2nd International Conference on Advances in Science & Technology (ICAST-2019)
K. J. Somaiya Institute of Engineering & Information Technology, University of Mumbai, Maharashtra, India

Applicability of Blockchain for Synchrophasor Network

Shivani Thakkar
Department of Information Technology
K.J. Somaiya College of Engineering
Mumbai, India.
shivani.st@somaiya.edu

Prof. Ashwini Dalvi
Department of Information Technology
K.J. Somaiya College of Engineering
Mumbai, India.
ashwinidalvi@somaiya.edu

Prof. Irfan Siddavatam
Department of Information Technology
K.J. Somaiya College of Engineering
Mumbai, India.
irfansiddavatam@somaiya.edu

Prof. Faruk Kazi
Department of Electrical Engineering
Veermata Jijabai Technological Institute
Mumbai, India.
fskazi@el.vjti.ac.in

Abstract— **Modern power grids highly use synchrophasor communication networks. The synchrophasor network is the backbone of the smart grid. It collects and communicates the measurement data which includes important parameters like phasors, frequency and time. Synchrophasor networks include hardware like Phasor Measurement Units (PMU) and Phasor Data Concentrators (PDC) which majorly communicate the measurement data using IEEE C37.118 standard. This communication architecture has two major drawbacks. First, the IEEE C37.118 Standard lacks encryption mechanism. Second, the communication architecture is centralized in nature. In this paper, we highlight the security analysis of IEEE C37.118 standard and discuss the proposed solutions like Hadoop, Distributed Intrusion Detection System (IDS) and Blockchain. We identify the role of blockchain in Smart Grids and also validate its role as a trust model.**

Keywords— Synchrophasor communication, Phasor Measurement Unit (PMU), Phasor Data Concentrator (PDC), Smart Grid, Blockchain

I. Introduction

Smart grid uses a variety of networking technologies. The networking technologies should be advanced enough to make the smart grid highly reliable [1]. Synchrophasor communication networks are widely used in the smart grids. It forms the backbone of the smart grid and collects and communicates the measurement data upstream. The measurement data includes voltage phasors, current phasors, frequency and time. The accuracy of this data is of vital importance in the decision making of the synchrophasor network.

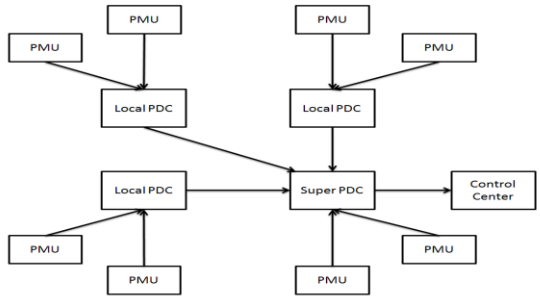

Fig. 1. Smart Grid WAMS layout comprising of PMUs and PDCs.

Fig. 1 shows the layout of a smart grid WAMS [2]. It consists of devices like PMUs and PDCs. The PMU is a device which timestamps the measurement data using Global Positioning System (GPS). It then sends it to the PDC. A PDC receives the measurement data from multiple geographically distributed PMUs and time synchronizes the data. It then further sends the data to the control center. The decision making of the control center relies heavily on the correctness of the data received. The communication standard used by PMU and PDC to communicate in a synchrophasor network is IEEE C37.118 Standard.

Synchrophasor networks, involving PMU and PDC, have certain drawbacks. The communication of the measurement data is done over the public networks. IEEE C37.118 standard lacks encryption and hence is vulnerable to cyber-attacks. The PMU-PDC-control center architecture is a centralized architecture and hence it is not tolerant to failure of node in the network.

The background work for this paper includes security analysis of the IEEE C37.118 standard and also discusses proposed distributed architectures like Hadoop, Distributed IDS and Blockchain. Section III discusses the role of blockchain in the smart grid synchrophasor network. Section IV discusses about its validation.

II. Background Work

A. *Security Analysis of IEEE C37.118 Standard*

There are three main security objectives for the synchrophasor networks. They are Confidentiality, Integrity and Availability [2-4] .

Confidentiality deals with protection and privacy of information. It is necessary that the data exchanged in PMU-PDC communication should be protected. If this data is exposed then the attacker would be able to know the consumption values and hence will be able to trace the consumer behavior. Confidentiality can be breached by unauthorized disclosure of data or well-planned attacks. Confidentiality can be achieved by using encryption techniques and access control lists.

Integrity deals with the correctness of data. It is necessary that the data/packets exchanged by PMU-PDC should be accurate and correct. If there is a loss of integrity of the data/ packets exchanged by PMU-PDC then it would result in incorrect decisions made by control center related to power measurements and as a result may affect the devices of the synchrophasor network. Integrity of the data can be achieved by using hash verifications, checksums and authentication systems.

Availability deals with uninterrupted communication of data between sender and receiver. It is necessary that there is timely and reliable access to the data in the synchrophasor network. Loss of availability will lead to interruption of access to information, which may affect the power delivery decisions.

The limitations and cyber vulnerabilities of IEEE C37.118 standard are discussed in [5]. There is no built in security for IEEE C37.118 standard as discussed by the authors. The authors in this paper have performed security analysis of the IEEE C37.118 Communication system using CIA (Confidentiality, Integrity, Availability). Table 1 shows the summary of the security analysis.

TABLE I. SECURITY ANALYSIS [5]

Security Objectives	Description	IEEE C37.118	Attacks Possible
Confidentiality	It deals with information privacy.	None (lacks security mechanism)	Packet Analysis Attack
Integrity	It deals with the correctness of data.	Weak (IEEE C37.118 Standard uses Cyclic Redundancy Check (CRC) code to ensure integrity of data. But a predefined algorithm is used (without using secret key) to calculate the CRC code. As a result, an attacker may get access to the packet and will be able to modify the packet and send new packet to the receiver after recalculating the CRC code.)	Man-In-The-Middle Attack
Availability	It deals with uninterrupted communication of data between sender and receiver.	Vulnerable (Availability of data can be targeted by launching a Denial of Service attack)	Denial of Service Attack

Authors of the paper [5] have also discussed the resiliency of the IEEE C37.118 standard against certain cyber-attacks. Table 2 summarizes the resiliency of IEEE C37.118 standard against the attacks.

TABLE II. RESILIENCY OF IEEE C37.118 AGAINST ATTACKS [5]

Attack Type	Attack Description	IEEE C37.118
Reconnaissance	This attack discovers the open ports, protocol types and unencrypted packets.	Vulnerable (Encryption is not used)
Authentication/ Access	This attack inspects packet content.	Vulnerable (Authentication process is not used)
Replay/Reflection	It deals with uninterrupted communication of data between sender and receiver.	Vulnerable (Availability of data can be targeted by launching a Denial of Service attack)
Man In The Middle	This attack intercepts and alters the packet and sends to the receiver.	Vulnerable(Authentication and Encryption process is not used)
Denial of Service	This attack sends spam packets and attacks the availability of data.	Vulnerable

From the above tables we know that the IEEE C37.118 standard which is used for the PMU-PDC communication is vulnerable to a number of attacks. The devices and communication network of the synchrophasor network are vulnerable to attacks like MITM attack, DoS attack, False data injection attack, Snooping , Delay attack, GPS Spoofing attack and SQL Injection attack [2][6-8]

B. *Proposed Solutions*

PMU and PDC devices use the IEEE C37.118 communication framework and are already implemented in the smart grid networks which are costly to replace. Hence there is need to find a way to mitigate the effects of the attacks mentioned before. Authors of paper [9] and [10] suggest for the decentralized synchrophasor communication architectures. In a centralized communication architecture, the PMUs report to single control center. It uses simple communication techniques. But it is less reliable than decentralized architecture. Centralized communication architecture is vulnerable to single point failures. The failure of communication may affect the monitoring systems of the synchrophasor networks. Decentralized communication architecture has several control centers and they coordinate with each other to take control actions. This architecture is robust and expensive than the centralized architecture.

In [11], the authors have proposed to use Hadoop framework as it provides a scalable fault-tolerant distributed system for data storage and processing. In [12], the authors have proposed a distributed Intrusion Detection System (IDS) with a decentralized nature to detect and the malicious activities and enhance the security. The research in [2] is summarized by specifying solutions to the cyber-security challenges. The solutions for the cyber-attacks on the communication between devices of smart grid include Cyber trust model with blockchain i.e. decentralized blockchain based model and publish subscribe hub-spoke architecture proposed by NASPInet [7].

1) Hadoop:

Hadoop is a scalable, fault tolerant, distributed system for data storage and data processing. It has two primary components: HDFS (Hadoop Distributed File System) and MapReduce [13]. HDFS is Hadoop's storage system that has master - slave architecture. Each cluster consists of a single NameNode and a set of DataNodes. When the data is pushed, HDFS replicates the data and stores it in form of blocks in various Data Nodes and the Name Node consists the index of all locations. Hadoop provides an efficient storage, processing and analyzing power for the huge PMU measurements data. It provides a distributed storage by dividing the data into blocks and storing and replicating them. Hence it becomes fault tolerant in nature and is resilient to failure of a node/machine [11], [14]. The Tennessee Valley Authority (TVA) collects data from the geographically distributed PMUs [15].It collects the data from the PMUs and sends the real time data to the participation companies and simultaneously archives the files. It then sends the archived files to Hadoop via secure Virtual Private Network (VPN) tunnels. This ensures reliability and resistance against failure of a single node or machine in the cluster.

2) *Distributed IDS:*

Intrusion Detection Systems (IDS) can monitor the network traffic. IDS requires rules to detect the attacks. IDS is divided in to three categories i.e. model-based, signature-based and anomaly-based IDS. In [16], the authors have proposed a signature based SNORT IDS which requires IDS rules to detect attacks against IEEE C37.118 standard. In [12], the authors have proposed distributed IDS structure to detect the malicious activities.

3) *Blockchain:*

Blockchain technology is a decentralized ecosystem for record keeping. It is used as a trust model in a wide range of applications. Blockchain technology is used as it has many advantages such as immutability, confidentiality and high safety. By using a smart contract approach based on blockchain, we can add a security to the application. Here PDCs can interact with the smart contract and based on the rules in the smart contract the blocks can be mined and added to the blockchain. In [2], the authors have mentioned blockchain trust model as a solution to mitigate the cyber-attacks.

From the above solutions proposed by different authors, we propose to use blockchain as a solution to mitigate the effects of cyber-attacks on the synchrophasor system. Hadoop provides the distributed architecture but has to make use of VPN tunnels to send the archived files. Use of VPN in synchrophasor networks [5] has limitations like being vulnerable to attacks as mentioned in Table II. Distributed IDS provides protection against stealthy cyber-attacks but the IDS requires a set of rules to continuously learn and analyze the system behavior. Blockchain technology provides confidentiality, decentralized architecture, information security and privacy in the smart grids [17].

III. Role of Blockchain in Smart Grids

Smart grid uses various technologies to automate decisions and responses. This automation in decisions and responses requires an added layer of security. In the above background work we discussed different solutions that add a layer of security in the smart grids. In [18], the authors have discussed the use of blockchain and trust management systems. Blockchain technology helps mitigate attacks like Man-In-The-Middle (MITM) attack and Denial of Service (DoS) attack.

Blockchain technology provides solutions for both the major drawbacks mentioned in Section I of this paper. The major drawbacks of the PMU-PDC communication architecture:

- IEEE C37.118 standard lacks encryption. Hence the confidentiality of the data is affected.
- PMU-PDC communication architecture in centralized in nature.

Blockchain provides confidentiality of data and gives decentralized communication architecture [19]. Blockchain technology is secure by design [20] and helps achieve the security objectives i.e. confidentiality, integrity and availability for synchrophasor networks. Blockchain technology by default provides features like data privacy, data integrity, authentication and authorization. Hence blockchain can be used as a solution in the synchrophasor networks of the smart grids.

IV. Validation of Use of Blockchain For Secure Synchrophasor Communication

The blockchain is built on a peer to peer network. Therefore to use blockchain technology and to include its advantages in a synchrophasor network we require decentralized communication architecture for synchrophasor network as shown in Fig. 2.

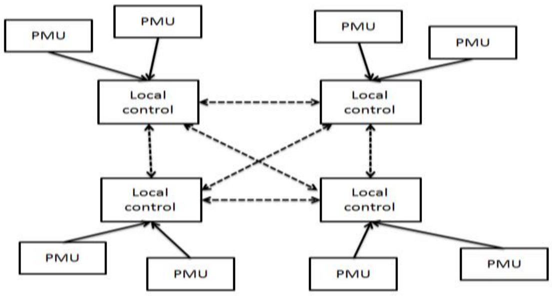

Fig. 2. Decentralized architecture [9].

In this section we validate the use of blockchain for secure synchrophasor communication. In [21], the authors have used blockchain technology to preserve users' privacy in the smart grid and aggregate real-time data in a decentralized manner. Similarly we can use blockchain technology to preserve data privacy in the synchrophasor network as shown in Fig 3.

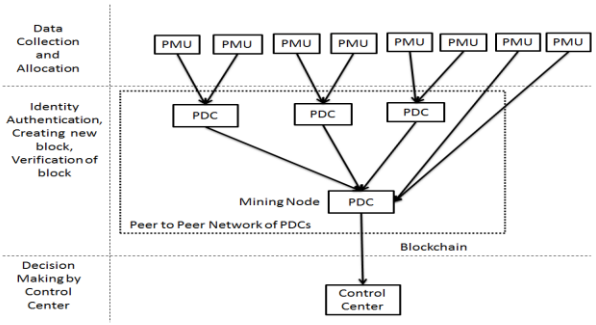
Data Collection and Allocation
Identity Authentication, Creating new block, Verification of block
Decision Making by Control Center
PMU
PMU
PMU
PMU
PMU
PMU
PMU
PMU
PDC
PDC
PDC
Mining Node
PDC
Peer to Peer Network of PDCs
Blockchain
Control Center

Fig. 3. Blockchain Integration with Synchrophasor Network

The data is collected and published by multiple PMUs to the PDC in a local substation [22]. A PDC is not a standalone device or a software package. It is a function which can be integrated with a system. The PDC time synchronizes the data and creates a set of the time synchronized correlated synchrophasor data. This is then sent to higher level PDCs or to the further applications. Local PDCs will time align the measurement data and sends it to the data applications. Super PDCs will perform data aggregation and archive the data files in a database.

The functions of PDC include data quality checks, flags check for correlated data, check for disturbance flags and recording of data files for analysis purpose. The output stream is given to the control center (SCADA or EMS system).

A PDC can perform data quality checks and monitor the measurement data received from PMUs. The measurement data includes phasors, frequency, time and PMU ID. The decision making unit of PDC can decide whether these parameters are in the specified range. The mining node mines these action taking events in the synchrophasor network. The block is then recorded and verified by the other nodes. After successful verification this block can be added to the blockchain. We can also maintain a hierarchical blockchain to add another layer of security. Local PDCs may maintain an individual blockchain. It will be a distributed ledger of data from PMUs. Super PDCs may maintain a global blockchain. It will be a distributed ledger of data from local PDCs.

V. Conclusion

Cyber Security is of vital importance and plays a major role in critical infrastructures like smart grid. Any attack on the security of the smart grid could lead to huge consequences. These consequences include blackout, failure of devices in the network or delay in power delivery.

This paper highlights the synchrophasor part of the smart grid system and discusses solutions to add a security layer. We preferred blockchain as a solution due to its advantages over the others. Hence blockchain integration with the synchrophasor network of the smart grid proves highly advantageous by adding security features like data privacy and decentralized communication architecture.

References

[1] Synchrophasor Networks for Grid monitoring https://www.nist.gov/programs-projects/synchrophasor-networks-grid-monitoring

[2] Sundararajan, Aditya, K. H. A. N. Tanwir, Amir Moghadasi, and Arif I. Sarwat. "Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies." Journal of Modern Power Systems and Clean Energy (2018): 1-19.

[3] Kumar, Surender, M. K. Soni, and D. K. Jain. "Cyber security threats in synchrophasor system in wide area monitoring system." Int J Comput Appl 115, no. 8 (2015): 17-22.

[4] Stewart, John, Thomas Maufer, Rhett Smith, Chris Anderson, and Eren Ersonmez. "Synchrophasor security practices." In 14th Annual Georgia Tech Fault and Disturbance Analysis Conference. 2011.

[5] Khan, Rafiullah, Kieran McLaughlin, David Laverty, and Sakir Sezer. "Analysis of IEEE C37. 118 and IEC 61850-90-5 synchrophasor communication frameworks." In 2016 IEEE Power and Energy Society General Meeting (PESGM), pp. 1-5. IEEE, 2016.

[6] Beasley, Christopher, Xingsi Zhong, Juan Deng, Richard Brooks, and Ganesh Kumar Venayagamoorthy. "A survey of electric power synchrophasor network cyber security." In IEEE PES Innovative Smart Grid Technologies, Europe, pp. 1-5. IEEE, 2014.

[7] Ashok, Aditya, Adam Hahn, and Manimaran Govindarasu. "Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment." Journal of advanced research 5, no. 4 (2014): 481-489.

[8] Basumallik, Sagnik, Sara Eftekharnejad, Nathan Davis, Nagarjuna Nuthalapati, and Brian K. Johnson. "Cyber security considerations on PMU-based state estimation." In Proceedings of the Fifth Cybersecurity Symposium, p. 14. ACM, 2018.

[9] Appasani, Bhargav, and Dusmanta Kumar Mohanta. "A review on synchrophasor communication system: communication technologies, standards and applications." Protection and Control of Modern Power Systems 3, no. 1 (2018): 37.

[10] Xin, Yufeng, and Aranya Chakrabortty. "A study on group communication in distributed wide-area measurement system networks in large power systems." In 2013 IEEE Global Conference on Signal and Information Processing, pp. 543-546. IEEE, 2013.

[11] M. Golshani, G. A. Taylor, I. Pisica and P. Ashton, "Laboratory-based deployment and investigation of PMU and openPDC capabilities," 10th IET International Conference on AC and DC Power Transmission (ACDC 2012), Birmingham, 2012, pp. 1-6.

[12] Khan, Rafiullah, Kieran McLaughlin, John Hastings David Laverty, Hastings David, and Sakir Sezer. "Demonstrating Cyber-Physical Attacks and Defense for Synchrophasor Technology in Smart Grid." In 2018 16th Annual Conference on Privacy, Security and Trust (PST), pp. 1-10. IEEE, 2018.

[13] Petterson Josh, "Hadoop as the Platform for the Smartgrid at TVA" at http://www.slideshare.net/cloudera/hadoop-as-the-platform-for-thesmartgrid-at-tva

[14] Edwards, Matthew, Aseem Rambani, Yifeng Zhu, and Mohamad Musavi. "Design of hadoop-based framework for analytics of large synchrophasor datasets." Procedia Computer Science 12 (2012): 254-258.

[15] The Smart Grid: Hadoop at the Tennessee Valley Authority (TVA) https://blog.cloudera.com/blog/2009/06/smart-grid-hadoop-tennessee-valley-authority-tva/

[16] Sprabery, Read, Thomas H. Morris, Shengyi Pan, Uttam Adhikari, and Vahid Madani. "Protocol mutation intrusion detection for synchrophasor communications." In Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, p. 41. ACM, 2013.

[17] Li, Shuling. "Application of Blockchain Technology in Smart City Infrastructure." In 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), pp. 276-2766. IEEE, 2018.

[18] Alexopoulos, Nikolaos, Jörg Daubert, Max Mühlhäuser, and Sheikh Mahbub Habib. "Beyond the hype: On using blockchains in trust management for authentication." In 2017 IEEE Trustcom/BigDataSE/ICESS, pp. 546-553. IEEE, 2017.

[19] Ali, Muhammad Salek, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. "Applications of Blockchains in the Internet of Things: A Comprehensive Survey." IEEE Communications Surveys & Tutorials (2018).

[20] Panarello, Alfonso, Nachiket Tapas, Giovanni Merlino, Francesco Longo, and Antonio Puliafito. "Blockchain and IoT integration: A systematic survey." Sensors 18, no. 8 (2018): 2575.

[21] Guan, Zhitao, Guanlin Si, Xiaosong Zhang, Longfei Wu, Nadra Guizani, Xiaojiang Du, and Yinglong Ma. "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities." IEEE Communications Magazine 56, no. 7 (2018): 82-88.

[22] IEEE Standards Association. "IEEE Standard for Synchrophasor Data Transfer for Power Systems." IEEE Std C 37.