Analysis of IEEE C37.118 and IEC 61850-90-5 Synchrophasor Communication Frameworks

Analysis of IEEE C37.118 and IEC 61850-90-5 Synchrophasor Communication Frameworks

Rafiullah Khan, Kieran McLaughlin, David Laverty and Sakir Sezer
Queen's University Belfast, Belfast, United Kingdom
Email: {rafiullah.khan, kieran.mclaughlin, david.laverty, s.sezer}@qub.ac.uk

***Abstract*—ICT in smart grid provides enormous opportunities for real-time and wide-area grid monitoring, protection and control. To this aim, synchrophasor technology was proposed for reliable and secure transmission of grid status information. IEEE C37.118 and IEC 61850-90-5 emerged as two well known communication frameworks for synchrophasor technology. However, literature lacks a comprehensive analysis of some key features and limitations. Further, knowledge of cyber vulnerabilities in both communication frameworks is still quite limited. This paper analyzes characteristics of both communication frameworks inferred from their complete implementation. In particular, it addresses their embedded features, required network characteristics/resources and their resilience against cyber attacks.**

I. Introduction

Synchrophasor technology has the potential to become an integral part of modern power systems. It involves transmission of electrical quantities measured across different parts of the grid synchronized to a common precise time source e.g., GPS [1]. Today, numerous synchrophasor applications on Wide-Area Monitoring, Protection And Control (WAMPAC) have been developed including but not limited to islanding detection, grid dynamics recording/visualization, determining stability margins, enhancing situational awareness etc [2]–[4].

At present, there are two well-known communication frameworks for synchrophasor technology; IEEE C37.118 and IEC 61850-90-5. Initially published in 2005, IEEE C37.118 emerged as the most successful synchrophasor communication framework and is widely adopted [5]. However, research still lacks a proper analysis of its requirements, limitations and security challenges. Whereas, IEC 61850-90-5 was published in 2012 with several unique features [6]. However, its adoption is still quite limited and proper investigation of its features, requirements and limitations is required.

This paper summarizes findings inferred from a complete implementation of both, IEEE C37.118 and IEC 61850-90-5 and provides detailed comparison of their features and capabilities. Due to the involvement of critical infrastructure in synchrophasor applications, communication security is crucial. To this aim, this paper analyzes both communication frameworks considering security attributes such as confidentiality, integrity and availability. Further, the paper also explores vulnerabilities which could be exploited by intruders in single or multi-stage attacks to leave different power system components unable to communicate or unintentionally performing actions. This may result in severe damage to physical equipment. In short, the main contributions of the paper include: (i) features and limitations analysis of available synchrophasor communication frameworks, (ii) security and cyber vulnerabilities analysis, and (iii) identifying required network characteristics/resources.

II. Related Work

Several research efforts focused on the design of a suitable synchrophasor communication framework [7]. IEEE published a series of standards that were revised over time. Authors in [5] explained the evolution of IEEE C37.118 from IEEE 1344 and also highlighted key differences between old and new versions. Similarly, IEC 61850-90-5 originally evolved from IEC 61850 in 2012. Authors in [8] explained the evolution of IEC 61850-90-5 and addressed challenges in its commissioning.

The adoption of communication frameworks and creation of suitable interface in Phasor Measurement Units (PMU) and Phasor Data Concentrators (PDC) have been addressed in [9]. Authors have addressed practical aspects and requirements for the design of WAMPAC based on IEEE C37.118 and IEC 61850-90-5. Further, an open source OpenPMU project has been addressed in [10], which integrates IEEE C37.118 as communication protocol in the PMU. A similar work focusing on the importance of IP-based communication and especially the use of multicast has been presented by Seewald [11].

Synchrophasor systems frequently involve communication over insecure networks (e.g., Internet) which makes communication security crucial. Most research in literature focuses on addressing security challenges and cyber vulnerabilities for power systems in general but few have addressed synchrophasor systems. Authors in [12] outlined cyber security testing of components (e.g., PMUs, PDCs) from multiple vendors against port scanning, network congestions, protocol mutation, denial of service etc. Authors in [13] identified that C37.118 communication is vulnerable and a secure VPN is necessary to prevent packet modification/injection and eavesdropping on network traffic by external attackers. A similar work in [14] proposed a multi-layer architecture protected through firewall and VPN enabled security gateways which prevents access of external attackers to local power system network. The VPN tunnel securely encapsulates IEEE C37.118 messages to mitigate against potential cyber risks. Vulnerabilities in IEEE C37.118 have also been highlighted in [15] through demonstration of SQL injection attack. Authors concluded that such attack could be easily launched due to unencrypted traffic and lack of sanitization by the receiver. The literature still lacks to address security features of IEC 61850-90-5.

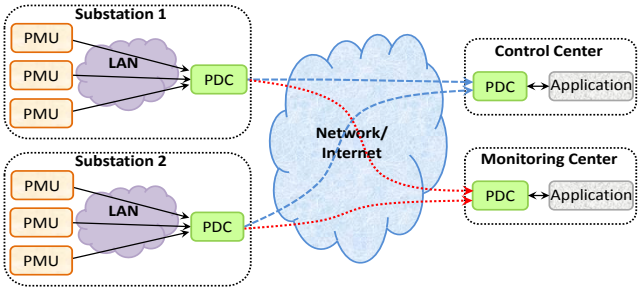

Figure 1. Generic synchrophasor system.

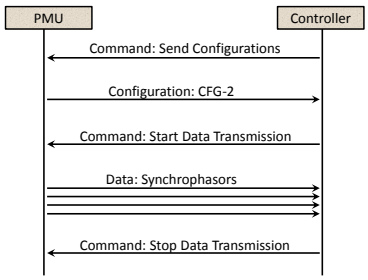

Figure 2. Generic IEEE C37.118-2 communication scenario with data source operating in commanded mode.

III. Generic Synchrophasor Measurement System

A synchrophasor system in general consists of PMUs, PDCs, communication network and control, monitoring or visualization application as depicted in Fig. 1. A PMU is a device that performs synchrophasor measurements from one or more voltage/current waveforms. It may operate either in commanded mode (i.e., its operations can be controlled by its remote peer) or spontaneous mode (i.e., it cannot receive control messages from its remote peer). It transmits synchrophasor data to remote peers either in unicast or multicast fashion. The remote peer may be either a PDC or control or monitoring center application. A PDC is a device that receives data from multiple PMUs (or other PDCs), aggregates and transmits as a single output stream. The generic synchrophasor system shown in Fig. 1 consists of two levels of PDCs; local/substation PDCs and control center or super PDCs. Local PDCs receive data from multiple PMUs inside substation whereas control center PDCs receive data from multiple substation PDCs.

IV. Communication Frameworks

This section analyzes unique features and highlights limitations of available synchrophasor communication frameworks.

A. IEEE C37.118 Communication System

IEEE C37.118 is the improved version of IEEE 1344 which was the first available synchrophasor communication standard. It defines methods for evaluation of synchrophasor measurements, time synchronization, application of time-tags and format of messages exchanged over the network. It does not put any restriction on the communication mode, protocol or media and messages can be transmitted in unicast, multicast or broadcast fashion over any communication medium and transport protocol. Originally, IEEE C37.118 addressed the performance of synchrophasors only under steady state conditions ignoring system disturbances and noise. However, a revision of IEEE C37.118 in 2011 accounts for more precision and support for dynamic power system conditions.

IEEE C37.118 describes four types of messages: data, configuration, header and command. Data messages are used to send actual real time measurements made by the PMU. Data from multiple PMUs may be transmitted in a single message correlated to a particular time stamp (i.e., PDC functionality). Configuration messages are in machine-readable format and contain information about calibration factors, data types and other meta data required by proper decoding of data messages by the receiver. Configuration messages are of three different types: CFG-1, CFG-2 and CFG-3. CFG-1 represents type of data and capability of PMU/PDU. CFG-2 indicates the synchrophasor measurements which are currently being transmitted/reported. Whereas, CFG-3 is similar to CFG-2 but contains some added flexibility and information about PMU characteristics and measurements. Header messages contain descriptive information (e.g., filtering, scaling algorithms etc) which is sent by the PMU/PDC but actually provided by the user. Command messages are used to control the operation of device sending synchrophasor measurements. In short, data, configuration and command messages are expressed in machine-readable format while header is descriptive information in human-readable format. Further, data, configuration and header are the message types sent by the data sources whereas command message is received by the data sources. The communication scenario is depicted in Fig. 2.

IEEE C37.118 has several limitations: (i) the lack of standard data names prevent auto-discovery and self-description without knowledge of configuration message, (ii) vendor specific features and customization weaken interoperability and integration support, and (iii) no built-in security mechanism.

B. IEC 61850-90-5 Communication System

IEC 61850-90-5 is derived from IEC 61850 which was initially proposed for substation automation. IEC 61850 is a complete communication system that addresses modeling of power system components, abstraction of services and communication protocols and methods [16]. It was designed with several objectives in mind: (i) interoperability and integration between power system components from different vendors, (ii) device/service modeling, (iii) self description and object auto-discovery due to structured meta-data, (iv) reliability mechanism through retransmission, (v) reduced substation cost through multicast and replacing of expensive relay-to-relay wiring with wireless communication, and (vi) support for machine to machine sharing of configuration data using Substation Configuration Language (SCL). However, IEC 61850 also has limitations including lack of security mechanism and restricted communication to only the local network. IEC 61850-90-5 inherits all the features of IEC 61850 while also overcoming its limitations. The key differences between IEC 61850 and IEC 61850-90-5 are shown in Fig. 3. IEC 61850-

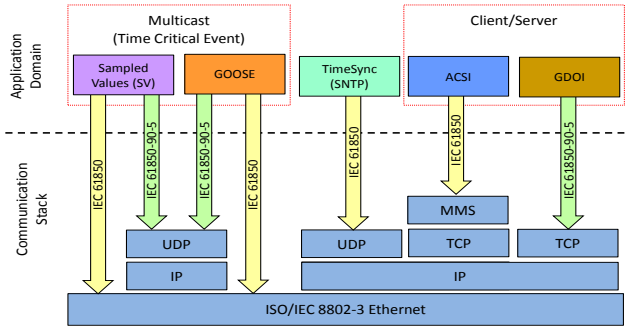

Figure 3. Difference between IEC 61850 and IEC 61850-90-5 protocol stack.

Table I
SUMMARY OF SUPPORTED FEATURES AND CAPABILITIES.

	IEEE C37.118	IEC 61850-90-5
Device/Service Modeling	No	Yes
Interoperability & Integration	Limited	Yes
Self Description	No	Yes
Auto-discovery	No	Limited
Local Network Communication	Supported	Supported
Wide-area Communication	Supported	Supported
Transport Protocols	Not-Specified	Specified
Communication Reliability	Only if TCP	Built-in
Multicast	Possible	Possible
Security/Encryption	No	Yes
Key-based Signature	No	Yes

90-5 includes a security mechanism based on Group Domain of Interpretation (GDOI) and also allows transmission of time-critical protocols over wide-area networks by relying on transport and network layer protocols.

As shown in Fig. 3, IEC 61850-90-5 consists of two time critical protocols; Sampled Values (SV) and Generic Object Oriented Substation Event (GOOSE), both designed to operate in multicast fashion. SV is stream based whereas GOOSE is event based messaging protocol. SV is the most suitable protocol for applications involving stream-based synchrophasor data transmissions. The data inside SV and GOOSE protocols is protected through encryption and signature algorithms which rely on a secret key. The secret key is provided by GDOI with assigned validity (TimeToNextKey attribute) and is periodically replaced with a new one. The security attributes can be observed in Wireshark capture (shown in Fig. 4) from our implemented IEC 61850-90-5 libraries. It can be observed in Fig. 4 that the encryption and signature calculation can be performed using any supported algorithm. The receiver determines the algorithms based on their identification tags in received packets. Table I summarizes key features of IEEE C37.118 and IEC 61850-90-5. IEEE C37.118 clearly lacks several features reported in Table I.

V. SECURITY ANALYSIS

Security of the synchrophasor communication frameworks is crucial as any incorrect information could cause severe damage to physical equipment. This section compares IEEE C37.118 and IEC 61850-90-5 from a security point of view and analyzes their degree of resistance/protection against different cyber attacks. The analysis is performed using CIA (Confidentiality, Integrity and Availability), a widely adopted model for cyber security. Table II summarizes the analysis.

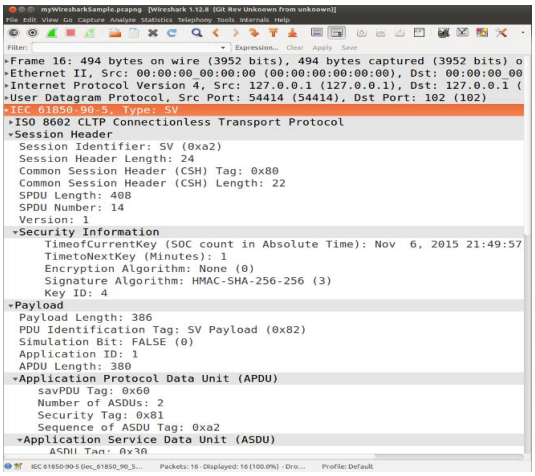

Figure 4. Captured packet with developed Wireshark plug-in from our implemented IEC 61850-90-5 libraries.

A. Confidentiality

Confidentiality deals with information privacy when packets are being transmitted over insecure networks. It prevents attackers access to the sensitive information sent inside packets. Confidentiality in communication is normally achieved through encryption. This allows only intended recipients able to decode packets with the knowledge of encryption algorithm and secret key. IEC 61850-90-5 has built-in security mechanism based on GDOI and assumes that Key Distribution Center (KDC) and communicating devices are secure. The strength of confidentiality in IEC 61850-90-5 is very high due to periodic refreshing of secret key by GDOI. Whereas, IEEE C37.118 offers no confidentiality as it lacks such a security mechanism.

B. Integrity

Integrity deals with accuracy and trustworthiness of data. It ensures that the packets have not been altered during transit. Non-repudiation is sometimes also regarded as part of integrity and ensures that a sending device cannot deny of sending a specific packet. IEEE C37.118 includes Cyclic Redundancy Check (CRC) code inside packets which ensures integrity against any modification. However, the CRC code is calculated using a predefined algorithm without using a secret key. Thus, an intruder may get access to the packet, modify its content, easily recalculate a new CRC code and transmit the modified packet to the receiver. The receiver will fail to detect unauthorized modification to packet content as it will pass the CRC verification process. On the other hand, IEC 61850-90-5 includes cryptographic signature inside packets using a secret key. This enables the receiver to easily detect unauthorized modifications even if no encryption is used.

C. Availability

Availability ensures uninterrupted communication between sender and receiver. Such attacks can be achieved by bombarding a receiving device with non-relevant or spam packets to exhaust its resources and prevent it from processing packets from intended/authorized senders. Availability can be targeted

Table II
SUMMARY OF SECURITY ANALYSIS.

	IEEE C37.118	IEC 61850-90-5
Confidentiality	None	Strong
Integrity	Weak	Strong
Availability	Vulnerable	Vulnerable

in both IEEE C37.118 and IEC 61850-90-5. However, availability attacks could be mitigated in IEC 61850-90-5 to some degree due to forming a group of authorized devices. The GDOI security mechanism mitigates against an unauthorized device being able to communicate with authorized devices. A device may simply discard packets without processing if received from unauthorized devices using a cookie mechanism.

D. Resilience Against Cyber Attacks

Vulnerabilities in communication could be exploited in the form of different attacks to impair the communication or cause damage to the physical equipment in a synchrophasor system. Reconnaissance attacks could take place on the network traffic to discover vulnerabilities such as open ports at a receiver, protocol types, unencrypted packets etc. Itself, it is not a harmful attack but an attacker may exploit discovered vulnerabilities to launch severe attacks e.g., authentication/access, denial of service etc. Due to no encryption, eavesdropping on IEEE C37.118 traffic could reveal useful information to an attacker e.g., name and current state of substation, location of devices (PMUs, breakers etc), communication configurations etc.

An attacker may launch authentication or access attack to get unauthorized access to information. Such an attack could be launched on a physical device or network traffic (by inspecting packet content). With no authentication process in IEEE C37.118, it is possible that a device assumes data is received from genuine sender but it may indeed generated by an intruder. This allows an intruder to control functionalities of the receiving device. IEC 61850-90-5 is protected against unauthorized access attacks as security credentials are only known to GDOI authorized devices (assuming that KDC and communicating devices are secure). Replay or reflection is another similar attack. It stores network traffic between communicating peers and replays it to the receiver to hide real time status of the sender (e.g., power system). The outdated replayed packets will leave receiver unintentionally performing wrong decisions. Replay/reflection attacks could be launched on both, unencrypted (e.g., IEEE C37.118) as well as encrypted (e.g., IEC 61850-90-5) traffic. However, the GDOI based security mechanism of IEC 61850-90-5 prevents such attacks by using short validity period for security credentials.

Man In The Middle (MITM) attacks are normally considered very harmful.These attacks intercept packets in transit, alter them and send modified packets to the receiver. In case of IEEE C37.118, a receiving device could be easily deceived about the authenticity of the packets and unintentionally perform wrong decisions. E.g., MITM attack on the configuration message of IEEE C37.118 could permanently leave a receiver unable to decode upcoming data messages (i.e., actual synchrophasors). IEC 61850-90-5 based communication is protected against MITM attacks due to encryption.

Table III
RESILIENCE AGAINST CYBER ATTACKS.

Attack Type	IEEE C37.118	IEC 61850-90-5
Reconnaissance	Vulnerable	Protected
Authentication/Access	Vulnerable	Protected
Replay/Reflection	Vulnerable	Protected
Man In The Middle	Vulnerable	Protected
Denial of Service	Vulnerable	Vulnerable

Another common attack in communication system is Denial of Service (DoS) which targets availability (addressed in Section V-C). As addressed before, both IEEE C37.118 and IEC 61850-90-5 are vulnerable to DoS/availability attacks. However, it could be mitigated to some degree in IEC 61850-90-5 communication. Table III summarizes resilience of IEEE C37.118 and IEC 61850-90-5 against different cyber attacks.

E. Protection using Secure VPN

Protection against cyber attacks can be achieved by using secure VPN. The VPN technology securely connects two remote devices or networks over insecure network using authentication, tunneling and encryption. Normally in corporate environment, a secure tunnel is established between VPN gateways of two remote networks e.g., a VPN tunnel can be established between gateways of substation and control center networks in Fig. 1. All PMUs in Fig. 1 will send synchrophasor data normally which will be encapsulated by substation gateway into VPN tunnel before traversing insecure Internet and de-capsulated by control center gateway back into original packets. VPN technology can be adopted for both, IEEE C37.118 and IEC 61850-90-5 but is more beneficial for IEEE C37.118 due to its no built-in security mechanism. VPN ensures confidentiality and integrity, availability is still vulnerable. The absolute protection against DoS attacks is hard to achieve. Although, VPN technology provides privacy, security and freedom, it has also few limitations: (1) it provides protection from external attackers but vulnerabilities in Table III remain valid for internal attacks (unless each PMU uses its own dedicated VPN tunnel with control center), (2) it increases the overall communication overhead and bandwidth requirement due to encapsulation, (3) it has reduced reliability and increased latency depending on the number, location and performance of VPN servers, (4) it assumes that the VPN peers are protected from any kind of malware, (5) due to immature standards, VPN technology from different vendors may face interoperability issues, (6) VPN tunnel normally uses fix security unlike IEC 61850-90-5 whose security credentials are refreshed periodically for protection against cryptanalysis, (7) ISPs in some countries block VPN traffic due to government regulations on keeping track of Internet activities/traffic.

VI. NETWORK CHARACTERISTICS

This section briefly compares the synchrophasor communication frameworks in terms of packet size, communication overhead and required bandwidth. The reported results assume that each data packet is carrying 2 analog and phasor values,

Table IV
SUMMARY OF NETWORK CHARACTERISTICS.

OVERHEAD ANALYSIS						
	IEEE C37.118				IEC 61850-90-5	
	Data	Config.	Command	Header	SV	GOOSE
RealInfo	26.83%	86.70%	3.33%	21.62%	50.16%	56.48%
Formatting	21.95%	3.67%	26.67%	21.62%	36.25%	31.41%
Total Overhead	73.17%	13.3%	96.67%	78.38	49.84%	43.52%
BANDWIDTH REQUIREMENT						
	IEEE C37.118				IEC 61850-90-5	
	Data Messages				SV	GOOSE
With UDP	65.6 kbps				0.247 Mbps	0.278 Mbps
With TCP	84.8 kbps				–	–

Note: Overhead analysis presents percentage of real information, protocol formatting and total overhead (includes protocol formatting plus communication i.e., headers) in a single packet sent over UDP. The bandwidth requirement assumes 100 messages per second as data transmission rate over UDP or persistent TCP connection.

1 digital word, frequency in integer and rate of change of frequency in floating point format. These settings are also reflected in IEEE C37.118 configuration message. It is assumed that IEC 61850-90-5 is carrying dataset of size 74 Bytes based on implementations in [10].

A. Communication Overhead

The overhead indirectly reflects the maximum size of data that can be included in a single packet (i.e., PDC aggregating data from multiple PMUs). It is also a factor determining how much additional channel bandwidth is required due to overhead information. High communication overhead for synchrophasor applications which involve high data transmission rates significantly increases the channel bandwidth requirement. It can be observed in Table IV that the communication overhead for IEEE C37.118 is significantly high while lower for IEC 61850-90-5. The IEEE C37.118 overhead will further increase if TCP is used as transport protocol.

B. Bandwidth Requirements

The channel bandwidth requirement depends on the message size and rate of data transmission. It increases rapidly if bulk packets are transmitted at higher rates (i.e., PDC aggregating data from large number of PMUs). To avoid traffic congestion and packet loss, minimum required bandwidth should be available for synchrophasor applications. It can be observed in Table IV that IEEE C37.118 has lower network bandwidth requirement although has higher communication overhead compared to IEC 61850-90-5. It is due to the fact that IEC 61850-90-5 has large packet size due to metadata and carrying complete decoding information in each packet. IEEE C37.118 data messages are very compact in size due to reporting configuration/decoding information separately in infrequent configuration message, resulting in much lower bandwidth requirement.

VII. CONCLUSIONS

At present, two established communication frameworks are available for synchrophasor systems; IEEE C37.118 and IEC 61850-90-5. A comparison of both communication frameworks can enable synchrophasor application developers to choose the right protocol based on their requirements and available resources. However, existing research literature lacks a comparison of certain features and specifically cyber security. IEEE C37.118 has been widely studied in literature and some previous works have pointed out its cyber vulnerabilities (as addressed in Section II). However, it superiority or inferiority over IEC 61850-90-5 in terms of security features, network requirements or embedded features and capabilities need to be investigated.

This paper has analyzed findings inferred from the implementation of both communication frameworks. The findings were classified into three categories: (i) supported features and capabilities (summarized in Table I), (ii) security analysis based on CIA model and resilience against cyber attacks (summarized in Table II & Table III, respectively), and (iii) network characteristics and required resources (summarized in Table IV). IEEE C37.118 is a weak communication framework from a security point of view due to no built-in security mechanism. On the other hand, IEC 61850-90-5 provides strong protection against cyber attacks by relying on GDOI based security mechanism. However, this assumes the KDC and communicating devices secure from unauthorized access. In terms of required network resources, IEEE C37.118 is highly efficient with very small packet size compared to IEC 61850-90-5. This results in much lower bandwidth requirement for IEEE C37.118 compared to IEC 61850-90-5.

REFERENCES

[1] S. Thakur and A. Chakrabortty, "Multi-Dimensional Wide-Area Visualization of Power System Dynamics Using Synchrophasors," in *IEEE Power and Energy Society General Meeting (PES-GM)*, 2013.

[2] M. S. Almas *et al.*, "Synchrophasor Network, Laboratory and Software Applications Developed in the STRONg2rid Project," in *PES-GM*, 2014.

[3] E. O. Schweitzer *et al.*, "Advanced Real-Time Synchrophasor Applications," in *35th Annual Western Protective Relay Conference*, 2008.

[4] J. Liu and C. C. Chu, "Short-Term Voltage Instability Detections of Wind Generators Using Synchrophasors," in *PES-GM*, 2014.

[5] K. E. Martin *et al.*, "Exploring the IEEE Standard C37.118-2005 Synchrophasors for Power Systems," in *IEEE Transactions on Power Delivery, VOL. 23, NO. 4*, 2008.

[6] "Communication Networks and Systems for Power Utility Automation," in *IEC 61850-90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118*, 2012.

[7] K. Martin, "Synchrophasor Standards and Guides for the Smart Grid," in *PES-GM*, 2013.

[8] V. Madani *et al.*, "Challenges and Lessons Learned from Commissioning an IEC 61850-90-5 based Synchrophasor System," in *68th Annual Conference for Protective Relay Engineers*, 2015.

[9] G. Renal *et al.*, "Practical Aspects of Testing Phasor Data Concentrators for Wide-area Monitoring Systems," in *IEEE CCECE*, 2014.

[10] D. Laverty *et al.*, "The OpenPMU Project: Challenges and Perspectives," in *PES-GM*, 2013.

[11] M. Seewald, "Building an Architecture Based on IP-Multicast for Large Phasor Measurement Unit (PMU) Networks," in *PES ISGT*, 2013.

[12] T. Morris *et al.*, "Cybersecurity Testing of Substation Phasor Measurement Units and Phasor Data Concentrators," in *ACM Annual Workshop on Cyber Security and Information Intelligence Research*, 2011.

[13] L. Coppolino, S. DAntonio, and L. Romano, "Exposing Vulnerabilities in Electric Power Grids: An Experimental Approach," in *International Journal of Critical Infrastructure Protection vol:7(1), pp:51-60*, 2014.

[14] J. Stewart *et al.*, "Synchrophasor Security Practices," in *14th Annual Georgia Tech Fault and Disturbance Analysis Conference*, 2011.

[15] S. D'Antonio, L. Coppolino, I. Elia, and V. Formicola, "Security Issues of a Phasor Data Concentrator for Smart Grid Infrastructure," in *13th ACM European Workshop on Dependable Computing*, 2011.

[16] A. Apostolov, "Impact of IEC 61850 on the Interoperability and Reliability of Protection Schemes," in *PES-GM*, 2013.