IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 2, 2020, accepted January 28, 2020, date of publication February 3, 2020, date of current version February 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2971011

Implementing Secure Routable GOOSE and SV Messages Based on IEC 61850-90-5

TAHA SELIM USTUN[1], (Member, IEEE), SHAIK MULLAPATHI FAROOQ[2,3], (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, Proddatur 516360, India
[3]Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College (Autonomous), Tirupati 517102, India

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

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

ABSTRACT Next generation power systems are active networks that handle two-way power flow. They are equipped with extensive communication capabilities to perform dynamic monitoring, protection and control operations. Synchrophasors provide a pseudo real-time representation of grid's current state. Phasor Measurement Units (PMU) placed in different parts of the grid periodically collect synchrophasor data. Then, they send it to a Phasor Data Concentrator (PDCs) through Wide Area Monitoring Systems (WAMS). The entire system formed as PMU Communication Network (PMU-CN) is based on two available frameworks: IEEE C37.118.2 and IEC 61850-90-5. As New York Blackout of 2003 showed that accurate and timely delivery of phasor measurements is vital for secure grid operation. Attacks on PMU-CN may lead to several consequences in the grid and cause physical damage. IEEE C37.118.2 does not specify any security mechanism to mitigate security attacks. To address this gap, security mechanism specified in IEC 61850-90-5 have been implemented using OpenSSL library. A novel toolbox called R-GoSV has been developed to construct PMU messages with cybersecurity mechanisms. Thanks to this tool, custom messages have been transmitted in the network to investigate their effectiveness. Finally, the performance evaluation of the specified security algorithms in terms of computational time sis carried out.

INDEX TERMS Cyber security in wide area monitoring system (WAMS), routable-generic object-oriented substation event (R-GOOSE), routable-sample values (R-SV), IEC 61850-90-5, OpenSSL library.

I. INTRODUCTION

Integration of Distributed Energy Resources (DER), electric vehicles (EVs) and storage devices into traditional electrical power systems makes it more dynamic and increases its operational complexity. Smart Grid (SG) concept is developed to manage this situation through Wide Area Monitoring, Protection and Control (WAMPAC) applications [1]. WAMPAC applications make use of synchrophasor technology which is based on Phasor Measurement Units (PMUs), Phasor Data Concentrators (PDCs) and Wide Area Measurement Systems (WAMS). Synchrophasor technology plays a key role in monitoring, control and protection of electric power systems [2] and any failure in this field may lead to severe consequences such as blackouts [3].

PMUs measure synchrophasors which includes voltage and current values (amplitude and angle), frequency, Rate-Of-Change-Of-Frequency (ROCOF) and send them to PDCs through a communication framework. There are two popular communication frameworks for PMU communication; IEEE C37.118 [4] and IEC 61850-90-5 [5]. IEEE C37.118 framework further divided into IEEE C37.118.1 and IEEE C37.118.2. The first part deals with measurement details of synchrophasors under dynamic conditions while the second part focuses on transmission requirements of those synchrophasors. IEEE C37.118.2 is widely adopted in commercial PMUs and PDCs. It does not put restrictions on the choice of communication medium and transport protocol to be used in synchrophasor data transmission. IEEE C37.118.2 standard also does not specify security requirements to protect data communication over an insecure IP network.

Due to involvement of critical infrastructure in synchrophasor based communication, and transmission of data over insecure public network, a strong security mechanism is needed to mitigate cyber-attacks. Many attacks, e.g.

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

reconnaissance, Man-In-The-Middle (MITM), replay and Denial of Service (DoS), demonstrated in literature were proven to compromised synchrophasor communication based on IEEE C37.118.2 framework [6]–[9]. Authors in [6] analyses the impact of Black Energy malware which involved in several major cyber-attacks including coordinated DDoS attack on Georgia's finance, military and government agencies, fraudulent bank transactions and the Ukraine power grid.

Different security vulnerabilities of IEEE C37.118.2 compliant PMU communication is documented in [7]. Node authentication vulnerabilities have been documented and a certificate-based solution is developed in [8]. The impact of data integrity attacks on the system and how wrong decisions such as triggering protection elements based on falsified data causes a major loss have been documented in [9]. The vulnerability of IEEE C37.118.2 compliant PMU against DoS attack has been shown in [10]. Tests have been performed by flooding legitimate and forged packets to PMUs and checking their unresponsiveness. In PMU networks high time synchronization is achieved through GPS, but GPS spoofing attack may hamper it [11]. GPS spoofing may cause major damage to the system such as unintentional tripping of power generators [12]. As IEEE C37.118.2 framework does not specify transport layer protocol to be used for transmission of synchrophasors, it has security impacts on TCP and UDP protocols in transport layer communication among synchrophasors and phasor data concentrators [13]. False data injection attacks and DoS attacks on TCP and UDP transport layer protocols can be performed in Wide Area Monitoring and Control (WAMC) system [14], [15].

To address the cybersecurity issues in synchrophasor communication, a new framework for synchrophasor data communication based on IEC 61850 standard was developed. IEC 61850 is a default standard for substation automation system in a smart grid. It offers time critical protocols such as Generic Object-Oriented Substation Event (GOOSE) and Sample Value (SV) and information modelling based on logical nodes to achieve interoperability among Intelligent Electronic Devices (IEDs) developed by different vendors within a substation. To achieve compatibility between synchrophasor data transfer based on IEEE C37.118.2 with IEC 61850 substation automation standard, IEC 61850-90-5 was introduced [5]. It has additional security features and specifies Hash based Message Authentication Code (HMAC) for message authentication. In [16] authors developed a gateway and protocol converter for exchanging IEEE C37.118.2 and IEC 61850-90-5 synchrophasor data. However, in [16] cybersecurity features were not considered. In [17], in addition to IEC 61850-90-5 security features a Group Domain of Interpretation (GDOI) mechanism based on key distribution technique is proposed to secure IEC 61850-90-5 synchrophasor data communication. The main idea behind the theme is to secure the synchrophasor communication by refreshing a secret key periodically.

In this paper, a new toolbox called R-GoSV has been developed using openSSL library that generates secure R-GOOSE and R-SV messages which can be transmitted in insecure wide area public network [18]. To ensure the security of R-GOOSE and R-SV, the security mechanisms recommended in IEC 61850-90-5 standard are implemented in the session layer. The developed R-GoSV toolbox can be used to generate secure R-GOOSE and R-SV messages which can be further utilized for performing different tests and evaluating different security mechanisms.

Rest of the paper is organized as follows: section 2 describes about synchrophasor communication. Section 3 outlines the popular two communication frameworks: IEEE C37.118.2 and IEC 61850-90-5. Section 4 gives implementation details of the security mechanism specified in IEC 61850-90-5. It also reports Wireshark captures of the generated secure R-GOOSE and R-SV packets. Finally, section 5 concludes the paper.

II. SYNCHROPHASOR COMMUNICATION

Smart grid requires Information and Communication Technologies (ICT) to perform monitoring, control and protection operations effectively. Synchrophasor technology play crucial role in this regard. It includes IEDs such as PMUs, PDCs and a platform WAMS to perform the task. Synchrophasors are measurement values of electrical quantities captured at different parts of the grid. They are complex representation of sinusoidal voltage and current having magnitude and phase angle with timestamp synchronized with common precise time source [19]. Hence, PMUs are connected to Global Positioning Systems (GPS) clocks or GPS antenna. GPS time stamp provides higher accuracy and universal time. Geographically located PMUs periodically measures from different parts of the grid and sends these measurements to PDCs. The data fed to the PDCs can be used to view near real time snapshot of a grid and perform post incident analysis in case of blackouts [20]. Figure 1 describes about WAMS structure where PMUs collects phasor measurement and send to substation PDC, substation PDC forwards data to regional PDCs. Regional PDCs gather data from different PMUs, combines data according to timestamps Further, then forwards to central controller PDC via Wide Area Network (WAN). Generally, PDCs have local storage and verification facility along with application functions.

PMU operates in two modes: command and spontaneous. In command mode, PMU communication with local or regional PDC is bi-directional and unicast in nature where PDC can send command signals to PMU to control its operation. Whereas in spontaneous mode, PMU communication with PDC is unidirectional and multicast in nature. PDC can receive synchrophasor from multiple PMUs or from regional PDCs to control center PDC. It accumulates data and send as one output stream. As shown in the Figure 1, synchrophasor data is transmitted over an insecure public WAN. The accumulated data at control center is used in visualization, monitoring, control and protection operations. IEEE C37.118.2 communication framework is used to transmit data in WAN. As IEEE C37.118.2 doesn't specify any

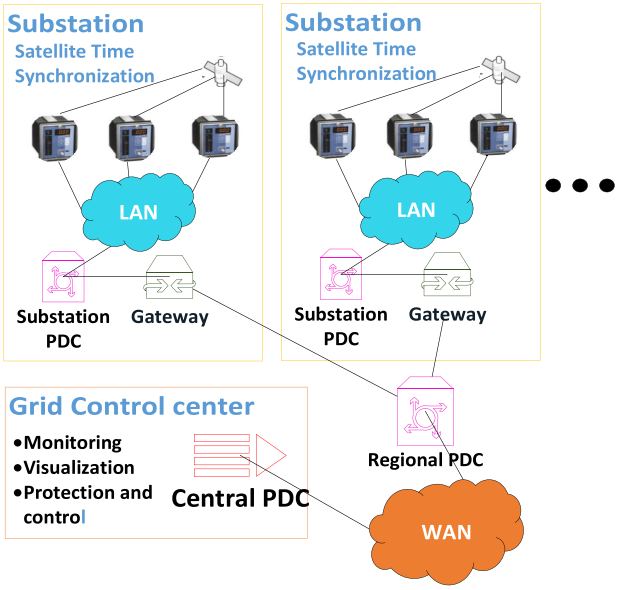

FIGURE 1. WAMS Architecture.

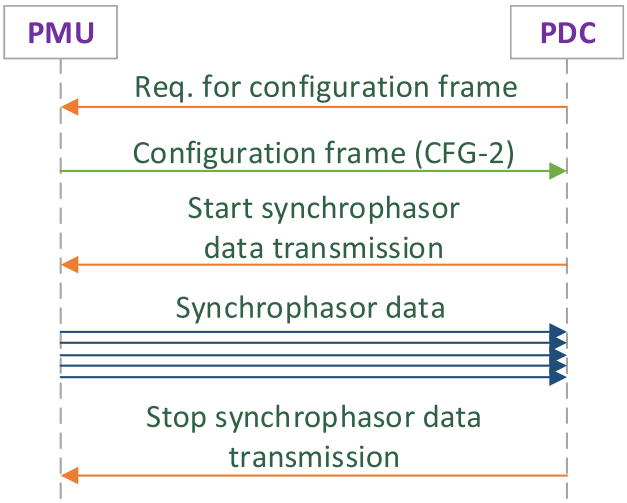

FIGURE 2. PMU communication with PDC based on IEEE C37.118.2 framework.

security features, IEC 61850-90-5 based communication is considered in this paper.

III. PMU COMMUNICATION BASED ON IEC 61850-90-5

A. IEEE C37.118.2 COMMUNICATION FRAMEWORK

IEEE C37.118.2 has four types of messages. They are data, header, configuration and command messages. Data message consists of synchrophasor data measured by PMU. Data, header and configuration messages are sent by source device PMU/PDC whereas command message is received by the PMU/PDC. Header message consists of information in human readable descriptive format given by user. Configuration message consists of information which is used to interpret information in data message. They are CFG-1, CFG-2 and CFG-3. CFG-1 describes about the reporting capability of PMU. CFG-2 explains about synchrophasor data transmission which are currently being transmitted. CFG-3 gives enhanced information about the measurements being done by PMU. Command messages are used to control the operation of PMU and transmission of data. In IEEE C37.118.2 communication as shown in the Figure 2, PDC send a request (command message) to PMU for the type of configuration message. PMU responds with CFG-2. PDC send command message to initiate synchrophasor data transfer. PMU send the measured values using data message continuously until PDC send another command message to stop sending the measured data. PMU recognizes the type of command messages based on CMD field.

B. IEC 61850-90-5 COMMUNICATION FRAMEWORK

Unlike IEEE C37.118.2 communication framework, IEC 61850-90-5 is based on IEC 61850 substation automation protocol which offers interoperability among different vendor's Intelligent Electronic Devices (IEDs) through modelling of devices using logical nodes, it also offers different protocols such as Sample Value (SV), Generic Object-Oriented Substation Event (GOOSE) and Manufacturing Measurement Specification (MMS) for the smooth operation of substation automation system. This standard also extended from substation automation domain to power utility automation domain such as Distributed Energy Resources (DERs), Demand-Response, wide area transmission of synchrophasor data according to IEEE C37.118.

Besides communication services, IEC 61850 define data modeling of IEDs and its operations in the communication. Data modeling provides standardized syntax and semantics of data exchanged between different devices in the communication. Data modeling initiated with physical device such as IED. An IED may consists of one or more logical devices. Each function of IED can be modelled with Logical Device (LD). Each LD may perform one or more substation operations which can be modelled with Logical Nodes (LNs).

Each LN contains data objects whose type and structure is defined by Common Data Class (CDC) standardized in IEC 61850-7-2. Each CDC contains one or more data attributes that can be categorized by functional constraints. For example, PMU is LD within an IED which consists of related LNs such as MMXU, LPHD etc. along with their data objects for PMU. Table 1 describes about MMXU LN which mainly deals with measurement data. IEEE C37.118.1 specifies that PMU must measure and send values of voltage, current, frequency and rate of change of frequency (ROCOF). Accordingly, MMXU LN contains data objects such as PhV, A, Hz, HZRte which are used to hold information about voltage, current, frequency and rate of change of frequency (ROCOF) respectively. Besides phasor data, information about the status of PMU is transmitted using PhyHealth data element of LPHD logical node.

In PMU communication based on IEC 61850-90-5 shown in the Figure 3, PDC send a MMS request to PMU to initiate

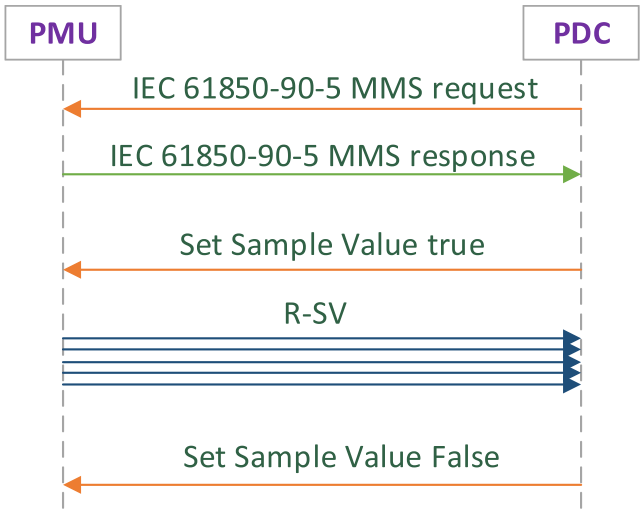

FIGURE 3. PMU communication with PDC based on IEC 61850-90-5 framework.

TABLE 1. Description of MMXU and LPHD logical nodes.

MMXU Class			
Attribute name	Attribute type	Explanation	M/O
PhV	WYE (Composite Common Data Class)	Phase to ground voltages	M
A	WYE (Composite Common Data Class)	Phase currents	M
Hz	MV (Simple command Data Class)	Frequency	M
HZRte	MV (Simple command Data Class)	Rate of change of frequency	M
LPHD Class			
PhyHealth	INS (Simple command Data Class)	Status of PMU	M

data transfer. PMU reply with MMS response message to PDC. Further, PMU sends measured sample values after the sample value control block is set to enable. The SV protocol defined in IEC 61850-9-2 [21] is used to transmit measurement data inside a substation local area network whereas GOOSE protocol is defined in IEC 61850-8-1 [22] used to transmit time critical event-based data. In order to transfer the GOOSE and SV over WANs. The IEC 61850-90-5 standard specifies two solutions for transmitting GOOSE and SV over WAN. First, the GOOSE and SV protocols can be tunneled over high speed communication networks such as SDH or SONNET in WANs. Second, GOOSE and SV messages are extended as R-GOOSE (Routable-GOOSE) and R-SV (Routable-SV) by adding network and transport layers so that it can communicated over WANs. Among both the solutions, tunneling is less advantageous because for establishing tunnel dedicated gateways must be employed and the message exchanges are strictly point to point in WAN. Whereas, R-GOOSE and R-SV messages can be multicast in WANs. Figure 4 illustrates the protocol stack with respect to Open Systems Interconnect (OSI) referent model for PMU communication based on IEC 61850 in local area network

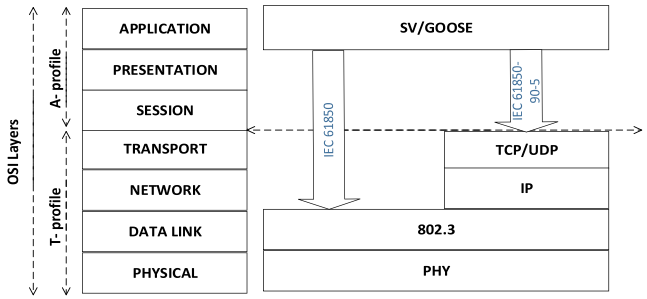

FIGURE 4. Protocol stack for PMU communication via wide area network and local area network.

and IEC 61850-90-5 in WAN. Due to the cyclic nature of SV and GOOSE protocols at transport level, UDP with multicasting protocol is suitable for implementation. Hence, we considered UDP in transport layer for our implementation. The scope of this work is to develop a software library that implements security mechanisms based on IEC 61850-90-5 specifications in R-SV and R-GOOSE to protect data from security attacks.

IV. IMPLEMENTATION OF R-GOSV TOOLBOX

Security is utmost important in PMU communication as PMU traffic travels through wide area communication network which is a public network. An eavesdropper may modify packets causing major loss to grid network [23]. IEC 61850-90-5 standard specifies message authentication and integrity as essential requirements whereas confidentiality as an optional requirement for PMU communication over WANs. To achieve message integrity and authentication, IEC 61850-90-5 standard specifies different Message Authentication Code (MAC) algorithms such as keyed Hash Message Authentication Code (HMAC), with SHA256 as inherent secure hash algorithm, and Advanced Encryption Standard – Galois Message Authentication Code (AES-GMAC) to generate hash values. Even though confidentiality is optional, the standard specifies AES-128 and AES-256 algorithms encryption for IEC 61850-90-5 R-GOOSE and R-SV messages. Hence, R-GoSV toolbox developed in this paper implements the recommended security mechanisms. It implements HMAC-SHA256 digital signature to ensure message authentication and integrity and AES-128 symmetric encryption algorithm to achieve confidentiality.

Application layer specifications in IEC 61850-90-5 are GOOSE and SV protocols, whereas session layer consists of security related header fields as shown in Figure 5. The packet generated at session layer starts with Session Identifier (SI) followed by length field which consists of the length of all the parameter fields of the session header excluding user information field. Further, each parameter field consists of Parameter Identifier (PI), Length Identifier (LI) followed by the Parameter Value (PV).

IP and Transport layer header such as UDP header of IEC 61850-90-5 R-GOOSE/R-SV packet is shown in the

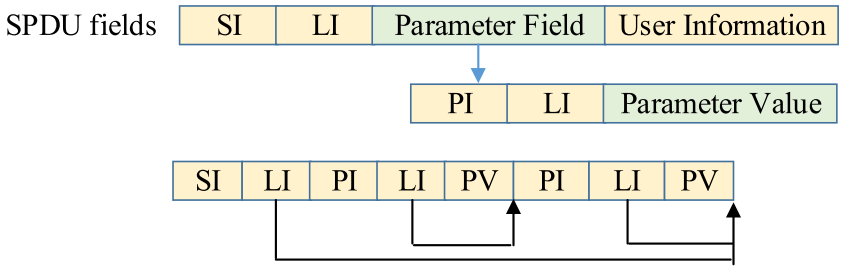

FIGURE 5. Session protocol structure.

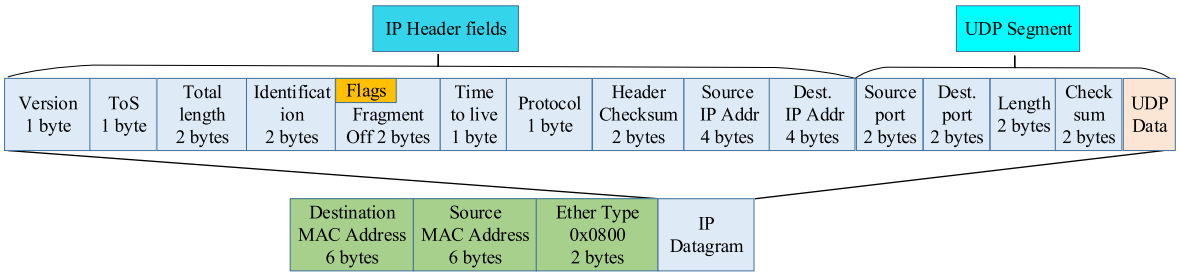

FIGURE 6. IEC 61850-90-5 R-GOOSE/R-SV Transport layer headers.

Figure 6. IP header fields consists of version, Type of Service (ToS), Total length, Identification, Fragment offset, Time to live, protocol, header checksum, source and destination IP addresses. Version field is of 1-byte that represents Internet protocol version either 4 or 6. In this implementation we consider IPv4. Type of Service (ToS) field is 1-byte size and represents IP precedence and differentiated code point. Total length field is 2 bytes size which consists of the total length of IP header fields plus UDP Segment length which includes UDP header and data. Identification field is 2 bytes size which represents unique identification of each packet to be transmitted in the network. Flags and Fragment Offset field is 2 bytes size deals with the issues related to packet fragmentation and defragmentation.

Time to live field is 1-byte size represents the lifetime of packet in the network. Protocol field is 2 bytes size represents the protocol used in the data field of IP packet. In our implementation we have considered it User Datagram Protocol (UDP) as transport layer protocol. Header Checksum field is 2 bytes to handle errors in the IP header fields. Source and Destination IP addresses are 4 bytes size each and represents the address of source and destination devices in the network where to where the packet should be traveled. UDP segment consists of Source and Destination fields, Length, Checksum fields followed by UDP data fields. Source and Destination port fields are 2 bytes each representing port numbers of source and destination devices on the network in which UDP connection is established. Length field is 2 bytes size consists of total length of UDP segment which includes UDP header and data. Checksum field is 2 bytes size for error checking of UDP header.

UDP data fields are further extended with session layer related fields. Each data packet generated at session layer is treated as Session Protocol Data Unit (SPDU). According to session protocol structure as shown in the Fig. 5, SPDU starts with Session Identifier (SI), Length Identifier (LI) of SI, Common session header as PI with value 0×80, Length Identifier (LI) of Common header and Parameter Value (PV). According to IEC 61850-90-5, SI has four possible values: $0\times A0$ (Tunneled GOOSE and Sampled Value packets), $0\times A1$ (Non-Tunneled GOOSE Application Protocol Data Units (APDUs)), $0\times A2$ (Non-Tunneled SV APDUs), $0\times A3$ (Non-tunneled management APDUs). Further, PV consists of SPDU Length, SPDU Number, Version Number, Time of Current Key, Time of Next Key, Security Algorithm and Key ID. As shown in the Figure 7, SPDU Length is 4 bytes size and consists of total length starting from SPDU Number to HMAC field. SPDU Number is 4 bytes size which represents unique identification of session packet and to detect duplication in packet at the destination device.

Version Number is 2 bytes that represent session protocol version number, which is 1 in this case. In IEC 61850-90-5, security information is provided by KDC (Key Distribution Center) protocol. Security information such as Time of Current Key, Time of Next Key are 4- and 2-bytes sizes respectively. Time of Current Key is the time the present key being used by the communicating devices whereas Time of Next key is the time period between old and s new keys being used in the encryption and authentication. Security Algorithm field is 2 bytes size and represents the type of encryption algorithm such as AES256-GCM and the type of Hashed Message Authentication Code (HMAC) algorithm

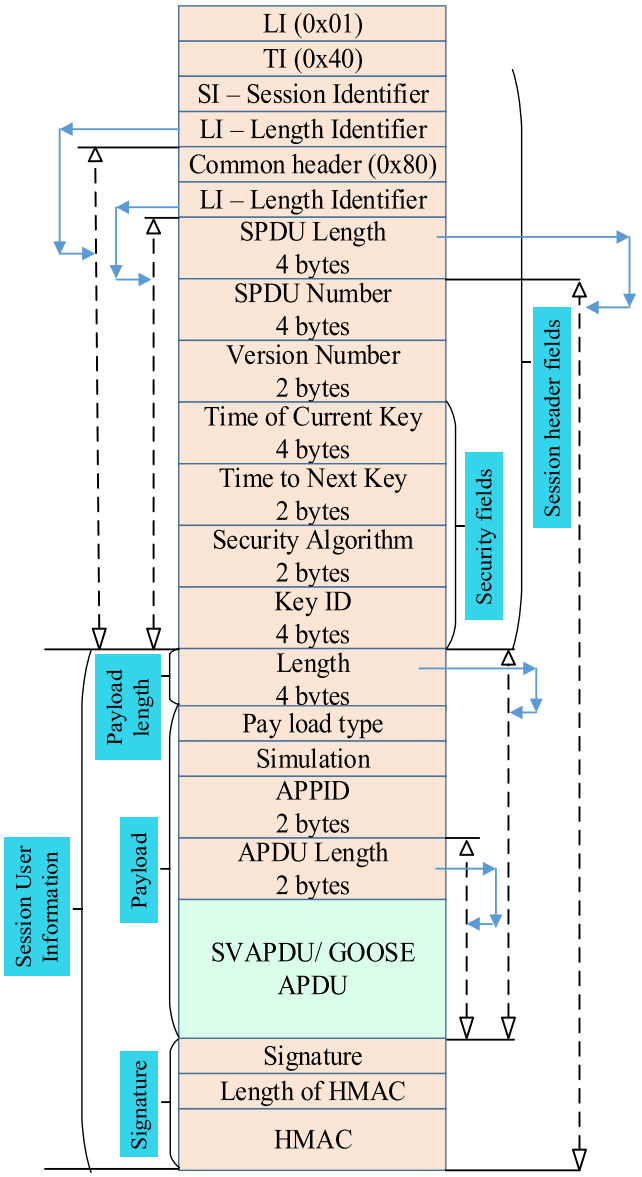

FIGURE 7. Session layer fields of IEC 61850-90-5.

such as HMAC-SHA256 for message authentication. The most significant byte is used for representing encryption algorithm whereas least significant byte is used for message authentication algorithm.

Key ID field is 4 bytes length that represents unique identification of key generated by KDC. After this session header information, session user information fields consist of payload length, payload and signature fields are encountered. Payload length is 4 bytes length which covers session user information except signature fields as shown in the Fig. 7. The IEC 61850-90-5 R-G OOSE or R-SV payload fields consists of payload type, simulation, APPID, APDU length and GOOSE or SV protocols defined by IEC 61850-8-1 and IEC 61850-9-2 respectively. IEC 61850-90-5 specifies payload types such as 0x81 (Non-Tunneled GOOSE APDU), 0x82 (Non-Tunneled SV PDU), 0x83 (Tunneled GOOSE and SV packets) and ox84 (Non-Tunneled management APDUs). Simulation is a Boolean type value used for testing the IEC 61850-90-5 R-GOOSE or R-SV packet. APPID (Application Identification) is a 2 bytes length that distinguishes between R-GOOSE and R-SV packets. APDU length contains the length of GOOSE or SV APDU. APDU length is 2 bytes. Payload field are followed by signature fields. Signature fields start with one-byte tag of 0x85, signature length which is of one byte and signature itself (HMAC).

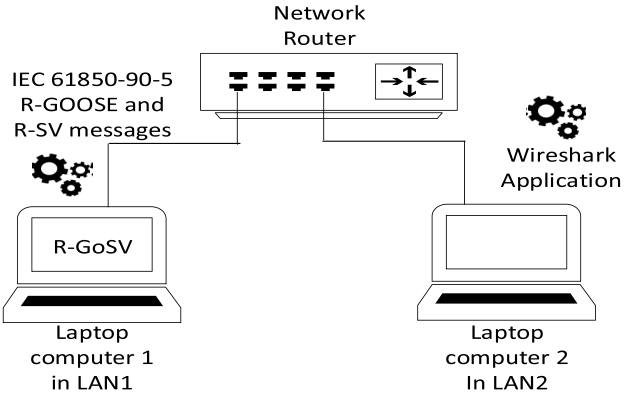

FIGURE 8. Testbed to generate secure IEC 61850-90-5 R-GOOSE and R-SV messages.

A. IMPLEMENTATION RESULTS

Figure 8 shows a testbed where computers are connected to a router via two different LANs. Laptop computer1 in LAN1 runs R-GoSV toolbox and sends into the network and laptop computer 2 is LAN2 runs Wireshark sniffer tool that captures generated packets.

R-GoSV software tool generates IEC 61850-90-5 R-GOOSE and R-SV packets with full stack of IP, UDP, Session layer followed by GOOSE and Sample Value Data.

Figures 9 and 10 shows the R-GOOSE and R-SV packets captures. Wireshark shows all the require fields staring from ethernet, IP, UDP and Session headers. Security Algorithms field consists of zero values indicating that there is no encryption and no digital signature algorithms were implemented to either R-GOOSE or R-SV packets. Hence the length of HMAC field also contains zero value.

As shown in the Figures 6 and 7, secure R-GoSV software library first construct R-GOOSE and R-SV packets by adding headers of ethernet, IP, UDP and Session layers followed by constructing GOOSE or SV frame formats according to IEC 61850-8-1 and IEC 61850-9-2 respectively along with implementation of encryption and authentication security algorithms at session layer. Authors have implemented AES256-GCM algorithm for encrypting R-GOOSE or R-SV APDU fields and HMAC-SHA-256, with 256-, 128- and 80-bit truncations, AES-GMAC-128 and AES-GMAC-64 for generating digital signature to achieve message integrity and authentication. Table 2 lists the size of R-GOOSE and

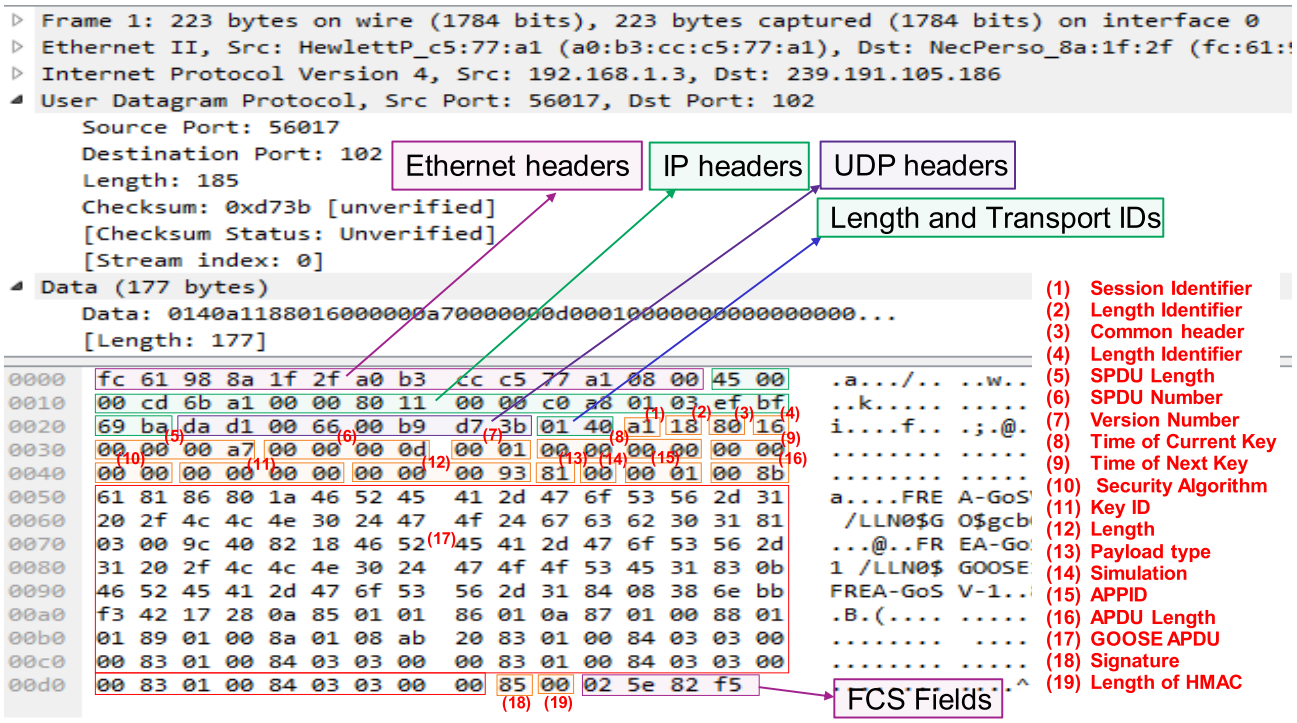

FIGURE 9. Wireshark capture of R-GOOSE without security.

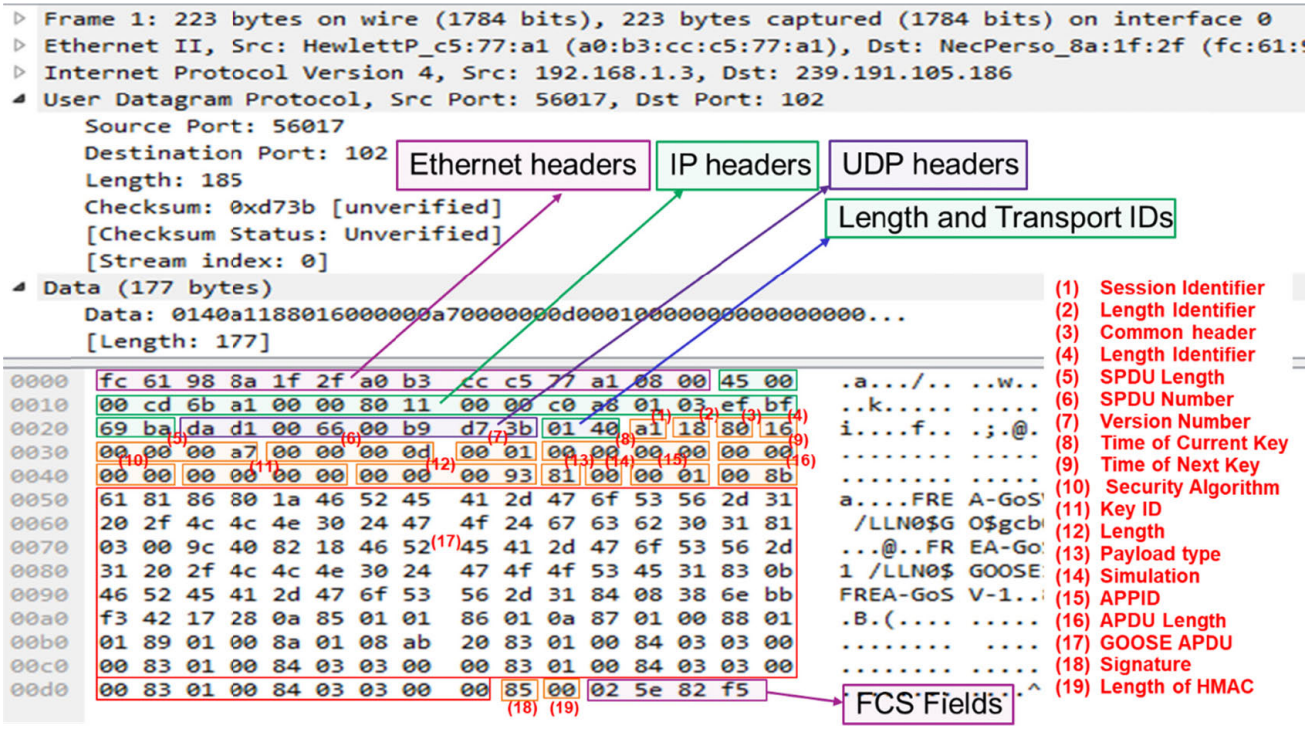

FIGURE 10. Wireshark capture of R-SV without security.

R-SV messages after appending the authentication signatures for different algorithms. Among the different algorithms, HMAC-SHA-256 results in largest size with signature length 32 bytes. Whereas, the AES-GMAC-64 is comparatively small with 8 bytes signature length. Table 2 also shows the computational times required for generating the signa-

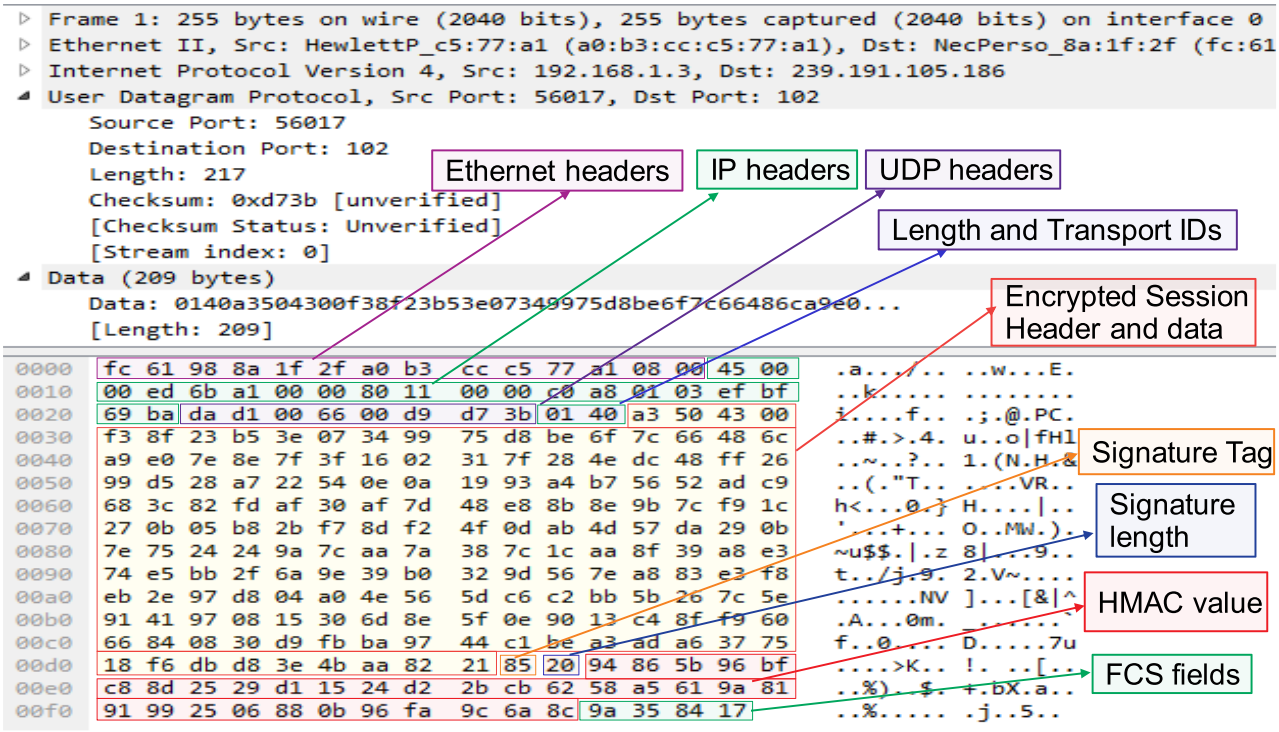

FIGURE 11. Wireshark capture of R-GOOSE with IEC 61850-90-5 security specifications.

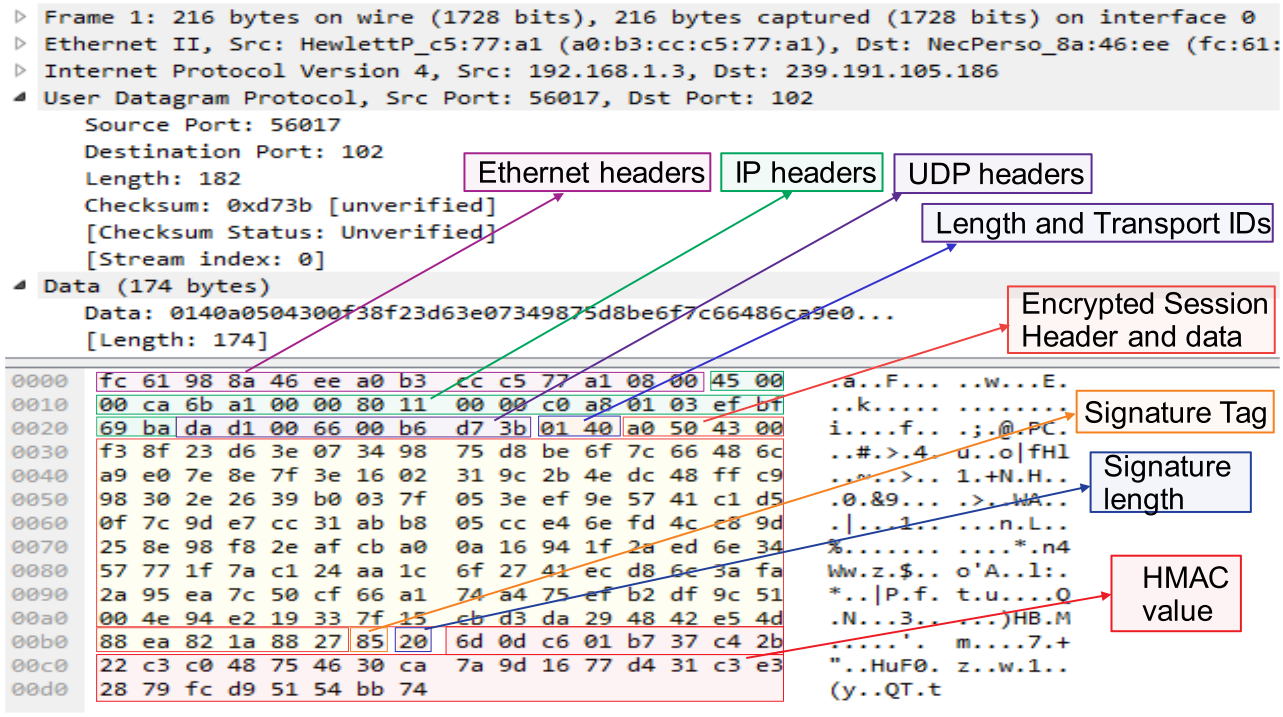

FIGURE 12. Wireshark capture of R-SV with IEC 61850-90-5 security specifications.

tures for different algorithms. The R-GoSV programs were executed on a system with Intel Celeron(R) processor with 4 GB RAM. The latest commercial IEDs supporting IEC 61850-90-5 PMU protocols have much higher computational power than the relatively old system selected in this paper [24]. Hence, it can be safely assumed that if the computational

TABLE 2. Communication delays and message size of R-GOOSE and R-SV for different security algorithms.

Protocol or security algorithm	R-GOOSE		R-SV	
	Signature length (bytes)	Computational time (ms)	Signature length (bytes)	Computational time (ms)
No security	--	--	--	--
HMAC-SHA256-256	32	0.008	32	0.007
HMAC-SHA256-128	16	0.008	16	0.007
HMAC-SHA256-80	10	0.008	10	0.007
AES-GMAC-64	8	0.0045	8	0.004
AES-GMAC-128	16	0.005	16	0.0045

TABLE 3. Computational time for encryption/decryption of R-GOOSE and R-SV.

Security Algorithms	R-SV		R-GOOSE	
	Encryption (ms)	Decryption (ms)	Encryption (ms)	Decryption (ms)
AES-GCM 256	0.210	0.178	0.286	0.221

timing results on this system are acceptable then it must be acceptable for current IEDs. From Table 2 it is quite evident that the computational times are very negligible in comparison to allowed end-to-end (ETE) delays for applications based on PMU data (which is of the order of 50 ms to 500 ms) [5].

Table 3 gives the results for computational time for encryption of R-GOOSE and R-SV using AES-GCM256 algorithm. From the results it is clear that additional encryption of R-GOOSE/R-SV introduces around 0.5 ms of computational delays, which is comparatively negligible to the allowed ETE delays for most of applications using PMU data. Hence, it can be concluded that for R-GOOSE and R-SV encryption can be safely employed without compromising the performance.

Figures 11 and 12 shows Wireshark captures of R-GOOSE and R-SV encrypted with AES-GCM256 and signature generated with HMAC-SHA-256 algorithms respectively. The developed R-GoSV toolbox can be further used to investigate the effect of security attacks on IEC 61850-90-5 R-GOOSE and R-SV packets. Furthermore, it can be extended for implementing different security algorithms and different operating environments for IEC 61850 messages such as software defined network (SDN) [25], eXtensible Messaging and Presence Protocol (XMPP) [26], etc.

V. CONCLUSION

Mitigating cybersecurity vulnerabilities is an essential requirement in PMU communication networks. IEEE C37.118.2 standard specifies the syntax and semantics of synchrophasor data communication, but it does not specify any security mechanism to protect PMU data in the network. IEC 61850-90-5 standard addresses this gap with specifying encryption and authentication as an essential security requirement. Furthermore, it specifies AES-GCM algorithm for encryption of data to protect from accessing by unauthorized party and HMAC algorithm to achieve message authentication. In this paper, a new toolbox has been developed by implementing an openSSL library. It constructs packet format based on IEC 61850-90-5 standard to transmit GOOSE and SV based on IEC 61850-8-1 and IEC 61850-9-2, respectively. Additionally, it encrypts data using AES256-GCM algorithm and HMAC-SHA256 for message authentication. The computational delays experienced for different security algorithms is analyzed and it is found the computational delays for all the algorithms is within the acceptable limits. Real network message exchanges are captured in Wireshark sniffer tool.

Implementation of encryption and message authentication algorithms can mitigate data integrity attack so that it protects the grid from causing huge loss. Furthermore, utilizing the developed R-GoSV toolbox, future research can be focused to implement security mechanisms to mitigating several types of attacks such as Denial of Service attacks, Distributed Denial of Service (DDoS) attacks etc.

REFERENCES

[1] M. A. Aftab, S. Roostaee, S. Suhail Hussain, I. Ali, M. S. Thomas, and S. Mehfuz, "Performance evaluation of IEC 61850 GOOSE-based inter-substation communication for accelerated distance protection scheme," *IET Gener., Transmiss. Distrib.*, vol. 12, no. 18, pp. 4089–4098, Oct. 2018.

[2] I. Ali, S. M. S. Hussain, and A. Aftab, "Communication modeling of phasor measurement unit based on IEC 61850-90-5," in *Proc. Annu. IEEE India Conf. (INDICON)*, New Delhi, India, Dec. 2015, pp. 1–6.

[3] *NERC-DOE, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, US-Canada Power System Outage Task Force*. Accessed: Apr. 5, 2004. [Online]. Available: http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf

[4] K. E. Martin, "Synchrophasor standards development—IEEE C37.118 & IEC 61850," in *Proc. 44th Hawaii Int. Conf. Syst. Sci.*, Jan. 2011, pp. 1–8, doi: 10.1109/HICSS.2011.393.

[5] *Communication Networks and Systems for Power Utility Automation, Part 90-5: Use of IEC 61850 to Transmit Synchrophasor Information According to IEEE C37.118*, IEC Standard IEC TR 61850-90-5:2012, 2012.

[6] R. Khan, K. McLaughlin, P. Maynard, D. Laverty, and S. Sezer, "Threat analysis of black energy malware of synchrophasor based real-time control and monitoring in smart grid," in *Proc. 4th Int. Symp. ICS SCADA Cyber Secur. Res. (ICS-CSR)*, 2016, pp. 1–11.

[7] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "IEEE C37.118-2 synchrophasor communication framework–overview, cyber vulnerabilities analysis and performance evaluation," in *Proc. ICISSP*, 2016, pp. 159–170.

[8] S. M. Farooq, S. M. Hussain, S. Kiran, and T. S. Ustun, "Certificate based authentication mechanism for PMU communication networks based on IEC 61850-90-5," *Electronics*, vol. 7, no. 12, p. 370, 2018.

[9] S. Paudel, P. Smith, and T. Zseby, "Data integrity attacks in smart grid wide area monitoring," in *Proc. 4th Int. Symp. ICS SCADA Cyber Secur. Res. (ICS-CSR)*, Aug. 2016, pp. 74–83.

[10] T. Morris, S. Pan, J. Lewis, J. Moorhead, N. Younan, R. King, M. Freund, and V. Madani, "Cyber security risk testing of substation phasor measurement units and phasor data concentrators," in *Proc. 7th Annu. Workshop Cyber Secur. Inf. Intell. Res. (CSIIRW)*, 2011, p. 1.

[11] Shepard, D., Humphreys, T., and Fansler, A. (2012). "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Crit. Infrastruct. Protection*, vol. 5, nos. 3–4, pp. 146–153, 2012.

[12] D.-Y. Yu, A. Ranganathan, T. Locher, S. Capkun, and D. Basin, "Short paper: Detection of GPS spoofing attacks in power grids," in *Proc. Int. Conf. Secur. Privacy Wireless Mobile Netw.*, 2014, pp. 99–104.

[13] Y. Wang, T. T. Gamage, and C. H. Hauser, "Security implications of transport layer protocols in power grid synchrophasor data communication," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 807–816, Mar. 2016.

[14] K. Demir, F. Nayyer, and N. Suri, "MPTCP-H: A DDoS attack resilient transport protocol to secure wide area measurement systems," *Int. J. Crit. Infrastruct. Protection*, vol. 25, pp. 84–101, Jun. 2019.

[15] s. M. Farooq, S. Nabirasool, S. Kiran, S. S. Hussain, and T. S. Ustun, "MPTCP based mitigation of denial of service (DoS) attack in PMU communication networks," in *Proc. IEEE Int. Conf. Power Electron., Drives Energy Syst. (PEDES)*, Chennai, India, Dec. 2018, pp. 1–5.

[16] S. R. Firouzi, L. Vanfretti, A. Ruiz-Alvarez, H. Hooshyar, and F. Mahmood, "Interpreting and implementing IEC 61850-90-5 routed-sampled value and routed-GOOSE protocols for IEEE C37.118.2 compliant wide-area synchrophasor data transfer," *Electr. Power Syst. Res.*, vol. 144, pp. 255–267, Mar. 2017.

[17] R. Khan, K. Mclaughlin, D. Laverty, and S. Sezer, "Design and implementation of security gateway for synchrophasor based real-time control and monitoring in smart Grid," *IEEE Access*, vol. 5, pp. 11626–11644, 2017.

[18] *R-GoSV*. Accessed: Feb. 2, 2020. [Online]. Available: https://github.com/61850security/R-GoSV

[19] M. S. Almas, L. Vanfretti, R. S. Singh, and G. M. Jonsdottir, "Vulnerability of synchrophasor-based WAMPAC applications' to time synchronization spoofing," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4601–4612, Sep. 2018.

[20] R. Pourramezan, Y. Seyedi, H. Karimi, G. Zhu, and M. Mont-Briant, "Design of an advanced phasor data concentrator for monitoring of distributed energy resources in smart microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3027–3036, Dec. 2017.

[21] *Communication Networks and Systems for Power Utility Automation—Part 9-2: Specific Communication Service Mapping (SCSM)—Sampled Values Over ISO/IEC 8802-3*, Standard IEC 61850-9-2:2011, 2011.

[22] *IEC Standard for Communications Networks and Systems for Power Utility Automation—Part 8-1: Specific Communication Service Mapping (SCSM)—Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*, Standard IEC 61850-8-1-2011, 2011.

[23] S. M. Farooq, S. M. Hussain, S. Kiran, and T. S. Ustun, "Certificate based security mechanisms in vehicular ad-hoc networks based on IEC 61850 and IEEE WAVE standards," *Electronics*, vol. 8, no. 1, p. 96, 2016.

[24] *Data Sheet-SEL 3555 Real Time Automation Controller (RTAC)*. Accessed: Nov. 21, 2019. [Online]. Available: https://goo.gl/jjnfnV

[25] G. Li, J. Wu, L. Guo, J. Li, and H. Wang, "SDN based dynamic and autonomous bandwidth allocation as ACSI services of IEC61850 communications in smart grid," in *Proc. IEEE Smart Energy Grid Eng. (SEGE)*, Oshawa, ON, Canada, Aug. 2016, pp. 342–346.

[26] S. M. S. Hussain, M. A. Aftab, and I. Ali, "IEC 61850 modeling of DSTATCOM and XMPP communication for reactive power management in microgrids," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3215–3225, Dec. 2018.

TAHA SELIM USTUN (Member, IEEE) 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 the Smart Grid Cybersecurity Laboratory. He has edited several books and special issues with international publishing houses. 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). 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 the IEEE 2800 Working Groups and IEC Renewable Energy Management Working Group 8. He is an Associate Editor of IEEE Access and a Guest Editor of the IEEE Transactions on Industrial Informatics. He is a reviewer in reputable journals and has taken active roles in organizing international conferences and chairing sessions.

SHAIK MULLAPATHI FAROOQ (Member, IEEE) 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 with 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. He is also an Assistant Professor with the Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College (Autonomous), Tirupati, India. His research interest includes cryptography, cyber physical systems, cybersecurity in vehicular networks, and power systems.

S. M. SUHAIL HUSSAIN (Member, IEEE) 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 from 2014–2015. He is a Guest Editor of the IEEE Transactions on Industrial Informatics.