Toward an SDN-Assisted Protocol-Aware Unified Intrusion Detection Framework for IEC 61850 GOOSE, SV and MMS Traffic

Hark Yoo, Ryangsoo Kim, Giha Yoon, Seunghyun Yoon* and Hyuk Lim*
Honam Research Division, Electronics and Telecommunications Research Institute (ETRI), Gwangju, Republic of Korea
*Department of Energy Engineering, Korea Institute of Energy Technology (KENTECH), Naju, Republic of Korea
{harkyoo, rskim, ygh}@etri.re.kr, {syoon, hlim}@kentech.ac.kr

Abstract—IEC 61850 has become the de facto communication standard for digital substation automation, but its core protocols, GOOSE, Sampled Values (SV), and MMS, were designed for availability and real-time performance rather than security, leaving process- and station-bus traffic exposed to spoofing, replay, false-data injection, suppression, and denial-of-service attacks. Because the three protocols differ fundamentally in communication semantics, namely event-driven bursts, high-frequency periodic streams, and client–server transactions, a single generic anomaly model is insufficient for substation-wide intrusion detection. This paper presents the design and intermediate evaluation of an SDN-assisted, protocol-aware unified IDS framework in which an SDN switch mirrors substation LAN traffic to a hybrid IDS that classifies traffic by protocol and dispatches it to fit-for-purpose engines: an invariant-rule and anomaly-based detector for GOOSE, a physics-guided and explainable detector for SV, and a service-sequence/state-machine rule engine for MMS. Completed single-protocol evaluations show over 96% GOOSE detection accuracy on the IEC61850SecurityDataset with OpenFlow-based containment, and 98.19% F1 at 1.4 µs per-sample latency for the standalone SV detector on QUT-ZSS 2023, while MMS provides parser-level validation and rule design. A unified alert schema, specification-driven synthetic attack generation, and a defined measurement protocol for the pending end-to-end evaluation together form a practical step toward protocol-complete IDS deployment for MVDC converter-station environments.

Keywords—IEC 61850, intrusion detection, GOOSE, Sampled Values, MMS, software-defined networking, explainable AI, substation cybersecurity

I. INTRODUCTION

IEC 61850 standardizes communication for substation automation systems (SAS), defining three principal protocols: GOOSE for event-driven protection signaling, Sampled Values (SV) for high-frequency streaming of digitized current and voltage measurements, and MMS for supervisory client–server operations [1]. Replacing hard-wired signals and vendor-specific protocols with a single Ethernet-based standard simplifies wiring and improves protection precision, but the standard was optimized for availability and real-time performance: GOOSE and SV are unencrypted layer-2 multicast frames, and MMS runs over TCP/IP with limited authentication in practice. Although IEC 62351 later specified protective mechanisms, processing overhead and field-deployment constraints have prevented widespread adoption [2], leaving substations exposed to data deletion, tampering, false data injection, replay, and denial-of-service attacks.

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Climate, Energy and Environment (MCEE) of the Republic of Korea (No. RS-2022-KP002871).

A large body of prior work addresses anomaly detection for a single IEC 61850 protocol, most commonly GOOSE, using rule-based checks, single statistical detectors, or deep-learning black-box models [3]. Each approach in isolation has known limitations: rule-based methods struggle with semantically well-formed malicious traffic and cross-channel anomalies, single statistics cannot capture composite symptoms, and deep models incur latency and provide little insight into why an alert was raised. More fundamentally, a substation LAN carries all three protocols simultaneously, and each exhibits distinct packet-generation patterns and invariants, so a detector tuned for the monotonic state-number sequence of GOOSE is meaningless for the modular sample counter of SV.

This paper reports the design and intermediate results of a research program that extends our previous single-protocol studies, namely real-time GOOSE attack detection using SDN-based traffic inspection [4] and physics-guided, explainable anomaly detection for SV [5], toward a protocol-aware unified IDS. Those studies contributed standalone detectors evaluated in isolation; what is new here is the framework layer that makes them operate as one substation-wide system: a single mirrored ingest path, a classifier and parser layer that abstracts GOOSE, SV, and MMS into a common packet representation with protocol-specific session keys, a newly designed MMS service-sequence engine that neither prior study addressed, a unified alert schema, and an explicit separation of passive monitoring from optional policy-graded containment.

The contributions are fourfold. First, an SDN-assisted monitoring architecture in which OpenFlow port mirroring supplies substation traffic to an IDS whose classifier dispatches GOOSE, SV, and MMS to dedicated parser and detector engines. Second, a protocol-aware detection strategy using deterministic invariant rules as the primary safety layer, with lightweight anomaly models added selectively per protocol. Third, a unified alert schema that normalizes protocol-specific evidence, including GOOSE state-number violations, SV physical-consistency deviations, and MMS InvokeID/state-machine anomalies, into a common operator-facing format. Fourth, specification-driven synthetic attack generation with an explicit account of evidence-level differences across datasets.

The main findings are as follows. (i) Protocol-aware dispatch is necessary rather than optional, since a detector tuned to one protocol's invariant is inapplicable to the others. (ii) Deterministic invariant rules cover most GOOSE attacks, exceeding 96% accuracy, but their coverage is bounded: the SV rule layer alerts on only two of five specification-driven

variants. (iii) Learned detection closes part of that gap within the process-bus timing budget, the standalone SV detector reaching 98.19% F1 at 1.4 µs per sample while remaining interpretable. (iv) Detector maturity is uneven across planes, so evidence levels are reported per protocol. (v) Monitoring and containment must be separated and confidence-graded, since only containment alters substation forwarding behavior.

II. System Architecture

A. SDN-Based Monitoring Pipeline

In a digital substation, merging units (MUs), IEDs, and HMI/engineering workstations share an Ethernet LAN. The architecture uses SDN switches managed through OpenFlow to replicate IEC 61850 traffic to an IDS monitoring port. The IDS receives mirrored traffic during normal monitoring and does not introduce inline packet-processing overhead into operational flows, which distinguishes it from the optional response plane: when a high-confidence GOOSE attack is detected, the SDN controller may intentionally modify forwarding behavior, such as isolating the suspected IED port through an OpenFlow rule update.

The IDS pipeline (Fig. 1) consists of three layers. First, a lightweight classifier separates protocols using EtherType values for GOOSE and SV and TCP-port/application-layer context for MMS. Second, protocol-specific parsers convert raw frames into a common PacketInfo abstraction while preserving session keys such as srcMAC/goID/gocbRef for GOOSE, MsvID for SV, and association or InvokeID context for MMS. Third, per-protocol detector engines analyze the parsed traffic and export their outputs to a unified alert schema, so that the IDS retains protocol-specific detection logic while presenting a consistent alert stream to operators, dashboards, or SIEM systems.

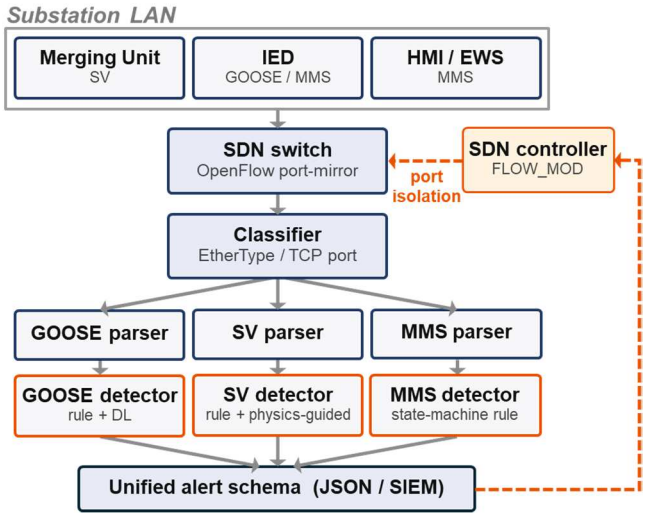


Fig. 1. Overall architecture of the protocol-aware unified IDS for IEC 61850 GOOSE / SV / MMS traffic.

B. Protocol Characteristics and Invariants

Table I summarizes the communication semantics of the three protocols. GOOSE is an event-driven multicast burst protocol on the process bus: a protection event triggers rapid retransmissions whose state number (stNum) increases monotonically per event while the sequence number (sqNum) counts retransmissions within a state. SV is a periodic high-frequency stream (80 or 256 samples per cycle, i.e., 4 or 12.8 kHz at 50/60 Hz) from MU to IED, in which the sample counter (smpCnt) increases modularly, the synchronization flag (smpSynch) stays in global-sync state, and one frame may bundle multiple ASDUs. MMS is a client–server protocol on the station bus pairing each confirmed request with a response through an InvokeID under an authorization context. These invariants form the first-line evidence of the framework because they are directly interpretable and checkable with low latency, but they are not sufficient alone: some attacks preserve syntactic correctness while manipulating payload values, timing, or physical consistency, and fields such as smpCnt can be spoofed outright [6]. The framework therefore uses invariant rules as a deterministic primary layer, supplemented by protocol-specific anomaly models where necessary.

TABLE I. Packet-Generation Characteristics and Invariants of the Three IEC 61850 Protocols

Aspect	GOOSE	SV	MMS
Bus	Process bus	Process bus	Station bus
Transport	Multicast L2 (0x88B8)	Multicast L2 (0x88BA)	TCP/IP unicast
Pattern	Event-driven burst	Periodic stream (4/12.8 kHz)	Request–response
Key fields	stNum, sqNum, TAL, allData	smpCnt, smpSynch, confRev	InvokeID, service code
Invariant	Monotonic stNum; contiguous sqNum	Modular smpCnt; smpSynch = 2	Service order; InvokeID pairing; authorization

III. Protocol-Aware Detection Engines

A. GOOSE: SDN-Assisted Hybrid Detection and Containment

Most GOOSE attacks, such as replay, fake-open command injection, suppression, payload modification, masquerade, and flooding, violate the stNum/sqNum/rate invariants. The GOOSE engine therefore combines two complementary methods, following our earlier design [4]: rule-based detection groups messages by source MAC, GOOSE ID, and control-block reference and verifies state number, sequence number, configuration revision, and timestamp consistency within each group, while an anomaly module analyzes inter-arrival times, sequence-number variation, and payload consistency over observation windows to catch semantically correct but malicious messages.

The GOOSE engine also supports an optional active-containment mode. Upon a high-confidence detection, the IDS may notify the SDN controller (e.g., ONOS [7]) to issue an OpenFlow FLOW_MOD command isolating the suspected IED port. In deployment this response follows operator policy: alert-only for low-confidence events, operator-confirmed isolation for medium confidence, and automatic isolation only for high-confidence attacks such as flooding or clearly invalid state transitions, since monitoring is passive whereas containment intentionally changes substation forwarding behavior. Validation on the IEC61850SecurityDataset [8] (Fig. 2) showed injection and replay reliably detected through state- and sequence-number anomalies and flooding through burst detection, with accuracy exceeding 96%; only subtle data-manipulation attacks occasionally evaded detection [4]. The engine exports the violated invariant, session key, confidence level, and recommended containment policy to the common alert schema.

B. SV: Physics-Guided and Explainable Anomaly Detection

SV traffic poses two constraints that rule out heavyweight models: the stream rate leaves a per-sample budget far below 1 ms, and operators need an explanation of why a sample was flagged. The engine therefore adopts the physics-guided, explainable detector of [5], whose four-stage structure is shown in Fig. 3.

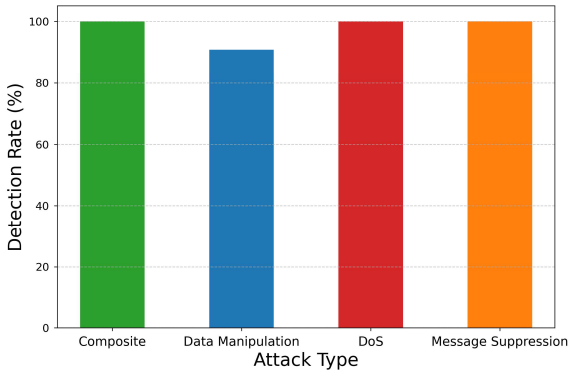


Fig. 2. GOOSE attack detection rate per attack type on the IEC61850SecurityDataset [4].

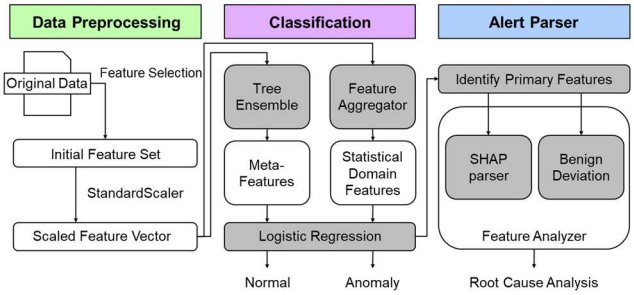


Fig. 3. Stage diagram of the physics-guided and explainable SV anomaly detector [5]: preprocessing, feature engineering, interpretable classification, and alert parsing.

For each preprocessed sample, an 11-dimensional feature vector is constructed. Four lightweight physics-guided statistical proxies, namely the mean, standard deviation, maximum, and minimum across the synchronized measurement channels of each SV packet, capture whether collective physical consistency among phase voltages and currents has degraded. Seven ensemble meta-features are derived from two heterogeneous base classifiers (Random Forest and Gradient Boosting): the two attack probabilities, the two confidence scores, inter-model agreement, mean confidence, and maximum attack probability. The final decision is made by an L2-regularized logistic regression whose explicit per-feature weights make the judgment stage interpretable.

An integrated alert parser turns detections into actionable alerts. For each flagged sample it selects the dominant feature $j^* = \text{argmax}_j |w_j z_j|$ and branches by feature type: a meta-feature explanation highlights base-model contributions and inter-model disagreement, whereas a physics-guided feature explanation quantifies the deviation from the benign baseline (e.g., "the channel standard deviation is 5.2× higher than the benign average") [5], [7].

Table II reports performance on the QUT-ZSS 2023 SV dataset [9] with scenario-aware 70/30 splits, in which attack scenarios are kept disjoint between the training and test partitions so that no frame from a test scenario is seen during training; this leakage-safe protocol applies to every learned model in the framework and will apply to the MMS engine once its corpus is complete. The detector attains the highest F1 (98.19%) and accuracy (99.80%), slightly surpassing a highly optimized XGBoost baseline and clearly outperforming ANN and LSTM, while its 1.4 µs per-sample latency remains far below the practical 1 ms bound. The key point is not the marginal gain but that this is achieved by an architecture designed for transparency [5].

TABLE II. SV DETECTION PERFORMANCE ON THE QUT-ZSS 2023 DATASET [5]

Method	F1 (%)	Accuracy (%)	Time (µs/sample)
Proposed	98.19	99.80	1.4
XGBoost	97.24	99.70	0.2
ANN	90.61	99.04	0.5
LSTM	90.69	99.03	8.8

C. MMS: Service-Sequence and State-Machine Rule Design

MMS attacks manifest primarily as violations of service sequence, authorization context, InvokeID pairing, or engineering-domain constraints: unauthorized Operate/Write commands from unexpected clients, directory scanning through abnormal GetNameList rates, responses without matching requests, replayed services with duplicate InvokeIDs, out-of-range SetDataValues requests, and file-service abuse such as configuration dumps. Because MMS is a supervisory client–server protocol rather than a hard real-time stream, the engine is designed as a service-sequence and state-machine rule module tracking application associations, request–response pairs, InvokeID reuse, service ordering, and rate anomalies per client/server context. At present the parser has been validated against the ITI corpus (176/176 packets); detector-level validation is limited by the scarcity of public MMS attack pcaps, so MMS results should be read as parser-level validation and rule-design readiness rather than a completed benchmark.

IV. DATASETS, SYNTHETIC ATTACKS, AND EVALUATION

A. Public Corpora and Their Gaps

Public IEC 61850 datasets are scattered per protocol. PowerDuck provides the largest packet-level labeled GOOSE corpus (1.13 M packets, 16 attack scenarios) and the IEC61850SecurityDataset [8] offers pcap traces of representative GOOSE attacks; QUT-ZSS [9] covers SV with GOOSE across 21 scenarios including multi-ASDU SV; SEAPATH and the mgadelha traces supply synthetic and real benign SV; for MMS, only the small ITI corpus is available. Evidence levels therefore differ: GOOSE rests on real attack traces and cross-dataset evaluation, SV on a standalone learned-detector evaluation plus a rule-layer baseline against synthetic variants, and MMS on parser validation and rule design only.

B. Specification-Driven Synthetic Attack Generation

Specification-driven synthetic attack generation is used as an evaluation-support mechanism rather than a substitute for real attack traces: controlled specification violations are injected into benign baselines so that the location and type of each anomaly are known exactly. The current prototype covers five SV variants (smpSynch transition, confRev change, smpCnt jump, svID swap, value spike) and MMS variants including unauthorized Operate/Write, service-

sequence violation, duplicate InvokeID replay, and abnormal directory scanning.

Because these traces carry exact ground truth, they also fix the reporting protocol for the next evaluation cycle: precision, recall, and false-alarm rate will be given per attack family for each GOOSE, SV, and MMS variant, including families the current rule layer does not cover, with benign-only runs used to measure the false-alarm rate independently of attack prevalence and with scenario-disjoint splits retained for all learned components.

C. Intermediate Evaluation Results

The evaluation layers must be distinguished: Table II reports the standalone learned SV detector on QUT-ZSS, whereas Table III reports the rule-layer and parser-level status of the unified prototype, so the two measure different layers and do not contradict each other. For GOOSE, invariant and rate-based rules give high coverage in controlled scenarios, while cross-dataset evaluation on PowerDuck is effective on frequent flood frames but weaker on rarer families. For SV, the invariant-rule layer bounds the coverage of invariant checks that the learned detector of Section III-B is intended to complement, with no false positives over the real benign traffic tested. For MMS, the result is parser validation only.

D. Planned End-to-End Evaluation Protocol

The results above characterize individual engines, not the integrated pipeline under simultaneous load, which we regard as the decisive test of the unified IDS claim. The measurement protocol is therefore fixed here so that the pending evaluation is directly comparable once the MVDC testbed campaign is complete. Mixed traffic will be replayed with SV at the process-bus rate, periodic and burst GOOSE, and concurrent MMS sessions, and five quantities will be measured: dispatch throughput per protocol and in aggregate, including the load level at which classification saturates; end-to-end alert latency as a distribution, so that tail behavior is visible against the sub-millisecond SV budget; packet loss at the mirror and parser stages; alert-correlation accuracy, namely whether concurrent anomalies on different planes are consolidated into the correct incident; and CPU and memory utilization. For the containment path, the containment false-positive rate, namely port isolations triggered on benign traffic per operating hour under each confidence policy, will also be reported.

TABLE III. PER-PROTOCOL STATUS OF THE CURRENT PROTOTYPE

Protocol	Evaluation item	Result
GOOSE	Data manipulation / suppression	100% (11/11) / 100% (7/7), controlled scenarios
GOOSE	DoS / flooding	97.25% detection, 94.32% precision
GOOSE	Cross-dataset (PowerDuck)	Macro-recall 0.67; micro-recall 0.997 (flood-dominated)
SV	Synthetic attacks (5 variants)	2 alerts, 1 diagnostic, 2 missed (rule layer only)
SV	Real benign (6 sources, 333 k ASDU)	0 false positives
MMS	Parser validation and rule-design readiness	176/176 packets parsed correctly; detector-level evaluation pending

E. Limitations

Four limitations remain. First, public attack corpora are limited and unevenly distributed, giving an evidence asymmetry across protocol planes. Second, some datasets are highly imbalanced, since sustained attacks such as flooding dominate frame-level counts and inflate micro-averaged metrics, so macro-level and per-attack-family results must be reported together. Third, and most importantly for the unified IDS claim, the integrated prototype has not been evaluated under simultaneous mixed GOOSE/SV/MMS load, so the quantities defined in Section IV-D are not yet measured; the results here support the feasibility of the architecture and its individual engines, not a validated end-to-end performance claim. Fourth, MMS evidence is limited to parser correctness and rule design, and the SV rule layer covers only part of the synthetic variant set. Quantifying the interpretability of the SV alert parser through a structured operator study also remains future work.

V. CONCLUSION AND FUTURE WORK

We presented the design and intermediate evaluation of an SDN-assisted, protocol-aware unified IDS framework for IEC 61850 traffic. Beyond the standalone detectors of our earlier work, it contributes the common ingest, parsing, dispatch, and alerting layer that lets the three protocol planes be monitored as one system, adds a newly designed MMS service-sequence engine, and separates passive monitoring from confidence-graded containment. Completed single-protocol results demonstrate feasibility: GOOSE detection exceeding 96% accuracy with OpenFlow-assisted containment, and physics-guided, explainable SV detection at 98.19% F1 with microsecond-level latency, while MMS contributes parser validation and rule design. The central lesson is that protocol-aware detection is necessary, since the three protocols differ in packet-generation patterns, timing constraints, and semantic invariants. Ongoing work follows the protocol of Section IV-D: completing the MMS attack corpus and per-attack detector evaluation, quantifying end-to-end performance under mixed traffic, and validating the integrated IDS on an MVDC converter-station testbed.

REFERENCES

[1] International Electrotechnical Commission, Communication networks and systems for power utility automation, IEC 61850, 2nd ed., 2011.

[2] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 5643–5654, 2020.

[3] H. Nhung-Nguyen et al., "Machine-learning-based anomaly detection for GOOSE in digital substations," Energies, vol. 17, no. 15, p. 3745, 2024.

[4] S. Yoon, R. Kim, H. Yoo, and H. Lim, "Real-time GOOSE attack detection in IEC 61850 substations using SDN-based traffic inspection," in Proc. IEEE/IFIP Int. Conf. on Dependable Systems and Networks (DSN), Naples, Italy, 2025.

[5] S. Ryu, R. Kim, H. Yoo, H. Lim, and S. Yoon, "Physics-guided and explainable anomaly detection for IEC 61850 sampled values," in Proc. IEEE 30th Pacific Rim Int. Symp. on Dependable Computing (PRDC), Seoul, Korea, 2025, pp. 130–131.

[6] A. Pal, A. Jolfaei, and K. Kant, "A fast prekeying-based integrity protection for smart grid communications," IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5751–5758, 2021.

[7] P. Berde et al., "ONOS: Towards an open, distributed SDN OS," in Proc. HotSDN, Chicago, IL, USA, 2014, pp. 1–6.

[8] P. Biswas et al., "A synthesized dataset for cybersecurity study of IEC 61850-based substation," in Proc. IEEE SmartGridComm, 2019.

[9] CSCRC-SCREED, "QUT-ZSS-2023-SV: QUT zone substation security – SV attack datasets," 2023. [Online]. Available: https://github.com/CSCRC-SCREED/QUT-ZSS-2023-SV