IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 23 November 2023, accepted 26 January 2024, date of publication 2 February 2024, date of current version 8 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3361753

RESEARCH ARTICLE

A Geometrical Approach to Enhance Security Against Cyber Attacks in Digital Substations

MOHAMED F. ELRAWY[1,2], **(Member, IEEE),**
CAMILLA FIORAVANTI[3], **(Graduate Student Member, IEEE),**
GABRIELE OLIVA[3], **(Senior Member, IEEE), MARIA K. MICHAEL**[1,2], **(Member, IEEE),**
AND ROBERTO SETOLA[3], **(Senior Member, IEEE)**
[1]Department of Electrical and Computer Engineering, University of Cyprus, Aglantzia, 2109 Nicosia, Cyprus
[2]KIOS Research and Innovation Center of Excellence, University of Cyprus, Aglantzia, 2109 Nicosia, Cyprus
[3]Department of Engineering, University Campus Bio-Medico of Rome, 00128 Rome, Italy

Corresponding author: Camilla Fioravanti (c.fioravanti@unicampus.it)

This work was supported in part by the European Union—Next Generation EU—NRRP M4.C2—Investment 1.5 (Project ECS00000024 Rome Technopole—CUP C83C22000510001); in part by the European Union's Horizon 2020 Research and Innovation Program under Grant 101021936 (ELECTRON); in part by the European Union's Horizon 2020 Grant under Grant 739551 (KIOS CoE—TEAMING); and in part by the Republic of Cyprus through the Deputy Ministry of Research, Innovation and Digital Policy.

ABSTRACT Smart grid technology drives economic and social development but raises vulnerability to cyber threats due to digital substations' growing reliance. To counter these risks, recent updates to communication standards, including encryption and authentication processes, have been integrated into the infrastructure. Notably, adhering to the IEC 62351 standard governing the GOOSE protocol for substation communication faces practical challenges due to conflicting time requirements with traditional security procedures. In this paper, we present an innovative geometric approach for GOOSE message authentication and encryption. Utilizing vector coordinate shifts, our method exhibits efficiency and speed of implementation, ensuring compliance with the protocol's stringent time constraints. Importantly, unlike other approaches in the literature, our technique has the potential to be easily applicable and effective for a wide range of infrastructures without requiring the use or addition of specific hardware components or changes to the GOOSE message format, while guaranteeing high performances and computational simplicity. The paper is complemented by a simulation campaign on a digital substation model, assessing the approach's performance and its efficacy in countering cyber threats.

INDEX TERMS Cyber-physical systems, cyber-security, digital substation, GOOSE protocol, IEC 61850, IEC 62351, smart grid.

I. INTRODUCTION

The recent revolution of Information and Communication Technology (ICT) in the power sector infrastructure has resulted in increased efficiency and stability through the digitization of power systems [1]. Thanks to digitalization, the traditional power grid is transformed into a smart grid, allowing communication between power systems to perform smart and automated decisions [2]. In this view, the digital substation is one of the most important elements of the smart grid paradigm. The substations consist of a group of Intelligent Electronic Devices (IEDs), such as relays, connected via a Substation Communication Network (SCN) to exchange data. To solve interoperability issues between multi-vendor equipment, the International Electrotechnical Commission (IEC) 61850 communication standard has been established, providing flexibility and real-time communications between different equipment in digital substations [3]. In particular, the IEC 61850 standard introduces the Generic Object-Oriented Substation Events (GOOSE) communication protocol with the aim to enable real-time communications between protective relays and

The associate editor coordinating the review of this manuscript and approving it for publication was Bin Xu.

to enhance the real-time protection capabilities of the substations [4].

In recent years, increasing attention has been paid to security issues affecting critical infrastructures such as power grids, on both network and physical layer [5], [6], [7], [8]. However, in order to meet the high-speed communication requirements necessary for the protocol to operate efficiently, the establishment of the GOOSE does not include any encryption or authentication mechanism [9]. Consequently, with the progressive development of cyber threats, some recommendations have been provided in the new IEC 62351 standard to secure the GOOSE protocol. Specifically, the IEC 62351 standard requires a digital signature approach for protecting the integrity and authenticity of the GOOSE messages, while it recommends encryption for protecting the confidentiality of these messages. Interestingly, authentication is defined as mandatory, while encryption is defined as optional due to the high computation time required for the encryption algorithms. For instance, Rivest-Shamir-Adleman (RSA) algorithms have been mentioned as possible applicable asymmetric cryptography schemes for digital signatures [10].

Although the recommendations imposed by the IEC 62351 standard are needed to remedy the security gaps in the GOOSE protocol, their actual application clashes with the operational speed requirement, since the IEC 61850 standard specifies that GOOSE messages must be generated, transmitted, and processed in less than 3 milliseconds [3], [10], [11]. This dual requirement challenges the implementation of the IEC 62351 security recommendations in real life and makes traditional security methods inapplicable or ineffective. As a matter of fact, the GOOSE protocol is often implemented in real life without any security measures, threatening the protection functionalities of substations as well as the stability and reliability of the smart grid. In particular, the exploitation of security vulnerabilities in the GOOSE protocol by cyber attackers compromises the integrity, confidentiality, and availability of GOOSE data, which may lead to a regional blackout and/or critical damage to the power system infrastructure [6], [12].

To solve these issues, several approaches have been proposed in the literature to prevent cyber-attackers from exploiting GOOSE protocol vulnerabilities. Some approaches in the state of the art mainly focus on providing authentication for GOOSE messages, in order to protect the integrity of the message only, such as [5], [13], [14], [15], [16], [17], and [18]. However, based on the analysis presented in these works, digital signature algorithms (e.g., RSA and Elliptic Curve Digital Signature Algorithm (ECDSA)) do not represent suitable solutions for implementation due to the high calculation time required by these schemes, which considerably exceeds the time requirements of the protocol.

In [18] and [19], the authors proposed two digital signature models, i.e., Less-online/More-offline signatures (LoMoS) and Caching-based Multicast Message Authentication (CMMA), based on two-phase authentication approach to decrease the required computational time of the digital signature algorithms. However, these models increase the communication overhead in SCN, which increases the end-to-end delay significantly. Consequently, they are not optimal solutions to secure GOOSE messages in legacy substations that cannot provide gigabit network throughput.

A different solution to strengthen cybersecurity against GOOSE protocol attacks in smart grids is the one proposed in [20], where the authors develop a hybrid cybersecurity procedure based on knowledge of the cyber and physical domains of the electricity system. Although successful in detecting malicious distortions carried out on GOOSE messages, this methodology might be ineffective in counteracting eavesdropping, as it does not provide for a proper message encryption and authentication process. On the other hand, when considering symmetric encryption schemes, such as Hash-based Message Authentication Code (HMAC) and Galois Message Authentication Code (GMAC), although they proved to be viable solutions in terms of processing time performance overhead for GOOSE messages, they are mainly exploited to provide authentication [5], [17], [18]. In [21], the authors propose three different methods to provide encryption and authentication for GOOSE messages using Advanced Encryption Standard (AES) and HMAC-Secure Hash Algorithm (SHA)-256 Algorithms. Besides, in [11], both authentication and encryption of GOOSE messages are provided using AES with Galois/Counter Mode (AES-GCM) algorithm.

Although both approaches proposed in [11] and [21] provide a light-weight solution for encrypting and authenticating the GOOSE message, they violate the format structure of the GOOSE messages presented in the IEC 61850. In particular, these approaches encrypt the entire Application Protocol Data Unit (APDU) field as a single unit, which leads to hiding the subfield structure of the ADPU field in the encrypted message. In this way, encrypted GOOSE messages risk being dropped or blocked by some network security measures (e.g., signature-based intrusion detection systems or deep packet inspection firewalls) in the substation network, considering these messages as false or invalid. Moreover, the approach presented in [11] requires the addition of hardware components, which increases the complexity and cost of the solution.

Therefore, designing an authentication and encryption mechanism that is capable of simultaneously encrypting and authenticating the exchanged GOOSE messages, without violating the format structure of the messages, and meeting the time requirements imposed by the standard is required and considered as a research gap.

A. CONTRIBUTION

The analysis of the IEC 61850/62351 standards and the different approaches in the literature have revealed the lack of a security protocol capable of meeting the strict time limits imposed by the standards while remaining easy to implement and capable of performing both encryption and

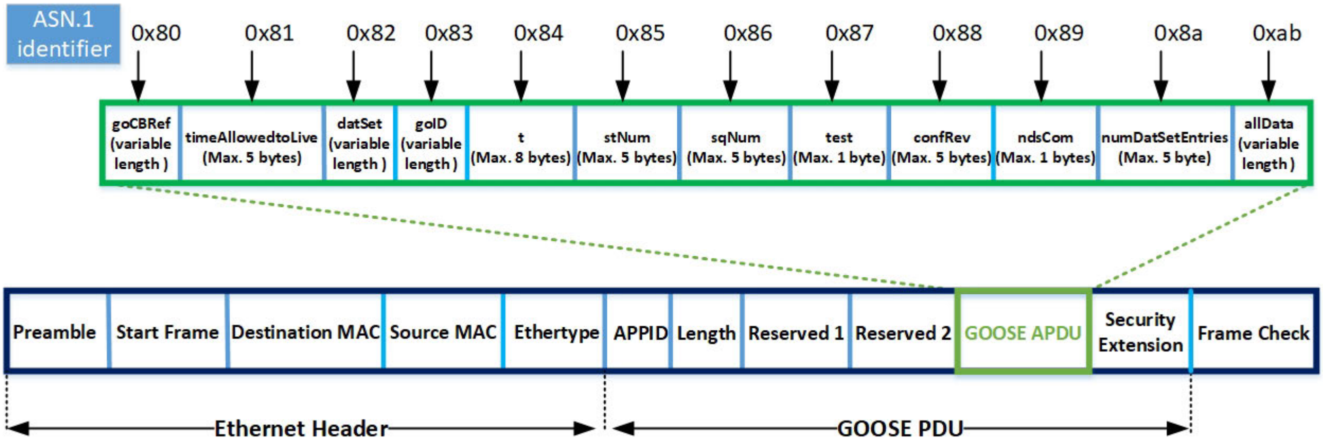

FIGURE 1. Format structure of the GOOSE message according to the IEC 61850 standard.

authentication. To fill this gap, in this paper we propose an innovative methodology for encryption and authentication based on a geometric approach that proves to be particularly fast and easy to implement while preserving the integrity and confidentiality characteristics of the messages. The main strengths of the proposed approach are summarized below.

- The proposed authentication and encryption algorithms, based on a geometric-cryptographic mechanism, have execution times that prove to be well below the 3-millisecond constraint imposed by the standard. Furthermore, by using such algorithms, the integrity and confidentiality of GOOSE messages in the SCN are provided without changing the format structure of the messages.
- The proposed implementation of the authentication and encryption algorithm in the IED can reduce the processing time required to detect data manipulation in GOOSE messages.
- The proposed algorithms can be applied to GOOSE messages of any length and are effective in several infrastructures without requiring the use or addition of specific hardware components.

We point out that, a cybersecurity approach characterized by minimal computational demands, impressive speed, and simple implementation, while ensuring a strong security level, opens the door to its practical use across a variety of real-world scenarios. It enables such algorithms to operate in real-time on hardware with constrained computational capabilities, including various IEDs such as overcurrent relays, which are used in critical protective applications in digital substations, and to face the requirements of different power grid infrastructures.

B. PAPER OUTLINE

The remainder of this paper is organized as follows. Section II overviews IEC 68150 GOOSE protocol and the threat model. In Section III, the proposed algorithms for encryption and authentication are presented, followed by a description of their implementation on GOOSE messages. Section IV discusses the experimental setup and the results of the performance evaluation, while conclusions and directions for future work are outlined in Section V.

II. PRELIMINARIES

The purpose of this section is to provide useful details for understanding the structure provided by the IEC standard for the GOOSE protocol. Specifically, the structure of the GOOSE messages, the transmission model of the messages, and possible threats related to the procedure are presented.

A. GOOSE MESSAGE STRUCTURE

In order to be able to efficiently work in a real-time environment and meet fast and reliable communication requirements, the GOOSE message has been designed to be directly connected with the data link layer [9], [17]. Going into greater detail, the structure of the GOOSE message is described in the IEC 61850 standard, as shown in Fig. 1. In particular, for the purposes of applying the security measures required by the IEC 62351 standard, in this work we focus on the **GOOSE APDU** and **Security Extension** fields. The **GOOSE APDU** field contains 12 subfields, defined by means of ASN.1 (Abstract Syntax Notation One) identifiers, whose length properties, distinguished between fixed-length and variable-length, are also defined by the IEC 61850 standard. In the fixed-length property, the publisher uses a specific length of bytes for each different sub-field, whereas the publisher defines the length of each sub-field using the Tag-Length-Value (TLV) format in the variable-length property [22].

Specifically, the **GOOSE APDU** is divided into the following subfields, each of them representing [23]

- **goCBRef**: publisher GOOSE control block name;
- **timeAllowedtoLive**: maximum wait time to receive a GOOSE message before the publisher sends a new one;

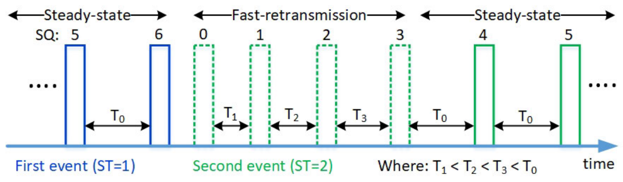

FIGURE 2. GOOSE transmission model [9].

- **datSet**: publisher dataset name;
- **goID**: control block identifier name;
- **t**: time of the last event;
- **stNum**: State number (ST), which is a counter that increments with every new GOOSE event;
- **sqNum**: Sequence number (SQ), which is a counter that increments with every retransmission of the same GOOSE message;
- **test**: a boolean number that indicates whether the transmitted message is in a test;
- **confRev**: a counter representing the number of changes in the dataset configuration;
- **ndsCom**: a boolean number that indicates whether the configuration of GOOSE control block is incorrect;
- **numDatSetEntries**: number of elements in the dataset;
- **allData**: contains all information within the dataset.

B. GOOSE TRANSMISSION MODEL

The GOOSE transmission model has been designed based on a multicast communication approach that exploits two transmission mechanisms, i.e., steady-state and fast mechanisms, to provide fast and reliable communications between IEDs in digital substations [24].

As shown in Fig. 2, in the absence of particular events, the publisher IED (e.g., transmitter relay) exploits the steady-state retransmission mechanism, i.e., it re-transmits the same GOOSE messages synchronously to multiple subscriber IEDs (e.g., receiver relays) using a constant time interval T_0. Otherwise, if the publisher IED detects a new event (e.g., overcurrent detection, circuit breaker failure, etc.), it announces this event by resending the GOOSE messages using the fast retransmission mechanism, which exploits shorter retransmission time intervals (i.e., T_1, T_2, T_3) [25].

C. SECURITY THREATS IN DIGITAL SUBSTATION

In recent years, cyber attackers took advantage of the numerous vulnerabilities of the GOOSE protocol, in order to affect physical and communication operations in substations [26], [27]. In the case that an attacker aiming to read the information content transmitted in the various substations succeeds in gaining access to the SCN, it automatically becomes able to receive GOOSE messages from the various publisher IEDs, since GOOSE messages are sent using the multicast communication approach. In this context, a third party aiming to perform a cyber attack on the GOOSE protocol can mainly act on two levels, namely compromising the *confidentiality* and the *integrity* of GOOSE messages. Regarding the first aspect, as long as GOOSE messages are not encrypted, it is also easy for an attacker to access the private content of the data, thus compromising the confidentiality, i.e., the limitation or restriction on certain types of information [28]. Consequently, the attacker can spoof the Media Access Control (MAC) address of the publisher IEDs using the captured GOOSE messages to deceive subscriber IEDs [29].

Moreover, the problem of the lack of confidentiality on sensitive data and their exposition to possible eavesdroppers is directly connected to the integrity, i.e., the adherence to the protocol, since the malicious entity, after collecting the necessary data, can develop an ad-hoc attack injecting manipulated and false GOOSE data into the SCN with the aim to compromise the processes. Fig. 3 shows the steps of a cyber-attack targeting the confidentiality and integrity of GOOSE messages using an example of a digital substation with a main relay (i.e., IED1) and two downstream relays (i.e., IED2 and IED3) for backup protection. As shown in Fig. 3, the attacker exploits the vulnerability of the multicast mechanism of the GOOSE protocol to receive the GOOSE messages transmitted between different IEDs and analyzes these messages in the first step. Then, in the following step, the attacker operates using one of the attack techniques (i.e., replay attack, False Data Injection (FDI), and Denial of Service (DoS)) targeting the GOOSE messages to affect the protective physical operations of the digital substation (e.g., open/close Circuit Breaker 1 (CB 1)).

Cyber-attackers can exploit the lack of confidentiality and integrity of the GOOSE messages by using several attack techniques, such as replay attack, FDI, and DoS (e.g., Message Suppression (MS)). In a typical replay attack technique, the attacker records the GOOSE messages between the publisher IEDs and subscriber IEDs; and then he/she retransmits one of these recorded messages, without making any change in the data, to deceive subscriber IEDs. However, this attack technique can be limited in its effectiveness unless the attacker updates the **timeAllowedtoLive** and **stNum** fields of the retransmitted GOOSE message [30].

FDI and MS attacks are two typical examples of attack techniques that cyber-attackers can use to affect substation operations [24], [31]. In the FDI technique, the attacker injects manipulated data into the payload of the benign GOOSE message in order to influence the IEDs decisions. On the other hand, in the MS attack technique, the attacker sends a fake GOOSE message to the IEDs in the substation to prevent them from receiving the benign GOOSE messages generated by the publisher IED and to lead them to take wrong actions due to neglecting of those messages. Therefore, IEDs need a security mechanism that can distinguish between benign and fake messages and detect the manipulation of the original messages.

In this paper, we propose a new encryption and authentication approach that can prevent the manipulation of messages. Therefore, FDI and MS attacks are used to test the efficiency

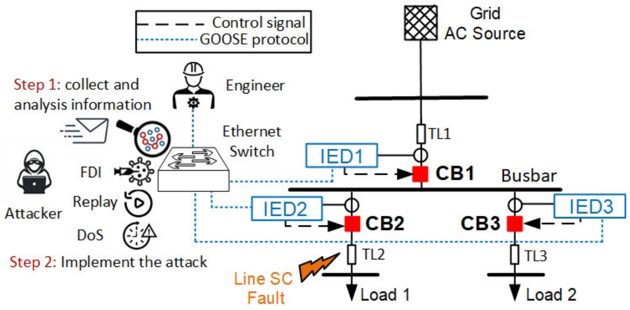

FIGURE 3. Digital substation scheme and cyber-attack steps.

of the proposed approach due to their impact on the substation operations.

III. PROPOSED APPROACH

In this section, we aim to describe the geometric-cryptographic approach developed to perform both authentication and encryption of the messages to be exchanged according to the IEC 62351-6 standard.

A. GEOMETRICAL SHIFT APPROACH FOR ENCRYPTION

In order to keep the computational burden low and to be able to perform encryption quickly, we rely on a geometric approach that involves modifying the entries and, possibly, the size of the vector containing the information to be encrypted [32]. To this aim, let us consider the set of information to be encrypted as if it were a single vector[1] whose entries coincide with the respective data

$$d = \left[\mathtt{data}_1, \mathtt{data}_2, \ldots, \mathtt{data}_n\right]^T . \qquad (1)$$

The desired hidden dynamics is calculated by multiplying the vector $\boldsymbol{d} \in \mathbb{R}^n$ with a constant weight matrix (or vector) $Q \in \mathbb{R}^{p \times n}$, with entries that are known to all legitimate agents, and which plays the role of a pre-deposited shared key. Specifically, to obtain the cyphertext we have to compute

$$c = Qd, \qquad (2)$$

with $c \in \mathbb{R}^p$. Since the geometric encryption methodology proves to be effective in enhancing the secrecy of the message's information content while maintaining very low computational costs and a remarkable speed of execution, we propose to exploit it in both the authentication and encryption phases. We point out that, starting from the knowledge of the ciphertext **c** it is not possible for an intruder to get to know the entries of either the matrix Q or the vector **d**, since the equation $c = Qd$ is verified for an infinite number of different Q and **d**. Therefore, without the knowledge of the matrix Q (and the assumption this matrix is also nonsingular), there is no chance of getting to know the value of the plaintext **d**, since it is not univocally determined.

Let us provide some numerical examples.

Algorithm 1 Encryption Protocol

```
Initialization (Sender)
    Set matrix $Q \in \mathbb{R}^{n \times n}$;
    Set vector $v \in \mathbb{R}^n$;
    Transmit $Q$ and v to the receiver;
Initialization (Receiver)
    Receive $Q$ and v;
    Compute matrix $Q^{-1} \in \mathbb{R}^{n \times n}$;
Execution (Sender)
    Collect data in the vector d;
    Compute $enc = Q(d + v)$;
    Transmit enc to the receiver;
Execution (Receiver)
    Receive enc;
    Compute $dec = (Q^{-1}enc) - v$;
```

Examples Let us consider the plaintext vector $d_1 \in \mathbb{R}^5$

$$d_1 = [0.92, 0.28, 0.50, 0.89, 0.50]^T .$$

If we select the weight transformation matrix $Q_1 \in \mathbb{R}^{7 \times 5}$ as follows

$$Q_1 = \begin{bmatrix} 1.06 & 19.25 & -8.38 & -2.25 & 10.83 \\ 11.96 & 2.04 & 13.45 & 7.12 & -3.33 \\ 7.33 & 14.29 & 13.61 & -5.38 & -1.07 \\ 0.51 & -5.35 & 7.82 & 18.95 & 6.10 \\ 17.75 & 3.53 & -6.29 & 3.76 & -0.53 \\ 12.72 & 14.11 & -3.97 & 3.82 & 4.52 \\ 5.73 & 5.97 & 10.11 & 3.94 & 1.85 \end{bmatrix}$$

we obtain the ciphertext $c \in \mathbb{R}^7$

$$c = [5.67, 22.97, 12.21, 22.79, 17.36, 19.43, 16.44]^T .$$

However, even if we have chosen the following transformation matrix $Q_2 \in \mathbb{R}^{7 \times 7}$

$$Q_2 = \begin{bmatrix} 0.67 & 0.65 & 0.01 & 0.90 & 0.71 & 0.06 & 0.52 \\ 0.84 & 0.15 & 0.87 & 0.62 & 0.37 & 0.97 & 0.99 \\ 0.43 & 0.71 & 0.98 & 0.70 & 0.96 & 0.49 & 0.20 \\ 0.75 & 0.01 & 0.20 & 0.01 & 0.54 & 0.58 & 0.71 \\ 0.69 & 0.29 & 0.12 & 0.07 & 0.19 & 0.56 & 0.78 \\ 0.08 & 0.87 & 0.18 & 0.75 & 0.53 & 0.63 & 0.39 \\ 0.20 & 0.59 & 0.11 & 0.09 & 0.42 & 0.61 & 0.51 \end{bmatrix},$$

with the aim to encrypt the following vector $d_2 \in \mathbb{R}^7$

$$d_2 = [28.21, -3.30, -22.25, 4.89, 1.72, 54.11, -37.34]^T ,$$

we would have obtained exactly the same value for cipher **c**. This shows that there are infinite combinations of vectors **d** and matrices Q, even with different dimensions, capable of providing exactly the same cipher vector, making it impossible for the intruder to reconstruct the **d** vectors in the absence of knowledge of the associated Q matrices.

[1] We denote vectors by boldface lowercase letters and matrices with uppercase letters.

B. ENCRYPTION ALGORITHM

The proposed encryption and decryption protocol is based on the geometric coordinate shift approach described above. It is divided into an *initialization phase*, in which the selection and sharing of the matrices required to encrypt/decrypt the message takes place, and an *execution phase*, in which message encryption and decryption are actually performed (the detailed procedure is reported in Algorithm 1). The initialization phase involves the following steps

- The selection of a transformation matrix $Q \in \mathbb{R}^{n \times n}$, where n is the length of the message we need to encrypt. Notice that the matrix is required to be nonsingular;
- The calculation of the inverse of this matrix Q^{-1};
- The selection of a vector $v \in \mathbb{R}^n$;
- The sharing of this information, so that the sender has Q and $\mathbf{v}$ stored in its memory and the receiver has Q^{-1} and $\mathbf{v}$ stored in its own.

It should be noted that the sequence of these operations can be performed offline and that, to strengthen security at this stage, the matrices involved could be sent encrypted (using traditional encryption methods such as RSA, since we have no execution time constraints at this stage) or during a secure and controlled preventive phase.

The execution phase, on the other hand, is performed in real time and used for message transmission. Specifically, considering the information to be sent as aggregated in a single message $\mathbf{d}$ (as in Eq. (1)), the corresponding cipher vector is calculated as

$$enc = Q(d + v), \tag{3}$$

where $enc \in \mathbb{R}^n$ retains the length of the original vector $\mathbf{d}$. Notice that, through the proposed approach, the data vector is first modified through the sum with the vector $\mathbf{v}$, and then this sum undergoes a coordinate transformation through pre-multiplication with the transformation matrix Q. The encrypted message $\mathbf{enc}$ is then transmitted to the receiver, which can easily decode it based on its knowledge of the vector $\mathbf{v}$ and matrix Q^{-1} as follows

$$dec = (Q^{-1}enc) - v. \tag{4}$$

1) ANALYSIS

With the proposed encryption procedure, the length and type of the data vector remain unchanged, as the coordinate transformation causes the original vector to be mapped to different coordinates from the original; therefore, during transmission, what will be displayed will be the same fields as in the original message but with values that are different from the original ones. Notice that the only way to reconstruct the original vector is based on the knowledge of the vector $\mathbf{v}$ and the matrix Q^{-1} together (Eq. (4)) since the dependency of the encrypted message on them introduce $n \times (n+1)$ degrees of freedom and make the estimation of the original vector unresolvable without their knowledge. Moreover, while on the one hand the vector $\mathbf{v}$ creates an immediate but decoupled shift on the fields of the original data, the transformation via the matrix Q creates a coupling and dependency between them, so that the modification of a single field of the unencrypted message $\mathbf{d}$ causes a modification on all the fields of the encrypted message $\mathbf{enc}$.

Algorithm 2 Authentication Protocol

```
Initialization (Sender)
  Set vector $p \in \mathbb{R}^n$;
  Compute $n-1$ vectors orthogonal to $\mathbf{p}$;
  Collect vectors into a matrix $P \in \mathbb{R}^{n \times n}$;
  Compute matrix $P^{-1} \in \mathbb{R}^{n \times n}$;
  Set vector $s \in \mathbb{R}^n$;
  Transmit $\mathbf{p}$, $\mathbf{s}$ and $P^{-1}$ to the receiver;
Initialization (Receiver)
  Receive $\mathbf{p}$, $\mathbf{s}$ and $P^{-1}$;
Execution (Sender)
  Compute enc as described in Algorithm 1;
  Compute $\boldsymbol{\alpha}_{\mathrm{s}} = P^{-1}enc$;
  Compute $h_{\mathrm{s}} = p^T(\boldsymbol{\alpha}_{\mathrm{s}} + s)$;
  Transmit $h_{\mathrm{s}}$ to the receiver;
Execution (Receiver)
  Receive enc and $h_{\mathrm{s}}$;
  Compute $\boldsymbol{\alpha}_{\mathrm{r}} = P^{-1}enc$;
  Compute $h_{\mathrm{r}} = p^T(\boldsymbol{\alpha}_{\mathrm{r}} + s)$;
  Compare $h_{\mathrm{s}}$ and $h_{\mathrm{r}}$;
  if $h_{\mathrm{r}} = h_{\mathrm{s}}$ then
      Compute dec as described in Algorithm 1;
  else
      Discard the message;
  end
```

C. AUTHENTICATION ALGORITHM

To perform the authentication phase, which is indicated as mandatory within the IEC 62351-6 standard, we rely on the well-known structure of the HMAC standard. In particular, based on the original HMAC scheme, we developed a protocol in which the computationally burdensome hash function used in several protocols (e.g., SHA, MD5) is replaced by a simple and fast geometric protocol. Also in this case, the procedure involves an offline initialization phase in which some matrices are selected and shared in a secure manner (as reported in Algorithm 2); this phase includes

- The selection of a vector $p \in \mathbb{R}^n$;
- The calculation of $n - 1$ additional vectors that, together with $\mathbf{p}$, constitute an orthogonal basis for $\mathbb{R}^n$;
- The collection of all the previous vectors as columns of a matrix $P \in \mathbb{R}^{n \times n}$;
- The calculation of the inverse of this matrix P^{-1};
- The selection of a *signature* vector $s \in \mathbb{R}^n$, which is specific to each sender;
- The sharing of this information, so both the sender and receiver store in their memory the matrix P^{-1} and the vectors $\mathbf{s}$ and $\mathbf{p}$.

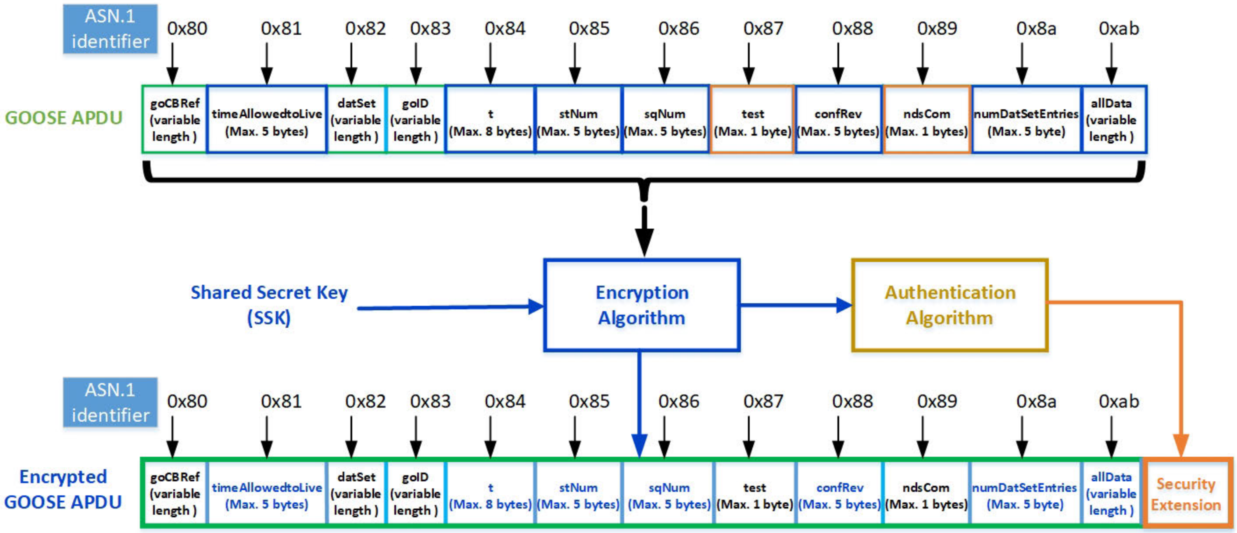

FIGURE 4. Implementation of the encryption and authentication algorithms at the publisher IED.

According to the HMAC protocol, the vector **s** serves as the sharing secret, while the matrix P^{-1} is used for the realization of the hash function. Specifically, for the implementation of a geometric and computationally inexpensive hash function, we relied on the fact that each vector **a** in $\mathbb{R}^n$ can be rewritten as

$$a = \sum_{i=1}^{n} \alpha_i p_i, \tag{5}$$

for some choice of the coefficients $\alpha_i \in \mathbb{R}$, and the vectors $p_i \in \mathbb{R}^n$ being an orthogonal basis for $\mathbb{R}^n$. Starting from Eq. (5) and collecting all the vectors p_i as columns of the matrix P, it is possible to reconstruct

$$\boldsymbol{\alpha} = P^{-1} a, \tag{6}$$

thus obtaining a vector of values $\boldsymbol{\alpha}$ which are uniquely determined.

For the execution of the authentication protocol (see Algorithm 2), we exploit such uniqueness in calculating the vector $\boldsymbol{\alpha}$ and the geometrical approach discussed in Section III-A. Therefore, starting from the encrypted vector **enc** and from the knowledge of the matrix P^{-1}, it is possible to calculate the vector of the α_i associated with the decomposition of **enc** according to Eq. (6)

$$\boldsymbol{\alpha} = P^{-1} enc,$$

Then, for the computation of the scalar value of the hash code, we rely on the vector **p** that generates the orthogonal basis and the signature vector **s** as follows

$$h = p^T(\boldsymbol{\alpha} + s), \tag{7}$$

with $h \in \mathbb{R}$.

1) ANALYSIS

Also in this case, the geometric approach exploited for the calculation of the hash code ensures a combination of the entries of the vector $\boldsymbol{\alpha}$ shifted to the entries of the signature vector **s**, which is specific to each sender and thus ensures verification of the origin of the message. Notice that with the pre-multiplication by the vector p^T we perform a transformation from a vector in $\mathbb{R}^n$ to a scalar in $\mathbb{R}$, which is a non-reversible operation since the inverse of a vector (like p^T) does not exist. Hence, it is not possible to re-obtain the original sum vector ($\boldsymbol{\alpha} + s$) starting from the knowledge of **h**, even knowing the vector **p**. Moreover, since for the calculation of the hash code we do not consider the original encrypted vector **enc** but the vector $\boldsymbol{\alpha}$ uniquely determined starting from it, this ensures the generation of very different hash codes **h** starting from very similar **enc** vectors.

It should be noted that the choice of carrying out the calculation of the hash code from the encrypted vector and not from the original data vector makes it possible to speed up the verification process and to discard any corrupted or tampered vectors more quickly. This procedure indeed ensures that the receiver can immediately calculate its hash code h_{r} from the encrypted vector just received and compare it with the sender's hash code h_{s}, without first having to spend time to perform decryption.

D. IMPLEMENTATION

The proposed approach is overall implemented in the substation as follows: (i) the publisher IED uses encryption and authentication algorithms to secure the transmitted GOOSE message (Fig. 4); (ii) the subscriber IEDs verify and decrypt the GOOSE message before processing it. In the publisher IED, all sub-fields of GOOSE APDU are used in the encryption and/or authentication phases except three sub-fields (i.e., **goCBRef**, **datSet**, and **goID**) to reduce the processing time of detecting data manipulation in GOOSE messages. Such sub-fields are used by IED subscribers to identify the GOOSE messages: if a subscriber IED receives a GOOSE message containing one of the aforementioned sub-fields that does not correspond to the configuration of the IED subscriber, the message is immediately discarded even before verification or decryption is performed. The implementation of encryption and authentication algorithms at the publisher IED level is shown in Fig. 4, where the blue boxes represent the sub-fields used in the encryption and authentication phases, and the orange boxes represent the sub-fields used in the authentication phase only. Specifically, the subfields **test** and **ndsCom** have a data size limit of one byte imposed by the standard, so they are not encrypted but are only used for authentication.

At the subscriber IED level, the procedure of implementation involves: (1) the GOOSE message is identified using **goCBRef**, **datSet**, and **goID** sub-fields; (2) the GOOSE message is verified using the authentication check function to detect any manipulation of the message during the communication process; (3) the GOOSE APDU is decrypted using the decryption algorithm; (4) the clear-text GOOSE message is processed according to the IEC 61850 standard instructions [33]. These four steps of processing GOOSE messages at the subscriber IED level are described using Algorithm 3, where ST_{in} and SQ_{in} represent the **stNum** and **sqNum** of the incoming message, ST_{LA} and SQ_{LA} represent the **stNum** and **sqNum** of the last accepted message, AV_{in} is the authentication value attached with the incoming message, AV_C is the authentication value calculated using data in the incoming message, and SC is the subscriber IED configuration for **goCBRef**, **datSet**, and **goID** sub-fields. The four main steps of Algorithm 3 are summarized as follows:

- Step 1: Identify and filter each incoming GOOSE message, as shown in lines 2-4.
- Step 2: Verify the authentication phase, as shown in lines 6-9. In this phase, the AV_{in}, which represents the value of the hash code calculated by the sender, is extracted and compared to AV_C, which represents the value of the hash code calculated at the receiver.
- Step 3: Decrypt the incoming GOOSE message and extract ST_{in} and SQ_{in}, as shown in lines 11-12.
- Step 4: Verify that the incoming message is a new message and it represents a new event, as shown in lines 13-25. Particularly, the incoming GOOSE message represents a new event if its **stNum** (i.e., ST_{in}) is greater than **stNum** of the previous message (i.e., ST_{LA}). Besides, it should be received before the expiration time.

Algorithm 3 Subscriber IED Algorithm for Processing GOOSE Messages

```
   Input: Encrypted Message(EM), Time-To-Live (TTL),
          SC
   Output: $ST_{LA}$, $SQ_{LA}$
   Initialization $ST_{LA} = 0$, $SQ_{LA} = 0$ ;
1  foreach New incoming message do
2      Extract (goCBRef, datSet, goID) from EM;
3      if goCBRef $\neq$ SC $\vee$ datSet $\neq$ SC $\vee$ goID $\neq$ SC
       then
4          Discard the message (EM);
5      else
6          Extract ($AV_{in}$) from EM;
7          Calculate ($AV_C$) from EM;
8          if $AV_{in} \neq AV_C$ then
9              Discard the message (EM);
10         else
11             M = Decrypt (EM);
12             Extract ($ST_{in}$, $SQ_{in}$) from M;
13             if $ST_{in} \neq ST_{LA}$ then
14                 if $ST_{in} > ST_{LA}$ then
15                     Process the message (M);
16                     $ST_{LA} = ST_{in}$;
17                     $SQ_{LA} = SQ_{in}$;
18                 else
19                     if $ST_{in}$ roll-over Or TTL time-out
                       then
20                         $Age$ = current timestamp –
                           message timestamp ;
21                         if $Age < 2$ minute skew then
22                             Re-establish $ST_{in}$;
23                             Process the message (M);
24                             $ST_{LA} = ST_{in}$;
25                             $SQ_{LA} = SQ_{in}$;
26                         else
27                             Discard the message (M);
28                         end
29                     else
30                         Discard the message (M);
31                     end
32                 end
33             else
34                 Discard the message (M);
35             end
36         end
37     end
38 end
39 return $ST_{LA}$, $SQ_{LA}$
```

IV. PERFORMANCE EVALUATION

In this section, we aim to examine the performance of the proposed encryption and authentication protocols using the simulation model of a digital substation. In particular, we first provide details of the experimental setup and then present a discussion of the results obtained in the simulation.

A. EXPERIMENTAL SETUP

In order to verify the proposed approach for encryption and authentication and to comprehensively evaluate its performance, the simulation model of a digital substation described in [24] is exploited. In such a model, three overcurrent (OC) relays with three different Circuit Breakers (CBs) are used to simulate the protection operations in digital substations (see Fig. 3 for further details). Starting from this structure, the GOOSE protocol is simulated inside the model and used as a communication protocol between the relays. Notice that the GOOSE message contains both measurement parameters, i.e., three-phase RMS current and voltage values, and control parameters, i.e., *Trip*, *Block*, *CB Fail*, and *Fault*, which are used to control other relays in the substation.

When the *Trip* parameter is set to one, it indicates that the relay is requesting immediate backup protection from the main relay. The downstream relays can stop the Trip operation of the main relay, to avoid unnecessary opening of the main CB, by setting the *Block* parameter to one in the GOOSE message. Moreover, the relay can set the *CB Fail* parameter to one when it can not open its CB to isolate the fault. The *Fault* parameter is set to one by the relay if it detects a Short Circuit (SC) fault (i.e., fault produces a high current that exceeds a defined threshold). The physical and communication operations of relays included in this simulation model are described as follows:

1) In the event that a relay detects an SC fault, it sends a Fault signal to inform other relays about the fault.
2) After a definite time (e.g., 100[ms]) that is specified by the protection scheme of the substation, the relay sends an opening command to its CB to isolate the fault, and also a Block signal to the other relays to avoid unnecessary opening of their CBs.
3) In the case of a CB failure, the relay sends an Inter-trip signal to the backup relay (e.g., the main relay IED1).
4) Based on this Inter-trip signal, the main relay opens its CB to isolate the fault.

In order to meet the requirements of the IEC 62350 standard regarding the length of each GOOSE APDU field in terms of bytes, we consider the single precision as the data type for the individual fields of the GOOSE message and for all vectors and matrices required for encryption and authentication. However, since the proposed encryption process is natively designed to be applied on double-precision data, as it exploits the inverse computation of a matrix, the restriction to single precision may generate errors in the computation of Q^{-1} that result in accuracy problems during decryption. To overcome this issue, for the implementation, we choose to use diagonally dominant Q matrices to greatly reduce the error on the computation of its inverse Q^{-1} and guarantee an average accuracy to the third decimal digit of the decrypted message. Notice that this choice for the matrix Q does not affect the robustness or the effectiveness of the encryption process.

B. RESULTS AND DISCUSSION

For the experimental campaign, we exploit six different cases to verify the efficacy of the proposed encryption and authentication approaches using the substation scheme shown in Fig. 3. In all the presented cases, we analyze the behavior of the protective relay, i.e., an OC relay that is responsible to detect and isolate the SC faults.

TABLE 1. Examples of inter-trip GOOSE messages extracted during the experiment.

Message Field	Original Message	Encrypted Message	Decrypted Message
timeAllowedtoLive	1000	-1.44489×10^5	999.99
t	2.1670	4.42388×10^5	2.1669
stNum	4	6.50004×10^5	4
sqNum	0	1.78620×10^5	0
test	0	0	0
confRev	1	5.23303×10^4	1
ndsCom	0	0	0
numDatSetEntries	12	1.73479×10^5	11.9999
allData: RMS voltage1	12404.396	3.28874×10^6	12404.397
allData: RMS voltage2	12404.421	-1.35461×10^5	12404.419
allData: RMS voltage3	12404.125	-2.49768×10^6	12404.126
allData: RMS current1	13361.577	-4.15964×10^6	13361.577
allData: RMS current2	13361.681	4.33598×10^6	13361.682
allData: RMS current3	13361.589	-1.23569×10^6	13361.591
allData:TRIP	1	4.70153×10^5	0.9991
allData:BLOCK	0	6.18264×10^5	-6.1035×10^{-5}
allData:CB Fail	1	2.07678×10^5	0.9999
allData:Fault	1	7.08295×10^5	0.9999

1) Case 1 and Case 2 express the normal operations of the protective relay in the digital substation.
2) Case 3 and Case 4 express the potential attacks targeting GOOSE protocol according to the threat model in Section II-C.
3) Case 5 and Case 6 show the effect of the implementation of the proposed encryption and authentication algorithms on the protective relay while applying the attacks presented in Case 3 and Case 4.

Below, we analyze the different cases in detail.

1) CASE 1 AND 2: NORMAL OPERATIONS

- Case 1: a Short Circuit (SC) fault occurs in Transmission Line 2 (TL2), while both CB1 and CB2 are working properly. Based on the substation configuration of Fig. 3, relay1 and relay2 detect SC fault and send a Fault signal (i.e., Trip=0, Block=0, CB Fail =0, and Fault=1) to each other. After a defined time, relay2 sends a Block signal (i.e., Trip=0, Block=1, CB Fail =0, and Fault=1) to relay1 and an opening commend to CB2. Once the CB2 opens and the SC fault is cleared, relay2 sends a Fault-clear signal (i.e., Trip=0, Block=1, CB Fail =0, and Fault=0) to relay1. After 1 second from removing the fault, relay2 closes CB2 again, as shown in Fig. 6.
- Case 2: an SC fault occurs in TL2, while CB2 has a failure (e.g., mechanical failure). Similar to Case 1, relay1 and relay2 detect the SC fault and send a fault signal to each other. After a defined time, relay2 sends a block signal to relay1 and an opening commend to CB2. Relay2 cannot open CB2 in this case, so it sends

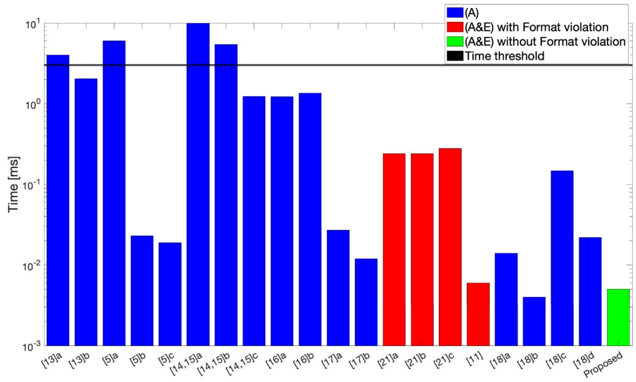

FIGURE 5. Comparison on the time performance of the proposed approach against 20 other state of the art methods which consider only Authentication *A* (blue color) or both Authentication and Encryption *A&E*. In particular, methodologies for Authentication and Encryption that require a format violation of the GOOSE protocol are indicated in red, while the proposed approach (in green) is the only one for *A&E* that does not involve violations. The black line indicates the maximum time threshold of 3[*ms*] set by the protocol.

an Inter-trip signal (i.e., Trip=1, Block=0, CB Fail =1, and Fault=1) to relay1. Relay1 accepts the Inter-trip signal and opens CB1. Consequently, relay2 detects that the fault is cleared and sends a CB failure signal (i.e., Trip=0, Block=0, CB Fail =1, and Fault=0), as shown in Fig. 7.

2) CASE 3 AND 4: ATTACKS

- Case 3: the FDI attack is applied to Case 1. First, the FDI attacker captures a benign Fault signal from the substation network, and then he/she injects a fake Inter-trip signal to this benign signal. Moreover, the attacker uses the Media Access Control (MAC) address of the relay2 to spoof the relay2 identity. After that, the attacker sends the fake Inter-trip signal to relay1 with an increase of the ST of the fake message. Relay1 accepts the fake message and opens CB1, as shown in Fig. 8. The impact of this attack is an unnecessary opening of CB1, leading to a blackout to all the downstream feeders (healthy and faulty).
- Case 4: the MS attack is applied to Case 2. First, the MS attacker captures a benign Block signal from the substation network, and then he/she resends a fake Block signal to Relay1 with an increase of the ST of the fake message. Similar to Case 3, the MS attacker uses the MAC address of the relay2 to spoof the relay2 identity. Relay1 accepts the fake Block signal and ignores the benign Inter-trip signal sent by relay2, as shown in Fig. 9. The impact of this attack is unable to clear the SC fault, which can cause critical damage to the power system infrastructure.

3) CASE 5 AND 6: ADDITION OF THE PROPOSED ALGORITHMS

- Case 5: the procedure is the same as the one presented in Case 3 but with the addition of our proposed authentication and encryption algorithms to verify that our methodology can prevent the attack without affecting the normal operations of the protective relay. Fig. 10 shows that relay1 ignores the fake Inter-trip signal that has $ST = 3$ and considers only the messages sent by relay2.
- Case 6: the procedure is the same as the one presented in Case 4 but with the addition of our proposed authentication and encryption algorithms. Fig. 11 shows that relay1 ignores the fake block signal that has $ST = 4$ and considers only the messages sent by relay2.

From the analysis of the results obtained by the simulations emerges the effectiveness of the proposed authentication methodology in detecting attacks, as in both Case 5 and Case 6 the protection relays are not affected by the attacker and can continue to carry out their normal operations to isolate faults. Moreover, in order to assess the effectiveness of the proposed encryption methodology, we have reported in Table 1 an example of a GOOSE message extracted from the simulations in its original, encrypted, and decrypted formats. As can be observed from the table, the encrypted data belong to completely different scales than the original data (notice that the boolean "test" and "ndsCom" fields are not encrypted because of the data size limitation on these fields), while the decrypted data fully reflect the original message. Note that by applying the proposed approach to single-precision fields and considering diagonal dominant Q matrices, the average accuracy that is achieved on decryption is to the third decimal digit.

After evaluating the effectiveness of the proposed methodology, we investigate its performance, in order to verify that the entire authentication and encryption/decryption procedure is within the time limits imposed by the IEC 61850 standard. Specifically, what emerged from the simulations was an average overall latency of 0.005 milliseconds, well below the 3-millisecond limit imposed by the standard. In Table 2 we report a comparison between the proposed approach and related works, according to a number of relevant criteria. Specifically, the following symbols are used.

- (A), indicates that the approach focuses on providing Authentication for the message;
- (E), indicates that the approach focuses on providing Encryption for the message;
- (A&E), indicates that the approach focuses on providing both Authentication and Encryption for the message;
- (SW), indicates that the approach is based on Software implementation;
- (HW), indicates that the approach is based on Hardware implementation.

The table shows that the proposed approach is the only one capable of providing both authentication and encryption, staying well below the time limits imposed by the protocol, with only 0.17% use of delivery time, and guaranteeing complete compatibility with the GOOSE protocol (without

TABLE 2. Comparison table for proposed security approaches to secure GOOSE messages in digital substations.

Reference	Algorithm	Security Approach		Latency [ms]	Delivery Time Usage	Compatibility with IEC 61850
Hohlbaum et al. [13] (2010)	RSA 1024-bit	(A)	(SW)	4	133%	Time constraint violation
	RSA 1024-bit	(A)	(HW)	2.04	68%	✓
Ishchenko and Nuqui [5] (2018)	RSA 1024-bit	(A)	(SW)	6	200%	Time constraint violation
	HMAC	(A)	(SW)	0.023	0.78%	✓
	GMAC	(A)	(SW)	0.019	0.63%	✓
Farooq et al. [14], [15] (2019)	RSA 1024-bit	(A)	(SW)	10	333%	Time constraint violation
	RSASSA-PSS	(A)	(SW)	5.45	182%	Time constraint violation
	RSASSA-PKCS	(A)	(SW)	1.23	41%	✓
Ustun et al. [16] (2019)	RSASSA-PKCS 1024-bit	(A)	(SW)	1.22	40%	✓
	ECDSA prime256v1	(A)	(SW)	1.35	45%	✓
Hussain et al. [17] (2019)	HMAC-SHA256 80-bit	(A)	(SW)	0.027	0.9%	✓
	AES-GMAC 64-bit	(A)	(SW)	0.012	0.4%	✓
Hussain et al. [21] (2020)	Encrypt-then-MAC AES 256 &HMAC-SHA256	(A&E)	(SW)	0.24	8%	Format violation partially
	Encrypt-and-MAC AES 256 &HMAC-SHA256	(A&E)	(SW)	0.24	8%	Format violation partially
	MAC-then-Encrypt AES 256 &HMAC-SHA256	(A&E)	(SW)	0.28	9.3%	Format violation partially
Rodríguez et al. [11] (2021)	AES-GCM 128-bit	(A&E)	(HW)	0.006	0.2%	Format violation partially
Tefek et al. [18] (2022)	HMAC	(A)	(SW)	0.014	0.46%	✓
	AES-GMAC 128-bit	(A)	(SW)	0.004	0.13%	✓
	LoMoS 16-bit	(A)	(SW)	0.147	4.9%	✓
	CMMA 16-messages	(A)	(SW)	0.022	0.73%	✓
Proposed approach	**Geometric-cryptographic**	**(A&E)**	**(SW)**	**0.005**	**0.17%**	✓

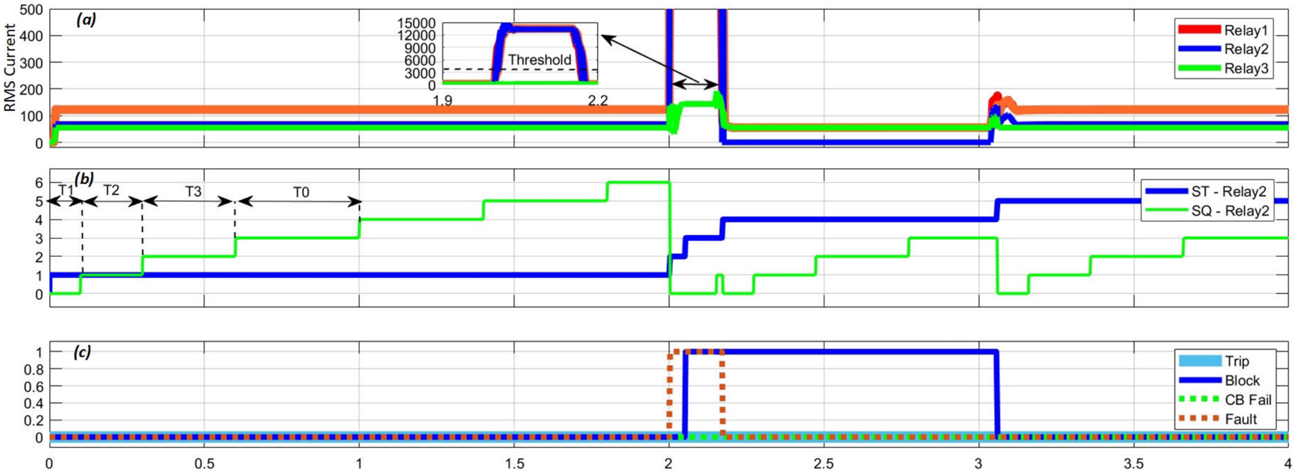

FIGURE 6. Simulation results of Case 1. (a) RMS currents of the relays, (b) ST and SQ of messages sent by relay2 and received by relay1, and (c) the control parameters of the GOOSE message.

additional hardware, latency, and respecting the structure of the GOOSE format). This result is particularly relevant when compared to the most recent and effective state-of-the-art works [16], [17], [18] in terms of speed and applicability, which are only able to offer authentication.

To conclude our analysis, in Fig. 5 we show a comparison of the proposed algorithm against the approaches in Table 2 in terms of authentication, or authentication and encryption (if provided by the approach) time usage. In accordance with the discussion above, the figure shows that, even though several of the existing methods satisfy the 3-milliseconds requirement of the GOOSE protocol, the comparable methods that satisfy both the time and format requirements of GOOSE [16], [17], [18], do not provide

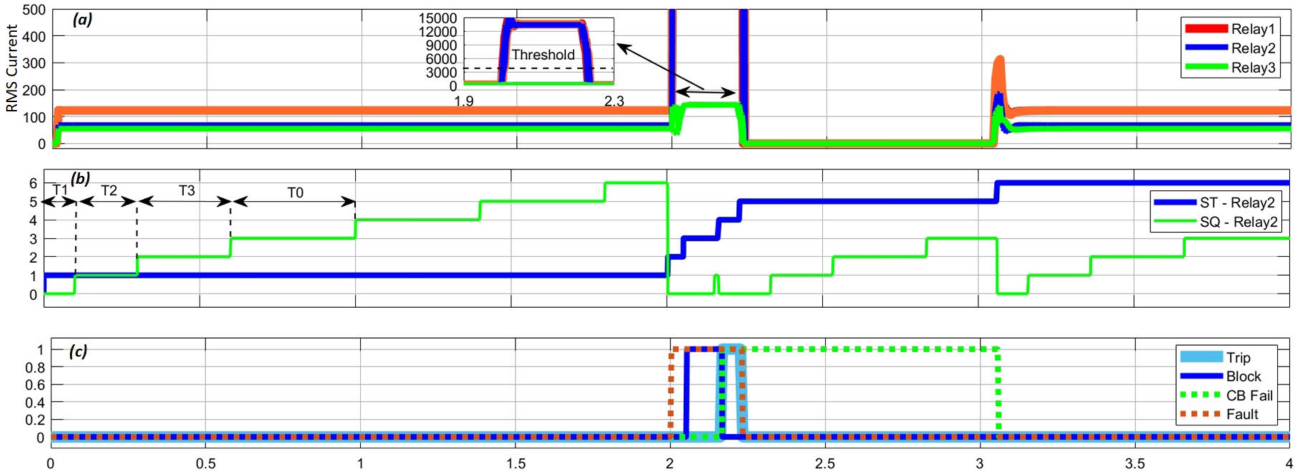

FIGURE 7. Simulation results of Case 2. (a) RMS currents of the relays, (b) ST and SQ of messages sent by relay2 and received by relay1, and (c) the control parameters of the GOOSE message.

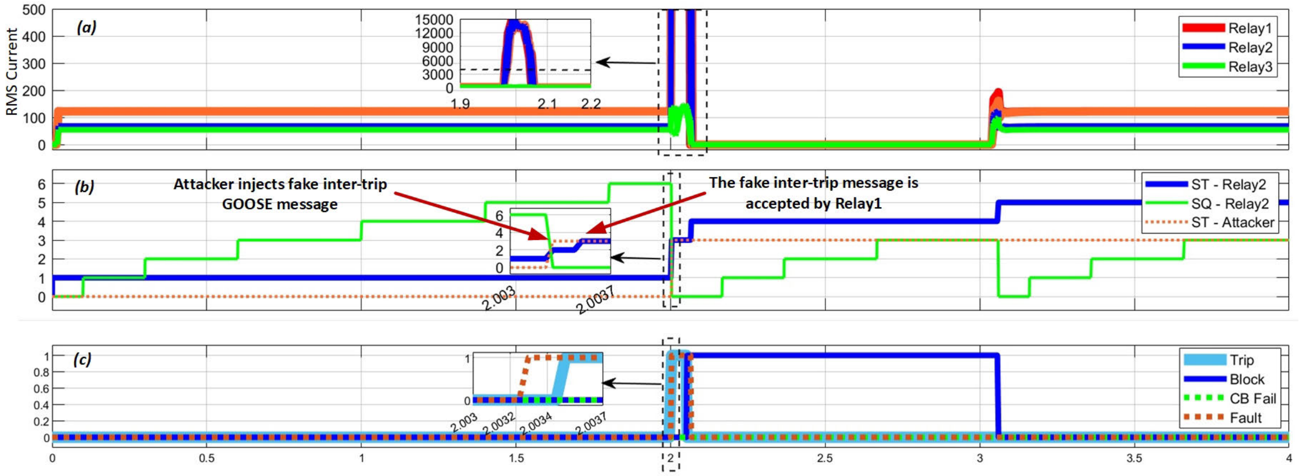

FIGURE 8. Simulation results of Case 3. (a) RMS currents of the relays, (b) ST and SQ of messages sent by relay2/attacker and received by relay1, and (c) the control parameters of the GOOSE message.

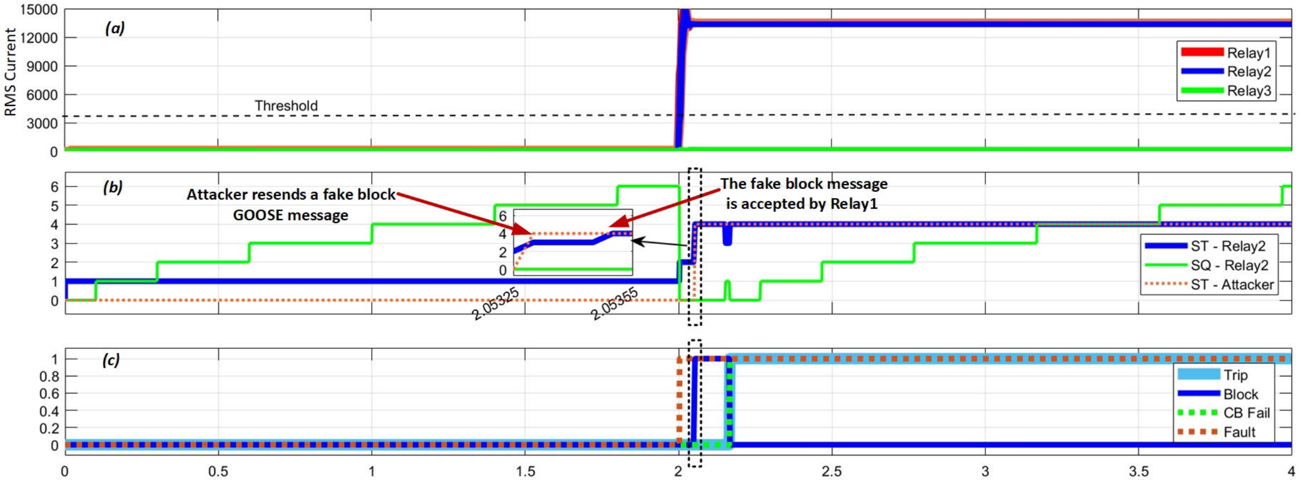

FIGURE 9. Simulation results of Case 4. (a) RMS currents of the relays, (b) ST and SQ of messages sent by relay2/attacker and received by relay1, and (c) the control parameters of the GOOSE message.

encryption. The proposed approach is the only one that can provide authentication and encryption while satisfying both the time and message format requirements.

C. THREATS TO VALIDITY

This subsection discusses the penetration and vulnerability testing of the proposed approach to verify its capability as

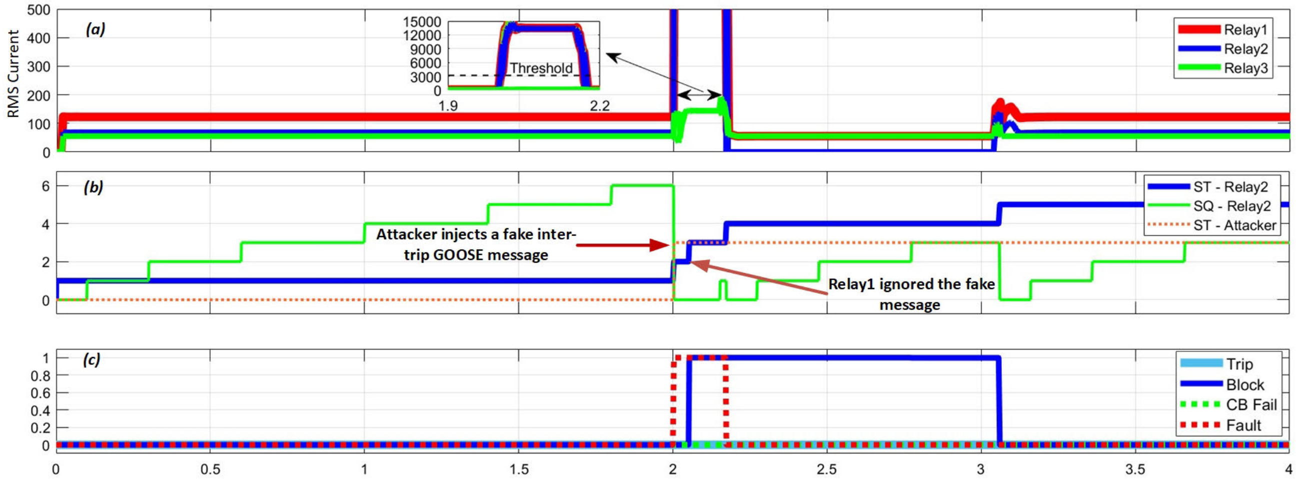

FIGURE 10. Simulation results of Case 5. (a) RMS currents of the relays, (b) ST and SQ of messages sent by relay2/attacker and received by relay1, and (c) the control parameters of the GOOSE message.

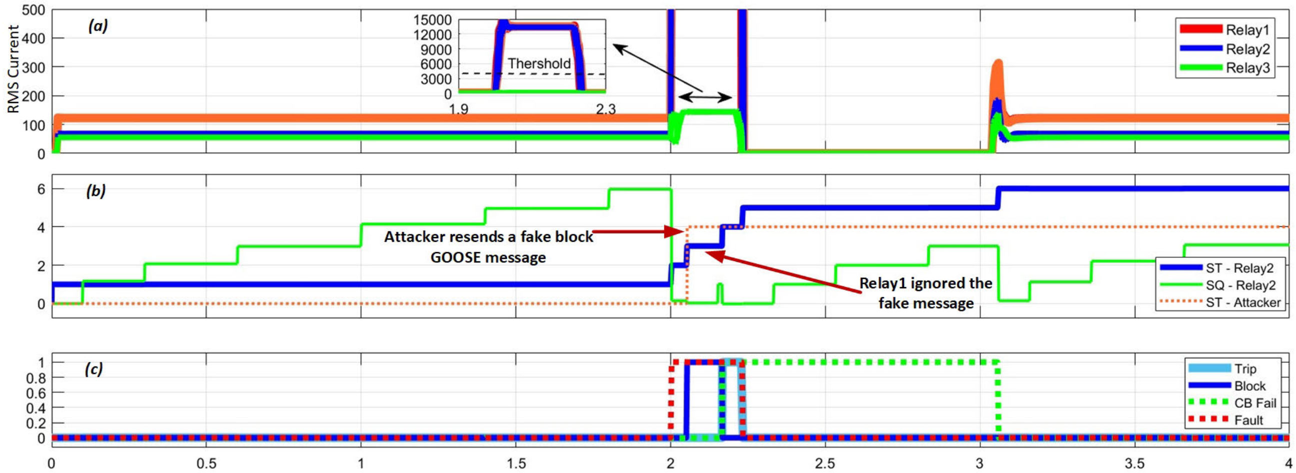

FIGURE 11. Simulation results of Case 6. (a) RMS currents of the relays, (b) ST and SQ of messages sent by relay2/attacker and received by relay1, and (c) the control parameters of the GOOSE message.

a product to secure the GOOSE messages in the digital substation. Previously, in the experiment stage, we simulated an attacker using two different attack techniques, i.e., FDI and MS, to verify the robustness of the proposed approach against these attacks in various cases. Moreover, the technical strength of the proposed approach is discussed in Section III-A, which shows that it is impossible for an attacker to decrypt the message without using the required matrices.

A limitation of the proposed approach is that it relies on a symmetric cryptography scheme. Therefore, the matrices required for encrypting/decrypting the GOOSE messages are stored in the memory of the publisher and subscriber IEDs in the simulation testbed. By assuming that an attacker has access to the publisher and subscriber IEDS, he/she could use the stored matrices to illegally generate encrypted and authenticated GOOSE messages. However, we point out that this assumption is difficult to achieve in real life.

V. CONCLUSION

The paper proposes an innovative methodology for the authentication and encryption of GOOSE messages, addressing the crucial challenge of meeting the strict time constraints imposed by IEC 61850/62351 standards. Adopting a geometric approach that exploits the coordinate shift of a vector, the proposed technique demonstrates remarkable efficiency and speed of implementation. The main advantage of the methodology lies in its ability to meet the strict timing requirements of the protocol, while remaining easy to implement and computationally undemanding, without requiring additional hardware components or changes to the GOOSE message format. Enabling integration into existing infrastructures, our work succeeds in improving the security and reliability of digital substations and critical infrastructure systems without compromising performance or incurring additional costs. As cyber threats evolve, this innovative methodology provides a solid foundation to protect the integrity and confidentiality of critical control messages in power systems.

Through a comprehensive simulation campaign conducted on a digital substation model, the performance of the proposed approach was evaluated and its effectiveness in nullifying cyber attacks was shown. The authentication methodology demonstrated its ability to detect and prevent attacks by ensuring the continuity of normal operations and eliminating failures in the protection system, while the performance investigation of the entire authentication and encryption/decryption process revealed that the proposed methodology performed well within the strict time limits specified by the IEC 61850 standard. Specifically, the overall average latency of 0.005 milliseconds obtained from the simulations falls well within the 3-millisecond limit imposed by the standard, further affirming the feasibility and practicality of this solution in real-world applications.

Future work directions include the application of the proposed methodology to different communication protocols (e.g., Sample Value (SV)) which are used in digital substations. Moreover, alternative approaches including asymmetric encryption mechanisms and time-varying encryption matrices will be investigated, as well as the application of the model to a physical testbed to further explore the performance of the proposed methodology in a realistic environment.

REFERENCES

[1] M. L. Di Silvestre, S. Favuzza, E. Riva Sanseverino, and G. Zizzo, "How decarbonization, digitalization and decentralization are changing key power infrastructures," *Renew. Sustain. Energy Rev.*, vol. 93, pp. 483–498, Oct. 2018.

[2] P. Kalkal and V. K. Garg, "Transition from conventional to modern grids: Modern grid include microgrid and smartgrid," in *Proc. 4th Int. Conf. Signal Process., Comput. Control (ISPCC)*, Sep. 2017, pp. 223–228.

[3] M. A. Aftab, S. M. S. Hussain, I. Ali, and T. S. Ustun, "IEC 61850 based substation automation system: A survey," *Int. J. Electr. Power Energy Syst.*, vol. 120, Sep. 2020, Art. no. 106008.

[4] M. L. De Klerk and A. K. Saha, "A review of the methods used to model traffic flow in a substation communication network," *IEEE Access*, vol. 8, pp. 204545–204562, 2020.

[5] D. Ishchenko and R. Nuqui, "Secure communication of intelligent electronic devices in digital substations," in *Proc. IEEE/PES Transmiss. Distribution Conf. Expo.*, Apr. 2018, pp. 1–5.

[6] M. F. Elrawy, L. Hadjidemetriou, C. Laoudias, and M. K. Michael, "Modelling and analysing security threats targeting protective relay operations in digital substations," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Jul. 2023, pp. 523–529.

[7] Q. Hou and J. Dong, "Distributed dynamic event-triggered consensus control for multiagent systems with guaranteed L_2 performance and positive inter-event times," *IEEE Trans. Autom. Sci. Eng.*, vol. 21, no. 1, pp. 746–757, Jan. 2024.

[8] Q. Hou and J. Dong, "Robust adaptive event-triggered fault-tolerant consensus control of multiagent systems with a positive minimum interevent time," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 53, no. 7, pp. 4003–4014, Jul. 2023.

[9] M. F. Elrawy, L. Hadjidemetriou, C. Laoudias, and M. K. Michael, "Light-weight and robust network intrusion detection for cyber-attacks in digital substations," in *Proc. IEEE PES Innov. Smart Grid Technol.*, Dec. 2021, pp. 1–5.

[10] 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.

[11] M. Rodríguez, J. Lázaro, U. Bidarte, J. Jiménez, 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.

[12] G. Elbez, K. Nahrstedt, and V. Hagenmeyer, "Early attack detection for securing GOOSE network traffic," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 899–910, Jan. 2024.

[13] F. Hohlbaum, M. Braendle, and F. Alvarez. *Cyber Security Practical Considerations for Implementing*, Standard IEC 62351, 2022. [Online]. Available: https://library.e.abb.com/

[14] 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.

[15] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "S-GoSV: Framework for generating secure IEC 61850 GOOSE and sample value messages," *Energies*, vol. 12, no. 13, p. 2536, Jul. 2019.

[16] T. S. Ustun, S. M. Farooq, and S. M. S. Hussain, "A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard," *IEEE Access*, vol. 7, pp. 156044–156053, 2019.

[17] 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.

[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)*, Oct. 2022, pp. 224–230.

[19] E. Esiner, U. Tefek, H. S. M. Erol, D. Mashima, B. Chen, Y.-C. Hu, Z. Kalbarczyk, and D. M. Nicol, "LoMoS: Less-online/more-offline signatures for extremely time-critical systems," *IEEE Trans. Smart Grid*, vol. 13, no. 4, pp. 3214–3226, Jul. 2022.

[20] S. Hussain, A. Iqbal, S. M. S. Hussain, S. Zanero, A. Shikfa, E. Ragaini, I. Khan, and R. Alammari, "A novel hybrid methodology to secure GOOSE messages against cyberattacks in smart grids," *Sci. Rep.*, vol. 13, no. 1, p. 1857, Feb. 2023.

[21] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, "A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages," *IEEE Trans. Power Del.*, vol. 35, no. 5, pp. 2565–2567, Oct. 2020.

[22] P. Matoušek, "Description of IEC 61850 communication," Brno Univ. Technol., Brno, Czechia, Tech. Rep., 2018.

[23] M. G. D. Silveira and P. H. Franco, "IEC 61850 network cybersecurity: Mitigating GOOSE message vulnerabilities," in *Proc. PAC World Americas Conf.*, 2019, pp. 1–9.

[24] M. F. Elrawy, E. Tekki, L. Hadjidemetriou, C. Laoudias, and M. K. Michael, "Protection and communication model of intelligent electronic devices to investigate security threats," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Jan. 2023, pp. 1–5.

[25] A. Ingalalli, K. S. Silpa, and R. Gore, "SCD based IEC 61850 traffic estimation for substation automation networks," in *Proc. 22nd IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2017, pp. 1–8.

[26] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure," in *Proc. IEEE Globe Work*, Dec. 2012, pp. 1508–1513.

[27] N. S. Kush, E. Ahmed, M. Branagan, and E. Foo, "Poisoned GOOSE: Exploiting the GOOSE protocol," in *Proc. 12th Australas. Inf. Secur. Conf., Conf. Res. Pract. Inf. Technol. (AISC)*, vol. 149, 2014, pp. 17–22.

[28] H. T. Reda, B. Ray, P. Peidaee, A. Anwar, A. Mahmood, A. Kalam, and N. Islam, "Vulnerability and impact analysis of the IEC 61850 GOOSE protocol in the smart grid," *Sensors*, vol. 21, no. 4, p. 1554, Feb. 2021.

[29] J. Hong, T.-J. Song, H. Lee, and A. Zaboli, "Automated cybersecurity tester for IEC61850-based digital substations," *Energies*, vol. 15, no. 21, p. 7833, Oct. 2022.

[30] M. Boeding, M. Hempel, H. Sharif, J. Lopez, and K. Perumalla, "A flexible OT testbed for evaluating on-device implementations of IEC-61850 GOOSE," *Int. J. Crit. Infrastruct. Protection*, vol. 42, Sep. 2023, Art. no. 100618.

[31] J. G. Wright and S. D. Wolthusen, "Stealthy injection attacks against IEC61850's goose messaging service," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. Eur. (ISGT-Europe)*, Feb. 2018, pp. 1–6.

[32] C. Fioravanti, L. Faramondi, G. Oliva, and C. Hadjicostis, "A geometrical approach for consensus security," *Syst. Control Lett.*, vol. 185, Mar. 2024, Art. no. 105717.

[33] M. El Hariri, T. Youssef, and O. Mohammed, "On the implementation of the IEC 61850 standard: Will different manufacturer devices behave similarly under identical conditions?" *Electronics*, vol. 5, no. 4, p. 85, Dec. 2016.

MOHAMED F. ELRAWY (Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from the Electrical Engineering Department, Assiut University, Egypt, in 2010 and 2014, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Cyprus. He is also a Researcher with the KIOS Research and Innovation Center of Excellence (CoE). His research interests include the field of computer networks, cloud computing, cybersecurity, and smart environments.

CAMILLA FIORAVANTI (Graduate Student Member, IEEE) received the M.Sc. degree in biomedical engineering from the University Campus Bio-Medico of Rome, Italy, in 2020, where she is currently pursuing the Ph.D. degree in science and engineering for humans and the environment, under the supervision of Prof. Gabriele Oliva. She spent a visiting period with the University of Cyprus, Nicosia, Cyprus. Her main research interests include distributed systems, distributed estimation, security and privacy-preserving approaches, and fault detection.

GABRIELE OLIVA (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science and automation engineering from the University Roma Tre of Rome, Italy, in 2008 and 2012, respectively. He is currently an Associate Professor in automatic control with the University Campus Bio-Medico of Rome, Italy, where he directs the Complex Systems & Security Laboratory (CoserityLab). His main research interests include distributed multi-agent systems, optimization, decision-making, and critical infrastructure protection. Since 2019, he has been serving as an Associate Editor on the Conference Editorial Board of the IEEE Control Systems Society. Since 2020, he has been serving as an Academic Editor for the journal *PLOS One* on subject areas, such as systems science, optimization, and decision theory. Since 2022, he has been an Associate Editor for IEEE Control Systems Letters journal.

MARIA K. MICHAEL (Member, IEEE) received the B.Sc. and M.Sc. degrees in computer science and the Ph.D. degree in engineering sciences (specialization in computer engineering) from Southern Illinois University (SIU), USA. She is currently an Associate Professor with the ECE Department, University of Cyprus (UCY). Prior to joining UCY, she taught as a Lecturer with the ECE Department, SIU, and an Assistant Professor in computer science and engineering with the University of Notre Dame, USA. She is also a co-founding Faculty Member of the KIOS Center of Excellence, UCY. Her research interests include the areas of dependability and security in embedded and the IoT-enabled cyber-physical systems. She has extensive expertise in the areas of electronic design automation (CAD), test, diagnosis, reliability, fault tolerance, and the safety of large-scale integrated circuits and (safety-critical) embedded systems. Her current research interests include hardware-enabled security and cyber-security in intelligent embedded systems and cyber-physical systems, the optimization of performance and the dependability of AI/ML edge intelligence, the reliability and security of resource-constrained edge-based accelerators, with applications in intelligent critical infrastructure systems, such as smart grids, UAVs, robotics, and autonomous vehicles. Her research has been funded by several local and international agencies and industry in Europe and the United States, such as EU FP7, EU H2020, Horizon Europe, EU COST, NSF, Intel Corporation, and the Cyprus Research and Innovation Foundation.

ROBERTO SETOLA (Senior Member, IEEE) received the Laurea degree in electronic engineering and the Ph.D. degree in control engineering from the University of Naples Federico II, in 1992 and 1996, respectively. He was responsible for the Italian Government Working Group on Critical Information Infrastructure Protection (CIIP) and a member of the G8 Senior Experts' Group for CIIP. He is currently a Full Professor with the University Campus Bio-Medico of Rome, where he directs the Automation Research Unit and the Master Program in Homeland Security. He has been the Coordinator of several EU projects. He has authored nine books and more than 250 scientific articles. His research interests include the simulation, modeling, and control of complex systems, and critical infrastructure protection.

Open Access funding provided by 'Università "Campus Bio-Medico" di Roma' within the CRUI CARE Agreement