Bridging Network Forensics and Kirchhoff Residuals for Stealthy GOOSE Attacks Detection

Muhammad Nasar1, 2, a) and János Csatár1, b)

1Department of Electric Power Engineering, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Műegyetem rkp. 3., H-1111 Budapest, Hungary.   
 2Department of Electrical Engineering, Faculty of Engineering, University of Muhammadiyah Malang, Jl. Raya Tlogomas 246 Malang 65144, Indonesia.

a) Corresponding author: muhammad.nasar@edu.bme.hu  
b) csatar.janos@vik.bme.hu

**Abstract.** This paper introduces a hybrid defense framework that integrates Network Forensics and Kirchhoff residuals to detect subtle attacks in IEC 61850 GOOSE messages. Conventional approaches--both packet-based anomaly detection and physics residual analysis--have their own limitations, allowing synchronized or physics-compliant attacks to escape detection. This hybrid method combines the advantages of both: Network Forensics detects timing and sequence mismatches, while Kirchhoff residuals identify violations of physics laws in electrical systems. Evaluation through analytical scenarios, including replay attacks with modified sequences, demonstrates that this collaborative approach is capable of uncovering hidden manipulations undetected by single method. A predicate-based decision matrix is used to formalize the detection coverage, and complexity analysis shows that both Dynamic Bayesian Network (DBN) updates *(O(|E|))* and residual computations *(O(n))* are computationally light, with residuals requiring only about half the cost of DBN. These findings support the feasibility of real-time implementations below the 4 ms limit of IEC 61850, as well as opening up opportunities for implementing hybrid cyber-physical defenses in more advanced substation protections.

**Keyword**. Cyber-physical power systems, GOOSE stealthy attack, IEC 61850 forensics, substation protection communication

# Introduction

IEC 61850 Generic Object-Oriented Substation Event (GOOSE) messaging is a digital substation standard designed for protection and control actions with strict end-to-end delivery times of 4 ms or less[1]. It achieves ultra-low latency and minimal overhead to support critical operations like breaker tripping, interlocking, and rapid topology changes. These features have led to widespread adoption across high-medium voltage (HV/MV) networks and complex microgrids. However, its performance-focused design--especially the limited use of cryptographic safeguards--makes it vulnerable to adversarial manipulation[2].

The absence of strong authentication and encryption mechanisms makes GOOSE susceptible to a range of cyber-physical threats, including false trip commands, blocking of legitimate protection signals, replay of outdated messages, and coordinated manipulations across multiple Intelligent Electronic Devices (IEDs)[3]. Sophisticated adversaries can launch stealth attacks that maintain short-term Kirchhoff consistency, which preserve electrical plausibility while evading detection by conventional physics-based monitoring systems.

GOOSE security measures offer complementary but incomplete protection[3]. Network-based methods detect malformed or misordered packets but cannot assess physical plausibility. Physics-based approaches using Kirchhoff’s Current and Voltage Law (KCL/KVL) residuals catch inconsistent states, yet miss stealthy attacks that maintain plausible residuals while issuing malicious commands[4], [5]. Crucially, no existing solution unifies cyber events and physical responses into a coherent, causally linked detection framework.

To address this gap, this paper proposes a Hybrid Cyber-Physical Causal Framework that fuses network forensics with Kirchhoff residual analysis in a unified, real-time model. Cyber events and physical states are mapped as nodes in a causal graph enriched with physics-informed priors. Temporal constraints enforce expected timing between commands and responses, enabling detection of subtle inconsistencies even with low residuals. Analytical validation confirms the framework meets IEC 61850 requirements for detection, latency, and coverage.

The remainder of this paper is organized as follows. Section 2 reviews existing network-based and physics-based GOOSE defense mechanisms and identifies the unresolved gaps motivating this work. Section 3 details the proposed hybrid causal framework, including its representation, feature set, and causal reasoning process. Section 4 presents an analytical assessment of its feasibility, detection coverage, and timing performance. Finally, Section 5 concludes the paper.

# related work and research gap

Research on IEC 61850 GOOSE security has split between network anomaly detection and physics-based validation. Each effective but insufficient alone against stealthy attacks that mimic normal traffic and preserve short-term plausibility. Network forensics, defined here as protocol-aware, causality-driven analysis, has remained disconnected from real-time physical reasoning. This section reviews both domains, highlights the missing cyber-physical linkage, and introduces a hybrid framework that unifies them within GOOSE’s sub-4 ms constraint.

## Network-Based Defenses for IEC 61850 GOOSE

Network-based defenses for GOOSE messaging operate entirely on the communication layer, analyzing packet structure, timing, and protocol compliance without referencing the power system’s physical state[6]. In this study, we group these methods under network forensics, defined as the protocol-aware, causality-driven analysis of network traffic to reconstruct events for security and operational assurance. Within IEC 61850, network forensics seeks to detect cyber anomalies before they trigger harmful control or protection actions[7], [8]. These approaches leverage GOOSE’s distinctive communication traits (multicast Ethernet, sub-4 ms timing, and ASN.1/BER encoding) to extract signatures and identify anomalies.

One common adopted strategy is packet structure validation, where GOOSE frames are inspected for syntactic correctness. Prior works [6], [9], [10], [11], [12] utilize ASN.1 BER encoding, field lengths, VLAN tags, and multicast addressing rules to verify GOOSE messages. Such methods are highly efficient in detecting malformed or rogue packets and incur negligible latency, making them compatible with the 4 ms protection requirement. However, they are inherently incapable of identifying adversaries who manipulate payload values while still conforming to all encoding and protocol rules.

A second line of research leverages sequence and state tracking [13]. Because GOOSE employs monotonically increasing state numbers (stNum) and sequence numbers (sqNum), monitoring their evolution over time enables detection of replayed packets, stale commands, or denial-of-service (DoS) attempts through abnormal retransmission rates. Replayed trip signals [14], [15] can often be identified by observing inconsistencies in state progression. Nonetheless, this approach presumes that the attacker fails to synchronize counters correctly; sophisticated adversaries can craft packets with consistent counters and thus remain undetected.

Beyond structural validation, timing and traffic analysis [16], [17] has been applied to detect anomalies at the flow level. These methods examine inter-arrival times, traffic bursts, entropy of flows, or other statistical descriptors of the packet stream. Sudden bursts of GOOSE frames, as observed during flooding or broadcast amplification attacks, can therefore be recognized with high accuracy. While scalable to large substation networks, these techniques remain blind to low-rate, stealthy payload manipulations that mimic nominal traffic dynamics.

A fourth category adapts signature- and rule-based intrusion detection systems (IDS) with IEC 61850-specific patterns[18], [19], [20]. These provide operational solutions as they integrate seamlessly into existing IDS deployments. Nevertheless, their reliance on predefined signatures renders them effective only against previously documented attack vectors, leaving zero-day or stealth variants largely invisible.

Finally, recent studies have investigated statistical and machine learning (ML) classifiers for GOOSE anomaly detection. By training on features such as packet size distributions, inter-packet timing, and flag combinations, both supervised and unsupervised models have shown promise in learning subtle deviations from baseline traffic[7], [21], [22], [23]. While these approaches extend detection capabilities beyond rigid signatures, they remain data-driven and subject to limitations of training coverage, model drift, and adversarial adaptation. Importantly, like all network-only defenses, they cannot reason about the semantic validity of payload commands relative to the physical system state.

## Residual-Based Defenses for IEC 61850 GOOSE

In parallel to purely cyber-layer defenses, several studies have investigated residual detection, which exploits the laws of electrical grid physics to identify attacks[24], [25]. Residual-based methods differ from network forensics by validating cyber events through Kirchhoff’s laws in power systems. In a consistent grid, current and voltage measurements must obey KCL and KVL; any violation from tampered data creates detectable residuals for real-time monitoring.

The common implementation is through model-based state estimation, where a redundancy of measurements is leveraged to estimate the expected electrical state and compute deviations[24], [26], [27], [28]. For example, when breaker commands in GOOSE are inconsistent with sampled values (SV) or phasor measurements (PMU), the resulting mismatch in current injections at a bus yields a nonzero KCL residual. Such discrepancies can reveal cyber-physical manipulations even if the packet itself appears structurally correct at the network level.

Extensions of this approach apply incidence matrix formulations, where topology and connectivity constraints are explicitly encoded in a matrix representation of the grid[5], [29]. Incoming measurements--whether currents, voltages, or breaker states--are then projected onto this topology, and violations manifest as residual vectors orthogonal to the physical laws. These methods are attractive because they allow scalable computation and can be updated dynamically as topology changes occur.

Residual-based detection has also been implemented in real-time protection testbeds, where SV streams and GOOSE events are continuously validated against Kirchhoff constraints. Several studies demonstrate that even under fast fault-clearing conditions (≤4 ms), residual checks can identify injected false trip or block commands that are inconsistent with the simultaneous flow of current and voltage in the monitored circuit[24], [30]. This line of work highlights the feasibility of enforcing cyber-physical consistency as a lightweight alternative to cryptographic integrity.

However, the literature also indicates inherent limitations of residual-only approaches. First, their effectiveness depends on measurement redundancy and accuracy; noise or missing data can mask or mimic residuals[5]. Second, sophisticated adversaries may craft stealthy attacks that remain topology-consistent, such as coordinated manipulations of both breaker commands and sampled values, thereby preserving Kirchhoff residuals within tolerance thresholds for short time windows[30]. For example, if a forged trip signal is paired with falsified SV measurements, the residuals may remain near zero despite an ongoing attack. Third, computational latency grows with system size and complexity, raising concerns about scalability to large substations with dense monitoring infrastructures[31]. Table 1 summarizes this landscape.

**TABLE 1.** Summary of Residual-Based Defenses for IEC 61850 GOOSE

|  |  |  |  |
| --- | --- | --- | --- |
| **Approach / Reference** | **Core Method** | **Strengths** | **Limitations** |
| **State Estimation Residuals** (PMU- or SCADA-based) | Use redundant measurements and power flow equations to compute residuals between estimated and observed states | Physically grounded; detects measurement tampering or device failures | Computationally intensive; not suitable for ≤4 ms GOOSE protection; depends on measurement redundancy |
| **Incidence Matrix Validation** | Apply Kirchhoff’s Current/Voltage Law (KCL/KVL) over substation topology; mismatch = anomaly | Lightweight, mathematically rigorous; topology-aware | Cannot detect coordinated attacks that remain Kirchhoff-consistent (e.g., false trip + falsified currents) |
| **Model-Based Residual Monitoring** | Compare real-time measurements with physics-based digital twin or dynamic model | Captures transient inconsistencies; good for wide-area monitoring | Requires accurate models and parameter tuning; high latency in practice |
| **Hybrid PMU-GOOSE Validation** | Cross-check GOOSE breaker status with SV/PMU currents and voltages | Detects false trips/blocks by mapping cyber commands to physical effects | Depends on synchronized high-resolution SV/PMU data; added complexity; vulnerable to multi-point stealthy attacks |

In summary, residual defenses uncover attacks that elude network analysis, particularly protocol-based manipulation. However, on their own, these approaches are vulnerable to coordinated manipulation that keeps the residuals hidden. This observation motivates a hybrid paradigm, where residual checks are fused with network-layer forensic signals to establish causal links between cyber anomalies and their physical plausibility, thereby closing the blind spots of each individual approach.

# methods

This section describes a hybrid causal framework that combines network forensics and Kirchhoff residual validation for real-time defense against stealthy GOOSE attacks. Unlike methods that separate cyber and physical analysis, this approach uses a causal graph to link network anomalies to electrical system responses.

## Concept Overview

The system is modeled as a multiplex causal graph with two tightly coupled layers:

* **Cyber Layer (C-layer):** encapsulates GOOSE packet features such as inter-arrival time, sequence counters, retransmission patterns, VLAN priority, and quality/test flags. This layer enforces protocol causality, i.e., the legitimate evolution of dataset updates governed by sqNum and stNum.
* **Physical Layer (P-layer):** represents breaker/disconnector states, currents, voltages, and Kirchhoff residuals. This layer enforces physics causality, i.e., that any commanded topology change must be accompanied by consistent flows obeying KCL/KVL.

The hybrid framework operates by checking whether both layers satisfy their predicates simultaneously. If not, the system enters a detection region. Figure 1 illustrates the architecture.

|  |  |
| --- | --- |
|  |  |
| 1. High level view | 1. Detailed architecture |

**Figure 1.** The Proposed Architecture of GOOSE Stealthy Attacks Detection

## Causal Relationships Construction

The logical design of the proposed causal hybrid framework centers on detecting stealthy GOOSE payload manipulations that evade both traditional network defenses and physics-only residual checks. Causal mappings are defined as:

…(1)

where *C* denotes a cyber command, *B* the resulting breaker action, and *P* the observed physical parameter shift. To achieve this, we establish causal invariants that anchor cyber actions to their physical consequences:

* Delay bounds: A cyber-to-physical edge must respect relay and trip timings, denoted by *τmin ≤ τC → P ≤ τmax*.
* Physics constraints: Each *P* is bound by KCL/KVL invariants, formally represented as residual norms ‖r‖≤ϵ.

An adversary-induced mismatch (e.g., a breaker opens without a corresponding causal cyber trigger, or with flows inconsistent with KCL) constitutes a predicate violation. Thus, the causal graph provides the formal proof for validating consistency.

## Features Selection

The sensitivity of the proposed causal detection relies on extracting measurable and discriminative features from both the cyber and the physical power-system layer. Features are selected not by heuristics, but for their alignment with predicates of causal validity:

* Cyber predicates: inter-arrival distributions, burst entropy, counter increments (ΔsqNum, ΔstNum), VLAN PCP stability, MAC identity persistence, dataset length constancy, and quality/test flag evolution.
* Physical predicates: residual norms (‖rI‖1, ‖rV‖1), power flow rebalancing, breaker-induced topology shifts, and imbalance indices.

These features collectively define the predicate regions used in an analytic detection landscape: if cyber and physical predicates both hold *(Pf ∧ Pr),* the system remains benign; otherwise, detection is triggered.

## Violation Indicators

The proposed framework operationalizes detection through the concept of causal violation indicators, which signal departures from the expected alignment between cyber-layer events and physical-layer responses. It detects adversaries by proving the presence of causal violations, expressed as:

* Timing violations: observed delay τ∉[τmin, τmax].
* Order violations: physical change (*P*) occurs before cyber command (*C*).
* Counterfactual mismatch: predicted physical state under a legitimate *C* differs from observed *P*:

…(2)

These indicators correspond to predicate partitions that map attacks to detection zones based on violated conditions. They enable identification of stealth-consistent manipulations by integrating cyber and physical data into a unified filter--unlike packet-level or residual-only methods. Table 2 illustrates how timing, order, and counterfactual mismatches act as systematic cues to uncover stealthy GOOSE attacks.

**TABLE 2.** Violation Indicators for Stealthy GOOSE Attack Detection

|  |  |  |
| --- | --- | --- |
| **Violation Type** | **Violation Type** | **Attack Type Exposed** |
| Timing Violation | Physical response occurs outside [τmin, τmax] window after GOOSE trigger | Delayed injection, anticipatory/pre-emptive manipulation |
| Order Violation | Physical change observed **before** corresponding cyber-layer command | Pre-emptive actuation, forged replay simulating legitimacy |
| Counterfactual Mismatch | Observed physical state ≠ predicted trajectory under legitimate command | Subtle falsification that preserves plausibility at packet-level but violates physics. |

## Latency Considerations

The architecture is strict to the 4 ms IEC 61850 timing requirement. To ensure feasibility, each functional component of the architecture has been profiled in terms of computational latency. Cyber-layer feature extraction, when implemented using high-performance packet processing frameworks such as DPDK (Data Plane Development Kit) and eBPF (extended Berkeley Packet Filter), completes in approximately ≤0.1 ms[32], [33]. Physical-layer residual computation, formulated as sparse matrix operations over the incidence structure, similarly requires ≤0.1 ms[34]. The dominant cost arises in the causal consistency check, executed as a lightweight update of a linear Dynamic Bayesian Network (DBN), which completes in ≤0.5 ms[35]. The full pipeline remains within 1-2 ms.

## Evaluation Scenario

Detection outcomes are formalized using the cyber-layer predicate *(Pf)* and physical-layer predicate (*Pr*), which capture forensic and residual consistency, respectively. Attacks are classified as: physics-consistent false trips (*Pf ∧ ¬Pr*), replay with resequenced counters *(¬Pf ∧ Pr*), coordinated multi-breaker manipulations *(¬Pf ∧ ¬Pr*), and stealthy low-magnitude injections *(Pf ∧ Pr).* For clarity, we define these functions as follow:

* Physics-consistent false trips: Passes cyber checks (*Pf)* but breaks KCL residuals *(¬Pr).*
* Resequenced replay: Passes residuals *(Pr)* but fails forensic checks *(¬Pf).*
* Multi-breaker manipulation: Fails both layers *(¬Pf ∧ ¬Pr).*
* Stealth injection: Stays within residual and cyber limits *(Pf ∧ Pr),* entering the stealth zone.

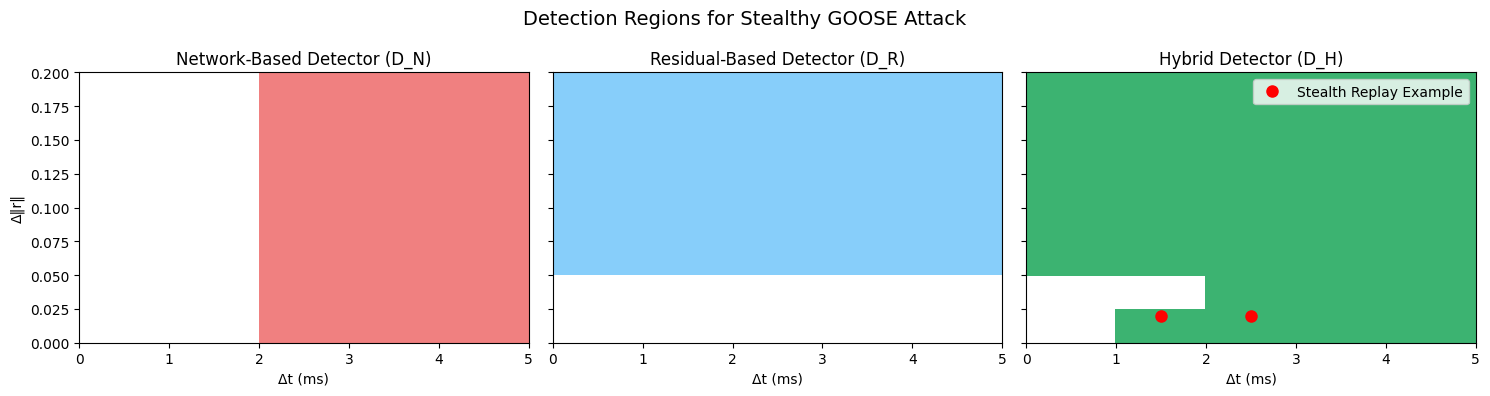
To evaluate the framework, we consider a replay scenario where an adversary captures a valid GOOSE stream and replays it with modified sqNum/stNum counters. The replay is done by injecting these packets with resequenced counters, and formally simulated by aligning them with breaker state changes. At the network level, packets should remain valid, but counter monotonicity is violated *(¬Pf).* At the physical level, breaker-current relationships should also remain consistent, keeping residuals within tolerance *(Pr).* Only the combined framework localizes the attack in the forensics-only detection region. This scenario emphasizes the complementarity of network and residual defenses: network-only methods miss physics-consistent false trips, while Kirchhoff-only methods overlook resequenced replays. The hybrid approach captures both.

# result

This section analyzes the feasibility of the proposed causal hybrid framework by formally evaluating its detection capability and computational efficiency. Each subsection corresponds to a distinct analytical construct, with results visualized in the accompanying figures.

## Detectability of Stealthy GOOSE Replay Attacks

Having the scenario executed, Figure 2 illustrates the comparative detection regions for three distinct defense strategies: a network-based detector *DN*, a residual-based detector *DR*, and their hybrid composition *DH*. The horizontal axis (Δt) represents deviations in packet timing relative to nominal inter-arrival expectations, while the vertical axis (Δ∥r∥) quantifies residual deviations from Kirchhoff consistency, expressed in per-unit.

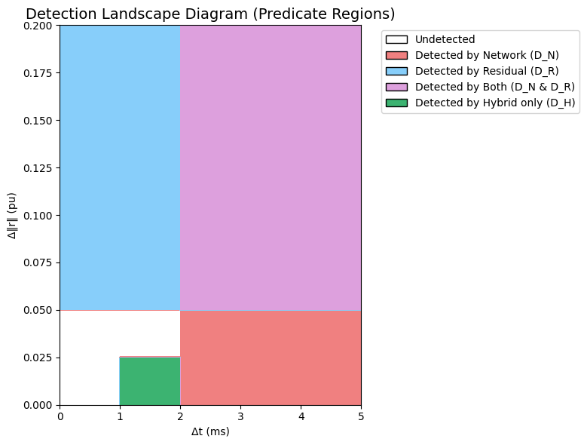


**Figure 2.** Detection Regions for Stealthy GOOSE Attack

The first panel shows that network-only detection triggers alarms only when timing deviations exceed 2 ms, missing attacks with resequenced messages within acceptable delays. The second panel reveals that residual-only detection flags violations of physics consistency (δ = 0.05 pu) but overlooks replayed commands that maintain valid electrical states. The third illustrates the hybrid approach, which combines timing and residual checks with a causal-mismatch rule to detect stealthy replays--those with low residuals and suspicious timing (1-3 ms). Only the hybrid method *(DH)* identifies these anomalies, as shown by the red markers. This reveals a key insight: detecting stealthy GOOSE attacks requires jointly analyzing network and physics constraints through a causal framework. The hybrid detector not only covers what individual methods do but also extends detection into stealth attack zones, offering broader protection without added computational cost.

## Detection Coverage

To evaluate the relative effectiveness of individual and collaborative detection, we map the logic to two key parameters: time deviation (Δt) and residual deviation (Δ‖r‖). Figure 3 shows the detection landscape divided into four zones: network-based detection (coral) that triggers an alarm when the time deviation exceeds a threshold ε even if the physical system remains consistent; residual-based detection (blue) that identifies current-voltage mismatches even if the delivery time is normal; combined detection (purple) that triggers alarms from both mechanisms simultaneously; and a hybrid-exclusive zone (green) that is detected only by the collaborative approach through causal analysis.



**Figure 3.** The Detection Landscape Diagram (Predicate Region)

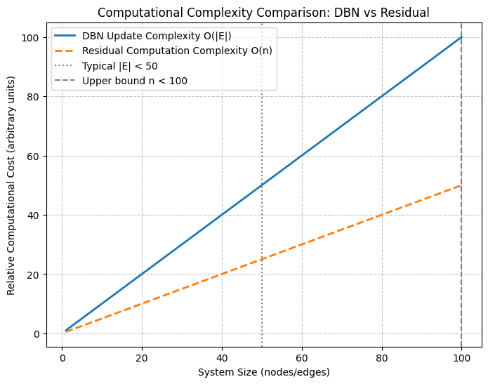
This green zone is the most important finding because it uncovers stealthy replay attacks designed to stay within the tolerances of ε and δ, such as GOOSE packets reordered in the 1-3ms range with low residuals. This hybrid approach enables the detection of hidden manipulations that are unreachable by traditional methods, significantly expanding the defense coverage without relying on the additive contributions of individual detectors.

## Computational Complexity

The framework introduces two primary sources of computational cost: the update of the Dynamic Bayesian Network (DBN), and the computation of Kirchhoff residual. In DBN, each update requires a traversal of the graph edges, leading to a complexity of *O(|E|),* where *|E|* denotes the number of edges. In typical substation models, |*E|* remains well below 50, ensuring that the update cost per step is relatively minor to the 4 ms operational constraint of IEC 61850. As shown in Figure 4, the DBN curve increases linearly with system size, but remains modest for typical operational bounds (|*E|*<50). We express this as:

…(3)

where *NIED* is the number of IED, *b* is the maximum number of links per IED, *Nbrk* is the number of breakers, and *ccorr* captures additional correlations. To illustrate, with *NIED*=10 and *Nbrk*=12, we obtain *|E|≤*43, which aligns with the gray dotted boundary in Figure 4 and marks the realistic substation configuration (*|E|<*50). Within this region, the DBN curve remains shallow, confirming that inference costs are reasonable for the 4 ms operational budget.



**Figure 4.** Computational Complexity Analysis: DBN vs Residual

In residual, the evaluation is performed via sparse summations of incidence or loop matrices, scaling as *O(n),* where *n* is the number of nodes or buses. In Figure 4, the residual curve (dashed line) exhibits the same linear slope as the DBN but lies consistently below it by approximately 50%, indicating a smaller constant factor. For instance, with *n*=100, residual computation requires at most 200 summations (*n⋅b*, with *b*=2), corresponding to only 0.002 ms on a modest CPU --well within the 4 ms GOOSE update window.

# Conclusion

This study proposes a hybrid framework combining Network Forensics and Kirchhoff residuals to enhance the security of IEC 61850 GOOSE messages. This approach can detect cyber-physical stealth attacks that escape traditional methods, such as reordered replays and false trips while remaining physically consistent. Analysis shows that Dynamic Bayesian Network updates and residual computation are lightweight, with processing times below 4ms and cost efficiency up to 50%. These findings demonstrate that the hybrid approach is capable of expanding the detection scope without sacrificing performance.

# References

[1] IEC, “IEC 61850‑8‑1, Communication networks and systems in substations – Part 8‑1: GOOSE.”

[2] H. T. Reda *et al.*, “Vulnerability and Impact Analysis of the IEC 61850 GOOSE Protocol in the Smart Grid,” *Sensors*, vol. 21, no. 4, p. 1554, Feb. 2021, doi: 10.3390/s21041554.

[3] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, “A Method for Achieving Confidentiality and Integrity in IEC 61850 GOOSE Messages,” *IEEE Trans. Power Delivery*, vol. 35, no. 5, pp. 2565–2567, Oct. 2020, doi: 10.1109/TPWRD.2020.2990760.

[4] R. Macwan *et al.*, “Collaborative defense against data injection attack in IEC61850 based smart substations,” in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, USA: IEEE, Jul. 2016, pp. 1–5. doi: 10.1109/PESGM.2016.7741376.

[5] A. Valdes, C. Hang, P. Panumpabi, N. Vaidya, C. Drew, and D. Ischenko, “Design and simulation of fast substation protection in IEC 61850 environments,” in *2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Seattle, WA, USA: IEEE, Apr. 2015, pp. 1–6. doi: 10.1109/MSCPES.2015.7115402.

[6] Carl Krige, Shaheen Behardien, and John-Charly Retonda-Modiya, “A Detailed Analysis of the GOOSE Message Structure in an IEC 61850 Standard-Based Substation Automation System,” *INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL*, Aug. 2013.

[7] H. Nhung-Nguyen, M. Girdhar, Y.-H. Kim, and J. Hong, “Machine-Learning-Based Anomaly Detection for GOOSE in Digital Substations,” *Energies*, vol. 17, no. 15, p. 3745, Jul. 2024, doi: 10.3390/en17153745.

[8] G. Elbez, K. Nahrstedt, and V. Hagenmeyer, “Early Attack Detection for Securing GOOSE Network Traffic,” *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 899–910, Jan. 2024, doi: 10.1109/TSG.2023.3272749.

[9] M. T. A. Rashid, S. Yussof, and Y. Yusoff, “Trust System Architecture for Securing GOOSE Communication in IEC 61850 Substation Network,” *IJSIA*, vol. 10, no. 4, pp. 289–302, Apr. 2016, doi: 10.14257/ijsia.2016.10.4.27.

[10] V. K. Singh, A. S. Thoke, and C. P. Awasthi, “Procedures for testing control and protection scheme based on GOOSE messages-methodology and constraints from engineering perspective,” in *2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES)*, Delhi, India: IEEE, Jul. 2016, pp. 1–5. doi: 10.1109/ICPEICES.2016.7853201.

[11] M. Rodriguez, J. Lazaro, U. Bidarte, J. Jimenez, and A. Astarloa, “A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems,” *IEEE Access*, vol. 9, pp. 51646–51658, 2021, doi: 10.1109/ACCESS.2021.3069088.

[12] W. Huang, “A Practical Guide of Troubleshooting IEC 61850 GOOSE Communication,” in *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, Denver, CO: IEEE, Apr. 2018, pp. 1–6. doi: 10.1109/TDC.2018.8440522.

[13] S. Hussain *et al.*, “A novel hybrid methodology to secure GOOSE messages against cyberattacks in smart grids,” *Sci Rep*, vol. 13, no. 1, p. 1857, Feb. 2023, doi: 10.1038/s41598-022-27157-z.

[14] T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, “A Novel Approach for Mitigation of Replay and Masquerade Attacks in Smartgrids Using IEC 61850 Standard,” *IEEE Access*, vol. 7, pp. 156044–156053, 2019, doi: 10.1109/ACCESS.2019.2948117.

[15] M. Bouslimani, F. B.-S. Tayeb, Y. Amirat, and M. Benbouzid, “Replay Attacks on Smart Grids: A Comprehensive Review on Countermeasures,” in *IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society*, Chicago, IL, USA: IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/IECON55916.2024.10905194.

[16] Tasmi, D. Stiawan, B. Y. Suprapto, H. Setiawan, and M. A. S. Arifin, “Introduction to GOOSE Data Communication Attack Traffic Pattern in IEC 61850,” in *2024 11th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Yogyakarta, Indonesia: IEEE, Sep. 2024, pp. 256–261. doi: 10.1109/EECSI63442.2024.10776142.

[17] M. Jover, A. Ballesteros, M. Barranco, and J. Proenza, “Mapping IEC 61850 GOOSE Messages into Time-Sensitive Networking,” in *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)*, Padova, Italy: IEEE, Sep. 2024, pp. 1–4. doi: 10.1109/ETFA61755.2024.10711096.

[18] S. M. S. Hussain, Mohd. A. Aftab, S. M. Farooq, A. Latif, C. Konstantinou, and M. A. Abido, “A Public key Based Quantum Secure Digital Signature Scheme for Securing IEC 61850 R-GOOSE and R-SV Messages,” *IEEE Trans. on Ind. Applicat.*, vol. 61, no. 3, pp. 5135–5147, May 2025, doi: 10.1109/tia.2025.3542726.

[19] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, “Performance Evaluation and Analysis of IEC 62351-6 Probabilistic Signature Scheme for Securing GOOSE Messages,” *IEEE Access*, vol. 7, pp. 32343–32351, 2019, doi: 10.1109/ACCESS.2019.2902571.

[20] S. Yoon, R. Kim, H. Yoo, and H. Lim, “Real-Time GOOSE Attack Detection in IEC 61850 Substations Using SDN-Based Traffic Inspection,” in *2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, Naples, Italy: IEEE, Jun. 2025, pp. 271–272. doi: 10.1109/DSN-S65789.2025.00077.

[21] S. Bhattacharya, N. Saqib, and M. Govindarasu, “ML-based Anomaly Detection System for IEC 61850 Communication in Substations,” in *2024 IEEE Power & Energy Society General Meeting (PESGM)*, Seattle, WA, USA: IEEE, Jul. 2024, pp. 1–5. doi: 10.1109/PESGM51994.2024.10688773.

[22] P. K. Reddy Shabad, A. Alrashide, and O. Mohammed, “Anomaly Detection in Smart Grids using Machine Learning,” in *IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society*, Toronto, ON, Canada: IEEE, Oct. 2021, pp. 1–8. doi: 10.1109/iecon48115.2021.9589851.

[23] T. S. Ustun, S. M. S. Hussain, A. Ulutas, A. Onen, M. M. Roomi, and D. Mashima, “Machine Learning-Based Intrusion Detection for Achieving Cybersecurity in Smart Grids Using IEC 61850 GOOSE Messages,” *Symmetry*, vol. 13, no. 5, p. 826, May 2021, doi: 10.3390/sym13050826.

[24] M. Gao, J. Yu, Z. Yang, and J. Zhao, “A Physics-Guided Graph Convolution Neural Network for Optimal Power Flow,” *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 380–390, Jan. 2024, doi: 10.1109/TPWRS.2023.3238377.

[25] J. Choi and J. Kim, “Kirchhoff’s Circuit Law Applications to Graph Simplification in Search Problems,” 2020, doi: 10.48550/ARXIV.2009.11675.

[26] D. Celeita, M. A. Rios, D. M. Laverty, J. Forero, A. F. Moreno-Jaramillo, and S. McLoone, “IEC 61850-9-2 based module for state estimation in co-simulated power grids,” *IJECE*, vol. 13, no. 3, p. 2555, Jun. 2023, doi: 10.11591/ijece.v13i3.pp2555-2567.

[27] J.-S. Brouillon, K. Moffat, F. Dörfler, and G. Ferrari-Trecate, “Power grid parameter estimation without phase measurements: Theory and empirical validation,” *Electric Power Systems Research*, vol. 235, p. 110709, Oct. 2024, doi: 10.1016/j.epsr.2024.110709.

[28] Q. Li, H. Sun, J. Wang, B. Zhang, W. Wu, and Q. Guo, “Substation three-phase nonlinear state estimation based on KCL,” in *2011 IEEE/PES Power Systems Conference and Exposition*, Phoenix, AZ, USA: IEEE, Mar. 2011, pp. 1–5. doi: 10.1109/PSCE.2011.5772532.

[29] Y. Wang, Z. Lu, J. Ma, and Q. Jin, “Locational False Data Injection Attack Detection in Smart Grid Using Recursive Variational Graph Auto-Encoder,” *IEEE Internet Things J.*, pp. 1–1, 2025, doi: 10.1109/JIOT.2025.3526672.

[30] Y. Hu, H. Li, H. Yang, Y. Sun, L. Sun, and Z. Wang, “Detecting stealthy attacks against industrial control systems based on residual skewness analysis,” *J Wireless Com Network*, vol. 2019, no. 1, p. 74, Dec. 2019, doi: 10.1186/s13638-019-1389-1.

[31] Z. Gao, F. Sun, R. Rohrer, and D. S. Boning, “KirchhoffNet: A Scalable Ultra Fast Analog Neural Network,” in *Proceedings of the 43rd IEEE/ACM International Conference on Computer-Aided Design*, Newark Liberty International Airport Marriott New York NY USA: ACM, Oct. 2024, pp. 1–9. doi: 10.1145/3676536.3676662.

[32] T. Høiland-Jørgensen *et al.*, “The eXpress data path: fast programmable packet processing in the operating system kernel,” in *Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies*, Heraklion Greece: ACM, Dec. 2018, pp. 54–66. doi: 10.1145/3281411.3281443.

[33] R. D. G. Pacífico, L. F. S. Duarte, L. F. M. Vieira, B. Raghavan, J. A. M. Nacif, and M. A. M. Vieira, “eBPFlow: A Hardware/Software Platform to Seamlessly Offload Network Functions Leveraging eBPF,” *IEEE/ACM Trans. Networking*, vol. 32, no. 2, pp. 1319–1332, Apr. 2024, doi: 10.1109/TNET.2023.3318251.

[34] J. Zhang and L. Gruenwald, “Regularizing irregularity: bitmap-based and portable sparse matrix multiplication for graph data on GPUs,” in *Proceedings of the 1st ACM SIGMOD Joint International Workshop on Graph Data Management Experiences & Systems (GRADES) and Network Data Analytics (NDA)*, Houston Texas: ACM, Jun. 2018, pp. 1–8. doi: 10.1145/3210259.3210263.

[35] K. Frank, M. Rockl, M. J. Vera Nadales, P. Robertson, and T. Pfeifer, “Comparison of exact static and dynamic Bayesian context inference methods for activity recognition,” in *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, Mannheim: IEEE, Mar. 2010, pp. 189–195. doi: 10.1109/PERCOMW.2010.5470671.