IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 25, 2019, accepted October 13, 2019, date of publication October 17, 2019, date of current version November 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2948117

A Novel Approach for Mitigation of Replay and Masquerade Attacks in Smartgrids Using IEC 61850 Standard

TAHA SELIM USTUN[1], (Member, IEEE), SHAIK MULLAPATHI FAROOQ[2], (Member, IEEE), AND S. M. SUHAIL HUSSAIN[1], (Member, IEEE)

[1]Fukushima Renewable Energy Institute, AIST (FREA), Koriyama 963-0298, Japan
[2]Department of Computer Science and Engineering, YSR Engineering College, Yogi Vemana University, Kadapa 516360, India

Corresponding author: Shaik Mullapathi Farooq (smfarooq@ieee.org)

This work was supported in part by the Fukushima Prefecture's Reconstruction Grant, under Grant 2019.

ABSTRACT There is growing awareness towards cybersecurity threats in power systems. Deployment of more intelligent electronic devices (IEDs) and the communication lines increase the probability of such attacks. IEC 61850 standard facilitates communication between different IEDs and eases interoperable operation with set data and message structures. An unwanted consequence of this standardized communication over ethernet is increased viability to cyber threats. Replay and masquerade attacks are, especially, of concern due to their imminent impact on the operation. While detecting replay attacks is easier, since the original messages are used for the attack, masquerade attack messages may be difficult to distinguish from original ones. Furthermore, inadequate mitigation approaches may be tricked by the hackers and the system starts the attacker as the authentic sender and discards original messages from authentic sources. It is vital to develop an approach that incorporates message authentication. In this fashion, when the hackers modify the message contents to by-pass security systems, the tampering can be detected, and the messages will be discarded. This paper analyses replay and masquerade attacks on IEC 61850 GOOSE messages and develops a solution to mitigates both of those. To detect modified messages, two distinct authentication mechanisms are utilized: RSA since it is the algorithm stipulated in IEC 62351-6 and Elliptic Curve Digital Signature Algorithm (ECDSA) due to its widespread use in smartgrid cybersecurity solutions. A full solution to mitigate GOOSE replay and masquerade attacks is developed based on the proposed framework in IEC 62351 standard. Full implementation is tested in the lab and results are included to show the viability of the solution.

INDEX TERMS Cyber-physical systems, cybersecurity in power systems, IEC 61850, IEC 62351, digital signature algorithms, message integrity check.

NOMENCLATURE

Symbol	Explanation
goosePDU	GOOSE data frame
gooseAPDU	The payload field of GOOSE packet consists of data in TLV format
goosePDU.extension	Extension field of GOOSE data frame
PrKey	Private Key of Digital Signature Algorithm
PubKey	Public Key of Digital Signature Algorithm
DSA	Digital Signature Algorithm (RSA or ECDSA)
h, h1	Hash value generated by SHA256
ds	Digital signature
Stnum	Status number of GOOSE frame
Sqnum	Sequence number of GOOSE frame
Sqnumarr	An array to store received the Sqnum values of received GOOSE messages

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

t	Time to Stnum increase algorithm
$timeAllowedToLive$	Maximum waiting time for GOOSE frame

I. INTRODUCTION

IEC 61850 is the de-facto communication standard for Substation Automation Systems (SAS) [1]. It integrates different functions in a substation into a single protocol. Besides interoperability among multi-vendor substation intelligent electronic devices (IEDs), it also offers seamless communication, lower configuration and installation cost [2]. Logical nodes and data sets define substation communication equipment based on Substation Configuration Description (SCD) files. IEC 61850 utilized three distinct messages for different operation purposes. Generic Object-Oriented Substation Event (GOOSE) and Sample Value (SV) protocols are utilized for operations related to events and measurements, respectively. Manufacturing Message Service (MMS) is utilized for supervisory control information among IEDs.

IEC 61850's popularity can be attributed to two main factors: ease of connection via ethernet instead of traditional hard-wired systems and standardized message structures which ensures interoperability [3]. An unwanted consequence of these is the increased vulnerability to cyber-attacks. It is easier to access ethernet-based networks and standardized messages allow hackers to know exactly what instructions to give. IEC 62351-6 standard is published to complement IEC 61850 by adding security features [4].

Reliance on information infrastructure for monitoring, control and operation of substation operations increases the importance of data security. Compromising on this may lead to a plethora of attacks which may lead to significant losses in power systems [5]. The inputs from IEDs are used by the Supervisory Control and Data Acquisition (SCADA), Power System Automation PSA) [6], energy management (EM) [7] subsystems for monitoring and control operations. Authors in [8] analyzed and documented three major weaknesses in IEC 62351 protected smart grid systems such as replay attack on GOOSE, SV and attack on Simple Network Time Protocol (SNTP) protocol. Authors in [9] presented a new methodology to detect security attacks in IEC 61850 based systems with anomaly detection. GOOSE packets which behave differently are treated as intrusion. However, this solution cannot differentiate between anomalies caused during operation, such as packet switch due to traffic, and malicious attacks. Furthermore, this system is helpless against masquerade attacks where a smart hacker can change the contents of GOOSE packages and trick the system. Authors, in [10], tested safety related functions of IEC 61850 GOOSE messaging experimentally and showed that some IEC 61850 compliant devices can detect incorrect sequence, unacceptable delay, unintended repetition, although they cannot detect if these anomalies are caused by local traffic. In other words, these devices cannot detect if they are under attack or packets are delayed due to heavy transmission load.

Therefore, there is a clear need in the literature for a mitigation technique that can detect replay and masquerade attacks with IEC 61850 GOOSE messages. It is also required that this technique follows IEC 62351-6 standard for full compliance. This paper develops a full mitigation solution against GOOSE replay and masquerade attacks. It analyzes and evaluates authentication mechanisms using RSA (Rivest-Shamir-Adleman) [11] with different key sizes and Elliptic Curve Digital Signature Algorithm (ECDSA) [12] with different elliptic curves. RSA algorithm is selected as it is stipulated by IEC 62351-6 while ECDSA is selected to be the comparison case due to its popularity in smartgrid cybersecurity domain [13]. Using these two digital signature algorithms (DSAs). A security mechanism is implemented to mitigate masquerade and replay attacks based on the proposed framework in the standard. Results of lab tests and message authentication timing performances are noted for comparison and analysis.

Rest of the paper is organized as follows: Section III explains how replay and masquerade attacks are done with GOOSE messages. Section IV explains the developed technique to mitigate both attacks. Section V shows experimental results of masquerade and replay attacks and how they are mitigated. The developed mitigation mechanism is evaluated using openSSL C libraries. Finally, Section VI concludes the paper with future recommendations.

II. REPLAY AND MASQUERADE ATTACKS WITH GOOSE

Cyber-physical systems (CPS) are at the interface of information and energy exchange. Failure in securing information security may cause unwanted events in energy exchange with high-scale impacts. Many reports discuss possible cyber-attacks on the power grid [8]–[9], [14], such as SAS, Distribution Automation System (DAS), Advanced Metering Infrastructure (AMI) and Electricity markets. In order to understand these vulnerabilities, it is important to understand physical topology and messaging structure utilized.

Ensuring security of these messages is critical by satisfying requirements such as integrity, authentication, service availability and message confidentiality. Compromising any of these requirements lead to many types of vulnerabilities. Examples of possible attacks making use of these vulnerabilities are False Data Injection, Denial of Service, Man in the Middle, Replay and Masquerade attacks.

In literature, different types of attacks on IEC 61850 substation such as PTP delay attack [15], anomaly detection in GOOSE and SV messages [16], integrity attack [17], etc., are reported. Except for IEC 61850-90-5 which only focuses on cybersecurity of Routable-GOOSE and SV values (R-Goose and R-SV), current IEC 61850 standard does not specify security features to address these cyber-security vulnerabilities [18]. IEC 62351 is published to complement IEC 61850 standard. It specifies necessary cryptographic features without compromising the performance of the protocols. As SV and GOOSE has strict timing requirements, IEC 62351 proposes use of lightweight algorithms for all aspects

mentioned above. However, IEC 62351 does not have full solutions geared towards mitigating certain attacks. It simply recommends some techniques such as message integrity and node authentication.

This paper considers replay and masquerade attacks that can be performed on power system communication networks that run on IEC 61850 standard. The below sections talks about how these attacks can be performed and presents a new technique to mitigate these based on IEC 62351 standard's framework.

A. GOOSE PROTOCOL OPERATION

One of the promising features of IEC 61850 is unification of data exchange in the power utility automation. This unification is achieved based on Logical Nodes (LNs). A LN is a representation of a physical functional unit such as merging unit or protection IED. Data can be exchanged between two LNs which represent different IEDs. Interoperability among the multivendor devices is achieved with LNs as they consist of data objects which may be associated with other LNs as well. Data objects are defined by Common Data Classes (CDC) that are predefined data types. For example, Fig. 1 shows an LN called XCBR for a Circuit Breaker IED which consists of Pos (switching position). This is as a data object with Controllable Double Point (DPC) as its designated CDC. On the other hand, CBOpCap (Circuit Breaker operating) is a data object with INS as its CDC designation. Each data object of a LN consists of one or more data attributes. Pos has attributes stVal, quality, and timestamp. Grouping of data objects and attributes can be done with data sets. The figure shows a dataset of POS data object. Datasets are configurable sets of CDCs and attributes of one logical node that can be used for communication with other logical nodes.

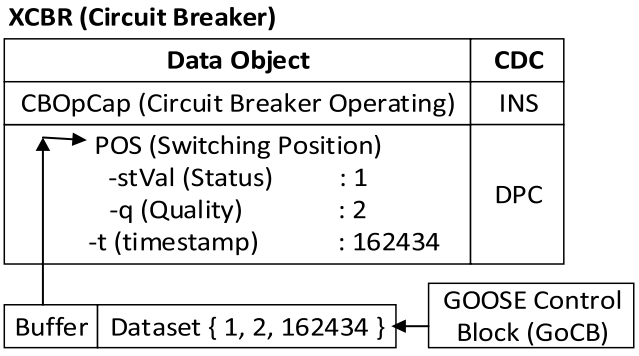

FIGURE 1. XCBR Logical Node and Data Objects.

The communication protocols defined by IEC 61850 such as SV and GOOSE make use of this LN structure in data exchange in their publish-subscribe model. For example, the dataset shown in the Fig. 1 for the data attributes *stVal*, *q* and *t* will be transmitted from a circuit breaker to a protection IED using GOOSE protocol messages to update the status of the breaker. Each dataset has a buffer to store the data. The data values are defined by the control block (e.g., GOOSE Control Block (GoCB)) which defines the communication relationship among the sender and receiver nodes. GoCB defines many parameters such as GoID (buffer id), GoCBRef (GOOSE Control Block Reference), t (timestamp), and timeAllowedToLive (lifetime of the GOOSE messages).

GOOSE messages are event driven. They are published when an event happens such as high voltage detection. When a fault occurs, protection IED sends bursts of GOOSE messages. In order to ensure the message is delivered, after the event, GOOSE messages are sent periodically. In this situation, the transmission interval of GOOSE messages sequentially increases to normal periodic nature as shown in the Fig. 2.

T_0 is the time interval between GOOSE messages in periodic mode. T_0, T_1, T_2, T_3, ... T_n are the time intervals of GOOSE messages in burst mode. The relationship $T_1 < T_2 < T_3 < T_4 ..... < T_n$ holds for the burst mode time interval. GOOSE messages contain *Sqnum* values from 0 to 4294967295. For each GOOSE message released, the *Sqnum* value is incremented by one. *Stnum* value ranges from 1 to 4294967295 and it is updated with a new event. Fig. 2 shows how *Sqnum* and *Stnum* values change with periodic publication and an event. With the event, Stnum is incremented to 2 and Sqnum is initialized to zero.

B. REPLAY ATTACK ON GOOSE MESSAGES

Figure 3 demonstrates how a replay attack works on a GOOSE message sent between two terminals. The figure shows that protection IED picks up a fault and sends a trip command to breaker IED via GOOSE messages. Initially, a message with sequence number (*Sqnum*) 0 is sent. After receiving it, breaker IED performs the trip operation. Further messages are retransmitted with increasing sequence numbers for the same event, i.e. *Stnum* is kept the same.

An attacker who has access to the network captures the first frame with $Sqnum = 0$. After the fault is cleared and the breaker recloses, the attacker *replays* the captured packet. Breaker IED receives this frame as a new trip command and performs trip operation immediately. Unless there is a mitigation technique that uses *Sqnum and Stnum* values, attacker can make the relay trip whenever he desires. Mitigating this attack is much simpler as the contents of the captured packet are not modified at all. If the receiver IED keeps track of received GOOSE frames, it can clearly detect if a back-dated frame is re-sent and can discard it.

C. MASQUERADE ATTACK ON GOOSE MESSAGES

Masquerade attack is much harder to detect as the hacker modifies the GOOSE frame data values. As shown in Fig. 4, hacker captures the first packet sent to the breaker IED with $Sqnum = 0$. In order to avoid basic replay attack mitigation techniques that keep track of these values, attacker modifies *Sqnum* as 4 and sends the packet. Although it is identical to the captured packet, increase in *Sqnum* makes breaker IED to believe that this is a new, legitimate packet.

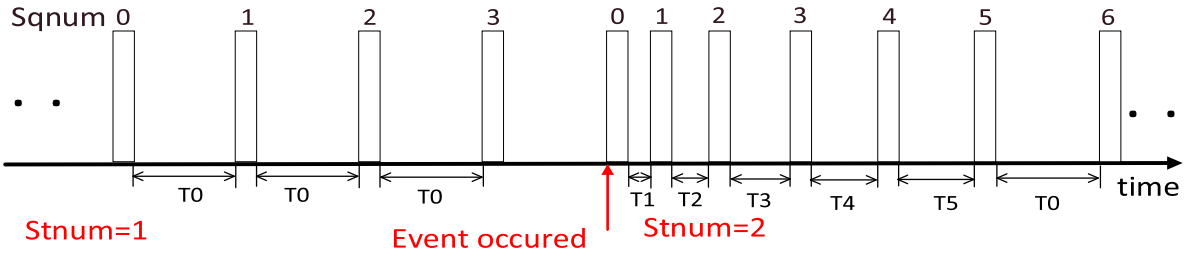

FIGURE 2. GOOSE messages after event occurred.

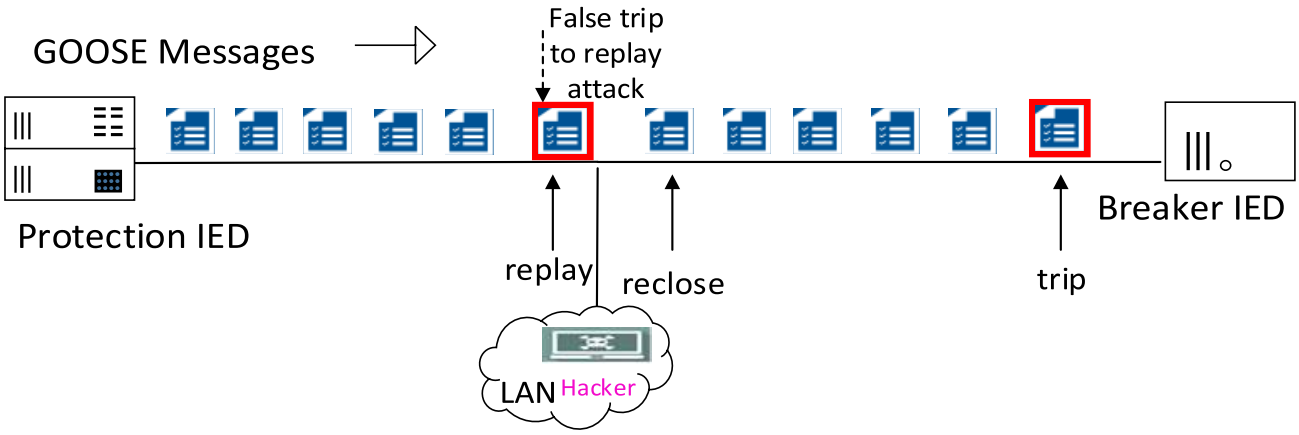

FIGURE 3. Replay attack on GOOSE messages.

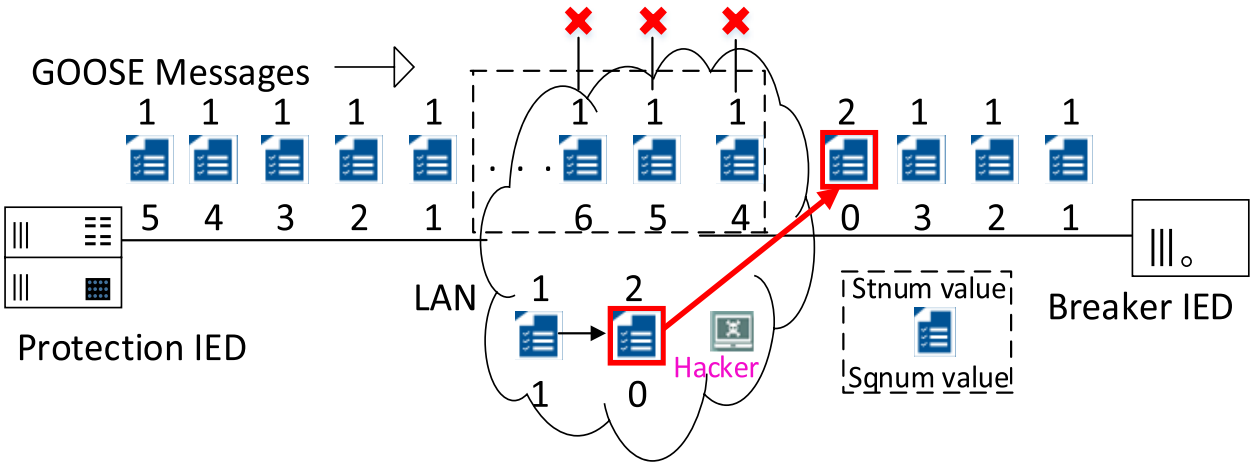

FIGURE 4. Masquerade attack on GOOSE messages.

By using masquerade attack, a smart hacker is able to get ahead of the basic replay attack mitigation techniques as presented in [9]. The algorithm presented in [9] compares the *Sqnum* and *Stnum* values and discards GOOSE messages with older entries, considering that the new one messages must be from the legitimate sender while old entries must be sent by the attacker. When the hacker has the ability to change the contents of the message, it is possible to trick this mechanism. As shown in Fig. 4, hacker can artificially increase *Stnum* and *Sqnum* values, thereby posing its messages as the legitimate ones. GOOSE messages coming from the authentic IED will be discarded as they have older *Stnum* and *Sqnum* values, when compared with the incoming messages from the hacker. In this fashion, hacker will be treated as the authentic sender and the protection IED will lose communication completely.

Masquerade attack can cause false tripping even with basic mitigation techniques mentioned above. Those techniques keep track of the trip signals received and refuses to react to the signals with same *Sqnum* and *Stnum* values. As shown in Fig. 4, a smart hacker may circumvent this by changing

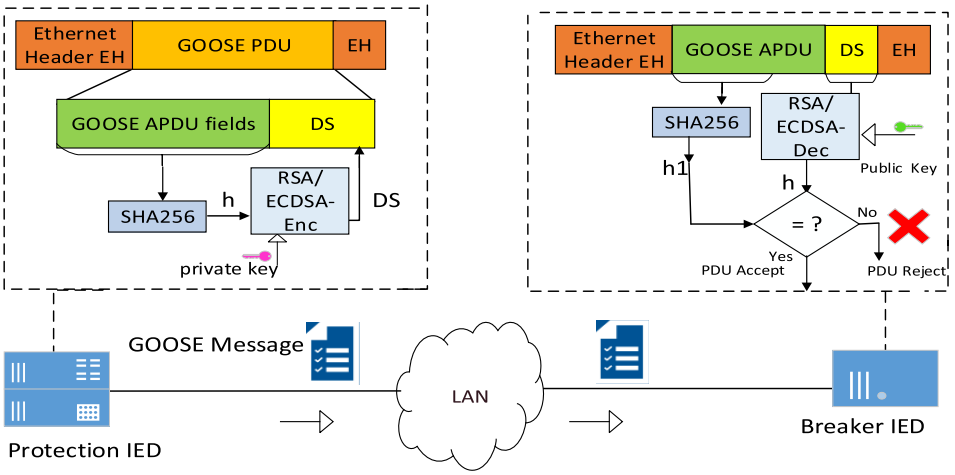

FIGURE 5. Security Suite for Masquerade and Replay attack with GOOSE messages.

Algorithm Gen_DS(goosePDU)
1: gooseAPDU ← *goosePDU.payload*
2: $h \leftarrow SHA256\ (gooseAPDU)$
3: $ds \leftarrow DSA_{PrKey}(h)$
4: goosePDU.Extension ← *ds*

these values and send trip commands as if they belong to a new event, i.e. with a new *Stnum* value. Algorithms present in the literature do not have any means to detect these attacks. In addition to following GOOSE message numbers, a holistic approach should be developed where message tempering is checked. Next section presents the novel mitigation technique which includes message integrity check with digital certificate algorithms.

III. DEVELOPED MITIGATION TECHNIQUE BASED ON IEC 62351-6

IEC 62351-6 standard recommends digital signatures generated by SHA256 and RSA public key algorithm to ensure integrity and authentication of the GOOSE messages. These security algorithms are applied on the GOOSE messages before being sent to the network. In this paper, two different security algorithms are implemented to detect the security attacks. These are RSA and ECDSA with different curves, the former as stipulated by IEC 62351 and the latter due to its popularity in smartgrid cybersecurity domain.

The developed cyber-security solution is depicted in Fig. 5. At publisher side, a simple algorithm is followed, ***Algorithm Gen_DS.*** Initially, the payload field of GOOSE is copied to *gooseADPU*. Then, hash value h is generated using the recommended SHA256 authentication algorithm for the Application Protocol Data Unit (APDU) fields of GOOSE Protocol Data Unit (PDU) in the ethernet frame.

In the third step, the hash value is signed by the DSA to generate a Digital Signature (DS). The signing process

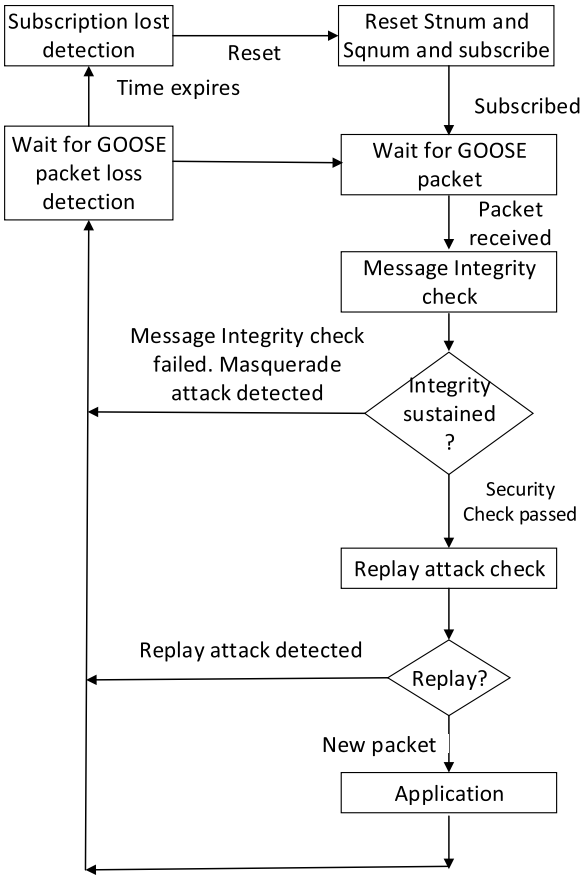

FIGURE 6. GOOSE message integrity and replay attack check in the client.

includes encrypting the hash value with the private key, (*PrKey*), of DSA, which can be RSA or ECDSA. The generated digital signature is stored in the extension field of GOOSE PDU. In this fashion, hash value can be used to check whether the message content is modified while signing with DSA makes sure that the hash value in the GOOSE message

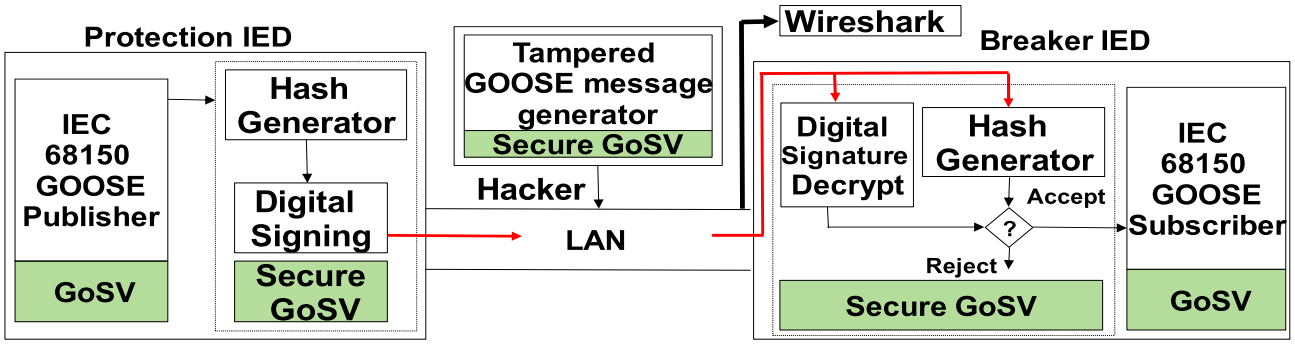

FIGURE 7. Experimental Test Setup.

is the genuine value sent by the authentic publisher and not an imposter.

At the subscriber side, ***Algorithm verify_GOOSE***, is implemented to perform several checks, as shown in Fig. 6. Firstly, the message integrity and digital security are checked to ensure that the payload and hash values are not tampered with and sent by the authorized publisher. The hash value (*h1*) of the received GOOSE APDU fields is computed with SHA256 algorithm. Then, the hash value, *h*, computed and appended by the publisher is decrypted with public key, *PubKey,* of DSA. If this hash value was modified by someone, then, it cannot be decrypted with *PubKey,* and this detects message integrity infringement in the hash value. If it is not modified and the decryption is successful, decrypted output *h* is compared with newly calculated *h1*. If both hash values match, then it is also confirmed that the message content is not modified. This ensures that there is no masquerade attack as the message contents are not modified. However, it is not clear whether this is a legitimate packet arriving for the first time or a legitimate packet held and replayed by a hacker. An additional check is required to check against a replace attack.

In replay attack check, *Stnum, Sqnum* and *timestamp (t)* values are checked as shown in the algorithm and Fig. 6. Under normal conditions, *Stnum* of the current package cannot be smaller than *Stnum* of the previous package while *Sqnum* value has to be larger. Otherwise, it means that a package that is earlier in time is being sent. This can be due to two reasons, a packet switch during transmission due to heavy traffic or a replay attack. Previous solutions in the literature cannot distinguish between these two cases. However, in *verify_GOOSE,* step 6 performs two additional checks: whether the current package has been received earlier and whether the delay between two packets is greater than *timeAllowedToLive*. If not, incoming packet is still legitimate but arrives late due to heavy traffic. If the all the conditions outlined in Fig. 6 are met, then the GOOSE frame is accepted as a legitimate frame. Otherwise it is discarded by the client. Depending on the security check the package fails, the attack can also be classified as *masquerade or replay* attack.

Algorithm verify_GOOSE(goosePDU previous, goosePDU current)

1: *ds*← current.*extension*
2: *gooseAPDU*←*current.payload*
3: *h1*← *SHA256 (gooseAPDU)*
4: *h* ← $DSAC_{PubKey}(ds)$
5: if *h* =*h1*
then
6: *st*←*(current.Stnum*≥*previous.Stnum) and current.Sqnum*≠*(previousSqnumarr[]) and previous.t-current.t <= timeAllowedToLive*
7: if *st* then
return "Accept GOOSE packet"
8: *else*
9: *return "Replay attack detected reject"*
10: *end if*
11. *else*
12. *return "Masquerade attack detected reject"*
11: *endif*

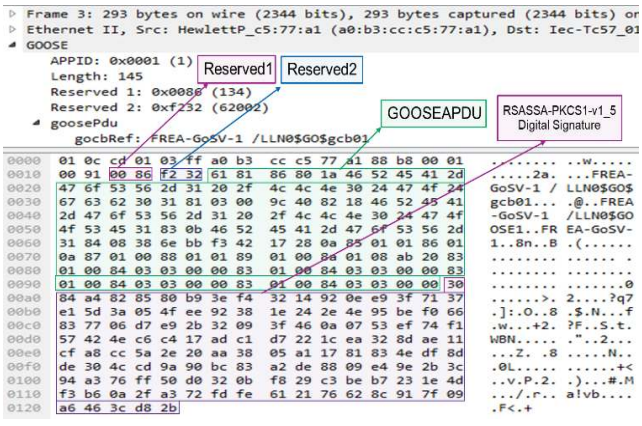

FIGURE 8. Secure GOOSE message with RSA digital signature.

IV. IMPLEMENTATION RESULTS

Authors have developed a custom-software framework, GoSV [19], to generate custom GOOSE and Sample Values.

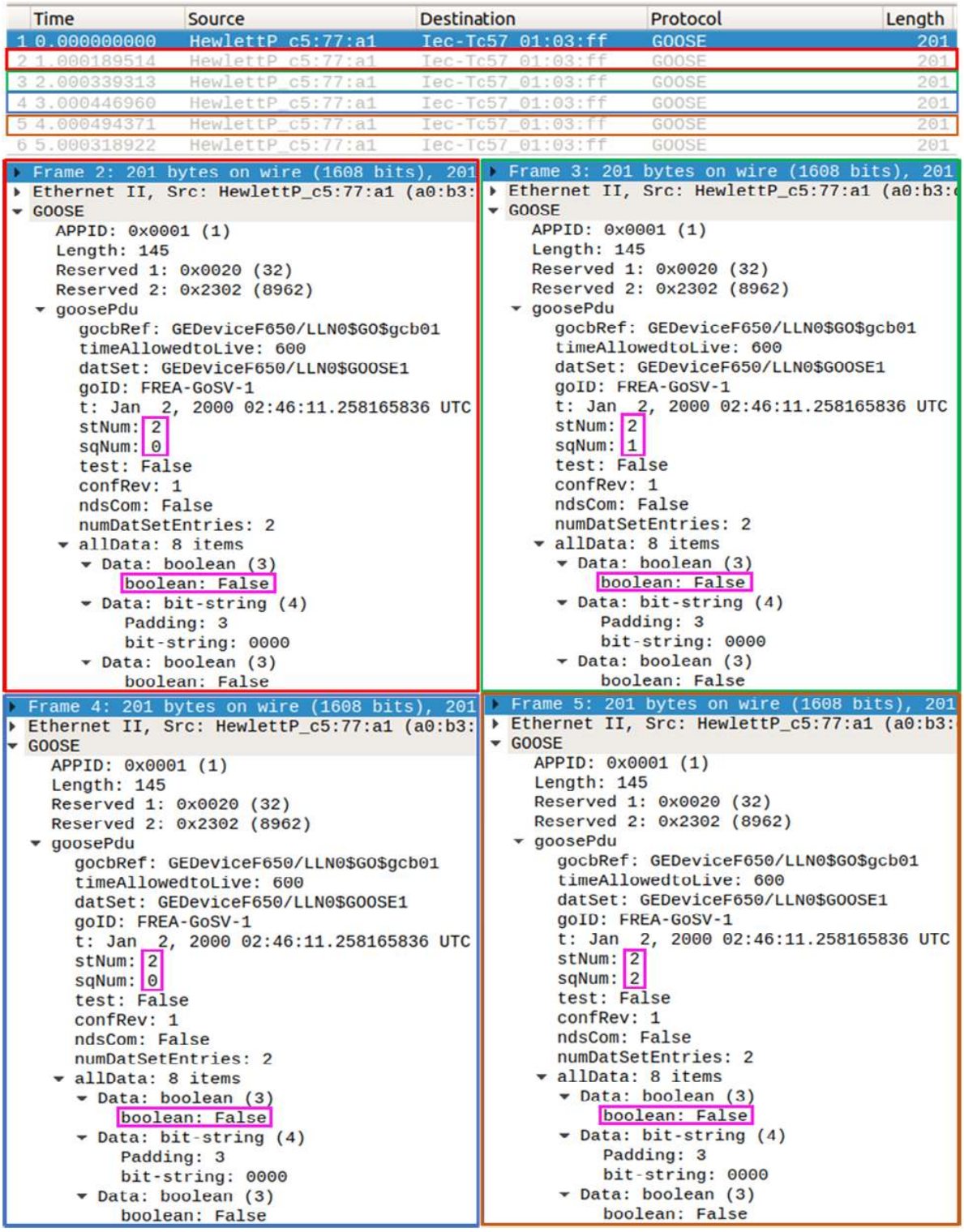

FIGURE 9. Replay attack on GOOSE packet.

To validate the generated GOOSE and Sample Values, the packets were sent to commercial Infotech Avenue GOOSE receiver [20] running in Windows platform and Libiec61850 GOOSE subscriber module [21] running on Linux platform. Both software modules successfully detected the stream of custom values. Security mechanism described in section III is integrated with GoSV and GOOSE messages are sent. Figure 7 shows the experimental setup with two

```
GOOSE Frame:[1] with stnum value:[2] and sqnum value:[0] is received
GOOSE Frame:[2] with stnum value:[2] and sqnum value:[1] is received
GOOSE Frame:[3] with stnum value:[2] and sqnum value:[0] is received
GOOSE Frame with Previous sqnum value is received

**REPLAY ATTACK DETECTED**

GOOSE Frame:[4] with stnum value:[2] and sqnum value:[2] is received
```

FIGURE 10. Replay attack detection by subscriber.

PCs connected through a LAN running the secure GoSV (S-GoSV) frameworks. A capture of secure GOOSE message with RSA based digital signatures published by S-GoSV framework is shown in Fig. 8.

Figure 9 shows the Wireshark captures of the detection of replay attack. Figure shows the captured GOOSE frame fields. *Stnum* and *Sqnum* values are 2 and 0, respectively, for the second GOOSE frame shown in green. This frame is captured by the attacker. *Sqnum* value is incremented for each retransmission of GOOSE message. Captured frame is retransmitted after the third frame shown in blue in Fig. 9. Upon receiving the packets, subscriber compares the *Sqnum* of current packet with the previous packet. If the current value is less than or equal to previous value the packet is identified as replayed packet. As shown in Fig. 10 the GOOSE frame 3 is detected with *Sqnum* value less than the previous value. Hence the packet is identified as replayed packet and is discarded.

Figure 11 shows Wireshark captures of masquerade attack with GOOSE messages. The second GOOSE message shown in green has *Stnum* and *Sqnum* values of 1 and 4, respectively. It contains boolean data *false* which means no trip operation is instructed. The next GOOSE message which is shown by red border is a masquerade message which contains modified information in the packet such as boolean value *true,* a trip instruction. The next message in blue is, again, a legitimate message.

The masquerade GOOSE message is generated by an attacker. However, the attacker is unable to generate the exact digital signature for the GOOSE message, since the attacker has no knowledge of the key and algorithm used for generating digital signature by legitimate publisher and subscriber. The attacker may append any arbitrary digital signature to the masquerade message. Upon receiving the masquerade message, the subscriber as usual generates the digital signature using the legitimated secret keys and compares it with the received digital signature received with the masquerade message. The generated digital signature will not match with the digital signature received in masquerade message. Hence the masquerade packet is detected successfully. Figure 12, shows the output of the Secure GoSV program run at subscriber successfully detecting the masquerade attack.

Finally, a timing performance analysis is run for different key sizes of RSA and different curves of ECDSA. The results are given in Table 1. It can be noted that ECDSA algorithms perform better than the RSA algorithms. Further, it can be noticed that among the different key sizes for RSA algorithm, only 1024 key size is suitable GOOSE algorithms. The other key sizes results in much higher signing and verification times. Protection automation implementations are the most time-critical in IEC 61850 based communication

	Time	Source	Destination	Protocol	Length
1	0.000000000	HewlettP_c5:77:a1	NecPerso_ea:bc:20	GOOSE	201
2	1.000219668	HewlettP_c5:77:a1	NecPerso_ea:bc:20	GOOSE	201
3	2.000479252	HewlettP_c5:77:a1	NecPerso_ea:bc:20	GOOSE	201
4	3.000668435	HewlettP_c5:77:a1	NecPerso_ea:bc:20	GOOSE	201
5	4.000909794	HewlettP_c5:77:a1	NecPerso_ea:bc:20	GOOSE	201
6	5.001044804	HewlettP_c5:77:a1	NecPerso_ea:bc:20	GOOSE	201

```
Frame 2: 201 bytes on wire (1608 bits),
Ethernet II, Src: HewlettP_c5:77:a1 (a0:
GOOSE
  APPID: 0x0001 (1)
  Length: 145
  Reserved 1: 0x0020 (32)
  Reserved 2: 0x2302 (8962)
▾ goosePdu
    gocbRef: GEDeviceF650/LLN0$GO$gcb01
    timeAllowedtoLive: 600
    datSet: GEDeviceF650/LLN0$GOOSE1
    goID: FREA-GoSV-1
    t: Jan  2, 2000 02:46:11.258165836
    stNum: 1
    sqNum: 4
    test: False
    confRev: 1
    ndsCom: False
    numDatSetEntries: 2
  ▾ allData: 8 items
    ▾ Data: boolean (3)
        boolean: False
```

```
Frame 3: 201 bytes on wire (1608 bits),
Ethernet II, Src: HewlettP_c5:77:a1 (a0:
GOOSE
  APPID: 0x0001 (1)
  Length: 145
  Reserved 1: 0x0020 (32)
  Reserved 2: 0x2302 (8962)
▾ goosePdu
    gocbRef: GEDeviceF650/LLN0$GO$gcb01
    timeAllowedtoLive: 600
    datSet: GEDeviceF650/LLN0$GOOSE1
    goID: FREA-GoSV-1
    t: Jan  2, 2000 02:46:11.258165836
    stNum: 2
    sqNum: 0
    test: False
    confRev: 1
    ndsCom: False
    numDatSetEntries: 2
  ▾ allData: 8 items
    ▾ Data: boolean (3)
        boolean: True
```

```
Frame 4: 201 bytes on wire (1608 bits),
Ethernet II, Src: HewlettP_c5:77:a1 (a0:
GOOSE
  APPID: 0x0001 (1)
  Length: 145
  Reserved 1: 0x0020 (32)
  Reserved 2: 0x2302 (8962)
▾ goosePdu
    gocbRef: GEDeviceF650/LLN0$GO$gcb01
    timeAllowedtoLive: 600
    datSet: GEDeviceF650/LLN0$GOOSE1
    goID: FREA-GoSV-1
    t: Jan  2, 2000 02:46:11.258165836
    stNum: 1
    sqNum: 5
    test: False
    confRev: 1
    ndsCom: False
    numDatSetEntries: 2
  ▾ allData: 8 items
    ▾ Data: boolean (3)
        boolean: False
```

FIGURE 11. Masquerade attack on GOOSE packet.

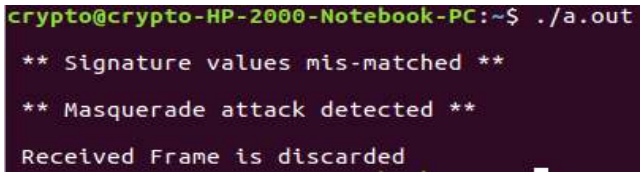

FIGURE 12. Masquerade attack detection by subscriber.

TABLE 1. Computation times for security algorithms.

DS Algorithm	Key Size (bits)/ Curve	Digital Signature Signing time (ms)	Digital Signature verification time (ms)
RSA	1024	0.926	0.293
	2048	3.48	0.79
	3072	8.521	1.396
ECDSA	secp384r1	0.9285	0.8571
	secp224r1	0.75	0.7
	secp521r1	1.125	1.5
	prime384v1	0.75	0.7
	prime256v1	0.675	0.675
	brainpoolP384r1	0.95	0.9
	brainpoolP512r1	1.2	0.975
	brainpoolP384t1	0.85	0.8625
	brainpoolP512t1	1.15	0.9875

systems and a strict 4 ms delay limit is enforced. These results show that DS verification is still not optimum solution for these applications. Further research needs to focus on alternative algorithms such as Hash based Message Authentication Codes (HMAC) etc.

V. CONCLUSION

IEC 61850 is gaining more ground as the de facto communication standard in smartgrids. However, it does not have necessary tools to mitigate or detect cyber-attacks such as masquerade or replay attacks. IEC 62351 has been recently revised to recommend cybersecurity features for IEC 61850 based communication in smartgrids. However, these recommendations are individual cybersecurity techniques and not holistic systems to mitigate a certain type of attack.

This paper develops a novel security solution to address these cybersecurity vulnerabilities. It utilizes a DSA to ensure authenticity and hash algorithms to ensure integrity of GOOSE protocol messages. This is the first such solution that can detect replay attacks and distinguish them with packet switch due to heavy traffic. It is also the first system to mitigate masquerade attacks with hash and DSA while strictly following the framework set forth in IEC 62351.

RSA with different key sizes and ECDSA with different elliptic curves have been implemented as DSA and timing performances have been documented. The full security solution is implemented in the lab to verify its operation, where both masquerade and replay attacks are successfully detected and malicious packets are discarded. The developed solution can detect and report the type of the attack as well. The developed system is fully scalable between all nodes of the smartgrid as long as public keys are known to everyone. This ensures safe and secure communication in IEC 61850 based communication systems.

REFERENCES

[1] *Communication Networks and Systems In Substations: An Overview for Users*, 2nd ed., Standard IEC 61850, 2013.
[2] T. S. Ustun, A. Hadbah, and A. Kalam, "Interoperability and interchangeability considerations in microgrids employing IEC61850 standard," in *Proc. IEEE Int. Conf. Smart Energy Grid Eng. (SEGE)*, Oshawa, ON, Canada, Aug. 2013, pp. 1–5.
[3] A. Hadbah, T. S. Ustun, and A. Kalam, "Using IEDScout software for managing multivendor IEC61850 IEDs in substation automation systems," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Venice, Italy, Nov. 2014, pp. 67–72.
[4] *Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 6: Security for IEC 61850*, Standard IEC/TS 62351-6, 2007.
[5] *Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?* NERC Steering Group, Princeton, NJ, USA, Jul. 2004.
[6] T. S. Ustun, C. Ozansoy, and A. Zayegh, "Simulation of communication infrastructure of a centralized microgrid protection system based on IEC 61850-7-420," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Tainan, Taiwan, Nov. 2012, pp. 492–497.
[7] I. Ali, S. M. S. Hussain, and S. Hussain, "Communication design for energy management automation in microgrid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 2055–2064, May 2018.
[8] M. Strobel, N. Wiedermann, and C. Eckert, "Novel weaknesses in IEC 62351 protected smart grid control systems," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Sydney, NSW, Australia, Nov. 2016, pp. 266–270.
[9] L. E. da Silva and D. V. Coury, "A new methodology for real-time detection of attacks in IEC 61850-based systems," *Electric Power Syst. Res.*, vol. 143, pp. 825–833, Feb. 2017.
[10] M. C. Magro, P. Pinceti, L. Rocca, and G. Rossi, "Safety related functions with IEC 61850 GOOSE messaging," *Int. J. Elect. Power Energy Syst.*, vol. 104, pp. 515–523, Jan. 2019.
[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978. [Online]. Available: https://dl.acm.org/citation.cfm?doid=359340.359342
[12] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.
[13] T. T. Tesfay and J.-Y. Le Boudec, "Experimental comparison of multicast authentication for wide area monitoring systems," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4394–4404, Sep. 2018.
[14] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 3954–3965, Sep. 2018.
[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] 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.
[17] B. Kordy, L. Piètre-Cambacédès, and P. Schweitzer, "DAG-based attack and defense modeling: Don't miss the forest for the attack trees," *Comput. Sci. Rev.*, vols. 13–14, pp. 1–38, Nov. 2014.
[18] S. M. Farooq, S. M. S. Hussain, S. Kiran, and T. S. Ustun, "Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5," *Electronics*, vol. 7, p. 370, Dec. 2018.
[19] 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, 2019.
[20] *SAV Sender and Receiver—INFO TECH*. Accessed: Oct. 19, 2019. [Online]. Available: https://goo.gl/8yLw9A
[21] *LibIEC61850*. Accessed: Oct. 19, 2019. [Online]. Available: http://libiec61850.com/libiec61850/

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

He was an Assistant Professor of electrical engineering with the School of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA. He is currently a Researcher with the Fukushima Renewable Energy Institute, AIST (FREA) and leads Smart Grid Cybersecurity Laboratory. His research interests include power systems protection, communication in power networks, distributed generation, microgrids, electric vehicle integration, and cybersecurity in smartgrids.

Dr. Ustun is a member of IEEE 2004, IEEE 2800 Working Groups, and IEC Renewable Energy Management Working Group Eight. He has edited severalbooks and special issues with international publishing houses. He is a Reviewer in reputable journals and has taken active roles in organizing international conferences and chairing sessions. He has been invited to run specialist courses in Africa, India and China. He delivered talks for Qatar Foundation, World Energy Council, Waterloo Global Science Initiative and European Union Energy Initiative (EUEI). He is an Associate Editor of IEEE Access and a Guest Editor of the IEEE Transactions on Industrial Informatics.

SHAIK MULLAPATHI FAROOQ received the B.Tech. and M.Tech. degrees in computer science engineering from Jawaharlal Nehru Technological University, Hyderabad, India. He is currently pursuing the Ph.D. degree in computer science and engineering from Yogi Vemana University, Kadapa, India. He was a Visiting Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), Japan, from September 2018 to December 2018. His research interests include cryptography, cyber physical systems, cybersecurity in vehicular networks, and power systems.

S. M. SUHAIL HUSSAIN received the Ph.D. degree in electrical engineering from Jamia Millia Islamia (a Central University), New Delhi, India, in 2018.

He is currently an AIST Postdoctoral Researcher with the Fukushima Renewable Energy Institute, AIST (FREA), Koriyama, Japan. His research interests include power system communication, cybersecurity in power systems, substation automation systems, IEC 61850 standards, electric vehicle integration, and smart grid.

Dr. Hussain 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 2014–15. He is a Guest Editor of the IEEE Transactions on Industrial Informatics.