Turkish Journal of Computer and Mathematics Education
DOI: https://doi.org/10.17762/turcomat.v9i3.13890 *Vol.09 No.03 (2018), 1025- 1031*

Research Article

Cyber-Physical System Analysis of Communication Networks Utilising Synchrophasors in a Smart Grid

Amit Gupta

Asst. Professor, Department of CSE (Computer sc),

GEHU-Dehradun Campus

Abstract: The electrical grid is often hailed as one of the 20th century's greatest technical achievements. While it is undeniably a feat of engineering, it is in dire need of updating to keep up with things like two-way dynamic energy management, load balancing, enhanced metering, the incorporation of renewable energy sources, protection and control, etc. The term "Smart Grid" (SG) is used to describe this updated electrical network. Rapid progress in communication technology has made it possible to create the envisioned SG. The SG may be seen as a Cyber Physical System (CPS), with the physical system being the infrastructure of the power grid and the cyber system being the communication and computing technologies, sensors, actuators, etc. A Smart Grid Cyber Physical System (SGCPS) is a CPS-based conceptualization of an SG. CPS technology is expanding rapidly, which has allowed the SG's capabilities to grow even further. In SGCPS in particular, the SG's security and management are tweaked to improve consistency of functioning. With synchrophasor measurement, SG has gained traction from a safety and regulation perspective. The sinusoidal voltage and current of electrical buses in the smart grid may be measured using a time-synchronized phasor measurement called synchrophasor measurement. High-speed sensors, known as Phasor Measurement Units (PMUs), collect the synchrophasor information. The Phasor Data Concentrator (PDC) at the command centre receives the synchrophasor information. Synchrophasor data is sent from PMUs to PDCs through a communication network known as the Synchrophasor Communication Network (SCN), which serves as the backbone of the synchrophasor applications.

Keywords: Phasor Data Concentrator (PDC), Synchrophasor Communication Network (SCN), Smart Grid (SG), a Smart Grid Cyber Physical System (SGCPS).

Introduction

The transformation of the traditional electrical grid into the Smart Grid (SG) is being heralded as a feat of engineering [1]. Renewable energy's integration into the grid, together with the necessity for sophisticated metering infrastructure, real-time load balancing, real-time grid protection and control, etc., has necessitated change. The widespread use of Cyber Physical System (CPS) technology, known as the Smart Grid Cyber Physical System (SGCPS), has increased the SG's efficiency in light of recent developments in ICT. Enhancing the SGCPS's real-time protection and control relies in large part on the Synchrophasor Measurement System (SMS).

Multiple high-speed sensors, or Phasor Measurement Units (PMUs), and data concentrators, or Phasor Data Concentrators (PDCs), exchange synchrophasor data about the health of the grid. SMS relies on a communication system, the Synchrophasor Communication Network (SCN), to function. The PDC in the control centre receives synchrophasor data on the health of the grid from a PMU mounted on an electrical bus in the grid. This study begins to fill that gap by analysing and designing the SCN for optimal monitoring and regulation. The SCN of the SGCPS is a very sophisticated network with several moving parts. Normal operation exposes these parts to wear and tear, as well as additional hazards including natural disasters and man-made disasters, all of which may cause failure. Real-time monitoring and control capabilities of the SMS may be compromised if a failure in any one component causes failure in other dependent components, and so on. Because of this, it's important to correctly construct the SCN in order to evaluate its efficiency. Synchrophasor data is sent in packet form between PMUs and PDCs through the SCN. Monitoring and security of the SGCPS rely heavily on packets being sent and received without incident and in a timely manner. Successful and timely packet transport relies heavily on SCN topologies. As a result, it's crucial to investigate how data transmission and latency affect the performance of various SCN topologies. Accordingly, many SCN topologies have been suggested, the performance of which is measured with respect to two primary metrics: the Packet Delivery Ratio (PDR) and the Average End-to-End Delay (AE2ED).

Successful packet delivery from source to destination and overall latency experienced by the SCN during transmission are measured by the PDR and AE2ED. In addition, PDR is used to characterise the SCN's data reliability in the same way as failure probability characterises the hardware dependability. The SCN spans a large region and is vulnerable to a number of threats that might cause the SGCPS to deviate from its intended functionality. The potential outcomes of risk must be predicted, however, and a strategic aversion solution must be created. The SCN is especially at danger because to flaws in both its technology and its data. Therefore, the risks connected with the SCN must be reduced by the implementation of a suitable risk assessment system. Because of this, a risk assessment paradigm has been suggested to examine SCN efficiency from a risk perspective. The suggested architecture for SCN takes into account both hardware dependability and data reliability as availability measures.

Transformation from conventional power grid to smart grid

Despite Benjamin Franklin's creation of electricity in 1752, the power grid didn't come into existence until 1890 thanks to the effective transmission of electricity over long distances and the linking of several generating and distribution units. One of the greatest and most difficult technical achievements is the electrical grid. The electricity system, often hailed as one of the century's greatest innovations, has struggled to keep up with the demands of the twenty-first century. In particular, modern demands for renewable energy integration, enhanced metering, dynamic pricing, real-time load balancing, real-time grid protection and management, etc., were beyond the capabilities of the traditional power grid.

Through the use of pervasive communication and networking technologies, the smart grid enhances the intelligence of the traditional power grid to provide more productive, cost-effective, and open services. The old electrical grid has been replaced with a consumer-interactive distributed network thanks to the smart grid. SG has a number of benefits, including [4]:

• High reliability

• Integration of renewable energy sources such as biomass, geothermal, solar, geothermal, wind, ocean thermal, tidal and wave to the existing power grid

• Enhancing affordability

• Encouraging carbon footprint reduction

• Improving efficiency

• Real time monitoring and control.

A Smart Grid from the Perspective of Cyber Physical System

The goal of integrating CPS technology into the smart grid is to take full use of its many benefits [13]. The acronym "SGCPS" refers to this kind of smart grid that uses CPS technology. Power grid infrastructure is the physical world of the SGCPS, while information, computing, and communication technologies make up the cyber world of the SGCPS [14]. As seen in Figure 1, this is a typical SGCPS. Generation, transmission, distribution, consumer, service provider, operation, and market are only some of the seven domains that make up the smart grid, as described by the National Institute of Standards and Technology (NIST) [15]. There are several parts of the electricity system that fall under these categories. Here are some instances of physical components from different domains to illustrate the SG as described in [15]. Substations, distributed storage, distributed generation, etc. are all part of the transmission domain; advanced metering infrastructure, utility metres, etc. are all part of the distribution domain; and the customer domain includes the physical components associated with various power platforms such as coal, nuclear, hydro, wind, solar, geothermal, etc. Cyber components of the SGCPS include service providers, operations, and market domains rather than physical components such as power network infrastructure. In particular, electricity is tracked as it moves from power plants to the grid through distribution centres and finally to individual consumers. For the SGCPS to be efficient, effective, and dependable, however, CPS technologies must be integrated with the service provider, operation, and market domains.

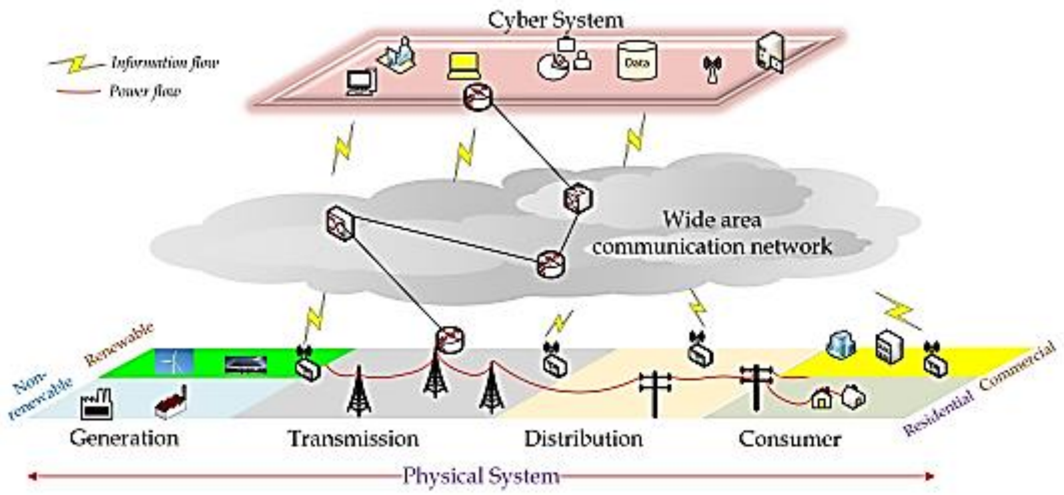

Figure 1: An overview of SGCPS

Synchrophasor communication network

PMUs are placed at various electrical buses in a synchrophasor application, measuring line voltages and currents in a time-synchronized phasor [12]. Several applications rely on time-synchronized phasor measurements, known as synchrophasor data [13]. These applications include those for fault detection, state estimation, energy management, grid automation, monitoring, protection, and control. For synchrophasor applications, it is also necessary for data to be sent from PMUs to PDCs in the control centre. Due to their physical separation, PDCs and PMUs must rely on the communication network to share information with one another. Synchrophasor data sharing between PMUs and PDCs requires a special kind of communication network called a Synchrophasor Communication Network (SCN). Figure 2 depicts an example of an IEEE definition–compliant synchrophasor communication network. Within a substation, there are several PMUs that provide information to the regional PDC via LAN. Several substations are linked to the command centre through a wide area communication network. In the command centre, a regional PDC collects synchrophasor data from several local PDCs, each of which is associated with a different substation. Multiple synchrophasor applications make use of PDC's collected data. The data collected by the PMUs may be sent directly to the regional PDC at the control centre, bypassing the need for a local PDC at the substation. However, this would result in higher communication overhead and latency than if the data were sent in a single stream (local PDC produces stream of data from several PMUs).

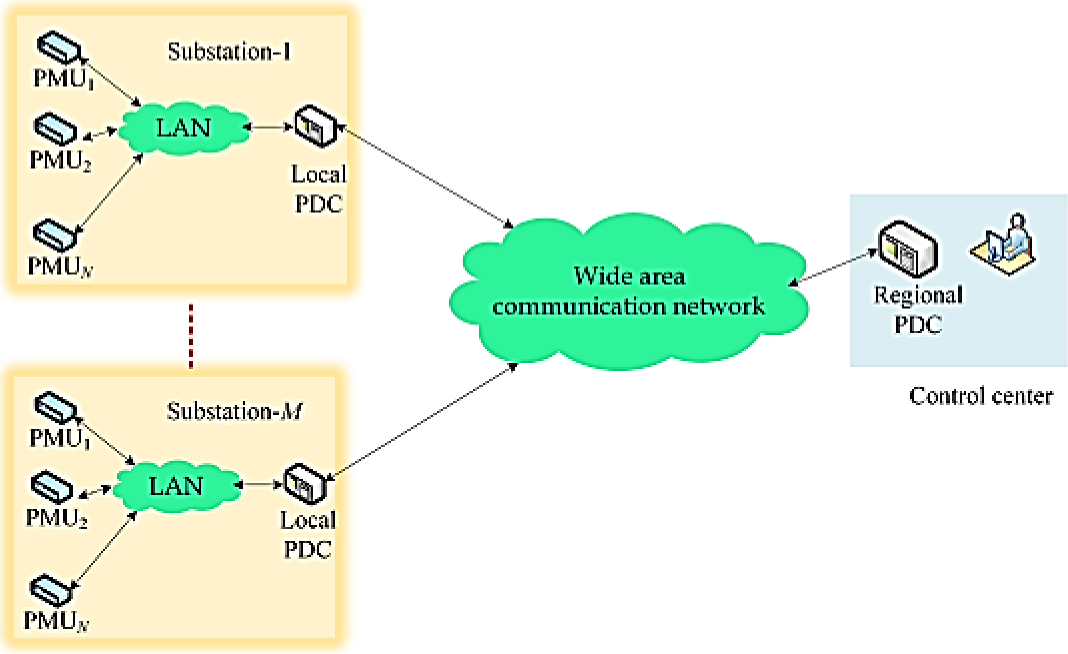

Figure 2: A generic synchrophasor communication network.

Review on Synchrophasor Applications of the SGCPS

The SGCPS is an impressive feat of engineering that integrates many different aspects of the conventional power grid, including generation, transmission, distribution, customers, and more. Their mutual reliance on information and communication technologies just adds layers of complication. Real-time monitoring is crucial to safeguarding the SGCPS against significant eventualities in light of its increasing complexity. Several unforeseen events have caused widespread power failures and blackouts in the past. In light of several cascading power failures over the last two decades, the United States Department of Energy launched the North American Synchrophasor Initiative (NASPI) with a wide range of interested parties to conduct synchrophasor measurements. With the goal of preventing any unforeseen events in the SGCPS, the different power system characteristics, including voltage, current, and frequency, are constantly monitored in real-time. The term "synchrophasor application" is often used to refer to the many possible uses for synchrophasor measurements. There are three basic types of synchrophasor uses: control applications based on responses, grid operations in real time, and system planning and analysis. Transmission and distribution domains of the SGCPS are covered in Usman et al.'s [23] most thorough examination of synchrophasor technology from a variety of perspectives, including applications, designs, and optimum placement techniques. The allocation domain of the SGCPS has been highlighted in this state-of-the-art review of synchrophasor uses of PMU in a WAMS. Wache et al. [18] emphasise the importance of synchrophasor applications in the distribution domain of SGCPS, which includes renewable energy sources in the generating domain. Solutions based on synchrophasor measurements have been presented for the challenges of real-time monitoring and control in the current power grid, which is highly linked.

Comparative analysis of different SCNs in terms of RMuDR for 150 Kbps synchrophasor data rate

Table 1 displays the results of simulations run on various SCNs using a synchrophasor data rate of 150 kbps. When compared to shared and hybrid SCNs, dedicated SCN excels in simulation outcomes.

Table 1: RMuDR comparison findings from simulations using a synchrophasor data rate of 150 Kbps

PMU	$\tilde{R}_{DS_{l-1}}$	$\tilde{R}_{SS_{l-1}}$	$\tilde{R}_{HS_{l-1}}$
PMU_1	0.0502	2.4549	4.2023
PMU_2	0.0376	1.7691	2.7156
PMU_3	0.0189	1.8335	3.2325
PMU_4	0.1689	2.3829	3.1741
PMU_5	0.0189	1.9037	3.1824
PMU_6	0.0918	2.4097	4.3404
PMU_7	0.2918	3.3955	4.4151
$\tilde{R}^{mean}_{DeSCN} = 0.0969$		$\tilde{R}^{mean}_{ShSCN} = 2.3070$	$\tilde{R}^{mean}_{HySCN} = 3.6089$
$\tilde{R}^{min}_{DeSCN} = 0.0189$		$\tilde{R}^{min}_{ShSCN} = 1.7691$	$\tilde{R}^{min}_{HySCN} = 2.7156$
$\tilde{R}^{max}_{DeSCN} = 0.2918$		$\tilde{R}^{max}_{ShSCN} = 3.3955$	$\tilde{R}^{max}_{HySCN} = 4.4151$

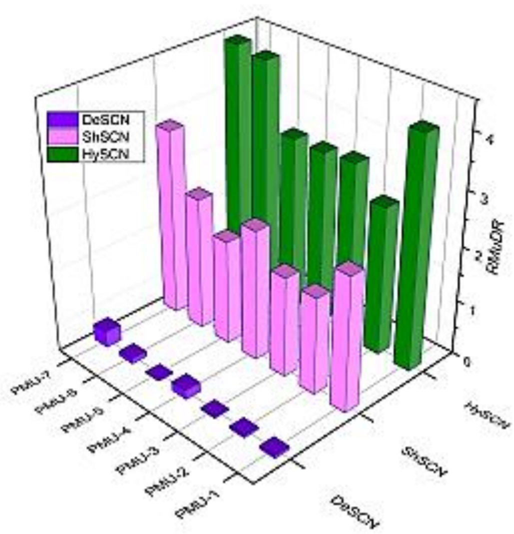

Figure 3: Comparative study of different SCNs with 150 Kbps synchrophasor data rate.

When considering a synchrophasor data rate of 150 Kbps, Figure 3 indicates that dedicated SCN performs better than shared and hybrid SCNs for all PMUs. In contrast, a comparison of the RMuDR performance of a shared SCN and a hybrid SCN shows that they are quite close. And among all SCNs, PMU7 is the one with the highest risk. In contrast, PMU2 in shared and hybrid SCN and PMU5 in dedicated SCN are more resilient to disruptions due to the reduced risk they face.

Conclusion

The data in synchrophasor communication networks is just as crucial to their dependability as the hardware components. The consistency of synchrophasor communication networks is severely impacted by packet losses. Packet losses are influenced by the design of the communication network and the amount of noise in the system. Since packet losses in the dedicated synchrophasor communication network are negligible, the network's dependability is mostly dependent on the availability of its hardware components. However, missed packets owing to background traffic severely impact the dependability of shared systems. Different synchrophasor communication network designs were analysed using established reliability models for both hardware and data. The results show that even with 80% background traffic, shared and hybrid synchrophasor communication networks continue to function successfully. However, when these networks are exposed to more than 90% background traffic, their performance decreases. In spite of the lower cost of using a shared network compared to a dedicated one, achieving highly dependable performance for synchrophasor applications depends on making the right selection that guarantees little background traffic. Hybrid synchrophasor communication networks are desirable due to their scalability and adaptability, and their performance is on par with that of shared synchrophasor communication networks.

References

1. H. Farhangi, “The path of the smart grid”, IEEE Power and Energy Magazine, vol. 8, no. 1, pp. 18–28, 2010. DOI: 10.1109/MPE.2009.934876.
2. E. Mica R. and G. Daniel J., Eds., Situation Awareness Analysis and Measurement, 1st ed. New York: CRC Press, 2000, ISBN: 9780429228131. DOI: https: //doi.org/10.1201/b12461.
3. A. Annaswamy, “IEEE vision for smart grid control: 2030 and beyond roadmap”, IEEE Vision for Smart Grid Control: 2030 and Beyond Roadmap, pp. 1– 12, 2013. DOI: 10.1109/IEEESTD.2013.6648362.
4. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, “Cyber-physical systems: The next computing revolution”, in Design Automation Conference, 2010, pp. 731– 736. DOI: 10.1145/1837274.1837461.
5. S. K. Khaitan and J. D. McCalley, “Design techniques and applications of cyberphysical systems: A survey”, IEEE Systems Journal, vol. 9, no. 2, pp. 350– 365, 2015. DOI: 10.1109/JSYST.2014.2322503
6. N. Mohamed, J. Al-Jaroodi, and I. Jawhar, “Cyber-physical systems forensics”, in 2020 IEEE Systems Security Symposium (SSS), 2020, pp. 1–7. DOI: 10. 1109/SSS47320.2020.9174199
7. R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, “Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications”, IEEE Access, vol. 8, pp. 151 019–151 064, 2020. DOI: 10.1109/ACCESS.2020.3016826
8. G. Locke and P. D. Gallagher, “NIST Special Publication 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0”, Tech. Rep., 2010.
9. J. Zhao, F. Wen, Y. Xue, X. Li, and Z. Dong, “Cyber physical power systems: Architecture, implementation techniques and challenges”, Automation of Electric Power Systems, vol. 34, no. 16, pp. 1–7, 2010
10. Z. Q. Bo, X. N. Lin, Q. P. Wang, Y. H. Yi, and F. Q. Zhou, “Developments of power system protection and control”, Protection and Control of Modern Power Systems, vol. 1, no. 1, pp. 1–8, Dec. 2016, ISSN: 2367-2617.
11. V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, “Wide-area monitoring, protection, and control of future electric power networks”, Proceedings of the IEEE, vol. 99, no. 1, pp. 80– 93, 2011
12. J. E. Dagle, “The north american synchrophasor initiative (NASPI)”, in IEEE PES General Meeting, 2010, pp. 1–3. DOI: 10.1109/PES.2010.5590048.
13. H. Gharavi and B. Hu, “Synchrophasor sensor networks for grid communication and protection”, Proceedings of the IEEE, vol. 105, no. 7, pp. 1408–1428, 2017. DOI: 10.1109/JPROC.2017.2696881.
14. R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, “IEEE C37. 118-2 synchrophasor communication framework-overview, cyber vulnerabilities analysis and performance evaluation”, in International Conference on Information Systems Security and Privacy, SciTePress, vol. 2, 2016, pp. 167–178.
15. A. Phadke and J. Thorp, “Communication needs for wide area measurement applications”, in 2010 5th International Conference on Critical Infrastructure (CRIS), 2010, pp. 1–7. DOI: 10.1109/CRIS.2010.5617484.
16. C.-h. Yang, G. Zhabelova, C.-W. Yang, and V. Vyatkin, “Cosimulation environment for event-driven distributed controls of smart grid”, IEEE Transactions on Industrial Informatics, vol. 9, no. 3, pp. 1423–1435, 2013
17. M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, “A survey on smart grid cyber-physical system testbeds”, IEEE Communications Surveys Tutorials, vol. 19, no. 1, pp. 446–464, 201

18. X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective", Proceedings of the IEEE, vol. 104, no. 5, pp. 1058–1070, 2016. DOI: 10.1109/JPROC. 2015.2503119.
19. P. Palensky, E. Widl, and A. Elsheikh, "Simulating cyber-physical energy systems: Challenges, tools and methods", IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 3, pp. 318–326, 2014. DOI: 10.1109/TSMCC. 2013.2265739
20. M. U. Tariq, B. P. Swenson, A. P. Narasimhan, S. Grijalva, G. F. Riley, and M. Wolf, "Cyber-physical co-simulation of smart grid applications using NS-3", in Proceedings of the 2014 Workshop on Ns-3, ser. WNS3 '14, Atlanta, Georgia, USA: Association for Computing Machinery, 2014, ISBN: 9781450330039. DOI: 10.1145/2630777.2630785.
21. E. Hossain, E. Kabalci, R. Bayindir, and R. Perez, "Microgrid testbeds around the world: State of art", Energy Conversion and Management, vol. 86, pp. 132– 153, 2014, ISSN: 0196-8904. DOI: https://doi.org/10.1016/j.enconman. 2014.05.012
22. K. V. Katsaros, B. Yang, W. K. Chai, and G. Pavlou, "Low latency communication infrastructure for synchrophasor applications in distribution networks", in 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2014, pp. 392–397. DOI: 10.1109/SmartGridComm.2014.7007678
23. R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid", in 4th International Symposium for ICS & SCADA Cyber Security Research 2016 4, 2016, pp. 53–63
24. H. Jiang, X. Dai, D. W. Gao, J. J. Zhang, Y. Zhang, and E. Muljadi, "Spatialtemporal synchrophasor data characterization and analytics in smart grid fault detection, identification, and impact causal analysis", IEEE Transactions on Smart Grid, vol. 7, no. 5, pp. 2525–2536, 2016
25. D. Zhou, J. Guo, Y. Zhang, J. Chai, H. Liu, Y. Liu, C. Huang, X. Gui, and Y. Liu, "Distributed data analytics platform for wide-area synchrophasor measurement systems", IEEE Transactions on Smart Grid, vol. 7, no. 5, pp. 2397–2405, 2016. DOI: 10.1109/TSG.2016.2528895