. Collectively, these contributions demonstrate the importance of spatial relationships, measurement consistency, and network topology in cyberattack identification.

Distributed learning and advanced feature extraction have also been explored to improve cybersecurity monitoring. A vertical federated learning framework for FDIA detection in distribution networks was presented in [12], addressing the potential of collaborative learning across distributed data sources. An adaptive adversarial dual-autoencoder incorporating graph representation learning was investigated in [13] to identify abnormal measurement patterns in cyber-physical power systems. Multiscale feature fusion using deep learning was examined in [14] to extract informative characteristics associated with false data injection attacks. In parallel, the effects of distributed

generation on distribution-system performance were analyzed in [15], highlighting the operational significance of accurately representing DG-integrated feeders. These studies indicate that cyberattack detection must account for both measurement characteristics and variations in physical network operating conditions.

The increasing sophistication of cyberattacks has motivated research into stealthy measurement manipulation and spatiotemporal anomaly detection. Tensor-completion-enabled stealthy false data injection attacks were investigated in [16], emphasising the potential limitations of detection methods that rely exclusively on conventional measurement consistency. A deep learning deviation-based defence scheme for power distribution systems was developed in [17], using deviations in operating information to support attack identification. A detection architecture combining graph spatial features with temporal convolutional neural networks was explored in [18], incorporating spatial and temporal information for identifying suspicious behaviour. Concurrent planning of DG and SOPs for enhancing distribution-system performance was addressed in [19], providing additional background for the modeling of controllable resources in active feeders. These contributions highlight the need to distinguish cyber-induced measurement abnormalities from legitimate changes caused by distributed energy resources and network operation.

Recent research has further emphasised the localisation and interpretation of false data injection attacks. A recursive variational graph autoencoder was investigated in [20] for identifying compromised locations in smart grids. Spectral graph neural networks were employed in [21] to leverage graph-level features for improved attack detection. An ensemble of convolutional neural networks combined with explainable artificial intelligence was presented in [22] for detecting and localizing FDIAs in power distribution systems. A cloud-edge architecture based on split learning was investigated in [23], addressing distributed computation for detecting locational attacks. These studies demonstrate growing interest in identifying not only whether a cyberattack has occurred but also where suspicious measurements originate.

Beyond individual measurement attacks, coordinated manipulation and cyber-resilient operation represent important research directions. Detection and defence against multipoint false data injection attacks targeting load-frequency control were investigated in [24], highlighting the importance of considering simultaneous manipulation across multiple measurement channels. A statistical hypothesis testing and artificial neural network-based approach for attack detection and mitigation in DC microgrids was explored in [25], connecting cybersecurity monitoring with control-system protection. Furthermore, techno-economic planning of DG and SOPs using optimisation and network reconfiguration was investigated in [26] to enhance distribution-system resilience. These contributions provide complementary perspectives on coordinated attack detection and mitigation, as well as the operational flexibility of modern distribution networks.

A. Research Gaps

Despite the progress reported in the literature, several challenges remain in developing effective cyberattack detection frameworks for active distribution networks. Digital twin-based approaches [1], [2], [4] provide a foundation for virtual monitoring, whereas graph-based techniques [6], [7], [9]-[11], [20], [21] focus on exploiting network relationships for anomaly detection and localisation. However, their use alone does not establish reliable node-specific detection under varying network conditions. Similarly, learning-based methods [12]-[14], [17], [18], [22], [23] require careful evaluation under operating conditions and attack patterns that differ from those represented during model development.

A further challenge is identifying coordinated attacks that affect multiple measurement channels simultaneously. Advanced stealth attacks [16] and multipoint manipulation strategies [24] demonstrate the importance of considering spatially distributed abnormalities. Moreover, changes associated with DG integration and network reconfiguration [3], [15], [19], [26] can complicate the interpretation of measurement deviations. Consequently, additional investigation is required into monitoring architectures that preserve node-level information, account for temporal persistence, and support attack localisation without relying exclusively on aggregated feeder-level indicators.

B. Motivation and Contribution of the Present Study

Motivated by these challenges, the present study investigates a four-stage per-node digital twin-based framework for cyberattack detection, localization, and attribution in an IEEE 33-bus distribution network. Four monitored buses-9, 13, 28, and 33-are considered to examine the effectiveness of node-specific digital twin identification and measurement-residual analysis. The framework combines local digital twin predictions with cumulative sum (CUSUM)-based temporal monitoring and attack-attribution logic.

The evaluation considers the provided per-node identification results, a ramp false data injection attack targeting bus 33, and a coordinated stealth attack involving multiple measurement channels. Unlike feeder-level monitoring approaches that rely solely on aggregated indicators, the considered framework retains separate residual information for individual monitored nodes. This enables an investigation of spatially resolved anomaly detection and the identification of potentially compromised measurement locations.

The main focus is therefore on integrating node-specific digital twin modeling, residual-based anomaly monitoring, temporal change detection, and coordinated attack attribution within a unified cyber-physical monitoring architecture. The study aims to assess the potential of this integration for improving the interpretability and localization capability of cyberattack detection in active distribution networks

II. SYSTEM AND MEASUREMENT MODEL

A. Monitored feeder and twin bank

The supplied architecture identifies an IEEE 33-node feeder, a D-PMU voltage vector, and four node-specific

twins. The monitored set is S = {9, 13, 28, 33}. Each twin produces a prediction for its associated measurement channel. The figure labels a shared weight α; its numerical value and training procedure are not reported.

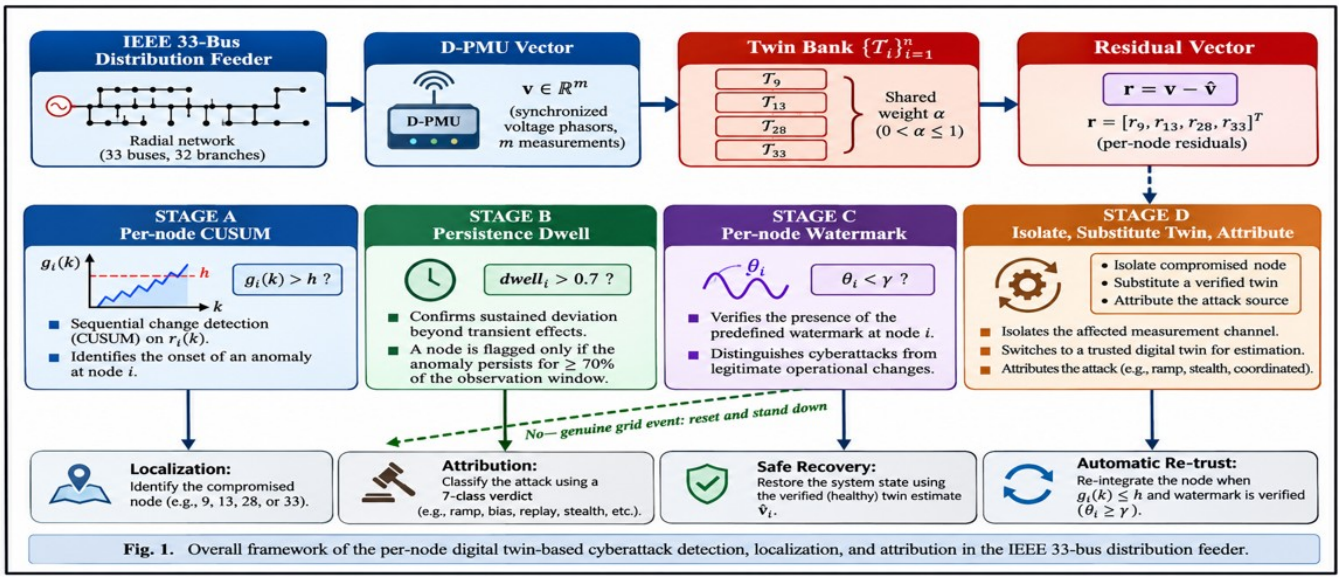

Fig. 1 Overall framework of the proposed per-node digital twin-based cyberattack detection, localization, and attribution method.

Fig. 1 illustrates the proposed four-stage cyberattack detection framework for the IEEE 33-bus radial distribution network using a bank of per-node digital twins. Initially, synchronized voltage measurements are acquired through distribution-level phasor measurement units (D-PMUs) and supplied to the digital twin bank, which maintains individual virtual representations of the monitored buses. The considered framework includes four digital twins corresponding to buses 9, 13, 28, and 33, with a shared weighting parameter used in the identification process. Each digital twin generates a predicted voltage measurement, which is compared with the corresponding observed measurement to construct a node-specific residual vector. Retaining individual residuals enables the framework to examine spatially distributed abnormalities that may be concealed by aggregate monitoring indicators.

The detection procedure consists of four sequential stages. Stage A employs a per-node cumulative sum (CUSUM) detector to accumulate residual deviations over time. An initial anomaly is indicated when the corresponding CUSUM statistic exceeds a predefined threshold. Stage B evaluates the persistence of the detected abnormality using a dwell criterion to distinguish sustained measurement deviations from short-duration transients. Stage C incorporates per-node watermark verification to assess whether the observed response is consistent with the expected system behaviour. This additional verification stage helps distinguish between potentially malicious measurement manipulation and legitimate network disturbances. If the verification indicates a genuine operating event, the detection process is reset, and normal monitoring continues.

Following confirmation of suspicious behaviour, Stage D isolates the potentially compromised measurement channel and substitutes a trusted digital twin estimate to maintain reliable monitoring. The framework also supports attack attribution by examining the characteristics of the detected abnormality and its distribution across monitored nodes. The resulting outputs include identification of the affected node, classification of the suspected attack, and recovery using validated state estimates. An automatic re-trust mechanism is considered for restoring the isolated measurement channel once the required residual and verification conditions are satisfied. Overall, the framework integrates node-specific modelling, sequential anomaly detection, persistence analysis, watermark verification, and measurement recovery to support interpretable cyberattack detection and localisation in active distribution networks.

B. Attack and residual representation

For an additive FDI scenario, a received measurement can be represented as [1], [2]

$$v^a(k) = v(k) + a(k) \quad (1)$$

where v(k) is the uncompromised measured voltage vector and a(k) denotes an injected vector. The node-specific prediction residual is

$$r_i(k) = v^a{}_i(k) - \hat{v}_i(k), \; i \in S \quad (2)$$

and the residual vector retains spatial identity:

$$r(k) = [r_9(k), r_{13}(k), r_{28}(k), r_{33}(k)]^T \quad (3)$$

The supplied schematic writes the residual in the form r = v − v̂; the attacked-voltage notation above makes explicit which received signal is being tested. It does not establish the twins' internal dynamic equations.

III. FOUR-STAGE DETECTION LOGIC

A. Per-node CUSUM screening

The first stage tests whether a per-node cumulative statistic exceeds a threshold. A generic one-sided magnitude CUSUM consistent with this stage is

$$g_i(k) = \max\{0, g_i(k-1) + |r_i(k)| - \kappa_i\}. \quad (4)$$

An alarm candidate is raised when $g_i(k) > h_i$. The allowance κ_i and threshold h_i are not specified in the supplied material; (4) is a generic formulation rather than a verified reproduction of the simulation implementation [19].

B. Persistence, watermark and response

Stage B asks whether the event persists for a specified dwell time. Stage C applies per-node watermark evidence. The schematic denotes a thresholded watermark quantity, but does not provide a complete watermark signal model or threshold value. Stage D isolates, substitutes, twins, and attributes affected channels. The diagram also distinguishes localization (which node lied), attribution (a seven-class verdict), safe recovery (live twin estimate), and automatic re-trust after verification. The seven class labels and detailed recovery logic are not available; therefore, no unreported classifier accuracy or recovery time is claimed.

IV. RESULTS AND DISCUSSION

A. Identification quality of four node twins

Table I presents the identification accuracy of the four per-node digital twins associated with buses 9, 13, 28, and 33 of the IEEE 33-bus distribution network. The estimated time constants are compared with a reference value of 20.00 ms to evaluate the accuracy of the digital twin identification process. The estimated values range from 19.91 to 19.95 ms, corresponding to relative errors between 0.25% and 0.45%. The lowest relative error of 0.25% is observed at bus 28, whereas bus 33 exhibits the highest error of 0.45%. Buses 9 and 13 achieve identical estimated time constants of 19.94 ms, with relative errors of 0.30%.

TABLE I. IDENTIFICATION ACCURACY OF THE FOUR PER-NODE DIGITAL TWINS

Bus	Est. τ (ms)	Ref. τ (ms)	Error (%)
9	19.94	20.00	0.30
13	19.94	20.00	0.30
28	19.95	20.00	0.25
33	19.91	20.00	0.45

The average relative error across the four monitored buses is 0.325%, indicating close agreement between the estimated and reference time constants. These results demonstrate accurate time-constant identification for the considered digital twins and provide a basis for subsequent node-specific residual analysis and cyberattack detection.

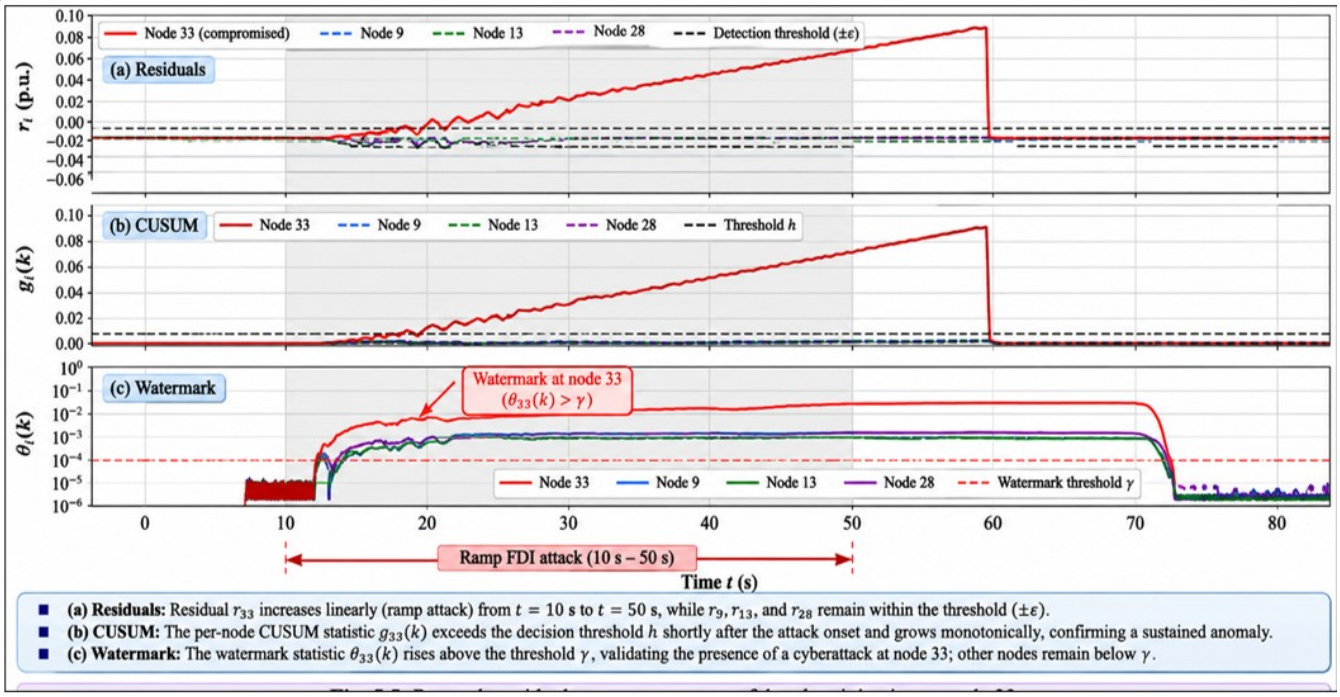

Fig. 2. Per-node residual response to a ramp false-data injection attack at node 33

B. Ramp false-data injection

Fig. 2 illustrates the response of the per-node digital twin-based detection framework to a ramp false-data injection (FDI) attack targeting node 33 of the IEEE 33-bus distribution network. The figure presents the evolution of the measured and estimated voltage signals, node-specific residual responses, and the corresponding detection statistics for nodes 9, 13, 28, and 33. The purpose of this experiment is to evaluate the proposed monitoring framework's ability to detect a gradually increasing measurement manipulation while preserving information about the affected network location.

The upper subplot compares the reported voltage at node 33 with the corresponding reference and digital twin-estimated signals. Before the attack, the measurements exhibit close agreement, indicating normal tracking behavior. Following attack initiation, the compromised measurement gradually deviates from its expected trajectory, producing a ramp-shaped increase. The difference between the manipulated measurement and the digital twin estimate becomes more pronounced as the attack progresses. This behavior demonstrates how a slowly increasing FDI attack can introduce a sustained measurement inconsistency rather than an abrupt change.

The middle subplot illustrates the residual responses associated with the monitored nodes. The residual corresponding to node 33 increases during the attack interval, whereas the other monitored nodes exhibit comparatively smaller deviations. This spatial difference provides evidence that node 33 is the principal affected measurement location. The preservation of separate node-level residuals is particularly important because a feeder-wide aggregate indicator could obscure the contribution of an individual compromised measurement channel.

The lower subplot presents the temporal evolution of the per-node detection statistics on a logarithmic scale. Following attack initiation, the statistics increase as evidence of abnormal measurement behaviour accumulates. The figure indicates a confirmed detection at approximately 2.52 s, with node 33 identified as the ramp-attack location. The different responses of the monitored nodes demonstrate the role of node-specific monitoring in supporting attack localization and distinguishing the dominant compromised channel from secondary network responses.

Overall, the results illustrate the capability of the considered per-node digital twin framework to reveal gradual measurement manipulation through deviations between reported and predicted operating conditions. The combined examination of voltage tracking, residual evolution, and temporal detection statistics provides a basis for identifying the affected node and assessing the persistence of the cyber-induced anomaly.

magnitudes.

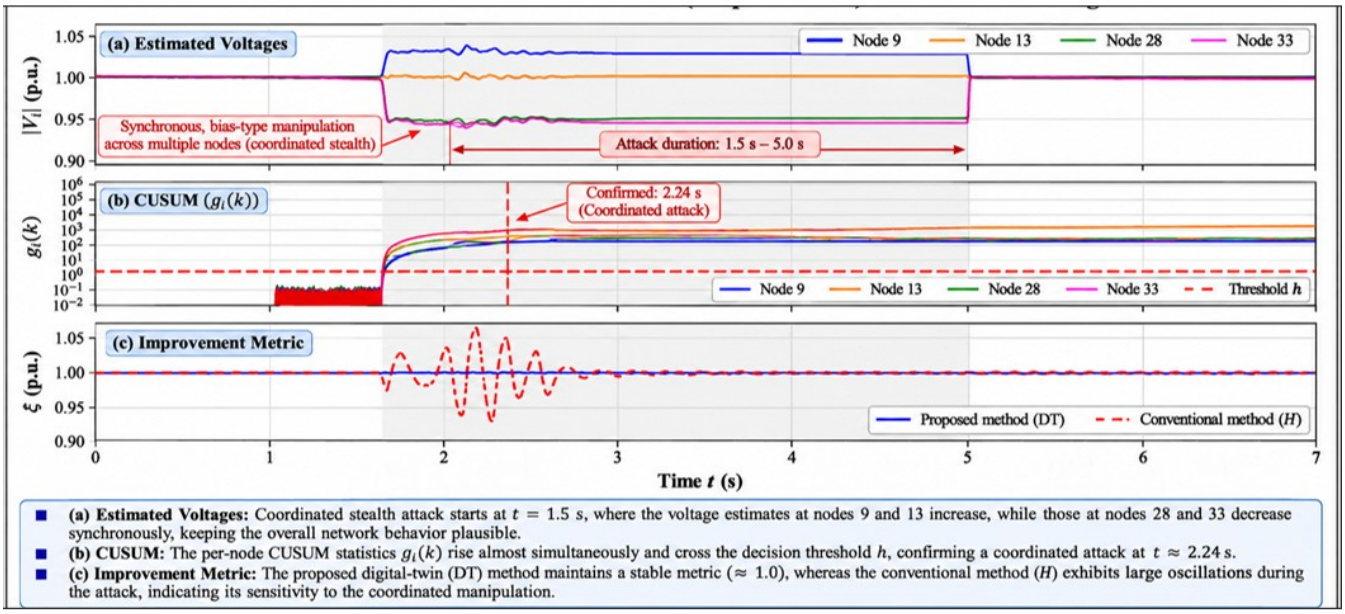

Fig. 3. Detection of the coordinated stealth false-data injection attack using per-node digital twins

Figure 3 illustrates the response of the proposed per-node digital twin-based detection framework under a coordinated stealth false-data injection (FDI) attack in the IEEE 33-bus distribution network. The attack involves simultaneous manipulation of multiple measurement channels to reduce the visibility of malicious deviations in aggregated monitoring indicators. The figure presents three complementary responses: node-specific measurement deviations, cumulative sum (CUSUM) detection statistics, and a comparative monitoring indicator with the proposed method enabled and disabled.

The upper subplot demonstrates the spatial characteristics of the coordinated attack. During the attack interval, the manipulated measurements exhibit deviations of different magnitudes and opposite signs. In particular, the responses associated with nodes 9 and 13 illustrate how coordinated measurement changes can partially cancel when combined into a feeder-level indicator. Consequently, an aggregate monitoring approach may fail to reveal the individual abnormalities even when the underlying measurements have been compromised. By retaining separate residual information for each monitored node, the proposed framework preserves the spatial signatures needed to identify suspicious channels.

C. Coordinated stealth attack

The middle subplot presents the evolution of the node-specific CUSUM detection statistics. Following the introduction of the coordinated attack, the detection statistics increase and exceed the predefined decision threshold, indicating persistent abnormalities in multiple measurement channels. The original simulation result reports attack confirmation at approximately 2.50s, identifying nodes 9 and 13 as the affected locations. This result illustrates the ability of per-node monitoring to reveal coordinated deviations that may be obscured by aggregation.

The lower subplot compares the monitoring response with the proposed method enabled and disabled. The method-disabled response exhibits pronounced fluctuations during the coordinated attack, whereas the method-enabled response remains comparatively stable. This comparison highlights the potential benefit of incorporating node-specific monitoring and verification mechanisms when evaluating coordinated measurement manipulation. However, the plotted indicator should be explicitly defined before its stability is interpreted as a quantitative improvement in voltage regulation or cybersecurity performance.

Overall, the results demonstrate the relevance of spatially resolved digital twin residuals and sequential change detection for identifying coordinated stealth attacks. The simultaneous abnormalities observed across multiple monitored nodes provide evidence for attack localization, while the temporal detection statistics support confirmation of persistent malicious behavior. The findings emphasize the limitations of relying exclusively on aggregated monitoring indicators and motivate the integration of per-node detection, coordinated attack attribution, and trusted measurement recovery.

D. Interpretation and limits

The four reported identification errors are small relative to the 20.00 ms reference. The ramp and coordinated-attack plots show detection behavior in the depicted scenarios, but do not support broad claims of universal detection, guaranteed stealth resistance, or statistically validated superiority. Reproducibility would require the feeder data, sampling rate, twin fitting procedure, attack onset, threshold parameters, noise levels, and independent test runs.

V. CONCLUSION

This paper presented a per-node digital twin-based framework for cyberattack detection, localisation, and attribution in the IEEE 33-bus distribution network. The framework integrates node-specific digital twin modeling, residual analysis, cumulative sum (CUSUM)-based anomaly detection, persistence verification, and measurement recovery to address false-data injection (FDI) and coordinated stealth attacks. Four digital twins associated with buses 9, 13, 28, and 33 were considered to evaluate identification accuracy and cyberattack detection performance. The identification results demonstrated close agreement between the estimated and reference time constants, with estimated values ranging from 19.91 to 19.95ms against a reference of 20.00ms. The relative identification errors remained between 0.25% and 0.45%, with an average error of 0.325%, indicating accurate identification across the monitored nodes. Under the ramp FDI attack at bus 33, the node-specific residuals exhibited a progressive deviation from the expected measurements, enabling identification of the compromised node. The corresponding detection statistics confirmed the ramp attack at approximately 2.52s. Furthermore, the coordinated stealth attack scenario demonstrated the importance of preserving individual nodal information, as oppositely signed measurement deviations could partially cancel in an aggregated monitoring indicator. The per-node detection framework identified suspicious behavior associated with buses 9 and 13, with attack confirmation reported at approximately 2.50 s. These findings highlight the potential of spatially resolved digital twin monitoring to detect gradual and coordinated measurement manipulation while supporting attack localization and attribution. Overall, the presented results establish the feasibility of combining per-node digital twins with sequential anomaly detection for improving cyber-physical monitoring in active distribution networks. Future research should investigate robustness under measurement noise, communication delays, topology changes, and varying attack intensities, together with hardware-in-the-loop validation and quantitative assessment of recovery performance.

REFERENCES

[1] Attack Detection and Mitigation for DC Microgrids," IEEE Trans. Smart Grid, vol. 16, no. 2, pp. 876–889, 2025, doi: 10.1109/TSG.2024.3487049.

[2] S. Thapa, A. Asrari, and M. Saffari, "Enhancing Fault and Cyberattack Detection in Power Systems Using Digital Twin and SVM," in Proc. IEEE Int. Conf. Electro Information Technology (EIT), 2025, pp. 115–119, doi: 10.1109/EIT64391.2025.11103680.

[3] H. Patel, A. K. Bohre, O. Yadav, J. Thakkar, and M. L. Kolhe, "DG, SOP, and EVCS deployment in a distribution system: Multi-scenario analysis using HHO and TLBO," AIMS Energy, vol. 14, no. 2, pp. 358–386, 2026, doi: 10.3934/energy.2026016

[4] "Real-Time Cyber Attack Detection and Response Using Digital Twins in Protection Relays," in Proc. IECON 2024—50th Annual Conf. IEEE Industrial Electronics Society, 2024, doi: 10.1109/IECON55916.2024.10905313.

[5] A. Salehpour and I. S. Al Anbagi, "RTAP: A Real-Time Model for Attack Detection and Prediction in Smart Grid Systems," IEEE Access, vol. 12, pp. 130425–130443, 2024, doi: 10.1109/ACCESS.2024.3458874.

[6] "Joint Detection and Localization of Stealth False Data Injection Attacks in Smart Grids Using Graph Neural Networks," IEEE Trans. Smart Grid, vol. 13, no. 1, pp. 807–819, 2022, doi: 10.1109/TSG.2021.3117977.

[7] A. Takiddin et al., "Generalized Graph Neural Network-Based Detection of False Data Injection Attacks in Smart Grids," IEEE Trans. Emerg. Topics Comput. Intell., vol. 7, no. 3, pp. 618–630, 2023, doi: 10.1109/TETCI.2022.3232821.

[8] "Detection of False Data Injection Attacks in Smart Grid Based on Joint Dynamic and Static State Estimation," IEEE Access, vol. 11, pp. 45028-45038, 2023, doi: 10.1109/ACCESS.2023.3273730.

[9] "Locational Detection of False Data Injection Attacks in Smart Grids: A Graph Convolutional Attention Network Approach," IEEE Internet Things J., vol. 11, no. 6, pp. 9324–9337, 2024, doi: 10.1109/JIOT.2023.3323565.

[10] W. Xia, Y. Li, L. Yu, and D. He, "Locational Detection of False Data Injection Attacks in the Edge Space via Hodge Graph Neural Network for Smart Grids," IEEE Trans. Smart Grid, vol. 15, no. 5, pp. 5102–5114, 2024, doi: 10.1109/TSG.2024.3389948.

[11] "DAMGAT-Based Interpretable Detection of False Data Injection Attacks in Smart Grids," IEEE Trans. Smart Grid, vol. 15, no. 4, pp. 4182–4195, 2024, doi: 10.1109/TSG.2024.3364665.

[12] M. Kesici, B. Pal, and G. Yang, "Detection of False Data Injection Attacks in Distribution Networks: A Vertical Federated Learning Approach," IEEE Trans. Smart Grid, vol. 15, no. 6, pp. 5952–5964, 2024, doi: 10.1109/TSG.2024.3399396.

[13] "Detection of False Data Injection Attacks in Cyber-Physical Power Systems: An Adaptive Adversarial Dual Autoencoder With Graph Representation Learning ApproachY. Lu, M. Zhang, L. Nordström, and Q. Xu, "Digital Twin-Based Cyber-IEEE Trans. Instrum. Meas., vol. 73, Art. no. 9000411, 2024, doi: 10.1109/TIM.2023.3331398.

[14] "False Data Injection Attack Detection Method Based on Deep Learning With Multi-Scale Feature Fusion," IEEE Access, vol. 12, pp. 89262–89274, 2024, doi: 10.1109/ACCESS.2024.3418883.

[15] H. Patel, B. K. Saw, A. K. Bohre, and O. Yadav, "Analyze the impact of distributed generation units on distribution system performances," in Proc. IEEE Int. Conf. Power Electronics, Smart Grid, and Renewable Energy (PESGRE), 2023, doi: 10.1109/PESGRE58662.2023.10404345.

[16] "Tensor-Completion-Enabled Stealthy False Data Injection Attacks on IoT-Based Smart Grid," IEEE Internet Things J., vol. 11, no. 22, pp. 36660–36672, 2024, doi: 10.1109/JIOT.2024.3416839.

[17] M. R. Dehbozorgi, M. Rastegar, and M. F. M. Arani, "A deep learning deviation-based scheme to defend against false data injection attacks in power distribution systems," Electr. Power Syst. Res., vol. 238, Art. no. 111076, 2025, doi: 10.1016/j.epsr.2024.111076.

[18] X. Wang, M. Hu, X. Luo, and X. Guan, "A detection model for false data injection attacks in smart grids based on graph spatial features using temporal convolutional neural networks," Electr. Power Syst. Res., vol. 238, Art. no. 111126, 2025, doi: 10.1016/j.epsr.2024.111126.

[19] H. Patel, A. K. Bohre, and O. Yadav, "Enhancing distribution system performace with concurrent planning of DG and soft open point," in Proc. IEEE North-East India Int. Energy Conversion Conf. Exhibition

(NE-IECCE), 2025, pp. 1–6, doi: 10.1109/NE-IECCE64154.2025.11183424

[20] Y. Wang, Z. Lu, J. Ma, and Q. Jin, "Locational False Data Injection Attack Detection in Smart Grid Using Recursive Variational Graph Autoencoder," IEEE Internet Things J., vol. 12, no. 10, pp. 13697–13708, 2025, doi: 10.1109/JIOT.2025.3526672.

[21] N. Li, J. Zhang, D. M. Ma, and J. Ding, "Enhancing Detection of False Data Injection Attacks in Smart Grid Using Spectral Graph Neural Network," IEEE Trans. Ind. Informat., vol. 21, no. 6, pp. 4543–4553, 2025, doi: 10.1109/TII.2025.3545044.

[22] "False Data Injection Attack Detection and Localization Framework in Power Distribution Systems Using a Novel Ensemble of CNNs and Explainable Artificial Intelligence," IEEE Trans. Ind. Appl., vol. 61, no. 3, pp. 4801–4811, 2025, doi: 10.1109/TIA.2025.3532917.

[23] "Locational Detection of False Data Injection Attacks in Smart Grids: A Cloud-Edge Framework Based on Split Learning," IEEE Trans. Smart Grid, vol. 16, no. 6, pp. 5378–5391, 2025, doi: 10.1109/TSG.2025.3580683.

[24] "Detection and Defense Against Multi-Point False Data Injection Attacks of Load Frequency Control in Smart Grid," IEEE Trans. Smart Grid, vol. 16, no. 5, pp. 4143–4154, 2025, doi: 10.1109/TSG.2025.3578985.

[25] Alankrita, A. Pati, and N. Adhikary, "Detection and mitigation against false data injection attacks using SHT and ANN in distributed control of DC microgrid," Electr. Power Syst. Res., Art. no. 111356, 2025, doi: 10.1016/j.epsr.2024.111356.

[26] H. Patel, A. K. Bohre, O. Yadav, and B. K. Saw, "Enhancing distribution system resiliency through techno-economic planning of DG & SOP using optimization with reconfigurations," IEEE Trans. Ind. Appl., early access, 2026, doi: 10.1109/TIA.2026.367964