Implementing Secure Layer 2 Tunneling Protocols for IEC 61850-90-5 Based Routable and Non-Routable GOOSE and SV Messages

Stephen Ugwuanyi
PNDC
University of Strathclyde
Glasgow, United Kingdom
stephen.ugwuanyi@strath.ac.uk

Kinan Ghanem
PNDC
University of Strathclyde
Glasgow, United Kingdom
kinan.ghanem@strath.ac.uk

Ibrahim Abdulhadi
PNDC
University of Strathclyde
Glasgow, United Kingdom
ibrahim.f.abdulhadi@strath.ac.uk

***Abstract*—In this paper, the performance of layer 2 tunnelling for IEC 61850 inter-substation communication is presented for a teleprotection function use case. Generic Object-Oriented Substation Events (GOOSE) and Sampled Value (SV) packets routed over layer 2/3 VPN using Multiprotocol Label Switching (MPLS) network and the end-to-end timing and latency of packets were evaluated. The performance and impact of using MACsec and IPsec security schemes are also presented. The paper also aims to show the minimal if not negligible, impact of end-to-end encryption of securing GOOSE and SV Messages over layer 2 VPN.**

***Keywords*—IEC 61850, GOOSE, Sampled Values, MACsec, IPsec, Tunnelling Protocol.**

I. Introduction

Modern digital grids are designed to handle two-way power flow while making use of IEEE C37.118.2 [1] and IEC 61850 standards [2] to reliably deliver grid monitoring and protection applications which require reliable Wide Area Network (WAN) and Local Area Network (LAN) integration [3]. In the context of IEC 61850 power utility automation, securely routing Sampled Values (SV) and Generic Object Oriented Substation Events (GOOSE) data streams over IP networks presents a significant challenge. This is due to the conflicting demands of stringent real-time requirements and the inherent overhead and complexity associated with secure communication protocols. Security protocols require extremely low latency to ensure timely control and protection actions, however, secure communication methods such as encryption and authentication can introduce additional processing delays, which might exceed the acceptable latency limits. The consistency of SV and GOOSE transmissions (low jitter) can also be impacted by multicast routing-based communication methods, which increase data overhead because encryption keys and secure channels need to be managed for multiple recipients simultaneously.

Reliable and secure connectivity for digital substations integration plays an important role in enabling critical protection and control function deployment in a smart grid. Generic Routing Encapsulation (GRE), Layer 2 Tunnelling Protocol (L2TP), Multiprotocol Label Switching (MPLS), and Virtual Private LAN Services (VPLS) are a few standard tunneling and encapsulation methods. The Distribution Network Operators (DNOs) and Transmission System Operators (TSOs) are currently evaluating the viability and benefits of applying tunneling protocol for IEC 61850 process data over secure layer 2 communications compared with secure layer 3 (e.g. Routable (R-GOOSE)) data exchange.

While some studies have implemented tunneling and encapsulation methods of SV and GOOSE messages routing for inter-substation communication of protection, teleprotection, and phasor measurement data at the layer 2 level, the methods are often based on a simple test network involving two network nodes which lack the true representation of a growing complex grid deployment requirements [2]. Enabling large-scale deployment of IEC 61850 for inter-substation communication implies advanced routing of SV and GOOSE over the data link layer as well as the WAN using Multiprotocol Label Switching (MPLS) based technology.

Also, the impacts of applying security protocols such as Media Access Control Security (MACsec) and Internet Protocol Security (IPsec) on teleprotection applications and to the time synchronization signals on the devices within the network have only been explored by limited literature. Implementing encryption and authentication algorithms for process bus data can mitigate potential application and data integrity attacks and protect the grid from cyber security events but may introduce unacceptable latencies with increased computational costs [4]. Hence, this paper will provide experimental results of layer 2 tunnelling for inter-substation communication as well as identify any issues for improvement required for the future rollout of this communication model in smart grid networks.

For secure transmission of synchrophasor data over WAN, a security toolbox (R-GoSV) based on OpenSSL Library has been used to encrypt GOOSE and SV data streams using AES256-GCM algorithm and HMAC-SHA256 for message authentication [5]. However, the findings show computation delays for the security algorithms which fall within safe operational limits. The communication services defined in IEC 61850 include SV and GOOSE for the transfer of time-critical functions. IEC 61850 supports the transfer of digital states, time synchronisation and interoperability of Merging Units (MUs) and Intelligent Electronic Devices (IEDs) data streams over wide area transmissions.

The IEC 61850 GOOSE and SV protocols are intended to be used for communication inside the substation for critical protection applications. Both are designed to operate in Layer 2 and transmitted inside an Ethernet frame. Therefore, within the substation LAN, GOOSE and SV traffic use Ethernet as a transmission medium between substation devices inside the same LAN. However, if the traffic (i.e., GOOSE and SV) is to be transmitted between different substation LANs over a wide area network, a special network configuration is required. Like building a tunnel where the IEC 61850-90-1 Routable GOOSE and IEC 61850-90-5 Routable SV can be transmitted inside the tunnel using UDP over Internet Protocol (IP). One real application for this can be transmitting Phasor Measurement Unit (PMU) data between digital substations.

979-8-3503-9042-1/24/$31.00 ©2024 IEEE

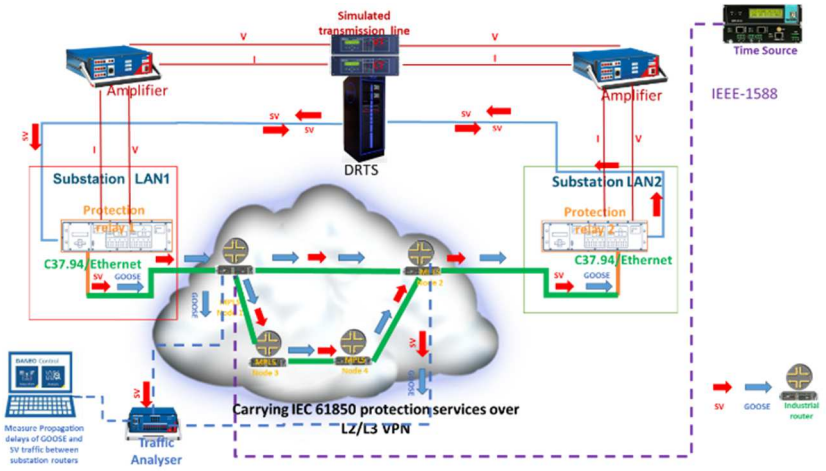

Figure 1. Test Network

The main contributions of the papers are:

1. Verify IEC 61850 SV and GOOSE protection services stability and reliability over layer 2 VPN using IP-MPLS technology.
2. Verify IEC 61850 R-SV and R-GOOSE protection services stability and reliability over layer 3 WAN using IP-MPLS technology.
3. Demonstrate the capabilities of IP-MPLS technology and validate its implementation performance to carry protection services for future digital substation.
4. Investigate MACsec encryption technique end-to-end delay on protection services described in contribution 2 and 3.
5. Timing synchronization test to demonstrate the effects of any loss of synchronisation source on the stability of the IEC 61850 services.

II. Time Synchronisaton Test

Time-critical applications that rely on GOOSE and SV messages require precise synchronisation in substations. Communication protocols for connecting substations require various levels of synchronisation accuracy based on the criticality of the end application [6]. For substation GOOSE and SV messaging, Precision Time Protocol (PTP) within submicrosecond is needed to enable time and phase distribution through the network based on IEEE 1588-2002 standard (time accuracy needed for SV to be exchanged properly among the IEDs inside the substation will require an accurate time of 1 µs). The synchronisation loss test will monitor changes in the performance of both the MPLS communication network and the IEC 61850 protection services covering the main source of synchronisation from the grandmaster. The effects of loss of external time synchronisation (i.e., the main external source of synchronisation) on triggering relay alarms and impacting the operation of the MPLS teleprotection service in IP/MPLS networks are evaluated. Validating the response rate from the substation (i.e. MPLS nodes) upon communication network incidents such as loss of synchronisation and link failure. The test grandmaster time source ensures that the communication networks and the relays are interfaced with the time source for test synchronization.

This project was funded under the core research programme of the University of Strathclyde's PNDC (HTTP://PNDC.CO.UK).

III. Testbed Configuration

A laboratory-based Hardware-in-the-Loop (HIL) test setup is configured to enable the demonstration of MACsec and IPsec for secure data transmission between substations, focusing on IEC61850-based SV and GOOSE messaging. The high-level test setup shown in Figure 1 while the physical implementation is shown in **Figure 2** consists of Digital Real-Time Simulator (DRTS) for IEC 61850-based SV and GOOSE data streams generation and associated faults simulations, traffic analyser, MPLS SAR routers for IP-MPLS traffic routing to the test relays, time source for synchronisation based on C37.238, and 2 IEDs (protection relays) with C37.94 interfaces, and a Maximum Transmission Unit (MTU) of 8000.

The tests involved using DRTS to simulate transmission line with fault conditions and frequency events based on IEC

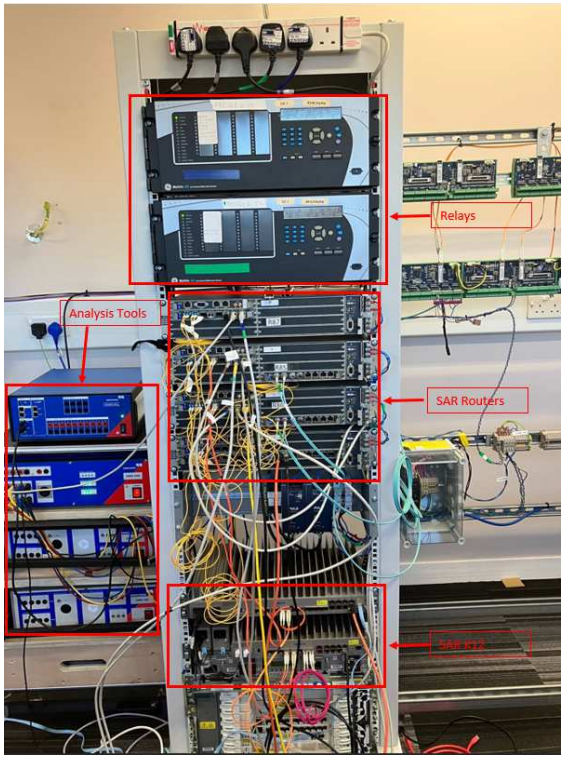

Figure 2. Physical Scheme implementation at PNDC

61850 (i.e. for layer 2 - GOOSE, SV, and layer 3 – Routable GOOSE (R-GOOSE and), and Routable Sampled Values (R-SV)). The GOOSE and SV streams generated by the DRTS are duplicated into two streams. One stream was forwarded to the IP-MPLS network whilst the other stream was timestamped for network latency measurement. The simulation parameters were based on the following:

- Line/cable type and impedance
- Nominal current magnitude and direction of flow
- Substation fault levels
- Charging current compensation
- Fault types, location and resistance, e.g phase-to-ground, phase-to-phase, three-phase

As shown in Figure 1 above, IP-MPLS packet-switched technology is used to carry IEC 61850 GOOSE and SV measurements over an Ethernet/C37.94 communication interface between the two IEDs (i.e., protection relays). As shown in Figure 4, the test network uses MPLS for traffic forwarding via the four routers configured to enable the right digital paths for the generated traffic to flow. Path one includes routers connected to test relays and security switches (K12 and K30). The other path includes routers connected to test relays via the routers on the alternative path without MACsec. The DRTS system is used to inject voltage and current to the protection relays and equally generate the power line fault for each test. Upon detection of a line differential fault, the relay issues trip signals to corresponding circuit breakers and sends a trip message to the end relay via the MPLS communication channel, fed back to the DRTS. The HIL testbed as shown in Figure 1 ensures that the relays and communication equipment are adequately interfaced and communicate with each other as expected, which helped to validate the correct functionality of the IP-MPLS hitless technology and indicate any mal-operation during the test.

Hitless technology is an IP-MPLS networking feature that enables seamless network operations in high availability and reliability for mission-critical systems. Failover enabled by hitless technology between the three paths as shown in Figure 3 is seamless because relay traffic is replicated by the IP-

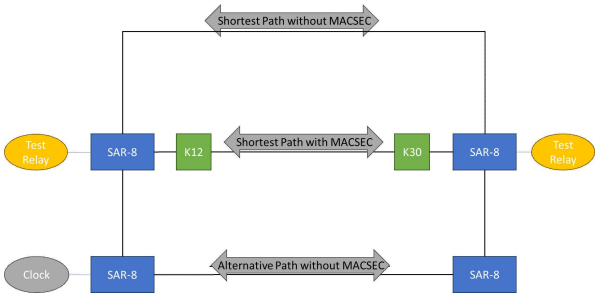

Figure 3. High-Level Test Setup for IP-MPLS SAR-8 Routing Nodes

MPLS SAR-8 routers for all active IP-MPLS paths. This ensures that the integrity of the grid is protected since the communication between the protection relays is continuously up and running without interruption due to SAR-8 routers' Asymmetric Delay Compensation (ADC) capability. The tests mainly focused on the three paths failure scenarios over layers 2 and 3 and the associated latency of recovery paths for each test to validate multipath communication requirements of IEC 61850-based protection and control function.

The core network consists of two substation LANs interconnected via an MPLS network. The IP-MPLS network illustrated in Figure 3 above is a combination of four industrial MPLS nodes configured to support the key protection services under test. That is, Protection Service 1 which carries GOOSE messages and Protection Service 2 which carries Sampled Values for direct path and multi-hop path performance tests. The primary route (shorted path) is between the test relay-connected SAR-8 routers and the secondary route (longest path) is via the clock source connected to the SAR-8 routers. For wide area testing of R-GOOSE and R-SV over layer 3, the DRTS publisher and subscriber devices were configured to be in different subnets with associated multicast IP addresses routing over the IP-MPLS test network. The Publish–subscribe approach was

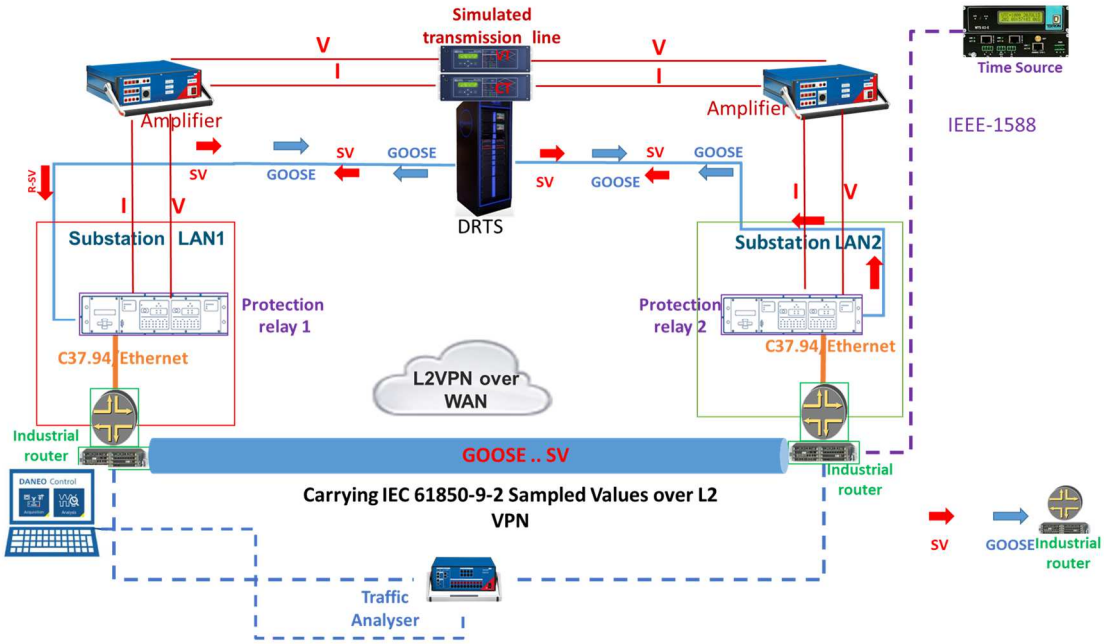

Figure 4. Secure GOOSE and SV Messages over Layer 2 VPN

employed, where publishers send messages directly to specific subscribers.

IV. Layer 2 VPN for SV and GOOSE Messages

Layer 2 Tunneling Protocols (L2TP) are used to create virtual paths between devices on substation networks and also to provide isolation between them. L2TP is used in the test as a layer 2 VPN over IP-MPS WAN configured to enhance the security of transmitted messages. The SV and GOOSE tests over layer 2 VPN (L2VPN) using a shared IP-MPLS network are shown in Figure 4. L2VPN tunnel enabled secure SV and GOOSE stream transmission between MUs and IEDs in LAN1 and LAN2 through an IP-MPLS network.

V. Layer 3 VPN for Routable SV and Routable GOOSE Messages

The test scenario that examined the routing of R-SV and R-GOOSE traffic over layer 3 is based on Internet Group Management Protocol (IGMP)-Snooping. IGMP protocol is used by routers and hosts to manage multicast group membership and multicast traffic within a LAN and equally help switches optimise the forwarding of multicast traffic. R-SV and R-GOOSE data streams are routed between substation LAN1 and LAN2 over IP-MPLS network as shown in Figure 5.

VI. Security Considerations

The analysis of the impact of MACsec and IPsec security techniques on the test network performance for transmitting SV/R-SV and GOOSE/R-GOOSE data streams over MPLS and IP-MPLS networks was evaluated. MACsec as an encryption and authentication algorithm defined by IEEE standard 802.1AE is used in MACsec-capable routers to encrypt layer 2 SV/GOOSE and layer 3 R-SV/R-GOOSE data streams. The test network configurations were implemented such that when used with security techniques like IPSec, an end-to-end of layer 2 SV/GOOSE and layer 3 R-SV/R-GOOSE attacks can be prevented.

With the MPLS routers configured to enable encrypted services between the substation LAN as shown in Figure 3, two SAR K12 switches were used to enable AES 256 bits of MACsec encryption for end-to-end security of real-time critical applications such as teleprotection. The maximum propagation delay for SV and GOOSE with MACsec encryption is 20 µs. Trip tests were performed as expected without impact on the test network while tripping a signal connected to the protection relay.

In layer 3 network, the IPSec approach is used to encrypt MPLS traffic over Wide Area Networks (WAN). The test involved tunneling layer 3 IP traffic through a layer 2 tunnel, thereby ensuring that layer 2 traffic is authenticated and encrypted using layer 3 IPsec. In this scenario, IPsec is implemented with L2TP to enhance the confidentiality inherent in the L2TP protocol and provide strong encryption mechanisms for packet transmission. L2TP and IPsec together provided a much more secure system compared with the MACsec, but it could be slower and could get blocked by firewalls if not properly configured. IPsec provided a variety of encryption features required to establish bidirectional IPsec tunnels. For the test, the authentication algorithm used is the SHA2_512_256 HMAC (256 bit) and auth-encryption of an AES256 (256 bit AES-GCM with 128 bit ICV).

For the IPSec test scenario, the transmission of R-SV/R-GOOSE over an MPLS network with data encryption and measured end-to-end packet propagation delay is demonstrated. IPSec technique was used to encrypt layer 3 traffic in MPLS Wide Area Networks (WAN). An established IPsec tunnel secures the network point-to-point connection layer 3 traffic over WAN. The test involved tunneling layer 3 IP traffic through layer 2 tunnel, ensuring layer 2 traffic is authenticated and encrypted using layer 3 IPsec. IPsec is used along with Layer 2 Tunneling Protocol (L2TP) to enhance the confidentiality inherent in the L2TP protocol and provide strong encryption or authentication for end-to-end security that authenticates and encrypts IP packets. L2TP and IPSec together improved the encryption, authentication and integrity but it can be slower than others and sometimes gets blocked by firewalls.

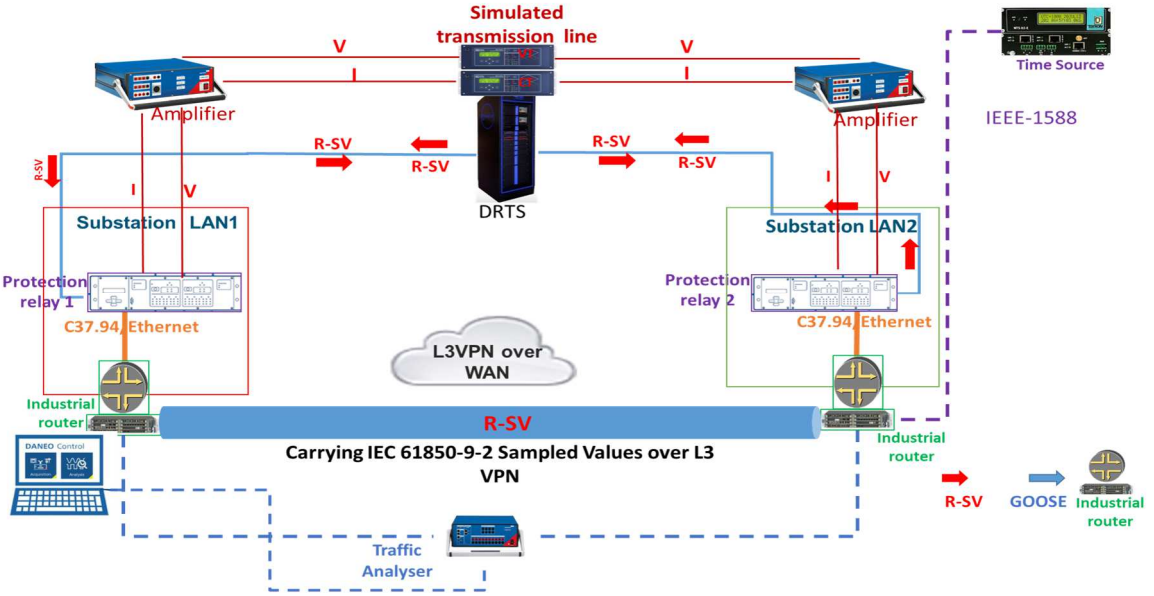

Figure 5. Secure R-SV and R-GOOSE over Layer 3 VPN

IPsec can be used to secure and encrypt L2 Tunnelling packets. The combination of IPsec and L2 VPN creates a secure channel that encapsulates L2 traffic to provide a secure solution for data transmission and ensure the confidentiality, authentication and integrity of the Layer 2 communication over the VPN connection. IPSec provides a variety of encryption features required to establish bidirectional IPSec tunnels. SHA-512 is used as a cryptographic hash algorithm for authentication to comply with the related standards (IEC 62351-6, 2020).

VII. Results and Discussion

The feasibility of layer 2 tunnelling in providing secure cost-effective and reliable connectivity between substation Ethernet LANs is demonstrated by investigating MACsec and IPsec protocols performance and compared in terms of the lowest impact on latency, ease of operation and configuration. As shown in Table 1, both MACsec and IPsec introduced approximately 20 µs of additional delay to IEC 61850-based GOOSE and SV packet propagation, with no observed impact on the test network or the packets delivered (i.e., no packet loss has been registered by the traffic analysis software used to capture the IEC 61850 GOOSE, and SV messages). Similar Propagation delay results were observed for Multi-hop (4 hops) IEC 61850 GOOSE/SV messages, with an additional delay of 20 µs to GOOSE and SV packet over layer 2 tunnelling was recorded and no impact observed on the test network.

Table 1. L2TP Propagation Delays for IEC 61850 GOOSE/SV Messages over Different Paths Direct Link

Propagation Delay	No Encryption	Encryption IPsec	Encryption MACsec
GOOSE (direct link)	59.88 µs	80.21 µs	79.3 µs
SV (direct link)	62.22 µs	81.71 µs	82.23 µs
GOOSE (Multi-hop)	61.19 µs	81.27 µs	81.05 µs
SV (Multi-hop)	63.16 µs	84.31 µs	82.87 µs

VIII. CONCLUSIONS

In this paper, GOOSE and SV transmission between simulated substations over a secure layer 2 tunnel as well as the definition of a communication architecture to enable the realisation of this communication approach for DNO have been demonstrated. The network's performance with MACsec and IPSec protocols over layer 2 tunnel for IE 61850 traffic was analysed, comparing their impact on application latency. The analysis involved securing IEC 61850 communication between substation LANs using these protocols. An AES 256 encryption type is used to secure the exchanged data between the MPLS routers (network nodes), while SHA-512 was used as a cryptographic hash algorithm for authenticating connections. Two tests were conducted to evaluate the performance of IEC 61850 over IP-MPLS in terms of propagation latency and the effects of MACsec and IPsec security techniques on the end-to-end latency for each test. The tests involved analysing the capabilities of the IP-MPLS test network to carry encrypted IEC 61850 packets over layer 2 tunneling without causing packet loss that could impact application requirements. Layer 2 tunnelling with security ensures cost-effective and reliable connectivity between substation's Ethernet LANs.

The results show that the encryption of the IEC 61850 GOOSE & SV traffics contributed approximately 20 µs to the propagation delay over Layer 2 and did not cause any issue to the power system (test network). This has been achieved for both MACsec and IPsec with SHA-512 for authentication and AES256 for encryption. Importantly, the encryption did not cause any loss of precise timing, critical for synchronization, over L2 tunneling. Because the timing source is localized by one of the routers.

Future work will evaluate the latency implication of transmitting encrypted R-SV and R-GOOSE data streams for various scenarios over layer 3 networks for IEC 61850 inter-substation communication.

Acknowledgment

The authors acknowledge the contributions of Nokia, SP Energy Networks, UK Power Networks and Scottish and Southern Electricity Networks towards the successful completion of this PNDC research project.

References

[1] K. Martin *et al.*, "An overview of the IEEE standard C37. 118.2—synchrophasor data transfer for power systems," *IEEE Transactions on Smart Grid,* vol. 5, no. 4, pp. 1980-1984, 2014.

[2] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in *2006 IEEE Power Engineering Society General Meeting*, 2006: IEEE, p. 8 pp.

[3] S. R. Firouzi, L. Vanfretti, A. Ruiz-Alvarez, H. Hooshyar, and F. Mahmood, "Interpreting and implementing IEC 61850-90-5 Routed-Sampled Value and Routed-GOOSE protocols for IEEE C37. 118.2 compliant wide-area synchrophasor data transfer," *Electric power systems research,* vol. 144, pp. 255-267, 2017.

[4] M. El Hariri, E. Harmon, T. Youssef, M. Saleh, H. Habib, and O. Mohammed, "The iec 61850 sampled measured values protocol: Analysis, threat identification, and feasibility of using nn forecasters to detect spoofed packets," *Energies,* vol. 12, no. 19, p. 3731, 2019.

[5] T. S. Ustun, S. M. Farooq, and S. S. Hussain, "Implementing secure routable GOOSE and SV messages based on IEC 61850-90-5," *IEEE Access,* vol. 8, pp. 26162-26171, 2020.

[6] H. León, C. Montez, O. Valle, and F. Vasques, "Real-time analysis of time-critical messages in IEC 61850 electrical substation communication systems," *Energies,* vol. 12, no. 12, p. 2272, 2019.