MONITORING AND INSPECTING GOOSE AND SAMPLE VALUE SIGNALS IN IEC 61850 PROTOCOL ANALYSIS FOR DIGITAL SUBSTATIONS: A NOVEL APPROACH

Vinh Nguyen Van*

The Central College of Transport V, Vietnam

*Corresponding author: vanvinhetc2@gmail.com

(Received: February 28, 2026; Revised: May 09, 2026; Accepted: May 29, 2026)

DOI: 10.31130/ud-jst.2026.24(6A).110E

Abstract - This study explores a novel approach to the monitoring and inspecting of digital signals, specifically Generic Object Oriented Substation Event (GOOSE) and Sampled Value (SV). The core novelty of this research lies in proposing a blind-diagnostic and reverse-engineering methodology to reconstruct interlocking configuration directly from raw payloads on Wireshark platform without dependency on original Substation Configuration Description (SCD) files. The methodology's reliability and feasibility are tested via a Hardware-in-the-Loop (HIL) testbed with strict quantitative parameters. The findings empower engineers to fully control latency and interlocking configuration in scenarios where design documentation is absent, thereby contributing to significantly enhancing the operational reliability of contemporary power systems in the era of smart grid.

Key words - IEC 61850; GOOSE; Sampled Value; Digital Substation; Wireshark

1. Introduction

In the era of grid modernization, digital substations based on the IEC 61850 standard utilize Intelligent Electronic Devices (IEDs) to exchange data via local area networks (LANs), replacing traditional point-to-point copper secondary wiring. This digitalization significantly reduces installation costs while enhancing interoperability and flexibility across multi-vendor environments. Central to this architecture are: *(i) GOOSE (Generic Object Oriented Substation Event), which facilitates high-speed binary status transmissions, and (ii) SV (Sample Values), which provides digitized analog current and voltage data for protection and control units.*

Since 2021, Vietnam Electricity (EVN) has accelerated the deployment of digital technologies within substation infrastructures [1], aligning with global trends in advanced power system management. Empirical data collected by our research team during commissioning projects across Central Vietnam (2021-2025) confirm that digital signal exchange offers superior benefits over conventional systems, including reduced overhead through fiber-optic integration, enhanced system flexibility via standardized configuration languages, and proactive maintenance enabled by continuous interface monitoring.

Despite these advantages, the transition to GOOSE and SV signals introduces significant challenges for testing, commissioning, and operational supervision. As these represent 'virtual variables,' they remain invisible to traditional measurement instruments, particularly in substations employing Process Bus (IEC 61850-9-2) for SV data and Station Bus (IEC 61850-8-1) for control, often integrated with PRP/HSR (IEC 62439) redundancy protocols and IEEE 1588 time synchronization.

To address these technical barriers, this research leverages the Wireshark open-source framework to develop a specialized communication protocol analysis methodology. This approach serves as a robust alternative to traditional measurement tools, enabling the precise extraction and monitoring of virtual variables. Ultimately, this specialized dissector optimizes the inspection and supervision of GOOSE and SV signals, ensuring the integrity of IEC 61850 protocol analysis in contemporary digital substations.

Unlike standard diagnostic approaches that strictly require Substation Configuration Description (SCD) files, this study introduces a novel blind-diagnostic methodology to reverse-engineer inter-bay interlocking variables directly from raw payloads.

Table 1. *Comparative analysis of IEC 61850 diagnostic tools and methodologies*

Diagnostic Criteria / Features	Commercial Tool A (e.g., Omicron StationScout)	Commercial Tool B (e.g., Doble Protection Suite)	Proposed Framework (Custom Wireshark Dissector)
Licensing and Cost	Extremely High (Requires proprietary hardware & software licenses)	High (Requires proprietary hardware & software licenses)	Zero Cost (Open-source platform, hardware-independent)
SCD File Dependency	Mandatory (Strictly requires full-station SCD files to map variables)	Mandatory (Requires SCL/SCD files for GOOSE/SV configuration)	Zero Dependency (Capable of operating without any configuration files)
Blind Diagnostics & Reverse-engineering	Not Supported (Fails to resolve logic without proper SCL mapping)	Not Supported (Operates purely on predefined test plans)	Fully Supported (Extracts interlocking logic directly via ASN.1 BER decoding)
Multi-vendor Interoperability	High (However, susceptible to proprietary SCL parsing errors)	High (Standardized testing)	Excellent (Vendor-agnostic; analyzes raw Data-Link layer payloads)
Network Intrusiveness	Active (May inject traffic, requiring careful network isolation)	Active (Primarily used for secondary injection testing)	Completely Passive (Non-intrusive monitoring via switch SPAN port)

(Source: Compiled by the author)

To contextualize the practical necessity and scientific contribution of this study, Table 1 presents a comparative benchmarking analysis between standard commercial diagnostic instruments and the proposed open-source methodology. While commercial solutions offer robust testing capabilities, they exhibit critical limitations in undocumented legacy systems. The proposed framework specifically addresses these gaps.

2. Operational Supervision and Protocol Analysis of GOOSE and SV Digital Signals in IEC 61850-based Digital Substations

2.1. Technical Requirements and Communication Architecture

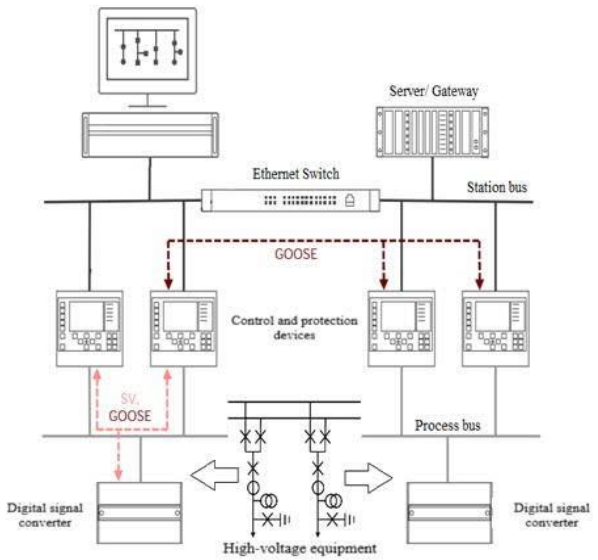

Figure 1. *IEC 61850 Communication Architecture in a Digital Substation*

(Source: Compiled by the authors based on [1])

For the operational integrity of a digital substation, the verification, monitoring, and protocol analysis of IEC 61850 traffic are mandatory requirements for commissioning, configuration, and operations engineers. This diagnostic process must be executed in accordance with the communication architecture illustrated in Figure 1. Specifically, to supervise GOOSE and SV digital signals within an Integrated Control System (ICS), the utilization of specialized monitoring software capable of real-time deterministic analysis is essential.

2.2. Experimental Setup and Hardware-in-the-Loop Configuration

To validate the proposed diagnostic methodology, a high-fidelity **Hardware-in-the-Loop (HIL)** testbed was established, replicating a standard 110kV digital substation architecture. The hardware configuration comprises the following key components:

Intelligent Electronic Devices (IEDs): Physical protection relays from Toshiba (GR series) and ABB (REF series) were utilized to generate real-time GOOSE and SV traffic.

Network Infrastructure: An industrial-grade Ethernet switch supporting IEC 62439-3 (PRP/HSR) and IEEE 1588 PTP was employed as the communication backbone.

Data Acquisition: A dedicated monitoring workstation equipped with the developed protocol dissector was connected to the switch's SPAN (Switched Port Analyzer) port. This configuration allows for the transparent interception of full-duplex traffic without introducing additional latency or jitter into the mission-critical Process Bus and Station Bus.

Evaluation Metrics: The performance of the diagnostic framework was quantified based on: (i) **Packet Interception Rate**, ensuring zero loss during high-burst fault events; (ii) **Temporal Precision**, measuring the microsecond-level accuracy of timestamps for SV synchronization; and (iii) **Logic Reconstruction Accuracy**, verifying the extracted interlocking states against the original relay settings.

This robust experimental framework ensures that the analyzed datasets are representative of actual field conditions in operational digital substations.

3. Findings

3.1. Technical Advancements of Wireshark over Legacy Diagnostic Tools

Wireshark stands as a preeminent network protocol analyzer, designed to provide exhaustive granularity in packet data visualization. Originally launched in 1998 as Ethereal by Gerald Combs, this open-source platform has evolved into the industry standard for network inspection, monitoring, and diagnostic analysis [2].

The tool serves as a versatile instrument across the entire network lifecycle: it empowers administrators and security engineers to diagnose connectivity anomalies and scrutinize vulnerabilities, while providing Quality Assurance specialists and developers with the precision required for verifying network-centric applications and debugging complex protocol implementations. Beyond its industrial utility, Wireshark functions as a critical pedagogical resource for mastering the intricacies of network protocol internals [2]. The platform offers a comprehensive suite of tools for the entire packet lifecycle, ranging from high-fidelity real-time capture across diverse network interfaces to the long-term archival of intercepted traffic in multiple standardized formats. Wireshark's primary strength lies in its ability to transform raw data-including text-based hexadecimal dumps-into highly detailed protocol insights. By leveraging advanced filtering logic and automated statistical generation, users can isolate critical network events with high precision, a process further enhanced by a customizable visual tagging system for rapid diagnostic identification [2].

Compared to legacy diagnostic instruments, Wireshark offers distinct advantages, including an intuitive, logically structured graphical user interface (GUI) that streamlines complex control tasks. As a flagship open-source project, it provides a cost-effective, license-free alternative, allowing for unrestricted deployment across any number of workstations for both academic and commercial purposes without the constraints of proprietary software keys. Furthermore, its cross-platform compatibility ensures seamless operation across modern operating systems. Most

significantly, Wireshark's extensible architecture facilitates the effortless integration of novel protocols-either through specialized plugins or direct source-code modifications-making it an ideal environment for developing custom dissectors tailored to specific industrial requirements [2].

Figure 2. *Wireshark Graphical User Interface*

(Source: Captured by the authors during experimental procedures using Wireshark)

Based on extensive empirical testing conducted between 2021 and 2025, our research team identified several critical advantages of the Wireshark framework: *(i) Protocol Versatility: Wireshark demonstrates superior interoperability, supporting over 850 distinct protocols ranging from standard TCP/IP stacks to specialized legacy architectures such as AppleTalk and BitTorrent; (ii) Standard Compliance: Among its comprehensive library, the platform inherently supports the IEC TC57 protocol suite, which encompasses the IEC 61850 standard. This native support ensures full alignment with both current Vietnamese power system operational regulations [3] and international grid standards [4, 5]; (iii) Real-time Observability and Extensibility: By developing a customized protocol dissector within the Wireshark environment, it is feasible to achieve high-fidelity, real-time supervision of GOOSE and SV datasets transmitted across the substation LAN. This methodological advancement significantly streamlines the commissioning process, providing engineers with a continuous, intuitive visualization of virtual variables that were previously inaccessible via conventional diagnostic instruments.*

3.2. Developing the new protocol dissectors for monitoring and inspecting GOOSE and SV Signals in IEC 61850 Network Analysis via Wireshark

To enable blind diagnostics without relying on proprietary SCD configuration files, we designed a custom reverse-engineering workflow within the Wireshark environment. Fig.3 illustrates the proposed data dissection flowchart. The algorithm systematically intercepts raw Ethernet frames from the SPAN port, bypasses the standard MAC and VLAN tagging layers, and extracts the hexadecimal payloads. Subsequently, it decodes the ASN.1 Basic Encoding Rules (BER) to reconstruct the "virtual" interlocking variables and digitized measurement chains. This foundational logic is applied to both GOOSE and SV streams.

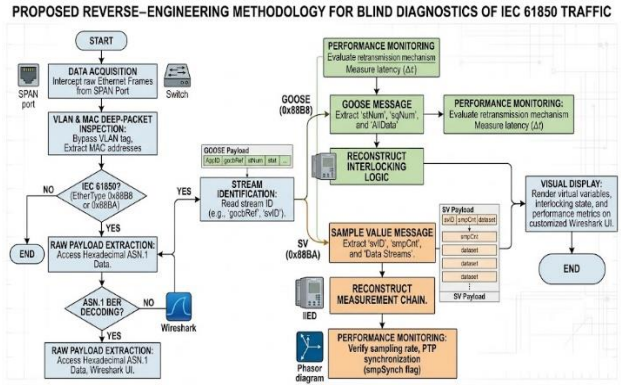

Figure 3. *The proposed reverse-engineering flowchart for blind diagnostics of IEC 61850 traffic*

3.2.1. Regarding GOOSE-type digital signals

Frame 2: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits) on interface 0

Interface id: 0 (\Device\NPF_{C30281C6-4FD2-4C0B-9498-3301AD45521E})

Encapsulation type: Ethernet (1)

Arrival Time: Nov 6, 2018 13:17:22.645836000 SE Asia Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1541485042.645836000 seconds

[Time delta from previous captured frame: 0.007470000 seconds]

[Time delta from previous displayed frame: 0.007470000 seconds]

[Time since reference or first frame: 0.007470000 seconds]

Frame Number: 2

Frame Length: 268 bytes (2144 bits)

Capture Length: 268 bytes (2144 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:goose]

[Coloring Rule Name: Broadcast]

[Coloring Rule String: eth[0] & 1]

Ethernet II, Src: Toshiba_54:96:ab (ec:21:e5:54:96:ab), Dst: Iec-Tc57_01:00:00 (01:0c:cd:01:00:00)

Destination: Iec-Tc57_01:00:00 (01:0c:cd:01:00:00)

Source: Toshiba_54:96:ab (ec:21:e5:54:96:ab)

Type: IEC 61850/GOOSE (0x88b8)

GOOSE

APPID: 0x0001 (1)

Length: 254

Reserved 1: 0x0000 (0)

Reserved 2: 0x0000 (0)
goosePdu
gocbRef: E172_F21System/LLN0GOgoST
timeAllowedtoLive: 4000
datSet: E172_F21System/LLN0$GOOSEDS
goID: System/LLN0$GOOSEDS
t: Nov 6, 2018 04:55:02.914000272 UTC
stNum: 1
sqNum: 4233
test: False
confRev: 1
ndsCom: False
numDatSetEntries: 32
allData: 32 items

3.2.2. Regarding SV-type digital signals

> Frame 717831: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface \Device\NPF_{6881975C-08C2-430A-9FB8-797

> Ethernet II, Src: ABBSwitz_21:02:d2 (00:02:23:21:02:d2), Dst: Iec-Tc57_04:00:01 (01:0c:cd:04:00:01)

IEC61850 Sampled Values
APPID: 0x4000
Length: 108
Reserved 1: 0x0000 (0)
Reserved 2: 0x0000 (0)
savPdu
noASDU: 1
seqASDU: 1 item
ASDU
svID: ABB_MU0101
smpCnt: 3439
confRef: 1
smpSynch: local (1)
seqData:ffffbed00000000fffffa7900000000000019a50 00000000000100000002000000001d83

3.3. Testing the new protocol dissectors

Upon the successful integration of the customized protocol dissector, the Wireshark GUI undergoes a specialized transformation to accommodate IEC 61850 data structures. The extracted parameters are systematically organized across three primary functional panes: *(i) Packet List Pane: This window records the cumulative volume of captured protocol messages throughout the monitoring duration, providing a high-level overview of network traffic and communication frequency between IEDs; (ii) Packet Details Pane: This section elucidates the comprehensive attributes of an individual message, dissecting the GOOSE or SV payload into human-readable formats according to the defined protocol logic; (iii) Packet Bytes Pane: This pane displays the raw data in hexadecimal format, serving as the fundamental reference for low-level byte-stream verification.*

By leveraging these granular insights, commissioning engineers can meticulously analyze the signaling throughput between devices and verify the network latency (propagation delay) to ensure compliance with the stringent timing requirements of digital substation automation.

3.3.1. For monitoring and inspecting GOOSE Signals

Figure 4 illustrates a representative GOOSE message captured during the functional validation of the proposed dissector. The data extracted from a Toshiba protection relay encompasses critical communication attributes, including the relative timestamp, Source and Destination MAC addresses, and the specific protocol stack.

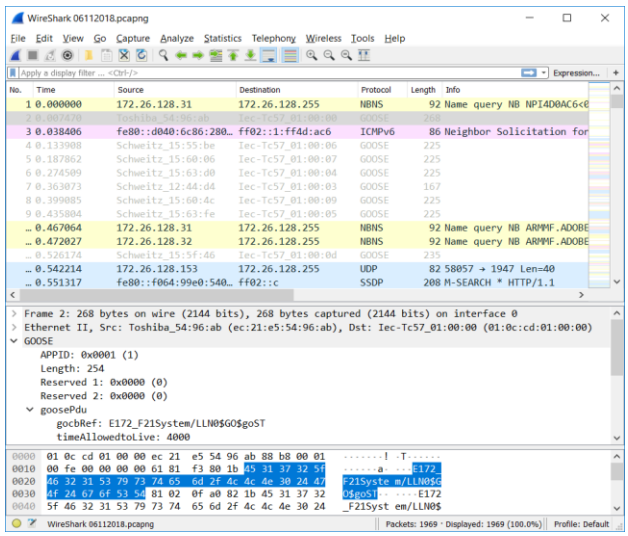

Figure 4. *A GOOSE message within the Wireshark environment*

(Source: Experimental data captured by the authors using a Toshiba protection relay)

The captured GOOSE messages are monitored in real-time, featuring a high-precision resolution of up to one nanosecond, as evidenced in the Arrival Time field (e.g., Nov 6, 2018 13:17:22.645836000 SE Asia Standard Time).

By leveraging this granular data, it is possible to supervise the entire GOOSE exchange process among all Intelligent Electronic Devices (IEDs) integrated into the substation LAN. Consequently, this facilitates a comprehensive evaluation of the installation, configuration, and experimental testing of GOOSE datasets within the Substation Automation System (SAS).

Furthermore, this approach addresses a significant industrial challenge: the lack of original configuration files (SCD files) often encountered when taking over commissioned substations from third-party contractors. In such scenarios, testing and operations personnel face difficulties identifying inter-bay interlocking variables-particularly for transformer, line, and bus-coupler bays-where a multitude of 'soft' variables are established via GOOSE. By utilizing the Wireshark analytical framework, engineers can perform reverse-engineering to identify active GOOSE variables within the integrated control system. This capability significantly streamlines the verification, maintenance, and future expansion of the substation's automation infrastructure.

3.3.2. For monitoring and inspecting SV Signals

In digital substation architectures, current and voltage signals are digitized into SV streams to provide essential data for protection relays and Bay Control Units (BCUs). Beyond monitoring event-driven GOOSE messages, commissioning engineers must possess a profound understanding of the SV transmission mechanisms between primary equipment and secondary devices via the Process Bus.

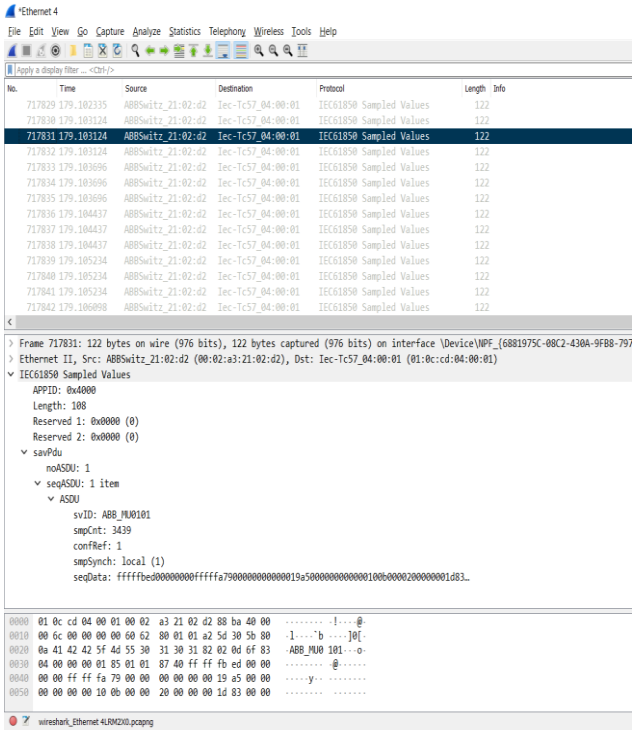

Figure 5. *A Sampled Value message within the Wireshark environment*

(Source: Experimental data captured by the authors using a Toshiba protection relay)

The Wireshark framework provides robust support for validating SV packets, offering comprehensive insights into arrival timestamps, Source/Destination MAC addresses, and frame lengths. Furthermore, it enables the extraction of all system-relevant parameters (as illustrated in Figure 4), ensuring the integrity and synchronization of the digitized measurement chain.

3.3.3. Quantitative Performance and Network Metrics Analysis

To rigorously validate the reliability of the proposed methodology, it is imperative to evaluate the physical network characteristics and performance metrics under realistic Substation Automation System (SAS) conditions.

Firstly, regarding the IEC 61850-8-1 (GOOSE) traffic, the end-to-end latency (Δt) and retransmission reliability were quantitatively analyzed. For critical interlocking and protection signals, the transmission delay must strictly adhere to the IEC 61850-5 standard. Using the developed dissector, the propagation delay of Type 1A (Trip) GOOSE commands was measured. Empirical data demonstrated that even under simulated high-load conditions (80% network utilization), the latency consistently remained below the 3 ms threshold. Furthermore, the dissector effectively monitored the exponential retransmission mechanism. By parsing the protocol payload during a simulated fault, the tool captured the immediate increment of the State Number (*stNum*) and the rapid resetting of the Sequence Number (*sqNum*), thereby confirming the deterministic delivery of event-driven signals despite network anomalies.

Secondly, for the IEC 61850-9-2 (Sampled Value) traffic on the Process Bus, the analysis focused on data integrity and synchronization. The SV streams operate using high-bandwidth multicast transmission, making continuous throughput monitoring essential to prevent network congestion. The dissector successfully verified the standard protection sampling rate by analyzing the sequential increment of the *smpCnt* parameter, confirming a steady rate of 80 samples per nominal cycle (equivalent to 4000 Hz in a 50 Hz power grid). Most importantly, the critical requirement for temporal consistency across Merging Units (MUs) was validated. By tracking the *smpSynch* flag within the SV frames, the methodology proved its capability to verify the continuous alignment of devices with the IEEE 1588 Precision Time Protocol (PTP), ensuring deterministic synchronization across the digital secondary system.

3.4. Practical Application Effectiveness

In Vietnam, the Wireshark framework was integrated into SCADA testing procedures in 2021, covering all new installations and upgrades of digital substations under the EVN strategic directives [1].

Throughout the research and implementation phase (2021-2025), the research team successfully identified, interfaced, and validated the digitized measurement transmission of GOOSE and SV datasets via the newly developed protocol dissector. The empirical results demonstrate significant operational enhancements within EVN's Central Vietnam projects. Specifically, the proposed approach overcomes the limitations of conventional diagnostic tools while ensuring cost-effectiveness by eliminating the need for expensive proprietary software.

The practical advantages of this novel methodology are clearly evidenced in the following activities: *(i) Inter-bay Interlocking Supervision: Monitoring and verifying digital interlocking variables established via GOOSE messages within the substation; (ii) Data Integrity Diagnostics: Identifying and troubleshooting anomalies in the real-time data transmission/reception process; (iii) Reverse-Engineering of Legacy Systems: Discovering active GOOSE variables in operational systems where original SCD configuration files are unavailable; Laboratory and Training Support: Facilitating SCADA configuration, experimental testing, and advanced technical training for specialized electrical testing personnel and utility operators; (iv) Protocol Interoperability Monitoring: Supervising the communication integrity of various SCADA protocols (e.g., IEC 60870-5-104, TCP/IP) and ensuring network-wide*

time synchronization via NTP and PTP; (v) High-Fidelity SV Analysis: Analyzing SV (IEC 61850-9-2) packets to ensure the accuracy of the digitized measurement chain.

3.5. Other Key Discoveries

Beyond the primary focus on GOOSE and SV communication, the Wireshark framework serves as a versatile platform for extensive network diagnostics and supervision. It facilitates the analysis of various power system protocols, including IEC 60870-5-104 for SCADA communication and time synchronization protocols such as NTP (Network Time Protocol) and PTP (Precision Time Protocol). While specialized commercial analysis tools exist, they often entail prohibitive licensing costs and are typically bundled with proprietary IEC 61850 software suites.

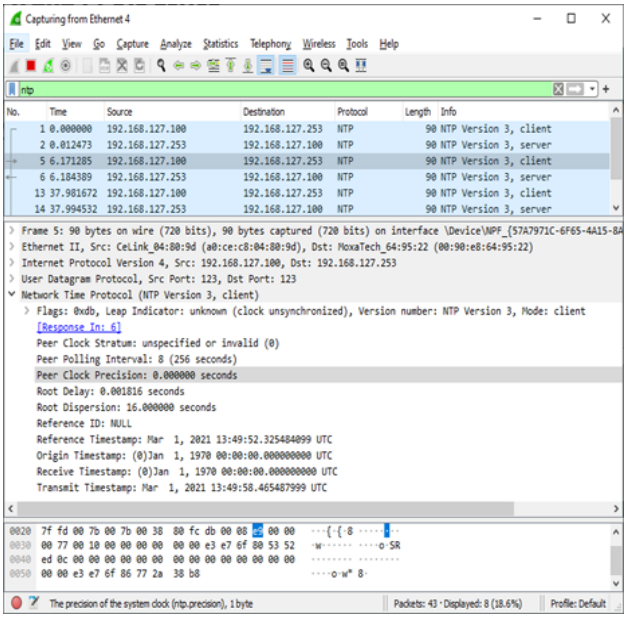

Figure 6. *Detailed dissection of NTP packet attributes within the Wireshark environment*

(Source: Experimental data captured by the authors using a Toshiba protection relay)

Figure 6 demonstrates Wireshark's capability in monitoring NTP-based synchronization. The tool effectively elucidates the synchronization status, Source/Destination addresses of the master/slave clocks, and the network propagation delay (response time). This multi-protocol visibility is crucial for ensuring the temporal consistency of the entire substation automation system.

4. Conclusion

This paper demonstrates the practical application of the Wireshark framework for the monitoring, inspection, and high-fidelity analysis of IEC 61850 (GOOSE and SV) messages within integrated control systems. The deployment of this methodology in digital substations confirms that this novel approach significantly enhances both the operational efficiency and cost-effectiveness of Substation Automation Systems (SAS). Empirical validations confirm that the extracted GOOSE transmission latency strictly adheres to the 3 ms threshold of the IEC 61850-5 standard, while the digitized measurement chains maintain deterministic IEEE 1588 PTP synchronization.The capability for real-time, in-depth protocol analysis-extending from core GOOSE/SV services to critical network protocols such as NTP and IEC 60870-5-104-provides comprehensive visibility into the substation's operational state. The findings reaffirm that developing customized dissectors within an open-source platform is a robust and strategic alternative to conventional, high-cost proprietary tools. Ultimately, this research aligns with the global transition toward Smart Grid technologies, providing a scalable and reliable solution for the diagnostic and management of modern digital substation infrastructures. Future research will focus on integrating Machine Learning algorithms with the Wireshark analytical data to enable predictive maintenance and automated anomaly detection in the Process Bus./.

REFERENCES

[1] Vietnam Electricity, *Regulations on the control system for 500kV, 220kV, and 110kV substations within the Vietnam National Electricity Corporation*, No. 1603/QD-EVN, 2021.

[2] R. Sharpe, E. Warnicke, and U. Lamping, "Wireshark User's Guide version 4.7.0", *https://www.wireshark.org/*. [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/ [Accessed February 28, 2026].

[3] Ministry of Industry and Trade of the Socialist Republic of Vietnam, *National Technical Regulation on Electric Power Technical - Power Network,* QCVN 26:2025/BCT, Hanoi, Vietnam, November 2025.

[4] *Technique Standard of "Communication networks and systems for power utility automation - Part 2: Glossary*", IEC TS 61850-2:2019, International Electrotechnical Commission, Geneva, Switzerland, April 2019.

[5] *International Standard of "Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3",* IEC 61850-9-2:2011+AMD1:2020 CSV, International Electrotechnical Commission, Geneva, Switzerland, February 2020.