sustainability

MDPI

Article

Analytical Design of Synchrophasor Communication Networks with Resiliency Analysis Framework for Smart Grid

Amitkumar V. Jha [1,*], Bhargav Appasani [1], Deepak Kumar Gupta [2] and Taha Selim Ustun [3,*]

[1] School of Electronics Engineering, Kalinga Institute of Industrial Technology (KIIT), Deemed to be University, Bhubaneswar 751024, India
[2] School of Electrical Engineering, Kalinga Institute of Industrial Technology (KIIT), Deemed to be University, Bhubaneswar 751024, India
[3] Fukushima Renewable Energy Institute, AIST (FREA), Koriyama 963-0298, Japan
* Correspondence: amit.jhafet@kiit.ac.in (A.V.J.); selim.ustun@aist.go.jp (T.S.U.)

Abstract: The advent of synchrophasor technology has completely revolutionized the modern smart grid, enabling futuristic wide-area monitoring protection and control. The Synchrophasor Communication Network (SCN) is a backbone that supports communication of synchrophasor data among Phasor Measurement Units (PMUs) and Phasor Data Concentrators (PDCs). The operator at the control center can visualize the health of the smart grid using synchrophasor data aggregated at PDCs from several PMUs. Since the core of the SCN is the existing IP network as an underlying communication infrastructure, the synchrophasor data is subjected to attacks that can compromise its security. The attacks, such as denial-of-service (DoS), can result in degradation of performance and even can disrupt the entire operation of the smart grid, if not controlled. Thus, a resilient SCN is a pertinent requirement in which the system continues to operate with accepted levels of performance even in response to the DoS. This article endeavors to propose a comprehensive resiliency framework for the SCN with enhanced resiliency metrics based on hardware reliability and data reliability. The proposed framework is deployed for a SCN pertaining to a practical power grid in India for its resiliency analysis. The proposed work can be regarded as a significant contribution to smart grid technology, as it provides a framework for resiliency analysis covering different aspects such as hardware reliability, data reliability, and parameters validation using the QualNet network simulator. Nevertheless, an analytical design of the hybrid SCN proposed in this work can even be extended to other topological designs of SCN.

Keywords: smart grid; cyber physical system; resiliency; reliability; synchrophasor communication network; synchrophasor technology; QualNet network simulator

Citation: Jha, A.V.; Appasani, B.; Gupta, D.K.; Ustun, T.S. Analytical Design of Synchrophasor Communication Networks with Resiliency Analysis Framework for Smart Grid. *Sustainability* **2022**, *14*, 15450. https://doi.org/10.3390/su142215450

Academic Editor: Tomonobu Senjyu

Received: 11 October 2022
Accepted: 14 November 2022
Published: 21 November 2022

1. Introduction

It is expected that energy requirements will soar to 82% by end of 2030 as per the report from International Energy Outlook [1]. In order to cope with the ever-growing demands of electricity, it will be necessary to incorporate non-conventional sources such as solar, wind, etc., into the mainstream of electricity generation. Further, the flow of electricity in the power system must be bidirectional. The burgeoning information and communication technologies must be incorporated into the existing power system to effectively monitor, control, and protect the power system. Nevertheless, high penetration of information and communication technologies are required across all domains of the power system including generation, transmission, distribution, and consumer domains. To achieve these objectives, the existing power grid is modernized as the Smart Grid (SG) [2].

Several power outages have been observed in the last few years. Out of several power outages, some major outages are those in Canada and U.S in 2003, Brazil and Paraguay in 2009, India in 2012, Bangladesh in 2014, Pakistan in 2015, Indonesia in 2019, etc. [3]. The systematic analysis of these outages revealed the need for the implementation of a

Wide Area Monitoring System (WAMS) to achieve real-time protection and control of the SG. However, the existing Supervisory Control and Data Acquisition (SCADA) was not feasible due to its low resolution, which cannot capture the real-time dynamics of the SG. Further, SCADA is not even capable of providing synchronized measurements of system parameters. The unsynchronized measurements from SCADA suffer from communication latency, resulting in inaccurate reports on the health of the SG in real-time. Therefore, the North American Synchrophasor Initiative (NASPI) was initiated with the objective to enhance power system visibility by incorporating synchrophasor technology in WAMS [4].

The synchrophasor technology uses high-speed sensors known as Phasor Measurement Unit (PMU) which are capable of measuring vital system parameters such as voltage, currents, frequency, and rate of change of frequency in real time [5]. Further, these measurements are measured at a very high rate and in a synchronized manner. The synchronized measurements are communicated to the Phasor Data Concentrator (PDC) which acts as an aggregator. The PDC is responsible for processing, storage, and handling of synchrophasor data. The operator can use the synchrophasor data from PMUs to visualize the SG in real-time. The communication systems involved in facilitating synchrophasor data communication between PMUs and PDCs are referred to as the Synchrophasor Communication Network (SCN) [6]. In nutshell, the complete system behavior can be captured in real-time using synchrophasor technology by which PMUs communicate synchrophasor data to PDC over SCN.

Due to the amalgamation of various components, computational technologies, information and communication technologies, etc., a significant impact on the reliability of the power system is observed from its cyber physical aspects [7]. Since the SCN uses an existing IP network as its core communication infrastructure, the synchrophasor data is susceptible to security attacks. The attacks on a particular PMU will result in the loss of the corresponding synchrophasor data or even pose a data integrity risk. This disrupts the normal operation of the SCN, resulting in degradation in its performance. Thus, a SCN must be resilient in order to restore itself to normal operation and improve its performance in response to the attacks. The panoramic survey of different threats and attacks for Internet-based systems is presented in [8] where authors presented a taxonomy of threats and attacks with possible mitigation strategies.

The growth of a country and its economy largely depends on electricity. The uninterrupted availability of electricity requires reliable and resilient SCN which entails enhancing the monitoring and controlling capability of the SG using synchrophasor applications. The lesson learned from blackouts that have occurred in the past has necessitated enhancing the resiliency of the SCN. A resilient SCN has the potential to avoid huge economic losses, which can be justified by the *cost-effect* analysis of some of the major outages such as Pacific Southwest in 2011, Brazil in 2011, India in 2012, Vietnam in 2013, Thailand in 2013, Bangladesh in 2014, Pakistan in 2015, Turkey in 2016, Kenya in 2016, etc. which are comprehensively discussed in [3]. All these power outages have catastrophically affected the human life and economy of the countries and as a result, resiliency is given enormous attention thereafter. The most common definition of resiliency in the literature is the ability of the system to respond, adapt, and absorb unwanted extreme events so as to continue its intended operations.

To comprehensively summarize the organization of the article, the rest of the article is planned as follows: In Section 2, related work is briefly reviewed based on which the motivation of the present work is extracted. The systemic analytical modeling, parameterization, and design of hybrid SCN are presented in Section 3. In Section 4, a comprehensive resiliency analysis framework is presented which is extended for resiliency analysis of the designed hybrid SCN in Section 5, where resiliency metrics are obtained. The hybrid SCN pertaining to a practical power grid of India is considered for which resiliency analysis is performed in Section 6 with extensive simulation results and discussions. Lastly, the conclusion of the present work is included in Section 7.

2. Related Work and Motivation

2.1. Related Work

The SCN has been discussed sufficiently in literature such as [8–12] to list a few. However, none of these articles have discussed SCN from the perspective of resiliency analysis. For example, V. Katsaros et al. in [9] studied the impact of delay and approaches to minimize it in the implementation of synchrophasor applications. Appasani et al. in [10] considered the synchrophasor communication system from different perspectives and proposed a communication infrastructure for situational awareness enhancement. Whereas a comprehensive situational awareness framework for the SCN in the context of SG cyber physical system is proposed in [11]. Cybersecurity aspects of these messages and related attacks are discussed in [12,13]. However, the resiliency perspective of the SCN is not covered in these articles, even though some insights on mathematical modeling were presented.

In literature, resiliency is defined differently in various contexts since its first occurrence in ecology in 1973 [14]. But, in general, resiliency can be defined as the ability of the system to respond, adapt, or absorb unwanted extreme events, and to restore back to the original functional state from the partially or fully failed state [15]. Without loss of generality (W.L.O.G), it is emphasized that resiliency is a function of both time and operating environment. Hosseini et al. in [16] presented a review of definitions and measures of resiliency for a system.

Jena et al. in [17] considered the market domain of SG for estimating its resiliency. Particularly, the authors here used optimal sensor placement techniques for the SG communication network to analyze the network resiliency. The seminal work by Venkataramanan et al. in [18] considered the transmission domains of the SG for which the resiliency analysis framework is proposed. With respect to the distribution domain, a novel and resilient scheduling model for the microgrid has been analyzed by G. Liu et al. in [19]. In this study, the authors considered the scheduling in microgrids where the resiliency is guaranteed. Bedoya et al. in [20] considered resiliency analysis of the distribution domain where a reinforcement learning model of distribution system using artificial intelligence has been proposed with validation using the IEEE 13-bus system. Borghei et al. in [21] proved that the resiliency of the smart grid distribution network can be enhanced with an optimal placement strategy of the microgrid distribution network.

The resiliency analysis of the communication infrastructure of the SG has been performed by AlMajali et al. in [22] in which authors have modelled a cyber-attack to validate the proposed resiliency analysis framework. Under contingencies and cyber-attacks, the resiliency analysis of SG is performed by integrating the software-defined networking (SDN) platform to the SG by Jakaria et al. in [23]. The resiliency analysis of SG based on topological characteristics is proposed by Al Mtawa et al. in [24] where authors have considered the IEEE 14-bus system as a case study. For a microgrid system, the resiliency analysis using the attack-restore method has been presented by Ibrahim et al. in [25]. Saad et al. in [26] have placed the emphasis on the cyber aspects of the SG cyber physical system, and discussed the scope of the Internet of Things (IoT) in enhancing the resiliency of the microgrid under cyber-attacks. Several authors have considered cyber attacks and resiliency in parallel to each other for analysis of the SG. Another resiliency assessment model for SG systems under cyber-attack has been considered by Tabar et al. in [27]. However, in this study, its authors have evaluated the resiliency as counter to the false data injection threats to the communication network of multi-area microgrids. The resiliency estimation of WAMS is considered in [28] where the Monte-Carlo based simulations are used which do not exclusively involve analysis of the SCN. In [29], the SCN is considered for resiliency analysis; the authors commented on the sufficient scope for resiliency metric improvement and performance enhancement of the SCNs.

Khalkho et al. in [30] have considered the SCN pertaining to the IEEE 39-bus system for which resiliency analysis methodology has been discussed with an objective of operational enhancement. From the perspective of cybersecurity, the resiliency of SG using emerging

technologies such as artificial intelligence has been discussed by Iftimie et al. in [31]. A deep-learning based model is proposed by Khediri et al.in [32] to enhance resiliency of the SG. Singh et al. in [33] proposed a resiliency framework for a PMU network capable of detecting an intrusion in order to develop a potential mitigation strategy.

2.2. Motivation

The systematic literature review reveals that the SCN has been sparsely explored in the past from the resiliency perspective. In fact, though, the enormous contribution on resiliency under different contexts can be utilized for resiliency analysis of the SCN. Further, even the resiliency analysis of the SG is also explored to a small extent. Thus, this paper is motivated to bridge such gaps in the literature by presenting a resiliency analysis framework for SCN in the SG. The proposed framework can be utilized for resiliency analysis of the SG from various other perspectives. To summarize, the present work is motivated to fill a gap in terms of resiliency framework of SCN which exists in the literature.

2.3. Contribution

The proposed work envisages a contribution in the literature in the SG paradigm for resiliency analysis of the SCN. The vital contributions of the present work are as follows:

- The proposed work presents a mathematical modelling of the SCN pertaining to the SG.
- The design perspective of a SCN is presented spanning communication infrastructures, communication protocols, and communication technologies.
- A resiliency analysis framework, including resiliency estimation metrics, is proposed. The resiliency framework is based on both key parameters: hardware reliability and data reliability, ensuring a wide perspective of disturbances for resiliency analysis.
- The proposed resiliency framework is validated for resiliency analysis of a SCN pertaining a practical power grid of India, (West Bengal State) as a case study.

3. System Model and Parametrization

3.1. System Modelling

We consider a SCN system with θ number of PMUs and ϕ number of PDCs. The SCN system is designed for a SG with K number of electrical buses. The PMU installed over an electrical bus is capable of monitoring more than one of the buses simultaneously as the PMUs are optimally placed over the electrical buses. Due to optimally placed PMUs, a smaller number of PMUs are required to monitor all of the buses of the grid, which leads to $\theta < K$, and $\theta = \kappa$, where κ is the number of buses with at least one PMU. Further, since a PDC acts as an aggregator for more than one PMUs, it is obvious that the relation $\phi < \theta$ holds true. As a result, in the SCN system with optimally placed PMUs and PDCs, the following inequality holds true: $\phi < \theta; \theta \leq K;\ \theta = \kappa$.

If we denote collection of all PMUs by a set A = $\{\mathrm{PMU}_1, \mathrm{PMU}_2 \ldots, \mathrm{PMU}_\theta\}$ and PDCs by a set B = $\{\mathrm{PDC}_1, \mathrm{PDC}_2 \ldots, \mathrm{PDC}_\phi\}$, then sets A and B are finite sets with cardinality of $|\mathrm{A}| = \theta$ and $|\mathrm{B}| = \phi$. The electrical buses with at least a PMU can be represented by a finite set C = $\{\mathrm{Bus}_1, \mathrm{Bus}_2 \ldots, \mathrm{Bus}_\kappa\}$ such that C $\subseteq \{\mathrm{Bus}_1, \mathrm{Bus}_2 \ldots, \mathrm{Bus}_K\}$, and $|\mathrm{C}| = \kappa$.

Further, a $\mathrm{PMU}_{i\in\{1,2\ldots,\theta\}} : \mathrm{PMU}_i \in \mathrm{A} = \{\mathrm{PMU}_1, \mathrm{PMU}_2 \ldots, \mathrm{PMU}_\theta\}$ is located on a $\mathrm{Bus}_{k\in\{1,2\ldots,\kappa\}} : \mathrm{Bus}_\kappa \in \{\mathrm{Bus}_1, \mathrm{Bus}_2 \ldots, \mathrm{Bus}_K\}$. Hence, in terms of the corresponding bus location, a PMU can be represented as $\mathrm{PMU}^{k\in\{1,2\ldots,\kappa\}}_{i\in\{1,2\ldots,\theta\}}$. Similarly, a $\mathrm{PDC}_{j\in\{1,2\ldots,\phi\}} : \mathrm{PDC}_j \in \mathrm{B} = \{\mathrm{PDC}_1, \mathrm{PDC}_2 \ldots, \mathrm{PDC}_\phi\}$ can be represented in terms of its bus location as $\mathrm{PDC}^{k\in\{1,2\ldots,\kappa\}}_{j\in\{1,2\ldots,\phi\}}$ where $\mathrm{Bus}_{k\in\{1,2\ldots,\kappa\}} : \mathrm{Bus}_\kappa \in \{\mathrm{Bus}_1, \mathrm{Bus}_2 \ldots, \mathrm{Bus}_K\}$.

It is worthwhile to recall that a single PDC acts as a data aggregator for multiple PMUs. A PDC observable set β_{PDC_j} can be defined as a collection of all PMUs which communicate their synchrophasor data to a particular PDC i.e., PDC_j. A PDC observable set and its element are given by Equation (1).

$$\mathrm{PMU}^{k\in\{1,2,\ldots,\kappa\}}_{i\in\{1,2,\ldots,\theta\}} \in \beta_{PDC_j};\ \text{if } \mathrm{PMU}^{k\in\{1,2,\ldots,\kappa\}}_{i\in\{1,2,\ldots,\theta\}} \text{ communicates its synchrophasor data to } \mathrm{PDC}^{k\in\{1,2,\ldots,\kappa\}}_{j\in\{1,2,\ldots,\phi\}} \tag{1}$$

Nevertheless, a PMU observable set λ_{PMU_i} can be defined such that it is a collection of all electrical buses which can simultaneously be monitored by a PMU_i. A PMU observable set and its elements are given by Equation (2).

$$\left.\begin{array}{l}\text{if } k = k' \text{ or} \\ \text{if } \mathrm{PMU}_{i\in\{1,2,\ldots,\theta\}}^{k\in\{1,2,\ldots,\kappa\}} \text{ can monitor } \mathrm{Bus}_{k'}\end{array}\right\} \text{then } \mathrm{Bus}_{k'} \in \lambda_{PMU_i}, \mathrm{Bus}_k \in \lambda_{PMU_i} \tag{2}$$

For example, if $\mathrm{PMU}_1^{k\in\{1,2,\ldots,\kappa\}}$, $\mathrm{PMU}_3^{k\in\{1,2,\ldots,\kappa\}}$, and $\mathrm{PMU}_4^{k\in\{1,2,\ldots,\kappa\}}$ treat $\mathrm{PDC}_2^{k\in\{1,2\ldots,\kappa\}}$ as a data aggregator, then the PDC observable set β_{PDC_2} is given as $\beta_{PDC_2} = \left\{\mathrm{PMU}_1^{k\in\{1,2,\ldots,\kappa\}}, \mathrm{PMU}_3^{k\in\{1,2,\ldots,\kappa\}}, \mathrm{PMU}_4^{k\in\{1,2,\ldots,\kappa\}}\right\}$. For a $\mathrm{PMU}_6^{k\in\{1,2,\ldots,\kappa\}}$ installed on Bus_2, if Bus_1, Bus_4, and Bus_5 can simultaneously be monitored then the PMU observable set λ_{PMU_6} can be given as $\lambda_{PMU_6} = \{\mathrm{Bus}_1, \mathrm{Bus}_2, \mathrm{Bus}_4, \mathrm{Bus}_5\}$.

Since the SCN is designed in an optimal way in terms of PMUs placement on electrical buses, the following inequalities hold valid.

$$\left.\begin{array}{l}\lambda_{PMU_i} \neq \mathrm{C}; \lambda_{PMU_i} \subset \mathrm{C} \\ \beta_{PDC_j} \neq \mathrm{A}; \beta_{PDC_j} \subset \mathrm{A}\end{array}\right\} \tag{3}$$

3.2. Design of Hybrid SCN

The objective of hybrid SCN is to communicate synchrophasor data from PMUs to the PDC, which can then be further utilized by remotely located control center to monitor and protect the SG in real-time. For synchrophasor data, PMUs are used which are installed over several electrical buses in a substation. A PMU monitors the vital buses parameters such as voltage, currents, frequency, rate of change of frequency, phase angle, etc.; and these measurements are time-synchronized using Global Positioning System data before being sent to the PDC for visualization at the control center. Presently, a generic architecture of the hybrid SCN is presented in this section that can be used to facilitate synchrophasor data exchanged between optimally distributed PMUs and PDCs.

The prime constituents of the hybrid SCN are PMUs, PDCs, and the core communication infrastructure. The Internet Protocol (IP) network is considered to be the core communication infrastructure. The hybrid SCN is shown in Figure 1, where hybrid network topologies are used. The PMUs are connected over a Wireless Local Area Network (WLAN) in which all devices such as End Devices (ED), PMU, etc. use wireless interfaces such as WiFi to connect to the WLAN network. On the other hand, the PDC and the other EDs at the control center use wired interfaces such as Ethernet to connect to the network. Such network is simply referred to as an LAN. In a SCN, there are several geographically distributed PMUs. Thus, a WLAN can be introduced to accommodate each PMU, which results in θ number of WLANs. Both WLAN as well as LAN are considered to be shared networks, since the communication resources are shared among all devices such as PMUs, PDCs, EDs, etc. The WLANs, and LANs are connected using Wide Area Network (WAN) based on IP network topology.

With respect to the interfacing, the devices on WLAN use WiFi based on IEEE 802.11 protocols for data communication over an IP network. Alternatively, LAN uses Ethernet based IEEE 802.3 protocols for data communication. The IP network is meant to facilitate the communication of data from the EDs using different application layer protocols such as HTTP, FTP, TFTP, TELNET, etc. The existing IP network has not evolved to support synchrophasor data communication from PMUs and PDCs, however. Thus, a communication framework is required to achieve compatibility between synchrophasor data and the IP network. In this context, IEEE developed IEEE C37.118 standards in two parts: IEEE C37.118.1 and IEEE C37.118.2 in 2011 [34].

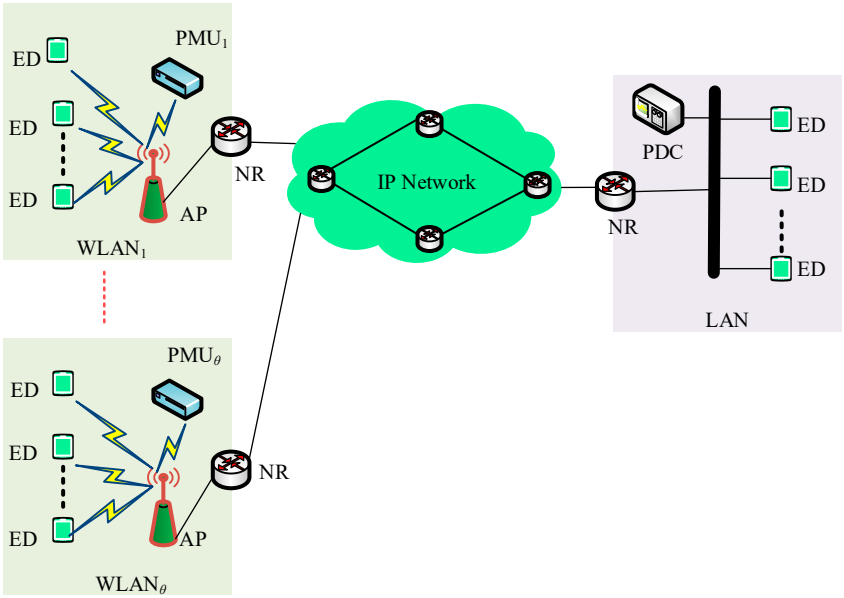


Figure 1. Design of hybrid SCN.

The IEEE C37.118.1 (also known as IEEE C37.118.1-2011) standards define parameters of synchrophasor measurements such as input/output quantities, phasor measurements, ROCOF, frequency, evaluation of synchrophasor measurements, evaluation of measurements compliance, etc. [35]. Alternatively, the communication of synchrophasor data among different power system components, including PMUs and PDCs, is governed by the IEEE C37.118.2 (also known as IEEE C37.118.2-2011) standard [36]. Particularly, it describes messaging including types, use, contents, and data formats for real-time communication between PMUs and PDCs, in addition to the other power system equipment for different synchrophasor applications. This standard governs a communication framework that can use an IP network as a communication infrastructure for synchrophasor applications. It is worthy to note that this standard only defines message formatting applicable to the application layer of the TCP/IP protocol suite, and does not define any other layer protocols of the TCP/IP. Thus, no restriction related to the physical and data link layer (in terms of communication media), transport layer (in terms of transport protocols such as TCP, UDP, etc.) are implied by IEEE C37.118 standards [37].

The combined efforts of IEEE and IEC led to the development of IEEE/IEC 60255-118-1-2018 standards in 2018, which superseded IEEE C37.118.1 standard [38]. Further, in 2019, IEEE has instituted the IEEE C37.247-2019 standard, which defines functionality, performance requirements, performance metrics including latency, throughput, etc. of the PDC [39]. In this standard, the detailed mechanism for aggregating, processing and handling of synchrophasor data at PDC from several PMUs are presented.

4. Comprehensive Resiliency Analysis Framework

Having traced an overview of the design of a hybrid SCN, we can now develop a resiliency analysis framework for the designed hybrid SCN. In this section, we proceed to institute a resiliency analysis framework for the hybrid SCN. Firstly, a resiliency framework will be presented, followed by the resiliency metrics for resiliency analysis of the hybrid SCN.

4.1. Resiliency Framework

The resiliency of a SCN is its ability to adapt, configure, and respond to contingencies in order to maintain its intended performance. A contingency arises in response to a disturbance (internal or external) which may deviate the system from its normal operation. If the performance of a SCN can be denoted as '*P*', then the performance before the

contingency (in ideal condition) and after the recovery can be expressed as 'P_{ideal}', and 'P_{rec}' respectively. Moreover, the performance at the time of contingency is not necessarily the same as in ideal condition. Thus, 'P_{cont}' can be used to denote performance at the time of contingency.

To ensure real-time protection and control of the SG using SCN, the system performance must be measured with respect to time. Let us consider that a disturbance occurs at time 't_{cont}' leading to contingency. The resiliency operation begins at time 't_{deg}' which avoids further degradation in the system performance. At some time 't_{rec}', which is referred to as a time of recovery, the system begins its recovery. Thus, the system performance starts improving from time 't_{rec}'. The system completely recovers at time 't_{full}' as a measure of resiliency.

The resiliency operation of the SCN can be further described by different states of the systems. The state prior to the contingency is referred to as fully operational state where performance of the system is measured by P_{ideal} (in ideal condition) or P_{cont} The performance of the system degrades when contingency occurs, which results in degradation of the system performance. This state can be referred to as a degradation state. The resiliency function becomes operational in response to a contingency which restricts further degradation of the system after a certain level. Of note, the system can be said still to be operational under such level, but with the least performance index. Such a state is referred to as a partial operational state in which the system performance can be regarded as threshold performance, and denoted as 'P_{th}'. As a result of resiliency, the system starts recovery from partial operational state towards fully operational state. The transition state between the partial operational state and the fully operational state is referred to as the recovery state.

The instantaneous performance of the system is used as a Figure of Merit (FoM) to describe the system's resilient behaviors in response to contingencies. The instantaneous performance of the system as a function of time can be denoted as 'P_{inst}'. The different states of a resilient system are shown using Figure 2. As shown in the figure, the disturbance occurs at time t_{cont} where the performance is measured as $FoM = P_{ideal} = P_{cont}$. Thus, degradation of the performance starts at time t_{cont} and the system enters into a degradation state in which the performance is measured by its instantaneous value, given as $FoM_{inst} = P_{inst}$. In response to contingency, the resiliency function becomes operational, which restricts performance degradation to its threshold value P_{th} at time t_{deg}. Due to resiliency, the system starts recovering from the partially operational state at time t_{rec} and enters into recovery state, in which the performance is measured by its instantaneous value given as $FoM_{inst} = P_{inst}$. The system recovers to a fully operational state at time t_{full} with $FoM = P_{rec}$. If the system fails to maintain the threshold performance metric i.e., $FoM < P_{th}$, then such a state is referred to as a failed state and the system ceases to be operational. A failed state is observed for t_{fail} with $FoM = P_{inst} < P_{th}$

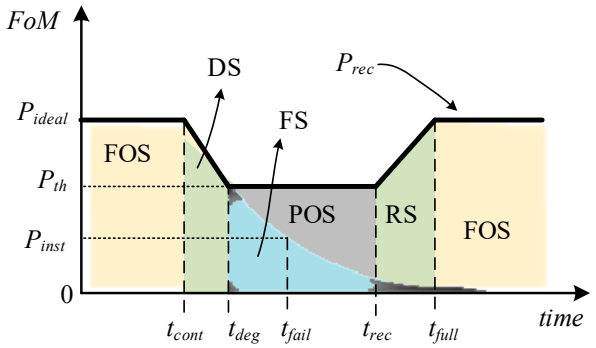


Figure 2. A typical resiliency curve. Here, FOS: fully operational state, POS: partially operational state, DS: degradation state, and RS: recovery state.

4.2. Resiliency Metric

The performance of the system primarily depends on two key factors: hardware reliability and data reliability. The hardware reliability measures the availability of individual components of the system such that they remain functional in order to make the system fully operational. Another key factor for determining the performance of the system is data reliability, which reflects the number of successful packets at the destination compared to the packets transmitted by the source. Thus, for measuring the system performance, both of the factors, i.e., hardware reliability and data reliability are considered as FoM. The FoM which is used to reflect the system performance can be given by Equation (4).

$$FoM = R \times PDR \tag{4}$$

where, R represents the hardware reliability, and PDR represents Packet Delivery Ratio (PDR) which measures the data reliability. The instantaneous resiliency in terms of instantaneous FoM (FoM_{inst}) and ideal FoM (FoM_{ideal}) can be defined by Equation (5).

$$\Re_{inst} = FoM_{ideal} - \left| \frac{FoM_{ideal} - FoM_{inst}}{FoM_{ideal}} \right| \tag{5}$$

The system that has recovered from disturbance does not necessarily perform the same as it performed before the disturbance. Thus, there exists a performance gap between before the disturbance and after the disturbance. The resiliency based on such a performance gap can be measured in terms of the net resiliency, which is given by Equation (6).

$$\Re_{net} = FoM_{cont} - \left| \frac{FoM_{cont} - FoM_{rec}}{FoM_{cont}} \right| \tag{6}$$

Further, the degradation rate, which measures the system ability to degrade in response to contingency without resilient action in force, can be given by Equation (7).

$$\xi_{\text{deg}} = \frac{FoM_{t_i} - FoM_{t_j}}{t_i - t_j} \tag{7}$$

where, FoM_{t_i} represents instantaneous FoM at time t_i. In particular, t_{i} and t_{j} represents contingency start time (t_{cont}) and mitigation start time (t_{deg}). Moreover, the recovery rate which measures the system's ability to recover to operational state in response to contingency with resilient action in force can be given by Equation (8).

$$\xi_{rec} = \frac{FOM_{t_k} - FOM_{t_l}}{t_k - t_l} \tag{8}$$

In particular, t_k and t_l represent recovery start time (t_{rec}) and recovered time (t_{full}).

5. Parameters for Resiliency Analysis of Hybrid SCN

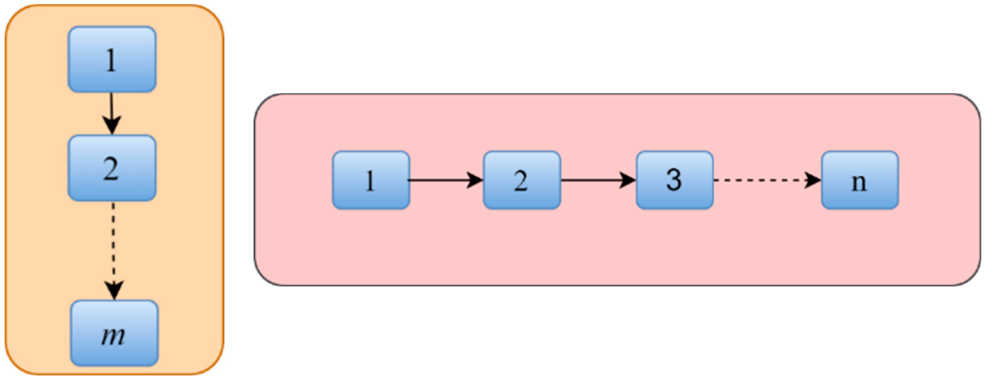
In this section, we institute several parameters to develop a resiliency analysis framework. Based on these parameters, resiliency analysis of a hybrid SCN can be performed. For the resiliency analysis, two key parameters are considered, which are hardware reliability and data reliability. The hardware reliability is measured in terms of a device's availability to perform the intended function while deployed in the network. The hardware reliability analysis is presented in this section. The data reliability, however, is based on simulation approach which will be discussed in a later section.

5.1. Reliability Analysis of Series and Parallel Configures System

Consider that there are n components connected with series configuration and m components connected with parallel configuration as shown in Figure 3. If R_l represents

the hardware reliability of l^{th} components such that $l \in \{1, 2, \ldots, n\}$, then the hardware reliability of such a series configuration system can be given by using (9).

$$R_s = \prod_{l=1}^{n} R_l \tag{9}$$



(**a**) (**b**)

Figure 3. A system with: (**a**) m components in series configuration, and (**b**) n components in parallel configurations.

Similarly, if R_x represents the hardware reliability of x^{th} components such that $x \in \{1, 2, \ldots, m\}$, then the hardware reliability of such a parallel configuration system can be evaluated using (10).

$$R_p = 1 - \prod_{l=1}^{m}(1 - R_x) \tag{10}$$

5.2. Hardware Reliability for Hybrid SCN

To measure hardware reliability, a SCN corresponding to one pair of PMU and PDC can be considered, which is shown in Figure 4.

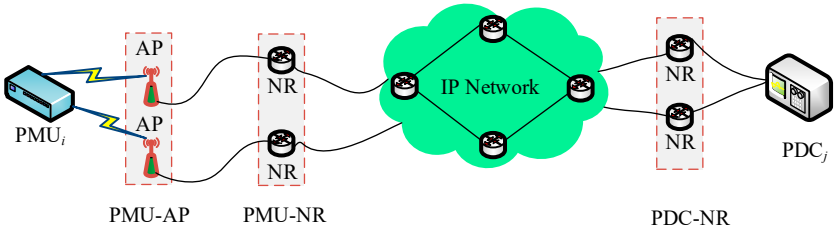


Figure 4. A one-pair reliable hybrid SCN with components in redundancy configurations.

The redundant configuration of AP and NR routers is used in WLAN corresponding to the PMU for reliability enhancement. Likewise, redundant configuration of NRs are used in LAN corresponding to the PDC at the control center for reliability enhancement. The hardware reliability of such a one-pair SCN can be given as:

$$R_{\mathrm{PMU}_i-\mathrm{PDC}_j} = R_{\mathrm{PMU}_i} \times \left\{1 - (1 - R_{\mathrm{AP}})^2\right\} \times \left\{1 - (1 - R_{\mathrm{NR}})^2\right\}^2 \times R_{\mathrm{PDC}_j} \times R_{\mathrm{IP}} \tag{11}$$

where reliability of $\mathrm{PMU}_{i\in\{1,2\ldots,\theta\}}^{k\in\{1,2\ldots,\kappa\}}$, $\mathrm{PDC}_{j\in\{1,2\ldots,\phi\}}^{k\in\{1,2\ldots,\kappa\}}$, AP, NR and IP network are represented as R_{PMU_i}, R_{PDC_j}, R_{AP}, R_{NR}, and R_{IP}.

For the hybrid SCN with $\mathrm{PMU}_{i\in\{1,2\ldots,\theta\}} : \mathrm{PMU}_i \in A = \{\mathrm{PMU}_1, \mathrm{PMU}_2 \ldots, \mathrm{PMU}_\theta\}$ and $\mathrm{PDC}_{j\in\{1,2\ldots,\phi\}} : \mathrm{PDC}_j \in \mathrm{B} = \{\mathrm{PDC}_1, \mathrm{PDC}_2 \ldots, \mathrm{PDC}_\phi\}$ such that $\mathrm{Bus}_{k\in\{1,2\ldots,\kappa\}}$:

$\text{Bus}_\kappa \in \{\text{Bus}_1, \text{Bus}_2 \ldots, \text{Bus}_K\}$, the average reliability of hybrid SCN can be obtained using Equation (12).

$$R_{HySCN} = \frac{\sum_{j=1}^{\phi} \sum_{i=1}^{\theta} R_{\text{PMU}_i - \text{PDC}_j}}{\sum_{j=1}^{\phi} \left| \beta_{\text{PDC}_j} \right|} \tag{12}$$

The hardware reliability of the prime constituents of hybrid SCN can be considered from [40]. Thus, with $R_{\text{PMU}} = 0.9983$, $R_{\text{PDC}} = 1$, $R_{\text{AP}} = 0.9999697$, $R_{\text{NR}} = 0.99985$, and $R_{\text{IP}} = 0.99$, the hardware reliability of hybrid SCN having similar topologies of all one-pair hybrid SCN is obtained as 0.988316.

5.3. Data Reliability of Hybrid SCN

The data reliability is measured in terms of PDR which represents a ratio of number of packets received at the PDC and number of packets sent by a PMU. If a hybrid SCN with a PMU and a PDC is considered, then the PDR corresponding to one pair of PMU and PDC can be given by Equation (13).

$$PDR_{\text{PMU}_{i\in\{1,2,\ldots,\theta\}}^{k\in\{1,2,\ldots,\kappa\}} - \text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}} = \frac{\sum_{t=\tau_0}^{t=\tau_\infty} RP_{\text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}}(t)}{\sum_{t=\tau_0}^{t=\tau_\infty} SP_{\text{PMU}_{i\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}}(t)} \tag{13}$$

where, $RP_{\text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}}$, and $SP_{\text{PMU}_{i\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}}$ represent instantaneous values of the number of received packets at $\text{PDC}_{j\in\{1,2\ldots,\phi\}}^{k\in\{1,2\ldots,\kappa\}}$, and the number of sent packets at $\text{PMU}_{i\in\{1,2\ldots,\theta\}}^{k\in\{1,2\ldots,\kappa\}}$ with time ranging from starting time τ_0 and final time τ_∞. It is worthy to note that the Equation (13) can be extended to calculate the PDR corresponding to any PMUs and PDCs in the hybrid SCN.

5.4. Resiliency Metrics for Hybrid SCN

Hardware reliability and PDR metrics can be used for evaluation of resiliency of a hybrid SCN. Since the hybrid SCN is analyzed for a short span of time, the instantaneous hardware reliability $R(t_{inst})_{HySCN}$ can be assumed to be independent of the time. Hence, we can represent instantaneous hardware reliability of hybrid SCN as $R(t_{inst})_{HySCN} = R_{HySCN}$. In accordance with the instantaneous performance measurements, the instantaneous PDR corresponding to a $\text{PMU}_{i\in\{1,2\ldots,\theta\}}$: $\text{PMU}_i \in A = \{\text{PMU}_1, \text{PMU}_2 \ldots, \text{PMU}_\theta\}$ and a $\text{PDC}_{j\in\{1,2\ldots,\phi\}}$: $\text{PDC}_j \in \text{B} = \{\text{PDC}_1, \text{PDC}_2 \ldots, \text{PDC}_\phi\}$ can be represented as $PDR(t_{inst})_{\text{PMU}_{i\in\{1,2,\ldots,\theta\}}^{k\in\{1,2,\ldots,\kappa\}} - \text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}}$. Hence, the instantaneous FoM ($FoM_{HySCN(t_{iinst})}$) for resiliency estimation of hybrid SCN corresponding to a $\text{PMU}_{i\in\{1,2\ldots,\theta\}}$: $\text{PMU}_i \in A = \{\text{PMU}_1, \text{PMU}_2 \ldots, \text{PMU}_\theta\}$ and a $\text{PDC}_{j\in\{1,2\ldots,\phi\}}$: $\text{PDC}_j \in \text{B} = \{\text{PDC}_1, \text{PDC}_2 \ldots, \text{PDC}_\phi\}$ can be given by Equation (14) using Equation (4).

$$FoM_{HySCN(t_{iinst})} = R_{HySCN} PDR(t_{inst})_{\text{PMU}_{i\in\{1,2,\ldots,\theta\}}^{k\in\{1,2,\ldots,\kappa\}} - \text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}} \tag{14}$$

Using (5), the instantaneous resiliency of the hybrid SCN corresponding to a $\text{PMU}_{i\in\{1,2\ldots,\theta\}}$: $\text{PMU}_i \in A = \{\text{PMU}_1, \text{PMU}_2 \ldots, \text{PMU}_\theta\}$ and a $\text{PDC}_{j\in\{1,2\ldots,\phi\}}$: $\text{PDC}_j \in \text{B} = \{\text{PDC}_1, \text{PDC}_2 \ldots, \text{PDC}_\phi\}$ can be expressed by Equation (15).

$$\Re_{inst} = FoM_{ideal} - \left| \frac{FoM_{ideal} - R_{HySCN} PDR(t_{inst})_{\text{PMU}_{i\in\{1,2,\ldots,\theta\}}^{k\in\{1,2,\ldots,\kappa\}} - \text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}}}{FoM_{ideal}} \right| \tag{15}$$

For the hybrid SCN with $\text{PMU}_{i\in\{1,2\ldots,\theta\}} : \text{PMU}_i \in A = \{\text{PMU}_1, \text{PMU}_2 \ldots, \text{PMU}_\theta\}$ and $\text{PDC}_{j\in\{1,2\ldots,\phi\}} : \text{PDC}_j \in \text{B} = \{\text{PDC}_1, \text{PDC}_2 \ldots, \text{PDC}_\phi\}$, the instantaneous resiliency is given by Equation (16).

$$\Re_{inst} = FoM_{ideal} - \left| \frac{FoM_{ideal} - R_{HySCN} \frac{\prod_{j=1}^{\phi}\prod_{i=1}^{\theta} PDR(t_{inst})_{\text{PMU}_{i\in\{1,2,\ldots,\theta\}}^{k\in\{1,2,\ldots,\kappa\}} - \text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}}}{\sum_{j=1}^{\phi}\left|\beta_{\text{PDC}_j}\right|}}{FoM_{ideal}} \right| \tag{16}$$

Moreover, the net resiliency of the hybrid SCN with $\text{PMU}_{i\in\{1,2\ldots,\theta\}} : \text{PMU}_i \in A = \{\text{PMU}_1, \text{PMU}_2 \ldots, \text{PMU}_\theta\}$ and $\text{PDC}_{j\in\{1,2\ldots,\phi\}} : \text{PDC}_j \in \text{B} = \{\text{PDC}_1, \text{PDC}_2 \ldots, \text{PDC}_\phi\}$ can be expressed using Equation (17) where $PDR(t_{rec})_{\text{PMU}_{i\in\{1,2,\ldots,\theta\}}^{k\in\{1,2,\ldots,\kappa\}} - \text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}}$ is given by Equation (18).

$$\Re_{net} = FoM_{cont} - \left| \frac{FoM_{cont} - R_{HySCN} PDR(t_{rec})_{\text{PMU}_{i\in\{1,2,\ldots,\theta\}}^{k\in\{1,2,\ldots,\kappa\}} - \text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}}}{FoM_{cont}} \right| \tag{17}$$

$$PDR(t_{rec})_{\text{PMU}_{i\in\{1,2,\ldots,\theta\}}^{k\in\{1,2,\ldots,\kappa\}} - \text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}} = \frac{\prod_{j=1}^{\phi}\prod_{i=1}^{\theta} PDR(t_{rec})_{\text{PMU}_{i\in\{1,2,\ldots,\theta\}}^{k\in\{1,2,\ldots,\kappa\}} - \text{PDC}_{j\in\{1,2,\ldots,\phi\}}^{k\in\{1,2,\ldots,\kappa\}}}}{\sum_{j=1}^{\phi}\left|\beta_{\text{PDC}_j}\right|} \tag{18}$$

6. Resiliency Analysis of Hybrid SCN

6.1. Simulation Framework

The proposed resiliency framework can be deployed for the SCN for results validation and analysis. To design the SCN, a practical power grid of West Bengal, India, has been considered as a case study. The bus topology of the practical power grid to be considered as a case study is shown in Figure 5. The power grid consists of 24 buses where 7 PMUs are optimally placed to cover the entire power grid. The power grid is comprised of only one PDC to aggregate data from seven PMUs. The geographical distribution of the PMUs and PDCs are reported in Table 1.

The resiliency FoM is based on two key factors: hardware reliability and data reliability. The hardware reliability can be estimated for the designed SCN pertaining to the case study using the methodology presented in Section 5.2. For the case study with one-pair hybrid SCN having similar characteristics, the hardware reliability is obtained to be 0.988316.

Further, in order to obtain the PDR, the hybrid SCN pertaining to the case study is implemented in QualNet network simulator. The rationality behind choosing QualNet as a network simulator is its wide adoption across several governments, academic, commercial, and non-commercial organizations due to its high accuracy and industry standards [41]. Some of the key simulation parameters are reported in Table 2. The coordinate system is choosen for the West Bengal's practical power grid comprising 24-bus system such that the Southwest (SW) corner = 20.21°, Northeast (NE) corner = 30.41° for latitude; and Southwest (SW) corner = 73.57°, Northeast (NE) corner = 94.44° for longitude. The node placements for PMUs and PDCs are done in accordance with their locations as reported in Table 1. An altitude of 1500 m above mean sea level and 0 m below mean sea level is considered. To mimic the dynamic environmental conditions, a weather mobility of 98 ms is considered. Since the nodes corresponding to end devices (ED) other than PMUs and PDCs can be of mobile in nature, the random walk mobility model for such nodes are considered in

the QualNet. The nodes corresponding to PMUs and PDCs, however, do not follow any mobility model.

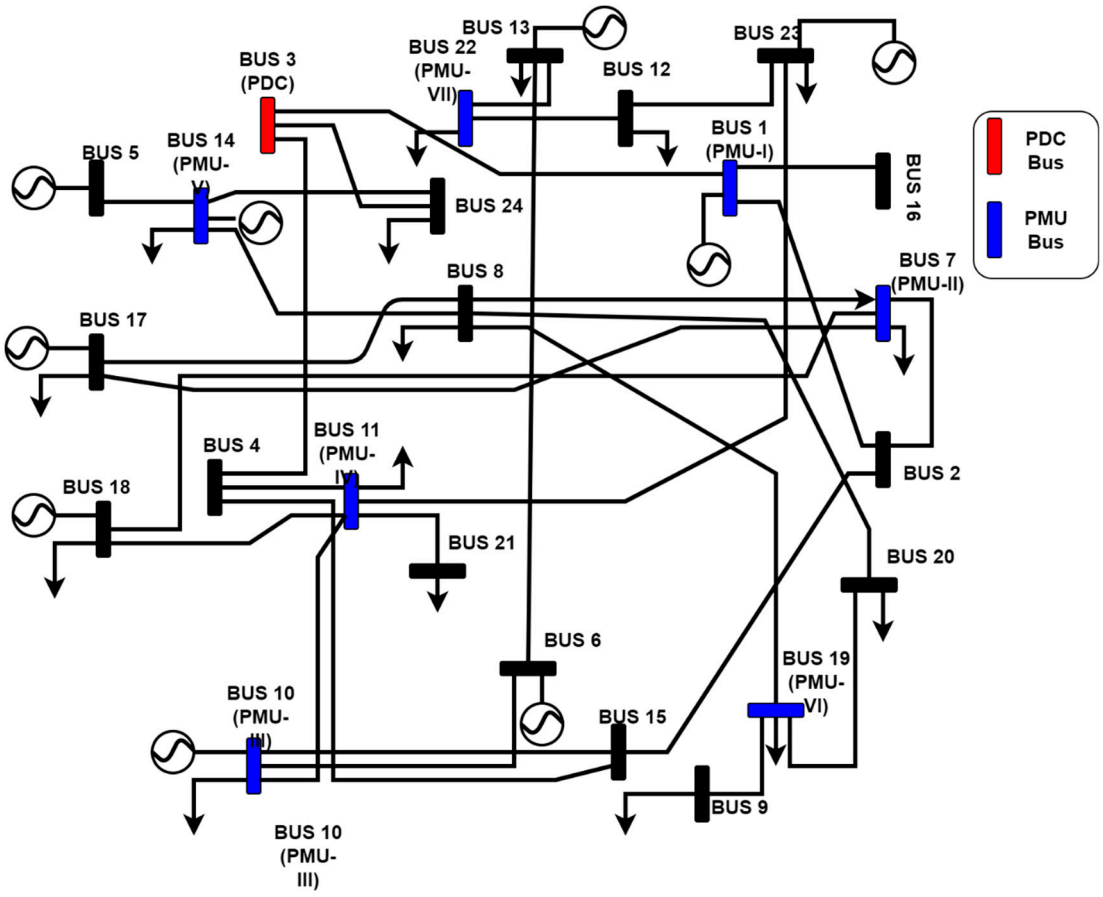


Figure 5. Bus topology for practical power grid of West Bengal, India.

Table 1. Geographical distribution of PMUs and PDCs.

Bus with a PMU	ID of PMU/PDC	Bus Locations		Distance from PDC (Km)
		Latitude	Longitude	
Bus-1	PMU-1	24.7828	87.9041	154.11
Bus-3	PDC-1	23.4814	87.4464	-
Bus-7	PMU-2	22.7494	88.5417	141.03
Bus-10	PMU-3	22.4442	87.8672	124.07
Bus-11	PMU-4	22.8361	87.9594	90.78
Bus-14	PMU-5	22.3997	88.2177	145.61
Bus-19	PMU-6	22.1188	88.3319	177.71
Bus-22	PMU-7	25.8502	87.8500	265.57

6.2. Simulation Results and Discussions

To enable the attack scenario which occurs in a real-time environment, the attacks on PMUs are required to be configured. Further, it is very unlikely that all PMUs will be affected simultaneously. Thus, for the resiliency analysis, about 50% of the PMUs i.e., four PMUs are modelled with DoS attack. The DoS attack is configured to capture all probabilistic impacts on SCNs, such as low degradation time, high degradation time, equal degradation and recovery time, and random degradation and recovery time. The simulations are performed to analyze the PDR corresponding to each PMU for the resiliency analysis of the hybrid SCN pertaining to the case study. The simulations are performed for

300 s of simulation time to record FoM for the resiliency calculation. The resiliency curve from simulation results with DoS attack on PMU_1, PMU_2, PMU_3, and PMU_4 are plotted in Figures 6a, 6b, 6c and 6d, respectively.

Table 2. Simulations parameters.

Parameters	Values	
Coordinate System	Latitude	Longitude
	SW Corner = 20.21 **NE Corner = 30.41**	**SW Corner = 73.57** **NE Corner = 94.44**
Altitude	1500 m above mean sea level 0 m below mean sea level	
Weather mobility	98 ms	
Node placement	As per geographical distribution of PMUs and PDCs	
Mobility model	Random walk for EDs	

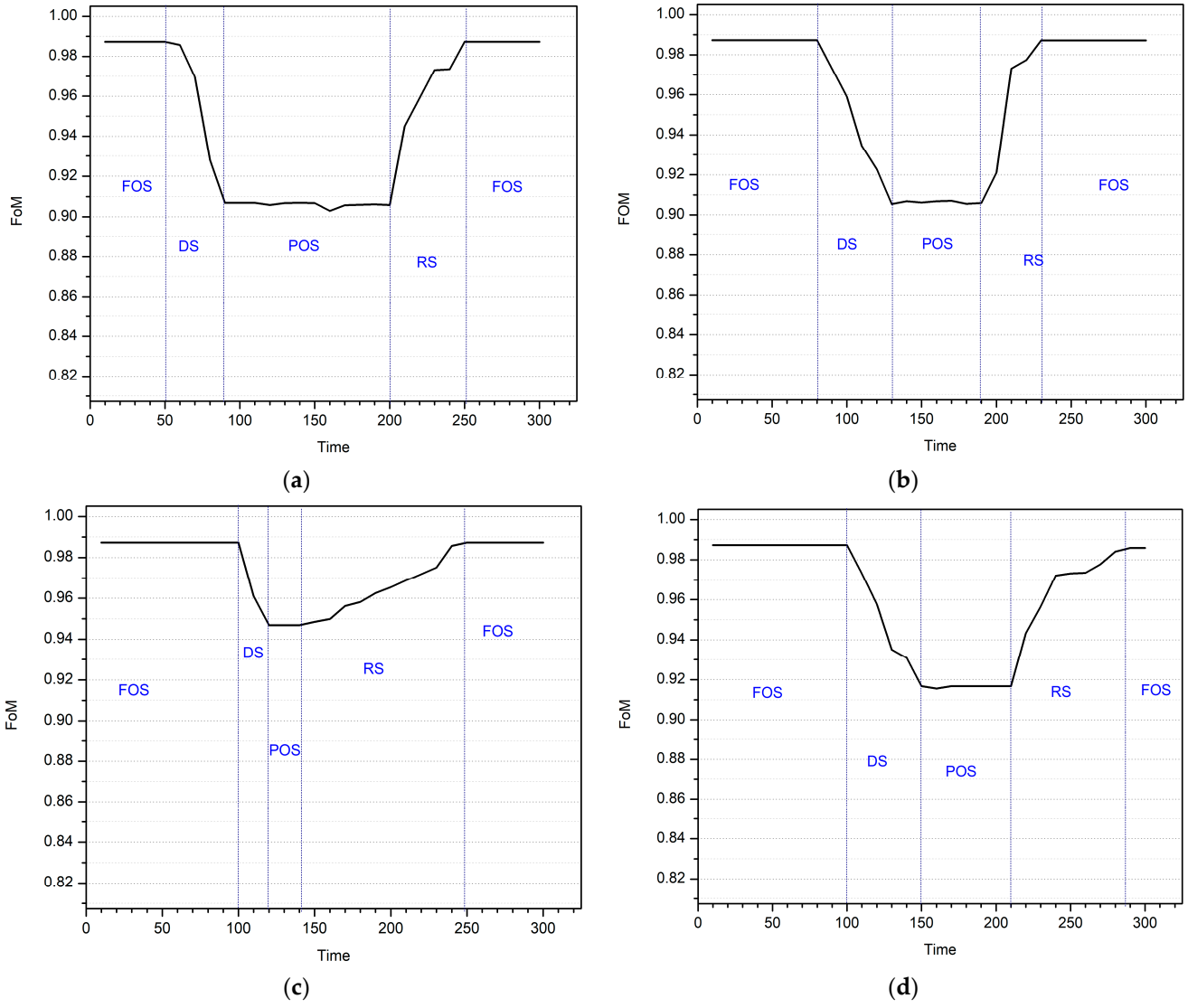


Figure 6. Resiliency performance of hybrid SCN with DoS attack on: (**a**) PMU_1, (**b**) PMU_2, (**c**) PMU_3 and (**d**) PMU_4.

Since comprehensive parametric analyses are important for the purpose of analysis, some of the vital parameters for resiliency analysis of the hybrid SCN are recorded in Table 3. The performance (in terms of PDR) of vulnerable PMUs i.e., PMU_1, PMU_2, PMU_3, and PMU_4 are observed for degradation state as well as recovery state in addition to the instantaneous FoM of the hybrid SCN. In degraded states, the PDR of vulnerable PMUs are noted prior to the disturbance occurrence i.e., P_{cont} at t_{cont}, and when mitigation started P_{deg} at t_{deg}. On the other hand, performance of vulnerable PMUs in the recovery state are also recorded at the point when recovery starts i.e., P_{rec} at t_{rec} and after recovery i.e., P_{full} at t_{full}. To be noted, the instantaneous FoM is obtained for the hybrid SCN pertaining to the case study for all these timing instances.

Table 3. Simulation results for hybrid SCN pertaining to the case study.

PMU with DoS Attack	Degradation State						Recovery State					
	P_{cont}	*FoM*	t_{cont}	P_{deg}	*FoM*	t_{deg}	P_{rec}	*FoM*	t_{rec}	P_{full}	*FoM*	t_{full}
PMU_1	0.987639	0.985745	50	0.429894	0.906998	90	0.698939	0.944984	200	0.998939	0.987341	250
PMU_2	0.897155	0.973222	80	0.427155	0.906863	130	0.527155	0.920982	190	0.996521	0.987251	230
PMU_3	0.998939	0.987341	90	0.712439	0.946890	110	0.712439	0.946890	130	0.998939	0.987341	240
PMU_4	0.899277	0.973222	100	0.491277	0.915617	150	0.499299	0.916750	200	0.989277	0.985929	280

The instantaneous resiliency (with $FoM_{ideal} = 1$), net-resiliency, degradation rate, and recovery rate for all the cases are reported in Table 4. For a high-resiliency operation, the hybrid SCN must have low degradation rate and high recovery rate under disturbances. It is observed that the minimum performance degradation under disturbance is observed to be for PMU_4 such that $\xi_{\text{deg}} = -1.15$. Further, the maximum recovery rate as a result of resiliency actions is observed for PMU_2 with DoS such that $\xi_{rec} = 1.66$. Moreover, the net resiliency of the hybrid SCN pertaining to the case study is observed to be greater than 98.628% for all the cases.

Table 4. Resiliency parameters for the hybrid SCN pertaining to the case study.

PMU with DoS Attack	Degradation State				Recovery State				$\Re_{net}$	ξ_{deg} (per ms)	ξ_{rec} (per ms)
	t_{cont}	$\Re_{inst}$	t_{deg}	$\Re_{inst}$	t_{rec}	$\Re_{inst}$	t_{full}	$\Re_{inst}$			
PMU_1	50	0.985745	90	0.906998	200	0.944984	250	0.987341	0.98736	−1.97	0.85
PMU_2	80	0.973222	130	0.906863	190	0.920982	230	0.987251	0.98764	−1.33	1.66
PMU_3	90	0.987341	110	0.946890	130	0.946890	240	0.987341	0.98734	−2.02	0.37
PMU_4	100	0.973222	150	0.915617	200	0.916750	280	0.985929	0.98628	−1.15	0.86

6.3. Resiliency Metrics for WASA

The resiliency metric can play a vital role in the Wide Area Situational Awareness (WASA) of the SG. For WASA, the operator must know the status of the grid to take proactive control actions. The operator also utilizes the previously available grid data in predicting the future state of the grid. Such data should be reliable and must reach the operator in minimum time. The SCN plays an important role in providing high reliability and minimum delay to the data pertaining to grid for its WASA. In order to strengthen this objective, the SCN must be highly resilient, as reliability and delay are correlated with resiliency of the SCN. Thus, one can use the resiliency metric in combination with delay incurred in the synchrophasor data communication over the SCN to institute a WASA metric. The authors would also like to carry the present work to extend the use of resiliency metric for developing a WASA framework for the SG cyber physical system.

6.4. Resiliency Metric for DTR SCN Model

The Dynamic Thermal Rating (DTR) is one of the more widely used technologies used to enhance line ratings of the smart grid system by enforcing the system to work at its maximum ratings [42]. However, the deployment of DTR in SG is dependent on the reliability of the communication network. An important aspect of the reliability enhancement of communication network for the SG cyber physical system with DTR system is presented in [43]; the resiliency and reliability are highly correlated, and thus another paradigm for evaluating resiliency of the SCN with the DTR system might attract the researchers. A brief overview of evaluating resiliency of SCN with DTR system is presented as follows.

A one pair SCN with a PMU and a PDC with a DTR system for resiliency analysis framework is shown in Figure 7. For such a system, the reliability can be obtained using (19). A resiliency framework can be developed based on the methodologies presented in this paper. For evaluation of the efficacy, a test system can be considered. The authors keep the resiliency framework for such SCN system with DTR as an open research problem. The authors also suggest the seminal work by Jimada et. al. [43] to be considered as a reference to proceed on the said research problem.

$$R_{\mathrm{PMU}_i-\mathrm{PDC}_j} = R_{\mathrm{PMU}_i} \times \left\{1-(1-R_{\mathrm{AP}})^2\right\} \times \left\{1-(1-R_{\mathrm{NR}})^2\right\}^2 \times R_{\mathrm{PDC}_j} \times R_{\mathrm{IP}} \times R_{\text{DTR system}} \tag{19}$$

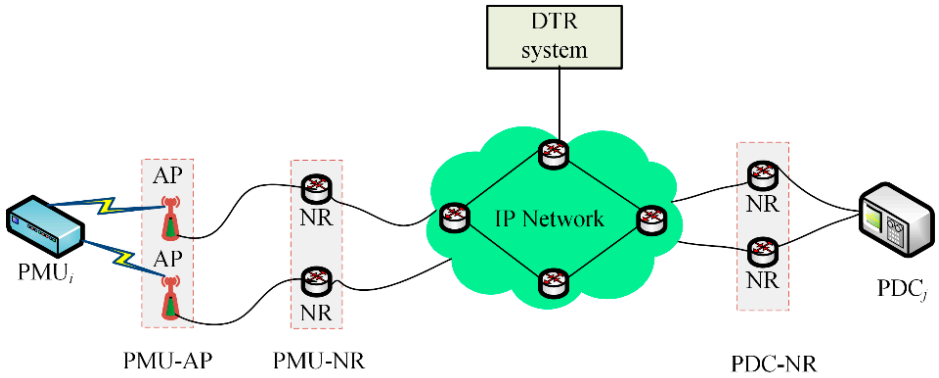


Figure 7. A hybrid SCN with DTR system with a PMU and a PDC for resiliency analysis.

7. Conclusions

The resiliency of SCN is of paramount interest as it uses IP as a communication infrastructure for synchrophasor data communication between PMUs and PDCs, which is vulnerable to security attacks. In this paper, a mathematical modelling is presented for designing a hybrid SCN. Further, a resiliency evaluation framework is proposed for resiliency analysis of SCN. For resiliency analysis, the hardware reliability as well as the data reliability are considered for parameterization of resiliency metrics. The proposed framework is deployed for a practical power grid of India as a case study for which hybrid SCN is designed and its resiliency analysis is performed. The simulation results are carried out for DoS attack on 50% PMUs which includes PMU_1, PMU_2, PMU_3, and PMU_4. When subjected to DoS attack, the performance of PMU_3 is highly affected with $\xi_{\mathrm{deg}} = -2.02$. On the other hand, the least impact in terms of degradation rate is observed for PMU_4 such that $\xi_{\mathrm{deg}} = -1.15$. In terms of recovery in response to DoS attack, PMU_2 recovers quickly to the fully functioning state with $\xi_{rec} = 1.66$, whereas, a significantly higher response time is observed by PMU_3 under the DoS attack, since $\xi_{rec} = 0.37$. Nevertheless, the hybrid SCN is resilient even if 50% of the PMUs are vulnerable to DoS attack, since it achieves a minimum resiliency of 98.628% under all cases. The resiliency analysis of SCN with a DTR system for improving network capacity, which authors intend to include in the model in their future research. Further, the extension of resiliency analysis framework for more general case studies is also kept as a future research problem.

Author Contributions: A.V.J.: Conceptualization, Methodology, Investigation, and Writing—Original draft preparation; A.V.J. and B.A.: Conceptualization, Methodology, Supervision, Writing, Reviewing and Editing, and Validation; D.K.G.: Conceptualization, Methodology, Supervision, Writing—Reviewing and Editing, and Validation; T.S.U.: Conceptualization, Investigation, Supervision, Funding Acquisition, Reviewing and Editing, and Validation. All authors have read and agreed to the published version of the manuscript.

Funding: There is no funding available for this.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. International Energy Outlook 2020. 2020. Available online: https://www.eia.gov/outlooks/ieo/ (accessed on 30 September 2022).
2. Jha, A.V.; Appasani, B.; Ghazali, A.N. Analytical Channel Modelling of Synchrophsor Communication Networks in a Smart Grid Cyber Physical System. In Proceedings of the 2021 3rd Global Power, Energy and Communication Conference (GPECOM), Antalya, Turkey, 5–8 October 2021; pp. 257–262. [CrossRef]
3. Haes Alhelou, H.; Hamedani-Golshan, M.E.; Njenda, T.C.; Siano, P. A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges. *Energies* **2019**, *12*, 682. [CrossRef]
4. Usman, M.U.; Faruque, M.O. Applications of synchrophasor technologies in power systems. *J. Mod. Power Syst. Clean Energy* **2018**, *7*, 211–226. [CrossRef]
5. Chawla, A.; Aftab, M.A.; Hussain, S.S.; Panigrahi, B.K.; Ustun, T.S. Cyber–physical testbed for Wide Area Measurement System employing IEC 61850 and IEEE C37. 118 based communication. *Energy Rep.* **2022**, *8*, 570–578. [CrossRef]
6. Jimada-Ojuolape, B.; Teh, J. Impacts of Communication Network Availability on Synchrophasor-Based DTR and SIPS Reliability. *IEEE Syst. J.* **2021**, 1–12. [CrossRef]
7. Jimada-Ojuolape, B.; Teh, J. Surveys on the reliability impacts of power system cyber–physical layers. *Sustain. Cities Soc.* **2020**, *62*, 102384. [CrossRef]
8. Krishna, R.R.; Priyadarshini, A.; Jha, A.V.; Appasani, B.; Srinivasulu, A.; Bizon, N. State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. *Sustainability* **2021**, *13*, 9463. [CrossRef]
9. Katsaros, K.V.; Yang, B.; Chai, W.K.; Pavlou, G. Low latency communication infrastructure for synchrophasor applications in distribution networks. In Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; pp. 392–397.
10. Appasani, B.; Jha, A.V.; Mishra, S.K.; Ghazali, A.N. Communication infrastructure for situational awareness enhancement in WAMS with optimal PMU placement. *Prot. Control Mod. Power Syst.* **2021**, *6*, 1–12. [CrossRef]
11. Jha, A.V.; Appasani, B.; Ghazali, A.N. A Comprehensive Framework for the Assessment of Synchrophasor Communication Networks from the Perspective of Situational Awareness in a Smart Grid Cyber Physical System. *Technol. Econ. Smart Grids Sustain. Energy* **2022**, *7*, 1–18. [CrossRef]
12. Farooq, S.M.; Hussain, S.M.S.; Kiran, S.; Ustun, T.S. Certificate Based Authentication Mechanism for PMU Communication Networks Based on IEC 61850-90-5. *Electronics* **2018**, *7*, 370. [CrossRef]
13. Farooq, S.M.; Nabirasool, S.; Kiran, S.; Hussain, S.S.; Ustun, T.S. MPTCP based mitigation of denial of service (DoS) attack in PMU communication networks. In Proceedings of the 2018 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Chennai, India, 18–21 December 2019; pp. 1–5.
14. Holling, C.S. Resilience and Stability of Ecological Systems. *Annu. Rev. Ecol. Syst.* **1973**, *4*, 1–23. [CrossRef]
15. Southwick, S.M.; Bonanno, G.A.; Masten, A.S.; Panter-Brick, C.; Yehuda, R. Resilience definitions, theory, and challenges: Interdisciplinary perspectives. *Eur. J. Psychotraumatol.* **2014**, *5*, 25338. [CrossRef] [PubMed]
16. Hosseini, S.; Barker, K.; Ramirez-Marquez, J.E. A review of definitions and measures of system resilience. *Reliab. Eng. Syst. Saf.* **2016**, *145*, 47–61. [CrossRef]
17. Jena, P.K.; Ghosh, S.; Koley, E. Identification of Optimal Sensor Location Based on Trade-Off Approach to Improve Resiliency of Electricity Market in Smart Grid. *IEEE Sens. J.* **2021**, *21*, 17271–17281. [CrossRef]
18. Tushar; Venkataramanan, V.; Srivastava, A.; Hahn, A. CP-TRAM: Cyber-Physical Transmission Resiliency Assessment Metric. *IEEE Trans. Smart Grid* **2020**, *11*, 5114–5123. [CrossRef]
19. Liu, G.; Ben Ollis, T.; Zhang, Y.; Jiang, T.; Tomsovic, K. Robust Microgrid Scheduling With Resiliency Considerations. *IEEE Access* **2020**, *8*, 153169–153182. [CrossRef]
20. Bedoya, J.C.; Wang, Y.; Liu, C.-C. Distribution System Resilience Under Asynchronous Information Using Deep Reinforcement Learning. *IEEE Trans. Power Syst.* **2021**, *36*, 4235–4245. [CrossRef]
21. Borghei, M.; Ghassemi, M.; Liu, C.C. Optimal capacity and placement of microgrids for resiliency enhancement of distribution networks under extreme weather events. In Proceedings of the 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 17–20 February 2020; pp. 1–5.
22. AlMajali, A.; Viswanathan, A.; Neuman, C. Analyzing Resiliency of the Smart Grid Communication Architectures under Cyber Attack. In *CSET 12: Proceedings of the 5th USENIX conference on Cyber Security Experimentation and Test, Bellevue, WA, USA, 6 August 2012*; USENIX Association: Berkeley, CA, USA, 2012.

23. Jakaria, A.H.M.; Rahman, M.A.; Gokhale, A. Resiliency-Aware Deployment of SDN in Smart Grid SCADA: A Formal Synthesis Model. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1430–1444. [CrossRef]
24. Al Mtawa, Y.; Haque, A. Clustering-Coefficient Based Resiliency Approach for Smart Grid. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin City, China, 28 June–2 July 2021; pp. 1569–1574.
25. Ibrahim, M.; Alkhraibat, A. Resiliency Assessment of Microgrid Systems. *Appl. Sci.* **2020**, *10*, 1824. [CrossRef]
26. Saad, A.; Faddel, S.; Youssef, T.; Mohammed, O.A. On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks. *IEEE Trans. Smart Grid* **2020**, *11*, 5138–5150. [CrossRef]
27. Tabar, V.S.; Ghassemzadeh, S.; Tohidi, S. Increasing resiliency against information vulnerability of renewable resources in the operation of smart multi-area microgrid. *Energy* **2021**, *220*, 119776. [CrossRef]
28. Appasani, B.; Jha, A.V.; Swain, K.; Cherukuri, M.; Mohanta, D.K. Resiliency Estimation of Synchrophasor Communication Networks in a Wide Area Measurement System. *Front. Energy Res.* **2022**, *10*, 350. [CrossRef]
29. Jha, A.V.; Appasani, B.; Ustun, T.S. Resiliency assessment methodology for synchrophasor communication networks in a smart grid cyber–physical system. *Energy Rep.* **2022**, *8*, 1108–1115. [CrossRef]
30. Khalkho, A.M.; Mohanta, D.K. Operational Resiliency Enhancement Using Synchrophasor Measurement. In *Advances in Smart Grid Automation and Industry 4.0*; Springer: Singapore, 2021; pp. 613–621.
31. Iftimie, I.A.; Huskaj, G. Strengthening the Cybersecurity of Smart Grids: The Role of Artificial Intelligence in Resiliency of Substation Intelligent Electronic Devices. In Proceedings of the 19th European Conference on Cyber Warfare and Security, a Virtual Conference, University of Chester, Chester, UK, 25–26 June 2020; Academic Conferences and Publishing International Limited: Oxfordshire, UK, 2020; pp. 143–150.
32. Khediri, A.; Laouar, M.R.; Eom, S.B. Enhancing Resiliency Feature in Smart Grids through a Deep Learning Based Prediction Model. *Recent Adv. Comput. Sci. Commun. (Former. Recent Patents Comput. Sci.)* **2020**, *13*, 508–518. [CrossRef]
33. Singh, V.K.; Vaughan, E.; Rivera, J. SHARP-Net: Platform for Self-Healing and Attack Resilient PMU Networks. In Proceedings of the 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 17–20 February 2020; pp. 1–5.
34. Ustun, T.S.; Farooq, S.M.; Hussain, S.M.S. Implementing Secure Routable GOOSE and SV Messages Based on IEC 61850-90-5. *IEEE Access* **2020**, *8*, 26162–26171. [CrossRef]
35. *IEEE Std C37118-2005*; IEEE Standard for Synchrophasor Measurements for Power Systems. IEEE Std C371181-2011 Revis; IEEE: Piscataway, NJ, USA, 2011; pp. 1–61. [CrossRef]
36. *IEEE Std C37118-2005*; IEEE Standard for Synchrophasor Data Transfer for Power Systems. IEEE Std C371182-2011 Revis; IEEE: Piscataway, NJ, USA, 2011; pp. 1–53. [CrossRef]
37. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. IEEE c37. 118-2 synchrophasor communication framework-overview, cyber vulnerabilities analysis and performance evaluation. In Proceedings of the International Conference on Information Systems Security and Privacy, Rome, Italy, 19–21 February 2016; SciTePress: Setúbal, Portugal, 2016; Volume 2, pp. 167–178.
38. *IEC/IEEE 60255-118-1:2018*; IEEE/IEC International Standard-Measuring Relays and Protection Equipment-Part 118-1: Synchrophasor for Power Sys-tems-Measurements. IEEE: New York, NY, USA, 2018; pp. 1–78. [CrossRef]
39. *IEEE Std C37.247-2019*; IEEE Standard for Phasor Data Concentrators for Power Systems. IEEE: New York, NY, USA, 2019; pp. 1–44. [CrossRef]
40. Jha, A.V.; Ghazali, A.N.; Appasani, B.; Ravariu, C.; Srinivasulu, A. Reliability analysis of smart grid networks Iincorporating hardware failures and packet loss. *Rev. Roum. Sci. Tech. El* **2021**, *65*, 245–252.
41. QualNet Network Simulator-Keysight. Available online: https://www.keysight.com/us/en/assets/3122-1395/technical-overviews/QualNet-Network-Simulator.pdf (accessed on 7 November 2022).
42. Metwaly, M.K.; Teh, J. Fuzzy Dynamic Thermal Rating System-Based SIPS for Enhancing Transmission Line Security. *IEEE Access* **2021**, *9*, 83628–83641. [CrossRef]
43. Jimada-Ojuolape, B.; Teh, J. Composite Reliability Impacts of Synchrophasor-Based DTR and SIPS Cyber–Physical Systems. *IEEE Syst. J.* **2022**, *16*, 3927–3938. [CrossRef]