Implementation of Secure Sampled Value (SeSV) Messages in Substation Automation System

Junho Hong, *Member, IEEE*, Ramya Karnati, *Student Member, IEEE*, Chee-Wooi Ten, *Senior Member, IEEE*, Soonwoo Lee, *Member, IEEE*, and Sungsoo Choi, *Member, IEEE*

***Abstract*—IEC61850 is the mainstream of the development for substation automation. This paper presents a practical consideration and analysis for implementing a secure sampled measured value (SeSV) message in substation automation system. Due to the lack of security features in the standard, IEC Working Group 15 of Technical Committee 57 published IEC62351 on security for IEC61850 profiles. However, the use of authentication methods for SV based on IEC62351 standards are still not integrated, and computational capabilities and performance are not validated and tested with commercial grade equipment. Hence, this paper shows the performance of security feature enabled SeSV packets transmitted between protection and control devices by appending a message authentication code (MAC) to the extended IEC61850 packets. A prototype implementation on a low cost commodity embedded system has proved that the MAC-enabled SV message can fully secure the process bus communication in the digital substation with negligible time delay.**

***Index Terms*—Digital relays, ethical hacking, IEC61850, IEC62351, message authentication code, substation security.**

I. Introduction

POWER substations are the critical juncture of an interconnected grid that transfer energy in long distance. Many substations are still operated with conventional monitoring and control schemes through hardwired cables and serial communication protocols [1]. The Ethernet-based communication brought many advantages, e.g., standardized system modeling and communication between different vendors. Furthermore, the use of standards based engineering brought many benefits to the power utilities. For instance, IEC61850 based engineering can (1) reduce the cost of configuration, installation, and commissioning, (2) enhance the multi-vendor interoperability, (3) increase the long-term stability, and (4) reduce the impact on the existing utility automation systems by upgrading the device capabilities through changing the communication stack in the system. This would only require to change the communication stack of the product when new revision of IEC61850 standard can become available [2]–[6].

Sampled value (SV) is a layer-2 protocol that is defined in IEC61850-9, and it contains measurements, e.g., three-phase currents and voltages with neutral values [7], [8]. Two types of SV messages are defined in IEC61850-9-2 LE, e.g., 80 samples per cycle for protection and 256 samples per cycle for measurement [9]. In the IEC61850 based digital substation, a merging unit (MU) is the device where SV is published, and it is also connected to circuit breakers via hardwires for control and status monitoring [10]. Once protective intelligent electronic device (IED) receives SV from MU, it calculates the protection functions, e.g., distance and time overcurrent protection. Then it will send a trip signal to MU for opening the circuit breaker (CB). Therefore, the digital substation has a high penetration of information and communication technology (ICT), and cyberinfrastructures have been widely deployed for monitoring, control, and operation, e.g., IEC61850 based system models and communications [11]. As a result, the number of cyber attacks on substations is increasing, and it becomes a major threat that may cause damages to the substation [12]. Monitoring-control attacks (MCA) may be stealthy, depending on the sophistication of the attacker.

Substation communication protocols are crucial for the operation. Its data integrity shall not be fabricated or modified by others [13]. However, its security features are not included in IEC61850 standard since (1) the need for high speed performance in SV, e.g., publishing 4800 samples per second in a 60-Hz system, (2) limited performance of the processor in IEDs and (3) cybersecurity was not a major concern when IEC61850 was published. Due to the lack of security establishment in IEC61850 standard, IEC Working Group (WG) 15 of Technical Committee (TC) 57 published IEC62351 on security for IEC61850 profiles [14]. One of the main objectives of IEC62351 standard is to develop cybersecurity features for SV message since the multicast scheme has potential cyber vulnerabilities, e.g., group center trust and group access control. Due to the limited processing power of IED, most encryption schemes or other security features are not applicable for the SV (it may delay

Manuscript received August 1, 2020; revised November 12, 2020; accepted February 18, 2021. Date of publication February 23, 2021; date of current version January 24, 2022. This work was supported in part by the projects of Korea Electrotechnology Research Institute (KERI) 20A01005 entitled "IEC61850 Message Authentication Code for Process Bus," and in part by U.S. National Science Foundation (NSF) Cyber-Physical System (CPS) 1739422 entitled "Collaborative Research: An Actuarial Framework of Cyber Risk Management for Power Grids." Paper no. TPWRD-01179-2020. *(Corresponding author: Junho Hong.)*

Junho Hong and Ramya Karnati are with the Department of Electrical and Computer Engineering, University of Michigan – Dearborn, Dearborn, MI 48128 USA (e-mail: jhwr@umich.edu; karnatir@umich.edu).

Chee-Wooi Ten is with the Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI 49931 USA (e-mail: ten@mtu.edu).

Soonwoo Lee and Sungsoo Choi are with Korea Electrotechnology Research Institute (KERI), Ansan-si 426-170, South Korea (e-mail: rheesw@keri.re.kr; sschoi@keri.re.kr).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPWRD.2021.3061205.

Digital Object Identifier 10.1109/TPWRD.2021.3061205

the protection function). Therefore, IEC62351-6 Ed.1 standard could be enhanced with authentication scheme with the 1024 b Rivest-Shamir-Adleman (RSA) digital signature for SV [14].

Based on the recommendation from IEC62351-6 Ed.1, different types of hardware and cryptography algorithms, e.g., RSA with 1024 and 512 keys, have been tested for generic object-oriented substation events (GOOSE) message; however, test results cannot meet the performance requirements using the state-of-art hardware as of 2010 [15], [16]. In order to find better performance algorithms, authors of [17] investigated the elliptic curve digital signature algorithm (ECDSA) and proved that ECDSA is faster than RSA and required lower computational power. The IEC62351-6:2020 Ed.2 standard will be released to recommend a more realistic and better performance authentication scheme with a digital signature using the hash-based message authentication code (HMAC) or Galois message authentication code (GMAC) for SV [18]. The flexible and plug-and-play security filter with GMAC and HMAC has been proposed and tested to secure the GOOSE communication for protection and control devices in a digital substation. The authors showed that the proposed GMAC based security filter could meet the transmission time requirement of GOOSE (i.e., 3 msec) [19]. The reference [20] provides a review of IEC62351 security mechanisms for IEC61850 based messages that include GOOSE, R-GOOSE, SV, R-SV and MMS. However, it is still not common to apply the GMAC and HMAC to SV (i.e., IEC61850-9-2LE), and need more research for a practical consideration for implementation, and also performance tests.

Practically, this paper shows the implementation and performance analysis of IEC62351 Ed.2 schemes for secure SV (SeSV) by modifying the structure of the SV protocol data unit (PDU). Different MAC algorithms, e.g., HMAC and GMAC, with different sizes of private keys are tested and validated. A hardware-in-the-loop (HIL) testbed with different hardware and software platform has been designed and implemented in a laboratory environment. The main contributions of this paper are (1) implementation of different MAC algorithms as per IEC62351-6:2020 to secure SV message, (2) SV intrusion detection algorithms when the preshared key is compromised and used by attacker, (3) laboratory based SV message related cyber attacks, impact analysis, and mitigations using HIL, (4) recommendations from performance and feasibility analysis of SeSV. In the remainder of this paper, Section II describes the potential cyber threats and existing vulnerabilities of the substation automation system. Section III explains the message authentication code (MAC) algorithms recommended by IEC62351-6:2020 standard. The implementation methods of cybersecurity features for SV have been proposed in Section IV. Section V provides the hardware-in-the-loop testbed and Section VI provides test results using HIL testbed of the proposed methods and algorithms. Conclusions and recommendations for future work are given in Section VII.

II. Security of Sampled Values

A. Substation Automation Features

A substation automation system (SAS) consists of hardware and software platforms with control and monitor processes that are connected through communication networks. An IED refers to a microprocessor equipped device that can perform a dynamic range of functions that include analog/digital conversion, protection scheme, and reporting system status. An MU IED converts analog currents and voltages signal to digital, and then send sampled digital information to protection and control (P&C) IED using SV message. SV message provides a multicast mechanism for communicating data between one or more IEDs over an Ethernet network. In this case, MU IED becomes a publisher and P&C IEDs will be subscribers. The layer 2 (data link) of the OSI model is used to map SV message data, and the payload datagram is shown in Fig. 1. The SV packet frame has the following fields:

Fig. 1. SV packet frame.

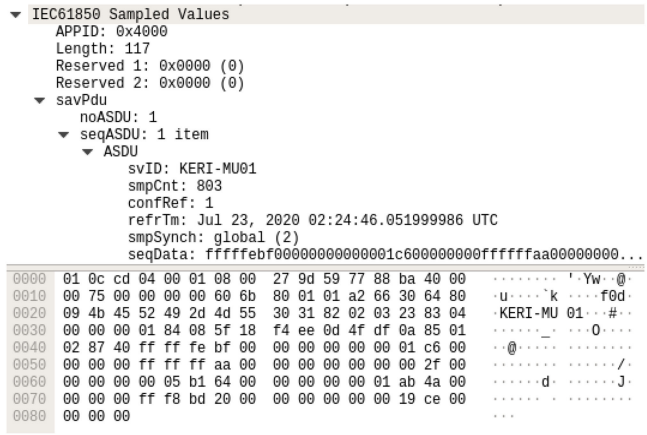

Fig. 2. APDU of SV packet (no security features).

1) Destination address: The first three octets are assigned by IEEE with `01-0C-CD` whereas the fourth octet will be `04` for multicast sampled values.
2) Source address: The address of the publisher.
3) VLAN priority tag: Priority tagging according to IEEE 802.1Q.
4) Ethertype: SV Ethertype is set to `88-BA`.
5) APPID: Application identifier.
6) Length: The total number of bytes in the SV message.
7) Reserved 1: Reserved for future standardization.
8) Reserved 2: Reserved for future standardization.
9) APDU: Application protocol data unit (APDU) that contains SV data structure.

The SV buffer is encoded as the APDU that contains information to be distributed in the process bus network, as described in Fig. 2.

The APDU of SV packet has the following fields:

1) `svID`: Should be a system-wide unique identification.
2) `smpCnt`: This will be incremented each time a new sampling value is taken. The counter shall be set to zero if the sampling is synchronised by clock signal and the synchronising signal occurs.
3) `ConfRef`: Configuration revision of the APDU.
4) `RefrTm`: Contains the refresh time of the SV buffer.
5) `smpSynch`: Synchronised by an external clock signal.
6) `seqData`: List of data values related to the data set definition.

Subscriber of protective IED receives this SV packet, and decode the necessary information. For instance, `smpCnt` is used for the synchronization between multiple SV streams.

B. Potential Threats and Vulnerabilities

Typically, most of the high voltage substations are unmanned due to the nature of the power transmission system (located in wide-spread and remote sites). Furthermore, substations communicate with a control center (for monitor and control) through gateways and wide area networks, so they are not isolated. Therefore, remote access functionality that operators or engineers can have access to the substations is crucial [21]. The main problem of the remote access point is that remote access points may not be installed with adequate security features, e.g., misconfigured firewall, weak combination of password and its policy. Successful electronic intrusion to substation can be initiated in multiple ways, e.g., malware infection and gaining credential of remote access. An adversary may infect the laptop who has access to the substation communication network or gain remote login credentials using social engineering [22]. When attackers gain access, they could compromise either or both the station equipment (P&C relays, remote terminal units or user-interfaces) or communication protocols; One could gain access to the process bus network once the bay-level equipment is compromised.

Due to the characteristics of the SV protocol, such as, plain text message and multicast at the data link layer, it exposes all data information in the communication network. If someone or device has access to the process bus, they can analyze the semantics of the SV message. Then they can find useful information that can be used for future cyber attacks. For instance, SV contains three-phase currents and voltages value. Modification of current measurements to 20 times the original value may trigger the protection scheme at the P&C IEDs. Another way to compromise the SV message and disrupt the regular operation of the substation system is to exploit the vulnerabilities of the processing process of the subscriber. More details will be discussed in the next Section.

C. Attacks Upon Sampled Values

1) Replay Attack: A replay attack can be initiated by playing back older SV packets that contain fault currents and voltages, which are critical information to pass on. In order to achieve the replay attack, attackers need to gain access to the monitoring port of process bus Ethernet switch, and capture the critical status of SV messages. The expected impact of a successful attack is to open the circuit breakers by triggering the protection functions of the SV subscriber (P&C IED).

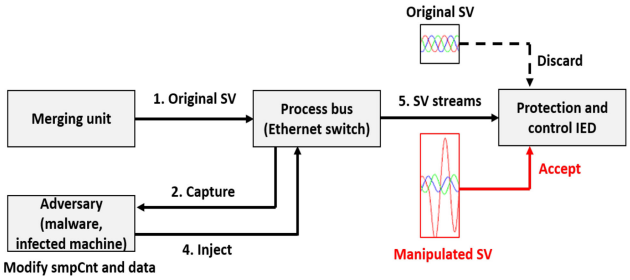

Fig. 3. An example of spoofing attacks for SV messages.

TABLE I
PARAMETERS OF ORIGINAL AND MANIPULATED SV PACKETS

Parameter	Original SV	Manipulated SV
`smpCnt`	N	N+10
`ConfRef`	1	1
`RefrTm`	7/18/2020 13:12	7/18/2020 13:12
`smpSynch`	2	2
`seqData`	I_1, I_2, I_3, V_1, V_2, V_3	$I_1 \times 20$, I_2, I_3, $V_1/20$, V_2, V_3

2) Spoofing With a False Data Injection: The main objective of spoofing false SV data injection attacks is to capture, modify, and inject the original message with abnormal information [23]. After capture the original SV message, an adversary can manipulate the `smpCnt` and `seqData`. So the SV subscriber (P&C IED) will discard the original SV but subscribe to the compromised SV messages as illustrated in Fig. 3. By modification of time synchronization information `smpCnt` and measurements `seqData` as shown in Table I, the adversary can manipulate the normal operation of SV subscribers. The increased smpCnt of manipulated SV packet will be accepted by the SV subscriber first, and then the lower number of `smpCnt` contained original SV packet will be dropped by SV subscriber. This is because SV subscriber programmed to receive the latest `smpCnt` contained SV packets for the synchronization. The injected increased I_1 and decreased V_1 data will trigger the protection function of P&C IED, and attackers can open the connected circuit breakers as described in Table I.

3) Flooding Attack: Availability is one of the keys to the normal operation in a substation. When a fault happened at the transmission line, if the fault current and voltage information cannot be reached to the P&C IED, backup protection will be initiated with unwanted outage areas. Attackers could identify the semantics of original SV messages in the process bus network. Then they can reproduce the lots of SV messages with the maximum size of Ethernet packets. This attack will disrupt the normal SV subscriber function of P&C IEDs, and they cannot process the protection functions due to the limited computational power.

4) High `smpCnt` Attack: Some IEDs are designed to subscribe the highest `smpCnt` contains SV packets. In this case,

TABLE II
SV MESSAGE SENDING PROFILE

	Protection	Measurement
Sample/cycle	80	256
Samples/package	1	8
Package/cycle	4,000 (50 Hz)	1,600 (50 Hz)
	4,800 (60 Hz)	1,920 (60 Hz)
Time interval between packets	250 μsec (50 Hz)	625 μsec (50 Hz)
	208 μsec (60 Hz)	520 μsec (60 Hz)

if SV subscriber continuously receives the highest number of `smpCnt` contained SV message, they will drop all other normal SV packets. By this cyber attack, the adversary could disrupt the normal SV processing operation in the substation. This will disrupt the normal monitoring on the measurement function of SV subscribers.

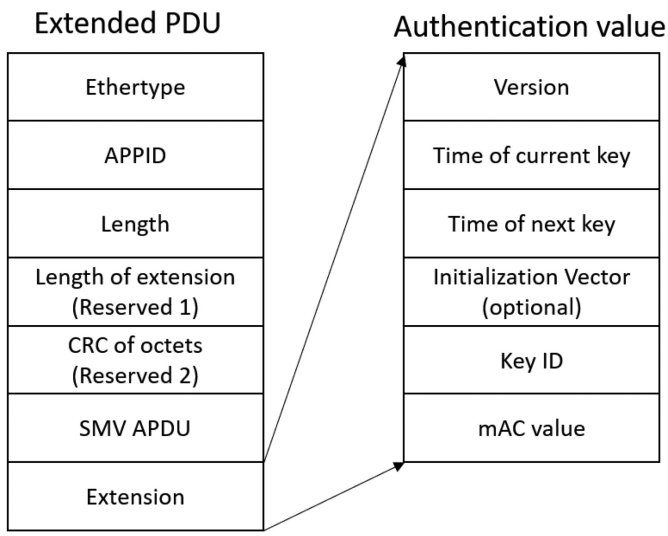

Fig. 4. Extended PDU for SV.

III. MESSAGE AUTHENTICATION CODE

A message authentication code (MAC) is known as a signed security tag, and it is used to authenticate a plaintext communication message. The MAC can be generated from the original message, and it contains a short length of security information for confirming the integrity of the transferred message from the sender [24]. Therefore, the receiver can identify whether the message is not manipulated by the adversary. Typically both the sender and the receiver should possess a shared secret key to detect any changes to the original message content. However, generating MAC from the message context will require computational power and time, and this is a crucial problem for the real-time operation of the substation automation system. For instance, power system protection applications (e.g., distance and overcurrent protection functions) in P&C IEDs need to receive 4800 SV packets per second in the 60-Hz power system (i.e., 0.208 [msec] packet interval as shown in Table II), and SV has to arrive within 3 [msec] as defined in IEC61850 [25]. Hence, SV message needs to have a higher priority than other input data, and encryption algorithms are not recommended due to the increased computational time and limited processing resources of the IEDs. In other words, the MAC should be calculated and encoded within appropriate time windows at the sender, and the receiver should decode and compare the MACs faster than the time interval between packets.

A. Galois Message Authentication Code (GMAC)

Galois/Counter Mode (GCM) has been widely adopted because of its efficiency and performance. It has a combined structure from counter (CTR) mode and message authentication code. GCM uses GHASH function (defined in Galois Field) for the message authentication code. Due to its fast throughput rate, it is known for the appropriate cryptography method that can be used for the high speed communication channels with low-cost commodity hardware. GCM can be used for only generating authentication code since GMAC uses encrypted data (i.e., no need to decrypt the data for MAC calculation). So GMAC is an authentication-only variant of the GCM. Any length of initialization vectors can be used and accepted by GMAC. GMAC can support parallel processing, so the speed of encoding and decoding could be faster than other algorithms.

B. Hash Message Authentication Code (HMAC)

HMAC is hash-based and it can guarantee the integrity and authentication of the message. Any cryptographic hash function could be used in the calculation of an HMAC. The advantages of HMAC could be (1) short and fixed length of the tag, (2) avoiding the duplication, and (3) hide the original message. Due to the characteristics of collision resistance (it is hard to find two inputs that the hash function generates the same output) and one-way function (mathematical function that takes an input and converts it into a fixed-length binary sequence that is computationally difficult to invert), calculating the same inputs from the generated HMAC tags is almost impossible.

IV. SV WITH MAC

This paper developed and implemented GMAC and HMAC PDU extensions to original SV packets. In order to integrate MAC algorithms, new cybersecurity functions, i.e., secure SV (SeSV), are introduced in the existing open-source code library [26]. It secures SV message communication by applying the MAC algorithms with preshared keys between publishers and subscribers. The SeSV functions are written in C language and combined with OpenSSL library.

Fig. 4 describes the implemented extended SV PDU that contains authentication value for cybersecurity. The reserved 1 and 2 fields need to be calculated. Reserved 1 refers to the length of the extension. Reserved 2 indicates the 16-bit CRC that is computed using the first 8 bytes of the SV PDU. The authentication value frame has the following fields [18]:

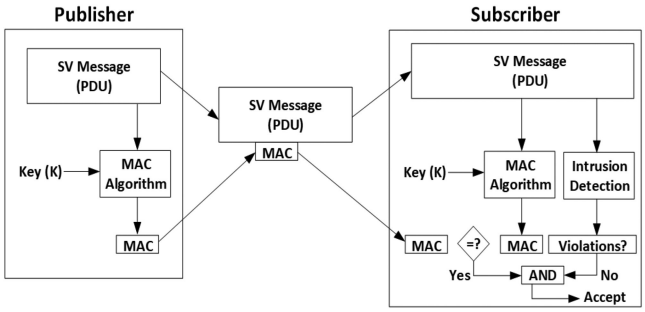

Fig. 5. Proposed SeSV MAC integration for publisher and subscriber.

TABLE III
ALGORITHM FOR PUBLISHER

SeSV_Publisher(SV PDU)
Step 1: Generate SV PDU without security, $SV^t_{ori} \leftarrow [V^t_{a,b,c}, I^t_{a,b,c}, \text{Time}]$
Step 2: Generate extension field, $SV^t_{ext1} \leftarrow \text{MAC}[\texttt{Key(K)}, SV^t_{ori}]$
Step 3: Appending the extension to the original SV PDU, $SV^t_{SeSV} \leftarrow [SV^t_{ori}, SV^t_{ext1}]$
Step 4: Publish to the process bus

1) Version: Extension protocol version number.
2) Time of current key: Time information of the current key.
3) Time of next key: Indication of the number of minutes prior to the new key being placed into service. A negative value is reserved to indicate that no new key has been scheduled to be placed into service.
4) Initialization vector: An initialization value for the MAC or encryption algorithm.
5) Key ID: Assigned by the key distribution center (KDC) as a reference.
6) MAC value: The calculated MAC value for the authentication/integrity of the messages.

Both additional features in extended PDU and the authentication values are considered to generate the SeSV frame. The following Section shows more details of generating MAC during the communication process in the digital substation environment.

A. MAC for Publisher and Subscriber

In order to secure the SV messages from the merging unit (publisher) to the P&C IED (subscriber), MAC algorithms (GMAC and HMAC) are applied. The overall authentication process of the proposed MAC scheme is shown in Fig. 5. Table III describes more details of the proposed SeSV. The SeSV engine generates original SV PDU SV^t_{ori} using three-phase currents $I^t_{a,b,c}$, voltages $V^t_{a,b,c}$, and time information (Time). The publisher and subscriber share the same shared symmetric key, `Key(K)`. The publisher will generate an extension field SV^t_{ext1} using MAC algorithms together with the key and the original SV PDU. Then the extension is appended to the original SV PDU, and the SeSV SV^t_{SeSV} will be published into the process bus network.

TABLE IV
ALGORITHM FOR SUBSCRIBER

SeSV_Subscriber(SV PDU)
Step 1: Capture and filter the SeSV packet, $C^t_{pkt,p}[SV^t_{SeSV}]$
Step 2: Generate extension field using the delivered SeSV, $SV^t_{ext2} \leftarrow \text{MAC}[\texttt{Key(K)}, SV^t_{SeSV}[SV^t_{ori}, SV^t_{ext1}]]$
Step 3: Compare SV^t_{ext1} and SV^t_{ext2}, a. If $SV^t_{ext1} = SV^t_{ext2}$, go to Step 4 b. If $SV^t_{ext1} \neq SV^t_{ext2}$, go to Step 7
Step 4: Check the semantics of each SV message as follows: a. If $SV^t_{cnt} + 1 = SV^{t+1}_{cnt}$ b. If $N^{su,T}_{same} >$ N numbers of same packets, $[SV^t_{dst}, SV^t_{aid}, SV^t_{cnt}] = [SV^{t+1}_{dst}, SV^{t+1}_{aid}, SV^{t+1}_{cnt}]$ c. If $SV^t_{cnt} + N < SV^t_{cnt}$
Step 5: If [3(b) OR 4(a,b,c)]=`true`, go to Step 7 otherwise go to Step 6
Step 6: Accept the SeSV packet
Step 7: Drop the SeSV packet and issue an alarm

Once the subscriber receives the packet with the MAC tag, it will calculate the MAC tag again using the pre-shared symmetric key, `Key(K)`. If the calculated MAC tag and delivered MAC tag are matched, the delivered SeSV message is verified and checked the integrity of the SV message. More details are illustrated in Table IV. Once the subscriber captures all incoming packets $C^t_{pkt,p}$ in the process bus, it will filter the SeSV packets. Then the parsed SeSV data is saved in the security buffer. New MAC SV^t_{ext2} is calculated from the delivered SeSV using the same key. If they match, the subscribed SeSV will be processed for the next "AND" logic as shown in Fig. 5. If attackers gain access or finish the reverse engineering to get the symmetric key, they can execute the cyberattacks that mentioned in Section II-C. In order to check such an attack, the intrusion detection module has been proposed for the SV subscriber. The semantics of SV messages can be used to check abnormal behaviors of SeSV. Step 4 detects a lost SV packet or replay attack by checking the SV counter number (`SmpCnt`, SV^t_{cnt}). `SmpCnt` will be incremented each time SV is published and will be reset to zero every second via pulse per second (PPS) signal. If attackers have the same symmetric key, they can generate the abnormal SV packet. This cannot be detected by the MAC algorithm since the delivered and calculated MAC will be the same. However, the injection of fabricated SV packets can be detected by Step 4-(b). This method will monitor the SV destination MAC address SV^t_{dst}, svID SV^t_{sid}, and APPID SV^t_{aid} of every packet. For instance, if more than N numbers of identical SV packets have the same SV counter number SV^t_{cnt} within short range of time window, this will not be an error but a SV injecting attack. Step 4-(c) shows `SmpCnt` SV^t_{cnt} violation. If there are more than N number of

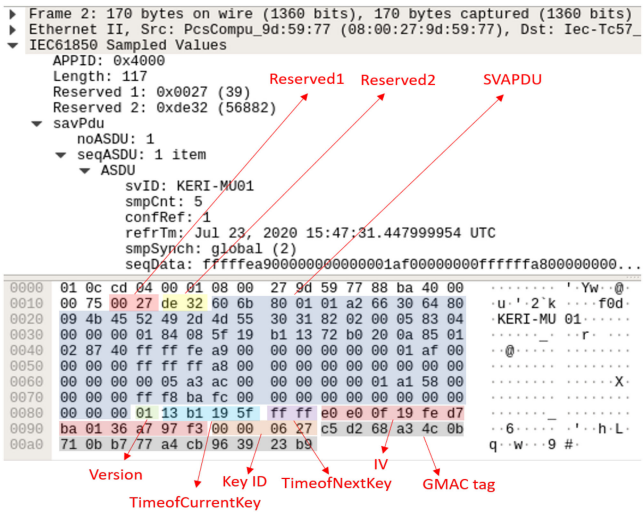

Fig. 6. Captured SV packet with AES-GMAC.

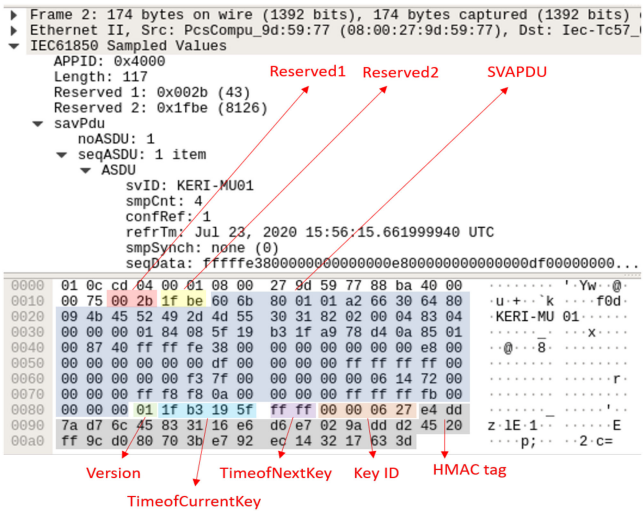

Fig. 7. Captured SV packet with HMAC-SHA.

lost SV packets, this will be regarded as "high `SmpCnt` attack." Once a violation is detected in Step 4, the P&C IED will drop all SeSV packets, and send an alarm to operators.

B. GMAC for SV

Fig. 6 shows the captured SeSV packet with AES-GMAC algorithm. It contains all the relative authentication values of SV PDU that is described in Fig. 4. The Reserved 1 field shows the 39 bytes of GMAC extension that is appended to the original SV packet whereas the Reserved 2 value indicates the 16-bit CRC calculation. The length of the generated GMAC tag is 16 bytes.

C. HMAC for SV

Similarly, Fig. 7 shows the captured SeSV packet with AES-HMAC algorithm. It also contains all the relative authentication values of SV PDU that is described in Fig. 4. One of the main differences between GMAC and HMAC tags is the IV field that is needed for GMAC calculation but not for the HMAC.

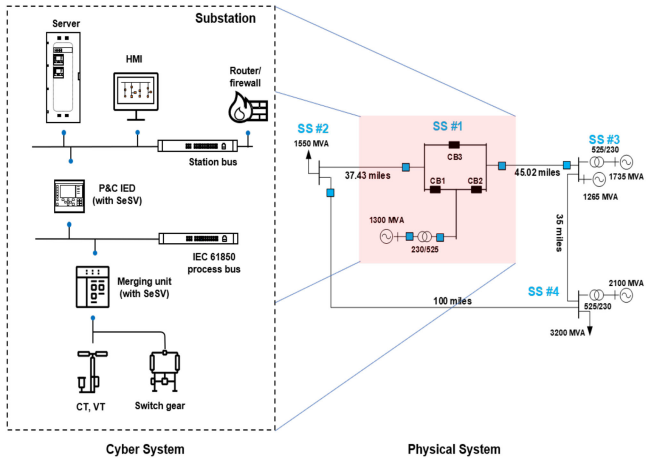

Fig. 8. HIL Testbed.

D. Key Distribution for MAC

The security key management methods for SV messages is described in IEC 62351-9 standard. It also explains methods of device authentication and authorization, and methods of policy and keying material agreement for IEC 61850 message encryption and data integrity protection [27]. There are two types of key management methods, (1) automated pairwise (unicast) and (2) group based (multicast) Group Domain of Interpretation (GDOI, RFC6407) to distribute the security policy and session keying material used to protect IEC 61850 messages when the messages are sent to a group of devices. The unicast method is used to secure TCP based communication between two peers whereas GDOI is used for group based security key distribution between key distribution center (KDC) and multiple devices in the substations. Note that the key distribution algorithms and methods for MAC (GDOI) will be discussed in future research.

V. Hardware-in-The-Loop (HIL) Testbed

To validate the proposed algorithms in a more realistic environment, a time-domain electromagnetic transient power system simulation model has been developed using MATLAB-Simulink Simscape Power Systems and extracted the simulated currents and voltages as input for the merging unit. The power system model used for the HIL simulation is shown in Fig. 8.

The model is created for a representative high voltage 500 kV substation and includes a number of controllable loads system. Additionally, a medium voltage network is also modeled with a distribution grid connected to the 230 kV side. A total of 2 embedded devices (TE0729-02-02IF-S, ARM Cortex-A9, 16-Bit wide 512 MByte DDR3 SDRAM, 4 GByte e.MMC Memory) are implemented for IEC61850 based merging unit and P&C IED with the proposed SeSV functions, respectively. In order to validate the performance of Intel CPU equipped IED [28], i5 CPU with 4 GB ram is also used for testing. A key requirement of the demonstration is that the proposed SeSV must not delay

TABLE V
PERFORMANCE EVALUATION OF GMAC FOR SV

Platform	Algorithms	Packet size (Bytes)	Average processing time (μsec)		
			Publisher	Subscriber	
			MAC	MAC	Comp.
Intel Core i5	AES-GMAC-128	170	6.392	6.402	1.021
	AES-GMAC-192	170	6.458	6.453	1.025
	AES-GMAC-256	170	6.505	6.509	1.026
ARM Cortex-A9	AES-GMAC-128	170	34.613	34.619	1.284
	AES-GMAC-192	170	34.849	34.884	1.345
	AES-GMAC-256	170	34.935	34.897	1.234

existing protection system's capability to detect and protect against faults in the system. It was confirmed in the lab set up that the distributed cybersecurity functions performed dependably in blocking simulated cyber attacks with timing performance that did not compromise the relays' protection times.

VI. CASE STUDY

A. *Case Study 1: Performance of MAC Algorithms*

Table V shows the results of the performance test using the different GMAC algorithms and hardware for the proposed SeSV. The GMAC encoding times at both publisher and subscriber and comparison times are calculated to check the average SeSV processing time. Due to the diverse of the microprocessors in the merging unit and P&C IEDs, one high performance and the other low processor have been chosen. The results show that AES-GMAC-128 algorithm has the most top processing performance, whereas AES-GMAC-256 has the most inferior performance. By considering the SV packet intervals as described in Table II, even AES-GMAC-256 can be used for the ARM core implemented device. Fig. 9 illustrates the overall results of different MAC algorithms with different hardware during 500 times of test cases.

Compare to the GMAC algorithms, HMAC showed much higher computational times to calculate the MAC tag as shown in Table VI and Fig. 10. Even though HMAC-SHA512 shows the highest average computational time, it is still faster than the lowest SV interval time (208 μsec). One interesting observation from the experiments is that HMAC algorithms showed a similar performance using Intel CPU; however, it showed different performance using the ARM core processor as described in Fig. 10.

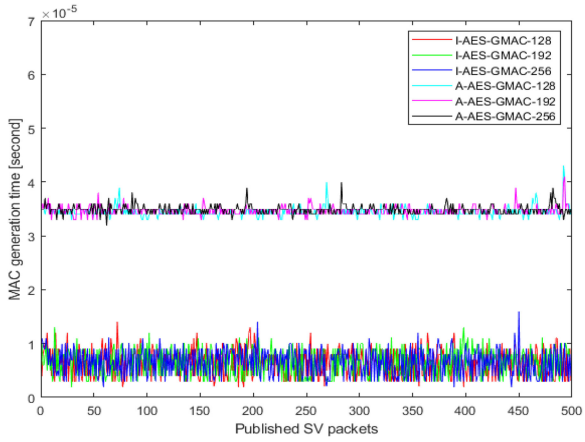

Fig. 9. GMAC generation time (I: Intel Core i5, A: ARM Cortex-A9).

TABLE VI
PERFORMANCE EVALUATION OF HMAC FOR SV

Platform	Algorithms	Packet size (Bytes)	Average processing time (μsec)		
			Publisher	Subscriber	
			MAC	MAC	Comp.
Intel Core i5	HMAC-SHA256-128	158	17.080	17.455	1.034
	HMAC-SHA256	174	17.933	17.930	1.061
	HMAC-SHA512	190	19.579	19.577	1.026
ARM Cortex-A9	HMAC-SHA256-128	158	96.212	96.250	1.134
	HMAC-SHA256	174	96.188	96.189	1.149
	HMAC-SHA512	190	172.815	173.224	1.127

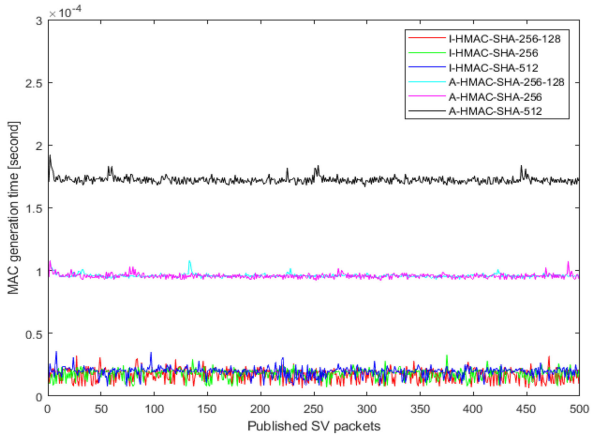

Fig. 10. HMAC generation time (I: Intel Core i5, A: ARM Cortex-A9).

TABLE VII
RESULTS OF SV ATTACKS

	Without SeSV		With SeSV	
Attack type	Attack result	Impact	Attack result	Impact
Replay	Success	Open CB	Fail	Alarm issued
Spoofing	Success	Open CB	Fail	Alarm issued
Flooding	Success	P&C IED comm. error	Fail	Alarm issued
High smpCnt	Success	Drop lots of SV packets	Fail	Alarm issued
Preshared key	N/A	N/A	Fail	Alarm issued

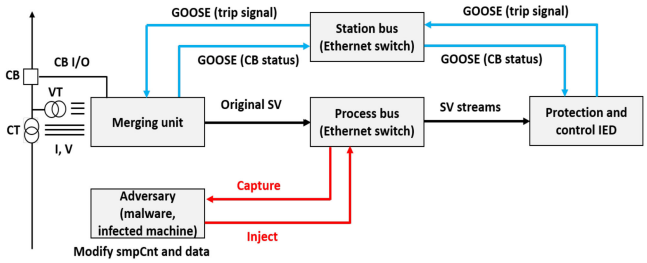

Fig. 11. Communication diagram for the case study.

B. Case Study 2: SV Attack Without MAC

The four different types of cyber attacks have been used for the case study of SV attacks as shown in Table VII. Once an adversary gains access to the process bus of the digital substation, they could monitor the SV packets and analyze the semantics of SV PDU. After finish the analysis of SV streams, they could initiate the four different types of SV attacks. For instance, they injected the malicious SV packets that contain fault currents and voltages, and the P&C IED will subscribe to the manipulated SV packet as illustrated in Fig. 11. The fault currents information of SV will initiate the overcurrent function of IED, and then the IED will send trip GOOSE messages back to the merging unit. The circuit breakers that are connected to the merging unit will be opened and attackers successfully finished the cyber attacks. In this scenario, the proposed SeSV has not been implemented in the merging unit and P&C IED. So the results show that the impacts of the successful attacks are critical.

C. Case Study 3: SV Packet Injection Attack With MAC

The proposed SeSV structures are implemented in this case study scenarios. As explained in Section IV-A, the MAC algorithms of SeSV detects the four types of cyber attacks including the preshared key based attack. Without the IDS module in SeSV subscriber, an SV injection attack using the same preshared key cannot be detected at the subscriber. The results show that the IDS module can bridge the gaps of the MAC based algorithms.

TABLE VIII
TOTAL PROTECTION TIME DELAY USING SESV

Platform	Algorithm	The total protection time delay (msec)
Intel Core i5	AES-GMAC-128	1.377
	AES-GMAC-192	1.361
	AES-GMAC-256	1.379
	HMAC-SHA256-128	1.384
	HMAC-SHA256	1.387
	HMAC-SHA512	1.386
ARM Cortex-A9	AES-GMAC-128	3.198
	AES-GMAC-192	3.159
	AES-GMAC-256	3.146
	HMAC-SHA256-128	3.195
	HMAC-SHA256	3.194
	HMAC-SHA512	3.199

D. Case Study 4: Time Delay for Protection

Cybersecurity functions must not interrupt the existing protection functions of P&C IED. Any delays or interruptions of the normal operation of P&C IED during the power system fault may damage or disrupt the life of expensive substation equipment, e.g., transformer. Therefore, the total time delay has been measured to validate the performance of the proposed SeSV that includes delays in the merging unit t_{MU}, process bus Ethernet switch t_{SWp}, delay in P&C IED t_{PI} to calculate the protection algorithm, SV communication delay t_{SV}, GOOSE communication delay t_{GS}, and station bus Ethernet delay t_{SWs} as shown in (1).

$$t_{total} = t_{MU} + t_{SWp} + t_{P1} + t_{SV} + t_{GS} + t_{SWs} \quad (1)$$

The merging unit starts to measure the time when a fault occurred at a transmission line, and then calculate the total time delay when MU receives trip GOOSE signal from the P&C IED. The simulated protection function is the instantaneous overcurrent function with root mean squared (RMS) calculation in the P&C IED. Table VIII shows the results of the total protection time delay from the fault to receiving a trip signal. Since the implemented HIL system only focused on the necessary functions, e.g., SeSV, GOOSE, and overcurrent protection, the actual implementation in the commercial IED may have more delays (subscribe multiple SV messages). The highest total delay to use ARM Cortex-A9 processor is when HMAC is chosen for the authentication algorithm, and this can be used for the applications with a total of 3.2 [msec] delay.

E. Case Study 5: Compromise SeSV

As shown in Table VII, potential cyber threats (Section II-C) against SV messages can be detected and mitigated by the proposed SeSV framework. Please note that there is no such thing as 100% security, and the proposed SeSV can be compromised with more efforts by attackers. However, the proposed SeSV increased sophistication of the attacker required to hack the Secure SV as described in Table IX, and this additional security layer can reduce the vulnerability of process bus network in a digital substation.

TABLE IX
POTENTIAL CYBER THREATS WITHOUT AND WITH SESV

Attack type	Without SeSV	With SeSV
Replay	Capture the event and reply the packets later.	Gain access to the root permission of Ethernet switch. Disable the original SV packets and replay the captured packets.
Spoofing	Capture the packet and learn the semantics of SV. Then inject the abnormal SV packets.	Gain access to the secret key for MAC generation. Gain access to the root permission of Ethernet switch. Disable the original SV packets and inject the abnormal SV packets.
SV flood	Capture the packet and modify the size of the packet. Then inject lots of manipulated SV packets.	Gain access to the secret key for MAC generation. Gain access to the root permission of Ethernet switch. Disable the original SV packets. Compromise the IDS module of SeSV IED. Inject lots of manipulated SV packets.
High smpCnt	Capture the packet and modify the smpCnt number. Then inject the modified SV every second.	Gain access to the secret key for MAC generation. Gain access to the root permission of Ethernet switch. Disable the original SV packets and inject the modified SV every second.
Preshared key	Gain access to the secret key. Generate the abnormal SV packets with MAC implementation.	Gain access to the secret key for MAC generation. Gain access to the root permission of Ethernet switch. Disable the original SV packets. Compromise the IDS module of SeSV IED.

VII. CONCLUSION

The increased numbers of cyber-physical attacks on power grid applications show that the need for improving security measures of the existing industrial communication protocols, e.g., SV message of IEC61850-9-2LE. Although IEC62351-6:2020 recommended to use GMAC and HMAC as cybersecurity mitigation to check the integrity of SV, practical considerations and performance tests to apply the MAC algorithms are not shown. Furthermore, the compromised symmetric key between publisher and subscriber may expose other security vulnerabilities and cyber threats. This paper proposed a SeSV framework to handle the above-mentioned problems using HIL testbed. The performance of the proposed SeSV has been evaluated and validated with different types of GMAC and HMAC algorithms and hardware platforms. The results of SeSV framework show promising and meeting the performance requirements of IEC61850. This can be implemented on existing IEDs in digital substations. Future work includes (1) interoperability issues between different products should be addressed, (2) performance evaluation of multiple SV streams, as well as (3) key distributed algorithms can be established. The proposed SeSV will be implemented and integrated into FPGA module (e.g., Xilinx Zynq) of the merging unit and then performance will be exhaustively tested.

ACKNOWLEDGMENT

The authors would like to thank Mr. R. Mackiewicz of Systems Integration Specialists Company, Inc. (SISCO) for the preliminary discussion of recent IEC61850 development and his technical insights for making this implementation possible.

REFERENCES

[1] D. C. Elizondo, J. de La Ree, A. G. Phadke, and S. Horowitz, "Hidden failures in protection systems and their impact on wide-area disturbances," in *Proc. IEEE Power Eng. Soc. Winter Meeting. Conf.*, 2001, pp. 710–714.
[2] G. N. Ericsson, "Cyber security and power system communication - essential parts of a smart grid infrastructure," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1501–1507, Jul. 2010.
[3] IEC 61850–1, "Part 1: Introduction and overview," *in Commun. Netw. Syst. Power Utility Automat.*, Mar. 2013.
[4] D. M. E. Ingram, P. Schaub, R. R. Taylor, and D. A. Campbell, "System-level tests of transformer differential protection using an IEC61850 process bus," *IEEE Trans. Power Del.*, vol. 29, no. 3, pp. 1382–1389, Jun. 2014.
[5] L. Zhu, D. Shi, and P. Wang, "IEC61850-based information model and configuration description of communication network in substation automation," *IEEE Trans. Power Del.*, vol. 29, no. 1, pp. 97–107, Feb. 2014.
[6] Q. Huang, S. Jing, J. Li, D. Cai, J. Wu, and W. Zhen, "Smart substation: State of the art and future development," *IEEE Trans. Power Del.*, vol. 32, no. 2, pp. 1098–1105, Apr. 2017.
[7] S. Kariyawasam, A. D. Rajapakse, and N. Perera, "Investigation of using IEC61850-sampled values for implementing a transient-based protection scheme for series-compensated transmission lines," *IEEE Trans. Power Del.*, vol. 33, no. 1, pp. 93–101, Feb. 2018.
[8] R. Wójtowicz, R. Kowalik, and D. D. Rasolomampionona, "Next generation of power system protection automation-virtualization of protection systems," *IEEE Trans. Power Del.*, vol. 33, no. 4, pp. 2002–2010, Aug. 2018.
[9] UCA International Users Group, "IEC 61850-9-2 LE: Implementation guideline for digital interface to instrument transformer using IEC 61850-9-2," Jul. 2004.
[10] J. Hong and C. Liu, "Intelligent electronic devices with collaborative intrusion detection systems," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 271–281, Jan. 2019.
[11] I. Lim and T. S. Sidhu, "Design of a backup ied for IEC61850-based substation," *IEEE Trans. Power Del.*, vol. 28, no. 4, pp. 2048–2055, Oct. 2013.
[12] J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4332–4341, Jul. 2019.
[13] Y. Yang, H. Xu, L. Gao, Y. Yuan, K. McLaughlin, and S. Sezer, "Multidimensional intrusion detection system for IEC61850-based scada networks," *IEEE Trans. Power Del.*, vol. 32, no. 2, pp. 1068–1078, Apr. 2017.
[14] IEC 62351–6:2007, "Power systems management and associated information exchange - data and communication security," *in Part 6: Security for IEC 61850*, 2007.
[15] F. Hohlbaum, M. Braendle, and F. Alvarez, "Cyber security practical considerations for implementing IEC62351," in *Proc. PAC World Conf.*, Dublin, Ireland, Jun. 2010, pp. 1–8.
[16] M. Strobel, N. Wiedermann, and C. Eckert, "Novel weaknesses in IEC62351 protected smart grid control systems," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, 2016, pp. 266–270.
[17] T. T. Tesfay and J. 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.
[18] IEC62351-6:2020 PRV, "Power systems management and associated information exchange - data and communication security," in Part 6: *Security for IEC61850*, 2020.
[19] D. Ishchenko and R. Nuqui, "Secure communication of intelligent electronic devices in digital substations," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo.*, 2018, pp. 1–5.
[20] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC62351 security mechanisms for IEC61850 message exchanges," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 5643–5654, Sep. 2020.
[21] J. Wang, G. Constante, C. Moya, and J. Hong, "Semantic analysis framework for protecting the power grid against monitoring-control attacks," *IET Cyber-Phys. Syst.: Theory Appl.*, vol. 5, no. 1, pp. 119–126, Mar. 2020.
[22] Y. Zhang, L. Wang, Y. Xiang, and C. Ten, "Inclusion of scada cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4379–4394, Nov. 2016.
[23] H. Smith and H. Morrison, *Ethical Hacking: A Comprehensive Beginner's Guide to Learn and Master Ethical Hacking*. Create Space Independent Publishing Platform, Jun. 2018.

[24] 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, Jun. 2019.
[25] "Consolidated version, communication networks and systems for power utility automation," in *Part 9-2: Specific Commun. Serv. Mapping - Sampled Values Over ISO/IEC8802-3*, IEC61850-9-2:2020 CSV, 2020.
[26] Michael Zillgith, "Open source libraries for IEC 61850," Mar. 2021. [Online]. Available: https://libiec61850.com/libiec61850/
[27] B. Weiss, M. Seewald, and H. Falk, "GDOI protocol support for IEC 62351 security services," in *Netw. Work. Group*, Oct. 28, 2016. [Online]. Available: https://tools.ietf.org/html/draft-weis-gdoi-iec62351-9-10
[28] SEL, "SEL-3555 real-time automation controller (RTAC)," Mar. 2021. [Online]. Available: https://selinc.com/products/3555/

Junho Hong (Member, IEEE) received the B.S.E.E. and M.S.E.E. degrees from Myonji University, Seoul, South Korea, in 2008 and 2010, respectively, and the Ph.D. degree from Washington State University, Pullman, WA, USA, in 2014. He is currently an Assistant Professor with the University of Michigan - Dearborn, Dearborn, MI, USA.

Ramya Karnati (Student Member, IEEE) received the B.S.E.E degree from Jawaharlal Nehru Technological University, Kakinada, India, in 2016 and the M.S.C.I.S. degree from the University of Michigan-Dearborn, MI, USA, in 2020. She was System Engineer at Tata Consultancy Services from 2017 to 2018.

Chee-Wooi Ten (Senior Member, IEEE) received the B.S.E.E. and M.S.E.E. degrees from Iowa State University, Ames, IA, USA, in 1999 and 2001, respectively, and the Ph.D. degree in electrical engineering from University College Dublin, Dublin, Ireland, in 2009. He is currently an Associate Professor with Michigan Technological University, Houghton, MI, USA.

Soonwoo Lee (Member, IEEE) received the Ph.D. degree in mechatronics from Korea University, Seoul, South Korea, in 2018. Since 2005, he has been with Korea Electrotechnology Research Institute, Gyeongsangnam-do, South Korea, and is currently a Principal Researcher with Power ICT Research Center.

Sungsoo Choi (Member, IEEE) received the B.S.E.E. degree from Gachon University, Seongnam, South Korea, in 1996, and the M.S.E.E. and Ph.D. degrees from the Gwangju Institute of Science and Technology, Gwangju, South Korea, in 1998 and 2003, respectively. From 2004 to 2015, he was a Professor with the University of Science and Technology, Daejeon, South Korea. He is currently a Principal Researcher with Korea Electrotechnology Research Institute, Gyeongsangnam-do, South Korea.