ISSN: **3107-6513**

Digital Twin-Based Cyberattack Detection in Active Distribution Networks: A Review

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 integration of distributed generation (DG), renewable energy sources, electric vehicle charging infrastructure, and intelligent control devices has transformed conventional distribution networks into complex cyber-physical systems. Although these advancements improve operational flexibility and efficiency, they also increase vulnerability to cyberattacks, including false data injection (FDI), denial-of-service (DoS), replay, and coordinated attacks. Such attacks can compromise measurement integrity, disrupt state estimation, and adversely affect voltage regulation and overall system reliability. Digital twin (DT) technology has emerged as a promising approach for enhancing cybersecurity by establishing a continuously updated virtual representation of the physical distribution network. This paper presents a comprehensive review of digital twin-based cyberattack detection and resilient voltage regulation strategies in active distribution networks. Various digital twin architectures, including model-based, data-driven, hybrid, and node-level approaches, are examined alongside residual-based detection, cumulative sum (CUSUM) analysis, machine learning, and active watermarking techniques. Furthermore, the integration of cyberattack detection with secure measurement reconstruction and adaptive voltage control mechanisms is discussed to highlight potential approaches to maintaining reliable network operation under compromised conditions. A comparative analysis identifies the strengths, limitations, and practical challenges of existing methods, particularly regarding model uncertainty, measurement observability, communication delays, detection accuracy, and computational complexity. Finally, key research gaps and future directions are identified, emphasising topology-aware detection, uncertainty-conscious digital twin adaptation, and experimentally validated cyber-resilient voltage-control frameworks.

Keywords: Active distribution networks, cyberattack detection, cyber-physical security, digital twin, false data injection, resilient voltage regulation, state estimation, CUSUM, smart grid.

I. INTRODUCTION

Distribution networks were traditionally operated as comparatively passive systems, with limited real-time observability and predominantly one-way power flow. High penetration of photovoltaic generation, electric-vehicle charging, battery storage, and flexible loads is changing this operating model. Voltage conditions can now vary rapidly with local generation and demand, while control decisions increasingly depend on network measurements, communication links, and supervisory software. The existing literature on cyberattack detection, digital twin technology, distribution-system state estimation, and resilient voltage regulation provides a foundation for developing secure and reliable active distribution networks. The relevant studies are reviewed sequentially as follows.

In [1], false data injection attacks against power-system state estimation were investigated. The study demonstrated that carefully constructed malicious measurements can bypass conventional bad-data detection mechanisms and manipulate estimated system states. This work established the importance of developing advanced detection techniques to identify stealthy cyberattacks. In [2], malicious data attacks on smart grids were examined by considering the vulnerability of state estimation to manipulated measurements. The study explored attack strategies and their effects on measurement integrity, highlighting the limitations of conventional residual-based detection methods in the face of coordinated data manipulation.

In [3], the vulnerability of AC state estimation to false data injection attacks was investigated. The research considered nonlinear power-system measurement relationships and demonstrated how attackers could exploit system-model information to compromise state estimation. The findings emphasized the need for physically consistent and robust detection mechanisms. In [4], cybersecurity vulnerabilities in power-system state estimators were analyzed. The study examined how malicious modifications to measurement data could influence estimated operating conditions and investigated the relationship between attack strategies and detection capabilities. The work provided a theoretical foundation for evaluating cyberattack resilience in monitoring systems.

In [5], a detection approach for false data injection attacks targeting DC state estimation was investigated. The study focused on identifying manipulated measurements that could remain undetected by conventional bad-data detection techniques. The findings highlighted the importance of measurement protection and improved monitoring strategies for maintaining estimation reliability. In [6], attack detection and identification in cyber-physical systems were studied using system-theoretic principles. The research examined the conditions under which malicious attacks could be detected and localized through system measurements and dynamic behavior. The findings provided a foundation for model-based anomaly detection and attack identification.

In [7], secure control against replay attacks was investigated. The study examined how previously recorded measurements could be retransmitted to deceive monitoring and control systems. It introduced the concept of using control-system dynamics and active verification to distinguish legitimate

ISSN: **3107-6513**

measurements from replayed information, supporting the development of secure feedback-control mechanisms. In [8], a secure control framework considering resource-limited adversaries was developed. The study investigated the relationship between attacker capabilities, system vulnerabilities, and defensive control strategies. The findings highlighted the importance of incorporating realistic attack constraints into cyber-physical security analysis.

In [9], the digital twin concept was introduced in the context of complex aerospace systems. The study described how a virtual representation of a physical system could support monitoring, prediction, and lifecycle assessment. Although the application was outside electrical distribution networks, the underlying concept provided a foundation for digital twin-based monitoring and predictive analysis. In [10], the state of digital twin technology in industrial applications was reviewed. The study discussed the integration of physical models, operational data, and virtual representations to support monitoring, simulation, and decision-making. The findings highlighted the potential of digital twins to improve system visibility and support intelligent operational management.

In [11], distribution-system state estimation methods were comprehensively reviewed. The study examined estimation techniques, measurement configurations, and challenges associated with limited observability in distribution networks. The findings emphasized the importance of reliable state estimation for monitoring active distribution systems with distributed energy resources. In [12], a composable framework for real-time control of active distribution networks using explicit power setpoints was presented. The study addressed the coordination of distributed resources and the constraints of network operations. The framework provided relevant concepts for designing supervisory voltage-control strategies that coordinate multiple controllable devices.

In [13], distributed Volt/VAr control using photovoltaic inverters was investigated. The study considered the use of local inverter reactive power capabilities to regulate distribution network voltages. The findings highlighted the effectiveness of decentralised voltage-support strategies and their relevance to active distribution systems with high photovoltaic penetration.

In [14], the digital twin concept was examined as a means of addressing unpredictable and undesirable behavior in complex systems. The study discussed the relationship between physical systems and their digital representations, emphasising simulation and system-level understanding. These concepts are relevant to detecting abnormal operating conditions and supporting predictive decision-making.

In [15], digital twin-driven prognostics and health management for complex equipment were investigated. The research discussed integrating operational measurements with virtual models to support equipment condition assessment and predictive maintenance. The study demonstrated the broader applicability of digital twins for condition monitoring and reliability improvement.

In [16], a generalised approach to power-system state estimation was presented. The work discussed mathematical formulations, estimation procedures, and the treatment of measurement errors in electrical networks. These concepts support the development of physically consistent state-estimation models for cyberattack detection.

In [17], a branch-current-based state estimation method for distribution systems was proposed. The method utilized branch-current relationships to estimate distribution-network operating states. The study contributed to the development of estimation techniques suitable for distribution feeders, where measurement availability and network characteristics differ from transmission systems. In [18], a multilevel state estimation framework for smart grids was investigated. The study considered the integration of estimation processes across different network levels to improve system monitoring and information coordination. The findings highlighted the potential benefits of hierarchical estimation architectures for complex and interconnected power networks.

In [19], an adaptive cumulative sum (CUSUM) detection technique was investigated for identifying false data injection attacks in smart grids. The study considered sequential statistical monitoring to identify abnormal measurement behavior. The approach demonstrated the relevance of temporal change-detection techniques for identifying persistent cyber-induced deviations.

In [20], optimal capacitor placement in radial distribution systems was investigated. The study examined the allocation of reactive power compensation devices to improve distribution network operating conditions. The work provided a foundation for voltage-support planning and reactive-power management in radial feeders. In [21], distribution network reconfiguration for power loss reduction and load balancing was investigated. The study examined how changing network switching configurations could improve operating performance while maintaining network constraints. The findings established the importance of topology-aware optimization in distribution-system operation.

In [22], reactive-power control strategies for distributed photovoltaic generators were investigated. The study examined how inverter-interfaced generation could provide reactive-power support to improve voltage regulation. The findings highlighted the potential of distributed inverter control for managing voltage variations in active distribution networks.

In [23], optimal dispatch strategies for photovoltaic inverters in residential distribution systems were developed. The study considered coordinated inverter operation to support network objectives and manage distribution-system constraints. The research demonstrated the importance of optimisation-based control for utilising distributed energy resources in voltage management.

A key research need is the integration of digital twin-based measurement validation, spatially localized cyberattack detection, temporal anomaly analysis, and resilient voltage regulation within a unified framework for active distribution networks. In particular, further investigation is required to determine how node-level digital twins can distinguish malicious measurements from legitimate operating disturbances, how compromised channels can be isolated without significantly reducing observability, and how voltage-control actions can remain safe during detection and recovery.

ISSN: 3107-6513

II. Review Scope And Network Architecture

The literature was organised around four intersecting themes: cyberattack models in distribution systems, DT design for power networks, detection and localisation methods, and mitigation through voltage control. Peer-reviewed surveys and research papers on FDI attacks, distribution-system state estimation, DT integration, and DT-assisted cyber-resilient control were prioritized. The synthesis is thematic rather than a statistical meta-analysis; numerical performance values reported by different papers are not directly comparable because feeder models, attack assumptions, measurement rates, and evaluation metrics differ.

Review methodology: the studies are compared qualitatively by threat model, twin architecture, detection signal, mitigation action, and validation level. Priority is given to peer-reviewed power-system cybersecurity literature and relevant standards. Because search coverage and screening counts were not recorded as a reproducible systematic-review protocol, this paper is a structured narrative review rather than a PRISMA systematic review.

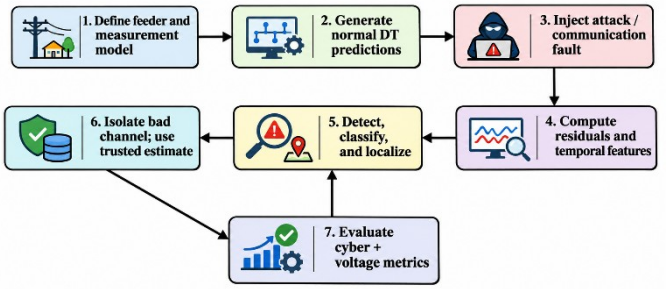

Fig. 1. Review methodology and evaluation workflow

Fig.1 illustrates the systematic workflow for evaluating digital twin (DT)-based cyberattack detection and resilient voltage regulation in active distribution networks. Initially, the distribution feeder and measurement model are defined, followed by the generation of normal operating predictions using the digital twin. Subsequently, cyberattacks or communication faults are introduced to assess system vulnerability. The differences between actual measurements and DT predictions are analyzed using residual and temporal features to detect, classify, and localize potential cyberattacks. Once suspicious measurements are identified, compromised channels are isolated, and trusted state estimates are used to support reliable system operation. Finally, cyber-physical performance is evaluated using detection accuracy, localization capability, and voltage-regulation metrics. The feedback process supports further assessment and refinement of the detection framework under different operating and attack conditions.

III. Cyberattacks And Their Physical Consequences

A. False data injection

An FDI adversary changes a measurement vector from y(k) to $y^a(k)=y(k)+a(k)$, where a(k) is the injected attack vector and k denotes the sample index. The attack may target voltage magnitudes, phase angles, branch flows, nodal injections, or control feedback. A model-aware attacker can select a so-called stealthy vector consistent with the estimator model, thereby weakening conventional residual tests [3], [4]. In distribution networks, limited sensor coverage, uncertain loads, unbalanced operation, and pseudo-measurements complicate the separation of malicious changes from ordinary model error [2].

The additive false-data-injection model is expressed as follows:

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

B. Denial of service and replay

DoS attacks reduce measurement availability by dropping, delaying, or congesting packets. Their impact depends on the control timescale: a short loss may be bridged by a local controller, whereas sustained loss can leave a supervisory controller operating on stale states. Replay attacks reuse previously recorded valid values. Because replayed data may be statistically plausible, detection requires freshness checks, temporal consistency, or a challenge-response signal rather than a static range test alone.

C. Coordinated and stealthy attacks

Coordinated attacks manipulate multiple measurement channels so that local anomalies cancel in an aggregate index or resemble a legitimate operating transition. A detector that compresses many nodal measurements into a single scalar may lose the spatial signature needed to identify the affected buses. Similarity-only tests may also miss a change that preserves the shape of a signal while shifting its magnitude. This does not mean aggregation is always unsafe; rather, aggregate indicators should be supplemented by channel-level residuals and network constraints.

D. From cyber anomaly to voltage risk

A compromised voltage measurement can cause an inverter or regulator to inject or absorb reactive power unnecessarily. Incorrect topology or load data can distort state estimation and Volt–VAR optimization. DoS can delay corrective action, and replay can make a controller respond to a voltage condition that no longer exists. Potential consequences include undervoltage, overvoltage, excess losses, actuator saturation, control oscillation, and reduced operator awareness. Cyber detection should therefore be evaluated against physical outcomes, not classification accuracy alone.

IV. Digital Twin Architectures For Distribution Networks

A. Model-based twin

A model-based DT combines network equations with real-time measurements. For a feeder, a power-flow model predicts bus voltages and branch flows from estimated loads, distributed generation, and control settings. A state estimator reconciles redundant measurements, while parameter adaptation updates uncertain quantities such as load levels or line impedances. Model-based twins are interpretable and can evaluate physically meaningful constraints, but their predictions deteriorate when topology, phase imbalance, inverter controls, or component parameters are represented inaccurately.

ISSN: 3107-6513

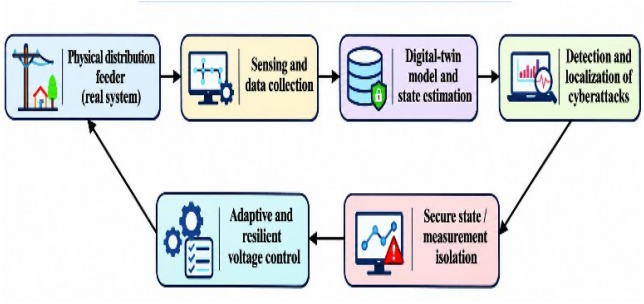

Fig. 2. Closed-loop digital twin cybersecurity architecture

Fig. 2 illustrates the closed-loop digital twin-based cybersecurity architecture for enhancing voltage regulation and operational resilience in active distribution networks. Initially, real-time measurements from the physical distribution feeder are collected through sensing and communication devices and transmitted to the digital twin for network modeling and state estimation. The predicted system states are then compared with received measurements to detect and localize potential cyberattacks. Upon identifying suspicious data, secure measurement isolation and state reconstruction are employed to prevent compromised information from influencing control decisions. Subsequently, adaptive and resilient voltage-control strategies are applied to maintain acceptable voltage conditions and reliable network operation. The resulting control actions are fed back to the physical distribution network, completing the closed-loop process for continuous monitoring, cyberattack detection, mitigation, and voltage regulation.

B. Data-driven and hybrid twins

Data-driven twins use learned mappings, time-series models, or neural networks to predict normal behaviour. They can capture nonlinear dynamics that are difficult to model explicitly, but may fail under operating conditions not present in the training data and may be vulnerable to adversarial inputs. Hybrid twins combine physics-informed constraints with data-driven correction. A practical design should expose uncertainty alongside a point prediction so that a high residual due to model uncertainty is not automatically labelled as malicious.

C. Aggregate twin versus per-node twin bank

An aggregate DT may produce a feeder-level performance index, average voltage error, or global similarity score. It is computationally economical and useful for screening, but spatial aggregation can hide localized or coordinated anomalies. A bank of per-node twins instead produces a vector of local predictions and residuals. This preserves location-specific evidence and supports isolation, but requires more computation, calibration, and channel management. A hierarchical design can use a global twin for network-wide consistency and local twins for detection and localization.
A generic measurement residual is defined as

$$r_i(k) = v_{i,meas}(k) - v_{i,DT}(k), \qquad i = 1, \ldots, N \qquad (2)$$

where $v_{i,meas}$ is the received voltage and $v_{i,DT}$ is the corresponding twin estimate. Residual magnitude alone is insufficient; thresholds should account for noise, load ramps, model uncertainty, and temporal correlation. Normalized residuals, cumulative-sum statistics, temporal derivatives, and cross-node consistency can provide complementary evidence. The twin must also be protected from poisoning; if attacked measurements are blindly fed back into model adaptation, the reference itself may drift toward the compromised state.

$$g_i(k) = \max\{0, g_i(k-1) + |r_i(k)| - \kappa\} \qquad (3)$$

V. Detection, Localization, And Mitigation Methods

A. Residual and state-estimation methods

Residual-based methods compare measurements with state-estimator predictions or physical constraints. They are lightweight and explainable, but their performance depends on measurement redundancy, accurate models, and a suitable threshold. An adversary with sufficient knowledge of the model may construct attacks that lie near the estimator's feasible measurement space. Distribution-system state estimation is additionally affected by sparse instrumentation and pseudo-measurement uncertainty [2]. Consequently, a DT residual should be treated as one evidence stream rather than an infallible attack label.

B. Temporal statistics and change detection

CUSUM and related sequential tests accumulate evidence over time, allowing small persistent deviations to be detected without reacting to every noisy sample. Windowed variance, trend, and change-point tests help distinguish step, ramp, noise-like, and stale-data behaviours. Thresholds must be tuned against realistic load and renewable variability. A fixed threshold that performs well at one operating point may generate false alarms during a legitimate feeder reconfiguration or rapid photovoltaic ramp.

C. Machine learning and hybrid detection

Supervised classifiers can learn attack signatures when representative labelled data are available; unsupervised methods can identify deviations from learned normal behaviour. Sequence models can exploit temporal dependencies, while graph-based models can encode feeder connectivity. However, high test accuracy on a synthetic dataset does not establish robustness to unseen attack strategies, class imbalance, topology changes, or domain shift. Hybrid detectors can combine learned scores with physical residuals, voltage limits, and network constraints to improve interpretability and reduce reliance on a single model family.

D. Active watermarking and data freshness

Watermarking injects a small, known excitation into a control or measurement pathway and checks whether the observed response is consistent with that excitation. It can help distinguish fresh physical feedback from replayed or fabricated data. The signal must be designed to avoid violating voltage quality, actuator limits, or customer constraints. Detection also depends on sufficient excitation, system dynamics, timing accuracy, and the attacker's knowledge. Watermarking should therefore complement-not replace-

ISSN: 3107-6513

residual analysis, secure time-stamping, authentication, and communication monitoring.

E. Detection-triggered resilient voltage regulation

A secure control chain should separate detection from action. First, the system estimates confidence in each measurement; second, suspicious channels are flagged and localized; third, the controller substitutes a trusted estimate or switches to a safe fallback; and fourth, the controller verifies that the physical voltage response is stable before restoring the channel. Candidate actions include local Volt-VAR control, conservative reactive-power limits, topology-aware optimization, actuator saturation, and operation from a last-known-safe state. Automatic isolation must avoid creating an observability gap larger than the attack itself.

A robust implementation uses a supervisory state machine: normal operation, suspected attack, confirmed attack, isolation/reconstruction, and recovery. Hysteresis and minimum dwell times can prevent rapid switching due to noisy residuals. Re-entry should require sustained agreement between the field channel, DT prediction, and independent measurements. Where communication is lost, local inverter controls should preserve essential voltage support without depending on a remote optimizer.

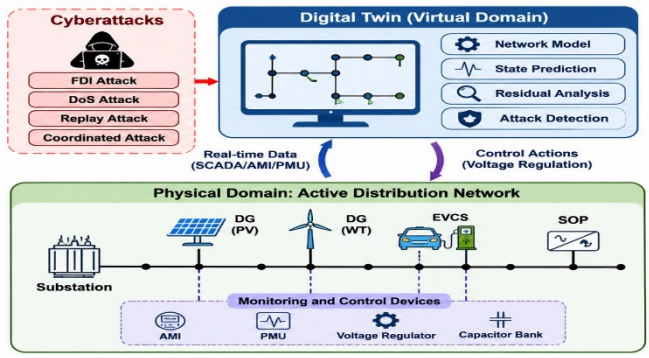

Fig. 3. Overall architecture of digital twin-based cyberattack detection and resilient voltage regulation in active distribution networks

Fig. 3 illustrates the integration of digital twin technology with cyberattack detection and resilient voltage regulation in active distribution networks. The physical network consists of a substation, distributed generation (DG) units, photovoltaic (PV) and wind energy systems, electric vehicle charging stations (EVCS), and soft open points (SOP), supported by advanced metering infrastructure (AMI), phasor measurement units (PMUs), voltage regulators, and capacitor banks. Real-time measurements are transmitted to the digital twin, where network modeling, state prediction, residual analysis, and attack detection are performed. Various cyber threats, including false data injection (FDI), denial-of-service (DoS), replay, and coordinated attacks, are considered. The digital twin compares measured and predicted operating conditions to identify suspicious deviations and support appropriate voltage-control decisions. The resulting control actions are communicated to the physical network, establishing a closed-loop framework for enhancing cybersecurity, voltage stability, and operational resilience.

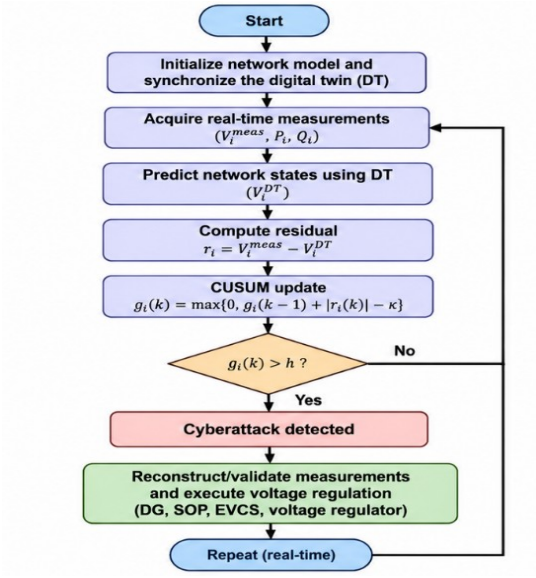

Fig. 4. Flowchart of the digital twin-assisted cyberattack detection and resilient voltage regulation process

Fig.4 illustrates the sequential process of digital twin (DT)-assisted cyberattack detection and resilient voltage regulation in active distribution networks. Initially, the network model is initialized and synchronized with the digital twin, followed by the acquisition of real-time voltage and power measurements. The digital twin predicts network operating states, which are compared with actual measurements to calculate voltage residuals. Subsequently, a cumulative sum (CUSUM) algorithm evaluates the residuals to identify abnormal deviations. When the CUSUM statistic exceeds the predefined threshold, a potential cyberattack is detected, and suspicious measurements are reconstructed or validated to support reliable voltage-control decisions. Appropriate control actions are then applied through distributed generation (DG), soft open points (SOP), electric vehicle charging stations (EVCS), and voltage regulators. If no attack is detected, the monitoring process continues under normal operation. This iterative framework illustrates how cyberattack detection can be integrated with measurement validation and voltage regulation to support continuous monitoring and resilient network operation.

VI. Performance Metrics and Validation

A rigorous evaluation should report both cyber and physical metrics. Cyber metrics include detection rate, precision, recall, false alarm rate, F_1 Score, localization accuracy, and detection latency. Physical metrics include maximum and root-mean-square voltage deviation, number of buses outside permissible limits, active-power losses, reactive-power effort, actuator saturation, and recovery time. Availability-oriented attacks also require tolerance to packet loss and a sufficient stale-data duration. Reporting a single accuracy number can hide a detector that is slow, poorly localized, or operationally disruptive.

The mean absolute voltage-deviation index is defined as:

$$J_v = (1/N) \sum_{i=1}^{N} |V_i - V_{ref}| \quad (4)$$

ISSN: **3107-6513**

Comparisons should use identical feeder models, measurement placements, attack windows, sampling rates, and computational budgets. Normal operating disturbances must be included, such as load changes, photovoltaic ramps, switching events, parameter drift, and sensor noise. Attack cases should cover step, ramp, random/noise-like, replay, DoS, non-additive, and coordinated multi-channel attacks, with explicit assumptions about the attacker's access and the model's knowledge. Ablation studies can quantify the contribution of temporal tests, per-node twins, watermarking, and fallback control.

VII. CONCLUSION

This paper presents a comprehensive review of digital twin-based cyberattack detection and resilient voltage regulation in active distribution networks. Various cyberattack scenarios, including false data injection, denial-of-service, replay attacks, and coordinated attacks, are discussed, along with their potential impacts on network security and voltage stability. The review highlights the effectiveness of digital twin architectures, residual-based detection, CUSUM analysis, machine learning, and active watermarking as complementary approaches for identifying cyber threats. Furthermore, integrating attack detection with secure measurement reconstruction and adaptive voltage control offers a promising strategy for improving system resilience. However, challenges related to model uncertainty, communication delays, measurement observability, and computational complexity remain. Future research should focus on developing robust, topology-aware, and computationally efficient digital twin frameworks, supported by realistic simulations and hardware-in-the-loop validation, to enhance the cybersecurity, voltage stability, and reliability of future active distribution networks.

REFERENCES

[1] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” ACM Transactions on Information and System Security, vol. 14, no. 1, Art. 13, 2011. DOI: 10.1145/1952982.1952995.

[2] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Malicious data attacks on the smart grid,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 645–658, 2011.

[3] 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, no. 3, pp. 1362–1370, 2012.

[4] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, “Cyber security analysis of state estimators in electric power systems,” in Proc. IEEE CDC, 2010.

[5] R. B. Bobba et al., “Detecting false data injection attacks on DC state estimation,” in Proc. First Workshop Secure Control Systems, 2010.

[6] F. Pasqualetti, F. Dörfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715–2729, 2013.

[7] Y. Mo and B. Sinopoli, “Secure control against replay attacks,” in Proc. 47th Annual Allerton Conference on Communication, Control, and Computing, 2009.

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

[9] E. Glaessgen and D. Stargel, “The digital twin paradigm for future NASA and U.S. Air Force vehicles,” in Proc. AIAA Structures, Structural Dynamics, and Materials Conference, 2012.

[10] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, “Digital twin in industry: State-of-the-art,” IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2405–2415, 2019.

[11] A. Anggoro Primadianto and C.-N. Lu, “A review on distribution system state estimation,” IEEE Transactions on Power Systems, vol. 32, no. 5, pp. 3875–3883, 2017. DOI: 10.1109/TPWRS.2016.2632156.

[12] A. Bernstein, L. Reyes-Chamorro, J.-Y. Le Boudec, and M. Paolone, “A composable method for real-time control of active distribution networks with explicit power setpoints. Part I: Framework,” Electric Power Systems Research, vol. 125, pp. 254–264, 2015.

[13] P. Jahangiri and D. C. Aliprantis, “Distributed Volt/VAr control by PV inverters,” IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 3429–3439, 2013.

[14] M. Grieves and J. Vickers, “Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems,” in Transdisciplinary Perspectives on Complex Systems, Springer, 2017.

[15] F. Tao, M. Zhang, Y. Liu, and A. Y. C. Nee, “Digital twin driven prognostics and health management for complex equipment,” CIRP Annals, vol. 67, no. 1, pp. 169–172, 2018.

[16] A. Monticelli, State Estimation in Electric Power Systems: A Generalized Approach. Springer, 1999.

[17] M. Baran and A. W. Kelley, “A branch-current-based state estimation method for distribution systems,” IEEE Transactions on Power Systems, vol. 10, no. 1, pp. 483–491, 1995.

[18] A. Gómez-Expósito, A. Abur, A. de la Villa Jaén, and C. Gómez-Quiles, “A multilevel state estimation paradigm for smart grids,” Proceedings of the IEEE, vol. 99, no. 6, pp. 952–976, 2011.

[19] Y. Huang, H. Li, K. A. Campbell, and Z. Han, “Defending false data injection attack on smart grid network using adaptive CUSUM test,” in Proc. Annual Conference on Information Sciences and Systems, 2011.

[20] M. E. Baran and F. F. Wu, “Optimal capacitor placement on radial distribution systems,” IEEE Transactions on Power Delivery, vol. 4, no. 1, pp. 725-734, 198

[21] M. E. Baran and F. F. Wu, “Network reconfiguration in distribution systems for loss reduction and load balancing,” IEEE Transactions on Power Delivery, vol. 4, no. 2, pp. 1401–1407, 1989.

[22] K. Turitsyn, P. Šulc, S. Backhaus, and M. Chertkov, “Options for control of reactive power by distributed photovoltaic generators,” Proceedings of the IEEE, vol. 99, no. 6, pp. 1063–1073, 2011.

[23] E. Dall'Anese, S. V. Dhople, and G. B. Giannakis, “Optimal dispatch of photovoltaic inverters in residential distribution systems,” IEEE Transactions on Sustainable Energy, vol. 5, no. 2, pp. 487–497, 2014.