IEEE Open Access Journal of Power and Energy

Received 30 September 2022; revised 19 February 2023; accepted 6 March 2023.
Date of publication 10 March 2023; date of current version 24 March 2023.

Digital Object Identifier 10.1109/OAJPE.2023.3255790

An Effective Security Scheme for Attacks on Sample Value Messages in IEC 61850 Automated Substations

S. M. SUHAIL HUSSAIN[1,2] (Senior Member, IEEE), MOHD ASIM AFTAB[3] (Member, IEEE), SHAIK MULLAPATHI FAROOQ[4] (Senior Member, IEEE), IKBAL ALI[5] (Senior Member, IEEE), TAHA SELIM USTUN[6] (Member, IEEE), AND CHARALAMBOS KONSTANTINOU[3] (Senior Member, IEEE)

[1]Electrical Engineering Department, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran 31261, Saudi Arabia
[2]Interdisciplinary Research Center for Renewable Energy and Power Systems (IRC-REPS), King Fahd University of Petroleum and Minerals (KFUPM), Dhahran 31261, Saudi Arabia
[3]Computer, Electrical and Mathematical Sciences and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955, Saudi Arabia
[4]School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore 632014, India
[5]Department of Electrical Engineering, Jamia Millia Islamia (a Central University), New Delhi 110025, India
[6]Fukushima Renewable Energy Institute, AIST (FREA), Koriyama 963-0298, Japan

CORRESPONDING AUTHOR: S. M. S. HUSSAIN (suhail@ieee.org)

This work was supported in part by the Department of Science and Technology (DST) through Fund for Improvement of S&T Infrastructure (FIST) Project under Grant SR/FST/ETI-390; and in part by the King Abdullah University of Science and Technology (KAUST), Saudi Arabia.

ABSTRACT The trend of transforming substations into smart automated facilities has led to their swift digitalization and automation. To facilitate data exchange among equipment within these substations, the IEC 61850 standard has become the predominant standard. However, this standardization has inadvertently made these substations more susceptible to cyberattacks, which is a significant concern given the confidential information that is transmitted. As a result, cybersecurity in substations is becoming an increasingly critical topic. IEC 62351 standard provides guidelines and considerations for securing the IEC 61850 messages to mitigate their vulnerabilities. While securing Generic Object-Oriented Substation Event (GOOSE) messages has received considerable attention in literature, the same level of scrutiny has not been applied to Sampled Value (SV) messages despite their susceptibility to cyberattacks and similar frame format. This paper presents the impact of replay and masquerade attacks on SV messages. It also develops a scheme for securing SV messages against these attacks. Due to high sampling rate and time critical nature of SV messages, the time complexity of security scheme is critical for its applicability to SV messages. Hence, in this work, SV emulators have been developed in order to send these modified secure SV messages and investigate their timing performance. The results show that the proposed scheme can mitigate replay and masquerade attacks on SV messages while providing the necessary high sampling rate and stringent timing requirements.

INDEX TERMS Substation automation, IEC 61850, IEC 62351, cybersecurity, power system communication, sample values, communication protocols, hardware-in-the-loop testing.

I. INTRODUCTION

WITH the introduction of information and communication technology (ICT) for advanced control and automation of power grids, traditional power systems are transforming into smart grids. They provide various benefits such as higher efficiency, energy savings, improved quality of service, reliability, and security. Substations are a core component of grid operation. Under the smart grid paradigm, existing supervisory control and data acquisition (SCADA) systems are replaced with advanced digital communication technologies to realize substation automation [1]. In this regard, IEC 61850 has emerged as the most widely accepted communication standard [2]. The object-oriented information model and interoperable features make it effective and popular. On the other hand, this standardized communication makes substations more vulnerable to cyberattacks [3]. In recent years, reports of cyberattacks on control and automation units of power systems to

disrupt power supplies and force blackouts are on the rise [4], [5].

Researchers have been actively investigating the field of cyberattacks on IEC 61850 substation automation systems (SAS), which is still emerging and growing [6], [7], [8]. In [6], the authors discussed the impact of cyberattacks and potential exploits in SAS. In [7], authors developed an active command mediation defense (A∗CMD) solution as an additional layer of security in gateways. With A∗CMD, all the commands (i.e., messages) are artificially delayed until each message is scrutinized by some attack detection system. However, such a system is very complex to design and depends heavily on external attack detection systems for identification. Furthermore, such a system is designed for securing messages coming from outside the substation.

IEC 61850's Generic Object-Oriented Substation Event (GOOSE) and Sampled Value (SV) messages are layer 2 messages. These messages are sent within substations LAN. Since these messages were initially developed for LANs behind gateways and firewalls, no security mechanisms were defined by IEC 61850. It has been noticed that the GOOSE and SV messages are also vulnerable to cyberattacks and many attacks have been reported in literature [6], [8].

IEC 62351 standard was developed by the TC57 committee to provide security recommendations for different power automation standards including IEC 61850. IEC 62351 standard complements the IEC 61850 standards by providing the necessary security recommendations for securing them against cyberattacks. Part 3 and 4 of IEC 62351 standard provides guidelines for securing the IEC 61850 Manufacturing Message Specification (MMS) messages [9]. On the other hand, part 6 provides the security guidelines for securing GOOSE and SV messages [9]. In literature, a lot of studies focus on securing GOOSE [10], [11], and MMS messages [12]. Previous studies showed that a single contaminated GOOSE message can result in successful maloperation of breakers and have severe consequences on SAS performance [13]. Due to its quite evident vulnerability, much research attention was focused on securing GOOSE messages. GOOSE and SV messages have similar multicast Ethernet frame format. The impact of cyberattacks on SV messages has not been investigated in depth. This paper addresses this gap, by demonstrating the impact and consequences of replay and masquerade attacks on SV messages.

Furthermore, in literature very little attention has been given regarding the design of security mechanisms for SV messages against replay and masquerade attacks. In [14], the authors developed neural network forecasters to detect spoofed SV messages. This detection technique is based on comparing the measured data values received in the SV message with the neural network based forecasted values. In [15], the authors developed network based integrated anomaly detection system for multicast SV messages. Anomaly detection system used different parameters of SV message, such as sample count (*smpCnt*), as violation indicators. However, these works do not discuss any security mechanism at protocol or data link layer level. In [16], the work proposed distributed intrusion mechanism utilizing RSA based digital signatures for SV messages. However, it has been observed that the processing times required for generating and verifying RSA based digital signatures is on the order of few milli seconds and would not be suitable for both high sampling rate IEC 61850-9-2 LE SV and time critical GOOSE messages [10]. SV messages have a high sampling rate and their computational processing times are even more stringent. The previous works on SV security do not present the evaluations on computational complexity of the security schemes and its applicability to time critical SV messages. Recently, in [17] and [18], the authors presented a Message Authentication Code (MAC) based security scheme for SV messages. However, the security scheme proposed in [17] and [18] does not provide confidentiality of data, and the security scheme in [17] is prone to replay attacks. In [19], the authors have proposed use of Advanced Encryption Standard with Galois/Counter Mode (AES-GCM) algorithm for securing the GOOSE and SV messages. Furthermore, in [19], authors presented the performance evaluation of AES-GCM algorithm over a powerful FPGA platform. However, the legacy intelligent electronic devices (IEDs) in substations may have low computational capacities. Hence, an investigation of the security schemes for SV messages on low computing platforms is required to test its applicability.

In this regard, this paper presents a holistic security scheme based on IEC 62351:2020 recommended MAC and encryption algorithms to secure SV messages. Furthermore, a C-language based SV emulator 'S-SV' is developed to publish these secure SV messages. The result of lab tests on practical processing times for generating SV messages with proposed security mechanisms on low computing platforms is presented. The major contributions of this paper are the following:

1) Investigation of impact and consequence of replay and masquerade attacks on SV messages through real time hardware-in-the-loop (HIL) experiments.
2) Proposed a holistic security scheme for SV messages using authentication value and encryption algorithms against different security attacks.
3) Open-Source framework 'S-SV' for generating SV messages with proposed security scheme is developed.
4) Experimental evaluation of the computational performance of proposed security scheme to test its applicability to SV messages.

The rest of the paper is organized as follows. Section II demonstrates the impact of replay and masquerade attacks on SV messages. Section III presents proposed security scheme for securing SV messages. Section IV presents the performance evaluation and applicability of proposed security scheme to SV messages. Finally, section V presents the conclusions.

II. THREAT MODEL AND IMPACT OF CYBERATTACK ON IEC 61850 SV STREAMS

A SAS consists of various IEDs such as merging unit (MU) IED, protection and control (P&C) IED and breaker IED. MU is the primary equipment in process level and receives the voltage and current samples from the instrument transformer and converts them into a digital data packet to be communicated to other IEDs. These digital packets are formed according to the guidelines set forward by IEC 61850-9-2 standard, known as SVs. The SV stream is time-synchronized and stamped at the MU and is sent to the P&C IED. The P&C IED is responsible for carrying out control and protection functions by taking values from the MU IED. The P&C IED then sends a signal to the breaker IED for isolating the faulty portion. The breaker IED is a circuit controlling device that controls and monitors the status of the circuit breaker.

A. ADVERSARIAL MODEL OF CYBERATTACKS

The threat model of a cyberattack in a SAS is presented in this section. The engineering and operator workplace of a SAS is designed using human machine interface (HMI) to provide a graphical interface to the operating personnel for monitoring and controlling devices. Although the operator workplace has restricted access, the engineering workstations may have remote access facilities to allow access through corporate offices and control centers [20]. This makes the substations a soft target for the adversaries to infiltrate and gain unauthorized access. Also, cyberattacks on the SAS could originate from operator personnel who have access to the substation communication network (SCN). These personnel can infect the substation infrastructure with malware, intentionally (e.g., disgruntled employee) or unintentionally (e.g., improper usage of infected devices), and can compromise the cybersecurity of the substation. Moreover, cyberattacks can originate from the supply chain where malware contamination occurs during the production phase of IEDs [21].

Based on any of the scenarios, the intruders can gain a foothold in the substation network and can launch several cyberattacks as in the case of Ukraine's power grid attack [22]. After gaining access to the SCN, an intruder having no login credentials can hijack the valid credentials of legitimate personnel while they log into their system. The attack models for IEC 61850 SAS have been developed in [14], [23], and [24]. Once into the SCN, the intruder can gain knowledge about topology of substation, and the IED's information along with their login credentials. Thus, the intruder can now launch an attack on any IED of the SCN. A generalized adversarial model of cyberattack is shown in Fig. 1. It shows the control diagram of a SAS system considered in this paper under cyberattack from an intruder [25].

The test system receives measurements from current transformer (CT) and potential transformer (PT) which are

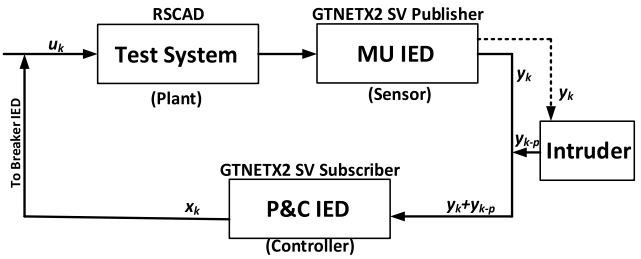

FIGURE 1. **Schematic diagram of adversarial model for the cyberattack.**

then used as input to the MU IED, which acts as a sensor. As illustrated in Fig. 1, the intruder can access the true observations from the sensor (IEC 61850-9-2 SV from the MU IED). This access is assumed to be for a finite duration but for a sufficiently long-time interval and after capturing these observations, they can be used at a later point in time. The IEC 61850-9-2 SV stream is received by the P&C IED. Under the attack, the true values y_k are replaced by a stream of values $y_k + y_{k-p}$, where y_{k-p} are the values at an unknown but definite time delay. The values y_{k-p} are older observations captured by the intruder for a finite time interval during normal or faulty system state. It has been assumed that noise signals (process and observation) are zero.

Under practical situations, the time instant p depends on when the system is compromised by the intruder. The intruder need not have any information about control logic for launching the cyberattack of the considered adversarial model. The intruder can read and modify the SVs generated from the MU IED in the SAS. Based upon the modified streams to the P&C IED, the decision 'x_k', whether to trip or not trip, is transferred to the Breaker IED as per (1)

$$x_k = \begin{cases} 0, & Notrip \\ 1, & Trip \end{cases} \tag{1}$$

The intruder can perform two main types of attacks on SVs, i.e., replay and masquerade attacks which are examined in the next subsection.

B. REPLAY AND MASQUERADE ATTACKS IN SAS

In a replay attack, the intruder eavesdrops on an SCN and captures an SV message packet with the current and voltage samples during normal operation. The intruder then replays the captured packets into the SCN during a fault. This causes the relay to receive normal values of current and voltage during the fault. This would make the relay to keep the circuit breaker closed even though the fault is present. The fault level could rise tremendously, and the system could even crash. This would lead to huge equipment damage, service interruptions and could tamper the system stability.

In a masquerade attack, the intruder gains access to the SCN by taking a false identity and reads an SV message packet and intercepts it to change or modify the measured values. This would result in complete tampering on the

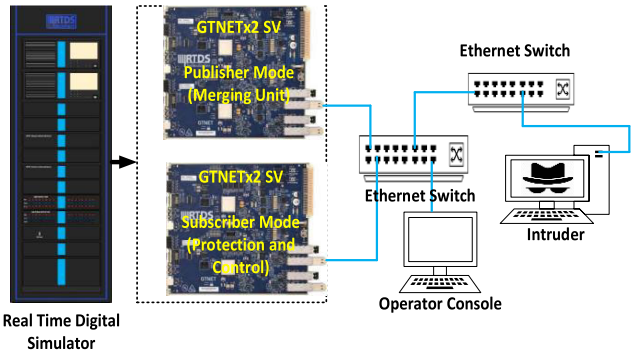

FIGURE 2. Hardware-in-the-loop (HIL) test setup for cyberattack tests.

original SV packet. The modification in measured values lead to distortion in waveform received at the relay. An adversarial attacker may tamper the SV data such that the relay algorithm gives unexpected outputs and in turn could lead to detrimental effects.

The replay and masquerade attacks are carried out on a test SCN developed in RTDS environment for validating the attacks and their consequences in the next subsection.

C. VALIDATION OF RESULTS BY RTDS EXPERIMENTS

1) HARDWARE-IN-THE-LOOP (HIL) SETUP

For realizing the cyberattacks on a SAS feeder, an experimental HIL setup has been developed in the laboratory as shown in Fig. 2. The developed test system represents an 11kV feeder that supports a dynamic load. The substation feeder setup is developed in RSCAD as shown in Fig. 3. The simulation is carried out with and without fault for studying the consequences of different cyberattacks. In one of the feeders, a CT and PT are connected to acquire the current and voltage values. The GTNETx2 card is configured to send and receive SV according to IEC 61850-9-2 LE standard, henceforth referred as 9-2 LE. To mimic the behavior of a MU, the GTNET SV card is used in publisher mode which generates SV according to the current and voltage signals. MU receives current and voltage values from CT and PT at a sampling rate of 80 samples per cycle. According to 9-2 LE each SV packet contains one set of values for current and voltage [26]. Hence, 9-2 LE MU sends 4000/4800 SV packets per second for 50/60 Hz system. The circuit breaker in the feeder mimics the operation of Breaker IED.

The P&C IED receives SV stream at 4000/4800 packets per second. The protection algorithm in commercial P&C IEDs normally operate with sample rate of 8 to 12 times a cycle [27]. In RTDS, the protection algorithms in relays are modeled to operate with sample rate of 10 samples per cycle [28]. Hence, the P&C IED averages eight consecutive SV messages to get 10 current and voltage samples per cycle. The protection algorithm calculates current and voltage phasors for each cycle using these 10 averaged values. The P&C IED, then, compares these phasor values of currents and voltages with the permissible values to detect a fault condition. If a fault is detected, it sends a command to the Breaker IED for isolating the fault. In the test system, the P&C IED is realized using GTNET SV card in subscriber mode along with an Overcurrent (OC) relay to send trip signal as shown in Fig. 3.

2) TESTS FOR REPLAY AND MASQUERADE ATTACKS

To study the implications of cyberattack, fault and non-fault scenarios are developed in HIL tests. Based on these, there are various possible scenarios in which an intrusion can occur.

a: FAULTY SV PLAYBACK DURING NORMAL CONDITIONS

In this scenario, the intruder sends SV streams, recorded when fault is present, which leads to detection of a fault by the relay. GTNET uses the destination multicast address of the SV packets to identify the intended SV stream, and since the replayed SV message are captured at the same feeder, the destination multicast address remains unaltered. The P&C IED reads the replayed or tampered message and sends the signals in the form of current to the overcurrent relay.

In order to monitor the consequences of replaying a series of messages, an intrusion is carried by replaying a single SV packet from the SV stream. In the HIL setup, the intruder sends one intruded SV packet to the same relay. Figure 4 shows the Wireshark capture at the P&C IED in RTDS. It can be noticed that old SV message with smpCnt 3561 (frame 21) is the replayed while current value smpCnt counter is 3743. Since the sampling rate of relay is 10 samples per cycle, it averages eight SV messages to a single value of current and voltage [27], [28]. Hence, when a single faulty SV is replayed no disturbance is noted as shown in Fig. 5(a). The intruded SV packets are increased from one to twenty-five, a disturbance is noted as shown in Fig. 5(b). In another scenario, the intruded SV packets are continuously sent, this resulted in a continuous disturbance as shown in Fig. 5(c). It is observed that the P&C IED detected the change when there are more than nine SV messages as shown in Figs. 5(b) and 5(c). The intrusion is detrimental if faulty SV messages are replayed at least for one cycle (i.e. 80 SV messages are replayed). The OC relay detected the condition as a fault, when more than eighty fault condition SV streams are intruded during normal scenario. The consequence can be maloperation of protection scheme, unnecessary tripping of circuit breakers, unnecessary isolation of a healthy power system, all of which affect system stability.

b: NORMAL SV PLAYBACK DURING FAULT CONDITIONS

Generally, once a fault is detected by the relay it opens the circuit breaker thereby isolating the faulty portion. In this scenario, maloperation in the system occurs, when circuit breaker is erroneously closed while the fault is not yet cleared. The intruder replays the SV stream captured during healthy operation of feeder (i.e., normal condition) when fault is still present. Based on this intruded SV stream, relay closes

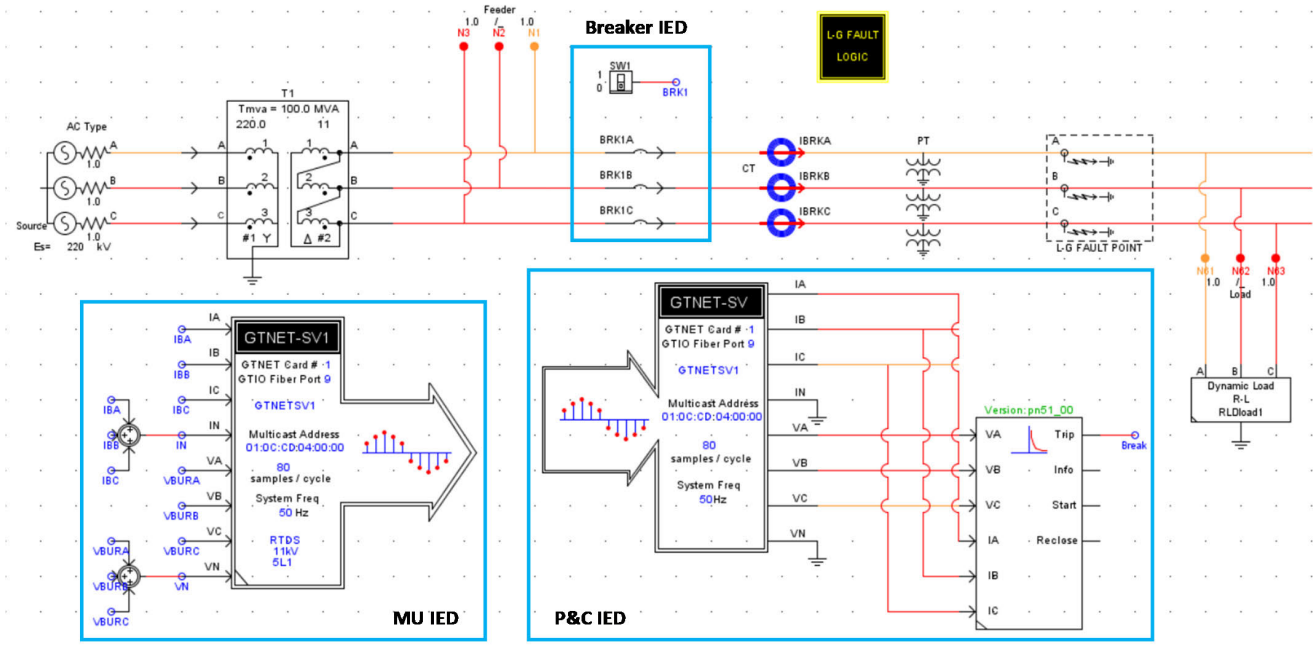

FIGURE 3. **RSCAD simulation setup.**

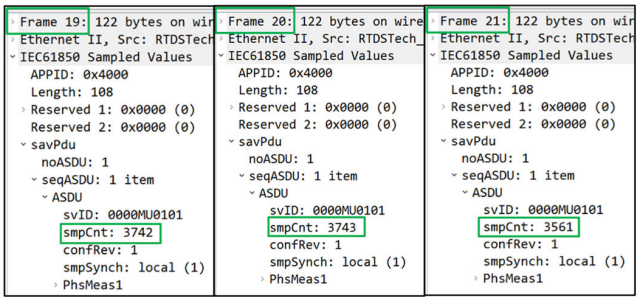

FIGURE 4. **Wireshark capture at P&C IED in RTDS during replay attack.**

the circuit breaker contacts even though there is still a fault present in the power system. This is a more serious condition as compared to the former. Closing a circuit during fault condition could result in multiple equipment failures and a blackout. This scenario is realized in the same manner as discussed in the previous section. The intruder replays more than eighty SV samples of healthy operation during the LG fault in the system. The P&C IED sends healthy current and voltages to OC relay and the circuit breaker is closed on a fault situation leading to maloperation of protection scheme.

c: MASQUERADE ATTACK DURING NORMAL OPERATION

On similar lines, masquerade attack is also replicated on the hardware setup. The captured SV stream by the intruder is modified and tampered to change its measurement data and smpCnt values. For implementing masquerade attack, the modified SV packets with current value equal to five times the normal values and high smpCnt value are continuously sent. This resulted in a continuous disturbance with high current values at P&C IED as shown in Fig. 6 resulting in maloperation of relays. Wireshark capture at the P&C IED during masquerade attack is shown in Fig. 7. It can be noticed from Fig. 7 that frame 21 is a modified SV packet having high smpCnt value. The masquerade attack is realized by sending the tampered packet stream in the SCN by the intruder. Overall, it is found that the conventional IEC 61850-9-2 SV is vulnerable to replay and masquerade attacks.

III. SECURITY SCHEME FOR IEC 61850 SVs

In this section, a cybersecurity solution is proposed to mitigate the replay and masquerade attacks on SV messages. In masquerade attack, the attacker can inject packets with modified contents. Hence, for mitigating the masquerade attacks the proposed mechanism in this paper employs the IEC 62351-6 recommended authentication value extension and encryption of SV APDU in SV messages.

IEC 62351-6:2007 recommends use of RSA based digital signatures as authentication value. The processing time (generation and comparison) of RSA based digital signatures is 2-3 msec. Hence, it is clearly not suitable for SVs. Alternatively, MAC algorithms can be used for generating this authentication value as MAC algorithms are lightweight and have comparatively low computational times [11]. In the proposed mechanism, different MAC algorithms recommended in the recently published IEC 62351-6:2020 are used for generating the authentication value. These algorithms and their corresponding sizes of MAC values are given in Table 1. Furthermore, Advanced Encryption

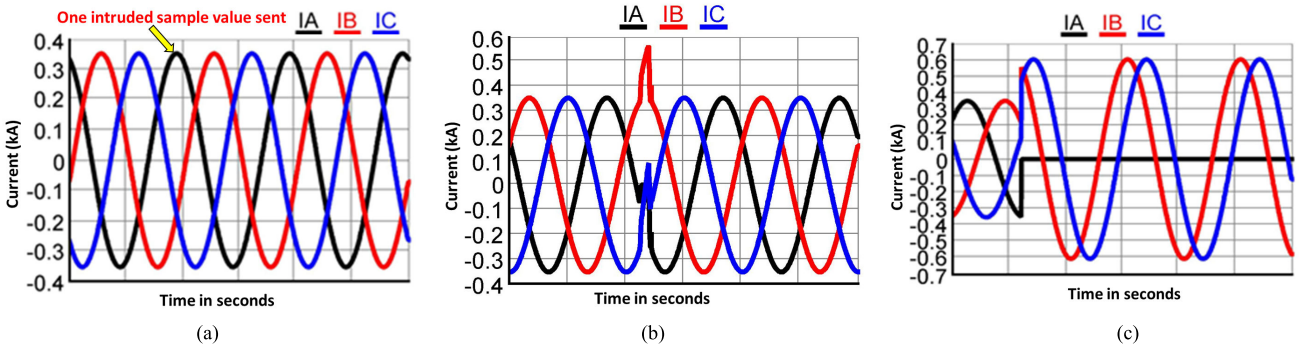

FIGURE 5. Current waveform when (a) a single faulty SV packet was replayed, (b) 25 faulty SV packets replayed, and (c) faulty SV packets replayed continuously.

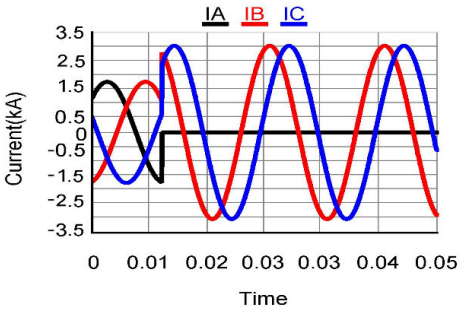

FIGURE 6. Current waveform during masquerade attack.

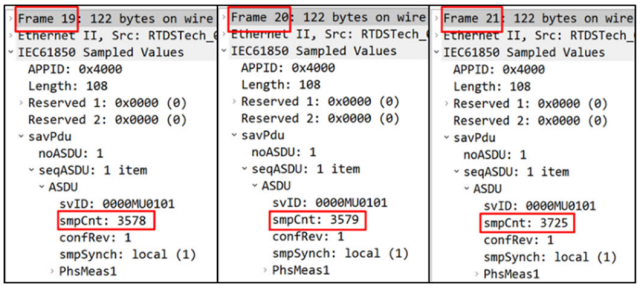

FIGURE 7. Wireshark capture at P&C IED in RTDS during masquerade attack.

TABLE 1. MAC algorithms recommended in IEC 62351-6.

MAC Algorithm	Hash Function	*MAC* value (bytes)	*Initialization Vector* (bytes)
HMAC-SHA256-80	SHA-256	10	-
HMAC-SHA256-128	SHA-256	16	-
HMAC-SHA256-256	SHA-256	32	-
AES-GMAC-64	-	8	4
AES-GMAC-128	-	16	8

Standard with Galois/Counter Mode 128/256 (AES-*GCM-128/256*) algorithm is employed for encrypting the SV APDU.

The SV APDU is encrypted using the AES-GCM-128/256 algorithm. The authentication value generated for SV message is appended to SV PDU as *Extension* field,

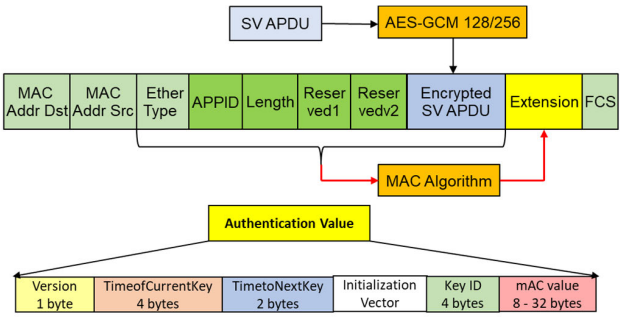

FIGURE 8. Extended frame format of SV message with security extensions.

as shown in Fig. 8. This authentication value (i.e., MAC value) is calculated for SV PDU starting from *Ethertype* field till the end of encrypted SV APDU. The length of *Extension* field appended to the SV PDU is added to the 2nd byte of *reserved1* field of SV PDU. The *reserved2* field contains the CRC value of the first 8 bytes of the SV PDU (i.e., *Ether-type*, *APPID*, *Length* and *reserved 1* fields).

At the publisher, while formatting the SV packets, first the SV APDU is encrypted and then MAC value is generated and added to the *extension* field. Any of the algorithms listed in Table 1 can be used for MAC value generation. The publisher sends the secure SV packets. Upon receiving the secure SV packet, the subscriber IED reads the MAC value in *extension* field and stores it in *m1*. Next, the MAC value for the SV PDU of the received packet is calculated as *m2*. If *m1* matches with *m2*, the packet is considered to be legitimate, and the encrypted SV APDU is decrypted and processed further. Otherwise, the packet is discarded as the MAC value mismatch indicates that at least one of the received encrypted SV PDU or MAC value is tampered. The proposed security mechanism for SVs against masquerade attacks is depicted in red font in the flowchart as shown in Fig. 9.

The MAC and AES-GCM encryption algorithms require a secret key to be pre-shared between the subscriber and publisher. In SAS, the communication network is LAN and spread over a small distance. Hence, the secret keys can be physically installed in all IEDs. Alternatively, key

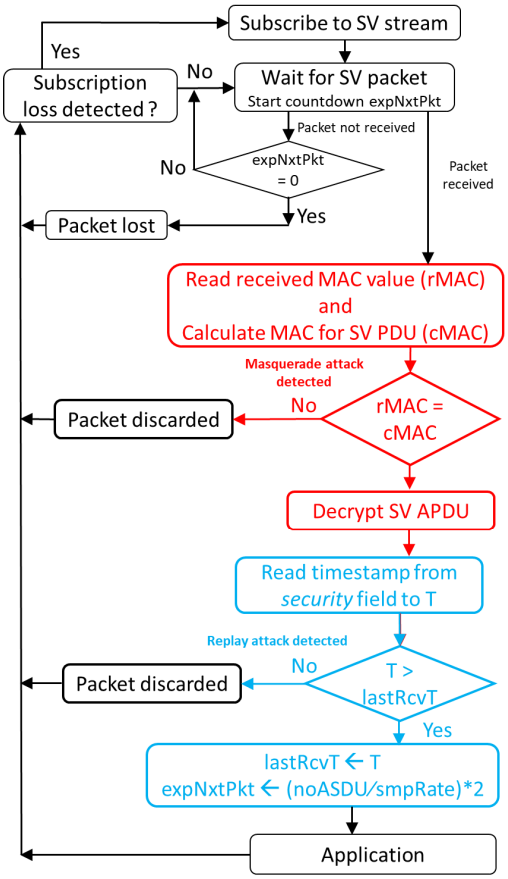

FIGURE 9. Flowchart for the proposed security mechanism for SVs.

distribution center (KDC) concept where a trusted center with authority to allocate and revoke keys for IEDs can be utilized. The key distribution via KDC is accomplished in two steps. First, all the subscribers and publishers obtain digital certificates (X.509) using Secure Certificate Enrollment Protocol (SCEP) and/or Enrolment over Secure Transport (EST) protocols from a Certificate Authority (CA). Secondly, the publisher/subscriber establishes a secure communication channel with the KDC using Transport Layer Security (TLS). The publisher/subscriber using its digital certificate (issued by CA) generates a signature and sends it to KDC along with a request to share the secret key. The KDC verifies the signature and certificate used to generate it via Online Certificate Status Protocol (OCSP) to validate if the certificate is valid and legitimate. Upon verification, the KDC shares the secret key to the publisher/subscriber via the same established TLS channel. Typically, secret symmetric keys used for generating MAC values may be valid for about 36 hours before they are changed [29]. The KDC communicates new keys to the IEDs with additional information about the time till the current key is valid and time to the next key. Prior to expiry of current key, IEDs may request KDC to allocate new key without any hinderance to application traffic. The guidelines and recommendations for procedures and formats for key exchanges between KDC and IED are discussed in [29].

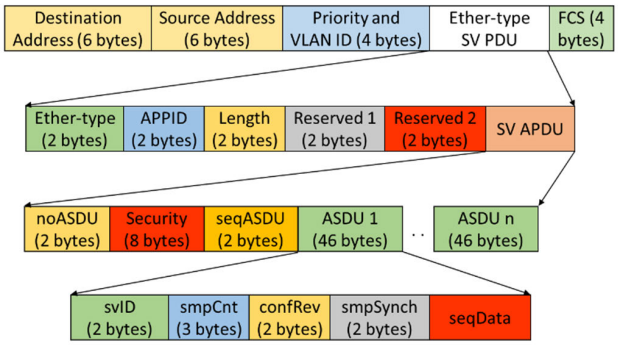

FIGURE 10. Frame format of IEC 61850-9-2 SV.

However, the above discussed authentication value extension and encryption of SV message is still prone to replay attacks. In GOOSE messages, replay attacks can be easily identified by comparing the values of *stNum* and *sqNum* fields of current GOOSE message with the last received GOOSE message. The *sqNum* value is incremented for every new GOOSE message. Whereas *stNum* value is incremented when there is change in data set information i.e., when a new event occurs. When the *stNum* is incremented, the value of *sqNum* is reset to 0. Hence, any replay attack in GOOSE messages can be easily identified by comparing the *stNum* and *sqNum* values of current GOOSE message with previous GOOSE message. In SV message, the *smpCnt* field is incremented for every new SV message and its value is reset to 0 every second. The *smpCnt* value in SV message is like *sqNum* value of GOOSE message. However, the SV message doesn't contain a value similar to *stNum* in GOOSE message. As the *smpCnt* value resets every second, it is alone not enough to identify replay attack in SV messages.

The IEC 61850-9-2 SV APDU contains an optional field *Security* which is reserved for future definition and use. *Security* field is utilized to contain the timestamp, i.e., the time, at which the SV frame is formatted. The timestamp has a size of 8 bytes and its value shall be encoded as per RFC 1305. The frame format of SV with security field of 8 bytes is shown in Fig. 10. *Security* field timestamp value along with *smpCnt* value is utilized to identify replay attacks in SV messages in the proposed security scheme.

In the proposed security scheme, each SV packet, now, contains the time at which the packet is created in the *Security* field. The subscriber IED maintains a record of 2 variables 'last received timestamp' (*lastRcvT*) and the expected delay for next packet (*expNxtPkt*). The subscriber IED, upon receiving the first SV packet, sets the value of '*lastRcvT*' to timestamp value taken from the security field of the received SV packet. And '*expNxtPkt*' is calculated as per (2) with the information of number of ASDU (*noASDU*) and sampling rate (*smpRate*) obtained from the received SV packet.

$$expNxtPkt = \left(noASDU \,/\, smpRate\right) * 2 \qquad (2)$$

TABLE 2. Security requirements of different attacks and proposed security scheme.

Attacks	Security requirements	Proposed Security Scheme
Replay	-	☑ by adding timestamp to SV APDU
Unauthorized tampering (masquerade)	Message Authentication and integrity	☑ by employing authentication value using MAC algorithms
Unauthorized access or theft of information	Message confidentiality	☑ by employing encryption for SV APDU
Man-In-The-Middle	Message Authentication	☑ by employing authentication value using MAC algorithms
Spoofing and False Data Injection attacks	Message Authentication and confidentiality	☑ by employing authentication value using MAC algorithms and employing encryption

'*expNxtPkt*' is the time for which the subscriber waits to receive the next SV packet before assuming that the packet is dropped or lost. The subscriber discards the packet if it arrives after '*expNxtPkt*' has elapsed, deeming the packet is no longer required. If the packet is received before the expiry of '*expNxtPkt*', it is processed further and checked for a possible replay attack. The timestamp value (i.e., value in security field) of the received SV packet is compared with '*lastRcvT*' value. If the timestamp value of the received SV packet is less than or equal to '*lastRcvT*', replay is detected, and the packet is discarded. If the value is greater, the SV packet is processed further and '*lastRcvT*' value is updated with timestamp value (i.e. value in security field) of the current SV packet.

The proposed security scheme against both replay and masquerade attack in SV messages is depicted in the flowchart as shown in Fig. 9. The proposed security mechanism meets message authentication, integrity, and confidentiality requirements. Moreover, the proposed security mechanism is also effective in providing security against other attacks such as unauthorized access of information, spoofing attacks, false data injection attacks, Man-In-The-Middle attacks, etc. Table 2 describes the security requirements for different attacks and how the proposed security scheme address it.

IV. PERFORMANCE EVALUATION OF THE SECURITY SCHEME

In this section, experimental evaluations are carried out to test the applicability of the proposed security scheme to SV messages.

According to IEC 61850-9-2 LE guidelines, the SAS protection functions require the current and voltage samples at the rate of 80 samples/cycle. Each SV packet contains a set of voltage and current values. Hence, the SV packets are multicast at 4000/4800 packets per second for 50/60 Hz systems. The interarrival time between two consecutive SV packets is 0.25/0.2ms for 50/60 Hz systems, assuming the

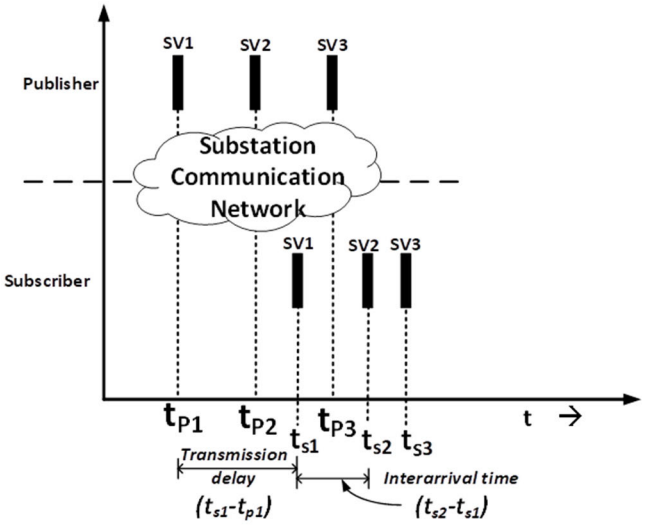

FIGURE 11. Illustration of interarrival time and transmission delay of SV messages.

jitter in substation communication network is negligible or zero. This implies that both at publisher and subscriber, each SV packet must be processed within this time frame. The additional security mechanisms must also be completed within this time frame. If each SV packet takes longer than 0.25/0.2ms to process, the maximum number of packets that the publisher/subscriber can handle per second will drop below 4000/4800. As a result, the system will process fewer SV messages per second, which can have a detrimental effect on the performance of the protection function. Fig. 11 depicts the interarrival time of an SV stream.

Total End-to-End (ETE) transmission time for SV messages for implementing protection functions of performance class P1 and P2/3 is 10 and 3ms, respectively [30]. The transmission time is the time required to transfer a message including the processing time at both ends. The transmission time starts as soon as the publisher puts SV application data on the protocol stack and ends when the subscriber extracts data from the protocol stack. Hence, the transmission time includes processing time delays at both ends, propagation time delays in communication links, processing, and queuing time delays in intermediate switches.

The proposed additional security mechanisms on SVs must adhere to the above discussed timing requirements for successful practical implementation. In order to evaluate the performance of proposed security mechanism, SV emulator framework 'S-SV' is developed in this paper [31]. 'S-SV' framework is developed in C-language using openSSL libraries and is capable of publishing and subscribing SV packets with proposed security mechanisms.

An experimental setup consisting of two terminals running 'S-SV' framework and connected via switch is considered as shown in Fig. 12. One terminal act as SV publisher while the other acts as SV subscriber. In this paper, it is assumed that both the publisher and subscriber already have the secret

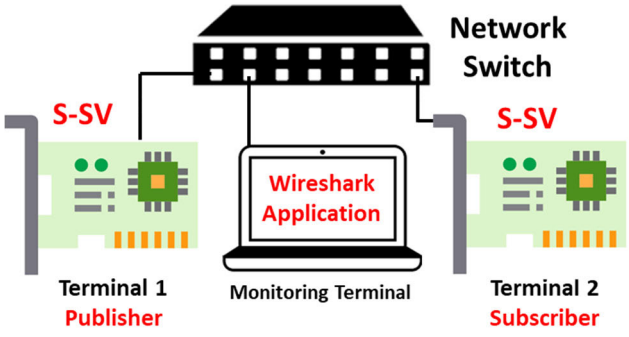

FIGURE 12. **Experimental test setup.**

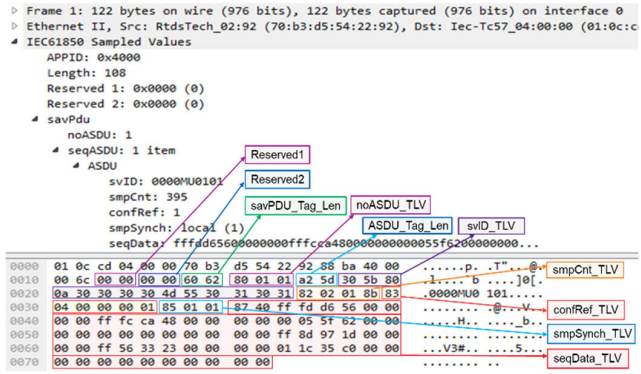

FIGURE 13. **Wireshark capture of normal SV packet published by S-SV.**

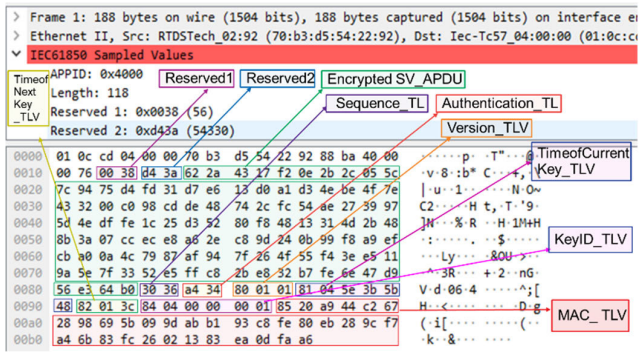

FIGURE 14. **Wireshark capture of secure SV packet published by S-SV framework.**

keys available. The Wireshark capture of normal SV frame generated by 'S-SV' when no security mechanism is applied is as shown in Fig. 13.

'S-SV' generates secure SV frames by encrypting the APDU and adding the *Security* and *Extension* fields at the SV frame. The current terminal time in NTP format (i.e., as a 64-bit unsigned fixed-point number, in seconds relative to 0h on 1 January 1900) is added to the *Security* field. The MAC value of SV PDU is calculated using any one of the algorithms listed in Table 1 and added to *Extension* field. For encryption of the SV APDU AES-GCM-128/256 algorithm is employed. Figure 14 shows the Wireshark capture of secure SV frame with security modifications proposed in section III. It can be noticed that the secure SV frame has a *Security* field of 8 bytes

TABLE 3. **Computational processing times for encryption and decryption of SV APDU.**

Algorithm / Processor	Computational processing times (ms)			
	AES-GCM-128		AES-GCM-256	
	Encryption	Decryption	Encryption	Decryption
Celeron	0.00692	0.00572	0.00800	0.00592
Raspberry pi	0.02084	0.01992	0.02212	0.02052

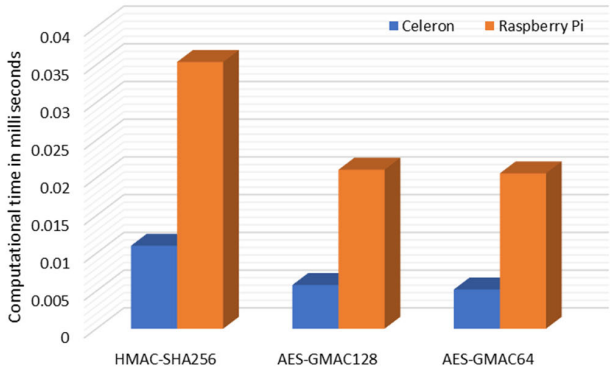

FIGURE 15. **Computational processing times for different MAC algorithms.**

and *Extension* field as described in Fig. 10 appended at the end of SV frame. Also, the SV APDU field is encrypted.

To observe timing performance, the computational times required for generating SV messages with security extensions are calculated. This is done by sampling the CPU times at the start and end of codes in C program using the clock() functions of sys/time.h header files. In this work, two test systems are considered, 1. Raspberry Pi 4 Model B platform with Broadcom BCM2711 Quad core Cortex-A72 (ARM v8) 64-bit processor and 2. Intel(R) Celeron (R) with 4GB RAM both running Ubuntu 18.04 LTS operating system and 'S-SV' library with GCC compiler. This slow system is intentionally selected for experimental analysis as the latest commercial SV publishers (merging units) and SV subscribers (protection and control relays) have much higher processing capabilities [32]. If the proposed scheme can meet strict timing requirements in the test setup, it can easily be deployed in these faster units. Figure 15 shows the computational processing times for generating authentication values for different MAC algorithms using Raspberry Pi 4 and Celeron processors. Similarly, the computational processing times for encrypting and decrypting the SV APDU for AES-GCM-128/256 algorithms using Raspberry Pi 4 and Celeron processors are shown in Table 3.

Table 4 lists the computational times obtained for processing the SV frames, generating MAC values for different MAC algorithms, and encrypting the SV APDU at publisher using Raspberry Pi 4. It also lists the times obtained for processing the received SV frames, regenerating the MAC values for different MAC algorithms, and decrypting the SV APDU at the subscriber side. Furthermore, Table 4 shows the size of secure SV frames obtained from S-SV

TABLE 4. Processing and communication delays for Secure SV frames for different MAC algorithms.

MAC Algorithm	Size of SV frame (bytes)	Throughput in Mbps	Communication delay (ms)	Processing delays (ms)								Total ETE delay (ms)
				Publisher				Subscriber				
				Processing stack	MAC value generation	Encryption	Total processing delay	Processing stack	MAC value generation	Decryption	Total processing delay	
No Security	122	4.6848	0.0026	0.0240	-	-	0.024	0.0230	-	-	0.023	0.0496
HMAC-SHA-256	188	7.2192	0.0037	0.0252	0.0353	0.0221	0.0826	0.0250	0.0353	0.0205	0.0808	0.1671
HMAC-SHA-128	172	6.6048	0.0034	0.0248	0.0353	0.0221	0.0822	0.0245	0.0353	0.0205	0.0803	0.1659
HMAC-SHA-80	166	6.3744	0.0033	0.0241	0.0353	0.0221	0.0815	0.0238	0.0353	0.0205	0.0796	0.1644
AES-GMAC-128	182	7.1424	0.0036	0.0252	0.0211	0.0221	0.0684	0.0248	0.0211	0.0205	0.0664	0.1384
AES-GMAC-64	170	6.0648	0.0034	0.0249	0.0206	0.0221	0.0676	0.0245	0.0206	0.0205	0.0656	0.1366

TABLE 5. Inter-arrival times for different number of SV streams and computational times of proposed security algorithms.

Platform		Raspberry pi					Celeron				
Security algorithms	Encryption	AES-GCM-256					AES-GCM-256				
	MAC	HMAC-SHA256	HMAC-SHA256-128	HMAC-SHA256-80	AES-GMAC128	AES-GMAC64	HMAC-SHA256	HMAC-SHA256-128	HMAC-SHA256-80	AES-GMAC128	AES-GMAC64
Processing time for each packet (ms)		0.0808	0.0803	0.0796	0.0664	0.0656	0.0169	0.0166	0.0163	0.0117	0.0111
No. of SV streams (inter-arrival time in ms)	1 (0.2)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	2 (0.1)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	3 (0.067)	×	×	×	✓	✓	✓	✓	✓	✓	✓
	5 (0.04)	×	×	×	×	×	✓	✓	✓	✓	✓
	10 (0.02)	×	×	×	×	×	✓	✓	✓	✓	✓
	15 (0.013)	×	×	×	×	×	×	×	×	✓	✓

* × denotes processor is not capable to support SV streams for given encryption and MAC algorithm. ✓ denotes processor can support the SV streams for given encryption and MAC algorithms.

implementations when different MAC algorithms are applied. The application of security mechanisms results in almost 50% increase in SV frame length. This also results in a 50% increase in throughput on the communication links. The throughput in Mbps for secure SV frames generated by different MAC algorithms is also shown. In order to calculate the communication delays for secure SV packets, substation communication network simulation is carried out in Riverbed Modeler network simulator tool. The process bus for a bay of typical D2-1 type substation consisting of a merging unit, protection IED and breaker IED connected through 100 Mbps ethernet links is simulated in Riverbed Modeler. SV traffic along with typical background traffic for a bay of substation communication network is set in simulation. The communication delays for exchanging different secure SV messages are obtained. From Table 4, it can be observed that the highest communication delay is with HMAC-SHA-256 algorithm while the lowest is with HMAC-SHA-80 algorithm.

Finally, from Table 4 it can be observed that the processing time delays at both the publisher and subscriber for processing secure SV frames for different MAC algorithms is less than the 0.2ms limit. It is also evident that the total ETE delays including processing and communication time delays for different MAC algorithms are less than the 3ms limit as per the IEC 61850 standards.

In practice, the P&C IEDs deployed in substations perform multiple functions, hence the P&C IEDs are subscribed to multiple SV streams. When a subscriber receives multiple SV streams at the same time, the inter-arrival time of packets decreases. The processing times for each SV packet, including the computational times for security mechanisms must be less than the inter-arrival time for successful operation. Otherwise, the processing of incoming packets is delayed which leads to overflow of buffer and eventually packet drops. Table 5 shows the computational processing times of proposed security algorithms using different platforms and the inter-arrival times for different number of SV streams. From Table 5 it is observed that proposed security scheme can be applied to two SV streams using the Raspberry Pi platform. The Celeron processor can support up to eleven SV streams at the same time. Hence, it can be concluded that the proposed security mechanism can be safely applied to two SV streams on a low computing power IED without any issues.

V. CONCLUSION

Through real-time HIL simulations of SAS, this paper has demonstrated the impact of replay and masquerade attack on SV messages used in protection schemes. Towards mitigating these threats, a MAC and AES-GCM algorithm-based security mechanism is proposed to secure the SV messages against replay and masquerade attacks. Necessary format modifications in SV frame and proposed additional fields are clearly presented. The security scheme is presented in conjunction with these novel fields. In order to verify the applicability of proposed MAC algorithm-based security scheme on high sampling rate time critical SV messages, a C-language based framework capable of generating secure

SV messages is developed. With the help of this framework, the computational times for processing SV messages are calculated. From the results, it has been observed that the proposed MAC algorithms and AES-GCM algorithms can be applied to SV messages without any issues. Furthermore, SV emulators are integrated with a co-simulation platform to obtain realistic communication delays in a SCN. Results show that the ETE delays for secure SV messages for different MAC algorithms are within the specified limit of IEC 61850 standards. These results are useful for researchers and practitioners in understanding how SV messages can be secured, what additional fields are needed in the message frame, and how these schemes impact the message size and delivery time.

REFERENCES

[1] R. Hunt, B. Flynn, and T. Smith, "The substation of the future: Moving toward a digital solution," *IEEE Power Energy Mag.*, vol. 17, no. 4, pp. 47–55, Jul. 2019.

[2] I. Ali, S. M. S. Hussain, A. Tak, and T. S. Ustun, "Communication modeling for differential protection in IEC-61850-based substations," *IEEE Trans. Ind. Appl.*, vol. 54, no. 1, pp. 135–142, Jan./Feb. 2018.

[3] T. S. Ustun and S. M. S. Hussain, "A review of cybersecurity issues in smartgrid communication networks," in *Proc. Int. Conf. Power Electron., Control Autom. (ICPECA)*, New Delhi, India, Nov. 2019, pp. 1–6.

[4] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[5] *Cyber-Attack Against Ukrainian Critical Infrastructure*, ICSCERT, Washington, DC, USA, Feb. 2016.

[6] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward threat of implementation attacks on substation security: Case study on fault detection and isolation," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2442–2451, Jun. 2018.

[7] D. Mashima, P. Gunathilaka, and B. Chen, "Artificial command delaying for secure substation remote control: Design and implementation," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 471–482, Jan. 2019.

[8] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5643–5654, Sep. 2020.

[9] *Power Systems Management and Associated Information Exchange—Data and Communications Security*, document IEC 62351, IEC, Geneva, Switzerland, 2018.

[10] 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.

[11] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, "Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security," *IEEE Access*, vol. 7, pp. 80980–80984, 2019.

[12] T. S. Ustun and S. M. S. Hussain, "An improved security scheme for IEC 61850 MMS messages in intelligent substation communication networks," *J. Modern Power Syst. Clean Energy*, vol. 8, no. 3, pp. 591–595, 2020.

[13] J. G. Wright and S. D. Wolthusen, "Stealthy injection attacks against IEC 61850's GOOSE messaging service," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT-Europe)*, Oct. 2018, pp. 1–6.

[14] 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, Sep. 2019.

[15] J. H. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643–1653, Jul. 2014.

[16] J. Hong and C.-C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 271–281, Jan. 2019.

[17] J. Hong, R. Karnati, C.-W. Ten, S. Lee, and S. Choi, "Implementation of secure sampled value (SeSV) messages in substation automation system," *IEEE Trans. Power Del.*, vol. 37, no. 1, pp. 405–414, Feb. 2022.

[18] U. Tefek, E. Esiner, D. Mashima, and Y.-C. Hu, "Analysis of message authentication solutions for IEC 61850 in substation automation systems," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Singapore, Oct. 2022, pp. 224–230.

[19] 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.

[20] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima, and B. Chen, "A synthesized dataset for cybersecurity study of IEC 61850 based substation," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Beijing, China, Oct. 2019, pp. 1–7.

[21] O. Duman, M. Ghafouri, M. Kassouf, R. Atallah, L. Wang, and M. Debbabi, "Modeling supply chain attacks in IEC 61850 substations," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Beijing, China, Oct. 2019, pp. 1–6.

[22] (Mar. 2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[23] J. G. Wright and S. D. Wolthusen, "Access control and availability vulnerabilities in the ISO/IEC 61850 substation automation protocol," in *Critical Information Infrastructures Security* (Lecture Notes in Computer Science), vol. 10242. Cham, Switzerland: Springer, 2017.

[24] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, "A review of security attacks on IEC 61850 substation automation system network," in *Proc. 6th Int. Conf. Inf. Technol. Multimedia*, Putrajaya, Malaysia, Nov. 2014, pp. 5–10.

[25] A. Naha, A. M. H. Teixeira, A. Ahlen, and S. Dey, "Sequential detection of replay attacks," *IEEE Trans. Autom. Control*, vol. 68, no. 3, pp. 1941–1948, Mar. 2023, doi: 10.1109/TAC.2022.3174004.

[26] *Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2*, document IEC 61850-9-2 LE, UCA Int. Users Group (UCAIug), Shell Knob, MO, USA, 2004.

[27] J. Bettler, R. McDaniel, and D. Bowen, "Performance of IEC 61850 sampled values relays for a real-world fault," in *Proc. 49th Annu. Western Protective Relay Conf.*, Washington, DC, USA, Oct. 2022, pp. 1445–1454. [Online]. Available: https://selinc.com/api/download/137357/

[28] *RSCAD Tutorial Manual*, RTDS Technologies Inc., Winnipeg, MD, Canada, 2018.

[29] *Communication Networks and Systems for Power Utility Automation—Part 90–5: Use of IEC 61850 to Transmit Synchrophasor Information According to IEEE C37.118, 1.0*, document IEC 61850-90-5, IEC, Geneva, Switzerland, 2012.

[30] *Communication Networks and Systems in Substations—Part 5: Communication Requirements for Functions and Device Models, 2.0*. document IEC 61850-5, IEC, Geneva, Switzerland, 2013.

[31] *S-SV Framework*. Accessed: Mar. 14, 2023. [Online]. Available: https://github.com/61850security/S-SV

[32] *Data Sheet—SEL 3555 Real Time Automation Controller (RTAC)*. Accessed: Mar. 14, 2023. [Online]. Available: https://selinc.com/api/download/107766/

S. M. SUHAIL HUSSAIN (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Jamia Millia Islamia (a Central University), New Delhi, India, in 2018. Currently, he is an Assistant Professor with the Electrical Engineering Department, Interdisciplinary Research Center for Renewable Energy and Power Systems (IRC-REPS), King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia. Prior to that, he was an AIST Postdoctoral Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), Koriyama, Japan; and a Senior Research Fellow with the Department of Computer Science, National University of Singapore (NUS), Singapore. His research interests include power system communication, cybersecurity in power systems, and substation automation.

He was a recipient of the IEEE Standards Education Grant approved by the IEEE Standards Education Committee for implementing project and submitting a student application paper in 2014–2015. He is the Guest Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.

MOHD ASIM AFTAB (Member, IEEE) received the B.Tech. degree (Hons.) in electrical and electronics engineering from Uttar Pradesh Technical University, Lucknow, in 2012, and the M.Tech. degree in control and instrumentation systems and the Ph.D. degree in electrical engineering from Jamia Millia Islamia (a Central University), New Delhi, India, in 2015 and 2020, respectively. Currently, he is a Postdoctoral Researcher with SENTRY Laboratory, King Abdullah University of Science and Technology (KAUST), Saudi Arabia. Prior to this, he was an Assistant Professor with the Electrical and Instrumentation Engineering Department, Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, Punjab. His research interests include microgrids, active distribution networks, IEC 61850 standards, PMU communication networks, electric vehicle integration, and smart grid. He was a recipient of the Best Reviewer Award by Elsevier in 2018.

SHAIK MULLAPATHI FAROOQ (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Yogi Vemana University (YVU), Kadapa, India, in 2020. He was a Visiting Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), Koriyama, Japan, in 2018. Currently, he is an Assistant Professor with the School of Computer Science and Engineering, Vellore Institute of Technology (VIT), Vellore, India. His research interests include cryptography, cyber physical systems, cybersecurity in vehicular networks, and power systems.

IKBAL ALI (Senior Member, IEEE) graduated from Aligarh Muslim University (AMU), Aligarh, India. He received the M.Tech. degree from the Indian Institute of Technology, Roorkee, India, and the Ph.D. degree in electrical engineering from Jamia Millia Islamia (a Central University), New Delhi, India. Currently, he is a Professor with the Department of Electrical Engineering, Jamia Millia Islamia (a Central University). As a Principal Investigator, he is executing research projects on substation automation, micro-grid, and IEC 61850 based utility automation, funded by DST, AICTE, JMI, and IEEE Standards Education Society. His research interests include IEC 61850 based utility automation, substation communication networks architecture, and smart grid.

TAHA SELIM USTUN (Member, IEEE) received the Ph.D. degree in electrical engineering from Victoria University, Melbourne, VIC, Australia.

Currently, he is a Senior Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), and leads the Smart Grid Cybersecurity Laboratory. Prior to that, he was an Assistant Professor of electrical engineering with the School of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA. His research interests include power systems protection, communication in power networks, distributed generation, microgrids, electric vehicle integration, and cybersecurity in smartgrids. He is an Associate Editor of the IEEE Access and the Guest Editor of the IEEE Transactions on Industrial Informatics.

CHARALAMBOS KONSTANTINOU (Senior Member, IEEE) received the M.Eng. degree in electrical and computer engineering from the National Technical University of Athens (NTUA), Greece, in 2012, and the Ph.D. degree in electrical engineering from New York University (NYU), NY, USA, in 2018. He is currently an Assistant Professor of electrical and computer engineering (ECE) and an Affiliate Professor of computer science (CS) with the Computer, Electrical and Mathematical Science and Engineering Division (CEMSE), King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia. He is also the Principal Investigator of the Secure Next Generation Resilient Systems Laboratory and a member of the Resilient Computing and Cybersecurity Center (RC3), KAUST. Before joining KAUST, he was an Assistant Professor with the Center for Advanced Power Systems (CAPS), Florida State University (FSU). His research interests include secure, trustworthy, and resilient cyber-physical, and the embedded IoT systems. He is also interested in critical infrastructures security and resilience with special focus on smart grid technologies, renewable energy integration, and real-time simulation. He is a member of ACM. He is the Chair of the IEEE Task Force on Resilient and Secure Large-Scale Energy Internet Systems and the Co-Chair of the IEEE Task Force on Cyber-Physical Interdependence for Power System Operation and Control. He is an Associate Editor of the IEEE Transactions on Industrial Informatics. He is an ACM Distinguished Speaker (2021–2024).